



ATIS-0300008

ATIS Standard on -

**Next Generation Interconnection Interoperability (NGIIF)
Reference Document**

Version 14.0



As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-IP transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [http://www.atis.org/legal/patentinfo.asp] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

Copyright © 2020 by Alliance for Telecommunications Industry Solutions
All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < <http://www.atis.org> >.

Master Table of Contents

TITLE OF EACH PART	PART #	FILE NAME
Table of Contents (this document)	--	--
Installation and Maintenance Responsibilities Special Access Services, WATS Access Lines and Switched Access Services Feature Group A	I	ATIS-0300009
Installation and Maintenance Responsibilities Switched Access Services Feature (Groups B, C, and D)	II	ATIS-0300010
Installation and Maintenance Responsibilities SS7 Link and Trunk Installation and Maintenance Access Service	III	ATIS-0300011
Part III Attachments		
A - MTP Compatibility Tests		ATIS-0300012
B - ISUP Compatibility Tests		ATIS-0300013
C - SCCP Compatibility Tests		ATIS-0300014
D - Test Severity Analysis Criteria		ATIS-0300015
E - SS7 Network Gateway Screening		ATIS-0300016
F - SS7 ISUP Tests for ISDN Network Interconnection		ATIS-0300017
G - Link Diversity Validation Guidelines		ATIS-0300018
H - Cause Codes, Tones and Announcements		ATIS-0300019
I - Network Security Base Guideline		ATIS-0300020
J - SS7 Software Validation		ATIS-0300021
K - Dual STP Failure Prevention Procedures		ATIS-0300022
Installation and Maintenance Responsibilities X.75 Gateway Services	IV	ATIS-0300023
Test Line Guidelines	V	ATIS-0300024
Part V Attachment A - Test Line Directory Dictionary		ATIS-0300025
Network Management Guidelines	VI	ATIS-0300026
Part VI Attachment A - Emergency SS7 Restoration Operations Planning Considerations		ATIS-0300027

Information Sharing	VII	ATIS-0300028
Cable LOCATE Guidelines	VIII	ATIS-0300029
Installation, Testing, and Maintenance Responsibilities for Facilities	IX	ATIS-0300030
Part IX Attachment A - SONET Facilities		ATIS-0300031
Interconnection Between LECs Operations Handbook Local Interconnection Service Arrangement	X	ATIS-0300032
Part X Attachment A - Security Guidelines		ATIS-0300033
Local Number Portability Interconnection Testing Document	XI	ATIS-0300034
Toll Free Industry Test Plan	XII	ATIS-0300035
Terms and Definitions	XIII	ATIS-0300036

Revision History, Version: 14.0

Location of Revisions	Sections of Revision	Reason for Revisions	Date of Final Closure
ATIS-030010, Installation and Maintenance Responsibilities Switched Access Services Feature (Groups B, C, and D)	Section 6	Updated to add new language on code opening contact information, which includes a link to the NGIIF Contact Directories. NGIIF Issue 0065.	09/17/2020
ATIS-030010, Installation and Maintenance Responsibilities Switched Access Services Feature (Groups B, C, and D)	Entire document was also updated according to proper ATIS format.	Update references to INC documents given the publication of ATIS-0300119, Thousands-Block (NPA-NXX-X) & Central Office Code (NPA-NXX) Administration Guidelines (TBCOCAG). NGIIF Issue 0060	11/8/2019
ATIS-0300032, Interconnection Between LECs Operations Handbook Local Interconnection Service Arrangement	Entire document was also updated according to proper ATIS format.	Update references to INC documents given the publication of ATIS-0300119, Thousands-Block (NPA-NXX-X) & Central Office Code (NPA-NXX) Administration Guidelines (TBCOCAG). NGIIF Issue 0060	11/8/2019
ATIS-0300036, Terms and Definitions	Entire document was also updated according to proper ATIS format.	Update references to INC documents given the publication of ATIS-0300119, Thousands-Block (NPA-NXX-X) & Central Office Code (NPA-NXX) Administration Guidelines (TBCOCAG). NGIIF Issue 0060	11/8/2019
ATIS-0300010, Next Generation Interconnection Interoperability (NGIIF) Reference Document, Part II, Installation and Maintenance Responsibilities Switched Access Services, Feature Group B, C, and D	Section 7, Telecommunications Service Priority (TSP) Guidelines) F, TSP Maintenance, sub-subsection, Example 1, G, Competition for Resources between	New text added from the resolution of Issue #030.	11/08/11

	Provisioning and Restoration Priorities		
ATIS-0300011, Network Interconnection Interoperability (NIIF) Reference Document, Part III, Installation and Maintenance Responsibilities for SS7 Links and Trunks	Section 5, Trunk Responsibilities, Subsection B, Conversion of Multi-frequency trunks to SS7, in the New Parameters sub-subsection	New text in the resolution statement of Issue #008 was added to the end of the New Parameter section of ATIS-0300011	11/07/11
ATIS-0300024, Next Generation Interconnection Interoperability (NGIIF) Reference Document, Part V, Test Line Guidelines	N/A	Closure of Issue #024 resulted in the text change of LERG Assignee now being Code Holder.	02/09/11
ATIS-0300010, Next Generation Interconnection Interoperability (NGIIF) Reference Document, Part II, Installation and Maintenance Responsibilities Switched Access Services, Feature Group B, C, and D	N/A	Closure of Issue #024 resulted in the text change of LERG Assignee now being Code Holder.	02/09/11
ATIS-0300031, NIIF Reference Document, Part IX, Installation, Testing and Maintenance Responsibilities of Facilities, Attachment A, SONET Facilities	Various	Closure of Issue #006 resulted in revisions and additions made throughout the ATIS 0300031 document. The revised work is too large to list in this table. The changes made are available for review in the 262strawman011210ATIS0300031 contribution.	Closed 2/5/10, Updates made 12/27/11



ATIS-0300009

**Next Generation Interconnection Interoperability (NGIIF)
Reference Document**

**Part I, Installation and Maintenance Responsibilities
Special Access Services, WATS Access Lines
And Switched Access Services
Feature Group A**

Version 12.0



ATIS is the leading technical planning and standards development organization committed to the rapid development of global, market-driven standards for the information, entertainment and communications industry. More than 200 companies actively formulate standards in ATIS' Committees, covering issues including: IPTV, Cloud Services, Energy Efficiency, IP-Based and Wireless Technologies, Quality of Service, Billing and Operational Support, Emergency Services, Architectural Platforms and Emerging Networks. In addition, numerous Incubators, Focus and Exploratory Groups address evolving industry priorities including Smart Grid, Machine-to-Machine, Connected Vehicle, IP Downloadable Security, Policy Management and Network Optimization.

ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications' Sectors, and a member of the Inter-American Telecommunication Commission (CITEL). ATIS is accredited by the American National Standards Institute (ANSI). For more information, please visit www.atis.org.

Notice

This document was developed by the Alliance for Telecommunications Industry Solutions' (ATIS) sponsored Next Generation Interconnection Interoperability Forum (NGIIF). The NGIIF addresses next-generation network interconnection and interoperability issues associated with emerging technologies. Specifically, it develops operational procedures which involve the network aspects of architecture, disaster preparedness, installation, maintenance, management, reliability, routing, security, and testing between network operators. In addition, the NGIIF addresses issues which impact the interconnection of existing and next generation networks and facilitate the transition to emerging technologies. All changes to this document shall be made through the NGIIF issue resolution process. **Note Regarding Previous Versions**

The NIIF Reference Document was formerly known as the Network Operations Forum (NOF) Reference Document. The NOF Reference Document was published and maintained by Bellcore. The last version of the NOF Reference Document is Issue 13.

Disclaimer and Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

ATIS-0300009, *Next Generation Interconnection Interoperability (NGIIF) Reference Document, Formerly NIIF 5005*

The Next Generation Interconnection Interoperability (NGIIF) Reference Document is an ATIS standard developed by the NGIIF.

Published by

Alliance for Telecommunications Industry Solutions

1200 G Street, NW, Suite 500

Washington, DC 20005

Copyright © 2011 by Alliance for Telecommunications Industry Solutions

All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < <http://www.atis.org> >.

Printed in the United States of America.

INSTALLATION AND MAINTENANCE RESPONSIBILITIES SPECIAL ACCESS SERVICES, WATS ACCESS LINES AND SWITCHED ACCESS SERVICES FEATURE GROUP A

Table of Contents

1	GENERAL.....	5
2	RESPONSIBILITIES.....	5
2.1	ACCESS SERVICE CUSTOMERS (ASC).....	5
2.2	ACCESS SERVICE PROVIDER (ASP)	6
3	TELECOMMUNICATION SERVICE PRIORITY (TSP) GUIDELINES.....	7
3.1	DOMESTIC NSEP SERVICES.....	7
3.2	CONTROL SERVICES AND ORDERWIRES.....	7
3.3	OTHER SERVICES	7
3.4	TSP CODE IDENTIFICATION	8
3.5	TSP INSTALLATION	8
3.6	TSP MAINTENANCE.....	9
3.7	COMPETITION FOR RESOURCES BETWEEN PROVISIONING AND RESTORATION PRIORITIES	9
3.8	TSP INSTALLATION PREEMPTION	10
3.9	TSP MAINTENANCE PREEMPTION	10
4	ACCESS SERVICE INSTALLATION	10
4.1	SERVICE ORDER ACTIVITY	10
4.2	ESTABLISHING INTERFACES.....	10
4.3	PRE-SERVICE TESTING	11
4.4	COOPERATIVE ACCEPTANCE TESTING.....	11
4.5	DIGITAL DATA SPECIAL ACCESS SERVICES.....	12
4.6	DIGITAL DATA SERVICES STRESS TEST PATTERNS.....	12
4.7	DIGITAL DATA SERVICES ACCEPTANCE /MAINTENANCE REQUIREMENTS	12
4.8	ACCEPTANCE OF DS-0/VOICE GRADE SERVICE ADDED TO DS-1 FACILITIES ALREADY IN SERVICE.....	13
4.9	ACCEPTANCE OF WATS ACCESS LINES AND FEATURE GROUP A ADDED TO DS-1 FACILITIES ALREADY IN SERVICE 13	
4.10	ACCEPTANCE OF DS-1 SERVICE	13
4.11	ACCEPTANCE OF DS-1 SERVICE RIDING WITHIN AN EXISTING DS-3 SERVICE.....	13
4.12	ACCEPTANCE TESTING OF DS-3 SERVICE	14
4.13	DS-3 TESTING - OPTICAL INTERFACE	14
4.14	REMOTE LOOPBACK VERIFICATION.....	14
4.15	COMPLETION REPORTING	15
4.16	DISCONNECTION OF SERVICE.....	15
4.17	COORDINATED CONVERSIONS	15
4.18	REARRANGEMENTS.....	16
4.19	CHANGE ORDERS.....	16
5	ACCESS SERVICE MAINTENANCE	16
5.1	TROUBLE REPORTING	16
5.2	SECTIONALIZATION AND REPAIR	16
5.3	SYNCHRONIZATION	17
5.4	DIGITAL DATA SPECIAL ACCESS SERVICES.....	18
5.5	DIGITAL DATA SERVICES STRESS TEST PATTERNS.....	18
5.6	DIGITAL DATA SERVICES ACCEPTANCE/MAINTENANCE REQUIREMENTS	19
5.7	MAINTENANCE OF DS-0/VOICE GRADE SERVICE WITHIN DS-1 FACILITIES.....	19
5.8	MAINTENANCE OF DS-1 SERVICE.....	19
5.9	CHRONIC TROUBLE OF DS-1 SERVICE	19
5.10	MAINTENANCE OF DS-1 SERVICE WITHIN A DS-3 SERVICE	20

5.11	MAINTENANCE TESTING OF DS-3 SERVICE.....	20
5.12	DS-3 TESTING - OPTICAL INTERFACE	20
5.13	VERIFICATION TESTS.....	20
5.14	MAKE-BUSY OF SWITCHED ACCESS TERMINATED SERVICES	20
5.15	EXPEDITED MAKE-BUSY	21
5.16	REQUESTS FOR CIRCUIT TRACE	21
5.17	EMERGENCY CALL TRACING	21
5.18	ROUTINE MAINTENANCE ACTIVITIES	22
5.19	TROUBLE REPORT STATUS	22
5.20	NETWORK MODIFICATION NOTIFICATION	22
6	END-TO-END AND INTERCARRIER TESTING.....	23
7	ESCALATIONS.....	23
8	TEST LINES	23
9	ADDITIONAL BILLING	24
9.1	OVERTIME INSTALLATION AND REPAIR.....	24
9.2	ADDITIONAL COOPERATIVE ACCEPTANCE TESTING.....	24
9.3	STAND-BY TIME	24
9.4	NON-SCHEDULED TESTING.....	24
9.5	MAINTENANCE OF SERVICE CHARGE.....	25
9.6	OTHER LABOR	25
10	ACCESS SERVICES PROVIDED BY MULTIPLE EXCHANGE CARRIERS	25
10.1	INSTALLATION.....	26
10.2	MAINTENANCE	27
10.3	COMMON COMPLETION	29
10.4	JEOPARDY.....	29

1 GENERAL

This document has been developed to provide the operations personnel of the Access Service Providers (ASP) and Access Service Customers (ASC) with general procedures for the installation and maintenance of Special Access Services, and WATS Access Lines and Switched Access Services Feature Group "A". The contents of this document are generic. Specific operational procedures are covered in documentation provided by the ASP(s) and ASC(s). This document does not replace nor supersede tariffs, contracts or any other legally binding documents. In addition to other operational and technical agreements made at the Next Generation Interconnection Interoperability Forum (NGIIF), this document is being reissued to incorporate the following changes:

- Standardization of the Issue Number and publication date to agree with other sections of the NGIIF Reference Document.

The Installation, Testing and Maintenance of facilities that are utilized for the transport of all Special Access and Feature Group A services is covered in the Facilities Document.

2 RESPONSIBILITIES

2.1 Access Service Customers (ASC)

The ASC has the overall installation and maintenance responsibility for the total service to its end user. It is responsible for the overall coordination of installation and testing of its services.

The following are the responsibilities of the ASCs:

- Provides trained personnel.
- Advise the ASP when there is an ASC network failure that may affect the ASPs services.
- Provides a contact number for trouble reporting that is readily accessible 24 hours a day, 7 days a week.
- Maintains complete and accurate installation and repair records.
- Provides ASP personnel access to the Point of Termination (POT) when required.
- Provides access to testlines where appropriate.
- Provides billing authorization to the ASP for any additional labor requested.
- Ensures the test equipment used is compatible with the ASP's test equipment.
- Cooperates with the ASP ensuring that services are installed in accordance with the ASC service requests.
- Notifies the ASP of any change affecting the service requested, including the service due date.
- Assumes control functions for maintenance of its facilities.
- Consults with the ASP before making any changes that would affect service except under emergency conditions.
- Accepts trouble reports from their end users.
- Accepts trouble reports from the ASPs.

- Sectionalizes and clears the trouble in its own network.
- Keeps their end user advised of the status of all trouble report(s).
- Performs cooperative analysis to determine if a trouble pattern exists.
- Refers troubles to the ASP using the trouble reporting procedures.
- Dispatches its own maintenance forces.
- Performs verification tests to ensure that trouble has been cleared.
- Performs scheduled testing and other maintenance services when requested.
- Participates cooperatively with the ASP to further isolate and clear the trouble when trouble exists and cannot be sectionalized.
- Acts as their end user's contact in all matters involving installation and maintenance of ASC provided services.

2.2 Access Service Provider (ASP)

The ASP is responsible for ensuring that the services furnished to an ASC are installed and function properly. In addition, the ASP should work cooperatively with the ASC in the testing of the services it provides.

The following are the responsibilities of the ASPs:

- Provides trained personnel.
- Advises the ASC when there is a potential service affecting ASP network failure.
- Provides a contact number for trouble reporting that is readily accessible 24 hours a day, 7 days a week.
- Maintains complete and accurate installation and repair records.
- Provides access to testlines where appropriate.
- Coordinates with the ASC ensuring that Services are installed in accordance with the service request.
- Notifies the ASC of any changes affecting the service requested, including the service due date.
- Assumes control functions for installation of the Service(s).
- Accepts trouble reports from the ASC.
- Sectionalizes and clears the trouble in its own network.
- Tests cooperatively with the ASC to identify and clear a trouble when the trouble has not been sectionalized to the ASC network.
- Performs cooperative analysis to determine if a trouble pattern exists.
- Refers troubles to the ASC using the trouble reporting procedures.
- Dispatches its own maintenance forces.
- Performs verification test to ensure that trouble has been cleared in their own network.
- Performs scheduled testing and other maintenance services when requested,
- Notifies the ASC of due date jeopardies in a timely manner.

- Establishes local service restoral objectives and may provide them to the ASC upon request.
- Provides status reports to the ASCs regarding installation and repair activity.

3 TELECOMMUNICATION SERVICE PRIORITY (TSP) GUIDELINES

This section provides TSP installation and maintenance guidelines for access services and generic administrative procedures and interfaces between ASCs and the ASPs.

The TSP system provides for the priority treatment of National Security Emergency Preparedness (NSEP) telecommunication services in order to prioritize their installation and maintenance.

In order for the TSP system to be effective, it **MUST** be incorporated into the day-to-day operating procedures for all ASPs and ASCs. All communications carriers are expected to cooperate in the installation and restoration of services with TSP that involve the facilities of more than one carrier.

3.1 Domestic NSEP Services

The NSEP TSP system and procedures provide priority treatment to the following domestic telecommunication services (including portions of U.S. international telecommunication services provided by U.S. providers) for which provisioning or restoration priority levels are requested, assigned, and approved:

- Commercially provided private services and public switched services:

Note: Initially, the NSEP TSP system's applicability to public switched services is limited to provisioning of such services (e.g., business, centrex, cellular, foreign exchange, Wide Area Telephone Service (WATS) and other services that the selected provider is able to provision) and restoration of services that the selected provider is able to restore.

- Services that are provided by Government and/or non common carriers and are interconnected to common carrier services assigned a priority level pursuant to Section 9 of the FCC's TSP system rules.

3.2 Control Services and Orderwires

The NSEP TSP system and procedures are not applicable to authorize priority treatment to control services or orderwires owned by a service provider and needed for provisioning, restoration or maintenance of other services owned by that service provider. Such control services and orderwires shall have priority of provisioning and restoration over all other telecommunications services (including NS/EP services) and shall be exempt from preemption. However, the NSEP TSP system and procedures are applicable to control services or orderwires leased by a service provider or user from another service provider.

3.3 Other Services

The NS/EP TSP system may apply, at the discretion of and upon special arrangements by the entities involved, to authorized priority treatment to the following telecommunications services:

- 1) Government or non-common carrier services which are not connected to common carrier-provided services assigned a priority level.
- 2) Portions of U.S. international services which are provided by foreign correspondents.

3.4 TSP Code Identification

The TSP Authorization Code is composed of twelve characters and is divided into two parts. The first nine characters comprise the TSP Control ID, a computer generated number, which is for the government's tracking purposes. A hyphen is always the tenth character and it separates the TSP Control ID from the TSP Code. The final two characters are the TSP Code. The first character of the TSP Code (the eleventh character of the entire series) indicates the provisioning priority. Acceptable values are: E (Emergency), 1, 2, 3, 4, 5, or 0. A value of "0" indicates no provisioning priority is assigned. The second character of the TSP Code (the twelfth character of the entire series) indicates the restoration priority. Acceptable values: 1, 2, 3, 4, 5, or 0. A value of "0" indicates no restoration priority is assigned.

A TSP Authorization Code is illustrated below:

T S P 1 2 3 4 5 C - 1 2

| |

Control ID Code

Table 1 below depicts the codes (eleventh and twelfth digits) allowable in the TSP system.

Table 1: TSP Codes Reference Table

		TSP Provisioning/Restoration Priority Levels								
		P-R	P-R	P-R	P-R	P-R	P-R	P-R		
HIGHER	↑	E-1	1-1	2-1	3-1	4-1	5-1	0-1	↓ LOWER	
		E-2	1-2	2-2	3-2	4-2	5-2	0-2		
		E-3	1-3	2-3	3-3	4-3	5-3	0-3		
	←	E-4	1-4	2-4	3-4	4-4	5-4	0-4		→
		E-5	1-5	2-5	3-5	4-5	5-5	0-5		
		E-0	1-0	2-0	3-0	4-0	5-0	0-0		

E = Emergency Priority Level

P = Provisioning Priority Level

R = Restoration Priority Level

A code of "0-0" indicates "Revocation", the removal of a previously assigned TSP code.

3.5 TSP Installation

Circuits with an E (Emergency) provisioning priority have the highest priority and must be installed As Soon As Possible (ASAP), dispatching outside of normal business hours when necessary. Circuits with TSP provisioning

priorities 1 - 5 will be installed by the due date according to the TSP provisioning priority assigned (see reference table above). For example, a circuit with a provisioning priority of "1" would be installed before a circuit with a provisioning priority of "2" when they both carry the same due date.

3.6 TSP Maintenance

Available resources should be allocated to restore NSEP services as quickly as practicable, dispatching outside normal business hours to restore services assigned priority levels "1", "2" and "3" when necessary and services assigned priority levels "4" and "5" when the next business day is more than 24 hours away.

The day-to-day administration for repair and restoral of services assigned a TSP restoration priority is shown in the following examples:

Example 1: If there are several pending Trouble Reports for circuits that do not have TSP restoration codes and a Trouble Report is received for a circuit with a TSP code of 23, the TSP23 circuit Trouble Report moves to the next Trouble Report to be worked ahead of the other circuit Trouble Reports that have no TSP restoration codes. Upon completion of the repair/restoral of the TSP23 circuit, work continues on the Trouble Reports for the circuits that have no TSP restoration codes.

Example 2: If there are several Trouble Reports to be worked (which includes a circuit with a TSP23 code) and two additional Trouble Reports are received for circuits with higher TSP restoration codes (such as TSP21 and TSP22), the circuit Trouble Report with the TSP21 code will move to the next Trouble Report to be worked, followed by the TSP22 circuit Trouble Report. Then, the TSP23 circuit Trouble Report moves ahead of the other Trouble Reports for the circuits that have no TSP codes. Upon completion of the repair/restoral of the TSP21, TSP22 and TSP23 circuits, work then continues on the Trouble Reports for the circuits that have no TSP codes.

3.7 Competition For Resources Between Provisioning and Restoration Priorities

In general, service providers should restore existing services assigned TSP priority before provisioning new service; an exception is the provisioning of services assigned emergency priority, which should always be done before the restoration of services assigned restoration priorities "2", "3", "4" or "5". Restoration of any service assigned restoration priority "1" takes precedence over any other service assigned any other provisioning and restoration priority.

When two or more TSP services are competing for resources, the priority sequence listed below will ensure proper handling of these circuits:

- Restore TSP services with restoration priority of "1".
- Provision TSP services with provisioning priority of "E".
- Restore TSP services with restoration priority of 2, 3, 4, 5.
- Provision TSP services with provisioning priority of 1, 2, 3, 4, 5.

Using the priority sequence listed above, the following examples of two TSP services competing for the same resources at the same time, the underlined TSP service has the higher priority and should be worked on first:

- TSP code 2-1 and E-2 both in trouble status. 2-1
- TSP code 2-1 in trouble and E-2 to be provisioned. 2-1
- TSP code 2-1 to be provisioned and E2 in trouble. E-2
- TSP code 2-1 and E-2 to be provisioned. E-2

3.8 TSP Installation Preemption

Where facilities and/or equipment are not available to install a service assigned a TSP priority, preemption (interruption of an existing service) of a non-priority or lower priority circuit may be required. User consent is NOT required to preempt any user's existing service to provision an NSEP service assigned a provisioning priority level "E" (Emergency) or to provision an NSEP service assigned a provisioning priority level "1" through "5".

3.9 TSP Maintenance Preemption

Facilities of message circuits may be used for restoral of services assigned a TSP restoration priority after ensuring that sufficient message circuits are available for public switched network use.

Where facilities and/or equipment are not available to restore a service assigned a TSP restoration priority preemption (interruption of an active service) may be required. Interruption of a non-priority or lower priority circuit is authorized for the purpose of restoring the service assigned a TSP restoration priority.

To restore interrupted NSEP services: User consent is not required to preempt any user's existing service to restore any NSEP service assigned a restoration priority level from "1" through "5".

NSEP services: If no suitable spare or non-NSEP services are available, then existing NSEP services may be preempted to restore NSEP services with higher priority level assignments. When this is necessary, NSEP services will be selected for preemption in the inverse order of priority level assignment.

Service providers who are preempting services will ensure their best effort to notify the service user of the preempted service and state the reason for and estimated duration of the preemption.

4 ACCESS SERVICE INSTALLATION

Installation as used in this document pertains to that portion of the total provisioning process which starts when the order, e.g., "Work Order Record and Detail" (WORD) or equivalent is received by the ASP and includes installations, changes, and disconnects.

4.1 Service Order Activity

The ASC will order the access service(s) required to provide its overall service from the ASPs. Where applicable TSP provisioning and restoration codes should be on the WORD or equivalent.

The order, after processing by the Interexchange Customer Service Center (ICSC) or equivalent, will flow to the ASP, which will coordinate the access service turn-up with the ASC. The ICSC or equivalent is an Access Service Negotiation work group that will handle inquires and orders. It is to serve as a point of contact for the access service needs of Interexchange Customers. Where applicable, installation priority will be in accordance with the TSP Provisioning code ordered.

4.2 Establishing Interfaces

It is the responsibility of the ASC to arrange for suitable space and electrical power at the POT, if required. The space furnished shall be in a safe working area and accessible during normal working hours as determined locally to ASP personnel for installation and maintenance purposes.

Where digital equipment is utilized, synchronization/loop timing equipment and options should be verified.

The Frame Relay Service Provider should establish the circuit ID that will be used to coordinate trouble resolution.

4.3 Pre-Service Testing

The ASP should ensure the following before contacting the ASC to perform cooperative acceptance tests:

- That the access service has been installed correctly.
- That pre-service tests have been performed and the requirements met.
- That all pre-service test measurements have been recorded.

ASC personnel or their designate may be requested to participate in the pre-service testing activity.

4.4 Cooperative Acceptance Testing

Upon completion of the pre-service tests, the ASP will contact the ASC and advise that the access service is ready to be turned up. The ASC has the option of acceptance with or without cooperative acceptance testing. If the ASC requests cooperative acceptance tests, the ASP will coordinate all normal and additional acceptance testing. Test equipment compatibility should be verified at this time. The ASC is not obligated to accept the service prior to the due date.

When a DS-1 loopback device is deployed by the ASP, the subsequent dispatch to the End User's POT to perform "Cooperative Acceptance Tests" will be waived by the ASC. The ASC, upon request, will be provided the test results obtained by the ASP. If the ASC requests "Cooperative Acceptance Testing" be performed, they will be performed remotely. Excluding the following conditions, an ASP technician will not normally be dispatched to the End User's premises to perform tests. The conditions are:

- The DS-1 Service is not equipped with the DS-1 loopback device.
- Test results do not meet service acceptance immediate action limits and trouble is sectionalized to the ASP network.
- The unit is inoperable.
- Unless the ASC requests a dispatch.

The tests results will be viewed as valid (assuming they are within service parameters) for the purpose of service acceptance/maintenance.

When Intelligent NCTE is deployed by the ASP, the dispatch to perform Cooperative Acceptance tests will be waived by the ASC. The ASC, upon request, will be provided the remotely aligned tests results obtained by the ASP. If the ASC requests Cooperative Acceptance testing, the ASP will test remotely, using the diagnostic features of the Intelligent NCTE. Excluding the following conditions, an ASP technician will not normally be dispatched to the end user's location to perform Cooperative Acceptance tests. The conditions are:

- The unit is not equipped to perform the basic turn-up tests.
- The ASC requests specific Additional Cooperative Acceptance Tests, i.e., conditioning.
- The unit is inoperable.
- If the circuit does not meet Acceptance parameters.

4.5 Digital Data Special Access Services

The following test patterns can be used to perform cooperative testing when access is gained at two (2) points on the circuit. Each test unit transmits a known test pattern toward the other, and the data received by each is analyzed. It can also be used to do loopback testing if a 108 Type Test Line or other manual DSO loopback functions are provided. The test device will attempt to frame on the received data and count bit and 1-second block error rates. Bit and 1-second block errors will be reported upon termination of the test, and must be possible for intermediate results to be reported at specified intervals.

4.6 Digital Data Services Stress Test Patterns

Any of four (4) repetitive patterns should be placed in the six-or seven-bit data field of the byte with the eighth bit set to one (1) and may be applied as follows:

Table A.1 (From ANSI T1.510)

Test	Pattern Length Bytes	Binary Representation (see notes 1 & 2)	Test Interval	# of test (see note 3)	ES Limit	Test
S1	100 100	1111 1111 0000 0000	(see note 4)	1	0	
S2	100 100	0111 1110 0000 0000	(see note 4)	1	0	
S3	Continuous	0100 1100	(see note 4)	1	0	
S4	Continuous	0000 0010	(see note 4)	1	0	
S5 (see note 5)	(see note 5)	(see note 5)	(see note 4)	1	0	
NOTES: For 56 kbit/s service, these patterns will appear only in the customers' data bits. All binary presentations are transmitted left to right. One retest is allowed if the initial test fails. 3-minute intervals are currently used: longer intervals may be recommended by the service provider. If test intervals of 15 minutes or longer are used, the test procedures, intervals and limits given in 8.1.2 and 8.1.3 should be followed. This test utilizes all the test patterns defined above and, and as an option, may be used in lieu of any or all of the tests S1 through S4 if available. S1 through S4 are run sequentially; a minimum pattern length of 200 bytes for S3 and S4 is suggested.						

4.7 Digital Data Services Acceptance /Maintenance Requirements

These test patterns, selected by the OS Application or tester, are transmitted in the test direction. Each byte is repeated according to customer data rate. The first bit transmitted is shown on the right of the pattern.

DDS ACCEPTANCE / MAINTENANCE REQUIREMENTS

Test limits and objectives for 56/64 kbit/s service

Table 5 (From ANSI T1.510)

Parameter Limit For:	Short-duration Tests 15-minute stages						Long-duration Test 24 hour	
	ES			SES			ES	SES
	15 min	30 min	45 min	15 min	30 min	45 min	24 hour	24 hour
Access	0	≤ 2	≤ 3	0	0	≤ 2 (see note)	≤ 60	≤ 7
Transit	0	≤ 2	≤ 3	0	0	≤ 2 (see note)	≤ 60	≤ 16
End-to-End	0	≤ 2	≤ 4	0	0	≤ 2 (see note)	≤ 120	≤ 21
NOTE – Accept at 2 only if the cause of the SES is identified as an isolated event.								

4.8 Acceptance of DS-0/Voice Grade Service Added To DS-1 Facilities Already In Service

If the DS-0/Voice grade service is being extracted from the DS-1 facility at the POT cooperative acceptance tests should be performed from the ASC POT to the End-User POT. If the ASC does not extract the DS-0/Voice Grade Service at the ASC POT, in lieu of cooperative acceptance test, the ASP will perform applicable tests from the End-User POT through the ASP's Channel Unit and if requested provide test results to the ASC.

4.9 Acceptance of WATS Access Lines and Feature Group A Added To DS-1 Facilities Already In Service

If the DS-0/Voice grade service is being extracted from the DS-1 facility at the POT cooperative acceptance tests should be performed from the POT to the WATS Serving Office/Dial Tone Office. If the ASC does not extract the WATS Access Lines or Feature Group A at the ASC POT, in lieu of cooperative acceptance testing, the ASP will perform applicable Operational and Transmission tests from the WATS Serving Office/Dial Tone Office. These tests will be performed through the ASP's Channel Unit and if requested provide test results to the ASC.

4.10 Acceptance of DS-1 Service

Acceptance testing parameters for DS-1 Services are addressed in the Facilities document.

4.11 Acceptance of DS-1 Service Riding Within an Existing DS-3 Service

Acceptance testing parameters for DS-1 Services riding within an existing DS-3 Service is addressed in the Facilities document.

4.12 Acceptance Testing Of DS-3 Service

Acceptance testing parameters for DS-3 Service is addressed in the Facilities document.

4.13 DS-3 Testing - Optical Interface

Acceptance testing parameters for DS-3 Testing is addressed in the Facilities document.

4.14 Remote Loopback Verification

In some cases, both the ASP and the ASC may have voice grade tone activated remote loopback devices in a circuit to aid in sectionalization. There are two equipment configuration scenarios that can exist:

- Tone activated loopback devices provisioned on both sides of the network interface at the ASC-POT; and
- Tone activated loopback devices provisioned on both sides of the network interface at the End User POT.

These devices should be identified and any conflicts resolved after pre-service testing and during cooperative testing. Cooperative testing will be required to insure that both devices activate and deactivate properly.

The possibility exists that both devices will be activated into the loopback mode during testing. When the deactivation tone is transmitted, the tone will be received by only one device, leaving the other device still in the loopback mode. Where devices cannot be returned to normal with tone local negotiations should occur to:

- Allow for the removal of one or more devices; or
- Develop specific documentation and testing procedures to ensure all devices are returned to normal when future maintenance activities are performed on these circuits.

The ASC will specify on its initial order to the ASP, any additional tests required at the time acceptance tests are to be cooperatively performed. However, additional tests may be requested by the ASC subsequent to its original order. In all cases, it is the responsibility of the ASC to use test equipment compatible with that being used by the ASP for such measurements. Additional billing may be applicable. Additional acceptance tests include but are not limited to the following examples:

- Attenuation Distortion
- Dial Pulse Percent Break
- Envelope Delay Distortion
- Frequency Shift
- Impulse Noise
- Inter Modulation Distortion
- Phase Jitter

Completion of the order will not be contingent on parameters beyond those specified in the technical reference and/or tariff description for each of the respective access services.

To mitigate inadvertent loopbacks, 64kb data services should be provisioned with loopback recognition timers. Where loopback recognition timers are an ordering option for such services this option should be selected.

4.15 Completion Reporting

Upon acceptance of the ASP access service by the ASC, the ASP will record the name of the ASC representative and the date the service is accepted. When an access service has a TSP code, this code should be verified between the ASC and ASP at this time.

4.16 Disconnection of Service

Disconnect procedures will be in accordance with ASP developed practices.

4.17 Coordinated Conversions

Coordinated conversion is a process that may be used to facilitate a change in service from one ASC to another that involves the reuse of a portion of the ASP provided equipment and/or facilities previously assigned to the services being converted. It requires the issuance and processing of related disconnect and connect orders and coordination of these orders throughout the entire cutover process.

Note: In some cases, the new ASC and the former ASC could be the same entity (e.g., when an ASC rehomes an Access Service to a new Point of Termination).

The new ASC is expected to bear full responsibility for the overall installation and coordination of the various service orders and all related activities involved in the provision of its end-to-end service. The actual ASP work operations performed remain in control of the ASP according to mutually agreed upon schedules.

The new ASC will establish and coordinate conversion activities with the ASP, former ASC and end user when required. Those activities will include but are not limited to:

- Completion Testing and Notification
- Requests for Continuation of Service,
- Conversion Timing,
- Circuit Release,
- Circuit Conversion Sequence.
- TSP verification, where applicable.

Every effort must be made jointly by the new ASC and the ASP to successfully complete the conversion. If a new ASC encounters difficulties in activating its end-to-end service after work has begun or acceptance tests have been completed on the ASP provided facilities, the new ASC may negotiate and coordinate continuation of the service with the former ASC and involved ASP. Following successful negotiations for continuation of service, the new ASC must advise the ASP and the former ASC that continuation of service has been negotiated and restoral procedure should be started.

Since continuation of the former ASC service does not automatically defer the due date of the disconnect order, the new ASC must request the former ASC to contact the ASP ICSC, or equivalent, to request a due date change in order to prevent the disconnect of the former service. This must take place prior to the disconnect due date.

It is the responsibility of the ASP to inform the new ASC that all work involved in restoring the former ASC service and subsequent cut-over activities of the new ASC facilities is work over and above that required for normal coordinated conversion cut-overs. This work may result in appropriate additional labor charges.

4.18 Rearrangements

A rearrangement as described in this document is a coordinated activity initiated by either the ASP or the ASC, which will usually be transparent to the ASC's end user and will not change the operation or design of the affected circuit(s). In the rearrangement process, circuit releases, rearrangement timing, and completion testing will be negotiated on an Individual Case Basis (ICB) by the initiating party. If rearrangement affects transmission parameters, both entities will cooperatively verify that circuits are within acceptance limits.

4.19 Change Orders

Change orders cover any changes in the design or operation of an existing circuit or circuit group(s) administered through the ICSC or equivalent center procedures.

5 ACCESS SERVICE MAINTENANCE

The ASC is responsible for performing all necessary tests to determine the nature of the trouble. If the trouble is found to be in the ASP provided service, the ASC will report the trouble to the ASP's designated trouble reporting office.

The ASP will be responsible for accepting, from the ASC, trouble reports sectionalized to ASP facilities and/or equipment. The ASP will test cooperatively or independently to assist in trouble sectionalization.

5.1 Trouble Reporting

The following is the type of information that should be exchanged at the time of the trouble referral.

- ASP circuit identification number.
- Date and time of trouble referral.
- Nature of the trouble and any other information that may be of assistance to the ASP.
- The name or initials and the telephone number of the person referring the trouble.
- Trouble report number(s) or equivalent and the name or initials of the person accepting the trouble.
- TSP restoration priority, where applicable.

When ASPs and ASCs are using different methods of in-service Performance Monitoring (i.e., scanned vs. dedicated), differences will occur in measured performance. The performance reported by the provider using dedicated monitoring, will be more indicative of the actual service. These reports should be accepted by the other entity.

5.2 Sectionalization and Repair

While trouble sectionalization is the responsibility of the ASC, it could involve cooperative testing with participation by both the ASP and ASC.

Maintenance problems sectionalized to HiCap facilities carrying the Switched Access Service/Special Access Services should be tested using the Facility Document.

The ASP will coordinate the isolation of the trouble within the ASP provided service.

Communication may also be necessary on services that involve an ASC, their intermediate agent, and an ASP. In these situations the cooperation of all three organizations may be necessary to expedite trouble clearance. When it is necessary for communication between the ASC and ASP, it is required that this contact be made through the intermediate agent.

The ASP employees will limit their repair activities to ASP provided facilities and/or equipment. No attempt should be made to adjust or repair equipment belonging to the ASC. The ASC or others may not rearrange, move, disconnect, remove or attempt to repair any equipment or facilities provided by the ASP.

When trouble tickets are being closed out between an Access Service Provider/Access Service Customer, whether they are using a mechanized system or a verbal notification, the disposition should be furnished by the company clearing the trouble, and the following information shall be provided:

- Circuit ID/telephone number,
- Trouble Ticket Number (ASC/ASP number),
- Name or initials of person closing out trouble,
- Nature of the trouble found (e.g., bad cable),
- Resolution details (e.g., cut over to new cable),
- ASC will inform ASP if this trouble is measured,
- Date and time trouble cleared,
- Date and time trouble referred from the ASC to the ASP,
- Date and time trouble report closed,
- No access time (the period of time that the service is unavailable for maintenance activities),
- Service charge information, if applicable,
- Status of circuit(s) (working or made busy).

When there is a disagreement on the disposition, the parties engaged in the dispute shall document their respective positions, and the names of the individuals engaged in the dispute for audit purposes. Escalations if necessary shall be in accordance with identified procedures.

If after a trouble has been cleared and either the ASP or ASC wishes to change the Disposition, such changes shall be negotiated.

5.3 Synchronization

Improper synchronization can result in circuit impairments that should be investigated and synchronization problems corrected. Problems that cannot be resolved should be referred to your Synchronization Coordinator. The NGIIF publishes a Service Provider Contact Directory, which contains the number for the company's Synchronization Coordinator. This is updated, as required, and is available from your companies' NGIIF Representative.

If the ASC/ASP has its own primary frequency standard that meets the CCITT standard for national networks (G.811, G.822), synchronization of the digital SS7 link(s) will be by the plesiochronous method of operation. If either network does not conform to the CCITT standard, the non-conforming company will use loop timing to accept SS7 link(s) timing from the conforming company. When the link interface is a DSOA interface, the interface must be plesiochronous or timed to the same source as the facility.

5.4 Digital Data Special Access Services

The following test patterns can be used to perform cooperative testing when access is gained at two (2) points on the circuit. Each test unit transmits a known test pattern toward the other, and the data received by each is analyzed. It can also be used to do loopback testing if a 108 Type of Test Line or other manual DSO loopback functions are provided.

The test device will attempt to frame on the received data and count bit and 1-second block error rates. Bit and 1-second block errors will be reported upon termination of the test, and must be possible for intermediate results to be reported at specified intervals.

5.5 Digital Data Services Stress Test Patterns

Any of four (4) repetitive patterns should be placed in the six-or seven-bit data field of the byte with the eighth bit set to one (1) and may be applied as follows:

Table A.1 (From ANSI T1.510)

Test	Pattern Length Bytes	Binary Representation (see notes 1 & 2)	Test Interval	# of test (see note 3)	ES Limit	Test
S1	100 100	1111 1111 0000 0000	(see note 4)	1	0	
S2	100 100	0111 1110 0000 0000	(see note 4)	1	0	
S3	Continuous	0100 1100	(see note 4)	1	0	
S4	Continuous	0000 0010	(see note 4)	1	0	
S5 (see note 5)	(see note 5)	(see note 5)	(see note 4)	1	0	

NOTES:

For 56 kbit/s service, these patterns will appear only in the customers' data bits.

All binary presentations are transmitted left to right.

One retest is allowed if the initial test fails.

3-minute intervals are currently used: longer intervals may be recommended by the service provider. If test intervals of 15 minutes or longer are used, the test procedures, intervals and limits given in 8.1.2 and 8.1.3 should be followed.

This test utilizes all the test patterns defined above and, and as an option, may be used in lieu of any or all of the tests S1 through S4 if available. S1 through S4 are run sequentially; a minimum pattern length of 200 bytes for S3 and S4 is suggested.

5.6 Digital Data Services Acceptance/Maintenance Requirements

These test patterns, selected by the OS Application or tester, are transmitted in the test direction. Each byte is repeated according to customer data rate.

DDS ACCEPTANCE / MAINTENANCE REQUIREMENTS

Table 5 (From ANSI T1.510)

Parameter Limit For:	Short-duration Tests 15-minute stages						Long-duration Test 24 hour	
	ES			SES			ES	SES
	15 min	30 min	45 min	15 min	30 min	45 min	24 hour	24 hour
Access	0	≤ 2	≤ 3	0	0	≤ 2 (see note)	≤ 60	≤ 7
Transit	0	≤ 2	≤ 3	0	0	≤ 2 (see note)	≤ 60	≤ 16
End-to-End	0	≤ 2	≤ 4	0	0	≤ 2 (see note)	≤ 120	≤ 21
NOTE – Accept at 2 only if the cause of the SES is identified as an isolated event.								

5.7 Maintenance of DS-0/Voice Grade Service Within DS-1 Facilities

If initial testing of the DS-0 Service indicates the trouble is toward the DS-1 Service/facility the following procedures should be followed:

- Use test equipment to extract the DS-0/Voice Grade service from the DS-1 bit stream. The ASC will perform a cooperative test with the ASP from the ASC POT location to either the End User POT or the ASP HUB location.
- If the ASC does not normally staff the POT or have remote test access, the ASP will, upon an ASC request, determine if the trouble is at the DS-0 level, which may involve substituting the channel unit.
- If changing the channel unit does not clear the trouble, the ASC will dispatch to their POT to perform cooperative tests.

5.8 Maintenance of DS-1 Service

Maintenance parameters for DS-1 Services is addressed in the Facilities document.

5.9 Chronic Trouble of DS-1 Service

Maintenance parameters for Chronic Trouble of DS-1 Service is addressed in the Facilities document.

5.10 Maintenance of DS-1 Service Within A DS-3 Service

Maintenance parameters for DS-1 Service within a DS-3 Service is addressed in the Facilities document.

5.11 Maintenance Testing Of DS-3 Service

Maintenance requirements for the testing of DS-3 Service is addressed in the Facilities document.

5.12 DS-3 Testing - Optical Interface

Maintenance requirements for the testing of DS-3, Optical Interface, are addressed in the Facilities Document.

5.13 Verification Tests

After each trouble has been cleared the ASP will contact the ASC to advise that the trouble has been cleared and the nature of the trouble found and action taken.

If the requested tests are other than those specified for the type of service involved, the ASP should notify the ASC that the time required to perform these additional tests will be billed to the ASC.

When repair verification tests identify a trouble that was not apparent due to the nature of the original trouble, clearance activity will continue until the service is restored.

Where remote loopback devices have been activated in the process of performing maintenance tests, verification should be made that all loopback devices in the circuit are returned to normal.

5.14 Make-Busy of Switched Access Terminated Services

Requests for make-busy may be categorized as follows:

- Single Circuit
- Trunk Group (facility failure)
- Trunk Group (preventive maintenance)

Single Trunk Make-Busy

- An ASC requesting an ASP to make-busy a line terminated service should contact the ASP responsible for the access service. The ASC shall provide the ASP with the necessary information. At the time of request, the ASC should indicate whether the circuit is busy or idle and whether it wants the signaling leads opened (disabled).
- Upon receipt of the request, the ASP shall determine the condition of the circuit (idle or seized). If idle, and requested by the ASC, the ASP will leave the signaling leads closed to enable the ASC to test into the switching machine. The ASP will then call the appropriate work center and request a make busy of the circuit. If the circuit has a seizure on it, the ASP will advise the ASC that the signaling leads will be opened until the seizure is removed.
- If trouble is experienced on the circuit while it is made busy and the signaling leads are closed, the ASP should disable them and notify the ASC. The ASC must inform the ASP upon final completion of its tests and coordinate the removal of the make-busy.

Trunk Group Make-Busy (Facility Failure)

- In the event the ASC detects a facility or equipment failure, the ASC will advise the ASP of the involved trunks and the need to have them made busy. Likewise, if the ASP detects a facility or equipment failure, the ASP will have the trunks made busy and signaling leads disabled, when required. The ASP will then advise the ASC of the action taken.
- When the facilities and/or equipment have been restored the ASC will coordinate removal of the make-busy.

Trunk Group Make-Busy (Preventive Maintenance)

- If an ASC requests a trunk group be made-busy for preventive maintenance purposes, the request will only be honored outside the normal business day. Such requests could have an impact upon other users of the switching machine if honored during the normal business day.
- Upon receipt of this type of request, the ASP should advise the ASC that this is additional labor and is billable. If the ASC agrees, the request should be honored. The time required to make the circuits busy, and later, to remove the make-busy is billable as additional labor. For example, if the ASC requests to have an individual trunk released while they make a specific test (and then release another and so on), the time is billable. Upon completion of the tests, the ASC must coordinate the removal of the make-busy.

5.15 Expedited Make-Busy

The ASC may request an expedited circuit(s) make-busy. Such requests are to be handled by ASP on an expedited basis.

If the request for an expedite cannot be handled on an expedited basis the ASP will inform the ASC.

5.16 Requests for Circuit Trace

It may become necessary to request a hold and trace in order to resolve a difficult trouble that cannot be identified by conventional testing methods. This request should be handled on an expedited basis. When an end user is involved, the ASP will hold the call and release the end user. When the trace is completed, sectionalization and repair should take place.

5.17 Emergency Call Tracing

Emergency Call Tracing is directed toward identifying the source of an in-progress call for urgent physical assistance. These traces may require both ASC and ASP involvement. An ASC and/or ASP receiving such a request will initiate the trace on an expedited basis recognizing that human life may be at stake. Information relative to these traces will be handled according to local security guidelines.

The originator of an emergency call trace assumes responsibility of the validity of a trace request and also is the controlling entity. These traces may require both ASC and ASP involvement. An ASC and/or ASP receiving such a request will initiate the trace on an expedited basis recognizing that human life may be at stake. When an emergency trace is passed to an ASC, the ASC will trace the call to the distant ASP and provide the distant ASP with information to continue the trace. After completion of the trace, the distant ASP will provide the source information to the originator, either directly, via the ASC or the originating ASP may elect to remain on line throughout the trace. Security of the information relative to these traces will be handled according to local guidelines.

5.18 Routine Maintenance Activities

It is the recommendation of the NGIIF that all routine maintenance and scheduled work activities be performed during hours of minimum traffic (e.g., during an 11:00 pm to 5:00 am "maintenance window") so that any inadvertent failure impacts the least number of customers.

At a minimum, high risk, potentially service affecting maintenance and growth procedures should be scheduled during weekend and off-hours. The overall methods, procedures and scheduling of these work activities should be reviewed by a second tier maintenance organization.

The activities that may affect other network service providers must be coordinated, which includes both intra- and inter-carrier networks. (See NGIIF Reference Document, Section III, Installation and Maintenance - SS7).

Non-Scheduled Work Activity - If customer service is being impacted, the minimum work activity will occur to restore the system to a stable performance state. Complete system recovery activity will be scheduled for the next maintenance window period.

5.19 Trouble Report Status

The ASP and/or ASP receiving the initial trouble referral shall provide a status on the disposition of that referral based on local agreements negotiated at the time of referral or requested on an individual case basis.

Subsequent to the initial status report on the disposition of the trouble report, periodic statuses shall occur based on the following criteria:

- When the trouble has been isolated
- When there is a significant change in the status of the trouble.
- The negotiated status interval has expired.

Where mechanized trouble notification is utilized, the receiving company shall status their appropriate systems, in addition it shall be the responsibility of the company issuing the trouble report to poll the mechanized status system for the status of the trouble report.

Escalations if necessary shall be in accordance with identified procedures.

5.20 Network Modification Notification

A Network Modification is any type of planned equipment, software, trunk or facility activity that has the potential to significantly affect interconnected networks (e.g. rearrangement of existing network elements, switch homing arranges, SS7 rehomeing).

The NGIIF has developed the following guidelines outlining the medium by which internetwork affecting maintenance activity notification will be provided to the interconnected company and the time frame prior to the planned activity:

- Notification when possible should be made at least 5 working days prior to the planned change activity.
- Notification should be made in the form of:
 - E-Mail (recommended where available),
 - FAX or,
 - Telephone call.

- Notification should be provided to the affected company's appropriate notification center. Contact information is included in the NGIIF Service Provider Contact Directory. An example of a notification form is located in the NM Section, Part VI, of the NGIIF Reference Document.

When a Network Modification is scheduled that could significantly affect traffic between directly interconnected networks, it is recommended that the interconnecting parties notify each other, prior to the event.

The following information should be exchanged at the time of notification:

- Originator, (company name/contact number)
- Affected Network Element
- Date and Time of the Change
- Expected Duration
- Traffic Types Affected During Change
- Description of the Work to be Completed

6 END-TO-END AND INTERCARRIER TESTING

Circuit networks comprising ASP and ASC services may experience trouble conditions that cannot be isolated by each carrier testing and maintaining its own services. Although, the portions provided by each ASC and each ASP apparently perform properly, a trouble may be identifiable on an end-to-end service. In such cases the ASC may require coordinated testing. It is the responsibility of the ASC to coordinate inter-carrier and/or end-to-end testing with each sectional provider (i.e., other ASCs, ASPs). ASP participation in coordinated testing may be billable to the ASC.

7 ESCALATIONS

Escalation is a means of bringing provisioning and maintenance problems to the attention of individuals responsible for or having appropriate authority to initiate corrective action. When either the ASC or ASP is experiencing provisioning or maintenance difficulties that are not being resolved, the ASC and/or ASP shall contact the designated reporting office and request status from the responsible technician or first level supervisor. If the ASC or ASP is not satisfied with the effort to resolve a problem, the ASC and/or ASP may escalate according to locally negotiated guidelines.

8 TEST LINES

Feature Group A (FG A, line-side terminated) Switched Access Service provides seven digit access to balance (100 type) and milliwatt (102 type) test lines in the terminating direction where equipment is available.

Access to ASP test lines for WATS Access Lines where available will be provided.

ASC may obtain test line access information by contacting the Test Line Coordinator of the company with which they are performing testing. The contact number for ASP Test line Coordinators are listed in the NGIIF Service Provider Contact Directory under Testline Coordinator.

9 ADDITIONAL BILLING

The additional billing information contained in this document is of a general nature.

Provision has been made for billing the ASC for labor costs which are in excess of those that the ASP would have incurred had normal installation and repair functions been performed during scheduled hours. Provision has also been made for billing labor charges for work other than normal installation and repair.

9.1 Overtime Installation and Repair

Overtime is the time spent by ASP personnel doing installation and repair functions outside their scheduled working hours. The ASP must insure that internal documents include the appropriate entry to establish and uniquely identify any charges, which result from restoration or installation of a service with TSP assignments.

When an ASC requests work to be done outside scheduled hours, such requests should be coordinated through the ASP.

The ASP employee should ascertain the nature of the work being requested and the specific date and time the ASC wishes to begin the work.

Repair and installation overtime hours, which are considered billable to the ASC, are outlined in the following:

- When ASP personnel are required to work on a non-scheduled basis, the billable overtime hours begin at the start time requested by the ASC and end when the job is completed or the ASP personnel have been released by the ASC. Only those hours worked outside scheduled hours are billable. This includes travel time to and from a work location if a change in work location is required.
- When ASP personnel are called out for ASC installation or repair work, the normal travel time from home, the work time, and the normal travel time back home are billable. A call out of a ASP employee is subject to a minimum charge of 4 hours.

9.2 Additional Cooperative Acceptance Testing

Any transmission measurements or signaling tests over and above those specified as the normal acceptance test requirements in the Access Service Technical References and/or the appropriate tariff(s) are considered additional and will be billed to the ASC.

9.3 Stand-by Time

Stand-by Time includes all time in excess of one half (1/2) hour during which ASP personnel stand-by to make cooperative tests to verify repair of a given service with the ASC.

9.4 Non-Scheduled Testing

Non-scheduled testing can be requested by an ASC and may consist of any test, e.g., loss, noise, etc. which the ASC may require.

The ASC may request non-scheduled testing when maintenance testing, end-to-end service testing, intercarrier testing, or other testing is desired and ASP assistance is required.

Requests for and agreement to participate in the performance of an ASC's non-scheduled tests must be between the ASC and the ASP and will be performed at a mutually agreed upon schedule. The ASP should advise the ASC that non-scheduled testing is billable.

The ASC may use the provisions of non-scheduled testing to schedule meets of ASP, Vendor, and ASC technicians.

If during non-scheduled testing a trouble is found in ASP provided facilities, the ASC will not be billed for the time spent repairing any ASP specific trouble found.

9.5 Maintenance of Service Charge

The ASC shall be responsible for payment of a Maintenance of Service Charge for dispatches to the ASC location and/or its end user's premises by the ASP if either of the following conditions apply:

- Where the trouble results from equipment or communications systems provided by other than the ASP
- In the event the trouble is not found to be in the ASP facilities

If trouble is subsequently found to be in the ASP equipment or facilities, where a Maintenance of Service Charge has been applied, the charge will be canceled.

9.6 Other Labor

As agreed to by the ASP and the ASC, additional labor not identified by the following, may also be undertaken:

- Overtime Installation and Repair
- Additional Cooperative Acceptance Testing,
- Stand-by Time,
- Non-scheduled Testing,
- Maintenance of Service Charge,
- TSP Service

Requests from the ASC to provide additional labor, not identified above, must be mutually agreed to by the ASP and the ASC before such work is undertaken. This work is billable.

10 ACCESS SERVICES PROVIDED BY MULTIPLE EXCHANGE CARRIERS

These procedures apply when Access Service is provided by two or more ASPs within the same LATA.

The ASC will order from the ASPs the access service(s) required to provide its overall service.

For multi-ASP Access Service, it is recommended that a single Access Service Provider Coordination (ASPC) point, specific to the installation function being performed, be specified.

Before an Access Service Request (ASR) is issued by the ASC for an access service involving multiple ASPs, the ASPs involved should have a mutually agreeable working arrangement in place to allow one of the ASPs to be the ASPC, for the installation of access service.

Each ASP is responsible for working cooperatively with ASCs and other ASPs to ensure that access services are installed, tested, and turned up in a timely manner and that trouble conditions are resolved without undue delay and participate in repair verification as required.

10.1 Installation

Installation as used in this document pertains to that portion of the total provisioning process which starts when the order, e.g., "Work Order Record and Detail (WORD) or equivalent is received by the ASPs and includes installations, changes, and disconnects.

The ASPC will:

- Ensure that its company's equipment and facilities are installed and tested by the Plant Test Date (PTD).
- Receive and log status from the Other Access Service Provider (OASP) on the Designed Verified and Assigned Date (DVA) or equivalent. If the OASP has not provided status within 24 hours after DVA or equivalent, the ASPC will contact the OASP and request status.
- Prior to cooperative acceptance tests, schedule and coordinate pre-service tests to ensure that the overall access service is installed correctly and meets design parameters.
- Upon completion of the pre-service tests, the ASPC will contact the ASC and advise that the access service is ready to be turned up. The ASC has the option of acceptance with or without cooperative acceptance testing. The ASC is not obligated to accept the service prior to the due date.
- When an access service has a TSP code, this code should be verified between the ASPC and OASP.

When Intelligent NCTE is deployed by the ASP, the dispatch to perform Cooperative Acceptance tests will be waived by the ASC. The ASC, upon request, will be provided the remotely aligned tests results obtained by the ASP. If the ASC requests Cooperative Acceptance testing, the ASP will test remotely, using the diagnostic features of the Intelligent NCTE. Excluding the following conditions, an ASP technician will not normally be dispatched to the end user's location to perform Cooperative Acceptance tests. The conditions are:

- The unit is not equipped to perform the basic turn-up tests.
- The ASC requests specific Additional Cooperative Acceptance Tests, i.e., conditioning.
- The unit is inoperable.
- If the circuit does not meet Acceptance parameters.

The OASP will:

- Ensure that its company's equipment and facilities are installed and tested by PTD.
- Contact the ASPC and provide circuit status.
- Cooperate with the ASPC to perform the pre-service tests and acceptance tests as required.
- When an access service has a TSP code, this code should be verified between the OASP and ASPC.

The end user ASP for Special Access and WATS Access Lines will arrange for field forces to be dispatched when required and participate in the acceptance testing with the ASC.

When Intelligent NCTE is deployed by the ASP, the dispatch to perform Cooperative Acceptance tests will be waived by the ASC. The ASC, upon request, will be provided the remotely aligned tests results obtained by the ASP. If the ASC requests Cooperative Acceptance testing, the ASP will test remotely, using the diagnostic features of the Intelligent NCTE. Excluding the following conditions, an ASP technician will not normally be dispatched to the end user's location to perform Cooperative Acceptance tests.

The conditions are:

- The unit is not equipped to perform the basic turn-up tests.
- The ASC requests specific Additional Cooperative Acceptance Tests, i.e., conditioning.

- The unit is inoperable.
- If the circuit does not meet Acceptance parameters.

For FG A, the first point of switching ASP will arrange for field forces to be dispatched when required and participate in the acceptance testing with the ASC.

10.2 Maintenance

The ASC will be responsible for acceptance of trouble reports from its end user. The ASC should first test its facilities to determine if the trouble is in its network. If a trouble is found, the ASC will clear the trouble and no referral to an ASP is necessary. If the trouble is sectionalized by the ASC towards a connecting ASP the trouble report will be referred to the appropriate ASP based on the following criteria:

- Switched Services - the ASP with the 1st point of switching.
- Multipoint Specials (ASP Bridged Services) - the ASP that is providing the bridging function.
- Point-to-point Specials - at the discretion of the ASC based on available information/analysis.

The ASP(s) will work cooperatively with the ASC to sectionalize the trouble.

The following information should be exchanged when handing off or referring the trouble:

- Trouble report number or equivalent
- Contact telephone number
- Circuit ID (i.e. name or initials)
- Time and date report was received from ASC
- ASC testing information (If requested by ASP)
- Contact ID (41 Character CLCI)
- Non-Circuit specific (Circuit ID may not be appropriate)
- Trouble reported
- Other information that may be of assistance (e.g., history, subsequent reports)

Upon receipt of a trouble report from the ASC, the ASP will conduct, independently or cooperatively with the ASC, tests required to determine if the trouble is in its own equipment and facilities or the point of interface of an adjacent OASP(s).

If the trouble is found to be in the ASP's equipment or facilities, the trouble report will be closed out with the ASC and the following information will be provided:

- Trouble report number or equivalent
- Date & Time Cleared
- Status of Circuit(s) [temporary or permanent repair]
- -- If temporary, estimated time of restoral
- Contact name or initials and telephone number of the person closing out the report
- Type & Nature of trouble found and action taken

- ASP Testing Information (if Requested by ASC)
- Circuit ID (e.g., 41 character CLCI where applicable)

If no trouble is found in the ASP's own network, they shall refer/hand-off the trouble to the OASP and provide the following information:

- Trouble report number or equivalent (ASC)
- Contact telephone number (ASC)
- Circuit ID (ASC) (i.e., name or initials)
- Time and date report was received from ASC
- ASP Testing information (If requested by OASP)
- 41 Character CLCI for circuit specific problems
- Non-Circuit specific (If applicable e.g., 41 CLCI character where available)
- Trouble reported
- Other information that may be of assistance (e.g., history, subsequent reports, ASC Testing information, if available)

In the event a premature or improper hand-off has occurred, the ASP will resume cooperative testing with the OASP in order to sectionalize the trouble.

When the ASP has referred/handed off the trouble report to an OASP, the ASP will close out the trouble report with the ASC and provide the following information:

- Trouble report number or equivalent (ASC)
- Trouble report number of OASP
- Time and date report was referred/handed off to the OASP
- Contact telephone number (OASP)
- Contact ID (OASP) (i.e., name or initials)
- ASP Testing information (If requested by ASC)
- Trouble disposition (Test OK, NTF, Found OK)
- Circuit Identification (if applicable e.g., 41 character CLCI where available)
- Contact Name or initials of person closing the report

If the trouble report requires further hand-off/referral by the OASP to succeeding ASPs, the identity of the OASP switches to ASP when the referral is made.

The OASP will:

- Cooperatively test with the ASP to determine trouble location.
- Accept the trouble report when sectionalized into its equipment or facilities.
- The OASP will provide status to the ASC upon request.
- Upon clearing trouble, contact the ASC to close out the trouble report.

Trouble Ticket Exceptions - The following information is provided in an effort to assist service providers and service Customers in the resolution of troubles that fall outside of the normal ticket resolution flow once the original ticket has been closed out with the ASC.

Request for Test Assistance - When a request for a test assist is made to an ASP, the ASP shall provide the necessary assistance to facilitate the request. A ticket (non-measured) shall be created for administration of test assist referrals. A subsequent request for a test assist may result in additional tickets being created. In the event that additional tickets are created all relevant information from the prior trouble tickets/test assist tickets should be cross-referenced.

Request for Escalation Assistance From ASC - It is the responsibility of all service providers and service customers to work cooperatively to resolve all trouble reports as expeditiously as possible. The ASC is responsible for escalations to an OASP associated with trouble tickets when the trouble has been isolated/referred by an ASP to an OASP. When a request for escalation assistance is made by the ASC to an ASP, the ASP will provide any information concerning escalation numbers or names that they may have to the requesting ASC. At the ASC manager's request, the ASP manager may participate on a phone call in an attempt to assist the ASC in escalating to the OASP. If the ASC refers the problem back to the ASP, it should be understood that the process will reinitiate at the escalation level when the problem was initially referred into the OASP.

In the event the trouble cannot be sectionalized (e.g., no trouble found, intermittent type of problems), then the ASC and all ASPs/OASPs will cooperatively work together (e.g., cooperative testing) to locate and/or isolate the problem. Once the problem has been sectionalized then the previously developed process for ASP/OASPs shall be followed.

If repair verification with the ASC indicates trouble is still present, the ASP attempting to close out the trouble report will reinitiate testing with the other ASP(s).

10.3 Common Completion

A common completion date will be utilized by all involved ASPs. Therefore, no ASP may complete its order until the entire Access Service is completed and accepted by the ASC.

10.4 Jeopardy

If one or more ASPs cannot complete its portion of the overall Access Service on the Due Date, this should be considered a jeopardy situation by all ASPs involved. If, after a specified period of time (to be determined locally) past the due date, the overall Access Service remains incomplete due to ASP problems, those ASPs who completed their portion of the Access Service will review the status of the incomplete portions via the ASPC. The ASP whose portion of the work is incomplete will determine the actual or approximate duration of the existing jeopardy condition and notify the ICSC or equivalent.



ATIS-0300010

ATIS Standard on -

**Next Generation Interconnection Interoperability (NGIIF)
Reference Document: Part II, Installation and Maintenance
Responsibilities Switched Access Services Feature Group B, C,
and D**



As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-IP transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [http://www.atis.org/legal/patentinfo.asp] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

Copyright © 2020 by Alliance for Telecommunications Industry Solutions
All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < <http://www.atis.org> >.

ATIS Standard on

Next Generation Interconnection Interoperability (NGIIF) Reference Document: Part II, Installation and Maintenance Responsibilities Switched Access Services Feature Group B, C, and D

Alliance for Telecommunications Industry Solutions

Approved September 17, 2020

Abstract

This document outlines telecommunications service provider and customer installation and maintenance responsibilities for Switched Access Services (SAS) as established by the Next Generation Interconnection Interoperability Forum (NGIIF) and includes Telecommunications Service Priority (TSP) Guidelines. It includes procedures on installation and maintenance of trunk side connected Access Services Feature Groups (FG) B, C, and D. It specifically includes areas such as NXX Code Openings, FG D CIC Testing, Network Modification Notification, Trouble Detection Responsibilities, Trouble Reporting Procedures, 500/800/900 NXX Services, Toll-Free Database and LIDB Services Trouble Handling, and access services provided by multiple exchange carriers. Where applicable, this document may address Next Generation Network (NGN) aspects.

Foreword

The Alliance for Telecommunications Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The Next Generation Interconnection Interoperability Forum (NGIIF) addresses next-generation network interconnection and interoperability issues associated with emerging technologies. Specifically, it develops operational procedures which involve the network aspects of architecture, disaster preparedness, installation, maintenance, management, reliability, routing, security, and testing between network operators. In addition, the NGIIF addresses issues which impact the interconnection of existing and next generation networks and facilitate the transition to emerging technologies.

The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages. The word *may* denotes an optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, NGIIF, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, NGIIF, which was responsible for its development, had the following leadership:

Karen Riepenkroger, Sprint

Randee Ryan, Comcast

Trademark Acknowledgements

iconectiv®, Telcordia®, and Common Language® are registered trademarks and CLCI™, CLI™, LERG™ Routing Guide and TPM™ Data Source are trademarks and the Intellectual Property of Telcordia Technologies, Inc. dba as iconectiv.

Table of Contents

1	SCOPE, PURPOSE, & APPLICATION	1
2	INFORMATIVE REFERENCES	1
3	DEFINITIONS, ACRONYMS, & ABBREVIATIONS.....	2
3.1	ACRONYMS & ABBREVIATIONS.....	2
4	GENERAL.....	3
5	RESPONSIBILITIES.....	3
5.1	ACCESS SERVICE CUSTOMER (ASC)	3
5.2	ACCESS SERVICE PROVIDER (ASP)	4
6	NXX OR NXX-X CODE OPENINGS.....	5
6.1	NXX OF NXX-X CO CODE ACTIVATION PLANNING.....	6
6.2	PRE-NXX OR NXX-X ACTIVATION	6
6.2.1	<i>BIRRDS</i>	6
6.2.2	<i>iconectiv® LERG™ Routing Guide</i>	6
6.2.3	<i>Facilities</i>	6
6.2.4	<i>Points of Interconnection</i>	6
6.3	TRANSLATION VALIDATION/CALL THROUGH TESTING.....	7
6.4	INTERMEDIATE OFFICE(S) (TANDEMS/ACCESS TANDEMS)	7
6.5	LEC TERMINATING OFFICE (SERVING OFFICE)	7
6.6	ORIGINATING OFFICE	8
6.7	MECHANIZED TESTING	8
6.8	VERIFICATION OF NXX OR NXX-X CODE OPENINGS	8
6.9	CODE OPENING JEOPARDY SITUATIONS	8
6.10	CODE OPENING CONTACT INFORMATION	8
7	FG D CIC TESTING.....	9
8	NETWORK SERVICE CENTER (NSC)	9
9	NETWORK MODIFICATION NOTIFICATION.....	9
9.1	NETWORK MODIFICATION SUSPENSION PERIODS	11
10	TELECOMMUNICATIONS SERVICE PRIORITY (TSP) GUIDELINES.....	12
11	SWITCHED ACCESS SERVICE INSTALLATION.....	12
11.1	SAS ORDER ACTIVITY	12
11.2	ESTABLISHING AN INTERFACE	12
11.3	PRE-SERVICE TESTING.....	12
11.4	COOPERATIVE ACCEPTANCE TESTING - ANALOG	12
11.5	SWITCHED DIGITAL DATA ACCESS SERVICE (56KBS, 64KBS, ISDN PRIMARY & BASIC RATE).....	13
11.5.1	<i>Switched Digital Data Services Stress Test Patterns (56kbs, 64kbs, ISDN Primary & Basic Rates)</i>	13
11.5.2	<i>Switched Digital Data Services Acceptance/ Maintenance Requirements (56kbs, 64kbs, ISDN Primary & Basic Rates)</i>	15
11.6	ADDITIONAL COOPERATIVE ACCEPTANCE TESTING (ACAT).....	15
11.7	TRAFFIC ROUTING & BILLING ACCEPTANCE TESTING	16
11.7.1	<i>ASC</i>	16
11.7.2	<i>ASP</i>	16
11.8	COMPLETIONS	16
11.9	SAS DISCONNECTS.....	16
11.10	SAS REARRANGEMENTS	16
11.11	COORDINATED CONVERSIONS	17
11.12	GLARE	17
12	SWITCHED ACCESS SERVICE MAINTENANCE.....	18

ATIS-0300010

12.1	ROUTINE MAINTENANCE	18
12.2	POTENTIAL SERVICE AFFECTING ACTIVITIES	18
12.3	DEFERRED SERVICE RESTORATION	18
12.4	SCHEDULED & NONSCHEDULED TESTING	18
12.5	LOCAL/TANDEM PAD OPERATION	18
12.6	TEST LINES.....	19
12.7	LINESIDE (CALL THROUGH/ROUTING) TESTING	19
12.8	TESTING THROUGH AN ACCESS TANDEM.....	19
13	TROUBLE DETECTION RESPONSIBILITIES.....	19
13.1	INOPERATIVE & IMPAIRED CIRCUITS	19
13.2	SYNCHRONIZATION	19
13.3	REPAIR VERIFICATION TESTS	19
13.4	RESTORAL PRIORITIZATION	20
13.5	NORMAL MAKE-BUSY PROCEDURE FOR SAS.....	20
13.5.1	Single Trunk Make-Busy.....	20
13.5.2	Trunk Group Make-Busy (Facility Failure).....	20
13.5.3	Trunk Group Make-Busy (Maintenance).....	21
13.6	EXPEDITED MAKE-BUSY PROCEDURE	21
13.7	REQUESTS FOR CIRCUIT TRACE	21
13.8	EMERGENCY CALL TRACING	21
13.9	KILLER TRUNK IDENTIFICATION.....	22
14	TROUBLE REPORTING PROCEDURES FOR FGS B, C, & D.....	22
14.1	CHRONIC TRUNK FAILURES	22
14.2	SWITCHED ACCESS NETWORK TROUBLE.....	22
14.3	CALL SETUP TIME TROUBLE REPORTING & SECTIONALIZATION.....	23
14.4	TROUBLE CLEARANCE REPORTING.....	24
14.4.1	Access Provider/Access Customer Trouble.....	24
14.5	ESCALATION	25
14.6	TROUBLE REPORT STATUS	25
15	ADDITIONAL BILLING	25
15.1	BILLABLE OVERTIME INSTALLATION & REPAIR	26
15.2	ADDITIONAL COOPERATIVE ACCEPTANCE TESTING.....	26
15.3	NON-SCHEDULED TESTING.....	26
15.4	MAINTENANCE OF SERVICE CHARGE.....	26
15.5	STAND-BY TIME.....	26
15.6	OTHER LABOR.....	26
16	5XX/8YY/9YY NXX SERVICES	27
16.1	RESPONSIBILITIES.....	27
16.2	INSTALLATION.....	27
16.3	TROUBLE REPORTING/REFERRAL	28
17	TOLL-FREE DATABASE SERVICES.....	28
17.1	RESPONSIBLE ORGANIZATION (RESP ORG).....	28
17.2	TREATMENT.....	29
17.3	TROUBLE REPORTING	29
17.4	DISASTER RECOVERY PLANS.....	29
17.5	ROUTINE MAINTENANCE FOR SERVICE END POINT (SEP) POWER SOURCES	29
18	TOLL-FREE DATABASE SERVICES-TROUBLE HANDLING PROCEDURES	29
18.1	TROUBLE REPORT.....	30
18.1.1	Trouble Report - NON-SMS Access (e.g., Resellers)	30
18.1.2	Trouble Report - SMS Access.....	30
18.2	TROUBLE REFERRAL.....	30
18.2.1	Resp Org Responsibilities	30

18.2.2	Severity Level Matrix	31
18.3	TROUBLE CLOSURE	31
19	INDUSTRY INTER-COMPANY ABS/LIDB TROUBLE REPORTING	31
19.1	SCOPE	31
19.2	BACKGROUND	32
19.3	TROUBLE IDENTIFICATION	32
19.3.1	LIDB Problems	33
19.3.2	LIDB Trouble Referrals	33
19.3.3	OSS Detected Problems	33
19.3.4	SS7 Network Problems	34
19.3.5	LASS/LARG Data Problems	34
19.4	TROUBLE REPORTING	34
19.4.1	Reporting Network Routing Troubles	34
19.5	TROUBLE CLOSURE	35
20	ACCESS SERVICES PROVIDED BY MULTIPLE EXCHANGE CARRIERS	35
20.1	INSTALLATION	35
20.2	COMMON COMPLETION	36
20.3	JEOPARDY	36
20.4	MAINTENANCE	36
20.5	TROUBLE REPORT EXCEPTIONS	38
20.5.1	Request for Test Assistance	38
20.5.2	Request for Escalation Assistance from ASC	38
20.5.3	Additional Escalation Information	38
21	LOCAL NUMBER PORTABILITY	38
21.1	DEFAULT ROUTING TRANSLATIONS	38
21.2	BACKGROUND ON DEFAULT ROUTING TRANSLATIONS:	39
21.2.1	Originating Test Procedure	41
21.2.2	Terminating Test Procedures	41

Table of Figures

FIGURE 21.1 - ACCEPTANCE TESTING DECISION CHART	39
FIGURE 21.2 - CALL SETUP TIME (CST) TESTING METHODOLOGY	40
FIGURE 21.3 - CALL SETUP TIME	41
FIGURE 21.4 - CALL SETUP TIME	41
FIGURE 21.5 - INDUSTRY INTER-COMPANY ABS/LIDB TROUBLE REPORTING	42

Table of Tables

TABLE 9.1 - NETWORK MODIFICATION SUSPENSION TIME PERIODS	11
TABLE 11.1 - PATTERN SENSITIVITY TEST CRITERIA FOR 56/64 KBIT/S	13
TABLE 11.2 -TEST LIMITS AND OBJECTIVES FOR 56/64KBIT/S SERVICE	15

ATIS Standard on –

Next Generation Interconnection Interoperability (NGIIF) Reference Document: Part II, Installation and Maintenance Responsibilities Switched Access Services Feature Group B, C, and D

1 Scope, Purpose, & Application

This document outlines telecommunications service provider and customer installation and maintenance responsibilities for Switched Access Services (SAS) as established by the NGIIF and includes Telecommunications Service Priority (TSP) Guidelines. It includes procedures on installation and maintenance of trunk side connected Access Services Feature Groups (FG) B, C and D. It specifically includes areas such as NXX Code Openings, FG D CIC Testing, Network Modification Notification, Trouble Detection Responsibilities, Trouble Reporting Procedures, 500/800/900 NXX Services, Toll-Free Database and LIDB Services Trouble Handling, and access services provided by multiple exchange carriers. Where applicable, this document may address Next Generation Network (NGN) aspects.

2 Informative References

The following standards contain provisions which, through reference in this text, constitute provisions of this Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

ATIS-0100510, *Digital Services for Rates Up to and Including DS3-Specifications*.¹

ATIS-0300010, *Next Generation Interconnection Interoperability (NGIIF) Reference Document: Part II, Installation and Maintenance Responsibilities Switched Access Services Feature Group B, C, and D*.¹

ATIS-0300011, *Next Generation Interconnection Interoperability (NGIIF) Reference Document: Part III, Installation and Maintenance Responsibilities for SS7 Links and Trunks*.¹

ATIS-0300024, *Next Generation Interconnection Interoperability (NGIIF) Reference Document Part V, Test Line Guidelines*.¹

ATIS-0300026, *Next Generation Interconnection Interoperability (NGIIF) Reference Document: Part VI, Network Management Guidelines*.¹

ATIS-0300032, *Next Generation Interconnection Interoperability (NGIIF) Reference Document: Part X, Interconnection Between LECS Operations Handbook – Local Interconnection Service Arrangement*.¹

ATIS-0300046, *Recommended Notification Procedures to Industry for Changes in Access Network Architecture*.¹

ATIS-0300119, *Thousands-Block (NPA-NXX-X) & Central Office Code (NPA-NXX) Administration Guidelines (TBCOCAG)*.¹

ATIS-0300104, *Next Generation Interconnection Interoperability Forum (NGIIF) NGN Reference Document - NGN Basics, Emergency Services, NGN Testing, and Network Survivability*.¹

¹ This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at: < <https://www.atis.org/docstore> >.

ATIS-0300206.2001(S2016), *Digital Exchanges and PBXs - Digital Circuit Loopback Test Line with N [infinity] DSO Capability*.¹

ATIS-0404000, *Access Service Request Guidelines*.¹

3 Definitions, Acronyms, & Abbreviations

For a list of common communications terms and definitions, please visit the *ATIS Telecom Glossary*, which is located at < <http://www.atis.org/glossary> >.

3.1 Acronyms & Abbreviations

ACAT	Additional Cooperative Acceptance Testing
AMA	Automatic Message Accounting
ASC	Access Service Customer
ASP	Access Service Provider
ASPC	Access Service Provider Coordinator
ASR	Access Service Request
ATIS	Alliance for Telecommunications Industry Solutions
CPE	Customer Premises Equipment
FCC	Federal Communications Commission
FG	Feature Group
ICSC	Interconnection Customer Service Center
INC	Industry Numbering Committee
LEC	Local Exchange Carrier
LSC	Local Service Customer
LSP	Local Service Provider
NGIIF	Next Generation Interconnection Interoperability Forum
NSC	Network Service Center
NS/EP	National Security Emergency Preparedness
POT	Point of Termination
PUC	Public Utilities Commission
SAS	Switched Access Services
SS7	Signaling System 7
TCIC	Trunk Circuit Identification Code
TQ	Translation Questionnaire
TSP	Telecommunication Service Priority

4 General

This document outlines Access Service Customer (ASC) and Access Service Provider (ASP) responsibilities for Switched Access Services (SAS) as established by the Next Generation Interconnection Interoperability Forum (NGIIF). It is intended to be a living document to aid operations work forces. It does not replace nor supersede Tariffs, Contracts, or any other legally binding documents. It is limited to procedures on installation and maintenance of trunk side connected Access Services FG B, C, and D.

Guidelines for the Installation and Maintenance of Facilities, Signaling System 7 (SS7), Specials, Network Management, Test Coordinator, and FG A are included in separate Clauses of the NGIIF Reference Document.

This document covers other operational and technical agreements made at the Next Generation Interconnection Interoperability Forum.

The ASCs are communications common carriers authorized by the Federal Communications Commission (FCC) to provide interLATA, interstate communications and/or by state Public Utilities Commissions (PUCs) to provide interLATA, intrastate or intraLATA communications services to their end users. The ASCs may request ASPs provide various facilities to be used as part of the ASC's services.

5 Responsibilities

5.1 Access Service Customer (ASC)

The ASC has the overall installation and maintenance responsibility for the total service to its end user. It is responsible for the overall coordination of installation and testing of its services.

The following are the responsibilities of the ASC:

- Provide end-to-end service for their end users
- Provide trained personnel
- Advise the ASP when there is a potential service affecting ASC network failure
- Provide a contact number for trouble reporting that is readily accessible 24 hours a day, 7 days a week
- Maintain complete and accurate installation and repair records
- Provide ASP personnel access to the Point of Termination (POT) when required
- Provide access to testlines where appropriate
- Provide billing authorization to the ASP for any additional labor requested
- Ensure that test equipment used is compatible with the Local Service Provider's (LSP's) test equipment
- Cooperate with the ASP ensuring that trunks are installed in accordance with the service requests
- Notify the ASP of any changes affecting the service request, including the service due date
- Assume control functions for maintenance of its trunk(s)
- Consult with the ASP before making any changes that could affect service, except under emergency conditions
- Accept trouble reports from their end users
- Accept trouble reports from the ASPs
- Sectionalize and clear the trouble in its own network
- Tests cooperatively with the ASP to further isolate and clear the trouble
- Keep their end users advised of the status of all trouble report(s)

- Perform cooperative analysis to determine if a trouble pattern exists
- Refer troubles to the ASP using the trouble reporting procedures
- Dispatch its own maintenance forces
- Perform verification test to ensure that trouble has been cleared
- Perform scheduled testing and other maintenance services when requested
- Participate cooperatively with the LSP to further isolate and clear the trouble when trouble exists and cannot be sectionalized
- Provide access to the CIC validation number that is 700-555-4141 for routing/billing verification purposes. Such a CIC validation number shall terminate at a recorded announcement and shall indicate the carrier reached
- Where it is technically feasible, signaling for all internetwork calls to a 10-digit telephone number should always be sent or received using 10 digits for the called party number, independent of how the call is dialed.

5.2 Access Service Provider (ASP)

The ASP is responsible for ensuring that the SAS furnished to an ASC is installed and functions properly. In addition, the ASP should work cooperatively with the ASC in the acceptance testing of the SAS it provides.

Where the ASC is unable to perform cooperative testing at its POT, the ASP will provide test results from nearest ASP test access point, toward the ASC's POT. An Access Service Provider Coordinator (ASPC) will perform the control function for the installation of FG B, C, and D, SAS provided to the ASCs.

The following are the responsibilities of the ASP:

- Provide SAS to ASCs as set forth by their Access Service Tariffs and will show no discrimination between different ASCs
- The SAS provided by the ASP will include all wiring, cable, and facilities up to the POT
- Installation, operation and maintenance of Access Service within its operating area including the right to negotiate control responsibility to another entity
- Provide trained personnel
- Advise the ASC when there is a potential service affecting ASP network failure
- Provide a contact number for trouble reporting that is readily accessible 24 hours a day, 7 days a week
- Maintain complete and accurate installation and repair records
- Consult with the ASC before making any changes that could affect service except under emergency conditions
- Provide access to testlines where appropriate
- Assume control functions for installation of the trunk(s)
- Cooperate with the ASC ensuring that trunks are installed in accordance with the service requests
- Notify the ASC of any changes affecting the service request, including the service due date
- Accept trouble reports from the ASC
- Sectionalize and clear the trouble in its own network
- Test cooperatively with the ASC to identify and clear a trouble when the trouble has been sectionalized to the ASC network
- Perform cooperative analysis to determine if a trouble pattern exists
- Refer troubles to the ASC using the trouble reporting procedures

- Dispatch its own maintenance forces
- Clear troubles in its own network
- Perform verification test to ensure that trouble has been cleared
- Provide status reports to the ASCs regarding installation and repair activity
- Perform scheduled testing and other maintenance services when requested
- Participate cooperatively with the Local Service Customer (LSC) to further isolate and clear the trouble when trouble exists and cannot be sectionalized to the ASC or ASP portion
- Provide ASC personnel access to the POT
- Inform the ASC when additional billing is required
- Advise the ASC when there is a potential service affecting ASP network failure
- Cooperate with other ASP offices and the ASC in testing to isolate and clear the trouble
- Perform scheduled or non-scheduled testing (billable as per the tariff) when requested
- Where it is technically feasible, signaling for all internetwork calls to a 10-digit telephone number should always be sent or received using 10 digits for the called party number, independent of how the call is dialed.

6 NXX or NXX-X Code Openings²

NOTE: For information related to NPA-NXX testing refer to ATIS-0300024, *Next Generation Interconnection Interoperability (NGIIF) Reference Document Part V, Test Line Guidelines*.

This Clause outlines the process and procedures for the testing of newly assigned Central Office NXX or NXX-X Codes opened for the first time. In addition, this Clause provides references for the user to ensure that they are familiar with the obligations associated with obtaining codes and notifying the industry of the pending opening of CO NXX Codes. In a Thousands Block Number Pooling environment the first thousands block that is opened in an NPA/NXX will follow the same rules as outlined in all NXX Code opening procedures. NPA/NXX and NPA/NXX-X are interchangeable in NXX Code opening scenarios throughout the NGIIF documentation. In these cases, the Code Holder is responsible for the testing.

The non-operational aspects contained in this Clause do not replace or supersede existing industry forum agreements or documents covering NXX or NXX-X Code opening processes. Listed below is specific documentation provided by ATIS' Industry Numbering Committee (INC) and NGIIF that provides guidance to Code Administrators, Service Providers and Service Customers when obtaining, activating, and testing NXX or NXX-X codes:

- ATIS-0300046, *Recommended Notification Procedures to Industry for Changes in Access Network Architecture*
- ATIS-0300010, *Next Generation Interconnection Interoperability (NGIIF) Reference Document: Part II, Installation and Maintenance Responsibilities Switched Access Services Feature Group B, C, and D*
- ATIS-0300032, *Next Generation Interconnection Interoperability (NGIIF) Reference Document: Part X, Interconnection Between LECS Operations Handbook – Local Interconnection Service Arrangement*
- ATIS-0300119, *Thousands-Block (NPA-NXX-X) & Central Office Code (NPA-NXX) Administration Guidelines (TBCOCAG)*

² Clause 7 of ATIS-0300032, *Next Generation Interconnection Interoperability (NGIIF) Reference Document: Part X, Interconnection Between LECS Operations Handbook – Local Interconnection Service Arrangement*, includes the same information on NXX Code Openings. Any changes to the current Clause should also be reflected in Clause 7 of ATIS-0300032, *Next Generation Interconnection Interoperability (NGIIF) Reference Document: Part X, Interconnection Between LECS Operations Handbook – Local Interconnection Service Arrangement*.

6.1 ***NXX of NXX-X CO Code Activation Planning***

Service Providers requesting CO Code activation where the code involves the use of newly established switching facilities or additional interconnection trunking should perform the following prior to call through testing:

- Set up a planning session with the appropriate service providers where the code is being opened to determine what types of interconnection arrangements are required.
- Issue Service Orders to establish the appropriate facilities using the Access Service Request (ASR) and or translations using the Translation Questionnaire (TQ) for routing purposes. The following practices can be found within ATIS-0404000, Access Service Request Guidelines (ASR):³
 - ATIS-0404001, *Access Service Request (ASR) Form Preparation Guide*
 - ATIS-0404000, *Feature Group B, C, D (FG-B, C, D) Form Preparation Guide (Clause 10, Trunking)*
 - ATIS-0404019, *Translation Questionnaire (TQ) Form Preparation Guide.*

6.2 ***Pre-NXX or NXX-X Activation***

The following reference is provided to aid in the performance of activation and testing of CO NXX or NXX-X Codes.

6.2.1 **BIRRDs**

Before a CO Code (NXX or NXX-X) can become active, the service provider requesting a new CO Code is responsible for either directly inputting the information in Part 2 of the CO Code Assignment Request form into BIRRDs, providing it to the Code Administrator, or another party with BIRRDs access for entry.

6.2.2 **iconectiv® LERG™ Routing Guide**

During the process of entering the new CO Code (NXX or NXX-X) in the iconectiv LERG Routing Guide, the Code Holder must identify the points of interconnection in the LATA where the CO Code resides. In addition, the Code Holder shall immediately assign a number to be utilized for call through testing purposes upon receipt of the CO Code and shall place the test number in the iconectiv LERG Routing Guide when entering the CO Code into the iconectiv LERG Routing Guide.

6.2.3 **Facilities**

Offices attempting to complete a call through test to the new CO Code (NXX or NXX-X) when the facilities are not in place shall contact the Code Holder and inform them that the routing of calls will not take place until the appropriate facility orders have been completed.

In cases where orders have been placed with Local Exchange Carriers (LECs) for facilities, but have not been implemented, the LEC shall provide the appropriate support to ensure that the orders are completed and appropriate testing has been performed to meet the due date.

6.2.4 **Points of Interconnection**

In cases where points of interconnection in the home NPA have not been identified and/or facilities have not been placed, the Code Holder (NXX or NXX-X) will accept full responsibility for placing such orders with the LEC and schedule the due date for facilities testing. This will ensure that the facilities are in place prior to the date of the code opening identified in the iconectiv LERG Routing Guide. The LEC cannot be expected to meet the original effective date in the iconectiv LERG Routing Guide if all supporting information is not received in a timely manner.

³ Access Service Ordering Guidelines (ASOG), available at <https://www.atis.org/docstore/>.

If interconnection already exists between service providers and a CO Code is being opened, the Code Holder shall provide appropriate routing information in the iconectiv LERG Routing Guide to inform other service providers with which they do not have direct interconnection.

Where direct interconnection exists between service providers, it is presumed that all new CO Codes would be routed the same way as existing CO Codes, unless otherwise specified by the Code Holder in the ASR.

6.3 *Translation Validation/Call through Testing*

The following process is outlined for the activation of new CO Codes (NXXs or NXX-X's) to provide assurance that routing and billing translations are tested/validated appropriately by all LECs and IXCs.

- Upon receipt of notification (iconectiv LERG Routing Guide) that a new CO Code is to be activated, the LECs and the IXCs shall ensure the integrity of routing and billing by the effective date in the iconectiv LERG Routing Guide.
- The new CO Code owner will provide a test number in the LERG that terminates to a recorded announcement (preferable) or milliwatt (1004 Hz) to provide assurance to personnel performing call through tests that they have reached the terminating (serving) office.
- Where billing is required, Automatic Message Accounting (AMA) validation shall take place by the LECs and the IXCs.

6.4 *Intermediate Office(s) (Tandems/Access Tandems)*

An Intermediate Office is an office(s) that calls would route through for InterLATA and IntraLATA purposes to reach someone in the newly opened CO Code (NXX or NXX-X). An intermediate Office shall:

- Complete all translations work five (5) calendar days prior to the date identified in the iconectiv LERG Routing Guide as the effective date.
- Perform call through testing starting five (5) calendar days prior to the date identified in the iconectiv LERG Routing Guide as the effective date.
- Identify problems during call through testing and resolve such problems prior to the effective date identified in the iconectiv LERG Routing Guide.

6.5 *LEC Terminating Office (Serving Office)*

The LEC Terminating Office is the office where a call terminates. The LEC will:

- Validate that all translations work is complete five (5) calendar days prior to the date identified in the iconectiv LERG Routing Guide as the effective date.
- Perform call through tests to ensure that calls can be initiated from the newly opened CO Code (NXX or NXX-X) starting five (5) calendar days prior to the date identified in the iconectiv LERG Routing Guide as the effective date. An interLATA or intraLATA call, and an intraoffice call to an existing CO Code, where applicable, should be performed within the serving office.
- Perform, where applicable, an intraoffice call from an existing CO Code within the serving office to the newly opened CO Code.
- Identify problems during call through testing and resolve such problems prior to the due date identified in the iconectiv LERG Routing Guide.

NOTE: If the above functions are not performed, the originating office and intermediate office cannot perform their respective functions.

6.6 *Originating Office*

LEC end offices with direct interconnection to, or located within the same NPA as the LEC with the newly opened CO Code (NXX or NXX-X), will:

- Validate that all translations work is complete five (5) calendar days prior to the date identified in the iconectiv LERG Routing Guide as the effective date.
- Initiate a call through test to the test number to ensure that the call routes correctly. Call through testing should start no earlier than five (5) calendar days prior to the date identified in the iconectiv LERG Routing Guide as the effective date.
- Identify problems during call through testing and resolve such problems prior to the effective date identified in the iconectiv LERG Routing Guide.

6.7 *Mechanized Testing*

Where mechanized translation input and validation is available, such mechanized capabilities should be used to validate the routing and AMA capability. This function should be performed on or before the effective date identified in the iconectiv LERG Routing Guide.

6.8 *Verification of NXX or NXX-X Code Openings*

During the CO Code (NXX or NXX-X) Opening process, some Code Holders may want to verify that test calls to their new CO Code have been completed. Therefore, it is recommended that entities performing call through tests to CO Codes being activated provide the necessary Caller ID information required to verify the NPA-NXX or NPA/NXX-X from where the test call is being placed. Where contractual, technical, or regulatory restrictions apply, this capability cannot be utilized.

6.9 *Code Opening Jeopardy Situations*

If prior to the iconectiv LERG Routing Guide effective date for an NXX or NXX-X code opening, a Code Holder realizes that any problem in its own network jeopardizes the scheduled NXX or NXX-X code opening date, the Code Holder will notify the interconnected carrier(s) immediately.

If prior to the iconectiv LERG Routing Guide effective date for an NXX or NXX-X Code opening, an interconnected carrier realizes that it will not be able to meet the iconectiv LERG Routing Guide effective date for opening the NXX or NXX-X Code, that carrier will notify the Code Holder and other interconnected carrier(s) immediately.

Any carrier that identifies a problem within another carrier's network during call through testing will notify that carrier immediately.

Contact should be made using industry escalation procedures or published/mutually agreed to contact information.

6.10 *Code Opening Contact Information*

Should an SP encounter a situation where a code opening did not occur on the effective date or the testing outlined in section 3.5 was not completed, the SP may utilize the contact information in the NGIIF Contact Directory⁴ to contact the company to resolve the testing/code opening issue.

⁴ <https://www.atis.org/committees-forums/ngiif/ngiif-contact-directories/>

7 FG D CIC Testing

The following process is recommended for the routing and billing when CICs are expanded or introduced. This process can be used to validate the opening of newly assigned CICs.

On completion of the switch translation for CIC expansion, the ASP will:

- Perform a validation of such translations and keep a record for audit purposes
- Place a call to each carrier assigned within that switch, utilizing a test CIC
- Call through tests will consist of:
 - Calls from all major classes of service within the switch
 - Calls will be made to an IntraLATA and InterLATA termination
 - Calls from 1+, 0+, 011+, 01+, 8YY+⁵, and 1-710-NCS-GETS
 - Utilizing a test number and an appropriate test response
- Ensure that Casual Dialing (101XXXX) is allowed and that routing and AMA recording are correct
- Generate an AMA record to ensure that the 4-digit CIC is present. All AMA records shall be retained for audit purposes
- Verify the AMA record for the presence of the 4-digit CIC when mechanized call through testing is utilized.

ASCs that are issued 4-digit CICs should coordinate with all interconnecting companies to ensure that calls will be passed from all selected areas of service.

The following announcement should be used when an invalid carrier access code is dialed: "we're sorry; your call cannot be completed with the access code you dialed. Please check the code and try again or call your long-distance company for assistance."

Subsequent to the end of the 3-digit to 4-digit CIC expansion transition period, the following announcement should be used when an invalid carrier access code is dialed: "Your call cannot be completed as dialed. If you dialed a 5-digit code, it has changed. Please redial adding a one and a zero before the 5-digit code, or for assistance, contact the carrier you are trying to use."

Any announcement associated with the end of the 5-digit CAC permissive dialing period should be played at a minimum until July 1, 1999.

8 Network Service Center (NSC)

The NGIIF recommends immediate reporting of non-circuit-specific troubles via telephone in order to facilitate the rapid restoral of service.

The NSC, or other regionally designated centers, will be the contact point for non-circuit specific trouble reports from the ASCs. The ASP will provide the ASC with a contact number, escalation, and guidelines for the reporting of non-circuit specific troubles. The NSC will provide status and feedback to the reporting ASC, when requested.

9 Network Modification Notification

A Network Modification is any type of planned equipment, software, trunk, or facility activity that has the potential to significantly affect interconnected networks (e.g. rearrangement of existing network elements, switch homing arranges, SS7 rehomings).

⁵ For Toll-Free, YY can be any of the following: 99, 88, 77, 66, 55, 44, 33, 22, and 00 when assigned.

ATIS-0300010

The NGIIF has developed the following guidelines outlining the medium by which internetwork affecting maintenance activity notification and the time frame prior to the planned activity will be provided to the interconnected company:

- Notification, when possible, should be made at least five (5) working days prior to the planned change activity.
- Notification should be made in the form of:
 - E-mail (recommended where available)
 - FAX
 - Telephone call
- Notification should be provided to the affected company's appropriate notification center. Contact information is included in the NGIIF Service Provider Contact Directory.⁶ An example of a notification form can be found in ATIS-0300026, *Next Generation Interconnection Interoperability (NGIIF) Reference Document: Part VI, Network Management Guidelines*.

Notifications that are made via the LERG Routing Guide:

- Network modifications (such as a rehome) will have an effective date in the LERG Routing Guide.

Any network modification not completed or rescheduled prior to the effective date in the LERG Routing Guide may result in routing errors, blocked, or incomplete calls etc.

Any network modification which has an effective date in the LERG Routing Guide must be completed by the effective date in the LERG Routing Guide. If rescheduled prior to the effective date in the LERG Routing Guide, it is recommended that an emergency notification request be submitted to iconectiv.

NOTE: Effective dates rescheduled seven (7) days prior to the effective date in the LERG Routing Guide can be entered into BIRRDs by the AOCN. However, effective dates rescheduled less than seven (7) days prior to the effective date in the LERG Routing Guide must be entered into BIRRDs by iconectiv.

Any network modification that will not be completed by the effective date in the LERG Routing Guide by the service provider initiating the change will be required to update BIRRDs to return the network entries back to what it was prior to the effective date in the LERG Routing Guide. It is recommended that an emergency notification request be submitted to iconectiv.

- The originating service provider may elect to have their AOCN contact iconectiv directly to "zap" the records with the current view thereby returning the records to what they were prior to the most recent effective date in the LERG Routing Guide of the previous view
- The originating company's AOCN will then update the LERG Routing Guide with the new effective date
- The originating company's AOCN will then issue an emergency notification request to iconectiv.

When the zapping method is used, it significantly increases the probability that the "zapped" record changes may be missed by the industry and interconnected companies will not react. This may result in network outages and or blocked calls because other service providers were unaware that the proposed changes did not take place.

When network modifications are scheduled that could significantly affect traffic between directly interconnected networks, it is recommended that the affected ASPs and ASCs notify each other prior to the event.

The following information should be exchanged at the time of notification:

- Originator, (company name/contact number)
- Affected Network Element
- Date and Time of the Change
- Expected Duration

⁶ The Service Provider Contact Directory and instructions for gaining access can be found on ATIS' website: https://www.atis.org/01_committ_forums/ngiif/contact-directories/.

- Traffic Types Affected During Change
- Description of the Work to be Completed

9.1 *Network Modification Suspension Periods*

Due to the volumes of traffic and the potential for negative impacts to the Network, the following table identifies when Network Modifications should not be performed.

Table 9.1 - Network Modification Suspension Time Periods

Network Modification Suspension Time Periods		
Event	Start of Suspension Period (Inclusive)	End of Suspension Period (Inclusive)
Mother's Day	SATURDAY	MONDAY
Father's Day	SATURDAY	SUNDAY
Thanksgiving (US Only)	WEDNESDAY	MONDAY
Christmas	12/22	12/26
New Years	12/31	1/1

Network modifications (e.g. Generic Changes, Parameter Changes, Switch Rehomes) will not occur during the above-mentioned time periods unless agreed to by the interconnecting companies.

Emergency exceptions should be coordinated.

10 Telecommunications Service Priority (TSP) Guidelines

The TSP system provides for the priority treatment of National Security Emergency Preparedness (NS/EP) telecommunication services in order to prioritize their installation and maintenance. For more information, refer to ATIS-0300104, *Next Generation Interconnection Interoperability Forum (NGIIF) NGN Reference Document - NGN Basics, Emergency Services, NGN Testing, and Network Survivability*.

11 Switched Access Service Installation

11.1 SAS Order Activity

SAS Order Activity, or equivalent, is an Access Service Negotiation. The ASC will order the required SAS from each ASP through an ICSC (Interconnection Customer Service Center) or equivalent negotiation. The ICSC work group will handle inquiries and orders. The ICSC work group is to serve as a point of contact for the access service needs of Interexchange Customers. The ASP will negotiate the SAS due date intervals either on a standard or individual case basis. Ordering procedures are described in the Access Services Tariff. During the installation period, all ASC inquiries will be referenced by ASP order number and trunk identification number.

To mitigate inadvertent loopbacks, 64kb data services should be provisioned with loopback recognition timers. Where loopback recognition timers are an ordering option for such services, this option should be selected.

11.2 Establishing an Interface

It is the responsibility of the ASC to designate the POT. It is also the responsibility of the ASC to arrange for suitable equipment space in a safe working area and for suitable electrical power, if required, at the POT. The space furnished shall be accessible to ASP personnel during normal working hours for installation and maintenance purposes. If necessary, ASC personnel will be available to work with ASP personnel.

11.3 Pre-service Testing

Each company is responsible for pre-service testing to ensure that their circuit segments have been installed correctly, prior to cooperative acceptance tests.

11.4 Cooperative Acceptance Testing - Analog

The ASC has the option of accepting the service with or without performing cooperative acceptance testing. Prior to the due date, the ASP will contact the ASC and advise when the SAS will be ready for turn up. If the ASC requests cooperative acceptance tests, the ASP will schedule a mutually agreeable date and time and coordinate all normal and additional acceptance testing (as specified on the order). Test equipment compatibility should be verified at this time. In the event that the ASC does not request cooperative testing, the ASP will perform their own testing and not test directly with the ASC.

Once acceptance testing has been completed, whether or not cooperative acceptance testing was performed, the trunk will be Made-Busy to prevent false seizures from affecting the switching machines. It will be necessary for the ASC to coordinate with the designated ASP (both ends of their overall service) for the removal of the Make Busy.

At the time of acceptance testing, the ASP personnel will not test directly with the ASC unless otherwise directed. Once the acceptance tests have been completed on the SAS, the ASP will "make-busy" the termination to prevent selection and false seizures from affecting the switching machines.

If the ASC is neither available nor ready to perform normal installation acceptance tests at the scheduled time and does not request the ASP personnel to reschedule such tests by the due date, the ASP will consider the order complete on the due date. Unless otherwise specified in local tariffs, normal acceptance tests are:

- 3-Tone Slope
- Loss

- DC Continuity
- Operational Signaling
- Balance (ERL-SRL)
- C-Message Noise
- C-Notched Noise

NOTE: See Figure 21.1 - Acceptance Testing Decision Chart

11.5 Switched Digital Data Access Service (56Kbs, 64KBS, ISDN Primary & Basic Rate)

The following test patterns can be used to perform cooperative testing when access is gained at two (2) points on the circuit. Each test unit transmits a known test pattern toward the other. The data received by each unit is analyzed. It can also be used to do loopback testing if a 108 Type Test Line or other manual DSO loopback functions are provided. The test device will attempt to frame on the received data and count bit and 1-second block error rates. Bit and 1-second block errors will be reported upon termination of the test and must be possible for intermediate results to be reported at specified intervals.

To mitigate inadvertent loopbacks, 64kb data services should be provisioned with loopback recognition timers. Where loopback recognition timers are an ordering option for such services, this option should be selected.

11.5.1 Switched Digital Data Services Stress Test Patterns (56kbs, 64kbs, ISDN Primary & Basic Rates)

Any of four repetitive patterns should be placed in the six-or seven-bit data field of the byte with the eighth bit set to one and may be applied as follows:

Table 11.1 - Pattern Sensitivity Test Criteria for 56/64 kbit/s⁷

Test	Pattern Length Bytes	Binary Representation (see notes 1 & 2)	Test Interval	# of test (see note 3)	ES Test Limit
S1	100 100	1111 1111 0000 0000	(see note 4)	1	0
S2	100 100	0111 1110 0000 0000	(see note 4)	1	0
S3	Continuous	0100 1100	(see note 4)	1	0
S4	Continuous	0000 0010	(see note 4)	1	0
S5 (see note 5)	(see note 5)	(see note 5)	(see note 4)	1	0

⁷ Table A.1 in ATIS-0100510, *Digital Services for Rates Up to and Including DS3-Specifications*

ATIS-0300010

NOTES:

For 56 kbit/s service, these patterns will appear only in the customers' data bits.

All binary presentations are transmitted left to right.

One retest is allowed if the initial test fails.

3-minute intervals are currently used: longer intervals may be recommended by the service provider. If test intervals of 15 minutes or longer are used, the test procedures, intervals and limits given in 8.1.2 and 8.1.3 should be followed.

This test utilizes all the test patterns defined above and, and as an option, may be used in lieu of any or all of the tests S1 through S4 if available. S1 through S4 are run sequentially; a minimum pattern length of 200 bytes for S3 and S4 is suggested.

11.5.2 Switched Digital Data Services Acceptance/ Maintenance Requirements (56kbs, 64kbs, ISDN Primary & Basic Rates)

These test patterns, selected by the OS Application or tester, are transmitted in the test direction. Each byte is repeated according to customer data rate.

Table 11.2 -Test Limits and Objectives for 56/64kbit/s Service⁸

Parameter Limit For:	Short-duration Tests 15-minute stages						Long-duration Test 24 hour	
	ES			SES			ES	SES
	15 min	30 min	45 min	15 min	30 min	45 min	24 hour	24 hour
Access	0	≤ 2	≤ 3	0	0	≤ 2 (see note)	≤ 60	≤ 7
Transit	0	≤ 2	≤ 3	0	0	≤ 2 (see note)	≤ 60	≤ 16
End-to-End	0	≤ 2	≤ 4	0	0	≤ 2 (see note)	≤ 120	≤ 21
NOTE: Accept at 2 only if the cause of the SES is identified as an isolated event.								

11.6 Additional Cooperative Acceptance Testing (ACAT)

Time required to perform ACAT, such as additional installation transmission or signaling tests over and above those specified in normal installation acceptance testing, is considered additional and is billable to the ASC. The ASC should be advised that additional charges would be billed for these tests. Additional acceptance test should be specified on its initial order to the ASP or be mutually agreed upon at time of installation. These additional acceptance tests may include:

- Dial Pulse Percent Break
- Others as specified in the Tariff
- Data Parameters:
 - Envelope Delay Distortion
 - Frequency Shift
 - Impulse Noise
 - Intermodulation Distortion
 - Phase Jitter
 - Signal to C-Notched Noise Ratio.

Completion of the order will not be contingent on these additional tests parameters being met, provided the required design criteria have been satisfied.

⁸ Table 5 in ATIS-0100510, *Digital Services for Rates Up to and Including DS3-Specifications*.

11.7 Traffic Routing & Billing Acceptance Testing

Many different traffic arrangements are available to the ASCs when ordering FG B, C, and D Switched Access Services (e.g. unique CIC Code arrangements; Service Class Screening). Traffic Routing Acceptance testing requirements vary accordingly. If either the ASP or ASC require Traffic Routing acceptance testing for those arrangements not covered by Clause 11.4, terms, conditions and procedures should be negotiated on an individual case basis.

Outlined below are guidelines associated with Call Through Testing to provide assurance for the appropriate routing and generation of billing records.

11.7.1 ASC

When establishing a new trunk group or engaging in a rearrangement of an existing trunk group, the ASC shall perform, at a minimum, a call through test to a number furnished by the ASP. The switch supporting the furnished telephone number shall provide answer supervision.

The ASC shall initiate test call(s) to ensure that correct AMA recording and routing occurs. The scheduling of this call(s) shall be negotiated by the interconnecting companies so that the ASP can validate that the correct AMA recording and routing has taken place for the trunk group under test. The validation results, or the acknowledgment that routing and recording is functioning, shall be provided to the ASP upon request.

11.7.2 ASP

When establishing a new trunk group or engaging in a rearrangement of an existing trunk group, the ASP shall perform a call through test at a minimum. The switch supporting the furnished telephone number used for testing purposes shall provide answer supervision.

The ASP, upon completion of the call through test(s), shall validate that this call(s) was recorded for billing purposes. In addition, the ASP shall ensure that the call is routed over the correct trunk group. The validation results or the acknowledgment that routing and recording is functioning shall be provided to the ASC upon request.

11.8 Completions

Upon acceptance of the SAS order by the ASC, the ASPC should record the name of the ASC representative accepting the order and the basis of the acceptance, for example:

- Cooperative Acceptance Testing criteria being satisfied
- Automatic tests, where available, being completed
- Without acceptance testing.

The ASP should report the order as completed and furnish all the required information to the ICSC or equivalent, including any additional labor charges.

11.9 SAS Disconnects

Prior to performing disconnect activity, the ASC or ASP should be contacted to coordinate disconnect activities. When the trunks are removed from service and translation messages entered, order tracking documents should be updated, and the ASC or ASP notified.

11.10 SAS Rearrangements

SAS rearrangements may include ASC and/or ASP changes in switching and/or facility assignments. When the rearrangement requires physical work by the ASP, the ASP shall contact the ASC to determine the extent of the required coordination. If, however, the rearrangement can be accomplished solely by the ASC, requests for trunk(s)

make-busy will be handled as specified in the Clause titled Trouble Detection Responsibilities. Requests for non-scheduled testing will be handled as specified in the Clause titled Additional Billing.

A sufficient time period should be agreed upon for all entities to complete rearrangement work and appropriate tests. Credit allowance rules will only apply when trunks are out of service for a duration, which exceeds this period due to ASP caused problems.

Upon completion of the rearrangement, the ASP and the ASC may perform cooperative tests to determine that the rearrangement meets service requirements.

11.11 ***Coordinated Conversions***

Coordinated conversions are processes that may be used to facilitate changes requested by the ASC(s) that involves the reuse of a portion of the ASP provided equipment and/or facilities previously assigned. Coordinated conversions require the issuance and processing of related disconnect and connect orders, and coordination of these orders throughout the entire conversion process.

ASC(s) are expected to bear full responsibility for the overall coordination of the various Service Orders associated with the conversion activities involved with its end-to-end service.

Where a coordinated conversion involves a change of service from one ASC to another, the new ASC will establish and coordinate conversion activities with the ASP, former ASC and End User when required. Those activities will include, but are not limited to:

- completion testing and notification
- requests for continuation of service
- conversion timing
- trunk release
- conversion sequence

Every effort must be made jointly by the new ASC and the ASP to successfully complete the conversion. If the new ASC encounters difficulties in activating end-to-end service following acceptance testing on the ASP provided facilities, the new ASC may negotiate and coordinate continuation of the use of the previous arrangement with the ASP and former ASC, and the restoral procedure should commence.

Since continuation of the former ASC service does not automatically defer the due date of the disconnect order, the new ASC must request the former ASC to contact the ASP ICSC, or equivalent, to request a due date change in order to prevent the disconnect of the former ASC service. This must take place prior to the disconnect due date.

It is the responsibility of the ASP to inform the new ASC that all work involved in restoring the former ASC service and subsequent cut-over activities of the new ASC facilities is above and beyond that required for normal coordinated conversion cutovers. This work may result in appropriate additional labor charges.

11.12 ***Glare***

The ASC has the responsibility to determine Glare Master based on the following alternatives:

- ASC as Glare Master (default)
- ASP as Glare Master
- TCIC (Trunk Circuit Identification Code) where interconnecting companies' technology exists:
 - The ASC is Glare Master for odd-numbered circuits (SS7 only)
 - The ASP is Glare Master for the even-numbered circuits (SS7 only)

Implementation of hunting methodology to mitigate the occurrence of Glare should take into account differing options, their compatibility and efficiency and should be based on local negotiations. Where interconnected companies' technology exists, calls encountering subsequent glare should be route advanced.

12 Switched Access Service Maintenance

12.1 *Routine Maintenance*

Routine Maintenance is defined as preventive maintenance or work activities that, under normal circumstances, do not adversely affect interconnected networks. Where possible, routine maintenance should occur during maintenance windows (e.g., off-normal hours, 11:00 PM-5:00 AM).

12.2 *Potential Service Affecting Activities*

Other maintenance and scheduled work activities that can adversely affect interconnected networks should be performed during hours of minimum traffic (e.g., during an 11:00 PM to 5:00 AM "maintenance window") so that any inadvertent failure impacts the least number of customers.

At a minimum, high risk, activities that could potentially affect service, such as growth procedures and generic issue changes, should be scheduled during weekend and off-hours. The overall methods, procedures and scheduling of these work activities should be reviewed by a second-tier maintenance organization.

The activities that may affect other interconnected networks must be coordinated. See ATIS-0300011, *Next Generation Interconnection Interoperability (NGIIF) Reference Document: Part III, Installation and Maintenance Responsibilities for SS7 Links and Trunks*.

12.3 *Deferred Service Restoration*

If customer service is impacted and total restoration would adversely affect the network, efforts will be devoted to re-establishing at least a minimum level of service as soon as possible. Total restoration will be cooperatively scheduled no sooner than the next maintenance window period.

12.4 *Scheduled & Nonscheduled Testing*

Switched access in-service testing is comprised of two categories of tests; scheduled and nonscheduled.

Scheduled tests are those tests performed by the ASP/ASC on a regular basis, e.g., monthly, quarterly. Scheduled tests may be done on an automatic basis [no ASP or ASC technician(s) involved] or on a cooperative basis [ASP technician(s) involved at ASP office(s) and ASC technician(s) involved at the ASC location].

Nonscheduled testing of SAS is when the ASC determines a need to test its services and contacts the ASP to perform (billable) tests in one of the following manners:

- The ASP performs automatic testing using ASC provided remote office test line and associated responder access, or their functional equivalent.
- The ASP performs cooperative testing utilizing a technician at its office(s) and the ASC provides a technician at its location, with suitable test equipment to perform the required tests.

The ASC may specify that testing include loss, noise, slope, envelope delay, etc.

Switch-to-Switch testing of SAS may be necessary to isolate troubles or to verify their clearance. It is expected that the use of test lines will minimize the need for far end support.

When the ASP performs automatic scheduled testing, a monthly test report (at no extra cost) will be provided, indicating the number of trunks tested and the test results. When cooperative scheduled testing is used, the ASP will provide the ASC with a quarterly report (at no extra cost) indicating the number of trunks tested and the test results.

12.5 *Local/Tandem Pad Operation*

When testing trunks that terminate into offices with local/tandem capabilities, the proper switch pad operation must be considered. The ASP should verify proper switch pad operation, or the ASP will provide the ASC with test line numbers for local/tandem operation, allowing the ASC to verify proper switch pad operation.

12.6 **Test Lines**

Test line information is contained in the ATIS-0300024, *Next Generation Interconnection Interoperability (NGIIF) Reference Document: Part V, Test Line Guidelines*.

12.7 **Lineside (Call Through/Routing) Testing**

When it is necessary for an ASP or end user to perform a lineside/call through test, the recommended number to call is 1-700-555-4141 for interLATA pre-subscription validation or (HNPA) 700-4141 for intraLATA toll pre-subscription validation and (101XXXX)-1-700-555-4141 for alternate carrier validation. These calls will not impact end-user billing.

12.8 **Testing through an Access Tandem**

Testing from an End Office through an Access Tandem to an ASC may be impossible due to Access Tandem test line number screening. It is recommended that the ASCs provide access to terminating test lines via the 700 Service Access Code (SAC), where available (e.g. 1-700-958-1102 or 1-700-959-1020).

13 **Trouble Detection Responsibilities**

13.1 **Inoperative & Impaired Circuits**

When ASP or ASC personnel become aware of an inoperative trunk, they will ensure the trunk is removed from service and cannot be accessed. The ASP or ASC detecting the inoperative condition will then sectionalize and repair or refer the trouble.

When ASP or ASC personnel become aware of an impaired trunk, the removal from service is to be determined by the ASC. When detected by the ASP, the ASC will be notified of the condition and will determine action and timing desired. If maintenance is to be delayed, a mutually agreed upon time should be negotiated for removal and sectionalization.

13.2 **Synchronization**

Improper synchronization can result in circuit impairments that should be investigated, and synchronization problems corrected. Problems that cannot be resolved should be referred to the appropriate Synchronization Coordinator.

If the ASC/ASP has its own primary frequency standard that meets the ITU standard for national networks (Recommendation ITU-T G.811, Timing Characteristics of Primary Reference Clocks, and Recommendation ITU-T G.822, Controlled Slip Rate Objectives on an International Digital Connection.), synchronization of the digital SS7 link(s) will be by the plesiochronous method of operation. If either network does not conform to the ITU standard, the non-conforming company will use loop timing to accept SS7 link(s) timing from the conforming company. When the link interface is a DSO-A interface, the interface must be plesiochronous or timed to the same source as the facility.

13.3 **Repair Verification Tests**

Cooperative repair verification tests will be performed when deemed necessary or when requested. The ASP will not normally dispatch an employee to make verification tests when a trouble has been cleared without dispatching; however, there may be cases when dispatch is necessary.

When repair verification tests identify a trouble that was masked by the original trouble, clearance activity will continue until the service is restored.

13.4 **Restoral Prioritization**

Trunk trouble reports will normally be given equal restoration priority by the ASP. When blockage/overflow conditions exist, the ASP will determine restoral priority by analyzing trouble reports and information from both internal and external sources, including overflow/blockage severity statistics (i.e., weighted percentage overflow).

The restoration priority shall be reassessed on a daily basis as needed as well as in emergency situations.

13.5 **Normal Make-Busy Procedure for SAS**

Requests for make-busy may be categorized as follows:

- Single trunk
- Trunk group (facility failure)
- Trunk group (maintenance)

Upon receipt of any request for make-busy, a trouble report will be generated. The trouble report shall be used as an informational report, and a trouble report number will be assigned for tracking purposes.

13.5.1 **Single Trunk Make-Busy**

When a trunk make busy is requested, the following actions are required:

- Contact the responsible interconnected company
- Provide the necessary information
- Indicate the required action(s)
- Determine the status of the trunk (idle or busy)
- Make the trunk busy
- Keep signaling enabled if the trunk was idle
- Disable signaling if the trunk was seized until the trunk becomes idle
- Complete all testing and/or repairs and coordinate release of make busy.

If an incoming trunk problem is encountered, the affected company has the right to demand that the trunk be made busy immediately.

When a trunk has been made-busy, either interconnected company could request a release to perform maintenance testing, at a mutually agreed time.

13.5.2 **Trunk Group Make-Busy (Facility Failure)**

When a facility failure is detected, the following actions are required:

- Contact the responsible interconnected company
- Advise the interconnected company of the detected failure
- Request the interconnected company for a make-busy
- Make trunk group(s) busy
- Correct the problem
- Complete all testing and/or repairs and coordinate release of make busy

13.5.3 Trunk Group Make-Busy (Maintenance)

When a request for a trunk group(s) make-busy is made for maintenance purposes, the following actions are required:

- Contact the interconnected company to schedule the activity
- Make trunk group(s) busy
- Perform maintenance activities
- Complete all testing and/or repairs and coordinate release of make busy

13.6 Expedited Make-Busy Procedure

An ASC or ASP must be able to promptly remove trunks from service. In order to accomplish this, the ASC or ASP may request that the affected trunk(s) be made-busy on an expedited basis to prevent selection by the other switch. The following actions are required:

- Provide trunk identification numbers(s)
- Generate informational report
- State reason for request
- Make the trunk(s) busy immediately
- Perform work operations
- Coordinate testing and the release of trunk(s) for service

NOTE: If an expedited make-busy requires a dispatch, the request will be handled as soon as possible.

If a trouble is identified in the interconnected company's network, a trouble report will be generated referencing the expedited make-busy request report number. The trouble report will be handled in the normal manner.

13.7 Requests for Circuit Trace

It may become necessary to request a hold and trace on a trunk in order to resolve a difficult trouble that cannot be isolated by conventional testing methods. This request should handle on an expedited basis. When an end user is involved, the ASP will hold the trunk and release the end user.

Sectionalization and repair should take place once the trace has been completed.

13.8 Emergency Call Tracing

Emergency Call Tracing is directed toward identifying the source of an in-progress call for urgent physical assistance. These traces may require both ASC and ASP involvement. An ASC and/or ASP receiving such a request will initiate the trace on an expedited basis, recognizing that human life may be at stake. Information relative to these traces will be handled according to local guidelines.

The originator (ASC or ASP) of an emergency call trace assumes responsibility of the validity of a trace request and also is the controlling entity. When an emergency trace is passed from one company to another, the appropriate information (e.g., 41 character Common Language® Circuit Identification (CLCI™) Code or equivalent at the POT) should be exchanged in order to continue the trace. The originator and any interconnected company involved may elect to remain online throughout the trace. After completion of the trace, the trace information will be provided to the appropriate parties. The security of the trace information will be handled according to local guidelines.

Where on-line call traces cannot be completed, trace information may be retrieved from AMA records immediately after the call is disconnected.

13.9 *Killer Trunk Identification*

An Automatic Trunk Test (e.g., Automatic Progression Trunk Testing) should be performed on all trunk groups where switches with test line access have the ability to perform operational tests (i.e., 102 milliwatt or 103 synchronous) on a recurring basis. The trunks that fail should be removed from service and repaired per local procedures.

ASPs and/or ASCs must make compatible test line access available per previous NGIIF agreements and TR-NPL-000258, Compatibility Information for FG D Switched Access Service.

Some ASCs and/or ASPs have the ability to monitor short holding times on a per trunk real time basis. A trunk experiencing consistent short holding times associated with a high attempt rate may indicate a killer trunk condition. Killer trunks may be caused by a number of operational/transmission impairments such as low levels, one-way transmission, noise, echo, no answer supervision, etc. Killer trunks should be investigated to determine the reason for the short holding times. A talk-listen test should always be performed in the investigation/resolution of killer trunks.

14 Trouble Reporting Procedures for FGs B, C, & D

The NGIIF recommends immediate reporting of non-circuit-specific troubles via telephone in order to facilitate the rapid restoral of service.

Trouble reporting procedures can be divided into the following categories:

- Chronic Trunk Failures
- Switched Access Network Trouble
- Call Setup Time Trouble Reporting and Sectionalization

The reporting entity is responsible for performing all necessary tests to determine the nature of the trouble. If the trouble is found to be in the other entity, the ASC and/or ASP will report the trouble to the designated trouble reporting office.

14.1 *Chronic Trunk Failures*

Investigation of chronic trunk failures will involve exchange of information relative to the recurring failures. A detailed investigation should be completed to determine the cause of the trouble condition. This activity may involve cooperative testing and should be handled as an Impaired Trunk trouble report.

14.2 *Switched Access Network Trouble*

The following information should be mutually exchanged between the ASCs and ASPs:

- ASP 41-character Common Language Circuit Identification (CLCI) Code at the POT or equivalent. Where this is not available, local alternatives should be established and used
- Date and time of reported trouble
- Nature of trouble
- Any other information that may be of assistance (e.g., what tests have been made)
- The name or initials of the tester(s) referring and receiving the trouble
- Trouble report number or equivalent

Switched access network trouble reports will include two basic categories for FGs B, C, and D.

- Trunk specific troubles (i.e.: no wink on trunk number 4) will be reported to the designated trouble reporting center.

- The ASCs/ASPs will be provided with specified contact number(s) for the designated trouble reporting center.
- Non-trunk specific troubles (e.g., noisy when calling area code XXX) will be reported to NSC or the designated trouble reporting center.
- The ASCs and/or ASPs will be provided with a contact NSC or the designated trouble reporting center number.

14.3 Call Setup Time Trouble Reporting & Sectionalization

End user reported troubles of excessive call setup time, for interLATA FG-D originating and/or interLATA FG B/D terminating will be analyzed by the ASC. If the ASP receives a call setup time trouble from an end user for an interLATA call(s), the end user will be referred to the ASC.

NOTE: See Figure 21.2- Call Setup Time (CST) Testing Methodology

Upon receiving a call setup time trouble report, the ASC will obtain specific information from the end user to aid in the trouble analysis process. The dialogue should include, but is not limited to, the following questions:

- Type of Customer Premises Equipment (CPE), etc.
- Type of access (e.g., 101XXXX, DDD)
- Directionality of the call(s) on which trouble was reported
- Calling and called telephone number
- Time of day the reported problem is experienced
- End user's estimation of call setup time
- Any other pertinent information which can be supplied by the end user.

Contributing factors to call setup time troubles could include:

- Manual/auto dialing
- Customer call forwarding options
- PBX equipment
- Dial repeating tie lines.

The ASC is responsible for sectionalizing the call setup time trouble to the:

- Terminating CPE
- Terminating ASP
- ASC network
- Originating ASP
- Originating CPE

Should the sectionalization/analysis require that a test call(s) be made, it is recommended that the test call be made to the 102 type test line. Testing to a 105 type test line may distort the intended call setup time results.

Originating ASP and/or ASC test calls to the ASC's first point of switching should be placed to 700-958-1102 or 700-959-1020 as appropriate (See Figure 21.3 or 21.4).

Access performance limits have been established based on the information contained in the Local Switching System Generic Requirements (LSSGR), and other performance criteria, to aid in the isolation of any suspected trouble

associated with call setup time. The ASC should specifically identify any parameters that have been exceeded when referring the trouble.

The ASP will accept a trouble report from the ASC when sectionalized to the ASP's network. The trouble report should include, but is not be limited to, the following information:

- ASC determined ASP call setup time
- Call direction
- FG B-D
- Direct versus tandem routing
- End Office CLLI™ Code
- Test line telephone number used

Upon receipt of the trouble report from the ASC, the ASP will initiate their own analysis and treat the report as an impaired trunk report. This analysis will include the following components as necessary:

- Pattern analysis - process of analyzing known information to determine particular scenarios where certain events are repeated.
- Translations verification, particularly trunk group routing, timing, and overlap outpulsing operation.
- Placing of test calls including those identified in Figures 21.3 and 21.4. A description of those tests follows:
 - The ASP places a call from the line side of the originating end office to a 102 test line in the ASC Switch (first point of switching in the ASC Network). It is recommended that dialing 700-958-1102 or 700-959-1020 as appropriate to access the ASC 102 test line.

NOTE: See Call Setup Time: Figure 21.3 and Clause 21.2.1, Originating Test Procedure.

- The ASC places a call from a test access point in the last point of switching in the ASC network to the 102 test line in the terminating ASP end office. Terminating ASC-ASP test calls should be placed to 7-digit directory number of the end office 102 test line.

NOTE: See Call Setup Time: Figure 21.4 and Clause 21.2.2, Terminating Test Procedures.

If the ASP determines there is a problem in their network, they will exercise diligence in repairing the out-of-limits parameters. If the trouble cannot be found in the ASP's network, this information will be communicated to the ASC. If the ASC and ASP agree there appears to be no call setup time problem, the ASC will discuss this with the end user. If the end user is still encountering a call setup time trouble, further analysis/joint testing may be conducted between the ASC and ASP.

14.4 *Trouble Clearance Reporting*

14.4.1 Access Provider/Access Customer Trouble

When trouble reports are being closed between an ASP/ASC, whether they are using a mechanized system or a verbal notification, the disposition should be furnished by the company clearing the trouble and the following information shall be provided:

- Circuit ID/telephone number
- Trouble report number (ASC/ASP number)
- Name or initials of person closing out trouble
- Nature of the trouble found (e.g., bad cable)
- Resolution details (e.g., cut over to new cable)
- ASC will inform ASP if this trouble is measured

- Date and time trouble cleared
- Date and time trouble referred from the ASC to the ASP
- Date and time trouble report closed
- No access time (the period of time that the service is unavailable for maintenance activities)
- Service charge information, if applicable
- Status of trunk(s) (working or made busy)

When there is a disagreement on the nature of the trouble found, the parties engaged in the dispute shall document their respective positions, the names of the individuals engaged in the dispute for audit purposes and close the trouble report. Escalations shall be in accordance with identified procedures if necessary.

When a trouble report has been cleared and either the ASP or ASC requests to change the nature of the trouble found, such changes should be negotiated.

14.5 *Escalation*

Escalation is a means of bringing problems to the attention of individuals who have responsibility and authority to expedite corrective action.

When either the ASC or the ASP experiences installation or maintenance difficulties, and progress toward resolution is not satisfactory, either company may contact the other company for escalation to a higher level of management.

The rate at which a problem is escalated through successive levels of management should allow each level a reasonable period of time to resolve the problem before it is presented to the next level for action.

Escalation procedures and contacts are based on local negotiations.

14.6 *Trouble Report Status*

The ASC and/or ASP receiving the initial trouble referral shall provide a status on the disposition of that referral based on local agreements negotiated at the time of referral or requested on an individual case basis.

Status reports shall be provided based on the following events:

- When the trouble has been isolated
- When there is a significant change in the status of the trouble
- When the negotiated status interval has expired

When mechanized trouble notification is utilized, the receiving company shall update their system based on paragraphs 1 and 2. In addition, it shall be the responsibility of the company issuing the trouble report to poll the mechanized system for the status of the trouble report.

15 **Additional Billing**

Additional billing may be applied in the following situations:

- Overtime for installation and repair
- Additional Cooperative Acceptance Testing
- Non-scheduled testing
- Maintenance of service charge
- Stand-by time
- Other labor.

Accurate records regarding additional billing must be forwarded to the ICSC or equivalent. A positive means of identifying ASP personnel engaged in these work activities must be established and used. It is the responsibility of the ASP to ascertain when additional billing applies and to ascertain the name of the ASC person who authorizing the additional billing.

Overtime is the time spent by ASP personnel doing the installation and repair functions outside their scheduled working hours.

Overtime installation and repair charges are computed on a fixed rate per half-hour fraction basis, at a rate dependent on when the work was done, as follows:

- Outside scheduled hours but on a scheduled day.
- Outside a scheduled day

15.1 *Billable Overtime Installation & Repair*

Request for billable overtime should be made by the ASC.

When ASP personnel are required to work on a non-scheduled basis, the billable overtime hours begin at the start time requested by the ASC. Billable overtime hours end when the job is completed, or the ASP personnel have been released by the ASC. Only those hours worked outside the normally scheduled hours are billable at the overtime rate. This includes travel time to and from a home or work location.

In the event ASP personnel are called out for ASC installation or repair work, the normal travel time from home, the work time, and the normal travel time back home are billable. A call out of an ASP employee is subject to a minimum charge of 4 hours.

15.2 *Additional Cooperative Acceptance Testing*

Time required to perform ACAT, such as additional installation transmission or signaling tests over and above those specified in normal installation acceptance testing, is considered additional and is billable to the ASC.

15.3 *Non-Scheduled Testing*

Non-scheduled testing occurs when an ASC determines a need to test its services and contacts the ASP to perform (billable) tests (e.g. loss, noise, envelope delay).

15.4 *Maintenance of Service Charge*

When an ASC reports a trouble to the ASP and requests that the ASP clear the trouble, the ASC shall be responsible for payment of a Maintenance Service Charge if dispatch to the POT is required and the trouble is determined not to be in the ASP equipment.

When a trouble is subsequently found in the ASP equipment or facilities, where a Maintenance Service Charge has been applied, the charge will be canceled or adjusted.

15.5 *Stand-By Time*

Stand-By Time authorized by the ASC may be billable and is predicated on local negotiated agreements and shall be documented by both the ASP and the ASC.

15.6 *Other Labor*

As agreed to by the ASP and the ASC, other labor is anything not identified above.

16 5XX/8YY/9YY NXX Services

This Clause describes the general responsibilities for ASCs, Transport Providers (TPs), and Designated Agents (DAs). It also provides guidelines for installation, and trouble/referral for 5XX/8YY/9YY NXX access services. For trouble reporting contacts, reference the ATIS Service Provider Contact Directory (SPCD).⁹

16.1 Responsibilities

The ASC, Transport Provider (TP), or Designated Agent (DA) has the overall coordination, installation and maintenance responsibilities for its 5XX/8YY/ NXX Subscriber's end-to-end service. The ASC, TP, or DA will provide to the ASP:

- A test number for each new NXX code when placing the order for service. It is recommended that the test number will be 5XX/8YY-NXX-4141
- Identification of an announcement response on the terminating test number
- Personnel to work with the ASP technicians on cases of trouble during service turn-up
- Notification of any changes affecting the service requested, including the due date
- Authorization to bill Additional labor for any additional testing or expedite requests

The ASC, TP, or DA is responsible for providing a trouble reporting number to its 5XX/8YY/9YY NXX Subscriber.

8YY-NXX Service Providers will transport disconnect referral messages across the Network, as appropriate for the disconnect service request.

The ASP is responsible for the installation, testing and maintenance of the 5XX/8YY/9YY NXX service within its operating area, in accordance with local tariffs. In addition, the ASP will work cooperatively with the 5XX/8YY/9YY NXX ASC, TP, or DA during the acceptance and maintenance of the access services.

16.2 Installation

When 5XX/8YY/9YY NXXs are opened (new translations installed) by ASPs, call through testing should be performed. It is recommended that the implementation of Test Line(s), as described in ATIS-0300206.2001(S2016), *Digital Exchanges and PBXs - Digital Circuit Loopback Test Line with N [infinity] DS0 Capability*, be instituted at offices equipped for Switched Digital Services. The plant test date (PTD) is the date by which the ASP, ASC, TP, or DA will complete all work necessary to perform the required tests. The intent of these tests is to ensure that the code being tested is routed to the correct ASC, TP, or DA on the correct Trunk Group and that appropriate billing takes place:

- From an Equal Access End Office - for each new NXX installed the ASP shall place a minimum of one test call to the new ASC 5XX/8YY/9YY NXX-XXXX test number. This number should provide an announcement identifying the ASC, TP, or DA.
- From a Non-Conforming End Office - for offices subtending an Access Tandem that performs 5XX, 8YY or 9YY NXX 6 digit translations, one Non-Conforming End Office will have a call through test performed to the new ASC 5XX, 8YY, or 9YY-NXX test number by the ASP.
- If either the ASC, TP or DA requires 5XX/8YY/9YY NXX acceptance testing other than described above, terms conditions and procedures should be negotiated on an individual case basis. The ASP will notify the ASC, TP or DA of overall work completion by the due date. In non-subscribed areas, the ASP will route 5XX/8YY/9YY NXX calls to a vacant code announcement.

⁹ The SPCD and instructions for gaining access to the Directory can be accessed on ATIS's website: http://www.atis.org/01_committ_forums/ngiif/contact-directories/.

In the case of non-conforming office(s) utilizing the 00Y codes, the access tandem should pass on the dialed digits to the interconnected carriers.

16.3 *Trouble Reporting/Referral*

For trouble reporting contacts, reference the ATIS SPCD. The ASC, TP, or DA is responsible for providing a trouble reporting number to its 5XX/8YY/9YY NXX Subscriber.

It is expected that the 5XX/8YY/9YY NXX Subscriber will report troubles to the ASC, TP, or DA.

The entity receiving the original trouble report from the subscriber is responsible for performing all necessary tests to determine the nature of the trouble. If the trouble is found not to be in the receiving entities network, the trouble will be referred to the appropriate designated trouble reporting center.

When a report is received by the ASP from the End User and dialog or testing determines that there may be a trouble external to the ASP's network, the ASP should refer the End User to the trouble reporting number listed in the 5XX/8YY/9YY NXX lookup table.

If the End User experiences difficulty in reaching the appropriate ASC, TP, or DA trouble reporting number, the ASP will accept the report and refer it to the ASC, TP or DA per local agreements.

If the ASP operator receives a call from the End User experiencing difficulty in reaching a 5XX/8YY/9YY NXX number, assistance may be offered. This may include the operator attempting to complete the call for the End User, suggesting the End User contact 800 Directory Assistance by calling 800-555-1212 (only 8YY troubles) or transferring the call to the ASP's Repair Service Center to report a case of trouble.

The ASC, TP, or DA will sectionalize the trouble. If the trouble is sectionalized to the ASP's network, the ASC, TP, or DA will refer the trouble to the appropriate ASP entity.

17 Toll-Free Database Services

This Clause provides guidance for RESP ORGs and ASCs/ASPs regarding Toll-Free Database Services trouble reporting, referrals, and closure. In addition, this Clause addresses Disaster Recovery Plans for SMS/800, SCPs/NCPs, and routine maintenance for SEP power sources.

17.1 *Responsible Organization (Resp Org)*

The Resp Org is the entity identified by the Toll-Free subscriber, or the subscribers' agent, that assumes the duty of managing the appropriate records in 800 Database Service Management Systems (SMS/800). Resp Org management and administration shall include data entry, record change, trouble acceptance, referral, and/or clearance of Toll-Free services. It is recommended that any entity performing the above function comply with this and other Toll-Free database services associated documents.

The Resp Org is responsible for:

- Providing a contact number that is readily accessible 24 hours a day, 7 days a week
- Providing trained personnel
- Overall coordination of testing of its Toll-Free database services
- Acting as the Toll-Free Subscriber's contact in all matters involving provisioning and maintenance of Toll-Free database services
- Accepting all trouble reports pertaining to their Toll-Free services
- Sectionalizing trouble to determine if the reported trouble is in its translations or facilities, or in another provider's network
- Testing cooperatively, if necessary, with other providers to further identify and clear a trouble when the trouble has been sectionalized to another provider's network

- Keeping the Toll-Free Subscriber advised of the status of trouble clearance
- Maintaining accurate repair records

Each Toll-Free Service Provider should provide Toll-Free database test numbers within the reserved range (Toll-Free NPA-250-0001/250-1499). These test numbers shall be obtained through the SMS/800 Help Desk at 888-SMS-3300.

17.2 *Treatment*

If a service provider has not provided trunking from a particular switch, the call shall be routed to a vacant code announcement.

17.3 *Trouble Reporting*

These are the recommended procedures for ASPs and ASCs to follow for trouble reporting:

- It has been recognized that the existing trouble handling procedure for Toll-Free database services failures between companies is satisfactory. However, the current procedures for referral of trouble among ASPs and/or ASCs need to be modified to ensure the appropriate information is exchanged for resolution of troubles in a timely manner. It is recommended that the following guidelines be used when referring or reporting Toll-Free database trouble between ASPs and ASCs.
- RESP ORG contact information for trouble reporting handling is obtainable through the SMS/800 Database System.

17.4 *Disaster Recovery Plans*

All SCP Owner/Operators should have Disaster Recovery Plans in place within their respective companies. The administrative organization for the SMS/800 system has a Disaster Recovery Plan in place. However, it has been determined that these plans are proprietary and will not be made available in public forums.

17.5 *Routine Maintenance for Service End Point (SEP) Power Sources*

Service Control Point (SCP)/Network Control Point (NCP) Owner/Operators should have SCP/NCP power source maintenance routines (e.g., uninterruptable power supplies, batteries, emergency generators, and loss of commercial power) in place and should perform based on their respective requirements.

18 Toll-Free Database Services-Trouble Handling Procedures

End users who experience trouble completing Toll-Free calls will most likely report the trouble to the following:

- Local repair bureau (ASP)
- Interexchange carrier (ASC)
- An operator
- The Resp Org- Entity identified by the Toll-Free Subscriber's agent who assumes the duty of managing the appropriate records in 800 Database Service Management Systems (SMS/800)

Written procedures using these guidelines should take into account the following requirements:

- The ability to identify a Toll-Free originating call as an IntraLATA/InterLATA call
- The ability to identify the Resp Org
- Information and methods to pass information to/from the ASP/ASC/Resp Org

- The ability to receive the trouble report on a 24 hour per day, 7 days a week basis
- Tracking and reporting of the trouble report and notifying the end user as to the disposition of their report

18.1 ***Trouble Report***

18.1.1 **Trouble Report - NON-SMS Access (e.g., Resellers)**

- Entities receiving trouble reports for Toll-Free calls need to establish agreements to acquire information from the SMS/800 Database
- Entities receiving trouble reports should contact their SMS agent

18.1.2 **Trouble Report - SMS Access**

The entity receiving the trouble report should proceed as follows:

- Acquire the Toll-Free number dialed
- If not the appropriate Resp Org, identify the appropriate Resp Org or its trouble agent and refer/hand-off the reporting customer to the appropriate Resp Org
- If the Resp Org, or trouble reporting agent obtain all trouble reporting information, including the originating NPA-NXX-XXXX of the Toll-Free database call, and date and time of the failure

18.2 ***Trouble Referral***

18.2.1 **Resp Org Responsibilities**

When referring troubles, the following information will be passed to the receiving entity:

- Trouble report number
- Originating telephone number
- Dialed number
- Time and date call was made
- Resp Org ID, contact name and telephone number

If required, the following carrier specific information should be passed to the receiving entity:

- Area of service
- CIC(s)/LATA routing at date/time of call
- Vertical features enabled
- POTS termination number

The Resp Org is responsible for the following activities:

- Coordinate repair activities
 - Parallel trouble referral to the ASP and/or ASC will only occur when Percent Allocation is used
- Status shall be provided based on locally negotiated agreements
- Final clearance and closure of customer troubles
- Escalations when necessary

Escalations of customer troubles will be based on locally negotiated agreements. The Resp Org making the escalation should specify to the level of severity to the receiving company. The following matrix is provided to determine the severity of the situation/trouble condition.

18.2.2 Severity Level Matrix

Severity	Description
S1-M1	Total out-of-service condition on all carriers.
M2	Total out-of-service condition on one carrier.
M3	Partial out-of-service. Possible problem with multi-carrier distribution.

LEGEND: M = Multiple Carrier
S = Single Carrier

Trouble Report handling should be prioritized according to severity level matrix.

18.3 Trouble Closure

The following information should be provided when closing out a trouble report:

- Circuit ID/telephone number
- Trouble ticket number (ASC and/or ASP number)
- The nature of the trouble (e.g., bad cable)
- Resolution details (e.g., cut over to new cable)
- ASC will inform ASP if this trouble is measured
- Date and time trouble cleared
- Date and time trouble referral from the ASC to the ASP
- Date and time trouble report closed
- No access time (the period of time that the service is unavailable for maintenance activities)
- If trouble report results in a service charge, the ASP will provide this information to the ASC

When there is a disagreement on the disposition, the parties engaged in the dispute shall document their respective positions and the names of the individuals engaged in the dispute for audit purposes. Escalations, if necessary, shall be based on locally negotiated agreements.

If after a trouble has been cleared and either the ASP or ASC wishes to change the disposition, such changes shall be negotiated.

19 Industry Inter-Company ABS/LIDB Trouble Reporting

19.1 Scope

Recognizing that ABS (Alternate Billing Service) and ABS validation have been a part of the telecommunications industry for many years, this process describes trouble reporting procedures needed specifically for ABS/LIDB (Line Information Database) service in an interconnected SS7 (Signaling System Seven)/LIDB network environment. This document does not cover trouble processes already defined for link and trunk problems. This document specifically covers routing/data problems pertaining to ABS/LIDB service.

LIDB database related problems, and customer perceived problems with billing restrictions are described in this procedure, but the primary purpose is in identifying, reporting, and resolving network routing errors, node

translations, and outages. The process of ABS/LIDB network trouble identification requires an understanding of customer perceived problems, whether they are network-related or database-related.

Some problems encountered by customers stem from options made by a specific company in their OSSs (Operator Service Systems); while these problems are neither database nor network related, there may be difficulties identifying the exact trouble, and the customer still perceives a problem.

An industry ABS/LIDB trouble reporting process can be broken down into the following major categories:

- Trouble Identification
- Trouble Reporting
- Trouble Resolution

19.2 *Background*

Alternate Billing Service is the name given to a group of billing options that describes how a customer can choose to bill a call to other than the originating number (this does not include "Toll-Free" service). These billing options include Calling Card, Collect, and Bill to Third. Collect and Bill to Third are also collectively called Billed Number Screening (BNS). The telecommunication networks are designed to validate the billing number each time a call is attempted to check the validity of the billing number and to keep track of queries to monitor for potential fraud.

LIDBs are the databases that contain all the working line numbers for a company and specific information regarding line numbers including Calling Card PINs (Personal Identification Numbers). Most LECs that provide dial tone and allow Collect and Bill to Third to those line numbers have made arrangements for those line numbers to be housed in a LIDB. The LIDB may be owned and maintained by the LEC, or the LEC may contract with a LIDB owner for LIDB service. Line number based Calling Cards, and Special Billing Number Calling Cards issued by the LEC are also maintained in a LIDB.

In order for a transporting carrier, either an exchange carrier or an interexchange carrier, to validate an end user's (customer) billing number, the transporting carrier has to determine the appropriate LIDB to send the validation query. iconectiv administers the LIDB Access Support System (LASS, formerly named RDBS/ABS), that has all Billing Number Groups (BNG, NPA-NXX & RAO-0/1XX format) identified and the corresponding LIDB identifier. The output report of the LASS is the LIDB Access Routing Guide (LARG) to which carriers can subscribe. This monthly report provides the transporting carrier with basic BNG information needed to direct an ABS query to the correct LIDB for validation. Other information for ABS validation is required to access the LIDBs. This data (e.g., originating Point Codes) is normally provided with interconnection questionnaires or sales ordering documents.

The LARG report also provides contact information for each LIDB's BNG coordinator, and SNCC (Signaling Network Control Center), or equivalent, for information and trouble resolution.

19.3 *Trouble Identification*

ABS validation problems will appear in several ways. End users (customers) will report trouble to the operator serving the phone from which they are initiating an ABS call. In addition, they may also report trouble to their billing service provider (usually their business office) or to a number printed on the back of their Calling Card. The customer may call the local Repair Service serving the phone from which they are initiating an ABS call. Companies should use local practices to refer these customer-reported troubles. This may result in the customer's billing number service provider initiating a trouble report back to the company attempting to validate the billing number.

Other indicators of trouble may be network generated. For example, STPs (Signaling Transfer Points) may generate GTT (Global Title Translation) failure reports when an accessing network incorrectly routes ABS queries. The STP owner/operator experiencing the GTT failure may need to research the failing BNG to ensure correct translations. Depending on the volume of GTT failures, the STP owner/operator may want to inform the accessing company of the incorrectly routed query. STPs or SCPs (Service Control Points) may not recognize Originating Point Code (OPC) or Calling Party Address information in the query.

OSSs may generate reports regarding ABS validation queries and query responses. For example, excessive amounts of time-outs (ABS queries with no response or late response to the OSS) may indicate GTT problems in the home or distant STP. Time-outs may also indicate other network problems (e.g., links, nodes, and major outages).

ABS validation problems can be identified by the following reporting mechanisms:

- LIDB
- OSS reports
- SS7 network - STP/SCP/Internet Transport Provider (Hub) reports
- LASS/LARG data error reports

19.3.1 LIDB Problems

LIDB problems are normally errors in the database, or customer related problems regarding billing number functionality. Examples of database errors include:

- Working line number missing (missing customer record)
- Incorrect Toll Billing Exception (TBE) against line number
- Incorrect/missing PIN
- PIN/service denied in error

Examples of customer related errors include:

- Customer doesn't remember PIN
- Customer has incorrect PIN
- Customer doesn't know about TBE (e.g., customer calling collect when not authorized)
- PIN/service denied without customer's knowledge - problems with account, suspected fraud, etc.

19.3.2 LIDB Trouble Referrals

In the event of suspected database errors, or customer related problems, customers should be referred to either (1) the card issuing service provider, or (2) the billing number service provider (Collect, Bill to Third type calls), or companies may use local practices to handle these customer-reported troubles. However, it is recommended that customers experiencing validation problems should be able to report troubles on a 24-hour a day, 7-day a week basis.

In the event the customer will not receipt for contacting their service provider, or fraud is suspected on a specific billing number, then the appropriate LIDB owner/operator should be contacted by the company identifying the situation.

19.3.3 OSS Detected Problems

Examples of OSS detected problems include:

- Block calls based on time-outs - billing denied on time-out condition (no query response received)
- Block calls based on "missing customer record" (no record found in LIDB)
- Incorrect entry in a translation table - either BNG blocked in error (denies billing) or allows in error (potential fraud - sometimes detected by high number of time-outs).

While companies may choose to block or not block calls on time-outs or missing customer record, it is helpful to understand what the conditions are when identifying troubles. Some OSSs do not differentiate between an operator or customer call queries. In addition, some OSSs do not differentiate between LIDB denial or an option denial.

19.3.4 SS7 Network Problems

Examples of network problems include:

- STP Global Title Translation (GTT) failures
- OSS time-outs - needs correction whether or not the OSS blocks or allows on time-outs (both conditions cause problems, either in customer service or potential fraud) - OSS time-outs can be indications of GTT failures, or "circular" routing problems
- OSS "Return on error" - needs research to determine if GTT problem exists at local or distant STP
- Misc. failures - appear as SS7 error messages that are not identifiable to the originating OSS sometimes in the form of protocol errors (OSS cannot interpret error code)
- Network node failures - SS7 networks need to notify entities that access the node within specified time period (this may be a contractual issue) of expected/planned outages, more importantly, notification of emergency outages lasting more than "X" amount of time is recommended (this is a contractual issue). This is especially necessary for ASCs and ASPs that are major users of the node
- STP/SCP Originating Point Code (OPC) data missing or incorrect
- STP Gateway Screening translations incorrect
- STP Point Code to link set translations incorrect
- Internetwork Transport Provider (Hub) - incorrect Point Code/linkset translations
- SCP congestion – overload

19.3.5 LASS/LARG Data Problems

iconectiv administers the LIDB Access Support System (LASS). Each LIDB owner maintains the LASS BNG information for data residing in its respective LIDB. The LIDB Access Routing Guide (LARG) is the monthly output report from LASS.

Examples of LASS/LARG data problems that could result in misrouted queries:

- BNG with LIDB ID of "blank" - this may mean that the LEC has not chosen a LIDB, however the BNG may belong to a participating LEC and the BNG has no LIDB ID in error. This may mean that the BNG is due to change ownership and the receiving company has not yet "claimed" the BNG
- BNG completely missing - this is an error, as all BNGs are to be identified
- BNG with incorrect LIDB ID

19.4 *Trouble Reporting*

Prior to referring problems, the referring company needs to perform the appropriate investigation. Once the trouble has been identified, the trouble needs to be reported to the destination or terminating network. The focus of this process is network troubles, but it is sometimes difficult to determine the difference between LIDB problems, customer related troubles, and network troubles.

19.4.1 Reporting Network Routing Troubles

Once a validation problem is identified, a process of communication takes place. For this procedure, it is assumed that all the appropriate investigative work has taken place in the company originating the trouble report.

The LARG report contains a list of contact numbers (phone and facsimile) for SNCC (Signaling Network Control Center), or equivalent, for the LIDB networks. These contacts should be the point of contact for ABS/LIDB network routing trouble reporting. For ASP that do not have LIDB (i.e., no LIDB in their own network), the accessing company should exchange trouble contact numbers with the LIDB owner company under the LIDB contract or interconnection questionnaire. Companies utilizing an Internetwork Transport Provider as their agent should specify trouble contact numbers and referral processes in their LIDB contracts.

The following information should be provided when reporting network routing troubles:

- Name and phone number of contact originating trouble report
- Company name of contact originating trouble report
- Originating company's trouble report number
- Date and time problem encountered
- Billing number (10-digit billing number - if Calling Card, the PIN is not required to check routing)
- Billing Number Group (BNG) if 10-digit billing number not available
- Type of call - billing attempted (Calling Card, Collect, Bill to Third)
- Calling number; or at least, location of call origination
- Called number; or at least, location of attempted call termination
- Brief description of perceived trouble
- Brief description of investigative work already done

The reporting company should expect confirmation of the trouble report from the receiving company with some identification of the report, (e.g., the receiving company's trouble report number, name and number of the contact taking the report).

19.5 *Trouble Closure*

If the receiving company determines that the problem is not in its network, the receiving company will contact the reporting company and close out the report. Once the receiving company has reconciled the problem, the appropriate information should be provided to the reporting company to close out the report. Companies should use negotiated time frames for resolution reports and/or status reports. A flow chart (See Figure 21.5 – Industry Inter-company ABS/LIDB Trouble Reporting) is provided as a job aid for trouble reporting and closure.

20 Access Services Provided by Multiple Exchange Carriers

These procedures apply when Access Service is requested by an ASC and is provided by two or more ASPs. The ASC will order the access services required to provide its overall service from the ASPs.

It is recommended that a single ASPC point, specific to the function being performed, be identified for multi-ASP access service.

Before an ASR is issued by the ASC for an access service involving multiple ASPs, the ASPs involved should have a mutually agreeable working arrangement in place to allow one of the ASPs to be the ASPC for the installation of access service.

Each ASP is responsible for working cooperatively with ASCs and other ASPs to ensure that access services are installed, tested, and turned up in a timely manner. Each ASP should also work cooperatively with ASCs and other ASPs to ensure that trouble conditions are resolved without undue delay and to participate in repair verification as required.

20.1 *Installation*

Installation as used in this document pertains to that portion of the total provisioning process that starts when the order, e.g., "Work Order Record and Detail" (WORD) or equivalent, is received by the ASPs. The order includes installations, changes and disconnects.

The ASPC will:

- Ensure that their company's equipment and facilities pertaining to the ASC are installed and tested by the Plant Test Date (PTD)

ATIS-0300010

- Receive and log status on the Designed Verified and Assigned Date (DVA) or equivalent. If the Other Access Service Provider (OASP) has not provided status within 24 hours after DVA or equivalent, the ASPC will contact the OASP and request status
- Schedule and coordinate pre-service tests prior to cooperative acceptance tests to ensure that the overall access service is installed correctly and meets design parameters
- Contact the ASC upon completion of the pre-service test and advise that the access service is ready to be turned up. The ASC has the option of acceptance with or without cooperative acceptance testing. The ASC is not obligated to accept the service prior to the due date

The OASP will:

- Ensure that their company's equipment and facilities pertaining to the specific ASR are installed and tested by PTD
- Contact the ASPC and provide circuit status
- Cooperate with the ASPC to perform the pre-service tests and acceptance tests as required

The first point of switching ASP will arrange for field forces to be dispatched when required and participate in the acceptance testing with the ASC.

20.2 Common Completion

All involved ASPs will utilize a common completion date. Therefore, no ASP may complete its order until the entire Access Service is completed and accepted by the ASC.

20.3 Jeopardy

If one or more ASPs cannot complete its portion of the overall Access Service on the due date, this should be considered a jeopardy situation by all ASPs involved. If, after a specified period of time (to be determined locally) past the due date, the overall Access Service remains incomplete due to ASP problems, those ASPs who completed their portion of the access service will review the status of the incomplete portions via the ASPC to determine the actual or approximate duration of the existing jeopardy condition and notify the ICSC or equivalent.

20.4 Maintenance

The ASC will be responsible for acceptance of trouble reports from their end user(s). The ASC should test its facilities first to determine if the trouble is located in its own network. If a trouble is found, the ASC will clear the trouble and no referral to an ASP is necessary. If the trouble is sectionalized by the ASC towards a connecting ASP, the trouble report will be referred to the ASP. The ASP(s) will work cooperatively with the ASC to sectionalize the trouble.

The following information should be exchanged when handing off or referring the trouble:

- Trouble report number or equivalent
- Contact telephone number
- Contact ID (i.e., name or initials)
- Time and date report was received from ASC
- ASC testing information (if requested by ASP)
- Circuit ID (41 Character CLCI Code)
- Non-circuit specific (Circuit ID may not be appropriate)

ATIS-0300010

- Trouble reported
- Other information that may be of assistance (e.g., history, subsequent reports)

Upon receipt of a trouble report from the ASC, the ASP will conduct tests required to determine if the trouble is in its own equipment and facilities or to the point of interface of an adjacent OASP(s). These tests will be conducted independently or cooperatively with the ASC.

If the trouble is found to be in the ASP's equipment or facilities, the trouble report will be closed out with the ASC and the following information will be provided:

- Trouble report number or equivalent
- Date & time cleared
- Status of circuits(s) [temporary or permanent repair]
 - If temporary, estimated time of restoral
- Contact name or initials and telephone number of the person closing out the report
- Type & nature of trouble found and action taken
- ASP testing information (if requested by ASC)
- Circuit ID (if applicable)

If there is no trouble found in the ASP's own network, the ASP shall refer/hand-off the trouble to the OASP and provide the following information:

- Trouble report number or equivalent (ASC)
- Contact telephone number (ASC)
- Contact ID (ASC) (i.e., name or initials)
- Time and date report was received from ASC
- ASP testing information (if requested by OASP)
- 41-character CLCI Code for circuit specific problems
- Non-circuit specific (Circuit ID may not be appropriate)
- Trouble reported
- Other information that may be of assistance (e.g., history, subsequent reports, ASC testing information, if available)

In the event a premature or improper hand-off has occurred, the ASP will resume cooperative testing with the OASP in order to sectionalize the trouble.

When the ASP has referred/handed off the trouble report to an OASP, the ASP will close out the trouble report with the ASC and provide the following information:

- Trouble report number or equivalent (ASC)
- Trouble report number of OASP
- Time and date report was referred/handed off to the OASP
- Contact telephone number (OASP)
- Contact ID (OASP) (i.e., name or initials)
- ASP testing information (if requested by ASC)
- Trouble disposition (Test OK, NTF, Found OK)

- Circuit identification (if applicable)
- Contact name or initials of person closing the report

If the trouble report requires further hand-off/referral by the OASP to succeeding ASPs, the identity of the OASP switches to ASP when the referral is made.

The OASP will:

- Cooperatively test with the ASP to determine trouble location
- Accept the trouble report when sectionalized into its equipment or facilities
- Provide status to the ASC upon request
- Contact the ASC upon clearing trouble to close out the trouble report

20.5 *Trouble Report Exceptions*

The following information is provided in an effort to assist service providers and service customers in the resolution of troubles that fall outside of the normal ticket resolution flow once the original report has been closed out with the ASC.

20.5.1 Request for Test Assistance

- When a request for test assistance is made to an ASP, the ASP shall provide the necessary assistance to facilitate the request.
- A report (non-measured) shall be created for administration of test assist referrals. Subsequent request for a test assist may result in additional reports being created. In the event that additional reports are created, all relevant information from the prior trouble report/test assist reports should be cross-referenced.

20.5.2 Request for Escalation Assistance from ASC

- It is the responsibility of all service providers and service customers to work cooperatively to resolve all trouble reports as expeditiously as possible.
- The ASC is responsible for escalations to an OASP associated with trouble reports when the trouble has been isolated/referred by an ASP to an OASP. When a request for escalation assistance is made by the ASC to an ASP, the ASP will provide any information concerning escalation numbers or names that they may have to the requesting ASC. At the ASC managers' request, the ASP manager may participate on a phone call in an attempt to assist the ASC in escalating to the OASP.

20.5.3 Additional Escalation Information

- If the ASC refers the problem back to the ASP, it should be understood that the escalation process would reinitiate at the level when the problem was initially referred into the OASP.
- In the event the trouble cannot be sectionalized by a single company, the ASC and all ASPs/OASPs will cooperatively work together to locate and/or isolate the problem. Once the problem has been sectionalized, previously developed process for ASP/OASPs shall be followed.

21 Local Number Portability

21.1 *Default Routing Translations*

All interconnecting parties, for LNP purposes, should agree on having "Default Routing Translation" in place prior to implementation of LNP. Acceptance of inter-network LNP queries should be locally negotiated.

Carriers may block default routed calls in specific circumstances when failure to do so is likely to impair network reliability.

If the N-1 carrier experiences LNP database congestion and receives a 10-digit Automatic Code Gap (ACG) from its database, it should gap the queries to its LNP database for that 10-digit DN and abort the call. If the N-1 switch receives a 3 or 6-digit ACG from its database, it should gap such queries to its LNP database and default route the call. If the database fails to respond to a query from the N-1 switch, the call is default routed.

If the default carrier experiences LNP database congestion (e.g., the default switch receives an ACG from its database), it should gap the queries to its LNP database and abort the call.

21.2 *Background on Default Routing Translations:*

If a carrier cannot successfully query an LNP database, it should default route the call based on the dialed digits to the default carrier.

A “default routed call” situation may occur in a LNP environment when a call is made to a telephone number in an exchange with any ported numbers and the N-1 carrier (or its contracted entity) queries a number portability database to determine if the called number has been ported. If the N-1 carrier fails to perform the query, the call is routed by default to the service provider that originally serviced the telephone number. The original service provider, who may or may not still be serving the called number, should try to complete the call which may include an LNP database query.

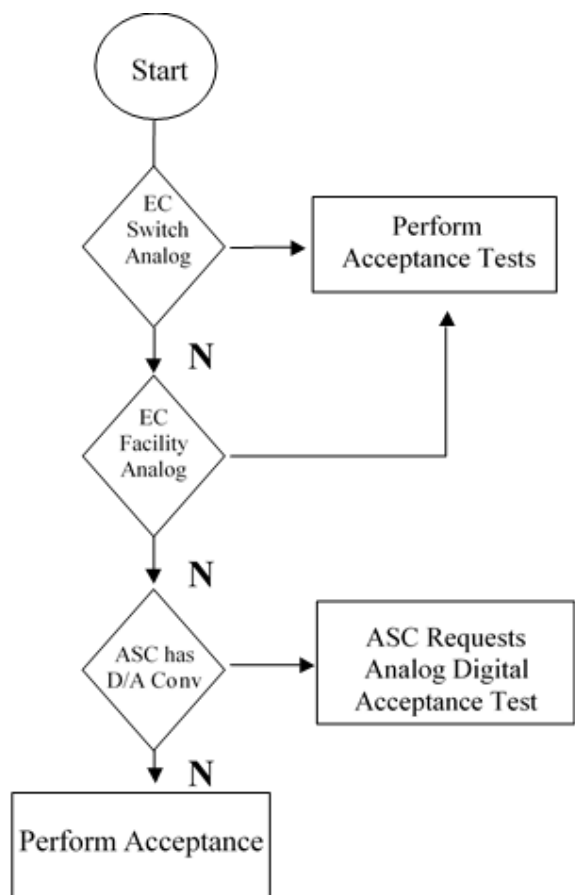


Figure 21.1 - Acceptance Testing Decision Chart

**CST Testing Methodology for
1+ FG D origination and
FG B/D terminating**

**Stored Program Control
Equal Access End Offices Only**

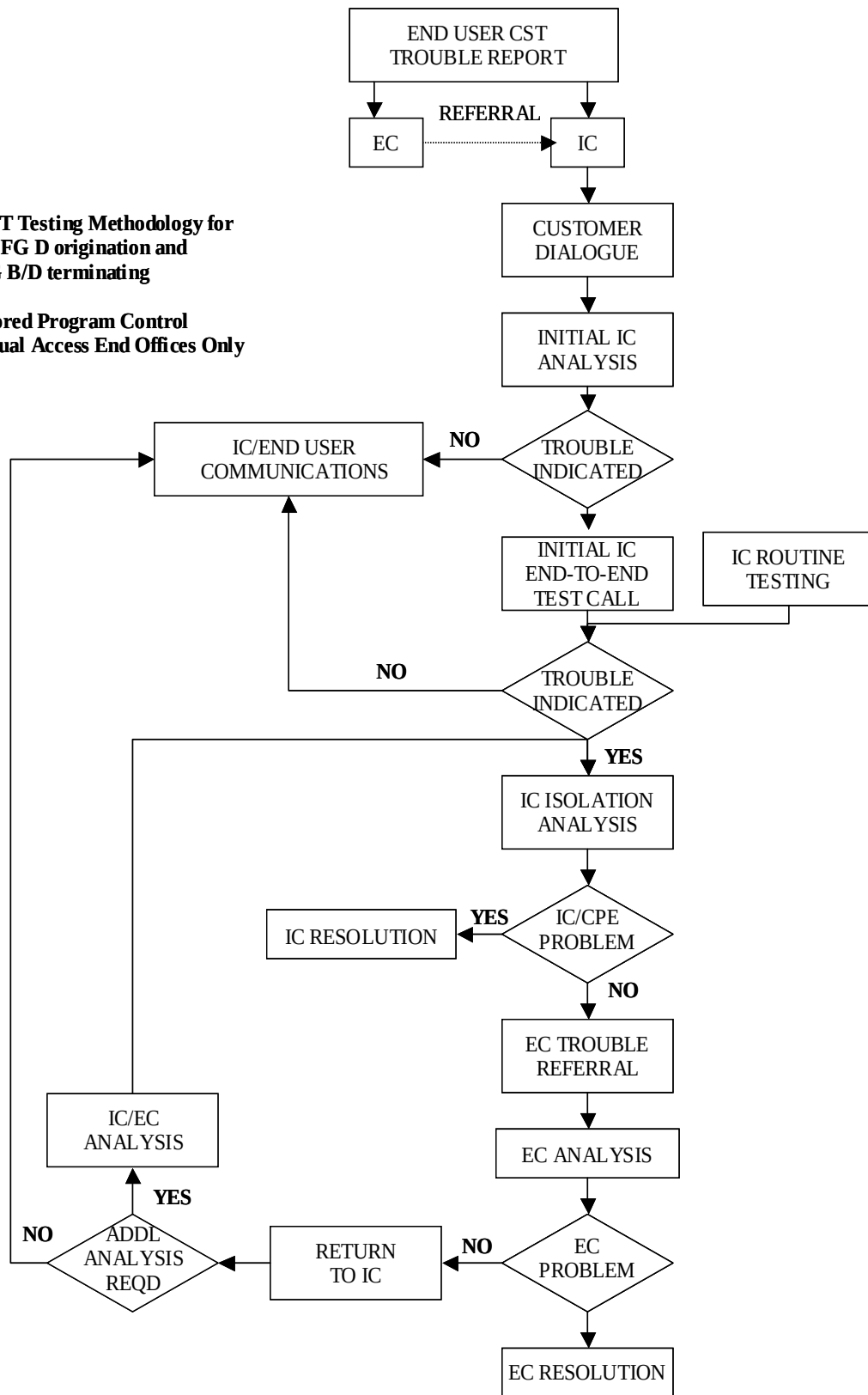


Figure 21.2 - Call Setup Time (CST) Testing Methodology

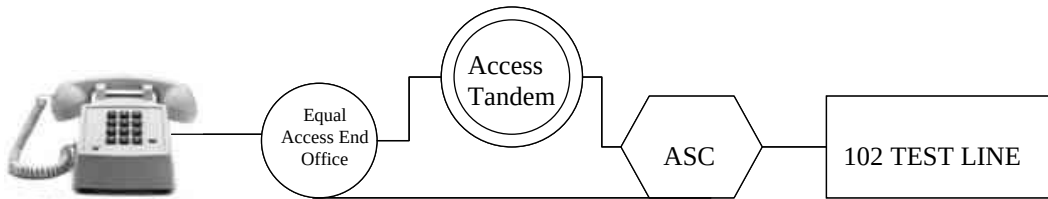


Figure 21.3 - Call Setup Time

21.2.1 Originating Test Procedure

1. Place call from line side of originating EO to 102 test line in ASC switch. It is recommended that the ASC 102 test line be accessed by dialing 700 958-1102 or 700 959-1020, as appropriate.
2. Time stamp:
 - a. Start at end of last digit dialed
 - b. Stop at Network response

May be accomplished with Personal Computer, stopwatch, or other test equipment, as available.

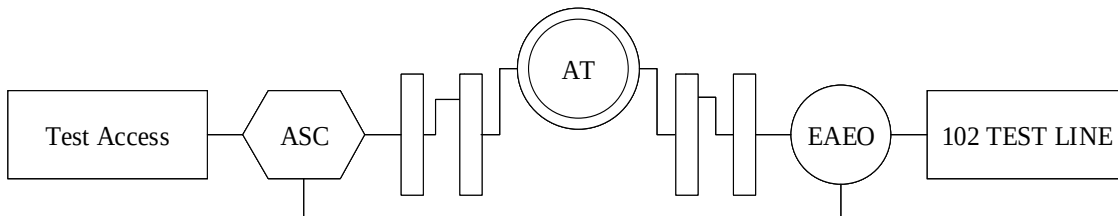


Figure 21.4 - Call Setup Time

21.2.2 Terminating Test Procedures

1. Place call from Test Access in the ASC switch to 102 test line in End Office (EO)
2. Time stamp:
 - a. Start at ASP trunk seizure
 - b. Stop at network response

May be accomplished with personal computer, stopwatch, or other test equipment, as available.

3. ASC switch time not included

ATIS-0300010

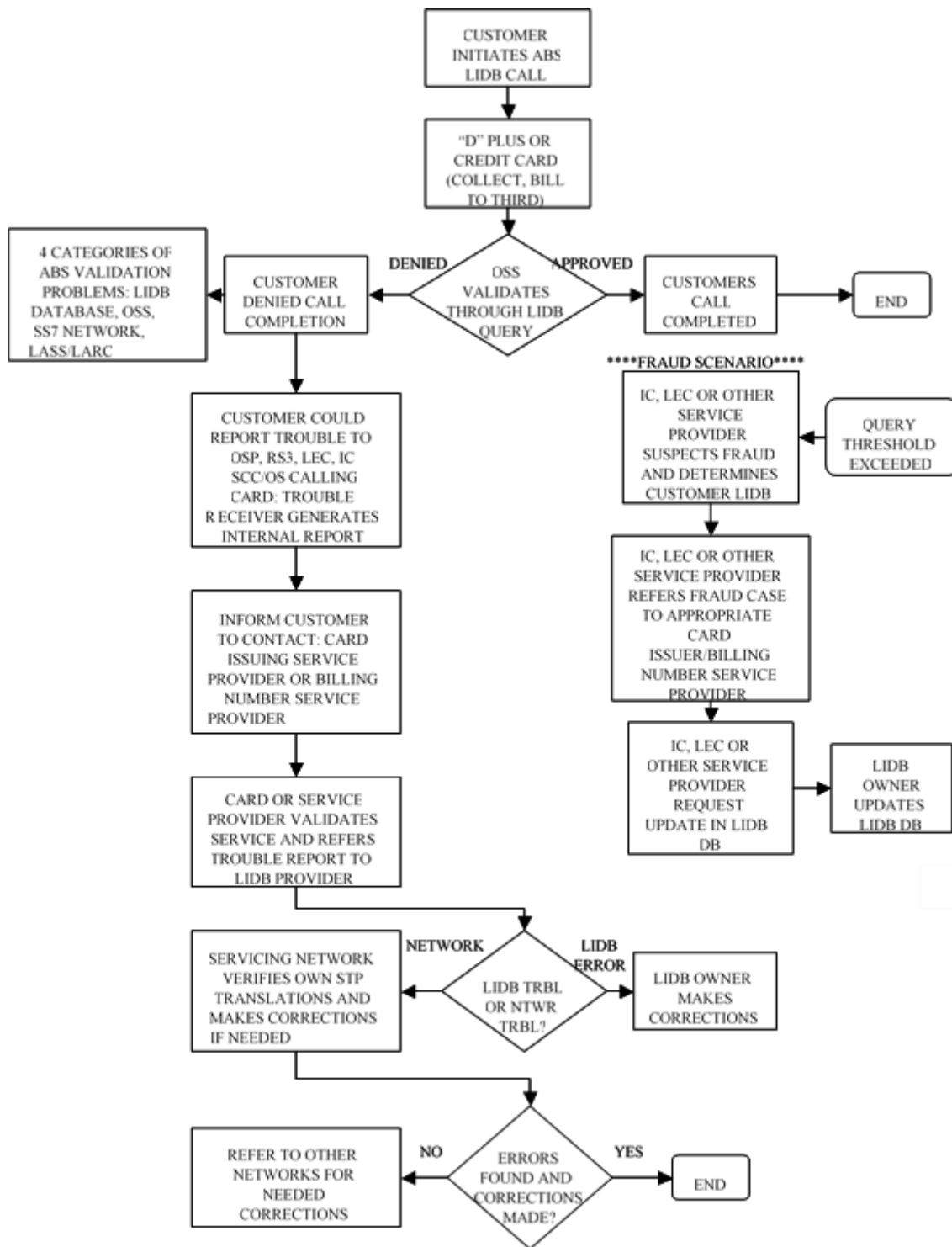


Figure 21.5 - Industry Inter-Company ABS/LIDB Trouble Reporting



ATIS-0300011

**Next Generation Interconnection Interoperability (NGIIF)
Reference Document**

**Part III, Installation and Maintenance Responsibilities for
SS7 Links and Trunks**

Version 12.0



ATIS is the leading technical planning and standards development organization committed to the rapid development of global, market-driven standards for the information, entertainment and communications industry. More than 200 companies actively formulate standards in ATIS' Committees, covering issues including: IPTV, Cloud Services, Energy Efficiency, IP-Based and Wireless Technologies, Quality of Service, Billing and Operational Support, Emergency Services, Architectural Platforms and Emerging Networks. In addition, numerous Incubators, Focus and Exploratory Groups address evolving industry priorities including Smart Grid, Machine-to-Machine, Connected Vehicle, IP Downloadable Security, Policy Management and Network Optimization.

ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications' Sectors, and a member of the Inter-American Telecommunication Commission (CITEL). ATIS is accredited by the American National Standards Institute (ANSI). For more information, please visit www.atis.org.

Notice

This document was developed by the Alliance for Telecommunications Industry Solutions' (ATIS) sponsored Next Generation Interconnection Interoperability Forum (NGIIF). The NGIIF addresses next-generation network interconnection and interoperability issues associated with emerging technologies. Specifically, it develops operational procedures which involve the network aspects of architecture, disaster preparedness, installation, maintenance, management, reliability, routing, security, and testing between network operators. In addition, the NGIIF addresses issues which impact the interconnection of existing and next generation networks and facilitate the transition to emerging technologies. All changes to this document shall be made through the NGIIF issue resolution process

Note Regarding Previous Versions

The NIIF Reference Document was formerly known as the Network Operations Forum (NOF) Reference Document. The NOF Reference Document was published and maintained by Bellcore. The last version of the NOF Reference Document is Issue 13.

Disclaimer and Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

ATIS-0300011, NGIIF Reference Document, Part III, Installation and Maintenance Responsibilities for SS7 Links and Trunks, Formerly NIIF 5018

The NGIIF Reference Document, Part III, Installation and Maintenance Responsibilities for SS7 Links and Trunks is an ATIS standard developed by the NGIIF..

Published by

Alliance for Telecommunications Industry Solutions

1200 G Street, NW, Suite 500

Washington, DC 20005

Copyright © 2011 by Alliance for Telecommunications Industry Solutions

All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < <http://www.atis.org> >.

Printed in the United States of America.

INSTALLATION, TESTING & MAINTENANCE RESPONSIBILITIES FOR SS7 LINKS AND TRUNKS

Table of Contents

1	GENERAL.....	5
2	LINK RESPONSIBILITIES.....	6
2.1	SS7 LINK CONTROL.....	6
2.2	ACCESS SERVICE CUSTOMER (ASC)	6
2.3	ACCESS SERVICE PROVIDER (ASP)	7
2.4	LINK DEFINITIONS	8
2.5	LINK AUGMENTATION	8
2.6	DIVERSITY	8
2.7	CATASTROPHIC SS7 NETWORK FAILURES	11
3	LINK INSTALLATION.....	11
3.1	SIGNALING POINT OF INTERCONNECTION (SPOI)	11
3.2	PRE-SERVICE TESTING	11
3.3	ACCEPTANCE TESTS FOR SS7 LINK CIRCUITS	11
3.4	ASP PROVE IN PERIOD	11
3.5	SYNCHRONIZATION	11
3.6	COMPATIBILITY TESTING	12
3.7	TEST SEVERITY ANALYSIS CRITERIA - PART III (ATTACHMENT D).....	13
3.8	COMPLETIONS	13
3.9	REARRANGEMENTS.....	13
3.10	TIMER VALUES	13
4	LINK MAINTENANCE.....	13
4.2	TROUBLE REPORTING	14
4.3	SECTIONALIZATION AND REPAIR	14
4.4	MAINTENANCE OF SS7 LINKS WITHIN A HIGHER RATE FACILITY	14
4.5	TROUBLE CLEARANCE.....	14
4.6	ASP NODE TO ASC NODE INTERCONNECT TESTING AND ANALYSIS	15
5	TRUNK RESPONSIBILITIES.....	15
5.1	ACCESS SERVICE CUSTOMER ASC/ASP.....	15
5.2	CONVERSION OF MULTI-FREQUENCY TRUNKS TO SS7	15
5.3	TRUNK CIRCUIT IDENTIFICATION CODE (TCIC)	20
5.4	TRUNK CIRCUIT IDENTIFICATION CODE (TCIC) NUMBERING PLAN.....	20
5.5	TONES AND ANNOUNCEMENTS	20
5.6	TROUBLE REPORT DISPOSITION.....	21
6	TRUNK INSTALLATION	21
6.1	POINT OF PRESENCE (POP) SERVING MULTIPLE SWITCHES	21
7	TRUNK TROUBLE DETECTION RESPONSIBILITIES	21
8	SCREENING AND TRANSLATIONS.....	22
8.1	FINAL GLOBAL TITLE TRANSLATIONS (FGTT)	22
8.2	TRANSLATION TYPES.....	22
8.3	TCAP TRANSACTION LOOPING	23
9	RULES FOR POPULATING JIP	23
10	SS7 NETWORK SECURITY BASE GUIDELINES.....	24

11	SS7 SOFTWARE VALIDATION	24
12	DUAL STP FAILURE PREVENTION PROCEDURES	24
13	COMBINED NODE - MINIMUM SET OF GUIDELINES	25
13.1	ARCHITECTURE	25
13.2	ROUTING AND CONFIGURATION.....	26
13.3	NETWORK MANAGEMENT	26
13.4	DIVERSITY	26
13.5	TESTING	27

1 GENERAL

This document outlines Access Service Customer (ASC) and Access Service Provider (ASP) responsibilities for the Signaling System 7 (SS7) interface between carriers. It deals with the physical interconnecting trunks and link(s) as well as the software necessary to support the use of the link(s) to transport SS7 messages between carriers. It is intended to be a living document to aid operations work forces. It does not replace or supersede Tariffs, Contracts or any other legally binding documents. It is limited to procedures relating to the installation and maintenance of the SS7 trunks and link(s) and associated software used to interconnect and provide services between Interexchange and Access Service Providers. All networks which connect to ASCs and ASPs via SS7, should be expected to recognize these operational guidelines, as providers of public switched services regardless of whether or not they provide Public Switched Telephone Network services. For the purpose of this document, the terms, SS7 and CCS are interchangeable.

The ASC, for the purposes of this document, is defined as the Interexchange Customer engaged for hire between two or more exchanges, including interstate or foreign communication by wire or radio.

The ASP, for purposes of this document, denotes a company engaged in the business of furnishing access service in a franchised territory.

The Wireless Service Provider (WSP), for the purposes of this document, is defined as those carriers engaged in Intra/Interstate communication via radio frequency.

Local Service Provider (LSP) is defined as the Local Exchange Carrier (LEC) selling local interconnection service arrangement trunk(s) to another LEC.

Local Service Customer (LSC) is defined as the LEC purchasing local interconnection service arrangement trunk(s) from another LEC.

Where ASP/ASC interconnection statements are made or identified, specific to their purpose, WSP/LSP/LSC may be substituted as appropriate.

In addition to other operational and technical agreements made at the Next Generation Interconnection Interoperability Forum, this document is being reissued to incorporate the following changes:

- Standardization of the Issue Number and publication date to agree with other sections of the NGIIF Reference Document.
- Addition of a new Part III Attachment G - titled SS7 Diversity Validation Guidelines
- Addition of new document Part III Attachment H - titled "SS7 Cause Codes & Tones and Announcements."

The SS7 link(s) may be considered as a network enhancement for certain existing services between Interexchange and Access Service Providers as well as providing a transport to new services.

The term node is used in this document to mean any SS7 capable network element without regard to its specific function i.e. Signal Transfer Point (STP), Signal Point (SP), Service Switching Point (SSP), Service Control Point (SCP).

The software resident programs, in both ASP and ASC interconnecting nodes for the purpose of providing services transported on SS7 link(s), will be referred to as applications.

The NGIIF has developed the following guidelines outlining the medium by which internetwork affecting maintenance activity notification will be provided to the interconnected company and the time frame prior to the planned activity:

- Notification when possible should be made at least 5 working days prior to the planned change activity.
- Notification should be made in the form of:
 - E-Mail (recommended where available),
 - FAX or,

- Telephone call.
- Notification should be provided to the affected company's appropriate notification center. Contact information is included in the NGIIF Service Provider Contact Directory. An example of a notification form is located in the NM Section, Part VI, of the NGIIF Reference Document.

When network modifications are planned to any SS7 network element that has the potential of affecting traffic, the ASP/ASC must notify the interconnecting carrier(s) of the planned change. Sufficient information should be exchanged to ensure that all parties understand:

Affected Network Element

- Date and time of change
- Expected duration
- Traffic effect during change
- Potential hazards

Compatibility test requirements and procedures should be considered.

The need exists to install and maintain time of day clock settings to coordinated universal time standards for SS7 network elements. In the absence of automated clock update standards and systems, it will be necessary to manually install and maintain time of day clock settings, as follows:

- Internal Network Element (NE) clocks set to + or - 15 seconds from the Coordinated Universal Time (UTC) minute register would degrade service.
- Daily routine to check NE clock (e.g., 8 am) to UTC.
- Weekly routine to check clock source to National Institute of Science and Technology (NIST), e.g., WWV, Naval Observatory. etc., to nearest second + or - 1 seconds.
- Upon initialization of NE (boot) there is a need to load time of day, otherwise NE sets to 0000 hours 1/1/00 - (operationally sensitive.)

2 LINK RESPONSIBILITIES

2.1 SS7 Link Control

The ASC will have overall responsibility for the installation and maintenance of the SS7 link(s). The designation of an ASC as having overall responsibility does not relieve the ASP of the responsibility for taking prompt appropriate actions needed to correct an identified failure condition. The ASPs and ASCs are responsible for the portion of an SS7 link, which they maintain.

The ASP is responsible for ensuring that its portion of the SS7 link(s) provided to the ASC are installed and functioning properly. In addition, the ASP should work cooperatively with the ASC to perform SS7 protocol tests to ensure the ability of the interfaces to correctly transmit and respond to SS7 messages being passed between carriers.

2.2 Access Service Customer (ASC)

The following are the responsibilities of the ASC:

Provides trained personnel

- Designates a Control office(s) for the overall responsibility for SS7 link(s).
- Cooperates with the ASP to ensure that the SS7 link(s) are installed in accordance with the ASCs service request.
- Notifies the appropriate ASP Interexchange Customer Service Center (ICSC or equivalent) when the service due date is to be changed.
- Sectionalizes troubles to determine if the trouble is located in its facility, interface, or application or if the trouble is in the ASP facility, interface, or application.
- Ensures that any manually initiated tests performed on the SS7 link(s) or applications will not negatively affect the ASPs SS7 network.
- Coordinates any changes to its translations which may require changes to the ASPs translations.
- Cooperatively participate with the ASP to further identify, isolate and clear troubles which cannot be sectionalized into the ASP or ASC portion of the link or application software.
- Provides a trouble reporting number(s) that is readily accessible 24 hours, 7 days a week.
- Accepts and refer trouble reports from the ASP relating to SS7 and the services being provided over the link(s).
- Provides the ASP Notification of Maintenance Releases
- Overall coordination of control responsibilities
 - Tracking of orders
 - Coordination of testing
 - Coordination of link specific maintenance releases
 - Referral to appropriate groups for repair
 - Establishing of interface agreements
 - Responsibility for trouble agreements
 - Link(s) surveillance

Maintains complete and accurate installation and repair records

2.3 Access Service Provider (ASP)

The following are the responsibilities of the ASP:

- Provides trained personnel
- Designates Control Office for the ASP portion of the SS7 link(s) provided for the ASC interconnection.
- Cooperates with the ASC to ensure that the SS7 interconnection is installed and functioning properly.
- Notifies the ASC of due date jeopardy in a timely manner.
- Sectionalizes troubles to determine if the trouble is located in its facility, interface, or application or if the trouble is in the ASC facility, interface, or application.
- Ensures that any manually initiated tests performed on the SS7 link(s) or applications will not negatively affect the ASC's SS7 network.
- Coordinates any changes to its translations which may require changes to the ASC's translations.
- Cooperatively participates with the ASC to further identify, isolate and clear troubles which cannot be sectionalized into the ASP or ASC portion of the link or application software.
- Provides a trouble reporting number that is readily accessible 24 hours, 7 days a week.

- Accepts and refers trouble reports from the ASC relating to SS7 and the services being provided over the link(s).
- Provides the ASC with notification of maintenance releases.
- Maintains complete and accurate installation and repair records.

2.4 LINK DEFINITIONS

A-Link - Access Links connecting a switching point or a database to its home Signal Transfer Point (STP).

B-Link - Bridge Links interconnecting STP pairs of the same hierarchical level within the same network.

C-Links - Cross Links connecting mates of an STP pair in the same network

D-Links - Diagonal Links 1) connecting STP pairs between different networks or

2) connecting STP pairs of different hierarchical levels within the same network.

E-Links - Extension Links connecting a Signaling Point (SP) to an STP pair other than its home STP pair.

F-Links - Fully associated Links directly connecting two switching points to one another or a switching point to a database node.

2.5 Link Augmentation

The following thresholds are recommended for augmentation of existing SS7 linksets between interconnected companies:

2.5.1 Warning Threshold

Linkset augmentation investigation/initiation should take place no later than when the linkset utilization reaches 25%.

2.5.2 Critical Threshold

Linkset augmentation of the linkset should be completed before the linkset utilization reaches 32%.

2.6 Diversity

Documentation pertaining to the Link Diversity Validation guidelines is covered in Part III Attachment G.

The following describes recommended criteria for Interconnecting Link diversity;

- The architecture with ASP STPs connected to ASC STPs (Figure 1) requires three-way physical diversity of CCS link facilities.
- The architecture with ASP STPs connected to ASC SPs (Figure 2) requires two-way physical diversity of CCS link facilities.
- Three-way physical diversity between ASP STPs and ASC STPs means that no two failures should simultaneously disable all three physical diverse link sets¹ between ASP STPs and ASC STPs (see Ex. Figure 1).

¹ A (signaling) link set is a set of signaling links directly connecting two signaling nodes.

- Two-way physical diversity between ASP STPs and ASC SPs means that no single failure should simultaneously disable both two physically diverse link sets between ASP STPs and ASC SPs (see Ex. Figure 2).

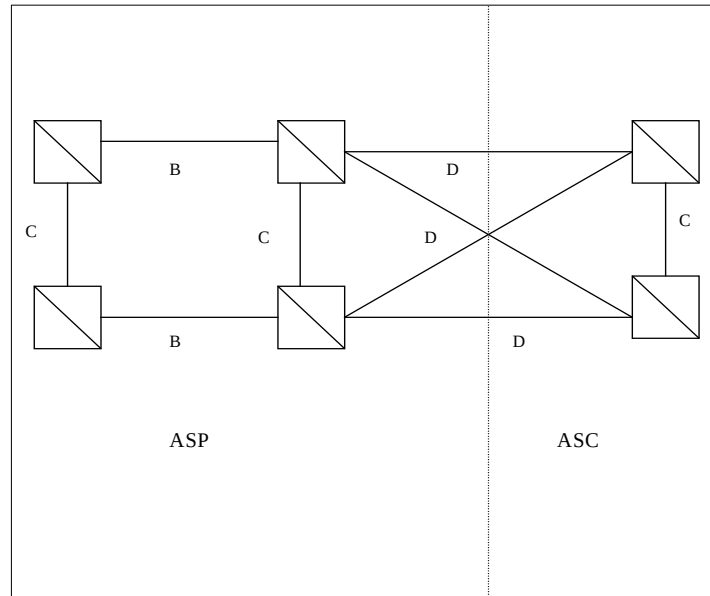


Figure 1 - STP to STP Interface (Example)

STP LINK CONFIGURATION

B LINKS

C LINKS

D LINKS

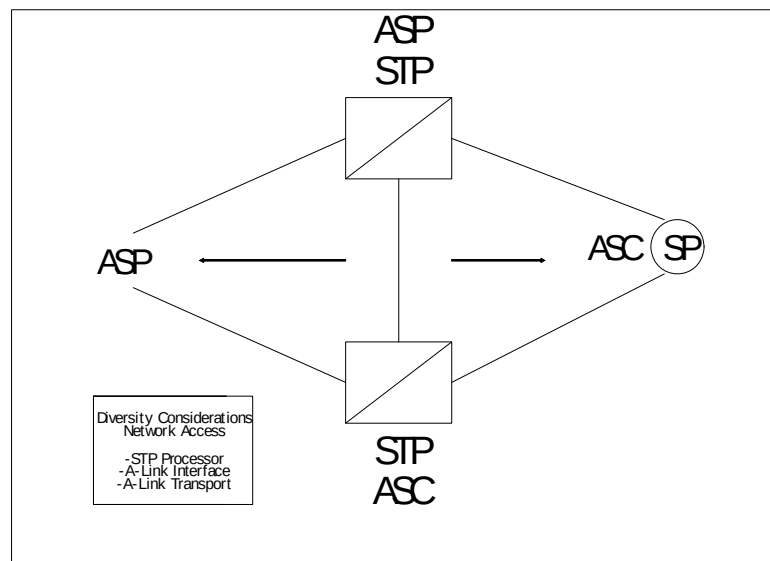


Figure 2 - STP to SP Interface (Example)

In general, n-way diversity between two portions of a network connected by multiple link sets means that no instance of (n-1) or less simultaneous failures will cause there to be no available link set between the two portions.

To avoid common cause failures (i.e., single failures that disable more than one link set), ideally link sets should not share common resources (e.g., electronic equipment), and wherever possible, should be physically separated.

2.6.1 Other Considerations

CCS/SS7 route diversity, which assumes a network architecture that encompasses interconnecting mated STPs, is defined as signaling link sets that are on physically and electrically separate routes; exceptions to this guideline may apply to building entrances, circuit distribution frames, power plants and some remote signaling points.

2.6.2 A-Link Concentrators for Local Service Providers (LSPs)

LSCs/LSPs using A-Link Concentrators (ALCs) in their network are strongly encouraged to employ the mated pair architecture. If the LSCs/LSPs elect to use other architectures (Stand-Alone or Dual Access) and full point code routing (non-cluster routing) is utilized, the maximum number of subtending SPs should be negotiated between the operator of the ALC and the operator of the STP to minimize network management messages.

2.6.3 CCS Link Interconnectivity

Physical Link diversity is achieved first in the provisioning process and then maintained by operational procedures. When SS7 link facilities are leased it is the responsibility of both the user and the provider(s) to validate diversity. For example, if hypothetical company X leases SS7 link facilities from separate companies Y and Z, company X may assume the facilities, for the SS7 links, to be diverse per NGIIF recommendations. However, company Z may also lease facilities from company Y, possibly resulting in company X's SS7 link facilities not meeting NGIIF diversity validation recommendations.

2.6.4 Provisioning

The provisioning process should take into account facility routing and equipment assignments such as:

- Cable routing
- Separate Equipment
- Powering and Fusing
- Building Entrance locations
- Distribution Frames
- Equipment Cable Racks
- Nailed Up Connections, e.g. Digital Cross Connect Equipment

2.6.5 Maintenance

In order to maintain link diversity, operational procedures should address the following link set maintenance considerations;

- Notification of ASC and ASP Centers.
- Determination of the status of all links in the combined link set.
- Expedient return of the repaired/operational link to service.

Once diversity is designed into a combined link set, the ASC/ASP should ensure that the diversity is maintained:

- Diversity on all link sets should be routinely confirmed following the procedures described in the Link Diversity Validation Guidelines document, Part III (Attachment G).
- Whenever maintenance or circuit order activity occurs on a link, or a failed link is restored, diversity on the combined link set should be confirmed following the procedures described in the Link Diversity Validation Guidelines document, Part III (Attachment G).
- At a minimum, validation of diversity on all interconnected links in all link sets should be performed at least once every six (6) months following the procedures described in the Link Diversity Validation

2.7 Catastrophic SS7 Network Failures

Each ASP/ASC is responsible for providing a point of contact. Contact numbers should be non toll free numbers and associated with the organization responsible for handling SS7 Catastrophic Network Failure reports. A contact list for SS7 Catastrophic failures is available in the NGIIF Service Provider Contact Directory.

3 LINK INSTALLATION

During the installation period, all inquiries will be referenced by the ASP Service Order number and circuit identification.

3.1 Signaling Point of Interconnection (SPOI)

Signaling Point of Interconnection is a physical location on SS7 links, where the ASP and ASC exchange SS7 messages. The SPOI location may be provisioned at the POT for testing of links with a theoretical point of physical demarcation, be co-located with a POT, or remotely located from present POT locations. Diversity requirements for Signaling Links should be considered in developing SPOI locations.

3.2 Pre-service Testing

Each company is responsible for that portion of the overall SS7 link(s) circuit they are providing.

Each company must ensure that their link segments have been installed correctly, prior to cooperative acceptance testing.

3.3 Acceptance Tests For SS7 Link Circuits

Link circuits that are being installed, as a facility should first be tested at Level 1.

The recommended tests for DS-1 acceptance testing is documented in, PART IX, Section 5F; Acceptance of DS-1.

When such testing meets the parameters for acceptance of the DS-1 facility, the recommended tests to ensure compatibility of the DS-1 to pass MTP Levels 2 & 3, is documented in, PART III, Attachment A; MTP Compatibility Tests, (Levels 2 & 3)

3.4 ASP Prove In Period

A prove in period, not to exceed seven (7) days is recommended, subject to the bilateral agreement of the Service Providers. The 24 hour SP to SP Acceptance limits should not be exceeded in any 24 hour interval during the prove in period.

3.5 Synchronization

Improper synchronization can result in circuit impairments which should be investigated and synchronization problems corrected. Problems that cannot be resolved, should be referred to your Synchronization Coordinator.

Companies' Synchronization Coordinators are listed in the NGIIF Service Provider Contact Directory, which is available from the NGIIF.

If the ASC/ASP has its own primary frequency standard that meets the CCITT standard for national networks (G.811, G.822), synchronization of the digital SS7 link(s) will be by the plesiochronous method of operation. If either network does not conform to the CCITT standard, the non-conforming company will use loop timing to accept SS7 link(s) timing from the conforming company. When the link interface is a DSOA interface, the interface must be plesiochronous or timed to the same source as the facility.

3.6 Compatibility Testing

3.6.1 SS7 Inter-Network Testing

SS7 Inter-Network trunk signalling testing is a pre-cutover requirement.

The following tests, MTP, ISUP and SCCP compatibility tests, are recommended to verify the compatibility of networks during interconnection. These tests are intended to be used as a recommended set of minimum tests of the SS7 protocol.

It is assumed that the two (2) interconnecting networks may have some additional tests they may wish to perform during interconnection. In this case, these tests should be part of the bilateral agreements developed for SS7 network interconnections.

Network compatibility testing verifies the correct interworking of two SS7 implementations. The tests are written for the interconnection of two given implementations.

The full test suite of all recommended tests should be run between the two interconnecting companies for any interconnection configuration that was not previously tested. Both the manufacturer model and software load of the interconnecting signaling network elements defines the interconnection configuration. Subsequent interconnections, using configurations previously tested by the two interconnecting companies, may be tested at their discretion.

The tests in this document have been divided into Intrusive Tests and Non-Intrusive Tests and defined as follows:

- Intrusive Tests - The interconnecting circuit shall be interrupted, with the testing unit inserted into the circuit and acting as an emulator to the signaling point under test.
- Non-Intrusive Tests - The test shall be able to observe traffic traversing the link(s) between the two (2) signaling points, in a monitor mode.

3.6.2 Message Transfer Part (MTP) Compatibility Tests - Part III (Attachment A)

The minimum set of MTP level 1,2, and 3, protocol compatibility tests are required for switches between interconnecting (ASP/ASC) networks in support of SS7 link interconnection.

3.6.3 ISDN User Part (ISUP) Compatibility Tests – Part III (Attachment B)

The minimum set of ISUP protocol compatibility tests are required for switches between interconnecting (ASP/ASC) networks implementing ISUP trunk interconnection.

Signaling Connection Control Part (SCCP) Compatibility Tests-Part III (Attachment C)

The minimum set of SCCP tests are required for switches between interconnecting (ASP/ASC) networks implementing Toll Free Database and LIDB interconnecting services. Prior to the initiation of any testing, bilateral agreements will need to be reached defining entries to the Gateway screening, routing and global title tables required to support the testing.

3.7 Test Severity Analysis Criteria - Part III (Attachment D)

The Test Severity Analysis Criteria describes the potential impact of performing these compatibility tests on the network.

3.8 Completions

After performance of the link(s) circuit acceptance tests and alignment of the link(s) by the SS7 protocol, the control office should report the order as completed. The acceptance of Level 1, 2, 3 tests would constitute a link in service.

3.9 Rearrangements

The ASP or ASC will coordinate rearrangements not resulting in a change of operation or design. Removal from service, rearrangement timing and completion testing will be negotiated on an individual basis. Upon completion of the rearrangement, sufficient cooperative testing should be performed to ensure the proper operation of the service.

3.10 Timer Values

ASC and ASPs need to exchange T2 timer settings prior to interconnection.

4 LINK MAINTENANCE

The ASC is responsible for performing the necessary tests and performance monitoring to determine the nature of the SS7 link (s) trouble. Cooperative testing and Performance Monitoring may be required to identify troubles that are not associated with the physical circuit transport. If the trouble is found to be in the ASP/ASC provided portion of the link (s), the ASP/ASC will report the trouble to the appropriate ASP/ASC control office or the designated trouble reporting office. These links are to be treated as Order Wires for restoration priority purposes. Restoration of these links is to be pre-planned, through bilateral agreements.

4.1.1 Routine Maintenance Activities

- It is the recommendation of the NGIIF that all routine maintenance and scheduled work activities be performed during hours of minimum traffic (e.g., during an 11:00 pm to 5:00 am "maintenance window") so that any inadvertent failure impacts the least number of customers.
- At a minimum, high risk, potentially service affecting maintenance and growth procedures should be scheduled during weekend and off-hours. The overall methods, procedures and scheduling of these work activities should be reviewed by a second tier maintenance organization.
- The activities that may affect other network service providers must be coordinated, which includes both intra- and inter-carrier networks.

4.1.2 Non Scheduled Work Activity

- If customer service is being impacted, the minimum work activity will occur to restore the system to a stable performance state. Complete system recovery activity will be scheduled for the next maintenance window period.

4.2 Trouble Reporting

The following types of information should be exchanged at the time of the trouble referral.

- Circuit identification number [ASP circuit identification 41 Character Common Language (CLCI)] for circuit specific troubles.
- Date and Time of referral
- Nature of the trouble and any other information that may be of assistance in resolving the trouble.
- The name or initials and telephone number of the person referring the trouble.
- Trouble ticket number(s) or equivalent and the name or initials of the person accepting the trouble. Identify trouble report as a link. SS7 Link "Circuit Specific" troubles will be reported to the control office.
- The ASCs/ASPs will provide specific contact numbers for the control offices or other designated report centers. This information is conveyed through the Ordering process.
- SS7 Link "Non Circuit Specific" troubles (e.g. Data Base, Point Code) will be reported to the appropriate Network Service Center (NSC) or equivalent center.
- The ASCs/ASPs will provide a contact NSC or equivalent center number.

4.3 Sectionalization and Repair

While link facility sectionalization is the responsibility of the ASC, it could involve cooperative testing with the participation of both ASC and ASP.

The ASP/ASC employees will limit their repair activities to their respective facilities and/or equipment.

4.4 Maintenance of SS7 Links Within a Higher Rate Facility

When a SS7 link fails because of a failure in higher rate facility e.g. DS1, DS3, etc., the ASP or ASC receiving the alarm should notify the other party of the expected impact on the SS7 interconnection. Maintenance of the higher rate facility will be in accordance with existing procedures.

4.5 Trouble Clearance

After a link trouble has been cleared the ASP/ASC shall contact the other to advise that the trouble has been cleared, the nature of the trouble found and the action taken.

4.5.1 Trouble Report Status

- The Access Service Customer/Access Service Provider receiving the initial trouble referral shall provide a status on the disposition of that referral based on local agreements negotiated at the time of referral or requested on an individual case basis.
- Subsequent to the initial status report on the disposition of the trouble report periodic status's shall occur based on the following criteria:
 - When the trouble has been isolated
 - When there is a significant change in the status of the trouble.
 - The negotiated status interval has expired.
- Where mechanized trouble notification is utilized the receiving company shall status their appropriate systems based on paragraphs A and B, in addition it shall be the responsibility of the company issuing the trouble report to poll the mechanized status system for the status of the trouble report.

- Escalations if necessary shall be in accordance with identified procedures.

When a SS7 link(s) trouble has been cleared, the link(s) may or may not be automatically restored to service. If manual intervention is necessary on the part of the ASP/ASC or both, it should be coordinated by both parties. Each party will verify that the affected link(s) have been restored and are carrying traffic. If the link(s) fail to align or to carry traffic, the parties will continue the maintenance effort until the problem is resolved.

When trouble reports are being closed out between an Access Service Provider/Access Service Customer, whether they are using a mechanized system or a verbal notification, the disposition should be furnished by the company clearing the trouble, and the following information shall be provided:

The ASC and/or ASP should agree to provide the following information when closing a mutual trouble report:

- Circuit ID/telephone number
- Trouble Report Number (ASC/ASP number)
- Trouble Disposition (e.g., bad cable)
- Resolution details (e.g., cut to new cable)
- ASC will inform ASP if this trouble is measured.
- Referral time, returned time, No Access Time.
- If trouble report results in a service charge, the ASP will provide this info to the ASC

When there is a disagreement on the disposition, the parties engaged in the dispute shall document their respective positions, and the names of the individuals engaged in the dispute for audit purposes. Escalations if necessary shall be in accordance with identified procedures.

If after a trouble has been cleared and either the ASP or ASC wishes to change the Disposition, such changes shall be negotiated.

4.6 ASP Node To ASC Node Interconnect Testing And Analysis

The SS7 link(s) between an ASP and ASC are network to network interconnections. Trouble conditions may be experienced that cannot be resolved by each carrier testing and maintaining its own portion of the link(s). Some conditions may only be apparent to either the ASP or the ASC and require cooperative analysis of each others trouble indications or other data to sectionalize troubles. While it is the responsibility of the ASC to coordinate such activity, the ASP has the responsibility to notify the ASC of problems which may not be apparent to the ASC.

5 TRUNK RESPONSIBILITIES

5.1 Access Service Customer ASC/ASP

(See NGIIF Reference Document, Part II, Installation and Maintenance Responsibilities Switched Access Services Feature Groups B, C, and D).

5.2 Conversion of Multi-frequency Trunks to SS7

Conversion from in-band signaling to SS7 cannot be accomplished without a thoroughly planned process. The ASP/ASC implementation team should meet to discuss and identify all of the steps necessary for a successful trunk conversion. Each ASP/ASC should establish a Cutover Committee consisting of permanent members from the Ordering, Provisioning, Engineering, Operations, SS7 Control Center and Billing disciplines. Account

Representation for the ASC desiring interconnect may also be present when appropriate. The responsibility of the committee is to ensure a smooth conversion through scheduling and addressing, at a minimum, the concerns listed below. The following guidelines are offered as a starting point for discussion between an ASC and the ASP. They are not all inclusive.

5.2.1 TIME OF THE CONVERSION

On what day will the actual conversion start? What time during the day will it take place? If it is out of hours, there may be expense related concerns of work force adjustments. Times may have to be correlated with traffic volumes dependent upon trunk capacity.

5.2.2 TRUNK OPERATIONS TEST

Is this the first time a specific configuration (End Office Switch-Access Tandem-ASC Switch) has been tested? If so, a comprehensive test plan is suggested. If not, a substantially abbreviated test procedure may be appropriate. Will transmission test be performed?

5.2.3 TRANSITION TRUNK REQUIREMENTS

Will a transition trunk group need to be built? It should also be determined how the trunks will be converted with minimal service interruption. One method is to create a new trunk group for the SS7 trunks and overflow the MF trunk group to the SS7 group (or vice versa). Converting in this manner allows all trunks to be in service with the exception of those which are actively in the conversion process.

5.2.4 MAXIMUM NUMBER OF TRUNKS FOR CONVERSION

During that time that the trunks are actually being converted, they will be out of service. It must be determined how many trunks can be removed from service without adversely affecting traffic. Dependencies are the size of the trunk group, spare capacity and the time of conversion. Specific identification of trunks must be coordinate between the companies to ensure that both companies are converting the same trunks at the same time.

5.2.5 MANUAL VS AUTOMATIC

Will the ASP/ASC be using a mechanized procedure for converting the trunks? This information may be useful in scheduling the work.

5.2.6 FACILITIES CHANGES

It is not anticipated that there will be facility changes associated with the conversion of trunks. If they are required, the information should be conveyed at the preconversion meeting.

5.2.7 EQUIPMENT CHANGES

Most trunk equipment used for in band signaling should also work with SS7. However, some manufacturers may have designed their trunk equipment to work properly in the off-hook state only. This equipment, when used for SS7, would provide degraded transmission since, in relation to E&M signaling, the circuit will always be on-hook.

5.2.8 SWITCH TYPES

The switch types involved in the conversion should be identified to address special needs of specific switches. For example, a switch may require that the Trunk Circuit Identification Code (TCIC) and the trunk number be of the same value. Identification of the switches will also allow the companies to determine the extent of testing that will take place (see TRUNK OPERATIONS TEST above).

5.2.9 NMC NOTIFICATION

The NMC should be notified of the conversion to enable the center to monitor the trunk group, especially during the time of conversion/reduced capacity. The NMC may also be able to inform the Conversion Team of any special calling events (mass calling) which may be occurring at the time of the conversion.

5.2.10 SCHEDULE

As offices become equipped for Common Control Switching Access Capability (CCSAC), it is likely that more than one ASC will want to interconnect with a specific end office. The scheduling of conversions must be coordinated by the ASP, with individual ASCs, and agreed to by the involved companies.

5.2.11 TIMER VALUES

The ASC and ASP switches and STPs have many timers associated with link operation and call setup. Since only parameters and not the actual values are stated in technical references, it is likely that the ASC and the ASP will have different time settings for the same timer. Although there is no requirement that the value of specific timers be the same (see note) in both companies, the sharing of the values will provide each company with additional information for trouble resolution.

Note: The T2 Link Timer is the only known exception and must have different values at each end.

To ensure network integrity and reliability, SS7 Timer settings (MTP Level 2 and Level 3, ISUP and SCCP) should be exchanged at time of interconnection negotiation.

5.2.12 POINT CODES

If an ASC/ASP is contemplating interconnecting, it is essential that point code range information be known well in advance to enable the control center to update the STP during the scheduled split mode operation. Point codes include those of the STP, the interconnecting switches and any alias point codes.

5.2.13 RCT (Route-Set-Congestion Test) METHODOLOGIES

It is recommended by the NGIIF that interconnected networks adopt the practice of responding to TFC (Transfer Controlled) messages by assigning RCT (Route-Set-Congestion test) messages using SLS (Signaling Link Selection) codes that ensure an equal distribution on all the links in the linkset (combined). Prior to CCS interconnection the interconnecting companies should exchange RCT methodologies.

5.2.14 TRUNK CONFIGURATION

Using In Band signaling, it is possible for an ASC to have one large trunk group from the ASP to the POP and then split the facilities to several different switches on their side of the POP. In this arrangement, the ASP routes all traffic to the single trunk group and the ASC splits it according to their needs. This same configuration will not work using SS7 unless the trunk group is split on the ASP side of the POP as well. It is necessary to split the trunk group because in the SS7 environment, traffic is routed between switches and not between a POP and a switch. One method of accommodating an ASC with this situation, would be to split the trunk groups between switches and then first route all traffic to one of the groups. That trunk group could then route advance to another. The ASC would be able to balance loads between switches through proper sizing of the trunk groups. At the conversion meeting it should be determined if this situation exists and if it does, how it will be handled. How will traffic be routed to the separate trunk groups? What are the switched nomenclature? Will the trunk groups have to be resized/rearranged? Will the trunk groups be rearranged, prior to SS7 conversion?

As a result of technological changes in the network due to the implementation of SS7 there has been an increase in short duration calling patterns (Abandoned Calls) in an Interworking environment. Therefore it is the recommendation of the NGIIF that the following actions take place where interworking is encountered between interconnected carriers. Where appropriate to reconcile the situation:

All Service Providers having switches with:

- TCRA Timer should be in compliance with ANSI (T1.113 Issue 3) which recommends a setting of twenty (20) seconds.
- Inter Stage Timer (IST)* should be set at fifteen (15) seconds.
- Partial Signal Partial Dial (PSPD) Timer should be set at a minimum of twenty (20) seconds and at a maximum of thirty (30) seconds.

5.2.15 FREQUENCY OF CONTINUITY TESTS

When In Band signaling is used, continuity of the trunk selected is assured by call setup. Continuity testing is also available on SS7 trunks. The switch will automatically send, receive and measure tones placed on the trunk prior to setting up a call. The switch will perform continuity on a circuit at a variable rate of 1 out of n times where n has a value of 1 to 16. It is this information (the value of n) which should be exchanged with the ASC. The NGIIF has agreed to perform continuity operation tests, at a minimum rate of (1) one out of (8) eight.

NOTE: Where technology does not exist to facilitate meeting the above criteria, local negotiations should take place.

5.2.16 2-WIRE CONTINUITY CHECK EMULATION ON A 4-WIRE SWITCH

An exchange terminating a 4-wire circuit is recommended to provide an additional procedure using two tone continuity check procedures. Optionally, by agreement between connecting 4-wire exchanges, either:

- Both exchanges emulate 2-wire exchanges in the continuity check procedure of Section B.2 (Continuity-check for 2-wire speech circuits) of T1.113.4. Note, this requires an equipment upgrade of both exchanges to detect 1780 Hz tone.
- One of the exchanges terminating a 4-wire circuit may emulate operation of a 2-wire exchange in the continuity check procedure in Section B.3 (continuity-check between a 2-wire and 4-wire exchange) of T1.113.4, while the far end exchange must furnish 4-wire to 2-wire procedure. Note, in this case, only one exchange requires an equipment upgrade, however, there is increased administration requirement to ensure correct 4-wire/2-wire configuration.

The use of two tone continuity check procedures will allow detection of inadvertent loops in the trunk facility between exchanges that terminate 4-wire circuits because different frequencies are transmitted and received.

5.2.17 DIVERSITY ARRANGEMENTS

The ASP/ASC should exchange link diversity arrangements (Planned and Current).

5.2.18 NEW PARAMETERS

Companies who have completed SS7 interconnection and acquire customers with ISDN capabilities have a need and responsibility to communicate to their interconnected network providers the passage of such parameters.

3.1 KHz audio and speech should be passed by all interconnecting SS7 partners. Where known non-conformances exist, dialogue needs to take place.

Per local negotiations, all interconnecting companies utilizing ACC should acknowledge and respond when an ACC message is received.

Interconnecting parties should exchange the initial value of the Hop Counter at the time of negotiation for interconnection and as changes are anticipated/made in signaling between the two networks.

If no hop counter is received with the incoming IAM, then if the hop counter capability is active, a non-forwarding transit exchange should include the hop counter parameter in the outgoing Initial Address Message. For technologies where the hop counter cannot be set on a per call type basis and for non-ETS calls, the network operator should set the initial count value within a range between 15 and 20. In addition, if the initial count value can be set by the network operator on a per-call type basis, then the initial count value for ETS calls should be the maximum value allowed in the exchange.

The value received should be accepted as a valid value, and the recipient switch should not reinitialize the Hop Counter. For SIP-I, the I-IWU acting as an independent exchange should perform the normal BICC/ISUP Hop Counter procedure using the Hop Counter taken from the encapsulated IAM.

The NGIIF has looked at customer call forwarding/call looping issues and the related network parameters (such as the HOP counters, max forwards in an IP network, redirection information [RI], history information) which are available in either the TDM or IP networks. The current state of the implementation in the industry will not support a full resolution of problems induced by customer call forwarding using these capabilities; therefore, the NGIIF offers the following recommendations in addition to the recommendations listed above and located in the NGN document:

- Network providers should review the use of simultaneous call forwarding restrictions that limits the number of times calls can be forwarded through a single line.
- Service providers should review their services to determine whether they easily allow configurations that can generate call looping. For example, it might be desirable to design restrictions so that a customer can't simultaneously forward their mobile calls to their land line at that same time their land line is forwarding calls to their mobile line.

5.2.19 EMERGENCY COMMUNICATIONS

In the remote event that a total SS7 failure is experienced, some means of communication between personnel in interconnecting networks, may be required. The ASP/ASC should determine what emergency communications are already available and/or what alternative methods, if any, will be provided.

- It is recommended that all interconnecting networks (ICNs) and manufacturers interconnect via Public Packet Switched Network (PPSN), non PSN Access, as part of a Closed User Group, in support of and to provide backup of the voice emergency communications network. The PPSN is to be utilized as a backup to the PSN as part of the Emergency Communications System (ECS). Information to be communicated between entities should be identified and shared for ECS information. The following information was developed by the NGIIF and should be utilized, where possible:
 - Security Password: (Exchangeable)
 - Station Handshake: (ASCII Text)
 - To: (Addressee)
 - From: (Company who sent message)
 - Date: (Current Date)
 - Time: (Current Time)
 - Outage Date: (Outage Date)
 - Outage Time: (Outage Time)
 - Node Type: (STP,SCP,Etc.)
 - Location: (Office where incident occurred)
 - Point Code: (Point Code of Office)
 - Severity: (Isolation, Critical, Major, Minor, etc.)
 - Vendor:
 - Comments (if any)
 - End of Comments
 - END: (Identifies End of Message)

5.2.20 LINK RESTORAL OBJECTIVE

5.2.21 AVAILABLE OPTIONAL AUTOMATIC TESTING

Signaling Link Test Message (SLTM). Automatically run during link alignment. Not necessary for trunk conversion.

Circuit Validation Test Message (CVTM/CVR). Verifies that the translations at each end of the will select the same trunk. Essential for trunk conversion and should also be performed on a periodic basis.

5.3 Trunk Circuit Identification Code (TCIC)

The ASC will administer/assign the Trunk Circuit Identification Codes (TCICs). Certain switches require that the Common Language Circuit Identifier (CLCI) trunk number equals the TCIC.

5.4 Trunk Circuit Identification Code (TCIC) Numbering Plan

5.4.1 Assignment Criteria

The (TCIC) assignment is a five (5) digit number. Numbers are right justified with leading zeros. The ten thousand digit should always be a zero, due to trunk number restrictions in some switches.

The five (5) digit numbers (00001 - 09996) should be broken down into sub-blocks of 96 numbers (i.e., 0001 - 00096, 00101 - 00196, etc.). Numbers ending in 97, 98, 99 and 00 will not be assigned, due to the limitations of some digital switches.

Sub-blocks of 96 will not be split between groups of trunks with the same customer Point Code and Exchange Company Point Code. This assures a group will always start with 1 and provides for consecutive numbering.

The smallest available will be selected for new groups or augments requiring an additional sub-block. Ascending order of assignments is required for minimizing memory loss in some machines.

TCIC assignments will not be duplicated on groups between the same point codes. A mechanized assignment process with edits is recommended to prevent dual assignments.

TCIC assignments will be provided on all add, change and disconnect Access Service Request (ASR) activity requests. TCIC numbers should be reused on coordinated disconnects and add activity to assure reassignment of the lower sub-blocks to minimize loss in some machines.

5.5 Tones and Announcements

Where possible, based upon SS7 connectivity and interworking, the terminating ASP should release calls that have encountered network situations such as, reorder, vacant code, no circuit and line busy to the ASC, with a specific cause indication. The ASC, based upon agreements with the originating ASP, may either connect the call to a tone/announcement and subsequently release the call with a normal cause indicator to the originating ASP, or release the call to the originating ASP. This release with a specific cause indicator for the originating ASP should provide the tone or announcement. ASCs in agreement with the originating ASP and compliance to all applicable SS7 message sequences may choose to recognize specific release cause messages and connect tone or announcement. The ASC will return to the originating ASP, a suitable coded ACM message prior to connecting the call to a ASC tone or announcement. Properly coded release messages will be forwarded to the ASP at the completion of the tone and announcement application. All response message sequences will need to be within the tolerances defined in timing parameter "T-IAM" of ANSI T1.113. Customized announcements, such as automatic intercept for number changes, would have to be played by the terminating ASP. If there is not total SS7 connectivity in the terminating connection the terminating ASP may have to play all tones and announcements. If there is not SS7 connectivity in the originating access, the originating ASP may not be able to play tones and announcements.

An SS7 Cause Codes & Tones and Announcements document is included as Part III Attachment H. This document provides a single source for definitions, application of cause codes with the associated treatment and the appropriate verbiage to be played to the customer where an announcement is required.

5.6 *Trouble Report Disposition*

When trouble reports are being closed out between an Access Service Provider/Access Service Customer, whether they are using a mechanized system or a verbal notification, the disposition should be furnished by the company clearing the trouble, and the following information shall be provided:

The ASC/ASP should agree to provide the following information when closing a mutual trouble report:

- Circuit ID/telephone number
- Trouble Ticket Number (ASC/ASP number)
- Trouble Disposition (e.g., bad cable)
- Resolution details (e.g., cut to new cable)
- ASC will inform ASP if this trouble is measured.
- Referral time, returned time, No Access Time.
- If trouble ticket results in a service charge, the ASP will provide this info to the ASC

When there is a disagreement on the disposition, the parties engaged in the dispute shall document their respective positions, and the names of the individuals engaged in the dispute for audit purposes. Escalations if necessary shall be in accordance with identified procedures.

If after a trouble has been cleared and either the ASP or ASC wishes to change the disposition, such changes shall be negotiated.

6 TRUNK INSTALLATION

6.1 *Point of Presence (POP) Serving Multiple Switches*

Where an Access Service Customer (ASC) has multiple switches served by one POP, a separate trunk group for each switch must be established from the ASP switch to the POP to accommodate SS7 trunk traffic. Each trunk group will require the unique Signaling Point Code (SPC) for each ASC switch and ASP switch. When an ASC has multiple switches connecting through a single POP or a single switch connecting to multiple POPs, separate trunk groups must be established using the unique Signaling Point Code of each ASC switch and ASP switch.

7 TRUNK TROUBLE DETECTION RESPONSIBILITIES

It is recommended that continuity checks (COT) be performed by ASPs and ASCs on a one (1) out of eight (8) statistical basis. Because of different manufactures implementation of COT capabilities, this may have to be performed at either the trunk group level, or at the office level. If the COT must be performed at the trunk group level, then the one (1) out of eight (8) COT will only be performed on all access trunk groups. If the COT is designated at the office level, then the one (1) out of eight (8) requirement is performed on the entire office base. Between 4-wire switching offices, COT is performed on a loop basis, however, when one or both offices involved are 2-wire switches, each transmission direction is checked independently. As long as the continuity check is performed at recommended levels, a "killer" trunk condition should only occur if the trunk is looped.

NOTE: Where technology does not exist to facilitate meeting the above criteria, local negotiations should take place.

8 SCREENING AND TRANSLATIONS

8.1 Final Global Title Translations (FGTT)

Final Global Title Translations (FGTT) should be performed in the terminating network. Interconnecting parties should discuss their routing and Gateway Screening of Network Management Messages between interconnected STPs to ensure that all appropriate messages can be routed in the presence of route failures.

In order to interconnect to a network which utilizes cluster routing, the NGIIF recommends that each network demonstrate that network management features are being provided to the other network, and conform to the following interworking rules:

- The interconnecting network should not ignore TFP, TFR, TFA, TCP, TCR, TCA, and signaling route set test messages, and shall respond, and/or send the appropriate RSx/RCx message if the above TFP/TFR, TCP/TCR messages received are in conformance with ANSI Standards.
- Network elements performing cluster routing in receipt of a network management message should create and maintain a status listing of all members within the defined cluster to which it performs routing until appropriate allow messages have been associated with all such members.
- When the TFC message is sent, the message shall contain the full Point Code (PC) of the message Point Code of the Message Destination (DPC) and the affected Point Code (the route to which is in congestion).
- In the event of routing methodology changes the interconnected network should be notified by the company initiating the change, before implementing cluster routing.
- Member 000 should never be assigned for a cluster used for an End Office/Tandem /SCP point code, i.e. point codes of a signaling end point. The cluster member code 000 is reserved for addressing signaling points that serve as a signaling transfer point.
- When performing any live network testing, a non-working cluster should be used to avoid network incidents due to misinterpretations of signaling protocols.

NOTE: Where technology does not exist to facilitate meeting the above criteria, local negotiations should take place.

8.2 Translation Types

A uniform application/utilization of a numbering scheme will prolong the life of the resource.

The ANSI Standard (T1.112.3-1996, Annex A) specifies standard Translation Types (TTs) which should be used. The standard also specifies multiple translation types (TTs) for two applications (CLASS and LIDB) TTs 251 or 6; 253 or 2 should be used in accordance with the standard. The following recommendations be considered when interconnecting TTs 251 or 6; 253 or 2 with another Service Provider:

- Translation Types being utilized by the ILEC should be considered for adoption by the newly established CLECs during local negotiations.
- In the event that translation types are already being used by the interconnecting CLEC that differ from the ILEC then the parties involved should engage in local negotiations to determine their numbering convention.
- In the event that a CLEC is interconnecting with multiple ILECs then the involved parties shall engage in local negotiations.
- Existing service Providers/Customers already utilizing specific Translation Types shall engage in local negotiations to determine what Translation Types should be utilized.
- Where existing service providers/service companies are already interconnected and are now proposing to provide services new to the area, then local negotiations should take place to determine the Translation Type (TT) to be used.

8.3 TCAP Transaction Looping

TCAP transaction looping can congest B links very quickly. Several mechanisms are available (T1S1.6) to prevent such looping and should be implemented through bi-lateral agreements. Two mechanisms, Gateway Screening and Translation-Type mapping loop-prevention, were proven through industry (NTC Phase 10) testing to prevent looping caused by incoming messages.

The NGIIF recommends the following:

For TCAP transactions, interconnected companies should utilize loop detection/prevention mechanisms bi-laterally.

Reference: T1S1.6 - Technical Requirements for Number Portability - Database and Global Title Translations. (T1S1/98-174)

9 Rules for Populating JIP

1. JIP should be populated in the IAMs of all wireline and wireless originating calls where technically feasible.
2. JIP should be populated with an NPA-NXX that is assigned in the LERG to the originating switch or MSC.
3. The NGIIF does not recommend proposing that the JIP parameter be mandatory since calls missing any mandatory parameter will be aborted. However, the NGIIF strongly recommends that the JIP be populated on all calls where technologically possible.
4. Where technically feasible if the originating switch or MSC serves multiple states/LATAs, then the switch should support multiple JIPs such that the JIP used for a given call can be populated with an NPA-NXX that is specific to both the switch as well as the state and LATA of the caller.

If the JIP cannot be populated at the state and LATA level, the JIP should be populated with an NPA-NXX specific to the originating switch or MSC where it is technically feasible.
5. Where the originating switch cannot signal JIP it is desirable that the subsequent switch in the call path populate the JIP using a data fill default associated with the incoming route. The value of the data fill item is an NPA-NXX associated with the originating switch or MSC and reflects its location.
6. When call forwarding occurs, the forwarded from DN (Directory Number) field will be populated, the JIP will be changed to a JIP associated with the forwarded from DN and the new called DN will be inserted in the IAM.
7. As per T1.TRQ2, the JIP should be reset when a new billable call leg is created.

It is recommended that the Gateway node be pre-positioned to support a set of configurable options for populating the JIP field in order to more quickly deploy the solution when agreement has been reached. These options include one value per Gateway, a separate value per IP source entering the Gateway or any other Jurisdiction Information like parameter carried in the SIP Invite message. In the event these values are necessary in the future, they can be stored in memory and administered by the operating company of the Gateway. The values could be any 6 digit values.

This recommendation only resolves the SS7 protocol requirements as specified in ATIS-1000113.2005. The concerns regarding the generic usefulness of JIP for billing and other operational procedures remain unresolved.

10 SS7 NETWORK SECURITY BASE GUIDELINES

This section specifies the minimum set of security features to be adopted by Access Service Providers and the Access Service Customers and is documented in Part III Attachment I.

SS7 network providers are responsible for ensuring the reliability and security of their own SS7 networks with respect to defending against the propagation of abnormal SS7 signaling messages when interconnected with other networks. This responsibility should ensure protection against unexpected SS7 messages, SS7 messages with protocol errors, attempts at sabotage, or any other harmful conditions that may be propagated across interconnected SS7 networks.

It should be noted that SS7 network intermediate nodes generally examine those parts of incoming messages with respect to routing of the message. The SS7 destination node examines additional information for the proper processing of the message, and this may include additional security considerations. Examination of the content of every message routinely is not done, and may not be practical. Various methods of protocol analyzation that further examine message content are available to detect and resolve troubles, but are generally utilized only on an exception basis.

A variety of processes and responsibilities intended to ensure reliability, network security, and risk minimization associated with SS7 network interconnection are outlined elsewhere in the document.

11 SS7 SOFTWARE VALIDATION

Service providers and vendor/manufacturers have an obligation to their customers to provide the highest standard of error free software possible. In light of this obligation the industry has developed a set of recommendations for the validation of software and is documented in Part III Attachment J.

12 DUAL STP FAILURE PREVENTION PROCEDURES

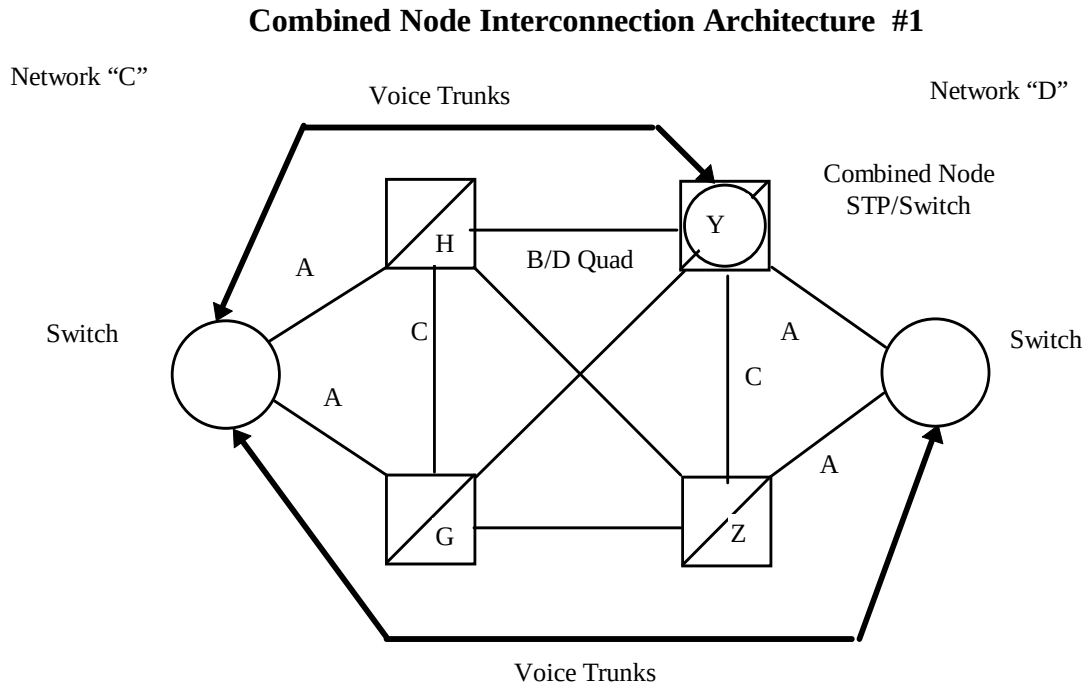
The NGIIF recommends that each STP Owner/Operator have in place a written procedure to assist in the prevention of dual STP failure. Part III Attachment K provides a minimum set of recommended guidelines to prevent dual STP failures.

13 COMBINED NODE - MINIMUM SET OF GUIDELINES

13.1 Architecture

Typical Combined Node Architectures are identified in the following two network diagrams:

Figure 3 - Combined Node Interconnection Architecture #1



Combined Node Interconnection Architecture #2

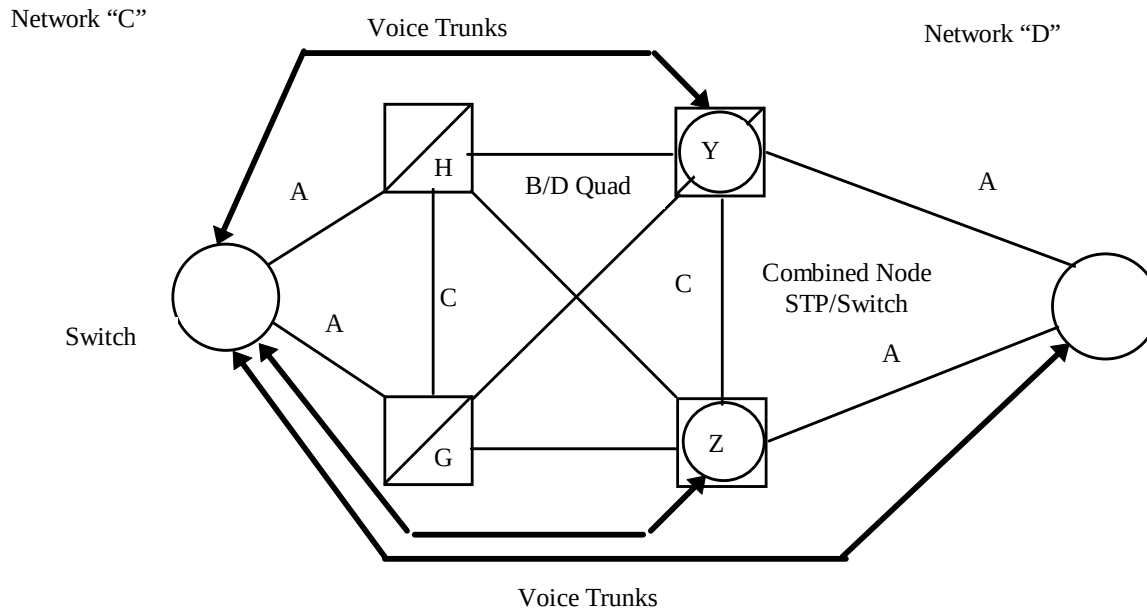


Figure 4 - Combined Node Interconnection Architecture #2

13.2 Routing And Configuration

Load Balancing of the interconnecting Links (A, B/D) is required as specified in Load Balance Tests in the NGIIF SS7 Reference Document –Part III (Attachment A - Test 1.27).

It is the responsibility of each network operator to send balanced traffic. In situations where special translations and screening are required to achieve load balancing on traffic originating from the combined node, those translations are the responsibility of the combined node owner/operator.

13.3 Network Management

Where Combined Nodes are utilized in an interconnected environment, the interconnected parties need to identify and resolve operational concerns (e.g., Load Balance)

It is preferred that a single point code be established for the switch portion of the combined node, and a different point code be established for the STP portion of that switch.

Functionality of the combined node must send and respond to Network Management Messages (TFP/TFR/etc.) in accordance with established NGIIF Procedures as found in the NGIIF Reference Document (Part III - Section 8. Screening and Translations)

13.4 Diversity

The node should meet the established NGIIF Link Diversity guidelines. (Part III - Section 2 - Subsection E - Diversity)

13.5 Testing

When interconnecting with a Combined Node, all applicable tests are referenced in the NGIIF Reference Document - Part III - Attachments A, B, C, D, E, and F should be performed.



ATIS-0300012

**Next Generation Interconnection Interoperability (NGIIF)
Reference Document**

**Part III, Installation, Testing and Maintenance
Responsibilities for SS7 Links and Trunks**

**Attachment A
MTP Compatibility Tests**

Version 12.0



ATIS is the leading technical planning and standards development organization committed to the rapid development of global, market-driven standards for the information, entertainment and communications industry. More than 200 companies actively formulate standards in ATIS' Committees, covering issues including: IPTV, Cloud Services, Energy Efficiency, IP-Based and Wireless Technologies, Quality of Service, Billing and Operational Support, Emergency Services, Architectural Platforms and Emerging Networks. In addition, numerous Incubators, Focus and Exploratory Groups address evolving industry priorities including Smart Grid, Machine-to-Machine, Connected Vehicle, IP Downloadable Security, Policy Management and Network Optimization.

ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications' Sectors, and a member of the Inter-American Telecommunication Commission (CITEL). ATIS is accredited by the American National Standards Institute (ANSI). For more information, please visit www.atis.org.

Notice

This document was developed by the Alliance for Telecommunications Industry Solutions' (ATIS) sponsored Next Generation Interconnection Interoperability Forum (NGIIF). The NGIIF addresses next-generation network interconnection and interoperability issues associated with emerging technologies. Specifically, it develops operational procedures which involve the network aspects of architecture, disaster preparedness, installation, maintenance, management, reliability, routing, security, and testing between network operators. In addition, the NGIIF addresses issues which impact the interconnection of existing and next generation networks and facilitate the transition to emerging technologies.. All changes to this document shall be made through the NGIIF issue resolution process.

Note Regarding Previous Versions

The NIIF Reference Document was formerly known as the Network Operations Forum (NOF) Reference Document. The NOF Reference Document was published and maintained by Bellcore. The last version of the NOF Reference Document is Issue 13.

Disclaimer and Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

ATIS-0300012, NGIIF Reference Document, Part III, Installation and Maintenance Responsibilities for SS7 Links and Trunks, Attachment A, MTP Compatibility Tests, Formerly NIIF 5007

The NGIIF Reference Document, Part III, Installation and Maintenance Responsibilities for SS7 Links and Trunks is an ATIS standard developed by the NGIIF.

Published by

Alliance for Telecommunications Industry Solutions

1200 G Street, NW, Suite 500

Washington, DC 20005

Copyright © 2011 by Alliance for Telecommunications Industry Solutions

All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < <http://www.atis.org> >.

Printed in the United States of America.

INSTALLATION, TESTING AND MAINTENANCE RESPONSIBILITIES FOR SS7 LINKS AND TRUNKS, ATTACHMENT A - MTP COMPATIBILITY TESTS

Table of Contents

1	GENERAL TESTS	5
1.1	MTP LEVELS 2 AND 3 COMPATIBILITY TESTING	5
1.2	INITIAL SS7 INTERCONNECTION	5
1.3	TESTING ENVIRONMENT	5
1.4	OTHER TESTING CONSIDERATIONS.....	5
2	TEST SCRIPTS	6
2.1	TIMER T2.....	6
2.2	TIMER T3.....	7
2.3	TIMERS T1 AND T4.....	8
2.4	TIMER T4 EMERGENCY.....	9
2.5	DEACTIVATION DURING INITIAL ALIGNMENT	10
2.6	DEACTIVATION DURING ALIGNMENT	11
2.7	SIO RECEIVED DURING LINK IN-SERVICE.....	12
2.8	SIO RECEIVED DURING IN-SERVICE STATE	13
2.9	DEACTIVATION DURING THE PROVING PERIOD	14
2.10	BREAK TRANSMISSION PATH - LINK ALIGNED AND READY	15
2.11	CORRUPT FIBS	16
2.12	FLAG INSERTION WITHIN OCTET BOUNDARIES	17
2.13	SIGNAL UNIT ERROR RATE MONITOR	18
2.14	SIGNAL UNIT ERROR RATE MONITOR	19
2.15	CONSECUTIVE CORRUPT SIGNAL UNITS	20
2.16	ALIGNMENT ERROR RATE MONITOR	21
2.17	ALIGNMENT ERROR RATE MONITOR	23
2.18	NEGATIVE ACKNOWLEDGMENT	25
2.19	RETRANSMISSION BUFFER FULL.....	26
2.20	ERRONEOUS FIB.....	29
2.21	ERRONEOUS RETRANSMISSION -MULTIPLE FISU	30
2.22	ABNORMAL BACKWARD SEQUENCE NUMBER.....	31
2.23	ABNORMAL BACKWARD SEQUENCE NUMBER.....	32
2.24	DELAY OF ACKNOWLEDGMENT	33
2.25	LINK ACTIVATION - MULTIPLE LINKS	34
2.26	DISCRIMINATION OF INVALID POINT CODE	36
2.27	LOAD DISTRIBUTION	37
2.28	LOAD SHARING BETWEEN LINK-SETS - BETWEEN TWO LINK-SETS.....	38
2.29	CHANGEOVER INITIATED AT ONE SIDE OF A LINK-SET	39
2.30	CHANGEOVER TO AN ALTERNATE LINKSET.....	40
2.31	CHANGEBACK WITHIN A LINK-SET	41
2.32	CHANGEBACK FROM ANOTHER LINK-SET.....	42
2.33	INHIBIT AVAILABLE LINK.....	43
2.34	INHIBIT AVAILABLE LINK.....	44
2.35	INHIBIT UNAVAILABLE LINK	45
2.36	LINK FORCED UNINHIBIT.....	46
2.37	MANAGEMENT INHIBITING TEST - NORMAL PROCEDURE	47
2.38	NORMAL ALIGNMENT.....	48
2.39	BROKEN TRANSMISSION PATH TRANSMISSION PATH”	49
2.40	MSU GENERATION.....	50
2.41	MANAGEMENT UNINHIBIT WITH CHANGEBACK	51
2.42	MANUAL UNINHIBITION OF A LINK - WITHOUT CHANGEBACK	52
2.43	SIGNALING ROUTE MANAGEMENT TESTS (ISSUE 11, PAGE 19 & 20)	53
2.44	SIGNALING ROUTE MANAGEMENT TESTS.....	54
2.45	SIGNALING ROUTE MANAGEMENT TESTS.....	55

2.46	SIGNALING ROUTE MANAGEMENT TESTS.....	56
2.47	SIGNALING ROUTE MANAGEMENT TESTS.....	57
2.48	PROCESSOR OUTAGE	59
2.49	LEVEL 2 FLOW CONTROL	61
2.50	HUBBING INTERCONNECTION TEST	64
3	ATTACHMENT A – MTP COMPATIBILITY TESTS, TEST DIAGRAMS	65
4	ANNEX REFERENCES	67

1 General Tests

The following tests are recommended by the Next Generation Interconnection Interoperability Forum (NGIIF) to verify the compatibility of two networks during interconnection. These tests are intended to be used as a recommended set of minimum tests of levels two and three of the SS7 protocol.

It is assumed that the two interconnecting networks may have some additional tests they may wish to perform during interconnection. In that case, these tests should be part of the bilateral agreements developed for SS7 network interconnection.

1.1 MTP Levels 2 and 3 Compatibility Testing

Compatibility testing checks for the correct interworking of two SS7 implementations. The tests are written for the interconnecting of two given implementations. These tests will be performed not only on new signaling points but may also be performed between already-connected signaling points.

1.2 Initial SS7 Interconnection

The full test suite should be run between the two interconnecting companies for any interconnection configuration that was not previously tested. The configuration is defined by both manufacturer model and software load of the interconnecting signaling network elements. Subsequent interconnections, using configurations previously tested by the two interconnecting companies, may be tested at their discretion.

1.3 Testing Environment

The tests in this document are Intrusive and Non-Intrusive Tests. These terms are defined as follows:

- Intrusive - The interconnecting circuit shall be interrupted and the testing unit inserted into the circuit to act as an emulator to the Signaling Point under test. Level 3 tests require a message generating device to create traffic, allowing protocol messages to be viewed for proper changeover, changeback, SIOS, FISU, etc.
- Intrusive Testing may impact a live working network. Therefore testing should be based on locally negotiated agreements.
- Non-Intrusive - The test unit shall be able to observe traffic, and/or messages traversing the link or links between the two Signaling Points under test in a monitor mode.

1.4 Other Testing Considerations

The Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS) provide priority call completion to authorized users during times of network stress or congestion. GETS and WPS include the capability of coding the ISUP Calling Party's Category parameter with the NS/EP code point (11100010) and setting the SS7 MTP link level priority for IAM to 1. When performing MTP compatibility tests, SS7 MTP link level priority for IAM testing should be performed as described in Part D of Section 1, Introduction, of NGIIF Reference Document 5008: Installation, Testing and Maintenance Responsibilities for SS7 Links and Trunks, Part III - Attachment B, ISUP Compatibility Tests.

2 Test Scripts

NGIIF Test #: **ANSI T1-234-2000 Test #:** **GR-CORE-905 Test #**

2.1 Timer T2	M2-1.2	1.2 Timer T2

PROTOCOL REFERENCE: ANSI T1.111, chapter 3, clause 7

TITLE: Link State Control - Expected signal units/orders

SUBTITLE: Timer T2

PURPOSE: To check "Not Aligned" Timer T2

PRE-TEST CONDITIONS: Link out of service

CONFIGURATION: 1

EXPECTED SIGNAL UNIT SEQUENCE:

SP B		SP A
<u>Link</u>		<u>Link</u>
1-1 SIOS	----->	
	<-----	SIOS
		: start
	<-----	1-1 SIO
		T2
	<-----	1-1 SIOS

TEST DESCRIPTION:

1. The terminal being tested (SP A) will send SIO-status Indicator out of Alignment (state 01). Timer T2 is started upon entry into state 01. The low and high values of T2 are 11.5 and 23.0 secs.
2. The test unit (SP B) will send continuous SIO.
3. After expiration of Timer T2, the terminal (SP A) shall suspend alignment and send SIOS.

Note: When testing between signaling points, ensure that the time-out value is different at each end.

NGIIF Test #: _____ **ANSI T1-234-2000 Test #:** _____ **GR-CORE-905 Test #** _____

2.2 Timer T3	M2-1.3	1.3 Timer T3

PROTOCOL REFERENCE: ANSI T1.111, chapter 3, clause 7

TITLE: Link State Control - Expected signal units/orders

SUBTITLE: Timer T3

PURPOSE: To check "Aligned" Timer T3

PRE-TEST CONDITIONS: Link out of service

CONFIGURATION: 1

EXPECTED SIGNAL UNIT SEQUENCE:

SP B			SP A	
<u>Link</u>			<u>Link</u>	
		<-----	1-1	SIOS
1-1	SIOS	----->		
				:start
		<-----	1-1	SIO
1-1	SIO	----->		
		<-----	1-1	SIN or SIE
				T3
		<-----	1-1	SIOS

TEST DESCRIPTION:

1. The terminal being tested (SP A) will send SIO.
2. The test unit (SP B) responds with SIO.
3. The terminal sends SIN/SIE (normal or emergency).
4. The test unit continues to send SIO.
5. After the terminal timer T3 expires, the terminal sends SIOS.

Note: Time T3 has a nominal value of 11.5 sec., and an accuracy range from 5 to 14 secs.

2.3 Timers T1 and T4	M2-1.4	1.4 Timers T1 and T4 (Normal)

PROTOCOL REFERENCE: ANSI T1.111, chapter 3, clause 7

TITLE: Link State Control - Expected signal units/orders

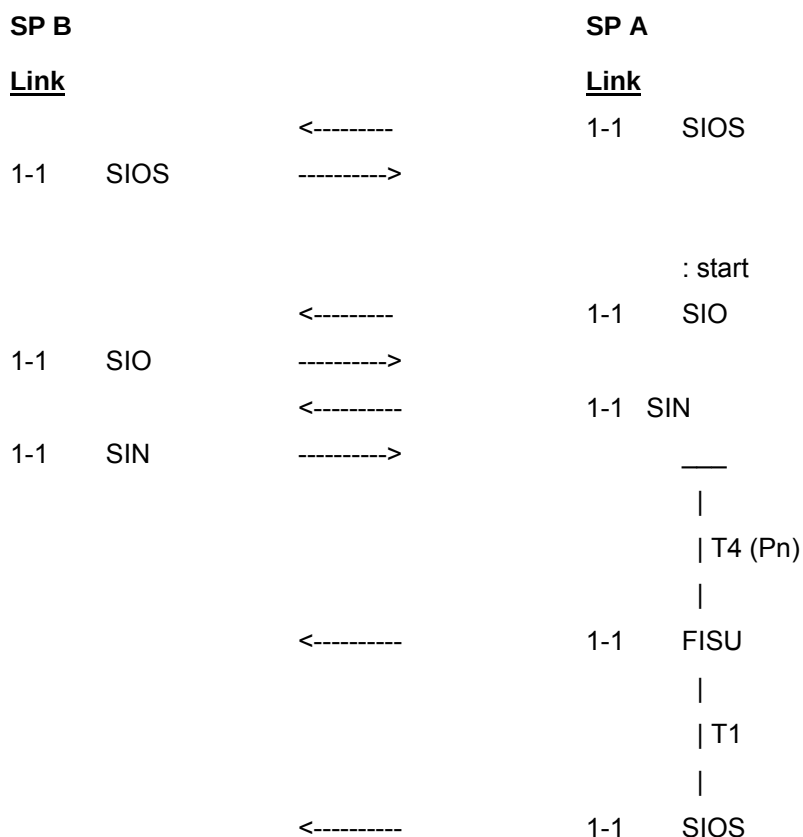
SUBTITLE: Timer T1 & Timer T4 (Normal)

PURPOSE: To check "Aligned ready" Timer T1 and "Proving period" Timer T4 (Normal)

PRE-TEST CONDITIONS: Link out of service

CONFIGURATION: 1

EXPECTED SIGNAL UNIT SEQUENCE:



TEST DESCRIPTION:

1. The terminal being tested (SP A) sends SIO.
2. The test unit (SP B) responds with SIO.
3. The terminal sends continuous SIN, and the test unit sends continuous SIN.
4. After normal alignment proving period (T4), the terminal sends FISUs.
5. The test unit continues to send SIN. After the terminal timer T1 expires, the terminal sends SIOS.

Note: Timer T4 (normal) has a value of 2.3 secs., with an accuracy of $\pm 10\%$. T1 has a value of 13.0 secs., with an accuracy range from 13 to 30 secs.

2.4 Timer T4 Emergency	M2-1.6	1.19 Timer T4 (Emergency)

PROTOCOL REFERENCE: ANSI T1.111, chapter 3, clause 7

TITLE: Link State Control - Expected signal units/orders

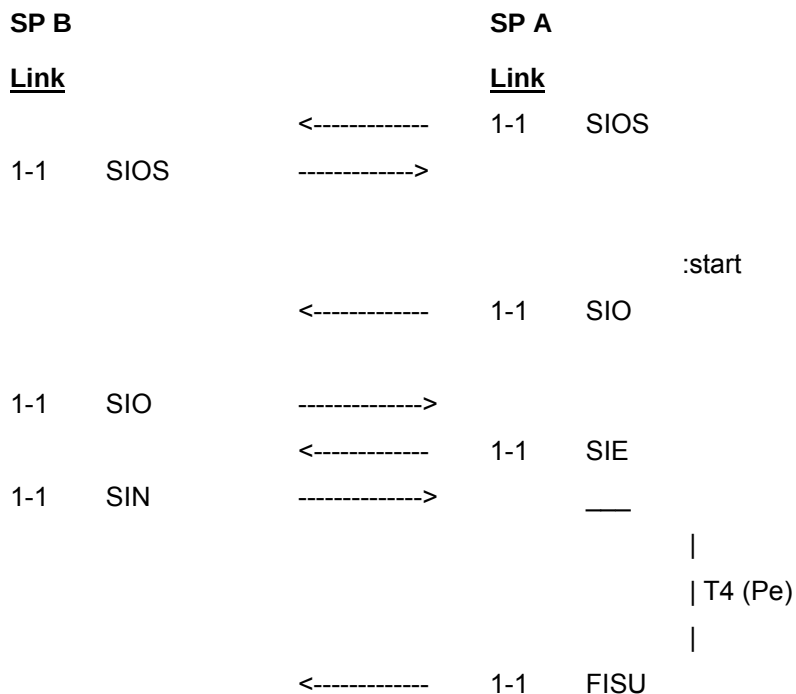
SUBTITLE: Set emergency while in "Not aligned state"

PURPOSE: To test that emergency proving can be set during normal initial alignment

PRE-TEST CONDITIONS: Link out of service

CONFIGURATION: 1

EXPECTED SIGNAL UNIT SEQUENCE:



TEST DESCRIPTION:

1. Start emergency alignment on the terminal (SP A) side.
2. The terminal and test unit (SP B) send SIOs.
3. The terminal sends continuous SIE (emergency). The test unit sends continuous SIN (normal).
4. After timer T4 (emergency) expires, the terminal sends FISU.

Note: Timer T4 (emergency) has a value of 0.6 secs., with an accuracy of $\pm 10\%$.

NGIIF Test #:

ANSI T1-234-2000 Test #:

GR-CORE-905 Test #

2.5 Deactivation During Initial Alignment

M2-1.7

**1.25 Deactivation During Initial
Alignment**

PROTOCOL REFERENCE: ANSI T1.111, chapter 3, clause 7

TITLE: Link State Control - Expected signal units/orders

SUBTITLE: Deactivation during initial alignment

PURPOSE: To test the response to the receipt of the Stop (MML) command while in the initial alignment state (initial alignment is Not Aligned State)

PRE-TEST CONDITIONS: Link out of service

CONFIGURATION: 1

EXPECTED SIGNAL UNIT SEQUENCE:

SP B

SP A

Link

Link

1-1 SIOS <----- 1-1 SIOS
----->

:start

<----- 1-1 SIO

:wait (<T2)

:stop*

<----- 1-1 SIOS

TEST DESCRIPTION:

1. Check that alignment ceases after Stop (MML) command given.
2. The Stop (MML) command must be issued before timer T2 expires.
3. Timer T2 has a low value of 11.5 secs. with an accuracy range from 5 to 14 secs, and a high value of 23.0 secs. with an accuracy range from 16 to 30 secs.

NOTE: The stop command is a Man Machine Language (MML) command to terminate initial alignment, and is system/vendor dependent.

2.6 Deactivation During Alignment	M2-1.8	1.26 Deactivation During Alignment

PROTOCOL REFERENCE: ANSI T1.111, chapter 3, clause 7

TITLE: Link State Control - Expected signal units/orders

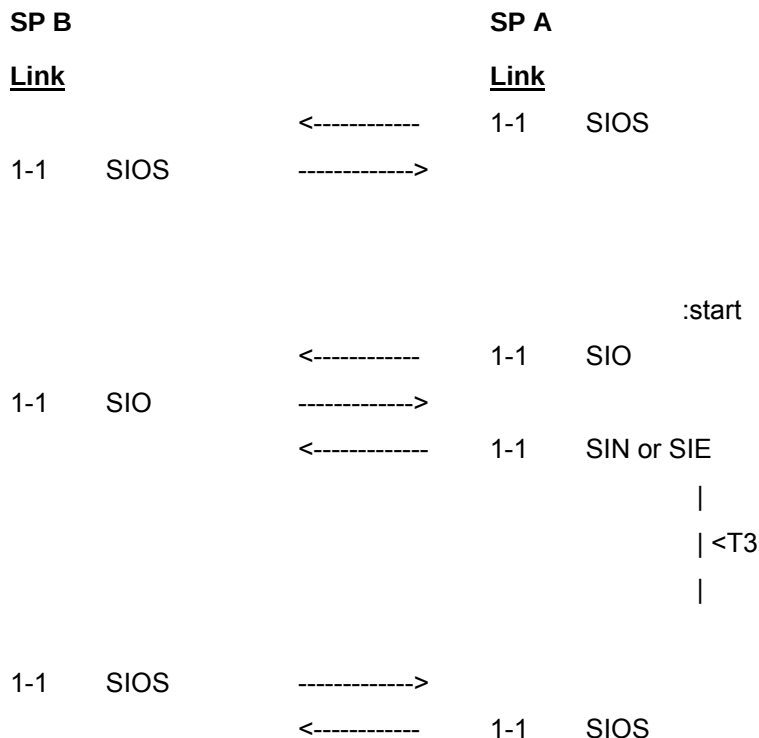
SUBTITLE: Deactivation during aligned state

PURPOSE: To test the response to the receipt of an SIOS while in the initial alignment state (initial alignment is Aligned State)

PRE-TEST CONDITIONS: Link out of service

CONFIGURATION: 1

EXPECTED SIGNAL UNIT SEQUENCE:



TEST DESCRIPTION:

1. Start normal or emergency alignment on the terminal (SP A) side.
2. After receiving SIN or SIE from the terminal being tested, the test unit (SP B) sends SIOS (before timer T3 expires).
3. The terminal shall send SIOS.

Note: Timer T3 has a nominal value of 11.5 secs., and an accuracy range from 5 to 14 secs.

NGIIF Test #:

ANSI T1-234-2000 Test #:

GR-CORE-905 Test #

2.7 SIO Received During Link In-Service	M2-1.9	1.28 SIO Received During Link In-Service

PROTOCOL REFERENCE: ANSI T1.111, chapter 3, clause 7

TITLE: Link State Control - Expected signal units/orders

SUBTITLE: SIO received during link in service

PURPOSE: To check that the link is taken out of service if SIO is received during link in-service

PRE-TEST CONDITIONS: Link in service

CONFIGURATION: 1

EXPECTED SIGNAL UNIT SEQUENCE:

SP B

SP A

Link

Link

1-1 FISU ----->
<-----

1-1 FISU

1-1 SIO ----->
<-----

1-1 SIOS

TEST DESCRIPTION:

1. The test unit (SP B) sends SIO to the terminal being tested (SP A) during link in service.
2. The terminal shall send SIOS.

NGIIF Test #:

ANSI T1-234-2000 Test #:

GR-CORE-905 Test #

2.8 SIOS Received During In-Service State	M2-1.10	1.29 SIOS Received During In-Service State

PROTOCOL REFERENCE: ANSI T1.111, chapter 3, clause 7

TITLE: Link State Control - Expected signal units/orders

SUBTITLE: SIOS received during link in service

PURPOSE: To check that the link is removed from service if SIOS is received while link is in the in-service state

PRE-TEST CONDITIONS: Link in service

CONFIGURATION: 1

EXPECTED SIGNAL UNIT SEQUENCE:

SP B			SP A	
<u>Link</u>			<u>Link</u>	
1-1	FISU	----->		
		<-----	1-1	FISU
1-1	SIOS	----->		
		<-----	1-1	SIOS

TEST DESCRIPTION:

1. The test unit (SP B) sends SIOS to the terminal being tested (SP A) during link in service.
2. The terminal shall send SIOS.

2.9 Deactivation During the Proving Period	M2-1.11	1.32 Deactivation During the Proving Period

PROTOCOL REFERENCE: ANSI T1.111, chapter 3, clause 7

TITLE: Link State Control - Expected signal units/orders

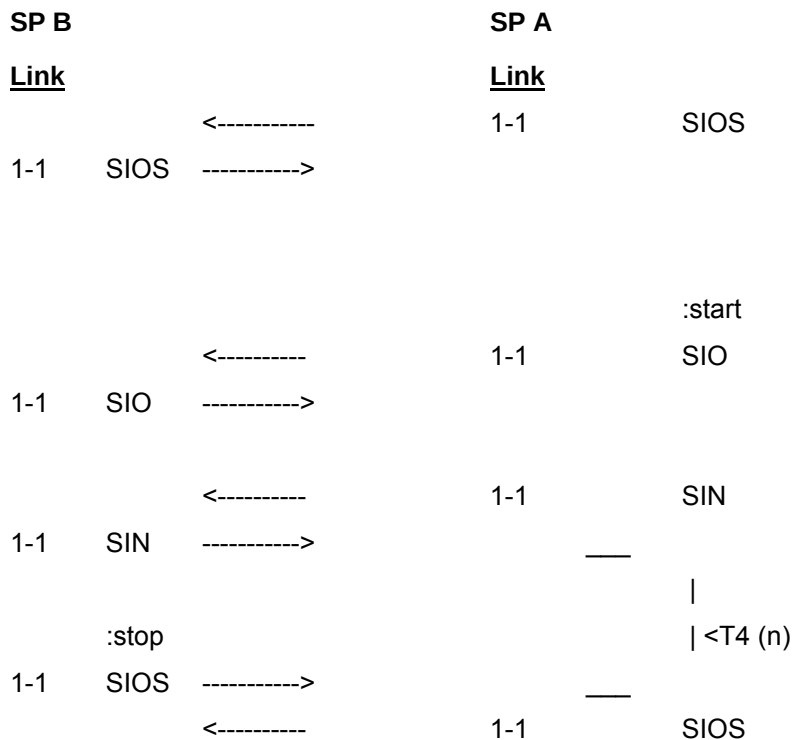
SUBTITLE: Deactivation during the proving period

PURPOSE: To test the response to the receipt of SIOS during the proving period

PRE-TEST CONDITIONS: Link out of service

CONFIGURATION: 1

EXPECTED SIGNAL UNIT SEQUENCE:



TEST DESCRIPTION:

1. Start normal alignment on the terminal side (SP A).
2. The test unit (SP B) sends SIOS (before terminal timer T4 expires) during the proving period.
3. The terminal shall send SIOS.

Note: Timer T4 (normal) has a value of 2.3 secs. with an accuracy of $\pm 10\%$.

2.10 Break Transmission Path - Link Aligned and Ready	M2-2.1	3.1 Break Transmission Path - Link Aligned and Ready

PROTOCOL REFERENCE: ANSI T1.111, chapter 3, clause 4, subclause 10.2

TITLE: Transmission failure - break Tx path

SUBTITLE: Link aligned ready

PURPOSE: To test the response to transmission failure - detected by SUERM - when in "Aligned ready" state

PRE-TEST CONDITIONS: Link out of service

CONFIGURATION: 1

EXPECTED SIGNAL UNIT SEQUENCE:

SP B			SP A	
<u>Link</u>			<u>Link</u>	
		<-----	1-1	SIOS
1-1	SIOS	----->		
				:start
		<-----	1-1	SIO
1-1	SIO	----->		
		<-----	1-1	SIN
1-1	SIN	----->		
		<-----	1-1	FISU
	:break Tx			
	(abort)	----->		
		<-----	1-1	SIOS

TEST DESCRIPTION:

1. Start normal alignment on the terminal being tested side (SP A).
2. When the link is in the Aligned Ready state, the test unit (SP B) sends continuous aborts to the terminal. Aborts are signals to simulate an open in the transmission path, e.g., signal with a bit pattern of all 1's.
3. The Signaling Unit Error Rate Monitor (SUERM) shall detect the errors, and the terminal shall send SIOS.

2.11 Corrupt FIBs	M2-2.2	3.2 Corrupt FIBs

PROTOCOL REFERENCE: ANSI T1.111, chapter 3, subclause 5.3

TITLE: Corrupt FIBs - Basic

SUBTITLE: Link aligned ready

PURPOSE: To check the response to a link failure after corruption of two FIBs - detected by reception control - while in aligned ready state

PRE-TEST CONDITIONS: Aligned ready

CONFIGURATION: 1

EXPECTED SIGNAL UNIT SEQUENCE:

SP B			SP A	
<u>Link</u>			<u>Link</u>	
		<-----	1-1	FISU
1-1	FISU corrupt FIB (FIB + FSN=7F)	----->		
1-1	FISU corrupt FIB (FIB + FSN=7F)	----->		
		<-----	1-1	SIOS

Note: "7F" is a hexadecimal number.

TEST DESCRIPTION:

1. When the link is in the Aligned Ready state, test the unit (SP B) sends two FISUs, both having inverted FIBs.
2. The terminal being tested (SP A) shall send SIOS.

2.12 Flag Insertion Within Octet Boundaries	M2-3.1	5.1 Flag Insertion Within Octet Boundaries

PROTOCOL REFERENCE: ANSI T1.111, chapter 3, subclause 4.1

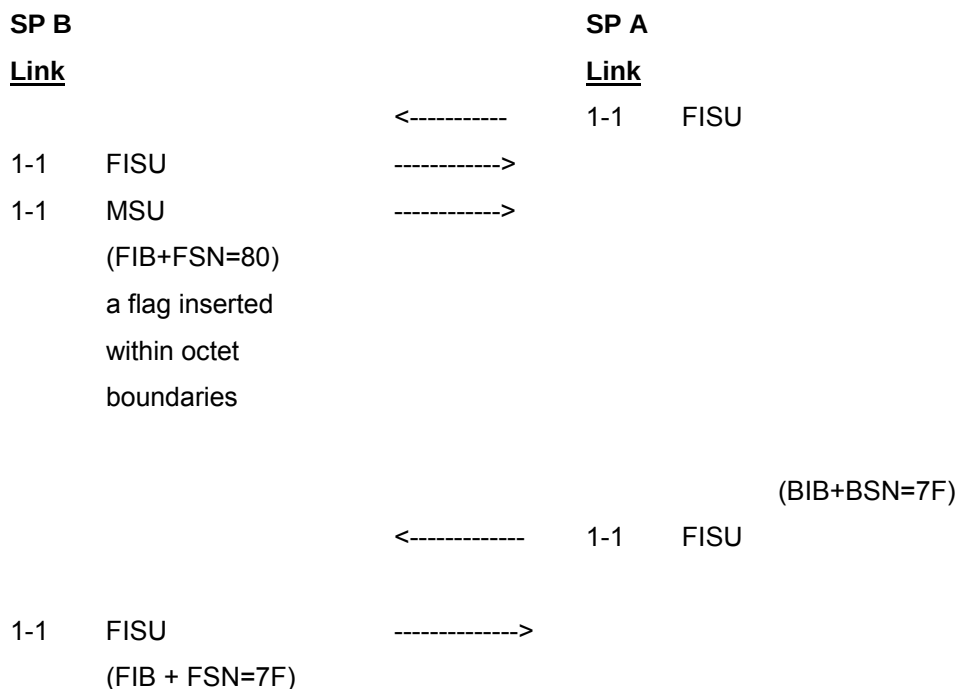
TITLE: Flag insertion within octet boundaries

PURPOSE: To test the signal unit delimitation, alignment, and error detection action on receipt of an MSU with a flag inserted within the boundaries of the signal unit

PRE-TEST CONDITIONS: Link in service

CONFIGURATION: 1

EXPECTED SIGNAL UNIT SEQUENCE:



Note: "80" and "7F" are hexadecimal numbers.

TEST DESCRIPTION:

1. The test unit (SP B) sends an MSU with a flag (Hex 7F) inserted within the octet boundaries.
2. The terminal being tested (SP A) shall discard the MSU up to the inserted flag, and the remaining portion of the original MSU beyond the flag insertion.
3. The terminal shall respond with a negative acknowledgment.

NGIIF Test #:

ANSI T1-234-2000 Test #:

GR-CORE-905 Test #

**2.13 Signal Unit Error
Rate Monitor**

M2-4.1

**6.1 Signal Unit Error Rate Monitor
(Below Threshold)**

PROTOCOL REFERENCE: ANSI T1.111, chapter 3, subclause 10.2

TITLE: Signal Unit Error Rate Monitor check

SUBTITLE: Error rate below threshold 1/256 - Link remains in service

PURPOSE: To check the SUERM at a link error rate below threshold 1/256

PRE-TEST CONDITIONS: Link in service

CONFIGURATION: 1

EXPECTED SIGNAL UNIT SEQUENCE:

SP B

SP A

Link

Link

		<-----	1-1	FISU
1-1	FISU	----->		
1-1	FISU	----->		
	(error rate			
	below 1/256)			

TEST DESCRIPTION:

1. The test unit (SP B) sends good FISUs with a single corrupt FISU (e.g., invalid cyclic redundancy check [CRC]) inserted every 300 ms.
2. The test unit continues to send a single corrupt FISU every 300 ms for several minutes.
3. The link shall remain in service.

2.14 Signal Unit Error Rate Monitor	M2-4.2	6.2 Signal Unit Error Rate Monitor (Above Threshold)

PROTOCOL REFERENCE: ANSI T1.111, chapter 3, subclause 10.2

TITLE: SUERM check

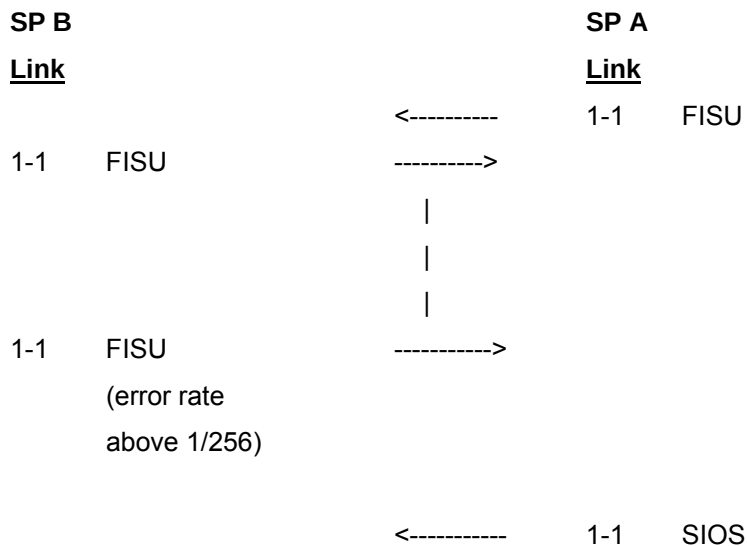
SUBTITLE: Error rate above threshold 1/256 - Link out of service

PURPOSE: To check the SUERM at a link error rate above threshold 1/256

PRE-TEST CONDITIONS: Link in service

CONFIGURATION: 1

EXPECTED SIGNAL UNIT SEQUENCE:



TEST DESCRIPTION:

1. The test unit (SP B) sends good FISUs with a single corrupt FISU (e.g., invalid cyclic redundancy check [CRC]) inserted every 200 ms.
2. The test unit continues to send a single corrupt FISU every 200 ms for several minutes.
3. The error rate threshold shall be exceeded, and the terminal being tested (SP A) shall send SIOS in the order of minutes.

NGIIF Test #:

ANSI T1-234-2000 Test #:

GR-CORE-905 Test #

2.15 Consecutive Corrupt Signal Units	M2-4.3	6.3 Consecutive Corrupt Signal Units

PROTOCOL REFERENCE: ANSI T1.111, chapter 3, subclause 10.2

TITLE: SUERM check

SUBTITLE: Consecutive corrupted SUs

PURPOSE: To test the SUERM on consecutive corrupted signal units

PRE-TEST CONDITIONS: Link in service

CONFIGURATION: 1

EXPECTED SIGNAL UNIT SEQUENCE:

SP B

Link

1-1 FISU

<-----

----->

|

|

|

1-1 FISU
(64 corrupt
FISUs)

----->

<-----

SP A

Link

1-1 FISU

1-1 SIOS

TEST DESCRIPTION:

1. The test unit (SP B) sends continuously corrupt FISUs (e.g., invalid CRC)
2. After receiving about 64 consecutive corrupt FISUs, the terminal being tested (SP A) shall send SIOS in the order of hundreds of milliseconds.

NGIIF Test #:

ANSI T1-234-2000 Test #:

GR-CORE-905 Test #

2.16 Alignment Error Rate Monitor	M2-5.1	7.1 Alignment Error Rate Monitor (Below Threshold)

PROTOCOL REFERENCE: ANSI T1.111, chapter 3, subclause 10.3

TITLE: Alignment Error Rate Monitor check

SUBTITLE: Error rate below the normal threshold

PURPOSE: To test the AERM at error rates below the normal threshold

PRE-TEST CONDITIONS: Link out of service

CONFIGURATION: 1

EXPECTED SIGNAL UNIT SEQUENCE:

SP B		SP A	
<u>Link</u>		<u>Link</u>	
	<-----	1-1	SIOS
1-1	SIOS ----->		
			:start
	<-----	1-1	SIO
1-1	SIO ----->		
	<-----	1-1	SIN
1-1	SIN ----->		
1-1	4 corrupt FISUs ----->		
	<-----	1-1	SIN
1-1	SIN ----->		
1-1	4 corrupt FISUs ----->		
	<-----	1-1	SIN
1-1	SIN ----->		
1-1	4 corrupt FISUs ----->		
	<-----	1-1	SIN
1-1	SIN ----->		
1-1	4 corrupt FISUs ----->		
	<-----	1-1	SIN
1-1	SIN ----->		
			T4 (n)
1-1	good FISUs ----->		
	<-----	1-1	FISU

TEST DESCRIPTION:

1. Start normal alignment on the terminal being tested side (SP A).
2. During the T4 (normal) proving period, the test unit (SP B) sends good FISUs with four corrupt FISUs (e.g., CRC error) inserted every 2 secs.
3. The test unit will repeat this pattern until a total of 16 corrupt FISUs have been sent. The test unit will send good FISUs thereafter.
4. The link shall be aligned (on the fifth cycle).

Note: Timer T4 (normal) has a value of 2.3 secs. with an accuracy of + 10%.

NGIIF Test #:

ANSI T1-234-2000 Test #:

GR-CORE-905 Test #

***2.17 Alignment Error
Rate Monitor***

M2-5.2

7.3 Alignment Error Rate Monitor
(Above Threshold)

PROTOCOL REFERENCE: ANSI T1.111, chapter 3, subclause 10.3

TITLE: Alignment Error Rate Monitor check

SUBTITLE: Error rate above the normal threshold

PURPOSE: To test the AERM at error rates above the normal threshold over five proving periods

PRE-TEST CONDITIONS: Link out of service

CONFIGURATION: 1

EXPECTED SIGNAL UNIT SEQUENCE:

SP B

Link

SP A

Link

1-1 SIOS <----- 1-1 SIOS
----->

: start

1-1 SIO <----- 1-1 SIO
----->

1-1 SIN <----- 1-1 SIN
----->

1-1 4 corrupt FISUs ----->
<----- 1-1 SIN

1-1 SIN ----->
1-1 4 corrupt FISUs ----->

<----- 1-1 SIN
1-1 SIN ----->

1-1 4 corrupt FISUs ----->
<----- 1-1 SIN

1-1 SIN ----->
1-1 4 corrupt FISUs ----->

<----- 1-1 SIN
1-1 SIN ----->

1-1 4 corrupt FISUs ----->
<----- 1-1 SIOS

TEST DESCRIPTION:

1. Start normal alignment on the terminal being tested side (SP A).
2. During the T4 (normal) proving period, the test unit (SP B) sends good FISUs with four corrupt FISUs (e.g., CRC error) inserted every 2 secs. This pattern will be repeated.
3. The terminal shall send SIOS on the fifth cycle.

Note: Timer T4 (normal) has a value of 2.3 secs. with an accuracy of + 10%.

NGIIF Test #:

ANSI T1-234-2000 Test #:

GR-CORE-905 Test #

2.18 Negative Acknowledgment	M2-6.2	8.2 Negative Acknowledgment

PROTOCOL REFERENCE: ANSI T1.111, chapter 3, subclause 5.3

TITLE: Negative acknowledgment of a MSU

PURPOSE: To test the response to a negatively acknowledged MSU

PRE-TEST CONDITIONS: Link in service

CONFIGURATION: 1

EXPECTED SIGNAL UNIT SEQUENCE:

SP B			SP A
<u>Link</u>			<u>Link</u>
		<-----	1-1 FISU
1-1 FISU		----->	
		<-----	1-1 MSU (FIB+FSN=80)
1-1 FISU		----->	
(BIB+BSN=7F)			
		<-----	1-1 MSU (FIB + FSN=00)

Note: "7F", "80" and "00" are hexadecimal numbers.

TEST DESCRIPTION:

1. The terminal being tested (SP A) sends a MSU to the test unit (SP B).
2. The test unit sends a FISU with an inverted FIB and BSN one less than the last received FSN indicating a request for retransmission.
3. The terminal shall respond by retransmitting the last MSU with the BIB inverted.

2.19 Retransmission Buffer Full	M2-6.3-A (see Note 2)	

PROTOCOL REFERENCE: T1.111, chapter 3, clause 5, subclause 5.2, subclause 5.3

TITLE: Retransmission buffer full

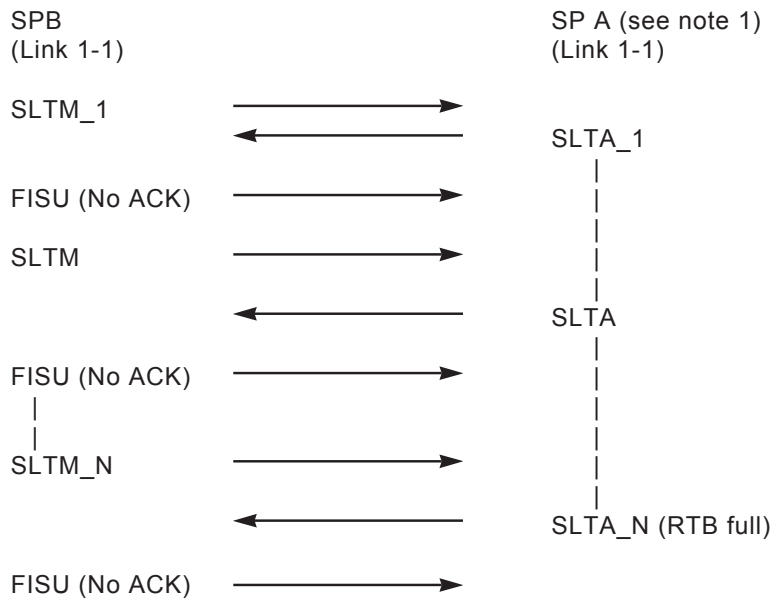
PURPOSE: To test the proper operation of the System Under Test (SUT) when its Retransmission Buffer (RTB) is full.

PRETEST CONDITIONS: Link 1-1 is in service

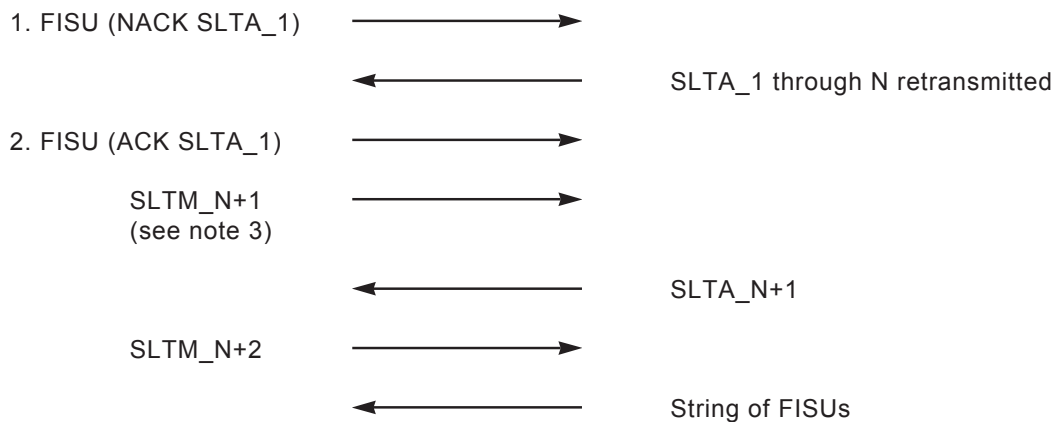
CONFIGURATION: 1

EXPECTED SIGNAL UNIT SEQUENCE:

SP B		SP A
(Link 1-1)		(Link 1-1)
SLTM_1	----->	SLTA_1
	<-----	
FISU (No ACK)	----->	
SLTM	----->	
	<-----	SLTA
FISU (No ACK)	----->	
SLTM_N	----->	
	<-----	SLTA_N (RTB full)
FISU (No ACK)	----->	
Choice of Option 1 or 2		
1. FISU (No ACK SLTA_1)	----->	
	<-----	SLTA_1 through N retransmitted
2. FISU (ACK SLTA_1)	----->	
SLTM_N+1	----->	
(see note 3)		
	<-----	SLTA_N+1
SLTM_N+2	----->	
	<-----	String of FISUs



Choice of Option 1 or 2



TEST DESCRIPTION:

1. The test unit (SP B) sends SLTMs at a rate of 100 per second, and the SUT (SP A) responds with SLTAs at this rate. SP B does not acknowledge any of the SLTAs received.
2. When continuous FISUs are received by SP B in the place of the SLTAs, this indicates that the RTB in SP A is full.

Option 1:

1. Once SP B detects that no more SLTAs are received, then SP B sends a FISU to NACK an SLTA_I message, $I=1, \dots, N$ in the SPAs RTB.
2. SPB should check that SP A retransmits all of the SLTAs, i.e. SLTA_I, $I= 1, \dots, N$, in its RTB.

Option 2:

1. Once SP B detects that no more SLTAs are received, then SP B sends a FISU to SP A, positively acknowledging one message, i.e. SLTA_1.
2. SP B sends an SLTM (N+1) to SP A.
3. SP A sends an SLTA (N+1) to SP B acknowledging SLTM (N+1).
4. SP B sends an SLTM (N+2) to SP A.
5. SP A will send a string of FISUs to SP B.

NOTES:

1. Consideration must be given to SP A's level 2 timer T7 setting (0.5 - 2 sec) and SP A's congestion mechanism.
2. This test is an alternative to M2-6.3B. The choice of whether to use M2-6.3A or M2-6.3B test is predicated on the capability of the test equipment
3. The rate of SLTMs at 100 per second may need to be adjusted so that the FISU can be sent before SLTM_N+1.

2.20 Erroneous FIB	M2-6.4	8.4 Erroneous Fib

PROTOCOL REFERENCE: ANSI T1.111, chapter 3, subclause 5.2

TITLE: Single MSU with erroneous FIB

PURPOSE: To ensure correct performance when a MSU with erroneous FIB is received.

PRE-TEST CONDITIONS: Link in service

CONFIGURATION: 1

EXPECTED SIGNAL UNIT SEQUENCE:

SP B	SP A
<u>Link</u>	<u>Link</u>
	<-----1-1 FISU (BIB+BSN=7F)
1-1 FISU (FIB+FSN=7F)	----->
1-1 MSU (FIB+FSN=80)	----->
	<-----1-1 FISU (BIB+BSN=7F)
1-1 FISU (FIB+FSN=00)	----->
	<-----1-1 FISU (BIB+BSN=FF)
1-1 MSU (FIB+FSN=80)	----->
	<-----1-1 FISU (BIB+BSN=80)

Note: "7F", "80", "00", "FF" are hexadecimal numbers.

TEST DESCRIPTION:

1. The test unit (SP B) sends a MSU with an erroneous FIB.
2. The terminal being tested (SP A) shall discard the MSU received, and the next received FISU or MSU. A negative acknowledgment shall be returned to the test unit.
3. The test unit retransmits the MSU. A positive acknowledgment shall be returned by the terminal.

2.21 Erroneous Retransmission - Multiple FISU	M2-6.5	82.7 Erroneous Retransmission Multiple FISU

PROTOCOL REFERENCE: ANSI T1.111, chapter 3, subclause 5.3

TITLE: Erroneous retransmission - Multiple FISUs

PURPOSE: To test reception control response to retransmission of multiple FISUs

PRE-TEST CONDITIONS: Link in service

CONFIGURATION: 1

EXPECTED SIGNAL UNIT SEQUENCE:

SP B			SP A	
<u>Link</u>			<u>Link</u>	
		<-----	1-1	FISU
1-1	FISU	----->		
	(FIB+FSN=FF)			
1-1	FISU	----->		
	(FIB+FSN=7F)			
1-1	FISU	----->		
	(FIB+FSN=FF)			
1-1	FISU	----->		
	(FIB+FSN=7F)			
		<-----	1-1	SIOS

Note: "FF" and "7F" are hexadecimal numbers.

TEST DESCRIPTION:

1. The test unit (SP B) sends FISUs with inverted FIB every other signal unit.
2. The terminal being tested (SP A) shall send SIOS after receiving the fourth FISU of the above pattern.

2.22 Abnormal Backward Sequence Number	M2-6.6	8.10 Abnormal Backward Sequence Number (Single MSU)

PROTOCOL REFERENCE: ANSI T1.111, chapter 3, subclause 5.3

TITLE: Abnormal Backward Sequence Number - Single MSU

PURPOSE: To test the response to an abnormal BSN

PRE-TEST CONDITIONS: Link in service

CONFIGURATION: 1

EXPECTED SIGNAL UNIT SEQUENCE:

SP B			SP A	
<u>Link</u>			<u>Link</u>	
		<-----	1-1	FISU
1-1	FISU	----->		
	(FIB+FSN=FF)			
	(BIB+BSN=FF)			
1-1	MSU	----->		
	(FIB+FSN=80)			
	(BIB+BSN=BF)			
1-1	FISU	----->		
	(FIB+BSN=80)			
	(BIB+BSN=FF)			
1-1	FISU	----->		
	(FIB+FSN=80)			
	(BIB+BSN=FF)			
		<-----	1-1	FISU
				(BIB+BSN=7F)
1-1	MSU	----->		
	(FIB+FSN=00)			
	(BIB+BSN=FF)			
		<-----	1-1	FISU
				(BIB+BSN=00)

Note: "FF", "80", "BF", "00" and "7F" are hexadecimal numbers.

TEST DESCRIPTION:

1. The test unit (SP B) sends a MSU with an invalid BSN (one that has already been removed from the retransmission buffer), followed by FISUs with correct BSN.
2. The terminal being tested (SP A) responds with a negative acknowledgment.
3. The test unit retransmits the MSU with a correct BSN.
4. The terminal shall return a positive acknowledgment.

2.23 Abnormal Backward Sequence Number	M2-6.7	8.11 Abnormal Backward Sequence Number (Multiple FISUs)

PROTOCOL REFERENCE: ANSI T1.111, chapter 3, subclause 5.3

TITLE: Abnormal BSN - two consecutive FISUs

PURPOSE: To test the response to abnormal BSNs in two consecutive FISUs

PRE-TEST CONDITIONS: Link in service

CONFIGURATION: 1

EXPECTED SIGNAL UNIT SEQUENCE:

SP B		SP A
<u>Link</u>		<u>Link</u>
	<-----	1-1 FISU
1-1 FISU	----->	
(BIB+BSN=FF)		
1-1 FISU	----->	
(BIB+BSN=BF)		
1-1 FISU	----->	
(BIB+BSN=BF)		
1-1 FISU	----->	
(BIB+BSN=FF)		
	<-----	1-1 SIOS

Note: "FF" and "BF" are hexadecimal numbers.

TEST DESCRIPTION:

1. The test unit (SP B) sends two consecutive FISUs with invalid BSNs (those that have already been removed from the retransmission buffer).
2. The terminal being tested (SP A) shall send SIOS.

2.24 Delay of Acknowledgment	M2-6.8	8.12 Delay of Acknowledgment

PROTOCOL REFERENCE: ANSI T1.111, chapter 3, subclause 5.3

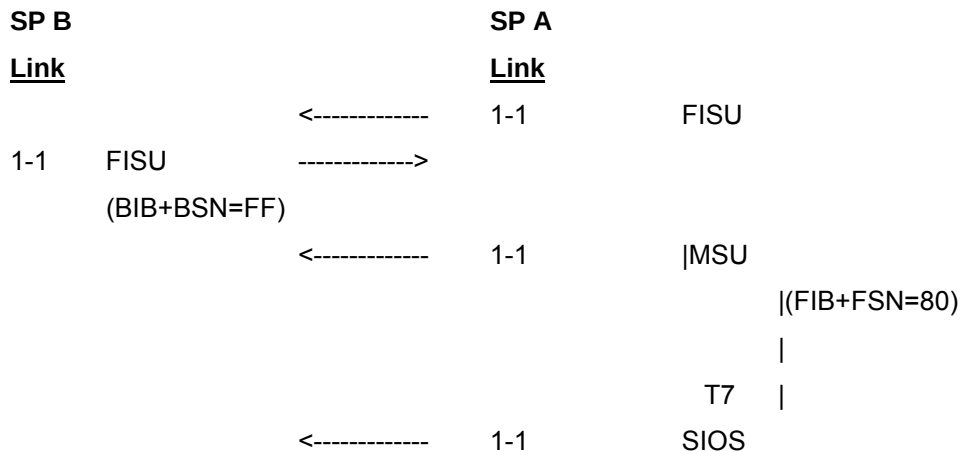
TITLE: Excessive delay of acknowledgment

PURPOSE: To test the transmission control response to the expiration of EDA (Excessive Delay of Acknowledgment) timer T7

PRE-TEST CONDITIONS: Link in service

CONFIGURATION: 1

EXPECTED SIGNAL UNIT SEQUENCE:



Note: "FF" and "80" are hexadecimal numbers.

TEST DESCRIPTION:

1. The terminal being tested (SP A) sends a MSU.
2. The test unit (SP B) does not acknowledge the receipt of the MSU.
3. After Timer T7 expires, the terminal shall send SIOS.

Note: Timer T7 has a value ranging from 0.5 to 2.0 secs.

2.25 Link Activation - Multiple Links	M3-1.3	1.3 Link Activation Multiple Links

PROTOCOL REFERENCE: ANSI T1.111, chapter 4, subclause 12.2.4.1

TITLE: Signaling link management

SUBTITLE: Signaling linkset activation

PURPOSE: To put into service a signaling linkset

PRE-TEST CONDITIONS: Signaling links out-of-service

CONFIGURATION: A

MESSAGE SEQUENCE:

SP A	SP B
<u>Link</u>	<u>Link</u>
1-1 :Activate	1-1 :Activate
1-2 :Activate	1-2 :Activate
1-3 :Activate	1-3 :Activate
1-4 :Activate	1-4 :Activate
:start traffic	
1-1 TRAFFIC ----->	1-1 TRAFFIC
<-----	
1-2 TRAFFIC ----->	1-2 TRAFFIC
<-----	
1-3 TRAFFIC ----->	1-3 TRAFFIC
<-----	
1-4 TRAFFIC ----->	1-14 TRAFFIC
<-----	
:Wait	
:Stop traffic	

Note: Changeover and/or changeback should occur during signaling linkset activation.

TEST DESCRIPTION:

1. Activate the signaling links in the linkset.
2. Check that the signaling links become available and start traffic between A and B.
3. Check the reception and sending of variable length messages on the activated linkset from/to the SP at the other end of this linkset.

4. Check that all messages are correctly received (no loss of messages, no duplication, and no missequencing).

Note: The term "traffic" is the MSUs, e.g., SLTM/SLTA, sent or received by the SP.

NGIIF Test #:

ANSI T1-234-2000 Test #:

GR-CORE-905 Test #

***2.26 Discrimination of
Invalid Point Code***

M3-2.1

2.1 Discrimination of Invalid Point
Code

PROTOCOL REFERENCE: ANSI T1.111, chapter 4, subclause 2.4

TITLE: Discrimination of Invalid Point Code

SUBTITLE: Signaling message handling

PURPOSE: Test the ability to discard and/or respond to MSUs with invalid Originating Point Codes (OPC)/DPC/Signaling Link Code

PRE-TEST CONDITIONS: Signaling linkset activated

CONFIGURATION: A

MESSAGE SEQUENCE:

SP A

SP B

Link

Link

<-----

1-1

Multiple SLTMs

(Invalid OPC/DPC/SLC)

Messages Discarded

TEST DESCRIPTION:

1. The test unit (SP B) sends an MSU (SLTM) with an invalid OPC/DPC/SLC.
2. The terminal being tested (SP A) shall discard the MSU (SLTM) received. (An SLTA shall not be sent in response.)

2.27 Load Distribution	M3-3.1	2.4.1 Load Distribution

PROTOCOL REFERENCE: ANSI T1.111, chapter 4, subclause 2.3

TITLE: Signaling message handling

SUBTITLE: Load sharing within a linkset - all links available

PURPOSE: To check the load sharing within a linkset with all links available

PRE-TEST CONDITIONS: Signaling linkset activated

CONFIGURATION: A

MESSAGE SEQUENCE:

SP A		SP B	
<u>Link</u>		<u>Link</u>	
:start traffic			
1-1	TRAFFIC	----->	
		<-----	1-1 TRAFFIC
1-2	TRAFFIC	----->	
		<-----	1-2 TRAFFIC
1-3	TRAFFIC	----->	
		<-----	1-3 TRAFFIC
1-4	TRAFFIC	----->	
		<-----	1-4 TRAFFIC
:Wait			
:Stop traffic			

TEST DESCRIPTION:

1. Start traffic between SP A and SP B.
2. Stop traffic, check that the messages have been transmitted on the correct link in accordance with the SLS field.
3. Check that there was no loss of messages, no duplication and no missequencing.

2.28 Load Sharing Between Link-Sets - Between Two Link-Sets	M3-3.2	2.5.1 Load Sharing between Link Sets of a Combined Link Set

PROTOCOL REFERENCE: ANSI T1.111, chapter 4, subclause 2.3

TITLE: Signaling message handling

SUBTITLE: Load sharing between linksets - between two linksets

PURPOSE: To check the load sharing between two linksets under normal conditions

PRE-TEST CONDITIONS: All linksets and routes available

CONFIGURATION: B

MESSAGE SEQUENCE:

SP A	SP B'	SP B	SP C
<u>Link</u>	<u>Link</u>	<u>Link</u>	<u>Link</u>

:start traffic

```

1-1 TRAFFIC -----> 4-1 ----->
                    <----- 1-1 <----- 4-1 TRAFFIC
1-2 TRAFFIC -----> 4-1 ----->
                    <----- 1-2 <----- 4-1 TRAFFIC
    
```

2-1 TRAFFIC ---> 5-1 ----->

2-2 TRAFFIC ---> 5-1 ----->

:Wait

:Stop traffic

TEST DESCRIPTION:

1. Start traffic between SP A and SP C for all SLS.
2. Stop the traffic and check that the messages have been transmitted on the correct linksets in accordance with the SLS and DPC.
3. Check that there was no loss of messages, no duplication and no missequencing.

2.29 Changeover Initiated at One Side of a Link-Set	M3-4.1	3.1 Changeover initiated at one side of a linkset

PROTOCOL REFERENCE: ANSI T1.111, chapter 4, subclause 2.3

TITLE: Changeover

SUBTITLE: Changeover initiated at one side of a linkset (COO <--> COA)

PURPOSE: To check that the changeover completes within the allotted time frame

PRE-TEST CONDITIONS: Linkset with two available links

CONFIGURATION: A

MESSAGE SEQUENCE:

<u>SP A</u>		<u>SP B</u>
<u>Link</u>		<u>Link</u>
1-1 TRAFFIC	----->	
	<-----	1-1 TRAFFIC
1-2 TRAFFIC	----->	
	<-----	1-2 TRAFFIC
1-1	:Deactivate (MML command or failure)	
1-2 COO, SLC 1-1	----->	
	<-----	1-2 COA, SLC 1-1
1-2 TRAFFIC (from 1-1)	----->	
	<-----	1-2 TRAFFIC (From 1-1)
:Wait		
:Stop traffic		

TEST DESCRIPTION:

1. Start traffic from A to B on all the links.
2. Deactivate link 1-1, check that a COO is sent (from A) for 1-1 on 1-2 and SP b responds with a COA within T2.
3. Check that the time between the deactivation and the sending of the COO is inside the specified value (See T1.111, chapter 6, subclause 5.5.4).
4. Check that the traffic from link 1-1 is changed over to 1-2 and check that the traffic normally carried by 1-1 is passed over to 1-2.
5. Stop traffic and check it has been received correctly (no lost messages, no duplication and no missequencing).
6. Repeat the test by sending COO from B (instead of A). In addition, check that the time between the reception of the COO and the sending of the COA is inside the specified value.(See T1.111, chapter 6, subclause 5.5.4.)

Note: Timer T2 has a value ranging from 0.7 to 2.0 secs.

2.30 Changeover to an alternate linkset	M3-4.2	3.16 Changeover to an alternate linkset

PROTOCOL REFERENCE: ANSI T1.111, chapter 4, clause 5

TITLE: Changeover

SUBTITLE: Changeover to an alternate linkset

PURPOSE: To check that the system performs changeover to an alternate route when the last link of a linkset becomes unavailable

PRE-TEST CONDITIONS: Link 1-1 unavailable

CONFIGURATION: B

MESSAGE SEQUENCE:

SP A	SP B'	SP B	SP C
<u>Link</u>	<u>Link</u>	<u>Link</u>	<u>Link</u>
:start traffic			
1-2 TRAFFIC	-----> 4-1	----->	
	<----- 1-2	<----- 4-1	TRAFFIC
2-1,2 TRAFFIC	--> 5-1----->		
	<-- 2-1,2 <-----	5-1	TRAFFIC
1-2 :Deactivate (MML command or failure)			
2-X COO,	----> 3-1 ---->		
SLC 1-2			
	<-----2-X <-----	3-1 COA, SLC 1-2	
2-1,2 TRAFFIC	---->5-1----->		
(from 1-2)			
	<--- 2-1,2<-----	5-1	TRAFFIC
:Wait			
:Stop traffic			

TEST DESCRIPTION:

1. Start traffic from A to C.
2. Deactivate link 1-2 and check that a COO (for 1-2) is sent from A to B via B' within T2.
3. Check that the COO and COA messages contain the proper FSNs of the last MSU accepted.
4. Check that the traffic will be routed to the alternative links 2-1 and 2-2.
5. Check that, for each SLS, there were no lost messages, no duplication and no missequencing.

Note: Timer T2 has a value ranging from 0.7 to 2.0 secs.

2.31 Changeback Within a Link-Set	M3-5.1	4.1 Changeback within a Link Set Containing Multiple Links

PROTOCOL REFERENCE: ANSI T1.111, chapter 4, clause 6

TITLE: Changeback

SUBTITLE: Changeback within a linkset

PURPOSE: To check that the changeback procedure is correctly performed on restoration of a link in a linkset

PRE-TEST CONDITIONS: Linkset with one available link and one unavailable link

CONFIGURATION: A

MESSAGE SEQUENCE:

SP A		SP B
<u>Link</u>		<u>Link</u>
:Start traffic		
1-2 TRAFFIC	----->	
	<-----	1-2 TRAFFIC
1-1 :Activate		
1-2 CBD, SLC 1-1	----->	
	<-----	1-X CBA, SLC 1-1
TRAFFIC(from 1-2)	----->	
	<-----	1-2 CBD, SLC 1-1
1-X CBA, SLC 1-1	----->	
	<-----	1-1 TRAFFIC (from 1-2)
1-2 TRAFFIC	----->	
	<-----	1-2 TRAFFIC
:Wait		
:Stop traffic		

TEST DESCRIPTION:

1. Start traffic from A to B on link 1-2
2. Activate the link 1-1 and check that it enters the correct in service state.
3. Check that a CBD for SLC 1-1 is received and that traffic for link 1-1 is switched back after a CBA is sent.
4. Stop traffic and check that it has been received correctly, no lost messages, no duplication and no missequencing.

2.32 Changeback from another Link-Set	M3-5.2	4.8 Changeback from another linkset

PROTOCOL REFERENCE: ANSI T1.111, chapter 4, clause 6

TITLE: Changeback

SUBTITLE: Changeback from another linkset

PURPOSE: To check the changeback procedure when it is performed from another linkset

PRE-TEST CONDITIONS: Linkset 1 is unavailable

CONFIGURATION: B

MESSAGE SEQUENCE:

	SP A	SP B'	SP B	SP C
	<u>Link</u>	<u>Link</u>	<u>Link</u>	<u>Link</u>
:Start traffic				
	2-1,2	TRAFFIC-->	5-1----->	
			<-----2-1,2<-----	5-1 TRAFFIC
1-2	:Activate			
2-1,2	CBD, -----	3-1----->		
	SLC 1-2			
		<-----1-2	CBA, SLC 1-2	
			CHANGEBACK	
2-1,2	TRAFFIC----	5-1----->		
			<-----2-1,2<-----	5-1 TRAFFIC
1-2	TRAFFIC-----	4-1 ----->		
	(from 2-1, 2)			
		<-----1-2<-----	4-1 TRAFFIC	
:Wait				
:Stop traffic				

Note: After activation of link 1-2, CBDs are sent from A to B via B' and acknowledged by B.

TEST DESCRIPTION:

1. Start traffic from A to C.
2. Activate link 1-2 and check that CBDs are received and that CBAs are sent before T4 expires in A.
3. Check that the traffic is changed back on linkset 1 accordance with the load sharing rules in A.
4. Stop traffic and check that there were no lost messages, no duplication and no missequencing.

Note: Time T4 has a value ranging from 0.5 to 1.2 secs.

2.33 Inhibit Available Link	M3-6.1	7.1.1 Inhibit an available link

PROTOCOL REFERENCE: ANSI T1.111, chapter 4, clause 10

TITLE: Management inhibiting

SUBTITLE: Inhibition of an available link

PURPOSE: To check for the correct response when link inhibition is requested for an available link

PRE-TEST CONDITIONS: Linkset with two available links

CONFIGURATION: A

MESSAGE SEQUENCE:

SP A			SP B
<u>Link</u>			<u>Link</u>
:Start traffic			
1-1 TRAFFIC	----->		
	<-----	1-1 TRAFFIC	
1-2 TRAFFIC	----->		
	<-----	1-2 TRAFFIC	
1-1 :Request inhibition			
1-X LIN, SLC 1-1	----->		
	<-----	1-X LIA, SLC 1-1	
CHANGEOVER	(see note)		
1-2 TRAFFIC	----->		
(from 1-1)			
	<-----	1-2 TRAFFIC	
		(from 1-1)	

:Wait

:Stop traffic

Note: A changeover is performed after the inhibition of link 1-1 but it is not described in this test, which checks only the inhibition procedure.

TEST DESCRIPTION:

1. Start traffic from A to B on links 1-1 and 1-2.
2. Initiate inhibition of link 1-1 and check that LIN is received and an LIA is received in A within T14.
3. Check that the traffic normally carried by link 1-1 is transferred to link 1-2.

Note: Timer T14 has a value ranging from 2.0 to 3.0 secs.

2.34 Inhibit Available Link	M3-6.1	7.1.1 Inhibit an available link

PROTOCOL REFERENCE: ANSI T1.111, chapter 4, clause 10

TITLE: Management inhibiting

SUBTITLE: Inhibition of an available link

PURPOSE: To check for the correct response when link inhibition is requested for an available link

PRE-TEST CONDITIONS: Linkset with two available links

CONFIGURATION: A

MESSAGE SEQUENCE:

SP A			SP B
<u>Link</u>			<u>Link</u>
:Start traffic			
1-1 TRAFFIC	----->		
	<-----	1-1 TRAFFIC	
1-2 TRAFFIC	----->		
	<-----	1-2 TRAFFIC	
1-1 :Request inhibition			
1-X LIN, SLC 1-1	----->		
	<-----	1-X LIA, SLC 1-1	
CHANGEOVER	(see note)		
1-2 TRAFFIC	----->		
(from 1-1)			
	<-----	1-2 TRAFFIC	
		(from 1-1)	
:Wait			
:Stop traffic			

Note: A changeover is performed after the inhibition of link 1-1 but it is not described in this test, which checks only the inhibition procedure.

TEST DESCRIPTION:

1. Start traffic from A to B on links 1-1 and 1-2.
2. Initiate inhibition of link 1-1 and check that LIN is received and an LIA is received in A within T14.
3. Check that the traffic normally carried by link 1-1 is transferred to link 1-2.

Note: Timer T14 has a value ranging from 2.0 to 3.0 secs.

2.35 Inhibit Unavailable Link	M3-6.2	7.1.2 Inhibit Unavailable Link

PROTOCOL REFERENCE: ANSI T1.111, chapter 4, clause 10

TITLE: Management inhibiting

SUBTITLE: Inhibition of an unavailable link

PURPOSE: To check for the correct response when link inhibition is requested for an unavailable link

PRE-TEST CONDITIONS: Linkset with one available link and one unavailable link

CONFIGURATION: A

MESSAGE SEQUENCE:

SP A		SP B
<u>Link</u>		<u>Link</u>
:Start traffic		
1-1 TRAFFIC	----->	
	<-----	1-1 TRAFFIC
1-2 :Request inhibition		
1-1 LIN, SLC 1-2	----->	
	<-----	1-1 LIA, SLC 1-2
1-2 :Activate		
1-1 TRAFFIC	----->	
	<-----	1-1 TRAFFIC
:Wait		
:Stop traffic		

TEST DESCRIPTION:

1. Start traffic from A to B on link 1-1.
2. Request inhibition of link 1-2 which is unavailable. Check the reception of LIN at B and send LIA in response within T14.
3. Check that the inhibition was performed.
4. Activate link 1-2 and check that it stays in the inhibited state.
5. Stop traffic and check that it was not disturbed.

Note: Timer T14 has a value ranging from 2.0 to 3.0 secs.

2.36 Link Forced Uninhibit	M3-6.9	7.10 Link Forced Uninhibit

PROTOCOL REFERENCE: ANSI T1.111, chapter 4, clause 10

TITLE: Management inhibiting

SUBTITLE: Forced uninhibition of a link - sending of an LFU (Link Force Uninhibit)

PURPOSE: To check forced uninhibition procedure when the last available link in a linkset goes out-of-service.

PRE-TEST CONDITIONS: Link 1-1 available, link 1-2 inhibited by B

CONFIGURATION: A

MESSAGE SEQUENCE:

SP A	SP B
<u>Link</u>	<u>Link</u>
:Start traffic	
1-1 TRAFFIC	----->
	<----- 1-1 TRAFFIC
1-1 :Deactivate (failure)	
1-2 LFU, SLC 1-2	----->
	<----- 1-2 LUN, SLC 1-2
	CHANGEBACK (See note)
1-2 TRAFFIC	----->
	<----- 1-2 TRAFFIC

:Wait

:Stop traffic

Note: When link 1-2 becomes available, changeback should take place, but it is not described here to simplify the test description.

TEST DESCRIPTION:

1. Start traffic from A to B on link 1-1.
2. Deactivate link 1-1 and check the reception of an LFU at B on link 1-2. B responds with an LUN. Check that T13 is stopped and that an LUA is received at B.
3. Check that uninhibition is performed and that the traffic is carried on link 1-2.
4. Stop traffic, some messages have been lost.

Note: Timer T13 has a value ranging from 0.8 to 1.5 secs.

2.37 Management Inhibiting Test - Normal Procedure	M3-6.10	7.17.1 Management Inhibiting

PROTOCOL REFERENCE: ANSI T1.111, chapter 4, clause 10

TITLE: Management inhibiting

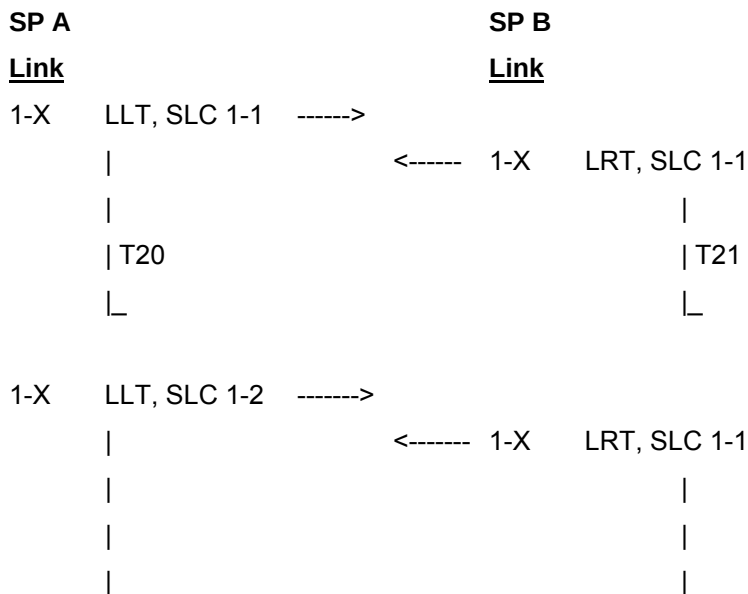
SUBTITLE: Management inhibiting test - Normal procedure

PURPOSE: To check that the system performs correctly the management inhibiting test.

PRE-TEST CONDITIONS: Link 1-1 inhibited by A, other links are available

CONFIGURATION: A

MESSAGE SEQUENCE:



:Wait

:Stop traffic

TEST DESCRIPTION:

1. Check that an LLT is periodically sent by A and check that the duration of timer T20 is inside the specified range.
2. Check that an LRT is periodically (T21) sent from B to A.
3. Check that on the reception of an LRT, no action is taken in A.
4. Stop traffic, some messages have been lost.

Note: Timer T20 or T21 has a value ranging from 90 to 120 secs.

2.38 Normal Alignment	M2-1.5	1.5 Normal Alignment

PROTOCOL REFERENCE: ANSI T1.111, chapter 3, clause 7

TITLE: Link State Control - Expected signal units/orders

SUBTITLE: Normal alignment - correct procedure (FISU)

PURPOSE: To check normal alignment procedure

PRE-TEST CONDITIONS: Link out of service

CONFIGURATION: 1

EXPECTED SIGNAL UNIT SEQUENCE:

SP B			SP A	
<u>Link</u>			<u>Link</u>	
		<-----	1-1	SIOS
1-1	SIOS	----->		
				:start
		<-----	1-1	SIO
1-1	SIO	----->		
		<-----	1-1	SIN
1-1	SIN	----->		
		<-----	1-1	FISU
1-1	FISU	----->		

TEST DESCRIPTION:

1. Start normal alignment procedure.
2. Check link aligns and enters "in service" state.
3. Check that "in service" state is maintained.

NOTE: Tests 1.38, 1.39 and 1.40 are non-intrusive for test simulation but require manual intervention to create trouble conditions to stimulate the nodes to perform automatic rerouting, recovery and management procedures (1.e. changeover, changeback, etc.). Links will be established between STPs and monitored to ensure the compatibility of the message formats between the nodes. Level 3 tests require a message generation device to create traffic which allows monitoring proper changeover, changeback, inhibits, etc.

2.39Broken Transmission Path Transmission Path”	M2-2.3	3.5 Broken Transmission Path

PROTOCOL REFERENCE: ANSI T1.111, chapter 3, clause 4, subclause 10.2

TITLE: Broken Transmission Path

SUBTITLE: Link in service

PURPOSE: To test the response to a broken transmit path when the link is "In service"

PRE-TEST CONDITIONS: Link in service

CONFIGURATION: 1

EXPECTED SIGNAL UNIT SEQUENCE:

SP B		SP A
<u>Link</u>		<u>Link</u>
	<-----	1-1 FISU
1-1 FISU	----->	
: break Tx		
	<-----	1-1 SIOS

TEST DESCRIPTION:

1. When the link is in the In Service state, the transmit side of the link from SP B to SP A is broken.
2. The terminal (SP A) shall send SIOS.

2.40 MSU Generation	M2-6.1	8.1 MSU Generation

PROTOCOL REFERENCE: ANSI T1.111, chapter 3, subclause 5.2

TITLE: Transmission and reception control (Basic)

PURPOSE: To check basic MSU transmission and reception

PRE-TEST CONDITIONS: Link in service

CONFIGURATION: 1

EXPECTED SIGNAL UNIT SEQUENCE:

SP B	SP A
<u>Link</u>	<u>Link</u>
	<-----1-1 FISU
1-1 FISU	----->
1-1 MSU	----->
(FIB+FSN=80)	
(BIB+BSN=FF)	
	<-----1-1 FISU (FIB+FSN=FF)
	(BIB+BSN=80)
1-1 FISU	----->
(FIB+FSN=80)	
(FIB+FSN=FF)	
	<-----1-1 MSU (FIB+FSN=80)
	(BIB+BSN=80)
1-1 FISU	----->
(FIB+FSN=80)	
(BIB+BSN=80)	
	<-----1-1 FISU (FIB+FSN=80)
	(BIB+BSN=80)

Note: "80", "FF" are hexadecimal numbers.

TEST DESCRIPTION:

1. The test unit (SP B) sends a MSU (e.g., SLTM)
2. Check that the terminal being tested (SP A) receives the MSU correctly, and returns a positive acknowledgment.
3. The terminal sends an MSU (e.g., SLTA).
4. Check that the test unit receives the MSU correctly, and returns a positive acknowledgment.

2.41 Management Uninhibit with Changeback	M3-6.6.	7.6.1 Management Uninhibit with Changeback

PROTOCOL REFERENCE: ANSI T1.111, chapter 4, clause 10

TITLE: Management inhibiting

SUBTITLE: Manual uninhibition of a link - with changeback

PURPOSE: To check for correct restoration when link uninhibition is requested

PRE-TEST CONDITIONS: Linkset with one available link and one inhibited link

CONFIGURATION: A

MESSAGE SEQUENCE:

SP A		SP B
<u>Link</u>		<u>Link</u>
:Start traffic		
1-2 TRAFFIC	----->	
	<-----	1-2 TRAFFIC
1-1 :Request uninhibition		
1-2 LUN, SLC 1-1	----->	
	<-----	1-2 LUA, SLC 1-1
CHANGEBACK(See note)		CHANGEBACK (See note)
1-1 TRAFFIC	----->	
(from 1-2)		
	<-----	1-1 TRAFFIC (FROM 1-2)
1-2 TRAFFIC	----->	
	<-----	1-2 TRAFFIC
:Wait		
:Stop traffic		

Note: A changeback procedure is performed after uninhibition of link 1-1, but it is not described in this test which checks only uninhibition procedure.

TEST DESCRIPTION:

1. Start traffic from A to B on link 1-2.
2. Request uninhibition of link 1-1, check the reception of an LUN and response with an LUA inside T12.
3. Check that the uninhibition is performed, and stop traffic.
4. Check that the traffic was shared on links 1-1 and 1-2 according to the load sharing rules.

Note: Timer T12 has a value ranging from 0.8 to 1.5 secs.

2.42 Manual Uninhibition of a Link - Without changeback	M3-6.7	7.6.2 Manual Uninhibition of a Link - Without changeback

PROTOCOL REFERENCE: ANSI T1.111, chapter 4, clause 10

TITLE: Management inhibiting

SUBTITLE: Manual uninhibition of a link - without changeback

PURPOSE: To check manual uninhibition procedure when the uninhibited link stays unavailable

PRE-TEST CONDITIONS: Linkset with one available link and one link deactivated and inhibited

CONFIGURATION: A

MESSAGE SEQUENCE:

SP A		SP B
<u>Link</u>		<u>Link</u>
:Start traffic		
1-1 TRAFFIC	----->	
	<-----	1-1 TRAFFIC
1-2 :Request uninhibition		
1-1 LUN, SLC 1-2	----->	
	<-----	1-1 LUA, SLC 1-2
1-1 TRAFFIC	----->	
	<-----	1-1 TRAFFIC
:Wait		
:Stop		

TEST DESCRIPTION:

1. Start traffic from A to B on link 1-1.
2. Request uninhibition of link 1-2 at A and check that an LUN is received at B and that an LUA is sent from B in response inside T12.
3. Check that the uninhibition is performed correctly and that link 1-2 stays unavailable.
4. Stop traffic and check that it was not disturbed.

Note: Timer T12 has a value ranging from 0.8 to 1.5 secs.

NGIIF Test #: _____ **ANSI T1-234-2000 Test #:** _____ **GR-CORE-905 Test #** _____

2.43 Signaling Route Management Tests (Issue 11, Page 19 & 20)	M3-7.1	Section 9.0 Signaling Route Management

PROTOCOL REFERENCE: ANSI T1.111, chapter 4, subclauses 13.4, 13.5, 15.9, 15.10

TITLE: Test of TFR and RSR

SUBTITLE:

PURPOSE: To verify the proper initiations of TFR and RSR

PRE-TEST CONDITIONS: All links are operative

CONFIGURATION: C

MESSAGE SEQUENCE:

SP C		SP A-A'		SP B-B'		SP D
<u>Link</u>		<u>Link</u>		<u>Link</u>		
TRAFFIC	1-1, 2-1	----->				
		<-----				7-1, 8-1 TRAFFIC
	:Deactivate	1-1				
		TFR	3-1	----->		
		TFR	4-1	----->		
		<-----	3-1	RSR		
		<-----	4-1	RSR		
TRAFFIC	2-1	----->				7-1, 8-1 ----->
<-----	2-1	<-----				7-1, 8-1 TRAFFIC

NOTE: Danger of congestion of the lower priority linkset used as the alternate route, or expiration of T11 (30-90 sec) characterizes long-term failure. Of these two events, whichever arrives first, causes invocation of the transfer-restricted procedure.

TEST DESCRIPTION:

1. Start traffic between C and D.
2. Place link 1-1 out of service.
3. Check that TFRs are sent from A to B, and from A to B'.
4. Check that RSRs are sent from B to A, and from B' to A.
5. Check that traffic can be sent and received at C and D via available links.

NOTE: TFR and RSR may be sent over any available signaling route.

NGIIF Test #:

ANSI T1-234-2000 Test #:

GR-CORE-905 Test #

***2.44 Signaling Route
Management Tests***

M3-7.2

Section 9.0 Signaling Route
Management

PROTOCOL REFERENCE: ANSI T1.111, chapter 4, subclauses 13.2, 13.5, 15.7, 15.10

TITLE: Test of TFP and RSR

SUBTITLE:

PURPOSE: To verify the proper initiations of TFP and RSR

PRE-TEST CONDITIONS: End of test M3-7.1 (Link 1-1 is out of service)

CONFIGURATION: C

MESSAGE SEQUENCE:

SP C

SP A-A'

SP B-B'

SP D

Link

Link

Link

:Deactivate 2-1

TFP 3-1, 4-1 ----->

TFP 5-1, 6-1 ----->

<----- 3-1, 5-1 RSP

<----- 4-1, 6-1 RSP

TEST DESCRIPTION:

1. Place link 2-1 out of service.
2. Check that TFPs are sent from A to B and B', and from A' to B and B'.
3. Check that RSPs are sent from B to A and A', and from B' to A and A'.
4. Check that traffic between C and D has stopped.

NOTE: TFP and RSP may be sent over any available signaling route.

NGIIF Test #:

ANSI T1-234-2000 Test #:

GR-CORE-905 Test #

***2.45 Signaling Route
Management Tests***

M3-7.3

Section 9.0 Signaling Route
Management

PROTOCOL REFERENCE: ANSI T1.111, chapter 4, subclauses 13.3, 13.4, 13.5, 15.8, 15.9, 15.10

TITLE: Test of TFA, TFR and RSR

SUBTITLE:

PURPOSE: To verify the proper initiations of TFA, TFR and RSR

PRE-TEST CONDITIONS: End of test M3-7.2 (Link 1-1 and 2-1 are out of service)

CONFIGURATION: C

MESSAGE SEQUENCE:

SP C	SP A-A'	SP B-B'	SP D
Link	Link	Link	
	:Activate	2-1	
	TFA	5-1, 6-1 ----->	
	TFR	3-1, 4-1 ----->	
	<-----	3-1, 4-1 RSR	
TRAFFIC	2-1	----->	7-1, 8-1 ----->
<-----	2-1	<-----	7-1, 8-1 TRAFFIC

TEST DESCRIPTION:

1. Restore link 2-1 to in service (link 1-1 is still out of service).
2. Check that TFAs are sent from A' to B and B'.
3. Check that TFRs are sent from A to B and B'.
4. Check that RSRs are sent from B to A, and from B' to A.
5. Check that traffic between C and D can start on available links.

NOTE: TFA, TFR, and RSR may be sent over any available signaling route.

2.46 Signaling Route Management Tests	M3-7.4	Section 9.0 Signaling Route Management

PROTOCOL REFERENCE: ANSI T1.111, chapter 4, subclauses 13.3, 15.8

TITLE: Test of TFA

SUBTITLE:

PURPOSE: To verify the proper initiations of TFA.

PRE-TEST CONDITIONS: End of test M3-7.3 (Link 1-1 is out of service)

CONFIGURATION: C

MESSAGE SEQUENCE:

SP C		SP A-A'		SP B-B'		SP D
<u>Link</u>		<u>Link</u>		<u>Link</u>		
TRAFFIC	2-1	----->		7-1, 8-1	----->	
<-----	2-1			<-----	7-1, 8-1	TRAFFIC
	:Activate	1-1				
		TFA		3-1, 4-1	----->	
		<-----		3-1, 4-1	RSR	
TRAFFIC	1-1, 2-1	----->		7-1, 8-1	----->	
<-----	1-1, 2-1	<-----		7-1, 8-1	TRAFFIC	

TEST DESCRIPTION:

1. Restore link 1-1 to in service (link 2-1 has been in service).
2. Check that TFAs are sent from A to B and B'.
3. Check that traffic between C and D is sent and received normally on all available links.

NOTE: TFA may be sent over any available signaling route.

NGIIF Test #:

ANSI T1-234-2000 Test #:

GR-CORE-905 Test #

2.47 Signaling Route Management Tests

M3-7.5

Section 9.0 Signaling Route Management

PROTOCOL REFERENCE: ANSI T1.111, chapter 4, subclauses 13.7, 13.9

TITLE: Test of TFC and RCT

SUBTITLE:

PURPOSE: To test the response to TFC.

PRE-TEST CONDITIONS: All links are operative

CONFIGURATION: D

MESSAGE SEQUENCE:

SP D		SP C		SP B-B'		SP A
<u>Link</u>		<u>Link</u>		<u>Link</u>		
		TFC	1-1	----->	4-1	----->
		cs=3	2-1		5-1	
<-----	6-1	<-----	1-1	<-----	4-1	MSU
			2-1		5-1	PRI=3
<-----	6-1	<-----	1-1	<-----	4-1	RCT____
			2-1		5-2	PRI=2
						T16
<-----	6-1	<-----	1-1	<-----	4-1	MSU
			2-1		5-1	PRI > 2
<-----	6-1	<-----	1-1	<-----	4-1	RCT____
			2-1		5-1	PRI=1
						T16
<-----	6-1	<-----	1-1	<-----	4-1	MSU
			2-1		5-1	PRI > 1
<-----	6-1	<-----	1-1	<-----	4-1	RCT____
			2-1		5-1	PRI=0
						T16
<-----	6-1	<-----	1-1	<-----	4-1	MSU
			2-1		5-1	PRI > 0

TEST DESCRIPTION:

1. The test unit (SP C) sends a TFC with congestion status of 3 to the unit under test (SP A) via B and B'.
2. Check that only MSU's with PRI=3 can be sent from A to D. Check that RCT with congestion priority of 2 is sent from A to D.
3. After timer T16 expires, MSUs with PRI = 2,3 can be sent from A to D. An RCT with congestion priority of 1 is sent from A to D.
4. After timer T16 expires, MSUs with PRI = 1,2,3 can be sent from A to D. An RCT with congestion priority of 0 is sent from A to D.
5. After timer T16 expires, MSUs with PRI = 0,1,2,3 can be sent from A to D. Check that no RCT is sent from A to D

NOTE: Timer T16 has a value ranging from 1.4 to 2.0 sec.

2.48 Processor Outage	M2-7.1	8.13 Processor Outage

REFERENCE: ANSI T1.111.3

TITLE: Processor Outage

PURPOSE: Test the response to remote processor outage indication on MTP Level 2 and Level 3. Verify that the T111.3 procedures for response to remote processor outage indication are implemented properly.

PRE-TEST CONDITIONS: Link is aligned and in service. Arrange for SP A (SUT --- System Under Test) to send one MSU/second to SP B on each link. Have a two-link linkset in service between SP A and SP B so a time-controlled changeover can take place. Message sequence exchange below takes place on link one of the linkset.

CONFIGURATION: 1

EXPECTED SIGNAL UNIT SEQUENCE:

SP B	SP A
<u>Link</u>	<u>Link</u>
1)	<----- (BSN/FSN = 0/1) MSU
(BSN/FSN=1/0) FISU	----->
(BSN/FSN=1/1) MSU	----->
2) (BSN/FSN=1/1) SIPO	-----> (T111.3 timers T5, T6 & T7 stopped. Processor Outage stage entered, Level 3 timer T1 (0.5 to 1.2 sec.) started
3)	<----- (BSN/FSN=1/1) FISU
4) (BSN/FSN=1/1) SIPO	----->
5) (BSN/FSN=1/1) FISU	----->
(BSN/FSN=1/2) MSU	----->
6)	<----- (BSN/FSN=2/1) FISU
	<----- (BSN/FSN=2/2) MSU
(BSN/FSN=2/2) FISU	

TEST DESCRIPTION:

- SP A is configured to send one MSU/second to SP B.
- SP B enters Level 2 (L2) Processor Outage State. SP B discards all received messages, sends continuous SIPO.
- SP A is expected to send only FISU and acknowledge all received messages.
- SP B continues to send SIPO for 7 seconds to verify that link remains in alignment. Level 3 timer T1 should expire and SP A should do a time-controlled changeover to link two.
- SP B exits Level 2 Processor Outage State.
- SP A is expected to restart T111.3 timers T5, T6, T7, do a changeback, and return link to the in-service state. The CBD (ChangeBack Declaration) and CBA (ChangeBack Acknowledged) messages should be observed on link 2.

EXPECTED RESULTS:

- The System Under Test (SP A) stops sending MSUs on the affected link during receipt of SIPO.
- Link stays aligned.
- SP A acknowledges received MSU.

4. SP A should do a time-controlled changeover when SP A's Level 3 timer T1 expires.
5. When L2 Processor Outage Condition clears (SP A receives FISU) SP A should do a changeback and normal operation resumes.

Level 2 Timers

T3 = Aligned

T5 = Send Status Indication Busy

T6 = Remote Congestion

T7 = Excessive Delay of Acknowledgment

Level 3 Timer

T1 = Represents the overall message transfer time for a signaling relation between the node that originates the message and the destination node of the message.

2.49 Level 2 Flow Control	ANSI (N/A)	8.14 Level 2 Flow Control

REFERENCE: ANSI T1.111.3

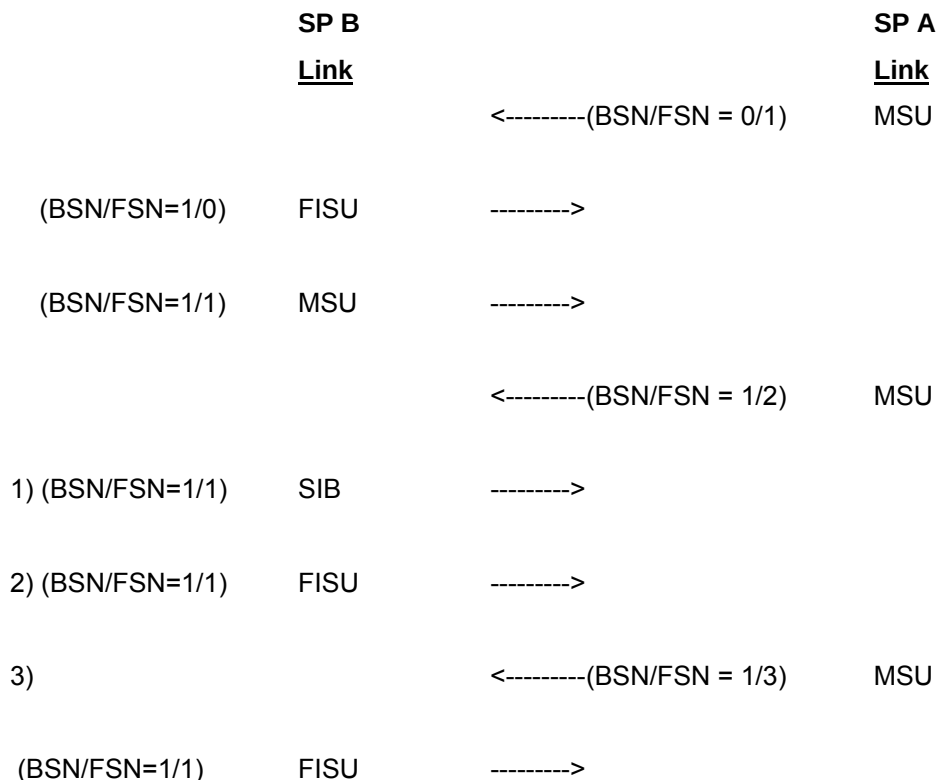
TITLE: Level 2 Flow Control

PURPOSE: Test the response to remote Level 2 flow control indication.

Verify that the T111.3 procedures for remote response to Level 2 flow control are implemented using two test cases. Test Case 1 verifies that the signaling link remains in service for a flow control event less than the system under test (SUT -- SP A) T111.3 timer T6 (remote congestion) value. Test case 2 verifies that the link goes out of service for a flow control event exceeding SP A's T111.3 timer T6 value, and that SP A's MTP Level 3 procedures execute a changeover. A two link linkset between SP A and SP B is necessary to allow the changeover procedure to execute.

PRE-TEST CONDITIONS: SP B to SP A, the links are aligned and in-service at the start of the test. SP A is configured to send one MSU/(second) to Tester.

1. Obtain T6 value from SPA, configure test script T6 timer.
2. Obtain YOUR OWN network's T5 value, configure the test script T5 timer.
3. Arrange for SP A to send one MSU/sec to SP B on the links.



THIS SECTION REPEATS UNTIL TEST CASE EXIT PROCEDURE OCCURS.

4) (BSN/FSN=1/1) SIB ----->

5) (BSN/FSN=1/1) FISU ----->

6) <------(BSN/FSN = 1/N) MSU

(BSN/FSN=1/1) FISU ----->

Case 1 Exit Procedure: SP B leaves Level 2 Congestion Discard Mode just before SP A's timer T6 expires.

Case 2 Exit Procedure: SP B leaves L2 Congestion Discard Mode after SP A's timer T6 expires. Note: SP A (SUT -- System Under Test) should remove the link from service before the SP B reaches the CASE 2 exit condition.

Test Case 1 Exit Procedure: (Before timer T6 expires.)

	SP B		SP A
	<u>Link</u>		<u>Link</u>
		<------(BSN/FSN = 1/M)	MSU
7) (BSN/FSN=*1/1)	FISU	----->(* = BIB inverted indication)	
		(BIB = Backward Indicator Bit)	
		<-----MSUs 2 to M re-sent	
(BSN/FSN=M/1)	FISU	----->	

8) End of Test Case 1, link stays in service.

TEST CASE 2 EXIT PROCEDURE:

	SP B		SP A
	<u>Link</u>		<u>Link</u>
9)		<------(BSN/FSN = 1/M)	MSU
		<------(BSN/FSN = 1/M)	SIOS

End of Test Case 2, link removed from service.

TEST DESCRIPTION:

1. SP B's L2 Basic Reception Control (BRC) enters Congestion Discard Mode.
2. SP B starts script timer T5 and script timer T6. SP B stops acknowledging messages. SP A is expected to reset T111.3 timers T6 and T7.
3. SP A continues to send messages. (SP A's retransmission buffer is not full.)
4. SP B's script timer, T5, expires and SP B sends a single SIB.
5. SP B restarts timer T5. SP A is expected to reset T111.3 timer T7.
6. SP A continues to send messages. (SP A's retransmission buffer is not full.)

TEST CASE 1 EXIT PROCEDURE

1. SP B's Level 2 BRC leaves Congestion Discard Mode at time SP A: $T6 \times 0.9$ seconds. SP B requests retransmission of messages. (* = BIB inverted indication)
2. SP A stops T6. Cancel SIB received mode and basic transmission control.

TEST CASE 2 EXIT PROCEDURE

1. SP A's timer T6 SHOULD EXPIRE and the link is removed. SP A should execute a changeover using the other link in the linkset. SP B's Level 2 BRC leaves Congestion Discard Mode at time SP A ($T6 + 2$ seconds). If SP A does not remove the link it would be an indication that the test failed.

Expected Results

Test Case 1:

1. SP A continues sending MSUs (transmit buffer not full).
2. When SP B leaves Level 2 congestion and sends FISU requesting retransmission, SP A re-sends unacknowledged MSUs and normal operation resumes.
3. SP A should not perform a changeover.

Test Case 2:

1. SP A continues sending MSUs (transmit buffer not full).
2. When SP A timer T6 expires the link is removed from service.
3. SP A should perform a changeover.

Level 2 Timers

T3 = Aligned

T5 = Send Status Indication Busy

T6 = Remote Congestion

T7 = Excessive Delay of Acknowledgment

Level 3 Timer

T1 = Represents the overall message transfer time for a signaling relation between the node that originates the message and the destination node of the message.

2.50 Hubbing Interconnection Test	M3-7.6	

PROTOCOL REFERENCE: T1.111, chapter 4, clause 13, subclause 13.3 & 13.5

TITLE: Hubbing Interconnection Testing

SUBTITLE: MTP Routing

PURPOSE: The purpose of this test is to ensure that MTP routing capabilities are correctly provisioned when SS7 interconnection involves a Hub Provider.

PRE-TEST CONDITIONS:

CONFIGURATION: Figure 6 Configuration E

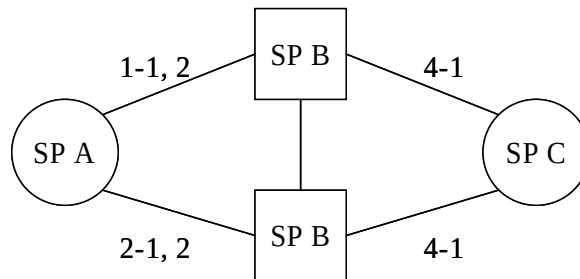
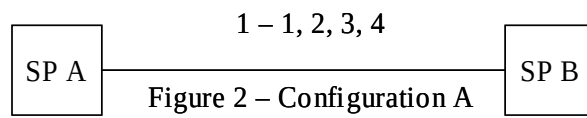
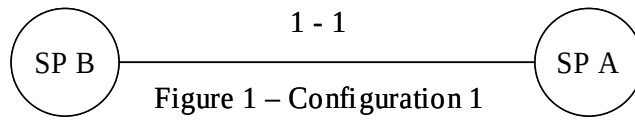
TEST DESCRIPTION:

1. Connect the LTU A to STP 1&2.
2. Connect the LTU Z to STP X&Y.
3. Send a CVT from LTU A to STP 1 to destination LTU Z. A CVR is returned from LTU Z to LTU A. (Verifies Network Routing).
4. Remove the mate link from service (LTU A – STP 2) and the B link between STP 1 and STP 4.
5. LTU A Sends an RSR/RSP message with an OPC of STP1 to STP 3 with a DPC of STP3 and an Affected Point Code of LTU Z.
6. The result should be that a TFA is sent from STP 3 to STP 1.
7. Restore the links previously removed from service.
8. Remove the mate link from service (LTU A – STP 1) and the B link between STP 2 and STP 3.
9. LTU A Sends an RSR/RSP message with an OPC of STP2 to STP 4 with a DPC of STP4 and an Affected Point Code of LTU Z.
10. The result should be that a TFA is sent from STP 4 to STP 2.
11. Restore the links previously removed from service.
12. In the event that there is more than one HUB Provider in the interconnected network, then the test should be performed from both ends of the interconnected network (LTU A & LTU Z).

NOTES:

1. A Hub Provider (STP 3&4) is an entity that provides for the transport of SS7 messages between Network 1 (STP 1&2) and Network 2 (STP X&Y).
2. Screening capabilities should be provisioned and be based on intercompany locally negotiated agreements.

3 Attachment A – MTP Compatibility Tests, Test Diagrams



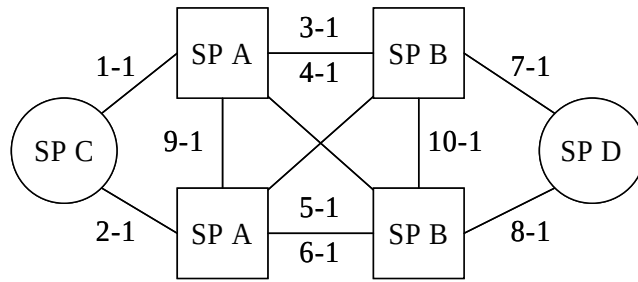


Figure 4 – Configuration B

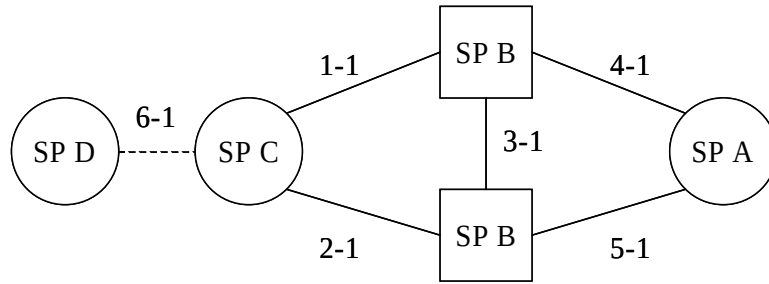


Figure 5 – Configuration D

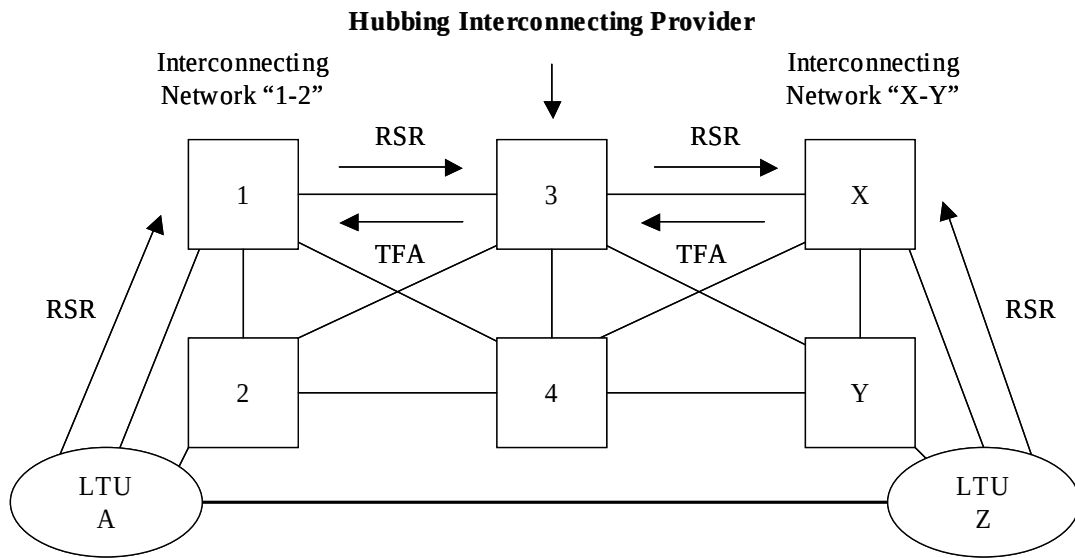


Figure 6 - Configuration E

4 ANNEX REFERENCES

Telcordia Specification of Signaling System Number 7, (GR-NWT-000246)

Signaling System Number 7 (SS7) - MTP Levels 2 and 3 Compatibility Testing, ANSI T1.234

Signaling System Number 7 (SS7) - SCCP Class 0 Compatibility Testing, ANSI T1.235

Signaling System Number 7 (SS7) - ISDN User Part Compatibility Testing, ANSI T1.236



ATIS-0300013

**Next Generation Interconnection Interoperability (NGIIF)
Reference Document**

**Part III, Installation, Testing and Maintenance
Responsibilities for SS7 Links and Trunks**

**Attachment B
ISUP Compatibility Tests**

Version 12.0



ATIS is the leading technical planning and standards development organization committed to the rapid development of global, market-driven standards for the information, entertainment and communications industry. More than 200 companies actively formulate standards in ATIS' Committees, covering issues including: IPTV, Cloud Services, Energy Efficiency, IP-Based and Wireless Technologies, Quality of Service, Billing and Operational Support, Emergency Services, Architectural Platforms and Emerging Networks. In addition, numerous Incubators, Focus and Exploratory Groups address evolving industry priorities including Smart Grid, Machine-to-Machine, Connected Vehicle, IP Downloadable Security, Policy Management and Network Optimization.

ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications' Sectors, and a member of the Inter-American Telecommunication Commission (CITEL). ATIS is accredited by the American National Standards Institute (ANSI). For more information, please visit www.atis.org.

Notice

This document was developed by the Alliance for Telecommunications Industry Solutions' (ATIS) sponsored Next Generation Interconnection Interoperability Forum (NGIIF). The NGIIF addresses next-generation network interconnection and interoperability issues associated with emerging technologies. Specifically, it develops operational procedures which involve the network aspects of architecture, disaster preparedness, installation, maintenance, management, reliability, routing, security, and testing between network operators. In addition, the NGIIF addresses issues which impact the interconnection of existing and next generation networks and facilitate the transition to emerging technologies. All changes to this document shall be made through the NGIIF issue resolution process.

Note Regarding Previous Versions

The NIIF Reference Document was formerly known as the Network Operations Forum (NOF) Reference Document. The NOF Reference Document was published and maintained by Bellcore. The last version of the NOF Reference Document is Issue 13.

Disclaimer and Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

ATIS-0300013, NGIIF Reference Document, Part III, Installation and Maintenance Responsibilities for SS7 Links and Trunks, Attachment B, ISUP Compatibility Tests, Formerly NIIF 5008

The NGIIF Reference Document, Part III, Installation and Maintenance Responsibilities for SS7 Links and Trunks is an ATIS standard developed by the NGIIF.

Published by

Alliance for Telecommunications Industry Solutions

1200 G Street, NW, Suite 500

Washington, DC 20005

Copyright © 2011 by Alliance for Telecommunications Industry Solutions

All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < <http://www.atis.org> >.

Printed in the United States of America.

ISUP Compatibility Tests

Table of Contents

1	INTRODUCTION	5
1.1	PURPOSE OF TESTS	5
1.2	TEST METHOD	5
1.3	DESCRIPTION OF TESTS.....	5
1.4	OTHER TESTING CONSIDERATIONS.....	6
1.5	CIRCUIT VALIDATION TEST (CVT).....	8
1.6	CONTINUITY CHECK REQUEST (CCR)	9
1.7	CONTINUITY TEST - SUCCESSFUL	10
1.8	2.4 CONTINUITY TEST - UNSUCCESSFUL.....	11
1.9	CONTINUITY TEST - PREVIOUS CIRCUIT - IAM.....	12
1.10	CONTINUITY TEST - SUCCESSFUL CRM.....	13
1.11	CONTINUITY TEST - UNSUCCESSFUL - CRM.....	14
1.12	SINGLE CIRCUIT BLOCK/UNBLOCK - BLO/UBL	15
1.13	SINGLE CIRCUIT BLOCK/RESET CIRCUIT/UNBLOCK - BLO/RSC/UBL.....	16
1.14	BLOCK/UNBLOCK FROM CALL ORIGINATING END - BLO/BLU	18
1.15	BLOCK/UNBLOCK FROM CALL RECEIVING END - BLO/UBL	20
1.16	CIRCUIT GROUP BLOCKING/UNBLOCKING - CGB/CGU (BLOCK WITHOUT RELEASE).....	22
1.17	CIRCUIT GROUP BLOCKING/UNBLOCKING - CGB/CGU (BLOCK WITH IMMEDIATE RELEASE).....	24
1.18	RESET CIRCUIT - DURING AN ESTABLISHED OUTGOING CALL - RSC.....	26
1.19	RESET CIRCUIT - DURING AN ESTABLISHED INCOMING CALL - RSC.....	27
1.20	DUAL SEIZURE.....	28
1.21	CALL TO IDLE TEST LINE.....	30
1.22	CALL TO BUSY TEST LINE	31
1.23	IAM WITH AN UNEQUIPPED CIRCUIT IDENTIFICATION CODE	32
1.24	TONES AND ANNOUNCEMENTS - BUSY LINE	33
1.25	TONES AND ANNOUNCEMENTS - UNALLOCATED NUMBER.....	34
1.26	TONE AND ANNOUNCEMENTS - NO CIRCUIT AVAILABLE	35
1.27	RELEASE - ABANDONED CALL.....	36
1.28	RELEASE - CALLING PARTY	37
1.29	SUSPEND, RESUME AND RELEASE - CASE 1	38
1.30	SUSPEND, RESUME AND RELEASE - CASE 2	40
1.31	UNSUCCESSFUL CALL - IAM - NO CPN, NO CHG, WITH OLI	41
1.32	UNSUCCESSFUL CALL - IAM - WITH CPN, WITH CHG, NO OLI	42
1.33	CALLING PARTY DISCONNECT BEFORE RECEIPT OF ACM	43
1.34	SINGLE CIRCUIT BLOCK/RESET CIRCUIT/UNBLOCK - BLO/RSC/UBL (ALSO SEE NGIIF TEST 2.9).....	44
1.35	CIRCUIT GROUP BLOCKING/UNBLOCKING CGB/CGU (BLOCK WITHOUT RELEASE) (ALSO SEE NGIIF TEST 2.12)...	47
1.36	RESET CIRCUIT - DURING AN ESTABLISHED OUTGOING CALL - RSC (ALSO SEE NGIIF TEST 2.14)	49
1.37	RESET CIRCUIT - DURING AN ESTABLISHED INCOMING CALL - RSC (ALSO SEE NGIIF TEST 2.15).....	50
1.38	IAM RECEIVED ON A REMOTELY BLOCKED CIRCUIT	51
1.39	CALL TO CIRCUIT BLOCKED AT BOTH ENDS	52
1.40	DUAL SEIZURE (ALSO SEE NGIIF TEST 2.16)	53
1.41	TIMER TIAM TIME-OUT	55
1.42	IAM WITH AN UNEQUIPPED CIRCUIT (ALSO SEE NGIIF 2.19)	56
1.43	UNSUCCESSFUL CALL - IAM NO CPN, NO CHG, WITH OLI (ALSO SEE NGIIF TEST 2.27)	57
1.44	UNSUCCESSFUL CALL - IAM - WITH CPN, WITH CHG, NO OLI (ALSO SEE TEST 2.28).....	58
1.45	CALLING PARTY DISCONNECT BEFORE RECEIPT OF ACM (ALSO SEE NGIIF 2.29)	59
1.46	SIMULTANEOUS RELEASE MESSAGES.....	60
1.47	BLO AFTER IAM RECEIVED AND BEFORE BACKWARD MESSAGE.....	61
1.48	SENDING IAM AND RECEIVING CGBs BEFORE ANY BACKWARD MESSAGES	62
1.49	SENDING IAM AND RECEIVING CGBs AFTER RECEIVING A BACKWARD MESSAGE	64
1.50	CIRCUIT GROUP RESET MESSAGES - GRS	66
1.51	CIRCUIT GROUP RESETS DURING AN ESTABLISHED CALL -GRS	67
1.52	RESET CIRCUIT AFTER IAM BUT BEFORE BACKWARD MESSAGES - RSC.....	68
1.53	IAM PRIORITY TEST FOR INTERCONNECTS.....	69

1.54	IAM PRECEDENCE TEST FOR INTERCONNECTS.....	72
1.55	SIP INVITE TO ISUP IAM MAPPINGS.....	74
1.56	ISUP IAM TO SIP INVITE MAPPINGS.....	79

1 INTRODUCTION

These tests scripts were developed as a minimum set of tests to be performed during interconnection of two networks.

These tests presume that the interconnected network elements have been tested for conformance to applicable standards. Since no suite of conformance tests has been adopted, in the interest of the service, the interconnecting parties should exchange known specification non-compliances and discuss conformance testing that they have performed.

Because of the current lack of conformance tests, interconnecting networks may agree on additional tests to be performed.

NOTE: The test message sequence and expected test results described below are applicable to interconnecting trunk groups FG-D type interconnections and can also accommodate wireline to wireless, LEC to LEC interconnections. For all other types, it is expected that the call shall complete as per standards. The interconnecting parties should discuss all parameters and codings prior to testing taking place.

1.1 Purpose of Tests

This document provides a recommended minimum set of script-driven tests and manually interactive tests that should be performed to test the compatibility of the network elements.

1.2 Test Method

Tests should be generated via test scripts and manually by Access Service Provider End Office (ECEO), Access Service Provider Access Tandem (ECAT), and Access Service Customer (ASC) personnel per the "DESCRIPTION OF TESTS" section of this document. The Access Service Provider (ASP) and the ASC should non-intrusively monitor the ISDN USER Part (ISDN-UP) messages between the system under test.

1.3 Description of Tests

This document provides the Trunk Maintenance, Call Set-Up, and Intrusive tests that should be performed. These tests are guidelines and each ASP/ASC may elect to add to these tests by mutual agreement. Some tests, as noted in the descriptions, may not be able to be performed due to implementation constraints.

NOTE: The test message sequence and expected test results described below are applicable to interconnecting trunk groups FG-D type interconnections and can also accommodate wireline to wireless, LEC to LEC interconnections. For all other types, it is expected that the call shall complete as per standards. The interconnecting parties should discuss all parameters and codings prior to taking place.

In the "TEST SEQUENCE" descriptions of the following tests - arrows, dashes, and the abbreviations "SS7" and "MF" are used to indicate the directionality of messaging and type of circuit group(s) (Signaling System 7 and/or Multi-Frequency) i.e., ECEO(A)/ECAT <--SS7--> ASC indicates that the test should be performed in both directions using an SS7 circuit group (four tests total).

The "EXPECTED RESULT" is included as a guide to aid in analysis. Detailed verification of the following items should be performed as applicable using the TR-TSV-000905 section(s) listed under "REFERENCE(S)" for each test:

- Correct Termination of Calls
- Correct Message Sequences Between the Switches
- Correct Parameters in Messages

- Correct Coding of Parameters in Messages
- Correct Timer Functionality
- Correct Handling of Error and Abnormal Events
- Correct Circuit States
- Automatic Message Accounting (AMA) Billing Data Collected.

1.4 Other Testing Considerations

1.4.1 IAM Priority Level Testing

In the event of a national emergency, the Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS) provide priority call completion to authorized users during times of network stress or congestion. GETS was fielded on September 30, 1994 and includes the capability of coding the ISUP Calling Party's Category parameter with the NS/EP code point (11100010) and setting the IAM priority level to 1. Priority call handling features, such as call/trunk queuing and exemption from network management controls, are based on recognizing the NS/EP code point. The normal POTS priority setting of 0 must be maintained in accordance with ANSI T1.111 in order for the GETS and WPS calls to have a higher probability of completion during SS7 congestion.

Annexes A and B in Chapter T1.111.5 specify priority assignments for ISUP messages transferred between U.S. SS7 networks and establish engineering principles for priority assignment. Table A1/T1.111.5 requires that all IAMs be assigned priority level 0 with the exception that "Message priority level 1 shall be limited to those network services or capabilities that have been approved in ANSI T1 standards to have an IAM message priority of 1 (e.g., High Probability of Completion, Multi-level Precedence and Preemption, Emergency Calling Service)."

Interconnecting networks should exchange their respective IAM priority assignments in conformance with T1.111 such that the priority assignment for normal POTS (non-emergency) IAMs are set to 0. The interconnecting participants are responsible for performing the appropriate tests to verify such conformance. See Test 2.92.

1.4.2 ISUP IAM Precedence Parameter Testing

The Precedence parameter is defined as an optional parameter within the SS7 ISUP IAM. Technical Report 3GPP TR 22.952 V6.3.0 (2005-09), Table A.2, defines how a Mobile Switching Center (MSC) uses the ISUP Precedence parameter to send WPS information across the PSTN to a terminating MSC. The ISUP Precedence parameter encoding is specified in ANSI T1.111.5. This parameter ensures that a "precedence level 1" call originated at an MSC will receive the same "precedence level 1" treatment at a terminating MSC (i.e., queuing and servicing before "precedence level 2" and lower precedence level calls). Without transmission of the Precedence parameter, all terminating WPS calls have the same default priority and treatment. All switches are required to pass optional parameters and values that they do not understand, such as the Precedence parameter (according to ANSI T1.113-1995, "American National Standard for Telecommunication Signaling System No. 7 (SS7) – Integrated Service Digital Network (ISDN) User Part"). Interconnecting networks should verify transit switches pass the Precedence parameter and WPS terminating switches establish a call based on the IAM with the Precedence parameter. See Test 2.93.

1.4.3 IAM Priority Level Mapping to IP SIP Priority Level

The Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS) provides priority call completion to authorized users during times of network stress or congestion. As networks migrate to Internet Protocol (IP) based signaling, proper mappings between TDM and IP networks are imperative to the GETS and WPS mission. GETS and WPS will make use of the Session Initiation Protocol (SIP) Resource Priority Header (RPH) in the IP domain. SIP RPH is an IEEE standard (RFC 4412). The IP mappings found in this document are based on the ATIS document PTSC-SAC-2007-060R2 and are valid as of February 2007. Test

scripts should be derived on a carrier by carrier basis using frameworks 2.94, SIP INVITE to ISUP IAM Mappings, and 2.95, ISUP IAM to SIP INVITE Mappings, in this document along with the PTSC-SAC-2007-060R2.

NGIIF Test #:

ANSI T1.236 Test #:

TR-905 Test #

1.5 Circuit Validation Test (CVT)	I-1.1	Circuit Validation Test (CVT)

REFERENCE: ANSI T1.113, chapter 3, tables 6D, 18; ANSI T1.113, chapter 4, annex C.3

TITLE: Circuit Validation Test (CVT)

PURPOSE: To verify the correct response to a CVT message.

PRE-TEST CONDITIONS: A stable MTP signaling relation and the circuit (under test) exist between SP B and SP A.

CONFIGURATION: 1

MESSAGE SEQUENCE:

SP B

SP A

CVT----->

<----- CVR

TEST DESCRIPTION:

1. Send a CVT message from SP B to SP A for the circuit being tested.
2. Verify that a Circuit Validation Response (CVR) message is returned from SP A to SP B concerning the circuit being tested.
3. Verify correct coding of parameters in the CVT and CVR messages.
4. The state of the circuit under test should be checked upon completion of this test.

NGIIF Test #:

ANSI T1.236 Test #:

TR-905 Test #

1.6 Continuity Check Request (CCR)	I-2.1	Continuity Check Request (CCR)

REFERENCE: ANSI T1.113, chapter 3, table 18; ANSI T1.113, chapter 4, annex B

TITLE: Continuity Check Request (CCR)

PURPOSE: To verify that the continuity check for the circuit under test is to be properly performed in response to a CCR message.

PRE-TEST CONDITIONS: A stable MTP signaling relation and the circuit (under test) exist between SP B and SP A.

CONFIGURATION: 1

MESSAGE SEQUENCE:

SP B

SP A

CCR ----->

<----- LPA

TEST DESCRIPTION:

1. Send a CCR message from SP B to SP A for the circuit being tested.
2. Verify that a Loop Back Acknowledgment (LPA) message is returned from SP A to SP B concerning the circuit being tested.
3. Verify that the continuity check is successfully performed on the circuit.

NGIIF Test #:

ANSI T1.236 Test #:

TR-905 Test #

1.7 Continuity Test - Successful

I-2.2

Continuity Test - Successful

REFERENCE: ANSI T1.113, chapter 3, tables 9, 14; ANSI T1.113, chapter 4, subclause 2.1.6

TITLE: Continuity Test Successful - Initial Address Message (IAM)

PURPOSE: To verify that the continuity check for the circuit under test is to be properly performed in response to a request for continuity check in the IAM.

PRE-TEST CONDITIONS: A stable MTP signaling relation and the circuit (under test) exist between SP B and SP A.

CONFIGURATION: 1

MESSAGE SEQUENCE:

SP B

SP A

IAM ----->

cc request

--

| -check loop

--

COT ----->

cc successful

TEST DESCRIPTION:

1. Send an IAM from SP B to SP A requesting continuity check for the circuit under test.
2. SP A shall connect a continuity-check loop to the circuit.
3. Verify that the continuity check is successfully performed on the circuit.
4. Verify that a Continuity (COT) message with a successful indication is received by SP A from SP B.

NGIIF Test #:

ANSI T1.236 Test #:

TR-905 Test #

1.8 2.4 Continuity Test - Unsuccessful	I-2.3	Continuity Test - Unsuccessful

REFERENCE: ANSI T1.113, chapter 3, tables 9, 14, 18; ANSI T1.113, chapter 4, table 3, subclause 2.1.6, annex B

TITLE: Continuity Test Unsuccessful - Initial Address Message (IAM)

PURPOSE: To verify that the continuity check for the circuit under test fails in response to a request for continuity check in the IAM.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A. The circuit (under test) is pre-conditioned so as to cause the continuity test to fail.

CONFIGURATION: 1

MESSAGE SEQUENCE:

```

SP B                                     SP A
IAM ----->
cc request
COT ----->
cc unsuccessful
CCR ----->
<----- LPA

```

TEST DESCRIPTION:

1. Send an IAM from SP B to SP A requesting continuity check for the circuit under test.
2. Verify that a Continuity (COT) message with an unsuccessful indication is received by SP A from SP B.
3. Verify that a Continuity Check Request (CCR) message is received by SP A from SP B before the 20-second timer $T_{CCR,r}$ expires.
4. Verify that a Look Back Acknowledgment message (LPA) is received by SP B from SP A.

Note: The continuity recheck procedure (steps 2, 3 and 4) should be repeated until either the continuity test passes or maintenance intervenes.

Note: When continuity recheck procedure is repeated T_{27} (>3 minutes) instead of $T_{CCR,r}$ shall be used in step 3.

NGIIF Test #:

ANSI T1.236 Test #:

TR-905 Test #

1.9 Continuity Test - Previous Circuit - IAM	I-2.4	Continuity Test - Previous Circuit - IAM

REFERENCE: ANSI T1.113, chapter 3, tables 9, 14; ANSI T1.113, chapter 4, subclause 2.1.6

TITLE: Continuity Test on Previous Circuit - Initial Address Message (IAM)

PURPOSE: To verify the proper response to the continuity-check-on-previous-circuit request in the IAM.

PRE-TEST CONDITIONS: A stable MTP signaling relation and the circuit (under test) exist between SP B and SP A. A continuity test is being performed on a previous circuit incoming to SP B, and SP B is awaiting a Continuity (COT) message from SP C.

CONFIGURATION: 2

MESSAGE SEQUENCE:

SP C	SP B	SP A
IAM ----->	IAM ----->	
cc ind	cc previous ckt	
COT ----->	COT ----->	
	cc successful	

TEST DESCRIPTION:

1. Send an IAM from SP B to SP A indicating continuity-check-on-previous circuit.
2. Verify that upon receiving a Continuity (COT) message with a successful indication from SP C, SP B shall send to SP A a COT message with a successful indication.

Note: A continuity check is not performed for the circuit between SP B and SP A.

NGIIF Test #:

ANSI T1.236 Test #:

TR-905 Test #

**1.10 Continuity Test -
Successful CRM**

I-2.5

Continuity Test - Successful CRM

REFERENCE: ANSI T1.113, chapter 3, tables 6C, 9, 18; ANSI T1.113, chapter 4, subclause 2.1.3B

TITLE: Continuity Test Successful - Circuit Reservation Message (CRM)

PURPOSE: To verify the proper responses to 1.) the CRM, and 2.) the continuity check request in the CRM.

PRE-TEST CONDITIONS: A stable MTP signaling relation and the circuit (under test) exist between SP B and SP A. SP B has an incoming MF circuit.

CONFIGURATION: 2

MESSAGE SEQUENCE:

```
SP B                                     SP A
CRM ----->
cc request
      <----- CRA
                                     --
                                     |-check loop
                                     --

COT ----->
cc successful
```

TEST DESCRIPTION:

1. Send a CRM from SP B to SP A indicating continuity check on the circuit (under test).
2. Verify that a Circuit Reservation Acknowledgment (CRA) message is sent from SP A to SP B.
3. Verify that upon completion of the continuity check, a Continuity (COT) message is sent from SP B to SP A.

Note: The CRA message may precede, or follow the receipt of a COT message.

1.11 Continuity Test - Unsuccessful - CRM	I-2.6	Continuity Test - Unsuccessful - CRM

REFERENCE: ANSI T1.113, chapter 3, tables 6C, 9, 18; ANSI T1.113, chapter 4, subclause 2.1.3B

TITLE: Continuity Test Unsuccessful - Circuit Reservation Message (CRM)

PURPOSE: To verify the proper response to the CRM, and to verify that the continuity check for the circuit under test fails in response to a request for continuity check in the CRM

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A. The circuit (under test) is pre-conditioned so as to cause the continuity test to fail. SP B has an incoming MF circuit.

CONFIGURATION: 2

MESSAGE SEQUENCE:

```

SP B                                     SP A
CRM ----->
cc request
    <----- CRA
COT ----->
cc unsuccessful
CCR ----->
    <----- LPA

```

TEST DESCRIPTION:

1. Send a CRM from SP B to SP A indicating continuity check on the circuit (under test).
2. *Verify that a Circuit Reservation Acknowledgment (CRA) message is sent from SP A to SP B.
3. *Verify that a Continuity (COT) message is sent from SP B to SP A indicating that the continuity check fails.
4. Verify that a Continuity Check Request (CCR) message is received by SP A from SP B before the 20-second timer $T_{CCR,r}$ expires.
5. Verify that a Loop Back Acknowledgment message (LPA) is received by SP B from SP A.
6. **The continuity recheck procedure (steps 3, 4 and 5) should be repeated until either the continuity test passes or maintenance intervenes.

*Note: The CRA message may precede, or follow the receipt of a COT message.

**Note: When continuity recheck procedure is repeated, timer T_{27} (>3 minutes) instead of $T_{CCR,r}$ shall be used in step 4.

1.12 Single Circuit Block/Unblock - BLO/UBL	I-3.1	Single Circuit Block/Unblock - BLO/UBL

REFERENCE: ANSI T1.113, chapter 3, tables 6B, 18, 21; ANSI T1.113, chapter 4, subclause 2.8.2

TITLE: Single Circuit Blocking/Unblocking - BLO/UBL

PURPOSE: To verify the proper response to the Blocking and Unblocking on the circuit under test.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A. The circuit (under test) has a circuit state, e.g., idle, prior to the test.

CONFIGURATION: 1

MESSAGE SEQUENCE:

SP B	SP A
CQM ----->	
	<----- CQR
BLO ----->	
	<----- BLA
CQM ----->	
	<----- CQR
UBL ----->	
	<----- UBA
CQM ----->	
	<----- CQR

TEST DESCRIPTION:

1. Send a Circuit Query Message (CQM) from SP B to SP A for the circuit under test.
2. Verify that a Circuit Query Response (CQR) message is sent from SP A to SP B, and the state of the circuit carried in the CQR is correct.
3. Send a Blocking (BLO) message from SP B to SP A for the circuit under test.
4. Verify that a Blocking Acknowledgment (BLA) message is sent from SP A to SP B.
5. Send a Circuit Query Message (CQM) from SP B to SP A for the circuit under test.
6. Verify that a Circuit Query Response (CQR) message is sent from SP A to SP B, and the state of the circuit carried in the CQR is "remotely blocked" at SP A.
7. Send an Unblocking (UBL) message from SP B to SP A for the circuit under test.
8. Verify that a Unblocking Acknowledgment (UBA) message is sent from SP A to SP B.
9. Send a Circuit Query Message (CQM) from SP B to SP A for the circuit under test.
10. Verify that a Circuit Query Response (CQR) message is sent from SP A to SP B and the state of the circuit carried in the CQR shall be the same as that prior to the test.

1.13 Single Circuit Block/Reset Circuit/Unblock - BLO/RSC/UBL	I-3.2	Single Circuit Block/Reset Circuit/Unblock - BLO/RSC/UBL

REFERENCE: ANSI T1.113, chapter 3, tables 6B, 18, 21; ANSI T1.113, chapter 4, subclauses 2.8.2, 2.9.3

TITLE: Single Circuit Blocking/Reset Circuit/Unblocking - BLO/RSC/UBL

PURPOSE: To verify the proper responses to the Blocking, Rest Circuit and Unblocking on the circuit under test.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A. The circuit (under test) has a circuit state, e.g., idle, prior to the test.

CONFIGURATION: 1

MESSAGE SEQUENCE:

SP B		SP A
CQM ----->		
	<-----	CQR
BLO ----->		
	<-----	BLA
CQM ----->		
	<-----	CQR
RSC ----->		
	<-----	RLC
CQM ----->		
	<-----	CQR
UBL ----->		
	<-----	UBA
CQM ----->		
	<-----	CQR
	<-----	BLO
BLA ----->		
CQM ----->		
	<-----	CQR
RSC ----->		
	<-----	BLO
	<-----	RLC
BLA ----->		
	<-----	CQM
CQR ----->		
	<-----	UBL
UBA ----->		
	<-----	CQM
CQR ----->		

TEST DESCRIPTION:

1. Send a Circuit Query Message (CQM) from SP B to SP A for the circuit under test.
2. Verify that a Circuit Query Response (CQR) message is sent from SP A to SP B, and the state of the circuit carried in the CQR is correct, e.g., idle.
3. Send a Blocking (BLO) message from SP B to SP A for the circuit under test.
4. Verify that a Blocking Acknowledgment (BLA) message is sent from SP A to SP B.
5. Send a Circuit Query Message (CQM) from SP B to SP A for the circuit under test.
6. Verify that a Circuit Query Response (CQR) message is sent from SP A to SP B, and the state of the circuit carried in the CQR is "remotely blocked" at SP A.
7. Send a Reset Circuit (RSC) message from SP B to SP A for the circuit under test.
8. Verify that a Release Complete (RLC) message is sent from SP A to SP B.
9. Send a Circuit Query Message (CQM) from SP B to SP A for the circuit under test.
10. Verify that a Circuit Query Response (CQR) message is sent from SP A to SP B, indicating that the circuit is back in its original state, e.g., idle, with the "remotely blocked" state removed at SP A.
11. Send a Unblocking (UBL) message from SP B to SP A for the circuit under test.
12. Verify that a Unblocking Acknowledgment (UBA) message is sent from SP A to SP B.
13. Send a Circuit Query Message (CQM) from SP B to SP A for the circuit under test.
14. Verify that a Circuit Query Response (CQR) message is sent from SP A to SP B, indicating that the circuit is in its original state, e.g., idle.
15. Send a Blocking (BLO) message from SP A to SP B for the circuit under test.
16. Verify that a Blocking Acknowledgment (BLA) message is sent from SP B to SP A.
17. Send a Circuit Query Message (CQM) from SP B to SP A for the circuit under test.
18. Verify that a Circuit Query Response (CQR) message is sent from SP A to SP B and the state of the circuit carried in the CQR is "locally blocked" at SP A.
19. Send a Reset Circuit (RSC) message from SP B to SP A for the circuit under test.
20. Send a Blocking (BLO) message from SP A to SP B for the circuit under test.
21. Verify that a Release Complete (RLC) message is sent from SP A to SP B before or after a Blocking Acknowledgment (BLA) message is received by SP A.
22. Send a Circuit Query Message (CQM) from SP A to SP B for circuit under test.
23. Verify that a Circuit Query Response (CQR) message is sent from SP B to SP A and the state of the circuit carried in the CQR is "remotely blocked" at SP B.
24. Send a Unblocking (UBL) message from SP A to SP B for the circuit under test.
25. Verify that an Unblocking Acknowledgment (UBA) message is sent from SP B to SP A.
26. Send a Circuit Query Message (CQM) from SP A to SP B for the circuit under test.
27. Verify that a Circuit Query Response (CQR) message is sent from SP B to SP A, indicating that the circuit is in its original state (e.g., idle).

1.14 Block/Unblock from Call Originating End - BLO/BLU	I-3.3	Block/Unblock from Call Originating End - BLO/BLU

REFERENCE: ANSI T1.113, chapter 3, tables 5, 6, 14, 14A, 18; ANSI T1.113, chapter 4, subclauses 2.1, 2.3.1, 2.8.2

TITLE: Blocking/Unblocking from Call Originating End - BLO/UBL

PURPOSE: To verify the proper responses to the Blocking on the circuit when the call is active, and Unblocking on the same circuit when the call is released.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A. There may be signaling points preceding SP B, and succeeding SP A to establish an end-to-end call.

CONFIGURATION: 1

MESSAGE SEQUENCE:

SP B		SP A
IAM	----->	
	<-----	ACM
	<-----	ANM
	-----connectivity-----	
BLO	----->	
	<-----	BLA
REL	----->	
	<-----	RLC
UBL	----->	
	<-----	UBA

TEST DESCRIPTION:

1. Initiate a call from SP B to SP A.
2. Verify that the Initial Address Message (IAM), Address Complete (ACM), and Answer Message (ANM) are properly sent and received, and that the circuit connectivity is made.
3. Send a Blocking (BLO) message from SP B to SP A for the circuit.
4. Verify that a Blocking Acknowledgment (BLA) message is sent from SP A to SP B and that the connectivity is still established.
5. Release the call by sending a Release (REL) message from SP B to SP A.
6. Verify that a Release Complete (RLC) message is sent from SP A to SP B, and that a call

cannot be originated from SP A.

7. Send a Unblocking (UBL) message from SP B to SP A for the circuit under test.
8. Verify that a Unblocking Acknowledgment (UBA) message is sent from SP A to SP B, and that either SP A or SP B can originate a call over this circuit.

1.15 Block/Unblock from Call Receiving End - BLO/UBL	I-3.4	Block/Unblock from Call Receiving End - BLO/UBL

REFERENCE: ANSI T1.113, chapter 3, tables 5, 6, 14, 14A, 18; ANSI T1.113, chapter 4, subclauses 2.1, 2.3.1, 2.8.2

TITLE: Blocking/Unblocking from Call Receiving End - BLO/UBL

PURPOSE: To verify the proper responses to the Blocking on the circuit when the call is active, and the Unblocking on the same circuit when the call is released.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A. There may be signaling points preceding SP B, and succeeding SP A to establish an end-to-end call.

CONFIGURATION: 1

MESSAGE SEQUENCE:

SP B	SP A
IAM ----->	
	<----- ACM
	<----- ANM
	-----connectivity-----
	<----- BLO
BLA ----->	
REL ----->	
	<----- RLC
	<----- UBL
UBA ----->	

TEST DESCRIPTION:

1. Initiate a call from SP B to SP A.
2. Verify that the Initial Address Message (IAM), Address Complete Message (ACM), and Answer Message (ANM) are properly sent and received, and that the circuit connectivity is made.
3. Send a Blocking (BLO) message from SP A to SP B for the circuit.
4. Verify that a Blocking Acknowledgment (BLA) message is sent from SP B to SP A, and that the connectivity is still established.
5. Release the call by sending a Release (REL) message from SP B to SP A.

6. Verify that a Release Complete (RLC) message is sent from SP A to SP B, and that a call cannot be originated from SP B.
7. Send a Unblocking (UBL) message from SP A to SP B for the circuit under test.
8. Verify that a Unblocking Acknowledgment (UBA) message is sent from SP B to SP A, and that either SP B or SP A can originate a call over this circuit.

1.16 Circuit Group Blocking/Unblocking - CGB/CGU (Block Without Release)	I-4.1	Circuit Group Blocking/Unblocking - CGB/CGU (Block Without Release)

REFERENCE: ANSI T1.113, chapter 3, tables 6B, 20, 21; ANSI T1.113, chapter 4, subclause 2.8.2.2

TITLE: Circuit Group Blocking/Unblocking - CGB/CGU (Block Without Release)

PURPOSE: To verify the proper responses to the Circuit Group Blocking (block without release or maintenance oriented) and Circuit Group Unblocking on the concerned circuits.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A. The circuits (under test) are idle.

CONFIGURATION: 1

MESSAGE SEQUENCE:

```

SP B                                SP A
CQM ----->
<----- CQR
--
--
--
--

CGB** ----->
CGB** ----->
<----- CGBA**
CQM ----->
<----- CQR
--
--
--
--

CGU ----->
<----- CGUA

CQM ----->
<----- CQR
--
--

```

--
--

TEST DESCRIPTION:

1. Send Circuit Query Message (CQM) from SP B to SP A for the circuits under test.
2. Verify that Circuit Query Response (CQR) messages are sent from SP A to SP B, and the states of the circuits carried in the CQR are correct.
3. Send a Circuit Group Blocking (CGB) message from SP B to SP A with the Range/Status field specified to cover the circuits under test, and the Circuit Group Supervision message Type Indicator to "block without release".
4. Send an identical Circuit Group Blocking (CGB) message from SP B to SP A within 5 seconds.
5. **Verify that a Circuit Group Blocking Acknowledgment (CGBA) message is sent from SP A to SP B, and that the received CGBA at SP B matches the Trunk Circuit Identification Code (TCIC*), Circuit Group Supervision Message Type Indicator, and Range/Status field of the previously sent CGB message.
6. Send Circuit Query Message (CQM) from SP B to SP A for the circuits under test.
7. Verify that Circuit Query Response (CQR) messages are sent from SP A to SP B, and the circuit states of the concerned circuits are "remotely blocked" at SP A.
8. Send a Circuit Group Unblocking (CGU) message from SP B to SP A with the Range/Status field specified to cover the circuits under test, and the Circuit Group Supervision Message Type Indicator set to "block without release".
9. Verify that a Circuit Group Unblocking Acknowledgment (CGUA) message is sent from SP A to SP B, and that the received CGUA at SP B matches the Trunk Circuit Identification Code (TCIC*), Circuit Group Supervision Message Type Indicator, and Range/Status field of the previously sent CGU message.
10. Send Circuit Query Message (CQM) from SP B to SP A for the circuits under test.
11. Verify that Circuit Query Response (CQR) messages are sent from SP A to SP B, and the circuit states of the concerned circuits are idle and no longer "remotely blocked" at SP A.

*Note: TCIC is also known as CIC in ANSI T1 standards.

**Note: Optionally, SP A can send a CGBA to SP B after the first CGB is received, and discard the second CGB received. Or, SP A can send a CGBA to SP B after each CGB is received.

1.17 Circuit Group Blocking/Unblocking - CGB/CGU (Block With Immediate Release)	I-4.2	Circuit Group Blocking/Unblocking - CGB/CGU (Block With Immediate Release)

REFERENCE: ANSI T1.113, chapter 3, tables 6B, 20, 21; ANSI T1.113, chapter 4, subclause 2.8.2.2

TITLE: Circuit Group Blocking/Unblocking - CGB/CGU (Block With Immediate Release)

PURPOSE: To verify the proper responses to the Circuit Group Blocking (block with immediate release or hardware oriented) and Circuit Group Unblocking on the concerned circuits.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A. The circuits (under test) are idle.

CONFIGURATION: 1

MESSAGE SEQUENCE:

SP B SP A

CQM ----->
 <----- CQR

--
 --
 --
 --

CGB + ----->
 CGB + ----->
 <----- CGBA +

CQM ----->
 <----- CQR

--
 --
 --
 --

CGU ----->
 <----- CGUA

CQM ----->
 <----- CQR

--
--
--

--

TEST DESCRIPTION:

1. Send Circuit Query Message (CQM) from SP B to SP A for the circuits under test.
2. Verify that Circuit Query Response (CQR) messages are sent from SP A to SP B, and the states of the circuits carried in the CQR are correct.
3. Send a Circuit Group Blocking (CGB) message from SP B to SP A with the Range/Status field specified to cover the circuits under test, and the Circuit Group Supervision Message Type Indicator set to "block with immediate release".
4. Send an identical circuit Group Blocking (CGB) message from SP B to SP A within 5 seconds.
5. + (See notes.) Verify that a Circuit Group Blocking Acknowledgment (CGBA) message is sent from SP A to SP B, and that the received CGBA at SP B matches the Trunk Circuit Identification Code (TCIC), Circuit Group Supervision Message Type Indicator, and Range/Status field of the previously sent CGB message.
6. Send Circuit Query Message (CQM) from SP B to SP A for the circuits under test.
7. Verify that Circuit Query Response (CQR) messages are sent from SP A to SP B, and the circuit states of the concerned circuits are "remotely blocked" at SP A.
8. Send a Circuit Group Unblocking (CGU) message from SP B to SP A with the Range/Status field specified to cover the circuits under test, and the Circuit Group Supervision Message Type Indicator set to "block with immediate release".
9. Verify that a Circuit Group Unblocking Acknowledgment (CGUA) message is sent from SP A to SP B, and that the received CGUA at SP B matches the Trunk Circuit Identification Code (TCIC), Circuit Group Supervision Message Type Indicator, and Range/Status field of the previously sent CGU message.
10. Send Circuit Query Message (CQM) from SP B to SP A for the circuits under test.
11. Verify that Circuit Query Response (CQR) messages are sent from SP A to SP B, and the circuit states of the concerned circuits are idle and no longer "remotely blocked" at SP A.

Note: If there is a circuit connection, the receiving SP A of the CGB message should release the circuits without the exchange of any release messages.

Note: TCIC is also known as CIC in ANSI T1 standards.

+Note: Optionally, SPA can send a CGBA to SP B after the first CGB is received, and discard the second CGB. Or SP A can send a CGBA to SP B after each CGB is received.

1.18 Reset Circuit - during an Established Outgoing Call - RSC	I-5.1	Reset Circuit - during an Established Outgoing Call - RSC

REFERENCE: ANSI T1.113, chapter 3, tables 5, 6, 6B, 14, 18, 21; ANSI T1.113, chapter 4, subclauses 2.1, 2.9.3.1

TITLE: Reset Circuit from Call Receiving End - RSC

PURPOSE: To verify the proper responses when Reset Circuit is initiated at the call receiving end.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A. There may be signaling points preceding SP B, and succeeding SP A to establish an end-to-end call.

CONFIGURATION: 1

MESSAGE SEQUENCE:

SP B		SP A
IAM	----->	
	<-----	ACM
	<-----	ANM
	-----connectivity-----	
	<-----	RSC
RLC	----->	
	<-----	CQM
CQR	----->	

TEST DESCRIPTION:

1. Send an Initial Address Message (IAM) from SP B to SP A for the circuit under test.
2. Verify that an Address Complete Message (ACM) and an Answer Message (ANM) are sent from SP A, and the circuit connectivity is made.
3. Send a Reset Circuit (RSC) message from SP A to SP B for the circuit under test.
4. Verify that a Release Complete (RLC) message is sent from SP B.
5. Send a Circuit Query Message (CQM) from SP A to SP B for the circuit under test.
6. Verify that a Circuit Query Response (CQR) message is sent from SP B to SP A, and the circuit state of the circuit under test is idle.

1.19 Reset Circuit - During an Established Incoming Call - RSC	I-5.2	Reset Circuit - During an Established Incoming Call - RSC

REFERENCE: ANSI T1.113, chapter 3, tables 5, 6, 6B, 14, 18, 21; ANSI T1.113, chapter 4, subclauses 2.1, 2.9.3.1

TITLE: Reset Circuit from Call Originating End - RSC

PURPOSE: To verify the proper responses when Reset Circuit is initiated at the call originating end.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A. There may be signaling points preceding SP B, and succeeding SP A to establish an end-to-end call.

CONFIGURATION: 1

MESSAGE SEQUENCE:

SP B		SP A
IAM	----->	
	<-----	ACM
	<-----	ANM
	-----connectivity-----	
RSC	----->	
	<-----	RLC
CQM	----->	
	<-----	CQR

TEST DESCRIPTION:

1. Send an Initial Address Message (IAM) from SP B to SP A for the circuit under test.
2. Verify that an Address Complete Message (ACM) and an Answer Message (ANM) are sent from SP A, and the circuit connectivity is made.
3. Send a Reset Circuit (RSC) message from SP B to SP A for the circuit under test.
4. Verify that a Release Complete (RLC) message is sent from SP A.
5. Send a Circuit Query Message (CQM) from SP B to SP A for the circuit under test.
6. Verify that a Circuit Query Response (CQR) message is sent from SP A to SP B, and the circuit state of the circuit under test is idle.

1.20 Dual Seizure

I-7.1.

Dual Seizure

REFERENCE: ANSI T1.113, chapter 3, tables 5, 6, 14, 14A, 18; ANSI T1.113, chapter 4, subclauses 2.1, 2.9.1

TITLE: Dual Seizure

PURPOSE: To verify the proper responses when a dual seizure of the circuit occurs.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A. There may be signaling points preceding SP B, and succeeding SP A to establish an end-to-end call.

CONFIGURATION: 1

MESSAGE SEQUENCE:

SP B

SP A

IAM(cic=x) -----> <----- IAM(cic=x)

ACM(cic=x) ----->

ANM(cic=x) ----->

-----connectivity-----

IAM(cic=y) ----->

<----- ACM(cic=y)

<----- ANM(cic=y)

-----connectivity-----

REL(cic=y) ----->

<----- RLC(cic=y)

<----- REL(cic=x)

RLC(cic=x) ----->

TEST DESCRIPTION:

1. *Send Initial Address Message (IAM) from both SP B and SP A at the same time for the circuit under test.
2. Upon detection of a dual seizure by the control (glaremaster) signaling point, SP A, it discards the incoming IAM and lets the outgoing IAM to proceed in a normal manner.
3. Verify that an Address Complete Message (ACM) and an Answer Message (ANM) are sent from SP B to SP A and the circuit connectivity is made.
4. At SP B, the original call is reattempted over another circuit by sending an Initial Address Message (IAM) from SP B to SP A.
5. Verify that an Address Complete Message (ACM) and an Answer Message (ANM) are sent from SP A to SP B and the circuit connectivity is made.
6. Release the circuit (cic=y) at SP B and verify the exchange of Release (REL) and Release Complete (RLC) messages.

7. Release the circuit (cic=x) at SP A and verify the exchange of Release (REL) and Release Complete (RLC) messages.

*Note: Multiple attempts may be required to reach the desired results.

NGIIF Test #:

ANSI T1.236 Test #:

TR-905 Test #

1.21 Call to Idle Test Line	I-8.1.	Call to Idle Test Line

REFERENCE: ANSI T1.113, chapter 3, tables 5, 6, 14, 14A, 18; ANSI T1.113, chapter 4, annex C, C.1

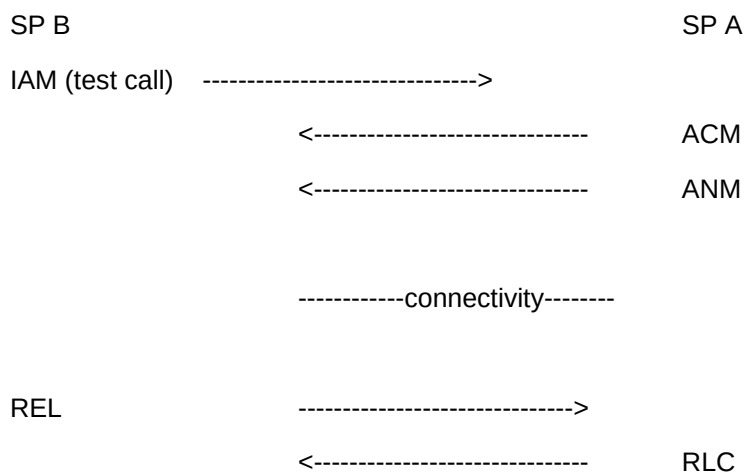
TITLE: Call to an Idle Test Line

PURPOSE: To verify the proper responses of a call to an idle test line

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A. There may be signaling points preceding SP B and succeeding SP A for an end-to-end test call. The test line on the side of SP A is idle.

CONFIGURATION: 1

MESSAGE SEQUENCE:



TEST DESCRIPTION:

1. Send a test with an Initial Address Message (IAM) from SP B to SP A. The test line is one of those specified in T1.113.4 Annex C, e.g., milliwatt test line (type 102).
2. Verify that an Address Complete Message (ACM) and Answer Message (ANM) are sent from SP A to SP B.
3. Verify that the circuit connection is established, and the desirable test is to be performed.
4. Release the circuit when the test is done, and verify the exchange of Release (REL) and Release Complete (RLC) messages.

NGIIF Test #:

ANSI T1.236 Test #:

TR-905 Test #

1.22 Call to Busy Test Line	I-8.2	Call to Busy Test Line

REFERENCE: ANSI T1.113, chapter 3, tables 14, 14A, 18; ANSI T1.113, chapter 4, annex C, C.1

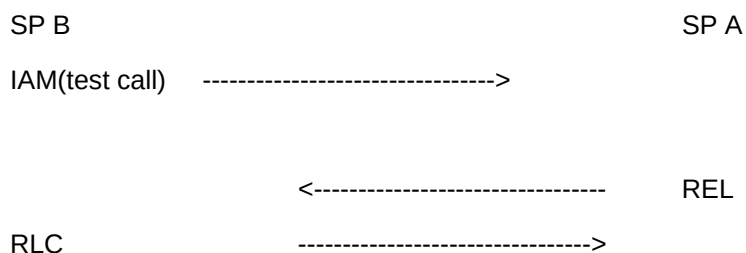
TITLE: Call to a Busy Test Line

PURPOSE: To verify the proper responses of a call to a busy test line

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A. There may be signaling points preceding SP B and succeeding SP A for an end-to-end test call. The test line on the side of SP A is busy.

CONFIGURATION: 1

MESSAGE SEQUENCE:



TEST DESCRIPTION:

1. Send a test call with an Initial Address Message (IAM) from SP B to SP A. The test line is one of those specified in T1.113.4 Annex C, e.g., milliwatt test line (type 102).
2. Verify that a Release (REL) message with a cause value of "user busy" is sent from SP A to SP B.
3. Verify that a Release Complete (RLC) message is sent from SP B to SP A.

TR-905 Test #

1.24 Tones and Announcements - Busy Line	I-9.1.	Tones and Announcements - Busy Line

Call Set-up Tests

REFERENCE: ANSI T1.113, chapter 3, tables 5, 14, 14A, 18; ANSI T1.113, chapter 4, subclause 2.2.4

TITLE: Tone and Announcements - Busy Line

PURPOSE: To verify the proper tones and announcements when the called line is busy.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A. There may be signaling points preceding SP B and succeeding SP A for an end-to-end call. The called line is busy.

CONFIGURATION: 1

MESSAGE SEQUENCE:

```

SP B                                     SP A
IAM  ----->
      <----- ACM
      <-----busy tones & announcements----->
      <----- REL
RLC  ----->

```

TEST DESCRIPTION:

1. Send an Initial Address Message (IAM) from SP B to SP A.
2. Verify that an Address Complete Message (ACM) is sent from SP A to SP B, carrying the cause value of "user busy" and the inband information indicator set to "1" in the Optional Backward Call Indicator parameter.
3. *Based on the cause value of "user busy" in the Release (REL) message from the signaling point on the called party side, SP A may apply busy tones and announcements toward SP B.
4. **Verify that a Release (REL) message is sent from SP A to SP B.
5. Verify that a Release Complete (RLC) message is sent from SP B to SP A.

* Note: Based on intercompany agreements, the signaling point SP A (in a transit network) exercises the right to intercept the REL message, and apply a busy tone/announcement.

**Note: SP A can only send a Release (REL) message if the calling party has not yet disconnected and a time-out period at SP A associated with tone and announcements is exceeded. Otherwise, a REL message will be sent from SP B to SP A.

1.25 Tones and Announcements - Unallocated Number	I-9.2.	Tones and Announcements - Unallocated Number

REFERENCE: ANSI T1.113, chapter 3, tables 5, 14, 14A, 18; ANSI T1.113, chapter 4, subclause 2.2.4

TITLE: Tones and Announcements - Unallocated Number

PURPOSE: To verify the proper tones and announcements when the called number is unallocated.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A. There may be signaling points preceding SP B and succeeding SP A for an end-to-end call. The called number is unallocated.

CONFIGURATION: 1

MESSAGE SEQUENCE:

```

SP B                                     SP A
IAM  ----->
      <----- ACM
      <-----tones & announcements-----
      <----- REL
RLC  ----->

```

TEST DESCRIPTION:

1. Send an Initial Address Message (IAM) from SP B to SP A.
2. Verify that an Address Complete Message (ACM) is sent from SP A to SP B, carrying the cause value of "unallocated number" and the inband information indicator set to "1" in the Optional Backward Call Indicator parameter.
3. *Based on the cause value of "unallocated number" in the Release (REL) message from the signaling point on the called party side, SP A may apply the proper tones and announcements toward SP B.
4. **Verify that a Release (REL) message is sent from SP A to SP B.
5. Verify that a Release Complete (RLC) message is sent from SP B to SP A.

*Note: Based on intercompany agreements, the signaling point SP A (in a transit network) exercises the right to intercept the REL message, and apply a tone/announcement.

**Note: SP A can only send a Release (REL) message if the calling party has not yet disconnected and a time-out period at SP A associated with tone and announcements is exceeded. Otherwise, a REL message will be sent from SP B to SP A.

1.26 Tone and Announcements - No Circuit Available	I-9.3.	Tone and Announcements - No Circuit Available

REFERENCE: ANSI T1.113, chapter 3, tables 5, 14, 14A, 18; ANSI T1.113, chapter 4, subclause 2.2.4

TITLE: Tones and Announcements - No Circuit Available

PURPOSE: To verify the proper tones and announcements when no outgoing circuits are available.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A. The outgoing circuits at SP A are conditioned so that no circuits are available for the incoming call.

CONFIGURATION: 1

MESSAGE SEQUENCE:

```

SP B                               SP A
IAM  ----->
      <----- ACM
      <-----tone & announcements-----
      <----- REL
RLC  ----->

```

TEST DESCRIPTION:

1. Send an Initial Address Message (IAM) from SP B to SP A.
2. Verify that an Address Complete Message (ACM) is sent from SP A to SP B, carrying the cause value of "no circuit available" and the inband information indicator set to "1" in the Optional Backward Call Indicator parameter.
3. *SP A applies the proper tones and announcements toward SP B indicating no circuit available.
4. **Verify that a Release (REL) message is sent from SP A to SP B.
5. Verify that a Release Complete (RLC) message is sent from SP B to SP A.

*Note: The signaling point SP A (in a transit network) exercises the right to apply its own tone/announcement.

**Note: SP A can only send a Release (REL) message if the calling party has not yet disconnected and a time-out period at SP A associated with tone and announcements is exceeded. Otherwise, a REL message will be sent from SP B to SP A.

NGIIF Test #:

ANSI T1.236 Test #:

TR-905 Test #

1.27 Release - Abandoned Call	I-10.2.	Release - Abandoned Call

REFERENCE: ANSI T1.113, chapter 3, tables 5, 14, 14A, 18; ANSI T1.113, chapter 4, subclause 2.3.1

TITLE: Release - Abandoned Call (Calling Party Disconnect After ACM and before ANM)

PURPOSE: To verify the proper responses when the calling party disconnects after the receipt of an ACM and before the receipt of an ANM.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A. There may be signaling points preceding SP B and succeeding SP A for an end-to-end call.

CONFIGURATION: 1

MESSAGE SEQUENCE:

SP B		SP A
IAM	----->	
	<-----	ACM
REL	----->	
	<-----	RLC

TEST DESCRIPTION:

1. Send an Initial Address Message (IAM) from SP B to SP A.
2. The calling party disconnects after an Address Complete Message (ACM) is received and before the arrival of an Answer Message (ANM) at SP B.
3. Verify that a Release (REL) message is sent from SP B to SP A. The REL message has a cause value of "normal release" and general location of "user".
4. Verify that a Release Complete (RLC) message is sent from SP A to SP B.

NGIIF Test #:

ANSI T1.236 Test #:

TR-905 Test #

1.28 Release - Calling Party	I-10.3.	Release - Calling Party

REFERENCE: ANSI T1.113, chapter 3, tables 5, 6, 14, 14A, 18; ANSI T1.113, chapter 4, subclause 2.1, 2.3.1

TITLE: Release - Calling Party (after the call has been answered)

PURPOSE: To verify the proper responses when the calling party disconnects after the call has been answered.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A. There may be signaling points preceding SP B and succeeding SP A for an end-to-end call.

CONFIGURATION: 1

MESSAGE SEQUENCE:

SP B		SP A
IAM	----->	
	<-----	ACM
	<-----	ANM
	-----connectivity-----	
REL	----->	
	<-----	RLC

TEST DESCRIPTION:

1. Send an Initial Address Message (IAM) from SP B to SP A.
2. Verify that an Address Complete Message (ACM) is received at SP B.
3. Verify that an Answer Message (ANM) is received at SP B, and the circuit connection is made.
4. The calling party disconnects.
5. Verify that a Release (REL) message is sent from SP B to SP A. The REL message has a cause value of "normal release" and general location of "user".
6. Verify that a Release Complete (RLC) message is sent from SP A to SP B.

1.29 Suspend, Resume and Release - Case 1	I-10.4.	Suspend, Resume and Release - Case 1

REFERENCE: ANSI T1.113, chapter 3, tables 5, 6, 14, 14A, 17A, 18; ANSI T1.113, chapter 4, subclause 2.1, 2.5, table 3

TITLE: Suspend, Resume, and Release - Case 1

PURPOSE: To verify the proper responses to the Suspend, Resume and Release messages. This shall only apply to those test cases where the suspend/resume indicator is set to "network initiated." This test case is network initiated and should not be attempted if the call party (on the SP A side) is an ISDN user.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A. There may be signaling points preceding SP B and succeeding SP A for an end-to-end call.

CONFIGURATION: 1

MESSAGE SEQUENCE:

SP B		SP A
IAM	----->	
	<-----	ACM
	<-----	ANM
	-----connectivity-----	
	<-----	SUS
-within T6		
	<-----	RES
	-----connectivity-----	
	<-----	SUS
-T6 expires		
	<-----	REL

RLC ----->

TEST DESCRIPTION:

1. Send an Initial Address Message (IAM) from SP B to SP A. Verify that an Address Complete Message (ACM) is received at SP B. Verify that an Answer message (ANM) is received at SP B, and the circuit connection is made.
2. The called party on the side of SP A goes on-hook. Verify that a Suspend (SUS) message is sent from SP A to SP B. Verify that the circuit connection is still established.
3. *The called party goes off-hook within timer T6 (10-32 seconds). Verify that a Resume (RES) message is sent from SP A to SP B. Verify that the circuit connection is still established. The called party on the side of SP A goes on-hook. Verify that a Suspend (SUS) message is sent from SP A to SP B.
4. *The called party stays on-hook and the timer T6 expires. Verify that a Release (REL) message is sent from SP A, and a Release Complete (RLC) message is sent from SP B.

*Note: SP A is the controlling exchange, and thus, controls/operates the T6 timer.

1.30 Suspend, Resume and Release - Case 2	I-10.5.	Suspend, Resume and Release - Case 2

REFERENCE: ANSI T1.113, chapter 3, tables 5, 6, 14, 14A, 17A, 18; ANSI T1.113, chapter 4, subclause 2.1, 2.5, table 3

TITLE: Suspend, Resume, and Release - Case 2

PURPOSE: To verify the proper responses to the Suspend, Resume and Release messages.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP B and SP A. There may be signaling points preceding SP B and succeeding SP A for an end-to-end call.

CONFIGURATION: 1

MESSAGE SEQUENCE:

```

SP B                                     SP A
IAM ----->
<----- ACM
<----- ANM

-----connectivity-----

<----- SUS
|
|
|-within T6
|
|
REL ----->
<----- RLC

```

TEST DESCRIPTION:

1. Send an Initial Address Message (IAM) from SP B to SP A.
2. Verify that an Address Complete Message (ACM) is received at SP B.
3. Verify that an Answer Message (ANM) is received at SP B, and the circuit connection is made.
4. The called party on the side of SP A goes on-hook.
5. Verify that a Suspend (SUS) message is sent from SP A to SP B.
6. Verify that the circuit connection is still established.
7. The calling party on the side of SP B goes on-hook before timer T6 (10-32 seconds) expires.
8. Verify that a Release (REL) message is sent from SP B and a Release Complete (RLC) message is sent from SP A.

NGIIF Test #:

ANSI T1.236 Test #:

TR-905 Test #

<i>1.31 Unsuccessful Call - IAM - no CPN, no CHG, with OLI</i>	I-11.2	Unsuccessful Call - IAM - no CPN, no CHG, with OLI

REFERENCE: ANSI T1.113, chapter 3, tables 14, 14A, 18; ANSI T1.113, chapter 4, subclauses 2.1, 2.2, 2.3, 2.9.5, table 3

TITLE: Unsuccessful Call - IAM - no CPN, no CHG, with OLI

PURPOSE: To verify the proper responses to an IAM without CPN, without CHG and with OLI.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A.

CONFIGURATION: 1

MESSAGE SEQUENCE:

```
SP B                                     SP A
IAM  ----->
(w/CPN)
(w/CHG)
(w/OLI)
      <----- REL
RLC  ----->
```

TEST DESCRIPTION:

1. Send an Initial Address Message (IAM) without a Calling Party Number (CPN), without a Charge Number (CHG), and with an Originating Line Information (OLI) from SP B to SP A.
2. Verify that SP A discards the IAM.
3. *Verify that a Release (REL) message is sent from SP A to SP B.
4. Verify that a Release Complete (RLC) message is sent from SP B to SP A.

*Note: It is also possible that SP A relies on the expiration of timer T7 (20-30 seconds) at SP B to release the circuit, and thus, no REL is sent from SP A.

<i>1.32 Unsuccessful Call - IAM - with CPN, with CHG, no OLI</i>	I-11.3	Unsuccessful Call - IAM - with CPN, with CHG, no OLI

REFERENCE: ANSI T1.113, chapter 3, tables 14, 14A, 18; ANSI T1.113, chapter 4, subclauses 2.1, 2.2, 2.3, 2.9.5, table 3

TITLE: Unsuccessful Call - IAM - CPN, with CHG, no OLI

PURPOSE: To verify the proper responses to an IAM with CPN, with CHG and without OLI.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A.

CONFIGURATION: 1

MESSAGE SEQUENCE:

```

SP B                                     SP A
IAM  ----->
(w/CPN)
(w/CHG)
(wo/OLI)
      <----- REL
RLC  ----->

```

TEST DESCRIPTION:

1. Send an initial Address Message (IAM) with a Calling Party Number (CPN), with a Charge Number (CHG), and without an Originating Line Information (OLI) from SP B to SP A.
2. Verify that SP A discards the IAM.
3. *Verify that a Release (REL) message is sent from SP A to SP B.
4. Verify that a Release Complete (RLC) message is sent from SP B to SP A.

*Note: It is also possible that SP A relies on the expiration of timer T7 (20-30 seconds) at SP B to release the circuit, and thus, no REL is sent from SP A.

NGIIF Test #:

ANSI T1.236 Test #:

TR-905 Test #

1.33 Calling Party Disconnect Before Receipt of ACM	I-10.1.	Calling Party Disconnect Before Receipt of ACM

REFERENCE: ANSI T1.113, chapter 3, tables 14, 14A, 18; ANSI T1.113, chapter 4, subclause 2.3.1

TITLE: Calling Party Disconnect before Receipt on an ACM

PURPOSE: To verify the proper responses when the calling party disconnects before the receipt of an ACM.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A. There may be signaling points preceding SP B and succeeding SP A for an end-to-end call.

CONFIGURATION: 1

MESSAGE SEQUENCE:

```
SP B                                     SP A
IAM  ----->
REL  ----->
      <-----> RLC
```

TEST DESCRIPTION:

1. Send an Initial Address Message (IAM) from SP B to SP A.
2. Upon disconnect by the calling party, verify that a Release (REL) message is sent from SP B to SP A. The REL message has a cause value of "normal release" and general location of "user".
3. Verify that a Release Complete (RLC) message is sent from SP A to SP B.

1.34 Single Circuit Block/Reset Circuit/Unblock - BLO/RSC/UBL (also see NGIIF Test 2.9)	I-3.2	Single Circuit Block/Reset Circuit/Unblock - BLO/RSC/UBL

Intrusive Tests

The tests specified in this part require the use of test equipment installed on signaling links to simulate the action of network elements. CAUTION: Some of the following tests may be disruptive to live signaling traffic and/or call flow.

REFERENCE: ANSI T1.113, chapter 3, tables 6B, 18, 21; ANSI T1.113, chapter 4, subclauses 2.8.2, 2.9.3

TITLE: Single Circuit Blocking/Reset Circuit/Unblocking - BLO/RSC/UBL

PURPOSE: To verify the proper responses to the Blocking, Rest Circuit and Unblocking on the circuit under test.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A. The circuit (under test) has a circuit state, e.g., idle, prior to the test.

CONFIGURATION: 1**SEQUENCE:**

SP B	SP A
CQM ----->	
<-----	CQR
BLO ----->	
<-----	BLA
CQM ----->	
<-----	CQR
RSC ----->	
<-----	RLC
CQM ----->	
<-----	CQR
UBL ----->	
<-----	UBA
CQM ----->	
<-----	CQR
<-----	BLO
BLA ----->	
CQM ----->	
<-----	CQR
RSC ----->	

```

    <----- BLO
    <----- RLC
BLA ----->
    <----- CQM
CQR ----->
    <----- UBL
UBA ----->
    <----- CQM
CQR ----->

```

TEST DESCRIPTION:

1. Send a Circuit Query Message (CQM) from SP B to SP A for the circuit under test.
2. Verify that a Circuit Query Response (CQR) message is sent from SP A to SP B, and the state of the circuit carried in the CQR is correct, e.g., idle.
3. Send a Blocking (BLO) message from SP B to SP A for the circuit under test.
4. Verify that a Blocking Acknowledgement (BLA) message is sent from SP A to SP B.
5. Send a Circuit Query Message (CQM) from SP B to SP A for the circuit under test.
6. Verify that a Circuit Query Response (CQR) message is sent from SP A to SP B, and the state of the circuit carried in the CQR is "remotely blocked" at SP A.
7. Send a Reset Circuit (RSC) message from SP B to SP A for the circuit under test.
8. Verify that a Release Complete (RLC) message is sent from SP A to SP B.
9. Send a Circuit Query Message (CQM) from SP B to SP A for the circuit under test.
10. Verify that a Circuit Query Response (CQR) message is sent from SP A to SP B indicating that the circuit is back in its original state, e.g., idle, with the "remotely blocked" state removed at SP A.
11. Send a Unblocking (UBL) message from SP B to SP A for the circuit under test
12. Verify that a Unblocking Acknowledgement (UBA) message is sent from SP A to SP B.
13. Send a Circuit Query Message (CQM) from SP B to SP A for the circuit under test.
14. Verify that a Circuit Query Response (CQR) message is sent from SP A to SP B, indicating that the circuit is in its original state, e.g., idle.
15. Send a Blocking (BLO) message from SP A to SP B for the circuit under test.
16. Verify that a Blocking Acknowledgement (BLA) message is sent from SP B to SP A.
17. Send a Circuit Query Message (CQM) from SP B to SP A for the circuit under test.
18. Verify that a Circuit Query Response (CQR) message is sent from SP A to SP B and the state of the circuit carried in the CQR is "locally blocked" at SP A.
19. Send a Reset Circuit (RSC) message from SP B to SP A for the circuit under test.
20. Send a Blocking (BLO) message from SP A to SP B for the circuit under test.
21. Verify that a Release Complete (RLC) message is sent from SP A to SP B before or after a Blocking Acknowledgement (BLA) message is received by SP A.
22. Send a Circuit Query Message (CQM) from SP A to SP B for circuit under test
23. Verify that a Circuit Query Response (CQR) message is sent from SP B to SP A and the state of the circuit carried in the CQR is "remotely blocked" at SP B.

24. Send a Unblocking (UBL) message from SP A to SP B for the circuit under test.
25. Verify that an Unblocking Acknowledgement (UBA) message is sent from SP B to SP A.
26. Send a Circuit Query Message (CQM) from SP A to SP B for the circuit under test.
27. Verify that a Circuit Query Response (CQR) message is sent from SP B to SP A, indicating that the circuit is in its original state (e.g., idle).

NGIIF Test #:	ANSI T1.236 Test #:	TR-905 Test #
1.35 Circuit Group Blocking/Unblocking CGB/CGU (Block Without Release) (also see NGIIF Test 2.12)	I-4.1.	Circuit Group Blocking/Unblocking - CGB/CGU (Block Without Release)

REFERENCE: ANSI T1.113, chapter 3, tables 6B, 20, 21; ANSI T1.113, chapter 4, subclause 2.8.2.2

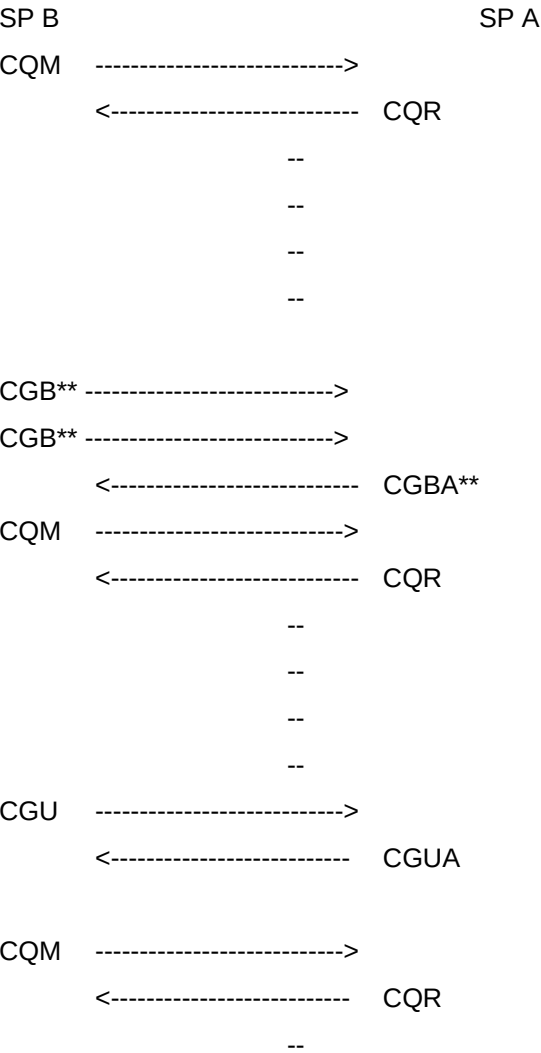
TITLE: Circuit Group Blocking/Unblocking - CGB/CGU (Block Without Release)

PURPOSE: To verify the proper responses to the Circuit Group Blocking (block without release or maintenance oriented) and Circuit Group Unblocking on the concerned circuits.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A. The circuits (under test) are idle.

CONFIGURATION: 1

MESSAGE SEQUENCE:



--
--
--

TEST DESCRIPTION:

1. Send Circuit Query Message (CQM) from SP B to SP A for the circuits under test.
2. Verify that Circuit Query Response (CQR) messages are sent from SP A to SP B, and the states of the circuits carried in the CQR are correct.
3. Send a Circuit Group Blocking (CGB) message from SP B to SP A with the Range/Status field specified to cover the circuits under test, and the Circuit Group Supervision message Type Indicator to "block without release".
4. Send an identical Circuit Group Blocking (CGB) message from SP B to SP A within 5 seconds.
5. **Verify that a Circuit Group Blocking Acknowledgement (CGBA) message is sent from SP A to SP B, and that the received CGBA at SP B matches the Trunk Circuit Identification Code (TCIC*), Circuit Group Supervision Message Type Indicator, and Range/Status field of the previously sent CGB message.
6. Send Circuit Query Message (CQM) from SP B to SP A for the circuits under test.
7. Verify that Circuit Query Response (CQR) messages are sent from SP A to SP B, and the circuit states of the concerned circuits are "remotely blocked" at SP A.
8. Send a Circuit Group Unblocking (CGU) message from SP B to SP A with the Range/Status field specified to cover the circuits under test, and the Circuit Group Supervision Message Type Indicator set to "block without release".
9. Verify that a Circuit Group Unblocking Acknowledgement (CGUA) message is sent from SP A to SP B, and that the received CGUA at SP B matches the Trunk Circuit Identification Code (TCIC*), Circuit Group Supervision Message Type Indicator, and Range/Status field of the previously sent CGU message.
10. Send Circuit Query Message (CQM) from SP B to SP A for the circuits under test.
11. Verify that Circuit Query Response (CQR) messages are sent from SP A to SP B, and the circuit states of the concerned circuits are idle and no longer "remotely blocked" at SP A.

*Note: TCIC is also known as CIC in ANSI T1 standards.

**Note: Optionally, SP A can send a CGBA to SP B after the first CGB is received, and discard the second CGB received. Or, SP A can send a CGBA to SP B after each CGB is received.

1.36 Reset Circuit - during an Established Outgoing Call - RSC (also see NGIIF Test 2.14)	I-5.1	Reset Circuit - during an Established Outgoing Call - RSC

REFERENCE: ANSI T1.113, chapter 3, tables 5, 6, 6B, 14, 18, 21; ANSI T1.113, chapter 4, subclauses 2.1, 2.9.3.1

TITLE: Reset Circuit from Call Receiving End - RSC

PURPOSE: To verify the proper responses when Reset Circuit is initiated at the call receiving end.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A. There may be signaling points preceding SP B, and succeeding SP A to establish an end-to-end call.

CONFIGURATION: 1

MESSAGE SEQUENCE:

SP B		SP A
IAM	----->	
	<-----	ACM
	<-----	ANM
	-----connectivity-----	
	<-----	RSC
RLC	----->	
	<-----	CQM
CQR	----->	

TEST DESCRIPTION:

1. Send an Initial Address Message (IAM) from SP B to SP A for the circuit under test.
2. Verify that an Address Complete Message (ACM) and an Answer Message (ANM) are sent from SP A, and the circuit connectivity is made.
3. Send a Reset Circuit (RSC) message from SP A to SP B for the circuit under test.
4. Verify that a Release Complete (RLC) message is sent from SP B.
5. Send a Circuit Query Message (CQM) from SP A to SP B for the circuit under test.
6. Verify that a Circuit Query Response (CQR) message is sent from SP B to SP A, and the circuit state of the circuit under test is idle.

1.37 Reset Circuit - During an Established Incoming Call - RSC (also see NGIIF Test 2.15)	I-5.2	Reset Circuit - During an Established Incoming Call - RSC

REFERENCE: ANSI T1.113, chapter 3, tables 5, 6, 6B, 14, 18, 21; ANSI T1.113, chapter 4, subclauses 2.1, 2.9.3.1

TITLE: Reset Circuit from Call Originating End - RSC

PURPOSE: To verify the proper responses when Reset Circuit is initiated at the call originating end.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A. There may be signaling points preceding SP B, and succeeding SP A to establish an end-to-end call.

CONFIGURATION: 1

MESSAGE SEQUENCE:

SP B		SP A
IAM	----->	
	<-----	ACM
	<-----	ANM
	-----connectivity-----	
RSC	----->	
	<-----	RLC
CQM	----->	
	<-----	CQR

TEST DESCRIPTION:

1. Send an Initial Address Message (IAM) from SP B to SP A for the circuit under test.
2. Verify that an Address Complete Message (ACM) and an Answer Message (ANM) are sent from SP A, and the circuit connectivity is made.
3. Send a Reset Circuit (RSC) message from SP B to SP A for the circuit under test.
4. Verify that a Release Complete (RLC) message is sent from SP A.
5. Send a Circuit Query Message (CQM) from SP B to SP A for the circuit under test.
6. Verify that a Circuit Query Response (CQR) message is sent from SP A to SP B, and the circuit state of the circuit under test is idle.

1.38 IAM Received on a Remotely Blocked Circuit	I-3.5.	IAM Received on a Remotely Blocked Circuit

REFERENCE: ANSI T1.113, chapter 3, tables 6B, 14, 18, 21; ANSI T1.113, chapter 4, subclauses 2.1, 2.8.2

TITLE: Title: IAM Received on a Remotely Blocked Circuit

PURPOSE: To verify the proper circuit state when an IAM is received on a remotely blocked circuit.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A. The circuit (under test) has a circuit state, e.g., idle, prior to the test.

CONFIGURATION: 1

MESSAGE SEQUENCE:

SP B		SP A
BLO	----->	
	<-----	BLA
CQM	----->	
	<-----	CQR
IAM	----->	
CQM	----->	
	<-----	CQR

TEST DESCRIPTION:

1. Send a Blocking (BLO) message from SP B to SP A for the circuit under test.
2. Verify that a Blocking Acknowledgement (BLA) message is sent from SP A to SP B.
3. Send a Circuit Query Message (CQM) from SP B to SP A for the circuit under test.
4. Verify that a Circuit Query Response (CQR) message is sent from SP A to SP B, and the state of the circuit carried in the CQR is "remotely blocked" at SP A.
5. Send an Initial Address Message (IAM) from SP B to SP A for the circuit under test.
6. Send a Circuit Query Message (CQM) from SP B to SP A for the circuit under test.
7. Verify that a Circuit Query Response (CQR) message is sent from SP A to SP B, and the circuit is no longer remotely blocked at SP A.

1.39 Call to Circuit Blocked at Both Ends	I-3.6.	Call to Circuit Blocked at Both Ends

REFERENCE: ANSI T1.113, chapter 3, tables 14, 18; ANSI T1.113, chapter 4, subclauses 2.1, 2.8.2

TITLE: Call to Circuit Blocked at Both Ends

PURPOSE: To verify the proper responses when an IAM is received on a locally blocked circuit.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A. The circuit (under test) is idle.

CONFIGURATION: 1

MESSAGE SEQUENCE:

SP B		SP A
BLO	----->	
	<-----	BLA
	<-----	BLO
BLA	----->	
IAM	----->	
	<-----	BLO
BLA	----->	
	<-----	IAM
BLO	----->	
	<-----	BLA

TEST DESCRIPTION:

1. Send a Blocking (BLO) message from SP B to SP A for the circuit under test.
2. Verify that a Blocking Acknowledgement (BLA) message is sent from SP A to SP B.
3. Send a Blocking (BLO) message from SP A to SP B for the circuit under test.
4. Verify that a Blocking Acknowledgement (BLA) message is sent from SP B to SP A.
5. Send an Initial Address Message (IAM) from SP B to SP A for the circuit under test.
6. Verify that a Blocking (BLO) message is sent from SP A, and a Blocking Acknowledgement (BLA) message is sent from SP B, and the received IAM is discarded at SP A.
7. Send an Initial Address Message (IAM) from Sp A to SP B for the circuit under test.
8. Verify that a Blocking (BLO) message is sent from SP B, and a Blocking acknowledgement (BLA) message is sent from SP A, and the received IAM is discarded at SP B.

NGIIF Test #:

ANSI T1.236 Test #:

TR-905 Test #

1.40 Dual Seizure (also see NGIIF Test 2.16)	I-7.1.	Dual Seizure

REFERENCE: ANSI T1.113, chapter 3, tables 5, 6, 14, 14A, 18; ANSI T1.113, chapter 4, subclauses 2.1, 2.9.1

TITLE: Dual Seizure

PURPOSE: To verify the proper responses when a dual seizure of the circuit occurs.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A. There may be signaling points preceding SP B, and succeeding SP A to establish an end-to-end call.

CONFIGURATION: 1

MESSAGE SEQUENCE:

SP BSP A

IAM(cic=x) -----> <----- IAM(cic=x)

ACM(cic=x) ----->

ANM(cic=x) ----->

-----connectivity-----

IAM(cic=y) ----->

<----- ACM(cic=y)

<----- ANM(cic=y)

-----connectivity-----

REL(cic=y) ----->

<----- RLC(cic=y)

<----- REL(cic=x)

RLC(cic=x) ----->

TEST DESCRIPTION:

1. *Send Initial Address Message (IAM) from both SP B and SP A at the same time for the circuit under test.
2. Upon detection of a dual seizure by the control (glaremaster) signaling point, SP A, it discards the incoming IAM and lets the outgoing IAM to proceed in a normal manner.
3. Verify that an Address Complete Message (ACM) and an Answer Message (ANM) are sent from SP B to SP A and the circuit connectivity is made.
4. At SP B, the original call is reattempted over another circuit by sending an Initial Address Message (IAM) from SP B to SP A.
5. Verify that an Address Complete Message (ACM) and an Answer Message (ANM) are sent from SP A to SP B and the circuit connectivity is made.
6. Release the circuit (cic=y) at SP B and verify the exchange of Release (REL) and Release Complete (RLC) messages.
7. Release the circuit (cic=x) at SP A and verify the exchange of Release (REL) and Release Complete (RLC) messages.

*Note: Multiple attempts may be required to reach the desired results.

NGIIF Test #:

ANSI T1.236 Test #:

TR-905 Test #

1.41 Timer TIAM Time-Out	I-12.1	Timer TIAM Time-Out

REFERENCE: ANSI T1.113, chapter 3, tables 14, 14A, 18; ANSI T1.113, chapter 4, subclauses 2.1, 2.2, 2.3, table 3

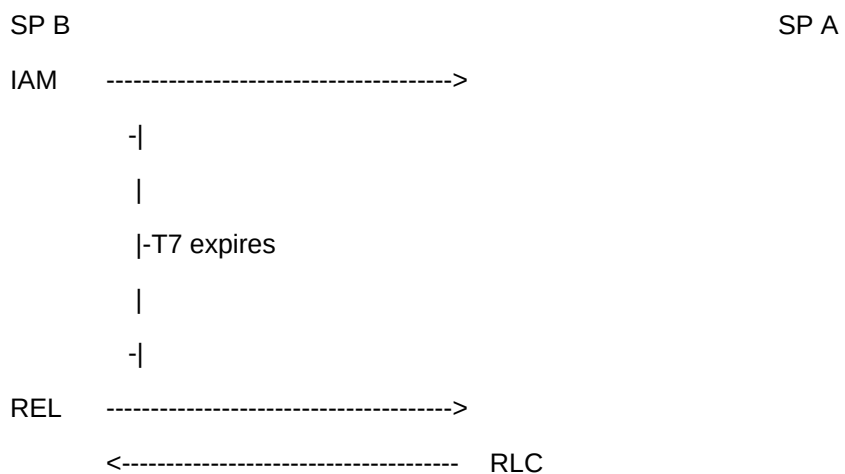
TITLE: Timer T7 (T_iam) Time-out

PURPOSE: To verify the proper responses when the timer T7 (T_iam) expires.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A.

CONFIGURATION: 1

MESSAGE SEQUENCE:



TEST DESCRIPTION:

1. Send an Initial Address Message (IAM) from SP B to SP A.
2. No backward message is returned to SP B from SP A, and the timer T7 (20-30 seconds) expires.
3. Verify that a Release (REL) message is sent from SP B to SP A.
4. Verify that a Release Complete (RLC) message is sent from SP A to SP B.

NGIIF Test #:

ANSI T1.236 Test #:

TR-905 Test #

1.42 IAM with an Unequipped Circuit (also see NGIIF 2.19)	I-11.1.	IAM with an Unequipped Circuit

REFERENCE: ANSI T1.113, chapter 3, tables 14, 18; ANSI T1.113, chapter 4, subclauses 2.1, 2.9.8.3A

TITLE: IAM with an Unequipped Circuit Identification Code

PURPOSE: To verify the proper responses to an IAM with UCIC.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A.

CONFIGURATION: 1

MESSAGE SEQUENCE:

SP B

SP A

IAM ----->

(ucic)

<----- UCIC

TEST DESCRIPTION:

1. Send an Initial Address Message (IAM) with an unequipped circuit identification code from SP B to SP A.
2. Verify that SP A discards the IAM.
3. Verify that an Unequipped Circuit Identification Code (UCIC) message is sent from SP A to SP B.

NGIIF Test #:

ANSI T1.236 Test #:

TR-905 Test #

1.43 Unsuccessful Call - IAM no CPN, no CHG, with OLI (also see NGIIF Test 2.27)	I-11.2	Unsuccessful Call - IAM - no CPN, no CHG, with OLI

REFERENCE: ANSI T1.113, chapter 3, tables 14, 14A, 18; ANSI T1.113, chapter 4, subclauses 2.1, 2.2, 2.3, 2.9.5, table 3

TITLE: Unsuccessful Call - IAM - no CPN, no CHG, with OLI

PURPOSE: To verify the proper responses to an IAM without CPN, without CHG and with OLI.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A.

CONFIGURATION: 1

MESSAGE SEQUENCE:

```
SP B                                     SP A
IAM ----->
(w/CPN)
(w/CHG)
(w/OLI)
      <----- REL
RLC ----->
```

TEST DESCRIPTION:

1. Send an Initial Address Message (IAM) without a Calling Party Number (CPN), without a Charge Number (CHG), and with an Originating Line Information (OLI) from SP B to SP A.
2. Verify that SP A discards the IAM.
3. *Verify that a Release (REL) message is sent from SP A to SP B.
4. Verify that a Release Complete (RLC) message is sent from SP B to SP A.

*Note: It is also possible that SP A relies on the expiration of timer T7 (20-30 seconds) at SP B to release the circuit, and thus, no REL is sent from SP A.

NGIIF Test #:

ANSI T1.236 Test #:

TR-905 Test #

<i>1.44 Unsuccessful Call - IAM - with CPN, with CHG, no OLI (also see Test 2.28)</i>	I-11.3	Unsuccessful Call - IAM – with CPN, with CHG, no OLI

REFERENCE: ANSI T1.113, chapter 3, tables 14, 14A, 18; ANSI T1.113, chapter 4, subclauses 2.1, 2.2, 2.3, 2.9.5, table 3

TITLE: Unsuccessful Call - IAM - CPN, with CHG, no OLI

PURPOSE: To verify the proper responses to an IAM with CPN, with CHG and without OLI.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A.

CONFIGURATION: 1

MESSAGE SEQUENCE:

SP B

SP A

IAM ----->

(w/CPN)

(w/CHG)

(wo/OLI)

<----- REL

RLC ----->

TEST DESCRIPTION:

1. Send an initial Address Message (IAM) with a Calling Party Number (CPN), with a Charge Number (CHG), and without an Originating Line Information (OLI) from SP B to SP A.
2. Verify that SP A discards the IAM.
3. *Verify that a Release (REL) message is sent from SP A to SP B.
4. Verify that a Release Complete (RLC) message is sent from SP B to SP A.

*Note: It is also possible that SP A relies on the expiration of timer T7 (20-30 seconds) at SP B to release the circuit, and thus, no REL is sent from SP A.

TR-905 Test #

1.45 Calling Party Disconnect Before Receipt of ACM <i>(also see NGIIF 2.29)</i>	I-10.1.	Calling Party Disconnect Before Receipt of ACM

REFERENCE: ANSI T1.113, chapter 3, tables 14, 14A, 18; ANSI T1.113, chapter 4, subclause 2.3.1

TITLE: Calling Party Disconnect before Receipt on an ACM

PURPOSE: To verify the proper responses when the calling party disconnects before the receipt of an ACM.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A. There may be signaling points preceding SP B and succeeding SP A for an end-to-end call.

CONFIGURATION: 1

MESSAGE SEQUENCE:

SP B

SP A

IAM ----->

REL ----->

<-----> RLC

TEST DESCRIPTION:

1. Send an Initial Address Message (IAM) from SP B to SP A.
2. Upon disconnect by the calling party, verify that a Release (REL) message is sent from SP B to SP A. The REL message has a cause value of "normal release" and general location of "user".
3. Verify that a Release Complete (RLC) message is sent from SP A to SP B.

1.46 Simultaneous Release Messages	I-10.6	Simultaneous Release Messages

REFERENCE: ANSI T1.113, chapter 3, tables 5, 6, 14, 14A, 18; ANSI T1.113, chapter 4, subclauses 2.1, 2.3.1

TITLE: Simultaneous Release Messages

PURPOSE: To verify the proper responses to the simultaneous release messages

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A. There may be signaling points preceding SP B and succeeding SP A for an end-to-end call.

CONFIGURATION: 1

MESSAGE SEQUENCE:

SP B		SP A
IAM	----->	
	<-----	ACM
	<-----	ANM
	-----connectivity-----	
REL	-----> <-----	REL
	<-----	RLC
RLC	-----	

TEST DESCRIPTION:

1. Send an Initial Address Message (IAM) from SP B to SP A.
2. Verify that an Address Complete Message (ACM) is received at SP B.
3. Verify that an Answer Message (ANM) is received at SP B, and the circuit connection is made.
4. SP A and SP B send Release (REL) messages simultaneously toward each other.
5. Verify that a Release Complete (RLC) message is sent from SP B and a Release Complete (RLC) message is sent from SP A.

1.47 BLO after IAM Received and Before Backward Message	I-3.7.	BLO after IAM Received and Before Backward Message

REFERENCE: ANSI T1.113, chapter 3, tables 14, 14A, 18; ANSI T1.113, chapter 4, subclauses 2.1, 2.8.2

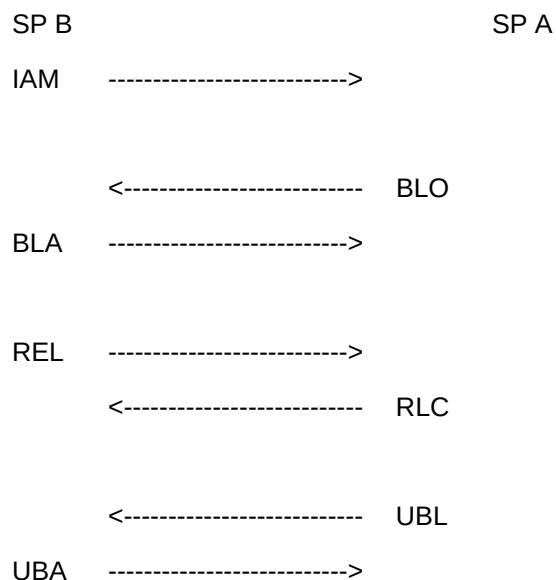
TITLE: Blocking Received After IAM (Sent) and Before Backward Message (received)

PURPOSE: To verify the proper responses when a Blocking is received after an IAM is sent, and before any backward message is received for the circuit under test.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A. The circuit (under test) is idle.

CONFIGURATION: 1

MESSAGE SEQUENCE:



TEST DESCRIPTION:

1. Send an Initial Address Message (IAM) from SP B to SP A for the circuit under test.
2. Send a Blocking (BLO) message from SP A to SP B for the circuit under test.
3. *Verify that a Blocking Acknowledgement (BLA) message is sent from SP B to SP A.
4. Verify that a Release (REL) message is sent from SP B, and a Release Complete (RLC) message is sent from SP A.
5. Send a Unblocking (UBL) message from SP A to SP B for the circuit under test.
6. Verify that a Unblocking Acknowledgement (UBA) message is sent from SP B, and the circuit is ready for service.

*Note: The original call should be reattempted on another circuit.

1.48 Sending IAM and Receiving CGBs Before any Backward Messages	I-4.3.	Sending IAM and Receiving CGBs Before any Backward Messages

REFERENCE: ANSI T1.113, chapter 3, tables 14, 14A, 18, 20; ANSI T1.113, chapter 4, subclauses 2.1, 2.8.2.2

TITLE: Circuit Group Blocking Received After IAM (sent) and Before Backward Message (received)

PURPOSE: To verify the proper responses when Circuit Group Blocking messages (2) are received after an IAM(s) is sent, and before any backward message(s) is received for the circuit(s) under test.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A. The circuits (under test) are idle.

CONFIGURATION: 1

MESSAGE SEQUENCE:

SP B		SP A
IAM	----->	
	<-----	CGB+
	<-----	CGB+
CGBA+	----->	
REL	----->	
	<-----	RLC
	<-----	CGU
CGUA	----->	

TEST DESCRIPTION:

1. Send Initial Address Message (IAM) from SP B to SP A for the circuit(s) under test.
2. Send a Circuit Group Blocking (CGB) message from SP A to SP B with the Range/Status field specified to cover the circuits under test, and the Circuit Group Supervision Message Type Indicator set to "block with release".
3. Send an identical Circuit Group Blocking (CGB) message from SP A to SP B within 5 seconds.
4. *+Verify that a Circuit Group Blocking Acknowledgement (CGBA) message is sent from SP B to SP A, and that the received CGBA at SP A matches the Trunk Circuit Identification Code (TCIC), Circuit Group Supervision Message Type Indicator, and Range/Status field of the previously sent CGB message.

5. Verify that Release (REL) message(s) is sent from SP B, and Release Complete (RLC) is sent from SP A.
6. Send a Circuit Group Unblocking (CGU) message from SP A to SP B with the Range/Status field specified to cover the circuits under test, and the Circuit Group Supervision Message Type Indicator set to "block without release".
7. Verify that a Circuit Group Unblocking Acknowledgement (CGUA) message is sent from SP B to SP A, and that the received CGUA at SP A matches the Trunk Circuit Identification Code (TCIC), Circuit Group Supervision Message Type Indication, and Range/Status field of the previously sent CGU message.

*Note: The original call should be reattempted on another circuit.

+Note: Optionally, SP B can send a CGBA to SP A after the first CGB is received, and discard the second CGB. Or, SP B can send a CGBA to SP A after each CGB is received.

1.49 Sending IAM and Receiving CGBs After Receiving a Backward Message	I-4.4.	Sending IAM and Receiving CGBs After Receiving a Backward Message

REFERENCE: ANSI T1.113, chapter 3, tables 5, 6, 14, 14A, 18, 20; ANSI T1.113, chapter 4, subclauses 2.1, 2.3, 2.8.2.2

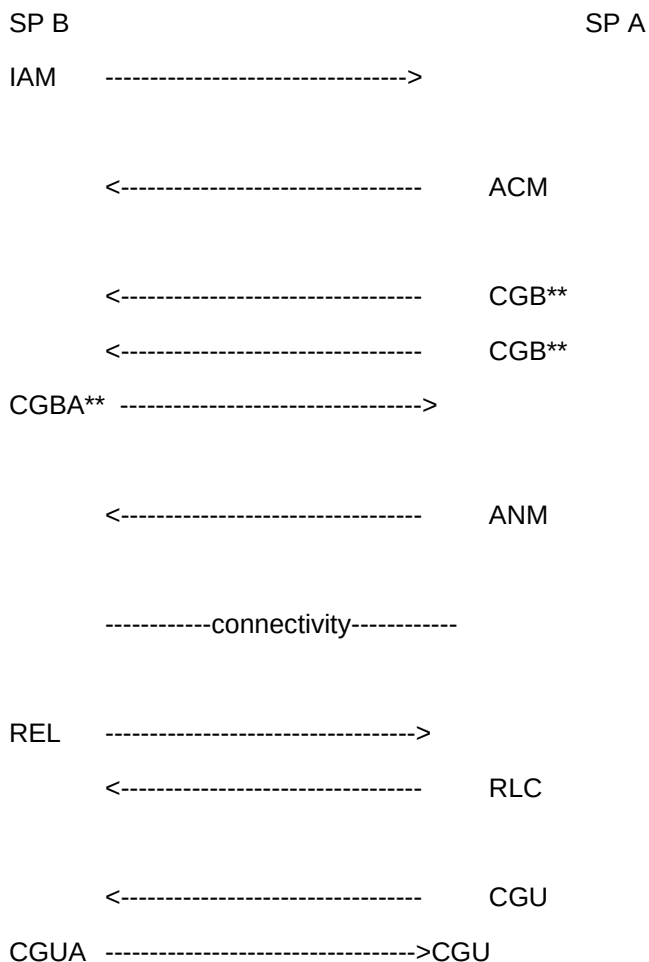
TITLE: Circuit Group Blocking Received After IAM (sent) and After Backward Message (received)

PURPOSE: To verify the proper responses when Circuit Group Blocking messages (2) are received after an IAM(s) is sent, and after backward message(s) is received for the circuit(s) under test.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A. There may be signaling points preceding SP B, and succeeding SP A to establish an end-to-end call.

CONFIGURATION: 1

MESSAGE SEQUENCE:



TEST DESCRIPTION:

1. Send Initial Address Message (IAM) from SP B to SP A for the circuit(s) under test.
2. Send Address Complete Message (ACM) from SP A to SP B for the circuit(s) under test.

3. Send a Circuit Group Blocking (CGB) message from SP A to SP B with the Range/Status field specified to cover the circuits under test, and the Circuit Group Supervision Message Type Indicator set to "block without release".
4. Send an identical Circuit Group Blocking (CGB) message from SP A to SP B within 5 seconds.
5. **Verify that a Circuit Group Blocking (CGB) message is sent from SP B to SP A, and that the received CGBA at SP A matches the Trunk Circuit Identification Code (TCIC)*, Circuit Group Supervision Message Type Indicator, and Range/Status field of the previously sent CGB message.
6. Verify that Answer Message (ANM) is sent from SP A to SP B for the circuit(s) under test, and the circuit connection(s) is established.
7. Send Release (REL) message(s) from SP B, and verify that Release Complete (RLC) is sent from SP A.
8. Send a Circuit Group Unblocking (CGU) message from SP A to SP B with the Range/Status field specified to cover the circuits under test, and the Circuit Group Supervision Message Type Indicator set to "block without release".
9. Verify that a Circuit Group unblocking Acknowledgement (CGUA) message is sent from SP B to SP A, and that the received CGUA at SP A matches the Trunk Circuit Identification Code (TCIC), Circuit Group Supervision Message Type Indicator, and Range/Status field of the previously sent CGU message.

*Note: TCIC (Trunk Circuit Identification Code) is also known as CIC (Circuit Identification Code) in T1 standard.

**Note: Optionally, SP B can send a CGBA to SP A after the first CGB is received, and discard the second CGB. Or, SP B can send a CGBA to SP A after each COG is received.

1.50 Circuit Group Reset Messages - GRS	I-6.1.	Circuit Group Reset Messages - GRS

REFERENCE: ANSI T1.113, chapter 3, tables 6B, 21; ANSI T1.113, chapter 4, subclause 2.9.3.2

TITLE: Circuit Group Reset Message - GRS

PURPOSE: To verify the proper responses to a GRS message.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A. The circuits under test have some initial circuit states, e.g., idle, locally blocked.

CONFIGURATION: 1

MESSAGE SEQUENCE:



TEST DESCRIPTION:

1. Send Circuit Query Message (CQM) messages from SP B to SP A for the circuits under test.
2. Verify that Circuit Query Response (CQR) messages are sent from SP A to SP B. The circuit states of the circuits under test are noted.
3. Send a Circuit Group Reset (GRS) message (carrying a non-zero range field) from SP B to SP A for the circuits under test.
4. Send an identical Circuit Group Reset (GRS) message (carrying a non-zero range field) from SP B to SP A within 5 seconds.
5. *Verify that a Circuit Group Reset Acknowledgement (GRA) message is sent from SP A to SP B for the circuits under test, and the blocking/no-blocking status in the Status field should agree with the original circuit states with respect to the local blocking at SP A. Any remote blocking states at SP A shall be cleared and cannot be reinstated by SP A.

*Note: Optionally, SP A can send a GRA to SP B after the first GRS is received, and discard the second GRS. Or, SP A can send a GRA to SP B after each GRS is received.

1.51 Circuit Group Resets During an Established Call - GRS	I-6.2	Circuit Group Resets During an Established Call -GRS

REFERENCE: ANSI T1.113, chapter 3, tables 5, 6, 14, 21; ANSI T1.113, chapter 4, subclause 2.9.3.2

TITLE: Circuit Group Reset during an Established call GRS

PURPOSE: To verify the proper responses to a GRS during an established call.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A. There may be signaling points preceding SP B and succeeding SP A for an end-to-end call.

CONFIGURATION: 1

MESSAGE SEQUENCE:

SP B	SP A
IAM ----->	
<-----	ACM
<-----	ANM
-----connectivity-----	
GRS* ----->	
GRS* ----->	
<-----	GRA*

TEST DESCRIPTION:

1. Send an Initial Address Message (IAM) from SP B to SP A for the circuit under test.
2. Verify that an Address Complete Message (ACM) and Answer Message (ANM) are sent from SP A to SP B, and the circuit connection is established.
3. Send a Circuit Group Reset (GRS) message from SP A to SP B with the Range field covered the circuit under test.
4. Send an identical Circuit Group Reset (GRS) message from SP A to SP B within 5 seconds.
5. *Verify that a Circuit Group Reset Acknowledgement (GRA) message is sent from SP B to SP A, and the Range/Status field indicates no-blocking for the circuit.

*Note: Optionally, SP A can send a GRA to SP B after the first GRS is received, and discard the second GRS. Or, SP A can send a GRA to SP B after each GRS is received.

1.52 Reset Circuit After IAM but before Backward Messages - RSC	I-5.3.	Reset Circuit After IAM but before Backward Messages - RSC

REFERENCE: ANSI T1.113, chapter 3, tables 5, 6, 14, 21; ANSI T1.113, chapter 4, subclause 2.9.3.2

TITLE: Reset Circuit after Receiving IAM any before Sending any Backward Message - RSC

PURPOSE: To verify the proper responses when Reset Circuit is initiated after receiving IAM and before sending any backward message.

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between SP B and SP A. The circuit under test is idle.

CONFIGURATION: 1

MESSAGE SEQUENCE:

SP B		SP A
IAM	----->	
	<-----	RSC
RLC	----->	
	<-----	CQM
CQR	----->	

TEST DESCRIPTION:

1. Send an Initial Address Message (IAM) from SP B to SP A for the circuit under test.
2. Send a Reset Circuit (RSC) message from SP A to SP B for the circuit under test.
3. *Verify that a Release Complete (RLC) message is sent from SP B.
4. Send a Circuit Query Message (CQM) from SP A to SP B for the circuit under test.
5. Verify that a Circuit Query Response (CQR) message is sent from SP B to SP A, and the circuit state of the circuit under test is idle.

*Note: The call at SP B should be reattempted over another circuit.

1.53 IAM Priority Test for Interconnects		

REFERENCE: National Standard, ANSI T1.111-2001(R) [T1.111.5, Annex A].

TITLE: IAM Priority Test for Interconnects

PURPOSE: To verify the proper ISUP IAM Message Transfer Part (MTP) Priority Setting for Interconnect Calls

PRE-TEST CONDITIONS: A stable MTP signaling relation exists between EO A/MSC A and the ICN. There may be signaling points preceding EO B and succeeding EO A/MSC A for an end-to-end test call. Calls are made from test line on the side on an End Office (EO) or a wireless mobile set (MS) on a Mobile Switching Center (MSC).

For Wireless Priority Service (WPS) calls, if the MSC is not equipped with the Wireless Priority Service feature or the MS is not provisioned with WPS service, the call will be denied.

CONFIGURATION: 1

MESSAGE SEQUENCE:

```

EO A                                ICN
IAM (test call)  ----->
                <-----
                ACM
                -----transmission path-----

```

TEST DESCRIPTION:

A tester at EO A should originate a POTS (NPA-NXX-XXXX, non-GETS, non-WPS) call destined for EO B via an interconnecting network.

Verify Initial Address Message (IAM) parameters settings from EO A.

- Originating Point Code Setting
- Destination Point Code Setting
- Message Priority set to 0
- Calling Party's Category set to non-National Security/Emergency Preparedness (NS/EP) call (not 1110 0010)

Verify that the transmission path is established.

Release the call when the test is done.

A tester at EO A should originate a GETS, call destined for EO B via an interconnecting network.

Verify Initial Address Message (IAM) parameters settings from EO A.

- Originating Point Code Setting
- Destination Point Code Setting
- Message Priority set to 1

- Calling Party's Category set to NS/EP call (1110 0010)

Verify that the transmission path is established.

Release the call when the test is done.

CONFIGURATION: 2

MESSAGE SEQUENCE:



TEST DESCRIPTION:

A tester at MSC A should originate a POTS (NPA-NXX-XXXX, non-GETS, non-WPS) call destined for EO B via an interconnecting network.

Verify Initial Address Message (IAM) parameters settings from MSC A.

- Originating Point Code Setting
- Destination Point Code Setting
- Message Priority set to 0
- Calling Party's Category set to non-NS/EP call (not 1110 0010)

Verify that the transmission path is established.

Release the call when the test is done.

A tester at MSC A should originate a WPS (*272+NPA-NXX-XXXX) call destined for EO B via an interconnecting network.

Verify Initial Address Message (IAM) parameters settings from MSC A.

- Originating Point Code Setting
- Destination Point Code Setting
- Message Priority set to 1
- Calling Party's Category set to NS/EP call (1110 0010)

Verify that the transmission path is established.

Release the call when the test is done.

A tester at MSC A should originate a GETS (710-NCS-GETS) call destined for EO B via an interconnecting network.

Verify Initial Address Message (IAM) parameters settings from MSC A.

- Originating Point Code Setting
- Destination Point Code Setting
- Message Priority set to 1
- Calling Party's Category set to NS/EP call (1110 0010)

Verify that the transmission path is established.

Release the call when the test is done.

1.54 IAM Precedence Test for Interconnects		IAM Precedence Test for Interconnects

REFERENCE: National Standard, ANSI T1.111-2001 [T1.111.5, Annex A].

TITLE: IAM Precedence Test for Interconnects

PURPOSE: To verify Transit Switches pass the Precedence Parameter and non-WPS Terminating Switches establish a call based on an IAM with the Precedence parameter.

LAB TEST

PRE-TEST CONDITIONS:

1. A stable MTP signaling relation exists between Originating Node A, the Transit Switch and Terminating Switch (TS) B.
2. Originating Node A is provisioned to send the Precedence parameter over the trunk group connected to the Transit Switch
3. Originating Node A may be a test call generator or a Mobile Switching Center (MSC) with WPS capability

CONFIGURATION:

Each Transit Switch and Terminating Switch in the Service Provider's network should be tested.

MESSAGE SEQUENCE:

Originating Node	Transit Switch	Terminating Switch
A	X	B

IAM (test call) ----->
 <----- ACM

TEST DESCRIPTION:

A tester at Originating Node A originates a WPS (*272+NPA-NXX-XXXX) call destined for TS B via an interconnecting network. Only one test call, with a single Precedence parameter setting (priority level), is required to be sent to each switch to which the test is intended.

Verify the Initial Address Message (IAM) parameter settings from the Originating Node A.

- Message Priority set to 1
- Calling Party's Category set to NS/EP call (1110 0010)
- Precedence parameter is set as defined in Table A.2 below

Verify the IAM received at TS B has the same parameter values as sent from MSC A.

- Message Priority set to 1
- Calling Party's Category set to NS/EP call (1110 0010)
- Precedence parameter is set to the same values as sent from MSC A

Establishment of the transmission path is optional.

Verify that any switch through which the IAM transits or terminates to experiences no adverse behavior based on the call.

If TS B forwards the call, verify that the forwarding IAM sent at TS B has the same NS/EP parameter values as the IAM received at TS B.

- Message Priority set to 1
- Calling Party's Category set to NS/EP call (1110 0010)
- Precedence parameter is set to the same values as received at TS B.

RESULTS REPORTING:

For tests conducted, carriers are requested to report one of the following results

1. Transit Switch X, software generic Y received and passed a call with the Precedence parameter successfully
2. Transit Switch X, software generic Y received a call successfully, but did not pass the Precedence parameter
3. Transit Switch X, software generic Y experienced the following adverse behavior when attempting to transit a call with the Precedence parameter: [problem experienced]
4. Terminating Switch B, software generic Y terminated a call with the Precedence parameter successfully
5. Terminating Switch B, software generic Y experienced the following adverse behavior when attempting to terminate a call with the Precedence parameter: [problem experienced]
6. Terminating Switch B, software generic Y forwarded a call with the Precedence parameter successfully
7. Terminating Switch B, software generic Y forwarded a call successfully, but did not pass the Precedence parameter
8. Terminating Switch B, software generic Y experienced the following adverse behavior when attempting to forward a call with the Precedence parameter: [problem experienced]

PRECEDENCE PARAMETER DEFINITION AND EXAMPLES:

Table A.1 below shows the definition and values for the Precedence Parameter. Tables A.2-A-4 provide examples of the Precedence Parameter.

**1.55 SIP INVITE to ISUP
IAM mappings**

REFERENCE: PTSC-SAC-2007-060R2

TITLE: Session Initiation Protocol (SIP) INVITE to ISUP IAM to mappings

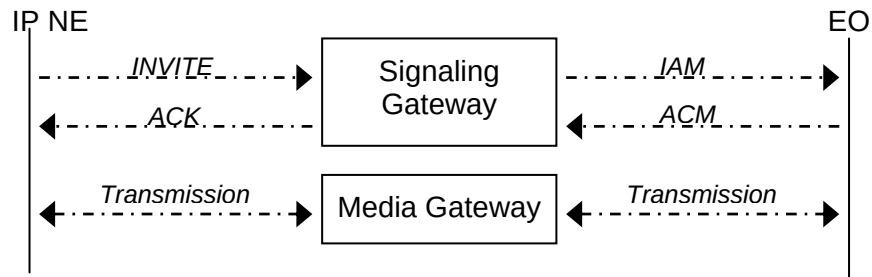
PURPOSE: To verify SIP Resource Priority Header (RPH) messaging maps correctly to ISUP IAM signaling across network boundaries.

PRE-TEST CONDITIONS: A stable SIP signaling relation exists between IP Network Element (NE) and the Signaling Gateway. A stable MTP signaling relation exists between the Signaling Gateway and EO/MSC. Calls are made from a SIP phone. Calls are made to a test line on the side of an End Office (EO) or a wireless mobile set (MS) on a Mobile Switching Center (MSC). Calls traverse IP Service Providers (SP) to TDM SPs.

For Wireless Priority Service (WPS) calls, if the MSC is not equipped with the Wireless Priority Service feature or the MS is not provisioned with WPS service, the call will be denied.

CONFIGURATION 1:

IP to TDM Landline



MESSAGE SEQUENCE:

TEST DESCRIPTIONS:

A tester at IP NE should originate a non-NS/EP SIP (R-URI/To: = Destination Number) call destined for EO via an interconnecting gateway.

Verify SIP RPH INVITE message parameter settings from the Signaling Gateway.

- Identification of R-URI/To set to the Destination Number
- Identification of the lack of an RPH namespace

Verify IAM parameters setting to EO.

- Identification of carrier associated with the Originating Point Code
- Identification of carrier associated with the Destination Point Code
- Message Priority set to 0
- Calling Party Category set to non-NS/EP call (not 1110 0010)
- The lack of a Precedence Parameter

Verify that the transmission path is established.

Release the call when it is done.

A tester at IP NE should originate a SIP (R-URI/To: = ETS-DN, 710-NXX-XXXX) call destined for EO via an interconnecting gateway.

Verify SIP RPH INVITE message parameter settings from the Signaling Gateway.

- Identification of R-URI/To set to the ETS-DN
- Identification of the lack of an RPH namespace

Verify IAM parameters setting to EO.

- Identification of carrier associated with the Originating Point Code
- Identification of carrier associated with the Destination Point Code
- Message Priority set to 1
- Calling Party Category set to NS/EP call (1110 0010)
- The lack of a Precedence Parameter

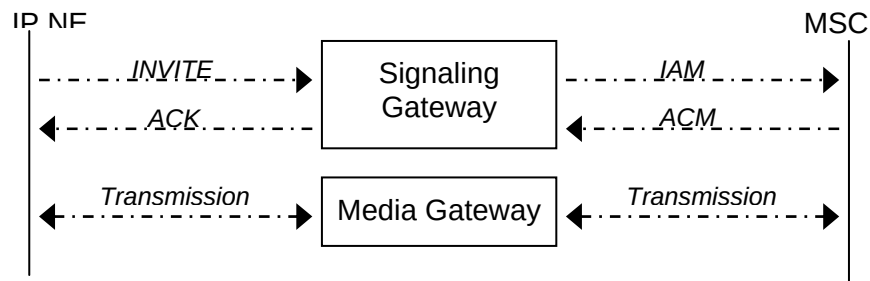
Verify that the transmission path is established.

Release the call when it is done.

CONFIGURATION 2:

IP to TDM Wireless

MESSAGE SEQUENCE:



TEST DESCRIPTION:

A tester at IP NE should originate an SIP (ETS-DN, 710-NXX-XXXX) call destined for MSC via an interconnecting gateway.

Verify SIP RPH INVITE message parameter settings from the Signaling Gateway.

- Identification of R-URI/To set to the Destination Number
- Identification RPH namespace set to ets.x and wps.y

Verify IAM parameters setting to MSC.

- Identification of carrier associated with the Originating Point Code
- Identification of carrier associated with the Destination Point Code
- Message Priority set to 1
- Calling Party Category set to NS/EP call (1110 0010)
- Verify the Precedence parameter settings
 - o Look ahead for Busy is set to 10
 - o Precedence level is set to a level 0 – 4
 - o Network Identity is set to 0100
 - o MLPP Service Domain is set to a value from H'40024B' to H'40024F'

Verify that the transmission path is established.

Release the call when it is done.

A tester at IP NE should originate an SIP (ETS-DN, 710-NXX-XXXX) call destined for MSC via an interconnecting gateway.

Verify SIP RPH INVITE message parameter settings from the Signaling Gateway.

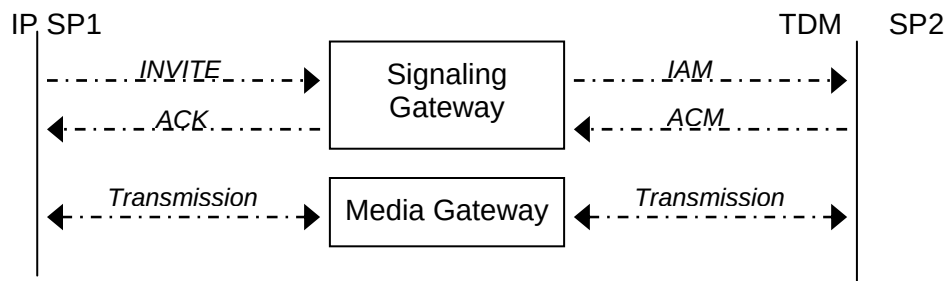
- Identification of R-URI/To set to the ETS-DN
- Identification RPH namespace set to wps.y

Verify SIP RPH INVITE message is rejected.

CONFIGURATION 3:

IP Service Provider to TDM Service Provider

MESSAGE SEQUENCE:



TEST DESCRIPTION:

A trusted IP network SP1 should originate a SIP (R-URI/To: = Destination Number) call destined for TDM SP 2 via an interconnecting gateway.

Verify SIP RPH INVITE message parameter settings from the Signaling Gateway.

- Identification of R-URI/To set to the Destination Number
- Identification RPH namespace set to ets.x

Verify IAM parameters setting to EO.

- Identification of carrier associated with the Originating Point Code
- Identification of carrier associated with the Destination Point Code
- Message Priority set to 1
- Calling Party Category set to NS/EP call (1110 0010)
- The lack of a Precedence Parameter

Verify that the transmission path is established.

Release the call when it is done.

A trusted IP network SP 1 should originate a SIP (Destination Number, NPA-NXX-XXXX) call destined for TDM SP2 via an interconnecting gateway.

Verify SIP RPH INVITE message parameter settings from the Signaling Gateway.

- Identification of R-URI/To set to the Destination Number
- Identification RPH namespace set to ets.x and wps.y

Verify IAM parameters setting to MSC.

- Identification of carrier associated with the Originating Point Code
- Identification of carrier associated with the Destination Point Code
- Message Priority set to 1
- Calling Party Category set to NS/EP call (1110 0010)

- Verify the Precedence parameter settings
 - o Look ahead for Busy is set to 10
 - o Precedence level is set to a level 0 – 4
 - o Network Identity is set to 0100
 - o MLPP Service Domain is set to a value from H'40024B' to H'40024F'

Verify that the transmission path is established.

Release the call when it is done.

A trusted IP network SP 1 should originate a SIP (Destination Number, NPA-NXX-XXXX) call destined for TDM SP2 via an interconnecting gateway.

Verify SIP RPH INVITE message parameter settings from the Signaling Gateway.

- Identification of R-URI/To set to the Destination Number
- Identification RPH namespace set to wps.y

Verify SIP RPH INVITE message is rejected.

**1.56 ISUP IAM to SIP
INVITE mappings**

REFERENCE: PTSC-SAC-2007-060R2

TITLE: ISUP IAM to Session Initiation Protocol (SIP) INVITE mappings

PURPOSE: To verify ISUP IAM messaging maps correctly to SIP Resource Priority Header (RPH) signaling across network boundaries.

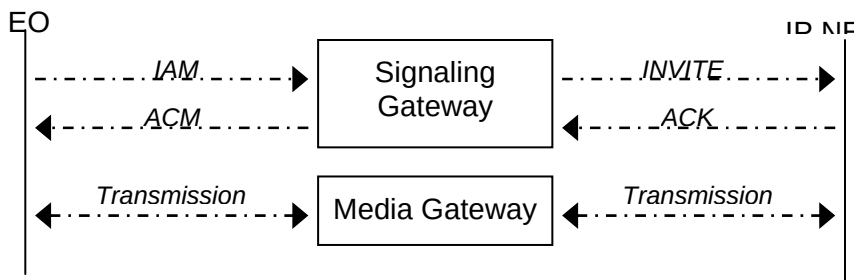
PRE-TEST CONDITIONS: A stable MTP signaling relation exists between EO/MSC and the Signaling Gateway. A stable SIP signaling relation exists between the Signaling Gateway and IP Network Element (NE). Calls are made from a test line on the side of an End Office (EO) or a wireless mobile set (MS) on a Mobile Switching Center (MSC). Calls are made to a SIP phone.

For Wireless Priority Service (WPS) calls, if the MSC is not equipped with the Wireless Priority Service feature or the MS is not provisioned with WPS service, the call will be denied.

CONFIGURATION: 1

TDM Landline to IP

MESSAGE SEQUENCE:



TEST DESCRIPTION:

A tester at EO should originate a POTS (NPA-NXX-XXXX) call destined for IP NE via an interconnecting gateway.

Verify IAM parameters setting from EO.

- Identification of carrier associated with the Originating Point Code
- Identification of carrier associated with the Destination Point Code
- Message Priority set to 0

- Calling Party Category set to non-NS/EP call (not 1110 0010)

Verify SIP RPH INVITE message parameter settings from the Signaling Gateway.

- Identification of R-URI/To set to the Destination Number
- Identification of the lack of an RPH namespace

Verify that the transmission path is established.

Release the call when it is done.

A tester at EO should originate an ETS-DN (710-NXX-XXXX) call destined for IP NE via an interconnecting gateway.

Verify IAM parameters setting from EO.

- Identification of carrier associated with the Originating Point Code
- Identification of carrier associated with the Destination Point Code
- Message Priority set to 1
- Calling Party Category set to NS/EP call (1110 0010)

Verify SIP RPH INVITE message parameter settings from the Signaling Gateway.

- Identification of R-URI/To set to the ETS-DN
- Identification RPH namespace set to ets.DF

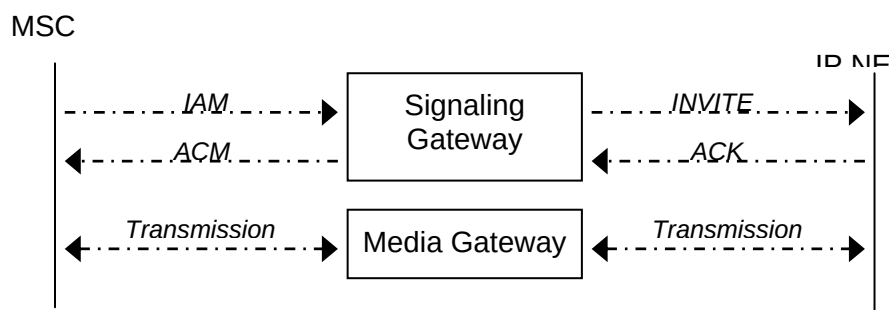
Verify that the transmission path is established.

Release the call when it is done.

CONFIGURATION: 2

TDM Wireless to IP

MESSAGE SEQUENCE:



TEST DESCRIPTION:

A tester at MSC should originate an ETS-DN (*272 710-NXX-XXXX) call destined for IP NE via an interconnecting gateway.

Verify IAM parameters setting from MSC.

- Identification of carrier associated with the Originating Point Code
- Identification of carrier associated with the Destination Point Code
- Message Priority set to 1
- Calling Party Category set to NS/EP call (1110 0010)
- Verify the Precedence parameter settings
 - o Look ahead for Busy is set to 10
 - o Precedence level is set to a level 0 – 4
 - o Network Identity is set to 0100
 - o MLPP Service Domain is set to a value from H'40024B' to H'40024F'

Verify SIP RPH INVITE message parameter settings from the Signaling Gateway.

- Identification of R-URI/To set to the Destination Number
- Identification RPH namespace set to ets.DF or ets.y and wps.y

Verify that the transmission path is established.

Release the call when it is done.

A tester at MSC should originate an ETS-DN (*272 NPA-NXX-XXXX) call destined for IP NE via an interconnecting gateway.

Verify IAM parameters setting from MSC.

- Identification of carrier associated with the Originating Point Code
- Identification of carrier associated with the Destination Point Code
- Message Priority set to 0
- Calling Party Category set to non-NS/EP call (not 1110 0010)
- Verify the Precedence parameter settings
 - o Look ahead for Busy is set to 10
 - o Precedence level is set to a level 0 – 4
 - o Network Identity is set to 0100
 - o MLPP Service Domain is set to a value from H'40024B' to H'40024F'

Verify SIP RPH INVITE message parameter settings from the Signaling Gateway.

- Identification of R-URI/To set to the Destination Number
- Identification RPH namespace set to ets.DF and wps.y

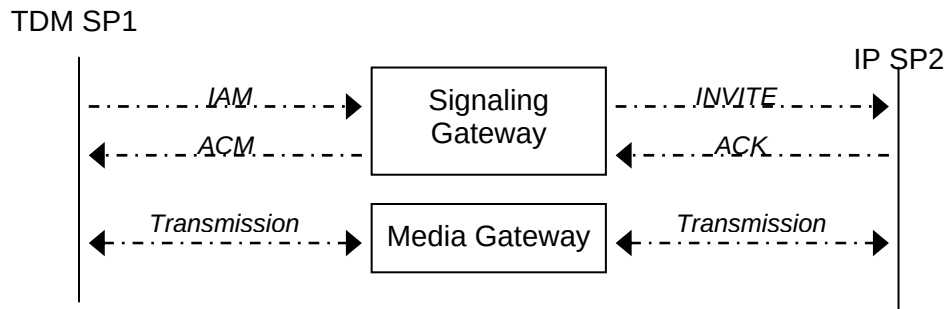
Verify that the transmission path is established.

Release the call when it is done.

CONFIGURATION: 3

TDM Service Provider to IP Service Provider

MESSAGE SEQUENCE:



TEST DESCRIPTION:

A trusted TDM network SP1 originates a POTS (NPA-NXX-XXXX) call destined for IP SP2 via an interconnecting gateway.

Verify IAM parameters setting from EO.

- Identification of carrier associated with the Originating Point Code
- Identification of carrier associated with the Destination Point Code
- Message Priority set to 0
- Calling Party Category set to NS/EP call (1110 0010)

Verify SIP RPH INVITE message parameter settings from the Signaling Gateway.

- Identification of R-URI/To set to the Destination Number
- Identification RPH namespace set to ets.DF

Verify that the transmission path is established.

Release the call when it is done.

A trusted TDM network SP 1 originates an ETS-DN (710-NXX-XXXX) call destined for IP SP2 via an interconnecting gateway.

Verify IAM parameters setting from EO.

- Identification of carrier associated with the Originating Point Code

- Identification of carrier associated with the Destination Point Code
- Message Priority set to 0
- Calling Party Category set to non-NS/EP call (not 1110 0010)

Verify SIP RPH INVITE message parameter settings from the Signaling Gateway.

- Identification of R-URI/To set to the ETS-DN
- Identification RPH namespace set to ets.DF

Verify that the transmission path is established.

Release the call when it is done.

A trusted TDM network SP1 originates a POTS (NPA-NXX-XXXX) call destined for IP SP2 via an interconnecting gateway.

Verify IAM parameters setting from MSC.

- Identification of carrier associated with the Originating Point Code
- Identification of carrier associated with the Destination Point Code
- Message Priority set to 0
- Calling Party Category set to non-NS/EP call (not 1110 0010)
- Verify the Precedence parameter settings
 - o Look ahead for Busy is set to 10
 - o Precedence level is set to a level 0 – 4
 - o Network Identity is set to 0100
 - o MLPP Service Domain is set to a value from H'40024B' to H'40024F'

Verify the IAM is rejected.

A trusted TDM network SP1 originates a POTS (NPA-NXX-XXXX) call destined for IP SP2 via an interconnecting gateway.

Verify IAM parameters setting from MSC.

- Identification of carrier associated with the Originating Point Code
- Identification of carrier associated with the Destination Point Code
- Message Priority set to 1
- Calling Party Category set to NS/EP call (1110 0010)
- Verify the Precedence parameter settings
 - o Look ahead for Busy is set to 10
 - o Precedence level is set to a level 0 – 4
 - o Network Identity is set to 0100
 - o MLPP Service Domain is set to a value from H'40024B' to H'40024F'

Verify SIP RPH INVITE message parameter settings from the Signaling Gateway.

- Identification of R-URI/To set to the Destination Number
- Identification RPH namespace set to ets.DF or ets.y and wps.y

Verify that the transmission path is established.

Release the call when it is done.

Table A.1: ISUP Precedence Parameter Encoding

Field	Description	Value
Look Ahead for Busy	Indicates whether look ahead for busy is allowed or whether the path has been reserved	Binary "10" (Look Ahead for Busy not allowed)
Precedence Level	Calling Party's Priority Level	Binary, 4 bits "0000" through "0100", based on Calling Party's Priority Level, as assigned to the Service User: Service User priority 1 = Precedence Level 0 (highest priority) Service User priority 2 = Precedence Level 1 Service User priority 3 = Precedence Level 2 Service User priority 4 = Precedence Level 3 Service User priority 5 = Precedence Level 4 (lowest priority)
Network Identity	Telephone Country Code of the originating network	Binary Coded Decimal, 4 digits, "0100" (indicating networks in the U.S.A.)
MLPP Service Domain	Priority Service Domain	Binary, 3 octets: NCS Wireless Priority Service-1 (Decimal 4194891) Binary: 0100 0000 0000 0010 0100 1011 NCS Wireless Priority Service-2 (Decimal 4194892) Binary: 0100 0000 0000 0010 0100 1100 NCS Wireless Priority Service-3 (Decimal 4194893) Binary: 0100 0000 0000 0010 0100 1101 NCS Wireless Priority Service-4 (Decimal 4194894) Binary: 0100 0000 0000 0010 0100 1110 NCS Wireless Priority Service-5 (Decimal 4194895) Binary:

		0100 0000 0000 0010 0100 1111

Table A.2: Example of Precedence Parameter set to 3 (WPS Priority 4)

Precedence

0041	00111010	3a	Precedence Type	58
0042	00000110	06	Precedence Length	6
0043	01000011	43		
	----0011		Precedence level	0011 - priority
	---0----		Spare	0
	-10-----		Look ahead for busy (LFB)	10 - path reserved
	0-----		Extension	0 - octet continues thru
	next octet			
0044	00000001	01	NI Digits	1000
0045	00000000	00		
0046	01000000	40	MLPP service domain	40 02 4e
0047	00000010	02		
0048	01001110	4e		

Table A.3: Example of IAM with Precedence Parameter set to 0 (WPS Priority 1)

ANSI S7 Decode:

RS09 C7TU101 JUN14 15:32:03 3450 INFO INCOMING LINK MSG
C7 HEADER: LEN=68 MSG=#01 LINK=3 SLC=0 CLLI=RS29LINK
C7 SIO: NETWORK= 2 PRIORITY= 1 SERV IND= 5 ISUP

MTP priority = 1

C7 LABEL: DPC = ANSI7 222 222 222 OPC = ANSI7 111 111 111 SLS = 9
S7 DATA FOLLOWING ROUTING LABEL:
04 00 01 11 20 01 E2 03 06 0D 03 80 90 A2 07 03
10 09 84 44 14 48 0A 07 04 13 79 02 00 01 88 3D
01 02 EB 07 07 10 79 62 58 00 08 EA 01 3E C4 03
12 74 20 3A 06 40 01 00 40 02 4B 00

3A 06 44 01 00 40 02 4B

PRECEDENCE PARAMETER #3A
LENGTH #06 OPT. DATA #44 #01 #00 #40 #02 #4B

<u>Precedence ID</u>	<u>Length</u>	<u>Spare/LFB/Precedence Level</u>	<u>Network ID</u>	<u>Service Domain</u>
3A	06	40	0100	40024B

3A = 00111010 = Precedence Parameter Identifier

06 = Length (number of octets)

	<u>spare</u>	<u>LFB</u>	<u>spare</u>	<u>precedence level</u>
40 = 1000 0000 =	1	00	1	0000 = 0 = WPS level 1

01 00 = USA Network ID

40 02 4B = 4194891 = Service Domain for WPS priority 1

Table A.4: Example of decoded IAM Message with Precedence Parameter set to 4 (WPS Priority 5)

Octets: 62

Octet001	ANSI SS7	Count=000001	Time=04/28/2004 04:25:18:580 AM
00101011	BIB/BSN	(43)	0/43
10110001	FIB/FSN	(177)	1/49
..111011	SU type/length	(59)	MSU59
00.....	Spare	0	
Octet004	Service information octet		
....0101	Service indicator	(5)	ISUP ISDN User Part
..01....	Message priority	1	
10.....	Network indicator	(2)	N National network
Octet005	Routing label		
.....	DPC: Net-Clstr-Mbr	222-222-222	
.....	OPC: Net-Clstr-Mbr	111-111-111	
00000010	SLS	2	
Octet012	Circuit identification code		
.....	CIC	5048	
00.....	Spare	0	
Octet014	ISUP Initial Address Message		
00000001	Message type	(1)	IAM Initial Address
Octet015	Nature of connection indicators parameter		
.....00	Satellite	(0)	No satellite circuit in connection
....00..	Continuity check	(0)	Continuity check not required
...1....	Echo control out	(1)	Outgoing half echo control device included

```

000..... Spare                                0
-----
Octet016 Forward call indicators parameter
-----
.....0 Nat'l/International (0) Not an incoming international call/incoming
national call
.....00. End-to-end method (0) No end-to-end method available
....0... Interworking (0) No interworking encountered (No. 7 signaling
all the way)
...0.... IAM segmentation (0) No indication
..1..... indicator (1) ISDN user part used all the way
00..... preference (0) ISDN user part preferred all the way
.....1 Orig ISDN access (1) Originating access ISDN
.....00. SCCP method (0) No indication
....0... Spare 0
...0.... PortedNumTranslation (0) Number not translated
..0..... Query On Release (0) No QoR routing attempt in progress
00..... Reserved for nat'l 0
-----
Octet018 Calling party's category parameter
-----
11100010 Cllg party category (226) National Security and Emergency Preparedness
(NS/EP) call
00000011 Pointer->user svc 3
00000110 Pointer->called # 6
00001101 Pointer->optionals 13
-----
Octet022 User service information parameter
-----
00000011 Parameter length 3
-----
Octet023 user service info octet 1
-----
...00000 Info Txfr Capability (0) Speech
.00..... Coding standard (0) ITU-T standardized coding
1..... Extension bit (1) last octet
-----
Octet024 user service info octet 2
-----
...10000 Info Transfer Rate (16) 64 Kbit/s

```


.00.....	Transfer mode	(0) Circuit mode
1.....	Extension bit	(1) last octet

Octet025 user service info octet 3

...00010	Layer 1 protocol	(2) Recommendation G.711 u-law speech
.01.....	Layer 1 identifier	1
1.....	Extension bit	(1) last octet

Octet026 Called party number parameter

00000111	Parameter length	7
.0000011	Nature of address	(3) National significant number
0.....	Odd/even	(0) even number of address signals
....0000	Reserved	00
.001....	Numbering plan	(1) ISDN (Telephony) numbering plan (ITU-T Rec. E.164, E.163)
0.....	Test Ind	(0) Not a Test Call
.....	Address signals	7038183924

Octet034 ISUP Calling Party Number Parameter

00001010	Parameter name code	(10) ISUP Calling Party Number Parameter
00000111	Parameter length	7
.0000011	Nature of address	(3) Unique national (significant) number
0.....	Odd/even	(0) even number of address signals
.....11	Screening indicator	(3) Network provided
....00..	No addr presentation	(0) Presentation allowed
.001....	Numbering plan	(1) ISDN numbering plan (ITU-T Rec. E.164)
0.....	Spare	0
.....	Address signals	7038184001

Octet043 ISUP Hop Counter Parameter

00111101	Parameter name code	(61) ISUP Hop Counter Parameter
00000001	Parameter length	1
...10100	Hop counter	20
000.....	Spare	0

Octet046 ISUP Originating Line Information Parameter

```

-----
11101010  Parameter name code    (234) ISUP Originating Line Information Parameter
00000001  Parameter length          1
00111110  Orig line info            (62) Cellular/wireless PCS service (type 2) -
mobile DN identified
-----

Octet049  ISUP Jurisdiction Information Parameter
-----

11000100  Parameter name code    (196) ISUP Jurisdiction Information Parameter
00000011  Parameter length        3
.....   Address signals    703818
-----

Octet054  ISUP Precedence Parameter
-----

00111010  Parameter name code    (58) ISUP Precedence Parameter
00000110  Length                  6
....0100  Precedence              (4) Routine (4)
...0....  Spare                   0
.10.....  Look ahead for busy  (2) Look ahead for busy not allowed
0.....  Spare                   0
.....   Network ID          1 0 0 0
.....   Service domain       4F0240
-----

Octet062  ISUP End of Optional Parameters
-----

00000000  Parameter name code    (0) ISUP End of Optional Parameters
-----

Checksum  CRC16..... 0000000000000000 hex=0000
-----

```



ATIS-0300014

**Next Generation Interconnection Interoperability (NGIIF)
Reference Document**

**Part III, Installation, Testing and Maintenance
Responsibilities for SS7 Links and Trunks**

**Attachment C
SCCP Compatibility Tests**

Version 12.0



ATIS is the leading technical planning and standards development organization committed to the rapid development of global, market-driven standards for the information, entertainment and communications industry. More than 200 companies actively formulate standards in ATIS' Committees, covering issues including: IPTV, Cloud Services, Energy Efficiency, IP-Based and Wireless Technologies, Quality of Service, Billing and Operational Support, Emergency Services, Architectural Platforms and Emerging Networks. In addition, numerous Incubators, Focus and Exploratory Groups address evolving industry priorities including Smart Grid, Machine-to-Machine, Connected Vehicle, IP Downloadable Security, Policy Management and Network Optimization.

ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications' Sectors, and a member of the Inter-American Telecommunication Commission (CITEL). ATIS is accredited by the American National Standards Institute (ANSI). For more information, please visit www.atis.org.

Notice

This document was developed by the Alliance for Telecommunications Industry Solutions' (ATIS) sponsored Next Generation Interconnection Interoperability Forum (NGIIF). The NGIIF addresses next-generation network interconnection and interoperability issues associated with emerging technologies. Specifically, it develops operational procedures which involve the network aspects of architecture, disaster preparedness, installation, maintenance, management, reliability, routing, security, and testing between network operators. In addition, the NGIIF addresses issues which impact the interconnection of existing and next generation networks and facilitate the transition to emerging technologies. All changes to this document shall be made through the NGIIF issue resolution process.

Note Regarding Previous Versions

The NIIF Reference Document was formerly known as the Network Operations Forum (NOF) Reference Document. The NOF Reference Document was published and maintained by Bellcore. The last version of the NOF Reference Document is Issue 13.

Disclaimer and Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

ATIS-0300014, NGIIF Reference Document, Part III, Installation and Maintenance Responsibilities for SS7 Links and Trunks, Attachment C, SCCP Compatibility Tests, Formerly NIIF 5009

The NGIIF Reference Document, Part III, Installation and Maintenance Responsibilities for SS7 Links and Trunks, Attachment C, SCCP Compatibility Tests is an ATIS standard developed by the NGIIF.

Published by

Alliance for Telecommunications Industry Solutions

1200 G Street, NW, Suite 500

Washington, DC 20005

Copyright © 2011 by Alliance for Telecommunications Industry Solutions

All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < <http://www.atis.org> >.

Printed in the United States of America.

SCCP Compatibility Tests

Table of Contents

1	INTRODUCTION AND TESTING ENVIRONMENT.....	4
1.1	SCCP PROTOCOL CLASS 0 COMPATIBILITY TESTING	4
1.2	TESTING ENVIRONMENT	4
1.3	DESCRIPTION OF THE SCCP PROTOCOL CLASS 0 COMPATIBILITY TESTS	4
2	SCCP COMPATIBILITY TESTS	5
3	TEST SCRIPTS	5
3.1	SUCCESSFUL UDT QUERIES/RESPONSES - FGTT IN THE TERMINATING NETWORK.....	6
3.2	FAILURE - UNASSIGNED CODES	8
3.3	FAILURE - INVALID ADDRESS INDICATOR IN THE CALLED PARTY ADDRESS	9
3.4	FAILURE GTT (TRANSLATION TYPE AND GT DIGITS).....	10
3.5	FAILURE - GTT (NO ENTRIES FOR THE GT IN TRANSLATION TABLES).....	12
3.6	FAILURE - MTP NETWORK ROUTING AT AN STP WITH GTT FUNCTIONS	13
3.7	FAILURE - OF THE SIGNALING END POINT (SEP), E.G., SERVICE-SPECIFIC DATABASE, IN THE TERMINATING NETWORK; STP PERFORMING FGTT HAS SCCP MANAGEMENT (SCMG) FUNCTIONS	14
3.8	FAILURE- OF THE SIGNALING END POINT (SEP), E.G., SERVICE SPECIFIC DATABASE, IN THE TERMINATING NETWORK	16
3.9	SUCCESSFUL UDT QUERIES/RESPONSES - FGTT IN THE ORIGINATING NETWORK.....	17
3.10	SSP AND SST MESSAGES DURING SUBSYSTEM FAILURE AND SSA MESSAGE(S) AFTER SUBSYSTEM RECOVERY - FGTT IN THE ORIGINATING NETWORK	18
3.11	SST AND SSA MESSAGES DURING SUBSYSTEM NORMAL OPERATION - FGTT IN THE ORIGINATING NETWORK	20

1 INTRODUCTION AND TESTING ENVIRONMENT

The following tests were developed by the NGIIF/SS7 Ad hoc Committee to verify the compatibility of networks during interconnection. These tests are intended to be used as a set of minimum tests of the SCCP protocol portion of the network service part for connectionless services only (Class 0).

It is assumed that the interconnecting networks may have some additional tests they may wish to perform during interconnection. In that case, these tests will be part of the bilateral agreements developed for SS7 network interconnection.

Schematics included with the test scripts indicate a minimum network configuration. The actual test network may include intermediate STPs.

1.1 SCCP Protocol Class 0 Compatibility Testing

Compatibility testing checks for the correct interworking of SCCP Protocol Class 0 Compatibility Testing implementations. The tests are written for the interconnecting of two (2) given implementations. These tests should be performed on new signaling points as well as between already connected signaling points.

The full tests suite should be run for any interconnection configuration between the interconnecting companies, unless previously tested. The configuration is defined by manufacturer model and software load of the interconnecting signaling network elements and the application being supported. Subsequent interconnections, using configurations previously tested by the interconnecting companies, may be tested at their discretion.

1.2 Testing Environment

The following test scripts provide the ability to test interconnected networks. Test scripts that have the potential to impact service are so noted.

Some test scripts indicate an insertion point for test equipment that will be used to stimulate test conditions. The test environment may be configured differently if network conditions require, provided the desired test objectives are met.

Exact message format and codings are not discussed in these tests. Bilateral discussions and pre-test agreements are required prior to executing any of the tests, in particular, the contents of the Called Party Address field to produce the desired result; either successful message translation or message failure simulation. In addition, the content of screening tables shall be discussed so that the test messages are not discarded. Message content should be discussed individually for each of the tests to be conducted.

1.3 Description of the SCCP Protocol Class 0 Compatibility Tests

The following table summarizes the set of SCCP Protocol Class 0 compatibility tests.

2 SCCP Compatibility Tests

<u>Test #</u>	<u>Test Title</u>

3.1	Successful UDT queries/responses - FGTT in the terminating network
3.2	Failure - unassigned codes
3.3	Failure - invalid Address Indicator in the called party address
3.4	Failure - GTT (Translation Type and GT digits)
3.5	Failure - GTT (no entries for the GT in translation tables)
3.6	Failure - MTP network routing at an STP with GTT functions
3.7	Failure - of the signaling end point, e.g., service-specific database, in the terminating network. STP performing FGTT has SCMG functions.
3.8	Failure - of the signaling end point, e.g., service-specific database, in the terminating network.
3.9	Successful UDT queries/responses - FGTT in the originating network
3.10	SSP and SST messages during subsystem failure and SSA message(s) after subsystem recovery - FGTT in the originating network
3.11	SST and SSA messages during subsystem normal operation FGTT in the originating network

3 Test Scripts

Test scripts for the above tests follow.

3.1 Successful UDT queries/responses - FGTT in the terminating network	S-1.1	No corresponding test

REFERENCE: ANSI T1.112, chapter 4, clause 2

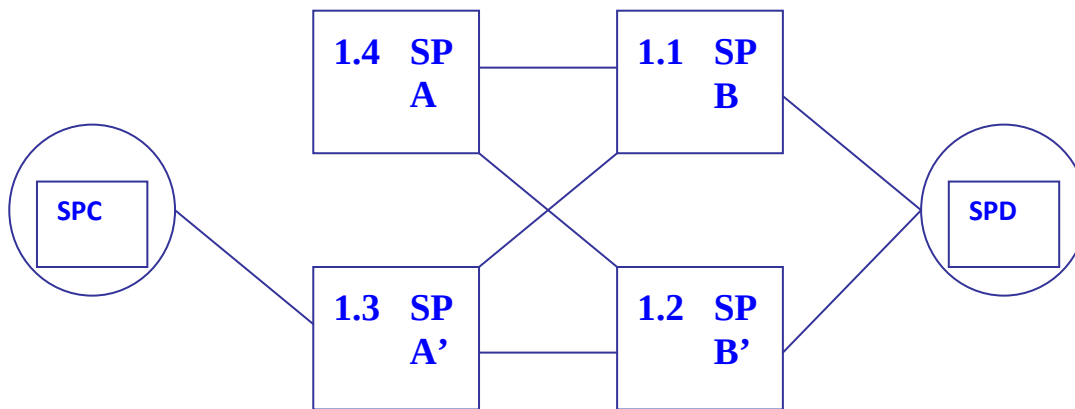
TITLE: 3.1 Successful UDT Queries/Responses -- FGTT (Final Global Title Translation) in the terminating network

PURPOSE: To verify that:

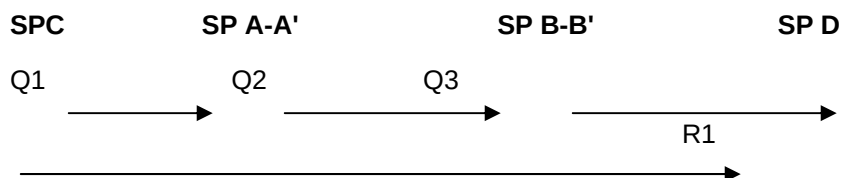
- 1.) the global title translation functions at the STPs are performed correctly;
- 2.) the UDT query message is routed correctly to the destination; and
- 3.) the UDT response message is properly returned to the query originator.

PRE-TEST CONDITIONS: Global title translation tables are populated at the appropriate STPs.

CONFIGURATION:



MESSAGE SEQUENCE:



TEST DESCRIPTION

1. Send a UDT test query message, Q1 from SP C.
2. Intermediate global title translation (IGTT) is performed at SP A (or SP A') of Network 1. UDT query message, Q2, should be routed to SP B (or SP B').
3. Final global title translation (FGTT) is performed at SP B (or SP B') of Network 2. UDT query message, Q3, should be routed to the destination SP D.
4. Verify that the UDT response message, R1, is sent from SP D and received in the correct format SP C.

NGIIF Test #:

ANSI T1.235 Test #:

TR-905 Test #

3.2 Failure - unassigned codes	S-2.1	No corresponding test

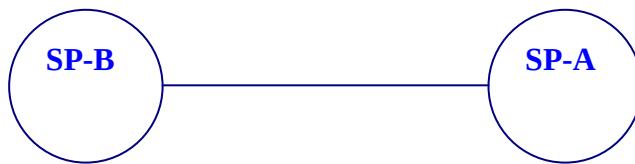
REFERENCE: ANSI T1.112, chapter 4, clause 4.3

TITLE: 3.2 Failure - unassigned codes

PURPOSE: To verify that the UDT message with unassigned codes of Message Type, Protocol Class, or Return Option will be discarded.

PRE-TEST CONDITIONS: Connect the test unit SP B to SP A.

CONFIGURATION:

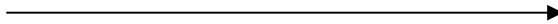


MESSAGE SEQUENCE:

SP B

SP A

Q1



TEST DESCRIPTION:

1. Send a UDT test message, Q1, from the test unit SP B to SP A. Consider testing the cases where Q1 has:
 - unassigned message type code
 - unassigned protocol class code
 - unassigned return option code.

2. Verify that in each case, the message Q1 is discarded at SP A, and no UDTS is returned.

Note: Alternatively, the test unit can be located on the A-link side of an STP, and the UDT message may be MTP routed to SP A.

3.3 Failure - invalid Address Indicator in the called party address	S-2.2	No corresponding test

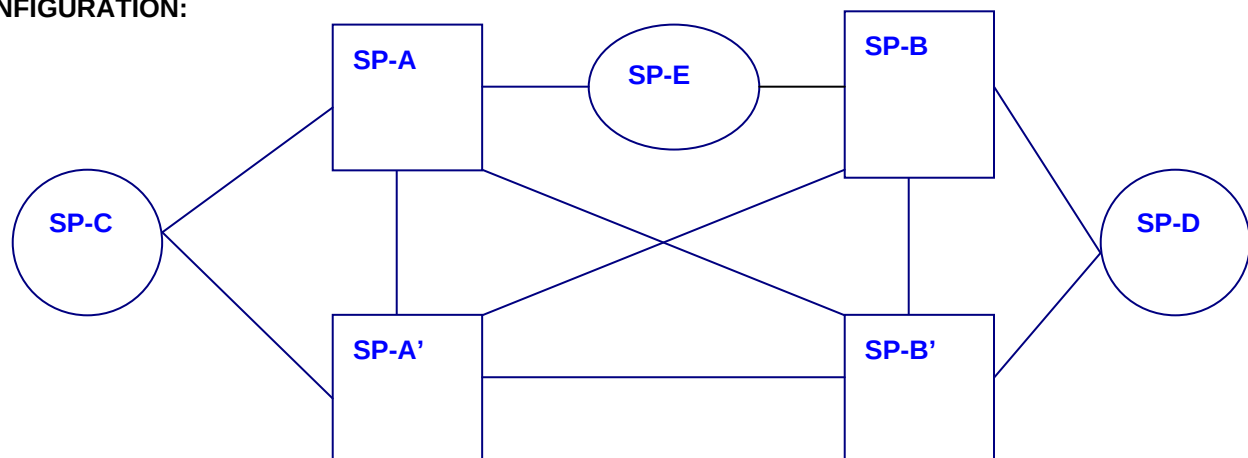
REFERENCE: ANSI T1.112, chapter 3, subclause 3.4.1 and ANSI T1.112, chapter 4, subclause 4.2

TITLE: 3.3 Failure - invalid Address Indicator in the called party address

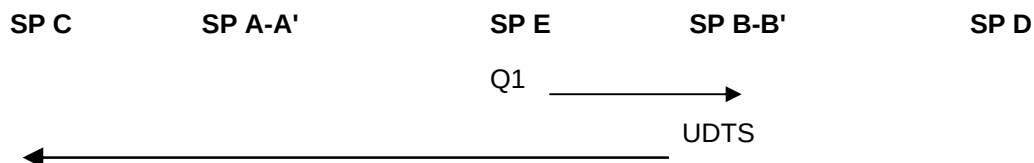
PURPOSE: To verify that the UDTS message will be returned if the information in the Address Indicator of the called party address of the sent UDT message is invalid, and the "return message on error" option is set in the sent UDT message.

PRE-TEST CONDITIONS: Insert the test unit SP E between SP A and SP B.

CONFIGURATION:



MESSAGE SEQUENCE:



TEST DESCRIPTION:

1. Send UDT test messages, Q1, from SP E to SP B, with the "return message on error" option set. Simulate Q1 as if it were the query message from SP C via SP A.
2. Test the following separate cases - invalid Address Indicators in Called Party Address (C'dPA) of Q1:
 - nat'l/int'l indicator = 0 (int'l)
 - routing indicator = 0 and global title indicator = 0
 - routing indicator = 0 and global title indicator = nor-applicable value (other than zero)
 - routing indicator = 1 and SSN indicator = 0
3. Verify that in all four cases, a UDTS is returned from SP B addressed to SPC with Return Cause set to "no translation of an address of such nature."

Notes: Alternatively, SP E can be located on the A-link side of SP A and the UDT message may be MTP routed to SP B.

3.4 Failure GTT (Translation Type and GT digits)

S-3.1

No corresponding test

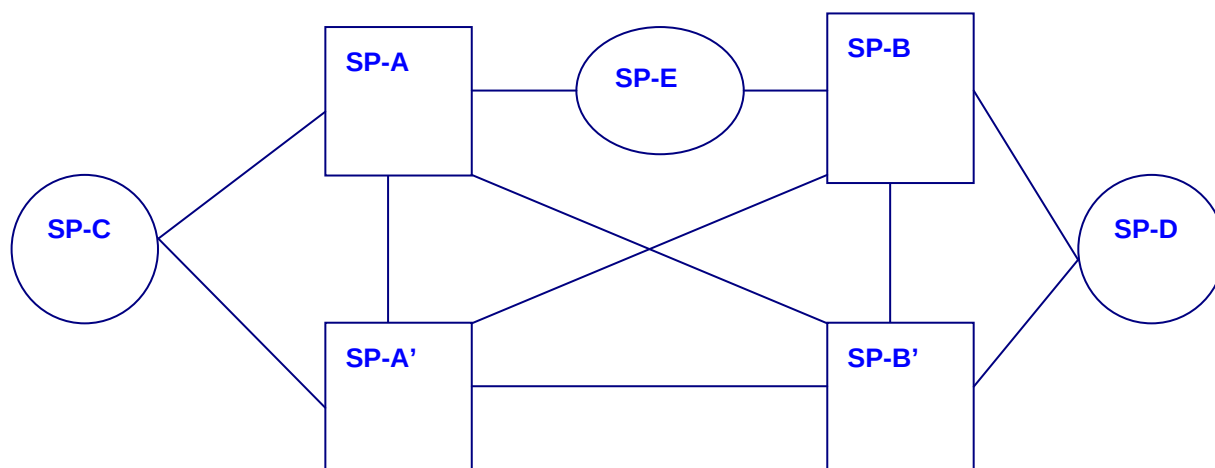
REFERENCE: ANSI T1.112, chapter 3, subclauses 3.4.2, 3.12 and ANSI T1.112, chapter 4, subclauses 2.3, 2.4, 4.2

TITLE: 3.4 Failure GTT (Translation Type and GT digits)

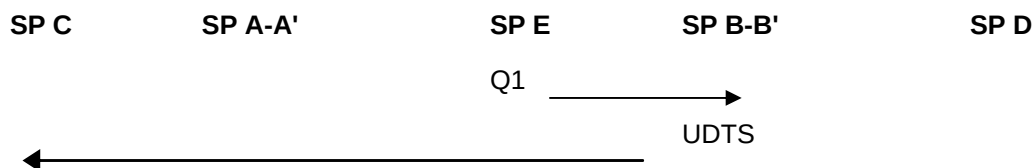
PURPOSE: To verify that the UDTS message will be returned if the information in the address of the Called Party Address of the received UDT message is invalid, i.e., invalid translation type or GT digits are outside of the applicable range, and the "return message on error" is set in the received UDT message.

PRE-TEST CONDITIONS: Insert the test unit SP E between SP A and SP B. GTT tables are populated at the appropriate STPs.

CONFIGURATION:



MESSAGE SEQUENCE:



TEST DESCRIPTION:

1. Send UDT test messages, Q1, from SP E to SP B, with the "return message on error" option set. Simulate Q1 as if it were the query message from SP C via SP A.
2. Test the following separate cases.
 - invalid translation type
 - GT digits outside of the applicable range (correct number of digits)
 - GT digits outside of the applicable range (incorrect number of digits)
3. Verify that in all cases, a UDTS is returned from SP B addressed to SP C with Return Cause set to "no translation for this specific address". Case i may fail screening, and may not return UDTS.

Note 1: Alternatively, SP E can be located on the A-link side of SP A and the UDT message may be MTP routed to SP B.

Note 2: For IGTT, SP B (SP B') belongs to an intermediate network. For FGTT, SP B (SP B') belongs to an intermediate or terminating network.

3.5 Failure - GTT (no entries for the GT in translation tables)	S-3.2	No corresponding test

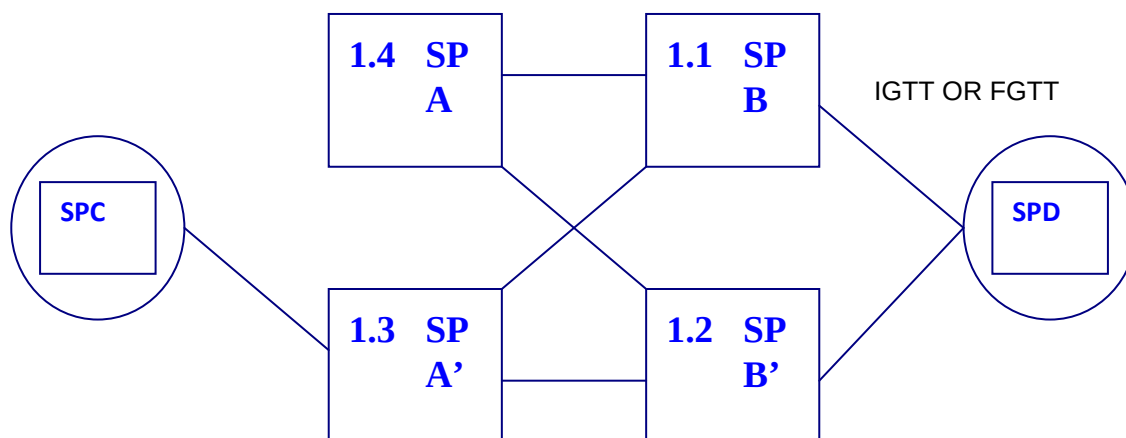
REFERENCE: ANSI T1.112, chapter 3, subclause 3.12 and ANSI T1.112, chapter 4, subclauses 2.3, 2.4, 4.2

TITLE: 3.5 Failure - GTT (no entries for the GT in translation tables)

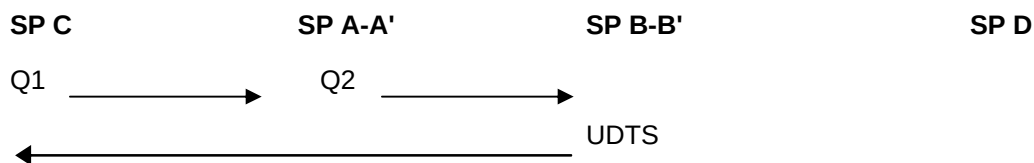
PURPOSE: To verify that a UDTS message will be returned if GTT fails due to no entries for the GT, and the "return message on error" option is set in the received UDT message.

PRE-TEST CONDITIONS: No entries in the translation tables for the GT at SP B (or SP B'). GTT tables are populated at the appropriate STPs.

CONFIGURATION:



MESSAGE SEQUENCE:



TEST DESCRIPTION:

1. Send a UDT test query message, Q1, from SP C with "return message on error" option set. The GT digits in the called party address have no corresponding entries for GTT at SP B (or SP B').
2. Verify that a UDTS is returned from SP B (or SP B') to SP C with Return Cause set to "no translation for this specific address".

Notes: For IGTT, SP B (SP B') belongs to an intermediate network. For FGTT, SP B (SP B') belongs to an intermediate or terminating network.

NGIIF Test #:	ANSI T1.235 Test #:	TR-905 Test #
3.6 Failure - MTP network routing at an STP with GTT functions	S-3.3	No corresponding test

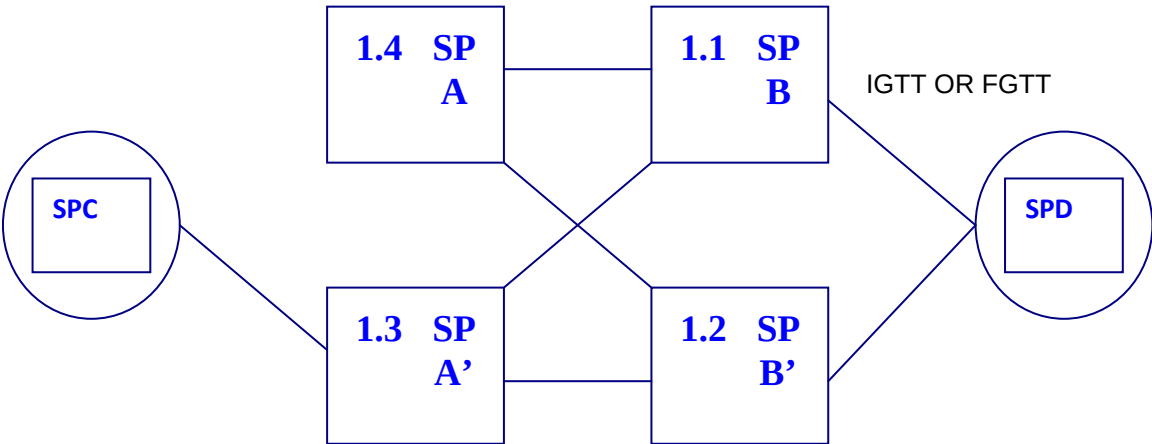
REFERENCE: ANSI T1.112, chapter 3, subclause 3.12 and ANSI T1.112, chapter 3, subclauses 2.3, 2.4, 4.2

TITLE: 3.6 Failure - MTP network routing at an STP with GTT functions

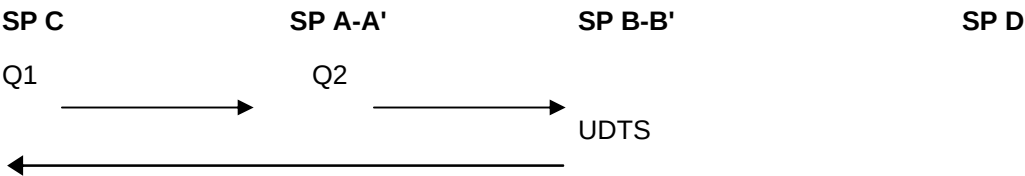
PURPOSE: To verify that a UDTS message will be returned if GTT is successful and the destination is inaccessible due to network failure, and the "return message on error" option is set in the received UDT message.

PRE-TEST CONDITIONS: GTT tables are populated at the appropriate STPs. This test can be simulated with a non-existing point code for SP D.

CONFIGURATION:



MESSAGE SEQUENCE:



TEST DESCRIPTION:

1. Send a UDT test query message, Q1, from SP C. The GT digits in the called party address have correct entries for GTT at SP A (or SP A') of the originating network, and at SP B (or SP B) of an intermediate or terminating network.
 2. Intermediate global title translation (IGTT) is performed at SP A (or SP A'). UDT query message, Q2, should be routed to SP B (or SP B').
 3. Global title translation (GTT) is performed at SP B (or SP B'). The UDT query message cannot be routed to the destination from SP B (or SP B') due to network failure.
 4. Verify that a UDTS is returned from SP B (or SP B') to SP C with Return Cause set to "network failure".
- Notes: For IGTT, SP B (SP B') belongs to an intermediate network. For FGTT, SP B (SP B') belongs to an intermediate or terminating network.

3.7 Failure - of the Signaling End Point (SEP), e.g., service-specific database, in the terminating network; STP performing FGTT has SCCP Management (SCMG) functions

S-3.4

No corresponding test

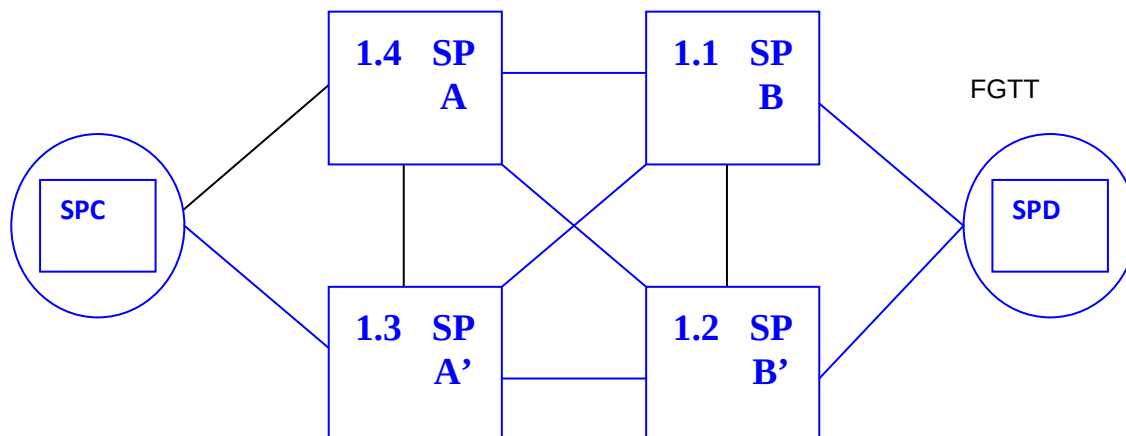
REFERENCE: ANSI T1.112, chapter 3, subclause 3.12 and ANSI T1.112, chapter 4, subclauses 2.3, 2.4, 4.2 and clause 5

TITLE: 3.7 Failure - of the Signaling End Point (SEP), e.g., service-specific database, in the terminating network; STP performing FGTT has SCCP Management (SCMG) functions

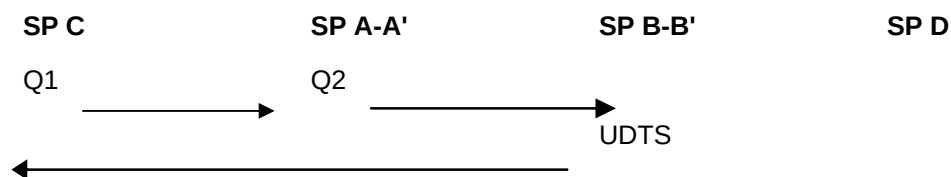
PURPOSE: To verify that a UDTs message will be returned by SP B (or SP B') if the SSN of the destination is out of service, and the "return message on error" option is set in the received UDT message.

PRE-TEST CONDITIONS: GTT tables are populated in the STPs. All replicated SSNs must be out of service.

CONFIGURATION:



MESSAGE SEQUENCE:



TEST DESCRIPTION:

1. Send a UDT test query message, Q1, from SP C.
 - Intermediate global title translation (IGTT) is performed at SP A (or SP A'). UDT query message, Q2, should be routed to SP B (or SP B').
 - Final global title translation (FGTT) is successful performed at SP B (or SP B') having SCCP Management (SCMG) functions. Consider testing the case of SSN failure, i.e., the SSN of SP D is out of service.
 - Verify that a UDTS is returned from SP B (or SP B') to SP C with Return Cause set to "SSN failure".

Notes: SP B (SP B') belongs to:

- intermediate network, or
- terminating network.

3.8 Failure- of the Signaling End Point (SEP), e.g., service specific database, in the terminating network	S-3.5	No corresponding test

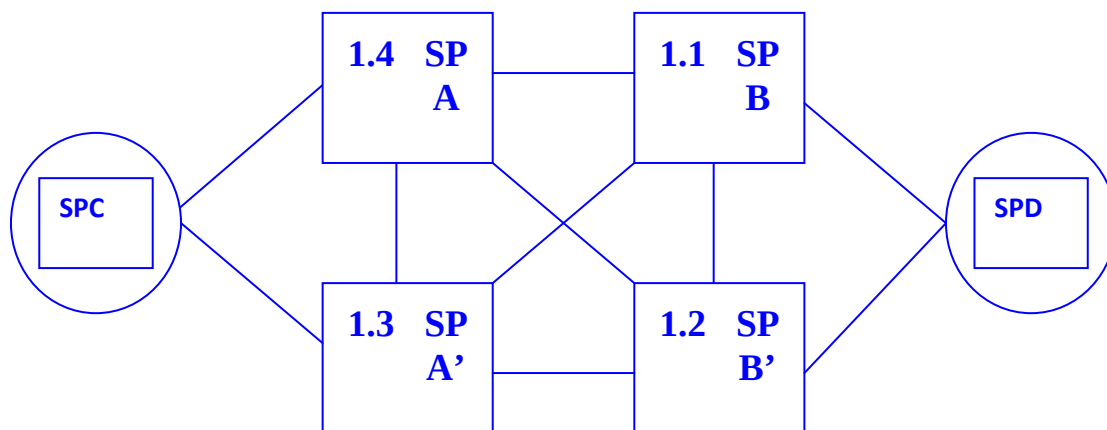
REFERENCE: ANSI T1.112, chapter 3, subclause 3.12 and ANSI T1.112, chapter 4, subclauses 2.3, 4.2

TITLE: 3.8 Failure- of the Signaling End Point (SEP), e.g., service specific database, in the terminating network

PURPOSE: To verify that a UDTS message will be returned by SP D if the SSN of the destination is either unequipped or out of service, and the "return message on error" option is set in the received UDT message.

PRE-TEST CONDITIONS: GTT tables are populated in the STPs.

CONFIGURATION:



MESSAGE SEQUENCE:



TEST DESCRIPTION:

1. Send a UDT test query message, Q1, PC routed from SP C to SP D.
2. Consider testing the two cases of the addressed SSN of SP D:
 - unequipped user; and
 - SSN failure.
3. Verify that a UDTS message is returned from SP D to SP C with Return Cause set to "unequipped user", and "SSN failure".

3.9 Successful UDT Queries/Responses - FGTT in the originating network	S-4.1	No corresponding test

REFERENCE: ANSI T1.112, chapter 3, clause 2

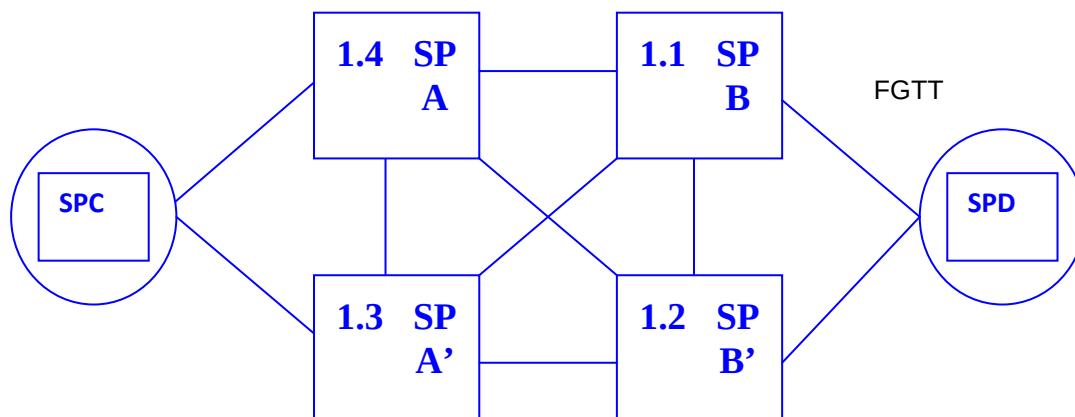
TITLE: 3.9 Successful UDT Queries/Responses - FGTT in the originating network

PURPOSE: To verify that:

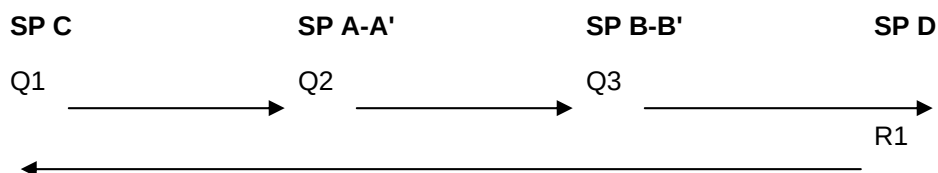
- the global title translation functions at the STPs are performed correctly
- the UDT query message is routed correctly to the destination
- the UDT response message is properly returned to the query originator.

PRE-TEST CONDITIONS: Final global title translation tables are populated at SP A and SP A'.

CONFIGURATION:



MESSAGE SEQUENCE:



TEST DESCRIPTION:

1. Send a UDT test query message, Q1, from SPC.
2. Final global title translation (FGTT) is performed at SP A (or SP A'). UDT query message, Q2, should be routed to the destination SP D via SP B (or SP B').
3. Verify that the UDT response message, R1, is sent from SP D and received in the correct format by SP C.

3.10 SSP and SST messages during subsystem failure and SSA message(s) after subsystem recovery - FGTT in the originating network	S-4.2	No corresponding test

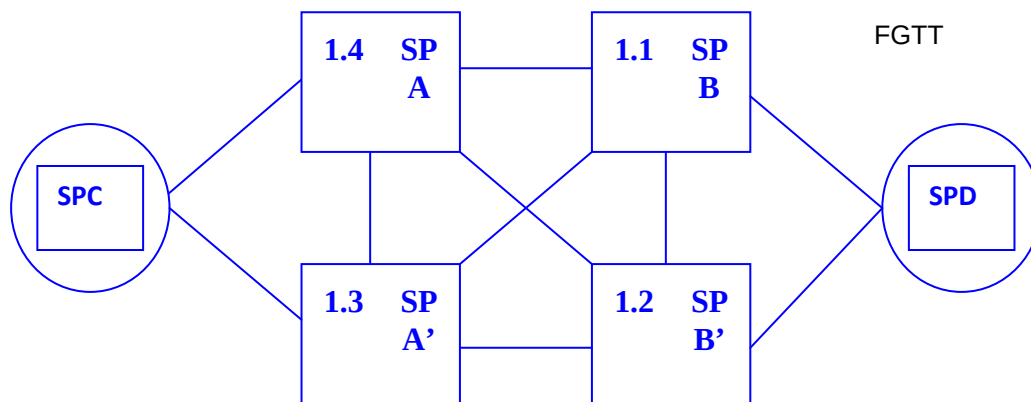
REFERENCE: ANSI T1.112, chapter 4, subclause 5.3

TITLE: 3.10 SSP and SST messages during subsystem failure and SSA message(s) after subsystem recovery - FGTT in the originating network

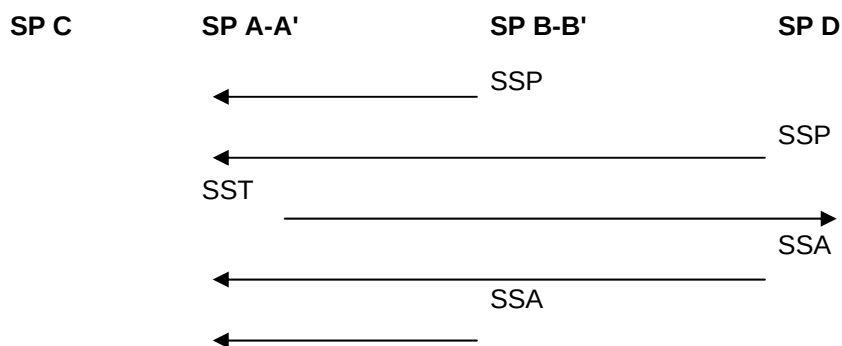
PURPOSE: To verify that the exchange of SSP and SST messages takes place during subsystem failure, and SSA message(s) after subsystem recovery.

PRE-TEST CONDITIONS: Normal query/response messages are being exchanged between the originating and terminating networks.

CONFIGURATION:



MESSAGE SEQUENCE:



TEST DESCRIPTION:

1. Make the subsystem at SP D unavailable.
2. Verify that SP A (SP A') receives a Subsystem Prohibited (SSP) message originated from SP D and/or SP B/SP B', and then stops sending SCCP query messages to SP D.
3. Verify that SP A (SP A') sends Subsystem Status Test (SST) messages periodically (30 sec's) destined to SP D, and that no SCCP query messages are sent from SP A/SP A' to the SSN at SP D.
4. Make the subsystem at SP D available.
5. Verify that SP A (SP A') receives an SSA message from
 - SP D [if SP D has SP A (SP A') as concerned point code(s), or in response to SST (without a concerned point code list at SP D)], and/or
 - SP B (SP B') [in broadcast mode].
6. Verify that SP A (SP A') starts sending SCCP query messages to the SSN at SP D.

Note 1: SP A (SP A') belongs to the originating network and performs FGTT.

Note 2: Respective network screening should allow SSP, SST and SSA.

3.11 SST and SSA <i>messages during subsystem normal operation - FGTT in the originating network</i>	S-4.3	No corresponding test

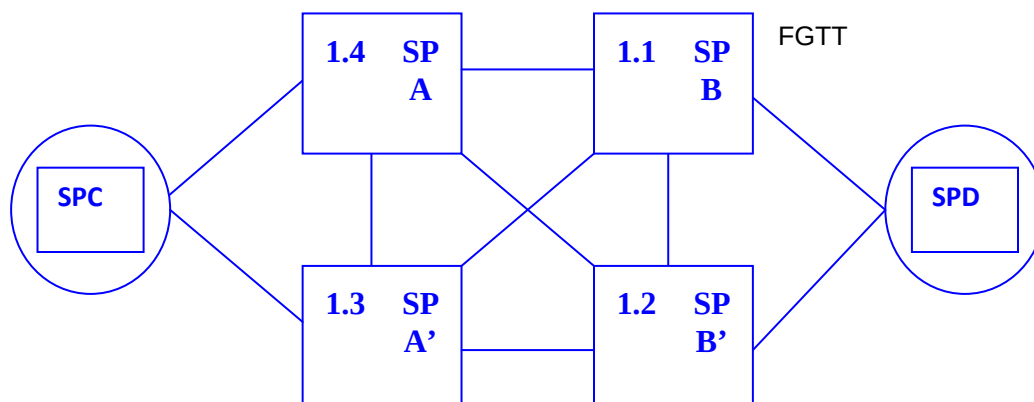
REFERENCE: ANSI T1.112, chapter 4, subclause 5.3

TITLE: 3.11 SST and SSA messages during subsystem normal operation - FGTT in the originating network

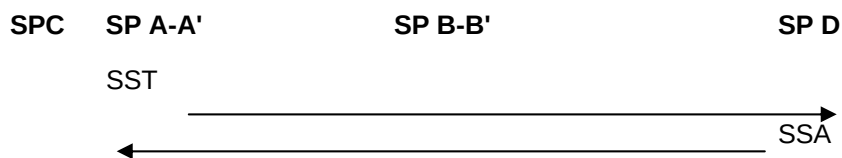
PURPOSE: To verify that an SSA message is returned from the terminating network in response to the SST.

PRE-TEST CONDITIONS: Test SSN at SP D is in service.

CONFIGURATION:



MESSAGE SEQUENCE:



TEST DESCRIPTION:

1. An SST concerning the test SSN is sent from SP A (SP A') to SP D during subsystem normal operation.
2. Verify that SP A (SP A') receives a Subsystem Allowed (SSA) message originated from SP D in response to the SST.

Note 1: SP A (SP A') belongs to the originating network and performs FGTT.

Note 2: Respective network screening should allow SST and SSA



ATIS-0300015

**Next Generation Interconnection Interoperability (NGIIF)
Reference Document**

**Part III, Installation, Testing and Maintenance
Responsibilities for SS7 Links and Trunks**

**Attachment D
Test Severity Analysis Criteria**

Version 12.0



ATIS is the leading technical planning and standards development organization committed to the rapid development of global, market-driven standards for the information, entertainment and communications industry. More than 200 companies actively formulate standards in ATIS' Committees, covering issues including: IPTV, Cloud Services, Energy Efficiency, IP-Based and Wireless Technologies, Quality of Service, Billing and Operational Support, Emergency Services, Architectural Platforms and Emerging Networks. In addition, numerous Incubators, Focus and Exploratory Groups address evolving industry priorities including Smart Grid, Machine-to-Machine, Connected Vehicle, IP Downloadable Security, Policy Management and Network Optimization.

ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications' Sectors, and a member of the Inter-American Telecommunication Commission (CITEL). ATIS is accredited by the American National Standards Institute (ANSI). For more information, please visit www.atis.org.

Notice

This document was developed by the Alliance for Telecommunications Industry Solutions' (ATIS) sponsored Next Generation Interconnection Interoperability Forum (NGIIF). The NGIIF addresses next-generation network interconnection and interoperability issues associated with emerging technologies. Specifically, it develops operational procedures which involve the network aspects of architecture, disaster preparedness, installation, maintenance, management, reliability, routing, security, and testing between network operators. In addition, the NGIIF addresses issues which impact the interconnection of existing and next generation networks and facilitate the transition to emerging technologies. All changes to this document shall be made through the NGIIF issue resolution process.

Note Regarding Previous Versions

The NIIF Reference Document was formerly known as the Network Operations Forum (NOF) Reference Document. The NOF Reference Document was published and maintained by Bellcore. The last version of the NOF Reference Document is Issue 13.

Disclaimer and Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

ATIS-0300015, NGIIF Reference Document, Part III, Installation and Maintenance Responsibilities for SS7 Links and Trunks, Attachment D, Test Severity Analysis Criteria, Formerly NIIF 5018

The NGIIF Reference Document, Part III, Installation and Maintenance Responsibilities for SS7 Links and Trunks, Attachment D, Test Severity Analysis Criteria, is an ATIS standard developed by the NGIIF.

Published by

Alliance for Telecommunications Industry Solutions

1200 G Street, NW, Suite 500

Washington, DC 20005

Copyright © 2011 by Alliance for Telecommunications Industry Solutions

All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < <http://www.atis.org> >.

Printed in the United States of America.

Test Severity Analysis Criteria

Table of Contents

1	SEVERITY LEVELS	4
2	REASONS	4
3	LEVEL 2 SS7 LINK TEST	4
4	LEVEL 2 SS7 LINK TEST	5
5	LEVEL 3 SS7 LINK TEST	6
6	ISUP TESTS.....	7
7	SCCP MANAGEMENT MESSAGES ACROSS SS7 NETWORKS	8

1 Severity Levels

1. Very low probability of causing Network Harm.
2. Low probability of causing Network Harm.
3. May cause Network harm if tests run for a long time or are improperly performed.
4. Will cause Network harm if tests run for a long time or are improperly performed.
5. Too risky to be performed during normal Traffic periods.
6. Not recommended to be done where it affects Live network traffic.

2 Reasons

Tests are only performed over test trunks that are not yet carrying live traffic. There should be minimal or no affect on other trunks or the switch itself.

Only affects one Link.

Tests are only performed over test trunks that are not carrying live Traffic. Other trunks and the switch itself may be affected.

Affects two or more Links.

Test Scripts messages may cause problems if they are left on for a long time.

Test Scripts messages could enter the network.

Test Scripts messages will not go over the network.

May be disruptive to live signaling.

High probability of being disruptive to live signaling.

Will be disruptive to live signaling.

3 Level 2 SS7 Link Test

The tests listed are referenced in Part III, Attachment A.

TEST DESCRIPTION	NGIIF TEST #	SEVERITY LEVEL	REASON	TYPE
Timer T2	1.1	1	B & G	I*
Timer T3	1.2	1	B & G	I*
Timer T1 & T4	1.3	1	B & G	I*
Timer T1 & Emergency	1.4	1	B & G	I*

Deactivation during Initial Alignment	1.5	1	B & G	I*
Deactivation during Alignment	1.6	1	B & G	I*
SIO received during Link In-Service	1.7	1	B & G	I*
SIOs received during In-Service State	1.8	1	B & G	I*
Deactivation during the Proving Period	1.9	1	B & G	I*
Break Transmission Path	1.10	1	B & G	I*
Corrupt FIBs	1.11	1	B, E & G	I*
Flag Insertion within OCTET Boundaries	1.12	1	B, E & G	I*
Signal Unit Error Rate Monitor	1.13	1	B & G	I*
Signal Unit Error Rate Monitor	1.14	1	B & G	I*
Consecutive Corrupt Signaling Units	1.15	1	B & G	I*

I* = INTRUSIVE TESTS

The interconnecting circuit shall be interrupted, with the testing unit inserted into the circuit and acting as an emulator to the signaling point under test.

NI* = NON-INTRUSIVE TESTS

The test shall be able to observe traffic traversing the link(s) between the two (2) signaling points in a monitor mode.

4 Level 2 SS7 Link Test

The tests listed are referenced in Part III, Attachment A.

TEST DESCRIPTION	NGIIF #	TEST	SEVERITY LEVEL	REASON	TYPE
Alignment Error Rate Monitor	1.16	1		B & G	I*
Alignment Error Rate Monitor	1.17	1		B & G	I*
Negative Acknowledgement	1.18	1		B & G	I*
Retransmission Buffer Full	1.19	1		B & G	I*
Erroneous FIB	1.20	1		B, E & G	I*
Erroneous Retransmission of Multiple FISU's	1.21	1		B, E & G	I*
Abnormal Backward Sequence Number	1.22	1		B & G	I*
Abnormal Backward Sequence Number	1.23	1		B & G	I*
Delay of Acknowledgement	1.24	1		B & G	I*
Normal Align	1.38	1		B & G	NI*

Broken Transmission Path	1.39	1	B & G	NI*
MSU Transmission and Reception	1.40	2	B & F	NI*

I* = INTRUSIVE TESTS

The interconnecting circuit shall be interrupted, with the testing unit inserted into the circuit and acting as an emulator to the signaling point under test.

NI* = NON-INTRUSIVE TESTS

The test shall be able to observe traffic traversing the link(s) between the two (2) signaling points in a monitor mode.

5 Level 3 SS7 Link Test

The tests listed are referenced in Part III, Attachment A.

TEST DESCRIPTION	NGIIF #	TEST LEVEL	SEVERITY	REASON	TYPE
Link Activation - Multi Links	1.25	1		D & G	I
Discrimination of Invalid Point Code	1.26	1		D & G	I
Load Distribution	1.27	1		D & G	NI
Load Sharing between Link Sets/between Two (2) Link Sets	1.28	1		D & G	NI
Changeover initiated at one side of a Link Set	1.29	3		D & G	NI
Changeover to alternate Link Set	1.30	3		D, G & I	NI
Change-Back within a Link Set	1.31	3		D, G & I	NI
Change-Back from another Link Set	1.32	2		D, G & I	NI
Inhibit Available Link	1.33	2		C, G & I	NI
Inhibit Unavailable Link	1.34	2		C, G & I	NI
Inhibit Denied	1.35	5		D, G & H	NI
Management Un-Inhibit with Change-Back	1.42	2		D, G & I	NI
Manual Un-Inhibition of a Link without Change-Back	1.43	1		D & G	NI
Link Forced Un-Inhibit	1.44	5		D & G	NI
Management Inhibiting Test	1.37	3		D & G	NI
Signaling Route Management Tests	1.45	5		D, F & H	I
	1.46	5		D, F & H	I

1.47	5	D, F & H	I
1.48	5	D, F & H	I
1.49	4	D, F & H	I

I* = INTRUSIVE TESTS

The interconnecting circuit shall be interrupted, with the testing unit inserted into the circuit and acting as an emulator to the signaling point under test.

NI* = NON-INTRUSIVE TESTS

The test shall be able to observe traffic traversing the link(s) between the two (2) signaling points in a monitor mode.

6 ISUP Tests

The tests listed are referenced in Part III, Attachment B.

TEST DESCRIPTION	NGIIF #	TEST SEVERITY LEVEL	REASON	TYPE
Circuit Validation Test (CVT) EO-IC (Org) * (CVT) AT-IC (Org) * (CVT) IC-EO (Term)* (CVT) IC-AT (Term)*	2.1	1	A	NI
Continuity Check Request (CCR) EO-IC (Org) * (CCR) AT-IC (Org) * (CCR) IC-EO (Term) * (CCR) IC-AT (Term) * (CCR) EO-AT-IC (Org) *	2.2	1	A	NI
Continuity Test Successful *	2.3	1	A	NIEO-IC (Org)
Continuity Test Unsuccessful EO-AT-IC (Org) *	2.4	1	A	NI
Continuity Test - Previous Circuit	2.5	1	A	NI
Continuity Test Successful - CRM	2.6	1	A	NI
Continuity Unsuccessful - CRM	2.7	1	A	NI
Single Circuit Block/Unblock	2.8	1	A	NI BLO/UBL
Single Circuit Block/Reset Circuit/ Unblock - BLO/RSC/UBL	2.9	3	C	NI

I* = INTRUSIVE TESTS

The interconnecting circuit shall be interrupted, with the testing unit inserted into the circuit and acting as an emulator to the signaling point under test.

NI* = NON-INTRUSIVE TESTS

The test shall be able to observe traffic traversing the link(s) between the two (2) signaling points in a monitor mode.

7 SCCP Management Messages Across SS7 Networks

The tests listed are referenced in Part III, Attachment C.

TEST DESCRIPTION	NGIIF #	TEST	SEVERITY	REASON	TYPE
			LEVEL		
Successful UDT Queries/Responses - FGTT	3.1		2	F	
Failure - Unassigned Codes	3.2		1	G	
Failure - Invalid Address Indicator in Called Party	3.3		1	G	
Failure - GTT (TT & GT Digits)	3.4		1	G	
Failure - (no entries for GT)	3.5		1	G	
Failure - MTP Network Routing at an STP with GTT Functions	3.6		1	G	
Failure - of the Signaling End Point	3.7		6	J	
Failure - of the Signaling End Point	3.8				
Successful UDT Queries/Responses - FGTT in the Originating Network	3.9		2	F	
SSP/SST and SSA - FGTT in Originating Network	3.10		6	J	
SST/SSA - FGTT in Originating Network	3.11		2	F	



ATIS-0300016

**Next Generation Interconnection Interoperability (NGIIF)
Reference Document**

**Part III, Installation, Testing and Maintenance
Responsibilities for SS7 Links and Trunks**

**Attachment E
SS7 Network Gateway Screening**

Version 12.0



ATIS is the leading technical planning and standards development organization committed to the rapid development of global, market-driven standards for the information, entertainment and communications industry. More than 200 companies actively formulate standards in ATIS' Committees, covering issues including: IPTV, Cloud Services, Energy Efficiency, IP-Based and Wireless Technologies, Quality of Service, Billing and Operational Support, Emergency Services, Architectural Platforms and Emerging Networks. In addition, numerous Incubators, Focus and Exploratory Groups address evolving industry priorities including Smart Grid, Machine-to-Machine, Connected Vehicle, IP Downloadable Security, Policy Management and Network Optimization.

ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications' Sectors, and a member of the Inter-American Telecommunication Commission (CITEL). ATIS is accredited by the American National Standards Institute (ANSI). For more information, please visit www.atis.org.

Notice

This document was developed by the Alliance for Telecommunications Industry Solutions' (ATIS) sponsored Next Generation Interconnection Interoperability Forum (NGIIF). The NGIIF addresses next-generation network interconnection and interoperability issues associated with emerging technologies. Specifically, it develops operational procedures which involve the network aspects of architecture, disaster preparedness, installation, maintenance, management, reliability, routing, security, and testing between network operators. In addition, the NGIIF addresses issues which impact the interconnection of existing and next generation networks and facilitate the transition to emerging technologies. All changes to this document shall be made through the NGIIF issue resolution process.

Note Regarding Previous Versions

The NIIF Reference Document was formerly known as the Network Operations Forum (NOF) Reference Document. The NOF Reference Document was published and maintained by Bellcore. The last version of the NOF Reference Document is Issue 13.

Disclaimer and Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

ATIS-0300016, NGIIF Reference Document, Part III, Installation and Maintenance Responsibilities for SS7 Links and Trunks, Attachment E, SS7 Network Gateway Screening, Formerly NIIF 5011

The NGIIF Reference Document, Part III, Installation and Maintenance Responsibilities for SS7 Links and Trunks, Attachment E, SS7 Network Gateway Screening, is an ATIS standard developed by the NGIIF.

Published by

Alliance for Telecommunications Industry Solutions

1200 G Street, NW, Suite 500

Washington, DC 20005

Copyright © 2011 by Alliance for Telecommunications Industry Solutions

All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < <http://www.atis.org> >.

Printed in the United States of America.

SS7 NETWORK GATEWAY SCREENING

Table of Contents

1	GENERAL.....	4
1.1	SS7 NETWORK GATEWAY SCREENING	4
1.2	ESSENTIAL MTP MANAGEMENT INHIBIT/UNINHIBIT/TEST	4
1.3	ESSENTIAL SIGNALING ROUTE MANAGEMENT MESSAGES.....	4
1.4	ESSENTIAL SIGNALING TRAFFIC MANAGEMENT MESSAGES	4
1.5	ALLOWED SIGNALING NETWORK TESTING AND MAINTENANCE MESSAGE	5
1.6	ESSENTIAL ISUP MESSAGES	5
1.7	ESSENTIAL SCCP (TCAP) MESSAGES.....	5
1.8	ESSENTIAL SCCP MANAGEMENT MESSAGES.....	6
1.9	DESIRABLE SS7 MESSAGES	6
1.10	PROTOCOL AMBIGUITIES/ISSUES/CONCERNS	6
1.11	HUBBING INTERCONNECT TEST	6
1.12	SS7 MESSAGE TYPE VALUES	6
1.13	GATEWAY SCREENING POLICIES REFERENCE	8
1.14	OPTIONAL BLANK GATEWAY SCREENING POLICY FORM	15
1.15	GLOSSARY	16

1 General

1.1 SS7 Network Gateway Screening

SS7 messages will only be allowed to pass from one network to another, between network elements which have been identified by both networks as a supporting element of a jointly provided service or application. A network element will be specified by OPC, DPC, C'gPA, C'dPA.

Other message fields applicable to screening include, but are not limited to, SI, PRI, H0-H1, message type, internetwork translation types, APC, ASSN, and DF. Where applicable, appropriate values are specified/assigned in national standards.

Network Gateway Screening tables are configured based on the requirements and security concerns of the screening network. At the time of network interconnection, both networks should share screening information, to ensure no network incompatibility has been introduced by the interaction of the screening functions.

After interconnection is established, screening changes which affect the terms and conditions of the interconnection agreement require prior notification to the affected interconnected network provider.

1.2 Essential MTP Management Inhibit/Uninhibit/Test

- Link Inhibit (LIN)
- Link Inhibit Acknowledgement (LIA)
- Link Uninhibit (LUN)
- Link Uninhibit Acknowledgment (LUA)
- Link Inhibit Denied (LID)
- Link Forced Uninhibit (LFU)
- Link Local Inhibit (LLI)
- Link Remote Inhibit Test (LRI)

1.3 Essential Signaling Route Management Messages

- Transfer Prohibited/Transfer Cluster Prohibited (TFP/TCP)
- Transfer Allowed/Transfer Cluster Allowed (TFA/TCA)
- Transfer Restricted/Transfer Cluster Restricted (TFR/TCR)
- Route Set Test (RSM)
- Transfer Controlled (TFC)
- Route Set Congestion Test (RCT)

1.4 Essential Signaling Traffic Management Messages

- Changeover (COO)
- Changeover Acknowledgement (COA)
- Emergency Changeover (ECO)
- Emergency Changeover Acknowledgement (ECA)
- Changeback (CBO)
- Changeback Acknowledgement (CBA)

1.5 Allowed Signaling Network Testing and Maintenance Message

- Signaling Link Test Message (SLTM)
- Signaling Link Test Acknowledgement (SLTA)

1.6 Essential ISUP Messages

- Address Complete (ACM)
- Answer (ANM)
- Blocking (BLO)
- Blocking Acknowledgement (BLA)
- Circuit Group Blocking (CGB)
- Circuit Group Blocking Acknowledgement (CGBA)
- Circuit Group Reset (GRS)
- Circuit Group Reset Acknowledgement (GRA)
- Circuit Group Unblocking (CGU)
- Circuit Group Unblocking Acknowledgement (CGUA)
- Circuit Query (CQM)
- Circuit Query Response (CQR)
- Circuit Reservation Acknowledgement Message (CRA)
- Circuit Reservation Message (CRM)
- Circuit Validation Response (CVR)
- Circuit Validation Request (CVT)
- Continuity (COT)
- Continuity Check Request (CCR)
- Initial Address (IAM)
- Loop Back Acknowledgement (LPA)
- Release (REL)
- Release Complete (RLC)
- Reset Circuit (RSC)
- Resume (RES)
- Suspend (SUS)
- Unblocking (UBL)
- Unblocking Acknowledgement (UBA)
- Unequipped Circuit Identification Code (UCIC)

1.7 Essential SCCP (TCAP) Messages

- Unit Data (UDT)

- Unit Data Service (UDTS)

1.8 Essential SCCP Management Messages

- Subsystem Prohibited (SSP)
- Subsystem Allowed (SSA)
- Subsystem Test (SST)

1.9 Desirable SS7 Messages

- MTP Routing Verification Test (MRVT)
- SCCP Routing Verification Test (SRVT)

1.10 Protocol Ambiguities/Issues/Concerns

- TFP response method is recommended at the STP gateways.
- TFR response method is recommended at the STP gateway.

TCx - Some vendors do not support TCx messages. There are protocol ambiguities in the ANSI standards regarding the Transfer Cluster and Route Set Test (cluster) procedures that need to be clarified in T1 standards.

TFC - There are only two methods currently available within the North American network to handle Signaling Message Congestion and Signaling Message Transmit Congestion. These methods are Message Discard and Transmit Congestion Control. Each of these methods has significant impact on messages attempting to cross a point of congestion and on the signaling end-nodes attempting to utilize that point of congestion. Message Discard alone will shed offered traffic at the point of congestion. Transmit Congestion Control will attempt to reduce offered traffic at it's source, notifying the sending SP utilizing the TFC message and then shed traffic at the point of congestion using Discard if TFC alone does not relieve the congestion. It is important that network operators understand the consequences of each method. Determination of which method to utilize should be agreed to between interconnected network operators.

1.11 Hubbing Interconnect Test

The NGIIF recommend that the Hubbing Interconnect MTP test be performed. This test can be found in Attachment A - MTP Compatibility Tests.

1.12 SS7 Message Type Values

Table 1: SI Values

SI	Message Type	Description	Notes
0	Signaling Network Management	Network Management Messages	See SI 0 H0 H1 Table
1	Signaling Network Test (Regular)	Link Test Messages (Regular)	

2	Signaling Network Test (Special)	Link Test Messages (Special)	
3	SCCP	CLASS/LNP/CNAM/ Toll Free etc	
4	TUP	Telephone User Part	Unused?
5	ISDNUP	Call Setup/Trunk Maintenance	
6	Banded Signaling		Unused?

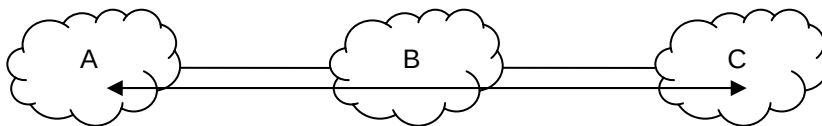
Table 2: SI 0 H0 and H1 Values

Message Type	Acronym	Service Information Octet	H0	H1	Notes
Level 2 Link Management	LSSU				
Change Over Order	COO	0	1	1	
Change Over Acknowledgement	COA	0	1	2	
Change Back Declaration	CBD	0	1	5	
Change Back Acknowledgement	CBA	0	1	6	
Emergency Changeover Order	ECO	0	2	1	
Emergency Changeover Ack.	ECA	0	2	2	
Signaling Route Set Congestion Test	RCT	0	3	1	
Transfer Controlled	TFC	0	3	2	
Transfer Prohibited	TFP	0	4	1	
Transfer Cluster Prohibited	TCP	0	4	2	
Transfer Restricted	TFR	0	4	3	
Transfer Cluster Restricted	TCR	0	4	4	
Transfer Allowed	TFA	0	4	5	
Transfer Cluster Allowed	TCA	0	4	6	
Signaling Route Set Prohibited	RSP	0	5	1	
Signaling Route Set Restricted	RSR	0	5	2	
Signaling Route Set Prohibited Cluster	RCP	0	5	3	
Signaling Route Set Restricted Cluster	RCR	0	5	4	
Link Inhibit	LIN	0	6	1	
Link Uninhibit	LUN	0	6	2	

Link Inhibit Acknowledgement	LIA	0	6	3	
Link Uninhibit Acknowledgement	LUA	0	6	4	
Link Inhibit Denial	LID	0	6	5	
Link Force Uninhibit	LFU	0	6	6	
Link Local Inhibit Test	LLI	0	6	7	
Link Remote Inhibit Test	LRI	0	6	8	
Traffic Restart Allowed	TRA	0	7	1	
Traffic Restart Waiting	TRW	0	7	2	
Signaling Data Link Connection Order	DLC	0	8	1	Unused?
Signaling Data Link Connection Successful		0	8	2	Unused?
Signaling Data Link Connection Not Successful		0	8	3	Unused?

1.13 Gateway Screening Policies Reference

SS7 networks may transport SS7 signaling messages between parties. A carrier (B) with an SS7 network, with SS7 connections to parties A and C, can, with appropriate permissions and translations, deliver SS7 messages received from Party A to Party C.

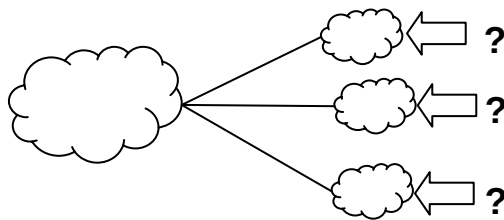


A potential problem exists when an SS7 network delivers messages from more than one sending party to a given receiving party. (The terms “sending” and “receiving” are used as opposed to “source” and “destination” to allow for the possibility that the “sending” party need not be the originator of the message, and the “receiving” party is not necessarily its ultimate destination.)

The SS7 protocol has no mechanism for authenticating the identities of message originators contained in the Originating Point Code and/or the Calling Party Address parameters. These parameters, like all other SS7 parameters, are assumed to be populated correctly by their originating network element. Messages that are generated by one node, but which improperly contain the point code of another node in either the Originating Point Code and / or Calling Party Address can be referred to as being “spoofed” messages. Spoofed messages are viewed as hazardous because they can cause receiving network elements to take measures in response to conditions that do not actually exist. Spoofed messages can enter a network either through a compromise in the integrity of targeted network (e.g., a compromised switch or facility), or from a directly or indirectly interconnected network which has mistakenly accepted it or improperly generated it.

A network can perform screening on the messages that it receives from a prior SS7 network to insure that their Originating Point Code and/or Calling Party Address are consistent with the traffic expected from the prior network. But each network must rely on the screening performed by the previous network that handles a message. The receiving network is unable to distinguish whether the received message actually came from the party identified in that parameter. If, for example, an intermediate SS7 network delivers traffic from parties W, X and Y to network Z over a given interconnection, then network Z has no ability to determine whether messages having a point code from party W in the Originating Point Code or Calling Party Address were actually received (by the intermediate SS7 network) from party W, as opposed to parties X or Y. Network Z can only be assured that the given message was sent by party W if the intermediate SS7 network (as well as any other intermediate networks) has performed originator screening at the point of its interconnection with party W.

Each signaling network therefore relies on the authentications performed by preceding signaling networks, and may want to understand the screening policies employed by those networks.



Similarly, a signaling network may pass signaling to many different receiving networks. As a result, intermediate networks may receive inquiries from multiple networks about their screening policies.

In order to facilitate discussions about screening and authentication that may occur among multiple networks, a common format for documenting screening practices has been developed. The tables below have been developed to describe the screening that is applied to each message type, covering OPC, DPC, CgPA and CdPA and other header parameters, as appropriate. These tables may also indicate the extent to which addresses are screened (i.e., Network ID only, Network ID and Cluster Number, or full point code). It is suggested that a signaling network provider use the tables to determine the policies for screening different signaling link access arrangements (A-links, B-links, etc.).

Example screening guidelines for each of the following type of signaling link connections are provided:

- A-links (and E-links) [Reference A-link example]
- B/D-links [Reference B/D-link example]
- F-links [Reference F-link example]

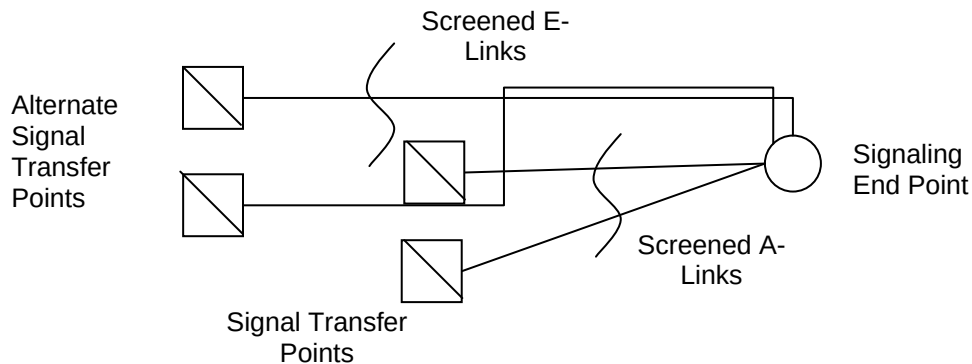
C-links are not expected to be external connections, and therefore no screening example is provided.

The examples demonstrate reasonable screening policies for common situations. They may be used as a guide when developing screening policies. These examples assume traditional PSTN network configurations. Specific policies may need to consider individual technical and business circumstances applicable to the connection(s).

Notes for A-link Example (Also addressing E-links)

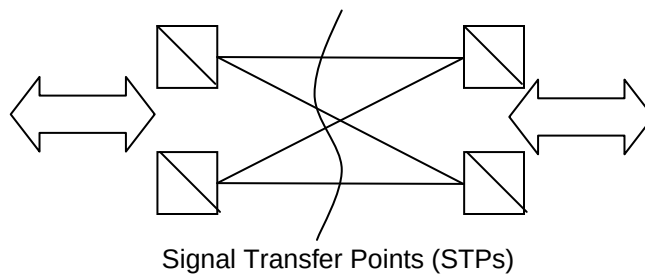
A-links connect signaling end points to an STP. Such end points originate or terminate signaling messages. Depending on the services provided by the signaling end point, it may originate and terminate ISUP and/or TCAP signaling.

E-links connect a signaling end point to an alternate pair of STPs, and operate in the same manner as A-links. The same screening as identified for A-links would be appropriate for E-links.



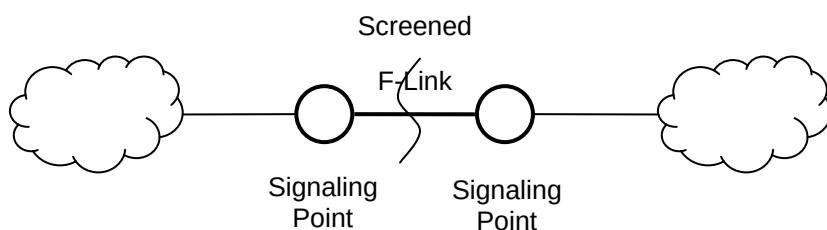
Notes for B/D-link Example

B/D-links connect one pair of STPs to another pair of STPs, and may pass ISUP and/or TCAP signaling depending on the arrangements between the networks.



Notes for F-Link Example

Signaling points on each end of the subject F-link may have connectivity to additional signaling points via A-links, E-links, or F-links. This example screening policy is appropriate for an F-link that carries ISUP signaling only locally between the two signaling points connected by the F-link. This screening policy assumes that TCAP signaling may originate or terminate at signaling points beyond the ends of the F-links.



Notes for Signaling Link Concentrators

Signaling link concentrators are devices that aggregate signaling traffic between multiple signaling points and their serving STPs. If the device performs network management functions on the connections between itself and the signaling points it serves, and those network management functions are visible to the serving STPs (e.g., if the concentrator generates TFX messages), then the signaling link concentrator devices should be subject to the B/D-link screening policy. If that local management between the concentrator and signaling points is not visible to the serving STPs, then the arrangement simply looks like a signaling point assigned multiple point codes, and the A-link screening policy would apply.

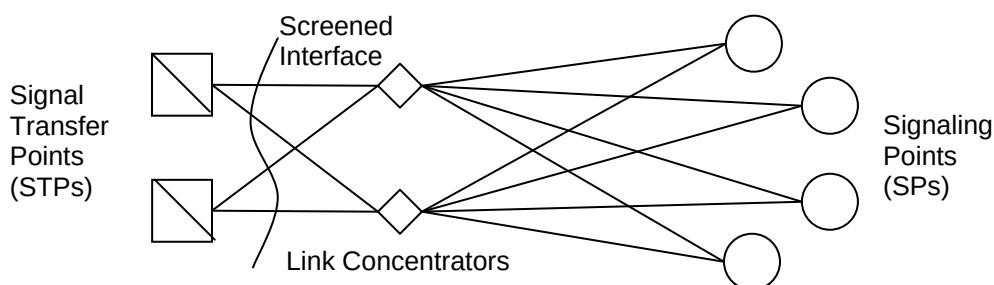


Table 3: B/D Link Screening Policy, External Links

OPC	Msg Type	SI	H0	H1	DPC	Nat /Int	CgPA	CdPA	TT	Aff PC/SSN	Notes
	L2 Link Mgt	NA	NA	NA	Screening Not performed on Level 2 messages						
Link Far End	CO/CB/ECO	0	1&2	All	Self	N					
Agree STP's along signaling path	TFC	0	3	2	Agree per signaling relation	N				Agree per signaling relation	
Agree per signaling relation	RCT	0	3	1	Agree per signaling relation	N					
Link Far End	TFP/TFR/TFA	0	4	All	Self	N				Agree per signaling and link relation	

Link Far End	RSM	0	5	All	Self	N				Agree per signaling relation	
Link Far End	Mgt Inhibit	0	0-6	All	Self	N					
Link Far End	Traffic Restart	0	7	All	Self	N					
Link Far End	Signaling Link Test	1&2	NA	NA	Self	N					
Link Far End	MTP User UA	0	10	1	Agree	N					
Agree per signaling relation	SCCP Msgs	3	NA	NA	Agree per signaling relation	N	Agree per signaling relation	Agree per signaling relation	Agree per signaling relation		
Agree per signaling relation	ISUP	5	NA	NA	Agree per signaling relation	N					

Table 4: A-Link Screening Policy, External Links, ISUP and/or TCAP services (Also for E-Links and A-Link Concentrators)

OPC	Msg Type	SI	H0	H1	DPC	Nat/Int	CgPA	CdPA	TT	Affected PC/SSN	Notes
	L2 Link Mgt	NA	NA	NA	Screening not performed on Level 2 messages.						1
Link Far End	CO/CB/ECO	0	1 or 2	Any defined	Self	Natl					
Link Far End	RCT	0	3	1	By Agreement	Natl					
Block All	TFC	0	3	2	Block All						2
Block All	TFP/TFR/TFA	0	4	Any defined	Block All						2
Link Far End	RSM	0	5	Any defined	<u>Self</u>	Natl				<u>By Agreement</u>	
Link Far End	Mgt Inhibit	0	6	Any defined	Self	Natl					

Link Far End	Traffic Restart	0	7	Any defined	Self	Natl					
Link Far End	MTP User UA	0	10	1	By Agreement	Natl					3
Link Far End	Signaling Link Test Msgs	1 or 2	NA	NA	Self	Natl					
Link Far End	SCCP Msgs	3	NA	NA	By Agreement	Natl	Link Far End	By Agreement	By Agreement		3
Link Far End	ISUP	5	NA	NA	By Agreement	Natl					3

Notes:

- 1) Link management messages have no address field and are limited to the local interface.
 - 2) Message type not expected in this configuration
 - 3) Assumes both ISUP and TCAP messages are allowed. Otherwise only agreed message types (ISUP or TCAP) allowed.
- "By Agreement" means that the A-link user and DPC have both indicated their agreement to exchange this type of message.
 - All messages not defined by the table should be blocked.

Table 5: F-Link Screening Policy, External Links, ISUP and/or TCAP services (Assumes only direct ISUP signaling)

OPC	Msg Type	SI	H0	H1	DPC	Nat/Int	CgPA	CdPA	TT	Affected PC/SSN	Notes
	L2 Link Mgt	NA	NA	NA	Screening not performed on Level 2 messages.						1
Link Far End	CO/CB/ECO	0	1 or 2	Any defined	Self	Natl					
By Agreement	RCT	0	3	1	By Agreement	Natl					2
By Agreement	TFC	0	3	2	By Agreement	Natl				By Agreement	2
Link Far End	TFP/TFR/TFA	0	4	Any defined	Self	Natl				By Agreement	2
Link Far End	RSM	0	5	Any defined	Self	Natl				By Agreement	2
Link Far	Mgt Inhibit	0	6	Any	Self	Natl					

End				defined							
Link Far End	Traffic Restart	0	7	Any defined	Self	Natl					
Link Far End	MTP User UA	0	10	1	By Agreement	Natl					3
Link Far End	Signaling Link Test Msgs	1 or 2	NA	NA	Self	Natl					
By Agreement	SCCP Msgs	3	NA	NA	By Agreement	Natl	Link Far End	By Agreement	By Agreement		3
Link Far End	ISUP	5	NA	NA	Self	Natl					3

Notes:

- 1) Link management messages have no address field and are limited to the local interface.
 - 2) Route set messages would only be expected in relation to directly routed TCAP messages. These message types would have little value for TCAP messages routed by global title translation (GTT).
 - 3) Assumes both ISUP and TCAP messages are allowed. Otherwise only agreed message types (ISUP or TCAP) allowed.
- "By Agreement" means that the OPC and DPC have both indicated their agreement to exchange this type of message.
 - All messages not defined by the table should be blocked.

1.14 Optional Blank Gateway Screening Policy Form

The following form may be used to formulate your response should you desire to use it

OPC	Msg Type	SI	H0	H1	DPC	Nat /Int	CgPA	CdPA	TT	Aff PC/SSN
	L2 Link Mgt	NA	NA	NA	Screening Not performed on Level 2 messages					
	CO/CB/ECO	0	1&2	All		N				
	TFC	0	3	2		N				
	RCT	0	3	1		N				
	TFP/TFR/TFA	0	4	All		N				
	RSM	0	5	All		N				
	Mgt Inhibit	0	0-6	All		N				
	Traffic Restart	0	7	All		N				
	Signaling Link Test	1&2	NA	NA		N				
	MTP User UA	0	10	1		N				
	SCCP Msgs	3	NA	NA		N				
	ISUP	5	NA	NA		N				

1.15 GLOSSARY

AC	Address Complete
ANM	Answer
APC	Affected Point Code
ASSN	Affected Subsystem Number
BLA	Blocking Acknowledgement
BLO	Blocking
C'dPA	Called Party Address
C'gPA	Calling Party Address
CBA	Changeback Acknowledgement
CBO	Changeback
CCR	Continuity Check Request
CGB	Circuit Group Blocking
CGBA	Circuit Group Blocking Acknowledgement
CGU	Circuit Group Unblocking
CGUA	Circuit Group Unblocking Acknowledgement
COA	Changeover Acknowledgement
COO	Changeover
COT	Continuity
CQM	Circuit Query
CQR	Circuit Query Response
CRA	Circuit Reservation Message Acknowledgement
CRM	Circuit Reservation Message
CVR	Circuit Validation Response
CVT	Circuit Validation Test
DF	Destination Field
DPC	Destination Point Code
ECA	Emergency Changeover Acknowledgement
ECO	Emergency Changeover
GRA	Circuit Group Reset Acknowledgement
GRS	Circuit Group Reset
H0	Heading Code Zero

H1	Heading Code One
IAM	Initial Address Message
ICIC	Unequipped Circuit Identification Code
LFU	Link Forced Uninhibit
LIA	Link Inhibit Acknowledgement
LID	Link Inhibit Denied
LIN	Link Inhibit
LLI	Link Local Inhibit
LPA	Loop Back Acknowledgement
LRI	Link Remote Inhibit
LUA	Link Uninhibit Acknowledgement
LUN	Link Uninhibit
MTP	Message Transfer Part
MRVT	MTP Routing Verification Test
OPC	Originating Point Code
PRI	Priority
RCT	Route Set Congestion Test
REL	Release
RES	Resume
RLC	Release Complete
RSC	Reset Circuit
RSM	Route Set Test Messages
RSP	Route Set Test Prohibited
RSR	Route Set Test Restricted
SCCP	Signaling Connection Control Part
SI , SIO	Signaling Information Octet
SLTA	Signaling Link Test Acknowledgement
SLTM	Signaling Link Test Message
SRVT	SCCP Routing Verification Test
SSA	Subsystem Allowed
SSP	Subsystem Prohibited
SST	Subsystem Test
SUS	Suspend

TCA	Transfer Cluster Allowed
TCP	Transfer Cluster Prohibit
TCR	Transfer Cluster Restricted
TFA	Transfer Allowed
TFC	Transfer Controlled
TFP	Transfer Prohibit
TFR	Transfer Restricted
UBA	Unblocking Acknowledgement
UBL	Unblocking
UDT	Unit Data
UDTS	Unit Data Service



ATIS-0300017

**Next Generation Interconnection Interoperability (NGIIF)
Reference Document**

**Part III, Installation, Testing and Maintenance
Responsibilities for SS7 Links and Trunks**

**Attachment F
SS7 ISUP Tests for ISDN Network Interconnection**

Version 12.0



ATIS is the leading technical planning and standards development organization committed to the rapid development of global, market-driven standards for the information, entertainment and communications industry. More than 200 companies actively formulate standards in ATIS' Committees, covering issues including: IPTV, Cloud Services, Energy Efficiency, IP-Based and Wireless Technologies, Quality of Service, Billing and Operational Support, Emergency Services, Architectural Platforms and Emerging Networks. In addition, numerous Incubators, Focus and Exploratory Groups address evolving industry priorities including Smart Grid, Machine-to-Machine, Connected Vehicle, IP Downloadable Security, Policy Management and Network Optimization.

ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications' Sectors, and a member of the Inter-American Telecommunication Commission (CITEL). ATIS is accredited by the American National Standards Institute (ANSI). For more information, please visit www.atis.org.

Notice

This document was developed by the Alliance for Telecommunications Industry Solutions' (ATIS) sponsored Next Generation Interconnection Interoperability Forum (NGIIF). The NGIIF addresses next-generation network interconnection and interoperability issues associated with emerging technologies. Specifically, it develops operational procedures which involve the network aspects of architecture, disaster preparedness, installation, maintenance, management, reliability, routing, security, and testing between network operators. In addition, the NGIIF addresses issues which impact the interconnection of existing and next generation networks and facilitate the transition to emerging technologies. All changes to this document shall be made through the NGIIF issue resolution process.

Note Regarding Previous Versions

The NIIF Reference Document was formerly known as the Network Operations Forum (NOF) Reference Document. The NOF Reference Document was published and maintained by Bellcore. The last version of the NOF Reference Document is Issue 13.

Disclaimer and Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

ATIS-0300017, NGIIF Reference Document, Part III, Installation and Maintenance Responsibilities for SS7 Links and Trunks, Attachment F, SS7 ISUP Tests for ISDN Network Interconnection, Formerly NIIF 5012

The NGIIF Reference Document, Part III, Installation and Maintenance Responsibilities for SS7 Links and Trunks, Attachment F, SS7 ISUP Tests for ISDN Network Interconnection, is an ATIS standard developed by the NGIIF.

Published by

Alliance for Telecommunications Industry Solutions

1200 G Street, NW, Suite 500

Washington, DC 20005

Copyright © 2011 by Alliance for Telecommunications Industry Solutions

All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < <http://www.atis.org> >.

Printed in the United States of America.

SS7 ISUP TESTS FOR ISDN NETWORK INTERCONNECTION

Table of Contents

1 GENERAL.....3

2 PURPOSE.....3

3 ISDN IMPACTS ON SS7 MESSAGES 3

3.1 CALL PROGRESS MESSAGE (CPG).....3

3.2 CONFUSION MESSAGE (CFN) 3

3.3 ADDRESS COMPLETE MESSAGE (ACM) 3

3.4 INITIAL ADDRESS MESSAGE (IAM) 4

3.5 ANSWER MESSAGE (ANM) 5

3.6 RELEASE MESSAGE (REL) 5

4 DESCRIPTION OF TESTS.....5

4.1 CALL-THROUGH TESTS 5

5 TEST SET GENERATED TESTS 8

5.1 BASIC CALLS 8

5.2 SENDING AND RECEIVING CONFUSION MESSAGE 9

5.3 IAM FOLLOWED BY ANM 9

5.4 REL WITH CAUSE, TEMPORARY FAILURE 9

5.5 TERMINATING REL WITH CAUSE, BEARER CAPABILITY NOT IMPLEMENTED, USER 10

5.6 TERMINATING REL WITH CAUSE, BEARER CAPABILITY NOT IMPLEMENTED, REMOTE LOCAL NETWORK 10

5.7 TERMINATING REL WITH CAUSE, NORMAL RELEASE (DATA).....10

5.8 ORIGINATING REL AFTER ACM (DATA) 10

5.9 ORIGINATING REL WITH CAUSE, NORMAL RELEASE (DATA).....10

5.10 TERMINATING REL WITH CAUSE, USER BUSY 11

5.11 TERMINATING REL WITH CAUSE, CALL REJECTED, LOCATION USER.....11

5.12 UPGRADE ROUTING (OPTIONAL TEST, NETWORK ARCHITECTURE DEPENDENT 11

5.13 TERMINATING REL WITH CAUSE, USER ALERTING, NO ANSWER 11

5.14 TERMINATING REL WITH CAUSE, NO USER RESPONDING 12

5.15 ACM WITH EXCESSIVE DELAY.....12

5.16 ACM WITH EXCESSIVE DELAY, ANM.....12

5.17 5.17 INTERCEPT RELS 12

5.18 INTERCEPT ACM, PROVIDE TONE OR ANNOUNCEMENT 13

5.19 REL ON ANNOUNCEMENT TIME-OUT 13

5.20 INTERCEPT ACM, ROUTE TO TONE OR ANNOUNCEMENT.....13

5.21 CPG AFTER ACM.....14

5.22 T-T EXPIRATION.....14

5.23 CPG WITH ALERTING 14

5.24 CPG WITH ALERTING, ANM 15

5.25 ASC ROUTE DOES NOT SUPPORT REQUESTED BEARER 15

5.26 GAP WITHOUT CPN 15

5.27 GAP WITH CPN.....15

6 CONFIGURATION A - CALL THROUGH TESTS 16

7 CONFIGURATION B (TEST SET GENERATED TESTS) 16

8 APPENDIX A FACILITY AND TRANSLATION REQUIREMENTS 17

8.1 CALL-THROUGH TEST FACILITY AND TRANSLATION REQUIREMENTS 17

8.2 INTRUSIVE TEST FACILITY AND TRANSLATION REQUIREMENTS.....17

9 APPENDIX B.....17

1 General

The NGIIF ISDN Ad Hoc Committee developed the tests included in this document. They are intended to be used as a recommended set of Interconnection Tests between Access Service Providers (ASP) and Access Service Customers (ASC) to assure that the SS7 interconnection between an ASP and an ASC can be used to support ISDN-Basic Rate services.

Tests to be performed will be based on bi-lateral agreements. Although not specified in the tests, verification of AMA records should be performed to assure proper billing.

The tests in this document are divided into two categories, Test Set Generated (TSG) and Call Through. TSG tests require the capability to direct ISUP messages toward the network interface under test and to send and detect tones on interconnected trunks. Call-through tests can be executed by manual calling in conjunction with monitoring of SS7 links.

The tests outlined in this document have been developed with concern for the ongoing integrity and reliability of existing services. Therefore, these tests have been deemed to have no negative impact on the network during the application of such tests.

2 Purpose

To ensure that the interconnected ASPs and ASCs can exchange the appropriate protocol messages for Basic Rate ISDN services in a way that provides the desired level of Quality Assurance and identifies adherence/deviations from industry standards.

Appendix A provides a list of facility and switch translation requirements for the included tests.

3 ISDN Impacts on SS7 Messages

This section is included for background and reference purposes. The following message types are impacted by ISDN:

- Call Progress Message
- Confusion Message
- Address Complete Message
- Initial Address Message
- Answer Message
- Release Message

The subsections below describe the ISDN impacts.

3.1 Call Progress Message (CPG)

This is a new SS7 message introduced by ISDN. It is sent by the terminating switch in the following two cases:

- To report ALERTing (after ISDN/T303 expiration) on the access
- To report clearing with inband tone.

3.2 Confusion Message (CFN)

This is the other new message introduced by ISDN and it is not expected in normal call processing, rather it is sent by a switch in response to any ISUP message (other than a confusion message), when the switch does not recognize the message or detects part of a message as being unrecognized.

3.3 Address Complete Message (ACM)

Differences due to ISDN are in the cause indicators and optional backward call indicators parameters. Codings will be verified in normal and abnormal call processing situations (see Sections 4.2 and 4.3).

Cause Indicators Parameter

- Cause value classes (octet 2, bits 7-5)
 - 011 service or option not available
 - 100 service or option not implemented
- Cause values (octet 2, bits 4-1)

000	0010	(2)	no route to specified transit network
001	0010	(18)	no user responding
001	0011	(19)	user alerting, no answer
001	0101	(21)	call rejected
010	1011	(43)	access information discarded
011	1010	(58)	bearer capability not presently available
011	1111	(63)	service/option not available - unspecified (default, this class)
100	0001	(65)	bearer capability not implemented
100	1111	(79)	service/option not implemented - unspecified (default, this class)
110	0001	(97)	message type non-existent or not implemented
110	0011	(99)	parameter non-existent or not implemented - discarded

Diagnostics may be included.

Optional Backward Call Indicators Parameter

This parameter is used to signal the availability of inband information in certain cases (e.g., for calls routed to intercept at the terminating office).

3.4 Initial Address Message (IAM)

The parameters impacted by ISDN are described below.

Forward Call Indicators Parameter

ISDN access indicator (I bit)

0	originating access non-ISDN
1	originating access ISDN

User Service Information Parameter

Codings for the five following bearer capabilities will be verified:

- Speech
- 3.1 kHz audio
- 7 kHz audio
- 64 kbps, unrestricted digital information
- 64 kbps, unrestricted digital information, rate adapted from 56 kbps

Calling Party Number (CPN) and Generic Address Parameter (GAP)

When the user-provided calling party number is either "not screened or "failed screening," both the CPN and GAP should be included in the IAM. The user-provided calling party number should be included in the GAP. A network-provided number should be included in the CPN.

New codings for the CPN for ISDN are as follows:

Screening Indicator

0	0	reserved for user provided, not screened
0	1	user provided, passed network screening
1	0	reserved for user provided, failed network screening
1	1	network provided

Accept "01" or "11" codings only for screening indicator. Code as "unique" user-provided numbers passing screening.

Codings for the GAP are as follows:

- Type of address
 - 0000 0010 user-provided, failed screening
 - 0000 0011 user-provided, not screened
- Presentation restriction indicator
 - 0 0 presentation allowed
 - 0 1 presentation restricted (default)
 - 1 0 number unavailable (per TR-NWT-000444) spare (per ANSI standard)
 - 1 1 spare

Access Transport Parameter

Whether or not this parameter is passed to the interconnecting network (ICN) is dependent on translations. Its value is not affected by call processing for testing in conjunction with basic rate access.

3.5 Answer Message (ANM)

Backward Call Indicators Parameter

Bits DC set to 01, "subscriber free"

3.6 Release Message (REL)

Cause Indicators Parameter

See ACM.

4 Description of Tests

Prior to the commencement of testing, it is presumed that the interconnected network elements have been tested for conformance to applicable standards and that MTP level 2 and 3 and basic ISUP protocol compatibility testing has been performed.

Distribution of signaling link selection codes should be checked for ISUP messages between networks.

Depictions of basic network configuration are included in this document. Other configurations may be applicable, based on individual network requirements.

4.1 Call-Through Tests

The tests listed in this section use configuration A. A recommended sub-set of call-through tests may be found in appendix B.

4.1.1 Normal Calls

Audible ringing will be detected for speech and 3.1-kHz calls and tones or data test patterns will be passed to verify the establishment of a circuit for all calls. Echo control will be verified for voice calls.

Calls should be made varying the following as required:

- Topology
 - Direct to ASC
 - Via access tandem (AT)

- Interoffice Signaling
 - SS7 all the way
 - SS7 ASP to ASC, MF ASC to ASP

- Originating Access Type
 - ISDN
 - Non-ISDN

- Terminating Access Type
 - ISDN
 - Non-ISDN

- Access Signaling Method
 - Use of Keypad Information Element
 - Use of Called Party Number, Transit Network Selection, and Operator Services

- Access Elements
 - Bearer Capability
 - Speech
 - 3.1 kHz audio
 - 64 kbps, unrestricted digital information, rate adapted from 56 kbps
 - 64 kbps, unrestricted digital information
 - 7 kHz audio

- Dialing (including ASC-selection method)
 - (101XXXX)+(1)+7D
 - (101XXXX)+1+10D
 - (101XXXX)+0+7D
 - (101XXXX)+0+10D
 - (101XXXX)+011+CC+NN(#)

Address length should be varied.

- (101XXXX)+01+CC+NN(#)
- Address length should be varied.
- 101XXXX+0(0)
- 101XXXX+00
- 101XXXX+#
- 700-NXX-XXXX
- 8YY-NXX-XXXX
 - Route on NXX
 - SCP query at ASP EO
 - SCP query at ASP AT
- 9YY-NXX-XXXX
- 950-WXXX
- Calling Party Number and Generic Address Parameter Values
 - Number delivery
 - Network provided only
 - User provided, passed screening
 - User provided, failed screening; network provided
 - User provided, not screened; network provided
 - Presentation restriction indicator
 - For calling party non-ISDN, calling party number nature of address indicator (national unique vs. national non-unique)
- Access Transport Information
 - Called party subaddress
 - Calling party subaddress
 - High layer compatibility
 - Low layer compatibility
- Translation Confirmation Tests
 - Sending/receiving calling party number and generic address parameters to/from ASC

- Sending/receiving access transport parameter to/from ASC (per ASC and per trunk group for receiving)
 - Pegging received access transport parameters (by trunk group)
 - Sending a confusion message (by trunk group, originating and terminating).
- Peg Counts
 - Access Transport Parameter per terminating ASC trunk group

5 Test Set Generated Tests

These tests primarily cover cases that may not arise during call-through testing. When call-through testing is minimal or not performed, test set generated tests should be added to substitute for the missing call through tests.

The tests listed in this section use test configuration B when using test equipment to initiate the sequence of messages and tones.

Throughout this section the term "ISDN IAM is used to indicate an IAM with a coding of "originating access ISDN" (I 1 in the Forward Call Indicators)

Tests which have the notation "(data)" should use an IAM with a 64kbps unrestricted data bearer capability coded in the User Service Information parameter.

5.1 Basic Calls

5.1.1 Test Description

These tests simulate basic calls and verify the ability to pass the appropriate voice or data signals on the selected trunks.

5.1.2 Test Procedure

These tests require the test initiator to send IAMs and tones or test patterns, as appropriate, for calls as indicated below:

- Speech
 - 3.1 kHz audio
 - 56 kbps data
 - 7 kHz audio
 - 64 kbps data

For data calls, the following two test patterns should be used:

- 30 seconds of all 0's
- 30 seconds of all 1's

For the 64 kbps bearer, place two simultaneous calls.

5.1.3 Expected Results

Results should be as indicated below:

USI	Expected Result	Expected Result
Bearer Capability	56kbps Trunk	64kbps Trunk
Speech	NCP	NCP
3.1 khz	NCP	NCP

56 kbps	NCP	NCP
7 khz	REL	NCP
64 kbps	REL	NCP

Note: NCP = Normal Call Processing

Normal call set-up, speech, audio or data passed correctly, with no errors, on selected trunk.

5.2 Sending and Receiving Confusion Message

5.2.1 Test Description

This test verifies that a normal call setup will occur when a confusion message is sent for the trunk being used for the test. This test has six cases, three initiated by the ASP and three by the ASC.

5.2.2 Test Procedure

The test initiator sends an ISDN IAM to the connected network for each case.

- After sending an IAM, send an IAM with an unrecognized message type to the othe network, before receiving the ACM.
- After sending an IAM, send a message with an unrecognized message type to the other network, after the ACM, but before the ANM.
- Send a message with an unrecognized message type to the othe network, after the ANM.

Repeat the above tests with the ASC originating the IAM and the ASP sending the CFN.

5.2.3 Expected Results

Normal call set-up (Receipt of the CFN should not interfere with call set-up by the interconnecting networks.) In all cases the CFN should be coded with a Cause Value of "message type non-existent or not implemented". For case (c), the established connection should remain stable.

5.3 IAM followed by ANM

5.3.1 Test Description

This test verifies the proper coding of ANM parameters when ANM is sent by terminating switch instead of an ACM. This occurs when there is a terminating CONNect in response to SETUP.

5.3.2 Test Procedures

The test initiator sends an ISDN IAM to the ASC switch. Upon receipt of an IAM, the simulated terminating network should return tone and return an ANM with the called party's status indicator bits set to "subscriber free". Other backward call indicators should be coded as they would have been had an ACM been returned.

5.3.3 Expected Results

Detect tone and receive correctly-coded ANM.

5.4 REL with cause, temporary failure

5.4.1 Test Description

This case applies when contention is not allowed. It simulates the case where the access replies to SETUP with an ALERT requesting an unacceptable channel.

5.4.2 Test Procedure

The test initiator sends an ISDN IAM to the ASC switch. Upon receipt of an IAM, the simulated terminating network should return a REL message with the cause indicator coded "temporary failure" and general location of "user.

5.4.3 Expected Results

Successful release; Correct cause value and location in REL received at originating network.

5.5 Terminating REL with cause, bearer capability not implemented, user

5.5.1 Test Description

This test verifies the proper coding of the release message sent to the originating network when the called line cannot support the requested bearer.

5.5.2 Test Procedure

The test initiator sends an ISDN IAM to the ASC switch. Upon receipt of an IAM, the simulated terminating network should return a REL message with the cause indicator coded "bearer capability not implemented" and general location of "user".

5.5.3 Expected Results

Successful release; Correct cause value and location in REL received at the originating network.

5.6 Terminating REL with cause, bearer capability not implemented, remote local network

5.6.1 Test Description

This test verifies the proper coding of the release message sent to the originating network when the terminating switch does not have the bearer capability implemented.

5.6.2 Test Procedure

The test initiator sends an ISDN IAM to the ASC switch. Upon receipt of an IAM, the simulated terminating network should return a REL message with the cause indicator coded "bearer capability not implemented" and general location of "remote local network".

5.6.3 Expected Results

Successful release; Correct cause value and location in REL received by the originating network.

5.7 Terminating REL with cause, normal release (data)

5.7.1 Test Description

This test verifies the proper called party release of a normal ISDN data call.

5.7.2 Test Procedure

The test initiator sends a data ISDN IAM to the ASC switch. Upon receipt of an IAM, the simulated terminating network should return normal ACM. After 1 second, the simulated terminating network should send a normal ANM. After 5 seconds the simulated terminating network should send a REL message with the cause indicator coded "normal release" and a general location of "user".

5.7.3 Expected Results

Successful call and release; Correct cause value and location in REL received by the originating network.

5.8 Originating REL after ACM (data)

5.8.1 Test Description

This test verifies the proper release when the calling party clears immediately after ALERT.

5.8.2 Test Procedure

The test initiator sends a data IAM to the ASC switch. Upon receipt of an IAM, the simulated terminating network should return a normal ACM. (Do not send ANM) Upon receipt of the ACM, the simulated originating network should send a REL message with the cause indicator coded "normal release" and a general location of "user".

5.8.3 Expected Results

Successful release; Correct cause value and location in REL received by the terminating network.

5.9 Originating REL with cause, normal release (data)

5.9.1 Test Description

This test verifies a normal calling party release after answer.

5.9.2 Test Procedure

The test initiator sends a data IAM to the ASC switch. Upon receipt of IAM, the simulated terminating network should return a normal ACM. After 5 seconds, the simulated terminating network should send a normal ANM. After 5 seconds the simulated originating network should send a REL message with the cause indicator coded "normal release" and a general location of "user".

5.9.3 Expected Results

Successful call and release; Correct Cause Value and Location in REL received by the terminating network.

5.10 Terminating REL with cause, user busy

5.10.1 Test Description

This test verifies the proper coding of the REL when the terminating ISDN line is busy.

5.10.2 Test Procedure

The test initiator sends an ISDN IAM to the ASC switch. Upon receipt of an IAM at simulated terminating network, return a REL message with the cause indicator coded "user busy" and general location of "user".

5.10.3 Expected Results

Successful release; Correct cause value and location in REL received by the originating network.

5.11 Terminating REL with cause, call rejected, location user

5.11.1 Test Description

This test verifies the proper release when there is DISConnect before ALERTing from the terminating ISDN station.

5.11.2 Test Procedure

The test initiator sends an ISDN IAM to the ASC switch. Upon receipt of IAM, the simulated terminating network should return a REL message with the cause indicator coded "call rejected" and general location of "user".

5.11.3 Expected Results

Successful release; Correct cause value and location in REL received by the originating network.

5.12 Upgrade routing (optional test, network architecture dependent)

5.12.1 Test Description

These tests verify the ability of the interconnected networks to complete ISDN calls using a higher grade facility (trunk), when the type of facility requested by the originating ISDN line is not available.

5.12.2 Test Procedure

The test initiator places normal calls, with first-choice routes blocked or busy, to verify upgrade routing as follows:

- Speech to 64 kbps CCC facilities
- 3.1 kHz audio to 64 kbps CCC facilities
- 56 kbps data to 64 kbps CCC facilities.

5.12.3 Expected Results

Successful call completions.

5.13 Terminating REL with cause, user alerting, no answer

5.13.1 Test Description

This test verifies the proper release when there is an expiration of ISDN timer T301.

5.13.2 Test Procedure

The test initiator sends a speech IAM to the ASC switch. Upon receipt of IAM, the simulated terminating network should return a normal ACM. Then, after 7:05 minutes, the simulated terminating network should return a REL message with the cause indicator coded "user alerting, no answer" and general location of "remote local network.

5.13.3 Expected Results

Successful release; Correct cause value and location in REL message received by the originating network.

5.14 Terminating REL with cause, no user responding

5.14.1 Test Description

This test verifies the proper REL when there is a second ISDN timer T303 expiration without clearing on a data call.

5.14.2 Test Procedure

The test initiator sends a data IAM to the ASC switch. Upon receipt of IAM, the simulated terminating network should return a REL message with the cause indicator coded "no user responding" and general location of "remote local network.

5.14.3 Expected Results

Successful release; Correct cause value and location in the REL message received by the originating network.

5.15 ACM with excessive delay

5.15.1 Test Description

This is a contention not allowed case. This test verifies the proper network interactions when there is a first ISDN timer T303 expiration and no clearing.

5.15.2 Test Procedure

The test initiator sends an ISDN IAM with the user service information parameter coded for 3.1 kHz audio to the ASC switch. Upon receipt of an IAM, the simulated terminating network should return tone and an ACM with called party's status indicator bits set to "excessive delay.

5.15.3 Expected Results

Successful receipt of ACM at simulated originating network with correctly coded ACM.

5.16 ACM with excessive delay, ANM

5.16.1 Test Description

This test verifies that a call will complete after an ACM is received indicating "excessive delay

5.16.2 Test Procedure

The test initiator (simulated terminating network) continues the preceding test by sending an ANM 200 msec. after the ACM. The ANM should be coded with called party's status indicator set to "subscriber free.

5.16.3 Expected Results

Successful call completion.

5.175.17 Intercept RELs

5.17.1 Test Description

These tests verify the proper REL of attempted 64kbps data calls when encountering various types of intercept. The test has three cases.

5.17.2 Test Procedure

The test initiator sends a 64 kbps data IAM to the ASC switch for each of the three cases. Upon receipt of IAM, the simulated terminating network should return a REL message as follows:

cause	general location

unallocated number	remote local network
number changed	remote local network
destination out of order	remote local network

5.17.3 Expected Results

For each of the three different RELs, successful release; Correct cause value and location in the REL messages received by the originating network.

5.18 Intercept ACM, provide tone or announcement

5.18.1 Test Description

These tests verify the correct coding of the ACM message when the attempt terminates to an intercept system. The test has two cases.

5.18.2 Test Procedure

The test initiator sends a voice IAM to the ASC. Upon receipt of IAM, the simulated terminating network should return tone and an ACM with backward call indicators, cause indicator, and optional backward call indicators. The backward call indicators should contain "terminating access non-ISDN." The cause indicators and locations for the two cases are given in the table. The optional backward call indicators should contain "inband information or appropriate pattern now available.

service	cause, general location
speech	unallocated number, remote local network
3.1 kHz audio	destination out of order, remote local network

5.18.3 Expected Results

For each of the two cases, successfully intercepted call; Correctly coded parameters in the ACM message received at the originating network.

5.19 REL on announcement time-out

5.19.1 Test Description

This test verifies the proper REL on an announcement timeout across the interconnection.

5.19.2 Test Procedure

The test initiator continues one of the above tests as follows: Thirty seconds after sending the ACM, send an REL with the cause indicator coded "normal release" and a location of "local local network.

5.19.3 Expected Results

Successful release; ASC network should map location "local local" to "remote local" before sending REL to ASP originating network.

5.20 Intercept ACM, route to tone or announcement

5.20.1 Test Procedure

The test initiator sends a voice IAM to the ASC. Upon receipt of IAM, the simulated terminating network should return tone and an ACM with backward call indicators and cause indicator coded as follows:

The backward call indicators should contain

- no indication of charge (BA 00)
- no indication of called party's status (DC 00)
- no indication of called party's category (FE 00)

- interworking encountered (I 1)
- ISDN User Part not used all the way (K 0)
- terminating access non-ISDN (M 0).

The cause indicators should contain "number changed" and "remote local network."

5.20.2 Expected Results

Successfully intercepted calls and properly coded ACMs received at originating network.

5.21 CPG after ACM

5.21.1 Test Description

These tests verify the proper coding of the ACM and CPG when there is a first ISDN timer T303 expiration and no clearing (on voice calls). The test has five cases.

5.21.2 Test Procedure

The test initiator sends an ISDN IAM with the User Service Information parameter set for speech to the ASC switch. Upon receipt of IAM, the simulated terminating network should return tone and an ACM with called party's status indicator bits set to "excessive delay. Following the ACM by 5 seconds, the simulated terminating network should return a CPG as follows:

cause	general location
user busy	user
no user responding	remote local network
call rejected	user
call rejected	remote local network
temporary failure	user

The CPG should have the Event Information parameter coded "inband information or appropriate pattern now available" and "no indication" of presentation restricted.

5.21.3 Expected Results

For each of the five different CPGs, successful transmission of the CPG by the ASC switch with the correct message coding received at the originating network.

5.22 T-t expiration

5.22.1 Test Description

This tests verifies the proper REL when ISDN timer T-t expires.

5.22.2 Test Procedure

For the fourth case in the preceding test, the test initiator should not clear the call at the originating end. This will allow timer T-t to expire at the terminating end. Upon expiration of T-t, the simulated terminating network should return a REL message with the cause indicator coded "normal clearing" and a general location of "remote local network."

5.22.3 Expected Results

Successful release; Correct cause value and location in REL message received by the originating network.

5.23 CPG with ALERTing

5.23.1 Test Description

This test verifies the ACM and CPG received at the originating network when there is a first ISDN timer T303 expiration and no clearing followed by ALERT.

Note: T-t starts when CPG is sent and stops when REL is received from the originating network.

5.23.2 Test Procedure

The test initiator sends ISDN IAM to the ASC switch. Upon receipt of IAM, the simulated terminating network should return tone and ACM with called party's status indicator bits set to "excessive delay. Following the ACM by 5 seconds, the simulated terminating network should return a CPG with the Event Information parameter coded as "ALERTing" with "no indication" of presentation restriction.

5.23.3 Expected Results

Successful transmission of CPG by the ASC and correct coding received by the originating network.

5.24 CPG with ALERTing, ANM

5.24.1 Test Description

This test verifies the successful completion of a call after a CPG has been sent.

5.24.2 Test Procedure

The test initiator (simulated terminating network) should continue the preceding test by sending an ANM with "subscriber free 200 msec. after the CPG.

5.24.3 Expected Results

Successful call.

5.25 ASC route does not support requested bearer

5.25.1 Test Description

This test verifies the proper release when the ASC does not support the requested bearer capability.

5.25.2 Test Procedure

The test initiator sends an IAM to the ASC requesting a bearer capability not supported by the ASC.

5.25.3 Expected Results

Successful release; REL message received by the originating network with the cause value "not available" or "not implemented

5.26 GAP without CPN

5.26.1 Test Description

This test validates the action of an ASC when the ASP sends an IAM with a GAP but no CPN.

5.26.2 Test Procedure

The test initiator sends an IAM to the ASC containing GAP but no CPN.

5.26.3 Expected Results

Completed call; With or without GAP (Whether or not GAP is passed is Network implementation dependent).

5.27 GAP with CPN

5.27.1 Test Description

This test verifies the proper transmission of GAP AND CPN parameters to a terminating ASP, through the ASC

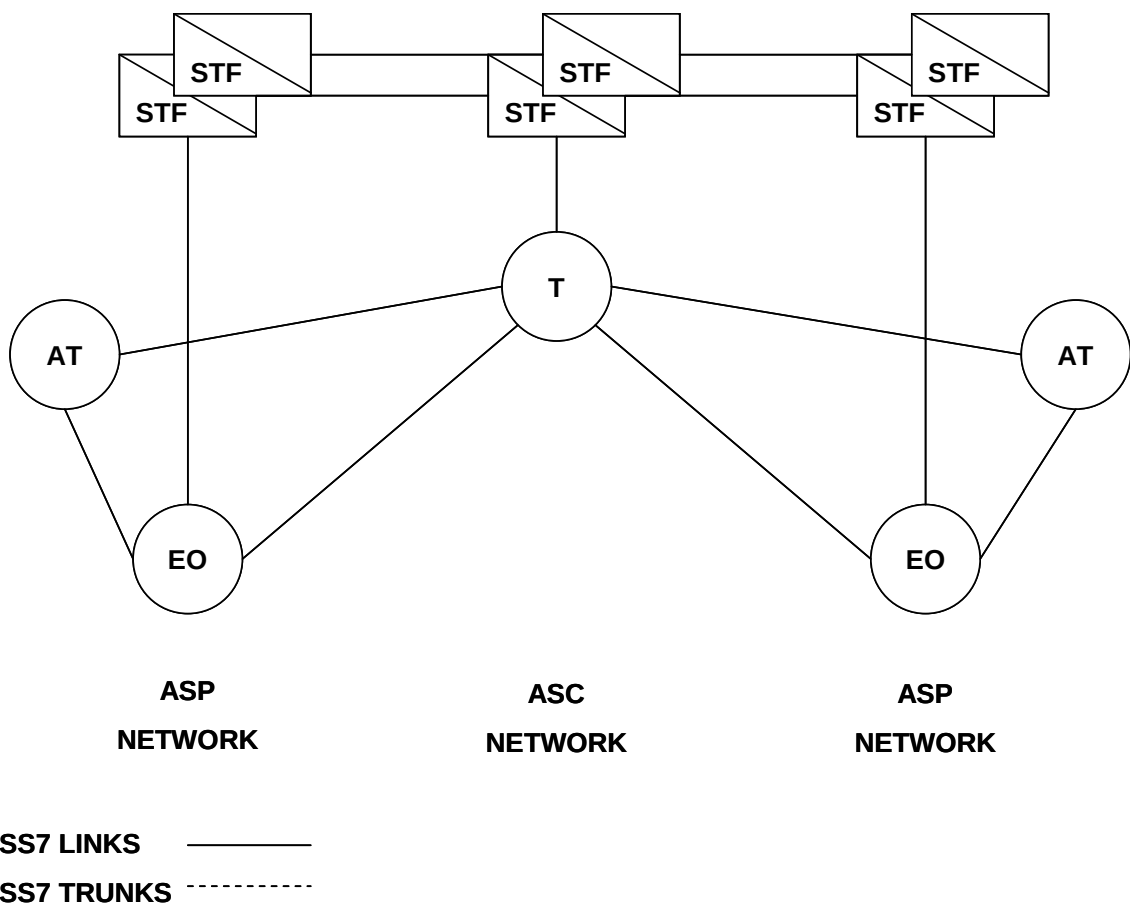
5.27.2 Test Procedure

The test initiator sends an ISDN IAM to the ASC with both CPN and GAP parameters present. The CPN should contain a presentation indicator coded as "presentation allowed" and a screening indicator coded as "network provided". The GAP should contain a presentation restriction indicator coded as "presentation allowed" and the type of address coded as "user provided, not screened

5.27.3 Expected Results

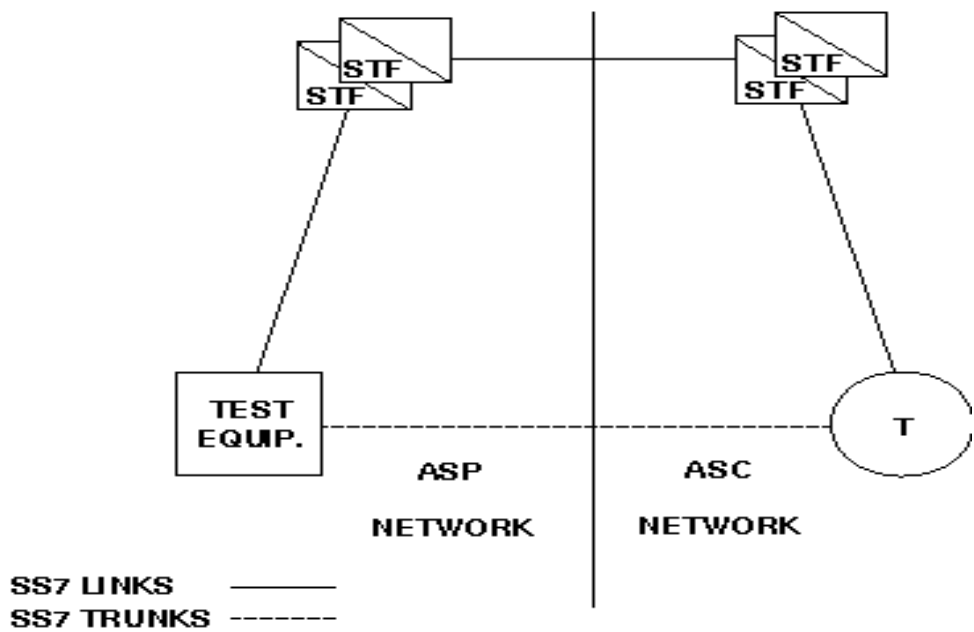
Completed call; GAP and CPN passed to terminating network

6 Configuration A - Call Through Tests



7 Configuration B (Test Set Generated Tests)

Configuration B (Test Set Generated Tests)



8 APPENDIX A FACILITY AND TRANSLATION REQUIREMENTS

8.1 Call-Through Test Facility and Translation Requirements

- ISDN lines and station equipment at originating switch should support ISDN capabilities
- ISDN lines and station equipment at terminating switch. One line should be provisioned to allow contention, another not.
- POTS line at the originating switch
- POTS line at the terminating switch
- MF trunks to the ASC network (either direct or from tandem)
- Direct SS7-controlled 56 and 64 kbs trunks between ASP and ASC networks
- Tandem SS7-controlled 56 and 64 kbs trunks between ASP and ASC networks
- Non-restricted, pre-subscribed line (can be line assigned above)
- On one DN of the pre-subscribed line, at least one bearer should be presubscribed to the ASC under test, at least one should be unpresubscribed, and at least one should be presubscribed to test carrier 034.
- Non-presubscribed line
- ISDN lines should support five bearer capabilities mentioned in test plan
- ASC-provided international number for test purposes
- A 700 number to be provided by the ASC
- An Toll Free number using NXX routing to be provided by the ASC
- An Toll Free number that is translated at an SCP accessed from an end office
- An Toll Free number that is translated at an SCP accessed from an access tandem
- A 900 number to be provided by the ASC

8.2 Intrusive Test Facility and Translation Requirements

- ASC switch
- Two 56 kbs trunks on ASC switch
- Two 64 kbs trunks on ASC switch
- Intrusive SS7 access to ASC switch.

9 APPENDIX B

Direct to IC or via tandem

Originating access type ISDN

All SS7 except where noted

NOTE: Calls should be made to validate proper treatment of attempts to:

- Unallocated Number
- Number Changed
- Destination Out of Order

Dialing	Bearer	CPN/GAP	GAP	ATP	Term
			Presentation		
101XXXX+(1)+7D	3.1 kHz audio				POTS
101XXXX+(1)+7D	3.1 kHz audio				MF, POTS
101XXXX+(1)+7D	56 kbps data			low	ISDN
101XXXX+(1)+7D	64 CCC			high	ISDN
101XXXX+1+10D	speech				ISDN
101XXXX+1+10D	3.1 kHz audio	User provided, passed screening			ISDN

101XXXX+1+10D	56 kbps data	User provided, failed screening	allowed	high, low	ISDN
101XXXX+1+10D	56 kbps data	User provided, failed screening	allowed	called, low	ISDN
101XXXX+1+10D	64 CCC	User provided, not screened	restricted	called	ISDN
101XXXX+1+10D	64 CCC	User provided, not screened	restricted	called, high	ISDN
101XXXX+1+10D	7 kHz audio				ISDN
1+10D	speech				ISDN
1+10D	speech				NOTE
1+10D	56 kbps data				NOTE
1+10D	3.1 kHz audio	User provided, passed screening			ISDN
1+10D	56 kbps data	User provided, failed screening	allowed	calling	ISDN
1+10D	56 kbps data	User provided, failed screening	allowed	called, high, low	ISDN
1+10D	56 kbps data	User provided, failed screening	allowed	calling, high	ISDN
1+10D	64 CCC	User provided, not screened	restricted	calling, low	ISDN
1+10D	64 CCC	User provided, not screened	restricted	calling, high, low	ISDN
1+10D	64 CCC	User provided, not screened	restricted	calling, called	ISDN
1+10D	64 CCC	User provided, not screened	restricted	calling, called, high, low	ISDN
1+10D	7 kHz audio				ISDN
101XXXX+011+CC+NN(#)	speech				ISDN
101XXXX+011+CC+NN(#)	3.1 kHz audio	User provided, passed screening			ISDN
101XXXX+011+CC+NN(#)	56 kbps data	User provided, failed screening	allowed	calling, called, low	ISDN
101XXXX+011+CC+NN(#)	64 CCC	User provided, not screened	restricted	calling, called, high	ISDN



ATIS-0300018

**Next Generation Interconnection Interoperability (NGIIF)
Reference Document**

**Part III, Installation, Testing and Maintenance
Responsibilities for SS7 Links and Trunks**

**Attachment G
Link Diversity Validation Guidelines**

Version 12.0



ATIS is the leading technical planning and standards development organization committed to the rapid development of global, market-driven standards for the information, entertainment and communications industry. More than 200 companies actively formulate standards in ATIS' Committees, covering issues including: IPTV, Cloud Services, Energy Efficiency, IP-Based and Wireless Technologies, Quality of Service, Billing and Operational Support, Emergency Services, Architectural Platforms and Emerging Networks. In addition, numerous Incubators, Focus and Exploratory Groups address evolving industry priorities including Smart Grid, Machine-to-Machine, Connected Vehicle, IP Downloadable Security, Policy Management and Network Optimization.

ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications' Sectors, and a member of the Inter-American Telecommunication Commission (CITEL). ATIS is accredited by the American National Standards Institute (ANSI). For more information, please visit www.atis.org.

Notice

This document was developed by the Alliance for Telecommunications Industry Solutions' (ATIS) sponsored Next Generation Interconnection Interoperability Forum (NGIIF). The NGIIF addresses next-generation network interconnection and interoperability issues associated with emerging technologies. Specifically, it develops operational procedures which involve the network aspects of architecture, disaster preparedness, installation, maintenance, management, reliability, routing, security, and testing between network operators. In addition, the NGIIF addresses issues which impact the interconnection of existing and next generation networks and facilitate the transition to emerging technologies. All changes to this document shall be made through the NGIIF issue resolution process.

Note Regarding Previous Versions

The NIIF Reference Document was formerly known as the Network Operations Forum (NOF) Reference Document. The NOF Reference Document was published and maintained by Bellcore. The last version of the NOF Reference Document is Issue 13.

Disclaimer and Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

ATIS-0300018, NGIIF Reference Document, Part III, Installation and Maintenance Responsibilities for SS7 Links and Trunks, Attachment G, Link Diversity Validation Guidelines, Formerly NIIF 5013

NGIIF Reference Document, Part III, Installation and Maintenance Responsibilities for SS7 Links and Trunks, Attachment G, Link Diversity Validation Guidelines, is an ATIS standard developed by the NGIIF.

Published by

Alliance for Telecommunications Industry Solutions

1200 G Street, NW, Suite 500

Washington, DC 20005

Copyright © 2011 by Alliance for Telecommunications Industry Solutions

All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < <http://www.atis.org> >.

Printed in the United States of America.

LINK DIVERSITY VALIDATION GUIDELINES SIGNALING SYSTEM 7

Table of Contents

1	GENERAL.....	4
1.1	PURPOSE OF DOCUMENT.....	4
1.2	DEFINITIONS	4
2	BASIC PREMISES.....	4
3	OPERATING PRINCIPLES	4
4	SERVICE PROVIDER RESPONSIBILITY.....	5
4.1	INSTALLATION.....	5
4.2	AUDITING PROCESS	5
5	RECORDS (DATABASE AND/OR PAPER).....	6
6	PHYSICAL VALIDATION.....	6
7	LINK DIVERSITY GUIDELINES AND AUDITING PROCESS.....	6
7.1	DISTRIBUTION FRAMES AND MOUNTING BLOCKS	6
7.2	OFFICE REPEATER BAYS, DSX BAYS, PATCH BAYS.....	7
7.3	DIGITAL CROSS-CONNECT SYSTEM (DCS).....	7
7.4	D4/D5 BAYS (AND ASSOCIATED CHANNEL BANK EQUIPMENT).....	7
7.5	FIBER OPTIC TERMINALS AND MULTIPLEXERS.....	7
7.6	POWER AND FUSING	8
7.7	CLOCK/TIMING SUPPLIES/SYNCHRONIZATION	8
7.8	ACCESS EQUIPMENT (TEST, BILLING, MONITORING).....	8
7.9	CABLE (INSIDE)	8
7.10	CABLE (ENTRANCE).....	9
7.11	INTEROFFICE ROUTE.....	9
7.12	CABLE (AERIAL/BURIED/UNDERGROUND).....	9
7.13	RADIO.....	9
8	LEASED AND SUB-LEASED FACILITIES.....	10

1 General

1.1 Purpose of Document

The purpose of this document is to provide guidance for the validation of diversity to providers of Signaling System 7 links to ensure the integrity of the Signaling System 7 network.

CAUTION:

Physical Validation should be considered as being able to cause link failures. Existing NGIIF Maintenance procedures (SS7 III) should be followed. When and if a company intends to perform physical validation of diversification by intrusive methods, the interconnected companies shall agree on the methodology, date, and time for the intrusive validation.

This document does not replace or supersede any existing contracts, tariffs or any other legally binding document.

1.2 Definitions

For the purpose of this document, the following definitions shall apply:

- Service Provider is any company providing telecommunications access services.
- Vendor/Manufacturers are any companies providing hardware/software to the telecommunications industry.
- Physical Validation shall be accomplished by an actual non-intrusive (i.e., not service affecting) check of the physical assignment compared to the documented assignment.
- Physical Diversification is the separation of all cables, cable runs, equipment bays, facilities and structures.
- Electrical Diversity is the separation of common power supplies, electronic equipment and fusing.
- Logical Diversification is defined as the condition where link facilities are physically diverse but not logically protected.
- Quad Links are CCS links that form the STP - to - STP interconnection.
- Link Pairs are combined link sets consisting of a link in each link set.

2 Basic Premises

Full SS7 Link diversity is essential to ensure the robustness of the entire telecommunications network. The lack of diversity on SS7 routes places the entire telecommunications network at risk.

Information included in this document is a result of Network Interconnection Interoperability Forum agreements and pertains to the validation of SS7 link diversification.

3 Operating Principles

Link diversification validation should be performed at a minimum of twice a year. At least one of those validations shall include a physical validation of equipment compared to the recorded documentation of diversity.

The validation of diversification is the responsibility of every network service provider that provides or utilizes SS7 links.

Diversification shall be in accordance with the Network Interconnection Interoperability Forum minimum recommended criteria for two-way and three-way diversity, as identified in the NGIIF Reference Document in Section III, SS7 Link and Trunk Document.

Limitations on diversification should be considered at the time of deployment; such limitations may consist of, geography, facilities, circuit design and tariffs.

4 Service Provider Responsibility

This section covers the responsibilities of the service provider in ensuring and maintaining link diversification.

4.1 Installation

When new links are being ordered it is the responsibility of the service provider to ensure that the assignment of links maintains all aspects of diversification for the purchasing customer.

Where it has been identified at the time of assignment that diversification cannot be maintained, the service provider shall ensure the maximum level of diversification possible at that point in time. The service provider shall inform the customer immediately and develop a path forward to reconcile the situation.

Documentation shall be generated to record the lack of diversification for future reference.

In the event that a database assigns and maintains diversification, the service provider shall have in place an alerting mechanism to inform them if an assignment violates diversification.

Where diversification cannot be implemented at the time of interconnection, the customer shall be informed and the service provider shall have a mechanism (automatic or manual) in place that will re-address the lack of diversification periodically.

The service provider shall provide diverse link assignments at the earliest time possible so that diversification can be achieved. Where a rearrangement is required, the company initiating the rearrangement shall follow existing NGIIF guidelines associated with the affected interconnecting companies.

Every effort must be made to avoid the use of a tandem or hub office link circuit design.

Leased facilities must be verified, as facilities of different carriers may have a common Point of Presence (POP).

Interconnected link records (including office assignment records) must include adequate detail for link diversity to be verified.

4.2 Auditing Process

Once a year, the service provider shall verify all supporting documentation of link assignments to ensure that diversification is maintained. In the event that diversification violations have been detected, which affect the provisioning of the circuit, the service provider shall:

- notify the customer of the violation and provide a commitment for reconciliation, and
- initiate corrective actions to eliminate the violation.

In order to validate that all supporting documentation is correct and consistent, the service provider shall compare all sources of documented link assignments to ensure diversification. Where a conflict between two or more sources is identified, such conflicts shall be reconciled.

It may be in the best interest of the service provider and the customer that when anomalies in records are identified, a physical check be performed to ascertain the correct assignment.

Six months after the documentation validation process has been completed, the service provider shall conduct an additional validation of diversification. At this point in time, a physical validation shall be performed.

A physical validation shall be performed by comparing the documented assignment with the physical assignment of one end of the link. The interconnected party shall be required to perform the same function at their end of the connection. (See caution note in Section 1)

5 Records (Database and/or Paper)

Link assignment records should include all aspects of diversification (Physical, Electrical, and Logical).

Where link assignment records are in a database, a back up of the database should be maintained.

Records must be verified for all aspects of diversity prior to physical verification. Where a compromise of diversification is identified in the supporting documentation, a physical check should be performed to ensure physical diversification is maintained and the associated documentation corrected.

Where rerouting has taken place for any reason, diversification should be verified and records should be updated within 24 hours internally as well as between interconnected companies.

6 Physical Validation

When a company intends to perform physical validation of diversification by intrusive methods, the interconnected companies shall agree on the methodology, date and time for the intrusive validation.

Physical validation can be performed by ensuring that the documentation for the links being audited is consistent with the physical assignment. The interconnected parties should confirm that the data is consistent.

Physical verification is a confirmation of records by an actual on-site physical check.

Physical validation includes the verification of identification of SS7 nodes and associated components as outlined in the NGIIF Reference Document, Section 11, SS7 Component Identification.

7 Link Diversity Guidelines and Auditing Process

This section covers network components that should be validated for diversification.

7.1 Distribution Frames and Mounting Blocks

7.1.1 Guideline

Termination of diverse CCS links should be on separate Main Distributing Frame (MDF) mounting blocks.

7.1.2 Process

- Verify that diverse CCS links are assigned to separate blocks on circuit records.
- Visually inspect MDF locations to ensure that CCS links are installed as indicated in the records.

7.2 Office Repeater Bays, DSX Bays, Patch Bays.

7.2.1 Guideline

Diverse CCS links should not traverse a single bay of these types. Each link should be routed through separate and distinct bays.

7.2.2 Process

- Verify in records that diverse CCS links are assigned to separate bays.
- Visually inspect bay locations to ensure that CCS links appear as indicated on the records.

7.3 Digital Cross-connect System (DCS)

7.3.1 Guideline

Diverse CCS links should not traverse a single DCS.

7.3.2 Process

- Verify that diverse CCS links are assigned to separate Digital Cross-connect Systems.
- Interrogate DCS databases to ensure that CCS links are assigned as indicated on records.

7.4 D4/D5 Bays (and associated channel bank equipment)

7.4.1 Guideline

The channel bank equipment associated with each diverse CCS link should be located in separate bays, separate line-ups if possible.

7.4.2 Process

- Verify in records that diverse CCS links are assigned to separate bays.
- Visually inspect bay locations to ensure that diverse CCS links appear as indicated on records

7.5 Fiber Optic Terminals and Multiplexers.

7.5.1 Guideline

Diverse CCS links should not transit the same fiber terminal or the same multiplex equipment.

7.5.2 Process

- Verify in records that CCS links are assigned to separate equipment.
- Visually inspect bay locations to ensure that CCS links appear as indicated on records.

7.6 Power and Fusing

7.6.1 Guideline

No components of diverse CCS transmission paths should share a common fuse within the same power distribution unit (PDU).

7.6.2 Process

- Verify in records that diverse CCS links are assigned to separate equipment bays. This will usually ensure service through separate fuses.
- Visually inspect bay locations to ensure that diverse CCS links appear on equipment that is served through separate fuses.

7.7 Clock/Timing Supplies/Synchronization

7.7.1 Guideline

Synchronization of diverse CCS Links should be in accordance with NGIIF established guidelines as outlined in Part III of the NGIIF Reference Document, Installation & Maintenance Responsibilities - SS7 Link and Trunk Installation and Maintenance Access Services, Section 3, Subsection E, Synchronization.

7.7.2 Process

- Visually inspect bay locations to ensure that diverse CCS links appear on equipment that is connected to a primary and secondary timing source.

7.8 Access Equipment (Test, Billing, Monitoring)

7.8.1 Guideline

Diverse CCS links from the same network element should not traverse a single access unit.

7.8.2 Process

- Verify in records that diverse CCS links are assigned to separate access units.
- Visually inspect diverse CCS Links to ensure that they are connected to separate access units.

7.9 Cable (inside)

7.9.1 Guideline

Diverse CCS Links should be placed in separate inside cables and on separate cable runs where possible.

7.9.2 Process

- Verify in records that diverse CCS links are assigned to separate inside cables.
- Visually inspect cable runs to ensure that diverse CCS Links are not on the same cable racks.

7.10 Cable (entrance)

7.10.1 Guideline

If available, diverse ingress facilities should be utilized for diverse CCS Links. If not available, the following hierarchy of protection is recommended:

- Diverse Conduit Runs, or
- Diverse Cables, or
- Diverse Binder groups.

7.10.2 Process

- Verify that diverse CCS links are assigned to separate facilities as listed above on circuit records.
- Visually inspect facility locations to ensure that diverse CCS links are installed as indicated on the records.

7.11 Interoffice Route

7.11.1 Guideline

Diverse CCS links from the same network element should not traverse the same physical interoffice route.

7.11.2 Process

- Verify that diverse CCS links are assigned to cables (metallic/fiber) that follow physically separated routes.
- Visually inspect MDF locations and cross connection points to ensure that diverse CCS links are installed within the cable (metallic/fiber) indicated on route records.

7.12 Cable (aerial/buried/underground)

7.12.1 Guideline

No single cable should carry diverse CCS links. Cables should be placed in spatially separated conduit systems and in spatially separated right-of-way.

7.12.2 Process

- Verify that diverse CCS links are assigned to cables (metallic/fiber) that follow physically separated routes.
- Visually inspect MDF locations and cross connection points to ensure that diverse CCS links are installed within the cable (metallic) as indicated on records.

7.13 Radio

7.13.1 Guidelines

All diverse CCS links from the same network element should not traverse the same radio route.

7.13.2 Process

Verify that diverse CCS links are assigned to radio systems that follow physically separated routes.

8 Leased and Sub-leased Facilities

Leased and sub-leased Facilities should be validated for CCS link diversity in accordance with the established criteria as outlined in section 7.



ATIS-0300019

**Next Generation Interconnection Interoperability (NGIIF)
Reference Document**

**Part III, Installation, Testing and Maintenance
Responsibilities for SS7 Links and Trunks**

**Attachment H
SS7 Cause Code and Tones & Announcements**

Version 12.0



ATIS is the leading technical planning and standards development organization committed to the rapid development of global, market-driven standards for the information, entertainment and communications industry. More than 250 companies actively formulate standards in ATIS' 20 Committees, covering issues including: IPTV, Service Oriented Networks, Home Networking, Energy Efficiency, IP-Based and Wireless Technologies, Quality of Service, Billing and Operational Support. In addition, numerous Incubators, Focus and Exploratory Groups address emerging industry priorities including "Green", IP Downloadable Security, Next Generation Carrier Interconnect, IPv6 and Convergence.

Notice

This document was developed by the Alliance for Telecommunications Industry Solutions' (ATIS) sponsored Next Generation Interconnection Interoperability Forum (NGIIF). The NGIIF addresses next-generation network interconnection and interoperability issues associated with emerging technologies. Specifically, it develops operational procedures which involve the network aspects of architecture, disaster preparedness, installation, maintenance, management, reliability, routing, security, and testing between network operators. In addition, the NGIIF addresses issues which impact the interconnection of existing and next generation networks and facilitate the transition to emerging technologies. All changes to this document shall be made through the NGIIF issue resolution process.

Note Regarding Previous Versions

The NIIF Reference Document was formerly known as the Network Operations Forum (NOF) Reference Document. The NOF Reference Document was published and maintained by Bellcore. The last version of the NOF Reference Document is Issue 13.

Disclaimer and Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

ATIS-0300019, NGIIF Reference Document, Part III, Installation and Maintenance Responsibilities for SS7 Links and Trunks, Attachment H, SS7 Cause Code and Tones & Announcements, Formerly NIIF 5014

The NGIIF Reference Document, Part III, Installation and Maintenance Responsibilities for SS7 Links and Trunks, Attachment H, SS7 Cause Code and Tones & Announcements, is an ATIS standard developed by the NGIIF.

Published by

Alliance for Telecommunications Industry Solutions

1200 G Street, NW, Suite 500

Washington, DC 20005

Copyright © 2011 by Alliance for Telecommunications Industry Solutions

All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < <http://www.atis.org> >.

Printed in the United States of America.

SS7 CAUSE CODES & TONES AND ANNOUNCEMENT

Table of Contents

1	INTRODUCTION	4
1.1	PURPOSE OF DOCUMENT.....	4
1.2	DEFINITIONS	4
2	BASIC PREMISES.....	4
3	OPERATING PRINCIPLES	4
4	SCOPE OF THIS DOCUMENT	5
5	GENERAL NOTES	5
5.1	CAUSE CODE STANDARDS	5
5.2	MAPPING MATRIX	5
5.3	CAUSE CODE CLASSES AND CAUSE CODE DEFAULT	5
6	CAUSE CODE TREATMENTS	6
6.1	NO CIRCUIT ANNOUNCEMENT (NCA).....	6
6.2	REORDER ANNOUNCEMENT (ROA).....	6
6.3	INTERCEPT (INT).....	6
6.4	VACANT CODE ANNOUNCEMENT (VCA)	6
6.5	INEFFECTIVE OTHER	7
6.6	BUSY TONE (BT)	7
6.7	REORDER TONE (RO)	7
7	MAPPING MATRIX.....	7
8	TECHNICAL REFERENCES	8
9	SS7 CAUSE CODE MATRIX	1

1 Introduction

1.1 Purpose of Document

The purpose of this document is to provide a single source for definitions of application of Cause Codes with the associated treatment, and the appropriate verbiage to be played to the customer where an announcement is required.

This document does not replace or supersede any existing Contracts, tariffs or any other legally binding document.

1.2 Definitions

In this document is a matrix that provides Cause Code Definition, Treatments and the appropriate mapping of cause codes across the network. Within this matrix there are the following abbreviations and or terms, RWC, TP, and STATUS, the definitions for these terms are as follows:

Release With Cause (RWC): This term is utilized to indicate that the terminating switch will release the call with a cause code (RWC) and that the treatment for this cause code will be applied at the originating end of the call.

Terminating Play (TP): This term is utilized to indicate that the terminating switch will apply the appropriate treatment to the originating party(s) line.

Status: This term indicates that the terminating switch or CPE is providing a status message as to the condition or state of the call in progress.

2 Basic Premises

Telecommunication Service providers need to have a universal understanding for SS7 treatment, definition of cause codes and the associated announcements to be applied.

Universal application of cause codes and their associated definitions and appropriate announcements will enhance the standard of service provided to our Customers.

3 Operating Principles

Application of Cause Codes and their associated Tones and Announcements shall be consistent with industry agreements (e.g., ANSI T1 Standards and the NGIIF).

Information in this document that is contrary to any other industry documentation shall require a liaison to the publishers of those documents to gain clarification and changes if necessary.

As Information is generated for inclusion in this document, the Communications' technician is taken into account. The definition of Cause Codes may differ slightly from Industry Standards (e.g. T1.113.2) definitions, however the intent is to provide clarity.

It is the responsibility of the individual companies as part of the SS7 user community to provide updates for inclusion to this document.

4 Scope of This Document

The scope of this document is to include SS7 Cause Code Treatment, Definitions for Usage and Announcement verbiage to be applied where applicable and the appropriate mapping of cause codes as they traverse the network.

5 General Notes

At the time of publication, differences between this document and the ANSI T1 Standards, have been channeled to the appropriate committees and or Forums to develop standard definitions and treatments. Where there are any differences, the reader needs to utilize any documentation to enhance their clarification.

To ensure accessibility by hearing-impaired persons, announcements incorporate TTY messages using a methodology such as the one provided in Annex B of T1M1.3/2002 085. The specifications for TTY tones and coding are in ANSI/TIA/EIA 825.

5.1 Cause Code Standards

There are three standards by which Cause Codes are utilized within the telecommunications industry with one being held in reserve, they are as follows:

00 = CCITT

01 = OTHER INTERNATIONAL

10 = ANSI

11 = RESERVED

The Coding Standards are used in the subfields of the cause indicator parameter field:

Cause Indicators Parameter Field

8	7	6	5	4	3	2	1				
Ext	Coding Standard		Spare	Location							
Ext	Recommendation										
Ext	Cause Value										

In some instances an alpha character "N" is utilized in the Cause Code matrix to indicate the Cause Code as a National standard.

5.2 Mapping Matrix

The cause code mapping matrix in this document identifies the action, and direction of the Cause Codes as they traverse the network. This matrix is provided for example only. The specific Cause Code mapping may be different in your network (e.g., switch type, local translations, CPE and interconnection agreements).

5.3 Cause Code Classes and Cause Code Default

Any Cause Code not being recognized will be routed to a default code in the appropriate Cause Code Class. Cause Codes should only be mapped to the applicable default code for that class.

CAUSE CODE CLASS	CAUSE CODE GROUPING DESCRIPTION	CAUSE CODE GROUPS	CAUSE CODE DEFAULT
001	Normal Event	1-30	31
010	Resource Unavailable	32-46	47
011	Service Option not Available	48-62	63
100	Service Option not Implemented	64-78	79
101	Invalid Massage	80-94	95
110	Protocol Error	96-110	111
111	Interworking	112-126	127

6 Cause Code Treatments

This section provides the definition of the different announcements that can be applied to the appropriate Cause Codes.

6.1 No Circuit Announcement (NCA)

This announcement is played when there are no circuits available for the call to be completed. An example of such a recording is as follows:

“All circuits are busy now. Please try your call again later”.

6.2 Reorder Announcement (ROA)

This announcement is played when a call did not traverse the network to completion for a myriad of reasons. An example of such a recording is as follows:

“We’re sorry, your call did not go through. Please try your call again later”.

6.3 Intercept (INT)

This announcement is played when a customer dials a number that has been disconnected or no longer in service. An example of such a recording is as follows.

“We’re sorry, you have reached a number that has been disconnected or is no longer in service. If you feel you have reached this recording in error, please check the number and try your call again.”

6.4 Vacant Code Announcement (VCA)

This announcement is played when a customer mis-dialed or the NPA/NXX is not valid. An example of such a recording is as follows.

“We’re sorry, your call cannot be completed as dialed. Please check the number and dial again.”

6.5 *Ineffective Other*

There should be announcements with the appropriate verbiage for the following situations, and will be determined by the service provider.

- Prefix or Access code dialing irregularity
- Improper Initial Coin deposit
- Screened line access denial
- Dialing Irregularity

At a minimum the announcements should include the following information.

- The call cannot be completed as dialed
- Instructions for correct dialing procedures
- The customer should try the call again (except for Customer Calling Feature Calling)

In addition to announcements, there are instances when the application of a tone is the applicable treatment for a call. The following are tones that are normally applied as treatments:

6.6 *Busy Tone (BT)*

Busy Tone is applied to an originating customer's line when the called party is engaged in another call or the phone is at an off hook condition. The tone applied to the originating customer's line will be at a rate of 60 impulses per minutes (60 IPM).

6.7 *Reorder Tone (RO)*

Reorder tone is applied to the originating customer's line when the call cannot be completed, which may be due to insufficient facilities. In such instances a tone will be applied at a rate of 120 impulses per minute (120 IPM). This tone may be applied in lieu of an announcement.

7 MAPPING MATRIX

Indicated below are examples of Cause Codes received by each network or Customer Premises Equipment (CPE) and the Cause Codes sent by each network or CPE. The Action that generated the Cause Code is listed to indicate the network or CPE where the event occurred. (YY and XX represent different Cause Codes).

- ➔ Indicates direction of Cause Code
- ← Indicates direction of Cause Code

Arrow facing towards Cause Code indicates Cause Code being generated.

Arrow facing away from Cause Code indicates Cause Code being passed.

XX	(message)	Cause Code Generated by or Received at Network of CPE
XX←	(action/message)	Network or CPE generated Cause Code XX
→XX	(action/message)	Network or CPE generated Cause Code XX
→XX←	(action/message)	Network or CPE generated Cause Code XX in both directions
←XX	(action/message)	Cause Code XX being passed to next network or CPE ←
XX→	(action/message)	Cause Code XX being passed to next network or CPE←
←XX→	(action/message)	Cause Code XX being passed in both directions
←YY←XX	(message)	Network or CPE receives Cause Code XX from (message) XX→YY→ previous network or CPE and maps Cause Code XX to Cause Code YY

← At the end office, treat the call per Cause Code XX for analog or Non-ISDN call.

8 TECHNICAL REFERENCES

GR-317-CORE - Switching System Generic Requirements for Call Control Using the Integrated Services Digital Network User Part (ISDNUP), Issue 1 (Bellcore, February 1994)

GR-394-CORE - Switching System Generic Requirements for Call Interexchange Carrier Interconnection Using the Integrated Services Digital Network User Part (ISDNUP), Issue 1 (Bellcore, February 1994)

TR-NWT-000444 - Switching System Requirements Supporting ISDN access Using the ISDN User Part, Issue 3 (Bellcore, May 1993)

TR-TSY-000268 - ISDN Access Call Control Switching and Signaling Generic Requirements, Issue 3 (Bellcore, July 1994)

TR-NWT- 001268 - ISDN Primary Rate Interface Call Control Switching and Signaling Generic Requirements for Class II Equipment

GR-246-CORE - Bellcore Specification of Signaling System Number 7 (SS7), Issue 1 (Bellcore, December 1994)

SR-3137 - Generic Requirements for Uniform Cause Values on National ISDN Basic Rate Interfaces, Issue 1 (Bellcore, June 1994)

SR-3138 - Summary View of the use of Uniform Cause Code Values on National ISDU 3 Primary Rate Interfaces, Issue 1 (Bellcore, September 1994)

T1M1.3/2002 085 - Operations, Administration, Maintenance and Provisioning (OAM&P) –

Network Tones and Announcements

ANSI/TIA/EIA 825 - A Frequency Shift Keyed Modem For Use On The Public Switched Telephone Network

9 SS7 Cause Code Matrix

Cause Code	Event	References/Definition	Preferred Treatment Release With Cause	D// DI	Calling Party	ORIG EO/AT	INTNET	TERM EO/AT	Called Party
1	Unallocated Number	Refer to GR-317/394, TR-444, TR-268, TR-1268, GR-246 and SR-3137 This cause indicates that the called party cannot be reached because, although this number is in a valid format, it is not currently assigned (allocated). NGIIF Note: Valid codes in the North American Numbering Plan (NANP) can be found in the LERG.	INT (\$)	DI	1 1	←1 ←1←2 2	←1 ←22	1← RWC \$ 22← RWC	
2	No Route to Specified Transit Network	Refer to TR-444, TR-268, TR-1268, GR-246 and SR-3137 This cause indicates that the equipment sending this cause has received a request to route the call through a particular transit network that it does not recognize. The equipment sending this cause does not recognize the transit network either because the transit network does not exist, or because that particular transit while it does exist, does not serve the equipment that is sending this cause. This cause is supported on a network-dependent basis. (Routes on Carrier Identification Code (CIC))	VCA	DI	2	2 ← RWC			
3	No Route to Destination	Refer to GR-317/394, TR-444, TR-268, TR-1268, GR-246 and SR-3137 This cause indicates that the called party cannot be reached because the network through which the call has been routed does not serve the destination desired. This cause is supported on a network-dependent basis.	VCA	DI	3	← 3	3← RWC		

\$ - Due to existing technical limitations within the United States terminating play may continue to be used.

* - Clearing Message w/o cause code.

** - Clearing Message with cause code other than 17, 27, 34, 65 or 88.

*** - It may be more appropriate to map these ISDN access cause codes to 21 rather than 18 or 41.

xN (e.g., 23N) - Indicates National ANSI standard only, not ITU-T standard. This coding standard should be used only when the desired cause value cannot be represented with the ITU-T standardized code.

IO - Implementation Option.

D/ I/ DI - Identifies where the cause code event is determined (D = DSS1 Access [CG/ CD Party to Switch])/ (I = Network, ISUP [Switch to Switch])/ (DI = Either D or I)

← → - Indicates direction of ISUP Message.

Cause Code	Event	References/Definition	Preferred Treatment Release With Cause	D// DI	Calling Party	ORIG EO/AT	INTNET	TERM EO/AT	Called Party
4	Undetermined Longterm Event	Refer to ANSI T1.113.2 and GR-246 This cause indicates that the called party cannot be reached for reasons that are of long term nature and that the special information tone should be returned to the calling party. (Currently not used)	See Special Note - (Default)	I	31	31←4	←4	4 ← RWC	
4N	Vacant area code or central office code	Refer to ANSI T1.607 This cause indicates the destination requested by the calling user cannot be reached because the area code or office code is not assigned.	See Special Note - (Default)	I	31 31 31	31←4 31←4 31← RWC	←4 4← RWC	4← RWC	
5	Mis-dialed trunk prefix - See Note 1	Refer to GR-246 No procedures specified for World Zone 1.	Note 2						
6	Channel Unacceptable	Refer to ANSI T1.607, TR-268, TR-1268, and SR-3137 This cause indicates the channel most recently identified by the called user equipment is not acceptable to the SPCS for use in this call. (ISDN Parameter) Specified exclusively for ISDN.	Note 2	D	17	←17	←17	RWC→6 17← RWC	6
7	Call awarded and being delivered in an established channel	Refer to ANSI T1.607, TR-268, TR-1268, and SR-3137 This cause indicates the user has been awarded the incoming call, and that the call is being connected to a channel already established to that user for similar calls (e.g., packet-mode X.25 virtual calls). (ISDN Parameter) Specified exclusively for ISDN.	Note 2	D				RWC→7	7
8	Preemption	Refer to ANSI T1.113.2-7 and GR-246 This cause indicates that the call is being preempted.	Note 2	DI	8 8 8	← 8 ← 8 8 ← RWC	← 8 8 ← RWC	8← RWC	

No Reference - Indicates that there is no reference to these cause codes in ANSI, ITU-T, TR-268, GR-246, GR-317/394, TR-444, TR-1268, SR-3137 and SR-3138

Special Note - Any Cause Code received that is not specified in the protocol specification of the switch is interpreted as unrecognized and will be treated by routing to the default code of that specific class.

Note 1 - Not being used by the Switched Public Network at this time.

Note 2 - If the release is received before the ACM, reorder (120IPM) will be applied. If the REL is received after the ACM, normal clearing will take place.

Cause Code	Event	References/Definition	Preferred Treatment Release With Cause	D// DI	Calling Party	ORIG EO/AT	INTNET	TERM EO/AT	Called Party
8N	Prefix 0 dialed but not allowed	Refer to ANSI T1.607 This cause indicates that the called user cannot be reached because the prefix 0 was used where not allowed.	Note 2	DI	8	8 ← RWC			
9	Preemption - circuit reserved for reuse	Refer to ANSI T1.113.2-7, GR-246, ANSI T1-619a-1994 (MLPP) This cause indicates that the call is being preempted and the circuit is reserved for reuse by the preempting exchange.	Note 2	I	9 9 9	← 9 ← 9 9 ← RWC	← 9 9 ← RWC	9 ← RWC	
9N	Prefix 1 dialed but not allowed	Refer to ANSI T1.607 This cause indicates that the called party cannot be reached because the prefix 1 was used where not allowed.	Note 2	D	9	9 ← RWC			
10N	Prefix 1 not dialed but required	Refer to ANSI T1.607 This cause indicates that the called party cannot be reached because the prefix 1 was not used where required.	Note 2	D	10	10 ← RWC			

\$ - Due to existing technical limitations within the United States terminating play may continue to be used.

* - Clearing Message w/o cause code.

** - Clearing Message with cause code other than 17, 27, 34, 65 or 88.

*** - It may be more appropriate to map these ISDN access cause codes to 21 rather than 18 or 41.

xN (e.g., 23N) - Indicates National ANSI standard only, not ITU-T standard. This coding standard should be used only when the desired cause value cannot be represented with the ITU-T standardized code.

IO - Implementation Option.

D/ I/ DI - Identifies where the cause code event is determined (D = DSS1 Access [CG/ CD Party to Switch])/ (I = Network, ISUP [Switch to Switch])/ (DI = Either D or I)

← → - Indicates direction of ISUP Message.

Cause Code	Event	References/Definition	Preferred Treatment Release With Cause	D//DI	Calling Party	ORIG EO/AT	INTNET	TERM EO/AT	Called Party
11N	More digits received than allowed, call is proceeding	Refer to ANSI T1.607 This cause indicates that the called party number address information is too long, and that the network has truncated it.	See Special Note (Default) No treatment with status message	D	11	11 ←STAT	11N		
12	No Reference								
13	No Reference								
14	No Reference								
15	No Reference								
16	Normal Call Clearing	Refer to GR-317/394, TR-444, TR-268, TR-1268, GR-246 and SR-3137 This cause indicates that the call is being cleared because one of the users involved in the call has requested that the call be cleared. Under normal situations, the source of this cause is not the Network.	Note 2	DI	16 disc 16 →16 16	← 16 ← 31 RWC → 31 RWC → 16 ← 16 16 → ← 16	← 31 31 → 16 → ← 16 16 → ← 16	31 RWC 31 → 16 → 16 → 16 ← RWC 16 → ← 16	16 16 disc 16 16 ←

No Reference - Indicates that there is no reference to these cause codes in ANSI, ITU-T, TR-268, GR-246, GR-317/394, TR-444, TR-1268, SR-3137 and SR-3138

Special Note - Any Cause Code received that is not specified in the protocol specification of the switch is interpreted as unrecognized and will be treated by routing to the default code of that specific class.

Note 1 - Not being used by the Switched Public Network at this time.

Note 2 - If the release is received before the ACM, reorder (120IPM) will be applied. If the REL is received after the ACM, normal clearing will take place.

Cause Code	Event	References/Definition	Preferred Treatment Release With Cause	D// DI	Calling Party	ORIG EO/AT	INTNET	TERM EO/AT	Called Party
17	User Busy	Refer to ANSI T1.113.2, ITU-T Recommendation Q.850, GR-317/394, TR-444, TR-268, TR-1268, GR-246 and SR-3137 This cause is used to indicate that the called party is unable to accept another call because the user busy condition has been encountered. This cause value may be generated by the called user or by the network. In the case of user determined user busy, it is noted that the user equipment is compatible with the call.	Busy Tone (60 IPM)	DI	17 17 17	←17 ←17 ←17	←17 ←17 ←17	← 17 ← 17← 34 17← RWC	17 ← 34 ← busy
18	No user Responding	Refer to ANSI T1.113.2, TR-444, TR-268, TR-1268, GR-246 and SR-3137 This cause is used when a user does not respond to a call establishment message with either an alerting or connect indication within the presubscribed period of time allocated	ROA	DI	18 18	←18 ←18	←18 ←18	18← RWC ← 18← 88	88 ←

\$ - Due to existing technical limitations within the United States terminating play may continue to be used.

* - Clearing Message w/o cause code.

** - Clearing Message with cause code other than 17, 27, 34, 65 or 88.

*** - It may be more appropriate to map these ISDN access cause codes to 21 rather than 18 or 41.

xN (e.g., 23N) - Indicates National ANSI standard only, not ITU-T standard. This coding standard should be used only when the desired cause value cannot be represented with the ITU-T standardized code.

IO - Implementation Option.

D/ I/ DI - Identifies where the cause code event is determined (D = DSS1 Access [CG/ CD Party to Switch])/ (I = Network, ISUP [Switch to Switch])/ (DI = Either D or I)

← → - Indicates direction of ISUP Message.

Cause Code	Event	References/Definition	Preferred Treatment Release With Cause	D// DI	Calling Party	ORIG EO/AT	INTNET	TERM EO/AT	Called Party	CC
19	No Answer from User (User Alerted)	Refer to ANSI T1-113.2, ITU-T Recommendation Q.850, TR-444, TR-268, TR-1268, GR-246 and SR-3137 This value is used when the called party has been alerted but does not respond with a correct indication within a presubscribed period of time. Note - This cause is not necessarily generated by Q.931 procedures but may be generated by internal network timers.	Audible Ringing	DI	19	←19	←19	19 ← RWC		19
20	Subscriber absent - See Note 1	Refer to ANSI T1.113.2 and ITU-T Recommendation Q.850 Mobile applications.	Note 2							20
21	Call Rejected	Refer to T1.607 (5.2.5.3), GR-317/394, TR-444, TR-268, TR-1268, GR-246 & SR-3137 This cause indicates that the equipment sending this cause code does not wish to accept this call, although it could have accepted the call because the equipment sending this cause is neither busy nor incompatible. (ISDN Related) This cause may also be generated by the network, indicating that the call was cleared due to a supplementary service constraint. The diagnostic field may contain additional information about the supplementary service and reason for the rejection	(T) ROA	DI	21 21 21 21	←21 ← 21←31 ←21 ←21	←21 ←31 ←21 ←21	← 21 31← RWC 21← RWC 21← RWC	21 ← none* other**	21
22	Number changed	Refer to ANSI T1.113, GR-317/394, TR-444, TR-268, GR-246 and SR-3137 This cause is returned to the calling party when the called number indicated by the calling party is no longer assigned. The new called number may optionally be included in the diagnostic field. If the network does not support this capability, cause code 1 shall be used.	INT (\$)	DI	22	←22	←22	22← RWC (\$)		22 IO

No Reference - Indicates that there is no reference to these cause codes in ANSI, ITU-T, TR-268, GR-246, GR-317/394, TR-444, TR-1268, SR-3137 and SR-3138

Special Note - Any Cause Code received that is not specified in the protocol specification of the switch is interpreted as unrecognized and will be treated by routing to the default code of that specific class.

Note 1 - Not being used by the Switched Public Network at this time.

Note 2 - If the release is received before the ACM, reorder (120IPM) will be applied. If the REL is received after the ACM, normal clearing will take place.

Cause Code	Event	References/Definition	Preferred Treatment Release With Cause	D/I/ DI	Calling Party	ORIG EO/AT	INTNET	TERM EO/AT	Called Party	CC
23N	Unallocated destination number	Refer to ANSI T1.113.2-9, ANSI T1.611 and GR-246 Indicates failure of a business group call because the destination number is unallocated in the business group numbering plan. This ANSI specific cause code is used to support Multi-location Business Group (MBG) service.	Note 2	DI	23	←23	←23	23← RWC		23N
24N	Undefined business group	Refer to ANSI T1.113.2-9 and GR-246 Indicates failure of a business group call because the business group identification is unknown. This ANSI specific cause code is used to support Multi-location Business Group (MGB) service.	Note 2	DI	24	←24	←24	24← RWC		24N

\$ - Due to existing technical limitations within the United States terminating play may continue to be used.

* - Clearing Message w/o cause code.

** - Clearing Message with cause code other than 17, 27, 34, 65 or 88.

*** - It may be more appropriate to map these ISDN access cause codes to 21 rather than 18 or 41.

xN (e.g., 23N) - Indicates National ANSI standard only, not ITU-T standard. This coding standard should be used only when the desired cause value cannot be represented with the ITU-T standardized code.

IO - Implementation Option.

D/ I/ DI - Identifies where the cause code event is determined (D = DSS1 Access [CG/ CD Party to Switch])/ (I = Network, ISUP [Switch to Switch])/ (DI = Either D or I)

← → - Indicates direction of ISUP Message.

Cause Code	Event	References/Definition	Preferred Treatment Release With Cause	D// DI	Calling Party	ORIG EO/AT	INTNET	TERM EO/AT	Called Party
25N	Exchange routing error	Refer to ANSI T1.113.2-9, GR-317/394 and GR-246 Indicates that the called party cannot be reached because of an error in exchange number translation tables used to route the call (results when the hop counter parameter value decrements to 0). This event can occur at intermediate exchanges only.	Note 2	I	25	←25	←25	25← RWC	
26N	Misrouted call to a ported number	Referred ANSI T1.113 & ANSI T1.160. This cause indicates that the called party can not be reached because the “ported number” in the GAP identifies a called party that in not served by the exchange.	ROA	I	26	←26	←26	26← RWC	
26	Non-selected user clearing	Refer to ANSI T1.607 (5.3.2), TR-268 and SR-3137 This cause indicates that the user has not been awarded the incoming call. In response to a SETUP message, the user or network can reject a call (e.g., because of the unavailability of a suitable B-channel). In the case of multipoint terminal configuration, non-selected user clearing will be initiated with RELEASE message(s) from the network containing this cause.	Note 2	DI				RWC→26	26
27	Destination out of order	Refer to ANSI T1.113.2, ITU-T Recommendation Q.850, GR-317/394, TR-444, TR-268, TR-1268, GR-246 and SR-3137 This cause indicates that the destination indicated by the user cannot be reached because the interface to the destination is not functioning correctly. The term “not functioning correctly” indicates that a signaling message was unable to be delivered to the remote party; e.g., a physical layer or data link layer failure of the remote party, or user equipment off-line. NGIIF Note: This cause is used to indicate that the destination cannot be reached because the interface to the destination has been placed in a trouble-busy condition (out-of-service state)	Note 2 (\$)	DI	27	←27	←27	27← RWC (\$)	
28	Address Incomplete	Refer to T1.607 (5.1.5.2), GR-317/394, TR-444, TR-268, TR-1268, GR-246 and SR-3137, ANSI T1.113.2 This cause indicates that the called party cannot be reached because the number* is not a valid format or is not complete. (* -Called Party Number)	VCA	DI	28	← 28	← 28	28 RWC ←	

No Reference - Indicates that there is no reference to these cause codes in ANSI, ITU-T, TR-268, GR-246, GR-317/394, TR-444, TR-1268, SR-3137 and SR-3138

Special Note - Any Cause Code received that is not specified in the protocol specification of the switch is interpreted as unrecognized and will be treated by routing to the default code of that specific class.

Note 1 - Not being used by the Switched Public Network at this time.

Note 2 - If the release is received before the ACM, reorder (120IPM) will be applied. If the REL is received after the ACM, normal clearing will take place.

Cause Code	Event	References/Definition	Preferred Treatment Release With Cause	D/I/ DI	Calling Party	ORIG EO/AT	INTNET	TERM EO/AT	Called Party
29	Facility rejected	Refer to ANSI T1.113, GR-246 and SR-3137 This cause is returned when a facility requested by the user can not be provided by the network.	Note 2	DI	29	← 29	← 29	29 RWC ←	
30	Response to STATUS ENquiry	Refer to TR-268, TR-1268, and SR-3137 This cause code is included in the STATUS message the user sends to the SPCS when the reason for generating this message was the prior receipt of a STATUS ENquiry message. (ISDN Related)	See Special Note (Default) No treatment with status Message	D	30	STAT → 30	← 30 →	30 STAT ←	30
31	Normal Unspecified -	Refer to GR-317/394, TR-444, GR-246 and SR-3137 This cause is used to report a normal event only when no other cause in the normal class (Cause Codes 1-30) applies.	Note 2	DI	none* 31 16	RWC → 31 ← 31 ← 16 ← 31	31 → ← 31 ← 31	31 → 31 RWC ← 31 RWC ←	31 none*

\$ - Due to existing technical limitations within the United States terminating play may continue to be used.

* - Clearing Message w/o cause code.

** - Clearing Message with cause code other than 17, 27, 34, 65 or 88.

*** - It may be more appropriate to map these ISDN access cause codes to 21 rather than 18 or 41.

xN (e.g., 23N) - Indicates National ANSI standard only, not ITU-T standard. This coding standard should be used only when the desired cause value cannot be represented with the ITU-T standardized code.

IO - Implementation Option.

D/ I/ DI - Identifies where the cause code event is determined (D = DSS1 Access [CG/ CD Party to Switch])/ (I = Network, ISUP [Switch to Switch])/ (DI = Either D or I)

← → - Indicates direction of ISUP Message.

Cause Code	Event	References/Definition	Preferred Treatment Release With Cause	D// DI	Calling Party	ORIG EO/AT	INTNET	TERM EO/AT	Called Party
31IO			Note 2	DI	31 21	← 31 RWC → 31 ← 21 ← 31	← 31 31 → ← 31	31 ← RWC 31 → 16 → 31 ← RWC	16
32	No Reference								
33	No Reference								
34	No Circuit Available	Refer to ANSI T1.113, GR-317/394, TR-444, TR-268, TR-1268, GR-246 and SR-3137 This cause indicates that there is no appropriate circuit presently available to handle the call.	NCA	DI	17 34 34	←17 ←34 ← 34← 58	←17 ←34 ←58	← 17← 34 ←34← RWC ←58← RWC	34 ←
35	No Reference								
36	No Reference								
37	No Reference								

No Reference - Indicates that there is no reference to these cause codes in ANSI, ITU-T, TR-268, GR-246, GR-317/394, TR-444, TR-1268, SR-3137 and SR-3138

Special Note - Any Cause Code received that is not specified in the protocol specification of the switch is interpreted as unrecognized and will be treated by routing to the default code of that specific class.

Note 1 - Not being used by the Switched Public Network at this time.

Note 2 - If the release is received before the ACM, reorder (120IPM) will be applied. If the REL is received after the ACM, normal clearing will take place.

Cause Code	Event	References/Definition	Preferred Treatment Release With Cause	D/I/ DI	Calling Party	ORIG EO/AT	INTNET	TERM EO/AT	Called Party
38	Network out of order	Refer to ANSI T1.607 (5.1.1), TR-444 and GR-246, ANSI T1.113.2 This cause indicates that the network is not functioning correctly and that the condition is likely to last a relatively long period of time. Immediately re-attempting the call is not likely to be successful.	ROA	DI	38	←38	←38	38← RWC	
39	Permanent virtual connection out-of-service	Refer to ANSI T1.617 This cause is sent by the user or the network (STATUS message) in response to a STATUS ENQUIRY message or at any time to indicate the status of permanent virtual connections; i.e., active or inactive. This cause may be sent in both directions and has local significance only. Specified exclusively for ISDN.	See Special Note (Default) No treatment with status message	D	39	39 ← STAT		STAT → 39	39
40	Permanent virtual connection operational	Refer to ANSI T1.617 This cause is sent by the user or the network (STATUS message) in response to a STATUS ENQUIRY message or at any time to indicate the status of permanent virtual connections; i.e., active or inactive. This cause may be sent in both directions and has local significance only. Specified exclusively for ISDN.	See Special Note (Default) No treatment with status message	D	40	40← STAT		STAT → 40	40

\$ - Due to existing technical limitations within the United States terminating play may continue to be used.

* - Clearing Message w/o cause code.

** - Clearing Message with cause code other than 17, 27, 34, 65 or 88.

*** - It may be more appropriate to map these ISDN access cause codes to 21 rather than 18 or 41.

xN (e.g., 23N) - Indicates National ANSI standard only, not ITU-T standard. This coding standard should be used only when the desired cause value cannot be represented with the ITU-T standardized code.

IO - Implementation Option.

D/ I/ DI - Identifies where the cause code event is determined (D = DSS1 Access [CG/ CD Party to Switch])/ (I = Network, ISUP [Switch to Switch])/ (DI = Either D or I)

← → - Indicates direction of ISUP Message.

Cause Code	Event	References/Definition	Preferred Treatment Release With Cause	D// DI	Calling Party	ORIG EO/AT	INTNET	TERM EO/AT	Called Party
41	Temporary failure	Refer to GR-317/394, TR-444, TR-268, TR-1268, GR-246 and SR-3137, T1.113.2 This cause indicates that the network is not functioning correctly and that the condition is not likely to last a long period of time. The user may wish to try another call attempt almost immediately.	ROA	DI	41 41 41 41 41 41 41 41 41	41←47 41←63 41←79 41←97 41←99 41←101 ←41 ←41	←47 ←63 ←79 ←97 ←99 101←111 ←41 ←41	47←RWC 63←RWC 79←RWC 97←RWC 99←RWC 111←RWC 41↔101 41←RWC	101
42	Switching equipment congestion	Refer to ANSI T1.113, GR-317/394, TR-444, TR-268, TR-1268, GR-246 and SR-3137 This cause indicates the switching equipment generating the cause is experiencing a period of high traffic.	ROA	DI	42	←42	←42	42←RWC	
43	User [Access] information discarded	Refer to ANSI T1.607 (5.8.7.2), TR-444, TR-268, TR-1268, GR-246, SR-3137, T1.113.2 This cause indicates the network could not deliver user information to the remote user as requested (i.e., user-to-user information, low-layer compatibility, high-layer compatibility, or subaddress, as indicated in the diagnostic). Specified exclusively for ISDN.	See Special Note - (Default) No treatment with status message	D	43	43←STAT		STAT→43	43
44	Requested circuit/channel not available	Refer to TR-444, TR-268, TR-1268, GR-246 and SR-3137, T1.113.2 This cause is returned, e.g., for origination from an ISDN loop interface, if no circuit or channel can be allocated to the call that the requesting user equipment has indicated "exclusive", the switch should reject the call request by sending a release complete message (RLC) to the calling user equipment with this cause.	(A/T 120ipm) =	DI	44	←44	←44	→44←	44

No Reference - Indicates that there is no reference to these cause codes in ANSI, ITU-T, TR-268, GR-246, GR-317/394, TR-444, TR-1268, SR-3137 and SR-3138

Special Note - Any Cause Code received that is not specified in the protocol specification of the switch is interpreted as unrecognized and will be treated by routing to the default code of that specific class.

Note 1 - Not being used by the Switched Public Network at this time.

Note 2 - If the release is received before the ACM, reorder (120IPM) will be applied. If the REL is received after the ACM, normal clearing will take place.

Cause Code	Event	References/Definition	Preferred Treatment Release With Cause	D/I/ DI	Calling Party	ORIG EO/AT	INTNET	TERM EO/AT	Called Party
45		Replaced by ITU-T Cause Code 9 in ANSI T1-619a-1994 (MLPP)							
46	Precedence call blocked	Refer to GR-246 This cause indicates that there are no preemptable circuits or that the called user is busy with a call of equal or higher preemptable level. Used with MLPP service.	See Special Note - (Default)	DI	46	←46	←46	46← RWC	
47	Resource unavailable, unspecified	Refer to GR-317/394, TR-444, GR-246 and SR-3137 This is a default cause used to report a resource unavailable event only when no other cause code in the resource unavailable class (Class 010) applies.	Reorder Tone (A/T = 120 IPM)	DI	41 47	←41 ←47	41←47 ←47	←47 RWC ←47 RWC	
48	No Reference								
49	Quality of Service unavailable.	Refer to ANSI T1.607 This cause is used to report that the requested quality of service, as defined in ITU-T X.213, cannot be provided (e.g., throughput or transit delay cannot be supported) Specified exclusively for ISDN.	See Special Note - (Default)	D	49	←49	←49	49← RWC	
50	Requested facility not subscribed	Refer to ANSI T1.607, ANSI T1.113, GR-246 and SR-3137 This cause indicates that the user has requested a supplementary service that is supported by the network element(s) but the user is not authorized to use.	(A/T = 120ipm) See Special Note - (Default)	DI	50	←50	←50	50 ←RWC	

\$ - Due to existing technical limitations within the United States terminating play may continue to be used.

* - Clearing Message w/o cause code.

** - Clearing Message with cause code other than 17, 27, 34, 65 or 88.

*** - It may be more appropriate to map these ISDN access cause codes to 21 rather than 18 or 41.

xN (e.g., 23N) - Indicates National ANSI standard only, not ITU-T standard. This coding standard should be used only when the desired cause value cannot be represented with the ITU-T standardized code.

IO - Implementation Option.

D/ I/ DI - Identifies where the cause code event is determined (D = DSS1 Access [CG/ CD Party to Switch])/ (I = Network, ISUP [Switch to Switch])/ (DI = Either D or I)

← → - Indicates direction of ISUP Message.

Cause Code	Event	References/Definition	Preferred Treatment Release With Cause	D// DI	Calling Party	ORIG EO/AT	INTNET	TERM EO/AT	Called Party
51N	Call type incompatible with service request	Refer to ANSI T1.113.2 This cause indicates that an action was rejected because it was not compatible with the bearer capability of the call.	See Special Note - (Default)	DI	51	←51	←51	51←RWC	
52	No Reference								
53	Left Blank Intentionally								
53N	Service operation violated	Refer to ANSI T1.625, ANSI T1.632, ANSI T1.639 This cause is used to report a service operation violation.	See Special Note - (Default)						
54N	Call blocked due to Group restrictions	Refer to ANSI T1.113. This cause indicates failure of a business group call because it did not pass line privileges and/or subgroup screening. This, ANSI specific, cause code is used to support Multi-location Business Group (MBG) service.	See Special Note - (Default)	DI	54	54←R WC		RWC→54	54
55	Incoming calls barred within CUG - See Note 1	Refer to ANSI T1.113, not used for World Zone 1. Refer to GR-246	See Special Note - (Default)						
56	No Reference								
57	Bearer capability not authorized	Refer to ANSI T1.113, ANSI T1.607 (5.1.5.2), TR-444, TR-268, TR-1268, GR-246 and SR-3137 This cause indicates that the user has requested a bearer capability which is implemented by the equipment which generated this cause but the user is not authorized to use	(A/T 120ipm) =	D	57	←57	←57	→57←	57

No Reference - Indicates that there is no reference to these cause codes in ANSI, ITU-T, TR-268, GR-246, GR-317/394, TR-444, TR-1268, SR-3137 and SR-3138

Special Note - Any Cause Code received that is not specified in the protocol specification of the switch is interpreted as unrecognized and will be treated by routing to the default code of that specific class.

Note 1 - Not being used by the Switched Public Network at this time.

Note 2 - If the release is received before the ACM, reorder (120IPM) will be applied. If the REL is received after the ACM, normal clearing will take place.

Cause Code	Event	References/Definition	Preferred Treatment Release With Cause	D// DI	Calling Party	ORIG EO/AT	INTNET	TERM EO/AT	Called Party
58	Bearer capability not presently available	Refer to ANSI T1.113, ANSI T1.607 (5.1.5.2), TR-444, GR-246 and SR-3137 This cause indicates that the user has requested a bearer capability that is implemented by the equipment which generated this cause but which is not available at this time.	(A/T 120ipm) =	DI	34	34←58	←58	58←RWC	
58IO				DI	58	←58	←58	58←RWC	
59	No Reference								
60	No Reference								
61	No Reference								
62	- See Note 1	Refer to ANSI T1.113.2 and ITU-T This cause indicates that there is an inconsistency in the designated outgoing access information and subscriber class	See Special Note - (Default)						
63	Service option or not available, unspecified	Refer to ANSI T1.113, which is a default for this class. Refer to TR-444, GR-246 and SR-3137 This cause is used to report a service or option not available event only when no other cause in the service or option not available class (class 011) applies.	(A/T 120ipm) =	DI	41	41←63 C	←63	63←RWC	
63IO				DI	63	←63	←63	63←RWC	
64	No Reference								

\$ - Due to existing technical limitations within the United States terminating play may continue to be used.

* - Clearing Message w/o cause code.

** - Clearing Message with cause code other than 17, 27, 34, 65 or 88.

*** - It may be more appropriate to map these ISDN access cause codes to 21 rather than 18 or 41.

xN (e.g., 23N) - Indicates National ANSI standard only, not ITU-T standard. This coding standard should be used only when the desired cause value cannot be represented with the ITU-T standardized code.

IO - Implementation Option.

D/ I/ DI - Identifies where the cause code event is determined (D = DSS1 Access [CG/ CD Party to Switch])/ (I = Network, ISUP [Switch to Switch])/ (DI = Either D or I)

← → - Indicates direction of ISUP Message.

Cause Code	Event	References/Definition	Preferred Treatment Release With Cause	D// DI	Calling Party	ORIG EO/AT	INTNET	TERM EO/AT	Called Party
65	Bearer Capability not implemented	Refer to ANSI T1.113, TR-444, TR-268, TR-1268, GR-246 and SR-3137 This cause indicates that the equipment sending this cause does not support the bearer capability requested.	(A/T 120ipm) =	DI	65	←65	←65	65←RWC	
66	Channel type not implemented	Refer to: ANSI T1.607 This cause indicates that the equipment sending this cause does not support the channel type requested. Specified exclusively for ISDN.	(A/T 120ipm) =	D	66	66←RWC			
67	No Reference								
68	No Reference								
69	Requested facility not implemented	Refer to ANSI T1.113, ANSI T1.607, GR-246 and SR-3137 This cause indicates that the equipment sending this cause does not support the requested supplementary service. [Specified for POTS & ISDN].	(A/T 120ipm) =	DI	69	←69	←69	69←RWC	
70	Only restricted digital information bearer capability is available	Refer to ANSI T1.113, ANSI T1.607 and GR-246 This cause indicates that the calling party has requested an unrestricted bearer service but that the equipment sending this cause only supports the restricted version of the requested bearer capability.	(A/T 120ipm) =	DI	70	←70	←70	70←RWC	
71	No Reference								
72	No Reference								
73	No Reference								
74	No Reference								
75	No Reference								
76	No Reference								

No Reference - Indicates that there is no reference to these cause codes in ANSI, ITU-T, TR-268, GR-246, GR-317/394, TR-444, TR-1268, SR-3137 and SR-3138

Special Note - Any Cause Code received that is not specified in the protocol specification of the switch is interpreted as unrecognized and will be treated by routing to the default code of that specific class.

Note 1 - Not being used by the Switched Public Network at this time.

Note 2 - If the release is received before the ACM, reorder (120IPM) will be applied. If the REL is received after the ACM, normal clearing will take place.

Cause Code	Event	References/Definition	Preferred Treatment Release With Cause	D//DI	Calling Party	ORIG EO/AT	INTNET	TERM EO/AT	Called Party
77	No Reference								
78	No Reference								
79	Service or option not implemented, unspecified	Refer to TR-444, GR-246 and SR-3137 This is the default for this class and is used to report a service or option not implemented event, only when no other cause in the service or option not implemented class (class 100) applies.	(A/T 120ipm) =	DI	41 79	41←79 ←79	←79 ←79	79←RWC 79←RWC	
80	No Reference								
81	Invalid call reference value	Refer to TR-268, TR-1268, and GR-246 Has local significance only, not sent over the network. This cause code indicates that the "called" address is currently not in use on the user interface. Specified exclusively for ISDN.	(A/T 120ipm) =	D	81	81←RWC		RWC→81	81
82	Identified channel does not exist.	Refer to ANSI T1.607 This cause indicates that the equipment sending this cause has received a request to use a channel not activated on the interface for a call. Specified exclusively for ISDN.	(A/T 120ipm) =	D	82	82←RWC		RWC→82	82
83	No Reference		See Special Note - (Default)						

\$ - Due to existing technical limitations within the United States terminating play may continue to be used.

* - Clearing Message w/o cause code.

** - Clearing Message with cause code other than 17, 27, 34, 65 or 88.

*** - It may be more appropriate to map these ISDN access cause codes to 21 rather than 18 or 41.

xN (e.g., 23N) - Indicates National ANSI standard only, not ITU-T standard. This coding standard should be used only when the desired cause value cannot be represented with the ITU-T standardized code.

IO - Implementation Option.

D/ I/ DI - Identifies where the cause code event is determined (D = DSS1 Access [CG/ CD Party to Switch])/ (I = Network, ISUP [Switch to Switch])/ (DI = Either D or I)

← → - Indicates direction of ISUP Message.

Cause Code	Event	References/Definition	Preferred Treatment Release With Cause	D// DI	Calling Party	ORIG EO/AT	INTNET	TERM EO/AT	Called Party
84	Call identity in use - See Note 1	Specified exclusively for ISDN.	See Special Note - (Default)						
85	No call suspended - See Note 1	Specified exclusively for ISDN.	See Special Note - (Default)						
86	Call having the requested call identity has been cleared - See Note 1	Specified exclusively for ISDN.	See Special Note - (Default)						
87	Called user not member of CUG - See Note 1	Refer to ITU-T Q.850 and GR-246	See Special Note - (Default)						
88	Incompatible destination	Refer to ANSI T1.607 (5.2.2), GR-317/394, TR-268, TR-1268, GR-246 and SR-3137, T1.113.2 This cause indicates that the terminating user equipment sending this cause has received a request to establish a call having compatibility attributes (bearer capability, Directory Number, subaddress, or low-layer compatibility) that cannot be accommodated. Specified exclusively for ISDN.	(A/T 120ipm) =	DI	88 18	←88 18←88	←88 ←88	88←RWC 88←RWC	
89	No Reference								
90	Non-existent CUG - See Note 1		See Special Note - (Default)						
91	Invalid transit network selection	Refer to ANSI T1.113, GR-317/394 and GR-246 This cause indicates that a transit network identification was received which is of an incorrect format (Annex C of T1.607).	(A/T 120ipm) =	DI	91	←91	←91	91←RWC	

No Reference - Indicates that there is no reference to these cause codes in ANSI, ITU-T, TR-268, GR-246, GR-317/394, TR-444, TR-1268, SR-3137 and SR-3138

Special Note - Any Cause Code received that is not specified in the protocol specification of the switch is interpreted as unrecognized and will be treated by routing to the default code of that specific class.

Note 1 - Not being used by the Switched Public Network at this time.

Note 2 - If the release is received before the ACM, reorder (120IPM) will be applied. If the REL is received after the ACM, normal clearing will take place.

Cause Code	Event	References/Definition	Preferred Treatment Release With Cause	D// DI	Calling Party	ORIG EO/AT	INTNET	TERM EO/AT	Called Party
92	No Reference								
93	No Reference								
94	No Reference								
95	Invalid message, unspecified	Refer to ANSI T1.113, GR-317/394, and GR-246 This is a default cause used to report an invalid message event only when no other cause code in the invalid message class (class 101) applies.	(A/T 120ipm) =	DI	95	➔95◀	◀95➔	➔95◀	95
96	Mandatory information element is missing	Refer to ANSI T1.607, TR-268, TR-1268 and SR-3137 This cause indicates that the equipment sending this cause has received a message that is missing an information element that must be present in that message before that message can be processed. Specified exclusively for ISDN.	(A/T 120ipm) =	D	96	◀96	◀96	➔96◀	96
97	Message type non-existent/not implemented-discarded.	Refer to ANSI T1.607 (5.8.4), GR-317/394, TR-444, TR-268, TR-1268, GR-246 and SR-3137, ANSI T1.113.2, ANSI T1.113.4 This cause indicates that the equipment sending this cause has received a message with a message type it does not recognize either because this is a message not defined or defined but not implemented by the equipment sending this cause.	(A/T 120ipm) =	DI	41 97	41◀97 ◀97	◀97 ◀97	➔97◀ ➔97◀	97 97

\$ - Due to existing technical limitations within the United States terminating play may continue to be used.

* - Clearing Message w/o cause code.

** - Clearing Message with cause code other than 17, 27, 34, 65 or 88.

*** - It may be more appropriate to map these ISDN access cause codes to 21 rather than 18 or 41.

xN (e.g., 23N) - Indicates National ANSI standard only, not ITU-T standard. This coding standard should be used only when the desired cause value cannot be represented with the ITU-T standardized code.

IO - Implementation Option.

D/ I/ DI - Identifies where the cause code event is determined (D = DSS1 Access [CG/ CD Party to Switch])/ (I = Network, ISUP [Switch to Switch])/ (DI = Either D or I)

◀ ➔ - Indicates direction of ISUP Message.

Cause Code	Event	References/Definition	Preferred Treatment Release With Cause	D// DI	Calling Party	ORIG EO/AT	INTNET	TERM EO/AT	Called Party
98	Message not compatible with call state or message type non-existent or non-implemented	Refer to ANSI T1.607 (5.8.4) This cause indicates that the equipment sending this cause has received a message such that the procedures do not indicate that this is a permissible message to receive while in the call state, or a STATUS message was received indicating an incompatible call state.	(A/T 120ipm) =	D	98	←98	←98	→98←	98
99	Parameter non-existent or not implemented	Refer to ANSI T1.113, ANSI T1.607, GR-317/394, TR-444, TR-268, TR-1268, GR-246 and SR-3137 This cause indicates that the equipment sending this cause has received a message with optional parameters not recognized because the parameter name is not defined or it is defined but not implemented by the equipment sending the cause.	(A/T 120ipm) =	DI	41 99	41←99 ←99	←99 ←99	→99← →99←	99 99
100	Invalid information element content	Refer to ITU - Q850, GR-317/394, TR-444, TR-268, TR-1268 and GR-246 This cause indicates that the equipment sending this cause has received a parameter which it has implemented but for which one or more of the fields in the parameter are coded in a way which has not been implemented by the equipment sending this cause.	(A/T 120ipm) =	D	100	←100	←100	←100	100
101	Message not compatible with call state	Refer to ANSI T1.607 (same as ITU-T - Q.850), TR-444, TR-268, TR-1268, and SR-3137 This cause indicates that the message has been received that is incompatible with the call state. Specified exclusively for ISDN.	(A/T 120ipm) =	DI	101	←101	←101	→101←	101
101N	Protocol error threshold exceeded	ANSI T1.650-1995 This cause indicates that the network is clearing a call because a threshold is being exceeded for multiple protocol errors occurring during an active call.							

No Reference - Indicates that there is no reference to these cause codes in ANSI, ITU-T, TR-268, GR-246, GR-317/394, TR-444, TR-1268, SR-3137 and SR-3138

Special Note - Any Cause Code received that is not specified in the protocol specification of the switch is interpreted as unrecognized and will be treated by routing to the default code of that specific class.

Note 1 - Not being used by the Switched Public Network at this time.

Note 2 - If the release is received before the ACM, reorder (120IPM) will be applied. If the REL is received after the ACM, normal clearing will take place.

Cause Code	Event	References/Definition	Preferred Treatment Release With Cause	D// DI	Calling Party	ORIG EO/AT	INTNET	TERM EO/AT	Called Party
102	Recovery on timer expiration	Refer to GR-317/394, TR-268, TR-1268, GR-246, SR-3137, T1.113.2, and ITU-T-Q.850 This cause is used when a user does not send further indication of progress in call establishment within the prescribed time period. [It indicates that a Q.931 (ANSI T1.607) error handling procedure has been initiated.] Specified exclusively for ISDN.	See Special Note - (Default)	D	102	➔102 ←	←102➔	➔102←	102
103	Parameter non-existent or not implemented - passed on - See Note 1	Refer to ANSI T1.113, GR-317/394 and GR-246	See Special Note - (Default)						
104	No Reference								
105	No Reference								
106	No Reference								
107	No Reference								
108	No Reference								
109	No Reference								

\$ - Due to existing technical limitations within the United States terminating play may continue to be used.

* - Clearing Message w/o cause code.

** - Clearing Message with cause code other than 17, 27, 34, 65 or 88.

*** - It may be more appropriate to map these ISDN access cause codes to 21 rather than 18 or 41.

xN (e.g., 23N) - Indicates National ANSI standard only, not ITU-T standard. This coding standard should be used only when the desired cause value cannot be represented with the ITU-T standardized code.

IO - Implementation Option.

D/ I/ DI - Identifies where the cause code event is determined (D = DSS1 Access [CG/ CD Party to Switch])/ (I = Network, ISUP [Switch to Switch])/ (DI = Either D or I)

← ➔ - Indicates direction of ISUP Message.

Cause Code	Event	References/Definition	Preferred Treatment Release With Cause	D// DI	Calling Party	ORIG EO/AT	INTNET	TERM EO/AT	Called Party
110	Message with Unrecognized Parameter discarded (See Note 1)	Refer to ANSI T1.113.2 and ITU-T -Q.850 This cause indicates that the equipment sending this cause has discarded a received message which includes a parameter that is not recognized	See Special Note - (Default)						
111	Protocol error, unspecified	Refer to ANSI T1.113, GR-317/394, TR-444, TR-268, TR-1268, GR-246 and SR-3137 This is a default cause used to report a protocol error event only when no other cause code in the protocol error class (class 110) applies.	(A/T 120ipm) =	DI	41 111	41←11 1	←111 ←111	111←RWC 111←RWC	
112	No Reference								
113	No Reference								
114	No Reference								
115	No Reference								
116	No Reference								
117	No Reference								
118	No Reference								
119	No Reference								
120	No Reference								
121	No Reference								
122	No Reference								
123	No Reference								
124	No Reference								

No Reference - Indicates that there is no reference to these cause codes in ANSI, ITU-T, TR-268, GR-246, GR-317/394, TR-444, TR-1268, SR-3137 and SR-3138

Special Note - Any Cause Code received that is not specified in the protocol specification of the switch is interpreted as unrecognized and will be treated by routing to the default code of that specific class.

Note 1 - Not being used by the Switched Public Network at this time.

Note 2 - If the release is received before the ACM, reorder (120IPM) will be applied. If the REL is received after the ACM, normal clearing will take place.

Cause Code	Event	References/Definition	Preferred Treatment Release With Cause	D//DI	Calling Party	ORIG EO/AT	INTNET	TERM EO/AT	Called Party
125	No Reference								
126	No Reference								
127	Interworking, unspecified	Refer to ANSI T1.113, GR-317/394, TR-444, TR-268, TR-1268, GR-246 and SR-3137 This is a default cause used to indicate that there has been interworking with a network which does not provide causes for actions taken; thus, the precise cause for the message which is being sent cannot be ascertained.		DI	127	←127	←127	127←RWC	

\$ - Due to existing technical limitations within the United States terminating play may continue to be used.

* - Clearing Message w/o cause code.

** - Clearing Message with cause code other than 17, 27, 34, 65 or 88.

*** - It may be more appropriate to map these ISDN access cause codes to 21 rather than 18 or 41.

xN (e.g., 23N) - Indicates National ANSI standard only, not ITU-T standard. This coding standard should be used only when the desired cause value cannot be represented with the ITU-T standardized code.

IO - Implementation Option.

D/ I/ DI - Identifies where the cause code event is determined (D = DSS1 Access [CG/ CD Party to Switch])/ (I = Network, ISUP [Switch to Switch])/ (DI = Either D or I)

← → - Indicates direction of ISUP Message.



ATIS-0300020

**Next Generation Interconnection Interoperability (NGIIF)
Reference Document**

**Part III, Installation, Testing and Maintenance
Responsibilities for SS7 Links and Trunks**

**Attachment I
SS7 Network Security Base Guidelines**

Version 12.0



ATIS is the leading technical planning and standards development organization committed to the rapid development of global, market-driven standards for the information, entertainment and communications industry. More than 200 companies actively formulate standards in ATIS' Committees, covering issues including: IPTV, Cloud Services, Energy Efficiency, IP-Based and Wireless Technologies, Quality of Service, Billing and Operational Support, Emergency Services, Architectural Platforms and Emerging Networks. In addition, numerous Incubators, Focus and Exploratory Groups address evolving industry priorities including Smart Grid, Machine-to-Machine, Connected Vehicle, IP Downloadable Security, Policy Management and Network Optimization.

ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications' Sectors, and a member of the Inter-American Telecommunication Commission (CITEL). ATIS is accredited by the American National Standards Institute (ANSI). For more information, please visit www.atis.org.

Notice

This document was developed by the Alliance for Telecommunications Industry Solutions' (ATIS) sponsored Next Generation Interconnection Interoperability Forum (NGIIF). The NGIIF addresses next-generation network interconnection and interoperability issues associated with emerging technologies. Specifically, it develops operational procedures which involve the network aspects of architecture, disaster preparedness, installation, maintenance, management, reliability, routing, security, and testing between network operators. In addition, the NGIIF addresses issues which impact the interconnection of existing and next generation networks and facilitate the transition to emerging technologies. All changes to this document shall be made through the NGIIF issue resolution process.

Note Regarding Previous Versions

The NIIF Reference Document was formerly known as the Network Operations Forum (NOF) Reference Document. The NOF Reference Document was published and maintained by Bellcore. The last version of the NOF Reference Document is Issue 13.

Disclaimer and Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

ATIS-0300020, NGIIF Reference Document, Part III, Installation and Maintenance Responsibilities for SS7 Links and Trunks, Attachment G, SS7 Network Security Base Guidelines, Formerly NIIF 5015

The NGIIF Reference Document, Part III, Installation and Maintenance Responsibilities for SS7 Links and Trunks, Attachment G, SS7 Network Security Base Guidelines, is an ATIS standard developed by the NGIIF.

Published by

Alliance for Telecommunications Industry Solutions

1200 G Street, NW, Suite 500

Washington, DC 20005

Copyright © 2011 by Alliance for Telecommunications Industry Solutions

All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < <http://www.atis.org> >.

Printed in the United States of America.

SS7 NETWORK SECURITY BASE GUIDELINES

Table of Contents

1	GENERAL.....	4
1.1	PURPOSE OF THIS DOCUMENT	4
2	SECURITY BASELINE FOR SS7.....	4
2.1	DATA SECURITY FEATURES OF CRITICAL SS7 NODES.....	4
2.2	IDENTIFICATION.....	4
2.3	AUTHENTICATION.....	4
2.4	SYSTEM ACCESS CONTROL.....	5
2.5	RESOURCE ACCESS CONTROL	5
2.6	SECURITY LOG (AUDIT).....	5
2.7	SECURITY ADMINISTRATION	6
2.8	DOCUMENTATION.....	6
3	CONCLUSION	7

1 General

The following SS7 Network Security Base Guidelines should be used as a minimum set of guidelines to be adopted by the Access Service Providers and the Access Service Customers.

1.1 Purpose of this Document

This document is intended to provide a minimum set of general guidelines to be adopted by the Access Service Providers and Access Service Customers.

2 Security Baseline for SS7

2.1 Data Security Features of Critical SS7 Nodes

This section specifies the desirable security features that any SS7 Network Element (NE), Network System (NS), Operations System (OS) or Data Communications Network (DCN) should provide in order to reduce the risk of potentially service affecting security compromises. Highlights of the critical components of those documents are listed below. For the sake of brevity, the term "SS7 node" in the following list is used to imply an NE, NS, OS, or a DCN and its nodes.

2.2 Identification

The SS7 node should not allow an existing user-ID to be assigned to another active user (i.e., user-IDs should be unique).

Each operations related process running in the SS7 node should be associated with the corresponding user-ID (so that an audit trail can be established if there is a need).

The SS7 node should disable a user-ID if it has remained inactive (i.e., never used) over a specifiable time period.

2.3 Authentication

All OAM&P input ports of the SS7 node (including direct, dial-up and network access) should require authentication of a session requester, without any provision for a bypass mechanism.

A single stored password entry (e.g., in a password file) should not be allowed to be shared by multiple user-IDs. However, the SS7 node should not prevent a user from choosing (unknowingly) a password that is already being used by some other user. Nor should the SS7 node volunteer this information to either user.

Passwords should be stored in a one-way encrypted form, and should not be retrievable by any user including managers or administrators (of system and security). Also, there should be no clear text display (on a device such as a screen, typewriter, or printer) of a password at any time (e.g., login, file dump, etc.).

The SS7 node should allow passwords to be user changeable (requiring reauthentication), and should require that the user change it the first time he/she establishes a session with the password assigned to him/her. The default should be non-trivial in nature.

The password should have an "aging" feature, and it should have a complexity requirement to make it not easily guessable. The SS7 node should not accept common words or names as valid passwords. Also, it should not allow a recently obsolete password to be readily reselected by the said user.

2.4 System Access Control

The SS7 node should not allow access to any session requester unless identified and authenticated. There should be no default mechanism to circumvent it.

The SS7 node should not allow any session to be established via a port that is not authorized to accept input commands. For example, if an output port receives a login request, the SS7 node should not respond.

The entire login procedure should be allowed to be completed without interruption, even if incorrect parameters (such as an incorrect user-ID or an incorrect password) are entered, and no "help message" should be transmitted to the session requester as to which part of the authentication is incorrect. The only information to be conveyed at the end of the login attempt is that the login is invalid.

After a specified number of incorrect login attempts carried out in succession, the SS7 node should lock out the channel and raise an alarm in real time for the administrator.

Before the session begins, the SS7 node should provide a warning message explicitly alerting the user of the consequences of unauthorized access and use.

At the beginning of the session, the SS7 node should display the date and time of the user's last successful access and the number of unsuccessful attempts, if any, that have been made to establish a session since the last successful access.

There should be a "time-out" feature - i.e., the SS7 node should disconnect or reauthenticate users after a specified time interval during which no messages were exchanged. Also, there should be a mechanism for user-initiated keyboard locking.

The SS7 node should provide a mechanism to end a session through a secure logoff procedure. If a session gets interrupted due to reasons such as time-out, power failure, link disconnection, etc., the port should be dropped immediately.

For dial-up access over untrusted channels, authentication involving one time passwords should be required (e.g., smart card, third party authentication, etc.).

2.5 Resource Access Control

Access to resources should be controlled on the basis of "privilege" (i.e., access permission) associated with user-ID and channel. It should not be based on a "password" associated with the access function, because that password will have to be necessarily shared among all users requiring such access. Neither should encryption be used as a primary access control mechanism (though encryption may be used to enhance it).

The granularity of resource access control should be such that for each resource it should be possible to grant (or deny) access privilege to any single user (or a prescribed group of users). For example, the control should be adequately fine-grained so that user access and channel access can be restricted on the basis of commands, database views (i.e., objects), records (i.e., object instances), and fields (i.e., attributes).

If external entities - e.g., customers, are allowed access to the resources, each SS7 node's resource (e.g., proprietary data) should be protected from access by unauthorized persons.

Executable/loadable/fetchable software should be access controlled for overwrite, update, and execution rights.

2.6 Security Log (Audit)

The SS7 node should generate a security log containing information sufficient for after-the-fact investigation of loss or impropriety.

The security log should be protected from unauthorized access. No user should be allowed to modify or delete a security log. There should be no mechanism to disable the security log. There should be an alarm in real time if the security log does not function properly.

The security log should, at a minimum, record events such as all sessions established, invalid user authentication attempts, and unauthorized attempts to access resources (including data and transactions). It should also include changes in users' security profiles and attributes, changes in access rights to resources, changes in the SS7 node security configuration, and modification of SS7 node software. For each such event, the record should, as a minimum, include date and time of event, initiator of the event such as: user-ID, terminal, port, network address, etc., names of resources accessed, and success or failure of the event.

Actual or attempted passwords should not be recorded in the security log.

There should be audit tools to produce exception reports, summary reports, and detailed reports on specifiable data items, users, or communication facilities.

2.7 Security Administration

The SS7 node should support functions for the "management" of security related data (e.g., security parameters such as user-IDs, passwords, privileges, etc.) as "separate" from other user functions. Security administration should be reserved only for an appropriate administrator.

The administrator should be able to display all currently logged-in users as well as a list of all authorized user-IDs.

The administrator should be able to independently and selectively monitor, in real time, the actions of any one or more users based on respective user-IDs, terminals, ports, or network addresses.

The administrator should be able to identify all resources owned by or accessible to any specific user along with the associated access privileges.

The administrator should be able to enter, edit, delete or retrieve all attributes of a user-ID (except for a password, which should not be retrievable).

The administrator should limit the use of a "null password" during system login on a per user or per port basis (i.e., during new release installation).

The administrator should be able to save the security log for safe storage, so that it is not written over when the buffer is full.

All security parameters (e.g., password aging interval, time-out interval, various alarm conditions) should be specifiable and adjustable by the administrator. This implies that the SS7 node should not have any security parameters hard coded.

2.8 Documentation

Any SS7 node supplier/vendor should provide documentation on security considerations for administrators, operators, and users. They can be stand alone documents or sections incorporated in appropriate vendor manuals.

The administrator's guide should contain items such as: functions and privileges that need to be controlled to secure the facility, proper usage of security audit tools, procedures for examining and maintaining audit files, and procedures for periodic saving and backup of security logs. It should also include recommendations on setting the minimum access permissions on all files, directories, and databases, guidelines on security assessment techniques.

The operator's guide should contain procedures necessary to initially start the SS7 node in a secure manner and to resume secure operation after any lapse that may have occurred.

The user's guide should describe the protection mechanisms that are non-transparent to the user, should explain their purpose, and provide guidelines on their use. It should not contain any information that could jeopardize the security of the SS7 node if made public.

The above list is not exhaustive. There are requirements related to other areas such as: data and system integrity, and various phases of life cycle involving design, packaging, delivery, and support by the vendor.

3 Conclusion

The following table includes a list of questions that should be addressed when performing a security analysis. The list is not a complete list but is provided as a starting point.

Table 1: Systems Engineering Approach to Security Baseline for SS7

CCSN Logical Security Checklist		
Question	Yes/No	If No, Why not?
Is security addressed across the entity's entire CCS network?		
Are CCSN Critical Common Environments defined and isolated (e.g., by firewall perimeters) to limit access to authorized processes and users?		
If fire walls are deployed are they placed around the CCSN CCE e.g., a "perimeter" or perimeters placed around the OAM&P of critical CCS components, NEs, NSs and OSs ?		
Are software changes controlled and verified to maintain the established security perimeter?		
Has a security baseline been established for Network Elements, NEs, Network Systems, NSs, and Operations Support Systems, OSs and Data Communication Network DCNs?		
Is that baseline specified or referenced in procurement RFPs and contracts?		
Do new NEs, NSs, OSs and DCNs meet those requirements?		
Are organizational responsibilities for network security defined?		
Is that responsibility clearly placed within CCSN common management reporting?		
Is security part of the defined responsibilities for the personnel that monitor, maintain and control various CCSN and SS7 components?		
Are all CCS network connectivity and network mappings documented?		
If documented, has the connectivity been verified?		
Have the following generic countermeasures been implemented for all key CCSN nodes (NEs, NSs and OSs):		

CCSN Logical Security Checklist		
Question	Yes/No	If No, Why not?
Assignment of command privileges to each class of user by functional responsibility, to allow the power to get the job done, while reserving special power (e.g., the ability to change user passwords) to the security administrator ?		
Use of (COMPLIANT) commercially-available access-control systems (e.g., dial-back modems that do not utilize a pass-through feature) to secure remote access to CCS nodes?		
Use of encryption equipment at each end of an OAM&P access session which transits an open PPSN?		
Use of available access control software at the host system?		
Use of established access procedures and security routines (e.g., periodic re-authorization of users and the use of security tools)?		
Elimination of uncontrolled dial access?		
Controlled access for vendor support?		
Controlled access to dial-in protocol analyzers on the signaling links and X.25 facilities between CCSN nodes e.g., STPs?		
Intrusion recovery plans for the entity's CCSN?		
Security on the gateway screening tables?		
Adequate security on the node restart capability?		
Adequate security on vendor-specific node restart procedures?		
Back-up tapes and media available and secured off-site?		



ATIS-0300021

**Next Generation Interconnection Interoperability (NGIIF)
Reference Document**

**Part III, Installation, Testing and Maintenance
Responsibilities for SS7 Links and Trunks**

**Attachment J
SS7 Software Validation**

Version 12.0



ATIS is the leading technical planning and standards development organization committed to the rapid development of global, market-driven standards for the information, entertainment and communications industry. More than 200 companies actively formulate standards in ATIS' Committees, covering issues including: IPTV, Cloud Services, Energy Efficiency, IP-Based and Wireless Technologies, Quality of Service, Billing and Operational Support, Emergency Services, Architectural Platforms and Emerging Networks. In addition, numerous Incubators, Focus and Exploratory Groups address evolving industry priorities including Smart Grid, Machine-to-Machine, Connected Vehicle, IP Downloadable Security, Policy Management and Network Optimization.

ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications' Sectors, and a member of the Inter-American Telecommunication Commission (CITEL). ATIS is accredited by the American National Standards Institute (ANSI). For more information, please visit www.atis.org.

Notice

This document was developed by the Alliance for Telecommunications Industry Solutions' (ATIS) sponsored Next Generation Interconnection Interoperability Forum (NGIIF). The NGIIF addresses next-generation network interconnection and interoperability issues associated with emerging technologies. Specifically, it develops operational procedures which involve the network aspects of architecture, disaster preparedness, installation, maintenance, management, reliability, routing, security, and testing between network operators. In addition, the NGIIF addresses issues which impact the interconnection of existing and next generation networks and facilitate the transition to emerging technologies. All changes to this document shall be made through the NGIIF issue resolution process.

Note Regarding Previous Versions

The NIIF Reference Document was formerly known as the Network Operations Forum (NOF) Reference Document. The NOF Reference Document was published and maintained by Bellcore. The last version of the NOF Reference Document is Issue 13.

Disclaimer and Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

ATIS-0300021, NGIIF Reference Document, Part III, Installation and Maintenance Responsibilities for SS7 Links and Trunks, Attachment J, SS7 Software Validation, Formerly NIIF 5016

The NGIIF Reference Document, Part III, Installation and Maintenance Responsibilities for SS7 Links and Trunks, Attachment J, SS7 Software Validation, is an ATIS standard developed by the NGIIF.

Published by

Alliance for Telecommunications Industry Solutions

1200 G Street, NW, Suite 500

Washington, DC 20005

Copyright © 2011 by Alliance for Telecommunications Industry Solutions

All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < <http://www.atis.org> >.

Printed in the United States of America.

SS7 SOFTWARE VALIDATION

Table of Contents

1	GENERAL.....	5
1.1	PURPOSE.....	5
1.2	DEFINITIONS	5
1.3	PURPOSE OF SOFTWARE VALIDATION.....	5
2	BASIC PREMISES.....	5
3	OPERATING PRINCIPLES	6
4	CRITERIA FOR SERVICE PROVIDERS AND VENDOR/MANUFACTURERS	6
5	SERVICE PROVIDER (ASP/ASC) REQUIREMENTS.....	6
5.1	WRITTEN REQUIREMENTS	6
5.2	STANDARDS INTERPRETATIONS.....	7
5.3	GENERAL NETWORK DOCUMENTATION	7
5.4	NETWORK UNIQUENESS DOCUMENTATION	7
6	VENDOR/MANUFACTURER SOFTWARE VALIDATION CRITERIA.....	7
6.1	VENDOR/MANUFACTURER REQUIREMENTS	7
7	VENDOR/MANUFACTURER PRODUCT IMPLEMENTATION.....	7
7.1	OPTIONAL REQUIREMENTS.....	8
7.2	CONFORMANCE TO REQUIREMENTS	8
7.3	CROSS-PRODUCT IMPLEMENTATION	8
8	VENDOR/MANUFACTURER PRODUCT TESTING	8
8.1	TESTING ENVIRONMENT	8
8.2	CONFORMANCE TO PRODUCT REQUIREMENTS	8
8.3	PRODUCT PERFORMANCE	9
8.4	SYSTEM FAULT TOLERANCE.....	9
8.5	SYSTEM RECOVERY	9
8.6	METHODS AND PROCEDURES.....	9
8.7	REGRESSION TESTING.....	9
8.8	FEATURE INTERACTION TESTING.....	9
8.9	MULTI-VENDOR INTEROPERABILITY	9
8.10	SOFTWARE UPDATES/CHANGES	10
8.11	TESTING INFORMATION	10
9	VENDOR/MANUFACTURER PRODUCT DEPLOYMENT	10
9.1	PROBLEM RESOLUTION.....	10
9.2	ROOT CAUSE ANALYSIS	10
10	SERVICE PROVIDER TESTING/DEPLOYMENT	10
10.1	INTEGRATION TESTING.....	10
10.2	METHODS AND PROCEDURES.....	11
10.3	SOFTWARE UPDATE/CHANGES	11
10.4	MULTI-VENDOR INTEROPERABILITY TESTING.....	11
10.5	VENDOR/MANUFACTURER DOCUMENTATION	11
10.6	NEW SOFTWARE	11
10.7	UPDATES	11

1 General

1.1 Purpose

This document is intended to provide general guidelines for the Development and Validation of Software for use in the Telecommunications industry as it applies to Interconnected switching/signaling nodes. It represents Network Interconnection Interoperability Forum (NGIIF) consensus arrived at by participating members consisting of Access Service Providers, Access Service Customers and Vendor/Manufacturers. Although aimed at SS7 software, the guidelines are deemed generally applicable to other types of software in use by the Telecommunications Industry.

This document does not replace or supersede any existing Contracts, Tariffs or any other legally binding documents.

1.2 Definitions

For the purposes of this document the following terms apply:

- Vendor/Manufacturer refers to those companies that develop and supply software to the Telecommunications industry for switching/signaling node application.
- Service Provider refers to Access Service Providers and Access Service Customers purchasing software from Vendor/Manufacturers of telecommunications software products.
- Product: In the context of this document the term product shall be defined as the "software" package under development or validation.
- Service Provider Product requirements: Capabilities as defined by the Service Provider and Industry standards which drive the development of the product.
- Product Implementation: The process by which the Service Provider Product requirements are incorporated into a soft-ware product whether or not it currently exists.

1.3 Purpose of Software Validation

The purpose of software product validation as described in this document is to provide assurance to all users of software as it applies to the telecommunications industry, that the software products perform according to "agreed upon" service provider product requirements and that all reasonable care has been taken to identify and correct any anomalies that have the potential to negatively impact the operation of switching/signaling nodes so that the quality of service is continually enhanced to meet or exceed the customers' expectations.

2 Basic Premises

Service Providers of telecommunications service have an obligation to their Customers to provide the highest standard of error free service.

Vendor/Manufacturers of telecommunications switching/signaling node software have a responsibility to the Service Providers of telecommunications services to provide the highest standard of error free software possible.

An uncompromised focus on the development/validation of error free software will result in improved quality and reliability of the switching/signaling nodes and networks.

3 Operating Principles

Service Providers should have "agreed upon" procedures in place with their Vendor/Manufacturers to provide continuous assurance for the quality of software prior to and after deployment in their respective switching/signaling networks.

When the need for information exchange is identified, such information should be shared in accordance with the guidelines outlined in the Network Interconnection Interoperability Forum (NGIIF) document, titled Information Sharing. For example, signaling anomalies identified in the NGIIF Internetwork Interoperability Test Plan (IITP) testing, or individual software customer problems as they relate to potential non-conformance with industry standards should be shared with the affected Service Provider.

Vendor/Manufacturers should review their software development/validation processes to continually enhance their capability to identify and fix potential software problems prior to deployment.

The Vendor/Manufacturer and their respective Service Provider(s) should utilize knowledge gained during software product testing and deployment phases to augment their testing procedures, for the purpose of identifying and eliminating potential non-conformance prior to subsequent product to deployment.

4 Criteria for Service Providers and Vendor/Manufacturers

In the subsections that follow, this document defines criteria that should be followed by the Service Provider and/or Vendor/Manufacturer for software product validation throughout the development process, to achieve the general objectives defined in section 2 of this document. The following subsections are:

- Service Provider's requirements
- Vendor/Manufacturer's requirements
- Vendor/Manufacturer's Implementation
- Vendor/Manufacturer's Testing
- Service Provider's Pre-deployment Testing
- Service Provider's Deployment Testing

5 Service Provider (ASP/ASC) Requirements

This section defines the responsibilities of the Service Providers in regard to providing their requirements to the Vendor/Manufacturer.

5.1 *Written Requirements*

Service Providers should provide explicit written requirements for capabilities requested from their Vendor/Manufacturers. Service Providers should ensure that their requirements are clear and complete; these requirements may reference industry standards.

Service Providers should define in writing those standards/requirements that they desire the capabilities to conform to. Specific documents and versions should be identified during the requirements phase.

When the standards/requirements specifications used include optional capabilities, the Service Providers should identify in writing those options desired.

5.2 Standards Interpretations

If the Service Provider perceives a standard to be ambiguous, incorrect or flawed, (e.g., open to multiple interpretations), the Service Provider should document their required implementation as early in the requirements phase as possible. In addition the Service Provider should interface with the appropriate standards body to clarify any ambiguities. The Vendor/Manufacturer should review this information, and provide feedback to the Service Provider during the requirements phase.

5.3 General Network Documentation

Service Providers may provide documentation to their Vendor/Manufacturer before the end of the requirements phase describing their network environment.

5.4 Network Uniqueness Documentation

This documentation may include any specific test scenarios or situations that may be unique to their network to the Vendor/Manufacturer during the requirements phase.

Where requirements are Service Provider specific, the Service Provider shall engage in dialogue with their Vendor/Manufacturer to ensure understanding of those requirements.

6 Vendor/Manufacturer Software Validation Criteria

6.1 Vendor/Manufacturer Requirements

The software validation criteria for the requirements are as follows:

Known Non-conformance to Requirements - The Vendor/Manufacturer shall provide documentation to the Service Provider identifying all known/anticipated non-conformance(s) to Service Provider Product requirements. For example, a known non-conformance could exist when a Vendor/Manufacturer only implements a subset of a standard. The Service Provider should review this information, and provide prompt feedback to the Vendor/Manufacturer during the requirements phase.

Standards Interpretations - If the Vendor/Manufacturer perceives a standard to be ambiguous, incorrect or flawed, (e.g., open to multiple interpretations), the Vendor/Manufacturer should document their planned implementation as early in the requirements phase as possible. In addition the Vendor/Manufacturer should interface with the appropriate standards body for clarification of any ambiguities. The Service Provider should review this information, and provide feedback to the Vendor/Manufacturer during the requirements phase.

Service Provider Changes/Upgrades - All Service Provider requirements including "agreed upon" changes/upgrades will be documented by the Vendor/Manufacturer and Service Provider prior to completion of the requirements phase.

7 Vendor/Manufacturer Product Implementation

The software validation criteria for Product Implementation are as follows:

7.1 Optional Requirements

When Service Provider Product requirements include options (e.g., optional parameters or procedures), the Vendor/Manufacturer should provide documentation to the Service Provider identifying which option(s), if any, the Vendor/Manufacturer plans to implement. The Service Provider should review this information, and provide feedback to the Vendor/Manufacturer proactively.

7.2 Conformance to Requirements

The Vendor/Manufacturer should ensure that the software implemented conforms to all specified and "agreed upon" requirements taking into consideration any documented non-conformance(s) and "agreed upon" interpretations. The Vendor/Manufacturer shall document all known deviations from Service Provider requirements in regards to capability of the product being implemented.

Such information should be provided to the Service Provider at commencement of the software implementation phase and on an ongoing basis. Service Providers should review such information and provide feedback to their Vendor/Manufacturer.

7.3 Cross-product Implementation

The Vendor/Manufacturer should ensure that interoperability incompatibilities are not implemented between Switching/Signaling Nodes in their product line.

8 Vendor/Manufacturer Product Testing

The software validation criteria for the Product Testing Phase are as follows:

8.1 Testing Environment

The Vendor/Manufacturers should utilize a testing environment which enables verification of conformance to Service Provider requirements while simulating, as closely as possible, the Service Provider's networks into which the software products are to be deployed (using information referenced in the General Network Documentation and Network Uniqueness Documentation sections of this document).

The extent to which a Service Provider's network uniqueness, as referenced in the Network Uniqueness Documentation section of the document, requires customization of the Vendor/Manufacturer's testing environment, may have to be negotiated.

8.2 Conformance to Product Requirements

The Vendor/Manufacturer should test all Service Provider software releases (e.g., generic upgrades) to ensure that the software releases conform to all specified and "agreed upon" Service Provider Product requirements, taking into consideration any documented non-conformance and interpretations.

The Vendor/Manufacturer should maintain and make available to the Service Provider detailed documentation identifying its conformance or non-conformance correlated with the Service Provider's Product requirements. Where non-conformances are identified, the behavior of the product should be fully described.

Where conformance is asserted based on testing, the above documentation should identify the test(s) performed and the software release(s) on which those tests were performed. Where conformance is asserted in the absence of testing, that fact should be clearly noted.

8.3 Product Performance

The Vendor/Manufacturer should test whether the product performance (e.g., all processing capacity) meets or exceeds the product performance requirements as specified in documentation exchanged with the Service Provider. If any inconsistencies are identified with information previously provided to the Service Provider, the updated information should be provided no later than the time of software delivery.

Where software or hardware design interactions result in measured performance being dependent on factors other than those specified in the requirements, those dependencies will be documented by the Vendor/Manufacturer and furnished to the Service Provider. The vendor/manufacturer will perform sufficient testing (and provide results to the Service Provider) so that the Service Provider can reliably estimate actual performance in the target network.

8.4 System Fault Tolerance

Testing should be done to ensure that system/entity faults in the switching/signaling node under test do not cause network outages or degradation to service. This testing should include the simulation of catastrophic failures, and should be tested at both minimum and maximum (engineered) SS7 message traffic capacity.

8.5 System Recovery

The Vendor/Manufacturer should verify full system recovery for the Switching/Signaling Node under test from catastrophic failures (e.g., power loss). This would include ensuring that automatic recovery takes place for system software and verifies recoverability of all system components. System recovery should be tested at both minimum and maximum (engineered) SS7 message traffic capacity.

8.6 Methods and Procedures

The Vendor/Manufacturer should validate the accuracy of all installation methods and procedures, as well as supporting documentation.

8.7 Regression Testing

Where currently supported software releases are already in service, any enhancement/change shall be regression tested to ensure that no adverse affects occur.

8.8 Feature Interaction Testing

The Vendor/Manufacturer shall validate feature interaction and compatibility in currently supported software releases.

8.9 Multi-Vendor Interoperability

The Vendor/Manufacturer should participate in "agreed upon" multi-vendor testing which is initiated and facilitated by the Service Provider.

8.10 Software Updates/Changes

The Vendor/Manufacturer should test all updates/changes applied to in service software products to ensure that the updates/changes will not result in any SS7 protocol non-conformance; or increase the potential for loss of service or compromise in the reliability, capacity, or performance in a single network or interconnected networks.

8.11 Testing Information

The Vendor/Manufacturer should maintain detailed descriptions of the tests performed pursuant to the above activities and the results obtained. This information should be made available to the Service Provider upon request.

9 Vendor/Manufacturer Product Deployment

The software validation criteria for the Deployment Phase are as follows:

9.1 Problem Resolution

The Vendor/Manufacturer should ensure that identified troubles are corrected, if necessary, across all supported products of the Vendor/Manufacturer that could have the same or similar trouble.

9.2 Root Cause Analysis

After determining that one or more of its products contributed to a network outage, simplex failure, or service degradation event or a possibility of any of the above, the Vendor/Manufacturer should perform a root cause analysis to determine the source of the trouble. The purpose of this analysis is to reduce or eliminate the likelihood of similar future events and to provide information for use in improvement to the software development process.

10 Service Provider Testing/Deployment

The following describes the software validation activities recommended to be performed by the Service Provider to ensure the highest possible software quality.

10.1 Integration Testing

Service Providers should perform integration testing for their network configuration for all new capabilities and update/changes. This integration testing should include but is not limited to other Vendor/Manufacturers equipment and interconnected networks.

Problems identified during testing should be reported to the respective Vendor/Manufacturers and information shared in accordance with the Network Interconnection Interoperability Forum (NGIIF) Information Sharing Guidelines. In addition, any problems resulting from testing between interconnected Service Providers, whether industry sponsored (e.g., NGIIF, Internetwork Interoperability Test Plan) or not, should be reported to the affected Vendor/Manufacturer via existing processes.

10.2 Methods and Procedures

Service Providers should carefully follow software installation procedures and report any problems to their Vendor/Manufacturer immediately.

10.3 Software Update/Changes

Service Providers should ensure that all updates/changes are applied in accordance with the Vendor/Manufacturers recommended priority sequence.

10.4 Multi-Vendor Interoperability Testing

The Service Provider should initiate and facilitate multi-vendor interoperability testing when appropriate.

Where Service Providers do not have laboratory facilities to engage in their own integration testing, or as an alternative, it is recommended that they facilitate the means to perform testing that satisfies their business responsibilities to ensure quality of service.

10.5 Vendor/Manufacturer Documentation

This section describes the expectations for the provision and update of documentation.

10.6 New Software

Where new software is provided to the Service Provider the supporting documentation should be provided. This documentation shall be reviewed by the Service Provider for understanding. Any questions should be addressed to the Vendor/Manufacturer for clarification.

10.7 Updates

The Vendor/Manufacturer should provide updated documentation to the Service Provider. The Service Provider should review this documentation and provide feedback to the Vendor/Manufacturer.



ATIS-0300022

**Next Generation Interconnection Interoperability (NGIIF)
Reference Document**

**Part III, Installation, Testing and Maintenance
Responsibilities for SS7 Links and Trunks**

**Attachment K, Dual STP Failure Prevention Procedures
(Formerly NIIF 5017)**

Version 12.0



ATIS is the leading technical planning and standards development organization committed to the rapid development of global, market-driven standards for the information, entertainment and communications industry. More than 200 companies actively formulate standards in ATIS' Committees, covering issues including: IPTV, Cloud Services, Energy Efficiency, IP-Based and Wireless Technologies, Quality of Service, Billing and Operational Support, Emergency Services, Architectural Platforms and Emerging Networks. In addition, numerous Incubators, Focus and Exploratory Groups address evolving industry priorities including Smart Grid, Machine-to-Machine, Connected Vehicle, IP Downloadable Security, Policy Management and Network Optimization.

ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications' Sectors, and a member of the Inter-American Telecommunication Commission (CITEL). ATIS is accredited by the American National Standards Institute (ANSI). For more information, please visit www.atis.org.

Notice

This document was developed by the Alliance for Telecommunications Industry Solutions' (ATIS) sponsored Next Generation Interconnection Interoperability Forum (NGIIF). The NGIIF addresses next-generation network interconnection and interoperability issues associated with emerging technologies. Specifically, it develops operational procedures which involve the network aspects of architecture, disaster preparedness, installation, maintenance, management, reliability, routing, security, and testing between network operators. In addition, the NGIIF addresses issues which impact the interconnection of existing and next generation networks and facilitate the transition to emerging technologies. All changes to this document shall be made through the NGIIF issue resolution process.

Note Regarding Previous Versions

The NIIF Reference Document was formerly known as the Network Operations Forum (NOF) Reference Document. The NOF Reference Document was published and maintained by Bellcore. The last version of the NOF Reference Document is Issue 13.

Disclaimer and Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

ATIS-0300022, NGIIF Reference Document, Part III, Installation and Maintenance Responsibilities for SS7 Links and Trunks, Attachment K, Dual STP Failure Prevention Procedures, Formerly NIIF 5017

The NGIIF Reference Document, Part III, Installation and Maintenance Responsibilities for SS7 Links and Trunks, Attachment K, Dual STP Failure Prevention Procedures, is an ATIS standard developed by the NGIIF..

Published by

Alliance for Telecommunications Industry Solutions

1200 G Street, NW, Suite 500

Washington, DC 20005

Copyright © 2011 by Alliance for Telecommunications Industry Solutions

All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < <http://www.atis.org> >.

Printed in the United States of America.

Dual STP Failure Prevention Procedures

Table of Contents

1	GENERAL.....	4
1.1	PURPOSE.....	4
1.2	DEFINITIONS	4
2	BASIC PREMISES.....	4
3	SCOPE OF THIS DOCUMENT	5
4	SS7 COMPONENT IDENTIFICATION.....	5
5	DECLARING ORGANIZATIONS.....	5
6	NOC/SCC JOINT RESPONSIBILITIES.....	5
7	STP MAINTENANCE WORK GROUP RESPONSIBILITIES.....	6
8	INTERCONNECTION RESPONSIBILITIES.....	6
9	ORGANIZATION IDENTIFICATION	6
10	COMMUNICATIONS	7
11	AWARENESS TRAINING.....	7
12	ATTACHMENTS	7
13	ATTACHMENT 1, SIMPLEX/DUPLEX OUTAGE/RESTORATION NOTIFICATION FORM	8
14	ATTACHMENT 2, EXAMPLE OF STICKER AND TAGS.....	10
15	ATTACHMENT 3, TABLE 1 SS7 STICKERS, TAGS AND DUMMY PLUGS.....	11
16	ATTACHMENT 4, LISTING OF ESSENTIAL EQUIPMENT/FACILITIES.....	12
16.1	SS7 COMPONENT IDENTIFICATION LISTING.....	12

1 General

The NGIIF recommends that each STP Owner/Operator have in place a written procedure to assist in the prevention of Dual STP failures. This section outlines a minimum set of “recommended” guidelines.

1.1 Purpose

This document provides guidance to operators and maintenance organizations of Signaling Transfer Points (STP) in the telecommunications industry. Suggested work functions and preventative measures are included in this document that should be performed and or taken in order to minimize the potential for loss of an STP and the subsequent customer impact.

This document is generic in principle, and should be modified to meet particular companies operating needs and procedures. Acronyms describing systems or work centers are provided for example only.

Where organizational structures differ from company to company it is recommended, where applicable that the responsibilities and actions outlined in this document be assigned and performed by the appropriate organization.

This document does not replace or supersede any existing contracts, tariffs or any other legally binding document.

1.2 Definitions

For the purpose of this document the following definitions shall apply:

Duplex Condition - A condition in which the both STPs are in service and in a stable call processing condition.

Simplex Condition - A condition in which a single STP has failed (simplex condition).

Essential Equipment - That equipment that has been deemed necessary to maintain the health of the SS7 network.

SCC - Switching Control Center (surveillance center Tier 1 support). The Center that has operational responsibility for surveillance of the STPs and SS7 compatible switches in their respective geographical areas.

SNCC/SNSC/SEAC - Signaling Network Control Center/Signaling Network Support Center/Signaling Engineering & Administration Center. The site with overall responsibility for the maintenance and control of the Signaling Network.

NOC - Network Operations Center (Tier II Support). The center that provides Surveillance and Support for the entire network which includes the Signaling Network (SS7).

2 Basic Premises

STP owner/operators have an obligation to ensure the integrity of the signaling network by having in place the appropriate organizational structure, guidelines for maintenance personal and procedure for the restoration of STPs in the event of a network failure.

Proactive provisioning, identification and marking of all facilities that affect the integrity of the SS7 network can and will reduce the risk of accidental network events.

Wherever possible provisioning arrangements should segregate CCS7 DS0 signals from non-CCS7 DS0s on a DS1 to ensure the integrity of the CCS7 network.

This document addresses suggested process enhancements to current processes associated with the maintenance of STPs and their environments.

3 Scope of this Document

The scope of this document is restricted to:

The identification of SS7 related equipment

Associated organizational responsibilities to declare a Duplex/Simplex condition (Internally and Externally)

Maintenance of network integrity during an incident

STP node simplex outages

4 SS7 Component Identification

All STP and SCP communications equipment that supports CCS links or systems that support communications equipment should be marked with SS7 stickers or tag indications to avoid accidental outages (see Attachment 4).

Main Frame Link appearances should be identified using tags and stickers. Bare pins, should be protected, where possible, with red slip on covers.

The DSX bay appearance of all SS7 links should be equipped with red "dummy" plugs. Each plug should be inscribed with the letters CCS or SS7.

As new equipment is added to the network that has a direct impact on the integrity of the STPs they should be identified and marked appropriately, in addition they should be added to the list of critical equipment listings.

Responsible organizations should perform a review of critical equipment at least every six months to provide assurance for the integrity of the STPs.

5 Declaring Organizations

This section describes the responsibilities of the NSMC (SEAC, SNCC/SNSC), Tier II support organizations associated with an STP Simplex/Duplex alert condition.

In the event of an STP simplex condition, the Network Operations Center (SEAC, SNCC/SNSC) is responsible for declaring a failure of the STP mated pairs. The Network Operations Center (SEAC, SNCC/SNSC) is also responsible for declaring a return to service of the mated STP pair.

When a Simplex condition requirement has been met, the NOC is responsible for notifying the SCC supporting the remaining working STP and declaring a Simplex condition.

6 NOC/SCC Joint Responsibilities

This section describes the responsibilities of the NOC, SCC in the event of a Simplex/Duplex condition associated with an STP.

NOC, SCC personnel are responsible for notifying the appropriate internal organizations and levels of management of a Simplex condition.

When the Out of Service STP has recovered and is in a stable condition, the NOC is responsible for declaring a Duplex condition by notifying the same SCC contact as used to declare the Simplex condition.

All NOC, SCCs shall maintain an EMERGENCY PROCEDURES and contact listings document for notification purposes, the contact listings should be updated as soon as changes are identified and on a six month basis, a verification of those contact listings should be performed.

It is recommended that the Emergency Procedures and Contact list be kept in an "SS7 Emergency Procedures Binder" at the appropriate NOC, SCC work station. Copies of this document should be provided to the NOC, SCC duty supervisor for use in the event of an emergency.

The NOC, SCC is responsible for the identification of all associated equipment that is deemed essential for the integrity of the STP and the SS7 network (see attachment 4).

7 STP Maintenance Work Group Responsibilities

This section outlines the responsibilities of the organization that maintains the STPs.

In an STP environment (e.g., physical plant), when a Simplex condition exist, all routine work in the mate STP location shall cease, in addition all applicable work being performed in any location considered essential to maintaining the health of the working STP shall be suspended.

All routine software input on the working STP must be suspended at the appropriate time during a Simplex condition, and should only resume once a Duplex condition has been declared.

Where work that is underway that is deemed critical, such work shall be completed. At that point all further work shall cease. When this situation arises notification shall be made to the controlling SCC.

When a node is isolated from the working STP during a Simplex condition the link(s) should be restored to service immediately. If links are out of service at the working STP but no nodes are isolated or experiencing congestion due to links being out of service, the links should not be restored until a Duplex condition has been declared.

When a Simplex condition has been declared, it is the responsibility of the personnel at the site of the working STP to ensure that all work activities being performed that may impact the STP are aware of the condition and that all related work operations are suspended.

8 Interconnection Responsibilities

This section outlines the responsibility the company experiencing the STP outage has in regards to notifying their interconnected parties.

Where it has been determined that there is a direct interconnection to an ASC/ASP the company declaring the Simplex/Duplex condition should contact the interconnected parties as soon as possible and inform them of the situation.

9 Organization Identification

This section covers the identification of some of those organizations that may need to be informed in the event of a Simplex condition.

The organization that has the responsibility for the maintenance of the STP is responsible for identifying those organizations that need to be informed of the Simplex/Duplex condition.

All locations/work groups identified as being essential to the integrity of the STP and SS7 network shall provide an emergency contact number to the NOC, SCC.

10 Communications

This section outlines responsibilities for the establishment of communications prior to a Simplex condition being declared.

All service providers should have in place an internal methodology to communicate in the event that the Public Switched network is in a degraded condition or completely out of service. In addition as recommended by the Network Interconnection Interoperability Forum all service providers should subscribed to an emergency communications network to assist in facilitating the restoration of the network node that is out of service.

In the event of a Simplex/Duplex condition being declared the appropriate organizations as determined by each provider should be notified immediately in accordance with locally determined procedures.

11 Awareness Training

This section covers recommendations for awareness training associated with the prevention of a dual STP failure.

An awareness training program should be implemented to educate all work groups of the impact a failed STP may have in their respective network.

The awareness training should include a detailed review of the locally produced dual STP failure prevention document.

12 Attachments

This section lists all of the attachments which should be associated with this document.

- Attachment 1 - Simplex/Duplex Outage/Restoration Notification form
- Attachment 2 - Example of Sticker and Tags
- Attachment 3 - Table 1 SS7 Stickers, Tags and Dummy Plugs
- Attachment 4 - Listing of Essential Equipment/Facilities

13 Attachment 1, Simplex/Duplex Outage/Restoration Notification form

CONDITION RED/GREEN FORM

FAILED STP ID: _____

MATE STP ID: _____

CHECKLIST REQUIREMENTS

1. CONDITION RED – DECLARE A WORK SUSPENSION IN THE AREAS LISTED BELOW:
2. CONDITION GREEN – RESUME WORK IN AREAS LISTED BELOW:

NOC/SCC CONTACT NUMBER: _____

(All STP maintenance, routines, (REX, etc.) unnecessary link maintenance)

STP SOFTWARE CONTACT NUMBER: _____

(All STP translations, patches, etc.)

TOLL CONTACT NUMBER: _____

(Carrier banks, DCS systems, CSU/DSU, DSX, office timing supply work)

ENGINEERING/INSTALLATION WORK CONTRACT NUMBER: _____

(Engineering/Installation work in all buildings containing critical STP equipment/links)

ESSENTIAL EQUIPMENT CONTACT NUMBER: _____

(Essential non-collocated DCS equipment transporting SS7 links to the working STP)

POWER CONTACT NUMBER: _____

(All STP – related power work on batteries, rectifiers, converters/inverters, control bays, distribution bays, switches, fuses, and breakers)

FRAME WORK CONTACT NUMBER: _____

(SS7 main frame blocks)

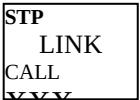
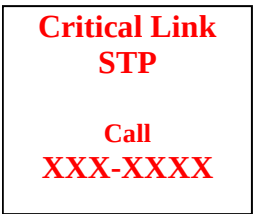
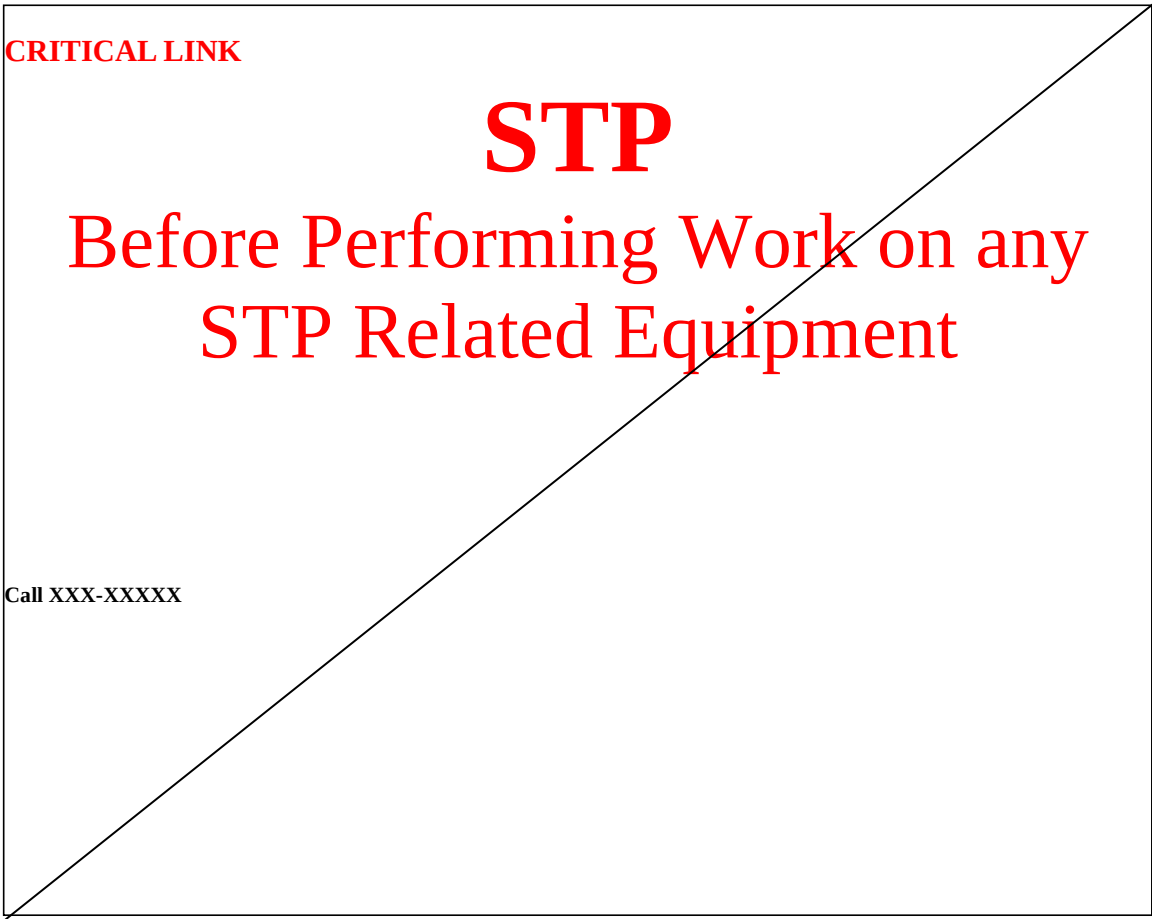
OUTSIDE PLANT WORK CONTACT NUMBER: _____

(Cable vaults in the working STP building)

BUILDING MAINTENANCE CONTACT NUMBER: _____

(Cleaning, air conditioning, electrical work, and fuel lines supporting the STP's power supply)

14 Attachment 2, Example of Sticker and Tags



15 Attachment 3, Table 1 SS7 Stickers, Tags and Dummy Plugs

15.1.1.1.1.1	<u>Item</u> <u>Organizations</u>	<u>Inscription</u>	<u>Where</u> <u>Deployed</u>
Small "Critical Link" Sticker	STP Critical Link Call NPA-NXX-	DS0DP Plug In @ D4, Data Sets, DCS I/O Unit, Main Frame, etc	NOC/SCC, Toll Group, Link Audit Group
SS7 Wire Tag	STP Critical Link Call NPA-NXX- XXXX	DSX Plugs and Frame Area	NOC/SCC, Toll, Frame and/or Link Audit Group
DSX Type B Protector	CCS or SS7	DSX Frames – Type B	Toll and/or Link Audit Group
DSX Type C Protector	CCS or SS7	DSX Frames – Type C	Toll and/or Link Audit Group
Large Rectangular Sticker	STP Critical Link Call NPA-NXX- XXXX	Power Equipment Supporting the STP's: Batteries, Rectifiers, Converters, Inverters, Power Control Bays, Distribution Bays, Switches Breakers, Fuses, and STP Frame Blocks	NOC/SCC Power Group, Frame Techs, Link Audit Group

16 Attachment 4, Listing of Essential Equipment/Facilities

16.1 SS7 COMPONENT IDENTIFICATION LISTING

- A. HORIZONTAL & VERTICAL FRAME APPEARANCES
- B. DSX BAY APPEARANCES
- C. SMAS APPEARANCES
- D. PATCH PANEL APPEARANCES
- E. CARRIER EQUIPMENT LAOCATIONS (D5, D4, UNITS)
- F. MAIN FRAME CARRIER TERMINATION LOCATIONS
- G. FUSE BAY OR FUSE PANEL LOCATIONS
- H. CLOCK DISTRIBUTION EQUIPMENT
- I. FIBER TERMINALS AND MULTIPLEXERS
- J. SWITCHING AND TRANSMISSION CIRCUIT PACKS
- K. MODEMS
- L. ALL TIE CABLE APPEARANCES
- M. REPEATER SHELVES
- N. DSX – 1, DSX – 3 AND DSX – FIBER BAYS



ATIS-0300023

**Next Generation Interconnection Interoperability (NGIIF)
Reference Document**

**Part IV, Installation and Maintenance Responsibilities
X.75 Gateway Services**

Version 12.0



ATIS is the leading technical planning and standards development organization committed to the rapid development of global, market-driven standards for the information, entertainment and communications industry. More than 200 companies actively formulate standards in ATIS' Committees, covering issues including: IPTV, Cloud Services, Energy Efficiency, IP-Based and Wireless Technologies, Quality of Service, Billing and Operational Support, Emergency Services, Architectural Platforms and Emerging Networks. In addition, numerous Incubators, Focus and Exploratory Groups address evolving industry priorities including Smart Grid, Machine-to-Machine, Connected Vehicle, IP Downloadable Security, Policy Management and Network Optimization.

ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications' Sectors, and a member of the Inter-American Telecommunication Commission (CITEL). ATIS is accredited by the American National Standards Institute (ANSI). For more information, please visit www.atis.org.

Notice

This document was developed by the Alliance for Telecommunications Industry Solutions' (ATIS) sponsored Next Generation Interconnection Interoperability Forum (NGIIF). The NGIIF addresses next-generation network interconnection and interoperability issues associated with emerging technologies. Specifically, it develops operational procedures which involve the network aspects of architecture, disaster preparedness, installation, maintenance, management, reliability, routing, security, and testing between network operators. In addition, the NGIIF addresses issues which impact the interconnection of existing and next generation networks and facilitate the transition to emerging technologies. All changes to this document shall be made through the NGIIF issue resolution process.

Note Regarding Previous Versions

The NIIF Reference Document was formerly known as the Network Operations Forum (NOF) Reference Document. The NOF Reference Document was published and maintained by Bellcore. The last version of the NOF Reference Document is Issue 13.

Disclaimer and Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

ATIS-0300023, NGIIF Reference Document, Part IV, Installation and Maintenance Responsibilities X.75 Gateway Services, Formerly NIIF 5010

The NGIIF Reference Document, Part IV, Installation and Maintenance Responsibilities X.75 Gateway Services is an ATIS standard developed by the NGIIF.

Published by

Alliance for Telecommunications Industry Solutions

1200 G Street, NW, Suite 500

Washington, DC 20005

Copyright © 2011 by Alliance for Telecommunications Industry Solutions

All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < <http://www.atis.org> >.

Printed in the United States of America.

INSTALLATION AND MAINTENANCE RESPONSIBILITIES

X.75 GATEWAY SERVICES

TABLE OF CONTENTS

1	GENERAL.....	4
2	RESPONSIBILITIES.....	4
2.1	ACCESS SERVICE CUSTOMERS.....	4
2.2	ACCESS SERVICE PROVIDERS	5
3	INSTALLATION OF X.75 GATEWAY	5
3.1	PRE-SERVICE TESTING OF X.75 GATEWAY.....	6
3.2	COOPERATIVE ACCEPTANCE TESTING.....	6
3.3	COMPLETION REPORTING	6
3.4	DISCONNECTION OF SERVICE.....	6
3.5	REARRANGEMENTS.....	6
3.6	CHANGE ORDERS.....	6
3.7	ROUTINE MAINTENANCE ACTIVITY.....	6
4	MAINTENANCE.....	7
4.1	TROUBLE REPORTING	7
4.2	SECTIONALIZATION AND REPAIR	7
4.3	CERTIFICATION TESTS	8
4.3.1	<i>Trouble cleared - No Dispatch Required</i>	<i>8</i>
4.3.2	<i>Trouble cleared - Dispatch Required.....</i>	<i>8</i>
4.4	TROUBLE TICKET STATUS	9
5	END-TO-END AND INTERCARRIER TESTING.....	9
6	ESCALATIONS.....	9

1 General

This document has been developed to provide a guideline for the operations personnel of the Access Service Providers (ASP) and Access Service Customers (ASC) to prepare procedures for the installation and maintenance of X.75 Gateway Services. The contents of this document are generic. Specific operational procedures shall be covered in bilateral agreements between ASP(s) and ASC(s). This document does not replace nor supersede tariffs, contracts or any other legally binding documents.

Whenever this document is reissued, the reason for reissue shall be listed in this paragraph.

In addition to other operational and technical agreements made at the Network Interconnection Interoperability Forum (NGIIF), this document is being reissued to incorporate the following changes:

- Standardization of the Issue Number and publication date to agree with other sections of the NGIIF Reference Document.

2 Responsibilities

2.1 Access Service Customers

The ASC has the overall installation and maintenance responsibility for the X.75 Gateway Service it provides and is responsible for the coordination of cooperative testing of these Gateway Services.

The ASC:

- Provides trained personnel.
- Provides the ASP with a trouble reporting number that is staffed 24 hours a day, 7 days a week.
- Provides X.75 access to testlines where available.
- Coordinates test equipment compatibility with the ASP where possible, this test equipment should conform with established standards (e.g., CCITT Series O).
- Maintains complete and accurate installation and repair records of the X.75 Gateway Service.
- Accepts trouble reports from its customers and the ASP.
- Tests cooperatively, if necessary, with the ASP Data Network Control Center to further identify and clear a trouble when the trouble has been sectionalized to the ASP.
- Sectionalizes to determine if the reported trouble is in its facility or service, or in the ASP provided service.
- Coordinates with the ASP to ensure that X.75 Gateway Service is installed in accordance with the service requested by the ASC.
- Advises the ASP Data Network Control Center when there is an ASC facility failure affecting the X.75 Gateway Service.
- Except under emergency conditions consults with the ASP before making any changes which would affect the service. All reasonable efforts should be made to utilize established maintenance windows for route maintenance activities.
- Provides ASP personnel access to the POT when required.
- Notifies the appropriate Interexchange Customer Service Center (ICSC) or other designated center when there are any changes affecting X.75 Gateway Service, facility requests, including due date changes.

2.2 Access Service Providers

The ASP has the overall installation and maintenance responsibility for the X.75 Gateway Services it provides. In addition, the ASP shall work cooperatively with the ASC in the testing of these services.

The ASP:

- Provides trained personnel.
- Notifies the ASC of due date jeopardies in a timely manner.
- Provides the ASC with a trouble reporting number that is staffed 24 hours a day, 7 days a week.
- Provides X.75 access to testlines where available.
- Ensures test equipment compatibility with the ASC where possible, this test equipment should conform with established standards (e.g., CCITT Series O).
- Maintains complete and accurate installation and repair records of its own customers and the X.75 Gateway.
- Accepts trouble reports from the ASC or End User and provides status upon request.
- Cooperates with the ASC in testing to sectionalize and clear troubles.
- Sectionalizes to determine if the reported/detected trouble is in its facility or service, or in the ASC provided service.
- Cooperates with the ASC to ensure that X.75 Gateway services are installed in accordance with the service requested by the ASC.
- Advises the ASC Data Network Control Center when there is an ASP furnished X.75 Gateway facility failure or ASP equipment failure.
- Except under emergency conditions consults with the ASC before making any changes which would affect the service. All reasonable efforts should be made to utilize established maintenance windows for route maintenance activities.
- Initiates corrective action on service affecting conditions affecting X.75 Gateway Service and if appropriate reports to the ASC the trouble noted and action taken.
- Establishes local service restoral objectives and provides them to the ASC upon request.
- Performs cooperative maintenance testing with the ASC when requested.
- Designates a Data Network Control Center for the X.75 Gateway Service furnished to an ASC.

3 Installation of X.75 Gateway

Installation, as used in this document, means that portion of the total provisioning process which starts when an order is received by the Data Network Control Center and includes new connect, change, and disconnect activities.

3.1 Pre-Service Testing of X.75 Gateway

The ASP DNCC should ensure the following before contacting the ASC to perform cooperative acceptance tests:

- That pre-service tests have been performed and the service is ready for acceptance tests.
- That all pre-service test results have been recorded.
- That the ASP portion of the X.75 Gateway Service has been installed correctly.

ASC personnel or their designate may be invited to participate in the pre-service testing activity.

3.2 Cooperative Acceptance Testing

Upon completion of the pre-service tests, the ASP DNCC shall contact the ASC and advise that the ASP portion of the X.75 Gateway service is ready for acceptance testing. The ASC's DNCC shall coordinate all normal and additional acceptance testing. Test equipment compatibility should be verified at this time. The ASC is not obligated to accept the service prior to the due date. The ASC is also not obligated to accept the service without successful acceptance test completion.

Basic acceptance test requirements may be found in the X.75 Gateway Service, Technical References tariffs or bilateral agreements.

3.3 Completion Reporting

Upon acceptance of the ASP access service by the ASC, the ASP DNCC shall record the name of the ASC representative and the date the service is accepted.

3.4 Disconnection of Service

Disconnect procedures shall be in accordance with ASP and ASC developed practices or as stated in the applicable X.75 Gateway tariff, or bilateral agreements.

3.5 Rearrangements

A rearrangement as described in this document is a coordinated activity initiated by either the ASP or the ASC which will usually be transparent to the end users and will not change the operation of virtual calls. In the rearrangement process, circuit releases, rearrangement timing, and acceptance testing shall be negotiated on an individual case basis (ICB).

3.6 Change Orders

Change orders cover any changes in the design or operation of an existing X.75 Gateway Service administered through the ICSC or equivalent center procedures.

3.7 Routine Maintenance Activity

- It is the recommendation of the NGIIF that all routine maintenance and scheduled work activities be performed during hours of minimum traffic (e.g., during an 11:00 pm to 5:00 am "maintenance window") so that any inadvertent failure impacts the least number of customers.

- At a minimum, high risk, potentially service affecting maintenance and growth procedures should be scheduled during weekend and off-hours. The overall methods, procedures and scheduling of these work activities should be reviewed by a second tier maintenance organization.
- The activities that may affect other network service providers must be coordinated, which includes both intra- and inter-carrier networks. (See NGIIF Reference Document, Section III, Installation and Maintenance - SS7).
- Non Scheduled Work Activity. If customer service is being impacted, the minimum work activity will occur to restore the system to a stable performance state. Complete system recovery activity will be scheduled for the next maintenance window period.

4 Maintenance

The ASC is responsible for performing all necessary tests in its service to determine the nature of the trouble detected or reported by its customer or an ASP. If the trouble is sectionalized to an ASP provided service, the ASC shall report the trouble to the appropriate ASP DNCC. Likewise the ASP is responsible for performing all necessary tests to determine the nature of the trouble detected, or reported by its customers. If the trouble is sectionalized to an ASC, the ASP will report the trouble to the appropriate ASC's point of contact.

The ASP shall accept trouble reports from the ASC, sectionalized to the ASP's network. Likewise, the ASC shall accept from the ASP trouble reports sectionalized to the ASC's network. The ASP and ASC shall test cooperatively and/or independently, as required to sectionalize the trouble.

4.1 Trouble Reporting

The following is the type of information which should be exchanged at the time of the trouble referral.

- Circuit identification number.
- Date and time of trouble referral.
- Nature of the trouble and any other information that may be of assistance to the ASP Control Office.
- The name or initials and the telephone number of the person referring the trouble.
- Trouble ticket number(s) or equivalent and the name or initials of the person accepting the trouble.

4.2 Sectionalization and Repair

Trouble sectionalization may involve cooperative testing by the ASC and ASP(s) which shall be provided when requested. The carrier requesting cooperative testing assumes coordination responsibility.

Communication may also be necessary on services that involve an ASC, its designated agent, and an ASP. In these situations the cooperation of all three organizations may be necessary to expedite trouble clearance. When it is necessary for communication between the ASC and ASP, it is required that this contact may be made through the designated agent.

The ASC may not rearrange, move, disconnect, remove or attempt to repair any equipment or facilities provided by the ASP.

4.3 Certification Tests

After each trouble has been cleared the ASP/ASC shall contact the other to advise that the trouble has been cleared and the nature of the trouble found and action taken.

Requests for verification tests shall be handled as follows:

4.3.1 Trouble cleared - No Dispatch Required

The ASP will not normally dispatch a technician to make verification tests when a trouble has been cleared without dispatching. When a trouble has been corrected, the ASP DNCC will assure itself that the service is functioning properly by performing cooperative testing on the X.75 Gateway Service. If the ASC insists on a verification test and it requires an ASP dispatch, the ASP DNCC should advise the ASC that a charge may be made for the dispatch if the ASP service and facilities meet(s) requirements.

4.3.2 Trouble cleared - Dispatch Required

The ASC may request verification of any parameter specified for the type of service provided when a trouble has been reported and a dispatch is required. The ASP DNCC, prior to dispatch, should determine the nature of the requested tests; however, it is expected that such verification tests will be related to the trouble found. This will enable the technician to be equipped with the necessary test equipment.

If the tests requested by the ASC are other than those required for verification of the maintenance performance and are billable, the ASP DNCC should notify the ASC that the time required to perform these additional tests will be billed to the ASC.

When repair verification tests identify additional trouble that was not apparent due to the nature of the original trouble, clearance activity shall continue until the service is restored.

When trouble tickets are being closed out between an ASP/ASC, whether they are using a mechanized system or a verbal notification, the company clearing the trouble should furnish the disposition, and the following information shall be provided:

The ASC/ASP should agree to provide the following information when closing a mutual trouble report:

- Circuit ID/telephone number
- Trouble Ticket Number (ASC/ASP number)
- Trouble Disposition (e.g., bad cable)
- Resolution details (e.g., cut to new cable)
- ASC will inform ASP if this trouble is measured.
- Referral time, returned time, no access time.
- If a trouble ticket results in a service charge, the ASP will provide this information to the ASC

When there is a disagreement on the disposition, the parties engaged in the dispute shall document their respective positions, and the names of the individuals engaged in the dispute for audit purposes. Escalations if necessary shall be in accordance with identified procedures.

If after a trouble has been cleared and either the ASP or ASC wishes to change the Disposition, such changes shall be negotiated.

4.4 Trouble Ticket Status

The ASC/ASP receiving the initial trouble referral shall provide a status on the disposition of that referral based on local agreements negotiated at the time of referral or requested on an individual case basis.

Subsequent to the initial status report on the disposition of the trouble ticket, periodic status's shall occur based on the following criteria:

- When the trouble has been isolated
- When there is a significant change in the status of the trouble.
- The negotiated status interval has expired.

Where mechanized trouble notification is utilized, the receiving company shall status their appropriate systems based on paragraphs A and B. In addition, it shall be the responsibility of the company issuing the trouble ticket to poll the mechanized status system for the status of the trouble ticket.

Escalations if necessary shall be in accordance with identified procedures.

5 End-to-End and Intercarrier Testing

Networks comprising ASP and ASC services may experience trouble conditions which cannot be isolated by each carrier individually testing and maintaining its own services. Although the portions provided by each ASC and each ASP apparently perform properly, a trouble may only be identifiable on an end-to-end service. In such cases, the ASC may require coordinated testing. It is the responsibility of the ASC to coordinate intercarrier and/or end-to-end testing with each sectional provider (i.e., other ASCs, ASPs).

6 ESCALATIONS

Escalation is a means of bringing problems to the attention of individuals responsible for, or having appropriate authority to expedite corrective action.

Each ASP and ASC shall establish the necessary procedures to ensure timely escalation of problems to successive levels of management. These procedures should address the provision of status reports to the other carrier regarding service restoral activities. Contacts for the resolution of technical problems should also be included in the escalation process.



ATIS-0300024

**Next Generation Interconnection Interoperability (NGIIF)
Reference Document**

Part V, Test Line Guidelines

Version 13.0



As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-IP transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

Notice

This document was developed by the Alliance for Telecommunications Industry Solutions' (ATIS) sponsored Next Generation Interconnection Interoperability Forum (NGIIF). The NGIIF addresses next-generation network interconnection and interoperability issues associated with emerging technologies. Specifically, it develops operational procedures which involve the network aspects of architecture, disaster preparedness, installation, maintenance, management, reliability, routing, security, and testing between network operators. In addition, the NGIIF addresses issues which impact the interconnection of existing and next generation networks and facilitate the transition to emerging technologies. All changes to this document shall be made through the NGIIF issue resolution process.

Note Regarding Previous Versions

The NIIF Reference Document was formerly known as the Network Operations Forum (NOF) Reference Document. The NOF Reference Document was published and maintained by Bellcore. The last version of the NOF Reference Document is Issue 13.

Disclaimer and Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [http://www.atis.org/legal/patentinfo.asp] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

Trademark Acknowledgements

iconectiv®, Telcordia®, and Common Language® are registered trademarks and CLCI™, CLLI™, LERG™ Routing Guide and TPM™ Data Source are trademarks and the Intellectual Property of Telcordia Technologies, Inc. dba as iconectiv.

ATIS-0300024, NGIIF Reference Document, Part V, Test Line Guidelines (formerly NIIF 5020)

The NGIIF Reference Document, Part V, Test Line Guidelines, is an ATIS standard developed by the NGIIF.

Published by

Alliance for Telecommunications Industry Solutions

1200 G Street, NW, Suite 500

Washington, DC 20005

Copyright © 2018 by Alliance for Telecommunications Industry Solutions

All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < <http://www.atis.org> >.

Printed in the United States of America.

Table of Contents

1	General	1
2	Test Line Access.....	1
3	Lineside (Call-through/Routing Testing/Service Provider Verification)	3
3.1	Service Provider Verification	3
3.2	Call-Through/Routing Testing	3
4	Testing Through an Access Tandem	3
5	9YY NXX, NPA/NXX, Toll Free, and International Call-Through Testing	3
5.1	Testing NPA/NXX or NPA/NXX-X	3
5.1.1	New NPA/NXX	4
5.1.2	New NPA/NXX-X in Thousands Block Pooling Situations.....	4
5.1.3	NXXs Affected by NPA Relief Activity	4
5.2	Testing NPA/NXX	4
5.2.1	New NPA/NXX	4
5.2.2	NXXs Affected by NPA Relief Activity, Switch Change, Switch Homing Arrangements	4
5.2.3	Migration of NXX Code(s).....	4
5.2.4	Changing a Tandem Association with an End Office Switch.....	5
5.3	Testing Toll Free	5
5.4	Testing International Direct Distance Dialing (IDDD)	5
5.4.1	New IDDD Number Range	5
5.4.2	New IDDD Routing	5
6	Test Line Directory	6
7	Bibliography	6

1 General

The purpose of this document is to provide exchange, interexchange, and international carriers with guidelines for the deployment of test lines and assignment of test line numbers.

Specific local operational procedures should be covered in documentation provided by the Carriers. Additional copies of this document for individual company distribution should be obtained by contacting your company's Next Generation Interconnection Interoperability Forum (NGIIF) representative.

This document does not replace or supersede tariffs, contracts, or any other legally binding documents. Availability of test lines, specific procedures, and numbering plans may require individual company documentation or negotiation between the companies involved.

The test lines and test line numbers contained herein are in accordance with ATIS-0300207, *Operations, Administration, Maintenance, and Provisioning (OAM&P) – Terminating Test Line Access and Capabilities*. This Standard contains further information and descriptions of test lines.

2 Test Line Access

Access Service Customers (ASCs) will be provided access to Access Service Provider (ASP) terminating test lines in the End Offices and in the Access Tandems. ASPs should be provided with access to ASC terminating test lines.

The following test lines, where applicable, should be provided and their access numbers exchanged by the ASCs and ASPs:

- 100 Type Test Line
- 101 Type Test Line
- 102 Type Test Line
- 103 Type Test Line
- 104 Type Test Line
- Non-Synchronous Test Line
- Synchronous Test Line
- 105 Type Test Line
- 107 Type Test Line
- 108 Type Test Line
- 109 Type Test Line
- Short Circuit
- Open Circuit
- Analog Loop Around Test Lines.

The following test line numbers are recommended to be used for ASP trunk side access to ASC test lines. Information on ASC/ASP test line access can be obtained from each company's Test Line Coordinator. Company contact information can be found in the NGIIF Service Provider Contact Directory.¹

The recommended outpulsing and numbering for ASC test lines is as follows:

TEST LINE

100 TL

101 TL

7 DIGIT TEST LINE ACCESS

KP - 958-1100 - ST

KP - 958-1101 - ST

¹ The Service Provider Contact Directory and instructions for gaining access to the Directory can be accessed on ATIS's website: http://www.atis.org/01_committ_forums/NGIIF/contact_directories.asp.

102 TL	KP - 958-1102 - ST
103 TL	KP - 958-1103 - ST
104 TL	KP - 958-1104 - ST
105 TL	KP - 958-1105 - ST
107 TL	KP - 958-1107 - ST
108 TL	KP - 958-1108 - ST
60ipm/Echo Canceller109 TL	KP - 958-1109 - ST
100 TL	KP - 100 - ST
101 TL	KP - 101 - ST
102 TL	KP - 102 - ST
103 TL	KP - 103 - ST
104 TL	KP - 104 - ST
105 TL	KP - 105 - ST
107 TL	KP - 107 - ST
108 TL	KP - 108 - ST
60ipm/Echo Canceller	KP - 109 – ST

EMBEDDED AT&T

TEST LINE ACCESS

100 TL	KP - 959-1000 - ST
101 TL	KP - 959-1010 - ST
102 TL	KP - 959-1020 - ST
103 TL	KP - 959-1030 - ST
104 TL	KP - 959-1040 - ST
105 TL	KP - 959-1050 - ST
107 TL	KP - 959-1070 - ST
108 TL	KP - 959-1080 - ST
Echo Canceller	KP - 959-1090 - ST
100 TL	KP - 100 - ST
101 TL	KP - 101 - ST
102 TL	KP - 102 - ST
103 TL	KP - 103 - ST
104 TL	KP - 104 - ST

105 TL	KP - 105 - ST
107 TL	KP - 107 - ST
108 TL	KP - 108 - ST
Echo Cancellor	KP - 109 - ST

NOTE: ASC Switches should recognize 10 or 95 ANI information digit as incoming test calls and not to expect ANI.

When testing trunks terminating into end offices with local and tandem capabilities, verification of the proper switch pad must be taken into account. Testing of switch pad operation may be done in two manners:

- The ASP will (through manual or software control) operate the switch pad for proper configuration (local/tandem).
- The ASP will make available the test line numbers for tandem and/or local operation, so the ASC can verify the proper designed loss of the trunk.

When ASP switching machines detect a Machine Detected Interoffice Irregularity (MDII) on ASP-ASC FGD service, test line number access is required for efficient and economical circuit isolation and repair. With the installation of such test access, MDII's may be tested from the originating switch location without assistance from the terminating switch location.

3 Lineside (Call-through/Routing Testing/Service Provider Verification)

3.1 Service Provider Verification

When it is necessary for an ASP to perform a SP verification, the recommended internal only numbers to use to make the verification calls are 700-555-4141 for interLATA pre-subscription validation or (HNPA) 700-4141 for intraLATA toll pre-subscription validation and (101XXXX) 1-700-555-4141 for alternate carrier validation. These internal only calls will verify access to the current service provider and will not result in end-user billing.

3.2 Call-Through/Routing Testing

To facilitate call-through tests, the Automatic Number Identification (ANI) of the line to be used in making the test call may be needed to verify routing, if requested by the ASC. ANI should be provided by the ASP, prior to the call-through test via local agreements. ASC response to a call-through test should contain the ASC name and should be a "Barge in" type of announcement.

4 Testing Through an Access Tandem

Testing from an End Office through an Access Tandem to an ASC may be impossible due to Access Tandem test line number screening. It is recommended that the ASCs provide access to terminating test lines via the 700 Service Access Code (SAC), where available e.g., (101XXXX) 1-700-958-1102 or (101XXXX) 1-700-959-1020.

5 9YY NXX, NPA/NXX, Toll Free, and International Call-Through Testing

5.1 Testing NPA/NXX or NPA/NXX-X

NOTE: Additional information related to all other aspects of NPX-NXX Code Opening can be found in ATIS-0300032, *Part X, Interconnection Between LECS Operations Handbook – Local Interconnection Service Arrangement* and ATIS-0300010, *NGIIF*

5.1.1 New NPA/NXX

The company opening a new NXX shall establish a working test number for call through purposes. The test number shall be established for a minimum period of 180 days.

5.1.2 New NPA/NXX-X in Thousands Block Pooling Situations

The above testing rules also apply for a Code Holder opening an NPA/NXX-X block for the first time in a new NPA/NXX.

NPA/NXX-X Code reallocations occur after a code has already been opened and established, generally have viable working numbers at the time of reallocation and would not typically require retesting.

5.1.3 NXXs Affected by NPA Relief Activity

The company moving an NXX or NXX-X to another or a new NPA or rehomeing an NXX or NXX-X, shall have a test number established for the purpose of translation and billing validation call through testing. The test number shall be established for a minimum period of 180 days.

Where possible the preferred termination for these test numbers shall be a recorded announcement that identifies the terminating NPA/NXX or NPA/NXX-X.

5.2 Testing NPA/NXX

All communications companies (wireline, cable, VoIP, wireless etc.) applying to the NANPA administrator and receiving a new NPA/NXX or Thousands Block(s) are expected to follow testing procedures as Code Holder.

5.2.1 New NPA/NXX

The company opening a new NXX shall establish a working test number for call through purposes. The test number shall be established for a minimum period of 180 days.

5.2.2 NXXs Affected by NPA Relief Activity, Switch Change, Switch Homing Arrangements

The company moving an NXX to another or a new NPA or rehomeing (migrating, transferring or moving) an NXX to a different switch or a switch rehome to a different tandem shall have a test number established for the purpose of translation and billing validation call through testing. The test number shall be established for a minimum period of 180 days.

5.2.3 Migration of NXX Code(s)

Code migration is transferring a code from one switch to another and/or from one OCN to another and/or one service provider to another and should be a coordinated project. Testing and testing timeframes would be determined by the interconnected project partners and does not need industry testing participation. A test line number should be published in the LERG™ Routing Guide for any company choosing to participate in testing NXX migration scenarios may include, but are not limited to, the following:

- Migrating all NXX codes from a switch to another switch/same or different tandem
- Migrating one or more but not all NXX codes from a switch to another switch (OCN of the switch may or may not stay the same)

- Type 1 to Type 2 wireless code migration (OCN of the switch changes).

When the “A” record is moving from one switch to another switch, then the test number and test response field on the NXD screen should be populated with the appropriate test number and test response.

5.2.4 Changing a Tandem Association with an End Office Switch

For tandem rehome activity the test number shall remain in effect until the tandem rehome has been completed. However, this situation should be a coordinated project. Testing and testing timeframes shall be determined by the interconnected project partners and does not need industry testing participation.

For new NPA-NXX codes where required trunking is in place at least 20 days prior to the LERG Routing Guide effective date, validate that all translations work is complete five (5) calendar days prior to the date identified in the LERG as the effective date.

Where possible the preferred termination for these test numbers shall be a recorded announcement that identifies the terminating NPA/NXX. For rehome activity, when a recorded announcement is not possible, the test number may terminate to a milliwatt tone response.

5.3 Testing Toll Free

Each Toll Free Service Provider should provide Toll Free test numbers within the reserved range (8NN-250-0000 to 8NN-250-1499).

5.4 Testing International Direct Distance Dialing (IDDD)

When a new IDDD number range is opened, or when new routing is applied to an IDDD number range, testing may be performed by Local Exchange Carriers (LECs), Interexchange Carriers (IXCs), and International Carriers.

5.4.1 New IDDD Number Range

The International Carrier shall identify working IDDD numbers in the new number range for use in call-through testing. A LEC that chooses to participate in the call-through testing shall check that it does not screen out IDDD calls to numbers in the new number range. An IXC that chooses to participate in the call-through testing shall verify that it appropriately routes IDDD calls to numbers in the new number range.

Where possible the preferred termination for IDDD call-through testing via the International Carrier shall be a recorded announcement that identifies the called number.

5.4.2 New IDDD Routing

The International Carrier shall identify working IDDD numbers that have new routing for use in call-through testing. Typically, initial digits of an IDDD number are analyzed to determine the appropriate routing for an IDDD call to that number.

Call-through testing verifies that, for IDDD calls to the numbers with new routing, such calls are being routed to the correct end point.

Call-through testing may also be used to demonstrate that, for IDDD numbers in nearby number ranges for which routing is unchanged, such calls are being routed to the correct end point.

Where possible the preferred termination for IDDD call-through testing via the International Carrier shall be a recorded announcement that identifies the called number.

6 Test Line Directory

A Test Line Directory(ies) should be developed, maintained and distributed in accordance with ATIS-0300025, *Next Generation Interconnection Interoperability (NGIIF) Reference Document: Part V, Test Line Guidelines Attachment A Test Line Directory Dictionary*.

The NGIIF recommends that each carrier maintain a current directory of test line information (See Figure 1 of ATIS-0300025). This directory should be made available via electronic file transfer/download (e.g., secure FTP, website, email).

In the event that a published test line number is not working, the trouble should be referred to the test line company's appropriate trouble reporting center.

In the event that a test line number has not been established, contact should be made to the appropriate company's test line coordinator. Trouble Reporting/Repair Contact Information is supplied by the industry and included in the Service Provider Contact Directory. Additions, deletions, or changes should be submitted to ngiif-admin@atis.org.

Test Lines have the potential for fraud and abuse. Legitimate users must make reasonable effort to control distribution of test line numbers to those who have the need for the information.

7 Bibliography

The following standards contain provisions which, through reference in this text, constitute provisions of this Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

- ATIS-0300207, *Operations, Administration, Maintenance, and Provisioning (OAM&P) – Terminating Test Line Access and Capabilities*²
- ATIS-0300025, *Next Generation Interconnection Interoperability (NGIIF) Reference Document: Part V, Test Line Guidelines Attachment A Test Line Directory Dictionary*³
- ATIS-0300010, *Next Generation Interconnection Interoperability (NGIIF) Reference Document: Part II, Installation and Maintenance Responsibilities Switched Access Services Feature Group B, C, and D*⁴

² This document is available from ATIS at: < <https://www.atis.org/docstore/product.aspx?id=24984> >.

³ This document is available from ATIS at: < <https://www.atis.org/docstore/product.aspx?id=26059> >.

⁴ This document is available from ATIS at: < <https://www.atis.org/docstore/product.aspx?id=26044> >.



ATIS-0300025

**Next Generation Interconnection Interoperability (NGIIF)
Reference Document**

Part V, Test Line Guidelines

**Attachment A
Test Line Directory Dictionary**

Version 12.0



ATIS is the leading technical planning and standards development organization committed to the rapid development of global, market-driven standards for the information, entertainment and communications industry. More than 200 companies actively formulate standards in ATIS' Committees, covering issues including: IPTV, Cloud Services, Energy Efficiency, IP-Based and Wireless Technologies, Quality of Service, Billing and Operational Support, Emergency Services, Architectural Platforms and Emerging Networks. In addition, numerous Incubators, Focus and Exploratory Groups address evolving industry priorities including Smart Grid, Machine-to-Machine, Connected Vehicle, IP Downloadable Security, Policy Management and Network Optimization.

ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications' Sectors, and a member of the Inter-American Telecommunication Commission (CITEL). ATIS is accredited by the American National Standards Institute (ANSI). For more information, please visit www.atis.org.

Notice

This document was developed by the Alliance for Telecommunications Industry Solutions' (ATIS) sponsored Next Generation Interconnection Interoperability Forum (NGIIF). The NGIIF addresses next-generation network interconnection and interoperability issues associated with emerging technologies. Specifically, it develops operational procedures which involve the network aspects of architecture, disaster preparedness, installation, maintenance, management, reliability, routing, security, and testing between network operators. In addition, the NGIIF addresses issues which impact the interconnection of existing and next generation networks and facilitate the transition to emerging technologies. All changes to this document shall be made through the NGIIF issue resolution process.

Note Regarding Previous Versions

The NIIF Reference Document was formerly known as the Network Operations Forum (NOF) Reference Document. The NOF Reference Document was published and maintained by Bellcore. The last version of the NOF Reference Document is Issue 13.

Disclaimer and Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

ATIS-0300025, NGIIF Reference Document, Part V, Test Line Guidelines, Attachment A, Test Line Directory Dictionary, Formerly NIIF 5021

The NGIIF Reference Document, Part V, Test Line Guidelines, Attachment A, Test Line Directory Dictionary, is an ATIS standard developed by the NGIIF.

Published by

Alliance for Telecommunications Industry Solutions

1200 G Street, NW, Suite 500

Washington, DC 20005

Copyright © 2011 by Alliance for Telecommunications Industry Solutions

All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < <http://www.atis.org> >.

Printed in the United States of America.

TEST LINE DIRECTORY DICTIONARY

Table of Contents

1	TEST LINE DIRECTORY DICTIONARY	4
1.1	NPA - NUMBERING PLAN AREA CODE	4
1.2	NXX - CENTRAL OFFICE CODE	4
1.3	OFFICE LOCATION	4
1.4	100 TYPE TEST LINE - QUIET TERMINATION	4
1.5	101 TYPE TEST LINE - COMMUNICATION.....	4
1.6	102 TYPE TEST LINE - MILLIWATT	5
1.7	104 TYPE TEST LINE - TRANSMISSION MEASURING & NOISE CHECKING	5
1.8	105 TYPE TEST LINE - AUTOMATIC TRANSMISSION MEASURING	5
1.9	107 TYPE TEST LINE - DATA TRANSMISSION TEST LINE	5
1.10	108 TYPE TEST LINE - NON-INVERTING LOOPBACK	5
1.11	109 TYPE TEST LINE - ECHO CANCELLER TESTING	6
1.12	606 TYPE TEST LINE - INVERTING LOOPBACK.....	6
1.13	103 TYPE TEST LINE - SIGNAL-SUPERVISORY TESTING.....	6
1.14	ANALOG AROUND TEST LINE	6
1.15	SIGNAL-SUPERVISORY TESTING/SYNCHRONOUS TEST LINE (NO 10X CODE ASSIGNED)	7
1.16	NONSYNCHRONOUS TEST LINE.....	7
1.17	SHORT CIRCUIT TEST LINE	7
1.18	OPEN CIRCUIT TEST LINE	7
1.19	COMPANY NAME	8
2	TEST LINE NUMBERS FOR NPA 209/415.....	1

1 Test Line Directory Dictionary

1.1 NPA - Numbering Plan Area Code

Identifies a geographical area and permits calls to be routed to the proper destination.

USAGE: This field is required.

NOTE 1: The NPA code, combined with "the Central Office Unit Code (COC)", is the destination code reported.

DATA CHARACTERISTICS: 3 numeric characters

EXAMPLE: 209

1.2 NXX - Central Office Code

Identifies, within a NPA, an exchange telephone switching entity used for access to tandems and testboards.

USAGE: This field is required.

DATA CHARACTERISTICS: 3 numeric characters

EXAMPLE: 276

1.3 Office Location

Identifies the COMMON LANGUAGE\rg Code of the switching entities for the EC providing the service.

USAGE: This field is required.

DATA CHARACTERISTICS: 11 alpha/numeric characters

EXAMPLE: FRSNCA11CG1; SNFCCA1101T

1.4 100 Type Test Line - Quiet Termination

Provides a termination consisting of 900 or 600 ohms (depending on office impedance) in series with a 2.16 MF capacitor.

USAGE: This field is required.

DATA CHARACTERISTICS: 8 characters; 3 to 7 numeric, 1 delimiter (when 7 numeric used) 1

EXAMPLE: ____100; 95y-XXXX; NXX-XXXX

1.5 101 Type Test Line - Communication

The number assigned to this terminating test as specified in the referenced draft standard.

USAGE: This field is required.

DATA CHARACTERISTICS: 8 characters; 7 numeric, 1 delimiter

EXAMPLE: 765-4321

1.6 102 Type Test Line - Milliwatt

Provides a tone for 1-way loss measurements.

USAGE: This field is required.

DATA CHARACTERISTICS: 8 characters; 3 to 7 numeric, 1 delimiter (when 7 numeric used)

EXAMPLE: _____102; 95y-XXXX; NXX-XXXX

1.7 104 Type Test Line - Transmission Measuring & Noise Checking

The number assigned to this terminating test as specified in the referenced draft standard.

USAGE: This field is required.

DATA CHARACTERISTICS: 8 characters; 7 numeric, 1 delimiter

EXAMPLE: 543-2109

1.8 105 Type Test Line - Automatic Transmission Measuring

Provides far-end access to a responder and permits 2-way loss and noise measurements to be made on trunks from a near-end office equipped with a Remote Office Test Line (ROTL) and responder or other suitable control device. 105-type test lines may be associated with one common responder.

USAGE: This field is required

DATA CHARACTERISTICS: 8 characters; 3 to 7 numeric, 1 delimiter (when 7 numeric used)

EXAMPLE: _____105; 95y-XXXX; NXX-XXXX

1.9 107 Type Test Line - Data Transmission Test Line

Identifies a connection to a signal source that provides test signals for 1 way testing of data and voice transmission parameters. The test line provides a Peak-to-Average Ration (P/AR) signal, gain slope frequencies, quiet termination, and intermodulation-distortion test signals. It also allows measurement of return loss, frequency shift, phase jitter, C-notched noise, impulse noise, gain hits, phase hits, and dropouts.

USAGE: This field is required.

DATA CHARACTERISTICS: 8 characters; 3 to 7 numeric, 1 delimiter (when 7 numeric used)

EXAMPLE: _____107; 95y-XXXX; NXX-XXXX

1.10 108 Type Test Line - Non-Inverting Loopback

Provides for digital testing capabilities between digital exchanges and/or digital PBX's.

USAGE: This field is required.

DATA CHARACTERISTICS: 8 characters; 3 to 7 numeric, 1 delimiter (when 7 numeric used)

EXAMPLE: _____108; 95y-XXXX; NXX-XXXX

1.11 109 Type Test Line - Echo Canceller Testing

Provides loopback arrangements for in-service testing of far-end echo cancellers.

USAGE: This field is required.

DATA CHARACTERISTICS: 8 characters; 3 to 7 numeric, 1 delimiter (when 7 numeric used)

EXAMPLE: _____109; 95y-XXXX; NXX-XXXX

1.12 606 Type Test Line - Inverting Loopback

The digital loopback/complement test line provides operation and digital testing capability for switched digital trunks.

USAGE: This field is required.

NOTE 1: This test line used for diagnostic (routine and demand) tests to digital switching system trunks.

DATA CHARACTERISTICS: 8 characters; 3 to 7 numeric, 1 delimiter (when 7 numeric used)

EXAMPLE: 959-6060; NXX-XXXX

1.13 103 Type Test Line - Signal-Supervisory Testing

Provides a connection to a supervisory and signaling test circuit for overall testing of these features on intertoll trunks equipped with ring forward (re-ring) features that can be reached by an automatic trunk test frame or by dialing manually.

USAGE: This field is required.

DATA CHARACTERISTICS: 3 numeric characters

EXAMPLE: 103

1.14 AnaLog Around Test Line

Provides for the interconnection of two lines or trunks to facilitate two-way loss measurements from the distant end.

USAGE: This field is required.

NOTE 1: The Loop Around Test Line is used in conjunction with a line or trunk of known loss, selected as a reference.

DATA CHARACTERISTICS: Two 8 characters; 7 numeric, 1 delimiter

EXAMPLE: 321-9926, 321-9927

1.15 Signal-Supervisory Testing/Synchronous Test Line (No 10X Code Assigned)

Indicates a test line number which provides access to a synchronous test line.

USAGE: This field is required.

NOTE 1: Synchronous test lines are required for offices where ringing, tripping and supervisory features are in the incoming trunk relay equipment. Marginal tests of the supervisory and tripping functions are provided.

DATA CHARACTERISTICS: 8 characters; 7 numeric, 1 delimiter

EXAMPLE: 95y-XXXX; NXX-XXXX

1.16 Nonsynchronous Test Line

Provides an operational test which is not as complete as the synchronous test but can be made more rapidly.

USAGE: This field is required.

DATA CHARACTERISTICS: 8 characters; 7 numeric, 1 delimiter

EXAMPLE: NXX-XXXX

1.17 Short Circuit Test Line

Identifies a test line number that denotes an arrangement in an end office which provides for an AC short circuit termination of a trunk or line by means of a capacitor of at least four microfarads.

USAGE: This field is required.

DATA CHARACTERISTICS: 8 characters; 7 numeric, 1 delimiter

EXAMPLE: NXX-XXXX

1.18 Open Circuit Test Line

Identifies a test line number that denotes an arrangement in an end office which provides an AC open circuit termination of a trunk or line by means of an inductor of several Henrys.

USAGE: This field is required.

DATA CHARACTERISTICS: 8 characters; 7 numeric, 1 delimiter

EXAMPLE: NXX-XXXX

1.19 Company Name

Identifies the name of the Exchange/Interexchange Carrier providing the test number/line information.

NOTE: Company name should appear at top, right-hand corner of each page of the Directory.

USAGE: This field is required.

DATA CHARACTERISTICS: 25 alpha characters

EXAMPLE: UNIVERSAL CARRIERS_____

2 TEST LINE NUMBERS FOR NPA 209/415

NPA	NXX	OFFICE	QUIET LINE 100	MILLI	ATMS	DATA	NINV	ECHO	INV	SYNC	NSYN	AC OPEN	SIGNAL
				WATT		TSTL	LPBK	CANC	LPBK	SUPV			SUPV TSTG
209	276	FRSNAC14CG0	276-0049	276-0020	276-0037	276-XXXX		276-XXXX		276-XXXX		XXX-XXXX	276-0021
209	279	MKHLCA12CG1	279-1290	279-1100	279-1537	279-XXXX		279-XXXX		279-XXXX		279-XXXX	279-1120
209	286	FRSNCA14CGO	276-0049	276-0020	276-0037	276-XXXX		276-XXXX		276-XXXX		276-XXXX	276-0021
415		OKLDCA0301T	95Y-0100	95y-0102	95y-0105	95y-0107	95y-0108	95y-0109	959-6060				103
			100	102	105	107	108	109					
415		OKLDCA0349T	95-1506	95y-1526	95y-1556	95y-0107	95y-0108	95y-0109	959-6060				103
			100	102	105	107	108	109					
415		SNFCCA2143T	100	102	105	107	108	109	606				103

Figure 1: Sample Format for Test Line Directory using NPA 209/415



ATIS-0300026

**Next Generation Interconnection Interoperability (NGIIF)
Reference Document**

Part VI, Network Management Guidelines

Version 12.0



ATIS is the leading technical planning and standards development organization committed to the rapid development of global, market-driven standards for the information, entertainment and communications industry. More than 200 companies actively formulate standards in ATIS' Committees, covering issues including: IPTV, Cloud Services, Energy Efficiency, IP-Based and Wireless Technologies, Quality of Service, Billing and Operational Support, Emergency Services, Architectural Platforms and Emerging Networks. In addition, numerous Incubators, Focus and Exploratory Groups address evolving industry priorities including Smart Grid, Machine-to-Machine, Connected Vehicle, IP Downloadable Security, Policy Management and Network Optimization.

ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications' Sectors, and a member of the Inter-American Telecommunication Commission (CITEL). ATIS is accredited by the American National Standards Institute (ANSI). For more information, please visit www.atis.org.

Notice

This document was developed by the Alliance for Telecommunications Industry Solutions' (ATIS) sponsored Next Generation Interconnection Interoperability Forum (NGIIF). The NGIIF addresses next-generation network interconnection and interoperability issues associated with emerging technologies. Specifically, it develops operational procedures which involve the network aspects of architecture, disaster preparedness, installation, maintenance, management, reliability, routing, security, and testing between network operators. In addition, the NGIIF addresses issues which impact the interconnection of existing and next generation networks and facilitate the transition to emerging technologies. All changes to this document shall be made through the NGIIF issue resolution process.

Note Regarding Previous Versions

The NIIF Reference Document was formerly known as the Network Operations Forum (NOF) Reference Document. The NOF Reference Document was published and maintained by Bellcore. The last version of the NOF Reference Document is Issue 13.

Disclaimer and Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

ATIS-0300026, NGIIF Reference Document, Part VI, Network Management Guidelines, formerly NIIF 5022

The NGIIF Reference Document, Part VI, Network Management Guidelines, is an ATIS standard developed by the NGIIF.

Published by

Alliance for Telecommunications Industry Solutions

1200 G Street, NW, Suite 500

Washington, DC 20005

Copyright © 2011 by Alliance for Telecommunications Industry Solutions

All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < <http://www.atis.org> >.

Printed in the United States of America.

Table of Contents

1	GENERAL.....	3
2	MINIMUM SET OF NETWORK MANAGEMENT CONTROLS.....	3
3	TERMINATING REROUTES INVOLVING AN INTEREXCHANGE CARRIER.....	4
4	TC SWITCH OR NETWORK FAILURES OR EXTENDED OUTAGES.....	4
5	MEDIA STIMULATED MASS CALLING (MSMC) EVENTS	5
6	NETWORK MANAGEMENT SS7 CONTROLS FOR HIGH VOLUME CALL IN (HVCi) EVENTS	5
6.1	DESCRIPTION.....	5
6.2	SOLUTION.....	6
6.3	CONCLUSION	6
7	SS7 NETWORK FAILURES.....	7
7.1	NETWORK RESTORATION PLANS	7
8	EMERGENCY COMMUNICATIONS	8
8.1	PUBLIC PACKET SWITCHED NETWORK (PPSN)	8
9	TERMINATION OF TELECOMMUNICATIONS CUSTOMER SERVICE	8
10	RESPONSIBLE ORGANIZATION (RESPORG).....	9
11	RESPORG TROUBLE REPORTING RESPONSIBILITIES	9
12	RECORDED ANNOUNCEMENTS	9
13	SS7 NETWORK OUTAGE MEASUREMENT.....	9
14	NETWORK MODIFICATION NOTIFICATION FORM.....	10
15	BLOCKED CALL MEASUREMENT FOR INTERCONNECTED COMPANY.....	10
16	GLOSSARY	10
17	APPENDIX A, MEDIA STIMULATED MASS CALLING EVENT NOTIFICATION FORM	11
18	APPENDIX B, COMPANY NAME	12
18.1	NETWORK MODIFICATION NOTIFICATION FORM.....	12

1 GENERAL

This document has been developed to provide the Network Management personnel of the Telecommunications Provider (TP) and Telecommunications Customers (TC) with alternative guidelines for traffic management when the following conditions arise.

- Network congestion due to facility failures or abnormal calling periods.
- TC Switch or Network Failures or Extended Outages.
- SS7 Network failures.
- Termination of TC Service.

Specific procedures will require preplanning and negotiations between the companies involved. This document does not replace nor supersede tariffs, contracts, or any other legally binding documents.

This document is being revised to delete the Contact Directories and add reference to a Service Provider Contact Directory.

The Telecommunications Providers invite and encourage frequent TP and TC Network Management meetings to discuss and plan traffic management options.

If a TC has a need or desire to investigate the availability and use of the options described in the following, they should contact the Telecommunications Provider Network Management Center listed in the Service Provider Contact Directory.

2 MINIMUM SET OF NETWORK MANAGEMENT CONTROLS

The following Network Management Controls represent a minimum level of control that is needed in every interconnected network switching node in order to ensure the overall integrity and reliability of the interconnected network:

- Automatic Code Gap (ACG)
- Call Gap (CG)
- Cancel To (CANT)
- Skip (SKIP)
- Automatic Congestion Control (ACC)

Automatic Code Gap (ACG) - ACG is a code control that is implemented automatically in response to a request from a database to limit traffic. This control can be in the form of six (6) through ten (10) digits. A six-digit control is used to protect the database in instances of a general overload. A ten-digit control is used to control focused overloads.

Call Gap - CG is a code control that regulates the maximum rate at which calls are released toward a destination code. Equipment vendors commonly provide the capability to Call Gap at intervals of 0.10 to 600 seconds on a range of numbers from three (3), six (6), or seven (7), through ten (10) digits.

Cancel To - CANT is a trunk group control that allows traffic to be canceled before hunting for a circuit to a destination. Equipment vendors commonly provide the capability to implement this control on a percentage basis.

SKIP - SKIP is a trunk group control that allows traffic to be directed to the next route before hunting for a circuit to a destination. Equipment vendors commonly provide the capability to implement this control on a percentage basis.

Automatic Congestion Control - ACC is a two-part feature. In order for ACC to function properly it must be implemented in the originating and terminating nodes of an interconnected network. The first part enables a (terminating) network node to alert interconnected nodes that it is in Machine Congestion 1 or 2 (MC1 or MC2). The second part allows a distant (originating) network node to automatically react to an ACC message and enact trunk group controls (CANT and SKIP) on specific trunk groups.

3 TERMINATING REROUTES INVOLVING AN INTEREXCHANGE CARRIER

Where the capability exists, terminating reroutes may be implemented temporarily to relieve network congestion due to facility failures or recognized abnormal calling periods (e.g., Mother's Day, disasters, etc). Under these circumstances, reroutes have the potential to improve call completions and service to the customer. This procedure will not be used to circumvent normal trunk servicing.

The only calls, from an TC, to be rerouted are terminating calls from an TC to an Access Tandem (AT) and are to be rerouted from the AT using a qualified office as a Via Office to the called End Office.

The guidelines for rerouting are as follows:

- Only one additional link should be added to the overall connection.
- At an TC's request a mutually agreed upon sample of potential reroutes should be activated at an agreed upon time and tested by the TC for transmission. As part of the pre-planning process, all involved links should meet TP's design requirements. The test results will be provided to the TP who will furnish them to the other TC's, upon request.
- A count of rerouted calls should be furnished to the TP trunk servicing, forecasting and design engineers so that rerouted traffic will not be reflected as capacity requirement for future capital expenditures.
- The Network Management Center should monitor the via office performance prior to and during the reroute to assure the quality of the network is maintained.

4 TC SWITCH OR NETWORK FAILURES OR EXTENDED OUTAGES

In the case where an TC suffers an extended network outage, the following options may be available to the TP and TC to reroute end users. TP and TC pre-planning is strongly advised since this option list is not all inclusive.

- The TC or TCs have a reciprocal agreement to carry the traffic. This will require preplanning to assess the work necessary to reroute originating traffic (e.g., Translations and Billing).
- If the TC has multiple switching POPs in the LATA, reroute to the working POP.
- The TP may provide a special recorded announcement at the request of the affected TC.
- The TP may route originating traffic to a recorded announcement with 101XXXX codes of TC's that volunteer to carry the traffic on an interim basis.
- The TP and TC may decide to do nothing.

5 MEDIA STIMULATED MASS CALLING (MSMC) EVENTS

The TP and/or TC needs to be advised of MSMC event, prior to the event taking place. The company receiving a customer request for a planned Media Stimulated Calling Event must notify the affected company's Network Management Center using the MSMC Event Notification Form (Appendix A). With respect to the fields "Nature of Service" and Contest Rules and Prize Information", requesting such information on the MSMC Event Notification Form, it shall be understood that the provision of such information or any part thereof is optional and voluntary. Contact will be made via FAX or E-Mail which may be followed by a confirming telephone call to numbers listed in the NGIIF Service Provider Contact Directory for Media Stimulated Calling Event Contact.

Control of the TP or TC network load during the event, should first be attempted by the TP/TC in their respective network. The amount of control should be at the discretion of the individual TP/TC. Although cooperative Network Management controls during the event may be required, the TP/TC should not be expected to invoke controls before the actual event occurs.

The TPs will provide the following information when network management controls are used on Toll Free calls:

- The start and stop time of control activities,
- The level of control,
- The number of blocked calls, where technology is available,
- The reason for the control.

The party experiencing the outage will inform their interconnected companies, as soon as possible. Existing FCC outage guidelines shall be utilized for reporting purposes. When a Toll Free number is identified, that number should only be passed to the TC(s) or RESP ORG carrying that traffic.

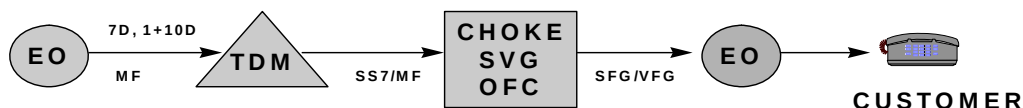
6 NETWORK MANAGEMENT SS7 CONTROLS FOR HIGH VOLUME CALL IN (HVCI) EVENTS

6.1 Description

High Volume Call In (HVCI) choke networks are designed to mitigate network congestion from large numbers of incoming calls solicited by an individual customer such as a radio station. Existing FCC guidelines specify in-band Multi-Frequency signaling trunking between the originating switch and choke tandem switch.

Figure 1 presents a simple diagram of the HVCI network. In this arrangement, excessive call attempts are terminated at the originating switch by limiting available outgoing trunks associated with HVCI NPA-NXX routing.

Choke (HVCI) Network Architecture



Historically, separate dedicated MF trunks between end offices and the choke tandem were used for HVCI codes. In this case, the volume of HVCI call attempts to the tandem was limited by the number of dedicated trunks to the choke tandem. Often such trunk groups are limited to 2-12 members.

Network Operators using newer technologies do not typically support MF signaling, or dedicated trunks to the choke tandem. Therefore calls for HVCI codes are carried to the choke tandem over common trunks. In this case,

the volume of HVCI call attempts to the tandem depends on the size of the common trunk groups carrying HVCI calls.

The volume of SS7 signaling associated with HVCI impacts signaling network capacity. The unsuccessful call attempt rate at a choke tandem can be large enough to trigger A-link growth for the tandem. This can especially be a problem for choke tandems where common trunks are used to deliver HVCI calls to the tandem.

Since unsuccessful calls are not completing, it is desirable to handle them in a way that minimizes demands on signaling network capacity.

6.2 Solution

“Far End Busy” is one approach that can be used to reduce the frequency of call attempts to HVCI codes at a choke tandem. With this scheme, the tandem switch supplies the audible busy tone (or announcement) to the calling party. The incoming trunk is held up while busy tone is applied by the tandem and is not released until the calling party goes “on-hook” or until the tone announcement cycle completes. (Normally when an incoming SS7 trunk encounters a “no trunk available” condition, the call is quickly released back to the originating switch, and the tone/announcement is provided from the originating switch.)

Implementation to hold trunks up to tone/announcement for blocked calls is relatively simple. An overflow route is configured for the HVCI trunk leaving the tandem. The overflow route can be pointed to appropriate tone/announcement circuits. When a call to an HVCI number encounters “no trunk available”, the call progresses to the route to the tone/announcement circuit, instead of being released back to the originating office for tone/announcement. This slows the volume of unsuccessful call attempts to HVCI numbers, and reduces the load on the signaling network.

In one case, before such a configuration was introduced, nearly 50% of calls at the choke tandem to HVCI codes had a duration of less than 1 second. After the choke tandem was re-configured to overflow HVCI calls to tone/announcement, less than 4% of calls had durations of less than 2 seconds. This demonstrates that an appropriate application of “far end busy” for HVCI codes can reduce call attempts for SS7 links to rates expected for traditional MF HVCI trunk groups.

The “far end busy” solution has the advantage that it can be implemented unilaterally by the carrier operating the choke tandem. No changes to other networks are required. Further, changes are only necessary to the choke tandem. No changes are required in originating switches.

“Far end busy” can be configured to work whether separate dedicated trunks are used for calls to HVCI numbers, or whether such calls are delivered to the choke tandem over common trunks. The use of separate dedicated trunks for HVCI codes remains the preferred configuration since it not only minimizes the impact of HVCI calls on the signaling network, but also minimizes the impact of HVCI calls on other traffic.

The overflow configuration at the choke tandem may need to be engineered and fine tuned in different manners depending on the capabilities of the choke tandem. The size of the overflow tones/ announcements route may need to be adjusted to appropriately slow call attempt rates. It should be noted the number of tone/announcement resources needed at the choke tandem to implement “far end busy” depends on the number of all trunks (both MF and SS7) delivering HVCI calls. If all HVCI traffic at the choke tandem arrives over dedicated trunks, then simple math can be used to determine how many tone/announcement resources must be provided to implement “far end busy”. If some HVCI calls arrive over common trunks, then a process is needed to adjust the number of tone/announcement resources until the desired result is obtained.

6.3 Conclusion

The “Far end busy” solution has been shown as a successful method to reduce call attempt rates for HVCI calls over SS7 trunks to approximate volumes traditionally achieved using MF choke trunks. With appropriate implementation of a “far end busy” configuration at a choke tandem, the impact of using SS7 trunks for HVCI calls can be reduced to an acceptable level.

It should be noted that the use of separate dedicated trunk groups can be a key factor in limiting the impact on the signaling network of calls to HVCI codes.

This solution does not address the impacts of mass calling to non-HVCI codes, such as 8XX numbers. Solutions for mass calling to non-HVCI codes may still need to be considered.

7 SS7 NETWORK FAILURES

With Pre-Interconnection, the TC is virtually blind to any failure in the SS7 network which will affect its database controlled traffic. The TPs providing SCP services to the TCs should, as locally agreed, notify all TCs utilizing the TP SS7 network of any SS7 network failures affecting the TC's traffic. Notification of SS7 failures will be according to local agreements and could be completed utilizing the following suggested organizations and methods:

- The local TP SS7 Network Management group or Number Administration Service Center.
- Telephone call to the TC.
- SMS mail feature or bulletin board feature.
- Failure notification could include:
 - Brief description of the trouble
 - Time trouble occurred
 - Location of the trouble (e.g., CLLI)
 - Estimated fix time (e.g., 10:00 a.m. EST)
 - Time trouble cleared, when available

Each TP/TC is responsible for providing a Point of contact. Contact numbers should be non 800 numbers and associated with the organization responsible for handling SS7 Catastrophic Network Failure reports.

7.1 Network Restoration Plans

7.1.1 Manual Intervention in the SS7 Network

Current network management procedures between the Telecommunications Provider and the Telecommunications Customer should remain in place assuming the SS7 network is stable. However, when a serious SS7 network failure occurs, new contingency plans are required.

The SS7 protocols designed to manage the network may not be sufficient in some failure scenarios. The potential for propagating a trouble in an integrated network increases the need for some manual network management capabilities. It should be noted that Manual controls applied to the SS7 network represents a serious undertaking and must be implemented only under extreme failure conditions. In these circumstances the interconnecting carrier should be informed in accordance with the SS7 Network Failures procedures in Section 6.

The specific actions to be taken will be dependent upon the particular network failure, the TP/TC network traffic management strategy and the manual control capabilities available by the vendor network element.

The following options may be available to the TP and the TC to restore and manage network or node stability in the event of a catastrophic SS7 outage. TP and TC preplanning is strongly advised since these options may not be all inclusive and could be interrelated. Attachment A, entitled Emergency SS7 Restoration Operations Planning Considerations, is recommended to be used as a guide for preparing such pre-plans:

- Deactivation of specific links to a SS7 network node.

- Deactivation of all links in internetwork gateway link sets.
- Use of STP Gateway screening to block additional incoming traffic from the remote SS7 network.
- Activation of protective controls to CANCEL traffic destined for the node and route it to the announcement. (CANT, CANF, CODE, BusyTrk)
- Activation of expansive controls to REROUTE traffic to nodes/trunk groups that do not normally carry that traffic. (REROUTE, SKIP, DRE, PRE).
- The Network Management Centers should monitor the traffic performance of the offices affected to assure quality controls are being implemented.
- Before any public switched traffic is allowed to proceed, every effort should be made to ensure the SS7 network is up and stable. It is recommended that the first traffic to flow should be the POTS traffic since other services, such as 800 Service, etc. require a POTS network.
- Re-introduction of POTS traffic on to the SS7 network should be assessed in the same manner that network managers currently use today. (i.e. Type of office and time of day). See Attachment A-Emergency SS7 Restoration Operations Planning Considerations.

8 EMERGENCY COMMUNICATIONS

Recognizing that all SS7 Network Providers and Manufacturers of SS7 Network System hardware and software have an obligation and responsibility to provide an adequate level of support for their products and/or service, it is recommended that they participate in an emergency communications system.

A depiction of Network configurations that are recommended to achieve interconnection for Emergency Communications purposes only, is reflected in Part VI, Attachment A-Emergency SS7 Restorations Operations Planning Considerations.

8.1 Public Packet Switched Network (PPSN)

It is recommended that all interconnecting networks (ICNs) and manufacturers interconnect via Public Packet Switched Network, non PSN Access, as part of a Closed User Group, in support of and to provide backup to the voice emergency communications network. The PPSN is to be utilized as a backup to the PSN as part of the emergency Communications System (ECS). Information to be communicated between entities should be identified and shared for ECS information.

9 TERMINATION OF TELECOMMUNICATIONS CUSTOMER SERVICE

The following options are available to the Industry to provide information to the users in the case of an TC leaving the market place. This is not an all inclusive list.

The TP can provide a recorded announcement with instructions to call the TP or another TC. The following is an example of the wording of the recorded announcement:

"The long distance company of your choice can no longer complete your calls. Please contact another long distance company or (local exchange company name and phone) to arrange for a new long distance company."

The TP can provide a recorded announcement with a list of 101XXXX codes of volunteers TCs, that the customers have available to them. There are technical issues that must be resolved prior to implementation of this option (e.g., The TCs must be willing to open their switches to 101XXXX casual calling).

The TP may provide a special recorded announcement at the request of the affected TC.

A media announcement may be released.

10 RESPONSIBLE ORGANIZATION (RespOrg)

The entity identified by the 800 Subscriber or the subscriber's agent assumes the duty of managing the appropriate records in 800 Database Service Management Systems (SMS). Management and Administration shall include Data Entry, Record Change, Trouble Acceptance, Referral, and/or Clearance. It is recommended that any entity performing the above function comply with this and other 800 Data Base associated documents.

11 RespOrg TROUBLE REPORTING RESPONSIBILITIES

The RespOrg trouble reporting entity has the overall provisioning, maintenance responsibility for the total service to the 800 Subscriber. It is responsible for the overall coordination of testing of its 800 Database Service.

The RespOrg is responsible for:

- Providing a contact number that is readily accessible 24 hours a day, 7 days a week.
- Providing trained personnel.
- Acting as the 800 Subscriber's contact in all matters involving provisioning and maintenance of 800 Database Service.
- Accepting trouble reports from both 800 Subscribers and casual end users or other parties receiving 800 Database trouble reports.
- Sectionalizing trouble to determine if the reported trouble is in its translations or facilities, or in other providers service.
- Testing cooperatively, if necessary, with other providers to further identify and clear a trouble when the trouble has been sectionalized to another providers service.
- Keeping the 800 Subscriber advised of the status of trouble clearance.
- Maintaining accurate records.
-

12 Recorded Announcements

Call Completion Announcements when utilized, should not make reference to a trouble causing network (company), unless the network experiencing the trouble has been identified.

13 SS7 Network Outage Measurement

Each TP/TC should use the methods provided in T1 Technical Report 38, A Technical Report on Analysis of FCC Reportable outage Data, to measure, analyze and develop trend analysis of their network outages.

14 Network Modification Notification Form

This form, Appendix B, is to be used in conjunction with the Network Modification Notification Guidelines.

15 Blocked Call Measurement for Interconnected Company

Measurement of blocked calls as it relates to network performance should be negotiated locally between interconnected companies. Below are some terms and definitions that may be used by individual companies:

Blocking: Blocking is said to have occurred when a request for a connection to final trunk group (common transport trunk group or access connection) is denied because of unavailability of a transmission path for any reason.

Final Trunk Group: A trunk group that does not route advance or alternate route to another trunk group if all of its trunks are busy.

Blocked Call: A blocked call is said to have occurred when a call presented to a telecommunications Service Provider (SP) facility cannot be completed due to Blocking.

Network Impacting Event: A failure (hardware, software, human, or process) of a telecommunications network component that prevents call completion.

16 Glossary

Telecommunications Customer (TC): The term "Telecommunications Customer" (TC) denotes any individual, partnership, association, joint-stock company, trust, governmental entity or corporation engaged for hire in interstate or foreign communication by wire, radio, or internet protocol between two or more exchanges or entities.

Telecommunications Provider (TP): The term "Telecommunications Provider" (TP) denotes a company engaged in the business of supplying telecommunications or access services.

Please see Part XIII, Terms and Definitions, of the NGIIF Reference Document for the definitions of other terms used in this document.

17 APPENDIX A, Media Stimulated Mass Calling Event Notification Form

Name of Promotion: _____

Nature of Service: Ticket sales _____ Tele-vote contest _____ Other _____

Scope of Promotion: National _____ Regional _____ Local _____

Promotional Media: Internet _____ Newspaper _____ Radio _____ TV _____ Other _____

Event Start Date: _____ Event End Date: _____

Time of Program(s): Start time(s)/zone(s) _____

Finish time(s)/zone(s) _____

Dialed Advertised Number(s): _____

Terminating Characteristics: POTS return number _____

Voice _____ Automatic Response Unit (ARU) _____ Other _____

Type of Event: Planned Event _____ Unplanned Event _____

Event Description: _____

• Estimated participation volume (total calls) _____

• Projected average holding time per completed call _____

• # of terminating lines _____

• # of operators _____

• Contest rules and "prize" information _____

Date/Time sent: _____ Initial Notice: _____ Follow Up Notice: _____

Originator's Name: _____ Company: _____

Originator's Tel Number: _____

While it is suggested that all fields be completed, provision of information on this form is voluntary.

18.1 NETWORK MODIFICATION NOTIFICATION FORM

Method of Cut: Flash ☐ Phase ☐ Facilities: If Reuse, list swing New ☐ Reuse ☐
locations under NTWK IMP

Glare Setting: _____ Reverse Setting: _____

105 Test #: _____ NPA/NXX Test #: _____

Local Mtce. Contact/Night of Cut: Name: _____ Number: _____

Estimated Time to Repair (for unplanned event): _____



ATIS-0300027

**Next Generation Interconnection Interoperability (NGIIF)
Reference Document**

Part VI, Network Management Guidelines

Attachment A

**Emergency SS7 Restoration Operations Planning
Considerations**

Version 12.0



ATIS is the leading technical planning and standards development organization committed to the rapid development of global, market-driven standards for the information, entertainment and communications industry. More than 200 companies actively formulate standards in ATIS' Committees, covering issues including: IPTV, Cloud Services, Energy Efficiency, IP-Based and Wireless Technologies, Quality of Service, Billing and Operational Support, Emergency Services, Architectural Platforms and Emerging Networks. In addition, numerous Incubators, Focus and Exploratory Groups address evolving industry priorities including Smart Grid, Machine-to-Machine, Connected Vehicle, IP Downloadable Security, Policy Management and Network Optimization.

ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications' Sectors, and a member of the Inter-American Telecommunication Commission (CITEL). ATIS is accredited by the American National Standards Institute (ANSI). For more information, please visit www.atis.org.

Notice

This document was developed by the Alliance for Telecommunications Industry Solutions' (ATIS) sponsored Next Generation Interconnection Interoperability Forum (NGIIF). The NGIIF addresses next-generation network interconnection and interoperability issues associated with emerging technologies. Specifically, it develops operational procedures which involve the network aspects of architecture, disaster preparedness, installation, maintenance, management, reliability, routing, security, and testing between network operators. In addition, the NGIIF addresses issues which impact the interconnection of existing and next generation networks and facilitate the transition to emerging technologies. All changes to this document shall be made through the NGIIF issue resolution process.

Note Regarding Previous Versions

The NIIF Reference Document was formerly known as the Network Operations Forum (NOF) Reference Document. The NOF Reference Document was published and maintained by Bellcore. The last version of the NOF Reference Document is Issue 13.

Disclaimer and Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

ATIS-0300027, NGIIF Reference Document, Part VI, Network Management Guidelines, Attachment A, Emergency SS7 Restoration Operations Planning Considerations, Formerly NIIF 5023

The NGIIF Reference Document, Part VI, Network Management Guidelines, Attachment A, Emergency SS7 Restoration Operations Planning Considerations, is an ATIS standard developed by the NGIIF.

Published by

Alliance for Telecommunications Industry Solutions

1200 G Street, NW, Suite 500

Washington, DC 20005

Copyright © 2011 by Alliance for Telecommunications Industry Solutions

All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < <http://www.atis.org> >.

Printed in the United States of America.

EMERGENCY SS7 RESTORATION OPERATIONS PLANNING CONSIDERATIONS

Table of Contents

1.	GENERAL	4
2.	FAILURE TYPES	4
A.	Signaling Transfer Point (STP) Failures	4
B.	Link and Linkset Failures	5
C.	Congestion	5
3.	LINES OF DEFENSE	5
A.	Traffic Categories and Considerations	6
B.	Preventing Propagation and Lessening Impacts of Failures	7
C.	Manual Intervention in the CCSN	7
D.	NM Preplans	8
E.	Access to Preplans	9
F.	Customer Notification	9
G.	Media	9
H.	Announcements	9
I.	Operator Alert	9
4.	RESTORATION	10
A.	Restoring the CCSN	10
B.	Release and Patch Administration	10
C.	Restoring Service	12
D.	Network Management and CCSN Events	13

1 GENERAL

Throughout this document the CCSN and PSTN are addressed as separate networks, even though both subnetworks comprise the new public switched network and both are necessary to complete calls. This is done in order to better focus on their uniqueness and concerns, separately, before attempting to merge the two, and perhaps miss some important issues. In addition, although more is presented on the maintenance side, maintenance should not be construed as more important than network traffic management. In the order of things, however, maintenance is vital with the advent of the CCSN. The CCSN must evolve to a consistently stable network to allow Network Traffic Management (NTM) efforts to be effective. Additionally, NTM functions can greatly assist in this stability.

Recent Common Channel Signaling Network (CCSN) outages are causing speculation that more severe problems will occur in the future. The industry in general is concerned that they may not be properly prepared to diagnose troubles quickly and contain their proliferation in an integrated CCSN. One of several areas being addressed in this document is the recovery procedures for CCSN failures. Also addressed are actions that might be taken to contain the spread, or worsening, of network failures when Telecommunications Providers (TPs) and Telecommunications Customers (TCs) are interconnected. These two areas of concern are inter-related and require both an understanding of their inter-relationship and a comprehensive plan of action.

This document assumes a 100% deployment of CCS interconnection between an TP and TC.

It provides a view of factors that a typical Network Provider might consider in planning responses to potential network events.

2 FAILURE TYPES

As with any network, there are numerous events that can cause failures. In this respect the CCSN is quite similar to other networks. Unlike most other networks, however, the CCSN comes the closest to being self-managed. It automatically takes preprogrammed actions (via the SS7 protocol) to continue functioning when various abnormal conditions exist. Signaling Network Management functions provide for reconfiguration of CCSN resources in the event of signaling link or signaling point failures. When a failure occurs, the objective is that, the reconfiguration should be carried out so that messages are not lost, duplicated or put out of sequence and that the number of messages in the network does not become excessive. These types of failures, which are transparent to the PSTN and the traditional Network Traffic Management (NTM), are not reviewed in this document except when, in combination with other events, they will have an impact on service. A point to be made, however, is that efforts are being made to review and enhance the protocol, if necessary, to make it more reliable and effective in failure scenarios since self-healing networks is the strategic direction. We do not suggest that these failures are not important. Any failure in the CCSN must be viewed as extremely crucial and expeditiously dealt with since combinations of events can impact customers and have potentially far reaching consequences.

Failures that will be discussed in this document include those described in the following subsections.

2.1 Signaling Transfer Point (STP) Failures

STP failures, at present, represent the greatest threat to the overall reliability of a CCSN, since links from all associated Signaling End Points (SEP) terminate on the STP pair. The failure of a single STP should not, in and of itself, cause any severe impact on the ability of the PSTN to route calls. It is only when an STP failure is coupled with another condition in the CCSN that signaling traffic is impaired, causing an impact on the PSTN. Examples of conditions under which an STP failure will impact the CCSNs message processing capabilities are as follows:

If software errors in either the mated STP or an associated SEP trigger an abnormal reaction to the failed STP, individual SEPs or all associated SEPs could become isolated from the CCSN.

If individual signaling linkset failures to the mated STP are in effect prior to and during the STP failure; offices could be isolated.

If the CCSN network and its components have not been engineered adequately, congestion etc. could be encountered.

2.2 Link and Linkset Failures

As in the case of a single STP failure, the failure of a single link or linkset should have no severe impact on signaling traffic since the CCSN is engineered to self manage. It is only when coupled with other conditions in the CCSN that there would be an impact. The impact could range from complete SEP isolation (no messages to or from an SEP) to a condition where some individual SEPs cannot send and receive messages to or from other individual SEPs. Conditions which could impact an SEP's ability to send and receive signaling messages include the following:

Failure of an SEP's combined linkset to communicate with the mated STPs due to one or a combination of causes:

- SEP hardware
- SEP software
- facility failure
- facility failure and no physical route diversity of links making up combined linkset
- Failure of a combination of linksets in the routing path to another SEP due to the same causes listed above.

2.3 Congestion

The levels of congestion in the CCSN refer to the queued messages in the buffers associated with the network elements. There are four congestion levels (0, 1, 2 and 3) that are specified by the SS7 protocol. There are also four levels of priorities for messages, such as Transaction Capabilities Application Part (TCAP) messages which are usually a priority one. These priorities are used in concert with levels of congestion. For example, a congestion level of two would indicate to all nodes coming into an STP not to send any messages with priority less than two. A congestion level of three would advise not to send any messages with priority less than three.

Since maintenance messages are assigned a priority three, and the highest congestion level is three, maintenance messages would continue to flow (which is mandatory for the CCSN to function).

The SS7 protocol is designed to throttle-back volumes of messages when experiencing congestion. In the event this process fails, the congestion may become unmanageable, resulting in internal STP congestion which can then cause links and linksets to fail. If this condition is replicated in mated STPs, network outages may occur, isolating an office.

3 LINES OF DEFENSE

Controlling the impact of network failures, particularly with common channel signaling, is an essential activity. The spread of certain type failures (e.g. STPs) is not only extensive, but rapid. TPs and TCs should carefully review the layout of their PSTN, with an overlay of their CCSN, and consider key lines of defense. There should be a realization that the impact of one network event can be boundless across network boundaries. It is not only widespread, but deep, in its effect. One TP event may not only impact a Local Access Transport Area (LATA), and all its offices, but also the inter-LATA traffic. Conversely, trouble in an TC network can affect one or more TP networks and possibly other TC networks. For these reasons, this Section reviews activities applicable to the

CCSN, including a discussion on Network Management in a CCSN environment and pre-plans for the PSTN. The following section divides traffic into unique categories with corresponding lines of defense and activities to be considered.

3.1 Traffic Categories and Considerations

The transition from MF signaling to common channel signaling demands a new awareness of the potentially widespread outages due to CCSN failures. The result can be total loss of service to a customer. This section categorizes traffic into groups whose vulnerabilities are similar and whose control activities may be unique. After each discussion regarding outages affecting each category, there is a brief discussion on action considerations.

NOTE: In the considerations that are addressed in the following sections, F-links are suggested as a possible alternative. It should be noted that requirements for F-links do not currently exist, but are being reviewed. It should also be noted that with the advent of new services that may require the use of an SCP, F-links may not be a good long term investment in some scenarios. This is an individual assessment and should depend on the strategic directions of the interconnecting companies.

3.1.1 Intraswitch (AP)

During the failure types discussed in Section 2, calls outside the switch will not be completed, causing abnormal numbers of retries, in turn, congesting the switch and potentially disabling it. Network Traffic Management techniques, such as call-gapping, would be ineffective in this situation, since dial tone is not selective, but responsive to any off-hook condition, and the dialed digits must still be entertained. Switch processing is not split between pre-disposition and final disposition, i.e., there is no capability to up-front drop any NXX code not resident in the switch and only process resident codes. The capability to introduce an announcement (e.g., "only calls to the following NXX codes will be processed at this time"), before dial tone, is also not available.

Consideration: The objective here is to alert the public in an effort to stop redialing calls that have no chance of being completed, hence avoiding switch congestion. There needs to be a review of requirements or techniques that can be implemented to prevent congesting the switch, so intraswitch traffic can still be executed. It should be noted that the introduction of Integrated Services Digital Network (ISDN) may reduce congestion since these calls would not require an analog, sequential, time-consuming process. Announcements before dial tone may be a practical solution for digital switches, although perhaps not for analog switches.

It should be understood that the concern stated here is applicable to the following categories.

3.1.2 Interswitch/Intraoffice

Two different switches that are co-located are introduced to a new concern with CCS. In the CCS environment, signaling for trunks connecting these switches may venture well beyond the co-located office. The reader is reminded that a mated pair of STPs does not reside in a common location, for purpose of diversification, and on any specific call set up, if both STPs are in service messages will most likely visit both STPs. So, even in those cases where an STP shares a location with co-located switches, some of those call set up and tear down messages will route via the distant, mated STP.

Consideration: Co-located switches may be a prime candidate for F-links (CCS links connecting two switches - no STP involved), eliminating the need for any trunking or signaling beyond a central office. Assuming that there is no switch congestion those interswitch trunks would be excluded from any propagation of CCSN failures and events involving STPs.

3.1.3 Interswitch/Interoffice

These calls have been reviewed, to some extent, in a previous section. The isolation of an end office due to a combined link set failure introduces a situation in which network traffic management and/or other techniques may be ineffective (other than code blocking) until the A-links can be restored.

Consideration: Similar to Interswitch/Intraoffice, these groups may be candidates for F-link deployment and/or possibly some retention of MF trunking. In addition, E-link deployment can be considered.

These three different categories of traffic whose elimination would have a dramatic impact on TP and/or TC customers, especially since these categories represent traffic that is particularly sensitive to emergency situations. The above has introduced two important lines of defense - the switch and any local trunk group associated with local emergency traffic.

3.1.4 InterLATA Access

InterLATA access is a major concern, particularly as it affects major businesses and the complexities that are introduced with the interaction of other CCSNs. Current network management procedures between local exchange and interexchange carriers (TCs) will remain in place assuming the CCSN is stable. Serious CCSN failures, however, will require new contingency plans. These are addressed in some detail in this document.

3.2 Preventing Propagation and Lessening Impacts of Failures

Recent CCSN outages created some concern that the protocol, designed to manage the network, may not be sufficient in some failure scenarios. The potential for propagating a trouble in an integrated network increases that concern, causing speculation that some form of manual network management may be needed. What is included in the following section addresses the subject of manual intervention (e.g., in cases of Network Instability/Node Corruption).

What seem to be appropriate are predetermined contingencies that address the subject of isolating a CCSN from one or more interconnected CCSNs. These CCSN capabilities should be identified and ways found to implement these blockages when necessary. It should be stated, however, that all efforts should be made to mechanize these contingencies where possible.

3.3 Manual Intervention in the CCSN

It should also be noted that some manual controls applied to the CCSN represents a serious undertaking and must be implemented only under extreme failure conditions. In these circumstances the interconnecting carrier should be informed.

One component for an overall network recovery plan, TP/TC personnel should prepare contingencies or manual intervention actions that may be used to mitigate the effects of CCSN failures,. This will alleviate traffic overloads in the CCSN, and/or allow CCS network elements (NEs) to be restored to their proper operation.

The specific actions to be taken will be dependent upon the particular network failure or trouble scenario anticipated and the carrier's network traffic management strategy, as well as the manual control capabilities facilitated by supplier implementations of the CCS NEs, their operations interfaces, and supporting operations systems (OSs). A prior knowledge of the percentage and number of trunks using CCS and MF signaling on a per switch, per LATA, and per interconnected network will facilitate the network managers anticipation of customer isolation impacts that will result from manual control actions that are suggested below to obtain nodal and network CCS isolations.

The following subsections provide at least a partial list of the manual intervention actions that might be prepared.

3.3.1 Node Isolation

Operations personnel should prepare contingencies to isolate individual signaling points from the network in cases where hardware or software failures may result in the inability of a given node to detect internal outages and/or trigger the appropriate automatic SS7 signaling route management and signaling traffic management actions. This isolation action diverts or throttles signaling message traffic to this individual signaling point.

Currently, network operations personnel may accomplish this objective by executing prepared scripts maintained in a maintenance OS to invoke supplier-specific NE commands that deactivate the signaling links connecting the subject signaling point to its adjacent signaling points. Contingency preplans should be made if a Network Element (NE) does not respond to supplier-specific commands to deactivate the signaling links. In such a case, a contingency preplan to remove the links physically (e.g. removing a circuit pack) should be employed.

There are currently no published generic requirements for uniform capabilities or procedures to accomplish this action. The control would involve the forced manual declared failure of signaling links in designated link sets.

3.3.2 Network Isolation

Network operations personnel should prepare contingencies to isolate a CCSN from other interconnected CCSNs in cases where replicated software errors in CCS NEs causing failure condition to propagate or co-exist across the network. Also prepare contingencies when automatic SS7 congestion controls have failed to protect a CCSN from severe traffic overloads originating in the interconnected CCSN. Procedures should be prepared for cases involving both directly connected CCSNs and remote CCSNs interconnected via an intermediate network or networks.

In the case of a directly interconnected CCSN (i.e., whose STPs or CCS is directly connected to a CCSN via signaling links), such a network isolation action may be achieved as discussed above by network personnel invoking prepared scripts to deactivate all links in all appropriate internetwork gateway link sets.

However, in the case of a remote CCSN interconnected through an intermediate CCSN or "hub provider," such actions would not be sufficiently selective to ensure isolation of the a CCSN from the subject network only. There are two alternatives that may be used in order to isolate a remote CCSN. The first alternative uses 1) Gateway STP screening to block all incoming traffic from the remote CCSN and 2) Trunk Group (TG) protective controls (e.g. CANT) to block traffic destined to the remote CCSN network. The second alternative would require coordinated action from the hub provider to fail the signaling links used to access the signaling services by the remote CCSN.

3.4 NM Preplans

The use of NM preplans via a Network Traffic Management Operation System (NTMOS) is a viable way to lessen the impact of a CCSN failure. Although the signaling network is capable of protecting itself for most failures, when CCSN failures do occur, the impact on the PSTN can be quite severe, and reaction time very limited.

One of the capabilities of controlling the severity of a failure is via the implementation of preplans. Preplans are used to protect or route around sector or access tandems and/or a major facility failure. Preplans are built by the Network Manager and reside in the NTMOS database.

There are two types of plans: Code control and Trunk Group control. Controls fall into two categories: Protective and Expansive.

Protective controls CANCEL the traffic and route it to an announcement. Expansive controls REROUTE the traffic to trunk groups that do not normally carry that traffic.

3.4.1 Protective Controls

Code controls (Call Gaps) limit the number of attempts from a controlled office to a particular called number or NXX. A code control is typically effective on from three (3) to sixteen (16) digits. Nominally, Call Gaps are in levels of 1 to N. The disposition of the call is determined by the Network Manager. The call can be sent to an Emergency Announcement (EA) with a timely announcement pertaining to the situation or to the normal No Circuit Announcement (NCA).

Cancel To (CANT) and SKIP are Prehunt controls; CANT prevents the affected traffic from making an attempt on the controlled trunk group. SKIP causes the affected traffic to skip the controlled trunk group and hunt for a trunk in the next alternate trunk group.

Cancel From (CANF) is a Posthunt control; CANF prevents the affected traffic from overflowing from the controlled trunk group.

3.4.2 Expansive Controls

Immediate Reroute (IRR) and Overflow Reroute (ORR) also called a Regular Reroute (RR), are Expansive Trunk Group Controls.

IRR is a prehunt control, IRR diverts the affected traffic away from the controlled trunk group and causes it to hunt for a trunk in the designated trunk group. ORR or RR is posthunt control. ORR diverts the affected traffic after it overflows the controlled trunk group.

Some restrictions of such plans may be:

- Maximum number of controls in a plan.
- Maximum total of controls in all plans.
- Maximum number of plans.

Preplans must be updated whenever a change takes place in the network. An outdated Preplan is of little use in a failure scenario.

3.5 Access to Preplans

There may be occasion when access to the Network Management OS is blocked, the OS, or the intermediate OS is not on-line, or access from the OS to the switch is unavailable. In certain critical situations this may be unacceptable and require an alternative plan. Such a plan is envisioned by implementing critical preplans (also resident in the network management OS) via the maintenance OS over the switch maintenance channel interface. Some service providers do not use an automated method to apply preplans.

3.6 Customer Notification

A concern in any major failure is the potential to congest a switch due to reattempts on dialing a call that cannot be completed. A knowledgeable public at this point can lessen that concern. Not being able to call a distant relative or business partner is one thing; not being able to call the police, doctor, fire department, neighbor, etc. can be a different matter. Every effort must be made to complete emergency calls.

The advent of CCS increases the potential of end office isolation due to the greater potential for widespread disruption, causing fewer call completions and consequently, dramatic increases in redialing.

If customers know the only calls that can be completed are to NXX numbers within their switch, the potential for switch congestion could greatly diminish.

3.7 Media

One of the ways to inform the public is via the media (e.g. radio and TV). Prearranged agreements and plans for quick notification can be most beneficial in alerting the customers.

3.8 Announcements

Announcements were discussed in previous section.

3.9 Operator Alert

Operator calls dramatically increase during network congestion or failures. An uninformed operator can add to the problem. An informed operator can advise the public. What is needed here is the capability to alert operators via their operator service position screen, etc., using a maintenance workstation. There should be the ability to quickly instruct operators on options available.

4 RESTORATION

The introduction of common channel signaling has significantly complicated the restoration process involving failures that impact the PSTN. CCSN failures, particularly those necessitating node restart procedures (e.g., STP), have the potential for message loss and congestion problems. In addition, careful coordination is required between the CCSN and PSTN in any restoration procedure. These concerns are discussed in some detail in the following two sections.

4.1 Restoring the CCSN

A failed CCSN should be restored in accordance with the type of outage encountered. The following are examples of different scenarios involving failed STPs:

- Both STPs in a mated pair have failed gracefully
- If both STPs can be restored, normal SS7 restoration procedures should be followed.

It is difficult to provide specific details on how to restore a CCSN after a major failure because of the uniqueness of each network and each failure. There are, however, several factors to be considered when developing any restoration strategy. They include:

- Whether the Failure cause has been determined and remedied
- The number of signaling links connected to the STPs
- The number of links used for STP interconnections (B and D links)
- Amount of traffic left on the CCSN, if any, at the time of restoration
- Any known idiosyncrasies of the Vendor STP product.

As described earlier in this document, a major failure is one that has affected both STPs of a mated pair to the point where the CCSN can't support the services using the network. After such a failure, as much normal traffic as possible should be prevented from entering the network until all available components are up and stable; e.g., no links going up and down and no unusual maintenance messages being generated in the STPs. NM control actions on the traffic network may be necessary subsequent to signaling network controls in order to allow the gradual return of traffic to the recovering node(s). These traffic controls may also be necessary to reduce congestion conditions that may arise from CCS controls. Note that when Trunk Group or Code Controls are used, strategies should allow MF trunk groups (if and while they exist) to continue to operate at full capacity thus avoiding unnecessary isolation or overcontrol.

If the failure cause has been remedied, the CCSN may restore itself. If not, normal vendor provided STP node restart procedures should be sufficient to restore the CCSN to normal. The recommended order to restore signaling links is C, then B and D, and finally A. If, however, the cause of the trouble has not been determined or remedied, consideration should be given to restoring the STPs in the simplex mode (C links forced out of service). If necessary, consideration should also be given to manually restoring B and D links, observing that the network remains stable as the links are restored. If any instability appears, the C links should be forced out of service and the network should be operated in the simplex mode until the problem has been resolved. If any A link linksets have failed, signaling point isolations may result from forcing the STPs into simplex operations.

Once the network has been restored and all appears stable, traffic should be restored according to a pre-planned strategy. The CCSN should be closely monitored to confirm that the restoration of traffic doesn't cause any instability.

4.2 Release and Patch Administration

It is important that a database or databases containing information on current release level and patches that have been applied to all Network Elements (NEs) exist and be kept current. This information must be readily available

to center personnel responsible for trouble resolution. In many cases these databases are currently resident in an Electronic Systems Assistance Center (ESAC) administration system and are kept current with the aid of network element vendor OSs which support the patch administration process. It is advisable that this database is updated concurrent with the update to the NE. It is also advisable that when new releases are received from an NE provider that they be loaded in only one NE for a period sufficient to evaluate performance of the software. It is desirable that the NE chosen for this SOAK period be one that does not serve a major downtown area or critical service element; e.g., 9-1-1. In analysis of a trouble condition, consideration of release and patch level may be beneficial in resolution.

It is also preferable that these databases provide the ability for:

4.2.1 CCSN Stabilization

CCSN stabilization can be defined in many ways, but as a minimum, to be considered stable a CCSN must be prepared to receive traffic. Various indicators and parameters can be watched for signs of CCSN stabilization or destabilization. General criteria for CCSN stabilization are the following:

- Number of change-overs and change-backs is within acceptable limits.
- Number of congestion status changes over parts of CCS network is within acceptable limits.
- Number of MTP flow-control messages is within acceptable limits.
- Number of MTP traffic control and MTP-user restricting messages are within acceptable limits.
- Number of ISUP automatic control messages is within acceptable limits.
- Number of TCAP and OMAP control and test messages are within acceptable limits.

If all these parameters are within acceptable limits, then it is a good indication that the CCSN is stable. In all other cases the limits must be defined on a regional basis prior to CCS operation within the region.

4.2.2 Node Restart Procedures

Node restart procedures enable an unavailable node, which is in the process of becoming available, to bring a sufficient number of signaling links into the available state and to update its routing tables before user signaling traffic is restarted to that node. A node is considered to be unavailable when all of its connected signaling links are unavailable. Node restart is a network management function and occurs at Level 3 of the Message Transfer Part (MTP) of a node. The node restart procedures are specified in Bellcore Specification of Signaling System Number 7 (TR-NWT-000246), where the procedures are referred to as MTP Restart. These procedures should help alleviate the burden placed on restarting nodes, allowing them to enter a stable state before accepting user signaling traffic. This is expected to reduce the potential for problems which may cause a restarting node to regress to an unavailable state.

4.2.3 Motivation

The primary motivation for the node restart procedures is the potential for message loss which currently exists in the way a signaling point, specifically an STP, behaves upon restart. No requirements currently specify special procedures for how a restarting signaling point should behave in order to accept traffic from adjacent nodes in a graceful and efficient manner. Currently, a restarting signaling point activates its signaling links serially, until all links, or a sufficient number of links, are available. Problems may occur due to this situation. Link congestion, for example, may occur when the STP receives traffic on a newly available links and an insufficient number of links have been activated on which to route outgoing signaling traffic, or traffic is destined for a point code that is not yet available. In addition to the potential for lost signaling traffic, there also exists the potential for congestion problems to occur on the newly available links.

The proposed node restart procedures prevent signaling points from sending user signaling traffic to an adjacent node which is restarting before the restarting node is ready to receive traffic. Being ready to receive traffic means having accurate routing information, as well as having a sufficient number of signaling links in the available state in order to perform the appropriate signaling point functions effectively and efficiently. Having accurate routing

information prevents an unusual amount of signaling route management messages being transmitted across the network.

4.2.4 Overview of Node Restart Procedures

Two new network management messages to be used in conjunction with the node restart procedures have been defined in standards. The Traffic Restart Waiting (TRW) message is an indication to the receiving node that user signaling traffic should not be sent to the originator of the TRW until a Traffic Restart Allowed (TRA) message is received from the same node. A TRA is an indication to the receiving node that all signaling traffic may be resumed to the originator of the message.

The node restart procedures are not only performed at a restarting node, but also at nodes adjacent to the one which is restarting. >From the perspective of the restarting node, the procedure can be broken down into several stages. First, the restarting node attempts to make available, in parallel, its signaling links. As links become available, the starting node sends TRWs to adjacent nodes, indicating that it is not ready to receive any user signaling traffic. The restarting node expects to receive a TRW from adjacent STPs, as well as signaling route management messages, specifically Transfer Prohibited (TFPs), Transfer Restricted (TFRs), Transfer Cluster Prohibited (TCPs) and Transfer Cluster Restricted (TCRs) from adjacent STPs, and will update its routing tables upon receipt of these signaling route management messages. Also, the restarting node expects to receive TRAs from each adjacent node indicating that they are themselves ready to receive user signaling traffic. When a sufficient number of signaling links have been made available, and a sufficient number of adjacent nodes have indicated that they are ready to receive traffic, the restarting node, if an STP, will then broadcast to adjacent nodes the status of its routes using TFPs and TFRs, as well as TCPs and TCRs if cluster management is implemented. Upon completing the broadcast of signaling route management messages, the restarting STP will be ready to receive all signaling traffic, and will indicate this to adjacent nodes by broadcasting TRAs. If the restarting node is not an STP, it will not broadcast signaling route management messages, and will simply broadcast TRAs. At this point, the restarting node will have reasonably accurate routing tables, and will have a sufficient number of signaling links available to handle the expected traffic.

From the perspective of a node adjacent to one which is restarting, the procedure can also be broken down into stages. When the first link of a link set to a previously unavailable node comes up, the adjacent node will behave in one of two ways, depending on its capabilities. More specifically, if the adjacent node is an STP, it will first send the restarting node a TRW, followed by the necessary signaling route management messages indicating the status of each destination to which it routes which is not allowed. No signaling route management messages will be sent by the adjacent STP if all the point codes to which it directly routes have a status of allowed. These messages allow the restarting node to update its routing tables prior to receiving any user signaling traffic. Once all the necessary signaling route management messages have been sent to the restarting node, the adjacent STP should send it a TRA indicating that it is ready to receive all signaling traffic. If the adjacent node is not an STP, a TRW will not be sent, and a TRA should be sent to the restarting node when it is ready for user signaling traffic. The adjacent node will then wait for an indication from the restarting node that it is ready to receive user signaling traffic.

4.3 Restoring Service

Before any public switched traffic is allowed to proceed, every effort should be made to make certain the CCSN is up and stable. It is recommended that the first traffic to flow should be the POTS traffic since other services, such as 800 Service, etc. require a POTS network.

How that POTS traffic is reintroduced depends upon the type of outage (e.g., entire LATA, single isolated office, etc.), the type of traffic in offices involved (heavy business, heavy residential, combinations), time of day (busy office hour, etc.), those concerns that network managers currently take into account. Consideration must also be given to any pre-plans activated in defense of the failure, i.e., how they were deactivated, were they deactivated, etc.

Applications on the CCSN will intensify and acceleration of extremely high-speed transmission capabilities will follow. In short, managing the CCSN, in the manner traditionally used to manage the PSTN, will not only not be feasible, it will not be advisable. Every effort must be made to enhance the protocol to enable self-management of

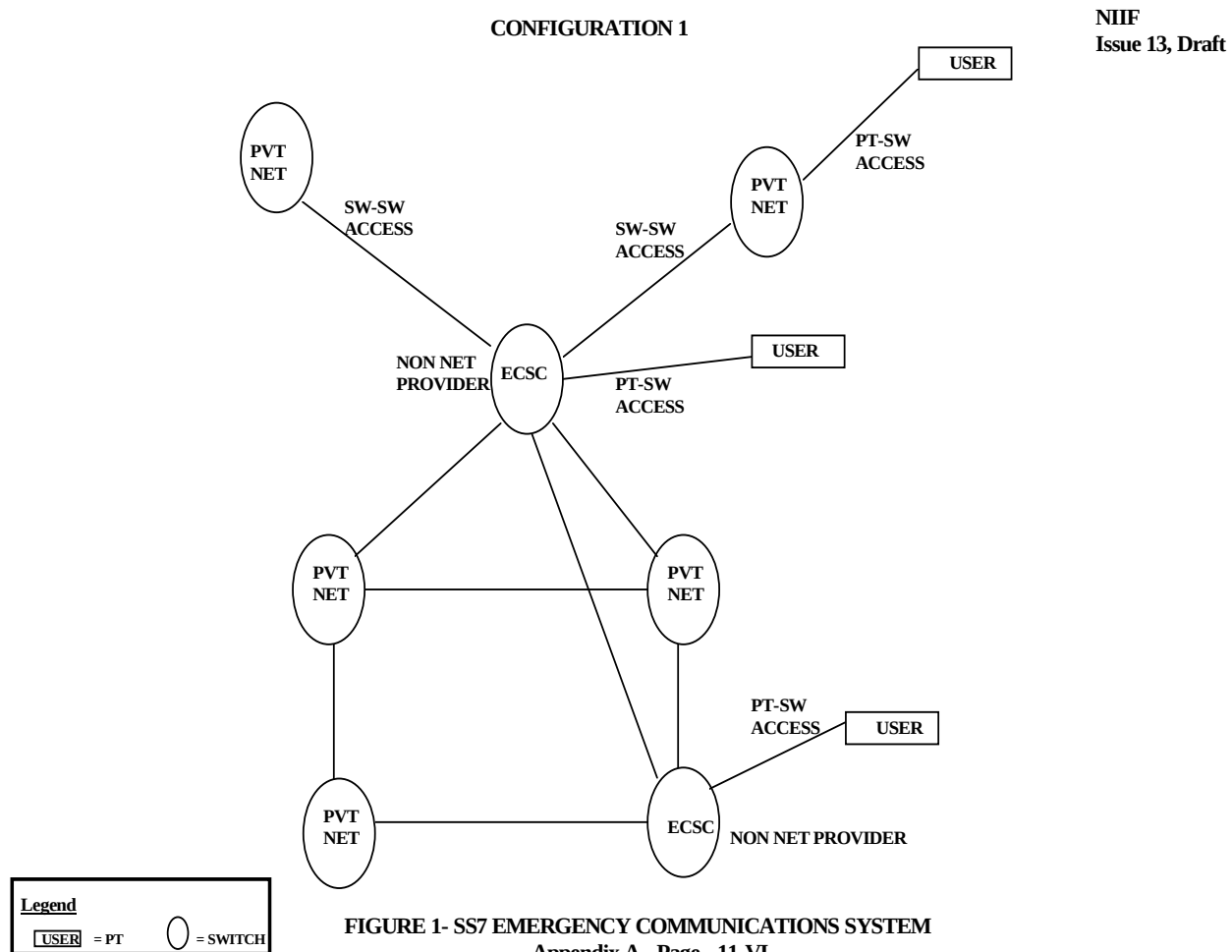
the CCSN. There may be a manual role required to prevent propagation of a failure. This was discussed in some detail in a previous section.

Acknowledging the fact that the Public Network (for want of a better reference) will transition to two subnetworks, the CCSN and the PSTN, both required for call completion, does not eliminate the need to view these sub-networks on an individual basis from a Network Management perspective. On an individual basis, one should begin with the CCSN. When the CCSN is stable, NTM of the PSTN is implemented in the traditional manner. Most, but not all, of the failures experienced in the CCSN will be transparent to the PSTN, a product of redundancy and protocol.

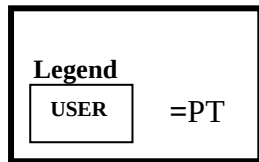
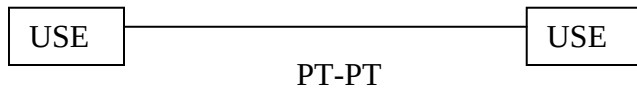
Some failures in the CCSN will impact the PSTN and, unexpected, high concentration of traffic loads (e.g., media) may cause congestion in the A-links associated with that traffic load.

4.4 Network Management and CCSN Events

Events in the CCSN that impact the PSTN will probably occur at one of two levels, isolation of an end office or isolation of a complete LATA (assuming a mated pair of STPs per LATA and no E-links). Other events such as SCP isolations have been referenced by this plan, and should be considered in any comprehensive operations plan.



CONFIGURATION 2





ATIS-0300028

**Next Generation Interconnection Interoperability (NGIIF)
Reference Document**

Part VII, Information Sharing

Version 12.0



ATIS is the leading technical planning and standards development organization committed to the rapid development of global, market-driven standards for the information, entertainment and communications industry. More than 200 companies actively formulate standards in ATIS' Committees, covering issues including: IPTV, Cloud Services, Energy Efficiency, IP-Based and Wireless Technologies, Quality of Service, Billing and Operational Support, Emergency Services, Architectural Platforms and Emerging Networks. In addition, numerous Incubators, Focus and Exploratory Groups address evolving industry priorities including Smart Grid, Machine-to-Machine, Connected Vehicle, IP Downloadable Security, Policy Management and Network Optimization.

ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications' Sectors, and a member of the Inter-American Telecommunication Commission (CITEL). ATIS is accredited by the American National Standards Institute (ANSI). For more information, please visit www.atis.org.

Notice

This document was developed by the Alliance for Telecommunications Industry Solutions' (ATIS) sponsored Next Generation Interconnection Interoperability Forum (NGIIF). The NGIIF addresses next-generation network interconnection and interoperability issues associated with emerging technologies. Specifically, it develops operational procedures which involve the network aspects of architecture, disaster preparedness, installation, maintenance, management, reliability, routing, security, and testing between network operators. In addition, the NGIIF addresses issues which impact the interconnection of existing and next generation networks and facilitate the transition to emerging technologies. All changes to this document shall be made through the NGIIF issue resolution process.

Note Regarding Previous Versions

The NIIF Reference Document was formerly known as the Network Operations Forum (NOF) Reference Document. The NOF Reference Document was published and maintained by Bellcore. The last version of the NOF Reference Document is Issue 13.

Disclaimer and Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

ATIS-0300028, *NGIIF Reference Document, Part VII, Information Sharing, Formerly NIIF 5024*

The NGIIF Reference Document, Part VII, Information Sharing, is an ATIS standard developed by the NGIIF

Published by

Alliance for Telecommunications Industry Solutions

1200 G Street, NW, Suite 500

Washington, DC 20005

Copyright © 2011 by Alliance for Telecommunications Industry Solutions

All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < <http://www.atis.org> >.

Printed in the United States of America.

INFORMATION SHARING

Table of Contents

1.	GENERAL	3
A.	Purpose	3
B.	Applicability	3
C.	Definition	3
D.	Document Organization	3
E.	Purpose Of Information Sharing	3
2.	BASIC PREMISES	4
3.	CRITERIA FOR SHARING INFORMATION	4
4.	OPERATING PRINCIPLES	4
5.	SCOPE	5
6.	SERVICE PROVIDER RESPONSIBILITIES	6
A.	Service Provider Stand Alone Testing Environment	6
B.	Compatibility Testing Between Service Providers	6
C.	Service Provider Daily Operation	6
D.	Service Providers	6
E.	Documentation	6
7.	VENDOR/MANUFACTURER RESPONSIBILITIES	7
A.	Vendor/Manufacturer And Customer (Customer Reported)	7
B.	Customer/Vendor/Manufacturer To Interconnected Service Providers	7
C.	Vendors/Manufacturers	7
D.	Vendor/Manufacturer Discovered Problems	8
E.	Differences In Specifications Interpretation	8
8.	INFORMATION TO BE SHARED BETWEEN VENDOR/MANUFACTURER AND CUSTOMER	8
9.	INFORMATION TO BE SHARED BETWEEN CUSTOMER AND VENDOR/MANUFACTURER	9
10.	MODES OF COMMUNICATION	9
A.	Proactive Notification Mode	10
B.	Vendor/Manufacturer Electronic Message System Mode	10
11.	FACILITY OUTAGE REPORTING GUIDELINES	10

1 GENERAL

1.1 Purpose

This document is intended to provide the appropriate guidance to facilitate the sharing of information. It identifies types of information which may be shared, the circumstances under which it should be shared, the extent to which sharing is appropriate, and the mechanisms and timing for that sharing. It represents industry consensus arrived at with the full participation of members of the Network Interconnection Interoperability Forum which consists of Access Service Providers, Access Service Customers and Vendor/Manufacturers.

1.2 Applicability

This document is intended to be a living document, therefore subject to revision and upgrading under the Carrier Liaison Committee guidelines.

This document does not replace or supersede any existing Contracts, Tariffs or any other legally binding documents.

1.3 Definition

For the purposes of this document the term Service Provider is used to indicate both Access Service Providers (ASP) and Access Service Customers (ASC).

1.4 Document Organization

The remainder of this document is organized into the following sections:

- Purpose of Information Sharing
- Basic premises
- Criteria
- Operating principles
- Scope
- Service Provider responsibilities
- Vendor/Manufacturer responsibilities
- Information to be shared
- Modes of communication(s)

1.5 Purpose of Information Sharing

The purpose of information sharing as described in this document is to enable all service providers and vendor/manufacturers to utilize information uncovered by other service providers and/or vendor/manufacturers through the testing, validation and application of software, hardware, and documentation; procedural issues; and conformance to agreed upon standards in order to:

- Minimize the possibility of major outages and service interruptions that can affect our collective customers' service,
- Maintain and improve the reliability, security, capacity, and performance of our interconnected networks,
- Meet or exceed the expectations of our "customers".

Such information sharing may also serve to reduce the need for repetitive or redundant testing.

2 BASIC PREMISES

Telecommunications Service Providers and Vendors/Manufacturers have an obligation to their collective Customers to cooperatively provide assurance for the integrity of the public switched telephone network.

Information associated with testing and/or problem/failure scenarios of the network can and will provide invaluable assistance when shared with other Service Providers and/or Vendors/Manufacturers. The sharing and use of this information may:

- Minimize and/or prevent failures
- Minimize and/or prevent degradation of the network
- Minimize and/or prevent reoccurrence of the same problem in another network
- Assist in problem resolution

3 CRITERIA FOR SHARING INFORMATION

Information uncovered by any Service Provider or Vendor/Manufacturer which reveals the potential for loss of service or compromise in the reliability, security, capacity, or performance in a single network or interconnected networks should be proactively shared with those parties whose networks and/or products may be impacted by the problem.

4 OPERATING PRINCIPLES

The party(ies) identifying a problem should determine/agree on the source/cause of the problem prior to communicating the source/cause to other parties.

No party(ies) should divulge information concerning a problem/failure that is believed to be attributable to a Vendor/Manufacturer or Service Provider without first obtaining written permission to disclose such information from the Vendor/Manufacturer or Service Provider in question. The party(ies) uncovering an actual or potential problem are in a unique position to see that the problem is communicated to the appropriate parties and resolved. Although they may not bear responsibility for the problem and/or may not be in a position to actually share the appropriate information, the party(ies) uncovering a potential problem should assume a proactive role in encouraging those parties in a position to share the information to follow the guidelines outlined in this document.

Vendors/Manufacturers should research all troubles/issues referred to them to ensure that any similar or related troubles/issues in other platforms are addressed. In addition Vendor/Manufacturers should research all generic troubles/issues made available to the industry (e.g., IITP reports) to ensure that these anomalies are not replicated in their product(s) or platform(s).

Implementation of these guidelines represents a cooperative effort on the part of industry participants to assure the reliability and security of the interconnected telecommunications networks. It may occur that in the interest of

promoting network reliability, parties may exchange information about their networks/products that could be used in a negative fashion against that companies image, products or network. Use of such information for purposes of securing a competitive advantage is contrary to the spirit and intent of these guidelines. Misuse of information provided under these guidelines may jeopardize subsequent information exchange.

Each industry participant has an individual responsibility to develop and maintain procedures for reporting events related to network security.

5 SCOPE

The scope of this Document includes the exchange of information between the following parties:

- A Vendor/Manufacturer and its Customer(s)
- A Vendor/Manufacturer and its Customer and that Customer's interconnected
- Service Providers
- Vendors/Manufacturers
- Access Service Providers
- Access Service Providers and Access Service Customers

The exchange of information between the following parties is explicitly outside the scope of this Document:

- Access Service Customers/Providers and the FCC
- Access Service Customers

This Document is intended both to supplement existing practices and to establish new practices for information exchange.

The following list is intended to represent a complete list of sources of information for sharing. The identified sources include:

- Service Provider Stand alone Testing environment
- Compatibility testing between Service Providers
- Service Provider daily operations
- Service Provider outage reports and analysis
- Service Provider and/or Vendor/Manufacturer documentation
- Service Provider Security Reports and Analysis
- Vendor/Manufacturer development testing
- Vendor/Manufacturer trouble information reports and analysis
- Vendor/Manufacturer trouble resolution reports
- Observed ambiguities or differences in requirements interpretations

6 SERVICE PROVIDER RESPONSIBILITIES

This section describes the responsibilities of Access Service Providers and Access Service Customers in the area of information exchange.

Service Provider sharing of information is subject to the "General Operating Principles" described in Section 4 of this Document.

6.1 Service Provider Stand Alone Testing Environment

Any testing results obtained by the Service Provider that identify defects or potential defects with a Vendor/Manufacturer product should be communicated to the Vendor/Manufacturer within 1 business day of the completion of testing analysis.

Where conformance to accepted industry standards is in question the Service Provider should inform/consult with their Vendor/Manufacturer within 1 business day of such a determination.

6.2 Compatibility Testing Between Service Providers

Where compatibility testing between interconnected Service Providers identifies an incompatibility or problem due for example to translations, differences in software releases, software changes, network architecture, and/or differences in requirements interpretations between Vendor/Manufacturer products, they should work individually or cooperatively to ascertain the cause of the problem. Once identified they should initiate information sharing to potentially affected Carriers/Vendor/Manufacturers as per these guidelines.

6.3 Service Provider Daily Operation

Any problems encountered during the normal course of day-to-day operations that are identified as resulting in whole or part from problem(s) with the Vendor/Manufacturer's product should be communicated to the Vendor/Manufacturer within 1 business day of such a determination.

The information to be shared is described in Section 9.

Problems that are identified as other than a Vendor/Manufacturer's product and have the potential to cause loss of service or compromise in the reliability, security, capacity, or performance in an interconnected network should be communicated by the identifying Service Provider to potentially affected Service Provider(s). These problem should be referred within 1 business day of such a determination, or in the case of security, in accordance with internal company or inter company security procedures.

6.4 Service Providers

Where a breach of network security has been experienced and it has been determined to be a Vendor/Manufacturer Hardware/Software problem, the Service Provider shall notify their Vendor/Manufacturer in accordance with their internal company and inter-company security procedures.

6.5 Documentation

When the utilization of Standards or Methods and Procedures identifies a problem with Service Provider and/or Vendor/Manufacturer documentation that could result in the loss of service or compromise in the reliability, security, capacity, or performance of the network, should be reported to the issuing company. This problem should be referred within 1 business day, or in the case of security, in accordance with internal company or inter company security procedures.

The company that issued the methods and procedures should evaluate the identified problem and initiate a correction. The correction should be provided to all known users of the affected documentation.

7 VENDOR/MANUFACTURER RESPONSIBILITIES

This section describes the responsibilities of the Vendor/manufacturer in the area of information exchange.

Vendor/Manufacturer sharing of information is subject to the "Operating Principles" described in Section 4 of this Document.

7.1 Vendor/Manufacturer and Customer (Customer Reported)

Vendor/Manufacturers have the responsibility to promptly inform their Customers of known information relating to their product(s) which reveals the potential for loss of service or compromise in the reliability, security, capacity, or performance in the Customer's own and/or interconnected networks.

Vendors/Manufacturers should make available to a particular Customer all trouble report information reported by that Customer.

In addition, Vendors/Manufacturers can only share Customer specific information between Customers, provided that they have the permission of the Customer reporting the trouble to disclose such information. The format of this permission (e.g. written, verbal) is part of the Vendor/Manufacturer/Customer relationship.

If the situation allows, the Vendor/Manufacturer should also inform its Customers of the long-term or short-term solution to the problem at the time of informing them of the potential problem.

In the event that the Vendor/Manufacturer has not developed a solution at the time of notification, the Vendor/Manufacturer should inform its Customers of the action plan to avoid/correct the situation.

The information to be shared is described in Section 8.

7.2 Customer/Vendor/Manufacturer to Interconnected Service Providers

When a Customer/Vendor/Manufacturer recognizes that a problem related to a Vendor/Manufacturer's product has the potential to cause loss of service or compromise in the reliability, security, capacity, or performance in the network of an interconnected service provider, the Customer should notify the Vendor/Manufacturer. The reporting Customer and the Vendor/Manufacturer should jointly determine the nature of the information to be shared. The reporting Customer should initiate the information sharing process per these guidelines, or in the case of security, in accordance with internal company or inter company security procedures.

7.3 Vendors/Manufacturers

Although Vendors/Manufacturers do not directly share information, if a Customer determines that Vendor/Manufacturer to Vendor/manufacturer communication is needed to resolve an interoperability problem, the Customer should make such a request to the Vendors/Manufacturers involved. The Customer(s) of the Vendors should provide each Vendor/Manufacturer with the appropriate information to allow them to resolve the interoperability problem, and should actively participate in the joint Vendor/Manufacturer meetings.

7.4 Vendor/Manufacturer Discovered Problems

When Vendors/Manufacturers identify problems with their software or hardware that has the potential to cause loss of service or compromise in the reliability, security, capacity, or performance in the network(s) of a Customer(s), such information should be communicated to the customer within 1 business day.

If the situation allows, the Vendor/Manufacturer should also inform its Customers of the long-term or short-term solution to the problem at the time of informing them of the potential problem. In the event that the Vendor/Manufacturer has not developed a solution at the time of notification, the Vendor/Manufacturer should inform its Customers of the action plan to avoid/correct the situation.

The information to be shared is described in Section 8.

Where notification of a problem has taken place in regards to a network security violation issue, such information shall be shared by the Vendor/Manufacturer with all of their customers (where applicable) in accordance with their internal company and inter company security procedures.

7.5 Differences in Specifications Interpretation

Where industry standards are perceived to be ambiguous or flawed, and have the potential to cause loss of service, compromise in the reliability, security, capacity, or performance in the network of a Customer(s). The Vendor/Manufacturer implementing such standards should inform their Customer(s) in writing of their interpretation. The affected Vendors/Manufactures and or Service Providers should address the issue with the appropriate standards bodies.

8 INFORMATION TO BE SHARED BETWEEN VENDOR/MANUFACTURER AND CUSTOMER

Vendors/Manufacturers should share the following information with their Customers:

- Background: Introductory information on how the problem was identified and under what circumstances.
- Problem: Technical description of the problem.
- Service Impact: The actual or potential impact to service that the problem poses.
- Products/Generics Affected: A list of the products and generics/ releases that are affected by the problem.
- Interim Solution: When available, a description of how to recover the node or prevent the problem from occurring should be provided until a long-term solution is available.
- Contact: A single point of contact through whom the Customer can communicate regarding the problem for clarification, and/or request additional information.
- Resolution: A Customer view of what is being done to resolve the problem and when a solution might be generally available. This will probably not be available on initial notification, but will require subsequent updates to the Customer.

9 INFORMATION TO BE SHARED BETWEEN CUSTOMER AND VENDOR/MANUFACTURER

Customers should report to their Vendor/Manufacturers all known problem(s) and/or potential problem(s) associated with the Vendor/Manufacturer's product(s) based on agreements between the parties. For this information sharing purpose the Vendor/Manufacturers products include hardware, software, firmware and documentation.

The information provided is dependent on the nature of the problem. As such, not all of the items listed below may be applicable. The information provided for the problem or potential problem should/could include the following:

- Date: Date problem was encountered.
- Time: Time problem was encountered.
- Product: Specify which of the Vendor/Manufacturer's product(s) are involved.
- Priority: Severity of problem
- Problem Description: Complete description of the problem.
- Affected Sites: Location/Site identification.
- Services Impacted: Identify services impacted (e.g. Toll Free)
- Customer Impact: Describe end user and/or service provider impact (e.g. blocked calls).
- Actions Taken: Describe work around as applicable.
- Office Print outs: Maintenance terminal output or equivalent 1 hour prior to and 2 hours after the event or as requested.
- Product Version: Identify version of product(s) (e.g. software release level and patch level).
- Product Logs: Maintenance/error logs and measurements as specified in advance or as requested.
- Protocol data: If applicable
- Hardware: Provide suspected hardware information as requested.
- Contact: Service providers point of contact and phone number for issue resolution.

The timing of the sharing of this information is specified in section 6 of this document.

10 MODES OF COMMUNICATION

Established communication channels should be used wherever applicable. Changes to existing communication channels should be driven by the affected user organizations (e.g., technical support organizations).

Two modes of communication are recommended:

- Proactive notification
- Vendor/Manufacturer Electronic Message System

10.1 Proactive Notification Mode

In this communication mode the Vendor/Manufacturer or Service Provider should notify its Customers, interconnected Service Providers and or Vendor/Manufacturer(s) in accordance with the timing requirements defined in Section 6 or 7.

This mode of communication should be used either when there is imminent danger of an outage or significant impact known for the reliability, security, capacity or performance of network operation. When possible, it is desirable that the notification refer to additional related information (e.g., related trouble reports).

10.2 Vendor/Manufacturer Electronic Message System Mode

This mode of communication is applicable between Vendor/Manufacturers and their Customers.

In the Vendor/Manufacturers Electronic Message System communication mode, the Customer has the ability to receive/retrieve, prioritized trouble report information. How this communication mode is provided should be determined as part of the Vendor/Manufacturer Customer relationship. Examples include Vendor/Manufacturer systems and paper records.

11 FACILITY OUTAGE REPORTING GUIDELINES

It is recommended that companies that are directly interconnected should establish procedures, where they currently do not exist, for notification and information exchange in the event a facility outage (cable, fiber, microwave) occurs that directly impacts the other company.

It is recommended that the following information be exchanged upon notification of an outage to the directly interconnected company. This information should be exchanged upon detection of the outage or as soon as possible.

- Date And Time Of Outage
- Location
- Cause If Known
- Estimated Restoration
- Contact Name And Number
- Type Of Facility Outage (If Known)

Guidelines should be established to define minimum levels or thresholds for outage reporting. Minimum level recommendations:

- 30,000 customers or
- 90,000 blocked calls

It is also recommended that when service is restored, notification be provided to the companies impacted. The notification should be provided upon restoral of service. This notification should include the following information:

- Time Of Restoration
- Cause
- Temporary Solution Or Permanent Fix



ATIS-0300029

**Next Generation Interconnection Interoperability (NGIIF)
Reference Document**

Part VIII, Cable Locate Guidelines

Version 12.0



ATIS is the leading technical planning and standards development organization committed to the rapid development of global, market-driven standards for the information, entertainment and communications industry. More than 200 companies actively formulate standards in ATIS' Committees, covering issues including: IPTV, Cloud Services, Energy Efficiency, IP-Based and Wireless Technologies, Quality of Service, Billing and Operational Support, Emergency Services, Architectural Platforms and Emerging Networks. In addition, numerous Incubators, Focus and Exploratory Groups address evolving industry priorities including Smart Grid, Machine-to-Machine, Connected Vehicle, IP Downloadable Security, Policy Management and Network Optimization.

ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications' Sectors, and a member of the Inter-American Telecommunication Commission (CITEL). ATIS is accredited by the American National Standards Institute (ANSI). For more information, please visit www.atis.org.

Notice

This document was developed by the Alliance for Telecommunications Industry Solutions' (ATIS) sponsored Next Generation Interconnection Interoperability Forum (NGIIF). The NGIIF addresses next-generation network interconnection and interoperability issues associated with emerging technologies. Specifically, it develops operational procedures which involve the network aspects of architecture, disaster preparedness, installation, maintenance, management, reliability, routing, security, and testing between network operators. In addition, the NGIIF addresses issues which impact the interconnection of existing and next generation networks and facilitate the transition to emerging technologies. All changes to this document shall be made through the NGIIF issue resolution process.

Note Regarding Previous Versions

The NIIF Reference Document was formerly known as the Network Operations Forum (NOF) Reference Document. The NOF Reference Document was published and maintained by Bellcore. The last version of the NOF Reference Document is Issue 13.

Disclaimer and Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

ATIS-0300029, *NGIIF Reference Document, Part VIII, Cable Locate Guidelines*

The NGIIF Reference Document, Part VIII, Cable Locate Guidelines, is an ATIS standard developed by the NGIIF.

Published by

Alliance for Telecommunications Industry Solutions

1200 G Street, NW, Suite 500

Washington, DC 20005

Copyright © 2011 by Alliance for Telecommunications Industry Solutions

All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < <http://www.atis.org> >.

Printed in the United States of America.

CABLE LOCATE GUIDELINES

Table of Contents

1	GENERAL.....	3
1.1	PURPOSE.....	3
1.2	APPLICABILITY	3
1.3	DEFINITIONS	3
2	BASIC PREMISES.....	3
3	SCOPE OF THIS DOCUMENT	3
4	LOCATE ASSUMPTIONS.....	4
5	SERVICE PROVIDERS LOCATE GUIDELINES	4
6	ABNORMAL CONDITION PROCEDURES.....	5

1 General

1.1 Purpose

This document is intended to provide a set of guidelines that address industry concerns regarding the prevention of damage to the network caused by accidental damage to the Access Service Provider's or Access Service Customer's outside plant facilities.

1.2 Applicability

This document is intended to be a living document, and is therefore subject to revision and upgrading under the Carrier Liaison Committee guidelines.

This document does not replace or supersede any existing Contract(s), Tariff(s), State Law(s) or Regulations(s), or any other legally binding document(s).

1.3 Definitions

For the purposes of this document, the term Service Provider is used to indicate both Access Service Providers (ASP) and Access Service Customer (ASC).

The term Facility, as used in this document, describes buried plant to include but not be restricted to, Copper Cable or Fiber Optical Cable.

The term Call Before You Dig or CBUD, as used in this document describes a telecommunications entity operations center responsible for implementing the guidelines described in this document. The CBUD centers are commonly responsible for interactions with facility "One Call" agencies.

The term One Call, as used in this document describes an agency, a center, or an operator that performs the duties associated with the American Public Works Association (APWA) utility locate requests/referrals for all buried facilities, including telecommunications facilities.

The term Utility, as used in this document describes a public utility company, or consortium that delivers its service to the consumer public at large via buried facilities (e.g., electrical, gas, water, sewer, telecommunications, CATV, etc.).

LOCATE is a procedure that involves various mechanisms to identify telecommunications facilities deemed at risk. Notification may be to a One Call system, or directly to the individual Service Provider.

2 Basic Premises

Network Service Providers have an obligation to ensure that appropriate procedures are in place to proactively assure the integrity of buried facilities.

Other parties concerned with preventing damage to network facilities include One Call operators, construction and demolition companies and employees, and concerned telecommunications users.

3 Scope of this Document

The guidelines in this document address the following major areas of concern:

- Normal preventative measures. In most states, these are based on state laws that require prior notification of activity that has the potential to result in telecommunication cables being damaged.
- Emergency response to contractors who, for various reasons, failed to involve the organization responsible for LOCATE prior to beginning work in an unmarked area.
- Reactions to observations by Service Provider personnel that work has started, or is about to begin, in an area that has not been protected by required LOCATE practices.
- Reactions to observations by concerned telecommunications users that work is being performed in an area where they feel it is possible that utility facilities may not be protected.
- Recommendations for Service Providers who operate in jurisdictions that do not require mandatory notification programs.

4 Locate Assumptions

This section describes baseline assumptions/understandings that form the basis for the Service Provider guidelines.

As a result of state and local regulations, most areas are covered by an arrangement that provides a single contact, or "One Call," for parties to notify utilities of their intention to work in an area, and to request that the utilities LOCATE their facilities prior to the commencement of any work in that area.

In an area served by a One Call agency, any party proposing to conduct construction or demolition activities is expected to call the One Call agency and request a utility LOCATE be performed at the work site.

In an area not served by a One Call agency, the above parties should notify the individual utility directly. Many individual utilities maintain "Call Before You Dig" centers or CBUDs, to provide these services. In the case of telecommunications CBUD, the party should request a cable LOCATE at the site.

Network Service Providers should maintain, or be associated with, an organization that has the responsibility for interfacing with any party concerned with preventing telecommunication network damage.

Where local or state requirements do not exist, it is recommended that Service Providers at a minimum should adhere to the American Public Works Association recommendations for utility locating.

The One Call center will request specific information from the referring party as necessary to facilitate LOCATE and field meet procedures (e.g., contact name, company/individual reporting, site location, start date, activity being performed, field appointment information). The One Call center determines which utilities are to be notified and provides the referral information specifics to each affected utility.

5 Service Providers Locate Guidelines

On receipt of a request for LOCATE, the Service Provider shall make a record of the request for tracking and auditing purposes.

Service Providers shall be responsible for reviewing referral information to ensure that all necessary data is provided, and for contacting the referring party or the on site personnel for any corrections and/or clarifications.

The following information should be requested from the referring party:

- Name of the company (or individual) requesting the LOCATE service.
- Name and phone numbers for on site representatives, and if available, other back up information.

- Specific site location information, such as street address or map locations.
- Proposed start date of construction or demolition activities at the site.
- Descriptions of the type and extent of the activities to be conducted at the site.
- Dates and times available for a field meet, if required and/or requested.
- Provide any special site access information, such as site phone numbers, entrance locations, etc.

Service Providers' field representatives are required to verify the proposed field meet, coordinating any changes with the site contact.

Service Providers' field representatives shall follow company practices, state laws, or industry recommendations in visiting the site and locating and marking the facilities as required. It is recommended that this activity be performed at the same time as the field meet.

There are circumstances that may require special action by the LOCATE field representative. In these instances, it is strongly recommended that additional efforts, including frequent revisits and on site standby, be considered to protect the facilities. Examples of these circumstances are:

- The representative believes that the type of activities planned will harm the facilities.
- Facilities in the affected area contain priority, or critical, circuits and/or service.
- Contractors at the site have a history of ignoring cable locations and markings.
- Weather conditions such as mud, snow or rain require the remarking of facility locations
- The site is in an area subject to frequent vandalism.

Procedures should be in place to provide rapid response to emergency calls.

All telecommunication providers should participate in a cable LOCATE program in each geographic location. This can be accomplished as a stand alone operation of each Service Provider, or other owners of buried utilities, or it can be a coordinated effort including all utilities.

All incidences where cable damage has occurred should be reviewed monthly.

Regular meetings should be held with that group of contractors who are not contacting cable owner companies for cable LOCATE services and who are damaging the cables.

Major/significant buried cable routes should have cable warning signs requesting that you call before digging. These warnings should, at a minimum, conform to the American Public Works Association guidelines.

Call before you dig awareness programs should be in effect.

6 Abnormal Condition Procedures

In instances where calls are made to either CBUDs or One Calls reporting that site activity is underway that may cause damage to utility facilities, as much information pertaining to the site and the activities should be obtained from the caller.

The utility receiving the referral should ensure that this activity is not coincident with one already referred.

The entity receiving the referral, on determining that this is a new situation, should notify all other utilities.



ATIS-0300030

**Next Generation Interconnection Interoperability (NGIIF)
Reference Document**

**Part IX, Installation, Testing and Maintenance
Responsibilities of Facilities**

Version 12.0



ATIS is the leading technical planning and standards development organization committed to the rapid development of global, market-driven standards for the information, entertainment and communications industry. More than 200 companies actively formulate standards in ATIS' Committees, covering issues including: IPTV, Cloud Services, Energy Efficiency, IP-Based and Wireless Technologies, Quality of Service, Billing and Operational Support, Emergency Services, Architectural Platforms and Emerging Networks. In addition, numerous Incubators, Focus and Exploratory Groups address evolving industry priorities including Smart Grid, Machine-to-Machine, Connected Vehicle, IP Downloadable Security, Policy Management and Network Optimization.

ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications' Sectors, and a member of the Inter-American Telecommunication Commission (CITEL). ATIS is accredited by the American National Standards Institute (ANSI). For more information, please visit www.atis.org.

Notice

This document was developed by the Alliance for Telecommunications Industry Solutions' (ATIS) sponsored Next Generation Interconnection Interoperability Forum (NGIIF). The NGIIF addresses next-generation network interconnection and interoperability issues associated with emerging technologies. Specifically, it develops operational procedures which involve the network aspects of architecture, disaster preparedness, installation, maintenance, management, reliability, routing, security, and testing between network operators. In addition, the NGIIF addresses issues which impact the interconnection of existing and next generation networks and facilitate the transition to emerging technologies. All changes to this document shall be made through the NGIIF issue resolution process.

Note Regarding Previous Versions

The NIIF Reference Document was formerly known as the Network Operations Forum (NOF) Reference Document. The NOF Reference Document was published and maintained by Bellcore. The last version of the NOF Reference Document is Issue 13.

Disclaimer and Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

ATIS-0300024, NGIIF Reference Document, Part IX, Installation, Testing and Maintenance Responsibilities of Facilities, Formerly NIIF 5026

The NGIIF Reference Document, Part IX, Installation, Testing and Maintenance Responsibilities of Facilities, is an ATIS standard developed by the NGIIF.

Published by

Alliance for Telecommunications Industry Solutions

1200 G Street, NW, Suite 500

Washington, DC 20005

Copyright © 2011 by Alliance for Telecommunications Industry Solutions

All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < <http://www.atis.org> >.

Printed in the United States of America.

INSTALLATION, TESTING, AND MAINTENANCE RESPONSIBILITIES FOR FACILITIES

Table of Contents

1	GENERAL	5
2	RESPONSIBILITIES	5
2.1	ACCESS SERVICE CUSTOMER (ASC)	5
2.2	ACCESS SERVICE PROVIDER (ASP)	6
3	NETWORK SERVICE CENTER (NSC)	7
4	NETWORK MODIFICATION NOTIFICATION	7
5	FACILITIES INSTALLATION	8
5.1	FACILITY ORDER ACTIVITY	8
5.2	ESTABLISHING INTERFACE	8
5.3	PRE-SERVICE TESTING	8
5.4	COOPERATIVE ACCEPTANCE TESTING	8
5.5	DIGITAL ACCEPTANCE TESTING GUIDELINES	9
5.6	ACCEPTANCE OF DS-1	9
5.6.1	Performance Limits, Using QRSS (From ANSI T1.510)	10
5.6.2	Performance, Using Pattern Sensitive Testing AMI and B8ZS MATRIX	10
5.6.3	Long Term Performance Testing (From ANSI T1.510)	11
5.6.4	Line Code Option Verification	11
5.6.5	AMI/B8ZS Mismatch Testing	11
5.7	ACCEPTANCE TESTING OF DS-3 SERVICE	11
5.7.1	Test limits and objectives for 44.736 Mbit/s service (T1-510-1999)	11
5.8	DS-3 TESTING - OPTICAL INTERFACE	12
5.9	COMPLETIONS	12
5.10	FACILITY DISCONNECTS	12
5.11	FACILITY REARRANGEMENTS	12
5.12	COORDINATED CONVERSIONS	12
5.13	CHANGE ORDERS	13
6	FACILITIES MAINTENANCE	13
6.1	ROUTINE MAINTENANCE	13
6.2	POTENTIAL SERVICE AFFECTING ACTIVITIES	14
6.3	DEFERRED SERVICE RESTORATION	14
6.4	TROUBLE REPORTING	14
6.5	TROUBLE CLEARANCE REPORTING	15
6.6	SPECIALIZED TROUBLE HANDLING	15
6.6.1	Inoperative and Impaired Facilities	15
6.6.2	Chronic Facility Failures	16
6.6.3	Synchronization	16
6.7	ESCALATION	16
6.8	TROUBLE REPORT STATUS	16
6.9	SECTIONALIZATION AND REPAIR	17
6.10	MAINTENANCE OF DS-1 SERVICE	17
6.10.1	AMI and B8ZS MATRIX	18
6.11	CHRONIC TROUBLE OF DS-1 SERVICE	18
6.12	MAINTENANCE OF DS-1 SERVICE WITHIN A DS-3 SERVICE	19
6.13	MAINTENANCE TESTING OF DS-3 SERVICE	19
6.14	DS-3 TESTING - OPTICAL INTERFACE	20
6.15	FACILITY RESTORATION PROCEDURES	20
6.16	MAINTENANCE MAKE-BUSY PROCEDURE FOR FACILITIES	20

6.16.1	Facility Make-Busy (Facility Failure)	20
6.16.2	Maintenance Removal from Service.....	20
6.16.3	Expedited Make-Busy Procedure for Facilities	20
6.17	VERIFICATION TESTS.....	21
6.18	END TO END INTERCARRIER TESTING.....	21
7	ADDITIONAL BILLING	21
7.1	BILLABLE OVERTIME INSTALLATION AND REPAIR	22
7.2	ADDITIONAL COOPERATIVE ACCEPTANCE TESTING (ACAT).....	22
7.3	NON-SCHEDULED TESTING.....	22
7.4	MAINTENANCE OF SERVICE CHARGE.....	22
7.5	STAND-BY TIME	22
7.6	OTHER LABOR	22
8	FACILITIES PROVIDED BY MULTIPLE EXCHANGE CARRIERS.....	22
8.1	INSTALLATION.....	23
8.2	COMMON COMPLETION	23
8.3	JEOPARDY.....	23
8.4	MAINTENANCE	23
8.4.1	Trouble Report Exceptions.....	25
8.4.2	Request for Test Assistance.....	25
8.4.3	Request for Escalation Assistance from ASC.....	25
9	OPTIONAL DS-1 TEST PATTERNS	26
9.1	BACKGROUND – CCITT / ITU-T TEST SIGNALS, OTHER TESTS, AND TEST SIGNALS	26
9.1.1	2^{15} -1 32,757-bit PRBS ^{note 1} test pattern (Inverted) ^{note 2}	26
9.1.2	2^{20} -1 1,048,575-bit PRBS test pattern ^{note 2}	26
9.1.3	2^{23} -1 8,388,607-bit PRBS test pattern (Inverted) ^{note 2}	26
9.1.4	1-IN-16 (1:15) A single ONE bit followed by fifteen ZERO-bits.....	26
9.1.5	55-Octet Stress Test Pattern	26

1 General

This document outlines Access Service Customer (ASC) and Access Service Providers (ASP) responsibilities for Installation, Testing and Maintenance of Facilities as established by the Network Interconnection Interoperability Forum (NGIIF). It is intended to be a living document to aid operations work forces. It does not replace nor supersede Tariffs, Contracts or any other legally binding documents.

The installation and maintenance of SS7, Specials and Feature Group A, Feature Groups B, C, and D are included in separate sections of the NGIIF Reference Document. In addition, Network Management Guidelines and Testline Guidelines are included as well.

In addition to other operational and technical agreements made at the Network Interconnection Interoperability Forum, this document is being issued to incorporate the following changes.

This document is a new addition to the Network Interconnection Interoperability Forum library of documentation, exclusively for Facilities.

The ASCs are communications common carriers authorized by the appropriate regulatory bodies, the Federal Communications Commission (FCC) to provide interLATA, interstate communications and/or by State or Provincial Public Utilities Commissions (PUCs) to provide interLATA, intrastate or intraLATA communications to their end users. The ASCs may request Access Service Providers (ASP) to provide various facilities as addressed in this document to be used as part of the ASC's services. The fundamental principles governing the relations between the ASPs and the ASCs are:

The ASCs have responsibility for the end-to-end service of their end users.

The ASPs will provide facility connectivity to the ASCs as set forth by their Access Service Tariffs and will show no discrimination between different ASCs.

2 Responsibilities

This section outlines the responsibilities for Access Service Customers (ASC) and Access Service Providers (ASP).

2.1 Access Service Customer (ASC)

The ASC has the overall installation and maintenance responsibility for the total facility to its end user. The ASC is responsible for the overall coordination of installation and testing of its facilities. The ASC is responsible for negotiation of control to another entity.

The following are the responsibilities of the ASCs:

- Provides trained personnel.
- Advises the ASP when there is an ASC network failure that may affect the ASP services.
- Provides a contact number for trouble reporting that is readily accessible 24 hours a day, 7 days a week.
- Maintains complete and accurate installation and repair records.
- Provides ASP personnel access to the Point of Termination (POT) when required.
- Provides access to testlines where appropriate.
- Provides billing authorization to the ASP for any additional labor requested.

- Ensures the test equipment used is compatible with the ASP's test equipment.
- Cooperates with the ASP ensuring that facilities are installed in accordance with the service requests.
- Notifies the ASP of any changes affecting the service requested, including the service due date.
- Assumes control functions for maintenance of its facilities.
- Consulting with the ASP before making any changes that would affect service except under emergency conditions.
- Accepts trouble reports from their end users.
- Accepts trouble reports from the ASPs.
- Sectionalizes and clears the trouble in its own network.
- Test cooperatively and with the ASP to further isolate and clear the trouble.
- Keeps their end user advised of the status of all trouble report(s).
- Performs cooperative analysis to determine if a trouble pattern exists.
- Refers troubles to the ASP using the trouble reporting procedures.
- Dispatches its own maintenance forces.
- Performs verification test to ensure that trouble has been cleared.
- Performs scheduled testing and other maintenance services when requested.
- Participates cooperatively with the ASP to further isolate and clear the trouble when trouble exists and cannot be sectionalized.

2.2 Access Service Provider (ASP)

The ASP is responsible for ensuring that the facilities furnished to an ASC are installed and function properly. In addition, the ASP should work cooperatively and with the ASC in the testing of the facilities it provides.

The following are the responsibilities of the ASPs:

- Provides trained personnel.
- Advise the ASC when there is a potential service affecting ASP network failure.
- Provides a contact number for trouble reporting that is readily accessible 24 hours a day, 7 days a week.
- Maintain complete and accurate installation and repair records.
- Consults with the ASC before making any changes that could affect service except under emergency conditions. (See Network Modification section).
- Provides access to testlines where appropriate.
- Assumes control functions for the installation of the facilities.
- Coordinates with the ASC ensuring that facilities are installed in accordance with the service requests.
- Notifies the ASC of any changes affecting the service requested, including the service due date.
- Accepts trouble reports from the ASCs.

- Sectionalizes and clears the trouble in its own network.
- Test cooperatively with the ASC to identify and clear a trouble when the trouble has been sectionalized to an ASC network.
- Performs cooperative analysis to determine if a trouble pattern exists.
- Refers troubles to the ASC using the trouble reporting procedures.
- Dispatches its own maintenance forces.
- Performs verification tests to ensure that trouble has been cleared.
- Provide status reports to the ASC regarding installation and repair activity.
- Perform scheduled testing and other maintenance services when requested.
- Participates cooperatively with the ASC to further isolate and clear the trouble when trouble exists.
- Provides ASC personnel access to the Point of Termination (POT) when required.
- Ensures that test equipment used is compatible with the ASC's test equipment.

3 Network Service Center (NSC)

The NSC, or other regionally designated centers, will be the contact point for non-circuit specific trouble reports from the ASC. The ASP will provide the ASC with a contact number, escalation and guidelines for reporting of non-circuit specific troubles. The NSC will provide status and feedback to the Reporting ASC, when requested.

4 Network Modification Notification

A Network Modification is any type of planned equipment, software, trunk or facility activity that has the potential to significantly affect interconnected networks (e.g. rearrangement of existing network elements, switch homing arranges, SS7 rehomings)

The NGIIF has developed the following guidelines outlining the medium by which internetwork affecting maintenance activity notification will be provided to the interconnected company and the time frame prior to the planned activity:

Notification when possible should be made at least 5 working days prior to the planned change activity.

Notification should be made in the form of:

- E-Mail (recommended where available),
- FAX or,
- Telephone call.

Notification should be provided to the affected company's appropriate notification center. Contact information is included in the NGIIF Service Provider Contact Directory. An example of a notification form is located in the NM Section, Part VI, of the NGIIF Reference Document.

When network modifications are scheduled that could significantly affect traffic between directly interconnected networks, it is recommended that the affected ASPs and ASCs will notify each other, prior to the event.

The following information should be exchanged at the time of notification:

- Originator, (company name/contact number)
- Affected Network Element
- Date and Time of the Change
- Expected Duration
- Traffic Types Affected During Change
- Description of the Work to be Completed

5 Facilities Installation

5.1 Facility Order Activity

The ASC will order from each ASP the required facility through their Interexchange Customer Service Center (ICSC) or equivalent organization. The ICSC or equivalent is an Access Service Negotiation work group that will handle inquiries and orders. It is to serve as a point of contact for the access service order needs of Interexchange Customers. During the installation period ASP order number will reference all inquiries.

Each of the ASPs will negotiate facility due date intervals, either on a standard or individual case basis. Ordering procedures are described in the Access Services Tariff.

5.2 Establishing Interface

The point of connection between the ASP and the ASC facilities or equipment is referred to as the Point of Termination (POT). It is the responsibility of the ASC to arrange for suitable equipment space and electrical power, if required, at the POT. The space furnished shall be in a safe working area and will be accessible during normal working hours to ASP personnel for installation and maintenance purposes or ASC personnel will be available to work with ASP personnel.

5.3 Pre-service Testing

Each company is responsible for that portion of the overall facility that they are providing. Each company must ensure that its facility segments have been installed correctly, prior to cooperative acceptance testing being performed, i.e.:

- The facility has been installed correctly.
- The pre-service tests have been performed and the requirements met.
- Records of the tests and their subsequent results have been documented.

5.4 Cooperative Acceptance Testing

The ASC has the option of accepting the facilities with or without cooperative acceptance testing on or before the due date. Prior to the due date, the Access Service Provider (ASP) will contact the ASC and advise when the facility will be ready for turn up. If the ASC requests cooperative acceptance tests, the ASP will schedule a mutually agreeable date and time and coordinate all normal and additional (as specified on the order) acceptance testing. The ASP and the ASC will verify test equipment compatibility at this time.

At the time of acceptance testing, the ASP personnel will not test directly with the ASC unless otherwise directed. Once the acceptance tests have been completed on the new facilities, the ASP will disable the termination to these facilities preventing false selection and seizures of these facilities until the due date. It will be necessary for the ASC to coordinate with the ASP for the turn up of the facility.

When the ASP deploys a DS-1 loopback device, the subsequent dispatch to the End User's POT to perform "Cooperative Acceptance Tests" will be waived by the ASC. The ASC, upon request, will be provided with the test results from the ASP. If the ASC requests "Cooperative Acceptance Testing" be performed, they will be performed remotely. Excluding the following conditions, an ASP technician will not normally be dispatched to the End User's premises to perform tests. The conditions are:

- The DS-1 Service is not equipped with the DS-1 loopback device.
- The test results do not meet service acceptance immediate action limits and the trouble is sectionalized to the ASP network.
- The loopback unit is inoperable.
- Unless the ASC requests a dispatch.

The test results will be viewed as valid (assuming they are within service parameters) for the purpose of service acceptance/maintenance.

When the ASP deploys Intelligent NCTE, the dispatch to perform "Cooperative Acceptance Tests" will be waived by the ASC.

The ASC, upon request will be provided the remotely assigned test results obtained by the ASP. If the ASC requests "Cooperative Acceptance Testing", the ASP will test remotely, using the diagnostic features of the Intelligent NCTE. Excluding the following conditions, an ASP technician will not normally be dispatched to the end user's location to perform "Cooperative Acceptance tests". The conditions are:

- The unit is not equipped to perform basic turn-up tests.
- The ASC requests specific Additional Cooperative Acceptance tests i.e., conditioning.
- The Intelligent NCTE is inoperable.
- The facility does not meet acceptance parameters.

5.5 Digital Acceptance Testing Guidelines

The purpose of this section is to serve as a guide for Installation & Maintenance personnel in determining when the digital acceptance testing guidelines would apply.

When the ASP receives a work order that provides Switched Access Service FG B, C or D to a digital switch, the facility design should be reviewed to determine whether Digital to Analog (D/A) conversion takes place on the ASP(s) side of the POT. When the design shows no D/A conversion on the ASP(s) side of the POT, Digital Acceptance Tests are preferred. If the ASP has D/A conversion, the final choice of which acceptance tests are performed remains with the ASC. This determination will be made at the time cooperative acceptance testing is scheduled.

5.6 Acceptance of DS-1

Acceptance testing for DS-1 Service should be performed on a POT to POT basis using Errored Second Performance Parameters. This test is typically performed utilizing a Quasi Random Signal Source (QRSS). In addition to QRSS, the 3/24 and 1/8 and All ones Test Patterns are acceptable diagnostic stress tests for DS-1 Service. These tests are not mandatory but will be performed, upon request, according to the AMI/B8ZS testing Matrix. It is recognized, that not all locations will have the test equipment to perform these tests. In these

instances, appropriate loopback techniques should be utilized. It should also be recognized, that some Network elements may not be transparent to these test patterns. Normal signaling test patterns should be framed. However, due to test equipment limitations, Unframed patterns may be sent, per local agreements, between the ASPs and ASCs.

Frame bit and Pattern bit phase verifications may occur after some test equipment frames these defined patterns. This may result in alarm and/or excessive (0s) zeros indications.

In addition, it is recognized that no single or multiple group of patterns i.e., AMI and B8ZS Matrix can detect all possible troubles. Additional tests may be required, using other patterns to detect certain troubles i.e., Bridge Tap.

5.6.1 Performance Limits, Using QRSS (From ANSI T1.510)

15 minute objective = 0 ES

If errors are observed, continue the test for an additional 15 minutes:

30 minute objective ≤ 3 ES

If more than 3 ES are observed, continue testing for an additional 15 minutes:

45 minute objective ≤ 5 ES

The service performance shall be considered acceptable if 0 ES are observed in 15 minutes, or 3 ES or less are observed in a total of 30 minutes, or if 5 ES or less are observed in a total of 45 minutes of testing. It should be noted that an isolated error event is not necessarily indicative of a service affecting problem.

5.6.2 Performance, Using Pattern Sensitive Testing AMI and B8ZS MATRIX

Test Pattern	Applicable Line Code	Binary Representation (Note 1)	Test Interval	Errored Second Limit
All 1s	All	F11111111 11111111 11111111....F	5 min	0
3 in 24	AMI only	F01000100 00000000 00000100....F	5 min	0
1 in 8	All	F01000000 01000000 01000000....F	5 min	0
All 0s (Note 2)	B8ZS only	F00000000 00000000 00000000....F	30 sec	(Note 3)

(Guidelines for the use of these patterns are found in ATIS/ECSA Technical Report #25 Test Patterns for DS1 Circuits)

Note 1: F represents the framing bits; the bit patterns repeat as indicated to complete the 192-bit payload of the frame. All binary representations are transmitted left to right.

Note 2: Some DS-3 multiplex equipment may cause multiple DS-1 failures if the equipment is not properly optioned. This pattern should be applied only in the sequence recommended in the Job Aid (Figure 2).

Note 3: Incorrectly optioned equipment will be indicated by large errors counts. Low error counts, e.g., 1 or 2 errors, are not indicative of an optioning problem.

Note 4: 2 in 8 F01000010 Bit 2+7=1 while not defined in ANSI T1.510, the use of this pattern is for line code option verification as detailed in ATIS/ECSA, Technical Report 25, and is not required for Acceptance Testing

5.6.3 Long Term Performance Testing (From ANSI T1.510)

Long term testing is optional, and it is performed remotely. The objectives for a 24 hour long duration test are:

$$ES \leq 150 \quad \quad \quad SES \leq 7$$

5.6.4 Line Code Option Verification

Pattern Sensitivity Testing is recommended to verify that line coding equipment is properly optioned for either AMI or B8ZS line codes. Figure 1 and Figure 2 provide guidelines on the sequence to be used to uncover optioning problems using pattern testing.

5.6.5 AMI/B8ZS Mismatch Testing

The following is an optional test that can be used to identify the existence of AMI/B8ZS mismatches on interconnected facilities:

AMI/B8ZS Mismatch Test

Procedure	Termination	Duration	Threshold
Simultaneous impulse noise test	0db looparound	30 seconds	<10 hits (60dBmC0)
(on adjacent channels 12 & 13)			<10 hits (64dBmC0)
			<10 hits (68dBmC0)

5.7 Acceptance Testing Of DS-3 Service

This procedure is in lieu of DS-1 tests performed on the 28 individual DS-1's within the DS-3. Perform one 1 hour test from DSX-3 to DSX-3 (or equivalent) using Framed Format.

Up to two sequential 1-hour stages shall be conducted to validate the general performance of the service. The service performance shall be considered acceptable and the test terminated if, after 1 hour, the test results for all parameters do not exceed the limits for the 1-hour tests in table below. The service performance shall be considered unacceptable if any test result is greater than the 2-hour limit. If the test result is between these two limits, continue the test. After 2 hours the service performance shall be considered acceptable if the test results do not exceed the limits for the 2-hour test. The service performance shall be considered unacceptable if any test result is greater than the 2-hour limit. Testing for longer periods such as 24 hours or continuous monitoring will provide greater confidence and should be considered for marginal

5.7.1 Test limits and objectives for 44.736 Mbit/s service (T1-510-1999)

		Short-Duration test				Long-Duration test	
		(15 minute stages)				(24 hours)	
		ES		SES		ES	SES
Parameter							
limits for	1 hour	2 hour	1 hour	2 hour		24 hour	24 hour
Access	=/ < 4	=/ < 8	0	=/ < 2 (see note)		=/ < 80	=/ < 7
Transit	=/ < 4	=/ < 8	0	=/ < 2 (see note)		=/ < 80	=/ < 16
End to End	=/ < 8	=/ < 16	0	=/ < 2 (see note)		=/ < 160	=/ < 21

NOTE: Accept at 2 only if the cause of the SES is identified as an isolated event

5.8 DS-3 Testing - Optical Interface

In the case of an optical interface, where the DS-3 is transported via fiber, the Fiber Optical Interface is located at or beyond the ASC and/or End User POT, cooperative testing should be performed to ensure that the facility meets the performance criteria. The facilities at the POT are tested in accordance to the manufacturer's guidelines for the Fiber Optical Termination equipment installed.

5.9 Completions

Upon acceptance of the facility order by the ASC, the ASP shall record the ASC representative's name and the basis of the acceptance.

Cooperative Acceptance Testing

Automatic tests, where available

Without acceptance testing

The ASP should report the order as completed and furnish all the required information to the ICSC or equivalent. ASPs will provide to the ICSC or equivalent any additional labor charges.

5.10 Facility Disconnects

Prior to performing disconnect activity the ASC and or ASP should be contacted for order coordination. When the facilities are removed from service and translation messages entered, order tracking documents should be updated and the ASP notified.

5.11 Facility Rearrangements

Any facility rearrangement or reassignment by the ASC and or the ASP shall be communicated to ensure that minimum impact to service is experienced. If, however, the rearrangement can be accomplished solely by the ASC and or the ASP, requests for facility make busy will be handled as specified in Section 7.

A sufficient time period should be agreed upon for all entities to complete rearrangement work and appropriate tests. Credit allowance rules will only apply when facilities are out of service for a duration that exceeds this period due to ASP caused problems.

Upon completion the ASP and ASC will perform cooperative tests to determine if the rearrangement was successful. If the rearrangement affects transmission parameters, both entities will cooperatively verify that the facilities are within acceptance limits.

5.12 Coordinated Conversions

Coordinated conversion is a process that may be used to facilitate a change in service from one to another that involves the reuse of a portion of the ASP provided equipment and/or facilities previously assigned to the services being converted. It requires the issuance and processing of related disconnect and connect orders and coordination of these orders throughout the entire cutover process.

Note: In some cases, the new Interconnecting Company and Former Interconnecting Company could be the same entity (e.g., when an Interconnecting Company rehomes an Access Service to a new Point of Termination).

The new Interconnecting Company is expected to bear full responsibility for the overall installation and coordination of the various service orders and all related activities involved in the provision of its end-to-end service. The actual ASP work operations performed remain under control of the ASP, according to mutually agreed upon schedules.

The new Interconnecting Company will establish and coordinate conversion activities with the ASP, former Interconnecting Company and End User when required. Those activities will include but are not limited to:

- Completion Testing and Notification
- Requests for Continuation of Service
- Conversion Timing
- Trunks Release
- Trunks Conversion Sequence

Every effort must be made jointly by the new ASC and the ASP to successfully complete the conversion. If the new ASC encounters difficulties in activating its end-to-end service after work has begun or acceptance tests have been completed on the ASP provided facilities, the new ASC may negotiate and coordinate continuation of the use of the previous arrangement with the ASP and former ASC, and restoral procedure should commence. Since continuation of the former ASC service does not automatically defer the due date of the disconnect order, the new ASC must request the former ASC to contact the ASP ICSC, or equivalent, to request a due date change in order to prevent the disconnect of the former ASC service. This must take place prior to the disconnect due date.

It is the responsibility of the ASP to inform the ASC initiating the conversion that all work involved in restoring the former ASC's service and subsequent cut-over activities of their facilities is work over and above that required for normal coordinated conversion cut-overs. This work may result in appropriate additional labor charges.

5.13 Change Orders

Change orders cover any changes in the design or operation of an existing facility or group of facilities administered through the ICSC or equivalent center procedures.

6 Facilities Maintenance

Maintenance is made up of two different elements; preventive maintenance and repair. Preventive maintenance is made up of routine (scheduled) maintenance and non-scheduled maintenance. Repair is the correction of troubles identified by customers, employees, machines and other telecommunication companies.

The ASC is responsible for performing all necessary tests to determine the nature of the trouble. If the trouble is found to be in the ASP provided service, the ASC will report the trouble to the appropriate ASP or the designated trouble reporting office.

The ASP will be responsible for accepting from the ASC the trouble report sectionalized to the ASP facilities. The ASP will test cooperatively or independently to assist in trouble sectionalization.

6.1 Routine Maintenance

Routine Maintenance is defined as preventive maintenance or work activities that, under normal circumstances, do not adversely affect interconnected networks. Where possible, routine maintenance should occur during maintenance windows (e.g., off-normal hours, 11:00 PM-5:00 AM).

6.2 Potential Service Affecting Activities

Other maintenance and scheduled work activities that can adversely affect interconnected networks should be performed during hours of minimum traffic (e.g., during an 11:00 PM to 5:00 AM "maintenance window") so that any inadvertent failure impacts the least number of customers.

At a minimum, high risk, potentially service-affecting activities, such as growth procedures and generic issue changes should be scheduled during weekend and off-hours. The overall methods, procedures and scheduling of these work activities should be reviewed by a second tier maintenance organization.

The activities that may affect other interconnected networks must be coordinated. (See NGIIF Reference Document, Part III, Installation, Testing and Maintenance Responsibilities for SS7 Links and Trunks)

6.3 Deferred Service Restoration

If customer service is impacted and total restoration would adversely affect the network, efforts will be devoted to re-establish at least a minimum level of acceptance as soon as possible. Total restoration will be cooperatively scheduled no sooner than the next maintenance window period.

6.4 Trouble Reporting

The NGIIF recommends immediate reporting of non circuit-specific troubles via telephone in order to facilitate the rapid restoral of service.

The following information should be mutually exchanged between the ASCs and ASPs:

- ASP facility identification number at the POT or equivalent. Where this is not available, local alternatives should be established and used.
- Date and Time of reported trouble
- Nature of the trouble
- The name or initials and the telephone number of the person referring the trouble
- The trouble report number(s) or equivalent and the name or initials of the person accepting the trouble
- Any other information that may be of assistance to the ASP, for example, what test have been made

When ASPs and ASCs are using different methods of in-service Performance Monitoring (i.e., scanned vs. dedicated), differences will occur in measured performance. The performance reported by the provider using dedicated monitoring will be more indicative of the total service. These reports should be accepted by the other company.

The ASP will coordinate the isolation of the trouble within the ASP provided service.

Communication may also be necessary on services that involve an ASC, their intermediate agent, and an ASP. In these situations the cooperation of all three organizations may be necessary to expedite trouble clearance. When it is necessary for communication between the ASP and ASC, it is required that the contact be made through the intermediate agent.

The ASP employees will limit their repair activities to ASP provided facilities. No attempt should be made to adjust or repair equipment belonging to the ASC. The ASC or others may not rearrange, move, disconnect, remove or attempt to repair any facilities provided by the ASP.

6.5 Trouble Clearance Reporting

Upon repair of the trouble, the ASP or the ASC should report to the trouble originator the specific parameters that were out of tolerance and the repair action taken, including the tested performance results of the repaired or modified parameters.

When trouble reports are being closed out between an ASP and an ASC, whether they are using a mechanized system or a verbal notification, the disposition should be furnished by the company clearing the trouble. The following information shall be provided:

- Facility Identification number
- Trouble Report Number (ASC/ASP number)
- Name or initials of person closing out trouble
- Nature of the trouble found (e.g., bad cable)
- Resolution details (e.g., cut to new cable)
- ASC will inform ASP if this trouble is measured
- Date and time trouble cleared
- Date and time trouble referred from the ASC to the ASP
- Date and time trouble report closed
- No access time (the period of time that the service is unavailable for maintenance activities)
- Service charge information, if applicable
- Status of facility (working or made busy)

When there is disagreement on the nature of the trouble found, the parties engaged in the dispute shall document their respective positions, and the names of the individuals engaged in the dispute for audit purposes and then close the trouble report. Escalations if necessary shall be in accordance with identified procedures.

When a trouble has been cleared and either the ASP or ASC requests to change the nature of trouble found, such changes shall be negotiated.

6.6 Specialized Trouble Handling

6.6.1 Inoperative and Impaired Facilities

When ASP or ASC personnel become aware of an inoperative facility, they will ensure that the facility is removed from service and cannot be accessed from either direction. The ASP or ASC detecting the inoperative condition will then sectionalize and repair or refer the trouble.

When ASP or ASC personnel become aware of an impaired facility, the removal from service of such facility shall be determined by the Interconnected Company.

If the maintenance of such facility is delayed a mutually agreed upon time should be determine for removal from service and sectionalization.

6.6.2 Chronic Facility Failures

Investigation of chronic facility failures will involve exchange of information relative to the chronic failure and a detailed investigation should be made to determine the cause of the trouble condition. This activity may involve cooperative testing and should be handled as an impaired facility trouble report.

If the ASC determines that a DS1, including a DS1 riding a DS3, is experiencing chronic trouble (more than or equal to 3 reports per month), the ASC will request the ASP to provide continuous performance monitoring on its portion of the DS1, in order to locate the offending network element. As part of the long term cooperative test arrangement, the ASC and ASP shall share the detailed performance monitoring data (15 min. and 24 hr.) with each other. Where non-intrusive performance monitoring equipment is not available, other methods of trouble isolation should be agreed upon. Prior trouble report information should also be shared between the ASC and ASP.

6.6.3 Synchronization

Improper synchronization can result in circuit impairments that should be investigated and synchronization problems corrected. Problems that cannot be resolved should be referred to your Synchronization Coordinator. The NGIIF publishes a Service Provider Contact Directory that contains the number to reach the Synchronization Coordinator. This is updated, as required, and is available from your companies NGIIF representative.

If the ASC/ASP has its own primary frequency standard that meets the CCITT standard for national networks (G.811, G.822), synchronization of the digital SS7 link(s) will be by the plesiochronous method of operation. If either network does not conform to the CCITT standard, the non-conforming company will use loop timing to accept SS7 link(s) timing from the conforming company. When the link interface is a DSOA interface, the interface must be plesiochronous or timed to the same source as the facility.

6.7 Escalation

Escalation is a means of bringing provisioning and maintenance problems to the attention of individuals responsible for or having appropriate authority to initiate corrective action. When the ASC or the ASP is experiencing provisioning or maintenance difficulties that are not being resolved, the ASC or the ASP shall contact the designated reporting office and request status from the responsible technician or first level supervisor. When either the ASC or the ASP experiences installation or maintenance difficulties and progress toward resolution is not satisfactory, either company may contact the other company for escalation to a higher level of management.

6.8 Trouble Report Status

The ASC and/or ASP receiving the initial trouble referral shall provide a status on the disposition of that referral based on local agreements negotiated at the time of referral or requested on an individual case basis.

Subsequent to the initial status report on the disposition of the trouble report periodic statuses shall occur based on the following criteria:

- When the trouble has been isolated
- When there is a significant change in the status of the trouble.
- When the negotiated status interval has expired.

Where mechanized trouble notification is utilized the receiving company shall status their systems based on the above paragraphs. In addition, it shall be the responsibility of the company issuing the trouble report to poll the mechanized status system for the status of the trouble report.

6.9 Sectionalization and Repair

Sectionalization is the joint responsibility of the ASP and ASC. The ASC will be responsible for coordination of the sectionalization of the facility in trouble. It is anticipated that the sectionalization may involve cooperative testing and in the interest of maintaining continuity of service, both entities are expected to participate in this activity when requested. In cases where the POT location is not normally staffed, the entity responsible for sectionalizing the trouble will arrange for cooperative testing or dispatch as required.

If the trouble sectionalizes to the originating ASP side of the facility, they shall perform the functions listed below. If the trouble is sectionalized to the terminating ASC side of the facility, they shall perform the functions listed below:

- Repair the trouble.
- Perform tests (cooperatively with the terminating entity if necessary) to determine if the trouble is cleared. If the trouble found affects other transmission parameters, both entities will cooperatively verify that the other transmission parameters are within maintenance limits.
- Participate in making any necessary adjustments to correct the transmission levels.
- Return the facility to service and notify the other entity if required.

The ASP should coordinate the isolation of the trouble within the ASP provided facilities and/or equipment and should minimize the dispatch of technicians.

The ASPs employees will limit their repair activities to ASP provided facilities and/or equipment. No attempt should be made to adjust or repair terminal equipment belonging to the ASCs. The ASC or others may not rearrange, disconnect, move or attempt to repair any equipment or facilities provided by the ASP.

In order for an ASC to perform maintenance testing, it may be necessary for the ASC to request that the ASP have the facility removed from service. Additional communications may be necessary concerning the removal of facilities that involve an ASC, their agent and an ASP. When it is necessary for communication between the ASC and ASP it is required that this contact be made through the agent. In these situations the cooperation of all organizations may be necessary to expedite trouble clearance.

Cooperative repair verification tests will be performed when deemed necessary or when requested. The ASP will not normally dispatch an employee to make verification tests when a trouble has been cleared without dispatching, however, there may be cases when dispatch is necessary.

When repair verification tests identify a trouble that was masked by the original trouble, clearance activity will continue until the service is restored.

6.10 Maintenance of DS-1 Service

Maintenance testing for DS-1 Service should be performed on a POT to POT basis using Errored Second Performance Parameters. This test is typically performed utilizing a Quasi Random Signal Source (QRSS). In addition to QRSS, the 3/24 and 1/8 and All ones Test Patterns are acceptable diagnostic stress tests for DS-1 Service. These tests are not mandatory but will be performed, upon request, according to the AMI and B8ZS Matrix below. It is recognized, that not all locations will have the test equipment to perform these tests. In these instances, appropriate loopback techniques should be utilized. It should also be recognized, that some Network elements may not be transparent to these test patterns. Normal signaling test patterns should be framed. However, due to test equipment limitations, Unframed patterns may be sent, per local agreements, between the ASPs and ASCs.

Frame bit and Pattern bit phase verification may occur after these defined patterns are framed by some test equipment. This may result in alarm and/or excessive (0s) zeros indications.

It is recognized that no single or multiple group of patterns i.e., AMI and B8ZS Matrix can detect all possible troubles. Additional tests may be required, using other patterns to detect certain troubles, i.e., Bridge Tap. Optional DS-1 Test patterns may be found in Section 9 of this document.

Maintenance problems sectionalized to HiCap (DS-1 or DS-3) facilities carrying the Switched Access Service/Special Access Services should be tested using the maintenance parameters/matrix indicated below.

Repair verification measurements are made upon completion of a repair activity. Threshold levels for these tests are the same as acceptance test levels to ensure that a circuit will meet specified performance levels.

6.10.1 Abbreviated Acceptance Testing for DS-1s

Upon the repair of a circuit the Designed Service repair tester should clear the span performance monitor registers, run the quick test, retrieve the performance monitor results and if no errors have occurred contact the customer to return service to them. In the conversation with the customer they should ask to hold the ticket for 30 minutes to retrieve the performance monitor results again and if clean to close the ticket at that time or if the customer requests hold it for 24 or 48 hours for service assurance.

6.10.2 AMI and B8ZS MATRIX

<i>Test Pattern</i>	<i>Applicable Line Code</i>	<i>Binary Representation (Note 1)</i>	<i>Test Interval (Note 4)</i>	<i>Errored Second Limit</i>
<i>All 1s</i>	<i>All</i>	<i>F11111111 11111111 11111111....F</i>	<i>5 min</i>	<i>0</i>
<i>3 in 24</i>	<i>AMI only</i>	<i>F01000100 00000000 00000100....F</i>	<i>5 min</i>	<i>0</i>
<i>1 in 8</i>	<i>All</i>	<i>F01000000 01000000 01000000....F</i>	<i>5 min</i>	<i>0</i>
<i>All 0s (Note 2)</i>	<i>B8ZS only</i>	<i>F00000000 00000000 00000000....F</i>	<i>30 sec</i>	<i>(Note 3)</i>

Note 1: F represents the framing bits; the bit patterns repeat as indicated to complete the 192-bit payload of the frame. All binary representations are transmitted left to right.

Note 2: Some DS-3 multiplex equipment may cause multiple DS-1 failures if the equipment is not properly optioned. This pattern should be applied only in the sequence recommended in the Job Aid (Figure 2).

Note 3: Incorrectly optioned equipment will be indicated by large errors counts. Low error counts, e.g., 1 or 2 errors, are not indicative of an optioning problem.

Note 4: When testing DS1 HDSL, HDSL 2, or HDSL 4 spans, intrusive testing durations can be abbreviated. Upon the repair of a circuit the Designed Service repair tester should clear the span performance monitor registers, run the quick test that a company testing system could perform, retrieve the performance monitor results and if no errors have occurred contact the customer to return service to them. In the conversation with the customer the tester should ask to hold the ticket for 30 minutes to retrieve the performance monitor results again and if clean then close the ticket at that time. Technicians should include all additional tests results made available by technology to Test Center (i.e., if HDSL technology is used, technician must include PA/SNR results).

6.11 Chronic Trouble of DS-1 Service

If the ASC and/or ASP determines that a DS1 Service, including a DS1 riding a DS3 Service, is experiencing chronic trouble reports (>=3 reports per month), the ASC and/or ASP will request the other company to provide a continuous performance monitoring capability on its portion of the DS1 service, in order to locate the offending network element. As part of the long term cooperative test arrangement, the ASC and ASP will share the detailed

Performance Monitoring Data (15 min. and 24 hr.) with the ASC and/or ASP. Where non-intrusive performance monitoring equipment is not available, other methods of trouble isolation should be agreed upon. Prior trouble report information should also be shared between the ASC and ASP.

6.12 Maintenance of DS-1 Service within a DS-3 Service

Alarmed failures on MUX/DEMUX equipment should be handled as follows:

- When either an ASC or ASP receives a DS-1 alarm, which impacts the other company, they shall notify the other company.
- Equipment specific alarms (e.g., Fuse Alarms) shall be cleared by the company receiving the alarm and a clearance given to the ASC or ASP as applicable.
- Alarms that show a failure of the DS-1 shall be handled as follows:
- When the ASC MUX/DEMUX equipment is at the POT, cooperative tests will be made between the ASP and ASC including the MUX/DEMUX equipment of both companies.
- When there is no DS-1 test access at the ASC POT location or if the ASC POT location is not staffed, the ASP will, at the ASC's requests, give a loopback to the ASC at the ASP MUX/DEMUX equipment or the DSX-1 closest to the MUX/DEMUX. The ASC will then test the DS-1 segment from their test access point via the loopback at the ASP location.
 - If the trouble is still present and further sectionalization is required the ASC will dispatch to the Point of Termination (POT).
 - If the DS-1 tests good, the ASC will refer the trouble to the ASP.

The Industry has accepted the DDS maintenance termination unit as an alternative to a proposed (ASP Provider) loopback device. This device is described in the T1 Technical Report #39, January 1995, on termination devices for digital data at 64 kbp/s and subrates.

6.13 Maintenance Testing Of DS-3 Service

Special Access Arrangements:

- ASC POT - End User Premises
- ASC POT - ASP HUB
- ASC POT - ASC POT

All tests shall be performed Out of Service, using a framed format. Tests should be performed from the ASC POT DSX-3 to the ASP DSX-3 or End User DSX-3 (or equivalent) POT as applicable.

In those cases where the ASC does not staff their POT location or have remote test access, the ASP will, upon the ASC's request, provide a loopback at the ASP DSX-3 closest to the ASC POT location. The ASC will test the DS-3 from their test access point, via the loopback at the ASP DSX-3.

If the DS-3 then tests good the ASC will refer the trouble to the ASP.

If trouble is indicated and further sectionalization is required the ASC will dispatch to the Point of Termination (POT).

6.14 DS-3 Testing - Optical Interface

In the case of an optical interface, where the DS-3 Service is transported via fiber, and the Fiber Optical Termination (FOT) is located at or beyond the ASC and/or End User POT, cooperative testing should be performed to ensure the service meets the requirements.

The service at the POT is tested in accordance to the manufacturer's guidelines for the FOT equipment installed.

6.15 Facility Restoration Procedures

Trouble reports, either from an ASC or ASP internally generated, will be given equal priority by ASP maintenance forces. However, in cases where one or more facilities are out of service and is causing blockage, such trouble reports will be given a higher restoration priority. The ASP will determine priorities from both internal reporting and reports received from the ASC.

6.16 Maintenance Make-Busy Procedure for Facilities

Upon receipt of any request to remove a facility from service (maintenance request), the ASP shall initiate a trouble report to remove the facility from service. The trouble report shall be used as an information report, and a report tracking number (or some other form of identification) will be provided to the ASC for future reference. The ASCs shall provide a reciprocal process.

The following facility make-busy procedures must be followed in order that the ASC or ASP request be properly and expeditiously performed.

6.16.1 Facility Make-Busy (Facility Failure)

In the event of a detected facility failure, the ASC should advise the ASP of the involved facilities and the need to have them removed from service. The ASP should then advise the ASC of the action taken. When either the ASC or ASP has cleared its facilities, they should contact the ASP to request the facility be restored to service. The ASC and ASP must ensure that the facilities are in proper operating condition before the ASP restores them to service.

6.16.2 Maintenance Removal from Service

If an ASC requests a facility to be removed from service for maintenance purposes, the request should normally be honored. Such requests for maintenance purposes should be made in advance by the ASC where ASP work forces are required for assistance. This would allow for the scheduling of ASP work forces and times to be mutually agreed upon.

6.16.3 Expedited Make-Busy Procedure for Facilities

An ASC must be able to promptly remove a facility from service. In order to accomplish this, the ASC may request that trunks incoming to its switch be made-busy on an expedited basis.

An ASC request for make-busy of a facility or group of facilities is to be handled by the responsible ASP on an expedited basis. The ASP will require a facility identification number, the nature of the request must also be provided to aid in the work activity. The ASP shall, upon receipt of an expedited make-busy request from the ASC, respond by immediately taking the facility out of service to preclude subsequent reports.

If a dispatch is required and the request for make-busy cannot be handled at once, the ASP will inform the ASC of the report number and the make-busy request will be handled as soon as possible.

If, during testing, the ASC discovers trouble in the ASP portion of the facility, the ASC will report the suspected trouble to the ASP referencing the expedited make-busy trouble report. This trouble report by the ASC shall be handled in the normal manner and the sequence in which the trouble is received.

6.17 Verification Tests

After each trouble has been cleared, the ASP will contact the ASC to advise that the trouble has been cleared and the nature of the trouble found and action taken.

If the requested tests are other than those specified for the type of facility involved, the ASP should notify the ASC that the time required to perform additional tests will be billed to the ASC.

When repair verification tests identify a trouble that was not apparent due to the nature of the original trouble, clearance activity will continue until the facility is restored.

Where remote loopback devices have been activated in the process of performing maintenance tests, verification should be made to ensure that all loopback devices are returned to normal.

6.18 End to End Intercarrier Testing

Network facilities comprised of multiple ASPs and ASCs may experience trouble conditions that cannot be isolated by each carrier testing and maintaining its own facility. Although the portions provided by each ASC and each ASP apparently perform properly, a trouble may be identifiable on an end-to-end facility. In such cases the ASC may require coordinated testing. It is the responsibility of the ASC to coordinate intercarrier and/or end-to-end testing with each sectional provider (i.e., other ASCs ASPs). ASP participation in coordinated testing may be billable to the ASC.

7 Additional Billing

Additional Billing may be applied in the following situations:

- Overtime for Installation and Repair
- Additional Cooperative Acceptance Testing
- Non-Scheduled Testing
- Maintenance of Service Charge
- Stand-by Time
- Other Labor

Accurate records regarding additional billing must be forwarded to the ICSC or equivalent. A positive means of identifying ASP personnel engaged in these work activities must be established and used. It is the responsibility of the ASP to ascertain when additional billing applies and the name of the ASC person authorizing the additional billing.

Overtime is the time spent by ASP personnel doing the installation and repair outside their scheduled working hours.

Overtime installation and repair charges are computed on a fixed rate per half hour fraction basis at a rate dependent on when the work was done, as follows:

- Outside scheduled hours but on a scheduled day.
- Outside a scheduled day.

7.1 Billable Overtime Installation and Repair

Request for billable overtime should be made by the ASC.

When ASP personnel are required to work on a non-scheduled basis, the billable overtime hours begin at the start time requested by the ASC and end when the job is completed or the ASP personnel have been released by the ASC. Only those hours worked outside the normally scheduled hours are billable at the overtime rate. A call out of an ASP employee is subject to a minimum charge of 4 hours.

7.2 Additional Cooperative Acceptance Testing (ACAT)

Time required to perform ACAT, such as additional installation transmission or signaling tests over and above those specified in normal installation acceptance testing, is considered additional and is billable to the ASC.

7.3 Non-Scheduled Testing

Non-scheduled testing occurs when an ASC determines a need to test its services and contacts the ASP to perform (billable) tests (e.g., loss, noise, envelope delay).

7.4 Maintenance of Service Charge

When an ASC reports a trouble to the ASP and requests that the ASP clear the trouble, the ASC shall be responsible for payment of a Maintenance of Service Charge if dispatch to the POT is required and the trouble is determined not to be in the ASP facilities.

When a trouble is subsequently found in the ASP facilities, where a Maintenance of Service Charge has been applied the charge will be canceled or adjusted.

7.5 Stand-By Time

Stand-By Time authorized by the ASC may be billable and is predicated on local negotiated agreements and shall be documented by both the ASP and the ASC.

7.6 Other Labor

As agreed to by the ASP and the ASC, other labor is anything not identified by B through F.

8 Facilities Provided by Multiple Exchange Carriers

These procedures apply when facilities are requested by an ASC and are provided by two or more ASPs within the same LATA.

The ASC will order from the ASPs the facilities required to provide its overall service.

It is recommended that a single Access Service Provider Coordinator (ASPC) point, specific to the installation function being performed, be identified for multi-ASP facilities.

Before an Access Service Request (ASR) is issued by the ASC for facilities involving multiple ASPs, the ASPs involved should have a mutually agreeable working arrangement in place to allow one of the ASPs to be the "Access Service Provider Coordinator (ASCP), for the installation of facilities.

Each ASP is responsible for working cooperatively with ASCs and other ASPs to ensure that access services are installed, tested and turned up in a timely manner and that trouble conditions are resolved without undue delay and participate in repair verification as required.

8.1 Installation

Installation as used in this document pertains to that portion of the total provisioning process which starts when the order, e.g., "Work Order Record and Detail" (WORD) or equivalent is received by the ASPs and includes installations, changes, and disconnects.

The ASPC will:

- Ensure that their company's equipment and facilities are installed and tested by the Plant Test Date (PTD).
- Receive and log status from on the Other Access Service Provider (OASP) on the Design, Verified or Assigned Date (DVA) or equivalent. If the OASP has not provided status within 24 hours after DVA or equivalent, the ASPC will contact OASP and request status.
- Prior to cooperative acceptance tests, schedule and coordinate pre-service tests, to ensure that the overall facilities are installed correctly and meet design parameters.
- Upon completion of the preservice tests, the ASPC will contact the ASC and advise them the facility is ready to be turned up. The ASC has the option of acceptance with or without cooperative acceptance testing. The ASC is not obligated to accept the facility/service prior to the due date.

The OASP will:

- Ensure that their company's facilities pertaining to the specific ASR are installed and tested by PTD.
- Contact the ASPC and provide facility status.
- Cooperate with the ASPC to perform the pre-service tests and acceptance tests as required.

8.2 Common Completion

A common completion date will be utilized by all involved ASPs. Therefore, no ASP may complete its order until the entire facility is completed and accepted by the ASC.

8.3 Jeopardy

If one or more ASPs cannot complete its portion of the facility on the Due Date, this should be considered a jeopardy situation by all ASPs involved. If, after a specified period of time (to be determined locally) past the due date, the overall facility remains incomplete due to ASP problems, those ASPs who completed their portion of the facility will review the status of the incomplete portions via the ASPC to determine the actual or approximate duration of the existing jeopardy condition and notify the ICSC or equivalent.

8.4 Maintenance

The ASC will be responsible for acceptance of trouble reports from its end user. The ASC should first test its facilities to determine if the trouble is in its network. If a trouble is found, the ASC will clear the trouble and no referral to an ASP is necessary. If the trouble is sectionalized by the ASC towards a connecting ASP, the trouble report will be referred to the ASP. The ASP(s) will work cooperatively with the ASC to sectionalize the trouble.

The following information should be exchanged when handing off or referring the trouble:

- Trouble report number or equivalent
- Contact telephone number
- Contact ID (i.e., name or initials)
- Time and date report was received from ASC
- ASC testing information (If requested by ASP)
- Facility ID
- Trouble reported
- Other information that may be of assistance (e.g., history, subsequent reports)

Upon receipt of a trouble report from the ASC, the ASP will conduct, independently or cooperatively with the ASC, tests required to determine if the trouble is in its own facilities or the point of interface of an adjacent OASP(s).

If the trouble is found to be in the ASP's facilities, the trouble report will be closed out with the ASC and the following information will be provided:

- Trouble report number or equivalent
- Date & Time Cleared
- Status of Facility (temporary or permanent repair)
 - o If temporary, estimated time of restoral
- Contact name or initials and telephone number of the person closing out the report
- Type & Nature of trouble found and action taken
- ASP Testing Information (if Requested by ASC)
- Facility ID

If there is no trouble found in the ASP's own network, they shall refer/hand-off the trouble to the OASP and provide the following information:

- Trouble report number or equivalent (ASC)
- Contact telephone number (ASC)
- Contact ID (ASC) (i.e., name or initials)
- Time and date report was received from ASC
- ASP Testing information (If requested by OASP)
- Facility ID
- Trouble reported
- Other information that may be of assistance (e.g., history, subsequent reports, ASC Testing information, if available)

In the event a premature or improper hand-off has occurred, the ASP will resume cooperative testing with the OASP in order to sectionalize the trouble.

When the ASP has referred/handed off the trouble report to an OASP, the ASP will close out the trouble report with the ASC and provide the following information:

- Trouble report number or equivalent (ASC)
- Trouble report number of OASP
- Time and date report was referred/handed off to the OASP
- Contact telephone number (OASP)
- Contact ID (OASP) (i.e., name or initials)
- ASP Testing information (If requested by ASC)
- Trouble disposition (Test OK, NTF, Found OK)
- Facility Identification
- Contact Name or initials of person closing the report

If the trouble report requires further hand-off/referral by the OASP to succeeding ASPs, the identity of the OASP switches to ASP when the referral is made.

The OASP will:

- Cooperatively test with the ASP to determine trouble location.
- Accept the trouble report when sectionalized into its equipment or facilities.
- Provide status to the ASC upon request.
- Contact the ASC upon clearing trouble to closeout the trouble report.

8.4.1 Trouble Report Exceptions

The following information is provided in an effort to assist service providers and service Customers in the resolution of troubles that fall outside of the normal trouble report resolution flow once the original report has been closed out with the ASC.

8.4.2 Request for Test Assistance

When a request for a test assist is made to an ASP, the ASP shall provide the necessary assistance to facilitate the request. A report (non-measured) shall be created for administration of test assist referrals; subsequent request for a test assist may result in additional reports being created. In the event that additional reports are created all relevant information from the prior trouble report/test assist reports should be cross referenced.

8.4.3 Request for Escalation Assistance from ASC

It is the responsibility of all service providers and service customers to work cooperatively to resolve all trouble reports as expeditiously as possible. The ASC is responsible for escalations to an OASP associated with trouble reports when the trouble has been isolated/referred by an ASP to an OASP. When a request for escalation assistance is made by the ASC to an ASP, the ASP will provide any information concerning escalation numbers or names that they may have to the requesting ASC. At the ASC manager's request, the ASP manager may participate on a phone call in an attempt to assist the ASC in escalating to the OASP. If the ASC refers the problem back to the ASP, it should be understood that the process will reinitiate at the escalation level when the problem was initially referred into the OASP.

In the event the trouble can not be sectionalized (e.g., no trouble found, intermittent type of problems), then the ASC and all ASPs/OASPs will cooperatively work together (e.g., cooperative testing) to locate and/or isolate the problem. Once the problem has been sectionalized then the previously developed process for ASP/OASPs shall be followed.

If repair verification with the ASC indicates trouble is still present, the ASP attempting to close out the trouble report will reinitiate testing with the other ASP(s).

9 Optional DS-1 Test Patterns

It is recognized that DS-1 service will be tested, cooperatively or to loopback devices, through the use of the stated test patterns within the Facilities document. It is also recognized that test patterns identified in Committee T1, Technical Report 25, may also be utilized to sectionalize troubles. Although these patterns are not widely available within deployed test instruments, they will be recognized as valid optional test patterns for use. These tests will be recognized as valid to loopback devices or test set-to-test set.

9.1 Background – CCITT / ITU-T Test Signals, Other Tests, and Test Signals

This group of test patterns includes various PRBS ^{note 1} signals described in CCITT / ITU –T recommendations, plus other empirically-designed signals. Note that many of these signals violate the pulse density constraints, so error-free transmission of such signals cannot be expected unless clear channel coding is implemented.

Note that test patterns in CCITT / ITU-T recommendations typically provide their outputs in an inverted format. The user should be aware that some manufactures of digital test instruments have incorporated the same basic patterns in their sets using the non-inverted format – a factor leading to incompatibilities between test sets of different manufactures.

9.1.1 $2^{15} - 1$ 32,757-bit PRBS ^{note1} test pattern (Inverted) ^{note 2}

The pattern may be generated in fifteen-stage shift register whose 14th and 15th stage output are added in a modulo-two addition stage, and the results fed back to the input of the first stage.

9.1.2 $2^{20} - 1$ 1,048,575-bit PRBS test pattern ^{note 2}

The pattern may be generated in twenty-stage shift register whose 3rd and 20th stage outputs are added in a modulo-two addition stages, and the result is fed back to the input of the first stage.

9.1.3 $2^{23} - 1$ 8,388,607-bit PRBS test pattern (Inverted) ^{note 2}

The test pattern may be generated in a twenty-three stage shift register whose 18th and 23rd stage outputs added in a modulo-two addition stage, and the result is fed back to the input of the first stage.

9.1.4 1-IN-16 (1:15) A single ONE bit followed by fifteen ZERO-bits.

The 1-IN-16 pattern has been used successfully to detect mistuned span line repeaters not detected when using other test patterns.

NOTES:

¹ PRBS Pseudorandom Binary Sequences

² The $2^{15} - 1$, $2^{20} - 1$, and $2^{23} - 1$ PRBS inverted patterns are ITU-T Patterns. ITU-T considers the inverted patterns as being more stressful than non-inverted patterns when testing the clock recovery circuit in the network terminating devices they were designed to test

9.1.5 55-Octet Stress Test Pattern

As network services have advanced in support of new applications so has the demand for improved testing technologies. The 55 Octet stress pattern has been successful identifying AMI circuit problems on line cards, preamplifiers/equalizer circuits utilizing discrete component ALBOs. The 55 Octet pattern introduces rapid

transitions from long sequences of low-density octets to high-density octets, (high-low density switches back and forth). This pattern is used as a stress test to identify random anomalies unable to be detected with other stress testing.

The binary representation of the 55 Octet test pattern No.1 (Daly) and the information for two other versions of the pattern currently in use.

10000000	10000000	10000000	10000000	10000000
10000000	00000001	10000000	10000000	10000000
10000000	10000000	10000000	11000000	10000000
10000000	10000000	10000000	11100000	10000000
10000000	10000000	10000000	10101010	10101010
10101010	10101010	10101010	10101010	10101010
10101010	10000000	10000000	10000000	10000000
10000000	10000000	11111111	11111111	11111111
11111111	11111111	11111111	00000001	10000000
00000001	10000000	00000001	10000000	00000001
10000000	00000001	10000000	00000001	10000000

There are three versions of the 55-octet patterns in use:

1. Daly as shown above.
2. Uses 00000000 in place of the 00000001 in byte position 7.
3. Uses 11000000 in place of 10000000 in byte position 3 and 00000000 in place of 00000001 in byte position 7.

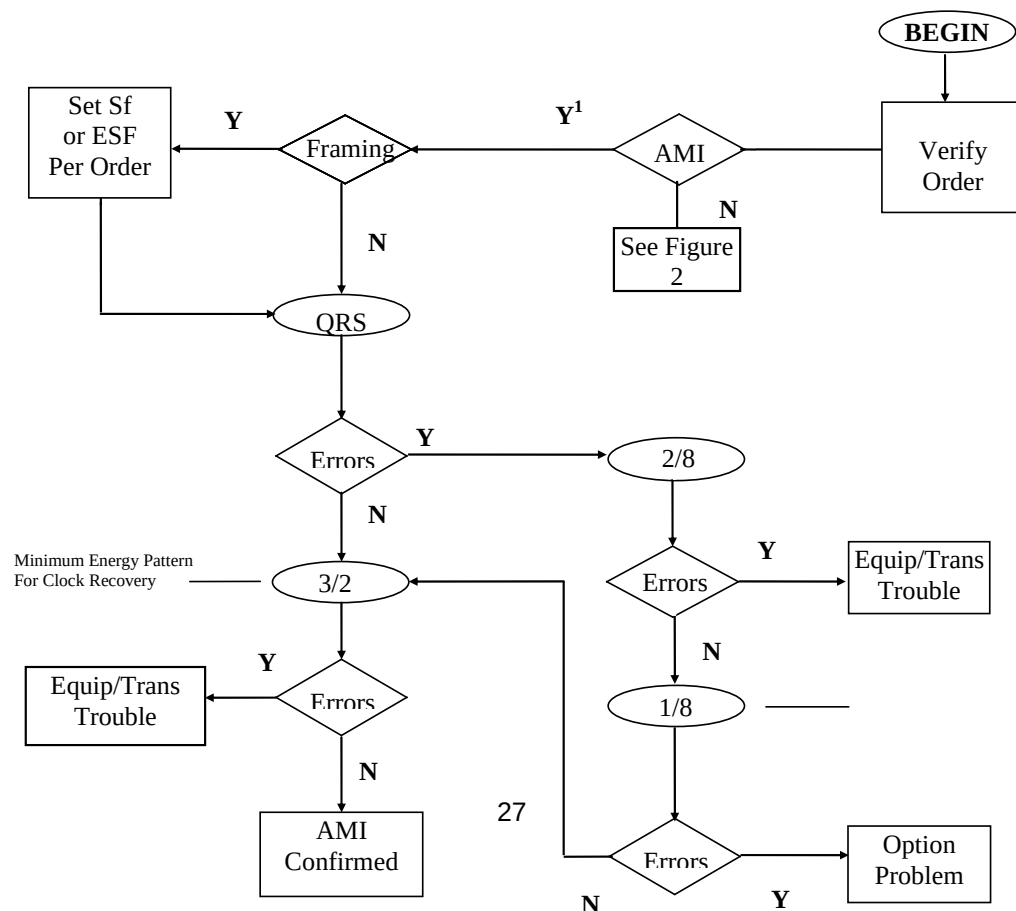


Figure 1 - DS-1 Line Code AMI Option Verification Job Aid

(Note: Figure 1 corresponds to Figure 6-1 in the T1-510 Technical Report 25)

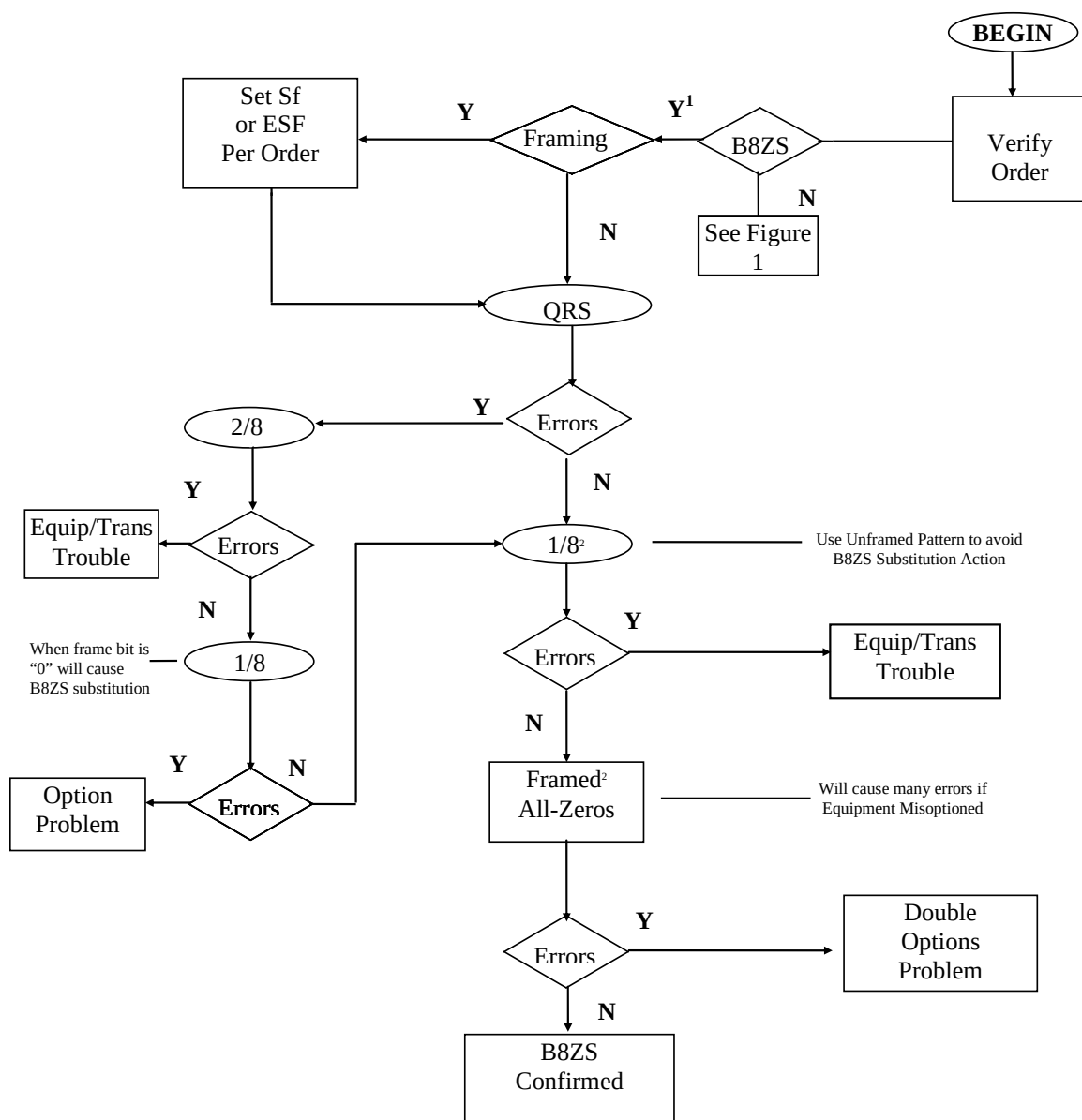
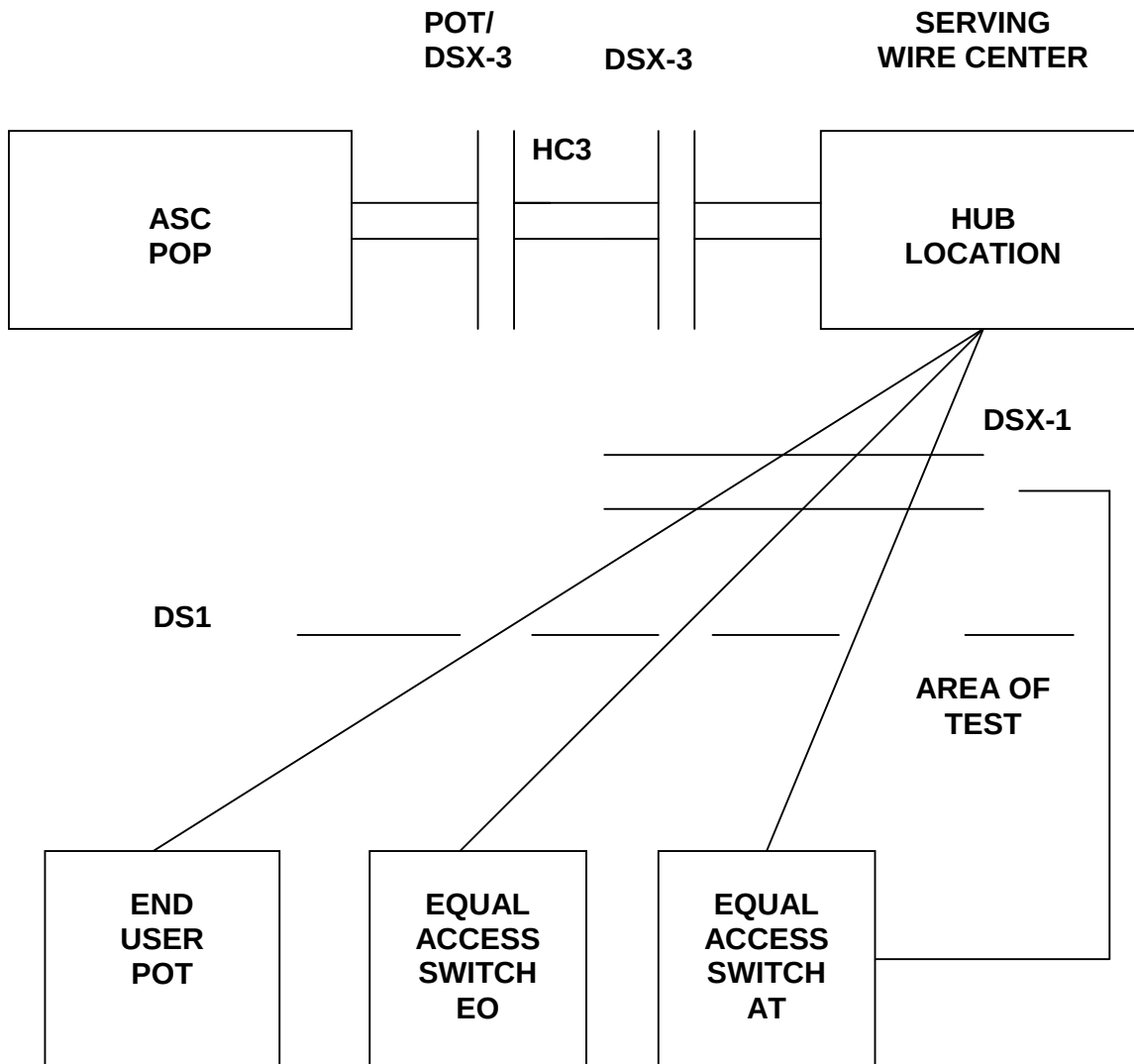


Figure 2 - DS-1 Line Code B8ZS Option Verification Job Aid

(Note: Figure 2 corresponds to Figure 6-2 in the T1-510 Technical Report 25)



- ADDING DS-1(s) to EXISTING DS-3

Figure 3 – Adding DS-1 (S) to an Existing DS-3



ATIS-0300031

**Next Generation Interconnection Interoperability (NGIIF)
Reference Document**

**Part IX, Installation, Testing and Maintenance
Responsibilities of Facilities**

**Attachment A
SONET Facilities**

Version 12.0



ATIS is the leading technical planning and standards development organization committed to the rapid development of global, market-driven standards for the information, entertainment and communications industry. More than 200 companies actively formulate standards in ATIS' Committees, covering issues including: IPTV, Cloud Services, Energy Efficiency, IP-Based and Wireless Technologies, Quality of Service, Billing and Operational Support, Emergency Services, Architectural Platforms and Emerging Networks. In addition, numerous Incubators, Focus and Exploratory Groups address evolving industry priorities including Smart Grid, Machine-to-Machine, Connected Vehicle, IP Downloadable Security, Policy Management and Network Optimization.

ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications' Sectors, and a member of the Inter-American Telecommunication Commission (CITEL). ATIS is accredited by the American National Standards Institute (ANSI). For more information, please visit www.atis.org.

Notice

This document was developed by the Alliance for Telecommunications Industry Solutions' (ATIS) sponsored Next Generation Interconnection Interoperability Forum (NGIIF). The NGIIF addresses next-generation network interconnection and interoperability issues associated with emerging technologies. Specifically, it develops operational procedures which involve the network aspects of architecture, disaster preparedness, installation, maintenance, management, reliability, routing, security, and testing between network operators. In addition, the NGIIF addresses issues which impact the interconnection of existing and next generation networks and facilitate the transition to emerging technologies. All changes to this document shall be made through the NGIIF issue resolution process.

Note Regarding Previous Versions

The NIIF Reference Document was formerly known as the Network Operations Forum (NOF) Reference Document. The NOF Reference Document was published and maintained by Bellcore. The last version of the NOF Reference Document is Issue 13.

Disclaimer and Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

ATIS-0300031, NGIIF Reference Document, Part IX, Installation, Testing and Maintenance Responsibilities of Facilities, Attachment A, SONET Facilities, Formerly NIIF 5027

The NGIIF Reference Document, Part IX, Installation, Testing and Maintenance Responsibilities of Facilities, Attachment A, SONET Facilities, is an ATIS standard developed by the NGIIF.

Published by

Alliance for Telecommunications Industry Solutions

1200 G Street, NW, Suite 500

Washington, DC 20005

Copyright © 2011 by Alliance for Telecommunications Industry Solutions

All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < <http://www.atis.org> >.

Printed in the United States of America.

INSTALLATION, TESTING, AND MAINTENANCE RESPONSIBILITIES FOR FACILITIES

SONET Facilities

Table of Contents

1	INTRODUCTION	4
2	REFERENCE MODEL.....	4
3	ERROR PERFORMANCE PARAMETERS AND BLOCK SIZES.....	4
4	BLOCK SIZE.....	5
5	PERCENT ERRORED SECONDS (% ES)	5
6	PERCENT SEVERELY ERRORED SECONDS (% SES).....	5
7	BACKGROUND BLOCK ERROR RATIO (BBER).....	5
8	SEVERELY ERRORED PERIOD INTENSITY (SEPI): THE NUMBER OF SEP EVENTS IN AVAILABLE TIME, DIVIDED BY THE TOTAL AVAILABLE TIME.	5
9	TEST DESIGN.....	6
9.1	ACCEPTANCE TESTS	6
9.2	REPAIR VERIFICATION TESTS	6
9.3	TROUBLE VERIFICATION TESTS.....	6
10	PERFORMANCE DETERMINATION	6
10.1	PARAMETERS MEASURED.....	6
10.2	TEST DURATION	6
11	SERVICE PERFORMANCE TESTING.....	6
12	TESTS FOR 51.84, 155.52, 622.08 MBIT/S, 2.488 GBIT/S, AND 9.865 GBIT/S SERVICES	7
13	TEST PROCEDURES.....	7
13.1	SHORT DURATION TESTS	7
13.2	LONG DURATION TESTS	8
13.3	TEST LIMIT TABLES	8
13.4	ACCEPTANCE AND REPAIR VERIFICATION TEST LIMIT TABLES.....	8

1 Introduction

The performance, test, and design parameter information in the document sections below, where required, have been updated from ATIS 0100514.2009 Network Performance Parameters and Objectives for Dedicated Digital Services – SONET Bit Rates. Additional or more detailed information can be obtained from ATIS 0100514.2009 if needed.

This standard covers dedicated digital services operating at the nominal 51.84 Mbit/s, 155.52 Mbit/s, 622.08 Mbit/s, 2.488 Gbit/s, and 9.865 Gbit/s interface rates of the SONET (Synchronous Optical Network) digital hierarchy. Rates above 9.865 Gbit/s and SONET virtual tributaries are for further study at PRQC.

2 Reference Model

The performance of dedicated digital networks shall be specified in terms of the reference model in Figure 1. End-to-end performance shall be specified from NI-to-NI with performance allocated for NI-to-INI (access) and INI-to-INI (transit). For intra-network connections (no INIs), end-to-end performance shall apply. Since dedicated digital services are characterized by established connections (i.e., no access or disengagement phases) with a constant rate of data transfer, entry and exit events consist solely of user information bits crossing a network interface.

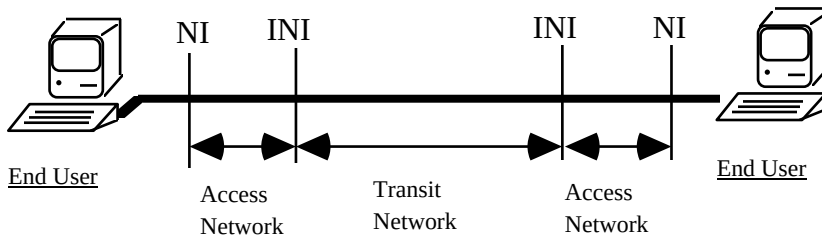


Figure 1 - Reference Model - SONET Dedicated Digital Service

NOTES

NI - Network Interface

INI - Internetwork Interface: INIs are only present when the service is provided across multiple networks. Where a point of termination (POT) exists, it will coincide with an INI.

3 Error Performance Parameters and Block Sizes

These guidelines are based on the error performance measurement of blocks. As defined, a block is a set of consecutive bits associated with the connection; each bit belongs to one and only one block.

4 Block Size

The following block sizes are given in assessing performance.

Table 1 - Block Size

Rate (Mbit/s)	51.84 (STS-1)	155.52 (STS-3c)	622.08 (STS-12c)	2,488.32 (STS-48c)	9,865.28 (STS-192c)
Bits/block	6,264	18,792	75,168	300,672	1,202,688

The block size corresponds to the number of bits in 125 microseconds for the SONET path (equivalent to synchronous payload envelope (SPE)); 50.112 Mbit/s, 150.336 Mbit/s, 601.344 Mbit/s, 2.405 Gbit/s, and 9.622 Gbit/s for STS-1, STS-3c, STS-12c, STS-48c, and STS-192c paths, respectively. A path that is multiplexed to a higher rate should be measured at its demultiplexed, original rate. Performance objectives apply at these rates to the SONET path that is not constrained to a particular physical signal type (i.e., objectives apply for electrical (STS-n) or optical (OC-n) signals). See Annex A in ATIS 0100514.2009 Network Performance Parameters and Objectives for Dedicated Digital Services – SONET Bit Rates for further details on block measurement with SONET path measures.

5 Percent Errored Seconds (% ES)

100 x the ratio of ES to total seconds in available time during a fixed measurement period.

6 Percent Severely Errored Seconds (% SES)

100 x the ratio of SES to total seconds in available time during a fixed measurement period.

7 Background Block Error Ratio (BBER)

The ratio of Background Block Errors (BBE) to total blocks in available time during a fixed measurement interval. The count of total blocks excludes all blocks during SESs.

Note - Background Block Error Ratio (BBER) does not include errored blocks occurring as part of SES.

8 Severely Errored Period Intensity (SEPI): The number of SEP events in available time, divided by the total available time.

NOTE - The SEPI parameter has a unit of (1/s). This is to enable any SEPI objective to be easily translated to the equivalent number of SEP events over a specific measurement interval. It should be noted that the SEP event has no significance over a time interval of less than three seconds.

9 Test Design

9.1 Acceptance Tests

Acceptance test measurements are made upon completion of a new service installation. Threshold levels for these tests are generally more stringent than the pro-rated levels derived from the associated long term objective, to provide a greater assurance that a circuit meets a specified performance level. This approach minimizes the probability that the circuit will require corrective maintenance.

9.2 Repair Verification Tests

Repair verification tests are made upon completion of a repair activity. Threshold levels for these tests are the same as acceptance tests levels to ensure that a circuit will meet specified performance levels.

9.3 Trouble Verification Tests

Trouble verification tests are made in response to a trouble indication. Trouble verification is an internal responsibility of the provider and is, therefore, not covered in this standard.

10 Performance Determination

10.1 Parameters Measured

For digital services operating at rates of 51.84 and 155.52 Mbit/s, the appropriate measures are percent ES and percent SES. For the 622.08 Mbit/s rate and higher rates, the appropriate measures are BBER and percent SES. The appropriate block size (number of bits per block) for each bit rate is given in Table 1.

10.2 Test Duration

Test durations have been specified from 1 hour to 24 hours. For the shorter test durations, sequential tests are specified; for the longer 24 hour duration only one test is specified. In-service monitoring, where available, may be used over longer periods of time to confirm conformance to long-term objectives.

11 Service Performance Testing

For each service included in this section, the following is provided: test criteria, sequential test procedures and performance value tables. The specified procedure applies to acceptance and repair verification tests (not trouble verification). Each procedure includes the following: the parameters to be measured, the duration of a single test stage, the number of sequential stages to be conducted, and performance determination criteria. The performance value tables include the threshold performance parameter values for each of the above tests. For each service there are two tables, one for test criteria and one for test limits.

The sequential short duration tests are structured in stages with one of three outcomes after each stage: acceptable performance, indicating confidence that the circuit under test will satisfy the long-term objective; unacceptable performance, indicating confidence that the circuit under test will not satisfy the long-term objective; or inconclusive, indicating insufficient evidence at this stage to predict the long-term performance (i.e. marginal). If at any stage the test indicates acceptable or unacceptable performance, the test is terminated. If the test is

inconclusive at the first stage, the procedure shall be continued to the second stage. Testing for longer periods such as 24 hours or continuous monitoring will provide greater confidence and should be considered for marginal circuits.

For the test specified, all measurements are to be made at the bit rate of the service. Tests conducted intrusively shall be the PRBS (Pseudo Random Binary Sequence) pattern appropriate for the service rate under test. Non-intrusive testing methods should be used where available.

12 Tests for 51.84, 155.52, 622.08 MBIT/S, 2.488 GBIT/S, and 9.865 GBIT/S Services

These are services with actual user payload capacity of up to 49.536, 149.760, 600.768 Mbit/s, 2.404 Gbit/s, and 9.621 Gbit/s respectively. Payload capacity is 576 kbit/s less than the SPE capacity to allow for the nine path overhead bytes in each 125 microsecond block. Test criteria are provided in Table 2.

Table 2 - Test Criteria

Bit Rate	51.84 Mbit/s (STS-1)	155.52 Mbit/s (STS-3c)	622.08 Mbit/s (STS-12c)	2.488 Gbit/s (STS-48c)	9,865 Gbit/s (STS-192c)
Parameters	ES, SES, SEP	ES, SES, SEP	BBE, SES, SEP	BBE, SES, SEP	BBE, SES, SEP
Test stage duration Short Long	1 Hour 24 Hour	1 Hour 24 Hour	1 Hour 24 Hour	1 Hour 24 Hour	1 Hour 24 Hour
Number of stages Short duration Long duration	1 or 2 1	1 or 2 1	1 or 2 1	1 or 2 1	1 or 2 1
Test limits	Table 5	Table 6	Table 7	Table 8	Table 9
NOTE: Use of the SEP parameter for test criteria is for further study.					

13 Test Procedures

13.1 Short Duration Tests

Up to two sequential one hour stages shall be conducted to validate the general performance of the service.

The service performance shall be considered acceptable and the test terminated if, after one hour, the test results for all parameters do not exceed the limits for the 1 hour tests in the table for the service (table 3, 4, 5, 6, 7, or 8). The service performance shall be considered unacceptable if any test result is greater than the 2 hour limit. If the test result is between these two limits, continue the test.

After two hours the service performance shall be considered acceptable if the test results do not exceed the limits in the table for the service (table 3, 4, 5, 6, 7, or 8) for the two hour test. If the test result is unacceptable after the two hour limit, the circuit will be referred for trouble isolation. In addition, if the circuit test results are marginal, additional long duration testing or continuous monitoring testing should be performed.

The tests limits as shown in Tables 3 - 8 are recommended values and may be modified by bi-lateral agreement between the interconnected parties.

13.2 Long Duration Tests

Long duration (i.e. 24 hour) test should be performed when results from short duration testing indicates marginal performance. If a 24 hour test is performed, the service performance shall be considered acceptable if the results for each parameter measured do not exceed the 24 hour limits in the table for the service (table 3, 4, 5, 6, 7 or 8).

The test limits as shown in tables 3 - 8 are recommended values and may be modified by bi-lateral agreement between the interconnected parties.

13.3 Test Limit Tables

The test limits in Tables 3-6 are designed to support the accuracy objectives given in Table 7. While some of the entries are "0", it should be noted that an isolated error event is not necessarily indicative of a service affecting problem. Because many SES are known to occur in pairs (protection switch and restoral switch) it is unreasonable to set a limit of one SES.

13.4 Acceptance and Repair Verification Test Limit Tables

The test limits in Tables 3 to 8 are designed to support the accuracy objectives given in Table 9. While some of the entries are "0", it should be noted that an isolated error event is not necessarily indicative of a service affecting problem. From the "weight of evidence" tables in Annex B ATIS 0100514.2009 Network Performance Parameters and Objectives for Dedicated Digital Services – SONET Bit Rates all the short duration test limits for SES would be 0 or 1. Because many SES are known to occur in pairs (protection switch and restoral switch), it is unreasonable to set a limit at one SES. Test limits for 51.84, 155.52, 622.08 Mbit/s, 2.488, and 9.865 Gbit/s are provided in Tables 3, 4, 5, 6, 7 and 8, respectively.

13.4.1 Test Limits for 51.84 Mbit/s Service

Table 3- Acceptance and Repair Verification Test Limits for 51.84 Mbit/s Service

Parameter limit for:	Short duration tests (1 hour stages)				Long duration test (24 hour)	
	ES		SES		ES	SES
	1 hour	2 hour	1 hour	2 hour	24 hour	24 hour
End-to-end	≤ 6	≤ 12	0	$\leq \frac{2}{\text{(Note 1)}}$	≤ 150	≤ 20
Transit	≤ 3	≤ 6	0	$\leq \frac{2}{\text{(Note 1)}}$	≤ 75	≤ 14
Access	≤ 3	≤ 6	0	$\leq \frac{2}{\text{(Note 1)}}$	≤ 75	≤ 5
NOTES 1 Accept at 2 only if the cause of the SES is identified as an isolated event. 2 This standard does not provide trouble verification test limits; see 7C.						

13.4.2 Test Limits for 155.52 Mbit/s Service

Table 4 - Acceptance and Repair Verification Test Limits for 155.52 Mbit/s Service

Parameter limit for:	Short duration tests (1 hour stages)				Long duration test (24 hour)	
	ES		SES		ES	SES
	1 hour	2 hour	1 hour	2 hour	24 hour	24 hour
End-to-end	≤ 12	≤ 24	0	$\leq \frac{2}{\text{(Note 1)}}$	≤ 300	≤ 20
Transit	≤ 6	≤ 12	0	$\leq \frac{2}{\text{(Note 1)}}$	≤ 150	≤ 14
Access	≤ 6	≤ 12	0	$\leq \frac{2}{\text{(Note 1)}}$	≤ 150	≤ 5
NOTES 1 Accept at 2 only if the cause of the SES is identified as an isolated event. 2 This standard does not provide trouble verification test limits, see 7C						

13.4.3 Test Limits for 622.08 Mbit/s Service using BBE-SES Criteria

Table 5 - Acceptance and Repair Verification Test Limits for 622.08 Mbit/s Service

Parameter limit for:	Short duration tests (1 hour stages)				Long duration test (24 hour)	
	BBE		SES		BBE	SES
	1 hour	2 hour	1 hour	2 hour	24 hour	24 hour
End-to-end	≤ 199	≤ 399	0	$\leq \frac{2}{\text{(Note 1)}}$	≤ 4792	≤ 20
Transit	≤ 99	≤ 199	0	$\leq \frac{2}{\text{(Note 1)}}$	≤ 2396	≤ 14
Access	≤ 99	≤ 199	0	$\leq \frac{2}{\text{(Note 1)}}$	≤ 2396	≤ 5

NOTES

- 1 Accept at 2 only if the cause of the SES is identified as an isolated event.
- 2 This standard does not provide trouble verification test limits, see 7C
- 3 FFS = For Future Study.
- 4 In the absence of test equipment and network elements that measure and report Background Block Errors, the SES parameter is used here as a measure of acceptance and repair verification. As an interim alternative, bilateral agreements could be established to use ES as a measure of acceptance and repair verification.

13.4.4 Test Limits for 622.08 Mbit/s Service using ES-SES Criteria

Table 6 – Test Limits for 622.08 Mbit/s Service (See Note 2)

Parameter limit for	Short duration tests (1 hour stages)				Long duration test (24 hour)	
	ES		SES		ES	SES
	1 hour	2 hour	1 hour	2 hour	24 hour	24 hour
End-to-end	≤ 48	≤ 96	0	$\leq \frac{2}{\text{(Note 1)}}$	≤ 750	≤ 20
Transit	≤ 24	≤ 48	0	$\leq \frac{2}{\text{(Note 1)}}$	≤ 375	≤ 14
Access	≤ 24	≤ 48	0	$\leq \frac{2}{\text{(Note 1)}}$	≤ 375	≤ 5
NOTES 1 Accept at 2 only if the cause of the SES is identified as an isolated event. 2 This table was generated as a result of industry consensus, and is not contained in T1 Standards. The use of this table is optional.						

13.4.5 Test Limits for 2.488 Gbit/s Service

Table 7 - Acceptance and Repair Verification Test Limits for 2.488 Gbit/s Service

Parameter limit for	Short duration tests (1 hour stages)				Long duration test (24 hour)	
	BBE		SES		BBE	SES
	1 hour	2 hour	1 hour	2 hour	24 hour	24 hour
End-to-end	≤ 199	≤ 399	0	$\leq \frac{2}{\text{(Note 1)}}$	≤ 4792	≤ 20
Transit	≤ 99	≤ 199	0	$\leq \frac{2}{\text{(Note 1)}}$	≤ 2396	≤ 14
Access	≤ 99	≤ 199	0	$\leq \frac{2}{\text{(Note 1)}}$	≤ 2396	≤ 5
NOTES 1 Accept at 2 only if the cause of the SES is identified as an isolated event. 2 This standard does not provide trouble verification test limits, see 7C 3 FFS = For Future Study. 4 In the absence of test equipment and network elements that measure and report Background Block Errors, the SES parameter is used here as a measure of acceptance and repair verification. As an interim alternative, bilateral agreements could be established to use ES as a measure of acceptance and repair verification.						

13.4.6 Test Limits for 9.865 Gbit/s Service

Table 8 - Acceptance and Repair Verification Test Limits for 9.865 Gbit/s Service

Parameter limit for	Short duration tests (1 hour stages)				Long duration test (24 hour)	
	BBE		SES		BBE	SES
	1 hour	2 hour	1 hour	2 hour	24 hour	24 hour
End-to-end	≤ 1996	≤ 3993	0	$\leq \frac{2}{\text{(Note 1)}}$	47930	≤ 20
Transit	≤ 998	≤ 1996	0	$\leq \frac{2}{\text{(Note 1)}}$	≤ 23965	≤ 14
Access	≤ 998	≤ 1996	0	$\leq \frac{2}{\text{(Note 1)}}$	≤ 23965	≤ 5
NOTES 1 Accept at 2 only if the cause of the SES is identified as an isolated event. 2 This standard does not provide trouble verification test limits, see 7C 3 FFS = For Future Study. 4 In the absence of test equipment and network elements that measure and report Background Block Errors, the SES parameter is used here as a measure of acceptance and repair verification. As an interim alternative, bilateral agreements could be established to use ES as a measure of acceptance and repair verification.						

13.4.7 Long-Term Accuracy Objectives

Table 9 - Long-Term Accuracy Objectives (All values in table 9 are provisional)

SEGMENT	PARAMETER	51.84 Mbit/s (STS-1)	155.52 Mbit/s (STS-3c)	622.08 Mbit/s (STS-12c)
End-to-End	BBER	NA	NA	10^{-5}
	%ES	0.25	0.5	(Note 2)
	%SES	0.035	0.035	0.035
Transit	BBER	NA	NA	5×10^{-6}
	%ES	0.125	0.25	(Note 2)
	%SES	0.025	0.025	0.025
Access	BBER	NA	NA	5×10^{-6}
	%ES	0.125	0.25	(Note 2)
	%SES	0.01	0.01	0.01

Note 1 - Actual performance may not meet objectives at all times

Note 2 - Due to the lack of information on the performance of paths operating above 160 Mbit/s, no %ES objectives are recommended at this time. Nevertheless, ES processing should be implemented within any error performance measuring devices operating at these rates for maintenance or monitoring purposes (including SONET section and line layer monitoring).

Note 3 – Additional Weight of Evidence tables (accuracy objectives) for STS 48c, 192c, and others are available in Annex B in ATIS 0100514.2009 *Network Performance Parameters and Objectives for Dedicated Digital Services – SONET Bit Rates*

Next Generation Interconnection Interoperability (NGIIF) Reference Document

Part X, Interconnection Between LECS Operations Handbook – Local Interconnection Service Arrangement

Version 14

Alliance for Telecommunications Industry Solutions

Approved November 8, 2019

Abstract

The purpose of this document is to outline the procedures for installation, testing, maintenance and arrangement of local interconnecting service trunks. Included within the document are: Responsibilities for Local Service Customers (LSC) and Local Service Providers; Telecommunication Service Priority (TSP) guidelines; NXX Code Opening Guidelines; Trunk trouble reporting, trunk make busy, clearance, restoration guidelines. Where applicable, this document may address NGN aspects.

Foreword

The Alliance for Telecommunications Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The Next Generation Interconnection Interoperability Forum (NGIIF) addresses next-generation network interconnection and interoperability issues associated with emerging technologies. Specifically, it develops operational procedures which involve the network aspects of architecture, disaster preparedness, installation, maintenance, management, reliability, routing, security, and testing between network operators. In addition, the NGIIF addresses issues which impact the interconnection of existing and next generation networks and facilitate the transition to emerging technologies.

The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages. The word *may* denotes an optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, NGIIF, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, NGIIF, which was responsible for its development, had the following leadership:

Karen Riepenkroger, Sprint

Randee Ryan, Comcast

Trademark Acknowledgements

iconectiv®, Telcordia®, and Common Language® are registered trademarks and CLCI™, CLLI™, LERG™ Routing Guide and TPM™ Data Source are trademarks and the Intellectual Property of Telcordia Technologies, Inc. dba as iconectiv.

Table of Contents

1	SCOPE, PURPOSE, & APPLICATION	1
2	INFORMATIVE REFERENCES	1
3	DEFINITIONS, ACRONYMS, & ABBREVIATIONS	2
3.1	ACRONYMS & ABBREVIATIONS	2
4	GENERAL.....	3
5	RESPONSIBILITIES	3
5.1	LOCAL SERVICE CUSTOMER (LSC)	3
5.2	LOCAL SERVICE PROVIDER (LSP)	4
6	TELECOMMUNICATIONS SERVICE PRIORITY (TSP) GUIDELINES	5
6.1	DOMESTIC NS/EP SERVICES.....	5
6.2	CONTROL SERVICES AND ORDERWIRES.....	5
6.3	OTHER SERVICES	5
6.3.1	TSP Code Identification	5
6.4	TSP INSTALLATION	6
6.5	TSP MAINTENANCE.....	6
6.5.1	Example 1	7
6.5.2	Example 2	7
6.6	COMPETITION FOR RESOURCES BETWEEN PROVISIONING AND RESTORATION PRIORITIES	7
6.7	TSP INSTALLATION PREEMPTION	7
6.8	TSP MAINTENANCE PREEMPTION	7
6.8.1	To Restore Interrupted NS/EP Services	8
6.8.2	NS/EP Services	8
7	NXX CODE OPENINGS	8
7.1	NXX OF NXX-X CO CODE ACTIVATION PLANNING.....	9
7.2	PRE-NXX OR NXX-X ACTIVATION	9
7.2.1	BIRRDS.....	9
7.2.2	iconectiv® LERG™ Routing Guide.....	9
7.2.3	Facilities	9
7.2.4	Points of Interconnection	9
7.3	TRANSLATION VALIDATION/CALL THROUGH TESTING	10
7.4	INTERMEDIATE OFFICE(S) (TANDEMS/ACCESS TANDEMS)	10
7.5	LEC TERMINATING OFFICE (SERVING OFFICE)	10
7.6	ORIGINATING OFFICE	11
7.7	MECHANIZED TESTING	11
7.8	VERIFICATION OF NXX OR NXX-X CODE OPENINGS, SWITCH CHANGE/REHOME, OR SWITCH TANDEM REHOME PROCESS.....	11
7.9	NXX OR NXX-X CODE OPENING, SWITCH CHANGE/REHOME, OR SWITCH TANDEM REHOME PROCESS IN JEOPARDY SITUATIONS	12
8	TRUNK INSTALLATION	12
8.1	PRE-SERVICE TESTING	12
8.2	ACCEPTANCE TESTING	13
8.3	ADDITIONAL COOPERATIVE ACCEPTANCE TESTING.....	14
8.4	TRAFFIC ROUTING AND BILLING ACCEPTANCE TESTING.....	14
8.5	COMPLETION	14
8.6	EXPEDITES	15
8.7	TRUNK DISCONNECTS.....	15
8.8	TRUNK REARRANGEMENTS	15
8.9	COORDINATED CONVERSION	15

9	TRUNK MAINTENANCE	16
9.1	TRUBLE DETECTION RESPONSIBILITIES	16
9.2	SECTIONALIZATION	16
9.3	TROUBLE REPORTING	17
9.4	REPAIR VERIFICATION	17
9.5	NON-TRUNK SPECIFIC TROUBLES.....	17
9.6	TROUBLE REPORT CLEARING INFORMATION	18
9.7	PRIORITY OF RESTORATION	18
9.8	MAKE-BUSY PROCEDURES	18
9.9	RESTORATION.....	18
9.10	HOLD AND TRACE TROUBLE ISOLATION.....	19
9.11	CALL TRACES.....	19
9.12	NETWORK MODIFICATION	19
9.12.1	<i>Network Modification Suspension Periods</i>	<i>20</i>
9.13	LEC-LEC NON-TRUNK OPERATIONAL AGREEMENTS.....	20
9.13.1	<i>Line Identification/Verification.....</i>	<i>20</i>
10	EXCEPTIONS	21
10.1	LINE IDENTIFICATION/VERIFICATION	21
10.2	CALLING PARTY NUMBER (CPN), CALLING PARTY NAME (CNAM)	21
10.2.1	<i>Calling Party Number (CPN)</i>	<i>21</i>
10.2.2	<i>Linking CPN & CNAM</i>	<i>21</i>
11	ESCALATIONS.....	21
12	TEST LINES	22
13	ADDITIONAL BILLING	22
13.1	BILLABLE OVERTIME INSTALLATION AND REPAIR	22
13.2	ADDITIONAL COOPERATIVE ACCEPTANCE TESTING (ACAT).....	22
13.3	NON-SCHEDULED TESTING.....	22
13.4	MAINTENANCE - SERVICE CHARGE	22
13.5	STAND-BY TIME	23
13.6	OTHER LABOR	23
14	LOCAL RECORDED ANNOUNCEMENTS	23
14.1	MANDATORY 10 DIGIT LOCAL DIALING	23
14.2	INTERCEPT NUMBER ANNOUNCEMENT - PORTED NUMBERS	23
15	LOCAL NUMBER PORTABILITY.....	23
15.1	LOCAL NUMBER PORTABILITY	23
15.2	DEFAULT ROUTING TRANSLATIONS	23
15.2.1	<i>Background.....</i>	<i>24</i>
15.3	HANDOFF OF TERMINATING	24
16	COMMON CHANNEL SIGNALING SYSTEM 7 (CCS7)	24
17	INSTALLATION, TESTING & MAINTENANCE OF TRANSPORT FACILITIES	24
18	NETWORK MANAGEMENT GUIDELINES	24
19	SPECIAL SERVICES	24
20	SECURITY.....	25

Table of Figures

FIGURE 1: TSP AUTHORIZATION CODE	6

Table of Tables

TABLE 6.1- TSP CODES REFERENCE TABLE.....	6
TABLE 9.1- NETWORK MODIFICATION SUSPENSION PERIODS	20

ATIS Standard on –

Next Generation Interconnection Interoperability (NGIIF) Reference Document

Part X, Interconnection Between LECS Operations Handbook – Local Interconnection Service Arrangement

1 Scope, Purpose, & Application

The purpose of this document is to outline the procedures for installation, testing, maintenance and arrangement of local interconnecting service trunks. Included within the document are: Responsibilities for Local Service Customers (LSC) and Local Service Providers; Telecommunication Service Priority (TSP) guidelines; NXX Code Opening Guidelines; Trunk trouble reporting, trunk make busy, clearance, restoration guidelines. Where applicable, this document may address NGN aspects.

2 Informative References

The following standards contain provisions which, through reference in this text, constitute provisions of this Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

ATIS-0300009, *Next Generation Interconnection Interoperability (NGIIF) Reference Document: Part I, Installation and Maintenance Responsibilities Special Access Services, WATS Access Lines and Switched Access Services Feature Group A*.¹

ATIS-0300010, *Next Generation Interconnection Interoperability (NGIIF) Reference Document: Part II, Installation and Maintenance Responsibilities Switched Access Services Feature Group B, C, and D*.¹

ATIS-0300011, *Next Generation Interconnection Interoperability (NGIIF) Reference Document: Part III, Installation and Maintenance Responsibilities for SS7 Links and Trunks*.¹

ATIS-0300013, *Next Generation Interconnection Interoperability (NGIIF) Reference Document: Part III, Installation, Testing and Maintenance Responsibilities for SS7 Links and Trunks Attachment B ISUP Compatibility Tests*.¹

ATIS-0300024, *Next Generation Interconnection Interoperability (NGIIF) Reference Document Part V, Test Line Guidelines*.¹

ATIS-0300026, *Next Generation Interconnection Interoperability (NGIIF) Reference Document: Part VI, Network Management Guidelines*.¹

ATIS-0300030, *Next Generation Interconnection Interoperability (NGIIF) Reference Document: Part IX, Installation, Testing and Maintenance Responsibilities of Facilities*.¹

ATIS-0300033, *Part X, Interconnection Between LECS Operations Handbook – Local Interconnection Service Arrangement, Attachment A, Security Guidelines*.¹

ATIS-0300046, *Recommended Notification Procedures to Industry for Changes in Access Network Architecture*.¹

¹ This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at: < <https://www.atis.org/docstore/> >.

ATIS-0300119, *Thousands-Block (NPA-NXX-X) & Central Office Code (NPA-NXX) Administration Guidelines (TBCOCAG)*.¹

GR-334, *Switched Access Service: Transmission Parameter Limits and Interface Combinations*.²

T1.TRQ.02-2001, *Number Portability Switching Systems (Revision of T1.TRQ.2-1999)*.¹

3 Definitions, Acronyms, & Abbreviations

For a list of common communications terms and definitions, please visit the *ATIS Telecom Glossary*, which is located at < <http://www.atis.org/glossary> >.

3.1 Acronyms & Abbreviations

ACAT	Additional Cooperative Acceptance Testing
AMA	Automatic Message Accounting
ANAC	Automatic Number Announcement Circuit
ASR	Access Service Request
ATIS	Alliance for Telecommunications Industry Solutions
CNAM	Calling Party Name
CPN	Calling Party Number
FCC	Federal Communications Commission
INC	Industry Numbering Committee
ISO	Issue Service Orders
LEC	Local Exchange Carrier
LSC	Local Service Customer
LSP	Local Service Provider
NGIIF	Next Generation Interconnection Interoperability Forum
NS/EP	National Security Emergency Preparedness
OBF	Ordering and Billing Forum
POT	Point of Termination
SP	Service Provider
SS7	Signaling System 7
TCIC	Trunk Circuit Identification Code
TQ	Translation Questionnaire

² This document is available from Telcordia at < <https://telecom-info.telcordia.com> >.

TSP	Telecommunication Service Priority

4 General

This document has been developed to provide operation personnel of interconnecting LECs with guidelines for the installation, testing, and maintenance of local interconnection service arrangement trunk(s) and services.

This document does not replace or supersede any tariffs, contracts or other legally binding documents. In case of conflict between this document and any legally binding document, such other document will prevail.

A Local Exchange Carrier (LEC), as referred to in this document, is any company that has been authorized to provide local exchange services.

Local Service Provider (LSP) is defined as the LEC selling local interconnection service arrangement trunk(s) to another LEC.

Local Service Customer (LSC) is defined as the LEC purchasing local interconnection service arrangement trunk(s) from another LEC.

The following are some examples of interconnection between LSPs and LSCs in an IntraLATA environment:

- End Office to End Office
- End Office to Tandem

Local interconnection service arrangements may include all wiring, cable, equipment and facilities up to the Point of Termination (POT). These guidelines also generally apply to E9-1-1 and Operator Assistance trunking.

5 Responsibilities

5.1 Local Service Customer (LSC)

The following are the responsibilities of LSCs:

- Provide trained personnel
- Advise the LSP when there is a potential service affecting LSC network failure
- Provide a contact number for trouble reporting that is readily accessible 24 hours a day, 7 days a week
- Maintain complete and accurate installation and repair records
- Provide LSP personnel access to the Point of Termination (POT) when required
- Provide access to test lines where appropriate
- Provide billing authorization to the LSP for any additional labor requested
- Ensure the test equipment used is compatible with the LSP's test equipment
- Cooperate with the LSP ensuring that trunks are installed in accordance with the service requests
- Notify the LSP of any changes affecting the service requested, including the service due date
- Assume control functions for maintenance of its trunk(s)
- Consult with the LSP before making any changes that could affect service, except under emergency conditions (See Clause on Network Modification)
- Accept trouble reports from their end users
- Accept trouble reports from the LSPs
- Sectionalize and clear the trouble in its own network
- Test cooperatively with the LSP to identify and clear a trouble, when the trouble has been sectionalized to an LSP network

ATIS-0300032

- Keep their end user advised of the status of all trouble report(s)
- Perform cooperative analysis to determine if a trouble pattern exists
- Refer troubles to the LSP using the trouble reporting procedures
- Dispatch its own maintenance forces
- Perform verification tests to ensure that trouble has been cleared
- Perform scheduled testing and other maintenance services when requested
- Participate cooperatively with the LSP to further isolate and clear the trouble when trouble exists and cannot be sectionalized to the LSP or LSC portion
- Where it is technically feasible, signaling for all internetwork calls to a 10-digit telephone number should always be sent or received using 10 digits for the called party number, independent of how the call is dialed.

5.2 Local Service Provider (LSP)

The following are the responsibilities of LSPs:

- Provide trained personnel
- Advise the LSC when there is a potential service affecting LSP network failure
- Provide a contact number for trouble reporting that is readily accessible 24 hours a day, 7 days a week
- Maintain complete and accurate installation and repair records
- Consult with the LSC before making any changes that could affect service except under emergency conditions (See Clause on Network Modification)
- Provide access to test lines where appropriate
- Assume control functions for installation of the trunk(s)
- Coordinate with the LSC, ensuring that trunks are installed in accordance with the service request
- Notify the LSC of any changes affecting the service requested, including the service due date
- Accept trouble reports from the LSC
- Sectionalize and clear the trouble in its own network
- Test cooperatively with the LSC to identify and clear a trouble when the trouble has been sectionalized to the LSC network
- Perform cooperative analysis to determine if a trouble pattern exists
- Refer troubles to the LSC using the trouble reporting procedures
- Dispatch its own maintenance forces
- Clear troubles in its own network
- Perform verification tests to ensure that trouble has been cleared
- Provide status reports to the LSCs regarding installation and repair activity, or provides access to systems that will provide trouble status
- Perform scheduled testing and other maintenance services when requested
- Where it is technically feasible, signaling for all internetwork calls to a 10-digit telephone number should always be sent or received using 10 digits for the called party number, independent of how the call is dialed

6 Telecommunications Service Priority (TSP) Guidelines

This Clause provides TSP installation and maintenance guidelines for access services. This Clause further provides generic administrative procedures and interfaces between LSCs and the LSPs.

The TSP system provides for the priority treatment of National Security Emergency Preparedness (NS/EP) telecommunication services in order to prioritize their installation and maintenance.

In order for the TSP system to be effective, it **MUST** be incorporated into the day-to-day operating procedures for all LSPs and LSCs. All communications carriers are expected to cooperate in the installation and restoration of services with TSP that involve the facilities of more than one carrier.

6.1 Domestic NS/EP Services

The NS/EP TSP system and procedures provide priority treatment to the following domestic telecommunication services (including portions of U.S. international telecommunication services provided by U.S. providers) for which provisioning or restoration priority levels are requested, assigned, and approved:

- Commercially provided private services and public switched services

NOTE: Initially, the NS/EP TSP system's applicability to public switched services is limited to provisioning of such services (e.g., business, centrex, cellular, foreign exchange, Wide Area Telephone Service (WATS), other services that the selected vendor is able to provision, and restoration of services that the selected vendor is able to restore.

- Services that are provided by Government and/or non-common carriers and are interconnected to common carrier services assigned a priority level pursuant to Section 9 of the FCC's TSP system rules.

6.2 Control Services and Orderwires

The NS/EP TSP system and procedures are not applicable to authorize priority treatment to control services or orderwires owned by a service provider and needed for provisioning, restoration or maintenance of other services owned by that service provider. Such control services and orderwires shall have priority of provisioning and restoration over all other telecommunications services (including NS/EP services) and shall be exempt from preemption. However, the NS/EP TSP system and procedures are applicable to control services or orderwires leased by a service provider or user from another service provider.

6.3 Other Services

The NS/EP TSP system may apply, at the discretion of and upon special arrangements by the entities involved, to authorize priority treatment to the following telecommunications services:

1. Government or non-common carrier services which are not connected to common carrier- provided services assigned a priority level
2. Portions of U.S. international services that are provided by foreign correspondents

6.3.1 TSP Code Identification

The TSP Authorization Code is composed of twelve characters and is divided into two parts. The first nine characters comprise the TSP Control ID, a computer-generated number used for the government's tracking purposes. A hyphen is always the tenth character and it separates the TSP Control ID from the TSP Code. The final two characters are the TSP Code. The first character of the TSP Code (the eleventh character of the entire series) indicates the provisioning priority. Acceptable values are: E (Emergency), 1, 2, 3, 4, 5, or 0. A value of "0" indicates no provisioning priority is assigned.

The second character of the TSP Code (the twelfth character of the entire series) indicates the restoration priority. Acceptable values: 1, 2, 3, 4, 5, or 0. A value of "0" indicates no restoration priority is assigned.

A TSP Authorization Code is illustrated below:

T S P 1 2 3 4 5 C - 1 2
 | |
 Control ID Code

Figure 1: TSP Authorization Code

Table 1 below depicts the codes (eleventh and twelfth digits) allowable in the TSP system. A code of "0-0" indicates "Revocation", the removal of a previously assigned TSP code.

Table 6.1- TSP Codes Reference Table

TSP Provisioning/Restoration Priority Levels

	P-R	P-R	P-R	P-R	P-R	P-R	P-R	
	E-1	1-1	2-1	3-1	4-1	5-1	0-1	
	E-2	1-2	2-2	3-2	4-2	5-2	0-2	
HIGHER ↑	E-3	1-3	2-3	3-3	4-3	5-3	0-3	↓ LOWER
←	E-4	1-4	2-4	3-4	4-4	5-4	0-4	→
	E-5	1-5	2-5	3-5	4-5	5-5	0-5	
	E-0	1-0	2-0	3-0	4-0	5-0	0-0	

E = Emergency Priority Level

P = Provisioning Priority Level

R = Restoration Priority Level

6.4 TSP Installation

Circuits with an E (Emergency) provisioning priority have the highest priority and must be installed As Soon As Possible (ASAP), dispatching outside of normal business hours when necessary. Circuits with TSP provisioning priorities 1 - 5 will be installed by the due date according to the TSP provisioning priority assigned (see Table 1 above). For example, a circuit with a provisioning priority of "1" would be installed before a circuit with a provisioning priority of "2" when they both carry the same appointment date.

6.5 TSP Maintenance

Available resources should be allocated to restore NS/EP services as quickly as practicable, dispatching outside normal business hours to restore services assigned priority levels "1", "2" and "3" when necessary and services assigned priority levels "4" and "5" when the next business day is more than 24 hours away.

The day-to-day administration for repair and restoral of services assigned a TSP restoration priority is shown in the following examples:

6.5.1 Example 1

If there are several pending Trouble Reports for circuits that do not have TSP restoration codes, and a new Trouble Report is received for a circuit with a TSP code of 23, that Trouble Report becomes the next Trouble Report to be worked, ahead of the other circuit Trouble Reports that have no TSP restoration codes. Upon completion of the repair/restoral of the TSP23 circuit, work continues on the Trouble Reports for the circuits that have no TSP restoration codes.

6.5.2 Example 2

If there are several Trouble Reports to be worked (which includes a circuit with a TSP23 code), and two new Trouble Reports are received for circuits with higher TSP restoration codes (such as TSP21 and TSP22), the circuit Trouble Report with the TSP21 code becomes the next Trouble Report to be worked, followed by the TSP22 circuit Trouble Report. The TSP23 circuit Trouble Report would then move ahead of the other Trouble Reports for the circuits that have no TSP codes. Upon completion of the repair/restoral of the TSP21, TSP22 and TSP23 circuits, work then continues on the Trouble Reports for the circuits that have no TSP codes.

6.6 Competition for Resources Between Provisioning and Restoration Priorities

In general, service providers should restore existing services assigned TSP priority before provisioning new service; an exception is the provisioning of services assigned emergency priority, which should always be done before the restoration of services assigned restoration priorities "2", "3", "4" or "5". Restoration of any service assigned restoration priority "1" takes precedence over any other service assigned any other provisioning and restoration priority.

When two or more TSP services are competing for resources, the priority sequence listed below will ensure proper handling of these circuits:

- Restore TSP services with restoration priority of "1"
- Provision TSP services with provisioning priority of "E"
- Restore TSP services with restoration priority of 2, 3, 4, and 5
- Provision TSP services with provisioning priority of 1, 2, 3, 4, and 5

Using the priority sequence listed above, the following are examples of two TSP services competing for the same resources at the same time. The underlined TSP service has the higher priority and should be worked on first:

• TSP code 2-1 and E-2 both in trouble status	2-1
• TSP code 2-1 in trouble and E-2 to be provisioned	2-1
• TSP code 2-1 to be provisioned and E-2 in trouble	E-2
• TSP code 2-1 and E-2 to be provisioned	E-2

6.7 TSP Installation Preemption

Where facilities and/or equipment are not available to install a service assigned a TSP priority, preemption (interruption of an existing service) of a non-priority or lower priority circuit may be required. User consent is NOT required to preempt any user's existing service to provision an NS/EP service assigned a provisioning priority level "E" (Emergency) or to provision an NS/EP service assigned a provisioning priority level "1" through "5".

6.8 TSP Maintenance Preemption

Facilities of message circuits may be used for restoral of services assigned a TSP restoration priority after ensuring that sufficient message circuits are available for public switched network use.

Where facilities and/or equipment are not available to restore a service assigned, a TSP restoration priority preemption (interruption of an active service) may be required. Interruption of a non-priority or lower priority circuit is authorized for the purpose of restoring the service assigned a TSP restoration priority.

6.8.1 To Restore Interrupted NS/EP Services

User consent is not required to preempt any user's existing service to restore any NS/EP service assigned a restoration priority lever from "1" through "5".

6.8.2 NS/EP Services

If no suitable spare or non-NS/EP services are available, existing NS/EP services may be preempted to restore NS/EP services with higher priority level assignments. When this is necessary, NS/EP services will be selected for preemption in the inverse order of priority level assignment.

Service vendors who are preempting services will ensure their best effort to notify the service user of the preempted service and state the reason for, and estimated duration of, the preemption.

7 NXX Code Openings³

NOTE: For information related to NPA-NXX testing refer to ATIS-0300024, Next Generation Interconnection Interoperability (NGIIF) Reference Document Part V, Test Line Guidelines.

This Clause outlines the process and procedures for the testing of newly assigned Central Office NXX or NXX-X codes opened for the first time. In addition, this Clause provides references for the user to ensure that they are familiar with the obligations associated with obtaining codes and notifying the industry of the pending opening of CO NXX codes. In a Thousands Block Number Pooling environment the first thousands block that is opened in a NPA/NXX will follow the same rules as outlined in all NXX code opening procedures. NPA/NXX and NPA/NXX-X are interchangeable in NXX code opening scenarios throughout the NGIIF documentation. In these cases, the Code Holder is responsible for the testing.

The non-operational aspects contained in this Clause do not replace or supersede existing industry forum agreements or documents covering NXX or NXX-X Code opening processes. Listed below are specific documentation provided by the Industry Numbering Committee (INC) and NGIIF that provides guidance to Code Administrators, Service Providers and Service Customers when obtaining, activating, and testing NXX or NXX-X codes:

- ATIS-0300046, Recommended Notification Procedures to Industry for Changes in Access Network Architecture
- ATIS-0300010, Next Generation Interconnection Interoperability (NGIIF) Reference Document: Part II, Installation and Maintenance Responsibilities Switched Access Services Feature Group B, C, and D
- ATIS-0300032, Next Generation Interconnection Interoperability (NGIIF) Reference Document: Part X, Interconnection Between LECS Operations Handbook – Local Interconnection Service Arrangement (this document)
- ATIS-0300119, Thousands-Block (NPA-NXX-X) & Central Office Code (NPA-NXX) Administration Guidelines (TBCOCAG)

³ Clause 6 of ATIS-0300010, *Part II, Installation and Maintenance Responsibilities, Switched Access Services, Feature Group B, C, and D, of the NGIIF Reference Document*, includes the same information on NXX Code Openings. Any changes to this Clause should also be reflected in Clause 6 of ATIS-0300010, *Part II, Installation and Maintenance Responsibilities, Switched Access Services, Feature Group B, C, and D, of the NGIIF Reference Document*.

7.1 NXX of NXX-X CO Code Activation Planning

Service Providers requesting CO Code activation where the code involves the use of newly established switching facilities or additional interconnection trunking should perform the following prior to call through testing:

- Set up a planning session with the appropriate service providers where the code is being opened to determine what types of interconnection arrangements are required.
- Issue Service Orders (SO) to establish the appropriate facilities using the Access Service Request (ASR) and or translations using the Translation Questionnaire (TQ) for routing purposes.⁴
 - Access Service Request (ASR) Form Preparation Guide
(ATIS/OBF - ASR - 001)
 - Trunking Service Request Form Preparation Guide.
(ATIS/OBF - ASR - 004)
 - Translation Questionnaire (TQ) Form Preparation Guide
(ATIS/OBF - ASR - 019)

7.2 Pre-NXX or NXX-X Activation

The following reference is provided to aid in the performance of activation and testing of CO NXX or NXX-X Codes:

7.2.1 BIRRDS

Before a CO Code (NXX or NXX-X) can become active, the service provider requesting a new CO Code is responsible for either directly inputting the information in Part 2 of the CO Code Assignment Request form into BIRRDS, providing it to the Code Administrator, or another party with BIRRDS access for entry.

7.2.2 iconectiv® LERG™ Routing Guide

During the process of entering the new CO Code (NXX or NXX-X) in the iconectiv LERG Routing Guide the code holder must identify the points of interconnection in the LATA where the CO Code resides. In addition, the code holder shall immediately assign a number to be utilized for call through testing purposes upon receipt of the CO Code and shall place the test number in the iconectiv LERG Routing Guide when entering the CO Code into the iconectiv LERG Routing Guide.

7.2.3 Facilities

Offices attempting to complete a call through test to the new CO Code (NXX or NXX-X) when the facilities are not in place shall contact the code holder and inform them that the routing of calls will not take place until the appropriate facility orders have been completed.

In cases where orders have been placed with LECs for facilities, but have not been implemented, the LEC shall provide the appropriate support to ensure that the orders are complete and appropriate testing has been performed to meet the due date.

7.2.4 Points of Interconnection

In cases where points of interconnection in the home NPA have not been identified and/or facilities have not been placed, the code holder (NXX or NXX-X) will accept full responsibility for placing such orders with the local exchange carrier (LEC) and schedule the due date for facilities testing. This will ensure that the facilities are in place prior to the date of the code opening identified in the iconectiv LERG Routing Guide. The LEC cannot be expected to meet

⁴ Access Service Ordering Guidelines (ASOG), available at <https://www.atis.org/docstore/>.

the original effective date in the iconectiv LERG Routing Guide if all supporting information is not received in a timely manner.

If interconnection already exists between service providers and a CO Code is being opened, the code holder shall provide appropriate routing information in the iconectiv LERG Routing Guide to inform other service providers with which they do not have direct interconnection.

Where direct interconnection exists between service providers, it is presumed that all new CO Codes would be routed the same way as existing CO Codes, unless otherwise specified by the code holder in the ASR.

7.3 Translation Validation/Call Through Testing

The following process is outlined for the activation of new CO Codes (NXXs or NXX-X's) to provide assurance that routing and billing translations are tested/validated appropriately by service providers and IXC's. The following information also includes activities for serving switch change or tandem rehome of switch serving CO Codes (NXXs or NXX-X's)

Upon receipt of notification (the iconectiv LERG Routing Guide) that a new CO Code is to be activated all service providers shall ensure the integrity of routing and billing by the effective date in the LERG Routing Guide. For established CO Codes where there is a change to the serving switch or a switch tandem rehome the service providers, not directly interconnected with the service provider making the changes, will ensure routing and billing changes on the LERG Routing Guide effective date. The service provider(s) directly interconnected and the service provider making the changes will negotiate a time as to when the translations changes will take place.

The service provider assigned the new CO Code or implementing changes to the serving switch or implementing a switch tandem rehome will provide a test number that terminates to a recorded announcement (preferable) or milliwatt (1004 Hz) to provide assurance to personnel performing call through tests that they have indeed reached the terminating (serving) office.

Where billing is required, Automatic Message Accounting (AMA) validation shall take place by the service providers.

7.4 Intermediate Office(s) (Tandems/Access Tandems)

Intermediate Office(s) are those in which InterLATA and IntraLATA calls are routed to reach someone in a newly opened CO Code (NXX or NXX-X). Intermediate Offices shall:

- Complete all translations work five (5) calendar days prior to the date identified in the iconectiv LERG Routing Guide as the effective date.
- Perform Call Through testing starting five (5) calendar days prior to the date identified in the iconectiv LERG Routing Guide as the effective date.
- Identify problems during call through testing and resolve such problems prior to the effective date identified in the iconectiv LERG Routing Guide.
- For established CO Code(s) where there is a change to the serving switch or a switch tandem rehome, the service provider(s), not directly interconnected with the service provider making the changes, will ensure routing and billing changes are completed on the LERG Routing Guide effective date. The service provider(s) directly interconnected and the service provider making the changes will negotiate a time as to when the translations changes will take place. Testing will take place after the changes have been completed.

7.5 LEC Terminating Office (Serving Office)

The LEC Terminating Office/serving office is the office where a call terminates. The LEC will:

- Validate that all translations work is complete five (5) calendar days prior to the date identified in the iconectiv LERG Routing Guide as the effective date.
- Perform Call Through tests to ensure that calls can be initiated from the newly opened CO Code (NXX or NXX-X) starting five (5) calendar days prior to the date identified in the iconectiv LERG Routing Guide as

the effective date. An interLATA or intraLATA call, and an intraoffice call to an existing CO Code, where applicable, should be performed within the serving office.

- Perform, where applicable, an intraoffice call from an existing CO Code within the serving office to the newly opened CO Code.
- Identify problems during call through testing and resolve such problems prior to the due date identified in the iconectiv LERG Routing Guide.
- For established CO Code(s) where there is a change to the serving switch or a switch tandem rehome the service provider responsible for the terminating office will ensure routing and billing changes are completed on the LERG Routing Guide effective date. The service provider responsible for the terminating office will negotiate with the interconnected service provider(s) as to the time when the translations changes will take place.

NOTE: If the above functions are not performed, the originating office and intermediate office cannot perform their respective functions.

7.6 Originating Office

LEC end offices with direct interconnection to, or located within the same NPA as the LEC with the newly opened CO Code (NXX or NXX-X), will:

- Validate that all translations work is complete five (5) calendar days prior to the date identified in the iconectiv LERG Routing Guide as the effective date.
- Initiate a call through test to the test number to ensure that the call routes correctly. Call through testing should start no earlier than five (5) calendar days prior to the date identified in the iconectiv LERG Routing Guide as the effective date.
- Identify problems during call through testing and resolve such problems prior to the effective date identified in the iconectiv LERG Routing Guide.
- For established CO Code(s) where there is a change to the serving switch or a switch tandem rehome the service provider(s), not directly interconnected with the service provider making the changes, will ensure routing and billing changes are completed on the LERG Routing Guide effective date. The service provider(s) directly interconnected and the service provider making the changes will negotiate a time as to when the translations changes will take place.

7.7 Mechanized Testing

Where mechanized translation input and validation is available, such mechanized capabilities should be used to validate the routing and AMA capability. This function should be performed on or before the effective date identified in the iconectiv LERG Routing Guide.

7.8 Verification of NXX or NXX-X Code Openings, Switch Change/Rehome, or Switch Tandem Rehome Process

During the CO Code (NXX or NXX-X) opening, switch change/rehome, or switch tandem rehome process, the code holder may want to verify that test calls to the CO Code have been completed. It is recommended that entities performing call through tests to CO Codes being activated or moved provide the necessary Caller ID information required to verify the NPA-NXX or NPA/NXX-X from which the test call is being placed. Where contractual, technical, or regulatory restrictions apply, Caller ID capability cannot be utilized.

7.9 NXX or NXX-X Code Opening, Switch Change/Rehome, or Switch Tandem Rehome Process in Jeopardy Situations

The NGIIF recommends immediate reporting of non-circuit-specific troubles via telephone in order to facilitate the rapid restoral of service.

If prior to the LERG Routing Guide effective date for an NXX or NXX-X code opening, change in serving switch or switch tandem rehome, a Code Holder realizes that any problem in its own network may jeopardize the scheduled NXX or NXX-X code opening date, serving switch change or switch tandem rehome, the Code Holder will notify the interconnected carrier(s) immediately.

If prior to the LERG Routing Guide effective date for a NXX or NXX-X code opening, change to the serving switch or switch tandem rehome, an interconnected carrier realizes that it will not be able to meet the LERG Routing Guide effective date for NXX or NXX-X code opening, serving switch change or switch tandem rehome, the NXX or NXX-X code, that carrier will notify the Code Holder and other interconnected carrier(s) immediately.

Any carrier that identifies a problem within another carrier's network during call through testing will notify that carrier immediately.

Contact should be made using industry escalation procedures or published/mutually agreed to contact information.

8 Trunk Installation

Installation, as referred to in this document, pertains to that portion of the total provisioning process that starts when the service order is received by the LSP and ends when the LSC accepts the trunk(s). Installation includes additions and rearrangements.

The LSC will order the trunk(s) through a service order center, or equivalent, and all inquiries will be referenced by the service order number and trunk group identification. The trunk group identification consists of a Trunk Group Serial Number (TGSN); also referred to as the Two-Six Code, which is a shorthand version of the initial portion of the Common Language® Message Trunk Circuit Code (CLCI™ MSG Code) trunk information. The complete 41-character CLCI MSG Message Circuit Code structure includes the TGSN and the 11-character Common Language Location Code (CLLI Code) and is used to identify the message trunk group.

The LSP will ensure that all portions of the trunk(s) are installed properly and that the Due Date is met. Should any condition jeopardize a Due Date, the LSP will notify the LSC and the LSP's service order center, or equivalent.

The point where the trunk(s) and the facilities/equipment are connected is referred to as the Point of Termination (POT). It is the responsibility of the LSC to arrange for suitable environmental requirements at the POT if requesting co-location. The space furnished shall be in a safe working area and will be accessible during normal working hours for installation and maintenance purposes. If a virtual co-location environment is requested or provided, the requesting LSC selects the equipment and the installation vendor from an approved list meeting the LSP's requirements for installation at the POT. The requesting LSC is responsible for training, spares, equipment and alarm monitoring. The LSP should provide an approved equipment and vendor list, arrange for suitable environmental and space requirements. The LSP may perform installation, maintenance or service hours (a time and material basis) upon request. Mutually agreed upon access to the location may be provided on a prearranged basis as determined by the LSC and the LSP.

8.1 Pre-Service Testing

Pre-Service Tests are basic tests performed to ensure that the trunk(s) have been designed, installed, and aligned. These tests are performed at the direction of the LSP.

Pre-Service Testing should be completed no later than the Plant Test Date.

In those cases where automatic testing or access to test lines is available, these methods will be used in lieu of more labor-intensive methods. The LSP must verify that the LSC has made its portion of the circuit available for Pre-Service Testing.

8.2 Acceptance Testing

Acceptance Testing must be completed prior to the turn up of service (Due Date).

Acceptance Testing may involve both LSP and LSC personnel and will be based on local tariffs or negotiated contracts to verify proper trunk(s) installation.

Prior to the Due Date, the LSP will contact the LSC to determine when the trunk(s) will be ready for Acceptance Testing. The LSC has the option of accepting the trunk(s) with or without Acceptance Testing. A mutually agreeable date and time will be established to coordinate any basic and/or Additional Cooperative Acceptance Testing (ACAT).

Either the LSC or the LSP may perform additional operational and/or transmission tests by utilizing terminating test lines at the distant end of the circuit.

The LSC has the option of turning up the trunk(s) for traffic prior to the Due Date if the installation work is completed by the LSP and acceptance testing is completed or waived by the LSC.

If the LSC requests turn-up of a trunk(s) prior to the Due Date, the LSP must verify that the LSC accepts any applicable billing coincident with turn-up of the trunk(s). Upon turn-up of the trunk(s) the order(s) will be processed per industry agreements.

If the LSC decides to delay billing until the Due Date, the trunk(s) should be made busy to ensure it is not used until billing begins. On the Due Date, the trunk(s) will be turned-up for service and the order(s) will be processed per industry agreements.

Where the Pre-Service Test results indicate the trunks(s) is within Acceptance Limits, the LSP will offer the LSC a copy of those test results in lieu of performing cooperative Acceptance Testing. The LSC has the option of accepting the service based on the Pre-Service Test results or by requesting a combination of basic and/or ACAT. If the LSC accepts the service based on the Pre-Service Test results, the LSP will forward a copy of the results to the LSC upon request.

The results of the Acceptance Tests must be within the Acceptance Limits for the service provided. Once the circuits are verified to be within the allowable range, additional time will not be spent making additional adjustments or retests. If the LSC requests that the LSP's technician stay on the line to make subsequent tests or optimize circuit adjustments, etc., this may be treated as billable.

If Acceptance Testing is performed and the test results are not within Acceptance Limits, sectionalization must be performed to determine where the problem is located.

Once the Acceptance Tests have been completed and accepted by the LSC, the LSP will make the trunk(s) busy to prevent selection and/or false seizures until the LSC requests service turn up.

If the LSC is not available to perform Acceptance Tests at the scheduled appointment time, the following alternatives are applicable:

- The LSC may reschedule the Acceptance Testing
- The LSC may waive Acceptance Testing and accept the trunk(s). Any tests desired by the LSC at a time later than the Due Date and after acceptance of the trunk(s) will be arranged by contacting the LSP and may be billable as Non-Scheduled Testing
- The LSC may request additional Stand-By Time from the LSP. This additional time is at the discretion of the LSP and is subject to the availability of scheduled personnel
- The LSC may change the Due Date
- The LSC may cancel the access order

If the LSC is unable to accept the trunk(s) within thirty (30) calendar days of the original Due Date, the LSC has the choice of either canceling the Service Order or getting billed for the service starting on the 31st day. The circuits shall be left in a make-busy state.

Any testing requested by the LSC after billing has commenced will be arranged for by the LSP and may be billable.

The LSC has the responsibility to determine Glare Master based on the following alternatives:

- LSC as Glare Master (default)

- LSP as Glare Master
- Trunk Circuit Identification Code (TCIC) where interconnecting companies' technology exists:
 - The LSC is Glare Master for odd-numbered circuits (SS7 only)
 - The LSP is Glare Master for the even-numbered circuits (SS7 only)

Implementation of the hunting methodology to mitigate the occurrence of Glare should take into account the differing options, their compatibility and efficiency, and should be based on local negotiations.

Where digital equipment is used, synchronization/loop timing options should be verified. Where synchronization problems are encountered, both the LSP and the LSC should work cooperatively to resolve the trouble. Synchronization problems that cannot be resolved by internal organizations should be referred to each carrier's Synchronization Coordinator or appropriate organization.

8.3 Additional Cooperative Acceptance Testing

Any requested transmission measurements or signaling tests that are not covered in the Basic Acceptance Testing tariffs or negotiated contracts shall be considered ACAT and may be billable.

Trunk(s) are designed to meet ordered transmission parameters. If it is determined that the trunk(s) do not meet the ordered parameter requirements, the LSC will not be billed for the tests that failed on a per trunk(s) basis. The LSP must determine whether the problem is due to an improper design or trunk trouble. The problem must be corrected prior to trunk turn-up or order completion reporting. If the LSC requests a retest of the repaired trunk, the initial retest will be non-billable. Subsequent re-tests will be billed as ACAT if the trunk meets designed parameters.

8.4 Traffic Routing and Billing Acceptance Testing

Outlined below are guidelines associated with Call Through Testing to provide assurance for the appropriate routing and generation of billing records.

When establishing a new trunk group or engaging in a rearrangement of an existing trunk group, the LSC shall perform, at a minimum, a call through test to a number furnished by the LSP. The switch supporting the furnished telephone number shall provide answer supervision.

The LSC shall initiate test call(s) to ensure that correct AMA recording and routing occurs. The scheduling of this call(s) shall be negotiated by the interconnecting companies, so that the ASP can validate that the correct AMA recording and routing has taken place for the trunk group under test. The validation results, or the acknowledgment that routing and recording is functioning, shall be provided to the LSP upon request.

When establishing a new trunk group or engaging in a rearrangement of an existing trunk group, the LSP shall perform, at a minimum, a call through test. The switch supporting the furnished telephone number used for testing purposes shall provide answer supervision.

Upon completion of the call through test(s), the LSP shall validate that this call(s) was recorded for billing purposes. In addition, the LSP shall ensure that the call is routed over the correct trunk group. The validation results, or the acknowledgment that routing and recording is functioning, shall be provided to the LSC upon request.

8.5 Completion

Service Order completion is contingent on the LSC accepting the service as requested on the Service Order.

Upon completion of the Service Order, the following information will be recorded:

- Name of the LSC representative accepting the service
- Basis of the acceptance
 - Test results
 - Test waived

8.6 Expedites

The Tariff, or negotiated contract for trunk(s), may provide an ordering option to request service with less than standard order intervals. These shortened-interval orders are referred to as "Expedites". Expedites may carry additional charge(s).

8.7 Trunk Disconnects

Before either the LSP or LSC disconnects a trunk(s), they will contact the interconnected company to coordinate the activity.

If the disconnect order is canceled or changed by the LSC, the LSC must then contact the LSP to avoid service disruptions.

8.8 Trunk Rearrangements

Rearrangements of a trunk(s) include changes in equipment, software assignments or facilities, and can be accomplished individually or cooperatively. Rearrangements may require a Service Order and coordination.

Requests for Trunk Make Busy and Non-Scheduled Testing should be referenced in cases where rearrangements to trunks do not require both the LSP and the LSC to be involved.

When a rearrangement requires a change to the trunk(s), the requesting LSP or LSC will contact the interconnected company and negotiate when the rearrangement, testing, and restoral will take place.

When a rearrangement potentially affects a transmission parameter, the LSC and the LSP may cooperatively test and verify that the trunk(s) are within Acceptance Limits.

Upon completion of the rearrangement, the initiating LSC or LSP will coordinate any testing necessary to ensure the rearrangement was performed satisfactorily.

Rearrangements may be billable.

8.9 Coordinated Conversion

Coordinated conversions are processes that may be used to facilitate changes requested by one interconnecting company that involve the reuse of portions of the former interconnected company's equipment and/or facilities previously assigned. Coordinated conversions require the issuance and processing of related disconnect and connect orders and the coordination of these orders throughout the entire conversion process.

The requesting interconnecting company is expected to bear full responsibility for the overall coordination of the various service orders associated with the conversion activities involved with its end-to-end service.

Where a coordinated conversion involves a change of service from one interconnecting company to another, the requesting interconnecting company will establish and coordinate conversion activities with other interconnecting companies and the End User when required. Those activities will include, but are not limited to:

- Completion Testing and Notification
- Requests for Continuation of Service
- Conversion Timing
- Circuit Release
- Circuit Conversion Sequence

Every effort must be made jointly by the new ASC and the ASP to successfully complete the conversion. If the new ASC encounters difficulties in activating end-to-end service following acceptance testing on the ASP provided

facilities, the new ASC may negotiate and coordinate continuation of the use of the previous arrangement with the ASP and former ASC, and the restoral procedure should commence.

Since continuation of the former ASC service does not automatically defer the due date of the disconnect order, the new ASC must request the former ASC to contact the ASP ICSC, or equivalent, to request a due date change in order to prevent the disconnect of the former ASC service. This must take place prior to the disconnect due date.

It is the responsibility of the ASP to inform the new ASC that all work involved in restoring the former ASC service and subsequent cut-over activities of the new ASC facilities is above and beyond that required for normal coordinated conversion cut-overs. This work may result in appropriate additional labor charges.

9 Trunk Maintenance

Maintenance of trunk(s) is based on the premise that each company has the responsibility for monitoring the performance of all trunks under its control. However, the company detecting trunk trouble or service impairment will take corrective action as outlined below. This does not include any responsibility for sectionalization beyond the POT or the repair of equipment or facilities owned by the other company.

Investigation of chronic trunk failures will involve the exchange of information between interconnected companies relative to the chronic failure. A detailed investigation should be made to determine the cause of the trouble condition. This activity may involve cooperative testing and may be handled as an impaired trunk trouble report.

All trunk(s) failing Maintenance Limits or Immediate Action Limits per GR-334, *Switched Access Service: Transmission Parameter Limits and Interface Combinations* will be restored to within Acceptance Limits.

9.1 Trouble Detection Responsibilities

When LSC personnel become aware of an inoperative trunk(s) (See Note 1), LSC personnel will ensure that the trunk(s) is removed from service. When LSP personnel become aware of an inoperative trunk(s), the LSC will determine the action to be taken. The above actions should be performed immediately after identification of the inoperative condition to prevent service failures.

NOTE 1: Inoperative trunks are those that do not work in service.

When LSP personnel become aware of an impaired trunk(s) (See Note 2), the LSC will determine the action to be taken. If maintenance is to be delayed, a mutually agreed upon time will be negotiated for removal from service and trouble sectionalization.

NOTE 2: Impaired trunk(s) are those that exhibit intermittent failures or degraded transmission performance. Impairment includes improper synchronization that can cause slips and chronic trunk/facility failures.

It is recommended that all routine and scheduled maintenance activities be performed during low traffic periods and not during Network Modification Suspension Periods to minimize the impact to the least number of customers. If customer service is affected by a trouble condition during periods of heavy calling, the minimum work activity to restore the service to a stable performance state should be undertaken and complete service recovery activities scheduled for a period of lighter traffic.

Where available, Automatic Trunk Testing (e.g., Automatic Progression Trunk Testing) may be performed. This capability can be configured to perform "operational" tests (e.g., 102 milliwatt or 103 synchronous) on a recurring basis. Compatible testline access is required in order to implement/continue such testing. The trunks that fail such testing should be removed from service and repaired.

9.2 Sectionalization

Sectionalization is a joint responsibility of the LSC and the LSP, with control for sectionalization under the direction of the LSC. It is anticipated that sectionalization may involve cooperative testing; both entities are expected to participate in this activity when requested.

9.3 Trouble Reporting

The NGIIF recommends immediate reporting of non-circuit specific troubles via telephone in order to facilitate the rapid restoral of service.

Each company will provide a 24-hour, 7-day point of contact and telephone number for Trouble Reporting.

The LSC will be responsible for the acceptance of trouble reports from their end user. The LSC should first test to determine if a trouble is in their network. If the trouble is found in their network, the LSC will clear the trouble and no referral to the LSP is necessary. If the trouble is sectionalized by the LSC towards the LSP, the trouble report will be referred to the LSP. The LSP will clear the trouble or will work cooperatively with the LSC to sectionalize the trouble where necessary.

The following information should be exchanged when handing off or referring the trouble:

- Trouble report number or equivalent
- Contact telephone number
- Contact ID (i.e., name or initials)
- Time and date report was received from LSC
- LSC testing information (if requested by LSP)
- Circuit ID (41-Character CLCI MSG Code)
- Non-Circuit specific (Circuit ID may not be appropriate)
- Trouble reported
- Other information that may be of assistance (e.g., history, subsequent reports)
- Dispatch Authorization

9.4 Repair Verification

When a trouble has been closed out by the LSP, the LSC may perform a repair verification test. If the repair verification test identifies a trouble condition(s), cooperative repair verification tests may be performed when requested.

The dispatch of an employee to make verification tests when a trouble has been cleared without dispatching will not normally take place. Requests for dispatch that result in a no trouble found condition may result in additional charges.

To perform repair verification tests, it may be necessary for the trunk to be made busy. Make-busy requests will be handled in accordance with established procedures.

9.5 Non-Trunk Specific Troubles

Non-trunk specific troubles are those that are not directly attributable to a given trunk. Non-trunk specific troubles generally fall into the following categories:

- Reorder
- No Ring
- Wrong number or misdirected
- Transmission Impairment
- Cut-off
- No answer supervision
- Other

When the non-trunk specific trouble has been detected and sectionalized, the trouble report will be referred to the appropriate company's trouble reporting center or equivalent.

9.6 Trouble Report Clearing Information

When the trouble has been cleared by either the LSP or the LSC, the trouble report will be closed out with the originating company and the following information will be exchanged:

- Trouble report number or equivalent
- Date and time cleared
- Trouble status (temporary or permanent repair)
 - If temporary, estimated time for restoral
- Contact name or initials and telephone number of the persons closing out the report
- Type & nature of trouble found and action taken
- Testing information (if requested)
- Trunk ID (if applicable)

All SS7 ISUP trunk and non-trunk specific troubles are covered in ATIS-0300013, *Next Generation Interconnection Interoperability (NGIIF) Reference Document: Part III, Installation, Testing and Maintenance Responsibilities for SS7 Links and Trunks Attachment B ISUP Compatibility Tests*.

9.7 Priority of Restoration

Trouble reports on trunk(s) will be given equal treatment by maintenance forces. However, in cases where one or more trunk(s) are out of service within a group and causing the group to overflow, such trouble reports may be given a higher priority for restoral.

9.8 Make-Busy Procedures

On any request for make-busy, the receiving company will initiate a trouble report or utilize the trouble report number provided by the initiating company. The trouble report will be an information report and will be used for future reference.

Make-busy procedures must be followed to ensure that the LSC or LSP request is properly and expeditiously handled. The company requesting the make busy of the trunk(s) or trunk group will contact the interconnected company with the necessary information at the time of the request.

Where a request is made to make busy a trunk or group of trunks for activities other than trouble resolution (e.g., routine maintenance, network management request), the previously outlined procedures shall be followed.

Conditions may exist where trunks/trunk groups are required to be made busy or released manually as soon as possible. If the request cannot be handled immediately, the LSP will inform the LSC of the nature of the delay and the ticket number. The request will be handled as soon as possible or based on local negotiations.

Interconnecting companies will inform each other if this activity is billable. Upon authorization, all time spent on the trunk /trunk group Make-Busy and its restoration may be billable.

9.9 Restoration

The LSCs and LSPs must ensure that trunk(s) and trunk group(s) made busy are in proper operating condition before returning them to service.

9.10 Hold and Trace Trouble Isolation

It may be necessary to request a Hold and Trace to resolve a difficult trouble that cannot be identified by conventional testing. Information should be exchanged between the LSP and the LSC when the request for Hold and Trace is made. The interconnecting companies will hold the trunk and release the end users. The trouble will be sectionalized and repaired.

9.11 Call Traces

The objective of emergency call tracing is to identify the source of an in-progress call for urgent assistance in the case of life threatening situations or property damage. In the case of non-emergency traces (e.g., Toll Fraud, computer hacking), the following processes still apply. These traces may require the involvement of many interconnecting companies. Any interconnecting company receiving such a request will initiate the trace on an expedited basis recognizing the emergency situation.

Requests for trace should come from a company's security organization in compliance with their security guidelines. The exchange of information relative to these traces will be handled according to local security guidelines.

The originator of an emergency call trace assumes responsibility for the validity of a trace request and also is the controlling entity. When an emergency trace is passed to another interconnecting company, they will trace the call to the distant interconnected company and provide them with information to continue the trace. After completion of the trace, the distant interconnected company will provide the information to the originator, either directly or via another interconnected company. The controlling entity may remain online throughout the trace.

The information to be exchanged should include the following:

- Circuit identification (41-character Common Language Message Trunk Circuit Code (CLCI MSG Code) of the trunk under trace
- Called or Calling Number
- Employee name, call back telephone number, and the name of the controlling entity originating the trace
- Any additional information or instructions

If there will be any delay in completing the trace, such as when a dispatch to an unattended office is required or when personnel are not available, the reporting office will advise the originator of the reason for the delay and its expected duration.

9.12 Network Modification

A Network Modification is any type of planned equipment, software, trunk or facility activity that has the potential to significantly affect interconnected networks (e.g. rearrangement of existing network elements, switch homing arranges, SS7 rehomeing)

The NGIIF has developed the following guidelines outlining the medium by which internetwork affecting maintenance activity notification will be provided to the interconnected company and the time frame prior to the planned activity:

- Notification when possible should be made at least 5 working days prior to the planned change activity.
- Notification should be made in the form of:
 - E-Mail (recommended where available)
 - FAX
 - Telephone call
- Notification should be provided to the affected company's appropriate notification center. Contact information is included in the NGIIF Service Provider Contact Directory. An example of a notification form

is located in ATIS-0300026, *Next Generation Interconnection Interoperability (NGIIF) Reference Document: Part VI, Network Management Guidelines*.

When network modifications are scheduled that could significantly affect traffic between directly interconnected networks, it is recommended that the affected LSPs and LSCs will notify each other prior to the event.

The following information should be exchanged at the time of notification:

- Originator (company name/contact number)
- Affected network element
- Date and time of the change
- Expected duration
- Traffic types affected during change
- Description of the work to be completed.

9.12.1 Network Modification Suspension Periods

Due to the volumes of traffic and the potential for negative impacts to the Network, the following table identifies when Network Modifications should not be performed.

Table 9.1- Network Modification Suspension Periods

Event	Start of Suspension Period (Inclusive)	End of Suspension Period (Inclusive)
Mothers Day	SATURDAY	MONDAY
Fathers Day	SATURDAY	SUNDAY
Thanksgiving (US Only)	WEDNESDAY	MONDAY
Christmas	12/22	12/26
New Years	12/31	1/1

Network modifications (e.g. Generic Changes, Parameter Changes, Switch Rehomes) will not occur during the above-mentioned time periods unless agreed to by the LSP and LSC.

Emergency exceptions should be coordinated.

9.13 LEC-LEC Non-Trunk Operational Agreements

9.13.1 Line Identification/Verification

The Automatic Number Announcement Circuit (ANAC) provides the capability to dial a number to identify a local loop that a field technician is working on. Where there are multiple local service providers and facilities are shared, there may be instances of each service provider having a different number to be dialed to access the ANAC. It is preferable to have a single number within a geographic area in order to alleviate any confusion on the part of the maintenance field forces. In the event that a universal number cannot be agreed upon, then the service providers shall negotiate and exchange ANAC access numbers.

The FCC requires the linking of the calling number and calling name such that the presentation status is either "presentation allowed" or "presentation restricted". In order to reduce unnecessary queries to the calling name (CNAM) database, the carrier should rely on the Calling Party Number Parameter field in the IAM to control whether or not the name and number be delivered to the called party. If the presentation status in the IAM is set to "presentation allowed", the carrier may reveal both the calling number and the calling name to the called party. If the presentation status in the IAM is set to "presentation restricted", the carrier will not reveal the caller's number or name to the called party. No calling name in the CNAM database should be preset to "private" or "public".

10 Exceptions

The following information is provided in an effort to assist LSPs and LSCs in the resolution of trouble reports that fall outside of the normal ticket resolution flow, once the original ticket has been closed out.

10.1 Line Identification/Verification

The ANAC provides the capability to dial a number to identify a local loop that a field technician is working on. Where there are multiple local service providers and facilities are shared, there may be instances of each service provider having a different number to be dialed to access the ANAC. It is preferable to have a single number within a geographic area in order to alleviate any confusion on the part of the maintenance field forces. In the event that a universal number cannot be agreed upon, then the service providers shall negotiate and exchange ANAC access numbers.

10.2 Calling Party Number (CPN), Calling Party Name (CNAM)

10.2.1 Calling Party Number (CPN)

The NGIIF recommends that the Calling Party Number field should be populated, by the originating network, with a valid 10-digit NANP subscriber line number or directory number.

10.2.2 Linking CPN & CNAM

The FCC requires the linking of the calling number and calling name such that the presentation status is either "presentation allowed" or "presentation restricted". In order to reduce unnecessary queries to the calling name (CNAM) database, the carrier should rely on the Calling Party Number Parameter field in the IAM to control whether or not the name and number be delivered to the called party. If the presentation status in the IAM is set to "presentation allowed", the carrier may reveal both the calling number and the calling name to the called party. If the presentation status in the IAM is set to "presentation restricted", the carrier will not reveal the caller's number or name to the called party. No calling name in the CNAM database should be preset to "private" or "public".

11 Escalations

Escalation is a means of bringing problems to the attention of individuals who have the responsibility and authority to expedite corrective action.

When either the LSP or the LSC experiences installation or maintenance difficulties and progress toward resolution is not satisfactory, either company may contact the other company for escalation to a higher level of management.

The rate at which a problem is escalated through successive levels of management should allow each level a reasonable period of time to resolve the problem before it is presented to the next level for action.

Escalation procedures and contacts are based on local negotiations.

12 Test Lines

It is the recommendation of the NGIIF that all companies provide test lines and test line information to facilitate installation testing and trouble resolution.

Access should be provided to the terminating test lines in the interconnected companies' end offices and/or Access Tandems, a listing of the available test line numbers can be obtained from the Test Line Coordinator of each company. Trouble Reporting/Repair Contact Information is listed in the NGIIF Service Provider Contact Directory.

Any problems associated with test lines/numbers should be referred to the appropriate company's trouble reporting center.

13 Additional Billing

This Clause describes the scenarios under which additional billing may take place.

Provisions have been made for additional billing in the following categories:

- Overtime for Installation and Repair
- Additional Cooperative Acceptance Testing
- Non-Scheduled Testing
- Maintenance of Service Charge
- Stand-By Time
- Other Labor

Accurate records regarding the work performed for additional billing purposes must be retained, which includes identification of personnel engaged in these work activities. It is the responsibility of the billing company to determine when additional billing applies and document the name of the person authorizing the additional billing.

Overtime is the time spent by personnel doing the installation and repair functions outside their normal working hours. Overtime installation and repair charges are based on individual company tariffs.

13.1 Billable Overtime Installation and Repair

Billable overtime must be authorized by the LSC.

Billable overtime hours begin at the start time requested and end when the work is completed or suspended. This includes travel time to and from a home or work location.

If applicable, a minimum charge for a call out may be applied.

13.2 Additional Cooperative Acceptance Testing (ACAT)

Time required to perform ACAT may be considered billable to the LSC.

13.3 Non-Scheduled Testing

When the LSC determines a need to test its services, they will contact the LSP to perform non-scheduled testing.

13.4 Maintenance - Service Charge

The LSC may be responsible for a service charge whenever the trouble/problem is not in the LSP's network and/or is isolated back to the LSC's network or end user's equipment/facility.

If trouble is subsequently found to be in the LSP's equipment or facilities and a Maintenance Service Charge has been applied, the charge will be canceled or adjusted.

13.5 Stand-By Time

Stand-By Time in excess of one half (1/2) hour authorized by the LSC may be billable and is predicated on local negotiated agreements and shall be documented by both the LSP and LSC.

13.6 Other Labor

As agreed to by the LSC and the LSP, other labor is anything not identified in the above billing Clause.

14 Local Recorded Announcements

14.1 Mandatory 10 Digit Local Dialing

In areas where 10-digit dialing is mandatory to complete local calls, the following wording is recommended for the announcement to be played if a customer dials only a 7 digit local number without an area code:

"We're sorry. When placing a local call, it is now necessary to dial an Area Code followed by the 7-digit number. Please hang-up and redial using the complete 10-digit number."

14.2 Intercept Number Announcement - Ported Numbers

Intercept Treatment should be provided by the recipient's switch where the ported number has been disconnected and is aging the number. Release With Cause should not be used during the aging period. At the end of the aging period, the disconnected number should snapback to the Code Holder for that code. The Code Holder for that code is then responsible for providing the Intercept Treatment. Any subsequent call to the disconnected number (after snapback) misrouted to the recipient switch should be given Cause Code 26 treatment.

15 Local Number Portability

15.1 Local Number Portability

In a local number portability environment, the Jurisdictional Information Parameter (JIP) in the SS7 ISUP Initial Address Message (IAM) should be populated at each call origination per T1.TRQ.02-2001, *Number Portability Switching Systems (Revision of T1.TRQ.2-1999)*.

15.2 Default Routing Translations

All interconnecting parties, for LNP purposes, should agree on having "Default Routing Translation" in place prior to implementation of LNP. Acceptance of inter-network LNP queries should be locally negotiated.

Carriers may block default routed calls in specific circumstances when failure to do so is likely to impair network reliability.

If the N-1 carrier experiences LNP database congestion and receives a 10-digit Automatic Code Gap (ACG) from its database, it should gap the queries to its LNP database for that 10 digit DN and abort the call. If the N-1 switch receives a 3 or 6-digit ACG from its database, it should gap such queries to its LNP database and default route the call. If the database fails to respond to a query from the N-1 switch, the call is default routed.

If the default carrier experiences LNP database congestion (e.g. - the default switch receives an Automatic Code Gap (ACG) from its database), it should gap the queries to its LNP database and abort the call.

15.2.1 Background

If a carrier cannot successfully query an LNP database, it should default route the call based on the dialed digits to the default carrier.

A “default routed call” situation may occur in a LNP environment when a call is made to a telephone number in an exchange with any ported numbers, and the N-1 carrier (or its contracted entity) queries a Number Portability database to determine if the called number has been ported. If the N-1 carrier fails to perform the query, the call is then routed by default to the service provider that originally serviced the telephone number. The original service provider, which may or may not still be serving the called number, should try to complete the call which may include an LNP database query.

15.3 Handoff of Terminating

In an LNP environment, the N-1 Carrier is responsible for making sure that calls to numbers in portable NPA NXXs have an LNP query performed.

If the N-1 carrier arranges with another entity to perform some or all of the LNP queries on their behalf, the N-1 carrier should make sure that proper trunking (e.g., meet-point billing trunks) and billing mechanisms to the recipient service provider are in place. This will ensure that the calls will complete and access billing will work properly.

16 Common Channel Signaling System 7 (CCS7)

ATIS-0300011, *Next Generation Interconnection Interoperability (NGIIF) Reference Document: Part III, Installation and Maintenance Responsibilities for SS7 Links and Trunks*, describes the responsibilities for the installation and maintenance of SS7 Links and Trunks.

In the case of a LEC to LEC interconnection, where the term ASP is used in the above-mentioned ATIS-0300011, the term LSP may be substituted. Where the term ASC is used in the above-mentioned ATIS-0300011, the term LSC may be substituted.

17 Installation, Testing & Maintenance of Transport Facilities

ATIS-0300030, *Next Generation Interconnection Interoperability (NGIIF) Reference Document: Part IX, Installation, Testing and Maintenance Responsibilities of Facilities*, describes the responsibilities for the installation and maintenance of facilities.

18 Network Management Guidelines

ATIS-0300026, *Next Generation Interconnection Interoperability (NGIIF) Reference Document: Part VI, Network Management Guidelines*, describes responsibilities associated with network management.

In the case of a LEC to LEC interconnection, where the term ASP is used in the above-mentioned ATIS-0300026, the term LSP may be substituted. Where the term ASC is used in the above mentioned ATIS-0300026, the term LSC may be substituted.

19 Special Services

ATIS-0300009, *Next Generation Interconnection Interoperability (NGIIF) Reference Document: Part I, Installation and Maintenance Responsibilities Special Access Services, WATS Access Lines and Switched Access Services Feature Group A*, describes responsibilities for the installation and maintenance of Special Services.

20 Security

LEC-LEC Security Guidelines are outlined in ATIS- 0300033, *Part X, Interconnection Between LECS Operations Handbook – Local Interconnection Service Arrangement, Attachment A, Security Guidelines*.



ATIS-0300033

**Next Generation Interconnection Interoperability (NGIIF)
Reference Document**

**Part X, Interconnection Between LECS Operations
Handbook – Local Interconnection Service Arrangement**

**Attachment A
Security Guidelines**

Version 12.0



ATIS is the leading technical planning and standards development organization committed to the rapid development of global, market-driven standards for the information, entertainment and communications industry. More than 200 companies actively formulate standards in ATIS' Committees, covering issues including: IPTV, Cloud Services, Energy Efficiency, IP-Based and Wireless Technologies, Quality of Service, Billing and Operational Support, Emergency Services, Architectural Platforms and Emerging Networks. In addition, numerous Incubators, Focus and Exploratory Groups address evolving industry priorities including Smart Grid, Machine-to-Machine, Connected Vehicle, IP Downloadable Security, Policy Management and Network Optimization.

ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications' Sectors, and a member of the Inter-American Telecommunication Commission (CITEL). ATIS is accredited by the American National Standards Institute (ANSI). For more information, please visit www.atis.org.

Notice

This document was developed by the Alliance for Telecommunications Industry Solutions' (ATIS) sponsored Next Generation Interconnection Interoperability Forum (NGIIF). The NGIIF addresses next-generation network interconnection and interoperability issues associated with emerging technologies. Specifically, it develops operational procedures which involve the network aspects of architecture, disaster preparedness, installation, maintenance, management, reliability, routing, security, and testing between network operators. In addition, the NGIIF addresses issues which impact the interconnection of existing and next generation networks and facilitate the transition to emerging technologies. All changes to this document shall be made through the NGIIF issue resolution process.

Note Regarding Previous Versions

The NIIF Reference Document was formerly known as the Network Operations Forum (NOF) Reference Document. The NOF Reference Document was published and maintained by Bellcore. The last version of the NOF Reference Document is Issue 13.

Disclaimer and Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

ATIS-0300033, NGIIF Reference Document, Part X, Interconnection Between LECS Operations Handbook – Local Interconnection Service Arrangement, Attachment A, Security Guidelines, Formerly NIIF 5029

The NGIIF Reference Document, Part X, Interconnection Between LECS Operations Handbook – Local Interconnection Service Arrangement, Attachment A, Security Guidelines is an ATIS standard developed by the NGIIF.

Published by

Alliance for Telecommunications Industry Solutions

1200 G Street, NW, Suite 500

Washington, DC 20005

Copyright © 2011 by Alliance for Telecommunications Industry Solutions

All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < <http://www.atis.org> >.

Printed in the United States of America.

INTERCONNECTION BETWEEN LECs OPERATIONS HANDBOOK, ATTACHMENT A NETWORK SECURITY
BASE GUIDELINES

Table of Contents

1	GENERAL.....	3
2	DATA SECURITY FEATURES OF CRITICAL SWITCHING NODES	3
2.1	IDENTIFICATION.....	3
2.2	AUTHENTICATION.....	3
2.3	SYSTEM ACCESS CONTROL.....	3
2.4	RESOURCE ACCESS CONTROL	4
2.5	SECURITY LOG (AUDIT).....	4
2.6	SECURITY ADMINISTRATION	5
2.7	DOCUMENTATION.....	5
3	SYSTEMS ENGINEERING APPROACH TO SECURITY BASELINE FOR TELECOMMUNICATIONS NETWORK NODES, LOGICAL SECURITY CHECKLIST	6

1 General

The following Network Security Base Guidelines should be used at a minimum as a set of guidelines to be adopted by the Local Service Providers as they interconnect and on an ongoing basis.

2 Data Security Features of Critical Switching Nodes

This section specifies the desirable security features that all LSP should have for any Network Element (NE), Network System (NS), Operations System (OS) or Data Communications Network (DCN) in order to reduce the risk of potentially service affecting security compromises.

2.1 Identification

The LSP node should not allow an existing user-ID to be assigned to another active user (i.e., user-IDs should be unique).

Each operations related process running in a switching node should be associated with the corresponding user-ID (so that an audit trail can be established if there is a need).

The node under query should disable a user-ID if it has remained inactive (i.e., never used) over a specific time period.

2.2 Authentication

All remote input ports of a node (including direct, dial-up and network access) should require authentication of a session requester, without any provision for a bypass mechanism.

A single stored password entry (e.g., in a password file) should not be allowed to be shared by multiple user-IDs. However, the node should not prevent a user from choosing (unknowingly) a password that is already being used by some other user. Nor should the node volunteer this information to either user.

Passwords should be stored in a one-way encrypted form, and should not be retrievable by any user including managers or administrators (of system and security). Also, there should be no clear text display (on a device such as a screen, typewriter, or printer) of a password at any time (e.g., login, file dump, etc.).

The node should allow passwords to be user changeable (requiring re-authentication), and should require that the user change it the first time he/she establishes a session with the password assigned to him/her. The default should be non-trivial in nature.

The password should have an "aging" feature, and it should have a complexity requirement to make it not easily determined. The node should not accept common words or names as valid passwords. Also, it should not allow a recently obsolete password to be readily re-selected by the said user.

2.3 System Access Control

The node should not allow access to any session requester unless identified and authenticated. There should be no default mechanism to circumvent it.

The node should not allow any session to be established via a port that is not authorized to accept input commands. For example, if an output port receives a Log on request, the node should not respond.

The entire Log on procedure should be allowed to be completed without interruption, even if incorrect parameters (such as an incorrect user-ID or an incorrect password) are entered, and no "help message" should be transmitted to the session requester as to which part of the authentication is incorrect. The only information to be conveyed at the end of the Log on attempt is that the Log on is invalid.

After a specified number of incorrect Log on attempts carried out in succession, the node should lock out the channel and raise an alarm in real time for the administrator.

Before the session begins, the node should provide a warning message explicitly alerting the user of the consequences of unauthorized access and use.

At the beginning of the session, the node should display the date and time of the user's last successful access and the number of unsuccessful attempts, if any, that have been made to establish a session since the last successful access.

There should be a "time-out" feature - i.e., the node should disconnect or re-authenticate users after a specified time interval during which no messages were exchanged. Also, there should be a mechanism for user-initiated keyboard locking.

The node should provide a mechanism to end a session through a secure log off procedure. If a session gets interrupted due to reasons such as time-out, power failure, link disconnection, etc., the port should be dropped immediately.

For dial-up access over un-trusted channels, authentication involving one time passwords should be required (e.g., smart card, third party authentication, etc.).

2.4 Resource Access Control

Access to resources should be controlled on the basis of "privilege" (i.e., access permission) associated with user-ID and channel. It should not be based on a "password" associated with the access function, because that password will have to be necessarily shared among all users requiring such access. Neither should encryption be used as a primary access control mechanism (though encryption may be used to enhance it).

The granularity of resource access control should be such that for each resource it should be possible to grant (or deny) access privilege to any single user (or a prescribed group of users). For example, the control should be adequately fine-grained so that user access and channel access can be restricted on the basis of commands, database views (i.e., objects), records (i.e., object instances), and fields (i.e., attributes).

If external entities (e.g., customers) are allowed access to the resources, each node's resource (e.g., proprietary data) should be protected from access by unauthorized persons.

Executable/loadable/fetchable software should be access controlled for overwrite, update, and execution rights.

2.5 Security Log (Audit)

The node should generate a security log containing information sufficient for after-the-fact investigation of loss or impropriety.

The security log should be protected from unauthorized access. No user should be allowed to modify or delete a security log. There should be no mechanism to disable the security log. There should be an alarm in real time if the security log does not function properly.

The security log should, as a minimum, record events such as all sessions established, invalid user authentication attempts, unauthorized attempts to access resources (including data and transactions), changes in users' security profiles and attributes, changes in access rights to resources, changes in the node security configuration, and modification of node software. For each such event, the record should, as a minimum, include date and time of event, initiator of the event such as: user-ID, terminal, port, network address, etc., names of resources accessed, and success or failure of the event.

Actual or attempted passwords should not be recorded in the security log.

There should be audit tools to produce exception reports, summary reports, and detailed reports on specific data items, users, or communication facilities.

2.6 Security Administration

The node should support functions for the "management" of security related data (e.g., security parameters such as user-IDs, passwords, privileges, etc.) as "separate" from other user functions. Security administration should be reserved only for an appropriate administrator.

The administrator should be able to display all currently logged-in users as well as a list of all authorized user-IDs.

The administrator should be able to independently and selectively monitor, in real time, the actions of any one or more users based on respective user-IDs, terminals, ports, or network addresses.

The administrator should be able to identify all resources owned by or accessible to any specific user along with the associated access privileges.

The administrator should be able to enter, edit, delete or retrieve all attributes of a user-ID (except for a password, which should not be retrievable).

The administrator should limit the use of a "null password" during system Log on on a per user or per port basis (i.e., during new release installation).

The administrator should be able to save the security log for safe storage, so that it is not written over when the buffer is full.

All security parameters (e.g., password aging interval, time-out interval, various alarm conditions) should be specific and adjustable by the administrator. This implies that the node should not have any security parameters hard coded.

2.7 Documentation

Any node supplier/vendor should provide documentation on security considerations for administrators, operators, and users. They can be stand-alone documents or sections incorporated in appropriate vendor manuals.

The administrator's guide should contain items such as: functions and privileges that need to be controlled to secure the facility, proper usage of security audit tools, procedures for examining and maintaining audit files, procedures for periodic saving and backup of security logs, recommendations on setting the minimum access permissions on all files, directories, and databases, guidelines on security assessment techniques.

The operator's guide should contain procedures necessary to initially start the node in a secure manner and to resume secure operation after any lapse that may have occurred.

The user's guide should describe the protection mechanisms that are non-transparent to the user, should explain their purpose, and provide guidelines on their use. It should not contain any information that could jeopardize the security of the node if made public.

The above list is not exhaustive. There are requirements related to other areas such as: data and system integrity, and various phases of life cycle involving design, packaging, delivery, and support by the vendor.

3 Systems Engineering Approach to Security Baseline for Telecommunications Network Nodes, Logical Security Checklist

Question	Yes/No	If No, Why not?
Is security addressed across the entity's entire network?		
Are Critical Common Environments defined and isolated (e.g. by firewall perimeters) to limit access to authorized processes and users?		
If fire walls are deployed are they placed around the "perimeter" or perimeters critical components, NEs, NSs and OSs?		
Are software changes controlled and verified to maintain the established security perimeter?		
Has a security baseline been established for Network Elements, NEs, Network Systems, NSs, and Operations Support Systems, OSs and Data Communication Network DCNs?		
Is that baseline specified or referenced in procurement RFPs and contracts?		
Do new NEs, NSs, OSs and DCNs meet those requirements?		
Are organizational responsibilities for network security defined?		
Is that responsibility clearly placed within common network management reporting environment?		
Is security part of the defined responsibilities for the personnel that monitor, maintain and control various network components?		
Are all network connectivity and network mappings documented?		
If documented, has the connectivity been verified?		
Have the following generic counter measures been implemented for all key nodes (NEs, NSs and OSs):		
Assignment of command privileges to each class of user by functional responsibility, to allow the power to get the job done, while reserving special power (e.g., the ability to change user passwords) to the security administrator?		
Use of (COMPLIANT) commercially-available access-control systems (e.g., dial-back modems that do not utilize a pass-through feature) to secure remote access to nodes?		
Use of encryption equipment at each end of an OAM&P access session which transits an open PPSN?		
Use of available access control software at the host system?		
Use of established access procedures and security routines (e.g., periodic re-authorization of users and the use of security tools)?		
Elimination of uncontrolled dial access?		
Controlled access for vendor support?		

Controlled access to dial-in protocol analyzers on the signaling links and X.25 facilities between nodes?		
Intrusion recovery plans for the entity's nodes?		
Security on the gateway screening tables?		
Adequate security on the node restart capability?		
Adequate security on vendor-specific node restart procedures?		
Back-up tapes and media available and secured off-site?		



ATIS-0300034

**Next Generation Interconnection Interoperability (NGIIF)
Reference Document**

**Part XI, Local Number Portability Interconnection Testing
Document**

Version 12.0



ATIS is the leading technical planning and standards development organization committed to the rapid development of global, market-driven standards for the information, entertainment and communications industry. More than 200 companies actively formulate standards in ATIS' Committees, covering issues including: IPTV, Cloud Services, Energy Efficiency, IP-Based and Wireless Technologies, Quality of Service, Billing and Operational Support, Emergency Services, Architectural Platforms and Emerging Networks. In addition, numerous Incubators, Focus and Exploratory Groups address evolving industry priorities including Smart Grid, Machine-to-Machine, Connected Vehicle, IP Downloadable Security, Policy Management and Network Optimization.

ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications' Sectors, and a member of the Inter-American Telecommunication Commission (CITEL). ATIS is accredited by the American National Standards Institute (ANSI). For more information, please visit www.atis.org.

Notice

This document was developed by the Alliance for Telecommunications Industry Solutions' (ATIS) sponsored Next Generation Interconnection Interoperability Forum (NGIIF). The NGIIF addresses next-generation network interconnection and interoperability issues associated with emerging technologies. Specifically, it develops operational procedures which involve the network aspects of architecture, disaster preparedness, installation, maintenance, management, reliability, routing, security, and testing between network operators. In addition, the NGIIF addresses issues which impact the interconnection of existing and next generation networks and facilitate the transition to emerging technologies. All changes to this document shall be made through the NGIIF issue resolution process.

Note Regarding Previous Versions

The NIIF Reference Document was formerly known as the Network Operations Forum (NOF) Reference Document. The NOF Reference Document was published and maintained by Bellcore. The last version of the NOF Reference Document is Issue 13.

Disclaimer and Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

ATIS-0300034, NGIIF Reference Document, Part XI, Local Number Portability Interconnection Testing Document, Formerly NIIF 5030, Published June 2009

The NGIIF Reference Document, Part XI, Local Number Portability Interconnection Testing Document, is an ATIS standard developed by the NGIIF.

Published by

Alliance for Telecommunications Industry Solutions

1200 G Street, NW, Suite 500

Washington, DC 20005

Copyright © 2011 by Alliance for Telecommunications Industry Solutions

All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < <http://www.atis.org> >.

Printed in the United States of America.

LOCAL NUMBER PORTABILITY INTERCONNECTION TESTING DOCUMENT

Table of Contents

1	GENERAL.....	5
1.1	PURPOSE.....	5
1.2	DEFINITIONS	5
2	BASIC PREMISES.....	5
3	OPERATING PRINCIPLES	6
4	SCOPE OF THIS DOCUMENT	6
5	NETWORK PROVIDERS RESPONSIBILITIES	6
6	INTERCONNECTION TESTS MATRIX	6
7	VERTICAL FEATURE TESTING.....	7
8	SIGNALING SYSTEM 7 INTERCONNECTION TESTING (CCS 7).....	7
9	SERVICES TESTING.....	7
10	TEST NUMBER GUIDELINES	8
11	INTERCONNECTION TEST CALLS.....	8
11.1	CAUSE CODE 26N VALIDATION TESTS	8
11.1.1	Test Number 1 - Intra-LATA Local via direct Trunks for Cause Code 26N Validation (Ported Number to Ported Number)	8
11.1.2	Test Number 2 - Intra-LATA Local via direct Access Tandem for Cause Code 26N Validation (Ported Number to Ported Number)	9
11.1.3	Test Number 3 - Intra-LATA/Inter-LATA Toll (PICd or Casual Dialing) via Direct Trunks to an IXC for Cause Code 26N Validation (Ported Number to Ported Number).....	10
11.2	CALL THROUGH TESTS	12
11.2.1	Test Number 4 - Intra- LATA Local via Direct Trunks (Ported Number to Ported Number)	12
11.2.2	Test Number 5 - Intra- LATA Local via Direct Trunks (Ported Number to Non Ported Number).....	13
11.2.3	Test Number 6 - Intra- LATA Local via Direct Trunks (Non Ported number to Ported Number)	14
11.2.4	Test Number 7 - Intra-LATA Local via an Access Tandem (Ported Number to Ported Number).....	15
11.2.5	Test Number 8 - Intra-LATA Local via an Access Tandem (Non Ported Number to Ported Number)	16
11.2.6	Test Number 9 - Intra-LATA/Inter-LATA Toll (PICd or Casual Dialing) via Direct Trunks to an IXC. (Ported Number to Ported Number)	17
11.2.7	Test Number 10 - Intra-LATA/Inter-LATA Toll (PICd or Casual Dialing) via Direct Trunks to an IXC. (Ported Number to Non Ported Number).....	18
11.2.8	Test Number 11 - Intra-LATA/Inter-LATA Toll (PICd or Casual Dialing) via Direct Trunks to an IXC (Non Ported Number to Ported Number).....	19
11.2.9	Test Number 12 - Intra-LATA/Inter-LATA Toll (PICd or Casual Dialing) via an Access Tandem to an IXC. (Ported Number to Ported Number)	20
11.2.10	Test Number 13 - Intra-LATA/Inter-LATA Toll (PICd or Casual Dialing) via an Access Tandem to an IXC. (Non Ported Number to Ported Number).....	21
11.3	DEFAULT ROUTING TESTS	22
11.3.1	Test Number 14 - Intra-LATA Local Default Routing via Direct Trunks. (Ported Number to Ported Number)	22
11.3.2	Test Number 15 - Intra-LATA Local Default Routing via an Access Tandem. (Ported Number to Ported Number)	24
11.3.3	Test Number 16 - Intra-LATA/Inter-LATA Toll Default Routing via an Access Tandem to an IXC. (Ported Number to Ported Number)	25

11.4	E-9-1-1 TEST CALLS.....	26
11.4.1	Test Number 17 - E9-1-1 Call from a Ported Number and a return call from the PSAP to the Ported Number. 26	
11.4.2	Test Number 18 - E9-1-1 Call from a Ported Number to PSAP(1), transfer from PSAP(1) to PSAP (2),and a return call from PSAP(2) to the Ported Number.	27

1 General

1.1 Purpose

The purpose of this document is to provide guidance to network providers when they are engaged in interconnection testing for local number portability to ensure that all areas of network integrity and customer service from an interconnection perspective are addressed proactively.

This document does not replace or supersede any existing contracts, tariffs or any other legally binding document.

1.2 Definitions

In general, the definitions for terms utilized within this document can be found in the Glossary section of the Network Interconnection Interoperability Forum (NGIIF) documentation. Any terms that are unique to this document are listed below, and will be included in the glossary.

- **Default Routing:** Default Routing occurs when the switch that normally performs the LRN Database query is unable to communicate with the SCP and the call is routed to the donor switch that performs the query and completes the call.
- **Local Number Portability:** The end-user's ability to retain their telephone number when moving to a different serving switch (Class 5).
- **Location Routing Number:** A 10-digit number used to uniquely identify a switch that is LNP capable.
- **Donor Switch:** The switch (Class 5) from where a number has been ported.
- **Recipient Switch:** The switch (Class 5) to where a number has been ported.
- **NXX Opened to Portability:** An NXX where numbers can be moved from a Donor Switch to a Recipient Switch.
- **Ported (Number):** A number that has been moved to a recipient switch.
- **Non-Ported (Number):** A number that has not been moved from a Class 5 switch.

2 Basic Premises

In order for Local Number Portability to be successful in terms of ensuring the integrity of Customer Service the industry needs to have in place an industry wide set of interconnection tests.

Quality of Customer Service is predicated on all network providers being responsible for the assurance of the integrity of their respective networks.

A nationally agreed to Local Number Portability Interconnection test document will provide the appropriate direction to all network providers for the quality and integrity of interconnection.

Information to be included in this document is a result of NGIIF agreements and pertains to interconnection negotiations between network providers.

3 Operating Principles

It is expected that all network providers have performed their respective internal network testing prior to interconnection testing taking place.

It is expected that all problems/troubles identified during internal network testing will be resolved prior to interconnection testing.

Prior to interconnection for Local Number Portability (LNP), it is expected that all network providers have performed their basic SS7 internal and interconnection testing.

It is expected that network providers have Number Portability Administration Center (NPAC) certification prior to network interconnection testing.

4 Scope of this Document

This document is limited to LNP interconnection tests that are recommended to be performed by network providers (i.e. Cause Code 26N Validation Tests, Call Through Tests and Default Routing Tests). The purpose of these tests is to provide assurance for the integrity of the interconnected networks.

5 Network Providers Responsibilities

This section covers the responsibilities of network providers as it pertains to Local number Portability interconnection testing.

Network providers are responsible to perform all necessary internal testing to ensure compatibility and compliance to standards and industry agreements for interconnection and network integrity.

Prior to the commencement of Intra-LATA and Inter-LATA testing, ported or non-portable test numbers will need to be exchanged in order to terminate test calls.

When testing has been completed and the expected test results have been achieved, then the test numbers shall be returned.

The network providers should work cooperatively to resolve network interconnection problems.

Network providers should be familiar with the appropriate NGIIF operations documentation.

6 Interconnection Tests Matrix

This section provides a summary matrix of interconnection tests that are recommended to be performed.

Test No.	CALL FLOW TYPES	Originating Destination	P P N P	Fig. No.
CAUSE CODE 26N VALIDATION TESTS				
1	Intra-LATA Local via Direct Trunks for Cause Code 26N Validation		X	1
2	Intra-LATA Local via an Access Tandem for Cause Code 26N Validation		X	2

Test No.	CALL FLOW TYPES	Originating Destination	P P	P N	N P	Fig. No.
3	Intra-LATA/Inter-LATA Toll (PICd or Casual Dialing) via Direct Trunks to an IXC for Cause Code 26N Validation		X			3
	CALL THROUGH TESTS					
4-6	Intra-LATA Local via Direct Trunks		X	X	X	4,5,6
7-8	Intra-LATA Local via an Access Tandem		X		X	7,8
9-11	Intra-LATA/Inter-LATA Toll (PICd or Casual Dialing) via Direct Trunks to an IXC		X	X	X	9,10,11
12-13	Intra-LATA/Inter-LATA Toll (PICd or Casual Dialing) via an Access Tandem to an IXC		X		X	12, 13
	DEFAULT ROUTING TESTS					
	See note in Section 12.3 ("Caution")					
14	Intra-LATA Local Default Routing via Direct Trunks		X			14
15	Intra-LATA Local Default Routing via an Access Tandem		X			15
16	Intra-LATA/Inter-LATA Toll (PICd or Casual Dialing) Default Routing (via Direct Trunks or Access Tandem) to an IXC		X			16

N = Non Ported Number in an NPA-NXX Open to Portability

P = Ported Number

7 Vertical Feature Testing

Vertical Feature (e.g., call waiting, call forwarding, and CLASS) tests are considered to be stand alone tests to be performed by each network provider and do not require interactions/cooperation between interconnected parties. The testing of vertical features should be performed prior to interconnection of network providers.

8 Signaling System 7 Interconnection Testing (CCS 7)

Signaling System 7, also known as SS7 or CCS 7 tests for interconnection are outlined in the NGIIF Document under SS7 Trunks and Links, Part III. For the purpose of Local Number Portability it is recommended that all appropriate SS7 interconnection tests be performed prior to the commencement of LNP Interconnection testing.

9 Services Testing

Service tests (e.g., E9-1-1, 611, and toll free services) are considered to be stand alone tests and are to be performed by each network provider and do not require interactions/cooperation between interconnected parties.

All services should be tested prior to interconnection for Local Number Portability.

10 Test Number Guidelines

The Company with the donor switch should exchange with the Company with the recipient switch, test number(s) associated with the NXX that has been opened for portability.

All test numbers will be provisioned as working numbers (i.e., billable).

Test numbers will only be assigned for the duration of the testing window as negotiated by the interconnecting companies. On completion of the LNP Interconnection Testing, the test number(s) will be disconnected and returned to the company with the donor switch immediately. In the event that a test number is not returned, the company with the donor switch can disconnect the assigned test number.

Test number termination treatment should be negotiated by the interconnecting companies.

11 Interconnection Test Calls

This section outlines the test calls that should be performed for interconnection.

The interconnection test calls are categorized as follows:

11.1 Cause Code 26N Validation Tests

11.1.1 Test Number 1 - Intra-LATA Local via direct Trunks for Cause Code 26N Validation (Ported Number to Ported Number)

11.1.1.1 Test Description

This will test that Cause Code 26N is returned on a local call via Direct Trunks when the called ported number is in the SCP (LSP-X), but has not been translated at the terminating switch (LSP-Y). (See Figure 1)

Cause Code 26: This Cause Code indicates that the called party can not be reached because the “ported number” in the GAP identifies a called party that is not served by the exchange.

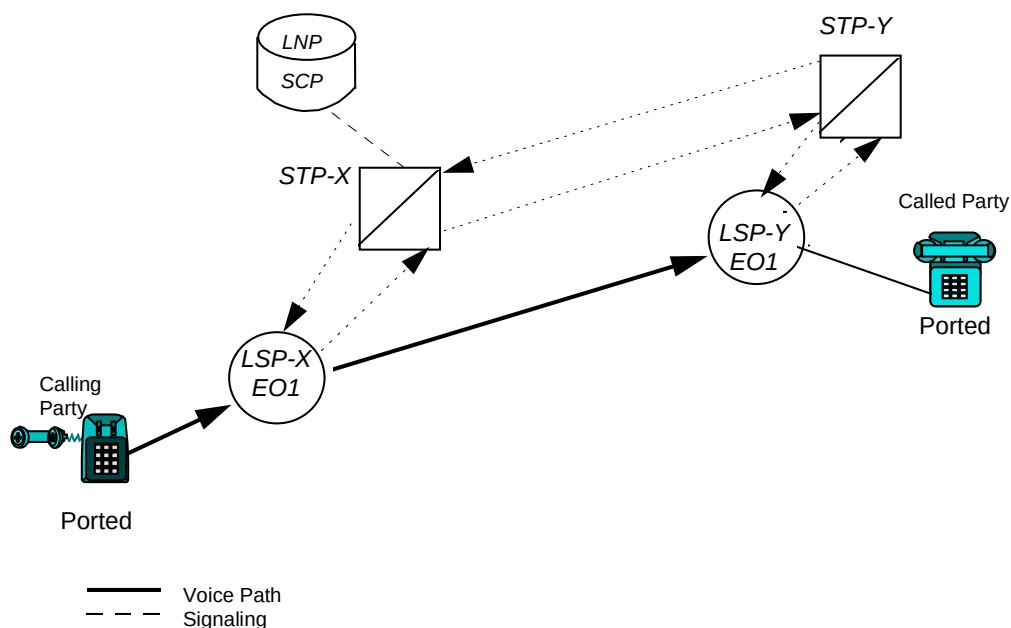
11.1.1.2 Test Procedure

- In LSP-X's SCP, create a record for the ported number that is under test
- Verify that the called ported number under test is not translated in LSP-Y's switch
- Ensure that the SS7 maintenance center (or like center) is monitoring and recording the signaling messages associated with the test call
- From a ported number in LSP-X place a call to the ported number under test in LSP-Y
- Document test results

11.1.1.3 Expected Test Results

- Verify that the originating LRN (in the JIP) is sent by LSP-X
- Verify that the terminating LRN is received by LSP-Y
- Verify that Cause Code 26N is received by LSP-X
- LSP-X and LSP-Y validate that the appropriate billing records (AMA) are created and the appropriate trunk group is used.

- Verify that the correct treatment is received for Cause Code 26



**Test #1: Intra-LATA Local via Direct Trunks for Cause Code 26N
Validation - Ported Number to Ported Number**

Figure 1

**11.1.2 Test Number 2 - Intra-LATA Local via direct Access Tandem for Cause Code 26N
Validation (Ported Number to Ported Number)**

11.1.2.1 Test Description

This will test that Cause Code 26N is returned on a local call via an Access Tandem when the called ported number is in the SCP (LSP-X), but has not been translated at the terminating switch (LSP-Y). (See Figure 2)

Cause Code 26: This Cause Code indicates that the called party can not be reached because the “ported number” in the GAP identifies a called party that is not served by the exchange.

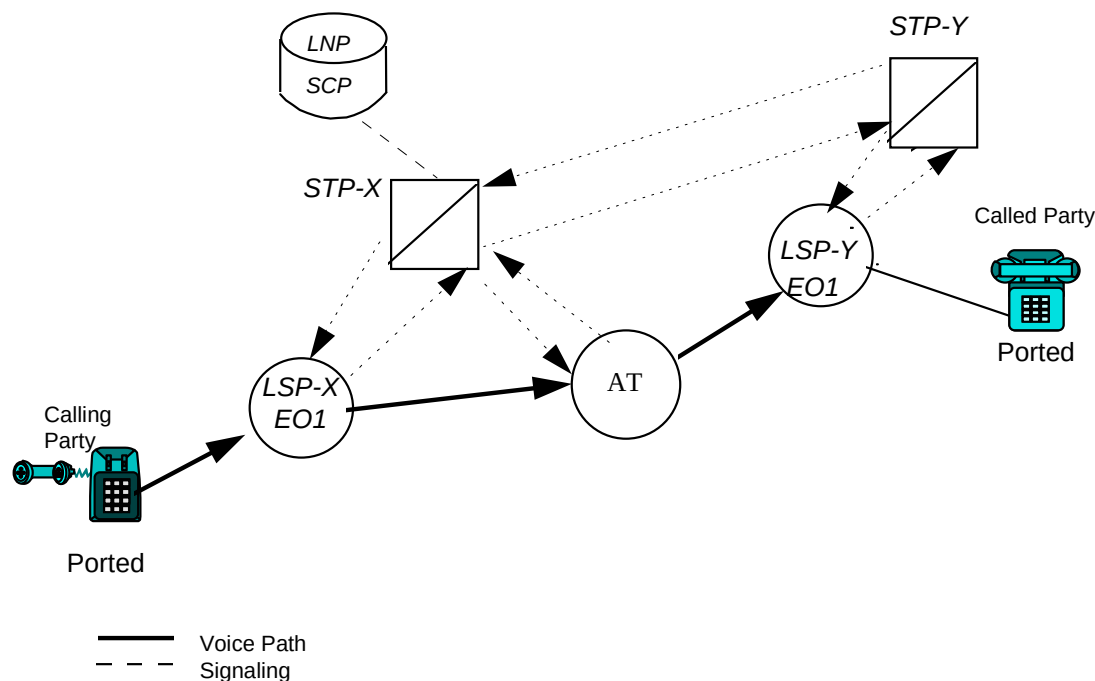
11.1.2.2 Test Procedure

- In LSP-X’s SCP, create a record for the ported number that is under test
- Verify that the called ported number under test is not translated in LSP-Y’s switch
- Ensure that the SS7 maintenance center (or like center) is monitoring and recording the signaling messages associated with the test call
- From a ported number in LSP-X place a call to the ported number under test in LSP-Y
- Document test results

11.1.2.3 Expected Test Results

- Verify that the originating LRN (in the JIP) is sent by LSP-X

- Verify that the terminating LRN is received by LSP-Y
- Verify that Cause Code 26N is sent by LSP-Y, and received by LSP-X via the Access Tandem
- LSP-X and LSP-Y validate that the appropriate billing records (AMA) are created and the appropriate trunk groups are used.
- Verify that the correct treatment is received for Cause Code 26N



Test #2: Intra-LATA Local via an Access Tandem for Cause Code 26N Validation - Ported Number to Ported Number

Figure 2

11.1.3 Test Number 3 - Intra-LATA/Inter-LATA Toll (PICd or Casual Dialing) via Direct Trunks to an IXC for Cause Code 26N Validation (Ported Number to Ported Number)

11.1.3.1 Test Description

This will test that Cause Code 26N is generated on a Toll call by the terminating switch, when the called ported number is in the SCP of the IXC doing the LRN database query, but has not been translated at the terminating switch (LSP-Y). (See Figure 3)

Cause Code 26: This cause indicates that the called party can not be reached because the "ported number" in the GAP identifies a called party that is not served by the exchange.

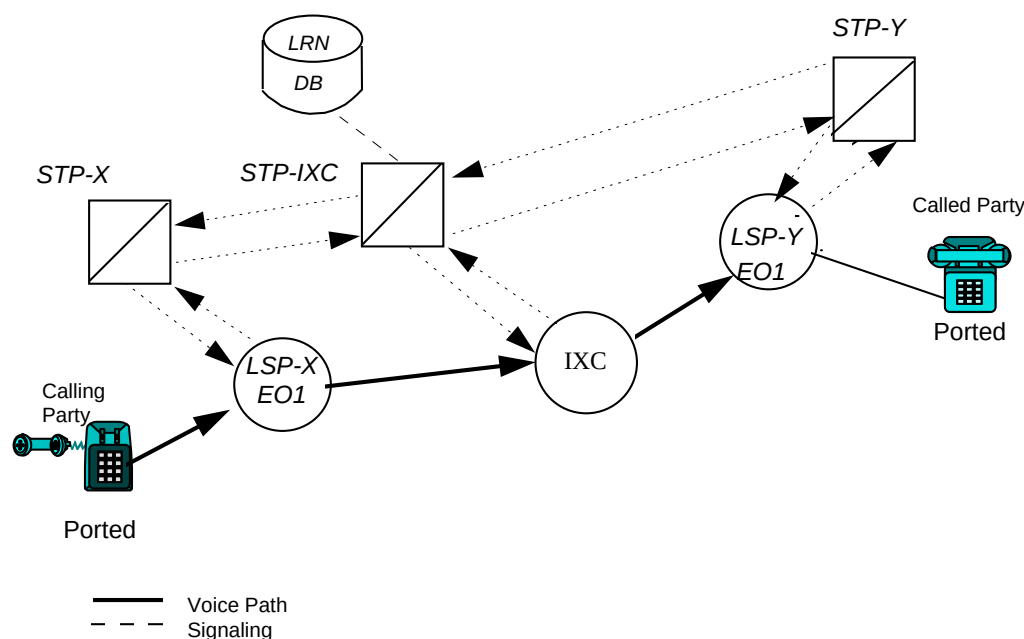
11.1.3.2 Test Procedure

- In the IXC's LNP database, create a record for the ported number that is under test

- Verify that the called ported number under test is not translated in recipient switch LSP-Y
- Ensure that the SS7 maintenance centers (or like center) are monitoring and recording the signaling messages associated with the test call
- From a ported number in recipient switch LSP-X place a call to the ported number under test in recipient switch LSP-Y using the IXC's toll network
- Document test results

11.1.3.3 Expected Test Results

- Verify that the originating LRN (in the JIP) is sent by LSP-X and received by LSP-Y via the IXC
- Verify that Cause Code 26N is sent by LSP-Y and received by the IXC
- Verify that the correct treatment is applied for Cause Code



Test #3: Intra-LATA/Inter-LATA Toll (PICd or Casual Dialing) via Direct Trunks to an IXC for Cause Code 26N Validation - Ported Number to Ported Number

Figure 3

11.2 Call Through Tests

11.2.1 Test Number 4 - Intra- LATA Local via Direct Trunks (Ported Number to Ported Number)

11.2.1.1 Test Description

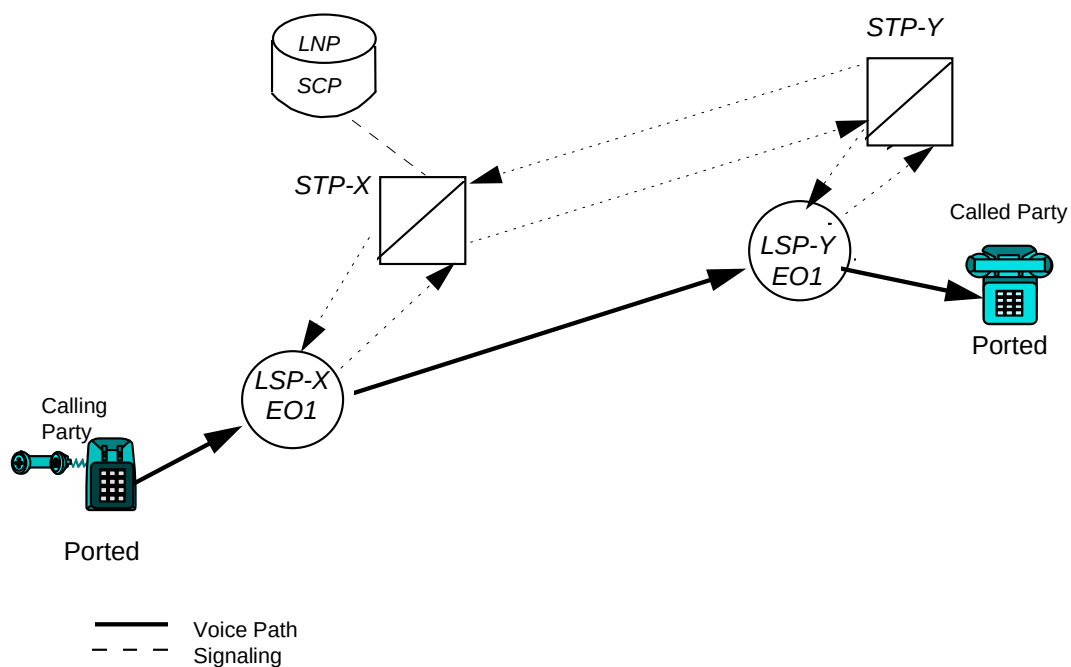
This will test that a local call can be completed from a ported number in a recipient switch (LSP-X) to a ported number in another recipient switch (LSP-Y) using direct trunks. (See Figure 4)

11.2.1.2 Test Procedure

- From a ported number in LSP-X, call a ported number in LSP-Y
- Document test results

11.2.1.3 Expected Test Results

- The call completes to the appropriate termination at LSP-Y
- LSP-X and LSP-Y validate that the appropriate billing records (AMA) are created and the appropriate trunk group is used.



Test #4: Intra-LATA Local via Direct Trunks - Ported Number to Ported Number

Figure 4

11.2.2 Test Number 5 - Intra- LATA Local via Direct Trunks (Ported Number to Non Ported Number)

11.2.2.1 Test Description

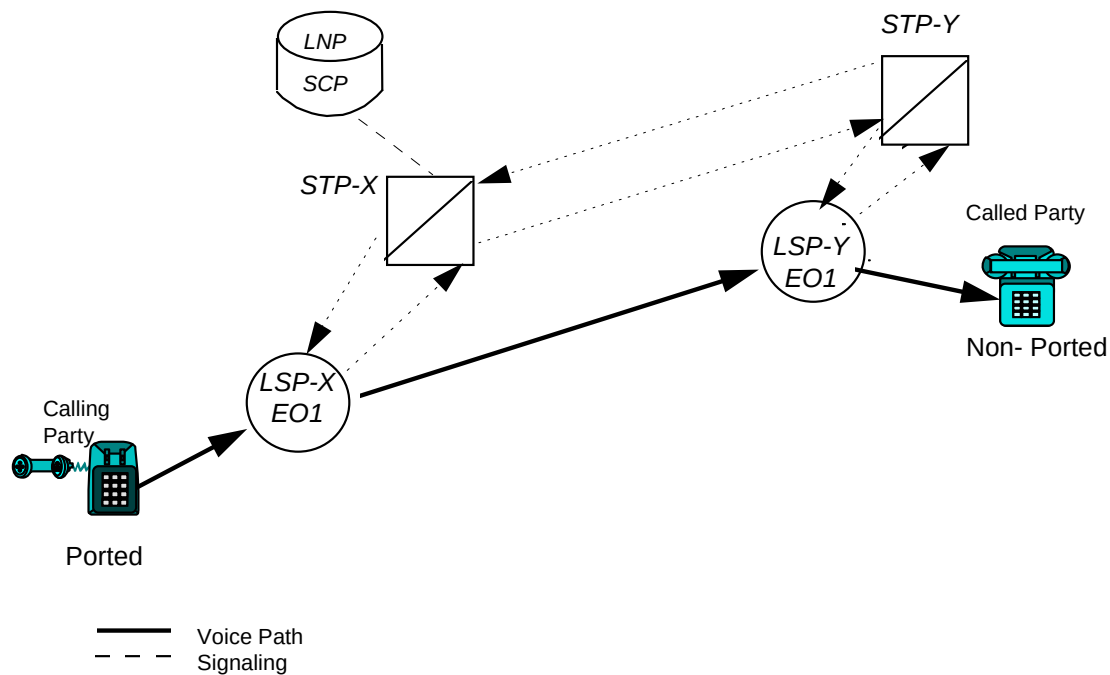
This will test that a local call can be completed from a ported number in a recipient switch (LSP-X) to a non-ported number in an NPA-NXX opened to portability in another switch (LSP-Y) using direct trunks. (See Figure 5)

11.2.2.2 Test Procedure

- From a ported number in LSP-X, call a non-ported number in LSP-Y

11.2.2.3 Expected Test Results

- The call completes to the appropriate termination at LSP-Y
- LSP-X and LSP-Y validate that the appropriate billing records (AMA) are created and the appropriate trunk group is used.



Test #5: Intra-LATA Local via Direct Trunks - Ported Number to Non-Ported Number

Figure 5

11.2.3 Test Number 6 - Intra- LATA Local via Direct Trunks (Non Ported number to Ported Number)

11.2.3.1 Test Description

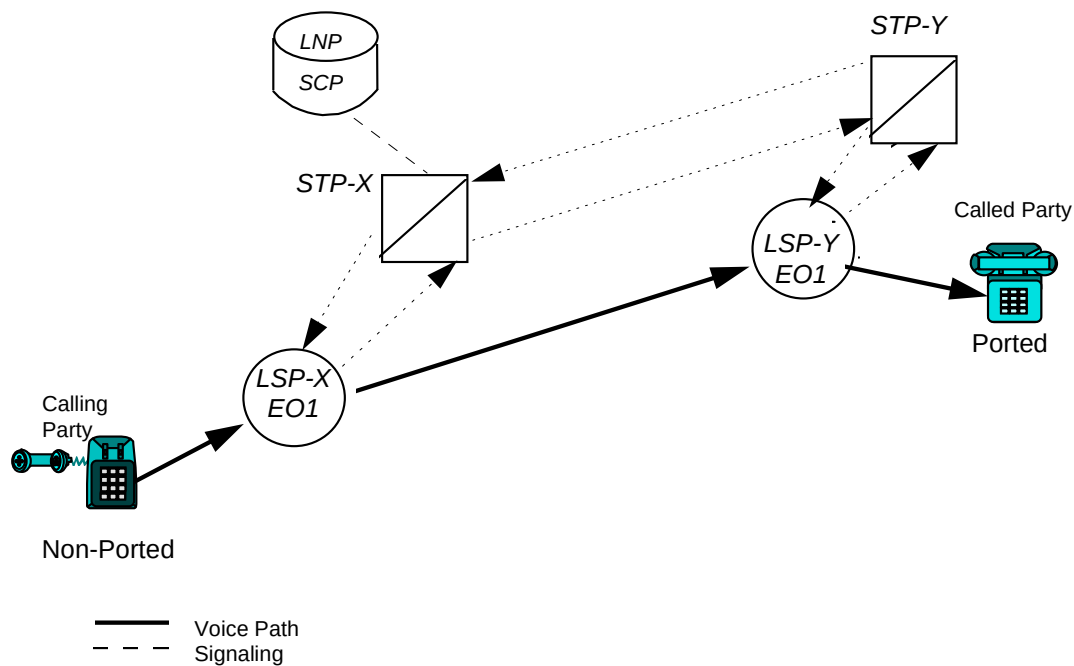
This will test that a local call can be completed from a non-ported number in an NPA-NXX opened to portability in a switch (LSP-X) to a ported number in a recipient switch (LSP-Y) using direct trunks. (See Figure 6)

11.2.3.2 Test Procedure

- From a non-ported number in LSP-X, call a ported number in LSP-Y
- Document test results

11.2.3.3 Expected Test Results

- The call completes to the appropriate termination at LSP-Y
- LSP-X and LSP-Y validate that the appropriate billing records (AMA) are created and the appropriate trunk group is used.



Test #6: Intra-LATA Local via Direct Trunks - Non-Ported Number to Ported Number

Figure 6

11.2.4 Test Number 7 - Intra-LATA Local via an Access Tandem (Ported Number to Ported Number)

11.2.4.1 Test Description

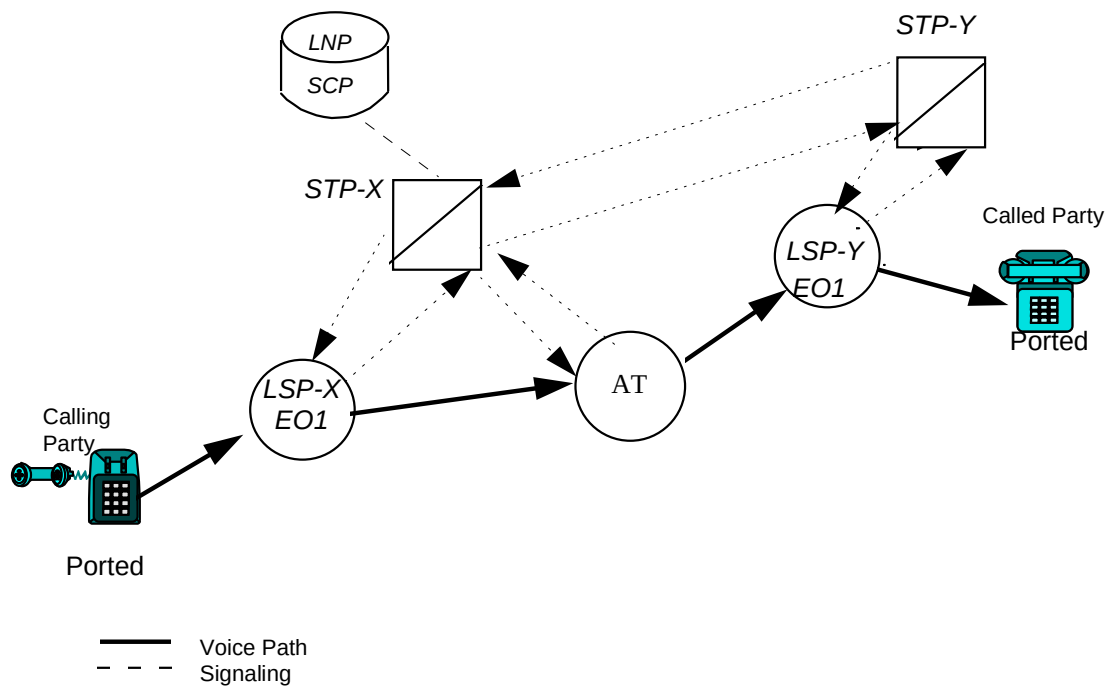
This will test that a local call can be completed from a ported number in a recipient switch (LSP-X) to a ported number in another recipient switch (LSP-Y) via an Access Tandem. (See Figure 7)

11.2.4.2 Test Procedure

- From a ported number in recipient switch LSP-X, call a ported number in recipient switch LSP-Y
- Document test results

11.2.4.3 Expected Test Results

- The call completes to the appropriate termination at LSP-Y
- LSP-X and LSP-Y validate that the appropriate billing records (AMA) are created and the appropriate trunk group is used.



Test #7: Intra-LATA Local via an Access Tandem - Ported Number to Ported Number

Figure 7

11.2.5 Test Number 8 - Intra-LATA Local via an Access Tandem (Non Ported Number to Ported Number)

11.2.5.1 Test Description

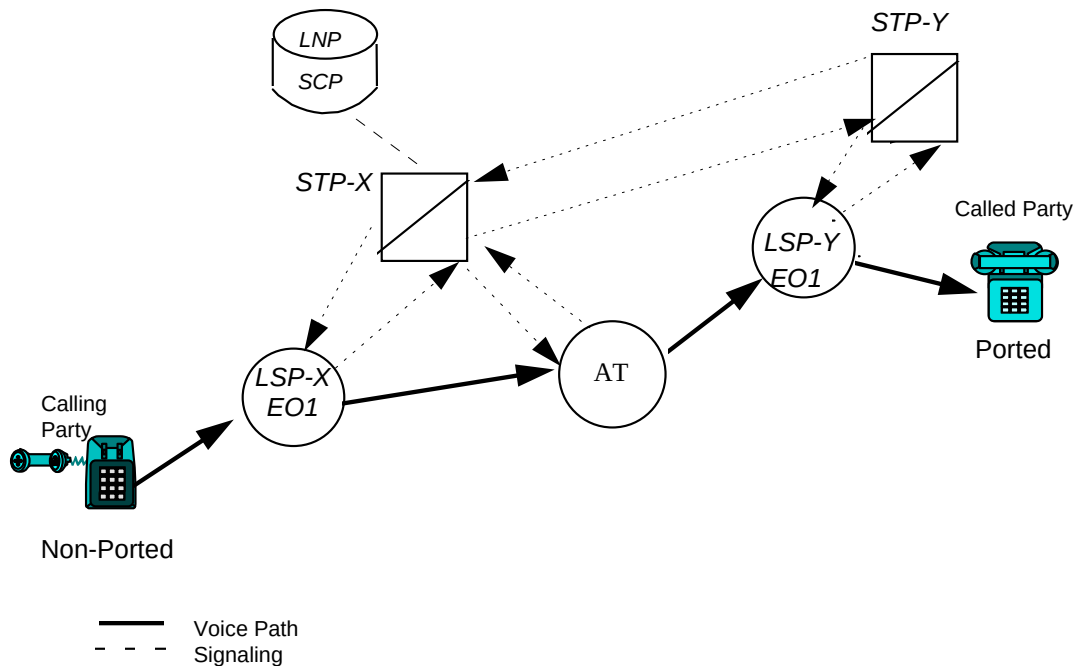
This will test that a local call can be completed from a non-ported number in an NPA-NXX opened to portability in LSP-X to a ported number in a recipient switch (LSP-Y) via an Access Tandem. (See Figure 8)

11.2.5.2 Test Procedure

- From a non-ported number in an NPA-NXX opened to portability in LSP-X, call a ported number in recipient switch LSP-Y.
- Document test results

11.2.5.3 Expected Test Results

- The call completes to the appropriate termination at LSP-Y
- LSP-X and LSP-Y validate that the appropriate billing records (AMA) are created and the appropriate trunk groups are used.



Test #8: Intra-LATA Local via an Access Tandem - Non-Ported Number to Ported Number

Figure 8

11.2.6 Test Number 9 - Intra-LATA/Inter-LATA Toll (PICd or Casual Dialing) via Direct Trunks to an IXC. (Ported Number to Ported Number)

11.2.6.1 Test Description

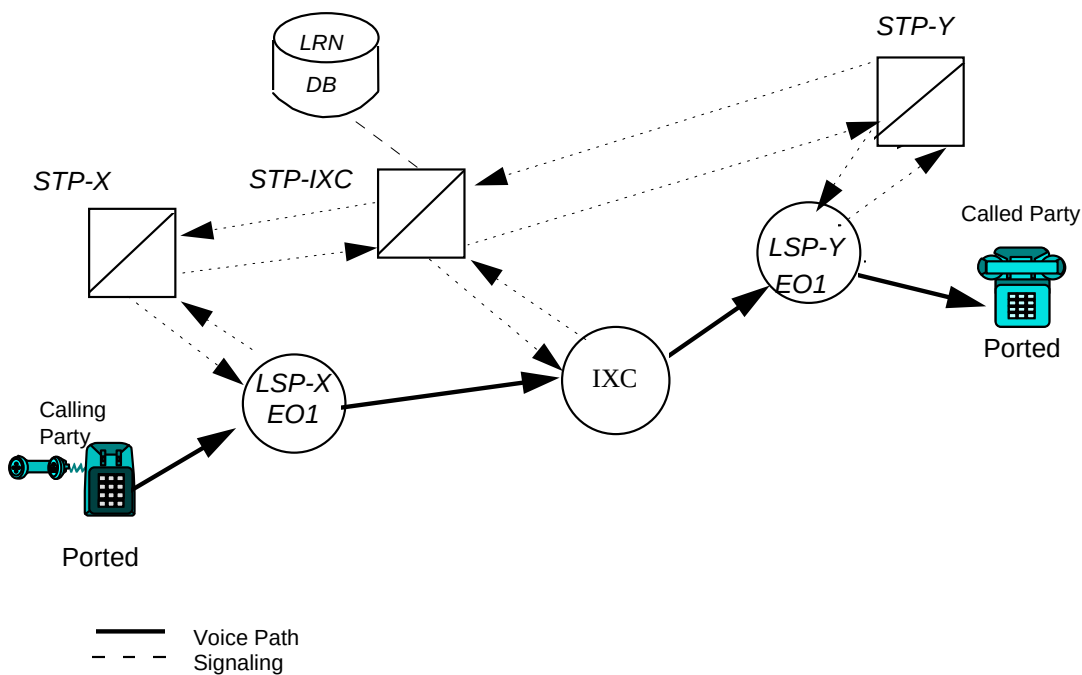
This will test that a toll call can be completed from a ported number in a recipient switch (LSP-X) to a ported number in another recipient switch (LSP-Y) using direct trunks to an IXC. (See Figure 9)

11.2.6.2 Test Procedure

- From a ported number in recipient switch LSP-X, call a ported number in recipient switch LSP-Y using direct trunks to an IXC (PICd or Casual Dialing)
- Document test results

11.2.6.3 Expected Test Results

- The call completes to the appropriate termination at LSP-Y
- Verify that the originating LRN (in the JIP) is sent by LSP-X
- Verify that the IXC performs the LNP database query
- LSP-X, LSP-Y and the IXC validate that the appropriate billing records are created and the appropriate trunk group is used.



Test #9: Intra-LATA/Inter-LATA Toll (PICd or Casual Dialing) via Direct Trunks to an IXC - Ported Number to Ported Number

Figure 9

11.2.7 Test Number 10 - Intra-LATA/Inter-LATA Toll (PICd or Casual Dialing) via Direct Trunks to an IXC. (Ported Number to Non Ported Number)

11.2.7.1 Test Description

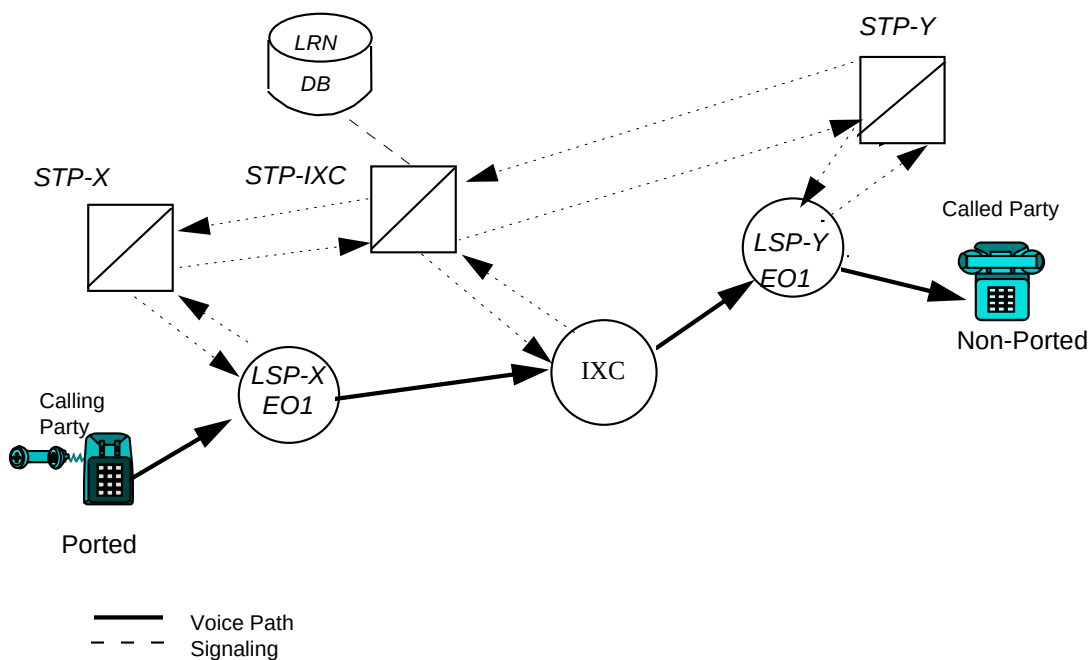
This will test that a toll call can be completed from a ported number in a recipient switch (LSP-X) to a non-portable number in another switch (LSP-Y) utilizing an NPA-NXX opened to portability using direct trunks to an IXC (See Figure 10)

11.2.7.2 Test Procedure

- From a ported number in recipient switch LSP-X, call a non-portable number in LSP-Y in an NPA-NXX opened to portability using an IXC. (PICd or Casual Dialing)
- Document test results

11.2.7.3 Expected Test Results

- The call completes to the appropriate termination at LSP-Y
- Verify that the originating LRN (in the JIP) is sent by LSP-X
- Verify that the IXC performs the LNP database query
- LSP-X, LSP-Y and the IXC validate that the appropriate billing records are created and the appropriate trunk group is used.



Test #10: Intra-LATA/Inter-LATA Toll (PICd or Casual Dialing) via Direct Trunks to an IXC - Ported Number to Non-Ported Number

Figure 10

11.2.8 Test Number 11 - Intra-LATA/Inter-LATA Toll (PICd or Casual Dialing) via Direct Trunks to an IXC (Non Ported Number to Ported Number)

11.2.8.1 Test Description

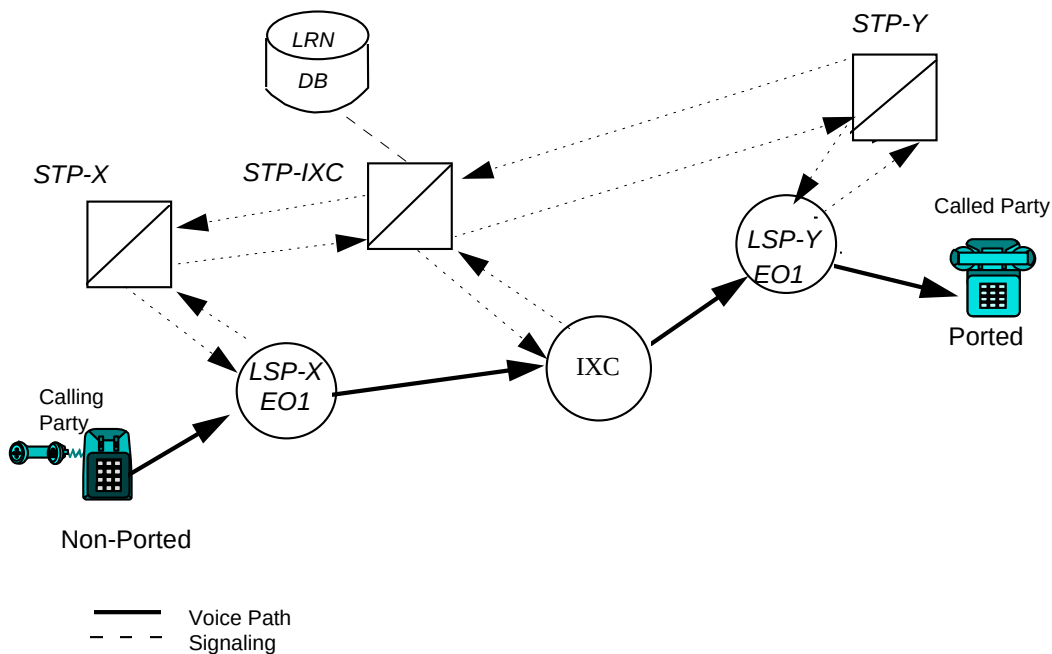
This will test that a toll call can be completed from a non-ported number in an NPA-NXX opened to portability in a switch (LSP-X) to a ported number in a recipient switch (LSP-Y) using direct trunks to an IXC (See Figure 11).

11.2.8.2 Test Procedure

- From a non-ported number in a NPA-NXX opened to portability in LSP-X, call a ported number in a recipient switch LSP-Y using an IXC (PICd or Casual Dialing).
- Document test results

11.2.8.3 Expected Test Results

- The call completes to the appropriate termination at LSP-Y
- Verify that the originating LRN (in the JIP) is sent by LSP-X
- Verify that the IXC performs the LNP database query
- LSP-X, LSP-Y and the IXC validate that the appropriate billing records are created and the appropriate trunk group is used.



Test #11: Intra-LATA/Inter-LATA Toll (PICd or Casual Dialing) via Direct Trunks to an IXC - Non-Ported Number to Ported Number

Figure 11

11.2.9 Test Number 12 - Intra-LATA/Inter-LATA Toll (PICd or Casual Dialing) via an Access Tandem to an IXC. (Ported Number to Ported Number)

11.2.9.1 Test Description

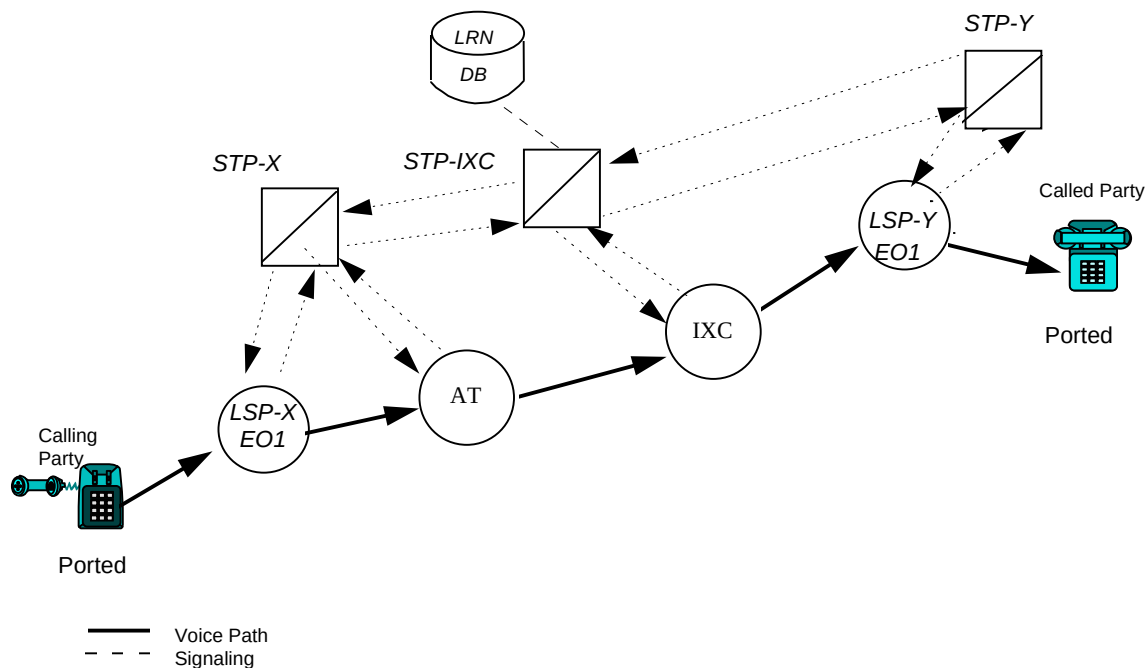
This will test that a toll call can be completed from a ported number in a recipient switch (LSP-X) to a ported number in another recipient switch (LSP-Y) via an Access Tandem to an IXC (See Figure 12)

11.2.9.2 Test Procedure

- From a ported number in recipient switch LSP-X, call a ported number in recipient switch LSP-Y using an IXC (PICd or Casual Dialing)
- Document test results

11.2.9.3 Expected Test Results

- The call completes to the appropriate termination at LSP-Y
- Verify that the originating LRN (in the JIP) is sent by LSP-X
- Verify that the IXC performs the LNP database query
- LSP-X, LSP-Y and the IXC validate that the appropriate billing records are created and the appropriate trunk groups are used.



Test #12: Intra-LATA/Inter-LATA Toll (PICd or Casual Dialing) via an Access Tandem to an IXC - Ported Number to Ported Number

Figure 12

11.2.10 Test Number 13 - Intra-LATA/Inter-LATA Toll (PICd or Casual Dialing) via an Access Tandem to an IXC. (Non Ported Number to Ported Number)

11.2.10.1 Test Description

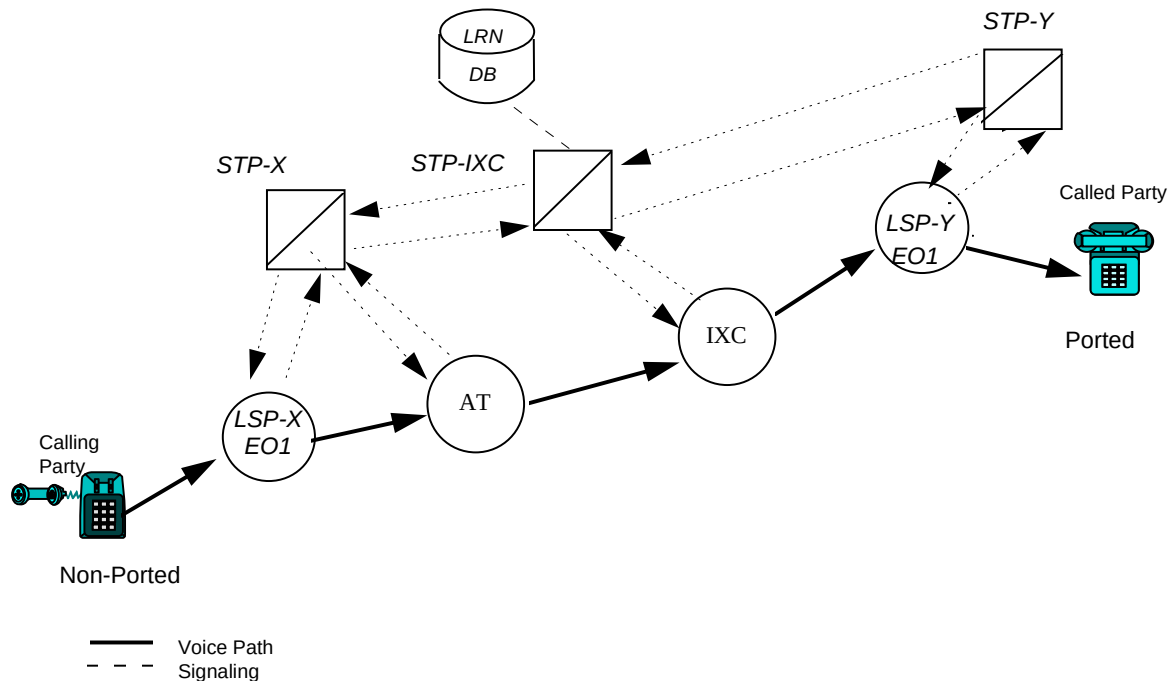
This will test that a toll call can be completed from a non-ported number in an NPA-NXX opened to portability in a switch (LSP-X) to a ported number in a recipient switch (LSP-Y) via an Access Tandem to an IXC (See Figure 13).

11.2.10.2 Test Procedure

- From a ported number in a NPA-NXX opened to portability in LSP-X, call a ported number in recipient switch LSP-Y using an IXC (PICd or Casual Dialing).
- Document test results

11.2.10.3 Expected Test Results

- The call completes to the appropriate termination at LSP-Y
- Verify that the originating LRN (in the JIP) is sent by LSP-X
- Verify that the IXC performs the LNP database query
- LSP-X, LSP-Y and the IXC validate that the appropriate billing records are created and the appropriate trunk groups are used.



Test #13: Intra-LATA/Inter-LATA Toll (PICd or Casual Dialing) via an Access Tandem to an IXC - Non-Ported Number to Ported Number

Figure 13

11.3 Default Routing Tests

CAUTION: The following three Default Routing tests (14, 15 and 16) are deemed to be intrusive in nature. For this reason, network impacts should be considered prior to performing these tests in a live network.

Default Routing occurs when the switch that normally performs the LRN Database query is unable to communicate with the SCP and the call is routed to the donor switch that performs the query and completes the call.

11.3.1 Test Number 14 - Intra-LATA Local Default Routing via Direct Trunks. (Ported Number to Ported Number)

11.3.1.1 Test Description

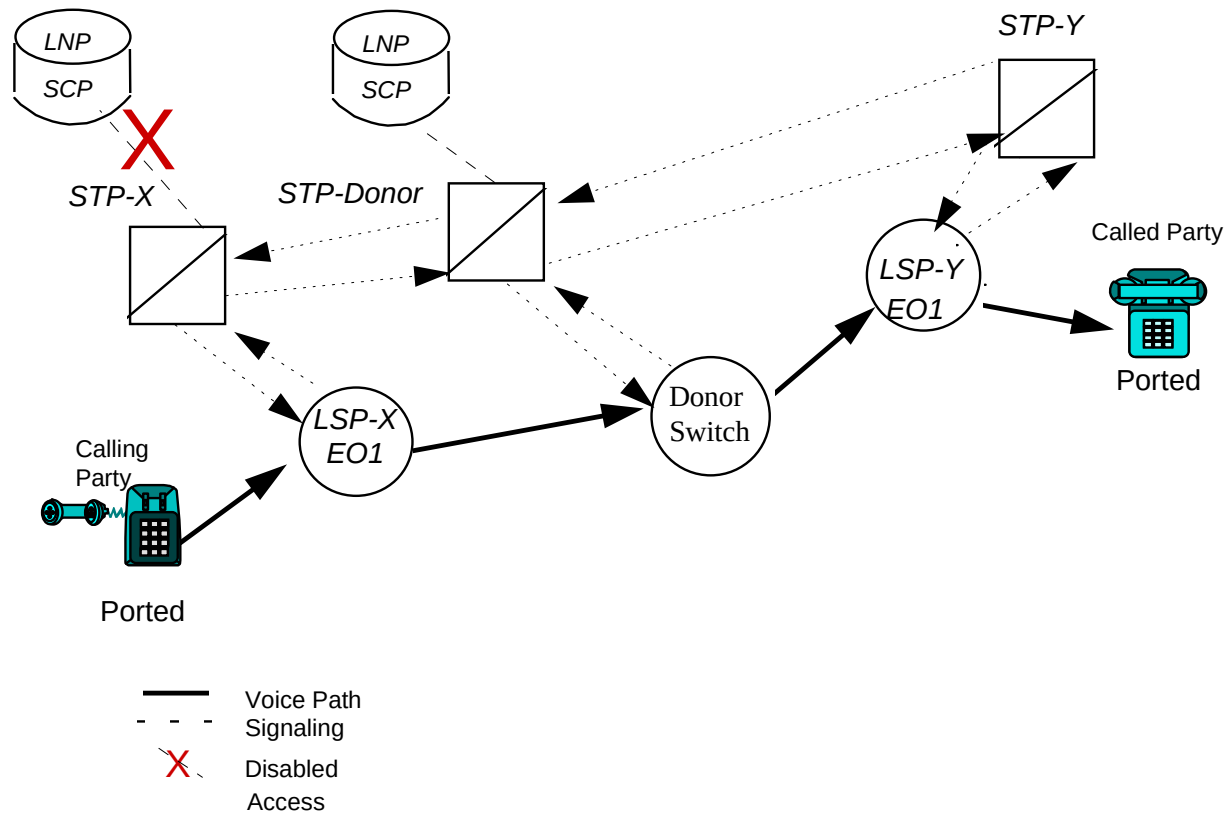
This will test that a local call can be completed from a ported number in a recipient switch (LSP-X) to a ported number in another recipient switch (LSP-Y) using direct trunks and default routing to the donor switch (See Figure 14).

11.3.1.2 Test Procedure

- Disable access to the SCP serving LSP-X
- From a ported number in recipient switch LSP-X, call the ported number in recipient switch LSP-Y.
- Document test results

11.3.1.3 Expected Test Results

- The call completes to the appropriate termination at LSP-Y
- LSP-X, LSP-Y and donor switch validate that appropriate billing records are created and the appropriate trunk groups are used. This is to ensure that:
 - o Originating LSP-X routes call to the donor switch
 - o Donor switch performs LRN database query
 - o Donor switch routes call to LSP-Y



Test #14: Intra-LATA Local Default Routing via Direct Trunks - Ported Number to Ported Number

Figure 14

11.3.3 Test Number 16 - Intra-LATA/Inter-LATA Toll Default Routing via an Access Tandem to an IXC. (Ported Number to Ported Number)

11.3.3.1 Test Description

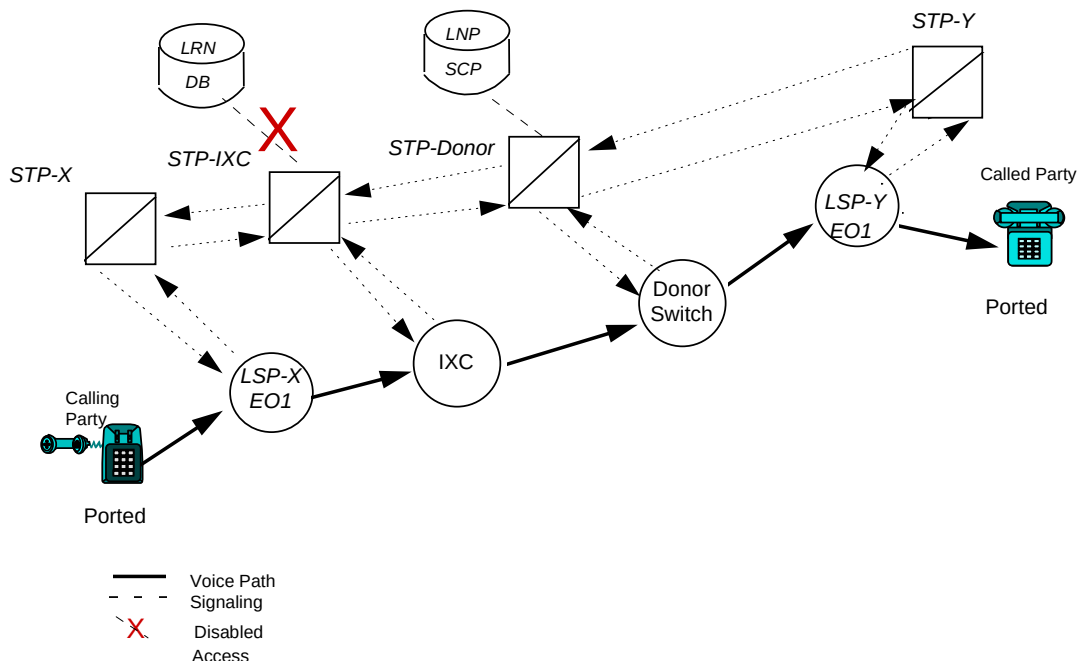
This will test that a toll call can be completed from a ported number in a recipient switch (LSP-X) to a ported number in another recipient switch (LSP-Y) via Direct Trunks or Access Tandem to an IXC. (See Figure 16)

11.3.3.2 Test Procedure

- Disable access to the LRN database serving the IXC
- From a ported number in recipient switch LSP-X, call the ported number in recipient switch LSP-Y
- Document test results

11.3.3.3 Expected Test Results

- The call completes to the appropriate termination at LSP-Y
- LSP-X, LSP-Y, donor switch and IXC validate that appropriate billing records are created and the appropriate trunk groups are used. This is to ensure that:
 - o LSP-X routes the call to the IXC
 - o LSP-X sends the originating LRN (in the JIP) to the IXC
 - o IXC default routes the call to the donor switch
 - o Donor switch performs the LRN database query
 - o Donor switch routes call to LSP-Y



Test #16: Intra-LATA/Inter-LATA Toll (PICd or Casual Dialing) Default Routing (via Direct Trunks or Access Tandem) to an IXC - Ported Number to Ported Number

Figure 16

11.4 E-9-1-1 Test Calls

Prior to any 9-1-1 test calls, the local service provider should call the non-emergency number of the serving PSAP(s) and verify and/or obtain authorization to perform the test calls.

Test calls should be performed after the number is ported to ensure that the E-9-1-1 database has been updated.

11.4.1 Test Number 17 - E9-1-1 Call from a Ported Number and a return call from the PSAP to the Ported Number.

11.4.1.1 Test Description

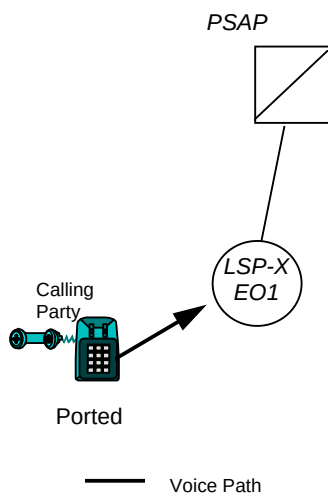
This will test that an E9-1-1 call can be completed from a ported number to a PSAP, the appropriate information will be displayed at the PSAP, and that the PSAP can call back the ported number.

11.4.1.2 Test Procedure

- From a ported number in LSP-X, dial 9-1-1.
- Explain to the PSAP that this is LSP-X making a test call.
- Verify that the PSAP received the correct ported number, subscriber address, and Company ID of LSP-X.
- Ask to be called back at the number they received on the display.
- Document test results.

11.4.1.3 Expected Test Results

- The call completes to the PSAP from the ported number.
- Correct ported number, subscriber address, and Company ID of LSP-X. is received by the PSAP.
- The call completes from the PSAP to the ported number.



Test #17 E911 Call from a Ported Number and a return call from the PSAP to the Ported Number

Figure 17

11.4.2 Test Number 18 - E9-1-1 Call from a Ported Number to PSAP(1), transfer from PSAP(1) to PSAP (2),and a return call from PSAP(2) to the Ported Number.

11.4.2.1 Test Description

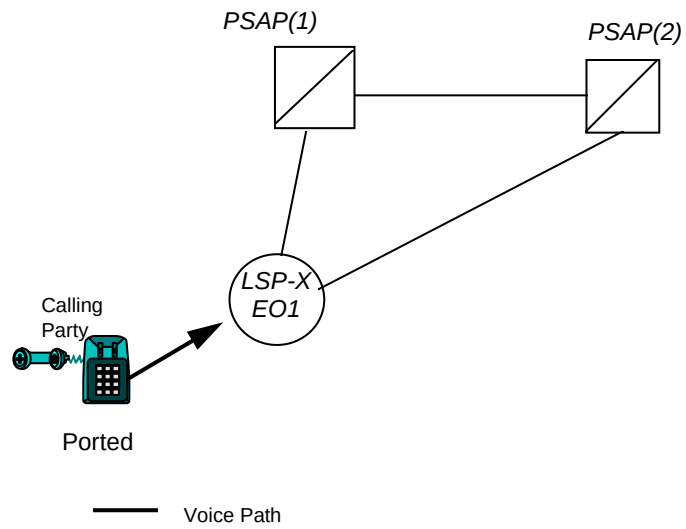
This will test that an E9-1-1 call can be completed from a ported number to a PSAP(1), the call be transferred to PSAP(2), the appropriate information will be displayed at both PSAPs, and that PSAP(2) can call back the ported number.

11.4.2.2 Test Procedure

- From a ported number in LSP-X, dial 9-1-1.
- Explain to the PSAP(1) that this is LSP-X making a test call.
- Verify that PSAP(1) received the correct ported number, subscriber address, and Company ID of LSP-X.
- Ask the dispatcher to transfer you to another PSAP(2).
- Explain to the PSAP(2) that this is LSP-X making a test call.
- Verify that PSAP(2) received the correct ported number, subscriber address, and Company ID of LSP-X.
- Ask to be called back at the number they received on the display.
- Document test results.

11.4.2.3 Expected Test Results

- The call completes to PSAP(1) from the ported number.
- Correct ported number, subscriber address, and Company ID of LSP-X is received by the PSAP(1).
- PSAP(1) can transfer the call to PSAP(2).
- Correct ported number, subscriber address, and Company ID of LSP-X is received by the PSAP(2).
- The return call completes from PSAP(2) to the ported number.



Test #18 E911 Call from a Ported Number to PSAP(1), transfer from PSAP(1) to PSAP (2), and a return call from PSAP(2) to the Ported Number

Figure 18



ATIS-0300035

**Next Generation Interconnection Interoperability (NGIIF)
Reference Document**

Part XII, Tollfree Industry Test Plan

Version 12.0



ATIS is the leading technical planning and standards development organization committed to the rapid development of global, market-driven standards for the information, entertainment and communications industry. More than 200 companies actively formulate standards in ATIS' Committees, covering issues including: IPTV, Cloud Services, Energy Efficiency, IP-Based and Wireless Technologies, Quality of Service, Billing and Operational Support, Emergency Services, Architectural Platforms and Emerging Networks. In addition, numerous Incubators, Focus and Exploratory Groups address evolving industry priorities including Smart Grid, Machine-to-Machine, Connected Vehicle, IP Downloadable Security, Policy Management and Network Optimization.

ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications' Sectors, and a member of the Inter-American Telecommunication Commission (CITEL). ATIS is accredited by the American National Standards Institute (ANSI). For more information, please visit www.atis.org.

Notice

This document was developed by the Alliance for Telecommunications Industry Solutions' (ATIS) sponsored Next Generation Interconnection Interoperability Forum (NGIIF). The NGIIF addresses next-generation network interconnection and interoperability issues associated with emerging technologies. Specifically, it develops operational procedures which involve the network aspects of architecture, disaster preparedness, installation, maintenance, management, reliability, routing, security, and testing between network operators. In addition, the NGIIF addresses issues which impact the interconnection of existing and next generation networks and facilitate the transition to emerging technologies. All changes to this document shall be made through the NGIIF issue resolution process.

Note Regarding Previous Versions

The NIIF Reference Document was formerly known as the Network Operations Forum (NOF) Reference Document. The NOF Reference Document was published and maintained by Bellcore. The last version of the NOF Reference Document is Issue 13.

Disclaimer and Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

ATIS-0300035, *NGIIF Reference Document, Part XII, Tollfree Industry Test Plan, Formerly NIIF 5031*

The NGIIF Reference Document, Part XII, Tollfree Industry Test Plan, is an ATIS standard developed by the NGIIF.

Published by

Alliance for Telecommunications Industry Solutions

1200 G Street, NW, Suite 500

Washington, DC 20005

Copyright © 2011 by Alliance for Telecommunications Industry Solutions

All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < <http://www.atis.org> >.

Printed in the United States of America.

TOLLFREE INDUSTRY TEST PLAN

Table of Contents

1	GENERAL.....	3
1.1	BACKGROUND	3
1.2	TESTING SCOPE	3
1.3	ASSUMPTIONS.....	3
1.4	RESPONSIBILITIES.....	3
1.4.1	SMS/800 Management Team (SMT)	3
1.4.2	NGIIF.....	3
1.4.3	Access Service Providers (ASPs)	4
1.4.4	Access Service Customers (ASCs).....	4
1.4.5	RESP ORGs	4
2	CALL-THROUGH TEST CALLS IN THE NEW TOLL FREE NPA.....	4
2.1	TEST CALLS	4
2.1.1	Assumptions	4
2.2	TEST SCRIPTS:	4
2.2.1	Calls from Within the Area of Service (AOS).....	4
2.2.2	Calls from Outside the Area of Service (AOS).....	5
2.2.3	Calls to a Non Working number in the new Toll Free NPA.....	5
3	PROCEDURES.....	5
3.1	PROCEDURES FOR FAILED TESTS	5
3.2	PROCEDURES FOR TROUBLE REPORTING AND STATUSING, AND MAINTENANCE	5
3.2.1	Trouble Reporting.....	5
3.2.2	Statusing.....	5
3.2.3	Maintenance Procedures	6
3.3	PERFORMANCE OBSERVATIONS.....	6
4	APPENDIX A – SMS/800 TEST NUMBER ASSIGNMENT PROCESS FOR TOLLFREE NPAS.....	7
4.1	TEST NUMBERS FOR THE DEPLOYMENT OF THE NEW TOLL FREE NPA.....	7
5	APPENDIX B - PERMANENT TEST NUMBER ASSIGNMENT.....	8
6	APPENDIX C – TROUBLE REFERRAL NUMBERS.....	24
6.1	SORTED BY RESP ORG ID	24
6.2	SORTED BY RESP ORG NAME.....	73

1 General

1.1 Background

The Industry Numbering Committee (INC) determined that additional numbering resources are needed to meet the future demands for Toll Free services. On January 25, 1995, INC designated several new codes (888, 877, 866, 855, etc.) to be reserved for Toll Free services. Implementation of additional Toll Free numbers may require many network modifications, including the upgrade of hardware and software in the Access Service Providers' (ASPs) networks, the Access Service Customers' (ASCs) networks, and the SMS/800 System. The national database of Toll Free numbers (SMS/800) is administered by the SMS/800 Management Team. The SMS/800 Management Team (SMT) utilize Unisys (SMS/800 Data Center), Sykes (SMS/800 Help Desk), and Telcordia (SMS/800 Site Support) as vendors under contract to support the SMS/800 system. Database Service Management, Inc. (DSMI) is the SMS/800 Business Manager who manages SMS/800 on behalf of the SMT. SCP Owner/Operators (SCP O/O) connect to SMS/800 through the SMS/800 Data Center.

1.2 Testing Scope

The purpose of this test plan is to verify and confirm that all service management and tollfree specific network components involved with the provisioning and processing of tollfree database access calls of all industry participants perform as expected.

1.3 Assumptions

- The testing will be performed via current SMS/800 access arrangements
- The type of test will govern whether or not the testing will be done in the live production system or on the new production hardware prior to being live.
- Test cases involving actual test calls require a live SCP connected to the real network for processing.
- The Industry Testing will be conducted during the time frames agreed to by the NGIIF based on the in service dates provided by the OBF/SNAC.
- Support for SMS/800 functionality testing will be provided by the SMS/800 Management Team using the SMS/800 Help Desk, the SMS/800 Data Center, and the SMS/800 Software Support Organization.

1.4 Responsibilities

Many organizations will be involved with the successful implementation of the Toll Free Database Industry Test Plan. Listed below are the organizations identified to date, and the activities in which they are responsible, if they wish to participate. Additional organizations and responsibilities will be added as required.

Each organization is responsible for identifying a "single point of contact".

1.4.1 SMS/800 Management Team (SMT)

- Responsible for providing SMS/800 toll free system under Tariff F.C.C. No. 1: The Bell Operating Companies 800 Service Management System (SMS/800) Functions.
- Responsible for administration and availability of new toll free NPA-250 Test Numbers (See Attachment 1 - SMS/800 Test Number Assignment Process).

1.4.2 NGIIF

- Facilitation of conference calls to review test plan development and testing progress.
- Provide the OBF- SNAC with the industry test start date, the industry test complete date, and the industry network ready date.

1.4.3 Access Service Providers (ASPs)

- Participate with the RESP ORGs as needed
- Provide to the industry availability of new toll free NPA functionality

1.4.4 Access Service Customers (ASCs)

- Ensure new toll free NPA-250 test calls can route through their networks with the appropriate ANI II digit combination; specifically, but not limited to, 00, 23, and 24.
- Provide the industry with information that will facilitate the processing of test calls.
- Provision terminations (New Toll Free NXX Number) for test calls which uniquely identify the termination.

1.4.5 RESP ORGs

- Provide SCP Owner/Operators with Information required to facilitate the processing of test calls.
- Overall coordination for executing test calls with ASPs and SCP owners (e.g. Area of Service (AOS), and Carrier Traffic Allocation).
- Building Test Records to test areas of SMS/800 functionality and to perform test calls they feel are important.
- Coordinate terminations for test calls which uniquely identify the termination.

2 Call-Through Test Calls in the New Toll Free NPA

2.1 Test Calls

To test the physical routing of a call when a number in a new Toll Free NPA is dialed from a telephone that is within the defined AOS as well as from a telephone that is outside the AOS.

2.1.1 Assumptions

- Either a POTS routing number or a turn around number in the new Toll Free NPA can be used on the Customer Records created for call through purposes.
- Test calls will be made to working -250 test numbers in the new Toll Free NPA and originate from within the AOS and outside the AOS of the new Toll Free NPA number dialed. Test calls will also be made to disconnected numbers and non working numbers.
- The logistics of the number of calls placed and the SCPs accessed will be decided jointly by the testing ASC and involved ASPs.
- The ASC will ensure that they have the capability of routing (including appropriate ANI II digits) 250 calls in the new Toll Free NPA in their Network.

2.2 Test Scripts:

2.2.1 Calls from Within the Area of Service (AOS)

2.2.1.1 Required Data

- Working 250 test numbers in the new Toll Free NPA
- Disconnected 250 test numbers in the new Toll Free NPA - with and without referral

2.2.1.2 Expected Results

When a call is placed to a number in the new Toll Free NPA that is in service, the caller with an originating ANI that is within the AOS will terminate to the POTS number or to the carrier routing the turnaround number. Calls placed to a number in the new Toll Free NPA that has been disconnected with referral will terminate to the POTS

number or to the carrier routing the turnaround number. Calls placed to a number in the new Toll Free NPA that has been disconnected without referral will result in the "disconnect no referral announcement" being returned.

2.2.2 Calls from Outside the Area of Service (AOS)

2.2.2.1 Required Data

- Working 250 test numbers in the new Toll Free NPA

2.2.2.2 Expected Results

When a call is placed to a number in the new Toll Free NPA that is in service, but the caller that is outside the AOS, Out of Band Announcement will be returned.

2.2.3 Calls to a Non Working number in the new Toll Free NPA

2.2.3.1 Required Data

- Assigned 250 test number in the new Toll Free NPA
- Transitional 250 test number in the new Toll Free NPA
- Spare 250 test number in the new Toll Free NPA

2.2.3.2 Expected Results

When a call is placed to a number in the new Toll Free NPA that is not in service, the caller will receive Vacant Code Announcement regardless of whether the originating ANI is within or outside the AOS.

2.2.3.3 Comments

The ASP will route the number in the new Toll Free NPA based on the originating ANI or LATA that is sent with the query and will return either a POTS number or the dialed number in the new Toll Free NPA and the CIC back to the network.

3 Procedures

3.1 Procedures for Failed Tests

Performance observations outside of acceptable parameters shall be considered as having Failed the agreed upon Expectations, and will be referred to the ASP or ASC [Access Service Provider/Access Service Customer] responsible for the resolution of the problem. The ASP or ASC will then develop and implement an Action Plan to bring performance levels up to agreed upon expectations.

Attachment 3 should be used for the referral of Trouble Reports related to database problems associated with the new Toll Free NPA during the Industry Test Interval.

3.2 Procedures for Trouble Reporting and Statusing, and Maintenance

3.2.1 Trouble Reporting

Troubles should be reported to the person/organization designated to receive transition test troubles.

Attachment 3 should be used for the referral of Trouble Reports related to database problems associated with the new Toll Free NPA during the Industry Test Interval.

3.2.2 Statusing

Maintenance Statusing and Escalation procedures will be done in accordance with locally agreed upon contracts and procedures.

3.2.3 Maintenance Procedures

Existing company trouble reporting procedures are deemed adequate and will be utilized. Therefore, they do not need to be tested within the context of this test plan.

3.3 Performance Observations

With the implementation of the new Toll Free NPA, the following types of performance criteria should be observed, and provided as noted in NGIIF Documents:

- Call Blocking
- Call Gapping
- Link Congestion
- Other Network Congestion

Observation of Network components should be monitored by ASPs and ASCs during Implementation of the new Toll Free NPA. Any abnormalities in the network that are service affecting should be transmitted to the "Operating Company" of the number in the new Toll Free NPA in a timely manner.

Any Industry Test Plan participant requiring additional information concerning the above data should contact the appropriate ASCs and/or ASPs, using the NGIIF Contact Directory. The information will be supplied on request.

4 APPENDIX A – SMS/800 TEST NUMBER ASSIGNMENT PROCESS FOR TOLLFREE NPAs

On September 8, 1995, the SMS/800 Management Team directed the SMS/800 Help Desk to implement the agreement reached by the SMS/800 Number Administration Committee (SNAC) and the Network Operations Forum (NOF) (now the NGIIF) regarding the utilization of the Toll Free (NPA-250) test numbers. This agreement stated that the line numbers from 0000 through 1499 (within the Toll Free NPA-250 code), would be reserved for testing purposes. The remaining line numbers in the Toll Free NPA-250 code are made available for general (customer) assignment. . It is assumed that this agreement will be extended for test numbers in all the new Toll Free NPAs.

4.1 Test Numbers for the Deployment of the new Toll Free NPA

Responsible Organizations (Resp Orgs) may obtain toll free test numbers by calling the SMS/800 Help Desk at 1-888-271-9300 Option 1.

The process by which the SMS/800 Help Desk will assign test numbers for the new toll free NPA is as follows:

Each Resp Org will have two (2) test numbers for each toll free NPA. These test numbers, as assigned, recaptured, or changed by the SMS/800 Help Desk, are from a block of numbers beginning with 250-0000 through 250- 1499. As in the past, this block of numbers will remain in “Unavailable”¹ status. A listing of these test numbers, as assigned to each Resp Org is shown in ATIS/NGIIF Document #0005 (Permanent Test Numbers)

¹ Unavailable – Not for general (customer) assignment.

5 APPENDIX B - PERMANENT TEST NUMBER ASSIGNMENT

The SMS/800 Help Desk (888-271-9300 Option 1) is responsible for assigning, recapturing and changing the 250 Permanent test numbers.

The numbers range from 250-0000 through 250-1499

(ATIS/NGIIF 0005)

Company Name	800	888	877	855	866
ABCO Communications Inc.	800-250-0003	888-250-0003	877-250-0003	855-250-0003	866-250-0003
ABCO Communications Inc.	800-250-0273	888-250-0273	877-250-0273	855-250-0273	866-250-0273
ACC Telecom	800-250-0005	888-250-0005	877-250-0005	855-250-0005	866-250-0005
ACC Telecom	800-250-0006	888-250-0006	877-250-0006	855-250-0006	866-250-0006
ACC Telecom	800-250-0209	888-250-0209	877-250-0209	855-250-0209	866-250-0209
ACC Telecom	800-250-0214	888-250-0214	877-250-0214	855-250-0214	866-250-0214
Access L.D./Western Int'l Media	800-250-0269	888-250-0269	877-250-0269	855-250-0269	866-250-0269
Access L.D./Western Int'l Media	800-250-0270	888-250-0270	877-250-0270	855-250-0270	866-250-0270
Accessline Communications Corp.	800-250-0044	888-250-0044	877-250-0044	855-250-0044	866-250-0044
Accessline Communications Corp.	800-250-0062	888-250-0062	877-250-0062	855-250-0062	866-250-0062
Advanced Communications - Feist	800-250-0359	888-250-0359	877-250-0359	855-250-0359	866-250-0359
Advanced Communications - Feist	800-250-0360	888-250-0360	877-250-0360	855-250-0360	866-250-0360
Advanced Routing Technologies	800-250-0289	888-250-0289	877-250-0289	855-250-0289	866-250-0289
Advanced Routing Technologies	800-250-0290	888-250-0290	877-250-0290	855-250-0290	866-250-0290
Advanced Tel. Inc.	800-250-0121	888-250-0121	877-250-0121	855-250-0121	866-250-0121
Advanced Tel. Inc.	800-250-0122	888-250-0122	877-250-0122	855-250-0122	866-250-0122
Advanced Telecommunications Network Inc.	800-250-0089	888-250-0089	877-250-0089	855-250-0089	866-250-0089
Advanced Telecommunications Network Inc.	800-250-0090	888-250-0090	877-250-0090	855-250-0090	866-250-0090
Alascom Inc.	800-250-0276	888-250-0276	877-250-0276	855-250-0276	866-250-0276
Alascom Inc.	800-250-0390	888-250-0390	877-250-0390	855-250-0390	866-250-0390
All Star Telecom	800-250-0345	888-250-0345	877-250-0345	855-250-0345	866-250-0345
All Star Telecom	800-250-0346	888-250-0346	877-250-0346	855-250-0346	866-250-0346
Alliance Group Services Inc.	800-250-0324	888-250-0324	877-250-0324	855-250-0324	866-250-0324
Alliance Group Services Inc.	800-250-0330	888-250-0330	877-250-0330	855-250-0330	866-250-0330
Allstate Communications Inc.	800-250-0337	888-250-0337	877-250-0337	855-250-0337	866-250-0337
Allstate Communications Inc.	800-250-0339	888-250-0339	877-250-0339	855-250-0339	866-250-0339
American Long Lines	800-250-0293	888-250-0293	877-250-0293	855-250-0293	866-250-0293

American Long Lines	800-250-0294	888-250-0294	877-250-0294	855-250-0294	866-250-0294
Amerigon Inc.	800-250-0301	888-250-0301	877-250-0301	855-250-0301	866-250-0301
Amerigon Inc.	800-250-0302	888-250-0302	877-250-0302	855-250-0302	866-250-0302
Ameritech Communications Inc.	800-250-0079	888-250-0079	877-250-0079	855-250-0079	866-250-0079
Ameritech Communications Inc.	800-250-0080	888-250-0080	877-250-0080	855-250-0080	866-250-0080
Ameritech Services Inc.	800-250-0297	888-250-0297	877-250-0297	855-250-0297	866-250-0297
Ameritech Services Inc.	800-250-0300	888-250-0300	877-250-0300	855-250-0300	866-250-0300
Ameritel	800-250-0146	888-250-0146	877-250-0146	855-250-0146	866-250-0146
Ameritel	800-250-0147	888-250-0147	877-250-0147	855-250-0147	866-250-0147
AmeriVision Communications	800-250-0412	888-250-0412	877-250-0412	855-250-0412	866-250-0412
AmeriVision Communications	800-250-0413	888-250-0413	877-250-0413	855-250-0413	866-250-0413
AT&A Canada Long Distance Service	800-250-0198	888-250-0198	877-250-0198	855-250-0198	866-250-0198
AT&A Canada Long Distance Service	800-250-0199	888-250-0199	877-250-0199	855-250-0199	866-250-0199
AT&T	800-250-0391	888-250-0391	877-250-0391	855-250-0391	866-250-0391
AT&T	800-250-0392	888-250-0392	877-250-0392	855-250-0392	866-250-0392
AT&T Canada Long Distance Services	800-250-0253	888-250-0253	877-250-0253	855-250-0253	866-250-0253
AT&T Canada Long Distance Services	800-250-0254	888-250-0254	877-250-0254	855-250-0254	866-250-0254
ATL Communications	800-250-0281	888-250-0281	877-250-0281	855-250-0281	866-250-0281
ATL Communications	800-250-0282	888-250-0282	877-250-0282	855-250-0282	866-250-0282
Atlantic Connections	800-250-0464	888-250-0464	877-250-0464	855-250-0464	866-250-0464
Atlantic Connections	800-250-0465	888-250-0465	877-250-0465	855-250-0465	866-250-0465
ATS Communications Corp.	800-250-0202	888-250-0202	877-250-0202	855-250-0202	866-250-0202
ATS Communications Corp.	800-250-0203	888-250-0203	877-250-0203	855-250-0203	866-250-0203
ATX Telecommunications Services	800-250-0285	888-250-0285	877-250-0285	855-250-0285	866-250-0285
ATX Telecommunications Services	800-250-0286	888-250-0286	877-250-0286	855-250-0286	866-250-0286
Bay Star Communications Inc.	800-250-0484	888-250-0484	877-250-0484	855-250-0484	866-250-0484
Bay Star Communications Inc.	800-250-0485	888-250-0485	877-250-0485	855-250-0485	866-250-0485
Beehive Telephone Inc.	800-250-0361	888-250-0361	877-250-0361	855-250-0361	866-250-0361
Beehive Telephone Inc.	800-250-0362	888-250-0362	877-250-0362	855-250-0362	866-250-0362
Bell Atlantic	800-250-0144	888-250-0144	877-250-0144	855-250-0144	866-250-0144
Bell Atlantic	800-250-0145	888-250-0145	877-250-0145	855-250-0145	866-250-0145
Bell Atlantic Long Distance	800-250-0262	888-250-0262	877-250-0262	855-250-0262	866-250-0262
Bell Atlantic Long Distance	800-250-0264	888-250-0264	877-250-0264	855-250-0264	866-250-0264

BellSouth Telecommunications	800-250-0042	888-250-0042	877-250-0042	855-250-0219	866-250-0042
BellSouth Long Distance	800-250-0219	888-250-0219	877-250-0219	855-250-0387	866-250-0219
BellSouth Long Distance	800-250-0387	888-250-0387	877-250-0387	855-250-0042	866-250-0387
BellSouth Telecommunications	800-250-0415	888-250-0415	877-250-0415	855-250-0415	866-250-0415
Bestline	800-250-0156	888-250-0156	877-250-0156	855-250-0156	866-250-0156
Bestline	800-250-0157	888-250-0157	877-250-0157	855-250-0157	866-250-0157
BH Telecom	800-250-0445	888-250-0445	877-250-0445	855-250-0445	866-250-0445
BH Telecom	800-250-0446	888-250-0446	877-250-0446	855-250-0446	866-250-0446
Birch Telecom Inc	800-250-0067	888-250-0067	877-250-0067	855-250-0067	866-250-0067
Birch Telecom Inc	800-250-0068	888-250-0068	877-250-0068	855-250-0068	866-250-0068
Broadwing Communications	800-250-0162	888-250-0162	877-250-0162	855-250-0162	866-250-0162
Broadwing Communications	800-250-0163	888-250-0163	877-250-0163	855-250-0163	866-250-0163
Broadwing Communications	800-250-0496	888-250-0496	877-250-0496	855-250-0496	866-250-0496
Broadwing Communications	800-250-0497	888-250-0497	877-250-0497	855-250-0497	866-250-0496
Business Telecom Inc.	800-250-0308	888-250-0308	877-250-0308	855-250-0308	866-250-0308
Business Telecom Inc.	800-250-0309	888-250-0309	877-250-0309	855-250-0309	866-250-0309
Buyers Online.com	800-250-0892	888-250-0892	877-250-0892	855-250-0892	866-250-0892
Buyers Online.com	800-250-0893	888-250-0893	877-250-0893	855-250-0893	866-250-0893
Cabel & Wireless	800-250-0229	888-250-0229	877-250-0229	855-250-0229	866-250-0229
Cabel & Wireless	800-250-0394	888-250-0394	877-250-0394	855-250-0394	866-250-0394
Cabelvision Lightpath	800-250-0353	888-250-0353	877-250-0353	855-250-0353	866-250-0353
Cabelvision Lightpath	800-250-0364	888-250-0364	877-250-0364	855-250-0364	866-250-0364
Call Management Systems Inc.	800-250-0130	888-250-0130	877-250-0130	855-250-0130	866-250-0130
Call Management Systems Inc.	800-250-0131	888-250-0131	877-250-0131	855-250-0131	866-250-0131
Call Sciences Inc.	800-250-0917	888-250-0917	877-250-0917	855-250-0917	866-250-0917
Call Sciences Inc.	800-250-0918	888-250-0918	877-250-0918	855-250-0918	866-250-0918
Capital Telecommunications Inc.	800-250-0315	888-250-0315	877-250-0315	855-250-0315	866-250-0315
Capital Telecommunications Inc.	800-250-0316	888-250-0316	877-250-0316	855-250-0316	866-250-0316
Caprock Communications	800-250-0207	888-250-0207	877-250-0207	855-250-0207	866-250-0207
Caprock Communications	800-250-0208	888-250-0208	877-250-0208	855-250-0208	866-250-0208
Carrier Network Services	800-250-0498	888-250-0498	877-250-0498	855-250-0498	866-250-0498
Carrier Network Services	800-250-0499	888-250-0499	877-250-0499	855-250-0499	866-250-0499
CGI Long Distance Services	800-250-0047	888-250-0047	877-250-0047	855-250-0047	866-250-0047

CGI Long Distance Services	800-250-0310	888-250-0310	877-250-0310	855-250-0310	866-250-0310
Cincinatti Bell Long Distance Inc.	800-250-0321	888-250-0321	877-250-0321	855-250-0321	866-250-0321
Cincinatti Bell Long Distance Inc.	800-250-0322	888-250-0322	877-250-0322	855-250-0322	866-250-0322
Citizens Communications	800-250-0323	888-250-0323	877-250-0323	855-250-0323	866-250-0323
Citizens Communications	800-250-0395	888-250-0395	877-250-0395	855-250-0395	866-250-0395
Cleartel Communications	800-250-0326	888-250-0326	877-250-0326	855-250-0326	866-250-0326
Cleartel Communications	800-250-0327	888-250-0327	877-250-0327	855-250-0327	866-250-0327
Commonwealth Long Distance Co.	800-250-0328	888-250-0328	877-250-0328	855-250-0328	866-250-0328
Commonwealth Long Distance Co.	800-250-0331	888-250-0331	877-250-0331	855-250-0331	866-250-0331
Communication Management Services	800-250-0474	888-250-0474	877-250-0474	855-250-0474	866-250-0474
Communication Management Services	800-250-0475	888-250-0475	877-250-0475	855-250-0475	866-250-0475
Communications Options Inc.	800-250-0334	888-250-0334	877-250-0334	855-250-0334	866-250-0334
Communications Options Inc.	800-250-0397	888-250-0397	877-250-0397	855-250-0397	866-250-0397
CommuniGroup Inc.	800-250-0332	888-250-0332	877-250-0332	855-250-0332	866-250-0332
CommuniGroup Inc.	800-250-0396	888-250-0396	877-250-0396	855-250-0396	866-250-0396
Community Networks	800-250-0060	888-250-0060	877-250-0060	855-250-0060	866-250-0060
Community Networks	800-250-0061	888-250-0061	877-250-0061	855-250-0061	866-250-0061
Connect America Inc.	800-250-0377	888-250-0377	877-250-0377	855-250-0377	866-250-0377
Connect America Inc.	800-250-0378	888-250-0378	877-250-0378	855-250-0378	866-250-0378
Cooperative Communications	800-250-0205	888-250-0205	877-250-0205	855-250-0205	866-250-0205
Cooperative Communications	800-250-0206	888-250-0206	877-250-0206	855-250-0206	866-250-0206
CTC Long Distance Services	800-250-0172	888-250-0172	877-250-0172	855-250-0172	866-250-0172
CTC Long Distance Services	800-250-0173	888-250-0173	877-250-0173	855-250-0173	866-250-0173
CTS/WorldXChange Communications	800-250-0338	888-250-0338	877-250-0338	855-250-0338	866-250-0338
CTS/WorldXChange Communications	800-250-0398	888-250-0398	877-250-0398	855-250-0398	866-250-0398
CYTEL	800-250-0375	888-250-0375	877-250-0375	855-250-0375	866-250-0375
CYTEL	800-250-0400	888-250-0400	877-250-0400	855-250-0400	866-250-0400
Destia Communications Services Inc.	800-250-0091	888-250-0091	877-250-0091	855-250-0091	866-250-0091
Destia Communications Services Inc.	800-250-0092	888-250-0092	877-250-0092	855-250-0092	866-250-0092
DTI	800-250-0861	888-250-0861	877-250-0861	855-250-0861	866-250-0861
DTI	800-250-0862	888-250-0862	877-250-0862	855-250-0862	866-250-0862
Eastern Tel Long Distance Service Inc.	800-250-0355	888-250-0355	877-250-0355	855-250-0355	866-250-0355
Eastern Tel Long Distance Service Inc.	800-250-0356	888-250-0356	877-250-0356	855-250-0356	866-250-0356

Eclipse Telecommunications Inc.	800-250-0150	888-250-0150	877-250-0150	855-250-0150	866-250-0150
Eclipse Telecommunications Inc.	800-250-0151	888-250-0151	877-250-0151	855-250-0151	866-250-0151
Efficacy Group Inc.	800-250-0853	888-250-0853	877-250-0853	855-250-0853	866-250-0853
Efficacy Group Inc.	800-250-0854	888-250-0854	877-250-0854	855-250-0854	866-250-0854
Electric Lightwave	800-250-0279	888-250-0279	877-250-0279	855-250-0279	866-250-0279
Electric Lightwave	800-250-0280	888-250-0280	877-250-0280	855-250-0280	866-250-0280
Excel Telcommunications Inc.	800-250-0085	888-250-0085	877-250-0085	855-250-0085	866-250-0085
Excel Telcommunications Inc.	800-250-0086	888-250-0086	877-250-0086	855-250-0086	866-250-0086
Federal Transtel Inc.	800-250-0136	888-250-0136	877-250-0136	855-250-0136	866-250-0136
Federal Transtel Inc.	800-250-0137	888-250-0137	877-250-0137	855-250-0137	866-250-0137
First Communications	800-250-0303	888-250-0303	877-250-0303	855-250-0303	866-250-0303
First Communications	800-250-0304	888-250-0304	877-250-0304	855-250-0304	866-250-0304
Florida Digital Network	800-250-0217	888-250-0217	877-250-0217	855-250-0217	866-250-0217
Florida Digital Network	800-250-0224	888-250-0224	877-250-0224	855-250-0224	866-250-0224
Focal Communications	800-250-0025	888-250-0025	877-250-0025	855-250-0025	866-250-0025
Focal Communications	800-250-0026	888-250-0026	877-250-0026	855-250-0026	866-250-0026
Fonorola Inc.	800-250-0363	888-250-0363	877-250-0365	855-250-0363	866-250-0363
Fonorola Inc.	800-250-0365	888-250-0365	877-250-0855	855-250-0365	866-250-0365
Fresh Start Communications	800-250-0021	888-250-0021	877-250-0021	855-250-0021	866-250-0021
Fresh Start Communications	800-250-0022	888-250-0022	877-250-0022	855-250-0022	866-250-0022
Frontier Communications International	800-250-0098	888-250-0098	877-250-0098	855-250-0098	866-250-0098
Frontier Communications International	800-250-0366	888-250-0366	877-250-0366	855-250-0366	866-250-0366
Frontier/Allnet Communications	800-250-0063	888-250-0063	877-250-0063	855-250-0063	866-250-0063
Frontier/Allnet Communications	800-250-0064	888-250-0064	877-250-0064	855-250-0064	866-250-0064
Frontier/American Sharecom Inc.	800-250-0027	888-250-0027	877-250-0027	855-250-0027	866-250-0027
Frontier/American Sharecom Inc.	800-250-0028	888-250-0028	877-250-0028	855-250-0028	866-250-0028
Frontier/Execuline of Sacramento	800-250-0357	888-250-0357	877-250-0357	855-250-0357	866-250-0357
Frontier/Execuline of Sacramento	800-250-0358	888-250-0358	877-250-0358	855-250-0358	866-250-0358
Frontier/Schneider Communications	800-250-0236	888-250-0236	877-250-0236	855-250-0236	866-250-0236
Frontier/Schneider Communications	800-250-0261	888-250-0261	877-250-0261	855-250-0261	866-250-0261
Frontier/West Telecommunications	Coast 800-250-0267	888-250-0267	877-250-0267	855-250-0267	866-250-0267
Frontier/West Telecommunications	Coast 800-250-0268	888-250-0268	877-250-0268	855-250-0268	866-250-0268

Full Service Network	800-250-0284	888-250-0284	877-250-0284	855-250-0284	866-250-0284
Full Service Network	800-250-0298	888-250-0298	877-250-0298	855-250-0298	866-250-0298
Full Spectrum Telecommunications Inc.	800-250-0333	888-250-0333	877-250-0333	855-250-0333	866-250-0333
Full Spectrum Telecommunications Inc.	800-250-0343	888-250-0343	877-250-0343	855-250-0343	866-250-0343
Galaxy Long Distance	800-250-0190	888-250-0190	877-250-0190	855-250-0190	866-250-0190
Galaxy Long Distance	800-250-0191	888-250-0191	877-250-0191	855-250-0191	866-250-0191
GCI Communications Corp.	800-250-0367	888-250-0367	877-250-0367	855-250-0367	866-250-0367
GCI Communications Corp.	800-250-0368	888-250-0368	877-250-0368	855-250-0368	866-250-0368
Global Telecommunications Solutions Inc.	800-250-0429	888-250-0429	877-250-0429	855-250-0429	866-250-0429
Global Telecommunications Solutions Inc.	800-250-0430	888-250-0430	877-250-0430	855-250-0430	866-250-0430
Global Tone Communications	800-250-0192	888-250-0192	877-250-0192	855-250-0192	866-250-0192
Global Tone Communications	800-250-0204	888-250-0204	877-250-0204	855-250-0204	866-250-0204
Globalcom Inc.	800-250-0894	888-250-0894	877-250-0894	855-250-0894	866-250-0894
Globalcom Inc.	800-250-0895	888-250-0895	877-250-0895	855-250-0895	866-250-0895
GST – Totalnet	800-250-0118	888-250-0118	877-250-0118	855-250-0118	866-250-0118
GST – Totalnet	800-250-0372	888-250-0372	877-250-0372	855-250-0372	866-250-0372
GST Call America	800-250-0311	888-250-0311	877-250-0311	855-250-0311	866-250-0311
GST Call America	800-250-0312	888-250-0312	877-250-0312	855-250-0312	866-250-0312
GTE Network Services	800-250-0109	888-250-0109	877-250-0109	855-250-0109	866-250-0109
GTE Network Services	800-250-0125	888-250-0125	877-250-0125	855-250-0125	866-250-0125
GTE Telephone Operators	800-250-0369	888-250-0369	877-250-0369	855-250-0369	866-250-0369
GTE Telephone Operators	800-250-0371	888-250-0371	877-250-0371	855-250-0371	866-250-0371
I.T. Group	800-250-0093	888-250-0093	877-250-0093	855-250-0093	866-250-0093
I.T. Group	800-250-0094	888-250-0094	877-250-0094	855-250-0094	866-250-0094
IDS Long Distance	800-250-0414	888-250-0414	877-250-0414	855-250-0414	866-250-0414
IDS Long Distance	800-250-0418	888-250-0418	877-250-0418	855-250-0418	866-250-0418
IDT Corporation	800-250-0482	888-250-0482	877-250-0482	855-250-0482	866-250-0482
IDT Corporation	800-250-0483	888-250-0483	877-250-0483	855-250-0483	866-250-0483
ILD Telecommunications Inc.	800-250-0879	888-250-0879	877-250-0879	855-250-0879	866-250-0879
ILD Telecommunications Inc.	800-250-0880	888-250-0880	877-250-0880	855-250-0880	866-250-0880
I-Link Communications	800-250-0421	888-250-0421	877-250-0421	855-250-0421	866-250-0421
I-Link Communications	800-250-0422	888-250-0422	877-250-0422	855-250-0422	866-250-0422

Illuminet	800-250-0240	888-250-0240	877-250-0240	855-250-0240	866-250-0240
Illuminet	800-250-0241	888-250-0241	877-250-0241	855-250-0241	866-250-0241
Information & Telephone Services Inc.	800-250-0158	888-250-0158	877-250-0158	855-250-0158	866-250-0158
Information & Telephone Services Inc.	800-250-0159	888-250-0159	877-250-0159	855-250-0159	866-250-0159
Infotel CommunicationsLLC	800-250-0245	888-250-0245	877-250-0245	855-250-0245	866-250-0245
Infotel CommunicationsLLC	800-250-0246	888-250-0246	877-250-0246	855-250-0246	866-250-0246
Intermedia Communications	800-250-0140	888-250-0140	877-250-0140	855-250-0148	866-250-0148
Intermedia Communications	800-250-0148	888-250-0148	877-250-0148	855-250-0149	866-250-0149
Intermedia Communications	800-250-0149	888-250-0149	877-250-0149	855-250-0174	866-250-0174
Intermedia Communications	800-250-0153	888-250-0153	877-250-0153	855-250-0175	866-250-0175
Intermedia Communications	800-250-0174	888-250-0174	877-250-0174	855-250-0352	866-250-0352
Intermedia Communications	800-250-0175	888-250-0175	877-250-0175	855-250-0354	866-250-0354
Intermedia Communications	800-250-0352	888-250-0352	877-250-0352	855-250-0374	866-250-0374
Intermedia Communications	800-250-0354	888-250-0354	877-250-0354	855-250-0376	866-250-0376
Intermedia Communications	800-250-0374	888-250-0374	877-250-0374		
Intermedia Communications	800-250-0376	888-250-0376	877-250-0376		
International Telecom LTC	800-250-0034	888-250-0034	877-250-0034	855-250-0034	866-250-0034
International Telecom LTC	800-250-0035	888-250-0035	877-250-0035	855-250-0035	866-250-0035
International TelecommunicationsService Inc.	800-250-0871	888-250-0871	877-250-0871	855-250-0871	866-250-0871
International TelecommunicationsService Inc.	800-250-0872	888-250-0872	877-250-0872	855-250-0872	866-250-0872
Interpath Communications Inc.	800-250-0865	888-250-0865	877-250-0865	855-250-0865	866-250-0865
Interpath Communications Inc.	800-250-0866	888-250-0866	877-250-0866	855-250-0866	866-250-0866
Ionex Telecommunications Inc.	800-250-0197	888-250-0197	877-250-0197	855-250-0197	866-250-0197
Ionex Telecommunications Inc.	800-250-0405	888-250-0405	877-250-0405	855-250-0405	866-250-0405
Ionex Telecommunications Inc.	800-250-0468	888-250-0468	877-250-0468	855-250-0468	866-250-0468
Ionex Telecommunications Inc.	800-250-0469	888-250-0469	877-250-0469	855-250-0469	866-250-0469
Iowa Communications Network	800-250-0113	888-250-0113	877-250-0113	855-250-0113	866-250-0113
Iowa Communications Network	800-250-0114	888-250-0114	877-250-0114	855-250-0114	866-250-0114
Iowa Network Services	800-250-0123	888-250-0123	877-250-0123	855-250-0123	866-250-0123
Iowa Network Services	800-250-0124	888-250-0124	877-250-0124	855-250-0124	866-250-0124
IT&E Overseas	800-250-0425	888-250-0425	877-250-0425	855-250-0425	866-250-0425
IT&E Overseas	800-250-0426	888-250-0426	877-250-0426	855-250-0426	866-250-0426

ITC Deltacom	800-250-0347	888-250-0347	877-250-0347	855-250-0347	866-250-0347
ITC Deltacom	800-250-0402	888-250-0402	877-250-0402	855-250-0402	866-250-0402
IXC Communications	800-250-0277	888-250-0277	877-250-0277	855-250-0277	866-250-0277
IXC Communications	800-250-0278	888-250-0278	877-250-0278	855-250-0278	866-250-0278
J.D. Services	800-250-0401	888-250-0401	877-250-0401	855-250-0401	866-250-0401
J.D. Services	800-250-0433	888-250-0433	877-250-0433	855-250-0433	866-250-0433
Lambda Operations	800-250-0043	888-250-0043	877-250-0043	855-250-0043	866-250-0043
Lambda Operations	800-250-0389	888-250-0389	877-250-0389	855-250-0389	866-250-0389
LCT Long Distance	800-250-0097	888-250-0097	877-250-0097	855-250-0097	866-250-0097
LCT Long Distance	800-250-0099	888-250-0099	877-250-0099	855-250-0099	866-250-0099
LDDS Metromedia (EDS)	800-250-0351	888-250-0351	877-250-0351	855-250-0351	866-250-0351
LDDS Metromedia (EDS)	800-250-0403	888-250-0403	877-250-0403	855-250-0403	866-250-0403
LDMI Long Distance	800-250-0494	888-250-0494	877-250-0494	855-250-0494	866-250-0494
LDMI Long Distance	800-250-0495	888-250-0495	877-250-0495	855-250-0495	866-250-0495
Legacy Long Distance	800-250-0381	888-250-0381	877-250-0381	855-250-0381	866-250-0381
Legacy Long Distance	800-250-0382	888-250-0382	877-250-0382	855-250-0382	866-250-0382
Legends Communications Inc.	800-250-0437	888-250-0437	877-250-0437	855-250-0437	866-250-0437
Legends Communications Inc.	800-250-0438	888-250-0438	877-250-0438	855-250-0438	866-250-0438
Level 3 Communications LLC	800-250-0058	888-250-0058	877-250-0058	855-250-0058	866-250-0058
Level 3 Communications LLC	800-250-0059	888-250-0059	877-250-0059	855-250-0059	866-250-0059
LightShip Telecom LLC	800-250-0890	888-250-0890	877-250-0890	855-250-0890	866-250-0890
LightShip Telecom LLC	800-250-0891	888-250-0891	877-250-0891	855-250-0891	866-250-0891
Local Communications Network Inc.	800-250-0470	888-250-0470	877-250-0470	855-250-0470	866-250-0470
Local Communications Network Inc.	800-250-0471	888-250-0471	877-250-0471	855-250-0471	866-250-0471
Logix Communications	800-250-0031	888-250-0031	877-250-0031	855-250-0031	866-250-0031
Logix Communications	800-250-0295	888-250-0295	877-250-0295	855-250-0295	866-250-0295
Long Distance Management	800-250-0126	888-250-0126	877-250-0126	855-250-0126	866-250-0126
Long Distance Management	800-250-0127	888-250-0127	877-250-0127	855-250-0127	866-250-0127
Long Distance Partnership	800-250-0128	888-250-0128	877-250-0128	855-250-0128	866-250-0128
Long Distance Partnership	800-250-0129	888-250-0129	877-250-0129	855-250-0129	866-250-0129
Lynx Telecom LLC	800-250-0416	888-250-0416	877-250-0416	855-250-0416	866-250-0416
Lynx Telecom LLC	800-250-0417	888-250-0417	877-250-0417	855-250-0417	866-250-0417
MCI Telecommunications Corp.	800-250-0379	888-250-0379	877-250-0379	855-250-0379	866-250-0379

MCI Telecommunications Corp.	800-250-0380	888-250-0380	877-250-0380	855-250-0380	866-250-0380
MCI Worldcom	800-250-0115	888-250-0115	877-250-0115	855-250-0115	866-250-0115
MCI Worldcom	800-250-0116	888-250-0116	877-250-0116	855-250-0116	866-250-0116
MCI Worldcom	800-250-0443	888-250-0443	877-250-0443		
MCI Worldcom	800-250-0444	888-250-0444	877-250-0444		
McLeod USA	800-250-0340	888-250-0340	877-250-0340	855-250-0340	866-250-0340
McLeod USA	800-250-0399	888-250-0399	877-250-0399	855-250-0399	866-250-0399
McLeod USA/Access Long Dist.	800-250-0054	888-250-0054	877-250-0054	855-250-0054	866-250-0054
McLeod USA/Access Long Dist.	800-250-0055	888-250-0055	877-250-0055	855-250-0055	866-250-0055
MetroCall	800-250-0170	888-250-0170	877-250-0170	855-250-0170	866-250-0170
MetroCall	800-250-0171	888-250-0171	877-250-0171	855-250-0171	866-250-0171
MetTel	800-250-0370	888-250-0370	877-250-0370	855-250-0370	866-250-0370
MetTel	800-250-0393	888-250-0393	877-250-0393	855-250-0393	866-250-0393
Midwestern Tel	800-250-0313	888-250-0313	877-250-0313	855-250-0313	866-250-0313
Midwestern Tel	800-250-0314	888-250-0314	877-250-0314	855-250-0314	866-250-0314
Mirage Marketing	800-250-0087	888-250-0087	877-250-0087	855-250-0087	866-250-0087
Mirage Marketing	800-250-0088	888-250-0088	877-250-0088	855-250-0088	866-250-0088
National Comtel Network Inc.	800-250-0259	888-250-0259	877-250-0259	855-250-0259	866-250-0259
National Comtel Network Inc.	800-250-0260	888-250-0260	877-250-0260	855-250-0260	866-250-0260
Net-tel Corp.	800-250-0052	888-250-0052	877-250-0052	855-250-0052	866-250-0052
Net-tel Corp.	800-250-0053	888-250-0053	877-250-0053	855-250-0053	866-250-0053
Network Operator Services	800-250-0152	888-250-0152	877-250-0152	855-250-0152	866-250-0152
Network Operator Services	800-250-0386	888-250-0386	877-250-0386	855-250-0386	866-250-0386
Network Plus Inc.	800-250-0095	888-250-0095	877-250-0095	855-250-0095	866-250-0095
Network Plus Inc.	800-250-0096	888-250-0096	877-250-0096	855-250-0096	866-250-0096
Network Telecom Inc.	800-250-0455	888-250-0455	877-250-0455	855-250-0455	866-250-0455
Network Telecom Inc.	800-250-0456	888-250-0456	877-250-0456	855-250-0456	866-250-0456
Network Telephone Services Inc.	800-250-0155	888-250-0155	877-250-0155	855-250-0155	866-250-0155
Network Telephone Services Inc.	800-250-0404	888-250-0404	877-250-0404	855-250-0404	866-250-0404
New South Communications	800-250-0447	888-250-0447	877-250-0447	855-250-0447	866-250-0447
New South Communications	800-250-0448	888-250-0448	877-250-0448	855-250-0448	866-250-0448
Nextlink Affinity	800-250-0341	888-250-0341	877-250-0341	855-250-0341	866-250-0341
Nextlink Affinity	800-250-0342	888-250-0342	877-250-0342	855-250-0342	866-250-0342

Nextlink Communications	800-250-0071	888-250-0071	877-250-0071		
Nextlink Communications	800-250-0072	888-250-0072	877-250-0072		
Nextlink Communications	800-250-0349	888-250-0349	877-250-0349		
Nextlink Communications	800-250-0350	888-250-0350	877-250-0350		
Nextlink Communications	800-250-0490	888-250-0490	877-250-0490		
Nextlink Communications	800-250-0491	888-250-0491	877-250-0491		
Nextlink Interactive	800-250-0335	888-250-0335	877-250-0335	855-250-0335	866-250-0335
Nextlink Interactive	800-250-0336	888-250-0336	877-250-0336	855-250-0336	866-250-0336
Nextlink Nevada	800-250-0439	888-250-0439	877-250-0439	855-250-0439	866-250-0439
Nextlink Nevada	800-250-0440	888-250-0440	877-250-0440	855-250-0440	866-250-0440
Nextlink Pennsylvania LP	800-250-0325	888-250-0325	877-250-0325	855-250-0325	866-250-0325
Nextlink Pennsylvania LP	800-250-0329	888-250-0329	877-250-0329	855-250-0329	866-250-0329
Nextlink/Chadwick	800-250-0317	888-250-0317	877-250-0317	855-250-0317	866-250-0317
Nextlink/Chadwick	800-250-0318	888-250-0318	877-250-0318	855-250-0318	866-250-0318
Norlight Telecommunications Inc.	800-250-0453	888-250-0453	877-250-0453	855-250-0453	866-250-0453
Norlight Telecommunications Inc.	800-250-0855	888-250-0454	877-250-0454	855-250-0454	866-250-0454
North American Telephone Network	800-250-0023	888-250-0023	877-250-0023	855-250-0023	866-250-0023
North American Telephone Network	800-250-0024	888-250-0024	877-250-0024	855-250-0024	866-250-0024
Northwest Nevada Telco	800-250-0274	888-250-0274	877-250-0274	855-250-0274	866-250-0274
Northwest Nevada Telco	800-250-0275	888-250-0275	877-250-0275	855-250-0275	866-250-0275
NOS Communications	800-250-0138	888-250-0138	877-250-0138	855-250-0138	866-250-0138
NOS Communications	800-250-0139	888-250-0139	877-250-0139	855-250-0139	866-250-0139
NTS Communications Inc.	800-250-0142	888-250-0142	877-250-0142	855-250-0142	866-250-0142
NTS Communications Inc.	800-250-0143	888-250-0143	877-250-0143	855-250-0143	866-250-0143
NTS Communications Inc.	800-250-0287	888-250-0287	877-250-0287	855-250-0287	866-250-0287
NTS Communications Inc.	800-250-0288	888-250-0288	877-250-0288	855-250-0288	866-250-0288
OCI	800-250-0472	888-250-0472	877-250-0472	855-250-0472	866-250-0472
OCI	800-250-0473	888-250-0473	877-250-0473	855-250-0473	866-250-0473
One Call Communications Inc.	800-250-0160	888-250-0160	877-250-0160	855-250-0160	866-250-0160
One Call Communications Inc.	800-250-0161	888-250-0161	877-250-0161	855-250-0161	866-250-0161
OneStar Long Distance	800-250-0228	888-250-0228	877-250-0228	855-250-0228	866-250-0228
OneStar Long Distance	800-250-0230	888-250-0230	877-250-0230	855-250-0230	866-250-0230
Overseas Globaltel Corp.	800-250-0419	888-250-0419	877-250-0419	855-250-0419	866-250-0419

Overseas Globaltel Corp.	800-250-0420	888-250-0420	877-250-0420	855-250-0420	866-250-0420
Pac West Telecomm Inc.	800-250-0291	888-250-0291	877-250-0291	855-250-0291	866-250-0291
Pac West Telecomm Inc.	800-250-0292	888-250-0292	877-250-0292	855-250-0292	866-250-0292
Pacific Bell	800-250-0168	888-250-0168	877-250-0168	855-250-0168	866-250-0168
Pacific Bell	800-250-0169	888-250-0169	877-250-0169	855-250-0169	866-250-0169
Pacific Centrex Services	800-250-0911	888-250-0911	877-250-0911	855-250-0911	866-250-0911
Pacific Centrex Services	800-250-0912	888-250-0912	877-250-0912	855-250-0912	866-250-0912
PaeTec Communications Inc.	800-250-0881	888-250-0881	877-250-0881	855-250-0881	866-250-0881
PaeTec Communications Inc.	800-250-0882	888-250-0882	877-250-0882	855-250-0882	866-250-0882
Phone USA Inc.	800-250-0263	888-250-0263	877-250-0263	855-250-0263	866-250-0263
Phone USA Inc.	800-250-0266	888-250-0266	877-250-0266	855-250-0266	866-250-0266
Pilgrim Telephone Inc.	800-250-0176	888-250-0176	877-250-0176	855-250-0176	866-250-0176
Pilgrim Telephone Inc.	800-250-0177	888-250-0177	877-250-0177	855-250-0177	866-250-0177
PNG Telecommunications	800-250-0869	888-250-0869	877-250-0869	855-250-0869	866-250-0869
PNG Telecommunications	800-250-0887	888-250-0887	877-250-0887	855-250-0887	866-250-0887
PointOne Telecom	800-250-0898	888-250-0898	877-250-0898	855-250-0898	866-250-0898
PointOne Telecom	800-250-0899	888-250-0899	877-250-0899	855-250-0899	866-250-0899
POPP Telecom	800-250-0164	888-250-0164	877-250-0164	855-250-0164	866-250-0164
POPP Telecom	800-250-0165	888-250-0165	877-250-0165	855-250-0165	866-250-0165
Powercom	800-250-0200	888-250-0200	877-250-0200	855-252-0200	866-250-0200
Powercom	800-250-0201	888-250-0201	877-250-0201	855-250-0201	866-250-0201
Prime Tel Communications Inc.	800-250-0100	888-250-0100	877-250-0100	855-250-0100	866-250-0100
Prime Tel Communications Inc.	800-250-0112	888-250-0112	877-250-0112	855-250-0112	866-250-0112
Primus/Trescom	800-250-0195	888-250-0195	877-250-0195	855-250-0195	866-250-0195
Primus/Trescom	800-250-0196	888-250-0196	877-250-0196	855-250-0196	866-250-0196
Prism Communications Services	800-250-0492	888-250-0492	877-250-0492	855-250-0492	866-250-0492
Prism Communications Services	800-250-0493	888-250-0493	877-250-0493	855-250-0493	866-250-0493
PT-1 Communications	800-250-0040	888-250-0040	877-250-0040	855-250-0040	866-250-0040
PT-1 Communications	800-250-0041	888-250-0041	877-250-0041	855-250-0041	866-250-0041
Puerto Rico Telephone Co.	800-250-0180	888-250-0180	877-250-0180	855-250-0180	866-250-0180
Puerto Rico Telephone Co.	800-250-0181	888-250-0181	877-250-0181	855-250-0181	866-250-0181
Quebec Telephone	800-250-0441	888-250-0441	877-250-0441	855-250-0441	866-250-0441
Quebec Telephone	800-250-0442	888-250-0442	877-250-0442	855-250-0442	866-250-0442

Questar InfoComm Inc.	800-250-0036	888-250-0036	877-250-0036	855-250-0036	866-250-0036
Questar InfoComm Inc.	800-250-0037	888-250-0037	877-250-0037	855-250-0037	866-250-0037
Qwest/LCI International	800-250-0166	888-250-0166	877-250-0166	855-250-0182	866-250-0182
Qwest/LCI International	800-250-0167	888-250-0167	877-250-0167	855-250-0183	866-250-0183
Qwest/LCI International	800-250-0182	888-250-0182	877-250-0182		
Qwest/LCI International	800-250-0183	888-250-0183	877-250-0183		
Qwest/LCI International	800-250-0344	888-250-0344	877-250-0344		
Qwest/LCI International	800-250-0348	888-250-0348	877-250-0348		
RCC Atlantic	800-250-0134	888-250-0134	877-250-0134	855-250-0134	866-250-0134
RCC Atlantic	800-250-0135	888-250-0135	877-250-0135	855-250-0135	866-250-0135
RCC Network Inc.	800-250-0056	888-250-0056	877-250-0056	855-250-0056	866-250-0056
RCC Network Inc.	800-250-0057	888-250-0057	877-250-0057	855-250-0057	866-250-0057
Regal Results Inc.	800-250-0120	888-250-0120	877-250-0120	855-250-0120	866-250-0120
Regal Results Inc.	800-250-0373	888-250-0373	877-250-0373	855-250-0373	866-250-0373
RSL/Westinghouse Communications	800-250-0271	888-250-0271	877-250-0271	877-250-0271	866-250-0271
RSL/Westinghouse Communications	800-250-0272	888-250-0272	877-250-0272	855-250-0272	866-250-0272
Scherers Communications Group Inc.	800-250-0184	888-250-0184	877-250-0184	855-250-0184	866-250-0184
Scherers Communications Group Inc.	800-250-0185	888-250-0185	877-250-0185	855-250-0185	866-250-0185
Selective Media	800-250-0075	888-250-0075	877-250-0075	855-250-0075	866-250-0075
Selective Media	800-250-0076	888-250-0076	877-250-0076	855-250-0076	866-250-0076
Signal One Inc.	800-250-0431	888-250-0431	877-250-0431	855-250-0431	866-250-0431
Signal One Inc.	800-250-0432	888-250-0432	877-250-0432	855-250-0432	866-250-0432
Siouxland Telephone Co. STC/MTI	800-250-0154	888-250-0154	877-250-0154	855-250-0154	866-250-0154
Siouxland Telephone Co. STC/MTI	800-250-0216	888-250-0216	877-250-0216	855-250-0216	866-250-0216
Sol Friedman Communications	800-250-0875	888-250-0875	877-250-0875	855-250-0875	866-250-0875
Sol Friedman Communications	800-250-0876	888-250-0876	877-250-0876	855-250-0876	866-250-0876
Southern New England Telephone	800-250-0186	888-250-0186	877-250-0186	855-250-0186	866-250-0186
Southern New England Telephone	800-250-0187	888-250-0187	877-250-0187	855-250-0187	866-250-0187
Southern States Telephone Inc.	800-250-0884	888-250-0884	877-250-0884	855-250-0884	866-250-0884
Southern States Telephone Inc.	800-250-0885	888-250-0885	877-250-0885	855-250-0885	866-250-0885
Southwestern Bell Corp.	800-250-0002	888-250-0002	877-250-0002	855-250-0002	866-250-0002
Southwestern Bell Corp.	800-250-0004	888-250-0004	877-250-0004	855-250-0004	866-250-0004
Sprint Communications Co. L.D.D.	800-250-0110	888-250-0110	877-250-0110	855-250-0110	866-250-0110

Sprint Communications Co. L.D.D..	800-250-0111	888-250-0111	877-250-0111	855-250-0111	866-250-0111
Starlink Communications	800-250-0213	888-250-0213	877-250-0213	855-250-0213	866-250-0213
Starlink Communications	800-250-0215	888-250-0215	877-250-0215	855-250-0215	866-250-0215
Startel	800-250-0101	888-250-0101	877-250-0101	855-250-0101	866-250-0101
Startel	800-250-0102	888-250-0102	877-250-0102	855-250-0102	866-250-0102
State Farm Insurance Companies	800-250-0048	888-250-0048	877-250-0048	855-250-0048	866-250-0048
State Farm Insurance Companies	800-250-0049	888-250-0049	877-250-0049	855-250-0049	866-250-0049
Stentor	800-250-0103	888-250-0103	877-250-0103	855-250-0103	866-250-0103
Stentor	800-250-0104	888-250-0104	877-250-0104	855-250-0104	866-250-0104
Suntel	800-250-0105	888-250-0105	877-250-0105	855-250-0105	866-250-0105
Suntel	800-250-0106	888-250-0106	877-250-0106	855-250-0106	866-250-0106
Switch 2000 LLC	800-250-0107	888-250-0107	877-250-0107	855-250-0107	866-250-0107
Switch 2000 LLC	800-250-0108	888-250-0108	877-250-0108	855-250-0108	866-250-0108
Switch Services Inc.	800-250-0299	888-250-0299	877-250-0299	855-250-0299	866-250-0299
Switch Services Inc.	800-250-0307	888-250-0307	877-250-0307	855-250-0307	866-250-0307
T.A.P.S.	800-250-0449	888-250-0449	877-250-0449	855-250-0449	866-250-0449
T.A.P.S.	800-250-0450	888-250-0450	877-250-0450	855-250-0450	866-250-0450
TelAmerica Long Distance	800-250-0255	888-250-0255	877-250-0255	855-250-0255	866-250-0255
TelAmerica Long Distance	800-250-0256	888-250-0256	877-250-0256	855-250-0256	866-250-0256
Tele Corp.	800-250-0427	888-250-0427	877-250-0427	855-250-0427	866-250-0427
Tele Corp.	800-250-0428	888-250-0428	877-250-0428	855-250-0428	866-250-0428
Telecall Long Distance	800-250-0406	888-250-0406	877-250-0406	855-250-0406	866-250-0406
Telecall Long Distance	800-250-0434	888-250-0434	877-250-0434	855-250-0434	866-250-0434
Telecom Affiliates Inc.	800-250-0220	888-250-0220	877-250-0220	855-250-0220	866-250-0220
Telecom Affiliates Inc.	800-250-0407	888-250-0407	877-250-0407	855-250-0407	866-250-0407
Telefonica Larga Distancia	800-250-0221	888-250-0221	877-250-0221	855-250-0221	866-250-0221
Telefonica Larga Distancia	800-250-0222	888-250-0222	877-250-0222	855-250-0222	866-250-0222
Teleglobe Business Solutions	800-250-0083	888-250-0083	877-250-0083	855-250-0083	866-250-0083
Teleglobe Business Solutions	800-250-0084	888-250-0084	877-250-0084	855-250-0084	866-250-0084
Teleglobe International Corp.	800-250-0451	888-250-0451	877-250-0451	855-250-0451	866-250-0451
Teleglobe International Corp.	800-250-0452	888-250-0452	877-250-0452	855-250-0452	866-250-0452
Telepacific Communications	800-250-0859	888-250-0859	877-250-0859	855-250-0859	866-250-0860
Telepacific Communications	800-250-0860	888-250-0860	877-250-0860	855-250-0860	866-250-0860

Telephone Express	800-250-0223	888-250-0223	877-250-0223	85-525-0223	866-250-0223
Telephone Express	800-250-0225	888-250-0225	877-250-0225	855-250-0225	866-250-0225
Telephone Service Bureau LLC	800-250-0032	888-250-0032	877-250-0032	855-250-0032	866-250-0032
Telephone Service Bureau LLC	800-250-0033	888-250-0033	877-250-0033	855-250-0033	866-250-0033
TeleQuest	800-250-0081	888-250-0081	877-250-0081	855-250-0081	866-250-0081
TeleQuest	800-250-0082	888-250-0082	877-250-0082	855-250-0082	866-250-0082
Telera	800-250-0863	888-250-0863	877-250-0863	855-250-0863	866-250-0863
Telera	800-250-0864	888-250-0864	877-250-0864	855-250-0864	866-250-0864
Telescan Inc.	800-250-0283	888-250-0283	877-250-0283	855-250-0283	866-250-0283
Telescan Inc.	800-250-0296	888-250-0296	877-250-0296	855-250-0296	866-250-0296
TeleServices Inc.	800-250-0226	888-250-0226	877-250-0226	855-250-0226	866-250-0226
TeleServices Inc.	800-250-0227	888-250-0227	877-250-0227	855-250-0227	866-250-0227
Telstar Communications	800-250-0077	888-250-0077	877-250-0077	855-250-0077	866-250-0077
Telstar Communications	800-250-0078	888-250-0078	877-250-0078	855-250-0078	866-250-0078
Telvue Corporation	800-250-0231	888-250-0231	877-250-0231	855-250-0231	866-250-0231
Telvue Corporation	800-250-0232	888-250-0232	877-250-0232	855-250-0232	866-250-0232
TGC Teleport Communications Group	800-250-0073	888-250-0073	877-250-0073	855-250-0073	866-250-0073
TGC Teleport Communications Group	800-250-0074	888-250-0074	877-250-0074	855-250-0074	866-250-0074
TH Inc.	800-250-0913	888-250-0913	877-250-0913	855-250-0913	866-250-0913
TH Inc.	800-250-0914	888-250-0914	877-250-0914	855-250-0914	866-250-0914
The Business Edge Group	800-250-0038	888-250-0038	877-250-0038	855-250-0038	866-250-0038
The Business Edge Group	800-250-0039	888-250-0039	877-250-0039	855-250-0039	866-250-0039
The Phone Company	800-250-0212	888-250-0212	877-250-0212	855-250-0212	866-250-0212
The Phone Company	800-250-0218	888-250-0218	877-250-0218	855-250-0218	866-250-0218
Toll-Less.com	800-250-1030	888-250-1030	877-250-1030	855-250-1030	866-250-1030
Toll-Less.com	800-250-1031	888-250-1031	877-250-1031	855-250-1031	866-250-1031
Total Axxess.Com Inc.	800-250-0457	888-250-0457	877-250-0457	855-250-0457	866-250-0457
Total Axxess.Com Inc.	800-250-0458	888-250-0458	877-250-0458	855-250-0458	866-250-0458
Total-Tel USA	800-250-0233	888-250-0233	877-250-0233	855-250-0233	866-250-0233
Total-Tel USA	800-250-0234	888-250-0234	877-250-0234	855-250-0234	866-250-0234
Touch America	800-250-0238	888-250-0238	877-250-0238	855-250-0238	866-250-0238
Touch America	800-250-0239	888-250-0239	877-250-0239	855-250-0239	866-250-0239
Transaction Network Services	800-250-0459	888-250-0459	877-250-0459	855-250-0459	866-250-0459

Transaction Network Services	800-250-0461	888-250-0461	877-250-0461	855-250-0461	866-250-0461
Transtel Communications	800-250-0235	888-250-0235	877-250-0235	855-250-0235	866-250-0235
Transtel Communications	800-250-0237	888-250-0237	877-250-0237	855-250-0237	866-250-0237
TSR Wireless LLC	800-250-0896	888-250-0896	877-250-0896	855-250-0896	866-250-0896
TSR Wireless LLC	800-250-0897	888-250-0897	877-250-0897	855-250-0897	866-250-0897
TTE of Charleston	800-250-0193	888-250-0193	877-250-0193	855-250-0193	866-250-0193
TTE of Charleston	800-250-0194	888-250-0194	877-250-0194	855-250-0194	866-250-0194
Twister Communications	800-250-0305	888-250-0305	877-250-0305	855-250-0305	866-250-0305
Twister Communications	800-250-0306	888-250-0306	877-250-0306	855-250-0306	866-250-0306
UniDial Communications	800-250-0065	888-250-0065	877-250-0065	855-250-0065	866-250-0065
UniDial Communications	800-250-0066	888-250-0066	877-250-0066	855-250-0066	866-250-0066
Union Telephone Company	800-250-0251	888-250-0251	877-250-0251	855-250-0251	866-250-0251
Union Telephone Company	800-250-0252	888-250-0252	877-250-0252	855-250-0252	866-250-0252
US LEC	800-250-0435	888-250-0435	877-250-0435	855-250-0435	866-250-0435
US LEC	800-250-0436	888-250-0436	877-250-0436	855-250-0436	866-250-0436
US Link Long Distance	800-250-0242	888-250-0242	877-250-0242	855-250-0242	866-250-0242
US Link Long Distance	800-250-0243	888-250-0243	877-250-0243	855-250-0243	866-250-0243
US Wats	800-250-0247	888-250-0247	877-250-0247	855-250-0247	866-250-0247
US Wats	800-250-0248	888-250-0248	877-250-0248	855-250-0248	866-250-0248
US West	800-250-0249	888-250-0249	877-250-0249	855-250-0249	866-250-0249
US West	800-250-0250	888-250-0250	877-250-0250	855-250-0250	866-250-0250
US West Long Distance	800-250-0488	888-250-0488	877-250-0488	855-250-0488	866-250-0487
US West Long Distance	800-250-0489	888-250-0489	877-250-0489	855-250-0489	866-250-0489
USC Telecom	800-250-0188	888-250-0188	877-250-0188	855-250-0188	866-250-0188
USC Telecom	800-250-0189	888-250-0189	877-250-0189	855-250-0189	866-250-0189
USC Telecom	800-250-0210	888-250-0210	877-250-0210	855-250-0210	866-250-0210
USC Telecom	800-250-0211	888-250-0211	877-250-0211	855-250-0211	866-250-0211
USXChange	800-250-0423	888-250-0423	877-250-0423	855-250-0423	866-250-0423
USXChange	800-250-0424	888-250-0424	877-250-0424	855-250-0424	866-250-0424
Valu-Line of Longview	800-250-0480	888-250-0480	877-250-0480	855-250-0480	866-250-0480
Valu-Line of Longview	800-250-0481	888-250-0481	877-250-0481	855-250-0481	866-250-0481
Vanity International	800-250-0478	888-250-0478	877-250-0478	855-250-0478	866-250-0478
Vanity International	800-250-0479	888-250-0479	877-250-0479	855-250-0479	866-250-0479

VarTec Telecom Inc.	800-250-0257	888-250-0257	877-250-0257	855-250-0257	866-250-0257
VarTec Telecom Inc.	800-250-0258	888-250-0258	877-250-0258	855-250-0258	866-250-0258
VD Corporation	800-250-0915	888-250-0915	877-250-0915	855-250-0915	866-250-0915
VD Corporation	800-250-0916	888-250-0916	877-250-0916	855-250-0916	855-250-0916
VoCall Communications Corp.	800-250-0476	888-250-0476	877-250-0476	855-250-0476	866-250-0476
VoCall Communications Corp.	800-250-0477	888-250-0477	877-250-0477	855-250-0477	866-250-0477
W.E.P.S. Inc.	800-250-0178	888-250-0178	877-250-0178	855-250-0178	866-250-0178
W.E.P.S. Inc.	800-250-0179	888-250-0179	877-250-0179	855-250-0179	866-250-0179
Wake Up Inc.	800-250-0462	888-250-0462	877-250-0462	855-250-0462	866-250-0462
Wake Up Inc.	800-250-0463	888-250-0463	877-250-0463	855-250-0463	866-250-0463
Warning Communications Inc.	800-250-0408	888-250-0408	877-250-0408	855-250-0408	866-250-0408
Warning Communications Inc.	800-250-0409	888-250-0409	877-250-0409	855-250-0409	866-250-0409
WesTel Inc.	800-250-0265	888-250-0265	877-250-0265	855-250-0265	866-250-0265
WesTel Inc.	800-250-0388	888-250-0388	877-250-0388	855-250-0388	866-250-0388
Williams Communications	800-250-0867	888-250-0867	877-250-0867	855-250-0867	866-250-0867
Williams Communications	800-250-0868	888-250-0868	877-250-0868	855-250-0868	866-250-0868
Winstar Telecommunications Inc.	800-250-0141	888-250-0141	877-250-0141	855-250-0141	866-250-0141
Winstar Telecommunications Inc.	800-250-0385	888-250-0385	877-250-0385	855-250-0385	866-250-0385
Word of Mouth Communications	800-250-0486	888-250-0486	877-250-0486	855-250-0486	866-250-0486
Word of Mouth Communications	800-250-0487	888-250-0487	877-250-0487	855-250-0487	866-250-0487
World Access Inc.	800-250-0319	888-250-0319	877-250-0319	855-250-0319	866-250-0319
World Access Inc.	800-250-0320	888-250-0320	877-250-0320	855-250-0320	866-250-0320
World Wide Telegraph	800-250-0019	888-250-0019	877-250-0019	855-250-0019	866-250-0019
World Wide Telegraph	800-250-0020	888-250-0020	877-250-0020	855-250-0020	866-250-0020
Worldcom	800-250-0069	888-250-0069	877-250-0069	855-250-0069	866-250-0069
Worldcom	800-250-0070	888-250-0070	877-250-0070	855-250-0070	866-250-0070
Xtel Communications	800-250-0050	888-250-0050	877-250-0050	855-250-0050	866-250-0050
Xtel Communications	800-250-0051	888-250-0051	877-250-0051	855-250-0051	866-250-0051
Z-Tel Network Services	800-250-0856	888-250-0856	877-250-0856	855-250-0856	866-250-0856
Z-Tel Network Services	800-250-0857	888-250-0857	877-250-0857	855-250-0857	866-250-0857

6 APPENDIX C – TROUBLE REFERRAL NUMBERS

6.1 Sorted by Resp Org ID

Resp Org Name	Resp Org ID	Trouble Referral Number
ALASCOM INC.	AAM01	(907) 264-8363
ALASCOM INC.	AAM99	(907) 264-8363
ABCO COMMUNICATIONS INC.	ABC01	(707) 887-7994
ABCO COMMUNICATIONS INC.	ABC99	(800) 275-2226
MCLEOD USA/ACCESS LD	ACC02	(800) 593-1177
MCLEOD USA ACCESS LONG DIST	ACC04	(888) 737-8335
MCLEOD USA/ACCESS LD	ACC99	(801) 238-2275
LOGIX COMMUNICATIONS	AET01	(800) 444-0258
LOGIX COMMUNICATIONS	AET99	(800) 444-0258
GLOBAL CROSSING	ALE01	(800) 466-4646
GLOBAL CROSSING	ALE99	(800) 466-4646
GLOBAL CROSSING	ALF01	(800) 783-2020
GLOBAL CROSSING	ALF99	(800) 783-2020
GLOBAL CROSSING	ALN01	(800) 466-4600
GLOBAL CROSSING	ALN03	(800) 783-2020
GLOBAL CROSSING	ALN99	(800) 783-2020
#EMPTY	AMLBA	(800) 956-7000
AMERITECH SERVICES	AMLBT	(800) 956-7000
AMERITECH SERVICES	AMLB1	(800) 956-7000
AMERITECH SERVICES	AMLD1	(800) 956-7000
AMERITECH SERVICES	AMMBA	(800) 956-7000
AMERITECH SERVICES	AMMB1	(800) 956-7000
AMERITECH SERVICES	AMNBA	(800) 956-7000
AMERITECH SERVICES	AMNB1	(800) 956-7000
AMERITECH SERVICES	AMNS2	(800) 956-7000
AMERITECH SERVICES	AMOBA	(800) 956-7000
AMERITECH SERVICES	AMOBT	#EMPTY
AMERITECH SERVICES	AMOB1	(800) 956-7000

AMERITECH SERVICES	AMSE1	(800) 956-7000
AMERITECH SERVICES	AMSM1	(800) 956-7000
AMERITECH SERVICES	AMT01	(800) 956-7000
AMERITECH SERVICES	AMWT1	(800) 956-7000
AMRIGON INC.	AON01	(248) 332-2300
AMRIGON INC.	AON99	(248) 332-2300
AMERVISION COMM., INC.	APV01	(405) 600-3605
AMERVISION COMM., INC.	APV99	(405) 600-3605
(RCC) ATLANTIC	AQC99	(802) 654-5083
ADVANCED ROUTING TECH.	ART01	(732) 356-6999
CSF CORPORATION	ART02	(732) 356-6999
CSF CORPORATION	ART03	(732) 356-6999
#EMPTY	ART04	(732) 356-6999
ADVANCED ROUTING TECHNOLOGIES	ART05	(732) 356-6999
CSF CORPORATION	ART06	(732) 356-6999
CSF CORPORATION	ART07	(732) 356-6999
CSF CORPORATION	ART08	(732) 356-6999
CSF CORPORATION	ART09	(732) 356-6999
CSF CORPORATION	ART10	(732) 356-6999
CSF CORPORATION	ART11	(732) 356-6999
CSF CORPORATION	ART12	(732) 356-6999
CSF CORPORATION	ART13	(732) 356-6999
CSF CORPORATION	ART14	(732) 356-6999
CSF CORPORATION	ART15	(732) 356-6999
CSF CORPORATION	ART16	(732) 356-6999
CSF CORPORATION	ART17	(732) 356-6999
CSF CORPORATION	ART18	(732) 356-6999
CSF CORPORATION	ART19	(732) 356-6999
CSF CORPORATION	ART20	(732) 356-6999
CSF CORPORATION	ART21	(732) 356-6999
CSF CORPORATION	ART22	(732) 356-6999
CSF CORPORATION	ART23	(732) 356-6999
CSF CORPORATION	ART24	(732) 356-6999

CSF CORPORATION	ART25	(732) 356-6999
CSF CORPORATION	ART26	(732) 356-6999
CSF CORPORATION	ART27	(732) 356-6999
CSF CORPORATION	ART28	(732) 356-6999
CSF CORPORATION	ART29	(732) 356-6999
CSF CORPORATION	ART30	(732) 356-6999
CSF CORPORATION	ART34	(732) 356-6999
CSF CORPORATION	ART35	(732) 356-6999
ADVANCED ROUTING TECH.	ART99	(732) 356-6999
AMERICAN LONG LINES	ASL01	(215) 442-9700
AMERICAN LONG LINES	ASL99	(215) 442-9700
AT&T	ATX01	(800) 222-3000
AT&T	ATX02	(800) 435-7375
AT&T	ATX03	(800) 248-1905
AT&T	ATX04	(800) 248-1903
AT&T	ATX06	(800) 222-3000
AT&T	ATX07	(800) 222-3000
AT&T	ATX09	(800) 222-3000
AT&T	ATX30	(800) 222-3000
AT&T	ATX40	(800) 222-3000
AT&T	ATX99	(800) 222-3000
ATL COMMUNICATIONS	AUA01	(800) 508-5200
ATL COMMUNICATIONS	AUA02	(800) 508-5200
ATL COMMUNICATIONS	AUA03	(800) 508-5200
ATL COMMUNICATIONS	AUA04	(800) 508-5200
ATL COMMUNICATIONS	AUA05	(800) 508-5200
ATL COMMUNICATIONS	AUA06	(800) 508-5200
ATL COMMUNICATIONS	AUA07	(800) 508-5200
ATL COMMUNICATIONS	AUA08	(800) 508-5200
ATL COMMUNICATIONS	AUA09	(800) 508-5200
ATL COMMUNICATIONS	AUA10	(800) 508-5200
ATL COMMUNICATIONS	AUA11	(800) 508-5200
ATL COMMUNICATIONS	AUA12	(800) 508-5200

ATL COMMUNICATIONS	AUA13	(800) 508-5200
ATL COMMUNICATIONS	AUA14	(800) 508-5200
ATL COMMUNICATIONS	AUA15	(800) 508-5200
ATL COMMUNICATIONS	AUA16	(800) 508-5200
ATL COMMUNICATIONS	AUA17	(800) 508-5200
ATL COMMUNICATIONS	AUA18	(800) 508-5200
ATL COMMUNICATIONS	AUA19	(800) 508-5200
ATL COMMUNICATIONS	AUA20	(800) 508-5200
ATL COMMUNICATIONS	AUA21	(800) 508-5200
ATL COMMUNICATIONS	AUA22	(800) 508-5200
ATL COMMUNICATIONS	AUA23	(800) 508-5200
ATL COMMUNICATIONS	AUA24	(800) 508-5200
ATL COMMUNICATIONS	AUA25	(800) 508-5200
ATL COMMUNICATIONS	AUA26	(800) 508-5200
ATL COMMUNICATIONS	AUA27	(800) 508-5200
ATL COMMUNICATIONS	AUA28	(800) 508-5200
ATL COMMUNICATIONS	AUA29	(800) 508-5200
ATL COMMUNICATIONS	AUA30	(800) 508-5200
ATL COMMUNICATIONS	AUA31	(800) 508-5200
ATL COMMUNICATIONS	AUA32	(800) 508-5200
ATL COMMUNICATIONS	AUA33	(800) 508-5200
ATL COMMUNICATIONS	AUA34	(800) 508-5200
ATL COMMUNICATIONS	AUA35	(800) 508-5200
ATL COMMUNICATIONS	AUA36	(800) 508-5200
ATL COMMUNICATIONS	AUA37	(800) 508-5200
ATL COMMUNICATIONS	AUA38	(800) 508-5200
ATL COMMUNICATIONS	AUA39	(800) 508-5200
ATL COMMUNICATIONS	AUA40	(800) 508-5200
ATL COMMUNICATIONS	AUA41	(800) 508-5200
ATL COMMUNICATIONS	AUA42	(800) 508-5200
ATL COMMUNICATIONS	AUA43	(800) 508-5200
ATL COMMUNICATIONS	AUA44	(800) 508-5200
ATL COMMUNICATIONS	AUA45	(800) 508-5200

ATL COMMUNICATIONS	AUA46	(800) 508-5200
ATL COMMUNICATIONS	AUA47	(800) 508-5200
ATL COMMUNICATIONS	AUA48	(800) 508-5200
ATL COMMUNICATIONS	AUA49	(800) 508-5200
ATL COMMUNICATIONS	AUA50	(800) 508-5200
ATL COMMUNICATIONS	AUA51	(800) 805-5200
ATL COMMUNICATIONS	AUA52	(800) 805-5200
ATL COMMUNICATIONS	AUA53	(800) 805-5200
ATL COMMUNICATIONS	AUA54	(800) 805-5200
ATL COMMUNICATIONS	AUA55	(800) 805-5200
ATL COMMUNICATIONS	AUA56	(800) 805-5200
ATL COMMUNICATIONS	AUA57	(800) 805-5200
ATL COMMUNICATIONS	AUA58	(800) 805-5200
ATL COMMUNICATIONS	AUA59	(800) 805-5200
ATL COMMUNICATIONS	AUA60	(800) 508-5200
ATL COMMUNICATIONS	AUA61	(800) 508-5200
ATL COMMUNICATIONS	AUA62	(800) 508-5200
ATL COMMUNICATIONS	AUA63	(800) 508-5200
ATL COMMUNICATIONS	AUA64	(800) 508-5200
ATL COMMUNICATIONS	AUA65	(800) 508-5200
ATL COMMUNICATIONS	AUA66	(800) 508-5200
ATL COMMUNICATIONS	AUA67	(800) 508-5200
ATL COMMUNICATIONS	AUA68	(800) 508-5200
ATL COMMUNICATIONS	AUA69	(800) 508-5200
ATL COMMUNICATIONS	AUA70	(800) 805-5200
ATL COMMUNICATIONS	AUA71	(800) 805-5200
ATL COMMUNICATIONS	AUA72	(800) 805-5200
ATL COMMUNICATIONS	AUA73	(800) 805-5200
ATL COMMUNICATIONS	AUA74	(800) 805-5200
ATL COMMUNICATIONS	AUA75	(800) 805-5200
ATL COMMUNICATIONS	AUA76	(800) 805-5200
ATL COMMUNICATIONS	AUA77	(800) 805-5200
ATL COMMUNICATIONS	AUA78	(800) 805-5200

ATL COMMUNICATIONS	AUA79	(800) 805-5200
ATL COMMUNICATIONS	AUA80	(800) 805-5200
ATL COMMUNICATIONS	AUA81	(800) 805-5200
ATL COMMUNICATIONS	AUA82	(800) 805-5200
ATL COMMUNICATIONS	AUA83	(800) 805-5200
ATL COMMUNICATIONS	AUA84	(800) 805-5200
ATL COMMUNICATIONS	AUA85	(800) 805-5200
ATL COMMUNICATIONS	AUA86	(800) 805-5200
ATL COMMUNICATIONS	AUA87	(800) 805-5200
ATL COMMUNICATIONS	AUA88	(800) 805-5200
ATL COMMUNICATIONS	AUA89	(800) 805-5200
ATL COMMUNICATIONS	AUA90	(800) 508-5200
ATL COMMUNICATIONS	AUA91	(800) 508-5200
ATL COMMUNICATIONS	AUA92	(800) 508-5200
ATL COMMUNICATIONS	AUA93	(800) 508-5200
ATL COMMUNICATIONS	AUA94	(800) 508-5200
ATL COMMUNICATIONS	AUA95	(800) 508-5200
ATL COMMUNICATIONS	AUA96	(800) 508-5200
ATL COMMUNICATIONS	AUA97	(800) 508-5200
ATL COMMUNICATIONS	AUA98	(800) 508-5200
ATL COMMUNICATIONS	AUA99	(800) 508-5200
ATL COMMUNICATIONS	AUB01	(800) 508-5200
ATL COMMUNICATIONS	AUB02	(800) 508-5200
ATL COMMUNICATIONS	AUB03	(800) 508-5200
ATL COMMUNICATIONS	AUB04	(800) 508-5200
AT; COMMUNICATIONS	AUB05	(800) 508-5200
ATL COMMUNICATIONS	AUB06	(800) 508-5200
ATL COMMUNICATIONS	AUB07	(800) 508-5200
ATL COMMUNICATIONS	AUB08	(800) 508-5200
ATL COMMUNICATIONS	AUB09	(800) 508-5200
ATL COMMUNICATIONS	AUB10	(800) 508-5200
ATL COMMUNICATIONS	AUB11	(800) 508-5200
ATL COMMUNICATIONS	AUB12	(800) 508-5200

ATL COMMUNICATIONS	AUB13	(800) 508-5200
ATL COMMUNICATIONS	AUB14	(800) 508-5200
ATL COMMUNICATIONS	AUB15	(800) 508-5200
ATL COMMUNICATIONS	AUB16	(800) 508-5200
ATL COMMUNICATIONS	AUB17	(800) 508-5200
ATL COMMUNICATIONS	AUB18	(800) 508-5200
ATL COMMUNICATIONS	AUB19	(800) 508-5200
ATL COMMUNICATIONS	AUB20	(800) 508-5200
ATL COMMUNICATIONS	AUB21	(800) 508-5200
ATL COMMUNICATIONS	AUB22	(800) 508-5200
ATL COMMUNICATIONS	AUB23	(800) 508-5200
ATL COMMUNICATIONS	AUB24	(800) 508-5200
ATL COMMUNICATIONS	AUB25	(800) 508-5200
ATL COMMUNICATIONS	AUB26	(800) 508-5200
ATL COMMUNICATIONS	AUB27	(800) 508-5200
ATL COMMUNICATIONS	AUB28	(800) 508-5200
ATL COMMUNICATIONS	AUB29	(800) 508-5200
ATL COMMUNICATIONS	AUN01	(800) 508-5200
ATL COMMUNICATIONS	AUN02	(800) 508-5200
ATL COMMUNICATIONS	AUN03	(800) 508-5200
ATL COMMUNICATIONS	AUN04	(800) 508-5200
ATL COMMUNICATIONS	AUN05	(800) 508-5200
ATL COMMUNICATIONS	AUN06	(800) 508-5200
ATL COMMUNICATIONS	AUN07	(800) 508-5200
ATL COMMUNICATIONS	AUN08	(800) 508-5200
ATL COMMUNICATIONS	AUN09	(800) 508-5200
ATL COMMUNICATIONS	AUN10	(800) 508-5200
ATL COMMUNICATIONS	AUN11	(800) 508-5200
ATL COMMUNICATIONS	AUN12	(800) 508-5200
ATL COMMUNICATIONS	AUN13	(800) 508-5200
ATL COMMUNICATIONS	AUN14	(800) 508-5200
ATL COMMUNICATIONS	AUN15	(800) 508-5200
ATL COMMUNICATIONS	AUN16	(805) 690-4198

ATL COMMUNICATIONS	AUN17	(800) 508-5200
ATL COMMUNICATIONS	AUN18	(800) 508-5200
ATL COMMUNICATIONS	AUN19	(800) 508-5200
ATL COMMUNICATIONS	AUN20	(800) 508-5200
ATL COMMUNICATIONS	AUN21	(800) 508-5200
ATL COMMUNICATIONS	AUN22	(800) 508-5200
ATL COMMUNICATIONS	AUN23	(800) 508-5200
ATL COMMUNICATIONS	AUN24	(800) 508-5200
ATL COMMUNICATIONS	AUN25	(800) 508-5200
ATL COMMUNICATIONS	AUN26	(800) 508-5200
ATL COMMUNICATIONS	AUN27	(800) 508-5200
ATL COMMUNICATIONS	AUN28	(800) 508-5200
ATL COMMUNICATIONS	AUN29	(800) 508-5200
ATL COMMUNICATIONS	AUN30	(800) 508-5200
ATL COMMUNICATIONS	AUN31	(800) 508-5200
ATL COMMUNICATIONS	AUN32	(800) 508-5200
ATL COMMUNICATIONS	AUN33	(800) 508-5200
ATL COMMUNICATIONS	AUN34	(800) 508-5200
ATL COMMUNICATIONS	AUN35	(800) 508-5200
ATL COMMUNICATIONS	AUN36	(800) 508-5200
ATL COMMUNICATIONS	AUN37	(800) 508-5200
ATL COMMUNICATIONS	AUN38	(800) 508-5200
ATL COMMUNICATIONS	AUN39	(800) 508-5200
ATL COMMUNICATIONS	AUN40	(800) 508-5200
ATL COMMUNICATIONS	AUN41	(800) 508-5200
ATL COMMUNICATIONS	AUN42	(800) 508-5200
ATL COMMUNICATIONS	AUN43	(800) 508-5200
ATL COMMUNICATIONS	AUN44	(800) 508-5200
ATL COMMUNICATIONS	AUN45	(800) 508-5200
ATL COMMUNICATIONS	AUN46	(800) 508-5200
ATL COMMUNICATIONS	AUN47	(800) 508-5200
ATL COMMUNICATIONS	AUN48	(800) 508-5200
ATL COMMUNICATIONS	AUN49	(800) 508-5200

ATL COMMUNICATIONS	AUN50	(800) 508-5200
ATL COMMUNICATIONS	AUN51	(800) 508-5200
ATL COMMUNICATIONS	AUN52	(800) 508-5200
ATL COMMUNICATIONS	AUN53	(800) 508-5200
ATL COMMUNICATIONS	AUN54	(800) 508-5200
ATL COMMUNICATIONS	AUN55	(800) 508-5200
ATL COMMUNICATIONS	AUN56	(800) 508-5200
ATL COMMUNICATIONS	AUN57	(800) 508-5200
ATL COMMUNICATIONS	AUN58	(800) 508-5200
ATL COMMUNICATIONS	AUN59	(800) 508-5200
ATL COMMUNICATIONS	AUN60	(800) 508-5200
ATL COMMUNICATIONS	AUN61	(800) 508-5200
ATL COMMUNICATIONS	AUN62	(800) 508-5200
ATL COMMUNICATIONS	AUN63	(800) 508-5200
ATL COMMUNICATIONS	AUN64	(800) 508-5200
ATL COMMUNICATIONS	AUN65	(800) 508-5200
ATL COMMUNICATIONS	AUN66	(800) 508-5200
ATL COMMUNICATIONS	AUN67	(800) 508-5200
ATL COMMUNICATIONS	AUN68	(800) 508-5200
ATL COMMUNICATIONS	AUN69	(800) 508-5200
ATL COMMUNICATIONS	AUN70	(800) 508-5200
ATL COMMUNICATIONS	AUN71	(800) 508-5200
ATL COMMUNICATIONS	AUN72	(800) 508-5200
ATL COMMUNICATIONS	AUN73	(800) 508-5200
ATL COMMUNICATIONS	AUN74	(800) 508-5200
ATL COMMUNICATIONS	AUN75	(800) 508-5200
ATL COMMUNICATIONS	AUN76	(800) 508-5200
ATL COMMUNICATIONS	AUN77	(800) 508-5200
ATL COMMUNICATIONS	AUN78	(800) 508-5200
ATL COMMUNICATIONS	AUN79	(800) 508-5200
ATL COMMUNICATIONS	AUN80	(800) 508-5200
ATL TELECOM SERVICES	AUN81	(800) 508-5200
ATL TELECOM SERVICES	AUN82	(800) 508-5200

ATL TELECOM SERVICES	AUN83	(800) 508-5200
ATL TELECOM SERVICES	AUN84	(800) 508-5200
ATL TELECOM SERVICES	AUN85	(800) 508-5200
ATL TELECOM SERVICES	AUN86	(800) 508-5200
ATL TELECOM SERVICES	AUN87	(800) 508-5200
ATL TELECOM SERVICES	AUN88	(800) 508-5200
ATL TELECOM SERVICES	AUN89	(800) 508-5200
ATL TELECOM SERVICES	AUN90	(800) 508-5200
ATL TELECOM SERVICES	AUN91	(800) 508-5200
ATL TELECOM SERVICES	AUN92	(800) 502-5200
ATL TELECOM SERVICES	AUN93	(800) 508-5200
ATL TELECOM SERVICES	AUN94	(800) 508-5200
ATL TELECOM SERVICES	AUN95	(800) 508-5200
ATL TELECOM SERVICES	AUN96	(800) 508-5200
ATL TELECOM SERVICES	AUN97	(800) 508-5200
ATL TELECOM SERVICES	AUN98	(800) 508-5200
ATL COMMUNICATIONS	AUN99	(800) 508-5200
AT&T LONG DISTANCE	AWCC1	(877) 973-7767
AT&T LONG DISTANCE	AWCC2	(877) 973-7767
AT&T LONG DISTANCE	AWCC3	(877) 973-7767
AT&T LONG DISTANCE	AWCC4	(877) 973-7767
AT&T LONG DISTANCE	AWCC5	(877) 973-7767
AT&T LONG DISTANCE	AWC01	(877) 973-7767
AT&T LONG DISTANCE	AWC99	(877) 973-7767
AT&T LONG DISTANCE	AWLD1	(877) 973-7767
AT&T LONG DISTANCE	AWMM1	(877) 973-7767
AT&T LONG DISTANCE	AWREG	(877) 973-7767
ALLSTATE COMMUNICATIONS	AYL01	(818) 598-1570
ALLSTATE COMMUNICATIONS	AYL99	(818) 598-1570
ALLSTREAM	AZC01	(866) 282-0111
ALLSTREAM	AZC99	(866) 282-0111
BELL ATLANTIC SOUTH	BANX1	(212) 338-7666
TOLL-LESS.COM	BBT01	(203) 341-0372

TOLL-LESS.COM	BBT99	(203) 967-9102
UCN	BCU01	(800) 538-0904
UCN	BCU02	(800) 538-0904
UCN	BCU03	(800) 538-0904
UCN	BCU04	(800) 538-0904
UCN	BCU05	(800) 538-0904
UCN	BCU06	(800) 538-0904
UCN	BCU07	(800) 538-0904
UCN	BCU46	(800) 538-0904
UCN	BCU58	(800) 538-0904
UCN	BCU88	(800) 538-0904
UCN	BCU98	(800) 538-0904
UCN	BCU99	(800) 363-6177
BELL SOUTH LONG DISTANCE	BDL01	(800) 684-2174
BELLSOUTH LONG DISTANCE	BDL07	(800) 684-2174
BELL SOUTH LONG DISTANCE	BDL29	(770) 352-3365
BELLSOUTH LONG DISTANCE	BDL30	(877) 456-4562
BELL SOUTH LONG DISTANCE	BDL77	(800) 684-2174
BELL SOUTH LONG DISTANCE	BDL99	(800) 684-2174
VERIZON COMM.	BELLA	(800) 275-2355
VERIZON COMM.	BEL99	(703) 526-3229
VERIZON COMMUNICATIONS	BESG1	(800) 483-3722
BIG RIVER TELEPHONE LLC	BFN01	(573) 651-3373
BIG RIVER TELEPHONE LLC	BFN99	(573) 651-3373
THE BUSINESS EDGE GROUP	BGE01	(732) 846-7302
BUSINESS EDGE GROUP	BGE02	(732) 846-7302
THE BUSINESS EDGE	BGE03	(732) 846-7302
THE BUSINESS EDGE GROUP	BGE99	(732) 846-7302
BROADVIEW NETWORKS	BJC01	(800) 260-8766
BROADVIEW NETWORKS	BJC02	(800) 260-8766
BROADVIEW NETWORKS	BJC03	(800) 260-8766
BROADVIEW NETWORKS	BJC04	(800) 260-8766
BROADVIEW NETWORKS	BJC99	(315) 442-9567

COVISTA COMMUNICATIONS	BKD01	(800) 493-0800
COVISTA COMMUNICATIONS	BKD99	(866) 254-6532
FIRST COMMUNICATIONS	BNT01	(800) 274-1015
FIRST COMMUNICATIONS	BNT99	(800) 274-1015
TONE NETWORKS INC	BOV01	(888) 526-8663
TONE NETWORKS	BOV02	(888) 526-8663
BOULEVARD MEDIA INC.	BOV99	(888) 526-8663
BUSINESS TECHNOLOGY SERVICES	BQT01	(305) 358-5850
BUSINESS TECHNOLOGY SERVICES	BQT99	(305) 358-5850
SMS/800	BRCNA	(888) 767-3300
STATE DUPLICATES	BRDUP	(888) 767-3300
SMS/800	BRD01	(888) 767-3300
SMS800 HELP DESK	BRD02	(888) 767-3300
SMS800 HELP DESK	BRD03	(888) 767-3300
SMS800 HELP DESK	BRD04	(888) 767-3300
SMS800 HELP DESK	BRD05	(888) 767-3300
SMS800 HELP DESK	BRD06	(888) 767-3300
SMS800 HELPDISK	BRD07	(888) 767-3300
SMS800 HELP DESK	BRD08	(888) 767-3300
SMS800 HELP DESK	BRD09	(888) 767-3300
SMS800 HELP DESK	BRD10	(888) 767-3300
SMS800 HELP DESK	BRD11	(888) 767-3300
SMS800 HELP DESK	BRD12	(888) 767-3300
SMS800 HELP DESK	BRD13	(888) 767-3300
SMS800 HELP DESK	BRD14	(888) 767-3300
SMS800 HELP DESK	BRD15	(888) 767-3300
SMS800 HELP DESK	BRD16	(888) 767-3300
SMS800 HELP DESK	BRD17	(888) 767-3300
SMS800 HELP DESK	BRD18	(888) 767-3300
SMS800 HELP DESK	BRD19	(888) 767-3300
SNS800 HELP DESK	BRD20	(888) 767-3300
SMS/800 HELP DESK	BRD78	(888) 767-3300
SMS/800 HELP DESK	BRD79	(888) 767-3300

SMS/800 HELP DESK	BRD80	(888) 767-3300
SMS/800 HELP DESK	BRD81	(888) 767-3300
SMS800 HELP DESK	BRD82	(888) 767-3300
SMS800 HELP DESK	BRD83	(888) 767-3300
SMS800 HELP DESK	BRD84	(888) 767-3300
SMS800 HELP DESK	BRD85	(888) 767-3300
SMS800 HELP DESK	BRD86	(888) 767-3300
SMS800 HELP DESK	BRD87	(888) 767-3300
SMS800 HELP DESK	BRD88	(888) 767-3300
SMS800 HELP DESK	BRD89	(888) 767-3300
HELP DESK	BRD90	(888) 767-3300
HELP DESK	BRD91	(888) 767-3300
HELPDESK	BRD92	(888) 767-3300
HELPDESK	BRD93	(888) 767-3300
HELPDESK	BRD94	(888) 767-3300
HELPDESK	BRD95	(888) 767-3300
HELPDESK	BRD96	(888) 767-3300
HELPDESK	BRD97	(888) 767-3300
HELPDESK	BRD98	(888) 767-3300
HELPDESK	BRD99	(888) 767-3300
SMS/800	BRERR	(888) 767-3300
SMS/800	BRGMB	(888) 767-3300
SMS/800	BRHDT	(888) 767-3300
SMS/800	BROPR	(888) 767-3300
SMS/800	BRREP	(888) 767-3300
SMS/800	BRSAC	(888) 767-3300
SMS/800	BRSWB	(816) 275-3030
SMS/800	BRTST	(888) 767-3300
UNISYS	BRUIS	(651) 687-2779
SMS/800	BRUNV	(888) 767-3300
#EMPTY	BRZXX	(888) 767-3300
BELL SOUTH TELECOM	BSSBA	(800) 515-1507
BELL SOUTH TELECOM	BSSBB	(800) 515-1507

BELL SOUTH TELECOM	BSSBT	(800) 515-1507
BELL SOUTH TELECOM	BSSB1	(800) 515-1507
BELL SOUTH TELECOM	BSSB2	(800) 515-1507
BELL SOUTH TELECOM	BSSE1	(800) 515-1507
BELL SOUTH TELECOM	BSSM1	(800) 515-1507
BELL SOUTH TELECOM	BSS99	(800) 515-1507
BUSINESS TELECOM INC.	BTI01	(800) 849-2111
#EMPTY	BTI99	#EMPTY
BUSINESS TELECOM INC.	BTM01	(800) 849-2111
BUSINESS TELECOM INC.	BTM99	(800) 849-2111
BUSINESS TELECOM, INC.	BTS01	(800) 849-9100
#EMPTY	BTS99	(800) 849-9100
BEEHIVE TELEPHONE	BVE01	(801) 234-0111
BEEHIVE TELEPHONE	BVE99	(435) 234-0111
BAY STAR COMM. INC.	BYS01	(800) 229-7827
BAY STAR COMM. INC.	BYS99	(800) 229-7827
MCGRAW COMMUNICATIONS, INC	BZY01	(888) 543-2000
MCGRAW COMMUNICATIONS	BZY02	(888) 543-2000
MCGRAW COMMUNICATIONS, INC	BZY99	(888) 543-2000
PACIFIC LIGHT NET	CAB01	(800) 733-5638
PACIFIC LIGHT NET	CAB99	(805) 547-6443
MCLEOD USA	CDN01	(800) 500-8000
MCLEOD USA	CDN02	(800) 500-8000
MCLEOD USA	CDN03	(800) 500-8000
MCLEOD USA	CDN04	(800) 500-8000
MCLEOD USA	CDN99	(800) 500-8000
MCLEOD USA	CDSM1	(800) 500-8000
RCN	CED01	(888) 972-6622
RCN	CED99	(800) 443-4253
COMMUNIGROUP, INC	CGI01	(800) 748-9090
COMMUNIGROUP, INC.	CGI99	(800) 748-9090
COMMUNICATIONS OPTION, INC.	CIO01	(614) 882-2030
COMMUNICATIONS OPTIONS, INC.	CIO99	(614) 882-2030

COOPERATIVE COMMUNICATIONS	CJI01	(800) 833-2700
COOPERATIVE COMMUNICATIONS	CJI99	(800) 833-2700
CGI LONG DISTANCE SERVICES	CKC01	(800) 747-8000
CGI LONG DISTANCE SERVICES	CKC99	(800) 747-8000
ACCERIS COMMUNICATIONS PARTNER	CMT01	(800) 576-7775
WORLDXCHANGE COMMUNICATIONS	CMT99	(800) 576-7775
BELL CANADA	CNM01	(800) 663-8725
BELL CANADA	CNM02	(800) 663-8725
BELL CANADA	CNM99	(800) 663-8725
CUDUP	CUDUP	(888) 767-3300
CYTEL	CZT01	(800) 324-6123
CYTEL	CZT99	(800) 324-6123
ATX TELECOMMUNICATIONS SERVICE	DAB01	(800) 220-4900
ATX TELECOMMUNICATIONS SERVICE	DAB99	(610) 668-3000
CINCINNATI BELL ANY DISTANCE	DBC01	(800) 422-1199
CINCINNATI BELL ANY DISTANCE	DBC03	(513) 768-4469
CINCINNATI BELL ANY DISTANCE	DBC99	(800) 735-3030
CTC LONG DISTANCE SERVICE	DDC01	(888) 200-0100
CTC LONG DISTANCE SERVICE	DDC99	(704) 722-2391
DIGITAL SOLUTIONS	DFN01	(800) 891-8203
DIGITAL SOLUTIONS	DFN99	(800) 891-8203
NUVOX COMMUNICATIONS	DHA01	(864) 672-5048
NUVOX	DHA99	(800) 600-5050
DC COMMUNICATIONS	DIC01	(866) 330-4322
X2 COMMUNICATIONS	DIC99	(908) 782-3177
TNCI	DJK01	(800) 800-8400
TNCI	DJK02	(617) 369-1023
TNCI	DJK03	(617) 369-1023
TNCI	DJK04	(617) 369-1023
TNCI	DJK99	(617) 369-1023
ANDIAMO TELECOM	DKT01	(602) 344-0115
ANIDAMO TELECOM	DKT99	(602) 344-0115
BH TELECOM	DLP01	(310) 273-9023

BH TELECOM	DLP99	(310) 273-9023
POINT ONE	DMZ01	(512) 735-1230
POINT ONE	DMZ99	(512) 735-1230
ADEPTEL, INC.	DPT01	(407) 682-3022
ADEPTEL, INC.	DPT99	(407) 682-3022
TELECON COMMUNICATIONS CORP	DQP01	(321) 263-5999
TELECON COMMUNICATIONS CORP	DQP99	(800) 659-4454
DSI TECHNOLOGIES	DSI01	(310) 636-3322
DSI TECHNOLOGIES	DSI99	(310) 636-3322
DTI	DTI01	(877) 742-5384
DTI	DTI99	(877) 742-5384
TALKPATH, LLC	DUN01	(800) 657-9553
TALKPATH, LLC	DUN99	(800) 657-9553
HELLOCOM, INC	DVC01	(714) 350-6931
HELLOCOM, INC	DVC99	(714) 350-6931
DOW NETWORKS	DWN01	(678) 631-2280
DOW NETWORKS	DWN99	(678) 631-2280
TIERRANET INC.	DXS01	(858) 560-8120
TIERRANET INC.	DXS99	(858) 560-8120
BULLETINS, INC.	DYR01	(714) 740-3000
BULLETINS, INC	DYR99	(714) 453-2360
TELEFYNE, INC	DZY01	(904) 394-1088
TELEFYNE, INC	DZY02	(914) 394-1088
TELEFYNE, INC	DZY03	(914) 394-1088
TELEFYNE, INC	DZY04	(914) 394-1088
TELEFYNE, INC	DZY05	(914) 394-1088
TELEFYNE, INC	DZY06	(914) 394-1088
TELEFYNE, INC	DZY07	(914) 394-1088
TELEFYNE, INC	DZY08	(914) 394-1088
TELEFYNE, INC	DZY09	(914) 394-1088
TELEFYNE, INC	DZY10	(914) 394-1088
TELEFYNE, INC.	DZY99	(904) 565-4051
AT&T LOCAL NETWORK SERVICES	EAC01	(800) 544-6317

AT&T LOCAL NETWORK SERVICES	EAC99	(800) 544-6317
MIJANDA, INC	EBO01	(866) 512-0200
MIJANDA, INC	EBO99	(866) 512-0200
LDDS/METROMEDIA (EDS)	EDS01	(601) 360-8600
LDDS/METROMEDIA (EDS)	EDS99	(601) 360-8600
ADVANCED TEL, INC.	EET01	(800) 621-4211
ADVANCED TEL, INC.	EET99	(877) 621-4167
E-RESPONSES.COM, INC.	EFJ01	(310) 902-5169
E-RESPONSES.COM, INC.	EFJ99	(310) 902-5169
EFFICY GROUP	EGI99	(888) 233-3429
ACCESS POINT INC.	EHT01	(919) 851-4838
ACCESS POINT INC.	EHT02	(919) 851-4838
ACCESS POINT INC	EHT03	(919) 851-4838
ACCESS POINT INC	EHT04	(919) 851-4838
ACCESS POINT, INC	EHT05	(919) 851-4833
ACCESS POINT INC	EHT06	(919) 851-4838
ACCESS POINT INC	EHT07	(919) 851-4838
ACCESS POINT, INC	EHT08	(919) 851-4838
ACCESS POINT INC.	EHT99	(919) 851-4838
NETRONIXS	EIX01	(800) 840-8708
NETRONIXS	EIX99	(800) 840-8708
EUREKAGGN	EJT01	(800) 562-4206
EUREKAGGN	EJT99	(800) 562-4206
PHONE PEOPLE HOLDINGS CORP	EKL01	(858) 569-4444
PHONE PEOPLE HOLDINGS CORP	EKL99	(858) 569-4444
EXCEL TELECOMMUNICATIONS INC.	ELT01	(800) 380-8089
EXCEL TELECOMMUNICATIONS INC.	ELT02	(514) 940-2978
EXCEL TELECOMMUNICATIONS INC.	ELT99	(800) 380-8089
EARNWARE CORPORATION	ENE01	(888) 388-4359
EARNWARE CORPORATION	ENE02	(888) 388-4359
EARNWARE CORPORATION	ENE99	(888) 388-4359
EASTERN TELEPHONE & TELECOMM	EOT01	(610) 433-1000
EASTERN TELEPHONE & TELECOMM	EOT99	(610) 433-1000

ECI CONFERENCE CALL SERVICES	EQC01	(800) 788-1085
ECI CONFERENCE CALL SERVICES	EQC99	(800) 788-1085
GLOBAL CROSSING	ESM01	(800) 783-2020
GLOBAL CROSSING	ESM99	(800) 783-2020
CAPITAL TELECOMMUNICATIONS	ETS01	(215) 628-4111
EASTERN TEL LONG DIST. S. INC.	ETS99	(215) 628-4111
TELUS CORPORATION	EUS01	(877) 700-4662
TELUS QUEBEC	EUS02	(800) 463-3794
TELUS CORPORATION	EUS03	(780) 493-6561
TELUS CORPORATION	EUS04	(780) 493-6561
TELUS CORPORATION	EUS05	(780) 493-6561
TELUS CORPORATION	EUS06	(780) 493-6561
TELUS COMMUNICATIONS	EUS07	(877) 700-4662
TELUS COMMUNICATIONS	EUS08	(877) 700-4662
TELUS COMMUNICATIONS	EUS09	(877) 700-4662
TELUS CORPORATION	EUS11	(780) 493-6561
TELUS CORPORATION	EUS12	(780) 493-6561
TELUS CORPORATION	EUS21	(780) 493-6561
TELUS CORPORATION	EUS22	(780) 493-6561
TELUS CORPORATION	EUS23	(780) 493-6561
TELUS CORPORATION	EUS31	(780) 493-6561
TELUS CORPORATION	EUS32	(780) 493-6561
TELUS CORPORATION	EUS33	(780) 493-6561
TELUS CORPORATION	EUS41	(780) 493-6561
TELUS CORPORATION	EUS42	(780) 493-6561
TELUS CORPORATION	EUS43	(780) 493-6561
TELUS CORPORATION	EUS44	(780) 493-6561
TELUS CORPORATION	EUS45	(780) 493-6561
TELUS COMMUNICATIONS, INC.	EUS99	(780) 493-6561
ELECTRIC LIGHTWAVE-ELI	EVW01	(800) 622-4354
ELECTRIC LIGHTWAVE	EVW02	(800) 622-4354
ELECTRIC LIGHTWAVE	EVW03	(800) 622-4354
ELECTRIC LIGHTWAVE	EVW04	(800) 622-4354

ELECTRIC LIGHTWAVE	EVW05	(800) 622-4354
ELECTRIC LIGHTWAVE-ELI	EVW99	(800) 622-4354
NEW NETWORK	EWN01	(877) 667-3463
NEW NETWORK	EWN99	(877) 667-3463
CABLE VISION LIGHTPATH	EYE01	(516) 393-3434
CABLEVISION LIGHTPATH	EYE02	(866) 611-3434
CABLE VISION LIGHTPATH	EYE99	(516) 393-3434
UCN	FAM01	(800) 393-8593
UCN	FAM07	(800) 393-8593
UCN	FAM28	(800) 393-8593
UCN	FAM32	(800) 393-8593
UCN	FAM56	(800) 393-8593
UCN	FAM87	(800) 393-8593
UCN	FAM99	(602) 264-8684
FULL SERVICE NETWORK	FCC01	(888) 281-4800
FULL SERVICE NETWORK	FCC02	(888) 281-4800
FULL SERVICE NETWORK	FCC03	(888) 281-4800
FULL SERVICE NETWORK	FCC99	(888) 281-4800
FDN COMMUNICATIONS	FDN01	(407) 835-0334
FLORIDA DIGITAL NETWORK	FDN99	(407) 835-0334
BIRCH/IONEX TELECOMMUNICATIONS	FEL01	(800) 860-8401
IONEX TELECOM, INC.	FEL99	(605) 332-3232
FOCAL COMMUNICATIONS	FGC01	(888) 362-2522
FOCAL COMMUNICATIONS	FGC99	(888) 362-2522
1800FORINFO	FHT01	(561) 243-6968
1800FORINFO	FHT99	(561) 243-6968
FIRST DIGITAL TELECOM	FJT01	(801) 456-1000
FIRST DIGITAL TELECOM	FJT99	(801) 456-1000
FRONTIER COMMUNICATIONS	FLX01	(518) 773-6122
FRONTIER COMMUNICATIONS	FLX99	(800) 726-3539
FUTURE DONTICS INC	FNA01	(310) 215-6400
FUTURE DONTICS INC	FNA99	(310) 215-6400
FONOROLA, INC.	FON01	(416) 718-7474

FONOROLA, INC.	FON99	(800) 905-2580
PREMIERE GLOBAL SERVICES	FPE01	(877) 490-3186
PREMIERE GLOBAL SERVICES	FPE02	(877) 490-3185
PREMIERE GLOBAL SERVICES	FPE03	(877) 490-3185
PREMIERE GLOBAL	FPE04	(877) 490-3185
PREMIERE GLOBAL SERVICES	FPE99	(877) 490-3186
BIRCH/IONEX TELECOMMUNICATIONS	FST01	(800) 860-8401
IONEX TELECOM	FST02	(316) 833-5235
IONEX TELECOM	FST99	(316) 337-8640
FULL SPECTRUM TELECOMM. INC.	FUL01	(727) 524-3900
FULL SPECTRUM TELECOMM. INC.	FUL99	(727) 524-3900
TOLL FREE EXPRESS, INC.	FVD01	(949) 777-0137
TOLL FREE EXPRESS, INC.	FVD99	(949) 777-0137
COMMPARTNERS LLC	FYI01	(800) 577-4021
COMMPARTNERS LLC	FYI99	(800) 577-4021
HBDC	FZF01	(954) 294-2534
HBDC	FZF99	(954) 294-2534
BBCOM	GBB01	(213) 489-2156
BBCOM	GBB99	(213) 489-2156
GCI COMMUNICATIONS CORP	GCI01	(800) 770-8725
GCI COMMUNICATIONS CORP	GCI99	(800) 770-8725
ANI-NETWORKS	GDG01	(702) 547-8786
RED RIVER NETWORKS	GDG02	(405) 820-5250
RED RIVER NETWORKS	GDG03	(405) 820-5250
RED RIVER NETWORKS	GDG04	(405) 820-5250
RED RIVER NETWORKS	GDG05	(405) 820-5250
RED RIVER NETWORKS	GDG06	(405) 820-5250
RED RIVER NETWORK	GDG99	(405) 820-5250
TSI	GFD01	(805) 277-0400
TSI	GFD02	(805) 277-0400
TSI	GFD03	(805) 277-0400
TSI	GFD04	(805) 277-0400
TSI	GFD05	(805) 277-0400

TSI	GFD06	(805) 277-0400
TSI	GFD07	(805) 277-0400
TSI	GFD08	(805) 277-0400
TSI	GFD09	(805) 277-0400
TSI	GFD10	(805) 277-0400
TSI	GFD11	(805) 277-0400
TSI	GFD12	(805) 277-0400
TSI	GFD13	(805) 277-0400
TSI	GFD14	(805) 277-0400
TSI	GFD15	(805) 277-0400
TSI	GFD16	(805) 277-0400
TSI	GFD17	(805) 277-0400
TSI	GFD18	(805) 277-0400
TSI	GFD19	(805) 277-0400
TSI	GFD20	(805) 277-0400
TSI	GFF01	(805) 277-0400
TSI	GFF02	(805) 277-0400
TSI	GFF03	(805) 277-0400
TSI	GFF04	(805) 277-0400
TSI	GFF05	(805) 277-0400
TSI	GFF06	(805) 277-0400
TSI	GFF07	(805) 277-0400
TSI	GFF08	(805) 277-0400
TSI	GFF09	(805) 277-0400
TSI	GFF10	(805) 277-0400
TSI	GFF11	(805) 277-0400
TSI	GFF12	(805) 277-0400
TSI	GFF13	(805) 277-0400
TSI	GFF14	(805) 277-0400
TSI	GFF15	(805) 277-0400
TSI	GFF16	(805) 277-0400
TSI	GFF17	(805) 277-0400
TSI	GFF18	(805) 277-0400

TSI	GFF19	(805) 277-0400
TSI	GFF20	(805) 277-0400
TSI	GFF99	(805) 277-0400
TSI	GFT01	(805) 277-0400
TSI	GFT02	(805) 277-0400
TSI	GFT03	(805) 277-0400
TSI	GFT04	(805) 277-0400
TSI	GFT05	(805) 277-0400
TSI	GFT06	(805) 277-0400
TSI	GFT07	(805) 277-0400
TSI	GFT08	(805) 277-0400
TSI	GFT09	(805) 277-0400
TSI	GFT10	(805) 277-0400
TSI	GFT11	(805) 277-0400
TSI	GFT12	(805) 277-0400
TSI	GFT13	(805) 277-0400
TSI	GFT14	(805) 277-0400
TSI	GFT15	(805) 277-0400
TSI	GFT16	(805) 277-0400
TSI	GFT17	(805) 277-0400
TSI	GFT18	(805) 277-0400
TSI	GFT19	(805) 277-0400
TSI	GFT20	(805) 277-0400
TSI	GFU01	(805) 277-0400
TSI	GFU02	(805) 277-0400
TSI	GFU03	(805) 277-0400
TSI	GFU04	(805) 277-0400
TSI	GFU05	(805) 277-0400
TSI	GFU06	(805) 277-0400
TSI	GFU07	(805) 277-0400
TSI	GFU08	(805) 277-0400
TSI	GFU09	(805) 277-0400
TSI	GFU10	(805) 277-0400

TSI	GFU11	(805) 277-0400
TSI	GFU12	(805) 277-0400
TSI	GFU13	(805) 277-0400
TSI	GFU14	(805) 277-0400
TSI	GFU15	(805) 277-0400
TSI	GFU16	(805) 277-0400
TSI	GFU17	(805) 277-0400
TSI	GFU18	(805) 277-0400
TSI	GFU19	(805) 277-0400
TSI	GFU20	(805) 277-0400
UNIPOINT SERVICES, INC.	GHI01	(512) 735-1200
UNIPOINT SERVICES, INC.	GHI99	(512) 735-1200
TELEGLOBE INTERNATIONAL CORP	GIC01	(514) 868-8787
TELEGLOBE INTERNATIONAL CORP	GIC99	(514) 868-8787
GRAND CIRCLE TRAVEL	GKL01	(617) 346-6825
GRAND CIRCLE TRAVEL	GKL99	(617) 346-3825
GLOBALCOM, INC	GMM01	(800) 589-1531
GLOBALCOM, INC	GMM99	(800) 589-1531
ALLIANCE GROUP SERVICES INC	GRP01	(203) 221-8700
ALLIANCE GROUP SERVICES	GRP02	(203) 221-8700
ALLINACE GROUP SERVICES	GRP03	(203) 221-8700
ALLINACE GROUP SERVICES	GRP04	(203) 221-8700
ALLINACE GROUP SERVICES	GRP05	(203) 221-8700
ALLIANCE GROUP SERVICES, INC.	GRP06	(203) 221-8700
ALLIANCE GROUP SERVICES INC	GRP99	(203) 845-9600
VERIZON SELECT SERVICES	GTSM1	(800) 483-8494
VERIZON SELECT SERVICES	GTWDA	(800) 483-8494
VERIZON SELECT SERVICES	GTWDT	(800) 483-8494
VERIZON SELECT SERVICES	GTWD1	(800) 483-8494
VERIZON SELECT SERVICES	GTWD2	(800) 483-8494
VERIZON SELECT SERVICES	GTWD3	(800) 483-8494
VERIZON SELECT SERVICES	GTWD4	(800) 483-8494
VERIZON SELECT SERVICES	GTWD5	(800) 483-8494

VERIZON SELECT SERVICES	GTWD6	(800) 483-8494
VERIZON SELECT SERVICES	GTW99	(800) 483-8494
THE SOFTWARE WERKS INC	GXC01	(904) 434-2774
THE SOFTWARE WERKS INC	GXC99	(904) 434-2774
RING9, INC	GYC01	(866) 746-4999
RING9, INC	GYC99	(866) 746-4999
TGEC COMMUNICATIONS CO.,L.L.C.	GZT01	(650) 596-7302
TGEC COMMUNICATIONS CO.,L.L.C.	GZT99	(650) 596-7302
HBNET	HBN01	(602) 504-4630
HBNET	HBN99	(602) 504-4630
NATIONAL COMTEL NETWORK, INC.	HCN01	(818) 881-7900
NATIONAL COMTEL	HCN02	(800) 987-0100
NATIONAL COMTEL NETWORK, INC.	HCN99	(818) 881-7900
LINE SYSTEMS INC	HDS01	(610) 355-9700
LINE SYSTEMS INC	HDS99	(610) 355-9700
CAVALIER TELEPHONE LLC	HER01	(866) 800-6855
NET 2000 COMMUNICATIONS	HER99	(703) 654-2000
ADVANCED COMMUNICATIONS INTEGR	HFG01	(714) 986-9666
ADVANCED COMMUNICATIONS INTEGR	HFG99	(714) 986-9666
LIVEOPS, INC	HHG01	(800) 898-2796
CALLCAST INC	HHG99	(650) 614-0750
HTC	HJK01	(618) 939-6112
HTC	HJK99	(618) 939-6112
HICKORY TECH	HKT01	(507) 387-1151
HICKORY TECH	HKT99	(507) 387-1151
EPANA NETWORKS	HMM01	(212) 931-8800
EPANA NETWORKS	HMM99	(212) 931-8800
SIGECOM	HOT01	(866) 976-7800
SIGECOM	HOT99	(812) 437-0301
DIAL-AROUND TELECOM	HVN01	(817) 329-7424
DIAL-AROUND TELECOM	HVN99	(817) 329-7424
NETWORK COMM. INT'L CORP.	HWK01	(888) 386-3709
NETWORK COMM. INT'L CORP.	HWK99	(888) 386-3709

HAWAIIAN TELCOM, INC	HXT01	(808) 643-4662
HAWAIIAN TELECOM, INC	HXT48	(808) 457-9963
HAWAIIAN TELECOM, INC.	HXT79	(808) 457-9963
HAWAIIAN TELCOM, INC.	HXT99	(808) 643-4662
ALLERGAN SALES LLC	HYT01	(714) 246-4579
ALLERGAN SALES LLC	HYT99	(704) 246-4579
IT&E OVERSEAS	IEO01	(671) 646-8886
IT&E OVERSEAS	IEO99	(671) 646-8886
CONVERGYS SPEECH SOLUTIONS	IHB01	(703) 620-4700
CONVERGYS SPEECH SOLUTIONS	IHB99	(703) 620-4700
PAYMENTECH LP	IJK01	(800) 354-8879
PAYMENTECH LP	IJK99	(800) 354-8879
IDS LONG DISTANCE	ILD01	(866) 872-2443
IDS LONG DISTANCE	ILD99	(866) 872-2443
INTEGRA TELECOM	IMT01	(218) 625-4312
INTEGRA TELECOM	IMT02	(503) 748-1945
INTEGRA TELECOM	IMT03	(503) 748-1945
INTEGRA TELECOM	IMT04	(503) 748-1945
INTEGRA TELECOM	IMT05	(503) 748-1945
INFOTEL COMMUNICATIONS, LLC	IMT99	(218) 825-7880
TIME WARNER TELECOM	INF01	(866) 654-2547
TIME WARNER TELECOM	INF99	(866) 654-2547
IOWA COMMUNICATIONS NETWORK	IOW01	(800) 358-5937
IOWA COMMUNICATIONS NETWORK	IOW99	(800) 358-5937
IDT CORPORATION	IPT01	(973) 438-4320
IDT CORPORATION	IPT09	(201) 928-4320
IDT	IPT22	(973) 438-1000
IDT CORPORATION	IPT53	(973) 438-4320
IDT CORPORATION	IPT99	(201) 928-2941
TOTAL CALL INTERNATIONAL, INC	IRN01	(213) 239-0910
TOTAL CALL INTERNATIONAL, INC	IRN99	(213) 239-0910
IOWA NETWORK SERVICES	ISV01	(800) 469-4000
IOWA NETWORK SERVICES	ISV99	(800) 469-4000

XO COMMUNICATIONS	IVN01	(503) 972-6833
XO COMMUNICATIONS	IVN99	(503) 972-6897
KALL8	IWL01	(206) 479-2322
INTERNATIONAL TELECOM LTD	IWL03	(206) 479-2322
ITL	IWL04	(206) 479-2322
INTERNATIONAL TELCOM LTD	IWL99	(800) 733-1335
BROADWING COMMUNICATIONS	IXC01	(800) 994-9638
BROADWING COMMUNICATIONS	IXC99	(800) 848-8459
INTELEMEDIA COMMUNICATIONS INC	IYM01	(972) 994-0700
INTELEMEDIA COMMUNICATIONS INC	IYM99	(972) 994-0700
BROADWING COMMUNICATIONS	IZC01	(800) 433-0630
BROADWING COMMUNICATIONS	IZC99	(800) 994-9683
NORLIGHT TELECOM, INC.	JCI01	(877) 792-7905
NORLIGHT TELECOM, INC.	JCI99	(414) 792-7914
TIMESHIFT	JFT01	(323) 817-3220
TIMESHIFT	JFT99	(323) 817-3220
TIMESHIFT	JFX01	(323) 817-3220
TIMESHIFT	JFX99	(323) 817-3220
24-7-365, INC.	JGL01	(310) 738-2500
24-7-365, INC.	JGL99	(310) 738-2500
NEXT-G COMMUNICATIONS	JHT01	(713) 952-5885
NEXT-G COMMUNICATIONS	JHT99	(713) 952-5885
COMMERCIAL LT BARODA, SA	JJJ01	(866) 870-7060
COMMERCIAL LT BARODA, SA	JJJ99	(800) 972-9631
ERESPORG LLC	JMN99	(866) 322-3800
800 IDEAS.COM, INC.	JON01	(858) 565-4000
800 IDEAS.COM, INC.	JON99	(858) 565-4000
IT CONNECT CANADA	JRC01	(888) 482-6663
IT CONNECT CANADA	JRC99	(888) 482-6663
TELCOVE	JSS01	(877) 321-5465
TELCOVE	JSS99	(814) 260-2745
DOLLAR PHONE ACCESS, INC	JUI01	(718) 889-1102
DOLLAR PHONE ACCESS, INC	JUI99	(718) 889-1102

WIRESTAR COMMUNICATIONS	JWS01	(800) 947-3782
WIRESTAR COMMUNICATIONS	JWS99	(800) 947-3782
AMTEC	JZJ01	(310) 766-2220
AMTEC	JZJ02	(310) 766-2222
AMTEC	JZJ03	(310) 766-2222
AMTEC	JZJ04	(310) 766-2222
AMTEC	JZJ05	(310) 766-2222
AMTEC	JZJ06	(310) 766-2222
AMTEC	JZJ07	(310) 766-2222
AMTEC	JZJ08	(310) 766-2222
AMTEC	JZJ09	(310) 766-2222
AMTEC	JZJ10	(310) 766-2222
AMTEC	JZJ11	(310) 766-2222
AMTEC	JZJ12	(310) 766-2222
AMTEC	JZJ13	(310) 766-2222
AMTEC	JZJ14	(310) 766-2222
AMTEC	JZJ15	(310) 766-2222
AMTEC	JZJ16	(310) 766-2222
AMTEC	JZJ17	(310) 766-2222
AMTEC	JZJ18	(310) 766-2222
AMTEC	JZJ19	(310) 766-2222
AMTEC	JZJ20	(310) 766-2222
AMTEC	JZZ01	(310) 766-2222
AMTEC	JZZ99	(310) 766-2222
TCAST COMMUNICATIONS, INC.	KAA01	(661) 253-5030
TCAST COMMUNICATIONS	KAT01	(661) 253-5030
TCAST COMMUNICATIONS	KAT99	(661) 253-5030
NETWORK US INC	KBT01	(888) 742-5523
NETWORK US INC.	KBT99	(888) 742-5523
AIRESPRING INC	KDB01	(888) 899-2789
AIRESPRING INC	KDB99	(888) 899-2789
SAGE TELECOM	KFV01	(214) 547-7195
SAGE TELECOM	KFV99	(214) 547-7195

WORLD ONE TELECOM, LLC	KGE01	(213) 675-0218
WORLD ONE TELECOM, LLC	KGE99	(213) 675-0218
SNIP LINK LLC	KIS01	(888) 764-7600
SNIP LINK LLC	KIS99	(888) 764-7600
C & C MANAGEMENT	KKM01	(251) 633-6990
C & C MANAGEMENT	KKM99	(251) 633-6990
TRANSACTION NETWORK SERVICES	KLS01	(703) 453-8500
TRANSACTION NETWORK SERVICES	KLS99	(703) 453-8465
NETWORK MANAGEMENT INC	KMT01	(801) 990-0325
NETWORK MANAGEMENT INC	KMT99	(801) 990-0325
SOUTINE ENTERPRISES	KOK01	(954) 275-8998
SOUTINE ENTERPRISES	KOK99	(954) 275-8998
TELRITE CORPORATION	KPK01	(770) 818-5305
TELRITE CORPORATION	KPK99	(770) 818-5305
GAFACHI	KRY01	(646) 723-0500
GAFACHI	KRY99	(646) 723-0500
WILLIAMS/WILTEL COMMUNICATIONS	KSW01	(877) 864-2309
WILLIAMS/WILTEL COMMUNICATIONS	KSW02	(877) 864-2309
WILLIAMS/WILTEL COMMUNICATIONS	KSW03	(877) 864-2309
WILLIAMS/WILTEL COMMUNICATIONS	KSW99	(877) 864-2309
SHEPHER CORPORATION	KUB01	(818) 700-7000
SHEPHER CORPORATION	KUB99	(818) 700-7000
GRANDE COMMUNICATIONS NETWORKS	KWN01	(800) 200-3694
GRANDE COMMUNICATIONS NETWORKS	KWN99	(512) 787-5408
PREMIERE CONFERENCING	KYT01	(913) 661-0700
PREMIERE CONFERENCING	KYT99	(913) 661-0700
SOVERNET INC	KZA01	(877) 877-2120
SOVERNET INC	KZA99	(877) 877-2120
CENTENNIAL PR OPERATIONS CORP	LAM01	(787) 717-9648
CENTENNIAL PR OPERATIONS CORP	LAM99	(787) 717-9648
LEGACY LONG DISTANCE	LBD01	(714) 826-0547
LEGACY LONG DISTANCE	LBD99	(714) 826-0547

CONSOLIDATED COMMUNICATIONS	LCT01	(800) 364-2528
CONSOLIDATED COMMUNICATIONS	LCT99	(800) 364-2528
MCI WORLDCOM	LDD01	(800) 264-1000
MCI WORLDCOM	LDD02	(800) 264-1000
MCI WORLDCOM	LDD03	(800) 264-1000
MCI WORLDCOM	LDD04	(800) 264-1000
MCI WORLDCOM	LDD05	(888) 872-9266
MCI WORLDCOM	LDD06	(888) 872-9266
MCI WORLDCOM	LDD07	(888) 872-9266
MCI WORLDCOM	LDD08	(888) 872-9266
MCI WORLDCOM	LDD20	(888) 872-9266
MCI WORLDCOM	LDD99	(800) 264-1000
QWEST/LCI INT'L	LGSM1	(800) 860-7678
QWEST/LCI INT'L	LGTTE	(800) 860-1020
QWEST/LCI INT'L	LGT01	(800) 860-1020
QWEST/LCI INT'L	LGT99	(800) 860-1020
LIGHTSHIP TELECOM DBA CTC	LHS01	(603) 314-2433
LIGHTSHIP TELECOM DBA CTC	LHS99	(603) 314-2433
POPP.COM	LIC01	(763) 797-7900
POPP.COM	LIC99	(763) 797-7900
LATAONE INC	LJK01	(800) 230-4451
LATAONE INC	LJK02	(800) 230-4451
LATAONE INC	LJK03	(800) 230-4451
LATAONE, INC	LJK04	(800) 230-4451
LATAONE, INC	LJK05	(800) 230-4451
LATAONE INC	LJK06	(800) 230-4451
LATAONE INC	LJK07	(800) 230-4451
LATAONE INC	LJK08	(800) 230-4451
LATAONE INC	LJK09	(800) 230-4451
LATAONE, INC	LJK10	(800) 230-4451
LATAONE, INC.	LJK11	(800) 230-4451
LATAONE, INC.	LJK12	(800) 230-4451
LATAONE, INC.	LJK13	(800) 230-4451

LATAONE, INC	LJK14	(800) 230-4451
LATAONE, INC.	LJK15	(800) 230-4451
LATAONE, INC	LJK16	(800) 230-4451
LATAONE, INC.	LJK17	(800) 230-4451
LATAONE, INC.	LJK18	(800) 230-4451
LATAONE, INC.	LJK19	(800) 230-4451
LATAONE, INC.	LJK20	(800) 230-4451
LATAONE INC	LJK99	(800) 230-4451
LOCUS TELECOM, INC.	LKS01	(800) 539-6016
LOCUS TELECOM, INC.	LKS99	(800) 539-6016
LDMI LONG DISTANCE	LMI01	(800) 374-5364
LDMI LONG DISTANCE	LMI99	(313) 664-2321
CINERGY COMMUNICATIONS CO	LOD01	(800) 599-1000
CINERGY COMMUNICATIONS CO	LOD99	(812) 456-4748
800 RESPONSE INFORMATION	LPS01	(802) 860-0378
800 RESPONSE INFORMATION	LPS99	(802) 860-0378
LEVEL 3 COMMUNICATIONS LLC	LVC01	(877) 453-8353
LEVEL 3 COMMUNICATIONS LLC	LVC99	(720) 888-7742
LINX COMMUNICATIONS	LXC01	(617) 747-3950
LINX COMMUNICATIONS	LXC99	(617) 747-3950
LYNX TELECOM L.L.C.	LYX01	(801) 254-6245
LYNX TELECOM L.L.C.	LYX99	(801) 295-2264
LONG DISTANCE BILLING SERVICES	LZO01	(888) 826-9414
LONG DISTANCE BILLING SERVICES	LZO99	(888) 826-9414
MCI	MCI01	(800) 888-1800
MCI	MCI02	(800) 888-1800
MCI	MCI99	(800) 888-1800
MCI WHOLESALE	MCW22	(800) 828-4984
MET TEL	MET01	(212) 607-6336
MET TEL	MET99	(212) 588-0319
SMARTBOX	MHT01	(514) 398-9355
SMARTBOX	MHT99	(514) 398-9355
WINSTAR COMMUNICATIONS INC.	MID01	(888) 888-3039

WINSTAR COMMUNICATIONS INC.	MID99	(888) 888-3039
MICKTEL CORP	MJC01	(858) 775-7240
MICKTEL CORP	MJC99	(858) 775-7240
MICRONESIAN TELECOMMUNICATIONS	MKN01	(670) 682-3878
MICRONESIAN TELECOMMUNICATIONS	MKN99	(670) 682-3878
CRICKET COMMUNICATIONS	MLK01	(858) 882-9279
CRICKET COMMUNICATIONS	MLK99	(858) 882-9279
COMMUNICATION MANAGEMENT SVC	MNS01	(858) 565-2800
COMMUNICATION MANAGEMENT SVC	MNS99	(619) 521-8531
MONMOUTH TELEPHONE & TELEGRAPH	MOT01	(732) 704-1000
MONMOUTH TELEPHONE & TELEGRAPH	MOT99	(732) 704-1000
MPOWER COMMUNICATIONS CORP	MPC01	(702) 310-7994
MPOWER COMMUNICATIONS	MPC99	(702) 310-4300
MISC-ETC	MQX01	(503) 234-1234
MISC-ETC	MQX99	(503) 639-5953
1-800 CONTACTS, INC.	MRG01	(801) 316-7878
1-800 CONTACTS, INC	MRG99	(801) 316-7878
SIOUXLAND TELEPHONE CO STC/MTI	MTI01	(605) 232-3457
SIOUXLAND TELEPHONE CO STC/MTI	MTI99	(605) 232-3457
SIERRA COMMUNICATIONS INC	MUI01	(866) 270-7560
SIERRA COMMUNICATIONS, INC	MUI99	(866) 270-7560
AMAX TWO	MXT01	(208) 475-6021
AMAX TWO	MXT99	(207) 475-6021
MAYFAIR COMMUNICATIONS, INC.	MYR01	(800) 629-3247
MAYFAIR COMMUNICATIONS, INC.	MYR99	(800) 629-3247
NTS COMMUNICATIONS	NCM01	(800) 658-2101
NTS COMMUNICAITONS	NCM99	(800) 658-2150
NETWORK ENHANCED TELECOM	NKS01	(903) 758-9350
NETWORK ENHANCED TELECOM	NKS99	(903) 758-9350
NETWORK ENHANCED TELECOM	NKT01	(903) 323-4544
XO COMMUNICATIONS	NLS01	(888) 575-6398
XO COMMUNICATIONS	NLS02	(888) 575-6398
XO COMMUNICATIONS	NLS03	(888) 575-6398

XO COMMUNICATIONS	NLS99	(888) 575-6398
XO COMMUNICATIONS	NLV99	(702) 990-1000
BESTLINE	NPH01	(800) 365-6030
BESTLINE	NPH99	(800) 365-6030
NOS COMMUNICATIONS	NRC01	(702) 547-8786
NOS COMMUNICATIONS	NRC02	(702) 547-8793
NOS COMMUNICATIONS	NRC03	(702) 547-8793
NOS COMMUNICATIONS	NRC99	(702) 547-8786
NETWORK TELEPHONE SERVICES INC	NSI01	(818) 227-1100
NETWORK TELEPHONE SERVICES INC	NSI99	(818) 227-1100
NAVIGATA COMMUNICATIONS	NUM01	(800) 668-9377
NAVIGATA COMMUNICATIONS	NUM02	(800) 668-9377
NAVIGATA COMMUNICATIONS	NUM99	(800) 668-9377
VERIZON (LEC)	NXCMP	(212) 692-0610
VERIZON (LEC)	NXNE1	(212) 692-0610
VERIZON (LEC)	NXNYT	(212) 338-7400
VERIZON (LEC)	NXNY1	(212) 338-7400
VERIZON LEC	NXN99	(212) 338-7400
VERIZON (LEC)	NXSE1	(212) 692-0610
VERIZON (LEC)	NXSM1	(212) 338-7400
ON-CALL RESP ORG SVSC, INC	OAK01	(800) 986-2501
ON-CALL RESP ORG SVSC, INC	OAK99	(800) 986-2501
ONE CALL COMMUNICATIONS	OCC01	(317) 575-3200
ONE CALL COMMUNICATIONS	OCC99	(800) 879-9939
INTERNATIONAL TELECOMMUNICATIO	OET01	(954) 862-2249
INTERNATIONAL TELECOMMUNICATIO	OET99	(954) 862-2249
INTERMETRO COMMUNICATIONS INC	OFT01	(805) 433-8000
INTERMETRO COMMUNICATIONS INC	OFT02	(805) 433-8000
INTERMETRO COMMUNICATIONS INC	OFT99	(805) 433-8000
CBeyond COMMUNICATIONS	OJB01	(678) 424-2663
CBeyond COMMUNICATIONS	OJB99	(678) 424-2663
ATG	OKB01	(800) 832-1754
ATG	OKB02	(800) 832-0754

ATG	OKB99	(480) 688-5760
ZONE TELECOM, INC	OOZ01	(866) 539-9663
ZONE TELECOM INC	OOZ02	(866) 539-9663
ZONE TELECOM, INC	OOZ03	(866) 539-9663
ZONE TELECOM, INC	OOZ04	(866) 539-9663
ZONE TELECOM, INC	OOZ05	(866) 539-9663
ZONE TELECOM, INC	OOZ99	(866) 539-9663
ORION TELECOMMUNICATIONS CORP.	ORN01	(732) 236-1938
ORION TELECOMMUNICATIONS CORP	ORN99	(732) 236-1938
GOSOLO TECHNOLOGIES INC	OSG01	(727) 821-6565
GOSOLO TECHNOLOGIES INC	OSG99	(727) 821-6565
CALL SOURCE	OUR01	(888) 763-6200
CALL SOURCE	OUR99	(818) 676-3417
CNE TELECOMMUNICATION LLC	OWL01	(866) 870-2464
CNE TELECOMMUNICATION LLC	OWL99	(866) 870-2464
FSC, LLC	OYL01	(800) 685-4001
FSC, LLC	OYL99	(800) 685-4001
PRIMUS CANADA	PBQ01	(416) 236-3636
PRIMUS CANADA	PBQ99	(416) 236-3636
PACIFIC BELL	PCLD1	(800) 933-0300
PACIFIC BELL	PCPTP	(800) 933-0300
PACIFIC BELL	PCPTR	(800) 933-0300
PACIFIC BELL	PCPTT	(800) 933-0300
PACIFIC BELL	PCPT1	(800) 933-0300
PACIFIC BELL	PCP99	(800) 933-0300
PACIFIC BELL	PCSM1	(800) 933-0300
THE PHONE COMPANY	PFC01	(215) 862-1508
THE PHONE COMPANY	PFC99	(215) 862-1508
PNG TELECOM	PGN01	(800) 860-9495
PNG TELECOM	PGN99	(800) 860-9495
PRIMETEL COMMUNICATIONS	PIT01	(888) 774-6383
PRIMETEL COMMUNICATIONS	PIT99	(888) 774-6383
PAETEC COMMUNICATIONS	PKC01	(877) 340-2555

PAETEC COMMUNICATIONS	PKC02	(877) 340-2555
PAETEC COMMUNICATIONS	PKC03	(877) 340-2555
PAETEC COMMUNICATIONS	PKC04	(877) 340-2555
PAETEC COMMUNICATIONS	PKC99	(877) 340-2555
PAETEC COMMUNICATIONS INC.	PK777	(877) 340-2555
PILGRIM TELEPHONE	PLG01	(617) 225-7000
PILGRIM TELEPHONE	PLG99	(617) 225-7000
WEPS	PMI01	(516) 378-9116
WEPS	PMI99	(800) 676-2223
VOICECOM TELECOMMUNICATIONS	PQC01	(770) 663-5062
VOICECOM TELECOMMUNICATIONS	PQC99	(404) 487-8475
PUERTO RICO TELEPHONE	PRT01	(787) 749-5500
PUERTO RICO TELEPHONE	PRT99	(787) 749-5500
PACIFIC CENTREX SERVICES	PSS01	(818) 623-2300
PACIFIC CENTREX SERVICES	PSS99	(818) 623-2300
PHONE USA, INC.	PUI01	(800) 390-0779
PHONE USA, INC.	PUI99	(800) 390-0779
PACWEST	PWT01	(800) 399-3389
PACWEST	PWT99	(888) 861-3351
TELEPACIFIC COMMUNICATIONS	PZC01	(877) 487-8722
TELEPACIFIC COMMUNICATIONS	PZC99	(800) 487-8722
COX TELECOM, LLC	QEQ01	(405) 600-6333
COX TELECOM, LLC	QEQ99	(405) 600-6333
CONVERGIA INC.	QKB01	(514) 693-6300
CONVERGIA INC.	QKB99	(514) 693-6300
PHOENIX INT'L TELEPORT SATELLI	QNE01	(800) 274-6030
PHOENIX INT'L TELEPORT SATELLI	QNE99	(800) 274-6030
TMC COMMUNICATIONS	QQA01	(877) 862-8655
TMC COMMUNICATIONS	QQA02	(877) 862-8655
TMC COMMUNICATIONS	QQA50	(877) 862-8655
TMC COMMUNICATIONS	QQA51	(877) 862-8655
TMC COMMUNICATIONS	QQA52	(877) 862-8655
TMC COMMUNICATIONS	QQA53	(877) 862-8655

TMC COMMUNICATIONS	QQA54	(877) 862-8655
TMC COMMUNICATIONS	QQA55	(877) 862-8655
TMC COMMUNICATIONS	QQA56	(877) 862-8655
TMC COMMUNICATIONS	QQA57	(877) 862-8655
TMC COMMUNICATIONS	QQA58	(877) 862-8655
TMC COMMUNICATIONS	QQA59	(877) 862-8655
TMC COMMUNICATIONS	QQA98	(877) 862-8655
TMC COMMUNICATIONS	QQA99	(866) 742-5862
GLOBALTRON COMMUNICATIONS CORP	QRS01	(888) 465-3731
PHONE 1	QRS99	(888) 465-3731
QUESTAR INFOCOMM, INC.	QST01	(801) 324-1960
QUESTAR INFOCOMM, INC.	QST99	(801) 799-2959
SOUTHERN TELECOM NETWORK INC	QTY01	(870) 404-7090
SOUTHERN TELECOM NETWORK INC	QTY99	(870) 404-7090
TELEPERFORMANCE INTERACTIVE	QVF01	(610) 941-1000
TELEPERFORMANCE INTERACTIVE	QVF99	(610) 941-1000
CLEAREND, LLC	QXP01	(646) 473-2404
CLEAREND, LLC	QXP99	(646) 473-2404
RESP-ORG.COM	QZA01	(800) 627-5383
RESP-ORG.COM	QZA99	(800) 327-5383
RINGCENTRAL INC.	RBI01	(800) 725-2730
RINGCENTRAL, INC.	RBI99	(650) 472-3670
GLOBAL CROSSING	RCI01	(800) 783-2020
GLOBAL CROSSING	RCI99	(800) 783-2020
GLOBAL CROSSING	RCMAD	(800) 783-2020
GLOBAL CROSSING	RCM99	(800) 783-2020
GLOBAL CROSSING	RCNDL	(800) 466-4600
GLOBAL CROSSING	RCNTE	(800) 724-3499
GLOBAL CROSSING	RCN99	(800) 783-2020
GLOBAL CROSSING	RCSM1	(800) 783-2020
GLOBAL CROSSING	RCUSW	(800) 783-2020
GLOBAL CROSSING	RCU99	(800) 783-2020
GLOBAL CROSSING	RCVST	(800) 783-2020

GLOBAL CROSSING	RCV99	(800) 783-2020
RADIANT TELECOM	RDT01	(305) 914-3381
RADIANT TELECOM	RDT02	(305) 914-3541
RADIANT TELECOM	RDT99	(305) 914-3454
BAK COMMUNICATIONS LLC	RFF01	(213) 688-8838
BAK COMMUNICATIONS LLC	RFF99	(213) 688-8838
RESPORG SOLUTIONS	RHL01	(904) 318-7271
RESPORG SOLUTIONS	RHL99	(904) 318-7271
RNK TELECOM, INC	RJT01	(781) 382-0124
RNK TELECOM, INC	RJT99	(781) 382-0124
ILD TELECOM, INC.	RMI01	(800) 743-1003
ILD TELECOM, INC.	RMI99	(800) 743-1003
RURAL CELLULAR CORP	RNI01	(320) 808-2135
RCC NETWORK INC.	RNI99	(320) 808-2135
ROLINIUM	ROL01	(718) 609-9700
ROLINIUM	ROL99	(718) 609-9700
TELESCAN, INC.	RPT01	(423) 282-5043
TELESCAN, INC.	RPT99	(423) 282-5043
REMI COMMUNICATIONS	RRC01	(724) 836-5800
REMI COMMUNICATIONS	RRC99	(724) 836-5800
ACCESSLINE COMM. CORP.	RSA01	(877) 880-0055
ACCESSLINE COMMUNICATIONS	RSA22	(206) 654-9904
ACCESSLINE COMM. CORP.	RSA99	(206) 621-3523
POINT TELECOM INC	RTI01	(818) 348-4466
POINT TELECOM, INC.	RTI99	(818) 348-4466
#EMPTY	RTX01	(800) 704-6363
WORLD WIDE TELEGRAPH	RUC01	(877) 272-2576
WORLD WIDE TELEGRAPH	RUC22	(877) 272-2576
WORLD WIDE TELEGRAPH	RUC25	(877) 272-2576
WORLD WIDE TELEGRAPH	RUC99	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN01	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN02	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN03	(877) 272-2576

WORLDWIDE TELEGRAPH	RUN04	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN05	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN06	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN07	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN08	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN09	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN10	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN11	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN12	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN13	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN14	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN15	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN16	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN17	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN18	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN19	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN20	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN21	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN22	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN23	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN24	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN25	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN26	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN27	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN28	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN29	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN30	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN31	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN32	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN33	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN34	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN35	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN36	(877) 272-2576

WORLDWIDE TELEGRAPH	RUN37	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN38	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN39	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN40	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN41	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN42	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN43	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN44	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN45	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN46	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN47	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN48	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN49	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN50	(877) 272-2576
FREEDOMVOICE SYSTEMS	RVE01	(858) 699-5312
FREEDOMVOICE SYSTEMS	RVE99	(858) 699-5312
R.W.LYNCH COMPANY INC	RWL01	(925) 837-3877
R. W. LYNCH COMPANY INC	RWL99	(925) 837-3877
I ELEMENT INC.	RXD01	(214) 254-3480
I ELEMENT INC.	RXD99	(214) 254-3480
BRAND800.COM	RYT01	(800) 214-4100
BRAND800.COM	RYT99	(800) 214-4100
#EMPTY	SBTST	(214) 454-6262
SWITCH 2000, INC.	SCT01	(507) 385-2363
SWITCH 2000, INC.	SCT99	(507) 385-2363
GLOBAL CROSSING	SDR01	(800) 783-2020
GLOBAL CROSSING	SDR99	(800) 783-2020
SELECTIVE MEDIA	SEM01	(415) 543-9033
SELECTIVE MEDIA	SEM99	(415) 543-9033
STATE FARM INSURANCE	SFI01	(309) 766-2233
STATE FARM INSURANCE	SFI99	(309) 766-1220
SCHERERS COMM. GROUP INC.	SGI01	(614) 841-2421
SCHERERS COMM. GROUP INC.	SGI99	(800) 356-6161

SBC	SHOC1	(214) 464-3308
SBC	SHOPR	(214) 464-3308
SBC	SHSE1	(214) 464-3308
SBC	SHSM1	(214) 464-3308
SBC	SHSWA	(214) 454-6262
SBC	SHSWD	(214) 454-6262
SBC	SHSW0	(214) 464-3308
SBC	SHSW1	(800) 286-8313
SBC	SHSW3	(214) 454-6262
SBC	SHSW6	(800) 286-8313
SOUTHWESTERN BELL CORP.	SHW99	(800) 286-8313
ITC DELTACOM	SIDLT	(800) 239-3000
ITC DELTACOM	SID99	(800) 239-3000
ITC DELTACOM	SIR01	(800) 240-0000
MARATHON COMMUNICATIONS	SJS01	(800) 919-1000
MARATHON COMMUNICATIONS	SJS99	(800) 919-1000
MERCANTEL COMMUNICATIONS, LP	SKV01	(800) 761-6713
MARCANTEL COMMUNICATIONS,LP	SKV99	(800) 761-6713
STARTEC GLOBAL COMMUNICATIONS	SMG01	(301) 610-4422
STARTEC GLOBAL COMMUNICATIONS	SMG99	(301) 610-4422
SOUTHERN NE TELEPHONE	SNETT	(203) 420-3131
SOUTHERN NE TELEPHONE	SNET1	(203) 420-3131
SOUTHERN NEW ENGLAND TELEPHONE	SNET2	(203) 420-3131
SOUTHERN NEW ENGLAND TELEPHONE	SNET3	(203) 420-3131
SOUTHERN NE TELEPHONE	SNE99	(203) 420-3131
SOUTHERN NE TELEPHONE	SNSM1	(203) 420-3131
SIGNAL ONE, INC	SOE01	(904) 280-5353
SIGNAL ONE, INC.	SOE99	(904) 247-9900
SPRINT COMMUNICATIONS CO. LP	SPBG1	(800) 795-1004
SPRINT COMMUNICATIONS CO. LP	SPBS1	(800) 795-1004
SPRINT COMMUNICATIONS CO. LP	SPBS2	(800) 795-1004
SPRINT COMMUNICATIONS CO. LP	SPBS3	(800) 795-1004
SPRINT COMMUNICATIONS CO. LP	SPBS4	(800) 795-1004

SPRINT COMMUNICATIONS CO. LP	SPBS5	(800) 795-1004
SPRINT COMMUNICATIONS CO. LP	SPCG1	(800) 877-4646
SPRINT COMMUNICATIONS CO. LP	SPDG3	(800) 795-1004
SPRINT COMMUNICATIONS CO. LP	SPFN1	(800) 795-1004
SPRINT COMMUNICATIONS CO. LP	SPGD1	(800) 795-1004
SPRINT COMMUNICATIONS CO. LP	SPGD2	(800) 795-1004
SPRINT COMMUNICATIONS CO. LP	SPHG1	(800) 786-5050
SPRINT COMMUNICATIONS CO. LP	SPIC1	(800) 795-1004
SPRINT COMMUNICATIONS CO. LP	SPNYN	(888) 696-3939
SPRINT COMMUNICATIONS CO. LP	SPR01	(800) 795-1004
SPRINT COMMUNICATIONS CO. LP	SPR99	(800) 795-1004
SPRINT COMMUNICATIONS CO. LP	SPSC1	(800) 600-1186
SPRINT COMMUNICATIONS CO. LP	SPSI1	(800) 795-1004
SPRINT COMMUNICATIONS CO. LP	SPST1	(800) 366-0707
SPRINT COMMUNICATIONS CO. LP	SPS01	(800) 795-1004
SPRINT COMMUNICATIONS CO. LP	SPS51	(800) 795-1004
INFORMATION TELCO SERVICES INC	SQC01	(847) 501-0472
INFORMATION TELCO SERVICES INC	SQC99	(408) 934-1787
GLOBAL CROSSING	SRC01	(800) 783-2020
GLOBAL CROSSING	SRC99	(800) 783-2020
ACCESS SERVICES, INC.	SVS01	(877) 256-6512
ACCESS SERVICES, INC.	SVS99	(877) 256-6512
CORDIA COMMUNICATIONS	SYS01	(877) 985-9900
CORDIA COMMUNICATIONS	SYS99	(877) 835-9900
TELEFONICA LARGA DISTANCIA	TFC01	(800) 496-3116
TELEFONICA LARGA DISTANCIA	TFC99	(800) 496-3116
POWERCOM CORPORATION	TGN01	(800) 444-4014
POWERCOM	TGN02	(800) 444-4014
POWERCOM CORPORATION	TGN99	(800) 444-4014
PRIMUS TELECOMMUNICATIONS	TIN01	(800) 899-1085
PRIMUS TELECOMMUNICATIONS INC	TIN02	(800) 899-1085
PRIMUS TELECOMMUNICATIONS INC	TIN03	(800) 899-1085
PRIMUS TELECOMMUNICATIONS	TIN04	(800) 899-1085

PRIMUS TELECOMMUNICATIONS	TIN05	(800) 899-1085
PRIMUS TELECOMMUNICATIONS	TIN06	(800) 899-1085
PRIMUS TELECOMMUNICATIONS	TIN07	(800) 899-1085
PRIMUS COMMUNICATIONS	TIN08	(800) 899-1085
PRIMUS COMMUNICATIONS	TIN09	(800) 899-1085
PRIMUS COMMUNICATIONS	TIN10	(800) 899-1085
PRIMUS TELECOMMUNICATIONS	TIN99	(800) 899-1085
TELESERVICES INC.	TJC01	(877) 870-8700
TELESERVICES INC.	TJC99	(877) 870-8700
TEL-AMERICA/UCN	TNT01	(866) 659-0000
TEL-AMERICA/UCN	TNT02	(866) 695-0000
TEL-AMERICA/UCN	TNT03	(866) 695-0000
TEL-AMERICA/UCN	TNT04	(866) 695-0000
TEL-AMERICA/UCN	TNT99	(866) 695-0000
COVISTA COMMUNICATION	TOT01	(800) 493-0800
COVISTA COMMUNICATION	TOT99	(800) 493-0800
TELECOM AFFILIATES	TSH01	(800) 754-1001
TELECOM AFFILIATES	TSH99	(800) 754-1001
BIRCH/IONEX TELECOMMUNICATIONS	TTH01	(800) 860-8401
IONEX COMM.	TTH02	(800) 234-2301
IONEX COMM.	TTH99	(800) 234-2301
EMERITUS COMMUNICATIONS	TUI01	(877) 835-2680
EMERITUS	TUI02	(877) 835-2680
EMERITUS COMMUNICATIONS	TUI99	(877) 835-2680
TELEQUEST	TVQ01	(816) 532-6015
TELEQUEST	TVQ99	(816) 532-6015
CAPSULE COMMUNICATIONS	UCW01	(800) 493-0800
CAPSULE COMMUNICATIONS	UCW99	(800) 493-0800
LIGHTYEAR/UNIDIAL COMM.	UDI01	(800) 393-7300
LIGHTYEAR/UNIDIAL COMM.	UDI02	(888) 864-7671
LIGHTYEAR/UNIDIAL COMM.	UDI99	(800) 393-7300
US LEC OF NC, LLC	UEC01	(800) 978-7532
US LEC	UEC02	(704) 319-1104

US LEC	UEC03	(704) 319-1104
US LEC	UEC04	(704) 319-1104
US LEC	UEC05	(704) 319-1104
US LEC	UEC06	(800) 978-7532
US LEC	UEC07	(800) 978-7532
US LEC	UEC08	(800) 978-7532
US LEC	UEC09	(800) 978-7532
US LEC	UEC10	(800) 978-7532
US LEC OF NC, LLC	UEC99	(800) 978-7532
TELESMART	UFO01	(503) 642-5569
TELESMART	UFO99	(503) 642-5569
AURIS TECHNOLOGY	UGO01	(305) 436-8486
AURIS TECHNOLOGY	UGO21	(305) 261-7778
AURIS TECHNOLOGY	UGO31	(305) 261-7778
AURIS TECHNOLOGY	UGO99	(305) 436-8486
US SOUTH COMMUNICATIONS	UHC01	(770) 240-6160
US SOUTH COMMUNICATIONS	UHC99	(770) 240-6160
VERISIGN INC (ILLUMINET)	UIN01	(800) 800-5443
ILLUMINET	UIN99	(800) 800-5443
TOLL FREE CONNECT INC	UKO01	(561) 802-4344
TOLL FREE CONNECT INC	UKO99	(561) 802-4344
QWEST/US WEST LONG DISTANCE	ULD01	(720) 540-1123
QWEST IT	ULD02	(800) 573-1311
QWEST/US WEST LONG DISTANCE	ULD99	(888) 878-5301
TRICOM USA	UMS01	(809) 334-7397
TRICOM USA	UMS99	(809) 334-7397
UNION TELEPHONE	UNT01	(307) 782-6131
UNION TELEPHONE	UNT99	(307) 782-6131
TDS METROCOM	USL01	(218) 568-4000
US LINK INC.	USL99	(218) 568-4000
CHOICE ONE COMMUNICATIONS	UUS01	(888) 493-7300
CHOICE ONE COMMUNICATIONS	UUS99	(616) 493-7028
QWEST/USWEST	UWMSA	(888) 826-0748

QWEST/US WEST	UWMST	(888) 826-0748
QWEST/US WEST	UWMS1	(888) 826-0748
QWEST/US WEST	UWM99	(800) 688-6102
QWEST/US WEST	UWNS1	(800) 688-6102
QWEST/US WEST	UWNWA	(800) 688-6102
QWEST/US WEST	UWNW1	(800) 443-3646
QWEST/US WEST	UWPN1	(800) 443-3646
QWEST/US WEST	UWSE1	(800) 443-3646
QWEST/US WEST	UWSM1	(800) 443-3646
ALLSTREAM	UXC01	(866) 282-0111
AT&T CANADA	UXC02	(866) 282-0111
ALLSTREAM	UXC99	(866) 282-0111
UTEL NETWORKS	UYT01	(877) 883-5638
UTEL NETWORKS	UYT02	(877) 883-5638
UTEL NETWORKS	UYT99	(877) 883-5638
UNITEL COMMUNICATIONS GROUP IN	UZL01	(800) 499-5912
UNITEL COMMUNICATIONS GROUP IN	UZL99	(800) 499-5912
VANITY INTERNATIONAL	VAN01	(858) 792-5000
VANITY INTERNATIONAL	VAN99	(858) 792-5000
BIRCH/IONEX TELECOMMUNICATIONS	VDL01	(800) 860-8401
IONEX TELECOMMUNICATIONS	VDL99	(800) 333-1124
RESPORG USA INC.	VGf01	(626) 940-0566
RESPORG USA INC.	VGf99	(626) 940-0566
CUSTOM TELECONNECT INC	VJC01	(702) 922-5225
CUSTOM TELECONNECT INC	VJC99	(702) 922-5225
BIRCH TELECOM	VLK01	(800) 860-8401
BIRCH TELECOM	VLK99	(316) 343-7071
GOTVMAIL COMMUNICATIONS	VML01	(888) 431-6800
GOTVMAIL COMMUNICATIONS	VML99	(617) 454-1256
VPT, INC.	VPT01	(512) 419-4600
VPT, INC.	VPT99	(512) 419-4600
VARTEC TELECOM	VRT01	(888) 702-4079
VARTEC TELECOM	VRT99	(888) 702-4079

CAPITAL TELECOMM	VST01	(800) 569-5185
CAPITAL TELECOMMUNICATIONS INC	VST05	(717) 815-6321
CAPITAL TELECOMMUNICATIONS INC	VST10	(717) 815-6321
CAPITAL TELECOMMUNICATIONS INC	VST15	(717) 815-6321
CAPITAL TELECOMMUNICATIONS INC	VST20	(717) 815-6321
CAPITAL TELECOMMUNICATIONS INC	VST25	(717) 815-6321
CAPITAL TELECOMMUNICATIONS INC	VST55	(717) 848-8800
CAPITAL TELECOMMUNICATIONS INC	VST66	(717) 848-8800
CAPITAL TELECOMMUNICATIONS INC	VST77	(717) 848-8800
CAPITAL TELECOMMUNICATIONS INC	VST88	(717) 848-8800
CAPITAL TELECOMM	VST99	(800) 569-5185
TELVUE CORP.	VUE01	(856) 273-8888
TELVUE CORP.	VUE99	(856) 273-8888
VIDEOTRON TELECON LTE'E	VVT01	(514) 380-4619
VIDEOTRON TELECON LTE'E	VVT99	(514) 380-4619
VOXEO CORPORATION	VXML1	(407) 835-0065
VOXEO CORPORATION	VXM99	(407) 835-0065
VERIZON SELECT SERVICES, INC.	VZR01	(800) 483-3722
VERIZON SELECT SERVICES, INC.	VZR99	(800) 483-3722
GLOBAL CROSSING	WCU01	(800) 783-2020
GLOBAL CROSSING	WCU99	(800) 783-2020
NATIONWIDE 800	WDE01	(602) 944-1210
NATIONWIDE 800	WDE99	(602) 944-1210
WESTEL, INC.	WES01	(512) 480-5500
WESTEL, INC.	WES99	(512) 480-5500
US PHONECOM, INC	WFF01	(818) 840-6969
US PHONECOM, INC	WFF99	(818) 840-6969
WHO'S CALLING INC.	WHO01	(800) 621-6871
WHO'S CALLING, INC.	WHO02	(800) 621-6871
WHO'S CALLING, INC.	WHO03	(800) 621-6871
WHO'S CALLING, INC.	WHO04	(800) 621-6871
WHO'S CALLING, INC.	WHO05	(800) 621-6871
WHO'S CALLING, INC.	WHO06	(800) 621-6871

WHO'S CALLING, INC.	WHO07	(800) 621-6871
WHO'S CALLING, INC.	WHO08	(800) 621-6871
WHO'S CALLING, INC.	WHO09	(800) 621-6871
WHO'S CALLING, INC.	WHO10	(800) 621-6871
WHOS CALLING INC	WHO11	(800) 621-6871
WHOS CALLING INC	WHO12	(800) 621-6871
WHOS CALLING INC	WHO13	(800) 621-6871
WHOS CALLING INC	WHO14	(800) 621-6871
WHOS CALLING INC	WHO15	(800) 621-6871
WHOS CALLING INC	WHO16	(800) 621-6871
WHOS CALLING INC	WHO17	(800) 621-6871
WHOS CALLING INC	WHO18	(800) 621-6871
WHOS CALLING INC	WHO19	(800) 621-6871
WHOS CALLING INC	WHO20	(800) 621-6871
WHOS CALLING INC	WHO21	(800) 621-6871
WHOS CALLING INC	WHO22	(800) 621-6871
WHOS CALLING INC	WHO23	(800) 621-6871
WHOS CALLING INC	WHO24	(800) 621-6871
WHOS CALLING INC	WHO25	(800) 621-6871
WHOS CALLING INC	WHO26	(800) 621-6871
WHOS CALLING INC	WHO27	(800) 621-6871
WHOS CALLING INC	WHO28	(800) 621-6871
WHOS CALLING INC	WHO29	(800) 621-6871
WHOS CALLING INC	WHO30	(800) 621-6871
WHOS CALLING INC	WHO31	(800) 621-6871
WHOS CALLING INC	WHO32	(800) 621-6871
WHOS CALLING INC	WHO33	(800) 621-6871
WHOS CALLING INC	WHO34	(800) 621-6871
WHOS CALLING INC	WHO35	(800) 621-6871
WHOS CALLING INC	WHO36	(800) 621-6871
WHOS CALLING INC	WHO37	(800) 621-6871
WHOS CALLING INC	WHO38	(800) 621-6871
WHOS CALLING INC	WHO39	(800) 621-6871

WHOS CALLING INC	WHO40	(800) 621-6871
WHOS CALLING INC	WHO41	(800) 621-6871
WHOS CALLING INC	WHO42	(800) 621-6871
WHOS CALLING INC	WHO43	(800) 621-6871
WHOS CALLING INC	WHO44	(800) 621-6871
WHOS CALLING INC	WHO45	(800) 621-6871
WHOS CALLING INC	WHO46	(800) 621-6871
WHOS CALLING INC	WHO47	(800) 621-6871
WHOS CALLING INC	WHO48	(800) 621-6871
WHOS CALLING INC	WHO49	(800) 621-6871
WHOS CALLING INC	WHO50	(800) 621-6871
WHOS CALLING INC	WHO51	(800) 621-6871
WHOS CALLING INC	WHO52	(800) 621-6871
WHOS CALLING INC	WHO53	(800) 621-6871
WHOS CALLING INC	WHO54	(800) 621-6871
WHOS CALLING INC	WHO55	(800) 621-6871
WHOS CALLING INC	WHO56	(800) 621-6871
WHOS CALLING INC	WHO57	(800) 621-6871
WHOS CALLING INC	WHO58	(800) 621-6871
WHOS CALLING INC	WHO59	(800) 621-6871
WHOS CALLING INC	WHO60	(800) 621-6871
WHOS CALLING INC	WHO61	(800) 621-6871
WHOS CALLING INC	WHO62	(800) 621-6871
WHOS CALLING INC	WHO63	(800) 621-6871
WHOS CALLING INC	WHO64	(800) 621-6871
WHOS CALLING INC	WHO65	(800) 621-6871
WHOS CALLING INC	WHO66	(800) 621-6871
WHOS CALLING INC	WHO67	(800) 621-6871
WHOS CALLING INC	WHO68	(800) 621-6871
WHOS CALLING INC	WHO69	(800) 621-6871
WHOS CALLING INC	WHO70	(800) 621-6871
WHOS CALLING INC	WHO71	(800) 621-6871
WHOS CALLING INC	WHO72	(800) 621-6871

WHOS CALLING INC	WHO73	(800) 621-6871
WHOS CALLING INC	WHO74	(800) 621-6871
WHOS CALLING INC	WHO75	(800) 621-6871
WHOS CALLING INC	WHO76	(800) 621-6871
WHOS CALLING INC	WHO77	(800) 621-6871
WHOS CALLING INC	WHO78	(800) 621-6871
WHOS CALLING INC	WHO79	(800) 621-6871
WHOS CALLING INC	WHO80	(800) 621-6871
WHOS CALLING INC	WHO81	(800) 621-6871
WHOS CALLING INC	WHO82	(800) 621-6871
WHOS CALLING INC	WHO83	(800) 621-6871
WHOS CALLING INC	WHO84	(800) 621-6871
WHOS CALLING INC	WHO85	(800) 621-6871
WHOS CALLING INC	WHO86	(800) 621-6871
WHOS CALLING INC	WHO87	(800) 621-6871
WHOS CALLING INC	WHO88	(800) 621-6871
WHOS CALLING INC	WHO89	(800) 621-6871
WHOS CALLING INC	WHO90	(800) 621-6871
WHOS CALLING INC	WHO91	(800) 621-6871
WHOS CALLING INC	WHO92	(800) 621-6871
WHOS CALLING INC	WHO93	(800) 621-6871
WHOS CALLING INC	WHO94	(800) 621-6871
WHOS CALLING INC	WHO95	(800) 621-6871
WHOS CALLING INC	WHO96	(800) 621-6871
WHOS CALLING INC	WHO97	(800) 621-6871
WHOS CALLING INC	WHO98	(800) 621-6871
WHO'S CALLING, INC.	WHO99	(800) 621-6871
MCI NETWORK SERVICES, INC.	WILSB	(800) 828-4984
MCI NETWORK SERVICES, INC.	WIL01	(800) 828-4984
MCI NETWORK SERVICES, INC.	WIL04	(800) 828-4984
MCI NETWORK SERVICES, INC.	WIL20	(800) 828-4984
MCI NETWORK SERVICES, INC	WIL99	(800) 828-4984
GRANITE TELECOMMUNICATIONS LLC	WKE01	(866) 847-5500

GRANITE TELECOMMUNICATIONS LLC	WKE99	(866) 847-5500
WHOLESALE CARRIER SERVICES INC	WLS01	(954) 227-1700
WHOLESALE CARRIER SERVICES INC	WLS99	(954) 227-1700
WARNING COMMUNICATIONS, INC.	WNM01	(602) 230-0420
WARNING COMMUNICATIONS, INC	WNM02	(602) 230-0420
WARNING COMMUNICATIONS, INC.	WNM99	(800) 746-6396
WORD OF MOUTH COMMUNICATIONS	WOM01	(847) 926-4444
WORD OF MOUTH COMMUNICATIONS	WOM99	(847) 272-7737
ACCERIS SOLUTIONS	WST01	(800) 447-2111
ACCERIS SOLUTIONS	WST99	(800) 447-2111
WAKE UP INC.	WUP01	(404) 365-0800
WAKE UP INC.	WUP99	(404) 365-0800
ANPI	WWT01	(217) 698-3023
ANPI	WWT99	(217) 698-3023
WCI	WXI01	(206) 652-4470
WORLD COMMUNICATIONS INC	WXI99	(206) 652-4470
MBI SERVICES GRP LLC	WZD01	(941) 586-5694
MBI SERVICES GRP LLC	WZD99	(641) 586-5694
GABRIEL WIRELESS LLC	YGW01	(561) 999-0999
GABRIEL WIRELESS LLC	YGW99	(561) 999-0999
THEBESTNUMBERS.COM	YHN01	(888) 888-8585
THEBESTNUMBERS.COM	YHN02	(888) 888-8585
THEBESTNUMBERS.COM	YHN03	(888) 888-8585
THEBESTNUMBERS.COM	YHN04	(888) 888-8585
THEBESTNUMBERS.COM	YHN05	(888) 888-8585
THEBESTNUMBERS.COM	YHN06	(888) 888-8585
THEBESTNUMBERS.COM	YHN07	(888) 888-8585
THEBESTNUMBERS.COM	YHN08	(888) 888-8585
THEBESTNUMBERS.COM	YHN09	(888) 888-8585
THEBESTNUMBERS.COM	YHN10	(888) 888-8585
THEBESTNUMBERS.COM	YHN11	(888) 888-8585
THEBESTNUMBERS.COM	YHN12	(888) 888-8585
THEBESTNUMBERS.COM	YHN13	(888) 888-8585

THEBESTNUMBERS.COM	YHN14	(888) 888-8585
THEBESTNUMBERS.COM	YHN15	(888) 888-8585
THEBESTNUMBERS.COM	YHN16	(888) 888-8585
THEBESTNUMBERS.COM	YHN17	(888) 888-8585
THEBESTNUMBERS.COM	YHN18	(888) 888-8585
THEBESTNUMBERS.COM	YHN19	(888) 888-8585
THEBESTNUMBERS.COM	YHN20	(888) 888-8585
THEBESTNUMBERS.COM	YHN99	(888) 888-8585
TELCO GROUP, INC	YOU01	(888) 844-5390
TELCO GROUP INC	YOU02	(888) 844-5390
TELCO GROUP INC.	YOU03	(888) 844-5390
TELCO GROUP, INC	YOU99	(888) 844-5390
MCLEOD USA/CAPROCK	YSG01	(800) 687-1600
MCLEOD USA/CAPROCK	YSG99	(800) 687-1600
NOBEL TEL LLC	YUI01	(760) 405-0105
NOBEL TEL LLC	YUI99	(760) 405-0105
XTEL COMMUNICATIONS	YXT01	(856) 596-4000
XTEL COMMUNICATIONS	YXT99	(856) 596-7000
TEXAS COMMUNICATIONS	YYT01	(325) 658-3566
TEXAS COMMUNICATIONS	YYT99	(915) 658-3566
SMS/800 HELP DESK TRAINING	ZATST	(888) 767-3300
Z-TEL NETWORK SERVICES	ZNS01	(813) 233-4554
Z-TEL NETWORK SERVICES	ZNS02	(813) 233-4554
Z-TEL NETWORK SERVICES	ZNS03	(813) 233-4554
Z-TEL NETWORK SERVICES	ZNS04	(813) 233-4554
Z-TEL NETWORK SERVICES	ZNS05	(813) 233-4554
Z-TEL NETWORK SERVICES	ZNS99	(813) 262-3226
PSEUDO ENTITY 0110	0AXXX	(888) 767-3300
PSEUDO ENITY 0110	1AXXX	(888) 767-3300
PSEUDO ENTITY 0110	2AXXX	(888) 767-3300
PSEUDO ENTITY 0110	3AXXX	(888) 767-3300
PSEUDO ENTITY 0110	4AXXX	(888) 767-3300
PSEUDO ENTITY 0110	5AXXX	(888) 767-3300

6.2 Sorted by Resp Org Name

Resp Org Name	Resp Org ID	Trouble Referral Number
#EMPTY	AMLBA	(800) 956-7000
#EMPTY	ART04	(732) 356-6999
#EMPTY	BRZXX	(888) 767-3300
#EMPTY	BTI99	#EMPTY
#EMPTY	BTS99	(800) 849-9100
#EMPTY	RTX01	(800) 704-6363
#EMPTY	SBTST	(214) 454-6262
(RCC) ATLANTIC	AQC99	(802) 654-5083
1-800 CONTACTS, INC	MRG99	(801) 316-7878
1-800 CONTACTS, INC.	MRG01	(801) 316-7878
1800FORINFO	FHT01	(561) 243-6968
1800FORINFO	FHT99	(561) 243-6968
24-7-365, INC.	JGL01	(310) 738-2500
24-7-365, INC.	JGL99	(310) 738-2500
800 IDEAS.COM, INC.	JON01	(858) 565-4000
800 IDEAS.COM, INC.	JON99	(858) 565-4000
800 RESPONSE INFORMATION	LPS01	(802) 860-0378
800 RESPONSE INFORMATION	LPS99	(802) 860-0378
ABCO COMMUNICATIONS INC.	ABC01	(707) 887-7994
ABCO COMMUNICATIONS INC.	ABC99	(800) 275-2226
ACCERIS COMMUNICATIONS PARTNER	CMT01	(800) 576-7775
ACCERIS SOLUTIONS	WST01	(800) 447-2111
ACCERIS SOLUTIONS	WST99	(800) 447-2111
ACCESS POINT INC	EHT03	(919) 851-4838
ACCESS POINT INC	EHT04	(919) 851-4838
ACCESS POINT INC	EHT06	(919) 851-4838
ACCESS POINT INC	EHT07	(919) 851-4838
ACCESS POINT INC.	EHT01	(919) 851-4838
ACCESS POINT INC.	EHT02	(919) 851-4838

ACCESS POINT INC.	EHT99	(919) 851-4838
ACCESS POINT, INC	EHT05	(919) 851-4833
ACCESS POINT, INC	EHT08	(919) 851-4838
ACCESS SERVICES, INC.	SVS01	(877) 256-6512
ACCESS SERVICES, INC.	SVS99	(877) 256-6512
ACCESSLINE COMM. CORP.	RSA01	(877) 880-0055
ACCESSLINE COMM. CORP.	RSA99	(206) 621-3523
ACCESSLINE COMMUNICATIONS	RSA22	(206) 654-9904
ADEPTEL, INC.	DPT01	(407) 682-3022
ADEPTEL, INC.	DPT99	(407) 682-3022
ADVANCED COMMUNICATIONS INTEGR	HFG01	(714) 986-9666
ADVANCED COMMUNICATIONS INTEGR	HFG99	(714) 986-9666
ADVANCED ROUTING TECH.	ART01	(732) 356-6999
ADVANCED ROUTING TECH.	ART99	(732) 356-6999
ADVANCED ROUTING TECHNOLOGIES	ART05	(732) 356-6999
ADVANCED TEL, INC.	EET01	(800) 621-4211
ADVANCED TEL, INC.	EET99	(877) 621-4167
AIRESPRING INC	KDB01	(888) 899-2789
AIRESPRING INC	KDB99	(888) 899-2789
ALASCOM INC.	AAM01	(907) 264-8363
ALASCOM INC.	AAM99	(907) 264-8363
ALLERGAN SALES LLC	HYT01	(714) 246-4579
ALLERGAN SALES LLC	HYT99	(704) 246-4579
ALLIANCE GROUP SERVICES	GRP02	(203) 221-8700
ALLIANCE GROUP SERVICES INC	GRP01	(203) 221-8700
ALLIANCE GROUP SERVICES INC	GRP99	(203) 845-9600
ALLIANCE GROUP SERVICES, INC.	GRP06	(203) 221-8700
ALLINACE GROUP SERVICES	GRP03	(203) 221-8700
ALLINACE GROUP SERVICES	GRP04	(203) 221-8700
ALLINACE GROUP SERVICES	GRP05	(203) 221-8700
ALLSTATE COMMUNICATIONS	AYL01	(818) 598-1570
ALLSTATE COMMUNICATIONS	AYL99	(818) 598-1570
ALLSTREAM	AZC01	(866) 282-0111

ALLSTREAM	AZC99	(866) 282-0111
ALLSTREAM	UXC01	(866) 282-0111
ALLSTREAM	UXC99	(866) 282-0111
AMAX TWO	MXT01	(208) 475-6021
AMAX TWO	MXT99	(207) 475-6021
AMERICAN LONG LINES	ASL01	(215) 442-9700
AMERICAN LONG LINES	ASL99	(215) 442-9700
AMERITECH SERVICES	AMLBT	(800) 956-7000
AMERITECH SERVICES	AMLB1	(800) 956-7000
AMERITECH SERVICES	AML01	(800) 956-7000
AMERITECH SERVICES	AMMBA	(800) 956-7000
AMERITECH SERVICES	AMMB1	(800) 956-7000
AMERITECH SERVICES	AMNBA	(800) 956-7000
AMERITECH SERVICES	AMNB1	(800) 956-7000
AMERITECH SERVICES	AMNS2	(800) 956-7000
AMERITECH SERVICES	AM0BA	(800) 956-7000
AMERITECH SERVICES	AM0BT	#EMPTY
AMERITECH SERVICES	AM0B1	(800) 956-7000
AMERITECH SERVICES	AMSE1	(800) 956-7000
AMERITECH SERVICES	AMSM1	(800) 956-7000
AMERITECH SERVICES	AMT01	(800) 956-7000
AMERITECH SERVICES	AMWT1	(800) 956-7000
AMERVISION COMM., INC.	APV01	(405) 600-3605
AMERVISION COMM., INC.	APV99	(405) 600-3605
AMRIGON INC.	AON01	(248) 332-2300
AMRIGON INC.	AON99	(248) 332-2300
AMTEC	JZJ01	(310) 766-2220
AMTEC	JZJ02	(310) 766-2222
AMTEC	JZJ03	(310) 766-2222
AMTEC	JZJ04	(310) 766-2222
AMTEC	JZJ05	(310) 766-2222
AMTEC	JZJ06	(310) 766-2222
AMTEC	JZJ07	(310) 766-2222

AMTEC	JZJ08	(310) 766-2222
AMTEC	JZJ09	(310) 766-2222
AMTEC	JZJ10	(310) 766-2222
AMTEC	JZJ11	(310) 766-2222
AMTEC	JZJ12	(310) 766-2222
AMTEC	JZJ13	(310) 766-2222
AMTEC	JZJ14	(310) 766-2222
AMTEC	JZJ15	(310) 766-2222
AMTEC	JZJ16	(310) 766-2222
AMTEC	JZJ17	(310) 766-2222
AMTEC	JZJ18	(310) 766-2222
AMTEC	JZJ19	(310) 766-2222
AMTEC	JZJ20	(310) 766-2222
AMTEC	JZZ01	(310) 766-2222
AMTEC	JZZ99	(310) 766-2222
ANDIAMO TELECOM	DKT01	(602) 344-0115
ANIDAMO TELECOM	DKT99	(602) 344-0115
ANI-NETWORKS	GDG01	(702) 547-8786
ANPI	WWT01	(217) 698-3023
ANPI	WWT99	(217) 698-3023
AT&T	ATX01	(800) 222-3000
AT&T	ATX02	(800) 435-7375
AT&T	ATX03	(800) 248-1905
AT&T	ATX04	(800) 248-1903
AT&T	ATX06	(800) 222-3000
AT&T	ATX07	(800) 222-3000
AT&T	ATX09	(800) 222-3000
AT&T	ATX30	(800) 222-3000
AT&T	ATX40	(800) 222-3000
AT&T	ATX99	(800) 222-3000
AT&T CANADA	UXC02	(866) 282-0111
AT&T LOCAL NETWORK SERVICES	EAC01	(800) 544-6317
AT&T LOCAL NETWORK SERVICES	EAC99	(800) 544-6317

AT&T LONG DISTANCE	AWCC1	(877) 973-7767
AT&T LONG DISTANCE	AWCC2	(877) 973-7767
AT&T LONG DISTANCE	AWCC3	(877) 973-7767
AT&T LONG DISTANCE	AWCC4	(877) 973-7767
AT&T LONG DISTANCE	AWCC5	(877) 973-7767
AT&T LONG DISTANCE	AWC01	(877) 973-7767
AT&T LONG DISTANCE	AWC99	(877) 973-7767
AT&T LONG DISTANCE	AWLD1	(877) 973-7767
AT&T LONG DISTANCE	AWMM1	(877) 973-7767
AT&T LONG DISTANCE	AWREG	(877) 973-7767
AT; COMMUNICATIONS	AUB05	(800) 508-5200
ATG	OKB01	(800) 832-1754
ATG	OKB02	(800) 832-0754
ATG	OKB99	(480) 688-5760
ATL COMMUNICATIONS	AUA01	(800) 508-5200
ATL COMMUNICATIONS	AUA02	(800) 508-5200
ATL COMMUNICATIONS	AUA03	(800) 508-5200
ATL COMMUNICATIONS	AUA04	(800) 508-5200
ATL COMMUNICATIONS	AUA05	(800) 508-5200
ATL COMMUNICATIONS	AUA06	(800) 508-5200
ATL COMMUNICATIONS	AUA07	(800) 508-5200
ATL COMMUNICATIONS	AUA08	(800) 508-5200
ATL COMMUNICATIONS	AUA09	(800) 508-5200
ATL COMMUNICATIONS	AUA10	(800) 508-5200
ATL COMMUNICATIONS	AUA11	(800) 508-5200
ATL COMMUNICATIONS	AUA12	(800) 508-5200
ATL COMMUNICATIONS	AUA13	(800) 508-5200
ATL COMMUNICATIONS	AUA14	(800) 508-5200
ATL COMMUNICATIONS	AUA15	(800) 508-5200
ATL COMMUNICATIONS	AUA16	(800) 508-5200
ATL COMMUNICATIONS	AUA17	(800) 508-5200
ATL COMMUNICATIONS	AUA18	(800) 508-5200
ATL COMMUNICATIONS	AUA19	(800) 508-5200

ATL COMMUNICATIONS	AUA20	(800) 508-5200
ATL COMMUNICATIONS	AUA21	(800) 508-5200
ATL COMMUNICATIONS	AUA22	(800) 508-5200
ATL COMMUNICATIONS	AUA23	(800) 508-5200
ATL COMMUNICATIONS	AUA24	(800) 508-5200
ATL COMMUNICATIONS	AUA25	(800) 508-5200
ATL COMMUNICATIONS	AUA26	(800) 508-5200
ATL COMMUNICATIONS	AUA27	(800) 508-5200
ATL COMMUNICATIONS	AUA28	(800) 508-5200
ATL COMMUNICATIONS	AUA29	(800) 508-5200
ATL COMMUNICATIONS	AUA30	(800) 508-5200
ATL COMMUNICATIONS	AUA31	(800) 508-5200
ATL COMMUNICATIONS	AUA32	(800) 508-5200
ATL COMMUNICATIONS	AUA33	(800) 508-5200
ATL COMMUNICATIONS	AUA34	(800) 508-5200
ATL COMMUNICATIONS	AUA35	(800) 508-5200
ATL COMMUNICATIONS	AUA36	(800) 508-5200
ATL COMMUNICATIONS	AUA37	(800) 508-5200
ATL COMMUNICATIONS	AUA38	(800) 508-5200
ATL COMMUNICATIONS	AUA39	(800) 508-5200
ATL COMMUNICATIONS	AUA40	(800) 508-5200
ATL COMMUNICATIONS	AUA41	(800) 508-5200
ATL COMMUNICATIONS	AUA42	(800) 508-5200
ATL COMMUNICATIONS	AUA43	(800) 508-5200
ATL COMMUNICATIONS	AUA44	(800) 508-5200
ATL COMMUNICATIONS	AUA45	(800) 508-5200
ATL COMMUNICATIONS	AUA46	(800) 508-5200
ATL COMMUNICATIONS	AUA47	(800) 508-5200
ATL COMMUNICATIONS	AUA48	(800) 508-5200
ATL COMMUNICATIONS	AUA49	(800) 508-5200
ATL COMMUNICATIONS	AUA50	(800) 508-5200
ATL COMMUNICATIONS	AUA51	(800) 805-5200
ATL COMMUNICATIONS	AUA52	(800) 805-5200

ATL COMMUNICATIONS	AUA53	(800) 805-5200
ATL COMMUNICATIONS	AUA54	(800) 805-5200
ATL COMMUNICATIONS	AUA55	(800) 805-5200
ATL COMMUNICATIONS	AUA56	(800) 805-5200
ATL COMMUNICATIONS	AUA57	(800) 805-5200
ATL COMMUNICATIONS	AUA58	(800) 805-5200
ATL COMMUNICATIONS	AUA59	(800) 805-5200
ATL COMMUNICATIONS	AUA60	(800) 508-5200
ATL COMMUNICATIONS	AUA61	(800) 508-5200
ATL COMMUNICATIONS	AUA62	(800) 508-5200
ATL COMMUNICATIONS	AUA63	(800) 508-5200
ATL COMMUNICATIONS	AUA64	(800) 508-5200
ATL COMMUNICATIONS	AUA65	(800) 508-5200
ATL COMMUNICATIONS	AUA66	(800) 508-5200
ATL COMMUNICATIONS	AUA67	(800) 508-5200
ATL COMMUNICATIONS	AUA68	(800) 508-5200
ATL COMMUNICATIONS	AUA69	(800) 508-5200
ATL COMMUNICATIONS	AUA70	(800) 805-5200
ATL COMMUNICATIONS	AUA71	(800) 805-5200
ATL COMMUNICATIONS	AUA72	(800) 805-5200
ATL COMMUNICATIONS	AUA73	(800) 805-5200
ATL COMMUNICATIONS	AUA74	(800) 805-5200
ATL COMMUNICATIONS	AUA75	(800) 805-5200
ATL COMMUNICATIONS	AUA76	(800) 805-5200
ATL COMMUNICATIONS	AUA77	(800) 805-5200
ATL COMMUNICATIONS	AUA78	(800) 805-5200
ATL COMMUNICATIONS	AUA79	(800) 805-5200
ATL COMMUNICATIONS	AUA80	(800) 805-5200
ATL COMMUNICATIONS	AUA81	(800) 805-5200
ATL COMMUNICATIONS	AUA82	(800) 805-5200
ATL COMMUNICATIONS	AUA83	(800) 805-5200
ATL COMMUNICATIONS	AUA84	(800) 805-5200
ATL COMMUNICATIONS	AUA85	(800) 805-5200

ATL COMMUNICATIONS	AUA86	(800) 805-5200
ATL COMMUNICATIONS	AUA87	(800) 805-5200
ATL COMMUNICATIONS	AUA88	(800) 805-5200
ATL COMMUNICATIONS	AUA89	(800) 805-5200
ATL COMMUNICATIONS	AUA90	(800) 508-5200
ATL COMMUNICATIONS	AUA91	(800) 508-5200
ATL COMMUNICATIONS	AUA92	(800) 508-5200
ATL COMMUNICATIONS	AUA93	(800) 508-5200
ATL COMMUNICATIONS	AUA94	(800) 508-5200
ATL COMMUNICATIONS	AUA95	(800) 508-5200
ATL COMMUNICATIONS	AUA96	(800) 508-5200
ATL COMMUNICATIONS	AUA97	(800) 508-5200
ATL COMMUNICATIONS	AUA98	(800) 508-5200
ATL COMMUNICATIONS	AUA99	(800) 508-5200
ATL COMMUNICATIONS	AUB01	(800) 508-5200
ATL COMMUNICATIONS	AUB02	(800) 508-5200
ATL COMMUNICATIONS	AUB03	(800) 508-5200
ATL COMMUNICATIONS	AUB04	(800) 508-5200
ATL COMMUNICATIONS	AUB06	(800) 508-5200
ATL COMMUNICATIONS	AUB07	(800) 508-5200
ATL COMMUNICATIONS	AUB08	(800) 508-5200
ATL COMMUNICATIONS	AUB09	(800) 508-5200
ATL COMMUNICATIONS	AUB10	(800) 508-5200
ATL COMMUNICATIONS	AUB11	(800) 508-5200
ATL COMMUNICATIONS	AUB12	(800) 508-5200
ATL COMMUNICATIONS	AUB13	(800) 508-5200
ATL COMMUNICATIONS	AUB14	(800) 508-5200
ATL COMMUNICATIONS	AUB15	(800) 508-5200
ATL COMMUNICATIONS	AUB16	(800) 508-5200
ATL COMMUNICATIONS	AUB17	(800) 508-5200
ATL COMMUNICATIONS	AUB18	(800) 508-5200
ATL COMMUNICATIONS	AUB19	(800) 508-5200
ATL COMMUNICATIONS	AUB20	(800) 508-5200

ATL COMMUNICATIONS	AUB21	(800) 508-5200
ATL COMMUNICATIONS	AUB22	(800) 508-5200
ATL COMMUNICATIONS	AUB23	(800) 508-5200
ATL COMMUNICATIONS	AUB24	(800) 508-5200
ATL COMMUNICATIONS	AUB25	(800) 508-5200
ATL COMMUNICATIONS	AUB26	(800) 508-5200
ATL COMMUNICATIONS	AUB27	(800) 508-5200
ATL COMMUNICATIONS	AUB28	(800) 508-5200
ATL COMMUNICATIONS	AUB29	(800) 508-5200
ATL COMMUNICATIONS	AUN01	(800) 508-5200
ATL COMMUNICATIONS	AUN02	(800) 508-5200
ATL COMMUNICATIONS	AUN03	(800) 508-5200
ATL COMMUNICATIONS	AUN04	(800) 508-5200
ATL COMMUNICATIONS	AUN05	(800) 508-5200
ATL COMMUNICATIONS	AUN06	(800) 508-5200
ATL COMMUNICATIONS	AUN07	(800) 508-5200
ATL COMMUNICATIONS	AUN08	(800) 508-5200
ATL COMMUNICATIONS	AUN09	(800) 508-5200
ATL COMMUNICATIONS	AUN10	(800) 508-5200
ATL COMMUNICATIONS	AUN11	(800) 508-5200
ATL COMMUNICATIONS	AUN12	(800) 508-5200
ATL COMMUNICATIONS	AUN13	(800) 508-5200
ATL COMMUNICATIONS	AUN14	(800) 508-5200
ATL COMMUNICATIONS	AUN15	(800) 508-5200
ATL COMMUNICATIONS	AUN16	(805) 690-4198
ATL COMMUNICATIONS	AUN17	(800) 508-5200
ATL COMMUNICATIONS	AUN18	(800) 508-5200
ATL COMMUNICATIONS	AUN19	(800) 508-5200
ATL COMMUNICATIONS	AUN20	(800) 508-5200
ATL COMMUNICATIONS	AUN21	(800) 508-5200
ATL COMMUNICATIONS	AUN22	(800) 508-5200
ATL COMMUNICATIONS	AUN23	(800) 508-5200
ATL COMMUNICATIONS	AUN24	(800) 508-5200

ATL COMMUNICATIONS	AUN25	(800) 508-5200
ATL COMMUNICATIONS	AUN26	(800) 508-5200
ATL COMMUNICATIONS	AUN27	(800) 508-5200
ATL COMMUNICATIONS	AUN28	(800) 508-5200
ATL COMMUNICATIONS	AUN29	(800) 508-5200
ATL COMMUNICATIONS	AUN30	(800) 508-5200
ATL COMMUNICATIONS	AUN31	(800) 508-5200
ATL COMMUNICATIONS	AUN32	(800) 508-5200
ATL COMMUNICATIONS	AUN33	(800) 508-5200
ATL COMMUNICATIONS	AUN34	(800) 508-5200
ATL COMMUNICATIONS	AUN35	(800) 508-5200
ATL COMMUNICATIONS	AUN36	(800) 508-5200
ATL COMMUNICATIONS	AUN37	(800) 508-5200
ATL COMMUNICATIONS	AUN38	(800) 508-5200
ATL COMMUNICATIONS	AUN39	(800) 508-5200
ATL COMMUNICATIONS	AUN40	(800) 508-5200
ATL COMMUNICATIONS	AUN41	(800) 508-5200
ATL COMMUNICATIONS	AUN42	(800) 508-5200
ATL COMMUNICATIONS	AUN43	(800) 508-5200
ATL COMMUNICATIONS	AUN44	(800) 508-5200
ATL COMMUNICATIONS	AUN45	(800) 508-5200
ATL COMMUNICATIONS	AUN46	(800) 508-5200
ATL COMMUNICATIONS	AUN47	(800) 508-5200
ATL COMMUNICATIONS	AUN48	(800) 508-5200
ATL COMMUNICATIONS	AUN49	(800) 508-5200
ATL COMMUNICATIONS	AUN50	(800) 508-5200
ATL COMMUNICATIONS	AUN51	(800) 508-5200
ATL COMMUNICATIONS	AUN52	(800) 508-5200
ATL COMMUNICATIONS	AUN53	(800) 508-5200
ATL COMMUNICATIONS	AUN54	(800) 508-5200
ATL COMMUNICATIONS	AUN55	(800) 508-5200
ATL COMMUNICATIONS	AUN56	(800) 508-5200
ATL COMMUNICATIONS	AUN57	(800) 508-5200

ATL COMMUNICATIONS	AUN58	(800) 508-5200
ATL COMMUNICATIONS	AUN59	(800) 508-5200
ATL COMMUNICATIONS	AUN60	(800) 508-5200
ATL COMMUNICATIONS	AUN61	(800) 508-5200
ATL COMMUNICATIONS	AUN62	(800) 508-5200
ATL COMMUNICATIONS	AUN63	(800) 508-5200
ATL COMMUNICATIONS	AUN64	(800) 508-5200
ATL COMMUNICATIONS	AUN65	(800) 508-5200
ATL COMMUNICATIONS	AUN66	(800) 508-5200
ATL COMMUNICATIONS	AUN67	(800) 508-5200
ATL COMMUNICATIONS	AUN68	(800) 508-5200
ATL COMMUNICATIONS	AUN69	(800) 508-5200
ATL COMMUNICATIONS	AUN70	(800) 508-5200
ATL COMMUNICATIONS	AUN71	(800) 508-5200
ATL COMMUNICATIONS	AUN72	(800) 508-5200
ATL COMMUNICATIONS	AUN73	(800) 508-5200
ATL COMMUNICATIONS	AUN74	(800) 508-5200
ATL COMMUNICATIONS	AUN75	(800) 508-5200
ATL COMMUNICATIONS	AUN76	(800) 508-5200
ATL COMMUNICATIONS	AUN77	(800) 508-5200
ATL COMMUNICATIONS	AUN78	(800) 508-5200
ATL COMMUNICATIONS	AUN79	(800) 508-5200
ATL COMMUNICATIONS	AUN80	(800) 508-5200
ATL COMMUNICATIONS	AUN99	(800) 508-5200
ATL TELECOM SERVICES	AUN81	(800) 508-5200
ATL TELECOM SERVICES	AUN82	(800) 508-5200
ATL TELECOM SERVICES	AUN83	(800) 508-5200
ATL TELECOM SERVICES	AUN84	(800) 508-5200
ATL TELECOM SERVICES	AUN85	(800) 508-5200
ATL TELECOM SERVICES	AUN86	(800) 508-5200
ATL TELECOM SERVICES	AUN87	(800) 508-5200
ATL TELECOM SERVICES	AUN88	(800) 508-5200
ATL TELECOM SERVICES	AUN89	(800) 508-5200

ATL TELECOM SERVICES	AUN90	(800) 508-5200
ATL TELECOM SERVICES	AUN91	(800) 508-5200
ATL TELECOM SERVICES	AUN92	(800) 502-5200
ATL TELECOM SERVICES	AUN93	(800) 508-5200
ATL TELECOM SERVICES	AUN94	(800) 508-5200
ATL TELECOM SERVICES	AUN95	(800) 508-5200
ATL TELECOM SERVICES	AUN96	(800) 508-5200
ATL TELECOM SERVICES	AUN97	(800) 508-5200
ATL TELECOM SERVICES	AUN98	(800) 508-5200
ATX TELECOMMUNICATIONS SERVICE	DAB01	(800) 220-4900
ATX TELECOMMUNICATIONS SERVICE	DAB99	(610) 668-3000
AURIS TECHNOLOGY	UGO01	(305) 436-8486
AURIS TECHNOLOGY	UGO21	(305) 261-7778
AURIS TECHNOLOGY	UGO31	(305) 261-7778
AURIS TECHNOLOGY	UGO99	(305) 436-8486
BAK COMMUNICATIONS LLC	RFF01	(213) 688-8838
BAK COMMUNICATIONS LLC	RFF99	(213) 688-8838
BAY STAR COMM. INC.	BYS01	(800) 229-7827
BAY STAR COMM. INC.	BYS99	(800) 229-7827
BBCOM	GBB01	(213) 489-2156
BBCOM	GBB99	(213) 489-2156
BEEHIVE TELEPHONE	BVE01	(801) 234-0111
BEEHIVE TELEPHONE	BVE99	(435) 234-0111
BELL ATLANTIC SOUTH	BANX1	(212) 338-7666
BELL CANADA	CNM01	(800) 663-8725
BELL CANADA	CNM02	(800) 663-8725
BELL CANADA	CNM99	(800) 663-8725
BELL SOUTH LONG DISTANCE	BDL01	(800) 684-2174
BELL SOUTH LONG DISTANCE	BDL29	(770) 352-3365
BELL SOUTH LONG DISTANCE	BDL77	(800) 684-2174
BELL SOUTH LONG DISTANCE	BDL99	(800) 684-2174
BELL SOUTH TELECOM	BSSBA	(800) 515-1507
BELL SOUTH TELECOM	BSSBB	(800) 515-1507

BELL SOUTH TELECOM	BSSBT	(800) 515-1507
BELL SOUTH TELECOM	BSSB1	(800) 515-1507
BELL SOUTH TELECOM	BSSB2	(800) 515-1507
BELL SOUTH TELECOM	BSSE1	(800) 515-1507
BELL SOUTH TELECOM	BSSM1	(800) 515-1507
BELL SOUTH TELECOM	BSS99	(800) 515-1507
BELLSOUTH LONG DISTANCE	BDL07	(800) 684-2174
BELLSOUTH LONG DISTANCE	BDL30	(877) 456-4562
BESTLINE	NPH01	(800) 365-6030
BESTLINE	NPH99	(800) 365-6030
BH TELECOM	DLP01	(310) 273-9023
BH TELECOM	DLP99	(310) 273-9023
BIG RIVER TELEPHONE LLC	BFN99	(573) 651-3373
BIG RIVER TELEPHONE LLC	BFN01	(573) 651-3373
BIRCH TELECOM	VLK01	(800) 860-8401
BIRCH TELECOM	VLK99	(316) 343-7071
BIRCH/IONEX TELECOMMUNICATIONS	FEL01	(800) 860-8401
BIRCH/IONEX TELECOMMUNICATIONS	FST01	(800) 860-8401
BIRCH/IONEX TELECOMMUNICATIONS	TTH01	(800) 860-8401
BIRCH/IONEX TELECOMMUNICATIONS	VDL01	(800) 860-8401
BOULEVARD MEDIA INC.	BOV99	(888) 526-8663
BRAND800.COM	RYT01	(800) 214-4100
BRAND800.COM	RYT99	(800) 214-4100
BROADVIEW NETWORKS	BJC01	(800) 260-8766
BROADVIEW NETWORKS	BJC02	(800) 260-8766
BROADVIEW NETWORKS	BJC03	(800) 260-8766
BROADVIEW NETWORKS	BJC04	(800) 260-8766
BROADVIEW NETWORKS	BJC99	(315) 442-9567
BROADWING COMMUNICATIONS	IXC01	(800) 994-9638
BROADWING COMMUNICATIONS	IXC99	(800) 848-8459
BROADWING COMMUNICATIONS	IZC01	(800) 433-0630
BROADWING COMMUNICATIONS	IZC99	(800) 994-9683
BULLETINS, INC	DYR99	(714) 453-2360

BULLETINS, INC.	DYR01	(714) 740-3000
BUSINESS EDGE GROUP	BGE02	(732) 846-7302
BUSINESS TECHNOLOGY SERVICES	BQT01	(305) 358-5850
BUSINESS TECHNOLOGY SERVICES	BQT99	(305) 358-5850
BUSINESS TELECOM INC.	BTI01	(800) 849-2111
BUSINESS TELECOM INC.	BTM01	(800) 849-2111
BUSINESS TELECOM INC.	BTM99	(800) 849-2111
BUSINESS TELECOM, INC.	BTS01	(800) 849-9100
C & C MANAGEMENT	KKM01	(251) 633-6990
C & C MANAGEMENT	KKM99	(251) 633-6990
CABLE VISION LIGHTPATH	EYE01	(516) 393-3434
CABLE VISION LIGHTPATH	EYE99	(516) 393-3434
CABLEVISION LIGHTPATH	EYE02	(866) 611-3434
CALL SOURCE	OUR01	(888) 763-6200
CALL SOURCE	OUR99	(818) 676-3417
CALLCAST INC	HHG99	(650) 614-0750
CAPITAL TELECOMM	VST01	(800) 569-5185
CAPITAL TELECOMM	VST99	(800) 569-5185
CAPITAL TELECOMMUNICATIONS INC	VST55	(717) 848-8800
CAPITAL TELECOMMUNICATIONS INC	VST88	(717) 848-8800
CAPITAL TELECOMMUNICATIONS	ETS01	(215) 628-4111
CAPITAL TELECOMMUNICATIONS INC	VST05	(717) 815-6321
CAPITAL TELECOMMUNICATIONS INC	VST10	(717) 815-6321
CAPITAL TELECOMMUNICATIONS INC	VST15	(717) 815-6321
CAPITAL TELECOMMUNICATIONS INC	VST20	(717) 815-6321
CAPITAL TELECOMMUNICATIONS INC	VST25	(717) 815-6321
CAPITAL TELECOMMUNICATIONS INC	VST66	(717) 848-8800
CAPITAL TELECOMMUNICATIONS INC	VST77	(717) 848-8800
CAPSULE COMMUNICATIONS	UCW01	(800) 493-0800
CAPSULE COMMUNICATIONS	UCW99	(800) 493-0800
CAVALIER TELEPHONE LLC	HER01	(866) 800-6855
CBEYOND COMMUNICATIONS	OJB01	(678) 424-2663
CBEYOND COMMUNICATIONS	OJB99	(678) 424-2663

CENTENNIAL PR OPERATIONS CORP	LAM01	(787) 717-9648
CENTENNIAL PR OPERATIONS CORP	LAM99	(787) 717-9648
CGI LONG DISTANCE SERVICES	CKC01	(800) 747-8000
CGI LONG DISTANCE SERVICES	CKC99	(800) 747-8000
CHOICE ONE COMMUNICATIONS	UUS01	(888) 493-7300
CHOICE ONE COMMUNICATIONS	UUS99	(616) 493-7028
CINCINNATI BELL ANY DISTANCE	DBC01	(800) 422-1199
CINCINNATI BELL ANY DISTANCE	DBC03	(513) 768-4469
CINCINNATI BELL ANY DISTANCE	DBC99	(800) 735-3030
CINERGY COMMUNICATIONS CO	LOD01	(800) 599-1000
CINERGY COMMUNICATIONS CO	LOD99	(812) 456-4748
CLEAREND, LLC	QXP01	(646) 473-2404
CLEAREND, LLC	QXP99	(646) 473-2404
CNE TELECOMMUNICATION LLC	OWL01	(866) 870-2464
CNE TELECOMMUNICATION LLC	OWL99	(866) 870-2464
COMMERCIAL LT BARODA, SA	JJJ01	(866) 870-7060
COMMERCIAL LT BARODA, SA	JJJ99	(800) 972-9631
COMMPARTNERS LLC	FYI01	(800) 577-4021
COMMPARTNERS LLC	FYI99	(800) 577-4021
COMMUNICATION MANAGEMENT SVC	MNS01	(858) 565-2800
COMMUNICATION MANAGEMENT SVC	MNS99	(619) 521-8531
COMMUNICATIONS OPTION, INC.	CIO01	(614) 882-2030
COMMUNICATIONS OPTIONS, INC.	CIO99	(614) 882-2030
COMMUNIGROUP, INC	CGI01	(800) 748-9090
COMMUNIGROUP, INC.	CGI99	(800) 748-9090
CONSOLIDATED COMMUNICATIONS	LCT99	(800) 364-2528
CONSOLIDATED COMMUNICATIONS	LCT01	(800) 364-2528
CONVERGIA INC.	QKB01	(514) 693-6300
CONVERGIA INC.	QKB99	(514) 693-6300
CONVERGYS SPEECH SOLUTIONS	IHB01	(703) 620-4700
CONVERGYS SPEECH SOLUTIONS	IHB99	(703) 620-4700
COOPERATIVE COMMUNICATIONS	CJI01	(800) 833-2700
COOPERATIVE COMMUNICATIONS	CJI99	(800) 833-2700

CORDIA COMMUNICATIONS	SYS01	(877) 985-9900
CORDIA COMMUNICATIONS	SYS99	(877) 835-9900
COVISTA COMMUNICATION	TOT01	(800) 493-0800
COVISTA COMMUNICATION	TOT99	(800) 493-0800
COVISTA COMMUNICATIONS	BKD01	(800) 493-0800
COVISTA COMMUNICATIONS	BKD99	(866) 254-6532
COX TELECOM, LLC	QEQ01	(405) 600-6333
COX TELECOM, LLC	QEQ99	(405) 600-6333
CRICKET COMMUNICATIONS	MLK01	(858) 882-9279
CRICKET COMMUNICATIONS	MLK99	(858) 882-9279
CSF CORPORATION	ART02	(732) 356-6999
CSF CORPORATION	ART03	(732) 356-6999
CSF CORPORATION	ART06	(732) 356-6999
CSF CORPORATION	ART07	(732) 356-6999
CSF CORPORATION	ART08	(732) 356-6999
CSF CORPORATION	ART09	(732) 356-6999
CSF CORPORATION	ART10	(732) 356-6999
CSF CORPORATION	ART11	(732) 356-6999
CSF CORPORATION	ART12	(732) 356-6999
CSF CORPORATION	ART13	(732) 356-6999
CSF CORPORATION	ART14	(732) 356-6999
CSF CORPORATION	ART15	(732) 356-6999
CSF CORPORATION	ART16	(732) 356-6999
CSF CORPORATION	ART17	(732) 356-6999
CSF CORPORATION	ART18	(732) 356-6999
CSF CORPORATION	ART19	(732) 356-6999
CSF CORPORATION	ART20	(732) 356-6999
CSF CORPORATION	ART21	(732) 356-6999
CSF CORPORATION	ART22	(732) 356-6999
CSF CORPORATION	ART23	(732) 356-6999
CSF CORPORATION	ART24	(732) 356-6999
CSF CORPORATION	ART25	(732) 356-6999
CSF CORPORATION	ART26	(732) 356-6999

CSF CORPORATION	ART27	(732) 356-6999
CSF CORPORATION	ART28	(732) 356-6999
CSF CORPORATION	ART29	(732) 356-6999
CSF CORPORATION	ART30	(732) 356-6999
CSF CORPORATION	ART34	(732) 356-6999
CSF CORPORATION	ART35	(732) 356-6999
CTC LONG DISTANCE SERVICE	DDC01	(888) 200-0100
CTC LONG DISTANCE SERVICE	DDC99	(704) 722-2391
CUDUP	CUDUP	(888) 767-3300
CUSTOM TELECONNECT INC	VJC01	(702) 922-5225
CUSTOM TELECONNECT INC	VJC99	(702) 922-5225
CYTEL	CZT01	(800) 324-6123
CYTEL	CZT99	(800) 324-6123
DC COMMUNICATIONS	DIC01	(866) 330-4322
DIAL-AROUND TELECOM	HVN01	(817) 329-7424
DIAL-AROUND TELECOM	HVN99	(817) 329-7424
DIGITAL SOLUTIONS	DFN01	(800) 891-8203
DIGITAL SOLUTIONS	DFN99	(800) 891-8203
DOLLAR PHONE ACCESS, INC	JUI01	(718) 889-1102
DOLLAR PHONE ACCESS, INC	JUI99	(718) 889-1102
DOW NETWORKS	DWN01	(678) 631-2280
DOW NETWORKS	DWN99	(678) 631-2280
DSI TECHNOLOGIES	DSI01	(310) 636-3322
DSI TECHNOLOGIES	DSI99	(310) 636-3322
DTI	DTI01	(877) 742-5384
DTI	DTI99	(877) 742-5384
EARNWARE CORPORATION	ENE01	(888) 388-4359
EARNWARE CORPORATION	ENE02	(888) 388-4359
EARNWARE CORPORATION	ENE99	(888) 388-4359
EASTERN TEL LONG DIST. S. INC.	ETS99	(215) 628-4111
EASTERN TELEPHONE & TELECOMM	EOT01	(610) 433-1000
EASTERN TELEPHONE & TELECOMM	EOT99	(610) 433-1000
ECI CONFERENCE CALL SERVICES	EQC01	(800) 788-1085

ECI CONFERENCE CALL SERVICES	EQC99	(800) 788-1085
EFFICY GROUP	EGI99	(888) 233-3429
ELECTRIC LIGHTWAVE	EVW02	(800) 622-4354
ELECTRIC LIGHTWAVE	EVW03	(800) 622-4354
ELECTRIC LIGHTWAVE	EVW04	(800) 622-4354
ELECTRIC LIGHTWAVE	EVW05	(800) 622-4354
ELECTRIC LIGHTWAVE-ELI	EVW01	(800) 622-4354
ELECTRIC LIGHTWAVE-ELI	EVW99	(800) 622-4354
EMERITUS	TUI02	(877) 835-2680
EMERITUS COMMUNICATIONS	TUI01	(877) 835-2680
EMERITUS COMMUNICATIONS	TUI99	(877) 835-2680
EPANA NETWORKS	HMM01	(212) 931-8800
EPANA NETWORKS	HMM99	(212) 931-8800
E-RESPONSES.COM, INC.	EFJ01	(310) 902-5169
E-RESPONSES.COM, INC.	EFJ99	(310) 902-5169
ERESPORG LLC	JMN99	(866) 322-3800
EUREKAGGN	EJT01	(800) 562-4206
EUREKAGGN	EJT99	(800) 562-4206
EXCEL TELECOMMUNICATIONS INC.	ELT01	(800) 380-8089
EXCEL TELECOMMUNICATIONS INC.	ELT02	(514) 940-2978
EXCEL TELECOMMUNICATIONS INC.	ELT99	(800) 380-8089
FDN COMMUNICATIONS	FDN01	(407) 835-0334
FIRST COMMUNICATIONS	BNT01	(800) 274-1015
FIRST COMMUNICATIONS	BNT99	(800) 274-1015
FIRST DIGITAL TELECOM	FJT01	(801) 456-1000
FIRST DIGITAL TELECOM	FJT99	(801) 456-1000
FLORIDA DIGITAL NETWORK	FDN99	(407) 835-0334
FOCAL COMMUNICATIONS	FGC01	(888) 362-2522
FOCAL COMMUNICATIONS	FGC99	(888) 362-2522
FONOROLA, INC.	FON01	(416) 718-7474
FONOROLA, INC.	FON99	(800) 905-2580
FREEDOMVOICE SYSTEMS	RVE01	(858) 699-5312
FREEDOMVOICE SYSTEMS	RVE99	(858) 699-5312

FRONTIER COMMUNICATIONS	FLX01	(518) 773-6122
FRONTIER COMMUNICATIONS	FLX99	(800) 726-3539
FSC, LLC	OYL01	(800) 685-4001
FSC, LLC	OYL99	(800) 685-4001
FULL SERVICE NETWORK	FCC01	(888) 281-4800
FULL SERVICE NETWORK	FCC02	(888) 281-4800
FULL SERVICE NETWORK	FCC03	(888) 281-4800
FULL SERVICE NETWORK	FCC99	(888) 281-4800
FULL SPECTRUM TELECOMM. INC.	FUL01	(727) 524-3900
FULL SPECTRUM TELECOMM. INC.	FUL99	(727) 524-3900
FUTUREDONTICS INC	FNA01	(310) 215-6400
FUTUREDONTICS INC	FNA99	(310) 215-6400
GABRIEL WIRELESS LLC	YGW01	(561) 999-0999
GABRIEL WIRELESS LLC	YGW99	(561) 999-0999
GAFACHI	KRY01	(646) 723-0500
GAFACHI	KRY99	(646) 723-0500
GCI COMMUNICATIONS CORP	GCI01	(800) 770-8725
GCI COMMUNICATIONS CORP	GCI99	(800) 770-8725
GLOBAL CROSSING	ALE01	(800) 466-4646
GLOBAL CROSSING	ALE99	(800) 466-4646
GLOBAL CROSSING	ALF01	(800) 783-2020
GLOBAL CROSSING	ALF99	(800) 783-2020
GLOBAL CROSSING	ALN01	(800) 466-4600
GLOBAL CROSSING	ALN03	(800) 783-2020
GLOBAL CROSSING	ALN99	(800) 783-2020
GLOBAL CROSSING	ESM01	(800) 783-2020
GLOBAL CROSSING	ESM99	(800) 783-2020
GLOBAL CROSSING	RCI01	(800) 783-2020
GLOBAL CROSSING	RCI99	(800) 783-2020
GLOBAL CROSSING	RCMAD	(800) 783-2020
GLOBAL CROSSING	RCM99	(800) 783-2020
GLOBAL CROSSING	RCNDL	(800) 466-4600
GLOBAL CROSSING	RCNTE	(800) 724-3499

GLOBAL CROSSING	RCN99	(800) 783-2020
GLOBAL CROSSING	RCSM1	(800) 783-2020
GLOBAL CROSSING	RCUSW	(800) 783-2020
GLOBAL CROSSING	RCU99	(800) 783-2020
GLOBAL CROSSING	RCVST	(800) 783-2020
GLOBAL CROSSING	RCV99	(800) 783-2020
GLOBAL CROSSING	SDR01	(800) 783-2020
GLOBAL CROSSING	SDR99	(800) 783-2020
GLOBAL CROSSING	SRC01	(800) 783-2020
GLOBAL CROSSING	SRC99	(800) 783-2020
GLOBAL CROSSING	WCU01	(800) 783-2020
GLOBAL CROSSING	WCU99	(800) 783-2020
GLOBALCOM, INC	GMM01	(800) 589-1531
GLOBALCOM, INC	GMM99	(800) 589-1531
GLOBALTRON COMMUNICATIONS CORP	QRS01	(888) 465-3731
GOSOLO TECHNOLOGIES INC	OSG01	(727) 821-6565
GOSOLO TECHNOLOGIES INC	OSG99	(727) 821-6565
GOTVMAIL COMMUNICATIONS	VML01	(888) 431-6800
GOTVMAIL COMMUNICATIONS	VML99	(617) 454-1256
GRAND CIRCLE TRAVEL	GKL01	(617) 346-6825
GRAND CIRCLE TRAVEL	GKL99	(617) 346-3825
GRANDE COMMUNICATIONS NETWORKS	KWN01	(800) 200-3694
GRANDE COMMUNICATIONS NETWORKS	KWN99	(512) 787-5408
GRANITE TELECOMMUNICATIONS LLC	WKE01	(866) 847-5500
GRANITE TELECOMMUNICATIONS LLC	WKE99	(866) 847-5500
HAWAIIAN TELCOM, INC	HXT01	(808) 643-4662
HAWAIIAN TELCOM, INC.	HXT99	(808) 643-4662
HAWAIIAN TELECOM, INC	HXT48	(808) 457-9963
HAWAIIAN TELECOM, INC.	HXT79	(808) 457-9963
HBDC	FZF01	(954) 294-2534
HBDC	FZF99	(954) 294-2534
HBNET	HBN01	(602) 504-4630

HBNET	HBN99	(602) 504-4630
HELLOCOM, INC	DVC01	(714) 350-6931
HELLOCOM, INC	DVC99	(714) 350-6931
HELP DESK	BRD90	(888) 767-3300
HELP DESK	BRD91	(888) 767-3300
HELPDESK	BRD92	(888) 767-3300
HELPDESK	BRD93	(888) 767-3300
HELPDESK	BRD94	(888) 767-3300
HELPDESK	BRD95	(888) 767-3300
HELPDESK	BRD96	(888) 767-3300
HELPDESK	BRD97	(888) 767-3300
HELPDESK	BRD98	(888) 767-3300
HELPDESK	BRD99	(888) 767-3300
HICKORY TECH	HKT01	(507) 387-1151
HICKORY TECH	HKT99	(507) 387-1151
HTC	HJK01	(618) 939-6112
HTC	HJK99	(618) 939-6112
I ELEMENT INC.	RXD01	(214) 254-3480
I ELEMENT INC.	RXD99	(214) 254-3480
IDS LONG DISTANCE	ILD01	(866) 872-2443
IDS LONG DISTANCE	ILD99	(866) 872-2443
IDT	IPT22	(973) 438-1000
IDT CORPORATION	IPT01	(973) 438-4320
IDT CORPORATION	IPT09	(201) 928-4320
IDT CORPORATION	IPT53	(973) 438-4320
IDT CORPORATION	IPT99	(201) 928-2941
ILD TELECOM, INC.	RMI01	(800) 743-1003
ILD TELECOM, INC.	RMI99	(800) 743-1003
ILLUMINET	UIN99	(800) 800-5443
INFORMATION TELCO SERVICES INC	SQC01	(847) 501-0472
INFORMATION TELCO SERVICES INC	SQC99	(408) 934-1787
INFOTEL COMMUNICATIONS, LLC	IMT99	(218) 825-7880
INTEGRA TELECOM	IMT01	(218) 625-4312

INTEGRA TELECOM	IMT02	(503) 748-1945
INTEGRA TELECOM	IMT03	(503) 748-1945
INTEGRA TELECOM	IMT04	(503) 748-1945
INTEGRA TELECOM	IMT05	(503) 748-1945
INTELEMEDIA COMMUNICATIONS INC	IYM01	(972) 994-0700
INTELEMEDIA COMMUNICATIONS INC	IYM99	(972) 994-0700
INTERMETRO COMMUNICATIONS INC	OFT01	(805) 433-8000
INTERMETRO COMMUNICATIONS INC	OFT02	(805) 433-8000
INTERMETRO COMMUNICATIONS INC	OFT99	(805) 433-8000
INTERNATIONAL TELCOM LTD	IWL99	(800) 733-1335
INTERNATIONAL TELECOM LTD	IWL03	(206) 479-2322
INTERNATIONAL TELECOMMUNICATIO	OET01	(954) 862-2249
INTERNATIONAL TELECOMMUNICATIO	OET99	(954) 862-2249
IONEX COMM.	TTH02	(800) 234-2301
IONEX COMM.	TTH99	(800) 234-2301
IONEX TELECOM	FST02	(316) 833-5235
IONEX TELECOM	FST99	(316) 337-8640
IONEX TELECOM, INC.	FEL99	(605) 332-3232
IONEX TELECOMMUNICATIONS	VDL99	(800) 333-1124
IOWA COMMUNICATIONS NETWORK	IOW01	(800) 358-5937
IOWA COMMUNICATIONS NETWORK	IOW99	(800) 358-5937
IOWA NETWORK SERVICES	ISV01	(800) 469-4000
IOWA NETWORK SERVICES	ISV99	(800) 469-4000
IT CONNECT CANADA	JRC01	(888) 482-6663
IT CONNECT CANADA	JRC99	(888) 482-6663
IT&E OVERSEAS	IEO01	(671) 646-8886
IT&E OVERSEAS	IEO99	(671) 646-8886
ITC DELTACOM	SIDLT	(800) 239-3000
ITC DELTACOM	SID99	(800) 239-3000
ITC DELTACOM	SIR01	(800) 240-0000
ITL	IWL04	(206) 479-2322
KALL8	IWL01	(206) 479-2322
LATAONE INC	LJK01	(800) 230-4451

LATAONE INC	LJK02	(800) 230-4451
LATAONE INC	LJK03	(800) 230-4451
LATAONE INC	LJK06	(800) 230-4451
LATAONE INC	LJK07	(800) 230-4451
LATAONE INC	LJK08	(800) 230-4451
LATAONE INC	LJK09	(800) 230-4451
LATAONE INC	LJK99	(800) 230-4451
LATAONE, INC	LJK04	(800) 230-4451
LATAONE, INC	LJK05	(800) 230-4451
LATAONE, INC	LJK10	(800) 230-4451
LATAONE, INC	LJK14	(800) 230-4451
LATAONE, INC	LJK16	(800) 230-4451
LATAONE, INC.	LJK11	(800) 230-4451
LATAONE, INC.	LJK12	(800) 230-4451
LATAONE, INC.	LJK13	(800) 230-4451
LATAONE, INC.	LJK15	(800) 230-4451
LATAONE, INC.	LJK17	(800) 230-4451
LATAONE, INC.	LJK18	(800) 230-4451
LATAONE, INC.	LJK19	(800) 230-4451
LATAONE, INC.	LJK20	(800) 230-4451
LDDS/METROMEDIA (EDS)	EDS01	(601) 360-8600
LDDS/METROMEDIA (EDS)	EDS99	(601) 360-8600
LDMI LONG DISTANCE	LMI01	(800) 374-5364
LDMI LONG DISTANCE	LMI99	(313) 664-2321
LEGACY LONG DISTANCE	LBD01	(714) 826-0547
LEGACY LONG DISTANCE	LBD99	(714) 826-0547
LEVEL 3 COMMUNICATIONS LLC	LVC01	(877) 453-8353
LEVEL 3 COMMUNICATIONS LLC	LVC99	(720) 888-7742
LIGHTSHIP TELECOM DBA CTC	LHS01	(603) 314-2433
LIGHTSHIP TELECOM DBA CTC	LHS99	(603) 314-2433
LIGHTYEAR/UNIDIAL COMM.	UDI01	(800) 393-7300
LIGHTYEAR/UNIDIAL COMM.	UDI02	(888) 864-7671
LIGHTYEAR/UNIDIAL COMM.	UDI99	(800) 393-7300

LINE SYSTEMS INC	HDS01	(610) 355-9700
LINE SYSTEMS INC	HDS99	(610) 355-9700
LINX COMMUNICATIONS	LXC01	(617) 747-3950
LINX COMMUNICATIONS	LXC99	(617) 747-3950
LIVEOPS, INC	HHG01	(800) 898-2796
LOCUS TELECOM, INC.	LKS01	(800) 539-6016
LOCUS TELECOM, INC.	LKS99	(800) 539-6016
LOGIX COMMUNICATIONS	AET01	(800) 444-0258
LOGIX COMMUNICATIONS	AET99	(800) 444-0258
LONG DISTANCE BILLING SERVICES	LZO01	(888) 826-9414
LONG DISTANCE BILLING SERVICES	LZO99	(888) 826-9414
LYNX TELECOM L.L.C.	LYX01	(801) 254-6245
LYNX TELECOM L.L.C.	LYX99	(801) 295-2264
MARATHON COMMUNICATIONS	SJS01	(800) 919-1000
MARATHON COMMUNICATIONS	SJS99	(800) 919-1000
MARCANTEL COMMUNICATIONS,LP	SKV99	(800) 761-6713
MAYFAIR COMMUNICATIONS, INC.	MYR01	(800) 629-3247
MAYFAIR COMMUNICATIONS, INC.	MYR99	(800) 629-3247
MBI SERVICES GRP LLC	WZD01	(941) 586-5694
MBI SERVICES GRP LLC	WZD99	(641) 586-5694
MCGRAW COMMUNICATIONS	BZY02	(888) 543-2000
MCGRAW COMMUNICATIONS, INC	BZY01	(888) 543-2000
MCGRAW COMMUNICATIONS, INC	BZY99	(888) 543-2000
MCI	MCI01	(800) 888-1800
MCI	MCI02	(800) 888-1800
MCI	MCI99	(800) 888-1800
MCI NETWORK SERVICES, INC	WIL99	(800) 828-4984
MCI NETWORK SERVICES, INC.	WILSB	(800) 828-4984
MCI NETWORK SERVICES, INC.	WIL01	(800) 828-4984
MCI NETWORK SERVICES, INC.	WIL04	(800) 828-4984
MCI NETWORK SERVICES, INC.	WIL20	(800) 828-4984
MCI WHOLESALE	MCW22	(800) 828-4984
MCI WORLDCOM	LDD01	(800) 264-1000

MCI WORLDCOM	LDD02	(800) 264-1000
MCI WORLDCOM	LDD03	(800) 264-1000
MCI WORLDCOM	LDD04	(800) 264-1000
MCI WORLDCOM	LDD05	(888) 872-9266
MCI WORLDCOM	LDD06	(888) 872-9266
MCI WORLDCOM	LDD07	(888) 872-9266
MCI WORLDCOM	LDD08	(888) 872-9266
MCI WORLDCOM	LDD20	(888) 872-9266
MCI WORLDCOM	LDD99	(800) 264-1000
MCLEOD USA	CDN01	(800) 500-8000
MCLEOD USA	CDN02	(800) 500-8000
MCLEOD USA	CDN03	(800) 500-8000
MCLEOD USA	CDN04	(800) 500-8000
MCLEOD USA	CDN99	(800) 500-8000
MCLEOD USA	CDSM1	(800) 500-8000
MCLEOD USA ACCESS LONG DIST	ACC04	(888) 737-8335
MCLEOD USA/ACCESS LD	ACC02	(800) 593-1177
MCLEOD USA/ACCESS LD	ACC99	(801) 238-2275
MCLEOD USA/CAPROCK	YSG01	(800) 687-1600
MCLEOD USA/CAPROCK	YSG99	(800) 687-1600
MERCANTEL COMMUNICATIONS, LP	SKV01	(800) 761-6713
MET TEL	MET01	(212) 607-6336
MET TEL	MET99	(212) 588-0319
MICKTEL CORP	MJC01	(858) 775-7240
MICKTEL CORP	MJC99	(858) 775-7240
MICRONESIAN TELECOMMUNICATIONS	MKN01	(670) 682-3878
MICRONESIAN TELECOMMUNICATIONS	MKN99	(670) 682-3878
MIJANDA, INC	EBO01	(866) 512-0200
MIJANDA, INC	EBO99	(866) 512-0200
MISC-ETC	MQX01	(503) 234-1234
MISC-ETC	MQX99	(503) 639-5953
MONMOUTH TELEPHONE & TELEGRAPH	MOT01	(732) 704-1000
MONMOUTH TELEPHONE & TELEGRAPH	MOT99	(732) 704-1000

MPOWER COMMUNICATIONS	MPC99	(702) 310-4300
MPOWER COMMUNICATIONS CORP	MPC01	(702) 310-7994
NATIONAL COMTEL	HCN02	(800) 987-0100
NATIONAL COMTEL NETWORK, INC.	HCN01	(818) 881-7900
NATIONAL COMTEL NETWORK, INC.	HCN99	(818) 881-7900
NATIONWIDE 800	WDE01	(602) 944-1210
NATIONWIDE 800	WDE99	(602) 944-1210
NAVIGATA COMMUNICATIONS	NUM99	(800) 668-9377
NAVIGATA COMMUNICATIONS	NUM01	(800) 668-9377
NAVIGATA COMMUNICATIONS	NUM02	(800) 668-9377
NET 2000 COMMUNICATIONS	HER99	(703) 654-2000
NETRONIXS	EIX01	(800) 840-8708
NETRONIXS	EIX99	(800) 840-8708
NETWORK COMM. INT'L CORP.	HWK01	(888) 386-3709
NETWORK COMM. INT'L CORP.	HWK99	(888) 386-3709
NETWORK ENHANCED TELECOM	NKS01	(903) 758-9350
NETWORK ENHANCED TELECOM	NKS99	(903) 758-9350
NETWORK ENHANCED TELECOM	NKT01	(903) 323-4544
NETWORK MANAGEMENT INC	KMT01	(801) 990-0325
NETWORK MANAGEMENT INC	KMT99	(801) 990-0325
NETWORK TELEPHONE SERVICES INC	NSI01	(818) 227-1100
NETWORK TELEPHONE SERVICES INC	NSI99	(818) 227-1100
NETWORK US INC	KBT01	(888) 742-5523
NETWORK US INC.	KBT99	(888) 742-5523
NEW NETWORK	EWN01	(877) 667-3463
NEW NETWORK	EWN99	(877) 667-3463
NEXT-G COMMUNICATIONS	JHT01	(713) 952-5885
NEXT-G COMMUNICATIONS	JHT99	(713) 952-5885
NOBEL TEL LLC	YUI01	(760) 405-0105
NOBEL TEL LLC	YUI99	(760) 405-0105
NORLIGHT TELECOM, INC.	JCI01	(877) 792-7905
NORLIGHT TELECOM, INC.	JCI99	(414) 792-7914
NOS COMMUNICATIONS	NRC01	(702) 547-8786

NOS COMMUNICATIONS	NRC02	(702) 547-8793
NOS COMMUNICATIONS	NRC03	(702) 547-8793
NOS COMMUNICATIONS	NRC99	(702) 547-8786
NTS COMMUNICAITONS	NCM99	(800) 658-2150
NTS COMMUNICATIONS	NCM01	(800) 658-2101
NUVOX	DHA99	(800) 600-5050
NUVOX COMMUNICATIONS	DHA01	(864) 672-5048
ON-CALL RESP ORG SVSC, INC	OAK01	(800) 986-2501
ON-CALL RESP ORG SVSC, INC	OAK99	(800) 986-2501
ONE CALL COMMUNICATIONS	OCC01	(317) 575-3200
ONE CALL COMMUNICATIONS	OCC99	(800) 879-9939
ORION TELECOMMUNICATIONS CORP	ORN99	(732) 236-1938
ORION TELECOMMUNICATIONS CORP.	ORN01	(732) 236-1938
PACIFIC BELL	PCLD1	(800) 933-0300
PACIFIC BELL	PCPTP	(800) 933-0300
PACIFIC BELL	PCPTR	(800) 933-0300
PACIFIC BELL	PCPTT	(800) 933-0300
PACIFIC BELL	PCPT1	(800) 933-0300
PACIFIC BELL	PCP99	(800) 933-0300
PACIFIC BELL	PCSM1	(800) 933-0300
PACIFIC CENTREX SERVICES	PSS01	(818) 623-2300
PACIFIC CENTREX SERVICES	PSS99	(818) 623-2300
PACIFIC LIGHT NET	CAB01	(800) 733-5638
PACIFIC LIGHT NET	CAB99	(805) 547-6443
PACWEST	PWT01	(800) 399-3389
PACWEST	PWT99	(888) 861-3351
PAETEC COMMUNICATIONS	PKC01	(877) 340-2555
PAETEC COMMUNICATIONS	PKC02	(877) 340-2555
PAETEC COMMUNICATIONS	PKC03	(877) 340-2555
PAETEC COMMUNICATIONS	PKC04	(877) 340-2555
PAETEC COMMUNICATIONS	PKC99	(877) 340-2555
PAETEC COMMUNICATIONS INC.	PK777	(877) 340-2555
PAYMENTECH LP	IJK01	(800) 354-8879

PAYMENTECH LP	IJK99	(800) 354-8879
PHOENIX INT'L TELEPORT SATELLI	QNE01	(800) 274-6030
PHOENIX INT'L TELEPORT SATELLI	QNE99	(800) 274-6030
PHONE 1	QRS99	(888) 465-3731
PHONE PEOPLE HOLDINGS CORP	EKL01	(858) 569-4444
PHONE PEOPLE HOLDINGS CORP	EKL99	(858) 569-4444
PHONE USA, INC.	PUI01	(800) 390-0779
PHONE USA, INC.	PUI99	(800) 390-0779
PILGRIM TELEPHONE	PLG01	(617) 225-7000
PILGRIM TELEPHONE	PLG99	(617) 225-7000
PNG TELECOM	PGN01	(800) 860-9495
PNG TELECOM	PGN99	(800) 860-9495
POINT ONE	DMZ01	(512) 735-1230
POINT ONE	DMZ99	(512) 735-1230
POINT TELECOM INC	RTI01	(818) 348-4466
POINT TELECOM, INC.	RTI99	(818) 348-4466
POPP.COM	LIC01	(763) 797-7900
POPP.COM	LIC99	(763) 797-7900
POWERCOM	TGN02	(800) 444-4014
POWERCOM CORPORATION	TGN01	(800) 444-4014
POWERCOM CORPORATION	TGN99	(800) 444-4014
PREMIERE CONFERENCING	KYT01	(913) 661-0700
PREMIERE CONFERENCING	KYT99	(913) 661-0700
PREMIERE GLOBAL	FPE04	(877) 490-3185
PREMIERE GLOBAL SERVICES	FPE01	(877) 490-3186
PREMIERE GLOBAL SERVICES	FPE02	(877) 490-3185
PREMIERE GLOBAL SERVICES	FPE03	(877) 490-3185
PREMIERE GLOBAL SERVICES	FPE99	(877) 490-3186
PRIMETEL COMMUNICATIONS	PIT01	(888) 774-6383
PRIMETEL COMMUNICATIONS	PIT99	(888) 774-6383
PRIMUS CANADA	PBQ01	(416) 236-3636
PRIMUS CANADA	PBQ99	(416) 236-3636
PRIMUS COMMUNICATIONS	TIN08	(800) 899-1085

PRIMUS COMMUNICATIONS	TIN09	(800) 899-1085
PRIMUS COMMUNICATIONS	TIN10	(800) 899-1085
PRIMUS TELECOMMUNICATIONS	TIN01	(800) 899-1085
PRIMUS TELECOMMUNICATIONS	TIN04	(800) 899-1085
PRIMUS TELECOMMUNICATIONS	TIN05	(800) 899-1085
PRIMUS TELECOMMUNICATIONS	TIN06	(800) 899-1085
PRIMUS TELECOMMUNICATIONS	TIN07	(800) 899-1085
PRIMUS TELECOMMUNICATIONS	TIN99	(800) 899-1085
PRIMUS TELECOMMUNICATIONS INC	TIN02	(800) 899-1085
PRIMUS TELECOMMUNICATIONS INC	TIN03	(800) 899-1085
PSEUDO ENTITY 0110	1AXXX	(888) 767-3300
PSEUDO ENTITY 0110	0AXXX	(888) 767-3300
PSEUDO ENTITY 0110	2AXXX	(888) 767-3300
PSEUDO ENTITY 0110	3AXXX	(888) 767-3300
PSEUDO ENTITY 0110	4AXXX	(888) 767-3300
PSEUDO ENTITY 0110	5AXXX	(888) 767-3300
PUERTO RICO TELEPHONE	PRT01	(787) 749-5500
PUERTO RICO TELEPHONE	PRT99	(787) 749-5500
QUESTAR INFOCOMM, INC.	QST01	(801) 324-1960
QUESTAR INFOCOMM, INC.	QST99	(801) 799-2959
QWEST IT	ULD02	(800) 573-1311
QWEST/LCI INT'L	LGSM1	(800) 860-7678
QWEST/LCI INT'L	LGTTE	(800) 860-1020
QWEST/LCI INT'L	LGT01	(800) 860-1020
QWEST/LCI INT'L	LGT99	(800) 860-1020
QWEST/US WEST	UWMST	(888) 826-0748
QWEST/US WEST	UWMS1	(888) 826-0748
QWEST/US WEST	UWM99	(800) 688-6102
QWEST/US WEST	UWNS1	(800) 688-6102
QWEST/US WEST	UWNWA	(800) 688-6102
QWEST/US WEST	UWNW1	(800) 443-3646
QWEST/US WEST	UWPN1	(800) 443-3646
QWEST/US WEST	UWSE1	(800) 443-3646

QWEST/US WEST	UWSM1	(800) 443-3646
QWEST/US WEST LONG DISTANCE	ULD01	(720) 540-1123
QWEST/US WEST LONG DISTANCE	ULD99	(888) 878-5301
QWEST/USWEST	UWMSA	(888) 826-0748
R. W. LYNCH COMPANY INC	RWL99	(925) 837-3877
R.W.LYNCH COMPANY INC	RWL01	(925) 837-3877
RADIANT TELECOM	RDT01	(305) 914-3381
RADIANT TELECOM	RDT02	(305) 914-3541
RADIANT TELECOM	RDT99	(305) 914-3454
RCC NETWORK INC.	RNI99	(320) 808-2135
RCN	CED01	(888) 972-6622
RCN	CED99	(800) 443-4253
RED RIVER NETWORK	GDG99	(405) 820-5250
RED RIVER NETWORKS	GDG02	(405) 820-5250
RED RIVER NETWORKS	GDG03	(405) 820-5250
RED RIVER NETWORKS	GDG04	(405) 820-5250
RED RIVER NETWORKS	GDG05	(405) 820-5250
RED RIVER NETWORKS	GDG06	(405) 820-5250
REMI COMMUNICATIONS	RRC01	(724) 836-5800
REMI COMMUNICATIONS	RRC99	(724) 836-5800
RESPORG SOLUTIONS	RHL01	(904) 318-7271
RESPORG SOLUTIONS	RHL99	(904) 318-7271
RESPORG USA INC.	VGF01	(626) 940-0566
RESPORG USA INC.	VGF99	(626) 940-0566
RESP-ORG.COM	QZA01	(800) 627-5383
RESP-ORG.COM	QZA99	(800) 327-5383
RING9, INC	GYC01	(866) 746-4999
RING9, INC	GYC99	(866) 746-4999
RINGCENTRAL INC.	RBI01	(800) 725-2730
RINGCENTRAL, INC.	RBI99	(650) 472-3670
RNK TELECOM, INC	RJT01	(781) 382-0124
RNK TELECOM, INC	RJT99	(781) 382-0124
ROLINIUM	ROL01	(718) 609-9700

ROLINIUM	ROL99	(718) 609-9700
RURAL CELLULAR CORP	RNI01	(320) 808-2135
SAGE TELECOM	KFV01	(214) 547-7195
SAGE TELECOM	KFV99	(214) 547-7195
SBC	SHOC1	(214) 464-3308
SBC	SHOPR	(214) 464-3308
SBC	SHSE1	(214) 464-3308
SBC	SHSM1	(214) 464-3308
SBC	SHSWA	(214) 454-6262
SBC	SHSWD	(214) 454-6262
SBC	SHSW0	(214) 464-3308
SBC	SHSW1	(800) 286-8313
SBC	SHSW3	(214) 454-6262
SBC	SHSW6	(800) 286-8313
SCHERERS COMM. GROUP INC.	SGI01	(614) 841-2421
SCHERERS COMM. GROUP INC.	SGI99	(800) 356-6161
SELECTIVE MEDIA	SEM01	(415) 543-9033
SELECTIVE MEDIA	SEM99	(415) 543-9033
SHEPHER CORPORATION	KUB01	(818) 700-7000
SHEPHER CORPORATION	KUB99	(818) 700-7000
SIERRA COMMUNICATIONS INC	MUI01	(866) 270-7560
SIERRA COMMUNICATIONS, INC	MUI99	(866) 270-7560
SIGECOM	HOT01	(866) 976-7800
SIGECOM	HOT99	(812) 437-0301
SIGNAL ONE, INC	SOE01	(904) 280-5353
SIGNAL ONE, INC.	SOE99	(904) 247-9900
SIOUXLAND TELEPHONE CO STC/MTI	MTI01	(605) 232-3457
SIOUXLAND TELEPHONE CO STC/MTI	MTI99	(605) 232-3457
SMARTBOX	MHT01	(514) 398-9355
SMARTBOX	MHT99	(514) 398-9355
SMS/800	BRCNA	(888) 767-3300
SMS/800	BRD01	(888) 767-3300
SMS/800	BRERR	(888) 767-3300

SMS/800	BRGMB	(888) 767-3300
SMS/800	BRHDT	(888) 767-3300
SMS/800	BROPR	(888) 767-3300
SMS/800	BRREP	(888) 767-3300
SMS/800	BRSAC	(888) 767-3300
SMS/800	BRSWB	(816) 275-3030
SMS/800	BRTST	(888) 767-3300
SMS/800	BRUNV	(888) 767-3300
SMS/800 HELP DESK	BRD78	(888) 767-3300
SMS/800 HELP DESK	BRD79	(888) 767-3300
SMS/800 HELP DESK	BRD80	(888) 767-3300
SMS/800 HELP DESK	BRD81	(888) 767-3300
SMS/800 HELP DESK TRAINING	ZATST	(888) 767-3300
SMS800 HELP DESK	BRD02	(888) 767-3300
SMS800 HELP DESK	BRD03	(888) 767-3300
SMS800 HELP DESK	BRD04	(888) 767-3300
SMS800 HELP DESK	BRD05	(888) 767-3300
SMS800 HELP DESK	BRD06	(888) 767-3300
SMS800 HELP DESK	BRD08	(888) 767-3300
SMS800 HELP DESK	BRD09	(888) 767-3300
SMS800 HELP DESK	BRD10	(888) 767-3300
SMS800 HELP DESK	BRD11	(888) 767-3300
SMS800 HELP DESK	BRD12	(888) 767-3300
SMS800 HELP DESK	BRD13	(888) 767-3300
SMS800 HELP DESK	BRD14	(888) 767-3300
SMS800 HELP DESK	BRD15	(888) 767-3300
SMS800 HELP DESK	BRD16	(888) 767-3300
SMS800 HELP DESK	BRD17	(888) 767-3300
SMS800 HELP DESK	BRD18	(888) 767-3300
SMS800 HELP DESK	BRD19	(888) 767-3300
SMS800 HELP DESK	BRD82	(888) 767-3300
SMS800 HELP DESK	BRD83	(888) 767-3300
SMS800 HELP DESK	BRD84	(888) 767-3300

SMS800 HELP DESK	BRD85	(888) 767-3300
SMS800 HELP DESK	BRD86	(888) 767-3300
SMS800 HELP DESK	BRD87	(888) 767-3300
SMS800 HELP DESK	BRD88	(888) 767-3300
SMS800 HELP DESK	BRD89	(888) 767-3300
SMS800 HELPDESK	BRD07	(888) 767-3300
SNIP LINK LLC	KIS01	(888) 764-7600
SNIP LINK LLC	KIS99	(888) 764-7600
SNS800 HELP DESK	BRD20	(888) 767-3300
SOUTHERN NE TELEPHONE	SNETT	(203) 420-3131
SOUTHERN NE TELEPHONE	SNET1	(203) 420-3131
SOUTHERN NE TELEPHONE	SNE99	(203) 420-3131
SOUTHERN NE TELEPHONE	SNSM1	(203) 420-3131
SOUTHERN NEW ENGLAND TELEPHONE	SNET2	(203) 420-3131
SOUTHERN NEW ENGLAND TELEPHONE	SNET3	(203) 420-3131
SOUTHERN TELECOM NETWORK INC	QTY01	(870) 404-7090
SOUTHERN TELECOM NETWORK INC	QTY99	(870) 404-7090
SOUTHWESTERN BELL CORP.	SHW99	(800) 286-8313
SOUTINE ENTERPRISES	KOK01	(954) 275-8998
SOUTINE ENTERPRISES	KOK99	(954) 275-8998
SOVERNET INC	KZA01	(877) 877-2120
SOVERNET INC	KZA99	(877) 877-2120
SPRINT COMMUNICATIONS CO. LP	SPBG1	(800) 795-1004
SPRINT COMMUNICATIONS CO. LP	SPBS1	(800) 795-1004
SPRINT COMMUNICATIONS CO. LP	SPBS2	(800) 795-1004
SPRINT COMMUNICATIONS CO. LP	SPBS3	(800) 795-1004
SPRINT COMMUNICATIONS CO. LP	SPBS4	(800) 795-1004
SPRINT COMMUNICATIONS CO. LP	SPBS5	(800) 795-1004
SPRINT COMMUNICATIONS CO. LP	SPCG1	(800) 877-4646
SPRINT COMMUNICATIONS CO. LP	SPDG3	(800) 795-1004
SPRINT COMMUNICATIONS CO. LP	SPFN1	(800) 795-1004
SPRINT COMMUNICATIONS CO. LP	SPGD1	(800) 795-1004
SPRINT COMMUNICATIONS CO. LP	SPGD2	(800) 795-1004

SPRINT COMMUNICATIONS CO. LP	SPHG1	(800) 786-5050
SPRINT COMMUNICATIONS CO. LP	SPIC1	(800) 795-1004
SPRINT COMMUNICATIONS CO. LP	SPNYN	(888) 696-3939
SPRINT COMMUNICATIONS CO. LP	SPR01	(800) 795-1004
SPRINT COMMUNICATIONS CO. LP	SPR99	(800) 795-1004
SPRINT COMMUNICATIONS CO. LP	SPSC1	(800) 600-1186
SPRINT COMMUNICATIONS CO. LP	SPSI1	(800) 795-1004
SPRINT COMMUNICATIONS CO. LP	SPST1	(800) 366-0707
SPRINT COMMUNICATIONS CO. LP	SPS01	(800) 795-1004
SPRINT COMMUNICATIONS CO. LP	SPS51	(800) 795-1004
STARTEC GLOBAL COMMUNICATIONS	SMG01	(301) 610-4422
STARTEC GLOBAL COMMUNICATIONS	SMG99	(301) 610-4422
STATE DUPLICATES	BRDUP	(888) 767-3300
STATE FARM INSURANCE	SFI01	(309) 766-2233
STATE FARM INSURANCE	SFI99	(309) 766-1220
SWITCH 2000, INC.	SCT01	(507) 385-2363
SWITCH 2000, INC.	SCT99	(507) 385-2363
TALKPATH, LLC	DUN01	(800) 657-9553
TALKPATH, LLC	DUN99	(800) 657-9553
TCAST COMMUNICATIONS	KAT01	(661) 253-5030
TCAST COMMUNICATIONS	KAT99	(661) 253-5030
TCAST COMMUNICATIONS, INC.	KAA01	(661) 253-5030
TDS METROCOM	USL01	(218) 568-4000
TEL-AMERICA/UCN	TNT01	(866) 659-0000
TEL-AMERICA/UCN	TNT02	(866) 695-0000
TEL-AMERICA/UCN	TNT04	(866) 695-0000
TEL-AMERICA/UCN	TNT99	(866) 695-0000
TEL-AMREICA/UCN	TNT03	(866) 695-0000
TELCO GROUP INC	YOU02	(888) 844-5390
TELCO GROUP INC.	YOU03	(888) 844-5390
TELCO GROUP, INC	YOU01	(888) 844-5390
TELCO GROUP, INC	YOU99	(888) 844-5390
TELCOVE	JSS01	(877) 321-5465

TELCOVE	JSS99	(814) 260-2745
TELECOM AFFILIATES	TSH01	(800) 754-1001
TELECOM AFFILIATES	TSH99	(800) 754-1001
TELECON COMMUNICATIONS CORP	DQP01	(321) 263-5999
TELECON COMMUNICATIONS CORP	DQP99	(800) 659-4454
TELEFONICA LARGA DISTANCIA	TFC01	(800) 496-3116
TELEFONICA LARGA DISTANCIA	TFC99	(800) 496-3116
TELEFYNE, INC	DZY01	(904) 394-1088
TELEFYNE, INC	DZY02	(914) 394-1088
TELEFYNE, INC	DZY03	(914) 394-1088
TELEFYNE, INC	DZY04	(914) 394-1088
TELEFYNE, INC	DZY05	(914) 394-1088
TELEFYNE, INC	DZY06	(914) 394-1088
TELEFYNE, INC	DZY07	(914) 394-1088
TELEFYNE, INC	DZY08	(914) 394-1088
TELEFYNE, INC	DZY09	(914) 394-1088
TELEFYNE, INC	DZY10	(914) 394-1088
TELEFYNE, INC.	DZY99	(904) 565-4051
TELEGLOBE INTERNATIONAL CORP	GIC01	(514) 868-8787
TELEGLOBE INTERNATIONAL CORP	GIC99	(514) 868-8787
TELEPACIFIC COMMUNICATIONS	PZC01	(877) 487-8722
TELEPACIFIC COMMUNICATIONS	PZC99	(800) 487-8722
TELEPERFORMANCE INTERACTIVE	QVF01	(610) 941-1000
TELEPERFORMANCE INTERACTIVE	QVF99	(610) 941-1000
TELEQUEST	TVQ01	(816) 532-6015
TELEQUEST	TVQ99	(816) 532-6015
TELESCAN, INC.	RPT01	(423) 282-5043
TELESCAN, INC.	RPT99	(423) 282-5043
TELESERVICES INC.	TJC01	(877) 870-8700
TELESERVICES INC.	TJC99	(877) 870-8700
TELESMART	UFO01	(503) 642-5569
TELESMART	UFO99	(503) 642-5569
TELRITE CORPORATION	KPK01	(770) 818-5305

TELRITE CORPORATION	KPK99	(770) 818-5305
TELUS COMMUNICATIONS	EUS07	(877) 700-4662
TELUS COMMUNICATIONS	EUS08	(877) 700-4662
TELUS COMMUNICATIONS	EUS09	(877) 700-4662
TELUS COMMUNICATIONS, INC.	EUS99	(780) 493-6561
TELUS CORPORATION	EUS01	(877) 700-4662
TELUS CORPORATION	EUS03	(780) 493-6561
TELUS CORPORATION	EUS04	(780) 493-6561
TELUS CORPORATION	EUS05	(780) 493-6561
TELUS CORPORATION	EUS06	(780) 493-6561
TELUS CORPORATION	EUS11	(780) 493-6561
TELUS CORPORATION	EUS12	(780) 493-6561
TELUS CORPORATION	EUS21	(780) 493-6561
TELUS CORPORATION	EUS22	(780) 493-6561
TELUS CORPORATION	EUS23	(780) 493-6561
TELUS CORPORATION	EUS31	(780) 493-6561
TELUS CORPORATION	EUS32	(780) 493-6561
TELUS CORPORATION	EUS33	(780) 493-6561
TELUS CORPORATION	EUS41	(780) 493-6561
TELUS CORPORATION	EUS42	(780) 493-6561
TELUS CORPORATION	EUS43	(780) 493-6561
TELUS CORPORATION	EUS44	(780) 493-6561
TELUS CORPORATION	EUS45	(780) 493-6561
TELUS QUEBEC	EUS02	(800) 463-3794
TELVUE CORP.	VUE01	(856) 273-8888
TELVUE CORP.	VUE99	(856) 273-8888
TEXAS COMMUNICATIONS	YYT01	(325) 658-3566
TEXAS COMMUNICATIONS	YYT99	(915) 658-3566
TGEC COMMUNICATIONS CO.,L.L.C.	GZT01	(650) 596-7302
TGEC COMMUNICATIONS CO.,L.L.C.	GZT99	(650) 596-7302
THE BUSINESS EDGE	BGE03	(732) 846-7302
THE BUSINESS EDGE GROUP	BGE01	(732) 846-7302
THE BUSINESS EDGE GROUP	BGE99	(732) 846-7302

THE PHONE COMPANY	PFC01	(215) 862-1508
THE PHONE COMPANY	PFC99	(215) 862-1508
THE SOFTWARE WERKS INC	GXC01	(904) 434-2774
THE SOFTWARE WERKS INC	GXC99	(904) 434-2774
THEBESTNUMBERS.COM	YHN01	(888) 888-8585
THEBESTNUMBERS.COM	YHN02	(888) 888-8585
THEBESTNUMBERS.COM	YHN03	(888) 888-8585
THEBESTNUMBERS.COM	YHN04	(888) 888-8585
THEBESTNUMBERS.COM	YHN05	(888) 888-8585
THEBESTNUMBERS.COM	YHN06	(888) 888-8585
THEBESTNUMBERS.COM	YHN07	(888) 888-8585
THEBESTNUMBERS.COM	YHN08	(888) 888-8585
THEBESTNUMBERS.COM	YHN09	(888) 888-8585
THEBESTNUMBERS.COM	YHN10	(888) 888-8585
THEBESTNUMBERS.COM	YHN11	(888) 888-8585
THEBESTNUMBERS.COM	YHN12	(888) 888-8585
THEBESTNUMBERS.COM	YHN13	(888) 888-8585
THEBESTNUMBERS.COM	YHN14	(888) 888-8585
THEBESTNUMBERS.COM	YHN15	(888) 888-8585
THEBESTNUMBERS.COM	YHN16	(888) 888-8585
THEBESTNUMBERS.COM	YHN17	(888) 888-8585
THEBESTNUMBERS.COM	YHN18	(888) 888-8585
THEBESTNUMBERS.COM	YHN19	(888) 888-8585
THEBESTNUMBERS.COM	YHN20	(888) 888-8585
THEBESTNUMBERS.COM	YHN99	(888) 888-8585
TIERRANET INC.	DXS01	(858) 560-8120
TIERRANET INC.	DXS99	(858) 560-8120
TIME WARNER TELECOM	INF01	(866) 654-2547
TIME WARNER TELECOM	INF99	(866) 654-2547
TIMESHIFT	JFT01	(323) 817-3220
TIMESHIFT	JFT99	(323) 817-3220
TIMESHIFT	JFX01	(323) 817-3220
TIMESHIFT	JFX99	(323) 817-3220

TMC COMMUNICATIONS	QQA01	(877) 862-8655
TMC COMMUNICATIONS	QQA02	(877) 862-8655
TMC COMMUNICATIONS	QQA50	(877) 862-8655
TMC COMMUNICATIONS	QQA51	(877) 862-8655
TMC COMMUNICATIONS	QQA52	(877) 862-8655
TMC COMMUNICATIONS	QQA53	(877) 862-8655
TMC COMMUNICATIONS	QQA54	(877) 862-8655
TMC COMMUNICATIONS	QQA55	(877) 862-8655
TMC COMMUNICATIONS	QQA56	(877) 862-8655
TMC COMMUNICATIONS	QQA57	(877) 862-8655
TMC COMMUNICATIONS	QQA58	(877) 862-8655
TMC COMMUNICATIONS	QQA59	(877) 862-8655
TMC COMMUNICATIONS	QQA98	(877) 862-8655
TMC COMMUNICATIONS	QQA99	(866) 742-5862
TNCI	DJK01	(800) 800-8400
TNCI	DJK02	(617) 369-1023
TNCI	DJK03	(617) 369-1023
TNCI	DJK04	(617) 369-1023
TNCI	DJK99	(617) 369-1023
TOLL FREE CONNECT INC	UKO01	(561) 802-4344
TOLL FREE CONNECT INC	UKO99	(561) 802-4344
TOLL FREE EXPRESS, INC.	FVD01	(949) 777-0137
TOLL FREE EXPRESS, INC.	FVD99	(949) 777-0137
TOLL-LESS.COM	BBT01	(203) 341-0372
TOLL-LESS.COM	BBT99	(203) 967-9102
TONE NETWORKS	BOV02	(888) 526-8663
TONE NETWORKS INC	BOV01	(888) 526-8663
TOTAL CALL INTERNATIONAL, INC	IRN01	(213) 239-0910
TOTAL CALL INTERNATIONAL, INC	IRN99	(213) 239-0910
TRANSACTION NETWORK SERVICES	KLS01	(703) 453-8500
TRANSACTION NETWORK SERVICES	KLS99	(703) 453-8465
TRICOM USA	UMS01	(809) 334-7397
TRICOM USA	UMS99	(809) 334-7397

TSI	GFD01	(805) 277-0400
TSI	GFD02	(805) 277-0400
TSI	GFD03	(805) 277-0400
TSI	GFD04	(805) 277-0400
TSI	GFD05	(805) 277-0400
TSI	GFD06	(805) 277-0400
TSI	GFD07	(805) 277-0400
TSI	GFD08	(805) 277-0400
TSI	GFD09	(805) 277-0400
TSI	GFD10	(805) 277-0400
TSI	GFD11	(805) 277-0400
TSI	GFD12	(805) 277-0400
TSI	GFD13	(805) 277-0400
TSI	GFD14	(805) 277-0400
TSI	GFD15	(805) 277-0400
TSI	GFD16	(805) 277-0400
TSI	GFD17	(805) 277-0400
TSI	GFD18	(805) 277-0400
TSI	GFD19	(805) 277-0400
TSI	GFD20	(805) 277-0400
TSI	GFF01	(805) 277-0400
TSI	GFF02	(805) 277-0400
TSI	GFF03	(805) 277-0400
TSI	GFF04	(805) 277-0400
TSI	GFF05	(805) 277-0400
TSI	GFF06	(805) 277-0400
TSI	GFF07	(805) 277-0400
TSI	GFF08	(805) 277-0400
TSI	GFF09	(805) 277-0400
TSI	GFF10	(805) 277-0400
TSI	GFF11	(805) 277-0400
TSI	GFF12	(805) 277-0400
TSI	GFF13	(805) 277-0400

TSI	GFF14	(805) 277-0400
TSI	GFF15	(805) 277-0400
TSI	GFF16	(805) 277-0400
TSI	GFF17	(805) 277-0400
TSI	GFF18	(805) 277-0400
TSI	GFF19	(805) 277-0400
TSI	GFF20	(805) 277-0400
TSI	GFF99	(805) 277-0400
TSI	GFT01	(805) 277-0400
TSI	GFT02	(805) 277-0400
TSI	GFT03	(805) 277-0400
TSI	GFT04	(805) 277-0400
TSI	GFT05	(805) 277-0400
TSI	GFT06	(805) 277-0400
TSI	GFT07	(805) 277-0400
TSI	GFT08	(805) 277-0400
TSI	GFT09	(805) 277-0400
TSI	GFT10	(805) 277-0400
TSI	GFT11	(805) 277-0400
TSI	GFT12	(805) 277-0400
TSI	GFT13	(805) 277-0400
TSI	GFT14	(805) 277-0400
TSI	GFT15	(805) 277-0400
TSI	GFT16	(805) 277-0400
TSI	GFT17	(805) 277-0400
TSI	GFT18	(805) 277-0400
TSI	GFT19	(805) 277-0400
TSI	GFT20	(805) 277-0400
TSI	GFU01	(805) 277-0400
TSI	GFU02	(805) 277-0400
TSI	GFU03	(805) 277-0400
TSI	GFU04	(805) 277-0400
TSI	GFU05	(805) 277-0400

TSI	GFU06	(805) 277-0400
TSI	GFU07	(805) 277-0400
TSI	GFU08	(805) 277-0400
TSI	GFU09	(805) 277-0400
TSI	GFU10	(805) 277-0400
TSI	GFU11	(805) 277-0400
TSI	GFU12	(805) 277-0400
TSI	GFU13	(805) 277-0400
TSI	GFU14	(805) 277-0400
TSI	GFU15	(805) 277-0400
TSI	GFU16	(805) 277-0400
TSI	GFU17	(805) 277-0400
TSI	GFU18	(805) 277-0400
TSI	GFU19	(805) 277-0400
TSI	GFU20	(805) 277-0400
UCN	BCU01	(800) 538-0904
UCN	BCU02	(800) 538-0904
UCN	BCU03	(800) 538-0904
UCN	BCU04	(800) 538-0904
UCN	BCU05	(800) 538-0904
UCN	BCU06	(800) 538-0904
UCN	BCU07	(800) 538-0904
UCN	BCU46	(800) 538-0904
UCN	BCU58	(800) 538-0904
UCN	BCU88	(800) 538-0904
UCN	BCU98	(800) 538-0904
UCN	BCU99	(800) 363-6177
UCN	FAM01	(800) 393-8593
UCN	FAM07	(800) 393-8593
UCN	FAM28	(800) 393-8593
UCN	FAM32	(800) 393-8593
UCN	FAM56	(800) 393-8593
UCN	FAM87	(800) 393-8593

UCN	FAM99	(602) 264-8684
UNION TELEPHONE	UNT01	(307) 782-6131
UNION TELEPHONE	UNT99	(307) 782-6131
UNIPOINT SERVICES, INC.	GHI01	(512) 735-1200
UNIPOINT SERVICES, INC.	GHI99	(512) 735-1200
UNISYS	BRUIS	(651) 687-2779
UNITEL COMMUNICATIONS GROUP IN	UZL01	(800) 499-5912
UNITEL COMMUNICATIONS GROUP IN	UZL99	(800) 499-5912
US LEC	UEC02	(704) 319-1104
US LEC	UEC03	(704) 319-1104
US LEC	UEC04	(704) 319-1104
US LEC	UEC05	(704) 319-1104
US LEC	UEC06	(800) 978-7532
US LEC	UEC07	(800) 978-7532
US LEC	UEC08	(800) 978-7532
US LEC	UEC09	(800) 978-7532
US LEC	UEC10	(800) 978-7532
US LEC OF NC, LLC	UEC01	(800) 978-7532
US LEC OF NC, LLC	UEC99	(800) 978-7532
US LINK INC.	USL99	(218) 568-4000
US PHONECOM, INC	WFF01	(818) 840-6969
US PHONECOM, INC	WFF99	(818) 840-6969
US SOUTH COMMUNICATIONS	UHC01	(770) 240-6160
US SOUTH COMMUNICATIONS	UHC99	(770) 240-6160
UTEL NETWORKS	UYT01	(877) 883-5638
UTEL NETWORKS	UYT02	(877) 883-5638
UTEL NETWORKS	UYT99	(877) 883-5638
VANITY INTERNATIONAL	VAN01	(858) 792-5000
VANITY INTERNATIONAL	VAN99	(858) 792-5000
VARTEC TELECOM	VRT01	(888) 702-4079
VARTEC TELECOM	VRT99	(888) 702-4079
VERISIGN INC (ILLUMINET)	UIN01	(800) 800-5443
VERIZON (LEC)	NXCMP	(212) 692-0610

VERIZON (LEC)	NXNE1	(212) 692-0610
VERIZON (LEC)	NXNYT	(212) 338-7400
VERIZON (LEC)	NXNY1	(212) 338-7400
VERIZON (LEC)	NXSE1	(212) 692-0610
VERIZON (LEC)	NXSM1	(212) 338-7400
VERIZON COMM.	BELLA	(800) 275-2355
VERIZON COMM.	BEL99	(703) 526-3229
VERIZON COMMUNICATIONS	BESG1	(800) 483-3722
VERIZON LEC	NXN99	(212) 338-7400
VERIZON SELECT SERVICES	GTSM1	(800) 483-8494
VERIZON SELECT SERVICES	GTWDA	(800) 483-8494
VERIZON SELECT SERVICES	GTWDT	(800) 483-8494
VERIZON SELECT SERVICES	GTWD1	(800) 483-8494
VERIZON SELECT SERVICES	GTWD2	(800) 483-8494
VERIZON SELECT SERVICES	GTWD3	(800) 483-8494
VERIZON SELECT SERVICES	GTWD4	(800) 483-8494
VERIZON SELECT SERVICES	GTWD5	(800) 483-8494
VERIZON SELECT SERVICES	GTWD6	(800) 483-8494
VERIZON SELECT SERVICES	GTW99	(800) 483-8494
VERIZON SELECT SERVICES, INC.	VZR01	(800) 483-3722
VERIZON SELECT SERVICES, INC.	VZR99	(800) 483-3722
VIDEOTRON TELECON LTE'E	VVT01	(514) 380-4619
VIDEOTRON TELECON LTE'E	VVT99	(514) 380-4619
VOICECOM TELECOMMUNICATIONS	PQC01	(770) 663-5062
VOICECOM TELECOMMUNICATIONS	PQC99	(404) 487-8475
VOXEO CORPORATION	VXML1	(407) 835-0065
VOXEO CORPORATION	VXM99	(407) 835-0065
VPT, INC.	VPT01	(512) 419-4600
VPT, INC.	VPT99	(512) 419-4600
WAKE UP INC.	WUP01	(404) 365-0800
WAKE UP INC.	WUP99	(404) 365-0800
WARNING COMMUNICATIONS, INC	WNM02	(602) 230-0420
WARNING COMMUNICATIONS, INC.	WNM01	(602) 230-0420

WARNING COMMUNICATIONS, INC.	WNM99	(800) 746-6396
WCI	WXI01	(206) 652-4470
WEPS	PMI01	(516) 378-9116
WEPS	PMI99	(800) 676-2223
WESTEL, INC.	WES01	(512) 480-5500
WESTEL, INC.	WES99	(512) 480-5500
WHOLESALE CARRIER SERVICES INC	WLS01	(954) 227-1700
WHOLESALE CARRIER SERVICES INC	WLS99	(954) 227-1700
WHOS CALLING INC	WHO11	(800) 621-6871
WHOS CALLING INC	WHO12	(800) 621-6871
WHOS CALLING INC	WHO13	(800) 621-6871
WHOS CALLING INC	WHO14	(800) 621-6871
WHOS CALLING INC	WHO15	(800) 621-6871
WHOS CALLING INC	WHO16	(800) 621-6871
WHOS CALLING INC	WHO17	(800) 621-6871
WHOS CALLING INC	WHO18	(800) 621-6871
WHOS CALLING INC	WHO19	(800) 621-6871
WHOS CALLING INC	WHO20	(800) 621-6871
WHOS CALLING INC	WHO21	(800) 621-6871
WHOS CALLING INC	WHO22	(800) 621-6871
WHOS CALLING INC	WHO23	(800) 621-6871
WHOS CALLING INC	WHO24	(800) 621-6871
WHOS CALLING INC	WHO25	(800) 621-6871
WHOS CALLING INC	WHO26	(800) 621-6871
WHOS CALLING INC	WHO27	(800) 621-6871
WHOS CALLING INC	WHO28	(800) 621-6871
WHOS CALLING INC	WHO29	(800) 621-6871
WHOS CALLING INC	WHO30	(800) 621-6871
WHOS CALLING INC	WHO31	(800) 621-6871
WHOS CALLING INC	WHO32	(800) 621-6871
WHOS CALLING INC	WHO33	(800) 621-6871
WHOS CALLING INC	WHO34	(800) 621-6871
WHOS CALLING INC	WHO35	(800) 621-6871

WHOS CALLING INC	WHO36	(800) 621-6871
WHOS CALLING INC	WHO37	(800) 621-6871
WHOS CALLING INC	WHO38	(800) 621-6871
WHOS CALLING INC	WHO39	(800) 621-6871
WHOS CALLING INC	WHO40	(800) 621-6871
WHOS CALLING INC	WHO41	(800) 621-6871
WHOS CALLING INC	WHO42	(800) 621-6871
WHOS CALLING INC	WHO43	(800) 621-6871
WHOS CALLING INC	WHO44	(800) 621-6871
WHOS CALLING INC	WHO45	(800) 621-6871
WHOS CALLING INC	WHO46	(800) 621-6871
WHOS CALLING INC	WHO47	(800) 621-6871
WHOS CALLING INC	WHO48	(800) 621-6871
WHOS CALLING INC	WHO49	(800) 621-6871
WHOS CALLING INC	WHO50	(800) 621-6871
WHOS CALLING INC	WHO51	(800) 621-6871
WHOS CALLING INC	WHO52	(800) 621-6871
WHOS CALLING INC	WHO53	(800) 621-6871
WHOS CALLING INC	WHO54	(800) 621-6871
WHOS CALLING INC	WHO55	(800) 621-6871
WHOS CALLING INC	WHO56	(800) 621-6871
WHOS CALLING INC	WHO57	(800) 621-6871
WHOS CALLING INC	WHO58	(800) 621-6871
WHOS CALLING INC	WHO59	(800) 621-6871
WHOS CALLING INC	WHO60	(800) 621-6871
WHOS CALLING INC	WHO61	(800) 621-6871
WHOS CALLING INC	WHO62	(800) 621-6871
WHOS CALLING INC	WHO63	(800) 621-6871
WHOS CALLING INC	WHO64	(800) 621-6871
WHOS CALLING INC	WHO65	(800) 621-6871
WHOS CALLING INC	WHO66	(800) 621-6871
WHOS CALLING INC	WHO67	(800) 621-6871
WHOS CALLING INC	WHO68	(800) 621-6871

WHOS CALLING INC	WHO69	(800) 621-6871
WHOS CALLING INC	WHO70	(800) 621-6871
WHOS CALLING INC	WHO71	(800) 621-6871
WHOS CALLING INC	WHO72	(800) 621-6871
WHOS CALLING INC	WHO73	(800) 621-6871
WHOS CALLING INC	WHO74	(800) 621-6871
WHOS CALLING INC	WHO75	(800) 621-6871
WHOS CALLING INC	WHO76	(800) 621-6871
WHOS CALLING INC	WHO77	(800) 621-6871
WHOS CALLING INC	WHO78	(800) 621-6871
WHOS CALLING INC	WHO79	(800) 621-6871
WHOS CALLING INC	WHO80	(800) 621-6871
WHOS CALLING INC	WHO81	(800) 621-6871
WHOS CALLING INC	WHO82	(800) 621-6871
WHOS CALLING INC	WHO83	(800) 621-6871
WHOS CALLING INC	WHO84	(800) 621-6871
WHOS CALLING INC	WHO85	(800) 621-6871
WHOS CALLING INC	WHO86	(800) 621-6871
WHOS CALLING INC	WHO87	(800) 621-6871
WHOS CALLING INC	WHO88	(800) 621-6871
WHOS CALLING INC	WHO89	(800) 621-6871
WHOS CALLING INC	WHO90	(800) 621-6871
WHOS CALLING INC	WHO91	(800) 621-6871
WHOS CALLING INC	WHO92	(800) 621-6871
WHOS CALLING INC	WHO93	(800) 621-6871
WHOS CALLING INC	WHO94	(800) 621-6871
WHOS CALLING INC	WHO95	(800) 621-6871
WHOS CALLING INC	WHO96	(800) 621-6871
WHOS CALLING INC	WHO97	(800) 621-6871
WHOS CALLING INC	WHO98	(800) 621-6871
WHO'S CALLING INC.	WHO01	(800) 621-6871
WHO'S CALLING, INC.	WHO02	(800) 621-6871
WHO'S CALLING, INC.	WHO03	(800) 621-6871

WHO'S CALLING, INC.	WHO04	(800) 621-6871
WHO'S CALLING, INC.	WHO05	(800) 621-6871
WHO'S CALLING, INC.	WHO06	(800) 621-6871
WHO'S CALLING, INC.	WHO07	(800) 621-6871
WHO'S CALLING, INC.	WHO08	(800) 621-6871
WHO'S CALLING, INC.	WHO09	(800) 621-6871
WHO'S CALLING, INC.	WHO10	(800) 621-6871
WHO'S CALLING, INC.	WHO99	(800) 621-6871
WILLIAMS/WITEL COMMUNICATIONS	KSW01	(877) 864-2309
WILLIAMS/WITEL COMMUNICATIONS	KSW02	(877) 864-2309
WILLIAMS/WITEL COMMUNICATIONS	KSW03	(877) 864-2309
WILLIAMS/WITEL COMMUNICATIONS	KSW99	(877) 864-2309
WINSTAR COMMUNICATIONS INC.	MID01	(888) 888-3039
WINSTAR COMMUNICATIONS INC.	MID99	(888) 888-3039
WIRESTAR COMMUNICATIONS	JWS01	(800) 947-3782
WIRESTAR COMMUNICATIONS	JWS99	(800) 947-3782
WORD OF MOUTH COMMUNICATIONS	WOM01	(847) 926-4444
WORD OF MOUTH COMMUNICATIONS	WOM99	(847) 272-7737
WORLD COMMUNICATIONS INC	WXI99	(206) 652-4470
WORLD ONE TELECOM, LLC	KGE01	(213) 675-0218
WORLD ONE TELECOM, LLC	KGE99	(213) 675-0218
WORLD WIDE TELEGRAPH	RUC01	(877) 272-2576
WORLD WIDE TELEGRAPH	RUC22	(877) 272-2576
WORLD WIDE TELEGRAPH	RUC25	(877) 272-2576
WORLD WIDE TELEGRAPH	RUC99	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN01	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN02	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN03	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN04	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN05	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN06	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN07	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN08	(877) 272-2576

WORLDWIDE TELEGRAPH	RUN09	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN10	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN11	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN12	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN13	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN14	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN15	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN16	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN17	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN18	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN19	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN20	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN21	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN22	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN23	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN24	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN25	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN26	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN27	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN28	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN29	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN30	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN31	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN32	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN33	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN34	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN35	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN36	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN37	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN38	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN39	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN40	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN41	(877) 272-2576

WORLDWIDE TELEGRAPH	RUN42	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN43	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN44	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN45	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN46	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN47	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN48	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN49	(877) 272-2576
WORLDWIDE TELEGRAPH	RUN50	(877) 272-2576
WORLDXCHANGE COMMUNICATIONS	CMT99	(800) 576-7775
X2 COMMUNICATIONS	DIC99	(908) 782-3177
XO COMMUNICATIONS	IVN01	(503) 972-6833
XO COMMUNICATIONS	IVN99	(503) 972-6897
XO COMMUNICATIONS	NLS01	(888) 575-6398
XO COMMUNICATIONS	NLS02	(888) 575-6398
XO COMMUNICATIONS	NLS03	(888) 575-6398
XO COMMUNICATIONS	NLS99	(888) 575-6398
XO COMMUNICATIONS	NLV99	(702) 990-1000
XTEL COMMUNICATIONS	YXT01	(856) 596-4000
XTEL COMMUNICATIONS	YXT99	(856) 596-7000
ZONE TELECOM INC	OOZ02	(866) 539-9663
ZONE TELECOM, INC	OOZ01	(866) 539-9663
ZONE TELECOM, INC	OOZ03	(866) 539-9663
ZONE TELECOM, INC	OOZ04	(866) 539-9663
ZONE TELECOM, INC	OOZ05	(866) 539-9663
ZONE TELECOM, INC	OOZ99	(866) 539-9663
Z-TEL NETWORK SERVICES	ZNS01	(813) 233-4554
Z-TEL NETWORK SERVICES	ZNS02	(813) 233-4554
Z-TEL NETWORK SERVICES	ZNS03	(813) 233-4554
Z-TEL NETWORK SERVICES	ZNS04	(813) 233-4554
Z-TEL NETWORK SERVICES	ZNS05	(813) 233-4554
Z-TEL NETWORK SERVICES	ZNS99	(813) 262-3226

Next Generation Interconnection Interoperability Forum (NGIIF) Reference Document: Part XIII, Terms and Definitions

Alliance for Telecommunications Industry Solutions

Approved November 8, 2019

Abstract

This document provides definitions for many of the uncommon terms and abbreviations as used in the NIIF Reference Documents.

Foreword

The Alliance for Telecommunications Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The Next Generation Interconnection Interoperability Forum (NGIIF) addresses next-generation network interconnection and interoperability issues associated with emerging technologies. Specifically, it develops operational procedures which involve the network aspects of architecture, disaster preparedness, installation, maintenance, management, reliability, routing, security, and testing between network operators. In addition, the NGIIF addresses issues which impact the interconnection of existing and next generation networks and facilitate the transition to emerging technologies.

The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages. The word *may* denotes a optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, NGIIF, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, NGIIF, which was responsible for its development, had the following leadership:

Karen Riepenkroger, Sprint

Randee Ryan, Comcast

Trademark Acknowledgements

iconectiv®, Telcordia®, and Common Language® are registered trademarks and CLCI™, CLLI™, LERG™ Routing Guide and TPM™ Data Source are trademarks and the Intellectual Property of Telcordia Technologies, Inc. dba as iconectiv.

ATIS Standard on –

Next Generation Interconnection Interoperability Forum (NGIIF) Reference Document: Part XIII, Terms and Definitions

TERMS AND DEFINITIONS

The following are definitions of terms used in Next Generation Interconnection Interoperability (NGIIF) documents.

3-Tone Slope: The difference in loss between 1004 Hz and 404 Hz and 2804 Hz (also see “Attenuation Distortion”).

555 Assignee/Number Holder: The entity to whom a 555 number has been assigned.

Access Code: A uniform seven-digit code assigned by the Access Service Provider to an individual customer. The seven-digit code for Feature Group D has the form 101XXXX, and the seven-digit code for Feature Group B has the form 950-XXXX.

Access Gateway: An access interface between multiple types of line side services and devices and the packet network. Examples of these services and devices are Plain Old Telephone Service (POTS) telephones, Basic Rate Interface (BRI) sets, Coin telephones, as well as some Digital Subscriber Line (DSL) and private lines/special services on 2 and 4 wire DS0, DS1 interfaces, etc. The Access Gateway may also support an interface for line-based GR-303/TR-08 remote terminals. The Access Gateway may also provide functions such as audible ringing, power ringing, miscellaneous tones, etc. The Access Gateway may be connected to the network via various bit-rate and physical layer interfaces, and may be installed in controlled or outdoor environments. A Call Agent provides the specific call control, call processing and other management functions for the services and devices terminated on the Access Gateway.

Access Service Customer (ASC) or Interexchange Customer: 1) Any individual, partnership, association, joint-stock company, trust, governmental entity or corporation engaged for hire in interstate or foreign communication by wire or radio, between two or more exchanges. 2) In an evolving telecommunications environment, the term can also be used to denote wireless, internet protocol or other Next Generation Network (NGN) elements used between two or more networks.

Access Service Provider (ASP): 1) A company engaged in the business of furnishing access service in a franchised territory. 2) The term Access Service Provider (ASP) could also denote a company engaged in the business of supplying services such as wireless, internet protocol, or other Next Generation Network (NGN) elements.

Access Service Request (ASR): The ordering form used to request Access Services, both Special and Switched.

Access Tandem: 1) A telephone company or centralized equal access provider switching system that provides a concentration and distribution function for originating or terminating traffic between end offices and a customer-designated premises. [NECA/ FCC-5] 2) An exchange carrier switching system that provides a traffic concentration and distribution function for inter- Local Access & Transport Area (LATA) traffic originating/terminating within a Local Access & Transport Area (LATA). [T1.506-1989]

Active Code: An NPA-NXX code assigned to a Service Provider (SP) by the Central Office (CO) Code Administrator and implemented in the Public Switched Telephone Network (PSTN) for specific routing and rating requirements as of the LERG™ Routing Guide effective date.

Additional Cooperative Acceptance Testing (ACAT): ACAT of Switched Access Service involves the Access Service Provider provision of a technician at its office(s) and the customer provides a technician at its location, with suitable test equipment to perform the required tests.

ACATs may, for example, consist of the following tests:

- Impulse Noise
- Phase Jitter
- Signal to C-Notched Noise Ratio
- Intermodulation (Nonlinear) Distortion
- Frequency Shift (Offset)
- Envelope Delay Distortion
- Dial Pulse Percent Break

Administrative Numbers: Administrative numbers are numbers used by telecommunications carriers to perform internal administrative or operational functions necessary to maintain reasonable quality of service standards. (FCC 00-104 §52.15 (f)(1) (i))

Examples of administrative numbers are: Test numbers, employee/official numbers, Location Routing Numbers, Temporary Local Directory Numbers, soft dial tone numbers and wireless E9-1-1 (Emergency Service Routing Digits (ESRD)/Emergency Service Routing Key (ESRK)) numbers.

Administrative Operating Company Number (AOCN): A four character numeric or alphanumeric that identifies the administrator of one (or more) data records contained in iconectiv®'s Business Integrated Rating and Routing Database System (BIRRDs). Numeric/alphanumeric AOCNs are determined by Operating Company Number (OCN) assignment. The AOCN further identifies the entity authorized by the code holder to input and maintain data into BIRRDs.

Advanced Intelligent Network (AIN): A telecommunications network architecture that uses databases to facilitate call processing, call routing, and network management, allowing carriers to change the routing of both inbound and outbound calls from moment to moment. [FCC-5] 2. A proposed Intelligent Network (IN) architecture that includes both IN/1+ and IN/2 concepts.

Affected Parties: 1) those entities that have applied for and/or received central office code (NXX) assignments or reservations, or thousands-block (NXX-X) assignments; 2) all interested members of the industry within the affected NPA. This term is further defined in ATIS-0300119, Thousands-Block (NPA-NXX-X) & Central Office Code (NPA-NXX) Administration Guidelines (TBCOCAG).

Agency Authorization: See "Customer's Agent"

Alternate Mark Inversion (AMI) Signal: A pseudo ternary signal, representing binary digits, in which (a) successive "marks" are of alternately positive and negative polarity and the absolute values of their amplitudes are normally equal and (b) "spaces" are of zero amplitude. Synonym bipolar signal.

Answer/Disconnect Supervision: Denotes the transmission of the switch trunk equipment supervisory signal (off-hook or on-hook) to the customer's point of termination, typically as an indication that the called or calling party has answered or disconnected.

Applicant/Code Applicant: Service Providers who submit a Central Office Code Request to the Central Office (CO) Code Administrator for the purpose of being assigned a CO Code for their use. In thousands-block telephone number pooling, the Pooling Administrator is authorized to apply for the assignment of CO Codes as outlined in ATIS-0300119, Thousands-Block (NPA-NXX-X) & Central Office Code (NPA-NXX) Administration Guidelines (TBCOCAG).

ASC: See "Access Service Customer"

ASP: See "Access Service Provider"

Assigned Numbers: Assigned numbers are numbers working in the Public Switched Telephone Network (PSTN) under an agreement such as a contract or tariff at the request of specific end users or customers for their use, or numbers not yet working but having a customer service order pending. Numbers that are not yet working and have a service order pending for more than five calendar days shall not be classified as assigned numbers. (FCC 00-104 §52.15 (f)(1) (iii))

Attenuation Distortion: The difference in loss at specified frequencies relative to the loss at 1004 Hz, unless otherwise specified. [NECA/ FCC-5]

Audit: (relative to numbering guidelines and FCC regulations): The accumulation and evaluation of evidence about documented information of an auditee to determine and report on the degree of compliance with Industry Numbering Committee (INC) industry guidelines. Audit or auditing also refers to examination and verification during testing and other telecommunication switch functions.

Automatic Code Gap (ACG): A code control that is implemented automatically in response to a request from a database to limit traffic. This control can be in the form of six (6) through ten (10) digits. A six-digit control is used to protect the database in instances of a general overload. A ten-digit control is used to control focused overloads.

Automatic Congestion Control (ACC): ACC is a two-part feature. In order for ACC to function properly it must be implemented in the originating and terminating nodes of an interconnected network. The first part enables a (terminating) network node to alert interconnected nodes that it is in Machine Congestion 1 or 2 (MC1 or MC2). The second part allows a distant (originating) network node to automatically react to an ACC message and enact trunk group controls (Cancel To (CANT) and SKIP) on specific trunk groups.

Automatic Number Identification (ANI): 1) A service feature in which the directory number or equipment number of a calling station is automatically obtained. Note: ANI is used in message accounting. 2) The code that provides the billing number of the line or trunk that originated a call. [T1.104-1988] 3) A system that identifies the billing account for a call. For 9-1-1 systems, the ANI identifies the calling party and may be used as a call back number. [47CFR]

Automatic Scheduled Testing (AST): AST of Switched Access Services (Feature Groups B, C and D), where the customer provides remote office test lines and 105 test lines with associated responders or their functional equivalent, will consist of monthly loss and C-message noise tests and annual balance test.

B8ZS (Bipolar with 8-Zero Substitution): A code in which eight consecutive zeros are replaced with the sequence 000+-0-+ if the preceding pulse was + and with the sequence 000-+0+- of the preceding pulse was -, where + represents a positive pulse, - represents a negative pulse, and 0 represents no pulse.

Balance (100 TYPE) Test Line: An arrangement in an end office which provides for balance and noise testing. The test can be either 600 ohm or 900 ohm depending on office type.

Bit Error Rate: Deprecated term. See "Bit Error Ratio".

Bit Error Ratio (BER): The number of erroneous bits divided by the total number of bits transmitted, received, or processed over some stipulated period. Note 1: Examples of bit error ratio are (a) transmission BER, i.e., the number of erroneous bits received divided by the total number of bits transmitted; and (b) information BER, i.e., the number of erroneous decoded (corrected) bits divided by the total number of decoded (corrected) bits. Note 2: The BER is usually expressed as a coefficient and a power of 10; for example, 2.5 erroneous bits out of 100,000 bits transmitted would be 2.5 out of 105 or 2.5×10^{-5} .

Bit Error Rate Test: A test performed on a digital facility/service which counts erroneous bits and divides them by the bits sent over a set period of time. Usually expressed as a power of 10 e.g. (1×10^{-6}) .

Business Information Rating and Routing System (BIRRDs): A centralized database maintained by iconectiv® through which Service Providers or their authorized representatives enter and maintain routing and rating data in support of their NANP numbering assignments. Output from BIRRDs includes the iconectiv® LERG™ Routing Guide and the iconectiv® TPM™ Data Source.

Block Holder: The Service Provider to which a thousands-block (NXX-X) has been assigned for use.

Blocked Call: A blocked call is said to have occurred when a call presented to a telecommunications Service Provider facility cannot be completed due to Blocking.

Blocking: 1) The formatting of data into blocks for purposes of transmission, storage, checking, or other functions. 2) Denying access to, or use of, a facility, system, or component. 3) The failure of a telecommunications network to meet a user service demand, because of the lack of an available communications path.

C-Message Noise: The frequency weighted average noise within an idle voice channel. The frequency weighting, called C-message, is used to simulate the frequency characteristic of the 500-type telephone set and the hearing of the average subscriber.

C-Notched Noise: The C-message frequency weighted noise on a voice channel with a holding tone, which is removed at the measuring end through a notch (very narrow band) filter.

Call Agent: Provides call processing, call control, feature control and Operations Administration Maintenance & Provisioning to manage services for a packet network comprised of multiple types of media gateway endpoints.

ATIS-0300036

The network itself may transport traffic over many types of packet switching fabric, such as Internet Protocol (IP), Ethernet, Asynchronous Transfer Mode (ATM), or Frame Relay. The Media Gateways (i.e., Access and Trunk Gateways) may be connected to the network via various bit-rate and physical layer interfaces. The Call Agent may use one or many different control protocols to communicate with the media gateways. The Call Agent provides the intelligence and capability to control the overall node-to-node signaling for both on-net and off-net calls. This is sometimes referred to as a "Softswitch".

Call Gap (CG): A code control that regulates the maximum rate at which calls are released toward a destination code. Equipment vendors commonly provide the capability to Call Gap at intervals of 0.10 to 600 seconds on a range of numbers from three (3), six (6), or seven (7), through ten (10) digits.

Call Through Test: Confirms capabilities of the interface relative to an actual or simulated call: Basic call set-up; sequential, acknowledged transmission of user data; and call termination.

Called Party Pays: A service for which the end user receives and pays for call.

Calling Party Pays: A service for which the end user originates and pays for a call.

Canadian Central Office Code (NXX) Assignment Guidelines (Canadian COCAG): The Canadian Radio-television and Telecommunications Commission (CRTC) approves recommendations made by the Canadian Steering Committee on Numbering (CSCN), which recommends guidelines to the CRTC for the administration of Central Office (CO) Codes within Canadian Numbering Plan Areas (NPAs) by a Canadian independent third party administrator called the Canadian Numbering Administrator (CNA). The purpose of these Guidelines is to provide direction to the CNA, Code Applicants, and Code Holders with respect to the administration, assignment, activation, and use of CO Codes and the numbering resources contained therein.

Cancel To (CANT): A trunk group control that allows traffic to be canceled before hunting for a circuit to a destination. Equipment vendors commonly provide the capability to implement this control on a percentage basis.

Carrier Identification Code (CIC): Used to route and bill calls in the public switched telephone network. CICs are four-digit codes in the format XXXX, where X is any digit from 0 through 9. Separate CIC pools are maintained for Feature Group B (line side) access and Feature group D (trunk side) access. CICs are assigned by the North American Numbering Plan Administrator (NANPA) according to guidelines developed by the ATIS-sponsored Industry Numbering Committee.

Central Office (CO): 1) A common carrier switching center in which trunks and/or loops are terminated and switched. Note: In the DOD, "common carrier" is called "commercial carrier." Synonym switch. Other synonyms [loosely] end office, exchange, local central office, local exchange, local office, switching center (except in DOD DSN [formerly AUTOVON] usage), switching exchange, telephone exchange. 2) A switching unit, in a telephone system which provides service to the general public, having the necessary equipment and operations arrangements for terminating and interconnecting subscriber lines and trunks or trunks only. There may be more than one central office in a building. [47 CFR Pt.36-A]

Central Office (CO) Code: The second three digits (NXX) of a ten-digit telephone number in the form NXX-NXX-XXXX, where N represents any one of the numbers 2 through 9 and X represents any one of the numbers 0 through 9. (47 C.F.R. § 52.7(c))

Central Office (CO) Code Administrator: Responsible for the administration of the NXXs within a Numbering Plan Area.

Central Office Code (NXX) Exhaust: A point in time at which the quantity of TNs within existing CO codes (NXX) which are “Available for Assignment” equals zero within a switching entity/Point Of Interconnection (POI) or, conversely, when the quantities of “TNs Unavailable for Assignment” equal 10,000 times the quantity of existing CO codes (NXX) assigned to a switching entity/POI. Where CO code sharing occurs or partial CO codes are assigned to a switching entity/POI, the latter number should be adjusted accordingly.

Certify/Certification: The authorization of a carrier by a regulator to provide a telecommunications service in the relevant geographic area. FCC § 52.15 (g)(2)(i) requires that applications for initial numbering resources shall include evidence that the applicant is authorized to provide service in the area for which numbering resources are being requested.

Chronic Trunk: A trunk experiencing a much higher than normal rate of failure or switching irregularities, over a period of time, with resulting high incidence of test O.K. or no trouble found.

CLEC (Competitive Local Exchange Carrier): In the United States, a CLEC is a facility based communications company that competes with the already established local telephone business by providing its own network and switching. The term distinguishes competitors from established Local Exchange Carriers (LECs) and arises from the Telecommunications Act of 1996, which was intended to promote competition among both long-distance and local phone Service Providers. Similarly in Canada, CLECs are addressed by Telecom Decision CRTC 97-8, 1 May 1997 (Decision 97-8).

CLONES: CLONES is maintained by iconectiv® as the Location Registry for the creation and maintenance of Common Language® Location Code (CLLI™ Code) by Common Language subscribers. For an 11-character location identifier to be termed a CLLI™ Code, it must have been created and currently reside in CLONES. Associated information includes postal code, latitude and longitude, vertical and horizontal coordinates, and switching system type.

Code Holder: An assignee of a pooled or non-pooled NXX code that is assigned by the CO Code Administrator. The responsibilities of an assignee for a pooled NXX are defined in Section 8.2.1 and for a non-pooled NXX are defined in Section 8.3.1 of ATIS-0300119, Thousands-Block (NPA-NXX-X) & Central Office Code (NPA-NXX) Administration Guidelines (TBCOCAG). A given Code Holder is identified in the LERG™ Routing Guide as the NPA-NXX-A (Assignee) OCN record holder.

Common Language® Location Code (CLLI™ Code): An eleven-character alphanumeric descriptor used to identify switches, points of interconnection, and other categories of telephony network elements and their locations. For an 11-character location identifier to be termed a CLLI™ Code, it must reside in CLONES. Companies that are subscribers of Common Language® Location Information Service can refer questions to their company's CLLI™ Code Coordinator.

Competitive Access Provider (CAP): A telecommunications carrier that provides access services which are alternate to (or which bypass) a local exchange carrier.

Code Activation: See “Active Code”.

Code Holder: An assignee of an NXX code which was allocated by the Central Office (CO) Code Administrator.

Company Code: A unique four-character alphanumeric code (NXXX) assignable to all telecommunications Service Providers. For purposes of this document N=0-9 and X=0-9 or A-Z.

Compatibility Testing: Ensures that the software interface between the two contracting networks perform in a manner which demonstrates that all basic functions and utilities operate as specified.

Conservation (relative to numbering guidelines): Consideration given to the efficient and effective use of a finite numbering resource in order to minimize the cost and need to expand its availability in the introduction of new services, capabilities and features.

Contamination (relative to numbering guidelines and FCC regulations): Contamination occurs when at least one telephone number within a thousands-block of telephone numbers is not available for assignment to end users or customers. Blocks contaminated up to and including 10 percent are eligible for donation. For purposes of this provision, a telephone number is "not available for assignment" if it is classified as administrative, aging, assigned, intermediate, or reserved as defined in FCC rules (FCC 00-104, §52.7 (h)).

Control Office: An Access Service Provider (ASP) center or office that has been designated as Control Office on a given access service furnished to an Access Service Customer (ASC).

Conversion Timing: The actual agreed upon scheduled date and time to commence cutover in a coordinated conversion.

Cooperative Scheduled Testing (CST): CST of Switched Access Services (Feature Groups B, C and D), where the Access Service Provider provides a technician at its office(s) and the customer provides a technician at its location, with suitable test equipment to perform the required tests, will consist of quarterly loss and C-message noise tests, and annual balance tests. However, the customer may specify a more frequent schedule of tests. In addition to the loss/noise/balance measurements, the customer may also order, at additional charges, gain-slope and C-notched testing.

The Access Service Provider will provide, on a quarterly basis, a CST report that lists the test results for each trunk tested. Trunk test failures requiring customer participation for trouble resolution will be provided to the customer on an as-occurs basis.

Coordinated Conversion: A process whereby a portion of the equipment or facilities from an existing service is to be reused in a replacement service.

Customer(s): Any individual, partnership, association, joint-stock company, trust, corporation or governmental entity, or other entity which orders access services from an Access Service Provider including interexchange carriers and end users.

Customer's Agent: An entity which has an agreement between itself and its customer empowering it to act as the customer's agent in providing and maintaining that customer's service. The entity obtains an agency authorization for its customer specifying the degree and term of the responsibility.

Customer Premises Equipment (CPE): All telecommunications terminal equipment located on the customer premise, except equipment not covered by FCC exception or waiver.

Data Network Control Center (DNCC) or Equivalent: Is the name used to describe the center which administers and maintains Data Networks (e.g., X.75 Gateways).

Data Transmission (107 Type) Test Line: An arrangement which provides for a connection to a signal source which provides test signals for one-way testing of data and voice transmission parameters.

Decibel: A unit used to express relative difference in power, usually between acoustic or electric signals, equal to ten (10) times the common logarithm of the ratio of two signal powers.

Design, Verify, and Assign (DVA): Describes a given point in the order completion process in which the circuit design is checked for accuracy and all assignments are verified/available.

Di Group: A basic group of Pulse Code Modulation (PCM) channels assembled by Time Division Multiplex. In the United States it usually consists of 24 channels at 1.544 Mbs.

Digital to Analog (D/A): Used to describe when a digital to analog conversion takes place.

Digital/Analog Conversion: The changing of a digital signal to an analog signal carrying equivalent information.

Digital Switch: A Switch in which connections are established by operations on digital signals without conversion to analog.

Directory Assistance (DA): A service providing the requested telephone number for a given name and address.

Directory Assistance Call Completion (DACC): After the telephone number has been received, DACC is a service that permits a call to be completed to the requested number, typically at the calling party's option for an additional charge.

DSX: A digital cross connect field which can be utilized for DS1, DS2 or DS3 level cross connections at a digital level.

Echo Return Loss: A frequency weighted measure of return loss over the middle of the voice band, where talker echo is most annoying.

Effective 2-Wire: A condition which permits the simultaneous transmission in both directions over a channel, but it is not possible to insure independent information transmission in both directions. Effective 2-wire channels may be terminated with 2-wire or 4-wire interfaces.

Effective 4-Wire: A condition which permits the simultaneous independent transmission of information in both direction over a channel. The method of implementing effective 4-wire transmission is at the discretion of the Access Service Provider (physical, time domain, frequency-domain separation or echo cancellation techniques).

Effective Date: The date by which routing and rating changes must be complete for the assigned thousands-block or the assigned Central Office Code. Also, the date by which the thousands-block becomes an active block. (Also referred to as "the LERG™ Routing Guide effective date.")

End Office Switch: An Access Service Provider switching system where Telephone Exchange Service customer station loops are terminated for purposes of interconnection to trunks. It is the office providing dial-tone and is the first line in switching. An End Office may also be a Host Office or a Remote Switching Office.

End-to-End Testing: The testing, with assistance from the Access Service Providers (ASPs), of an Access Service Customer (ASC) provided service comprised of facilities and/or equipment of the ASC and the access services provided by the ASP(s).

End User: Any customer of an interexchange or foreign telecommunications service that is not a carrier, except that a carrier shall be deemed to be an "end user" to the extent that such carrier uses a telecommunications service for administrative purposes, without making such service available to others, directly or indirectly.

Envelope Delay Distortion: A measure of the linearity of the phase versus frequency of a channel.

Equal Level Echo Path Loss (ELEPL): The measure of Echo Path Loss (EPL) at a 4-wire interface which is corrected by the difference between the send and receive Transmission Level Point (TLP). $[ELEPL = EPL - TLP (send) + TLP (receive)]$.

Exchange: A geographic area tariffed by a state utilities commission and served by an incumbent Local Exchange Carrier (LEC). A LEC's franchise territory is comprised of multiple Exchanges and the Basic Local Calling Areas are defined by Exchanges. The Exchanges are generally in the state General Subscriber Services Tariff, Section A3.

The term "Exchange" denotes a geographic area generally smaller than a Local Access Transport Area (LATA) and usually embraces a city, town or village and its environs. Subscribers in a given Exchange area may be served by one or more central offices together with the associated facilities or subscribers in an Exchange area may be served by a central office located in an adjacent Exchange area. (A LATA is usually comprised of multiple Exchanges.)

Exchange Access Services: Service provided by Local Exchange Carriers (LECs) to interconnecting entities (such as interexchange carriers) in the areas in which the LECs offer telecommunication services.

Expected Measured Loss (EML): A calculated loss which specifies the end-to-end 1004-Hz loss on a terminated test connection between two readily accessible manual or remote test points. It is the sum of the inserted connection loss and test access loss including any test pads.

Facility: Medium that allows the movement of information by means of an electrical transmission system or path.

Feature Groups: Switched Access Service (SAS) will be provided by the ASPs in different arrangements known as feature groups.

Feature Group A (FGA): FGA is provided on a single or multiple line group basis and is arranged for originating calling only, terminating calling only, or two-way calling. FGA is arranged for use by the customer in the provision of its FX/ONAL service or MTS/WATS-type service.

ATIS-0300036

FGA provides a line side termination at the first point of switching. The line side termination will be provided with either ground start or loop start supervisory signaling at the option of the customer.

Feature Group B (FG B): Trunk side connections provided to an Access Service Provider (ASP) switch. End users will access the Access Service Customer (ASC) network by dialing 950-XXXX where the XXXX specifies a particular ASC's Switched Access Services (SAS) group. The following is an example of this feature group. The ASP switch will select an idle SAS in the group to the ASC switch and connect it to the end user's termination upon detection of a seizure on the SAS, the ASC switch will return dial tone to the end user indicating that it is prepared to receive the Personal Identification Number (PIN) and the address digits of the distant station. In the terminating direction, the ASC switch will select an idle SAS in the group to the ASP switch and, upon receipt of a start dial signal from the ASP switch, will send the address digits of the called party to the ASP switch which will complete handling of the call. FG B includes previous Exchange Network Facilities for Interstate Access (ENFIA) B and ENFIA C services only.

Feature Group C (FG C): Trunk side connections provided to the Access Service Provider (ASP) switch and will consist only of service provided to AT&T. Initially, this FG will be comprised of the access portion of existing Bell System toll completing, toll connecting and two-way non-intertoll trunks. Existing dialing patterns for originating and terminating calling will remain in effect for FG C.

Feature Group D (FG D): Trunk side connections provided to the Access Service Provider (ASP) switch and will be available to all Access Service Customer (ASCs) including AT&T-C. FG D will provide equal access to all ASCs such that end users will be required to dial the same number of digits to access each individual ASC. As currently proposed, the access digits dialed would be 101XXXX where XXXX specifies the ASC unless an end user "presubscribes" to a particular ASC. In this case the end user need only dial the called party's number (preceded by a 1 where required).

Federal Communications Commission (FCC): The board of commissioners, appointed by the president of the United States under the Communications Act of 1934, having the power to regulate interstate and foreign communications originating in the United States by wire and radio.

Final Trunk Group: A trunk group that does not route advance or alternate route to another trunk group if all of its trunks are busy.

First Point of Switching: The first Telephone Company location at which switching occurs on the terminating path of a call proceeding from the customer location to the terminating end office and, at the same time, the last Access Service Provider location at which switching occurs on the originating path of a call proceeding from the originating end office to the customer location.

Foreign NPA (FNPA): Any other Numbering Plan Area (NPA) different from the Home NPA (HNPA). This may be outside the geographic NPA from which a call originates or part of an overlay of the Home NPA.

Former ASC: The Access Service Customer (ASC) providing the existing service involved in a coordinated conversion.

Frequency Shift: The change in the frequency of a tone as it is transmitted over a channel.

Gateway: A network element that permits communication between two organizationally or technically dissimilar networks.

Glare: A condition where by two-way trunks are subject to occasional simultaneous seizures at both ends because of the unguarded interval between the seizure of the trunk at one end and the consequent recognition of seizure at the other end.

Glare Master/Control: The designated switch that retains control of a two-way trunk in the event of simultaneous seizure from both ends.

Home NPA (HNPA): Numbering Plan Area (NPA) in which a calling subscriber is located.

Homing Tandem Operating Company The company identified in the iconectiv® LERG™ Routing Guide as being the owner of the tandem to which the switching entity serving the NXX code homes.

iconectiv® LERG™ Routing Guide: Contains information about the local routing data obtained from the Telcordia Business Integrated Rating and Routing Database System (BIRADS) system. This information reflects the current network configuration and scheduled network changes for all entities originating or terminating Public Switched Telephone Network calls within the North American Numbering Plan.

Incumbent Local Exchange Carrier (ILEC): Incumbent local exchange carrier means (as stated in FCC 1996 Act, Section 251(h) (1)), with respect to area, the local exchange carrier that on February 8, 1996 provided telephone exchange service in such area; and on February 8, 1996, was deemed to be a member of the National Exchange Carrier Association (NECA) pursuant to section 69.601(b) of the Commission's regulation (47 C.F.R. 69.601(b)); or is a person or entity that, on or after February 8, 1996, became a successor or assign of a member described in clause (1). NOTE: The NECA categories of ILEC and Regional Bell Operating Company (RBOC) are used in the iconectiv® LERG™ Routing Guide to identify all incumbent exchange carriers. However, to differentiate between the incumbent independent telephone companies and the Bell Operating Companies (BOC) prior to 1984, the independent companies are identified by the ILEC category and the BOC are identified by the RBOC category.

Impaired: Is where an individual circuit exceeds the transmission limits or where the quality of service is diminished. A circuit is also impaired if its signaling functions (e.g., seizure, disconnect, ANI) are experiencing intermittent failures.

Impulse Noise: Any momentary occurrence of the noise on a channel over a specified level threshold. It is evaluated by counting the number of occurrences which exceed the threshold, over a set time period.

Individual Case Basis (ICB): Used to describe instances where normal procedures do not apply.

Industry Carriers Compatibility Forum (ICCF): A now retired forum for the discussion and resolution of national technical issues associated with network interconnection. This forum was merged into the Network Interconnection Interoperability Forum on January 1, 1997.

Industry Numbering Committee (INC): A standing committee of the Alliance for Telecommunications Industry Solutions (ATIS) that provides an open forum to address and resolve industry-wide issues associated with the planning, administration, allocation, assignment and use of numbering resources and related dialing considerations for public telecommunications within the North American Numbering Plan (NANP) area.

Initial Code: The first geographic NXX code assigned to a Service Provider for each rate center in which it provides service.

Inoperative: Is where an individual circuit will not function in service (e.g., open, shorted) or cannot transmit address signaling in either direction.

In Service: A code or block for which local routing information has been input to the LERG™ Routing Guide and the carrier has begun to activate and assign numbers within the NXX code or NXX-X block to end users (FCC 00-104, ¶240).

Institute of Electrical and Electronic Engineers (IEEE): The U.S. organization for professional electrical engineers.

Intercarrier Testing: The testing of multiple Access Service Customer (ASC) connected services, i.e., testing over the facilities and equipment provided by multiple ASC(s) and the access service(s) provided by the Access Service Providers.

Interexchange Carrier (IC or IXC): A telecommunications company engaged for hire that provides interprovincial/intraprovincial (Canadian), interstate/interLATA (US), or intrastate/interLATA (US) services.

Interexchange Customer Service Center (ICSC or equivalent): An Access Service Negotiation work group which will handle inquiries and orders. It is to serve as a point of contact for the access service needs of Interexchange Customers.

InterLATA: Term used to describe the traffic going between Local Access and Transport Areas or Market area.

Intermediate Network: Any interconnecting network(s) between the originating network and terminating network.

International Telegraph and Telephone Consultative Committee (CCITT): One of two committees that support the International Telecommunication Union by conducting studies on technical and operating questions and recommending standards; the other is the International Radio Consultative Committee.

IntraLATA: Term used to describe the traffic within a Local Access and Transport Area or Market area.

Inventory: All telephone numbers distributed, assigned or allocated:

- (1) To a Service Provider, or
- (2) To a pooling administrator for the purpose of establishing or maintaining a thousands-block number pool (FCC 00-104, § 52.7 (j)).

(Industry) Inventory Pool: Used in thousands-block number pooling to describe a reservoir of unassigned thousands-blocks administered by the Pooling Administrator for purposes of assignment to certified Service Providers participating in thousands-block number pooling.

ATIS-0300036

Internet Protocol Enabled Services (IPES): A Service Provider deploying Internet Protocol (IP)-enabled services, including Voice over Internet Protocol (VoIP) services, on a commercial basis to residential and business customers. Company Codes in this Category shall be used to identify IP-enabled Service Providers interconnecting to the Public Switched Telephone Network (PSTN) and can be used to enable the deployment of any new IP-enabled service, technology or advanced service. VoIP is transmission of voice (such as ordinary telephone calls) using Internet Protocol.

Isolation: The process of determining the circuit element which has failed (also see "sectionalization").

Jeopardy: A jeopardy condition exists when the forecasted and/or actual demand for NXX resources will exceed the known supply during the planning/implementation interval for relief. NOTE: This definition only applies to ATIS-0300037, Network and Routing Resources Educational Document: Intercompany Responsibilities in the Telecommunications Industry. There may be other defined uses of jeopardy in other NGIIF documents.

Killer Trunk: A trunk that is seized repeatedly, but is not held for an appreciable length of time due to a malfunction. Within a group these trunks have higher than average attempt rates and shorter than normal holding times.

LATA: See "Local Access Transport Area".

LATA Switching System Generic Requirements (LSSGR): Comprises a series of Technical References dealing with proposed generic requirements for switching systems based on the typical needs of a Bell Operating Company (BOC).

LEC: See "Local Exchange Carrier".

Lineside: Refers to that part of a Access Service Providers switching system, associated with the connection of a line (loop assigned to a customer) to the switching system.

Links:

A-Link - Access Links connecting a switching point or a database to its home Signal Transfer Point (STP).

B-Link - Bridge Links interconnecting STP pairs of the same hierarchical level within the same network.

C-Links - Cross Links connecting mates of an STP pair in the same network

D-Links - Diagonal Links 1) connecting STP pairs between different networks or 2) connecting STP pairs of different hierarchical levels within the same network.

E-Links - Extension Links connecting a Signaling Point to an STP pair other than its home STP pair.

F-Links - Fully associated Links directly connecting two switching points to one another or a switching point to a database node.

Local Access Transport Area (LATA): Denotes a geographic area established for the provision and administration of communications service. It encompasses one or more designated exchanges, which are grouped to serve common social, economic and other purposes. For some Access Service Providers this is synonymous with the term Market Area.

Local Exchange Carriers (LECs): A local telephone company, i.e., a communications common carrier that provides ordinary local voice-grade telecommunications service under regulation within a specified service area.

Local Number Portability (LNP): Permits telephone subscribers to retain their telephone numbers should they desire to change local Service Providers or their location within their Exchange Rate Center

Local Reseller: An access customer who resells the access service obtained from a Local Exchange Carrier.

Location Routing Number (LRN): The ten-digit (NPA-NXX-XXXX) number assigned to a switch/Point of Interconnection (POI) used for routing in a permanent local number portability environment.

Loop Around Test Line: Denotes an arrangement utilizing a Access Service Provider central office to provide a means to make certain two-way transmission tests on a manual basis. This arrangement has two central office terminations; each reached by means of separate telephone numbers and does not require any specific customer location equipment. Equipment subject to this test arrangement is at the discretion of the customer.

Loss Deviation: Denotes the variation of the actual loss from the designed value.

LSSGR: See "LATA Switching System Generic Requirements".

Maintenance Window: A published period of time (generally a 3 hour period, once a week) when ASP X.75 service maybe unavailable or disrupted. This period will be utilized for purposes of maintenance routines.

Manual Scheduled Testing (MST): MST of Switched Access Services (Feature Groups B, C or D and Directory Access Service not routed through an access tandem), where the Access Service Provider provides a technician at its office(s) and at the customer's location, will consist of quarterly loss and C-message noise tests, and annual balance tests. However, the customer may, at additional charge, specify a more frequent schedule of loss/noise/balance tests, the customer may also order, at additional charge in accordance with tariff, gain-slope and C-notched noise testing.

The Access Service Provider will provide, on a quarterly basis, an MST report that lists the test results for each trunk tested. Trunk test failures requiring customer participation for trouble resolution will be provided to the customer on an as-occurs basis.

Migration of NXX Code(s): Code migration is transferring a code from one switch to another and/or from one OCN to another and/or one Service Provider to another. This situation should be a coordinated project. Testing and testing timeframes would be determined by the interconnected project partners and does not need industry testing participation. A test line number should be published in the LERG™ Routing Guide for any company choosing to participate in testing NXX migration scenarios may include, but are not limited to, the following:

- Migrating all NXX codes from a switch to another switch/same or different tandem

ATIS-0300036

- Migrating one or more but not all NXX codes from a switch to another switch (OCN of the switch may or may not stay the same)
- Type 1 to Type 2 wireless code migration (OCN of the switch changes)

When the “A” record is moving from one switch to another switch, then the test number and test response field on the NXD screen should be populated with the appropriate test number and test response.

Milliwatt (102 Type) Test Line: Denotes an arrangement in an end office which provides a 1004 Hz tone at 0 dBm0 for one-way transmission measurements towards the customer's location from the Access Service Provider end office.

Months to Exhaust (MTE): A calculation that is used by Service Providers to document the need for an additional code or block as follows:

TNs Available for Assignment divided by Average Monthly Growth Rate.

A calculation used by the Pooling Administrator to document the need for an additional Central Office Code as follows:

Blocks Available for Assignment divided by Average Monthly Growth Rate.

Multi-ASP Service: A Switched Access or Special Access Service provided by 2 or more Access Service Providers.

North American Numbering Plan (NANP): An integrated telephone numbering plan serving countries as shown under NANP Area. According to Industry Numbering Committee, NANP is a numbering architecture in which every station in the NANP Area is identified by a unique ten-digit address consisting of a three-digit NPA code, a three digit central office code of the form NXX, and a four-digit line number of the form XXXX.

North American Numbering Plan Administration (NANPA): NANPA holds overall responsibility for the neutral administration of NANP numbering resources, subject to directives from regulatory authorities in the countries that share the NANP. NANPA's responsibilities include assignment of NANP resources, and, in the U.S. and its territories, coordination of area code relief planning and collection of utilization and forecast data.

NANP Area: Consists of the United States, Canada and the Caribbean countries: Anguilla, Antigua, Bahamas, Barbados, Bermuda, British Virgin Islands, Canada, Cayman Islands, Dominica, Dominican Republic, Grenada, Jamaica, Montserrat, Sint Maarten, St. Kitts & Nevis, St. Lucia, St. Vincent & Grenadines, Turks & Caicos Islands, Trinidad & Tobago, and U.S. Caribbean territories (including American Samoa, Puerto Rico, the U.S. Virgin Islands, Guam and the Commonwealth of the Northern Mariana Islands).

NECA Tariff FCC No. 4: The National Exchange Carrier Association (NECA) serves as the agent for this Federal Communications Commission (FCC) tariff. This tariff contains Service Providers' wire center and interconnection information that supports the ordering, billing, and provisioning of interstate access services.

Network Impacting Event: A failure (hardware, software, human, or process) of a telecommunications network component that prevents call completion.

Network Management: A set of procedures, equipment, and operations designed to keep a network (e.g., the public switched network) operating near maximum efficiency when unusual loads or equipment failures would otherwise force the network into a congested, inefficient state.

Network Modification: Any type of planned equipment, software, trunk or facility activity which has the potential to significantly affect interconnected networks (e.g. rearrangement of existing network elements, switch homing rearrangements, SS7 rehomings).

Network Service Center (NSC): The NSC is responsible for assuring the overall quality of network service. The NSC monitors, analyzes, tracks, reports results and issues referrals to other centers for follow-up work on trouble patterns. The NSC will be the contact point for non-circuit specific trouble reports from the Access Service Customer.

Nonconforming End Office: Office that is not yet equipped or incapable of being equipped, for provision of originating and terminating Feature Group D Local Access Transport Area (LATA) access service.

Nonscheduled Testing (NST): NST of Switched Access Services is where:

The customer determines a need to test its services and contacts the Access Service Provider (ASP) to perform (billable) tests in one of the following manners.

- The customer provides remote office test lines and 105 test lines with associated responders or their functional equivalent ("automatic testing") or
- The ASP provides a technician at its and the customer provides a technician at its location with suitable test equipment to perform the required tests ("cooperative testing") or
- The ASP provides a technician at its office(s) and/or at the customer's location with suitable test equipment to perform the required tests ("manual testing").

Nonscheduled Tests may consist of any tests, e.g., loss, noise, slope, envelope delay, which the Access Service Customer may require.

Nonsynchronous Test Line: An arrangement in step-by-step end offices which provides operational tests which are not as complete as those provided by the synchronous test lines, but can be made more rapidly.

Numbering Plan Area (NPA): Also called area code. An NPA is the 3-digit code that occupies the A, B, and C positions in the 10-digit North American Numbering Plan (NANP) format that applies throughout the NANP Area. Traditionally, NPAs were of in the form of NX0/1X, where N represents the digits 2-9 and X represents any digit 0-9. After 1/1/95, NPAs were changed to the form of NXX. In the NANP, NPAs are classified as either geographic or non-geographic.

a) Geographic NPAs are NPAs which correspond to discrete geographic areas within the NANP Area.

b) Non-geographic NPAs are NPAs that do not correspond to discrete geographic areas, but which are instead assigned for services with attributes, functionalities, or requirements that transcend specific geographic boundaries. The common examples are NPAs in the N00 format, e.g., 800.

Numbering Plan Area (NPA) Code Relief: NPA code relief refers to an activity that must be performed when and NPA nears exhaust of its 792 NXX capacity. Options for relief are described in the NPA Code Relief Planning & Notification Guidelines.

NXX: In the LERG™ Routing Guide, this may also be referred to as a Central Office Code (COC) or as a Destination Code. NXX's are technically the three digits following the NPA (Area Code) in the numbering schema used by countries participating in the North American Numbering Plan (NANP).

Open Circuit Test Line: An arrangement in an end office which provides an ac open circuit termination of a trunk or line by means of an inductor of several Henrys.

Operating Company Number (OCN): A four character numeric or alphanumeric code that uniquely identifies providers of communications service, excluding Interexchange Carriers. NOTE: NECA-assigned Company Codes may be used as OCNs.

Other Access Service Provider (OASP): An Access Service Provider designated to coordinate the installation and maintenance of a Multi-ASP Access service.

Overlap Outpulsing: Access Service Provider outpulsing to the Access Service Customer before customer has completed dialing.

Overtime: Any Access Service Provider (ASP) installation or repair effort performed outside of a craft person's scheduled working hours. If this work is performed at the specific request of an Access Service Customer (ASC), either for the convenience of the ASC or for reasons not within the control of the ASP, this work is billable to the ASC at applicable tariff rates.

Patch: Temporary use of other facilities or functions to restore service ability to a failed network or component.

Packet Switching: A data transmission technique where user information is segmented and routed in discrete data envelopes called packets.

Personal Communication System (PCS): A company that provides an all-digital, higher frequency (1900MHz) alternative to traditional cellular, telecommunications service.

Personal Communication System (PCS) Reseller: A company that obtains numbers from another Service Provider to resell PCS services to its customers.

Personal Identification Number (PIN): An identification number given by an Access Service Customer to its customer for billing and security purposes.

Phase Jitter: The unwanted phase variations of a signal.

Plain Old Telephone Service (POTS): Term used to refer to lines connected to a local switching system that have basic service capability. Such lines are not identified within a closed user group such as centrex or connected to Customer Premises Equipment, i.e., PBX.

Plant Test Date (PTD): Describes a given point in the order completion process. It is normally one to two days prior to the due date when the Local Exchange Carrier tests their portion of the circuit.

Plesiochronous: That relationship between two signals such that their corresponding significant instants occur at nominally the same rate, any variations being constrained within a specified limit. For example, two signals having the same nominal digit rate, but not stemming from the same clock or homochronous clocks, are usually plesiochronous. Note: There is no limit to the phase difference that can accumulate between corresponding significant instants over a long period of time.

Point of Interconnection (POI): The physical location where a Service Provider's connecting circuits interconnect for the purpose of interchanging traffic on the Public Switched Telephone Network. This term is sometimes referred to as Point of Interface.

Point of Presence (POP): The physical location (a structure where the environmental, i.e., power, air conditioning, etc., specification for Access Service Provider terminating equipment can be met) at which an Interexchange Customer establishes itself for the purpose of obtaining exchange access. The POP is the physical location within which the Plain Old Telephone Service occurs. POPs must be identified for both switched access and special access.

Point of Termination: The term "Point of Termination" denotes the point of demarcation within a customer-designated location i.e., Point of Presence at which the Access Service Provider's responsibility for the provision of Access Service ends.

POTS: See "Plain Old Telephone Service".

Pooling Administrator (PA): The entity or entities responsible for administering a thousands-block number pool (FCC 00-104, §52.7 (g)).

PPSN: See "Public Packet Switched Network".

Pre-service Tests: A procedure that ascertains the proven function and quality of the service to the ASC Terminal Location (POT), prior to cooperative turn-up of the service by the Bell Operating Company (BOC) and Access Service Customer (ASC). The BOC and ASC each have responsibility for pre-service testing up to their respective side of the POT.

Public Packet Switched Network (PPSN): A Bell Operating Company Public Packet Switched Network.

Public Switched Telephone Network (PSTN): A worldwide network of public circuit switched networks based on E.164 addressing, which is the International Telecommunication Union – Telecommunications Standardization Sector (ITU-T) recommendation defining the international public telecommunications numbering plan.

Public Utility Commission (PUC) or equivalent: Is that branch of the local or state government responsible for Public Utility Provider's Rate & Regulations.

Pulse Code Modulation (PCM): Is the conversion of an analog signal, such as voice, to a digital format, ordinarily in terms of binary-coded pulses representing the quantized amplitude sample of the analog signal.

Quasi/Pseudo Random Signal Source: A test signal consisting of a bit sequence which approximates a random signal.

Rate Area: A defined geographical division of an exchange area used as the basis for establishing uniform tariffs for local traffic (including multi-message unit traffic) for classes of service available within the area. Rate Areas are customarily found in larger metropolitan areas and may also be the basis for establishing tariffs for short-haul toll traffic.

Rate Center: Rate Center is used for numbering resource applications and reports to associate telephone numbers with a geographic area, as defined by the relevant regulatory agency. A Rate Center is also a uniquely defined point (Vertical & Horizontal Coordinates) located within an exchange area from which mileage measurements are determined. These measurements can be used with the tariffs in the message rating processes.

Rate Center Major Vertical & Horizontal Coordinate: A Coordinate used to pinpoint the location of a Rate Center within an exchange area. The Vertical and Horizontal Coordinates can be used to calculate air mileage measurements between two Rate Centers that are used to determine the appropriate mileage rates in determining the charge for message telephone service calls. (Note: In some service areas subsets of the Rate Center major vertical & horizontal coordinate are defined as minor vertical and horizontal coordinates. The Minor Vertical and Horizontal Coordinates can be used to divide Rate Centers into zones for more specific distance calculations. Most often used to rate interstate messages when straight distance between the calling and called point is less than forty miles.)

Reassignment: In a pooling environment, reassignment refers to the process of reestablishing the assignment of a thousands-block, which was previously assigned to another Service Provider (SP) or to a new SP. Reassignment may also mean the transfer of a working or assigned NXX from one switching entity/Point of Interconnection (POI) to another. Reassignment may also be related, but not limited, to facility rearrangements or Trunk Circuit Identification Code (TCIC) numbering plan rearrangements.

Reclamation: The process by which Service Providers are required to return numbering resources to the North American Numbering Plan Administration (NANPA) or Pooling Administration (PA) (FCC 00-104, § 52.15 (i) (1)). Reclamation is also required throughout the remainder of the North American Numbering Plan (NANP) area by the regulatory authorities that govern the appropriate numbering administrators i.e. Canada, Caribbean, and Atlantic.

Release: On the scheduled conversion date, the "new" Access Service Customer (ASC), upon being informed by the Access Service Provider (ASP) at each end of its service that they are ready, contacts the "former" ASC and obtains a release of the existing ASC service. The conversion then takes place with the new ASC coordinating the ASPs performing the conversion work.

Reseller: A Service Provider (SP) which purchases facilities and/or services and obtains numbering resources from another SP for resale. A reseller's services could include, but are not limited to: Local, switchless, and wireless technologies.

Responsible Organization: The entity identified by the Toll Free Subscriber or the subscribers agent assumes the duty of managing the appropriate records in 800 Data Base Service Management Systems (SMS). Management and Administration shall include Data Entry, Record Change, Trouble Acceptance, Referral and or Clearance. It is recommended that any entity performing the above function comply with this and other Toll Free Number Data Base associated documents.

Restoral: To place an Access Service back into service.

Restoration Priority (RP): Describes supremacy given to some Government and National Security circuits.

Return Loss: A measure of the similarity between the two impedances at the junction of two transmission paths. The higher the return loss, the higher the similarity.

Return Supervision: Signaling which responds to an incoming request for service or change of status.

Sectionalization: The process of determining on which side of the Point of Termination a trouble locates.

Sequence: Sequential circuit scheduling when converting more than one circuit or circuit group.

Service Continuation: The negotiated continuation of service in a coordinated conversion prior to the former Access Service Customer (ASC) disconnect due date.

Service Control Point (SCP): A logical entity that provides functions common to all applications, overload controls, and maintenance.

Service Provider (SP): A telecommunications carrier or other entity that receives numbering resources from the North American Numbering Plan Administrator, a Pooling Administrator or a telecommunications carrier for the purpose of providing or establishing telecommunications service (FCC 00-104, § 52.5 (i)).

Short Circuit Test Line: An arrangement in an end office which provides for an ac short circuit termination of a trunk or line by means of a capacitor of at least four microfarads.

Signal-to-C-Notched Noise Ratio: The ratio in dB of a test signal to the corresponding C-Notched Noise.

Signaling System 7 (SS7): An international standard, general purpose CCS (Common Channel Signaling) protocol.

Singing Return Loss (High & Low): The frequency weighted measure of return loss at the edges of the voice band, where singing (instability) problems are most likely to occur.

SKIP: SKIP is a trunk group control that allows traffic to be directed to the next route before hunting for a circuit to a destination. Equipment vendors commonly provide the capability to implement this control on a percentage basis.

Softswitch: See "Call Agent".

Special Service Center (SSC): The SSC is responsible for installation and maintenance of ASP Specially Installed and Maintained Services (SIMS) circuits, i.e., those that require the use of test sets, methods, and tools not normally associated with standard message services such as Feature Groups B, C, and D. Feature Group A services will normally be controlled by the SSC.

Switch Rehome: The changing of an existing homing arrangement between a lower class office and a higher class office, e.g., Class 5 end offices and Class 4 tandem, Class 4 tandem office(s) and Class 3 tandem, etc. A homing arrangement is the final route or the last-choice trunk group between switching systems in a specific routing hierarchy. (Not all final routes between a lower class office and a higher class office constitute a homing arrangement.)

Note: The telephony terms “homing”, “homing arrangements”, “homing tandem”, “rehome”, “rehomeing”, “tandem rehome”, etc., are specific to trunking arrangements between switches as defined above. However, it has become a common practice to apply these same terms when addressing activity associated with numbering resources. For example, an NPA-NXX code is “assigned to” or “served by” a switching entity. When the code moves, migrates, or transfers to another serving switch it is frequently referred to as a code “rehome”. Although the term “rehome” when used to describe code activity is not technically correct, it is understood within the PSTN that the serving switch for the code is changing. Caution is advised when using telephony terminology in a manner other than it was originally intended, e.g., contracts, interconnection agreements, industry guidelines, industry agreements, definitions, etc.

Switch Tandem Rehome: See “Switch Rehome”.

Switch-to-Switch Testing: The ability to perform tests between adjacent switching machines to evaluate the overall integrity of an ASC provided service comprised of facilities and equipment of the ASC and the access services provided by the ASP(s).

Switched Access Service (SAS): An Access Service Provider (ASP) provided switched electrical communications path between the ASC terminal location (POT) and the ASP switching office.

Switched Digital Acceptance Testing (SDAT): Describes acceptance testing procedures used when Switched Access Services are provided with a digital switch on digital facilities.

Switching Control Center (SCC): The SCC has overall responsibility for the administration and maintenance of Service Provider central offices. This responsibility will include installation and maintenance Control Office for FG B, C and D. The SCC may be the designated reporting location for Access Service Customer circuit specific trouble reports.

Switching Entity: An electromechanical, electronic, or digital system for connecting lines to lines, lines to trunks, or trunks to trunks for the purpose of originating/terminating calls. A single switching system may handle several Central Office (CO) codes.

Synchronous Test Line (103): An arrangement in an end office which performs marginal operational tests of supervisory and ring-tripping functions.

Tandem Switch: Connects one trunk to another and serves as a trunk concentration and distribution function to minimize direct end office interconnection. A tandem switch is an intermediate switch or connection between an originating switch and the final switch call destination. A tandem switch does not allow origination or termination of telephone calls. Tandems serve a designated geographic area consisting of specific rate centers.

Technical Requirement, Reason, Limitation or Constraint: A limitation of the Point of Interconnection or Switching Entity where an existing code, a thousands-block, and/or numbers cannot be used for designated network routing and/or rating of Public Switched Telephone Network calls. Examples that constitute “technical constraint”

ATIS-0300036

include limitations on a switch, network element, or planning constraint, Customer Premises Equipment limitations or unique Advanced Intelligent Network Triggers.

Telecommunications Customer (TC): See Part VI of the NGIIF Reference Document for the definition of Telecommunications Customer (TC).

Telecommunications Provider (TP): See Part VI of the NGIIF Reference Document for the definition of Telecommunications Provider (TP).

Terminating Direction: The use of Access Service for the completion of calls from an Access Service Customer (ASC) location to an End User location.

Test Line Coordinator: The contact person who coordinates the updating and distribution of test line information for their company and is responsible for providing test line information to the industry.

Test Number: A three to ten digit number assigned for inter- and intra-network testing purposes.

Thousands-Block: A range of one thousand line numbers within an NPA-NXX beginning with X000 and ending with X999, where X is a value from 0 to 9.

Thousands-Block (NPA-NXX-X) & Central Office Code (NPA-NXX) Administration Guidelines (TBCOCAG) (ATIS-0300119): ATIS Industry Numbering Committee (INC) developed these guidelines for the administration and assignment of Central Office (CO) Codes (NPA-NXX) and Thousands-Blocks (NPA-NXX-Xs) to Local Number Portability (LNP)-capable Service Provider (SPs) within geographic numbering plan areas (NPAs).

Thousands-Block (NXX-X) Number Pooling: Thousands-block number pooling is a process by which the 10,000 numbers in a Central Office (CO) Code (NXX) are separated into ten sequential blocks of 1,000 numbers each (thousands-blocks), and allocated separately within a rate center (FCC 00-104, § 52.20 (a)).

Three-Tone Slope: Please see “3-Tone Slope” at beginning of document.

TPM™ Data Source: A set of data files issued by iconectiv®, primarily to support call rating. The TPM™ includes all assigned NPA NXX and thousands-blocks within the NANP with associated data elements that include: OCN, Rate Center, Rate Center Major Vertical and Horizontal Coordinates, Rate Center LATA , RAO, Placename, state/province/country, daylight savings indicator, time zone, and portability indicator.

Transmission Level Point (TLP): A specification in decibels, of the relative level at a particular point in a circuit as referred to a zero transmission level point (0 TLP).

Transmission Measuring (105 Type) Test Line/Responder: An arrangement in an end office which provides far-end access to a responder and permits two-way loss and noise measurements to be made on trunks from a near end office.

Transmission Specifications: The appropriate limits, e.g., acceptance and immediate action limits, of the Access Service transmission parameters.

Trigger: An intelligent network switch functionality that allows suspension of call processing in order to query an external database to obtain additional information, e.g., routing or billing information. An example of one type trigger is analysis of the dialed digits, i.e., either 3 digits, 6 digits or 10 digits.

Trunk: A communications path connecting two switching systems in a network, used in the establishment of an end-to-end connection.

Trunk Gateway: Provides an access interface between traditional Public Switched Telephone Network (PSTN) circuit-based networks and packet networks. Examples of the PSTN trunk interfaces are Integrated Services Digital Network (ISDN) User Part (ISUP), Primary Rate Interface (PRI), Multi Frequency (MF) and Digital Tone Multi Frequency (DTMF). The Trunk Gateway may also support an interface for line based Generic Requirement GR-303/TR-08 remote terminals. The Trunk Gateway may be connected to the network via various bit-rate and physical layer interfaces. A Call Agent provides the specific call control, call processing and other management functions for the trunks terminated on the Trunk Gateway.

Trunk Group: A set of trunks which are traffic engineered as a unit for the establishment of connections between switching systems in which all of the communications Paths are interchangeable.

Trunkside: Refers to that part of an Access Service Provider's or Access Service Customer's switching system, associated with the connection of a Trunk to the switching system.

Type 1 Interconnection Service Provider: A wireless Service Provider (SP) that utilizes Type 1 (trunk side with line treatment) interconnection with another SP's end office switch.

Value Added Network (VAN): An underlying facility which has been optimized and has additional features and functions added to increase its value to the End User.

Vertical and Horizontal (V&H) Coordinates: For purposes of determining airline mileage between locations, vertical and horizontal coordinates are derived from geographic latitude and longitude coordinates.

Wide-Area Telecommunications Service (WATS): A specialized form of fixed rate long-distance telecommunications service. WATS lines are commonly used by businesses and government agencies. Some individuals in small corporations also have WATS subscriptions.

WATS Access Line (Frequently referred to as WAL): Provides a connection between a customer's end user's premises and an Access Service Provider end office switch capable of performing the necessary screening functions for Toll Free Service, WATS or similar services and is provided only for use at the closed end of such services.

WATS Access Lines are arranged for either originating calling only or terminating calling only. They are provided with rotary dial or dual tone multi-frequency address signaling and either loop start or ground start supervisory signaling, at the option of the customer.

Wire Center: A building in which one or more central offices, used for the provision of Telephone Exchange Services, are located.

ATIS-0300036

Work Order Record and Details (WORD): A WORD document contains the information and specifications required to install and maintain a specific Switched Access Service circuit.

X.75 Gateway Service: A protocol for network interworking which supports communication between adjacent networks and communication thru transit networks.