NORTEL NETWORKS

Passport 6400, 7400, 15000, 20000

Alarms

241-5701-500

Passport 6400, 7400, 15000, 20000

Alarms

Publication: 241-5701-500
Document status: Standard
Document version: 5.2S2
Document date: December 2003

Copyright © 2003 Nortel Networks.
All Rights Reserved.

Printed in Canada

NORTEL NETWORKS, the globemark design, the NORTEL NETWORKS corporate logo, DPN, DPN-100, and PASSPORT are trademarks of Nortel Networks.
Advanced Peer-to-Peer Networking and APPN are trademarks of International Business Machines Corporation.
VT100 is a trademark of Digital Equipment Corporation.

Publication history

December 2003

5.2S2 Standard
General availability. Contains information on Passport 6400, Passport 7400, Passport 15000, and Passport 20000 for the PCR 5.2 GA release.

Contents

About this document **9**
Who should read this document and why 9
What you need to know 9
How this document is organized 10
Text conventions 10
Interpreting alarms in this book 11
Software and engineering alarms 11
Alarm format 12
Related documents 18
Passport references 18
ITU-T references 19
How to get more help 19

Chapter 1
Alarms **21**

Appendix
Alarm causes **919**

List of tables

Table 1 Passport IndexGroups 13
Table 2 Alarm causes 919

About this document

This document describes Passport 6400, 7400, 15000, and 20000 alarms.

The following topics are discussed in this section:

- “Who should read this document and why” (page 9)
- “What you need to know” (page 9)
- “How this document is organized” (page 10)
- “Text conventions” (page 10)
- “Interpreting alarms in this book” (page 11)
- “Related documents” (page 18)
- “How to get more help” (page 19)

Who should read this document and why

This guide is for persons who operate and maintain the Passport 6400, 7400, 15000, and 20000 nodes.

What you need to know

Familiarity with fundamental data communications concepts and terms will be helpful in understanding the information in this document.

How this document is organized

241-5701-500 *Passport 6400, 7400, 15000, 20000 Alarms* contains the following sections:

- "Alarms" (page 21) contains a sequential listing of all Passport alarms. Each alarm description provides details on the condition(s) that generated the alarm, and the remedial action to be taken.
- "Alarm causes" (page 919) contains a listing of possible values for the cause field in a Passport alarm.

Text conventions

This document uses the following text conventions:

- `nonproportional spaced plain type`

  Nonproportional spaced plain type represents system generated text or text that appears on your screen.

- **`nonproportional spaced bold type`**

  Nonproportional spaced bold type represents words that you should type or that you should select on the screen.

- *italics*

  Statements that appear in italics in a procedure explain the results of a particular step and appear immediately following the step.

  Words that appear in italics in text are for naming.

- `[optional_parameter]`

  Words in square brackets represent optional parameters. The command can be entered with or without the words in the square brackets.

- `<general_term>`

  Words in angle brackets represent variables which are to be replaced with specific values.

- UPPERCASE,lowercase

  Passport commands are not case-sensitive and do not have to match commands and parameters exactly as shown in this document, with the exception of string options values (for example, file and directory names) and string attribute values.

- |

  This symbol separates items from which you may select one; for example, ON|OFF indicates that you may specify ON or OFF. If you do not make a choice, a default ON is assumed.

- ...

  Three dots in a command indicate that the parameter may be repeated more than once in succession.

The term absolute pathname refers to the full specification of a path starting from the root directory. Absolute pathnames always begin with the slash (/) symbol. A relative pathname takes the current directory as its starting point, and starts with any alphanumeric character (other than /).

Interpreting alarms in this book

After reading this section you will be able to read and interpret the alarms documented in this guide.

Software and engineering alarms

Passport “reuses” certain alarm indexes to indicate software or engineering fault or error conditions. In these cases the system indicates the condition by a common alarm code. All common alarm codes have initial digits of “0000”.

Internal software alarms

For internal software errors, the common alarms are 0000 9000, 0000 9002, and 0000 9003. The specifics of the alarm vary depending on the component. Internal details appear on the text interface as part of the alarm. The remedial action is always to open a service request (SR).

Engineering alarms

For engineering alarms there are two common alarms. For threshold/heap memory availability, the alarm is 0000 3001. For threshold message block availability, the alarm is 0000 3002. Details appear on the text interface as part of the alarm.

The specifics of the alarm vary depending on the component.

Alarm format

Alarm information in this document is divided into seven fields as shown in the following example:

xxxx xxxx

Component	Severity	Status
The full component name or a statement indicating that it is a common alarm which applies to all components.	One of: critical, major, minor, warning, indeterminate or cleared	One of: message, set, clear or set/clear:

Legend

Describes the possible values for anything in brackets in the component field.

Details

Provides details on the cause of the alarm, and where applicable, the impacts the alarm will have on the system or on other components.

Remedial action

Gives the suggested operator action for correcting the failure (if possible).

Alarm number

Each alarm heading consists of an eight-digit number identifying the alarm.

The alarm number is the principal alarm identifier and provides the means by which you can find your alarm quickly. Alarms appear sequentially in this book for easy access.

The alarm is made up of an Index Group (the first group of four digits) and a SubIndex (the second group of four digits). This is also referred to as the *NTP Index*.

- The IndexGroup is a four-digit number representing logical groupings of alarms. For example, it may represent:
  - — an application service
  - — an internal subsystem
  - — a component type
  - — a component class
  - — a software module
  - — a similarity of event

  For a complete list of all alarm IndexGroups, refer to table “Passport IndexGroups” (page 13).
- The SubIndex is a four-digit number which has significance only within the IndexGroup.

IndexGroups

The following table provides a complete list of all Passport IndexGroups.

Table 1
Passport IndexGroups

IndexGroup	Group
0000	Common alarms
0999	Preside Multiservice Data Manager-generated alarms For information on Preside Multiservice Data Manager-generated alarms, see 241-6001-501 *Preside MDM Proxy Alarms Reference Guide*.
1100	Router IP information
7000	Component administration system
7001	Virtual circuit
7002	Bus control system
7003	Data collection system
7004	Module interconnection link

(Sheet 1 of 4)

Table 1 (continued)
Passport IndexGroups

IndexGroup	Group
7005	Module interconnection transport
7006	Network management interface system
7007	Frame relay service
7008	File system
7009	Routing
7011	Port management system
7012	Processor control system
7013	Traffic management
7014	Memory management
7015	Network time synchronization
7016	Destination call routing
7017	Network clock synchronization
7018	Path Oriented Routing Service
7019	Voice Transparent Data Service, including Bit Transparent Data Service and HDLC Transparent Data Service
7020	Virtual router
7021	Internet protocol (IP)
7022	Bridge
7023	Novell internetwork packet exchange (IPX)
7026	LAN port management system
7031	Point-to-point protocol
7032	Frame Relay DTE
7035	Statistics Management System
7036	APPN Protocol Code
7037	SNA Common Tools
(Sheet 2 of 4)	

Table 1 (continued)
Passport IndexGroups

IndexGroup	Group
7038	LLC2 Protocol Code
7039	ATM
7040	Source route end station
7041	ATM Networking
7042	ATM AAL1
7043	Trace
7044	SNA
7046	SNA GvcIf
7047	SNA
7048	Frame Relay ISDN
7049	Voice Networking
7050	Remote Service Agent (Rsa)
7052	LAN Emulation Client (Lec)
7053	Multiservice Cut Through Switching (Mcs)
7054	Sparing Management
7056	Voice Server Processor (VSP)/Narrowband Service Trunk over ATM (Nsta)
7057	Digital Circuit Multiplication Equipment voice service
7058	Hunt Group (Hg)
7059	Virtual Router IP information
7060	Logical Processor Engineering
7061	Internet Protocol Security (IPSec)
7062	WirelessPCU project
7063	DPRS (Routing Protocol Tracing Tool)
7064	MPLS
(Sheet 3 of 4)	

Table 1 (continued)
Passport IndexGroups

IndexGroup	Group
7065	Signaling Gateway Radio Network Control Interface *
7066	Signaling ATM adaptation layer Network-to-Network interface *
7067	Virtual Media Gateway Interface *
7068	Serving GPRS support node *
7069	Wireless BCN services
7070	Adjunct Processor (AP)
7071	LAN Application
7072	Ethernet service
* Descriptions of these alarms are available in UMTS/GPRS documentation.	
(Sheet 4 of 4)	

Component field

The component field contains the name of the component needing repair or detecting the fault.

The component field always contains the abbreviated form of the component name. To find out component abbreviations, refer to 241-5701-060 *Passport 7400, 15000, 20000 Components*.

Common component fields

In cases where the alarm is common to all or most components the field contains <component_name> or <component_type>.

Severity field

Severity is always one of: indeterminate, critical, major, minor, warning, or cleared. These values and their definitions correspond to those defined by OSI in ITU-T X.733.

> ***Note:*** For Passport common alarms (alarms with an IndexGroup 0000), the severity is dependent on the component. To reflect this, the severity field says <severity> to indicate that the value may change with different components.

Following are explanations of the different types of severity:

- indeterminate—the system cannot determine the level of severity.
- critical—requires you to react immediately to the failure. Usually it implies that the resource is completely disabled and that service is affected.
- major—requires that you take immediate corrective measures. The resource is severely disabled and service is affected.
- minor—corrective action should be taken to prevent a more serious fault. The resource is partially disabled but service is not affected.
- warning—action should be taken to diagnose and correct a problem. Some problem has been detected but the resource is not disabled and service is not affected.
- cleared—all previous alarms on this component are cleared. Alarms that have a status of clear always have a severity of cleared.

Status field

Status is always one of message, set, clear or set/clear. In situations where the same alarm generates both a set and clear, this document represents it with set/clear.

Following are explanations of the different types of status:

- message—a message alarm indicates a condition in which you may be interested. All software alarms have the status of message.
- set—indicates that a fault or failure has occurred and that an operator action may be required to correct the problem.
- clear—when the fault is repaired, a clear alarm is generated to indicate that the condition has returned to normal. Alarms that have a status of clear always have a severity of cleared.
- set/clear—sometimes an alarm must be both set and cleared. In this situation, the alarm is issued twice, once to set the alarm and once to clear the alarm. The alarm appears with the same alarm index number in both cases. This occurrence is indicated in this document by set/clear in the status field.

Details field

The details field contains the following information:

- what has caused the alarm
- how the alarm impacts the network, service, and other components

Note: Alarm descriptions that include mention of the control processor (CP) are generally applicable to a control and function processor (CFP1).

Remedial action field

The action field contains information telling the operator what actions to take to correct the problem. The remedial action might include one of the following:

- issuing an operator command
- replacing hardware
- waiting until the alarm clears itself (no action is required)
- opening an service request (SR)

Related documents

The following sections list documents related to the information in this guide:

- “Passport references” (page 18)
- “ITU-T references” (page 19)

Passport references

Refer to the following Passport NTPs in conjunction with the material in this book:

- 241-5701-005 *Passport 7400, 15000, 20000 List of Terms*
- 241-5701-030 *Passport 7400, 15000, 20000 Overview*
- 241-7401-240 *Passport 7400 Hardware Installation, Maintenance and Upgrade*
- 241-1501-210 *Passport 15000, 20000 Hardware Installation Guide*
- 241-1501-215 *Passport 15000, 20000 Hardware Maintenance Guide*
- 241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing*

- 241-5701-600 *Passport 7400, 15000, 20000 Configuration Guide*
- 241-5701-060 *Passport 7400, 15000, 20000 Components*

ITU-T references

The following ITU-T references provide information related to the material in this book:

- ITU-T Recommendation X.731, Information technology - Open Systems Interconnection - Systems Management - Part 2: State management function
- ITU-T Recommendation X.733, Information technology - Open Systems Interconnection - Systems Management - Part 4: Alarm reporting function

How to get more help

For information on training, problem reporting, and technical support, see the "Nortel Networks support services" section in the product overview document.

Chapter 1
Alarms

This section lists and describes all possible alarms for Passport 6400, 7400, 15000, and 20000. For details on how to interpret alarm information, see “Interpreting alarms in this book” (page 11).

> ***Note:*** Bus technology refers to Passport 7400 and Passport 6400 and Fabric refers to Passport 15000 and 20000.

0000 0000

Component	Severity	Status
<component_name>	clear	clear

Legend

<component_name> = any Passport component

Details

A hierarchical clear has been issued.

This alarm clears all *set* alarms for components hierarchically below this component. There is a special case when <component_name> is a logical processor (LP) component. In addition to the components hierarchically below the LP, this alarm clears all *set* alarms for components that have specified the LP as a related component in that *set* alarm.

Probable Cause

Processor problem, Underlying resource unavailable, Operational condition, Procedural error

Type

Equipment, Processing, Operator

Remedial action

None.

0000 1000

Component	Severity	Status
<component_name>	<severity>	set/clear

Legend

<component_name> = any Passport component that supports the *lock* and *unlock* commands

<severity> = varies with component

Details

When the status is *set*, the component has gone into a locked state or a shutting down state.

The locked component is no longer permitted to provide service. As a result, dependent components may be operationally disabled as well.

When the status is *clear* the component is unlocked.

The OSI administrative state attribute in the alarm specifies the new administrative state for the component.

Probable Cause

Denial of service, Loss of signal, Operational condition

Type

Operator, Communication

Remedial action

When the status is *set*, issue the *unlock* command to attempt to unlock the component.

When the status is *clear*, no remedial action is required.

0000 1001

Component	Severity	Status
<component_name>	<severity>	set/clear

Legend

<component_name> = any Passport component that maintains OSI operational state

<severity> = varies with the component

Details

The component has changed OSI operational state.

When the status is *set*, the operational state has changed to disabled.

When the status is *clear*, the operational state has changed to enabled.

Probable Cause

Processor problem

Type

Equipment

Remedial action

When the status is *set*, the remedial action is dependent on the component. For information on individual components, refer to 241-5701-060 *Passport 7400, 15000, 20000 Components*. For information on resolving problems, refer to 241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing*. When the status is *clear*, no remedial action is required.

0000 3000

Component	Severity	Status
<component_name>	<severity>	set/clear

Legend

<component_name> = any Passport component

<severity> = varies with component

Details

When the status is *set*, the component has exceeded a threshold for heap or message blocks.

When the status is *clear*, the component has dropped below a threshold for heap or message blocks.

The impact on other components can vary.

Probable Cause

Timing problem, Configuration error, Protocol error, Out of memory

Type

Processing, Communication

Remedial action

When the component name is logical processor (LP), contact Nortel Networks global support.

If the component name is not LP then the remedial action is dependent upon the component. For information on individual components, refer to 241-5701-060 *Passport 7400, 15000, 20000 Components*. For information on resolving problems, refer to the 241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing*

0000 3001

Component	Severity	Status
<component_name>	<severity>	set/clear

Legend

<component_name> = any Passport component

<severity> = varies with component

Details

When the status is *set*, the component has exceeded a threshold for heap/memory availability.

When the status is *clear*, the component has dropped below a threshold for heap/memory availability.

The impact on other components can vary.

Probable Cause

Out of memory

Type

Processing

Remedial action

When the component name is logical processor (LP), contact Nortel Networks global support.

If the component name is not LP then the remedial action is dependent upon the component. Refer to the 241-5701-060 *Passport 7400, 15000, 20000 Components*, for more information on individual components.

0000 3002

Component	Severity	Status
<component_name>	<severity>	set/clear

Legend

<component_name> = any Passport component

<severity> = varies with component

Details

When the status is *set*, the component has exceeded a threshold for message block availability.

When the status is *clear*, the component has dropped below a threshold for message block availability.

The impact on other components can vary.

Probable Cause

Underlying resource unavailable

Type

Processing

Remedial action

When the component name is logical processor (LP), contact Nortel Networks global support.

If the component name is not LP then the remedial action is dependent upon the component. Refer to the 241-5701-060 *Passport 7400, 15000, 20000 Components*, for more information on individual components.

0000 9000

Component	Severity	Status
<component_name>	indeterminate	message

Legend

<component_name> = any Passport component

Details

An internal software error has been detected by a component. This alarm index is re-used by many subsystems upon detection of various types and severities of internal errors. Thus, one instance of an alarm with this index may be totally unrelated to another instance. In some cases, it is possible that the alarm comment text can give a hint about what has happened.

Because the circumstances which caused this event are unexpected, the impact can vary on a case-by-case basis from no impact at all to possibly a severe impact. In the latter case, it may be accompanied by other alarms.

The problem may or may not be reproducible. If the circumstances are known, this can greatly help the resolution of the problem.

Probable Cause

Software error

Type

Processing, Communications

Remedial action

Contact your local Nortel Networks technical support group.

0000 9001

Component	Severity	Status
<component_type>	indeterminate	message

Legend
<component_type> = any Passport component

Details
An internal software error (indicating a bad state) has been detected by a component.

The impact on other components can vary.

Probable Cause
Software error

Type
Communications

Remedial action
Contact your local Nortel Networks technical support group.

0000 9002

Component	Severity	Status
<component_type>	indeterminate	message

Legend
<component_type> = any Passport component

Details
An internal software error (indicating a bad function number) has been detected by a component.

The impact on other components can vary.

Probable Cause

Type

Remedial action
Contact your local Nortel Networks technical support group.

0000 9003

Component	Severity	Status
<component_type>	indeterminate	message

Legend
<component_type> = any Passport component

Details
An internal software error (indicating a bad message code) has been detected by a component.

The impact on other components can vary.

Probable Cause
Software error

Type
Communications

Remedial action
Contact your local Nortel Networks technical support group.

7000 0001

Component	Severity	Status
Prov	critical	message

Details

Initial loading of the boot file failed because it is missing.

Initial loading and initial activation have been aborted. The control processor (CP) will still come up and allow operator login, however it has incomplete configuration data and configured software/services have not been started.

The /system/commit file contains the name of the boot file. This boot file must be present in the /provisioning directory. If all files are present, then either the individual files or the complete file system is corrupt.

Probable Cause

File error, Corrupt Data

Type

Processing

Remedial action

Run disk diagnostic tests in order to provide additional problem information.

On a dual-CP system, if a spare CP is present, replace the defective CP, raise a SR and return the defective CP to Nortel Networks.

If the alarm is issued on a single-CP system, contact your local Nortel Networks technical support group.

7000 0002

Component	Severity	Status
Prov	minor	message

Details

A command from the boot file failed during initial loading.

Initial loading and initial activation are not aborted, they continue to completion.

Probable Cause

Corrupt data

Type

Processing

Remedial action

After initial loading and initial activation completes, enter provisioning mode and run semantic checks on the target component of the failed command. Make required changes, activate, and commit changes.

7000 0003

Component	Severity	Status
Prov	critical	message

Details

Initial loading of the boot file failed because it is corrupt.

Initial loading and initial activation have been aborted. The control processor (CP) will still come up and allow operator login, however it has incomplete configuration data and configured software/services have not been started.

The /system/commit file contains the name of the boot file. This boot file must be present in the /provisioning directory. If however all files are present, then it is likely that the individual files or the complete file system are corrupt.

Probable Cause

File error

Type

Processing

Remedial action

Run disk diagnostic tests in order to provide additional problem information.

On a dual-CP system, if a spare CP is present, replace the defective CP, raise an SR and return the defective one to Nortel Networks.

If the alarm is issued on a single-CP system, contact your local Nortel Networks technical support group.

7000 0004

Component	Severity	Status
Prov	critical	message

Details

A file system error has occurred while loading a provisioning file during initial loading.

If this occurs during initial booting, then initial loading and initial activation are aborted. The control processor (CP) will still come up and allow operator login, however it has incomplete configuration data and configured software/services have not been started.

Probable Cause

File error

Type

Processing

Remedial action

Run disk diagnostic tests in order to provide additional problem information.

On a dual-CP system, if a spare CP is present, replace the defective CP, raise an SR and return the defective one to Nortel Networks.

If the alarm is issued on a single-CP system, contact your local Nortel Networks technical support group.

7000 0005

Component	Severity	Status
Prov	warning	message

Details

A file system error occurred when attempting to close the provisioning after loading.

This will not affect operation, unless it is occurring repeatedly, each time a load or save command is performed.

Probable Cause

File error

Type

Processing

Remedial action

Contact your local Nortel Networks technical support group.

7000 0006

Component	Severity	Status
Prov	critical	message

Details

The control processor (CP) is crashing because there is an internal software corruption.

Usually there are related alarms (possibly software alarms) prior to this alarm being generated, which may indicate how the data was corrupted.

Probable Cause

File error

Type

Processing

Remedial action

Contact your local Nortel Networks technical support group.

If the CP repeatedly crashes due to this problem, replace the CP and return the defective CP to Nortel Networks for post-mortem.

7000 0007

Component	Severity	Status
Prov	<severity>	set/clear

Legend

<severity> = warning, minor, major, critical, or cleared.

Details

When the status is *set* and severity is *warning*, *ProvisioningSystem* (Prov) has just completed an activation of provisioning changes, and the confirmation timer has been set to 20 minutes.

This alarm is issued every 5 minutes with increasing severity (minor, major and critical) to remind you to enter the *confirm prov* command.

When the status is *clear*, either the *confirm prov* has been entered or *ProvisioningSystem* has just completed activating the provisioning view.

Note: it is possible to *confirm prov* before the alarm would have been *set*, in which case the *set* would not occur and the *clear* would simply indicate that activation has finished

Probable Cause

Operational condition

Type

Operator

Remedial action

When the status is *set*, enter *confirm prov* within 20 minutes of receiving the set alarm, to ensure rollback will not occur (validates connectivity).

7000 0008

Component	Severity	Status
Prov	major	message

Details

This alarm is issued when initial activation detects that the software has been patched. A “migration” style of loading takes place that is much slower than usual and as a result, the service outage times are much greater.

Probable Cause

File error

Type

Processing

Remedial action

Simply re-check, re-save and re-commit the current view as required.

7000 0009

Component	Severity	Status
Prov	major	message

Details

This alarm is issued when initial activation detects that the provisioning data is missing the commit format. The resulting activation is much slower than usual and as a result, the service outage times are much greater.

This scenario typically occurs when migrating to a new software version.

Probable Cause

File error

Type

Processing

Remedial action

Re-check, re-save and re-commit the current view as required.

7000 0010

Component	Severity	Status
<name>	minor/cleared	set/clear

Legend

<name> = any provisionable Passport component

Details

This alarm is issued when the reporting component cannot be updated with new provisioning data. This implies that the service provided by the reporting component will either not be created or not be modified to behave with the characteristics described in the new provisioning data.

Probable Cause

Underlying resource unavailable, Software program error, Software Program termination, Configuration Error

Type

Processing

Remedial action

Check the provisioning of the software for the specified component.

The *logicalProcessorType* attribute of the *Lp* component named in the alarm should be provisioned to the proper *Lpt* component. This *Lpt* component should have any necessary features provisioned in the *featureList* attribute.

Correct any provisioning errors and attempt re-activation.

Otherwise, contact your local Nortel Networks technical support group.

7000 0011

Component	Severity	Status
<name>	warning	message

Legend

<name> = any provisionable Passport component

Details

This alarm is issued when an application is slow in responding to provisioning data. It should not be considered failed, until alarm 7000 0010 is issued.

Probable Cause

Debugging

Type

Debug

Remedial action

No action is required, this is only a warning.

7000 0012

Component	Severity	Status
Prov	warning	message

Details

This alarm is issued when a network management interface (NMIF) session is forced off from the provisioning mode by the system administrator.

Probable Cause

Operational condition

Type

Operator

Remedial action

Contact your Nortel Networks technical support group.

7000 0013

Component	Severity	Status
Prov	minor	message

Details

This alarm is issued during initial loading when a provisioned component contains a semantically incorrect hardware link. The data of the alarm will contain the component in error. This component will not be created on the proper logical processor.

Probable Cause

Corrupt data

Type

Processing

Remedial action

After initial loading and initial activation completes, enter provisioning data and run semantic checks on the specified component. Make the required changes, activate, and commit the changes.

7000 0015

Component	Severity	Status
Prov	warning	message

Details

This alarm is issued during initial loading when a temporary file created to save the current view data cannot be removed from the disk.

Probable Cause

File error

Type

Processing

Remedial action

Contact your local Nortel Networks technical support group.

7000 0016

Component	Severity	Status
Prov	minor	message

Details

This alarm is issued when a logical processor first becomes active and the fast, boot-mode style of activation fails. The system will reset the logical processor, and use an alternative activation style.

Probable Cause

Type

Remedial action

Contact your local Nortel Networks technical support group.

7000 0029

Component	Severity	Status
Prov	minor	message

Details

This alarm is issued when an error is encountered while determining the *ProvisioningSystem* component's *nextFileSequenceNumber* attribute.

When this alarm is issued, the *nextFileSequenceNumber* attribute is set to 1.

Probable Cause

Type

Remedial action

Run disk diagnostic tests in order to provide additional problem information.

Contact your local Nortel Networks technical support group.

7000 0030

Component	Severity	Status
Prov	minor	message

Details

This alarm is issued when a disk open error is encountered while determining the *ProvisioningSystem* component's *nextFileSequenceNumber* attribute. When this alarm is issued, the *nextFileSequenceNumber* is set to 1.

Probable Cause

Type

Remedial action

Run disk diagnostic tests in order to provide additional problem information.

Contact your local Nortel Networks technical support group.

7000 0031

Component	Severity	Status
Prov	warning	message

Details

The provisioning *view* file has been corrupted or contains inconsistent data. This could be due to a file system error or manual modification of the data.

The component information will be built as part of the slow boot sequence.

Probable Cause

File error

Type

Processing

Remedial action

After the next *check prov*, do a *save prov* to generate a new provisioning file.

If the problem persists, contact your Nortel Networks technical support group.

7000 0032

Component	Severity	Status
Prov	warning	message

Details

This alarm is issued on an initial activation when the fast, boot-mode style of activation cannot be used due to a problem saving commit-format files. Activation will proceed, but with a slower style of activation.

Probable Cause

Type

Remedial action

Check for alarms indicating a problem with saving of commit-format files or with the disk.

If the problem persists, contact your Nortel Networks technical support group.

7000 0033

Component	Severity	Status
Prov Migration	warning/critical/cleared	set/clear

Details

If the status is set and the severity is critical, a software migration activation has paused. A software migration activation pauses before Migration-Switchover if any of the following occurs:

- a software alarm is issued on the migration shelf
- an engineering alarm is issued on the migration shelf
- an application cannot achieve its expected Migration-Switchover behavior

A clear is issued after the operator enters the appropriate commands to either continue with the software migration activation or to stop the software migration activation.

If the status is set and the severity is warning, a software migration activation has started. A clear is issued after the software migration activation completes either successfully or unsuccessfully.

Probable Cause

Operational condition

Type

Operator

Remedial action

If the status is set and the severity is warning then no remedial action is required. Be aware that a software migration activation has begun on this switch.

If the status is set and the severity is critical, review the set of Migration Visible Alarms raised during the software migration activation and consult the new software release documentation and/or Nortel Networks technical support to make a decision whether to continue with the software migration activation or to perform a hitless recovery. To continue with the software migration activation use the continue provisioningSystem command from within provisioning mode. To stop the software migration activation through a hitless recovery use the stop provisioningSystem command from within provisioning mode.

7000 0034

Component	Severity	Status
Prov	warning	message

Details

This alarm is issued when a fault condition occurs on the migration shelf. Text from the original alarm generated for the fault condition on the migration shelf is embedded within this alarm. Typically, the fault conditions represent:

- a software alarm
- an engineering alarm
- a condition which indicates that an application can not achieve its expected Migration-Switchover behavior.

Probable Cause

Debugging

Type

Debug

Remedial action

Refer to the alarm index within this alarm text in the new software release documentation for more information. If deemed appropriate, the software migration activation can be stopped by issuing the stop provisioningSystem command while in provisioning mode.

7000 0035

Component	Severity	Status
<name>	indeterminate	message

Legend

<name> = any provisionable Passport component.

Details

This alarm is raised against any component that fails to indicate whether it is ready for a Migration-Switchover. This alarm will pause a hitless software migration.

This message alarm is ONLY generated on the migration shelf; it is reformatted and regenerated against the Prov Migration component.

Probable Cause

Unknown

Type

Unknown

Remedial action

The component <name> may not be ready for a migration-switchover. If deemed appropriate, the software migration activation can be stopped by issuing the stop provisioningSystem command while in provisioning mode.

7000 0036

Component	Severity	Status
Prov	major/minor/warning/cleared	set/clear

Details

This alarm is raised when attribute *Prov currentJournal* reaches 75%, 85%, and 95% of its maximum at warning, minor, and major severity, respectively. If this attribute becomes greater than or equal to attribute *Prov maxNumberJournalFiles*, then journal log saving is disabled.

A *clear* is issued when the view is committed. This alarm is also cleared if journal log saving is disabled via provisioning, or if the switch resets to the committed view.

Probable Cause

Threshold crossed

Type

Quality of service

Remedial action

There is no immediate impact to the switch. The network operator should recommit, which cleans up all existing journal log files.

If neither the disaster recovery nor CP equipment protection feature are wanted, the operator can also clear this alarm by disabling journal log saving by setting attribute *Prov maxNumberJournalFiles* to none.

7000 0037

Component	Severity	Status
Prov	critical/cleared	set/clear

Details

This alarm indicates that the saving of journal logs is disabled. This can be caused by the following reasons:

- journaling has been enabled by provisioning and an initial commit is required
- journal log save failed because the File System is locked
- journal log save failed due to File System error
- the number of journal logs has exceeded the maximum
- a reload activation has occurred and a commit has not yet been done

If cpEquipmentProtection is hot, this alarm indicates that the standby CP has lost synchronization to the active CP. One or more FPs and possibly the standby CP will be reset by the system if a CP switchover occurs.

This alarm also indicates an impact to the disaster recovery feature, since these journal log files are required to restore the Passport configuration in the case of a complete switch reset or failure.

A *clear* is issued when the new view is committed. This alarm is also cleared if journal log saving is disabled by provisioning or if the switch resets to the committed view.

Probable Cause

File error, operational condition

Type

Quality of service

Remedial action

The attribute *Prov journalDisabledReason* can be queried. If this attribute has the value of fileSystemError, the operator should ensure the file system is not locked. If it is locked, the file system should be unlocked.

Otherwise, the operator should look for file system or disk alarms to determine the root cause of the failure. Once the root cause is determined and fixed, the operator should recommit to clear this alarm.

For any other value of *journalDisabledReason*, the operator should recommit the

current provisioning view and this will clear the alarm.

If neither the disaster recovery nor CP equipment feature are wanted, the operator can also clear this alarm by disabling journal log saving by setting attribute *Prov maxNumberJournalFiles* to none.

7000 0038

Component	Severity	Status
Prov	warning/cleared	set/clear

Details

If the status is *set*, a switch reset has occurred and the user can issue the restore provisioningSystem command to restore the previously journaled current view.

A *clear* is issued when the restore prov command is issued, the current view is recommitted, or the activate prov command is issued.

Probable Cause

Unknown

Type

Quality of service

Remedial action

If you want to restore the previously journaled current view, issue the restore prov command.

This alarm merely indicates the current view can be restored. There is no impact if this alarm is outstanding.

The first commit or activation following the switch reset also clears this alarm.

7000 0039

Component	Severity	Status
Prov	warning	message

Details

This alarm indicates that a commit command has just successfully completed. This alarm is only issued if the journaling is enabled.

Probable Cause

Operational condition

Type

Operator

Remedial action

None

7000 0040

Component	Severity	Status
Prov	major/cleared	set/clear

Details

If the status is *set*, a journal log file loading error has occurred and the standby CP is no longer synchronized with the active CP. This can occur in the following situations:

- File System is locked
- File System error
- log file is corrupted

A *clear* is issued when a commit prov is issued or when the journal log file that failed to load is successfully loaded on a subsequent attempt. This alarm is also cleared if the *Shelf cpEquipmentProtection* attribute is set to cold.

Probable Cause

Processing

Type

Corrupt data

Remedial action

The operator should ensure that the file system is not locked. If it is locked, the file system should be unlocked. Otherwise, the operator should look for file system or disk alarms to determine the root cause of the failure. Once the root cause is determined and fixed, the operator should perform a commit prov to clear the alarm and restore standby CP synchronization.

If CP equipment protection is not needed, the operator can clear this alarm by setting the *Shelf cpEquipmentProtection* attribute to cold.

7001 2000

Component	Severity	Status
<component_name>	minor	message

Legend

<component_name> = component of system which is using the Virtual Circuit (VC).

Details

The system was unable to establish the indicated permanent virtual circuit (PVC) due to incompatible options.

The comment string associated with the alarm indicates what was detected to be incompatible. Errors are due to options that do not match at either end or a PVC master calling another master or slave calling a slave.

Probable Cause

Type

Remedial action

Correct the options in the application so that the call may be established.

7001 2001

Component	Severity	Status
<component_name>	warning	message

Legend

<component_name> = component of system which is using the Virtual Circuit (VC).

Details

The Virtual Circuit system has detected a protocol violation and has cleared the associated call as a corrective action. The application is signalled with appropriate clear causes.

Expert data contains the state of the Virtual Circuit, the internal message code, the ITU-T protocol violation number and, optionally, 32 bytes of the data packet which caused the protocol violation.

Comment text describes the cause of the protocol violation detected.

Probable Cause

Type

Remedial action

No action is required since the call is cleared.

7001 2002

Component	Severity	Status
<component_name>	major	message

Legend

<component_name> = component of system which is using the Virtual Circuit (VC).

Details

A VC could not be established due to resource limitations.

Probable Cause

Type

Remedial action

If the alarm is isolated, then no action is required.

If this alarm appears with some frequency, then the engineering of this switch needs to be re-examined because call requests are being dropped. It may be necessary to disable the application to prevent repeated attempts to establish a call.

7001 2003

Component	Severity	Status
<component_name>	warning	message

Legend

<component_name> = component of system which is using the Virtual Circuit (VC).

Details

A data path error has been detected by the VC. The comment text associated with this alarm indicates the exact cause of the problem. Some typical examples include frame or credit congestion, VC windows running to their upper limits, or various interrupt frame errors. Internal data associated with this alarm will allow detection of the exact error.

Probable Cause

Type

Remedial action

No action is required if the alarm is isolated. Repeated alarms indicate a need to re-examine the engineering of the switch. It may be necessary to disable some applications to reduce traffic on this processor.

7001 5006

Component	Severity	Status
Lp/<num1> <type>/0	major/cleared	set/clear

Legend

<num1> = 1 - 15

<type> = 1pE1V and 1pDS1V

Details

If the status is set, the voice application was unable to make a connection to the far end.

A clear is issued when the busy out condition is cleared by the link.

Probable Cause

Type

Remedial action

Check the cabling between the far end port and the PBX. Look at the Logical Connection (LCo) subcomponent of the voice application(s) on this LP for clues as to why the connection is not up. Verify that the Permanent Logical Connection (PLC) attributes are correct and compatible with the far end. Ensure that sufficient bandwidth is available in the network for the connection to establish.

7002 0000

Component	Severity	Status
Shelf Bus/<instance>	warning/cleared	set/clear

Legend

<instance> = X or Y

Details

If the status is *set*, the main source of clock signals for the bus is defective. The reason is that one or more bus taps on the bus are unable to receive clock signals from the active control processor (CP).

If the status is *clear*, the alarm indicates that the main source of clock signals for the bus is no longer defective.

Probable Cause

Processor problem

Type

Equipment

Remedial action

Follow the standard procedure for testing the bus and remove or replace the defective unit(s). Refer to 241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing* for details on testing the bus.

7002 0001

Component	Severity	Status
Shelf Bus/<instance>	warning/cleared	set/clear

Legend

<instance> = X or Y

Details

If the status is *set*, the standby source of clock signals for the bus is defective. The reason is that one or more bus taps on the bus are unable to receive clock signals from the card at the opposite end of the module from the active control processor (CP).

If the status is *clear*, the standby source of clock signals for the bus is no longer defective.

Probable Cause

Processor problem

Type

Equipment

Remedial action

Ensure that the card at the opposite end of the module from the active CP is present and operational. If the alarm persists follow the standard procedure for testing the bus and remove or replace the defective unit(s). Refer to 241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing* for details on testing the bus.

7002 0002

Component	Severity	Status
Shelf FabricCard/<instance>	major/cleared	set/clear

Legend

<instance> = X or Y

Details

This alarm is issued on fabric-based shelves when the fabric card's secondary control bus (SCB) is no longer able to provide service. This can occur either because the SCB is not receiving a clock signal or because at least one operational card cannot access the SCB.The control processor (CP) gets its alarms from the fabrics over the bus.

When the status is *clear*, the fabric card's SCB is no longer defective.

Probable Cause

Equipment malfunction, corrupt data

Type

Equipment, processing

Remedial action

When the status is *set*, examine the operational attributes related to the secondary control bus of the *FabricCard* component to determine the cause of the alarm. If the attributes do not satisfactorily explain the cause of the alarm, see 241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing* for information on troubleshooting control processor (CP) cards and the fabric card.

7002 0003

Component	Severity	Status
Shelf FabricCard/<instance>	warning	set/clear

Legend

<instance> = X or Y

Details

This alarm is issued on fabric-based shelves when the FabricCard component's temperature has increased above the accepted operating temperature of 65 degrees Celsius (149 Fahrenheit). If the temperature continues to rise, the FabricCard component will be removed from service by the system to avoid damage.

When the status is *clear*, the FabricCard's temperature has returned to a normal operating temperature.

Probable Cause

Temperature unacceptable

Type

Equipment

Remedial action

When the status is *set*, ensure that the cooling unit is powered and properly inserted. Ensure that the ambient temperature in the room is not interfering with the system's ability to cool itself. If the problem persists, follow the standard procedure in NTP 241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing* to test the fabric card, and replace the defective cooling unit part or the fabric.

7002 0005

Component	Severity	Status
Shelf FabricCard/<instance>	major	set/clear

Legend

<instance> = X or Y

Details

This alarm is issued on fabric-based shelves when two fabric cards are running different versions of firmware. Although this condition does not cause operational problems, Nortel Networks recommends that you always run the same version of firmware on each fabric card, except during initial testing purposes.

When the status is *clear*, both fabric cards are running the same version of firmware, or the other fabric card has been removed.

Probable Cause

File error

Type

Processing

Remedial action

When the status is *set*, install the software version indicated by the *recommendedVersionToInstall* attribute of the *FabricCard* component.

7002 0006

Component	Severity	Status
Shelf FabricCard/<instance>	major	set/clear

Legend

<instance> = X or Y

Details

This alarm is issued on fabric-based shelves when the install command is interrupted by a CP switchover or other disruptive event, causing fabric card loading to be aborted.

When the status is *clear*, the firmware has been successfully loaded into the writeable bank of the fabric card.

Probable Cause

File error

Type

Processing

Remedial action

When the status is *set*, install the fabric card firmware again.

7002 0007

Component	Severity	Status
Shelf FabricCard/<instance>	major	set/clear

Legend

<instance> = X or Y

Details

This alarm is issued on fabric-based shelves when a fabric card is running firmware that is older than the latest available version.

When the status is *clear*, the fabric card is running the latest available firmware version.

Probable Cause

File error

Type

Processing

Remedial action

When the status is *set*, install the software version indicated by the *recommendedVersionToInstall* attribute of the *FabricCard* component.

7002 0008

Component	Severity	Status
Shelf Card/<instance>	warning	set/clear

Legend

<instance> = 0 - 15

Details

When the status is *set*, the fabric port has changed OSI operational state to disabled and is not in service.

When the status is *clear*, the fabric port has changed OSI operational state to enabled.

Probable Cause

Processor problem

Type

Equipment

Remedial action

No operator action is necessary if the alarm clears within 15 minutes.

If the auto-recovery mechanism has failed, follow the standard procedure for testing the fabric card, or remove or replace the defective unit(s). See 241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing* and 241-1501-215 *Passport 15000, 20000 Hardware Maintenance Guide* for information on testing and replacing the shelf card or fabric card.

When the status is *clear*, no remedial action is required.

7002 0009

Component	Severity	Status
Shelf FabricCard/<instance>	warning	set/clear

Legend

<instance> = X or Y

Details

When the status is *set*, the card port has changed OSI operational state to disabled and is not in service.

When the status is *clear*, the card port has changed OSI operational state to enabled.

Probable Cause

Processor problem

Type

Equipment

Remedial action

A fabric card test can correct this failure. See 241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing* for information on testing the fabric card.

7002 0010

Component	Severity	Status
Shelf FabricCard/<instance>	warning	message

Legend
<instance> = X or Y

Details
The fabric auto-recovery failed due to one of the following reasons:

- The fabric self test failed.
- None of the fabric ports passed the self test.

Probable Cause
Processor problem

Type
Equipment

Remedial action
System action: None

Operator action: Lock the fabric card, run the fabric card test, and unlock the fabric card. If either the fabric card test or unlock fails, contact your system administrator.

7002 0012

Component	Severity	Status
Shelf FabricCard/<instance>	warning	message

Legend

<instance> = X or Y

Details

One or more fabric ports failed the self test and remained at disabled state after the fabric unlock.

Probable Cause

Processor problem

Type

Equipment

Remedial action

System action: The FabricPort auto-recovery will recover the FabricPorts in the failed list.

Operator action: None

7002 0013

Component	Severity	Status
Shelf FabricCard/<instance>	warning	message

Legend
<instance> = X or Y

Details
The fabric unlock failed due to one of the following reasons:

- The fabric self test failed.
- None of the fabric ports passed the self test.

Probable Cause
Processor problem

Type
Equipment

Remedial action
System action: None

Operator action: Run the fabric card test. If the fabric card test fails, contact your system administrator.

7002 0014

Component	Severity	Status
Shelf FabricCard/<instance>	warning	message

Legend

<instance> = X or Y

Details

One or more fabric ports failed the self test and remained at disabled state after the fabric auto-recovery.

Probable Cause

Processor problem

Type

Equipment

Remedial action

System action: The FabricPort auto-recovery will recover the FabricPorts in the failed list.

Operator action: None

7002 1000

Component	Severity	Status
Shelf Card/<instance>	critical	message

Legend

<instance> = 0 - 15

Details

This alarm indicates that the card is not communicating properly over the backplane buses.

Probable Cause

Processor problem

Type

equipment

Remedial action

The active control processor (CP) attempts to correct the problem by re-initializing the card. If the alarm is repeated, replace the card.

7003 0001

Component	Severity	Status
Collector/<type> Agent/<cardnumber>	major/cleared	set/clear

Legend

<type> = accounting, alarm, log, scn, debug, trap, stats, rtStats

<cardnumber> = the card on which the Agent resides

Details

If the status is *set*, a data collection system (DCS) Agent's queue has reached a 75% full threshold. If the queue becomes full then subsequent records will be discarded. There are three possible reasons for this to occur. First, if there are no requestors for this particular DCS data type then the records will be held in the Agent queues. Second, the provisioned queue size may be insufficient for the amount of DCS data traffic. Thirdly, a requestor of this particular DCS data type could be slowing or blocking the flow of DCS records. For example, if spooling is provisioned to on, and the spooler is the only requestor of data then if the spooler is locked or not spooling because of a recoverable condition detected by the file system (for example, disk full), data flow will be blocked and the Agent queues will fill up.

A *clear* is issued when the queue size drops below 50% full and at least 5 minutes has elapsed since the *set* was issued. This delay provides a throttling mechanism so that bursts of records for relatively small queue sizes do not cause too many alarms within a short time. The clear will indicate how many records were discarded (if any) in the event that data arrived after the queue became 100% full.

Probable Cause

Threshold crossed

Type

Quality of service

Remedial action

If you do not wish to monitor or collect this particular type of DCS data, then you may want to provision the queue size to be zero for this data type. If this is done, then all records of this type will be discarded.

Verify that the queue size is provisioned to an adequate size for the expected amount of traffic.

Verify that there are no requestors of this DCS data type holding up the flow of records. For example, if spooling is provisioned to on, and the spooler is locked, then unlock it. If the spooler is not spooling because of a recoverable condition detected by the file system, then clear the file system problem. For information on resolving such problems, refer to the 241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing*.

When the status is *clear*, no action is required.

7003 0002

Component	Severity	Status
Collector/<type> Spooler	major/cleared	set/clear

Legend

<type> = accounting, alarm, log, scn, debug, stats, appl

Details

If the status is *set*, a DCS Spooler has stopped spooling records to the shadowed file system. Typically, the reason is due to a recoverable condition detected by the file system. The file system will have issued its own alarm(s) indicating the root cause. This DCS alarm is to indicate the effect of the file system being unavailable. The condition will likely affect other users of the file system as well. An example of a recoverable condition is *disk full*. The exact nature of the error will be displayed in the comment data field of the alarm.

This alarm can also appear under certain abnormal conditions detected by the Spooler, usually accompanied by other alarms, likely indicating some unexpected interaction with the file system. An example of such a condition is one where, after multiple CP switchover/failures, it is possible (but not guaranteed) for a file to be duplicated in both the **/spooled/opened/<type>** and **/spooled/closed/<type>** directories, causing a Spooler to fail.

A *clear* is issued after recovering from the condition.

Probable Cause

File error

Type

Processing

Remedial action

If the status is *set*, resolve the file system condition which caused this alarm to be generated. You may be required to take different actions to resolve the problem depending on the state or status of the disk or file system.

If the file system is full, clean up some files.

If the file system is locked, unlock it by issuing the *unlock* command.

If the file system fails, try to copy unprocessed spool files (for example, using FTP) from the control processor and then replace the control processor.

When a recoverable condition is resolved, the Spooler is notified and it automatically tries to continue spooling. The *clear* is issued when the Spooler is again able to spool data to the file system.

If you encounter an unexpected condition, the action may vary to some degree, but

most likely, at some point you will have to lock and then unlock the *FileSystem* component. This causes all active and failed DCS Spoolers to reset. In addition, file system commands may be needed to clean up certain files. For example, if the “duplicate file” scenario mentioned above occurs, one would have to remove or rename the file in the “closed” directory prior to locking/unlocking the *FileSystem* component.

If you are unable to resolve the file system condition, contact Nortel Networks technical support.

7003 0003

Component	Severity	Status
Collector/<type> Spooler	warning/cleared	set/clear

Legend

<type> = accounting, alarm, log, scn, debug, stats, appl

Details

If the status is *set*, then the DCS Spooler does not restrict the number of spool files to the value specified in the Spooler's *maximumNumberOfFiles* attribute.

This condition occurs when there are more than 250 files in the associated spool directory. At this point, it is no longer possible for the Spooler to enforce the value specified by *maximumNumberOfFiles* attribute. The condition persists until the number of spool files for the associated <type> is less than 250, at which time a clear alarm is issued.

Note: This condition is only expected to occur in the case where the *maximumNumberOfFiles* attribute is provisioned from zero to a non-zero value.

A *clear* is issued after recovering from the condition.

Probable Cause

Threshold crossed

Type

Quality of service

Remedial action

Reduce the number of spool files for the associated type to below 250. This can be done in one of following ways.

Ensure that MDP is configured to retrieve the spool files and remove them from the Passport.

Manually remove the spool files using the *Filesystem* component. The relevant directory to examine and from which to remove files is /spooled/closed/<type>.

If you are unable to resolve file condition, contact Nortel Networks technical support.

7003 0004

Component	Severity	Status
Collector/alarm Agent/<cardnumber>	warning	message

Legend

<cardnumber> = 0 - 15 (the card on which the Agent resides)

Details

The purpose of this alarm is to indicate if software alarms (that is, those alarms with indexes 0000 9000, 0000 9001, and 0000 9002) have been discarded and to specify how many have been discarded.

Software alarms are discarded when the rate at which they are generated exceeds a system defined threshold. This throttling mechanism is in place to protect services against an excessive number of software alarms.

Probable Cause

Threshold crossed

Type

Quality of service

Remedial action

There is no remedial action specific to this alarm.

The presence of this alarm, however, indicates that an excessive quantity of software alarms have been generated. The remedial action, when receiving software alarms, is to contact your local Nortel Networks technical support group.

7003 0005

Component	Severity	Status
Collector/applicationSpecific Spooler	major	message

Details

The data collection system (DCS) Spooler for the applicationSpecific stream is not able to send a file closure notification to the application generating the applicationSpecific records.

Probable Cause

Application subsystem failure

Type

Processing

Remedial action

Determine why the application generating the records is no longer registered or is not responding. Retrieve and remove the file(s) specified in the alarm from the disk.

7003 0006

Component	Severity	Status
Collector/applicationSpecific Spooler	minor	message

Details

The data collection system (DCS) Spooler for an applicationSpecific stream is not able to send a file deletion notification to the application generating the applicationSpecific records.

Probable Cause

Application subsystem failure

Type

Processing

Remedial action

Determine why the application generating the records is no longer registered or is not responding.

7003 0007

Component	Severity	Status
Lp/<x> Eng AAList	major/cleared	set/clear

Legend

<x> = 0 - 15

Details

If the status is *set*, the active alarm list residing on the LP has reached a 75% full threshold. If the list becomes full, subsequent SET alarms are not added to it. There are two possible reasons for the list to become full:

- There are many SET but no matching CLR alarms issued on the given LP. The active SET alarms are held in the active alarm list and the list gradually fills up.
- The provisioned size of the list may be insufficient for the amount of the SET alarm traffic.

If the status is *clear*, the size of the active alarm list that resides on the LP has dropped below 50% and at least five minutes has elapsed since the *set* was issued. This delay provides a throttling mechanism so that bursts of records for relatively small queue sizes do not cause too many alarms within a short time. The comment text of the clear alarm indicates how many active set alarms were discarded (if any, in the event that the list became 100% full) since the *set* was issued.

This alarm is also hierarchically cleared when the LP on which the active alarm list resides is cleared.

Probable Cause

Threshold crossed

Type

Quality of service

Remedial action

If you do not want to monitor or build active alarm lists, you can provision the list sizes to be disabled, delete the *ActiveAlarmServices* component, or remove the active alarm list feature from the feature lists. If any of these actions are done, all active alarm lists are empty.

Verify that the active alarm list sizes are provisioned to an adequate size.

7004 0101

Component	Severity	Status
<parent_name>/<instance> <type>	critical/cleared	set/clear

Legend

<parent_name> = Trunk or DpnGateway

<instance> = a decimal value

<type> = Utp, Unacked, AtmAccess, or FrAccess

Details

If the status is *set*, a link quality degradation has been detected, and its parent component is disabled. More specifically, the link error rate has exceeded the acceptable threshold as specified in the provisioning data of this component.

A *clear* is issued after its parent component completes restaging.

Probable Cause

Type

Remedial action

Determine why the link quality has degraded. Note that, for FrAccess, the only quality parameter is the lost frames by the external frame relay network. If it is exhibiting the expected or a higher yet acceptable rate, then change the provisioned error rate threshold to allow for a faultier connection. The amount of traffic allowed to be routed through the link should also be reduced.

7004 0102

Component	Severity	Status
<parent_name>/<instance> <type>	major/cleared	set/clear

Legend

<parent_name> = Trunk or DpnGateway

<instance> = a decimal value

<type> = Utp or Unacked

Details

If the status is set, it is indicative of an unsuccessful registration with the congestion management. An example is when the maximum number of DpnGateway/UTP registrations has been exceeded on a DS1C/E1C FP. Each DpnGateway that caused the maximum number of registrations to be exceeded is disabled and not allowed to come up.

A clear is issued for every Trunk or DpnGateway that successfully registers with the congestion management.

Probable Cause

Type

Remedial action

Manual intervention by the user may be necessary as a remedial action. On DS1C/E1C cards the provisioning has to be modified such that the total number of DpnGateways per card is less than or equal to the maximum of 23.

It is also possible to have more than 23 DpnGateways provisioned on a DS1C/E1C card. In this case, the *ifAdminStatus* attribute of the DpnGateways which have exceeded the maximum number of registrations must be set to down.

7004 0301

Component	Severity	Status
DpnGateway/<instance> Utp	critical/cleared	set/clear

Legend

<instance> = a decimal value

Details

If the status is *set*, the Utp has been disabled due to a protocol violation caused possibly by (1) A loop check frame not being received within an expected time, or (2) Utp trying to enter Are-You-There at a wrong state as a result of LastAckTimeout protocol violation.

See also alarms 7004 0305 and 7004 0306 for other types of protocol violations.

A *clear* is issued after the Utp has successfully restaged.

All protocol violation conditions may arise due to problems with the physical layer or due to a side effect of congestion recovery. Under congestion recovery the link receive buffers may be discarded to free up resources for the FP. The missing frames resulting from discarding this buffer could result in one of the protocol violations if the loss were severe enough.

Probable Cause

Type

Remedial action

Issue the *display statistics* command for the Framer subcomponent on both the local and remote ends of the connection. This is done to verify that the physical layer is good. Also issue a *display shelf card/n util* command to determine if the FP is running at high CPU or memory utilization. Revisit the engineering guidelines for this service if condition persists.

7004 0302

Component	Severity	Status
DpnGateway/<instance> Utp	major/cleared	set/clear

Legend

<instance> = a decimal value

Details

If the status is *set*, the Framer subcomponent has measured a transmit link speed that exceeds 2 Mbit/s.

A *clear* is issued after the link speed is less than or equal to 2 Mbit/s.

Probable Cause

Type

Remedial action

Determine whether the link speed of the hardware component has been provisioned incorrectly.

7004 0303

Component	Severity	Status
DpnGateway/<instance> Utp	critical/cleared	set/clear

Legend

<instance> = a decimal value

Details

If the status is *set*, the Utp has experienced a staging time-out by not completing staging within the expected time. This can occur if no frames are received or when the remote end is too slow.

The component will attempt to restage. As a result, the parent *DpnGateway* component will take longer to stage with the remote. A *clear* is issued after the Utp has successfully restaged.

Probable Cause

Type

Remedial action

Verify that the connection is valid and that the hardware components on both ends have been provisioned correctly. Perform a port and line test with manual looping if possible to verify the physical layer.

7004 0304

Component	Severity	Status
DpnGateway/<instance> Utp	critical/cleared	set/clear

Legend

<instance> = a decimal value

Details

If the status is *set*, the Utp has been disabled due to loss of communication with the far end. It can occur when Utp has detected a Yes-I-Am Timeout. This condition may arise due to far end disabling, problems with the underlying physical layer, or a side effect of congestion recovery.

A *clear* is issued after the Utp has successfully restaged.

Probable Cause

Type

Remedial action

Issue the *display statistics* command for Utp component and the Framer subcomponent on the local end and for the port on the remote end of the connection. This is done to verify that the connection is valid and physical layer is good. Also issue a *display shelf card/n util* command to determine if the FP is running at high CPU or memory utilization. Issue a *display statistics* command for the PE on the remote DPN to determine if the PE is running at high CPU or memory utilization. Revisit the engineering guidelines for this service if condition persists.

7004 0305

Component	Severity	Status
DpnGateway/<instance> Utp	critical/cleared	set/clear

Legend

<instance> = a decimal value

Details

If the status is *set*, the Utp has been disabled due to a LastAckTimeout protocol violation.

See also alarms 7004 0301 and 7004 0306 for other types of protocol violation.

A *clear* is issued after the Utp has successfully restaged.

This condition is related directly to the windowed protocol. It may arise when no acknowledgment is received from the far end.

All protocol violation conditions may arise due to problems with the physical layer or due to a side effect of congestion recovery. Under congestion recovery the link receive buffers may be discarded to free up resources for the FP. The missing frames resulting from discarding this buffer could result in one of the protocol violations if the loss were severe enough.

Probable Cause

Type

Remedial action

Issue the display statistics command for the *Framer* subcomponent on both the local and remote ends of the connection to verify that the physical layer is operational. Also issue a display shelf card/n util command to determine if the FP is running at high CPU or memory utilization. Revisit the engineering guidelines for this service if condition persists.

7004 0306

Component	Severity	Status
DpnGateway/<instance> Utp	critical/cleared	set/clear

Legend

<instance> = a decimal value

Details

If the status is *set*, the Utp has been disabled due to a large gap in acknowledgment protocol violation.

See also alarms 7004 0301 and 7004 0305 for other types of protocol violation.

A *clear* is issued after the Utp has successfully restaged.

This condition is related directly to the windowed protocol. It may arise due to lost of excessive number of frames within an acknowledgment window.

All protocol violation conditions may arise due to problems with the physical layer or due to a side effect of congestion recovery. Under congestion recovery the link receive buffers may be discarded to free up resources for the FP. The missing frames resulting from discarding this buffer could result in one of the protocol violations if the loss were severe enough.

Probable Cause

Type

Remedial action

Issue the display statistics command for the *Framer* subcomponent on both the local and remote ends of the connection to verify that the physical layer is operational. Also issue a *display shelf card/n util* command to determine if the FP is running at high CPU or memory utilization. Revisit the engineering guidelines for this service if condition persists.

7004 0401

Component	Severity	Status
DpnGateway/<instance> FrAccess	major	set

Legend

<instance> = a decimal value

Details

If the status is *set*, the *FrAccess* component has been disabled due to a protocol violation.

A *clear* is issued after the *FrAccess* component has successfully restaged.

Probable Cause

Type

Remedial action

Issue the display statistics command for the subcomponent on both the local and remote ends of the connection to verify that the physical layer is operational. Also issue a display shelf card/n util command to determine if the FP is running at high CPU or memory utilization. Revisit the engineering guidelines for this service if condition persists.

7004 0402

Component	Severity	Status
DpnGateway/<instance> FrAccess	major/cleared	set/clear

Legend

<instance> = a decimal value

Details

If the status is *set*, the provisioned CIR (committed information rate) exceeds 2 Mbit/s.

A *clear* is issued when the CIR is reprovisioned to less than or equal to 2 Mbit/s.

Probable Cause

Type

Remedial action

Determine whether the CIR has been provisioned correctly.

7004 0403

Component	Severity	Status
DpnGateway/<instance> FrAccess	critical/cleared	set/clear

Legend

<instance> = a decimal value

Details

If the status is *set*, the *FrAccess* component has experienced a staging time-out by not completing staging within the expected time. This can occur if no frames are received or when the remote end is too slow.

The component will attempt to restage. As a result, the parent *DpnGateway* component will take longer to stage with the remote.

A *clear* is issued after the *FrAccess* component has successfully restaged.

Probable Cause

Type

Remedial action

Verify that the connection is valid and that the hardware components on both ends have been provisioned correctly. Verify that the *Fr Dlci* components and the PVCs are provisioned correctly and operational.

7004 0404

Component	Severity	Status
DpnGateway/<instance> FrAccess	critical/cleared	set/clear

Legend

<instance> = a decimal value

Details

If the status is *set*, the *FrAccess* component has been disabled due to loss of communication with the far end. This can occur when the *FrAccess* component detects a Yes-I--Am timeout. This condition can arise due to far end disabling, problems with the underlying physical layer, or a sided effect of congestion recovery.

A *clear* is issued after the *FrAccess* component has successfully restaged.

Probable Cause

Type

Remedial action

Issue the display statistics command for the *FrAccess* component and the *FrMux Framer* subcomponent on the local end. Issue the pi n po m D stat command for the port on the remote end to verify that the connection is valid and that the physical layer is operational. Also issue the d frmux/n dlci/m command and similar frmux related commands to determine the status of the underlying PVC. Also issue a display shelf card/n util command to determine if the FP is running at high CPU or memory utilization. Issue a PE n D statistics command for the PE on the remote DPN to determine if the PE is running at high CPU or memory utilization. Revisit the engineering guidelines for this service if the condition persists.

7005 0101

Component	Severity	Status
<component_name>/<instance>	critical/cleared	set/clear

Legend

<component_name> = Trunk or DpnGateway

<instance> = a decimal value

Details

If the status is *set*, the component has experienced a staging time-out by not receiving all the required packets from the remote component within the expected time.This can result from excessive congestion on the link.

The component immediately attempts to restage and a *clear* is issued if successful.

Probable Cause

Type

Remedial action

Verify that the speeds on both ends of the connection are the same. Also, any other facility error (or unavailability) may cause the generation of this alarm.

7005 0102

Component	Severity	Status
<component_name>/<instance>	critical/cleared	set/clear

Legend

<component_name> = Trunk

<instance> = a decimal value

Details

If the status is *set*, the Trunk has been unable to stage logical network numbers (LNN) with the remote component.

The component attempts to restage in five minutes and a *clear* is issued if successful.

Probable Cause

Type

Remedial action

Verify that the provisioned supported address plan subcomponents match those provisioned at the remote.

7005 0103

Component	Severity	Status
<component_name>/<instance>	critical/cleared	set/clear

Legend

<component_name> = Trunk or DpnGateway

<instance> = a decimal value

Details

If the status is *set*, the routing system has not permitted the *Trunk* or *DpnGateway* component to stage with the remote for one of the following reasons:

- attempting to stage a fifth link in a link group.

- the Routing System is unable to communicate with the far end node. The alarm will probably occur about 2.5 minutes after the Trunk goes online each and every time that it does go online.

- attempting to stage a link between two nodes that have different region ids and are in the same RID subnet.

- there are multiple links in a link group and some are going down while the rest are coming up. It is possible for all to be down at the same time for a small window on one side of the link group only. This is more likely to occur when there is PORS traffic on the Trunks. In this case the alarm should occur once, the Trunks should restage and there should be no further problem.

- the node is a Passport cluster node and the remote node is a DPN-100 RM or CSRM.

- both the local and remote nodes are Passport cluster nodes. Since multi-node cluster is not supported, any link between two Passport cluster nodes are disabled.

A *clear* is issued when the *Trunk* or *DpnGateway* component is able to successfully stage with the remote.

Probable Cause

Type

Remedial action

Verify that the number of *Trunk* or *DpnGateway* components in the link group has not exceeded the maximum.

Check the region ids and RIDs of the two nodes and verify that the RIDs are also different if the region ids are non-zero and different.

Check that the traffic shaping is enabled on the NEP end (if UPC is enabled on backbone). Check that UPC and traffic shaping contracts are matching on all VCCs used for ATM logical trunks.

Verify the trunk end-to-end connectivity.

Check the *clusterNode* attribute of the node. If it is ***yes***, check the remote node and ensure it is not also a cluster node or an RM or a CSRM. If the connection to the RM or CSRM is required, the value for *clusterNode* should be configured as ***no***, or the connection to the RM should be established from another non-cluster node. If the remote end is also Passport cluster node, either disable the trunk between the two cluster nodes or provision one of the nodes to be a non-cluster node.

7005 0104

Component	Severity	Status
<component_name>/<instance>	critical/cleared	set/clear

Legend

<component_name> = Trunk or DpnGateway

<instance> = a decimal value

Details

If the status is *set*, the *Trunk* or *DpnGateway* component has not staged with the remote module/component as specified in the provisioning file.

A *clear* is issued when the *Trunk* or *DpnGateway* component stages with the expected remote.

Probable Cause

Type

Remedial action

For a *Trunk* component, verify that the *expectedRemoteNodeId* attribute is either set properly or left blank (that is, provisioned as “”). For a *DpnGateway* component, verify its *expectedRemoteNamsId* attribute in the same way.

7005 0105

Component	Severity	Status
<component_name>/<instance>	critical/cleared	set/clear

Legend

<component_name> = Trunk or DpnGateway

<instance> = a decimal value

Details

If the status is *set*, the *Trunk* or *DpnGateway* component has failed to stage with the remote due to poor link quality.

A *clear* is issued when the *Trunk* or *DpnGateway* component successfully restages with the remote.

Probable Cause

Type

Remedial action

Inspect and repair the facility to provide better link quality.

7005 0106

Component	Severity	Status
<component_name>/<instance>	critical/cleared	set/clear

Legend

<component_name> = Trunk or DpnGateway

<instance> = a decimal value

Details

If the status is *set*, the *Trunk* or *DpnGateway* component must disable due to poor link quality (with permission from the Routing System).

A *clear* is issued when the *Trunk* or *DpnGateway* component successfully restages with the remote.

Probable Cause

Type

Remedial action

Inspect and repair the facility to provide better link quality.

7005 0107

Component	Severity	Status
<component_name>/<instance>	critical	message

Legend

<component_name> = Trunk or DpnGateway

<instance> = a decimal value

Details

If the round trip delay (calculated from the timestamps of a Propagation Delay packet) exceeds the limit accepted by the Routing System (1500 ms), it is assumed that the Propagation Delay packet was lost at least once during transmission, due to a faulty link. The propagation delay reported to the Routing System is then overwritten to 1500 ms, enabling the *Trunk* or *DpnGateway* component to come up. The measured round trip delay will still indicate to the user the actual value (which exceeds 1500 ms).

Probable Cause

Type

Remedial action

Inspect and repair the facility to provide better link quality.

7005 0108

Component	Severity	Status
<component_name>/<instance>	critical	set/clear

Legend

<component_name> = Trunk or DpnGateway

<instance> = a decimal value

Details

If the status is *set*, the *Trunk* or *DpnGateway* component's *overrideRoundTripDelay* attribute has been provisioned with a value that does not match the value that is provisioned on the remote.

A *clear* is issued when the *Trunk* or *DpnGateway* component detects that the provisioned value on each end matches.

Probable Cause

Type

Remedial action

Determine which end of the connection has not been provisioned with the correct override value.

7005 0109

Component	Severity	Status
<component_name>/<instance>	critical	set/clear

Legend

<component_name> = Trunk or DpnGateway

<instance> = a decimal value

Details

If the status is *set*, the *Trunk* or *DpnGateway* component's *overrideTransmitSpeed* attribute has been provisioned with a value that does not match the value that is provisioned on the remote.

A *clear* is issued when the *Trunk* or *DpnGateway* component detects that the provisioned value on each end matches.

Probable Cause

Type

Remedial action

Determine which end of the connection has not been provisioned with the correct override value.

7005 0110

Component	Severity	Status
<component_name>/<instance>	minor/cleared	set/clear

Legend

<component_name> = Trunk or DpnGateway

<instance> = a decimal value

Details

This alarm is issued by Passport Unacknowledged Trunks, Passport Trunks over ATM and Passport DpnGateways over UTP.

When the status is *set*, the total average link or ATM VCC utilization has exceeded the value of the *minorLinkUtilAlarmThreshold* attribute or the value of the *minorVccUtilAlarmThreshold* attribute, for a sustained period of time.

When the status is *clear*, the total average link or ATM VCC utilization has subsequently fallen back to a level at or below the corresponding threshold value for a sustained period of time.

For Framer-based trunks and DPN gateways, the total average link utilization is calculated every minute based on comparing the number of bytes received by the link with the available bandwidth on the link. For ATM-based trunks, the total average ATM VCC utilization is calculated every minute based on comparing the number of cells received by the ATM VCC with the estimated available bandwidth on the ATM VCC.

Probable Cause

Type

Remedial action

The idea is that, with a proper threshold setting, a single instance of this alarm should not require any special action. It would only be an early indication of possible link or ATM VCC congestion. If this alarm is repeated over a relatively short period of time, it may be an indication that the threshold setting is too low. If so, adjust the threshold accordingly. Otherwise, it could indicate bursty traffic, in which case, it could be the indicator that you want. The occurrences of the alarm must be evaluated in the context of other parameters. For Framer-based trunks and

DpnGateways, examples include link speeds, availability of other links, and routing/loadsharing algorithms. For ATM-based trunks, examples include ATM VCC PCR, effective cell rate, availability of other VCCs, and routing/loadsharing algorithms. If the more severe alarms are also issued, you will likely need to consider re-engineering the links or ATM VCCs on this node in order to alleviate the congestion conditions.

7005 0111

Component	Severity	Status
<component_name>/<instance>	major/cleared	set/clear

Legend

<component_name> = Trunk or DpnGateway

<instance> = a decimal value

Details

This alarm is issued by Passport Unacknowledged Trunks, Passport Trunks over ATM and Passport DpnGateways over UTP.

When the status is *set*, the total average link or ATM VCC utilization has exceeded the values of the *majorLinkUtilAlarmThreshold* or *majorVccUtilAlarmThreshold* attributes respectively, for a sustained period of time.

When the status is *clear*, the total average link or ATM VCC utilization has subsequently fallen back to a level at or below the corresponding threshold value for a sustained period of time.

For Framer-based trunks and DpnGateways, the total average link utilization is calculated every minute based on comparing the number of bytes received by the link with the available bandwidth on the link. For ATM-based trunks, the total average ATM VCC utilization is calculated every minute based on comparing the number of cells received by the ATM VCC with the estimated available bandwidth on the ATM VCC.

Probable Cause

Type

Remedial action

The idea is that, with a proper threshold setting, a single instance of this alarm should not require any special action although it would likely be a good indication of pending link or ATM VCC congestion. If this alarm is repeated over a relatively short period of time, it may be an indication that the threshold setting is too low. The occurrences of the alarm must be evaluated in the context of other parameters For Framer-based trunks and DpnGateways, examples include link speeds, availability of other links, and routing/loadsharing algorithms. For ATM-based trunks, examples include ATM VCC PCR, effective cell rate, availability of other VCCs, and routing/loadsharing algorithms. If the more severe alarm is also issued, likely you will need to consider re-engineering the links or ATM VCCs on this node in order to alleviate the congestion conditions.

7005 0112

Component	Severity	Status
<component_name>/<instance>	critical/cleared	set/clear

Legend

<component_name> = Trunk or DpnGateway

<instance> = a decimal value

Details

This alarm is issued by Passport Unacknowledged Trunks, Passport Trunks over ATM and Passport DpnGateways over UTP.

When the status is *set*, the total average link or ATM VCC utilization has exceeded the values of the *criticalLinkUtilAlarmThreshold* or *criticalVccUtilAlarmThreshold* attributes respectively, for a sustained period of time.

When the status is *clear*, the total average link or ATM VCC utilization has subsequently fallen back to a level at or below the corresponding threshold value for a sustained period of time.

For Framer-based trunks and DpnGateways, the total average link utilization is calculated every minute based on comparing the number of bytes received by the link with the available bandwidth on the link. For ATM-based trunks, the total average ATM VCC utilization is calculated every minute based on comparing the number of cells received by the ATM VCC with the estimated available bandwidth on the ATM VCC.

Probable Cause

Type

Remedial action

With a proper threshold setting, this alarm should cause a serious evaluation of how to alleviate the congestion conditions. Most likely, many packets are being discarded which is obviously undesirable over the long term. The occurrences of the alarm must be evaluated in the context of other parameters. For Framer-based Trunks and DpnGateways, examples include link speeds, availability of other links, and routing/loadsharing algorithms. For ATM-based trunks, examples include ATM VCC PCR, effective cell rate, availability of other VCCs, and routing/loadsharing algorithms.

7005 0113

Component	Severity	Status
<component_name>/<instance>	warning/cleared	set/clear

Legend

<component_name> = Trunk

<instance> = a decimal value

Details

When the status is *set*, the measured speed of the trunk has dropped below the value which is specified by the attribute *lowSpeedAlarmThreshold* attribute.

When the status is *clear*, the measured speed of the trunk has returned to or exceeded the *lowSpeedAlarmThreshold* value.

Probable Cause

Type

Remedial action

1) For an elastic ATM trunk on a Passport 8-port DS1/E1 ATM FP with IMA feature, this alarm can indicate that the bandwidth allocated to Trunk on IMA group has been reduced.
This will generally result from the removal or failure of the IMA links.
Check the IMA alarms.

2) For an HDLC based trunk using third party Dial Backup equipment, this alarm can indicate that the Trunk is running at a decreased speed provided by the Backup lines. This will generally result from leased line failure and backup lines being dialed up. Check the operational mode of the Dial Backup equipment and the leased line connection.

3) For an HDLC-based trunk using third party Inverse Multiplexing equipment, this alarm can indicate that the Trunk is running at a decreased speed provided by the Inverse Multiplexing equipment. This will generally result from the removal or failure of links between the Inverse Multiplexing equipment. Check the operational mode of the Inverse Multiplexing equipment and the link connection.

7005 0114

Component	Severity	Status
<component_name>/<instance>	warning/cleared	set/clear

Legend

<component_name> = Trunk

<instance> = a decimal value

Details

When the status is *set*, the measured speed of the trunk has exceeded the value which is specified by the attribute *highSpeedAlarmThreshold* attribute.

When the status is *clear*, the measured speed of the trunk has returned to or fallen below the *highSpeedAlarmThreshold* value.

Probable Cause

Type

Remedial action

1) For an HDLC-based trunk using third party Bandwidth on Demand equipment, this alarm can indicate that the trunk is running at an increased speed when Bandwidth on Demand occurs. Check the operational mode of the Bandwidth on Demand equipment and the leased line connection.

2) For an HDLC-based trunk using third party Inverse Multiplexing equipment, this alarm can indicate that the Trunk is running at an increased speed provided by the Inverse Multiplexing equipment. This will generally result from the adding links between the Inverse Multiplexing equipment. Check the operational mode of the Inverse Multiplexing equipment and the link connection.

7005 0115

Component	Severity	Status
DpnGate/<instance>	indeterminate	message

Legend

<instance> = a decimal value

Details

This alarm is issued when a dial-in link becomes active. The following information is attached:

- own component ID

- Comment data containing the following 2 lines:

Link type: <DBNL or BWOD>

Remote id: <PM/<names mnemonic> PE/<#> PI/<#> PO/<#>.

Probable Cause

Type

Remedial action

For a dbnl link, the cause of the link failure at the remote end should be identified and dealt with. When the dedicated link comes into service, this DBNL link will be disabled automatically (if the DBNL Auto-Disable feature is active on the remote). For a BWOD link, no action is necessary.

7005 0116

Component	Severity	Status
DpnGate/<instance>	indeterminate	message

Legend

<instance> = a decimal value

Details

This alarm is issued when a dial-in link is deactivated. This could be due to automatic disabling (DBNL), automatic deactivation (BWOD), or manual disable. The following information is attached:

- own component ID

- Comment data containing the following 2 lines:

Link type: <DBNL or BWOD>

Remote id: <PM/<names mnemonic> PE/<#> PI/<#> PO/<#>.

Probable Cause

Type

Remedial action

Not applicable.

7005 0117

Component	Severity	Status
<component_name>/<instance>	major	set/clear

Legend

<component_name> = Trunk

<instance> = a decimal value

Details

This alarm is issued when the link speed (provided by the underlying link protocol) has exceeded the maximum speed supported by the *Trunk* component. The value of the *measuredSpeedToInterface* attribute (under the *Trunk* component) and the speed reported to the routing system is replaced by the maximum supported speed value. Although the speed has been adjusted to the maximum supported value, statistics can roll over prematurely if an excessive burst of data is received by the *Trunk* component. At this point the statistics should be considered unreliable.

When the status is *clear*, the link speed has fallen to or below the maximum supported link speed.

Probable Cause

Type

Remedial action

Lower the link speed to or below the trunk speed limit displayed in the alarm text.

7005 0118

Component	Severity	Status
Trk/<num>	warning	set/clear

Legend

<num> = 0 - 65535

Details

The connectivity of the trunk is not to the same node that is provisioned in attribute *Trk expectedRemoteNodeName*.

The provisioned value of attribute *Trk expectedRemoteNodeName* does not match the actual remote node name discovered by the trunk. The trunk is allowed to stage and function normally because attribute *Trk remoteValidationAction* is provisioned to continue.

Probable Cause

Configuration or customization error

Type

Processing

Remedial action

Ensure the connectivity of the trunk is to the desired remote node. Provision attribute *Trk expectedRemoteNodeName* to match the desired remote node name. Find the remote node name by executing the command “d -p Mod nodeName” on the remote node.

7005 0201

Component	Severity	Status
DpnGateway/<instance>	critical/cleared	set/clear

Legend

<instance> = a decimal value

Details

If the status is *set*, a problem with neighbor checking has been detected. Many consecutive neighbor checks are missing. Communication with the remote has been disrupted due to congestion or faults.

A *clear* is issued when the *DpnGateway* component successfully restages with the remote.

Probable Cause

Type

Remedial action

Verify that the *DpnGateway* component is neither overloaded, congested or faulty.

7005 0202

Component	Severity	Status
DpnGateway/<instance>	critical/cleared	set/clear

Legend

<instance> = a decimal value

Details

If the status is *set*, the *DpnGateway* component has detected that it is attempting to stage with another *DpnGateway* component.

The *DpnGateway* component attempts to restage in five minutes and a *clear* is issued if successful.

Probable Cause

Type

Remedial action

Verify that the connection is with the *DpnGateway* component that matches the one in the provisioning file.

7005 0203

Component	Severity	Status
DpnGateway/<instance>	critical/cleared	set/clear

Legend

<instance> = a decimal value

Details

If the status is *set*, the *DpnGateway* component has detected that it is attempting to stage with a DPN-100 AM that is in Trunk mode.

The *DpnGateway* component attempts to restage in five minutes and a *clear* is issued if successful.

Probable Cause

Type

Remedial action

Correct the remote's provisioning data to reflect that it is a Network Link.

7005 0204

Component	Severity	Status
DpnGateway/<instance>	critical/cleared	set/clear

Legend

<instance> = a decimal value

Details

If the status is *set*, the *DpnGateway* component has detected that it is attempting to stage with a DPN-100 RM that is in Network Link mode.

The *DpnGateway* component attempts to restage in five minutes and a *clear* is issued if successful.

Probable Cause

Type

Remedial action

Correct the remote's provisioning data to reflect that it is a Trunk.

7005 0205

Component	Severity	Status
DpnGateway/<instance>	critical/cleared	set/clear

Legend

<instance> = a decimal value

Details

If the status is *set*, the *DpnGateway* component has detected that it is attempting to stage with a DPN-50.

The *DpnGateway* component attempts to restage in five minutes and a *clear* is issued if successful.

Probable Cause

Type

Remedial action

Verify that the connection is with a non-DPN-50 (for example, DPN-100 RM/AM) module as specified in the provisioning data.

7005 0206

Component	Severity	Status
DpnGateway/<instance>	critical/cleared	set/clear

Legend

<instance> = a decimal value

Details

If the status is *set*, the *DpnGateway* component has detected that it is attempting to stage with an AM/RM that is not supported by Passport.

The *DpnGateway* component attempts to restage in five minutes and a *clear* is issued if successful.

Probable Cause

Type

Remedial action

Verify that the connection is with a module which is supported by Passport, and is as specified in the provisioning data.

7005 0207

Component	Severity	Status
DpnGateway/<instance>	critical/cleared	set/clear

Legend

<instance> = a decimal value

Details

If the status is *set*, a problem with neighbor checking has been detected. According to information in the neighbor check packets, the neighbor has changed. The link will restage with the new neighbor.

A *clear* is issued when the *DpnGateway* component successfully restages with the remote.

Probable Cause

Type

Remedial action

Verify that the *DpnGateway* component is connected to the expected neighbor. Follow-up with an investigation to discover why the neighbor identifiers changed in an unexpected manner.

7005 0208

Component	Severity	Status
DpnGateway/<instance>	critical/cleared	set/clear

Legend

<instance> = a decimal value

Details

If the status is *set*, a problem with neighbor checking has been detected. According to information in the neighbor check frames, the *DpnGateway* component is now looped back to itself, likely due to a loop at physical layer.

A *clear* is issued when the *DpnGateway* component successfully restages with the remote.

Probable Cause

Type

Remedial action

Verify that the *DpnGateway* component is neither overloaded, congested nor faulty.

7005 0301

Component	Severity	Status
Trunk/<instance>	critical/cleared	set/clear

Legend
<instance> = a decimal value

Details
If the status is *set*, communication with the remote is lost because of congestion or faults.

A *clear* is issued when the *Trunk* component successfully restages with the remote.

Probable Cause

Type

Remedial action
Verify that the Trunk is neither overloaded, congested or faulty.

7005 0302

Component	Severity	Status
Trunk/<instance>	critical/cleared	set/clear

Legend

<instance> = a decimal value

Details

If the status is *set*, the Trunk has discovered that the remote identification is different from the one discovered during staging.

The component will immediately attempt to restage. As a result, the connection that was provided to the routing system is discontinued.

A *clear* is issued when the *Trunk* component successfully restages with the remote.

Probable Cause

Type

Remedial action

Determine if the connection to the remote component has been changed. If it has changed then make sure to update it to the ones used during staging.

7005 0303

Component	Severity	Status
Trunk/<instance>	warning/cleared	set/clear

Legend

<instance> = a decimal value

Details

If the status is *set*, the number of supported address plan subcomponents exceeds the number of logical network numbers (LNN) that the Trunk's protocol is able to stage.

Staging of the excessive address plans will not be attempted. As a result, the routing system may not be provided with as much LNN connectivity as expected.

A *clear* is issued when the number of supported address plan subcomponents no longer exceeds the number of logical network numbers (LNN) that the Trunk's protocol is able to stage.

Probable Cause

Type

Remedial action

None.

7005 0304

Component	Severity	Status
Trunk/<instance>	critical/cleared	set/clear

Legend

<instance> = a decimal value

Details

If the status is *set*, the Trunk has discovered that it is attempting to stage with another Trunk from another Passport in the same topology region with the same node ID.

The Trunk attempts to restage in five minutes and a *clear* is issued if successful.

Probable Cause

Type

Remedial action

Modify the local Node Id or the remote passport node ID to be unique.

7005 0305

Component	Severity	Status
Trunk/<instance>	critical/cleared	set/clear

Legend

<instance> = a decimal value

Details

If the status is *set*, the Trunk has discovered that the remote Trunks has either attempted to restage or has been disabled.

The Trunk attempts to restage immediately and a *clear* is issued if successful.

Probable Cause

Type

Remedial action

If the Trunk does not restage, verify the remote Trunk as it may have been locked by an operator or disabled by the Routing System. If it is not obvious, examine any alarms issued by the remote Trunk.

7005 0306

Component	Severity	Status
Trunk/<instance>	critical/cleared	set/clear

Legend

<instance> = a decimal value

Details

The status is *set* when the Trunk component detects that the remote trunk does not recognize a 5-Digit instance value and this component has an instance with 5 digits. It indicates that the value in *remoteComponentName* attribute of the remote trunk is incorrect.

A clear is issued when the trunk re-stages and discovers that the remote end does support 5-digit Trunk instance value.

Probable Cause

Type

Remedial action

Either change the Trunk instance value to be less than 5 digits, or upgrade the other end to support 5-digit Trunk instance range.

7006 0001

Component	Severity	Status
Nmis <type>	major	message

Legend

<type> = Telnet, Fmip or Ftp

Details

An NMIS connection was attempted from an unauthorized IP address. The attempted connection was blocked. The source IP address of the connection is shown in the comment field.

Probable Cause

Unauthorized access

Type

Security

Remedial action

This alarm may appear in two general scenarios.

First, the unauthorized IP address may be a legitimate network management station whose IP address has not yet been provisioned on the Passport. In this case, simply provision an *AccessControlIpAccess* component with the new IP address.

Second, the unauthorized IP address may represent a hostile attack by a hacker attempting to penetrate the Passport. Your network security may be threatened. Verify that the source IP address is not a friendly address, or refer the alarm to your system administrator for investigation. It may be possible to trace the attack to the source computer by using the source IP address.

7006 0002

Component	Severity	Status
Nmis <type> Session/<n>	warning	message

Legend

<type> = Telnet, Fmip, Local or Ftp

<n> = session number

Details

A network management interface system (NMIS) login failed after three invalid userId and password attempts. The attempted session is frozen for two minutes, and then terminated. The last userId entered and the IP address of the node attempting the login are shown in the comment field.

Probable Cause

Authentication failure

Type

Security

Remedial action

This alarm may appear in two general scenarios.

First, a legitimate user may have incorrectly entered the password three successive times. If you can determine that the alarm was caused by a legitimate user, the alarm may be ignored.

Second, a hostile password attack may be underway by a hacker attempting to penetrate the Passport. Your network security may be threatened. The two-minute session freeze will slow the password attempts. To frustrate the attack even further, consider issuing a Lock command on the interface used in the attack, or refer the alarm to your system administrator for investigation. It may be possible to trace the attack back to its source by the userId and the IP address shown in the comment field.

7006 0003

Component	Severity	Status
Nmis <type> Session/<n>	major	message

Legend

<type> = Telnet, Fmip, or Ftp
<n> = session number

Details

A TCP connection into network management interface system (NMIS) failed, causing the session to terminate. It is possible to identify the node whose connection failed by the IP address shown in the comment field. There are several possible causes for this situation, all relating to a TCP/IP read/write failure. Some are:

The NMIS session was killed without using the logoff command.

The remote site has crashed.

The IPIVC connection has failed, causing all sessions on that IPIVC to crash.

Preside Multiservice Data Manager checks the Passport continually to see if it is operational. Under severe congestion conditions, or if the Passport CPU is at 100% capacity, it does not send a response to Preside Multiservice Data Manager. Preside Multiservice Data Manager then closes its side of the connection, thus killing the FMIP session.

If the Passport is isolated (no trunks connecting to it), the session is not registered for alarms, and the workstation has the TCP/IP keep alive option, the session shuts down after two hours.

Probable Cause

Loss of Signal

Type

Communications

Remedial action

None.

7006 0004

Component	Severity	Status
Nmis Fmip	<severity>	message

Legend

<severity> = major, minor or warning

Details

An FMIP protocol error has occurred. The alarm is typically associated with a command and the response to that command contains further information.

The command may have failed completely, or have been partially executed.

A *major* severity indicates software errors, while *minor* and *warning* severity are indicative of Preside Multiservice Data Manager workstation/Passport software version incompatibilities.

There may exist comment text with further information.

Probable Cause

Type

Remedial action

Typically, the Preside Multiservice Data Manager Workstation and Passport software are running incompatible versions. It may be necessary to upgrade the software on the Preside Multiservice Data Manager Workstation.

If upgrading the software does not eliminate the alarm, contact Nortel Networks global support.

7006 0005

Component	Severity	Status
Nmis Ftp Prov Migration	major	message

Details

An FTP connection to the Active CP has been attempted from a local 127.n.n.n IP address on one of the FPs. The connection was blocked. The FTP connection is typically established for an eprom firmware upgrade.

The FTP connection may be blocked for two reasons. The Passport may be running low on memory needed to set up the FTP session, or the FTP interface may be locked (not the case for Migration CP) or busy. Refer to the comment field for an indicated cause for blocking the connection.

Note that this alarm is issued only for FTP connections from a local 127.n.n.n IP address on the Passport itself, and not from general IP addresses outside the Passport.

Probable Cause

Out of memory

Type

Processing

Remedial action

If the FTP interface is locked, issue the Unlock command to enable FTP service.

If the FTP interface is busy because all allowable sessions are currently occupied, try to finish an FTP session, log off, and free it for reuse.

If CP heap memory is too low, the Passport may have to be re-engineered or reprovisioned to free up more heap.

Note that the eprom upgrade mechanism will re-attempt the FTP connection several times after the first alarm appears. Therefore, any attempt to unblock the FTP interface as soon as possible is useful.

7006 0006

Component	Severity	Status
Nmis Fmip	major	message

Details

Nine consecutive invalid login attempts have been made to establish an FMIP session.

This is probably caused by a Preside Multiservice Data Manager workstation that is continuously trying to establish a session with an invalid userid/password. This slows down response time considerably on the switch. The IP address of the node trying the login and userid for the last failed attempt are shown in the comments field.

Probable Cause

Authentication failure

Type

Security

Remedial action

Identify and stop the source attempting the continuous login. The IP address included in the alarm's comment field and the userid will help.

7006 0007

Component	Severity	Status
Nmis <type> Session/<n>	major	message

Legend

<type> = Telnet, Fmip or Ftp

<n> = session number

Details

An NMIS session is automatically terminated, generating this alarm, when the session is registered for a data stream (alarms, SCNs, logs, or debug) and the record could not be output within 1 min 30 s.The IP address of the remote host is indicated in the comment field.

Possible causes:

The Passport is isolated (no trunks connecting to it) and the connection not recovered within 1 min 30s.

The network is extremely congested, causing the writing of data to the network to take more than 1 min 30 s.

Probable Cause

Loss of Signal

Type

Communications

Remedial action

None.

7006 0008

Component	Severity	Status
Nmis <type>	major	message

Legend

<type> = Fmip

Details

This alarm is issued if a corrupted message is sent to NMIS, causing the session to terminate. It is possible to identify the node whose connection failed from the IP address shown in the comment field.

Probable Cause

Loss of Signal

Type

Communications

Remedial action

None.

7006 0009

Component	Severity	Status
Ac	warning	message

Details

This alarm notifies the system that an authentication attempt for a userID was successful using a centralized database with RADIUS, but the userID was not permitted to start a Passport session. This occurs because the Role VSA (vendor-specific attribute) in the Access-Accept PDU sent from the RADIUS server does not exist as an instance of *Ac Role/<string>* on this Passport. The role name is shown in the comment text of the PDU.

Note that Passport expects either a correct role name or a set of 7 privileges from the RADIUS server. If the role is not provisioned on Passport but all 7 privileges do come from the RADIUS server, Passport uses the 7 privileges and does not raise this alarm.

Probable Cause

Configuration error, unauthorized access, corrupt data

Type

Security, communications

Remedial action

Check the role name against the userID on the RADIUS server. Make sure it is spelled correctly on both the RADIUS server and in Passport provisioning.

7006 0100

Component	Severity	Status
Ac Radius	critical	set/clear

Details

This alarm occurs when attempts to authenticate with all RADIUS servers have failed (by time-outs). Authentication must be possible using RADIUS. A *clear* is issued when an attempt to authenticate with at least one RADIUS server has succeeded.

Probable Cause

Loss of Signal, authentication failure, configuration error

Type

Security

Remedial action

Verify IP connectivity is possible from the Passport to the RADIUS server(s). This can be done using the Ping command from the Passport and from the server.

If connectivity is stable, determine the average times and ensure that the value of attribute *Ac Radius timeOut* is not set to time-out too soon.

Verify the RADIUS server(s) with which the Passport authenticates are operational.

Verify there are no network congestion issues.

Use a backup userID and password to access the Passport to troubleshoot.

7006 0101

Component	Severity	Status
Ac Radius Server/<n>	major	message

Legend

<n> = 0 - 1

Details

This alarm notifies the system that an attempt to authenticate with the specified RADIUS server has timed out.

The IP addresses of the servers with which you attempted to authenticate are shown in the comment text.

Probable Cause

Loss of Signal, authentication failure, configuration error

Type

Security

Remedial action

Verify IP connectivity is possible from the Passport to the RADIUS server. This can be done using the Ping command from the Passport and from the server.

If connectivity is stable, determine the average times and ensure that the value of attribute *Ac Radius timeOut* is not set to time-out too soon.

Verify the RADIUS server with which the Passport authenticates is operational.

7006 0102

Component	Severity	Status
Ac Radius Server/<n>	major	message

Legend

<n> = 0 - 1

Details

This alarm notifies the system that an authentication attempt for a userID was successful with a centralized database using RADIUS. However the Access-Accept PDU sent from the RADIUS server is missing required access permissions that authorize the userID to start a session.

Probable Cause

Authentication error, configuration error, unauthorized access

Type

Security

Remedial action

Verify the userID on the RADIUS server is configured to send back the required access permissions in the Vendor Specific Attributes upon successful authentication.

Verify the RADIUS server is retrieving the access permissions correctly from the database.

Verify there are seven attributes being sent back to the Passport.

7006 0103

Component	Severity	Status
Ac Radius	major	message

Details

This alarm notifies the system that a RADIUS PDU is received with an IP address that does not match a RADIUS server that is currently provisioned.

The IP address of the server in question is shown in the comment text.

Probable Cause

Configuration error, intrusion detection

Type

Security

Remedial action

Verify the IP address in the alarm is the address of the RADIUS server.

Verify the attribute *Ac Radius Server serverIpAddress* is provisioned correctly with a RADIUS server that exists.

Verify the IP address is not from an intruder.

7006 0104

Component	Severity	Status
Ac Radius	major	message

Details

This alarm notifies the system that an unsupported RADIUS PDU has been received. The supported types are Access-Accept and Access-Reject.

The known types of RADIUS PDUs that could be received are Access-Request, Access-Challenge, Accounting-Request, and Accounting-Response.

Probable Cause

Configuration error, intrusion detection

Type

Security

Remedial action

Verify the RADIUS server with which the Passport authenticates is configured correctly.

Verify the IP address provisioned on the Passport is unique and is not being used as a RADIUS server address by another NAS device.

Verify an intruder is not sending the Passport packets to the port 1812 or 1645.

7006 0105

Component	Severity	Status
Ac Radius Server/<n>	major	message

Legend
<n> = 0 - 1

Details
This alarm notifies the system that a RADIUS PDU was received unexpectedly. There is no matching authentication request for this RADIUS PDU.

Probable Cause
Configuration error, intrusion detection

Type
Security

Remedial action
Verify the RADIUS server is not sending more than one RADIUS PDU.

Verify RADIUS PDUs are not being accidentally routed to the Passport.

7007 0000

Component	Severity	Status
FrAtm/<instance>	minor/cleared	set/clear

Legend

<instance> = a decimal value

Details

This alarm is issued if there is a DLCI in a troubled condition under the FrAtm Interface. A troubled condition exists when there is not enough bandwidth available for a DLCI on a FrAtm interface. This condition must be cleared before a connection can be enabled. The alarm is set only once when the initial DLCI on the interface experiences this troubled condition.

The alarm is cleared when all the DLCIs on the interface are no longer in a troubled condition.

Probable Cause

Type

Remedial action

Determine amount of bandwidth and the bandwidth pool that is being requested by the connection by displaying the *equivalentBitRate* and *assignedBandwidthPool* attributes respectively, under the interworking function. Ensure there is sufficient bandwidth to accommodate the request by displaying the Connection Administrator (CA).

Increase the percentage of bandwidth allocated in the bandwidth pool used by the troubled DLCI.

If CAC is not required, then it can be turned off.

7007 1000

Component	Severity	Status
<FrameRelay>/<instance> LMI	critical/cleared	set/clear

Legend

<FrameRelay> = FrUni, FrNni, FrMux, or FrAtm

<instance> = a decimal value

Details

This alarm is *set* when the number of frame relay Local Management Interface (LMI) procedure errors within the last *eventCount* events has exceeded the *errorEventThreshold* attribute. (Both the *eventCount* and *errorEventThreshold* attributes are provisionable.) In this situation, the local interface is declared insane. For *FrUni*, *FrNni* and *FrAtm* components, both the local and remote user equipment are signalled by the LMI asynchronous status report message if asynchronous notification is supported at their local interface. For the *FrMux* component, all local Applications are signalled. Data transfer for all connections associated with the local DLCIs is suspended.

A *clear* is issued after a fixed number (provisioning parameter) of correct message exchanges between the inter-operating LMI entities has occurred. Data transfer for all connections associated with the local DLCIs is resumed.

Probable Cause

Type

Remedial action

Verify that the other side of the interface has the LMI protocol enabled. Verify that the LMI parameters set on the other side are compatible with those on this side. Turn off the LMI protocol if the other side does not support the LMI protocol.

7007 2000

Component	Severity	Status
<FrameRelay>/<instance> LMI	warning	message

Legend

<x> = a decimal digit (0 to 9)

<FrameRelay> = FrUni or FrNni

<instance> = a decimal value

Details

This alarm occurs when the frame relay Local Management Interface (LMI) receives a report from an adjacent network that a PVC(s) has become inactive.

The PVCs that are reported inactive by the adjacent network are listed in decimal format by DLCI value as part of the comment for this alarm. Each 7007 200x alarm reports a maximum of 112 PVCs. If more than 112 PVCs on a single component become inactive, multiple 7007 200x alarms are issued. The value ‘x’ has an initial value of ‘0’ and is incremented by one for each alarm. FrUni or FrNni components only generate this alarm when the LMI *pvcAlarmsReporting* attribute is set to *external* or *both*. The default value for the *pvcAlarmsReporting* attribute is *external*.

Probable Cause

Type

Remedial action

Check the PVC connection associated with the DLCI value reported in the warning message.

7007 2010

Component	Severity	Status
<FrameRelay>/<instance> LMI	warning	message

Legend

<x> = a decimal digit (0 to 9)

<FrameRelay> = FrUni or FrNni

<instance> = a decimal value

Details

This alarm occurs when the frame relay Local Management Interface (LMI) receives a report from an adjacent network that a PVC(s) has become active.

The PVCs that are reported active by the adjacent network are listed in decimal format by DLCI value as part of the comment for this alarm. Each 7007 201x alarm reports a maximum of 112 PVCs. If more than 112 PVCs on a single component become active, multiple 7007 201x alarms are issued. The value ‘x’ has an initial value of ‘0’ and is incremented by one for each alarm. FrUni or FrNni components only generate this alarm when the LMI *pvcAlarmsReporting* attribute is set to *external* or *both*. The default value for the *pvcAlarmsReporting* attribute is *external*.

Probable Cause

Type

Remedial action

None.

7007 2020

Component	Severity	Status
<FrameRelay>/<instance> LMI	warning	message

Legend

<x> = a decimal digit (0 to 9)

<FrameRelay> = FrUni or FrNni

<instance> = a decimal value

Details

This alarm occurs when the frame relay Local Management Interface (LMI) reports that a PVC(s) in the local network has become inactive.

The PVCs that are reported inactive in the local network are listed in decimal format by DLCI value as part of the comment for this alarm. Each 7007 202x alarm reports a maximum of 112 PVCs. If more than 112 PVCs on a single component become inactive, multiple 7007 202x alarms are issued. The value ‘x’ has an initial value of ‘0’ and is incremented by one for each alarm. FrUni or FrNni components only generate this alarm when the LMI *pvcAlarmsReporting* attribute is set to *internal* or *both*. The default value for the *pvcAlarmsReporting* attribute is *external*.

Probable Cause

Type

Remedial action

Check both ends of the PVC connection associated with the DLCI value reported in the warning message in the local network.

7007 2030

Component	Severity	Status
<FrameRelay>/<instance> LMI	warning	message

Legend

<x> = a decimal digit (0 to 9)

<FrameRelay> = FrUni or FrNni

<instance> = a decimal value

Details

This alarm occurs when the frame relay Local Management Interface (LMI) reports that a PVC(s) in the local network has become active.

The PVCs that are reported active in the local network are listed in decimal format by DLCI value as part of the comment for this alarm. Each 7007 203x alarm reports a maximum of 112 PVCs. If more than 112 PVCs on a single component become active, multiple 7007 203x alarms are issued. The value ‘x’ has an initial value of ‘0’ and is incremented by one for each alarm. FrUni or FrNni components only generate this alarm when the LMI *pvcAlarmsReporting* attribute is set to *internal* or *both*. The default value for the *pvcAlarmsReporting* attribute is *external*.

Probable Cause

Type

Remedial action

None.

7007 2100

Component	Severity	Status
FrNni/<instance>	minor	message

Legend

<instance> = a decimal value

Details

This alarm is issued at the Frame Relay NNI after two attempts to send a RESTART message to the adjacent Frame Relay NNI fail to result in a response with a RESTART ACKNOWLEDGE message.

A restart request is sent out under certain conditions. This alarm is required for the interface to realize that attempts to synchronize the adjacent NNI have not been acknowledged. In compliance with procedures for restarts defined in the X.76 standard, the sender of the restart request can consider its interface available for use at this point. However, since no response indicates a possible lack of synchronization between the two adjacent NNIs, this warning is provided.

Probable Cause

Type

Remedial action

Ensure that all switched DLCIs on the adjacent Frame Relay NNI are released.

7007 2101

Component	Severity	Status
FrNni/<instance>	minor	message

Legend

<instance> = a decimal value

Details

This alarm is issued when the Frame Relay NNI is being requested to restart. Since a RESTART message can be received at any time, this alarm notifies the user that the FR NNI is being requested to restart by the adjacent Frame Relay NNI.

Probable Cause

Type

Remedial action

No action required.

7007 2102

Component	Severity	Status
FrNni/<instance>	warning	message

Legend

<instance> = a decimal value

Details

This alarm is issued when the Frame Relay NNI is being restarted. This alarm notifies the user that the FR NNI is being restarted after receiving a RESTART ACKNOWLEDGE message from the adjacent Frame Relay NNI, in response to its RESTART message. This alarm also indicates completion of the restart procedure.

Probable Cause

Type

Remedial action

No action required.

7007 2103

Component	Severity	Status
FrNni/<instance>	minor	message

Legend

<instance> = a decimal value

Details

This alarm is issued as a warning that the T317 timer has expired without the Frame Relay NNI receiving indication that the internal clearing has been completed. Timer T317 is started when the FR NNI receives a RESTART message from the adjacent FR NNI, and it enters the Restart state. The indication of the internal clearing prompts the FR NNI to stop the T317 timer and send a RESTART ACKNOWLEDGE message to the adjacent FR NNI, thereby completing the restart procedure.

Probable Cause

Type

Remedial action

No action required.

7007 2104

Component	Severity	Status
FrNni/<instance>	minor	message

Legend

<instance> = a decimal value

Details

This alarm is issued as a warning to indicate that a configured mismatch in the DLCI range of adjacent Frame Relay NNIs could be the cause of calls being rejected. This alarm indicates that the DLCI ranges on adjacent FR NNIs have not been set according to the recommendations defined in the Passport Frame Relay NNI Switched Connection configuration procedures.

Probable Cause

Type

Remedial action

Ensure that the *highestPvcDlci* attribute (under the *FrNni Sig* component) on adjacent FR NNIs is set to the same value. Furthermore, ensure that the DLCI allocation strategies on adjacent NNIs are opposite. If one NNI is set to allocate switched DLCIs from lowest-to-highest, its adjacent NNI must be configured to allocate switched DLCIs from highest-to-lowest.

7007 2200

Component	Severity	Status
FrUni/<n> BnxProtocol FrNni/<n> BnxProtocol	major/cleared	set/clear

Legend

<n> = instance of FrUni or FrNni

Details

The status is *set* when a FrUni/FrNni fails registration with the frame relay IP server (FRIP) because its associated IP address is already registered on that FRIP. The correct configuration is that each *BnxProtocol* component linked to a FRIP has a unique IP address under that FRIP.

A *clear* is issued when the operator redefines the IP addresses so that they are unique and activates the configuration view.

Remedial action

For all *BnxProtocol* components linked to the same FrIpServer, verify that each *ipAddress* attribute defines a unique IP address.

7007 3000

Component	Severity	Status
<FrameRelay>/<instance>	minor	message

Legend

<FrameRelay> = FrUni or FrNni or FrMux or FrAtm

<instance> = a decimal value

Details

This alarm is issued when the Frame Relay service fails to add a provisioned data link connection identifier (DLCI) subcomponent. This may happen when the total number of provisioned DLCIs has exceeded the engineering limit, and the Frame Relay service cannot allocate the resources required. The Frame Relay service itself does not explicitly check for whether the engineering limit has been exceeded.

Probable Cause

Type

Remedial action

Re-engineer the function processor (FP) by moving the affected Frame Relay service to another access line and copy over the required DLCIs again. If the problem persists contact Nortel Networks global support.

7007 3001

Component	Severity	Status
<FrameRelay>/<instance>	minor	message

Legend

<FrameRelay> = FrMux

<instance> = a decimal value

Details

This alarm occurs when the aggregated CIRs of current registered DLCIs are greater than link speed.

Probable Cause

Type

Remedial action

If running in oversubscribing mode is done on purpose, then no remedial action is needed. In this case, however, the user should be aware that effective throughput of any DLCI may be lower than the provisioned CIR.

Otherwise, re-configure the FP so as to avoid oversubscription.

7007 4000

Component	Severity	Status
<FrameRelay>/<instance> <Signaling>	critical/cleared	set/clear

Legend

<FrameRelay> = FrUni or Mpanl

<instance> = a decimal value

<Signaling> = Sig, or when <FrameRelay> = Mpanl, SigMpanl

Details

This alarm is *set* if the Frame Relay Switched Virtual Circuit (SVC) data link layer is down and cannot be used for SVC signalling, or if MPANL data link layer is down and cannot be used for MPANL signalling. If the port is enabled and the Frame Relay or MPANL service is not locked it will attempt to bring up the SVC data link layer continually.

A *clear* is issued if the data link layer returns to state informationTransfer, where it is again ready to process SVC or MPANL signalling.

Probable Cause

Type

Remedial action

Verify that the cabling to the port is correct. Verify that the Frame Relay or MPANL service and the port are both unlocked and enabled. Verify that the connected device is operating correctly.

7007 4001

Component	Severity	Status
<FrameRelay>/<instance> <Signaling>	major	message

Legend

<FrameRelay> = FrUni or Mpanl

<instance> = a decimal value

<Signaling> = Sig, or when <FrameRelay> = Mpanl, SigMpanl

Details

This alarm is issued if the length of the transmit queue at the Frame Relay Switched Virtual Circuit (SVC) or MPANL data link layer has exceeded the queue length threshold. The queue is purged.

Probable Cause

Type

Remedial action

The access data rate for the Frame Relay or MPANL service may not be high enough to support the Frame Relay traffic from the network as well as the SVC or MPANL signalling traffic. Verify whether there is congestion for traffic going to the port. Traffic re-engineering may be necessary if this alarm is issued frequently.

7007 4002

Component	Severity	Status
<FrameRelay>/<instance> <Signaling>	minor	message

Legend

<FrameRelay> = FrUni or SigMpanl

<instance> = a decimal value

<Signaling> = Sig, or when <FrameRelay> = Mpanl, SigMpanl

Details

This alarm is issued if one or more unacknowledged Frame Relay Switched Virtual Circuit (SVC) or MPANL signalling frames have been purged because the data link layer was reset by either the network or the user side. The reason for a user side link reset is because an unnumbered acknowledgment (UA) frame has been received in state linkSetup, a set asynchronous balanced mode extended (SABME) frame has been received in state informationTransfer or state waitingAck, or a frame reject frame (FRMR) has been received. The reason for a network side link reset is because of invalid receive sequence number (NR) received or invalid frame received in state informationTransfer.

This alarm is not issue after a link reset if there has been no loss of SVC signalling frames.

Probable Cause

Type

Remedial action

Frequent issuance of this alarm indicates a possible configuration error. Verify the data link layer parameters (the timers in particular) at both sides of the interface.

7007 5000

Component	Severity	Status
<FrameRelay>/<instance> Dlci/<instance>	warning	set/clear

Legend

<FrameRelay> = FrUni, FrNni, or Mpanl

<instance> = a decimal value

Details

This alarm is issued when the Data Link Connection Identifier (DLCI) is set to Data Loopback state by an operator command issued on the *loopBack* subcomponent of the DLCI. When the DLCI is in this state, traffic sent over this DLCI is looped back to its source. This state is used for test purposes only: to test PVC/SVC connectivity, pre-installation, and load testing. The DLCI must not be expected to support live production traffic in this state.

This alarm is cleared when the DLCI is out of Data Loopback state, by an operator command issued on the *loopBack* subcomponent of the DLCI. Traffic over this DLCI is now sent as normal.

Probable Cause

Type

Remedial action

No action needed. The alarm simply provides a tracking mechanism, to allow network operators know what DLCI's are currently in Data Loopback state.

7007 5100

Component	Severity	Status
FrAtm/<instance> Dlci/<instance> Niwf	warning	message

Legend

<instance> = a decimal value

Details

This alarm is issued when a subconnection is cleared by the Multiservice cut-through switching because the requested DLCI is already in use.

Probable Cause

Type

Remedial action

Change the provisioning to remove the duplicate use of the DLCI. To determine what access component is using the DLCI, display the *accessConnectionComponent* attribute under *Mcs frf5Group/<instance> EndPoint <instance> DLCI/<instance>* component.

7007 5101

Component	Severity	Status
FrAtm/<instance> Dlci/<instance> Siwf	warning	message

Legend

<instance> = a decimal value

Details

This alarm is issued when a Master end receives a setup message from another Master. *FrAtm/<instance> Dlci/<instance> Siwf SPvc* is provisioned at both ends of the intended connection.

Probable cause

Type

Remedial action

One end must be provisioned as *FrAtm/<instance> Dlci/<instance> Siwf SPvc* which makes that end the Master end. The remote end for this connection must be provisioned as *FrAtm/<instance> Dlci/<instance> Siwf*. This makes this end of the connection the Slave end.

7007 5102

Component	Severity	Status
FrAtm/<instance> Dlci/<instance> Siwf	minor	message

Legend

<instance> = a decimal value

Details

This alarm is issued when quality of service parameters being negotiated do not match the called end of a FR-ATM connection. There may be an unexpected quality of service behavior observed.

Probable Cause

Type

Remedial action

Check quality of service parameters on both sides of the FR-ATM connection under the interworking function and verify that they are equivalent. If there is a discrepancy, ensure that the connection is obtaining the correct provisioned values.

7007 5103

Component	Severity	Status
FrAtm/<instance> Dlci/<instance> Siwf	minor	message

Legend

<instance> = a decimal value

Details

This alarm is issued when an originating call is trying to establish a connection and fails due to a busy condition (connection already enabled and being used).

Probable Cause

Type

Remedial action

Check your FR-ATM connections to ensure that the correct values have been provisioned for the *remoteAddress* and *remoteConnectionIdentifier* attributes at the originating end. Choose a *remoteConnectionIdentifier* value (DLCI) that is not being used.

7007 5200

Component	Severity	Status
<FrameRelay>/<instance> Dlci/<instance>	warning	message

Legend

<FrameRelay> = FrUni, FrNni, or FrAtm

<instance> = a decimal value

Details

This alarm is issued when the Data Link Connection Identifier (DLCI) fails to enable due to underlying hardware resources being unavailable following an Unlock command.

The DLCI should return to the following OsiState:

adminState = locked
operationalState = disabled
usageState = idle
availabilityStatus = failed

Probable Cause

The logical processor (Lp) is over-engineered (maximum supported DLCIs exceeded).

Type

Engineering

Remedial action

Delete one or more DLCIs from any frame relay interface that is provisioned on the logical processor and unlock the troubled DLCI.

For more information, refer to the troubleshooting section of NTP 241-5701-901, Frame Relay Fundamentals.

7007 6000

Component	Severity	Status
<FrameRelay>/<instance>	warning	message

Legend

<FrameRelay> = FrMux

<instance> = a decimal value

Details

This alarm occurs when FrMux Local Management Interface (LMI) receives a report from the Third Party Frame Relay network indicating a new PVC has been added for which no application is provisioned. The Dlci value for this new PVC is indicated in decimal format as part of the comment for this alarm.

Probable Cause

Type

Remedial action

Check the PVC connection indicated in this alarm in the Third Party Frame Relay network connected to the FrMux that raised this alarm.

7007 7001

Component	Severity	Status
Mpanl/<instance> VoFr	warning	message

Legend

<instance> = a decimal value

Details

This alarm is issued when the MPA signals an out of bounds maximum VoFr frame size and it is substituted by the closest valid limit value. Signalled and substituted values appear in comment text.

Probable Cause

Type

Remedial action

The alarm is likely indicative of incorrect provisioning on MPA. Correct the provisioning and activate the Mpanl.

7007 7002

Component	Severity	Status
Mpanl/<instance> VoFr	warning	message

Legend

<instance> = a decimal value

Details

This alarm is issued when the MPA signals an out of bounds receive bandwidth, and it is substituted by the closest valid limit value. Signalled and substituted values appear in comment text.

Probable Cause

Type

Remedial action

The alarm is likely indicative of incorrect provisioning on MPA. Correct the provisioning and activate the Mpanl.

7007 8000

Component	Severity	Status
Mpanl/<instance> SigMpanl	minor	set/clear

Legend

<instance> = a decimal value

Details

This alarm is *set* when the MPANL service has not received any Profile Association command from MPA since the LAPF layer on DLCI-16 has been established. Default values shall be assumed for this interface, and Q.933 calls are allowed to proceed. A *clear* is issued when the Profile Association command is received from MPA.

This *set* alarm may also be indicative that a prefix DNA previously issued from the MPA has been deregistered by the Passport MPANL service, resulting no Q.933 calls to arrive at the MPA.

Probable Cause

Type

Remedial action

The alarm is probably indicative that there are software problems with the attached MPA. If MPA is operating at a software level of deployment quality, then a scope trace may be needed to ascertain that a syntactically well-formatted Profile Association command has actually been initiated by MPA.

7007 8001

Component	Severity	Status
Mpanl/<instance> SigMpanl	warning	message

Legend

<instance> = a decimal value

Details

This alarm is issued when the MPANL service is unsuccessful in its attempt to deregister its prefix DNA with the FDCR agent.

Probable Cause

Type

Remedial action

This alarm indicates that there may be a memory/engineering issue since heap was not available to deregister the prefix DNA.

7007 8002

Component	Severity	Status
Mpanl/<instance> SigMpanl	warning	message

Legend

<instance> = a decimal value

Details

This alarm indicates that the MPA has attempted to associate a prefix DNA after having already successfully associated and registered a prefix DNA previously.

Probable Cause

Type

Remedial action

The MPA must first de-associate its registered prefix DNA before attempting to associate an alternate prefix DNA.

7007 8003

Component	Severity	Status
Mpanl/<instance> SigMpanl	warning	message

Legend

<instance> = a decimal value

Details

This alarm indicates that the MPA has attempted to associate a prefix DNA that is too long or too short (that is, greater than 15 digits, or with no digits). No prefix DNA will be registered.

Probable Cause

Type

Remedial action

The MPA must send a prefix DNA association command, with a prefix DNA having at least one digit but no more than 14 digits long.

7007 8100

Component	Severity	Status
Mpanl/<instance> Sig	minor	message

Legend

<instance> = 1 - 65535

Details

This alarm is issued at the Mpanl after two attempts to send a RESTART message to the adjacent Passport 4400 fail to result in a response with a RESTART ACKNOWLEDGE message.

A restart request is sent out under certain circumstances. This alarm is required for the interface to realize that attempts to synchronize the adjacent MPA have not been acknowledged. In compliance with procedures for restarts defined in the X.76 standard, the sender of the restart request can consider its interface available for use at this point. However, since no response indicates a possible lack of synchronization between the two Passports, this warning is provided.

Probable Cause

Type

Remedial action

Ensure that all switched DLCIs on the adjacent Passport 4400 are released.

7007 8101

Component	Severity	Status
Mpanl/<instance> Sig	minor	message

Legend

<instance> = 1 - 65535

Details

This alarm is issued when the Mpanl is being requested to restart. Since a RESTART message can be received at any time, this alarm notifies the user that the Mpanl is being requested to restart by the adjacent MPA.

Probable Cause

Type

Remedial action

No action required.

7007 8102

Component	Severity	Status
Mpanl/<instance> Sig	minor	message

Legend

<instance> = 1 - 65535

Details

This alarm is issued when the Mpanl is being restarted. The alarm notifies the user that the Mpanl is being restarted after receiving a RESTART ACKNOWLEDGE message from the adjacent MPA in response to its RESTART message. This alarm also indicates completion of the restart procedure.

Probable Cause

Type

Remedial action

No action required.

7007 8103

Component	Severity	Status
Mpanl/<instance> Sig	minor	message

Legend

<instance> = 1 - 65535

Details

This alarm is issued as a warning that the T317 timer has expired without the Mpanl receiving indication that the internal clearing has completed. Timer T317 is started when the Mpanl receives a RESTART message from the adjacent MPA; the Mpanl then enters the restart state. The indication of the internal clearing prompts the Mpanl to stop the T317 timer and send a RESTART ACKNOWLEDGE message to the adjacent MPA, thereby completing the restart procedure.

Probable Cause

Type

Remedial action

No action required.

7008 1001

Component	Severity	Status
Fs	major/cleared	set/clear

Details

The file system disk space usage is above 85% of its total capacity.

A *clear* is issued when the used space is below 75% of the disk capacity.

Probable Cause

Storage capacity problem

Type

Processing

Remedial action

Remove some files from the disk immediately to prevent the file system from becoming full to avoid the risk of lost data. The active disk must be cleaned up immediately by doing one or more of the following:

- tidy the provisioning data

- tidy the software files

- off-load spooled data

7008 1002

Component	Severity	Status
Fs	critical/cleared	set/clear

Details
The file system disk is 100% full. This causes service to be affected.

A *clear* is issued when the disk space usage is below 90% of the total disk capacity.

Probable Cause
Storage Capacity

Type
Processing

Remedial action
Clean up the active disk immediately by doing one or more of the following:

- tidy the provisioning data

- tidy the software files

- off-load spooled data

7008 1003

Component	Severity	Status
Fs	major	message

Details

The root directory "/" is full. The number of directories or files in the root directory "/" has reached the maximum allowed (112 files and directories).

Probable Cause

Storage capacity problem

Type

Processing

Remedial action

Remove some files or directories in the root directory. Nortel Networks recommends that files be placed in subdirectories rather than in the root directory (The root directory should only contain directories).

7008 1004

Component	Severity	Status
Fs	critical/cleared	set/clear

Details

The file system is disabled and therefore cannot be accessed. This alarm will be cleared when the file system is accessible again. However, this is not likely to happen until the control processor card is reset.

Probable Cause

IO device error

Type

Equipment

Remedial action

Reset the active control processor card. This action is service-affecting if there is only one CP on the shelf. The action must be done with caution. If the problem persists, return the card to the manufacturer. The most likely cause is a bad disk.

7008 1005

Component	Severity	Status
Fs	minor/cleared	set/clear

Details

The synchronization of the standby disk to the active disk has failed. Among the possible causes are:

- the disks have different volume names

- there is insufficient standby disk capacity

- the standby disk is locked or disabled

A *clear* is issued when the synchronization succeeds.

Probable Cause

Processor problem

Type

Equipment

Remedial action

Display the disk attributes and check if the volume names are the same. If they differ re-synchronize the two disks manually.

If the standby disk is locked, unlock it and re-synchronize manually.

If the standby disk is disabled, reset the standby card.

If the standby disk capacity is less than the used disk space on the active disk, you may have to remove files on the active disk by issuing a *tidy prov* or a *tidy sw* command or alternatively you may have to upgrade your control processor with a larger disk.

7008 1006

Component	Severity	Status
Fs	major/cleared	set/clear

Details
The file system has too many open files.

Probable Cause
Storage capacity problem

Type
Processing

Remedial action
Contact Nortel Networks global support.

7008 1008

Component	Severity	Status
Fs Disk/<instance>	major/cleared	set/clear

Legend

For Passport 15000 and 20000:
<instance> = 0, 1

For Passport 7400:
<instance> = 0, 15

Details

A read/write has error occurred on the active disk causing the disk to become unavailable. If the system has a synchronized standby control processor (CP), the faulty disk will have its CP rebooted.

Probable Cause

Equipment malfunction

Type

Equipment

Remedial action

No action required.

If this error occurs frequently, run the disk tests on the faulty disk. See 241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing* for a description of possible disk tests.

7008 1009

Component	Severity	Status
Fs Disk/<instance>	major/cleared	set/clear

Legend

For Passport 15000 and 20000:
<instance> = 0, 1

For Passport 7400:
<instance> = 0, 15

Details

A disk media error test has found a read/write error in the disk boot area.

A *clear* is issued when the disk is replaced.

Probable Cause

Equipment malfunction

Type

Equipment

Remedial action

Return the card to the manufacturer.

7008 1010

Component	Severity	Status
Fs Disk/<instance>	major/cleared	set/clear

Legend

For Passport 15000 and 20000:
<instance> = 0, 1

For Passport 7400:
<instance> = 0, 15

Details

A disk surface analysis test has found bad clusters. They were re-mapped and the volume has been re-initialized. This alarm clears after resetting the card.

Probable Cause

Equipment malfunction

Type

Equipment

Remedial action

Reset the card. If the problem persists return the card to the manufacturer.

7008 1011

Component	Severity	Status
Fs Disk/<instance>	major/cleared	set/clear

Legend

For Passport 15000 and 20000:
<instance> = 0, 1

For Passport 7400:
<instance> = 0, 15

Details

A disk media test has found errors.

A *clear* is issued when the disk is fixed.

Probable Cause

Equipment malfunction

Type

Equipment

Remedial action

No action required.

If this error occurs frequently, run the disk tests on the faulty disk. See 241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing* for a description of possible disk tests.

7008 1012

Component	Severity	Status
Fs Disk/<instance>	warning	message

Legend

For Passport 15000 and 20000:
<instance> = 0, 1

For Passport 7400:
<instance> = 0, 15

Details

The file system check test has found some integrity errors and corrected them. No data is lost.

Probable Cause

Equipment malfunction

Type

Equipment

Remedial action

If the file system has a standby control processor, synchronize the file system immediately.

7008 1013

Component	Severity	Status
Fs Disk/<instance>	major	message

Legend

For Passport 15000 and 20000:
<instance> = 0, 1

For Passport 7400:
<instance> = 0, 15

Details

The *filesystemCheck test* has found some integrity errors and fixed them. Some data is lost.

Probable Cause

Equipment malfunction

Type

Equipment

Remedial action

If the file system has a standby control processor, synchronize the file system immediately.

7008 1014

Component	Severity	message
Fs Disk/<instance>	major	message

Legend

For Passport 15000 and 20000:
<instance> = 0, 1

For Passport 7400:
<instance> = 0, 15

Details

A disk test failed to complete and the cause is unknown.

Probable Cause

Unknown

Type

Unknown

Remedial action

Reset the card and run the test again. If the problem persists return the card to the manufacturer.

7008 1015

Component	Severity	Status
Fs Disk/<instance>	minor	message

Legend

For Passport 15000 and 20000:
<instance> = 0, 1

For Passport 7400:
<instance> = 0, 15

Details

An operation on the standby disk did not complete as expected. The standby control processor is rebooted and synchronizes automatically.

Probable Cause

Unknown

Type

Unknown

Remedial action

No action is required.

7008 1016

Component	Severity	Status
Fs Disk/<instance>	minor	message

Legend

For Passport 15000 and 20000:
<instance> = 0, 1

For Passport 7400:
<instance> = 0, 15

Details

A communication error has occurred between the active control processor and the standby control processor. The standby control processor is rebooted and synchronizes automatically.

Probable Cause

Unknown

Type

Unknown

Remedial action

No action is required. If the problem persists, contact Nortel Networks global support.

7008 1018

Component	Severity	Status
Fs Disk/<instance>	minor	message

Legend

For Passport 15000 and 20000:
<instance> = 0, 1

For Passport 7400:
<instance> = 0, 15

Details

The periodic disk access test has not received a response from the disk. The control processor with the failed disk is reset if it is in standby mode.

If the control processor is active, a recoverable software error is raised.

Probable Cause

Equipment or system busy

Type

Equipment

Remedial action

No action is required for the standby control processor.

For the active control processor, it needs to be manually reset if the disk problem persists.

7008 1019

Component	Severity	Status
Fs	minor/cleared	set/clear

Details

The File system is no longer synchronized for one of the following reasons:

- the standby disk is locked

- one disk is full

- the standby disk has been reset

- device can not be opened or closed

- controlling functions can not be performed on device

Probable Cause

Processor problem

Type

Equipment

Remedial action

Display the disk's attributes and check if the standby disk is locked. If it is locked, unlock it using the *unlock* command, and re-synchronize the software.

If the disk is full, clean up the disk by issuing a *tidy sw* (for software files) or a *tidy prov* command (for provisioning data) and re-synchronize.

If the standby disk resets, no action is required. The filesystem will re-synchronize automatically when the active disk becomes available.

If the device can not be opened or closed, it should be changed.

If the controlling functions can not be performed, contact Nortel Networks global support.

7008 1020

Component	Severity	Status
Fs	minor	message

Details

This alarm indicates that disk synchronization has failed due to heavy file system activity. The system will attempt to re-initiate disk synchronization automatically, to a maximum of 3 attempts. The alarm message also indicates the number of synchronization attempts made.

Probable Cause

Processor problem

Type

Equipment

Remedial action

If all three automatic synchronization attempts are unsuccessful, you must initiate disk synchronization manually.

7009 0202

Component	Severity	Status
Rtg Top	critical	message

Details

A neighbor node, in the host node's routing area, is provisioned with the same node identifier as the host node. The trunk between them will be automatically disabled. If this alarm occurs, it could indicate a problem with the trunk system, since this situation should be alarmed as 7005 0304.

Probable Cause

Type

Remedial action

Reprovision either this node's identifier or the node identifier of the remote node.

7009 0203

Component	Severity	Status
Rtg Top	warning	message

Details

This component has received a routing control packet from a neighbor node requesting a link state update for a node not in the host's topological database. The trunk will be automatically restaged and the databases re-synchronized.

Probable Cause

Type

Remedial action

No action required.

7009 0205

Component	Severity	Status
Rtg Top	warning	message

Details

The Passport network has reached the maximum number of nodes, which can be configured in a routing area.

No more nodes can be configured in this area.

Probable Cause

Type

Remedial action

No action is required.

7009 0208

Component	Severity	Status
Rtg Top	major	message

Details

The number of unique Logical Networks provisioned has exceeded the limit of 126 per network.

This alarm indicates that routing within some of the logical networks will not be reliable.

Probable Cause

Type

Remedial action

Remove Logical Networks until there are 126 or less in the network.

7009 0209

Component	Severity	Status
Rtg Top	major	message

Details

Another node which is using the same node id and/or the same node name has been detected in the network. This situation will lead to faulty routing and increased control traffic throughout the network.

Probable Cause

Type

Remedial action

Find the other node in the network with the same id and/or name, and change one of the two.

Note that this is easy to do if all nodes are running software with this alarm, since they will all be generating alarms for this condition.

7009 0210

Component	Severity	Status
Rtg Top	critical	message

Details

The host node detects that there have already been maximum number of Passport nodes in a network while more Passport nodes still try to join in the network. When this alarm is seen, the host node may not have the complete view of the network topology because the host node can only store maximum number of nodes in its topological database.

Probable Cause

Type

Remedial action

Contact Nortel Networks global support, the Passport software may needs to be upgraded.

7009 0211

Component	Severity	Status
Rtg Top	critical	message

Details

If a node has been staging with a neighbour for more than 10 minutes, the link group to the neighbour is brought down and an alarm is raised to indicate the situation.

Probable Cause

Type

Remedial action

If the problem persists, contact Nortel Networks global support.

7009 0212

Component	Severity	Status
Rtg Top	critical	message

Details

This alarm is issued when more than 65280 link groups with n number of PORS trunks (n = 0 to 4) are present in a topological region/cluster. When this situation occurs, the topology (Rtg Top) and transport resource manager (Trm) will probably become out of sync.

Probable Cause

Type

Remedial action

Reduce the number of link groups with n number of PORS trunks in the topological region/cluster.

7009 0301

Component	Severity	Status
Trm	indeterminate	message

Details

The transport resource manager (TRM) has detected the software error specified in the alarm text.

Probable Cause

Software error

Type

Processing

Remedial action

Contact Nortel Networks global support for frequent occurrences of this condition.

7009 0302

Component	Severity	Status
Trm	warning	message

Details

A trunk/gateway has been brought up which would exceed the capacity of Transport Resource. Up to 1023 trunks/gateways can be handled.

Probable Cause

Type

Remedial action

Remove a trunk/gateway running on an FP so that the total number that are present on active FPs is less than 1024.

7009 0303

Component	Severity	Status
Trm	warning	message

Details

A trunk/gateway has been brought up to a new neighbor module which would exceed the 255 neighbor modules limit.

Probable Cause

Type

Remedial action

Bring down a trunk/gateway to the new neighbor or an existing neighbor module so that the total number of neighbors is less than 256.

7009 0304

Component	Severity	Status
Trm	warning	message

Details

A trunk/gateway has been brought up which is the fifth link to an existing neighbor module. Four other links exist and are active to that neighbor. Up to 4 trunks or 4 gateways can belong to the same link group.

Probable Cause

Type

Remedial action

Disable the trunk/gateway. If this link is really desired in the link group, issue a ‘LIST trm lg <neighbor node name>’ to find out which links are in the link group. Disable one of them with the ‘LOCK’ command on the link component. Allow the new trunk/gateway to come up. It is possible to keep a fifth link in an unlocked state between two modules, but it will not be admitted to the link group and thus will not carry traffic. If an existing link in the link group then goes down, this idle link can be admitted.

7009 0305

Component	Severity	Status
Trm linkGroup/<m> link/<n>	minor/critical	set/clear

Legend

<m> = linkGroup/mnemonic

<n> = 1 - 1023

Details

If the status is *set*, the specified link in the link group is detected to be neither throughput nor delay preferred for loadsharing and the link is not 100% dedicated to pors.

A *clear* is issued when this link goes down or the link becomes preferred for loadsharing.

Probable Cause

Type

Remedial action

Engineering study is required to determine why the link is non-preferred, and whether it is appropriate to add the link in the link group.

7009 0306

Component	Severity	Status
Trm linkGroup/<m> link/<n>	minor/critical	set/clear

Legend

<m> = 1 - 255

<n> = 1 - 1023

Details

If the status is *set*, the specified link in the link group is detected to be neither throughput nor delay preferred for loadspreading and the link is not 100% dedicated to PORS.

A *clear* is issued when this link goes down or the link becomes preferred for loadspreading.

Probable Cause

Type

Remedial action

Engineering study is required to determine why the link is non-preferred, and whether it is appropriate to add the link in the link group.

7009 0307

Component	Severity	Status
Trm	warning	message

Details

This indicates a situation in which Transport Resource has received an LNN staging packet from an unknown neighbour node with the indicated node name.

Probable Cause

Type

Remedial action

This alarm occurs infrequently under normal conditions. The node will recovery automatically and the alarm should cease to occur. If these alarms start to occur frequently, contact Nortel Networks global support.

7009 0308

Component	Severity	Status
Trm	warning	message

Details

The TRM manager on the CP has reset the LP that is indicated in the message, because the TRM agent on the LP did not complete the recovery after a specific period of time.

Probable Cause

Timing problem

Type

Communications

Remedial action

No action is required if this condition occurs infrequently. Contact Nortel Networks global support for frequent occurrences of this condition on the same FP.

7009 0310

Component	Severity	Status
Trm	warning	set/clear

Details

In order for a Passport trunk to stage, the trmAgent process on the FP needs to register with the trmMaster process on the CP. This alarm is set when TRM Agent on the FP is not able to register with TRM Master on the CP even after 10 retries. This usually occurs during CP switchover when the CP is very busy.

A clear is issued after TRM Agent is able to register with TRM Master on the CP.

Probable Cause

Type

Remedial action

The alarm generally clears after some time. No action is required if the alarm status gets cleared.

7009 0311

Component	Severity	Status
Trm	warning/cleared	set/clear

Details

If the status is *set*, the routing system exchanges full topology information across the cluster link group detailed in the alarm text.

Probable Cause

The alarm is set on this cluster link group when this node and the far end node both have attribute *Rtg fullTopExchgOnClusterLinks* set to *enabled*.

Type

Operator

Remedial action

This alarm can be raised due to a temporary condition of clusters migration. It should only be seen during migration of backbone nodes to cluster nodes, and only on the planned cluster nodes. The alarm is cleared after the migration is complete.

To clear this alarm, check that attribute *Rtg fullTopExchgOnClusterLinks* is set to *disabled* on all nodes. This attribute should be set to *disabled* on all nodes unless they are planned cluster nodes undergoing clusters migration.

7009 0312

Component	Severity	Status
Trm	warning	message

Details

The transport resource manager (TRM) on a Passport cluster node has detected a link between the cluster node and another Passport node in a different RID. The link that connects these two nodes cannot carry DPRS traffic.

Probable Cause

Configuration or customization error

Type

Operator

Remedial action

No action is required. This condition can occur during a RID split/merge where Passport clusters are deployed.

7009 0401

Component	Severity	Status
Rtg Dpn	indeterminate	message

Details
The generic EAP manager has detected the software error specified in the alarm text.

Probable Cause
Software error

Type
Processing

Remedial action
Contact Nortel Networks global support for frequent occurrences of this condition.

7009 0402

Component	Severity	Status
Rtg Dpn	warning	message

Details

A new broadcast packet received from a neighbor, has an LRC error. This error may be due to transmission failures.

Probable Cause

Type

Remedial action

No action is required. Contact Nortel Networks global support only if this alarm appears frequently.

7009 0403

Component	Severity	Status
Rtg Dpn	warning	message

Details

Upon the reception of a broadcast packet from a neighbor module (containing Dpn control data), a shortage of shared memory was encountered. Dpn routing control data may be lost if this occurs.

Probable Cause

Type

Remedial action

No action is required if this occurs infrequently. Contact Nortel Networks global support only if other events also indicated that the control processor is inexplicably short of memory.

7009 0404

Component	Severity	Status
Rtg Dpn	warning	message

Details

A new broadcast packet received from a neighbor module has an age field that is zero. This indicates that there is a routing loop in the broadcast system. Such conditions can occur temporarily.

Probable Cause

Type

Remedial action

No action is required. Temporary looping may happen.

Contact Nortel Networks global support only if this alarm occurs frequently.

7009 0405

Component	Severity	Status
Rtg Dpn	major	message

Details

A broadcast packet received from a neighbor module originated from a node which has the same Node Id as this node. This alarm will also occur if a node receives a broadcast packet which it generated.

Probable Cause

Type

Remedial action

If the alarm occurs infrequently, and only when the network's topology has just changed (if a trunk has just come up or gone down, for example), then it can be ignored. If it occurs frequently, when the network topology is stable, then there may be duplicate node Ids provisioned in the network. In this case, reprovision one of the modules with a unique node Id.

7009 0406

Component	Severity	Status
Rtg Dpn	warning	message

Details

A new broadcast packet received from a neighbor, has a checksum error. This error may be due to transmission failures.

Probable Cause

Type

Remedial action

No action is required. Contact Nortel Networks global support only if this alarm appears frequently.

7009 0407

Component	Severity	Status
Rtg Dpn	warning	message

Details

A broadcast packet received from a neighbor is corrupted. This alarm is issued if the packet is too short or having a bad header length or data length value in the packet. This error may be due to transmission failures.

Probable Cause

Type

Remedial action

No action is required. Contact Nortel Networks global support only if this alarm appears frequently.

7009 0408

Component	Severity	Status
Rtg Dpn	major	message

Details

Broadcast packets for one or more data types have not been received for an extensive period of time from one or more nodes in the RID subnet. Those broadcasts were received before and contained data that are required for proper path calculations or call routing.

Probable Cause

Type

Remedial action

Contact Nortel Networks global support.

7009 0501

Component	Severity	Status
Rtg Dpn	indeterminate	message

Details
The RID/MID EAP manager has detected the software error specified in the alarm text.

Probable Cause
Software error

Type
Processing

Remedial action
Contact Nortel Networks global support for frequent occurrences of this condition.

7009 0502

Component	Severity	Status
Rtg Dpn	critical	message

Details

Broadcast data received from a neighbor module is originated from a node with a different RID value from this node.

Probable Cause

Type

Remedial action

Reprovision the module with the RID of the subnet.

7009 0503

Component	Severity	Status
Rtg Dpn	critical	message

Details

Broadcast data received from a neighbor module is originated from a node which has the same MID as this node.

Probable Cause

Type

Remedial action

Reprovision one of the two nodes sharing the same MID to use a unique MID.

7009 0504

Component	Severity	Status
Rtg Dpn	critical	message

Details

Broadcast data received from a neighbor module is originated from a node which has the same Node Id as this node.

Probable Cause

Type

Remedial action

Reprovision the module with a unique node Id.

7009 0505

Component	Severity	Status
Rtg Dpn	warning/cleared	set/clear

Details

Dpn external address plan (EAP) sets this alarm if it detects more than two call server resource modules (CSRM) RIDs in the subnet.

A *clear* is issued after recovering from the condition. The alarm lists the visible call server RIDs. Only the two lowest call server RIDs are used.

Probable Cause

Type

Remedial action

No action is required, but you may want to reprovision one or more of the call server RIDs to not support the subnet RID.

7009 0506

Component	Severity	Status
Rtg Dpn	major	message

Details

There can be a maximum of four nodes supporting gateways to any one MID. In other words, a cluster of access modules (AM) cannot connect to more than four different Passport nodes. If a fifth path through a different Passport node to a MID in such a cluster is detected, this alarm occurs. The alarm should list all nodes with connections to the cluster. Dpn Eap's view of the routes to the cluster may be inconsistent.

Probable Cause

Type

Remedial action

Disable one of the connections from the cluster to the subnet. If you disable the fifth connection no further action is required. If you disable one of the four connections that was originally up then you should also disable and re-enable the fifth connection again (to force it to be made visible to all Passport nodes once more).

7009 0507

Component	Severity	Status
Rtg Dpn	major	message

Details

A routing loop possibly exists in the network. A module in the network has issued a Ping command (Path for DPN equipment) and the Ping packet has travelled 20 hops. The alarm is issued on the 20th hop module. In the alarm comment, the list of modules that the Ping packet has travelled through is displayed.

Probable Cause

Type

Remedial action

No action is required. Temporary looping may happen.

Contact Nortel Networks global support only if there are no topology changes occurring when the command is issued and repeating the command produces the same results.

7009 0509

Component	Severity	Status
Rtg Dpn	major/cleared	set/clear

Details

The node now has a delay path but no throughput path or a throughput path but no delay path to the given RID(s).

The alarm is re-issued whenever the list of affected RIDs changes. Each new instance of the alarm supersedes the preceding instance. The alarm is cleared when the node has either both delay and throughput paths or neither delay nor throughput paths to each RID.

Probable Cause

Type

Remedial action

Adjust provisioned delay or throughput metric cutoff values in the subnet.

7009 0510

Component	Severity	Status
Rtg Dpn	warning	message

Details

An LRC error has been detected in a packet received by the DPN PPATH system. This error may be due to software error or due to trunk problems which have caused packets to be corrupted. Note that certain patterns of trunk packet corruption can cause any DPN packet to be incorrectly sent to the PPATH system.

Probable Cause

Type

Remedial action

Contact Nortel Networks global support only if it can be verified that the trunks are not causing the problem.

7009 0511

Component	Severity	Status
Rtg Dpn	warning	message

Details

MID broadcast received from a Passport node indicates that there is a Passport in the RID subnet that uses the MID of a dead AM. The substitute RID for this MID is removed (set to invalid).

Probable Cause

Operational condition

Type

Operator

Remedial action

No action is required. Contact Nortel Networks global support only if this alarm appears frequently for the same MID on a single Passport node.

7009 0601

Component	Severity	Status
Rtg Dpn	indeterminate	message

Details
The RID/MID RPI has detected the software error specified in the alarm text.

Probable Cause
Software error

Type
Processing

Remedial action
Contact Nortel Networks global support for frequent occurrences of this condition.

7009 0602

Component	Severity	Status
Rtg Dpn	warning	message

Details

The DPN routing protocol interface (Rpi) has received a routing packet with an LRC error from a neighbor DPN Gateway. This error may be due to transmission errors on links or due to software errors. The repeated occurrence of this alarm will cause the DPN routing system knowledge to be out of date with the actual network topology.

Probable Cause

Type

Remedial action

Contact Nortel Networks global support only if it can be verified that the link facilities are not causing the problem.

7009 0603

Component	Severity	Status
Rtg Dpn	major	message

Details

The RPI RID protocol has received a routing table update (RTU) from a resource module (RM) with invalid vintage value. The neighbor RM's RID is displayed in comment data.

Probable Cause

Type

Remedial action

Contact Nortel Networks global support if the neighbor RM is running the correct level of software.

7009 0604

Component	Severity	Status
Rtg Dpn	major	message

Details

The routing protocol interface (RPI) logical MID (LMID) protocol has received an LMID status packet with invalid vintage value.The neighbor RM's RID is displayed in comment data.

Probable Cause

Type

Remedial action

Contact Nortel Networks global support if the neighbor RM is running the correct level of software.

7009 0605

Component	Severity	Status
Rtg Dpn	major	message

Details

The routing protocol interface (RPI) MID protocol has received a MID routing table update (MRTU) with invalid vintage value. The neighbor MID is displayed in comment data.

Probable Cause

Type

Remedial action

Contact Nortel Networks global support if the neighbor AM is running the correct level of software.

7009 0606

Component	Severity	Status
Rtg Dpn	major	message

Details

The routing protocol interface (RPI) MID protocol has received a MID routing table update (MRTU) with invalid cluster type. The invalid cluster types are either one of RM cluster, AM cluster, or NM cluster.

Probable Cause

Type

Remedial action

Contact Nortel Networks global support.

7009 0607

Component	Severity	Status
Rtg Dpn	major	message

Details

The routing protocol interface (RPI) MID Broadcaster has exhausted the number of retries of MID broadcasting before the response packets from all MIDs are received. The non-responding MID(s) are displayed in comment data.

Probable Cause

Type

Remedial action

Contact Nortel Networks global support.

7009 0608

Component	Severity	Status
Rtg Dpn	indeterminate	message

Details

The routing protocol interface (RPI) had been waiting long enough and failed to receive routing table updates (RTUs) from its Passport neighbors in other subnets after the hitless CP switchover occurred. The non-responding Passport neighbor(s) are identified by RID/MID pairs and displayed in comment data. In order to let neighbor(s) send us RTUs, the link groups to the non-responding Passport neighbours are automatically taken down and brought up. Thereafter, along with this alarm, the set and clear of alarm 7005 0103 should be seen as well for each non-responding Passport neighbors.

Probable Cause

Type

Remedial action

Contact Nortel Networks global support if RPI is still not be able to receive RTUs from its Passport neighbors.

7009 0609

Component	Severity	Status
Rtg Dpn	warning	message

Details

The routing protocol interface (RPI) received corrupted routing table updates (RTUs) from its Passport neighbors in other RID subnets.

Probable Cause

Corrupt data

Type

Communications

Remedial action

No action is required. Contact Nortel Networks global support if this condition occurs frequently.

7009 0701

Component	Severity	Status
Rtg	indeterminate	message

Details

The Rtg routing table maintainer has detected the software error specified in the alarm text.

Probable Cause

Type

Remedial action

Contact Nortel Networks global support for frequent occurrences of this condition.

7009 0703

Component	Severity	Status
Rtg	minor	message

Details

The Rtg routing table manager has not received an acknowledgment to its last Rtg table update from the card specified in the alarm text. This error may be due to severe message block exhaustion on the CP and/or a fault with the card specified. The Rtg table manager will resynchronize the Rtg routing tables on the card with those of the CP.

Probable Cause

Type

Remedial action

Frequent occurrences of this condition indicate a system fault between the CP and card. Contact Nortel Networks global support only if it can be verified that a fault on either the CP and/or card is not causing the problem.

7009 0704

Component	Severity	Status
Rtg	major	message

Details

The Rtg routing table manager has detected a corruption in the Rtg routing table specified in the alarm text. The shelf may experience degraded congestion avoidance and/or routing performance. The fault may also manifest itself as a routing loop or, through a topology change, it may remedy itself.

Probable Cause

Type

Remedial action

Contact Nortel Networks global support.

7009 0705

Component	Severity	Status
Rtg	warning	message

Details

The Rtg routing table agent, specified in the alarm text, has detected an out of sequence routing table update received from the CP. This alarm will be accompanied by alarm 7009 0703. After which the Rtg table manager will resynchronize the Rtg routing tables on the card with those of the CP.

Probable Cause

Type

Remedial action

For frequent occurrences of this alarm contact Nortel Networks global support.

7009 0706

Component	Severity	Status
Rtg	warning	message

Details

The Rtg routing table agent, specified in the alarm text, has detected a corruption in the specified Rtg routing table. The card may experience degraded congestion avoidance and/or routing performance for up to 60 seconds. After which time, the Rtg routing table manager will resynchronize the card tables with those of the CP.

Probable Cause

Type

Remedial action

For frequent occurrences of this alarm contact Nortel Networks global support.

7009 0801

Component	Severity	Status
Rtg Dpn	indeterminate	message

Details

The DPN RID/MID System (Rms) routing table maintainer has detected the software error specified in the alarm text.

Probable Cause

Type

Remedial action

Contact Nortel Networks global support for frequent occurrences of this condition.

7009 0803

Component	Severity	Status
Rtg Dpn	minor	message

Details

The DPN RID/MID System (Rms) routing table manager has not received an acknowledgment to its last Rms table update from the specified card. This may be due to severe message block exhaustion on the CP and/or a fault with the card specified. The Rms table manager will resynchronize the Rms routing tables on the card with those of the CP.

Probable Cause

Type

Remedial action

Frequent occurrences of this condition indicate a system fault between the CP and card. Contact Nortel Networks global support only if it can be verified that a fault on either the CP and/or card is not causing the problem.

7009 0804

Component	Severity	Status
Rtg Dpn	major	message

Details

The DPN RID/MID System (Rms) routing table manager has detected a corruption in the Rms routing table specified in the alarm text. The shelf may experience degraded congestion avoidance and/or routing performance. The fault may also manifest itself as a routing loop or, through a topology change, it may remedy itself.

Probable Cause

Type

Remedial action

Contact Nortel Networks global support.

7009 0805

Component	Severity	Status
Rtg Dpn	warning	message

Details

The DPN RID/MID System (Rms) routing table agent, specified in the alarm text, has detected an out of sequence routing table update received from the CP. This alarm will be accompanied by alarm 7009 0803. After which the Rms table manager will resynchronize the Rms routing tables on the card with those of the CP.

Probable Cause

Type

Remedial action

For frequent occurrences of this alarm contact Nortel Networks global support.

7009 0806

Component	Severity	Status
Rtg Dpn	warning	message

Details

The DPN RID/MID System (Rms) routing table agent, specified in the alarm text, has detected a corruption in the specified Rms routing table. The card may experience degraded congestion avoidance and/or routing performance for up to 60 seconds. After which time, the Rms routing table manager will resynchronize the card tables with those of the CP.

Probable Cause

Type

Remedial action

For frequent occurrences of this alarm contact Nortel Networks global support.

7011 1100

Component	Severity	Status
For Passport 7400: Lp/<num1> Ima/<num2>	critical/cleared	set/clear
For Passport 15000 and 20000: Lp/<num1> DS3/<num3> Ima/<num4>		

Legend

<num1> = 1 - 15

<num2> = 0 - 113

<num3> = 0 - 3

<num4> = 0 - 13

Details

If the status is *set*, there are no links active in the IMA group, or there is a timing mismatch in the IMA group. If there are no links active in the IMA group, the IMA virtual link is not capable of carrying any user traffic.

A *clear* is issued when one or more links in the IMA group are activated, or when the timing mismatch no longer exists.

Probable Cause

Protocol error, Timing problem

Type

Communications

Remedial action

This condition is usually caused by incorrect connection of the links or configuration of the local and remote IMA groups. Check that the physical ports are properly connected at the local and remote ends, and that all port alarms are clear. Examine the alarm comment text and the *failureCause* and *remoteDefect* operational attributes of the IMA component to obtain an indication as to the cause of the problem, and check the configuration of the IMA and LINK components on the local and remote ends.

7011 1200

Component	Severity	Status
For Passport 7400: Lp/<num1> Ima/<num2> Lk/<num5> For Passport 15000 and 20000: Lp/<num1> DS3/<num3> Ima/<num4> Lk/<num5>	critical/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - 113

<num3> = 0 - 3

<num4> = 0 - 13

<num5> = 0 - 31

Details

If the status is *set*, the link is not an active member of the IMA group. The link will not be used by the IMA group for carrying any user traffic.

A *clear* is issued when the link is activated in the IMA group.

Probable Cause

Protocol error

Type

Communications

Remedial action

This condition is usually caused by incorrect connection or configuration of the link. First check that the physical port used by this link is properly connected at the local and remote ends, and that all port alarms are clear. If the problem persists then examine the *failureCause* and *remoteDefect* operational attributes of the LINK component to obtain an indication as to the cause of the problem, and check the configuration of the LINK components on the local and remote ends.

7011 1210

Component	Severity	Status
For Passport 7400: Lp/<num1> Ima/<num2> Lk/<num5> For Passport 15000 and 20000: Lp/<num1> DS3/<num3> Ima/<num4> Lk/<num5>	critical/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - 113

<num3> = 0 - 3

<num4> = 0 - 13

<num5> = 0 - 31

Details

If the status is *set*, a loss of IMA frame (LIF) alarm condition has been declared. The LIF alarm condition is declared when the a LIF defect has persisted on the link for 2.5 ± 0.5 seconds.

A *clear* is issued when the LIF defect has been absent for 10.0 ± 0.5 seconds.

A LIF defect is declared if IMA framing has not been recovered three IMA frame periods after the occurrence of an out of IMA frame (OIF) anomaly. An OIF anomaly is the occurrence of one of the following events:

- a missing ICP cell

- an invalid ICP cell

- two consecutive errored ICP cells

- a valid ICP cell at an unexpected position

A LIF defect is cleared if IMA framing has been maintained for two IMA frame periods.

Probable Cause

Protocol error

Type

Communications

Remedial action

This condition is usually caused by incorrect connection or configuration of the link. Check the *lastOifCause* operational attribute of the link for an indication of the

cause. Ensure that the physical port is properly connected at the local and remote ends, and check the configuration of the *link* component on the local and remote ends.

7011 1211

Component	Severity	Status
For Passport 7400: Lp/<num1> Ima/<num2> Lk/<num5> For Passport 15000 and 20000: Lp/<num1> DS3/<num3> Ima/<num4> Lk/<num5>	critical/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - 113

<num3> = 0 - 3

<num4> = 0 - 13

<num5> = 0 - 31

Details

If the status is *set*, a loss of delay synchronization (LODS) condition is present on the link.

A *clear* is issued once the LODS condition is no longer present.

A LODS condition is declared when the transit delay of a link being activated in the IMA group relative to the reference link in the IMA group exceeds the provisioned maximum acceptable differential delay, or when the transit delay of a link already active in the IMA group relative to the reference link in the IMA group exceeds the provisioned maximum acceptable differential delay plus one millisecond.

The LODS condition is cleared when the transit delay of the link relative to the reference link in the IMA group is within the provisioned maximum acceptable differential delay.

Probable Cause

Protocol error

Type

Communications

Remedial action

Check the *relativeDelay* operational attribute of the link to determine its differential delay. If an increase in the maximum differential delay across the IMA group is acceptable, increase the setting of the *maxDiffDelay* attribute of the parent IMA component. Alternatively, changing the setting of the *linkSelectionCriterion* attribute of the parent IMA component may result in a different reference link for the IMA group; however, be warned that this may result in the differential delay

becoming unacceptable for other links in the group. If the above actions do not solve the problem, replace the physical facility used by this link with one that exhibits a transit delay closer to that of the reference link.

7011 1212

Component	Severity	Status
For Passport 7400: Lp/<num1> Ima/<num2> Lk/<num5> For Passport 15000 and 20000: Lp/<num1> DS3/<num3> Ima/<num4> Lk/<num5>	critical/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - 113

<num3> = 0 - 3

<num4> = 0 - 13

<num5> = 0 - 31

Details

If the status is *set*, the link has been identified as being misconnected.

A *clear* is issued once the misconnection is no longer present.

A link is tested for misconnection during the IMA group start-up and link addition procedures. A link is identified as being misconnected if the remote end does not loop back a test pattern transmitted by the local end, or if the link belongs to a different IMA group than the one with which the local end has elected to stage.

Probable Cause

Protocol error

Type

Communications

Remedial action

This condition is usually caused by incorrect connection or configuration of the link. Check that the physical port is properly connected at the local and remote ends, and check the configuration of the LINK component on the local and remote ends.

7011 1213

Component	Severity	Status
For Passport 7400: Lp/<num1> Ima/<num2> Lk/<num5> For Passport 15000 and 20000: Lp/<num1> DS3/<num3> Ima/<num4> Lk/<num5>	critical/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - 113

<num3> = 0 - 3

<num4> = 0 - 13

<num5> = 0 - 31

Details

If the status is *set*, a remote failure indicator (RFI) alarm condition has been declared. The RFI alarm condition is declared when a remote defect indicator (RDI) defect has persisted on the link for 2.5 ± 0.5 seconds.

A *clear* is issued when the RDI defect has been absent for 10.0 ± 0.5 seconds.

An RDI defect is declared when one of the following remote defect indicators is received for this link from the remote IMA:

- physical link defect

- loss of IMA frame (LIF)

- loss of delay synchronization (LODS)

The RDI defect is cleared when a remote defect indicator is no longer being received for the link from the remote IMA.

Probable Cause

Protocol error

Type

Communications

Remedial action

Check the *remoteDefect* operational attribute of the link to determine what defect indicator is being received from the far end. Verify the operational attributes at the remote end to determine why the defect indicator is being transmitted.

7011 1214

Component	Severity	Status
For Passport 7400: Lp/<num1> Ima/<num2> Lk/<num5> For Passport 15000 and 20000: Lp/<num1> DS3/<num3> Ima/<num4> Lk/<num5>	critical/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - 113

<num3> = 0 - 3

<num4> = 0 - 13

<num5> = 0 - 31

Details

If the status is *set*, a fault alarm condition has been declared on the link. A fault alarm condition is declared if no ICP cells are detected on the link during a start-up or link addition attempt or if an invalid IMA group ID, frame length, group symmetry or logical link ID is received on the link during IMA group start-up or link addition.

A *clear* is issued when the fault alarm condition is not longer present.

Probable Cause

Protocol error

Type

Communications

Remedial action

This condition is usually caused by incorrect connection or configuration of the link. Check the *failureCause* operational attribute of the link to obtain an indication as to the cause of the problem. Ensure that the physical port is properly connected at the local and remote ends, and check the configuration of the LINK components on the local and remote ends.

7011 1215

Component	Severity	Status
For Passport 7400: Lp/<num1> Ima/<num2> Lk/<num5> For Passport 15000 and 20000: Lp/<num1> DS3/<num3> Ima/<num4> Lk/<num5>	critical/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - 113

<num3> = 0 - 3

<num4> = 0 - 13

<num5> = 0 - 31

Details

If the status is *set*, the remote link has gone to the Unusable state.

A *clear* is issued once the remote link is no longer in the Unusable state.

Probable Cause

Protocol error

Type

Communications

Remedial action

Check the operational attributes at the remote end to determine why it has gone to the Unusable state.

7011 1216

Component	Severity	Status
For Passport 7400: Lp/<num1> Ima/<num2> Lk/<num5> For Passport 15000 and 20000: Lp/<num1> DS3/<num3> Ima/<num4> Lk/<num5>	critical/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - 113

<num3> = 0 - 3

<num4> = 0 - 13

<num5> = 0 - 31

Details

If the status is *set*, a protocol error alarm condition has been declared on the link. A protocol error alarm condition is declared if, during IMA group start-up or link addition, the link could not be activated within the prescribed time-out period, and no other failure condition has been identified.

A *clear* is issued when the protocol error condition is not longer present.

Probable Cause

Protocol error

Type

Communications

Remedial action

This condition may be caused by incorrect configuration of the IMA group. Verify the *linkRetryTimeout* provisionable attribute of the IMA component at the local and remote ends, and check the operational attributes of the IMA and LINK components at the local and remote ends.

7011 1400

Component	Severity	Status
Lp/<num1> Mlfr/<num2>	critical/cleared	set/clear

Legend

<num1> = 2 - 15

<num2> = 0 - 111

Details

If the status is *set*, there is an insufficient number of links (determined by *activationClass* and *activationThreshold* attributes under the *MultiLinkFrameRelay* component) in the up state.

A *clear* is issued when a sufficient number of links (determined by *activationClass* and *activationThreshold* attributes under the *MultiLinkFrameRelay* component) are in the up state.

Remedial action

Check the state of the *MultiLinkFrameRelay* and *Link* components on local and remote endpoints and, if necessary, add more links to the bundle.

7011 1401

Component	Severity	Status
Lp/<num1> Mlfr/<num2>Link/<num3>	critical/cleared	set/clear

Legend

<num1> = 2 - 15

<num2> = 0 - 111

<num3> = 0 - 27

Details

If the status is *set*, there is a bundle link configuration mismatch between the expected and the received value for the *remoteName* attribute for the bundle.

A *clear* is issued when the expected value for the *remoteName* attribute for the bundle is received.

Remedial action

Check the *errorCause* and *remoteName* attributes and the configured data for the *Link* component. Lock and unlock the *MultiLinkFrameRelay* component to restart the MLFR link integrity protocol.

7011 1402

Component	Severity	Status
Lp/<num1> Mlfr/<num2>Link/<num3>	critical/cleared	set/clear

Legend

<num1> = 2 - 15

<num2> = 0 - 111

<num3> = 0 - 27

Details

If the status is *set*, there is an unrecognized OUI in a received Vendor Specific information field.

A *clear* is issued when the expected OUI is received.

Remedial action

Remove the Link and add it again to Mlfr component.

7011 1403

Component	Severity	Status
Lp/<num1> Mlfr/<num2>Link/<num3>	critical/cleared	set/clear

Legend

<num1> = 2 - 15

<num2> = 0 - 111

<num3> = 0 - 27

Details

If the status is *set*, the link is in *idle* state.

A *clear* is issued when the link leaves the *idle* state.

Remedial action

Check the *cause* attribute and the provisioned data for the *Link* component. Lock and unlock the *MultiLinkFrameRelay* component to restart the MLFR link integrity protocol.

7011 1404

Component	Severity	Status
Lp/<num1> Mlfr/<num2>Link/<num3>	critical/cleared	set/clear

Legend

<num1> = 2 - 15

<num2> = 0 - 111

<num3> = 0 - 27

Details

If the status is *set*, the link is in *down* state.

A *clear* is issued when the link leaves the *down* state.

Remedial action

Check the *cause* attribute and the provisioned data for the *Link* component. Lock and unlock the *MultiLinkFrameRelay* component to restart the MLFR link integrity protocol.

7011 1405

Component	Severity	Status
Lp<num1> Mlfr/<num2>Link/<num3>	major/cleared	set/clear

Legend

<num1> = 2 - 15

<num2> = 0 - 111

<num3> = 0 - 27

Details

If the status is *set*, a loopback was detected.

A *clear* is issued when the loopback is removed.

Remedial action

Check if the external loopback is installed.

7011 1406

Component	Severity	Status
Lp/<num1> Mlfr/<num2>Link/<num3>	critical/cleared	set/clear

Legend

<num1> = 2 - 15

<num2> = 0 - 111

<num3> = 0 - 27

Details

If the status is *set*, the bundle link differential delay exceeds the maximum allowed.

A *clear* is issued when the bundle link differential delay no longer exceeds the maximum allowed.

Remedial action

The operator may consider the increasing of the value of the *maxDiffDelay* attribute for this bundle, based on the length of the wires and the size of the frames between the near and far end.

7011 1407

Component	Severity	Status
Lp/<num1> Mlfr/<num2>Link/<num3>	critical/cleared	set/clear

Legend

<num1> = 2 - 15

<num2> = 0 - 111

<num3> = 0 - 27

Details

If the status is *set*, there was detected an error in the MLFR link integrity protocol between the near and far end.

A *clear* is issued when valid MLFR link integrity protocol messages are received.

Remedial action

Lock and unlock the *MultiLinkFrameRelay* component to restart the MLFR link integrity protocol.

7011 2000

Component	Severity	Status
Lp/<num1> <type>/<num2>	critical/cleared	set/clear

Legend

<num1> = 0 - 15

<type> = DS3, E3, SONET, SDH, DS1, E1, CHANNEL, V35, X21, HSSI, IMA and BridgedSonet

<num2> = 0 - n, where n is 1 less than the number of ports supported on the card type

Details

When a hardware failure has been found by port diagnostics, the port is automatically locked and disabled by the system. Alarm code 70112000 is raised when a user attempts to unlock the port before the failure is rectified.

A *clear* is issued after running the diagnostics successfully.

Probable Cause

Equipment malfunction

Type

Equipment

Remedial action

Replace the defective hardware.

7011 2001

Component	Severity	Status
Lp/<num1> <type>/<num2>	critical/cleared	set/clear

Legend

<num1> = 0 - 15

<type> = V35, X21 and HSSI

<num2> = 0 - n, where n is 1 less than the number of ports supported on the card type used.

Details

If the status is *set*, the link is in a state that renders the port *disabled*.

On a V35 or a X21 port, if the incoming line state is not consistent with that described in the provisionable attribute *readyLineState*, the port is disabled.

A *clear* is issued when the condition has been cleared.

Probable Cause

dteDce interface error

Type

Communications

Remedial action

Issue the *display* command on the component that has issued the alarm to discover the cause of the problem.

For a V35 or X21 port, check if the *readyLineState* attribute is set up as expected and verify that the cable is connected properly.

7011 2002

Component	Severity	Status
Lp/<num1> <type>/<num2>	major/cleared	message

Legend

<num1> = 0 - 15

<type> = DS3, E3, SONET, and SDH

<num2> = 0 - n, where n is 1 less than the number of ports supported on the card type

Details

The card is unable to synchronize its transmit clock to the CP's module clock. This may indicate an equipment malfunction on the FP, on the backplane, or on the active CP from which the module clock signal originates.

Probable Cause

Equipment malfunction

Type

Equipment

Remedial action

Check for defective FP, backplane, or CP hardware.

7011 5000

Component	Severity	Status
Lp/<num1> <type>/<num2> or Lp/<num1> SDH/0 VC4/0 VC12/<num3> E1 or Lp/<num1> Sonet/<num4> Sts/<num5> Vt1dot5/<num6> DS1	critical/cleared	set/clear

Legend

<num1> = 1 - 15

<type> = EDS1, EE1, DS1 and E1

<num2> = 0 - n, where n is 1 less than the number of ports supported on the card type used

<num3> = multiple indexes 1-3, 1-7, 1-3

<num4> = 0 - 15

<num5> = 0 - 11

<num6> = multiple indexes 1-7, 1-4

Details

If the status is *set*, the link has been in a Loss of Frame (LOF) state for greater than 2 seconds.

A *clear* is issued when the LOF condition has been cleared for more than 10 seconds.

Probable Cause

Loss of frame

Type

Communications

Remedial action

Check the far end for proper configuration.

7011 5001

Component	Severity	Status
Lp/<num1> <type>/<num2> or Lp/<num1> SDH/0 VC4/0 VC12/<num3> E1 or Lp/<num1> Sonet/<num4> Sts/<num5> Vt1dot5/<num6> DS1	minor/cleared	set/clear

Legend

<num1> = 1 - 15

<type> = EDS1, EE1, DS1 and E1

<num2> = 0-n, where n is 1 less than the number of ports supported on the card type used

<num3> = multiple indexes 1-3, 1-7, 1-3

<num4> = 0 - 15

<num5> = 0 - 11

<num6> = multiple indexes 1-7, 1-4

Details

If the status is *set*, then the far end Remote Alarm Indication (RAI) defect indicators have been received. This is indicated immediately and remains present for at least 1 second.

A *clear* is issued when no far end RAI defect indicators are detected.

Probable Cause

Local transmission error

Type

Communications

Remedial action

The far end is complaining about a Loss of Frame (LOF) condition. Check that the provisioning data is consistent on both ends of the connection.

7011 5002

Component	Severity	Status
Lp/<num1> <type>/<num2> or Lp/<num1> SDH/0 VC4/0 VC12/<num3> E1 or Lp/<num1> Sonet/<num4> Sts/<num5> Vt1dot5/<num6> DS1	critical/cleared	set/clear

Legend

<num1> = 1 - 15

<type> = EDS1, EE1,DS1 and E1

<num2> = 0-n, where n is 1 less than the number of ports supported on the card type used

<num3> = multiple indexes 1-3, 1-7, 1-3

<num4> = 0 - 15

<num5> = 0 - 11

<num6> = multiple indexes 1-7, 1-4

Details

If the status is *set*, the link has been in an Alarm Indication Signal (AIS) state for greater than 2 seconds.

A *clear* is issued when the AIS condition has been cleared for more than 10 seconds.

Probable Cause

Remote transmission error

Type

Communications

Remedial action

The far end is complaining about Loss of Signal (LOS) or the far end port is under test. Check the cabling between the two interfaces or check if there are any tests running on the far end interface.

7011 5003

Component	Severity	Status
Lp/<num1> <type>/<num2> or Lp/<num1> SDH/0 VC4/0 VC12/<num3> E1	critical/cleared	set/clear

Legend

<num1> = 1 - 15

<type> = EDS1, EE1, DS1 and E1

<num2> = 0-n, where n is 1 less than the number of ports supported on the card type used

<num3> = multiple indexes 1-3, 1-7, 1-3

Details

If the status is *set*, the link has been in an Loss of Signal (LOS) state for greater than 2 seconds.

A *clear* is issued when the LOS condition has been cleared for more than 10 seconds.

Probable Cause

Loss of Signal

Type

Communications

Remedial action

Check the cabling between this port and the far end port.

7011 5004

Component	Severity	Status
Lp/<num1> E1/<num2> or Lp/<num1> SDH/0 VC4/0 VC12/<num3> E1	critical/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0-n, where n is 1 less than the number of ports supported on the card type used

<num3> = multiple indexes 1-3, 1-7, 1-3

Details

If the status is *set*, the link has been in a Multiframe Remote Alarm Indication (RAI) state for greater than 2 seconds.

The far end interface is complaining that it has lost Multiframe alignment.

A *clear* is issued when the Multiframe RAI condition has been cleared for more than 10 seconds.

Probable Cause

Local transmission error

Type

Communications

Remedial action

Check the configuration of both ports.

7011 5005

Component	Severity	Status
Lp/<num1> E1/<num2> or Lp/<num1> SDH/0 VC4/0 VC12/<num3> E1	critical/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0-n, where n is 1 less than the number of ports supported on the card type used

<num3> = multiple indexes 1-3, 1-7, 1-3

Details

If the status is *set*, the link has been in a Multiframe Red state for greater than 2 seconds.

A *clear* is issued when the Multiframe Red condition has been cleared for more than 10 seconds.

Probable Cause

Loss of Frame

Type

Communications

Remedial action

Check the configuration of both ports.

7011 5006

Component	Severity	Status
Lp/<instance> DS1/<Instance>	major/cleared	set/clear
Lp/<instance> E1/<Instance>		

Legend

<instance> = provisioned decimal digit 0-9

Details

If the status is *set*, a yellow alarm is being asserted on the port. The yellow alarm is asserted because of voice services using this port, having connectivity problems through the subnet, which could be caused by numerous reasons.

A *clear* is issued when the yellow alarm is no longer being asserted on the port. The yellow alarm is no longer being asserted because the connectivity problems of the voice services using this port have been re-established.

Probable Cause

Communications subsystem failure

Type

Communications

Remedial action

The yellow alarm was asserted due to connectivity problems of the voice services using the port. This could be caused by two generic reasons. First, the operational state of the voice services using the port in yellow alarm state, should be checked to see if its enabled, as well as the remote voice service that they are connected to.

If not, maintenance action is required to restore the services on the DS1/E1 interface. If they are all enabled, connectivity problems are occurring within the subnet. Trunks that carry the voice traffic through the subnet should be investigated for problems and rectified in order to restore connectivity of the voice services.

7011 5007

Component	Severity	Status
Lp/<num1> E1/<num2>	minor/cleared	set/clear
or		
Lp/<num1> Sdh/<num2> Vc4/<num3> Vc12/<num4> E1		

Legend

<num1> = 1 - 15

<num2> = 0 - n, where n is 1 less than the number of ports supported on the card type used

<num3> = 0 - n, where n depends on the SDH port type (0 for STM-1)

<num4> = multiple indexes 1-3, 1-7, 1-3

Details

If the status is *set*, the link has been in a CRC-4 Multiframe LOF state for more than 2.5 seconds.

A *clear* is issued when the CRC-4 Multiframe LOF condition has been cleared for more than 10 seconds.

The CRC-4 Multiframe LOF alarm sets the E1 component state to degraded.

Probable Cause

The far end does not send CRC-4 Multiframe.

Type

Communications

Remedial action

Check the configuration of the ports on both ends.

7011 5010

Component	Severity	Status
Lp/<num1> <type>/<num2> or Lp/<num1> SDH/0 VC4/0 VC12/<num3> E1 or Lp/<num1> Sonet/<num4> Sts/<num5> Vt1dot5/<num6> DS1	minor/cleared	set/clear

Legend

<num1> = 1 - 15

<type> = DS1 and E1

<num2> = 0 - n, where n is 1 less than the number of ports supported on the card type used

<num3> = multiple indexes 1-3, 1-7, 1-3

<num4> = 0 - 15

<num5> = 0 - 11

<num6> = multiple indexes 1-7, 1-4

Details

If the status is *set*, the link has entered an Unavailable state. This condition is declared after 10 consecutive Severely Errored Seconds (SES).

A *clear* is issued after 10 consecutive seconds during which no SES are counted.

For DS1/E1, a Severely Errored Second is a second with 320 or more code violation error events or one or more SEF (Severely Errored Frame) events.

Probable Cause

Degraded signal

Type

Communications

Remedial action

Determine the cause of the errored seconds and fix the far end interface.

7011 5011

Component	Severity	Status
Lp/<num1> <type>/<num2>	warning/cleared	set/clear

Legend

<num1> = 1 - 15

<type> = DS1 and E1

<num2> = 0 - n, where n is 1 less than the number of ports supported on the card type used

Details

If the status is *set*, the transmit clock for the port has failed as a consequence of a failure of the locally generated asynchronous clock (Synchronous Residual Time Stamp (SRTS) mode. Under this condition the timing of the data on the DS1/E1 line may not conform to the appropriate standards.

If the status is *clear*, the alarm indicates that the transmit clock for the port is no longer defective.

Probable Cause

Type

Remedial action

Follow the standard procedure for testing the FP, and if the alarm does not clear the defective unit has to be replaced.

7011 5050

Component	Severity	Status
Lp/0 <type>/<num>	critical/cleared for active CP card; warning/cleared for standby CP card	set/clear

Legend

<type> = EDS1 or EE1

<num> = 0 - 1

Details

This alarm is set upon the provisioning of a BITS port on a CP card when either one or both CPs do not support BITS external timing.

If the active CP does not support BITS external timing, the alarm is raised as critical. If the standby CP does not support BITS external timing or if there is no standby CP (i.e., single CP switch), the alarm is raised as a warning message.

The operational state of the port depends solely on whether the active CP supports BITS external timing -- if the active CP supports BITS external timing, the port is up and operational; if the active CP does not support BITS external timing, the port is disabled.

The alarm is cleared when a card that supports BITS external timing is inserted into the slot or the BITS port is deleted.

Probable Cause

Equipment malfunction

Type

Equipment

Remedial action

Replace the card with one that supports BITS external timing.

7011 5100

Component	Severity	Status
Lp/<num1> <type>/<num2>	critical/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - 2

type = DS3 and E3

Details

If the status is *set*, a Loss Of Signal (LOS) condition has been present for at least 2 seconds on the incoming line. An LOS condition occurs when the port receives neither negative nor positive pulses.

A *clear* is issued when no LOS condition has been detected for at least 10 seconds.

Probable Cause

Loss of Signal

Type

Communications

Remedial action

Check the cabling between this port and the far end port.

7011 5101

Component	Severity	Status
Lp/<num1> <type>/<num2>	critical/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - 2

type = DS3 and E3

Details

If the status is *set*, an Loss Of Frame (LOF) condition has been present for at least 2 seconds on the incoming line. An LOF condition occurs when this port cannot frame to the incoming DS3 or E3 signal.

A *clear* is issued when this port has successfully framed the incoming signal for at least 10 seconds.

For DS3:

A DS3 far end SEF/AIS signal will be transmitted by this port for the duration of the time the LOF condition is present.

For E3:

In ITU-T G.751 framing mode, an E3 far end SEF/AIS signal will be transmitted by this port for the duration of the time the LOF condition is present.

In ITU-T G.832 framing mode, an E3 far end receive failure (FERF) signal will be transmitted by this port for the duration of the time the LOF condition is present.

Probable Cause

Loss of frame

Type

Communications

Remedial action

Check the configuration of the far end port.

7011 5102

Component	Severity	Status
Lp/<num1> <type>/<num2>	critical/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - 2

type = DS3 and E3

Details

If the status is *set*, Alarm Indication Signal (AIS) defects have been detected for at least 2 seconds on the incoming line.

A *clear* is issued when no AIS defects have been detected for at least 10 seconds.

For DS3:

Receiving an AIS means that the far end port has detected a problem beyond it. AIS could be generated by DS3 cross-connects located between Passport nodes.

A DS3 far end SEF/AIS signal will be transmitted by this port for the duration of the time that AIS defects are present.

For E3:

Receiving an AIS means that the far end port has been put in the LOCKED state.

In ITU-T G.751 framing mode, an E3 far end SEF/AIS signal will be transmitted by this port for the duration of the time that AIS defects are present.

In ITU-T G.832 framing mode, an E3 far end receive failure (FERF) signal will be transmitted by this port for the duration of the time that AIS defects are present.

Probable Cause

Remote transmission error

Type

Communications

Remedial action

Check the configuration and status of the far end port.

7011 5103

Component	Severity	Status
Lp/<num1> <type>/<num2>	critical/minor/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - 2

<type> = DS3 and E3

Details

For DS3:

When running in C-Bit Parity mode, the status is *set* to indicate that a far end alarm has been received over the Far End Alarm and Control (FEAC) channel. A *clear* is issued when the alarm signal is no longer received over the FEAC channel.

When not running C-Bit Parity mode, the status is *set* to indicate that far end SEF/AIS defect indicators have been received for at least 2 seconds. A *clear* is issued when no far end SEF/AIS defect indicators have been detected for the last 10 seconds.

For E3:

In ITU-T G.751 framing mode, the status is *set* to indicate that an E3 far end SEF/AIS signal has been received for at least 2 seconds. A *clear* is issued when no far end SEF/AIS signal has been received for at least 10 seconds.

In ITU-T G.832 framing mode, the status is *set* to indicate that an E3 far end receive failure (FERF) signal has been received for at least 2 seconds. A *clear* is issued when no FERF signal has been received for at least 10 seconds.

Probable Cause

Local transmission error

Type

Communications

Remedial action

Check the cabling between this port and the far end port, and the configuration and status of the far end port. If running in DS3 C-Bit Parity mode, also check the CBIT component operational data.

7011 5104

Component	Severity	Status
Lp/<num1> DS3/<num2>	critical/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - 2

Details

If the status is *set*, a DS3 Idle signal has been detected for at least 2 seconds on the incoming line.

The far end port has been locked and is not currently being used in operational testing.

A *clear* is issued when no DS3 Idle has been detected for at least 10 seconds.

Probable Cause

Underlying resource unavailable

Type

Communications

Remedial action

Check the status of the far end port.

7011 5105

Component	Severity	Status
Lp/<num1> DS3/<num2>	warning/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - 2

Details

If the status is *set*, there is a mismatch with the CBIT parity mode between the near end port and far end port. It is probable that the near end port is provisioned to support DS3 CBIT parity mode and the far end port is not.

A *clear* is issued when the far end port is provisioned to support CBIT parity mode.

Probable Cause

Configuration

Type

Communications

Remedial action

Check the configuration of the far end port to see if DS3 CBIT parity mode is provisioned.

7011 5110

Component	Severity	Status
Lp/<num1> DS3/<num2>	critical/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - 2

Details

If the status is *set*, this port has received a request from the far end to loopback the incoming DS3 signal. The far end port is currently under operational testing. Service on this port will be suspended.

A *clear* is issued when this port has received a request from the far end to stop looping the incoming DS3 signal, or when the port is locked, or when CBIT parity mode is turned off.

Probable Cause

Underlying resource unavailable

Type

Communications

Remedial action

Check the configuration of the far end port.

7011 5111

Component	Severity	Status
Lp/<num1> DS3/0	minor/cleared	set/clear

Legend

<num1> = 1 - 15

Details

If the status is *set*, the DS3 component has received a request from the far end to loopback an incoming DS1 tributary on the DS3. The loopback request is caused by the initiation of a remoteLoopThisTrib test at the far end. This request can come from a C-bit Parity channel only. The affected DS1 component is taken out of service. This alarm will remain set as long as at least one DS1 tributary is in loopback state.

A *clear* is issued when there are no more active DS1 loopbacks from the far end.

Probable Cause

Underlying resource unavailable

Type

Communications

Remedial action

If the loopback is not expected, check the far end DS3/0 DS1/x Test component to see if a remoteLoopThisTrib test type is active. The loopback can be removed at the near end by stopping the remoteLoopThisTrib test at the far end.

Alternatively, the loopback can be removed at the near end by Locking and then Unlocking the affected DS1 component.

7011 5112

Component	Severity	Status
Lp/<num1> DS3/0	minor	message

Legend

<num1> = 1 - 15

Details

The DS3 component receives a tributary loopback request for an unprovisioned tributary or is aborting an existing DS3 or DS1 cbit FEAC loopback.

Probable Cause

Underlying resource unavailable

Type

Communications

Remedial action

This alarm is provided for information only.

7011 5120

Component	Severity	Status
Lp/<num1> <type>/<num2>	minor/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - 2

type = DS3 and E3

Details

If the status is *set*, the near end path has entered an Unavailable state. This condition is declared after 10 consecutive Severely Errored Seconds (SESs).

A *clear* is issued after 10 consecutive seconds with no SES.

For DS3:

A SES is a second interval with more than 44 Path Code Violations (parity/frame errors) or one or more SEF/AIS defects.

For E3:

In ITU-T G.751 framing mode, a SES is a second interval with more than 22 Path Code Violations (frame errors) or one or more SEF/AIS defects.

In ITU-T G.832 framing mode, a SES is a second interval with more than 34 Path Code Violations (frame errors or BIP-8 errors) or one or more SEF/AIS defects.

Probable Cause

Degraded signal

Type

Communications

Remedial action

Determine the cause of the errored seconds and fix the far end port.

7011 5121

Component	Severity	Status
Lp/<num1> DS3/<num2>	minor/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - 2

Details

If the status is *set*, the link has entered a CBIT Unavailable state. This condition is declared after 10 consecutive CBIT Severely Errored Seconds (CSESs).

A *clear* is issued after 10 consecutive seconds with no CSES.

A CSES is a second interval with more than 44 CBIT Path Code Violations (CBIT parity errors) or one or more SEF/AIS defects.

Probable Cause

Degraded signal

Type

Communications

Remedial action

Determine the cause of the errored seconds and fix the far end port.

7011 5122

Component	Severity	Status
Lp/<num1> DS3/<num2>	minor/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - 2

Details

If the status is *set*, the link has entered a Far End Unavailable state. This condition is declared after 10 consecutive Far End Severely Errored Seconds (FESESs) or when a Remote Alarm Indicator (RAI) is declared.

A *clear* is issued after 10 consecutive seconds with no FESES and no RAI.

A FESES is a second interval with more than 44 Far End Code Violations (FEBEs) or one or more far end SEF/AIS defects. The occurrence of these events means that the far end does not receive properly what the local interface is transmitting to it.

Probable Cause

Degraded signal

Type

Communications

Remedial action

Determine the cause of the far end errored seconds and fix this port or the line between it and the far end.

7011 5130

Component	Severity	Status
Lp/<num1>	minor/cleared	set/clear

Legend

<num1> = 1 - 15

Details

If the status is *set*, one of the Multiport Aggregate Devices attached to the FP has a faulty power supply. This alarm will not be *set* again if the other Multiport Aggregate Devices connected to the FP develops a power supply problem.

A *clear* is issued when neither of the Multiport Aggregate Devices attached to the FP has a power supply problem.

Probable Cause

Power problem

Type

Equipment

Remedial action

Correct the problem as documented for the Multiport Aggregate Devices.

7011 5131

Component	Severity	Status
Lp/<num1>	major/cleared	set/clear

Legend

<num1> = 1 - 15

Details

If the status is *set*, one of the Multiport Aggregate Devices attached to the FP has a link problem. Possible causes could be Loss of signal, Loss of framing or a received Remote Alarm Indication in the signal. This alarm will not be *set* again if the other Multiport Aggregate Devices connected to the FP develops a link problem

A *clear* is issued when neither of the Multiport Aggregate Devices attached to the FP has a link problem.

Probable Cause

Input device error

Type

Equipment

Remedial action

Check cabling between Multiport Aggregate Devices and FP.

7011 5200

Component	Severity	Status
Lp/<num1> <type>/<num2>	critical/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - 2

<type> = SONET and SDH

Details

If the status is *set*, a Loss Of Signal (LOS) condition has been present for at least 2 seconds on the incoming line, or the LOS defect is present when the criteria for LOF failure declaration have been met. Declaration of an LOS failure clears any existing LOF failure.

A *clear* is issued when no LOS condition has been present for at least 10 seconds. If an LOF condition exists when the LOS is cleared, the LOF will be declared immediately.

Note: An LOS condition can also be caused by saturating the optical receiver with too strong a signal.

Probable Cause

Loss of signal

Type

Communications

Remedial action

Check the cabling between this port and the far end port. Verify that the strength of the signal is within specifications.

7011 5201

Component	Severity	Status
Lp/<num1> <type>/<num2>	critical/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - 2

<type> = SONET and SDH

Details

If the status is *set*, an Loss Of Frame (LOF) condition has been present for at least 2 seconds on the incoming line. An LOF condition occurs when this port cannot frame to the incoming SONET or SDH signal.

A *clear* is issued when this port has successfully framed the incoming signal for at least 10 seconds. LOF is also cleared when an LOS defect is declared.

Probable Cause

Loss of frame

Type

Communications

Remedial action

Check the configuration of the far end port and the section statistics.

7011 5202

Component	Severity	Status
Lp/<num1> <type>/<num2>	critical/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - 2

<type> = SONET and SDH

Details

If the status is *set*, Line Alarm Indication Signal (L-AIS) defects have been detected for at least 2 seconds on the incoming line. The L-AIS alarm is used to alert downstream equipment that a failure has been detected or that the port transmitting L-AIS has been locked.

A *clear* is issued when no L-AIS defects have been detected for at least 10 seconds.

Probable Cause

Remote transmission error

Type

Communications

Remedial action

Check the configuration and status of the far end port.

7011 5203

Component	Severity	Status
Lp/<num1> <type>/<num2>	minor/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - 2

<type> = SONET and SDH

Details

If the status is *set*, this port is receiving the Line Remote Defect Indicator (L-RDI). L-RDI is transmitted by the far end when it has been detecting L-AIS defects for some period of time.

A *clear* is issued when no L-RDI defects have been detected for 10 seconds.

Probable Cause

Local transmission error

Type

Communications

Remedial action

Check the cabling between this port and the far end port, and the configuration and status of the far end port.

7011 5204

Component	Severity	Status
Lp/<num1> <type>/<num2>	minor/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - 2

<type> = SONET and SDH

Details

If the status is *set*, a Sonet/Sdh port provisioned to act as a transmit clock reference has received the code “do not use for synchronization” in the S1 byte (in the SONET/SDH line overhead) for 2.5 +/- 0.5 seconds. A port is acting as a transmit clock reference if:

- it is provisioned with a *clockingSource* of *line*, or
- it is provisioned with a *clockingSource* of *module* and is being used by the *NetworkSynchronization* component as clock reference.

A *clear* is issued when the “do not use for synchronization” code is not received for 10 +/- 0.5 seconds, or when the port is no longer provisioned to act as a transmit clock reference.

Probable Cause

Remote transmission error

Type

Communications

Remedial action

This alarm is caused by the far end Sonet/Sdh port is transmitting an S1 value of “do not use for synchronization”. This is most likely caused by a loss of synchronization to the far end port’s provisioned transmit clocking source. Check the provisioning and operational state of the far end SONET or APS equipment.

7011 5210

Component	Severity	Status
Lp/<num1> <type>/<num2>	minor/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - 2

<type> = SONET and SDH

Details

If the status is *set*, this port has entered an Unavailable state. This condition is declared at the onset of 10 consecutive Line Severely Errored Seconds (L-SESs).

A *clear* is issued at the onset of 10 seconds with no L-SES.

A L-SES is a second interval with more than 32 Line Code Violations (BIP-24 errors) or one or more L-AIS defects.

Probable Cause

Type

Remedial action

Determine the cause of the errored seconds and fix the far end port.

7011 5211

Component	Severity	Status
Lp/<num1> <type>/<num2>	minor/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - 2

<type> = SONET or SDH

Details

If the status is *set*, this port has entered a Far End Line Unavailable state. This condition is declared at the onset of 10 consecutive Far End Line Severely Errored Seconds (FEL-SESs).

A *clear* is issued at the onset of 10 seconds with no FEL-SES.

A FEL-SES is a second interval with more than 32 Far End Line Code Violations (FEBE errors) or one or more line RDI defects. The occurrence of these events means that the far end does not receive properly what the local interface is transmitting to it.

Probable Cause

Degraded signal

Type

Communications

Remedial action

Determine the cause of the far end errored seconds and fix this port or the line between it and the far end.

7011 5250

Component	Severity	Status
Lp/<num1> <type1>/<num2> <type2>/0 Laps/<num3> <type2>/0 or Pbg/<num4> sts/0	critical/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - n, where n is one less than the number of ports on the card.

<num3> = 0 - 15999

<num4> = 0 - 15999

<type1> = SONET or SDH

<type2> = Path or STS or VC4

Details

If the status is *set*, a Loss Of Signal (LOP) condition has been present for at least 2 seconds on the incoming line. An LOP failure indicates that the interface is no longer detecting valid STS Payload Envelope (SPE) pointers.

A *clear* is issued when no LOP condition has been present for at least 10 seconds, or when an incoming P-AIS defect is detected.

Probable Cause

Loss of frame

Type

Communications

Remedial action

Check the cabling between this port and the far end port.

7011 5251

Component	Severity	Status
Lp/<num1> <type1>/<num2> <type2>/0 Laps/<num3> <type2>/0 or Pbg/<num4> sts/0	critical/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - n, where n is one less than the number of ports on the card.

<num3> = 0 - 15999

<num4> = 0 - 15999

<type1> = SONET or SDH

<type2> = Path or STS or VC4

Details

If the status is *set*, a Path AIS (P-AIS) condition has been present for at least 2 seconds on the incoming line. A P-AIS signal is used to alert downstream equipment that a failure has been detected or that the *Path/Sts/Vc4* component transmitting P-AIS has been locked.

A *clear* is issued when no P-AIS signal is detected for 10 seconds.

Probable Cause

Remote transmission error

Type

Communications

Remedial action

Check the configuration of the far end port.

7011 5252

Component	Severity	Status
Lp/<num1> <type1>/<num2> <type2>/0 Laps/<num3> <type2>/0 or Pbg/<num4> sts/0	minor/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - n, where n is one less than the number of ports on the card.

<num3> = 0 - 15999

<num4> = 0 - 15999

<type1> = SONET or SDH

<type2> = Path or STS or VC4

Details

If the status is *set*, Path RDI (P-RDI) defects have been detected for at least 2 seconds on the incoming line. The P-RDI signal is used by the far end to indicate that LOP or P-AIS defects, or an LCD state have been detected for some period of time.

A *clear* is issued when no P-RDI defects have been detected for at least 10 seconds.

Probable Cause

Local transmission error

Type

Communications

Remedial action

Check the configuration and status of the far end port.

7011 5253

Component	Severity	Status
Lp/<num1> <type1>/<num2> <type2>/0 Laps/<num3> <type2>/0 or Pbg/<num4> sts/0	critical/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - n, where n is one less than the number of ports on the card.

<num3> = 0 - 15999

<num4> = 0 - 15999

<type1> = SONET or SDH

<type2> = Path or STS or VC4

Details

If the status is *set*, this port is receiving an unexpected Path Signal Label. The Path Signal Label is used to indicate the content and format of the STS SPE. Expected Path Signal Labels are 0x13, the code for **ATM Mapping**, and 0x01, the code for **Equipped**.

A *clear* is issued when the correct Path Signal Label has been detected for 10 seconds.

A Path Signal Label Mismatch is not reported when receiving P-AIS or LOP defects.

Probable Cause

Protocol error

Type

Communications

Remedial action

Check the configuration and status of the far end port.

7011 5260

Component	Severity	Status
Lp/<num1> <type1>/<num2> <type2>/0 Laps/<num3> <type2>/0 or Pbg/<num4> sts/0	minor/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - n, where n is one less than the number of ports on the card.

<num3> = 0 - 15999

<num4> = 0 - 15999

<type1> = SONET or SDH

<type2> = Path or STS or VC4

Details

If the status is *set*, this port has entered an Unavailable state. This condition is declared at the onset of 10 consecutive Path Severely Errored Seconds (P-SESs).

A *clear* is issued at the onset of 10 seconds with no P-SES.

A P-SES is a second interval with more than 16 Path Code Violations (BIP-8 errors) or one or more P-LOP or P-AIS defects.

Probable Cause

Degraded signal

Type

Communications

Remedial action

Determine the cause of the errored seconds and fix the far end port.

7011 5261

Component	Severity	Status
Lp/<num1> <type1>/<num2> <type2>/0 Laps/<num3> <type2>/0 or Pbg/<num4> sts/0	minor/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - n, where n is one less than the number of ports on the card.

<num3> = 0 - 15999

<num4> = 0 - 15999

<type1> = SONET or SDH

<type2> = Path or STS or VC4

Details

If the status is *set*, this port has entered a Far End Path Unavailable state. This condition is declared at the onset of 10 consecutive Far End Path Severely Errored Seconds (FEP-SESs).

A *clear* is issued at the onset of 10 seconds with no FEP-SES.

A FEP-SES is a second interval with more than 16 Far End Path Code Violations (path FEBE errors) or one or more path RDI defects. The occurrence of these events means that the far end does not receive properly what the local interface is transmitting to it.

Probable Cause

Degraded signal

Type

Communications

Remedial action

Determine the cause of the far end errored seconds and fix this port or the line between it and the far end.

7011 5270

Component	Severity	Status
<type>/<num>	major/cleared	set/clear

Legend

<type> = Aps or Laps

<num> = 0 - 15999

Details

If the status is *set*, a Protection Switching Byte defect has persisted for 2.5 +/- 0.5 seconds. A Protection Switching Byte defect is declared when either an inconsistent APS byte or an invalid code is detected. An inconsistent APS byte occurs when no three consecutive K1 bytes (in the SONET/SDH line overhead) in the last 12 successive frames are identical, starting with the last frame containing a previously consistent byte. An invalid code occurs when the incoming K1 byte contains an unused code, a code irrelevant to the specific switching operation, or an invalid channel number, in three consecutive frames. An APS Protection Switching Byte Failure is treated as a signal failure on the protection line, preventing it from being used for protection.

A *clear* is issued when the Protection Switching Byte defect is absent for 10 +/- 0.5 seconds.

Probable Cause

Protocol error

Type

Communications

Remedial action

This alarm indicates that the far end equipment may be defective. Check the provisioning and operational state of the far end SONET or APS equipment.

7011 5271

Component	Severity	Status
<type>/<num>	minor/cleared	set/clear

Legend

<type> = Aps or Laps

<num> = 0 - 15999

Details

If the status is *set*, a Channel Mismatch defect has persisted for 2.5 +/- 0.5 seconds. A Channel Mismatch defect is declared when the channel number transmitted in the K1 byte (in the SONET/SDH line overhead) does not match the channel number received in the K2 byte for 50 ms.

A *clear* is issued when the Channel Mismatch defect is absent for 10 +/- 0.5 seconds.

Probable Cause

Protocol error

Type

Communications

Remedial action

This alarm indicates that the far end equipment may be defective. Check the provisioning and operational state of the far end SONET or APS equipment.

7011 5272

Component	Severity	Status
<type>/<num>	minor/cleared	set/clear

Legend

<type> = Aps or Laps

<num> = 0 - 15999

Details

If the status is *set*, an APS Mode Mismatch defect has persisted for 2.5 +/- 0.5 seconds. An APS Mode Mismatch defect is declared when either (1) an *Aps/Laps* component (which uses for 1+1 protection switching) receives an indication from the far end in the received K2 byte (SONET line overhead only) that is provisioned for 1:n, or (2) when an *Aps*/*Laps* component provisioned for bidirectional switching receives an indication from the far end in the received K2 byte that it is provisioned for unidirectional switching (or vice versa).

A *clear* is issued when the APS Mode Mismatch defect is absent for 10 +/- 0.5 seconds.

Probable Cause

Protocol error

Type

Communications

Remedial action

Check the provisioning of the near and far end APS systems and ensure that they both use the same provisioned architecture (1+1) and mode (unidirectional or bidirectional).

7011 5273

Component	Severity	Status
<type>/<num>	minor/cleared	set/clear

Legend

<type> = Aps or Laps

<num> = 0 - 15999

Details

If the status is *set*, a Far-End Protection-Line defect has persisted for 2.5 +/- 0.5 seconds. A Far-End Protection-Line defect is declared when the *Aps*/*Laps* component receives three consecutive K1 bytes (in the SONET/SDH line overhead) with the code indicating Signal Fail on the protection line. This alarm is not applicable when the *Aps*/*Laps* component is provisioned for 1+1 unidirectional switching.

A *clear* is issued when the Far-End Protection-Line defect is absent for 10 +/- 0.5 seconds.

Probable Cause

Degraded signal

Type

Communications

Remedial action

Correct the failure on the Sonet/Sdh component used as the protection line.

7011 5274

Component	Severity	Status
<type>/<num>	warning/cleared	set/clear

Legend

<type> = Aps or Laps

<num> = 0 - 15999

Details

If the status is *set*, an APS request other than doNotRevert or noRequest (or reverseRequest in bidirectional switching), has been sent by either the near end or the far end in the K1 byte (in the SONET/SDH line overhead). Note that if the *Aps*/*Laps* component is provisioned for unidirectional switching the far end request will not be monitored and will not factor into this alarm.

The alarm's text will indicate the highest priority request being sent by the near or far end. Thereafter, every time the highest priority request changes to a new value (not one of doNotRevert, noRequest or reverseRequest) the alarm will be reissued indicating the new request.

A *clear* is issued immediately when the APS requests being sent by both the near and far end change to either doNotRevert or noRequest.

Probable Cause

Degraded signal

Type

Communications

Remedial action

This alarm is informational in nature, and indicates that there is activity on the SONET/SDH APS channel which may restrict the *Aps*/*Laps* component's ability to deal with line failures. If the request is a signalFail or signalDegrade, the condition should be corrected at the SONET/SDH level. If the request is an operator command the Aps can be restored to full unrestricted operation by clearing the command.

7011 5275

Component	Severity	Status
<type>/<num>	critical/cleared	set/clear

Legend

<type> = Aps or Laps

<num> = 0 - 15999

Details

If the status is *set*, the *Aps*/*Laps* component's *nearEndRxActiveChannel* has experienced a signal failure (SF).

A *clear* is issued when the SF becomes absent from the *Aps*/*Laps* component's *nearEndRxActiveChannel*.

Probable Cause

Communications subsystem failure

Type

Communications

Remedial action

This alarm indicates that both the working and protection line are unavailable. Check for failures of the Sonet/Sdh components provisioned as the working and protection lines.

Display the *Aps*/*Laps* component's operational attributes and check for near and far end command requests which may be forcing the Aps to only use one of its lines, for instance the lockoutOfProtection command. If the request is from the near end the 'clear' verb can be used to clear the command. If the request is from the far end the command can only be cleared on the far end equipment.

7011 5276

Component	Severity	Status
Laps/<x>	minor/cleared	set/clear

Legend

<x> = 0 - 15999

Details

If the status is *set*, a primary section mismatch condition has been detected. This condition occurs when the primary section indicated in the received K2 byte does not equal the primary section transmitted in the K2 byte.

If this condition occurs and the primary section transmitted in the K2 byte is set to two, the local end changes its primary section to one and re-evaluates the position of the selector and the transmitted K1 byte.

If this condition occurs and the primary section transmitted in the K2 byte is set to one, the alarm remains until the far end changes its channel transmitted in the K2 byte.

A *clear* is issued when the K2 channel numbers match for 50 milliseconds.

Probable Cause

This condition can occur when the *Laps* component first comes into service after a provisioning change or after an unlock. It can also occur if the far end does not update the K2 channel number correctly or within 50 milliseconds of clearing a request for the primary section.

Type

Communications

Remedial action

No action is required on the local end because the local software automatically swaps the primary section if the local end does not have the primary section as one.

Check the far end configuration and/or support for automatic handling of primary section mismatch.

7011 5278

Component	Severity	Status
Laps/<instance>	minor	set/clear

Legend

<instance> = 0- 15999

Details

If the status is *set*, the Laps component configured with the Y-Protection protocol has detected that the standby line is unavailable. A *clear* is issued when both FPs are up and running without any port/line failure.

Probable Cause

Degraded signal.

Type

Communications.

Remedial action

Correct the failure on the Sonet/Sdh component used as the standby line.

7011 5279

Component	Severity	Status
Laps/<instance>	critical	set/clear

Legend

<instance> = 0- 15999

Details

If the status is *set*, the Laps component s nearEndRxActiveChannel configured with the Y-Protection protocol has been experiencing a signal failure (SF) for 2.5 +/- 0.5 seconds. A *clear* is issued when the SF has been absent from the Laps component s nearEndRxActiveChannel for 10 +/- 0.5 seconds.

Probable Cause

Communication subsystem failure.

Type

Communications.

Remedial action

Check for failures of the Sonet/Sdh components provisioned on the active lines.

7011 5280

Component	Severity	Status
Laps/<instance>	minor	set/clear

Legend

<instance> = 0- 15999

Details

If the status is *set*, the Laps component configured with the Y-Protection protocol is indicating that the active port is receiving RDI-L from the far-end equipment for 2.5 +/- 0.5 seconds. A *clear* is issued when the RDI-L has been absent from the active port for 10 +/- 0.5 seconds.

Probable Cause

Remote node transmission error.

Type

Communications.

Remedial action

Check for failures of the Sonet/Sdh components provisioned on the receive side of the far-end equipment.

7011 5290

Component	Severity	Status
Lp/<n> Sdh/0 Vc4/0 Vc12/<k>,<l>,<m>	minor/cleared	set/clear

Legend

<n> = 1 - 15

<k> = 1 - 3, <l> = 1 - 7, <m> = 1 - 3

Details

If the status is *set*, Low Order Path Remote Error Indicator (LP-REI) defects have been detected for at least 2 seconds on the incoming line. The LP-REI signal is used by the far end to indicate that one or more BIP-2 errors have been detected.

A *clear* is issued when no LP-REI defects have been detected for at least 10 seconds.

Probable Cause

Type

Remedial action

Check the status of the cable. Also check the status of the far end port.

7011 5291

Component	Severity	Status
Lp/<n> Sdh/0 Vc4/0 Vc12/<k>,<l>,<m>	minor/cleared	set/clear

Legend

<n> = 1 - 15

<k> = 1 - 3, <l> = 1 - 7, <m> = 1 - 3

Details

If the status is *set*, Low Order Path Remote Failure Indicator (LP-RFI) conditions have been detected for at least 2 seconds on the incoming line. The LP-RFI signal is used by the far end to declare a failure, which is a defect that persists beyond the maximum time allocated to the transmission system protection mechanisms.

A *clear* is issued when no LP-RFI conditions have been detected for at least 10 seconds.

Probable Cause

Type

Remedial action

Check the status of the far end port.

7011 5292

Component	Severity	Status
Lp/<n> Sdh/0 Vc4/0 Vc12/<k>,<l>,<m>	minor/cleared	set/clear

Legend

<n> = 1 - 15

<k> = 1 - 3, <l> = 1 - 7, <m> = 1 - 3

Details

If the status is *set*, Low Order Path Remote Defect Indicator (LP-RDI) defects have been detected for at least 2 seconds on the incoming line. The LP-RDI signal is used by the far end to indicate that a connectivity defect such as Low Order Path Unequipped (LP-UNEQ) or Low Order Path Trace Identifier Mismatch (LP-TIM), or a server defect such as Tributary Unit Alarm Indication Signal (TU-AIS) or Tributary Unit Loss of Pointer (TU-LOP) has been detected.

A *clear* is issued when no LP-RDI detects have been detected for at least 10 seconds.

Probable Cause

Type

Remedial action

Check the configuration and the status of the far end port.

7011 5293

Component	Severity	Status
Lp/<n> Sdh/0 Vc4/0 Vc12/<k>,<l>,<m>	minor/cleared	set/clear

Legend

<n> = 1 - 15

<k> = 1 - 3, <l> = 1 - 7, <m> = 1 - 3

Details

If the status is *set*, Tributary Unit Alarm Indication Signal (TU-AIS) defects have been detected for at least 2 seconds on the incoming line. The TU-AIS signal indicates that an upstream defect has been detected.

A *clear* is issued when no TU-AIS detects have been detected for at least 10 seconds.

Probable Cause

Type

Remedial action

Check the status of the far end port.

7011 5294

Component	Severity	Status
Lp/<n> Sdh/0 Vc4/0 Vc12/<k>,<l>,<m>	minor/cleared	set/clear

Legend

<n> = 1 - 15

<k> = 1 - 3, <l> = 1 - 7, <m> = 1 - 3

Details

If the status is *set*, Low Order Path Bit Interleaved Parity (BIP-2) defects have been detected for at least 2 seconds on the incoming line. The Low Order Path BIP-2 alarm is issued if the calculated BIP-2 does not equal to the received BIP-2.

A *clear* is issued when no Low Order Path BIP-2 detects have been detected for at least 10 seconds.

Probable Cause

Type

Remedial action

Check the status of the cable. Also check the status of the far end port.

7011 5295

Component	Severity	Status
Lp/<n> Sdh/0 Vc4/0 Vc12/<k>,<l>,<m>	critical/cleared	set/clear

Legend

<n> = 1 - 15

<k> = 1 - 3, <l> = 1 - 7, <m> = 1 - 3

Details

If the status is *set*, a Tributary Unit Loss of Pointer (TU-LOP) condition has been detected for at least 2 seconds on the incoming line. The TU-LOP signal indicates that an invalid pointer state is detected in the TU pointer.

A *clear* is issued when no TU-LOP detects have been detected for at least 10 seconds.

Probable Cause

Type

Remedial action

Check the configuration and the status of the far end port.

7011 5296

Component	Severity	Status
Lp/<n> Sdh/0 Vc4/0 Vc12/<k>,<l>,<m>	critical/cleared	set/clear

Legend

<n> = 1 - 15

<k> = 1 - 3, <l> = 1 - 7, <m> = 1 - 3

Details

If the status is *set*, a Low Order Path Unequipped (LP-UNEQ) condition has been detected for at least 2 seconds on the incoming line. The LP-UNEQ signal indicates that an unequipped defect has been detected.

A *clear* is issued when no LP-UNEQ detects have been detected for at least 10 seconds.

Probable Cause

Type

Remedial action

Check the configuration and the status of the far end port.

7011 5297

Component	Severity	Status
Lp/<n> Sdh/0 Vc4/0 Vc12/<k>,<l>,<m>	critical/cleared	set/clear

Legend

<n> = 1 - 15

<k> = 1 - 3, <l> = 1 - 7, <m> = 1 - 3

Details

If the status is *set*, a Tributary Unit Trace Identification Mismatch (TU-TIM) condition has been detected for at least 2 seconds on the incoming line. The TU-TIM signal indicates that the received trace identification does not match the provisioned value.

A *clear* is issued when no TU-TIM detects have been detected for at least 10 seconds.

Probable Cause

Type

Remedial action

Check the far end port to ensure that the correct equipment is connected. Also check if the provisioned value is correct.

7011 5300

Component	Severity	Status
Lp/<num1> <type>/<num2>	critical/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - 1

type = JT2

Details

If the status is *set*, a Loss Of Signal (LOS) condition has been present for at least 2 seconds on the incoming line. An LOS condition occurs when the port receives neither negative nor positive pulses.

A *clear* is issued when no LOS condition has been detected for at least 10 seconds.

Probable Cause

Loss of signal

Type

Communications

Remedial action

Check the cabling between this port and the far end port.

7011 5301

Component	Severity	Status
Lp/<num1> <type>/<num2>	critical/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - 1

type = JT2

Details

If the status is *set*, an Loss Of Frame (LOF) condition has been present for at least 2 seconds on the incoming line. An LOF condition occurs when this port cannot synchronize to the incoming JT2 frame.

A *clear* is issued when this port has successfully framed the incoming signal for at least 10 seconds.

Whilst the port is in the LOF alarm state, a far end RAI defect indicator is transmitted on the outgoing JT2 line.

Probable Cause

Loss of frame

Type

Communications

Remedial action

Check the configuration of the far end port.

7011 5302

Component	Severity	Status
Lp/<num1> <type>/<num2>	critical/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - 1

type = JT2

Details

If the status is *set*, Physical Alarm Indication Signal (AISPhys) defects have been detected for at least 2 consecutive seconds on the incoming line.

A *clear* is issued when no Physical AIS defects have been detected for at least 10 consecutive seconds.

Receiving an AIS means that the far end port has lost the capability to transmit valid JT2 frames or is has entered an *adminState* of *Locked*.

Whilst the rxAisPhysicalAlarm is *set*, a far end RAI defect indicator is transmitted on the outgoing JT2 line for the duration of the alarm condition.

Probable Cause

Remote transmission error

Type

Communications

Remedial action

Check the configuration and status of the far end port.

7011 5303

Component	Severity	Status
Lp/<num1> <type>/<num2>	critical/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - 1

type = JT2

Details

If the status is *set*, Payload Alarm Indication Signal (AISPayld) defects have been detected for at least 2 consecutive seconds on the incoming line.

A *clear* is issued when no Payload AIS defects have been detected for at least 10 consecutive seconds.

Receiving a Payload AIS means that the far end port has lost the capability to transmit valid JT2 frame payloads. The Payload AIS is defined as a bit array of the frame payload in which all binary bits are set to ‘1’.

Probable Cause

Remote transmission error

Type

Communications

Remedial action

Check the configuration and status of the far end port.

7011 5304

Component	Severity	Status
Lp/<num1> <type>/<num2>	minor/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - 1

type = JT2

Details

If the status is *set*, then the far end Remote Alarm Indication (RAI) defect indicators have been received. This is indicated immediately and remains present for at least 1 second.

A *clear* is indicated when no far end RAI defect indicators are detected.

Probable Cause

Local transmission error

Type

Communications

Remedial action

Check the cabling between this port and the far end port, and the configuration and status of the far end port.

7011 5400

Component	Severity	Status
Lp/<lpNumber> Ethernet/<port>	major/cleared	set/clear

Legend

<lpNumber> = 2 - 15

<port> = 0 - 3

Details

If the status is *set*, the port has lost synchronization with the Gigabit Ethernet signal on the incoming line. Declaration of the Loss of Synchronization failure clears any existing Auto-negotiation or Remote Link Failure alarms.

A *clear* is issued when synchronization has been acquired. The clearing of the alarm may be delayed by up to 10 seconds if an intermittent fault is detected.

Probable Cause

Loss of signal

Type

Communications

Remedial action

Check the cabling of the local and far end devices.

7011 5401

Component	Severity	Status
Lp/<lpNumber> Ethernet/<port>	major/cleared	set/clear

Legend

<lpNumber> = 2 - 15

<port> = 0 - 3

Details

If the status is *set*, the port has failed to Auto-Negotiate a common set of capabilities with the link partner.

A *clear* is issued when Auto-negotiation has been successful or synchronization is lost. The clearing of the alarm may be delayed by up to 10 seconds if an intermittent fault is detected.

Probable Cause

Configuration error

Type

Processing

Remedial action

Check the capability and possible configuration of the local and far end devices.

7011 5402

Component	Severity	Status
Lp/<lpNumber> Ethernet/<port>	major/cleared	set/clear

Legend

<lpNumber> = 2 - 15

<port> = 0 - 3

Details

If the status is *set*, the far end device has signaled that the link is offline.

A *clear* is issued when the far end device signals that the link is no longer offline or synchronization is lost. The clearing of the alarm may be delayed by up to 10 seconds if an intermittent fault is detected.

Probable Cause

Remote transmission error

Type

Communications

Remedial action

Check the status of the far end device.

7011 5403

Component	Severity	Status
Lp/<lpNumber> Ethernet/<port>	major/cleared	set/clear

Legend

<lpNumber> = 2 - 15

<port> = 0 - 3

Details

If the status is *set*, the far end device has signaled that the link is offline.

A *clear* is issued when the far end device signals that the link is no longer offline or synchronization is lost. The clearing of the alarm may be delayed by up to 10 seconds if an intermittent fault is detected.

Probable Cause

Remote transmission error

Type

Communications

Remedial action

Check the cabling of the local and far end devices.

7011 5480

Component	Severity	Status
Lp/<lpNumber> Ethernet/<port> OpticalModule	critical/cleared	set/clear

Legend

<lpNumber> = 2 - 15

<port> = 0 - 3

Details

If the status is *set*, the alarm may have resulted for any of the following reasons:

- the *Type* attribute does not match the optical module installed on this port. The actual optical module that is installed is displayed in the attribute *insertedType*.

- there is an internal error with the device

- the inserted optical module type or vendor is not approved

A *clear* is issued when the user provisions the attribute correctly with the optical module. The optical module is determined by the operational attribute *insertedType*.

In case of an internal error or vendor not allowed failure, a *clear* is issued when the optical module is replaced.

Probable Cause

Configuration error

Type

Processing

Remedial action

Check the configuration of the local device or replace the optical module if possible.

7011 5501

Component	Severity	Status
Lp/<num1> <type1>/<num2> Lp/<num1> <type2>/<num2> <type3>/0 Laps/<num3> <type3>/0 or Pbg/<num4> sts/0	major/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - n, where n is one less than the number of ports on the card.

<num3> = 0 - 15999

<num4> = 0 - 15999

<type1> = DS3, E3, DS1 and E1.

<type2> = SONET and SDH.

<type3> = Path or STS or VC4

Details

If the status is *set*, this port has been in a Loss of Cell Delineation state for T seconds, where T is the *alarmActDelay* attribute of the CELL component.

A *clear* is issued when the Loss of Cell Delineation state has not been present for 10 consecutive seconds.

For DS3 and E3, in direct mapping mode, Loss of Cell Delineation occurs when the interface is no longer able to identify ATM cell boundaries. In PLCP mapping mode, a Loss of Cell Delineation occurs when the interface is no longer able to identify PLCP frame boundaries.

Probable Cause

Loss of frame

Type

Communications

Remedial action

Check configuration of the far end port.

7011 5601

Component	Severity	Status
Lp/<num1> <type>/<num2>	minor/cleared	set/clear

Legend

<num1> = 1 - 15

<type> = DS3 and E3

<num2> = 0 - 2

Details

If the status is *set*, the link has entered a PLCP Far End Unavailable state. This condition is declared upon declaration of a PLCP RAI alarm state.

A *clear* is issued when the PLCP RAI alarm state is exited.

A PLCP RAI alarm state is entered when a 10 consecutive PLCP RAI bits are high in the incoming PLCP data stream, and cleared when 10 consecutive PLCP RAI bits are low on the incoming line, or when PLCP mode is disabled.

Probable Cause

Degraded signal

Type

Communications

Remedial action

Check the cabling and configuration of the far end port.

7011 5602

Component	Severity	Status
Lp/<num1> <type>/<num2>	minor/cleared	set/clear

Legend

<num1> = 1 - 15

<type> = DS3 and E3

<num2> = 0 - 2

Details

If the status is *set*, the link has entered a PLCP Near End Unavailable state. This condition is declared upon declaration of a PLCP LOF alarm state.

A *clear* is issued when the PLCP LOF alarm state is exited.

A PLCP LOF alarm state is entered when this port is not able to frame the incoming PLCP signal for 2 seconds, and exited when the port successfully frames the incoming PLCP signal for 10 seconds, or when PLCP mode is disabled.

Probable Cause

Degraded signal

Type

Communications

Remedial action

Check configuration of far end port.

7011 5603

Component	Severity	Status
Lp/<num1> <type>/<num2>	major/cleared	set/clear

Legend

<num1> = 1 - 15

<type> = DS3 and E3.

<num2> = 0 - 2

Details

If the status is *set*, this port has entered a PLCP LOF state. A PLCP LOF state is entered when the port cannot frame to the incoming PLCP signal for 2 seconds.

A *clear* is issued when PLCP LOF state is exited, which occurs when PLCP framing is recovered for 10 seconds or when PLCP is disabled.

A PLCP RAI signal will be transmitted by this port for the duration of the PLCP LOF state.

Probable Cause

Loss of frame

Type

Communications

Remedial action

Check configuration of this port and the far end port.

7011 5604

Component	Severity	Status
Lp/<num1> <type>/<num2>	major/minor/ cleared	set/clear

Legend

<num1> = 1 - 15

<type> = DS3 and E3

<num2> = 0 - 2

Details

If the status is *set*, this port has entered a PLCP RAI state. A PLCP RAI state is entered when the port receives ten consecutive high PLCP RAI bits on the incoming line.

A *clear* is issued when the PLCP RAI state is exited, which occurs when the port receives ten consecutive low PLCP RAI bits on the incoming line, or when PLCP mode is disabled.

The PLCP RAI signal will be transmitted by the far end port while it is in a PLCP LOF state.

Probable Cause

Local transmission error

Type

Communications

Remedial action

Check configuration of this port and the far end port.

7011 5701

Component	Severity	Status
Lp/<num1> E3/<num2>	minor/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - 2

Details

If the status is *set*, the far end port has entered a G832 Unavailable state. A G832 Far End Unavailable state is entered after ten consecutive G832 Far End Severely Errored Seconds. A G832 Far End Severely Errored Second (FESES) is counted during second intervals containing more than 34 Far End Coding Violations or one or more FERF defects.

A *clear* is issued when the G832 Far End Unavailable state is exited, which occurs after 10 consecutive seconds where no FESES are counted.

Probable Cause

Degraded signal

Type

Communications

Remedial action

Check configuration of this port and the far end port.

7011 5702

Component	Severity	Status
Lp/<num1> E3/<num2>	minor/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - 2

Details

If the status is *set*, this port has entered an G832 Unexpected Payload Type state. A G832 Unexpected Payload Type state is entered when the payload type in the received E3 signal fails to agree with the expected payload type for a period of 2 seconds.

A *clear* is issued when the G832 Unexpected Payload Type state is exited, which occurs when the received payload type agrees with the expected payload type for a period of 10 seconds.

Probable Cause

Protocol error

Type

Communications

Remedial action

Check configuration of this port and the far end port.

7011 5703

Component	Severity	Status
Lp/<num1> E3/<num2>	minor/cleared	set/clear

Legend

<num1> = 1 - 15

<num2> = 0 - 2

Details

If the status is *set*, this port has entered a G832 Trail Trace Mismatch state. A G832 Trail Trace Mismatch state is entered when the trail trace access point identifier in the received E3 signal fails to agree with the expected trail trace access point identifier for a period of 2 seconds.

A *clear* is issued when the G832 Trail Trace Mismatch state is exited, which occurs when the received trail trace access point identifier agrees with the expected trail trace access point identifier for a period of 10 seconds.

Probable Cause

Configuration error

Type

Communications

Remedial action

Check configuration of this port and the far end port.

7011 6500

Component	Severity	Status
Lp/<num1> <type>/<num2>	warning/cleared	set/clear

Legend

<num1> = 0 - 15

<type> = V35, X21 and HSSI

<num2> = 0-n, where n is 1 less than the number of ports supported on the card type used

Details

If the status is *set*, the link is in a *linkMode* different from the one provisioned.

A *clear* is issued when the *linkMode* is changed to be the same as that provisioned.

Probable Cause

Configuration error

Type

Processing

Remedial action

Connect the port to a patch panel that is configured for the expected *linkMode*.

7011 6501

Component	Severity	Status
Lp/<num1> X21/<num2>	warning/cleared	set/clear

Legend

<num1> = 0 - 15

<num2> = 0 - 7

Details

If the status is *set*, the physical termination configuration of the V.11 port is different from that specified in the *terminationRequired* field of the provisioning data.

A *clear* is issued when the *terminationRequired* attribute is changed to be the same as that physically configured.

Note that the card will have to be removed from the shelf for the physical termination configuration to be changed.

Probable Cause

Configuration error

Type

Processing

Remedial action

Check if the provisioning data is correct. If it is, remove the function processor and correct the physical termination configuration.

7011 6600

Component	Severity	Status
Lp/<num1> hssi/<num2>	critical	clear

Legend

<num1>=1-15

<num2> = 0

Details

If the status is *set*, this end dce has received a Local Digital Loopback request from the dte end and enabled the loopback properly. The service and control on this port dce will be suspended.

A *clear* is issued when this end dce has received a Local Digital Loopback request from the dte end and removed the loopback properly, or when this end dce has been put into the Locked state while handling loopback request from dte. The service and control on this port dce will be resumed after the loopback is removed.

Probable Cause

Underlying resource unavailable

Type

Communications

Remedial action

None.

7011 6601

Component	Severity	Status
Lp/<num1> hssi/<num2>	major	clear

Legend

<num1>=1-15

<num2> = 0

Details

If the status is *set*, the on-board dip switch has been closed to convert from the DCE to DTE interface, but the cable is improperly connected or of the wrong type.

A *clear* is issued when the right NT null cable is used or properly connected, or the on-board dip switch is opened (that is, the DCE interface is configured).

Probable Cause

Configuration error

Type

Processing

Remedial action

If the DTE configuration is selected (that is, the on-board dip switch is closed), use the NT null modem cable to connect with the dce properly.

If the DCE configuration is selected, set the on-board dip switch to open position and use the HSSI standard cable.

7011 7000

Component	Severity	Status
<application> Framer	warning/cleared	set/clear

Legend

<application> = Trunk/<instance> Unack,
DpnGateway/<instance> Utp,
Fruni/<instance>

<instance> = a decimal value

Details

If the status is *set*, the value set in the *flagsBetweenFrames* attribute of the *Framer* component is not supported on this FP version. The attribute is set to 1 internally.

A *clear* is issued if the *flagsBetweenFrames* attribute is set to 1.

Probable Cause

Configuration error

Type

Processing

Remedial action

Provision the *flagsBetweenFrames* attribute to 1, or replace the FP. Consult your Nortel Networks technical support group.

7011 7001

Component	Severity	Status
<application> Framer	warning/cleared	set/clear

Legend

<application> = Trunk/<instance> Unack,
DpnGateway/<instance> Utp,
Frdte/<instance>,
Fruni/<instance>

<instance> = a decimal value

Details

If the status is *set*, the value (crc16) set in the *frameCrcType* attribute of this *Framer* component is not recommended on this FP version. Excessive frame errors may result.

A *clear* is issued if the *frameCrcType* attribute is set to crc32 or noCrc.

Probable Cause

Configuration error

Type

Processing

Remedial action

Provision the *frameCrcType* attribute to crc32 or noCrc, or replace the FP. Consult your Nortel Networks technical support group.

7011 7002

Component	Severity	Status
<application> Framer	warning/cleared	set/clear

Legend

<application> = Trunk/<instance> Unack

<instance> = a decimal value

Details

If the status is *set*, the value (interrupting) set in the *framingType* attribute of this *Framer* component is not supported on this FP version. Excessive error may result.

A *clear* is issued if the *framingType* attribute is set to hdlc.

Probable Cause

Configuration error

Type

Processing

Remedial action

Provision the *framingType* attribute to hdlc, or replace the FP. Consult your Nortel Networks technical support group.

7011 7003

Component	Severity	Status
<application> Framer	major/cleared	set/clear

Legend

<application> = Htds/<instance>

<instance> = a decimal value

Details

If the status is *set*, then a Framer error for the current application/service has been detected. Currently, the only service that sets this alarm is HTDS, but other applications/services may use this alarm as well in the future.

Both ends of a Transparent Data Service path must have the *lineSignalTransport* attribute turned on for *lineSignalTransport* to work. This alarm is set when the 2 ends do not match in this respect.

Note that the transparent data portion of this feature is unaffected (only the transparent modem status lead transport part is affected).

A *clear* is issued if the problem indicated has been resolved.

Probable Cause

Degraded signal

Type

Communications

Remedial action

Provision the *lineSignalTransport* attribute to the same value as provisioned on the other end of the HTDS path.

7011 7004

Component	Severity	Status
<application> Framer	major/cleared	set/clear

Legend

<application> = Htds/<instance>

<instance> = a decimal value

Details

If the status is *set*, then a Framer error for the current application/service has been detected. Currently, the only service that sets this alarm is HTDS, but other applications/services may use this alarm as well in the future.

Incompatible VPort pathend configuration is detected. The Transparent Data Service path must be between a DCE-DTE pair for *lineSignalTransport* to work. This alarm is set when the 2 ends don't match in this respect.

Note that the transparent data portion of this feature is unaffected (only the transparent modem status lead transport part is affected).

A *clear* is issued if the problem indicated has been resolved.

Probable Cause

Degraded signal

Type

Communications

Remedial action

Reconfigure the VPort so that the operational attribute *actualLinkMode* is different from the value on the other end of the HTDS path. For example, if the other end of the path is configured as DCE, then the local end must be configured as DTE. If the other end of the path is configured as DTE, then the local end must be configured as DCE.

7011 7005

Component	Severity	Status
<application> Framer	major/cleared	set/clear

Legend

<application> = Htds/<instance>

<instance> = a decimal value

Details

If the status is *set*, then a Framer error for the current application/service has been detected. Currently, the only service that sets this alarm is HTDS, but other applications/services may use this alarm as well in the future.

Incompatible VPort pathend configuration is detected. Both ends of the Transparent Data Service path must be of the same cardType (for example, either both are V35 or both are V11) for *lineSignalTransport* to work. Attempting to run this feature (*lineSignalTransport*) on a non-Vport card (for example, DS1, E1, and so on) will also generate this alarm. This alarm is set when the 2 ends don't match in this respect.

Note that the transparent data portion of this feature is unaffected (only the transparent modem status lead transport part is affected).

A *clear* is issued if the problem indicated has been resolved.

Probable Cause

Degraded signal

Type

Communications

Remedial action

Make sure both ends of the Transparent Data Service path are of the same card type supporting Transparent Modem Status Transport (that is, either both are V35 or both are V11).

7011 7006

Component	Severity	Status
Vs Framer	major	message

Details

Framer service error encountered. Too many ABCD Signal changes for Voice Service. More then 25 ABCD changes per second or more than 450 ABCD changes on a whole link basis.

ABCD Signal Interpreter is disabled.

The ABCD Idle signal is transmitted to the egress/nearend side.

2 seconds later, an ABCD Seize signal is transmitted to the egress/nearend side. This seize is sent for 5 seconds, to prevent further calls from being initiated and to allow the LINK to settle down in case of a temporary noisy LINK.

Following the 5 second settle down period, the channel re-enables its' ABCD CAS signalling events.

Probable Cause

Degraded signal

Type

Communications

Remedial action

An excess of ABCD CAS Signaling changes emanating from an outside source is beyond our control. The excessive signalling has been seen to be a result of Framer Sync errors or Bit errors occurring on the link. Correct link quality.

7011 7007

Component	Severity	Status
Vs Framer	major	message

Details

Framer service error encountered. Too many ABCD Signal changes for Voice Service. More then 25 ABCD changes per second or more than 450 ABCD changes per second on a whole link basis.

ABCD Signal Interpreter is disabled.

The ABCD Idle signal is transmitted to the egress/near-end side.

2 seconds later, an ABCD Seize signal is transmitted to the egress/near-end side. This seize is sent for 5 seconds.This has a dual purpose, one is to prevent further calls to be initiated and second to allow the LINK to settle down in case of a temporary noisy LINK.

This alarm will not re-enable the Signal Interpreter such as alarm 7006. This is due to the fact that it has already gone through 2 re-enables and the problem still persist.

To re-enable the Signal Interpreter, LOCK then UNLOCK the Voice Service Framer.

Probable Cause

Degraded signal

Type

Communications

Remedial action

To re-enable the Signal Interpreter, LOCK then UNLOCK the Voice Service Framer.

An excess of ABCD CAS Signalling changes emanating from an outside source is beyond our control. The excessive signalling has been seen to be a result of Framer Sync errors or Bit errors occurring on the link. Correct link quality.

7011 8000

Component	Severity	Status
Lp/<num1> <type>/<num2>	warning	message

Legend

<num1> = 1 - 15

<num2> = 0 - 2

<type> = DS3, E3, Sonet, Sdh

Details

This warning message is issued to let the user know that the provisioning data that has just been activated will only be put into use when the test is terminated on the specified component.

Probable Cause

Operational Condition

Type

Communications

Remedial action

Stop the test to put the provisioning data in use.

7011 9000

Component	Severity	Status
Lp/<num1> <type>/<num2>	minor	set

Legend

<num1> = 1 - 15

<num2> = 0 - n, where n is one less than the number of ports supported on the card type

<type> = DS1 or E1

Details

There are four conditions under which this alarm is set:

1. Realtime pool is too large in DSP
2. Invalid reply from DSP
3. Timeout in getting a response from DSP stream process
4. Timeout in accessing echo canceller DSP

Probable Cause

Underlying resources unavailable

Type

Communications

Remedial action

1. Report problem to support
2. Reset cards to clear the problem
3. and 4. None. These alarms are provided for information only.

7012 0050

Component	Severity	Status
Shelf	major	set/clear

Details

On bus-based shelves, this alarms indicates that a power converter has failed.

On fabric-based shelves, this alarm indicates that one of the units related to the power supply has failed. This may due to any of the following conditions:

- an external AC rectifier has failed

- a processor card has had a power feed failure

- a breaker module has failed

Once the status changes, it takes approximately 2 minutes for the set or clear alarm to appear.

When the status is clear, the power supplies function correctly.

Probable Cause

Power problem

Type

Equipment

Remedial action

On bus-based shelves, replace the defective power converter.

On fabric-based shelves, examine the *hardwareFailure* attribute of the Shelf component to determine why the alarm was generated. If the attribute does not satisfactorily explain the cause of the alarm, see 241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing* for details on troubleshooting a power supply problem.

7012 0051

Component	Severity	Status
Shelf	major/warning	set/clear

Details

On bus-based shelves, when the severity is set to major, the cooling unit has failed. When the status is clear, the cooling unit functions correctly.

On fabric-based shelves, when the severity is set to major, one or more of the cooling unit fans have failed. When the severity is set to warning, the temperature is higher than normal. When the status is clear, the cooling unit functions correctly and the temperature is within the normal range.

Once the status changes, it takes approximately 2 minutes for the set or clear alarm to appear.

Probable Cause

Equipment malfunction

Type

Equipment

Remedial action

Ensure that the cooling unit is powered and properly inserted before replacing it.

7012 0052

Component	Severity	Status
Shelf	major	set/clear

Details

One or more processor cards have failed. Once the status changes, it takes approximately 2 minutes for the set or clear alarm to appear.

The alarm is also generated when a fabric card has failed.

Probable Cause

Processor/fabric problem, Equipment malfunction

Type

Equipment

Remedial action

Replace the defective processor/fabric cards. The light on a defective processor/fabric card is always red.

7012 0053

Component	Severity	Status
Shelf	major	set/clear

Details

On bus-based shelves, this alarm indicates that the terminator card has failed or the message sent from the terminator card to the CP is corrupted. A clear is issued if the terminator card has sent the message to the CP successfully.

On fabric-based shelves, this alarm indicates that the shelf's MAC address card has failed or has been removed, or the message sent from the MAC address card to the processor cards is corrupted. A clear is issued if the MAC address card has successfully sent the message to the processor cards.

Once the status changes, the set alarm appears only after 24 hours.

Probable Cause

Equipment malfunction, Corrupt data

Type

Equipment

Remedial action

For bus-based shelves, contact your local Nortel Networks technical support group.

For fabric-based shelves, follow the standard maintenance procedure for testing the MAC address card and remove or replace the defective unit(s).

7012 0054

Component	Severity	Status
Shelf	major	message

Details

On bus-based shelves, this alarm indicates that the MAC addresses provided by the terminator card are corrupted.

On fabric-based shelves, this alarm indicates that the MAC addresses provided by the shelf's MAC address card are corrupted, or that the MAC address card was replaced with another MAC address card that supplies a different range of MAC addresses.

Replacement of a MAC address card on a Passport 15000 shelf requires a careful insertion of the new card once the original card has been removed. Therefore, replacing the MAC address card is recommended as the final choice of remedial action after all other attempts to identify the root cause of the alarm have been exhausted.

When the status is *clear*, the MAC addresses provided by the MAC address card are no longer corrupted.

Probable Cause

Equipment malfunction, Corrupt data

Type

Equipment

Remedial action

For bus and fabric-based shelves, contact your local Nortel Networks technical support group.

7012 0055

Component	Severity	Status
Shelf	minor/major	set

Details

This alarm is issued when the MAC address is not available. A minor alarm is issued if it is unavailable when the CP starts up. A major alarm is issued if the MAC address is still unavailable after 4 minutes.

Probable Cause

Equipment malfunction, Timing problem

Type

Equipment

Remedial action

On bus-based shelves, replace the terminator card.

On fabric-based shelves, follow the standard maintenance procedure for testing the MAC address card and remove or replace the defective unit(s).

7012 0056

Component	Severity	Status
Shelf	minor	set/clear

Details

On fabric-based shelves, this alarm indicates that a failure of the Alarm/BITS card has been detected. The Alarm/BITS card is located at the back of the shelf, and is responsible for the generation of audible and visual alarms.

When the status is clear, the Alarm/BITS card is functioning properly.

Probable Cause

Equipment malfunction

Type

Equipment

Remedial action

Follow the standard maintenance procedure for testing the Alarm/BITS card and remove or replace the defective unit(s).

7012 0057

Component	Severity	Status
Shelf	major	set/clear

Details

On bus-based shelves, this alarm indicates that a power converter has failed.

On fabric-based shelves, this alarm indicates that the switch related to the power supply Feed A has tripped. Once the status changes, it takes approximately 2 minutes for the set or clear alarm to appear.When the status is clear, the power supplies function correctly.

Other related alarms are 7012 0103 and 7012 0104.

Probable Cause

Power problem

Type

Equipment

Remedial action

On bus-based shelves, replace the defective power converter.

On fabric-based shelves, examine the *hardwareFailure* attribute of the Shelf component to determine why the alarm was generated. If the attribute does not satisfactorily explain the cause of the alarm, see 241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing* for details on troubleshooting a power supply problem.

7012 0058

Component	Severity	Status
Shelf	major	set/clear

Details

On bus-based shelves, this alarm indicates that a power converter has failed.

On fabric-based shelves, this alarm indicates that the switch related to the power supply Feed B has tripped. Once the status changes, it takes approximately 2 minutes for the set or clear alarm to appear.When the status is clear, the power supplies function correctly.

Other related alarms are 7012 0103 and 7012 0104.

Probable Cause

Power problem

Type

Equipment

Remedial action

On bus-based shelves, replace the defective power converter.

On fabric-based shelves, examine the *hardwareFailure* attribute of the Shelf component to determine why the alarm was generated. If the attribute does not satisfactorily explain the cause of the alarm, see 241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing* for details on troubleshooting a power supply problem.

7012 0100

Component	Severity	Status
Shelf Card/<instance>	minor/critical	set/clear

Legend

<instance> = 0 - 15

Details

This alarm is issued when a card is not capable of running a logical processor (LP). A critical alarm is issued if an LP has been configured to run on the card, or a minor alarm is issued if no LP has been configured to run on the card. Note that no alarm is issued if the Card component's *cardType* attribute has not been set.

Probable Cause

Processor problem

Type

Equipment

Remedial action

No remedial action is needed if this is just a temporary condition (for example, when the card is re-initializing itself). If the condition persists, check the Card component's *availabilityStatus* and *failureCause* attributes for a more specific problem cause.

7012 0101

Component	Severity	Status
Shelf Card/<instance>	indeterminate	message

Legend

<instance> = 0 - 15

Details

This alarm is issued after a card reboots. It holds some diagnostic information (in the comment data field) that specifies why the card went down. Several instances of this alarm can be generated after the card reboots (depending on how much information needs to be displayed). This information is referred to as *Trap Data* information.

Probable Cause

Equipment malfunction

Type

Equipment

Remedial action

Read the *Trap Data* information to determine why the card rebooted. If the reboot reason in the *Trap Data* information does not satisfactorily explain the cause of the reboot, see 241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing* for details on troubleshooting a control processor or function processor crash.

7012 0102

Component	Severity	Status
Shelf Card/<instance>	warning	message

Legend

<instance> = 0 - 15

Details

This alarm is issued when a CP starts running as the active CP. It is issued on initial power up as well as after a CP switchover.

Probable Cause

Response time excessive

Type

Quality of service

Remedial action

None.

7012 0103

Component	Severity	Status
Shelf Card/<instance>	major	set/clear

Legend

<instance> = 0 - 15

Details

When the status is *set* on a processor, one of the units related to power supply has failed. This can result from any of the following:

- the fed -48V falls to less than 39.5V

- a processor interface module has failed, or

- battery A feed failure

Once the status changes, it takes approximately 2 minutes for the set or clear alarm to appear.

When the status is *clear*, the power supplies are functioning correctly.

Other related alarms are 7012 0057 and 7012 0058.

Probable Cause

Power problem

Type

Equipment

Remedial action

Examine the alarm record or the *hardwareAlarm* attribute under the *Shelf Card* component to determine which card is generating the alarm, and replace the defective power converter.

7012 0104

Component	Severity	Status
Shelf Card/<instance>	major	set/clear

Legend

<instance> = 0 - 15

Details

When the status is *set* on a processor, one of the units related to power supply has failed. This can result from any of the following:

- the fed -48V falls to less than 39.5V, or

- a processor interface module has failed.

- battery B feed failure

Once the status changes, it takes approximately 2 minutes for the set or clear alarm to appear.

When the status is *clear*, the power supplies are functioning correctly.

Other related alarms are 7012 0057 and 7012 0058.

Probable Cause

Power problem

Type

Equipment

Remedial action

Examine the alarm record or the *hardwareAlarm* attribute under the *Shelf Card* component to determine which card is generating the alarm, and replace the defective power converter.

7012 0105

Component	Severity	Status
Shelf Card/<instance>	warning	set

Legend

<instance> = 0 - 15

Details

This alarm is issued when a card executes a special script while booting. These scripts are usually not deployed in customer environments.

Probable Cause

Operational condition

Type

Operator

Remedial action

To clear the alarm you must remove the related files and reset the card.

To do this:

Issue the following command to go the bin directory, where the files are located: cd -p(“system/bin”) fs

Issue the following command to know which script files are present:ls fs

To remove the script files, issue either or both of the following commands, according to the result of the previous command: remove -r -f -p(startup.card<instance>) fs or remove -r -f -p(startup.rom.card<instance>) fs then, reset the card that causes the alarm: reset shelf card/<instance>.

7012 0151

Component	Severity	Status
Shelf Card/<instance>	major	message

Legend

<instance> = 0 - 15

Details

The Card component's provisioned card type does not match the inserted card's card type.

Probable Cause

Configuration error

Type

Processing

Remedial action

Replace the card with one of the appropriate type, or update the Card component's *cardType* attribute.

7012 0152

Component	Severity	Status
Shelf Card/<instance>	major	message

Legend
<instance> = 0 - 15

Details
No card is configured for this slot (the Card component's *cardType* attribute has not been set), but a card is present in the slot.

Probable Cause
Configuration error

Type
Processing

Remedial action
Remove the card, or set the Card component's *cardType* attribute.

7012 0153

Component	Severity	Status
Shelf Card/<instance>	major	message

Legend
<instance> = 0 - 15

Details
The card cannot load its software.

Probable Cause
Configuration error

Type
Processing

Remedial action
Replace the card or change the card's software load. The card's software load is determined by the *featureList* attribute of the Logical Processor Type (LPT) component associated with the card's LP.

7012 0154

Component	Severity	Status
Shelf Card/<instance>	major	message

Legend
<instance> = 0 - 15

Details
The card failed its self-test diagnostics.

Probable Cause
Processor problem

Type
Equipment

Remedial action
Replace the card.

7012 0155

Component	Severity	Status
Shelf Card/<instance>	major	message

Legend
<instance> = 0 - 15

Details
Except for enabling its access on the backplane, the card is not responding.

Probable Cause
Processor problem

Type
Equipment

Remedial action
Replace the card.

7012 0156

Component	Severity	Status
Shelf Card/<instance>	major	message

Legend
<instance> = 0 - 15

Details
The card has a backplane connectivity problem.

Probable Cause
Processor problem

Type
Equipment

Remedial action
Replace the card.

7012 0200

Component	Severity	Status
Lp/<instance>	critical	set

Legend

<instance> = 0 - 15

Details

This alarm is issued when the logical processor (LP) is not running. Note that no alarm is issued if the LP is not configured to run on any processor card (that is, when the LP component's *mainCard* and *spareCard* attributes have not been set).

Probable Cause

Underlying resource unavailable

Type

Processing

Remedial action

No remedial action is needed if this is just a temporary condition, for example, when the LP is re-initializing itself. If the condition persists, it is because the LP does not have a working processor card to run on. Clear the problem that is preventing the LP's processor card from being able to run the LP.

7012 0201

Component	Severity	Status
Lp/<instance>	warning	message

Legend

<instance> = 0 - 15

Details

Traffic will be disrupted in {15,10 and 5} minutes caused by an LP switchover to the spare card.

A deferred switchover has been scheduled for this LP. This message is displayed in order to notify the operator that a traffic disruption will occur for this LP. This message will appear three times, once at 15, 10 and 5 minutes, before switchover occurs. Each message indicates the time remaining.

Other related alarms are 7012 0200, 7012 0101 (message alarm for card), and 0000 0000 (hierarchical clear for LP). There are other related alarms generated due to the impact of the active card going down (attribute *Shelf Card standbyStatus* no longer has the value *providingService*) and the standby taking over.

Probable Cause

Operational condition, Underlying resource unavailable

Type

Operator

Remedial action

You can cancel the scheduled switchover with the following command:
switchover -cancel Lp/<instance>

7012 0202

Component	Severity	Status
Lp/<instance>	warning	message

Legend

<instance> = 0 - 15

Details

This alarm is issued to notify the operator that a scheduled LP switchover has failed.

A switchover was attempted for this LP but failed for one of the following reasons, which will be specified in the alarm:

1. A standby logical processor is not available.
2. A control processor software upgrade is currently in progress. (CPs only)
3. The two disks are currently out-of-synch. (CPs only)
4. Provisioning data is loading on the spare CP: <A>% done. (CPs only).

Probable Cause

Operational condition

Type

Operator

Remedial action

For each of the above reasons, respectively, the operator can perform the following:

1. Ensure that attribute *Lp spareCardStatus* is set to “available.” This attribute is automatically set to “available” when the spared card is provisioned and running.
2. Wait for the software upgrade to finish and then try the switchover again.
3. Wait for the disks to get in synch and then try the switchover again.
4. Wait for the provisioning data to be loaded and then try the switchover again.

7012 0203

Component	Severity	Status
Lp/0	warning	message

Legend

<time>: time stamp before outage.

<type of outage>: CP, module, swMigration.

Details

Active CP last time in service: <time> (<type of outage> outage).

This alarm is issued when an outage occurs. The last time that the active CP was in service is displayed.

There are three types of outages: CP, module and software migration. A CP outage indicates that a CP switchover occurred and the FPs may have stayed up. This happens when the conditions for hot standby CP redundancy are met. A module outage indicates that a CP went down and the entire module has gone out of service. This indicates that hot standby CP redundancy has been disabled or that the corresponding conditions for hot standby CP redundancy have not been met. A software migration outage indicates that a software migration switchover occurred.

Probable Cause

Processor problem

Type

Equipment

Remedial action

No remedial action is required. This information is used off-switch to calculate the duration of the outage.

7012 0204

Component	Severity	Status
Lp/<instance>	warning	message

Legend

<instance> = 0 - 15

Details

This LP cannot achieve its expected Migration-Switchover behavior. Refer to Prov Migration alarm for more details.

At the start of a software migration activation a response is generated indicating which LPs do not support the reduced service outage during software migration. This is based on operational and provisionable conditions.

This alarm is issued for an LP not identified in the response, whose operational conditions change during the software migration such that it can no longer support the reduced service outage. This alarm is issued when the FPs destined for the migration shelf are chosen.

Probable Cause

Operational condition

Type

Operator

Remedial action

If deemed appropriate, the software migration activation can be stopped by issuing the stop provisioningSystem command while in provisioning mode.

7012 0300

Component	Severity	Status
Shelf Card/<n> SparedServices	warning/critical	message

Legend

<n> = instance value of shelf card

Details

This alarm indicates that one of the standby service instances on the parent Card has encountered a condition which the user should be made aware of.

The standby service has likely encountered one of the following:

- a software error
- an engineering/resource limit reached
- an application-specific problem

If the standby service is unable to provide standby capability as a result, the severity is critical. This degrades the potential for a complete equipment protection switchover and an alarm (also against SparedServices) tracks the outstanding condition from the Preside Multiservice Data Manager perspective.

If the condition does not affect the ability to provide standby capability, the severity is warning.

The comment text contains the following information about the service which initiated the alarm coming out:

- ComponentName
- DateAndTime
- ActiveListStatus
- PerceivedSeverity
- AlarmType
- ProbableCause
- NTPIndex
- NotificationId
- CommentData

- FileInformation

Probable Cause
Software error, Resource at or nearing capacity, Application subsystem

Type
Processing

Remedial action
Look up the NTPIndex from the Comment text and perform its remedial action.

7012 0301

Component	Severity	Status
Shelf Card/<n> SparedServices	warning/cleared	set/clear

Legend

<n> = instance value of shelf card

Details

If the status is *set*, at least one of the standby service instances on the parent Card has been unable to provide standby capability, thus degrading the potential for a complete equipment protection switchover. Look for a previously issued 7012 0300 alarm (also against SparedServices) which could indicate more details.

A clear is issued after all standby service instances are once again able to provide standby service.

Note that during a standby card initialization, including HSM, the status can be set and cleared within a few seconds without alarm 7012 0300 being generated.

Probable Cause

Application subsystem

Type

Processing

Remedial action

If the status is set, the action to take is really based on the information in previously issued 7012 0300 alarms.

7013 0000

Component	Severity	Status
Lp/<instance>	minor/cleared	set/clear

Legend

<instance> = 0 - 15

Details

If the status is *set*, available shared memory for the logical processor (LP) has decreased below 12.5%. The LP is experiencing an unbalanced traffic flow resulting in high queueing delays and shared memory depletion. This alarm is set to warn of impending shared memory exhaustion.

A *clear* is issued when available shared memory for the LP has increased above 18.75%.

Probable Cause

Type

Remedial action

Frequent or prolonged occurrences of this condition indicate that re-engineering is required in order to balance the flow of traffic through this LP, thus reducing the amount of traffic congestion and length of queueing delays.

7013 0001

Component	Severity	Status
Lp/<instance>	major/cleared	set/clear

Legend

<instance> = 0 - 15

Details

If the status is *set*, available shared memory for the logical processor (LP) has decreased below 6.25%. The LP is experiencing an unbalanced traffic flow resulting in high queueing delays, and is approaching shared memory exhaustion. In the case of the control processor (that is, Lp/0), the alarm indicates that resources are being held up on the CP.

When this condition is detected, the largest shared memory traffic queues are purged automatically until available shared memory for the LP has increased above 9.39%. A *clear* is issued at this point.

Probable Cause

Threshold crossed

Type

Quality of service

Remedial action

Frequent or prolonged occurrences of this condition indicate that re-engineering must be performed to balance the flow of traffic through this LP and reduce the amount of traffic congestion and length of queueing delays.

7013 0002

Component	Severity	Status
Lp/<instance>	warning/cleared	set/clear

Legend

<instance> = 0 - 15

Details

If the status is *set*, the available ingress cell-blocks from the logical processor (LP) have decreased below 20% of total ingress cell-blocks. Under this condition, traffic flowing across this FP may encounter high queueing delays.

When this condition is detected, the less priority traffic will be discarded first. If the congestion still persists, even higher priority traffic will be discarded. This continues until available ingress cell-blocks for the LP have increased above 25% of total ingress cell-blocks. A *clear* is issued at this point. A filtering mechanism is implemented such that a set/clear is issued by one minute.

Probable Cause

Threshold crossed

Type

Quality of service

Remedial action

Frequent or prolonged occurrences of this condition indicate that re-engineering is required to balance the flow of traffic through this card in order to reduce the amount of traffic and the length of queues.

7013 0003

Component	Severity	Status
Lp/<instance>	warning/cleared	set/clear

Legend

<instance> = 0 - 15

Details

If the status is *set*, the available ingress frame-blocks from the logical processor (LP) have decreased below 20% of total ingress frame-blocks. Under this condition, traffic flowing across this FP may encounter high queueing delays.

When this condition is detected, the less priority traffic will be discarded first. If the congestion still persists, even higher priority traffic will be discarded. This continues until available ingress frame-blocks for the LP have increased above 25% of total ingress frame-blocks. A *clear* is issued at this point. A filtering mechanism is implemented such that a set/clear is issued by one minute.

Probable Cause

Threshold crossed

Type

Quality of service

Remedial action

Frequent or prolonged occurrences of this condition indicate that re-engineering is required to balance the flow of traffic through this card in order to reduce the amount of traffic and the length of queues.

7013 0004

Component	Severity	Status
Lp/<instance>	warning/cleared	set/clear

Legend

<instance> = 0 - 15

Details

If the status is *set*, the available egress cell-blocks from the logical processor (LP) have decreased below 20% of total egress cell-blocks. Under this condition, traffic flowing across this FP may encounter high queueing delays.

When this condition is detected, the less priority traffic will be discarded first. If the congestion still persists, even higher priority traffic will be discarded. This continues until available egress cell-blocks for the LP have increased above 25% of total egress cell-blocks. A *clear* is issued at this point. A filtering mechanism is implemented such that a set/clear is issued by one minute.

Probable Cause

Threshold crossed

Type

Quality of service

Remedial action

Frequent or prolonged occurrences of this condition indicate that re-engineering is required to balance the flow of traffic through this card-reducing the amount of traffic and length of queues.

7013 0005

Component	Severity	Status
Lp/<instance>	warning/cleared	set/clear

Legend

<instance> = 0 - 15

Details

If the status is *set*, the available egress frame-blocks from the logical processor (LP) have decreased below 20% of total egress frame-blocks. Under this condition, traffic flowing across this FP may encounter high queueing delays.

When this condition is detected, the less priority traffic will be discarded first. If the congestion still persists, even higher priority traffic will be discarded. This continues until available egress frame-blocks for the LP have increased above 25% of total egress frame-blocks. A *clear* is issued at this point. A filtering mechanism is implemented such that a set/clear is issued by one minute.

Probable Cause

Threshold crossed

Type

Quality of service

Remedial action

Frequent or prolonged occurrences of this condition indicate that re-engineering is required to balance the flow of traffic through this card-reducing the amount of traffic and length of queues.

7013 0011

Component	Severity	Status
Lp/<instance>	minor/cleared	set/clear

Legend

<instance> = 0 - 15

Details

If the status is *set*, available shared memory for the logical processor (LP) has fallen below 25%. The LP is experiencing an unbalanced traffic flow resulting in high queueing delays and shared memory depletion. This alarm is set to warn of FCI bit setting in packet header of data traffic and possible discard of data packets tagged as low, medium, and high discard priority. In the case of the control processor, which is Lp/0, this alarms indicates that resources are being held up on the CP.

A *clear* is issued when available shared memory for the LP has exceeded 25% after one minute.

Probable Cause

Threshold crossed

Type

Quality of service

Remedial action

Frequent or prolonged occurrences of this condition indicate that re-engineering is required in order to balance the flow of traffic through this LP, thus reducing the amount of traffic congestion and length of queueing delays, and preventing discard of data traffic. In the case of the CP, determine which services are holding up resources on t he CP, and take appropriate action.

7013 0021

Component	Severity	Status
Lp/<instance>	major/cleared	set/clear

Legend

<instance> = 0 - 15

Details

If the status is *set*, available message blocks in local memory for the logical processor (LP) has decreased below 6.25%. Local message blocks are used for local control messaging on the card. The LP is experiencing an unbalanced control message traffic flow resulting in high queuing delays, and is approaching local memory exhaustion.

As long as this level of congestion persists, some of the lower priority subsequent control activities on the LP will not be performed due to insufficient resources.

One minute after the set alarm has been issued, a *clear* is issued if the available message blocks in local memory have increased above 6.25%.

Probable Cause

Threshold crossed

Type

Quality of service

Remedial action

Frequent or prolonged occurrences of this condition indicate that re-engineering is required. Contact your local Nortel Networks technical support group, if necessary.

7014 0000

Component	Severity	Status
Lp/<instance>	minor/cleared	set/clear

Legend

<instance> = 0 - 15

Details

If the status is *set*, available memory for the logical processor (LP) has decreased below a threshold of 960 Kbytes of the memory on a control processor and 160 Kbytes of the memory on a function processor. Various systems will avoid allocating memory.

A *clear* is issued when available memory for the LP has increased above the clear threshold, which is 1010 Kbytes on a control processor and 180 Kbytes on a function processor.

Probable Cause

Threshold crossed

Type

Quality of service

Remedial action

Frequent or prolonged occurrences of this condition indicate that re-engineering is required in order to balance the memory consumption of the applications on this LP. Contact your local Nortel Networks technical support group for assistance if necessary.

7014 0001

Component	Severity	Status
Lp/<instance>	major/cleared	set/clear

Legend

<instance> = 0 - 15

Details

If the status is *set*, available memory for the logical processor (LP) has decreased below a threshold of 400 Kbytes of the memory on a control processor and 40 Kbytes of the memory on a function processor. Only critical systems will allocate memory. This condition must be resolved quickly because a total exhaustion of memory will result in the automatic resetting of the card.

A *clear* is issued when available memory for the LP has increased above the clear threshold, which is 480 Kbytes on a control processor and 60 Kbytes on a function processor.

Probable Cause

Threshold crossed

Type

Quality of service

Remedial action

Frequent occurrences of this condition indicate that re-engineering is required in order to balance the memory consumption of the applications on this LP. Contact your local Nortel Networks technical support group for assistance if necessary.

7014 0010

Component	Severity	Status
Lp/<instance>	minor/cleared	message

Legend

<instance> = 0 - 15

Details

If the status is *set*, available **high-speed** memory for the logical processor (LP) has decreased below a threshold of 8 Kbytes of the memory on a processor. Various systems will avoid allocating **high-speed** memory.

A *clear* is issued when available **high-speed** memory for the LP has increased above the clear threshold, which is 10 Kbytes of the **high-speed** memory on the processor.

Probable Cause

Threshold crossed

Type

Quality of service

Remedial action

Frequent or prolonged occurrences of this condition indicate that re-engineering is required in order to balance the memory consumption of the applications on this LP. Contact your local Nortel Networks technical support group for assistance if necessary.

7014 0011

Component	Severity	Status
Lp/<instance>	major/cleared	message

Legend

<instance> = 0 - 15

Details

If the status is *set*, available **high-speed** memory for the logical processor (LP) has decreased below a threshold of 4 Kbytes of the **high-speed** memory on a processor. Only critical systems will allocate additional memory. This condition should be resolved quickly because a total exhaustion of memory will result in degraded service.

A *clear* is issued when available **high-speed** memory for the LP has increased above the clear threshold, which is 6 Kbytes of the **high-speed** memory.

Probable Cause

Type

Remedial action

Frequent occurrences of this condition indicate that re-engineering is required in order to balance the memory consumption of the applications on this LP. Contact your local Nortel Networks technical support group for assistance if necessary.

7015 0000

Component	Severity	Status
Time	major/cleared	set/clear

Details

Module stops time synchronization with network time server

The status is *set* when Passport loses synchronization with the network time server. This happens when the network time server is not responding to the Passport's XNTP request.

Module starts time synchronization with network time server

A *clear* is issued when Passport starts synchronizing with the network time server, because Passport is now getting XNTP responses from the time server.

Probable Cause

Remote transmission error

Type

Environmental

Remedial action

Ensure that the network time server is running as a proper stratum time server and that the time server is reachable from the Passport.

7015 0001

Component	Severity	Status
Time	warning	message

Details

This alarm is issued when the network time has changed by more than one minute. The network time may change after synchronizing the module to the network or when the operator sets the time manually.

Probable Cause

Operational condition, Network server intervention, Unknown

Type

Operator, Environmental, Unknown

Remedial action

No action is required.

7015 0002

Component	Severity	Status
Time	Major/cleared	set/clear

Details

If the status is *set*, the time difference between the Passport UTC (moduleTime minus offset) and the network time server is greater than 1000 seconds.

The synchronization status of Passport XNTP is changed to unsynchronized and the main server is set to NULL. This allows the operator to correct the time by setting the moduleTime manually.

A *clear* is issued when the network time is corrected to within 1000 seconds of the network time server.

Probable Cause

Remote transmission error

Type

Environmental

Remedial action

Check the time of the network time servers and the time of Passport module, and correct the time manually by setting the moduleTime of the Passport module. After a few minutes, the Passport XNTP synchronizes with the network time server.

7015 0010

Component	Severity	Status
Time Sever/<n>	minor/clear	set/clear

Legend

<n> = 1 - 10

Details

The Server is disabled.

The status is *set* when the Passport XNTP fails to register an XNTP UDP port with vrIP at startup time. When Passport XNTP fails to register an XNTP UDP port with vrIP, and the ipStack of the network time server is provisioned to be vrIp, the network time server is disabled. Passport XNTP stops time synchronization with the network time server.

The Server is enabled

A *clear* is issued when Passport XNTP successfully registers an XNTP UDP port with vrIp. Passport XNTP starts to synchronize with the network time server.

Probable Cause

Communications subsystem failure

Type

Communications

Remedial action

Check the status of vrIp, to see if they are running correctly. Correct the errors if found. Passport XNTP tries to register with vrIp every 10 minutes until it succeeds.

7015 0011

Component	Severity	Status
Time Sever/<n>	minor/clear	set/clear

Legend

<n> = 1 - 10

Details

No response from the time server, the server is idle.

The status is *set* if Passport XNTP does not receive any packets from the network time server after it sends 8 packets to the network time server. This may be due to one of the following reasons:

1.Network error

The provisioned network time server does not exist, or a network error occurs prevents Passport XNTP from receiving any packets from the network time server.

2.Server configuration error

The network time server's configuration prevents this module from acting as a client to synchronize its time with the network time server.

3.Protocol error

The version of the XNTP running on the network time server is not compatible with Passport XNTP version, so that the network time server does not reply to the Passport XNTP time synchronization request.

Get response from the server, the Server is active.

A *clear* is issued when the error(s) listed above are corrected, and Passport XNTP receives responses from the network time server.

Probable Cause

Communications subsystem failure

Type

Communications

Remedial action

Check the existence and connectivity of the network time server and take the appropriate action.

7015 0012

Component	Severity	Status
Time Sever/<n>	minor/clear	set/clear

Legend

<n> = 1 - 10

Details

Module does not communicate with this network time server correctly.

The status is *set* when the network time server is not selected as one of the network time synchronization sources, although its OSI state is “unlocked”, “enabled” and “active”. This may be due to one of the following reasons:

- The network time server itself is not synchronized.

- The network time server’s stratum is higher than Passport XNTP’s stratum.

Module starts to communicate with this network time server correctly.

A *clear* is issued when the above errors are corrected and the network time server is selected as one of the time synchronization sources of this module.

Probable Cause

Remote transmission error

Type

Communications

Remedial action

Check the status, stratum, leap, and other XNTP protocol information of XNTP running on the network time server and correct any errors if found.

7016 1000

Component	Severity	Status
Fdcr	minor	message

Details

This alarm is issued if the FDCR cannot register a dynamic or static DNA requested by an application process, because another application process already either statically owns a DNA which is the subset/superset/same DNA of the specified DNA or dynamically owns a DNA which is the subset/superset DNA of the specified DNA.

Probable Cause

Type

Remedial action

Verify that the DNA statically provisioned for one of the Passport application processes does not clash with the DNA dynamically configured at the other application process.

7017 1000

Component	Severity	Status
NS	minor/cleared	set/clear

Details

If the status is *set*, a reference has been provisioned and the CP is not synchronized to the reference.

A *clear* is issued if no references are provisioned and the CP is currently free running or if the CP is synchronized to the incoming reference.

Probable Cause

Degraded signal

Type

Communications

Remedial action

The PLL algorithm should resynchronize the clock. However, if the alarm is not cleared after an hour of being set, the clocking source is probably unreliable and a new clocking source should be provisioned.

7017 1001

Component	Severity	Status
NS	warning	message

Details

Indicates a change in Synchronization Status Message (SSM) on the Active or Standby timing reference.

Probable Cause

SSM change reported from timing reference.

Type

Quality of service.

Remedial action

This alarm is for information only. If the reference is persistently reporting a degraded SSM quality level, it may be necessary to re-engineer the network timing distribution.

7018 0001

Component	Severity	Status
Trk/<num> Pa	warning	message

Legend

<num> = 0 - 65535

Details

This *Path Administrator* component has been provisioned with a *maxLc* value which is less than the value provisioned on the adjacent *Path Administrator* component running on the neighbor module. The neighbouring *Path Administrator* component will generate alarm 7018 0002.

Probable Cause

Type

Remedial action

Initially none because the *Path Administrator* components will resolve this conflict by choosing the smaller of the two provisioned *maxLc* values. Since both *Path Administrator* components resolve the conflict in the same manner, the *maxLc* values actually used will be the same at both ends. The resulting value can be seen in the *negotiatedMaxLc* operational attribute.

Some time in the future, reprovision one of the *Path Administrator* components so that its *maxLc* attribute agrees with its neighbor *Path Administrator* component.

7018 0002

Component	Severity	Status
Trk/<num> Pa	warning	message

Legend

<num> = 0 - 65535

Details

This *Path Administrator* component has been provisioned with a *maxLc* value which is greater than the value provisioned on the adjacent *Path Administrator* component running on the neighbor module. The neighbouring *Path Administrator* component will generate alarm 7018 0001.

Probable Cause

Type

Remedial action

Initially none because the *Path Administrator* components will resolve this conflict by choosing the smaller of the two provisioned *maxLc* values. Since both *Path Administrator* components resolve the conflict in the same manner, the *maxLc* values actually used will be the same at both ends. The resulting value can be seen in the *negotiatedMaxLc* operational attribute.

Some time in the future, reprovision one of the *Path Administrator* components so that its *maxLc* attribute agrees with its neighbor *Path Administrator* component.

7018 0003

Component	Severity	Status
Trk/<num> Pa	minor	message

Legend

<num> = 0 - 65535

Details

The *Path Administrator* component is unable to allocate enough high speed memory for all of the logical channels it is being asked to support. This happens when the value of the *maxLc* attribute for one or more of the *Path Administrator* components on a particular card is excessively large.

Probable Cause

Type

Remedial action

If the operator does not change the value of the *maxLc* attribute, the *Path Administrator* component will place all of the logical channels into slower memory where they will work, albeit more slowly. This will cause a noticeable reduction in trunk throughput.

Review the value of the *maxLc* attribute for each *Path Administrator* component on the card and make sure that none is larger than necessary.

7018 0004

Component	Severity	Status
Trk/<num> Pa	critical/cleared	set/clear

Legend

<num> = 0 - 65535

Details

The Path Administrator component is unable to allocate enough high or low speed memory for all of the logical channels it is being asked to support. This happens when the value of the *maxLc* attribute for one or more of the *Path Administrator* components on a particular card is excessively large.

As a result of this problem this *Path Administrator* component will not come up and hence will be unable to support path-oriented traffic.

Probable Cause

Type

Remedial action

Review the value of the *maxLc* attribute for each *Path Administrator* component on the card and make sure that none is larger than necessary. If you still find you have insufficient memory to support the number of channels you require, one or more of the trunks may have to be moved to a separate card.

7018 0007

Component	Severity	Status
Trk/<instance>	major/cleared	set/clear

Legend

<instance> = 0

Details

If the status is *set*, the PA subcomponent of this Trk/<instance> is not up. The PA was unable to stage with it's peer PA due to excessive retries and has given up. The Trk will go up and be able to carry connectionless traffic but will be unable to carry path oriented traffic until the alarm is cleared. There are two common causes of this alarm. Either there is no PA component provisioned under the peer Trk or the peer trunk was lock forced and unlocked very rapidly. A rapid lock force/unlock can cause the PA to be unable to stage with its peer. For this reason it is best only to issue an unlock on a Trk after the Trk has responded to the lock force with the locked *set* alarm.

A *clear* is issued when the PA is able to restage with its peer or when the PA and/or Trk component are deleted.

Probable Cause

Type

Remedial action

Check to ensure that a PA is provisioned at the far end under the peer Trk component. If this is not the problem then it is likely that the trunk was lock forced and unlocked in rapid succession. A rapid lock force/unlock is not recommended and the operator should wait until the trunk sets its locked alarm before issuing the unlock. (We plan to remove this restriction in a later release).

7018 0009

Component	Severity	Status
Trk/<num> Pa	minor/cleared	set/clear

Legend

<num> = 0 - 65535

Details

This Path Administrator component has been provisioned with an AtmAccess subcomponent which is provisioned for a mode that is different than the Path Administrator's peer AtmAccess subcomponent. One Path Administrator was provisioned for mapped mode and the other for multiplexed mode.

Probable Cause

Type

Remedial action

Initially none because the Path Administrators will resolve this conflict by ignoring the fact they were provisioned with an AtmAccess subcomponent. That is, all traffic will be routed over the parent trunk's AAL5 VCC.

Some time in the future, one of the Path Administrators should be reprovisioned such that it's mode agrees with its peer's mode.

7018 0010

Component	Severity	Status
Trk/<num> Pa	minor/cleared	set/clear

Legend

<num> = 0 - 65535

Details

The *Path Administrator* component has been provisioned with an *AtmAccess* subcomponent which is connected to another *Path Administrator*'s *AtmAccess* subcomponent, but that *Path Administrator* component is not this *Path Administrator* component's peer. That is, the two *Path Administrator* components do not belong to the same parent trunk.

Probable Cause

Type

Remedial action

Initially none because this *Path Administrator* component will resolve the problem by ignoring the fact it was provisioned with an *AtmAccess* subcomponent. That is, all traffic will be routed over the parent trunk's AAL5 VCC.

Reprovision this *Path Administrator* component or its peer *Path Administrator* component such that their *AtmAccess* subcomponents can connect.

7018 0011

Component	Severity	Status
Trk/<num> Pa	minor/cleared	set/clear

Legend

<num> = 0 - 65535

Details

This *Path Administrator* component has been provisioned with an *AtmAccess* subcomponent which is not connected to the peer *Path Administrator* component's *AtmAccess* subcomponent.

Probable Cause

Type

Remedial action

Initially none because the *Path Administrator* components will resolve the problem by ignoring the fact it was provisioned with an *AtmAccess* subcomponent. That is, all traffic will be routed over the parent trunk's AAL5 VCC.

Reprovision this *Path Administrator* component or its peer *Path Administrator* component such that their *AtmAccess* subcomponents can connect.

7018 0012

Component	Severity	Status
Trk/<num> Pa	minor/cleared	set/clear

Legend

<num> = 0 - 65535

Details

This *Path Administrator* component is provisioned with an *AtmAccess* subcomponent which is in mapped mode but there are insufficient VCCs available in the VP of the parent trunk's VCC to support the negotiated number of logical channels.

When the *Pa* component comes up it will look at the *AtmIf/n Ca* and *AtmIf/n ConnMap* components to determine the size and offset of the auto selected (dynamic) VCC space for this VP. It then exchanges this information with its peer *Pa* component. The two *Pa* components then compute the overlap in the two rectangles and restrict their allocation of VCC's to this rectangle. This alarm indicates that the computed overlapping rectangle is not large enough to support maxLc+10 channels. (The extra 10 channels are required for bumping and clash resolution).

Probable Cause

Type

Remedial action

Initially none because the Path Administrators will resolve this conflict by ignoring the fact they were provisioned with an AtmAccess subcomponent. That is, all traffic will be routed over the parent trunk's AAL5 VCC.

Some time in the future either the VCC space for this VP needs to be increased to support maxLc+10 VCIs past the *minAutoSelect* (dynamic) threshold or *maxLc* needs to be decreased to fit.

7018 0013

Component	Severity	Status
Trk/<num> Pa	minor/cleared	set/clear

Legend

<num> = 0 - 65535

Details

This alarm is issued by a *Trunk/n* with a *PathAdmin* component. The alarm can be *set* only if the *maxAdaptationLevel* of *Trunk/n PathAdmin* has a non-zero value.

If the status is *set*, the trunk utilization has exceeded the *level1* value specified by *adaptationThreshold* for the period of time specified by the *set* value of *adaptationHoldOffTime*, and PORS adaptation is now active, whereby calls are prevented from being established over the trunk.

A *clear* is issued, when the trunk utilization has subsequently fallen back to a level at or below the *level1* value specified by *adaptationThreshold* for the period of time specified by the *clear* value of *adaptationHoldOffTime*, PORS adaptation is no longer active, whereby new calls are allowed to be established over the trunk.

Probable Cause

Type

Remedial action

The alarm indicates that the trunk has sustained high utilization. When the alarm is issued, PORS prevents new connections from being established over the trunk, which helps to prevent the trunk getting more highly utilized. If the alarm is issued over a relatively short period of time, it may be an indication that the threshold setting is too low. If so, adjust the threshold accordingly. If the threshold setting is already high, the alarm is also issued, and it takes a relatively long time to clear the alarm, re-engineering the links or VCCs on this node may be needed in order to alleviate the high utilization condition.

7018 0014

Component	Severity	Status
Trk/<num> Pa	minor/cleared	set/clear

Legend

<num> = 0 - 65535

Details

This *Path Administrator* component has been provisioned with a value that does not match with the value provisioned on the adjacent Path Administrator component running on the neighbor module. The neighboring Path Administrator component will generate the same alarm.

Probable Cause

Type

Remedial action

Initially none because the Path Administrator components will resolve this conflict by choosing the correct value of the two provisioned values. Since both Path Administrator components resolve the conflict in the same manner, the values actually used will be the same at both ends. Some time in the future, reprovision one of the Path Administrator components so that its attribute agrees with its neighbor Path Administrator component.

7018 1001

Component	Severity	Status
<component_name>/<instance> LCo	critical	message

Legend

<component_name> = component of system that is using the path oriented routing virtual circuit

<instance> = a decimal value

Details

The *PermanentLogicalConnection* subcomponent of this service component specifies a *remoteName* attribute which does not match the name of the component which is attempting to establish a connection with it. This results in rejection of the call request and the service failing to come up.

Probable Cause

Type

Remedial action

Verify that the *remoteName* attribute of the PLC of this service matches the name of the component that is trying to connect to it and vice versa. Make sure that you use short forms for the names of the components in the *remoteName* attribute string.

7018 1002

Component	Severity	Status
<component_name>/<instance> LCo	critical	message

Legend

<component_name> = component of system that is using the path oriented routing virtual circuit

<instance> = a decimal value

Details

The *PermanentLogicalConnection* subcomponent of this service component specifies a *remoteName* attribute which refers to the same parent service component. This results in rejection of the call request and the service failing to come up.

Probable Cause

Type

Remedial action

You must reprovision the service component's PLC subcomponent to have a *remoteName* that does not refer to the parent service. Remember, the remoteName gives the full name of the component that you want to connect to including the module name on which that component resides.

7018 1003

Component	Severity	Status
<component_name>/<instance> LCo	warning	message

Legend

<component_name> = component of system that is using the path oriented routing virtual circuit

<instance> = a decimal value

Details

The *LogicalConnection* (*LCo*) subcomponent of this service component has detected that one or more provisional attributes at the called end of the connection differs in value from the calling end. This alarm only appears on the called end of the connection. The calling end values will be used until the connection is terminated. When this alarm occurs it indicates that the *LCo* operational attributes would differ depending on which end established the connection. This alarm is suppressed when a PLC does not have a *remoteName* attribute specified on both ends of the connection.

Probable Cause

Type

Remedial action

You must reprovision the service component's *PLC* subcomponent to have identical attributes at both ends. This ensures that for whichever end establishes the connection, the operational attribute will be consistent and that re-connection can occur from both ends of the *LCo*. This makes re-connection more robust. The alarm indicates all attributes that require reprovisioning.

7018 1004

Component	Severity	Status
<component_name>/<instance> LCo	minor	message

Legend

<component_name> = component of system that is using the path oriented routing virtual circuit

<instance> = a decimal value

Details

The *LogicalConnection* (*LCo*) subcomponent of this service has received a set overrideRemoteName command while the *remoteName* component of the PLC is non-blank. This prevents accidental overriding.

Probable Cause

Type

Remedial action

You must reprovision the service component's *PLC remoteName* attribute to blank to use the overrideRemoteName set command.

7018 1005

Component	Severity	Status
<component_name>/<instance> LCo	critical	message

Legend

<component_name> = component of system that is using the path oriented routing virtual circuit

<instance> = a decimal value

Details

The *LogicalConnection* (*LCo*) subcomponent of this service attempted to send a packet through its data path to measure the round trip delay of the path. The packet experienced a problem somewhere along the data path and never made it through the path. After several attempts to resend the packet, the *LCo* subcomponent was forced to bring the control path and data path down. The data path's integrity is considered compromised if a round trip delay packet cannot get through, and other data packets will also be affected.

The problem experienced by the path gather packet is most likely due to severe congestion somewhere along the control path. It could also be due to the fact that a hop along the data path is in mapped mode and using VP = 0, but this VP is not a point-to-point connection.

Probable Cause

Type

Remedial action

After the control path and data path go down, the *LCo* component will automatically try to re-establish the paths. If the problem recurs, the data path should be checked for congestion, hop by hop. If there is no congestion along the data path, ensure that for any hop along the data path that is in mapped mode and using VP = 0, the VP is a point-to-point connection.

7018 1006

Component	Severity	Status
<component_name>/<instance> LCo	critical	message

Legend

<component_name> = component of system that is using the path oriented routing virtual circuit

<instance> = a decimal value

Details

The *Logical Connection* (*LCo*) subcomponent of this service attempted to send a packet through its control path to gather the names of nodes and trunks along the path. The packet experienced a problem somewhere along the control path and never made it through the path. After several attempts to resend the packet, the *LCo* subcomponent was forced to bring the control path and data path down. The control path's integrity is considered compromised if a path gather packet cannot get through, as other control packets such as path clear will also be affected.

The problem experienced by the path gather packet is most likely due to severe congestion somewhere along the control path. It could also be due to the fact that a hop along the control path is in mapped mode and using VP = 0, but this VP is not a point-to-point connection.

Probable Cause

Type

Remedial action

After the control path and data path go down, the *LCo* component will automatically try to re-establish the paths. If the problem recurs, the control path should be checked for congestion, hop by hop. If there is no congestion along the control path, ensure that for any hop along the control path that is in mapped mode and using VP = 0, the VP is a point-to-point connection.

7018 2001

Component	Severity	Status
<component_name>/<instance> <LCOorPa>	warning	message

Legend

<component_name> = Trk or component of system that is using the path oriented routing virtual circuit.

<instance> = a decimal value

<LCOorPa> = LCO or Pa

Details

PORS detects an incorrect LRC value in one of its received control messages.

Probable Cause

Type

Remedial action

No action is required. Contact Nortel Networks global support only if this alarm appears frequently.

7018 2002

Component	Severity	Status
<component_name>/<instance>	warning	message

Legend

<component_name> = component of system that is using the path oriented routing virtual circuit

<instance> = a decimal value

Details

This alarm is raised when PORS detects an incorrect or unexpected message.

Probable Cause

Type

Remedial action

No action is required. Contact Nortel Networks global support if this alarm appears frequently.

7018 2003

Component	Severity	Status
<component_name>/<instance> <pid>	critical	message

Legend

<component_name> = Btds, Htds or Vs

<instance> = a decimal value

<pid> = processID of the component

Details

This happens when the attribute localAddress under subcomponent Plc is provisioned, but porsApi is deleted from the Sw Lpt's featureList.

Probable Cause

Type

Remedial action

Add porsApi to the feature list of the appropriate Sw Lpt.

7018 2004

Component	Severity	Status
Rtg Rs	warning	message

Details

In manual mode, component *Routing RouteSelector* (*Rtg Rs*) lets you modify the parameters in the route request data and initiate route selection using this route request data. This alarm is raised by component *Rtg Rs* in manual mode when an invalid destination attribute has been set.

Probable Cause

Incorrect provisioning

Type

Remedial action

Reprovision the destination attribute in component *Rtg Rs* with the correct address format. The destination attribute accepts the following address formats:

1) Node name, component name: “EM/NodeName Vs/N”
2) Node ID, component name: “NID/NodeId VRoute/N”
3) NSAP address: “NSAP/451234”

7019 0001

Component	Severity	Status
<component_name>/<instance>	major/cleared	set/clear

Legend

<component name> = A Vs, Btds or Htds component.

<instance> = a decimal value

Details

The *LogicalConnection* (*LCo*) subcomponent of the service is not up so that the service can not transmit or receive data across the network. The service is not providing service to the subscriber.

Probable Cause

Type

Remedial action

Look at the *LogicalConnection* (*LCo*) subcomponent for clues as to why the connection is not up. Verify that the *Permanent Logical Connection* (*PLC*) component's attributes are correct and compatible with the far end. Ensure that sufficient bandwidth is available in the network for the connection to establish.

7019 0002

Component	Severity	Status
<Shelf_Card>/<instance>	critical	message

Legend
< instance> = 0-15

Details
A feature is provisioned which is not supported by the vintage of this voice card.

Probable Cause

Type

Remedial action
Contact your Nortel Networks technical support group.

7020 0001

Component	Severity	Status
Vr/<string1> Pp/<string2>	warning	message

Legend

< string1> = name of the virtual router

<string2> = name of the protocol port

Details

This alarm indicates that IP Accounting data could not be retrieved from the media specified in the alarm text within the expected time interval. This implies that IP Accounting records will not be generated for this protocolPort (Pp) component for the current collection period.

Probable Cause

There may be message block congestion or heap exhaustion on:

- the CP
- LPs forwarding traffic for this Pp

Type

Processing

Remedial action

Frequent occurrences of this condition indicate that re-engineering is required to balance the memory block and/or heap consumption of applications on the CP and/or LPs forwarding traffic for this Pp. Contact your local Nortel Networks technical support group for assistance, if necessary.

7021 0000

Component	Severity	Status
Vr/<string> Ip	warning	message

Legend

<string> = name of the virtual router

Details

Lp is out of memory. Ip service is restarted with all the provisioned data. If more memory is not allocated for Ip, the problem may repeat. The comment data and the operator data contains the virtual router identifier that owns this IP service.

Probable Cause

Type

Remedial action

IP has restarted because of lack of memory. To avoid similar problems in future, allocate more memory for IP from Vr.

7021 0006

Component	Severity	Status
Vr/<string> Ip cache/<instance>	major	set/clear

Legend

<string> = name of the virtual router

<instance> = an Lp number

Details

The IP cache table of the *Vr* component has failed to allocate/deallocate memory on *lp/<instance>*.

This alarm is set when the IP cache table of the *Vr* component has failed to allocate/deallocate memory in *lp/<instance>*. The cache table size is specified by the *cacheTableSize* attribute.

A clear is issued after the cache table size is changed to be as same as the size specified in the *cacheTableSize* attribute.

Probable Cause

Type

Remedial action

IP service is not affected if the OSI usage state is not idle. To avoid similar problems in future, allocate more memory for IP. A retry timer is created to allocate the memory for every minute.

7021 0008

Component	Severity	Status
Vr/<string> Ip	critical	set

Legend

<string> = name of the virtual router

Details

FP hardware resource exhaustion has occurred, causing the route addition to fail. The IP forwarding table on the FP on which the virtual router resides is not synchronized with the IP forwarding table on the CP.

Even though CAS reports displaying the IP forwarding table may indicate that the route exists, IP traffic may be unable to be forwarded by the FP.

Probable Cause

FP hardware resource exhaustion

Type

Remedial action

Manually clear the alarm from Preside MDM. Reset the FP to restart the IP service to recover from the hardware resource exhaustion.

To avoid similar problems in future, contact Nortel Networks technical support.

7021 0010

Component	Severity	Status
Vr/<string> Ip cache/<instance>	minor	set

Legend

<string> = name of the virtual router

<instance> = cache on the FP

Details

When there are excessive IP LCM cache misses, the LCM cache is filled to exceed the threshold, raising the alarm to caution the operator. The excessive IP LCM cache misses can be caused by bad network configuration or viruses in the network.

Probable Cause

Threshold crossed.

Type

Processing.

Remedial action

Lock the VR or the port. Further diagnose can include increasing the cache. Or, if there is enough cache, more tests are required. In that case, contact Nortel Networks technical support.

7021 1000

Component	Severity	Status
Vr/<string> Ip Ospf	warning	message

Legend

<string> = name of the virtual router

Details

An OSPF packet has been received on a non-virtual interface from a router whose configuration parameters conflict with this router's configuration parameters. Due to this, adjacency cannot be formed. The comment data and the operator data has relevant information to resolve the error. The alarm provides the following information:

ospfRouterId - the originator of the alarm

ospfIfIpAddress - the IP Address of the interface on which the packet was received

ospfAddressLessIf - the IfIndex of the interface if it is an addressless interface

ospfConfigErrorType - type of error. Could be one of the following: badVersion(1), areaMisMatch(2), unknownNbmaNbr(3), unknownVirtualNbr(4), authTypeMismatch(5), authFailure(6), netMaskMismatch(7), helloIntervalMismatch(8), deadIntervalMismatch(9), optionMisMatch(10)

ospfPacketType - Type of OSPF Packet

Probable Cause

Configuration error

Type

Processing

Remedial action

Check the configuration of this router and the router from which the packet was received and solve any mismatch. The comment data and the operator data has all the necessary information to correct this problem.

7021 1001

Component	Severity	Status
Vr/<string> Ip Ospf	warning	message

Legend

<string> = name of the virtual router

Details

An OSPF packet has been received on a virtual interface from a router whose configuration parameters conflict with this router's configuration parameters. Due to this, adjacency cannot be formed. The comment data and the operator data has relevant information to resolve the error. The alarm provides the following information:

ospfRouterId - the originator of the Alarm

ospfVirtIfAreaId - the area to which this virtual interface belongs to

ospfVirtIfNeighbor - the IP address of the neighbor who generated this packet

ospfConfigErrorType - type of error. Could be one of the following: badVersion(1), areaMisMatch(2), unknownNbmaNbr(3), unknownVirtualNbr(4), authTypeMismatch(5), authFailure(6), netMaskMismatch(7), helloIntervalMismatch(8), deadIntervalMismatch(9), optionMisMatch(10)

ospfPacketType - type of OSPF Packet

Probable Cause

Configuration error

Type

Processing

Remedial action

Check the configuration of this router and the router from which the packet was received and solve any mismatch. The comment data and the operator data has all the necessary information to correct this problem.

7021 1002

Component	Severity	Status
Vr/<string> Ip Ospf	warning	message

Legend

<string> = name of the virtual router

Details

An OSPF packet has been received on a non-virtual interface from a router whose authentication key or authentication type conflict with this router's authentication key or authentication type. The comment data and the operator data has relevant information to resolve the error. The information provided are:

ospfRouterId - the originator of the Alarm

ospfIfIpAddress - the IP address of the interface on which the packet was received.

ospfAddressLessIf - the ifIndex of the interface if it is an addressless interface.

ospfConfigErrorType - type of error could be one of the following: authFailure and authTypeMismatch.

ospfPacketType - type of OSPF Packet

Probable Cause

Unexpected information

Type

Security

Remedial action

Check if the source is an authenticated user of the net. The comment data and the operator data has relevant information to resolve the error.

7021 1003

Component	Severity	Status
Vr/<string> Ip Ospf	warning	message

Legend

<string> = name of the virtual router

Details

An OSPF packet has been received on a virtual interface from a router whose authentication key or authentication type conflict with this router's authentication key or authentication type. The comment data and the operator data has relevant information to resolve the error. The information provided are:

ospfRouterId - the originator of the Alarm

ospfVirtIfAreaId - the area to which this virtual interface belongs to

ospfVirtIfNeighbor - the IP address of the neighbor who generated this packet

ospfConfigErrorType - type of error. Could be one of the following: authFailure and authTypeMismatch.

ospfPacketType - type of OSPF Packet

Probable Cause

Unexpected information

Type

Security

Remedial action

Check if the source is an authenticated user of the net. The comment data and the operator data has relevant information to resolve the error.

7021 1005

Component	Severity	Status
Vr/<string> Ip Ospf	warning	message

Legend

<string> = name of the virtual router

Details

Number of LSAs in the router's link-state database has exceeded ninety percent of external link-state entries that can be stored. The comment data and the operator data has relevant information to resolve the error. The alarm provides the following information:

ospfRouterId - the originator of the Alarm

ospfExtLsdbLimit - the current value of the maximum number of entries allowed.

Note that the *ospfExtLsdbLimit* attribute is of criticality component level. Changing this attribute will restart OSPF with the provisioned values.

Probable Cause

Storage capacity problem

Type

Processing

Remedial action

Set the *extLsdbLimit* attribute of the component given in the component name field to a larger value.

7021 1006

Component	Severity	Status
Vr/<string> Ip Ospf	warning	message

Legend

<string> = name of the virtual router

Details

OSPF is out of memory. OSPF service is restarted with all the provisioned data. If more memory is not allocated for IP, the problem may repeat. The comment data and the operator data contains the virtual router identifier that owns this IP service.

Probable Cause

Storage capacity problem

Type

Processing

Remedial action

OSPF has restarted because of lack of memory. To avoid similar problems in future, allocate more memory for IP from Vr.

7021 1007

Component	Severity	Status
Vr/<string> Ip Bgp	minor	set/clear

Legend

<string> = name of the virtual router

Details

When the status is *set*, BGP has failed to establish a transport protocol listen port on well known TCP port 179. Either Vr or TCP may be out of memory.

BGP will still be able to initiate transport connections to configured BGP peers, but will not be able to accept transport connections from configured BGP peers.

The router identification number of the local BGP application is included in the alarm text.

When the status is *clear*, BGP has successfully established a transport protocol listen port on well known TCP port 179.

Probable Cause

Type

Remedial action

When the status is *set*, BGP will attempt to establish the transport protocol listen port continually (every 30 seconds). If the status does not change to *clear* over time, memory may need to be made free through provisioning changes (either by allocating more memory for Vr or by reducing the number of services being run by this or other instances of Vr). Disabling BGP will also change the status to *clear*.

When the status is *clear*, no remedial action is required.

7021 1008

Component	Severity	Status
Vr/<string> Ip Bgp Peer/<address>	minor	set/clear

Legend

<string> = name of the virtual router

<address> = IP address of the BGP peer

Details

When the status is *set*, BGP has failed to initiate a transport protocol connection to a configured BGP peer.

The router identification number of the local BGP application and the IP address of the peer to which BGP cannot connect is included in the alarm text.

When the status is *clear*, BGP has successfully established a transport protocol connection to a configured BGP peer.

Probable Cause

Type

Remedial action

When the status is *set*, BGP will attempt to establish the transport protocol connection continually (every 120 seconds). If the status does not change to *clear* over time, ensure that the BGP peer identified in the alarm is provisioned properly and that the remote BGP application is enabled and configured properly. Disabling a BGP peer will also change the status to *clear*.

When the status is *clear*, no remedial action is required.

7021 1009

Component	Severity	Status
Vr/<string> Ip Bgp Peer/<address>	warning	message

Legend

<string> = name of the virtual router

<address> = IP address of the BGP static peer

Details

BGP has sent a NOTIFICATION message to a BGP static peer. This BGP static peer is transitioning to the *idle* state. To display the state of a BGP static peer, display the *connectionState* attribute of the *Peer* subcomponent.

The router identification number of the local BGP application and the IP address of the static peer to which BGP is sending the NOTIFICATION is included in the alarm text. Also, the error code and error subcode included in the NOTIFICATION message are displayed.

Probable Cause

Type

Remedial action

The BGP static peering session has reset due to some error or event (indicated by the error code and error subcode of the NOTIFICATION message). The BGP static peering session will attempt to re-establish every 120 seconds. Operator intervention may be required.

7021 1010

Component	Severity	Status
Vr/<string> Ip Bgp Peer/<address>	warning	message

Legend

<string> = name of the virtual router

<address> = IP address of the BGP peer

Details

BGP has received a NOTIFICATION message from a BGP peer. This BGP peer is transitioning to the *idle* state. To display the state of a BGP peer display the *connectionState* attribute of the *Peer* sub-component.

The router identification number of the local BGP application and the IP address of the peer which has sent the NOTIFICATION is included in the alarm text. Also, the error code and error subcode included in the NOTIFICATION message are displayed.

Probable Cause

Type

Remedial action

The BGP peering session has reset due to some error or event (indicated by the error code and error subcode of the NOTIFICATION message). The BGP peering session will attempt to re-establish every 120 seconds. Operator intervention may be required.

7021 1011

Component	Severity	Status
Vr/<string> Ip Ospf	warning	message

Legend

<string> = name of the virtual router

Details

Two OSPF routers located in the same area have the same IP address provisioned for their OSPF interfaces. The provisioned interfaces can be up or down. Immediate action should be taken to fix the situation as some OSPF routes will not be reachable and extra traffic generated.

The information provided is as follows:

Duplicate IP Address - The duplicate IP address to be fixed.

Found on RouterId - The first router having the duplicate IP address.

Found on RouterId - The second router having the duplicate IP address.

Note that this alarm is issued every few minutes until the problem is fixed.

Probable Cause

Configuration error

Type

Processing

Remedial action

Use the RouterId values displayed in the alarm to identify the routers that have the same provisioned IP address. To display the *routerId* value of an OSPF router, display the “routerId” attribute under the *Ospf* sub-component. Change the provisioned IP address on one of the routers to eliminate IP address duplication.

7021 1012

Component	Severity	Status
Vr/<string> Ip Bgp Peer/<address>	minor	set/clear

Legend

<string> = name of the virtual router

<address> = IP address of the BGP peer

Details

This alarm is issued when a BGP speaker is configured to support ipv4Vpn or mbgpVpn on the peer, but determines that its peer supports common capability(ies) other than ipv4Vpn or mbgpVpn. It indicates that auto discovery information or VPN routing information will not be exchanged over this backbone peer session although the session is established with commonly supported capability(ies).

In the scenario where both ends do not support any common capabilities, the peer session does not establish and this alarm does not display even if ipv4Vpn or mbgpVpn is configured. In this case, a BGP NOTIFICATION message (with error code 2 and subcode 7 and containing the unsupported capability(ies)) is expected from both ends. The peers will retry with the same capabilities advertisement repeatedly.

Probable Cause

Configuration error

Type

Processing

Remedial action

If exchange of the same address families' IP VPN information is desired across VPN sites over this backbone peer session, make sure the BGP software on both the local and remote peers are upgraded to support the same address families and capabilities. Moreover, the attribute *addressFamily* under both the local and the remote *Peer Descriptor* component must be provisioned to be the same.

7021 1013

Component	Severity	Status
Vr/<string> Ip Bgp	warning	message

Legend

<string> = name of the virtual router

Details

This alarm is issued when a BGP speaker has discovered a private tunnel endpoint IP address, through auto-discovery, which is not on the same subnet as the local tunnel endpoint or it happens to be the same as another private tunnel endpoint that is already discovered. As a result, the invalid private tunnel address, together with its corresponding public tunnel address, will not be populated to both the MultipointStaticEndPoint and ARP. Also, no corresponding dynamic BGP peer will be created.

Probable Cause

Configuration error

Type

Processing

Remedial action

Check the local and remote interface of the tunnel protocol ports and ensure they are on the same subnet and no duplicate IP addresses are assigned to the interfaces.

Note: Auto-discovery will rediscover remote customer information if, and only if, the duplicate address/netmask is fixed on the local interface of the tunnel protocol port (i.e. linked to the VCG that generated the alarm). If the problem is resolved on a remote interface, a lock/unlock of the local customer *Vr Ip Tunnel* component is required to restart auto-discovery.

7021 1014

Component	Severity	Status
Vr/<string> Ip Bgp Peer/<address>	warning	message

Legend

<string> = name of the virtual router

<address> = IP address of the BGP peer

Details

This alarm is issued when a BGP speaker on a shared domain virtual router has detected that the same VPN ID is being used by multiple associated customer virtual routers. As a result, only one of the customer virtual routers that is provisioned with this VPN ID participates in auto-discovery.

Probable Cause

Configuration error

Type

Processing

Remedial action

All customer virtual routers that participate in IP VPN auto-discovery and use the same shared domain virtual router have to have unique VPN IDs provisioned. Provision unique VPN IDs for those that are duplicates.

Note: The VPN ID change should be done on the customer Vr that is currently not participating in auto-discovery.

7021 1015

Component	Severity	Status
Vr/<string> Ip MBgp	warning	message

Legend

<string> = name of the virtual router

Details

This alarm is issued when MBGP on the customer VR (cVR) attempts to import/export more VPN routes than specified by the provisionable maximum number of routes allowed to be imported and exported for that cVR.

Probable Cause

Software program error

Type

Processing

Remedial action

Provision appropriate import/export policies to limit the number of routes being imported exported.

7021 1016

Component	Severity	Status
Vr/<string> Ip Ospf	major	message

Legend

<string> = name of the virtual router

Details

A unique Link State Identifier can not be assigned to a self-originated type 3, 5 or 7 LSA. In that case, the LSA is discarded and routing to the subnet or external address may be affected. This problem can occur if there are destination addresses in the network with the same network number but different netmask lengths. The comment data and the operator data have relevant information to resolve the error. The alarm provides the following information:

Area - The area to which the LSA belongs.
LSA type - The type of the LSA.
Network number - The network number of the LSA.
Network mask - The network mask of the LSA.

Probable Cause

Configuration error.

Type

Processing.

Remedial action

Remove the duplicate network number by modifying the network configuration or OSPF export policy.

7021 1017

Component	Severity	Status
Vr/<string> Ip Ospf	warning/cleared	set/clear

Legend

<string> = name of the virtual router

Details

An LSA installed in the OSPF Link State Database on the Active CP/XC can nor be journalled to the Standby processor because its size is too large. This alarm indicates that this event cause the CP or XC to be degraded. On a CP or XC switchover, only this VR instance will force the re-convergence of the Link State database with its OSPF neighbors.

Probable Cause

Configuration error.

Type

Processing.

Remedial action

Lock the VR IP OSPF component in question and the degraded state is removed.

7021 1051

Component	Severity	Status
For Passport 6400: Vr/<string> Ip IpVrrp	warning	message
For Passport 7400: Vr/<string> Ip Vrrp		

Legend

<string> = name of the virtual router

Details

The TimeToLive field in the IP header of the received VRRP packet is not equal to 255. This field is used to provide sanity check on the VRRP packet.

Probable Cause

Communications

Type

Protocol error

Remedial action

None.

Warning: There are possibly multiple master VRRPs running for the same set of IP addresses.

7021 1052

Component	Severity	Status
For Passport 6400: Vr/<string> Ip IpVrrp	warning	message
For Passport 7400: Vr/<string> Ip Vrrp		

Legend

<string> = name of the virtual router

Details

The Version field in the VRRP header of the received VRRP packet is not correct. This could be caused by using an obsolete version of software.

Probable Cause

Processing

Type

Version mismatch

Remedial action

Upgrade the switch with VRRP version 2 software.

7021 1053

Component	Severity	Status
For Passport 6400: Vr/<string> Ip IpVrrp	warning	message
For Passport 7400: Vr/<string> Ip Vrrp		

Legend

<string> = name of the virtual router

Details

The advertisement interval timers are provisioned with different values for the same VRRP on different routers.

Probable Cause

Processing

Type

Configuration or customization error

Remedial action

Change provisioning on the routers.

7021 1054

Component	Severity	Status
For Passport 6400: Vr/<string> Ip IpVrrp For Passport 7400: Vr/<string> Ip Vrrp	warning	message

Legend

<string> = name of the virtual router

Details

Checksum of the received VRRP packet is incorrect. Network could be in an unstable state.

Probable Cause

Processing

Type

Corrupt data

Remedial action

None.

Notes: might have to take down the network if this repeatedly happens.

7021 1055

Component	Severity	Status
For Passport 6400: Vr/<string> Ip IpVrrp	warning	message
For Passport 7400: Vr/<string> Ip Vrrp		

Legend

<string> = name of the virtual router

Details

IP addresses received in the VRRP packet do not match the locally provisioned addresses.

Probable Cause

Processing

Type

Configuration or customization error

Remedial action

Change the provisioned IP addresses on the routers.

7021 1056

Component	Severity	Status
For Passport 6400: Vr/<string> Ip IpVrrp For Passport 7400: Vr/<string> Ip Vrrp	warning	message

Legend

<string> = name of the virtual router

Details

An unknown VRRP authentication type was received in the advertisement. The only authentication type supported by the Passport implementation is “No authentication”. This corresponds to a value of 0 in the authentication field of the VRRP advertisement.

Probable Cause

Authentication failure

Type

Security

Remedial action

Change the authentication method on the non-Passport routers to use “No authentication”.

7021 1100

Component	Severity	Status
Vr/ <string> Ip Ospf	warning	message

Legend

<string> = name of the virtual router

Details

A change occurred in the state of the OSPF non-virtual neighbor. This change can either be due to a neighbor state regressing or progressing to the Full terminal state.

In the case of the broadcast or non-broadcast multi-access networks, this alarm should be generated by the designated router. The information provided is:

ospfRouterId - the originator of the alarm.

ospfNbrIpAddr - the IP address of the neighbor's interface.

ospfNbrAddressLessIndex - the IfIndex of the interface.

ospfNbrRtrId - the router id of the neighbor.

ospfNbrState - the new state of the neighbor.

Probable Cause

Loss of Signal

Type

Communications

Remedial action

Verify the running status of the router corresponding to this OSPF neighbor. The comment data and the operator data has all the necessary information to correct this problem.

7021 1200

Component	Severity	Status
Rtr/(rtr_id> Isis	warning	message

Legend
<rtr_id> = name of the virtual router

Details
ISIS has received a corrupted LSP packet. The LSP will be ignored.

Probable Cause
Communication protocol error

Type
Processing

Remedial action
No remedial action is required.

7021 1202

Component	Severity	Status
Rtr/(rtr_id> Isis	warning	message

Legend

<rtr_id> = name of the virtual router

Details

ISIS has received a a packet with an invalid sequence number. This packet will be ignored.

Probable Cause

Protocol error

Type

Processing

Remedial action

No remedial action is required.

7021 1203

Component	Severity	Status
Rtr/(rtr_id> Isis	warning	message

Legend

<rtr_id> = name of the virtual router

Details

ISIS has received a packet with a System Id length that is different from the one with which it is configured.

Probable Cause

Protocol error

Type

Processing

Remedial action

No remedial action is required.

7021 1204

Component	Severity	Status
Rtr/(rtr_id> Isis	warning	message

Legend

<rtr_id> = name of the virtual router

Details

ISIS has received a packet with a Maximum Area Addresses field that is different from the one with which it is configured.

Probable Cause

Protocol error

Type

Processing

Remedial action

No remedial action is required.

7021 1205

Component	Severity	Status
Rtr/(rtr_id> Isis	warning	message

Legend
<rtr_id> = name of the virtual router

Details
ISIS is purging its own LSP from the DB.

Probable Cause
Protocol error

Type
Processing

Remedial action
No remedial action is required.

7021 1206

Component	Severity	Status
Rtr/(rtr_id> Isis	major	set/clear

Legend

<rtr_id> = name of the virtual router

Details

The ISIS Link State Database has exceeded 90% of its LSP storage capacity.

Probable Cause

Storage capacity problem

Type

Processing

Remedial action

Verify that the number of LSPs generated by nodes within an ISIS Level-1 area doesn’t exceed the current threshold.

7021 1208

Component	Severity	Status
Rtr/(rtr_id> Isis	warning	message

Legend

<rtr_id> = name of the virtual router

Details

Local ISIS has received its own LSP with a higher sequence number. The sequence number of the local LSP will be skipped.

Probable Cause

Protocol error

Type

Processing

Remedial action

No remedial action is required.

7021 1209

Component	Severity	Status
Rtr/(rtr_id> Isis	warning	message

Legend
<rtr_id> = name of the virtual router

Details
ISIS has received a packet with an unsupported version number.

Probable Cause
Configuration or customization error

Type
Processing

Remedial action
No remedial action is required.

7021 1210

Component	Severity	Status
Rtr/(rtr_id> Isis	warning	message

Legend

<rtr_id> = name of the virtual router

Details

ISIS has received a packet with a supported protocol type that is different from the one with which it is configured.

Probable Cause

Configuration or customization error

Type

Processing

Remedial action

No remedial action is required.

7021 1211

Component	Severity	Status
Rtr/(rtr_id> Isis	warning	message

Legend

<rtr_id> = name of the virtual router

Details

ISIS has received a packet with an area ID type that does not match any of the area IDs that are supported by this router, as specified in the *Rtr Isis Net* components.

Probable Cause

Configuration or customization error

Type

Processing

Remedial action

Verify that the source and local nodes are configured with at least one area address in common.

7021 1212

Component	Severity	Status
Rtr/(rtr_id> Isis	warning	message

Legend
<rtr_id> = name of the virtual router

Details
ISIS has received a packet that is too large to propagate out of one of its interfaces.

Probable Cause
Protocol error

Type
Processing

Remedial action
No remedial action is required.

7021 1213

Component	Severity	Status
Rtr/(rtr_id> Isis	warning	message

Legend
<rtr_id> = name of the virtual router

Details
An adjacency state with a neighboring node has changed.

Probable Cause
Loss of signal

Type
Processing

Remedial action
No remedial action is required.

7021 1214

Component	Severity	Status
Rtr/(rtr_id> Isis	warning	message

Legend
<rtr_id> = name of the virtual router

Details
ISIS protocol activity has generated a failed request for system memory.

Probable Cause
Out of memory

Type
Processing

Remedial action
Allocate more memory for IP from the Rtr.

7021 1215

Component	Severity	Status
Rtr/(rtr_id> Isis	warning	message

Legend
<rtr_id> = name of the virtual router

Details
The ISIS protocol is configured to run on an unsupported media type.

Probable Cause
Configuration or customization error

Type
Processing

Remedial action
Ensure all of the ISIS interfaces are configured only on LAN or ATM media.

7021 2000

Component	Severity	Status
Vr/<string> Ip Rip	warning	message

Legend

<string> = name of the virtual router

Details

RIP is out of memory. RIP service is restarted with all the provisioned data. If more memory is not allocated for IP, the problem may repeat. The comment data and the operator data contains the virtual router identifier that owns this IP service.

Probable Cause

Type

Remedial action

RIP has restarted because of lack of memory. To avoid similar problems in future, allocate more memory for IP from Vr.

7021 2500

Component	Severity	Status
Vr/<string> Ip Tunnel Msep/<num>	warning	message

Legend

<string> = name of the virtual router

<num> = 0 - 1

Details

Duplicate Tunnel MultipointStaticEndPoint source IP addresses have been provisioned.

Probable Cause

Type

Remedial action

Reprovision the Tunnel MultipointStaticEndPoints so that they have unique source IP addresses.

7021 2501

Component	Severity	Status
Vr/<string> Ip Tunnel Msep/<num>	warning	message

Legend

<string> = name of the virtual router

<num> = 0 - 1, numeric Msep instance

Details

This alarm is issued when an IP TunnelMultipointStaticEndPoint attempts a discovered Tunnel destination IP address (DA) that is equal to the provisioned MultipointStaticEndPoint source IP address (SA).

Probable Cause

Configuration error

Type

Processing

Remedial action

Verify that all IP Tunnel MultipointStaticEndPoints within the same VPN have unique source IP addresses.

7021 2503

Component	Severity	Status
	warning	message

Details

This alarm indicates that an IP tunnel endpoint could not be fully initialized in hardware due to hardware resource unavailability. The IP tunnel endpoint remains in software, resulting in a performance degradation restricted to this endpoint.

Probable Cause

Hardware sources required for the setup of the IP tunnel in hardware on the FP were exhausted.

Type

qualityOfService

Remedial action

Frequent occurrences of this condition indicate that the number of IP tunnel endpoints requested to be setup in hardware on this FP exceeds the hardware resources available on this FP. Contact your local Nortel Networks technical support group for assistance if necessary.

7021 3000

Component	Severity	Status
Vr/<string> Ip Egp	warning	message

Legend

<string> = name of the virtual router

Details

EGP is out of memory. EGP service is restarted with all the provisioned data. If more memory is not allocated for IP, the problem may repeat. The comment data and the operator data contains the virtual router identifier that owns this IP service.

Probable Cause

Type

Remedial action

EGP has restarted because of lack of memory. To avoid similar problems in future, allocate more memory for IP from Vr.

7021 4000

Component	Severity	Status
Vr/<string> Ip	warning	message

Legend

<string> = name of the virtual router

Details

IP Rtm is out of memory. IP Rtm service is restarted with all the provisioned data. If more memory is not allocated for Ip, the problem may repeat. The comment data and the operator data contains the virtual router identifier that owns this IP service.

Probable Cause

Type

Remedial action

Ip Rtm has restarted because of lack of memory. To avoid similar problems in future, allocate more memory for IP from Vr.

7022 0000

Component	Severity	Status
Vr/<string> Br	critical	message

Legend
<string> = name of the virtual router

Details
A Bridge component's attempt to allocate working memory has failed.

Memory allocation failed. Reason: Exceeded Memory Manager provisioned limit.

Probable Cause

Type

Remedial action
If sufficient resources remain, allocate additional memory for Bridge use.

If not, re-evaluate bridge network design. (Maximum number of allowed hosts, number of spanning tree's, etc.)

7023 0001

Component	Severity	Status
Vr/<string> Ipx	minor	message

Legend

<string> = name of the virtual router

Details

The routing protocol provisioned for the routers at both the ends of the link do not match. Valid routing options supported on a Wan link for release 2.0 are numbered and unnumbered rip protocols.

Probable Cause

Type

Remedial action

Reprovision one or both the routers for running the same routing protocol on the link.

7023 0002

Component	Severity	Status
Vr/<string> Ipx	minor	message

Legend

<string> = name of the virtual router

Details

IpxWan Timer Request Packet received after an Information Request packet is sent or after IpxWan negotiations are complete. This indicates that the IpxWan peer wishes to restart negotiations.

Probable Cause

Type

Remedial action

Inform the peer router's service representative of the error.

7023 0003

Component	Severity	Status
Vr/<string> Ipx	minor	message

Legend

<string> = name of the virtual router

Details

Invalid IpxWan negotiation packet received from the peer. One of the following scenarios causes this alarm.

1) An IpxWan Timer Response packet received from the peer
   a) before a Timer Request packet is received (state 0; event 1)
   b) after a Timer response is sent to the peer (state 1; event 1)
   c) after an Information Request Packet is sent to the peer (state 4; event 1)
 or d) after IpxWan negotiations are complete. (state 5, event 1)

2) An Information Request packet is received
   a) before a Timer Request packet is received (state 0; event 2)
   b) after a Timer Request packet is sent out (state 1; event 2)
   c) after an Information Request packet is sent out (state 4, event 2)
 or d) after IpxWan negotiations are complete. (state 5; event 2)

3) An Information Response Packet is received
   a) before a Timer Request packet is received (state 0; event 3)
   b) before a Timer Request packet is sent out (state 2; event 3)
   c) before a Timer Response packet is sent out (state 3; event 3)
 or d) before a Timer Request packet is received (state 4; event 3).

Probable Cause

Type

Remedial action

Inform the peer router’s service representative of the error.

7023 0004

Component	Severity	Status
Vr/<string> Ipx	minor	message

Legend

<string> = name of the virtual router

Details

Although IpxWan negotiations determine that the peer router is a slave; it sends an Information request packet to us. The peer router thus considers itself to be the link master.

Probable Cause

Type

Remedial action

Inform the peer router's service representative of the error.

7023 0005

Component	Severity	Status
Vr/<string> Ipx	major	message

Legend

<string> = name of the virtual router

Details

Internal Network Number for both the IpxWan peers are the same. Thus IpxWan cannot determine the master or the slave using the internal network number.

Probable Cause

Type

Remedial action

Reprovision the routers so that their internal network numbers are different.

7023 0006

Component	Severity	Status
Vr/<string> Ipx	minor	set/clear

Legend

<string> = name of the virtual router

Details

When the status is *set*, the component has been administratively disabled.

The Administratively disabled component is no longer permitted to provide service. As a result, dependent components may be operationally disabled as well.

When the status is *clear* the component is administratively enabled.

The OSI administrative state attribute in the alarm specifies the new administrative state for the component.

Probable Cause

Type

Remedial action

When the status is *set*, set the *snmpAdminState* attribute to up to attempt to enable the component.

When the status is *clear*, no remedial action is required.

7023 0007

Component	Severity	Status
Vr/<string> Ipx	critical	set/clear

Legend

<string> = name of the virtual router

Details

When the status is *set*, the component has been locked.

The locked component is no longer permitted to provide service. As a result, dependent components may be operationally disabled as well.

When the status is *clear* the component is unlocked.

The OSI administrative state attribute in the alarm specifies the new administrative state for the component.

Probable Cause

Type

Remedial action

When the status is *set*, use the unlock verb to attempt to unlock the component. When the status is *clear*, no remedial action is required.

7023 0008

Component	Severity	Status
Vr/<string> Ipx	major	message

Legend

<string> = name of the virtual router

Details

An Ipx component's attempt to allocate memory has failed.
Reason: Exceeded Memory Manager provisioned limit.

Probable Cause

Type

Remedial action

If sufficient resources remain, allocate additional memory for the Ipx Component. If not, re-evaluate the ipx network design.

7023 0009

Component	Severity	Status
Vr/<string1> Pp/<string2> IpxPort/<encap>	minor	set/clear

Legend

<string1> = name of the virtual router

<string2> = name of the protocol port

<encap> = encapsulation type for the IPX port

Details

When the status is *set*, the component has been administratively disabled.

The Administratively disabled component is no longer permitted to provide service.

When the status is *clear* the component is administratively enabled.

The OSI administrative state attribute in the alarm specifies the new administrative state for the component.

Probable Cause

Type

Remedial action

When the status is *set*, set the *snmpAdminState* to up to attempt to enable the component.

When the status is *clear*, no remedial action is required.

7023 0010

Component	Severity	Status
Vr/<string1> Pp/<string2> IpxPort/<encap>	critical	set/clear

Legend

<string1> = name of the virtual router

<string2> = name of the protocol port

<encap> = encapsulation type for the IPX port

Details

When the status is *set*, the component has been locked.

The locked component is no longer permitted to provide service.

When the status is *clear* the component is unlocked.

The OSI administrative state attribute in the alarm specifies the new administrative state for the component.

Probable Cause

Type

Remedial action

When the status is *set*, use the unlock verb to attempt to unlock the component.When the status is *clear*, no remedial action is required.

7026 1000

Component	Severity	Status
Lp/<num1> <type>/<num2>	critical/cleared	set/clear

Legend

<num1> = 0 - 15

<type> = Enet and Fi

<num2> = 0 - 5

Details

When the status is *set*, diagnostics have detected a fault with the hardware associated with this port. The comment text of the alarm will indicate the nature of the fault. The port will remain out of service until action is taken to correct the fault. Diagnostics can be re-executed by locking and unlocking the component.

A *clear* is issued when diagnostics have executed successfully.

Probable Cause

Equipment malfunction

Type

Equipment

Remedial action

When the status is *set*, discontinue the use of the port. Provision and alternate port, activate the standby card, or replace the card if possible.

When the status is *clear*, no remedial action is necessary.

7026 1001

Component	Severity	Status
Lp/<num1> <type>/<num2>	critical/cleared	set/clear

Legend

<num1> = 0 - 15

<type> = Enet and Fi

<num2> = 0 - 5

Details

When the status is *set*, diagnostics have detected a fault with the hardware common to all ports on this card. The comment text of the alarm will indicate the nature of the fault. This port (and any others on the same Lp) will remain out of service until action is taken to correct the fault. Diagnostics can be re-executed by locking and unlocking the component.

A *clear* is issued when diagnostics have executed successfully.

Probable Cause

Equipment malfunction

Type

Equipment

Remedial action

When the status is *set*, discontinue the use of all ports on this Lp. Activate the standby card, or replace the card if possible.

When the status is *clear*, no remedial action is necessary.

7026 1002

Component	Severity	Status
Lp/<num1> <type>/<num2>	critical/cleared	set/clear

Legend

<num1> = 0 - 15

<type> = Enet and Fi

<num2> = 0 - 5

Details

The status is *set* when diagnostics have detected an error in the hardware or software configuration of this card. The comment text of the alarm will indicate the nature of the fault. This can include a missing FPGA file, or a missing hardware component. The port (and any others on the same Lp) will remain out of service until action is taken to correct the fault. Diagnostics can be re-executed by locking and unlocking the component.

A *clear* is issued when diagnostics have executed successfully.

Probable Cause

Equipment malfunction

Type

Equipment

Remedial action

When the status is *set*, discontinue the use of all ports on this Lp.

If the alarm comment text indicates that a required file is missing, ensure that the correct revision of the file is present in the correct directory on the CP disk.

If the alarm comment text indicates that a required hardware component is missing, activate the standby card, or replace the card if possible.

When the status is *clear*, no remedial action is necessary.

7026 2000

Component	Severity	Status
Lp/<num1> <type>/<num2>	critical/cleared	set/clear

Legend

<num1> = 0 - 15

<type> = Enet and Fi

<num2> = 0 - 5

Details

This alarm is issued if a fundamental internal operation fails during initial provisioning of the component. The comment text of the alarm should indicate the nature of the failed operation. The alarm may be preceded by related software alarms.

Probable Cause

Type

Remedial action

Contact your local Nortel Networks technical support group.

7026 2002

Component	Severity	Status
Lp/<num1> <type>/<num2>	critical	message

Legend

<num1> = 0 - 15

<type> = Enet and Fi

<num2> = 0 - 5

Details

This alarm is issued if a fundamental internal operation fails during initial provisioning of the component. The comment text of the alarm should indicate the nature of the failed operation. The alarm may be preceded by related software alarms.

Probable Cause

Underlying resource unavailable

Type

Processing

Remedial action

Contact your local Nortel Networks technical support group.

7026 2003

Component	Severity	Status
Lp/<num1> <type>/<num2>	critical/cleared	set/clear

Legend

<num1> = 0 - 15

<type> = Enet and Fi

<num2> = 0 - 5

Details

The status is *set* when an attempt to put this component into service has failed because the LanTest subcomponent is in a manufacturing, design verification, or product integrity test mode.

This mode can only be entered if all ports on the FP are out of service, and the LanTest subcomponent associated with one of the ports is placed in the Manufacturing/DVT/PI test mode. This mode is not intended for end-user use.

When the status is *clear*, the component may be placed into service.

Probable Cause

Procedural error

Type

Operator

Remedial action

When the status is *set*, reset the Lp associated with the component.

When the status is *clear*, no remedial action is necessary.

7026 2004

Component	Severity	Status
Lp/<num1> <type>/<num2>	critical	message

Legend

<num1> = 0 - 15

<type> = Enet and Fi

<num2> = 0 - 5

Details

This alarm is issued during initial provisioning of the component if a MAC address is not available for the component. This can be caused by a hardware failure that interferes with the distribution of MAC addresses to the Lp. It could also be caused if another component is using the MAC address designated for this component. If this is the case, this alarm should be preceded by a software alarm indicating that a requested MAC address ID is already in use.

Probable Cause

Underlying resource unavailable

Type

Processing

Remedial action

Contact your local Nortel Networks technical support group.

7026 3000

Component	Severity	Status
Lp/<num1> Enet/<num2>	critical/cleared	set/clear

Legend

<num1> = 0 - 15

<num2> = 0 - 5

Details

The status is *set* when the Ethernet component has detected the absence of heartbeat pulses on the twisted pair medium. The port is out of service and cannot receive or transmit packets until this condition is cleared. This condition can be caused by a bad connection to the ethernet cable, or a bad ethernet cable.

A *clear* is issued when heartbeat pulses are detected on the twisted pair medium.

Probable Cause

CableTamper,IOdevice error

Type

Communications, Equipment

Remedial action

When the status is *set*, check the connection between the ethernet port and the ethernet cable. Also check for a faulty cable.

When the status is *clear*, no remedial action is required.

7026 3001

Component	Severity	Status
Lp/<num1> Enet/<num2>	indeterminate	message

Legend

<num1> = 0 - 15

<num2> = 0 - 5

Details

When the status is *set*, the Ethernet component has detected an LRC error in a packet being transmitted. This indicates that the packet has been corrupted while in the data path and discarded. This could be caused by a hardware or software failure.

Since this error could potentially occur in many frames, the rate at which the alarm is issued may be throttled to avoid flooding the system with alarms. The number of packets discarded because of LRC errors is included in the count of output packets discarded. The port is not taken out of service due to this event but if LRC errors occur in sufficient number, performance will be adversely affected due to the number of packets being discarded.

Probable Cause

Corrupt data

Type

Processing

Remedial action

Normally there is no remedial action to be taken. The error could be caused by a hardware failure, so running diagnostics may help isolate the problem. If the error occurs frequently or for prolonged periods of time, contact your local Nortel Networks technical support group.

7026 3002

Component	Severity	Status
Lp/0 OamEthernet/0	indeterminate	message

Legend

<num> = 0

Details

This alarm indicates that a CP switchover event is about to occur due to a failure of one of the initial tests performed on the OamEthernet port. The initial tests are performed on the OamEthernet port prior to it being put into an open and unlocked state. This alarm, and the subsequent switchover, depend on the provisionable attribute *switchoverOnFailure* being set to enabled.

Probable Cause

Type

Remedial action

Check all cables leading from the affected CP Ethernet port for breaks or an improper connection. If the problem persists the affected CP card should be removed and replaced with one whose Ethernet port is fully functional.

7026 3003

Component	Severity	Status
Lp/0 OamEthernet/0	indeterminate	message

Legend

<num> = 0

Details

This alarm indicates that a CP switchover event is about to occur due to a short or break in the line or attached to the CP Ethernet port as detected by the steady state link test. The steady state link test is performed on the link connected to the OamEthernet port once every minute to determine its status. This alarm, and the subsequent switchover, depend on the provisionable attribute *switchoverOnFailure* being set to enabled.

Probable Cause

IOdevice error

Type

Equipment

Remedial action

Check all cables leading from the affected CP Ethernet port for breaks or an improper connection.

7026 3004

Component	Severity	Status
Lp/0 OamEthernet/0	warning	message

Legend
<num> = 0

Details
This alarm is issued when the OamEthernet port is provisioned on a PM1 based CP card.

Probable Cause

Type

Remedial action
Delete the provisioned OamEthernet port.

7026 3005

Component	Severity	Status
Lp/<num1> Enet/<num2>	minor/cleared	set/clear

Legend

<num1> = 0 - 15

<num2> = 0 - 5

Details

When the status is *set*, the Ethernet component has detected the absence of heartbeat pulses on the twisted pair medium for the standby CP. The port in the standby CP is out of service and cannot receive or transmit packets until this condition is cleared. This condition can be caused by a bad connection to the Ethernet cable or faulty Ethernet cable. A *clear* is issued when heartbeat pulses are detected on the twisted pair medium for the standby CP.

Probable Cause

Type

Remedial action

When the status is *set*, check the connection between the Ethernet port and the Ethernet cable. Also check for a faulty cable.

When the status is *clear*, no remedial action is necessary.

7026 3006

Component	Severity	Status
Lp/<0> OamEthernet/<0>	indeterminate	message

Legend

<num> = 0

Details

This alarm indicates that a CP switchover attempt, due to an OamEnet failure condition, has been suspended due to one of the following system conditions:

File system is synchronized
CIT is loaded on the standby
Standby port is available
FPs run committed view
Software upgrade is not in progress
Standby CP is available

A CP switchover with one of the above system conditions may cause unnecessary service outages.

Probable Cause

Type

Remedial action

Clear the system condition so that the CP switchover due to the OamEnet failure can proceed. Alternatively, you can perform a manual switchover, *switchover -force lp/0*, if the outages are acceptable.

7026 4002

Component	Severity	Status
Fddi/<instance>	warning	message

Legend

<instance> = decimal zero for current FDDI products

Details

When issued a connection established by this station possesses the unusual characteristic of connecting two PHY's of the same type. The connection doesn't violate the connection policy on both stations involved so it was accepted.

Probable Cause

Type

Remedial action

No remedial action necessary unless the condition occurred unintentionally, then change cabling to correct the condition.

7026 4004

Component	Severity	Status
Fddi/<instance>	warning	message

Legend

<instance> = decimal zero for current FDDI products

Details

When this alarm is issued, a connection policy violation has occurred. This means that the connection policy for this station doesn't allow a connection to the neighbors PHY type. The connection will ultimately be established or rejected depending on the neighbors connection policy.

Probable Cause

Type

Remedial action

When this condition occurs verify cabling of this station to its neighbors complies with standard FDDI convention. If the intention is to violate the standard FDDI convention for dual attach stations then modify the default connection policy attribute(s) to allow the desired connection, (e.i. if a PHY type A to PHY type A connection is desired modify the provisioning attribute "acceptAA" in the FDDI component to enable this connection.)

7026 4005

Component	Severity	Status
Fddi/<instance>	warning	message

Legend

<instance> = decimal zero for current FDDI products

Details

When this alarm is issued, a connection policy violation has been signalled by one of this stations neighbors. This means that the connection policy for the neighboring station doesn't allow a connection to this station PHY type. The connection will ultimately be established or rejected depending on the connection policy of this station.

Probable Cause

Type

Remedial action

When this condition occurs verify cabling of this station to it's neighbors complies with standard FDDI convention. If the intention is to violate the standard FDDI convention for dual attach stations then modify the default connection policy attribute(s) to allow the desired connection, (e.i. if a PHY type A to PHY type A connection is desired modify the provisioning attribute "acceptAA" in the FDDI component to enable this connection.). To eliminate the alarm the neighboring stations connection policy must also be modified to accept the non-standard connection.

7026 4006

Component	Severity	Status
Fddi/<instance>	warning	message

Legend

<instance> = decimal zero for current FDDI products

Details

Alarm issued when PCM state machine for a PHY connection that was withheld is restarted.

Probable Cause

Type

Remedial action

No remedial action required.

7026 4007

Component	Severity	Status
Fddi/<instance>	warning	message

Legend

<instance> = decimal zero for current FDDI products

Details

Issued when the FDDI SMT's PCM state machine for a particular PHY is unable to establish a connection to its neighboring station.

Probable Cause

Type

Remedial action

Verify that the PHY is question is properly connected to another active station. This alarm can be ignored if the users has intentionally elected to run the FDDI ring in a wrapped configuration, where only one PHY is being utilized

If difficulties persist contact your local Nortel Networks technical support group.

7026 4008

Component	Severity	Status
Fddi/<instance>	warning	message

Legend

<instance> = decimal zero for current FDDI products

Details

Issued after the FDDI MAC claim process, and beacon process fail. This alarm is used to signify the stuck beacon fault recovery trace process in the SMT has been started. This alarm is issued when a fault condition has occurred on the FDDI ring. If this station does not return to an active state it may mean that its neighbors have isolated this station as the source of the fault and removed it from the ring by going into a wrapped configuration.

Probable Cause

Type

Remedial action

Contact your local Nortel Networks technical support group.

7026 4009

Component	Severity	Status
Fddi/<instance>	warning	message

Legend

<instance> = decimal zero for current FDDI products

Details

Issued when the FDDI SMT's PCM state machine receives a trace propagation notification from its upstream neighbor. See alarm 7026-4008 for description and scenario that would cause the occurrence of this alarm.

Probable Cause

Type

Remedial action

Contact your local Nortel Networks technical support group.

7026 400A

Component	Severity	Status
Fddi/<instance>	warning	message

Legend

<instance> = decimal zero for current FDDI products

Details

Issued as notification of successful completion of the FDDI SMT trace function. This alarm will normally be followed by the alarm 7026-000B to indicate the start of the path test. See alarm 7026-4008 for description and scenario that would cause the occurrence of this alarm.

Probable Cause

Type

Remedial action

Contact your local Nortel Networks technical support group.

7026 400B

Component	Severity	Status
Fddi/<instance>	warning	message

Legend

<instance> = decimal zero for current FDDI products

Details

Notification of the start of the PATH test. The path test is used to verify this stations H/W for any problems that might effect the operation of the FDDI ring.

Probable Cause

Type

Remedial action

Contact your local Nortel Networks technical support group if the station doesn't return to an active operational state, or if this alarm is follow by the alarm 7026-400D.

7026 400C

Component	Severity	Status
Fddi/<instance>	warning	message

Legend

<instance> = decimal zero for current FDDI products

Details

Notification that the path test passed on this station. It is an indication that a problem on the FDDI ring is not being caused by this station See alarm 7026-400B for additional information on the path test.

Probable Cause

Type

Remedial action

No action required.

7026 400D

Component	Severity	Status
Fddi/<instance>	warning	message

Legend

<instance> = decimal zero for current FDDI products

Details

Notification that the path test failed on this station. It is an indication that a problem on the FDDI ring could be caused by this station. See alarm 7026-400B for additional information on the path test.

Probable Cause

Type

Remedial action

No action required.

7026 400E

Component	Severity	Status
Fddi/<instance>	warning	message

Legend

<instance> = decimal zero for current FDDI products

Details

Notification that this station is invoking the FDDI SMT trace function. This fault isolation procedure is initiated if the claim and beacon process performed by the MAC are unsuccessful.

Probable Cause

Type

Remedial action

If the station returns to an active state no action is necessary, otherwise, consult your local service representative for assistance.

7026 400F

Component	Severity	Status
Fddi/<instance>	warning	message

Legend

<instance> = decimal zero for current FDDI products

Details

Notification the link error rate has exceeded the warning threshold. Link error monitoring detects FDDI symbol errors in a given sample period. A rise in the error rate above the warning threshold may result in slightly degraded performance of the FDDI ring.

Probable Cause

Type

Remedial action

No action required.

7026 4010

Component	Severity	Status
Fddi/<instance>	warning	message

Legend

<instance> = decimal zero for current FDDI products

Details

Notification the link error rate has exceeded the cutoff threshold. When the error rate reaches this level it is sufficiently critical that the link between the two PHY's experiencing the errors is terminated to avoid severe performance degradation of the entire ring due to a single link. The connection will be restored provided the link confidence test is passed during the physical connection signalling process.

Probable Cause

Type

Remedial action

If condition persists or the connection remains disabled contact your local Nortel Networks technical support group.

7026 4011

Component	Severity	Status
Fddi/<instance>	warning	message

Legend

<instance> = decimal zero for current FDDI products

Details

Notification the link confidence test has failed during the attempt to establish a connection with the neighboring station. The link confidence test (LCT) is used to verify the connection quality prior to allowing a station to participate in the FDDI ring.

Probable Cause

Type

Remedial action

Verify the cable quality and connection cleanliness. If problems persist contact your local Nortel Networks technical support group.

7026 4012

Component	Severity	Status
Fddi/<instance>	warning	message

Legend
<instance> = decimal zero for current FDDI products

Details
A duplicate address condition has been detected on the FDDI ring.

Probable Cause

Type

Remedial action
This condition is usually caused by local administration of MAC addresses. Contact your local Nortel Networks technical support group if problems persists.

7026 4013

Component	Severity	Status
Fddi/<instance>	warning	message

Legend

<instance> = decimal zero for current FDDI products

Details

A condition occurred in the SMT process where more events where generated than could be handled by the process. This alarm may be appear when connecting and disconnecting cables on an active FDDI station.

Probable Cause

Type

Remedial action

If the FDDI station fails to achieve a connection delete the FDDI component and then reactivate the port. Under normal conditions the FDDI SMT should recover from this condition without intervention. Contact your local Nortel Networks technical support group if problems persist since there are numerous potential causes for this alarm including hardware, or signal integrity problems.

7026 4014

Component	Severity	Status
Fddi/<instance>	warning	message

Legend

<instance> = decimal zero for current FDDI products

Details

When one of the PHY's experiences an unusual condition that generates an excessive number of interrupts it may be disable to prevent side effects caused by to much processing time being consumed to service this condition. Several conditions may cause this alarm, one would be disconnecting or connecting cables on an active FDDI station.

Probable Cause

Type

Remedial action

If the FDDI station fails to establish a connection after this alarm has been issued delete the FDDI component and then reactivate the port. Under normal conditions the FDDI SMT should recover from this condition without intervention. Contact your local Nortel Networks technical support group if problems persist with a static cable configuration since there are numerous additional conditions that could generate this alarm including hardware, or signal integrity problems.

7026 4015

Component	Severity	Status
Fddi/<instance>	warning	message

Legend

<instance> = decimal zero for current FDDI products

Details

When the MAC experiences an unusual condition that generates an excessive number of interrupts it may be disabled to prevent side effects caused by to much processing time being consumed to service this condition. Several conditions may cause this alarm, one would be disconnecting or connecting cables on an active FDDI station.

Probable Cause

Type

Remedial action

If the FDDI station fails to establish a connection after this alarm has been issued delete the FDDI component and then reactivate the port. Under normal conditions the FDDI SMT should recover from this condition without intervention. Contact your local Nortel Networks technical support group if problems persist with a static cable configuration since there are numerous additional conditions that could generate this alarm including hardware, or signal integrity problems.

7026 5000

Component	Severity	Status
Lp/<num1> Tr/<num2>	warning	message

Legend

<num1> = 0 - 15

<num2> = 0 - 5

Details

Issued when an unrecoverable error is encountered by the TMS 380.

Probable Cause

Adaptor error

Type

Equipment

Remedial action

If this condition is not caused by a hardware failure the port will recover from this without intervention. There are numerous additional conditions that could generate this alarm including a hardware fault. Contact your local Nortel Networks technical support group if problems persist with a static cable configuration.

7026 5001

Component	Severity	Status
Lp/<num1> Tr/<num2>	warning	message

Legend

<num1> = 0 - 15

<num2> = 0 - 5

Details

Issued when an LRC error detected by the token ring transmit hardware. This interrupt implies that a frame has been corrupted some time after being received but prior to transmission.

Probable Cause

Software error

Type

Processing

Remedial action

This error will cause the port to be off line for a period of time, but under normal conditions it will recover without intervention. There are numerous additional conditions that could generate this alarm including a hardware fault. Contact your local Nortel Networks technical support group if problems persist.

7026 5002

Component	Severity	Status
Lp/<num1> Tr/<num2>	warning	message

Legend

<num1> = 0 - 15

<num2> = 0 - 5

Details

Issued when an invalid system request block (SRB) is encountered by the TMS 380.

Probable Cause

Adaptor error

Type

Equipment

Remedial action

This error is not expected under normal conditions. Contact your local Nortel Networks technical support group if problems persist since this error may indicate a hardware failure.

7026 5003

Component	Severity	Status
Lp/<num1> Tr/<num2>	warning	message

Legend

<num1> = 0 - 15

<num2> = 0 - 5

Details

Issued when the station has received a removed request MAC frame from configuration report server, that has resulted in this station withdrawing from the ring.

Probable Cause

lan error

Type

Communications

Remedial action

Modify the configuration report server to allow this station on the ring. Attempt insertion of this station back into the ring by performing a lock/unlock sequence on the port.

7026 5004

Component	Severity	Status
Lp/<num1> Tr/<num2>	critical/cleared	set/clear

Legend

<num1> = 0 - 15

<num2> = 0 - 5

Details

When the status is *set*, the token ring component has detected that no other stations are present on the ring.

A *clear* is issued when another station is detected on the ring.

Probable Cause

lan error

Type

Communications

Remedial action

When the status is *set*, verify the connection of other cables to the MAU, and the connection of the MAU to other MAU's. This alarm may also occur if all other stations on the ring are powered down, or off-line for some other reason.

When the status is *clear*, no remedial action is required.

7026 5005

Component	Severity	Status
Lp/<num1> Tr/<num2>	critical/cleared	set/clear

Legend

<num1> = 0 - 15

<num2> = 0 - 5

Details

When the status is *set*, the token ring component has detected an open or short circuit in the cable between the adapter and the MAU.

A *clear* is issued when the condition is no longer present.

Probable Cause

CableTamper

Type

Communications

Remedial action

When the status is *set*, verify the cable from the port to the MAU is securely attached to the MAU. If condition persists verify that the cable and/or the connector on the MAU is not defective.

When the status is *clear*, no remedial action is required.

7026 5006

Component	Severity	Status
Lp/<num1> Tr/<num2>	critical/cleared	set/clear

Legend

<num1> = 0 - 15

<num2> = 0 - 5

Details

When the status is *set*, the token ring adapter has detected a loss or absence of signal, and was unable to transmit to itself while wrapped through its lobe at the wiring concentrator.

A *clear* is issued when the condition is no longer present.

Probable Cause

CableTamper

Type

Communications

Remedial action

When the status is *set*, verify the cable is securely connected to the card. If condition persists verify that the cable is not defective.

When the status is *clear*, no remedial action is required.

7026 5007

Component	Severity	Status
Lp/<num1> Tr/<num2>	warning	message

Legend

<num1> = 0 - 15

<num2> = 0 - 5

Details

Issued when an error has been detected during the open phase of initialization. This alarm is issued when conditions such as signal loss, beaconing, insertion failure, active monitor ring purge time out, duplicate address, ring parameter server not responding, or remove ring station MAC frame received are present.

Probable Cause

lan error, Software error

Type

Communications, Processing

Remedial action

The remedial action for this alarm is dependent on the specifics provided in the alarm message. The duplicate address condition must be resolved before attempting another insertion into the ring. If a remove MAC frame is received it must be addressed as described in alarm 7026 5003. A beacon MAC frame received during the physical insertion phase could indicate a ring speed mismatch is present. Another attempt to insert the station into the ring can be attempted with a lock/unlock sequence on the port. Contact your local Nortel Networks technical support group if problems persist since this error may indicate a hardware failure.

7026 5008

Component	Severity	Status
Lp/<num1> Tr/<num2>	warning	message

Legend

<num1> = 0 - 15

<num2> = 0 - 5

Details

Issued when an interrupt request from the adapter fails to provide a stable status value within the allotted time window.

Probable Cause

Adaptor error

Type

Equipment

Remedial action

The remedial action for this alarm to perform a lock/unlock sequence on the port. This will allow the diagnostics to verify the integrity of the hardware. If diagnostics are successful another attempt will be made to insert the station into the ring. Contact your local Nortel Networks technical support group if problems persist since this error may indicate a hardware failure.

7026 5009

Component	Severity	Status
Lp/<num1> Tr/<num2>	warning	message

Legend

<num1> = 0 - 15

<num2> = 0 - 5

Details

Issued when the interrupt rate from the TMS 380 is faster than the processing rate for these interrupts. This message would indicate a ring that is unstable, or experiencing a large number or exceptions.

Probable Cause

Adaptor error

Type

Equipment

Remedial action

No remedial action is required, however it is recommended that a lock/unlock sequence on the port be performed to verify the integrity of the hardware. Contact your local Nortel Networks technical support group if problems persist since this error may indicate a hardware failure on this station or some other station on the ring.

7026 500A

Component	Severity	Status
Lp/<num1> Tr/<num2>	warning	message

Legend

<num1> = 0 - 15

<num2> = 0 - 5

Details

Issued when a failure occurs during the TMS 380 bring up diagnostics (BUD) test. The details of the specific problem are provided in the alarm message.

Probable Cause

Adapter error

Type

Equipment

Remedial action

Perform a lock/unlock sequence on the port to verify a consistent failure. Contact your local Nortel Networks technical support group if problems persist since this error may indicate a hardware failure.

7031 2000

Component	Severity	Status
Ppp/<instance>	critical/cleared	set/clear

Legend

<instance> = a decimal value

Details

When the status is *set*, the *Ppp* component has been taken out of service due to poor line quality.

When the status is *clear*, good line quality has been restored and the *Ppp* component will resume providing service.

The OSI administrative state attribute in the alarm specifies the new administrative state for the *Ppp* component.

Probable Cause

Type

Remedial action

When the status is *set*, the condition can be cleared by correcting the poor line quality condition, changing the quality threshold (*Ppp/<instance> LinkQualityThreshold*), or by disabling link quality monitoring (*Ppp/<instance> LinkQualityMonitor configStatus*).

When the status is *clear*, no remedial action is required.

7031 2001

Component	Severity	Status
Ppp/<instance>	critical/cleared	set/clear

Legend

<instance> = a decimal value

Details

When the status is *set*, the *Ppp* component has been taken out of service due to a looped back line. This condition has been detected because the *Ppp* component has received the same Magic Number it sent out.

When the status is *clear*, the looped back line condition has been cleared and the *Ppp* component will resume providing service.

The OSI administrative state attribute in the alarm specifies the new administrative state for the *Ppp* component.

Probable Cause

Type

Remedial action

When the status is *set*, the condition can be cleared by correcting the looped back line condition or by disabling Magic Number (*Ppp/<instance> Link configMagicNumber*) and locking and unlocking *Ppp* component.

When the status is *clear*, no remedial action is required.

7031 2002

Component	Severity	Status
Ppp/<instance>	critical/cleared	set/clear

Legend

<instance> = a decimal value

Details

When the status is *set*, the *Ppp* component has been taken out of service due to the Ppp Link Control Protocol (Lcp) leaving the Open state.

When the status is *clear*, Lcp has entered the Open state and the *Ppp* component will resume providing service.

When the status is *clear*, Lcp has entered the Open state and the *Ppp* component will resume providing service.

The OSI administrative state attribute in the alarm specifies the new administrative state for the *Ppp* component.

Probable Cause

Type

Remedial action

When the status is *set*, viewing of *Ppp/<instance>* and related component's operational attributes will help to further isolate the actual cause of the failure. This condition has occurred for one or more of the following reasons:
- Physical link connection is unavailable
- Peer PPP connection has been terminated
- PPP connection has been rejected
- Link Continuity Monitor has detected loss of connection

When the status is *clear*, no remedial action is required.

7032 0001

Component	Severity	Status
FrDte/<instance>	critical/cleared	set/clear

Legend

<instance> = a decimal value

Details

When the status is *set*, the *FrDte* component has been taken out of service due to a service-affecting condition detected by LMI at the user-network interface.

When the status is *clear*, service has been restored.

The OSI state attributes in the alarm specifies the OSI states for the *FrDte* component at the time of the alarm.

Probable Cause

Type

Remedial action

When the status is *set*, viewing of the *FrDte/<instance>* and related *Dlci* component operational attributes will help to further isolate the actual cause of the failure. This condition has occurred for one or more of the following reasons:
- The DCE is not responding to Status Enquiry polls.
- The DTE/DCE are running different LMI procedures.

When the status is *clear*, no remedial action is required.

7035 0001

Component	Severity	Status
EM/<node name>	warning	message

Legend

<node name> = name of the Passport node

Details

The Statistics Management System has detected that regular statistics update poll for one of the applications whose name is shown in the comment data of the alarm record was not successful after two consecutive attempts. The result of not being able to poll is that some of the statistics data is not collected properly on CP from LP's. Upon LP failures, statistics data may be lost forever. The cause of the alarm may be message excessive congestion on the module.

Probable Cause

Type

Remedial action

No action is required. The module will automatically attempt to poll same statistics again in 15 minutes. If the problem persists contact Nortel Networks support.

7035 0002

Component	Severity	Status
EM/<node name>	warning	message

Legend

<node name> = name of the Passport node

Details

The Statistics Management System has detected that more than one application regular statistics polls were not successful within last poll cycle. The result of multiple application poll failures is that the regular poll time duration had increased from fifteen minutes to some larger value. The cause of the alarm may be continuous excessive message congestion on the module.

Probable Cause

Type

Remedial action

No action is required. The module will automatically attempt to poll same statistics again in next poll cycle. If the problem persists contact Nortel Networks support.

7036 0005

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

APPN Resources Manager memory shortage. The operator data describes the problem in more detail.

0005 - Insufficient storage to start a transaction program instance and conversation requested by a received Attach (FMH5).

0008 - Insufficient storage to start a new conversation requested by ALLOCATE, MC_ALLOCATE or CMALLC.

0019 - Deactivating session because of insufficient storage.

0020 - Insufficient storage to initiate session activation requested by ALLOCATE, MC_ALLOCATE or CMALLC.

0028 - Insufficient storage to deactivate a limited resource session. This could result in a limited resource link being kept active while they are not required.

0048 - Insufficient storage to start the transaction program instance requested by TP_STARTED. If other instances of the same transaction program are active APPN queues the request waiting for one of them to become free. Otherwise the verb fails.

0049 - Insufficient storage to initiate automatic session activation. Fewer active sessions are available on the specified mode, which may cause application delays or failures.

0050 - Insufficient storage to initiate session activation requested by ACTIVATE_SESSION verb.

Probable Cause

Type

Remedial action

Attention: Local Admin

Investigate memory shortage. Re-engineer FP with less functionality to reduce memory usage.

Operator Data

DCL Problem Determination Index
Local LU Alias
Partner LU Alias
Mode Name
Session Identifier
Transaction Program name {optional)

7036 0027

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
APPN Resources Manager has failed to verify security on an LU-LU session.

Effect: The LU fails the session.

Probable Cause

Type

Remedial action
Attention: Local Admin

Check that the password defined for the specified local LU and partner LU matches that defined at the partner LU.

Operator Data
Local LU

Partner LU

Mode name

Session ID

7036 0042

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
LU-LU verification protocol error. This may indicate an interoperability problem.

The session is deactivated with the specified sense code.

Probable Cause

Type

Remedial action
Contact support with details of the problem.

Operator Data
SNA sense code

Local LU (Alias)

Partner LU (Alias)

Mode name

Session Identifier

7036 0047

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

APPN Resources Manager was unable to activate a new session because the maximum session limit specified for the session mode or the local LU would be exceeded.

Effect: **ALLOCATE**, **MC_ALLOCATE**, or **CMALLC** verbs either fail or hang waiting for a session to become free.

Probable Cause

Type

Remedial action

The mode session limit can be increased using **DEFINE_MODE** parameter mode_max_neg_sess_limit. The LU session limit can be increased using **DEFINE_LOCAL_LU**.

These resources are not currently accessible through the CAS or Preside Multiservice Data Manager interfaces.

Operator Data

Local LU

Partner LU

Mode name

7036 0051

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

Transaction program (APPC) bracket protocol error. This may indicate a problem in the partner LU. The sense codes are as follows:

2008 0000 - partner LU attempted to start bracket after sending BIS.

2003 0000 - partner LU attempted to start bracket after local LU hand BID for session successfully, unexpected RTR request received.

2010 0000 - received negative response to BID with sense code 088B0000 from a partner LU who supports parallel sessions, or BIS protocol error.

The session is deactivated with the specified sense code reported to the far end

Probable Cause

Type

Remedial action

This may indicate a configuration error at either end of the connection or an incorrectly implemented transaction program. Contact technical support.

Operator Data

Sense Code

Local LU (Alias)

Partner LU (Alias)

Mode name

Session identifier

Request code

7036 0052

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

Transaction program (APPC) attach protocol error. This may indicate a problem in the partner LU. The sense codes are as follows:

080F6051 - Attach security protocol violation

1008 6011 - Logical unit of work (LUW) identifier format error, or LUW identifier not specified when synchronization level is syncpt.

1008 6040 - synchronization level not supported by session, or already-verified not accepted from partner LU.

1008 6031 - APPC program initialization parameters (PIP) not allowed by transaction program.

The session is deactivated with the specified sense code reported to the far end.

Probable Cause

Type

Remedial action

This may indicate a configuration error at either end of the connection or an incorrectly implemented transaction program. Contact technical support.

Operator Data

Sense Code

Local LU (Alias)

Partner LU (Alias)

Mode name

Session identifier

Attach request unit

7036 0053

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
Attach conversation rejected because security information invalid. This indicates an attempt to access a secure transaction program by an unknown user, or a known user who has specified an incorrect password.

Effect: The LU fails the session.

Probable Cause

Type

Remedial action
Use the operator data to locate the attempted security violation.

Operator Data
Sense Code

Local LU

Partner LU

Mode name

Session ID

Transaction Program name

User identifier

supplied password

7036 0054

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
An APPC transaction attach was rejected because the specified sync level is not supported by the specified transaction program. This may be a mismatch in the capabilities of the originating transaction program and the destination transaction program, or it may simply be a configuration error.

Effect: the attach will be rejected.

Probable Cause

Type

Remedial action
Check the sync level supported by the specified transaction program.

Operator Data
Sense Code

Local LU (Alias)

Partner LU (Alias)

Mode name

Session Identifier

Transaction Program name

Sync Level

7036 0056

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

An APPC transaction attach was rejected because the specified transaction program is permanently disabled. This should only occur if the operator has explicitly disabled the transaction program by issuing a Lock on the Transaction Program component.

Note: The Transaction Program component is not currently visible through the CAS/Preside Multiservice Data Manager interface.

Probable Cause

Type

Remedial action

If the transaction program should not be disabled issue an Unlock on the Transaction Program component.

Operator Data

Sense Code

Local LU (Alias)

Partner LU (Alias)

Mode name

Session Identifier

Transaction Program name

7036 0057

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
The APPN node was unable to activate a new session because the mode name specified was not recognized.

Probable Cause

Type

Remedial action
Check the mode name.

Operator Data
Local LU (Alias)

Partner LU (Alias)

Mode name

7036 0058

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
An APPC transaction attach was rejected because security information was not specified. This indicates an attempt to access a secure TP without specifying a user identification or a password.

Effect: The attach will be rejected.

Probable Cause

Type

Remedial action
Locate the security mismatch.

Operator Data
Sense Code

Local LU (Alias)

Partner LU (Alias)

Mode name

Session Identifier

Transaction Program name

7036 0059

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
BIS protocol error. This may indicate a problem in the partner LU. The sense code is always set to 20100000.

Effect: The session is deactivated with the specified sense code.

Probable Cause

Type

Remedial action
Contact support with details of the problem.

Operator Data
Sense code

Local LU (Alias)

Partner LU (Alias)

Mode name

Session identifier

Reply

7036 0060

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

A type 3 XID containing an XID Negotiation Error (0x22) control vector was received from a remote node.

Probable Cause

Type

Remedial action

Use the sense data contained in the alarm to determine the cause of the XID negotiation error.

Operator Data

Sense Code

XID containing the error control vector.

7036 0061

Component	Severity	Status
APPN/<name> Port/<portname>	minor	message

Legend

<name> = name of the APPN router

<portname> = name of the logical port

Details

The number of XID frames received during link activation exceeded the limit defined for the port. This could indicate an XID protocol error by an attached station, or an excessively unreliable physical medium.

Effect: Link activation fails.

Probable Cause

Type

Remedial action

Attention: User/Local Admin/Remote Admin

Increase the XID frame exchange limit on the Port. If APPN is still unable to activate the link station, trace the link station or port to isolate the problem.

Note: The XID frame exchange limit is not currently modifiable through the CAS/Preside Multiservice Data Manager interface.

Operator Data

Port name

Link station name

Adjacent CP name

XID frame count

Port XID frame limit

Sense code

7036 0062

Component	Severity	Status
APPN/<name> Port/<portname>	minor	message

Legend

<name> = name of the APPN router

<portname> = name of the logical port

Details

The number of XID frames received during non-activation exchange exceeded that defined for the port. This could indicate an XID protocol error by an attached station, or an excessively unreliable physical medium.

Effect: Non-activation XID frame exchange fails and the link is deactivated.

Probable Cause

Type

Remedial action

Attention: User/Local Admin/Remote Admin

Note: The XID frame exchange limit is not currently modifiable through the

CAS/Preside Multiservice Data Manager interface.

Operator Data

Link station name

Adjacent CP name

non-activation XID frame count

Port non-activation XID frame limit

7036 0063

Component	Severity	Status
APPN/<name> LS/<linkstationname>	minor	message

Legend

<name> = name of the APPN router

<linkstationname> = name of the link station

Details

APPN Configuration Services was unable to perform some function due to a memory shortage. The operator data provides more details.

0063 Insufficient storage to activate a link. Activation fails.

0072 Insufficient storage to perform orderly link deactivation, performing immediate deactivation instead.

0074 Insufficient storage to update ANR routing tables following deactivation of an HPR-capable link.

0075 Insufficient storage to update ANR routing tables following activation of an HPR-capable link

0079 Insufficient storage to forward Alert generated by DLC.

0111 Insufficient storage to end intra-node sessions properly.

0114 Insufficient storage to generate link Alert.

0122 A DCL could not be started either because of insufficient resources, or because the specified DLC type is not supported.

0127 Insufficient storage to update topology database with link station information.

0128 Insufficient storage to update topology database with connection network information.

0129 Insufficient storage to enable intra-node sessions.

Probable Cause

Type

Remedial action

Attention: User/Local Admin

Investigate resource shortage. Re-engineer FP with less functionality or system load to reduce memory usage.

Operator Data

DCL Problem Determination Index

other fields dependent upon DCL Problem Determination Index

7036 0064

Component	Severity	Status
APPN/<name> LS/<linkstationname>	minor	message

Legend

<name> = name of the APPN router

<linkstationname> = name of the link station

Details

This alarm is issued when an XID3 is received from an adjacent back-level LEN node (not carrying a network name control vector) but there is no link configured to that back-level LEN node. An implicit link cannot be activated because the adjacent node's CP name is not known.

Effect: Inbound link activation fails.

Probable Cause

Type

Remedial action

Attention: User/Local Admin/Remote Admin

Define a link station (using DEFINE_LS) with adj_cp_type set to NAP_BACK_LEVEL_LEN_NODE.

Operator Data

Sense code

Port name

LS name

7036 0065

Component	Severity	Status
APPN/<name> LS/<linkstationname>	minor	message

Legend

<name> = name of the APPN router

<linkstationname> = name of the link station

Details

This alarm is issued when the link to host is not configured properly (that is, when it is configured as a link to a Type 2.1 node).

Effect: Link activation fails.

Probable Cause

Type

Remedial action

Attention: User/Local Admin/Remote Admin

Define or redefine link station (using DEFINE_LS) with adj_cp_type set to NAP_HOST_XID3 or NAP_HOST_XID0.

Operator Data

Sense code

Port name

LS name

7036 0066

Component	Severity	Status
APPN/<name> LS/<linkstationname>	minor	message

Legend

<name> = name of the APPN router

<linkstationname> = name of the link station

Details

This alarm is issued when there is an error in link activation, as described by the operator data. The sense codes have the following interpretation:

0801-0012 - an APPN connection cannot be established because the node has no available integers to represent a new TG.

0806-002C - the adjacent node has changed its network name during the course of an XID exchange

0809-003A - a null XID was received when an activation XID3 was expected.

0809-003B - a null XID was received when a non-activation XID3 was expected.

0809-003C - a prenegotiation XID was received when not expected.

0809-003D - a non-activation XID was received when a null XID or activation XID was expected.

0809-003E - an activation XID was received when a non-activation XID was expected.

0809-003F - adjacent node initiated a secondary-initiated non-activation XID exchange on a link that does not support secondary-initiated non-activation XID exchanges.

0809-0040 - a mode-setting command was received and was either not expected or invalid for the receiving node

0809-0042 - a non-activation exchange initiation indicator not set when expected.

0809-0045 - the adjacent node has stopped supporting exchange state indicators in the middle of an XID exchange.

0809-0046 - the adjacent node had previously indicated it did not support exchange state indicators, but has sent a XID with exchange state indicators set.

0809-0047 - received XID after receiving mode setting command.

0809-0048 - received unsolicited XID from NRM secondary link station.

0809-0049 - the adjacent node sent an XID error control vector (x’22’).

0809-004E - a non-null XID was received from a secondary NRM link station when a null XID was expected.

0809-0055 - invalid VRN in TG descriptor CV of XID3.

086F-0000 - XID3 control vector length error.

088C-1000 - the adjacent node is a network node, but did not include a product set identifier control vector in the XID3.

088C-0EF1 - the adjacent node is type 4 or 5, but did not include a PU name control vector.

088C-0EF4 - the adjacent node has no been inconsistent in including a network name control vector.

088C-4680 - an XID was received on an ATM port, but did not include a TG identifier TG descriptor subfield.

0891-0004 - the network name control vector does not contain a valid network identifier.

0891-0005 - the network name control vector does not contain a valid CP name.

0895-xxyy - XID3 control vector error (xx indicates key of first control vector in error, yy indicates offset of error within control vector).

0896-0000 - control vector too long.

0896-0001 - network name control vector is too long.

1015-0001 - received XID3 is too short (less than 29 bytes).

1015-0002 - length of received XID3 does not match length indicated in XID3.

1016-0000 - the adjacent node indicated an invalid BIND pacing setting.

1016-0001 - the maximum number of I-frames that the adjacent node can receive before sending an acknowledgement is set to zero.

1016-0002 - adjacent node has been inconsistent in its setting of ACTPU suppression indicator.

1016-0003 - the maximum BTU size the adjacent node can receive is set to less than 99 bytes.

1016-0004 - unexpected XID format.

1016-0005 - the adjacent end node supports receipt of BIND segments, but does not support BIND segment generation.

1016-0006 - the adjacent end node does not support receipt of BIND segments and has a maximum BTU size less than 265 bytes.

1016-0007 - the adjacent network node does not support receipt of BIND segments and has a maximum BTU size less than 521 bytes.

1016-0008 - adjacent node has been inconsistent in its setting of networking

capabilities.

1016-0009 - the adjacent network node supports CP-CP sessions but does not provide CP services.

1016-000B - the adjacent node has selected zero as the TG number (which is invalid).

1016-000C - the adjacent network node does not support BIND segment generation and has a maximum BTU size less than 521 bytes.

1016-000D - the adjacent node does not support the SDLC command/response profile (which is the only profile supported by APPN and LEN nodes).

1016-000E - product set identifier on XID3 has changed.

1016-0010 - the ABM support indicated in sent and received XID3s is inconsistent.

1016-0013 - the DLC type in sent and received XIDs are not in agreement.

1016-0014 - adjacent node changed role from non-negotiable to negotiable.

1016-0015 - the adjacent node supports BIND pacing as sender only.

1016-0017 - after two exchanges, randomized node IDs sent by this node and adjacent node are still identical.

1016-0019 - adjacent node has attempted to change its CP name when CP-CP sessions supported on link station, or link station not quiesced.

1016-001A - the adjacent node is inconsistent in its support for parallel TGs.

1016-001B - the adjacent node provides or requests CP services but does not support CP-CP sessions.

1016-001C - the adjacent node indicated an LS role that was not primary, secondary or negotiable.

1016-001E - the adjacent node did not send its CP name in XID3 but requested CP-CP sessions on this link.

1016-0020 - adjacent node is not type 2, 4 or 5.

1016-0022 - the adjacent node included an HPR Capabilities [X’61’] control vector in its XID3 but specified a maximum BTU size less than 768.

1016-0023 - the adjacent node included an HPR Capabilities [X’61’] control vector in its XID3 but specified an invalid ANR label length (i.e. less than 1 or greater than 8).

1016-0026 - NCE field lengths in the HPR Control Flows [X’81’] subfield are inconsistent with the length of the HPR Capabilities [X’61’] control vector.

1016-0027 - the adjacent node indicated support for control flows over RTP, but did not include a HPR Control Flows [X’81’] subfield.

1016-0028 - adjacent node has specified an invalid error mode in its HPR

Capabilities CV.

1016-0034 - adjacent node indicated no support for LDLC, but the local node only supports LDLC.

1016-0044 - adjacent node indicated support for LDLC, but did not include an LLC SAP subfield in the HPR Capabilities CV.

Effect: Link activation fails.

Probable Cause

Type

Remedial action

Attention: User/Local Admin

Run a trace on the link station or port to obtain more diagnostic information on the problem. Contact support with details of the problem.

Operator Data

Sense code

Port name

LS name

Adjacent CP name

Byte offset

Bit offset

XID frame

7036 0067

Component	Severity	Status
APPN/<name> LS/<linkstationname>	minor	message

Legend

<name> = name of the APPN router

<linkstationname> = name of the link station

Details

This alarm is issued when there are no free TG numbers available between this node and the specified adjacent node. This should only occur if there are already 236 parallel TGs between this node and the adjacent node.

Effect: Link activation fails.

Probable Cause

Type

Remedial action

Reconfigure the network to reduce the number of parallel TGs between this node and the specified adjacent node.

Operator Data

Sense Code

Port Name

Linkstation Name

Adjacent CP Name

7036 0069

Component	Severity	Status
APPN/<name> LS/<linkstationname>	minor	message

Legend

<name> = name of the APPN router

<linkstationname> = name of the link station

Details

There was an error in link activation, the link to a host is not configured correctly.

Effect: Link activation fails.

Probable Cause

Type

Remedial action

Reconfigure the linkstation with the correct adjacent CP type.

Operator Data

Sense code

Port Name

Linkstation Name

7036 0071

Component	Severity	Status
APPN/<name> LS/<linkstationname>	minor	message

Legend

<name> = name of the APPN router

<linkstationname> = name of the link station

Details

There was an attempt to activate more than one TG to an adjacent node that does not support parallel TGs.

Effect: Link activation fails.

Probable Cause

Type

Remedial action

Modify the configuration so that there is only one link station defined to the specified adjacent node.

Operator Data

Sense code

Port Name

Linkstation Name

Adjacent CP Name

7036 0082

Component	Severity	Status
APPN/<name> Port/<portname>	minor	message

Legend
<name> = name of the APPN router

<portname> = name of the logical port

Details
Port deactivation has failed.

Effect: Port may not restart successfully.

Probable Cause

Type

Remedial action
Verify that the virtual circuit is connected.

Operator Data
DLC Name

Port Name

7036 0084

Component	Severity	Status
APPN/<name> Port/<portname>	minor	message

Legend

<name> = name of the APPN router

<portname> = name of the logical port

Details

A DLC has ended abnormally or there is an unrecoverable DLC failure.

Effect: All ports and link stations defined on the DLC are inoperative.

Probable Cause

Type

Remedial action

Restart the DLC and ports (using START_DLC and START_PORT commands). If the problem persists, run a trace on the DLC and contact support with the log and trace information.

Operator Data

DLC Name

7036 0088

Component	Severity	Status
APPN/<name> Port/<portname>	minor	message

Legend

<name> = name of the APPN router

<portname> = name of the logical port

Details

APPN Configuration Services was requested to activate a link for a Connection Network it received an ACTIVATE_ROUTE) but was unable to perform this because the link-activation limit for the port had been reached.

Effect: The link is not activated and is not until other links serviced by the port are deactivated.

Developer note. When the alarms consolidated under 0065 are updated to include the LS name, and when the CN component is added to the management hierarchy, then this alarm will be consolidated with them.

Probable Cause

Type

Remedial action

Attention: Local Admin

Contact technical support.

Operator Data

CN name

[Port name moved to component name]

Sense code 0850-0001

7036 0089

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
APPN Configuration Services was requested to activate a link for a Connection Network (it received an ACTIVATE_ROUTE) that was unknown to it.

Effect: The link is not activated, and this may indicate a serious internal error.

Probable Cause

Type

Remedial action
Attention: Local Admin

Investigate why SS sent ACTIVATE_ROUTE.

Operator Data
VRN name

Sense code 0806-002B

7036 0090

Component	Severity	Status
APPN/<name> Port/<portname>	minor	message

Legend

<name> = name of the APPN router

<portname> = name of the logical port

Details

APPN Configuration Services was requested to activate an outbound link (it received a CONNECT_IN) but was unable to because the link activation limit for the port had been reached.

Effect: The link is not activated.

Probable Cause

Type

Remedial action

Attention: Local Admin

Contact technical support.

Operator Data

Port name

7036 0091

Component	Severity	Status
APPN/<name> LS/<linkstationname>	minor	message

Legend

<name> = name of the APPN router

<linkstationname> = name of the link station

Details

The format 3 XID received from an adjacent node indicates different parameter than are expected.

Effect: Link activation fails.

Probable Cause

Type

Remedial action

Check that the parameters defined for this linkstation are correct.

Operator Data

Sense code

Port Name

Linkstation Name

7036 0112

Component	Severity	Status
APPN/<name> LocTg/<vrnname>,<tgnum>	minor	message

Legend

<name> = name of the APPN router

<vrnname> = name of the adjacent node

<tgnum> = TG number of this TG

Details

APPN Configuration Services was requested to activate a link for a Connection Network (it received an ACTIVATE_ROUTE) for a Transmission Group number that was unknown to it.

Effect: The link is not activated. APPN Configuration Services discards the ACTIVATE_ROUTE but this may indicate an internal error.

Probable Cause

Type

Remedial action

Attention: Local Admin

Investigate why SS sent ACTIVATE_ROUTE.

Operator Data

VRN name

Transmission Group number

Sense code 0806002B

7036 0121

Component	Severity	Status
APPN/<name> Ls/<linkstationname>	minor	message

Legend

<name> = name of the APPN router

<linkstationname> = name of the link station

Details

Requested APPN Control Point CP-CP sessions could not be established on a link since the remote system did not support them.

Effect: CP-CP sessions are not established.

Probable Cause

Type

Remedial action

Attention: Remote Admin

Investigate configuration mismatch.

Operator Data

Link Station name

Adjacent APPN Control Point name

7036 0133

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
Conversation ended.

Probable Cause

Type

Remedial action
Attention: Local/Remote Admin

Investigate cause of protocol error.

Operator Data
DCL Problem Determination Index

APPN Transaction Program name

APPN Transaction Program ID

Conversation ID

Partner LU name

Local LU name

Mode name

Session ID

7036 0134

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
The session being used by a conversation has been deactivated because of a session outage, causing the conversation to fail.

Probable Cause

Type

Remedial action
Attention: Local/Remote Admin

Investigate the cause of the outage.

Operator Data
DCL Problem Determination Index

APPN Transaction Program name

APPN Transaction Program ID

Conversation ID

Partner LU name

Local LU name

Mode name

Session ID

7036 0137

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

The local TP or partner TP issued a [MC_]SEND_ERROR verb or DEALLOCATE verb. The operator data provides more details.

137 The partner TP issued the verb.

138 The local TP issued the verb.

Effect: A new conversation will fail to begin, or an existing one will experience a problem. Subsequent recovery or termination of the conversation will be determined by the applications.

Probable Cause

Type

Remedial action

Attention: Local/Remote Admin

Check that both transaction programs exist, are correctly named, and are working properly.

Operator Data

DCL Problem Determination Index

APPN Transaction Program name

APPN Transaction Program ID

Conversation ID

Partner LU name

Local LU name

Mode name

Session ID

Error Data

7036 0141

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

This alarm indicates that there is insufficient memory storage. The operator data provides more details.

141 The local LU failed to add an entry to the signed-on-to list when sending a PV sign-on Attach (FMH-5) due to resource shortage. The Attach is sent, but does not contain the sign-on request.

142 The local LU was unable to process a Sign-Off verb issued by a local TP due to resource shortage. The Sign-Off request fails, and any entries in the signed-on-to and sign-on-from lists remain valid.

159 Insufficient storage to initialize the half session. The half session fails to activate with the specified sense code.

Probable Cause

Type

Remedial action

Reduce the system load or make more storage available to SNAP APPN.

Operator Data

DCL Problem Determination Index

other fields dependent upon DCL Problem Determination IndexLocal

7036 0143

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

This alarm indicates that an error has been detected on an APPC mapped conversation. The operator data provides more details.

143 SNAP APPN detected a mapped conversation protocol error on an APPC mapped conversation.

144 SNAP APPN received an error data GDS variable on an APPC mapped conversation.

Effect: The conversation is terminated, either by an APPC primary_rc of NAP_CONV_FAILURE_NO_RETRY, or a CPI-C return-code of CM_RESOURCE_FAILURE_NO_RETRY. The partner TP fails the conversation with an APPC primary_rc of NAP_DEALLOCATE_ABEND or a CPI-C return_code of CM_DEALLOCATE_ABEND. The session is not deactivated.

Probable Cause

Type

Remedial action

Report the protocol error to partner LU support. If additional diagnostic information is required, run a link trace (the session identifier can be used to correlate this log to other logs which contain the appropriate link station name).

Operator Data

DCL Problem Determination Index

TP name

TP identifier

Conversation identifier

Local LU

Partner LU

Mode name

Session identifier

7036 0145

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
An LU received an aping with data length greater than the maximum allowed.

Effect: The conversation is terminated with primary_rc of DEALLOC_ABEND.

Probable Cause

Type

Remedial action
Report the error. SNAP APPN LUs should not be apinged with a data size greater than the defined maximum.

Operator Data
Local LU (Alias)

Partner LU(Alias)

Mode name

Max aping size allowed

7036 0150

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
The CRV exchange has failed, indicating that the cryptography keys configured at this LU and the partner LU are inconsistent.

Effect: Session is deactivated.

Probable Cause

Type

Remedial action
Correct the mismatch in cryptography keys.

Operator Data
DCL Problem Determination Index

other fields dependent upon DCL Problem Determination Index

7036 0151

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

LU6.2 session error or protocol error during CRV exchange. This may indicate an interoperability problem. Sense codes are as follows:

080F-6051 - security error

1002-0000 - CRV RU too short

1003-0000 - function not supported (unrecognized request code)

1005-0000 - SIGNAL or LUSTAT request too short

1008-4001 - invalid FM header type

2002-0000 - chaining sequence error

2003-0000 - bracket state error

2004-0000 - received normal flow request when half-duplex flip-flop state was not receive

2009-0000 - CRV request received from secondary LU, or CRV response received from primary LU, or CRV not received when expected.

200A-0000 - immediate request mode violated by partner LU

200B-0000 - queued response indicator invalid

200E-0000 - unexpected SIGNAL response, or uncorrelated positive response, or uncorrelated RTR response

200F-0000 - received unexpected response or received EXPD RU before previous EXPD RU has been acknowledged

2012-0000 - unexpected sense code on negative response

4003-0000 - BB not allowed

4004-0000 - received RQE, BB, CEB chain from contention loser, or CEB or EB not allowed

4008-0000 - CRV with PI set

4007-0000 - definite response not allowed

4009-0000 - CD not allowed

400B-0000 - chaining error or EC,RQE1/2,CD RU received on full-duplex conversation, or CRV chain indicators not set to BC,EC

400C-0000 - bracket error, or CRV request with BBI, EBI or CEB1 set

400D-0000 - CRV request with CDI set

400F-0000 - incorrect use of format indicator (FI), or CRV with FI not set

4010-0000 - alternate code not supported, or CRV request with CSI set to CODE1

4011-0000 - RU category of response does not match request, or incorrect specification of RU category, or CRV not expedited

4012-0000 - request code of response does not match request, or incorrect specification of request code

4013-0000 - incorrect specification of SDI and RTI, or CRV response RTI and SDI inconsistent

4014-0000 - incorrect use of DR1I, DR2I and ERI, or CRV not RQD1

4015-0000 - incorrect use of QRI, or CRV with QRI not set

4016-0000 - incorrect use of EDI, or CRV request with EDI set

4017-0000 - incorrect use of PDI, or CRV request with PDI set

4018-0000 - incorrect setting of QRI with bidder’s BB

4019-0000 - incorrect indications with last-in-chain request

4021-0000 - QRI setting on response does not match request

Probable Cause

Type

Remedial action

Use information on the session deactivated problem log (271) to identify the local LU and partner LU. If required, run a trace on the specified link station and contact support with the log and trace.

Operator Data

Sense code

Linkstation Name

LFSID

FQPCID

7036 0155

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
LU6.2 session ended abnormally because of insufficient storage.

Effect: session will be deactivated.

Probable Cause

Type

Remedial action
Investigate resource shortage. Re-engineer FP with less functionality to reduce memory usage.

Operator Data
Sense code

Linkstation Name

LFSID

FQPCID

7036 0157

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

A SIGNAL RU or EXPD RU has been received. The operator data provides more details.

157 An incoming SIGNAL RU has been received on a full-duplex conversation. The session is deactivated with the specified sense code (10030004).

158 An EXPD RU has been received while previous expedited data remains to be processed. The session is deactivated with the specified sense code (200F0000).

Probable Cause

Type

Remedial action

Contact support with details of the problem.

Operator Data

DCL Problem Determination Index

Sense code

Linkstation Name

LFSID

FQPCID

7036 0170

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
Session error or RU length error. This may indicate an interoperability problem. The session is deactivated with the specified sense code. Sense codes are as follows:

2011-0000 - sender has overrun pacing window, or PI not set on first RU of window

2011-0001 - unexpected IPM

2011-0002 - PI set on other than first RU in window

2011-0003 - invalid pacing response

1001-0003 - invalid IPM format

8007-0000 - segmenting error

8007-0001 - segmentation not supported on this link

1002-0000 - RU length error

Probable Cause

Type

Remedial action
Use the information on the session deactivated problem log (271) to identify the local LU and partner LU. If required, run a trace on the specified link station and contact support with the log and trace.

Operator Data
DCL Problem Determination Index

Sense code

Linkstation Name

LFSID

Max RU length (optional)

TH

RH

RU

7036 0184

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

This alarm indicates that there is insufficient memory storage. The operator data provides more details.

184 Insufficient storage to generate Alert to report invalid received data. Alert is not generated.

190 Insufficient storage to start link-inactivity timer. Limited resource link is not automatically deactivated. If the link is idle, deactivate it using STOP_LS.

191 Insufficient storage to forward HPR Network Layer Packet. NLP is discarded. If this error occurs frequently, it may cause RTP connections to path-switch or fail altogether.

192 Insufficient storage to register ANR label. HPR traffic using this ANR label is not routed correctly, which may cause RTP connections to path-switch, or fail altogether.

Probable Cause

Type

Remedial action

Attention: Local Admin

Investigate memory shortage. Re-engineer FP with less system load or functionality to reduce memory usage.

Operator Data

DCL Problem Determination Index

Other fields dependent upon DCL Problem Determination Index

7036 0195

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

Unable to correlate DLC credit for MLTG link

This alarm occurs during a window condition in normal link deactivation.

Probable Cause

Type

Remedial action

If several instances of this log appear and poor RTP connection performance is observed, investigate further by querying link stations which are members of MLTGs. Unexpectedly low quantities of data sent over a link may indicate problems with DLC credit. Contact support with details of the problem, including trace of signals sent to and from the DLCs underlying the affected links.

Operator Data

MLTG name

PC process ID

7036 0253

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
Node Operator Facility (NOF) failed to perform some function due to a memory shortage.The operator data provides more details.

253 Insufficient storage to start SNAP APPN. SNAP APPN was not started.

260 Insufficient storage to process received ACTLU. LU-SSCP session will not be started. (an ACTLU negative response with the specified sense code is sent).

Probable Cause

Type

Remedial action
Attention: Local Admin

Investigate memory shortage. Re-engineer FP to reduce memory usage.

Operator Data
DCL Problem Determination Index

Other fields dependent upon DCL Problem Determination Index

7036 0262

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

Required downstream PU template does not exist while activating implicit link on a port specifying implicit PU concentration.

Effect: Implicit link is not activated.

Probable Cause

Type

Remedial action

Define the downstream PU template (using DEFINE_DSPUJ_TEMPLATE) or change the port configuration (using DEFINE_PORT) to disable implicit PU concentration or specify an existing downstream PU template.

Operator Data

Template name

Link name

7036 0263

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

This alarm indicates that the limit on the number of active downstream PU template instances has been reached while activating implicit link on a port specifying implicit PU concentration.

Effect: Implicit link is not activated.

Probable Cause

Type

Remedial action

Raise the instance limit (using DEFINE_DSPU_TEMPLATE) or deactivate an existing link which uses the same template.

Operator Data

Template name

Link name

Instance limit

7036 0264

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

Host LU specified on downstream PU template was found to be a downstream LU while activating implicit link on a port specifying implicit PU concentration.

Effect: Implicit link is not activated.

Probable Cause

Type

Remedial action

Correct the definition of the downstream PU template (using DEFINE_DSPU_TEMPLATE).

Operator Data

Template name

Link name

Host LU name

7036 0265

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

An ACTLU was received for an LU from the wrong SSCP.

Effect: The ACTLU is rejected with sense code 084B0000 (that is, the LU activation attempt fails).

Probable Cause

Type

Remedial action

If the LU must accept the ACTLU for the activation attempt to succeed, the LU definition must be changed so that the LU requires the particular SSCP Identifier that is actually received from the SSCP or accepts any SSCP Identifier.

Operator Data

LU name

PU name

NAU address

Sense code

7036 0270

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

Session Manager failed to perform some function due to memory shortage. The operator data provides more details.

270 Insufficient storage to define a new LU type 6.2. DEFINE_LU or START_NODE will fail.

275 Insufficient storage to activate LU6.2 session. Session activation will fail with the specified sense code.

301 Insufficient storage to activate LU-SSCP session. ACTLU will be rejected with specified sense code.

Probable Cause

Type

Remedial action

Attention: Local Admin

Investigate memory shortage. Re-engineer FP to reduce memory usage.

Operator Data

DCL Problem Determination Index

Other fields depending upon DCL Problem Determination Index

7036 0271

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
Fatal error detected on LU6.2 session.

Effect: Session is deactivated with specified sense code.

Probable Cause

Type

Remedial action
Attention: Local Admin

This log gives additional information on the failed session, but is preceded by another alarm (150, 151, 153, 154, 155, 156 or 157) giving more specific information about the fatal error.

Operator Data
Sense code

Local LU name

Partner LU name

Mode name

LS name

LFSID

Session ID

7036 0272

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
An incoming BIND or +RSP(BIND) has specified a duplex support for the remote LU which is inconsistent with that for existing sessions between the partner LUs.

Effect: The BIND or +RSP(BIND) is rejected.

Probable Cause

Type

Remedial action
Attention: Local Admin

Contact support with details of the problem.

Operator Data
Sense code

New duplex support

Existing duplex support

Local LU (Alias)

Partner LU (Alias)

Mode name

Session ID

7036 0276

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

Abnormal UNBIND request received. This may indicate a configuration error, or a protocol error.

Effect: The session fails with the specified sense code.

Probable Cause

Type

Remedial action

Attention: Local Admin

If the sense code indicates a configuration error, check for inconsistencies between the configuration at the local LU and the configuration at the partner LU. If the configuration is consistent and the problem persists, contact support with details of the problem.

Operator Data

Sense code

Local LU name

Partner LU name

Mode name

UNBIND RU

7036 0302

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
Session limit exceeded.

Effect: Session is brought down or BIND rejected (though if a BIND race is occurring the other session may lose).

Probable Cause

Type

Remedial action
Attention: Local/Remote Admin

Raise the session limits.

Operator Data
LU name

Mode name

Polarity

FSP count

Bidder count

Total limit

FSP limit

Bidder limit

Sense code

7036 0306

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
Found other active mode for partner LU (no parallel sessions).

Effect: This session is not activated.

Probable Cause

Type

Remedial action
Attention: Local/Remote Admin

Investigate the configuration. It is probably mismatched.

Operator Data
Local LU name

Partner LU name

This Mode

Active Mode

Sense code

7036 0315

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

LU-LU verification failed. This is either configuration problem, a migration problem or evidence of a security attack.

Effect: session activation fails.

Probable Cause

Type

Remedial action

Verify the identity of the partner LU and correct any configuration, software or security problems.

Operator Data

Local LU

Partner LU

Sense Code

7036 0318

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
A BIND or BIND-RSP has been received in response to a BIND request. This may indicate a configuration error, or a protocol error. Common sense codes which typically indicate a configuration error or a normal race condition include:

0806-0014 - the partner LU is not known

0806-xxxx - the BIND specified a resource which is not known

080F-xxxx - security authorization failed

0821-xxxx - the BIND supplied an invalid session parameter

0835-xxxx - parameter error in BIND RU at offset xxxx

Other sense codes include:

0812-xxxx - invalid PCID in BIND RU

0852-xxxx - duplicate session activation request

0861-xxxx - invalid COS name in BIND RU

088C-xxxx - control vector or subfield missing from BIND RU

0895-xxxx - BIND RU contained in control vector that was in error

0896-xxxx - BIND RU contained a control vector that was too long

Effect: session activation will fail

Probable Cause

Type

Remedial action
If the sense code indicates a configuration error, check for inconsistencies between the configuration of the local LU and the configuration at the partner LU.

Operator Data
Sense code

Local LU name

Partner LU name

Mode name

BIND RU

7036 0319

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

An UNBIND request was received in response to a BIND request. This may indicate a configuration error or a protocol error.

Common sense codes which typically indicate a configuration error or a normal race condition include:

0805xxxx - the session could not be activated since session activation limits have been reached

0806-0014 - the partner LU is not known

0806-xxxx - the BIND specified a resource which is not known

080F-xxxx - security authorization failed

0821-xxxx - the BIND supplied an invalid session parameter

0835-xxxx - parameter error in BIND RU at offset xxxx

Other sense codes include:

0812-xxxx - session activation failed due to resource shortage at the remote node

083B-xxxx - invalid PCID in BIND RU

0852-xxxx - duplicate session activation request

0861-xxxx - invalid COS name in BIND RU

088C-xxxx - control vector or subfield missing from BIND RU

0895-xxxx - BIND RU contained a control vector that was in error

0896-xxxx - BIND RU contained a control vector that was too long

Effect: session activation will fail.

Probable Cause

Type

Remedial action

If the sense code indicates a configuration error, check for inconsistencies between the configuration at the local LU and the configuration at the partner LU.

Operator Data

Sense code

Local LU name

Partner LU name

Mode name

BIND RU

UNBIND RU

7036 0322

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
Insufficient memory storage. The operator data provides more details.

322 There is insufficient storage to generate an Alert to report a BIND segmentation or pacing error. The Alert will not be sent.

323 There is insufficient storage to process received BIND request. The BIND will be rejected with the specified sense code.

Probable Cause

Type

Remedial action
Investigate resource shortage. Re-engineer FP to reduce memory usage.

Operator Data
DCL Problem Determination Index

Other fields depending upon DCL Problem Determination Index

7036 0324

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
ACTPU, ACTLU, DACTPU or DACTLU received over a link on which dependent LUs are not supported. This may indicate an interoperability problem.

Effect: Request is rejected with the specified sense code.

Probable Cause

Type

Remedial action
Attention: Local Admin

Contact support with details of the problem.

Operator Data
Sense code

Link Station name

LFSID

RU

7036 0325

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
An interoperability problem. The operator data provides more details.

325 A Branch Network Node has received a BIND request with a badly-formed RSCV. Session activation will fail.

326 SNAP APPN received and rejected a badly-formed BIND request. Session activation will fail.

Probable Cause

Type

Remedial action
Attention: Local Admin

Contact support with details of the problem.

Operator Data
DCL Problem Determination Index

Other fields depending upon DCL Problem Determination Index

7036 0335

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

APPN Address Space Manager or APPN Address Space Instance failed to perform some function due to memory shortage.

Probable Cause

Type

Remedial action

Attention: Local Admin

Investigate memory shortage. Re-engineer FP with less functionality to reduce memory usage.

Operator Data

DCL Problem Determination Index

Other fields depending upon DCL Problem Determination Index

7036 0339

Component	Severity	Status
APPN/<name> LS/<linkstationname>	minor	message

Legend

<name> = name of the APPN router

<linkstationname> = name of the link station

Details

Received BIND using LFSID that is already in use. This is usually caused by a race condition

Effect: BIND will be rejected with specified sense code.

Probable Cause

Type

Remedial action

Attention: Local/Remote Admin

If problem is persistent, or occurs frequently, contact support with details of the problem.

Operator Data

Sense code

Linkstation name

LFSID

BIND RU

7036 0353

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
Management Services failed to perform some function due to a memory shortage.

Effect: The MU is returned to the sender noting the resource shortage error.

Probable Cause

Type

Remedial action
Attention: Local Admin

Investigate memory shortage. Re-engineer FP with less functionality to reduce memory usage.

Operator Data
DCL Problem Determination index

Other fields dependent upon DCL Problem Determination index.

7036 0368

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

The system was unable to correlate an error received on an alert send with the alerts stored in the send alert queue. The send alert queue is either too small and the original alert has been deleted or a previous error prevented the alert from being held on the queue.

Effect: The alert is not sent to the SNA management focal point.

Probable Cause

Type

Remedial action

Attention: Local Admin

Investigate definition of send alert queue size (configurable in the *Appn* component attribute *mdsTxAlertQueueSize*) or whether prior memory shortage caused alert not to be held on the queue.

7036 0458

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
There was insufficient storage to report RTM statistics to the host

Effect: RTM statistics displayed by host will be inconsistent.

Probable Cause

Type

Remedial action
Investigate resource shortage. Re-engineer FP with less functionality to reduce memory usage.

Operator Data
NAU address

7036 0460

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
APPN could not allocate necessary resource.

Effect: Some operation may fail. See other logs.

Probable Cause

Type

Remedial action
Attention: Local Admin

Investigate memory shortage. Re-engineer FP with less functionality to reduce memory usage.

Operator Data
DCL Problem Determination Index

7036 0462

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

A call from SNAP APPN to perform a cryptographic operation failed.

Effect: Session activation fails, or an active session ends abnormally with the given sense code.

Probable Cause

Type

Remedial action

Check the following logs for evidence of failed session activation. If this is evident, check MODE, LS, or INTERNAL PU definitions for cryptographic support. Check that any passwords necessary have been defined. If this problem occurs intermittently or with sessions already active with the same PLU, SLU and mode then make more storage available to SNAP APPN.

Operator Data

Sense code

7036 0470

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
A Class of Service name specified for a session activation could not be associated with a valid COS.

Effect: A session activation may fail.

Probable Cause

Type

Remedial action
Attention: Local Admin

This may indicate a configuration error. If so, the administrator should add the required *ClassOfService* component.

Operator Data
Unknown COS Name

Origin node

Destination node

Sense Code

7036 0483

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
Insufficient Memory was available to send an Alert.

Effect: The host does not see an Alert. The alert number below identifies the alert. 1 - CPDB001, 2 - CPDB002, 3 - CPDB003, 4,6 - CPDB004, 5,7 - CPDB005. The alerts are detailed in the Management Services Reference (C30-3346).

Probable Cause

Type

Remedial action
Attention: Local Admin

Investigate memory shortage. Re-engineer FP to reduce memory usage.

Operator Data
TRS Alert Number

7036 0484

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
An incorrectly formatted TDU has been received from an adjacent network node. This may indicate an interoperability problem.

Effect: CP-CP sessions with the adjacent network node are deactivated. An alert numbered CPBD001 is issued. See subsequent logs for other effects of this error.

Probable Cause

Type

Remedial action
Attention: Local Admin

Contact support with details of the problem.

Operator Data
Adjacent CP name

Sense Code

CV in error

Offset of error

TDU GDS variable

7036 0490

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

Unable to register resource owned by a served end node because the directory is full.

Effect: The specified resource is not registered (and the registration request is rejected). Network searches for the resource may fail if the end node is unable to register it.

Probable Cause

Type

Remedial action

Attention: Local Admin

Investigate configuration. If desirable, increase the value of *maximumDirectorySize* under the *Appn* component. Note that this is a process-critical attribute, and that setting it causes the network node to restart.

Operator Data

Sense code

Maximum entries

Adjacent CP name

Resource name

Resource type

7036 0491

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
Network search not started because it would exceed the maximum number of concurrent locates supported by this node.

Effect: Session activation will fail with the specified sense code.

Probable Cause

Type

Remedial action
Attention: Local Admin

Investigate setup. If desirable change the value of *maximumLocates* in the *Appn* component. Note that this is a process critical attribute so setting it causes the network node to restart.

Operator Data
Sense code

Origin CP name

Origin LU name

Destination LU name

Maximum locates

7036 0494

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
Directory Services had insufficient memory to perform some function.

Effect: Sessions are deactivated.

Probable Cause

Type

Remedial action
Attention: Local Admin

Investigate resource shortage. Re-engineer FP with less functionality to reduce memory usage.

Operator Data
DCL Problem Determination Index

other data depending upon DCL Problem Determination Index.

7036 0523

Component	Severity	Status
APPN/<name> ADJNN/<adjnode>	minor	message

Legend
<name> = name of the APPN router

<adjnode> = name of the adjacent APPN node

Details
APPN Control Point Capabilities exchange has failed due to remote protocol error.

Effect: CP-CP sessions are deactivated.

Probable Cause

Type

Remedial action
Investigate the protocol problem with the owner of the remote node identified by the operator data. If necessary reproduce the problem and trace the line.

Operator Data
Sense Code

Adjacent APPN Control Point name

Resource name

Resource type

7036 0524

Component	Severity	Status
APPN/<name> ADJNN/<adjnode>	minor	message

Legend

<name> = name of the APPN router

<adjnode> = name of the adjacent APPN node

Details

APPN Control Point Capabilities exchange has failed due to protocol error in APPN Control Point Capabilities GDS variable.

Effect: CP-CP sessions are deactivated.

Probable Cause

Type

Remedial action

Attention: Local / Remote Admin

Investigate protocol error.

Operator Data

Sense Code

Adjacent APPN Control Point name

Resource name

Resource type

7036 0533

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

A network search (originated by this node) or the network node server failed to locate the target LU. This may be caused by the target LU name being incorrect, the target system being inoperative, or by link errors in the backbone of the network.

Effect: Session activation fails with the specified sense code.

Probable Cause

Type

Remedial action

Attention: Local / Remote Admin

If the target LU name is correct, check that the system the LU is defined on is active. If the system is active, check the topology of the network (using the QUERY_NN_TOPOLOGY_* verbs) to ensure that the target system (or its network node server) is reachable from this node.

Operator Data

Sense Code

Origin CP name

Origin LU name

Destination LU name

7036 0536

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
SNAP APPN detected a protocol error in an PIU received on an intermediate session. This typically indicates a problem on an adjacent node. The sense codes are as follows.

1001-0003 - invalid IPM format

1002-0000 - RU length error

1003-0000 - CLEAR request on secondary stage, or CLEAR response on primary stage

2011-0000 - sender has overrun pacing window, or PI not set on first RU of window

2011-0001 - unexpected IPM

2011-0002 - PI set on other than first RU in window

2011-0003 - invalid pacing response

8007-0000 - segment error

Effect: The intermediate session will be deactivated.

Probable Cause

Type

Remedial action
Attention: Local / Remote Admin

Report the problem in the adjacent node to support (running a trace on the specified link if more diagnostics are required).

Operator Data
Sense Code

FQPCID

LS name

TH

BIU

7036 0537

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
This alarm indicates that the intermediate session is being deactivated because of insufficient storage.

Probable Cause

Type

Remedial action
Attention: Local / Remote Admin

Investigate memory shortage. Re-engineer FP to reduce memory usage.

Operator Data
Sense Code

FQPCID

7036 0540

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
No more intermediate sessions could be supported.

Effect: Session activation fails. See log.

Probable Cause

Type

Remedial action
Attention: Local Admin

Investigate configuration. If desirable change the value of *maximumIsrSessions* in the *Appn* component. Note that this is a process critical attribute so setting it causes the network node to restart.

Operator Data
Sense Code

Active ISR sessions

Link Station name

Primary LU name

Secondary LU name

BIND RU

7036 0564

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

LU Manager is unable to perform some function, for example Dynamic Definition of Dependent Logical Units (DDDLU) because of a lack of memory. ACTLU may not be sent by host.

Probable Cause

Type

Remedial action

Attention: Local Admin

Investigate memory shortage. If possible, reduce system load by reducing the number of active sessions.

Operator Data

PU name

NAU address

LU name

7036 0575

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

A BIND request was received by an LU type 0, 1, 2, or 3 that failed parameter checks. The sense code that applies to this condition is 0835xxxx, parameter error at offset xxxx in BIND RU, The offsets that apply to this sense code are:

0002 - invalid FM profile

0003 - invalid TS profile

0004 - invalid primary FM usage

0005 - invalid secondary FM usage

0006 - invalid common FM usage

0007 - invalid common FM usage

0008 - invalid secondary send pacing

0009 - invalid secondary receive pacing

000A - invalid secondary send RU size

000B - invalid secondary receive RU size

000E - invalid PS profile (that is, invalid session type)

000F - invalid PS usage (applies to RJE BIND only)

0010 - invalid primary half-session PS usage (applies to RJE BIND only)

0014 - invalid default screen or buffer size: rows

0015 - invalid default screen or buffer size: columns

0016 - invalid alternate screen or buffer size: rows

0017 - invalid alternate screen or buffer size: columns

Effect: BIND request will be rejected, PLU-SLU session is not activated.

Probable Cause

Type

Remedial action
Correct the configuration error on the system sending the BIND.

Operator Data
Sense code

PU name

NAU address

LU name

BIND RU

7036 0582

Component	Severity	Status
APPN/<name> DLUS/<dlusname>	minor	message

Legend

<name> = name of the APPN router

<dlusname> = name of the DLUS pipe

Details

DLUS rejects REQACTPU with given sense code.

An SSCP-PU session with the given DLUS is not activated. If a backup DLUS is configured for the PU, DLUR attempts to activate the PU through the backup DLUS.

Probable Cause

Type

Remedial action

Examine the sense code and, retry activation if appropriate.

Operator Data

Sense code

DLUS name

PU name

7036 0585

Component	Severity	Status
APPN/<name> DLUS/<dlusname>	minor	message

Legend

<name> = name of the APPN router

<dlusname> = name of the DLUS pipe

Details

CPSVRMGR pipe failed to specified DLUS.

Any PUs using the specified DLUS are deactivated (that is, DACTPU (cold) is sent.). DLUR may attempt to contact a backup DLUS, if configured.

Probable Cause

Type

Remedial action

If a pipe with backup DLUS is not initiated automatically, you must restart any required PUs manually.

Operator Data

DLUS partner

Sense code

7036 0589

Component	Severity	Status
APPN/<name> DLUS/<dlusname>	minor	message

Legend

<name> = name of the APPN router

<dlusname> = name of the DLUS pipe

Details

Protocol Error from DLUS. Received a RU too large for SSCP Session. This is typically due to the SSCP sending too large a LOGON Screen.

The data is discarded.

Probable Cause

Type

Remedial action

If expecting a SSCP LOGON screen, enter the LOGON command as usual.

7036 0590

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

The DLUR has failed to contact either the DLUS or the backup or default DLUSs after the configured number of retries

Effect: Contact is not made with the DLUS

Probable Cause

Type

Remedial action

Resolve any connectivity problems to the host, or increase the timeout or retry count and try again.

Operator Data

PU name

7036 0591

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
Received PLU-SLU BIND request with duplicate FQPCID.

Effect: Session activation fails with the specified sense code (083B0002).

Probable Cause

Type

Remedial action
Report the problem to support (running a trace on the specified link if more diagnostics are required).

Operator Data
Sense code

Primary LU name

Secondary LU name

FQPCID

7036 0630

Component	Severity	Status
APPN/<name> ADJNN/<adjnode>	minor	message

Legend
<name> = name of the APPN router

<adjnode> = name of the adjacent APPN node

Details
An HPR Route Setup RU has been received with format errors.

The message cannot be processed, and will be discarded.

Probable Cause

Type

Remedial action
Check the remote end.

Operator Data
Link Station name

TG number

Adjacent Node Name

7036 0631

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
Unable to correlate HPR Route Setup Reply.

The message cannot be processed, and will be discarded.

Probable Cause

Type

Remedial action
Check the remote end.

Operator Data
FQPCID

7036 0632

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
Unable to activate RTP Connection.

In certain situations, the origin may retry activation.

Probable Cause

Type

Remedial action
Examine sense code and retry activation if appropriate.

Operator Data
Sense code

Partner Node name

COS name

7036 0633

Component	Severity	Status
APPN/<name> LS/<linkstationname>	minor	message

Legend

<name> = name of the APPN router

<linkstationname> = name of the link station

Details

Link failure between this node and source of Route Setup request.

The route setup request is dropped by this node. The partner node on that link should generate negative reply.

Probable Cause

Type

Remedial action

Investigate link failure.

Operator Data

FQPCID

Link Station Name

7036 0634

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
HPR manager failed to get memory to send a RTP indication.

Probable Cause

Type

Remedial action
Check memory shortage.

7036 0635

Component	Severity	Status
APPN/<name> ADJNN/<adjnode>	minor	message

Legend
<name> = name of the APPN router

<adjnode> = name of the adjacent APPN node

Details
A NLP has been received with format errors.

The message cannot be processed, and will be discarded.

Probable Cause

Type

Remedial action
Check remote end.

Operator Data
Sense code

Link Station name

TG number

Adjacent Node name

7036 0636

Component	Severity	Status
APPN/<name> ADJNN/<adjnode>	minor	message

Legend

<name> = name of the APPN router

<adjnode> = name of the adjacent APPN node

Details

A NLP has been received, but this node does not support the HPR transport protocol stack.

The message cannot be processed, and will be discarded.

Probable Cause

Type

Remedial action

Check remote end.

Operator Data

Link Station name

7036 0638

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

A connection setup NLP has been received, specifying a previous instance of this NCE. The NCE must have been shut down and restarted since processing the Route Setup request.

No RTP connection can be started, the NLP will be discarded.

Probable Cause

Type

Remedial action

Check remote end.

Operator Data

Target NCE

Current NCE

Partner Node name

7036 0639

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

The local node has received a HPR Route Setup RU which it cannot forward because the next hop in the route is not HPR capable. If the local node support HPR it can act as the destination, otherwise it replies with the backout sense code and HPR may not be used by the session.

Probable Cause

Type

Remedial action

None.

Operator Data

FQPCID

Next hop CP name

Next hop TG number

Sense code

7036 0646

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

Unable to activate a Route Setup RTP Connection, during processing of a Route Setup request.

Effect: The Route Setup request fails with the sense code shown. The next Route Setup request triggers another attempt to activate the Route Setup RTP Connection.

Probable Cause

Type

Remedial action

Attention: Local Admin

Investigate memory shortage. If possible, reduce system load by reducing the number of active sessions.

Operator Data

Sense code

Partner node name

TG number

7036 0647

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

A connection Setup NLP was rejected because it specified the CP-CP session or Route Setup Topic ID, but was received on a TG that does not support the Control Flows over RTP Tower.

Effect: The CP-CP session or Route Setup RTP Connection fails with sense code HA0010017.

Probable Cause

Type

Remedial action

Contact support with details of the problem.

Operator Data

Sense code

Partner node name

Topic ID

TG Number

7036 0648

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
An HPR Route Setup RU has been received with an FQPCID that matches an existing route.

Effect: The message is rejected and the route is not established.

Probable Cause

Type

Remedial action
Report error to remote end.

Operator Data
FQPCID

Sense code

7036 0662

Component	Severity	Status
APPN/<name> RtpPipe/<rtpname>	minor	message

Legend
<name> = name of the APPN router

<rtpname> = name of the RTP pipe

Details
The RTP connection has disconnected due to an external error.

Sessions through the connection will fail.

Probable Cause

Type

Remedial action
Investigate the cause of error.

Operator Data
Sense code

Connection name

7036 0664

Component	Severity	Status
APPN/<name> RtpPipe/<rtpname>	minor	message

Legend
<name> = name of the APPN router

<rtpname> = name of the RTP pipe

Details
The RTP connection has disconnected due to a time out.

The RTP connection will attempt to re-route the pipe.

Probable Cause

Type

Remedial action
Investigate the cause of error based on the details given above.

Operator Data
Connection name

COS name

Remote Node name

Local TCID

Remote TCID

7036 0665

Component	Severity	Status
APPN/<name> RtpPipe/<rtpname>	minor	message

Legend
<name> = name of the APPN router

<rtpname> = name of the RTP pipe

Details
The RTP connection has been disconnected by a local link failure.

The RTP connection will attempt to re-route the pipe.

Probable Cause

Type

Remedial action
Investigate the cause of error based on the details given above.

Operator Data
Connection name

COS name

Remote Node name

Local TCID

Remote TCID

Link name

7036 0667

Component	Severity	Status
APPN/<name> RtpPipe/<rtpname>	minor	message

Legend
<name> = name of the APPN router

<rtpname> = name of the RTP pipe

Details
The RTP connection could not be re-routed.

Sessions through the connection will fail.

Probable Cause

Type

Remedial action
Investigate the cause of error based on the details given above.

Operator Data
Connection name

COS name

Remote Node name

Local TCID

Remote TCID

7036 0668

Component	Severity	Status
APPN/<name> RtpPipe/<rtpname>	minor	message

Legend

<name> = name of the APPN router

<rtpname> = name of the RTP pipe

Details

A Route Setup RTP Connection RTP process received a segmented NLP. All NLPs received should contain Route Setup GDS data, which cannot be segmented.

Effect: The NLP is dropped.

Probable Cause

Type

Remedial action

Contact support with details of the problem.

Operator Data

Connection name

Remote Node name

Local TCID

Remote TCID

7036 0669

Component	Severity	Status
APPN/<name> RtpPipe/<rtpname>	minor	message

Legend
<name> = name of the APPN router

<rtpname> = name of the RTP pipe

Details
A Route Setup RTP Connection has timed out waiting for status from the adjacent node.

Effect: The RTP Connection fails.

Probable Cause

Type

Remedial action
Investigate the cause of the error at the adjacent node.

Operator Data
Connection name

Remote Node name

Local TCID

Remote TCID

7036 0676

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

Timer expired before the Discovery request was completed. The operator data provides more details.

676 Find processing not complete on timer expiry. No retry of FIND frame on this timer expiry.

677 Invalid correlator on received FOUND frame. This may be due to a protocol error at a Discovery server, or may be caused by the FIND timer being set too low. Frame discarded.

678 Invalid correlator on received NOTIFY frame. This may be due to a protocol error at a Discovery server, or may be caused by the QUERY timer being set too low. Frame discarded.

680 Unexpected FIND frame response received, indicating that the FIND timer is set too low. Response discarded.

681 Unexpected QUERY frame response received, indicating that the QUERY timer is set too low. Response discarded.

682 Unexpected SOLICIT frame response received, indicating that the SOLICIT timer is set too low. Response discarded.

Probable Cause

Type

Remedial action

If possible, increase the FIND, QUERY or SOLICIT timer value to allow time for the Discovery request to complete. Otherwise, contact support with details of the problem.

Operator Data

DCL Problem Determination Index

7036 0679

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

Insufficient memory storage. The operator data provides more details.

679 Insufficient storage to start Discovery application. Discovery fails to initialize application.

688 Insufficient storage to process an incoming Discovery frame. Frame parsing abandoned and frame discarded.

693 Insufficient storage to send an Advertise frame for the given resource. This frame may be resent on a timer, so no effect unless this alarm is seen frequently.

694 Insufficient storage to send an Notify frame. Information about the given resource will not reach the requesting Discovery Client.

722 Insufficient storage to generate Alert CPSS003 (protocol error in received BIND or LOCATE). Alert will not be sent.

742 Insufficient storage to send RTM statistics to host. RTM statistics displayed by host will be inconsistent.

760 Insufficient storage to process CPI-C function. CPI-C function will fail with return_code of CM_PRODUCT_SPECIFIC_ERROR.

822 Insufficient storage to initialize the half session. The half session will fail to activate with the specified sense code.

Probable Cause

Type

Remedial action

Attention: Local Admin

Investigate memory shortage. If possible reduce system load by reducing the number of active sessions.

Operator Data

DCL Problem Determination Index

7036 0684

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
Subvector of unexpected length in frame. This protocol error may indicate an interoperability problem.

Effect: Subvector is ignored.

Probable Cause

Type

Remedial action
Contact support with details of the problem.

Operator Data
Frame

7036 0687

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
Error reported on adapter. Possible error types are as follows.

0x04 - All SAPs for this device must be closed down

0x07 - This SAP must be closed down

0x11 - General device open/lan insertion failure

0x12 - Ring close-down due to excessive Beaconing

0x13 - Hardware/microcode error in adapter

0x14 - PC Network failure

0x15 - Forced off ring during insertion process

0x16 - Error detected during wrap test

0x17 - Forced off ring

0x18 - Error detected in lobe wiring

0x19 - Beaconing error on insertion to the network

0x1A - Another adapter on the network with same address

0x1B - Network hardware error

0x1C - Adapter has been reset

0x30 - SAP has failed

Effect: Adapter is no longer used by Discovery.

Probable Cause

Type

Remedial action
Investigate the cause of the adapter failure.

Operator Data

Error type

Error code

7036 0690

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

An error frame was received. The operator data provides more details.

690 A request frame containing duplicate subvectors has been received. The frame will not be rejected for this reason alone, so possibly no effect. See other logs.

691 A request frame of inconsistent total length has been received. The frame will not be rejected for this reason alone, so possibly no effect. See other logs.

692 A received request frame does not contain the subvectors necessary to process it. The frame will be ignored.

Probable Cause

Type

Remedial action

The origin and target of the frame are supplied if known. Check that the Discovery Client being used by the originator is operating correctly. Contact support with details.

Operator Data

DCL Problem Determination Index

7036 0719

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
CP-CP sessions not supported to adjacent node.

Probable Cause

Type

Remedial action
Attention: Local/Remote Admin

Ensure that CP-CP sessions are allowed from both ends of the TG.

Operator Data
Sense code

Lu Name

Mode Name

Conversation Group Identifier

7036 0720

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

CP capabilities exchange failed because of contention loser (DCL problem index 720) or contention winner (problem index 731) CP-CP session failure.

The contention winner/loser CP-CP session (that is, the session in the opposite direction to the one which failed) is deactivated. APPN attempts to reactivate CP-CP sessions with this adjacent CP.

Probable Cause

Type

Remedial action

This alarm flags the fact that a CP-CP session has failed. Other alarms give further details on the reason for the session failure (for example, insufficient resources, link failure). Remedial actions indicated for those alarms should be taken.

Operator Data

DCL Problem Index

Sense code

Adjacent CP name

7036 0723

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

CP capabilities exchange failed because of a protocol error. This may indicate an interoperability problem. Sense codes describing the problem in more detail are as follows:

08060030 - CP capabilities requested by an unknown CP

08210002 - CP capabilities requested on other than the CPSVCMG session mode.

08150007 - CP capabilities requested when CP-CP session already established.

08B60000 - CP-CP sessions not supported by adjacent node.

08090039 - CP transaction error.

10101000 - CP capabilities length error

10101002 - Unexpected GDS identifier (not CP capabilities).

The CP-CP sessions with the specified adjacent node are deactivated. APPN does not attempt to reactivate CP-CP sessions with this adjacent CP.

Probable Cause

Type

Remedial action

Report this problem to the owner of the node identified by the Adjacent CP name in the operator data.

Operator Data

Sense code

Adjacent CP name

[CP Capabilities vector]

7036 0732

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

A CP-CP session was established between two network nodes in different networks, that is with different network identifiers. This is not supported by the current published APPN architecture.

The CP-CP sessions are deactivated.

Probable Cause

Type

Remedial action

Connections between APPN networks require a border node. The border node specification is not yet part of the published APPN architecture. There are three choices to deal with this:

1)
Connect the networks through the DPN T2.1 router. This provides a LEN network image which permits independent LU sessions to flow across the border between the networks, but requires manual definition of directory entries in the adjacent nodes.

2)
Connect the networks using an AS/400 with the basic Border Node feature. With this feature the AS/400 behaves as an APPN End Node and exchanges directory information, but no topology information. This supports independent LU sessions.

3)
Connect the networks using VTAM V4.2 with Extended Border Node. This feature provides full Network Node support across the border, and supports both dependent and independent LU sessions. This requires that VTAM V4.2 be on **both** sides of the connection.

Operator Data

Sense code

Adjacent CP name

7036 0742

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

APPN Physical Unit Manager is unable to send response time monitor statistics to the host because of a lack of memory.

Effect: RTM stats may be reported incorrectly to host

Probable Cause

Type

Remedial action

Attention: Local Admin

Investigate memory shortage. Re-engineer FP with less system load or functionality to reduce memory usage.

Operator Data

PU name

NAU address

7036 0762

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
A CPI-C application specified an unknown symbolic destination name on a CMINIT call.

Effect: The CMINIT call will fail with CM_PARAMETER_CHECK.

Probable Cause

Type

Remedial action
Attention: Local Admin

Define the symbolic destination name (using DEFINE_CPIC_SIDE_INFO), or modify the application to use a symbolic destination name that is already defined.

Operator Data
Symbolic destination name

7036 0765

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
CPI-C application attempted to start more than 64 concurrent conversations.

Effect: CMACCP, CMINIT, or CMINIC verb will fail with CM_PRODUCT_SPECIFIC_ERROR.

Probable Cause

Type

Remedial action
Attention: Local Admin

Modify TP to use 64 or fewer concurrent conversations.

Operator Data
conversations

7036 0776

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

The adjacent node is a back level LEN node but no adj_cp_name has been defined for the link.

Effect: The link activation fails.

Probable Cause

Type

Remedial action

Attention: Local Admin

Correct the link station configuration by using DEFINE_LS to define an adj_cp_name.

Operator Data

Sense code

Port name

LS name

7036 0777

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

A link activation race was detected on an ATM port. The operator data provides more details.

777 A link activation race has been detected on an ATM port. The local node is responsible for resolving this race, and disconnects its link. The remote node's link activation request succeeds.

778 A link activation race has been detected on an ATM port. The remote node is responsible for resolving this race. The local node sends a negotiation error CV, indicating that the remote link activation request should fail. The local node's link activation request succeeds.

Probable Cause

Type

Remedial action

This is a normal race condition - no action is required.

Operator Data

DCL Problem Index

Sense code

Port name

LS name

TG Number

Adjacent CP name

7036 0779

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

A PORT_BANDWIDTH_UPDATE signal has been received. The operator data provides more details.

779 A PORT_BANDWIDTH_UPDATE signal (status = QUIESCING) has been received. Any Connection Network TGs on this port will be advertised as quiescing. Any TGs that can be activated automatically will be advertised as non-operational.

780 A PORT_BANDWIDTH_UPDATE signal (status = OK) has been received. Any Connection Network TGs on this port which had been advertised as quiescing will be advertised as active. Any TGs that can be activated automatically and which had been advertised as non-operational will be advertised as operational.

Probable Cause

Type

Remedial action

Attention: Local Admin

If possible, increase the bandwidth available to the local port.

Operator Data

DCL Problem Index

Port name

7036 0781

Component	Severity	Status
APPN/<name> LS/<linkstationname>	minor	message

Legend

<name> = name of the APPN router

<linkstationname> = name of the link station

Details

A link station (LS) has been configured to assume a role incompatible with the underlying DLC. For example, DSPU services have been configured for a LS on a port over a Channel DLC. (SNAP APPN always assumes a secondary role on links over a channel DLC, but the role must be primary to provide DSPU services.)

Effect: The link activation fails.

Probable Cause

Type

Remedial action

Attention: Local Admin

Correct the configuration of the LS. In the example case, issue DEFINE_LS to set dspu_services to NAP_NONE, and ls_role to NAP_LS_SEC.

Operator Data

DLC name

Port name

LS name

LS role

7036 0782

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

SNAP APPN has been unable to locate a link station. The operator data provides more details.

782 SNAP APPN has been unable to locate a defined ANYNET link station. For any net routing to succeed a link station with the name $ANYNET$ must be defined on an ANYNET DLC.

783 SNAP APPN has been unable to locate a link station configured with DEFINE_LS_ROUTING.

Effect: The session activation request fails, with the specified sense code.

Probable Cause

Type

Remedial action

Attention: Local Admin

Check the local configuration (link definitions can be viewed using the QUERY_LS verb and routing definitions with the QUERY_LS_ROUTING verb).

Operator Data

DCL Problem Index

[LS name]

Sense code

7036 0784

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
The DLC has returned inconsistent data during creation.

Effect: The DLC is destroyed, and all ports and link stations defined on the DLC are inoperative.

Probable Cause

Type

Remedial action
Attention: Local Admin

Run a trace on the DLC and contact support with the log and trace information.

Operator Data
DLC name

DLC capabilities

7036 0785

Component	Severity	Status
APPN/<name> LS/<linkstationname>	minor	message

Legend

<name> = name of the APPN router

<linkstationname> = name of the link station

Details

An automatic retry link station is still inactive after the maximum allowed number of retries.

Effect: The link station will remain inactive awaiting operator intervention. In the mean time, the activation of any sessions relying on this link station will fail.

Probable Cause

Type

Remedial action

Attention: Local Admin

Check surrounding logs for link activation failures. Check the configuration of the link station. Check the state of the adjacent node. Issue START_LS to retry activation.

Operator Data

LS name

7036 0786

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

SNAP APPN cannot start a link to an adjacent node over a connection network TG. The operator data provides more details.

786 SNAP APPN cannot start a link to an adjacent node over a connection network TG because the link address on the local node is not compatible with the link address on the adjacent node.

787 SNAP APPN cannot start a link to an adjacent node over a connection network TG because the DLC does not support multiple links between the local and destination addresses.

Effect: The session will fail, with the specified sense code.

Probable Cause

Type

Remedial action

Attention: Local Admin

Check the local and destination link addresses.

Operator Data

DCL Problem Index

Sense code

CN name

Port name

DLC name

TG number

Local link address

Destination link address

7036 0788

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
TG characteristics mismatch for MLTG link.

Effect: Link activation fails.

Probable Cause

Type

Remedial action
Attention: Local Admin

Check the link station definitions (or port definitions, if they are implicit). The security, visibility, and user-defined parameters must be the same for two links to be added to the same MLTG. If the defined values differ, alter them to match.

Operator Data
MLTG name

Adjacent CP name

Adjacent CP type

Failed LS name

Port name

TG number

Conflicting LS name

Port name

TG number

Sense code

7036 0789

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
Activation of a Multi-Link TG (MLTG) link has failed due to conflict with an existing active or defined link.

Probable Cause

Type

Remedial action
Attention: Local Admin

If activation of the failing link station is desired, perform one of the following actions and retry activation.

o Deactivate the link station with which conflict occurs.

o Reconfigure the failing link station to remove the conflict.

o Reconfigure the conflicting link station.

The most likely causes of conflict are

o identical TG numbers (unless both links are MLTG links)

o the adjacent node is not configured to allow the activation of MLTG links, so a link configured as MLTG has been activated as a Singly-Linked TG (SLTG)

o different Maximum Send BTU sizes

o different Maximum Receive BTU sizes

o different TG security characteristics

o different TG user-defined characteristics

o different defined visibility.

Operator Data
MLTG name

Adjacent CP name

Adjacent CP type

Failed LS name

Port name

TG number

Conflicting LS name

Port name

TG number

Sense code

7036 0790

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

The remote node has negotiated MLTG support on a link to this node, but has requested SNA function not supported for MLTGs.

Effect: If activating, link activation fails. If active, the link may fail. Check following audit logs.

Probable Cause

Type

Remedial action

Attention: Local Admin

Investigate the illegal behavior of the remote node. Contact support with traces of the illegal behavior.

Operator Data

MLTG name

Adjacent CP name

Adjacent CP type

Failed LS name

Port name

TG number

Sense code

7036 0798

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

MLTG link speed disparity. Two links of very different speeds have been placed in the same MLTG.

Effect: The transmission rate which can be achieved on RTP connections passing over this MLTG may be reduced.

Probable Cause

Type

Remedial action

Attention: Local Admin

Use QUERY_RTP_CONNECTION to determine the send rate for an RTP connection passing over the MLTG. Remove the slowest link from the MLTG (issue STOP_LS) and see if the send rate improves.

Operator Data

MLTG name

Adjacent CP name

Adjacent CP type

High-speed LS name

Port name

Low-speed LS name

Port name

TG number

7036 0799

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
Non-activation XID received on MLTG link.

Effect: The link may fail. See surrounding logs.

Probable Cause

Type

Remedial action
Attention: Local Admin

Non-activation XIDs are prohibited by the architectural definition of MLTG links. Identify the remote node and notify support of this anomalous behavior.

Operator Data
MLTG name

Adjacent CP name

Adjacent CP type

LS name

TG number

7036 0800

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

Branch Network node has insufficient resources to register or deregister an adjacent LEN node.

Effect: The directory of this node and/or that of its NNS may become inconsistent, in that the LEN CP will still be there when it should not be, or vice versa. Thus session activation to the LEN may fail when a link to it is active, or neighboring nodes may believe that the LEN is reachable when the link to it is down.

Probable Cause

Type

Remedial action

Attention: Local Admin

Ensure that there are sufficient resources available to SNAP APPN and re-cycle the link to the required state.

Operator Data

Adjacent LEN name

7036 0840

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

A bind response was received that accepted session compression, but did not specify the compression levels required (because the response is from a back-level node or because the bind request was shortened).

Effect: The compression level negotiation fails and the standard compression levels are used - this means that compression will be used in both directions even though it may have been configured for one direction only.

Probable Cause

Type

Remedial action

None

Operator Data

Local LU name

7036 0841

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
The desired number of buffers could not be reserved for a buffer pool.

Effect: The receive pacing window size for the session will not increase as fast as configured.

Probable Cause

Type

Remedial action
Investigate memory shortage. Re-engineer FP to reduce memory usage.

Operator Data
Local LU name

Partner LU name

Mode name

Session identifier

7036 0880

Component	Severity	Status
APPN/<name>	minor	message

Legend

<name> = name of the APPN router

Details

An RTP connection is path-switching to a much longer path than it started with. Much more room is needed in each packet for routing information than was originally planned.

Effect: Performance across this RTP connection may degrade, since some packets may have to be segmented.

Probable Cause

Type

Remedial action

Attention: Local Admin

If performance degradation is noticed, reactivate failed links then issue the ‘PATH_SWITCH’ verb.

Operator Data

Connection name

7037 0242

Component	Severity	Status
APPN/<name>	minor	message

Legend
<name> = name of the APPN router

Details
The space for implicit aliases has wrapped.

Effect: There is a small possibility of APPN generating duplicate aliases. (To get this log you have used one million different aliases).

Probable Cause

Type

Remedial action
Attention: User/Local Admin

Shut down and restart the node to avoid possibility of conflict. Check the configuration to ensure that you have not introduced alias names inadvertently.

Operator Data
alias name

7038 0005

Component	Severity	Status
APPN/<name> or Vr/<string1> Pp/<string2> SnaPort	minor	message

Legend

<name> = name of the APPN router

<string1> = name of the virtual router

<string2> = name of the protocol port

Details

The identified LAN adapter has terminated due to an error it detected.

Effect: All links using this adapter are aborted

Note that this alarm cannot occur in the current release for APPN service because the LAN adapter is emulated by the Frame-Relay Virtual Circuit termination, which cannot fail.

Probable Cause

Type

Remedial action

Attention: User, Network Support

Correct the problem with the identified adapter.

Operator Data

LAN adapter id

Error code

7038 0054

Component	Severity	Status
APPN/<name> or Vr/<string1> Pp/<string2> SnaPort	minor	message

Legend

<name> = name of the APPN router

<string1> = name of the virtual router

<string2> = name of the protocol port

Details

The LAN adapter failed to activate.

Effect: LLC2 cannot gain network access via this device.

This cannot occur in the current version for APPN service because the LAN adapter is emulated by the Frame-Relay Virtual Circuit termination, which cannot fail to activate because it has no associated hardware resources.

Probable Cause

Type

Remedial action

Attention: User/Local Admin

Check cabling and adapter installation. Check device configuration.

Operator Data

LAN Adapter id.

return code from device activation

7038 0060

Component	Severity	Status
APPN/<name> or Vr/<string1> Pp/<string2> SnaPort	minor	message

Legend

<name> = name of the APPN router

<string1> = name of the virtual router

<string2> = name of the protocol port

Details

The identified LLC device (LAN adapter) failed to activate.

Effect: LLC2 cannot gain network access via this device.

Probable Cause

Type

Remedial action

Attention: User/Local Admin

Check cabling and adapter installation. Check device configuration.

Operator Data

LLC device id

Return code from device activation.

7038 0065

Component	Severity	Status
APPN/<name> or Vr/<string1> Pp/<string2> SnaPort	minor	message

Legend

<name> = name of the APPN router

<string1> = name of the virtual router

<string2> = name of the protocol port

Details

The named link has failed.

Effect: A SNA alert with the specified id is sent to the management services component. The link itself is closed.

Probable Cause

Type

Remedial action

Attention: User/Network Support

Determine reason for link failure (other messages logged at the same time may give further information) and attempt to correct it.

Operator Data

Link Failure code

Remote Station MAC address

Remote Station SAP

Local Station MAC address

Local Station SAP

7038 0066

Component	Severity	Status
APPN/<name> or Vr/<string1> Pp/<string2> SnaPort	minor	message

Legend

<name> = name of the APPN router

<string1> = name of the virtual router

<string2> = name of the protocol port

Details

The identified port has failed.

Effect: An alert with the specified id is sent to the management services component. The port itself and any links using this port are closed.

Probable Cause

Type

Remedial action

Attention: User/Network Support

Determine reason for port failure (other messages logged at the same time may give further information) and attempt to correct it.

Operator Data

LLC device adapter id

Port address

device failure code

Alert id

7038 0071

Component	Severity	Status
APPN/<name> or Vr/<string1> Pp/<string2> SnaPort	minor	message

Legend

<name> = name of the APPN router

<string1> = name of the virtual router

<string2> = name of the protocol port

Details

An attempt has been made to open a link connection to an adjacent link station that is not responding to TEST frames

Effect: The link activation request fails.

Probable Cause

Type

Remedial action

Attention: User/Network Support

Check the local configuration and/or the hardware and wiring on the adjacent link station.

Operator Data

Remote Station MAC address

Remote Station SAP

Local Station MAC address

Local Station SAP

7038 0072

Component	Severity	Status
APPN/<name> or Vr/<string1> Pp/<string2> SnaPort	minor	message

Legend

<name> = name of the APPN router

<string1> = name of the virtual router

<string2> = name of the protocol port

Details

An attempt to activate a port has failed because the MAC device specified for the port is currently resetting.

Effect: The port activation request fails.

Probable Cause

Type

Remedial action

Attention: User

Retry the port activation request, if problem persists, contact Network Support

7038 0075

Component	Severity	Status
APPN/<name> or Vr/<string1> Pp/<string2> SnaPort	minor	message

Legend

<name> = name of the APPN router

<string1> = name of the virtual router

<string2> = name of the protocol port

Details

LLC2 was unable to perform some function due to a lack of memory.

Probable Cause

Type

Remedial action

Attention: Local Admin

Investigate resource shortage. Re-engineer FP with less functionality to reduce memory usage.

7038 0083

Component	Severity	Status
APPN/<name> or Vr/<string1> Pp/<string2> SnaPort	minor	message

Legend

<name> = name of the APPN router

<string1> = name of the virtual router

<string2> = name of the protocol port

Details

An attempt was made to activate a link to the local MAC and SAP address.

Effect: The activation attempt is rejected.

Probable Cause

Type

Remedial action

Attention: User/Local Admin

Change the configuration of the link station to have the correct remote MAC address.

Operator Data

Remote Station MAC address

Remote Station SAP

7039 1000

Component	Severity	Status
AtmIf/<num1>	minor	set/clear

Legend

<num1> =1 - 4095

Details

If the status is *set*, the *AtmIf* component in question has detected that the count of associated troubled connections has changed from zero to a non-zero. This change in state signifies that at least one of the connections associated with this *AtmIf* component has become troubled, where none were before. A *clear* is issued when the count of troubled connections associated with this *AtmIf* component returns to zero.

Probable Cause

Framing error

Type

Communications

Remedial action

Display all of the *Vpc*, *Vpt*, and *Vcc* components associated with the *AtmIf* component to determine which ones are troubled. Troubleshoot the problem in the usual manner. See 241-5701-715 *Passport 7400, 15000, 20000 ATM Monitoring and Troubleshooting Guide* for details on troubleshooting ATM connections.

7039 2000

Component	Severity	Status
AtmIf/<num1> Vcc/<num2>.<num3>	minor	set/clear
AtmIf/<num1> Vpc/<num4>		
AtmIf/<num1> Vpt/<num5>		
AtmIf/<num1> Vpt/<num5> Vcc/<num3>		

Legend

<num1> = 1 - 4095

<num2> = 0 - 4095

<num3> = 0 - 65535

<num4> = 1 - 4095

<num5> = 0 - 4095

Details

If the status is *set*, the amount of bandwidth provisioned for the indicated connection exceeds the amount of bandwidth currently available.

A *clear* is issued when the connection is able to get the bandwidth it needs or is deleted.

Probable Cause

Storage capacity problem

Type

Processing

Remedial action

Bandwidth is provisioned in the *Vcd Tm* or *Vpd Tm* subcomponent of the *Vpc*, *Vpt*, or *Vcc* components. If the alarm is caused by a connection associated with an *AtmIf* component, re-configure the bandwidth until the total provisioned bandwidth of all connections on this interface falls within the maximum bandwidth limit that the interface can support.

If the alarm is caused by a connection associated with a *Vpt* component, re-configure the bandwidth until the total provisioned bandwidth of all connections associated with this *Vpt* component falls within the maximum bandwidth limit that the VPT can support.

You can reduce the provisioned bandwidth of one or more connections, delete one or more connections, or increase the available bandwidth of the *Vpt* component.

7039 2001

Component	Severity	Status
AtmIf/<num1> Vcc/<num2>.<num3>	minor	message
AtmIf/<num1> Vpc/<num4>		
AtmIf/<num1> Vpt/<num5>		
AtmIf/<num1> Vpt/<num5> Vcc/<num3>		

Legend

<num1> = 1 - 4095

<num2> = 0 - 4095

<num3> = 0 - 65535

<num4> = 1 - 4095

<num5> = 0 - 4095

Details

This alarm indicates that more connections have been created under this ATM interface than the interface is able to accept. The alarm is caused either by memory exhaustion or by exceeding the provisioned values of the *maxVpcs* or *maxVccs* attributes of the *Ca* component. The *Ca* component can be associated with an *AtmIf* or a *Vpt* component.

If the ATM interface is on a spared port, one or more connections on the interface may not be spared. If an FP switchover occurs in this state, one or more of the connections may go down. This may or may not come back up after the switchover.

PORS map mode trunks create VCCs in order to support PORS connections. These connections share the available connection space with ATM SVCs, SPVCs, and PVCs. ATM does not keep track of the connection space used by PORS. If PORS map mode trunks are consuming some of the connection space on an ATM interface, ATM may continue to attempt to set up new connections even though the *maxVccs* value has been reached.

Probable Cause

Storage capacity problem or configuration error.

Another probable cause can occur in a spared configuration when the spare card has less memory than the active card. At switchover time, all of the connections on the active card attempt to re-establish on the spared card but fail because of memory exhaustion.

Another probable cause can occur when ATM and PORS map mode trunks are competing for connection space on the ATM interface and have reached the *maxVccs* value.

Another probable cause can occur when the number of connections under the *AtmIf* component, including SPVCs and PVCs, are more than the value of attribute *AtmIf Ca maxVccs*.

Type

Processing

Remedial action

If provisioned values of the *maxVpcs* or *maxVccs* attributes have been exceeded, either reprovision the *Ca* component or delete one or more connections. If the alarm was raised due to memory exhaustion, delete one or more connections (or other components) to increase available memory.

Verify the operational value of both the connection pool capacity attributes (*connectionPoolAvailable* added to the *connectionPoolUsage* and *protectedConnectionPoolAvailable* added to the *protectedConnectionPoolUsage*). If these values differ from the active card to the associated spared card, provision the *Lp Eng Arc Ov connectonPoolCapacity* and/or *protectedConnectionPoolCapacity* according to the lower of the two memory capacities.

7039 2003

Component	Severity	Status
AtmIf/<num1> Vcc/<num2>.<num3>	minor	set/clear
AtmIf/<num1> Vpc/<num4>		
AtmIf/<num1> Vpt/<num5>		
AtmIf/<num1> Vpt/<num5> Vcc/<num3>		

Legend

<num1> = 1 - 4095

<num2> = 0 - 4095

<num3> = 0 - 65535

<num4> = 1 - 4095

<num5> = 0 - 4095

Details

This alarm indicates that more connections have been created under the UBR service category than the service category is able to accept (the *maxVpcs* and *maxVccs* attributes of the *Ubr* component). The UBR service category can be associated with the ATM interface or a virtual path terminator (VPT).

If the status is *set*, the unspecified bit rate (UBR) connection provisioned exceeds the number of UBR connections currently available.

A *clear* is issued when the connection is able to get the connection space it needs or is deleted.

Probable Cause

Storage capacity problem

Type

Processing

Remedial action

Check the value of the *maxVpcs* and *maxVccs* attributes of the *Ubr* component. If the UBR connection is associated with the ATM interface (*AtmIf Ca Ubr*), the values of these attributes control the UBR connections for that interface. If the UBR connection is associated with a virtual path terminator (*AtmIf Vpt Ca Ubr*), the values of these attributes control the UBR connections for that VPT.

Reprovision the *Ubr* component or delete one or more connections.

7039 2004

Component	Severity	Status
AtmIf/<num1> Vcc/<num2>.<num3> AtmIf/<num1> Vpc/<num4>	minor	set/clear

Legend

<num1> = 1 - 4095

<num2> = 0 - 4095

<num3> = 0 - 65535

<num4> = 0 - 4095

Details

If the status is *set*, the amount of bandwidth provisioned for the indicated connection under the 1pOC48SmSrPos FP exceeds 1,198,080 kbits/second (OC-24).

A *clear* is issued when the connection reduces its provisionable bandwidth to be equal to or less than 1,198,080 kbits/second (OC-24) or is deleted.

Probable Cause

Storage capacity problem

Type

Processing

Remedial action

Bandwidth is provisioned in the Vcd Tm or Vpd Tm subcomponent of the Vpc or Vcc components. If the alarm is raised, reconfigure the bandwidth of the connection to be equal to or less than 1,198,080 kbits/second (OC-24).

7039 2005

Component	Severity	Status
AtmIf/<num1> Vcc/<num2>.<num3> AtmIf/<num1> Vpc/<num4>	minor	set/clear

Legend

<num1> = 1 - 4095

<num2> = 0 - 4095

<num3> = 0 - 65535

<num4> = 0 - 4095

Details

If the status is *set*, the amount of bandwidth provisioned for the indicated connection under the 1pOC48SmSrPos FP exceeds the amount of bandwidth currently available at the selected ingress card datapath.

A *clear* is issued when the connection is able to get the bandwidth it needs or is deleted.

Probable Cause

Storage capacity problem

Type

Processing

Remedial action

Bandwidth is provisioned in the Vcd Tm or Vpd Tm subcomponent of the Vpc or Vcc components. If the alarm is raised, re-configure the receive service labels under *Vr Mpls LspGroup AtmSap ConnId Lbls* from either odd to even or even to odd values if enough bandwidth is available to admit this connection on the other ingress card datapath. Or you could re-configure the bandwidth until the total provisioned bandwidth of all connections on the selected ingress card datapath falls within the maximum bandwidth limit that each ingress card datapath can support.

7039 2006

Component	Severity	Status
AtmIf/<num1> Vcc/<num2>.<num3> AtmIf/<num1> Vpc/<num4>	minor	set/clear

Legend

<num1> = 1 - 4095

<num2> = 0 - 4095

<num3> = 0 - 65535

<num4> = 0 - 4095

Details

If the status is *set*, the amount of bandwidth provisioned for the indicated connection under the 1pOC48SmSrPos FP exceeds the amount of bandwidth currently available at the selected egress card datapath.

A *clear* is issued when the connection is able to get the bandwidth it needs or is deleted.

Probable Cause

Storage capacity problem

Type

Processing

Remedial action

Bandwidth is provisioned in the Vcd Tm or Vpd Tm subcomponent of the Vpc or Vcc components. If the alarm is raised, re-configure the transmit service labels under *Vr Mpls LspGroup AtmSap ConnId Lbls* from either odd to even or even to odd values if enough bandwidth is available to admit this connection on the other egress card datapath. Or you could re-configure the bandwidth until the total provisioned bandwidth of all connections on the selected egress card datapath falls within the maximum bandwidth limit that each egress card datapath can support.

7039 2007

Component	Severity	Status
AtmIf/<num1> Vcc/<num2>.<num3>	minor	set/clear
AtmIf/<num1> Vpc/<num4>		
AtmIf/<num1> Vpt/<num5>		
AtmIf/<num1> Vpt/<num5> Vcc/<num3>		

Legend

<num1> = 1 - 4095

<num2> = 0 - 4095

<num3> = 0 - 65535

<num4> = 1 - 4095

<num5> = 0 - 4095

Details

This alarm indicates that all the traffic shaping rates have been exhausted for all of the service categories (cbr, rtvbr, nrtvbr, ubr).

If the status is *set*, the connection provisioned does not have an available traffic shaping rate, since all of the traffic shaping rates have been used up by the existing connections.

A *clear* is issued when the shaping rate requested by the connection is available.

Probable Cause

Storage capacity problem

Type

Processing

Remedial action

Check the traffic shaping and the traffic usage parameters of the *AtmIf* component. Reprovision the traffic shaping rate of the new connection with one of the existing shaping rates, or delete one of the existing connections that is using one of the 32 shaping rates.

7039 3000

Component	Severity	Status
AtmIf/<num1> Vpt/<num2>	minor/cleared	set/clear

Legend

<num1> =1 - 4095

<num2> = 0 - 4095

Details

If the status is *set*, the *Vpt* component in question has detected that the count of associated troubled connections has changed from zero to a non-zero. This change in state signifies that at least one of the connections associated with this *Vpt* has become troubled, where none were before. A *clear* is issued when the count of troubled connections associated with this *Vpt* component returns to zero.

Probable Cause

Framing error

Type

Communications

Remedial action

Display all of the *Vcc* components associated with the *Vpt* component to determine which ones are troubled. Troubleshoot the problem in the usual manner. See 241-5701-715 *Passport 7400, 15000, 20000 ATM Monitoring and Troubleshooting Guide* for details on troubleshooting ATM connections.

7039 4000

Component	Severity	Status
AtmIf/<num1>	minor	message

Legend

<num1> =1 - 4095

Details

The ATM interface has detected one or more LRC errors over a one second interval. Each LRC error signifies that a potentially corrupted frame was passed to the interface for transmission. The number of LRC errors that occurred is included in the alarm text.

Probable Cause

Framing error

Type

Communications

Remedial action

LRC errors may be caused either by defective hardware somewhere in the network, or by transient network conditions, such as the removal or insertion of a card, resetting of a card, enabling or disabling of a bus, running of a bus test, or enabling or disabling of an ATM connection. Check to see if any such transient condition occurred around the time of the alarm; if so, correct the destabilizing condition. Continue to monitor the situation to see if additional LRC error alarms occur; if this alarm continues to appear, or if major alarm 7039 4001 is raised, apply the Diagnosing LRC Errors procedure documented in 241-5701-715 *Passport 7400, 15000, 20000 ATM Monitoring and Troubleshooting Guide*.

7039 4001

Component	Severity	Status
AtmIf/<num1>	major/cleared	set/clear

Legend

<num1> =1 - 4095

Details

If the status is *set*, the ATM interface has detected multiple LRC errors over a period of several seconds or more. Each LRC error signifies that a potentially corrupted frame was passed to the interface for transmission. Information describing the number of LRC errors detected by the ATM interface is included in the alarm text.

A *clear* is issued when no LRC errors have been detected by the ATM interface for at least 2.5 minutes. Information describing the number of LRC errors and the period over which they occurred is included in the alarm text.

Probable Cause

Framing error

Type

Communications

Remedial action

Consult the Diagnosing LRC Errors procedure documented in 241-5701-715 *Passport 7400, 15000, 20000 ATM Monitoring and Troubleshooting Guide*.

7039 5000

Component	Severity	Status
AtmIf/<num1>	critical/cleared	set/clear

Legend

<num1> = 1 - 4095

Details

This alarm is issued by a Passport AtmInterface (AtmIf). When the status is *set*, the total average link TxUtilization has exceeded the value of the *criticalTxUtilAlarmThreshold* attribute for a 3-minute period.

When the status is *clear*, the total average link TxUtilization has subsequently fallen back to a level at or below the corresponding threshold value for a 3-minute period. For the ATM interface, the total average link TxUtilization is calculated every minute based on comparing the number of cells transmitted by the interface with the available link bandwidth.

Probable cause

Type

Remedial action

With a proper threshold setting, this alarm should cause an evaluation of the threshold or potential congestion conditions. The occurrences of the alarm must be evaluated in the context of other parameters, for example, effective cell rate, availability of other atmInterfaces, and routing/loadsharing algorithms.

7040 0000

Component	Severity	Status
Vr/<string> Sres	critical/cleared	set/clear

Legend

<string> = name of the virtual router

Details

The identified *SourceRouteEndStation* (*Sres*) application was unable to obtain sufficient memory to create its forwarding table object.

Effect: SourceRouteEndStation will not function.

Probable Cause

Type

Remedial action

The problem can be corrected by allocate more memory for the *Sres* process. This is done by provisioning the *Mm sresMaxHeapSpace* attribute under the *Vr* component to a higher value.

Another way to fix this problem would be to make the Sres RouteEntry table smaller. This is done by provisioning the *Sres routeTableNumEntries* attribute under the *Vr* component to a smaller value.

Changes could also be made in other parts of the system to leave more memory for SourceRouteEndStation to use.

7040 0001

Component	Severity	Status
Vr/<string> Sres	minor/cleared	set/clear

Legend

<string> = name of the virtual router

Details

The identified *SourceRouteEndStation* (*Sres*) application was unable to obtain memory while in operation.

Effect: *SourceRouteEndStation* will continue to operate but will not be able to learn as many routes as it was provisioned to be able to learn.

Probable Cause

Type

Remedial action

The problem can be corrected by allocate more memory for the *Sres* process. This is done by provisioning the *Mm sresMaxHeapSpace* attribute under the *Vr* component to a higher value.

Another solution would be to make the Sres RouteEntry table smaller. This is done by provisioning the *Sres routeTableNumEntries* attribute under the *Vr* component to a smaller value.

Changes could also be made in other parts of the system to leave more memory for SourceRouteEndStation to use.

7040 0002

Component	Severity	Status
EM/<node name>	minor	message

Legend

<node name> = name of the Passport node

Details

When the SRES feature is enabled on a certain protocol port(s), it should be included in the software feature list of all LAN LPs on the shelf, in order to allow proper routing of traffic directed to and from it.

This alarm is issued for all LAN LPs that do not have *Sres* included in their software feature list.

Probable Cause

Type

Remedial action

Add the SRES feature to the software feature list of the LP indicated in the alarm.

7041 0000

Component	Severity	Status
Atmif/<num1> Uni	warning	msg

Legend

<num1> = 1 - 4095

Details

This alarm is issued when there is an address provisioned on the Uni and the same address is registered through ILMI. The provisioned index (primary or alternate) takes precedence over the registered value. (A registered address is added to the primary list.)

Probable Cause

Configuration error

Type

Operator

Remedial action

Delete the provisioned address.

7041 0001

Component	Severity	Status
Atmif/<num1> Uni	Minor/Cleared	msg

Legend
<num1> = 1 - 4095

Details
If the status is *msg*, the alarm that there is no MAC address available for the card.

If the status is *clear*, the alarm indicates that the Ilmi channel is up and has staged.

Probable Cause
Processor problem

Type
Equipment

Remedial action
The shelf that the card is on may be too old and does not have a MAC address or the termination card is faulty.

7041 0050

Component	Severity	Status
Atmif/<num1> Uni Ilmi	major/cleared	set/clear

Legend

<num1> = 1 - 4095

Details

If the status is *set*, the alarm indicates that the ILMI channel is down.

If the status is *clear*, the alarm indicates that the ILMI channel is up and has staged.

Probable Cause

Processor problem, Loss of signal

Type

Equipment, Communications

Remedial action

The alarm may be generated if the VCC cannot come up, if there is a protocol error, if the other side issues a cold start, if the provisioning is mismatched, or if communication on the link is bad.

Check the provisioning on both ends of the Uni and ensure one end is designated the user side and the other end is designated the network side. Check that both ends of the link are provisioned as addressEnabled. Check that the link is transmitting properly.

7041 0051

Component	Severity	Status
Atmif/<num1> Uni Ilmi	major	message

Legend

<num1> = 1 - 4095

Details

The alarm indicates that the local Uni and its peer are either both configured as Network or are both configured as User.

Probable Cause

Loss of signal

Type

Communications

Remedial action

Check the provisioning on both ends of the Uni and ensure one end is designated the user side and the other end is designated the network side.

7041 0150

Component	Severity	Status
Atmif/<num1> <atmif_type> Atmif/<num1> Vpt/<num2> <atmif_type>	critical/cleared	set/clear

Legend

<num1> = 1 - 4095

<num2> = 0 - 4095

<atmif_type> = Uni “or” Iisp “or” Pnni

Details

If the status is *set*, the alarm indicates that the signalling channel is down.

If the status is *clear*, the alarm indicates that the signalling channel is up.

Probable Cause

Protocol error

Type

Communications

Remedial action

If the alarm is on during the system startup, it is possible that

- the “side” attributes for both ends of the signalling channel may not be set properly (i.e. both ends may have been set to user-to-user or network-to-network).
- the vpi/vci value for the signalling channel for both ends may not be matched.
- one end of the signalling channel was down and the switch may required to be restarted.
- there are errors at the physical layer as indicated by “d -p atmif/<num1> interface” that cause the signalling channel or entire interface to be disabled.
- there are an excessive number of “failedConnections” under the UNI signalling component or AAL5 errors under VCC 0.5 due to incorrect provisioning of the traffic management parameters for the signalling VCC. Verify that the values displayed by
“d -p atmif/<num1> uni sig vcd” are correct.

If the <atmif type> is Pnni, it is possible that the Rcc channel is not up.

7041 0200

Component	Severity	Status
Atmif/<num1> <atmif_type>	major/cleared	set/clear
Atmif/<num1> Vpt/<num2> <atmif_type>		

Legend

<num1> = 1 - 4095

<num2> = 0 - 4095

<atmif_type> = Uni “or” Iisp “or” Pnni

Details

If the status is *set*, the alarm indicates that the Ilmi, signalling or Rcc channel fails to obtain a vcc in the local switch due to insufficient bandwidth.

If the status is *clear*, the alarm indicates that the vcc for the Ilmi, signalling or Rcc channel is created successfully.

Probable Cause

Communications subsystem failure

Type

Communications

Remedial action

User can de-provision some existing PVC/SPVC to release the bandwidth back to the bandwidth pool. Or else, user can clear SVC and return the bandwidth back to the pool. SVC call setup is done by the customer equipment. Issuing “clear” command may not be a permanent solution. Reprovisioning of end-point equipment may be necessary.

7041 0250

Component	Severity	Status
Atmif/<num1> Pnni Rcc	major/cleared	set/clear
Atmif/<num1> Vpt/<num2> Pnni Rcc		

Legend

<num1> = 1 - 4095

<num2> = 0 - 4095

Details

If the status is *set*, the alarm indicates that the Rcc channel fails to reach twoWayInside state.

If the status is *clear*, the alarm indicates that the Rcc channel has either reached twoWayInside state or that a provisioning change it has caused it to be deleted.

Probable Cause

Loss of signal

Type

Communications

Remedial action

Verify that the Vcc for the Rcc channel is up. Verify that the far end node is in the same peer group.

7041 0251

Component	Severity	Status
Atmif/<num1> Pnni Rcc Atmif/<num1> Vpt/<num2> Pnni Rcc	major	message

Legend

<num1> = 1 - 4095

<num2> = 0 - 4095

Details

The Vcc used for the Rcc channel has gone down.

Probable Cause

Loss of signal

Type

Communications

Remedial action

Check that both ends of the connection are using the same Vpi.Vci for the Rcc.

7041 0252

Component	Severity	Status
Atmif/<num1> Pnni Rcc Atmif/<num1> Vpt/<num2> Pnni Rcc	major	message

Legend

<num1> = 1 - 4095

<num2> = 0 - 4095

Details

The Hello FSM has left the twoWayInside state.

Probable Cause

Loss of signal

Type

Communications

Remedial action

Verify that the Rcc channel is up.Verify that the neighbor is in the same peer group.

7041 0253

Component	Severity	Status
Atmif/<num1> Pnni Rcc	major/cleared	set/clear
Atmif/<num1> Vpt/<num2> Pnni Rcc		

Legend

<num1> = 1 - 4095

<num2> = 0 - 4095

Details

If the status is *set*, the alarm indicates that the Hello FSM has detected a neighbor in a different peer group. This prevents the link from being used for PNNI routing.

If the status is *clear*, the alarm indicates that the Hello FSM has detected that the neighbor is now in the same peer group. The link will now be used for PNNI routing.

Probable Cause

Loss of signal

Type

Communications

Remedial action

The peer group of this node and/or its neighbor needs to be changed in order to make them be the same value.

7041 0301

Component	Severity	Status
Artg Pnni	major/cleared	set/clear

Details

This alarm is issued during initial provisioning of the component if a MAC address is not available for the component. This can be caused by a hardware failure that interferes with the distribution of MAC addresses.

Probable Cause

Loss of signal

Type

Communications

Remedial action

Contact your local Nortel Networks technical support group.

7041 0302

Component	Severity	Status
Artg Pnni CfgNode/<level> Rcc	major	set/clear

Legend

<level> = level in the hierarchy

Details

This alarm is set when one of the following conditions occur:

- The node is the one initiating the SVC and the SVC integrity timer expires or the Hello state goes out of 2-way inside
- The node is the one terminating the SVC and the SVCC establishment timer expires or the Hello state goes out of 2-way inside.

This alarm is cleared when one of the following conditions occur:

- The alarm was previously set and the SVCC RCC Hello FSM reaches 2-way inside
- The RCC component to the neighbour no longer exists (i.e. when there are no longer any inducing uplinks between the two nodes).

Probable Cause

Type

Remedial action

To determine what condition is causing the alarm, display the Rcc component helloState and the svcState attributes.

If the svcState is inactive, one of the following conditions may be present:

- The SVC cannot be successfully established. There may be a routing problem or a delay in the notification of uplink removal from lower levels.
  ACTION: Look at the lastFailureCauseCode to determine why the SVC is failing

- The SVCC RCC SVC was torn down due to a network failure.
  ACTION: Look at the lastFailureCauseCode to determine why the SVC was torn down.

If the svcState is active and the helloState is Attempt or 1-Way Inside, one of the following conditions may be present:

- The SVC is up but the Hello protocol running over the channel is stuck in Attempt state or 1-way inside state. If this is the node terminating the SVCC RCC and the svcState is Attempt, it is possible that the node is waiting for an inducing uplink before starting the Hello protocol over the channel.
  ACTION: If this is the node terminating the SVCC RCC and the svcState is Attempt, then wait a minute to see if the condition clears.

7041 0400

Component	Severity	Status
Atmif/<num1> <atmif_type> Atmif/<num1> Vpt/<num2> <atmif type>	warning/cleared	set/clear

Legend

<num1> = 1 - 4095

<num2> = 0 - 4095

<atmif_type> = Uni “or” Iisp “or” Pnni

Details

This alarm is issued when one or more Spvc or Spvp connections are in troubled condition.

Probable Cause

Degraded signal

Type

Communications

Remedial action

At end of each Spvc or Spvp retry period, this alarm is cleared if none of the Spvc and Spvp connections are in troubled condition.

7041 0401

Component	Severity	Status
Atmif/<num1>	major/cleared	set/clear

Legend

<num1> = 1 - 4095

Details

A major alarm is issued when a specified path connection as change state and at least one specified path connection is not using the primary path. A clear alarm is issued when all the specified path connections are using the primary path.

Probable Cause

Type

Remedial action

The network operator should poll the switch to determine which connection is not on the primary path.

If the connection is using a different path than the primary path, the network operator can use the reconnect command to re-establish the connection to the primary path.

7041 0500

Component	Severity	Status
Atmif/<num1> <atmif_type> Atmif/<num1> Vpt/<num2> <atmif_type>	warning/cleared	set/clear

Legend

<num1> = 1 - 4095

<num2> = 0 - 4095

<atmif_type> = Uni “or” Iisp “or” Pnni

Details

If the status is *set*, one or more connections under the given signalling interface have undergone a successful connection recovery. The alarm is only set if these connections are also subscribed to path optimization.

A *clear* is issued when the connections have been optimized or released.

Probable Cause

Type

Remedial action

The OPTIMIZE verb can be applied to the Ebr component to trigger an optimization of the connections at that interface. The triggering of an optimization results in an attempt to optimize the connection. The connection will only be rerouted if a better route is available.

7041 0600

Component	Severity	Status
Atmif/<num1> <atmif_type>	minor/cleared	set/clear

Legend

<num1> = 1 - 4095

<atmif_type> = Uni “or” Iisp “or” Pnni

Details

If the status is *set*, one or more of the switched connections under this ATM interface are not currently spared, due to a failure to create the connections on the standby port, or due to a loss of synchronization of the journaling software. If alarm 7039 2001 is seen shortly before this alarm occurs, this alarm may be due to a configuration error. If this alarm is not accompanied by alarm 7039 2001, it may be due to a software error.

If an FP switchover occurs in this state, one or more of the connections may go down. They may or may not come back up after the switchover.

A *clear* is issued when all switched connections under this ATM interface are again spared. This may be because the unspared connections have now been successfully created on the standby, or because the unspared connections have been deleted.

Probable Cause

Underlying resource unavailable

Type

Processing

Remedial action

If the provisioned values of the *maxVpcs* or *maxVccs* attributes have been exceeded (see alarm 7039 2001), either reprovision the *Ca* component or delete one or more connections. Otherwise, contact Nortel Networks global support.

7041 0601

Component	Severity	Status
Atmif/<num1> <atmif_type>	minor/cleared	set/clear

Legend

<num1> = 1 - 4095

<atmif_type> = Uni “or” Iisp “or” Pnni

Details

If the status is *set*, at least one control channel (Ilmi, Signalling, or Rcc) under this ATM interface is not currently spared, due to a failure to create the control channel on the standby port, or due to a loss of synchronization of the journaling software. This alarm may be due to a configuration error or a software error.

If an FP switchover occurs in this state, one or more of the control channels may go down. They may or may not come back up after the switchover.

A *clear* is issued when all control channels under this ATM interface are again spared. This may be because the unspared control channel has now been successfully created on the standby, or because the signalling component that owns the unspared control channels has been deleted.

Probable Cause

Underlying resource unavailable

Type

Processing

Remedial action

If the available bandwidth for the ATM interface (*Atmif/<num1> Ca poolAvailabilityBandwidth*) is not sufficient to meet the requirements of all provisioned connections and the control channels, the provisioned connections may consume all the bandwidth on the standby card so that the control channels cannot be created. In this case, either increase the configured bandwidth or delete some provisioned connections. Otherwise, contact Nortel Networks support.

7041 0602

Component	Severity	Status
ARtg Pnni Top/<level> Node/<node_id>	major	message

Legend

<level> = The hierarchy level of the originating node of the large PTSE

<node_id> = The node ID of the originating node of the large PTSE

Details

This alarm is raised when a large PTSE is received from a PNNI node and is installed in the topology database, but it failed to be journaled to the standby card.

Probable Cause

On i960 cards, this usually happens when the size of the received PTSE is larger than 1000 bytes.

On PQC cards, this usually happens when the size of the received PTSE is larger than 4000 bytes.

Type

Quality of service

Remedial action

If the originating node of the PTSE is a Passport node and the violating PTSE is an address PTSE, either some of the addresses on the specified node must be removed or a summary address should be provisioned on the node to summarize local addresses.

7041 0603

Component	Severity	Status
ARtg	major	message

Details

This alarm is raised when both the following conditions are met:

- The Hot PNNI CP Hitless Software Migration has been started for a minimum of 10 minutes (with attribute *ARtg SpServ sparing* set to enable) without completing successfully.

- The synchronization of the spared Application Ports between the spared active CP and the migration active CP cannot complete successfully because at least one of the standby FPs is not inserted in the migration active shelf. The alarm indicates which card is missing in the migration active shelf.

This alarm is pausable and you can either complete the Hitless Software Migration with a loss of service for the applications that are spared by that FP, or you can revert back and replace (or insert) the missing FP.

Probable Cause

This usually occurs when the provisioning indicates that two FPs are spared together. Therefore, the applications running on them are spared but

1. the standby FP is not physically inserted in the shelf.

2. the standby FP is locked.

3. the standby FP is inserted but not working properly.

Type

Equipment

Remedial action

There are two options:

1. Continue provisioning, which completes the Hitless Software Migration with a loss of service for the applications that are spared by the missing FP.

2. Stop provisioning, which stops the Hitless Software Migration. You can then either add or replace the missing (not working) FP.

7041 0604

Component	Severity	Status
Atmif/<num1> <atmif_type>	minor/cleared	set/clear

Legend

<num1> = 1 - 4095

<atmif_type> = Uni “or” Iisp “or” Pnni

Details

If the status is *set*, one or more of the provisioned connections under this ATM interface are not currently spared, due to a failure to create the connections on the standby port, or due to a loss of synchronization of the journaling software. If alarm 7039 2001 is seen shortly before this alarm occurs, this alarm may be due to a configuration error.

If an FP switchover occurs in this state, one or more of the connections may go down. They may or may not come back up after the switchover.

A *clear* is issued when all provisioned connections under this ATM interface are again spared. This may be because the unspared connections have now been successfully created on the standby, or because the unspared connections have been deleted.

Probable Cause

Underlying resource unavailable

Type

Processing

Remedial action

If the provisioned values of the *maxVpcs* or *maxVccs* attributes have been exceeded (see alarm 7039 2001), either reprovision the *Ca* component or delete one or more connections. Otherwise, contact Nortel Networks global support.

7041 0605

Component	Severity	Status
Atmif/<num1> <atmif_type>	minor/cleared	set/clear

Legend

<num1> = 1 - 4095

<atmif_type> = Uni “or” Iisp “or” Pnni

Details

If the status is *set*, one or more of the static addresses under this ATM interface are not currently spared, due to a failure to create the addresses on the standby port, or due to a loss of synchronization of the journaling software. If alarm 7039 2001 is seen shortly before this alarm occurs, this alarm may be due to a configuration error. If this alarm is not accompanied by alarm 7039 2001, it may be due to a software error.

If an FP switchover occurs in this state, one or more of the addresses may not be present and routing problems may occur. The addresses may or may not be added to the routing database after the switchover.

A *clear* is issued when all addresses under this ATM interface are again spared. This may be because the addresses have now been successfully created on the standby, or because the addresses have been deleted.

Probable Cause

Underlying resource unavailable

Type

Processing

Remedial action

If the problem persists, contact Nortel Networks global support.

7041 0606

Component	Severity	Status
Atmif/<num1> <atmif_type>	minor/cleared	set/clear

Legend

<num1> = 1 - 4095

<atmif_type> = Uni “or” Iisp “or” Pnni

Details

If the status is *set*, one or more of the PNNI PTSEs under this ATM interface are not currently spared, due to a failure to create the PTSEs on the standby port, or due to a loss of synchronization of the journaling software. If alarm 7039 2001 is seen shortly before this alarm occurs, this alarm may be due to a configuration error. If this alarm is not accompanied by alarm 7039 2001, it may be due to a software error.

If an FP switchover occurs in this state, one or more of the addresses may not be present and routing problems may occur. The addresses may or may not be added to the routing database after the switchover.

A *clear* is issued when all PNNI PTSEs under this ATM interface are again spared. This may be because the PTSEs have now been successfully created on the standby, or because the PTSEs have been deleted.

Probable Cause

Underlying resource unavailable

Type

Processing

Remedial action

If the problem persists, contact Nortel Networks global support.

7042 0001

Component	Severity	Status
Aal1Ces/<num1>	major	set/clear

Legend

<num1> = 1 - 16383

Details

When dummy data has been inserted continuously due to buffer underflow for a period equal to the *cellLossIntegrationPeriod*, a loss of cells alarm will be raised. The alarm will be cleared when the buffer has been re-initialized (i.e. filled to its nominal level with valid AAL1 cells), and the service has subsequently been in operation for a continuous period equal to ten times the *cellLossIntegrationPeriod* without experiencing further buffer underflow.

Probable Cause

thresholdCrossedCause

Type

qualityOfServiceType

Remedial action

Buffer underflow indicates that cells are arriving more slowly than expected, are being lost in the network, or are of the wrong type to be allowed into the buffer (i.e. do not conform to the AAL1 protocol). Ensure that both ends of the connection are provisioned to have the same traffic rate and that every hop in the network has enough bandwidth to carry the traffic. Ensure that cells which are arriving conform to the AAL1 protocol.

The AAL1 cells arriving at the module from the ATM network are managed by a *Vcc* component under a particular *AtmIf* component on an ATM FP. Check the OSI states of these components to ensure they are functioning appropriately. Check the *rxCell* count of the *Vcc* component to ensure that cells are actually arriving from the network. For more information refer to the Troubleshooting section of the ATM Core Services document.

7042 0002

Component	Severity	Status
Aal1Ces/<num1>	major	set/clear

Legend

<num1> = 1 - 16383

Details

When AAL1 processing of received cells fails for 2 consecutive seconds, an AAL1 layer alarm will be raised (note that this includes the scenario where no cells at all have been received). The alarm will be cleared when AAL1 processing of received cells resumes, and has been in synchronous operation for 10 consecutive seconds.

Probable Cause

corruptDataCause

Type

processingType

Remedial action

Ensure that cells are being received (check the *rxCells* attribute is incrementing).

Ensure that the remote end system is configured to generate AAL1 cells, and that the *Aal1Ces* is associated with the relevant *Vcc* which is managing the AAL1 cells arriving from the network.

Ensure the remote end system is generating valid AAL1 data. For example, arrange to have local diagnostics run at the far end.

Ensure that received cells are not being discarded due to congestion on the module. Check the *rxDiscard* attribute of the relevant *Vcc*.

Ensure that cells are not being discarded due to noise on the line. Check the error statistics for the physical port associated with the relevant *AtmIf* on the ATM FP.

7042 0003

Component	Severity	Status
Aal1Ces/<num1>	major	set/clear

Legend

<num1> = 1 - 16383

Details

When the *Aep* subcomponent of an *Aal1Ces* component has initiated a number of consecutive unsuccessful call setup attempts equal to the value of the provisioned *retryLimit*, no further setups are attempted and this alarm is raised.

Probable Cause

callEstablishmentErrorCause

Type

communicationsType

Remedial action

Check the *lastSetupFailureCause* in the *Aep* subcomponent of the *Aal1Ces* and take appropriate management action, such as reprovisioning.

When the appropriate management action has been taken, issue a *restart* against the relevant *Aep* subcomponent to restart the automatic connection procedure.

7043 0001

Component	Severity	Status
ServiceTrace	warning	message

Details

The Trace Manager was deleted while a trace session was active. Tracing is no longer possible on this module until the *ServiceTrace* component is provisioned off root.

Probable Cause

softwareProgramTerminationCause

Type

processingType

Remedial action

Provision the *ServiceTrace* component and receiver list and restart the trace if required.

7043 0002

Component	Severity	Status
<component_name> ServiceTrace	warning	message

Legend
<component_name> = The service component running the trace.

Details
Trace was stopped due to the specified duration limit being reached.

Probable Cause
outOfServiceCause

Type
operatorType

Remedial action
Increase the trace duration limit and restart the trace if required.

7043 0003

Component	Severity	Status
<component_name> ServiceTrace	warning	message

Legend

<component_name> = The service component running the trace.

Details

The trace audit message which is issued every 60 minutes while a Trace Session is active to remind the operator that the traced service performance is impacted while the trace is running.

Probable Cause

performanceDegradedCause

Type

qualityOfServiceType

Remedial action

None.

7043 0004

Component	Severity	Status
<component_name> ServiceTrace	warning	message

Legend

<component_name> = The service component running the trace.

Details

The trace queue is 50%, 75% or 100% full. At 100% full trace data will be discarded until the queue empties to 75% full.

The trace queue fills up because trace data is being generated faster than the trace VC to the receiver can carry it.

Probable Cause

queueSizeExceededCause

Type

qualityOfServiceType

Remedial action

Reduce the amount of trace data generated by applying filters or truncating the traced data.

It may also be possible to prevent trace data loss by increasing the trace queue size or increasing the trace VC carrying capacity.

7043 0005

Component	Severity	Status
<component_name> ServiceTrace	warning	message

Legend
<component_name> = The service component running the trace.

Details
The trace call to the receiver has disconnected and tracing has stopped. The clear cause and diagnostic code for the failure are given.

Possible causes for this alarm include a failure along the VC path or at the receiver.

Probable Cause
commSubsystemFailureCause

Type
communicationsType

Remedial action
Determine why the call to the receiver cleared and restart the trace if required.

7044 0005

Component	Severity	Status
Vr/<string1> Pp/<string2> SnaPort	minor	set/clear

Legend

<string1> = name of the virtual router

<string2> = name of the protocol port

Details

When the status is *set*, the *snmpAdminStatus* attribute has been set to DOWN.

The *SnaPort* component is administratively disabled.

When the status is *clear* the *snmpAdminStatus* attribute has been set to UP.

Probable Cause

Type

Remedial action

When the status is *set*, use the set verb to set the *snmpAdminStatus* attribute to UP.When the status is *clear*, no remedial action is required.

7044 0006

Component	Severity	Status
Vr/<string1> Sna	minor	set/clear

Legend
<string1> = name of the virtual router

Details
When the status is *set*, the *snmpAdminStatus* attribute has been set to DOWN.

The *Sna* component is administratively disabled.

When the status is *clear* the *snmpAdminStatus* attribute has been set to UP.

Probable Cause

Type

Remedial action
When the status is *set*, use the set verb to set the *snmpAdminStatus* attribute to UP.When the status is *clear*, no remedial action is required.

7044 0007

Component	Severity	Status
Vr/<string1> Sna	critical	set/clear

Legend

<string1> = name of the virtual router

Details

When the status is *set*, the *Sna* component has been locked.

When the status is *clear* the *Sna* component has been unlocked.

Probable Cause

Type

Remedial action

When the status is *set*, use the unlock verb to unlock the virtual router's *Sna* subcomponent.When the status is *clear*, no remedial action is required.

7044 0008

Component	Severity	Status
Vr/<string1> Mm	major	message

Legend

<string1> = name of the virtual router

Details

The range of *snaMaxHeapSpace* attribute is 0 to 100. When this attribute is set too low, there will be no memory available under the virtual router for the *Sna* component.

Probable Cause

Type

Remedial action

Use the set verb to set the *snaMaxHeapSpace* attribute to a higher number.

7044 0009

Component	Severity	Status
Vr/<string1> Sna	minor	set/clear

Legend

<string1> = name of the virtual router

Details

When the status is *set*, an error has been detected in the provisioning data delivered to data link routing (DLR).

When the status is *clear*, the provisioning data delivered to data link routing (DLR) has been accepted.

Probable Cause

Type

Remedial action

When the status is *set*, verify that the provisioning data defined for the *Sna* and *SnaPort* components is correct, then re-apply. When the status is *clear*, no remedial action is required.

7044 0010

Component	Severity	Status
Vr/<string1> Pp/<string2> SnaPort	critical	set/clear

Legend

<string1> = name of the virtual router

<string2> = name of the protocol port

Details

When the status is *set*, the *SnaPort* component has been locked.

When the status is *clear* the *SnaPort* component has been unlocked.

Probable Cause

Type

Remedial action

When the status is *set*, use the unlock verb to unlock the *SnaPort* subcomponent.When the status is *clear*, no remedial action is required.

7044 0011

Component	Severity	Status
Vr/<string1> Sna	major	message

Legend

<string1> = name of the virtual router

Details

An SnaPort component can only be added to a *ProtocolPort* component for which the media application is DLR media.

Probable Cause

Type

Remedial action

The *ProtocolPort* component under which the *SnaPort* component is defined must have a *linkToMedia* attribute provisioned as a valid *GvcIf Rg* component.

7046 0001

Component	Severity	Status
GvcIf/<num1> SubComponent	warning	message

Legend

SubComponent = none or Lcn/<n>

<num1> = Decimal [0-15]. Instance identifier of the GVC Interface component

<n> = Decimal [1-4095]. Instance identifier of the LCN component.

Details

This alarm is issued when the *issueLcnClearAlarm* attribute of the *GvcIf* component is set to allowed and a call is cleared.

The alarm is used for debugging purposes. It contains information about the reason for clearing the call as well as information about related components affected by the call clear.

If present, the related component information contains the Vr/n Pp/name SnaPort Circuit/mac,sap,mac,sap where the mac and sap information are those of the source and destination devices of the call.

The Com field contains an explanation about the clear reason. This could be one of the following:

- incoming call refused. Interface locked
- incoming call refused. No LCNs available
- requested application not registered

Probable Cause

Type

Remedial action

No operator intervention is required. Examining the alarm data gives a hint of why the call has been cleared.

7046 0002

Component	Severity	Status
GvcIf/<num1> Dlci/<num2> SubComponent	warning	message

Legend

SubComponent = none or Bnn (if PVC)

<num1> = Decimal [0-15]. Instance identifier of the GVC Interface component

<num2> = Decimal [16-4095]. Instance identifier of the DLCI component.

Details

This alarm indicates that a frame is received on a BNN DLCI VC containing a (lSap,rSap) pair which is not recognized on this BNN connection.

Probable Cause

Type

Remedial action

Verify that both end-devices are using RFC1490 BNN encoding on this DLCI.

7046 1000

Component	Severity	Status
GvcIf/<num1> SubComponent	indeterminate	message

Legend

SubComponent = Dna/<n> Ddm or

Dna/<n> Sdm/<dna> or

RemoteDnaMap/<npi>,<dna>

<num1> = Decimal [0-15]. Instance identifier of the GVC Interface component

<n> = Decimal [0-99].

<npi> = Enumeration(x121, e164)

<dna> = BCD(1 to 15 decimal digits).

Details

The most probable cause of this problem is the presence of a *RemoteDnaMap* component with an instance equivalent to that of the *Dna* attribute of a *Dna* component which has a *DefaultDnaMap* component defined, or it is equivalent to a subDna for which a *SubDnaMap* component exists.

Provisioning data for the component referred to by this alarm could not be handled properly by the switch. The service still activates without the functionality of the incorrect component.

Probable Cause

Type

Remedial action

Delete either the *RemoteDnaMap*, the *DefaultDnaMap* or the *SubDnaMap* component.

7046 3000

Component	Severity	Status
GvcIf/<num1>	indeterminate	message

Legend
<num1> = Decimal [0-15]. Instance identifier of the GVC Interface component

Details
The service cannot be created due to lack of memory.

Probable Cause

Type

Remedial action
Re-engineer the mix of services on the card.

7047 0000

Component	Severity	Status
Vr/<string1> Pp/<string2> SnaPort	minor	message

Legend

<string1> = name of the virtual router

<string2> = name of the protocol port

Details

The system has insufficient resources to allow SNA DLR to start

Probable Cause

Type

Remedial action

Re-engineer the services on the card.

7047 0002

Component	Severity	Status
Vr/<string1> Pp/<string2> SnaPort	minor	message

Legend

<string1> = name of the virtual router

<string2> = name of the protocol port

Details

The DLC provider was not created.

No circuit can be activated through the DLC provider.

Probable Cause

Type

Remedial action

Refer to DLC provider-specific logs for details of the error.

7047 0003

Component	Severity	Status
Vr/<string1> Pp/<string2> SnaPort	minor	message

Legend

<string1> = name of the virtual router

<string2> = name of the protocol port

Details

SNA DLR has insufficient resources to establish a connection initiated by a remote end.

Circuits cannot be activated.

Probable Cause

Type

Remedial action

If further attempts by the remote end to establish a connection fail, re-engineer the services on the card.

7047 0006

Component	Severity	Status
Vr/<string1> Pp/<string2> SnaPort	minor	message

Legend

<string1> = name of the virtual router

<string2> = name of the protocol port

Details

A DLR circuit for SNA has failed because of insufficient resources.

The DLR circuit is not established, or is deactivated.

Probable Cause

Type

Remedial action

Try to activate the circuit again. If this fails, reduce the load on SNA DLR by closing unnecessary circuits and connections, or decrease the system load on the DLR machine (for example, by stopping one or more applications), or re-engineer the services on the card.

7047 0008

Component	Severity	Status
Vr/<string1> Pp/<string2> SnaPort	minor	message

Legend

<string1> = name of the virtual router

<string2> = name of the protocol port

Details

A DLR circuit for SNA has failed because of insufficient resources.

The DLR circuit is not established, or is deactivated.

Probable Cause

Type

Remedial action

Try to activate the circuit again. If this fails: reduce the load on SNA DLR by closing unnecessary circuits and connections, or decrease the system load on the DLR machine (for example, by stopping one or more applications), or re-engineer the services on the card.

7047 0010

Component	Severity	Status
Vr/<string1> Pp/<string2> SnaPort	minor	message

Legend

<string1> = name of the virtual router

<string2> = name of the protocol port

Details

A DLR circuit has been idle for the configured timeout period.

The circuit is disconnected.

Probable Cause

Type

Remedial action

The cause could be a timing problem. Check that the SNA DLR user on the local LAN and remote end are functioning correctly.

Retry the operation, or restart the circuit.

7047 0011

Component	Severity	Status
Vr/<string1> Pp/<string2> SnaPort	minor	message

Legend

<string1> = name of the virtual router

<string2> = name of the protocol port

Details

A timer could not be started due to resource shortage.

One or more inactive circuits may not time out. This may cause subsequent attempts to activate the circuit to fail.

Probable Cause

Type

Remedial action

Restart SNA DLR.

7047 0014

Component	Severity	Status
Vr/<string1> Pp/<string2> SnaPort	minor	message

Legend

<string1> = name of the virtual router

<string2> = name of the protocol port

Details

SNA DLR has failed because it has insufficient resources.

All circuits are disconnected and SNA DLR stops.

Probable Cause

Type

Remedial action

Decrease the system load (for example, by stopping one or more applications) or re-engineer the service on the card and restart SNA DLR.

7047 0015

Component	Severity	Status
Vr/<string1> Pp/<string2> SnaPort	minor	message

Legend

<string1> = name of the virtual router

<string2> = name of the protocol port

Details

SNA DLR has experienced a critical resource failure while processing a data signal.

The circuit is deactivated.

Probable Cause

Type

Remedial action

Reduce the load on SNA DLR by closing unnecessary circuits and connections, or decrease the system load on the DLR machine (for example, by stopping one or more applications), or re-engineer the service on the card.

7047 0016

Component	Severity	Status
Vr/<string1> Pp/<string2> SnaPort	minor	message

Legend

<string1> = name of the virtual router

<string2> = name of the protocol port

Details

A DLC provider has abended.

Links established through the provider are deactivated.

Probable Cause

Type

Remedial action

Refer to DLC provider-specific logs for details of the problem.

7047 0017

Component	Severity	Status
Vr/<string1> Pp/<string2> SnaPort	minor	message

Legend

<string1> = name of the virtual router

<string2> = name of the protocol port

Details

A major SNA DLR subcomponent has failed.

All circuits are disconnected and SNA DLR terminates.

Probable Cause

Type

Remedial action

Check log file for supporting information and notify your Nortel Networks technical support group.

7047 0021

Component	Severity	Status
Vr/<string1> Pp/<string2> SnaPort	minor	message

Legend

<string1> = name of the virtual router

<string2> = name of the protocol port

Details

SNA DLR has experienced a critical resource failure while processing a SOF verb.

The verb has been returned with bad return codes.

Probable Cause

Type

Remedial action

Reduce the load on SNA DLR by closing unnecessary circuits and connections, or decrease the system load on the SNA DLR machine (for example, by stopping one or more applications), or make more storage (for example, machine memory) available to SNA DLR, and restart SNA DLR then retry the verb.

7047 0022

Component	Severity	Status
Vr/<string1> Pp/<string2> SnaPort	minor	message

Legend

<string1> = name of the virtual router

<string2> = name of the protocol port

Details

SNA DLR has abended because the component providing local switching support has abended.

All circuits are disconnected and SNA DLR stops.

Probable Cause

Type

Remedial action

Check log file for supporting information and notify your Nortel Networks technical support group.

7047 0051

Component	Severity	Status
Vr/<string1> Pp/<string2> SnaPort	minor	message

Legend

<string1> = name of the virtual router

<string2> = name of the protocol port

Details

An unrecognized or unexpected signal was received from a remote end of the circuit.

The signal is ignored.

Probable Cause

Type

Remedial action

Check log file for supporting information and notify your Nortel Networks technical support group.

7047 0052

Component	Severity	Status
Vr/<string1> Pp/<string2> SnaPort	minor	message

Legend

<string1> = name of the virtual router

<string2> = name of the protocol port

Details

An unrecognized or unexpected signal was received from a local end of the circuit.

The signal is ignored.

Probable Cause

Type

Remedial action

Check log file for supporting information and notify your Nortel Networks technical support group.

7047 0056

Component	Severity	Status
Vr/<string1> Pp/<string2> SnaPort	minor	message

Legend

<string1> = name of the virtual router

<string2> = name of the protocol port

Details

An ENTER_BUSY signal was received from a remote end for a circuit which is already in Busy state.

The ENTER_BUSY signal is treated as a duplicate and ignored.

Probable Cause

Type

Remedial action

Check log file for supporting information and notify your Nortel Networks technical support group.

7047 0057

Component	Severity	Status
Vr/<string1> Pp/<string2> SnaPort	minor	message

Legend

<string1> = name of the virtual router

<string2> = name of the protocol port

Details

An EXIT_BUSY signal was received from a remote end for a circuit which is not in Busy state.

The EXIT_BUSY signal is treated as a duplicate and ignored.

Probable Cause

Type

Remedial action

Check log file for supporting information and notify your Nortel Networks technical support group.

7047 0059

Component	Severity	Status
Vr/<string1> Pp/<string2> SnaPort	minor	message

Legend

<string1> = name of the virtual router

<string2> = name of the protocol port

Details

SNA DLR has failed to add a MAC cache entry due to a non-critical resource failure.

The number of circuit set-up messages sent to all partner switches on the WAN, rather than to one specific partner, will increase. The amount of extra WAN traffic generated will depend on the number of partners compared to the configured size of the cache.

SNA DLR will recover from the condition. If this log is repeated, performance will suffer and WAN traffic will increase.

Probable Cause

Type

Remedial action

If the problem persists: reduce the load on SNA DLR by closing unnecessary circuits and connections, or decrease the system load on the DLR machine (e.g. by stopping one or more applications), or re-engineer the service on the card.

7047 0062

Component	Severity	Status
Vr/<string1> Pp/<string2> SnaPort	minor	message

Legend

<string1> = name of the virtual router

<string2> = name of the protocol port

Details

SNA DLR has experienced a non-critical resource failure.

SNA DLR will recover from the condition. If this log is repeated, performance may suffer.

Probable Cause

Type

Remedial action

If the problem persists: reduce the load on SNA DLR by closing unnecessary circuits and connections, or decrease the system load on the DLR machine (e.g. by stopping one or more applications), or re-engineer the service on the card.

7047 0063

Component	Severity	Status
Vr/<string1> Pp/<string2> SnaPort	minor	message

Legend

<string1> = name of the virtual router

<string2> = name of the protocol port

Details

SNA DLR has experienced a severe resource failure.

The activation or deactivation of a circuit or connection may fail, or data transfer may stop.

Probable Cause

Type

Remedial action

Reduce the load on SNA DLR by closing unnecessary circuits and connections, or decrease the system load on the SNA DLR machine (for example, by stopping one or more applications), or re-engineer the service on the card.

7047 0064

Component	Severity	Status
Vr/<string1> Pp/<string2> SnaPort	minor	message

Legend

<string1> = name of the virtual router

<string2> = name of the protocol port

Details

SNA DLR has insufficient resources to establish a connection immediately to a partner DLR.

Circuits cannot currently be activated.

Probable Cause

Type

Remedial action

Re-engineer the service on the card.

7048 2001

Component	Severity	Status
DataSigChan/<x> Cc Cg/<y> Cgpn/<z>	warning	message

Legend

<x> = 1 - 255

<y> = 1 - 31

<z> = 1 - 14 (BCD)

Details

A *Cgpn* component has already been created under another *CallingGroup* component of the same *CallControl* component.

Probable Cause

Duplicate information

Type

Security

Remedial action

Change the provisioning to remove duplication of the *Cgpn* component under the *CallControl* component.

7048 2002

Component	Severity	Status
DataSigChan/<x> Cc Cg/<y>	warning	message

Legend

<x> = 1 - 255

<y> = 1 - 31

Details

The *channelList* attribute of the *CallingGroup* component includes a channel greater than 23 on a DS1C card.

Probable Cause

Duplicate information

Type

Security

Remedial action

Remove all channels greater than 23 from the *channelList* attribute.

7049 0000

Component	Severity	Status
SigChan/<instance> or DataSigChan/<instance>	critical	set/clear

Legend

<instance> = a decimal value

Details

If the status is *set*, the alarm indicates that the signalling channel is disabled for one of the following reasons:

1) the Sigchan or DataSigChan is being created
2) the Sigchan or DataSigChan is locked
3) the Sigchan or DataSigChan's framer is disabled
4) the peer or DataSigChan's d-channel is down

If the status is *clear*, the alarm indicates that the signalling channel is back in service

Probable Cause

Underlying Resource Unavailable

Type

Quality Of Service

Remedial action

If the alarm status is set for a long period of time:

1) Check the cabling.
2) Verify that the physical layer of the signalling channel is up (for example, Lp/x Ds1/y and Lp/x rDs1/y Chan/z).
3) Check the state of the external equipment connected to the Passport node.
4) Verify that the attached external equipment of the SigChan is properly configured (one must be master, the other must be slave).
5) Lock and unlock the *SigChan* component.

Contact your local Nortel Networks technical support group.

7049 0001

Component	Severity	Status
Lp/<num1> <type>/<num2>	warning	message

Legend

<num1> = 1 - 15

<type> = e1 or ds1

<num2>= 0 - 3

Details

This alarm indicates that all Uipe debug tracing activity on this port is disabled for one minute due to resource exhaustion. Tracing will be re-enabled automatically after one minute.

Probable Cause

At or near capacity

Type

Debug

Remedial action

Check the amount of traffic on this port.
Contact your local Nortel Networks technical support group

7049 0002

Component	Severity	Status
Lp/<num1> <type>/<num2>	warning	set/clear

Legend

<num1> = 1 - 15

<type> = e1 or ds1

<num2>= 0 - 3

Details

If the status is *set*, the alarm indicates that the Uipe's queue to port is full. This could cause many calls to fail on this port.

If the status is *clear*, the alarm indicates that the queue is no longer full.

Probable Cause

At or near capacity

Type

Quality of service

Remedial action

Check the amount of traffic on this port.
Contact your local Nortel Networks technical support group.

7049 0003

Component	Severity	Status
Lp/<num1> <type>/<num2>	warning	set/clear

Legend

<num1> = 1 - 15

<type> = e1 or ds1

<num2>= 0 - 3

Details

If the status is *set*, the alarm indicates that the Uipe's queue to Q921 is full. This could cause many calls to fail on this port.

If the status is *clear*, the alarm indicates that the queue is no longer full.

Probable Cause

At or near capacity

Type

Quality of service

Remedial action

Check the amount of traffic on this port.
Contact your local Nortel Networks technical support group.

7049 0004

Component	Severity	Status
Lp/<num1> <type>/<num2>	warning	set/clear

Legend

<num1> = 1 - 15

<type> = e1 or ds1

<num2>= 0 - 3

Details

If the status is *set*, the alarm indicates that the Uipe's queue to Q931 is full. This could cause many calls to fail on this port.

If the status is *clear*, the alarm indicates that the queue is no longer full.

Probable Cause

At or near capacity

Type

Quality of service

Remedial action

Check the amount of traffic on this port.
Contact your local Nortel Networks technical support group.

7049 0005

Component	Severity	Status
Lp/<num1> <type>/<num2>	warning	set/clear

Legend

<num1> = 1 - 15

<type> = e1 or ds1

<num2>= 0 - 3

Details

If the status is *set*, the alarm indicates that the Uipe's queue to APC is full. This could cause many calls to fail on this port.

If the status is *clear*, the alarm indicates that the queue is no longer full.

Probable Cause

At or near capacity

Type

Quality of service

Remedial action

Check the amount of traffic on this port.
Contact your local Nortel Networks technical support group.

7049 0006

Component	Severity	Status
Lp/<num1> <type>/<num2>	warning	set/clear

Legend

<num1> = 1 - 15

<type> = e1 or ds1

<num2>= 0 - 3

Details

If the status is *set*, the alarm indicates that the Uipe's ISDN buffer is full. This could cause many calls to fail on this port

If the status is *clear*, the alarm indicates that the buffer is no longer full

Probable Cause

At or near capacity

Type

Quality of service

Remedial action

Check the amount of traffic on this port.
Contact your local Nortel Networks technical support group.

7049 0007

Component	Severity	Status
sigChan/<instance>	critical	message

Legend

<instance> = a decimal value

Details

This alarm indicates that a B-channel is out of service because no RESTART ACKNOWLEDGE message is received prior to the second expiry of timer T316.

Probable Cause

Underlying resource unavailable

Type

Quality of service

Remedial action

Ensure that the attached B-channel is properly configured.

Contact your local Nortel Networks technical support group.

7049 0008

Component	Severity	Status
sigChan/<instance>	critical	message

Legend

<instance> = a decimal value

Details

This alarm indicates that a signalling channel is out of service because no RESTART ACKNOWLEDGE message is received prior to the second expiry of timer T316.

Probable Cause

Underlying resource unavailable

Type

Quality of service

Remedial action

Ensure that the attached signalling channel is properly configured.

Contact your local Nortel Networks technical support group.

7049 0009

Component	Severity	Status
VoiceSubroute/<instance>	critical	message

Legend

<instance> = a decimal value

Details

This alarm indicates that all of the resources required to maintain call states of busy channels are in use. No new calls are accepted by this subroute until these resources are released.

Probable Cause

Underlying resource unavailable

Type

Quality of service

Remedial action

This alarm may appear during very busy conditions due to congestions in the PP subnet and heavy use of non-call associated signalling (signalling required for some PBX features without the use of B-channel). It simply indicates that the internal resources are used to maximum capacity.

If this alarm is repeated consistently for every new call attempt, it indicates that resources are not being released.

If there is a frequent recurrence of this alarm, contact your local Nortel Networks technical support group.

7049 0010

Component	Severity	Status
VoiceSubroute/<instance>	warning	message

Legend

<instance> = a decimal value

Details

This alarm indicates that the call failed because no compatible voice, modem or fax capability was found during end-to-end negotiation. DNA routing information is displayed if available to aid in the remedial action. This alarm is only generated 5 times per hour per voiceSubRoute.

Probable Cause

Underlying resource unavailable

Type

Quality of service

Remedial action

To correct the problem the user must do one or more of the following:

- make provisioning changes to the selected Voice Profile
- modify the features available on the source card
- modify the features available on the destination card

7049 0011

Component	Severity	Status
VoiceSubroute/<instance>	warning	message

Legend

<instance> = a decimal value

Details

This alarm may appear on a PP provisioned as the network side, when an outgoing call tries to seize a channel which is not available for service on the PBX or in a glare situation.

The alarm indicates that the channel is marked unavailable for outgoing calls from the PP.The marking is done to prevent repetitive attempts to seize the same channel which is not available on the PBX.

The channel is put back in an available state by an incoming call from the PBX or by a midnight maintenance routine performed by the PP.

Probable Cause

Underlying resource unavailable

Type

Quality of service

Remedial action

To clear the alarm immediately, lock/unlock the channel.

7050 0001

Component	Severity	Status
Rsa/<instance> VncsAccess	critical/cleared	set/clear

Legend

<instance> = a string value

Details

If the status is *set*, the Remote Server Agent is unable to forward requests to the Voice Networking Call Server. While this alarm is *set*, all requests for the server are discarded.

Possible causes for this alarm are either the VNCS application is not provisioned on the CP or the CP is in the process of a switchover and VNCS is not yet available.

A *clear* is issued when the first request is successfully forwarded to the VNCS server.

Probable Cause

Communication subsystem failure

Type

Communications

Probable Cause

Configuration or customization error

Type

Processing

Remedial action

Verify that the VNCS application is provisioned on the CP.

If the cause is determined to be CP switchover, no action is required. The alarm will clear when VNCS begins accepting requests.

7050 0002

Component	Severity	Status
Rsa/<instance> Connection/<n>	warning	message

Legend

<instance> = a string value

<n> = a decimal value interpreted as the logical channel number

Details

The LAPF transmit queue for this connection has exceeded its maximum value of 300 frames and has been purged.

This alarm is caused by congestion along the connection path.

Probable Cause

Queue size exceeded

Type

Quality of service

Remedial action

The Remote Server Agent should be re-engineered to decrease the combined traffic from its connections. This could involve configuring an additional RSA in the network and re-homing some of the connections to this new RSA.

7050 0003

Component	Severity	Status
Rsa/<instance> Connection/<n>	warning	message

Legend

<instance> = a string value

<n> = a decimal value interpreted as the logical channel number

Details

The LAPF connection has been reset by the peer causing the LAPF transmit queue to be purged.

Possible causes for this alarm are either congestion along the connection path or a software error.

Probable Cause

Communication subsystem failure

Type

Communications

Remedial action

If the cause is determined to be congestion, the Remote Server Agent should be re-engineered to decrease the combined traffic from its connections. This could involve configuring an additional RSA in the network and re-homing some of the connections to this new RSA.

If a software error is suspected, contact your local Nortel Networks technical support group.

7050 0004

Component	Severity	Status
Rsa/<instance>	warning	message

Legend

<instance> = a string value

Details

The Remote Server Agent has received a request for an unknown server. The unknown server type and the connection which received the request are reported in the alarm. The request is discarded.

This alarm is caused by a software error.

Probable Cause

Protocol error

Type

Communications

Remedial action

Contact your local Nortel Networks technical support group.

7052 0000

Component	Severity	Status
Lec/<instance>	major/clear	set/clear

Legend

<instance> = a decimal value

Details

When the status is *set*, the number of SVCs used by this LAN Emulation Client (LEC) is greater than 95% of the provisioned maximum.

If the maximum is reached, the system automatically releases the oldest 10%.

A *clear* is issued when the number of SVCs used drops below 85% of the provisioned maximum, after a *set* has been issued.

Probable Cause

Type

Remedial action

The LEC should be provisioned with a larger *maxDataSvcs* value.

7052 0001

Component	Severity	Status
Lec/<instance>	major/clear	set/clear

Legend

<instance> = a decimal value

Details

When the status is *set*, the number of LE ARP entries used by this LAN Emulation Client (LEC) is greater than 95% of the provisioned maximum.

If the maximum is reached, the system automatically releases the oldest 10%.

A *clear* is issued when the number of LE ARP entries used drops below 85% of the provisioned maximum, after a *set* has been issued.

Probable Cause

Type

Remedial action

The LEC should be provisioned with a larger *maxArpEntries* value.

7052 0002

Component	Severity	Status
Lec/<instance>	critical/clear	set/clear

Legend

<instance> = a decimal value

Details

When the status is *set*, the LAN Emulation Client (LEC) is unable to join the Emulated LAN (ELAN).

A *clear* is issued when the LEC is able to join the ELAN. The LEC will now be operational.

Probable Cause

Type

Remedial action

The LEC may be provisioned with incorrect values than those provided by the LAN Emulation Server (LES) or LAN Emulation Configuration Server (LECS). In this case, the LES or LECS should either be changed or the provisioning of the LEC should be changed.

The LEC may be unable to contact the LES or LECS. The physical connections should be checked and the LES and LECS should be checked to ensure that they are operational

The LEC may be unable to register with the Broadcast and Unknown Server (BUS). The BUS should be checked to ensure that it is operational and the physical connections should be checked.

The LEC will not be operational until this is resolved.

7053 0000

Component	Severity	Status
McsMgr	clear	set/clear

Details

This alarm is a hierarchical alarm used to clear all outstanding alarms for the *McsMgr* component and its subcomponents. This alarm is used when the *McsMgr* component is coming up or being deleted to clear any alarms that may be active and are no longer valid. Note that there is no corresponding set for this alarm.

Probable Cause

Underlying resource unavailable

Type

Processing

Remedial action

None.

7053 0002

Component	Severity	Status
McsMgr	critical	set/clear

Details

This alarm is *set* when a critical error has occurred in the provisioning of the *McsMgr* component. This includes situations were there are insufficient resources available to continue.

Probable Cause

Underlying resource unavailable

Type

Processing

Remedial action

Attempt to re-activate provisioning to determine if resource utilization has improved such that the *McsMgr* component may not become active. If this fails, the *McsMgr* component should either be provisioned on a new LP that has more memory available, or the services on the existing LP should be reduced to free up memory for the *McsMgr* component. Note this alarm will be cleared by the McsMgr hierarchical clear once the *McsMgr* component becomes active.

7053 0003

Component	Severity	Status
McsMgr	major	set/clear

Details

This alarm is *set* when the number of end points under the *McsMgr* component exceeds the limit specified by the *maxEps* attribute. No new end points will be allowed until the alarm is cleared

Probable Cause

At or near capacity

Type

Quality of service

Remedial action

This alarm is cleared either when the number of end points falls below the limit specified by the *maxEps* attribute or when the value of the *maxEps* attribute is increased.

7053 0004

Component	Severity	Status
McsMgr	minor	set/clear

Details

This alarm is *set* when the number of end points exceeds the value specified by *epAlarmThreshold* attribute.

Probable Cause

Threshold crossed

Type

Quality of service

Remedial action

This alarm is cleared when the number of end points falls below the value specified by the *epAlarmThreshold* attribute. The number of end points may be reduced or the value of the *epAlarmThreshold* attribute may be increased.

7053 0005

Component	Severity	Status
McsMgr	minor	message

Details

This alarm indicates that there was insufficient memory for the *McsMgr* component to bring up an end point.

Probable Cause

Underlying resource unavailable

Type

Processing

Remedial action

Attempt to reactivate the provisioning. If this fails again, either move the *McsMgr* component to a new LP with more available memory or reduce the number of end points.

7053 0006

Component	Severity	Status
McsMgr	minor	message

Details

This alarm indicates a provisioning error where an address prefix has been associated to more than one *Frf5EpG* component.

Probable Cause

Duplicate information

Type

Security

Remedial action

Correct the provisioning to remove the duplication of the *addressPrefix* attribute. This attribute is located under the component *McsMgr Frf5EpG Addr* component.

7053 0007

Component	Severity	Status
McsMgr	warning	set/clear

Details

This alarm occurs when the feature lists of the currently active MCS Manager (LP) and the LP trying to register as the candidate MCS Manager do not match.

This can happen in the following scenarios:

1. The active MCS Manager has feature dprsMcsEp and the candidate has feature frf5EndPoint.

2. The active MCS Manager has feature frf5EndPoint and the candidate has feature dprsMcsEp.

3. The active MCS Manager has both dprsMcsEp and frf5EndPoint and the candidate has either dprsMcsEp or frf5EndPoint.

In these scenarios, the registering LP is not allowed to become a candidate MCS manager unless the active MCS Manager goes down (or is locked out, etc.), in which case the registering LP (with a different feature list) is elected as the active MCS Manager and this alarm is set.

This alarm is cleared when the feature lists are updated to be the same.

Impact

These scenarios that cause the alarm to be set can lead to a service outage, since the candidate MCS Manager that takes over cannot support the same services that were supported by the previously active MCS Manager.

Probable Cause

Configuration error

Type

Processing

Remedial action

If possible, update the feature lists of the active and candidate MCS Managers so that they are the same.

7053 0008

Component	Severity	Status
McsMgr	major	message

Details

This alarm occurs when the feature lists of the currently active MCS Manager and the previously active MCS Manager do not match.

This can happen in the following scenarios:

1. The previously active MCS Manager has feature dprsMcsEp and the currently active MCS Manager has feature frf5EndPoint.

2. The previously active MCS Manager has feature frf5EndPoint and the currently active MCS Manager has feature dprsMcsEp.

3. The previously active MCS Manager has both dprsMcsEp and frf5EndPoint and the currently active MSC Manager has either dprsMcsEp or frf5EndPoint.

Impact

These scenarios can lead to a service outage, since the currently active MCS Manager cannot support the same services that were supported by the previously active MCS Manager.

Probable Cause

Configuration error

Type

Processing

Remedial action

If possible, update the feature lists of the previously active and currently active MCS Managers so that they are the same.

7053 0100

Component	Severity	Status
McsMgr Frf5EpG/<instance> Ep/<instance>	warning	message

Legend

<instance> = a decimal value

Details

This alarm indicates that an Frf5 End Point provisioned as ‘master’ received a call request from the ATM network.

Probable Cause

Configuration or customization error

Type

Processing

Remedial action

Verify the provisioning of the two side of the connection. One side should be master and the other should be slave.

7053 0101

Component	Severity	Status
McsMgr Frf5EpG/<instance> Ep/<instance>	warning	message

Legend

<instance> = a decimal value

Details

This alarm indicates that an Frf5 End Point received a call request with invalid Traffic Management parameters. This is probably caused by an invalid provisioning of the Transfer Priority under one of the Frf5 end points. This attribute is located under McsMgr Frf5EpG/<instance> Ep/<instance> Epd

Probable Cause

Configuration or customization error

Type

Processing

Remedial action

Modify the provisioning of the two Frf5 End Point so their transfer priority is mapped into the same ATM service category.

7053 0102

Component	Severity	Status
McsMgr Frf5EpG/<instance> Ep/<instance>	major	message

Legend

<instance> = a decimal value

Details

This alarm is issued when an FRF.5 end point attempts to call its own McsMgr component. This configuration is not supported.

Probable Cause

Configuration or customization error

Type

Processing

Remedial action

Reprovision the value of the *remoteAddress* attribute under the *McsMgr Frf5EpG Addr* component.

7053 0103

Component	Severity	Status
McsMgr Frf5EpG/<instance> Ep/<instance>	minor	message

Legend

<instance> = a decimal value

Details

This alarm indicates that an FRF.5 end point provisioned as a slave has received a call request from the ATM network when there was already a call in progress.

Probable Cause

Configuration or customization error

Type

Processing

Remedial action

Verify the provisioning at the master end of the connection. There can only be one master end point attempting to connect to a slave end point.

7053 0104

Component	Severity	Status
McsMgr Frf5EpG/<instance> Ep/<instance>	minor	message

Legend

<instance> = a decimal value

Details

This alarm indicates that an FRF.5 end point provisioned as a slave has received a call request from the ATM network, from a calling address not matching the *McsMgr Frf5EpG/<instance> Address remoteAddress* attribute value.

Probable Cause

Configuration or customization error

Type

Processing

Remedial action

Verify the provisioning at the master end of the connection, and/or the *McsMgr Frf5EpG/<instance Address remoteAddress* attribute value.

7053 0105

Component	Severity	Status
McsMgr Frf5EpG/<instance> Ep/<instance>	major	message

Legend

<instance> = a decimal value

Details

This alarm indicates that an Frf5 End Point was not capable of allocating a DLCI subconnection. This is typically caused by the exhaustion of subcontexts available on an ATM FP.

Probable Cause

Configuration or customization error

Type

Processing

Remedial action

Verify that the number of Dlci components under all McsMgr Frf5EpG Ep instances is within the supported limit as stated in the Engineering Guidelines for FR-ATM network interworking.

7053 0150

Component	Severity	Status
McsMgr Frf5EpG/<instance> Ep/<instance> LMI	critical/cleared	set/clear

Legend

<instance> = a decimal value

Details

This alarm is *set* when the number of Frf5 End Point Local Management Interface (LMI) procedure errors within the last *eventCount* events has exceeded the threshold *errorEventThreshold*. (Both eventCount and errorEventThreshold are provisionable attributes) In this situation, the local interface is declared insane.

A *clear* is issued after a fixed number (provisioning parameter) of correct message exchanges between the inter-operating LMI entities. Data transfer in all connections associated with the local DLCIs is resumed.

Probable Cause

Protocol error

Type

Communications

Remedial action

Verify that the other side of the interface has the LMI protocol enabled. Verify that the LMI parameters set on the other side are compatible with those on this side. Turn off the LMI protocol if the other side does not support the LMI protocol.

7053 020x

Component	Severity	Status
McsMgr Frf5EpG/<instance> Ep/<instance>	warning	message

Legend

<x> = a decimal digit (0 - 9)

<instance> = a decimal value

Details

This alarm occurs when the Frf5 End Point Local Management Interface (LMI) receives a report from the remote end point that a PVC (at the remote end point) has become inactive. Data transfer to the external network is suspended, for the reported connections associated with a local DLCI.

The PVCs that have just been reported inactive by the remote end point are listed in decimal format as part of the comment for this alarm.

Each 7053 020x alarm reports a maximum of 112 PVCs. If there are more than 112 PVCs on a single component it will become inactive. There may be multiple 7053 020x alarms generated. The value ‘x’ has an initial value of ‘0’ and it is incremented by one for each alarm.

Probable Cause

VC active

Type

Communications

Remedial action

Check the PVC connections listed in this alarm, in the remote end point that raised this alarm.

7053 0300

Component	Severity	Status
McsMgr	warning	message

Details

This alarm occurs when the forwarding table for the MCS Agent cannot be dynamically allocated into fast memory. Degraded performance will occur because forwarding table is in normal memory instead of fast memory.

Probable Cause

Performance degraded

Type

Quality of service

Remedial action

Verify that the dprsMcsAgent feature has been provisioned first in the sw lpt featureList of the given lp. Otherwise, the lp must be engineered to make more fast memory available.

7053 0301

Component	Severity	Status
McsMgr	major	message

Details

This alarm occurs when the forwarding table for the MCS Agent cannot add an MCS Ep.

Probable Cause

Software program error

Type

Processing

Remedial action

Contact Nortel Networks global support.

7053 0302

Component	Severity	Status
McsMgr	major	message

Details

This alarm occurs when a CRC check failure occurs on the MCS Agent forwarding table.

Probable Cause

Corrupt data

Type

Processing

Remedial action

No action is required as MCS forwarding will recover eventually. There may be a temporary loss and/or re-route of traffic along the DPRS MCS switched path. If this alarm persists, contact Nortel Networks global support.

7053 0400

Component	Severity	Status
McsMgr DprsEpG/<instance> Ep/<instance>	warning	message

Legend

<instance> = a decimal value

Details

This alarm occurs when intercept cannot be dynamically allocated in fast memory. The intercept is the software entity on the trunk card responsible for forwarding data packets onto the Frame Relay access card for a DPRS MCS Switched Path set up over a PORS Trunk. Degraded performance will occur because the intercept is in normal memory instead of fast memory.

Probable Cause

Performance degraded

Type

Processing

Remedial action

Ensure that the total number of DPRS MCS Ups provisioned and/or created dynamically at the node are at or below the recommended engineering limit. Ensure that valid feature combinations are supported on this transport FP. The Lp may have to be re-engineered, or additional components reprovisioned to make more fast memory available.

7053 0401

Component	Severity	Status
McsMgr DprsEpG/<instance> Ep/<instance>	warning	message

Legend

<instance> = a decimal value

Details

This alarm occurs when the intercept located on the transport card cannot obtain a local message block to send the statistics record to its corresponding Ep on the McsMgr card when the underlying PORS VC or ATM SPVC, established dynamically, is cleared either by the user or the network.

Statistics are polled from the intercept by the Ep at intervals equal to the Spooled Statistics poll duration or when a CAS display command is issued. Therefore, inability to send the statistics record when the transport connection is cleared translates to a loss of DPRS MCS Switched Path statistics for a maximum duration equal to the polling period. Frequent occurrences of this lead to statistics loss for multiple poll durations.

Probable Cause

Out of memory

Type

Processing

Remedial action

Verify that the total number of DPRS MCS Eps provisioned and/or created dynamically at the node are at or below the recommended engineering limit. Verify that valid feature combinations are supported on this transport FP. Frequent or prolonged occurrences of this condition indicate that either there is a system fault causing local message block exhaustion or re-engineering is required. Contact your local Nortel Networks technical support group, if necessary.

7053 0402

Component	Severity	Status
McsMgr DprsEpG/<instance> Ep/<instance>	minor	set/clear

Legend

<instance> = a decimal value

Details

This alarm is *set* when the CAC bandwidth usage percentage exceeds the minor alarm threshold percentage for this Ep. This value is provisioned on the originating Ep in the Cac Cacd component. There are thresholds for both directions (forward and reverse) of the switched path.

A *clear* is issued when the bandwidth usage percentage has dropped to ten percent below the provisioned threshold value.

Probable Cause

Threshold crossed

Type

Processing

Remedial action

This alarm informs the operator that a specific bandwidth usage percentage has been reached on the switched path. Re-engineering may be required if this bandwidth usage percentage is not intended to be reached. Contact your local Nortel Networks technical support group, if necessary.

7053 0403

Component	Severity	Status
McsMgr DprsEpG/<instance> Ep/<instance>	major	set/clear

Legend

<instance> = a decimal value

Details

This alarm is *set* when the CAC bandwidth usage percentage exceeds the major alarm threshold percentage for this Ep. This value is provisioned on the originating Ep in the Cac Cacd component. There are thresholds for both directions (forward and reverse) of the switched path.

A *clear* is issued when the bandwidth usage percentage has dropped to ten percent below the provisioned threshold value.

Probable Cause

Threshold crossed

Type

Processing

Remedial action

This alarm informs the operator that a specific bandwidth usage percentage has been reached on the switched path. Re-engineering may be required if this bandwidth usage percentage is not intended to be reached. Contact your local Nortel Networks technical support group, if necessary.

7053 0404

Component	Severity	Status
McsMgr DprsEpG/<instance> Ep/<instance>	critical	set/clear

Legend

<instance> = a decimal value

Details

This alarm is *set* when the MCS CAC bandwidth usage percentage exceeds the critical alarm threshold percentage for this Ep. This value is provisioned on the originating Ep in the Cac Cacd component. There are thresholds for both directions (forward and reverse) of the switched path.

A *clear* is issued when the bandwidth usage percentage has dropped to ten percent below the provisioned threshold value.

Probable Cause

Threshold crossed

Type

Processing

Remedial action

This alarm informs the operator that a specific bandwidth usage percentage has been reached on the switched path. Re-engineering may be required if this bandwidth usage percentage is not intended to be reached. Contact your local Nortel Networks technical support group, if necessary.

7053 0405

Component	Severity	Status
McsMgr DprsEpG/<instance> Ep/<instance>	warning	set/clear

Legend

<instance> = a decimal value

Details

This alarm is *set* when the Ep rejects a CAC request because it has already admitted the maximum number (512)of connections.

A *clear* is issued under the following conditions (condition must persist for more than 90 seconds):

- when the Ep has less than 512 connections admitted,
- when the Ep is locked, or
- when Cac is deleted from the Ep.

Probable Cause

Call establishment error

Type

Communications

Remedial action

Re-engineering is required to admit the frame relay connections that are being rejected. Contact your local Nortel Networks technical support group, if necessary.

7053 0406

Component	Severity	Status
McsMgr DprsEpG/<instance> Ep/<instance>	warning	message

Legend

<instance> = a decimal value

Details

This alarm is issued when there are more than 512 frame relay connections on a switched path after CAC has been provisioned on the Ep. This can occur because connections are always admitted onto the switched path if CAC has not yet been provisioned.

The Ep can only track and display 512 of the connections.

Probable Cause

At or near capacity

Type

Quality of service

Remedial action

This situation exists until the number of frame relay connections on the switched path falls below 512. Contact your local Nortel Networks technical support group, if necessary.

7054 0100

Component	Severity	Status
Shelf card/<instance>	major/cleared	set/clear

Legend

<instance> = 0 - 15

Details

Card is not connected to a sparing panel.

The FP has been unable to connect to the sparing panel either because the cables have been incorrectly connected or a cable fault or due to a problem with the sparing panel.

Sets the status to major.

A *clear* is issued when the FP successfully connects to the sparing panel, (cable fault fixed or connectivity resolved) or the provisioning has been changed so that the FP does not need to register, or if a switchover occurs and the FP comes up as the standby card.

Probable Cause

Configuration or customization error

Type

Equipment

Remedial action

Check the cable for faults or check the provisioning is correct and that the FP should be connected to this sparing panel. Check the connectivity of the cables. Check that there are no problems with the sparing panel itself.

7054 0101

Component	Severity	Status
Shelf card/<instance>	major/cleared	set/clear

Legend

<instance> = 0 - 15

Details

Card is connected to the wrong sparing panel.
HSM will not work with a 1ForN Sparing panel
if the sparingconnections are not set.

The FP has successfully connected to a sparing panel, but it is not the correct sparing panel either because the cables have been incorrectly connected or there is a provisioning error.

Sets the status to major.

> ***Note:*** The spare card and each main card sharing this spare card must all be connected to the same sparing panel. This alarm warns you if you are using a 1ForN sparing panel and the *sh ca sparingconnection* attribute is set to NotApplicable. Hitless software migration (HSM) does not work if the *sparingconnection* attributes are set to NotApplicable.

A *clear* is issued when the FP successfully connects to the correct sparing panel, (connectivity resolved) or the provisioning has been changed so that the error is resolved.

Probable Cause

Configuration or customization error

Type

Equipment

Remedial action

Check the provisioning is correct and that the FP is connected to the same sparing panel as its spare card. Check the connectivity of the cables.

7054 0102

Component	Severity	Status
Shelf card/<instance>	major/cleared	set/clear

Legend
<instance> = 0 - 15

Details
Card is connected to the wrong sparing panel port.

The card was connected to an incorrect port on the sparing panel.

NOTE: The card must be connected to the same sparing panel port for which it was provisioned.

Sets the status to major.

A *clear* is issued when the FP registers with the correct connection on the sparing panel.

Probable Cause
Configuration or customization error

Type
Equipment

Remedial action
Ensure the card is cabled to the same sparing panel port for which it is provisioned or change the provisioned sparing connection to match the sparing panel port for which it is cabled.

7054 0103

Component	Severity	Status
Shelf card/<instance>	major/cleared	set/clear

Legend

<instance> = 0 - 15

Details

Sparing panel not responding.

This alarm is used to indicate when an FP is connected to a sparing panel but the sparing panel is not responding. This can be due to a faulty cable connection, a firmware or hardware fault in the sparing panel itself.

This alarm will be raised when either of the following occur:

1. During sparing panel monitoring, a sparing panel was detected, but failed to provide any information to the FP.

2. The sparing panel did not provide an acknowledgment of an FP's attempt to 'grab' a relay.

Sets the status to "major".

A *clear* is issued when the FP receives information from the sparing panel or gets an acknowledgment of the FP's attempt to 'grab' a relay.

Probable Cause

Configuration or customization error

Type

Equipment

Remedial action

Check the sparing panel to ensure that it is working correctly. Check the cable connectivity between this shelf card and the sparing panel.

7054 0104

Component	Severity	Status
Shelf card/<instance>	major/cleared	set/clear

Legend
<instance> = 0 - 15

Details
Spare card is in use.

A main FP had failed and the spare FP took over its failure. Sets the status to “major”.

A *clear* is issued when the spare FP is released.

Probable Cause
Configuration or customization error

Type
Equipment

Remedial action
Replace the main FP if failure is due to a hardware problem. A switchover must be issued to release the spare FP.

7054 0105

Component	Severity	Status
Shelf card/<instance>	major/cleared	set/clear

Legend
<instance> = 0 - 15

Details
Spare card is unavailable.

The spare card went down or was removed from the shelf. This breaks the sparing functionality of all LPs sharing this spare card.

Sets the status to “major”.

A *clear* is issued when the spare FP comes back up or is re-inserted in the shelf.

Probable Cause
Configuration or customization error

Type
Equipment

Remedial action
Re-insert the spare card in the shelf if it was removed. This can also be resolved by provisioning a new spare card. Replace the spare card if it does not come back up.

7056 0001

Component	Severity	Status
Lp/<x> Vsp	major	set/clear

Legend

<x> = 0 - 15

Details

There has been a severe failure on the VSP card. This may be as a result of the failure of a hardware device on the card which affects the transportation of all traffic. Any traffic still flowing through the card cannot be guaranteed to be reliable.

Probable Cause

Equipment malfunction

Type

Equipment

Remedial action

Restart the card. If a card failure is still raised, a new VSP card is required.

7056 0002

Component	Severity	Status
Lp/<x> Vsp PModule/<y>	major	set/clear

Legend

<x> = 0 - 15

<y> = 1 - 12

Details

The physical module on the VSP card does not match the provisioned *moduleType* in the corresponding *PModule* component.

Probable Cause

Procedural error

Type

Operator

Remedial action

Reprovision the *moduleType* attribute of *PModule* to match the module present on the VSP card and activate provisioning. If the problem persists and *PModule* has been provisioned correctly, a new hardware module is required

7056 0003

Component	Severity	Status
Lp/<x> Vsp PModule/<y> PBlock/<z>	critical	set/clear

Legend

<x> = x

<y> = 1 - 12

<z> = 1 - 2

Details

There has been a failure of a hardware component on the VSP card during diagnostic tests.

Probable Cause

Equipment malfunction

Type

Equipment

Remedial action

Re-run the diagnostic check by unlocking the *Vsp* component. If this fails, reboot the card. If a failure is still raised, a new hardware module is required.

7056 0004

Component	Severity	Status
Lp/<x> Vsp PModule/<y> PBlock/<z>	critical	message

Legend

<x> = 0 - 15

<y> = 1 - 12

<z> = 1 - 2

Details

This alarm is issued when there is a failure of a component on the VSP card during a provisioning activity.

The comment data includes information to identify the specific hardware module which is defective.

Probable Cause

Equipment malfunction

Type

Equipment

Remedial action

Reboot the card. If a failure is still raised, a new hardware module is required.

7056 0500

Component	Severity	Status
Lp/<x> Vsp GigE/<y>	major/cleared	set/clear

Legend

<x> = 0 - 15

<y> = 0 - 1

Details

If the status is *set*, the port has lost synchronization with the Gigabit Ethernet signal on the incoming line. Declaration of a Loss of Synchronization failure clears any existing Auto-negotiation or Remote Link Failure alarms.

If the status is *clear*, synchronization has been achieved. Clearing of the alarm can be delayed by up to 10 seconds if an intermittent fault is detected.

Probable Cause

Loss of signal or loss of frame

Type

Communications

Remedial action

Check the cabling between this port’s receiver and the far end transmitter.

7056 0501

Component	Severity	Status
Lp/<x> Vsp GigE/<y>	major/cleared	set/clear

Legend

<x> = 0 - 15

<y> = 0 - 1

Details

If the status is *set*, Auto-Negotiation is in progress with the link partner. Among the possible causes of the condition persisting are:

- The link partner does not support Auto-Negotiation.

- A bi-directional path to the link partner does not exist.

A *clear* is issued when Auto-Negotiation has been successful or synchronization is lost. Clearing of the alarm can be delayed by up to 10 seconds if an intermittent fault is detected.

Probable Cause

Cable fault at link partner

Type

Communications

Remedial action

Ensure the link partner has Auto-Negotiation enabled.

Check the cabling between the local port and the link partner.

7056 0502

Component	Severity	Status
Lp/<x> Vsp GigE/<y>	major/cleared	set/clear

Legend

<x> = 0 - 15

<y> = 0 - 1

Details

If the status is *set*, the link partner has signaled a remote fault indication.

If the status is *clear*, the link partner has signaled that the remote fault indication has cleared or synchronization is lost. Clearing of the alarm can be delayed by up to 10 seconds if an intermittent fault is detected.

Probable Cause

Link partner is offline or link failure

Type

Communications

Remedial action

Check compatibility of link partner. Check link partner documentation to determine reason for remote fault indication.

7056 1100

Component	Severity	Status
Nsta/<x> Conn/<y> Brag/<z> Ccst	major	set/clear

Legend

<x> = 0 - 15999

<y> = 0 - 47

<z> = 0 - 159999

Details

This signalling link layer alarm is raised when layer 2 of the CCS stream has been down for two consecutive seconds. It will be cleared when layer 2 has been up for ten consecutive seconds. When this alarm is set, all B channels will be assumed to be idle and they will not be transported over the AAL2 link. This alarm will be raised only when signalling monitoring is enabled.

Probable Cause

Type

Remedial action

Look at the *Ccst* component's operational attributes to check whether HDLC frames are received error free and transmitted over the ATM link. Similarly, check the reverse direction as well. If ATM cells or packets are transported over the ATM connection without any errors, check the status of the link layer in the narrowband device connected to the PVG service interface (DS1 TDM interface).

7056 1101

Component	Severity	Status
Nsta/<x> Conn/<y> Brag/<z> Ccst	warning	message

Legend

<x> = 0 - 15999

<y> = 0 - 47

<z> = 0 - 159999

Details

This signalling alarm is issued when an unexpected or an unsupported feature is indicated or requested through the CCS stream. The comment data will identify the feature.

Probable Cause

Type

Remedial action

Check the external devices using the narrowband services trunk for the identified feature. The feature identified should be removed from the external device's service interface as a facility.

7056 1200

Component	Severity	Status
Nsta/<x> Vgs	minor	set/clear

Legend

<x> = 0 - 15999

Details

If the status is *set*, the *Nsta/<num1> Vgs* component has detected that the count of associated disabled AtmTCon connections has changed from zero to a non-zero value. This change in state signifies that at least one of the AtmTCon components associated with this *Nsta/<num1> Vgs* component has become disabled.

A *clear* is issued when the count of disabled AtmTCon components associated with this *Nsta/<num1> Vgs* component returns to zero.

Probable Cause

Type

Remedial action

Display all of the AtmTCon components associated with the *Nsta/<num1> Vgs* component to determine which ones are troubled.

See 241-5701-715 *Passport 7400, 15000, 20000 ATM Monitoring and Troubleshooting Guide* for details on troubleshooting ATM connections.

7056 1201

Component	Severity	Status
Nsta/<x> Vgs IpMConn/<y>	major	set/clear

Legend

<x> = 0 - 15999

<y> = 0 - 21

Details

If the status is *set*, the *Nsta/<num1> Vgs IpMConn/<num2>* component has become disabled and can no longer carry any traffic.

A *clear* is issued when the *Nsta/<num1> Vgs IpMConn/<num2>* component becomes enabled and can carry traffic.

Probable Cause

Type

Remedial action

Each IpMConn is connected to the ATM network via a VCC component under a particular AtmIf component on an ATM FP. Check the status of these components to ensure they are functioning appropriately.

See 241-5701-715 *Passport 7400, 15000, 20000 ATM Monitoring and Troubleshooting Guide* for details on troubleshooting ATM connections.

7056 1202

Component	Severity	Status
Nsta/<x> Vgs Ctrl/<y>	major	set/clear

Legend

<x> = 0 - 15999

<y> = mg or sg

Details

If the status is *set*, the *Nsta/<num1> Vgs Ctrl/<num2>* component has become disabled and can no longer carry any traffic.

A *clear* is issued when the *Nsta/<num1> Vgs Ctrl/<num2>* becomes enabled and can carry traffic.

Probable Cause

Type

Remedial action

Each *Ctrl* is connected to the ATM network via a VCC component under a particular AtmIf component on an ATM FP. Check the status of these component to ensure they are functioning appropriately.

See 241-5701-715 *Passport 7400, 15000, 20000 ATM Monitoring and Troubleshooting Guide* for details on troubleshooting ATM connections.

7056 1203

Component	Severity	Status
Nsta/<w> Vgs Ctrl/<x> Aap	major	set/clear
Nsta/<w> Vgs Ctrl/<x> SpvcAp		
Nsta/<w> Vgs IpMConn/<y> Aap		
Nsta/<w> Vgs IpMConn/<y> SpvcAp		
Nsta/<w> Vgs AtmTConn/<z> Aap		
Nsta/<w> Vgs AtmTConn/<z> SpvcAp		

Legend

<w> = 0 - 15999

<x> = 1 - 2

<y> = 0 -21

<z> = 1 - 1024

Details

When an *Aap* or *SpvcAp* subcomponent has initiated a number of consecutive unsuccessful call setup attempts equal to the value of the provisioned retryLimit, no further setups are attempted and this alarm is raised.

Probable Cause

Type

Remedial action

Check the *lastSetupFailureCause* in the *Aap* or *SpvcAp* subcomponent management action, such as reprovisioning.

When the appropriate management action has been taken, issue a restart against the relevant *Aap* or *SpvcAp* subcomponent to restart the automatic connection procedure.

7056 1204

Component	Severity	Status
Nsta/<x> Vgs	minor	set/clear

Legend

<x> = 0 - 15999

Details

If the status is *set*, the *Nsta Vgs* component in question has detected that the connectivity to the MF remote signalling device has been lost. A clear is issued when the connectivity is restored.

Connectivity can be lost for the following reasons. Either the control connection that uses an ATM VCC to connect to the nearest IP router is disabled, or there is a connectivity problem somewhere in the IP network that prevents the PVG from communicating with the MF remote signalling device.

Probable Cause

Type

Remedial action

Display the ControlConnection subcomponent of the Vgs to determine whether or not the associated ATM connection is troubled. If it is troubled then troubleshoot the problem in the usual manner (see 241-5701-715 *Passport 7400, 15000, 20000 ATM Monitoring and Troubleshooting Guide* for details on troubleshooting ATM connections).

If the ATM connection is not troubled then there will be an IP connectivity problem within the network between the PVG and the MF remote signalling device.

7056 1208

Component	Severity	Status
Nsta/<x> Vgs LocalAnnouncements	minor	set/clear

Legend

<x> = 0 - 15999

Details

When the status is *set*, the *Nsta Vgs LocalAnnouncements* component in question has detected that the configured announcement file set is missing, too large, incompatible with the Announcement feature, or that the Announcement feature does not have a valid announcement file loaded.

When the status is *clear*, the component has detected that the currently configured announcement file set is present, of the correct size, is compatible with the Announcement feature, and a valid announcement file (not necessarily the latest configured one) is present and active in the FP.

Probable Cause

Type

Remedial action

Check attribute *Nsta Vgs LocalAnnouncements fileTransferStatus*.

If this attribute has value “missing,” ensure both file types (.ind and .aud) with the configured name are present in the configured location. Update the configured filename or rename or copy files to the correct location, as appropriate. Transfer is automatic.

If this attribute has value “fileTooLong,” reload the announcement files with a set with a combined length of <16MB. Re-export the new announcement fileset from UAS APS as required. Transfer is automatic.

If this attribute has value “fileError,” ensure both file types (.ind and .aud) are compatible with the file formats defined in this document. Re-export the new announcement fileset from UAS APS as required. Transfer is automatic.

If this attribute has value “inProgress,” check attribute *Nsta Vgs LocalAnnouncements currentFileName*. If this attribute returns a null string, wait. This alarm should clear in approximately 1 (one) minute under quiescent conditions. On a heavily loaded system, however, clearing may take longer.

If this attribute has value “cpNotResponding,” check that the CP disks are not locked. If they are not locked, the alarm should clear after a period of time.

7056 1209

Component	Severity	Status
Lp/<x> Vsp PModule/<y>	minor	set/clear

Legend

<x> = 0 - 15

<y> = 1 - 12

Details

If the status is *set*, the SSM, as indicated by component *Lp Vsp Pmod*, has undergone a failure as detected by the FP. Reset was tried once. If reset fails, or if it is apparently successful but there is a failure of the SSM again within the hour, the VSP FP will be reset. This may cause VSP protection switch.

If the status is *clear*, the SSM is functional. The functionality of individual tasks carried out by the SSM may be indicated by specific alarms associated with feature dependent components.

Probable Cause

Equipment malfunction

Type

Equipment

Remedial action

None. Either this is alarm will reset (within a minute), and full recovery has occurred, or the VSP will reset. At this point, the Pmod alarm will reset. This prior indication of a Pmod alarm may be used to indicate the reason for the VSP reset.

7056 1210

Component	Severity	Status
Nsta/<x> Vgs Brag/<y> Q921/<z>	major	set/clear

Legend

<x> = 0 - 15999

<y> = 0- 15999

<z> = 1- 31

Details

If the status is *set*, there has been a layer 2 failure of the PRI D-channel link. A *clear* is issued when the D-channel layer 2 failure has cleared.

Probable Cause

Type

Remedial action

Check cabling.

Check for transmission problems; for example, error bursts, slips, etc.

Check for disabling of the D-channel by an operator at the PRI-controlled device.

7056 1211

Component	Severity	Status
Nsta/<x> Vgs Iua	major	set/clear

Legend

<x> = 0 - 15999

Details

If the status is *set*, the SG is fully operational (i.e. there are no internal errors) but all the backhaul links between the SG and any MGCs are down.

A *clear* is issued when at least one of the backhaul links between the SG and an MGC has moved to the *up* or *active* state.

Probable Cause

Type

Remedial action

The operator can monitor the *Nsta/x Vgs Control/sg SctpPort/z SctpLink/w* components to determine the status of the SCTP links.

7056 1212

Component	Severity	Status
Nsta/<x> Vgs Iua	warning	message

Legend

<x> = 0 - 15999

Details

This message alarm is issued when a switchover between MGCs occurs (i.e. a standby MGC takes over from a primary). This may occur as a consequence of a failure condition or an operator initiated action, such as taking an MGC out of service.

Probable Cause

Type

Remedial action

The operator can examine the *Nsta/x Vgs Iua Asp/y* component to determine the status of the associated ASPs. This will indicate which MGC has gone down.

The operator can monitor the *Nsta/x Vgs Control/y SctpPort/z SctpLink/w* component to determine the status of the STCP links.

7056 1213

Component	Severity	Status
Nsta/<x> Vgs Brag/<y> V5Link LapV5/<z>	major	set/clear

Legend

<x> = 0 - 15999

<y> = 0 - 127

<z> = 15, 16, or 31

Details

If the status is *set*, there has been a layer 2 failure of the V5.2 C-channel link. A *clear* is issued when the C-channel layer 2 failure has cleared.

Probable Cause

Type

Remedial action

Check cabling.

Check for transmission problems; for example, error bursts, slips, etc.

Check for disabling of the C-channel by an operator at the V5.2-controlled device.

7056 1214

Component	Severity	Status
Lp/<x> Vsp PModule/<y>	major	message

Legend

<x> = 0 - 15

<y> = 1- 24

Details

For equipment protection or software migration to be hitless, the active VSP and the standby or migration VSP must remain synchronized. The alarm indicates that a problem has occurred when journaling data in order to keep the physical modules (as represented by *Lp Vsp PModule*) on the two cards synchronized.

There are a number of reasons for this alarm and the alarm comment displays more information about the cause of the alarm.

The alarm indicates a problem in communications between the two cards, such as data corruption or a protocol violation.

If the alarm comment indicates a ‘Data Restore Failure’, there may be a resource mismatch between the two VSPs, possibly caused by missing or failed physical modules on the standby or migration card. The ‘Data Restore Failure’ can also occur if PVCs are provisioned between the VSP and corresponding ATM card, since they are not supported for carrier grade.

Probable Cause

Communication protocol error, Underlying resource unavailable

Type

Communications, Processing

Remedial action

In an equipment protection scenario, the standby VSP card is usually restarted in an attempt to clear the problem. The exception to this is when the alarm raises a ‘Data Restore Failure’, in which case no action is taken. A switchover after a ‘Data Restore Failure’ may result in calls being dropped.

If the alarm occurs during a software migration, the migration is paused, at which point the options are to either abort migration or continue with it. Continuing with migration may result in calls being dropped.

7056 1215

Component	Severity	Status
Nsta/<x> Vgs BragS/<y>	major	message

Legend

<x> = 0 - 15999

<y> = 0 - 15

Details

For equipment protection or software migration to be hitless, the active VSP and the standby or migration VSP must remain synchronized. The alarm indicates that a problem has occurred when journaling data in order to keep the two cards synchronized. Resources have been allocated on the active VSP but the corresponding resources are not available on the standby or migration VSP.

The most likely reason for this alarm is missing or failed physical modules (as represented by *Lp Vsp PModule*) on the standby or migration VSP.

If this alarm is raised, alarm 7056 1214 may be seen if an attempt is made to set up a call that makes use of the resources that caused this alarm.

Probable Cause

Underlying resource unavailable

Type

Processing

Remedial action

In an equipment protection scenario, no action is taken. A switchover may result in calls being dropped.

If the alarm occurs during a software migration, the migration is paused, at which point the options are to either abort migration or continue with it. Continuing with migration may result in calls being dropped.

In both cases, some or all of the aal1Ces components that use the BragS become disabled over switchover. Where an aal1Ces component becomes disabled, any calls that are associated with that aal1Ces are dropped. Where possible, the aal1Ces is re-established after the switchover has completed.

7056 1216

Component	Severity	Status
Nsta/<x> Vgs	warning	set

Legend

<x> = 0 - 15999

Details

A Virtual Router Access Point has been provisioned on a VSP2 card equipped with a PQC1 type queue controller. This alarm does not apply to any other type of VSP card. A Virtual Router Access Point can be provisioned as a subcomponent of *Nsta Vgs IpMConn*, *Nsta Vgs Ctrl/mg*, *Nsta Vgs/Ctrl/sg*, or *Nsta Vgs DbgAccess*.

When a *VrAp* component has been provisioned on a VSP2 card equipped with a PQC1 queue controller, IP traffic service level differentiation is ignored. This means that features like IP CoS and DiffServ have no effect and all IP traffic on the card is routed with equal priority.

Probable Cause

Configuration error

Type

Processing

Remedial action

None required unless IP traffic service differentiation is needed. If this is the case, the VSP2 card can be replaced with a PQC2-based VSP2 card, a VSP3 card, or higher.

7056 1217

Component	Severity	Status
Nsta/<x> Vgs Tag/<y>	critical	set/clear

Legend

<x> = 0 - 15999

<y> = 0 - 16777215

Details

The processing resources required for the Tag are insufficient. The Tag remains disabled and the alarm in effect until either the Tag no longer requests resources or more resources are made available.

Probable Cause

The card is running at a reduced resource capacity.

Type

Remedial action

Increase the card resource capacity or decrease the Tag provisioned numbers.

7057 0001

Component	Severity	Status
DcmeLink/<instance>	major/cleared	set/clear

Legend

<instance> = instance of the DcmeLink (1-14)

Details

If the status is set, the number of rejected speech calls has reached a predefined threshold over a predefined time interval. The threshold value and the time interval are provisionable attributes under the corresponding *Dcme* component.

A clear is issued when the number of rejected speech calls drops below the threshold over the subsequent time interval.

Probable Cause

Threshold crossed

Type

Quality of service

Remedial action

A large number of rejected speech calls indicates that there were no network resources available to handle these calls. This may be due to network congestion, failure of network resources, or misconfiguration of the *preestablishedConnections* attribute under the corresponding *Dcme* component.

Verify the availability of network resources. The network may require re-engineering to handle higher traffic loads.

If network resources are available and the alarm is not cleared, the value of the *preestablishedConnections* attribute is too low for the actual call rate received from the ISC equipment.

If you set the *speechAlarmThreshold* attribute to 0, this alarm will not be generated.

7057 0002

Component	Severity	Status
DcmeLink/<instance>	major/cleared	set/clear

Legend

<instance> = instance of the DcmeLink (1-14)

Details

If the status is set, the number of rejected 3.1 kHz calls has reached a predefined threshold within a predefined time interval. The threshold value and the time interval are provisionable attributes under the corresponding *Dcme* component.

A clear is issued when the number of rejected 3.1 kHz calls drops below the threshold in the subsequent time interval.

Probable Cause

Threshold crossed

Type

Quality of service

Remedial action

A large number of rejected 3.1 kHz calls indicates that there were no network resources available to handle these calls. This may be due to network congestion, failure of network resources, or misconfiguration of the *preestablishedConnections* attribute under the corresponding *Dcme* component.

Verify the availability of network resources. The network may require re-engineering to handle higher traffic loads.

If network resources are available and the alarm is not cleared, the value of the *preestablishedConnections* attribute is too low for the actual call rate received from the ISC equipment.

If you set the *3kHzAlarmThreshold* attribute to 0, this alarm will not be generated.

7057 0003

Component	Severity	Status
DcmeLink/<instance>	major/cleared	set/clear

Legend

<instance> = instance of the DcmeLink (1-14)

Details

If the status is set, the number of rejected 64 Kbits/s calls has reached a predefined threshold over a predefined time interval. The threshold value and the time interval are provisionable attributes of the corresponding *Dcme* component.

A clear is issued when the number of rejected 64 Kbits/s calls drops below the threshold in the subsequent time interval.

Probable Cause

Threshold crossed

Type

Quality of service

Remedial action

A large number of rejected 64 Kbits/s calls indicates that there were no network resources available to handle these calls. This may be due to network congestion or failure of network resources.

Verify the availability of network resources. The network may require re-engineering to handle higher traffic loads.

If you set the *unrestricted64kAlarmThreshold* attribute to 0, this alarm will not be generated.

7057 0004

Component	Severity	Status
DcmeLink/<instance>	critical/cleared	set/clear

Legend

<instance> = instance of the DcmeLink (1-14)

Details

If the status is set, the DcmeLink negotiation with the far end *DcmeLink* component has failed.

Either the remote and local profile attributes are different or the DNAs are incorrect.

A clear is issued when the negotiation with the far end is successful.

Probable Cause

Version mismatch

Type

Communications

Remedial action

Verify the profile attributes values and the DNAs at the local and the remote end.

7057 0005

Component	Severity	Status
DcmeLink/<instance>	minor	message

Legend

<instance> = instance of the DcmeLink (1-14)

Details

This message indicates that an attempt to lock the *DcmeLink* component was unsuccessful, because the *vsType* attribute of at least one of the *Vs* subcomponents was provisioned to permanent64kVs.

Locking of this DcmeLink disables all of the *Vs* subcomponents, including the permanent64kVs type. By definition, this type of *Vs* component is permanent and it should not be disabled accidentally.

If you need to lock the *DcmeLink* component after the warning is issued, follow the steps described in the Remedial action section.

Probable Cause

Procedural error

Type

Operator

Remedial action

Disable all *Vs* components with *vsType* of *permanent64kVs* through the LOCK DcmeLink/<instance> Vs/<vsInstance>, then lock the *DcmeLink* component through the LOCK DcmeLink/<instance> command.

7058 0001

Component	Severity	Status
Hg/<num1>	warning/cleared	set/clear

Legend

<num1> = the hunt group instance (1-65535)

Details

If the status is *set*, this alarm indicates that the hunt group received an availability update from a service that was not configured as a member of the hunt group. The availability update is discarded and the *badPackets* attribute is incremented.

This occurs due to a provisioning inconsistency between the hunt group and the service. Either the hunt group is missing this service as a member; or the service is reporting availability to the wrong hunt group.

A *clear* is issued after a provisioning change is made to the *HuntGroupMember* components of the hunt group.

Probable Cause

Configuration or customization error

Type

Processing

Remedial action

Use the address reported in the alarm to identify the service reporting the availability update and determine if this service should be a member of the hunt group. If it should, add the member to the hunt group. If not, correct or delete the *HuntGroupAddress* component of the service.

A manual clear of this alarm is required if the provisioning is corrected on the service and not on the hunt group.

7059 0000

Component	Severity	Status
Vr/<string> Ip Nhrp	major/cleared	set/clear

Legend

<string> = name of the virtual router

Details

When the status is *set*, the number of *ResCacheEntry* entries used by this *Nhrp* component is greater than 95% of the provisioned maximum.

If the maximum number of entries is reached, the system automatically releases the oldest 10% of the entries.

A *clear* is issued when the number of *ResCacheEntry* entries used drops below 85% of the provisioned maximum, after a *set* has been issued.

Probable Cause

Type

Remedial action

Provision the *Nhrp* component with a larger *maxResCacheEntries* value.

7060 1000

Component	Severity	Status
Lp/<x> Eng Fcrc	major	set

Legend

<x> = 0 - 15

Details

IP routes/subconnections overbookings

The number of IP routing entries and/or subconnections has exhausted the amount of memory available. Since the *Lp/<instance> Eng Fcrc Pqc Ov* attribute *ipRoutesPoolCapacity* and the *LP/<instance> Eng Fcrc Ov* attribute *subConnectionPoolCapacity* share the same pool of memory, it is not always possible to guarantee the maximum value of both of these attributes. The alarm indicates the actual number of subconnections and/or IP routes allocated.

Probable Cause

Protocol error

Type

Communications

Remedial action

Decrease the number of IP routing entries in the *Lp/<instance> Eng Fcrc Pqc Ov* attribute *ipRoutesPoolCapacity* and/or the number of subconnections in the *Lp/<instance> Eng Fcrc Ov* attribute *subConnectionPoolCapacity*.

Warning: This causes the cards associated with the LP to reset.

7060 1100

Component	Severity	Status
Lp/<x> Eng Arc Aqm/<y>	warning/cleared	set/clear

Legend

<x> = 0 - 15

<y> = 0 - 3

Details

rxCellMemoryAvailable resources reaching a low level.

If the status is set, the available egress cell-blocks from the logical processor's specified AQM have fallen below 20% of total egress cell-blocks. Under this condition, traffic flowing across this AQM on this FP may encounter high queueing delays.

When this condition is detected, lower priority traffic is discarded first. If congestion persists, higher priority traffic is discarded. This continues until available egress cell-blocks for the logical processor's AQM have increased above 25% of the total egress cell-blocks. A clear is issued automatically at this point. A filtering mechanism is implemented such that a set/clear is issued by one minute.

Probable Cause

Protocol error

Type

Communications

Remedial action

Frequent or prolonged occurrences of this condition indicate that re-engineering is required to balance the flow of traffic through this card to reduce the amount of traffic and the length of queues.

Lower the connection pool capacity for this AQM.

Warning: This causes the card associated with the LP to reset.

7060 1200

Component	Severity	Status
Lp/<x> Eng Arc Ov	warning	message

Legend

<x> = 0 - 15

Details

The provisioned connection capacity, the sum of the *connectionPoolCapacity*, *protectedConnectionPoolCapacity*, *multicastBranchesCapacity* and *protectedMcastBranchesCapacity* attributes, for the *Arc Ov* component is higher than what this particular card can handle.

No serious damage occurs on the card, however the operational values do not reflect provisioned values.

Probable Cause

Underlying resource unavailable

Type

Processing

Remedial action

Determine the total connection capacity the card can support by checking the Arc component and reduce the provisioned connection capacity in the Arc Ov component accordingly.

Warning: This causes the card associated with the LP to reset.

7060 1201

Component	Severity	Status
Lp/<x> Eng Arc	warning/cleared	set/clear

Legend

<x> = 1 - 15

Details

perVcQueueAvailable resources reaching a low level.

If the status is *set*, the available perVc queues from the specified logical processor have fallen below 10% of the 32,000 total. If the available perVc queues reaches 0, ATM perVc queued connections fail to establish.

A *clear* is issued when at least 25% of the perVc queues become available. A filtering mechanism is implemented such that a set/clear alarm pair can be issued no more than one per minute.

Probable Cause

Threshold crossed

Type

Quality of service

Remedial action

No more than 32,000 connections can request a perVc queue resource. The remaining connections must use common queuing.

Whether a connection requires a perVc queue resource is determined by the connection's ATM service category provisioning. A perVc queue resource is required under either of the following conditions:

- when the ATM service category has the *trafficShaping* attribute provisioned as either enabled or inverseUpc
- when the ATM service category has the *unshapedTransmitQueueing* attribute provisioned as perVc

To enable common queuing on an ATM service category, set the *trafficShaping* attribute to disabled and set the *unshapedTransmitQueueing* attribute to common.

Warning: Changing ATM service category provisioning causes the ATM interface to reset.

7060 1300

Component	Severity	Status
Lp/<x> Eng	critical/major/minor/cleared	set/clear

Legend

<x> = 1 - 15

Details

The status is *set* with critical severity when hardware forwarding resource usage for incoming IP/MPLS connections is at 99% of maximum. It is cleared when hardware forwarding resource usage drops to 98% of maximum.

The status is *set* with major severity when hardware forwarding resource usage for incoming IP/MPLS connections is at 95% of maximum. It is cleared when hardware forwarding resource usage drops to 94% of maximum.

The status is *set* with minor severity when hardware forwarding resource usage for incoming IP/MPLS connections is at 85% of maximum. It is cleared when hardware forwarding resource usage drops to 84% of maximum.

Probable Cause

Resource at or near capacity

Type

Quality of service

Remedial action

Contact first level support for help with re-engineering the network to allow the resource usage to move below a critical level. Hardware forwarding performance is degraded when the hardware forwarding resource usage reaches the maximum value.

7060 1400

Component	Severity	Status
Lp/<x> Eng	critical/major/minor/cleared	set/clear

Legend

<x> = 1 - 15

Details

The status is *set* with critical severity when hardware forwarding resource usage for outgoing IP/MPLS connections is at 99% of maximum. It is cleared when hardware forwarding resource usage drops to 98% of maximum.

The status is *set* with major severity when hardware forwarding resource usage for outgoing IP/MPLS connections is at 95% of maximum. It is cleared when hardware forwarding resource usage drops to 94% of maximum.

The status is *set* with minor severity when hardware forwarding resource usage for outgoing IP/MPLS connections is at 85% of maximum. It is cleared when hardware forwarding resource usage drops to 84% of maximum.

Probable Cause

Resource at or near capacity

Type

Quality of service

Remedial action

Contact first level support for help with re-engineering the network to allow the resource usage to move below a critical level. Hardware forwarding performance is degraded when the hardware forwarding resource usage reaches the maximum value.

7060 1500

Component	Severity	Status
Lp/<x> Eng	warning	message

Legend

<x> = 1 - 15

Details

Rule Set resources for VRIs have been exhausted. Some protocol ports with IP classification may have reduced throughput performance.

Probable Cause

Resource exhaustion

Type

Quality of service

Remedial action

Frequent occurrences of this alarm indicate that a number of filters (component *Vr Ip Filter*), diffServ interfaces (component *Vr Ip DiffServ*), and/or policy groups (component *Vr Ip Pg*) with policies exceeds the IP classification hardware resources available on this PQC FP. Any of the filters, diffServ interfaces, or policy groups can be assigned to either a protocol port or a virtual router.

Contact your local Nortel Networks technical support group for help with re-engineering the network if necessary.

7060 1600

Component	Severity	Status
Lp/<x> Eng	warning	message

Legend

<x> = 1 - 15

Details

Rule Set resources for VROs have been exhausted. Some protocol ports assigned with IP DSCP marking may not mark IP packets with the expected DSCP.

Probable Cause

Resource exhaustion

Type

Quality of service

Remedial action

Frequent occurrences of this alarm indicate that a number of filters (component *Vr Ip Filter*), diffServ interfaces (component *Vr Ip DiffServ*), and/or policy groups (component *Vr Ip Pg*) exceeds the IP classification hardware resources available on this PQC FP. Any of the filters, diffServ interfaces, or policy groups can be assigned to either a protocol port or a virtual router.

Contact your local Nortel Networks technical support group for help with re-engineering the network if necessary.

7061 0001

Component	Severity	Status
Vr/<string> Ip Spd/<spd_name> Pol/<pol_id> Sa/<ip_addr,esp,spi>	major	message

Legend

<string> = name of the virtual router

<spd_name> = name of the security policy database

<pol_id> = instance number of the Policy component

<ip_addr,esp,spi> = IP address of the peer with which this SecurityAssociation component is established, the security protocol (ESP), and the Security Parameter Index (SPI) value

Details

This alarm is issued when a security violation is detected. Security violations include mismatch against the security policy and authentication and decryption failures.

The packet generating the alarm is discarded. Until remedial action is taken, packets continue to be discarded.

Probable Cause

Intrusion or misconfiguration.

Type

Security

Remedial action

Verify that the configuration is correct between both peers or verify the packet data contained in the alarm message to determine the origin of the intrusion.

7062 0001

Component	Severity	Status
Lp/<num1> Pcusp	major	set/clear

Legend

<num1> = 0 - 15

Details

There has been a severe failure on the PCUSP card. This may be as a result of the failure of a hardware device on the card which affects the transportation of all traffic. Any traffic still flowing through the card cannot be guaranteed to be reliable.

Probable Cause

Type

Remedial action

Restart the card. If a card failure is still raised, a new PCUSP card is required.

7062 0002

Component	Severity	Status
Lp/<num1> Pcusp PModule/<num2>	major	set/clear

Legend

<num1> = 0 - 15
<num2> = 1 - 12

Details

The physical module on the PCUSP card does not match the provisioned *moduleType* in the corresponding *PModule* component.

Probable Cause

Type

Remedial action

Reprovision the *moduleType* attribute of *PModule* to match the module present on the PCUSP card and activate provisioning. If the problem persists and *PModule* has been provisioned correctly, a new hardware module is required

7062 0003

Component	Severity	Status
Lp/<num1> Pcusp PModule/<num2> PBlock/<num3>	critical	set/clear

Legend

<num1> = 0 - 15
<num2> = 1 - 12
<num3> = 1

Details

There has been a failure of a hardware component on the PCUSP card during diagnostic tests.

Probable Cause

Type

Remedial action

Re-run the diagnostic check by unlocking the *Pcusp* component. If this fails, reboot the card. If a failure is still raised, a new hardware module is required.

7062 0004

Component	Severity	Status
Lp/<num1> Pcusp PModule/<num2> PBlock/<num3>	critical	message

Legend

<num1> = 0 - 15
<num2> = 1 - 12
<num3> = 1

Details

This alarm is issued when a SPM module on the PCUSP card is not responding to supervision heartbeat message.

The comment data includes information to identify the specific hardware module which is defective.

Probable Cause

Type

Remedial action

No action needed. The SPM module is being reset.

7062 0005

Component	Severity	Status
Lp/<num1> Pcusp PModule/<num2>	major	set/clear

Legend

<num1> = 0 - 15
<num2> = 1 - 12

Details

This alarm is issued when a PModule is not capable of running its software.

Probable Cause

Type

Remedial action

No remedial action is needed if this is just a temporary condition (for example, when the SPM is being reset). If the condition persists, check the *PMod* component's *osiOperationalStatus* and *failureCause* attributes for a more specific problem cause.

7062 0010

Component	Severity	Status
Lp/<num1> Pcusp PModule/<num2>	critical	message

Legend

<num1> = 0 - 15
<num2> = 1 - 12

Details

This alarm is issued when a SPM reboots. It hold some diagnostic information (in the comment data field) that specifies why the SPM went down.

Several instances of this alarm can be generated depending on how much information needs to be displayed. This information is referred as *Trap Data* information.

Probable Cause

Type

Remedial action

Read the *Trap Data* information to determine why the *PMod* rebooted. If the reboot reason in the *Trap Data* information does not satisfactorily explain the cause of the reboot, contact your local Nortel Networks technical support group for assistance.

7062 0011

Component	Severity	Status
Lp/<num1> Pcusp PModule/<num2>	major	set/clear

Legend

<num1> = 0 - 15
<num2> = 1 - 12

Details

This alarm is issued when a *PMod* is running out of ressource for memory or cpu usage.

Probable Cause

Type

Remedial action

If this alarm appears with some frequency, then the engineering of this PCU needs to be re-examined.

7062 0012

Component	Severity	Status
Lp/<x> Pcusp	critical/cleared	set/clear

Legend

<x> = 0 - 15

Details

This alarm is set when the *Lp/x Pcusp* is in a degraded redundancy condition.

A number of PModules (SPMs) located on the active or standby PCUSP are not available for sparing and cannot be used to process GPRS traffic.

A SPM on an active PCUSP is not available for sparing if it cannot be downloaded successfully. Note that a single SPM reset on the active PCUSP does not generate this alarm, but sets alarm 7062 0005 instead.

A SPM on a standby PCUSP is not available for sparing when it has been reset and is downloading or if it cannot be successfully downloaded.

A PCUSP switchover occurring when this alarm is set may have impacts on GPRS services.

This alarm is cleared when the *Lp/x Pcusp* is in full redundancy conditions:

1 PCUSP card is in standby mode

12 SPMs are processing traffic, or ready to process traffic, on the active PCUSP

12 SPMs are ready to process traffic on the standby PCUSP if the active PCUSP switchovers.

Probable Cause

Equipment malfunction

Type

Equipment

Remedial action

When this alarm is *set*, no remedial action is needed if this is just a temporary condition. For example, this happens just after a *Lp/x Pcusp* switchover occurs. If the condition persists, it means that the *Lp/x Pcusp* is in degraded redundancy conditions. In that case, check the content of alarm 7062 0013 to get the list of impacted PCUSP cards and PModules (SPMs) cards on both active and standby PCUSP. Check also if there are any 7062 0001, 7062 0003, 7062 0004, and 7062 0005 alarms for the related Lp. If any, this indicates that some faulty PModules are located on the active PCUSP card. Clear the problem that is preventing the *Lp/x Pcusp* from being in full redundancy conditions by replacing the faulty PCUSP card.

7062 0013

Component	Severity	Status
Lp/<x> Pcusp	warning	message

Legend

<x> = 0 - 15

Details

This alarm is issued when the status of alarm 7062 0012 is set. It lists the PModules (SPMs) that are not available on both active and standby PCUSP.

If the list of unavailable SPMs evolves at runtime, this alarm is sent again and contains the full list of unavailable SPMs for this *Lp Pcusp* component.

Probable Cause

Equipment malfunction

Type

Equipment

Remedial action

Refer to the remedial action described for alarm 7062 0012.

7062 0020

Component	Severity	Status
Pcusa/<num1> Conn/<num2> PcmLink/ <num3> Lapd/<num4>	major	set/clear

Legend

<num1> = 0 - 15999
<num2> = 1 - 256
<num3> = 0 - 47
<num4> = 0 - 31

Details

This signalling link layer alarm is raised when layer 2 has been down. It will be cleared when layer 2 has been re-established. This alarm is not generated if the *PcmLink* is not established.

Probable Cause

Type

Remedial action

Check the status of the link layer on the BSC.

7062 0021

Component	Severity	Status
Pcusa/<num1> Conn/<num2> PcmLink/ <num3> Lapd/<num4>	major	message

Legend

<num1> = 0 - 15999
<num2> = 1 - 256
<num3> = 0 - 47
<num4> = 0 - 31

Details

Lapd component overload.

The process that is running the *Lapd* component is running out of ressource for memory or cpu usage.

Probable Cause

Type

Remedial action

If this alarm appears with some frequency, then the engineering of this PCU needs to be re-examined.

7062 0023

Component	Severity	Status
Pcusa/<num1> Conn/<num2> PcmLink/ <num3>	major	message

Legend

<num1> = 0 - 15999
<num2> = 1 - 256
<num3> = 0 - 47

Details

The Bsc connected to the *PcmLink* component is not the same as provisioned on the *Conn* component.

Probable Cause

Type

Remedial action

Correct the connection between the Pcm card of the Pcu and the Bsc. Or correct the provisioning of the *Conn* component on the Passport. Or correct the provisioning on the Bsc side.

7062 0024

Component	Severity	Status
Pcusa/<num1> Conn/<num2> PcmLink/ <num3>	indeterminate	message

Legend

<num1> = 0 - 15999
<num2> = 1 - 256
<num3> = 0 - 47

Details

An internal software error has been detected by the *PcmLink* component. This alarm index is used by the PCU upon detection of various types and severities of internal errors. Refer to the alarm comment text to get a hint about what has happened.

Because the circumstances which caused this event are unexpected, the impact can vary on a case-by-case basis from no impact at all to possibly a severe impact. In the latter case, it may be accompanied by other alarms.

The problem may or may not be reproductible. If the circumstances are known, this can greatly help the resolution of the problem.

Probable Cause

Type

Remedial action

Contact your local Nortel Networks technical support group.

7062 0025

Component	Severity	Status
Pcusa/<k> Conn/<l> PcmLink/<m> CgiCell/ <n>, <o>	major	set/clear
Pcusa/<k> Conn/<l> PcmLink/<m> Cell/<p>		

Legend

<k> = 0 - 15999
<l> = 1 - 256
<m> = 0 - 47
<n> = 0 - 65535 (Cell Location Area Code)
<o> = 0 - 65535 (Cell Global Identifier)
<p> = a decimal value

Details

This alarm is set when the SGSN is not responding to a BSSGP protocol message for this cell instance. The GPRS service is not available for this cell instance. If NMO1 is activated, this fault induces some heavy impacts on circuit services (Mobile Terminated calls failing).

The reset procedure of the signalling BVC has been successfully completed; but, a PTP procedure related to this cell has failed.

The alarm is cleared when the PTP procedure is initiated again and successfully completed.

Probable Cause

Protocol error

Type

Communications

Remedial action

The alarm comment text contains more information on the cause of the failure.

If the non acknowledged message is a BVC-RESET, perform a lock/unlock of the related cell instance.

If the non acknowledged message is either a BVC-UNBLOCK, a BVC-BLOCK, or a BVC-FLOW-CTRL:

1. Deactivate and then reactivate the GPRS service for this cell using BTS flag gprsCellActivation

2 If the problem persists, perform a lock/unlock of the related cell instance

If the remedial action is unsuccessful and NMO1 is activated, then deactivate the GPRS service for this cell.

7062 0027

Component	Severity	Status
Pcusa/<num1> Conn/<num2> PcmLink/ <num3> Bvc/<num4>	critical	set/clear

Legend

<num1> = 0 - 15999
<num2> = 1 - 256
<num3> = 0 - 47
<num4> = 0

Details

This alarm is set when the reset of the signalling BVC has not been successfully completed. GPRS service is not available for the related BSC identified by the Conn instance. If NMO1 is activated, this fault induces some heavy impacts on circuit services (Mobile Terminated calls failing).

The alarm is cleared when the reset procedure is initiated again and successfully completed.

Probable Cause

Protocol error

Type

Communications

Remedial action

Check the SGSN status and/or the FR cloud.

If SGSN status is OK, lock/unlock all the *FrAtm/x* instances used by the related Nse instance to force a GbDown/GbUp transition. This should trigger a signalling BVC reset procedure. If the remedial action is unsuccessful and NMO1 is activated, then deactivate the GPRS service for this BSC.

7062 0028

Component	Severity	Status
Pcusa/<num1> Conn/<num2>	critical	set/clear

Legend

<num1> = 0 - 15999

<num2> = 1 - 256

Details

This alarm is set upon system failure of the Gb underlying network service. GPRS service is not available for the related BSC identified by the Conn instance. If NMO1 is activated, this fault induces some heavy impacts on circuit services (Mobile Terminated calls failing).

The alarm is cleared upon recovery of the Gb underlying network service.

Probable Cause

Subsystem failure

Type

Communications

Remedial action

Check Gb physical layer by displaying the *FrAtm/x Framer* osiState of each Bearer Channel used by this Nse. If it is not enabled (busy), check the cabling, the *fratm* provisioning, or the adjacent node in the frame relay network. Also display FR E1C port status *lp/m e1/n*.

Check the frame relay level by displaying the *FrAtm/x Lmi* osiState. If it is not enabled (busy) or the protocolStatus is not equal to *normalCondition*, check the *Lmi* provisioning on both SGSN and PCUSN sides.

Display *FrAtm/x Dlci/y Siwf AtmConn* state. If it is not connected, check the DLCI provisioning. Check that the remote address between *fratm* and *PcGtl/x Nse/y Nsvc/z* components are consistent.

Check all the *PcGtl/x Nse/y Nsvc/z* states for this Nse instance. If no one is unBlocked, find out on which side (PCUSN or SGSN) these Nsvcs have been blocked, and unblock these NSVCs or unblock the corresponding DLCIs.

If SGSN and FR clouds datafill are consistent, and corresponding status enabled, an NS Reset Procedure can be forced by locking/unlocking corresponding *FrAtm/x* related component instances or *lp/x El/y* ports. If the remedial action is unsuccessful and NMO1 is activated, then deactivate the GPRS service for this BSC.

7062 0029

Component	Severity	Status
Pcusa/<k> Conn/<l> PcmLink/<m> CgiCell/<n>, <o> Pcusa/<k> Conn/<l> PcmLink/<m> Cell/<p>	major	set/clear

Legend

<k> = 0 - 15999
<l> = 1 - 256
<m> = 0 - 47
<n> = 0 - 655345 (Cell Location Area Code)
<o> = 0 - 65535 (Cell Global Identifier)
<p> = a decimal value

Details

This alarm is set when the PCU has sent a CELL_GPRS_OPEN or a CELL_GPRS_CLOSE message to the BTS and no acknowledgment message is received from the BTS. GPRS service is not available for this cell instance. If NMO1 is activated, this fault induces some heavy impacts on circuit services (Mobile Terminated calls failing). Contact with BTS has been lost.

The alarm is cleared when the BTS acknowledges this message.

Probable Cause

Protocol error

Type

Communications

Remedial action

Check the BTS status, then lock/unlock the corresponding cell instance if needed. If the remedial action is unsuccessful and NMO1 is activated, then deactivate the GPRS service for this cell.

7062 0030

Component	Severity	Status
Pcusa/<num1> Conn/<num2> PcmLink/ <num3>	major	set/clear

Legend

<num1> = 0 - 15999
<num2> = 1 - 256
<num3> = 0 - 47

Details

This alarm is set when a *PcmLink* instance cannot be processed. This happens when processing resources are lacking on a Pcusp card.

The alarm is cleared when enough processing resources have been retrieved.

Probable Cause

Underlying resource unavailable

Type

Processing

Remedial action

Check if there are any 7062 0005 alarms for the related *Lp*.

If the condition persists, check the related *PMod*'s *osiOperationalStatus* and *failureCause* attributes.

7062 0031

Component	Severity	Status
Pcusa/<k> Conn/<l> PcmLink/<m> CgiCell/<n>, <o>	major	message
Pcusa/<k> Conn/<l> PcmLink/<m> Cell/<p>		

Legend

<k> = 0 - 15999
<l> = 1 - 256
<m> = 0 - 47
<n> = 0 - 65535 (Cell Location Area Code)
<o> = 0 - 65535 (Cell Global Identifier)
<p> = a decimal value

Details

This alarm is related to the CCCH management at the BTS level feature.

It is issued after two consecutive PDCH Assignment procedure failures: no response from BTS to PDCH ASSIGN PARAM message or receipt of PDCH ASSIGN PARAM NACK message.

CCCH at BTS level is disabled.

Probable Cause

Protocol error

Type

Communications

Remedial action

Check hardware and software compatibility (the feature is only supported starting from v13.3). In case of compatibility problems, you must deactivate the feature manually at OMC-R level: disable the feature activation flag CcchGprsAtBtsLevel.

When this alarm is raised, the feature is deactivated at the PCU side while still activated at the OMC-R side. To reactivate it at PCU side, trigger a CELL MODIFY REQ with the activation flag enabled at the OMC-R level.

7062 0032

Component	Severity	Status
Pcusa/<k> Conn/<l> PcmLink/<m> CgiCell/ <n>, <o>	major/cleared	set/clear

Legend

<k> = 0 - 15999
<l> = 1 - 256
<m> = 0 - 47
<n> = 0 - 65535 (Cell Location Area Code)
<o> = 0 - 65535 (Cell Global Identifier)
<p> = a decimal value

Details

This alarm is set when the configuration of the cell by the BSC remains incomplete for 90 minutes while the cell has been configured to support GPRS. The GPRS service is not available for this cell.

If NM01 is activated, this fault heavily impacts circuit services (Mobile Terminated Calls failing).

The alarm is cleared when the BSC completes the configuration of the cell or when the cell is deconfigured.

Probable Cause

Protocol error

Type

Communications

Remedial action

Deconfigure and then reconfigure the GPRS service for this cell using the BTS flag gprsCellActivation.

If this problem still exists, perform a lock/unlock of the related cell.

7063 0100

Component	Severity	Status
Rtg Dpn Art	major/cleared	set/clear

Details

This alarm is set by a node (specifically, by the DPRS routing system Automatic Route Tester on that node) that has detected a problem along its DPRS path to a certain RID or MID destination.

This alarm indicates a suspected DPRS routing system problem. As a result, user traffic on certain network path(s) may be experiencing excessively long delay and/or having difficulty routing to certain destination(s). If this situation persists, user traffic carried over DPRS in the network could be congested/discarded on the reported path(s).

Any of the following DPRS route errors can cause this alarm to be generated:
Timeout error: Repeated timeout encountered testing the route to a destination

Max Hops Reached: There is an upper limit on how many hops a DPRS packet can go in a Passport/DPN network before reaching its destination. If a packet is found to have reached this limit, it is normally suspected that there is a routing problem.

Loop problem: Based on the path information collected in the returned testing packet, the DPRS path chosen to reach the destination is in question because a specific node appears more than once on the path. Normally a routing loop is suspected.

More info about this error can be found under *Rtg Dpn Art* component on the node that raised this alarm.

When multiple errors are detected, only the first error will cause this alarm to be generated. However, all the detected errors will be recorded under *Rtg Dpn Art* component. A maximum of ten (10) simultaneous error destinations can be recorded and kept track of.

ART keeps re-testing all outstanding error routes regularly. A route error to a destination is considered to be no longer exist if a re-test indicates no error, or this destination has become unreachable. However, there is a waiting period between two successive re-tests (determined by the *Rtg Dpn Art testInterval* attribute), as a result, a route error that recovered during this waiting period will NOT be declared as recovered until the next re-test is conducted.

The alarm is cleared by the node that raised this alarm when all outstanding route errors are found to be no long exist by ART during its regular re-testing.

Probable Cause

Application subsystem

Type

Processing

Remedial action

The actions depend on what type of DPRS route error is detected.

Case 1:

If it's an occasional "timeout" with a short duration (less than a few times the value of *Rtg Dpn Art testInterval* attribute value), there's probably nothing really wrong, might just be a peak of traffic jammed the route. No action is needed except keeping this in system log for possible future reference.

Case 2:

If this is a long duration "timeout" error, network operator is recommended to verify the round-trip-delay of the DPRS path between the pair of nodes (the one that raised the alarm and the one to which the error is detected). This is done by issuing -rtd Ping command(s) from one node to the other. If the round-trip-delay is within acceptable limit, handle it the same way as Case 1. This alarm should be cleared by itself shortly.

In case the alarm persists and the network operator is sure the round-trip-delay is normal, you should collect all relevant on-switch information and contact Nortel. There could be a defect with this testing feature if this happens.

In case the round-trip-delay is indeed abnormal, the network operator is advised to treat it the same way as a link problem and/or traffic congestion. Normally, you would verify the links and the round-trip-delay, segment-by-segment and/or hop-by-hop among the nodes along the path between this pair of nodes.

Case 3:

If this is a "loop" error, your action also depends on the duration of this alarm.

For short duration ones (less than ten times the value of the *Rtg Dpn Art testInterval* attribute), no action is needed except keeping this in system log for possible future reference.

For those that lasts longer, get onto the node that raised the alarm, check the on-switch component *Rtg Dpn Art ErrRid/** and/or *Rtg Dpn Art ErrMid/**. You should be able to see the error path based on which the loop error was detected. Issues a Ping command (without the -rtd or -all options) from the node that raised the alarm to the node that the error is detected. You should get the path information (listing all the tandem nodes, hop-by-hop). Compare what you get here with the one you saw by displaying *Rtg Dpn Art ErrRid/** and/or *Rtg Dpn Art ErrMid/** component.

If you observe no abnormality from what you get after issuing the Ping command(s), there's probably nothing wrong. However, collect all relevant on-switch information and contact Nortel at your first convenient time (office hours). There could be a defect with this testing feature.

If you can see no less than 18 hops in the path information, especially when you see

this from both sources, please verify if the network traffic is going through ok between the pair of nodes. If yes, contact Nortel at your first convenient time (office hours). Otherwise, depend on the impact this may cause on your network, you may need to call Nortel as soon as possible. Remember to collect all relevant on-switch information.

If you can see a node appears more than once in the path information, especially when you see this from both sources, please verify if the network traffic is going through ok between the pair of nodes. If yes, contact Nortel at your first convenient time (office hours). Otherwise, depend on the impact this may cause on your network, you may need to call Nortel as soon as possible. Remember to collect all relevant on-switch information.

7064 0200

Component	Severity	Status
Vr/<vrId> Mpls LspGroup/<lsp_group_name> Lsp/<lspId>	<severity>	set/clear/ message

> ***Note:*** Generation of this alarm is controlled on a per-LSP basis by provisioning. By default, the alarm is not generated; the operator can enable alarm generation by provisioning the desired severity of the alarm.

Legend

<vrId> = name of the virtual router (an alphanumeric value)

<lsp_group_name> = the name assigned to the LSP Group instance (1 to 65535)

<lspId> = the name assigned to the LSP instance (a numeric value)

<severity> = user configurable to critical or major; clear and message severities are provided by the system

Details

If the status is *set*, this alarm indicates that a failure has either prevented LSP set up or resulted in tear down of an established LSP.

The comment field of the set alarm describes the cause of the LSP failure. Possible causes are listed and explained below.

“Notification message received--LDP status code 0x%X” indicates that while awaiting the label mapping message, a notification was received from downstream. The status codes are defined in the MPLS LDP IETF standard.

“Withdraw message received” indicates that a withdraw message was received from downstream, tearing down the LSP. The operator should follow the route downstream to find the culprit node/segment.

“LDP peer down” indicates that the LDP peer session on which the LSP relies was disabled. There should be an accompanying 7064 0400 alarm.

“Failed to send label request -- no resources” indicates that signalling could not allocate a label between the node and its LDP peer. The operator should check the label range through the attributes under component *vr pp mplsport ldpif* and possibly extend it.

“Failed to send label request -- no route” indicates that signalling could not send the label request downstream to its LDP peer. The operator should check the status of the associated *vr pp mplsport ldpif*.

“Release message received,” on interworking LSPs only, indicates that a release

message was received from upstream. The operator should follow the route upstream to find the culprit node/segment/LSP.

“LSP TE locked” indicates that the vr mpls lspg lsp te subcomponent, associated with the LSP, was locked by the operator.

A *clear* alarm is issued to report the successful setup of an LSP on initial creation or on recovery from a failure.

“LSP successfully established” indicates that the LSP was successfully setup.

Probable Cause

Operational condition: the operator has locked the Te subcomponent of the LSP.

Call establishment error: a problem on the LSR or along the path of the LSP is preventing its setup. Examples include failures under the associated Vr Pp and AtmIf components.

Type

Operator: used with operational condition cause.

Communications: used with call establishment error cause.

Remedial action

The LSP remains in the down state for automatic reattempt of setup on the next cycle. Refer to the 241-5701-445 *Passport 7400, 15000, 20000 Multiprotocol Label Switching Guide* for recommendations on analyzing LSP failures.

7064 0400

Component	Severity	Status
Vr/<string1> Pp/<string2> MplsPort LdpIf	unknown/critical/ cleared	set/clear/ message

Legend

<string1> = name of the virtual router

<string2> = name of the protocol port instance

<card_x> = card number that the LDP port is running

<card_y> = physical port number on card_x with which the LDP port is associated

<logIfSelf> = IP logical interface of the IP port under the protocol port. It is the instance value of the Vr/<string1> Pp/<string2> IpPort LogicalIf/<logIfSelf>

<logIfPeer> = IP logical interface port of the peer. This value has been signalled to this LDP port by the peer

<keep_tmr> = provisioned value of the Vr/<string1> Mpls Ldp keepAliveHoldTimer attribute

<hello_tmr> = provisioned value of the Vr/<string1> Mpls Ldp helloTimer attribute

<self_lblRange> = provisioned values of the label range for the LDP port under the Vr/<string1> Pp/<string2> MplsPort LdpIf

<peer_lblRange> = provisioned values of the label range for the LDP port of the peer. These values have been signalled to this LDP port by the peer

Details

A *message* alarm is issued with an unknown severity, when the LDP session is successfully established on the first attempt. The comment area of the alarm provides the following information:

card/<card_x> port/<port_y> LDP <logIfSelf>=><logIfPeer> : UP keepAlive=<keep_tmr>s, hello=<hello_tmr>s

If the session fails a *set* alarm is issued with a critical severity. The possible error conditions are:

- UDP hold time is exceeded. The comment area of the alarm provides the following information:

  card/<card_x> port/<port_y> LDP <logIfSelf>=><logIfPeer> : exceeded UDP hold time, resetting

- TCP hold time is exceeded. The comment area of the alarm provides the following information:

  card/<card_x> port/<port_y> LDP <logIfSelf>=><logIfPeer> : exceeded TCP hold time, resetting

- The provisioned label ranges between the two peers mismatch. The comment area of the alarm provides the following information:

  card/<card_x> port/<port_y> LDP <logIfSelf>=><logIfPeer> : label range <self_lblRange> no overlap with peer <peer_lblRange>

A *clear* alarm is issued with a cleared severity, when the LDP session is re-established.The comment area of the alarm provides the following information:

card/<card_x> port/<port_y> LDP <logIfSelf>=><logIfPeer> : UP keepAlive=<keep_tmr>s, hello=<hello_tmr>s

Probable Cause

Type

Remedial action

For set critical alarms, the system terminates the session and attempts to re-establish.

7064 0600

Component	Severity	Status
Rtr/<rtr_id> Ldp Neighbor/<neighbor_id>	critical/cleared	set/clear/message

Legend

<rtr_id> = name of the virtual router

<neighbor_id> = 48-bit LDP identifier of the label space of the neighbor LSR

Details

A *set* alarm is issued when: (1) an LDP session fails to establish, or (2) an established LDP session fails.

The possible error conditions are:

- An LDP session KeepAlive timer has expired without receipt of an LDP protocol data unit (PDU) from the neighboring LSR

- The LDP session transport (TCP) connection has failed either locally or remotely

- The neighboring LSR has shut down the LDP session

- The last established LDP adjacency in the LDP session has either failed or has been disabled

- A fatal LDP protocol error has been detected

- An internal software error has occurred and has necessitated shutdown of the LDP session

A *clear* alarm is issued when a failed LDP session successfully re-establishes.

A *message* alarm is issued when an LDP session establishes and no outstanding *set* alarm exists against that LDP session.

Probable Cause

Failure of the media over which the LDP-DU protocol is running.

A problem with the CAS provisioning associated with the *Ldp* component.

An LDP-DU protocol interworking problem with the neighboring LSR.

A TCP protocol problem either on the Passport or on the neighboring LSR.

The last established LDP adjacency in the LDP session has either failed or has been disabled.

Type

Communications

Remedial action

Verify that the media over which the LDP-DU is running is operational.

Verify that the CAS provisioning associated with the *Ldp* component is compatible with the MPLS provisioning on the neighboring LSR.

Verify that the TCP protocol is running on the neighboring LSR.

Verify that an IP route exists to the neighboring LSR.

7064 0800

Component	Severity	Status
Rtr/<rtr_id> Ldp Neighbor/<neighbor_id> Adjacency/<adj_id>	critical/cleared	set/clear

Legend

<rtr_id> = name of the virtual router

<neighbor_id> = 48-bit LDP identifier of the label space of the neighbor LSR

<adj_id> = 32-bit local interface address assigned to the local interface

Details

A *set* alarm is issued when: (1) an LDP Hello adjacency fails to establish, or (2) an established LDP Hello adjacency fails.

An LSR maintains a hold timer with each Hello adjacency; this timer is reset when an LSR receives a Hello message that matches the adjacency. If a hold timer expires -- without receipt of a matching Hello message from the neighboring LSR -- the Hello adjacency fails.

After a Hello adjacency fails, the Passport autonomously attempts to re-establish the Hello adjacency.

When no (Hello message) response is received from a neighboring LSR, that LSR is identified as Neighbor/0.0.0.0-0 in the alarm.

A *clear* alarm is issued when the failed Hello adjacency successfully re-establishes.

Probable Cause

Failure of the media over which the LDP-DU protocol is running.

A problem with the CAS provisioning associated with the *Ldp* component.

An LDP-DU protocol interworking problem with the neighboring LSR.

A UDP protocol problem either on the Passport or on the neighboring LSR.

Type

Communications

Remedial action

Verify that the media over which the LDP-DU protocol is running is operational.

Verify that the CAS provisioning associated with the *Ldp* component is compatible with the MPLS provisioning on the neighboring LSR.

Verify that the UDP protocol is running on the neighboring LSR.

Verify that an IP route exists to the neighboring LSR.

7064 0900

Component	Severity	Status
Rtr/<rtr_id> Ldp Bind/<fec_index>,<ldp_id_index>	critical/cleared	set/clear

Legend

<rtr_id> = name of the virtual router

<fec_index> = FEC with which an LSP is associated. This index is in the form of "IP Address[FEC Prefix Length]"

<ldp_id_index> = router identifier of the neighbor LSR. This index is in the form of "IP Address-Label Space Identifier"

Details

This alarm is set when there are no longer any LSPs available for a particular BGP next hop. This is an indication that the BGP next hop has lost its datapath.

The alarm is cleared by the successful setup of an LSP after a recovery from a failure.

The alarm can also be cleared if you change attribute *Rtr Ldp generateLspAlarms*. The comment text in the alarm indicates that the clear is in response to the attribute being changed.

Probable Cause

Remote node transmission error

Type

Communications

Remedial action

Refer to the 241-5701-445 *Passport 7400, 15000, 20000 Multiprotocol Label Switching Guide* for recommendations on analyzing LSP failures.

7064 0901

Component	Severity	Status
Rtr/<rtr_id> Ldp	critical/cleared	set/clear

Legend

<rtr_id> = name of the virtual router

Details

This alarm is set when there is no longer an LSP to one or more BGP next hops. This is an indication that at least one BGP next hop has lost its datapath.

The alarm can also be set if you change attribute *Rtr Ldp generateLspAlarms*. The comment text in the alarm indicates that the set is in response to the attribute being changed.

The alarm is cleared by the successful setup of all the LSPs that had previously failed.

The alarm can also be cleared if you change attribute *Rtr Ldp generateLspAlarms*. The comment text in the alarm indicates that the clear is in response to the attribute being changed.

Probable Cause

Remote node transmission error

Type

Communications

Remedial action

Refer to the 241-5701-445 *Passport 7400, 15000, 20000 Multiprotocol Label Switching Guide* for recommendations on analyzing LSP failures.

7070 0100

Component	Severity	Status
Lp/<x> Ap/<y>	major	set

Legend

<x> = 0 - 15

<y> = 0 - 31

Details

This alarm is set when an adjunct processor (AP) of a logical processor (LP) is not running.

Probable Cause

A software or hardware problem has occurred.

Type

Remedial action

No remedial action is needed. If the problem persists, the functional processor (FP) should be replaced.

7071 1000

Component	Severity	Status
La/<x>	critical	message

Legend

<x> = instance value of *LanApplication* component

Details

This alarm is issued during initial provisioning of a *LanApplication* component when a MAC address cannot be allocated for the component.

Probable Cause

This alarm can be caused by a hardware failure that interferes with the distribution of MAC addresses to the LP on which this *LanApplication* component is provisioned. It can also be caused if another component is using the MAC address designated for this component.

Type

Processing

Remedial action

Contact your local Nortel Networks technical support group for assistance.

7072 4000

Component	Severity	Status
La/<x> Trsp AtmTr Spvc/0	minor/cleared	set/clear

Legend

<x> = instance value of *LanApplication* component

Details

This alarm is issued when component *La Trsp AtmTr Spvc* is released and/or established.

This alarm is shown only on the calling end (source side).

Probable Cause

- Ethernet service failure of lock of the *LanApplication* component

- ATM-initiated connection tear-down by locking the ATM port

Type

Protocol Error Cause

Remedial action

7072 4100

Component	Severity	Status
La/<x> Trsp AtmTr Spvc/0	minor	message

Legend

<x> = instance value of *LanApplication* component

Details

This alarm is issued when the LAN SPVC fails to establish due to an invalid configuration.

Probable Cause

- The calling end receives a setup message.

- Master to Master call

Type

Configuration Error Cause

Remedial action

7072 4101

Component	Severity	Status
La/<x> Trsp AtmTr Spvc/0	minor	message

Legend

<x> = instance value of *LanApplication* component

Details

This alarm is issued when the LAN SPVC fails to establish due to invalid traffic management parameters.

Probable Cause

- The configured bandwidth is not acceptable.

- Setup IE parameters are not acceptable.

Type

Configuration Error Cause

Remedial action

7072 4102

Component	Severity	Status
La/<x> Trsp AtmTr Spvc/0	minor	message

Legend

<x> = instance value of *LanApplication* component

Details

This alarm is issued when the LAN SPVC fails to establish due to an invalid configuration.

Probable Cause

The calling address of the setup IE does not match the provisioned called local address.

Type

Configuration Error Cause

Remedial action

7072 4103

Component	Severity	Status
La/<x> Trsp AtmTr Spvc/0	minor	message

Legend

<x> = instance value of *LanApplication* component

Details

This alarm is issued when the LAN SPVC fails to establish due to an invalid configuration.

Probable Cause

The called end receives a second setup message after the SPVC is established.

Type

Configuration Error Cause

Remedial action

Appendix
Alarm causes

This appendix details the possible values for the alarm *cause* field that appears in Passport alarms.

ITU-T Recommendation X.733 and X.736 provide the basis for this appendix.

Table 2
Alarm causes

Cause	Description
Adapter error	Dependent on component issuing the alarm.
Application subsystem	A failure in an application subsystem has occurred (an application subsystem may include software to support the Session, Presentation, or Application layers).
At or near capacity	Resource at or near capacity.
Authentication failure	An attempt to authenticate a user was unsuccessful.
Bandwidth reduced	The available transmission bandwidth has decreased.
Breach of confidentiality	Information may have been read by an unauthorized user.
Cable tamper	A physical violation of a communications medium has occurred.
(Sheet 1 of 7)	

Table 2 (continued)
Alarm causes

Cause	Description
Call establishment error	An error occurred while attempting to establish a connection.
Communications protocol error	A communication protocol has been violated.
Communication subsystem failure	A failure in a subsystem that supports communications over telecommunications links. These may be implemented through leased telephone lines, by X.25 networks or in other ways.
Configuration or customization error	A system or device generation or customization parameter has been specified incorrectly, or is inconsistent with the actual configuration.
Congestion	A system or network component has reached its capacity or is approaching it.
Corrupt data	An error has caused data to be incorrect and thus unreliable.
CPU cycles limit exceeded	A central processing unit has issued an unacceptable number of instructions to accomplish a task.
Dataset or modem error	An internal error has occurred on a dataset or modem.
Debugging	Indicates some internal information used for specialized, targeted troubleshooting.
Degraded signal	The quality or reliability of transmitted data has decreased.
Delayed information	Information has been received later than expected.
Denial of service	A valid request for user service has been prevented or disallowed.
(Sheet 2 of 7)	

Table 2 (continued)
Alarm causes

Cause	Description
DTE-DCE interface error	A problem in a DTE-DCE interface, which includes the interface between the DTE and DCE, any protocol used to communicate between the DTE and DCE and information provided by the DCE about the circuit.
Duplicate information	An item of information has been received more than once, and therefore may be a replay attack.
Enclosure door open	
Equipment malfunction	An internal machine error has occurred for which no more specific probable cause has been identified.
Excessive vibration	Vibratory or seismic limits have been exceeded.
File error	The format of a file (or set of files) is incorrect and thus cannot be used reliably in processing.
Fire detected	
Flood detected	
Framing error	An error in the information that delimits the bit groups within a continuous stream of bits.
Heating/ventilation/ cooling system problem	
Humidity unacceptable	The humidity is not within acceptable limits.
Inactive virtual circuit	A virtual circuit has become inactive.
Information missing	Expected information has not been received.
Information modification detected	A data integrity mechanism has detected that information has been modified.
Information out of sequence	Information has been received in an incorrect sequence.
Input device error	An error has occurred on the input device.
(Sheet 3 of 7)	

Table 2 (continued)
Alarm causes

Cause	Description
Intrusion detection	The site on which the identified equipment is located may have been illegally entered, or the equipment itself has been modified.
I/O device error	An error has occurred on the I/O device.
Key expired	An out-of-date encipherment key has been presented or used.
LAN error	An error has been detected on a local area network.
Leak detected	A leakage of (non-toxic) fluid or gas has been detected.
Local node transmission error	An error occurred on a communication channel between.
Loss of frame	An inability to locate the information that delimits the bit grouping within a continuous stream of bits.
Loss of signal	An error condition in which no data is present on a communications circuit or channel.
Material supply exhausted	A supply of needed material has been exhausted.
Multiplexor problem	An error has occurred while multiplexing communications signals.
Network server intervention	A network server (for example, for network time synchronization) has caused the event reported by the alarm.
Non-repudiation failure	Communication has been prevented or halted due to the failure or unavailability of a non-repudiation service.
Operational condition	A human operator or an application using a programmatic command interface has sent a command to the Passport, which caused the condition.
(Sheet 4 of 7)	

Table 2 (continued)
Alarm causes

Cause	Description
Out of hours activity	Resource utilization has occurred at an unexpected time.
Out of memory	There is no program-addressable storage available.
Out of service	A valid request for service could not be satisfied due to the unavailability of the service provider.
Output device error	An error has occurred on the output device.
Performance degraded	Service agreements or service limits are outside of acceptable limits.
Power problem	There is a problem with the power supply for one or more resources.
Pressure unacceptable	A fluid or gas pressure is not within acceptable limits.
Procedural error	An incorrect procedure has been used in invoking a service.
Processor problem	An internal machine error has occurred on a central processing unit.
Protocol error	A software application is indicating a violation of an expected exchange of messages.
Pump failure	Failure of mechanism that transports a fluid by inducing pressure differentials within the fluid.
Queue size exceeded	The number of items to be processed (configurable or not) has exceeded the maximum allowable.
Receiver failure	Dependent on component issuing the alarm.
Remote node transmission error	An error occurred on a communication channel beyond the adjacent node.
Resource at or nearing capacity	The usage of a resource is at or nearing the maximum allowable capacity.

(Sheet 5 of 7)

Table 2 (continued)
Alarm causes

Cause	Description
Response time excessive	The elapsed time between the end of an inquiry and beginning of the answer to that inquiry is outside of acceptable limits.
Retransmission rate excessive	The number of repeat transmissions is outside of acceptable limits.
Software error	A software error has occurred for which no more specific probable cause can be identified.
Software program abnormally terminated	A software program has abnormally terminated due to some unrecoverable error condition.
Software program error	An error has occurred within a software program that has caused incorrect results.
Storage capacity problem	A storage device has very little or no space available to store additional data.
Temperature unacceptable	A temperature is not within acceptable limits.
Threshold crossed	A limit (configurable or not) has been exceeded.
Timing problem	A process that requires timed execution and/or coordination cannot complete, or has completed but cannot be considered reliable.
Toxic leak detected	A leakage of toxic fluid or gas has been detected.
Transmitter failure	Dependent on component issuing the alarm.
Unauthorized access attempt	An access control mechanism has detected an illegal attempt to access a resource.
Underlying resource unavailable	An entity upon which the reporting object depends has become unavailable.
Unexpected information	Information that was not expected has been received.
Unknown	
(Sheet 6 of 7)	

Table 2 (continued)
Alarm causes

Cause	Description
VC active	A software application is indicating that one or more virtual circuits (VCs) are now active.
VC inactive	A software application is indicating that one or more virtual circuits (VCs) are now inactive.
Version mismatch	There is a conflict in the functionality of versions of two or more communicating entities which may affect any processing involving those entities.
(Sheet 7 of 7)	

Passport 6400, 7400, 15000, 20000

Alarms

Release 5.2

Copyright © 2003 Nortel Networks.
All Rights Reserved.

NORTEL NETWORKS, the globemark design, the NORTEL NETWORKS corporate logo, DPN, DPN-100, and PASSPORT are trademarks of Nortel Networks. Advanced Peer-to-Peer Networking and APPN are trademarks of International Business Machines Corporation. VT100 is a trademark of Digital Equipment Corporation.

Publication: 241-5701-500
Document status: Standard
Document version: 5.2S2
Document date: December 2003
Printed in Canada