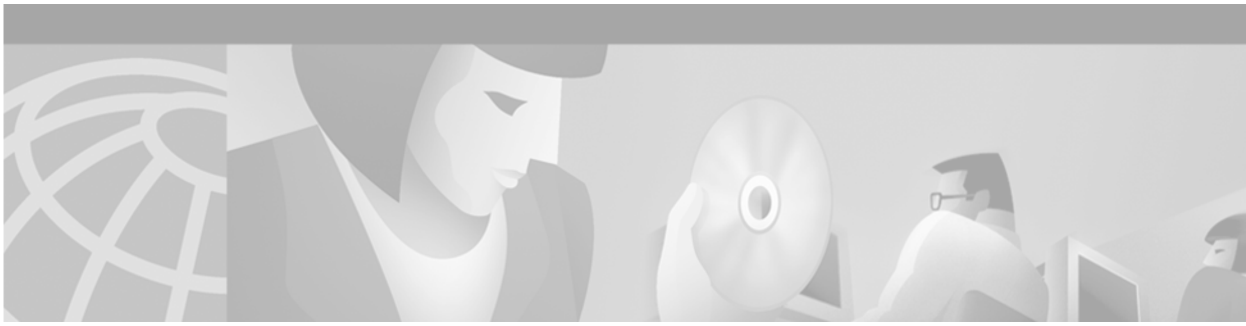


Preface

Objectives

This document describes the concepts and functions of Signaling System Number 7 (SS7). SS7 is widely deployed in the public switched telephone network (PSTN). It sources out-of-band signaling throughout the PSTN.

Audience

The guide is intended for system administrators and service technicians charged with configuring and maintaining end office switching systems.

Organization

This document describes SS7 functions and components in the following chapters:

:

Chapter 1	Overview	Briefly describes signaling methods used in the PSTN.
Chapter 2	SS7 Signaling Architecture	Describes SS7 components and link types.
Chapter 3	SS7 Protocol Stack	Describes protocol stack elements in relation to the layers of the OSI model.
Chapter 4	SS7 Signal Units	Describes the format and structure of SS7 signal types.
Chapter 5	ISUP and TCAP	Describes setup of calls and database queries using the ISUP and TCAP protocols.

Conventions

This document uses the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warning **Warning means *danger.* You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. To see translated versions of the warning, refer to the *Regulatory Compliance and Safety* document that accompanied the device.**

Related Documentation

Related documentation includes:

- *Cisco VCO/4K Hardware Planning Guide*
- *Cisco VCO/4K Site Preparation Guide*
- *Cisco VCO/4K Hardware Installation Guide*
- *Cisco VCO/4K System Maintenance Manual*
- *Cisco VCO/4K Troubleshooting Guide*
- *Cisco VCO/4K Mechanical Assemblies*
- *Cisco VCO/4K Card Technical Descriptions*
- *Cisco VCO/4K Software Installation Guide*
- *Cisco VCO/4K System Administrator's Guide*
- *Cisco VCO/4K Standard Programming Reference*
- *Cisco VCO/4K Extended Programming Reference*
- *Cisco VCO/4K System Messages*
- *Cisco VCO/4K Supervision and Call Progress Tone Detection*
- *Cisco VCO/4K Conferencing Guide*
- *Cisco VCO/4K SS7 Subsystem Manual, ANSI Software Version 5.2*
- *Cisco VCO/4K ITU Subsystem Manual, ITU Software Version 5.2*
- *Cisco VCO/4K China Integrated SS7 Manual*
- *Cisco VCO/4K ISDN Supplement*
- *Cisco VCO/4K ASIST/API Programming Reference*
- *Cisco VCO/4K TeleRouter Reference Guide*
- *Cisco VCO/4K Ethernet Guide*
- *Cisco VCO/4K MIB Reference*

- *Cisco VCO/4K Country Supplements*

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

http://www.cisco.com/register/

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

http://www.cisco.com/tac/caseopen

Contacting TAC by Telephone

If you have a priority level 1(P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

CHAPTER 1

Overview

Everything in the telecommunications network is based on signaling—call setup, connection, teardown, and billing. The two forms of signaling used by the network are:

- Channel Associated Signaling (CAS)
- Common Channel Signaling (CCS)

Signaling System Number Seven (SS7) is a form of common channel signaling, that provides intelligence to the network, and allows quicker call setup and teardown—saving time and money.

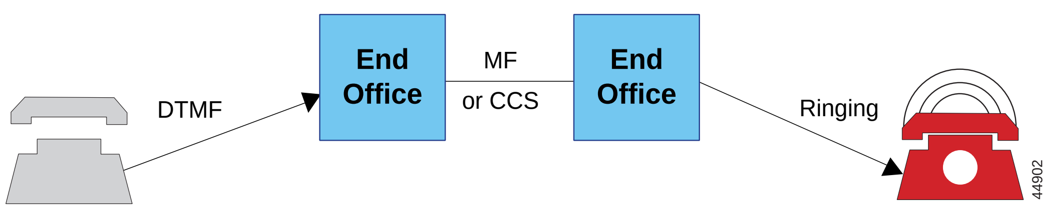
PSTN Signaling

In order to route telephone traffic through the Public Switched Telephone Network (PSTN), it is necessary to communicate with the switches that make up the PSTN. Signaling is a means for transferring network-related information between switching nodes, and also between the end office switches and their subscribers. (See Figure 1-1.)

Signaling is used to do the following:

- Request service from the central office switch (via going off-hook).
- Provide central office switch with the information necessary to route a telephone call (via DTMF addressing digits in a specific format).
- Alert destination address of incoming call (ringing).
- Provide status information and call supervision for billing.
- Manage network lines/trunks (set up and teardown calls).

Figure 1-1 End-to-End Signaling



Channel Associated Signaling (CAS)

When used for in-band signaling:

- Call setup information (off-hook, dialtone, address digits, ringback, busy) is transmitted in the same band of frequencies as used by the voice signal.
- Voice (talk) path is cut over only when the call setup is complete, using the same path that the call setup signals used.
- SF (single-frequency) signaling uses tones to represent on-hook or payphone deposits.
- MF (multi-frequency) signaling is used for switch-to-switch call setup

The principal advantage of CAS is that it is inexpensive to implement and can be used on any transmission medium.

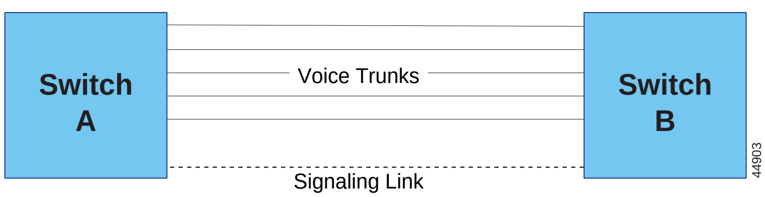
However, CAS has the following disadvantages:

- Fraud— "phone freaks" can build boxes to play call setup and teardown tones.
- Interference is possible between signaling tones used by the network and frequencies of human speech patterns.
- Speed—call setup and teardown is slower, less efficient use of resources.

Common Channel Signaling (CCS)

CCS employs a separate, dedicated path for signaling. (See Figure 1-2.) Voice trunks are used only when a connection is established, not before. Call setup time is quicker because resources are more efficiently used. CCS is the technology that makes ISDN and SS7 possible.

Figure 1-2 Common Channel Signaling



ISDN-PRI

Integrated Services Digital Network— Primary Rate Interface (ISDN-PRI) divides digital transport services into bearer channels (B-channels) for voice and data transmission and data channels (D-channels) for signaling data. (See Figure 1-3.)

In North America T1-PRI employs 24 channels (23B+1D at 64 Kbps per PCM channel) with an aggregate bandwidth of 1.536 Mbps. In Europe E1-PRI employs 32 channels (30B+2D at 64 Kbps per PCM channel) with an aggregate bandwidth of 2.048 Mbps.

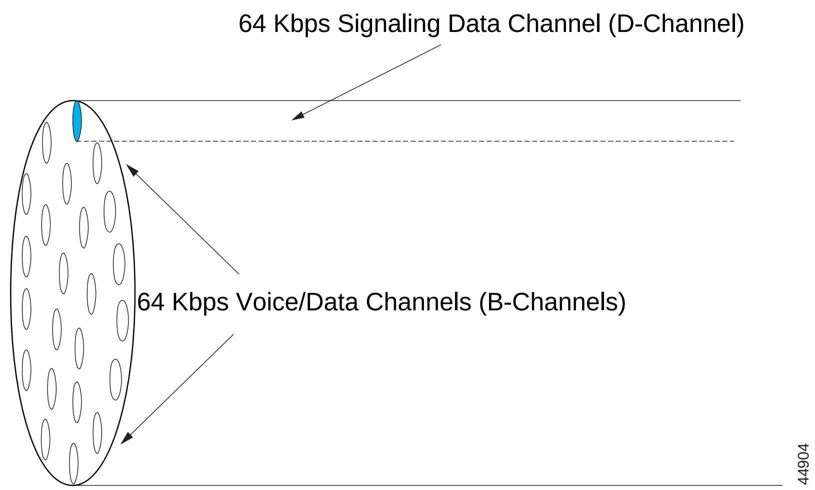
ISDN-PRI offers the following advantages:

- Data links running at either 56 or 64 Kbps are much quicker than outpulsing MF address digits.
- Signaling is possible at any time during the call, rather than only during call setup.

- Voice trunks are used more efficiently—others can use them during call setup.
- Allows better control over fraud.
- Supports enhanced services.

The principal disadvantage of ISDN-PRI is its use of Associated Signaling mode, which only works with directly trunked switches.

Figure 1-3 ISDN Bearer Vs. Data Channels



SS7

While similar to ISDN-PRI, Signaling System Number Seven (SS7) uses different messaging for call setup and teardown. SS7 lets any SS7-enabled node to talk to any other, regardless of whether they have direct trunk connections between them.

The preferred mode of signaling for SS7 networks is Quasi-Associated, whereas ISDN-PRI uses Associated Signaling mode.

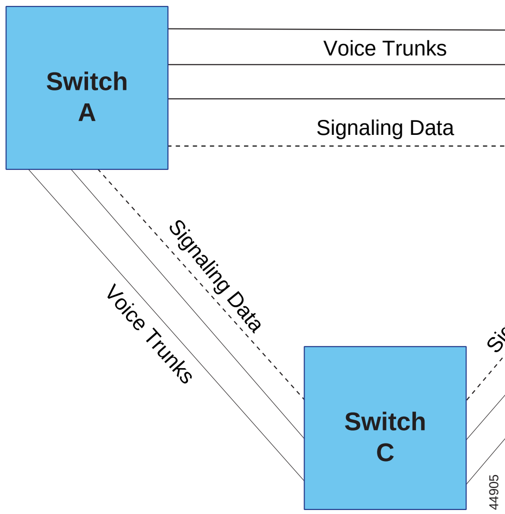
Signaling Modes

- **Associated Signaling**—Uses one dedicated path between switches as the signaling link. Examples: ISDN-PRI and E1-CAS.
- **Non-Associated Signaling**—Uses separate logical paths and multiple nodes.
- **Quasi-Associated Signaling—**Uses a minimal number of nodes (preferred for SS7, causes less delay).

Associated Signaling

With this type of signaling, the signaling link directly parallels associated voice trunks. Thus, dedicated links must be provisioned between every interconnected switch. (See Figure 1-4.)

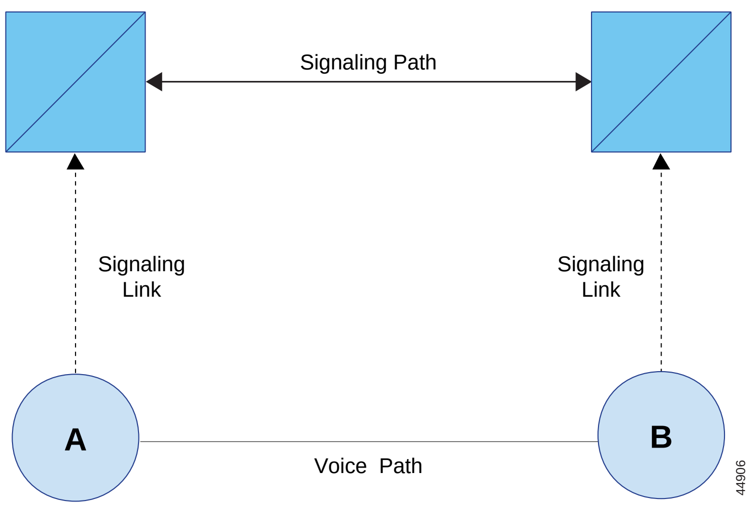
Figure 1-4 Associated Signaling



Non-Associated Signaling

With this type of signaling, voice/data and signaling are carried on separate, logical paths. Multiple nodes in the signaling path to the final destination can causes delays. Although used in the SS7 network, it is not preferred. (See Figure 1-5.)

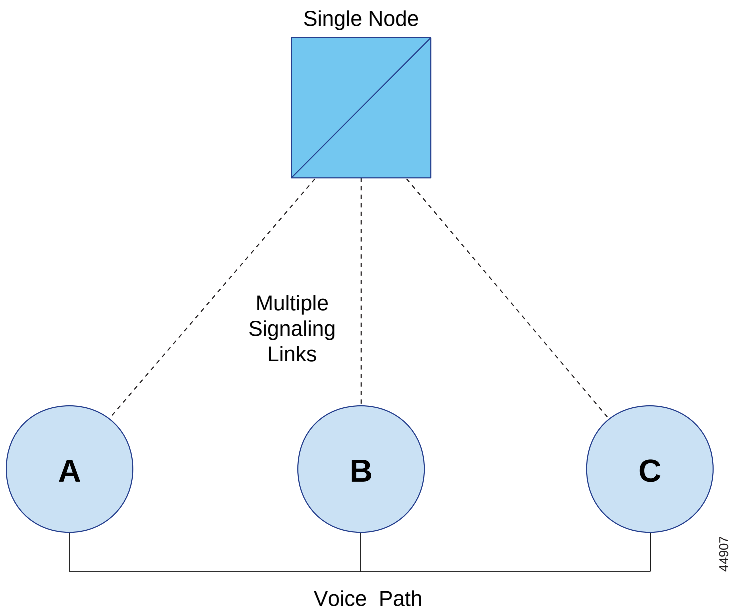
Figure 1-5 Non-Associated Signaling



Quasi-Associated Signaling

This type of signaling employs a minimal number of nodes, thus minimizing delays. Quasi-associated signaling is the preferred signaling mode for SS7. (See Figure 1-6.)

Figure 1-6 Quasi-Associated Signaling



The Evolution of SS7

In the mid-1960s, the CCITT (now the ITU) developed a digital signaling standard called Signaling System #6. SS6 was based on a packet-switched, proprietary data network. SS6 used 2.4 Kbps data links to send packets of data to distant switches to request services.

This was the first use of packet switching in the PSTN. SS6 packets consisted of 12 signal units of 28 bits each placed into a data block.

SS7 began deployment in 1983, and gradually phased out SS6. It was initially used only in the interoffice network (from central office to central office), but has gradually expanded and is now deployed in local central offices as well. SS7 provides a global standard for call setup, routing, and control.

SS7 Features

- High-speed data links (56 Kbps – national; 64 Kbps – international).
- Variable length signal units with a maximum size limitation.
- Plans to increase link speed to T1 and E1 speeds to be able to handle the increased demands required of the SS7 network.

SS7 Uses

The first use of SS7 was not for call setup and teardown, but rather for accessing databases. 800 numbers provided a problem for switches in that they could no longer route based on area code. A second “real number” for each 800 number needed to be placed in a centralized database which multiple central offices could access.

The call flow of an 800 number is as follows:

- 800 number dialed, CO switch receives digits and routes the call to a remote database via data link.
- “Real number” is determined from the database via SS7 message packet.
- Database responds with response message packet.
- Database provides routing number for call and billing information.
- CO switch is then able to route the call in the conventional manner.

SS7 Expansion

When 800 number lookups via SS7 proved successful, the network was expanded to include the ability to do call setup, teardown, and other services. Call setup/teardown is done using the ISDN User Part (ISUP) protocol. Database lookup uses the Transactional Capabilities Application Part (TCAP) protocol.

800, 900, 911 services, custom calling features, caller ID, and enhanced services are provided by SS7 and the Advanced Intelligent Network (AIN).

SS7 Deployment Planes

SS7 is deployed on two distinct levels or planes:

- International—ITU-TS standard
- National – country specific (North America—US and Canada - uses the ANSI standard)

Bellcore is an extension of the ANSI protocol and ensures the ability to interoperate with Bell Operating Company (BOC) networks.

Gateways convert national versions of SS7 to ITU-TS versions so that the networks of all nations can interoperate with each other.

Local Number Portability (LNP)

Prior to SS7, 800 numbers were not portable. If a company moved, they had to get a new number. The Telecom Act of 1996 mandated that personal phone numbers should also be portable. Telcos are required to support the porting of telephone numbers within a geographic area, increasing the demands on the SS7 network.

Seamless Roving

Seamless roving in cellular networks uses SS7 to share subscriber information from Home Location Registers (HLRs) so users do not have to register their cell phones with other providers when they travel. All cellular providers can access each others databases via SS7, enabling their subscribers to roam seamlessly from one network to another, while still allowing the home network to track and bill for all calls.

Summary

- SS7 is the world's largest data network. It links telcos, cellular, and long-distance networks nationwide and worldwide.
- SS7 interconnects thousands of telephone company providers into one common signaling network.
- SS7 will continue to evolve as new features are added to the Advanced Intelligent Network.

Review: Fundamentals

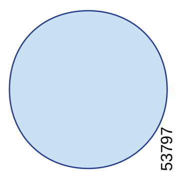
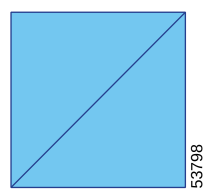
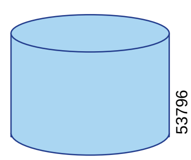
1. Name the two types of signaling used in the PSTN.
2. Which signaling type categorizes SS7?
3. How is ISDN-PRI similar to SS7?
4. What is an advantage of common channel signaling?
5. Name the three modes of common channel signaling.
6. Which mode is preferred for SS7? Why?
7. From which network was SS7 derived?
8. How fast are SS7 links?
9. What is the ISUP protocol used for?
10. What is the TCAP protocol used for?
11. What are the two versions of SS7?
12. What version of SS7 is used in the United States?
13. What function does an SS7 gateway perform?
14. How do cellular networks utilize SS7?
15. What is the AIN?

CHAPTER 2

SS7 Signaling Architecture

The SS7 signaling architecture consists of three essential components, interconnected via signaling links. Table 2-1 lists these components and their associated symbols.

Table 2-1 SS7 Network Signaling Components

Abbreviation	Name	Symbol
SSP	Signal Switching Point *- or -* Service Switching Point	
STP	Signal Transfer Point	
SCP	Signal Control Point *- or -* Service Control Point	

Signal Switching Point

SSPs are switches that have SS7 software and terminating signaling links. An SSP can be a combined voice/SS7 switch or an adjunct computer system (front end) connected to a voice (Class 5 or tandem) switch.

SSPs create packets (signal units) and send those messages to other SSPs, as well as queries to remote shared databases to find out how to route calls. They can originate, terminate, or switch calls.

SSPs communicate with the voice switch via the use of primitives and have the ability to send messages using ISUP (call setup and teardown) and TCAP (database lookup) protocols.

The SSP uses the calling party information (dialed digits) to determine how to route the call. It looks up the dialed digits in the SSP routing table to find the corresponding trunk circuit and terminating exchange. The SSP then sends an SS7 message out to the adjacent exchange requesting a circuit connection on the trunk which was specified in the routing table.

The adjacent exchange sends an acknowledgement back, giving permission to use that trunk. Using the calling party information contained in the setup info, the adjacent exchange determines how to connect to the final destination. This might require several trunks to be set up between several different exchanges.

SSP manages all of these connections until the destination is reached.

Signal Transfer Point

STPs are packet switches, and act like routers in the SS7 network. Messages are not usually originated by an STP. An STP can act like a firewall, screening messages with other networks.

STPs route SS7 messages (based on information contained in the message format) to outgoing signaling links over the SS7 network. They are the most versatile of all the SS7 entities, and are a major component in the network.

There are three levels of STPs. (See Figure 2-1.)

- National Signal Transfer Point
- International Signal Transfer Point
- Gateway Signal Transfer Point

National STP

A National STP exists within the national network (will vary with the country). It can transfer messages that use the same national standard of protocol.

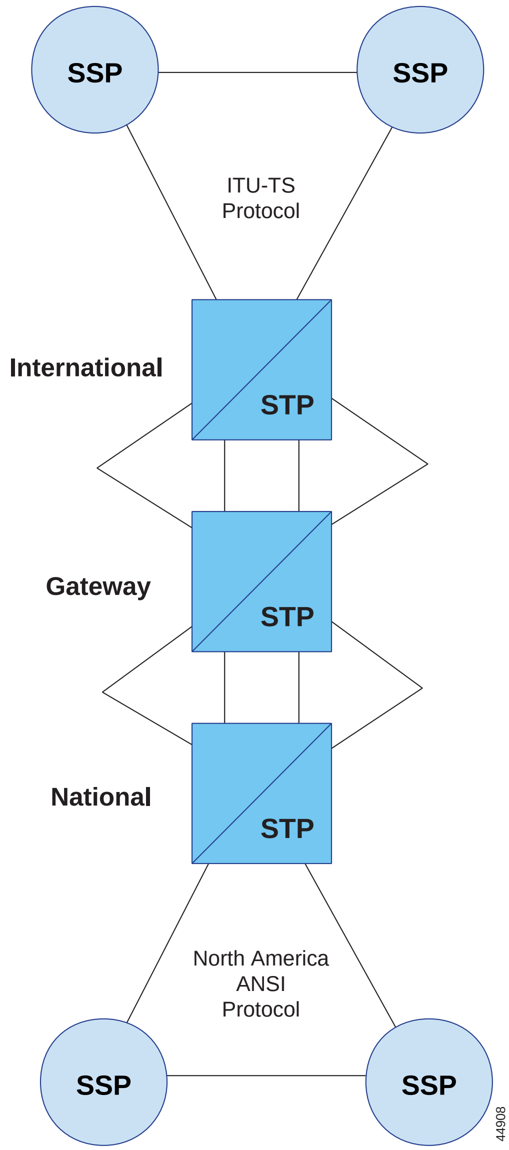
Messages can be passed to an International STP, but can not be converted by the National STP. Protocol converters often interconnect a National and an International STP by converting from ANSI to ITU-TS.

International STP

An International STP functions within an international network. It provides for SS7 interconnection of all countries, using the ITU-TS standard protocol.

All nodes connecting to an International STP must use the ITU-TS protocol standard.

Figure 2-1 STP Levels



Gateway STP

A Gateway STP converts signaling data from one protocol to another. Gateway STPs are often used as an access point to the international network. National protocols are converted to the ITU-TS protocol standard. Depending on its location, the Gateway STP must be able to use both the International and National protocol standards.

A Gateway STP also serves as an interface into another network's databases, such as from an interexchange carrier (IXC) to an end office. The Gateway STP can also be configured to screen for authorized users of the network.

Gateway STPs also provide measurements of traffic and usage via the following means:

- **Traffic**—Measures the peg counts of the type of messages entering or leaving the network.
- **Network events—**Track events such as link out-of-service or local processor outage, for maintenance purposes.
- **Usage—**Provides peg counts of the record number of messages by message type. Usage counts are sent to the Regional Accounting Office (RAO) for processing in Bell Networks. RAOs invoice customers such as IXCs and independent telcos, charging for access into the SS7 network, to help offset the cost of deploying the network.

Signal Control Point

An SCP is usually a computer used as a front end to a database system. It is an interface to telco databases, not usually to other, application-specific databases. (Refer to Table 2-2.)

Telco databases are usually linked to SCPs by X.25 links. The SCP can provide protocol conversion from X.25 to SS7, or can provide direct access to the database through the use of *primitives* which support access from one level of protocol to another.

Note Some new SCP applications are being implemented in STPs.

The address of an SCP is a *point code*, and the address of the database it interfaces with is a *subsystem number.* The database is an application entity which is accessed via the TCAP protocol.

Table 2-2 Telco Databases Accessible via SCP

Abbreviation	Name	Description
BSDB	Business Services Database	Allows companies to create and store proprietary databases, as well as create private networks.
CMSDB	Call Management Services Database	Provides information relating to call processing, network management (prevent congestion), call sampling (create reports for traffic studies), and the routing, billing and third-party billing for 800, 976 and 900 numbers.
HLR	Home Location Register	Used in cellular networks to store subscriber information.
LIDB	Line Information Database	Provides billing instructions.

Table 2-2 Telco Databases Accessible via SCP (continued)

Abbreviation	Name	Description
LNP	Local Number Portability	Allows people to change telco service providers but keep their same telephone number.
OSS	Operations Support Systems	Associated with remote maintenance centers for monitoring and managing SS7 and voice networks.
VLR	Visitor Location Register	Used when a cell phone is not recognized by the mobile switching center (MSC).

SS7 Links

An SS7 link is the physical transmission line (serial 56/64 Kbps or DS0 channel) that connects the individual nodes in an SS7 network.

SS7 networks are built to be highly reliable and redundant. Link diversity is built into the network design, providing multiple signaling paths, so that there is no single point of failure. This practice ensures that redundant links have the capacity to handle all rerouted network traffic.

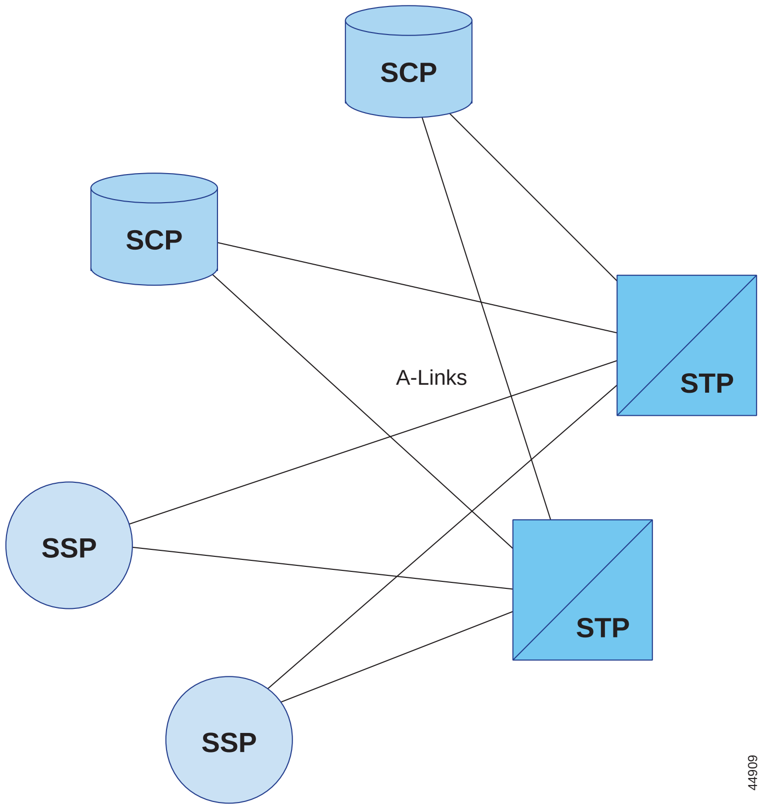
Link Types

A-Links

Access links (A-links) interconnect an STP and either an SSP or an SCP (signaling end points). Their sole purpose is to deliver signaling to and from signaling end points. End points always have at least two A-links (also called signaling beginning points).

Any signaling that an SSP or SCP needs to send to any other node in the SS7 network is sent on one of its A-links to its “home” STP, which processes and routes the message along its way. Messages addressed to an SSP or SCP are routed to its “home” STP, which forwards them to the addressed node over its A-links. (See Figure 2-2.)

Figure 2-2 A-Links

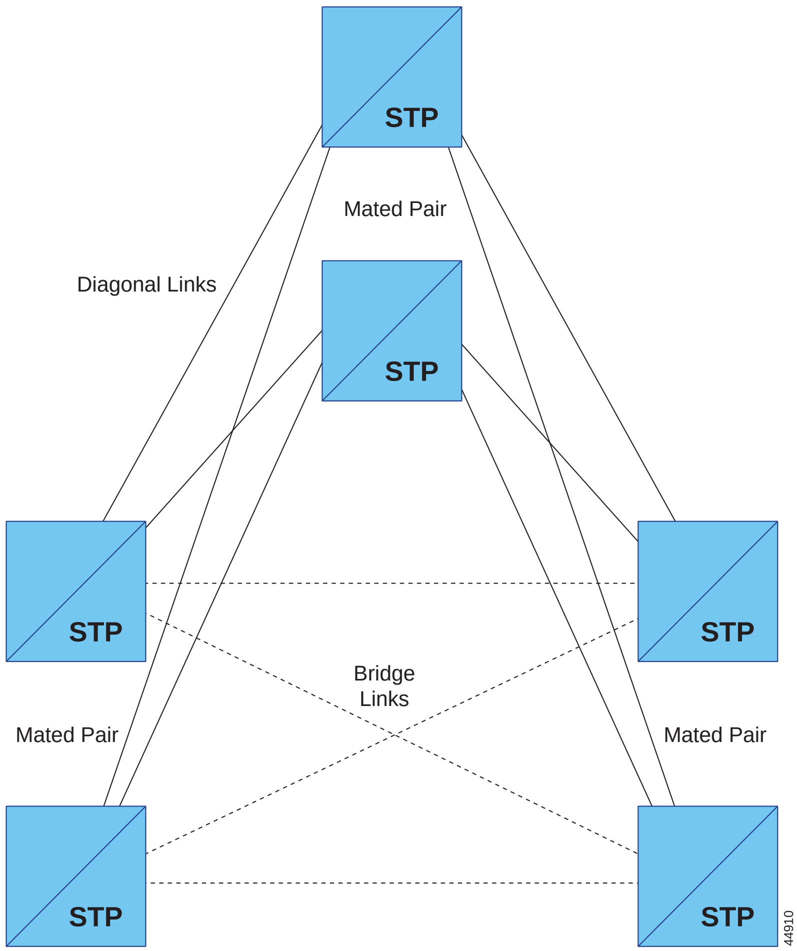


B- and D-Links

Bridge links (B-links) are the quad of links interconnecting peer pairs of STPs. Diagonal links (D-links) are the quad of links interconnecting mated pairs of STPs at different hierarchical levels. (See Figure 2-3.)

Since the SS7 network has no clear hierarchy, these links are referred to as B-links, D-links, or B/D-links.

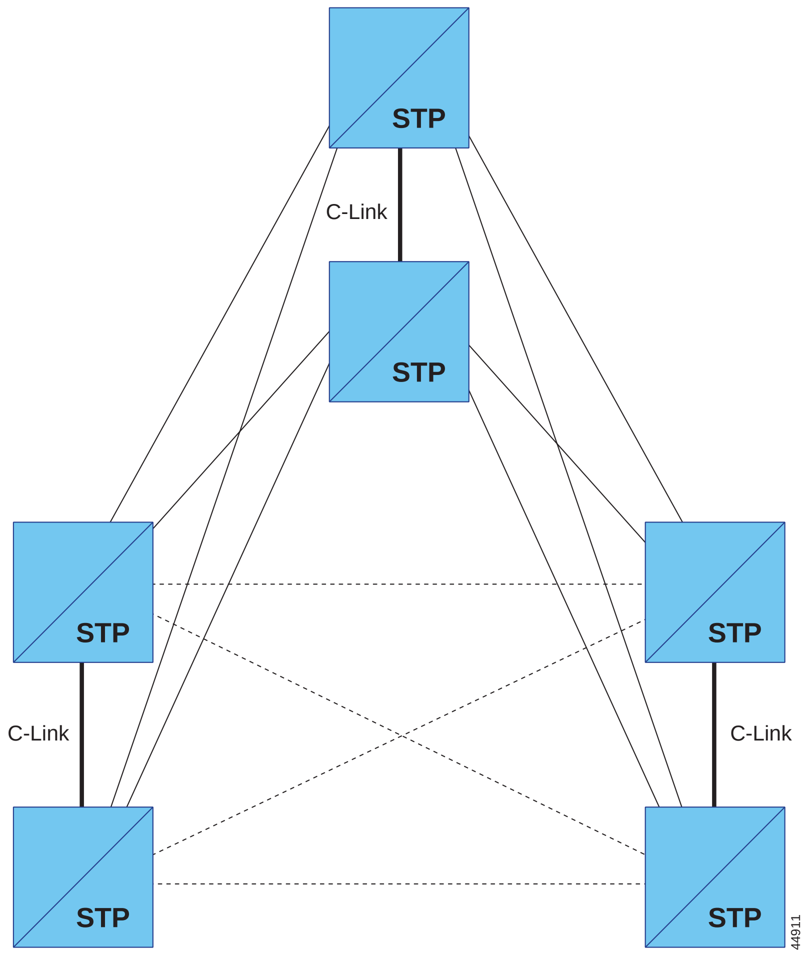
Figure 2-3 B/D-Links



C-Links

Cross links (C-links) interconnect mated STPs and are used to enhance the reliability of the signaling network not regularly used by SS7 traffic. (See Figure 2-4.) They are used only when there has been a link failure which causes an STP to have no other route.

Figure 2-4 C-Links



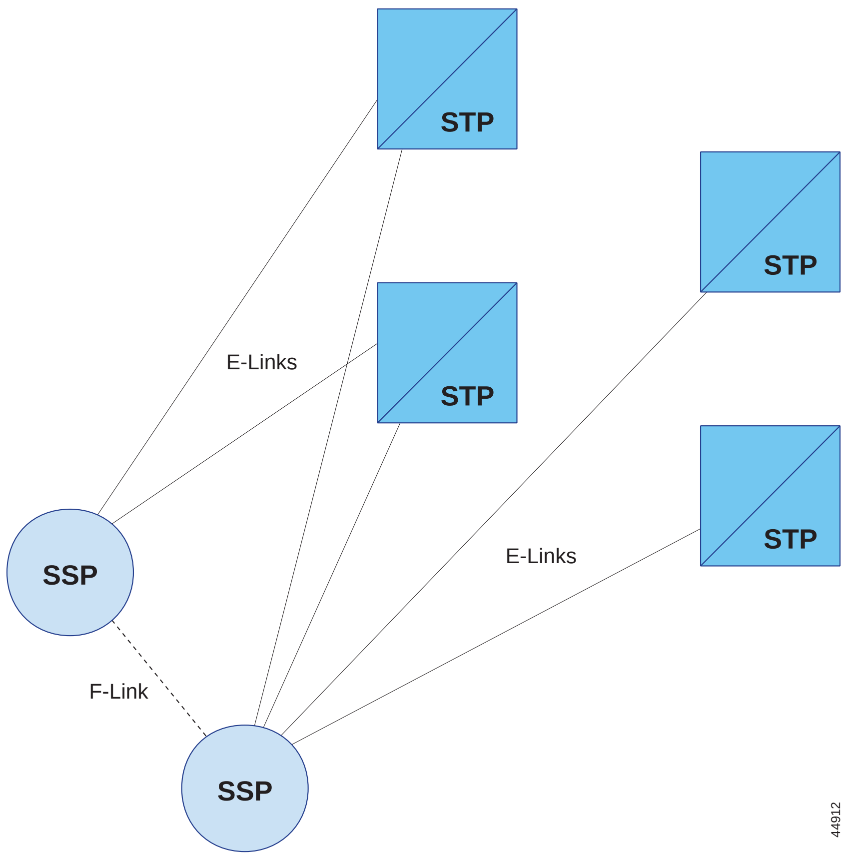
E- and F-Links

Extended links (E-links) connect an SSP to an alternate STP to provide backup connectivity to the network if the SSP's "home" STP cannot be reached on its A-link.

Note E-links are not usually provisioned, unless cost/reliability trade-offs justify the expense.

Fully associated links (F-links) directly connect two signaling end points (SSPs and/or SCPs). They are not usually used in networks with STPs because they allow associated signaling only, thus bypassing the security features provided with an STP. (See Figure 2-5.)

Figure 2-5 E- and F-Links

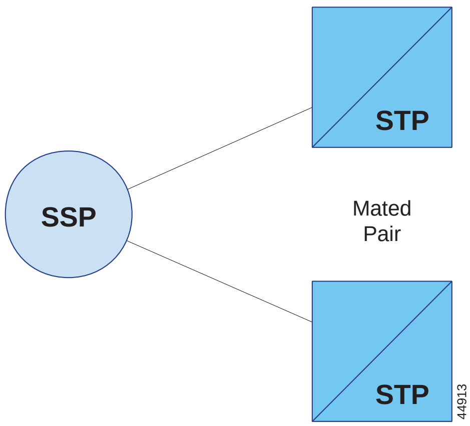


Linksets

Links are put into groups called linksets. Up to 16 links can be assigned to one linkset. All links in a linkset must have the same adjacent node. (See Figure 2-6.)

Switches will alternate traffic across all links in a linkset to ensure equal usage of all facilities in the network.

Figure 2-6 Linksets



Linkset Characteristics

If possible, links should be terrestrial. Satellite links can be used but are not preferred because of the inherent delay.

Alternate linksets are set up to provide backup paths when congestion occurs in the network. When a link fails, all other links within the linkset must take over. (See Figure 2-7.)

Note A maximum of 10 minutes downtime per year is allowed for any one linkset, to protect network integrity.

If an SS7 entity such as an STP fails, its mate assumes the full traffic load. For this reason, SS7 entities are designed to send less than 40 percent of the traffic on any given link. If an entity fails at 40-percent capacity, there is still enough room on its mate for it to carry the entire traffic load of the mated pair.

Physical Link Interfaces

The signaling link interface type will depend on the type of equipment used with the links. The V.35 interface is used to connect from the data service unit (DSU) to the signaling point. V.35 can also be used from a digital system cross-connect frame (DSX).

Note V.35 needs a clock source. Data links are 56 or 64 Kbps.

The most commonly used interface is a DS0A, one 56/64 Kbps channel of a DS1. A channel service unit (CSU) or DSU terminates the DS1 and separates DS0s from the T1 or E1 span circuit.

Routes

The signal point must define linksets and routes in SS7 messaging. The following entities are used in SS7 messaging:

- **Route**—A collection of linksets to reach a particular destination. A linkset can belong to more than one route.
- **Routeset**—A collection of routes that are assigned to destinations and also provide alternate routes.
- **Destination**—An address entered into the routing table of a remote signaling point. A destination need not be adjacent to the signaling point, but must be a point code that can be reached by the signaling point.

Point Codes

In SS7, addresses are assigned using a three-level hierarchy.

- **Member**—A signaling point within a cluster.
- **Cluster**—A collection of signaling points (members).
- **Network**—Each cluster is defined as being part of a network.

Any node in the SS7 network can be addressed by the three-level number defined by its network, cluster, and member numbers. Each of these numbers is an 8-bit number assigned a value from 0 to 255. This three-level address is called the *point code* of the signaling point.

Network Numbers

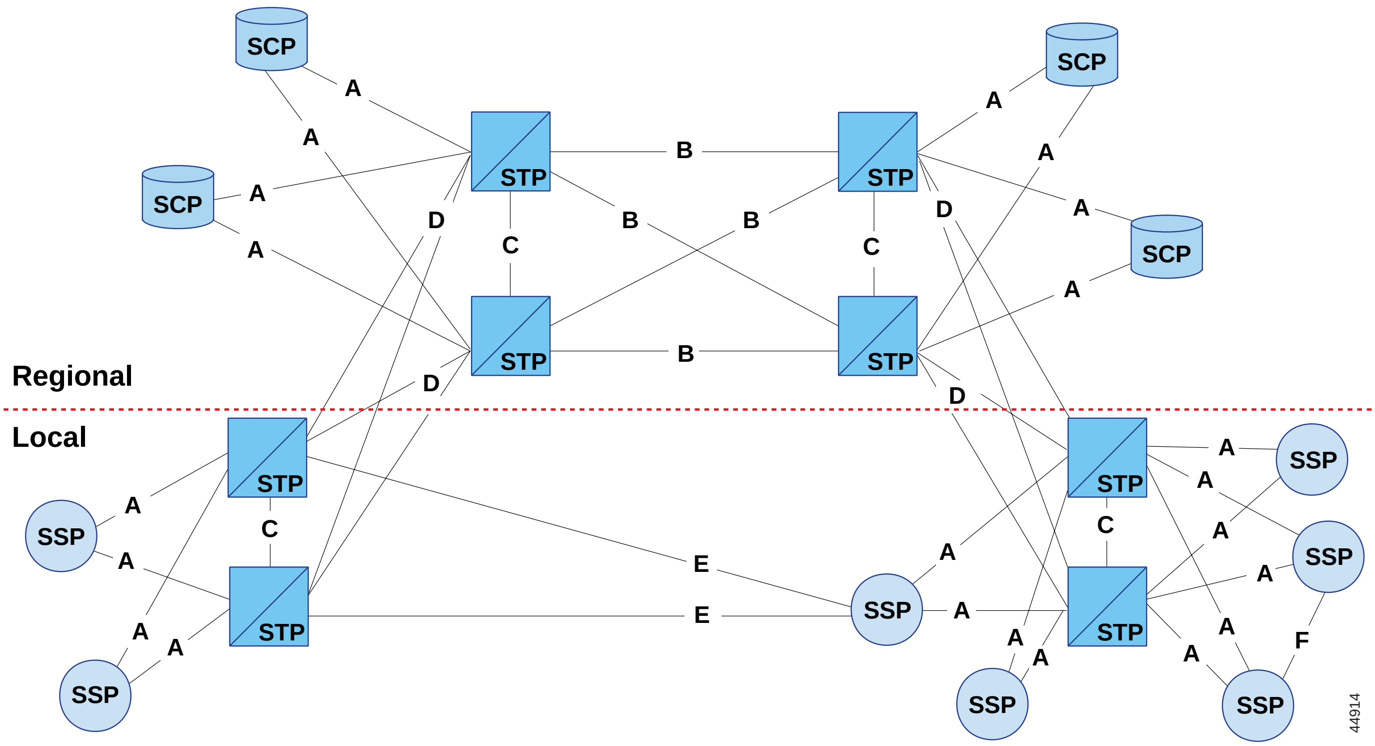
Network numbers are assigned on a nationwide basis. In North America, RBOCs, IXCs and telcos already have network numbers assigned to them.

Network numbers are relatively scarce. Companies are expected to meet size requirements in order to be assigned a network number.

Note Network number 0 is not available and 255 is reserved.

Smaller networks can be assigned one or more clusters within network numbers 1, 2, 3 and 4. The smallest networks are assigned point codes within network number 5. The cluster to which they are assigned determines the state or province they are in.

Figure 2-7 SS7 Network



Review: Signaling Architecture

1. Name the three essential SS7 components.
2. Which SS7 component functions like an SS7 network router?
3. Which SS7 component originates, terminates and switches calls?
4. Identify the three levels of STPs.
5. What interconnects a national and international STP?
6. Which protocol does an interjectional STP use?
7. Which SS7 component provides traffic measurements?
8. Which SS7 components provides interfaces to telco databases?
9. Name three types of telco databases in the SS7 network.
10. Which two databases are used in cellular networks?
11. What is meant by link diversity?
12. What does an A-link interconnect.
13. What are B- and D-links used for?
14. Are C-links used all of the time?
15. Define linkset.
16. Name two types of link interfaces. Which is the most common?
17. What is a route?
18. Define the three components of a point code.

SS7 Protocol Stack

This chapter describes the components of the SS7 protocol stack. A stack is a set of data storage locations that are accessed in a fixed sequence. The SS7 stack is compared against the Open Systems Interconnection (OSI) model for communication between different systems made by different vendors.

Figure 3-1 shows the components of the SS7 protocol stack.

SS7 Level 1: Physical Connection

This is the physical level of connectivity, virtually the same as Layer 1 of the OSI model. SS7 specifies what interfaces will be used, both Bellcore (Telecordia) and ANSI call for either the DS0A or the V.35 interface.

Because central offices are already using DS1 and DS3 facilities to link one another, the DS0A interface is readily available in all central offices, and is preferred in the SS7 network. As the demands on the SS7 network increase (local number portability), and as the industry migrates toward ATM networks, the DS1 interface will become the link interface.

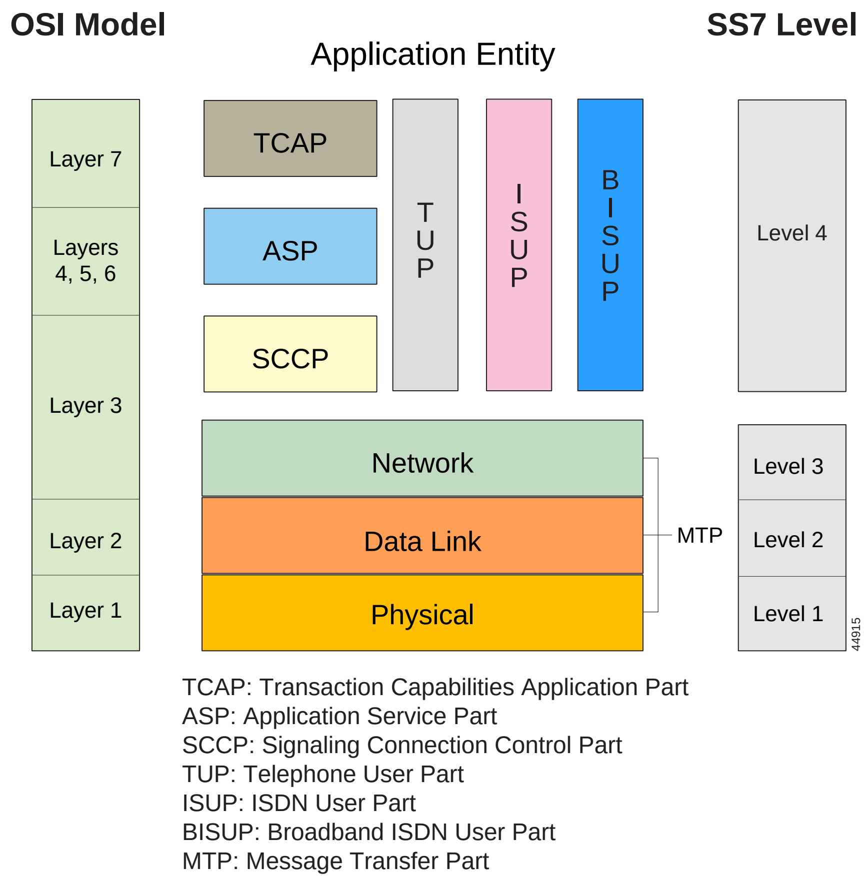
SS7 Level 2: Data Link

The data link level provides the network with sequenced delivery of all SS7 message packets. Like the OSI data link layer, it is only concerned with the transmission of data from one node to the next, not to its final destination in the network.

Sequential numbering is used to determine if any messages have been lost during transmission. Each link uses its own message numbering series independent of other links.

SS7 uses CRC-16 error checking of data and requests retransmission of lost or corrupted messages. Length indicators allow Level 2 to determine what type of signal unit it is receiving, and how to process it.

Figure 3-1 SS7 Protocol Stack



SS7 Level 3: Network Level

The network level depends on the services of Level 2 to provide routing, message discrimination and message distribution functions.

- Message Discrimination determines to whom the message is addressed.
- Message Distribution is passed here if it is a local message.
- Message Routing is passed here if it is not a local message.

Message Discrimination

This function determines whether a message is local or remote using the point code and data contained in a lookup table. Messages to remote destinations are passed to the message routing function for additional processing.

Message Distribution

Message distribution provides link, route and traffic management functions.

Link Management

This function uses the Link Status Signal Unit (LSSU) to notify adjacent nodes of link problems. Level 3 will send LSSUs via Level 2 to the adjacent node, notifying it of the problems with the link and its status.

Diagnostics consists of realigning and resynchronizing the link.

- **Realignment**—All traffic is removed from the link, counters are reset to zero, timers are reset and Fill-In Signal Units (FISUs) are sent in the meantime (called the proving period).
- **Proving Period**—Amount of time FISUs are sent during link realignment. The duration of the proving period depends on the type of link used. Bellcore specifies the proving period for a 56 Kbps DS0 link is 2.3 seconds for normal proving and 0.6 seconds for emergency proving.

Another form of link management uses changeover and changeback messages sent using Message Signal Units (MSUs). MSUs advise the adjacent node to send traffic over another link within the same linkset. The alternate link must be within the same linkset.

The bad link is being realigned by Level 3 while traffic is rerouted over alternate links. Changeback message is sent to advise the adjacent node that it can use the newly restored link again. Changeback messages are typically followed by a changeback acknowledgement message.

Route Management

This function provides a means for rerouting traffic around failed or congested nodes. Route management is a function of Level 3 and works together with link management.

Route management informs other nodes of the status of the affected node. It uses Message Signal Units (MSUs) generated by adjacent nodes and is not usually generated by the affected nodes. (Link management only informs adjacent nodes.)

Traffic Management

This function provides flow control if a node has become congested. It allows the network to control the flow of certain messages based on protocol. Traffic management deals with a specific user part within an affected node.

For example, if ISUP is not available at a particular node, a traffic management message can be sent to adjacent nodes informing them that ISUP is not available, without affecting TCAP messages on the same node.

Message Routing

Message discrimination in Level 3 will pass messages to message routing if it determines the message is not local. Message routing reads the called and calling party addresses to determine the physical address in the form of a point code.

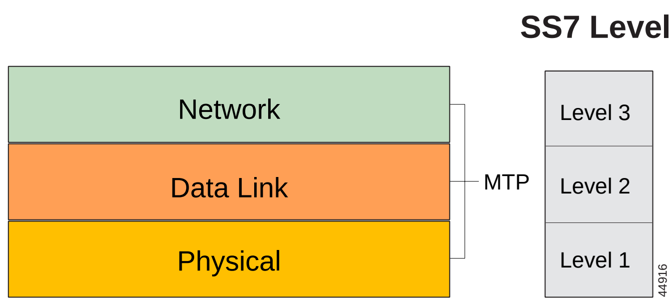
Every SS7 node must have its own unique point code. Message routing determines the point code from an address contained in the routing table.

Message Transfer Part

Protocols are used within the layers (levels) of the SS7 protocol to accomplish functions called for at each level. Levels 1, 2 and 3 are combined into one part, the Message Transfer Part (MTP). (See Figure 3-2.)

MTP provides the rest of the levels with node-to-node transmission, including basic error detection and correction schemes and message sequencing. It provides routing, message discrimination and distribution functions within a node.

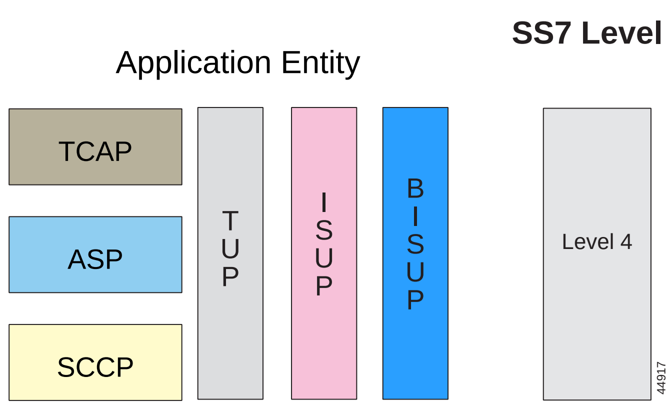
Figure 3-2 Message Transfer Part Components



SS7 Level 4: Protocols, User and Application Parts

Level 4 consists of several protocols, user parts and application parts. (See Figure 3-3.)

Figure 3-3 SS7 Level 4 Protocols, User and Application Parts



TCAP

Transactional Capabilities Application Part (TCAP) facilitates connection to an external database. Information/data received is sent back in the form of a TCAP message. TCAP also supports remote control—ability to invoke features in another remote network switch.

OMAP (Operations, Maintenance and Administrative Part) is an applications entity that uses TCAP services for communications and control functions through the network via a remote terminal.

MAP (Mobile Application Part) is used to share cellular subscriber information among different networks. It includes information such as the mobile identification number (MIN), and the serial number of the cellular handset. This information is used by the IS-41 protocol during cellular roaming.

ASP

Application Service Part (ASP) provides the functions of Layers 4 through 6 of the OSI model. These functions are not presently required in the SS7 network, and are under further study. However, the ITU-T and ANSI standards do reference ASP as viable.

SCCP

Signaling Connection Control Part (SCCP) is a higher level protocol than MTP that provides end-to-end routing. SCCP is required for routing TCAP messages to their proper database.

TUP

Telephone User Part (TUP) is an analog protocol that performs basic telephone call connect and disconnect. It has been replaced by ISUP, but is still used in some parts of the world (China).

ISUP

ISDN User Part (ISUP) supports basic telephone call connect/disconnect between end offices. Used primarily in North America, ISUP was derived from TUP, but supports ISDN and intelligent networking functions. ISUP also links the cellular and PCS network to the PSTN.

BISUP (Broadband ISUP) will gradually replace ISUP as ATM is deployed.

BISUP

Broadband ISDN User Part (BISUP) is an ATM protocol intended to support services such as high-definition television (HDTV), multilingual TV, voice and image storage and retrieval, video conferencing, high-speed LANs and multimedia.

Review: Protocol Stack

1. Define MTP and describe its components.
2. What is the preferred interface for MTP Level 1? Why?
3. How does the data link level (MTP Level 2) determine if any messages have been lost during transmission?
4. What method does MTP Level 2 use for error checking?
5. Identify three functions performed by message distribution.
6. What type of signal unit does link management use?
7. When a problem occurs with a link, which nodes does link management notify?
8. Identify the types of diagnostics available to link management.
9. What happens during the link alignment process?
10. FISUs are used for what function?
11. Define proving period.
12. What type of signal unit sends changeover and changeback messages?
13. Describe the function of a changeover message.
14. What is the expected response to a changeover message?
15. What is the function of route management?
16. Define flow control.
17. What does the message discrimination function do with non-local messages?
18. Define ISUP and describe its functions.
19. Define TCAP and describe its functions.
20. Define SCCP and describes its functions.
21. What are the differences between TUP, ISUP and BISUP?

CHAPTER 4

SS7 Signal Units

Signaling information is passed over the signaling links in messages, which are called signal units. Signal units are continuously transmitted in both directions on any link that is in service. (See Figure 4-1.) SS7 uses three different types of signal units:

- Message Signal Units (MSUs)
- Link Status Signal Units (LSSUs)
- Fill-In Signal Units (FISUs)

A signaling point sends FISUs over the link when it does not have any MSUs or LSSUs to transmit.

Signal Unit Structure

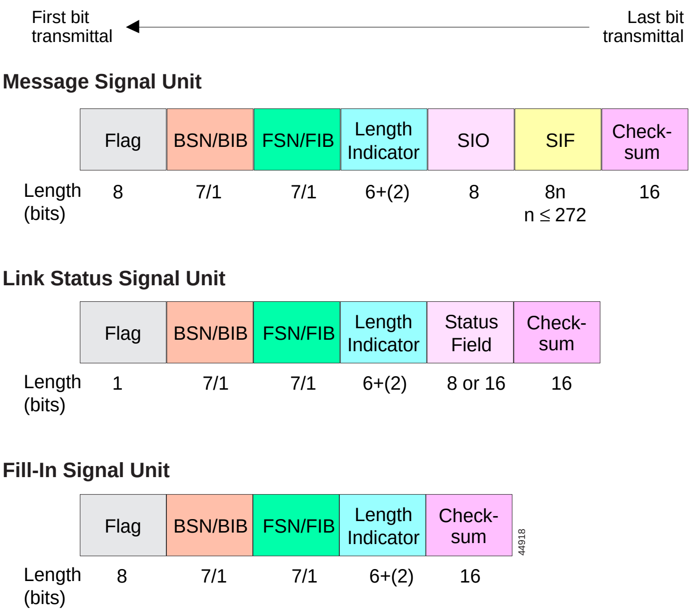
All types of signal units (MSU, LSSU, FISU) have a set of common fields which are used by MTP Level 2. Field types include the following:

- **Flag**—Delimiter in a signal unit which marks the end of one signal unit and the beginning of another. All signal units begin with a distinct 8-bit pattern (`0111 1110`).

Note Although the protocol allows an opening and closing flag, only one flag is used in North America.

- **Checksum**—An 8-bit sum calculated from the transmitted message by the transmitting signaling point and inserted in the message. It is recalculated by the receiving signaling point, and if corrupted, a retransmission is requested.
- **Length Indicator**—The number of octets between itself and the checksum. Checks the integrity of the signal unit and discriminates between different types of signal units. The default values are: FISU=0, LSSU=1 or 2, MSU>2
- **BSN/BIB FSN/FIB**—Octets that hold the backward sequence number (BSN) and backward indicator bit (BIB); the forward sequence number (FSN) and the forward indicator bit (FIB).

Figure 4-1 SS7 Signal Unit Types



Signal Unit Flow Control

The BSN/BIB and FSN/FIB fields in a signal unit (SU) confirm receipt of SUs and ensure that they are received in the order in which they were transmitted. These fields also provide flow control.

MSUs and LSSUs are assigned a sequence number when transmitted. That sequence number is placed in the FSN field of the outgoing signal unit, which is stored by the transmitting signaling point until it is acknowledged by the receiving signaling point. Signaling points acknowledge receipt of SUs by putting the sequence number of the last correctly received (and in sequence) SU in the backward sequence number (BSN) of every SU they transmit.

SU Error Detection

The check bit field and the sequence number of the signal unit are used to detect errors. Seven-bit sequence numbering is used. The forward sequence number (FSN) is incremented by one after every transmission. The backward sequence number (BSN) is used to acknowledge received signal units.

The transmitting signal point keeps all transmitted signal units in a buffer until acknowledged. Once the BSN is received, all acknowledged signal units are dropped from the buffer. Unacknowledged signal units stay in the buffer until a timer expires, causing a link failure indication to be sent to Level 3. The link is then tested and aligned.

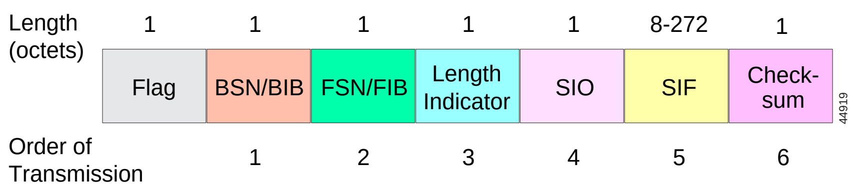
Types of Signal Units

Message Signal Units

MSUs are the workhorses of the SS7 network. All signaling associated with call setup and teardown, database query and response, and SS7 management requires the use of MSUs. (See Figure 4-2.)

MSUs provide MTP protocol fields, service indicator octet (SIO) and service information field (SIF). The SIO identifies the type of protocol (ISUP, TCAP) and standard (ITU-TS, ANSI). The SIF transfers control information and routing label.

Figure 4-2 MSU Format



SIO Structure

The functionality of the MSU lies in the contents of the service indicator octet (SIO) and the service information fields (SIF). The SIO is an 8-bit field that contains three types of information:

- Four bits to indicate the type of information contained in the service information field (referred to as the service indicator). (Refer to Table 4-1.)
- Two bits to indicate whether the message is for use in a national or international network.
- Two bits to identify the message priority. Not used to control the order of transmittal, but used when network is congested to determine if a message can be discarded. Value is from 0–3, with 3 the highest priority.

Table 4-1 SIO Service Indicator Bits

Value	Function
0	Signaling Network Management
1	Signaling Network Testing and Maintenance
2	Signaling Connection Control Part (SCCP)
3	ISDN User Part (ISUP)

SIF Structure

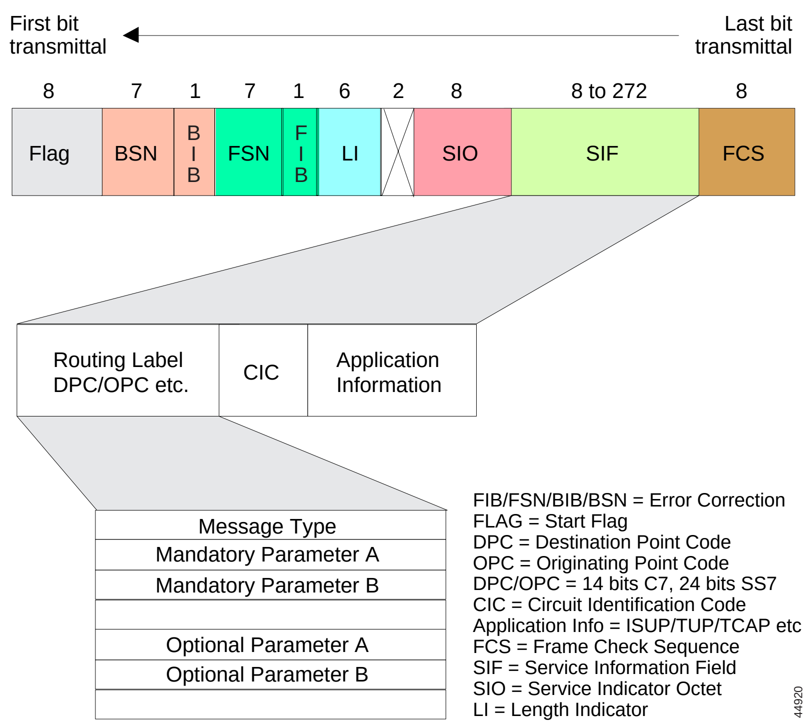
The service information field (SIF) provides the first piece of information necessary for routing and decoding the message. The SIF transfers control information and the routing label used by Level 3.

The routing label consists of the destination point code (DPC), originating point code (OPC) and signaling link selection (SLS) fields.

Note An ANSI point code consists of network, cluster and member octets (245-16-0). ANSI routing label uses 7 octets; ITU-T routing label uses 4 octets.

The SIF can contain up to 272 octets and is used by network management, ISUP, TCAP and MAP. (See Figure 4-3.)

Figure 4-3 MSU SIF Structure

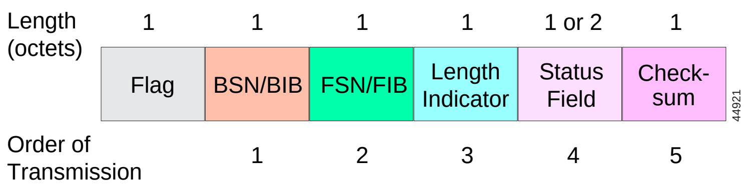


Link Status Signal Unit

LSSUs communicate information about the signaling link between the nodes on either end of the link. This information is contained in the status field of the signal unit. (See Figure 4-4.) They signal the initiation of link alignment, quality of received traffic, and status of processors at either end of the link.

LSSUs do not require any addressing information because they are only sent between signaling points.

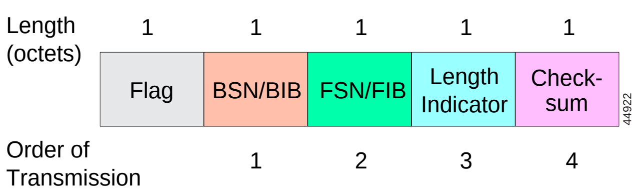
Figure 4-4 LSSU Format



Fill-in Signal Unit

FISUs do not carry any information; they simply occupy the link when there are no LSSUs or MSUs. FISUs support the monitoring of link traffic because they undergo error checking. They can also be used to acknowledge the receipt of messages using backward sequence number (BSN) and backward indicator bit (BIB). (See Figure 4-5.)

Figure 4-5 FISU Format



Link Alignment

When all signal units are received in sequence without ones-density violations and with the proper number of octets, the link is considered to be in alignment. The link is considered in error if the signal unit is not in 8-bit multiples or if the SIF exceeds the maximum 272-octet capacity.

The system uses a counter called the Signal Unit Error Rate Monitor (SUERM). Each link keeps its own unique counter. When more than 64 errors occur, the link is taken out of service, tested, and realigned by Level 3.

Review: Signal Units

1. Define signal unit.
2. Name the three types of signal units.
3. Name the four common fields found in all signal units.
4. What is a sequence number? In what field is it contained?
5. How do SS7 signaling points acknowledge the receipt of signal units?
6. Describe the functions that can be performed by an MSU.
7. What information is sent in the SIO field of an MSU.
8. Where is the routing label found?
9. Are ANSI and ITU routing labels the same length?
10. Do LSSUs need addressing information? Why?
11. What is the function of a flag field?
12. What happens when a signal unit is not acknowledged?

ISUP and TCAP

This chapter reviews the ISUP and TCAP protocols and their functions within the Public Switched Telephone Network (PSTN).

Basic ISUP Signaling

ISDN User Part (ISUP) defines the protocol and procedures used to set up, manage and release trunk circuits that carry voice and data calls over the PSTN. ISUP is used for both ISDN and non-ISDN calls. Calls that terminate within the same switch do not use ISUP signaling. (See Figure 5-1.)

In some parts of the world, such as China, the Telephone User Part (TUP) protocol supports basic call processing. TUP handles analog circuits only; digital circuits and data transmission capabilities are supported by the Data User Part protocol.

ISUP Message Format

ISUP information is carried in the service information field (SIF) of an MSU. The SIF contains the routing label followed by a 14-bit (ANSI) or 12-bit (ITU) circuit identification code (CIC). The CIC indicates the trunk circuit reserved by the originating switch to carry the call.

The CIC is followed by the message type field – IAM, ACM, ANM, REL, RLC – which defines the contents of the remainder of the message.

Each ISUP message contains a mandatory part that includes fixed-length parameters. Sometimes the mandatory fixed part is comprised only of the message type field.

The mandatory fixed part may be followed by a mandatory variable part and/or an optional part. The optional part contains parameters which are identified by a one-octet parameter code followed by a length indicator (“octets to follow”) field. (See Figure 5-2.)

Figure 5-1 Basic ISUP Signaling

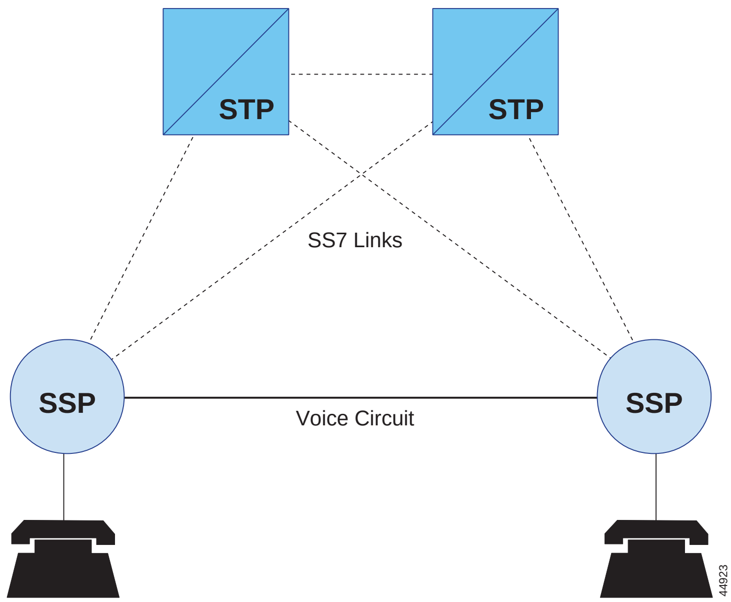
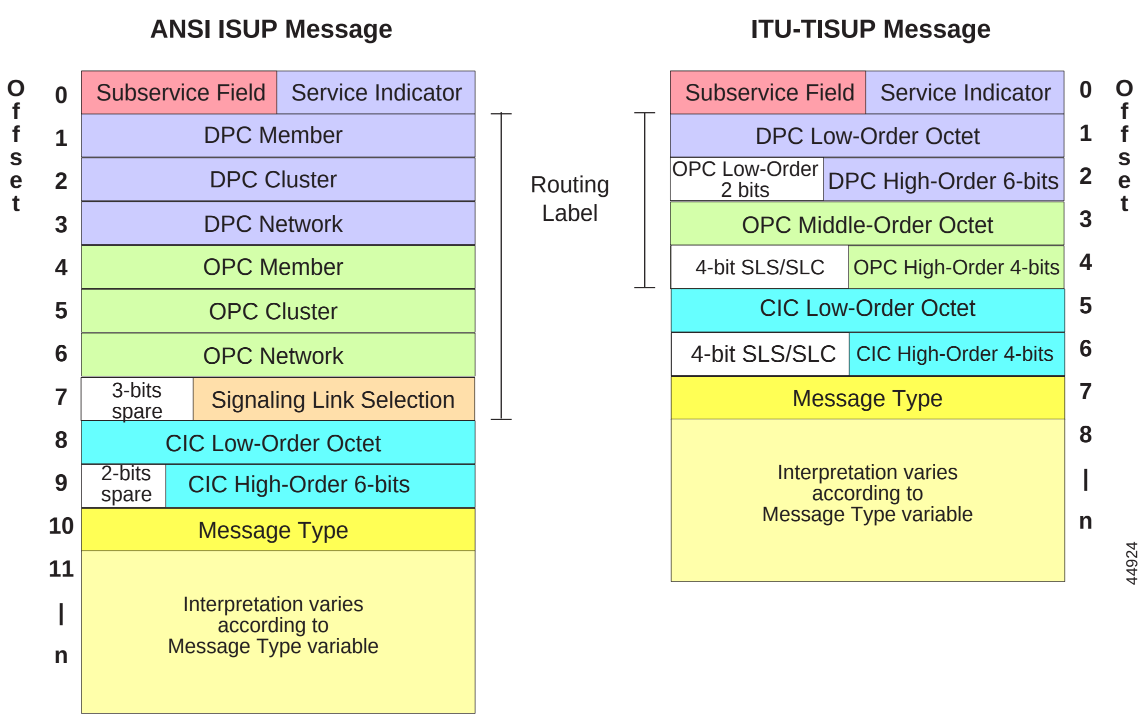


Figure 5-2 ISUP Message Format

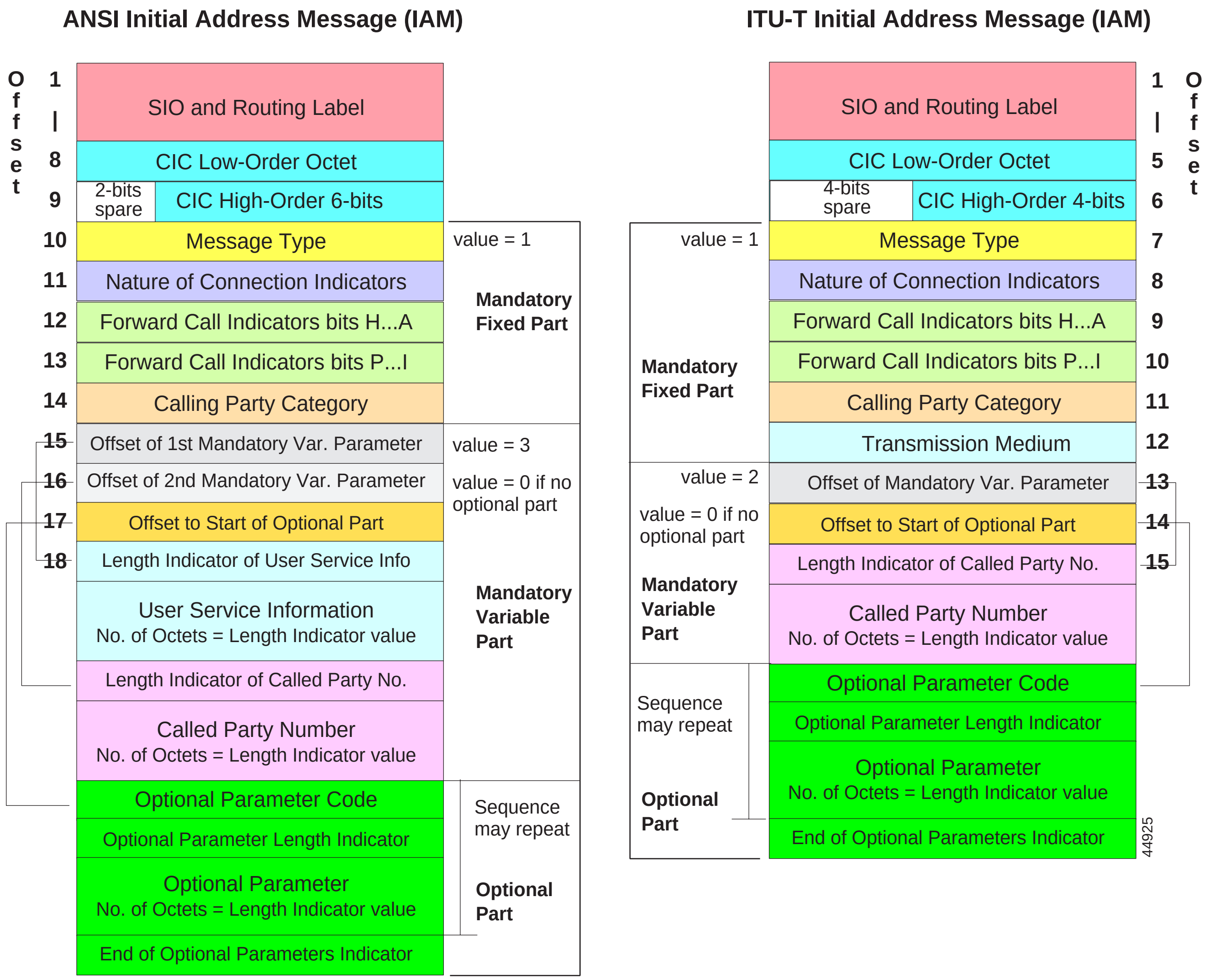


ISUP Message Types

IAM

An initial address message (IAM) is sent in the "forward" direction by each switch in the circuit between the calling party and the destination switch of the called party. An IAM contains the called party number in the mandatory variable part and may contain the calling party name and number in the optional part. (See Figure 5-3.)

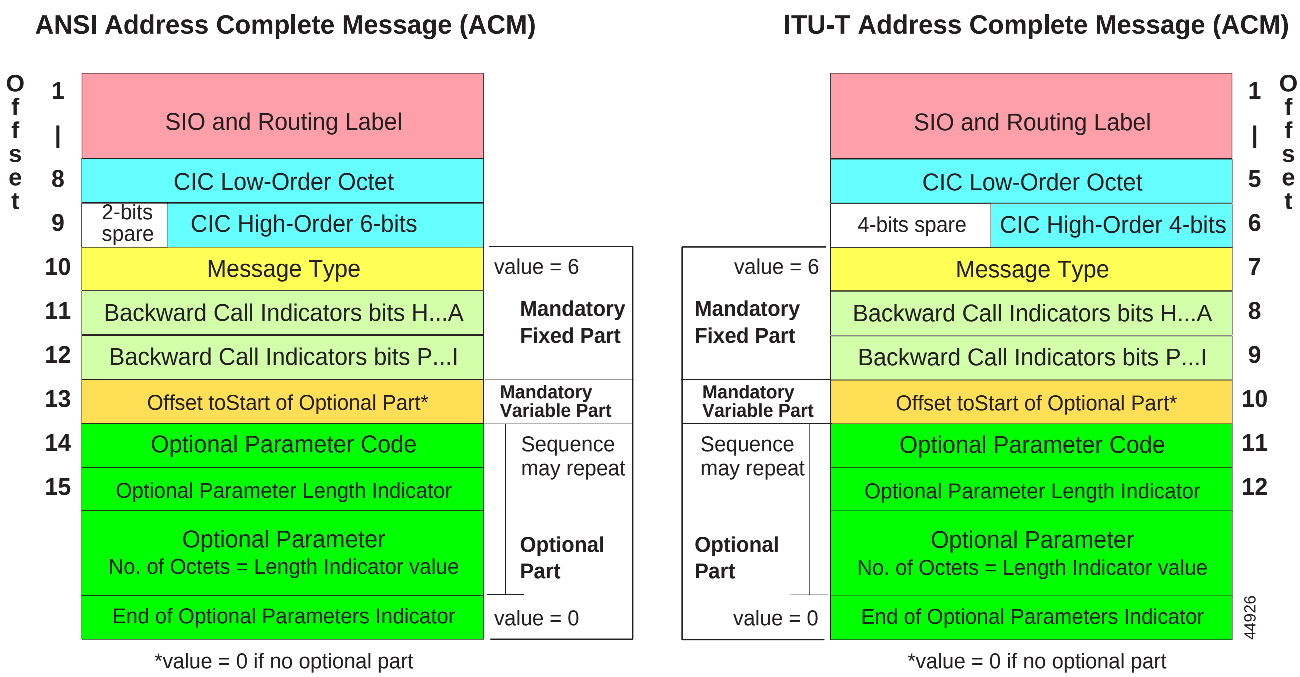
Figure 5-3 ANSI and ITU-T Initial Address Message (IAM) Format



ACM

An address complete message (ACM) is sent in the "backward" direction to indicate that the remote end of a trunk circuit has been reserved. The originating switch responds to an ACM message by connecting the calling party's line to the trunk to complete the voice circuit from the calling party to the called party. The calling party hears ringing on the voice trunk. (See Figure 5-4.)

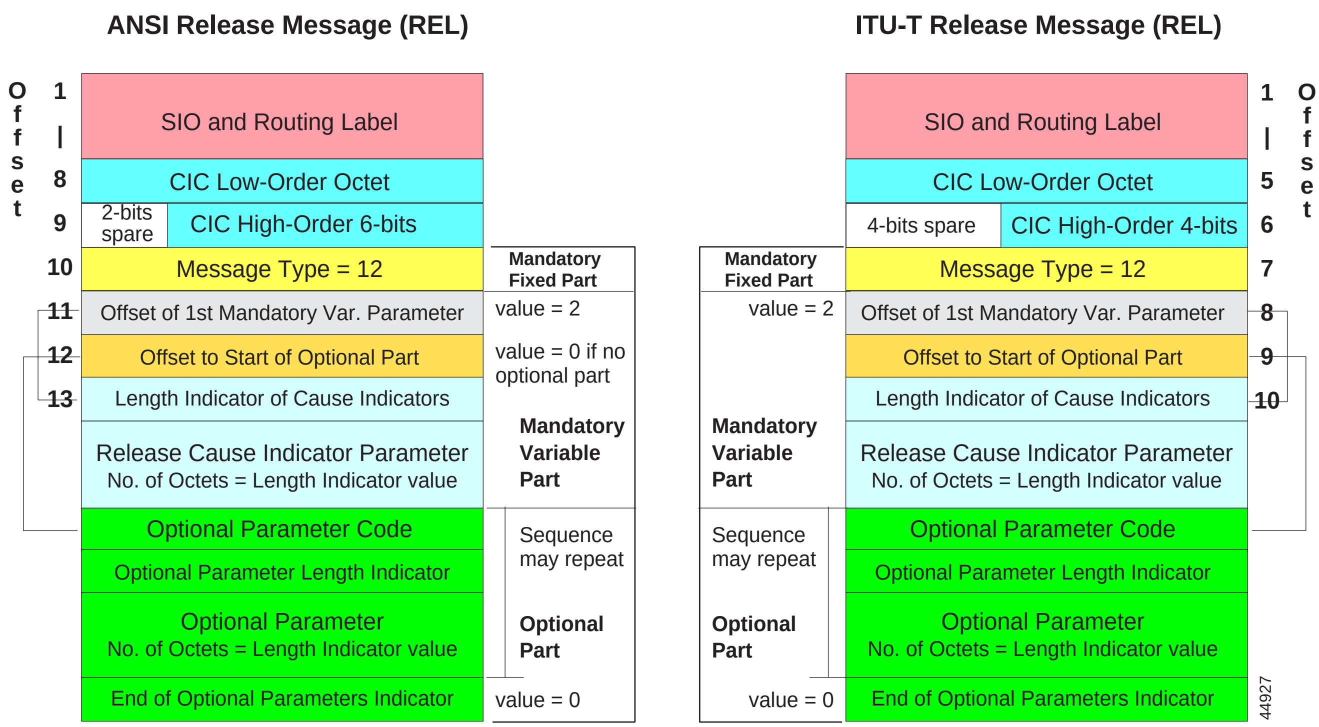
Figure 5-4 ANSI and ITU-T Address Complete Message (ACM) Format



REL

A release message (REL) is sent in either direction indicating that the circuit is being released due to a specified cause indicator. An REL is sent when either calling or called party hangs up the call (cause = 16). An REL is also sent back to the calling party if the called party is busy (cause = 17). (See Figure 5-5.)

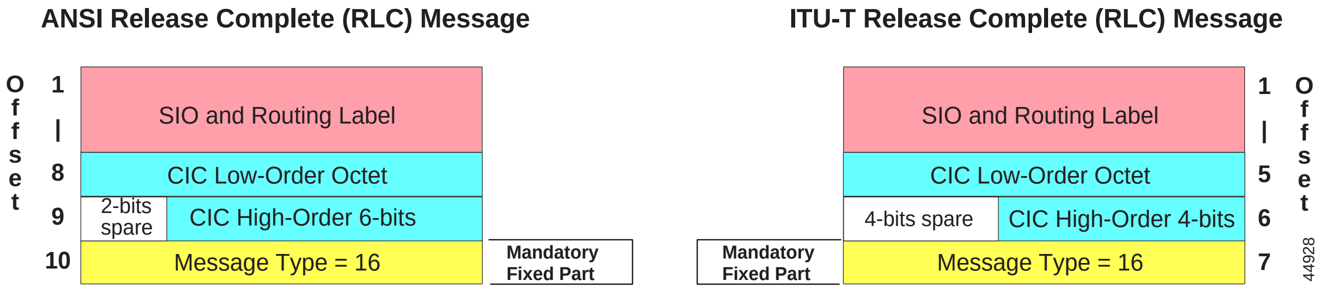
Figure 5-5 ANSI and ITU-T Release (REL) Message Format



RLC

A release complete message (RLC) is sent in the opposite direction of an REL to acknowledge the release of the remote end of a trunk circuit and to end the billing cycle, if appropriate. (See Figure 5-6.)

Figure 5-6 ANSI and ITU-T Release Complete (RLC) Message Format



ISUP Call Sequence

Call Initiated

See Figure 5-7 and Figure 5-8 as you review the following messaging sequence:

1. Calling party goes “off hook” on an originating switch (SSP) and dials the directory number of the called party.

1a. Originating SSP transmits ISUP IAM to reserve an idle trunk circuit. The IAM includes OPC, DPC, CIC, dialed digits, CPID, and calling party name (Caller ID option).

1b. IAM is routed via home STP of originating SSP.

2. Destination switch (SSP) checks the dialed number against its routing table and confirms that the called party’s line is available for ringing.

2.a Destination SSP transmits ACM to the originating SSP via its home STP to confirm that the remote end of the trunk circuit has been reserved.

2b. The STP routes the ACM to the originating SSP which connects the calling party’s line to the trunk to complete the voice circuit. The calling party hears ringback tone.

Figure 5-7 ISUP Call Initiation (1)

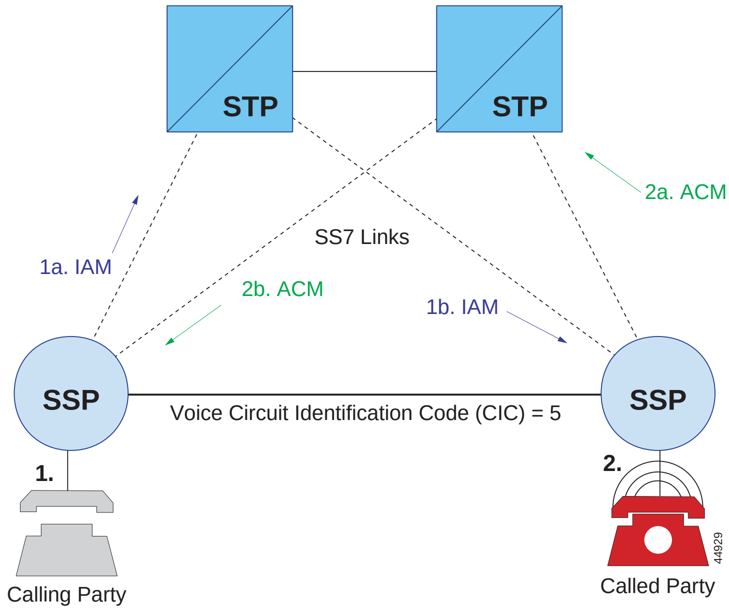
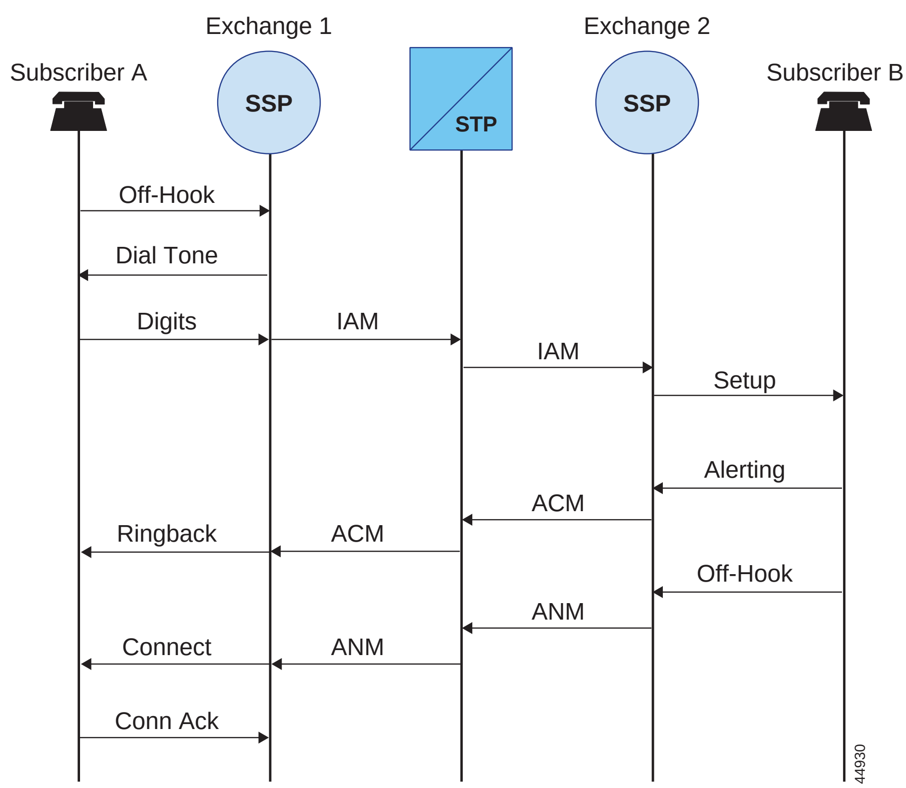


Figure 5-8 ISUP Call Initiation (2)



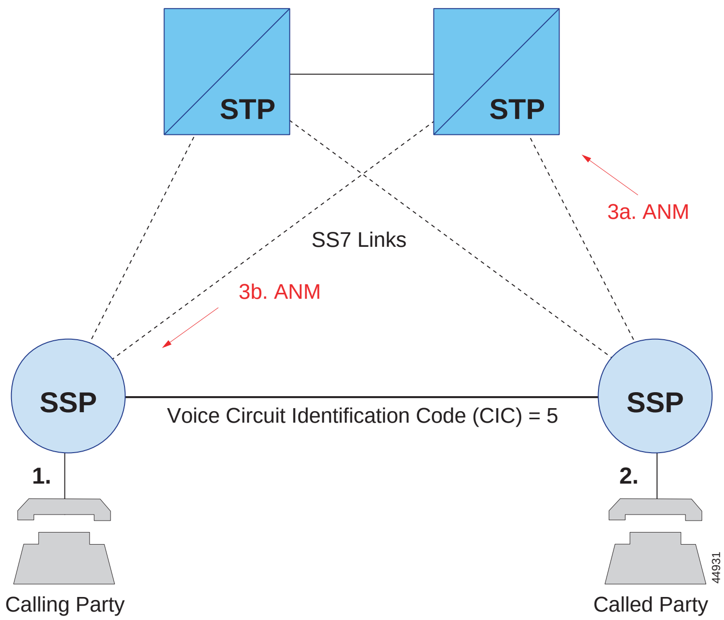
ISUP Call Answered

See Figure 5-9 as you review the following messaging sequence:

3a. Called party goes off-hook. Destination switch terminates ringing tone and transmits an ISUP answer message (ANM) to the originating switch via its home STP.

3b. STP routes ANM to originating switch which verifies that the calling party is connected to the reserved trunk. Billing is initiated.

Figure 5-9 ISUP Call Answered



ISUP Call Released

See Figure 5-10 and Figure 5-11 as you review the following messaging sequence:

4a./b. If the calling party hangs up first, the originating switch sends an ISUP release message (REL) to release the trunk between the two switches. If the called party releases first, the destination switch sends an REL message to the originating switch to release the circuit.

5a. When the destination switch receives the REL, it disconnects and idles the trunk, and transmits an ISUP release complete message (RLC) to the originating switch to acknowledge the release of the remote end of the circuit.

5b. When the originating switch receives or sends an RLC, the billing cycle ends and the trunk state is returned to idle.

Figure 5-10 ISUP Call Release (1)

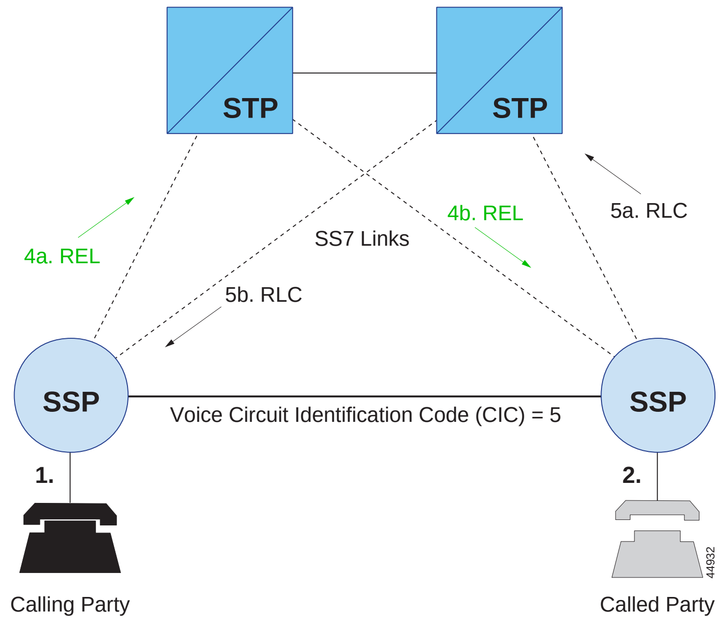
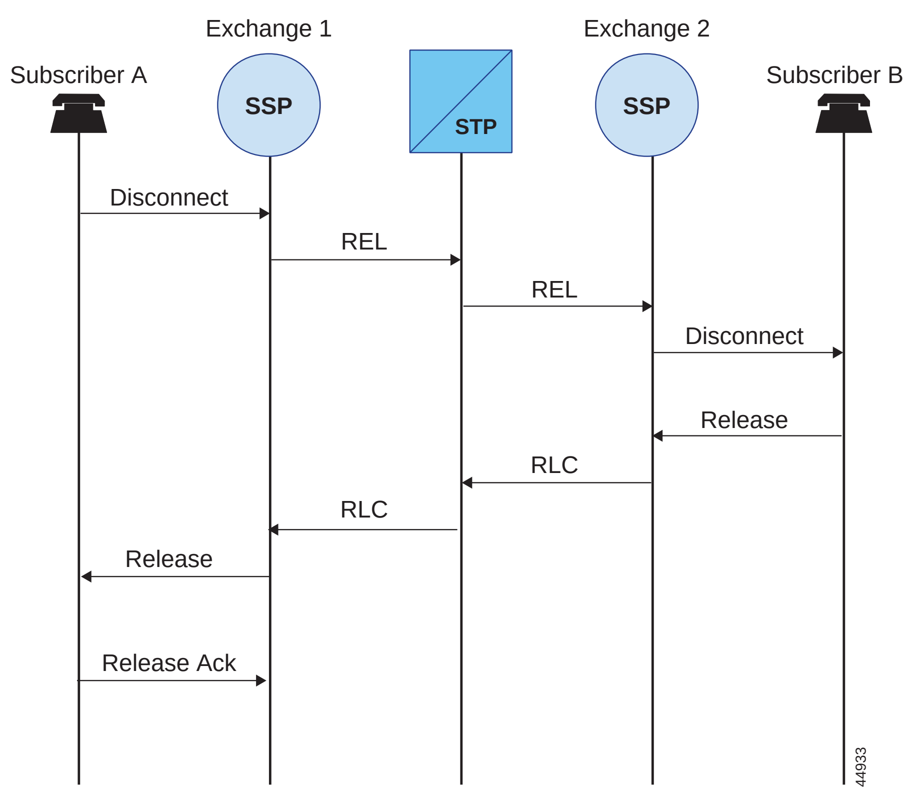


Figure 5-11 ISUP Call Release (2)



TCAP Functions

Transactional Capabilities Application Part (TCAP) enables deployment of advanced intelligent network (AIN) services by supporting information exchange between signaling points using SCCP. TCAP messages are contained within the SCCP portion of a Message Signal Unit (MSU). TCAP messages consist of a transaction portion and a component portion.

An SSP uses TCAP to query an SCP to find out the routing number for an 800, 888 or 900 number. Calling cards are validated using TCAP query and response messages.

Mobile subscribers roaming into a new mobile switching center (MSC) area cause the integrated Visitor Location Register (VLR) to request a service profile from the subscribers Home Location Register (HLR) using the Mobile Application Part (MAP) information carried in TCAP messages.

TCAP Transaction Portion

The transaction portion contains the package type identifier. There are several package types:

- **Unidirectional—**Transfers component(s) in one direction only (no reply expected).
- **Query with Permission**—Initiates a TCAP transaction. The destination node may not end the transaction.
- **Response**—Ends the TCAP transaction. A response to a 1-800 query with permission may contain the routing number(s) associated with the 800 number.
- **Conversation with Permission**—Continues a TCAP transaction. The destination node may not end the transaction.
- **Abort**—Terminates the transaction due to an abnormal situation.

The transaction portion also contains the Originating Transaction ID and Responding Transaction ID which associate the TCAP transaction with a specific application at the originating and destination signaling points.

TCAP Component Portion

The TCAP component portion contains several possible kinds of components:

- **Invoke (Last)—**Invokes an operation. For example, a Query with Permission transaction may include an Invoke (Last) component to request SCP translation of a dialed 800 number. The component is the last component in the query.
- **Invoke (Not Last)—**Similar to the Invoke (Last) component except that the component is followed by one or more components.
- **Return Result (Last)**—Returns the result of an invoked operation. The component is the last component in the response.
- **Return Result (Not Last)—**Similar to the Return Result (Last) component except that the component is followed by one or more components.
- **Return Error**—Reports the unsuccessful completion of an invoked operation.
- **Reject—**Indicates that an incorrect package type or component was received.

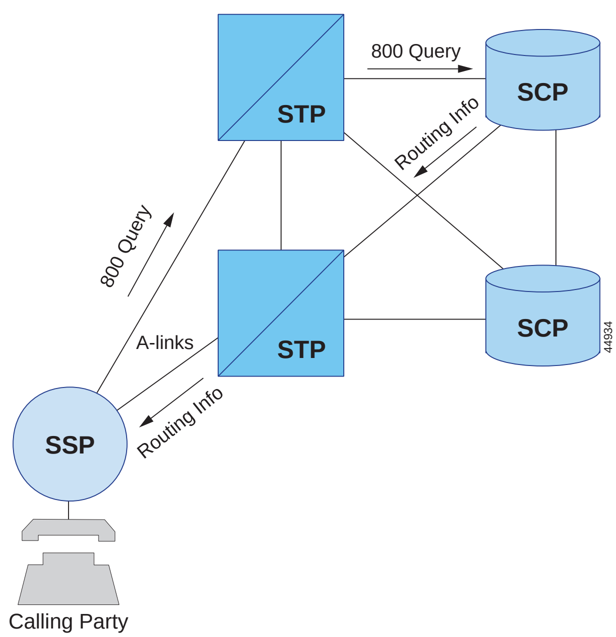
Note Components include parameters which contain application-specific data carried unexamined by TCAP.

Sample TCAP Database Query

This sample query describes how a dialed 800 number is processed using TCAP. See Figure 5-12 as you review the messaging sequence described below.

1. A subscriber goes off-hook and dials an 800 number. The end office switch (SSP) parses the digit string and sends an 800 query message to either of its STPs over its A-link.
2. The STP recognizes the 800 query and routes it to an appropriate database via an SCP.
3. The SCP receives the query, extracts the passed information and retrieves a real telephone number to which the call should be routed.
4. The SCP sends a response message with the information necessary to process the call to the originating SSP via an STP and an A-link.
5. The STP receives the response and routes it to the SSP.
6. The SSP receives the response and uses the information to route the call. It generates an IAM message and proceeds with ISUP call setup.

Figure 5-12 Sample TCAP "800" Number Query



Review: ISUP and TCAP

1. What is the principal function of ISUP?
2. Which field in an MSU carries ISUP information?
3. Define CIC.
4. What is the function of an IAM?
5. What does the receipt of an ACM indicate?
6. Which ISUP message initiates call billing?
7. What is the function of an REL message?
8. What is the response to an REL message?
9. What information is included in an IAM?
10. What happens when a called party goes off-hook?
11. What is the principal function of TCAP?
12. Where in an MSU are TCAP messages located?
13. Briefly describe the two portions of a TCAP message.