Interworking Switched Circuit and Voice-over–IP Networks Tutorial

Definition

The term operations support systems (OSSs) generally refers to the systems that perform management, inventory, engineering, planning, and repair functions for telecommunications service networks.

Overview

Originally, OSSs were mainframe-based, stand-alone systems designed to support telephone company staff members in their daily jobs. Essentially, these systems were designed to make the manual processes through which a telephone network was operated more efficient. Today's service providers, however, are required to manage a much more complex set of services and network technologies in order to remain competitive. As a result, new generations of OSSs are being developed—using state-of-the-art information technology—to address enterprise data information management. These systems make a company's information a more accessible and useful resource for managing the business, providing services, and delivering extraordinary customer care.

This tutorial focuses on the current and near-future states of OSS technology and its development to support emerging and hybrid network technologies. Note that the tutorial focuses only on the service-management layer of the telecommunications management network (TMN) model. Refer to the Web ProForum TMN tutorial (http://www.iec.org/online/tutorials/tmn) for a complete discussion of this model.

Topics

1. Introduction

Telephone companies offload voice calls from public switched telephone networks (PSTN) to voice-over–Internet Protocol (VoIP) networks because it is cheaper to carry voice traffic over Internet protocol (IP) networks than over switched-circuit networks. In the future, IP telephone networks are expected to enable innovative new multimedia services while working seamlessly with legacy telephone networks.

A VoIP network carries voice traffic cheaper than a switched-circuit telephone network because IP–telephony networks make better use of available bandwidth. In a PSTN, for example, a dedicated 64 kilobits per second (kbps) end-to-end circuit is allocated for each call. In a VoIP network, digitized voice data is highly compressed and carried in packets over IP networks. Using the same bandwidth, a VoIP network can carry many times the number of voice calls as a switched circuit network with better voice quality. The savings realized in using VoIP networks are often passed onto users in the form of lower costs.

In 2001, U.S. telephone companies are expected to offload between 15 and 20 percent of overseas voice calls to VoIP network operators such as iBasis, and the percentage is rising each year as VoIP network infrastructure is rolled out. Other countries, such as China, carry an even higher percentage of voice traffic over domestic and international VoIP networks.

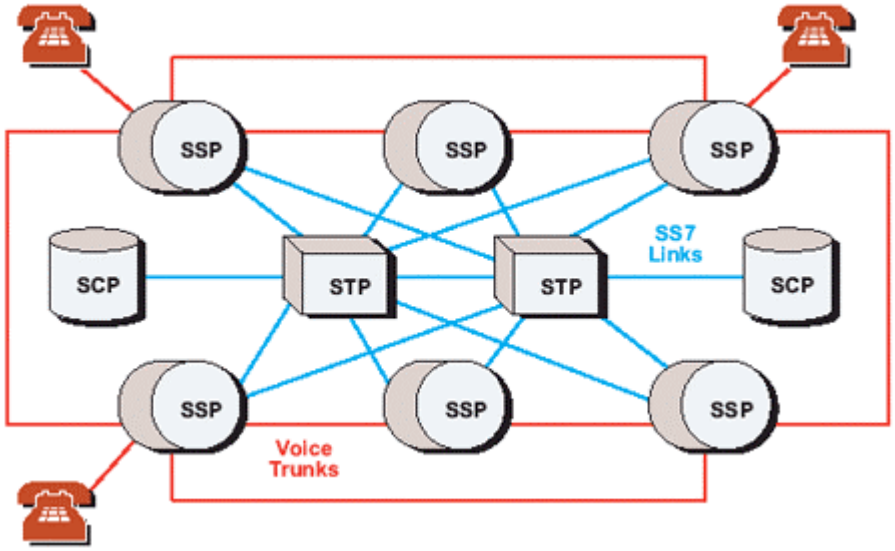
In addition to voice data, signaling data is exchanged between switched-circuit telephone networks and VoIP networks. Signaling information is used to setup, manage, and release voice calls, and support telephony services such as caller ID, toll-free calling, and mobile roaming and authentication.

The remainder of this tutorial introduces the topic of interworking the PSTN and next-generation VoIP networks to support voice calls and telephony services.

2. Signaling in Switched-Circuit and VoIP Networks

Switched-circuit telephone networks use a signaling protocol called Common Channel Signaling System #7 (more commonly called SS7 or C7). For more information, refer to the SS7 tutorial on this site. In the PSTN, signaling endpoints send and receive SS7 signaling messages. There are three kinds of signaling end points: a service switching point (SSP or central office switch), a signal transfer point (STP), and a service control point (SCP).

Figure 1. SS7 Signaling endpoints in a switched-circuit network



In SS7 networks, integrated services digital network (ISDN) user part (ISUP) signaling messages are used to setup, manage, and release trunk circuits that carry voice calls between central-office switches. ISUP messages also carry caller–ID information, such as the calling party's telephone number and name. ISUP is used for both ISDN and non–ISDN calls between central-office switches.

Transaction capabilities application part (TCAP) signaling messages support telephony services, such as toll-free (freephone), calling card, local number portability, and mobile (wireless) roaming and authentication. Mobile services are enabled by information carried in the mobile application part (MAP) of a TCAP message. TCAP supports non-circuit-related information exchange between signaling points using the signaling connection control part (SCCP) connectionless service.

Signaling in VoIP Networks

VoIP networks carry SS7–over–IP using protocols defined by Signaling Transport (sigtran) Working Group of the Internet Engineering Task Force (IETF), the international organization responsible for recommending Internet standards. The sigtran protocols support the stringent requirements for SS7/C7 signaling as defined by International Telecommunication Union (ITU) Telecommunication Standardization Sector.

In IP–telephony networks, signaling information is exchanged between the following functional elements:

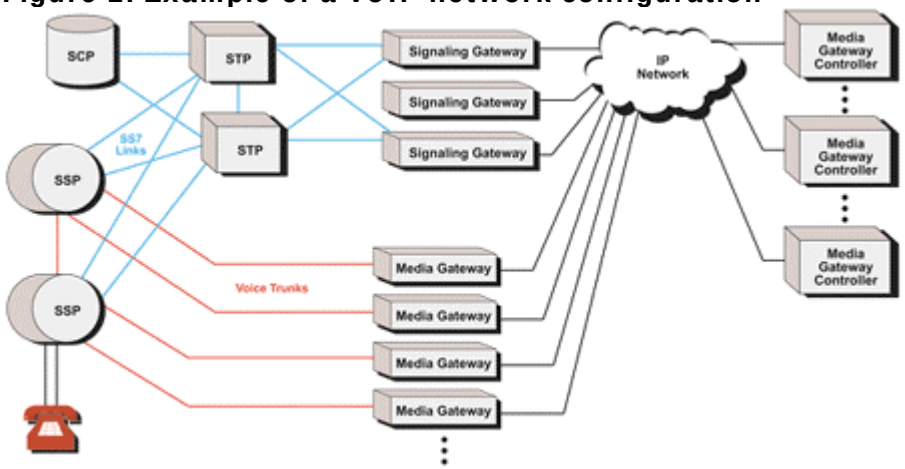
- **Media Gateway**: A media gateway terminates voice calls on inter-switch trunks from the PSTN, compresses and packetizes the voice data, and delivers compressed voice packets to the IP network. For voice calls originating in an IP network, the media gateway performs these functions in reverse order. For ISDN calls from the PSTN, Q.931 signaling information is transported from the media gateway to the media gateway controller (described below) for call processing.

- **Media Gateway Controller**: A media gateway controller handles the registration and management of resources at the media gateway(s). A media gateway controller exchanges ISUP messages with central-office switches via a signaling gateway (described below). Because vendors of media gateway controllers often use off-the-shelf computer platforms, a media gateway controller is sometimes called a softswitch.

- **Signaling Gateway**: A signaling gateway provides transparent interworking of signaling between switched-circuit and IP networks. The signaling gateway may terminate SS7 signaling or translate and relay messages over an IP network to a media gateway controller or another signaling gateway. Because of its critical role in integrated voice networks, signaling gateways are often deployed in groups of two or more to ensure high availability.

A media gateway, signaling gateway, or media gateway controller (softswitch) may be separate physical devices or integrated in any combination.

Figure 2. Example of a VoIP network configuration



Sigtran Protocols

The sigtran protocols specify the means by which SS7 messages can be reliably transported over IP networks. The architecture identifies two components: a common transport protocol for the SS7 protocol layer being carried and an adaptation module to emulate lower layers of the protocol. For example, if the native protocol is message transport layer (MTP) Level 3, the sigtran protocols provide the equivalent functionality of MTP Level 2. If the native protocol is ISUP or SCCP, the sigtran protocols provide the same functionality as MTP Levels 2 and 3. If the native protocol is TCAP, the sigtran protocols provide the functionality of SCCP (connectionless classes) and MTP Levels 2 and 3. The sigtran protocols provide all the functionality needed to support SS7 signaling over IP networks, including:

- flow control
- in-sequence delivery of signaling messages within a single control stream
- identification of the originating and terminating signaling points
- identification of voice circuits
- error detection, retransmission and other error-correcting procedures
- recovery from outages of components in the transit path
- controls to avoid congestion on the Internet
- detection of the status of peer entities (e.g., in service, out-of-service, etc.)

- support for security mechanisms to protect the integrity of the signaling information

- extensions to support security and future requirements

Restrictions imposed by narrowband SS7 networks, such as the need to segment and reassemble messages greater than 272 bytes, are not applicable to IP networks and therefore not supported by the sigtran protocols.

Performance Considerations for SS7 over IP

SS7 messages transported over IP networks must meet the stringent performance requirements imposed by both the ITU SS7/C7 standards and user expectations. For example, while the ITU standard specifies that the end-to-end call-setup delay cannot exceed 20 to 30 seconds after the ISUP initial address message (IAM) is transmitted, users have generally come to expect much faster response times. For this reason, VoIP networks must be engineered to satisfy user expectations and ITU standards for performance.

Security Requirements for SS7 over IP

If signaling messages are transported over a private intranet, security measures can be applied as deemed necessary by the network operator. For signaling messages transported over the public Internet, the use of security measures is mandatory. Several security mechanisms are currently available for use in IP networks. For transmission of signaling information over the Internet, sigtran recommends the use of IPSEC (see RFC2401). IPSEC provides the following security services:

Authentication: to ensure information is sent to/from a known and trusted partner

Integrity: to ensure that the signaling information has not been modified in transit

Confidentiality: to ensure that the transported information is encrypted to avoid illegal use or violation of privacy laws

Availability: to ensure communicating endpoints under attack remain in service for authorized use

The sigtran protocols do not define new security mechanisms as the currently available security protocols provide the necessary mechanisms for secure transmission of SS7 messages over IP networks.

3. SCTP: Stream Control Transmission Protocol

To reliably transport SS7 messages over IP networks, the IETF sigtran Working Group devised the stream control transmission protocol (SCTP), SCTP allows the reliable transfer of signaling messages between signaling endpoints in an IP network.

To establish an association between SCTP endpoints, one endpoint provides the other with a list of its transport addresses (multiple IP addresses in combination with an SCTP port). These transport addresses identify the addresses which will send and receive SCTP packets.

IP signaling traffic is usually composed of many independent message sequences between many different signaling endpoints. SCTP allows signaling messages to be independently ordered within multiple streams (unidirectional logical channels established from one SCTP endpoint to another) to ensure in-sequence delivery between associated endpoints. By transferring independent message sequences in separate SCTP streams, it is less likely that the retransmission of a lost message will affect the timely delivery of other messages in unrelated sequences (called head-of-line blocking). Because TCP/IP does enforce head-of-line blocking, the sigtran Working Group recommends SCTP rather than TCP/IP for the transmission of signaling messages over IP networks.

There are three types of messages in SS7:

- Message signal units (MSU)
- Link-status signal units (LSSU)
- Fill-in signal units (FISU)

MSUs originate at a higher level than MTP Level 2 and are destined for a peer at another node. LSSUs allow peer MTP Level-2 layers to exchange link-status information. FISUs are sent when no other signal units are waiting to be sent across the synchronous link. This purpose is preserved by the heartbeat messages in SCTP. FISUs also carry acknowledgment of messages, a function also assumed by SCTP.

In summary, SCTP provides:

- acknowledged error-free non-duplicated transfer of signaling information
- in-sequence delivery of messages within multiple streams, with an option for order-of-arrival delivery of individual messages

- optional bundling of multiple me
- ssages into a single SCTP packet
- data fragmentation as required
- network-level fault tolerance through support of multihoming at either or both ends of an association
- appropriate congestion-avoidance behavior and resistance to flooding (denial of service) and masquerade attacks

To meet stringent SS7 signaling-reliability and performance requirements for carrier-grade networks, VoIP network operators ensure that there is no single point of failure in the end-to-end network architecture between an SS7 node and a media gateway controller. To achieve carrier-grade reliability in IP networks, links in a linkset are typically distributed among multiple signaling gateways, media gateway controllers are distributed over multiple CPU hosts, and redundant IP network paths are provisioned to ensure survivability of SCTP associations between SCTP endpoints.

4. Transporting MTP Over IP

For MTP messages transported over SS7 or IP networks, the following requirements are specified by the ITU:

- MTP Level-3 peer-to-peer procedures require a response time within 0.5 sec (500 milliseconds) to 1.2 seconds (1200 ms).
- no more than 1 in 10 million messages will be lost because of transport failure.
- no more than 1 in 10,000 million (U.S. terminology: 1 in 10 billion) messages will be delivered out of sequence (including duplicated messages) because of transport failure.
- no more than 1 in 10,000 million (U.S.: 1 in 10 billion) messages will contain an error that is undetected by the transport protocol or 1 in 1,000 million (U.S.: 1 in 1 billion) for American National Standard Institute (ANSI) specifications.
- availability of any signaling route set (the complete set of allowed signaling paths from a given signaling point towards a specific destination) is 99.9998 percent or better (downtime of approximately 10 minutes per year or less).

- the message length (payload accepted) is 272 bytes for narrowband SS7 and 4091 bytes for broadband SS7.

To achieve the functional and performance requirements for MTP, the IETF sigtran Working Group has recommended three new protocols: M2UA, M2PA, and M3UA. Each protocol is described below.

M2UA: MTP2 User Adaptation Layer

M2UA is a protocol defined by the IETF sigtran Working Group for transporting SS7 MTP Level-2 user (i.e., MTP Level-3) signaling messages over IP using the SCTP. The M2UA protocol layer provides the equivalent set of services to its users as MTP Level 2 provides to MTP Level 3.

M2UA is used between the signaling gateway and media gateway controller in VoIP networks. The signaling gateway receives SS7 messages over an MTP Level-1 and Level-2 interface from a signaling end point (SCP or SSP) or signal transfer point (STP) in the public-switched telephone networks. The signaling gateway terminates the SS7 link at MTP Level 2 and transports MTP Level 3 and above to a media gateway controller or other IP endpoint using M2UA over SCTP/IP.

M2PA: MTP2 User Peer-to-Peer Adaptation Layer

Like M2UA, M2PA is a sigtran protocol for transporting SS7 MTP Level-2 user-part-signaling messages (i.e., MTP Level 3) over IP using the SCTP. Unlike M2UA, M2PA is used to support full MTP Level-3 message handling and network management between any two SS7 nodes communicating over an IP network. IP signaling points function as traditional SS7 nodes using the IP network instead of the SS7 network. Each switched circuit or IP signaling point has an SS7 point code. The M2PA protocol layer provides the same set of services as MTP Level 2 provides to MTP Level 3.

M2PA can be used between a signaling gateway and a media gateway controller, between a signaling gateway and an IP signaling point, and between two IP signaling points. Signaling points may use M2PA over IP or MTP Level 2 over standard SS7 links to send and receive MTP Level-3 messages.

M2PA facilitates the integration of SS7 and IP networks by enabling nodes in switched-circuit networks to access IP–telephony databases and other nodes in IP networks using SS7 signaling. Conversely, M2PA allows IP telephony applications to access SS7 databases, such as local-number portability, calling card, freephone, and mobile-subscriber databases. In addition, using M2UA over

IP may result in cost advantages if traditional SS7 links are replaced by IP connections.

In summary, M2PA and M2UA differ in the following ways:

- M2PA: the signaling gateway is an SS7 node with a point code;
  M2UA: the signaling gateway is not an SS7 node and has no point code.

- M2PA: the connection between the signaling gateway and IP signaling points is an SS7 link;
  M2UA: the connection between the signaling gateway and the media gateway controller is not an SS7 link. Rather, it is an extension of MTP from the signaling gateway to the media gateway controller.

- M2PA: the signaling gateway can have upper SS7 layers, such as SCCP;
  M2UA: the signaling gateway has no upper SS7 layers as it has no MTP Level 3.

- M2PA: relies on MTP Level 3 for management procedures;
  M2UA: uses M2UA management procedures.

- M2PA: IP signaling points processes MTP Level-3 and MTP Level-2 primitives;
  M2UA: the media gateway controller transports MTP Level-3 and MTP Level-2 primitives to the signaling gateway's MTP Level 2 for processing.

M3UA: MTP Level-3 User-Adaptation Layer

M3UA is a protocol defined by the IETF sigtran Working Group for transporting MTP Level-3 user-part signaling messages (e.g., ISUP, TUP, and SCCP) over IP using the SCTP. TCAP or RANAP messages, as SCCP user protocols, may be carried by SCCP using M3UA or by a different sigtran protocol called SUA, as described below.

M3UA is used between a signaling gateway and a media gateway controller or IP–telephony database. The signaling gateway receives SS7 signaling using MTP as transport over a standard SS7 link. The signaling gateway terminates MTP Level 2 and MTP Level 3 and delivers ISUP, TUP, SCCP and/or any other MTP Level-3 user messages, as well as certain MTP network-management events, over SCTP associations to media gateway controllers or IP–telephony databases.

The ISUP and/or SCCP layer at an IP signaling point is unaware that the expected MTP Level-3 services are not provided locally, but rather by the remote-signaling gateway. Similarly, the MTP Layer-3 at a signaling gateway may be unaware that its local users are actually remote parts over M3UA. Conceptually, M3UA extends access to MTP Layer-3 services at the signaling gateway to remote

IP endpoints. If an IP endpoint is connected to more than one signaling gateway, the M3UA layer at the IP endpoint maintains the status of configured SS7 destinations and route messages according to the availability and congestion status of the routes to these destinations via each signaling gateway.

M3UA does not impose a 272-octet signaling information field (SIF) length limit as specified by SS7 MTP Level 2. Larger information blocks can be accommodated directly by M3UA/SCTP without the need for an upper-layer segmentation/reassembly procedure as specified by the SCCP and ISUP standards. However, a signaling gateway will enforce the maximum 272-octet limit when connected to a SS7 network that does not support the transfer of larger information blocks to the destination. For broadband MTP networks, the signaling gateway will fragment ISUP or SCCP messages larger than 272 octets as required.

At the signaling gateway, the M3UA layer provides interworking with MTP Layer-3 management functions to support seamless operation of signaling between the SS7 and IP networks. For example, the signaling gateway indicates to remote MTP Layer-3 users at IP endpoints when an SS7 signaling point is reachable or unreachable or when SS7 network congestion or restrictions occur. The M3UA layer at an IP endpoint keeps the state of the routes to remote SS7 destinations and may request the state of remote SS7 destinations from the M3UA layer at the signaling gateway. The M3UA layer at an IP endpoint may also indicate to the signaling gateway that M3UA at an IP endpoint is congested.

5. Transporting SCCP over IP

SCCP user adaptation layer (SUA) is a protocol defined by the IETF sigtran Working Group for transporting SS7 SCCP user part signaling messages (e.g., TCAP and RANAP) over IP using the SCTP. SUA is used between a signaling gateway and an IP signaling endpoint and between IP signaling endpoints. SUA supports both SCCP unordered and in-sequence connectionless services and bidirectional connection-oriented services with or without flow control and detection of message loss and out-of-sequence errors (i.e., SCCP protocol classes 0 through 3).

For connectionless transport, SCCP and SUA interface at the signaling gateway. From the perspective of an SS7 signaling point, the SCCP user is located at the signaling gateway. SS7 messages are routed to the signaling gateway based on point code and SCCP subsystem number. The signaling gateway then routes SCCP messages to the remote IP endpoint. If redundant IP endpoints exist, the signaling gateway(s) can load share amongst active IP endpoints using a round-robin approach. Note that load sharing of TCAP messages occurs only for the first message in a TCAP dialogue; subsequent TCAP messages in the same dialogue are always sent to the IP endpoint selected for the first message, unless endpoints

share state information and the signaling gateway is aware of the message allocation policy of the IP endpoints. The signaling gateway may also perform global title translation (GTT) to determine the destination of an SCCP message. The signaling gateway routes on global title, i.e., digits present in the incoming message, such as called-party number or mobile-subscriber identification number.

For connection-oriented transport, SCCP and SUA interface at the signaling gateway to associate the two connection sections needed for connection-oriented data transfer between an SS7 signaling endpoint and an IP endpoint. Messages are routed by the signaling gateway to SS7 signaling points based on the destination point code (in the MTP Layer-3 address field) and to IP endpoints based on IP address (in the SCTP header).

SUA can also be used to transport SCCP user information between IP endpoints directly rather than via the signaling gateway. The signaling gateway is needed only to enable interoperability with SS7 signaling in the switched-circuit network.

If an IP resident application is connected to multiple signaling gateways, multiple routes may exist to a destination in the SS7 network. In this case, the IP endpoint must monitor the status of remote signaling gateways before initiating a message transfer.

6. SIP, PINT, SPIRITS, ENUM, TRIP

Session initiation protocol (SIP) is a signaling protocol for creating, modifying, and terminating sessions, such as IP voice calls or multimedia conferences, with one or more participants in an IP network. SIP is currently undergoing standardization by the IETF SIP Working Group. While the sigtran protocols are currently the protocols of choice for interworking IP networks with the PSTN, SIP is the protocol of choice for converged communications networks in the near future.

SIP provides the following functions:

- **Name Translation and User Location**: to ensure that a call reaches the called party regardless of location, SIP addresses users by an e-mail-like address. Each user is identified through a hierarchical URL built around elements such as a user's telephone number or host name (for example, SIP:user@company.com). Because of this similarity, SIP URLs are easy to associate with a user's e-mail address.

- **Feature Negotiation**: SIP allows all parties involved in a call to negotiate and agree on the features supported, recognizing that all participants may not be able to support the same kind of features. For example, a session between a mobile voice-only telephone user and two

video-enabled device users would agree to support voice features only. When the mobile telephone user leaves the call, remaining participants may renegotiate session features to activate video communications.

- **Call Participant Management**: during a session, a participant can bring other users into the call or transfer, hold, or cancel connections.

SIP Protocol Components

SIP has two basic components: the SIP user agent and the SIP network server. The user agent is effectively the end-system component for the call and the SIP network server is the network device that handles the signaling associated with multiple calls. The SIP user agent consists of the user agent client (UAC) which initiates calls and the user agent server (UAS) which answers calls. This architecture allows peer-to-peer calls to be made using a client-server protocol.

The SIP network server element consists of three forms of server: the SIP stateful proxy server, the SIP stateless proxy server, and the SIP redirect server. The main function of the SIP servers is to provide name resolution and user location, as callers are unlikely to recall the IP address or host name of called parties. Using an easier-to-remember e-mail-like address, the caller's user agent can identify a specific server (or server cluster) to resolve called-party address information.

SIP provides its own reliable transfer mechanism independent of the packet layer. For this reason, SIP does not require the services of the sigtran SCTP protocol and functions reliably over an "unreliable" datagram protocol like user diagram protocol (UDP).

SIP-T
SIP–T (SIP for telephones) is a mechanism that allows SIP to be used for ISUP call setup between SS7–based public switched telephone networks and SIP–based IP telephony networks. SIP–T carries an ISUP message payload in the body of a SIP message. The SIP header carries translated ISUP routing information. SIP–T also specifies the use of the SIP INFO method for effecting in-call ISUP signaling in IP networks.

PINT and SPIRITS
Sigtran is not the only IETF working group involved in defining new protocols to enable the integration of the PSTN with IP networks. PINT (PSTN and Internet Interworking) and SPIRITS (Service in the PSTN/IN Requesting Internet Service) are two IETF working-group recommendations that address the need to interwork telephony services between the PSTN and the Internet. PINT deals with services originating from an IP network; SPIRITS deals with services originating from the PSTN.

In PINT, PSTN network services are triggered by IP requests. An SIP Java client embedded in a Java servlet on a Web server launches requests to initiate voice calls on the PSTN. The current focus of this initiative is to allow Web access to voice content and enable click-to-dial/fax services. In SPIRITS, IP network services are triggered by PSTN requests. SPIRITS is primarily concerned with Internet call waiting, Internet caller–ID delivery, and Internet call forwarding.

ENUM

The IETF's ENUM (telephone number resolution) Working Group is devising a scheme to map E.164 telephone numbers to IP addresses using the Internet domain name server (DNS) so that any application, including SIP, can discover resources associated with a unique phone number. An SIP phone or proxy server would use number domain translation and DNS resolution to discover a DNS resource that would yield an SIP address at which a dialed number could be reached.

TRIP

The IPTEL working group is developing TRIP (telephony routing over IP), a policy-driven inter-administrative domain protocol for advertising the reachability of telephony destinations between location servers, and for advertising attributes of the routes to those destinations. TRIP is designed to allow service providers to exchange routing information to avoid over-provisioning or duplication of gateways using established Internet protocols.

If a telephone number does not have an associated SIP resource, the IP network routes the call to a telephone-routing gateway, which connects to the PSTN. In an interconnect environment with many peering relationships between service providers, resources in the IP network need to discover which telephone numbers are associated with which gateways.

Self-Test

1. The SS7 protocol is required to enable telephone calls between the PSTN and IP networks.

a. true

b. false

2. The SS7 protocol enables an Internet telephony switch to support which of the following?

a. toll-free calling

b. calling-card calling

c. local number portability

d. all of the above

3. Each Internet telephony media gateway needs its own dedicated SS7 link.

a. true

b. false

4. Supporting a large Internet telephony switch with over 1,000 trunks can cause _____.

a. inefficient use of the SS7 signaling links

b. excessive delays across the IP network

c. network congestion in the local loop

d. signal degradation in the PSTN

5. The media gateway controller, billing, and database application modules in a distributed IP telephony switch run on which of the following?

a. the same machine

b. different machines in the same CO

c. different machines distributed around the network

d. any of the above

6. A mated pair of SS7/IP gateways can support which of the following?

a. multiple media gateways and media gateway controllers

b. load sharing among redundant IP–telephony modules

c. primary and alternate routes

d. all of the above

7. IP networks provide guaranteed bandwidth for each phone call.

a. true

b. false

8. The voice/data and signaling packets on IP networks have all been standardized to enable interoperability between multiple IP–telephony vendors.

a. true

b. false

9. A single SS7 link can support more than 1,000 trunks.

a. true

b. false

10. An SS7/IP gateway can support multiple distributed IP–telephony switches with a single point code.

a. true

b. false

11. IP–telephony switches can support calls from which of the following?

a. the PSTN to the IP network

b. the PSTN to the PSTN via the IP network

c. the IP network to the PSTN

d. the IP network to the IP network

e. all of the above

Correct Answers

1. The SS7 protocol is required to enable telephone calls between the PSTN and IP networks.

a. true

b. false

See Topic 1

2. The SS7 protocol enables an Internet telephony switch to support which of the following?

a. toll-free calling

b. calling-card calling

c. local number portability

c. all of the above

See Topic 1

3. Each Internet telephony media gateway needs its own dedicated SS7 link.

a. true

b. false

See Topic 5

4. Supporting a large Internet telephony switch with over 1,000 trunks can cause _____.

a. inefficient use of the SS7 signaling links

b. excessive delays across the IP network

c. network congestion in the local loop

d. signal degradation in the PSTN

See Topic 4

5. The media gateway controller, billing, and database application modules in a distributed IP telephony switch run on which of the following?

a. the same machine

b. different machines in the same CO

c. different machines distributed around the network

d. any of the above

6. A mated pair of SS7/IP gateways can support which of the following?

a. multiple media gateways and media gateway controllers

b. load sharing among redundant IP–telephony modules

c. primary and alternate routes

d. all of the above

See Topic 6

7. IP networks provide guaranteed bandwidth for each phone call.

a. true

b. false

See Topic 1

8. The voice/data and signaling packets on IP networks have all been standardized to enable interoperability between multiple IP–telephony vendors.

a. true

b. false

See Topic 7

9. A single SS7 link can support more than 1,000 trunks.

a. true

b. false

See Topic 3

10. An SS7/IP gateway can support multiple distributed IP–telephony switches with a single point code.

a. true

b. false

See Topic 6

11. IP–telephony switches can support calls from which of the following?

a. the PSTN to the IP network

b. the PSTN to the PSTN via the IP network

c. the IP network to the PSTN

d. the IP network to the IP network

e. all of the above

See Topic 2

Glossary

C7
Common Channel Signaling System 7 (also called "SS7")

ISDN
Integrated Services Digital Network

ISUP
Signaling System 7 ISDN User Part

M2PA
MTP Level-2 Peer-to-Peer Adaptation Layer

M2UA
MTP Level-2 User Adaptation Layer

M3UA
MTP Level-3 User Adaptation Layer

MAP
Mobile Application Part

MTP
Signaling System 7 Message Transfer Part

PLMN
Public Land Mobile Network

PSTN
Public Switched Telephone Network

SCCP
SS7 Signaling Connection Control Part

SEP
Signaling Endpoint

SCP
SS7 Service Control Point

SS7
Common Channel Signaling System No. 7 (also called "C7")

SSP
SS7 Service Switching Point (also called a "central office" switch)

STP
SS7 Signal Transfer Point

SUA
SCCP User Adaptation Layer

TCAP
Signaling System 7 Transaction Capabilities Part

TCP
Transmission Control Protocol (often called "TCP/IP")