

Cisco IP Transfer Point

MTP3 User Adaptation (M3UA) and SCCP User Adaptation (SUA) Signaling Gateway

Executive Overview

Today's mobile operators have two primary business drivers: to lower costs as their networks grow to meet subscriber demand and to provide services that grow revenue streams and encourage subscriber acquisition and retention. Migrating the Signaling System 7 (SS7) network to an all-IP network provides operators the ability to achieve success in both areas.

The Cisco ITP is the company's product family for transporting SS7 signaling traffic over IP networks. The initial Cisco IP Transfer Point release, via support for the IETF's Signaling Transport (SIGTRAN) MTP2-User Peer-to-Peer Adaptation layer (M2PA) protocol, provided the first step in this migration by offloading selected SS7 traffic from expensive time-division multiplexing (TDM) networks to more cost-effective IP networks. This latest release of Cisco IP Transfer Point offers features, via SIGTRAN's MTP3-User Adaptation (M3UA) and SCCP-User Adaptation (SUA) layer protocols, that extend the migration by allowing IP-enabled end nodes and applications access to the legacy SS7 network.

Improving Network Efficiency

The transaction capacity of new high-performance signaling endpoints (SEPs), such as home location registers (HLRs), short message service centers (SMSCs), and signaling control points (SCPs), exceeds what traditional SS7 networks can deliver. The quest to fully use these applications and deploy them in a cost-effective and efficient manner has been a goal of operators. Until now, attempts to accomplish this have been costly and limited due to legacy SS7 network constraints.

The Cisco ITP M3UA/SUA signaling gateway breaks through the traditional SS7 limitations providing a high-performance, scalable solution able to deliver signaling traffic to fully use these applications. This allows the operator to realize higher return on investment for the SCP applications as well as savings on TDM and signaling transfer point (STP) costs.



Enabling Revenue-Generating Applications and Services

The SS7-over-IP (SS7oIP) signaling gateway allows companies to rapidly deploy emerging IP-based applications and services. The mobile Internet/intranet must take the same open approach as the wireline Internet, where entrepreneurial vendors can enter the market with unique and compelling applications and services. To be successful, these applications must be IP-based in order to run seamlessly over second-generation (2G), 2.5G, and third-generation (3G) wireless networks, and to scale as networks and subscriber bases grow.

These advanced applications and services provide the operator a source for new revenues. They also provide a means to acquire new subscribers and improve existing customer loyalty resulting in an increased customer base.

The Core Network Infrastructure

The core network infrastructure must be technically open to offer flexibility and adapt to a wide variety of applications and service offerings. Enabling new applications and services via the legacy intelligent network (IN) and advanced intelligent network (AIN) has proven cumbersome and arcane to a small, closed community of developers. Lowering barriers to entry, SS7oIP can fulfill the promise made by IN/AIN. Open standards lower market-entry barriers for application vendors. With the M3UA/SUA signaling gateway feature, the Cisco IP Transfer Point extends the ability for operators to achieve their objectives using a standards-based IP network.

SS7oIP Overview

The Internet Engineering Task Force (IETF) created the SIGTRAN working group to develop a set of standard protocols for transporting legacy SS7 signaling over IP networks (SS7oIP). The standards have been developed to address lower-layer functions first, providing SS7-equivalent redundancy and availability. Building on this foundation, mechanisms for transporting, or backhaul of, SS7 signaling to IP-based endpoints were added.

Visit the SIGTRAN home page at: <http://www.ietf.org/html.charters/sigtran-charter.html> for more information.

The protocols supported by the Cisco IPT family of IP transfer points are:

- Stream Control Transmission Protocol (SCTP, RFC2960) is the transport layer, similar to Transmission Control Protocol (TCP), and provides reliable data transfer, multiple streams, bundling and fragmentation of data, congestion and flow control, multihoming for added reliability, and other features. SCTP is the transport layer for the Cisco ITP product family.
- MTP2-User Peer-to-Peer Adaptation (M2PA, Internet-Draft status) together with SCTP provides MTP3 with equivalent transport layer services as MTP2. The Cisco ITP products implement M2PA to offload MTP3 messages from the legacy SS7 network.
- MTP3-User Adaptation (M3UA, Internet-Draft status) is a client/server protocol that provides a gateway to the legacy SS7 network for IP-based applications that interface at the MTP3 layer, for example ISDN-user part (ISUP) and signaling connection control part (SCCP). The Cisco ITP products implement M3UA.
- SCCP-User Adaptation (SUA, Internet-Draft status) is a client/server protocol that provides a gateway to the legacy SS7 network for IP-based applications that interface at the SCCP layer, for example transaction capabilities application part (TCAP). The Cisco ITP products implement SUA.

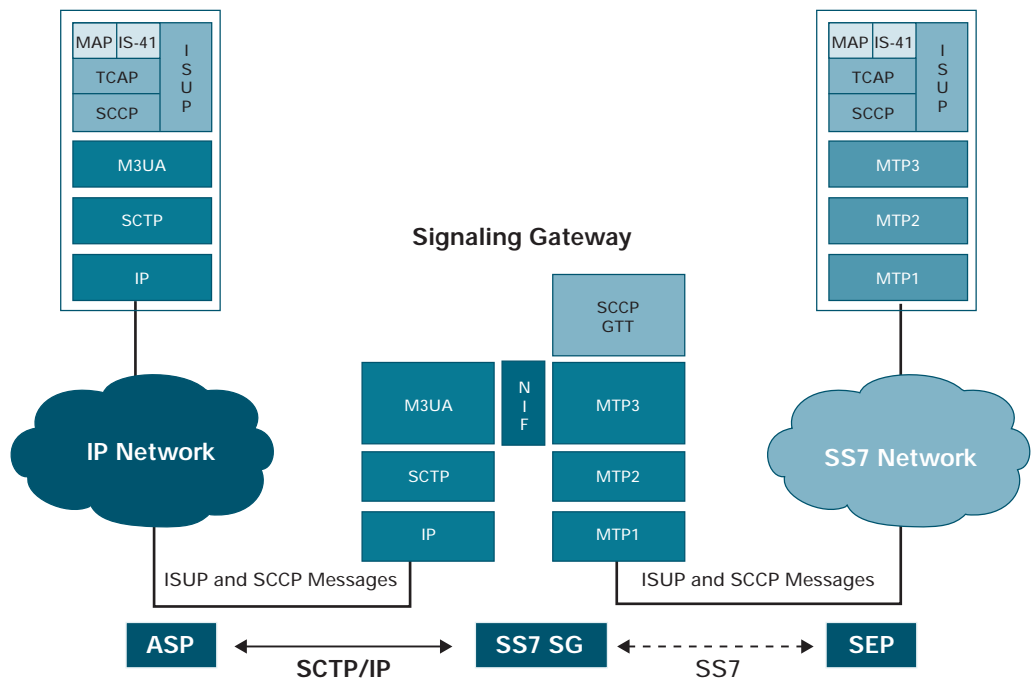


M3UA and SUA

M3UA describes a transport mechanism for delivering SS7 MTP3-User Part messages as well as certain MTP network management events over SCTP transport to IP-based application endpoint. The M3UA signaling gateway terminates the SS7 MTP2 and MTP3 protocol layers and delivers ISUP, SCCP and/or any other MTP3-User protocol messages. The application server process (ASP) is the signaling gateway's component of a process or database (for example, call agents, HLRs, and so on) existing on an application endpoint.

Figure 1 depicts the relationship between the legacy SS7 service control point, the M3UA signaling gateway, the IP-based ASP, and the protocol stacks.

Figure 1 M3UA-Based Architecture



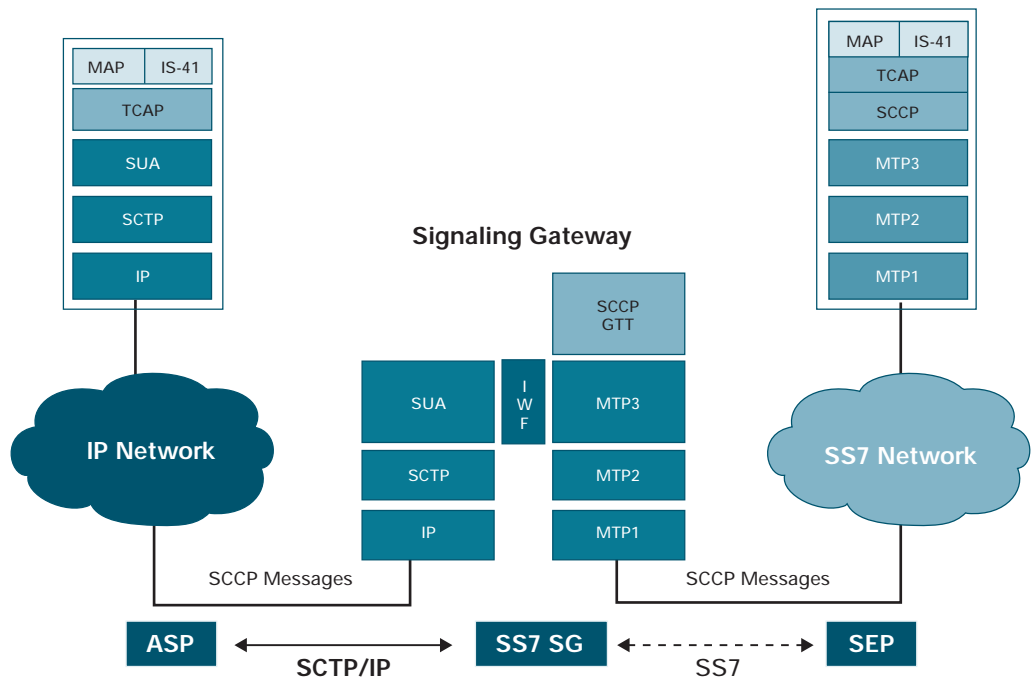
In Figure 1, the legacy SS7 SCP on the right uses MTP1, MTP2, and MTP3 for transporting SCCP and ISUP messages into the network. The signaling gateway terminates the SS7 links, translates the MTP3 messages into M3UA messages, and transports them to the ASP over SCTP/IP. M3UA at the ASP delivers SCCP and ISUP to the application in a manner equivalent to MTP3.

SUA describes a transport mechanism for delivering SS7 SCCP-User Part messages as well as certain SCCP network management events over SCTP transport to IP-based application endpoint. The SUA signaling gateway terminates the SS7 MTP2, MTP3, and SCCP protocol layers and delivers TCAP, radio access network application part (RANAP) and/or any other SCCP-User protocol messages. The ASP is the signaling gateway's component of a process or database (for example, call agents, HLRs, and so on) existing on an application endpoint.



Figure 2 depicts the relationship between the legacy SS7 service control point, the SUA signaling gateway, the IP-based ASP, and the protocol stacks.

Figure 2 UA-Based Architecture



In Figure 2 the legacy SS7 SCP on the far right uses MTP1, MTP2, and MTP3 for transporting SCCP messages into the network. The signaling gateway terminates the SS7 links, translates the SCCP messages into SUA messages, and transports them to the ASP over SCTP/IP. SUA at the ASP delivers TCAP to the application in a manner equivalent to SCCP.

Routing Keys, Application Server and ASP

The signaling gateway routes messages to the appropriate destination based on a routing key. The routing key is defined by an implementation dependent set of parameters that are used to filter SS7 messages. A routing key can be defined using combinations of the following parameters:

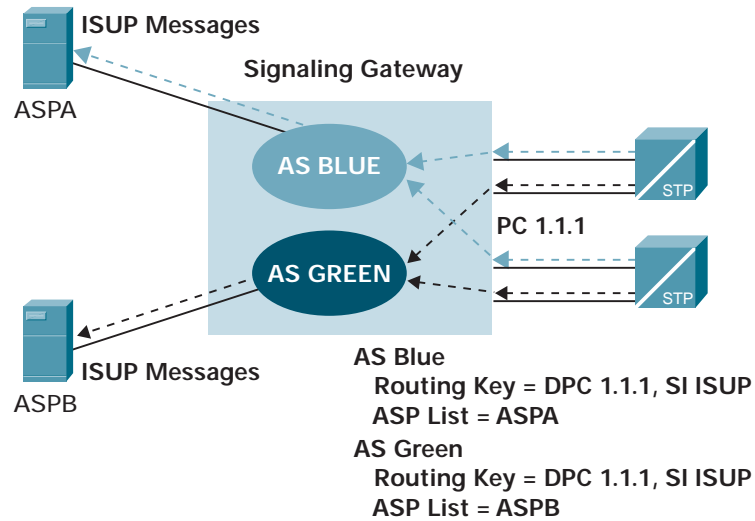
- Destination point code (DPC) (the minimum requirement)
- Origination point code (OPC)
- Service Indicator (SI)
- ISUP circuit identifier code (CIC)
- SCCP subsystem number
- Global title

The application server is a logical entity serving a specific routing key. An application server contains a set of one or more unique ASPs, which process the messages.



Figure 3 describes how a signaling gateway, at point code 1.1.1, routes ISUP messages to one ASP, ASPA, and SCCP messages to a second ASP, ASPB.

Figure 3 Routing Key Example



The signaling gateway routes messages belonging to a specific application server (for example, matching routing key) to one or more of the ASPs that are serving that application server. The ASP is selected based on the current traffic mode of the application server.

Traffic Modes

M3UA and SUA support three traffic modes: Over-ride, Load-share, and Broadcast.

An ASP sends the ASP Active message to a signaling gateway to indicate that it is ready to process signaling traffic for a particular application server. The ASP indicates its desired traffic mode in the Active message.

- The Over-ride value indicates that the ASP will take over all traffic in an application server, over-riding any currently active ASPs in the application server.
- In Load-share mode the ASP will share in the traffic distribution with any other currently active ASPs. The signaling gateway's load sharing algorithm is implementation-dependent.
- In Broadcast mode, the ASP will receive the same messages as any other currently active ASP.

Point Codes

Because the application server effectively represents an MTP3 user, it has its own point code. This is required for the signaling gateway to report management messages to the rest of the SS7 network. The application server point code is the minimum requirement within its routing key. The application server can share the signaling gateway's point code. A group of application servers can also share a single point code.

A Signaling Point Management Cluster (SPMC) is the complete set of application servers that is represented to the SS7 network under a single point code.

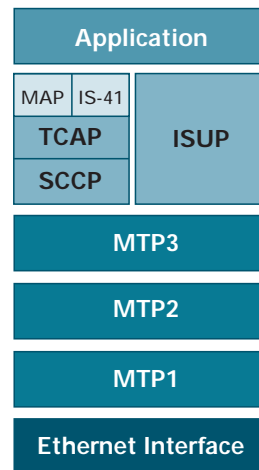


Application Platform Architectures

Legacy SS7 Architecture

Today, for applications to access information from the intelligent network the computing platform must provide legacy SS7 connectivity hardware and software. Figure 4 represents a typical application platform.

Figure 4 Legacy Protocol Stack



The application platform must have a T1/E1/V.35 interface card that provides a TDM link to an SS7 device, such as an STP. Software to support the MTP protocol stacks must also be present. An ISUP stack is necessary for applications that provide call control features. Applications that require information from mobile application part (MAP) or IS-41 require an SCCP stack and a TCAP stack.

Traditional telecommunications infrastructure vendors typically develop their own proprietary platforms and the standard SS7 protocol stacks to support their applications.

Application vendors who wish to offer new and innovative applications to operators typically select a standard platform, such as Solaris or NT, add a T1/E1 interface card, and license the SS7 stack from a software vendor. There are numerous vendors that provide SS7 connectivity solutions.

However, this is an expensive and complex solution, requiring a unique hardware interface and significant software investment. The scalability of these systems is also limited by the CPU requirements for MTP2 processing, the bandwidth of the SS7 links, and physical port capacity. Increasing transaction throughput requires additional hardware for more SS7 links. Migrating to an all-IP platform reduces costs and results in less complex systems.

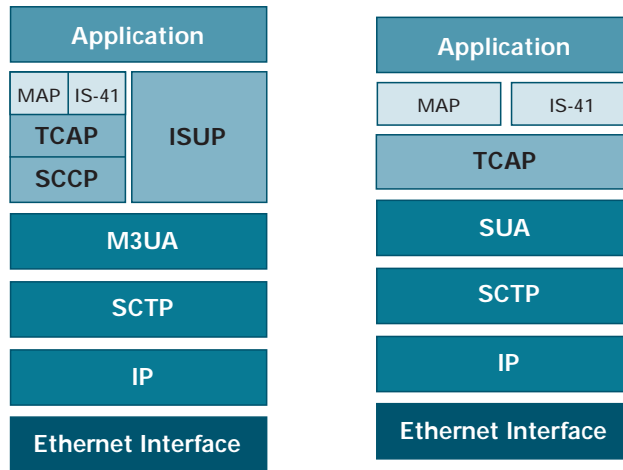
IP-Based Architecture

Today's standard platforms have Ethernet connectivity and support IP. This provides an initial reduction in platform cost and complexity while providing increased bandwidth.

For those applications that require ISUP support, the M3UA protocol must be used. Figure 5 represents the protocol architecture for this type of platform. Note that applications requiring access to MAP, IS-41, and other TCAP users can be supported, but the standard SCCP stack must be implemented to interface with M3UA.



Figure 5 SIGTRAN M3UA and SUA Protocol Stacks



Cisco IP Transfer Point Features

Standard Cisco IOS Software

The Cisco ITP features are implemented as part of the standard Cisco IOS® Software, and are currently supported on the proven and widely deployed Cisco 2600, 7200VXR, and 7500 Series router platforms. This offers several significant advantages.

- The Cisco IP Transfer Point may support many of the standard Cisco IOS features that customers may require, such as:
 - IP media: ATM, Gigabit Ethernet, Packet over SONET
 - IP Version 6 (IPv6), IPv4 to IPv6 translation and tunneling, quality of service (QoS) for IPv6
 - Network Address Translation
 - Firewalling
 - Mobile IP
 - Security features such as Remote Access Dial-In User Service (RADIUS) authentication, authorization, and accounting (AAA)
 - Voice over IP (VoIP)
- The goal of operators is an IP network extended end to end with no TDM links. When arriving at this point in the network evolution all that is required is a pure IP router with a global title translation (GTT) function for title routing and application load balancing. As part of Cisco IOS Software, the Cisco IP Transfer Point will always be supported on high-end carrier-class platforms that support all IP routing platforms. The customer's investment is protected as the network evolves.



M3UA/SUA Signaling Gateway

The Cisco ITP M3UA/SUA signaling gateway implements SIGTRAN standard M3UA and SUA, which is used for transporting SS7 signaling information to IP-based applications. Both M3UA and SUA are currently in draft status within the IETF. The Cisco IP Transfer Point will remain compliant with the 'latest' draft.

The Cisco ITP M3UA/SUA signaling gateway supports the following features:

- Full routing key configuration
- Complete traffic mode operation (Over-ride, Load-share and Broadcast)
- Complete signaling network management operation:
 - Destination unavailable (DUNA)
 - Destination available (DAVA)
 - Destination state audit (DAUD)
 - Signaling congestion (SCON)
 - Destination user part unavailable (DUPU)
 - Destination restricted (DRST)
- Complete ASP state and traffic maintenance operation:
 - ASP up (ASPUP)
 - ASP up acknowledgement (UPACK)
 - ASP down (ASPDN)
 - ASP down acknowledgement (DOWN ACK)
 - ASP active (and acknowledgement)
 - ASP inactive (and acknowledgement)
- SUA SCCP connectionless traffic (classes 0 and 1):
 - Connectionless data transfer (CLDT)
 - Connectionless data response (CLDR)
- Acknowledgement of heartbeat (BEAT)
- Concurrent support of M3UA, SUA, and M2PA
- Global Title address-prefix conversion (for example, E.212 to E.214)

The initial release of the Cisco ITP M3UA/SUA signaling gateway does not support:

- Dynamic registration request for routing keys
- Multiple network appearances
- SUA connection-oriented traffic
- Initiation of heartbeat (BEAT)



Load-Sharing Algorithm

When the traffic mode for an application server is determined to be Load-sharing, the Cisco IP Transfer Point uses a round-robin algorithm for selecting the appropriate ASP for sending messages. The Cisco IP Transfer Point maintains a list of active ASPs within an application server. When the first MSU is received it is sent to the first active ASP in the list for processing. When the next MSU is received it is sent to the next active ASP for processing, and so forth.

For Muses that belong to a single transaction or procedure (for example, TCAP transaction, ISUP call setup), the same ASP must be selected for processing. The concept of binding is applied to the ASP selection for maintaining proper sequencing. The binding is based on a load-share 'seed,' which is a parameter or set of parameters in an MSU and is traffic type dependent. For the Cisco IP Transfer Point's load-sharing algorithm, the seed can be either:

- DPC/OPC/CIC of the MSU for ISUP traffic.
- Signaling link selection (SLS) value for SCCP class 1. (Class 0 traffic does not require binding.)

When load-sharing is based on a load-share seed, the Cisco IP Transfer Point will first check to see if the load-share seed in the MSU has been bound to a specific ASP. If so, then the MSU will be directed to that ASP. If not, the Cisco IP Transfer Point will select the next active ASP, bind the load-share seed to that ASP, and direct the MSU to that ASP.

The first load-share seed received by the Cisco IP Transfer Point will be assigned to the first active ASP in the application server list. The second unique seed will be assigned to the next active ASP in the application server list, and so forth. When an ASP becomes inactive, all seed bindings for that ASP are cleared. Subsequent traffic with load-share seeds formerly bound to that ASP is distributed to other active ASPs in the list.

Point Code Usage

The Cisco ITP M3UA/SUA signaling gateway supports the following point code assignment and usage:

- The Cisco IP Transfer Point is assigned a point code. Any application server provisioned on the Cisco IP Transfer Point can share that point code.
- The Cisco IP Transfer Point can be assigned a Capability point code (or Alias point code). Any application server provisioned on the Cisco IP Transfer Point can use that point code. The application server is sharing the point code with the Cisco IP Transfer Point's mated-pair.
- An application server may have its own unique point code.
- An ASP can be assigned a unique point code by being the only ASP in an application server that has been assigned a unique point code.
- A group of application servers may share a common point code. This is referred to as a signaling point management cluster.

The Cisco IP Transfer Point reports SS7 management messages based on application server states. Special care should be taken when assigning more than one application server to the same point code. For example, if two application servers share a common point code and all of the active ASPs in one of the application servers become inactive, the Cisco IP Transfer Point cannot report a transfer prohibited (TFP) to the SS7 network. This is because the other application server sharing that point code remained active. Therefore the point code was still available.



Routing Key Assignment

The Cisco IP Transfer Point's options for routing key assignments for M3UA are DPC, OPC, and SI. For ISUP traffic a CIC range can be specified. For SCCP traffic a global title address (GTA) may be specified.

The Cisco IP Transfer Point's possible routing key assignments for SUA are DPC, OPC, SSN, or GTA.

The routing keys are prioritized by matching GTA keys first, followed by the longest matching routing key at the highest layer in the protocol stack.

Global Title Address-Prefix Conversion

This feature provides the ability to support E.212->E.214 and E.212->E.164 conversion in International Telecommunication Union (ITU) networks.

- The prefix-conversion process is only applied to digits in the called party address, and is only invoked when the routing indicator equals global title.
- Allows for a variable length prefix and resultant digit string (up to a maximum of 15 digits).
- Prefix conversion can occur before or after GTT.
- For ITU networks the numbering plan value in the GTA indicator may be changed.
- The conversion rules will perform the longest match on the defined input prefixes. Upon a successful match, the input prefix is replaced with the resulting output prefix.

Network Availability and Redundancy

Of critical importance to operators is high availability of the network. The SIGTRAN protocols, SCTP, M3UA, and SUA, are designed to provide the high availability required by operators. Key features among these protocols are SCTP multihoming, and M3UA/SUA traffic modes types and ASP management. In a properly designed network, operators should be able to achieve equivalent, or higher, availability than is currently realized in traditional TDM SS7 networks.

The Cisco ITP M3UA/SUA signaling gateway supports the full set of SIGTRAN management messages. This includes the signaling network management messages (DUNA, DAVA, SCON, DUPU, and DRST) and the ASP state and traffic maintenance messages (ASPUP, ASPDN, ASPAC, ASPIA).

Signaling Gateway Mate Protocol

Two Cisco ITP M3UA/SUA signaling gateways can act as a mated pair and exchange necessary state information using the Signaling Gateway Mate Protocol (SGMP). These mated-pair Cisco IP Transfer Points are used to load-share and/or back up each other in failover scenarios. The mated Cisco IP Transfer Point can be used as a backup point code when there is a failure of an association between this Cisco IP Transfer Point and the ASP.

The mated-pair Cisco IP Transfer Points must have equivalent M3UA/SUA configuration, including the same application server and routing-key definitions. However, the local point code of each Cisco IP Transfer Point must be unique and should not match the local point code, the capability point code, the secondary point code, any application server point code (DPC), or any application server route point code configured on its mate.

When the Cisco IP Transfer Point mate association is active, the Cisco IP Transfer Point is informed of application server state changes on the mate in real time. When an application server goes inactive, subsequent messages are only rerouted to the mate if the corresponding application server on the mate is active.



When the application server on the original Cisco IP Transfer Point returns to active state, new messages are temporarily queued to allow in-transit messages from the mated Cisco IP Transfer Point to arrive at the ASP. Queued messages are released to the ASP upon expiration of a 2-second application server-specific timer.

Quality of Service

Quality of service (QoS) refers to the performance of packet flow through networks. The goal in a QoS-enabled environment is to enable predictable service delivery of certain traffic classes or type regardless of what other traffic is flowing through the network at any given time. The ability to apply QoS to SS7 signaling traffic over the IP network is a key component of network availability and ensuring service level agreements.

There are a variety of types of messages that traverse the SS7 network. For example, there is ISUP for call control and mobile application part (MAP) for delivery of Short Message Service (SMS) messages. With QoS settings, ISUP traffic can be assigned highest priority to ensure timely delivery in the event of severe network congestion.

Deployed on proven Cisco IOS technology, the Cisco IP Transfer Point takes advantage of a vast array of QoS features, such as IP Precedence, Differentiated Services Code Point (DSCP) and access lists. The M3UA/SUA signaling gateway provides the ability to prioritize traffic based on the routing key.

SCTP Associations

In the current RFC, SCTP flow control is handled at the association level. For this reason, the Cisco ITP signaling gateway does not use the multiple streams feature of SCTP for transmission. The Cisco IP Transfer Point does support receiving multiple streams. All management messages are transmitted on Stream 0 and all data messages are transmitted on Stream 1. The Cisco ITP signaling gateway uses separate SCTP associations for achieving QoS.

The SIGTRAN Working Group is developing a SCTP Enhancements draft that includes streams-based flow control. When the standard has been developed the Cisco IP Transfer Point team will consider using multiple streams for QoS support.

QoS Classes

The Cisco IP Transfer Point QoS service model allows the definition of 8 QoS classes, 0 through 7. Only one QoS class can be assigned to an SCTP association. The QoS class can be assigned an IP Precedence value or a DSCP. The TOS field in the IP header is set to the IP Precedence or DSCP based on the QoS class.

QoS Selection

The Cisco ITP signaling gateway allows QoS class selection based on the application server (routing key). Upon receiving a message from the SS7 network, the signaling gateway performs its normal application server and ASP selection. If QoS has been provisioned for the application server, the QoS classification is set to the highest QoS class of the active application servers that are using the selected ASP. Since all traffic on a given association is delivered in sequence, the possibility of prioritization within the stream is eliminated.

For the signaling gateway to prioritize traffic to a host that is supporting more than one application server, that host must establish a separate association for each application server. Thus the host will have an ASP for each application server that it supports. For example, an application host supporting ISUP and SCCP traffic would set up unique associations to the signaling gateway. This would appear as two different ASPs to the signaling gateway, each supporting a unique application server with a different QoS class value.



Management

Network Management

The Cisco ITP signaling gateway can be managed from a variety of management applications, including:

Cisco Signaling Gateway Manager

The Cisco Signaling Gateway Manager (SGM) is specifically designed to manage the value-added features of a Cisco IP Transfer Point-based routed network. The Cisco SGM is a client-server application that provides the following key features:

- Automatically discovers and maps the Cisco IP Transfer Point network topology.
- Regularly polls the Cisco IP Transfer Point routers and reports status of the associated links and link sets.
- Displays Cisco IP Transfer Point capable routers and legacy SS7 equipment (SSPs, SCPs, and STPs) as nodes on the topology map.
- Displays nodes, link sets, and links in both topology and tabular views.
- Receives Simple Network Management Protocol (SNMP) traps natively or via HP OpenView to drive accurate and up-to-date status displays.
- Integrates with the CiscoWorks Desktop.
- Supports direct launching of CiscoView Element Manager and CiscoWorks Device Center directly from node icons on the topology map for quick granular analysis.
- Supports downloadable Solaris and Windows clients for easy distribution to users and easier access to important information.
- Supports high server uptime with automatic process management and several debugging and customization tools.

CiscoWorks

CiscoWorks is the premier Cisco network-management platform and includes a wide variety of applications for managing IP based networks. The CiscoWorks Routed WAN Management and CiscoWorks Mobile Wireless bundles both provide the necessary applications for managing a Cisco routed network providing Cisco IP Transfer Point services.

HP OpenView

HP OpenView is an industry-standard SNMP-based tool to display Management Information Base (MIB) variables. It is most commonly used for managing the physical and device layers. When used in combination with CiscoView, operators can view Cisco device statistics such as CPU usage, memory usage, and physical link/segment utilization.

Agilent

Agilent is a Cisco ecosystem partner that is developing the acceSS7IP product specifically for SS7oIP management. For additional details, contact Cisco IP Transfer Point product marketing via http://www.cisco.com/en/US/products/sw/wirelssw/ps1862/prod_literature.html



Signaling Gateway MIBs

The Cisco ITP M3UA/SUA signaling gateway will support standard M3UA and SUA MIBs. There will also be support for Cisco IP Transfer Point enhanced MIBs. The Cisco ITP signaling gateway can be supported by the Cisco SGM. Refer to the Cisco IP Transfer Point Product Web page for further information http://www.cisco.com/en/US/products/sw/wirelssw/ps1862/prod_literature.html

Provisioning

The Cisco IP Transfer Point uses the same text-based command-line interface (CLI) used for all products based on Cisco IOS. The Cisco SGM is a Cisco IP Transfer Point-specific graphical-user-interface (GUI) tool that allows for creation, editing, and versioning of route and global title tables.

Deployment Partner Applications

External Ecosystem Partners

The Cisco IP Transfer Point product team is working to build a Cisco IP Transfer Point partner ecosystem with industry leaders and innovative new vendors to deliver services to customers. This program is intended to seed the operator with time-to-revenue solutions.

The basic steps required to become a part of the Cisco IP Transfer Point partner ecosystem are:

- Based on value to the operator, Cisco invites a partner to apply to the ecosystem.
- The Cisco IP Transfer Point partner officially enters the Cisco ecosystem process.
- Cisco and the partner prove the solution through interoperability testing.
- Cisco and partner jointly perform a minimum of two customer field trials.
- Upon successful completion of customer field trials, Cisco and partner jointly deliver the solution to the marketplace.

The Cisco IP Transfer Point team is working with a number of external partners in developing SIGTRAN connectivity for HLRs, SMSCs, and platforms that provide other enhanced services.

Cisco IP Transfer Point Reference Documents

- For Cisco ITP product family information (data sheets, white papers, configuration guides, competitive analysis, uses cases, and so on) refer to the Cisco IP Transfer Point web page at http://www.cisco.com/en/US/products/sw/wirelssw/ps1862/prod_literature.html
- For Cisco IP Transfer Point ITU, ANSI, and Telcordia/Bellcore compliance, read the Cisco IP Transfer Point Data Sheet.
- For platforms, performance, and capacity planning, read the Cisco IP Transfer Point Data Sheet.

CISCO SYSTEMS



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11 Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the
Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2002, Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0208R)