Tekelec EAGLE® 5
Integrated Signaling System

SS7-over-IP Networks Using SIGTRAN

910-4925-001 Revision B
June 2007

TEKELEC

Notice
Information in this documentation is subject to change without notice. Unauthorized use or copying of this documentation can result in civil or criminal penalties.

Any export of Tekelec products is subject to the export controls of the United States and the other countries where Tekelec has operations.

No part of this documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying or recording, for any purpose without the express written permission of an authorized representative of Tekelec.

Other product names used herein are for identification purposes only, and may be trademarks of their respective companies.

RoHS 5/6 - As of July 1, 2006, all products that comprise new installations shipped to European Union member countries will comply with the EU Directive 2002/95/EC "RoHS" (Restriction of Hazardous Substances). The exemption for lead-based solder described in the Annex will be exercised. RoHS 5/6 compliant components will have unique part numbers as reflected in the associated hardware and installation manuals.

WEEE - All products shipped to European Union member countries comply with the EU Directive 2002/96/EC, Waste Electronic and Electrical Equipment. All components that are WEEE compliant will be appropriately marked. For more information regarding Tekelec's WEEE program, contact your sales representative.

Trademarks
The Tekelec logo, EAGLE, G-Flex, G-Port, IP^7, IP^{7}Edge, IP^7 Secure Gateway, and TALI are registered trademarks of Tekelec. TekServer is a trademark of Tekelec. All other trademarks are the property of their respective owners.

Patents
This product is covered by one or more of the following U.S. and foreign patents:

U.S. Patent Numbers:

5,008,929, 5,953,404, 6,167,129, 6,324,183, 6,327,350, 6,456,845, 6,606,379, 6,639,981, 6,647,113, 6,662,017, 6,735,441, 6,745,041, 6,765,990, 6,795,546, 6,819,932, 6,836,477, 6,839,423, 6,885,872, 6,901,262, 6,914,973, 6,940,866, 6,944,184, 6,954,526, 6,954,794, 6,959,076, 6,965,592, 6,967,956, 6,968,048, 6,970,542

Ordering Information
For additional copies of this document, contact your sales representative.

Table of Contents

List of Figures

List of Tables

Introduction

An SS7-over-IP network consists of a traditional SS7 network that utilizes an IP network. This document describes SS7-over-IP networks that use the Signaling Transport (SIGTRAN) protocol suite as an enabler to access IP networks. IP-enabled or all-IP networks are growing in popularity for both wireline and wireless operators as they promise higher bandwidth at a lower cost, higher efficiency, and access to an exploding number of revenue-generating services. Participation in such services becomes increasingly difficult because of the high bandwidth required and the link restriction imposed by the traditional SS7 network.

A first step to IP success is an SS7-over-IP or SIGTRAN converged network to make reliable signaling over IP possible without replacing the entire network. The goal is to eventually move from the converged TDM/IP network to an all-IP network to take advantage of bandwidth, redundancy, reliability, and access to IP-based functions and applications. Tekelec is prepared to take customers through this process at their own pace by offering expertise and tested products that will assist in achieving this goal.

Figure 1. Transition from SS7 to IMS

This document examines the reasons for transitioning to an SS7-over-IP (SSoIP) network, the considerations that go into planning and dimensioning, and helpful information for implementing the network. This document does not attempt to provide a beginning-to-end solution for such a transition; contact your Tekelec Sales Representative to discuss your specific needs.

Audience

The audiences for this document are Tekelec departments affected by the development, sale, or service of SIGTRAN-related products, as well as Tekelec customers that require an overview of SS7-over-IP networks, SIGTRAN, and products that are part of the Tekelec solution.

Manual Organization

The manual is organized into these sections:

- *"Introduction"* on page 1 provides the purpose of this document, the targeted audience, how the manual is organized, and Tekelec contact information.
- *"SS7-over-IP Networks"* on page 5 describes the concept of an SS7- over-IP network and the protocols it uses, the opportunities it provides now and what it means for future directions. This section takes the reader from current TDM limitations, to the role of SIGTRAN, to the reasoning of why and when to transition to an SS7-over-IP network.
- *"Tekelec solutions"* on page 19 describes how Tekelec products are a part of the SS7-over-IP solution. This section describes how the EAGLE 5 Integrated Signaling System (ISS) functions as a gateway to internet networks; and the Integrated Application Solution (IAS), which provides several network management and performance tools including IP traffic monitoring through the Integrated Message Feeder (IMF).
- *"Transition planning"* on page 23 provides a guideline on how to prepare for a transition to an SS7-over-IP network.
- *"Dimensioning"* on page 29 describes dimensioning issues and calculations required to maximize the efficiency of the new network. This section addresses scalability, redundancy schemes, throughput calculations for both normal and failover mode, LAN/WAN considerations, and retransmission concepts.
- *"Implementation"* on page 57 provides hardware information, high-level configuration steps for the IPLIMx and IPGWx applications, how to refine timers and parameters after the installation, and high-level system verification steps.
- *"Troubleshooting"* on page 71 offers troubleshooting procedures based on symptoms occurring in the network.
- *"Appendix A. Additional Deployment Scenarios"* on page 75 provides other possible deployment scenarios.
- *"Appendix B. References"* on page 83 lists Tekelec-internal and external references used in this manual. Customers requiring access to Tekelec-internal references should contact their Sales Representative to obtain equivalent information. This section also provides the location of customer documentation on the Tekelec Customer Support site.
- *"Glossary"* defines both acronyms and terminology used in this manual.

Several conventions are used in this document. While certain acronyms are standard in the telecom industry and are understood by most readers, this document treats network components and feature name as proper names and spells out their names to improve the reading of this document.

For some process descriptions, figures or tables are displayed at the beginning of the process to allow the reader to follow most of the process on the same page. This convention is identified with each process.

Tekelec customer documentation is transitioning to sentence-style section headings to accommodate new documentation development technologies.

Where "end points" are mentioned, the full range is included: Service Switching Points (SSPs), Signaling Control Points (SCPs), Home Locator Registers (HLRs), Short Message Service Centers (SMSCs)

Tekelec Customer Care Center

The Tekelec Customer Care Center offers a point of contact through which customers can receive support for problems that may be encountered during the use of Tekelec products. The Tekelec Customer Care Center is staffed with highly trained engineers to provide solutions to technical questions and issues seven days a week, twenty-four hours a day. A variety of service programs are available through the Tekelec Customer Care Center.

To receive technical assistance, call the Tekelec Customer Care Center at one of the following locations:

- Tekelec Headquarter, USA

  Phone: **1 888-FOR-TKLC** or 1-888-367-8552 (national)
  +1 919-460-2150 (international)

  Fax: +1 919 460 0877

  E-mail: **support@tekelec.com**

- Tekelec, Europe and UK

  Phone: **+44 1784 467 804**

  Fax: +44 1784 477 120

  E-mail: **ecsc@tekelec.com**

SS7-over-IP Networks

An SS7-over-IP network consists of a traditional SS7 network that can integrate IP-enabled or all-IP devices with protocols defined by the Internet Engineering Task Force (IETF) standards organization.

SS7-over-IP signaling primarily addresses the transport aspect of SS7. Call-control services and other types of services, therefore, can continue to be offered and deployed without concern for the method of interconnection. The method of service implementation, however, remains dependent on the particular network element chosen to support the service rather than the transport chosen.

This section looks at the limitations of the traditional SS7 network and its network components, the role of SIGTRAN protocols, the purpose of SS7-over-IP networks, the advantages of transitioning to this network, and when it is time to consider transitioning.

SS7 limitations

SS7 is a signaling network (data traffic) protocol used to send and receive signaling messages between Signaling End Points over dedicated signaling links. Operators deploy SS7 services over a dedicated network of 56- or 64-kbps Time Division Multiplexed (TDM) lines, or utilize high-speed T1 (1.5 Mbps) or E1 (2.048 Mbps) lines. SS7 uses centralized databases and services, achieves reliable connections through network management, and is secure because of its isolation from end users and the dedicated network. SS7 signaling is mature with standards and a rich feature set, and offers these advantages to both wireline and wireless services.

However, SS7 limitations in scalability, bandwidth, and network availability slow network growth and opportunities to participate in new IP services:

- Scalability limited by 16-link linksets consisting of 64 kbps transport

  Up to 16 links may be grouped into one circuit, or linkset. Adjacent network elements, such as Signal Transfer Points (STPs) and Service Control Points (SCPs), may be connected by no more than one linkset. The protocol further recommends that links and linksets are configured to no more than 40% of their maximum capacity, so that the alternate path can carry the full load of messages during failover.

- Bandwidth

  A traditional SS7 message size is limited to about 272 octets. E1/T1 links allow the transmission of larger messages, but not without originating, routing, or end points supporting either large messages or message segmentation.

  A bandwidth of 56 kbps or 64 kbps per link and dedicated links reduce flexibility and increase cost significantly when creating sufficient bandwidth for new service applications. In a TDM network, entire transmission segments must be reserved for each call, even if the TDM connection is idle.

TDM-based SS7 is continuing to evolve, but slowly. Instead, wireline and wireless operators are looking to IP solutions.

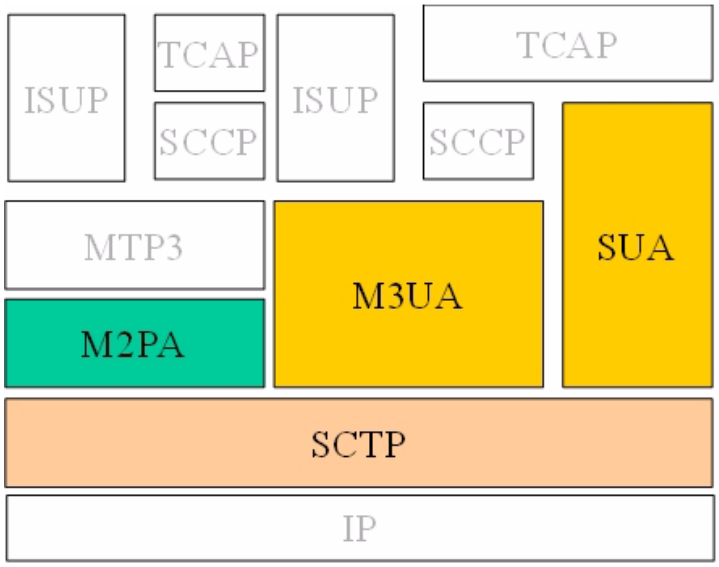
Role of SIGTRAN

SIGTRAN is a working group of the IETF, addressing packet-based Public Switched Telephone Network (PSTN) signaling over IP networks. A set of signaling transport protocols has been developed out of the group's work. For the purposes of this document, the protocols are collectively called the "SIGTRAN" protocols or suite.

The SIGTRAN architecture used by Tekelec includes the following protocols. See Figure 2 for their location in the protocol stack:

- Stream Control Transmission Protocol (SCTP); RFC 2960
- MTP2 User Peer-to-Peer Adaptation Layer (M2PA) protocol; RFC 4165
- MTP3 User Adaptation Layer (M3UA) protocol; RFC 4666
- SCCP User Adaptation Layer (SUA) protocol; RFC 3868

Figure 2. SIGTRAN protocols used by Tekelec



SCTP (Stream Control Transmission Protocol)

SCTP is a new reliable transport protocol that operates on top of a connectionless packet network such as IP, and operates at the same layer as TCP. It establishes a connection between two endpoints, called an association, for transmission of user messages. To establish an association between SCTP endpoints, one endpoint provides the other with a list of its transport addresses (one or more IP addresses in combination with an SCTP port). These transport addresses identify the addresses that will send and receive SCTP packets. SCTP was developed to eliminate deficiencies in TCP and offers acknowledged, error-free, non-duplicated user data transport.

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 end point to another) to ensure in-sequence delivery between associated end points. 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 does enforce head-of-line blocking, the SIGTRAN Working Group recommends SCTP rather than TCP for the transmission of signaling messages over IP networks.

Security

SCTP provides certain transport-related security features, such as resistance against blind denial of service attacks, masquerades, or improper monopolization of services.

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.

Tekelec deviations

The following sections summarize the most important deviations from the IETF RFCs that Tekelec has made. Refer to the Tekelec compliance matrices for details [5], [6], [7], and [8]. Contact your Sales Representative for access to the information contained in these documents.

SCTP multiple streams

There are several architectural issues regarding the use of multiple streams as described in the SCTP protocol. The issues include:

- Synchronization between data streams
- Synchronization from control stream to data streams
- Load-sharing implementation based on SLS across streams, either within a connection or across all the connections in an Application Server

  Since the underlying SS7 network is connectionless, a stringent requirement for missequenced messages has been set because it is often easier to recover from the loss of a message by a time-out than from one message delivered out-of-sequence. The Message Transfer Part (MTP) is able to maintain a high probability of message sequencing. This is ensured by the MTP user, which generates a value for a Signaling Link Selection (SLS) field as a parameter for each message. As the message is routed through the network, wherever there is a choice to be made between alternate routes, the link selection is made based on the SLS value in the message.
- Connection behavior when a stream becomes congested

A lack of consensus on the IETF SIGTRAN mailing list regarding these issues resulted in Tekelec supporting only two streams: a control stream and a data stream.

SCTP timers

Based on experiences in the field, Tekelec has deviated from some RFC-recommended timer settings, especially related to retransmission, to better accommodate signaling networks.

The Tekelec default mode for the retransmission timer (RMODE) is linear, whereas the RFC-recommended timer setting is exponential. Tekelec makes both settings available through configuring an association to use either the Linear (LIN) or the exponential (RFC) method. For more information about both modes and the timer settings, see *"SCTP timers"* on page 52.

M2PA (MTP2 User Peer-to-Peer Adaptation Layer) protocol

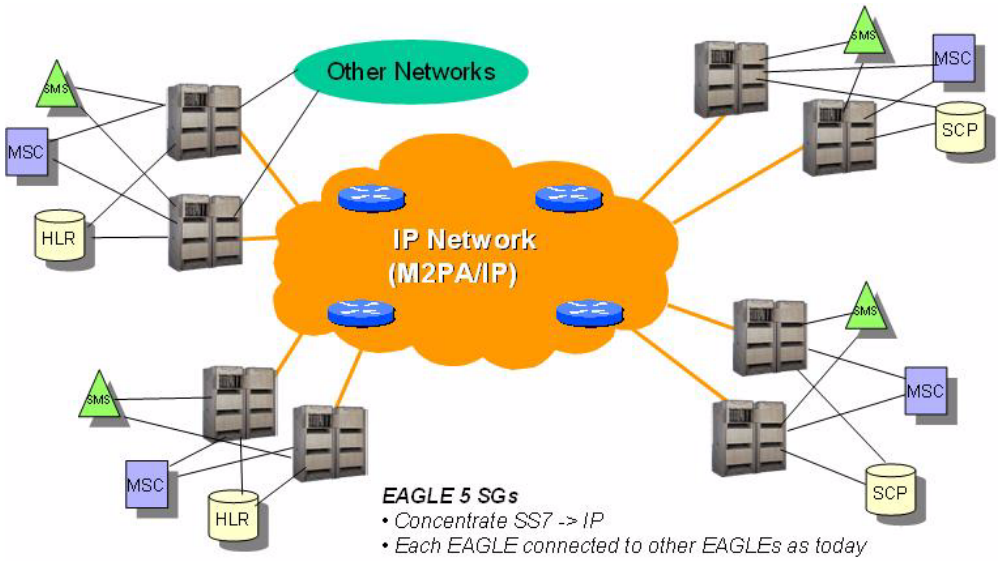
The M2PA protocol facilitates the integration of SS7 and IP networks by enabling nodes in circuit-switched networks to access IP-based databases and other nodes in IP networks using SS7 signaling. Conversely, M2PA allows IP applications to access SS7 databases such as local number portability, calling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

M2PA is used primarily to replace B-, C-, and D-links. When used with A-links, M2PA connects to Service Switching Points, Signaling Control Points, Home Locator Registers and other endpoints. M2PA is a direct replacement for channelized TDM circuits because it has specific controls for assurance of in-sequence delivery of messages. As such, M2PA is needed to connect points that pass call-related data that is time-sensitive, such as ISUP calling data.

Congestion procedures conform to those specified by the ANSI/ITU standards. The M2PA protocol can coexist in a linkset with other link types such as low-speed links and ATM high speed links. When using other link types, the throughput will always match the lowest-speed link in the linkset.

Tekelec implemented the M2PA protocol through its IPLIMx application. For more information on the IPLIMx application, see *"IPLIMx and IPGWx applications"* on page 20.

Figure 3. M2PA network



M3UA (MTP Level 3 User Adaptation Layer) protocol

M3UA seamlessly transports SS7 MTP3 user part signaling messages over IP using SCTP. M3UA-connected IP endpoints do not have to conform to standard SS7 topology, because each M3UA association does not require an SS7 link; there are no 16-link-per-linkset restrictions. Each M3UA-connected IP endpoint can be addressed by an SS7 point code unique from the signaling gateway's point code.

> **NOTE: A-links for nodes requiring in-sequence delivery of messages should be configured on the IPLIMx card using M2PA; M3UA does not have sequence numbers to support lossless changeover/changeback. For more information on the IPLIMx application, see *"IPLIMx and IPGWx applications"* on page 20.**

A routing key defines a set of IP connections as a network path for a portion of SS7 traffic, and is the IETF Signaling Gateway equivalent of an Signal Transfer Point's SS7 route. Routing keys are supported by the M3UA protocols to partition SS7 traffic using combinations of Destination Point Code (DPC), Origination Point Code (OPC), Service Indicator (SI), Network Indicator (NI), SS7 Subsystem Number (SSN), and/or Circuit Identification Code (CIC) message fields.

M3UA does not have a 272-octet Signaling Information Field (SIF) length limit as specified by some SS7 MTP3 variants. Larger information blocks can be accommodated directly by M3UA/SCTP without the need for an upper layer segmentation or re-assembly 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.

At the Signaling Gateway, M3UA indicates to remote MTP3 users at IP end points when an SS7 signaling point is reachable or unreachable, or when SS7 network congestion or restrictions occur.

SUA (SCCP User Adaptation) protocol

SUA transports any SS7 SCCP signaling messages over IP using SCTP, and is used between a Signaling Gateway and a signaling end point, or between signaling end points.

SUA is used to direct queries to the correct IP-based Application Server Process. It replaces the SCCP layer with its own SUA layer and is used when source and destination are both IP.

A Signaling Gateway can determine the "next hop" using the Global Title Translations delivered in the Called Party Address of the Message Signaling Unit (MSU).

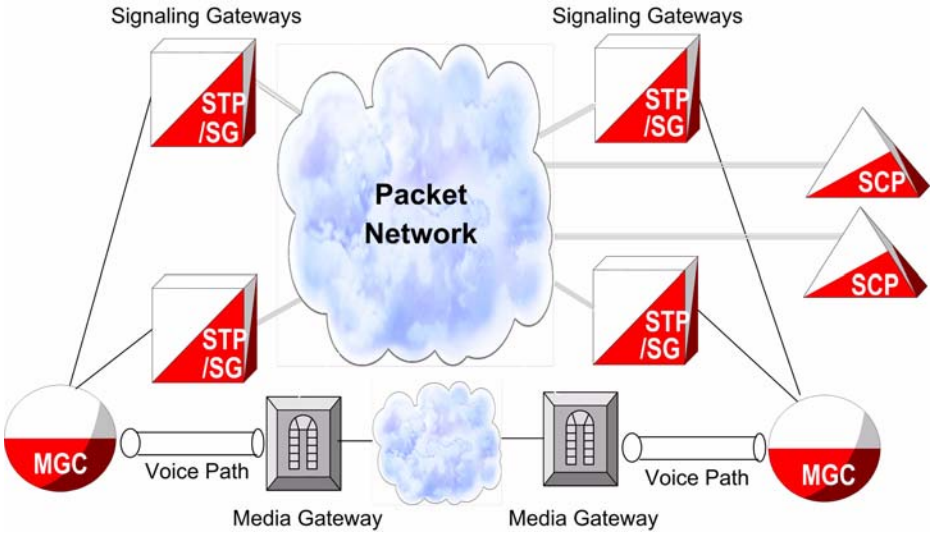
NOTE: A-links for nodes requiring in-sequence delivery of messages should be configured on the IPLIMx card using M2PA; SUA does not have sequence numbers to support lossless changeover/changeback. For more information on the IPLIMx application, see *"IPLIMx and IPGWx applications"* on page 20.

Routing keys are supported by the SUA protocol as in M3UA. Routing key parameters include DPC, OPC, SI, and SSN.

SS7-over-IP signaling transport

SIGTRAN protocols connect IP-based or IP-enabled Media Gateway Controllers (MGCs), Signaling Gateways (SGs), switches, databases and other Next Generation signaling applications with traditional circuit-switched signaling architecture; see Figure 4.

Figure 4. SS7-over-IP network



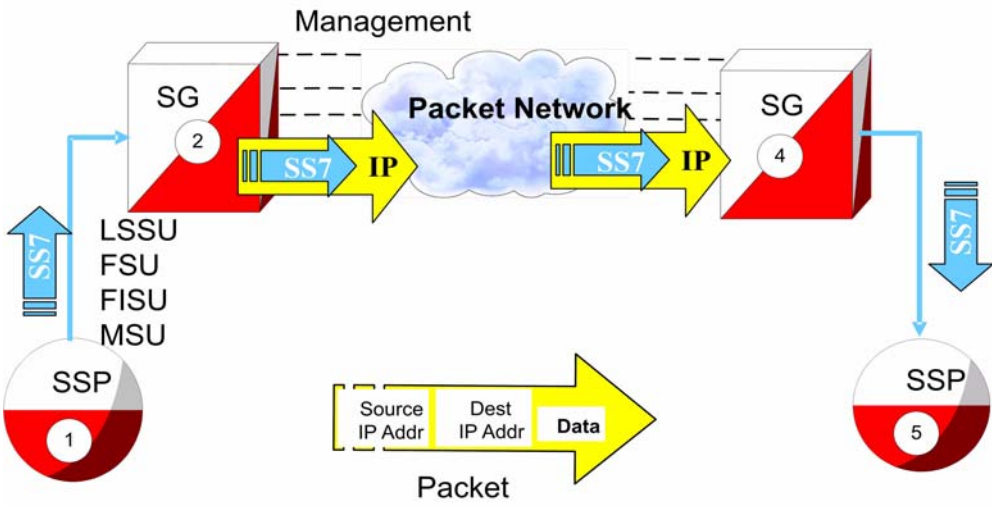
In SS7-over-IP networks, traditional SS7 signals from a telephone company switch are transmitted to a Signaling Gateway, which wraps the signals in an IP packet for transmission over IP to either the next Signaling Gateway or to a MGC, other Service Control Points, or Mobile Switching Centers (MSCs). SIGTRAN protocols define how the SS7 messages can be transported reliably over the IP network; see also *"Role of SIGTRAN"* on page 6.

The Signaling Gateway has a critical role in the integrated network and is often deployed in groups of two or more to ensure high availability. The Signaling Gateway provides transparent interworking of signaling between TDM and IP networks. The Signaling Gateway may terminate SS7 signaling or translate and relay messages over an IP network to a Signaling End Point (SEP) or another Signaling Gateway, which may be separate physical devices or integrated in any combination. For example, the EAGLE 5 ISS can perform the functions of an Signal Transfer Point in addition to those of a Signaling Gateway.

From SS7 message to IP packet

Figure 5 and the following description show how SS7 messages are encapsulated and sent over an IP network to a host in another network.

Figure 5. Change from SS7 message to IP packet

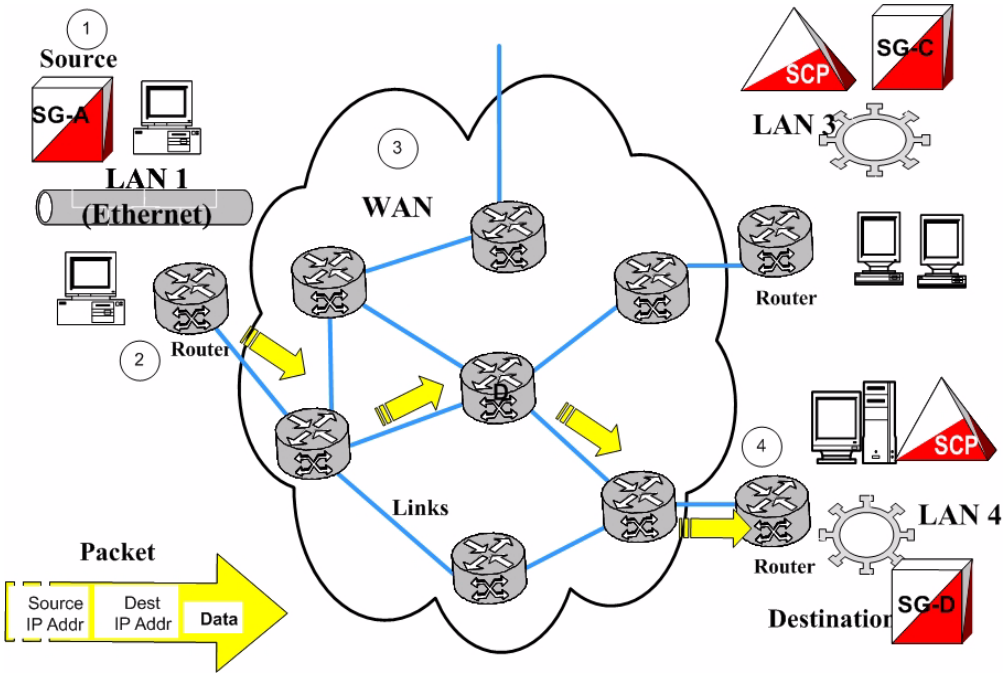


1. A signaling point issues an SS7 message, unaware that there is IP signaling in the network. The message contains Link Status Signaling Units (LSSU), Fill In Signal Units (FISU), Final Signal Units (FSU), and Message Signal Units (MSUs).
2. The Signaling Gateway receives the SS7 packet and encapsulates all necessary SS7 information into the data section of the IP packet. The packet includes the data, source and destination IP address.
3. The packet travels across the IP network. The network is unaware that it is delivering SS7 data. There is no need to modify the routers or gateways along the way.
4. The packet is delivered to the Signaling Gateway on the receiving network. The SS7 information is recovered from the IP packet.
5. A well-formed SS7 packet is sent to the destination Signaling Point.

Communication inside the Wide Area Network (WAN)

Figure 6 and the following description show the routing inside the WAN.

Figure 6. Communication inside the WAN



1. The Source Host (Signaling Gateway) builds a packet with a destination IP address.
2. A router on the LAN converts the packet to the WAN protocol and places it on the WAN.
3. Each router on the WAN looks at the destination IP address and determines the port to which it forwards the packet. Each router needs to know only how to get the packet closer to the destination.
4. The final router converts the packet to the local LAN format and delivers it to the Destination Host.

Reasons to transition to an SS7-over-IP SIGTRAN network

There are many reasons for transitioning to an SS7-over-IP network. The resulting network offers better cost effectiveness, increased capacity that can be further scaled as needed, a high Quality of Service (QoS) including redundancy and security, and efficient deployment using existing equipment.

Cost effectiveness

SS7-over-IP networks lower network capital and operational expenditures. SIGTRAN is based on the IP protocol; these networks use industry standard, off-the-shelf network interfaces, cables, switches, and software. Improvements in technology and reductions in cost found in the general computer industry can be applied readily in signaling applications. As an industry standard, SIGTRAN allows customers to interoperate in a multivendor environment.

Replacing long-haul point-to-point SS7 links between network elements with IP connectivity can reduce recurring signaling transport costs and the need for dedicated TDM lines. IP-based network monitoring and provisioning improve operation efficiencies.

Increased capacity

SS7-over-IP networks offer increased capacity. The bandwidth overall is greater, both due to inherent capacity and to dynamic bandwidth sharing. Data traffic including Short Message Service (SMS) can run more efficiently over SIGTRAN. For example, SMS data is saturating some SS7 networks. Using devices such as the Tekelec EAGLE 5 ISS with its gateway functions, operators can have a Short Message Service Center communicate directly to Home Location Registers and Mobile Switching Centers using SIGTRAN.

Flexibility

SIGTRAN uses the packet IP network to define logical connections between devices. Because the network developers, planners, and installers are no longer tied to deploying fixed circuits for signaling, they have the flexibility to define the network as needs and demands change. Flexibility is key in adapting bandwidth on demand; redimensioning the SS7-over-IP network can be done completely through software. With legacy SS7, users are limited to either 56 or 64 kbps links.

There is also flexibility when adding capacity for new IP-based solutions and value-added services; future enhancements are more transparent.

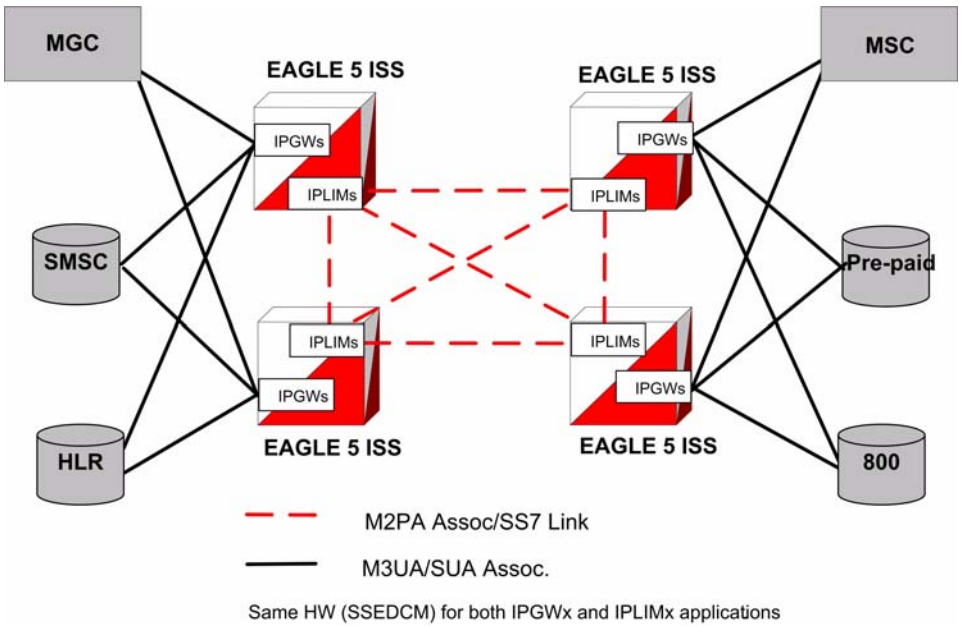
Integration

Enabling a network with IP does not require expensive investments or costly upgrades for existing end nodes; it enables migration to packet-based architecture without adding new point codes or reconfiguring the network.

For M2PA, there are no architectural changes. When using SIGTRAN, SS7 routing translations are the same for TDM or IP linksets.

An SS7-over-IP network is the first step to an all-IP network. Figure 7 shows the diversity of solutions that are possible using SIGTRAN protocols. For example, M3UA and SUA support an IP-enabled Short Message Service Center (SMSC) or Home Location Register (HLR). SS7-over-IP solves the throughput limitations that were inherited from the SS7 standards, thus allowing Short Message Service Center, Home Location Register, and other equipment to support heavy SS7 traffic needs.

Figure 7. Typical EAGLE 5 ISS SS7-over-IP deployment



Type of network change

When considering a transition, determine the type of change to make. Consider the advantages and disadvantages of a dedicated network versus a converged network. Does the equipment need to be phased out or will new equipment be added? Does the network require additional protection or supplier integration through diversity? All these issues should be considered in the initial planning because of their significant impact on the overall network architecture.

Dedicated network versus converged IP network

While a dedicated IP network offers inherent security and minimal routing, a converged network carrying both voice and data also will satisfy these needs at less cost, provided that the QoS attributes such as Round Trip Time (RTT), Packet Loss, and Jitter are satisfied. These attributes should always be given the highest priority on the IP network.

Implementing SS7-over-IP on an SS7 system creates a converged IP network that allows quick, cost-effective implementation of IP-based services using existing network elements. The Tekelec EAGLE 5 ISS with its Signaling Transfer Point and Signaling Gateway functions offers a reliable solution for this transition.

Decisions regarding the customization of the IP network are left up to the customer, but Tekelec Professional Services can provide recommendations based on their experiences with previous SIGTRAN deployments.

Replacement versus expansion

When transitioning to an SS7-over-IP network, consider these strategies:

- Replacement of out-phased (end of life) TDM equipment
- Gradual replacement, which means coexistence of the two technologies: there is no need to retire an existing switch if you are deploying purely for additional capacity
- Full accelerated replacement with a short transition period based on cost, efficiency, and fault management: even if complete transition is desired, it is unrealistic to expect to instantaneously cut over unless the subscriber base is very small.

  There is enormous leverage when one platform provides both TDM and SS7-over-IP. The issue is more than cost savings. A combined platform can support new multimodal voice, data and video services that utilize a combination of IP data with diverse messaging capabilities, location and presence information, voice connections, speech recognition and Intelligent Network control. Of course, not every application requires every capability, so flexibility is key.
- Maintaining the existing PSTN network, and use Next Generation Network (NGN) equipment to satisfy growing demands: legacy switches have many features and services. Operators may have to wait until new switches support all required features and services.
- Out-of-region or in-region expansion
- Traditional services or new features

Diversity

Supporting businesses with critical operations such as banking requires strategies for predictable recovery, not only from regular network faults, but also from attacks on signaling networks. When planning to move to an SS7-over-IP network, the operator should consider diversity to assist in recovery.

The range of diversity will differ from customer to customer and it may include a multitude of factors:

- Entry diversity offers more than one cable entrance into a building
- Pair and cable diversity provides a local loop connection through multiple, nonadjacent pairs in more than one cable
- Path or route diversity provides end-to-end, physically or logically separate routes for a circuit
- Central office diversity provides local loops that terminate in more than one central office
- Site diversity provides alternative or backup locations

When to transition to an SS7-over-IP SIGTRAN network

Consider transitioning to an SS7-over-IP network if:

- Traffic-volume growth on the network is demanding additional capacity
- New networks are planned or IP services will be added to existing networks
- Traffic volume between signaling points is surpassing the bandwidth of 16-link linksets
- A data or voice-over-IP network is already present
- Signaling traffic is deployed over very high latency or lossier networks, such as satellite links

If signaling messages are transported over a private intranet, security measures can be applied as deemed necessary by the network operator.

Tekelec solutions

Tekelec has set the standard for ultra-reliable, high-performance, scalable signaling in wireless and wireline networks around the world. Advanced solutions optimize network efficiency and save customer capital and operational costs. Tekelec addresses network transition by providing the signaling bridge to seamlessly converge circuit and packet-switched technologies.

Operators can leverage existing TDM and ATM network resources as they transition at their own pace to new IP-based transport and services. Tekelec's innovative switching solutions create cost-effective, fully scalable networks with built-in flexibility, making it quick and easy to roll out high-margin multimedia services to business and residential customers.

Tekelec is the IP signaling leader and the first to recognize the value of IP Signaling by developing the TALI protocol (RFC 3094) in 1998. Tekelec was first to market with an IP Signaling solution (IPLIMx application) in 2000, and has years of IP signaling deployment experience.

Products

There are a variety of Tekelec products available to implement a new IP network or upgrade an existing SS7 network.

EAGLE 5 ISS

The Tekelec EAGLE 5 ISS is a robust SS7-over-IP solution that delivers centralized signaling routing, and bridges the legacy circuit-switched and packet networks. It provides seamless interworking between TDM resources such as Service Control Points and IP-enabled elements such as Media Gateway Controllers and next-generation databases. With its packet-based technology, the EAGLE 5 ISS can handle signaling requirements of the most complex networks, delivering dynamic bandwidth sharing to support increases in signaling traffic without additional nodes. The same platform delivers full Signal Transfer Point capabilities and a complete portfolio of integrated applications.

Using the EAGLE 5 ISS to structure the network provides a predictable and reliable architecture with all required interfaces. It is easily scalable to cover huge core networks, with an independent control layer that allows expansion on different parts of the network independent of each other. The EAGLE 5 ISS provides ease of database management for the SS7-over-IP architecture.

Key benefits of using the Tekelec SS7-over-IP solution are:

- **Decreased network congestion.** Tekelec's packet-switched technology delivers dynamic bandwidth sharing to enable carriers to effectively expand their signaling networks and reduce network bottlenecks. By replacing TDM links with an IP interface, service providers can significantly increase signaling capacity to Service Control Points.
- **Reduced transport costs.** Replacing long-haul, point-to-point SS7 links between network elements with IP connectivity can reduce recurring signaling transport costs by 40% to 70%.
- **More efficient networks.** Transitioning to SS7-over-IP signaling does not require expensive equipment replacement or costly software upgrades for existing end nodes. With Tekelec solutions, carriers can streamline their networks while reducing administration, without service interruption during installation.
- **Migration to next-generation architecture.** The EAGLE 5 ISS can appear as an end office to the SS7 network by sharing its point code with the IP endpoints. This allows carriers to migrate to a packet-based architecture without adding a new point code or reconfiguring the network. Tekelec's open, multi-protocol architecture (SS7, SCTP, M2PA, M3UA, and SUA) gives carriers the capability to grow and migrate their network and the independence to choose best-in-class products.

IPLIMx and IPGWx applications

The EAGLE 5 ISS implements SIGTRAN with two applications:

- IPLIMx, which represents IPLIM for ANSI networks and IPLIMi for ITU-N and ITU-I networks
- IPGWx, which represents IPGWx for ANSI networks and IPGWi for ITU-N and ITU-I networks

The IPLIMx application uses SCTP with M2PA protocols to support B-, C-, and D- links; but it can also be used for A-links to connect to SEPs on other vendor equipment that have M2PA SIGTRAN specifications implemented. IPLIMx is fully compliant with RFC 4165.

IPLIMx is installed on either an SSEDCM card or an E5-ENET card. Based on the card type, IPLIMx allows up to 8 links per SSEDCM card and up to 16 links per E5-ENET card, each with one SCTP association per link. IPLIMx can be implemented with just one card and expanded to 100 cards per system.

The IPGWx application uses SCTP with M3UA and SUA protocols to provide user part support such as SCCP and ISUP over A-links to IP-resident network elements such as Service Switching Points, Mobile Switching Centers, Service Control Points and Home Location Registers using SIGTRAN. Since IPGWx applications use M3UA/SUA to replace MTP3 functions, it cannot be used in mixed linksets of both M3UA/SUA and MTP3, as the application will not participate in any changeover/changeback procedure. IPGWx supports statically provisioned routing keys by selecting IP connections based on DPC/OPC/SI/CIC/SSN. The application also supports the End Office mode where the EAGLE 5 ISS shares its point codes with IP-remote applications. However, A-links for nodes requiring in-sequence delivery of messages should be configured on the IPLIMx application using M2PA; M3UA/SUA does not have sequence numbers to support lossless changeover/changeback procedures.

IPGWx is installed on either an SSEDCM card or an E5-ENET card. IPGWx allows one link per card and up to 50 SCTP associations.The link terminates at a private adjacent point code. IPGWx is installed with just one card, and can be expanded to 64 cards per system.

Tekelec Integrated Application Solutions (IAS)

The Tekelec IAS platform, integrated with EAGLE 5 ISS, provides tools to capture network traffic data and convert it into useful business intelligence for troubleshooting, managing traffic, roamers, services, and revenues. With its powerful and configurable filtering, IAS sorts through the data to create comprehensive dashboards and reports for all departments within the service-provider company. IAS includes a comprehensive array of performance- and revenue-management capabilities that provide reliable real-time or historical information based on network traffic.

The IAS is based on industry-standard network protocols, and provides one platform for all network technologies including VoIP and IMS. It supports many different protocols including SS7, CLASS, SIGTRAN, IN, INAP, GSM, CDMA, CAMEL, WIN, MMS, SMPP, WAP, POP3, SMTP, FTP, and HTTP.

Integrated Message Feeder (IMF)

The IMF is an integrated site collector that provides integrated data acquisition in conjunction with the EAGLE 5 ISS. IMF connects to the EAGLE 5 ISS via Ethernet and monitors signaling links on the EAGLE 5 ISS including LSL, ATM HSL, SE HSL, M2PA and M3UA.

IMF allows remote access for administration and troubleshooting, and provides backup and upgrade capability, database management, and traffic management of captured signaling information.

IMF hardware supports NEBS 3 for central office environments. IMF provides a redundant LAN architecture for interface reliability and an N+1 server architecture in case of a single server failure within the managed subsystem.

For more information on IAS and IMF, contact your Tekelec Sales Representative.

Transition planning

The purpose of transitioning from an existing traditional SS7 network to an SS7-over-IP SIGTRAN network is to access valuable IP services at a reasonable cost and within the desired time frames, without losing any current functionality. While the transition can occur in phases and at the desired pace of the customer, the transition must be well planned to minimize impact on existing operations. This section provides guidelines on how to approach such a transition and points to the detailed information provided in this document.

Transition guidelines

The transition guidelines consist of these major steps:

1. Resolve high-level network design
2. Collect network information
3. Analyze data
4. Prepare configurations
5. Implement and test
6. Refine timers and parameters

Resolve high-level network design

Determine any issues by looking at the current network design compared to the new network architecture. Consider the protocols to be used, specific Tekelec implementations, mated-pair redundancy and link engineering, unihoming versus multihoming, and IP redundancy.

General considerations about the overall network include the following topics:

- *"Type of network change"* on page 15
  - *"Dedicated network versus converged IP network"* on page 15
  - *"Replacement versus expansion"* on page 16
  - *"Diversity"* on page 16
- *"Security"* on page 7

SIGTRAN protocols were designed to support specific paths between signaling points. The main protocols are M2PA and M3UA, each of which is built on top of the SCTP protocol. Read about the role of the protocols:

- *"SCTP (Stream Control Transmission Protocol)"* on page 7
- *"M2PA (MTP2 User Peer-to-Peer Adaptation Layer) protocol"* on page 9
- *"M3UA (MTP Level 3 User Adaptation Layer) protocol"* on page 10
- *"SUA (SCCP User Adaptation) protocol"* on page 10

Be aware of Tekelec-specific implementations or deviations and how they will impact your new network. Read about these implementations:

- Protocol deviations
  - *"SCTP timers"* on page 8
  - *"SCTP multiple streams"* on page 8
  - *"Multihoming"* on page 46
  - *"M2PA (MTP2 User Peer-to-Peer Adaptation Layer) protocol"* on page 9
- *"Products"* on page 19
- *"Scalability"* on page 30
- *"Appendix A. Additional Deployment Scenarios"* on page 75
- *"IPGWx congestion management options"* on page 45
- *"IPGWx mateset"* on page 48
- *"Signaling Link Selection (SLS) routing"* on page 49

Redundancy is achieved through linkset engineering, leveraging unihoming or multihoming, and IP network redundancy. Read about redundancy, links, linksets, and associations:

- *"Redundancy and link engineering"* on page 46
  - *"Unihoming versus multihoming"* on page 46
  - *"Mated Signal Transfer Point redundancy"* on page 48
  - *"IPGWx mateset"* on page 48
  - *"Signaling Link Selection (SLS) routing"* on page 49
- *"Appendix A. Additional Deployment Scenarios"* on page 75
- *"Scalability"* on page 30

Collect network information

Developing a physical and logical diagram of the network will help organize the information clearly. Detailed documentation should include:

- Hardware data of the infrastructure's physical structure
- Software data including the existence and configuration of protocols used on the network
- Logical organization of the network
- Name and address resolution methods
- The existence and configuration of services used
- Location of the network sites and the available bandwidth

The physical network diagram should present the following information about your existing network:

- Details of physical communication links, such as cable length, grade, and approximation of the physical paths of the wiring, analog, and ISDN lines
- Servers with name, IP address (if static), server role, and domain membership. A server can operate in many roles.
- Location of devices such as hubs, switches and routers that are on the network
- WAN communication links and the available bandwidth between sites (this could be an approximation or the actual measured capacity)

The logical network diagram should show the network architecture, including the following information:

- Domain architecture including the existing domain hierarchy, names, and addressing scheme.
- Server roles including primary and backup

IP addresses, subnet masks, default gateways and LAN parameters (e.g. Full/Half Duplex, 10/100 Speed, MAC Layer) will also be needed for implementation. Refer to the *Database Administration - IP^7 Secure Gateway Manual* of the current EAGLE 5 ISS documentation for affected parameters and detailed information.

Before an association is established, the exact RTT is impossible to measure accurately because only the transmitter’s SCTP will be able to measure the exact amount of elapsed time from each transmit until the acknowledgment. A good estimate can be gained using a number of ping requests at different times of the day or from a network analyzer. Remember, however, that ping uses ICMP echo packets that are often given a lower QoS in IP networks.

To gather the information required to determine configuration parameters of the M2PA and M3UA association(s) between an EAGLE 5 ISS node and each Signaling End Point (SEP), a spreadsheet per EAGLE 5 ISS node can be very helpful. Every node connected by a SIGTRAN link should appear as a row in the spreadsheet, with the headings listed in Table 1 along the top row.

Table 1. M2PA and M3UA configuration parameter data

Heading Text	Explanation
Node Name	The unique network name for the node
Node ID	The unique network ID for the node
Site Name	The unique network name for the site in which the node resides
Node Type	STP, MSC, HLR, SMSC, IN, MSS, MGC, etc.
Connected SGW(s)	The EAGLE 5 ISS node connection to which this data refer
Total # SGWs	Total number of STPs to which this node connects
SIGTRAN Protocol	M2PA, M3UA or SUA
RTT to STP	Measured or estimated RTT between the two nodes
Jitter %	The percentage variation in RTT
Dim. %	The normal designed maximum utilization of a link (20%, 40%, etc.)
Avg. MSU Size	The expected average MSU size between this node and the EAGLE 5 ISS
% SCCP Class 1	The percentage of SCCP Class 1 traffic expected to be sent to this node
Peak MSU/s	The planned number of MSU/s expected to be sent to this node from all EAGLE 5 ISSs in worst-case conditions
Max Assoc.	The maximum number of associations that this node supports to this EAGLE 5 ISS

See also:

- *"Configure the IPLIMx application"* on page 58
- *"Configure the IPGWx application"* on page 60
- *Database Administration - IP^7 Secure Gateway Manual* of your current EAGLE 5 ISS documentation

Analyze data

Follow the guidelines in *Engineering Rules for Determining IP7 Application Throughput*, Tekelec, TR005007 [2] to determine expected throughput from IPLIMx and IPGWx applications, and for details on other criteria to achieve these advertised capacities.

Additional information on card throughput (MSU/s) can be found in *"Achieving IPLIMx and IPGWx applications' Advertised Capacity"* on page 32.

Tekelec has guidelines for implementing SS7-over-IP, which can be found at:

- *"SIGTRAN engineering guidelines"* on page 42
- *"Calculate the number of cards required"* on page 44

To determine association configuration parameters, see:

- *"Define RTO parameter"* on page 65
- *"Configure Congestion Window Minimum (CWMIN) parameter"* on page 55

Prepare configurations

Once card and association throughput are determined, they can be compared to the traffic dimensioning required for signaling end points (from customers) to determine the number of linksets to use, number of cards in a linkset, and number of associations per card. Consider other factors such as limitations enforced by the connected node (e.g., limits to the number of supported associations).

NOTE: Combining IP links and low-speed links in same linkset will limit bandwidth availability and scalability. Creating dedicated linksets for IP links and low-speed links also can cause load sharing issues (load sharing across more than two linksets).

Implement and test

- *"Configuration"* on page 58
- *"Retransmission concept"* on page 51
- *"Define RTIMES association retransmits"* on page 64
- *"Define RTO parameter"* on page 65
- *"System verification"* on page 66
- *"Troubleshooting"* on page 71

Refine timers and parameters

"Refine timers and parameters" on page 64

Dimensioning

Dimensioning refers to network needs and likely use patterns on that network. It is especially important that an SS7-over-IP network maximizes network efficiency by examining the scalability; achieving maximum card capacity; setting up congestion management, status sharing, redundancy, routing; and configuring retransmission parameters.

About bandwidth, throughput, transaction units, and TPS

Bandwidth is the maximum amount of data that can pass through a network at any given time; it is the Advertised Capacity of a card.

Throughput is the amount of data that is actually transmitted in that given time. Throughput reflects an end-to-end rate, which is affected by various conditions during the transmission. Throughput is always lower than bandwidth.

Transactions versus transaction units and TPS

In SS7 signaling, a transaction is typically defined as one MSU transmitted and one MSU received, and assumes a worst-case scenario of that many MSUs both transmitted and received simultaneously per second.

IP signaling capacity is not usually constrained by the IP network (bandwidth), but rather by the processing platform (CPU or memory). The cost of a given transaction varies based upon the feature set triggered by the transaction. Not all MSUs are the same, and not all configurations are the same. Rather than to continue to engineer product capacity for the worst case and thereby penalizing customers who are not using worst-case scenarios, Tekelec is providing the Transaction Unit (TU) model to allow customers flexibility in how to use application or card capacity.

Under the TU model, a transaction unit indicates the relative cost of an IP signaling transaction; the base transaction unit is 1.0. Some transactions are more expensive than others in terms of IP signaling card capacity. A transaction that is less expensive than the base has a transaction unit less than 1.0, and a transaction that is more expensive is greater than 1.0. The total transaction units consumed by an MSU are the sum of the base transaction unit value and the additional transaction unit value. Transaction Units per Second (TPS) are then calculated with the total transaction unit value and the Advertised Card capacity.

For detailed information on how to calculate IP signaling TPS and the number of cards required to carry MSU traffic, see *"How to calculate transaction units per second (TPS)"* on page 36 and *"Calculate the number of cards required"* on page 44.

Scalability

Scalability is the ability to increase total throughput under an increased load proportionally to added resources such as hardware or software. For example, to add traffic and to increase throughput in a current system, the operator can replace low-speed links with IP-based links; IP-based links are much more efficient than standard TDM links. This change requires at least one card that runs the IPGWx or IPLIMx application.

Link equivalency

Figure 8 shows that a single IPLIMx application can take the place of 52 to 80 56K DS0 low-speed links; a single IPGWx application (M3UA) can take the place of 12 to 80 56K DS0 low-speed links.

Figure 8. E5-ENET link equivalency for M2PA/M3UA vs. low-speed links

Low speed link	M2PA<-> Low speed link			M3UA<->Low speed link		
Average MSU size (MTP 2 + MTP 3)	Eagle M2PA Msu/Sec	56K links IP equivalent	64K links IP equivalent	Eagle M3UA Msu/Sec	56K links IP equivalent	64K links IP equivalent
60	4000	35	30	4000	35	30
70	4000	40	35	4000	40	35
80	4000	46	40	4000	46	40
90	4000	52	45	4000	52	45
100	4000	58	50	4000	58	50
110	4000	63	55	4000	63	55
120	4000	69	60	4000	69	60
130	4000	75	65	4000	75	65
140	4000	80	70	4000	80	70
150	4000	86	75	2800	60	53
160	4000	92	80	2800	64	56

Hardware and software requirements

For SS7-over-IP networks, Tekelec uses two cards to achieve IP connectivity:

- Single-slot EDCM (SSEDCM) card
- EPM-based Ethernet (E5-ENET) card

Either of these cards can be loaded with the IPLIMx or IPGWx application:

- The IPLIMx application implements the M2PA protocol, which is used mainly for B-, C-, and D-links. Once either of the cards is loaded with the IPLIMx application, the card is referred to as the IPLIMx application.

- The IPGWx application implements the M3UA and SUA protocols, which are used for A-links. Once either of the cards is loaded with the IPGWx application, the card is referred to as the IPGWx application.

Each of these cards has a different maximum capacity for the number of TPSs that they will support. The older SSEDCM supports up to 2,000 TPS, while the E5-ENET card supports up to 4,000 TPS. The number of MSU/s supported by each of these cards is dependent on various factors including MSU size, percentage of MSUs triggering the SCCP Class 1 sequencing feature, and the Integrated Monitoring feature.

Node capacity

Per node, the Tekelec solution is scalable:

- Up to 4,000 SCTP associations (16 associations * 250 application servers)
- Up to 400,000 TPS via M2PA (100 cards * 4,000 TPS)
- Up to 256,000 TPS via M3UA (64 cards * 4,000 TPS)
- Up to 112,000 TPS via SUA

The system total depends on card limits. Table 2 list limits when combining cards and/or applications on a node.

- Number of IP cards per node for IPGWx:
  - Up to 64 SSEDCM or E5-ENET cards
  - Up to 256,000 TPS to SEPs (8 cards * 8 linksets *4000 TPS
  - Up to 256,000 TPS (64 cards * 4000 TPS)
- Number of IP cards per node for IPLIMx:
  - Up to 100 of any combination E5-ENET and SSEDCM cards
  - Up to 400,000 TPS IP Transport (100 cards * 4,000 TPS)

Table 2. Card limits by Application per Node

Application Type	Card Type		
	E5-ENET	SSEDCM	Mixed E5-ENET and SSEDCM
IPLIMx	100	100	100
IPGWx	64	64	64
Combined IPLIMx/IPGWx	100	164	*
* Contact your Sales Representative for IPLIMx configurations at or over 100.			

When considering other factors or additional configurations that impact the IMT, contact your Sales Representative for more information.

NOTE: The `rept-stat-iptps` command will provide current or peak TPS per card, linkset, and system for IPGWx applications.

Achieving IPLIMx and IPGWx applications' Advertised Capacity

A goal of properly engineered networks is to eliminate congestion. Advertised Capacity refers to the maximum TPS that can be sustained without congestion. Several factors affect TPS calculations and must be considered when calculating the expected throughput for the IPLIMx and IPGWx applications.

The IPGWx application implements traffic flow control based upon the TPS value allocated to its signaling link, which is derived from the **`iptps`** parameter setting of its linkset. Presenting a load in excess of the signaling link TPS value will result in congestion.

Factors affecting advertised capacity

The following factors affect the IP application's Advertised Capacity:

- Host card

  Some cards have different performance characteristics than others. For example, the E5-ENET card has much more memory for buffering traffic than the SSEDCM card.

- CPU utilization

  A wide variety of factors determine the processing resources required by IP applications to manage a given traffic load, and cause the processing of each MSU to be more expensive. For example, the EAGLE 5 ISS provides a feature that enables support of Class-1 Global Title traffic. When the feature is enabled and a triggering message is received by an IP signaling application, the application sends the MSU to an SCCP card for translation, and after translation, the MSU is sent back to the originating IP signaling card for post-translation routing. This extra IMT hop results in significant processing overhead in the receiving IP signaling card.

- Message buffers

  The amount of memory allocated for traffic buffers determines the maximum traffic rate and average message size that can be sustained for a certain network configuration. The buffer size is configurable through associations. For example, within the constraints of memory on the card, each association can have from 8 kb up to 400 kb of send-and-receive buffer space for SCTP.

- Card communication interfaces

  The capacity of the card's external interfaces can become a constraint for certain configurations. For example, the IMT interface capacity is affected by high-utilizing features, or the Ethernet interface configurable capacity is set to half-duplex (not 100Mb/sec full-duplex).

For detailed descriptions of factors that affect advertised card capacity, see *Engineering Rules for Determining IP^7 Application Throughput*, Tekelec, TR005007 [2].

Base transaction unit

The base IP signaling transaction unit involves an MSU sent and an MSU received, each having a Service Information Field (SIF) of less than or equal to 140 bytes, with the Data Feed feature disabled and a minimum set of features in use. A larger MSU, or an MSU that is monitored as part of the Data Feed feature, has a transaction unit cost of greater than 1.0.

The base Advertised Capacity of EAGLE 5 ISS IP signaling cards assumes an average transaction unit cost of 1.0, so a TPS rating of 2,000 = 2,000 Transaction Units per Second (TPS), each having a cost of 1.0. If the average transaction cost increases above 1.0, then the Advertised Capacity (TPS rating) of the IP signaling card decreases proportionally.

Table 3 shows the base Advertised Capacity for the SSEDCM and E5-ENET cards.

Table 3. Base Advertised Capacity

Card	Base Advertised Capacity (TPS)
SSEDCM	2,000
E5-ENET	4,000

Exceeding the Advertised Capacity may result in signaling congestion, and in combination with the Data Feed feature, may result in the application discarding Data Feed messages.

Base transaction unit rules

The base transaction unit rules are applied to establish the base transaction unit costs:

1. Sufficient IP TPS is assigned to the linkset to which the IPGWx signaling link is assigned. (IPGWx only)
2. The traffic is not monitored via the E5IS feature.
3. The percentage of received traffic that triggers the enabled EAGLE SCCP Class-1 Sequencing feature is less than or equal to 50%.
4. The IP packet loss rate is 25 per 100,000 or less.
5. IP connection message buffer memory is of a sufficient size on the IPGWx application and the peer network elements to sustain traffic for the network's RTT and worst-case packet loss.
6. The IP connection retransmission mode must be linear (RMODE=LIN) for SCTP associations.
7. The IP connection retransmit time-out is configured to a value that is appropriate for the expected network latency (RMIN for SCTP associations).
8. M2PA Timer T7 (Excess Delay in ACK) is configured to have a value appropriate for the expected network latency (IPLIMx only).

Base transaction unit costs

The base transaction unit cost is based on the configuration rules shown in *"Base transaction unit rules"*. Any additional configurations are applied to the adjusted transaction unit.

Table 4. Base transaction unit cost per MSU SIF size

MSU SIF	M2PA	M3UA	SUA		MSU SIF	M2PA	M3UA	SUA
0..140	1	1	1.33		2177..2448	9	9	N/A
141..272	1	1.43	2		2449..2720	10	10	N/A
273..544	2	2	N/A		2721..2992	11	11	N/A
545..816	3	3	N/A		2993.3264	12	12	N/A
817..1088	4	4	N/A		3265..3536	13	13	N/A
1089..1360	5	5	N/A		3537 3808	14	14	N/A
1361..1632	6	6	N/A		3809..4080	15	15	N/A
1633..1904	7	7	N/A		4081..4095	16	16	N/A
1905..2176	8	8	N/A					

Adjusted transaction unit

The adjusted transaction unit is the value calculated and tested by Tekelec that represents additional cost per base transaction unit when the configuration deviates from the base configuration.

Table 5 shows adjusted configuration scenarios and their TU values for IPGWx (M3UA) and IPLIMx (M2PA). For more information on calculating throughput based on transaction units, see *"How to calculate transaction units per second (TPS)"* on page 36.

Table 5. Additional Transaction Units for Advanced Configurations

MSU SIF Size	Adapter	Monitored by E5IS	Number of Open Conns	SLAN or SCCP Conversion	Base TU	TU Adjustment	Total TU	Max MSU/s 2000	Max MSU/s 4000
0..140	M3UA	Yes	<= 8	No	1.0	0.43	1.43	1400	2800
0..140	M3UA	Yes	<= 8	Yes	1.0	0.67	1.67	1200	2400
0..140	M3UA	Yes	> 8	No	1.0	0.82	1.82	1100	2200
0..140	M3UA	Yes	> 8	Yes	1.0	1.00	2.00	1000	2000
141..272	M3UA	Yes	<= 8	No	1.43	0.80	2.22	900	1800
141..272	M3UA	Yes	<= 8	Yes	1.43	1.24	2.67	750	1500
141..272	M3UA	Yes	> 8	No	1.43	1.65	3.08	650	1300
141..272	M3UA	Yes	> 8	Yes	1.43	1.91	3.33	600	1200

Table 5. Additional Transaction Units for Advanced Configurations (continued)

MSU SIF Size	Adapter	Monitored by E5IS	Number of Open Conns	SLAN or SCCP Conversion	Base TU	TU Adjustment	Total TU	Max MSU/s 2000	Max MSU/s 4000
0..140	M2PA	Yes	<= half max per card	No	1.0	0	1.00	2000	4000
0..140	M2PA	Yes	<= half max per card	Yes	1.0	0.38	1.38	1450	2900
0..140	M2PA	Yes	> half max per card	No	1.0	0.11	1.11	1800	3600
0..140	M2PA	Yes	> half max per card	Yes	1.0	0.54	1.54	1300	2600
141..272	M2PA	Yes	<= half max per card	No	1.0	0.54	1.54	1300	2600
141..272	M2PA	Yes	<= half max per card	Yes	1.0	1.00	2.00	1000	2000
141..272	M2PA	Yes	> half max per card	No	1.0	0.67	1.67	1200	2400
141..272	M2PA	Yes	> half max per card	Yes	1.0	1.11	2.11	950	1900

How to calculate transaction units per second (TPS)

See Table 6 to follow this process:

1. Determine which application will carry the traffic (IPGWx or IPLIMx).
2. Determine the type of card that will host the application (SSEDCM or E5-ENET).
3. Determine the adapter protocol type of the association(s) that will carry the traffic (in Table 6, the adapter is always M3UA).
4. Determine how many distinct categories of traffic will be carried by the card. Characteristics that distinguish categories include:
   - Average SIF size (1)
   - Whether or not the traffic is monitored (in Table 6, all rows have monitoring by E5IS)
   - How many connections per card will carry the traffic (2)
   - Whether Signal Transfer Point SLAN or SCCP Conversion is applied to the traffic (3)

   Distinct traffic categories are identified by rows in the table (A), (B).

5. Select the TU value that applies to each distinct category of traffic. (6)
6. If the total bi-directional MSU rate of each category ((A7), (B7)) is known in advance, then the:
   - Total TU rate for a category = MSU rate x TU value ((A7) x (A6))
   - Total TU rate to be carried by the card = Sum of all TU rates of the traffic categories ((A6) x (A7) + (B6) x (B7))

   Then compare that value to the Base Card Capacity (7).
7. If you know the fraction of total traffic that applies to each category, then you can determine maximum total MSU rate, that is, the actual Advertised Capacity, by dividing the Base Advertised Capacity (7) by the total TU value of the traffic mix (6).

Table 6. Calculating TPS

	1 MSU SIF Size	2 # of Open Conns	3 Conver-sion	4 Base TU	5 Adjust-ment	6 Total TU	7 Max MSU/s 2000	Max MSU/s 4000
A	0..140	<=8	No	1.0	0.43	1.43	1400	2800
	0..140	<=8	Yes	1.0	0.67	1.67		
	0..140	>8	No	1.0	0.82	1.82		
	0..140	>8	Yes	1.0	1.00	2.00		
	141..272	<=8	No	1.43	0.80	2.22		
B	141..272	<=8	Yes	1.43	1.24	2.67	750	1500
	141..272	>8	No	1.43	1.65	3.08		
	141..272	>8	Yes	1.43	1.91	3.33		

Calculation example

See Table 6 to follow this calculation:

- The signaling link is being monitored by E5IS (Data Feed) (A3, B3).
- Fail traffic uses M3UA adapter (A2, B2).
- Eight IP connections are open and allowed (A4, B4).
- Eighty percent of traffic involves ISUP MSUs having a SIF size less than or equal to 140 bytes (80% of A8).
- Twenty percent of traffic involves SCCP-converted MSUs having a SIF size greater than 140 bytes and less than or equal to 272 bytes (20% of B8).

(Base Advertised Capacity) =

((0.80 * (1.43)) + (0.20 * (2.67)) * (Actual Advertised Capacity)=

(1.14 + 0.53) * (Actual Advertised Capacity)=

1.67 * (Actual Advertised Capacity)

(Actual Advertised Capacity)= (Base Advertised Capacity) / (1.14 + 0.53)= 4000 / 1.67 = 2395

Once the needed throughput is established, calculate the number of cards required to support this need (see "Calculate the number of cards required" on page 5-44).

Rules for Integrated Datafeed using STC cards

Engineering Rules for Determining IP^7 Application Throughput, Tekelec, TR005007 [2] contains additional rules related to Integrated Datafeed (for IMF using STC cards).

Follow the guidelines and consult the tables in *Engineering Rules for Determining IP^7 Application Throughput*, Tekelec, TR005007 [2] to determine:

- Effects of different Integrated Monitoring configurations
- Association buffer sizes
- Throughput per association
- Congestion Window Minimum size

Functionality of configurable SCTP buffer sizes per association

The amount of memory allocated for traffic buffers determines the maximum traffic rate and average message size that can be sustained for a specific network configuration. Memory is a constraint in achieving advertised capacity due to queuing, message storing and packet retention for retransmission over the Ethernet physical transport. As a general rule, the greater the Round Trip Time (RTT) for a packet, the greater the need for memory to store the unacknowledged packets being sent to the peer. Since each card has a finite amount of memory, the allocation is spread across all the links or connections on the card. This means that as a card's hosted-association(s) buffer sizes increase, the maximum number of associations that can be hosted by the card decrease.

The SCTP buffer size is configurable per association. Within the constraints of memory on the card, each association can have 8 kb to 400 kb of send-and-receive buffer space for SCTP.

Table 7 lists the maximum memory available for SCTP buffers on each card type.

Table 7. SCTP Buffer Space per Connection, Card and Application

Card	IPLIMx Max # Conns	IPLIMx Default Conn Buffer	IPLIMx Max. Conn Buffer	IPLIMx Max. Total Buffer	IPGWx Max # Conns	IPGWx Default Conn Buffer	IPGWx Max. Conn Buffer	IPGWx Max. Total Buffer
SSEDCM	8	200KB	400KB	1,600KB	50	16KB	400KB	800KB
E5-ENET	16	200KB	400KB	3,200KB	50	16KB	400KB	3,200KB

NOTE: No card or application combination supports the maximum number of connections with each connection having the maximum buffer size.

System constraints affecting total IP card capacity

Table 8 shows constraints involved in using multiple IP signaling cards and applications.

Table 8. IPLIMx and IPGWx connectivity data

Feature	IPLIM (SSEDCM/ E5-ENET)	IPGWx (SSEDCM/ E5-ENET)	Notes
Cards per system	100	64	Worst-case inter-shelf IMT utilization is a key factor. Total number of E5-ENET cards for IPLIMx cannot exceed 100.
Link connectivity type	Point to point (1 connection per link)	Point to multipoint	
Link type replacement	Any	A	
Typical application	Interconnect transfer point	Interconnect a front-end SS7 gateway to a back-end service element	
Links per card	8/16	1/1	Worst-case inter-shelf IMT utilization is a key factor. Virtual signaling link. Terminates SS7 network (IPGWx)
Links per linkset	16	8	Assumes unmated configuration. Linkset defines the scope of a mateset/SG. If mated, then only one link is allowed in the linkset.
Supports combined linksets	Yes	No	
IP connections per system	4000		
IP connections per card	8/16	50/50	SCTP associations
Routing keys per system	---	2,500	
IP connections per routing key	---	16	
Application Servers per system	---	250	

Table 8. IPLIMx and IPGWx connectivity data (continued)

Feature	IPLIM (SSEDCM/ E5-ENET)	IPGWx (SSEDCM/ E5-ENET)	Notes
Associations per Application Server	---	16	
Ethernet interfaces per card	2		Unihomed connection on either interface, multihomed using both interfaces
EAGLE 5 ISS Hardware Redundancy Model	2N		
Capacity (TPS)	2000/4000 MSU/s	2000/4000 MSU/s	2.5/5K is the goal
Failure mode (80%)	1600/3200 MSU/s	1600/3200 MSU/s	Capacity growth required at this point
Multihoming support	Yes		
Connection model	Peer to peer	Server	
SS7 routing	Traditional least-cost based	Two-step traditional SS7 least-cost plus route keys	
Supports lossless changeover	Yes	No	IPGWx relies on SCTP for sequencing
Supports network management	Yes		
Number of DTA Point Codes	1		Implies one IPGWx mateset if DTA PC route involves IPGWx linkset
Number of internal point codes per network	1		Implies one IPGWx mateset per network domain for end-office mode of operation
IPTPS for System	---	Purchase quantity	Total pool of capacity distributed by user across IPGWx linksets
IPTPS per IPGWx linkset	---	System IPTPS	
IPTPS per IPGWx signaling link	---	Linkset IPTPS	
IMT Inter-Shelf Capacity, each bus, ring topology	1 Gb/sec		Full-Duplex

SIGTRAN engineering guidelines

This section provides general SIGTRAN engineering guidelines with examples of normal and failover scenarios and resulting MSU calculations. Some overall guidelines to keep in mind include:

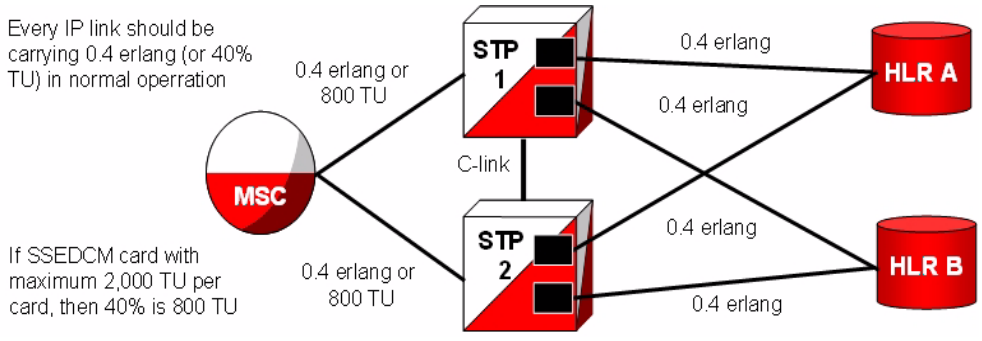
- Perform SIGTRAN engineering like TDM links
- Utilize Transaction Unit (TU/MSU) mapping
- For an IPGWx or IPLIMx card, the total capacity per card is considered one erlang

  Erlang is a statistical measure of the volume of telecommunications traffic. Traffic of one erlang refers to a single resource being in continuous use, or two channels being at 50% use, and so on.
- In a normal scenario, run the card at a maximum of 40% total capacity or 0.4 erlang
- In failover scenarios, the card runs at 80% of total capacity or 0.8 erlang

The IPLIMx and IPGWx applications can be configured as either an IPLIMx supporting M2PA B-, C-, and D-Links; or as an IPGWx card supporting A- and E-Links (see the note under *"M3UA (MTP Level 3 User Adaptation Layer) protocol"* on page 10 for more information about A-links).

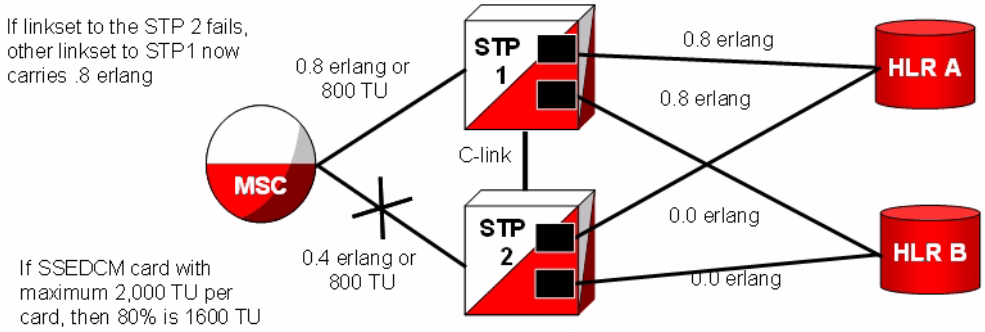
Every IP link should carry 0.4 erlang (or 40% TU) in normal operation. For an SSEDCM card with a maximum of 2,000 TU per card, 40% is 800 TU; see Figure 9.

Figure 9. SIGTRAN: Every IP link at 0.4 erlang



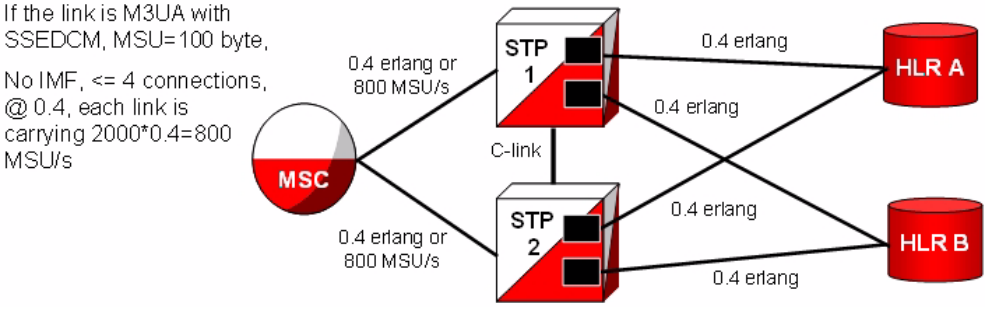
If the linkset to STP2 fails, another linkset to STP1 now carries 0.8 erlang. For an SSEDCM card with a maximum of 2,000 TU per card, 80% is 1,600 TU; see Figure 10.

Figure 10. SIGTRAN: Failover at 0.8 erlang



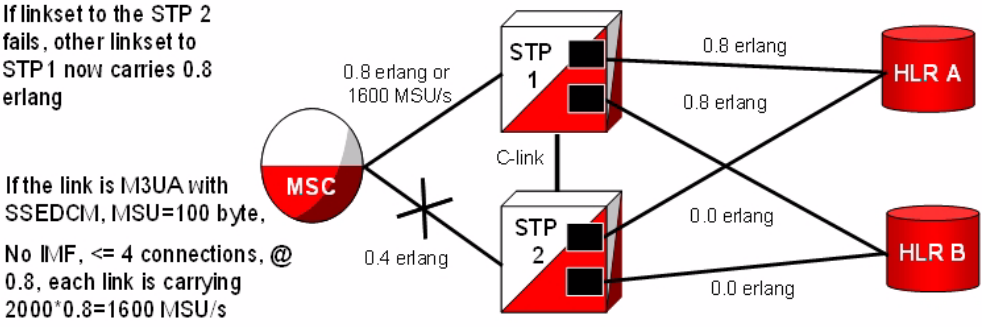
If the link is M3UA with an SSEDCM, a 100-byte MSU, no IMF, and 4 or less connections at 0.4 erlang, each link carries 800 MSU/s (2000*0.4); see Figure 11.

Figure 11. SIGTRAN: Every link at 0.4 erlang and 800 MSU/s



If the linkset to STP2 fails, another linkset to STP1 now carries 0.8 erlang. If the link is M3UA with an SSEDCM, a 100-byte MSU, no IMF, and 4 or less connections at 0.8 erlang, each link carries 1600 MSU/s (2000*0.8); see Figure 12.

Figure 12. EAGLE 5 ISS: Failover at 0.8 erlang and 1600 MSU/s



Calculate the number of cards required

Below are examples of calculations to determine how many cards are needed. These are somewhat simplified; precise calculations require data about the specific network and the traffic running over it.

Example (without monitoring)

Assumptions:

- Mated pair of Signal Transfer Points
- Customer needs 10,000 MSU/s from Mobile Switching Center to Signal Transfer Point
- Average MSU size is 100 bytes/MSU over M3UA
- Less than 5 connections per IP SSEDCM card
- No monitoring is required

Calculation:

- During normal operation, each Signal Transfer Point should handle 5000 MSU/s
- During failover operation, each Signal Transfer Point should handle 10,000 MSU/s
- Each SSEDCM over M3UA with up to 4 connections and 100 byte/MSU without monitoring can support 2000 MSU/s

  So 2,000 is 1 erlang

  @40% = 800 MSU/card

  To support 5,000 MSU/sec @ 40% rate, we need 7 cards per Signal Transfer Point.

Example (with monitoring)

Assumptions:

- Mated pair of Signal Transfer Points
- Customer needs 10,000 MSU/s from Mobile Switching Center to Signal Transfer Point
- Average MSU size is 100 bytes/MSU over M3UA
- Less than 5 connections per IP SSEDCM card
- Monitoring is required

Calculation:

- During normal operation, each Signal Transfer Point should handle 5000 MSU/s
- During failover operation, each Signal Transfer Point should handle 10,000 MSU/s
- Each SSEDCM over M3UA with up to 4 connections and 100 byte/MSU with monitoring can support 1400 MSU/s

  So 1,400 is 1 erlang

  @40% = 560 MSU/card

  To support 5,000 MSU/sec @ 40% rate, we need 9 cards per Signal Transfer Point.

  IPLIMx linksets are permitted up to 16 links or, if one link per card, 16 cards. IPGWx linksets are permitted up to 8 links; at one per card, 8 cards are allowed. An Application Server (i.e., in M3UA, a point code) is not permitted to span linkset boundaries, so the prescribed traffic rate would require a different architecture. For example, two Application Servers with different point codes could be used, one with 4 cards and one with 5 cards. A better solution, however, would be to segregate the traffic by type prior to reaching the SS7-over-IP cards, using smaller multiple servers and smaller linksets.

IPGWx congestion management options

There are two options for congestion management: either discard new messages (which is how MTP3 congestion is handled) or fail a connection.

The IPGWx application is designed to match MTP3 congestion procedures. With this option, the connection congestion status is not shared, and altering routing strategy based on congestion events is stopped. Instead, new messages destined to the congested connection are discarded, a new measurement is pegged, and response-method Transfer Controlled (TFC) messages are generated. This routing strategy only changes due to adapter state events.

A configurable timer (False Connection Congestion Timer) sets the maximum amount of time that a connection can remain congested before it is failed. This timer is similar to the MTP3 False Link Congestion timer (T31).

This Match MTP3 Congestion Procedures option has several advantages: it is simple to implement, prevents missequencing during connection congestion, and notifies the originator of a discarded MSU due to the congestion. The primary disadvantage is that MSUs may be discarded that otherwise may have been transmitted (which is the same as for link congestion).

The configurable UA Parameter Set (UAPS) Timer 'False Connection Congestion Timer' allows the user to specify the maximum amount of time an association can remain congested before it is taken out of service. The default setting for the timer is 3,000 ms, the minimum is 0 ms, and the maximum setting (enforced by the IPGWx L2 software, not by the **`chg-uaps command`**) is 30,000 ms.

Redundancy and link engineering

A properly designed SS7 network always provides at least two physically separate ways to transmit user data. To provide the same level of redundancy using the IP-based solution, node and card redundancy can be used.

The EAGLE 5 ISS can be deployed with completely redundant IP network paths, each of which must be capable of sustaining the worst-case traffic load; or a redundancy model that relies on a mate Signal Transfer Point for IP path redundancy, although this option is less robust (and less expensive).

Unihoming versus multihoming

The EAGLE 5 ISS can be deployed with completely redundant IP network paths, each of which must be capable of sustaining the worst-case traffic load. Either of these two methods can be applied, depending on the application used:

- Unihomed links (for M2PA links)
- Multihomed links (for M2PA, M3UA and SUA links)

Unihoming

For unihoming, a set of IPLIMx cards, which are configured for worst-case traffic load, hosts one signaling link per linkset. Each signaling link is assigned to a unihomed SCTP association, where half of the associations are assigned to one independent IP network path, and the other half are assigned to another independent IP network path. Each network path must have dedicated bandwidth sufficient to sustain the worst-case traffic load.

Multihoming

For multihoming, a set of IPLIMx cards, which are configured for worst-case traffic load, is hosting one signaling link per linkset. Each signaling link is assigned to a multihomed SCTP association, which is mapped to an IP network having at least two completely redundant paths. Each network path must have dedicated bandwidth sufficient to sustain the worst-case traffic load.

Multihoming is very important for M3UA and SUA connections because it is the only means of lossless handover in the event of a path failure.

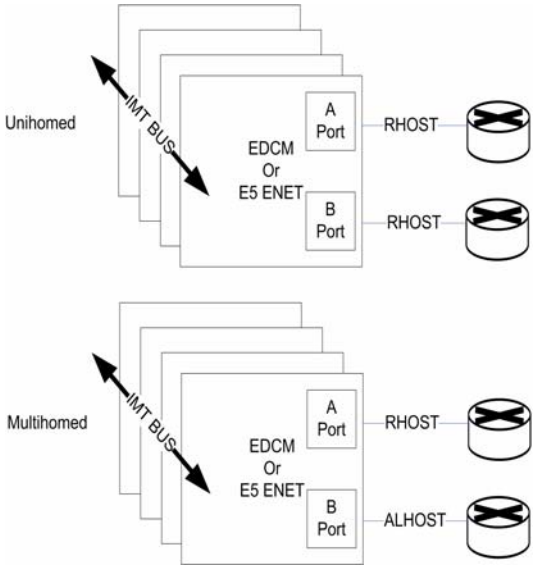
Multihoming provides network-level resilience for SCTP associations by providing information on alternate paths to a signaling end point for a single association.

SCTP multihoming supports only communication between two end points, of which one or both are assigned with multiple IP addresses on possibly multiple network interfaces. Each IPLIMx or IPGWx card maintains a single static IP route table, utilized by both Ethernet interfaces or ports. By checking the destination address in this IP route table, the router determines the port from which the message is transmitted by the IPLIMx or IPGWx card.

This means that it is not possible to have a route to a single destination from both ports of an IP card – it must be one port or the other.

SCTP multihoming does not support communication ends that contain multiple end points (i.e., clustered end points) that can switch over to an alternate end point in case of failure of the original end point.

Figure 13. Unihoming versus multihoming



Choosing a redundancy method for M2PA links

Unihoming is simpler to configure but more expensive than multihoming, in terms of computational power and network bandwidth to handle worst-case failure. Unihoming requires change-over procedures and rerouting if a network path is interrupted, whereas a multihomed SCTP association will simply switch to the alternate network path.

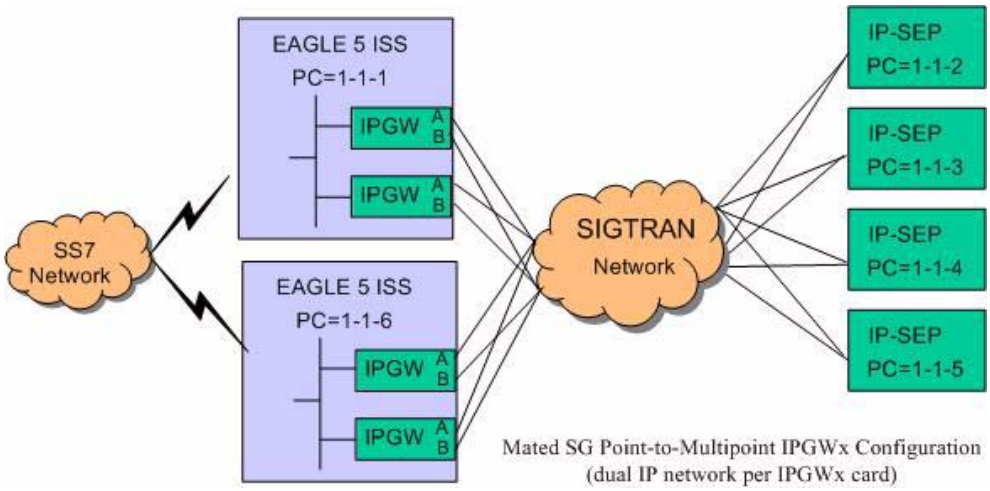
SCTP multihoming in general is less mature than MTP3 change-over procedures. In addition, the lack of ARHOST configurability in the EAGLE 5 ISS can result in asymmetrical traffic on a multihomed connection when both paths are available, which may be undesirable for the operator.

The EAGLE 5 ISS fully supports both options for M2PA, but Tekelec recommends unihoming.

Mated Signal Transfer Point redundancy

If a completely redundant IP network path is not available, then a redundancy model that relies on a mate Signal Transfer Point for IP path redundancy is supported by Tekelec. This model is less robust but also less expensive.

Figure 14. Mated Signal Transfer Point redundancy



IPGWx mateset

An IPGWx mateset is an IPGWx card linkset configuration with two mutually exclusive settings:

- Unmated: up to eight IPGWx cards can be defined in a single IPGWx linkset. The cards within each IPGWx mateset must work together to provide reliable transport for connected IP-based MTP user-part applications. Dynamic data, such as IP connection status, IP destination status, and SS7 connection status must be shared between IPGWx mate cards. Tekelec currently limits the maximum number of cards in a mateset to eight; this is a conservative number but necessary to ensure that the sharing of information between cards (in worst-case scenario) does not overload the IMT bus in the EAGLE 5 ISS.
- Mated: Two IPGWx linksets are allowed in a mateset by using the **`matelsn`** linkset parameter. The limitation of this approach is that each IPGWx linkset can have only one card. This configuration is supported to be backward compatible with previous EAGLE 5 ISS software versions.

IPGWx status sharing

Each IPGWx card supports up to 50 IP connections, each of which can be available or unavailable for SS7 traffic. Expanding the number of cards in a mateset also means that the worst-case number of status messages to be communicated during run-time grows by the square of the number of cards. The exponential increase in status messages can have a significant impact on IMT bus utilization.

IP destination status

Proper implementation of SS7 network management on behalf of IP-based point codes requires that the cards comprising an IPGWx linkset have a common view of destination availability. Destination availability status is based upon the availability of IP connections assigned to various routing keys. Each card must know which other cards in the linkset have connections available for a given destination. When the total count of available connections for a destination changes from 0 to 1, then a Transfer Allowed (TFA) needs to be generated. When the total count changes from 1 to 0, then a Transfer Prohibited (TFP) needs to be generated.

SS7 network status

IPGWx cards within a mateset must maintain a shared view of SS7 network status and inform IP Signaling Points of changes in this shared view. There are three kinds of SS7 network status:

- SS7 destination availability
- Route congestion status
- User part unavailability

Signaling Link Selection (SLS) routing

A Signaling Link Selection value is a 5- or 8-bit integer (ANSI) or 4-bit integer (ITU) that is used to identify the linkset and link to which a message is to be transported. The SLS value is included in the SLS field, which is part of the MSU's MTP routing label.

The SLS is used to evenly distribute traffic across routes and links, assuming that the SLS values are randomly distributed by the originating node.

The Tekelec SS7-over-IP solution follows standard SLS load sharing with IPLIMx. With IPGWx, SLS values are distributed over the associations in the Application Servers.

LAN/WAN considerations

The operational characteristics of the LAN/WAN need to be quantified. Following is a list of general rules for the LAN/WAN environment devoted to SS7-over-IP traffic.

- Keep the number of nodes per LAN subnet as low as possible.

  The number of nodes attached to a LAN segment is a major influence in overall LAN performance. As the number of nodes increases on a LAN segment, the performance will tend to decrease due to contention for the LAN resource. For optimal performance, this number should be kept as low as possible.

- Be aware of all the node and traffic types on the LAN.

  From the SS7-over-IP perspective, there are two types of nodes: SS7-over-IP-related nodes (which are IP-equipped nodes involved in the overall signaling solution, such as the EAGLE 5 ISS, IP Service Control Points, Media Gateway Controllers and Media Gateways, and any management platforms doing work directly related to the SS7-over-IP solution); and non-SS7-over-IP nodes. Non-SS7-over-IP nodes are any other devices that could be on the LAN using LAN bandwidth, such as file servers or other hosts not directly involved in the signaling solution. If non-SS7-over-IP nodes are deployed on the same LAN as SS7-over-IP nodes, then the nodes will have to share the LAN resources.

- Dedicate sufficient bandwidth to your IP Signaling traffic.

- Restrict, or severely limit, the number of non-SS7-over-IP nodes.

  If non-SS7-over-IP nodes are on the network, their LAN throughput needs to be well understood, and the worst-case traffic from these sources needs to be considered. Normally it is easier to monitor (baseline) and predict network behavior when the nodes are similar. This is an important factor that will influence network performance.

- Plan for and allocate LAN capacity to handle worst-case scenarios.

  Consider all traffic sources and compute worst-case numbers that estimate LAN throughput, including failure scenarios that may switch traffic from one LAN to another. The evaluation of throughput should always be based on the worst-case traffic for each device.

- Monitor LAN performance and make adjustments as necessary.

  Once the network is implemented, the LAN throughput and utilization should be monitored for a period of time sufficient to fully understand the traffic on that LAN. Measure the LAN utilization over time and ensure that it is always at an acceptable limit (<= 35 percent of maximum LAN throughput).

- Once the network is implemented, the RTT should be checked.

  Confirm that the RTT is appropriate to achieve the maximum desired throughput, and that the RTT is acceptable from the viewpoint of the applications that are originating the traffic.

IP network planning must be executed carefully to realize the benefits of SS7-over-IP deployments. Tekelec can assist with characterizing your LAN/WAN QoS parameters and engineering an SS7-over-IP solution. Contact your Tekelec Sales Representative for more information related to this Professional Service.

Retransmission concept

The Tekelec-recommended IP network environment for signaling traffic has:

- RTTs set according to traffic (see "Refine RTO parameter" on page 5-65)
- Minimal errors (< 0.01%)
- Minimal jitter

A transport protocol provides transport reliability through two mechanisms:

1. Explicit Data Acknowledgements: the sending side retains transmitted data until the receiving side explicitly acknowledges its receipt
2. Retransmission Timer: the sending side maintains a timer, and if the timer expires prior to receiving an acknowledgement for the transmitted data, then the sender will "retransmit" the data to the receive end

Retransmissions and destination status

When transmitting data on a multihomed association, the initial transmission is made to the primary address on the primary path. If the initial transmission times out, then the first retransmission is made to an alternate destination in a round-robin, consecutive fashion. The SCTP layer will continue to send the initial transmission of new data arriving for transmission from upper layers on the primary path.

If a unihomed SCTP endpoint is not in contact after RTIMES errors, the end point address is marked as unreachable. For multihomed associations, if an endpoint's address is not in contact after RTIMES/2 errors, the address is marked as unreachable.

An error is a failure to Selectively Acknowledge (SACK) a transmitted packet or acknowledge a heartbeat within a Retransmission Time Out (RTO). Alternate paths exchange heartbeats as a means of confirming connectivity, and failure to acknowledge heartbeats would cause an alternate destination to be marked as unreachable.

SCTP timers

Tekelec provides two retransmission modes: RFC and Linear. The SCTP retransmission control feature allows the tailoring of retransmissions to detect a network fault in a timely fashion through these configuration parameters:

- RMODE: Selects desired retransmission mode (RFC or LIN)
- RTIMES: Maximum number of retransmits attempted before the connection is declared lost (3 to 12); the default is 10
- RTO: Time to wait before the current retransmit attempt is declared a failure. This time is dynamic because it is a moving average of the network.
- RMAX: Upper bound of calculated RTO (10 ms to 1,000 ms); the default is 800; Tekelec suggests 3 * RMIN
- RMIN: Lower bound of calculated RTO (10 ms to 1,000 ms). The default is 120; Tekelec suggests the greater of (1.2 * average RTT) or (10 ms + average RTT).
- CWMIN: Minimum Congestion Window Size (1,500 to 192K); the default is 3K

RFC timer setting

With an exponential timer setting, the RTO value is doubled for each retransmit attempt. When transmitting a packet, the RTO has to expire before attempting to retransmit. With the second attempt, the last RTO value is doubled (RTO * 2) before retransmitting; with the third attempt, the last RTO value is doubled again (RTO * 4); and so on. This method significantly increases the time to determine that a link is lost.

For example, if data is being transmitted for five retransmits, the time to determine a lost link is:

```
RTO.min * Path.Max.Retransmits (or 1 + 2 + 4 + 8 + 16 + 32)
= 63 sec
```

Table 9 shows RFC timers and their RFC and Tekelec-recommended default values.

Table 9. SCTP Configuration Data Descriptions for Tekelec EAGLE 5 ISS

RFC Name	Description	RFC Recommend-ed Default Value	Tekelec Default Value	Tekelec Configurable?	Tekelec Ranges
RTO.initial	Initial RTO Value	3 seconds	120 ms	Yes Assoc RMIN parameter	10-1000 ms
RTO.max	Upper limit of RTO	60 seconds	800 ms	Yes Assoc RMAX parameter	10-1000 ms
RTO.min	Lower limit of RTO	1 second	120 ms	Yes Assoc RMIN parameter	10-1000 ms
Max.Init. Retransmits	Maximum Initial Retransmit Attempts	8 attempts	10 attempts	Yes Assoc RTIMES parameter. Not configurable independently of *Assoc.max. retrans*	1-12
Association.max. retrans	Maximum Association Data Retransmit Attempts	10 attempts	10 attempts	Yes Assoc RTIMES parameter	1-12
Path.max.retrans	Maximum Data Retransmit attempts per Destination (used for multi-homin g only)	5 attempts	5 attempts	Indirectly ½ of the assoc RTIMES parameter	1-6
Acknowledge-ment timer	SACK Transmit Timer	User Configurable not to exceed 500 ms	½ RTO or 200 ms, whichever is less	Indirectly RTO is bound by the assoc RMIN and RMAX parameters	5-200 ms

Table 9. SCTP Configuration Data Descriptions for Tekelec EAGLE 5 ISS (continued)

RFC Name	Description	RFC Recommend-ed Default Value	Tekelec Default Value	Tekelec Configurable?	Tekelec Ranges
T3-rtx	Data Retransmit Timer	RTO (see RTO.initial for initial value)	RTO (see RTO.initial for initial value)	Yes RTO is bounded by the assoc RMIN and RMAX parameters	10-1000 ms
T1-init	Init retransmit timer	Initially, 3 seconds RTO thereafter	Initially, 1 second RTO thereafter	No for initial value Indirectly thereafter via RMIN/RMAX bounding of RTO	10-1000 ms
HB.Interval	Heart Beat Interval	30 seconds	500 ms	No	500 ms
Shutdown timer	Shutdown timer t2	RTO	RTO	Indirectly RTO is bound by the assoc RMIN and RMAX parameters	10-1000 ms
Cookie Timer	Cookie-t1 – Cookie Echo retransmit timer	Initially 3 seconds RTO thereafter	Initially 1 second RTO thereafter	No for initial value Indirectly thereafter via RMIN/RMAX bounding of RTO	10-1000 ms
Cookie life	Cookie Life	60 seconds	5 seconds	No	5 seconds

LIN timer setting

Tekelec has implemented a more aggressive timer method called Linear (LIN), in which the RTO between attempts is constant. Tekelec recommends this setting to detect a failure more quickly than the RFC method.

With the LIN timer setting, the time to declare the association down is at least

```
RMIN * RTIMES
```

For very high throughput associations, RTIMES (and if possible, RMIN) should be lowered and CWMIN increased. CWMIN is the parameter that sets the minimum size of the congestion window, which determines the number of packets that can be sent without having received the corresponding ACK packets.

On the far end, the LIN mode can coexist with RFC mode, but in contrast to the Signaling Gateway, the far-end may experience congestion in the ASP-to-SGP direction because of network impairments.

Jitter effects

Since the RTO is a moving average of network RTT samples, as the jitter range increases, bounding the lower limit of the RTO at or near the average will cause the amount of unnecessary retransmissions to increase, since for each transmission that takes longer than the current RTO to acknowledge a retransmission will occur, wasting bandwidth.

If the lower limit of the RTO is bounded to the upper end of the jitter range to minimize retransmits, then connection failure detection time is similarly increased.

So, minimizing jitter in the network translates into a small range for network RTT, and the RTO can be bounded to minimize retransmissions while being able to detect a loss of connection in a timely fashion.

Configure Congestion Window Minimum (CWMIN) parameter

The CWMIN parameter is important in managing traffic flow and retransmissions under varying network conditions. Changing the congestion window by setting CWMIN to a higher value affects how long it takes to recover from the retransmit event. This limits how far the window gets closed in a retransmit-event condition. In the extreme case, one could set CWMIN to the configured buffer size, which allows the entire buffer bandwidth to be used.

As a general rule, setting CWMIN to a value equal to half of the traffic rate in an RTT interval should allow adequate retransmit-recovery time while preventing excessive load to the peer:

```
CWMIN = (Bytes/Sec * RTT) / 2 bytes
```

NOTE: Setting CWMIN to a value much higher than MTU will result in periodic intermediate node overloads. CWMIN can't be set less than 3K and should normally be set to ~64K or greater. The specific value chosen for the sender should take into account network latency, configuration, packet loss, capacity, and traffic characteristics. It is important that RMIN be set to a value greater than the expected average RTT to minimize false retransmissions.

Implementation

Hardware requirements

Some of the hardware requirements specific for a Tekelec SS7-over-IP network are described here. However, for a full list customized for your planned network, contact your Sales Representative.

EAGLE 5 ISS

A fully configured EAGLE 5 ISS configured for SS7-over-IP consists of at least one IPLIMx or one IPGWx application. The applications can be installed on either an SSEDCM or an E5-ENET card.

A HIPR card is required in shelves equipped with E5-ENET cards. If a HIPR card is installed, all other shelves must be equipped with either all HMUX cards or all HIPR cards in one shelf; no shelf can contain a mix of HMUX and HIPR.

Table 10 shows the cards and their Advertised Capacity in TPS. Also, review *"Card limits by Application per Node"* on page 32.

Table 10. EAGLE 5 ISS IP signaling maximum capacities by card and application

EAGLE 5 ISS Card Name	IPLIMx Capacity	IPGWx Capacity
Single-Slot Enhanced Database Communication Module (SSEDCM)	2,000	2,000
EAGLE 5 ISS Ethernet (E5-ENET)	4,000	4,000

The capacities listed in Table 10 are achieved when the traffic carried by the application involves no feature or network attribute that requires excessive CPU, memory or transport capacity. Rates in excess of the values shown will result in signaling link or IP connection congestion.

Integrated Message Feeder (IMF)

When monitoring IPLIMx or IPGWx links using IMF, Tekelec requires that HIPR cards and at least one STC card are configured on the same shelf as the IPLIMx or IPGWx cards. Only M2PA links that are RFC 4165 compliant can be monitored. A minimum of two STC cards are required per system to turn on the monitoring feature in the EAGLE 5 ISS.

When monitoring M2PA, M3UA and SUA links, the Data Feed or monitoring subsystem requires a significant amount of CPU and memory resources from the IPLIMx or IPGWx cards. When enabled, this capability causes the advertised capacity of the IPGWx and IPLIMx applications to drop well below the maximum capacity of the host platform. For a detailed analysis of IP^7 throughput for provisioning purposes, refer to *Engineering Rules for Determining IP^7 Application Throughput*, Tekelec, TR005007.

Installation of the SS7-over-IP system includes both hardware installation and software provisioning, and is detailed in the EAGLE 5 ISS customer documentation.

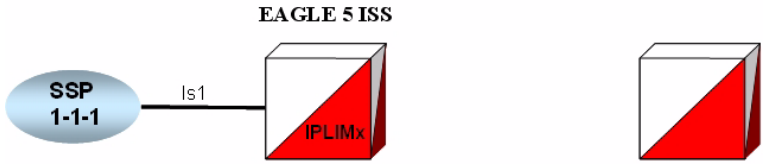
Configuration

This section describes the configuration sequence for the IPLIMx and IPGWx applications.

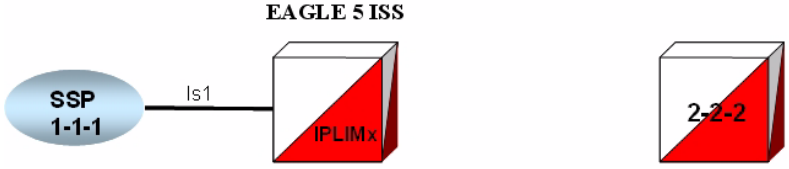
Configure the IPLIMx application

This section provides a basic overview of the steps involved to provision the IPLIMx application for M2PA. For detailed procedures, see the *Database Administration Manual - IP^7 Secure Gateway* of your current EAGLE 5 ISS documentation suite.

1. Declare the DCM to be iplim or iplimi (ent-card).

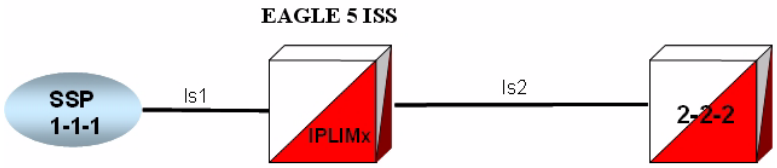


2. Enter adjacent point code (ent-dstn).



3. Define capacity and use alarm (ent-ls).

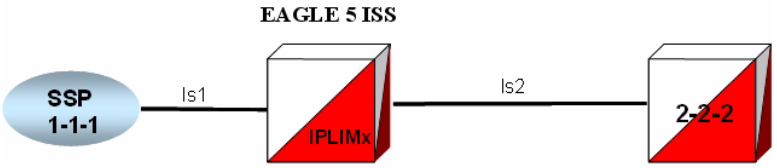
   `ent-ls:iptps:lsusealm=`



4. Tell the EAGLE 5 ISS that this is a SIGTRAN M2PA link (ent-slk).
5. Enter route (ent-rte).

SS7 Routing Table

DPC	lsn	rc
1-1-1	ls1	10
2-2-2	*ls2*	*10*



6. Define the IP settings for the Ethernet port (chg-ip-lnk):
   a. Declare what card and port you are defining with this command
   b. Associate an IP address to that card and port
   c. Set the Ethernet settings for the card and port
7. Define the host name of every IP address to be accessed (ent-ip-host).

   This step sets up a static IP address Host Table, which associates Domain Names to IP addresses so that the computer can look up Domain Names and place the corresponding IP address in the packet header. The alternative is to use a DNS server.
8. Define the network devices that the DCM card will access, for example, DNS or router (chg-ip-card).
9. Define routes through routers other than the default router defined in the ent-ip-rte command (optional).

   Limits:

   - 64 routes per card
   - 1,024 routes per EAGLE 5 ISS

10. Enter an Application Server Process and bind an SCTP association with it (ent-assoc).

This command configures the SCTP association in the Internet Protocol Application Socket (IPAPSOCK) table. This command permits the association to transport protocol data units and adaptive layer peer messages. Each association is connected to a process at the far end.

The IPAPSOCK table is used to associate the Local Host/Local Port to a Remote Host/Remote Port.

11. Allow card (alw-card).

12. Activate signaling link (act-slk).

Configure the IPGWx application

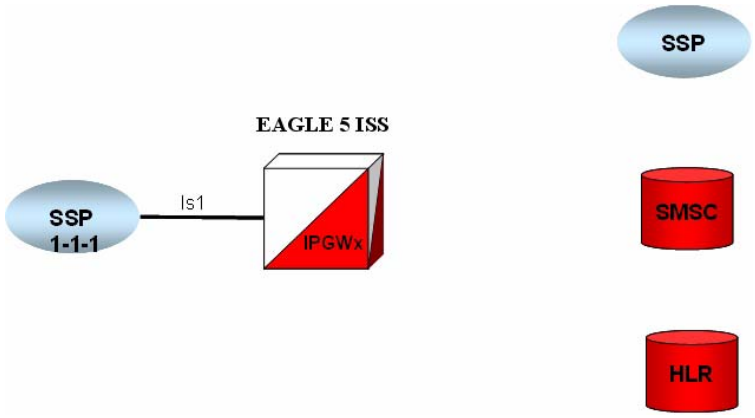
This section provides a basic overview of the steps involved to provision the IPGWx application for M3UA. For detailed procedures, see the *Database Administration Manual - IP^7 Secure Gateway* of your current EAGLE 5 ISS documentation suite.

1. Enable the feature with the part number and feature access key (FAK) (enable-ctrl-feat).

IPGWx IP TPS implies a true system limit. Each IPGWx linkset will have a configurable "linkset IP TPS", and the total of all the provisioned linkset IP TPS values must be less than or equal to the IPGWx system IP TPS.

2. To help manage IPGWx system IP TPS, view the system wide IP TPS usage (rept-stat-iptps).

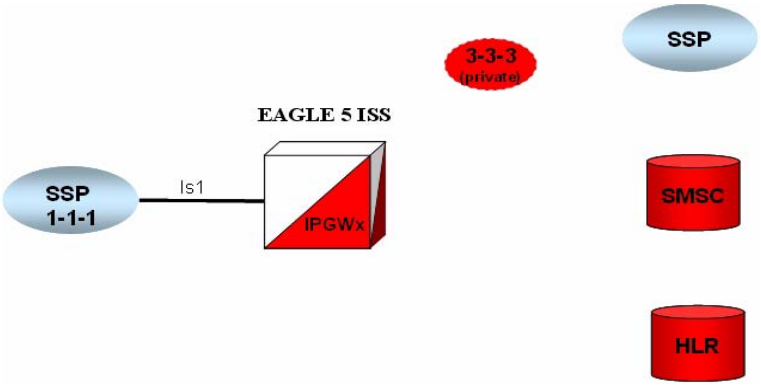
3. Declare the DCM to be ipgwx (ent-card).



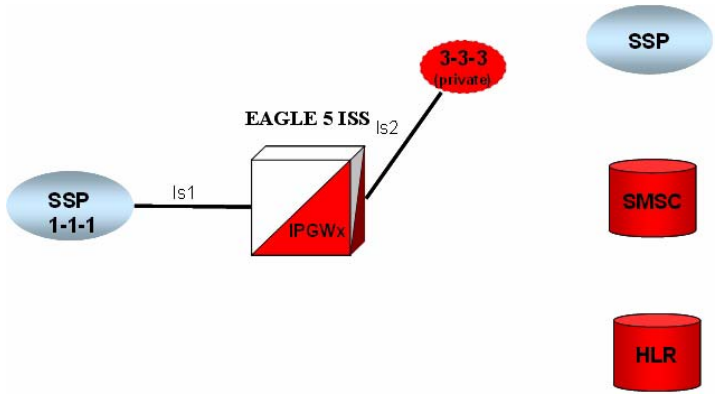
4. Enter the virtual point code (ent-dstn).

To create a virtual IPGWx SS7 link, first create an SS7 linkset and an Adjacent Point Code (APC).

The adjacent node functionality for an IPGWx linkset is performed by the IPGWx software to provide SS7-to-IP interworking. For this reason, IPGWx APCs are referred to as "adjacent" point codes. Syntaxes that are normally not allowed for point codes, such as 0-0-1, are allowed for virtual adjacent point codes to minimize depletion of point code space. In addition, beginning with EAGLE 5 ISS 34.0, private point codes can be utilized (and are recommended by Tekelec) for IPGWx APCs. Private point codes are used for internal routing within the EAGLE 5 ISS and are not known outside of the EAGLE 5 ISS. By making APCs private, it is possible to have a point code value indicated as private and still have the same point code value (as not private) available for network configuration.

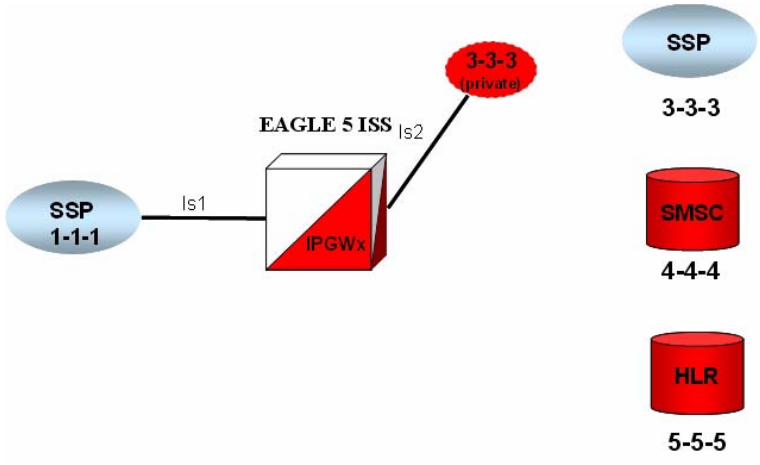


5. Define bandwidth and use alarm (ent-ls).

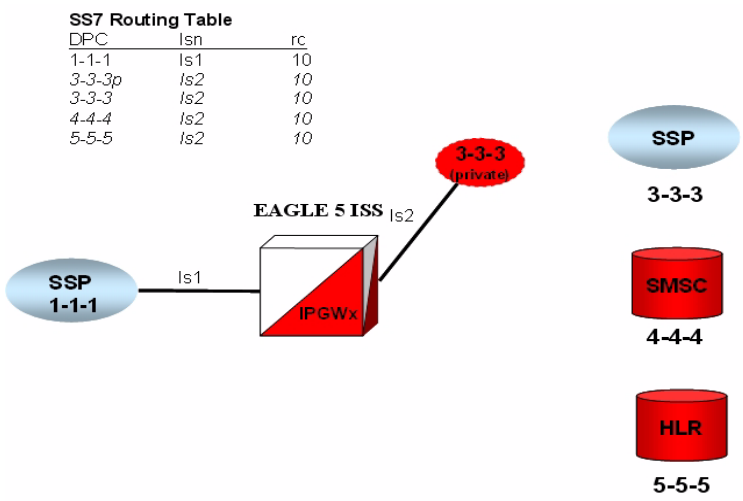


6. Tell the EAGLE 5 ISS that this is a SIGTRAN M3UA link (ent-slk).

7. Enter SEP point codes (ent-dstn).

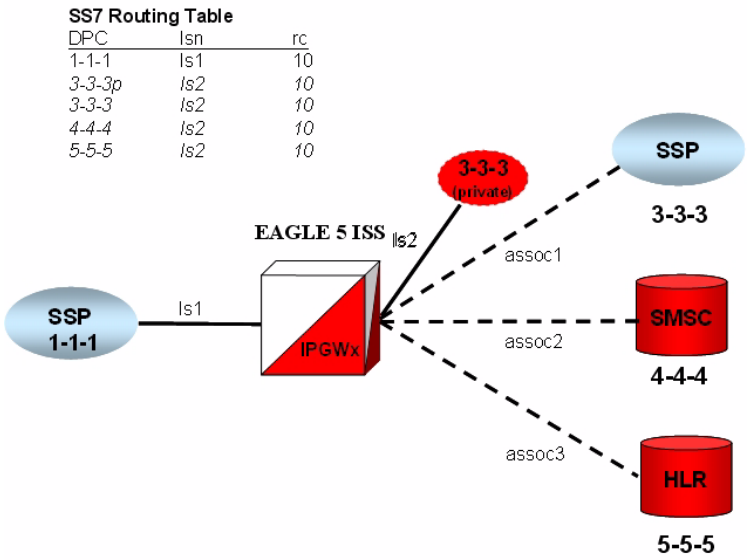


8. Enter route (ent-rte).



9. Define the IP settings for the Ethernet port (chg-ip-lnk).
10. Define the host name of every IP address to be accessed (ent-ip-host).
11. Define the network devices that the DCM card will access (chg-ip-card).
12. Enter an Application Server Process and bind an SCTP association with it (ent-assoc).

    A SCTP association is a connection to a process on the far end.



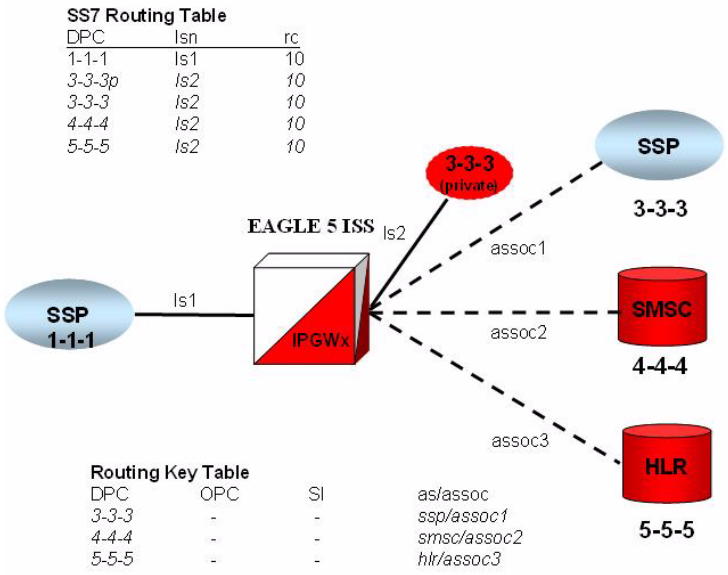
Multihomed end points are SCTP associations configured with both the LHOST and ALHOST parameters specified. In this case, the LHOST represents an IP address corresponding to one of the network interfaces (A or B) of the IP application card, while the ALHOST represents an IP address corresponding to the other network interface of the same IP application card.

This command includes the **rmin** and **rmax** parameters.

13. Associate a routing key to an association name (ent-as).

An Application Server is a logical entity serving a specific routing key or set of routing keys. The first **ent-as** command entered creates the Application Server, and subsequent **ent-as** commands add additional associations to the existing Application Server.

14. Define routes through routers other than the default router defined in the chg-ip-card command (ent-ip-rte and ent-appl-rtkey).



15. Set the network context for the message, either for the Signaling Gateway process or application server process (ent-na).

16. Allow card (alw-card).

17. Activate signaling link (act-slk).

Refine timers and parameters

Define RTIMES association retransmits

Set RTIMES such that an association will be marked unavailable after a reasonable amount of time based on RMODE, RMIN and RMAX.

For M2PA, this should be just after M2PA T7 expires (default 1.2 sec).

For example, consider a unihomed M2PA link with RMIN set to 100 msec and RMODE is LINEAR:

```
Time to mark as failed = RMIN * RTIMES 1200 msec
= 100 msec * 12
```

As long as RTIMES = 12, the association will fail at about the same time MTP3 starts changeover procedures (12 is the maximum for RTIMES).

In this case, decrease M2PA T7 slightly using the **`chg-m2pa-tset`** command to guarantee that it will expire before the association is taken down.

For M3UA connections, make this a reasonable amount of time for the network, remembering that multihomed associations could be taken down after only RTIMES/2 retransmits.

Define RTO parameter

Use the ping-result average RTT measurement for calculation of RMIN.

RMIN should be set to whichever is greater of 1.2 * (Avg. RTT) or (Avg. RTT) + 10 ms.

If errors are greater than 1 per 250,000, then investigate to determine if this can be improved in the network.

RMAX can be set to the worst recorded RTT and further tuned after the association has been established and **`assocrtt`** measured.

Measure jitter

Measure jitter by ping samples taken from the network; ideally, a relatively small subset of the samples deviate from the overall Average RTT for the network. The SCTP RMIN parameter value should be adjusted during deployment such that RMIN is approximately equal to 1.2 * Average RTT time in the network. RTT in the network should not exceed 70 ms for SSEDCMs and 120 ms for E5-ENETs.

Refine RTO parameter

After an association is established, the EAGLE 5 ISS **`pass`** command should be used to get the true RTT as experienced by the association.

1. Reset the counters: **`pass:loc=XXXX:cmd="assocrtt -r <assoc name>`**.
2. Wait a reasonable interval (preferably 24 hours) before collecting the measurements: **`pass:loc=XXXX:cmd="assocrtt <assoc name>`**.
3. Perform the **`sctp -g pegs`** or **`sctp -a assocname`** command to determine if any retransmissions have occurred.
4. Use the values reported to further tune RMIN and RMAX. Use the Weighted Average RTT in this case for defining RMIN.

Figure 15. assoc rtt output

```
;
   pass:loc=1105:cmd="assocrtt c7000"

Command Accepted - Processing

   rlghncxa03w 00-01-27 08:10:00 EST EAGLE5 31.6.0
   pass:loc=1105:cmd="assocrtt c7000"
   Command entered at terminal #1

   rlghncxa03w 00-01-27 08:10:00 EST EAGLE5 31.6.0
   PASS: Command sent to card

   rlghncxa03w 00-01-27 08:10:00 EST EAGLE5 31.6.0

   ASSOCRTT: Association round trip time report (in milliseconds)

   Retransmission Configuration
      Retransmission Mode              : LIN
      Minimum RTO : 120
      Maximum RTO : 800

   Traffic Round-Trip Times

      Minimum round-trip time          : 5
      Maximum round-trip time          : 120
      Weighted Average round-trip time : 10
      Last recorded round-trip time    : 10

   Measured Congested Traffic Round-Trip Times

      Minimum round-trip time          : 0
      Maximum round-trip time          : 0
      Weighted Average round-trip time : 0
      Last recorded round-trip time    : 0

   rlghncxa03w 00-01-27 08:10:00 EST EAGLE5 31.6.0
   ASSOCRTT command complete
```

System verification

Once you have finished configuring the EAGLE 5 ISS for SS7-over-IP, use the following steps to verify that it is correct. For details on the commands, see the *EAGLE 5 ISS Command Manual*.

Verify network connectivity

1. Is the IPLIM/IPGWx card IS-NR (In-service Normal)?

   rept-stat-card:mode=full:loc=<IP CARD location>

2. Is the Ethernet port up or down?

   rept-stat-card:mode=full:loc=<IP CARD location>

3. Are there errors on the Ethernet Interfaces? Are there collisions? CRC errors? Alignment errors? Retransmits?

   pass:loc=<IP card location>:cmd=netstat -d 0 <For Ethernet Interface A>

   pass:loc=<IP card location>:cmd=netstat -d 1 <For Ethernet Interface B>

4. Are there checksum errors?

   pass:loc=<IP card location>:cmd="netstat -p sctp

   Change the SCTP checksum if there are errors, **rtrv-sg-opts** will show you what checksum is set at; this must match on both ends.

5. Is the far end reachable? Does ping or traceroute work? Is the RTT acceptable? Is there Packet loss?

   pass:loc=<IP card location>:cmd=ping <far-end IP address>

   pass:loc=<IP card location>:cmd="traceroute <far-end IP Address>"

6. What is the delay or jitter of the network?

   pass:loc=<IP card location>:cmd="assocrtt <association>"

7. What is the far end advertising?

   pass:loc=<IP card location>:cmd="sctp -a association>"

Verify IPLIMx configuration

1. Is there an IPLIMx application in the system?

   rtrv-card

2. Is the IP-LNK table data filled properly? Duplex? 10 or 100 Mbps? Auto=no? IP address Correct? Subnet Mask Correct?

3. Is the IP-CARD table correct? Def router?

4. Is the IP-HOST table data filled? Local hosts specified? Remote hosts specified?

5. Are the Signaling Links built?

   rtrv-card:loc=<IP Card location>

   rtrv-slk:loc=<ip card location>:port=<SS7 port>

6. Is the IPLIMx linkset built?

   rtrv-ls:lsn=<IPLIM Linkset Name>

7. Is the adjacent point code built in the destination and route table?

   rtrv-dstn:dpc=<far end point code>

   rtrv-rte:dpc=<far end point code>

8. Are there associations using the IPLIMx application?

   rtrv-assoc:display=all

9. What is the status of the associations?

   rept-stat-assoc

10. What is the status of the linkset?

    rept-stat-ls:lsn=<IPLIM linkset>

11. What is the status of the SLKs?

    rept-stat-slk:loc=<ip card location>:port=<SS7 port>

12. What is the status of the adjacent point code?

    rept-stat-rte:mode=full:dpc=<adjacent point code

Verify IPGWx configuration

1. Is there an IPGWx application in the system?

   rtrv-card

2. Is the IP-LNK table data filled properly? Duplex? 10 or 100 Mbps? Auto=no? IP address Correct? Subnet Mask Correct?

3. Is the IP-CARD table correct? Def router?

4. Is the IP-HOST table data filled? Local hosts specified? Remote hosts specified?

5. Are the signaling links built?

   rtrv-card:loc=<IP Card location>

   rtrv-slk:loc=<ip card location>:port=<SS7 port>

6. Is the IPGWx linkset built? Does it have sufficient TPS?

   rtrv-ls:lsn=<IPLGW Linkset Name>

7. Is the virtual adjacent point code built in the destination and route table?

   rtrv-dstn:dpc=<far end point code>

   rtrv-rte:dpc=<far end point code>

8. Are the far end point codes built in the destination and route table?

   rtrv-dstn:dpc=<far end point code>

   rtrv-rte:dpc=<far end point code>

9. Are there associations using the IPGWx application?

   rtrv-assoc:display=all

10. Is an Application Server using the associations?

    rtrv-as

11. Is routing built in the APPL-RTKEY table for the far end nodes? SI of 0 is not necessary.

    rtrv-appl-rtkey:display=all

12. What is the status of the associations?

    rept-stat-assoc

13. What is the status of the Application Servers?

    rept-stat-as

    NOTE: Having associations from two different IPGWx linksets in the same Application Server is an unsupported configuration.

14. What is the status of the linkset?

    rept-stat-ls:lsn=<IPGW linkset>

15. What is the status of the adjacent point code?

    rept-stat-rte:mode=full:dpc=<adjacent point code>

16. What is the status of the far end point code?

    rept-stat-rte:mode=full:dpc=<far end point code>

Troubleshooting

If the following steps do not correct your issue, then contact the Tekelec Customer Care Center. See "Tekelec Customer Care Center" on page 3.

General troubleshooting

- Work from the bottom of the protocol stack up: first, IP Network; then the SS7 link or connection; then traffic routing.
- Review provisioning and verify configuration in this order:
  - Card
  - Signaling (SS7) link
  - Linkset
  - IP link or IP network
  - Association or Application Server (IPGWx only)
  - Traffic routing or SS7 route and route key (IPGWx only)

General troubleshooting tools include the following:

- Ethereal – PC-based network analyzer (sniffer) – www.ethereal.com/www.wireshark.com
- **`netstat/sctp`** pass commands to display TCP/IP or SCTP/IP network statistics
- **`ualog/asplog/linkinfo`** pass command to retrieve logs of events in stack and control messages transmitted or received
- **`msucount`** pass command to display traffic counts of MSUs that have been transmitted, received, rerouted, or discarded, and the discard reason

Verify UIMs and UAMs

If there are any UIMs or UAMs occurring related to the SIGTRAN configuration, refer to the Corrective Maintenance section in the *EAGLE 5 ISS Maintenance Manual*.

Is the card configured correctly?

- Card in system? (**`rtrv-card/rept-stat-card`**)
- IP link configured correctly? (**`rtrv-ip-lnk;`** preferred settings are 100/full duplex on card AND switch - no AUTO configure)
- IP routing configured? (**`rtrv-ip-rte/rtrv-ip-card`**)
- IP host table configured? (**`rtrv-ip-host;`** check for local and remote addresses)
- Signalling links (SLKs) and linksets configured correctly? (**`rept-stat-slk/rept-stat-ls`**)

Connection does not become established

- Card up and stable? (**`rept-stat-card`**)
- Association status? (**`rept-stat-assoc`**)
- Network connectivity? (**`netstat -I/rept-stat-card:mode=full`**)
- Errors (collisions, etc.) on the network interface? (**`netstat -d`** 0/1)
- Far end reachable? (**`ping, traceroute`**)
- Near end and far end use same SCTP CRC? (**`netstat -p sctp/rtrv-sg-opts`**)

Connection bounces and is unstable

- Transport stable? (**`netstat –i, netstat –d`**)
- RMIN set too low? (**`ping, assocrtt, rtrv-assoc`**; rule of thumb is above 1.2 * average RTT)

AS/PC in route key does not become available or ACTIVE (IPGWx only)

- Connection in correct AS? (**`rtrv-as`**)
- Routing key provisioned for AS? (**`rtrv-appl-rtkey`**)
- Network appearance/routing context required and matched? (**`rtrv-appl-rtkey, ualog`**)
- AS/ASP activated at far end? (**`aslog, ualog`**)

- SS7 APC/SAPC and associated route exists in the same network (and group code) as the PC? (**rtrv-rte, rtrv-ls**)

IP destination is not informed of SS7 destination status changes; network management is not working correctly (IPGWx only)

- Route key is not provisioned for IPGWx linkset virtual APC, but SS7 route is? (**rtrv-rte, rtrv-appl-rtkey/display-=all**)
- AS connections hosted by cards in different linksets/matesets; is the mateset equivalent to linkset? (**rtrv-as, rtrv-assoc, rtrv-ls**)

Traffic not arriving at IP destination or traffic is lost

- Route to destination's PC entered and available? (**rept-stat-dstn**)
- Traffic being received/discarded on IP card? IPGWx application has numerous discard reasons! (**msucount -l**)

Are connection(s) congesting?

- Is SCTP buffering set correctly for network RTT? (**rtrv-assoc, assocrtt, sctp**)
- Is IPTPS set correctly for IPGWx? (**rept-stat-iptps/rtrv-ls**)
- Is an interface set to half-duplex somewhere in the path to the far end, causing excessive retransmissions? (**rtrv-ip-lnk, sctp**)

Traffic not load-balanced properly

- Source traffic has uneven SLS distribution?
- All cards in linkset or mateset do not host a connection to the IP Application Server (IPGWx only)? (**rtrv-assoc, rtrv-as**)
- IPGWx cards in mateset with no established connections have signaling link deactivated to minimize 'double-hopping' (IPGWx only)? (**rept-stat-card, msucount -l**)

Link level events

- IPLIM pass command - **linkinfo -l**
- IPLIMx linkinfo has other interesting options (**-c/-m**)

- IPGWx pass command - **`ualog/aslog`**
- Both commands have event filtering (link events vs. traffic), so look at options

Association

- IPLIM/IPGWx pass command – **`sctp -a`**

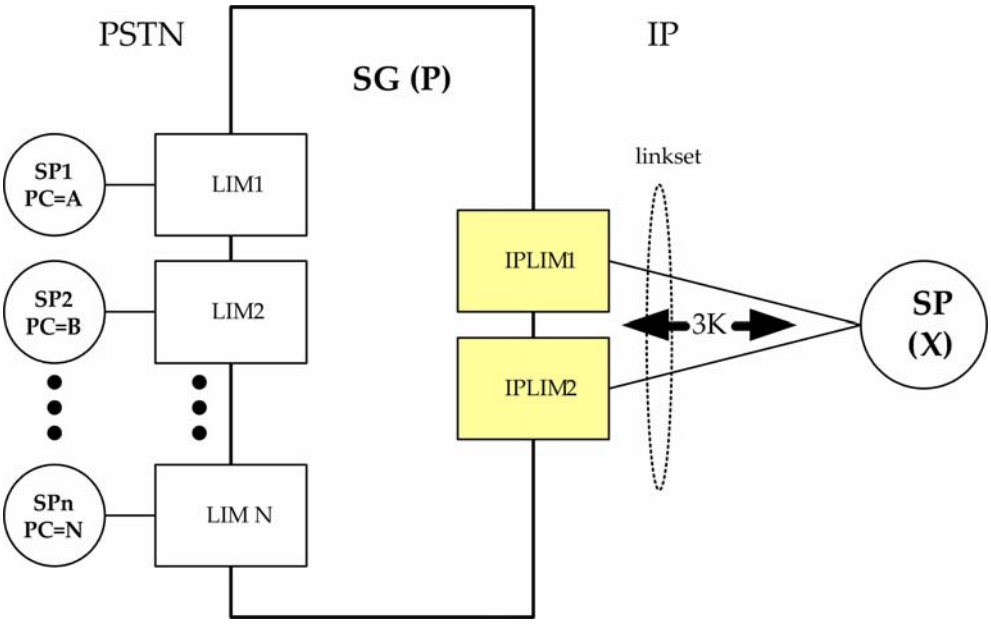
Appendix A. Additional Deployment Scenarios

IPLIM/M2PA deployment scenarios

Simple M2PA A-link configuration (3K TPS)

Figure 16 shows a Signaling Gateway (SG) connected to an IP-based Signaling End Point (SEP) via two M2PA links, one per IPLIMx card. Each M2PA link involves an SCTP association that is multihomed across two Ethernet interfaces. This configuration provides for 2,000 TPS with a single failure.

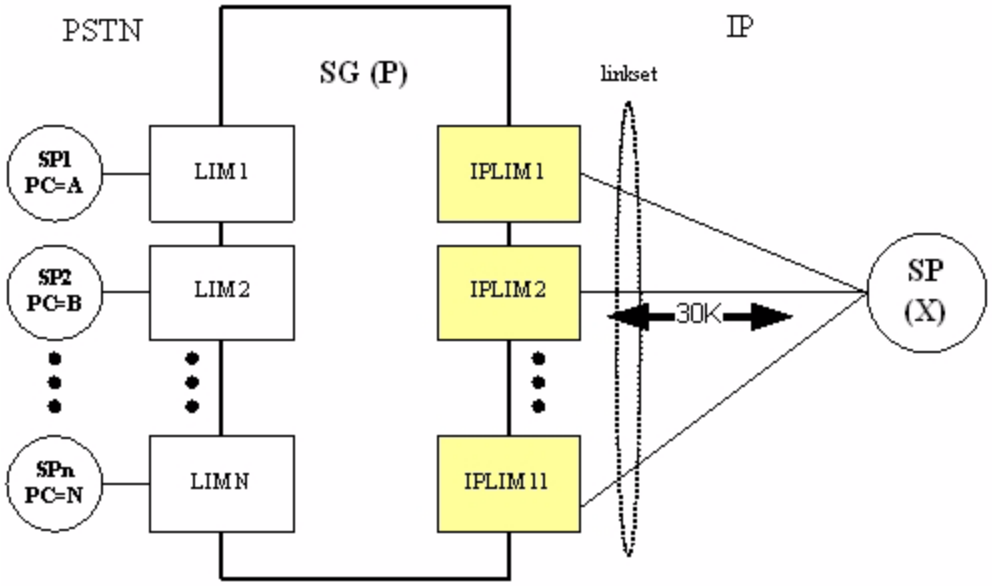
Figure 16. SG connected to IP SEP via two M2PA links



High-throughput M2PA A-link configuration (30,000 TPS)

Figure 17 shows a Signaling Gateway (SG) connected to an IP-based SEP via eleven M2PA links, one per IPLIMx card. Each M2PA link involves an SCTP association that is multihomed across two Ethernet interfaces. This configuration provides for 2,000 TPS with a single failure (N+1 redundancy). Up to 16 M2PA links can reside in a linkset, but the 30K TPS constraint still applies, even if 16 SSEDCMs are used.

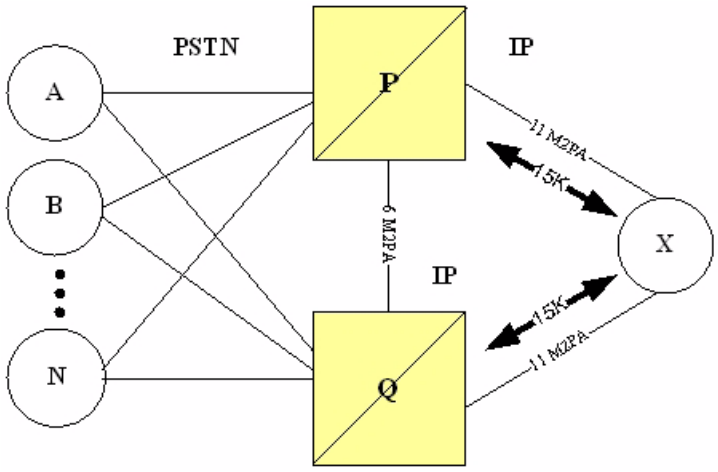
Figure 17. SG connected to IP SEP via eleven M2PA links



High-throughput M2PA C-link configuration (30K TPS)

Figure 18 shows two mated Signaling Gateways connected to an IP-based SEP. The C-links between the Signaling Gateways and the A-links to the IP signaling end point of the M2PA type. Enough C-links are provisioned to handle the case where one Signaling Gateways loses all connectivity to X. In this situation, 15K TPS unidirectional occurs for a short period of time across the C-links.

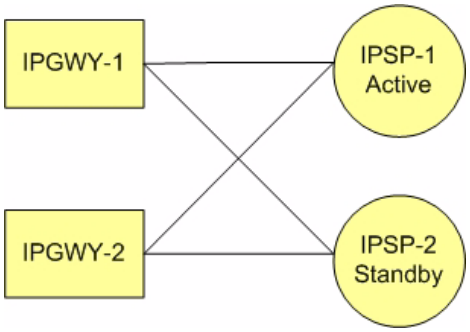
Figure 18. SG connected to IP SEP via eleven M2PA links



IPGW/M3UA deployment scenarios

Active/standby configurations

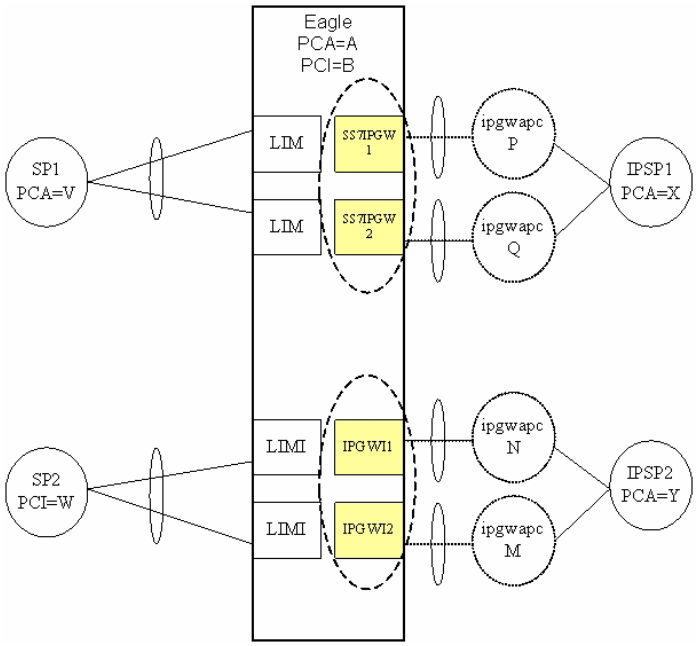
Figure 19. IPGWx active/standby configuration



- Active/standby configurations should be implemented at the IP Signaling Points (IPSPs) rather than at the EAGLE 5 ISS.
- All DCMs assigned to an IPGWx mateset should host connections to nodes comprising an Application Server and should loadshare traffic in the absence of failures. Deployments of active/standby DCMs result in excessive IMT utilization in the absence of failures due to double-hopped outbound traffic.

Two-pair IPGWx

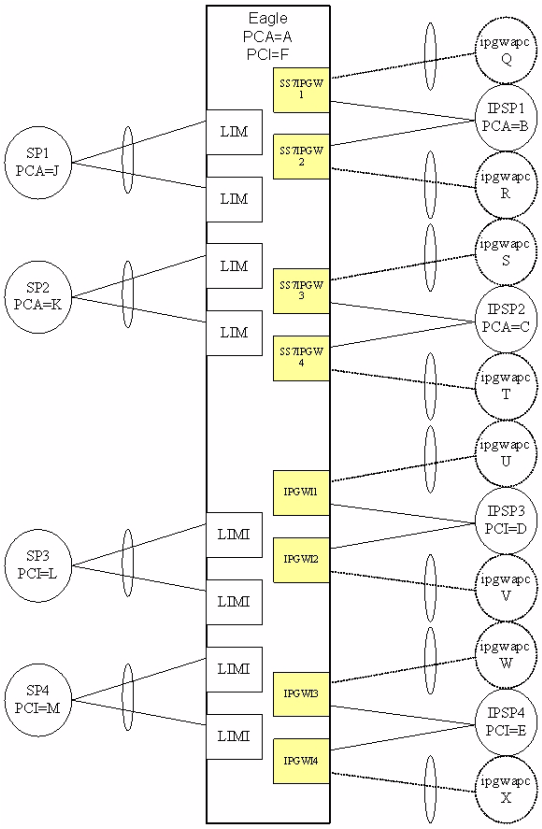
Figure 20. Two-Pair IPGWx for Maximum TPS



- Two IPGWx cards are deployed as a mateset. No more than two cards for each application are allowed.
- Each card has one signaling link, represented by a hatched line. Each IPGWx signaling link is alone in a linkset, represented by an ellipse.
- Each card has a fake adjacent signaling point represented by a hatched circle and having an IPGWx Adjacent Point Code. Each of the IPGWx linksets has an IPGWAPC.
- Two equal cost routes are provisioned for X, thereby combining the two SS7IPGW linksets. Two equal cost routes are provisioned for Y, thereby combining the two IPGWI linksets.
- Each card has one or more IP connections to the IPSP, represented by a solid line. Each IP connection has only an indirect relationship to a signaling link.
- If each card is rated at 2,000 TPS, then the maximum transaction rate to/from a point code is 2,000 TPS (1+1 redundancy), and the total system-wide TPS supported is 4,000 TPS.
- This feature will continue to allow the preceding deployment (two pairs, combined linksets) to be used, and will expand the number of deployment variations supported. It will do this by modifying the definition of a SS7IPGW or IPGWI mateset.

Four IPGWx pairs (two SS7IPW pairs and two IPGWI pairs)

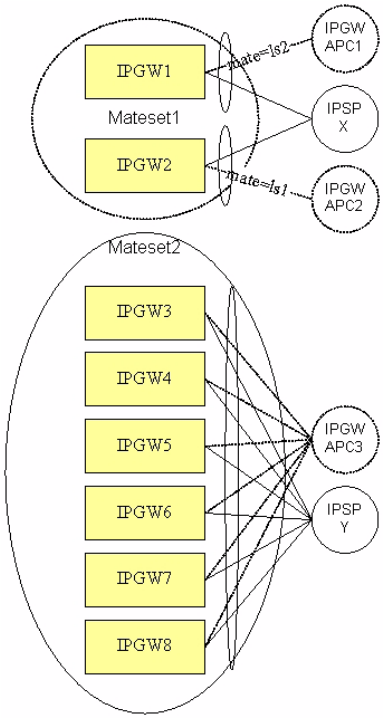
Figure 21. Four IPGWx pairs (two SS7IPW pairs and two IPGWI pairs)



- There are four IPGWx matesets, each comprised of two linksets (a combined linkset).
- Each IPSP is only connected to cards within an IPGWx mateset. No IPSP (or Application Server) crosses IPGWx mateset boundaries.
- This deployment is 1+1 redundancy.
- Another supported variation of this deployment would involve different numbers pairs or linksets, and possibly one linkset per pair.

Eight IPGWx cards, two mates, three linksets

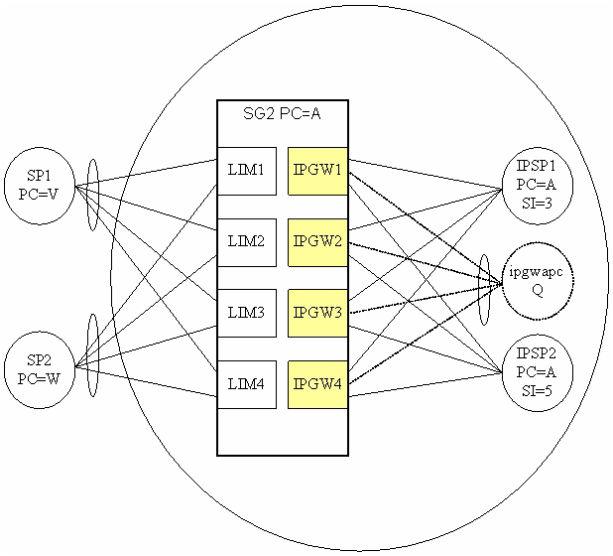
Figure 22. Eight IPGWx cards, two mates, three linksets



- Eight IPGWx cards are present, each having a single signaling link. IPGW1 and IPGW2 have their links assigned to distinct linksets. The remaining IPGWx cards have their links assigned to a common linkset.
- The route-set to PC X involves a combined linkset, i.e. two equal-cost routes.
- Connectivity to the IPSPs does not cross IPGWx mateset boundaries.
- More than two IPSPs can be supported in either IPGWx mateset. The actual limit is based on IP connections and routing keys.
- Other supported variations of this deployment involve different numbers of cards in the Mateset2 or different numbers of IPSPs.

Four IPGWx cards, one linkset for end office

Figure 23. Four IPGWx cards, one linkset for end office

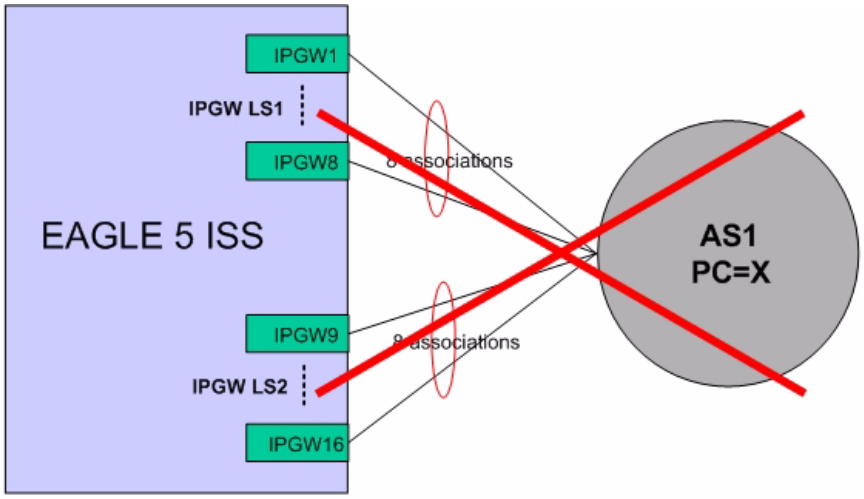


- Four IPGWx cards are present, each having a single signaling link. All of the IPGWx signaling links are assigned to a linkset having an IPGWAPC (virtual point code) of Q.
- Two IP-based signaling points or Application Servers are each connected to the full set of IPGWx cards and are distinguished by user part (SI).
- Because the IPGWx signaling links are part of a single linkset, each card cannot use TFP/TFA to divert traffic to other IPGWx cards.
- The EAGLE 5 ISS is operating in End Office Mode. This means that the IPSPs are IP-attached remote user-parts that share the true and secondary point codes of EAGLE 5 ISS (PC=A). In order to route from the inbound LIMs to the outbound IPGWx cards, an internal point code (IPC) is used.
- Because only one IPC is currently supported, only one IPGWx mateset is supported for End Office mode traffic. There can be other IPGWx matesets, but only one can serve End Office remote applications.
- Other supported variations of this deployment involve different numbers of cards in the mateset or different numbers of IPSPs.

Unsupported Scenarios

Figure 24 shows that the route to IPGWx linksets 1 and 2 are combined. Combined linksets are not supported.

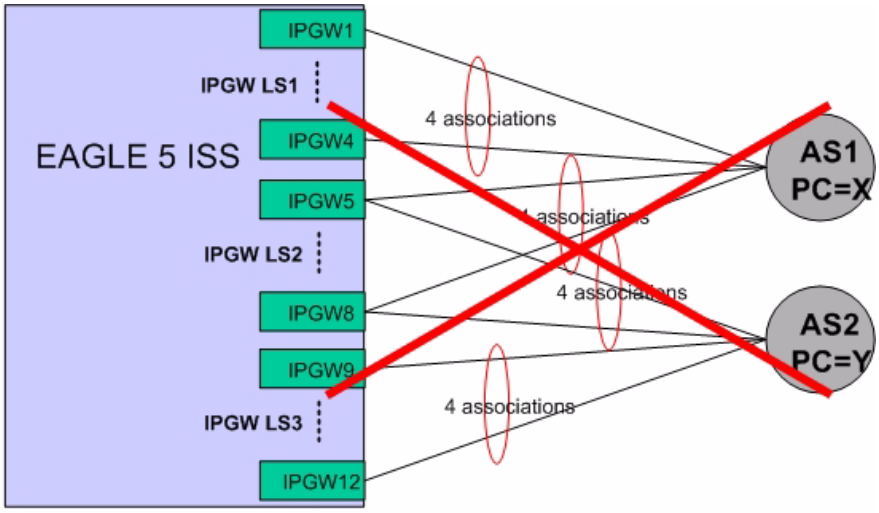
Figure 24. Unsupported deployment scenario: Combined linksets



- EAGLE 5 ISS route to PC=X is a combined linkset for IPGW LS1 and IPGW LS2
- SLS determines which card in either IPGWLS1 or IPGWLS2 is chosen to send traffic to AS1
- Each card in each IPGWLS has 1 association to AS1

Figure 25 shows that the route to IPGWx linksets 1 and 2 are combined for AS1; and linksets 2 and 3 are combined for AS2. Combined linksets are not supported.

Figure 25. Unsupported deployment scenario: Combined linksets



- EAGLE 5 ISS route to AS1 PC=X is combined linkset for IPGW LS1 and IPGW LS2
- EAGLE 5 ISS route to AS2 PC=Y is combined linkset for IPGW LS2 and IPGW LS3

Appendix B. References

Internal references

Internal references are available only to Tekelec personnel. External Customers should contact their Sales Representative for information contained in these documents.

[1] *Sigtran Implementation*, David Prince, April 2007, Tekelec.

[2] *Engineering Rules for Determining IP^7 Application Throughput*, Tekelec, TR005007.

[3] *Engineering Rules for IP Networks for IP^7 Application Deployment*, Tekelec, TR002826.

[4] TK149 V4.1 Student Guide.ppt.

[5] *SCTP RFC 2950 Compliance Matrix*, Tekelec, CM005012.

[6] *M2PA RFC 4165 Compliance Matrix*, Tekelec, CM005086.

[7] *M3UA RFC 4666 Compliance Matrix*, Tekelec, CM005022.

[8] *SUA RFC 3868 Compliance Matrix*, Tekelec, CM005002.

[9] *Increase System-Wide IPGWx TPS*, FD005446.

[10] Site Survey: Message Feeder on T1000 Platform.

[11] *SigTran_Training_24 October 06 for Customers*.ppt, Tekelec.

[12] *TK149-SIGTRAN IPLIM and IPGW Provisioning Student Guide*, Rev. 4.1, Tekelec, 2007.

External references

[13] *Database Administration - IP^7 Secure Gateway Manual* of your current EAGLE 5 ISS documentation set https://support.tekelec.com/index.asp.

[14] IETF RFCs. http://tools.ietf.org/wg/sigtran/

[15] *Site Security Handbook, RFC 2196*.

http://tools.ietf.org/html/rfc2196#section-1.5

[16] BITS GUIDE TO BUSINESS-CRITICAL TELECOMMUNICATIONS SERVICES.

http://www.bitsinfo.org/downloads/Publications%20Page/bitstelecomguide.pdf

[17] Quality of Service Technical White Paper.

http://www.microsoft.com/technet/prodtechnol/windows2000serv/plan/qosover2.mspx

[18] Linux Bandwidth.

http://www.skywayradio.com/tech/linux/bandwidth.html

[19] SS7 over IP Signaling Transport & SCTP.

http://www.iec.org/online/tutorials/ss7_over/index.html

Glossary

Application Server	A logical entity serving a specific routing key. An example of an Application Server is a virtual IP database element handling all requests for an SCCP user. The AS contains a set of one or more unique Application Server Processes, of which one or more is normally actively processing traffic.
Application Server Process	An active or backup process of an Application Server (e.g., part of a distributed signaling node or database element). Examples of ASPs are MGCs, IP SCPs, or IP-based HLRs. An ASP contains an SCTP endpoint and may be configured to process traffic within more than one Application Server.
AS	Application Server
ASP	Application Server Process
Association	An association refers to an SCTP association. The association provides the transport for the delivery of SCCP-User protocol data units and SUA layer peer messages.
Backhaul	The transport of signaling from the point of interface for the associated data stream (i.e., SG function in the MGU) back to the point of call processing (i.e., the MGCU), if this is not local.
Bandwidth	In computer networking, refers to the data rate supported by a network connection or interface; most commonly expressed in terms of bytes per second (bps).
Bundling	An optional multiplexing operation in which more than one user message may be carried in the same SCTP packet. Each user message occupies its own DATA chunk.
CMT	Concurrent Multipath Transfer
Concurrent Multipath Transfer	Concurrent multipath transfer (CMT) uses the Stream Control Transmission Protocol's (SCTP) multihoming feature to distribute data across multiple end-to-end paths in a multihomed SCTP association.

Configuration Dynamic and shorter-term management tasks. These include modifications to parameters. This term is often used interchangeably with provisioning.

Congestion Window An SCTP variable that limits the data, in number of bytes, that a sender can send to a particular destination transport address before receiving an acknowledgement.

Connectivity The complete path between two terminals over which one-way or two-way communications may be provided.

Convergence The synergistic combination of voice (and telephony features), data (and productivity applications), and video onto a single network. These previously separate technologies are now able to share resources and interact with each other, creating new efficiencies.

CWND Congestion Window

Data Feed EAGLE 5 ISS feature for which transmit and receive signaling traffic and L2 events are copied and sent to STC-attached servers for processing.

Destination Point Code The point code of the signaling point to which the MSU is routed. This point code can be adjacent to the EAGLE 5 ISS, but does not have to be.

Double-hopping If the IPGW that received the message does not have an available association to send the message out on, it will re-route the message over the IMT Bus to an IPGW card in the same IPGW linkset that does have an available association (double-hopping).

DPC Destination Point Code

Dynamic Addressing The Source host (e.g., EAGLE 5 ISS) must build a packet with all information needed to deliver it. It is up to the network to figure out how to deliver the packet. Once the packet is built, it is delivered by the network according to its destination address.

Greenfield network A new installation of equipment where none existed before. Contrast with “brownfield,” which is an upgrade to an existing system.

High-Speed IMT Packet Router A card that provides increased system throughput and traffic capacity. HIPR moves EAGLE from an intra-shelf ring topology to an intra-shelf switch topology. HIPR acts as a gateway between the intra-shelf IMT BUS running at 125 Mbps, and the inter-shelf

	operating at 1.0625Gbps. The HIPR card will seat in the same slot as an HMUX card (slots xx09 & xx10 of each shelf).
High-Speed Multiplexer	A card that supports the requirements for up to 1500 links, allowing communication on IMT buses between cards, shelves and frames. HMUX cards interface to 16 serial links, creating a ring from a series of point-to-point links. Each HMUX card provides a bypass multiplexer to maintain the ring's integrity as cards are removed and inserted into an operational shelf.
HIPR	High-Speed IMT Packet Router
HMUX	High-Speed Multiplexer
hop	An intermediate connection in a string of connections linking two network devices. On the Internet, for example, most data packets need to go through several routers before they reach their final destination. Each time the packet is forwarded to the next router, a hop occurs. The more hops, the longer it takes for data to go from source to destination. You can see how many hops it takes to get to another Internet host by using the PING or traceroute utilities.
Host	Addressable endpoint. The computing platform on which the SGP or ASP process is running.
IAS	Integrated Application Solution
IETF	Internet Engineering Task Force
IMF	Integrated Message Feeder
IMS	IP Multimedia Subsystem
Internet Engineering Task Force	IETF Delivering IP multimedia services to end users. It is a part of the vision for evolving mobile networks beyond GSM. In its original formulation (3GPP R5) it represented an approach to delivering Internet Services over GPRS. To ease the integration with the Internet, the IMS as far as possible utilizes IETF (i.e. Internet) protocols such as SIP.
IP connection	An IP connection is an SCTP association. IP[7] applications use SCTP associations as software mechanisms for communication between IP network elements.

IPGWx	IP Gateway Point-to-multipoint MTP-User signaling (e.g. ISUP, TCAP) over IP capability. Typically used for A-link connectivity that requires routing keys. Far End not required to support MTP3. The IPGWx GPL (IPGWI, SS7IPGW) runs on the SSEDCM hardware.
IPGW mateset	An IPGW card linkset configuration with two mutually exclusive settings: • Two IPGW linksets are allowed in a mateset by using the **matelsn** linkset parameter. • Up to 8 IPGW cards can be defined in a single IPGW linkset.
IPLIMx	Point-to-point MTP3 and MTP3-User signaling over IP capability. Typically used for B-C-D links; can be used for A-links. Far End required to support MTP3. The IPLIMx GPL (IPLIMI, IPLIM) runs on the SSEDCM or E5-ENET hardware.
IP Server Process	IPSP
IP Signaling End Point	IP destination supporting SS7 application protocols.
IPSP	IP Server Process
ISDN User Part	Signaling System 7 ISDN User Part
ISEP	IP Signaling End Point
ISUP	Signaling System 7 ISDN User Part
LAN	Local area network
Latency	Delays in processing network data
Local Area Network	A network controlled and configured by a company for local distribution of packets.
MAP	Mobile Application Part
Media Gateway	A Media Gateway terminates voice calls on inter-switch trunks from the public switched telephone network, compresses and packetizes the voice data, and delivers compressed voice packets to the IP network. For voice calls originating in an IP network, the MG performs these functions in reverse order. For ISDN calls from

	the PSTN, Q.931 signaling information is transported from the MG to the Media Gateway Controller for call processing.
Media Gateway Controller	A Media Gateway Controller (MGC) handles the registration and management of resources at the Media Gateways. An MGC may have the ability to authorize resource usage based on local policy. For signaling transport purposes, the MGC serves as a possible termination and origination point for SCN application protocols, such as SS7 ISDN User Part and Q.931/DSS1. T. Because vendors of MGCs often use off-the-shelf computer platforms, an MGC is sometimes called a softswitch.
Message Signaling Unit	The SS7 message that is sent between signaling points in the SS7 network with the necessary information to get the message to its destination and allow the signaling points in the network to set up either a voice or data connection between themselves. The message contains the following information: • The forward and backward sequence numbers assigned to the message that indicate the position of the message in the traffic stream in relation to the other messages. • The length indicator that indicates the number of bytes the message contains. • The type of message and the priority of the message in the signaling information octet of the message. • The routing information for the message, shown in the routing label of the message, with the identification of the node that sent message (originating point code), the identification of the node receiving the message (destination point code), and the signaling link selector which the EAGLE 5 ISS uses to pick the link set and signaling link to use to route the message.
Message Transfer Part	Signaling System 7 Message Transfer Part
MG	A Media Gateway terminates voice calls on inter-switch trunks from the public switched telephone network, compresses and packetizes the voice data, and delivers compressed voice packets to the IP network. For voice calls originating in an IP network, the MG performs these functions in reverse order. For ISDN calls from the PSTN, Q.931 signaling information is transported from the MG to the Media Gateway Controller for call processing.
MGC	Media Gateway Controller

Mobile Application Part — MAP

MSU — Message Signaling Unit

The SS7 message that is sent between signaling points in the SS7 network with the necessary information to get the message to its destination and allow the signaling points in the network to set up either a voice or data connection between themselves. The message contains the following information:

- The forward and backward sequence numbers assigned to the message that indicate the position of the message in the traffic stream in relation to the other messages.
- The length indicator that indicates the number of bytes the message contains.
- The type of message and the priority of the message in the signaling information octet of the message.
- The routing information for the message, shown in the routing label of the message, with the identification of the node that sent message (originating point code), the identification of the node receiving the message (destination point code), and the signaling link selector which the EAGLE 5 ISS uses to pick the link set and signaling link to use to route the message.

MTP — Signaling System 7 Message Transfer Part

Multihoming — Path redundancy to the WAN achieved by each association per card utilizing two IP networks.

Network management — The execution of the set of functions required for controlling, planning, allocating, deploying, coordinating and monitoring the resources of a telecommunications network, including performing functions such as initial network planning, frequency allocation, predetermined traffic routing to support load balancing, cryptographic key distribution authorization, configuration management, fault management, security management, performance management, and accounting management. Note: Network management does not include user-terminal equipment.

Packet — An independent unit of data (usually up to 1518 octets). Every packet includes delivery information in an area of the packet called the header.

In IP networks, this refers to SCTP packets, the unit of data delivery across the interface between SCTP and the connectionless packet network (e.g., IP). An SCTP packet includes the common

	SCTP header, possible SCTP control chunks, and user data encapsulated within SCTP DATA chunks.
Path	The route taken by the SCTP packets sent by one SCTP endpoint to a specific destination transport address of its peer SCTP endpoint. Sending to different destination transport addresses does not necessarily guarantee getting separate paths.
PLMN	Public Land Mobile Network
Primary path	The destination and source address that will be put into a packet outbound to the peer endpoint by default. The definition includes the source address, since an implementation MAY specify both destination and source address to better control the return path taken by reply chunks, and on which interface the packet is transmitted when the data sender is multihomed.
Provisioning	Static and longer-term management tasks. These may include selection of network equipment, replacement of network equipment, interface additions or deletions, link speed modifications, topology changes, and capacity planning. This term is often used interchangeably with configuration.
PSTN	Public Switched Telephone Network
Public Land Mobile Network	PLMN
Public Switched Telephone Network	PSTN
QoS	Quality of Service
Quality of Service	Throughput, timeliness, reliability and perceived quality are the foundations of what is known as QoS. For IP networks, QoS can be defined by four parameters: bandwidth, delay, packet loss and jitter.
Receiver Window	An SCTP variable that a data sender uses to store the most recently calculated receiver window of its peer, in number of bytes. This gives the sender an indication of the space available in the receiver's inbound buffer.

retransmission time-out	Retransmission timeout RTO is the time to wait before declaring the current retransmit attempt a failure. This time is dynamic because it is a moving average of the network
Round Trip Time	The elapsed time for transit of a signal over a closed circuit, or time elapsed for a message to travel to a remote place and back again.
Routing Context	An Application Server Process may be configured to process traffic within more than one Application Server. In this case, the Routing Context parameter is exchanged between the SGP and the ASP (or between two ASPs), identifying the relevant Application Server. From the perspective of an SGP/ASP, the Routing Context uniquely identifies the range of traffic associated with a particular Application Server which the ASP is configured to receive. There is a 1:1 relationship between a Routing Context value and a Routing Key within an AS. Therefore, the Routing Context can be viewed as an index into an AS Table containing the AS Routing Keys.
Routing Key	The Routing Key describes a set of SS7 parameters and/or parameter ranges that uniquely defines the range of signaling traffic configured to be handled by a particular Application Server. An example would be where a Routing Key consists of a particular SS7 SCCP SSN plus an identifier to uniquely mark the network that the SSN belongs to, for which all traffic would be directed to a particular Application Server. Routing Keys are mutually exclusive in the sense that a received SS7 signaling message cannot be directed to more than one Routing Key. Routing Keys can be provisioned by a MIB or registered using SUA's dynamic registration procedures. Routing Keys MUST NOT span multiple network appearances.
RTT	Round Trip Time
RWND	Receiver Window
SCAN	A network that carries traffic within channelized bearers of predefined sizes. Examples include Public Switched Telephone Networks (PSTNs) and Public Land Mobile Networks (PLMNs). Examples of signaling protocols used in SCN include Q.931, SS7 MTP Level 3 and SS7 Application/User parts.
SCCP	SS7 Signaling Connection Control Part
SCN	Switched Circuit Network A network that carries traffic within channelized bearers of predefined sizes. Examples include Public Switched Telephone

	Networks (PSTNs) and Public Land Mobile Networks (PLMNs). Examples of signaling protocols used in SCN include Q.931, SS7 MTP Level 3 and SS7 Application/User parts.
SCP	Service Control Point Provides a central location for data storage, enabling many services and features such as call forwarding, calling party name and number displays, and three-way calling.
SCTP	Stream Control Transmission Protocol
SCTP association	A protocol relationship between SCTP endpoints composed of the two SCTP endpoints and protocol state information, including Verification Tags and the currently active set of Transmission Sequence Numbers (TSNs), etc. An association can be uniquely identified by the transport addresses used by the endpoints in the association. Two SCTP endpoints MUST NOT have more than one SCTP association between them at any given time.
SCTP endpoint	The logical sender/receiver of SCTP packets. On a multihomed host, an SCTP endpoint is represented to its peers as a combination of a set of eligible destination transport addresses to which SCTP packets can be sent, and a set of eligible source transport addresses from which SCTP packets can be received. All transport addresses used by an SCTP endpoint must use the same port number, but can use multiple IP addresses. A transport address used by an SCTP endpoint must not be used by another SCTP endpoint. In other words, a transport address is unique to an SCTP endpoint.
SCTP packet	The unit of data delivery across the interface between SCTP and the connectionless packet network (e.g., IP). An SCTP packet includes the common SCTP header, possible SCTP control chunks, and user data encapsulated within SCTP DATA chunks.
SEP	Signaling End Point A node in an SS7 network that originates or terminates signaling messages. One example is a central office switch.
Service Control Point	Provides a central location for data storage, enabling many services and features such as call forwarding, calling party name and number displays, and three-way calling.
Service Information Field	MTP Service Information Field is the payload field of an SS7 MSU header. The first byte of the SIF is the start of the MTP3 routing label. For MTP3-variant networks, the maximum SIF size is 272

	bytes. For MTP3b-variant networks, the maximum SIF size is 4095 bytes.
Service Switching Point	A service switching point that provides voice-path connectivity from one telephone office to another, and uses the SS7 network for basic call setup, management, and tear down.
SG	Signaling Gateway
Signaling Gateway	A network element that receives/sends SCN native signaling at the edge of the IP network. The SG function may relay, translate or terminate SS7 signaling in an SS7-Internet Gateway. The SG function may also be coresident with the MG function to process SCN signaling associated with line or trunk terminations controlled by the MG (e.g., signaling backhaul). A Signaling Gateway could be modeled as one or more Signaling Gateway Processes, which are located at the border of the SS7 and IP networks. Where an SG contains more than one SGP, the SG is a logical entity and the contained SGPs are assumed to be coordinated into a single management view to the SS7 network and to the supported Application Servers. Signaling End Point A node in an SS7 network that originates or terminates signaling messages. One example is a central office switch.
SGP	Signaling Gateway Process
Short Message Service	Transmission of short text messages to and from a mobile phone, fax machine and/or IP address. Messages must be no longer than 160 alpha-numeric characters and contain no images or graphics.
SLS	Signaling Link Selection
SMS	Short Message Service
SMSC	Short Message Service Center
Short Message Service Center	A network element in the mobile telephone network which delivers SMS messages
SIF	Service Information Field
Signal Transfer Point	A node in an SS7 network that routes signaling messages based on their destination point code in the SS7 network

Signaling End Point	A node in an SS7 network that originates or terminates signaling messages. One example is a central office switch
Signaling Link Selection	Signaling Link Selection (SLS) A Signaling Link Selection value is an integer that identifies the link over which a message is to be transported. The SLS value is included in the Signaling Link Selection field, which is part of the MSU routing label.
Signaling Gateway	A network element that receives/sends SCN native signaling at the edge of the IP network. The SG function may relay, translate or terminate SS7 signaling in an SS7-Internet Gateway. The SG function may also be coresident with the MG function to process SCN signaling associated with line or trunk terminations controlled by the MG (e.g., signaling backhaul). A Signaling Gateway could be modeled as one or more Signaling Gateway Processes, which are located at the border of the SS7 and IP networks. Where an SG contains more than one SGP, the SG is a logical entity and the contained SGPs are assumed to be coordinated into a single management view to the SS7 network and to the supported Application Servers.
Signaling Gateway Process	SGP
Signaling Process	A process instance that uses SUA to communicate with other signaling processes. An ASP, a SGP and an IPSP are all signaling processes.
Signaling Transport	An IP protocol from the IETF that is used to transfer packet-based Public Switched Telephone Network (PSTN) or Public Land Mobile Network (PLMN) signaling over IP networks using a signaling gateway. SIGTRAN uses the Stream Control Transmission Protocol (SCTP) for reliable transport.
SIGTRAN	Signaling Transport The standard protocol used to transport SS7 signals over IP
SMS	Short Message Service Transmission of short text messages to and from a mobile phone, fax machine and/or IP address. Messages must be no longer than 160 alpha-numeric characters and contain no images or graphics.
Softswitch	A media gateway controller on an off-the-shelf computer platform
SS7	Signaling System No. 7

SS7oIP	SS7-over-IP
SS7-over-IP	Traditional SS7 signals from a telephone company switch are transmitted to an SG, which wraps the signals in an IP packet without translation for transmission over IP to either the next SG or to a media gateway controller (MGC), other Service Control Points (SCP), and mobile switching centers (MSCs).
SSP	Service Switching Point
STP	Signal Transfer Point
Stream	In SCTP, refers to a sequence of user messages that are to be delivered to the upper-layer protocol in order with respect to other messages within the same stream. This is in contrast to its usage in TCP, where it refers to a sequence of bytes (in this document a byte is assumed to be eight bits). The stream is a unidirectional logical channel established from one SCTP endpoint to another associated SCTP endpoint. Note: The relationship between stream numbers in opposite directions is strictly a matter of how the applications use them. It is the responsibility of the SCTP user to create and manage these correlations.
Stream Control Transmission Protocol	A new, reliable transport protocol that operates on top of a connectionless packet network such as IP and is functionally equivalent to TCP. It establishes a connection between two endpoints (called an association; in TCP, these are sockets) for transmission of user messages (RFC 2960).
Stream Sequence Number	A 16-bit sequence number used internally by SCTP to assure sequenced delivery of the user messages within a given stream. One stream sequence number is attached to each user message.
SUA	A protocol for the transport of any SCCP-User signaling over IP using the SCTP. The protocol is designed to be modular and symmetric, to allow it to work in diverse architectures
Switched Circuit Network	A network that carries traffic within channelized bearers of predefined sizes. Examples include Public Switched Telephone Networks (PSTNs) and Public Land Mobile Networks (PLMNs). Examples of signaling protocols used in SCN include Q.931, SS7 MTP Level 3 and SS7 Application/User parts.
Switched Circuit Network	A network that carries traffic within channelized bearers of pre-defined sizes. Examples include Public Switched Telephone

	Networks (PSTNs) and Public Land Mobile Networks (PLMNs). Examples of signaling protocols used in SCN include Q.931, SS7 MTP Level 3 and SS7 Application/User parts.
TCAP	Signaling System 7 Transaction Capabilities Part
TDM	Terminal Disk Module
Terminal Disk Module	A technology that transmits multiple signals simultaneously over a single transmission path
	Transactions per second; or transaction units per second
TFC	Transfer Controlled
TFA	Transfer Allowed
TFP	Transfer Prohibited
TPS	A method of measuring how quickly a network can transmit and receive data. Capacities listed with "TPS" units involve the maximum of the receive rate and the transmit rate, and the worst-case assumption is that the transmit and receive rates are the same.
	Under the TU model, transaction units per second are calculated with the total transaction unit value and the advertised card capacity.
Transaction	A sequence of information exchange and related work (such as database updating) that is treated as a unit for the purposes of satisfying a request and for ensuring database integrity. For a transaction to be completed and database changes to made permanent, a transaction has to be completed in its entirety. In IP Signaling, a transaction is an MSU sent and an MSU received with a certain feature set applied to the processing of the MSUs.
Transaction unit	Indicates the relative cost of an IP signaling transaction. Some transactions are more expensive than others in terms of IP signaling card capacity. The base transaction unit is 1.0. A transaction that is less expensive than the base has a transaction unit less than 1.0, and one that is more expensive has a transaction unit greater than 1.0.

Transaction units per Second	TPS A method of measuring how quickly a network can transmit and receive data. Capacities listed with "TPS" units involve the maximum of the receive rate and the transmit rate, and the worst-case assumption is that the transmit and receive rates are the same.
Transport address	An address that serves as a source or destination for the unreliable packet transport service used by SCTP. In IP networks, a transport address is defined by the combination of an IP address and an SCTP port number. Only one SCTP port may be defined for each endpoint, but each SCTP endpoint may have multiple IP addresses.
UAM	Unsolicited Alarm Message
UIM	Unsolicited Information Message
Unsolicited Alarm Message	UAM
Unsolicited Information Message	UIM
Value-added services	An enhancement added to a product or service by a company before the product is offered to customers. VAS Value-added service
Voice over Internet Protocol	VoIP Voice communications transmitted over the Internet.
VoIP	Voice over Internet Protocol
WAN	Wide Area Network
Wide Area Network	A network controlled and configured by a common carrier service for long distance delivery of packets TDMA
TDM	Time Division Multiplexing