Oracle® Communications

EAGLE SIGTRAN User's Guide

Release 47.1
F88477-01
October 2023

Oracle Communications EAGLE SIGTRAN User's Guide, Release 47.1

F88477-01

Contents

4 Transition Planning

5 Dimensioning

6 Implementation

7 Troubleshooting

A Additional Deployment Scenarios

My Oracle Support (MOS)

My Oracle Support (MOS) is your initial point of contact for any of the following requirements:

- **Product Support**:
  The generic product related information and resolution of product related queries.
- **Critical Situations**
  A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:
  - A total system failure that results in loss of all transaction processing capability
  - Significant reduction in system capacity or traffic handling capability
  - Loss of the system's ability to perform automatic system reconfiguration
  - Inability to restart a processor or the system
  - Corruption of system databases that requires service affecting corrective actions
  - Loss of access for maintenance or recovery operations
  - Loss of the system ability to provide any required critical or major trouble notification

  Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.
- **Training Need**
  Oracle University offers training for service providers and enterprises.

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support can assist you with My Oracle Support registration.

Call the Customer Access Support main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

- For Technical issues such as creating a new Service Request (SR), select **1**.
- For Non-technical issues such as registration or assistance with My Oracle Support, select **2**.
- For Hardware, Networking and Solaris Operating System Support, select **3**.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Acronyms

The following table provides information about the acronyms and the terminology used in the document:

Table Acronyms

Acronym	Description
AGW	Application Gateway
ANSI	American National Standards Institute
ATGW	Access Transfer Gateway
ATM	Asynchronous Transfer Mode
BITS	Building Integrated Timing System
BITS	Bits per Second or Bytes per Second
CAMEL	Customized Applications for Mobile networks Enhanced Logic
CCS7	Common Channel Signaling System
CDMA	Code Division Multiple Access
CGPA	Calling Party Address
CIC	Circuit Identiification Code
CLASS	Custom Local Area Signaling Service or Custom Local Area Subscribing Service
CWMIN	Congestion Window Minimum
DPC	Destination Point Code
E5-ENET	EPM-based Ethernet Card
FISU	Fill In Signal Unit
FSU	Final Signal Unit
HLR	Home Locator Register
IETF	Internet Engineering Task Force
IMF	Internet Message Feeder
IMT	Inter-Module-Transport
IP	Intelligent Peripheral or Internet Protocol
ISUP	ISDN User Part
ITU	International Telecommunications Union
LSSU	Link Status Signaling Unit
M2PA	MTP2 User Peer-to-Peer Adaptation
M3UA	MTP3 User Adaptation
MGC	Media Gateway Controller
MSC	Mobile Switching Center
MSU	Message Signal Units
MTP	Message Transfer Part
MTP3	Message Transfer Part, Level 3
NGN	Next Generation Network
NI	Network Indicator
OPC	Origination Point Code

Table (Cont.) Acronyms

Acronym	Description
PIC	Performance Intelligence Center
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RFC	Request For Comment
RTT	Round Trip Time
SCP	Service Control Point
SCCP	Signaling Connection Control Part
SCTP	Stream Control Transmission Protocol
SEP	Signaling End Point
SG	Signaling Gateway
SI	Service Indicator
SIF	Signaling Information Field
SIGTRAN	Signaling Transport
SLIC	Service and Link Interface Card
SLS	Signaling Link Selection
SMSC	Short Message Service Center
SSN	SS7 Subsystem Number
SSoIP	SS7-over-IP
SSP	Service Switching Point
STP	Signal Transfer Point
TALI	Transport Adaption Layer Interface
TCP/IP	Transmission Control Protocol/Internet Protocol
TDM	Time Division Multiplexed
TPS	Transaction Units per Second
TU	Transaction Unit

What's New in This Guide

This section introduces the documentation updates for Release 47.1 in Oracle Communications EAGLE.

Release 47.1 - F88477-01, October 2023

There are no updates in the document for this release.

1
Introduction

This chapter provides a brief description of Oracle Communication's SS7-over-IP using SIGTRAN feature of the EAGLE. It also includes the scope, audience, and organization of this guide; how to find related publications; and how to contact Oracle for assistance.

1.1 Overview

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. Oracle 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.

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 Sales Representative to discuss your specific needs.

1.2 Scope and Audience

This document is written for departments that are affected by the development, sale, or service of SIGTRAN-related products, as well as Oracle customers that require an overview of SS7-over-IP networks, SIGTRAN, and other products that are part of the solution.

1.3 References

For more information, refer to the following documents:

1. *Database Administration - IP7 User's Guide*
2. *IETF RFCs* http://tools.ietf.org/wg/sigtran/
3. *Site Security Handbook, RFC 2196* http://tools.ietf.org/html/rfc2196#section-1.5
4. *BITS GUIDE TO BUSINESS-CRITICAL TELECOMMUNICATIONS SERVICES* http://www.bitsinfo.org/downloads/Publications%20Page/bitstelecomguide.pdf
5. *Quality of Service Technical White Paper* http://www.microsoft.com/technet/prodtechnol/windows2000serv/plan/qosover2.mspx

2

SS7-over-IP Networks

This chapter 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. It takes the reader from the current TDM limitations to the role of SIGTRAN to the reasoning of why and when to transition to an SS7-over-IP network.

2.1 SS7-over-IP Networks Overview

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

The SS7-over-IP signaling primarily addresses the transport aspect of SS7. The 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 the SS7-over-IP networks, the advantages of transitioning to this network, and when it is time to consider transitioning.

2.2 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 use high-speed T1 (1.5 Mbps) or E1 (2.048 Mbps) lines. SS7 uses centralized databases and services, achieves reliable connections through network management. 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 is 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.

Note:

If an E5-ENET-B card running the IPSG application is used and the E5-ENET-B IPSG High Throughput feature is turned on, then the optimal SS7 message size is 120 octets or less. See Table 5-5 for optimal configurations.

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.

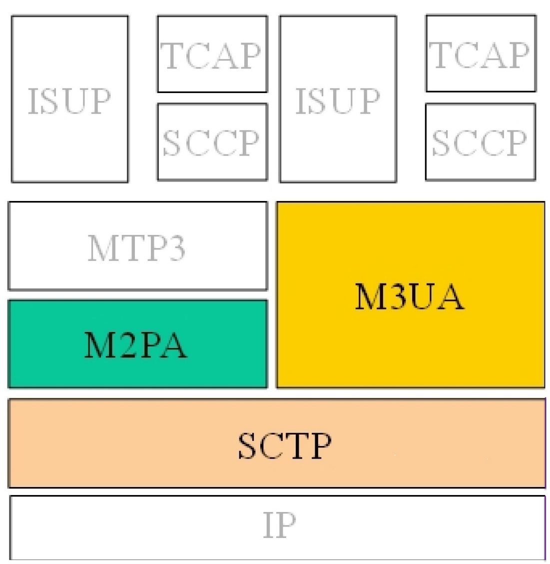
2.3 Role of SIGTRAN

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 Oracle Communications includes several IETF protocols. Figure 2-1 illustrates their location in the protocol stack:

- **MTP2 User Peer-to-Peer Adaptation Layer (M2PA)** protocol; RFC 4165
- **MTP3 User Adaptation Layer (M3UA)** protocol; RFC 4666
- **Stream Control Transmission Protocol (SCTP)**protocol; RFC 4960

Figure 2-1 SIGTRAN Protocols Used by Oracle Communications



2.3.1 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.

Deviations

The following sections summarize the most important deviations from the IETF RFCs that Oracle has made. Refer to the protocol compliance matrices for details. 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. These issues include:

- Synchronization between data streams
- Synchronization from control stream to data streams
- Load-sharing implementation based on Signaling Link Selection (SLS) across streams, either within a connection or across all of the connections in an **Application Server** Since the underlying SS7 network is connectionless, a stringent requirement for mis-sequenced 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 supporting a maximum of two streams: one control stream and one data stream.

SCTP Timer

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

The default mode for the retransmission timer (RMODE) is linear, whereas the RFC-recommended timer setting is exponential. Oracle 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.

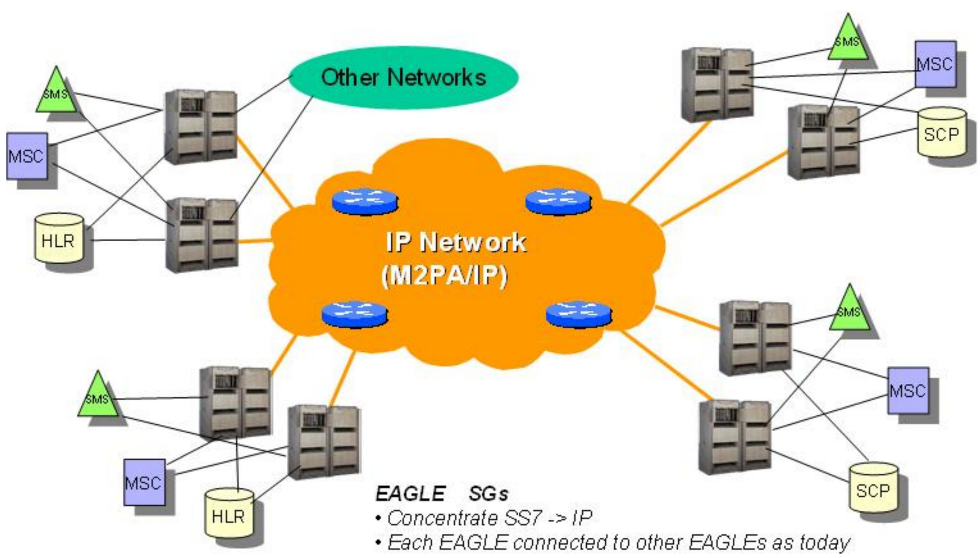
2.3.2 M2PA (MTP2 User Peer-to-Peer Adaptation Layer) Protocol

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 Location Registers and other endpoints. M2PA is a direct replacement for channelized TDM circuits because it provides specific controls for assurance of in-sequence delivery of messages. As such, M2PA is used 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.

Oracle implemented the M2PA protocol through its IPSG application. For more information on the IPSG application, see IPSG application.

Figure 2-2 M2PA Network



2.3.3 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. Oracle offers one type topology for M3UA: IPSG using IPSG-M3UA links.

> **Note:**
>
> A-links for nodes requiring in-sequence delivery of messages should be configured on the IPSG card using M2PA; M3UA does not have sequence numbers to support lossless changeover/changeback.

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 a 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 is implemented using IPSG, supporting routing keys in the form of SS7 Routes referencing IPSG M3UA linksets rather than as distinct 'routing key' managed elements. Instead, it performs similarly to the M2PA protocol. Each M3UA association is viewed as a link by the core EAGLE, and each IPSG card can have up to 128 associations/links per card. MTP Origin-Based Routing cannot be used with adjacent point codes.

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.

2.4 SS7-over-IP signaling transport

SIGTRAN protocols connect IP-based or IP-enabled **Media Gateway Controllers (MGCs)**, **Signaling Gateway (SG)**, switches, databases and other Next Generation signaling applications with traditional circuit-switched signaling architecture.

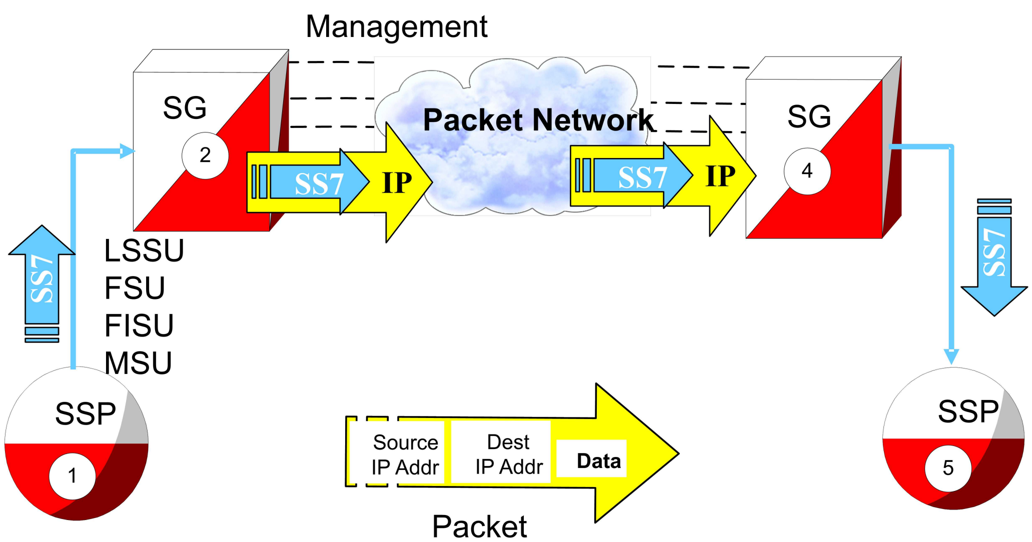
In SS7-over-IP networks, traditional SS7 signals from a telephone company switch are transmitted to a Signaling Gateway, which wraps the signals in an IP packet for transmission over IP to either the next Signaling Gateway or to a MGC, other Service Control Points, or Mobile Switching Centers (MSCs).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

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 can perform the functions of a Signal Transfer Point in addition to those of a Signaling Gateway.

2.4.1 From SS7 Message to IP Packet

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

Figure 2-3 Transmitting an SS7 Message using IP

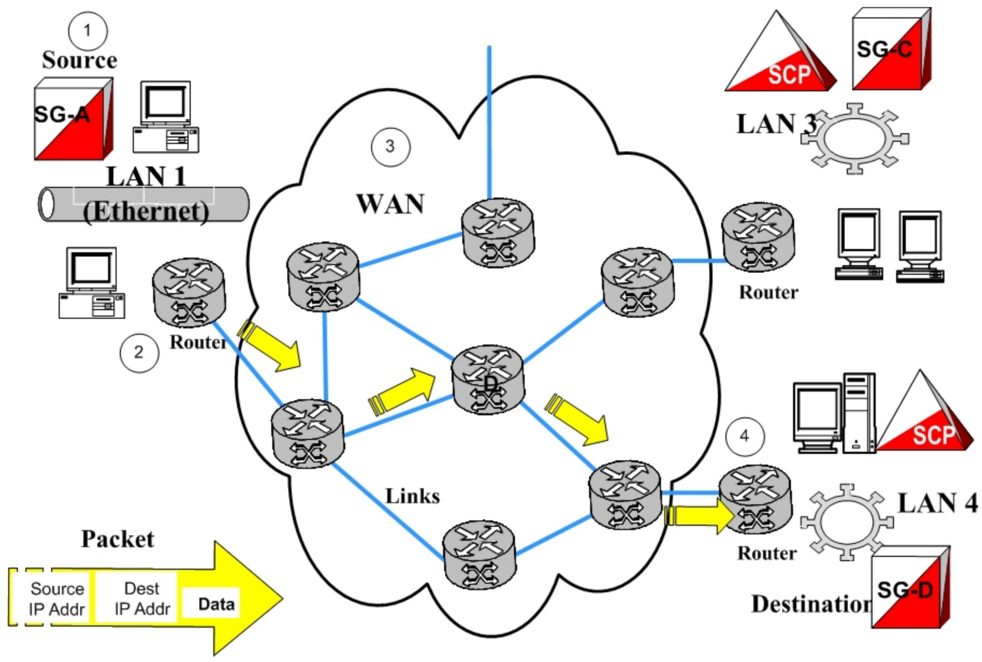


1. A signaling point issues an SS7 message, unaware that there is IP signaling in the network. The message contains Link Status Signaling Units (LSSU), Fill In Signal Units (FISU), Final Signal Units (FSU), and Message Signal Units (MSUs).
2. The Signaling Gateway receives the SS7 packet and encapsulates all necessary SS7 information into the data section of the IP packet. The packet includes the data, source and destination IP addresses.
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.

2.4.2 Communication inside the Wide Area Network (WAN)

The following figure and description show the routing inside the Wide Area Network (WAN).

Figure 2-4 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.

2.5 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 improved 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.

2.5.1 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 multi-vendor 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.

2.5.2 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 EAGLE with its gateway functions, operators can have a **Short Message Service Center** communicate directly to **Home Location Registers (HLR)** and **Mobile Switching Centers (MSCs)** 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; re-dimensioning 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.

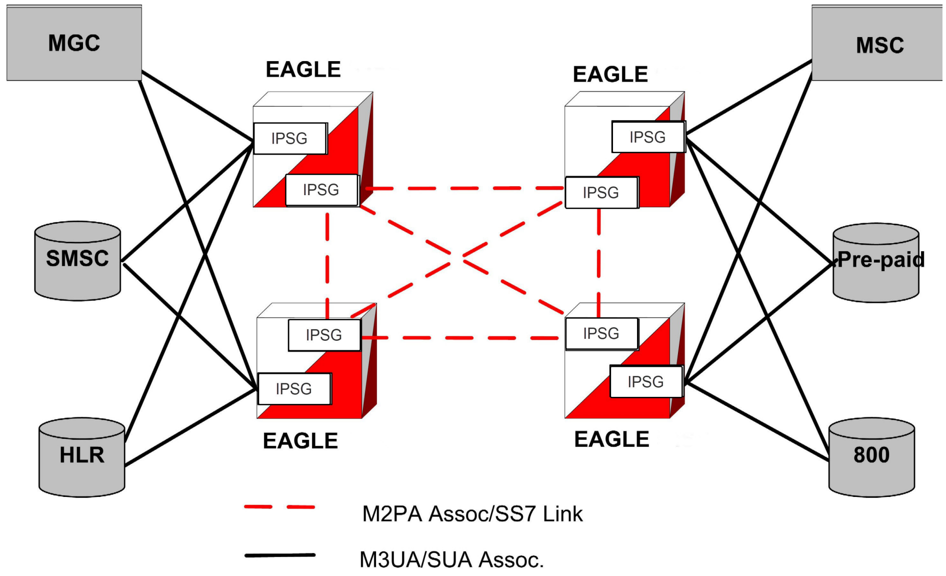
2.5.3 Integration

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 2-5 shows the diversity of solutions that are possible using SIGTRAN protocols. For example, M3UA 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 2-5 Typical EAGLE SS7-over-IP Deployment



2.6 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.

2.6.1 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 a lower 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 EAGLE, 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 Oracle Professional Services can provide recommendations based on their experiences with previous SIGTRAN deployments.

2.6.2 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 of traditional services or new features

2.6.3 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 equipment and connection 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

2.7 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 lossy 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.

3
Oracle Communications Solutions

This chapter describes how Oracle products are a part of the SS7-over-IP solution - how the EAGLE functions as a gateway to internet networks; and describes the PIC, which provides several network management and performance tools including IP traffic monitoring through the IMF.

3.1 Overview

Oracle 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, 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. Oracle'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, the IP signaling leader and the first to recognize the value of IP Signaling by developing the TALI protocol (RFC 3094) in 1998, was first to market with an IP Signaling solution in 2000, and has years of IP signaling deployment experience. Tekelec was acquired by Oracle in 2013.

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

3.2 EAGLE

The EAGLE is a robust SS7-over-IP solution that delivers centralized signaling routing and bridges legacy circuit-switched and packet networks. EAGLE 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 can handle signaling requirements of the most complex networks, delivering dynamic bandwidth sharing to support increases in signaling traffic without adding new nodes. The same platform delivers full Signal Transfer Point (STP) capabilities and a complete portfolio of integrated applications.

Using the EAGLE 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 provides ease of database management for the SS7-over-IP architecture. Key benefits of using the SS7-over-IP solution include:

- **Decreased network congestion:** Oracle's packet-switched technology delivers dynamic bandwidth sharing to enable carriers to effectively expand their signaling network 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 Oracle solutions, carriers can streamline their networks while reducing administration, without service interruption during installation.
- **Migration to next-generation architecture:** The EAGLE 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. Oracle's open, multi-protocol architecture (SS7, SCTP, M2PA, and M3UA) provides carriers the capability to grow and migrate their network with the independence to choose best-in-class products.

IPSG application

The EAGLE implements SIGTRAN with the IPSG application:

The IPSG represents a unified application for both ANSI and ITU links on a single association.

The IPSG application uses SCTP with the M2PA protocol to support A-, B-, C-, D-links. It also uses SCTP with the M3UA protocol to support such user part 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. IPSG supports routing keys in the form of SS7 Routes referencing IPSG M3UA linksets. IPSG is installed on an E5-ENET-B or SLIC card. IPSG can be implemented with just one card and expanded to 250 cards per system, as long as it does not exceed System TPS limitations (500K, 750K, or 1M).

The IPSG feature provides conforming M3UA functionality that behaves more like other LIMs, providing the following benefits:

- The IPSG-application M3UA operational model equates Linkset (LS) and Application Server (AS). It equates a Signaling Link (SLK) with an AS-ASP (Routing Context + Association) instance. This allows each AS-ASP instance to be administered as a signaling link.
- A new signaling link type, IPSG-M3UA, can be assigned to linksets having up to 16 signaling links.
- Each IPSG card will host up to 128 signaling links.
- Each IPSG card will host up to 128 SCTP associations. A maximum of 16 IPSG-M3UA signaling links can be assigned to a single association.
- The adjacent point code (APC) of the IPSG-M3UA linkset is the point code assigned to the Application Server serviced by the linkset. The IPSG-M3UA linkset does not require a fake adjacent point code.
- Each IPSG-M3UA signaling link can have a single IP connection, unlike the former IPGWx signaling link which can have up to 50 IP connections.
- The state of the IPSG-M3UA signaling link will be based on the states of the assigned IP connection and AS-ASP instance. If the IP connection is unavailable for traffic, then the IPSG-M3UA signaling link will also be unavailable. If the AS-ASP instance is not available, then the IPSG-M3UA signaling link will also be unavailable.

- Multiple IPSG-M3UA signaling links (up to 16) can share one IP connection, as long as all of the IPSG-M3UA signaling links and corresponding IP connection are hosted by the same card. This enables multiple SS7 variant support across a single IP connection.

3.3 Performance Intelligence Center (PIC)

The PIC platform, integrated with EAGLE, 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, PIC sorts through the data to create comprehensive dashboards and reports for all departments within the service-provider company. PIC includes a comprehensive array of performance- and revenue-management capabilities that provide reliable real-time or historical information based on network traffic.

The PIC is based on industry-standard network protocols, and provides one platform for all network technologies including **Voice over Internet Protocol (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.

For more information on PIC, contact your Sales Representative.

3.4 Integrated Message Feeder (IMF)

The IMF is an integrated site collector that provides integrated data acquisition in conjunction with the EAGLE. IMF connects to the EAGLE via Ethernet and monitors signaling links on the EAGLE 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 IMF, contact your Oracle Sales Representative.

4
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 frame, 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 chapter provides guidelines on how to approach such a transition and points to the detailed information provided in this document.

4.1 Transition guidelines

The following steps should be followed in making the transition to a SS7-over-IP network.

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

4.1.1 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 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
  - "Dedicated network versus converged IP network"
  - "Replacement versus expansion"
  - Diversity (see Type of Network Change)
- Security

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)
- "M2PA (MTP2 User Peer-to-Peer Adaptation Layer) protocol"
- M3UA (MTP Level 3 User Adaptation Layer) Protocol

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

- Protocol deviations
  - SCTP Timers
  - SCTP (Stream Control Transmission Protocol)
  - Multihoming
  - M3UA (MTP Level 3 User Adaptation Layer) Protocol
- Overview of products
- "Scalability"
- IPSG Deployment Scenario
- "Signaling Link Selection (SLS) routing"

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
  - "Unihoming versus multihoming"
  - "Mated Signal Transfer Point redundancy"
  - "Signaling Link Selection (SLS) routing"
- Additional Deployment Scenarios
- "Scalability"

4.1.2 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, 10/100/1000 Speed, MAC Layer) will also be needed for implementation. Refer to *Database Administration - IP7 User's Guide* manual of the current EAGLE 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 node and each Signaling End Point (SEP), a spreadsheet per EAGLE 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 the table along the top row.

Table 4-1 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 node connection to which this data refer
Total # SGWs	Total number of STPs to which this node connects
SIGTRAN Protocol	M2PA, M3UA
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
% 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 EAGLEs in worst-case conditions
Max Assoc	The maximum number of associations that this node supports to this EAGLE

See also:

- Configure the IPSG Application
- *Database Administration - IP7 User's Guide* of your current EAGLE documentation

4.1.3 Analyze data

Follow the guidelines in Engineering Rules for Determining IP7 Application Throughput (TR005007) to determine expected throughput from the IPSG application, and for details on other criteria to achieve these advertised capacities.

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

- “SIGTRAN engineering guidelines”
- “Calculate the number of cards required”

To determine association configuration parameters, see:

- “Define RTO parameter”
- “Configure Congestion Window Minimum (CWMIN) parameter”

4.1.4 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).

4.1.5 Implement and test

- "Configuration"
- “Retransmission concept"
- “Define RTIMES association retransmits”
- “Define RTO parameter”
- “System verification”
- “Troubleshooting”

4.1.6 Refine timers and parameters

Refine Timers and Parameters

5 Dimensioning

This chapter describes dimensioning issues and calculations required to maximize the efficiency of the new network, addressing scalability, redundancy schemes, throughput calculations for both normal and failover mode, LAN/WAN considerations, and retransmission concepts.

5.1 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.

5.1.1 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, Oracle 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) and Calculate the Number of Cards Required.

5.2 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 IPSG application.

5.2.1 Link Equivalency

Table 5-1 and Table 5-2 show Link Equivalency for IPSG on E5-ENET-B.

Table 5-3 and Table 5-4 show Link Equivalency for IPSG on SLIC.

Table 5-1 EAGLE Link Equivalency for IPSG on E5-ENET-B (E5-ENET-B when IPSG High Throughput Feature OFF)

ATM <-> Low Speed Link				M2PA <-> ATM <-> Low Speed Link				M3UA <-> ATM <-> Low Speed Link			
Avg. MSU Size (MTP 2 + MTP 3)	EAGLE ATM Link Msu/ Sec	56K Links ATM Equivalent	64K Links ATM Equivalent	EAGLE M2PA Msu/ Sec	ATM Link Equivalent	56K Links IP Equivalent	64K Links IP Equivalent	EAGLE M3UA Msu/ Sec	ATM Links Equivalent	56K Links IP Equivalent	64K Links IP Equivalent
20	2000	6	5	6500	3	19	16	6500	3	19	16
30	2000	9	8	6500	3	28	24	6500	3	28	24
40	1800	11	9	6500	4	37	33	6500	4	37	33
50	1800	13	12	6500	4	46	41	6500	4	46	41
60	1800	16	14	6500	4	56	49	6500	4	56	49
70	1800	18	16	6500	4	65	57	6500	4	65	57
80	1800	21	18	6500	4	74	65	6500	4	74	65
90	1200	16	14	6500	5	83	73	6500	5	83	73
100	1200	18	15	6500	5	92	81	6500	5	92	81
110	1200	19	17	6500	5	102	89	6500	5	102	89
120	1200	21	18	6500	5	112	97	6500	5	112	97
130	1200	23	20	6500	5	120	105	6500	5	120	105
140	900	18	16	6500	7	130	114	6500	7	130	114
150	900	20	17	6500	7	138	122	6500	7	138	122
160	900	21	18	6500	7	148	130	6500	7	148	130
170	900	22	20	6500	7	159	138	6500	7	159	139
180	900	24	21	6500	7	167	148	6500	7	167	148
190	720	20	18	6500	9	176	155	6500	9	176	155
200	720	21	18	6500	9	186	163	6500	9	186	163
210	720	22	19	6500	9	197	171	6500	9	197	171
220	720	23	20	6500	9	203	181	6500	9	203	181
230	720	24	21	6500	9	217	186	6500	9	217	186
240	600	21	18	6500	11	224	197	6500	11	224	197
250	600	22	19	6500	11	232	203	6500	11	232	203
260	600	23	20	6500	11	241	210	6500	11	241	210
270	600	24	21	6500	11	250	217	6500	11	250	217

Table 5-2 EAGLE Link Equivalency for IPSG on E5-ENET-B (E5-ENET-B IPSG High Throughput Feature ON)

ATM <-> Low Speed Link				M2PA <-> ATM <-> Low Speed Link				M3UA <-> ATM <-> Low Speed Link			
Avg. MSU Size (MTP 2 + MTP 3)	**EAGLE ATM Link Msu/Sec**	**56K Links ATM Equivalent**	**64K Links ATM Equivalent**	**EAGLE M2PA Msu/Sec**	**ATM Link Equivalent**	**56K Links IP Equivalent**	**64K Links IP Equivalent**	**EAGLE M3UA Msu/Sec**	**ATM Links Equivalent**	**56K Links IP Equivalent**	**64K Links IP Equivalent**
20	2000	6	5	9500	5	27	24	9048	4	25	22
30	2000	9	8	9500	5	41	36	9048	4	38	33
40	1800	11	9	9500	5	54	48	9048	4	50	44
50	1800	13	12	9500	5	68	59	9048	4	63	55
60	1800	16	14	9500	5	81	71	9048	4	76	66
70	1800	18	16	9500	5	95	83	9048	4	88	77
80	1800	21	18	9500	5	108	95	9048	4	101	88
90	1200	16	14	9500	8	122	107	9048	7	114	99
100	1200	18	15	9500	8	136	118	9048	7	126	110
110	1200	19	17	9500	8	148	132	9048	7	139	121
120	1200	21	18	9500	8	164	142	9048	7	151	132
130	1200	23	20	9387	8	176	153	8870	7	161	141
140	900	18	16	9277	11	190	167	8700	10	170	149
150	900	20	17	9170	11	202	179	8535	9	179	156
160	900	21	18	9065	11	216	190	8377	9	187	164
170	900	22	20	8962	11	232	202	8225	9	195	171
180	900	24	21	8862	11	244	216	8078	9	203	177
190	720	20	18	8764	13	257	226	7936	11	210	184
200	720	21	18	8668	13	271	238	7800	11	218	190
210	720	22	19	8574	13	288	250	7668	11	225	196
220	720	23	20	8482	13	297	264	7540	10	231	202
230	720	24	21	8392	13	317	271	7416	10	238	208
240	600	21	18	8304	16	328	288	7296	12	244	214
250	600	22	19	8218	16	339	297	7180	12	250	219
260	600	23	20	8134	16	352	306	7068	12	256	224
270	600	24	21	8051	16	365	317	6960	12	262	229

Table 5-3 EAGLE Link Equivalency for IPSG on SLIC for EAGLE 46.5

Avg. MSU Size (MTP2 + MTP3)	EAGLE ATM Link MSU/Sec	EAGLE M2PA/ M3UA MSU/Sec	ATM Link Equivalent	56K Link Equivalent	64K Link Equivalent
20	2000	10000	5	29	25
30	2000	10000	5	43	38
40	1800	10000	6	58	50
50	1800	10000	6	72	63

Table 5-3 (Cont.) EAGLE Link Equivalency for IPSG on SLIC for EAGLE 46.5

Avg. MSU Size (MTP2 + MTP3)	EAGLE ATM Link MSU/Sec	EAGLE M2PA/ M3UA MSU/Sec	ATM Link Equivalent	56K Link Equivalent	64K Link Equivalent
60	1800	10000	6	86	75
70	1800	10000	6	100	88
80	1800	10000	6	115	100
90	1200	10000	9	129	113
100	1200	10000	9	143	125
110	1200	10000	9	158	138
120	1200	10000	9	172	150
130	1200	10000	9	186	163
140	900	10000	12	200	175
150	900	10000	12	215	188
160	900	10000	12	229	200
170	900	10000	12	243	213
180	900	10000	12	258	225
190	720	10000	14	272	238
200	720	10000	14	286	250
210	720	10000	14	300	263
220	720	10000	14	315	275
230	720	10000	14	329	288
240	600	10000	17	343	300
250	600	10000	17	358	313
260	600	10000	17	372	325
270	600	10000	17	386	338

Table 5-4 EAGLE Link Equivalency for IPSG on SLIC for EAGLE 46.6 and Later Releases

Avg. MSU Size (MTP2 + MTP3)	EAGLE ATM Link MSU/Sec	EAGLE M2PA/M3UA MSU/Sec	ATM Link Equivalent	56K Link Equivalent	64K Link Equivalent
20	2000	12000	6	35	30
30	2000	12000	6	52	45
40	1800	12000	7	69	60
50	1800	12000	7	86	75
60	1800	12000	7	103	90
70	1800	12000	7	120	105
80	1800	12000	7	138	120
90	1200	12000	10	155	135
100	1200	12000	10	172	150
110	1200	12000	10	189	165
120	1200	12000	10	206	180
130	1200	12000	10	223	195
140	900	12000	14	240	210

Table 5-4 (Cont.) EAGLE Link Equivalency for IPSG on SLIC for EAGLE 46.6 and Later Releases

Avg. MSU Size (MTP2 + MTP3)	EAGLE ATM Link MSU/Sec	EAGLE M2PA/M3UA MSU/Sec	ATM Link Equivalent	56K Link Equivalent	64K Link Equivalent
150	900	12000	14	258	225
160	900	12000	14	275	240
170	900	12000	14	292	255
180	900	12000	14	309	270
190	720	12000	17	326	285
200	720	12000	17	343	300
210	720	12000	17	360	315
220	720	12000	17	378	330
230	720	12000	17	395	345
240	600	12000	20	412	360
250	600	12000	20	429	375
260	600	12000	20	446	390
270	600	12000	20	463	405

5.2.2 Hardware and software requirements

For SS7-over-IP networks, Oracle Communications uses E5-ENET-B and SLIC cards to achieve IP connectivity, using the IPSG application.

The IPSG application implements the M2PA and M3UA protocols, which are used for A-links (IPSG-M3UA) and B-, C-, and D-links (IPSG-M2PA) signaling links. Once the card is loaded with the IPSG application, it is referred to as an IPSG card.

The number of MSU/s supported by each card is dependent on various factors including MSU size, percentage of MSUs triggering the SCCP Class 1 sequencing feature, and the Integrated Monitoring feature.

5.2.3 System Capacity

Each of the IP7 applications may have a unique set of TPS ratings based on the card type used. System capacity for the EAGLE is assumed to include 160-byte average message size, including up to 150,000 Class-1 Sequenced SCCP TPS. The system capacity is defined as 10,000,00 TPS. While this limit is not enforced by the provisioning sub-system, the rated capacity of all IP7 applications running in an EAGLE must not exceed the available system capacity.

Note:

Other features, such as Integrated Monitoring, will also require system capacity and must be considered when calculating the available system capacity.

The EAGLE is engineered to support a system total capacity as defined in this section where:

- Each E5-ENET-B card running the IPSG application when the E5-ENET-B IPSG High Throughput feature is OFF has a maximum capacity of 6500 TPS.
- Each E5-ENET-B card running the IPSG application when the E5-ENET-B IPSG High Throughput feature is ON has a maximum capacity of 9500 TPS.
- Each SLIC card running the IPSG application has a maximum capacity of 12000 TPS. This capacity is applicable for both of the following scenarios:
  – When the IPSG High Throughput feature is OFF
  – When the IPSG High Throughput feature is ON

The system total depends on the system TPS. The total maximum allowed system TPS is 10,000,00.

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

5.3 Achieving IP Signaling 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 IPSG application.

5.3.1 Factors Affecting Advertised Capacity

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

- Host card
  Performance Characteristics of the host card can impact the capacity.
- CPU utilization
  Various 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 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).
- E5-ENET-B IPSG High Throughput feature

Turning on the E5-ENET-B IPSG High Throughput feature impacts the baseline configuration for the E5-ENET-B IPSG card as shown in Table 5-5

Table 5-5 Baseline Configuration Changes for the E5-ENET-B IPSG High Throughput Feature

E5-ENET-B Card Baseline Configuration	E5-ENET-B when IPSG High Throughput Feature OFF	E5-ENET-B IPSG High Throughput feature ON
Maximum TPS for the card	6500	9500
Average MSU size (bytes)	0-272	0-120
Max RTT (MS)	120	50
Max number of links/ associations	16	4
Protocol	M2PA and M3UA	M2PA

Table 5-6 Baseline Configuration Changes for SLIC

SLIC Card Baseline Configuration	SLIC
Maximum TPS for the card	10000
Average MSU size (bytes)	0-272
Max RTT (MS)	120
Max number of links/associations	16
Protocol	M3UA or M2PA

- Card de-rating
  If the E5-ENET-B IPSG High Throughput feature is turned on, the traffic rate is greater than 6500 TPS, and the E5-ENET-B IPSG card exceeds the limits shown in Table 5-5, then the card is de-rated according to the following calculations:
  - SLK TU cost factor = 1+ (RoundDown (((Number of links - 1)/4) * 0.025)
  - MSU size TU cost factor for M2PA links = 1+ (RoundUp(((Average MSU size - 120)/10) * 0.012)
  - MSU size TU cost factor for M3UA links = 1+ (RoundUp(((Average MSU size - 120)/10) * 0.02)
  - Association RTT cost factor (if greater than 50) = 1+ (RoundDown((Association RTT/25) * 0.04)
  - Protocol TU cost factor for M3UA links = 1.05

Note:

When calculating the values for the Average MSU SIF size >120, Number of Links >4, and Association RTT > 50, the values from the division in the formula are rounded to the quotient. In addition, the final values for the Transaction Unit Adjustment and Transaction Unit Cost values for Average MSU SIF size are rounded to the nearest 10 value if the delta is not a multiple of 10.

Given the derating factors, a derived SLK IP TPS for an MSU would be calculated as follows:

```
Derived SLK IP TPS for an MSU = 1 TU (Actual SLK IP TPS) +
(RoundDown (((Number of links - 1)/4) * 0.025) (for number of links >
4) +
(RoundUp(((Average MSU size - 120)/10) * 0.012) (for M2PA) OR
+ (RoundUp(((Average MSU size - 120)/10) * 0.02) (for M3UA)
+ (RoundDown((Association RTT/25) * 0.04) (for RTT>50 ms) +
0.05 (for M3UA)
```

For detailed descriptions of factors that affect advertised card capacity, see Engineering Rules for Determining IP7 Application Throughput.

5.3.2 Base transaction unit

The base IP signaling transaction unit involves an MSU sent and an MSU received. If using the E5-ENET-B when the IPSG High Throughput Feature is turned OFF, then each MSU has a **Service Information Field (SIF)** of less than or equal to 160 bytes. If the E5-ENET-B IPSG High Throughput feature is turned on, then each MSU has a SIF of less than or equal to 120 bytes.

The base Advertised Capacity of EAGLE 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 5-7 shows the base Advertised Capacity for IPSG application on applicable cards.

Table 5-7 Base Advertised Capacity for IPSG Cards

Card	Base Advertised Capacity (TPS)
E5-ENET-B (E5-ENET-B when IPSG High Throughput Feature OFF or SLIC)	6500 for IPSG
E5-ENET-B (E5-ENET-B IPSG High Throughput ON)	9500 for IPSG
SLIC[1]	12000 for IPSG

1 12K TPS requires EAGLE SW Release 46.6 or greater. Release 46.5 provides 10K TPS.

Exceeding the Advertised Capacity may result in signaling congestion, and in combination with the E5IS Data Feed feature, may result in the application discarding E5IS Data Feed messages.

5.3.2.1 Base Transaction Unit Rules: IPSG (E5-ENET-B when IPSG High Throughput Feature OFF)

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

1. Sufficient IP TPS (both Reserved and Max SLKPTS) is assigned to each link of an IPSG linkset.
2. The traffic is not monitored via the E5IS or Fast Copy features.
3. For IPSG, none of the received traffic triggers the enabled Eagle SCCP Class-1 Sequencing feature.
4. The IP packet-loss rate is 25 per 100,000 or less.
5. The IP connection message buffer memory is of a sufficient size on the local SCTP association and 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. Number of open IP connections is less than or equal to 16 (IPSG links).
9. M2PA Timer `T7` (Excess Delay in ACK) is configured to have a value appropriate for the expected network latency (IPSG M2PA links).
10. The IP connection minimum congestion window (CWMIN) is configured to an appropriate value to achieve the target IP TPS on the link.
11. The peer network element acknowledgment timer (SACK timer) is set to an appropriate value in correlation with the local IP connection RMIN and the expected network latency.

5.3.2.2 Base Transaction Unit Rules (E5-ENET-B IPSG High Throughput ON)

In addition to the rules specified in Base Transaction Unit Rules: IPSG (E5-ENET-B when IPSG High Throughput Feature OFF), the following base transaction rules apply to E5-ENET-B IPSG cards when the E5-ENET-B IPSG High Throughput feature is turned on:

1. Number of links provisioned is less than or equal to 4
2. The average MSU size per second carried by IPSG links is less than or equal to 120 bytes.
3. The network round trip time (RTT) is less than or equal to 50 ms.
4. The traffic is carried by M2PA links.

For IPSG configuration exceeding these rules, additional TU adjustment costs as shown in Table 5-11 are enforced for deriving TUs consumed by a signaling link (SLK). If the derived TU cost exceeds the configured SLKTPS/MAXSLKTPS on an IPSG SLK, it will result in congestion of the link and discard of the MSUs.

5.3.2.3 Base Transaction Unit Rules for SLIC IPSG

In addition to the rules specified in Base Transaction Unit Rules: IPSG (E5-ENET-B when IPSG High Throughput Feature OFF), the following rules apply:

1. E5-ENET-B capacity feature setting does not affect IPSG on SLIC below 10K TU.
2. GTT enabled on SLIC IPSG feature may generate additional traffic for GTT actions, for example, the DUPLICATE GTT action). When a GTT-enabled IPSG on SLIC card generates additional MSUs because of the configuration, an additional TU cost of one is added for each MSU duplicated or additional MSU generated because of the duplication.

For configuration deviating from the above rules, an additional TU cost need to be added to the base TU cost as described in the below table in order to derive total TU capacity consumed by the IPSG SLK. The additional TU cost is not enforced by the IPSG application, but any deviation from the above baseline will degrade the IPSG application performance eventually resulting in load shedding on IPSG application.

Table 5-8 IPSG Additional Transaction Units for Advanced Configurations

Configuration Attribute	Average MSU SIF size	Transaction Unit Adjustment (per MSU with Attribute)	Transaction Unit Cost (per MSU with Attribute)
MSU Size	0..160	0	1.0
	161..272	0.15	1.15
More than 16 Open IP Connections on IPSG card	0..272	0.135 * INT (# of connections / 16)	1 + (135 * INT(# of connections / 16)
MSU Triggers enabled SCCP Class-1 Sequencing feature	0..272	0.2	1.2
MSU Triggers SLAN copy	0..272	0.00143 * MSU Size	1 + (00143 * MSU size)
MTP-Routed SCCP Conversion feature enabled	0..272	0.00143 * MSU Size	1 + (00143 * MSU size)
MSU is copied by STC Data Feed	0..272	0.43	1.43
MSU is copied by Fast Copy	0..140	0.00	1.00
	141.272	0.32	1.32
GTT enabled on IPSG	0..160	0.00	1.00
	161..272	0.15	1.15

5.3.2.4 Base Transaction Unit Costs: IPSG

The base transaction unit cost for IPSG cards is based on the configuration rules shown in Base Transaction Unit Rules: IPSG (E5-ENET-B when IPSG High Throughput Feature OFF) and Base Transaction Unit Rules (E5-ENET-B IPSG High Throughput ON). Any additional configurations are applied to the adjusted transaction unit.

> **Note:**
>
> When calculating the values for the Average MSU SIF size >120, the values from the division in the formula are rounded to the quotient. In addition, the final values for the Transaction Unit Adjustment and Transaction Unit Cost values for Average MSU SIF size are rounded to the nearest 10 value if the delta is not a multiple of 10.

Table 5-9 Base Transaction Unit Cost Per MSU SIF Size for IPSG Cards

MSU SIF or UA Data Parm Size	E5-ENET-B IPSG Transaction Unit Cost*	E5-ENET-B IPSG High Throughput Feature
0-160	1	OFF
161-272	1.15	OFF
0-120	1	ON
121-272	M2PA: 1+ (RoundUp((Average MSU size – 120)/10)) * 0.012) M3UA: 1 + (RoundUp((Average MSU size – 120)/10)) * 0.02)	ON
273..4095	M2PA: RoundUp(msu size/272) + (RoundUp((272-120)/10)* 0.012) * RoundDown(msu size/ 272) + (RoundUp(((msu size % 272) – 120)/10) * 0.012) M3UA: RoundUp(msu size/272) + (RoundUp((272-120)/10)* 0.02) * RoundDown(msu size/ 272) + (RoundUp(((msu size % 272) – 120)/10) * 0.02)	ON
273..544	2	OFF
545..816	3	OFF
817..1088	4	OFF
1089..1360	5	OFF
1361..1632	6	OFF
1633..1904	7	OFF
1905..2176	8	OFF
2177..2448	9	OFF
2449..2720	10	OFF
2721..2992	11	OFF
2993..3264	12	OFF
3265..3536	13	OFF
3537..3808	14	OFF
3809..4080	15	OFF
4081..4095	16	OFF

Note:

*Values in the "E5-ENET-B IPSG Transaction Unit Cost" column aply to IPSG cards where `type=enetb` and the card is routing more than 6500 MSU/s.

5.3.3 Adjusted transaction unit

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

Configuration scenarios and their TU values for IPSG (M3UA and M2PA) are shown in Table 5-10, and Table 5-11. For more information on calculating throughput based on transaction units, see How to calculate transaction units per second (TPS).

> **Note:**
>
> When computing TU cost for configuration attributes such as size and number of connections/links on IPSG cards the TU used will be from Table 5-10 or Table 5-11, if an E5-ENET-B card is used and the status of the E5-ENET-B IPSG High Throughput feature.

Additional Transaction Units cost enforced by the IPSG application per Transaction for an E5-ENET-B card when the E5-ENET-B IPSG High Throughput feature is turned off is shown in Table 5-10.

Table 5-10 IPSG Additional Transaction Units for Advanced Configurations (E5-ENET-B when IPSG High Throughput Feature OFF)

Configuration Attribute	Average MSU SIF Size	Transaction Unit Adjustment (per MSU with attribute)	Transaction Unit Cost (per MSU with attribute)
MSU Size	0..160	0	1.0
	161..272	0.15	1.15
More than 16 open IP connections on IPSG card	0..272	0.135 * INT (# of connections / 16)	1 + (.135 * INT(# of connections / 16)
MSU triggers enabled SCCP Class-1 Sequencing feature	0..272	0.2	1.2
MTP-routed SCCP Conversion feature enabled	0..272	0.00143 * MSU Size	1 + (0.00143 * MSU Size)
MSU is copied by E5IS Data Feed	0..272	0.43	1.43
MSU is copied by Fast Copy	0..140	0.00	1.00
	141..272	0.32	1.32
GTT enabled on IPSG	0..160	0	1.0
	161..272	0.15	1.15

Additional Transaction Units cost enforced by IPSG application per Transaction when the E5-ENET-B IPSG configuration deviates from the configuration described in Table 5-5 and the E5-ENET-B IPSG High Throughput feature is turned on are shown in Table 5-11.

> **Note:**
>
> When calculating the values for the Average MSU SIF size >120, Number of Links >4, and Association RTT > 50, the values from the division in the formula are rounded to the quotient. In addition, the final values for the Transaction Unit Adjustment and Transaction Unit Cost values for Average MSU SIF size are rounded to the nearest 10 value if the delta is not a multiple of 10.

Table 5-11 IPSG Additional Transaction Units for Advanced Configurations (E5-ENET-B IPSG High Throughput Feature ON)

Configuration Attribute	Attribute Value	Transaction Unit Adjustment (per MSU with Attribute)	Transaction Unit Cost (per MSU with Attribute)
Average MSU SIF size >120 bytes	121-272	M2PA: (RoundUp((Average MSU size – 120)/10))) * 0.012[1]	M2PA: 1 + (RoundUp((Average MSU size – 120)/10))) * 0.012)
		M3UA: (RoundUp((Average MSU size – 120)/10))) * 0.02	M3UA : 1 + (RoundUp((Average MSU size – 120)/10))) * 0.02)
Number of links > 4	5 - 32	(RoundDown((Number of links – 1)/4))) * 0.025	1 + (RoundDown((Number of links – 1)/4))) * 0.025)
Association RTT > 50 ms	51 - 200 ms	(RoundDown(Association RTT / 25)) * 0.04[2]	1 + (RoundDown(Association RTT / 25)) * 0.04)
Protocol	M3UA	0.05	1.05
MSU is copied by Fast Copy	Card TPS > 6500	0.1[3]	1.1

1 Rounded to the next ten if the delta is not multiple of ten.
2 Quotient from the division is used in formula Derating formula applied only for RTT above 50 ms. Dearting factor for RTT <= 50 ms is 0.
3 If card TPS rate is > 6500 and copied by Fast Copy, De-rating factor is 0.1.

For an E5-ENET-B IPSG Capacity calculation with the E5-ENET-B IPSG High Throughput feature turned on, the total TU adjustments factors should be derived by adding TU factors for each of the following as applicable:

- Additional features such as SCCP Class-1 Sequencing, IMF copy, SCCP conversion as shown in Table 5-10
- Large MSU as shown in Table 5-9
- Configuration above baseline as shown in Table 5-11

5.3.4 How to calculate transaction units per second (TPS)

TPS can be calculated for IPSG cards. If E5-ENET-B cards are used as IPSG cards, then the TPS is calculated depending on whether the E5-ENET-B IPSG High Throughput feature is ON or OFF.

- Calculating TPS for IPSG Cards: E5-ENET-B when IPSG High Throughput Feature OFF

- Calculating TPS for IPSG Cards: E5-ENET-B IPSG High Throughput Feature ON

Calculating TPS for IPSG Cards: E5-ENET-B when IPSG High Throughput Feature OFF

Refer to Table 5-12 to follow the process:

1. Determine whether an E5-ENET-B card is used.
2. Determine the adapter protocol type of the association(s) that will carry the traffic .
3. 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 traffic is monitored
   - How many connections per card will carry the traffic (2)
   - Whether Signal Transfer Point SCCP Conversion applies to the traffic (4)
   - Whether the MSU is copied by E5IS Data Feed (5)

   Distinct traffic categories are identified by rows (**A**, **B**)
4. Select the TU value that applies (7).
5. The maximum total MSU rate, (actual Advertised Capacity), can be determined by dividing the Max MSU/s for the card by the total TU (7).

Table 5-12 Calculating TPS for IPSG Cards: E5-ENET-B when IPSG High Throughput Feature OFF

	1 MSU SIF Size	2 Number of links	3 Protocol	4 MSU Triggers SCCP copy	5 MSU Copied by E5IS Data Feed	6 TU Adjust - ment Factor	7 Total TU	8 Max MSU/s 5000 (E5-ENET)	9 Max MSU/s 6500 (E5-ENET-B)
A	0..160	<=16	M2PA	No	No	0	1.0	5000	6500
	0..160	<=16	M3UA	No	No	0	1.0	5000	6500
	0..160	<=16	M2PA	Yes	No	0.00143 * MSU Size	1 + (0.00143 * MSU Size)	-- (MSU size dependent)	5687
	0..160	<=16	M3UA	Yes	No	0.00143 * MSU Size	1 + (0.00143 * MSU Size)	-- (MSU size dependent)	5687
	0..160	<=16	M2PA	No	Yes	0.43	1.43	3496	4545
	0..160	<=16	M3UA	No	Yes	0.43	1.43	3496	4545
	0..160	>16	M2PA	No	No	0.135	1.135	4405	5727
	0..160	>16	M3UA	No	No	0.135	1.135	4405	5727
B	161..272	<=16	M2PA	No	No	0.15	1.15	4348	5652

Table 5-12 (Cont.) Calculating TPS for IPSG Cards: E5-ENET-B when IPSG High Throughput Feature OFF

1 MSU SIF Size	2 Number of links	3 Protocol	4 MSU Triggers SCCP copy	5 MSU Copied by E5IS Data Feed	6 TU Adjust - ment Factor	7 Total TU	8 Max MSU/s 5000 (E5-ENET)	9 Max MSU/s 6500 (E5-ENET-B)
161..272	<=16	M3UA	No	No	0.15	1.15	4348	5652
161..272	<=16	M2PA	Yes	No	0.00143 * MSU Size	1 + (0.00143 * MSU Size)	-- (MSU size dependent)	5687
161..272	<=16	M3UA	Yes	No	0.00143 * MSU Size	1 + (0.00143 * MSU Size)	-- (MSU size dependent)	5687
161..272	<=16	M2PA	No	Yes	0.43	1.43	3496	4545
161..272	<=16	M3UA	No	Yes	0.43	1.43	3496	4545
161..272	>16	M2PA	No	No	0.15	1.15	4348	5652
161..272	>16	M3UA	No	No	0.15	1.15	4348	5652

Calculating TPS for IPSG Cards: E5-ENET-B IPSG High Throughput Feature ON

Refer to Table 5-13 to follow the process for an IPSG card when the E5-ENET-B IPSG High Throughput feature is turned on.

1. Determine whether the card meets the standards shown in Table 5-5. If the card does not meet the optimized configuration, determine whether the card is being de-rated.
2. Determine the adapter protocol type of the association(s) that will carry the traffic (4).
3. Select the TU value that applies (6).
4. The maximum total MSU rate, (actual Advertised Capacity), can be determined by dividing the Max MSU/s for the card by the total TU (6).

Table 5-13 Calculating TPS for E5-ENET-B IPSG Cards: E5-ENET-B IPSG High Throughput Feature ON

1 Avg MSU SIF size (excluding large MSUs)	2 Association Round Trip Time RTT (ms)	3 Number of Links	4 Protocol	5 TU Adjust-ment Factor	6 Total TU	8 Max MSU/s 5000 (E5-ENET)	7 Max MSU/s 9500(E5-ENET-B)
0..120	<=50	<=4	M2PA	0	1.0	5000	9500
0..120	<=50	<=4	M3UA	0.05	1.05	5000	9048
160	<=50	<=4	M2PA	0.048	1.048	5000	9065
1..120	70	<=4	M3UA	0.13	1.13	5000	8407
1..120	<=50	8	M2PA	0.025	1.025	5000	9268
150	90	16	M3UA	0.281	1.281	5000	7416

5.3.4.1 Calculation example

This example uses a IPSG SLIC card. Refer to How to calculate transaction units per second (TPS) to follow this calculation:

- The signaling links are being monitored by E5IS (Data Feed)) (A3, B3).
- Traffic uses M3UA adapter.
- Eight IP connections are open and allowed.
- Eighty percent of traffic involves ISUP MSUs having a SIF size less than or equal to 160 bytes.
- Twenty percent of traffic involves SCCP-converted MSUs having a SIF size equal to 272 bytes.

```
(Base Advertised Capacity) =

((0.80 * (1+ 0.43)) + (0.20 * (1+ 0.43+ 0.15 + 0.00143*272) *
(Actual Advertised Capacity)=

(1.14 + 0.39) * (Actual Advertised Capacity)=

1.53 * (Actual Advertised Capacity)

(Actual Advertised Capacity)= (Base Advertised Capacity) /
(1.53) = 12000 / 1.53 = 2395 =7843
```

Once the needed throughput is established, calculate the number of cards required to support this need (see Calculate the Number of Cards Required).

5.3.4.2 Rules for Integrated Datafeed using STC cards

"Engineering Rules for Determining IP7 Application Throughput" contains additional rules related to Integrated Datafeed (for IMF using STC cards).

Follow the guidelines and consult the tables in "Engineering Rules for Determining IP7 Application Throughput" for the following information:

- Effects of different Integrated Monitoring configurations

- **Association** buffer sizes
- Throughput per association
- Congestion Window Minimum size

5.3.5 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 5-14 lists the maximum memory available for SCTP buffers on each card type.

Table 5-14 SCTP Buffer Space per Connection, Card and Application

Application	Card	Max # Conns	Default Conn Buffer	Max Conn Buffer	Max Total Buffer
IPSG	E5-ENET-B	32	200KB	400KB	6400KB
IPSG	SLIC	128	200KB	400KB	6400KB

For any given combination of Window Size and RTT between 2 devices, there exists an inherent limitation on the maximum throughput that can be achieved. Devices with larger buffer sizes supports a higher TPS rate and RTT combination. The equation to calculate the minimum required receive buffer size under ideal network conditions for the remote SCTP peer is:

```
Minimum SCTP receive buffer size (in bytes) required for an
association on remote SCTP node = ((Number of messages per
second/1000) * Network RTT in ms) * average SCTP payload size in bytes
```

Depending on specific network characteristics including packet loss, RTT, or level of jitter, doubling or quadrupling the calculated remote receive window value may be required to avoid buffer exhaustion and sustain the association.

The `BUFSIZE` parameter for the association will allocate memory for both transmit and receive buffers. If the advertised receive window from the remote peer is greater than the configured value for the association `BUFSIZE` parameter, the transmit buffer size on the Eagle will be limited to the provisioned value for `BUFSIZE`. Likewise, this will be the largest value that the congestion window minimum (CWMIN) variable will be allowed to take on while the association is established.

The `BUFSIZE` parameter will also set the maximum value for the advertised receive window (a_rwnd) that Eagle will send to the remote peer.

If value of the configured SCTP receive buffer size for an association on remote node is smaller than the SCTP transit buffer on EAGLE, then the maximum possible value of the receive window (rwnd) get reduced to the configured receive buffer size on the remote side. This effectively reduces the amount of data that can be transmitted on the association and causes high Tx buffer occupancy on EAGLE side during high traffic events. The data held in buffers can cause data transition delays between the nodes and may result in M2PA link failures reporting T7/T6 timeouts.

The following table shows an example of the required SCTP buffer size for a 140-byte MSU based on traffic rate and the round trip time calculated at the SCTP layer:

Table 5-15 Association Buffer Size in KB Required for 140-Byte MSU SIF Traffic

MSUs /sec	Round Trip Time (msec)							
	25	50	75	100	125	150	175	200
500	9	17	26	34	42	51	59	68
750	13	26	38	51	63	76	89	101
1000	17	34	51	68	84	101	118	135
1250	21	42	63	84	105	126	147	168
1500	26	51	76	101	126	152	177	202
1750	30	59	89	118	147	177	206	236
2000	34	68	101	135	168	202	236	269
2250	38	76	114	152	189	227	265	303
2500	42	84	126	168	210	252	294	336
2750	47	93	139	185	231	278	324	370
3000	51	101	152	202	252	303	353	404
3250	55	110	164	219	273	328	383	437
3500	59	118	177	236	294	353	412	471
3750	63	126	189	252	315	378	441	504
4000	68	135	202	269	336	404	471	538
4250	72	143	215	286	357	429	500	572
4500	76	152	227	303	378	454	530	605
4750	80	160	240	320	399	479	559	639
5000	84	168	252	336	420	504	588	672

The following table shows an example of the required SCTP buffer size for a 272-byte MSU based on traffic rate and the round trip time calculated at the SCTP layer:

Table 5-16 Association Buffer Size in KB Required for 272-Byte MSU SIF Traffic

MSUs /sec	Round Trip Time (msec)							
	25	50	75	100	125	150	175	200
500	15	30	45	60	75	90	105	120
750	23	45	68	90	113	135	158	180
1000	30	60	90	120	150	180	210	240
1250	38	75	113	150	188	225	263	300
1500	45	90	135	180	225	270	315	360

Table 5-16 (Cont.) Association Buffer Size in KB Required for 272-Byte MSU SIF Traffic

MSUs /sec	Round Trip Time (msec)							
	25	50	75	100	125	150	175	200
1750	53	105	158	210	263	315	368	420
2000	60	120	180	240	300	360	420	480
2250	68	135	203	270	338	405	473	540
2500	75	150	225	300	375	450	525	600
2750	83	165	248	330	413	495	578	660
3000	90	180	270	360	450	540	630	720
3250	98	195	293	390	488	585	683	780
3500	105	210	315	420	525	630	735	840
3750	113	225	338	450	563	675	788	900
4000	120	240	360	480	600	720	840	960
4250	128	255	383	510	638	765	893	1020
4500	135	270	405	540	675	810	945	1080
4750	143	285	428	570	713	855	998	1140
5000	150	300	450	600	750	900	1050	1200

The allocation of SCTP message buffer memory must be of sufficient size on the Eagle card, as well as the peer network element(s), to sustain the traffic for the network's round-trip time and worst-case packet loss.

Note:

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

5.3.6 System Constraints Affecting Total IP Signaling Capacity

Previous sections focused on the Maximum and Advertised Capacity of particular applications on particular cards for various configurations. This section focuses on constraints involved in using multiple IP signaling cards and applications.

Table 5-17 IPSG Connectivity Data

Feature	M2PA	M3UA	Notes
Cards per system	250	250	Worst-case inter-shelf IMT utilization is a key factor. The number of IPSG (including SLIC) cards that can be provisioned depends on various conditions, assuming each card is hosting links/linksets with max card capacity TPS values. See
Link connectivity type	Point to point (1 connection per link)	Point to multi-point	---
Link type replacement	Any	Any	---
Typical application	Interconnect transfer point	Interconnect a front-end SS7 gateway to a back-end service element	---
Links per card	32	32	Worst-case inter-shelf IMT utilization is a key factor. Virtual signaling link. Terminates SS7 network (IPSG).
Links per link set	16	16	Assumes unmated configuration. Link set defines the scope of a mateset/SG. If mated, then only one link is allowed in the link set.
Supports combined link sets	Yes	Yes	---
IP connections per system	4000	4000	---
IP connections per card	32	32	SCTP associations
Routing keys per system	---	---	---
IP connections per routing key	---	---	---
Application Servers per system	---	---	---
Associations per Application Server	---	---	---
Ethernet interfaces per card	2	2	Uni-homed connection on either interface, multi-homed using both interfaces
EAGLE Hardware Redundancy Model	2N	2N	---

Table 5-17 (Cont.) IPSG Connectivity Data

Feature	M2PA	M3UA	Notes
Capacity (TU)	6500 MSU/s (E5-ENET-B when IPSG High Throughput Feature OFF) 9500 MSU/s (E5-ENET-B card with E5-ENET-B IPSG High Throughput feature ON)	6500 MSU/s (E5-ENET-B when IPSG High Throughput Feature OFF) 9045 MSU/s (E5-ENET-B card with E5-ENET-B IPSG High Throughput feature ON)	
Failure mode (80%)	5200 MSU/s (E5-ENET-B when IPSG High Throughput Feature OFF,) 7600 MSU/s (E5-ENET-B card with E5-ENET-B IPSG High Throughput feature ON)	5200 MSU/s (E5-ENET-B when IPSG High Throughput Feature OFF,) 7236 MSU/s (E5-ENET-B card with E5-ENET-B IPSG High Throughput feature ON)	Capacity growth required at this point
Multi-homing support	Yes	Yes	---
Connection model	Server	Server	---
SS7 routing	Peer to peer	Traditional least-cost based	---
Supports lossless	Yes	No	---
Supports network management	Yes	Yes	---
Number of DTA Point Codes	1	1	---
Number of internal point codes per network	1	1	---
IPTPS for System	---	---	Total pool of capacity distributed by user across IPSG link sets
IPTPS OR M3UA link set	---	System IPTPS	---
IPTPS Signaling link	---	Link set IPTPS	---
IMT Inter-Shelf Capacity, each bus, ring topology	1 GB/sec	1 GB/sec	Full-Duplex
Maximum TPS per E5-ENET IPSG linkset	80000	8000	M3UA or M2PA
Maximum TPS per E5-ENET-B IPSG linkset with E5-ENET-B IPSG High Throughput feature turned OFF	104000	104000	M3UA or M2PA
Maximum TPS per E5-ENET-B IPSG linkset with E5-ENET-B IPSG High Throughput feature turned ON	152000	---	M2PA

Table 5-17 (Cont.) IPSG Connectivity Data

Feature	M2PA	M3UA	Notes
Maximum TPS per SLIC IPSG linkset	160000	160000	M3UA or M2PA

> **Note:**
>
> If an E5-ENET-B card is used and the E5-ENET-B IPSG High Throughput Capacity feature is turned ON, then the card must operate within the limits described in Table 5-5 or the card will de-rate.

5.4 SIGTRAN Engineering Guidelines

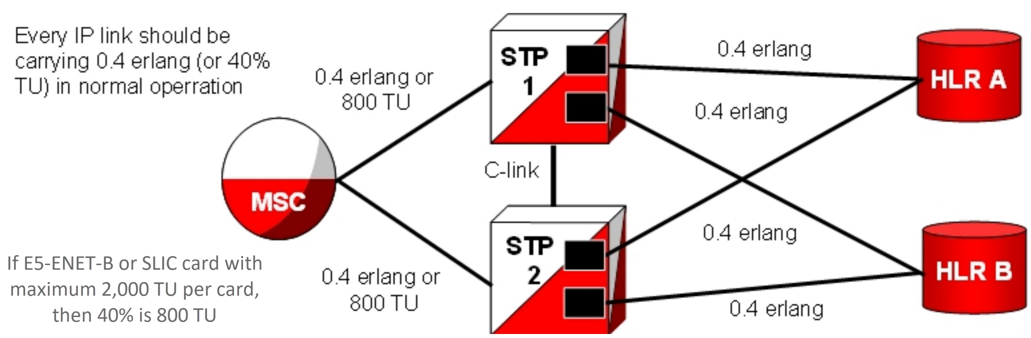
This section provides general SIGTRAN engineering guidelines with examples of normal and failover scenarios and resulting MSU calculations. Some overall guidelines to keep in mind include:

- Perform SIGTRAN engineering like TDM links
- Utilize Transaction Unit (TU/MSU) mapping
- For an IPSG card, the total capacity per card is considered as 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 (0.4 erlang)
- In failover scenarios, the card runs at 80% of total capacity (0.8 erlang)

The IPSG can be configured to support M2PA B-, C-, and D-Links; or to support A- and E-Links (see the note in M3UA (MTP Level 3 User Adaptation Layer) Protocol for more information about A-links).

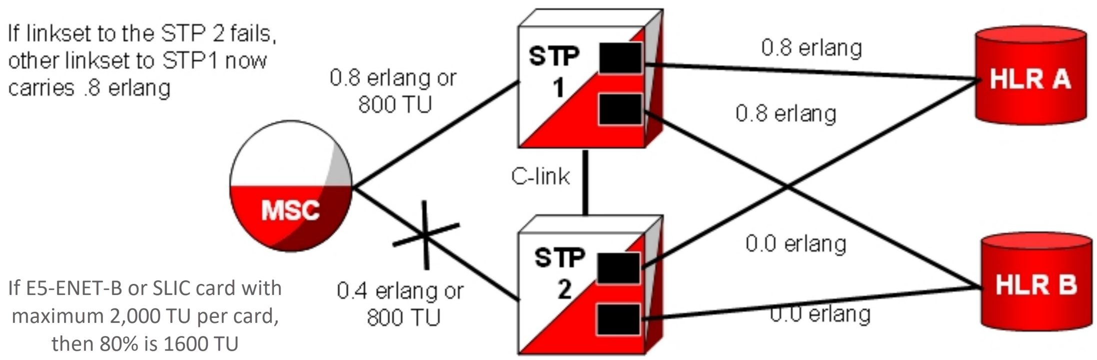
Every IP link should carry 0.4 erlang (or 40% TU) in normal operation. For an E5-ENET-B card with a maximum of 2,000 TU per card, 40% is 800 TU. This scenario is depicted in Figure 5-1.

Figure 5-1 SIGTRAN: Every IP Link at 0.4 Erlang



If the linkset to STP2 fails, another linkset to STP1 now carries 0.8 erlang. For a SLIC card with a maximum of 2,000 TU per card, 80% is 1,600 TU. This scenario is depicted in Figure 5-2.

Figure 5-2 SIGTRAN: Failover at 0.8 Erlang



5.4.1 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 E5-ENET-B 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 E5-ENET-B over M3UA with up to 4 connections and 100 byte/MSU without monitoring can support 2000 MSU/s.

So 2,000 MSU/s is 1 erlang

40% of 2,000 is 800 MSU/card

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

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 E5-ENET-B 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 E5-ENET-B over M3UA with up to 4 connections and 100 byte/MSU with monitoring can support 1400 MSU/s

So, 1,400 MSU/s is 1 erlang

40% of 1,400= 560 MSU/card

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

Guidelines for Maximum Provisionable IPSG Cards

The guidelines for maximum number of IPSG cards that can be provisioned depends on the following factors and is shown in Table 5-18.

- IPSG card hardware type (E5-ENET-B or SLIC)
- System TPS capacity
- Status of the E5-ENET-B IPSG High Throughput feature

Table 5-18 Guidelines for Maximum Provisionable IPSG Cards

HIPR2 High Rate Mode Feature	E5-ENET-B IPSG High Throughput Feature	E5-ENET-B IPSG	SLIC
ON	ON	78	75
ON	OFF	115	75
OFF	ON	52	N/A
OFF	OFF	76	N/A

5.5 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 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).

5.5.1 Unihoming versus Multihoming

EAGLE 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 links)

Unihoming

For unihoming, a set of IPSG 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 bandwidthsufficient to sustain the worst-case traffic load.

> **Note:**
>
> Since each IPx card maintains a single static IP route table utilized by all Ethernet interfaces or ports, associations from only one of the local hosts (IP ports) of an IP card to a particular remote host address is possible. Associations from multiple local hosts of an IP card to the same remote host address is not possible.

Multihoming

For multihoming, a set of IPSG 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.

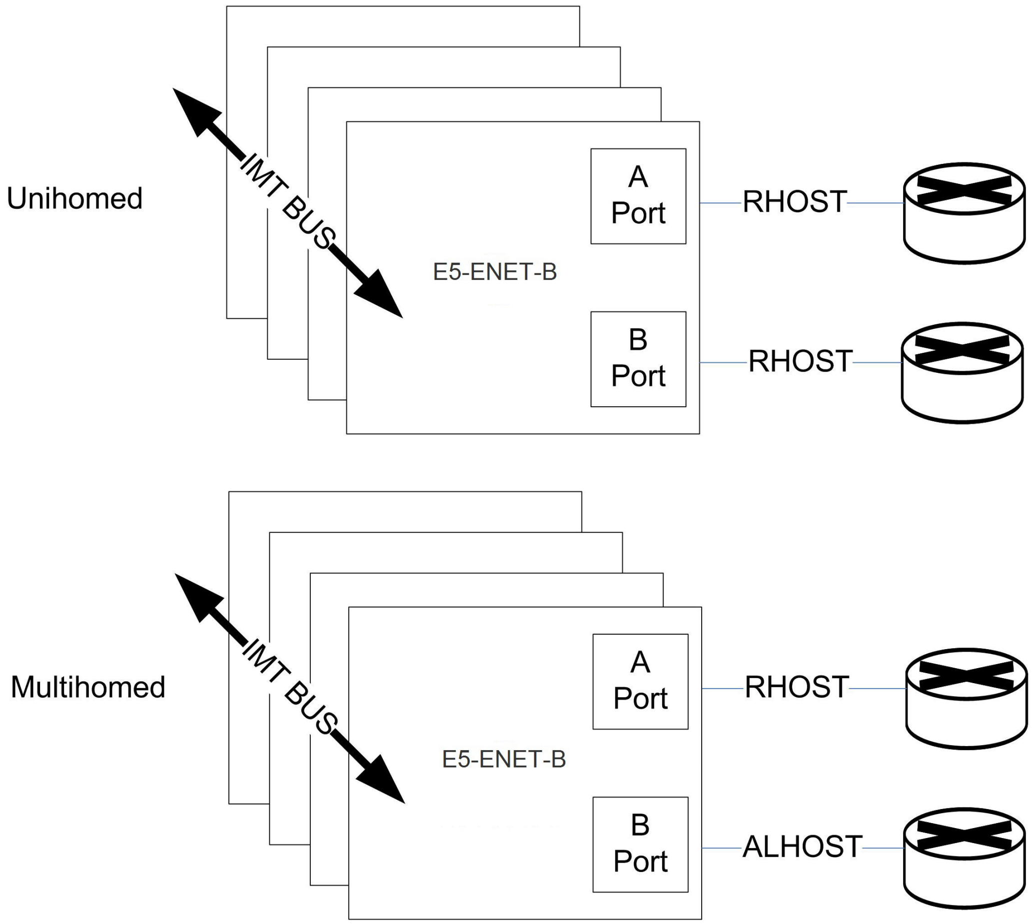
Multihoming is very important for M3UA connections because it is the only means of lossless handover in the event of a path failure.

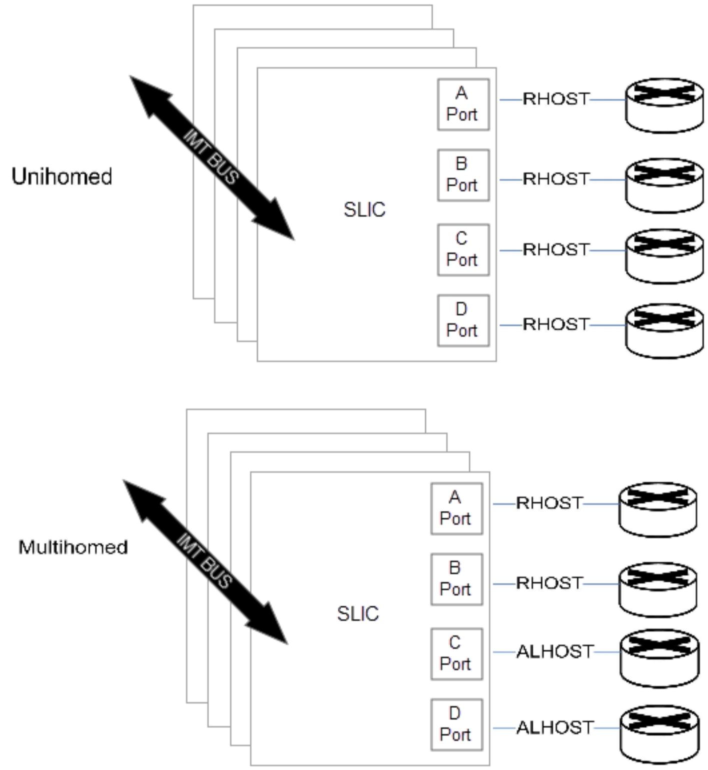
Multihoming provides network-level resilience for SCTP associations by providing information on alternate paths to a signaling end point for a single association.

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 IPx 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 IPx 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 5-3   Unihoming versus multihoming





Multi-homing can be used for M2PA links if the M2PA linkset has only one link.

If the M2PA linkset has more than one link, then the value of the M2PA Timer T7 should be lower than RMIN * RTIMES in order for the MTP3 level to trigger a Change Over procedure for MTP3 links.

> **Note:**
>
> RMIN*RTIMES is the minimum time required for an association to restart due to the RTIMES retransmission (via the primary and alternate path in round robin fashion) for an association without receiving any SACK. If the association is closed before the T7 expiration, then the buffer is cleared before the Change Over procedure is triggered by the MTP3 level.

5.5.2 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.

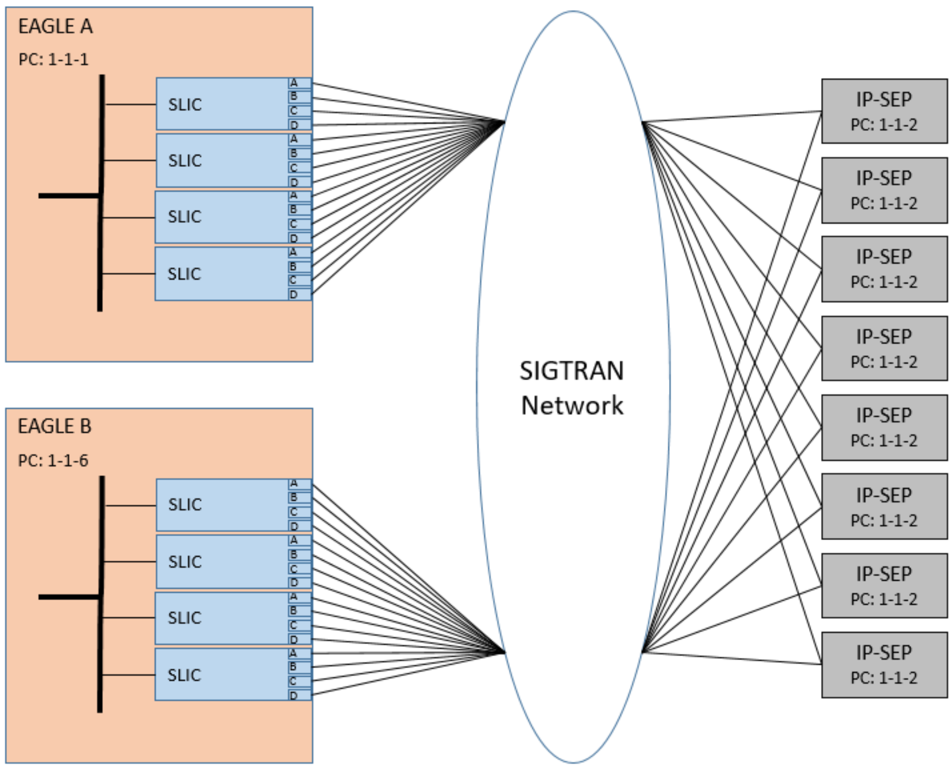
SCTP multihoming, in general, is less mature than MTP3 change-over procedures. In addition, the lack of ARHOST configurability in the EAGLE can result in asymmetrical traffic on a multihomed connection when both paths are available, which may be undesirable.

The EAGLE fully supports both options for M2PA, but Oracle recommends unihoming.

5.5.3 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 Oracle. This model is less robust but also less expensive.

Figure 5-4 Mated Signaling Transfer Point Redundancy With 4-Port SLIC Cards



5.5.4 IPSG Mateset

An **IPSG mateset** is an IPSG card linkset configuration with a setting of mated, meaning two IPSG linksets are allowed in a mateset by using the matelsn linkset parameter. The limitation of this approach is that each linkset can have only one card. This configuration for IPSG is supported to be backward compatible with previous EAGLE software versions.

IPSG status sharing

Each IPSG card supports up to 128 IP connections supported for SLIC cards, 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 IPSG 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

IPSG 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

5.5.5 Signaling Link Selection (SLS) Routing

A **Signaling Link Selection (SLS)** 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 Oracle Communications SS7-over-IP solution follows standard SLS load sharing with IPSG. With IPSG, SLS values are distributed over the associations in the Application Servers.

5.6 LAN/WAN Considerations

The operational characteristics of the LAN or WAN need to be quantified. General rules for the LAN or WAN environment devoted to SS7-over-IP traffic follow.

- 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 on the overall LAN performance. As the number of nodes increases on a LAN segment, the performance tends to decrease due to the 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.
- Dedicate sufficient bandwidth to your IP Signaling traffic.
  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 EAGLE, 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. The Non-SS7-over-IP nodes are any other devices that could be on the LAN using the LAN bandwidth, such as file servers or other hosts not directly

involved in the signaling solution. If the non-SS7-over-IP nodes are deployed on the same LAN as the SS7-over-IP nodes, then the nodes share the LAN resources.

- Restrict or severely limit the number of non-SS7-over-IP nodes.
  If the 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 the network behavior when the nodes are similar. This is an important factor that influences the network performance.
- Plan for and allocate the LAN capacity to handle worst-case scenarios.
  Consider all traffic sources and compute worst-case numbers to estimate the 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, RTT should be checked.
  Confirm that RTT is appropriate to achieve the maximum desired throughput and that RTT is acceptable from the viewpoint of the applications that are originating the traffic.

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

5.7 Retransmission Concept

The Oracle-recommended IP network environment for signaling traffic has the following components:

- RTTs set according to traffic (see Refine RTO Parameter)
- 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.

5.7.1 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 continues 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 the `RTIMES` errors, the end point address is marked as unreachable. For multihomed associations, if an endpoint's address is not in contact after the `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.

5.7.2 SCTP Timers

Oracle 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`: Desired retransmission mode (RFC or LIN) selected.
- `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. Oracle suggests 3 * `RMIN`.
- `RMIN`: Lower bound of calculated `RTO` (10 ms to 1,000 ms). The default is 120. Oracle 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 5-19 shows RFC timers and their RFC and Oracle-recommended default values.

Table 5-19 SCTP Configuration Data Descriptions for Oracle EAGLE

RFC Name	Description	RFC Recommended Default Value	Oracle Default Value	Oracle Configurable?	Oracle Ranges
RTO.initial	Initial RTO Value	3 seconds	120 ms	Yes Assoc RMIN parameter	1-1000 ms

Table 5-19 (Cont.) SCTP Configuration Data Descriptions for Oracle EAGLE

RFC Name	Description	RFC Recommended Default Value	Oracle Default Value	Oracle Configurable?	Oracle Ranges
RTO.max	Upper limit of RTO	60 seconds	800 ms	Yes Assoc RMAX parameter	1-1000 ms
RTO.min	Lower limit of RTO	1 second	120 ms	Yes Assoc RMIN parameter	1-1000 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 ms
Path.max. retrans	Maximum Data Retransmit attempts per Destination (used for multi-homing only)	5 attempts	5 attempts	Indirectly ½ of the assoc RTIMES parameter	1-6 ms
Acknowledge-ment timer	SACK Transmit	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
T3-rtx	Timer Data Retransmit	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	Timer 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	RTO+500 ms	Yes RTO + Assoc HBTIMER parameter	RTO+500 ms to RTO+10000 ms

Table 5-19 (Cont.) SCTP Configuration Data Descriptions for Oracle EAGLE

RFC Name	Description	RFC Recommended Default Value	Oracle Default Value	Oracle Configurable?	Oracle Ranges
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

Note:

SCTP Heart Beats (HBs) are sent after every HB interval on an idle path of the SCTP association. If more than one idle path exists, then HBs are sent alternately on each idle path, after each HB interval.

LIN Timer Setting

Oracle has implemented a more aggressive timer method called Linear (`LIN`) in which `RTO` between attempts is constant. Oracle 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 the `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 `RTO` is a moving average of the network RTT samples, as the jitter range increases, bounding the lower limit of the `RTO` at or near the average causes the amount of unnecessary retransmissions to increase, since for each transmission that takes longer than the current `RTO` to acknowledge a retransmission occurs, wasting bandwidth..

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

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

5.7.3 Configure Congestion Window Minimum (CWMIN) Parameter

The CWMIN parameter is important in managing the 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 results in periodic intermediate node overloads. CWMIN cannot be set less than 3K and should not exceed the remote peer reception window (Advertized Reception window). When possible, CWMIN is normally 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. CWMIN could be set to a value between 10% and 20% of the remote peer Reception window.

6 Implementation

This chapter provides hardware information, high-level configuration steps for the IPSG application, how to refine timers and parameters after the installation, and high-level system verification steps.

6.1 Hardware requirements

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

6.1.1 EAGLE

EAGLE fully configured for SS7-over-IP consists of at least one IPSG application. The application can be installed on an E5-ENET-B card or a SLIC card.

Table 6-1 shows the cards and their Advertised Capacity in TPS.

Table 6-1 EAGLE IP Signaling Maximum Capacities by Card and Application

EAGLE Card Name	IPSG Capacity
E5-ENET-B (E5-ENET-B when IPSG High Throughput Feature OFF, SLIC)	6,500
E5-ENET-B (E5-ENET-B IPSG High Throughput feature ON)	9,500
SLIC (IPSG High Throughput feature OFF)	12,000 as of Release 46.6; 10,000 in Release 46.5

The capacities listed in this table 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 results in signaling link or IP connection congestion.

6.1.2 Integrated Message Feeder (IMF)

When monitoring the IPx links using **IMF**, Oracle requires that the HIPR2 cards and at least one STC card are configured on the same shelf as the IPSG cards. The M2PA and M3UA 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 EAGLE.

The E5IS Data Feed or monitoring subsystem requires a significant amount of CPU and memory resources from the IPSG cards when monitoring the M2PA, M3UA links. When enabled, this capability causes the IPSG applications to drop well below the maximum capacity of the platform. For a detailed analysis of the IP7 throughput for provisioning purposes, refer to Engineering Rules for Determining IP7 Application Throughput.

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

6.2 Configuration

This section describes the configuration sequence for the IPSG application.

> **Note:**
>
> As of Release 44.0, all Ethernet ports are OFF by default. The in-service port and associated light will be turned ON by running the relevant application. The light for the unused port will remain OFF.

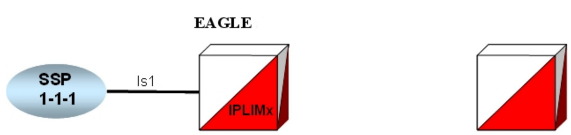
6.2.1 Configure the IPSG Application

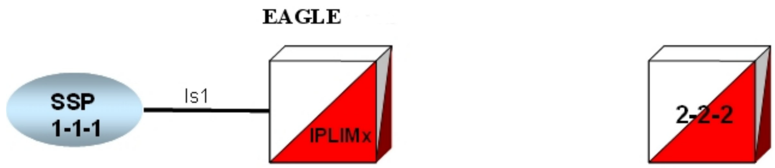
This section provides a basic overview of the steps involved to provision the IPSG application for M3UA. For detailed procedures, see *Database Administration - IP7 User's Guide* of your current EAGLE documentation suite.

1. Declare the E5-ENET-B card or the **SLIC** application to be ipsg (`ent-card`).
2. 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.
3. Associate an IP address to a host name used in configuring the association (`ent-iphost`).

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

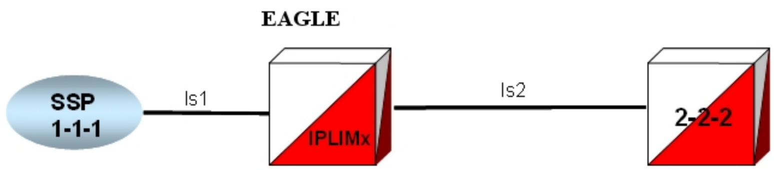
   This command configures the SCTP association in the Internet Protocol Application Socket (IPAPSOCK) table. This command permits the association to transport protocol data units and adaptive layer peer messages. Each association is connected to a process at the far end. The IPAPSOCK table is used to associate the Local Host or Local Port to a Remote Host or Remote Port.
5. Define the Site ID (`chg-sid`).
6. Enter the adjacent point code (`ent-dstn`).





7. Define the capacity and use the alarm (ent-ls).

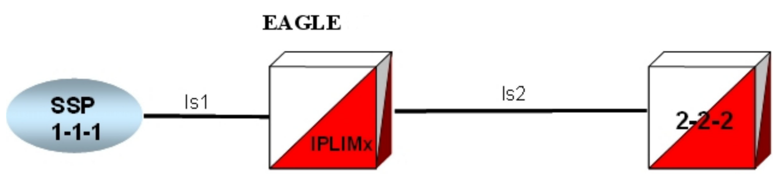
   ent-ls:lsn=ls1201:apc=10-10-10:lst=a:adapter=m3ua:ipsg=yes:rcontext=1:slktps=100



8. Tell EAGLE that this is a SIGTRAN M3UA link (`ent-slk`).
9. Enter the route (`ent-rte`).

SS7 Routing Table

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



10. Allow and open the SCTP association (`chg-assoc`).
11. Activate the signaling link (`act-slk`).

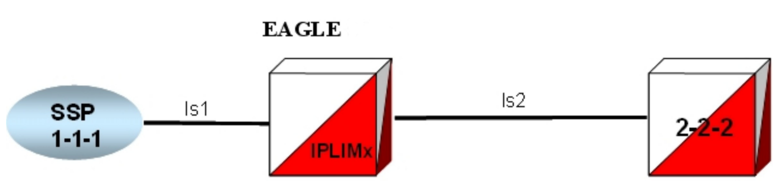
6.2.2 Configure the IPSG Application on the Same Card

The following series of commands may be used to provision an IPSG-M2PA link on the same card, assuming the card, IP addresses, and hosts are already configured.

1. Enter an Application Server Process and bind an SCTP association with it (`ent-assoc`).
2. Enter the adjacent point code (`ent-dstn`).
3. Define capacity and use the alarm (`ent-ls`).
4. Tell EAGLE that this is a SIGTRAN M2PA link (`ent-slk`).
5. Enter the route (`ent-rte`).

SS7 Routing Table

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



6. Allow and open the SCTP association (`chg-assoc`).
7. Activate the signaling link (`act-slk`).

6.3 Refine Timers and Parameters

The performance of SS7-over-IP may be improved by examining and setting timer values as described in the following sections.

- Define RTIMES Association Retransmits
- Define RTO Parameter
- Measure Jitter
- Refine RTO Parameter.

.

6.3.1 Define RTIMES Association Retransmits

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

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.

6.3.2 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.

6.3.3 Define RTXTHR Parameter

`:rtxthr` –The retransmission threshold for the association. The RTXTHR parameter value indicates the number of packet re-transmissions that can occur on the association (per monitoring time period of two seconds). Alarm "IP Connection Excess Retransmits" (UAM 536) will be raised if the number of packets re-transmitted is greater than the configured the RTXTHR parameter value, during five such consecutive monitoring periods. Once alarm is raised, it may require up to 12 consecutive monitoring periods with the number of re-transmissions < RTXTHR to clear the alarm. The design allows the alarm to come on at low error rates, and not come for occasional errors.

The value of this parameter is 0 to 65,535. The value of this parameter is shown in the RTXTHR field of the `rtrv-assoc:aname=<association name>` output. The rtxthr parameter value can be changed if the open parameter value is either "yes" or "no". It is possible to configure the RTXTHR so that UAM 536 alarms if the error rate on association is above the recommended maximum packet loss of 0.025%. If the error rate is more than 0.025%, investigate to determine if this can be improved in the network.

6.3.4 Measure Jitter

Measure jitter using 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 120 ms for the E5-ENET-B cards, or 50 ms for the E5-ENET-B cards running the IPSG application when the E5-ENET-B IPSG High Throughput feature is turned on.

6.3.5 Refine RTO Parameter

After an association is established, the EAGLE `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.

```
;
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
```

6.4 System Verification

Once EAGLE has been configured for SS7-over-IP, verify its correctness using the following section:

- Verify Network Connectivity

For more information on the commands, see *Commands User's Guide*.

6.4.1 Verify Network Connectivity

1. Is the SLIC IPSG 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>"
```

7 Troubleshooting

This chapter offers troubleshooting procedures based on symptoms occurring in the network.

7.1 General troubleshooting

1. Work from the bottom of the protocol stack up: first, IP Network; then the SS7 link or connection; then traffic routing.
2. Review provisioning and verify configuration in this order:
   - Card
   - Signaling (SS7) link
   - Linkset
   - IP link or IP network

   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

7.2 Verify UIMs and UAMs

- If there are any **Unsolicited Information Messages (UIMs)** or **Unsolicited Alarm Messages (UAMs)** occurring related to the SIGTRAN configuration, refer to *Unsolicited Alarms and Information Messages Reference*.

7.3 Is the card configured correctly?

1. 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 link configured correctly? (`rtrv-ip-lnk`; preferred settings are 100/full duplex on card AND switch - no AUTO configure)
   - 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`)

2. IP link configured correctly?

   `rtrv-ip-lnk`

   Preferred settings are 100/full duplex on card AND switch - no AUTO configure

3. IP routing configured?

   `rtrv-ip-rte`

   `rtrv-ip-card`

4. IP host table configured?

   `rtrv-ip-host`

   Check for local and remote addresses.

5. Signalling links (SLKs) and linksets configured correctly?

   `rept-stat-slk`

   `rept-stat-ls`

7.4 Connection does not become established

1. Card up and stable?

   `rept-stat-card`

2. Association status?

   `rept-stat-assoc`

3. Network connectivity?

   `netstat -I`

   `rept-stat-card:mode=full`

4. Errors (collisions, etc.) on the network interface?

   `netstat -d 0/1t`

5. Far end reachable?

   `ping`

   `traceroute`

6. Near end and far end use same SCTP CRC?

   `netstat –p`

   `sctp/rtrv-sg-opts`

7.5 Connection bounces and is unstable

1. Transport stable?

   `netstat –i`

   `netstat -d`

2. `RMIN` set too low?

`ping`

`assocrtt`

`rtrv-assoc`

Rule of thumb is above 1.2 * average RTT

7.6 Traffic not arriving at IP destination or traffic is lost

1. Route to destination's PC entered and available?

   `rept-stat-dstn`

2. Traffic being received/discarded on IP card? There can be numerous discard reasons!

   `msucount -l`

7.7 Are connection(s) congesting?

1. Is SCTP buffering set correctly for network RTT?

   `rtrv-assoc`

   `assocrtt,`

   `sctp`

2. Is an interface set to half-duplex somewhere in the path to the far end, causing excessive retransmissions?

   `rtrv-ip-lnk`

   `sctp`

7.8 Traffic not load-balanced properly

1. Source traffic has uneven SLS distribution?
2. All cards in linkset or mateset do not host a connection to the IP Application Server(IPSG only)?

   `rtrv-assoc`

   `rtrv-as`

3. IPSG cards in mateset with no established connections have signaling link deactivated to minimize '**double-hopping**' (IPSG only)?

   rept-stat-card

   `msucount -l`

7.9 Link Level Events

1. IPSG `pass` command

   `linkinfo -l`

2. IPSG `linkinfo` has other interesting options?

   `-c`

`-m`

3. IPSG `pass` command

   `ualog`

   `aslog`

4. Both commands have event filtering (link events vs. traffic), so look at options

7.10 Association

- IPSG/ `pass` command

  `sctp -a`

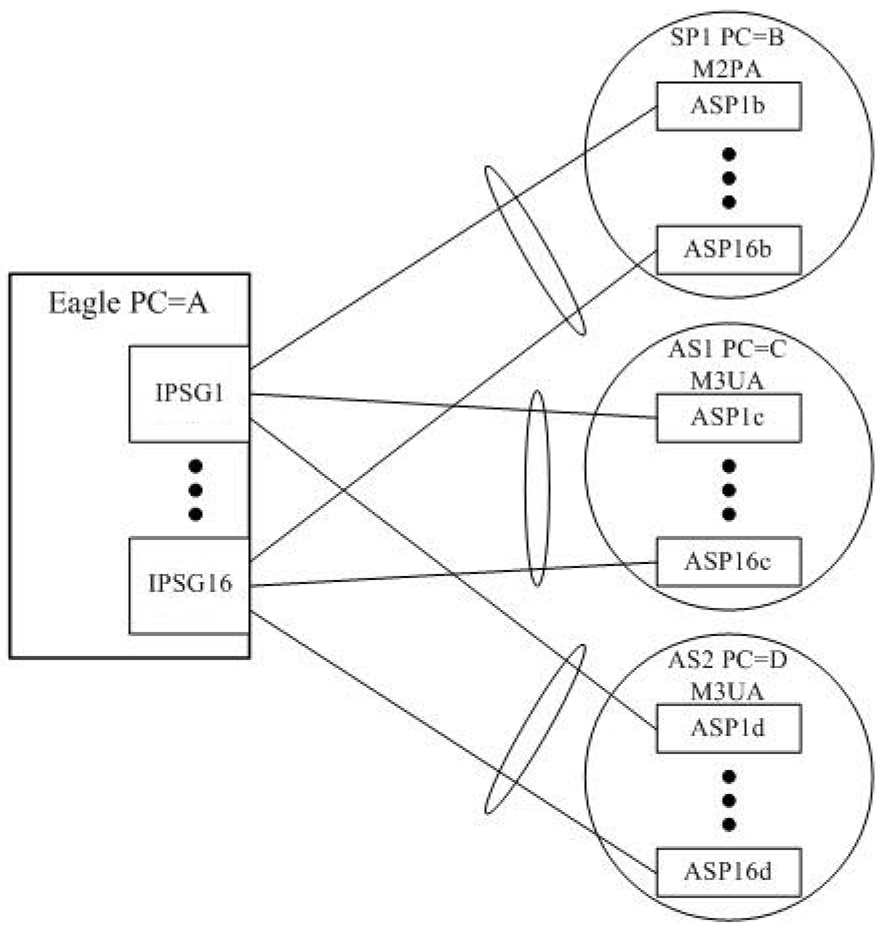
A

Additional Deployment Scenarios

This chapter provides additional scenarios for deployment of SS7-over-IP using SIGTRAN.

A.1 IPSG Deployment Scenario

Figure A-1 Example Deployment of IPSG Application



> **Note:**
>
> - Oracle Communications EAGLE Service and Link Interface Card (SLIC) is a single-slot, multi-use card that runs multiple applications.
> - Each IP-attached signaling point or application server is represented in EAGLE as a linkset (ovals).
> - Up to 16 IPSG links are supported per linkset
> - If an E5-ENET-B card is used as the IPSG card, and if the E5-ENET-B IPSG High Throughput feature is turned ON, then the card supports a maximum of 4 links before de-rating. See Factors Affecting Advertised Capacity for additional information.
> - Each connecting line represents an SS7 signaling link and an SCTP association.
> - Multiple linksets are supported.
> - Each linkset supports one SIGTRAN adapter type (M2PA or M3UA).
> - Point Codes 'B', 'C', and 'D' can involve any mixture of ANSI and ITU point codes. If different variants are in use, Eagle must have a point code in each of the networks.
> - Multiple signaling links per card are supported.

The IPSG feature provides the M3UA functionality that behaves more like other LIMs, providing the following benefits:

- The new IPSG application M3UA operational model equates Linkset (LS) and Application Server (AS). It equates Signaling Link (SLK) with an AS-ASP (Routing Context + Association) instance. This allows each AS-ASP instance to be administered as a signaling link.
- A new signaling link type, IPSG-M3UA, can be assigned to linksets having up to 16 signaling links. This is double the 8-link (and card) limitation of the former IPGWx linkset.
- Each IPSG card will host up to 128 signaling links.
- Each IPSG card will host up to 128 SCTP associations. A maximum of 16 IPSG-M3UA signaling links can be assigned to a single association.
- The adjacent point code (APC) of the IPSG-M3UA linkset is the point code assigned to the Application Server serviced by the linkset. The IPSG-M3UA linkset does not require a fake adjacent point code as the former IPGWx application does.
- Each IPSG-M3UA signaling link can have a single IP connection, unlike the former IPGWx signaling link, which can have up to 50 IP connections.
- The state of the IPSG-M3UA signaling link is based on the states of the assigned IP connection and AS-ASP instance. If the IP connection is unavailable for traffic, the IPSG-M3UA signaling link is also unavailable. If the AS-ASP instance is not available, then the IPSG-M3UA signaling link is also unavailable. *
- Multiple IPSG-M3UA signaling links (up to 16) can share one IP connection, as long as all of the IPSG-M3UA signaling links and corresponding IP connection are

hosted by the same card. This enables multiple SS7 variant support across a single IP connection.

- The IPSG-M3UA signaling links provide MTP3 routing only. The IPSG application does not implement secondary routing-key routing, so every attached AS must be uniquely identified in the network by a point code.