Internet Engineering Task Force
INTERNET-DRAFT
Transport Working Group
Category: Informational
June 1999
Expires: January 2000

Authors
Lyndon Ong, Nortel Networks
Ian Rytina, Miguel Garcia, Ericsson
HannsJuergen Schwarzbauer, Lode Coene, Siemens
Huai-an Paul Lin, Telcordia
Imre Juhasz, Telia
Matt Holdrege, Ascend
Chip Sharp, Cisco Systems

Architectural Framework for Signaling Transport

< draft-ietf-sigtran-framework-arch-02.txt >

Status of this Memo

Abstract

This document defines an architecture framework and functional requirements for transport of signaling information over IP. The framework describes relationships between functional and physical entities exchanging signaling information, such as Signaling Gateways and Media Gateway Controllers. It identifies interfaces where signaling transport may be used and the functional and performance requirements that apply from existing Switched Circuit Network (SCN) signaling protocols.

Table of Contents

1. Introduction

1.1 Overview

This document defines an architecture framework for transport of message-based signaling protocols over IP networks. The scope of this work includes definition of encapsulation methods, end-to-end protocol mechanisms and use of existing IP capabilities to support the functional and performance requirements for signaling transport.

The framework portion describes the relationships between functional and physical entities used in signaling transport, including the framework for control of Media Gateways, and other scenarios where signaling transport may be required.

The requirements portion describes functional and performance requirements for signaling transport such as flow control, in-sequence delivery and other functions that may be required for specific SCN signaling protocols.

1.2 Terminology

The following are general terms are used in this document:

Backhaul:

Backhaul refers to the transport of signaling from the point of interface for the associated data stream (i.e., SG function in the MGU) back to the point of call processing (i.e., the MGCU), if this is not local.

Signaling Transport (SIG):

SIG refers to signaling transport, which provides the interface for signaling transport across and within IP networks. SIG includes a set of functions supplementing a standard IP transport protocol to provide the SCN protocol being transported with the same service interface that is provided by its SCN lower layer.

Switched Circuit Network (SCN):

The term SCN is used to refer to a network that carries traffic within channelized bearers of pre-defined sizes. Examples include Public Switched Telephone Networks (PSTNs) and Public Land Mobile Networks (PLMNs). Examples of signaling protocols used in SCN include Q.931, SS7 MTP Level 3 and SS7 Application/User parts.

The following are terms for functional entities relating to signaling transport in a distributed gateway model.

Media Gateway (MG):

A MG terminates SCN media streams, packetizes the media data,, if it is not already packetized, and delivers packetized traffic to the packet network. It performs these functions in reverse order for media streams flowing from the packet network to the SCN.

Media Gateway Controller (MGC):

An MGC handles the registration and management of resources at the MG. The MGC may have the ability to authorize resource usage based on local policy. For signaling transport purposes, the MGC serves as a possible termination and origination point for SCN application protocols, such as SS7 ISDN User Part and Q.931/DSS1.

Signaling Gateway (SG):

An SG is a signaling agent that receives/sends SCN native signaling at the edge of the IP network. The SG function may relay, translate or terminate SS7 signaling in an SS7-Internet Gateway. The SG function may also be co-resident with the MG function to process SCN signaling associated with line or trunk terminations controlled by the MG (e.g., signaling backhaul).

The following are terms for physical entities relating to signaling transport in a distributed gateway model:

Media Gateway Unit (MGU)

An MG-Unit is a physical entity that contains the MG function. It may contain other functions, esp. an SG function for handling facility-associated signaling.

Media Gateway Control Unit (MGCU)

An MGC-Unit is a physical entity containing the MGC function.

Signaling Gateway Unit (SGU)

An SG-Unit is a physical entity containing the SG function.

Signaling End Point (SEP):

This is a node in an SS7 network that originates or terminates signaling messages. One example is a central office switch.

Signal Transfer Point (STP):

This is a node in an SS7 network that routes signaling messages based on their destination point code in the SS7 network

1.3 Scope

Signaling transport provides transparent transport of message-based signaling protocols over IP networks. The scope of this work includes definition of encapsulation methods, end-to-end protocol mechanisms and use of IP capabilities to support the functional and performance requirements for signaling.

Signaling transport shall be used for transporting SCN signaling between a Signaling Gateway Unit and Media Gateway Controller Unit. Signaling transport may also be used for transport of message-based signaling between a Media Gateway Unit and Media Gateway Controller Unit, between dispersed Media Gateway Controller Units, and between two Signaling Gateway Units connecting signaling endpoints or signal transfer points in the SCN.

Signaling transport will be defined in such a way as to support encapsulation and carriage of a variety of SCN protocols. It is defined in such a way as to be independent of any SCN protocol translation functions taking place at the endpoints of the signaling transport, since its function is limited to the transport of the SCN protocol.

Since the function being provided is transparent transport, the following

areas are considered outside the scope of the signaling transport work:

- definition of the SCN protocols themselves
- signaling interworking such as conversion from Channel Associated Signaling (CAS) to message signaling protocols
- specification of the functions taking place within the SGU or MGU
  - in particular, this work does not address whether the SGU provides mediation/interworking, as this is transparent to the transport function.
  - similarly, some management and addressing functions taking place within the SGU or MGU are also considered out of scope, such as determination of the destination IP address for signaling, or specific procedures for assessing the performance of the transport session (i.e., testing and proving functions).

2. Signaling Transport Architecture

2.1 Gateway Component Functions

Figure 1 defines a commonly defined functional model that separates out the functions of SG, MGC and MG. This model may be implemented in a number of ways, with functions implemented in separate devices or combined in single physical units.

Where physical separation exists between functional entities, Signaling Transport can be applied to ensure that SCN signaling information is transported between entities with the required functionality and performance.

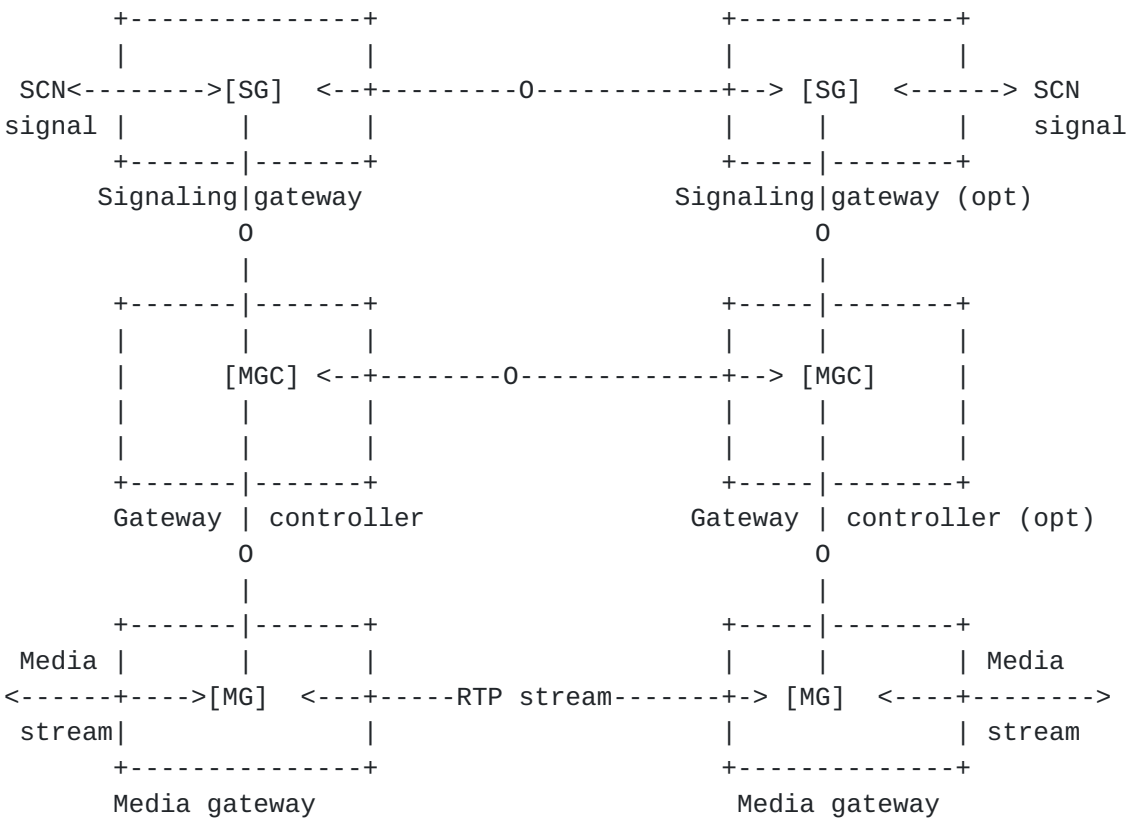


Figure 1: Sigtran Functional Model

As discussed above, the interfaces pertaining to signaling transport include SG to MGC, SG to SG and may potentially include MGC to MGC or MG to MGC as well.

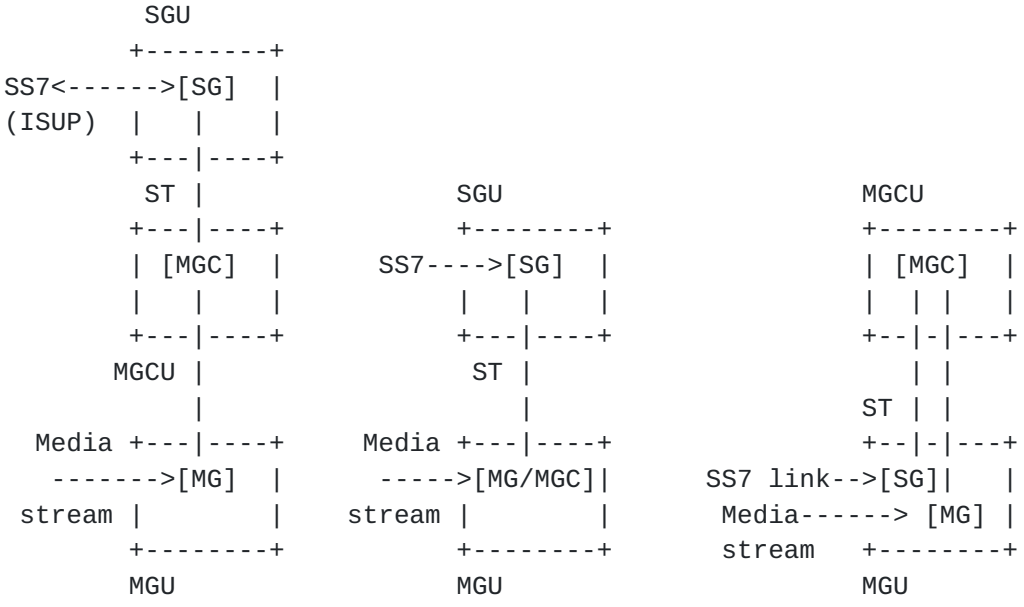
2.2 SS7 Interworking for Connection Control

Figure 2 below shows some example implementations of these functions in physical entities as used for interworking of SS7 and IP networks for Voice over IP, Voice over ATM, Network Access Servers, etc. No recommendation is made as to functional distribution and other implementations are possible.

For interworking with SS7-controlled SCN networks, the SG terminates the SS7 link and transfers the signaling information to the MGC using signaling transport. The MG terminates the interswitch trunk and controls the trunk based on the control signaling it receives from the MGC. As shown below in case (a), the SG, MGC and MG may be implemented in separate physical units, or as in case (b), the MGC and MG may be implemented in a single physical unit.

In alternative case (c), a facility-associated SS7 link is terminated by the same device (i.e., the MGU) that terminates the interswitch trunk. In this case, the SG function is co-located with the MG function, as shown below, and signaling transport is used to "backhaul" control signaling to the MGCU.

Note: SS7 links may also be terminated directly on the MGCU by cross-connecting at the physical level before or at the MGU.



(a) (b) (c)

Notes: ST = Signaling Transport used to carry SCN signaling

Figure 2: Example Implementations

In some implementations, the function of the SG may be divided into multiple physical entities to support scaling, signaling network management and addressing concerns. Thus, Signaling Transport can be used between SGs as well as from SG to MGC. This is shown in Figure 3 below.

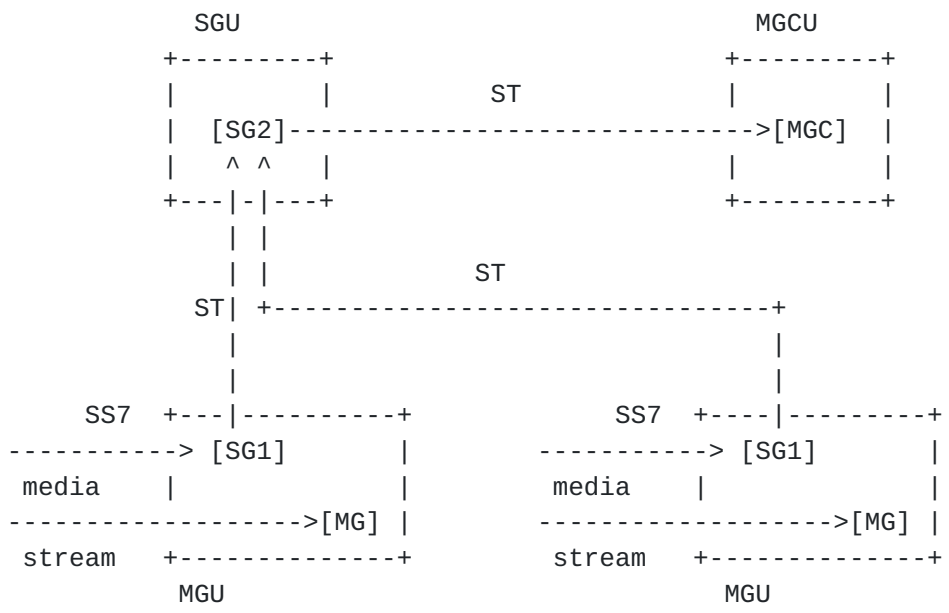


Figure 3: Multiple SG Case

In this configuration, there may be more than one MGU handling facility associated signaling (i.e. more than one containing it's own SG function), and only a single SGU. It will therefore be possible to transport one SS7 layer between SG1 and SG2, and another SS7 layer between SG2 and MGC. For example, SG1 could transport MTP3 to SG2, and SG2 could transport ISUP to MGC.

2.3 ISDN Interworking for Connection Control

In ISDN access signaling, the signaling channel is carried along with data channels, so that the SG function for handling Q.931 signaling is co-located with the MG function for handling the data stream. Where **Q.931 is then transported to the MGC for call processing, signaling** transport would be used between the SG function and MGC. This is shown in Figure 3 below.

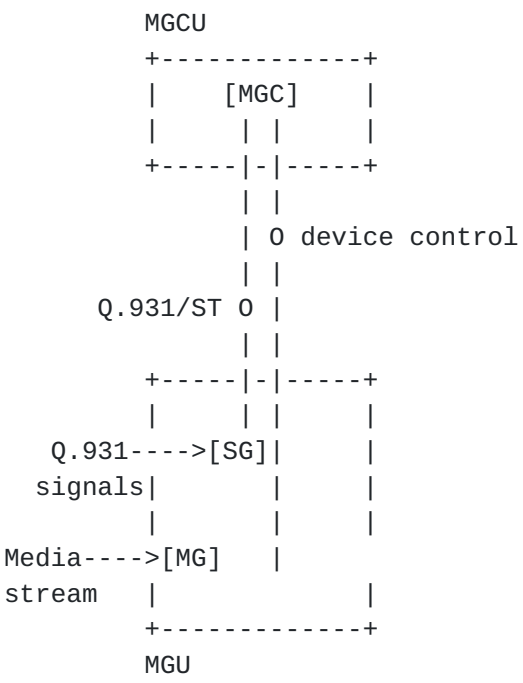


Figure 4: Q.931 transport model

2.4 Architecture for Database Access

Transaction Capabilities (TCAP) is the application part within SS7 that is used for non-circuit-related signaling.

TCAP signaling within IP networks may be used for cross-access between entities in the SS7 domain and the IP domain, such as:
- access from an SS7 network to a Service Control Point (SCP) in IP
- access from an SS7 network to an MGC
- access from an MGC to an SS7 network element
- access from an IP SCP to an SS7 network element

A basic functional model for TCAP over IP is shown in Figure 5.

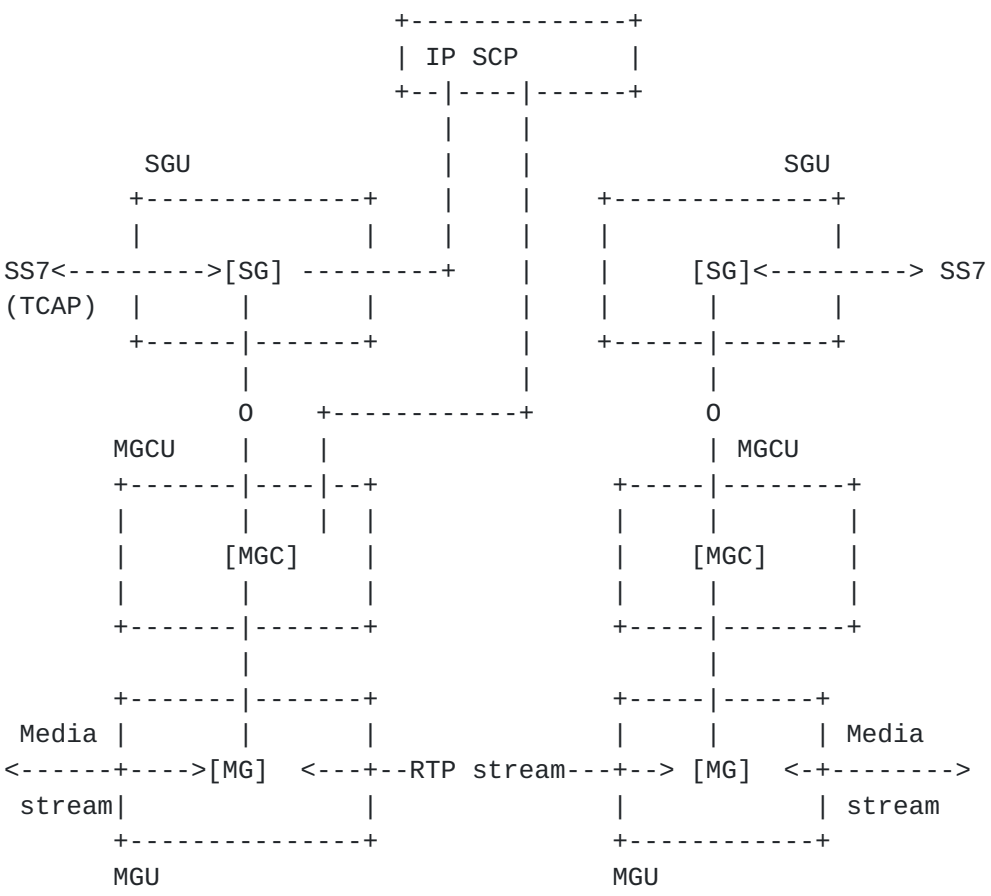


Figure 5: TCAP Signaling over IP

3. Protocol Architecture

This section provides a series of examples of protocol architecture for the use of Signaling Transport (SIG).

3.1 Signaling Transport Components

Signaling Transport in the protocol architecture figures below is assumed to consist of three components (see Figure 6):

1) an adaptation sub-layer that supports specific primitives, e.g., management indications, required by a particular SCN signaling application protocol.
2) a Common Signaling Transport Protocol that supports a common set of reliable transport functions for signaling transport.
3) a standard IP transport protocol provided by the operating system.

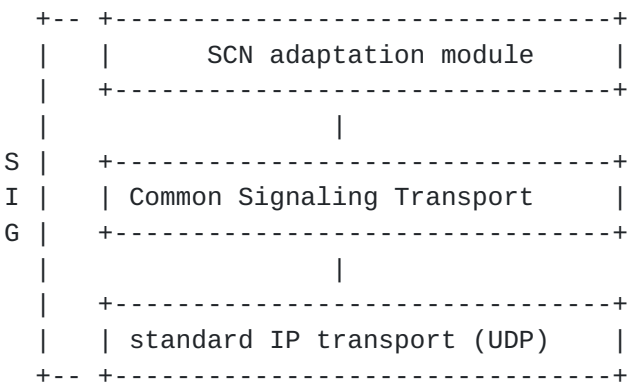
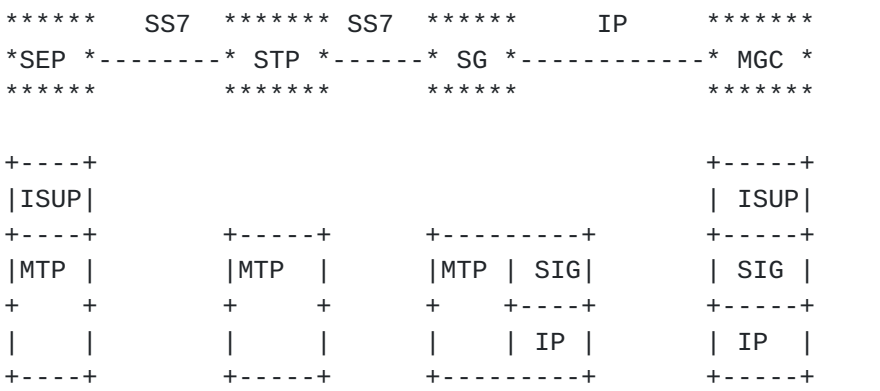


Figure 6: Signaling Transport Components

3.2. SS7 access for Media Gateway Control

This section provides a protocol architecture for signaling transport supporting SS7 access for Media Gateway Control.

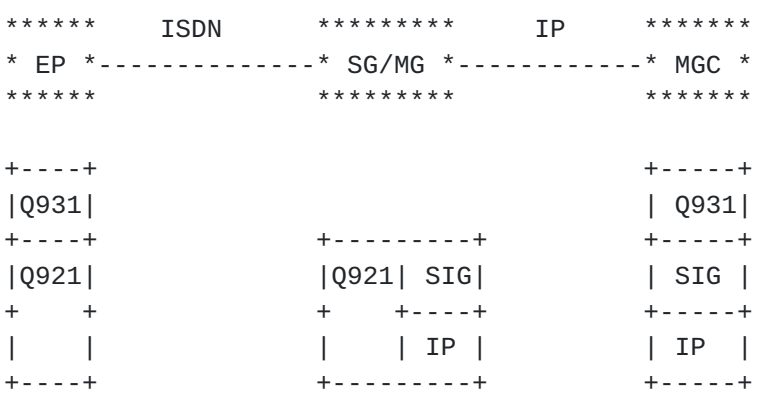


STP - Signal Transfer Point SEP - Signaling End Point
SG - Signaling Gateway SIG - Signaling Transport
MGC - Media Gateway Controller

Figure 7: SS7 Access to MGC

3.3. Q.931 Access to MGC

This section provides a protocol architecture for signaling transport supporting ISDN point-to-point access (Q.931) for Media Gateway Control.



MG/SG - Media Gateway with SG function for backhaul
EP - ISDN End Point

Figure 8: ISDN Access

3.4. SS7 Access to IP/SCP

This section provides a protocol architecture for database access, for example providing signaling between two IN nodes or two mobile network nodes. There are a number of scenarios for the protocol stacks and the functionality contained in the SIG, depending on the SS7 application.

In the diagrams, SS7 Application Part (S7AP) is used for generality to cover all Application Parts (e.g. MAP, IS-41, INAP, etc). Depending on the protocol being transported, S7AP may or may not include TCAP. The interface to the SS7 layer below S7AP can be either the TC-user interface or the SCCP-user interface.

Figure 9a shows the scenario where SCCP is the signaling protocol being transported between the SG and an IP Signaling Endpoint (ISEP), that is, an IP destination supporting some SS7 application protocols.

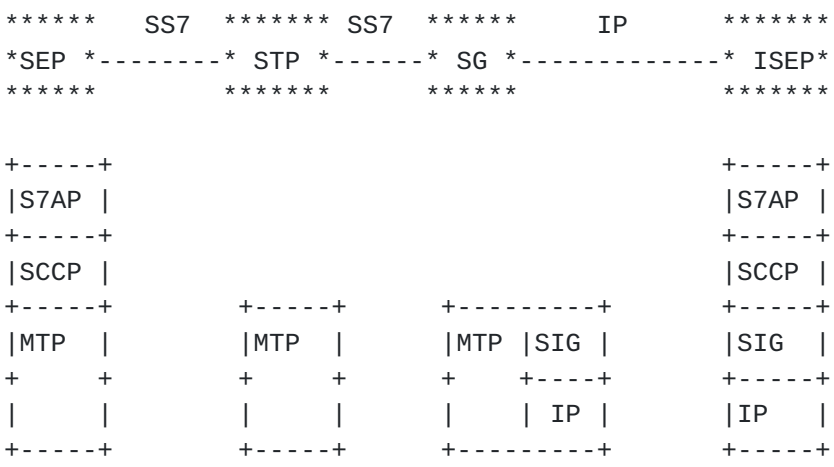


Figure 9a: SS7 Access to IP node - SCCP being transported

Figure 9b shows the scenario where S7AP is the signaling protocol being transported between SG and ISEP. Depending on the protocol being transported, S7AP may or may not include TCAP, which implies that SIG must be able to support both the TC-user and the SCCP-user interfaces.

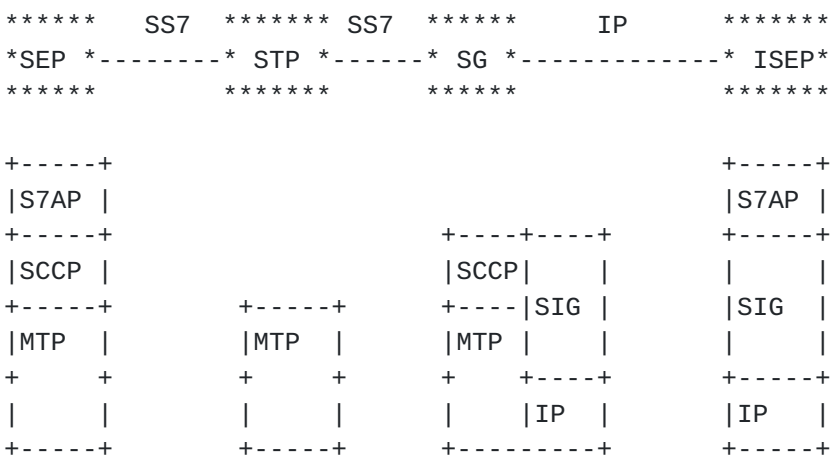


Figure 9b: SS7 Access to IP node - S7AP being transported

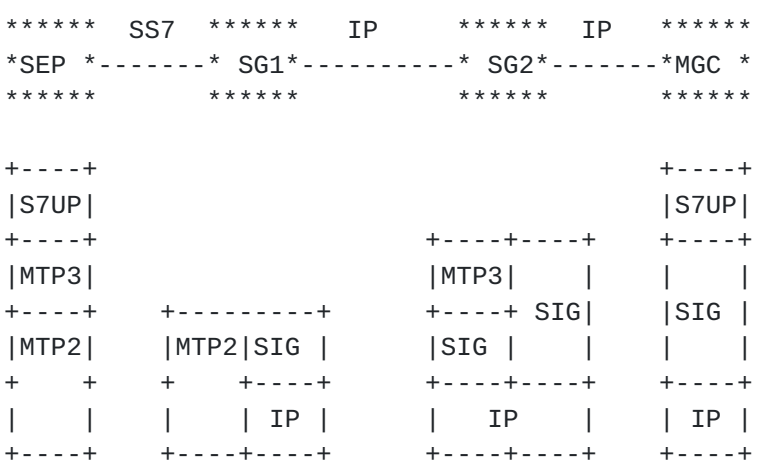
3.5. SG to SG

This section identifies a protocol architecture for support of signaling between two endpoints in an SCN signaling network, using signaling transport directly between two SGs.

The following figure describes protocol architecture for a scenario with two SGs providing different levels of function for interworking of SS7 and IP. This corresponds to the scenario given in Figure 3.

The SS7 User Part (S7UP) shown is an SS7 protocol using MTP directly for transport within the SS7 network, for example, ISUP.

In this scenario, there are two different usage cases of SIG, one which transports MTP3 signaling, the other which transports ISUP signaling.



S7UP - SS7 User Part

Figure 10: SG to SG Case 1

The following figure describes a more generic use of SS7-IP interworking for transport of SS7 upper layer signaling across an IP network, where the endpoints are both SS7 SEPs.

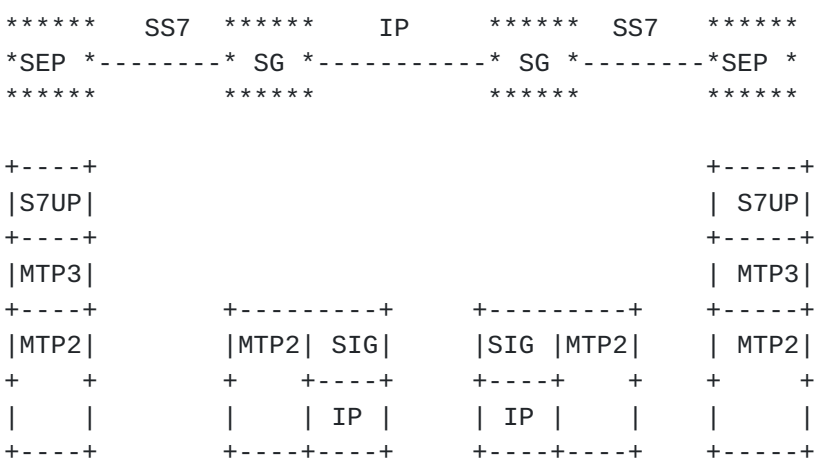


Figure 11: SG to SG Case 2

4. Functional Requirements

Signaling transport provides for the transport of native SCN protocol messages over a packet switched network.

Signaling transport shall:

1) Transport of a variety of SCN protocol types, such as the application and user parts of SS7 (including MTP Level 3, ISUP, SCCP, TCAP, MAP, INAP, IS-41, etc.) and layer 3 of the DSS1/PSS1 protocols (i.e. Q.931 and QSIG).

2) Provide a means to identify the particular SCN protocol being transported.

3) Provide a common base protocol defining header formats, security extensions and procedures for signaling transport, and support extensions as necessary to add individual SCN protocols if and when required.

4) In conjunction with the underlying network protocol (IP), provide the relevant functionality as defined by the appropriate SCN lower layer.

Relevant functionality may include (according to the protocol being transported):

- flow control
- in sequence delivery of signaling messages within a control stream
- logical identification of the entities on which the signaling messages originate or terminate
- logical identification of the physical interface controlled by the signaling message
- error detection
- recovery from failure of components in the transit path
- retransmission and other error correcting methods
- detection of unavailability of peer entities.

For example:

- if the native SCN protocol is ISUP or SCCP, the relevant functionality provided by MTP2/3 shall be provided.
- if the native SCN protocol is TCAP, the relevant functionality provided by SCCP connectionless classes and MTP 2/3 shall be supported.
- if the native SCN protocol is Q.931, the relevant functionality provided by Q.921 shall be supported.
- if the native SCN protocol is MTP3, the relevant functionality of MTP2 shall be supported.

5) Support the ability to multiplex several higher layer SCN sessions on one underlying signaling transport session. This allows, for example, several DSS1 D-Channel sessions to be carried in one signaling transport session.

In general, in-sequence delivery is required for signaling messages within a single control stream, but is not necessarily required for messages that belong to different control streams. The protocol should if possible take advantage of this property to avoid blocking delivery of messages in one control stream due to sequence error within another control stream. The protocol should also allow the SG to send different control streams to different destination ports if desired.

6) Be able to transport complete messages of greater length than the underlying SCN segmentation/reassembly limitations. For example, signaling transport should not be constrained by the length limitations defined for SS7 lower layer protocol (e.g. 272 bytes in the case of narrowband SS7) but should be capable of carrying longer messages without requiring segmentation.

7) Allow for a range of suitably robust security schemes to protect signaling information being carried across networks. For example, signaling transport shall be able to operate over proxyable sessions, and be able to be transported through firewalls.

8) Provide for congestion avoidance on the Internet, by supporting appropriate controls on signaling traffic generation (including signaling generated in SCN) and reaction to network congestion.

4.2 Performance of SCN Signaling Protocols

This section provides basic values regarding performance requirements of key SCN protocols to be transported. Currently only message-based SCN protocols are considered. Failure to meet these requirements is likely to result in adverse and undesirable signaling and call behavior.

4.2.1 SS7 MTP requirements

The performance requirements below have been specified for transport of MTP Level 3 network management messages. The requirements given here are only applicable if all MTP Level 3 messages are to be transported over the IP network.

- Message Delay
  - MTP Level 3 peer-to-peer procedures require response within 500 to 1200 ms. This value includes round trip time and processing at the remote end.
    Failure to meet this limitation will result in the initiation of error procedures for specific timers, e.g., timer T4 of ITU-T

Recommendation Q.704.

4.2.2 SS7 MTP Level 3 requirements

The performance requirements below have been specified for transport of MTP Level 3 user part messages as part of ITU-T SS7 Recommendations [SS7].

- Message Loss
  - no more than 1 in 10E+7 messages will be lost due to transport failure

- Sequence Error
  - no more than 1 in 10E+10 messages will be delivered out-of-sequence (including duplicated messages) due to transport failure

- Message Errors
  - no more than 1 in 10E+10 messages will contain an error that is undetected by the transport protocol (requirement is 10E+9 for ANSI specifications)

- Availability
  - availability of any signaling route set is 99.9998% or better, i.e., downtime 10 min/year or less. A signaling route set is the complete set of allowed signaling paths from a given signaling point towards a specific destination.

- Message length (payload accepted from SS7 user parts)
  - 272 bytes for narrowband SS7, 4091 bytes for broadband SS7

4.2.3 SS7 User Part Requirements

More detailed analysis of SS7 User Part Requirements can be found in [Lin].

ISUP Message Delay - Protocol Timer Requirements

- one example of ISUP timer requirements is the Continuity Test procedure, which requires that a tone generated at the sending end be returned from the receiving end within 2 seconds of sending an IAM indicating continuity test. This implies that one way signaling message transport, plus accompanying nodal functions need to be accomplished within 2 seconds.

ISUP Message Delay - End-to-End Requirements

- the requirement for end-to-end call setup delay in ISUP is that an end-to-end response message be received within 20-30 seconds of the sending of the IAM. Note: while this is the protocol guard timer value, users will generally expect faster response time.

TCAP Requirements - Delay Requirements

- TCAP does not itself define a set of delay requirements. Some work has been done [Lin2] to identify application-based delay requirements for TCAP applications.

4.2.4 ISDN Signaling Requirements

Q.931 Message Delay

- round-trip delay should not exceed 4 seconds.
  A timer of this length is used for a number of procedures, esp. RELEASE/RELEASE COMPLETE and CONNECT/CONNECT ACK where excessive delay may result in management action on the channel, or release of a call being set up. Note: while this value is indicated by protocol timer specifications, faster response time is normally expected by the user.

- 12 sec. timer (T309) is used to maintain an active call in case of loss of the data link, pending re-establishment. The related ETSI documents specify a maximum value of 4 seconds while ANSI specifications [T1.607] default to 90 seconds.

5. Management

Operations, Administration & Management (OA&M) of IP networks or SCN networks is outside the scope of SIGTRAN. Examples of OA&M include legacy telephony management systems or IETF SNMP managers. OA&M implementors and users should be aware of the functional interactions of the SG, MGC and MG and the physical units they occupy.

6. Security

6.1 Security requirements

When SCN related signaling is transported over an IP network two possible network scenarios can be distinguished:

- Signaling transported only within an Intranet;
  Security measures are applied at the discretion of the network owner.

- Signaling transported, at least to some extent, in the public Internet;
  The public Internet should be regarded generally as an "insecure" network and usage of security measures is required.

Generally security comprises several aspects

- Authentication:
  It is required to ensure that the information is sent to/from a known and trusted partner.

- Integrity:
  It is required to ensure that the information hasn't been modified while in transit.

- Confidentiality:
  It might be sometimes required to ensure that the transported information is encrypted to avoid illegal use.

- Availability:
  It is required that the communicating endpoints remain in service for authorized use even if under attack.

6.2 Security mechanisms currently available in IP networks

Several security mechanisms are currently available for use in IP networks.

- IPSEC ([RFC2401]):
  IPSEC provides security services at the IP layer that address the above mentioned requirements. It defines the two protocols AH and ESP respectively that
  essentially provide data integrity and data
  confidentiality services.

  The ESP mechanism can be used in two different modes:
  - Transport mode;
  - Tunnel mode.

  In Transport mode IPSEC protects the higher layer protocol data portion of an IP packet, while in Tunnel mode a complete IP packet is encapsulated in a secure IP tunnel.

  If the SIG embeds any IP addresses outside of the SA/DA in the IP header, passage through a NAT function will cause problems. The same is true for using IPsec in general, unless an IPsec ready RSIP function is used as described in draft-ietf-nat-terminology-02.txt.

  The use of IPSEC does not hamper the use of TCP or UDP as the underlying basis of SIG. If automated distribution of keys is required the IKE protocol (RFC[2409]) can be applied.

- SSL, TLS ([RFC2246]):
  SSL and TLS also provide appropriate security services but operate on

top of TCP/IP only.

It is not required to define new security mechanisms in SIG, as the use of currently available mechanisms is sufficient to provide the necessary security. It is recommended that IPSEC or some equivalent method be used, especially when transporting SCN signaling over public Internet.

7. Abbreviations

CAS	Channel-Associated Signaling
DSS1	Digital Subscriber Signaling
INAP	Intelligent Network Application Part
ISEP	IP Signaling End Point
ISUP	Signaling System 7 ISDN User Part
MAP	Mobile Application Part
MG	Media Gateway
MGU	Media Gateway Unit
MGC	Media Gateway Controller
MGCU	Media Gateway Controller Unit
MTP	Signaling System 7 Message Transfer Part
PLMN	Public Land Mobile Network
PSTN	Public Switched Telephone Network
S7AP	SS7 Application Part
S7UP	SS7 User Part
SCCP	SS7 Signaling Connection Control Part
SCN	Switched Circuit Network
SEP	Signaling End Point
SG	Signaling Gateway
SIG	Signaling Transport
SS7	Signaling System No. 7
TCAP	Signaling System 7 Transaction Capabilities Part

8. Acknowledgements

The authors would like to thank K. Chong, I. Elliott, Ian Spiers, Al Varney, Goutam Shaw, C. Huitema, Mike McGrew and Greg Sidebottom for their valuable comments and suggestions.

9. References

[NAT] IP Network Address Translator (NAT) Terminology and Considerations <draft-ietf-nat-terminology-02.txt>, P. Srisuresh and M. Holdrege, April 1999, work in progress.

[PSS1/QSIG] ECMA Standard ECMA-143 -Inter-Exchange Signalling Procedures and Protocol (QSIG-BC)

[Q.931/DSS1] ITU-T Recommendation Q.931, ISDN user-network interface layer 3 specification (5/98)

[SS7] ITU-T Recommendations Q.700-775, Signalling System No. 7

[SS7 MTP] ITU-T Recommendations Q.701-6, Message Transfer Part of SS7

[T1.607] ANSI T1.607-1998, Digital Subscriber Signaling System Number 1 (DSS1) - Layer 3 Signaling Specification for Circuit-Switched Bearer Services

[Lin] Performance Requirements for Signaling in Internet Telephony, <draft-seth-sigtran-req-00.txt>, H. Lin, T. Seth, et al, work in progress.

[Lin2] Performance Requirements for TCAP Signaling in Internet Telephony, <draft-ietf-sigtran-tcap-perf-req-00.txt>, H. Lin, et al, work in progress.

Authors' Contact Information

Lyndon Ong
Nortel Networks
4401 Great America Parkway
Santa Clara, CA 95054, USA
long@nortelnetworks.com

Ian Rytina
Ericsson Australia
37/360 Elizabeth Street
Melbourne, Victoria 3000, Australia
ian.rytina@ericsson.com

Matt Holdrege
Ascend Communications
1701 Harbor Bay Parkway
Alameda, CA 94502 USA
matt@ascend.com

Lode Coene
Siemens Atea
Atealaan 34
Herentals, Belgium
lode.coene@ntnet.atea.be

Miguel-Angel Garcia
Ericsson Espana
Retama 7
28005 Madrid, Spain
Miguel.A.Garcia@ericsson.com

Chip Sharp
Cisco Systems
7025 Kit Creek Road
Res Triangle Pk, NC 27709, USA
chsharp@cisco.com

Imre Juhasz
Telia
Sweden
imre.i.juhasz@telia.se

Haui-an Paul Lin
Telcordia Technologies
Piscataway, NJ, USA
hlin@research.telcordia.com

HannsJuergen Schwarzbauer
SIEMENS AG
Hofmannstr. 51
81359 Munich, Germany
HannsJuergen.Schwarzbauer@icn.siemens.de