INTERNET-DRAFT   L. Coene
Internet Engineering Task Force   Siemens
Issued: 30 june 2000   J. Loughney
Expires: 31 December 2000   Nokia
                                                      I. Rytina
                                                       Ericsson
                                                         L. Ong
                                                Nortel Networks

Signalling Transport over SCTP applicability statement
<draft-ietf-sigtran-signalling-over-sctp-applic-00.txt>

Status of this Memo

Abstract

   This document describes the applicability of the Stream Control
   Transmission Protocol for transport of signalling information over IP
   infrastructure. A few signalling application are descibed such as
   signalling System Nr7(SS7), Digital Subsciber Service 1/2
   (DSS1/2).... Specific info on signalling transport over
   IP(addressing, routing) is also provided. The use and specification
   of each of the adaptation layers for signalling transport in
   conjunction with SCTP is described.

TTTTaaaabbbbllllleeee ooooffff
CCCCoooonnnnttttteeeeennnnnttttssss

1 INTRODUCTION

     This applicability statement document covers subject terminology
and makes a overview of the solutions for transporting SS7, ISDN user or
any other form of signalling information over Internet Protocol infras-
tructure. This includes also a overview of the available Internet and
SS7 addressing. It tries to explain what the meaning is of the different
addressing modes in the internet and Signaling System Nr. 7 and where
their added value resides. Some example scenario's are provided as exam-
ple of how applications in the SS7 and/or internet may be able to reach
each other.

1.1 Terminology

     The following functions are commonly identified in related work:

     Signal Transfer Point (STP): This is a node in an SS7 network that
     routes signalling messages based on their destination address in
     the SS7 network

     Signal Relay Point (SRP): This is a node in an SS7 network that
     routes signalling messages based on their called party address in
     the SS7 network. (Translates Called party address to a destination
     pointcode and also translates Calling prty address when needed)

     Stream Control Transmission Protocol(SCTP): A transport protocol
     designed for the reliable transport of signalling information over
     a connectionless network(example: the Internet)

     Called Party Address(CLD): Address of the party the message wants

to reach.(Party can be a node, person, network..., a entity in general)(=Destination address)

Calling Party Address(CLG): Address of the party from which the message originated.(Originating address)

Global Title:(GT) A globally unique identifier used in the CLD and/or CLG for identifying a entity. A global title can consist of a pointcode, translation type, nature of address, numbering plan and the title itself(=digits).

Pointcode(PC) The Pointcode in SS7 and IP have the same meaning, but not necessary the same size and interpretation. A pointcode identifies a node within a particular network.

Routing Indicator: The routing indicator tells the SCCP routing function which part of the address has to use for routing the message(SSN + global title or SSN + pointcode).

Translation Type Number(TTN): The translation type number indicates the translation type of the address.

Numbering Plan(NP): This indicates the numbering plan to which the digits belong: that can be E164, E212, private numbering plans, Internet Numbering Plan, ...

Nature-Of-address(NA): The nature of address indicates whether a address is for national, international or other use.

Encoding Scheme(ES): The encoding scheme indicates how the digits are encoded. Encoding is normally in Binary Coded decimal(BCD) for-mat.

SubSystem Number(SSN) The SSN indicates the application entity that must be reached in the final destination node of the msg

Global Titel Format(GTI): Indicates which of the above mentioned parameters are actually present in the party address. If some parameters are not present in the address then default parameters are used for executing the Global Title Translation.

Portnumber: Indicates on the tranport level in IP which applica-tion needs to be reached in the layer above.

Subsystem number(SSN): Indicates on the networklayer in SS7 which application needs to be reached in the application layer.

Subnet: a subnet is a collections of nodes, belonging to the same

operator/ISP or collective of operators/ISP's. This may be
equivalent with a Internet domain. A MTP net is always a subnet.
Subnet may be owned by more than one operator(example MTP NAT0 sub-
net in the US)

Transport Address: An IP address and a port number pair which
identifies a SCTP association.

2 Signalling tranport using the Stream Control Transmission Protocol (SCTP)

2.1 INTRODUCTION

The Stream Control Transmission Protocol(SCTP) provides a high relial-
able, redundant transport between 2 endpoints. It also makes sure that
it will back off in case of congestion on the internet it is running on.
The interface between SCTP and its signalling applications is handled
via adaptation layers which provide a intermediation layer so that the
upper layer signalling protocols of a certain protocol stack architec-
ture does not have to change their interface towards the transport
medium and internal functionality when they start using SCTP instead of
a other transport protocol. Another issue is that the supported protocol
stack architecture will conform to the internet architecture as
described in [RFCblabla] without compromising its own rules.

For more information of how to use SCTP see [RFCSCTPA].

2.2 Adaptation layers for SCTP

Adaptation layers are used for transporting protocols without having to
change the interfaces between the tranported protocol and SCTP. SCTP is
a stream based protocol while some application of SCTP are message based
protocols. Without a adaptation layer, the transported protocol would
have to change in protocol structure or its underlaying interface or
some intermediate layer would be necessary.

It is the task of the adaptation layer to present the view towards its
application protocol as if it was the original protocol or protocol
stack that it is substituting for. therefore a adaptation layer is more
aptly called a Foo User adaptation layer, with foo the protocol is sub-
stituted for.

2.2.1 How to define and Use adaptation layers

Many different signaling applications may use SCTP for different pur-
poses. They go from replacing MPT functionality till replacing SCCP

signalling information transport.

The basic architecture is as in Figure 1 :

```
          User/Application level Protocols
                 |    |    |
        +-----------------------------------+
        |         User Adaptation modules   |
        +-----------------------------------+
                        |
        +-----------------------------------+
        |Stream Control Transmission protocol|
        +-----------------------------------+
                        |
        +-----------------------------------+
        |         Standard IP Transport     |
        +-----------------------------------+
                        |
                Network Layer (IP)
```
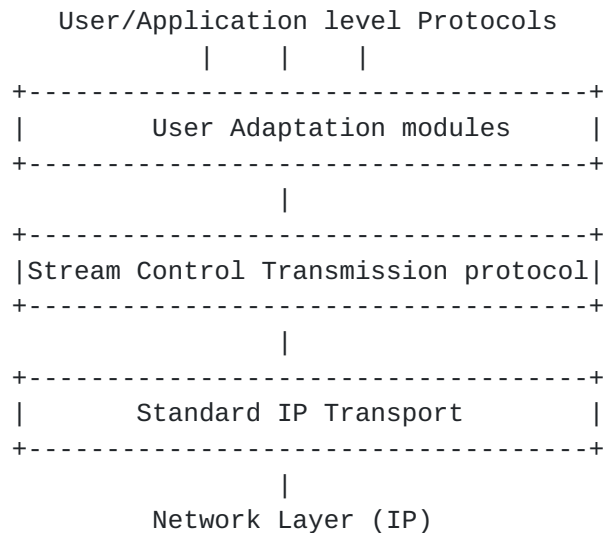

        Figure 2.4.1: Transport Components

The three components of the transport protocol are :

(1) Adaptation modules that support specific primitives, e.g. manage-
     ment indications, required by a particular user/ application proto-
     col.

(2) the Stream Control Transmission Protocol itself that supports a
     common set of reliable transport functions.

(3) a standard IP transport/network protocol provided by the operating
     system. In some network scenarios, it has been recognised that TCP
     can provide limited (but sufficient) reliable transport functional-
     ity for some applications, and this is discussed later in this
     document.

     Each of the interfaces described above may be implementation depen-
     dant. They are in general not specified by the protocol documents.

2.2.2 **Adapation layers for signalling transport**

Currently, there are four adaptation layers, to support carrying of SS7 application protocols over IP. These adaptation layers are being developed for different purposes, and there is no assumption that they should interwork - i.e. - M2UA carries M3UA. They should be thought of as individual protocols for specific uses.

Adataption layers can have a peer-to-peer or master-slave relationship. The master-slave relationship is mostly envisioned for very simple net-works while the peer-to-peer case is more for fullfledged signalling networks(akind to the present SS7 network worldwide).

2.2.2.1 IUA

There is a need for Switched Circuit Network (SCN) signaling protocol delivery from an ISDN Signaling Gateway (SG) to a Media Gateway Con-troller (MGC). The delivery mechanism should meet the following cri-teria

* Support for transport of the Q.921 / Q.931 boundary primitives

* Support for communication between Layer Management modules on SG and MGC

* Support for management of active associations between SG and MGC

This draft supports both ISDN Primary Rate Access (PRA) as well as Basic Rate Access (BRA) including the support for both point-to-point mode and point-to-multipoint modes of communication. QSIG adaptation layer requirements do not differ from Q.931 adaptation layer, hence the pro-cedures described in this draft are also applicable to QSIG adaptation layer.

2.2.2.2 M2UA

There is a need for SCN signaling protocol delivery from an Signaling Gateway (SG) to a Media Gateway Controller (MGC) or IP Signaling Point (IPSP). The delivery mechanism should meet the following criteria:

* Support for MTP Level 2 / MTP Level 3 interface boundary

* Support for communication between Layer Management modules on SG and MGC

* Support for management of active associations between the SG and MGC

In other words, the Signaling Gateway will transport MTP Level 3 messages to a Media Gateway Controller (MGC) or IP Signaling Point (IPSP). In the case of delivery from an SG to an IPSP, the SG and IPSP function as traditional SS7 nodes using the IP network as a new type of SS7 link. This allows for full MTP Level 3 message handling and network management capabilities.

2.2.2.3 M3UA

There is a need for SCN signaling protocol delivery from an SS7 Signaling Gateway (SG) to a Media Gateway Controller (MGC) or IP-resident Database as described in the Framework Architecture for Signalling Transport [11]. The delivery mechanism should meet the following criteria:

* Support for transfer of all SS7 MTP3-User Part messages (e.g., ISUP, SCCP, TUP, etc.)

* Support for the seamless operation of MTP3-User protocol peers

* Support for the management of SCTP transport associations and traffic between an SG and one or more MGCs or IP-resident Databases

* Support for MGC or IP-resident Database failover and loadsharing

* Support for the asynchronous reporting of status changes to management

In simplistic terms, the SG will terminate SS7 MTP2 and MTP3 protocols and deliver ISUP, SCCP and/or any other MTP3-User protocol messages over SCTP transport associations to MTP3-User peers in MGCs or IP-resident Databases.

2.2.2.4 SUA

This document details the delivery of SCCP-user messages (MAP & CAP over TCAP, RANAP, etc.) over IP, from an SS7 Signaling Gateway (SG) to an IP-based signaling node (such as an IP-resident Database) as described in the Framework Architecture for Signaling Transport [11]. The delivery mechanism SHOULD meet the following criteria:

* Support for transfer of SS7 SCCP-User Part messages (e.g., TCAP, RANAP, etc.)

* Support for SCCP connectionless service.

* Support for SCCP connection oriented service.

* Support for the seamless operation of SCCP-User protocol peers

* Support for the management of SCTP transport associations between an SG and one or more IP-based signaling nodes).

* Support for distributed IP-based signaling nodes.

* Support for the asynchronous reporting of status changes to management

2.2.3 **General issues for transporting signalling info over SCTP**

2.3.4 **SCTP Multihoming**

Redundant communication between 2 SCTP endpoints is achieved by using multihoming where the endpoint is able to send/receive over more than one IP transport address.

Under the assumption that every IP transport address will have a dif-ferent path towards the remote endpoint, (this is the responsability of the routing protocols(3.2.4) or of manual configuration), if the tran-sport to one of the IP address/port (= 1 particular path) fails then the traffic can migrate to the other remaining IP address/ports(= other paths).

2.2.5 **Routing protocols**

In order to provide redundant paths for a certain SCTP association throughout the network, Routing protocols must support multihoming and the endnodes must have at LEAST one transport address(that is have more than 1 interface with a IP address).

It is advisable to let the originator choose from which source addresss it can send the datagram towards the destination because the paths are based on source, destination pair and letting the network layer choose, would probably always yield a alternating selection of the source and

thus of the interface.

Do not forget that congestion control is an a per destination basis, which is not completely the same as congestion control on a path basis if the source PC cannot be explicitly stated form a datagram.

2.3.11 Congestion control & avoidance

A general overview of congestion control and avoidance can be found in the SCTP applicability statement[RFCSCTPA].

However some particular restrictions migth be observed when using SCTP for transporting signalling info over IP infrastructure. This restric-tions must be aplied with care as in most cases, the SCTP association is never in complete full control of the links between the 2 nodes exchang-ing the signalling info. See paragraph 2.3.12, use of QOS methods.

This restrictions are mostly based on restriction found in the origianl protocol, the adaptation layer is replacing. (Example: boundaries on message transmission time, retransmission timers and so on). Sometimes the restriction has a direct impact on some of SCTP protocol variables which might to be tunable for tranporting signalling traffic.

2.3.12 Use of QOS methods

SCTP is a end-to-end protocol which cannot guarantee the quality-of-service along the complete path taken by the messages of that particular association. It only guarantees that a message will be deliverred wintin a certain timeframe or otherwise be lost. If more guarantees are required(example: on the timeframe, message loss...) for improving the relialability of the transport, some form of QOS mechanism may be needed.

(1) Overprovisioning
      Overprovisioning of the links so that the total traffic running
     over over the link never excedes the link capacity. In practice,
     this may be difficult to ensure reliably. If the same performance
     as MTP is required(regarding msg delays and msg delivery), then it
     is advisable to assign at most a single SCTP association to a IP
     link. This would also mean that the 2 endpoints would be directly
     interconnected. A router may be present but should carry only the
     traffic of those SCTP associations between the 2 nodes. Any router
     that might be present and carries unrelated traffic would interfer

with the SCTP association esspecially in high load condition. Due the backoff of SCTP in high load conditions, that would mean that for example 2 associations would get each about the 50% of the link bandwith or router capacity if both where trying to run at the highest transmission rate possible(without packet loss).

If another transport protocol which does not behave as SCTP and/or TCP would be running on the same link, or through the same router as the signalling traffic, then the signalling traffic may be pushed aside by the more aggressive transport protocol.

The general rule is that if the associations try to obtain maximum throughput accross a single link in absence of any other traffic, they will over a long time divide the bandwith up in equal spaces(example 4 users => bandwith of 1 user = Total linkbandwith / 4)

If agressive transport protocols are used, then the SCTP assocaition will be pushed to use minimal bandwith(mathematical speaking : bandwith use of SCTP will go to 0)

(2) Specific intranet Use of a private network solely for signalling transport purposes. Private networks may allow better control and monitoring of resources available.

(3) Differentiated services: by providing a certain codepoint in the Type-of-service field (TOS), certain Differential services can be selected. Setting the code point for signaling transport requires some thought. It is good practice to give the signaling transport a higher priority than the traffic for which the signaling is being made.

(4) Integrated services By use of integrated services [RSVP reference needed], resources are reserved for signaling transport. If resources are unavailable for to initiate a new signaling transport, that request will be denied. In practice, RSVP may turn out not to scale very well for large number of signalling links and this solution may prove to be unfeasable.

2.3.13 Multiple associations.

The association may be spread out acrossn the IPv4 and IPv6 domain. /* editors note: Multiple associations: see in the MDTP drafts en SCTP drafts got lost in transit */

2.3.14 Efficiency

2.2.15 Bundeling

Bundling can be done on SCTP and/or on user adapatation layer. In case of the adapatation layer it has to specified by the adaptation protocol.

2.2.16 Portnumbers

The SG acts as a server and listen on the wellknown port of the adaptation layers that the SG supports. The clients can indicate to the SG to use different portnumbers. (dynamical portnumber assigment) The subsequent communication is then exchange via those portnumbers. If 2 servers try to connect, then the adaptation layer management should resolve to client-server model.

2.2.17 Sequenced / non-sequenced delivery

SCTP can deliver messages in sequence or not in sequence. Most signalling adaptation layers expect SCTP to deliver the msg in sequence. However not all SS7 applications (= applications located above the adaptation layer) do need sequenced delivery.

2.2.18 Stream usage

The application can choose on which stream he can send it data. Some application level protocols may standardize stream number usage convention, which, for instance, allows to send jpeg and gif portions of a page through certain stream while text through others, so as to avoid large graphics from blocking text content. This is not a must.

User adaptation layers data msg and adaptation layer management msg may be transported over different streams. The order of the management msg should be kept. Sequence is important. Management msg Should be on stream 0. It is alllowed for some management msg to use unordered , non-stream 0 streams. This should be specified by the management part of the user adaptation layer.

2.2.19 Network apperance Identifier

A similar id to the protocol id (see SCTP applicability statement[RFCSCTPAS]) is also contained in the adaptation layers, but it has not the same meaning. It is called the network apperance(akin to the network idnetifier in SS7: NAT0, NAT1...). It is a administrable number to be determined between or within the network operator. The network

apperance identifies a set of pointcodes. SG and Host can be present in
in different network apperances at the same time. Communication should
be done between nodes of the same network apperances(thus having the
same network apperance value).

3 **SPECIFIC ISSUES OF SIGNALLING ADAPTATION LAYERS**

3.1 **MTP lvl3 User Adaptation layers(M3UA)**

3.1.1 **Routing in M3UA**

a strict assignment must be made in the SG to reach the correct Applica-
tion Server(AS) (Example ISUP CICs and trunkgroups must match). The
Application Server Process being part of the AS must have common state
sharing between the ASPs. Each ASP of the same
 AS can be a different Application node(AN). Each application is a
 physical box or host. How the state is shared, is an internal
 implementation issue.

3.1.2 **M3UA heartbeats**

If a M3UA nodes fails,then this must be detected via the use of heart-
beats msg between the M3UA peers. The SCTP heartbeat is not sufficient
because it only determines if a path for the SCTP association exists,
not if M3UA is ready to process msg.

The transmission rate of sending keepalive msg should be engineerable
and the possible loss of keepalive msg could be used for the monitoring
and measurements of the concerned M3UA nodes.

3.2 **MTP lvl2 User Adaptation layer(M2UA)**

3.2.1 **Link and application redudancy**

Link reduncancy is accomplished via multihoming in SCTP itself. You have
multiple links towards your DPC. Application redundancy is handled in
the user adapatation layers via switching over from one association to
another association.

3.3 **ISDN User Adaptation layer(IUA)**

/* editors note: work in progress */

2 Addressing and signalling over IP infrastructure

One of the basic problems in any network is to get from point A to point **B**. **Another problem is how to chosse between different point B. The first** problem is solved via SCTP associations(you put the msg in SCTP at one end, and voila, it pos out at the other end). The second problem is solved via addressing. Some signalling is point-to-point, meaning that it simply needs a SCTP association to get to the other side(UIA, M2UA is a case in point). Other Signalling needs to route based on its address- ing contained in the message(M3UA, SUA).

2.1 Internet addressing

Every layer needs to determine the service to which it wants to deliver its information. The way in which this is done depends from layer to layer. The transport protocols above the IP network protocol are indi- cated in the protocol extension headers field contained at the end of the IP header. Every protocol has its own standardized protocol number.

The transport layer determines the application to which it wants to deliver the information by the portnumber.

The tuple destination address and portnumber uniqely identifies a appli- cation in the internet. Further selectors may be used in higher layers to obtain the desired application. The IP address itself is a pointcode. The following types of pointcode may de distinguished :

  - Unicast address: a unicast address designates a single node
  within a IP network. It can have some hierarchy in it or not. The
  address may be globally unique or be a private pointcode.

  - Multicast address: the message is send to all nodes
  belonging/attached to that multicast address/group.(Similar prin-
  ciple as with SCCP broadcast but different implementation)

  - Link-local address: these are addresses assigned to the link(wow
  local "private").

  - Site-local address: these are addresses assigned to a site(wow
  local, "private")

  - ...

As the meaning of the pointcodes is only known to IP and it has a rela-
tion to the link and its interface to the link, layers which only know
about destinations(such as SCCP), SHOULD NOT/MUST NOT try to to inter-
prete the IP address.

The IP pointcode does not strictly identify the node in the network but
rather the interface to the IP network layer. Thus IP nodes can have
more than 1 Pointcode(and those PC can be used for having 2 links
between 2 adjacend nodes, a feature that is called multihoming).

2.2 SS7 addressing

SS7 was develop in stages: ISUP and MTP were first developped. The deci-
sion to route was done by the application in a similar way as the
MFC/... signalling determined the trunk to the next exchange. ISUP had
to determine for a certain E164 number a DPC(= the pointcode of the
adjacend exchange) and then the msg was routed to the office where the
same procedure was done over all again.(=link-by- link routing)

(1) MTP addres: MTP routing label consists of a Network indicator(also
     called A MTP-SAP=service acces point) , a destination
     Pointcode(=DPC) and a origination Pointcode(OPC). The MTP-SAP indi-
     cates for which network the pointcode in the routing label is
     valid. If the routing table has been engineerd in a node for that
     network, the message can reach that destination. The size of a
     pointcode is fixed within a single network. Different networks can
     have different sizes of pointcodes:

          - ITU 14 bit

          - China 24 bit

          - ANSI 24 bit

          - Others.....

     A MTP pointcode is private to its own network. The global unique-
     ness is NEVER assured by the MTP pointcode but by global titles(as
     used in SCCP and in ISUP).

     The representation of pointcodes can be diverse: decimal, 3-4-3-4
     format, 8-8-8 format .... It is allowed to structure the
     pointcode(akind to CIDR and its prefixes in IP).

     MTP uses static routing: no routing protocols like RIP, OSPF or BGP
     are used for finding out routes between nodes in a MTP network.

However it is allowed to use dynamic routing in a MTP net. The ITU marked this as "For Further study", but they never got around to it.

(2) SCCP adress :   The SCCP address is a variable length address build as a collection of optional elements. It identifies destinations and has no notion about routes to those destinations. That is left to the underlying network layer(MTP or IP). A destination can be a network, node ,application entity, a person... Routing is static. The SCCP address is generally refered to as a Global title. The global title must be globally unique(at least on a world scale) as this allows the A-party to reach the B-party End-to-End without setting up a connection through the network. It can also be used for Link-by-link routing.

The function responsible for deriving a pointcode from a global title is (not surprisingly) called the global title translation function(GTT). The GTT is a local function which bases it transla- tion and routing decision on the local situation(translation rule, loadsharing of destinations, route to backup node...) It has no topological knowledge of the network(something MTP and certainly IP have). The GTT function can therefore not only be used by msg with SCCP address but also by Q931 or other signaling messages for find- ing out to which destination the message must be sent.

The elements of the Global Title consists of the following:

    - MTP pointcode AND Network indicator(=MTP-SAP). The network indicator indicates to which network the msg belongs.

    - Subsystem Number: indicates to which application the msg belongs.

    - Global title: a structure indicating a global identification of a node and/or application. A GT may occur in the SCCP Calling(=Originator address) and in the Called(Destination address) Party address.

If only a MTP pointcode, network indicator and SSN is present, then the message can only be routed within that particular MTP network. If a global title(meaning if translation type, nature of addres and/or Digits) is present (accompanied possibly by a MTP pointcode, network indicator and SSN), then the msg can be routed across mul- tiple MTP networks, provided the networks are interconnected and the destination is reachable.

(3)   Global Title and Global Title Translations:

A global title contains the following elements. They are nearly all optional, the occurrence of the field in the SCCP message itself is governed by the global title format field(GTI) in the message.

-Translation Type(TTN): should indicate what sort of translation is needed. The most used TTN is the UNKNOWN. In the US some of the TTN have been used to address the application(instead of the SSN), thus doubling as application entity selectors. The Translation Type Number has no counterpart in IP.

- Numbering plan(NP): this contains the numbering plan indication to which the rest of the address conforms. This may be the E164, E212, E211, private numbering plans, ... The Numbering plan indication has no explicit counterpart in IP. It is implicitly included in the IPv4 address and partly explicitly included in the IPv6(example : E164 numbers included in OSI-NSAP address in IPv6)

- Nature-of-address(NA): this indicates the national or international use of the address. The Nature-of-Address has no counterpart in IP. This could be interpreted as scope indication of the address, something that is explicitly present in Ipv6 pointcodes(Link local, site local...).

- Encoding scheme(ES): this is a implicit parameter used to indicate the format of the global title digits(BCD even or BCD uneven). The Encoding scheme has no counterpart in IP.

- Global title digits: digits in the format specified by the encoding scheme. They contain the global identification of node(and possibly also of the application within that node.) Also the number of digits is included(as GT is a variable length address.

- Subsystem Number(SSN): indicates the application entity which should be reached . Some of the SSN are universally defined while others are not. Some are even double used. The SSN corresponds roughly to the portnumber of IP. However SSNs are derived at the network layer and go straight through to the application layer. Portnumbers only obtain their visibility from the transportlayer.

- Global title format: indicates which of the field mentioned above are explicitly contained in the called or calling party address of the message. Some formats indicates that some

fields(like NA and NP) are specified implicitly.

Global title have no explicit counterpart in IP. IP addresses are implicitly assumed to be Global (NAT not included). A GT could also be a name(such as in Directory Naming service (DNS)).

Also some routing information is included in the calling/called party address.

- routing Indicator: indicates to the node processing calling/called party address how to route the message on. The message can be routed on the Pointcode (and SSN: applicable only in the final end-node) or on global title(this requires a translation).The routing indicator has no counterpart in IP.

Depending on the routing indicator the message will be routed by SCCP. If route-on-SPC then MTP will do the routing. If route-on-GT then the SCCP global Title translation function will be invoked to determine the next(possible final or intermediate) node of the message. The address will be examined on the TTN,NP,NA and Digits and a translation will be done yielding a MTP pointcode + network indicator. A SSN may also be the additional outcome of the Global Title Translation(GTT). This MTP address is then used by MTP to route to the next destination(intermediate or final).

If required, the TTN, NP, NA, SSN and possible all the digits may be transformed into a TTN', NP' , NA' , SSN' and digits'. It will change the address (if the routing policy prescribes it) in a effort to reach the final destination. The only rule to which it has to adhere is that the change in addresses must be so that the return message(from the B-party) must reach the originator of the start msg(=A-party). This means that the message routing is NOT symmetric. Global title translation conforms to the notion of a Store-Compute-and-Forward network as opposed to a IP network which is a Store-and-Forward network. This translation is completely stateless(we are routing unitdata messages). The same function can also be invoked for connections(see SCCP connection-oriented) then the translation is done only once at the connection setup phase and SCCP connection oriented will then contain the state.

The translation rules for digits consist of:

- Deleting digits.

- Inserting digits

- Replacing digits

- Copying digits

That means that your called party address may have completely
changed once it went through the GTT and at the same time the cal-
ling party address must also be changed to adhere to the rule that
the backward message MUST be routable so that a end-to-end dialogue
may be send up between 2 nodes.

2.3 How to reach applications in SS7

Every layer needs to determine the service access point to which it
wants to deliver its information. The basic element in SS7 to determine
this is the Subsystem Number(SSN for short). the SSN can be found in MTP
and SCCP. The MTP has a SSN which indicates along others ISUP, SCCP
,..etc... The SSN in MTP are standardized on international level.
Locally defined SSN are allowed but may not be used outside that net-
work.

The SSN used in SCCP indicates directly to which application the message
must be send to. These SSN may be standardized but that is not a
prerequisite(see Q715). Some applications have standardized SSN, while
others use(and sometimes reuse) not standardized SSN. When messages go
from a net with SSN1 to a net with SSN2(SSN1 and SSN2 indicate the same
protocol) global title translation must be invoke to convert the SSN's.
This is one of the most basic and simplest use of Global Title transla-
tion in SS7.

2.3.1 General SS7-over-IP architecture.

Examples of usage for SS7-over-IP include:

- terminating call-related and non-callrelated signalling to a
Media gatway Controller(MGC). (PSTN to IP)

- Transparant transport of signalling information accross a
intranet or internet infrastructure between 2 intermediate SS7
nodes.(PSTN-IP-PSTN)

- Originating call-related and non-callrelated signalling from the
SS7-over-IP net to the PSTN.(IP to PSTN)

- SS7-over-IP to SS7-over-IP networks (IP-PSTN-IP or IP-IP).

The general architecture is decribed in [RFC2719].

3 **SS7 Signalling transport using SCTP**

SS7 messages are transported across IP using the Stream Control
Transmission Protocol(SCTP). SCTP provides a high relialable, redundant
transport between 2 SS7-over-IP nodes. A SS7-over IP node is a SCTP end-
point.

The interface with SS7 is message based. Therefore a adaptationlayer is
needed to prevent changes to the upper layer SS7 protocols.

Within a asociation between 2 endpoint, 1 or more stream(s) may be avi-
alable. These streams are not directly visible to the adaptation layers.

The linkset towards a certain destination is the collection of all the
links which can send trfaffic to that destination, even with a inter-
mediate node in between(so different path towards that destination
exsist). The MTP linkset is thus equivalent to the SCTP association. The
streams within SCTP may be regarded as the links. A advantage of SCTP
streams is, when one of the multihomed paths fails, the stream will
migrate to one of the still open paths(Soft changeover). In SS7 when a
link fails, a a change over procedure has to be initiated towards a
still working link of the same linkset(=hard changeover)).

In a MTP based network, the capacity of the links is fixed at n times
64Kb (with n= 1,32,...). SCTP association do not have a fixed capacity
assigned to them. The bandwith used/provided by SCTP is dependant on
the rest of the traffic(other SCTP, TCP, RTP,UDP...) going through the
same links of the path followed by the SCTP association. See also the
SCTP applicability statement[17].

3.1 **MTP lvl 2 user adaptation layer(M2UA)**

The MTP lvl 2 user adaptation layer provides a emulation of a single MTP
link between 2 SS7 nodes.

3.2 **MTP lvl 3 User adaptation layer(M3UA)**

The MTP lvl 3 user adaptation layer provides a emulation of MTP lvl 3
towards its users. Its function is address translation and mapping,
stream mapping, congestion control and network management.

3.2.1 Address Mapping

The M3UA layer has to handle at least one or more SCTP associations. The selection of a SCTP association can be done by via a single part or multiple parts of the DPC, OPC, SLS, CIC fields of the MTP routing label. If a association were to fail then alternate mappings may be done (Implementation dependant).

3.2.2 Network Management

Management messages are exchanged between the M3UA peers for exchanging and updating the status of the SS7-over-IP nodes.

Influence of the IP routing protocols on M3UA routing and SCCP routing. Intradomain vs Interdomain

          - RIP

          - OSPF

          - BGMP

3.2.3 Network Maintenance

3.2.4 Multihoming within SCTP

Multihoming in SCTP is the process by where an SCTP endpoint has several transport addresses, which consist of an IP address and a UDP port pair, on which to send and receive on.

Multihoming provides redundant communication in SCTP by allowing communication between two endpoints to continue in the event of failure along a path between the endpoints.

Under the assumption that every IP address/UDP port will have a different path towards the remote endpoint, (this is the responsability of the routing protocols or of manual configuration), if the transport to one of the IP address/port (= 1 particular path) fails then the traffic can migrate to the other remaining IP address/ports(= other paths).

Multihoming could also be used for sharing the traffic load across the different paths. However as the througput of any of the paths is not known in advance and constantly changes due to the actions of other

associations and transport protocols along that particular path, this
would require very tight feedback of the paths to the loadsharing func-
tions of the adaptation layer.

3.2.5 Congestion control & avoidance

2 levels of congestion control/avoidance are present in a SS7-over-IP
net.

> - congestion control/avoidance within SCTP
>
> - Congestion control/avoidance present in the layers above the
> user adaptation layers(example: SCCP, ISUP ...)

For a more indepth description of congestion , see the SCTP applicabil-
ity statement[1].

SCTP conforms to the model of end-to-end congestion control located in
the transport leyer while ISUP and SCCP model themselves on a link and
destination based congestion control/overload mechanism located in the
network layer.

5.0 Routing of SS7 message in a IP net.

As the signalling is in fact transported over a "SS7" overlay network on
top of IP, both SS7 pointcodes and IP pointcodes are used. The basic
routing in the overlay network is done using SS7 pointcodes. However at
a certain point, that SS7 pointcode must be mapped to a IP pointcode
because (1) SCTP uses the IP pointcode(+portnumber) for selecting the
correct association and (2) IP routes only on IP pointcodes.

The way in way this mapping can be done, could be static or dynamic.
This is dependant on what adaptation layer is used and also on the sort

of network architecture(redundant servers, associations...).

/* editors note: work in progress */

5.1 **Routing using globally assigned IP addresses.**

/* editors note: This section might address a problem in SS7 of shor-
tage of pointcodes in certain SS7 nets, notably the international
(INAT0) SS7 network) */

IP addresses are required to be globally unique. If SS7 wants to tran-
sport its messages over a IP network, then they should be treated as
global addresses. This means that SS7 shall look at them as global
titles, it shall NOT rely on the specific handling of the addresses by
the underlying IP layer and below. This also means that SCCP is a prere-
quisite for transporting message over a IP infrastructure when non-call
related messages are to be transported over IP. ISUP and other signaling
protocols will have to the same for call related messages , translating
the addresses it has in the adaptation layers to IP addresses. They can
all invoke the GTT function if wanted.

The following cases may be envisioned:

> - E164,E212, (=telephone numbers) to IP address(depending on
> the underlying network Ipv4 or Ipv6) (equivalent to transla-
> tion MTP 14bit, 24bit ...)

> - IP address to IP address - IP address to MTP address

> - IP address to a form of a telephone address (=E164*) :
> needed if the message transit from a IP net to a IP net via a
> couple of MTP nets.

As some forms of IP addresses have a very limited scope(such as
link-local and site local), they should better not be used.

The following poitncodes can be used:

> - IPv4 unicast : Globally assigned - IPv4 multicast: Globaly
> assigned, very few avialable Note 1.

> - IPv6 unicast :

> - IPv6 multicast: Note 1

> - IPv6 anycast:

         - IPv6 link-local:

         - IPv6 site-local:

    Note 1: A word of care is advised when using multicast addresses.
    This is especially true if the routing indicator in SCCP is Route-
    on-GT. SCCP has no knowledge whether the translation yielded a uni-
    cast or multicast PC, so it cannot and it will not take action to
    relay or stop the message. The use of this form of address is
    dependant on the application in question.

    Note 2

    Implications of this are that GTT function could support IP
    pointcodes. The IP pointcode must be put in the digit block of the
    GT. The representation may be in BCD, the meaning of it should not.
    The length of a Ipv4 address(32bits) should then be 8 digits(always
    fixed). The length of a Ipv6 address(128bits) should be 32 digits.
    The GT number of digits in the SCCP header should allow for at
    least 32 digits(some extra digits may need to be inserted for
    proper routing). The result attached to a certain translation must
    be or a MTP PC(14,24) or a Ipv4 PC or a Ipv6 PC. The nature of
    address may be defined as indicating a international address with
    bitmap format. This could even lead to a new GTT operation (besides
    insert, copy, delete, replace) called bitmapPCCopy. The bit-
    mapPCcopy takes the IPvx poitncode out of the GT and uses it as the
    resulting pointcode of the GTT for further routing. The same effect
    can also be achieved via proper engineering of the GT database.

    Other possibilities include User adaptation layers which maps the
    MTP pointcode to IP pointcode or a mapping from MTP pointcode to a
    certain SCTP session.

    If GTT is used then IP must need a Numbering plan indicator(NP
    value normally assigned by SG11). This may or may not be agreed
    with SG11. This is not mandatory(but it is encouraged) as already
    there exists private numbering plans not known to SG11. As long as
    you make sure at the network border via GTT that the next network
    will be able to route the message NP , you can do pretty much any-
    thing. This is a bilateral agreement between operators/Internet
    Service providers) In general any value may be used as long as it
    is routable in your own subnet and that you or somebody else is
    able to route it further over its own net.

    Also maybe the portnumber may become part of the input/output to
    the GTT function.

(1) IPv4 Considerations

    When coding a Ipv4 address, the length of the address (32 bits)
    should then be 8 digits(always fixed). The GT number of digits in
    the SCCP header should allow for at least 32 digits (some extra
    digits may need to be inserted for proper routing). The result
    attached to a certain translation must be or a MTP PC(14,24) or a
    Ipv4 PC or a Ipv6 PC.

(2) IPv6 Considerations

    When coding a IPv6, the length of the address (128 bits) should be
    32 digits. The GT number of digits in the SCCP header should allow
    for at least 32 digits (some extra digits may need to be inserted
    for proper routing). The result attached to a certain translation
    must be or a MTP PC(14,24) or a Ipv4 PC or a Ipv6 PC.

(3) Routing SS7 messages and dynamic assigned adresses

    Problems may occur with dynamically assigned IP addresses. The node
    could obtain a IP address that is later reclaimed and/or replaced
    by another IP address out of a pool of IP addresses. The destina-
    tion address in the routing tables would have to be invalidated or
    changed. Therefore it is strongly recommended to use a fixed
    assigned IP address. Do not forget that the IP node which is work-
    ing in the SS7 net is supposed to be up all the time. It should not
    be regarded as a dial-up user(for which Dynamic assigned addresses
    are meant).

    Also, dynamically assigned address may invalidate security features
    of SCTP. If transport addresses may change during the lifetime of
    a SCTP association, it is impossible to reliably ensure that the
    current transport address is the transport address which was used
    in the setup of the association.

    If this practice should turn out to be unavoidable, then a Q3/SNMP
    Management msg would be required to be exchanged between DHCP and
    SCCP network element configuration part so that the pointcode
    attached to a certain GT must be updated, deleted or added. The
    same solution is also feasible for working in NAT's with dynamical
    assigned addresses.

(4) Routing SS7 message and Network address Translators.

    Network Address Translator(NAT) are boxes which map a private IP

net address to a globally assigned IP address. This happens because
there are many more users within the private IP net than there a
globally assigned IP addresses allocated to that private IP net.
That means that the mapping is ALWAYS dynamic. The mapping must be
both ways and via the same NAT and the NAT is always the final des-
tination. Also the association is based on state(thus breaking the
end-to-end principle). This amounts to crossing a network border.
It should be envisioned to use a static private address in the NAT.

It would be advisiable to termination the association from the pub-
lic network at the NAT, and have separate association(s) within the
private network. Then there is a clear network border at the cross-
ing between the NAT and that internet.

```
        Endpoint            Endpoint            Endpoint
         A(NAT)              B (NAT)                C
        +------+            +------+            +----+
        | ISEP |----------|  SG  |----------| SG |---
        +------+            +------+            +----+
            association 1  !  association 2 !
                           !                !
               NAT         !    internet    !  PSTN
                           !                !
```
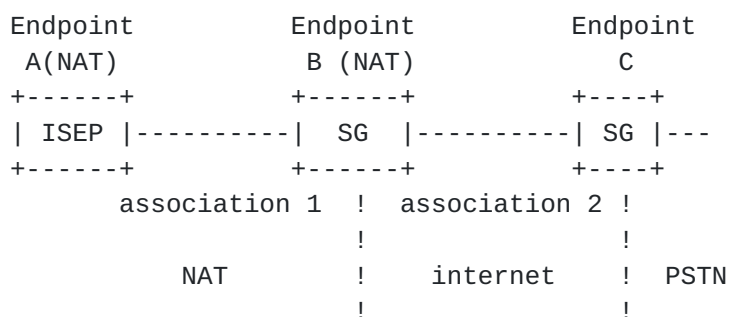
             Fig 5.x: use of SCTP associations with NAT's

Another solution is the use of name option for setting up the SCTP
association.

(5) Routing SS7 messages and routing protocols

The term routing protocols has a much broader sense in the Internet
than in the SS7 world. SS7 designates such protocols as Management
protocols(SCCP management, MTP management...) The scope of SS7
management protocols is much smaller. They only exchange informa-
tions of links in service and nodes in service(mostly only the own
links and the adjacend nodes) The topology of the network is NOT
exchanged between SS7 nodes. In general most nodes haven't got the
faintest idea how even the topology of its own subnet may look
like.(and they don't care).

The interaction between IP routing protocols and SS7 routing may
require some study especially in the case that routes start chang-
ing due to routing recomputation. The loadsharing and
primary/backup systems of GTT seems not to be impacted as it relies
on destinations and not on links. As long as a destination is
accessible/avialable in the IP net, then messages may be send to

it. If the destination is no longer avialable, then GTT must per-
form according to its own rules. Beware of changing conditions
being triggered by routing updates.

(6)   Routing SS7 messages and automatic renumbering

Automatic renumbering is the process of changing the IP addresses
of one or more nodes in a network so that the prefix of the address
(which is then common for all the changed nodes) allows to have a
routing table with a reduced number of entries. This renumbering is
mainly of interest in IPv6 networks.

If this happens, a similar solution(management request of the GT
tree) should be used to change the pointcode derived from GT.

6.0 Security

The following aspects of security are :

Authentication:

Information is sent/received from a known and/or trusted partner.
Until recently the number of interconnects of a SS7 node with
another SS7 node belonging to another operator was relativily lim-
ited and those other operators were implicitly known (and sometimes
trusted). Due to the increasing interconnect demands between dif-
ferent operators on a voluntary or mandatory basis, the trusted
relation does not longer exist. That mean that a operator will not
accept all SS7 msg send to him by another operator. This is done
using MTP and SCCP screening: depending on the inormation in the
different MTP fields(example OPC...) and/or SCCP fields(example
Calling party address, SSN...) a msg may be rejected or accepted
for transport across or termination into the network. In the worst
case it may try to screen up to the application level(example: the
user info in a IAM msg or in a TC INVOKE component, Application
Context name screening). See [16].

A SS7 gateway using screening does behave like a firewall.

Intergrity:

Information may not be modified while in transit. The integrity of
a msg in a public network is not guaranted. If it is transported

over a IP network the integrity may be guaranteed at 2 levels. (1)
the IP level using IPSEC: which is equivalent to providing
integrity on on SS7 link level basis. Keydistribution is at most
limited to the network of that operator. (2) End-To-End integrity
using TCAP: For further study in the ITU.

Confidentiality:

Confidentiality of the user data must be ensured. User data can
not be examined by unauthorized users.

Availability:

The communicating endpoint must remain in service in all circon-
stances. All SS7 nodes have to remain active for the 99.999% of the
time.

The description of the internet security architecture and the use of it
is described in [18].

10 References and related work

[SCTP] Stewart, R. R., Xie, Q., Morneault, K., Sharp, C. , ,
    Schwarzbauer, H. J., Taylor, T., Rytina, I., Kalla, M., Zhang, L.
    and Paxson, V."Stream Control Transmission Protocol", <draft-
    ietf-sigtran-sctp-09.txt>, April 2000. Work In Progress.

[Q1400] SG11, ITU-T Recommendation Q.1400, " architecture framework for
    the development of signaling and OA&M protocols using OSI concepts
    ",1993

[RFC2719] Ong, L., Rytina, I., Garcia, M., Schwarzbauer, H., Coene, L.,
    Lin, H., Juhasz, I., Holdrege, M., Sharp, C., "Framework Architec-
    ture for Signaling Transport", RFC2719, October 1999

[IANA] Internet Assigned Numbers Authority, http://www.iana.org/, April
    2000

[RFC814] Clark, D.D., "Names, addresses, ports and routes", RFC 0814,
     July 1982.

[M2UA] Morneault, K., Kalla, M., Sidebottom, G., Dantu, R., George, T.,
     "SS7 MTP2-User Adaptation Layer (M2UA)", <draft-ietf-sigtran-m2ua-
     02.txt> ,Work in progress

[M3UA] Sidebottom,G., Ong, L., Mousseau, G., Rytina, I., Schwarzbauer,
     HJ., Morneault, K., Kalla, M., "SS7 MTP3-User Adaptation Layer
     (M3UA)", <draft-ietf-sigtran-m3ua-02.txt> ,Work in progress

[IUA] Kalla, M., Rengasami, S., Morneault, K., Sidebottom, G. "ISDN
     Q.921-User Adaptation Layer(IUA)", <draft-ietf-sigtran-iua-02.txt>
     ,Work in progress

[RFCSCTPAS] Coene, L., Loughney, J., Rytina, I., Ong, L., "Stream Con-
     trol Transmission Protocol Applicability Statement", <draft-ietf-
     sigtran-sctp-applicability-01.txt>, Work in progress

[Q700] ITU-T Recommendation Q.700, "Introduction to CCITT Signaling Sys-
     tem No.7", March, 1993

[Q70X] ITU-T Recommendation Q.701-705, "Message Transfer part No. 7",
     1996

[Q71X] ITU-T Recommendation Q.710-715, "Signaling Connection Control
     Part No. 7", 1996

[Q77x] ITU-T Recommendation Q.770-775, "Transaction Capabilities Appli-
     cation Part No. 7", 1996

[Q1400] ITU-T Recommendation Q.1400, " architecture framework for the
     development of signaling and OA&M protocols using OSI concepts
     ",1993

[RFC1035] Mockapetris, P., "Domain Names, Implementation and specifica-
     tion", RFC1035, November 1987

[11](#) Author's Address

Lode Coene
Siemens Atea
Atealaan 34
B-2200   Herentals
Belgium

Phone: +32-14-252081
EMail: lode.coene@siemens.atea.be

John Loughney
Nokia
Research centre
Itamerenkatu 11-13
FIN-00180   Helsinki
Finland

Phone: +358-9-43761
EMail: john.loughney@nokia.com

Ian Rytina
Ericsson Australia
37/360 Elizabeth Street
Melbourne, Victoria 3000
Australia

Phone : -
EMail:ian.rytina@ericsson.com

Lyndon Ong
Nortel Networks
4401 Great America Parkway
Santa Clara, CA 95054
USA

Phone: -
EMail: long@nortelnetworks.com

Expires: December 2000

Full Copyright Statement