SIGTRAN

Signaling over IP — a step closer to an all-IP network

MIA IMMONEN

KTH Information and Communication Technology

Master of Science Thesis
Stockholm, Sweden 2005

IMIT/LCN 2005-14

SIGTRAN

Signaling over IP – a step closer to an all-IP network

Author: Mia Immonen
Examiner: Gerald Q. Maguire Jr.

Royal Institute of Technology (KTH)

2005-06-15

TABLE OF CONTENTS

Abstract

The mass popularization of telecommunication services in recent years have resulted in a heavily loaded signaling network. The Signaling System number 7 (SS7) is used in fixed and wireless networks and is needed for call control and services such as caller ID, roaming, and for sending SMS. The traditional SS7 networks are expensive to lease and to expand, hence a new suite of protocols have been designed to carry signaling messages over IP. This suite contains a transport protocol called Stream Control Transmission Protocol (SCTP) and various user adaptation layer protocols such as M2PA, M2UA, M3UA, and SUA. To transport the highly loss and delay sensitive signaling messages over IP, it is mandatory that the transport protocol meets the high performance requirements of SS7. Not before the IP-solution has been tested in detail, will it replace significant parts of the national telephone network.

In this thesis, the failover duration in the case of link failure was tested using the feature of SCTP called multi-homing. The results suggest that carrying SS7 signaling traffic over IP is possible, since the failover duration does not exceed the required limit.

Abstract

Under de senaste åren har telekommunikationstjänster blivit allt mer populära, vilket har lett till ett tungt belastat signaleringsnätverk. The Signaling System number 7 (SS7) används i fasta och trådlösa nätverk och behövs för att kontrollera telefonsamtal och för tjänster såsom caller ID, roaming och för att skicka SMS. De traditionella SS7-nätverken är dyra att hyra och att expandera, varför en ny grupp av protokoll har designats för att bära signaleringsmeddelanden över IP. De nya protokollen innehåller ett transportprotokoll som heter Stream Transmission Control Protocol (SCTP) och flera adaptionslagerprotokoll, bl.a. M2PA, M2UA, M3UA och SUA. För att transportera de förlust- och förseningskänsliga signaleringsmeddelandena över IP, måste transportprotokollet möta de höga krav som SS7 har. Inte förrän IP-lösningen har testats ingående, kommer den att ersätta betydelsefulla delar av det nationella telefonnätet.

I detta examensarbete har failovertiden mätts då en nätverkslänk mellan två noder har utsatts för ett avbrott. Resultaten pekar på att det är möjligt att bära SS7-trafik över IP eftersom failovertidskraven inte överstigs.

1. Signaling background

The traditional Public Switched Telephone Network (PSTN) and other telecom networks such as GSM, consist of a traffic network and a separate signaling network, where the latter handles the control information that is needed to supervise and manage calls and for the management of the network itself. In a telephone network, there are three kinds of signaling end points: a Service Switching Point (SSP), a Signal Transfer Point (STP), and a Service Control Point (SCP). Figure 1 shows how they are connected by either voice trunks or signaling links.

Since the number of mobile phone users has grown rapidly recently, and because of the mass popularity of communication services, the demand on signaling networks is growing as well. Also the demand for services such as Voice over IP (VoIP) or more generally Media over IP (MoIP) is increasing and the telecom operators must start planning for future networks that better support the resulting datagram traffic. IP has been considered the most promising network protocol, since it can offer improved resource utilization while reducing the operational, maintenance, and network infrastructure costs [20].

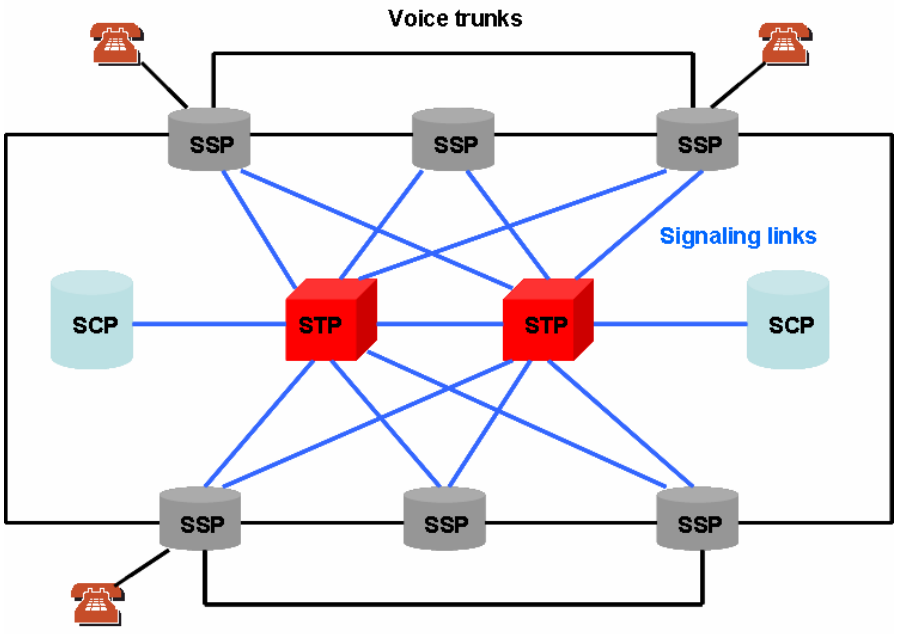

Figure 1: Telephone network with separate voice and signaling links.

The traditional Signaling System number 7 (SS7) networks are not as scalable as IP-networks because they are expensive to expand [20]. This is the reason why the Signaling Transportation (SIGTRAN) working group of the Internet Engineering Taskforce (IETF) has developed a new signaling protocol suite that will make it possible to carry the signaling messages over IP [11].

Today the task is to integrate these two types of existing networks, since a transition from traditional telecom networks to IP-networks will not happen overnight, and this co-existence is expected to last for a long period of time, perhaps even for decades. The goal, however, is an all-IP network, also called the Next Generation Network (NGN), where all types of networks are connected and where the end devices can range from a cellular phone to a TV.

The SS7 networks have existed for a long time and have gone through a lot of improvements over the years to meet the high performance demands (low loss and low delay) of a phone call. Therefore, it is very important to make sure that the SIGTRAN solution brings to packet networks all the proven and deployed qualities of the traditional SS7 networks.

The traditional IP transport protocols (TCP and UDP) do not support the high demands for low delay and reliable transmission for signaling messages, thus the Stream Control Transmission Protocol (SCTP) was designed. It is part of the new SIGTRAN protocol suite that consists of SCTP and some upper layer adaptation protocols (such as M2PA, M2UA, M3UA, SUA) that communicate with the traditional SS7 layers.

SCTP uses a new feature called multi-homing that will make it more suitable for signaling than traditional transport protocols. This thesis work will investigate the performance of the SCTP protocol in *link failure situations*. Specifically, the failover time of the multi-homing mechanism and the message transfer time will be measured to see if they meet the timing requirements of SS7.

2. Introduction to SS7

In telecommunication networks the signaling takes place in a network separate from the network where the voice is transported. Signaling messages manage phone calls and provides the user with functions such as addressing (the called number), call setup, and termination or information such as dial tone and busy tone. When electronic devices were introduced in telecom networks, new possibilities emerged with common channel signaling, which lets one common channel transport signaling messages for a number of voice trunks. It is an out-of-band signaling method which means that the signaling and the voice are sent in separate channels, which makes possible sending signaling messages also *during* a phone call and enabled signaling to network elements without voice trunks, such as data bases [8]. Having access to data bases introduced the Intelligent Network (IN) in the 1980´s with services such as toll free 800/888 numbers, calling cards, caller ID, and three-way calling.

SS7 is not only a standard for the fixed network, but also for VoIP, GSM, and 3G, where signaling is needed for the advanced management of mobile phone services; even a simple wireless call requires 6 times more SS7 messages than a wire line call. Additionally, Short Messages Services (SMS) are transported on the signaling links as well, which results in a large amount of traffic because of the increasing popularity of such services.

The SS7 networks are circuit switched networks with 56 or 64 kbit/s links, which clearly limit the transmission capacity compared to IP, which is not tied to traditional telephone bandwidths. The SS7 networks today are heavily loaded and need expansion to be able to deal with the demands of the telecom market. The need for a scalable network with a cheap infrastructure together with the fact that most telecommunication services are datagram based, made IP a suitable solution. The idea is to bring these two types of networks together, and the bridge that connects them is a Signaling Gateway (SGW), which contains both SS7 and SIGTRAN protocols and an interworking function that translates between these two. When using SS7 over IP, one or more of the underlying SS7 layers are exchanged for SIGTRAN layers. Below, each of the SS7 layers will be described very briefly and following this the SIGTRAN approach will be explained in greater detail.

2.1 MTP layers

The SS7 signaling messages are based on the Message Transfer Part (MTP) [10]; this is a reliable but connectionless link layer service in traditional SS7 networks that consists of three layers that correspond to the three lowest layers of the OSI model: the physical layer, the data link layer, and the network layer, see Figure 1.

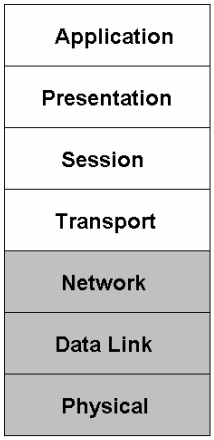

Figure 1: The OSI model layers.

- MTP1 defines the physical and electrical characteristics of the 56 or 64 kbit/s-based data link.

- MTP2 is in charge of the reliability aspects of data delivery. It ensures reliable end-to-end transmission between two signaling endpoints and performs flow control, checking of the Cyclic Redundancy Check (CRC) checksum, error monitoring and retransmissions.

- MTP3 provides routing of signaling messages between Signaling Points (SPs) in the SS7 network. All network elements that have an MTP3 instance are provided with a numeric SS7 address called a point code which is used in the routing process just like IP addresses. In case of congestion or failed links, the MTP3 layer is responsible for congestion control and re-routing of the signaling messages.

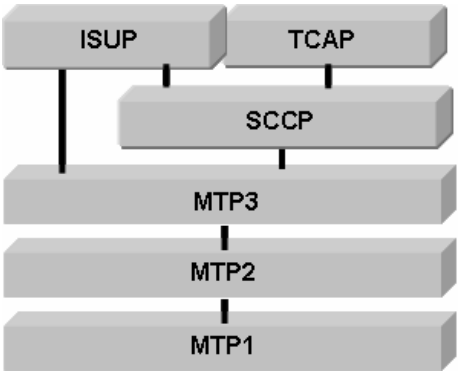

Figure 2: The SS7 stack.

2.2 SCCP

The Signaling Connection Control Part (SCCP) [10] is a part of the network layer together with MTP3 and enhances the MTP protocol with two main features: subsystem number (SSN) and Global Title Translation (GTT) which can be used when needed. MTP was developed before SCCP and therefore lacks some desirable functions, such as expanded addressing and connection oriented message transfer.

The subsystem numbers enable recognition of specific software applications (subsystems) within one physical node. The signaling node in Figure 3 has three subsystems (A, B, and C) that are all using the services of SCCP to transport their signaling messages. This is useful since MTP is node-to-node oriented and only distinguishes between complete nodes and not between the different SCCP-users within the node. This way a Mobile Switching Center (MSC) can work as a Home Location Register (HLR) at the same time, and the SCCP-messages are sent to the right subsystem by including the subsystem number in the message.

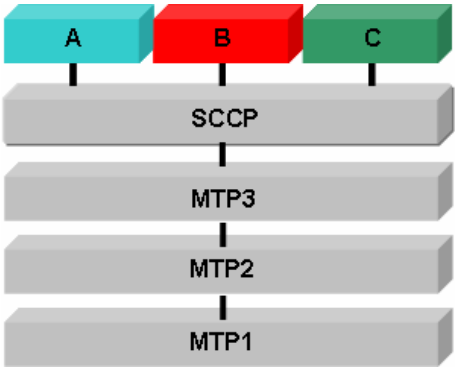

Figure 3: Different signaling applications (A, B, C) within one single network node can be distinguished by using subsystem numbers.

The GTT is a procedure where a sequence of digits (called the global title) is translated to a point code and subsystem numbers. A global title can be a toll free 800 number, calling card number, or mobile subscriber identification number, etc. The translation can take place at the originating point of the message or in a Signaling Transfer Point (STP). The MTP protocol can not route messages with global titles, e.g. TCAP messages, hence SCCP is needed to transport them.

2.3 TCAP

The Transaction Capabilities Application Part (TCAP) [8] is a connectionless protocol that runs on top of SCCP. It executes operations at remote nodes and receives the results from these processes, e.g. database queries. The information obtained is used by a TCAP application such as Customized Applications for Mobile Network Enhanced Logic (CAMEL) or Mobile Application Part (MAP), which are called Application Service Elements (ASEs) [8]. These are both parts of the SS7 stack and are used to extend traditional Intelligent Network services found in fixed telephone networks into GSM networks.

An application uses TCAP to query information at another node or to return the response. The queries can provide a user with information such as the routable number of an 800 number or obtaining a billing number from a telephone calling card. In a cellular network, when a mobile subscriber roams into a new MSC area, the Visitor Location Register (VLR) requests information about the subscriber in its HLR using MAP, and the information is transported within TCAP messages.

2.4 ISUP

The ISDN User Part (ISUP) [10] provides the traditional signaling procedures used to set-up, manage, and release voice and data calls over the public switched telephone network (PSTN). It reserves trunk circuits between the communicating signaling points and later releases them when one of the users terminates the call. ISUP is the protocol that enables ISDN services in the PSTN, but can also be used for non-ISDN calls. The ISUP signaling messages use the transport services of MTP3, while the SCCP interface may be employed for other additional services.

There is a SS7 protocol called Telephony User Part (TUP) [10], which provides the same services as the newer protocol ISUP. TUP has been replaced by ISUP in most countries and in the international network, but still exists in the telephone networks of e.g. China.

2.5 SS7 performance requirements

Since telephony is a real time service, it has to perform extremely well to keep the users satisfied. Therefore, the ITU-T recommendation Q.706 [21] was written and contains the following performance requirements [12]:

- No more than one in 10^7 messages can be lost due to failure in the network.
- No more than one in 10^{10} messages may be delivered unordered or duplicated.
- No part of a SS7 network should be out of service more than 10 minutes per year.

On top of this, both TCAP and ISUP have their own timing requirements on response times and processing times but are not specified in any recommendations of ITU-T.

The SS7 networks have existed for decades and have gone through a lot of improvements to meet the high performance demands (low loss and low delay) of a phone call. One fundamental measure to meet the requirements above is to connect all nodes in a signaling network, called Signaling Points (SP), by up to 16 links that form a linkset. They are used for load sharing and for redundancy in case of link failure. More common though, is that every SP has an alternative linkset to provide a backup path in the case of link failure. Figure 4 shows the alternative paths of the signaling network where each SP can reach two STPs (called mated pair) to provide redundancy. That way, in case of link failure on some link, there is always an alternative path to reach the destination. The mated pairs are interconnected with a link to enhance the reliability of the network. These links are used only when there has been a link failure and the STP has no other routing options.

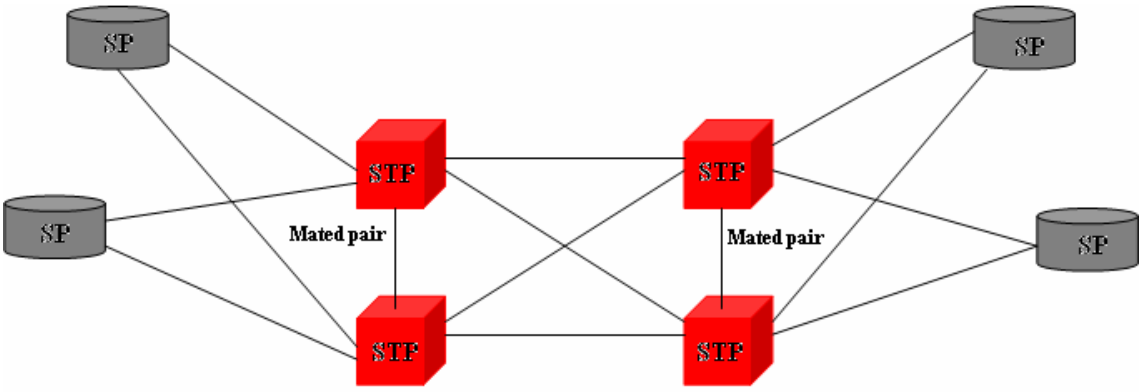

Figure 4: Redundancy in a SS7 network achieved by mated pairs [38].

3. SIGTRAN

The Signaling Transport (SIGTRAN) working group of the Internet Engineering Task Force (IETF) has designed a new set of protocols to transport SS7 signaling messages over IP. The suite of protocols consists of a new transport protocol and various adaptation protocols and became a standard in 2000 and 2001 and is described in various RFCs on the IETF homepage [11]. Using the SIGTRAN protocols is the first step to merge SS7 networks with IP networks. The primary reason for the use of IP is to off-load the heavily loaded SS7 networks and make them scalable for the increasing amount of telephone and mobile users. The SIGTRAN solution will also be used to connect isolated islands of SS7 networks, which otherwise would have required an expensive SS7 infrastructure. Today's telecom companies are moving towards an *all-IP network*, where IP will replace traditional telecom networks, but such a transition will not happen over night, perhaps never, and the main task now is to enable these systems to co-exist and to enhance the services they provide.

3.1 Why SIGTRAN?

For message delivery over IP on the Internet the transportation protocols Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are used, but for real time signaling they imply certain limitations. However, the desired characteristics of signaling transportation are:

- Ordered, reliable transfer.
- Redundancy in case of link failure.
- Low loss and delay.
- Security against Denial of Service (DoS).

UDP and TCP can not support all these requirements [2], hence a new transport protocol was designed by SIGTRAN, the Stream Control Transmission Protocol (SCTP) [22].

3.1.1 UDP

UDP is a connectionless transport protocol that does not intrinsically use acknowledgment (ACK) messages to guarantee reliable and ordered transportation. UDP is useful in situations when high transmission rates are needed, but does not have to fulfill the other performance requirements of signaling messages.

3.1.2 TCP

TCP is a byte oriented transport protocol that provides a stream of bytes and guarantees that it is delivered in order. This is ideal for transmitting large amounts of data, such as files or email, but the strictly in-order-delivery is also what makes it unsuitable for signaling messages. TCP is extremely sensitive to delay variance caused by the network or packet loss which often causes retransmissions. When waiting for a lost packet to be acknowledged, all other packets will be delayed, which is called head-of-line blocking. This generates unnecessary delays for other packets, hence TCP is inappropriate for real-time applications, such as signaling.

Another disadvantage of TCP is its vulnerability to DoS attacks. To establish a TCP connection, the client has to send an SYN message to the server that will be answered with a SYN ACK. The server waits for the corresponding ACK from the client, which is the last step in the three-way handshake in the TCP connection setup. However, this procedure can be susceptible to a certain DoS attack called SYN attack, caused by many SYN messages being sent to a server where they occupy memory resources and can lead to a server collapse, preventing legitimate users from getting service. This is not acceptable in a SS7 network where telephone services should **always** be available.

3.2 SIGTRAN architecture

The SIGTRAN protocol suite includes the transport protocol SCTP, along with several user adaptation (UA) layer protocols that are necessary for the transport of SS7 messages over IP. The SIGTRAN architecture consists of three layers [2]:

- IP layer,
- Transport layer (SCTP), and
- User adaptation layer (e.g. M2PA, M2UA, M3UA, and SUA).

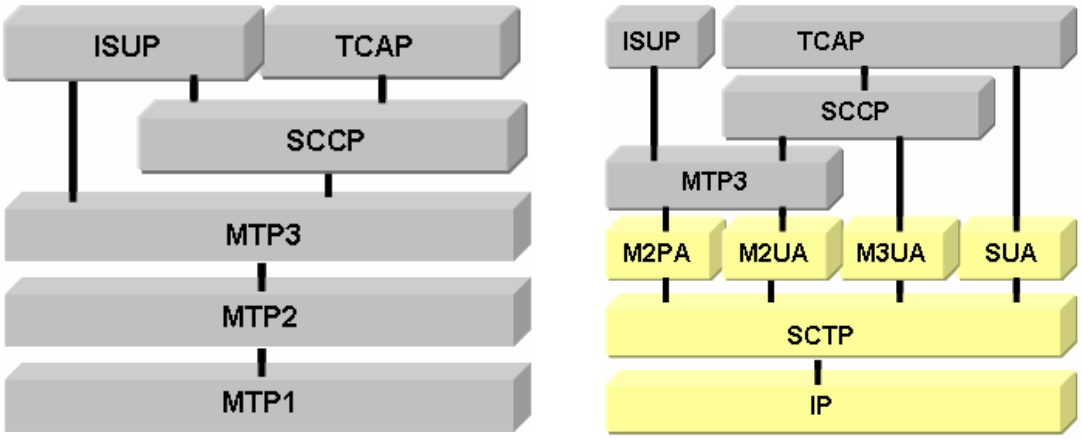

Figure 5: The MTP1 and MTP2 layers in the traditional SS7 stack (left) are replaced by SIGTRAN protocols (right) to enable signaling over IP.

In Figure 5, the three lower layers in the protocol stack show the new SIGTRAN protocols. They replace the lower layers of the SS7 stack (MTP1 and MTP2), enabling transportation over IP. SCTP is a transport protocol similar to TCP, but with a few changes to better suit SS7 signaling. A user adaptation protocol makes its SS7 user (MTP3, SCCP, TCAP, ISUP etc.) unaware of that the original lower SS7 layers have been replaced. In Figure 3 the ISUP connection to M3UA is not shown to simplify the figure, but it is also a frequent protocol combination. Depending on the telephone network, different user adaptation protocols can be chosen depending on their characteristic features.

3.3 SCTP

To send data over a connection in IP-networks, usually TCP or UDP are used. However, as mentioned above, SS7 signaling messages have very stringent loss and delay requirements, hence TCP is not a suitable choice, because the delays are too long and UDP does not provide sufficient reliability. The SCTP protocol is similar to TCP (as it provides both flow and congestion control mechanisms) but it has a few major differences, namely multi-homing and multi-streaming [2].

3.3.1 Multi-homing

A multi-homed node is one with several IP-addresses, where each IP-address pair between two nodes is called a **path**. In Figure 6, node A has 3 paths to node B and node B has two paths to A. In a SCTP connection (in SCTP this is called an "association") each node chooses a primary path. If a failure occurs on this path, retransmissions are sent via an alternative path (if possible). Each path is associated with heartbeat messages which indicate an active or inactive mode. After a specific number of retransmissions, a path is considered inactive and a new path is chosen, and if it is active, then it becomes the new primary path. This multi-homing feature enables a network to reroute data to other IP addresses, thus the network is more tolerant of physical link failures. In a classical SS7 network there are always at least two physically different paths over which to transmit data. Since SIGTRAN should provide an IP-solution with all the qualities of the SS7 network, the multi-homing feature can be used to provide the same level of redundancy.

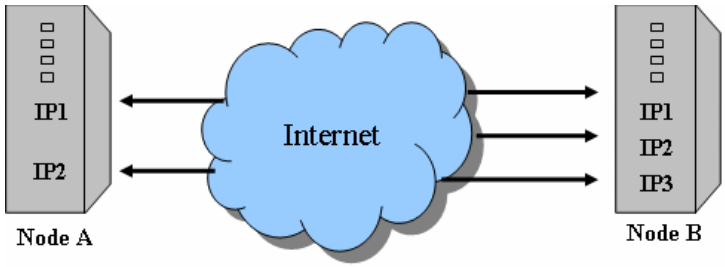

Figure 6: Multi-homed nodes.

3.3.2 Multi-streaming

Multi-streaming is used to avoid head-of-line blocking, which is a common phenomenon in TCP, as shown in Figure 7. When a signaling packet for call 2 is lost in a TCP-stream, the whole connection is blocked when waiting for a retransmission, resulting in head-of-line blocking. The delay for recovering the lost data can be several seconds, which is unacceptable while making a phone call.

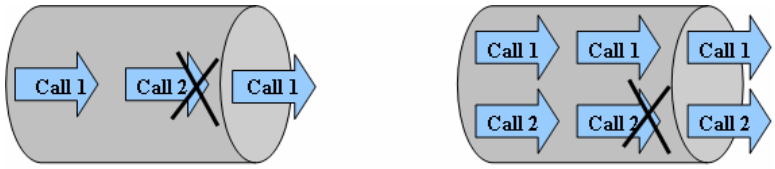

Figure 7: The multi-streaming feature avoids head-of-line blocking.

Therefore in SCTP, an association between two nodes can have several streams, each one assigned to a particular resource or application, thus these streams do not block each other in event of packet loss or delays. Creating several streams with TCP is also possible, but implies opening multiple TCP-connections where each acts as a stream. Every connection introduces a Transport Control Block (TCB) at the server side, which contains all the important information about a connection. These TCBs consume memory, and their numbers could be significant for a busy signaling point with various clients, hence multiple TCP connections is not a desirable alternative. Also using only one SCTP association with streams instead of several TCP connections, unnecessary setup times are avoided.

3.3.3 Other SCTP features

- *Message boundary preservation:* TCP is a byte oriented protocol, while SCTP is a message oriented protocol that places one or more complete signaling messages into a SCTP message. A SCTP message is composed of a common header and various chunks, where the chunks contain the user data of different lengths.

- *Out of order transmission:* a TCP node always receives packets in sequential order. With SCTP it is possible to send SCTP packets *in order* or *out of order*, depending on what the application prefers. When it comes to signaling, the sequence order **within** each stream/call is important, but not between the different streams.

- *Cookies:* both TCP and SCTP go through a handshake before establishing an end to end connection. While TCP uses a three-way handshake, SCTP uses a four-way handshake which includes cookies to protect the connection from DoS attacks. A DoS occurs when an attacker in one way or the other, withholds a service from a legitimate user.

  The SCTP handshake is initiated by an INIT message that contains many fundamental association parameter values, such as initial Transmission Sequence

Number (TSN), number of inbound and outbound streams and all IP addresses of a multi-homed endpoint. These values are negotiated during the handshake and the INIT ACK from the responding peer contains its preferable values. This message also contains the state cookie and to form it, a TCB has to be created and stored. A minimal subset of information from the TCB is then introduced to the state cookie that is sent within the INIT ACK message. After sending it, the stored TCB is deleted to avoid the DoS attacks present in TCP. To bring the handshake to an end, the receiver of the INIT ACK message immediately sends a COOKIE ECHO with the received state cookie. The receiver authenticates the state cookie and establishes an association with the parameters in the state cookie, and ends the handshake with a COOKIE ACK message.

3.4 User Adaptation Layers

3.4.1 M2PA

MTP2-user Peer-to-peer Adaptation layer (M2PA) [23] is a SIGTRAN protocol that transports SS7 MTP signaling messages over IP using SCTP. It is an adaptation protocol between MTP3 and SCTP and works between pairs of signaling nodes. Using M2PA makes it possible to maintain the original topology of the SS7 network, i.e. all the network elements such as Signaling Transfer Points (STPs), pointcodes, etc. The only thing that changes is that transportation of signaling occurs over IP instead of over traditional 64 kbit/s links; see Figure 8 [1].

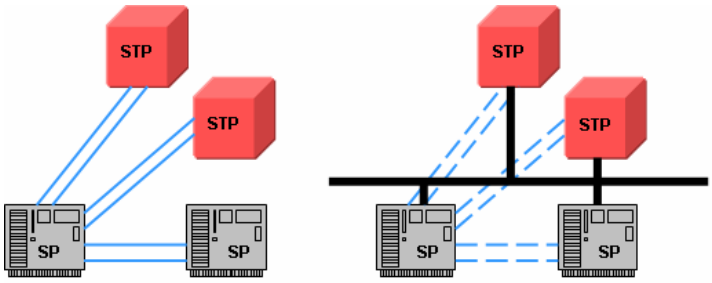

Figure 8: M2PA changes the physical links between nodes.

M2PA can be used between two IP-signaling nodes in an IP-network, or between a Signaling Gateway (SGW) and an IP-signaling node, but is most common between two SGWs, e.g. to interconnect two SS7 network islands (PSTN A and PSTN B) through an IP-network. Figure 9 shows the two distant SS7 networks that are combined together via a less expensive IP network. Since the SS7 links are dedicated to only signaling traffic, the bandwidth is continuously assigned, hence infrequently used SS7 links inefficiently use the bandwidth which is a scarce resource. The IP solution mixes signaling traffic with other IP traffic and therefore reduces the costs of signaling, since a link can be shared among many users.

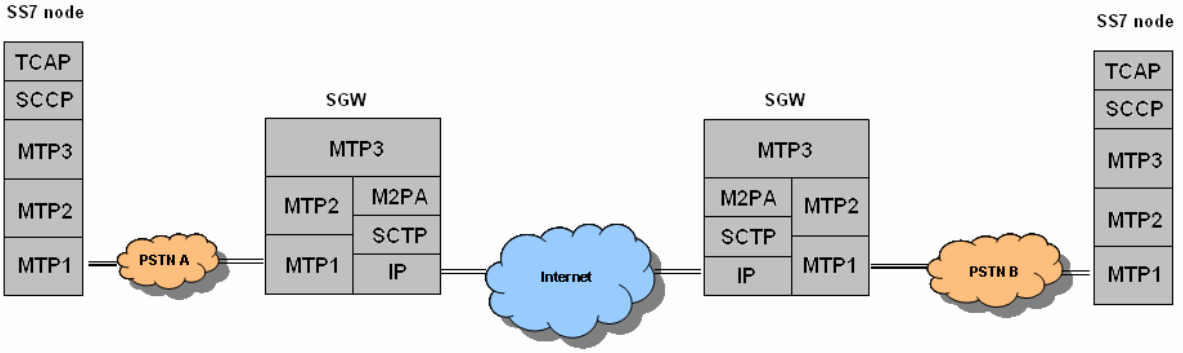

Figure 9: Two distant SS7 network islands are connected over Internet through M2PA [18].

Since both SGWs have an MTP3 layer they also have a point code and a SS7 PC must be assigned to each SGW. Because of the peer-to-peer feature of M2PA, it is possible for the MTP3-peers to communicate directly. The user of M2PA is MTP3 in both nodes, just as MTP3 is the user of MTP2 in the SS7 stack. This means that M2PA is actually just a replacement for MTP2 and therefore has functions similar to MTP2.

3.4.2 M2UA

MTP2-User Adaptation layer (M2UA) [24] also adapts MTP3 to SCTP, and is a protocol that sends signaling messages between the MTP3 layer on a media gateway controller (MGC) and the MTP2 layer on a SGW, e.g. in a VoIP network. Instead of being a peer-to-peer protocol like M2PA, it operates on a client-server basis, where the MGC (IP node) is the client and the SGW acts as the server. This way the MTP3 layer on the MGC is the user of the MTP2 layer on the SGW, and neither of them is aware that they actually are remote. This phenomenon when signaling messages are transported over IP from the top of one SS7 layer to the bottom of another, is called *backhauling*. Since the SGW does not have an MTP3 layer, only the MGC has a point code, see Figure 10.

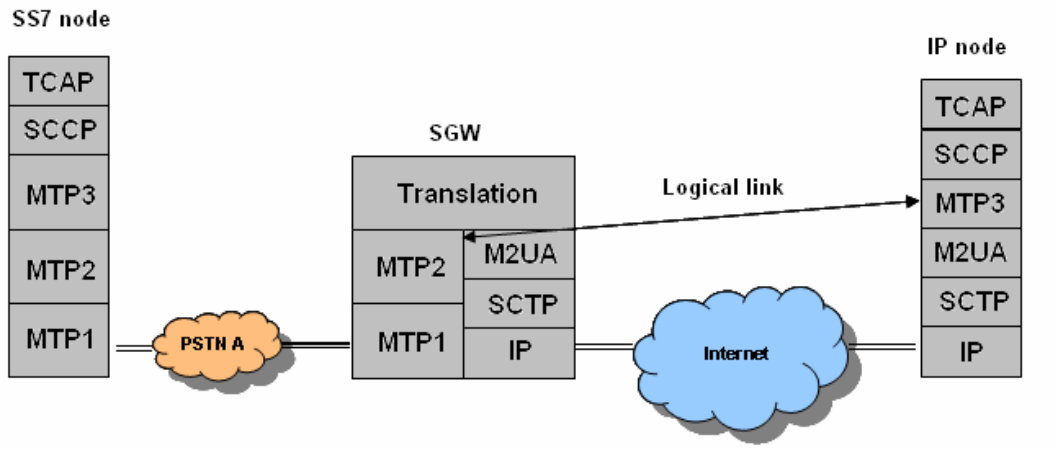

Figure 10: Back hauling with M2UA in two distant nodes. The SGW and the MGC are not aware that they are remote and each node thinks that MTP3 is directly communicating with MTP2.

M2UA is frequently used when there is a low density of physical SS7 links in some particular part of the network, or if the SGWs are at a great distance from each other. In this case backhauling can connect several of these signaling nodes to one centralized network element, thus allowing these distant nodes to share a single SGW. Since this is done over the IP network, it is much cheaper than SS7 links, hence M2UA is a cost saving alternative. Another advantage is the fact that each SGW, that connects a remote signaling point to a MGC, does not have a point code. The point code is assigned to the MGC, which saves many SS7 PCs that would otherwise have been required by each SGW (as when using M2PA).

3.4.3 M3UA

The MTP3 User Adaptation (M3UA) [25] layer operates on a client-server basis, just as M2UA, to provide remote connection between two SS7 layers in a SGW and a MGC (IP node). However, in this case, the SGW has a MTP3 layer (and a point code) that communicates with the ISUP/SCCP layer of the MGC, see Figure 9. Even in this case, the nodes are not aware of each other; the MTP3 in the SGW does not know that its user (ISUP or SCCP) is remote and similarly the ISUP/SCCP layer at the MGC does not know that the SGW´s MTP3 layer is not its own. This is another example of backhauling [19].

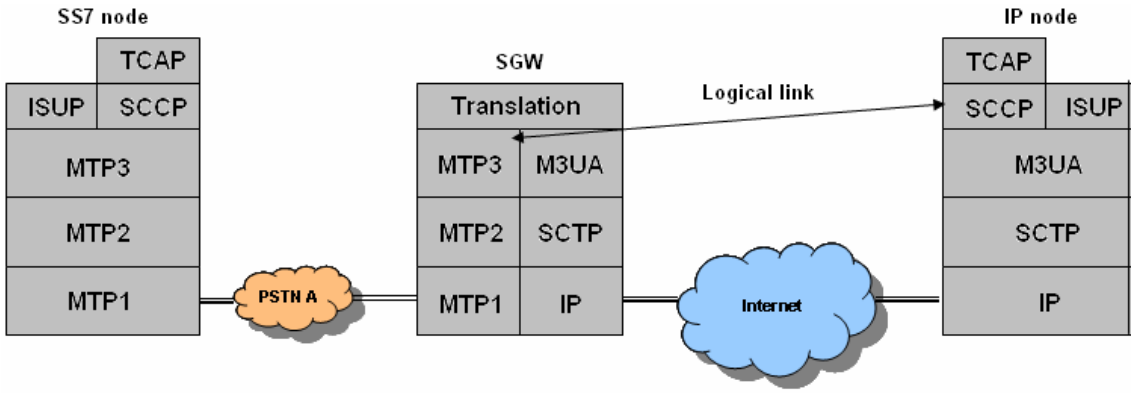

Figure 11: Backhauling using M3UA.

As with M2UA, M3UA does not process any signaling packets; it simply forwards them to their destination. This means that the M3UA in the IP node does not have routing tables and does not execute any other functions of the corresponding MTP3 layer.

If M3UA is used in an all-IP network with no pure SS7 nodes, it replaces the MTP3 layers of the both IP nodes and operates in a point to point manner that is known as IP Signaling Point (IPSP) behavior. M3UA is one of the user adaptation layer protocols that removes most SS7 layers from the signaling points and that changes the topology of the network to a more IP-like one. Thus the system can better make use of the more efficient IP-solutions and cheaper infrastructure. In an all-IP network, M3UA is not restricted to the SS7 requirements of maximum message size of 272 bytes, but can use the larger bandwidth of available via the IP network. The flexibility of M3UA and its ability to better use the IP network and its advantages have lead to it being chosen as the standard protocol for UMTS networks.

3.4.4 SUA

When migrating from an SS7 network, IP-network operators want to maintain many valuable applications from the traditional telecom networks such as toll free, prepaid and roaming. The SIGTRAN working group made this possible by defining the SCCP User Adaptation (SUA) [26] layer, which not only provides the IP-network with these services, but also eliminates even more of the SS7 stack than the other user adaptation protocols, see Figure 12; thus using the IP routing and bandwidth more efficiently. Moreover, IP-nodes with SUA are simpler and therefore cheaper than other adaptation layer nodes.

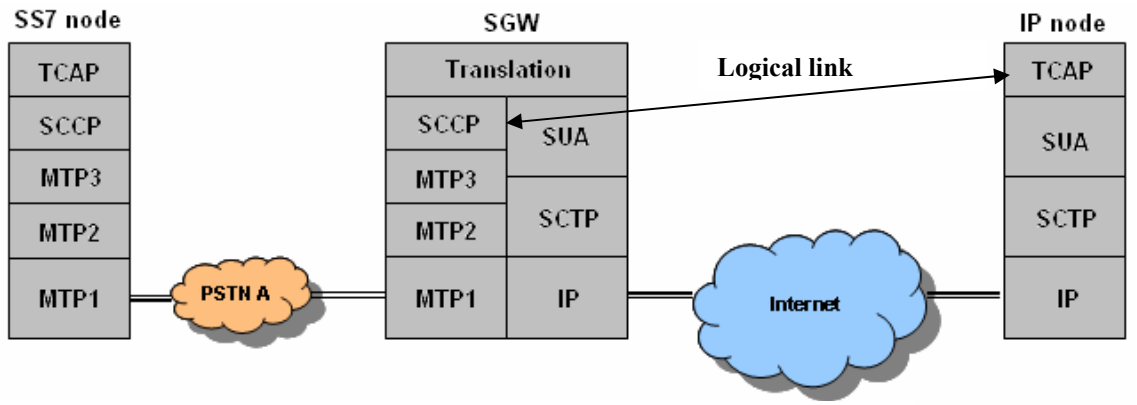

Figure 12: Backhauling with SUA.

The SUA-layer's main tasks are to transfer SCCP-user data between a SGW and a MGC (client-server model) and to map between SCCP addresses and IP addresses in the SGW. However, because of SUA´s inability to transport ISUP messages (see Figure 5, p. 8), 3GPP has chosen to use M3UA as the standard signaling protocol in the central parts of the UMTS networks while using SUA as a complement for nodes with databases, e.g. home location registers (HLRs).

3.8 Security

In a telephony access network, access protocols are used for signaling, and in the core network the SS7 protocol stack is used for signaling. SS7 networks are often physically inaccessible to end-users, so they are considered to be protected from attacks, since the network equipment is behind locked doors.

The access networks on the other hand are used for end-user signaling and here security issues are quite important [4]. The main threats are attackers that are passive and simply read messages on the network, thus observing passwords, etc., along with active attackers that write, delete, or modify messages. Some important security objectives are: authentication of peers, integrity, confidentiality of user data, avoidance of unauthorized and inappropriate use, and denial of service (DoS). All SIGTRAN user adaptation layer protocols use SCTP for transportation of data, which provides some security features such as resistance against blind denial of service attacks (flooding, masquerading and improper monopolization of services) [7]:

Cookies: In the SCTP four-way handshake cookies are exchanged; this prevents attackers from establishing connections without using them and in that way hindering legitimate users from establishing a connection (see 3.3.3).

Verification tag: The SCTP packet header contains a verification tag that indicates if a packet belongs to a certain association. If it does not, it is dropped; this protects the users from a man-in-the-middle attack.

In the experiments of this thesis the security issues were not considered, but to provide end-to-end security between two remote peers in real telecom networks, it is recommended that IPsec or TLS are used as well. With IPsec a secure tunnel is established between two peers that provides the equivalent of an isolated link such as used in a traditional SS7 network.

3.9 Interoperability tests

The ETSI Plugtest Service is a professional unit of the European Telecommunications Standards Institute (ETSI) that specializes in arranging interoperability test events for companies, organizations, and standardization bodies (ETSI, Internet Engineering Task Force (IETF), International Telecommunication Union (ITU), etc.). These tests are in the area of telecommunications, Internet, broadcasting, and multimedia. The participants are operators, vendors, or equipment manufacturers that want to test the interoperability of their products between each other, before placing them on the market. Other important participants are standardization bodies or other working groups that are developing a new standard and need feedback before continuing the standardization work.

During the interoperability tests the implementations are tested on a testbed provided by the Plugtest Service, with scenarios and cases that have been set up by experts. By doing these tests the engineers learn at an early stage of the development process how their prototype works together with other manufacturers´ solutions. The name, "PLUGTEST", was selected to reflect the idea of the interoperability event aiming at TESTing that all implementations can PLUG into the network or to its specific environment as well as interworking with each other, according to the homepage of Plugtests [6]. Despite compatibility with a standard, there might not be interoperability between two products using the same standard.

There was a SIGTRAN Plugtests 6 - 10 September 2004 in France where the interoperability between implementations of user adaptation layers (IUA, M2PA, M2UA, M3UA, and SUA) was tested. The results can be found on the SIGTRAN mailing list [27] and will be used to improve the internet drafts.

3.10 Commercial Implementations

The range of commercial SIGTRAN implementations is large and many of these companies have participated in ETSI Plugtests, e.g., Adax, Cisco Systems, Ericsson, Hewlett-Packard, Siemens, and Ulticom. The SIGTRAN functions are offered as either hardware or software depending on the demands of the network provider. There are physical signaling gateways (SGW) as well as stacks and blades, and some companies implement just one protocol while others implement the whole protocol suite. Most companies offer signaling gateways that enable 2.5G and 3G services, Intelligent Network (IN) services, SMS offload, SS7 offload, and VoIP. On the homepage of one of the SCTP founders, Randall Stewart [14], is a list of several telecom companies that have extended their business to SIGTRAN technology as well. Performance Technologies was the first to announce support for the SCTP protocol in February 2001, only 6 months after standardization. Others waited for the user adaptation protocols to be standardized before introducing SIGTRAN in their products. Performance Technologies is one of the newest companies in the signaling business, while others, such as Adax, have been providing traditional signaling solutions for more than 20 years.

In general, the SIGTRAN signaling products look the same; most companies offer SGWs that are customer adaptable to a great extent. Depending on the customer's networks and needs, a SGW can be provided with any suitable adaptation (UA) layer running over SCTP and with different capacities depending on the size and needs of the network. Table 1 compares four companies' SIGTRAN SGW implementations.

Table 1: Comparison of commercial implementations.

Company	Product	Protocols	Capacity	Other
Adax	SGW	M2PA, M2UA, M3UA, SUA	64-256 SS7 links	128-253 SCTP associations
Intellinet	SGW	M3UA, SUA	4,16 SS7 links	110 SCCP/ISUP per second
Performance Technologies	SGW or blades	M2PA, M3UA, SUA	8, 16, 24 SS7 links	16-32 M3UA associations
Ulticom	SGW software	M2PA, M3UA, SUA	4 SS7 links	--

Three companies offer a SGW as a box, while Ulticom has software that is installed on an already existing signaling infrastructure. Adax has the largest spectrum of hardware and software variants, while the others generally have one or two products that differ in capacity. The most frequently implemented UA protocols are M3UA and SUA, and for companies with one product, these are usually the two supported protocols. M2PA is available from many companies; it simply changes a traditional SS7 link to an IP link, while the infrastructure and topology of the networks remain the same. According to Performance Technologies, the cost for leasing a SS7 link can be $300 per link per month in the U.S. and up to five times that amount for international links. Therefore, by sharing an IP link with other IP traffic, the bandwidth can more efficiently be utilized and the cost of the link is reduced. So even though most of the network's functions remain the same, the cost savings are substantial using M2PA, which reduces costs by transporting SS7 messages over shared-use IP networks rather than over dedicated SS7 links.

The capacity of a SGW can be expressed and measured in many ways; one common metric is the number of SS7 links that can be terminated in it. The more links, the more calls that can be processed at the same time. The latter is sometimes expressed in throughput, e.g., 110 SCCP or ISUP messages per second at 1 Erlang. Another interesting quantity that is provided by Adax and Performance Technologies is the number of SCTP/M3UA associations that can be established with a SGW. Adax indicates it supports 3 to 25 secondary IP addresses on their SGWs, which provide different levels of redundancy for the network when using the multi-homing feature.

SIGTRAN products are well established in the market and there are many to choose from depending on the needs of each customer.

Figure 13: Adax Signaling Gateway.

Figure 14: A Performance Technologies SG5600 PICMG® 2.16-Compliant Signaling Gateway Blade.

3.11 Open Source Implementations

Additionaly, there are free SIGTRAN implementations available via the Internet [14], and the purpose of these was to be able to test an "SS7 over IP" solution. Most only implement the SCTP protocol, while the user adaptation layers are only available in a few of them.

OpenSS7

The OpenSS7 [29] project started in 1996 but was initially only an SS7 stack. The SIGTRAN features were introduced in 2001 and include the SCTP protocol and the M2PA user adaptation protocol. The other UA (user adaptation) protocols exist (M2UA, M3UA and SUA), but are still at a testing stage and have not yet been released. There is also a TCP implementation available for comparisons between the two transport protocols (SCTP vs. TCP).

There is an interest in widening the OpenSS7 SIGTRAN stack to also include mobile communication parts, such as a home location register (HLR) with GPRS capabilities. This project is still in the design stage and is currently on hold.

OpenSS7 was developed for the Linux kernel. It currently requires the 2.4.10+ kernel and a C compiler (gcc) capable of compiling the Linux kernel.

Siemens/University of Essen

This implementation [28] was designed by Siemens, the University of Essen, and the University of Applied Sciences, Germany. It is only an implementation of SCTP. It runs on Linux 2.4, and 2.6, FreeBSD 4.8, Solaris 8, Mac OS 10, and Windows (with some limitations). Moreover, it supports both IPv4 and IPv6 and includes a SCTP test tool. With the test tool you can verify that your installation is correct and try the test cases.

Additionally, there is an implementation of SUA that can be combined with this SCTP implementation.

KAME project

The KAME project [30] is a co-operation between six companies in Japan. It works on FreeBSD 4.0, OpenBSD 2.7, NetBSD 1.5, BSD/OS 4.2, and newer versions of these. The implementation provides an IPv6 and IPsec (for both IPv4 and IPv6) stack for BSD variants and provides advanced internetworking such as advanced packet queuing, mobility, etc.

Linux Kernel SCTP implementation

The LKSCTP project [31] was started by one of the inventors of SCTP – Randall Stewart – in cooperation with Motorola. This implementation supports SCTP, and also provides test tools with numerous test cases. It can be run on both IPv4 and IPv6. To install the package, a Linux-2.5.36 or later kernel version is necessary, and it has to be configured with the network options “SCTP Configuration” support enabled.

Sun SCTP

Sun Microsystems’ SCTP is another pure SCTP implementation which runs on Solaris 9, update 6 [32].

M3UA

There is a M3UA implementation [33] that is compatible with the three latter SCTP implementations above.

4. SCTP failover experiment

For a future migration to an IP based signaling network, it is mandatory that the SS7 network requirements are fulfilled even with the SIGTRAN protocol suite. Therefore, tests were performed of the multi-homing feature, where failover duration and message transfer times are measured. In the ITU-T Q.706 recommendations [21] a changeover time in a SS7 network in case of link failure is set to a maximum of 800 ms; which should not be exceeded by the SCTP protocol failover mechanism.

4.1 Experimental setup

The test bed consists of two computers A and B with two IP addresses each to create a multi-homed network. Path 1 is set to primary path where all data will be transmitted, and path 2 will be used for retransmissions or in case of link failure on path 1. A link failure is accomplished with NIST Net [15] on the third computer and a failover to path 1 is expected.

The IP addresses of the two paths should be configured as two different subnets to easily route data to the correct IP address. In Figure 15 we see that path 2 is subnet 192.168.1.0 with host addresses 1 and 2, while path 2 is divided into 2 subnets, 192.168.2.0 and 192.168.3.0 because of the third computer that will regulate the traffic.

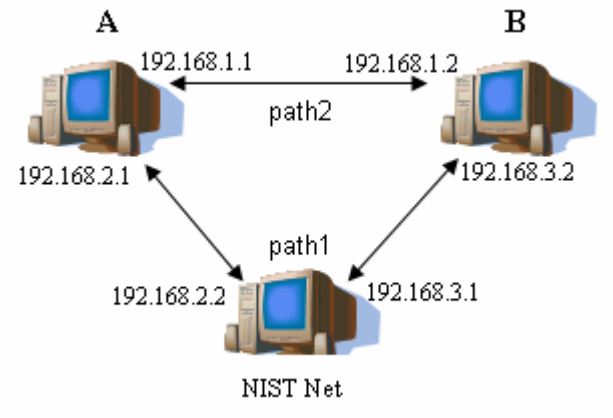

Figure 15: Experimental setup for the SCTP failover experiment.

In the routing table for computer A, see Table 2, we define that the subnet 1 should be assigned to interface eth1 and subnet 2 to interface eth2. To reach computer B through path 1, we need to pass through gateway 192.168.2.2, also using interface eth2. This way, packets to 192.168.1.2 will be sent on eth1 and packets to destination 192.168.3.2 will be sent on eth2.

Table 2: Computer A's routing table.

Destination	Gateway	Genmask	Iface
192.168.1.0	*	255.255.255.0	eth1
192.168.2.0	*	255.255.255.0	eth2
192.168.3.0	192.168.2.2	255.255.255.0	eth2

The same is true for the routing table of computer B, where packets to path 1 are sent on eth1 and packets to path 2 on eth2. In this direction, packets on path 2 have to pass through gateway 192.168.3.1.

4.2 The implementation

All tests are carried out using the SCTP implementation developed by the University of Essen and Siemens [16]. It follows the RFC 2960 [22] and is constantly being debugged and improved based on the problems that users report on the mailing list [34]. The implementation has been used in several experiments by others [35, 36, 37] and has some documentation for installation and use. The best help is obtained from the mailing list, where the authors frequently answer questions and provide help. The library contains several test programs, such as a day-time server, chargen-server, discard-server, and a client called "terminal". Using these programs provides a good way to gain experience about the implementation and the functions of SCTP, before developing one's own applications.

4.3 The SCTP failover parameters

When SCTP fails to deliver a packet or if no Selective acknowledgment (SACK) is received within a specified time period, called the retransmission time out (RTO), then the retransmission timer expires, and the lost data will be sent via another available link, e.g. the secondary path. To monitor if a link is available, heartbeat messages are sent regularly and if they are acknowledged with heartbeat ACKs, then the path is considered active.

The parameters that affect the failover time are the RTO and the maximum number of retransmissions (MPR) on a path before it is considered unreachable. The RTO is calculated from current Round-Trip-Times (RTTs) and can range from RTO_{min} to RTO_{max} (both user specified limits). RTO_{min} should not be too low, as this would cause unnecessary retransmissions and with a very low MPR could even cause the protocol to use the secondary path before a link failure has actually occurred. The MPR has a great

impact on the failover time as it determines how many retransmissions a path should attempt before it is considered unavailable and a new primary path is chosen.

According to RFC 2960, the suggested SCTP failover parameter values are the following [13]:

Table 3: Default values for SCTP configuration.

Parameter	RFC 2960
RTO_{init}	3000 ms
RTO_{min}	1000 ms
RTO_{max}	60000 ms
MPR	5
$SACK_{delay}$	200 ms

- RTO_{init} is the initial value of the RTO before any RTT measurements have been made.
- RTO_{min} is the lowest allowed value for RTO. If a calculated RTO is very small, then the value will be rounded up to RTO_{min}.
- RTO_{max} is the highest allowed value for RTO. Large RTO values will be rounded down to RTO_{max}.
- MPR is the number of maximum retransmissions on a path before it is considered unreachable. Until this value is exceeded a failover will not take place.
- $SACK_{delay}$ is the time the receiver waits before it acknowledges a chunk. SCTP can choose not to send a SACK for every chunk, and instead wait for additional chunks and acknowledge all of them in the same SACK message. However, it has to acknowledge at least every other SCTP packet (one SCTP packet can contain many chunks) or if there are no additional chunks arriving within the $SACK_{delay}$ time, a SACK has to be sent.

The default values lead to a failover time of 1s + 2s + 4s + 8s + 16s + 32s = 63 s, starting with RTO_{init} = RTO_{min} and doubling the RTO timer value for each retransmission to give the network time to recover from network congestion. However, according to SS7 requirements, the failover time has to be less or equal to 800 ms, so it is obvious that these parameters have to be modified to reduce the failover time.

4.4 The SCTP failover scenario

When setting up a multi-homed association, all IP addresses are exchanged in the INIT message of the initial four-way handshake, but the reachability of each path is not immediate and must be established during the first seconds of the association. Table 4 shows the four-way handshake from a tcpdump file:

Table 4: The initial four-way handshake used by SCTP.

No.	Time	Source	Destination	Bytes	Info
1	10:55:13.897002	192.168.2.1	192.168.3.2	102	INIT
2	10:55:13.897303	192.168.3.2	192.168.2.1	214	INIT_ACK
3	10:55:13.898268	192.168.2.1	192.168.3.2	174	COOKIE_ECHO
4	10:55:13.898575	192.168.3.2	192.168.2.1	50	COOKIE_ACK
5	10:55:13.899135	192.168.3.2	192.168.2.1	562	DATA
6	10:55:13.900433	192.168.2.1	192.168.3.2	62	SACK

DATA is immediately sent on the primary path after the handshake, while the secondary path's availability is being probed with a heartbeat message. When a heartbeat ACK is received, the secondary path is also considered reachable and at that point a link failure is caused on the primary path (path 1). When the first RTO timer expires, then these attempted packets are successfully resent on path 2 while new transmissions continue on the primary path. However, these can not be delivered on the failed path and a second RTO timer expires, this time twice as long as the first RTO. If MPR is set to 5, then the 6^{th} retransmission will be the one that triggers the failover, since the MPR limit has then been exceeded.

The failed primary path will be reported as unreachable and following this all data transmissions will occur on path 2, which is also set to be the new primary path by the application. Only when all enqueued messages from the failed path have been retransmitted on the new primary path and new data transmissions can take place, then the failover procedure is considered completed. The failover duration is defined as the time between the last received SACK on path 1 and the time of the first new data transmitted on path 2.

SS7 narrowband networks allow messages up to 272 bytes while broadband networks allow up to 4091 bytes. In IP networks the messages size limits differ between different links, but are generally more generous than SS7, however for co-existence of SS7 and IP networks, the SS7 limits have to be respected for proper function. Therefore, in the test, messages of 500 bytes will therefore be transmitted every 2 ms to simulate a broadband network, but still are very close to the narrowband requirements as well. To achieve this, the chargen-server code was slightly modified and the terminal program serves as a receiver. A chargen-server is a character generator that is used in this experiment to send packets from computer A to B on path 1 with the following commands:

```
[root@A]# ./chargen_server -s 192.168.1.1 -s 192.168.2.1 -V -l 500

[root@B]# ./terminal -d 192.168.1.1 -d 192.168.2.1 -r 19 -V
```

Specifying both IP addresses of the hosts **enables** the multi-homing feature of SCTP. The other options sets the message length (-l) to 500 bytes, the port (-r) to 19, and requests a very verbose output (-V), that prints network statuses and association information on the terminal window. In addition to this information, the communication between the two end points can be captured with tcpdump, thus exact time stamps, packet types, and further information for individual packets can be seen.

Each test was run 5 times. Each different test used a specific set of values for the parameters, as will be described below. A total of almost 90 test runs were made including the attempts to improve some failover times, and NTP [39] was used to keep the computers' clocks synchronized during the experiments.

4.4.1 RTO_{min}

As mentioned earlier, the association parameters for the failover have to be adjusted to achieve a faster failover. Knowing that there is essentially no delay on the links, the calculated RTOs will be very small; hence the RTO_{min} will be the limiting factor. Recalling also that for every retransmission the RTO is doubled, which leads to $2 \cdot RTO_{min}$, $4 \cdot RTO_{min}$, $8 \cdot RTO_{min}$, and so on depending on the MPR parameter. When deciding upon an appropriate value for RTO_{max} these series of doublings have to be considered to avoid making the RTO range too small or large.

Knowing that the choice of RTO_{min} value directly affects the failover time, because of the small RTTs of the paths, this value was set to 80 ms as in experiments carried out by K.J. Grinnemo and A. Brunström [5]. However, this results in failover times far greater than 1 second **even** with only 2 retransmissions, thus this value had to be reduced drastically.

If RTO_{min} is set too low, it will cause unnecessary retransmissions because of the very short time out value. However, the packets that are retransmitted are not necessary lost, just delayed and would have reached the receiver within an acceptable time. Early retransmissions lead to same data being sent on both paths and results in duplicates that are undesirable for a network. If the MPR parameter is also very low, a path can be considered as failed and new data will be sent on a secondary path, even though the

primary path has not actually failed. Considering this, the RTO_{min} was set to 40 ms which would hopefully not be too low, but would decrease the failover time remarkably.

4.4.2 RTO_{max}

After every RTO timer expiration the RTO is doubled to give the network a chance to recover from temporary congestion. The RTO_{max} parameter limits the upper value of a doubled RTO and should not be set too close to RTO_{min} as that would lead to too small RTO values that can not grow, which will lead to a failed path after a certain number of retransmissions. If the link is not temporary congested, but actually has failed, then the RTO_{max} shouldn't be set too high, as this would delay the failover process with high RTO times. Therefore, tests were done with RTO_{max} set to values between 80 and 350 ms.

4.4.3 $SACK_{delay}$

Because of the small RTT values of the two paths, there will be no significant packet delays, and considering the fact that a new packet is sent every 2 ms, there is a high arrival rate at computer B. Recalling that a SACK has to be sent for every other incoming SCTP packet or every $SACK_{delay}$ ms, thus packets will arrive at such a high rate that the $SACK_{delay}$ will **not** have any influence on the acknowledgment process. The default value is 200 ms, but was decreased to 10 ms only in the case of unexpected delays.

4.4.4 Maximum Path Retransmissions

Together with the RTO_{max}, the parameter MPR (Maximum Path Retransmissions) determines the failover duration when the first retransmission has already been triggered by RTO_{min}. The larger the MPR value, the more retransmissions allowed, with increasing RTO values each time, this significantly delays the detection of a link failure. Additionally, an early recognition of path failure leads to fewer enqueued packets that have to be retransmitted on the secondary path before new packets can be sent, thus further delaying the failover process.

The different failover tests are denoted a "Failover(MPR)", where MPR indicates the number of retransmissions. The default value MPR=5 was expected to result in very high failover times, hence tests were initiated with MPR=2, followed by MPR=3 and possibly even MPR=4. Allowing only one retransmission would have improved the results even further, but this is a very sensitive value and would similarly to low RTO_{min} and RTO_{max} lead to unnecessary failovers.

4.5 Message transfer time

The failover time of the SCTP protocol has an impact on the message transfer times as well. Packets on the primary path that are sent after the link failure are enqueued for retransmission on the secondary path. These should not be lost and must be sent before any new data is transmitted on the new primary path. Recommendations on message response time for MTP3 are 500-1200 ms for good signaling performance [12], which implies that even though a link failure has occurred, signaling messages should not be exposed to a delay much higher than 500 ms. Logically the message transfer times should follow the same pattern as the failover time, which means that short failover duration leads to short message transfer time during the failover and that longer failover times cause higher transfer delays for the packets.

5. Results

5.1 Failover

In Figure 16 the failover time is shown with, RTO_{min}=40 ms and MPR=2 for several RTO_{max}. It can be seen that the RTO_{max} does not affect the failover times, even when increased. Since the RTO can only grow to 160 ms before failover, RTO_{max} values larger than that will have no effect on the results, as at that point the MPR parameter determines the behavior.

Lower RTO_{max} values limit the growth of the RTO on the second or third retransmission, keeping it rather constant. There are limitations on this value up to 100 ms, then a large step up to 150 and 200 ms is allowed that gives the RTO room to grow to its maximum value, causing longer failover times.

The most important result is that with the Failover(2) setup, all times stay under the 800 ms limit which was the requirement on signaling networks. With a fixed RTO_{min} of 40 ms the values of RTO_{max} never cause the failover time to exceed the limit.

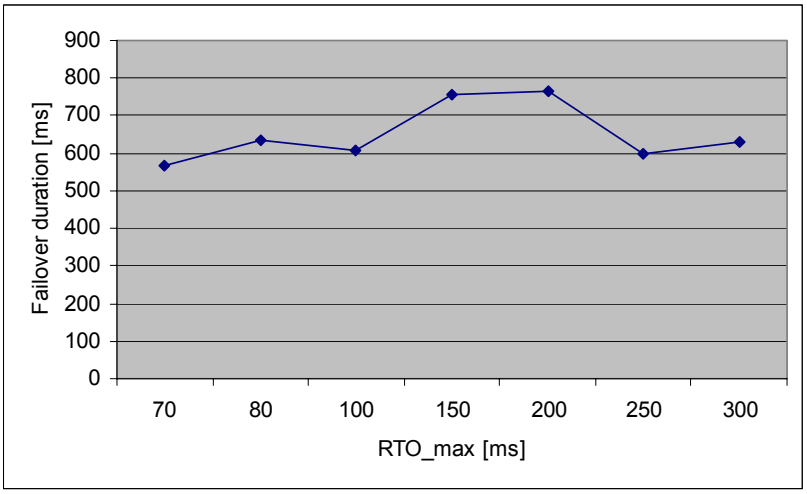

Figure 16: Failover duration with RTO_{min}=40ms and MPR=2.

Figure 17 shows the same test, but with 3 allowed retransmissions before failover. This means that the theoretical RTO values are 40, 80, 160, and 320 ms for each retransmission. We can clearly see the effect when RTO_{max} is 250 and 350 ms, letting the RTO double to 160 and 320 ms leading to failover delays of 1119 and 1427 ms. However, all failover times in this association setup exceed 800 ms and are therefore unsuitable from a signaling point of view. MPR=4 would have increased the failover duration even more by allowing one more retransmissions and was therefore not tested.

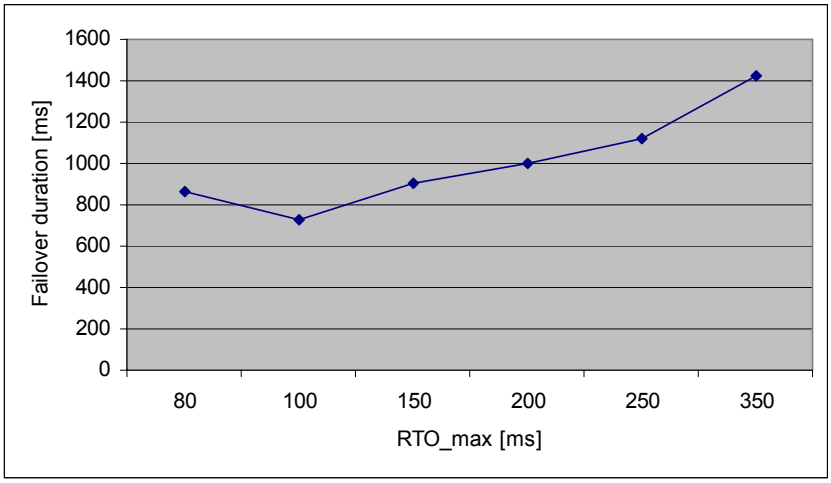

Figure 17: Failover duration with RTO_{min}=40ms and MPR=3.

Table 5 shows exact results of both Failover(2) and Failover(3) for interesting values of RTO_{max} and the values within brackets show the square root of the sample variance.

Table 5: Test results for Failover(2) and Failover(3) with RTO_{min}=40ms.

RTO_{max}	70	80	100	150	200	250	300	350
Failover(2)	569 ms (41)	637 ms (0.10)	608 ms (102)	757 ms (0.10)	767 ms (0.10)	601 ms (31)	631ms 6.8	--
Failover(3)	--	868 ms (44)	725 ms (108)	907 ms (0.13)	1003 ms (64)	1119 ms (78)	--	1427 ms (0.28)

Since the Failover(3) results did not coincide with the failover requirement, efforts were made to improve the results adjusting RTO_{min} to 20 ms, but the failover times remain almost the same; see Table 6. One last effort was made for improvements with RTO_{min}=20 ms and RTO_{max}=40 ms, which is a very aggressive combination, but only a small improvement was achieved as can be seen in Figure 18.

Table 6: Adjustments for Failover(3) improvements.

Attempts	1	2	3
RTO_{min} [ms]	40	20	20
RTO_{max} [ms]	80	80	40

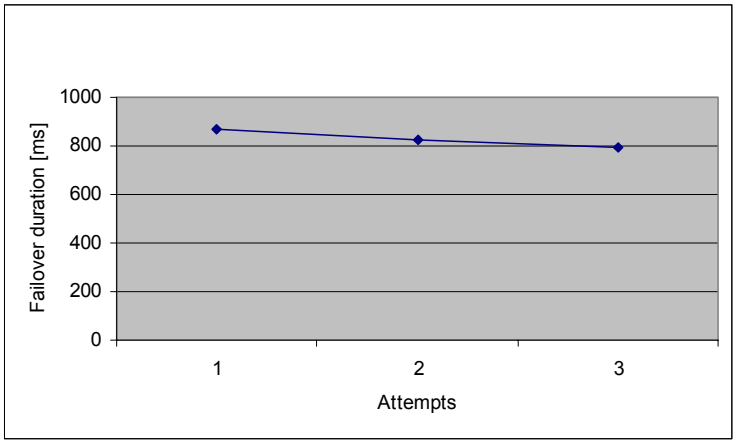

Figure 18: Attempts to improve the Failover(3) results by adjusting RTO_{min} and RTO_{max}.

This leads to the conclusion that at most 2 maximum retransmissions per path is the best option. Hence, RTO_{max} should be chosen so that it gives the network a chance to recover, but small enough not to lengthen the failover time more than necessary. In the tests, RTO_{max} values between 100 and 200 ms lead to a fast failover time and caused few unnecessary retransmissions.

5.2 Message transfer time

As seen in Figure 19, the message transfer times are affected by the failover duration as expected. The message transfer time has been measured for the most appropriate values of RTO_{max} from a failover point of view and shows the same increases in value (150 and 200 ms) as the Failover(2) scenario.

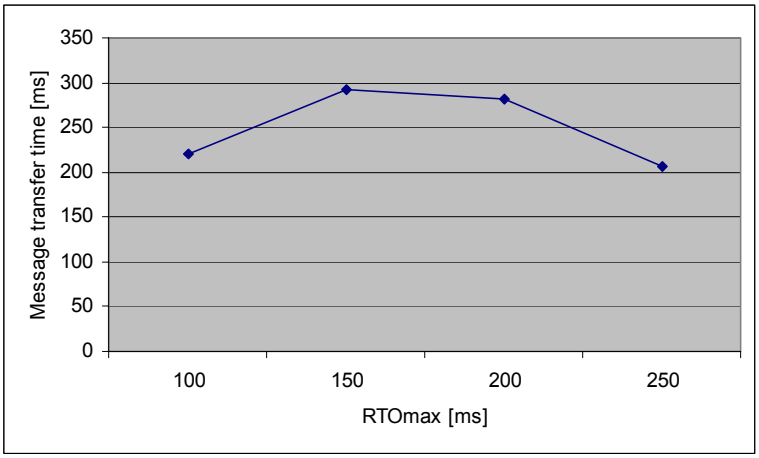

Figure 19: Message transfer time for RTO_{min}=40 ms and MPR=2.

With MPR set to 3, the failover times increase and become unacceptable for a signaling network. Even though the message transfer times follow the same pattern as for the failover scenario, they do stay within the specified bound of under 500 ms.

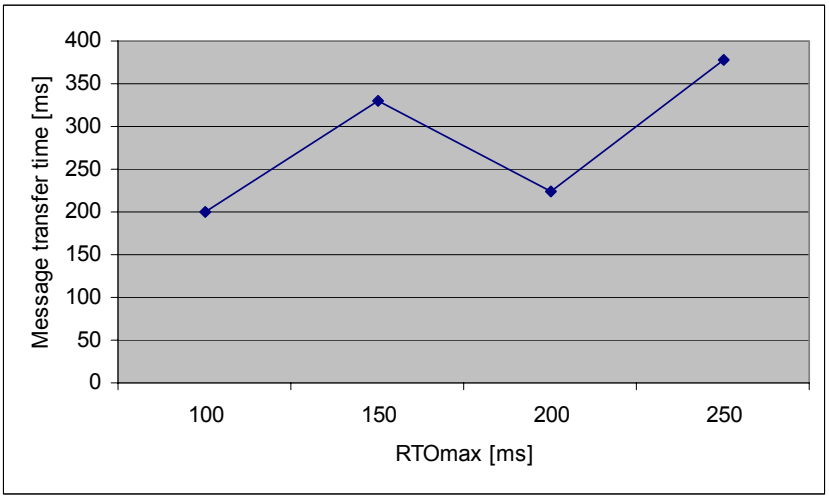

Figure 20: Message transfer time for RTOmin=40ms and MPR=3.

6. Discussion

The standardized SIGTRAN protocols have been around for five years and implementations have been developed to facilitate testing and also for commercial purposes. The purpose of SIGTRAN is to offer inexpensive extension possibilities for SS7 networks and to support future migration of all networks to an all-IP network. Since signaling happens in real-time in today's telecommunication networks, it is extremely important that it performs well and within certain bounds. The performance of today's SS7 networks is based on decades of experience and its services are needed to support modern telecommunication services.

It is clear that the SIGTRAN solution will increase the efficiency of signaling, while simultaneously providing much more signaling bandwidth, and that the Internet will offer a better economic alternative to leased links. The main issue, however, has been the uncertainty of whether SIGTRAN will perform as well as the traditional solution using dedicated links. The Internet is never as reliable as a separate signaling network without other user traffic, but hopefully these concerns will be proved false by SIGTRAN's alternative ways of achieving reliability.

One concern is the failover duration in case of a link failure, which should not introduce unacceptable delays for signaling applications and the users of them. In SS7 networks all signaling points have alternative linksets to mated pairs for backup paths in the case of link failure. This function is addressed in SCTP by multi-homing that performs a similar failover, but the failover duration must still not exceed the specified changeover time of 800 ms.

There are several parameters in the SCTP protocol that influence the performance of the failover mechanism. These have been collected in Table 7 together with their actual values in my experiments.

Table 7: SCTP failover experiment parameter values.

Parameter	Failover(2)	Failover (3)
RTO_{init}	40	40
RTO_{min}	40	40
RTO_{max}	70, 80, 100, 150, 200, 250, 300	80, 100, 150, 200, 250, 350
MPR	2	3
$SACK_{delay}$	10	10

The RTO_{min} was set knowing that this value is the one that actually causes retransmissions. Since the RTTs of the test bed were very small, each RTO will always be rounded up to RTO_{min}. Too small a value causes early and unnecessary retransmissions, which is not desirable considering increasing network load, but in this case 40 ms was the highest value that gave good failover times. RTO_{init} only affects the very first RTO value because of lack of RTT measurements and is therefore set equal to RTO_{min}. The $SACK_{delay}$ was irrelevant because of the fast transmission rate in these tests, hence it was assigned the value 10 ms just to handle the case of unexpected network delays.

At a very early stage it became apparent that the MPR has a large impact on the final results of the failover. Since MPR=2 gave failover times very close to the 800 ms limit, values other than MPR=3 did not need to be tested. The results show that only the Failover(2) association setup would be suitable for signaling for all the RTO_{max} values that were tested. Note that the MPR limits the use of RTO_{max} whenever using a parameter value higher than 150 ms.

Message transfer times were better than the performance requirements limit for MTP3 messages, e.g. all times were far below 500 ms on both Failover(2) and Failover(3) setups. However, similar experiments that have been performed by A. Jungmaier, E. P. Rathgeb, and M. Tuexen [35] show that slightly faster failover and message transfer times would make Failover(3) and Failover(4) possible association setups as well. Since the same SCTP implementation was used, the reason for the discrepancy must be due to the experimental setup of the network. Some suspicious communication problems have been observed on path 2 containing the NIST Net. The link between this computer and computer A has much larger RTT values compared to the other links and has problems generating ICMP messages (used in ping) which can be a sign of bad communication. Also, sometimes widely varying test results depending on day and time may have been caused by other resource consuming uses of computers A and B during tests.

In spite of this, considerable knowledge has been collected from these experiments yielding deeper understanding concerning SCTP. Even though failover and message transfer times did not correspond to earlier tests, the relations between all involved parameters and the actions of the implementation have been as expected.

7. Conclusions

This thesis presents an introduction to the SIGTRAN solution for signaling over IP and an evaluation of a critical feature called multi-homing that should provide redundancy in IP based signaling networks. Even though the SCTP protocol suite was standardized already in 2000, there are still many tests to be done before using it to completely replace SS7 in all telecom networks. Many of the commercial implementations available today have been tested in Plugtests to investigate their functionality and compatibility with the standard. These implementations can certainly be used in smaller telephony networks and in VoIP networks, but actually replacing significant parts of the national telephone network will probably take some time. The complete changeover from the traditional SS7 networks to IP based networks will not happen over night, maybe never, but even before considering this, we must be sure of that the SIGTRAN solution performs just as well or even better than the SS7 does.

The multi-homing experiments carried out in this paper, suggests that SCTP does meet the performance requirements for signaling. Even the message transfer times in the case of a link failure were achieved with a large margin of error. Observing that the time it takes to detect a failure strongly depends on the number of maximal path retransmissions and RTO_{max}, and taking into account that this detection time can be up to 80% of the total failover time, one realizes the importance of reducing this detection time as much as possible with the correct association parameters.

The SIGTRAN standard was originally developed for signaling over IP, but has over the years found new application areas. Being liberated from the extremely complex TCP retransmission behavior, the SCTP protocol can be used for a reliable transportation of Media over IP (MoIP). When providing a multimedia transfer with related but yet independent data streams, e.g. voice and video, the SCTP multi-streaming feature is suitable, so that head-of-line blocking and multiple TCP connections are avoided. Other uses are running FTP on top of SCTP in order to provide faster transfer using multi-streaming by avoiding unnecessary setup delays for each transfer while saving resources on the server side by only opening one association. S. Ladha and P. D. Amer [19] have carried out an experiment that shows that this is true for networks with losses, when the head-of-line blocking is avoided by streams. However, when losses are really low and there is no head-of-line blocking, TCP actually outperforms the SCTP transfer because of lower packet overhead.

The SIGTRAN protocol suite is a promising new way of carrying out message transfers over IP. Since IP based services are constantly expanding, there will definitely be a need for protocols such as SCTP, whether it will be for signaling or for multimedia services.

8. Future work

The experiments performed in conjunction with this thesis were conducted without significant local delays, losses, or other competing traffic which should be taken into account in any final decision on whether SCTP meets the failover time requirement. There are other experiments that have been done with delays [5], but they suggest that the propagation delay only had a minor impact on the SCTP failover time. The effects of losses and competing traffic are still unknown and would contribute with interesting information on whether the Failover(2) scenario would still perform well.

Ideas regarding load sharing on multi-homed nodes are circulating, but are not supported by the version of the SCTP implementation used. If all secondary IP addresses could be used for transmission instead of only providing redundancy, the throughput could be increased.

9. References

[1] http://www.ulticom.com/docs/SS7_Signaling_Convergence_White_Paper.pdf, accessed Oct. 18th 2004.

[2] http://www.artesyncp.com/pdf/wp_sigtran.pdf, accessed Oct. 22nd 2004.

[3] http://www.potaroo.net/ietf/ids/draft-ietf-sigtran-signalling-over-sctp-applic-09.txt, accessed Oct. 22nd 2004.

[4] http://www.rfc-archive.org/getrfc.php?rfc=3788, accessed Oct. 22nd 2004.

[5] http://www.scs.org/scsarchive/getDoc.cfm?id=1638, accessed Oct. 25th 2004.

[6] http://www.etsi.org/plugtests/, accessed Nov. 2nd 2004.

[7] http://www.zvon.org/tmRFC/RFC2960/Output/chapter11.html, accessed Nov. 8th 2004.

[8] A. R. Modaressi and R. A. Skoog. *"Signaling System No. 7: A Tutorial"*. IEEE Communications Magazine, p. 19-35, July 1990.

[9] http://tdrwww.exp-math.uni-essen.de/inhalt/forschung/sctp_fb/IvanAriasRodriguezMastersThesis.pdf, accessed Nov. 23rd 2004.

[10] http://www.pt.com/tutorials/ss7/index.html, accessed May 8th 2005.

[11] http://www.ietf.org/html.charters/sigtran-charter.html, accessed May 8th 2005.

[12] http://www.pt.com/tutorials/iptelephony/tutorial_ss7_ip_interworking.pdf, accessed Oct. 25th 2004.

[13] R. Stewart and Q. Xie. *"Stream transmission control protocol (SCTP): a reference guide"*, Addison-Wesley, 2001.

[14] http://www.sigtran.org, accessed Oct. 5th 2004.

[15] http://snad.ncsl.nist.gov/nistnet/, accessed, March 10th 2005.

[16] http://www.sctp.de/sctp.html, accessed Jan. 18th 2005.

[17] http://www.scs.org/scsarchive/getDoc.cfm?id=1638, accessed Nov. 23rd 2004.

[18] http://greco.dit.upm.es/~enrique/pub/jbento-Memoria.pdf, accessed Oct. 15th 2004.

[19] http://star.millersville.edu/symposium/spring2003/FTP-SCTP.pdf, accessed Feb. 15th 2005.

[20] http://www.iec.org/online/tutorials/ss7_over/, accessed Oct. 25th 2004.

[21] ITU-T Recommendation Q.706: Signalling System No. 7 – Message Transfer Part Signalling Performance, International Telecommunication Union, Geneva, March 1993.

[22] R. Stwewart, Q. Xie, K. Morneault, C. Sharp, H. J. Schwarzbauer, T. Taylor, I.Rytina, M. Kalla, L. Zhang, and V. Paxson, "*Stream Control Transmission Protocol*", RFC 2960, IETF, Oct. 2000.

[23] B. Bidulock, R. Dantu, H. J. Schwarzbeuer, and K. Morneault, "*Signaling System 7 (SS7) Message Transfer Part 2 (MTP2) – User Peer-to-Peer Adaptation Layer (M2PA)*", Internet draft, IETF, Feb. 2005, Work in progress.

[24] K. Morneault, R. Dantu, G. Sidebottom, B. Bidulock, and J. Heitz, "*Signaling System 7 (SS7) Message Transfer Part 2 (MTP2) – User Adaptation Layer*", RFC 3331, IETF, September 2002.

[25] G. Sidebottom, K. Morneault, and J. Pastor-Balbas, "*Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) – User Adaptation Layer (M3UA)*", RFC 3332, IETF, September 2002.

[26] G. Sidebottom, L. Coene, G. Verwimp, J. Keller, and B. Bidulock, "*Signalling Connection Control Part User Adaptation Layer (SUA)*", RFC 3868, IETF, Oct. 2004.

[27] sigtran@ietf.org

[28] http://www.sctp.de/sctp-download.html, accessed Jan. 21st 2005.

[29] http://www.openss7.org/, accessed Oct. 25th 2004.

[30] http://www.kame.net/, accessed Oct 25th 2004.

[31] http://lksctp.sourceforge.net/, accessed Oct 25th 2004.

[32] http://playground.sun.com/sctp/, accessed Oct 25th 2004.

[33] http://m3ua.sourceforge.net/, accessed Oct 25th 2004.

[34] http://www.sctp.de/mailman/listinfo/discussion, accessed Apr. 15th 2005.

[35] http://tdrwww.exp-math.uni-essen.de/inhalt/forschung/sctp_fb/sctp-failover.pdf, accessed Feb. 15th 2005.

[36] http://www.linux.ericsson.ca/ipv6/v6sctp.html, accessed Jan. 31st 2005.

[37] http://www.ensc.sfu.ca/~ljilja/cnl/pdf/thomas.pdf, accessed Mar. 3rd 2005.

[38]http://www.cisco.com/univercd/cc/td/doc/product/tel_pswt/vco_prod/ss7_fund/ss7fun02.htm#xtocid11, accessed May 27th 2005.

[39] http://www.ntp.org, accessed May 5th 2005.

IMIT/LCN 2005-14

www.kth.se