Transport of (Legacy) Signaling over IP

SCTP

SIGTRAN architecture
(http://www.ietf.org/html.charters/sigtran-charter.html)

Summary of course scope
Stream Control Transmission Protocol – SCTP - features

RFC - Request for Comments: 2960 defines SCTP (Oct 2000)

- Reliable transport of messages across a possibly unreliable network service such as IP
  - checksums, acknowledgements and message numbering (in streams)
  - detection of lost, corrupted and duplicated packets
  - selective retransmission
  - congestion control for associations
- Many streams (of packets) within an association
- Multihoming (hosts with $n$ IP addresses)

More SCTP features

- Data segmentation to MTU size at end systems
- Multiplexing of user messages to SCTP datagrams: chunks in messages.
- Resistance to flooding (denial of service) and masquerade attacks
What’s wrong with TCP for transport of signaling?

- **HOL blocking**: Two network nodes signal at the same time about many independent calls. TCP ties them together – one lost message concerning a single call causes signaling of other calls to halt until retransmission recovers the lost message.
- **TCP is byte stream oriented**: Application needs to add its own message delimiters and push operations.
- **TCP does not allow multihoming** does not reach the required level of **reliability** (UDP is even more unreliable).
- Nrof simultaneous TCP connections determined by the OS Kernel
- Application can not control **TCP timers** – signaling delay requirements are difficult to meet when TCP uses retransmission.
- **TCP is vulnerable to DOS attacks** (e.g. the **SYN attack**).

A use case: Signaling Gateway

- **M3UA – MTP3 User Adaptation layer extends MTP3 primitive i/f to remote user.**
An SCTP association looks like this

Association is identified by
- IP addresses,
- Port numbers
- Verification tags
- Checksums in msgs

Only one association at any time between a pair of EPs!

SCTP packets have a common header + control and data chunks

Port numbers as in UDP and TCP
During initiation of association, each EP gives the other the value of the Verification tag. The receiver must use that in each subseq. message.
- helps in tackling masquerade attacks

Control and data chunks have Type, Flags and Length information + the user info or control info itself.
Chunk types are:

<table>
<thead>
<tr>
<th>ID Value</th>
<th>Chunk Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Payload Data (DATA)</td>
</tr>
<tr>
<td>1</td>
<td>Initiation (INIT)</td>
</tr>
<tr>
<td>2</td>
<td>Initiation Acknowledgement (INIT ACK)</td>
</tr>
<tr>
<td>3</td>
<td>Selective Acknowledgement (SACK)</td>
</tr>
<tr>
<td>4</td>
<td>Heartbeat Request (HEARTBEAT)</td>
</tr>
<tr>
<td>5</td>
<td>Heartbeat Acknowledgement (HEARTBEAT ACK)</td>
</tr>
<tr>
<td>6</td>
<td>Abort (ABORT)</td>
</tr>
<tr>
<td>7</td>
<td>Shutdown (SHUTDOWN)</td>
</tr>
<tr>
<td>8</td>
<td>Shutdown Acknowledgement (SHUTDOWN ACK)</td>
</tr>
<tr>
<td>9</td>
<td>Operation Error (ERROR)</td>
</tr>
<tr>
<td>10</td>
<td>State Cookie (COOKIE ECHO)</td>
</tr>
<tr>
<td>11</td>
<td>Cookie Acknowledgement (COOKIE ACK)</td>
</tr>
<tr>
<td>12</td>
<td>Reserved for Explicit Congestion Notification Echo (ECNE)</td>
</tr>
<tr>
<td>13</td>
<td>Reserved for Congestion Window Reduced (CWR)</td>
</tr>
<tr>
<td>14</td>
<td>Shutdown Complete (SHUTDOWN COMPLETE)</td>
</tr>
<tr>
<td>15 to 255</td>
<td>reserved by IETF</td>
</tr>
<tr>
<td>63, 127,191,255</td>
<td>IETF-defined Chunk Extensions</td>
</tr>
</tbody>
</table>

SCTP association establishment 1

INIT[Ver-tag=0]

Type=01 Flags Chunk Length
Initiate Tag
Advertisement Receiver Window Credit
Nrof outbound streams Nrof inbound streams
Initial TSN

Optional/Variable length parameters

Initiate Tag gives the value for the verification tag the destination must use in this association in future msgs.
a-rwnd = buffer space in bytes reserved by Initiator for this association
TSN = transmission sequence number (msg number)
Optional: backup addresses, Host name, Increase state cookie time …

INIT ACK
SCTP association establishment 2

Initiator

Cookie wait

INIT ACK

Type=02 Flags Chunk Length

Initiate Tag

Advertised Receiver Window Credit

Nrof outbound streams Nrof inbound streams

Initial TSN

Optional/Variable length parameters

The same optional parameters as in INIT

One MANDATORY variable length parameter:

**State Cookie**
- contains all information for the destination to create this association

COOKIE ECHO

Type=10 Flags Chunk Length

Cookie

Cookie echoed

Destination

Closed

SCTP association establishment 3

Initiator

Cookie wait

INIT ACK

COOKE ECHO

Type=10 Flags Chunk Length

Cookie

Possible data chunks...

The Destination can now rely on that the Initiator is who it claims to be

4-way handshake prevents DOS attacks like the SYN attack in TCP

COOKIE ACK

Type=11 Flags Chunk Length

Possible data chunks...

Data transfer

Established

TCB — transmission control block contains association state

Destination

Closed
SCTP Data Transfer

**DATA**

- **Type=0**
- **Flags: UBE**
- **Chunk Length**
- **Transmission Sequence Nr**
- **Stream Identifier**
- **Stream Seq Nr**
- **Payload protocol Identifier**
- **User Data**

U – unordered, B – beginning fragment, E – ending fragment, TSN – sequence number of data chunk within an association

**SACK (selective acknowledgement)**

- **Type=3**
- **Flags**
- **Chunk Length**
- **Cumulative TSN Acknowledgement**
- **Advertised Receiver Window Credit**
- **Nrof Gap Ack blocks(G)**
- **Nrof Duplicate TSNs (D)**
- **Gap Ack Block #1 start**
- **Gap Ack block #1 End**
- **Gap Ack Block #G start**
- **Gap Ack block #G End**
- **Duplicate TSN #1**
- **Duplicate TSN #D**

The path heartbeat gives information about secondary IP address state

**HEARTBEAT CHUNK**

- **Type=4**
- **Flags**
- **Chunk Length**
- **Heartbeat info type=1**
- **Heartbeat info length**

**HEARTBEAT ACK**

- **Type=5**
- **Flags**
- **Chunk Length**
- **Heartbeat info type=1**
- **Heartbeat info length**

Not defined: usually IP address, time when sent etc… You can even find out MTU using this procedure…
SCTP can be easily extended

- ABORT and ERROR Chunks are used in exceptional cases – still part of the base specification
- New Chunk types are easy to add
- Example ideas: dynamic addition of IP addresses into an association, per-stream flow control …
SCP in an IP network uses SCTP

SUA supports the following

- Transfer of SCCP-User Part messages (TCAP, RANAP, etc.)
- Emulation of SCCP connectionless and connection oriented service.
- Seamless operation of SCCP-User protocol peers.
- Management of SCTP transport associations between an SG and one or more IP-based signalling nodes.
- Distributed IP-based signalling nodes.
- Asynchronous reporting of status changes to management.
**SUA Routing context ties the IP entities to SS7 address parameters**

Routing key = set of SS7 address parameters or parameter ranges: PC, SSN, SIO, Global title

Routing context

Created by management or dynamically

Routing context

1 : 1

Exchanged with the AS

Application Server

Fail-over AS

SCTP association

Host-name, IP address

**Application Server (AS) - A logical entity serving a specific Routing Key.**

An example of an Application Server is a SCP handling all requests for a SCCP-user. The AS contains a set of one or more unique Application Server Processes, of which one (or more) is normally actively processing traffic.

**SIGTRAN components can be used also in the All IP network**

**IPSP**

**SCCP**

**SUA**

**SCTP**

**IP**

**IPSP**

**SCCP**

**SUA**

**SCTP**

**IP**

SUAP - SCCP/SUA Application Protocol (e.g. RANAP/RNSAP in 3G)

IP Server Process (IPSP) - A process instance of an IP-based application. An IPSP is essentially the same as an AS Process, except that it uses SUA in a peer-to-peer fashion. An IPSP does not use the services of a Signalling Gateway.

This might be useful for carrying an existing originally for ISDN designed application into an IP environment.
**Signaling Gateway can use M3UA**

M3UA – MTP3 User Adaptation layer extends MTP3 primitive interface to remote user.

- M3UA extends MTP3 services to a remote AS in an IP network

Routing key = set of SS7 address parameters or parameter ranges: 
CIC, OPC, DPC, SLS, SSN, SIO

Created by management or registered dynamically

M3UA Supports:
- the transfer of all SS7 MTP3-User Part messages (e.g. ISUP, SCCP, TUP etc.)
- seamless operation of MTP3-User protocol peers
- management of SCTP transport associations and traffic between an SG and one or more MGCs or IP-resident Databases
- MGC or IP-resident Database process failover and load sharing
- asynchronous reporting of status changes to management
Alternative for SCP connectivity using SCTP

M2PA – MTP2 User Peer-to-Peer Adaptation layer makes IP network look like a signaling channel (including network management features) for MTP3. Carries all the CCS7 signaling network legacy to the IP environment. SCP is an SS7 signaling point. SG = STP in SS7 terms...

An alternative for MGC connectivity using SCTP

M2UA – MTP2 User Adaptation layer extends MTP2 primitive interface to the IP network: MTP3 of MGC uses SG MTP2 as its layer 2 protocol
M2UA extends MTP2 primitive interface to a remote system

- Each signaling link has IID – Interface Identifier
- Messages from many signaling links can be sent to one AS
- M2UA manages AS fail over.
- Each signaling link is mapped to its own stream in one association, thus messages from different links can be treated in different sequences.

M2UA extends primitive interface to IP
M2PA creates an SS7 signaling link

Differences between M2PA and M2UA include:

M2UA: MGC transports MTP3/MTP2 primitives between the SG's MTP2 and the MGC's MTP3 (via the NIF) for processing.

b. M2PA: SG-IPSP connection is an SS7 link.
M2UA: SG-MGC connection is not an SS7 link. It is an extension of MTP to a remote entity.

c. M2PA: SG is an SS7 node with a point code (SG = STP).
M2UA: SG is not an SS7 node and has no point code.

d. M2PA: SG can have upper SS7 layers, e.g., SCCP.
M2UA: SG does not have upper SS7 layers since it has no MTP3.

e. M2PA: relies on MTP3 for management procedures.
M2UA: uses M2UA management procedures. 

Source: draft-ietf-sigtran-m2pa-04.txt
SIGTRAN summary

- Has produced 3 RFCs and 11 Internet drafts
- SIGTRAN intends to create a comprehensive signaling architecture for integrating SCN and IP telephony
- SCTP is a generic new transport protocol not only for signaling – OS kernel implementations are available and under way
- These protocols are used in 3G, modernization of IN and IP Telephony

SIGTRAN Internet-Drafts: Status of Spring-2002
according to http://www.ietf.org/html.charters/sigtran-charter.html

- Signaling System 7 (SS7) Message Transfer Part (MTP)2 - User Adaption Layer (200731 bytes)
- SS7 MTP3-User Adaptation Layer (M3UA) (255043 bytes)
- Stream Control Transmission Protocol Management Information Base using SMIv2 (91359 bytes)
- Stream Control Transmission Protocol Applicability Statement (26493 bytes)
- Signalling Connection Control Part User Adaptation Layer (SUA) (304792 bytes)
- Telephony Signalling Transport over SCTP applicability statement (41358 bytes)
- SS7 MTP2-User Peer-to-Peer Adaptation Layer (90752 bytes)
- SS7 MTP3-User Adaptation Layer (M3UA)/Management Information Base using SMIv2 (129205 bytes)
- V5.2-User Adaption Layer (V5UA) (41441 bytes)
- DPNSS/DASS 2 extensions to the IUA protocol (21903 bytes)
- M3UA Implementer’s Guide (31462 bytes)

SIGTRAN Request For Comments:

- Architectural Framework for Signaling Transport (RFC 2719) (48646 bytes)
- Stream Control Transmission Protocol (RFC 2960) (297757 bytes)
- ISDN Q.921-User Adaptation Layer (RFC 3057) (140327 bytes)
SIGTRAN latest doc’s/04-2003

Internet-Drafts:
Stream Control Transmission Protocol Management Information Base (81420 bytes)
Signalling Connection Control Part User Adaptation Layer (SUA) (313013 bytes)
Telephony Signalling Transport over SCTP applicability statement (45919 bytes)
SS7 MTP2-User Peer-to-Peer Adaptation Layer (111091 bytes)
SS7 MTP3-User Adaptation Layer (M3UA/Management Information Base using SMiv2 (130389 bytes)
V5.2-User Adaption Layer (V5UA) (43810 bytes)
DPNSS/DASS 2 extensions to the IA protocol (25309 bytes)
M3UA Implementor’s Guide (151875 bytes)
IUA (RFC 3057) Outstanding Issues (94923 bytes)
Security Considerations for SIGTRAN Protocols (25730 bytes)
GR-303 extensions to the IUA protocol (20644 bytes)

Request For Comments:
Architectural Framework for Signaling Transport (RFC 2719) (48646 bytes)
Stream Control Transmission Protocol (RFC 2960) (297757 bytes)
ISDN Q.921-User Adaptation Layer (RFC 3057) (140327 bytes)
Stream Control Transmission Protocol Applicability Statement (RFC 3257) (24198 bytes)
Signaling System 7 (SS7) Message Transfer Part (MTP2 - User Adaptation Layer (RFC 3331) (210807 bytes)
SS7 MTP3-User Adaptation Layer (M3UA) (RFC 3332) (265055 bytes)

Status of 2.4.2004 at 9.05

Internet-Drafts:
Stream Control Transmission Protocol Management Information Base (82783 bytes)
Signalling Connection Control Part User Adaptation Layer (SUA) (930856 bytes)
Telephony Signalling Transport over SCTP applicability statement (45839 bytes)
SS7 MTP2-User Peer-to-Peer Adaptation Layer (110151 bytes)
SS7 MTP3-User Adaptation Layer (M3UA/Management Information Base using SMiv2 (110167 bytes)
V5.2-User Adaption Layer (V5UA) (46598 bytes)
DPNSS/DASS 2 extensions to the IA protocol (25954 bytes)
M3UA Implementor’s Guide (142894 bytes)
Security Considerations for SIGTRAN Protocols (28320 bytes)
ISDN Q.921-User Adaptation Layer (154710 bytes)

Request For Comments:
Architectural Framework for Signaling Transport (RFC 2719) (48646 bytes)
Stream Control Transmission Protocol (RFC 2960) (297757 bytes)
ISDN Q.921-User Adaptation Layer (RFC 3057) (140327 bytes)
Stream Control Transmission Protocol Applicability Statement (RFC 3257) (24198 bytes)
Signaling System 7 (SS7) Message Transfer Part (MTP2 - User Adaptation Layer (RFC 3331) (210807 bytes)
SS7 MTP3-User Adaptation Layer (M3UA) (RFC 3332) (265055 bytes)

http://www.ietf.org/html.charters/sigtran-charter.html