SCTP/SIGTRAN & SS7 Overview

April 2nd, 2008

Michael Tüxen

Wireshark Core Developer

SHARKFEST **'08**
Foothill College
March 31 - April 2, 2008

Outline

- Signaling System Number 7 (SS7).
- SS7 over IP.
- SIGTRAN Protocol Suite.
- Stream Control Transmission Protocol (SCTP).

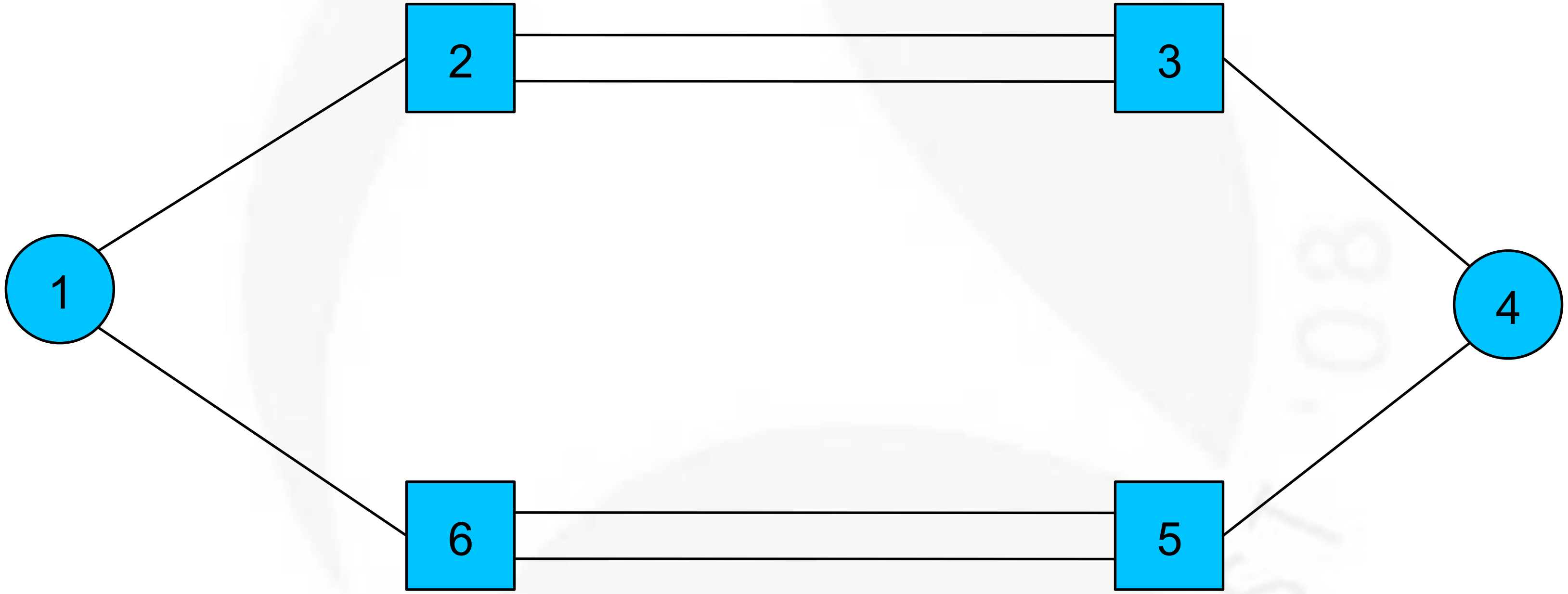
Signaling System Number 7

- A protocol suite used for classical telephony signaling.
- Standardized by the ITU and country specific variants by local standards bodies.
- It uses four levels:
  - MTP 1
  - MTP 2
  - MTP 3
  - User Parts

Some SS7 concepts

- Nodes are addressed by point codes.
- Links have limited bandwidth, typically 56/64 kbit/sec.
- Two adjacent nodes are connected by at most 16 links.
- Loadsharing is done based on SLS.
- Each MSU contains OPC, DPC, SLS.
- Defined failover proceduces.

Example SS7 network



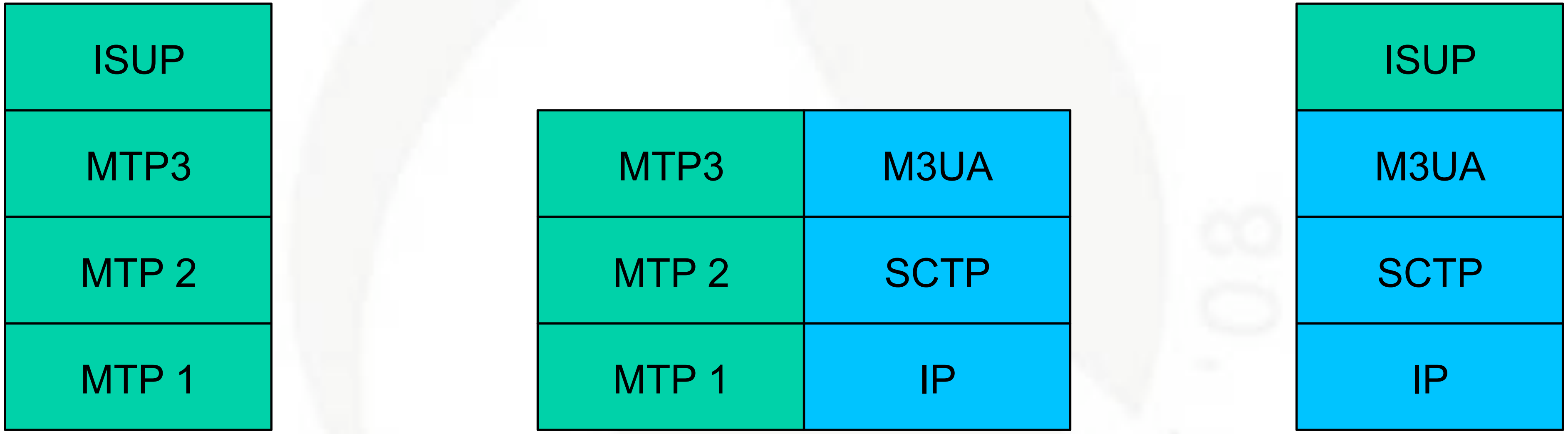
SS7 and Wireshark

- Wireshark supports a lot of SS7 protocols.
- Different protocol versions are supported:
  - ANSI
  - ITU
  - Japanese
  - Chinese
- The version is selected in Edit/Preferences/MTP3, even for SS7 protocols other than MTP3.

SS7 over IP

- Integrate IP-based nodes into the SS7 network.
- No special hardware requirements for the IP-based nodes.
- Interworking at different protocol layers.
- A common transport protocol is used.
- Similar performance requirements as the classical SS7 network:
  - Minimize end-to-end delay.
  - Short failover time in case of network failures.

M3UA example



ISUP
MTP3
MTP 2
MTP 1

SS7-based node

MTP3	M3UA
MTP 2	SCTP
MTP 1	IP

Signaling Gateway

ISUP
M3UA
SCTP
IP

IP-based node

SIGTRAN Protocols

- Several protocols are specified:
  - M2UA
  - M3UA
  - SUA
  - M2PA
  - IUA
- All protocols are supported by Wireshark (some in different versions depending on deployment)
- Some fields are affected by the SS7 preferences.

SIGTRAN Protocol Concepts

- All *UA are asymmetric.
- M2PA is something like a symmetric IP-based MTP-2 link.
- The *UA use a cluster concept to handle host failures with similar messages.
- M3UA is the protocol mostly deployed.
- All adaptation layers use the same transport protocol for reliable message transfer.

Stream Control Transmission Protocol

- Supports unicast
- Packet oriented
- Connection oriented
- Reliable Transport
- Flow and congestion control
- Supports multiple streams
- Supports multihoming
- Supports bundling of multiple user messages.
- Fragmentation and reassembly.

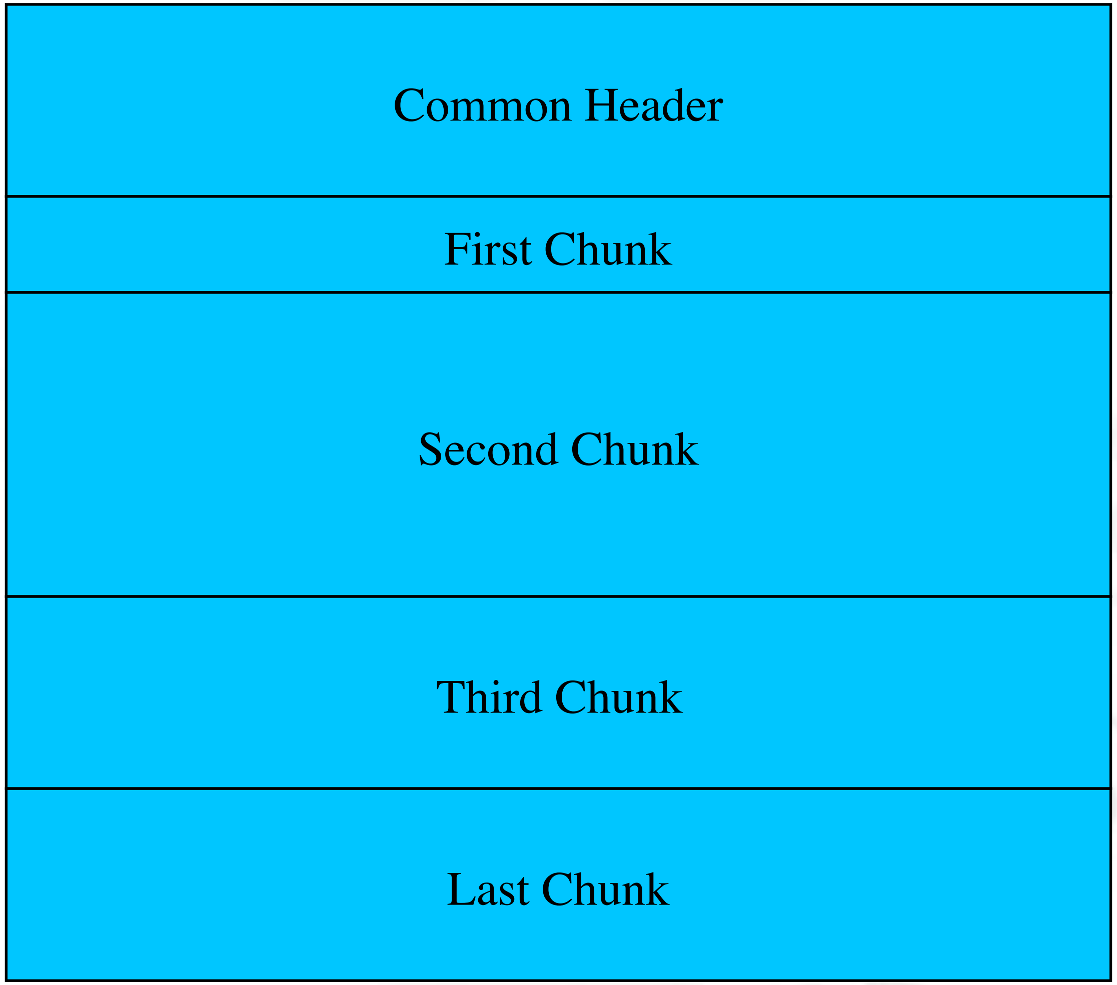
SCTP Terminology

- An SCTP connection is called an association.
- SCTP uses the port number concept of TCP and UDP.
- An SCTP endpoint can be identified by a pair of a list of IP-addresses and a port number.

Availability of Implementations

- Integrated in FreeBSD 7.
- For Linux: Part of 2.6 kernels and even back-ported to 2.4 kernels.
- Integrated in Solaris 10.
- For BSD Unix, Linux, Solaris, Mac OS X, HP-UX and Windows: sctplib (userland library).
- Several commercial implementations.
- Integrated in almost all SS7 nodes.

SCTP Message Format



Common Header

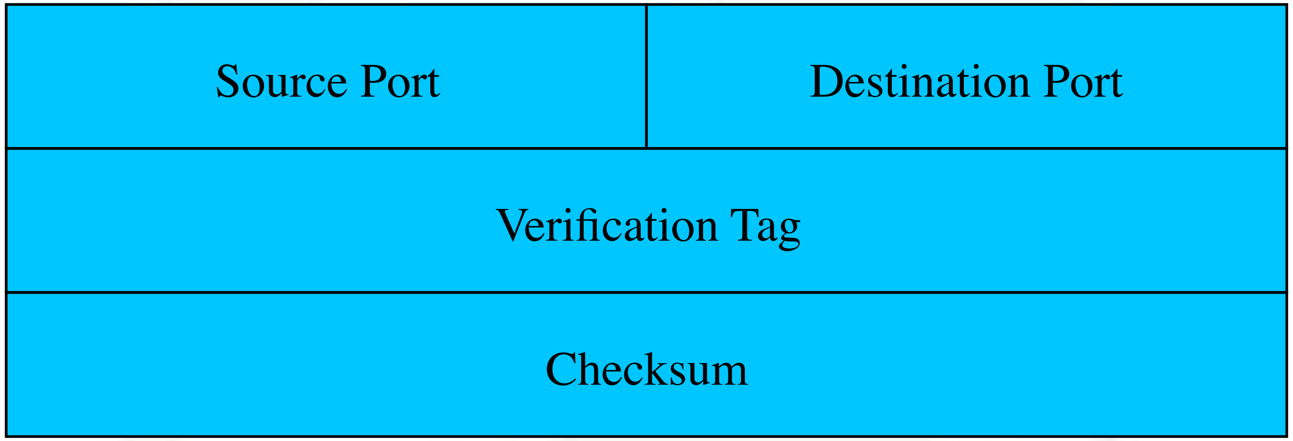
First Chunk

Second Chunk

Third Chunk

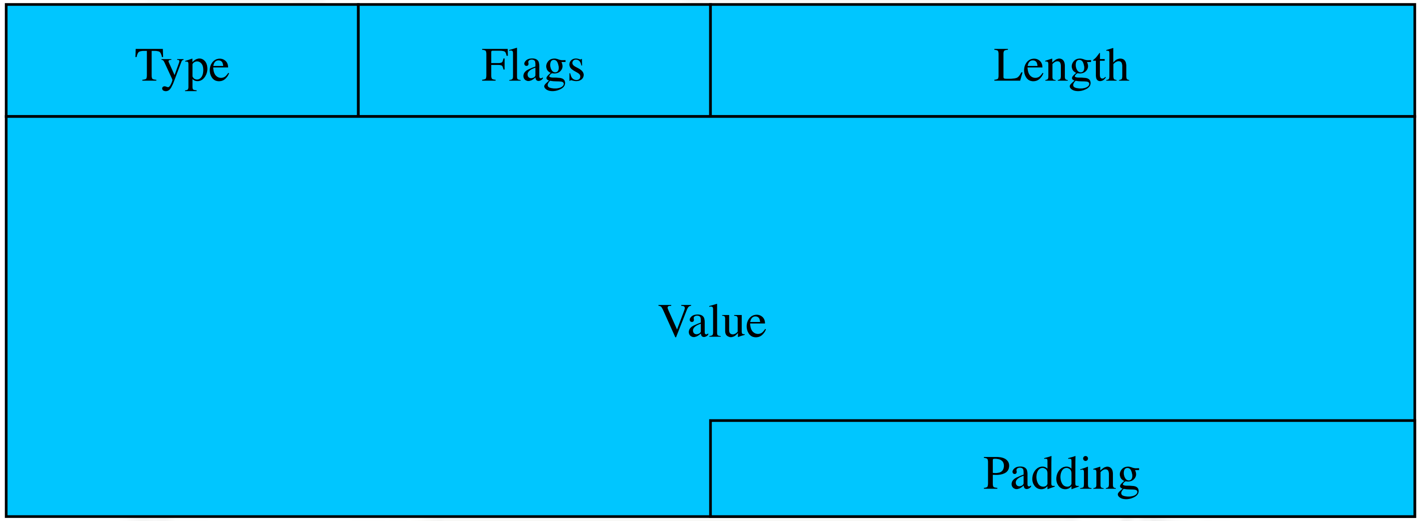
Last Chunk

SCTP Common Header Format



Source Port	Destination Port
Verification Tag	
Checksum	

SCTP Chunk Format



Type

Flags

Length

Value

Padding

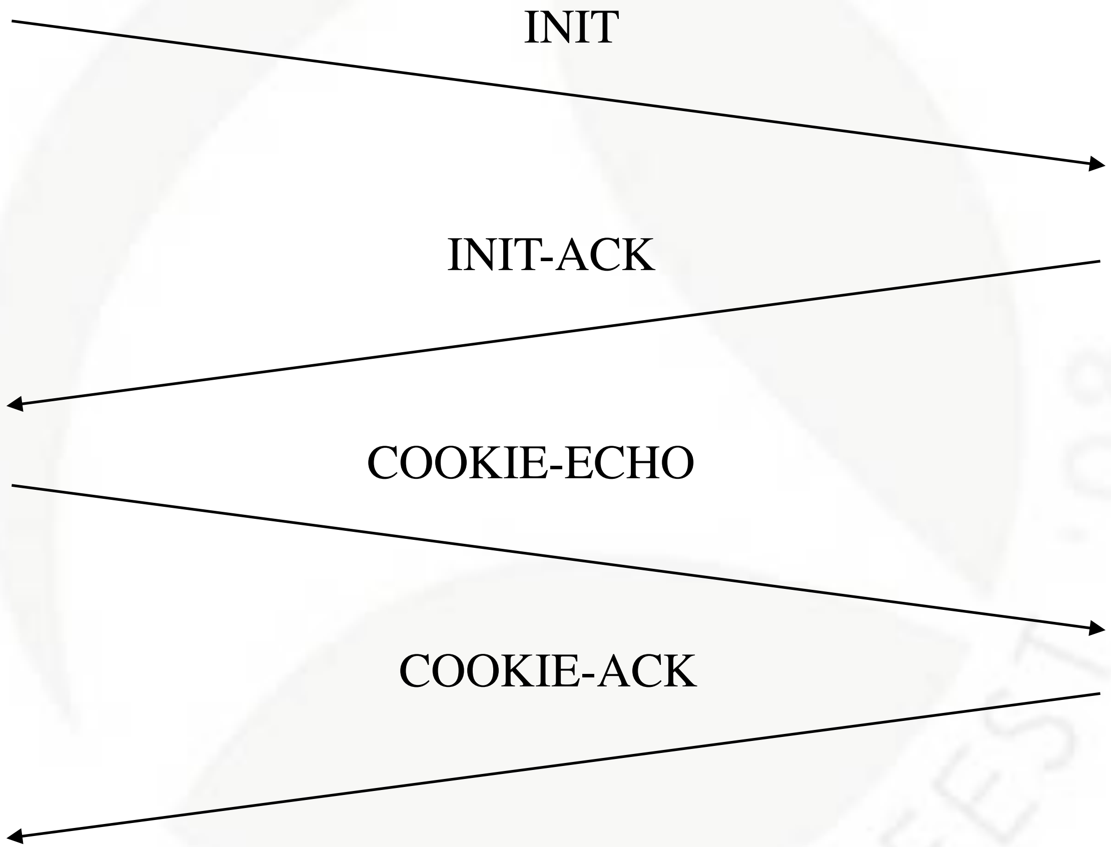
SCTP Chunk Types

- INIT, INIT-ACK, COOKIE-ECHO, COOKIE-ACK.
- DATA, SACK.
- SHUTDOWN, SHUTDOWN-ACK, SHUTDOWN-COMPLETE.
- HEARTBEAT, HEARTBEAT-ACK.
- ERROR, ABORT.
- FORWARD-TSN.
- ASCONF, ASCONF-ACK.
- AUTH.

Association Setup

- Peer to Peer Model.
- Four way handshake is used.
- Verification tags are exchanged.
- Maximal receiver window is exchanged.
- The number of streams are negotiated and can be different in each direction.
- The IP addresses of each endpoint are exchanged.
- The procedure is protected against ‚blind attacks‘.

Message Flow



The Role of the Verification Tag

- It is a 32-bit random number.
- It is chosen by each end-point.
- The protection against blind attackers is based on the verification tag.
- It stays the same during the lifetime of an association.
- Some implementations use it for looking up the association.
- If a packet is received with a wrong verification tag it is silently discarded.

Support of Multihoming

- Every IP address of the peer is considered as a path.
- All paths are continuously supervised and initially confirmed.
- One path, the so called primary path, is used for initial data transmission.
- In the case of (timer based) retransmissions an alternate path is used.
- Loadsharing is not part of RFC 4960 but subject of ongoing research.

Partial in-sequence delivery

- A lot of applications do not require all data to be delivered in sequence.
- Therefore SCTP supports the streams concept. Only data sent within the same stream is delivered in sequence relative to that stream.
- This minimizes the impact of head of line blocking in case of message loss.

Partial Reliability

- The sender has the capability of notifying the receiver that a particular DATA chunk will never arrive at the receiver.
- PR-SCTP is a general concept.
- Applications:
  - Data may have a limited life time.
  - Data may have one of several priorities and share a resource.
  - Data may only be transmitted a limited number of times.
- An extension of the protocol.

Address Reconfigration

- Reliable systems must be reconfigured without interruption of the service.
- ADDIP allows to delete and add IP-addresses during the lifetime of an association.
- For example, it supports IPv6 renumbering.
- Security is based on SCTP-AUTH.
- IP-addresses are transported inside ASCONF chunks.

Wireshark Support for SCTP

- SCTP is supported including all standardized extensions.
- Finding all packets of an SCTP association is harder than finding packets of a TCP connection.
- A verification tag based heuristic is used for association analysis.
- Graphing capabilities.
- Payload detected by payload protocol identifier and port numbers.
- Reassembly.

Conclusion

- SS7 can be transported over IP.
- SCTP is a generic transport protocol having a lot of interesting features.
- Wireshark
  - supports these protocols.
  - Has excellent support for SCTP.