

# NAT and SCTP

Randall Stewart ([rrs@cisco.com](mailto:rrs@cisco.com))

Michael Tüxen ([tuexen@fh-muenster.de](mailto:tuexen@fh-muenster.de))

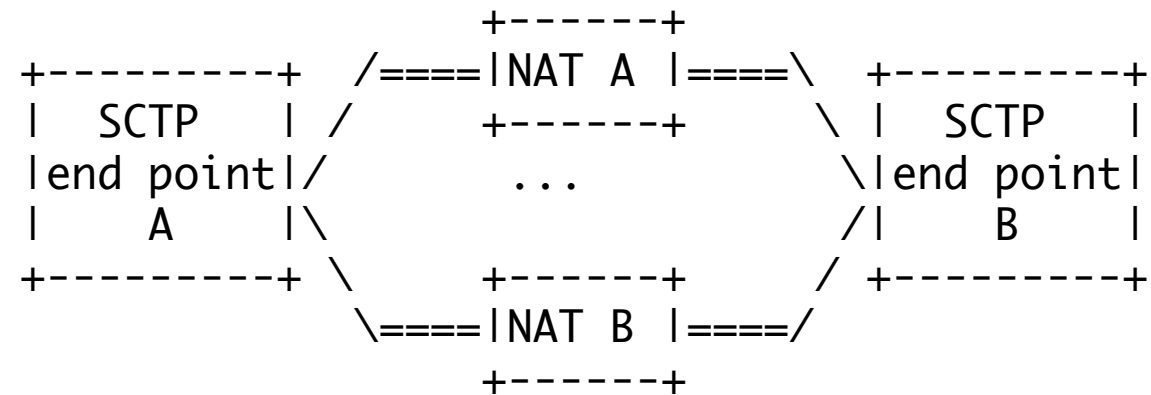
# Internet Drafts

- <http://www.ietf.org/internet-drafts/draft-xie-behave-sctp-nat-cons-03.txt>  
defines some terminology.
- <http://www.ietf.org/internet-drafts/draft-stewart-behave-sctpnat-03.txt>  
defines an SCTP aware NAT.

# Single Point Traversal

```
+-----+
| SCTP | +-----+ +-----+ | SCTP | | | | | |
|end point|===| NAT |=:|=| NAT |===|end point|
| A | +-----+ +-----+ | B |
+-----+ +-----+
```

# Multi Point Traversal



# General Considerations

- Changing part of an SCTP packet requires the complete recalculation of the CRC32C checksum.
- Changing the port number (like in NAT) requires a synchronization between NAT engines on different paths.

# SCTP Specific Variant of NAT

- NAPT uses client side port numbers to distinguish multiple clients behind a NAT using the same local port number and talking to the same server.
- The method proposed in draft-stewart-behave-sctpnat-03.txt uses the verification tag for this.
- This is an SCTP aware NAT with NAPT capabilities.
- Port numbers and therefore packets do not need to be changed.

# Handling Local Port Number Collisions

- If two clients behind the NAT use the same port number talking to the same SCTP endpoint, the later association looks like a restart of the earlier one from the server perspective.
- Add a NAT-supported parameter, which disables the restart feature and allow multiple associations between two SCTP end-points.

# Handling of Local Port Number and Verification Tag Collisions

- There is nothing which can be done here... But it is not likely, since two  $14+32 = 46$  bit random numbers have to match.
- The middlebox can send an ABORT using an M-bit indicating that the client has to reinitiate the association.



# Question

- Any technical questions?
- Can the IDs be adopted as WG items?