

SCTP and NAT

draft-stewart-behave-sctpnat-04.txt

Randall Stewart (rrs@lakerest.net)

Michael Tüxen (tuexen@fh-muenster.de)

Irene Rüngeler (i.ruengeler@fh-muenster.de)

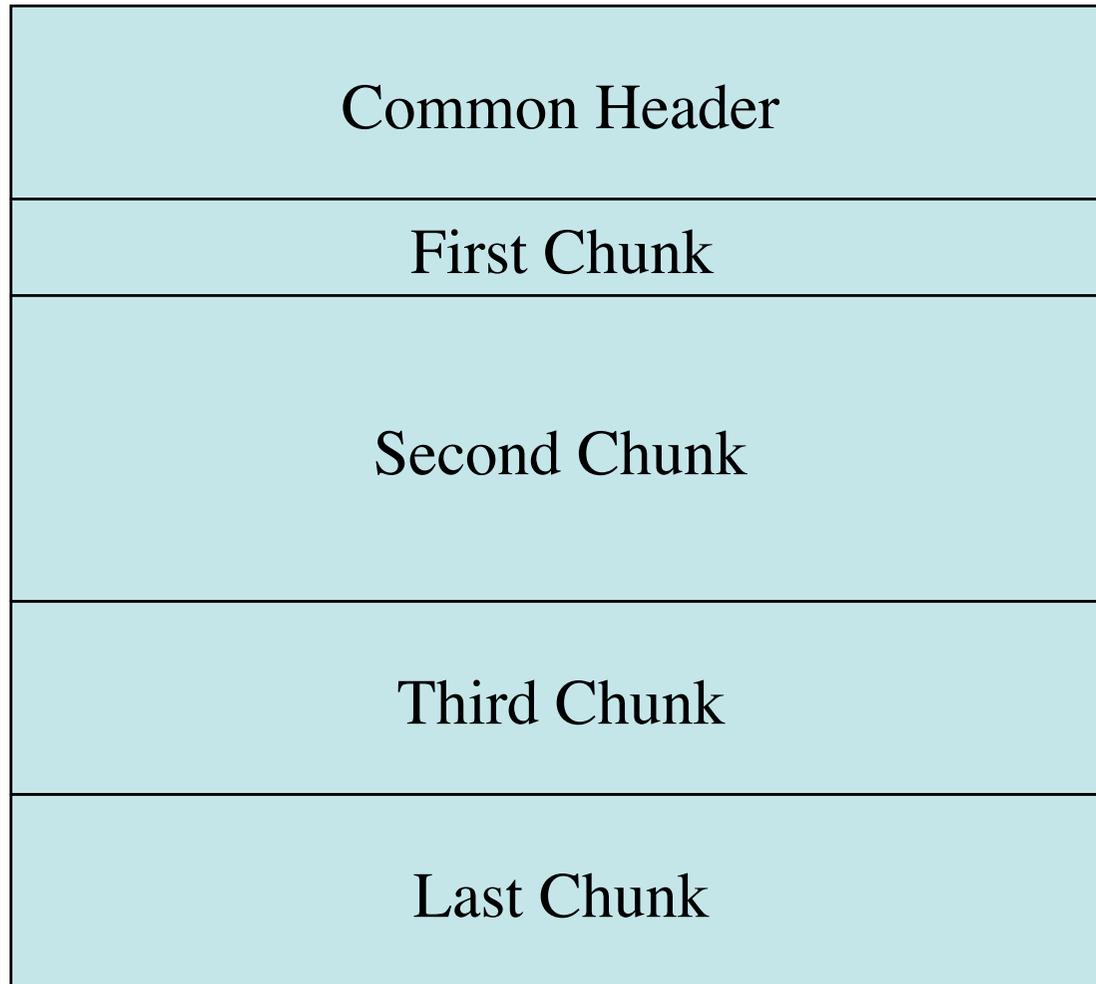
A Misperception

- Doing NAT for SCTP is hard, because ...
- ... is wrong!
- Doing NAT for SCTP appropriately is simple.
- SCTP is actually NAT-friendly because it has something like a connection identifier.

“Classical” NAT and SCTP

- One can use the same concept for SCTP as for TCP and UDP.
- In contrast to UDP or TCP one has to recompute the checksum over the whole packet.
- Works pretty well in the singlehomed case.
- Does not extend to the multihomed case.
 - Dealing IP-addresses in the IP payload.
 - Port number synchronization.
- So do NOT use this!

Message Format



Common Header Format

Source Port	Destination Port
Verification Tag	
Checksum	

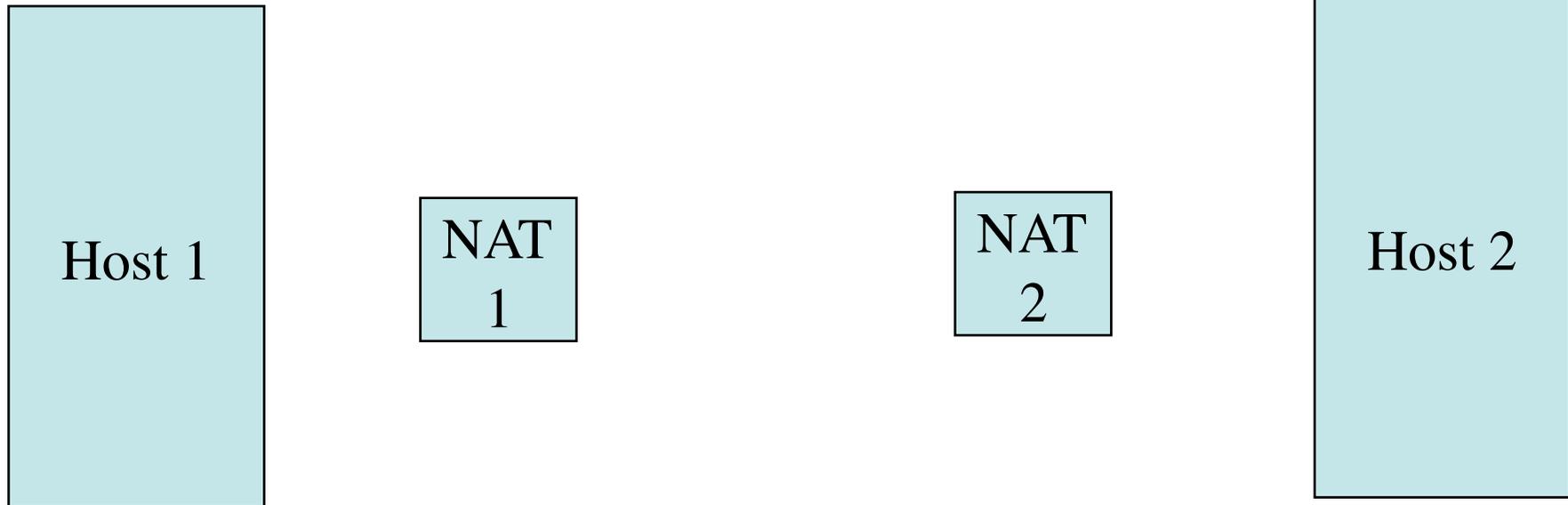
The role of the verification tag

- 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.

A NAT with NAPT capabilities for SCTP

- Does not use the port numbers to identify the SCTP association, but the verification tag.
- The IP address is modified based on the port numbers and the verification tag.
- No recalculation of the checksum is necessary.
- No change of the port number is required.
- If an ephemeral port number is used one has a $32+14 = 46$ bit random number for identifying the association.
- Every packet contains only one verification tag (except for the INIT-ACK).

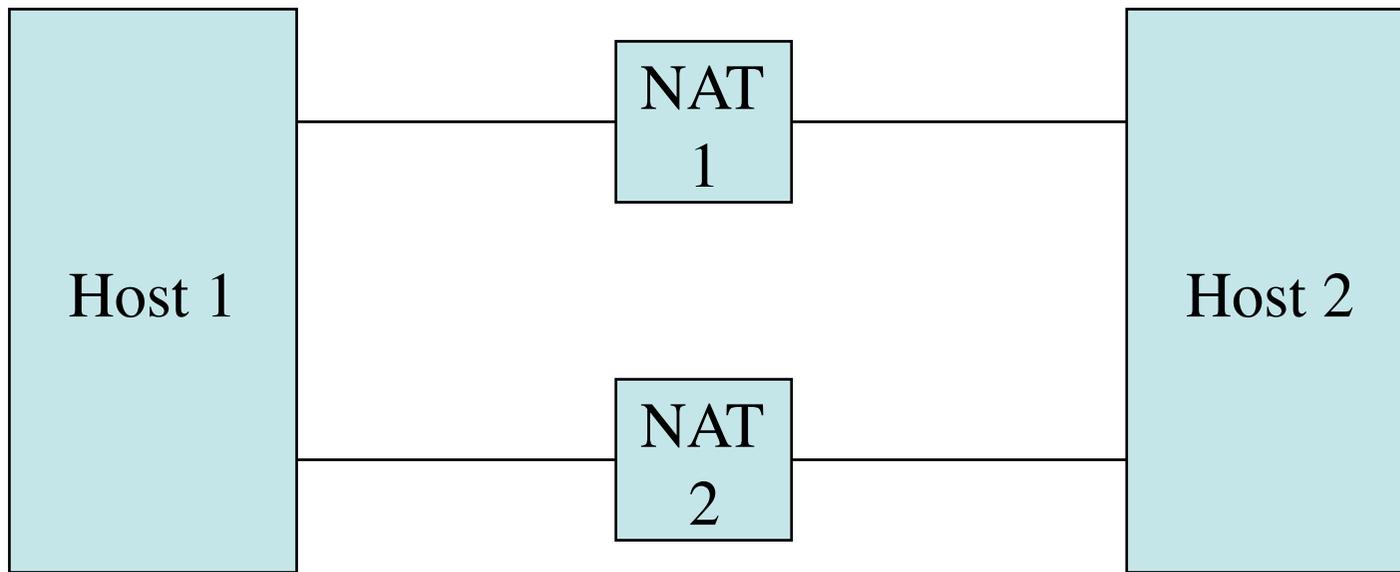
Peer to Peer



SCTP aware NAT in case of Peer to Peer communication

- Uses simulations association setup, INIT-collision procedures.
- The outgoing INITs punch a hole.
- There are special rules for letting INITs from outside in.
- This is standard SCTP behavior.

Multihoming



SCTP aware NAT in the multihoming case

- Port number synchronizing is no problem.
- Embedded IP-addresses are a problem.
- The principle:
 - Setup the association as a single homed one.
 - Add the other addresses with ADD-IP.
 - Use special addresses (0.0.0.0, for example) inside the ASCONF chunks to refer to the source address.
 - Use the verification tag to find the association.
 - Put the other verification tag in the ASCONF.

NAT without states

- A NAT box can request the state in case of
 - It lost its state
 - It is new in the path due to routing changes
- The endpoint will provide the necessary information.
- This procedure is using ADD-IP.