RFC4787, 5508, 5382 bis (a.k.a NAT RFCs) Updates

repenno@cisco.com

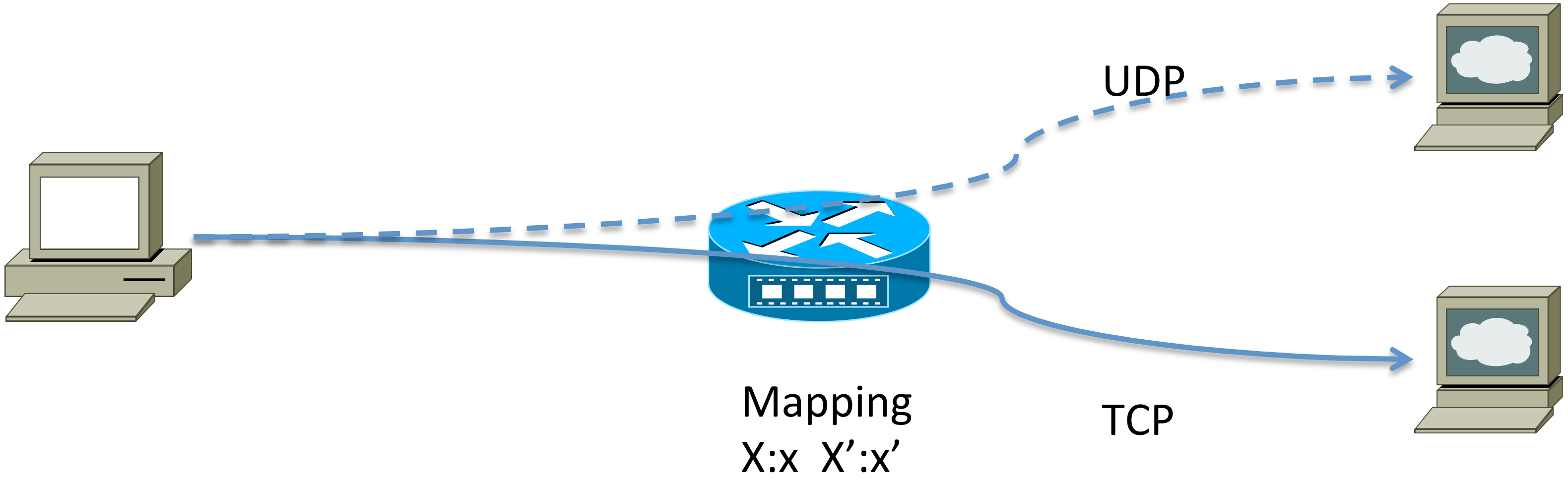
IETF84 – Vancouver

R. Penno, S. Perreault, S. Kamiset, M. Boucadair

Purpose

- Proposes fixes to current NAT44 RFCs based on operational and implementation experience
- Some examples follow. See draft for complete list.

EIM Protocol Independence

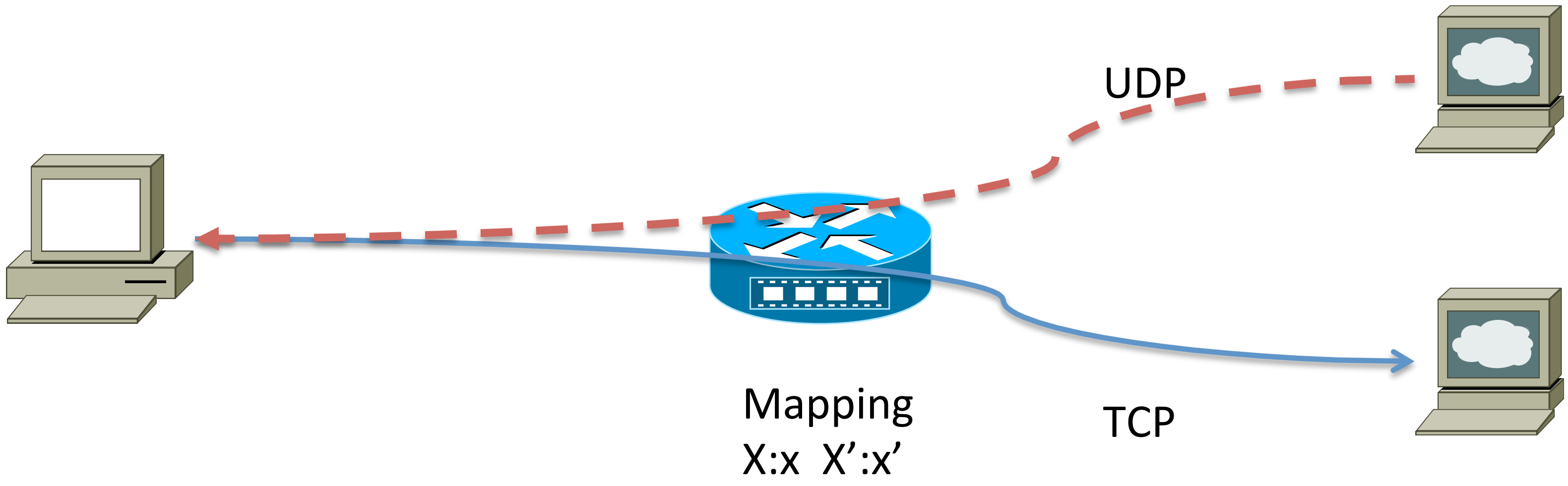


UDP

Mapping
X:x X’:x’

TCP

EIF Protocol Independence

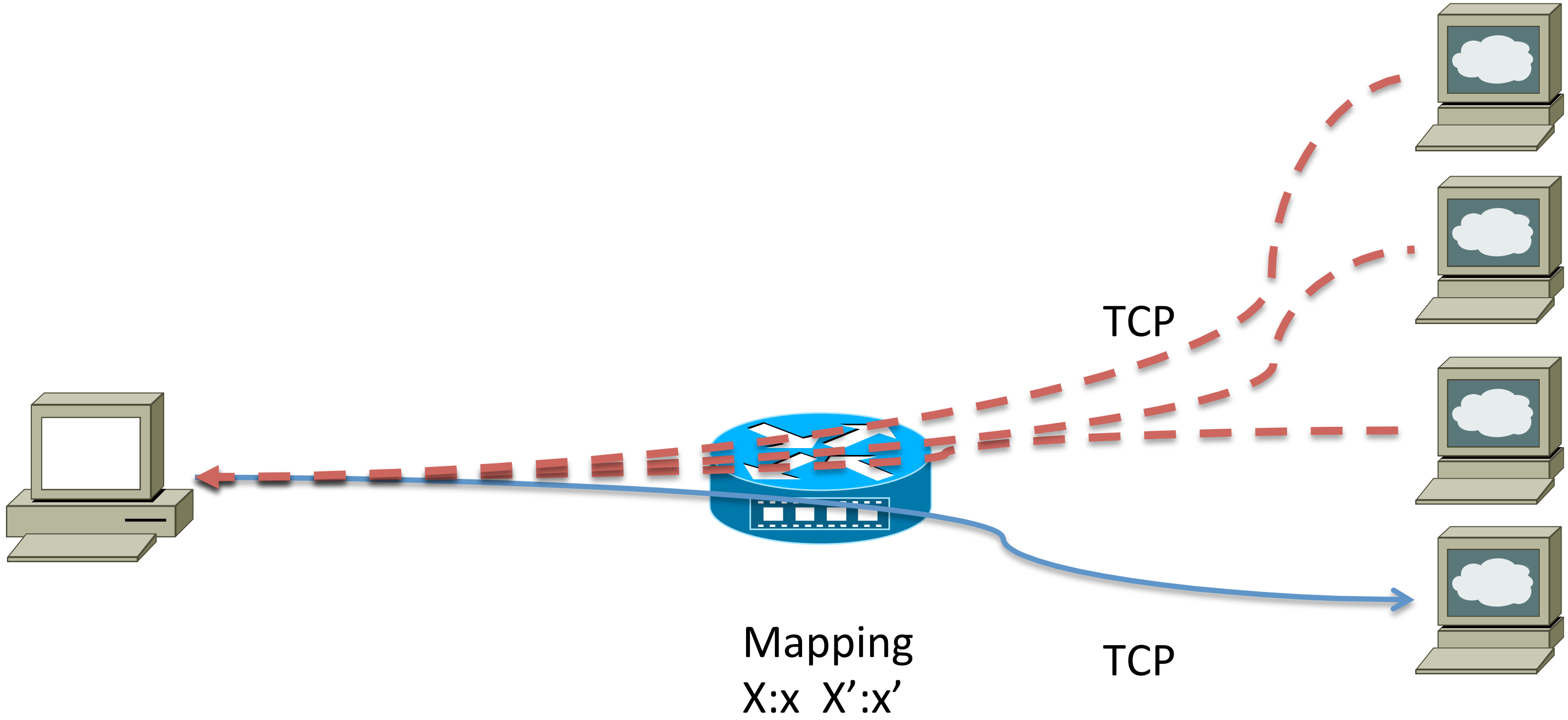


UDP

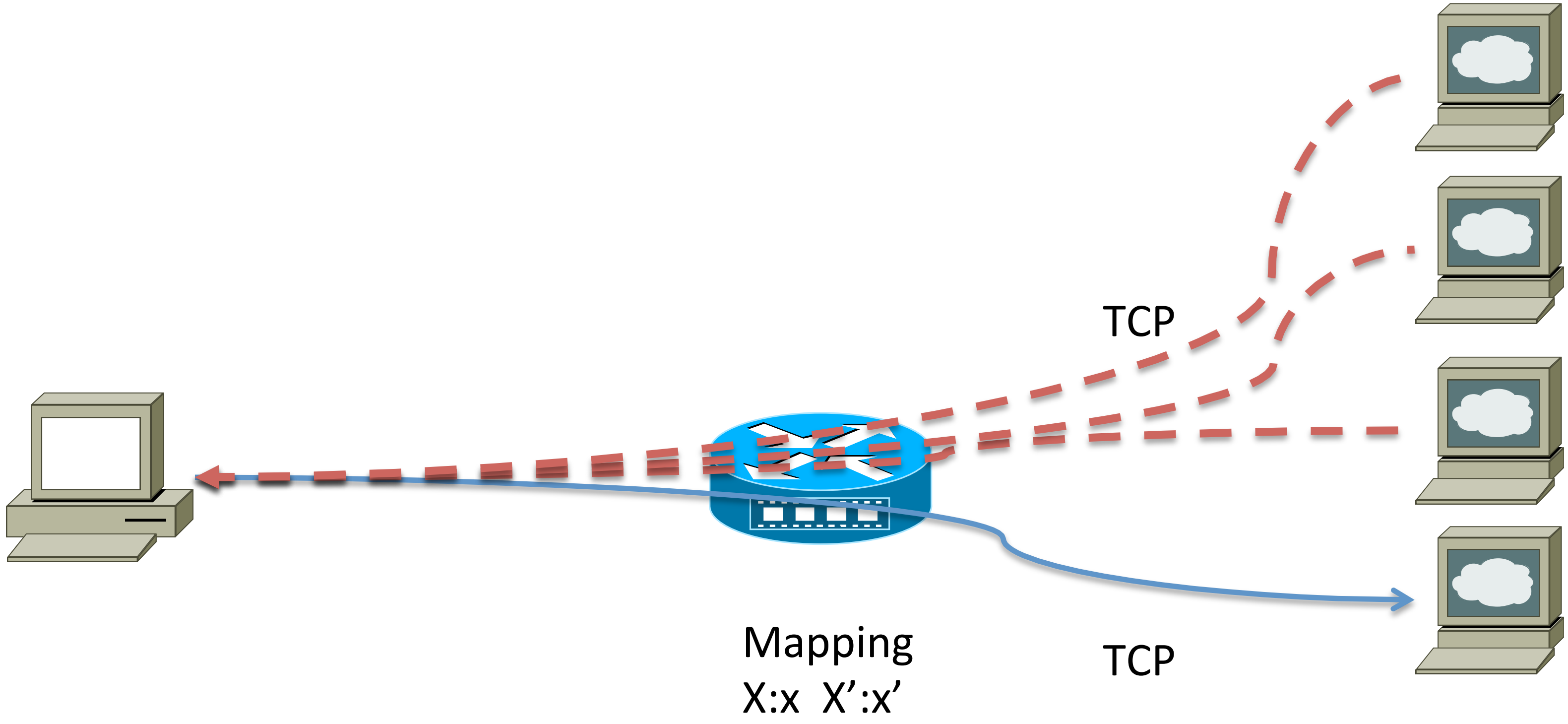
Mapping
X:x X’:x’

TCP

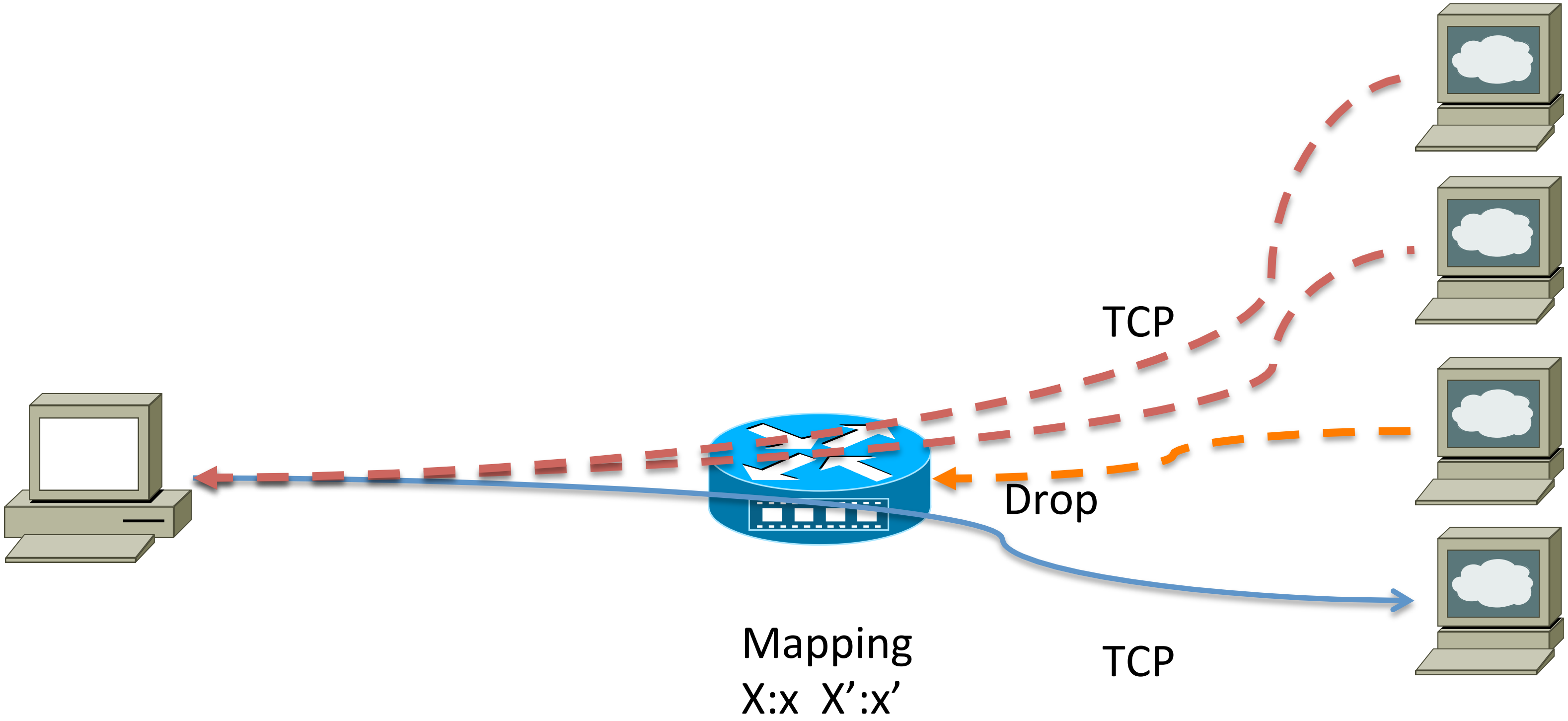
EIF Protocol Security



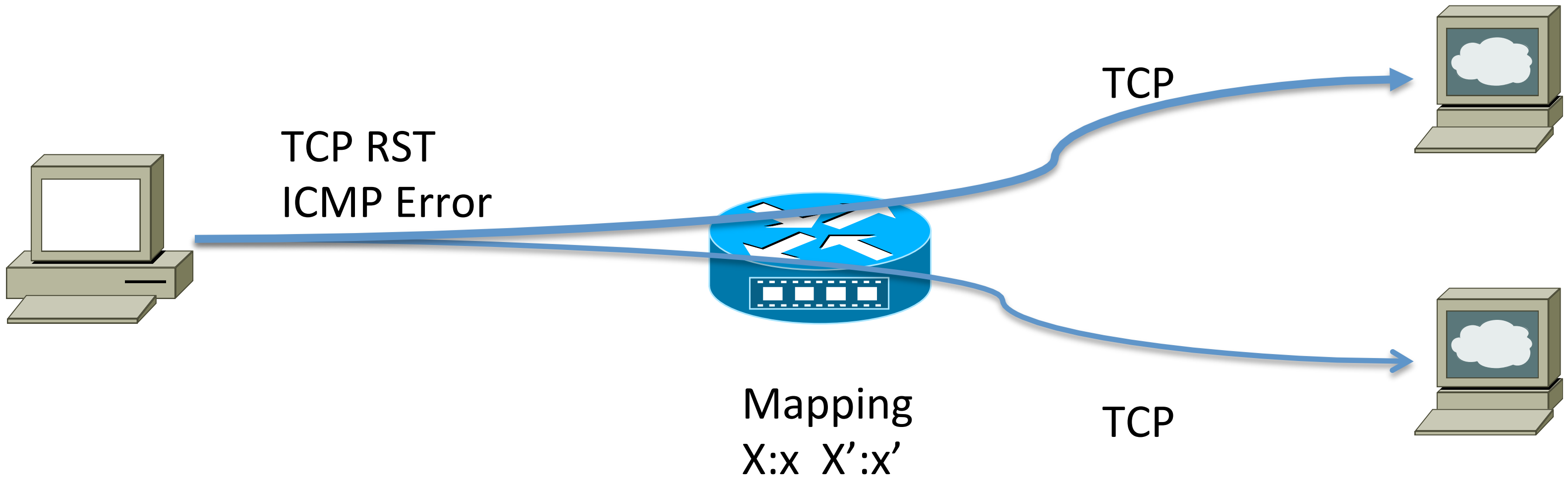
EIF Protocol Security



EIF Mapping Refresh



Outbound Refresh and Error Packets



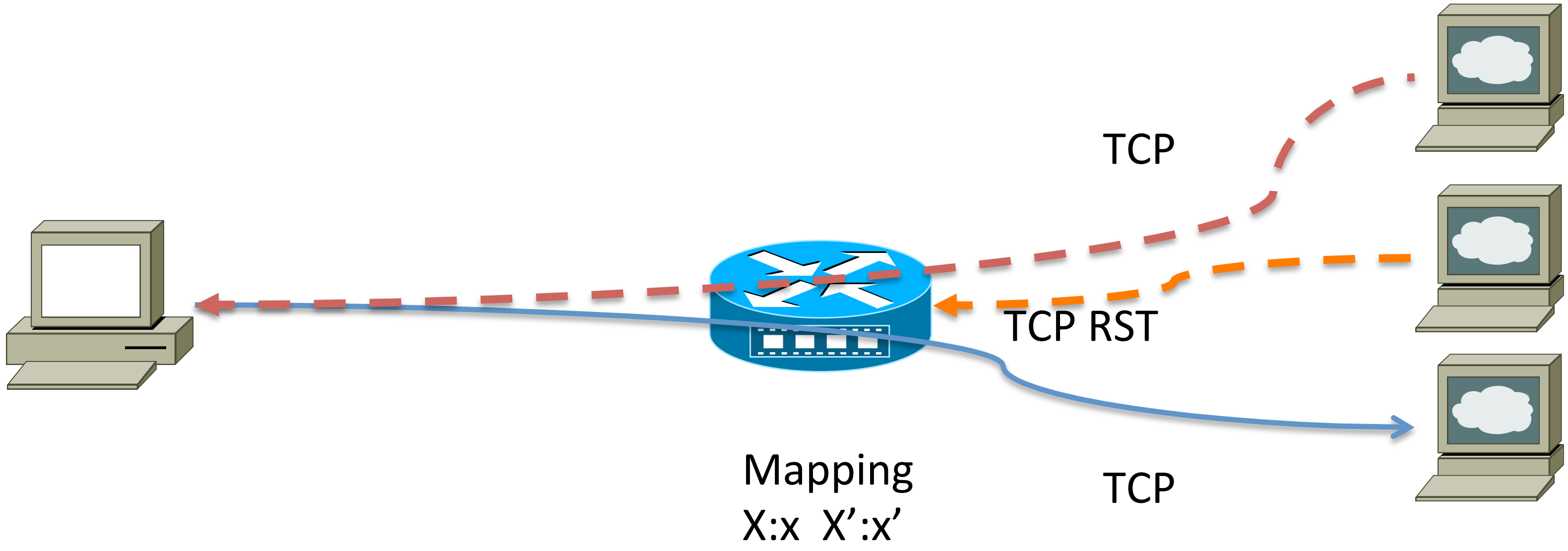
TCP RST
ICMP Error

TCP

TCP

Mapping
X:x X’:x’

TCP RST Processing



S2I: Forward and remove Session Immediately (anti-spoofing rules in place).
I2S in EST state: Forward, wait 4 minutes for S2I ACK or FIN packets.
Otherwise many attacks possible : Acceptable TCP RST followed by any packet
I2S in TRANS state: Forward and remove Session Immediately (anti-spoofing rules in place).

Other TCP

- Different timers for opening and closing TRANS state
- Ability to reduce opening TRANS to less than 4 minutes
  - There are other initiatives to reduce reclaim state at NAT devices faster [I-D.naito-nat-resource-optimizing-extension]

APP

- Address Pooling Paired behavior for NAT is recommended in previous documents but behavior when a public IPv4 run out of ports is left undefined.
- Drop new sessions?
- Move to another public IP? Only that one session? Or all sessions afterwards?

Others

- Drop port parity requirement
- Port randomization
- IP-ID field
- ICMP Mapping timeout vs. ICMP Session Timeout (similar to TCP).