

# NAT Behavioral Requirements for Unicast TCP

Saikat Guha, Kaushik Biswas, Bryan Ford, Paul  
Francis, Senthil Sivakumar, Pyda Srisuresh

draft-ietf-behave-tcp-00

IETF 65

# Overview

- ▶ Based on draft-hoffman-behave-tcp-03
- ▶ Incorporates IETF 64 and mailing-list discussion
- ▶ Three basic goals/requirements:
  1. Allow TCP simultaneous open
  2. Specify response to unsolicited SYN
  3. Minimum timer values and mapping expiry

# Requirement 1

## REQ-1: WG Consensus

**MUST** have endpoint independent mapping behavior

- ▶ Require so-called *cone* behavior
- ▶ Change from hoffman-03: explicit addition

# Requirement 2

## REQ-2: WG Consensus

**MUST** support TCP Simultaneous-Open  
(and other TCP corner cases)

- ▶ Standards compliant stacks should always work
- ▶ Change from hoffman-03: no FIN discussion

# Requirement 3

## REQ-3: WG Consensus Likely

**MUST** support inbound SYN/3-way from specific endpoints (based on endpoint filtering)

- ▶ Define behavior for so-called *restrictive cone* and *full cone*
- ▶ Change from hoffman-03: explicit addition

# Requirement 4

## REQ-4: WG Consensus

**SHOULD** silently discard unhandled inbound SYN

- ▶ Helps TCP NAT Traversal
- ▶ Change from hoffman-03: no mention of ICMP

# Requirement 5

## REQ-5: WG Consensus Likely

**RECOMMENDED** 2 hour idle timeout. 4 minutes for unestablished sessions. **MAY** be configurable.

- ▶ RFC 1122 values. Aligned wording with UDP
- ▶ Change from hoffman-03: now configurable

# Open Issues

## Application Level Gateways

- ▶ Are ALGs in-scope? (they are for UDP)
- ▶ Should FTP default to on?
- ▶ Anything else that should be on? IRC?
- ▶ Other ALGs default to off?



# Summary

- ▶ Requirements (WG consensus on all):
  1. MUST: endpoint independent mapping
  2. MUST: fully support TCP spec.
  3. MUST: have consistent endpoint filtering
  4. SHOULD: silently discard SYN-in
  5. SHOULD: use RFC 1122 timers.
    - 5.1 MAY: be configurable
- ▶ Security considerations updated
- ▶ Open Issue: ALGs

Questions?