draft-ford-shared-addressing-issues-01

M. Ford (Ed.), P. Roberts (Internet Society)
M. Boucadair, P. Lévis (France Telecom)
A. Durand (Comcast)

Purpose of the document

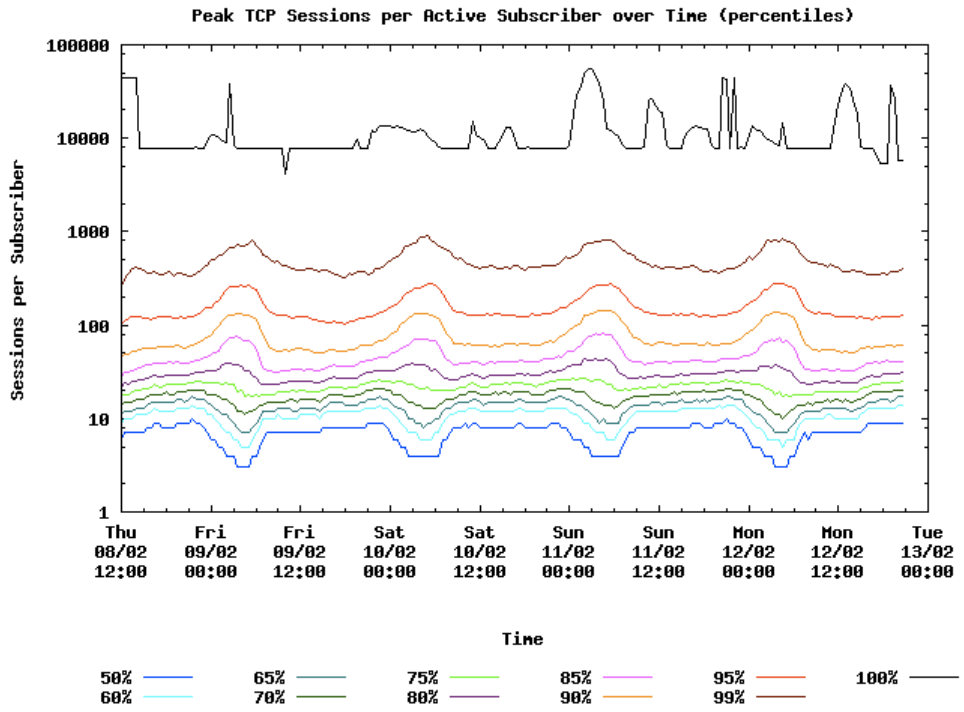
- Lots of documents specifying address sharing solutions
  - AplusP, NAT44, DS-lite, etc.
- Capture the issues that address sharing (in any form) creates, document them in one place
- Not about picking winners
- Not intended to get into detailed solution-specific discussions

Taxonomy

- CGN-based solutions
  - Introduce NAPT function in ISP network (CGN)
  - Subscribers allocated private addresses
  - Pool of public addresses resides at CGN
- Port-range solutions
  - Avoid use of CGN
  - Subscribers allocated public addresses with restricted port range
  - Introduces Port Range Routers

Background

- Long-tail of subscribers requiring >median number of ports



Source: http://www.wand.net.nz/~salcock/someisp/flow_counting/result_page.html

Service providers need to balance:

- Subscriber/address ratio
- Port churn
- Logging, traceability, signalling load

Port negotiation

- UPnP or NAT-PMP relays where there is only one layer of NAT
- Web interface to open incoming ports
  - This makes a previously private interface public
- For port-range solutions, port forwarding capabilities may still be present at CPE
  - Incoming port must be within allocated range

Impact on applications

- Breaks applications that
  - Establish inbound communications
  - Carry address and/or port information in their payload
  - Use fixed ports
  - Do not use any port (ICMP)
  - Assume uniqueness of source address
  - Explicitly prohibit concurrent connections from identical addresses

Application Layer Gateways

- Many current CPE embed ALGs to enable applications to operate correctly in the presence of NAT
- CGNs will render subscribers dependent on the set of ALGs available on the CGN
- Port-range solutions may require modifications to ALGs to accommodate port-range restriction

ICMP

- Sourcing ICMP from hosts behind an address-sharing solution is unproblematic
- Inbound ICMP sourced off-net
  - Will break
  - In response to outbound, could use ICMP ID value to correlate
- Inbound ICMP sourced on-net
  - Routed normally for CGN-based solutions
  - ICMP unroutable without special handling

Other issues

- Fragmentation
- Multicast
- Mobile-IP
- Single Point of Failure (for stateful address-sharing solutions)

Security-related issues

- Port randomisation
- Abuse logging, penalty boxes
  - Need to log source port as well as source address
- Spam
- IPsec
- Policing forwarding behaviour
- Authentication

Geo-proximity, geo-location

- Conforming with regional content licensing restrictions
- Targeting advertising
- Customising content
- Shared addressing may reduce level of confidence and location granularity
- Application performance may be effected in the presence of highly centralised CGN

Traceability

- Address sharing solutions must record and store all mappings they create
  - Potentially very large volume of data
  - Pre-allocating groups of ports mitigates
  - Trade-offs between
    - size of pre-allocated groups
    - ratio of public addresses to subscribers
    - Impact on logging requirements
    - Port randomisation security

Concluding

- Are there additional issues to include?
- Presentations this week in
  - softwires, behave, and intarea
- Hope to conclude a route toward publication by the end of the week
- Solution documents should then reference