Dual-stack lite

draft-durand-softwire-dual-stack-lite-01

A. Durand, R. Droms,
B. Haberman, J. Woodyatt
Router-based scenario:
Home router is provisioned with IPv6 on WAN and tunnel concentrator address; provides IPv4 transport for the home PC

IPv6 packet
IPv6 src: IPv6 address of home gateway (IGD)
IPv6 dst: IPv6 address of tunnel concentrator
IPv4 src: 192.168.1.3
IPv4 dst: www.nanog.org (198.108.95.21)
IPv4 src port: 1001
IPv4 dst port: 80

IPv4 packet
IPv4 src: from the pool of the ISP
IPv4 dst: www.nanog.org (198.108.95.21)
IPv4 src port: 45673
IPv4 dst port: 80

NAT binding
INSIDE:
IPv6 src: IPv6 address of home router + 192.168.1.3 + port 1001
OUTSIDE:
IPv4 src address: from pool of the ISP + port 45673

PC 192.168.1.3 SRC port 1001
Host-based scenario:
Dual-stack capable host is provisioned with IPv6 and tunnel concentrator address; IPv4 in host stack for applications

**IPv6 packet**
- IPv6 src: IPv6 address of host
- IPv6 dst: IPv6 address of tunnel concentrator
- IPv4 src: well known IPv4 address: (IANA defined)
- IPv4 dst: `www.nanog.org` (198.108.95.21)
- IPv4 src port: 1001
- IPv4 dst port: 80

**IPv4 packet**
- IPv4 src: from the pool of the ISP
- IPv4 dst: `www.nanog.org` (198.108.95.21)
- IPv4 src port: 45673
- IPv4 dst port: 80

**NAT binding**
**IN:**
IPv6 address of host + well known IPv4 address of end-node (IANA defined) + port 1001

**OUT:**
IPv4 src address: from pool of the ISP + port 45673
Changes since Dublin

• Merge of DS-lite & S-NAT
• CGN considerations
  – Port allocation discussion
    • No cookie cutter port allocation per customer for efficiency
    • control given to user on incoming ports (web page, DHCP...)
  – ALG discussion
  – 3rd party CGN
• Encapsulation (to be developed)
• Interface initialization (to be developed)
• IANA section to reserve a /30 IPv4 address block
Future developments

• Clarify encapsulation
  – IP/IP minimum to implement if no control is required
  – Use software encaps is any control is needed
• Reference port distribution work
• Reference tunnel endpoint DHCP option
• Reference interface encapsulation draft
  – to be written
• Define IANA reserved addresses
DS-lite Status

• IETF
  – Latest draft:
    • draft-durand-software-dual-stack-lite-01.txt (missed −00 deadline for WG work item)
    • Editorial changes to rev −00
      – IETF softwire WG has just been re-chartered to standardize DS-lite.
        • Target 1Q2009...

• Implementations
  – Router: Open source code (Open-WRT) for a Linksys router
  – CGN: Vendor code, open source project started
Tunnel-based solution

• Running a tunnel between the host or the home router and the CGN opens the door to several new things, simply by pointing the tunnel to the right place:
  – Placement of CGN where it makes sense
  – Use of well-known tunnel protocol (IP-in-IP)
  – Horizontal scaling of CGN
  – Use of 3rd party CGN (virtual ISP)
  – ...

2008-11-20
softwire WG - IETF 73
Questions?
Extra Slides
Common issues with address sharing

Things that DS-lite, SAM, A+P, NAT64, IVI & others must consider
Open issue 1: port reservation

- CGN are not the best place to implement ALGs
  - “The issue is not so much the placement of the NAT but the control of it” (Randy Bush).
  - Enable the end-node or the IGD to perform the ALG function, by reserving ports in the CGN
    - Dynamic: port mapping protocol between IGD & CGN (eg NAT-PMP)
    - Static: limited manual port reservation (web page?)
    - DHCPv4 option to allocate port numbers
- Port reservation algorithm need to be efficient
  - Difference between max # of port/customer & average # of port/customer
Open Issue 2: UPnP

• Apps that insist on running on a well-known port number (or port range) using UPnP to signal the home gateway

• Better semantic (NAT-PMP): ask for any mapping IPv4 address/port number

• This is true for any IPv4 address sharing mechanism, eg Double NAT, A+P, NAT64,...
Open Issue 3

- Logging IP address + time stamp is no longer enough to deal with abuse / lawful intercept.

- There is a need to adapt tools to log port numbers as well as IP addresses.

- Abuse mitigation on server side is more difficult
  - Can no longer put IP address in ‘penalty box’
Open issue 4

• All those solution involve tunneling or protocol header translation.
  – They change the packets size.

• How to account for the diminished MTU?
Conclusion

• IPv4 exhaustion is real. Moving to IPv6 is necessary.
  – Multiple layers of IPv4 NAT would make the network increasingly complex. Complexity implies fragility.

• Deploying “classic” dual-stack IPv4&IPv6 to all customers is not sustainable.
  – Provisioning with a global IPv4 address must remain an option (existing customers, value added service,...)

• IPv4 address sharing is required to deploy IPv6 at scale.
  – Such bridging technology need to be standardized and supported by vendors.