Simple Security in IPv6 Gateway CPE

james woodyatt <jhw@apple.com>

draft-ietf-v6ops-cpe-simple-security-00

What CPE Are We Talking About?

- Routers for home / small-office deployment.
- Provisioned by customer or by ISP.
- Typically integrated with IPv4/NAT.
- Acquires IPv6 service by tunnel or native.
- Routes to a global /64 on LAN bridge.

Simple Security for IPv4

- Driven by stateful filtering required by NAT.
- Outbound flows generally allowed.
- Inbound flows generally refused.
- Transparency helped by ALG as needed.

ALG for IPv4/NAT

- VPN transparency: PPTP, IPsec/L2TP.
- RTSP for QuickTime, RealPlayer, etc.
- File Transfer Protocol.
- SIP proxy.

Hole-punching services

- Manual configuration.
- UPnP Internet Gateway Device.
- NAT-PMP <draft-cheshire-nat-pmp-02>.
- IETF work: NSIS, MIDCOM, etc.

What's Required For IPv6 Gateways?

- Everything

IPv6 *replaces* IPv4/NAT

- Stateful filters for TCP, UDP, SCTP and DCCP.
- Transparency help for FTP, SIP, RTSP, IKE/IPsec, etc?
- ICE-like mechanisms can help for new protocols.
- Hole-punching protocols, e.g. ALD, UPnP IGD, NSIS, MIDCOM, others?

Is All This Really Necessary?

- IETF has consensus.
- U.S. government thinks so.
- Microsoft is on the record.
- Is there *any* noteworthy opposition?

Controversy!

- Hole-punching likely to be controversial.
- Existing IPv4/NAT protocols are proprietary.
- Open protocols are:
  - Not widely implemented.
  - Possibly not suitable for low-cost embedded devices.
- ALD <draft-woodyatt-ald-02> may give us a way out.