Lessons Learned Testing IPv6 Transition Mechanisms for IPv6-only

02-JUNE-2020

NANOG™

Experience with IPv6 Testing

- Tested IPv6 for 20 years at the UNH-IOL
  - Focusing on IPv6 Interoperability and Conformance testing
  - USGv6 and IPv6 Ready Test Lab
- CTO at QACafe
  - Company specializes in testing Home Gateway
- Author on USGv6 Profile Revision 1
- IPv6 Ready Logo Technical Chair

What is an IPv6-only network

- IPv6-only when no IPv4 addresses are provisioned to a network.
  - No IPv4 Gateways
  - No DHCP
- Network may filter IPv4 broadcast to lower network noise.
- IPv4 isn't removed from network devices, but is unused in those products.

Why IPv6-only?

- IPv4 address have run out
  - Carrier Grade Network Translation means more network functions in the network.
- Upkeeping two IP protocols causes issues with securing and maintaining multiple topologies.
- The United States Government Office of Management and Budget recently announced a memo that directed all agencies to plan for at least 80% of IP-enabled assets on Federal networks to be IPv6-only by the end of FY 2025.

Transition Mechanisms for IPv6-only

- We are focused on transition mechanisms that enable IPv4 connections over IPv6-only networks.
  - DS-Lite (Dual Stack Lite)
  - MAP-T (Mapping of Address and Port using Translation)
  - MAP-E (Mapping of Address and Port using Encapsulation)
  - DNS64/NAT64
  - 464XLAT

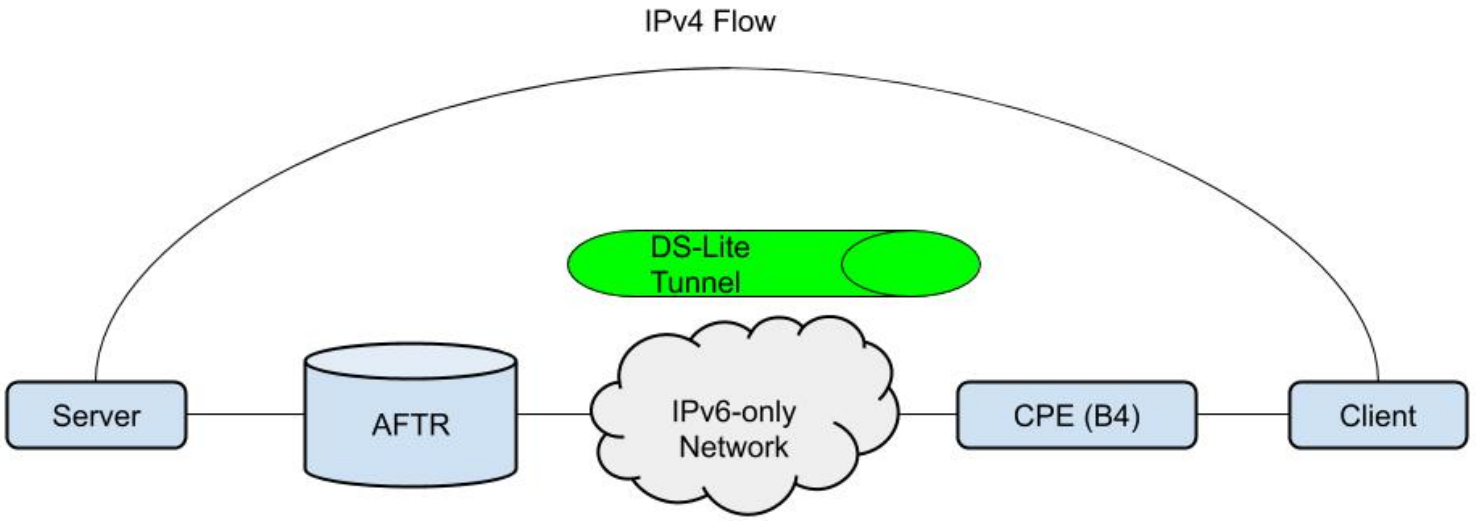
Common Testing Roadblocks

- Fragmentation
- Configuration Complexity
- Protocol Complexity

Fragmentation Issues

- IPv4 and IPv6 have different fragmentation rules that must be taken into account when transitioning from IP packets.
- Transition mechanism introduces more fragmentation due to encapsulation.
- Fragmented packets struggle to get thru all the security firewalls on devices.
- UDP doesn’t have a fragmentation built into like TCP.

DS-Lite topology



Fragmentation Example

- IPv4 Packets of size 1460 or bigger may cause fragmentation over the IPv6 Tunnel.
  - IPv6 header is 40 bytes.
- DS-Lite requires fragmentation occurs at IPv6 Layer, not the IPv4.
- CPE (B4) devices often confuse this and often break up the IPv4 packet which causes issues when DF flag in IPv4 is set.

Configuration complexity

- Network components need configuration to be synchronized across the different network functions.
- Transition Mechanism are transitioning IPv4/IPv6 the addressing and routing must be done correctly for both of these protocols.
- Home Gateways have multiple methods for configuration which makes it difficult to test all the possible methods a ISP might try to configure the needed functions for the transition mechanism to work.

Configuration Examples

- Network MTU configuration to account for overhead when running an encapsulation protocol.
- Ensuring a CPE will use the transition mechanism properly after a reboot or power outage consistently
  - We often see CPE have to be rebooted several times before attempting to utilize a transition mechanism.
- When using a management protocol TR-69 or DHCP you need to confirm that all the CPEs are getting the same information.

Address Complexity

- Transition mechanisms use some form of translation or encapsulation based on stateless addressing techniques that are complex requiring extra tools.
  - For example, MAP have complex addressing schemes that having an operator might want a tool to quickly decode.
- Issues that arise can be difficult to track across a network as addressing are often changing.

Protocol Complexity

- Many corner cases exist in the protocols to allow for stateless translation which can make manual testing difficult.
- Transition mechanisms adds functionally that needs to maintained, monitored, and reported on.
- Use both IPv4 and IPv6 which causes issues operators to understand both protocols (and deal with the problem areas).

Contact Information

- Timothy Winters
- tim@qacafe.com

Thank you

02-JUNE-2020

NANOG™