Enhanced DAD
6man, IETF 82, Taipei

Rajiv Asati, Hemant Singh, Wes Beebee, Eli Dart, Wes George, Carlos Pignataro

November 2011
Agenda

• Problem
• Mitigation
• Enhanced DAD Algorithm
Problem

• Looped back or reflected DAD probe is a well-known problem from Appendix A in RFC 4862.

• The circuit-switch SP community would like IPv6 to self-heal after a network Loopback test is stopped.

• Another SP deployment in cable broadband causes a serious problem due to looped back DAD probe.

• Reflected DAD probes have also been encountered in switched networks.

• 6man has DAD Proxy for a WG work item. Thus broadband access concentrators can now run into serious problems due to looped back DAD probe.
Circuit-switched Loopback

- Loopback testing is underway on a circuit connected to an interface on a router.
- Interface is enabled for IPv6. Interface issues a DAD probe.
- The DAD probe is looped back and interface is stuck in duplicate detected state.
- Loopback testing is stopped. IPv6 still does not self-heal while IPv4 does.
- Manual intervention is required.
Cable Broadband Problem

1st-hop IPv6 router, supports DAD Proxy

Access Concentrator

L3 interface

NS(DAD)

Modem (10.10.0.2)

Modem (10.10.0.1)

Hub
Cable Broadband Problem
Cable Broadband Problem

Access
Concentrator

NS(DAD)

Modem (10.10.0.2)

Modem (10.10.0.1)

Hub
Cable Broadband Problem

Access Concentrator

NS(DAD)

Modem (10.10.0.2)

Hub

Modem (10.10.0.1)
Cable Broadband Problem

Access Concentrator

NS(DAD)

Interface stuck in DUP state

Modem (10.10.0.1)

Modem (10.10.0.2)

Hub
Mitigation

• Disable DAD operation on the network interface. Compromises duplicate address detection.

• Certain L2 protocols such as PPP have a loopback message detection that can be used.
Enhanced DAD Algorithm: Use in unsecured non-SEND network…

• Use the Nonce Option defined in SEND (RFC 3971) to include in DAD Probe.
• No other ND message includes the Nonce Option.
• Similar to RFC 4862, the algorithm works for each address of an interface.
• Sender of NS(DAD) saves nonce per address.
Enhanced DAD Algorithm: Use in unsecured non-SEND network

• If interface address is in tentative or optimistic state and the interface receives a NS(DAD) matching nonce, a looped back NS(DAD) is declared (log message to sys admin and increment stats) and drop the NS(DAD).

• If nonce match is not found, DAD failure of RFC 4862 is declared.
Changes to RFC 4862

- A router that supports IPv6 DAD MUST implement the Enhanced DAD algorithm.
- A network interface on any other IPv6 node that is not a router SHOULD implement the Enhanced DAD algorithm.
Interoperation with SEND

• SEND should make explicit mention of detecting looped back DAD probes.

• In a mixed SEND environment with SEND and unsecured nodes, the lengths of the nonce used by SEND and unsecured nodes MUST be identical.
Actions to Perform on Detecting a Genuine Duplicate

- In certain networks such as a broadband access concentrator network, the concentrator is a trusted node in the SP domain that serves broadband modems in an un-trusted domain.

- In such a network if a client in the concentrator downstream issues a NS(DAD) that matches the IPv6 address of an interface on the concentrator serving the client, the client traffic is blocked and the NS(DAD) dropped.
Summary

• The Enhanced DAD algorithm can detect any looped back ND message. However not recommended for other ND messages – too many messages to maintain state for.

• Security Considerations: Use SEND.

• Pending work: allow catching looped back DAD probe in address assigned state, etc.
Thank you.