IETF 74 DHC

draft-dhankins-softwire-tunnel-option draft-ietf-dhc-option-guidelines
draft-ietf-dhc-dhcpinform-clarify

David W. Hankins

Internet Systems Consortium, Inc.

March, 2009

softwire-tunnel-option-03

- No material changes.
- Option name changed from OPTION_SOFTWIRES to OPTION_DS_LITE.
- Still encodes an IPv6 address, no discussion of this yet.
- Some feedback indicated a need for “make before break.”

ietf-dhc-option-guidelines-05

- Lots of good clarifying updates, thank you all.
- Draft author's primary goal was to give 'deployability' guidelines. Effort was extended to 'DHCP Option Author Better Practices'.

So what's the Better Practice?

- Differentiates between 'protocol' and 'data' options.
- Stresses the re-use of 'Option Format Fragments', existing well-deployed field types.
- Criminalizes conditional-formatting.
- Advises against aliasing.

So what's the Better Practice?

(cont'd)

- When 'well deployed fragments' are insufficient, recommends towards 'general' new fragments.
- Discusses the pros and cons of a sub options space.
- Discusses option size limitations.
- Discusses PRL/ORO mechanics.

So what's the Better Practice?

(security)

- Points out clear-text nature of DHCP.
- Advises validation of option content length and content as part of new option drafts.
- Points out that a DHCP client can be a “willing Trojan” in a user's system.

Next Steps

- Q&A?
- Ready for Last Call?

ietf-dhc-dhcpinform-clarify-03

- 'Subnet Selection Option' completely removed from server evaluation.
  - Because of 'ciaddr' vs 'giaddr' rules being swapped in DHCPINFORM processing, there is not a good place to insert this evaluation today.
- Various other clarifications.

Draft's main points.

- Acknowledge DHCPINFORM is not just for manually configured hosts.
- Document “de facto standard” of clients that zero htype/chaddr/ciaddr.
- Prohibit use of 'chaddr' for vendor identification. “To ARP or not to...”
- Clarify strange situation with 'giaddr'.

The de-facto-standard origins.

- The first client observed this author observed was a “Macromedia Flash Proxy Auto Discovery” widget.
- Rumor has it, this runs under Microsoft .Net, and has no **capability** to fetch MAC, ciaddr, or even know what interface(s) the host has. But it can send DHCP packets.

The de-facto-standard mess.

- ISC DHCP was changed to support zeroed ciaddr on May 6, 1999; use IP source address.
- The 'MFPAD' client triggered bugs in this when the message was relayed (giaddr is set).
- Bugfix had bugs – directing to giaddr even when ciaddr was set.

The curse gets worse.

- RFC 2131 prohibits 'checking for an existing binding'.
- This means scoped configuration on or near the lease may be lost when processing DHCPINFORM.
- And even though .Net sends the packet, the host OS consumes the ACK still. Client becomes 'broken.'

DHCPINFORM and 'giaddr'

- A BOOTP Relay (which DHCP traverses) transmits the reply packet to 'yiaddr and chaddr contents' when it is not broadcasting the reply (broadcast bit).
- DHCPINFORM sets ciaddr and not yiaddr. RFC 2131 directs the server 'SHOULD' direct replies to 'ciaddr'.

DHCPINFORM as amp. vector

- Basic DHCPv4 query packets are already pretty big, it seems unlikely that DHCPv4 could provide better than 5:1 amplification.
- But as better amplification vectors get shut down, it could emerge.
- So there's discussion in the security section.

Next Steps?

- Q&A?