IPv6 Address Accountability Considerations

draft-chown-v6ops-address-accountability-01

IETF81, Quebec

Tim Chown, tjc@ecs.soton.ac.uk

July 28th, 2011

Rationale

- Talking to many (academic) sites introducing IPv6 there is a common concern over lack of IPv6 address accountability due to
  - Autoconfiguration
  - Multi-addressing
  - Privacy addressing
  - Potentially rapidly changing addressing
  - Hosts being able to pick their own addresses manually with minimal chance of address conflict
- Today those sites have accountability with DHCPv4 and, often, Option 82 (RFC 3046)

Option 1: Switch-router polling

- Correlate polled data, including
  - IPv4 ARP tables
  - IPv6 ND tables
  - Switch port MAC tables
- Already used by tools like NAV, Netdot
  - Could integrate with 802.1X logs, if used
- May place load on devices
  - Need to poll rapidly enough that device cached data has not expired between polling

Option 2: Record all ND traffic

- Would allow address use to be recorded
- Some devices support forwarding function
  - e.g. RSPAN, but would need to be specific/filtered
  - Regardless, still a lot of traffic – bear in mind ND attacks discussed elsewhere this week
- Approach used by NDPmon, RAmond
  - Would thus allow more than just address accountability, e.g. rogue RA or DAD DoS detection

Option 3: Force use of DHCPv6

- Use same model as DHCPv4, possibly with RFC 4649 (similar to RFC 3046 for IPv4)
  - Not perfect, but the model commonly used now
- Issue RAs with M bit set, and Autonomous flag unset such that PIO is not used
  - Host should then use DHCPv6
- DHCPv6 supports temporary addresses
  - Offers privacy addresses with accountability
- But may not preclude manual configuration
  - If host can determine subnet prefix

Option 4: Re-use SAVI methods

- Not yet discussed in draft
- Have noted that logging in SAVI is apparently being encouraged to only record potential IP spoofing events
  - i.e. only record the minimum data required for the purpose
  - Thus not complete for accountability purposes
- Could SAVI be used to record all address usage?

Questions and next steps?

- Privacy concerns are important
  - Should privacy be expected *within* a host's site?
- Accountability measures might ideally be independent of address assignment method
- Are there Options 5, 6, …?

- Is this a topic worth discussing and progressing through a draft?
  - Seems to be a very common question raised by sites deploying IPv6 (dual-stack)