IPv6 End Station Addressing: Choosing SLAAC or DHCP

Jeff Harrington - NYSERNet

Important Planning Decisions

Planning for IPv6 on Campus

- Three major areas need to be addressed during planning.
- There are many changes in IPv6, but we have found consistency in implementation delays due to these factors:
  - Campus Addressing Plan
  - End Station/Host Addressing
  - Security

Important Planning Decisions

Planning for IPv6 on Campus

- Planning the mechanisms for end station addressing will be more complex in IPv6 than IPv4.
- New requirements, new tools, and new limitations must be accounted for.
- Consistency and coherency will be essential.
- Build up tool sets before deployment
  - Can be modeled after IPv4 tools, but you will have to make changes.

Important Planning Decisions

End Station/Host Addressing

- IPv6 adds more options to end station addressing.
- In addition to static addressing or DHCP, a new dynamic method of addressing is available called Stateless Address Autoconfiguration (SLAAC).
- There are advantages and disadvantages to both methods of host addressing.

Important Planning Decisions

End Station/Host Addressing

- No method of host addressing is complete without additional steps.
- There are ways to resolve the different limitations in each method.
- Organizations will have to determine which method of addressing hosts works in their environment…and the final decision may actually be to include both.

Assigning IPv6 Addresses

Static IPv6 Addresses

- Static IPv6 addresses can be used in a similar manner to static IPv4 addresses.
- Should be used for network devices and servers. Can be used in small subnets where DHCPv6 is either not available or not required.
- Not as easy to configure or remember addresses in IPv6 as IPv4.
- Does not change link-local addresses.

Assigning IPv6 Addresses

Static IPv6 Addresses

- IPv6 hosts can (and do) have more the one address.
- Just configuring a static address isn't enough.
- Must turn off end station autoconfiguration:
  - In Windows: netsh interface ipv6 set interface "Local Area Connection" routerdiscovery=disabled|enabled
  - In Linux: sudo sysctl -w net.ipv6.conf.eth1.autoconf=0
sudo sysctl -w net.ipv6.conf.eth1.accept_ra=0
  - MacOSX: net.inet6.ip6.use_tempaddr=0
- If the station gets a static and dynamic address it will decide on it's own which address to use for a given flow. (RFC 6724)

Assigning IPv6 Addresses

Dynamic Host Addressing

- For end stations that do not need a well-known, stable address, dynamic addressing should be used.
- In IPv4 only option is DHCP. For IPv6 the default dynamic addressing option is SLAAC, but DHCPv6 is available.
- With Dynamic addressing, consider the requirements: hosts receive an address, a default gateway, DNS resolvers, a lifetime, and potentially other parameters.

Assigning IPv6 Addresses

Dynamic Host Addressing

- Other considerations would be host support for the addressing method, DNS updates, user tracking/accounting, privacy and security.
- SLAAC and DHCPv6 approach host addressing differently, and fulfill different requirements.
- Depending on your needs, match the addressing method to your environment.
- Work is ongoing in both SLAAC and DHCPv6 to provide a solution that meets all requirements, but neither method is complete.

Assigning IPv6 Addresses

Stateless Autoconfiguration

- Stateless Address Autoconfiguration (SLAAC) is the default method IPv6 hosts obtain an IPv6 address.
- End stations automatically generate the Interface ID (lower 64 bits) of their address as an EUI-64 address based on the station MAC address.
- The Prefix is provided to the end station via a Router Advertisement (RA).
- The RA contains the prefix(es) for that subnet, the default gateway and prefix lifetime.

Assigning IPv6 Addresses

Stateless Autoconfiguration

- End stations request an RA during start up, or upon connecting to a network for the first time.
- RAs are also periodically sent by the router to refresh lifetimes.

Assigning IPv6 Addresses

Stateless Autoconfiguration

- Because all implementations of IPv6 support SLAAC, deployment can be ubiquitous.
  - All hosts and all OSes can implement SLAAC.
- Privacy, security and DNS resolution are major issues with implementing SLAAC.

Assigning IPv6 Addresses

Stateless Autoconfiguration

- Privacy Extenstions to SLAAC
- The original SLAAC standard bases the Interface ID on the station MAC address.
- With this configuration, mobile devices retain the lower 64 bits of the address regardless of their location.
- RFC 4941 defines privacy extensions for SLAAC. All major OSes implement this RFC by default.
- With privacy extensions enabled the end station IPv6 address is recalculated every 24 hours.

Assigning IPv6 Addresses

Stateless Autoconfiguration

- Privacy extensions do limit tracking of users as they move locations.
- Issues with privacy extensions include
  - Long lived connections lose connectivity after ~7 days
  - With users changing IPs regularly logging the user/IP address correlation is difficult
  - Security policies may need to be revisited – do you filter based on source address?
- Draft is under consideration to create ‘stable’ privacy addresses.
  - End Station addresses would still change based on location, fulfilling the privacy concerns. But would be stable inside each location.
  - draft-ietf-6man-stable-privacy-addresses-01.txt

Assigning IPv6 Addresses

Stateless Autoconfiguration

- SLAAC does not include any DNS functionality.
- Neither AAAA host entries into authoritative servers or providing resolvers to hosts is part of SLAAC.
  - Populating addresses or reverse records dynamically into DNS must be done by another method.
  - End stations are not given resolver(s) or local domain information.

Assigning IPv6 Addresses

Stateless Autoconfiguration

- End stations in dual stack environments can use the information provided via IPv4
- For IPv6 only hosts, need another method to provide DNS information.
  - Use the ‘O’ flag and have local router provide information.
  - Use the ‘O’ flag and have DHCP server provide information.

Assigning IPv6 Addresses

Stateless Autoconfiguration

- RFC 6106 specifies new extensions to SLAAC that allow DNS information to be included in RAs.
  - Routers can send out both resolvers and domains.
  - Supported in Linux implementations, Mac OS X and iOS.
  - Not supported in Android, Windows (third party applications can provide support), Cisco IOS or JUNOS.
  - Full support listed at http://en.wikipedia.org/wiki/Comparison_of_IPv6_support_in_operating_systems

Assigning IPv6 Addresses

Stateless Autoconfiguration

- Security issues surrounding SLAAC are concerned with ensuring that only legitimate routers send RAs.
  - Same concern for DHCPv6.
- Blocking rogue RAs should be considered standard practice
  - RA Guard
  - Manual filters
  - High preference on legitimate RAs

Assigning IPv6 Addresses

Stateless Autoconfiguration

- Additional security issue with SLAAC involves filtering based on source addresses.
- If your organizations security policy uses source IP filters to restrict access to sensitive systems or resources SLAAC with privacy extensions will eliminate this practice
  - Cannot predict the source address, and 24 hour rotation of addresses means constantly updating filters.
  - Stable privacy addressing will help, but not yet available.

Assigning IPv6 Addresses

DHCPv6

- SLAAC can be used in a production environment, but many organizations do not like the unpredictability, particularly with privacy options.
- Remaining option to addresses end hosts is DHCPv6.
- Must configure your network to stop announcing SLAAC prefixes and also to tell the host to look for a DHCPv6 server.
  - Done by setting the ‘M’ bit on the interface so the Router Advertisement includes the flag.

Assigning IPv6 Addresses

Development of DHCPv6

- Not everyone saw the need
  - Stateless address autoconfiguration allows clients to obtain IPv6 addresses.
  - Seen as providing same functionality as DHCPv4, so don't need DHCP in IPv6, right?
- Reasons for DHCPv6
  - Provide DNS information: currently no other automated way to do this (RFC 6106 is largely unimplemented).
  - Better control and tracking of IPv6 address usage.
  - Centralized mechanism for DDNS updates.
  - Use of DHCP options.

Assigning IPv6 Addresses

DHCPv6

- DHCPv6 operates similarly to DHCPv4. Client requests an address from a server, and receives a response with an address and other configured information.
- Just as in IPv4, the host receives complete addressing. Both the 64 bit prefix and the 64 bit Interface ID. The host does not get any addressing from the Router Advertisement.
  - Does not affect Link-local addresses, those remain generated by the host.

Assigning IPv6 Addresses

DHCPv6

- The other information from the DHCPv6 server could include DNS resolver(s), domain name(s) and other parameters.
- DHCPv6 servers however do not provide gateway information. The default gateway remains part of the router advertisement.
  - Current standard does still require this, Router Advertisements are still necessary, to tell the host to contact the DHCPv6 server and to receive the default gateway.

Assigning IPv6 Addresses

DHCPv6

- DHCPv6 also works like DHCPv4 for valid and preferred lifetimes on hosts.
- Addresses must be renewed within the configured interval.
- DHCPv6 servers can also trigger reconfigurations on end stations.

Assigning IPv6 Addresses

DHCPv6

- Most modern Operating Systems support DHCPv6
  - Windows Vista, 7 and 8
  - Mac OS 10.7 or later, iOS 4.1
  - Linux
  - Cisco, Juniper, HP (relaying)
- Many older Operating Systems do not support DHCPv6
  - Windows XP
  - OS X pre-Lion
  - Android

Assigning IPv6 Addresses

DHCPv6

- If your install base includes a substantial amount of older Operating Systems, DHCPv6 may not be applicable to your environment.
  - Upgrade if possible, or SLAAC is required.

Assigning IPv6 Addresses

DHCPv6

- DHCPv6 support among IPAM systems is widespread
  - Infoblox
  - Bluecat
  - 6Connect
  - Ipal
  - Others also support IPv6
- Talk to your vendor to determine how to include IPv6 in your Implementation.

Assigning IPv6 Addresses

DHCPv6

- DHCPv6, particularly when used with an IPAM system, allows for Dynamic DNS updates.
  - Just as in IPv4, when an address is assigned, the record can be created and zone files updated.

Assigning IPv6 Addresses

DHCPv6

- DHCPv6 does not have the privacy concerns of SLAAC.
  - Interface IDs are not generated by the host, and are not consistent as the host moves between networks.
  - Assumes hosts will always connect to DHCPv6 networks. Mobile users may connect to networks that use both types of addressing.

Assigning IPv6 Addresses

DHCPv6

- DHCPv6 Security includes concerns similar to SLAAC and DHCPv4.
  - Hosts still require RAs in order to get gateway information and to receive the M-bit.
    - Need to take steps to secure the RA messages so that only legitimate routers send them.
  - Securing DHCP announcements is still required
    - Need to take steps to secure the DHCP servers themselves.
    - Need to take steps to ensure only legitimate DHCP servers send out DHCPv6 responses.

Assigning IPv6 Addresses

DHCPv6 Lite

- Useful as a middle ground between SLAAC and full DHCP.
  - Routers provide DNS server and domain information to clients via router-based DHCP server.
  - Clients use SLAAC to assign global IPv6 address.
- Alleviates the need for a DHCP server, while at the same time providing all necessary information.
- Uses the ‘O’ bit on the interface configuration.

```
ipv6 dhcp pool dhcp-lite
dns-server [ipv6 DNS server address]
domain-name campus.edu
!
Interface FastEthernet0/0
ipv6 nd other-config-flag
Ipv6 dhcp server dhcp-lite
```

Tracking IPv6 Addresses

User Tracking using Dynamic Addressing

- Many organizations track their user community with IPv4.
  - What user has what IP at what time.
  - Useful for DMCA take down notices, security violations, or other needs.
  - Most tracking mechanisms use the correlation between IP address/MAC address/User ID
    - Easy in IPv4 and DHCP uses MAC address as the mechanism to assign the IPv4 address.
    - As long as users register their MAC address can correlate all three pieces of information into one whole.

Tracking IPv6 Addresses

User Tracking using Dynamic Addressing

- Tracking users with SLAAC
  - SLAAC without privacy extensions does not require hosts to change their IPv6 address regularly.
    - Once known, can correlate user/MAC/IP consitently
  - SLAAC with privacy extensions is more complex
    - End Station IPv6 address changes regularly
    - Still know user/MAC correlation
    - Must update IPv6 address/MAC correlation every time the privacy hash runs.
  - SLAAC with stable privacy addresses will work like SLAAC without privacy extenstions (while the user is on the same network).

Tracking IPv6 Addresses

User Tracking using Dynamic Addressing

- Tracking Users with DHCPv6 is also more complex
  - Client no longer uses the hardware address to identify itself.
  - Instead uses a DHCP User ID (DUID)
    - Used for both client IDs and server IDs.
    - If multiple interfaces on one client are configured via DHCPv6, use the SAME DUID for each.
    - Generated when the client is initially installed.

Tracking IPv6 Addresses

User Tracking using Dynamic Addressing

- With DHCPv6 there are 4 pieces of information that must be correlated.
  - Still have User and MAC address from registration process.
  - Now have IPv6 address and DUID.
  - Those pairs of information do not have to have any relation to one another.

Tracking IPv6 Addresses

User Tracking using Dynamic Addressing

- Use neighbor table:

```
#sh ipv6 nei
IPv6 Address                              Age  Link-layer Addr  State Interface
FE80::222:19FF:FE60:383D                  0    0022.196a.383d   STALE Vl101
FE80::212:44FF:FE60:6D02                  1    0012.4760.6d02   STALE Gi1/25
2001:468:901:1:2C0B:FF84:CD7C:5388        3    0016.d347.ddc4   STALE Vl101
2001:468:901:1:213:20FF:FE79:BB07         5    0013.2079.bb07   STALE Vl101
2001:468:901:1:211:43FF:FECE:150F         41    0011.43ce.150f  STALE Vl101
```

- Gives the correlation between IPv6 address and MAC address.
- Must be run periodically
  - Could be added to existing ARP polling scripts
- Will also have to adjust data storage.
  - What format will the data be stored, and for how long?
  - Make sure your databases can handle 128 bit addresses.

Tracking IPv6 Addresses

User Tracking using Dynamic Addressing

- Use SNMP scripts to pull MIB data.
  - SNMP IPv4: bulk-get
    - ipNetToMediaPhysAddress (1.3.6.1.2.1.4.22.1.2)
  - SNMP IPv6: bulk-get
    - ipv6NetToMediaPhysAddress (1.3.6.1.2.1.55.1.12.1.2)
      - Not in Cisco 12.2 SXJ nor 15.1
    - Cisco private MIB: cInetNetToMediaPhysAddress (1.3.6.1.4.1.9.10.86.1.1.3.1.3)
    - Juniper supports the ipv6NetToMediaTable
  - Other vendors may also support either the IETF standard MIBs or proprietary MIBs.

Tracking IPv6 Addresses

User Tracking using Dynamic Addressing

- ipv6mon (http://www.si6networks.com/tools/ipv6mon/)
  - Uses a mix of active and passive probes to discover nodes and place the addresses into log files.
- Nmap
  - Uses a variety of similar methods to discover hosts.

- Other tools exist as well.
- Tracking users and addresses may not be as straightforward in IPv6 – but it is possible.

Host Addressing Summary

End Station/Host Addressing

- SLAAC
  - Supported in all Implementations, and on by default.
  - Does not provide complete information to hosts for connectivity – no DNS information.
  - Privacy extensions make user tracking difficult.
- DHCPv6
  - Supported in most IPAM systems, administrators are familiar with the interface and comfortable with this method of address assignment.
  - Not supported in older OSes.
  - Does not provide complete information to hosts for connectivity – no default router/gateway.
  - Tracking users involves additional information that was previously not in IPv4, and is not intuitive.

Host Addressing Summary

End Station/Host Addressing

- Organizations may not be able to use a single method of addressing for hosts.
  - Would like to use DHCP but host support is unavailable.
  - Would like to use SLAAC but some users need DHCP stability.
- Mixed implementations are possible, but need to be planned for.
  - Only one method of addressing per VLAN – cannot mix SLAAC and DHCP in the same VLAN.
    - Might lead to issues with subnets and access control.

Host Addressing Summary

Summary

- Use the method of assigning addresses that makes sense in your environment:
  - Use static assignments for infrastructure and servers.
  - Use SLAAC for small implementations or in networks where DHCP is not available or required.
  - Use DHCPv6 for networks where needed.
  - Use DHCPv6 lite as a possible transition mechanism to deploy IPv6 to subnets before servers are available.
- Other considerations:
  - Do you really need DHCP anymore?
    - Was the only way to non-statically assign addresses in v4, and also track hosts.
      - Will other tracking methods work in v6?
      - If you don’t need DHCP to track users, can you let hosts autoconfigure?