Enterprise IPv6 Deployment

Shannon McFarland
CCIE# 5245, VCP
Corporate Consulting Engineer
Office of the CTO
Reference Materials

- CCO IPv6 Main Page: http://www.cisco.com/go/ipv6
- Cisco Network Designs: http://www.cisco.com/go/designzone
Recommended Reading


Coming Soon!!
Agenda

- The Need for IPv6
- Planning and Deployment Summary
- Address Considerations
- General Concepts
- Infrastructure Deployment
  - Campus/Data Center
  - WAN/Branch
  - Remote Access
- Provider Considerations
The Need For IPv6
Market Factors Driving IPv6 Deployment

Address Issues
- Exhaustion
- M&A
- Business Development

IPv6 OS, Content & Applications
Google
Facebook
Microsoft

Infrastructure Evolution
SmartGrid, SmartCities
DOCSIS 3.0, 4G/LTE, IPSO

National IPv6 Strategies
US DoD, China NGI, EU

www.oecd.org: Measuring IPv6 adoption
IPv6 Provides Benefits Across the Board

- Building sensors
- Media services
- Collaboration
- Mobility

Higher Education/Research

- Embedded devices
- Industrial Ethernet
- IP-enabled components

Manufacturing

- DoD
- WIN-T
- FCS
- JTRS
- GIG-BE

Government (Federal/Public Sector)

- Telematics
- Traffic control
- Hotspots
- Transit services

Transportation

- Animal tags
- Imagery
- Botanical
- Weather

Agriculture/Wildlife

- Set-top boxes
- Internet gaming
- Appliances
- Voice/video
- Security monitoring

Consumer

- Home care
- Wireless asset tracking
- Imaging
- Mobility

Health Care
Dramatic Increase in Enterprise Activity

Why?

- Enterprise that is or will be expanding into emerging markets
- Enterprise that partners with other companies who may use IPv6 (larger enterprise, located in emerging markets, government, service providers)
- Adoption of Windows 7, Windows 2008, DirectAccess
- Frequent M&A activity
- Energy – High density IP-enabled endpoints (SmartGrid)
Planning & Deployment Summary
Enterprise Adoption Spectrum

**Preliminary Research**
- Is it real?
- Do I need to deploy everywhere?
- Equipment status?
- SP support?
- Addressing
- What does it cost?

**Pilot/Early Deployment**
- Mostly or completely past the “why?” phase
- Assessment (e2e)
- Weeding out vendors (features and $)
- Focus on training and filling gaps

**Production/Looking for parity and beyond**
- Still fighting vendors
- Content and wide-scale app deployment
- Review operational cost of 2 stacks
- Competitive/Strategic advantages of new environment
# IPv6 Integration Outline

<table>
<thead>
<tr>
<th>Pre-Deployment Phases</th>
<th>Deployment Phases</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Establish the network starting point</td>
<td>• Transport considerations for integration</td>
</tr>
<tr>
<td>• Importance of a network assessment and available tools</td>
<td>• Campus IPv6 integration options</td>
</tr>
<tr>
<td>• Defining early IPv6 security guidelines and requirements</td>
<td>• WAN IPv6 integration options</td>
</tr>
<tr>
<td>• Additional IPv6 “pre-deployment” tasks needing consideration</td>
<td>• Advanced IPv6 services options</td>
</tr>
</tbody>
</table>
Integration/Coexistence Starting Points
Example: Integration Demarc/Start Points in Campus/WAN

1. Start dual-stack on hosts/OS
2. Start dual-stack in campus distribution layer (details follow)
3. Start dual-stack on the WAN/campus core/edge routers
4. NAT64 for servers/apps only capable of IPv4 (temporary only)
Address Considerations
Hierarchical Addressing and Aggregation

- Default is /48 – can be larger – “End-user Additional Assignment”
  [https://www.arin.net/resources/request/ipv6_add_assign.html](https://www.arin.net/resources/request/ipv6_add_assign.html)

- Provider independent – See Number Resource Policy Manual (NRPM) - [https://www.arin.net/policy/nrpm.html](https://www.arin.net/policy/nrpm.html)
Summary of Address Considerations

- Provider Independent and/or Provider Assigned
- ULA, ULA + Global, Global only
- Prefix-length allocation
  - /64 everywhere except loopbacks (/128)
  - /64 on host links, /126 on P2P links, /128 on loopbacks
  - Variable prefix-lengths on host links
What type of addressing should I deploy internal to my network? It depends:

- **ULA-only**—Today, no IPv6 NAT is useable in production so using ULA-only will not work externally to your network.
- **ULA + Global** allows for the best of both worlds but at a price—much more address management with DHCP, DNS, routing and security—SAS does not always work as it should.
- **Global-only**—Recommended approach but the old-school security folks that believe topology hiding is essential in security will bark at this option.

Let’s explore these options…
Unique-Local Addressing (RFC4193)

- Used for internal communications, inter-site VPNs
  - Not routable on the internet—basically RFC1918 for IPv6 only better—less likelihood of collisions
- Default prefix is /48
  - /48 limits use in large organizations that will need more space
  - Semi-random generator prohibits generating sequentially ‘useable’ prefixes—no easy way to have aggregation when using multiple /48s
  - Why not hack the generator to produce something larger than a /48 or even sequential /48s?
  - Is it ‘legal’ to use something other than a /48? Perhaps the entire space? Forget legal, is it practical? Probably, but with dangers—remember the idea for ULA; internal addressing with a slim likelihood of address collisions with M&A. By consuming a larger space or the entire ULA space you will significantly increase the chances of pain in the future with M&A
- Routing/security control
  - You must always implement filters/ACLs to block any packets going in or out of your network (at the Internet perimeter) that contain a SA/DA that is in the ULA range—today this is the only way the ULA scope can be enforced
- Generate your own ULA: [http://www.sixxs.net/tools/grh/ula/](http://www.sixxs.net/tools/grh/ula/)

Generated ULA = fd9c:58ed:7d73::/48

* MAC address=00:0D:9D:93:A0:C3 (Hewlett Packard)
* EUI64 address=020D9Dffe93A0C3
* NTP date=cc5ff71943807789 cc5ff71976b28d86
ULA-Only

- Everything internal runs the ULA space
- A NAT supporting IPv6 or a proxy is required to access IPv6 hosts on the internet — must run filters to prevent any SA/DA in ULA range from being forwarded
- Works as it does today with IPv4 except that today, there are no scalable NAT/Proxies for IPv6
- Removes the advantages of not having a NAT (i.e. application interoperability, global multicast, end-to-end connectivity)
ULA + Global

- Both ULA and Global are used internally except for internal-only hosts
- Source Address Selection (SAS) is used to determine which address to use when communicating with other nodes internally or externally
- In theory, ULA talks to ULA and Global talks to Global—SAS ‘should’ work this out
- ULA-only and Global-only hosts can talk to one another internal to the network
- Define a filter/policy that ensures your ULA prefix does not ‘leak’ out onto the Internet and ensure that no traffic can come in or out that has a ULA prefix in the SA/DA fields
- Management overhead for DHCP, DNS, routing, security, etc…
Considerations—ULA + Global

- Use DHCPv6 for ULA and Global—apply different policies for both (lifetimes, options, etc.)
- Check routability for both—can you reach an AD/DNS server regardless of which address you have?
- Any policy using IPv6 addresses must be configured for the appropriate range (QoS, ACL, load-balancers, PBR, etc.)
- If using SLAAC for both—Microsoft Windows allows you to enable/disable privacy extensions globally—this means you are either using them for both or not at all!!!
- One option is to use SLAAC for the Global range and enable privacy extensions and then use DHCPv6 for ULA with another IID value (EUI-64, reserved/admin defined, etc.)

<table>
<thead>
<tr>
<th></th>
<th>Temporary</th>
<th>Preferred</th>
<th>Lifespan</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP</td>
<td></td>
<td>Preferred</td>
<td>6d23h59m55s</td>
<td>23h59m55s 2001:db8:cafe:2:cd22:7629:f726:6a6b</td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td>Preferred</td>
<td>13d1h33m55s</td>
<td>6d1h33m55s fd9c:58ed:7d73:1002:8828:723c:275e:846d</td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td>Preferred</td>
<td>infinite</td>
<td>infinite fe80:8828:723c:275e:846d%8</td>
</tr>
</tbody>
</table>

- Unlike Global and link-local scopes ULA is not automatically controlled at the appropriate boundary—you must prevent ULA prefix from going out or in at your perimeter
- SAS behavior is OS dependent and there have been issues with it working reliably
ULA + Global Example

```
interface Vlan2
  description ACCESS-DATA-2
  ipv6 address 2001:DB8:CAFE:2::D63/64
  ipv6 address FD9C:58ED:7D73:1002::D63/64
  ipv6 nd prefix 2001:DB8:CAFE:2::/64 no-advertise
  ipv6 nd prefix FD9C:58ED:7D73:1002::/64 no-advertise
  ipv6 nd managed-config-flag
  ipv6 dhcp relay destination 2001:DB8:CAFE:11::9
```

<table>
<thead>
<tr>
<th>Addr Type</th>
<th>DAD State</th>
<th>Valid Life</th>
<th>Pref. Life</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dhcp</td>
<td>Preferred</td>
<td>13d23h48m24s 6d23h48m24s</td>
<td>2001:db8:cafe:2:c1b5:cc19:f87e:3c41</td>
<td></td>
</tr>
<tr>
<td>Dhcp</td>
<td>Preferred</td>
<td>13d23h48m24s 6d23h48m24s</td>
<td>fd9c:58ed:7d73:1002:8828:723c:275e:846d</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>Preferred</td>
<td>infinite</td>
<td>infinite</td>
<td>fe80::8828:723c:275e:846d%8</td>
</tr>
</tbody>
</table>

List DHCP Leases for Prefix VLAN2

<table>
<thead>
<tr>
<th>@</th>
<th>Address</th>
<th>State</th>
<th>Lookup Key</th>
<th>Flags</th>
<th>State Expire</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2001:db8:cafe:2:c1b5:cc19:f87e:3c41</td>
<td>leased</td>
<td>00:01:00:01:0d:7f:9c:f8:00:0d:60:84:2c:7a</td>
<td></td>
<td>Tue Sep 16</td>
</tr>
</tbody>
</table>

List DHCP Leases for Prefix VLAN2-ULA

<table>
<thead>
<tr>
<th>@</th>
<th>Address</th>
<th>State</th>
<th>Lookup Key</th>
<th>Flags</th>
<th>State Expire</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>f9c:58ed:7d73:1002:8628:723c:275e:846d</td>
<td>leased</td>
<td>00:01:00:01:0d:7f:9c:f8:00:0d:60:84:2c:7a</td>
<td></td>
<td>Tue Sep 16</td>
</tr>
</tbody>
</table>
Global-Only

- Global is used everywhere
- No issues with SAS
- No requirements to have NAT for ULA-to-Global translation—but, NAT may be used for other purposes
- Easier management of DHCP, DNS, security, etc.
- Only downside is breaking the habit of believing that topology hiding is a good security method 😊

2001:DB8:CAFE:2800::/64
2001:DB8:CAFE:3000::/64
2001:DB8:CAFE::/48
2001:DB8:CAFE:2::/64

Internet

Corporate Backbone

Branch 1

Global – 2001:DB8:CAFE::/48

Branch 2

Global – 2001:DB8:CAFE::/48

Corp HQ

Recommended
Randomized IID and Privacy Extensions

- Enabled by default on Microsoft Windows
- Enable/disable via GPO or CLI

```
netsh interface ipv6 set global randomizeidentifiers=disabled store=persistent
netsh interface ipv6 set privacy state=disabled store=persistent
```

- Alternatively, use DHCP (see later) to a specific pool
- Randomized address are generated for non-temporary autoconfigured addresses including public and link-local—used instead of EUI-64 addresses
- Randomized addresses engage Optimistic DAD—likelihood of duplicate LL address is rare so RS can be sent before full DAD completion
- Windows Vista/W7/2008 send RS while DAD is being performed to save time for interface initialization (read RFC4862 on why this is ok)
- Privacy extensions are used with SLAAC
## Link Level—Prefix Length Considerations

<table>
<thead>
<tr>
<th>64 bits</th>
<th>&lt; 64 bits</th>
<th>&gt; 64 bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recommended by RFC3177 and IAB/IESG</td>
<td>Enables more hosts per broadcast domain</td>
<td>Address space conservation</td>
</tr>
<tr>
<td>Consistency makes management easy</td>
<td>Considered bad practice</td>
<td>Special cases: /126—valid for p2p</td>
</tr>
<tr>
<td>MUST for SLAAC (MSFT DHCPv6 also)</td>
<td>64 bits offers more space for hosts than the media can support efficiently</td>
<td>/127—not valid for p2p (RFC3627)</td>
</tr>
<tr>
<td>Significant address space loss (18.466 Quintillion)</td>
<td></td>
<td>/128—loopback</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Complicates management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Must avoid overlap with specific addresses: Router Anycast (RFC3513)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Embedded RP (RFC3956) ISATAP addresses</td>
</tr>
</tbody>
</table>
Using Link-Local for Non-Access Connections
Under Research

- What if you did not have to worry about addressing the network infrastructure for the purpose of routing?
  - IPv6 IGPs use LL addressing
  - Only use Global or ULA addresses at the edges for host assignment
  - For IPv6 access to the network device itself use a loopback

- What happens to route filters? ACLs?—Nothing, unless you are blocking to/from the router itself

- Stuff to think about:
  - Always use a RID
  - Some Cisco devices require “ipv6 enable” on the interface in order to generate and use a link-local address
  - Enable the IGP on each interface used for routing or that requires its prefix to be advertised
Using LL + Loopback Only

```
ipv6 unicast-routing
!
interface Loopback0
  ipv6 address 2001:DB8:CAFE:998::1/128
  ipv6 eigrp 10
!
interface Vlan200
  ipv6 address 2001:DB8:CAFE:200::1/64
  ipv6 eigrp 10
!
interface GigabitEthernet1/1
  ipv6 enable
  ipv6 eigrp 10
!
ipv6 router eigrp 10
  router-id 10.99.8.1
  no shutdown

IPv6-EIGRP neighbors for process 10
0   Link-local address: Gi1/2
    FE80::212:D9FF:FE92:DE77
```
Interface-ID Selection

Network Devices

- Reconnaissance for network devices—the search for something to attack

- Use random 64-bit interface-IDs for network devices
  - 2001:DB8:CAFE:2::1/64—Common IID
  - 2001:DB8:CAFE:2::9A43:BC5D/64—Random IID
  - 2001:DB8:CAFE:2::A001:1010/64—Semi-random IID

- Operational management challenges with this type of numbering scheme
DHCPv6

- Updated version of DHCP for IPv4
- Client detects the presence of routers on the link
- If found, then examines router advertisements to determine if DHCP can or should be used
- If no router found or if DHCP can be used, then DHCP Solicit message is sent to the All-DHCP-Agents multicast address
  Using the link-local address as the source address
DHCPv6 Operation

- **All_DHCP_Relay_Agents_and_Servers** (FF02::1:2)
- **All_DHCP_Servers** (FF05::1:3)
- DHCP Messages: clients listen UDP port 546; servers and relay agents listen on UDP port 547
Stateful/Stateless DHCPv6

- Stateful and stateless DHCPv6 server

- DHCPv6 Relay—supported on routers and switches

```
interface FastEthernet0/1
  description CLIENT LINK
  ipv6 address 2001:DB8:CAFE:11::1/64
  ipv6 nd prefix 2001:DB8:CAFE:11::/64 no-advertise
  ipv6 nd managed-config-flag
  ipv6 nd other-config-flag
  ipv6 dhcp relay destination 2001:DB8:CAFE:10::2
```
Basic DHCPv6 Message Exchange

DHCPv6 Client

- Solicit(IA_NA)
- Advertise(IA_NA(addr))
- Request(IA_NA)
- Reply(IA_NA(addr))
- Renew(IA_NA(addr))
- Release(IA_NA(addr))

Address Assigned
Timer Expiring

DHCPv6 Relay Agent

- Relay-Forw(Solicit(IA_NA))
- Relay-Repl(Advertise(IA_NA(addr)))
- Relay-Forw(Request(IA_NA))
- Relay-Repl(Reply(IA_NA(addr)))
- Relay-Forw(Renew(IA_NA(addr)))
- Relay-Repl(Reply(IA_NA(addr)))
- Relay-Forw(Release(IA_NA(addr)))
- Relay-Repl(Reply(IA_NA(addr)))

DHCPv6 Server
IPv6 General Prefix

- Provides an easy/fast way to deploy prefix changes
- Example: 2001:db8:cafe::/48 = General Prefix
- Fill in interface specific fields after prefix

```
IPv6 General Prefix

```

```
interface GigabitEthernet3/2
ipv6 address ESE ::2/126
dv6 cef

interface GigabitEthernet1/2
ipv6 address ESE ::E/126
ipv6 cef

interface Vlan11
ipv6 address ESE ::11:0:0:0:1/64
ipv6 cef

interface Vlan12
ipv6 address ESE ::12:0:0:0:1/64
ipv6 cef

Global unicast address(es):
2001:DB8:CAFE:11::1, subnet is 2001:DB8:CAFE:11::/64
General Concepts – FHRP, Multicast and QoS
First Hop Router Redundancy

HSRP for v6
- Modification to Neighbor Advertisement, router Advertisement, and ICMPv6 redirects
- Virtual MAC derived from HSRP group number and virtual IPv6 link-local address

GLBP for v6
- Modification to Neighbor Advertisement, Router Advertisement—GW is announced via RAs
- Virtual MAC derived from GLBP group number and virtual IPv6 link-local address

Neighbor Unreachability Detection
- For rudimentary HA at the first HOP
- Hosts use NUD “reachable time” to cycle to next known default gateway (30s by default)

No longer needed
First-Hop Redundancy

- When HSRP, GLBP, and VRRP for IPv6 are not available
- NUD can be used for rudimentary HA at the first-hop (today this only applies to the Campus/DC—HSRP is available on routers)
  ```
  (config-if)#ipv6 nd reachable-time 5000
  ```
- Hosts use NUD “reachable time” to cycle to next known default gateway (30 seconds by default)
- Can be combined with default router preference to determine primary gw:
  ```
  (config-if)#ipv6 nd router-preference {high | medium | low}
  ```

<table>
<thead>
<tr>
<th>Default Gateway</th>
<th>10.121.10.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>fe80::211:bcff:fec0:d000%4</td>
<td></td>
</tr>
<tr>
<td>fe80::211:bcff:fec0:c800%4</td>
<td></td>
</tr>
</tbody>
</table>

Reachable Time : 6s
Base Reachable Time : 5s

---

**HSRP for IPv4**
**RA’s with adjusted reachable-time for IPv6**
HSRP for IPv6

- Many similarities with HSRP for IPv4
- Changes occur in Neighbor Advertisement, Router Advertisement, and ICMPv6 redirects
- No need to configure GW on hosts (RAs are sent from HSRP active router)
- Virtual MAC derived from HSRP group number and virtual IPv6 link-local address
- IPv6 Virtual MAC range: 0005.73A0.0000 - 0005.73A0.0FFF (4096 addresses)
- HSRP IPv6 UDP Port Number 2029 (IANA Assigned)
- No HSRP IPv6 secondary address
- No HSRP IPv6 specific debug

```
interface FastEthernet0/1
ipv6 address 2001:DB8:66:67::2/64
ipv6 cef
standby version 2
standby 1 ipv6 autoconfig
standby 1 timers msec 250 msec 800
standby 1 preempt
standby 1 preempt delay minimum 180
standby 1 authentication md5 key-string cisco
standby 1 track FastEthernet0/0
```

```
#route -A inet6 | grep ::/0 | grep eth2
::/0 fe80::5:73ff:fea0:1 UGDA 1024 0 0 eth2
```
GLBP for IPv6

- Many similarities with GLBP for IPv4 (CLI, load-balancing)
- Modification to Neighbor Advertisement, Router Advertisement
- GW is announced via RAs
- Virtual MAC derived from GLBP group number and virtual IPv6 link-local address

AVG=Active Virtual Gateway
AVF=Active Virtual Forwarder
SVF=Standby Virtual Forwarder
IPv6 Multicast Availability

- Multicast Listener Discovery (MLD)
  Equivalent to IGMP
- PIM Group Modes: Sparse Mode, Bidirectional and Source Specific Multicast
- RP Deployment: Static, Embedded
Multicast Listener Discovery: MLD

Multicast Host Membership Control

- MLD is equivalent to IGMP in IPv4
- MLD messages are transported over ICMPv6
- MLD uses link local source addresses
- MLD packets use “Router Alert” in extension header (RFC2711)
- Version number confusion:
  - MLDv1 (RFC2710) like IGMPv2 (RFC2236)
  - MLDv2 (RFC3810) like IGMPv3 (RFC3376)
- MLD snooping
Multicast Deployment Options
With and Without Rendezvous Points (RP)

SSM, No RPs

ASM Single RP—Static definitions

ASM Across Single Shared PIM Domain, One RP—Embedded-RP
IPv6 QoS Syntax Changes

- IPv4 syntax has used “ip” following match/set statements
  
  Example: `match ip dscp, set ip dscp`

- Modification in QoS syntax to support IPv6 and IPv4

  New `match` criteria
  
  - `match dscp` — Match DSCP in v4/v6
  - `match precedence` — Match Precedence in v4/v6

  New `set` criteria
  
  - `set dscp` — Set DSCP in v4/v6
  - `set precedence` — Set Precedence in v4/v6

- Additional support for IPv6 does not always require new Command Line Interface (CLI)

  Example—WRED
## Scalability and Performance

- **IPv6 Neighbor Cache = ARP for IPv4**
  
  In dual-stack networks the first hop routers/switches will now have more memory consumption due to IPv6 neighbor entries (can be multiple per host) + ARP entries

  ARP entry for host in the campus distribution layer:

  Internet 10.120.2.200 2 000d.6084.2c7a ARPA Vlan2

  IPv6 Neighbor Cache entry:

  - 2001:DB8:CAFE:2:2891:1C0C:F52A:9DF1 4 000d.6084.2c7a STALE Vl2
  - 2001:DB8:CAFE:2:7DE5:E2B0:D4DF:97EC 16 000d.6084.2c7a STALE Vl2
  - FE80::7DE5:E2B0:D4DF:97EC 16 000d.6084.2c7a STALE Vl2

- Full internet route tables—ensure to account for TCAM/memory requirements for both IPv4/IPv6—not all vendors can properly support both

- Multiple routing protocols—IPv4 and IPv6 will have separate routing protocols. Ensure enough CPU/Memory is present

- Control plane impact when using tunnels—terminate ISATAP/configured tunnels in HW platforms when attempting large scale deployments (hundreds/thousands of tunnels)
Infrastructure Deployment

Start Here: Cisco IOS Software Release Specifics for IPv6 Features
http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/ftipv6s.htm
IPv6 Co-existence Solutions

Dual Stack

Recommended Enterprise Co-existence strategy

Tunneling Services

Connect Islands of IPv6 or IPv4

Translation Services

Connect to the IPv6 community
Campus/Data Center

Deploying IPv6 in Campus Networks:

ESE Campus Design and Implementation Guides:
Campus IPv6 Deployment
Three Major Options

- Dual-stack—The way to go for obvious reasons: performance, security, QoS, multicast and management
  Layer 3 switches should support IPv6 forwarding in hardware
- Hybrid—Dual-stack where possible, tunnels for the rest, but all leveraging the existing design/gear
  Pro—Leverage existing gear and network design (traditional L2/L3 and routed access)
  Con—Tunnels (especially ISATAP) cause unnatural things to be done to infrastructure (like core acting as access layer) and ISATAP does not support IPv6 multicast
- IPv6 Service Block—A new network block used for interim connectivity for IPv6 overlay network
  Pro—Separation, control and flexibility (still supports traditional L2/L3 and routed access)
  Con—Cost (more gear), does not fully leverage existing design, still have to plan for a real dual-stack deployment and ISATAP does not support IPv6 multicast
Campus IPv6 Deployment Options
Dual-Stack IPv4/IPv6

- #1 requirement—switching/routing platforms must support hardware based forwarding for IPv6
- IPv6 is transparent on L2 switches but—
  - L2 multicast—MLD snooping
  - IPv6 management—Telnet/SSH/HTTP/SNMP
  - Intelligent IP services on WLAN
- Expect to run the same IGPs as with IPv4
- VSS supports IPv6
Access Layer: Dual Stack

- Catalyst 3560/3750—In order to enable IPv6 functionality the proper SDM template needs to be defined (http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3750/12225see/scg/swsdm.htm#)

```
Switch(config)#sdm prefer dual-ipv4-and-ipv6 default
```

- If using a traditional Layer-2 access design, the only thing that needs to be enabled on the access switch (management/security discussed later) is MLD snooping:

```
Switch(config)#ipv6 mld snooping
```

Distribution Layer: HSRP, EIGRP and DHCPv6-relay (Layer 2 Access)

ipv6 unicast-routing
!
interface GigabitEthernet1/0/1
description To 6k-core-right
ipv6 address 2001:DB8:CAFE:1105::A001:1010/64
ipv6 eigrp 10
ipv6 hello-interval eigrp 10 1
ipv6 hold-time eigrp 10 3
ipv6 authentication mode eigrp 10 md5
ipv6 authentication key-chain eigrp 10 eigrp
!
interface GigabitEthernet1/0/2
description To 6k-core-left
ipv6 address 2001:DB8:CAFE:1106::A001:1010/64
ipv6 eigrp 10
ipv6 hello-interval eigrp 10 1
ipv6 hold-time eigrp 10 3
ipv6 authentication mode eigrp 10 md5
ipv6 authentication key-chain eigrp 10 eigrp
!
interface Vlan4
description Data VLAN for Access
ipv6 address 2001:DB8:CAFE:4::2/64
ipv6 nd prefix 2001:DB8:CAFE:4::/64 no-advertise
ipv6 nd managed-config-flag
ipv6 dhcp relay destination 2001:DB8:CAFE:10::2
ipv6 eigrp 10
standby version 2
standby 2 ipv6 autoconfig
standby 2 timers msec 250 msec 750
standby 2 priority 110
standby 2 preempt delay minimum 180
standby 2 authentication ese
!
ipv6 router eigrp 10
no shutdown
router-id 10.122.10.10
passive-interface Vlan4
passive-interface Loopback0

Some OS/patches may need “no-autoconfig”
Distribution Layer: Example with ULA and General Prefix feature

```plaintext
ipv6 general-prefix ULA-CORE FD9C:58ED:7D73::/53
ipv6 general-prefix ULA-ACC FD9C:58ED:7D73:1000::/53
ipv6 unicast-routing
!
interface GigabitEthernet1/0/1
description To 6k-core-right
ipv6 address ULA-CORE ::3:0:0:0:D63/64
ipv6 eigrp 10
ipv6 hello-interval eigrp 10 1
ipv6 hold-time eigrp 10 3
ipv6 authentication mode eigrp 10 md5
ipv6 authentication key-chain eigrp 10 eigrp
ipv6 summary-address eigrp 10 FD9C:58ED:7D73:1000::/53
!
interface GigabitEthernet1/0/2
description To 6k-core-left
ipv6 address ULA-CORE ::C:0:0:0:D63/64
ipv6 eigrp 10
ipv6 hello-interval eigrp 10 1
ipv6 hold-time eigrp 10 3
ipv6 authentication mode eigrp 10 md5
ipv6 authentication key-chain eigrp 10 eigrp
ipv6 summary-address eigrp 10 FD9C:58ED:7D73:1000::/53
!
interface Vlan4
description Data VLAN for Access
ipv6 address ULA-ACC ::D63/64
ipv6 nd prefix FD9C:58ED:7D73:1002::/64
no-advertise
ipv6 nd managed-config-flag
ipv6 dhcp relay destination fd9c:58ed:7d73:811::9
ipv6 eigrp 10
standby version 2
standby 2 ipv6 autoconfig
standby 2 timers msec 250 msec 750
standby 2 priority 110
standby 2 preempt delay minimum 180
standby 2 authentication ese
!
ipv6 router eigrp 10
no shutdown
router-id 10.122.10.10
passive-interface Vlan4
passive-interface Loopback0
```
### Distribution Layer: OSPF with NUD (Layer 2 Access)

```plaintext
<table>
<thead>
<tr>
<th>Distribution Layer: OSPF with NUD (Layer 2 Access)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ipv6</strong> unicast-routing</td>
</tr>
<tr>
<td><strong>ipv6</strong> multicast-routing</td>
</tr>
<tr>
<td><strong>ipv6</strong> cef distributed</td>
</tr>
<tr>
<td>!</td>
</tr>
<tr>
<td><strong>interface GigabitEthernet1/1</strong></td>
</tr>
<tr>
<td>description To 6k-core-right</td>
</tr>
<tr>
<td><strong>ipv6</strong> address 2001:DB8:CAFE:1105::A001:1010/64</td>
</tr>
<tr>
<td>no ipv6 redirects</td>
</tr>
<tr>
<td><strong>ipv6</strong> nd suppress-ra</td>
</tr>
<tr>
<td><strong>ipv6</strong> ospf network point-to-point</td>
</tr>
<tr>
<td><strong>ipv6</strong> ospf 1 area 0</td>
</tr>
<tr>
<td><strong>ipv6</strong> ospf hello-interval 1</td>
</tr>
<tr>
<td><strong>ipv6</strong> ospf dead-interval 3</td>
</tr>
<tr>
<td>!</td>
</tr>
<tr>
<td><strong>interface GigabitEthernet1/2</strong></td>
</tr>
<tr>
<td>description To 6k-core-left</td>
</tr>
<tr>
<td><strong>ipv6</strong> address 2001:DB8:CAFE:1106::A001:1010/64</td>
</tr>
<tr>
<td>no ipv6 redirects</td>
</tr>
<tr>
<td><strong>ipv6</strong> nd suppress-ra</td>
</tr>
<tr>
<td><strong>ipv6</strong> ospf network point-to-point</td>
</tr>
<tr>
<td><strong>ipv6</strong> ospf 1 area 0</td>
</tr>
<tr>
<td><strong>ipv6</strong> ospf hello-interval 1</td>
</tr>
<tr>
<td><strong>ipv6</strong> ospf dead-interval 3</td>
</tr>
<tr>
<td>!</td>
</tr>
<tr>
<td><strong>interface Vlan2</strong></td>
</tr>
<tr>
<td>description Data VLAN for Access</td>
</tr>
<tr>
<td><strong>ipv6</strong> address 2001:DB8:CAFE:2::A001:1010/64</td>
</tr>
<tr>
<td><strong>ipv6</strong> nd reachable-time 5000</td>
</tr>
<tr>
<td><strong>ipv6</strong> nd router-preference high</td>
</tr>
<tr>
<td>no ipv6 redirects</td>
</tr>
<tr>
<td><strong>ipv6</strong> ospf 1 area 1</td>
</tr>
<tr>
<td>!</td>
</tr>
<tr>
<td><strong>ipv6</strong> router ospf 1</td>
</tr>
<tr>
<td>auto-cost reference-bandwidth 10000</td>
</tr>
<tr>
<td>router-id 10.122.0.25</td>
</tr>
<tr>
<td>log-adjacency-changes</td>
</tr>
<tr>
<td>area 2 range 2001:DB8:CAFE:xxxx::/xx</td>
</tr>
<tr>
<td>timers spf 1 5</td>
</tr>
</tbody>
</table>
```
Access Layer: Dual Stack (Routed Access)

ipv6 unicast-routing
ipv6 cef

! interface GigabitEthernet1/0/25
description To 6k-dist-1
ipv6 address 2001:DB8:CAFE:1100::CAC1:3750/64
no ipv6 redirects
ipv6 nd suppress-ra
ipv6 ospf network point-to-point
ipv6 ospf 1 area 2
ipv6 ospf hello-interval 1
ipv6 ospf dead-interval 3
ipv6 cef

! interface GigabitEthernet1/0/26
description To 6k-dist-2
ipv6 address 2001:DB8:CAFE:1101::CAC1:3750/64
no ipv6 redirects
ipv6 nd suppress-ra
ipv6 ospf network point-to-point
ipv6 ospf 1 area 2
ipv6 ospf hello-interval 1
ipv6 ospf dead-interval 3
ipv6 cef

! interface Vlan2
description Data VLAN for Access
ipv6 address 2001:DB8:CAFE:2::CAC1:3750/64
ipv6 ospf 1 area 2
ipv6 cef

! ipv6 router ospf 1
router-id 10.120.2.1
log-adjacency-changes
auto-cost reference-bandwidth 10000
area 2 stub no-summary
passive-interface Vlan2
timers spf 1 5
Distribution Layer: Dual Stack (Routed Access)

ipv6 unicast-routing
ipv6 multicast-routing
ipv6 cef distributed

interface GigabitEthernet3/1
description To 3750-acc-1
ipv6 address 2001:DB8:CAFE:1100::A001:1010/64
no ipv6 redirects
ipv6 nd suppress-ra
ipv6 ospf network point-to-point
ipv6 ospf 1 area 2
ipv6 ospf hello-interval 1
ipv6 ospf dead-interval 3
ipv6 cef

interface GigabitEthernet1/2
description To 3750-acc-2
ipv6 address 2001:DB8:CAFE:1103::A001:1010/64
no ipv6 redirects
ipv6 nd suppress-ra
ipv6 ospf network point-to-point
ipv6 ospf 1 area 2
ipv6 ospf hello-interval 1
ipv6 ospf dead-interval 3
ipv6 cef

ipv6 router ospf 1
auto-cost reference-bandwidth 10000
router-id 10.122.0.25
log-adjacency-changes
area 2 stub no-summary
passive-interface Vlan2
area 2 range 2001:DB8:CAFE:xxxx::/xx
timers spf 1 5
Campus IPv6 Deployment Options
Hybrid Model

- Offers IPv6 connectivity via multiple options
  - Dual-stack
  - Configured tunnels—L3-to-L3
  - ISATAP—Host-to-L3
- Leverages existing network
- Offers natural progression to full dual-stack design
- May require tunneling to less-than-optimal layers (i.e. core layer)
- ISATAP creates a flat network (all hosts on same tunnel are peers)
  - Create tunnels per VLAN/subnet to keep same segregation as existing design (not clean today)
- Provides basic HA of ISATAP tunnels via old Anycast-RP idea
IPv6 ISATAP Implementation

ISATAP Host Considerations

- ISATAP is available on Windows XP, Windows 2003, Vista/Server 2008, port for Linux
- If Windows host does not detect IPv6 capabilities on the physical interface then an effort to use ISATAP is started
- Can learn of ISATAP routers via DNS “A” record lookup “isatap” or via static configuration
  - If DNS is used then Host/Subnet mapping to certain tunnels cannot be accomplished due to the lack of naming flexibility in ISATAP
  - Two or more ISATAP routers can be added to DNS and ISATAP will determine which one to use and also fail to the other one upon failure of first entry
    - If DNS zoning is used within the enterprise then ISATAP entries for different routers can be used in each zone
- In the presented design the static configuration option is used to ensure each host is associated with the correct ISATAP tunnel
- Can conditionally set the ISATAP router per host based on subnet, userid, department and possibly other parameters such as role
Highly Available ISATAP Design

Topology

- ISATAP tunnels from PCs in access layer to core switches
- Redundant tunnels to core or service block
- Use IGP to prefer one core switch over another (both v4 and v6 routes) — deterministic
- Preference is important due to the requirement to have traffic (IPv4/IPv6) route to the same interface (tunnel) where host is terminated on — Windows XP/2003
- Works like Anycast-RP with IPmc 😊
IPv6 Campus ISATAP Configuration

Redundant Tunnels

**ISATAP Primary**

```conf
interface Tunnel2
 ipv6 address 2001:DB8:CAFE:2::/64 eui-64
 no ipv6 nd suppress-ra
 ipv6 ospf 1 area 2
 tunnel source Loopback2
 tunnel mode ipv6ip isatap
!
interface Tunnel3
 ipv6 address 2001:DB8:CAFE:3::/64 eui-64
 no ipv6 nd suppress-ra
 ipv6 ospf 1 area 2
 tunnel source Loopback3
 tunnel mode ipv6ip isatap
!
interface Loopback2
 description Tunnel source for ISATAP-VLAN2
 ip address 10.122.10.102 255.255.255.255
!
interface Loopback3
 description Tunnel source for ISATAP-VLAN3
 ip address 10.122.10.103 255.255.255.255
```

**ISATAP Secondary**

```conf
interface Tunnel2
 ipv6 address 2001:DB8:CAFE:2::/64 eui-64
 no ipv6 nd suppress-ra
 ipv6 ospf 1 area 2
 ipv6 ospf cost 10
 tunnel source Loopback2
 tunnel mode ipv6ip isatap
!
interface Tunnel3
 ipv6 address 2001:DB8:CAFE:3::/64 eui-64
 no ipv6 nd suppress-ra
 ipv6 ospf 1 area 2
 ipv6 ospf cost 10
 tunnel source Loopback3
 tunnel mode ipv6ip isatap
!
interface Loopback2
 ip address 10.122.10.102 255.255.255.255
delay 1000
!
interface Loopback3
 ip address 10.122.10.103 255.255.255.255
delay 1000
```
IPv6 Campus ISATAP Configuration
IPv4 and IPv6 Routing—Options

- To influence IPv4 routing to prefer one ISATAP tunnel source over another—alter delay/cost or mask length
- Lower timers (timers spf, hello/hold, dead) to reduce convergence times
- Use recommended summarization and/or use of stubs to reduce routes and convergence times

**ISATAP Secondary—Bandwidth adjustment**

```plaintext
interface Loopback2
ip address 10.122.10.102 255.255.255.255
delay 1000
```

**ISATAP Primary—Longest-match adjustment**

```plaintext
interface Loopback2
ip address 10.122.10.102 255.255.255.255
```

**ISATAP Secondary—Longest-match adjustment**

```plaintext
interface Loopback2
ip address 10.122.10.102 255.255.255.254
```

**IPv4—EIGRP**

```plaintext
router eigrp 10
eigrp router-id 10.122.10.3
```

**IPv6—OSPFv3**

```plaintext
ipv6 router ospf 1
router-id 10.122.10.3
```

---

Set RID to ensure redundant loopback addresses do not cause duplicate RID issues
Distribution Layer Routes
Primary/Secondary Paths to ISATAP Tunnel Sources

Before Failure

```
dist-1#show ip route | b 10.122.10.102/32
D 10.122.10.102/32 [90/130816] via 10.122.0.41, 00:09:23, GigabitEthernet1/0/27
```

After Failure

```
dist-1#show ip route | b 10.122.10.102/32
D 10.122.10.102/32 [90/258816] via 10.122.0.49, 00:00:08, GigabitEthernet1/0/28
```
IPv6 Campus ISATAP Configuration
ISATAP Client Configuration

Windows XP/Vista Host

C:\>netsh int ipv6 isatap set router 10.122.10.103
Ok.

interface Tunnel3
ipv6 address 2001:DB8:CAFE:3::/64 eui-64
no ipv6 nd suppress-ra
ipv6 eigrp 10
tunnel source Loopback3
tunnel mode ipv6ip isatap
!
interface Loopback3
description Tunnel source for ISATAP-VLAN3
ip address 10.122.10.103 255.255.255.255

Tunnel adapter Automatic Tunneling Pseudo-Interface:
Connection-specific DNS Suffix . :
IP Address . . . . . . . . . . . . . . . . . : 2001:db8:cafe:3:0:5efe:10.120.3.101
IP Address . . . . . . . . . . . . . . . . . : fe80::5efe:10.120.3.101%2
Default Gateway . . . . . . . . . . . . . : fe80::5efe:10.122.10.103%2
IPv6 Configured Tunnels
Think GRE or IP-in-IP Tunnels

- Encapsulating IPv6 into IPv4
- Used to traverse IPv4 only devices/links/networks
- Treat them just like standard IP links (only insure solid IPv4 routing/HA between tunnel interfaces)
- Provides for same routing, QoS, multicast as with dual-stack
- In HW, performance should be similar to standard tunnels

```
interface Tunnel0
  ipv6 cef
  ipv6 address 2001:DB8:CAFE:13::1/127
  ipv6 eigrp 10
  tunnel source Loopback3
tunnel destination 172.16.2.1
tunnel mode ipv6ip

interface GigabitEthernet1/1
  ipv6 address 2001:DB8:CAFE:13::4/127
  ipv6 eigrp 10
  ipv6 cef

interface Loopback3
  ip address 172.16.1.1 255.255.255.252
```
Campus Hybrid Model 1

QoS

1. Classification and marking of IPv6 is done on the egress interfaces on the core layer switches because packets have been tunneled until this point—QoS policies for classification and marking cannot be applied to the ISATAP tunnels on ingress.

2. The classified and marked IPv6 packets can now be examined by upstream switches (e.g. aggregation layer switches) and the appropriate QoS policies can be applied on ingress. These polices may include trust (ingress), policing (ingress) and queuing (egress).
Campus Hybrid Model 1
QoS Configuration Sample—Core Layer

```plaintext
mls qos
!
class-map match-all CAMPUS-BULK-DATA
   match access-group name BULK-APPS
class-map match-all CAMPUS-TRANSACTIONAL-DATA
   match access-group name TRANSACTIONAL-APPS
!
policy-map IPv6-ISATAP-MARK
   class CAMPUS-BULK-DATA
      set dscp af11
   class CAMPUS-TRANSACTIONAL-DATA
      set dscp af21
   class class-default
      set dscp default
!
ipv6 access-list BULK-APPS
   permit tcp any any eq ftp
   permit tcp any any eq ftp-data
!
ipv6 access-list TRANSACTIONAL-APPS
   permit tcp any any eq telnet
   permit tcp any any eq 22
!
interface GigabitEthernet2/1
description to 6k-agg-1
mls qos trust dscp
service-policy output IPv6-ISATAP-MARK
!
interface GigabitEthernet2/2
description to 6k-agg-2
mls qos trust dscp
service-policy output IPv6-ISATAP-MARK
!
interface GigabitEthernet2/3
description to 6k-core-1
mls qos trust dscp
service-policy output IPv6-ISATAP-MARK
```
Campus IPv6 Deployment Options
IPv6 Service Block—an Interim Approach

- Provides ability to rapidly deploy IPv6 services without touching existing network
- Provides tight control of where IPv6 is deployed and where the traffic flows (maintain separation of groups/locations)
- Offers the same advantages as Hybrid Model without the alteration to existing code/configurations
- Configurations are very similar to the Hybrid Model
  - ISATAP tunnels from PCs in access layer to service block switches (instead of core layer—Hybrid)
- 1) Leverage existing ISP block for both IPv4 and IPv6 access
- 2) Use dedicated ISP connection just for IPv6—Can use IOS FW or PIX/ASA appliance

Diagram:
- VLAN 2
- VLAN 3
- IPv4-only Campus Block
- ISATAP
- Primary ISATAP Tunnel
- Secondary ISATAP Tunnel
- Data Center Block
- WAN/ISP Block
- Dedicated FW
- IOS FW
- Internet

Presentation_ID © 2006 Cisco Systems, Inc. All rights reserved. Cisco Public
Campus Service Block
QoS from Access Layer

1. Same policy design as Hybrid Model—The first place to implement classification and marking from the access layer is after decapsulation (ISATAP) which is on the egress interfaces on the service block switches.

2. IPv6 packets received from ISATAP interfaces will have egress policies (classification/ marking) applied on the configured tunnel interfaces.

3. Aggregation/access switches can apply egress/ingress policies (trust, policing, queuing) to IPv6 packets headed for DC services.
Cisco VSS – DSM / Hybrid / Service Block

- Cisco VSS offers a greatly simplified configuration and extremely fast convergence for IPv6 deployment
- Dual stack – Place VSS pair in distribution and/or core layers – HA and simplified/reduced IPv6 configuration
- Hybrid model – If terminating tunnels against VSS (i.e. VSS at core layer), MUCH easier to configure tunnels for HA as only one tunnel configuration is needed
- Service Block – Use VSS as the SB pair – again, GREATLY simplified configuration and decrease convergence times!!
IPv6 Data Center Integration

- Front-end design will be similar to campus based on feature, platform and connectivity similarities – Nexus, 6500 4900M
- The single most overlooked and potentially complicated area of IPv6 deployment
- IPv6 for SAN is supported in SAN-OS 3.0
- Stuff people don’t think about:
  - NIC Teaming, iLO, DRAC, IP KVM, Clusters
- Build an IPv6-only server farm?
Virtualized DC Solutions

What about the apps?
IPv6 in the Enterprise Data Center

Biggest Challenges Today

- Network services above L3
  - SLB, SSL-Offload, application monitoring (probes)
  - Application Optimization
  - High-speed security inspection/perimeter protection

- Application support for IPv6 – Know what you don’t know
  - If an application is protocol centric (IPv4):
    - Needs to be rewritten
    - Needs to be translated until it is replaced
    - Wait and pressure vendors to move to protocol agnostic framework

- Virtualized and Consolidated Data Centers
  - Virtualization ‘should’ make DCs simpler and more flexible
  - Lack of robust DC/Application management is often the root cause of all evil
  - Ensure management systems support IPv6 as well as the devices being managed
Commonly Deployed IPv6-enabled OS/Apps

Operating Systems
- Windows 7
- Windows Server 2008/R2
- SUSE
- Red Hat
- Ubuntu
- The list goes on

Virtualization & Applications
- VMware vSphere 4.1
- Microsoft Hyper-V
- Microsoft Exchange 2007 SP1/2010
- Apache/IIS Web Services
- Windows Media Services
- Multiple Line of Business apps

Most commercial applications won’t be your problem – it will be the custom/home-grown apps
IPv6 Deployment in the Data Center

Services/Appliances Do Not Support IPv6

<table>
<thead>
<tr>
<th>Transparent</th>
<th>One-Armed</th>
<th>Routed</th>
<th>Dedicated Server Farm</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 traffic is bridged between VLANs</td>
<td>IPv6 traffic bypasses services</td>
<td>Create trunk between switch and server</td>
<td>New IPv6 only servers can be connected to existing access/agg pair on different VLANs</td>
</tr>
<tr>
<td>Permit Ethertype 0x86dd (IPv6)</td>
<td>IPv4 traffic is sent to one-arm attached module/appliance</td>
<td>IPv4 has default gateway on service module</td>
<td>New access/agg switches just for IPv6 servers</td>
</tr>
</tbody>
</table>

- IPv4 server
- IPv6 server
- Dual stack server

VLAN103
VLAN203
Switch
Dual stack server

VLAN10
Trunk
Switch
VLAN11
Dual stack server

Permit 0x86dd
Switch
IPv4
IPv6
Deploying IPv6 in Branch Networks:

ESE WAN/Branch Design and Implementation Guides:
http://www.cisco.com/en/US/netsol/ns656/networking_solutions_design_guidances_list.html#anchor1
WAN/Branch Deployment

- Cisco routers have supported IPv6 for a long time.
- Dual-stack should be the focus of your implementation—but, some situations still call for tunneling.
- Support for every media/WAN type you want to use (Frame Relay, leased-line, broadband, MPLS, etc.).
- Don’t assume all features for every technology are IPv6-enabled.
- Better feature support in WAN/branch than in campus/DC.
IPv6 Enabled Branch
Focus more on the provider and less on the gear

Branch
Single Tier
HQ
Internet
Dual-Stack
IPSec VPN (IPv4/IPv6)
Firewall (IPv4/IPv6)
Integrated Switch (MLD-snooping)

Branch
Dual Tier
HQ
Internet
Frame
Dual-Stack
IPSec VPN or Frame Relay
Firewall (IPv4/IPv6)
Switches (MLD-snooping)

Branch
Multi-Tier
HQ
MPLS
Dual-Stack
IPSec VPN or MPLS (6PE/6VPE)
Firewall (IPv4/IPv6)
Switches (MLD-snooping)

SP support for port-to-port IPv6?
SP support for various WAN types?
Single-Tier Profile

- Totally integrated solution—Branch router and integrated EtherSwitch module—IOS FW and VPN for IPv6 and IPv4
- When SP does not offer IPv6 services, use IPv4 IPSec VPNs for manually configured tunnels (IPv6-in-IPv4) or DMVPN for IPv6
- When SP does offer IPv6 services, use IPv6 IPSec VPNs (latest AIM/VAM supports IPv6 IPSec)
Single-Tier Profile
LAN Configuration—DHCPv6

ipv6 unicast-routing
ipv6 multicast-routing
ipv6 cef
!
ipv6 dhcp pool DATA_VISTA
  address prefix 2001:DB8:CAFE:1100::/64
domain-name cisco.com
!
interface GigabitEthernet1/0.100
  description DATA VLAN for Computers
  encapsulation dot1Q 100
  ipv6 address 2001:DB8:CAFE:1100::BAD1:A001/64
  ipv6 nd prefix 2001:DB8:CAFE:1100::/64 no-advertise
  ipv6 nd managed-config-flag
  ipv6 dhcp server DATA_VISTA

ipv6 mld snooping
!
interface Vlan100
  description VLAN100 for PCs and Switch management
  ipv6 address 2001:DB8:CAFE:1100::BAD2:F126/64
crypto isakmp policy 1
   encr 3des
   authentication pre-share
crypto isakmp key CISCO address 172.17.1.3
crypto isakmp key SYSTEMS address 172.17.1.4
crypto isakmp keepalive 10
!
crypto ipsec transform-set HE1 esp-3des esp-sha-hmac
crypto ipsec transform-set HE2 esp-3des esp-sha-hmac
!
crypto map IPv6-HE1 local-address Serial0/0/0
crypto map IPv6-HE1 1 ipsec-isakmp
   set peer 172.17.1.3
   set transform-set HE1
   match address VPN-TO-HE1
!
crypto map IPv6-HE2 local-address Loopback0
crypto map IPv6-HE2 1 ipsec-isakmp
   set peer 172.17.1.4
   set transform-set HE2
   match address VPN-TO-HE2
Single-Tier Profile
IPSec Configuration—2

interface Tunnel3
  description IPv6 tunnel to HQ Head-end 1
delay 500
ipv6 address 2001:DB8:CAF0E:1261::BAD1:A001/64
ipv6 mtu 1400
tunnel source Serial0/0/0
tunnel destination 172.17.1.3
tunnel mode ipv6ip
!
interface Tunnel4
  description IPv6 tunnel to HQ Head-end 2
delay 2000
ipv6 address 2001:DB8:CAF0E:1271::BAD1:A001/64
ipv6 mtu 1400
tunnel source Loopback0
tunnel destination 172.17.1.4
tunnel mode ipv6ip
!
interface Serial0/0/0
  description to T1 Link Provider (PRIMARY)
crypto map IPv6-HE1

interface Dialer1
  description PPPoE to BB provider
crypto map IPv6-HE2
!
ip access-list extended VPN-TO-HE1
  permit 41 host 172.16.1.2 host 172.17.1.3
ip access-list extended VPN-TO-HE2
  permit 41 host 10.124.100.1 host 172.17.1.4

- Adjust delay to prefer Tunnel3
- Adjust MTU to avoid fragmentation on router (PMTUD on client will not account for IPSec/Tunnel overheard)
- Permit “41” (IPv6) instead of “gre”
Single-Tier Profile
Routing

ipv6 unicast-routing
ipv6 cef
!
key chain ESE
  key 1
    key-string 7 111B180B101719
!
interface Tunnel3
  description IPv6 tunnel to HQ Head-end 1
delay 500
  ipv6 eigrp 10
  ipv6 hold-time eigrp 10 35
  ipv6 authentication mode eigrp 10 md5
  ipv6 authentication key-chain eigrp 10 ESE
!
interface Tunnel4
  description IPv6 tunnel to HQ Head-end 2
delay 2000
  ipv6 eigrp 10
  ipv6 hold-time eigrp 10 35
  ipv6 authentication mode eigrp 10 md5
  ipv6 authentication key-chain eigrp 10 ESE
!
interface Loopback0
  ipv6 eigrp 10
!
interface GigabitEthernet1/0.100
  description DATA VLAN for Computers
  ipv6 eigrp 10
!
ipv6 router eigrp 10
  router-id 10.124.100.1
  stub connected summary
  no shutdown
  passive-interface GigabitEthernet1/0.100
  passive-interface GigabitEthernet1/0.200
  passive-interface GigabitEthernet1/0.300
  passive-interface Loopback0

ipv6 route ::/0 Vlan100 FE80::217:94FF:FE90:2829

EtherSwitch Module
ipv6 inspect name v6FW tcp
ipv6 inspect name v6FW icmp
ipv6 inspect name v6FW ftp
ipv6 inspect name v6FW udp

interface Tunnel3
ipv6 traffic-filter INET-WAN-v6 in
no ipv6 redirects
no ipv6 unreachables
ipv6 inspect v6FW out
ipv6 virtual-reassembly

interface GigabitEthernet1/0.100
ipv6 traffic-filter DATA_LAN-v6 in

line vty 0 4
ipv6 access-class MGMT-IN in

Inspection profile for TCP, ICMP, FTP and UDP
ACL used by IOS FW for dynamic entries
Apply firewall inspection For egress traffic
Used by firewall to create dynamic ACLs and protect against various fragmentation attacks
Apply LAN ACL (next slide)
ACL used to restrict management access
ipv6 access-list MGMT-IN
  remark permit mgmt only to loopback
  permit tcp 2001:DB8:CAFE::/48 host 2001:DB8:CAFE:1000::BAD1:A001
  deny ipv6 any any log-input
!
ipv6 access-list DATA_LAN-v6
  remark PERMIT ICMPv6 PACKETS FROM HOSTS WITH PREFIX CAFE:1100::/64
  permit icmp 2001:DB8:CAFE:1100::/64 any
  remark PERMIT IPv6 PACKETS FROM HOSTS WITH PREFIX CAFE:1100::64
  permit ipv6 2001:DB8:CAFE:1100::/64 any
  remark PERMIT ALL ICMPv6 PACKETS SOURCED BY HOSTS USING THE LINK-LOCAL PREFIX
  permit icmp FE80::/10 any
  remark PERMIT DHCPv6 ALL-DHCP-AGENTS REQUESTS FROM HOSTS
  permit udp any eq 546 any eq 547
  remark DENY ALL OTHER IPv6 PACKETS AND LOG
  deny ipv6 any any log-input
ipv6 access-list INET-WAN-v6
remark PERMIT EIGRP for IPv6
permit 88 any any
remark PERMIT PIM for IPv6
permit 103 any any
remark PERMIT ALL ICMPv6 PACKETS SOURCED USING THE LINK-LOCAL PREFIX
permit icmp FE80::/10 any
remark PERMIT SSH TO LOCAL LOOPBACK
permit tcp any host 2001:DB8:CAFE:1000::BAD1:A001 eq 22
remark PERMIT ALL ICMPv6 PACKETS TO LOCAL LOOPBACK, VPN tunnels, VLANs
permit icmp any host 2001:DB8:CAFE:1000::BAD1:A001
permit icmp any host 2001:DB8:CAFE:1261::BAD1:A001
permit icmp any host 2001:DB8:CAFE:1271::BAD1:A001
permit icmp any 2001:DB8:CAFE:1100::/64
permit icmp any 2001:DB8:CAFE:1200::/64
permit icmp any 2001:DB8:CAFE:1300::/64
remark PERMIT ALL IPv6 PACKETS TO VLANs
permit ipv6 any 2001:DB8:CAFE:1100::/64
permit ipv6 any 2001:DB8:CAFE:1200::/64
permit ipv6 any 2001:DB8:CAFE:1300::/64
deny ipv6 any any log
Single-Tier Profile

QoS

class-map match-any BRANCH-TRANSACTIONAL-DATA
match protocol citrix
match protocol ldap
match protocol sqlnet
match protocol http url "*cisco.com"
match access-group name BRANCH-TRANSACTIONAL-V6

policy-map BRANCH-WAN-EDGE
class TRANSACTIONAL-DATA
  bandwidth percent 12
  random-detect dscp-based
!
policy-map BRANCH-LAN-EDGE-IN
  class BRANCH-TRANSACTIONAL-DATA
    set dscp af21
!
ipv6 access-list BRANCH-TRANSACTIONAL-V6
  remark Microsoft RDP traffic-mark dscp af21
  permit tcp any any eq 3389
  permit udp any any eq 3389

interface GigabitEthernet1/0.100
  description DATA VLAN for Computers
  service-policy input BRANCH-LAN-EDGE-IN
!
interface Serial0/0/0
  description to T1 Link Provider
  max-reserved-bandwidth 100
  service-policy output BRANCH-WAN-EDGE

- Some features of QoS do not yet support IPv6
- NBAR is used for IPv4, but ACLs must be used for IPv6 (until NBAR supports IPv6)
- Match/Set v4/v6 packets in same policy
Dual-Tier Profile

- Redundant set of branch routers—separate branch switch (multiple switches can use StackWise technology)
- Can be dual-stack if using Frame Relay or other L2 WAN type
Dual-Tier Profile Configuration

Branch Router 1

interface Serial0/1/0.17 point-to-point
description TO FRAME-RELAY PROVIDER
ipv6 address 2001:DB8:CAFE:1262::BAD1:1010/64
ipv6 eigrp 10
ipv6 hold-time eigrp 10 35
ipv6 authentication mode eigrp 10 md5
ipv6 authentication key-chain eigrp 10 ESE
frame-relay interface-dlci 17
class QOS-BR2-MAP
!
interface FastEthernet0/0.100
ipv6 address 2001:DB8:CAFE:2100::BAD1:1010/64
ipv6 traffic-filter DATA_LAN-v6 in
ipv6 nd other-config-flag
ipv6 dhcp server DATA_VISTA
ipv6 eigrp 10
standby version 2
standby 201 ipv6 autoconfig
standby 201 priority 120
standby 201 preempt delay minimum 30
standby 201 authentication ese
standby 201 track Serial0/1/0.17 90

Branch Router 2

interface Serial0/2/0.18 point-to-point
description TO FRAME-RELAY PROVIDER
ipv6 address 2001:DB8:CAFE:1272::BAD1:1020/64
ipv6 eigrp 10
ipv6 hold-time eigrp 10 35
ipv6 authentication mode eigrp 10 md5
ipv6 authentication key-chain eigrp 10 ESE
frame-relay interface-dlci 18
class QOS-BR2-MAP
!
interface FastEthernet0/0.100
ipv6 address 2001:DB8:CAFE:2100::BAD1:1020/64
ipv6 traffic-filter DATA_LAN-v6 in
ipv6 nd other-config-flag
ipv6 dhcp server DATA_VISTA
ipv6 eigrp 10
standby version 2
standby 201 ipv6 autoconfig
standby 201 preempt	hestandby 201 authentication ese
Multi-Tier Profile

- All branch elements are redundant and separate
  - WAN tier—WAN connections—can be anything (frame/IPSec)—MPLS shown here
  - Firewall tier—redundant ASA firewalls
  - Access tier—internal services routers (like a campus distribution layer)
  - LAN tier—access switches (like a campus access layer)

- Dual-stack is used on every tier—if SP provides IPv6 services via MPLS. If not, tunnels can be used from WAN tier to HQ site
Hybrid Branch Example

- Mixture of attributes from each profile
- An example to show configuration for different tiers
- Basic HA in critical roles is the goal
**DMVPN with IPv6**

**Hub Configuration Example**

crypto isakmp policy 1
   encr aes 256
   authentication pre-share
   group 2
!
crypto isakmp key CISCO address 0.0.0.0 0.0.0.0

crypto isakmp key CISCO address ipv6 ::/0
!
crypto ipsec transform-set HUB esp-aes 256 esp-sha-hmac
!
crypto ipsec profile HUB
   set transform-set HUB

interface Tunnel0
   description DMVPN Tunnel 1
   ip address 10.126.1.1 255.255.255.0
   ipv6 address 2001:DB8:CAFE:20A::1/64
   ipv6 mtu 1416
   ipv6 eigrp 10
   ipv6 hold-time eigrp 10 35
   no ipv6 next-hop-self eigrp 10
   no ipv6 split-horizon eigrp 10
   ipv6 nhrp authentication CISCO
   ipv6 nhrp map multicast dynamic
   ipv6 nhrp network-id 10
   ipv6 nhrp holdtime 600
   ipv6 nhrp redirect
   tunnel source Serial1/0
   tunnel mode gre multipoint
   tunnel key 10
   tunnel protection ipsec profile HUB
DMVPN with IPv6
Spoke Configuration Example

crypto isakmp policy 1
  encr aes 256
  authentication pre-share
group 2!
crypto isakmp key CISCO address 0.0.0.0 0.0.0.0
crypto isakmp key CISCO address ipv6 ::/0!
crypto ipsec transform-set SPOKE esp-aes 256 esp-sha-hmac!
crypto ipsec profile SPOKE
  set transform-set SPOKE

interface Tunnel0
  description to HUB
  ip address 10.126.1.2 255.255.255.0
  ipv6 address 2001:DB8:CAFE:20A::2/64
  ipv6 mtu 1416
  ipv6 eigrp 10
  ipv6 hold-time eigrp 10 35
  no ipv6 next-hop-self eigrp 10
  no ipv6 split-horizon eigrp 10
  ipv6 nhrp authentication CISCO
  ipv6 nhrp map 2001:DB8:CAFE:20A::1/64 172.16.1.1
  ipv6 nhrp map multicast 172.16.1.1
  ipv6 nhrp network-id 10
  ipv6 nhrp holdtime 600
  ipv6 nhrp nhs 2001:DB8:CAFE:20A::1
  ipv6 nhrp shortcut
tunnel source Serial1/0
tunnel mode gre multipoint
tunnel key 10
tunnel protection ipsec profile SPOKE
ASA with IPv6

Snippet of full config – examples of IPv6 usage

```
name 2001:db8:cafe:1003:: BR1-LAN description VLAN on EtherSwitch
name 2001:db8:cafe:1004:9db8:3df1:814c:d3bc Br1-v6-Server

interface GigabitEthernet0/0
description TO WAN
nameif outside
security-level 0
ip address 10.124.1.4 255.255.255.0 standby 10.124.1.5
ipv6 address 2001:db8:cafe:1000::4/64 standby 2001:db8:cafe:1000::5

! 
interface GigabitEthernet0/1
description TO BRANCH LAN
nameif inside
security-level 100
ip address 10.124.3.1 255.255.255.0 standby 10.124.3.2
ipv6 address 2001:db8:cafe:1002::1/64 standby 2001:db8:cafe:1002::2

! 
ipv6 route inside BR1-LAN/64 2001:db8:cafe:1002::3
ipv6 route outside ::/0 fe80::5:73ff:fea0:2
! 
ipv6 access-list v6-ALLOW permit icmp6 any any
ipv6 access-list v6-ALLOW permit tcp 2001:db8:cafe::/48 host Br1-v6-Server object-group RDP
! 
failover
failover lan unit primary
failover lan interface FO-LINK GigabitEthernet0/3
failover interface ip FO-LINK 2001:db8:cafe:1001::1/64 standby 2001:db8:cafe:1001::2
access-group v6-ALLOW in interface outside
```
ipv6 dhcp pool DATA_W7
dns-server 2001:DB8:CAFE:102::8
domain-name cisco.com
!
interface GigabitEthernet0/0
description to BR1-LAN-SW
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/0.104
description VLAN-PC
encapsulation dot1Q 104
ip address 10.124.104.1 255.255.255.0
ipv6 address 2001:DB8:CAFE:1004::1/64
ipv6 nd other-config-flag
ipv6 dhcp server DATA_W7
ipv6 eigrp 10
!
interface GigabitEthernet0/0.105
description VLAN-PHONE
encapsulation dot1Q 105
ip address 10.124.105.1 255.255.255.0
ipv6 address 2001:DB8:CAFE:1005::1/64
ipv6 nd prefix 2001:DB8:CAFE:1005::/64 0 0 no-autoconfig
ipv6 nd managed-config-flag
ipv6 dhcp relay destination 2001:DB8:CAFE:102::9
ipv6 eigrp 10
Remote Access
Cisco Remote VPN – IPv6

- Cisco VPN Client 4.x
  IPv4 IPSec Termination (PIX/ASA/IOS VPN/Concentrator)
  IPv6 Tunnel Termination (IOS ISATAP or Configured Tunnels)

- AnyConnect Client 2.x
  SSL/TLS or DTLS (datagram TLS = TLS over UDP)
  Tunnel transports both IPv4 and IPv6 and the packets exit the tunnel at the hub ASA as native IPv4 and IPv6.
AnyConnect 2.x—SSL VPN

asa-edge-1#show vpn-sessiondb svc

Session Type: SVC
Username: ciscoese
Assigned IP: 10.123.2.200
Protocol: Clientless SSL-Tunnel DTLS-Tunnel
License: SSL VPN
Encryption: RC4 AES128
Bytes Tx: 79763
Bytes Rx: 176080
Group Policy: AnyGrpPolicy
Login Time: 14:09:25 MST Mon Dec 17 2007
Duration: 0h:47m:48s
NAC Result: Unknown
VLAN Mapping: N/A

Cisco ASA
AnyConnect 2.x—Summary Configuration

interface GigabitEthernet0/0
  nameif outside
  security-level 0
  ip address 10.123.1.4 255.255.255.0
  ipv6 enable

interface GigabitEthernet0/1
  nameif inside
  security-level 100
  ip address 10.123.2.4 255.255.255.0
  ipv6 address 2001:db8:cafe:101::ffff/64

ipv6 local pool ANYv6POOL 2001:db8:cafe:101::101/64 200

webvpn
  enable outside
  svc enable
  tunnel-group-list enable
  group-policy AnyGrpPolicy internal
  group-policy AnyGrpPolicy attributes
    vpn-tunnel-protocol svc
    default-domain value cisco.com
    address-pools value AnyPool
  tunnel-group ANYCONNECT type remote-access
  tunnel-group ANYCONNECT general-attributes
    address-pool AnyPool
  ipv6-address-pool ANYv6POOL
default-group-policy AnyGrpPolicy
  tunnel-group ANYCONNECT webvpn-attributes
  group-alias ANYCONNECT enable

IPv6-in-IPv4 Tunnel Example—Cisco VPN Client
Considerations

- Cisco IOS® version supporting IPv6 configured/ISATAP tunnels
  - Configured—12.3(1)M/12.3(2)T/12.2(14)S and above (12.4M/12.4T)
  - ISATAP—12.3(1)M, 12.3(2)T, 12.2(14)S and above (12.4M/12.4T)
  - Catalyst® 6500 with Sup720/32—12.2(17a)SX1—HW forwarding

- Be aware of the security issues if split-tunneling is used
  - Attacker can come in IPv6 interface and jump on the IPv4 interface (encrypted to enterprise)
  - In Windows Firewall—default policy is to DENY packets from one interface to another

- Remember that the IPv6 tunneled traffic is still encapsulated as a tunnel when it leaves the VPN device

- Allow IPv6 tunneled traffic across access lists (Protocol 41)
Does It Work?

**Interface 2: Automatic Tunneling Pseudo-Interface**

<table>
<thead>
<tr>
<th>Addr Type</th>
<th>DAD State</th>
<th>Valid Life</th>
<th>Pref. Life</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public</td>
<td>Preferred</td>
<td>29d23h56m5s</td>
<td>6d23h56m5s</td>
<td>2001:db8:c003:1101:0:5efe:10.1.99.102</td>
</tr>
<tr>
<td>Link</td>
<td>Preferred</td>
<td>infinite</td>
<td>infinite</td>
<td>fe80::5efe:10.1.99.102</td>
</tr>
</tbody>
</table>

`netsh interface ipv6>show route`  
`Querying active state...`

<table>
<thead>
<tr>
<th>Publish</th>
<th>Type</th>
<th>Met</th>
<th>Prefix</th>
<th>Idx</th>
<th>Gateway/Interface Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Autoconf</td>
<td>9</td>
<td>2001:db8:c003:1101::/64</td>
<td>2</td>
<td>Automatic Tunneling Pseudo-Interface</td>
</tr>
<tr>
<td>no</td>
<td>Manual</td>
<td>1</td>
<td>::/0</td>
<td>2</td>
<td>fe80::5efe:20.1.1.1</td>
</tr>
</tbody>
</table>

**VPN 3000**

**Windows XP Client**

IPv6 address: 2001:db8:c003:1101:0:5efe:10.1.99.102

**Catalyst 6500/Sup 720 Dual-Stack**

VPN Address: 10.1.99.102—VPN Address

10.1.99.102—IPv6 address
Provider Considerations
Top SP Concerns for Enterprise Accounts

- Port to Port Access
- Multi-Homing
- IPv6
- Content
- Provisioning
Port-to-Port Access

Port to Port Access

Multi-Homing

IPv6

Content

Provisioning

Basic Internet

• Dual-stack or native IPv6 at each POP
• SLA driven just like IPv4 to support VPN, content access

MPLS

• 6VPE
• IPv6 Multicast
• End-to-End traceability

Hosted (see content)

• IPv6 access to hosted content
• Cloud migration (move data from Ent DC to Hosted DC)

* = most common issue
Multi-Homing

PI/PA Policy Concerns
- PA is no good for customers with multiple providers or change them at any pace
- PI is new, constantly changing expectations and no “guarantee” an SP won’t do something stupid like not route PI space
- Customers fear that RIR will review existing IPv4 space and want it back if they get IPv6 PI

NAT
- Religious debate about the security exposure – not a multi-homing issue
- If customer uses NAT like they do today to prevent address/policy exposure, where do they get the technology from – no scalable IPv6 NAT exists today

Routing
- Is it really different from what we do today with IPv4? Is this policy stuff?
- Guidance on prefixes per peering point, per theater, per ISP, ingress/egress rules, etc.. – this is largely missing today
Content

Port to Port Access
Multi-Homing
IPv6
Provisioning

Hosted/Cloud Apps today
- IPv6 provisioning and access to hosted or cloud-based services today (existing agreements)
- Salesforce.com, Microsoft BPOS (Business Productivity Online Services), Amazon, Google Apps

Move to Hosted/Cloud
- Movement from internal-only DC services to hosted/cloud-based DC
- Provisioning, data/network migration services, DR/HA

Contract/Managed Marketing/Portals
- Third-party marketing, business development, outsourcing
- Existing contracts – connect over IPv6
Provisioning

Port to Port Access

- IPv6

Multi-Homing

Content

Provisioning

SP Self-Service Portals

- Not a lot of information from accounts on this but it does concern them
- How can they provision their own services (i.e. cloud) to include IPv6 services and do it over IPv6

SLA

- More of a management topic but the point here is that customers want the ability to alter their services based on violations, expiration or restrictions on the SLA
- Again, how can they do this over IPv6 AND for IPv6 services
The Scope of IPv6 Deployment

Web Content Management

Applications & Application Suites

- Data Center Servers
- Client Access (PC’s)
- Printers
- Collaboration Devices & Gateways
- Sensors & Controllers

Networked Device Support

- DNS & DHCP
- Load Balancing & Content Switching
- Security (Firewalls & IDS/IPS)
- Content Distribution
- Optimization (WAAS, SSL acceleration)
- VPN Access

Networked Infrastructure Services

- Deployment Scenario
  - IPv6 over IPv4 Tunnels (Configured, 6to4, ISATAP, GRE)
  - Dual-Stack
  - IPv6 over MPLS (6PE/6VPE)

IP Services (QoS, Multicast, Mobility, Translation)

- Hardware Support
- Connectivity
- IP Addressing
- Routing Protocols
- Instrumentation

Basic Network Infrastructure

Roll-out Releases & Planning

Staff Training and Operations
Conclusion

- “Dual stack where you can – Tunnel where you must”
- Create a virtual team of IT representatives from every area of IT to ensure coverage for OS, Apps, Network and Operations/Management
- Microsoft Windows Vista, 7 and Server 2008 will have IPv6 enabled by default—understand what impact any OS has on the network
- Deploy it – at least in a lab – IPv6 won’t bite
- Things to consider:
  - Focus on what you must have in the near-term (lower your expectations) but pound your vendors and others to support your long-term goals
  - Don’t be too late to the party – anything done in a panic is likely going to go badly