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::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::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::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
```

Cisco Expo 2011

Rešitve in tehnike migracije omrežij podjetij na protokol IPv6

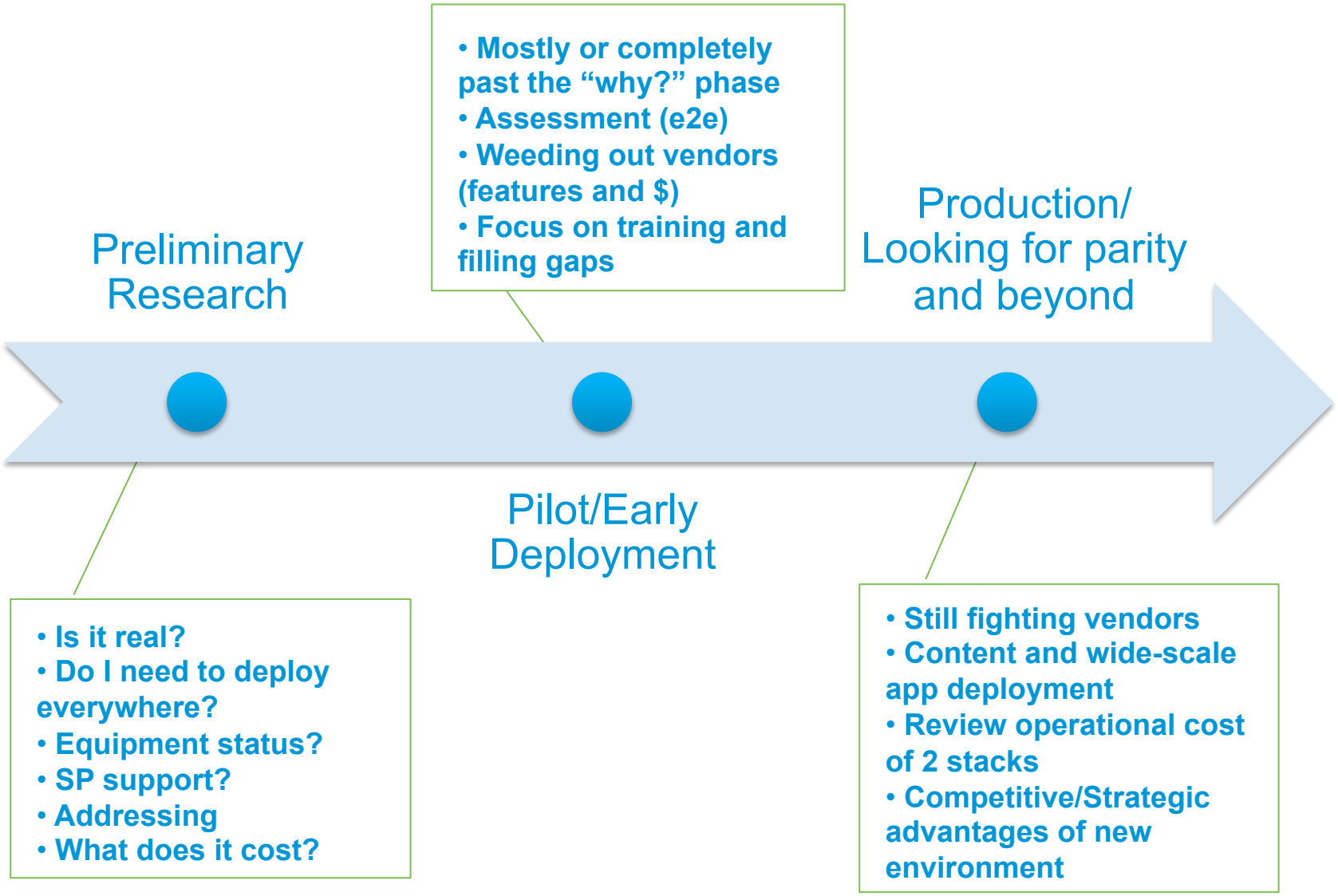
Dimitar (Mitko) Vasilev

Consulting System Engineer

Agenda

- Planning and Deployment Summary
- Address consideration
- FHRP, QoS and scalability
- Campus and Data Center
- WAN and Branch
- Remote access
- Conclusion

Enterprise Adoption Spectrum

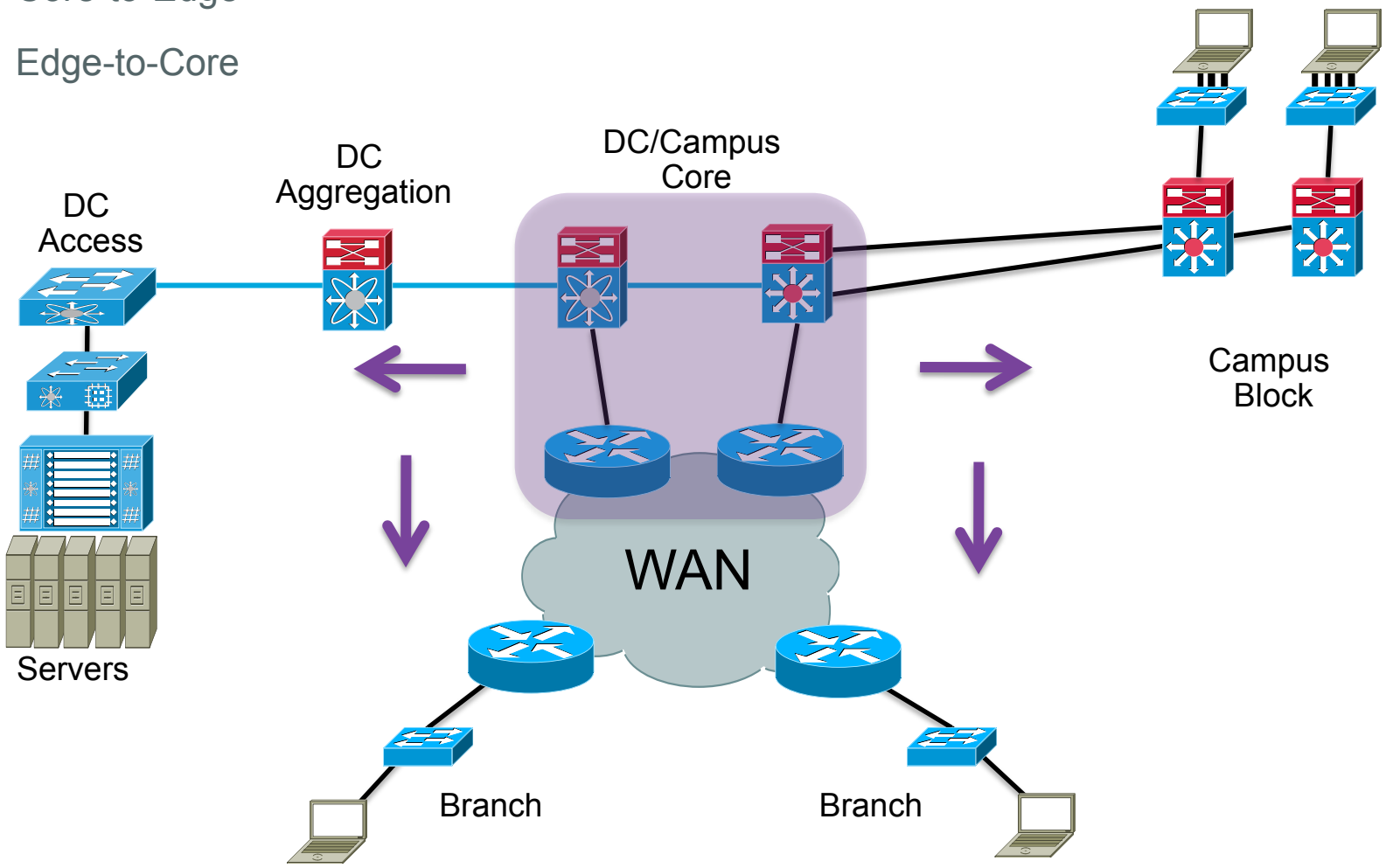


IPv6 Integration Outline

Pre-Deployment Phases	Deployment Phases
• Establish the network starting point • Importance of a network assessment and available tools • Defining early IPv6 security guidelines and requirements • Additional IPv6 “pre-deployment” tasks needing consideration	• Transport considerations for integration • Campus IPv6 integration options • WAN IPv6 integration options • Advanced IPv6 services options

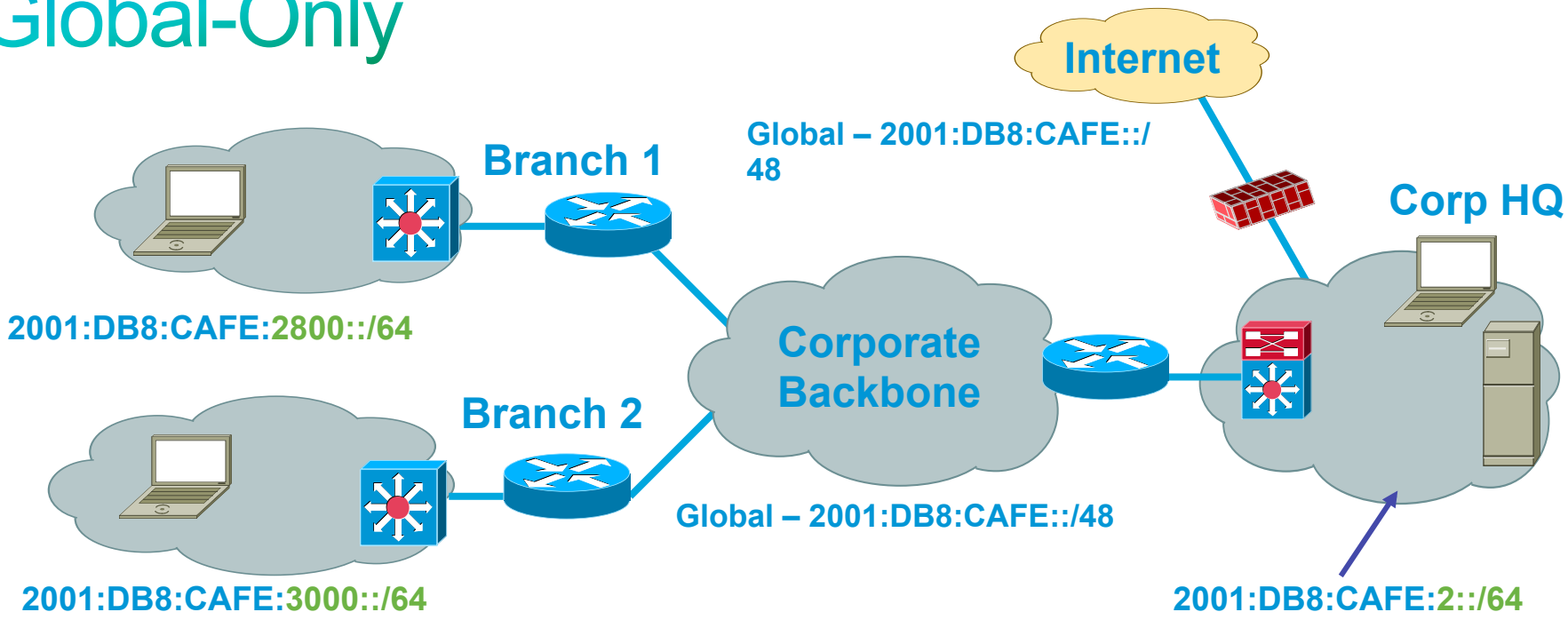
Where do I start?

- Based on Timeframe/Use case
- Core-to-Edge
- Edge-to-Core



Recommended

Global-Only



- Global is used everywhere
- Default is /48 – can be larger: http://www.ripe.net/ripe/docs/ipv6policy.html
- Provider independent – See Number Resource Policy Manual (NRPM) - http://www.ripe.net/rs/ipv6/
- Only downside is breaking the habit of believing that topology hiding is a good security method ☺

Link Level—Prefix Length Considerations

64 bits	> 64 bits
▪ Recommended by RFC5375 and IAB/IESG ▪ Consistency makes management easy ▪ MUST for SLAAC (MSFT DHCPv6 also) ▪ Significant address space loss (18.644 Quintillion)	▪ Address space conservation ▪ Special cases: /126—valid for p2p /127—not valid for p2p (RFC3627) /128—loopback ▪ Complicates management ▪ Must avoid overlap with specific addresses: Router Anycast (RFC3513) Embedded RP (RFC3956) ISATAP addresses

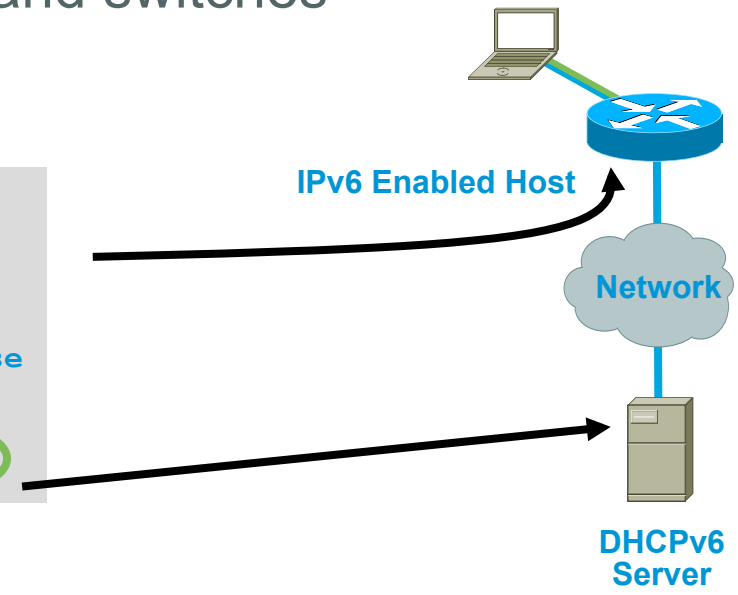
SLAAC & Stateful/Stateless DHCPv6

- StateLess Address AutoConfiguration (SLAAC)
- Stateful and stateless DHCPv6 server

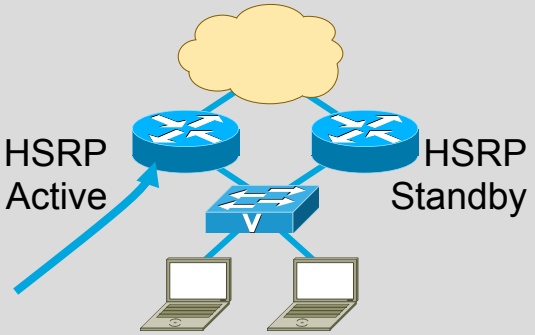
  Cisco Network Registrar:
  http://www.cisco.com/en/US/products/sw/netmgtsw/ps1982/

  Microsoft Windows Server 2008:
  http://technet2.microsoft.com/windowsserver2008/en/library/bab0f1a1-54aa-4cef-9164-139e8bcc44751033.mspx?mfr=true
- 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 dhcp relay destination 2001:DB8:CAFE:10::2
```

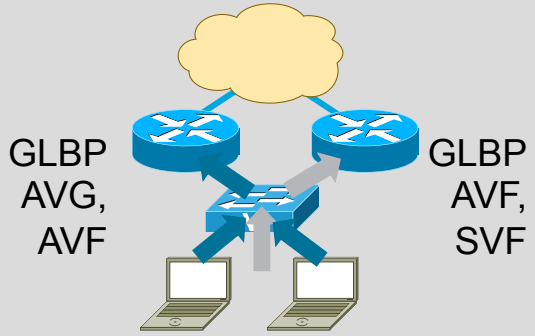


First Hop Router Redundancy



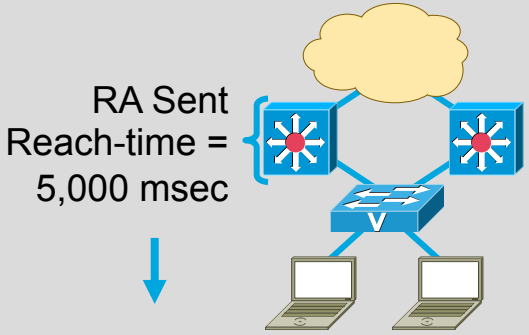
HSRP for v6

- 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



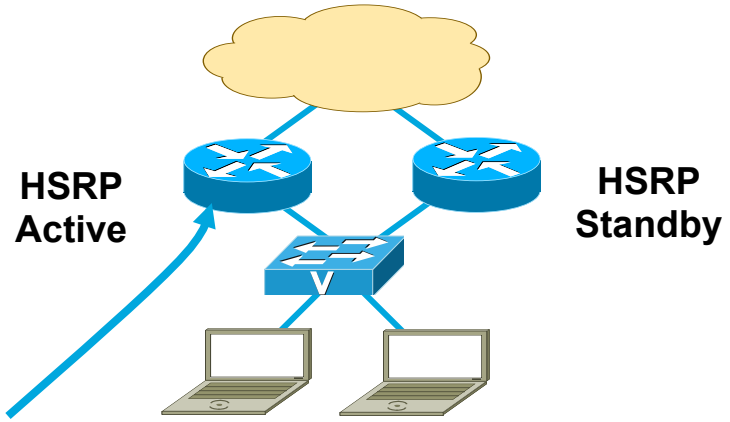
Neighbor **U**nreachability **D**etection

- 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

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
```

Host with GW of Virtual IP

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

IPv6 QoS Policy & Syntax

- Unified QoS Policy (v4/v6 in same policy) or separate?
- IPv4 syntax has used "ip" following match/set statements

  Example: `match ipdscp, set ipdscp`
- 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
```

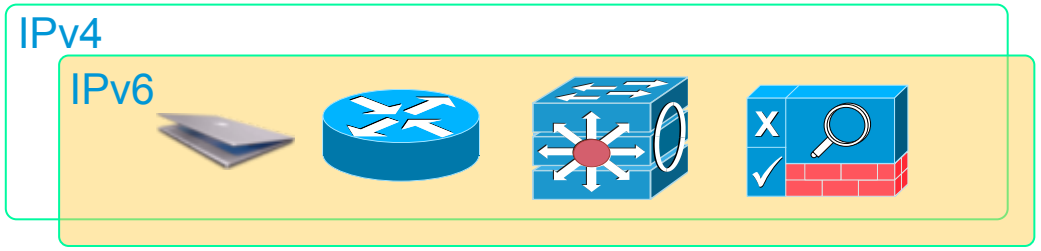
  IPv6 Neighbor Cache entry:

```
2001:DB8:CAFE:2:2891:1C0C:F52A:9DF1       4000d.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)

IPv6 Co-existence Solutions

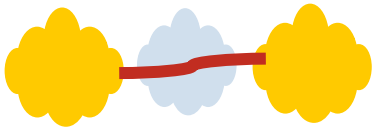
Dual Stack



Recommended Enterprise Co-existence strategy

Tunneling Services

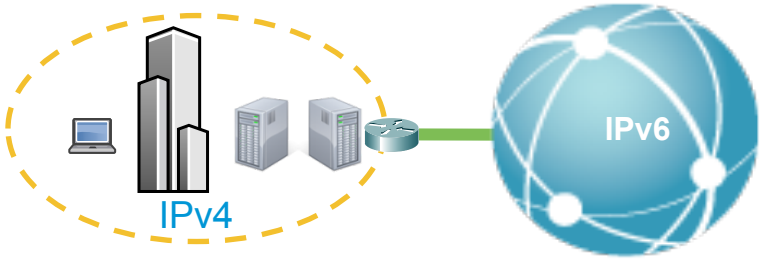
IPv4 over IPv6



IPv6 over IPv4

Connect Islands of IPv6 or IPv4

Translation Services

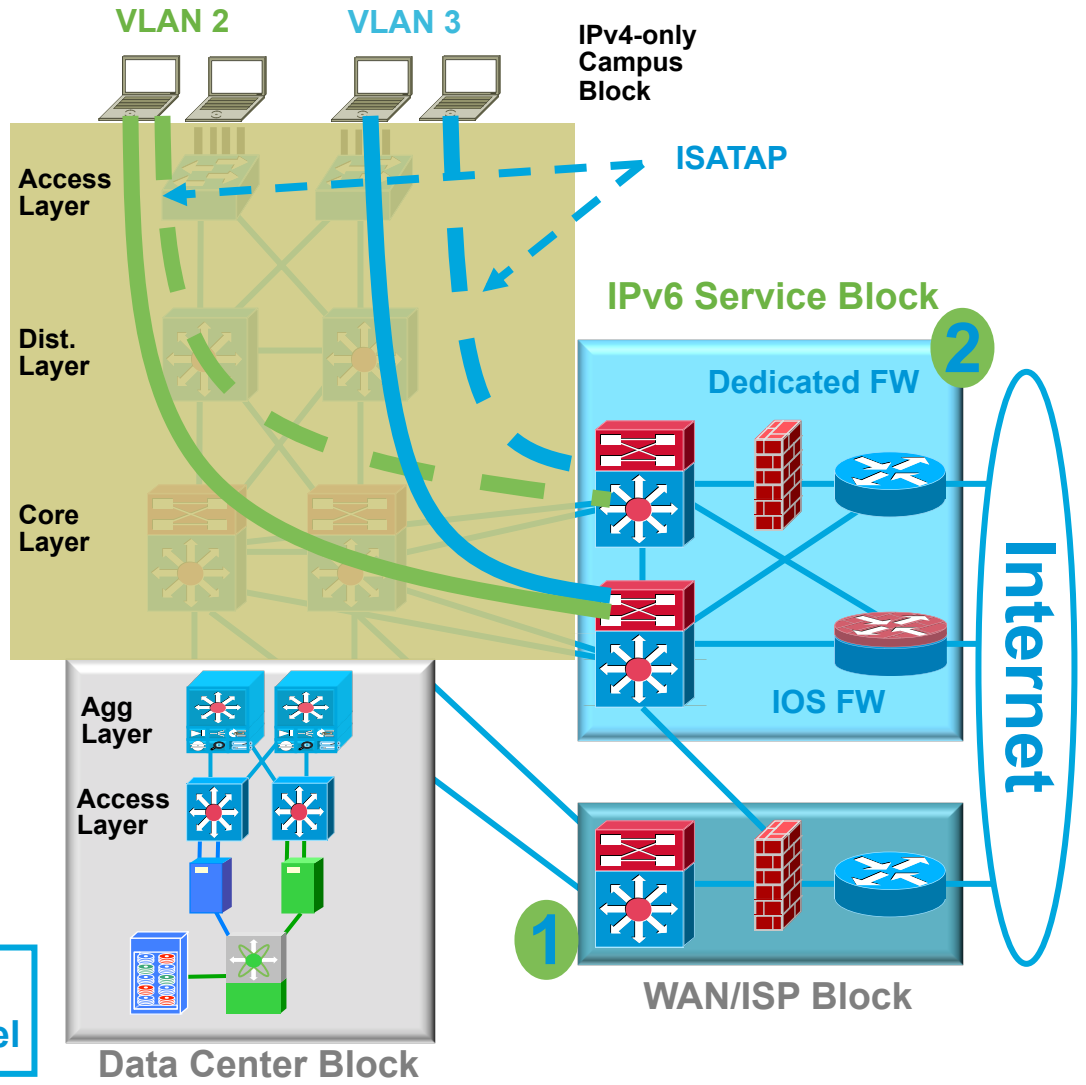


Connect to the IPv6 community

Campus IPv6 Deployment Options

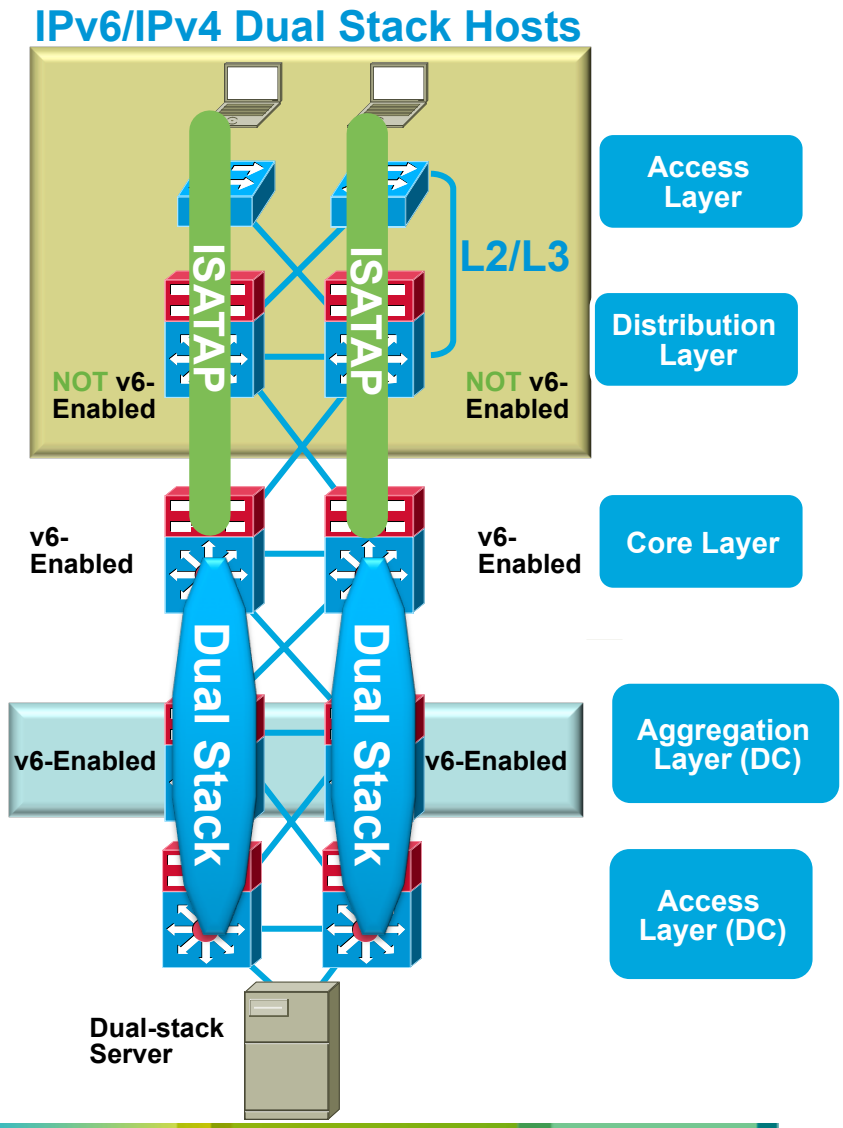
IPv6 Service Block—an Interim Approach

- 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



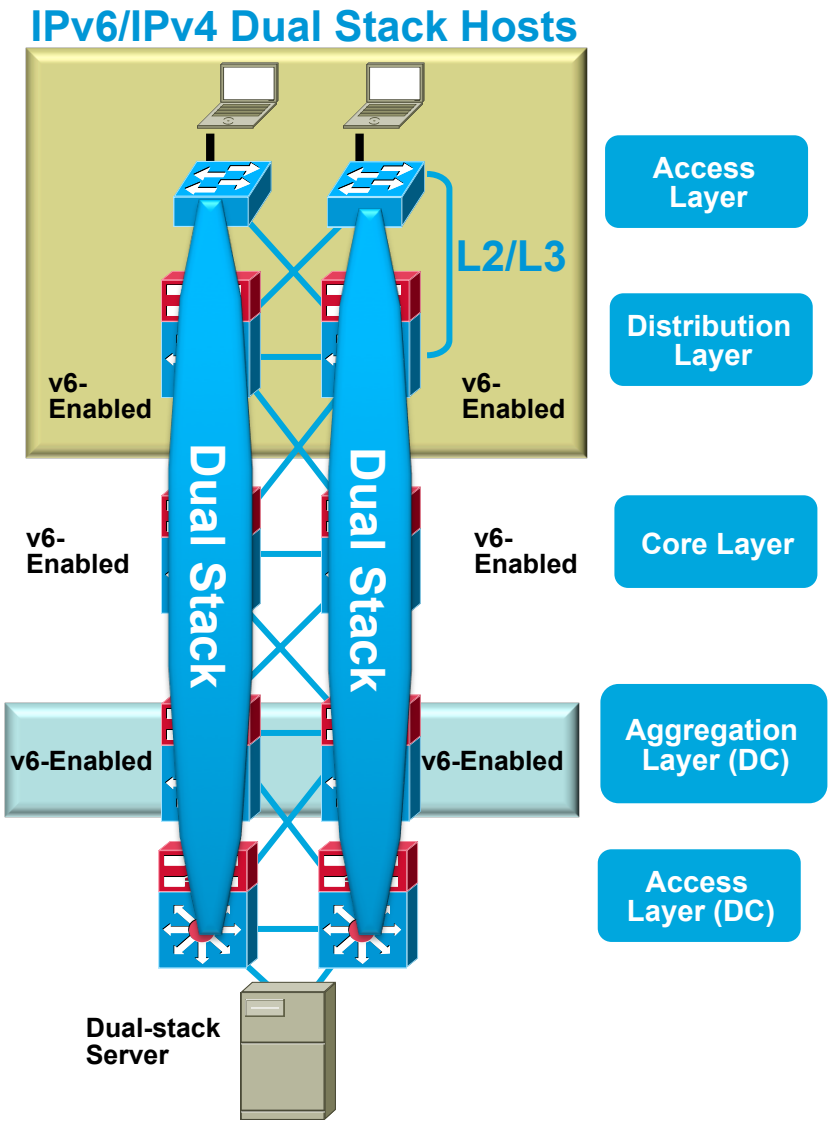
Campus IPv6 Deployment Options
Hybrid Model

- 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 (Intra-Site Automatic Tunneling Addressing Protocol) 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

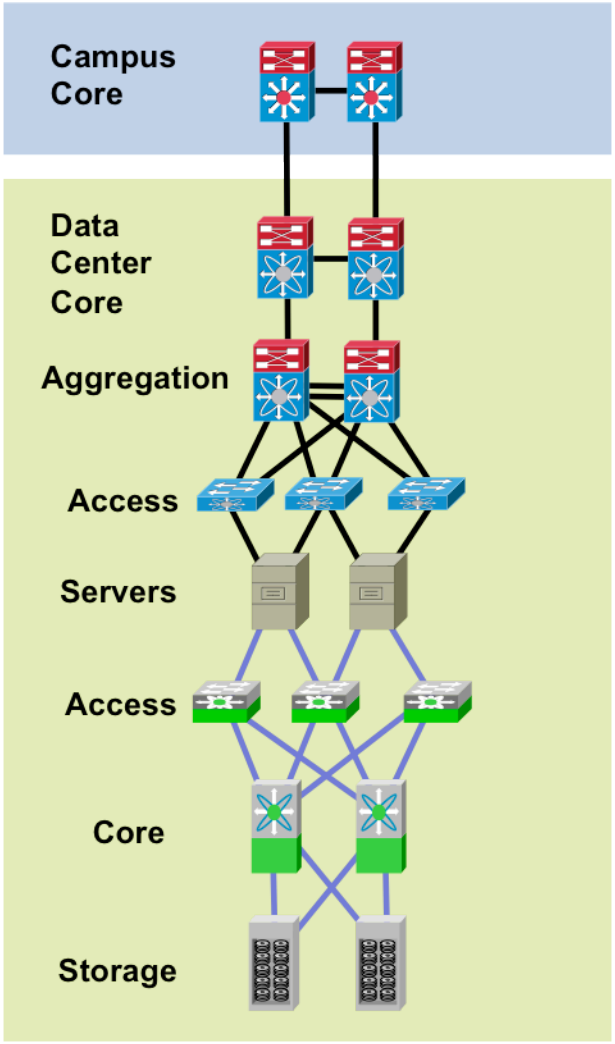


Campus IPv6 Deployment Options
Dual-Stack IPv4/IPv6

- #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
- Modify the SDM template to enable IPv6

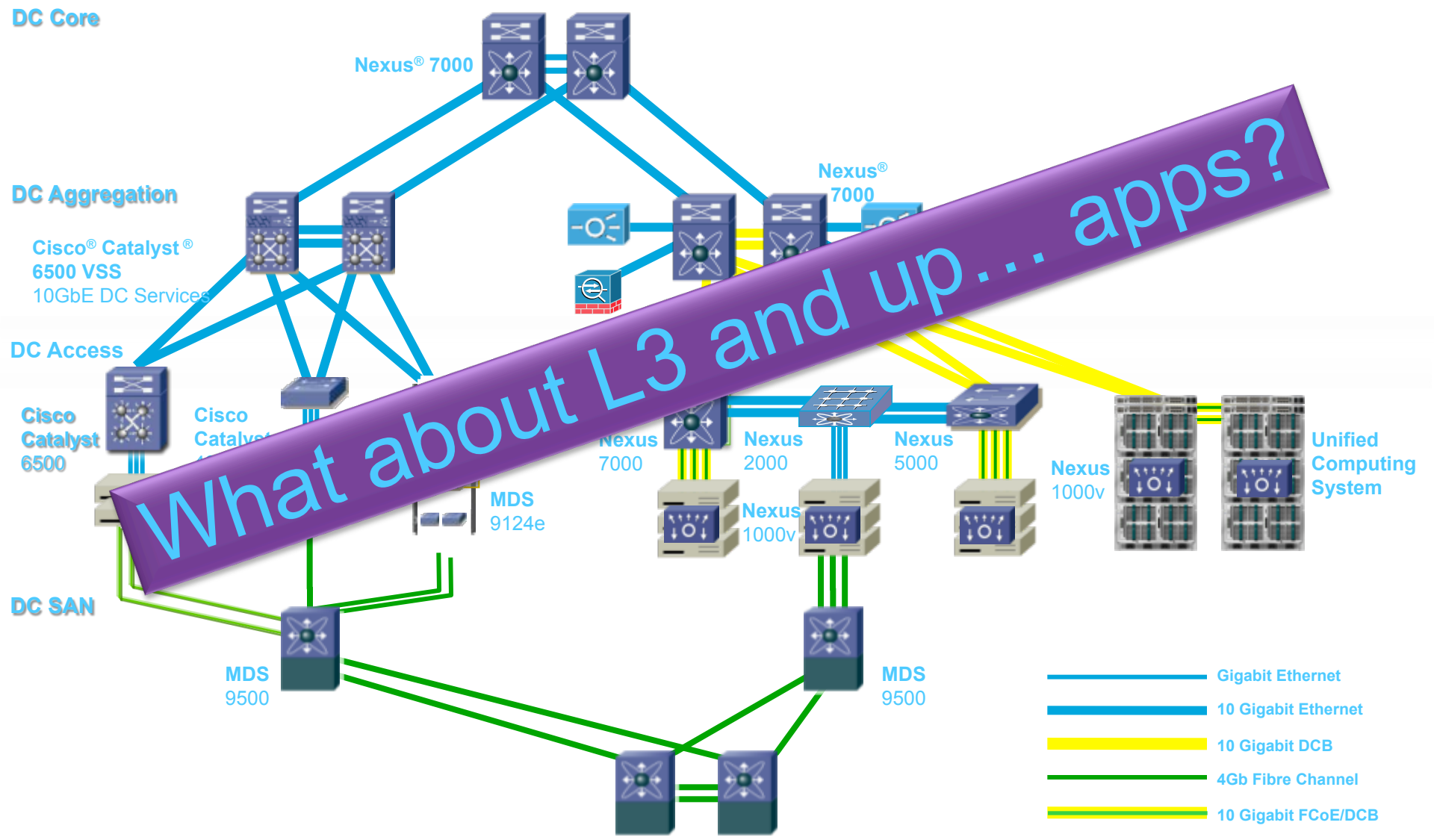


IPv6 Data Center Integration



- Route/Switch 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
- Stuff people don't think about:
  - NIC Teaming, iLO, DRAC, IP KVM, Clusters
  - Innocent looking Server OS upgrades – Windows Server 2008 - Impact on clusters – Microsoft Server 2008 Failover clusters full support IPv6 (and L3)
- Build an IPv6-only server farm?

Virtualized DC Solutions

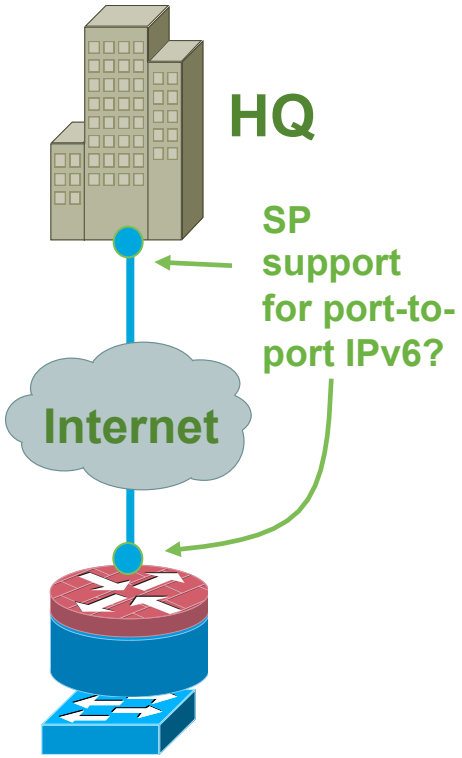


IPv6 in the Enterprise Data Center

Biggest Challenges Today

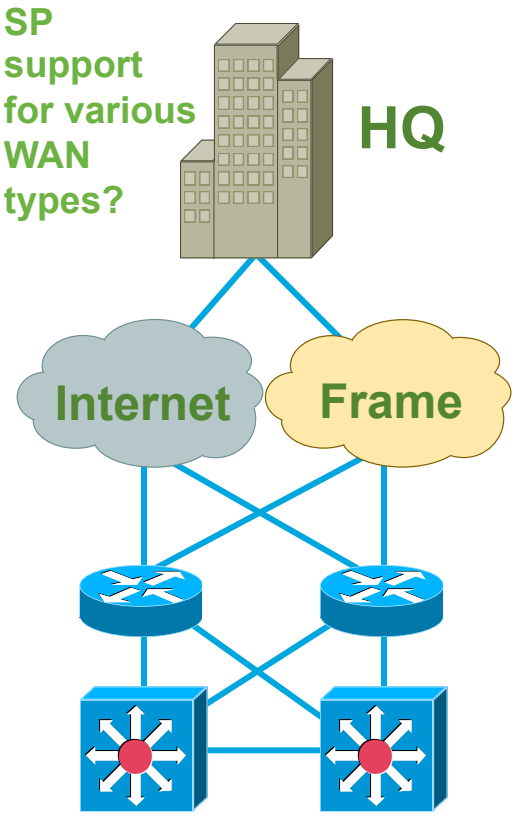
- Network services above L3
  - SLB, SSL-Offload, application monitoring (probes) – ACE and GSS
  - Application Optimization – WAAS and ACE
  - High-speed security inspection/perimeter protection – ASA/IPS/IDS/IronPort
- Application support for IPv6 – Know what you don't know
  - If an application is protocol centric (IPv4):
    - Leave as-is
    - 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

Branch Single Tier



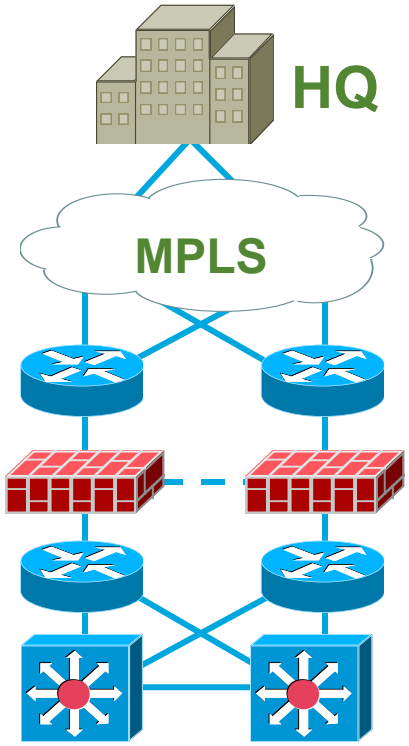
Dual-Stack
IPSec VPN (IPv4/IPv6)
Firewall (IPv4/IPv6)
Integrated Switch (MLD-snooping)

Branch Dual Tier



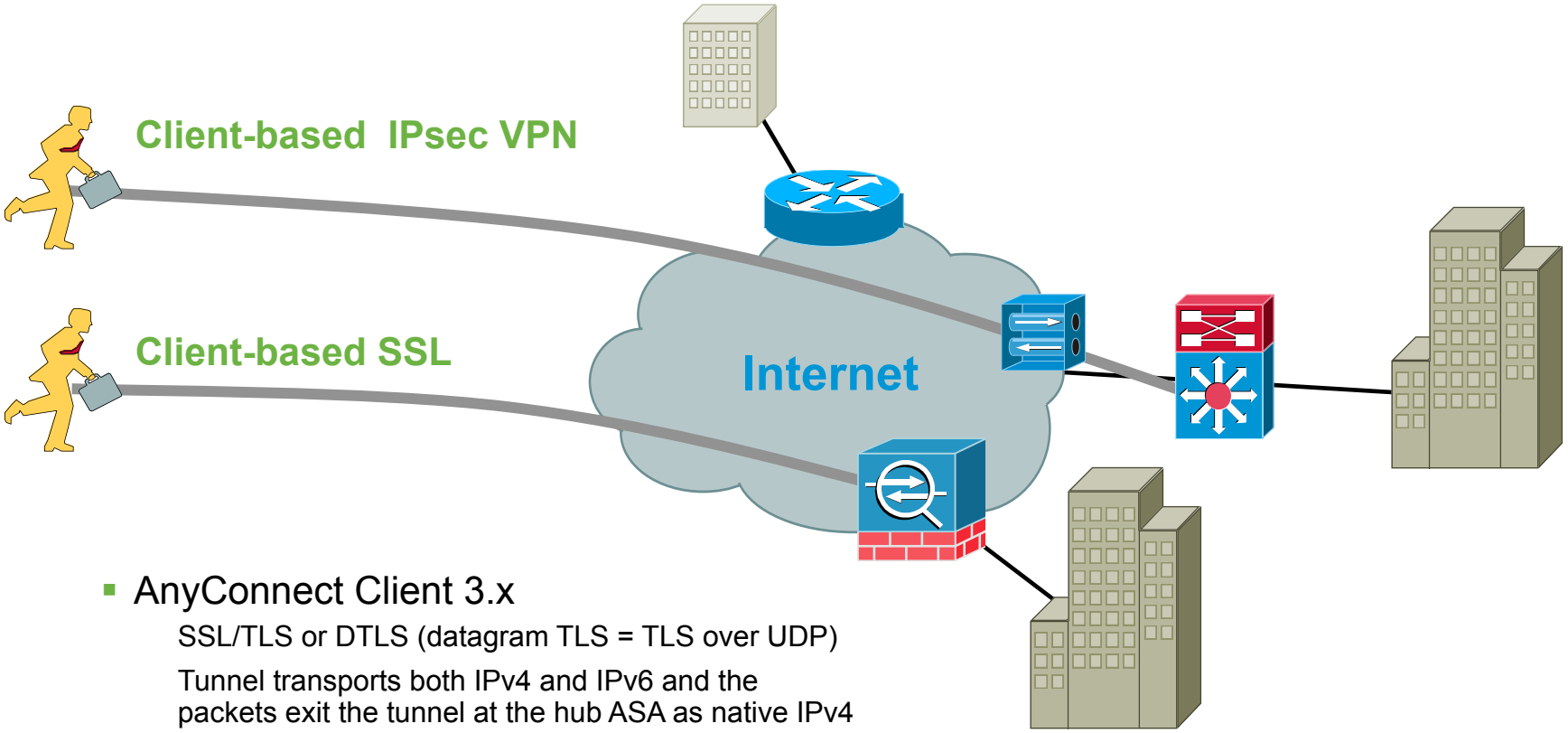
Dual-Stack
IPSec VPN or Frame Relay
Firewall (IPv4/IPv6)
Switches (MLD-snooping)

Branch Multi-Tier



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

Cisco Remote VPN – IPv6



- AnyConnect Client 3.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.

Conclusion

- **Create a virtual team of IT representatives from every area of IT to ensure coverage for OS, Apps, Network and Operations/ Management**

- “Dual stack where you can – Tunnel where you must – Translate only when you have a gun to your head”

- Microsoft Windows Vista, Windows 7 and Server 2008 will have IPv6 enabled by default—understand what impact any OS has on the network

Thank you.

Extra slides with Information

IPv6 – Introduction

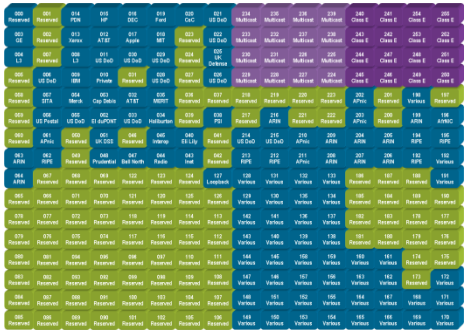
Agenda

- IPv6 – Why?
- IPv6 – Key Aspects
- IPv6 – Address Assignment

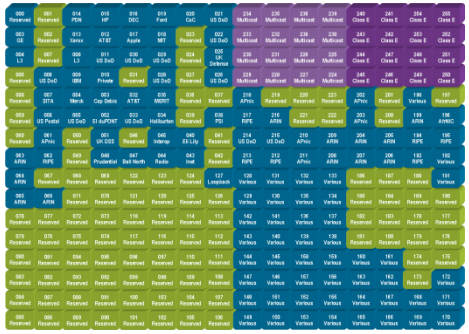
IPv6 – Why?

The Ozone Layer of IPv4 Addresses

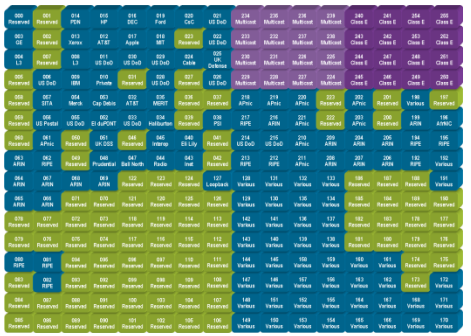
2000



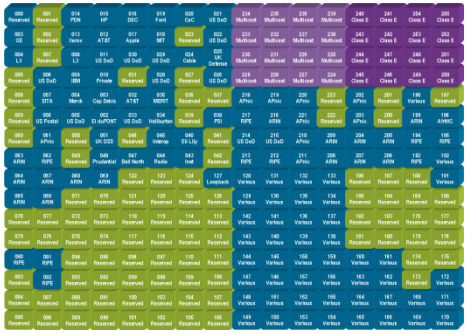
2001



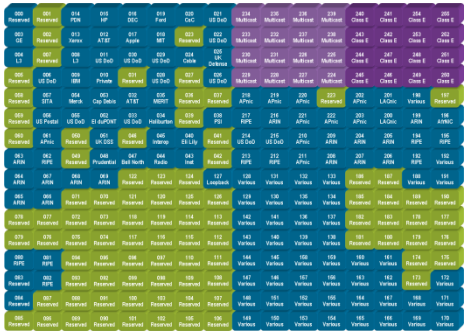
2002



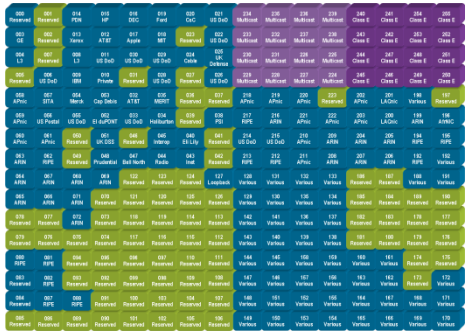
2003



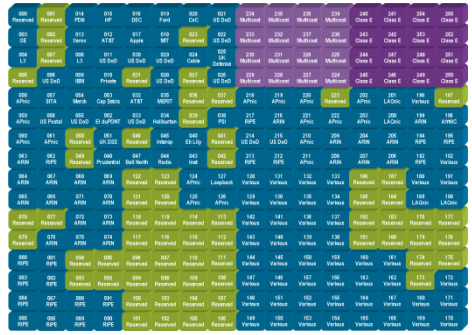
2004



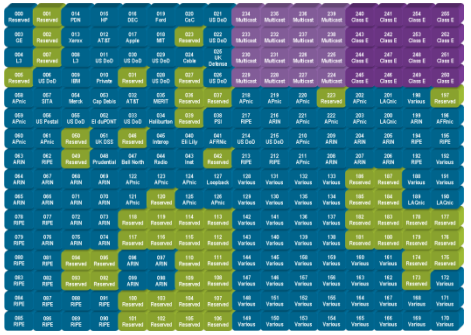
2005



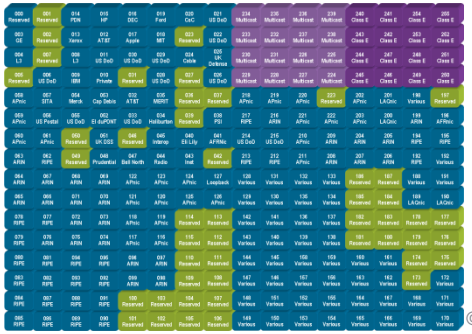
2006



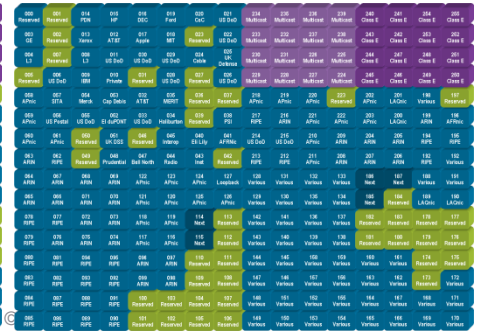
2007



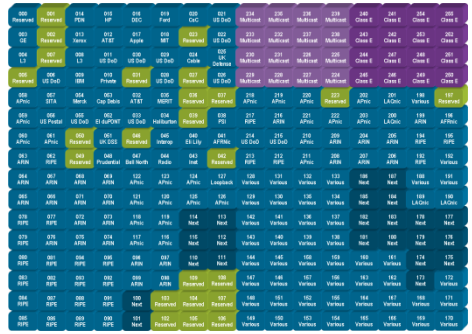
Today



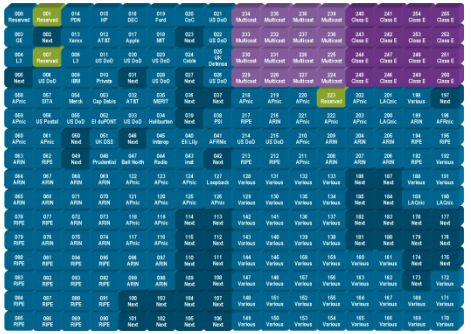
2008



2009



2010



IPv6 Drivers

IPv4 Address space completion

- Public or Private Space
- Limiting network expansion and putting at risk business continuity
- Introducing Operational challenges

National IPv6 Strategies

- Compliance: U.S. Federal Mandate, IPv6 task force
- Next Generation Internet (CNGI) project in China and Japan
- European Commission Recommendation

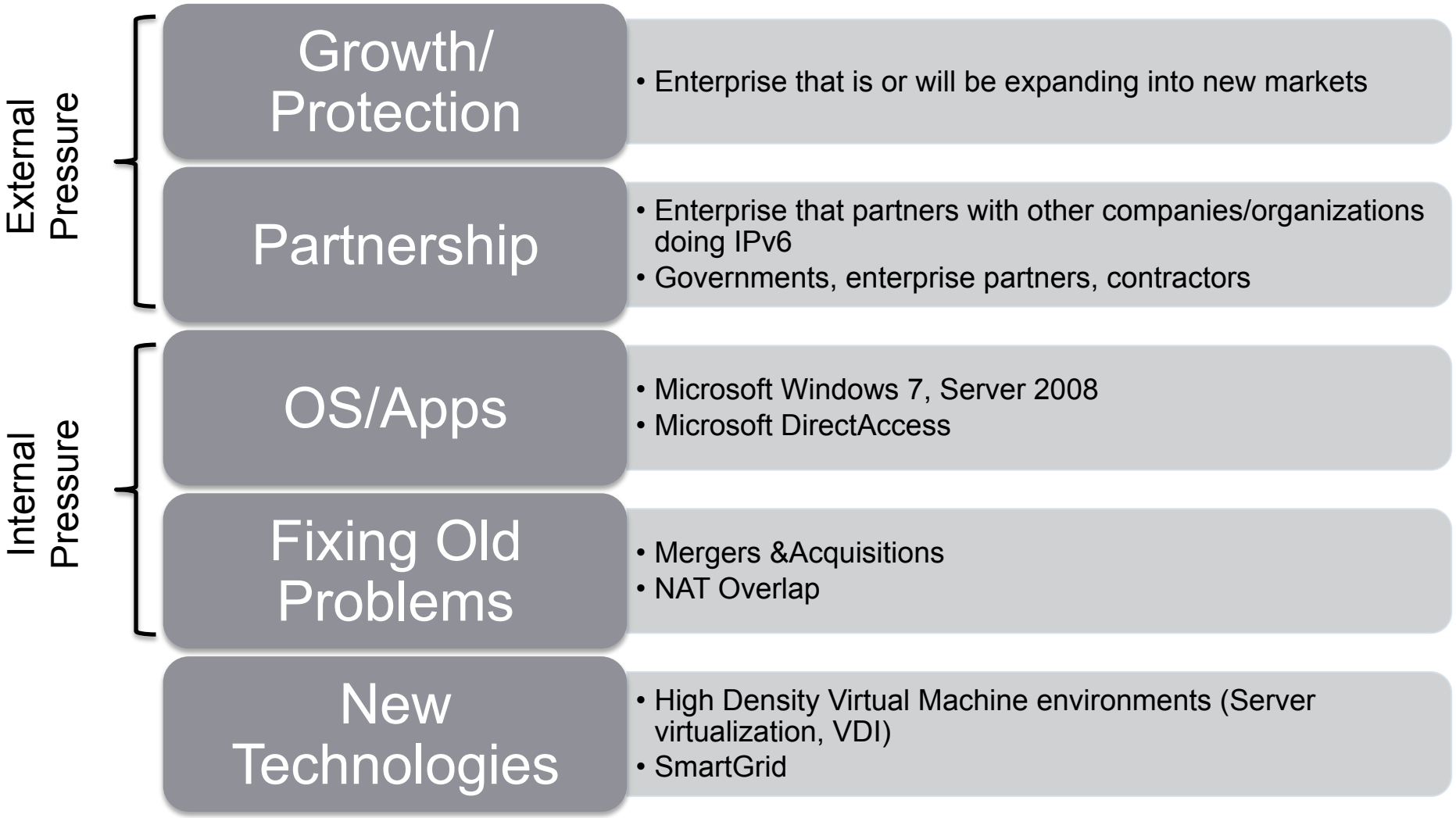
- IPv6 “on” in Microsoft Vista
- Sensor Networks
- Apple's “Back to My Mac”
- v6 over v4 OTT tunnel providers

IPv6 in Client Software

- Next generation Network architecture require IPv6
- DOCSIS 3.0,Quad Play
- Mobile SP
- Networks in Motion
- Networked Sensors, i.e.: AIRS

Infrastructure Evolution

Dramatic Increase in Enterprise Activity
Why?



Impact on the Enterprise Network

Internet Presence

Customer facing interface

The most visible thing

All the services and content offered by the enterprise to the Internet community.

This includes customers and partners of companies, students of schools, citizens of governments, potential donors to charities, etc.

Internet Access

For partners, to facilitate mergers & cooperation

Several approaches: dual-stack, proxies, tunnels

How the enterprise employees and applications access services and content on the Internet.

Intranet

For IPv6-only application, to get visibility on IPv6 traffic, to get a clean and easy-to-manage intranet

Easy to implement on the network, application qualification required

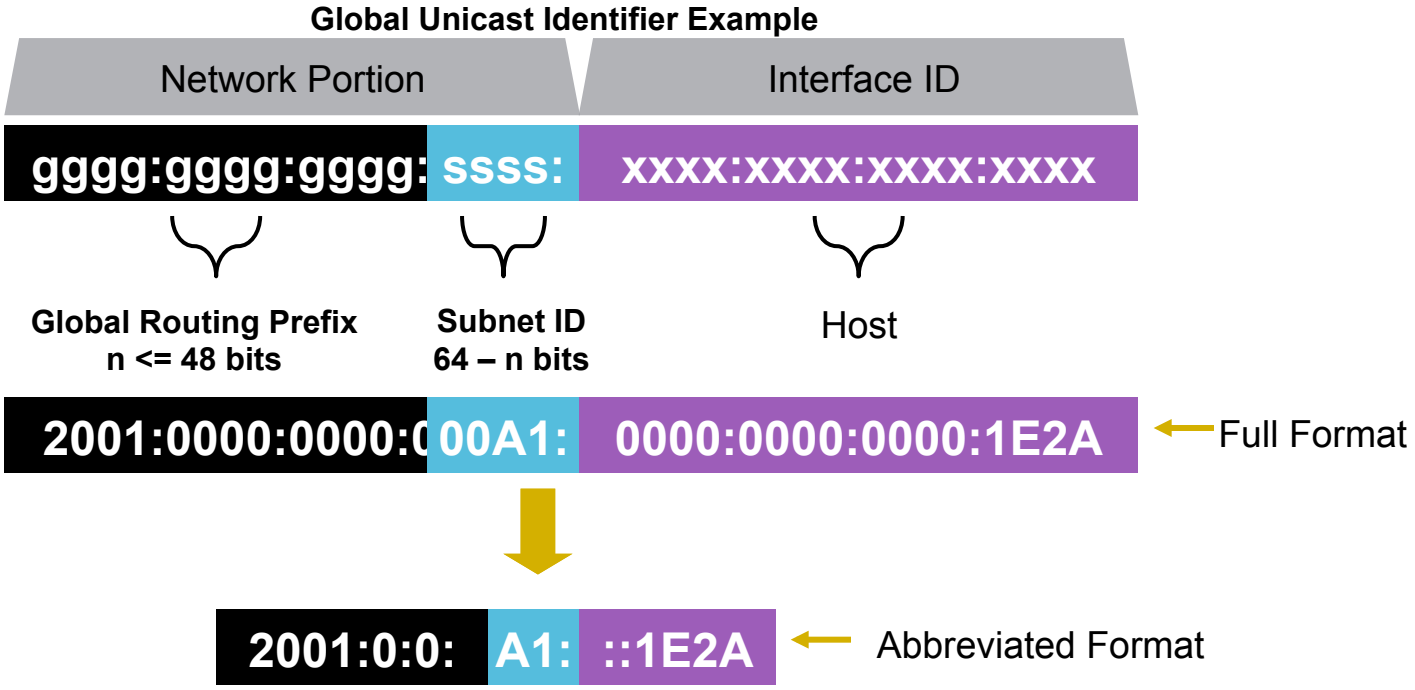
All the services and content located inside the enterprise and accessed only by enterprise users and applications.

The intranet itself can be divided into access (where all workstations are connected) and data center (where most applications and services are located).

IPv6 Technology – Key Aspects

IPv6 Addresses

- IPv6 addresses are 128 bits long
  - Segmented into 8 groups of four HEX characters
  - Separated by a colon (:)
  - 50% for network ID, 50% for interface ID
  - Network portion is allocated by Internet registries 2^64 (1.8×10^{19})
  - Still leaves us with ~ 3 billion network prefixes for each person on earth



IPv6 Address Representation and Simplification

- Base format (16-byte)

2001:0660:3003:0001:0000:0000:6543:210F

- Compact Format:

2001:660:3003:1::6543:210F

- Literal representation (e.g. used when browsing to IPv6 address directly and not through the DNS name)

  [2001:660:3003:2:a00:20ff:fe18:964c]

IPv6—Addressing Model

- Interface “expected” to have multiple addresses
- Addresses have scope
  - Link Local
  - Unique Local
  - Global
- Addresses have lifetime
  - Valid and preferred lifetime
- Types of IPv6 Addresses
  - Unicast
    - Address of a single interface. One-to-one delivery to single interface
  - Multicast
    - Address of a set of interfaces. One-to-many delivery to all interfaces in the set
  - Anycast
    - Address of a set of interfaces. One-to-one-of-many delivery to a single interface in the set that is closest
  - No more broadcast addresses

IPv6 Address Types

- Three types of unicast address scopes

Link-Local – Non routable exists on single layer 2 domain (FE80::/64)

Unique-Local (ULA) – Routable with an administrative domain (FC00::/7)

Global – Routable across the Internet (2000::/3)

- Interface “expected” to have multiple addresses

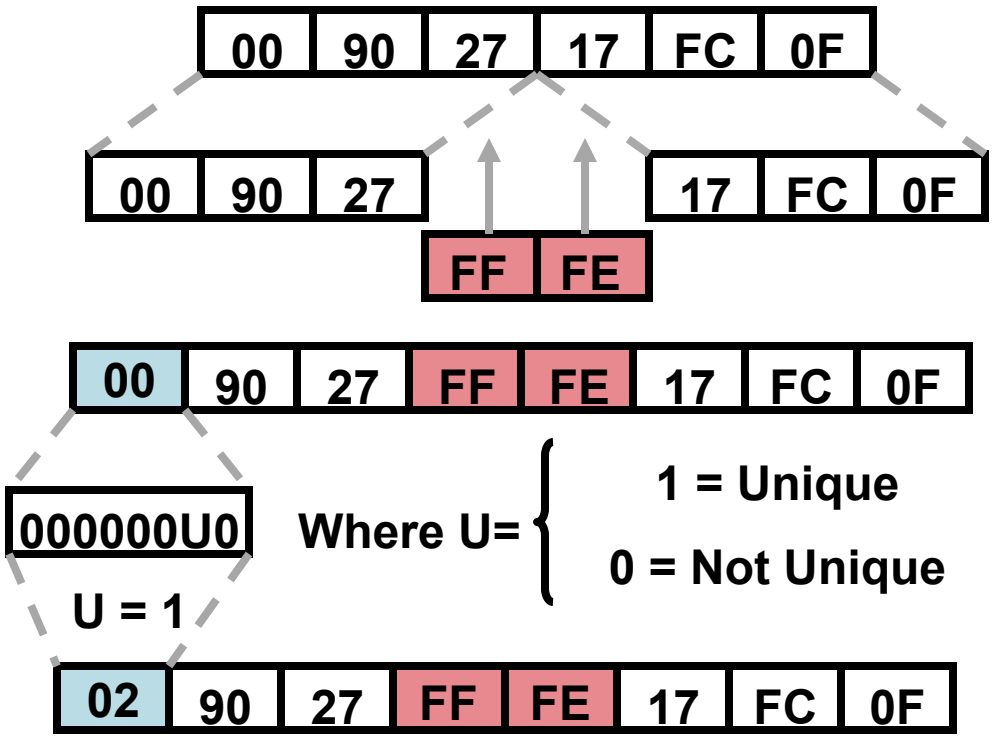
- Multicast addresses begin with FF00::/8

IPv6 Interface Identifier

- Interface-ID can be manually configured
- Cisco supports the EUI-64 format to do stateless auto-configuration

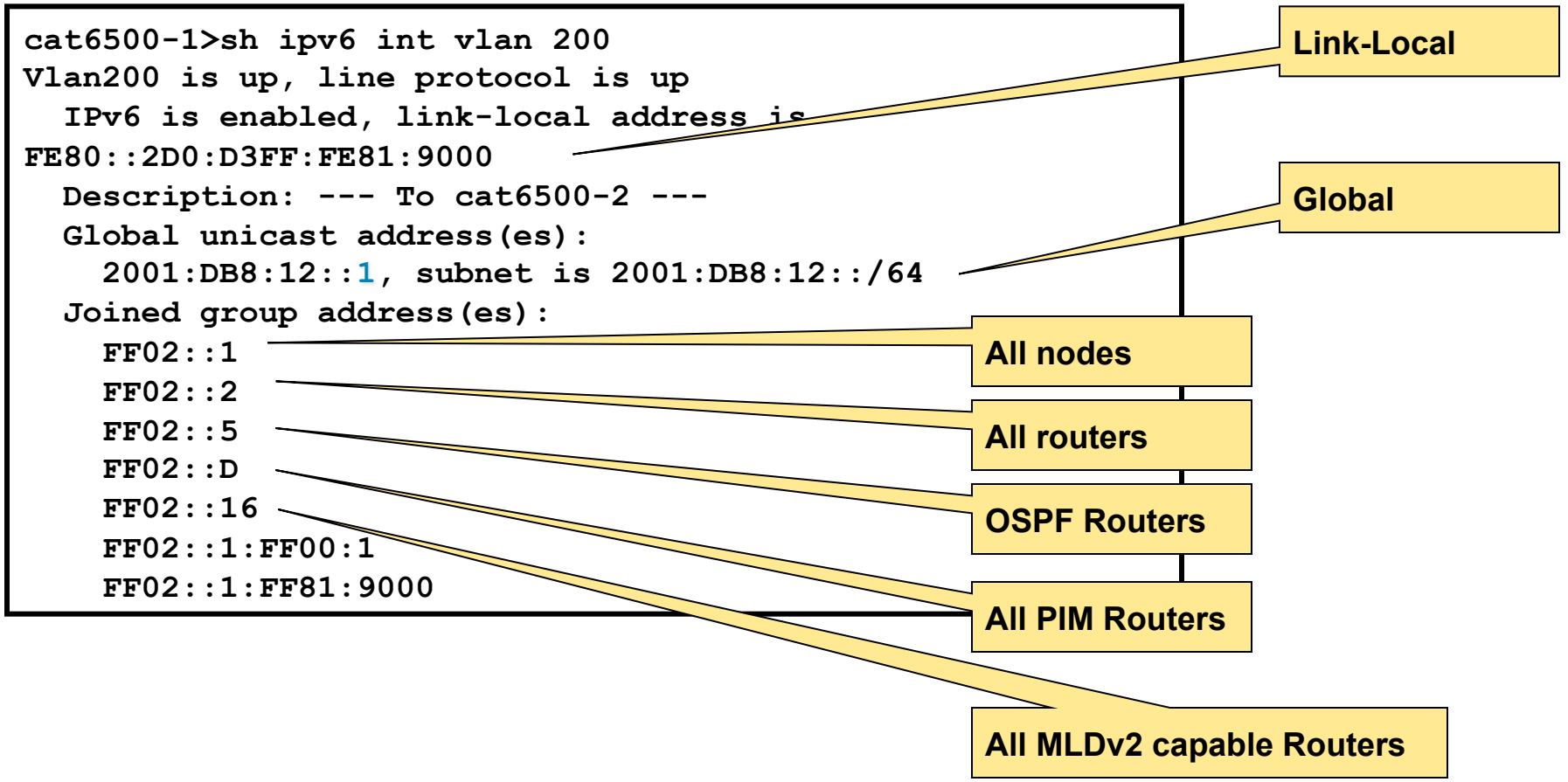
  This format expands the 48 bit MAC address to 64 bits by inserting FFFE into the middle 16 bits

  To make sure that the chosen address is from a unique Ethernet MAC address, the universal/ local (“u” bit) is set to 1 for global scope and 0 for local scope



EUI-64 Format

IPv6 Addresses – Unicast and Multicast
Examples



IPv6 Interface Identifier
Example – EUI-64 Format


```
cat3750-3#sh int gi 1/0/3
GigabitEthernet1/0/3 is down, line protocol is down (notconnect)
  Hardware is Gigabit Ethernet, address is 000c.30ae.84c7 (bia 000c.30ae.84c7)

cat3750-3#
```

```
cat3750-3#sh run int gi 1/0/3
!
interface GigabitEthernet1/0/3
 no switchport
 ip address 10.149.24.1 255.255.255.0
 ipv6 address 2001:DB8:24::/64 eui-64
!
```

```
cat3750-3#sh ipv6 interface gi 1/0/3
GigabitEthernet1/0/3 is down, line protocol is down
  IPv6 is enabled, link-local address is FE80::20C:30FF:FEAE:84C7 [TEN]
  Global unicast address(es):
    2001:DB8:24:0:20C:30FF:FEAE:84C7, subnet is 2001:DB8:24::/64 [EUI/TEN]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FFAE:84C7
cat3750-3#
```

IPv6 Interface Identifier
Example – Manual


```
cat3750-3#sh int gi 1/0/3
GigabitEthernet1/0/3 is down, line protocol is down (notconnect)
  Hardware is Gigabit Ethernet, address is 000c.30ae.84c7 (bia 000c.30ae.84c7)

cat3750-3#
```

```
cat3750-3#sh run int gi 1/0/3
!
interface GigabitEthernet1/0/3
 no switchport
 ip address 10.149.24.1 255.255.255.0
 ipv6 address 2006:149:24::/64 eui-64
 ipv6 address 2006:149:25::1/64
!
```

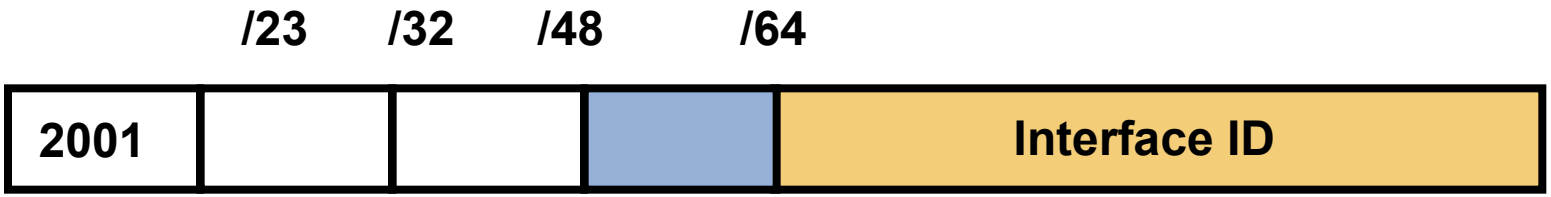
```
cat3750-3#sh ipv6 interface gi 1/0/3
GigabitEthernet1/0/3 is down, line protocol is down
  IPv6 is enabled, link-local address is FE80::20C:30FF:FEAE:84C7 [TEN]
  Global unicast address(es):
    2006:149:24:0:20C:30FF:FEAE:84C7, subnet is 2006:149:24::/64 [EUI/TEN]
    2006:149:25::1, subnet is 2006:149:25::/64 [TEN]
  Joined group address(es):
    FF02::1
    FF02::2
cat3750-3#
```

Windows 7 – Interface Identifier
netsh

- Windows 7 doesn't use the EUI-64 technique by default when forming its interface identifier, but uses their randomly-generated interface identifiers

```
C:\>netsh int ipv6 sh addr

Interface 1: Loopback Pseudo-Interface 1

Addr Type  DAD State   Valid Life Pref. Life Address
---------  ----------- ---------- ---------- ------------------------
Other      Preferred     infinite   infinite ::1

Interface 12: isatap.{7218C71C-E509-4EF9-AB57-C08863056588}

Addr Type  DAD State   Valid Life Pref. Life Address
---------  ----------- ---------- ---------- ------------------------
Other      Deprecated    infinite   infinite fe80::5efe:10.109.109.6%12

Interface 13: Local Area Connection* 9

Addr Type  DAD State   Valid Life Pref. Life Address
---------  ----------- ---------- ---------- ------------------------
Public     Preferred     infinite   infinite 2001:0:5ef5:73bc:a2:3ac1:f592:92f9
Other      Preferred     infinite   infinite fe80::a2:3ac1:f592:92f9%13

Interface 11: Local Area Connection

Addr Type  DAD State   Valid Life Pref. Life Address
---------  ----------- ---------- ---------- ------------------------
Temporary  Preferred  6d23h49m31s 6d23h49m31s 2001:db8:9:cafe:a133:5fb8:31df:864a
Public     Preferred  29d23h59m49s 6d23h59m49s 2001:db8:9:cafe:b407:e685:fb14:c12d
Other      Preferred     infinite   infinite fe80::b407:e685:fb14:c12d%11

C:\>
```

IPv6 Privacy Extensions (RFC 3041)

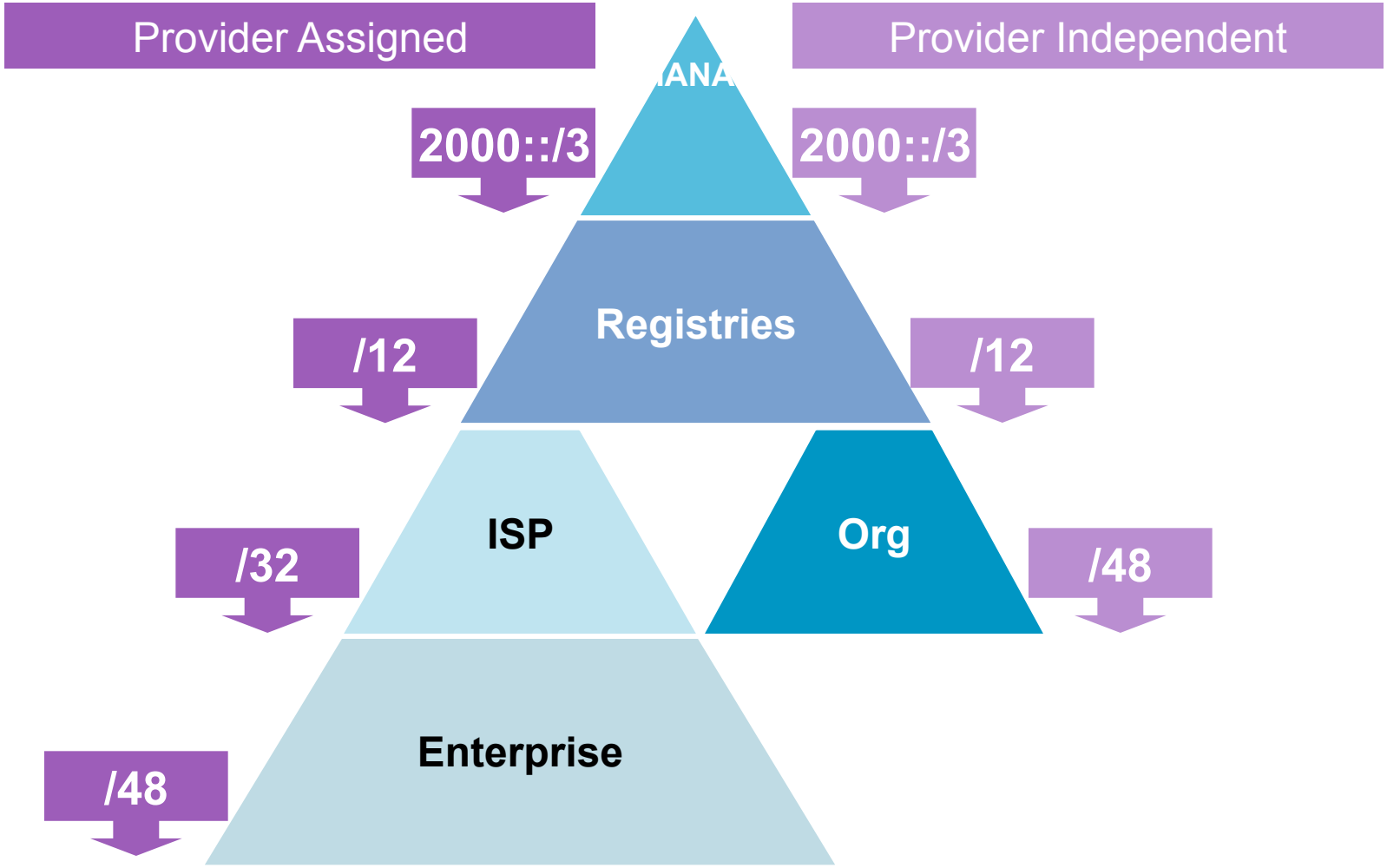


- IEEE 24 bits OUI can be used to identify hardware
  - http://standards.ieee.org/regauth/oui/oui.txt
- Temporary addresses for IPv6 host client application, e.g. web browser
  - Inhibit device/user tracking
  - Random 64 bit interface ID, then run Duplicate Address Detection before using it
  - Rate of change based on local policy

Recommendation: Use Privacy Extensions for External Communication but not for Internal Networks (Troubleshooting and Attack Trace Back)

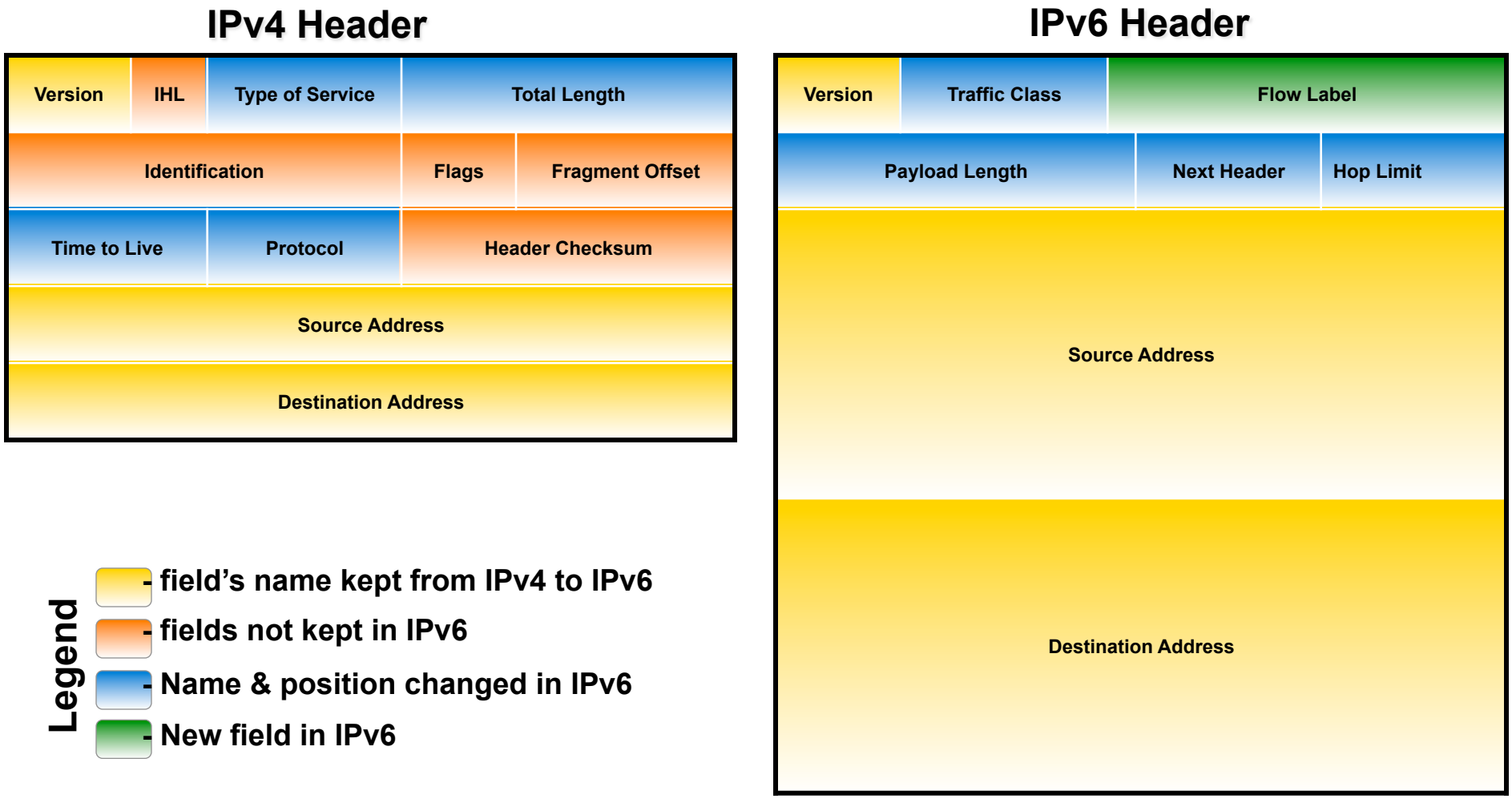
RFC4941

PI and PA Allocation Process

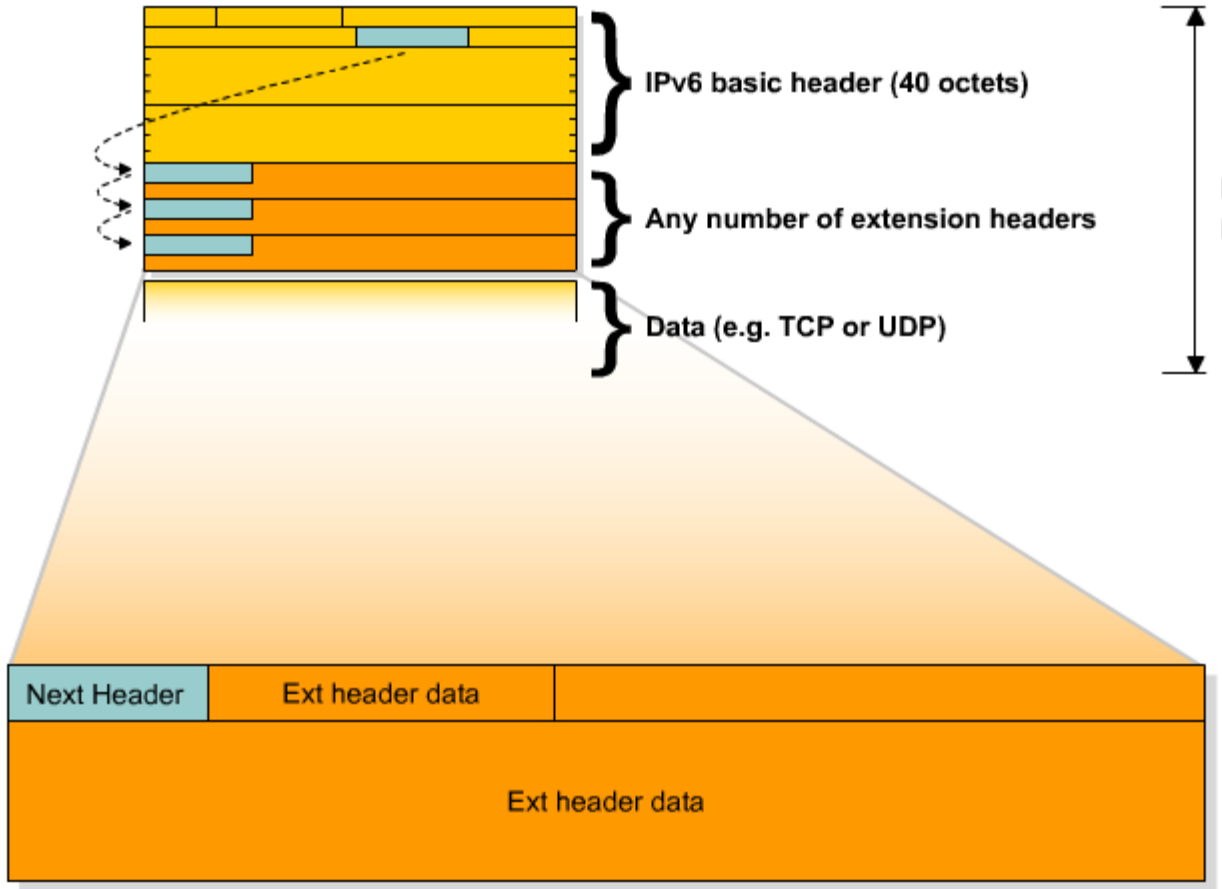


http://www.ripe.net/ripe/policies/proposals/2006-01.html
http://www.ripe.net/ripe/policies/proposals/2006-05.html

IPv4 & IPv6 Header Comparison

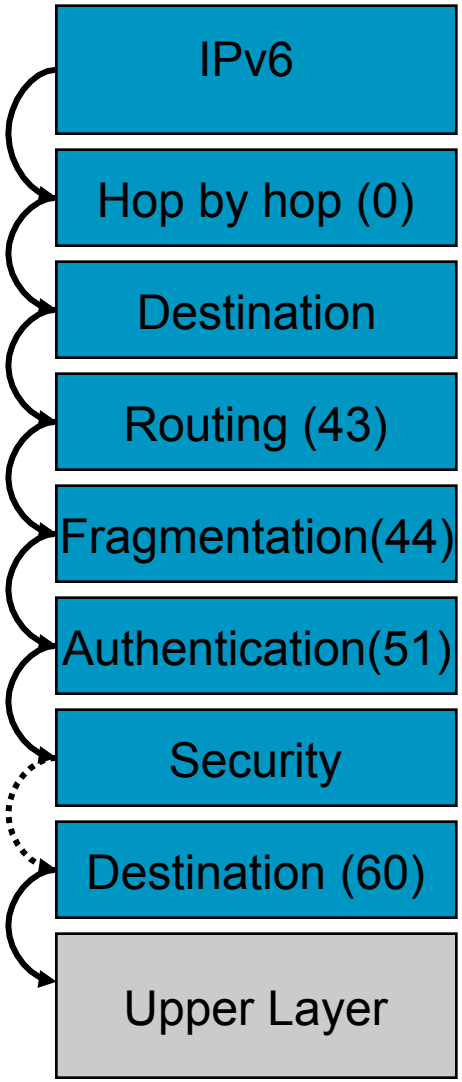


Extension Headers (RFC2460)



- Processed only by node identified in IPv6 Destination Address field => much lower overhead than IPv4 options
  - exception: Hop-by-Hop Options header
- Eliminated IPv4's 40-octet limit on options
  - In IPv6, limit is total packet size, or Path MTU in some

IPv6 extension headers
Order is important



RFC 2460

- Hop by hop (0): Processed by every router
- Destination: Processed by routers listed in Routing extension
- Routing (43): List of routers to cross
- Fragmentation(44): Processed by the destination
- Authentication(51): After reassembling the packet
- Security: Cipher the content of the remaining information
- Destination (60): Processed **only** by the destination

ICMPv4 vs. ICMPv6

Covers ICMP (v4) features: Error control, Administration, …

Transports ND messages: NS, NA, RS, RA
Transports MLD messages: Queries, Reports, …

ICMP Message Type	ICMPv4	ICMPv6
Connectivity Checks	X	X
Informational/Error Messaging	X	X
Fragmentation Needed Notification	X	X
Address Assignment		X
Address Resolution		X
Router Discovery		X
Multicast Group Management		X
Mobile IPv6 Support		X

- Significant changes
- More relied upon
- => ICMP policy on firewalls needs to change

Fundamentals on Neighbor Discovery

- Defined in RFC 4861, “Neighbor Discovery for IP Version 6 (IPv6)” and RFC 4862 (“IPv6 Stateless Address Autoconfiguration”)
- Used for:
  - Router discovery
  - Autoconfiguration of addresses (SLAAC)
  - IPv6 address resolution (replaces ARP)
  - Neighbor Reachability (NUD)
  - Duplicate Address Detection (DAD)
  - Redirection
- Operates above ICMPv6
  - Rely heavily on multicast (including L2-multicast)
- Works with icmp messages and messages “options”

Router Solicitation and Advertisement

1—ICMP Type = 133 (RS)

Src = link-local address (FE80::1/10)

Dst = all-routers multicast address (FF02::2)

Query = please send RA

2—ICMP Type = 134 (RA)

Src = link-local address (FE80::2/10)

Dst = all-nodes multicast address (FF02::1)

Data = options, subnet prefix, lifetime, autoconfig flag

- Router solicitations (RS) are sent by booting nodes to request RAs for configuring the interfaces
- Routers send periodic Router Advertisements (RA) to the all-nodes multicast address

Neighbor Solicitation and Advertisement

Neighbor Solicitation
ICMP type = 135

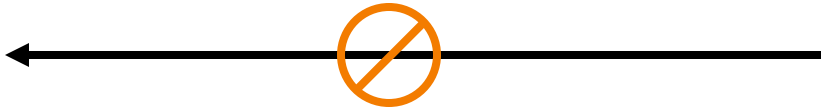
Src = A
Dst = Solicited-node multicast of B
Data = link-layer address of A
Query = what is your link address?

Neighbor Advertisement
ICMP type = 136
Src = B
Dst = A
Data = link-layer address of B

A and B can now exchange packets on this link

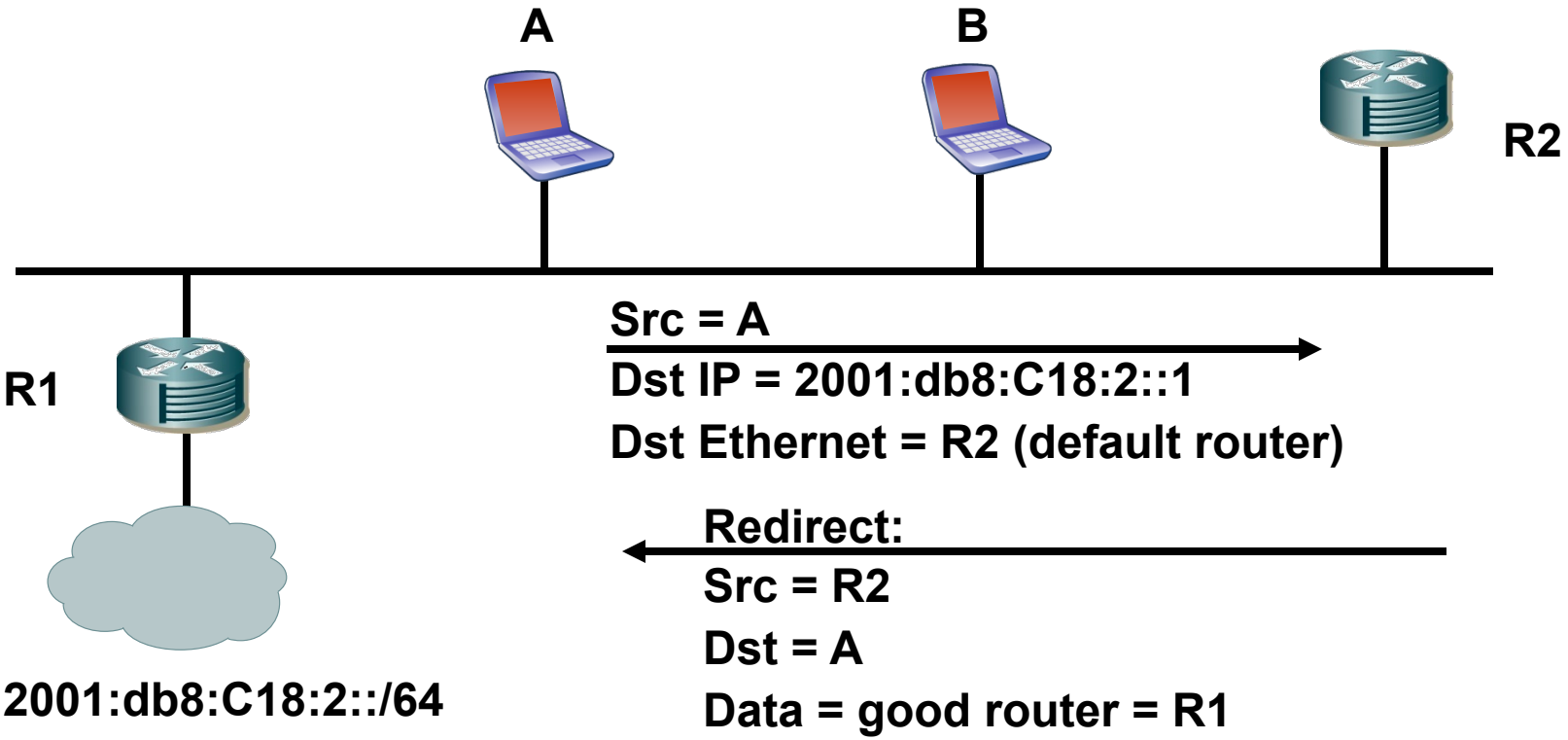
Duplicate Address Detection


```
ICMP type = 135
Src = 0  (::)
Dst = Solicited-node multicast of A
Data = link-layer address of A
Query = what is your link address?
```



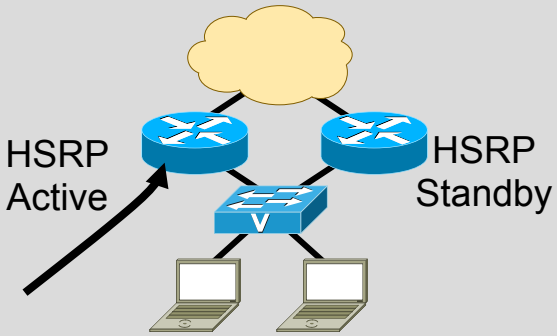
- Duplicate Address Detection (DAD) uses neighbor solicitation to verify the existence of an address to be configured

Redirect



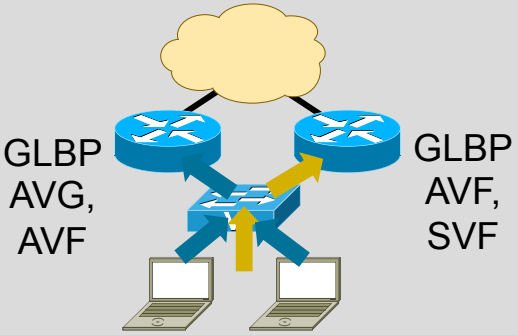
- Redirect is used by a router to signal the reroute of a packet to a better router

First Hop Router Redundancy



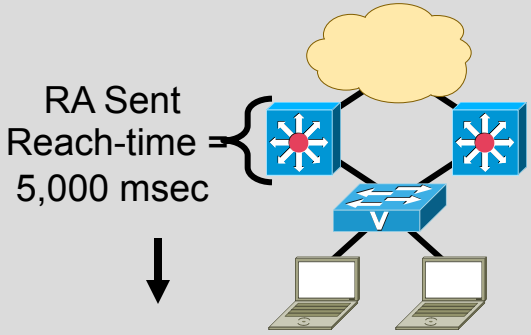
HSRP for v6

- 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 (NUD)

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

Routing: The IPv4 – IPv6 Parallel

RIP	RIPv2 for IPv4 RIPng for IPv6 Distinct but similar protocols with RIPng taking advantage of IPv6 specificities
OSPF	OSPFv2 for IPv4 OSPFv3 for IPv6 Distinct but similar protocols with OSPFv3 being a cleaner implementation that takes advantage of IPv6 specificities
IS-IS	Extended to support IPv6 Natural fit to some of the IPv6 foundational concepts Supports Single and Multi Topology operation
EIGRP	Extended to support IPv6 (IPv6_REQUEST_TYPE, IPv6_METRIC_TYPE, IPv6_EXTERIOR_TYPE) Some changes reflecting IPv6 characteristics
BGP	New MP_REACH_NLRI, MP_UNREACH_NLRI, AFI=2 with SAFI for Unicast/ Multicast/Label/VPN Peering over IPv6 or IPv4 (route maps)

- For all intents and purposes, IPv6 IGPs are similar to their IPv4 counterparts
- IPv6 IGPs have additional features that could lead to new designs

IPv4 and IPv6 Multicast Comparison

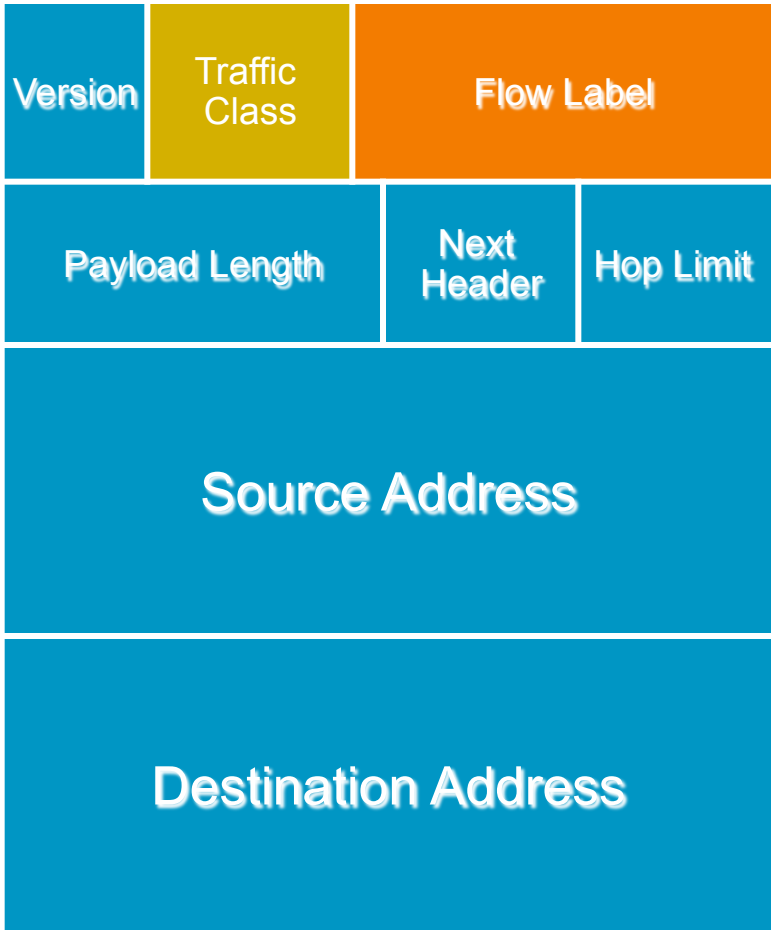
For Your Reference

Service	IPv4 Solution	IPv6 Solution
Addressing Range	32-bit, Class D	128-bit (112-bit Group)
Routing	Protocol Independent, All IGPs and MBGP	Protocol Independent, All IGPs and MBGP with v6 mcast SAFI
Forwarding	PIM-DM, PIM-SM, PIM-SSM, PIM-bidir, PIM-BSR	PIM-SM, PIM-SSM, PIM-bidir, PIM-BSR
Group Management	IGMPv1, v2, v3	MLDv1, v2
Domain Control	Boundary, Border	Scope Identifier
Interdomain Solutions	MSDP across Independent PIM Domains	Single RP within Globally Shared Domains

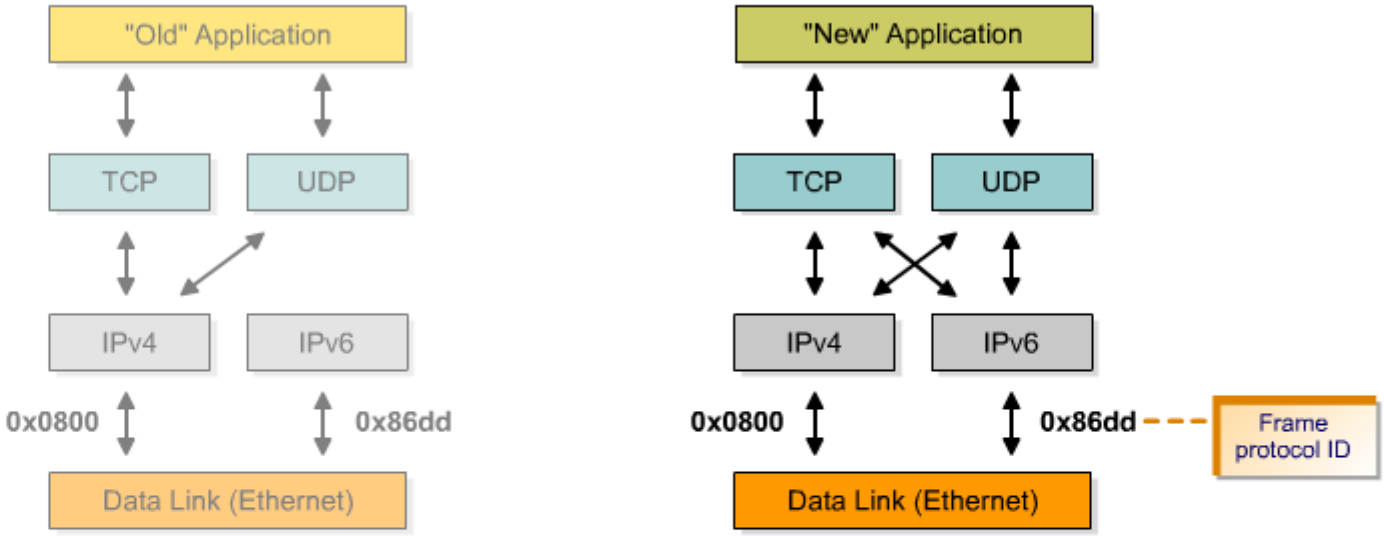
- Static RP, BSR, No Auto-RP
- Embedded RP

Quality of Service

- IPv6 QoS
  - Same architectural models as IPv4
  - *Differentiated Services (Traffic Class field)*
  - *Integrated Services (RSVP)*
- IPv6 traffic class
  - Value defined per applications, same DSCP for applications over both IPv4 and IPv6 – decision to differentiate per protocol is an operational one
- RSVP for IPv6
  - Major RSVP RFC's do support IPv6
  - Use Hop-by-Hop option header for Router Alert
- IPv6 flow label (RFC 3697)
  - A new 20-bit field in the IPv6 basic header
  - Its value cannot be changed by intermediate devices
  - No RFC regarding flow label usage yet
- Transition
  - Mapping between IPv6 DSCP & IPv4 ToS or MPLS EXP



Dual Stack

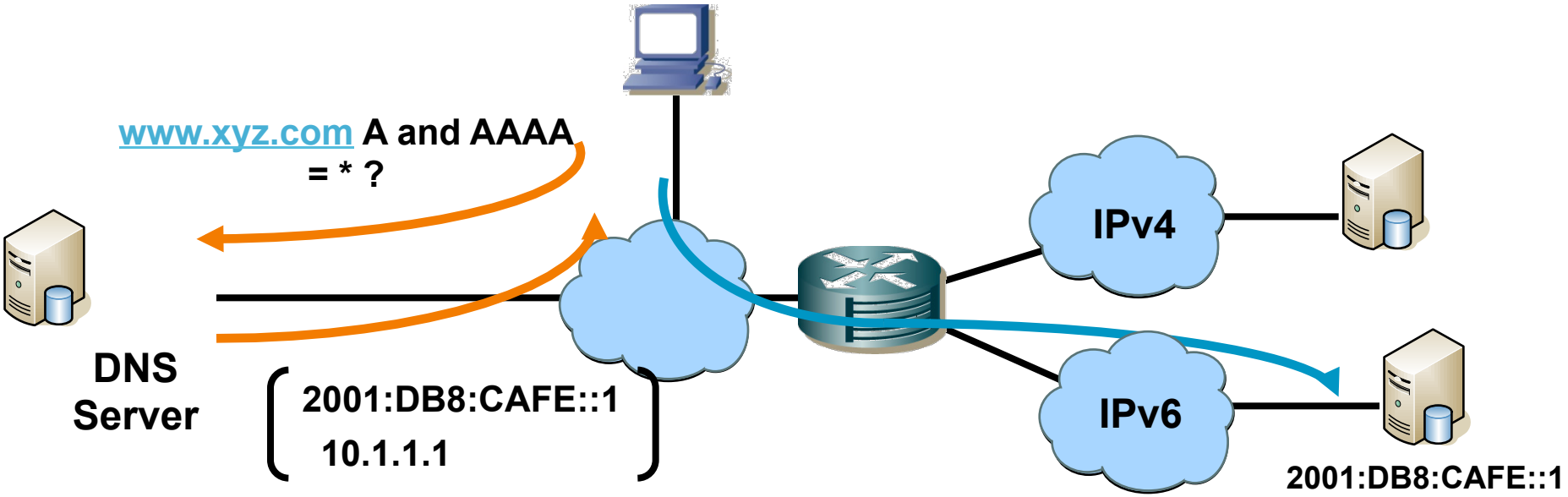


- Both IPv4 and IPv6 stacks are enabled.
- Applications can talk to both.
- Choice of the IP version is based on name lookup and application preference.

IPv6 and DNS

	IPv4	IPv6
Hostname to IP address	A record: www.abc.test. A 192.168.30.1	AAAA record: www.abc.test AAAA 2001:db8:C18:1::2
IP address to hostname	PTR record: 1.30.168.192.in-addr.arpa. PTR www.abc.test.	PTR record: 2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.8.1.c.0.8.b.d.0.1.0.0.2.ip6.arpa PTR www.abc.test.

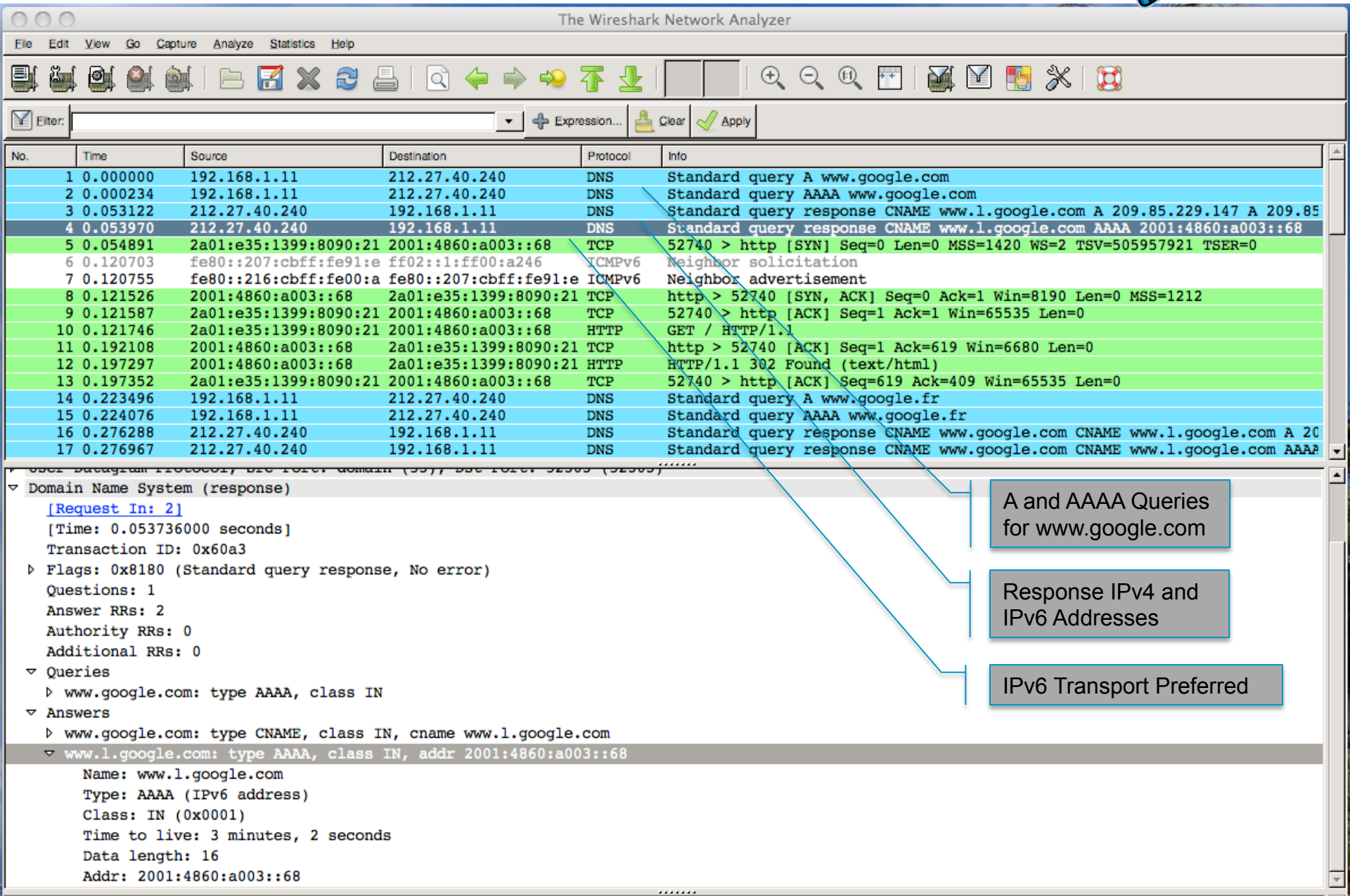
Host Running Dual Stack



- In a dual stack case, an application that:
  - Is IPv4- and IPv6-enabled
  - Asks the DNS for all types of addresses
  - Chooses one address and, for example, connects to the IPv6 address

DNS Example – AAAA Queries

For Your Reference



DNS Issues

- Upgrade DNS servers to support IPv6
- Adding AAAA record for a specific server to the DNS Server requires ALL services to be IPv6 aware
  - LDAP or AD IPv6 Aware
  - All Services running on the Server
- Interim solution is to use a temporary name (see Google IPv6 start in 2008)
  - ipv6.google.com vs. www.google.com

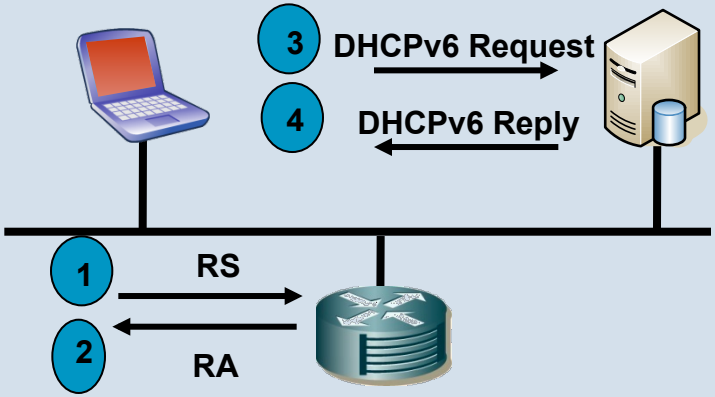
IPv6 – Address Assignment

IPv6 Address Assignment

Similar to IPv4

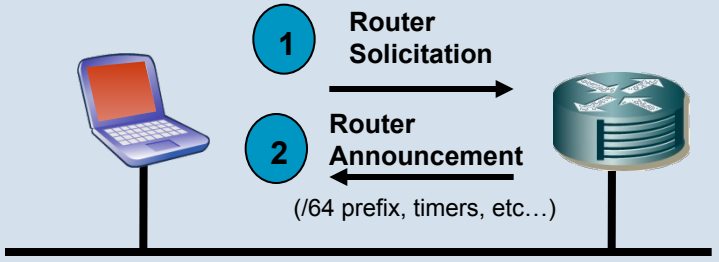
Manually configured

Assigned via DHCP



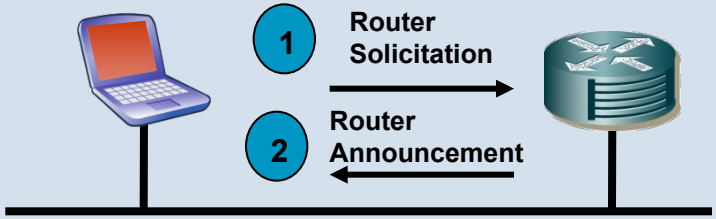
New in IPv6

Stateless configuration



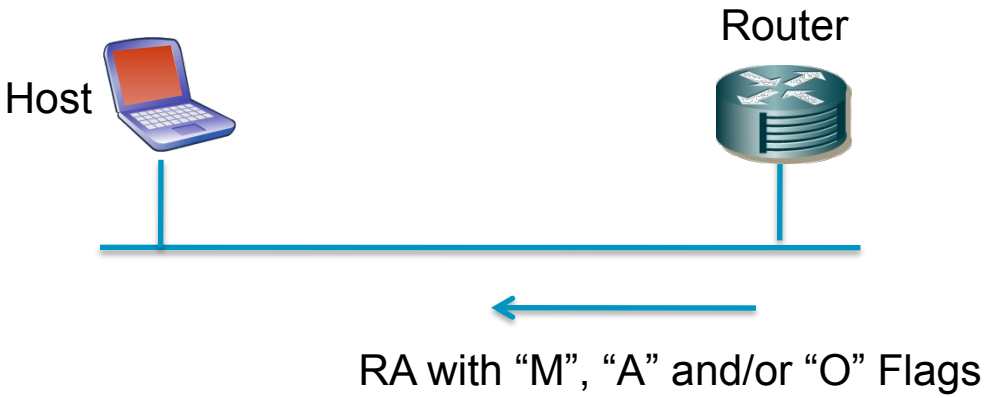
IPv6 Address = /64 prefix + EUI64 (e.g. MAC address)

Auto-generated pseudo-random number (rfc3041)



IPv6 Address = /64 prefix + Random 64 bits (rfc3041)

IPv6 Auto-Configuration
Managing Address Configuration via Router Advertisement



- 1 – Stateless Auto Address Configuration (SLAAC) (RFC2462)
  - Host autonomously configures its own Link-Local address
  - Router solicitation are sent by booting nodes to request RAs for configuring the interfaces.
- 2 – Stateful DHCPv6
  - Host uses DHCP to get its IPv6 address (Similar to IPv4 behavior)
- 3 – Stateless DHCP
  - host uses SLAAC and also DHCP to get additional parameters such as TFTP Server, WINS, etc
- Choice relies on RA Flags sent by the router on the LAN

Using Stateful DHCP
Using the appropriate Flags in RA messages

- Both SLAAC and DHCP runs independently. It's perfectly valid to have both at the same time. This is the default behaviour when setting the M-Flag
- M-Flag – Managed Flag

  if the RA has the M bit set, the host should do DHCP to acquire an IPv6 address

  To enable stateful DHCP

```
!
interface ethernet0/0
  ipv6 nd managed-config-flag
!
```

- A-Flag – Autoconfiguration Flag

  if the RA has the A bit set, the host should do address autoconfiguration (SLAAC)

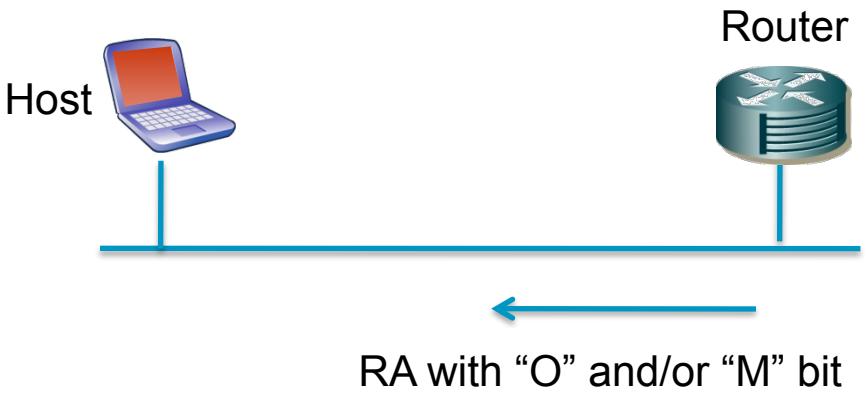
  To disable autoconfig and clear the A-flag

```
!
interface ethernet0/0
  ipv6 nd prefix 2001:DB8:1:CAFE::/64 300 300 no-autoconfig
!
```

- O-Flag – To enable stateless DHCP in addition to SLAAC, use the O-Flag

```
!
interface ethernet0/0
  ipv6 nd other-config-flag
!
```

RA: “M”, “A” and ”O” bits in RA Messages



- If neither the M bit, nor O bit are set

  The host will use SLAAC to acquire an IP address and will not use DHCP for other information.

- If the O bit is set in the router’s RAs

  The host will use SLAAC to acquire its IP address and use the DHCP server to acquire Other information e.g. the TFTP server address, DNS server address

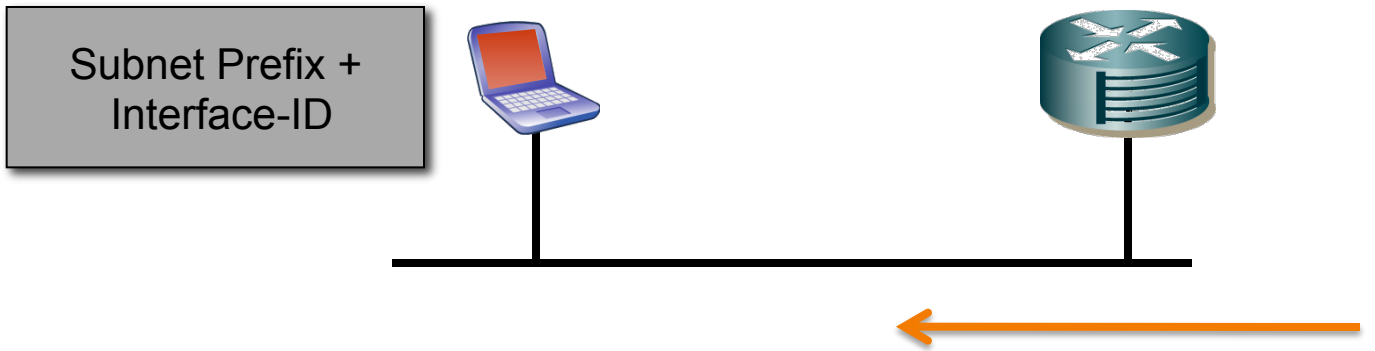
  This is known as Stateless DHCP.

- If the M bit is set in the router’s RAs

  will use the DHCP server to acquire its IP address and Other information (This is known as Stateful DHCP) .

  By default a Windows 7 host will also use SLAAC. To disable SLAAC, disable the A-Flag in RA Message

1 – Address Autoconfiguration (SLAAC)



- Autoconfiguration with “no collisions”
- Offers “plug and play”

RFC2462

Using Autoconfiguration
Default Configuration

A-Flag set to ON by default
M-Flag set to OFF by default

Indicates that the host should use auto-configuration for address assignment

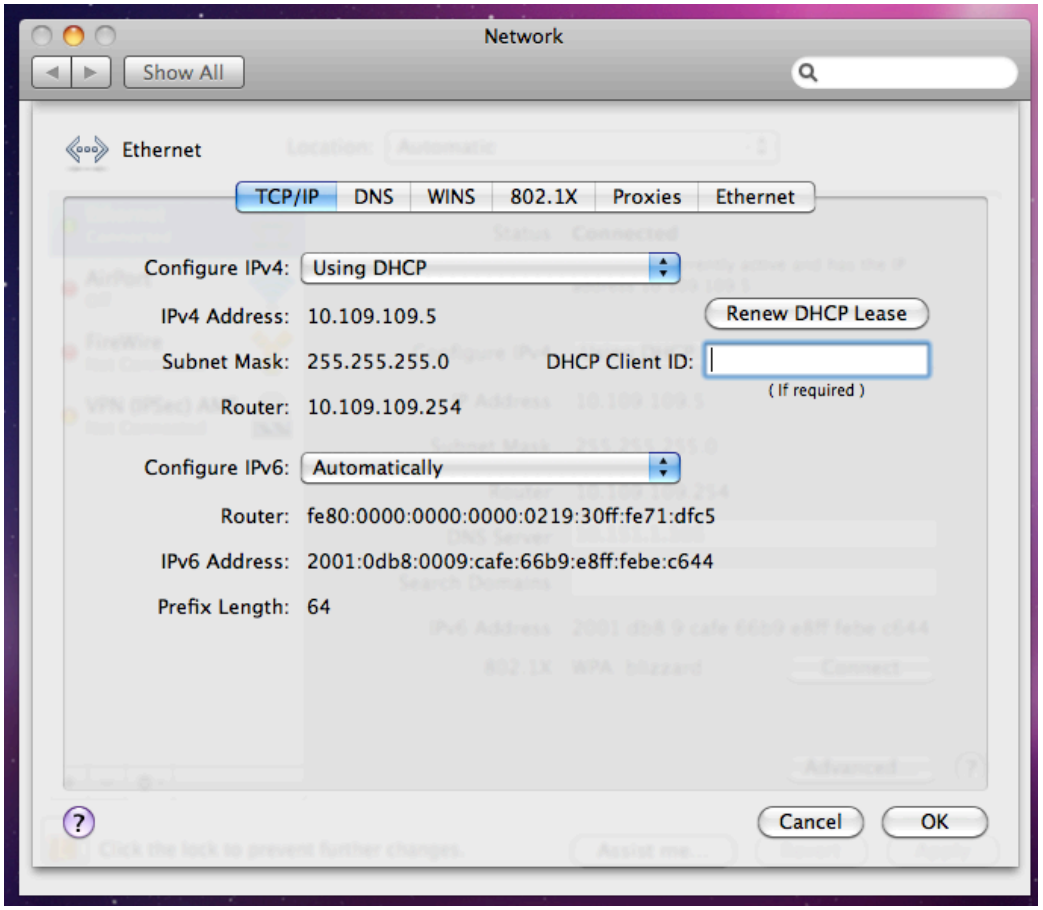
```
!
ipv6 unicast-routing
!
!
interface Vlan101
 ip address 10.101.101.254 255.255.255.0
 ipv6 address 2001:DB8:1:CAFE::1/64
 ipv6 enable
 ipv6 nd prefix 2001:DB8:1:CAFE::/64 300 300
!
```

Using Autoconfiguration
Results: Win7 host gets 2 Global Addresses

```
C:\> netsh int ipv6 sh addr

<snip>

Interface 11: Local Area Connection

Addr Type  DAD State   Valid Life Pref. Life Address
---------  ----------- ---------- ---------- ------------------------
Temporary  Preferred        4m26s      4m26s 2001:db8:1:cafe:a588:46c6:6024:33a5
Public     Preferred        4m26s      4m26s 2001:db8:1:cafe:b407:e685:fb14:c12d
Other      Preferred     infinite   infinite fe80::b407:e685:fb14:c12d%11

C:\>
```

- Windows 7 doesn't use the EUI-64 technique by default when forming its interface identifier.
- Randomized address are generated for non-Temporary autoconfigured addresses including public and link-local – used instead of EUI-64 addresses
- Win7 host gets 2 global addresses – using SLAAC (Public and Temporary)

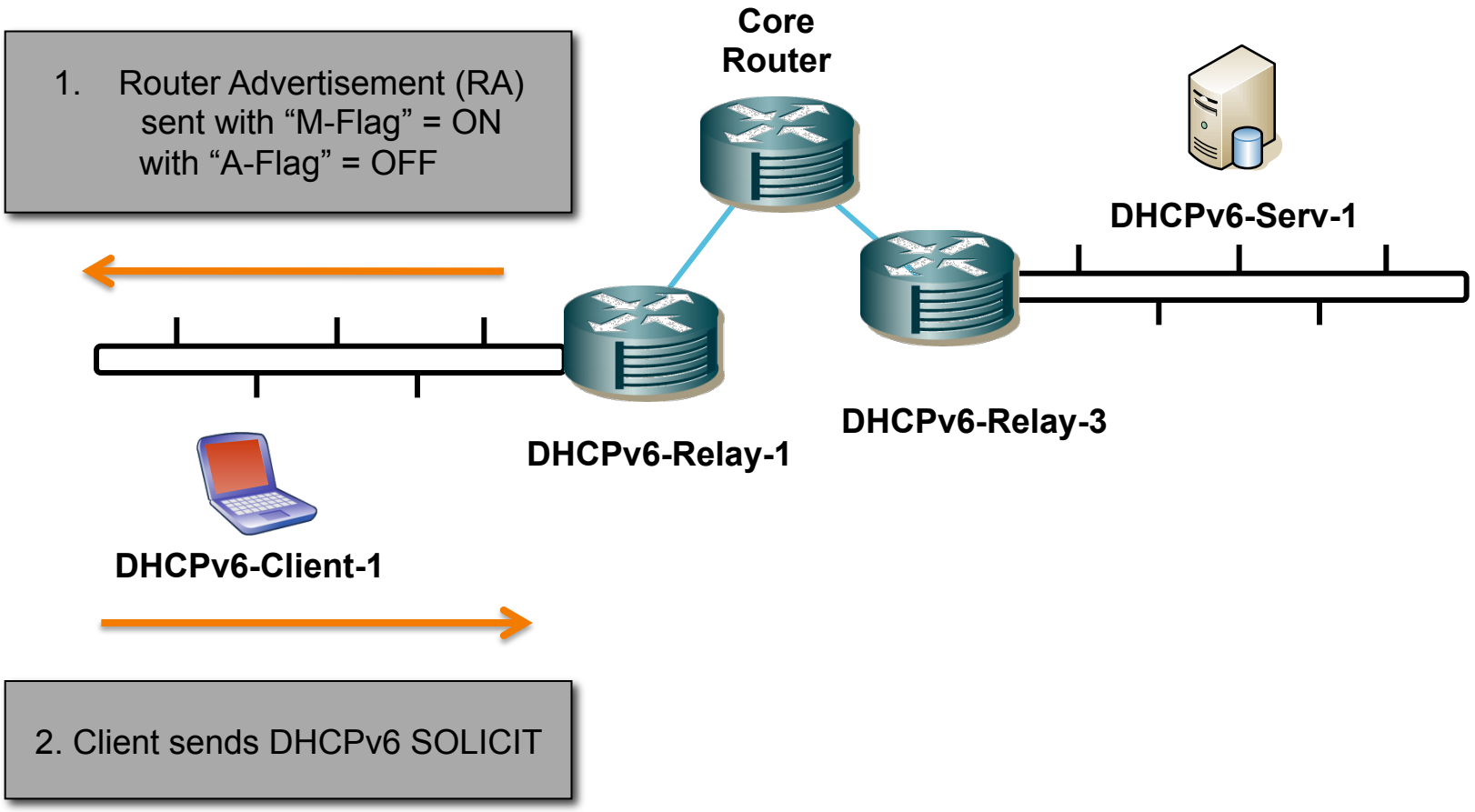
Using Autoconfiguration
MacOSX




```
mac:~$ ifconfig -L en0 inet6
en0: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        inet6 fe80::66b9:e8ff:febe:c644%en0 prefixlen 64 scopeid 0x4
        inet6 2001:db8:9:cafe:66b9:e8ff:febe:c644 prefixlen 64 autoconf pltime 0 vltime 2591981
mac:~$
```

2 – Stateful DHCP only

RA's can be used to control DHCPv6 Client Behavior



2a – Using only the M-Flag
Using Stateful DHCP – Configuration Sample

```
!
ipv6 unicast-routing
!
!
ipv6 dhcp pool DATA-IPv6
 address prefix 2001:DB8:1:CAFE::/64 lifetime 600 600
 domain-name rack-campus.cisco.com
!
interface Vlan101
 ip address 10.101.101.254 255.255.255.0
 ipv6 address 2001:DB8:1:CAFE::1/64
 ipv6 enable
 ipv6 nd prefix 2001:DB8:1:CAFE::/64
 ipv6 nd managed-config-flag
 ipv6 dhcp server DATA-IPv6
!
```

Specifies an address prefix for address assignment.

Set the M-Flag (Managed address configuration bit)
Indicates that the host should use DHCP for stateful address assignment

Specifies the IPv6 Pool name.

```
SW1#sh ipv6 dhcp binding
Client: FE80::B407:E685:FB14:C12D (Vlan101)
  DUID: 0001000112DFBC30000C29616F1F
  IA NA: IA ID 0x0E000C29, T1 300, T2 480
    Address: 2001:DB8:1:CAFE:5882:DEA4:A3C:570C
            preferred lifetime 600, valid lifetime 600
            expires at Apr 19 1993 09:50 PM (587 seconds)
SW1#
```

2a – Using only the M-Flag
Results: Win7 host gets 3 Global Addresses

```
C:\> netsh int ipv6 sh addr

<snip>

Interface 11: Local Area Connection

Addr Type  DAD State   Valid Life Pref. Life Address
---------  ----------- ---------- ---------- ------------------------
Dhcp       Preferred        9m28s      9m28s 2001:db8:1:cafe:5882:dea4:a3c:570c
Temporary  Preferred        4m26s      4m26s 2001:db8:1:cafe:a588:46c6:6024:33a5
Public     Preferred        4m26s      4m26s 2001:db8:1:cafe:b407:e685:fb14:c12d
Other      Preferred     infinite   infinite fe80::b407:e685:fb14:c12d%11

C:\>
```

- Win7 host gets 3 global addresses – one using DHCP, two using SLAAC (Public and Temporary)
- Both SLAAC and DHCP runs independently, and this is the default behavior when only setting the M-Flag
- To only have DHCP, the A-Flag has to be cleared (see next slide)

2b – Using Stateful DHCP and disabling SLAAC
Configuration Sample

```
!
ipv6 unicast-routing
!
!
ipv6 dhcp pool DATA-IPv6
 address prefix 2001:DB8:1:CAFE::/64 lifetime 600 600
 domain-name rack-campus.cisco.com
!
interface Vlan101
 ip address 10.101.101.254 255.255.255.0
 ipv6 address 2001:DB8:1:CAFE::1/64
 ipv6 enable
 ipv6 nd prefix 2001:DB8:1:CAFE::/64 300 300 no-autoconfig
 ipv6 nd managed-config-flag
 ipv6 dhcp server DATA-IPv6
!
```

Set the A-Flag (autoconfig bit) to OFF.
Indicates that the host should not use SLAAC.

Set the M-Flag (Managed address configuration bit) to ON.
Indicates that the host should use DHCP for stateful address assignment

2b – Using Stateful DHCP and disabling SLAAC
Results: Win7 host only uses DHCP

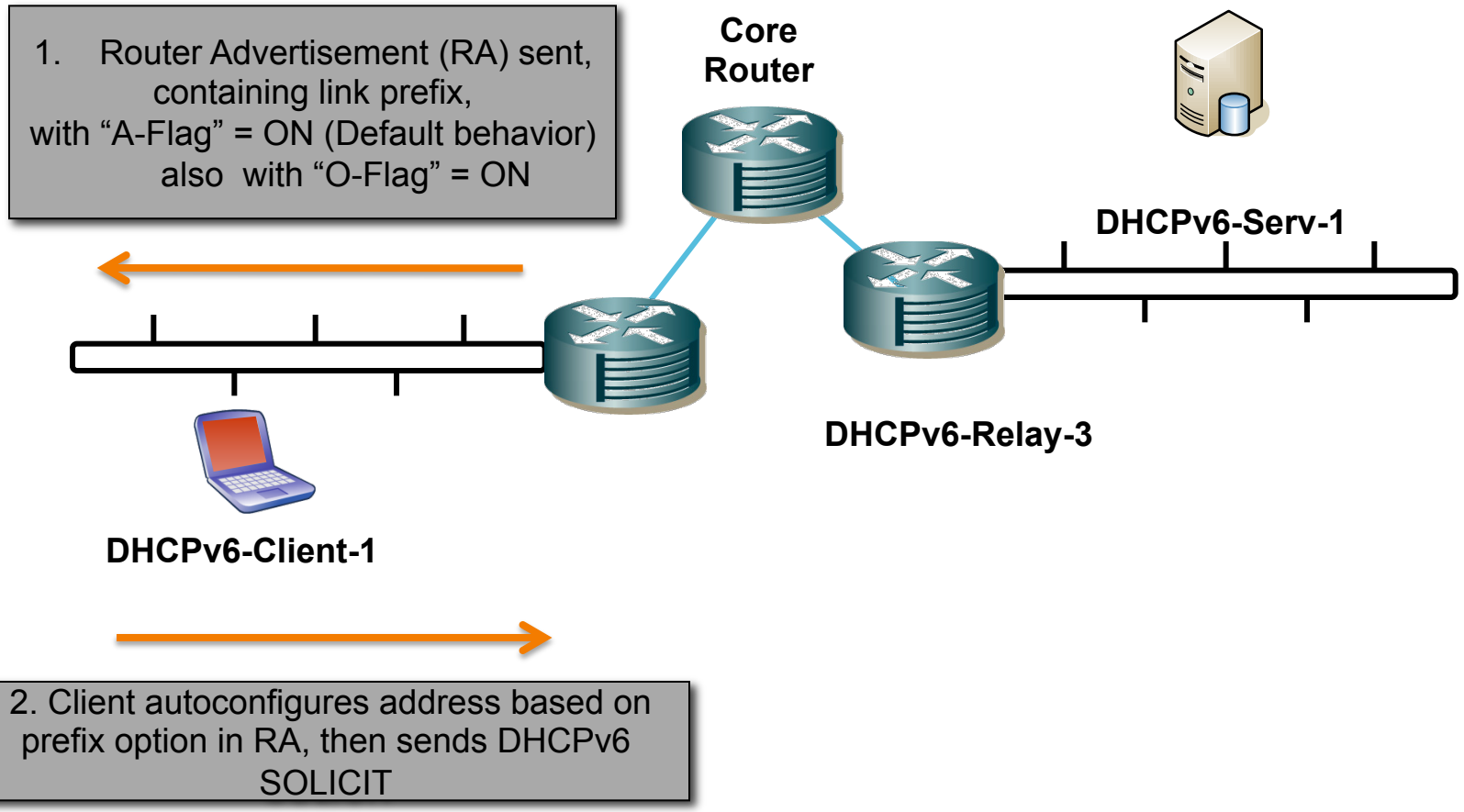
```
SW1#sh ipv6 dhcp binding
Client: FE80::B407:E685:FB14:C12D (Vlan101)
  DUID: 0001000112DFBC30000C29616F1F
  IA NA: IA ID 0x0E000C29, T1 300, T2 480
    Address: 2001:DB8:1:CAFE:A826:E48D:9153:3B23
             preferred lifetime 600, valid lifetime 600
             expires at Apr 19 1993 09:55 PM (512 seconds)
SW1#
```

```
C:\> netsh int ipv6 sh addr

<snip>

Interface 11: Local Area Connection

Addr Type  DAD State   Valid Life Pref. Life Address
---------  ----------- ---------- ---------- ------------------------
Dhcp       Preferred        9m47s      9m47s 2001:db8:1:cafe:a826:e48d:9153:3b23
Other      Preferred     infinite   infinite fe80::b407:e685:fb14:c12d%11

C:\>
```

- Win7 host has only one global address using DHCP

3 – Stateless DHCP

Stateless DHCPv6 normally combines stateless auto-configuration for address assignment, DHCPv6 exchange for all other configuration settings.



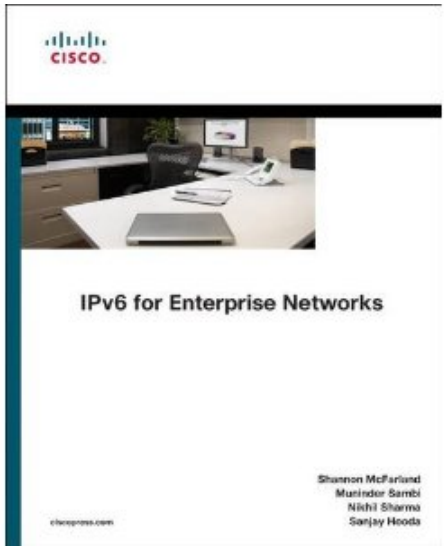
Agenda

- Introduction
- IPv6 in the Enterprise
- Routing Considerations
- Security for IPv6
- First Hop Security
- Unified Communications
- Multicast
- DNS
- Deployment and Operation Considerations

IPv6 – Enterprise Deployment Considerations

IPv6 in the Enterprise - Agenda

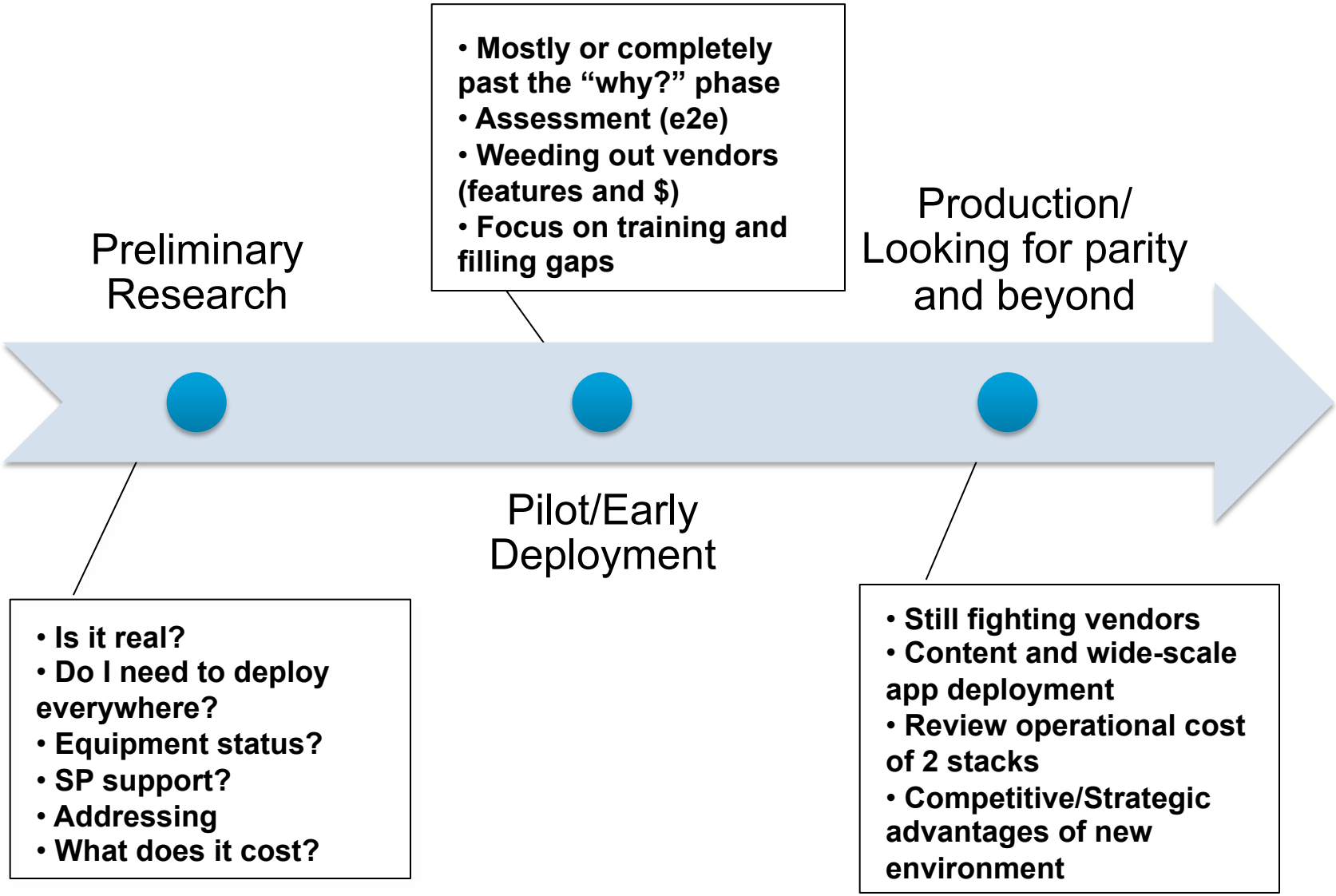
- Planning and Deployment Summary
- Address Considerations
- General Concepts
- Infrastructure Deployment
  - Campus/Data Center
  - WAN/Branch
  - Remote Access
- Communicating with the Service Providers
- Appendix—For Reference Only



Coming Soon!!

Planning and Deployment Summary

Enterprise Adoption Spectrum

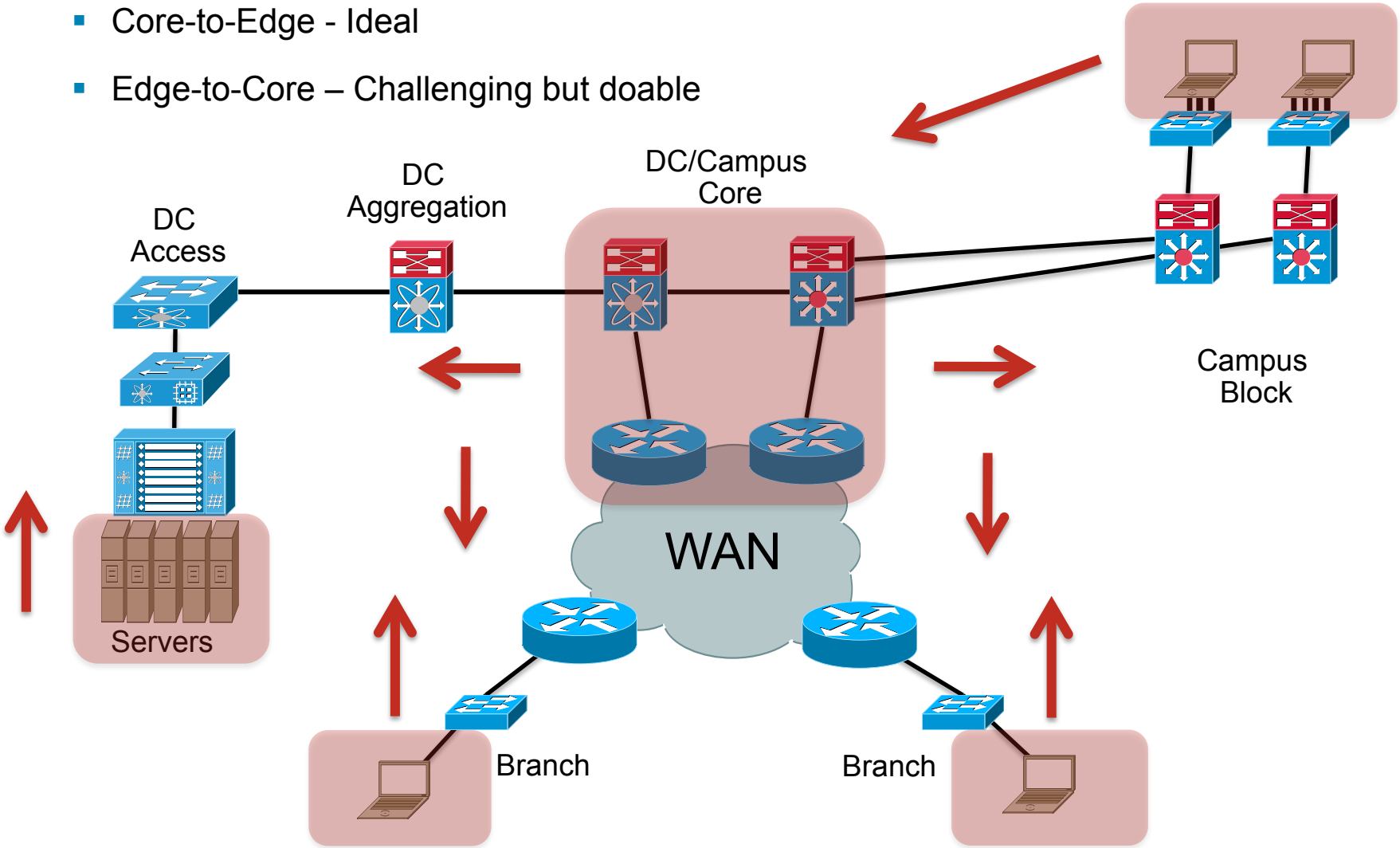


IPv6 Integration Outline

Pre-Deployment Phases	Deployment Phases
• Establish the network starting point • Importance of a network assessment and available tools • Defining early IPv6 security guidelines and requirements • Additional IPv6 “pre-deployment” tasks needing consideration	• Transport considerations for integration • Campus IPv6 integration options • WAN IPv6 integration options • Advanced IPv6 services options

Where do I start?

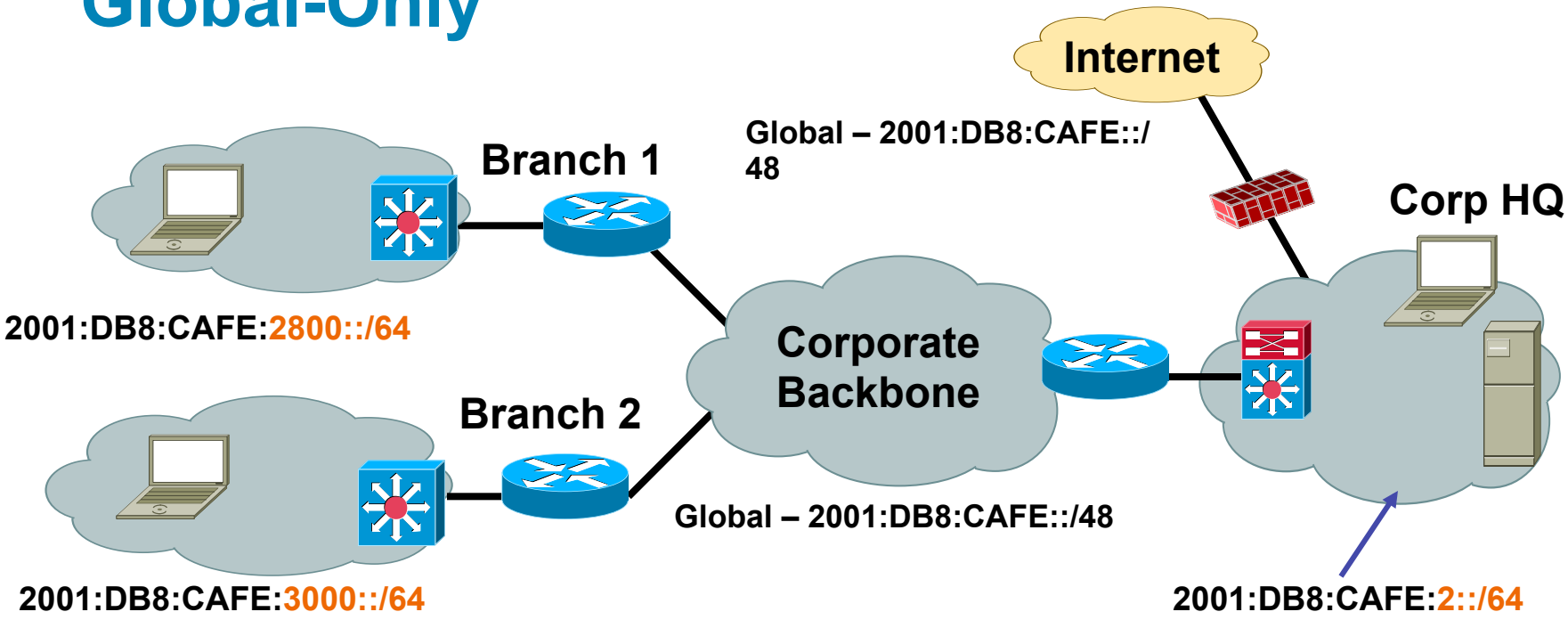
- Based on Timeframe/Use case
- Core-to-Edge - Ideal
- Edge-to-Core – Challenging but doable



Address Considerations

Recommended

Global-Only



- Global is used everywhere
- Default is /48 – can be larger: http://www.ripe.net/ripe/docs/ipv6policy.html
- Provider independent – See Number Resource Policy Manual (NRPM) - http://www.ripe.net/rs/ipv6/
- Only downside is breaking the habit of believing that topology hiding is a good security method ☺

Link Level—Prefix Length Considerations

64 bits	> 64 bits
▪ Recommended by RFC5375 and IAB/IESG ▪ Consistency makes management easy ▪ MUST for SLAAC (MSFT DHCPv6 also) ▪ Significant address space loss	▪ Address space conservation ▪ Special cases: /126—valid for p2p /127—not valid for p2p (RFC3627) /128—loopback ▪ Complicates management ▪ Must avoid overlap with specific addresses: Router Anycast (RFC3513) Embedded RP (RFC3956) ISATAP addresses

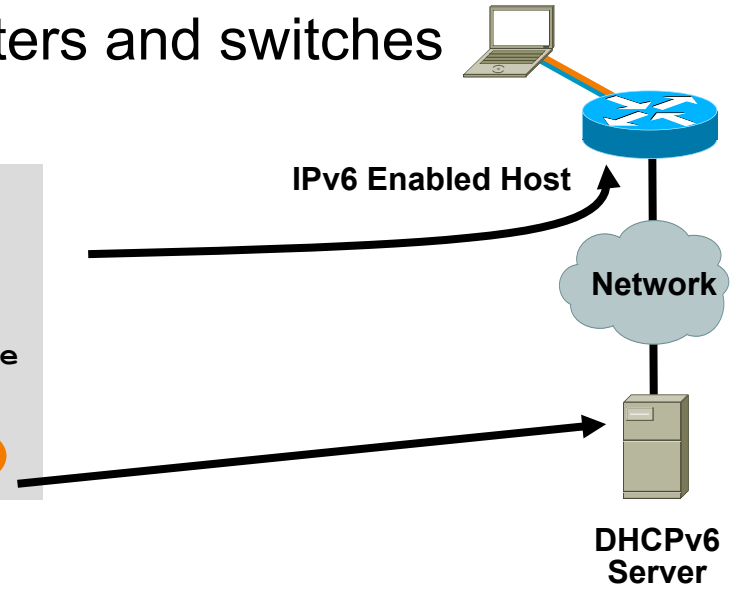
SLAAC & Stateful/Stateless DHCPv6

- StateLess Address AutoConfiguration (SLAAC)
- Stateful and stateless DHCPv6 server

  Cisco Network Registrar:
  http://www.cisco.com/en/US/products/sw/netmgtsw/ps1982/

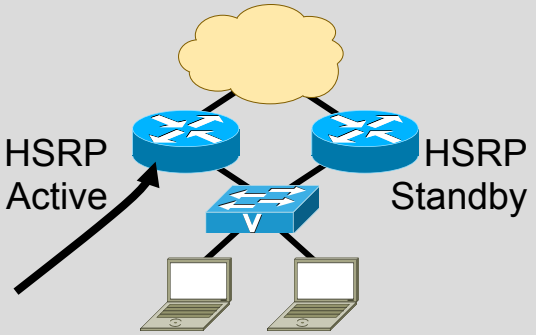
  Microsoft Windows Server 2008:
  http://technet2.microsoft.com/windowsserver2008/en/library/bab0f1a1-54aa-4cef-9164-139e8bcc44751033.mspx?mfr=true
- DHCPv6 Relay—supported on routers and switches

```
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 dhcp relay destination 2001:DB8:CAFE:10::2
```



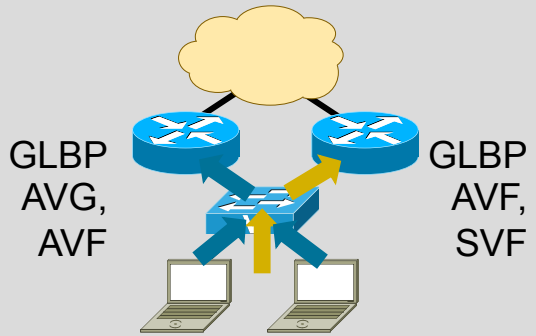
General Concepts—FHRP, QoS and Scalability

First Hop Router Redundancy



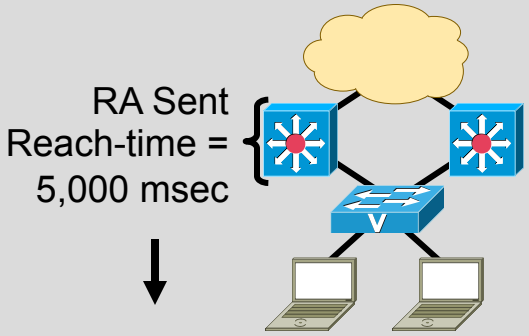
HSRP for v6

- 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



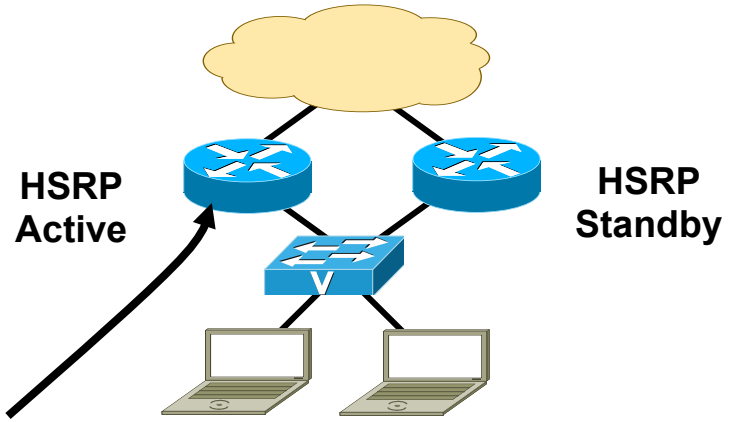
Neighbor **U**nreachability **D**etection

- 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

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
```

Host with GW of Virtual IP

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

IPv6 QoS Policy & Syntax

- Unified QoS Policy (v4/v6 in same policy) or separate?
- IPv4 syntax has used “ip” following match/set statements

  Example: `match ipdscp, set ipdscp`
- 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       4000d.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
```

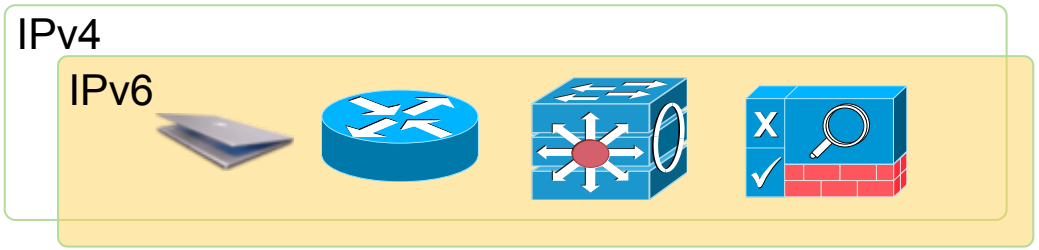
- Full internet route tables—ensure to account for TCAM/memory requirements for both IPv4/IPv6—not all vendors can properly support both
- Multiple routing protocols—IPv4 and IPv6 will have separate routing protocols. Ensure enough CPU/ Memory is present
- Control plane impact when using tunnels—terminate 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/en/US/docs/ios/ipv6/configuration/guide/ip6-roadmap.html

IPv6 Co-existence Solutions

Dual Stack

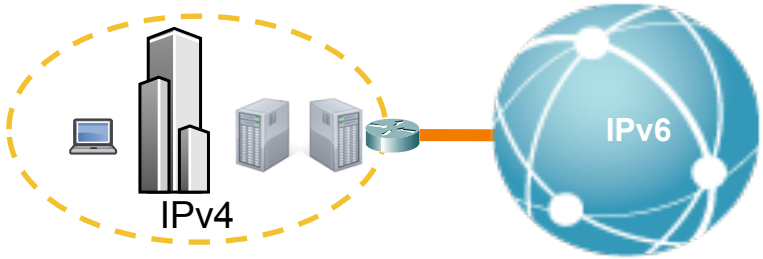


Recommended Enterprise Co-existence strategy

Tunneling Services

Connect Islands of IPv6 or IPv4

Translation Services



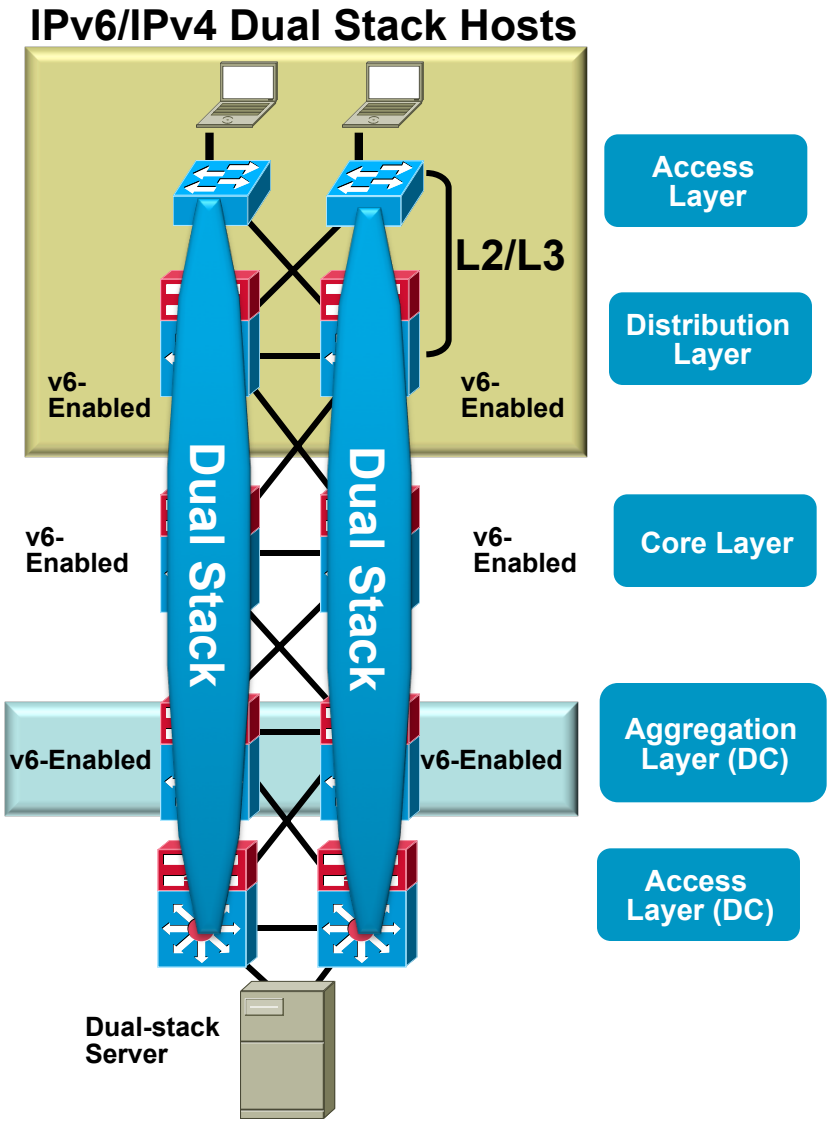
Connect to the IPv6 community

Campus/Data Center

Deploying IPv6 in Campus Networks:
http://www.cisco.com/univercd/cc/td/doc/solution/campipv6.pdf

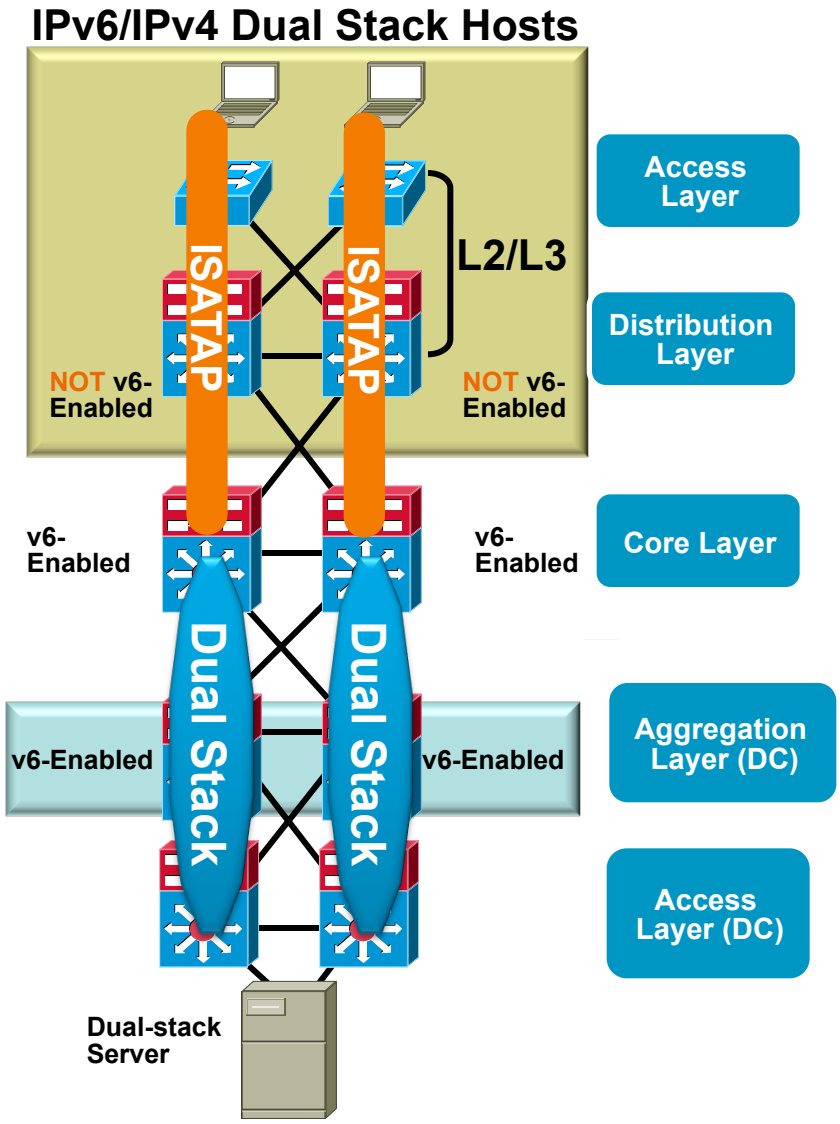
Campus IPv6 Deployment Options
Dual-Stack IPv4/IPv6

- #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



Campus IPv6 Deployment Options
Hybrid Model

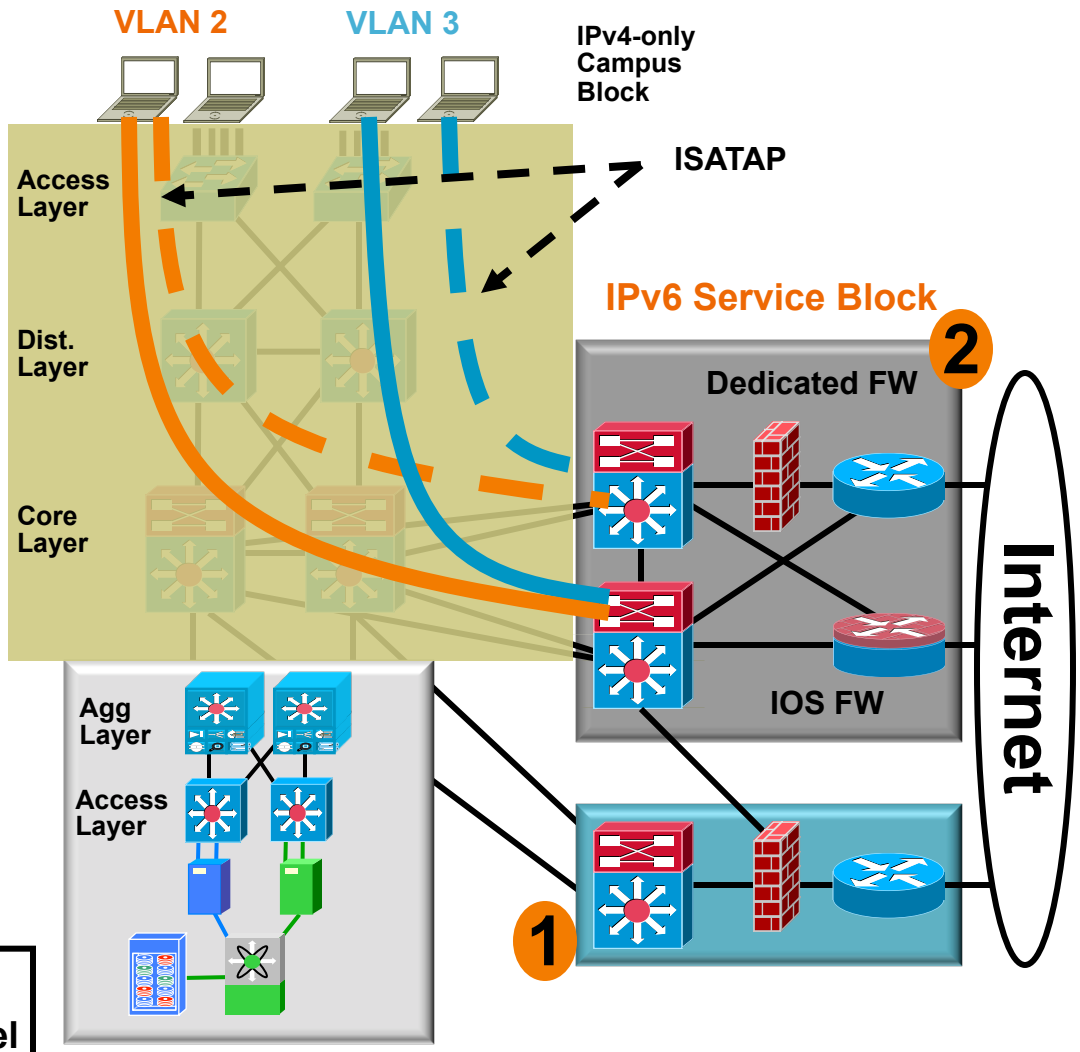
- Offers IPv6 connectivity via multiple options
  - Dual-stack
  - Configured tunnels—L3-to-L3
  - ISATAP—Host-to-L3
- Leverages existing network
- Offers natural progression to full dual-stack design
- May require tunneling to less-than-optimal layers (i.e. core layer)
- ISATAP creates a flat network (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



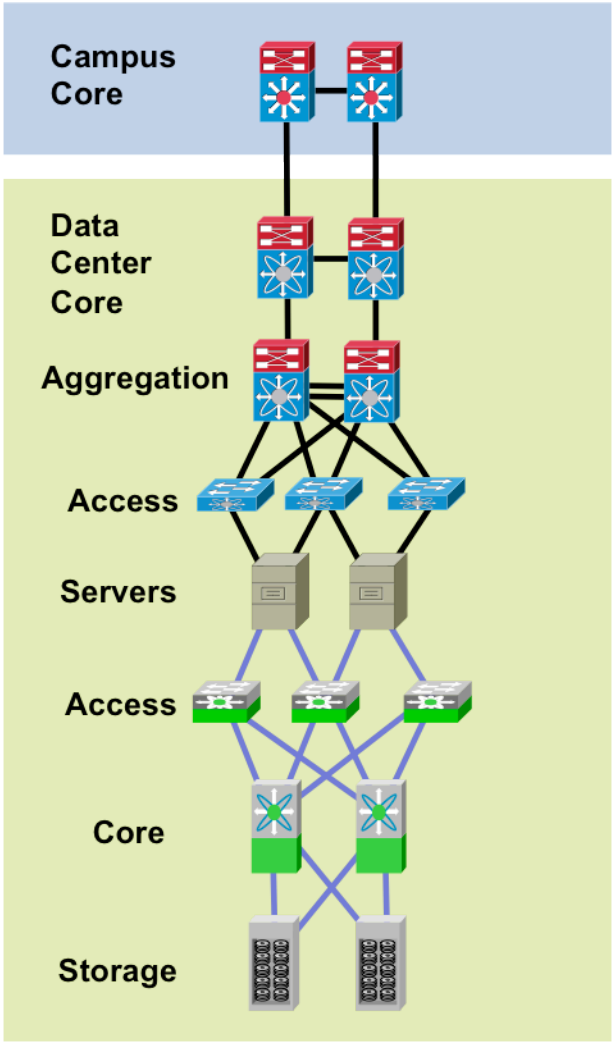
Campus IPv6 Deployment Options

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

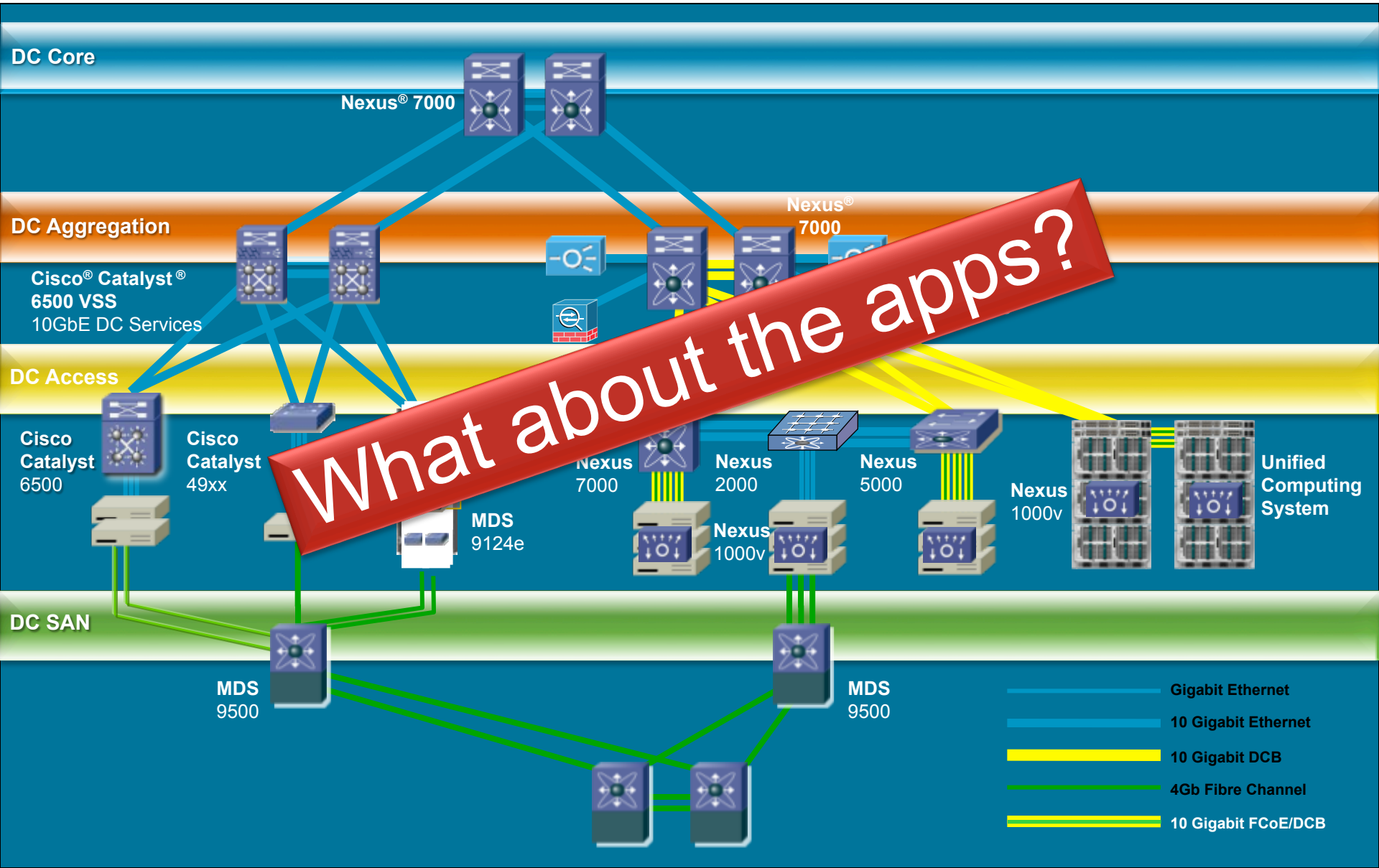


IPv6 Data Center Integration



- Route/Switch 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
  - Innocent looking Server OS upgrades – Windows Server 2008 - Impact on clusters – Microsoft Server 2008 Failover clusters full support IPv6 (and L3)
- Build an IPv6-only server farm?

Virtualized DC Solutions



IPv6 in the Enterprise Data Center
Biggest Challenges Today

- Network services above L3
  - SLB, SSL-Offload, application monitoring (probes) – ACE and GSS
  - Application Optimization – WAAS and ACE
  - High-speed security inspection/perimeter protection – ASA/IPS/IDS/IronPort
- Application support for IPv6 – Know what you don't know
  - If an application is protocol centric (IPv4):
    - Leave as-is
    - 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

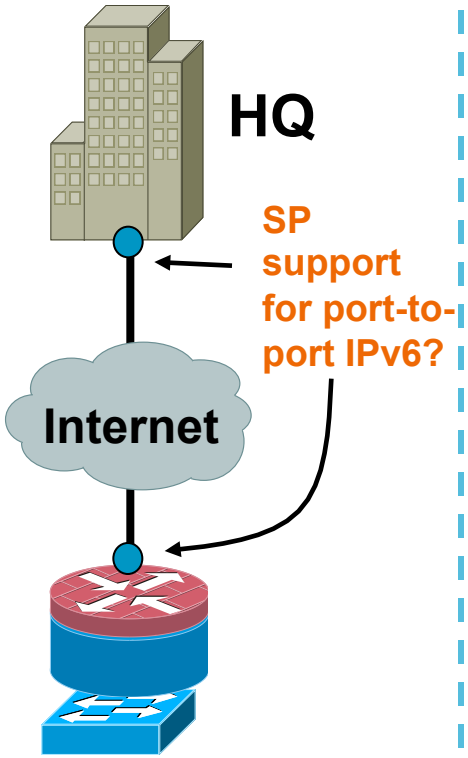
WAN/Branch

Deploying IPv6 in Branch Networks:
http://www.cisco.com/univercd/cc/td/doc/solution/brchipv6.pdf

IPv6 Enabled Branch

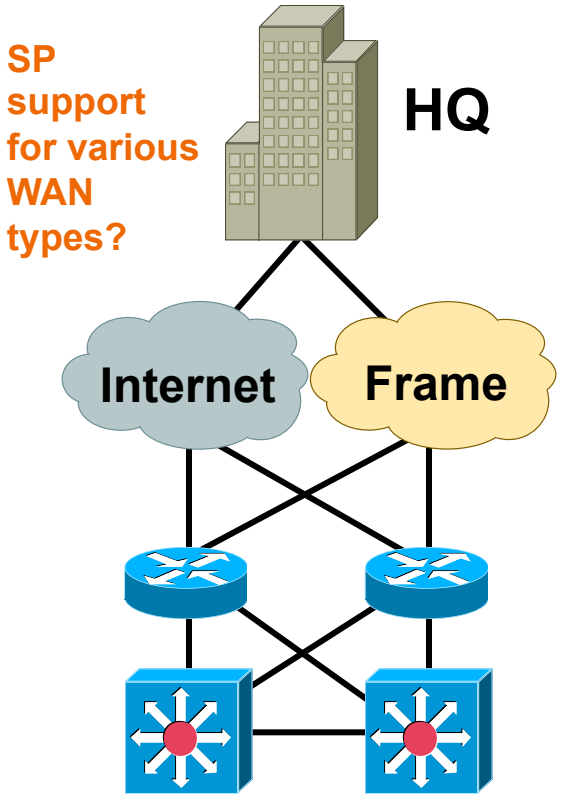
Focus more on the provider and less on the gear

Branch Single Tier



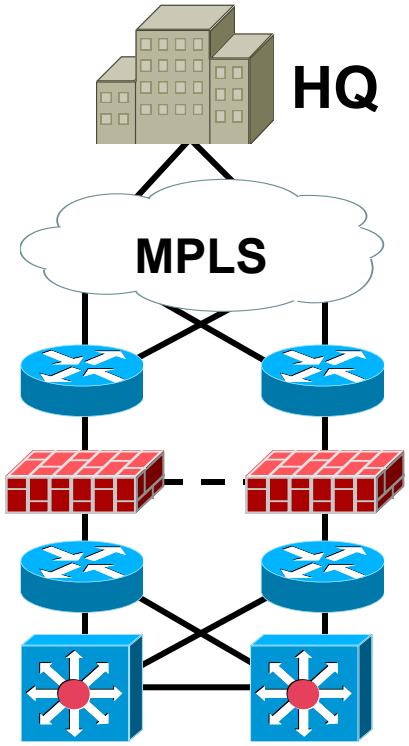
Dual-Stack
IPSec VPN (IPv4/IPv6)
Firewall (IPv4/IPv6)
Integrated Switch (MLD-snooping)

Branch Dual Tier



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

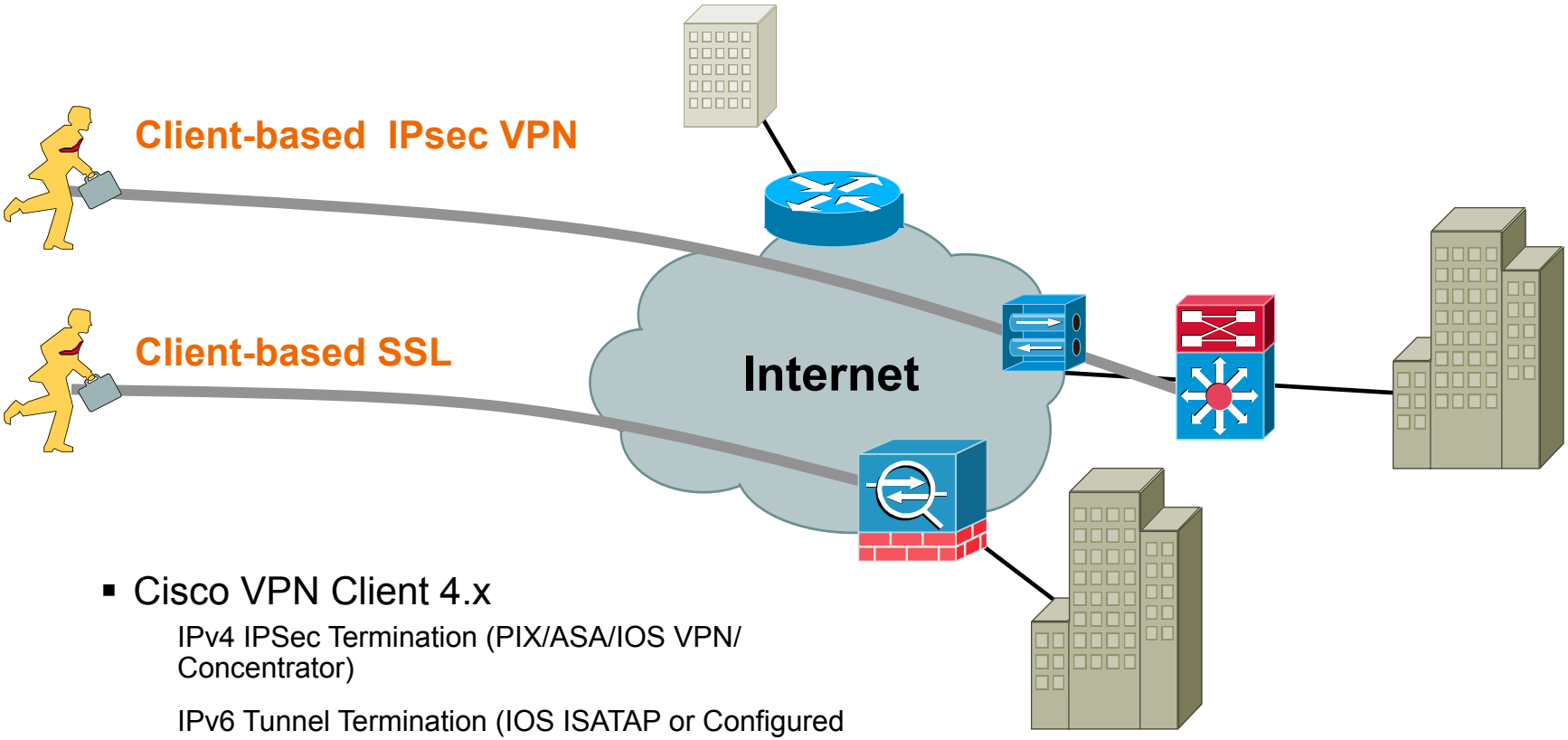
Branch Multi-Tier



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

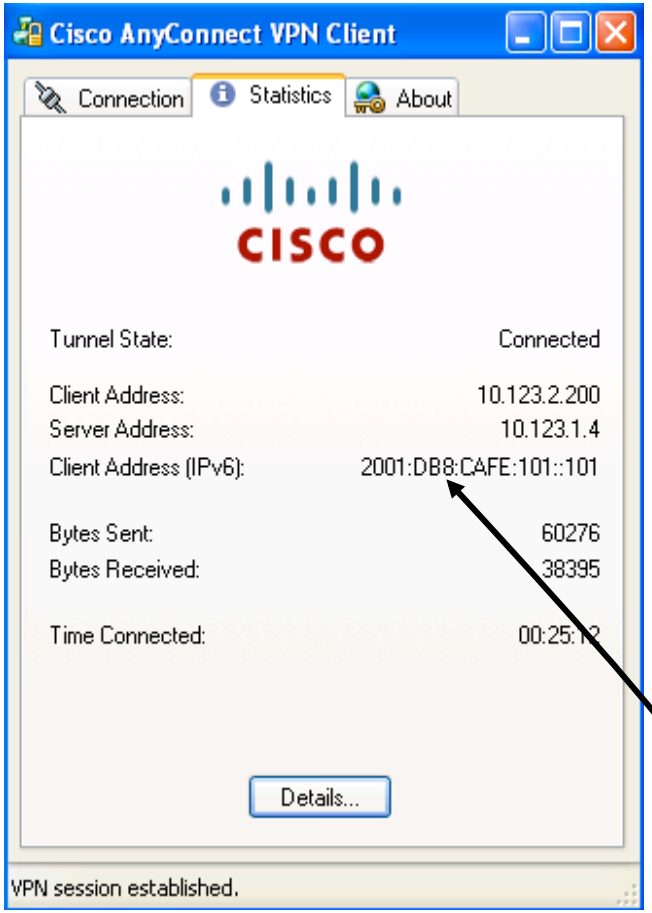
Remote Access

Cisco Remote VPN – IPv6

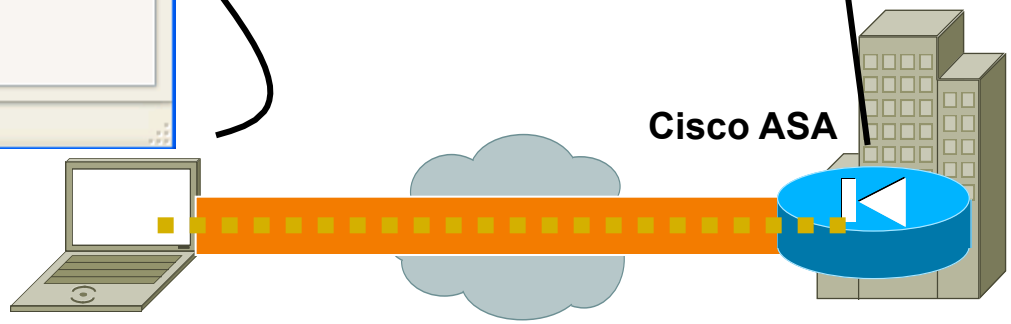


- Cisco VPN Client 4.x
  - IPv4 IPSec Termination (PIX/ASA/IOS VPN/ Concentrator)
  - IPv6 Tunnel Termination (IOS ISATAP or Configured Tunnels)
- AnyConnect Client 2.x
  - SSL/TLS or DTLS (datagram TLS = TLS over UDP)
  - Tunnel transports both IPv4 and IPv6 and the packets exit the tunnel at the hub ASA as native IPv4 and IPv6.

AnyConnect 2.x—SSL VPN



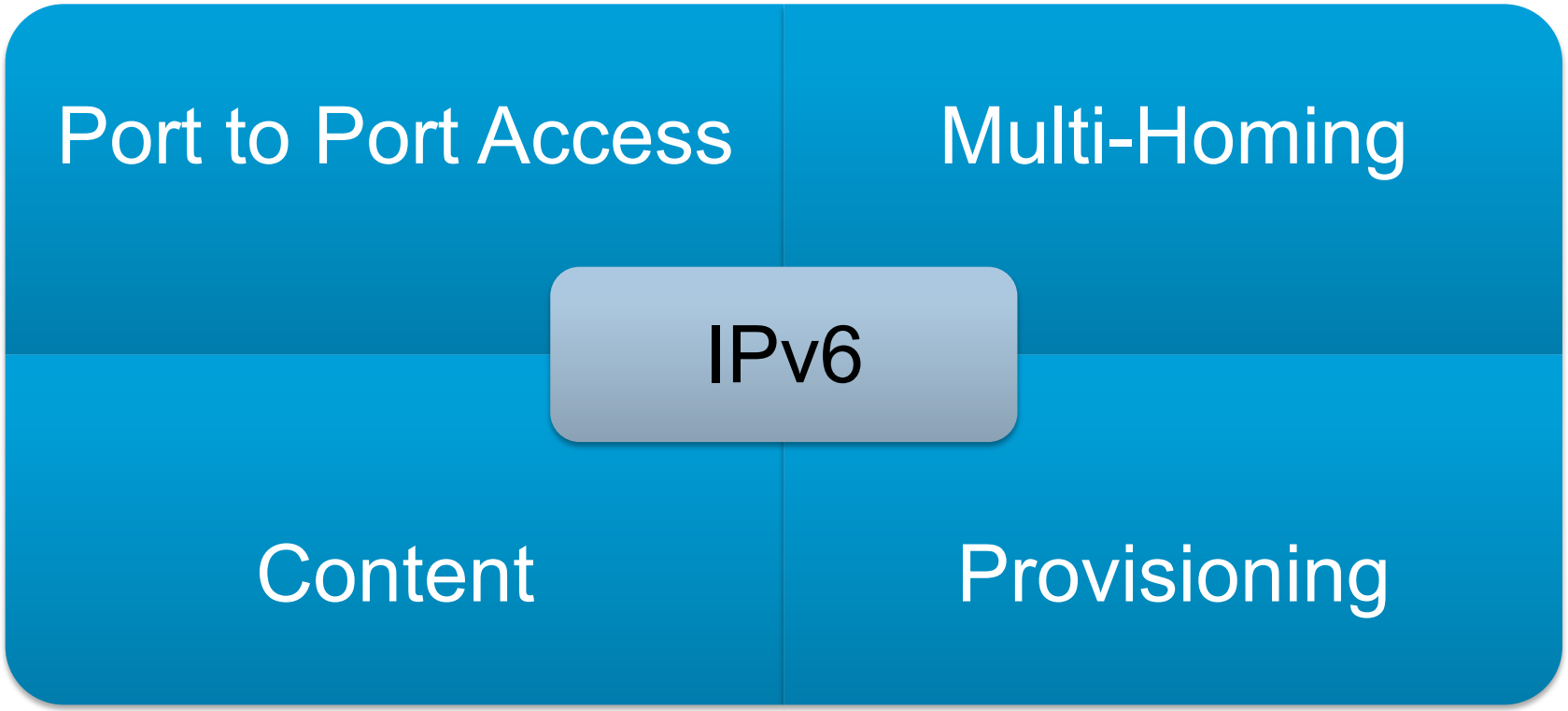

```
asa-edge-1#show vpn-sessiondb svc
Session Type: SVC
Username     : ciscoese              Index        : 14
Assigned IP  : 10.123.2.200          Public IP    : 10.124.2.18
Assigned IPv6: 2001:db8:cafe:101::101
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
License      : SSL VPN
Encryption   : RC4 AES128            Hashing      : SHA1
Bytes Tx     : 79763                 Bytes Rx     : 176080
Group Policy : AnyGrpPolicy          Tunnel Group: ANYCONNECT
Login Time   : 14:09:25 MST Mon Dec 17 2007
Duration     : 0h:47m:48s
NAC Result   : Unknown
VLAN Mapping : N/A                   VLAN         : none
```



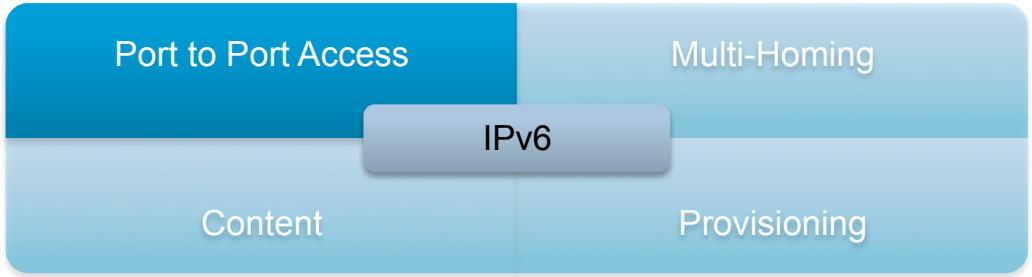
Dual-Stack Host
AnyConnect Client

Communicating with the Service Provider

Top SP Concerns for Enterprise Accounts



Port-to-Port Access



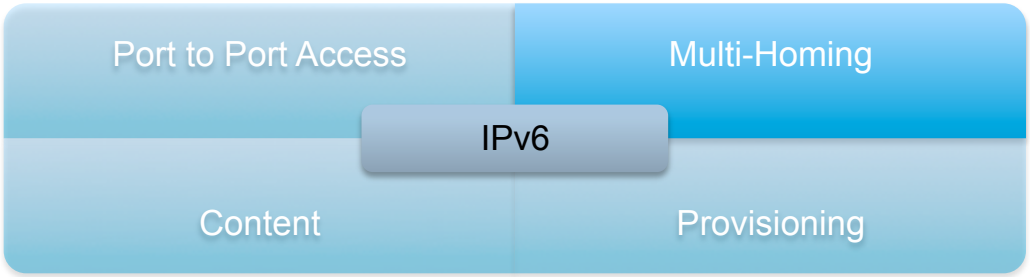
Basic Internet *
- Dual-stack or native IPv6 at each POP
- SLA driven just like IPv4 to support VPN, content access

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

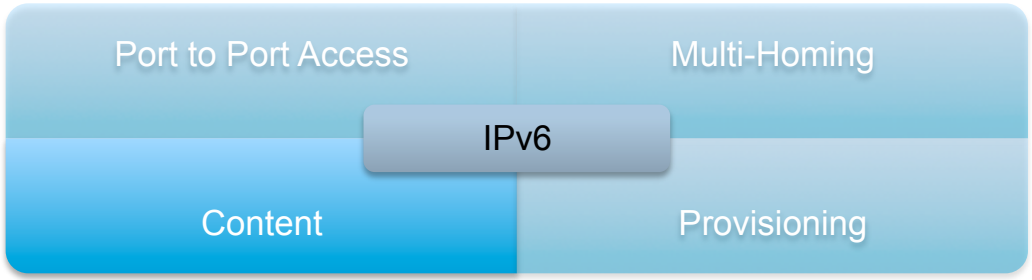
NAT

- 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



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

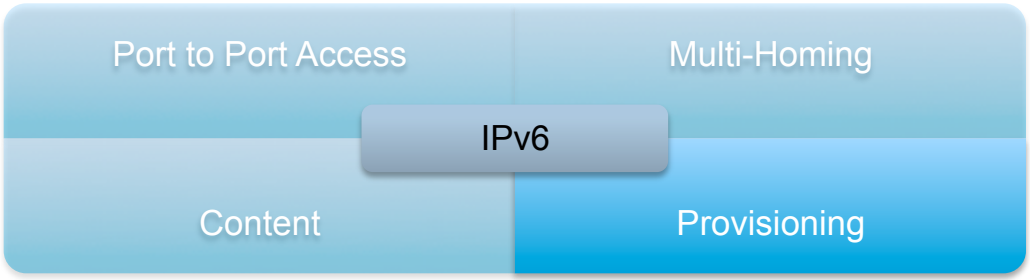
Move to Hosted/ Cloud

- 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



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

Conclusion

- “Dual stack where you can – Tunnel where you must – Translate only when you have a gun to your head”
- 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, Windows 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

Reference Materials

- New/Updated IPv6 Cisco Sites

  http://www.cisco.com/ipv6

  http://www.cisco.com/go/ipv6

  http://www.cisco.gom/go/entipv6

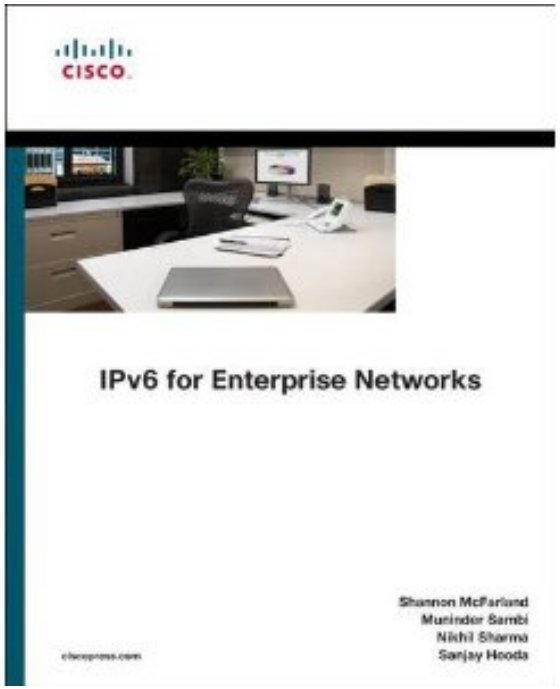
- Deploying IPv6 in Campus Networks:

  http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/CampIPv6.html

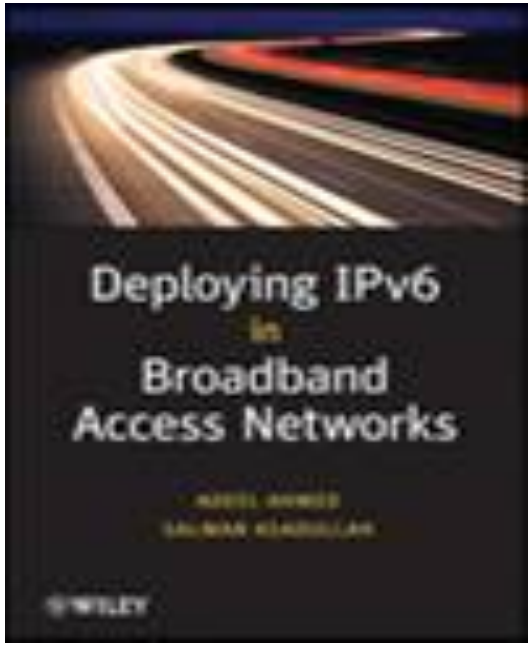
- Deploying IPv6 in Branch Networks:

  http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns816/landing_br_ipv6.html

Recommended Reading



Coming Soon!!



Deploying IPv6 in Broadband Networks
Adeel Ahmed, Salman Asadullah
ISBN0470193387,
John Wiley & Sons Publications®

Agenda

- Introduction
- IPv6 in the Enterprise
- Routing Considerations
- Security for IPv6
- First Hop Security
- Unified Communications
- Multicast
- DNS
- Deployment and Operation Considerations

IPv6 Routing Considerations

IPv6 Routing Considerations

- EIGRPv6
  - Protocol Modifications
  - Routing Considerations
- OSPFv3
  - Protocol Modifications
  - Routing Considerations
- IS-IS/IPv6
  - Protocol Modifications
  - Routing Considerations
- Summary

EIGRPv6 - Overview

- A new Protocol Dependent Module (PDM) to route IPv6
- A familiar “look and feel” means incumbent EIGRP operational expertise can be leveraged
- Add new TLV’s (Type, Length, Value) in EIGRP packets to carry IPv6 prefixes
  - Internal routes TLV (Type 0x0401)
  - External routes TLV (Type 0x0402)
- Uses proven Reliable Transport Protocol (RTP) for reliable delivery of packets
- DUAL performs route computations for IPv6 without modifications

EIGRP IPv6 - Overview

Implementation	Provides feature parity with most IPv4 Features (stubs, scaling, summarization, etc) EIGRP IPv6 uses the same Reliable Multicast Transport protocol used by IPv4 IPv6 Link-local address are used to establish an adjacency
Important Differences	32 bit Router ID must be explicitly configured if no IPv4 address is available Hellos are sourced from the link-local address and destined to FF02::A (all EIGRP routers); Neighbors are not required to share the same global prefix (with the exception of explicitly specified neighbors where traffic is sent unicast) Automatic summarization disabled by default for EIGRP IPv6, and is not even configurable for EIGRP IPv6 "no split-horizon" is the default configuration for EIGRP IPv6 (IPv6 supports multiple prefixes per interface) EIGRP IPv6 does not support the "default-information" command as there is no support in IPv6 for the configuration of default networks other than ::/0
Note	"ipv6 unicast" must be configured under global mode to enable ipv6 routing "ipv6 enable" must be configured under all interfaces which will be enabled for ipv6

EIGRPv6 - IPv6 Link-Local Address

- Used by EIGRP to source Hello packets
  - Hence adjacency packets can never be routed
- IPv6 forwarding must be configured on an interface to build an EIGRPv6 adjacency
- Link local addresses are auto assigned when you enable the interface
  - You can assign a link local address manually, as well

```
ipv6 unicast
interface Ethernet1/0
  ipv6 enable
```

EIGRPv6 - Configuration

- Named mode configuration only
- 32 bit router ID is required
  - Manually configured ID is selected first
  - Highest loopback IPv4 address is selected second
  - IPv4 address found on any physical interface is selected last

```
int Ethernet 0/0
  ipv6 eigrp 6473
!
router eigrp 6473
no shutdown
```

```
router eigrp simple-v6
  address-family ipv6 auto 6476
    af-interface default
      no shutdown
```

EIGRPv6 - Aggregation

- Auto-summarization is not supported
  - There are no “classful boundaries” on which auto-summarization could operate
- Summarization can be configured in two places
  - Under the interface
  - Under the named router

```
interface Ethernet0/0
  ipv6 summary-address eigrp 6473 ?
    X:X:X:X::X/<0-128>  IPv6 prefix
```

```
router eigrp nw010-ipv6
  address-family ipv6 auto 6473
    af-interface Ethernet0/0
      summary-address ?
    X:X:X:X::X/<0-128>  IPv6 prefix
```

EIGRPv6 - Show Commands

```
show ipv6 eigrp topology
EIGRP-IPv6 VR(nw010) Address-Family Topology Table for AS(6473)/ID(1.1.1.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply, r - reply
Status, s - sia Status

P 2040:3333::31:113:0/112 , 1 successors, FD is 281600
        via FE80::A8BB:CCFF:FE00:200 (281600/256), Ethernet0/0
P 2040:3333::31:114:0/112, 1 successors, FD is 281600
        via FE80::A8BB:CCFF:FE00:200 (281600/256), Ethernet0/0
```

Next hop is link local IPv6 address

EIGRPv6 - Show Commands

```
show ipv6 eigrp topology 2040:3333::31:113:0/112
EIGRP-IPv6 VR(nw010) Address-Family (AS 6473): Topology entry for 8:1:1::1/128
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 281600
  Routing Descriptor Blocks:
  FE80::A8BB:CCFF:FE00:200 (Ethernet0/0), from FE80::A8BB:CCFF:FE00:200, Send flag is 0x0
      Composite metric is (281600/256), Route is External
      Vector metric:
        Minimum bandwidth is 10000 Kbit
        Total delay is 1000 microseconds
        Reliability is 0/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
      External data:
        Originating router is 2.2.2.2
        AS number of route is 0
        External protocol is Static, external metric is 0
        Administrator tag is 0 (0x00000000)
```

Info source is link local IPv6 address

EIGRPv6 - Debugs

```
debug eigrp ?
  fsm         EIGRP Dual Finite State Machine events/actions
  neighbors   EIGRP neighbors
  nsf         EIGRP Non-Stop Forwarding events/actions
  packets     EIGRP packets
  transmit    EIGRP transmission events
```

```
debug eigrp packets
EIGRP Packets debugging is on
    (UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY,
     SIAREPLY)

00:52:47: EIGRP: Received HELLO on Ethernet1/0 nbr FE80::A8BB:CCFF:FE00:401
00:52:47: AS 6473, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0 peerQ
          un/rely 0/0
```

EIGRPv6 - Debugs

IPv6 Specific Debugs

```
debug eigrp address-family ipv6  ?
  <1-6473>      Autonomous System
  neighbor       EIGRP neighbor debugging
  notifications  EIGRP event notifications
  summary        EIGRP summary route processing
  <cr>
```

Event Log

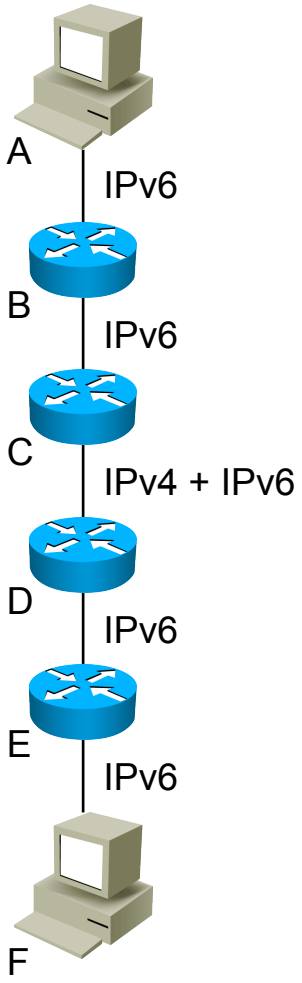
```
show eigrp address-family ipv6 event
1    06:27:52.115 Change queue emptied, entries: 1
2    06:27:52.115 Metric set: 2040:3333::31:113:0/112 281600
3    06:27:52.115 Update reason, delay: new if 4294967295
4    06:27:52.115 Update sent, RD: 2040:3333::31:113:0/112 4294967295
5    06:27:52.115 Update reason, delay: metric chg 4294967295
6    06:27:52.115 Update sent, RD: 2040:3333::31:113:0/112 4294967295
```

EIGRPv6 - Routing Considerations

- Assume only one EIGRP process throughout this network
- Router C forms an adjacency with D using IPv4
- The IPv6 routes are learned across this adjacency without any problems…

  The IPv6 reachability information is just another TLV in EIGRP

- But how does Router C insert the IPv6 routes learned from D into the routing table?



EIGRPv6 - Routing Considerations

- A single EIGRP process can only form one adjacency
  - A single EIGRP process can only have one next hop per neighbor –either IPv4 or IPv6
- There is no way to forward IPv6 traffic to an IPv4 next hop…
- So to deploy IPv6 on an existing IPv4 network, you must run two processes
  - One process which forms IPv4 adjacencies, and carries IPv4 routes
  - One process which forms IPv6 adjacencies, and carries IPv6 routes

OSPFv3 - Changes from OSPFv2

- Per Link Processing
- Addition of flooding scope
- New Link LSA
- Handling of unknown LSA types
- Virtual Link Changes
- Authentication changes

OSPFv3 - Per Link Processing

- IPv6 uses the term “link” instead of network or subnet to indicate communication
  - Interfaces connect to links
  - Adjacencies are formed on link local addresses
- Multiple IPv6 subnets can be assigned to a single link
  - Two nodes can talk directly over a single link, even if they do not share a common IPv6 subnet
  - Network address and mask do not impact the formation of adjacencies

OSPFv3 - Flooding Scope

- Each LSA now contains two bits indicating the flooding scope
  - AS scope, LSA is flooded throughout the AS
  - Area scope, LSA is flooded only within an area
  - Link-local scope, LSA is flooded only on the local link
- These changes also impact the names of the LSAs
  - Type 3 (Summary LSA) is now called the inter-area-prefix-LSA
  - Type 4 (Autonomous System Border LSA) is now called the inter-area-router-LSA
  - Other new LSAs have been added

OSPFv3 - Flooding Scope

LSA Name	LS Type code	Flooding scope	LSA Function code
Router LSA	0x2001	Area scope	1
Network LSA	0x2002	Area scope	2
Inter-Area-Prefix-LSA	0x2003	Area scope	3
Inter-Area-Router-LSA	0x2004	Area scope	4
AS-External-LSA	0x4005	AS scope	5
Group-membership-LSA	0x2006	Area scope	6
Type-7-LSA	0x2007	Area scope	7
Link-LSA	0x0008	Link-local scope	8
Intra-Area-Prefix-LSA	0x2009	Area scope	9

OSPFv3 - Link LSA

- Announces the IPv6 link local address to all the router(s) attached to the link
  - This is needed for the next hop calculation
- Announce a list of IPv6 prefixes associated with the link
  - This is used for a router attached to a LAN to announce its prefix to the DR so DR can include this IPv6 address in its intra-area-prefix-LSA
- Announce the router's options capability router to the DR
  - The DR will then perform an "OR" operation on the options received from all the attached routers
  - The final option field set in the network LSA

OSPFv3 - Link LSA

- Generated for every link that has two or more routers
- Not to be originated for virtual links
- May be suppressed

OSPFv3 - Handling Unknown LSA Types

- Each LSA now contains an “unknown LSA” bit
  - 0: Treat this LSA as a link local
  - 1: Store and flood this LSA even if you don’t understand it
- This allows the deployment of new features in the future
  - Routers that don’t understand the new feature will simply store and forward the LSA
  - Features can be deployed at edges, within a flooding domain, etc., without the need to upgrade all routers

OSPFv3 - Virtual Link Requirements

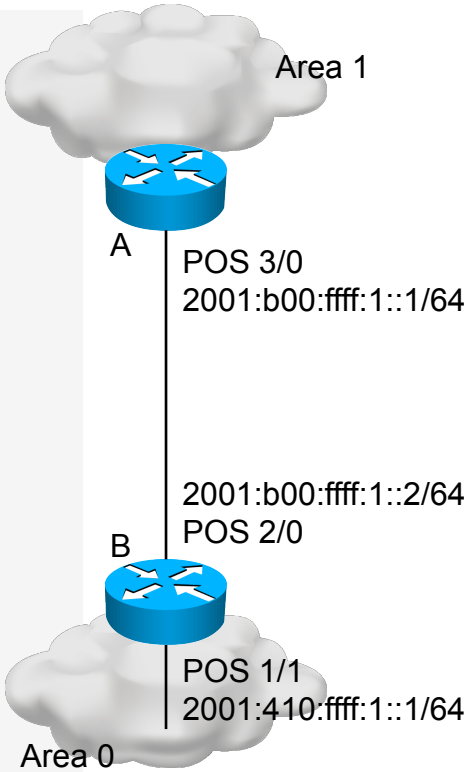
- At least one global/unique local IPv6 address in the transit area
  - OSPFv3 normally sends LSAs with a link local source address
  - This won't work over a virtual link –the packet needs to be forwarded through the intervening area
- Advertisement of a /128 prefix
  - If no /128 is available in the table, a /128 from within an existing prefix space will be used
  - This provides reachability between the endpoints of the virtual link

OSPFv3 - Authentication

- OSPFv3 currently only supports IPsec for authentication
  - Group keying is painful for IPsec
  - There is current work in GDOI and other spaces to make group keying work better for this space
- There is current work in the OSPF working group to allow HMAC-SHA and other forms of “in packet” authentication

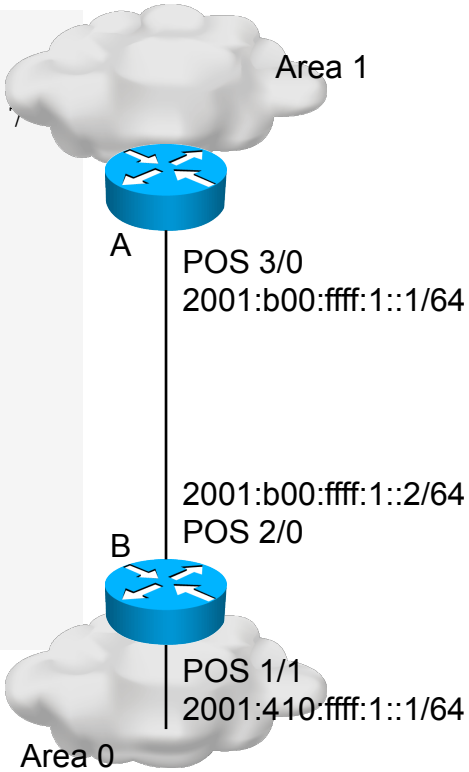
OSPFv3 - Configuration & Show Example

```
Router1#
interface POS1/1
 ipv6 address 2001:410:FFFF:1::1/64
 ipv6 enable
 ipv6 ospf 100 area 0

interface POS2/0
 ipv6 address 2001:B00:FFFF:1::2/64
 ipv6 enable
 ipv6 ospf 100 area 1

 ipv6 router ospf 100
   router-id 10.1.1.3

Router2#
interface POS3/0
 ipv6 address 2001:B00:FFFF:1::1/64
 ipv6 enable
 ipv6 ospf 100 area 1

ipv6 router ospf 100
   router-id 10.1.1.4
```



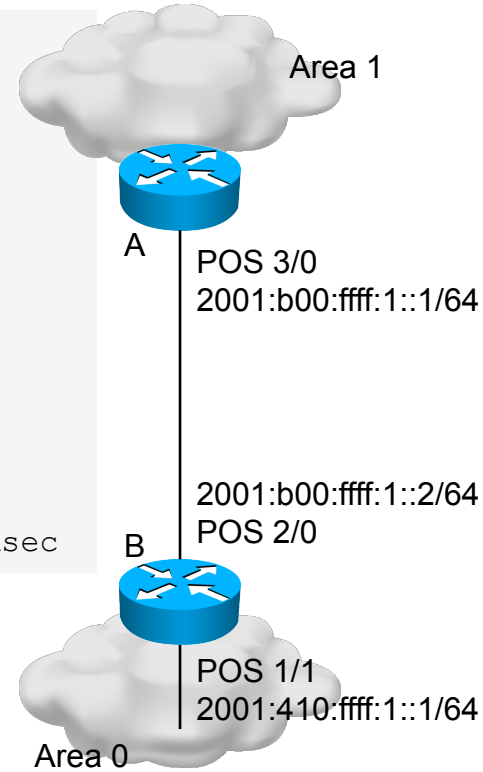
OSPFv3 - Configuration & Show Example

```
Router2#sh ipv6 ospf int pos 3/0
POS3/0 is up, line protocol is up
  Link Local Address FE80::290:86FF:FE5D:A000, Interface ID 7
  Area 1, Process ID 100, Instance ID 0, Router ID 10.1.1.4
  Network Type POINT_TO_POINT, Cost: 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
    Retransmit 5
    Hello due in 00:00:02
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 3, maximum is 3
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.1.1.3
  Suppress hello for 0 neighbor(s)
```



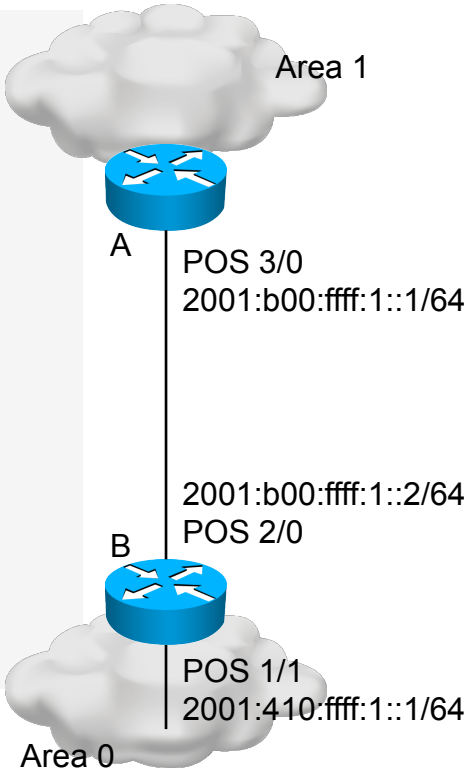
OSPFv3 - Configuration & Show Example

```
Router2#sh ipv6 ospf  neighbor detail
 Neighbor 10.1.1.3
    In the area 1 via interface POS3/0
    Neighbor: interface-id 8, link-local address
FE80::2D0:FFFF:FE60:DFFF
    Neighbor priority is 1, State is FULL, 12 state changes
    Options is 0x630C34B9
    Dead timer due in 00:00:33
    Neighbor is up for 00:49:32
    Index 1/1/1, retransmission queue length 0, number of
retransmission 1
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 2, maximum is 2
    Last retransmission scan time is 0 msec, maximum is 0 msec
```



OSPFv3 - Configuration & Show Example

```
Router2#sh ipv6 route
IPv6 Routing Table - 5 entries
Codes: C - Connected, L - Local, S - Static, R - RIP,
       B - BGP, U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1,
       OE2 - OSPF ext 2
OI  2001:410:FFFF:1::/64 [110/2]
     via FE80::2D0:FFFF:FE60:DFFF, POS3/0
C   2001:B00:FFFF:1::/64 [0/0]
     via ::, POS3/0
L   2001:B00:FFFF:1::1/128 [0/0]
     via ::, POS3/0
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
```



OSPFv3 - Routing Considerations

- New Routing Protocol
  - New training, show commands, troubleshooting procedures
  - Must run “dual stack” in the control plane
- Consider design carefully
  - Be intentional about flooding domain boundaries
  - Don’t just deploy “one big area” because you can, it’s simple, it’s a test, etc…
  - Probably best to place ABRs in the same places just to facilitate management and troubleshooting
- IPv6 rollout must be contiguous
  - Just like with the other IGPs…

IS-IS/IPv6 - Protocol Changes

- Two tag/length/values added to introduce IPv6 routing
- IPv6 reachability TLV (0xEC)

  Describes network reachability such as IPv6 routing prefix, metric information and some option bits. The option bits indicates the advertisement of IPv6 prefix from a higher level, redistribution from other routing protocols.

  Equivalent to IP Internal/external reachability TLVs described in RFC1195
- IPv6 interface address TLV (0xE8)

  Contains 128-bit address

  For Hello PDUs, must contain the link-local address (FE80::/10)

  For LSP, must only contain the non link-local address
- A new Network Layer Protocol Identifier (NLPID) is defined

  Allowing IS-IS routers with IPv6 support to advertise IPv6 prefix payload using 0x8E value (IPv4 and OSI uses different values)

IS-IS/IPv6 – Single versus Multi-Topology

- IS-IS supports IPv6 in two ways
- Single Topology
  - The IPv4 and IPv6 topologies must match
  - One SPF is run; IPv4 and IPv6 are mixed on the resulting SPT
- Multi-topology
  - Uses a different address family for IPv6 destinations
  - IPv4 and IPv6 topologies do not need to match

IS-IS/IPv6 - Single Topology

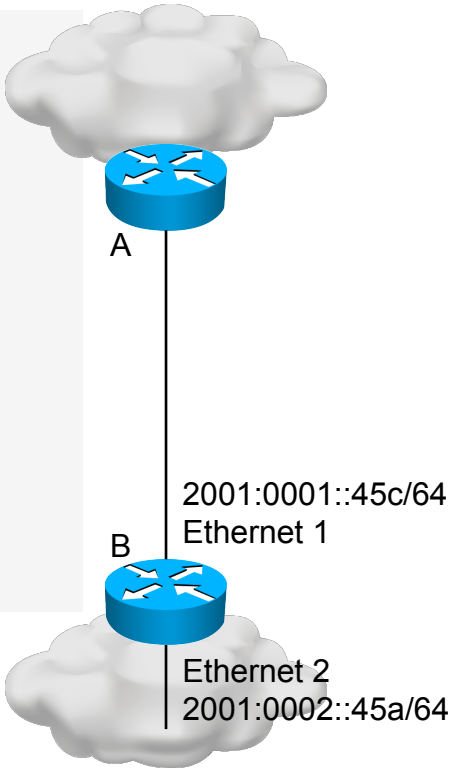
- Uses the same SPF for both IPv4 and IPv6
  - Not really suitable for overlaying pockets of IPv6 on an existing IPv4 network
  - If using both IPv4 and IPv6, topologies must match
  - Cannot run IPv4 on some interfaces, IPv6 on others
- Adjacencies on Level 1 interfaces only form when configuration is matched
- Cannot join two IPv6 areas via an IPv4-only area
  - L2 adjacencies will form OK but IPv6 traffic will black-hole in the IPv4 area.

IS-IS/IPv6 - Multi-Topology

- IPv4 and IPv6 have their own databases
- SPF is run for each topology
  - Once for IPv4, once for IPv6
- Cannot connect “islands” of IPv6 together
  - The problem here is the forwarding plane, not the control plane
  - Not really suitable for overlaying pockets of IPv6 on an existing IPv4 network
- Allows flooding domain boundaries to be in different places
- More complex to configure and maintain

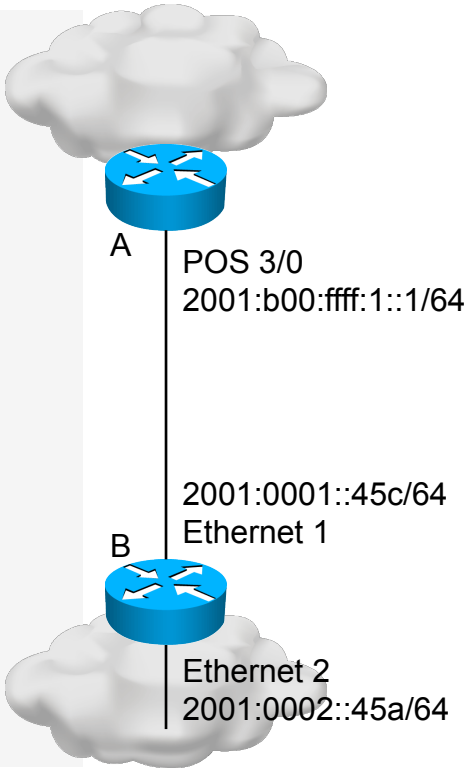
IS-IS/IPv6 - Configuration & Show Example

```
Router-B#
 interface ethernet-1
     ipv6 address 2001:0001::45c/64
     ipv6 router isis
     isis circuit-type level-2-only

  interface ethernet-2
     ipv6 address 2001:0002::45a/64
     ipv6 router isis

  router isis
      address-family ipv6
      redistribute static
      exit-address-family
      net 42.0001.0000.0000.072c.00
```



IS-IS/IPv6 - Configuration & Show Example

```
Router-B#
 interface ethernet-1
     ip address 10.1.1.1 255.255.255.0
     ipv6 address 2001:0001::45c/64
     ip router isis
     ipv6 router isis

  interface ethernet-2
     ip address 10.2.1.1 255.255.255.0
     ipv6 address 2001:0002::45a/64
     ip router isis
     ipv6 router isis

  router isis
      address-family ipv6
      redistribute static
      exit-address-family
      net 42.0001.0000.0000.072c.00
      redistribute static
```



Dual IPv4/IPv6 Configuration
Redistributing Both IPv6 Static Routes and IPv4 Static Routes

IS-IS/IPv6 - Configuration & Show Example

```
brum-45c#show ipv6 route is-is
IPv6 Routing Table - 14 entries
Codes: C - Connected, L - Local, S - Static, R - RIP,
       B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
Timers: Uptime/Expires

I1  2001:45A:1000::/64 [115/20]
     via FE80::210:7BFF:FEC2:ACCC, Ethernet1, 00:10:12/never
I1  2001:72B:2000::/64 [115/10]
     via FE80::210:7BFF:FEC2:ACCC, Ethernet1, 00:05:19/never
I1  2002:49::/64 [115/10]
     via FE80::210:7BFF:FEC2:ACCC, Ethernet1, 00:05:19/never
```

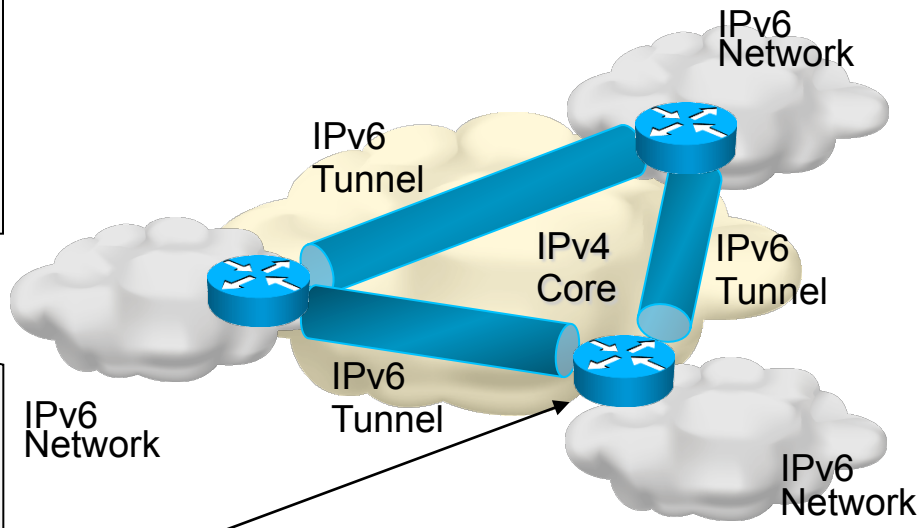
IS-IS/IPv6 - Configuration & Show Example

```
show clns is-neigh detail

System Id      Interface   State  Type Priority  Circuit Id         Format
brum-45a       Et1         Up     L1   64        brum-45c.01        Phase V
  Area Address(es): 47.0023.0001.0000.0001.0002.0001
  IPv6 Address(es): FE80::210:7BFF:FEC2:ACCC
  Uptime: 00:06:56

IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
brum-45c.00-00      * 0x00000003   0xA745        732               0/0/0
  Area Address: 47.0023.0001.0000.0001.0002.0001
  NLPID:        0x8E
  Hostname: brum-45c
  IPv6 Address: 3F02::45C
  IPv6 Address: 2001:45C:2000::45C
  Metric: 10         IPv6 2001:45C:1000::/64
  Metric: 10         IPv6 3F02::/64
  Metric: 10         IPv6 2001:45C:2000::/64
  Metric: 10         IS brum-45c.02
  Metric: 10         IS brum-45c.01
brum-45c.01-00      * 0x00000001   0x96DB        733               0/0/0
  Metric: 0          IS brum-45c.00
  Metric: 0          IS brum-45a.00
brum-45a.00-00        0x00000005   0xDDBA        1027              0/0/0
  Area Address: 47.0023.0001.0000.0001.0002.0001
  NLPID:        0x8E
  Hostname: brum-45a
  IPv6 Address: 2001:45A:1000::45A
  Metric: 10         IPv6 2001:45A:1000::/64
  Metric: 10         IS brum-45c.01
  Metric: 0          IPv6-Ext 2001:72B:2000::/64
  Metric: 0          IPv6-Ext 2002:49::/64
```

IS-IS for IPv6 on IPv6 Tunnels over IPv4

```
interface Tunnel0
 no ip address
 ipv6 address 2001:0001::45A/64
 ipv6 address FE80::10:7BC2:ACC9:10 link-local
 ipv6 router isis
 tunnel source Ethernet1
 tunnel destination 10.42.2.1
!
router isis
 passive-interface Ethernet2
 net 42.0001.0000.0000.045a.00
```

```
interface Tunnel0
 no ip address
 ipv6 address 2001:0001::45C/64
 ipv6 address FE80::10:7BC2:B280:11 link-local
 ipv6 router isis
tunnel source Ethernet2
 tunnel destination 10.42.1.1
!
router isis
 net 42.0001.0000.0000.045c.00
```



IS-IS for IPv6 on an IPv6 tunnel requires GRE tunnel, it can't work with IPv6 configured tunnel as IS-IS runs directly over the data link layer

IPv6 Routing

Summary

- EIGRP
  - Single protocol
  - Multiple instances
  - IPv6 domains must be contiguous within the deployment
  - Aggregation/failure domains may not coincide
- OSPF
  - New protocol (OSPFv3)
  - Lots of changes and capabilities
  - IPv6 domains must be contiguous within the deployment
  - Aggregation/failure domains may not coincide

IPv6 Routing

Summary

- IS-IS/IPv6 Single Topology
  - Single protocol
  - Multiple TLVs within the single protocol
  - Topologies must be congruent
  - IPv6 domains must be contiguous within the deployment
- IS-IS/IPv6 Multi-Topology
  - Single Protocol
  - Since instance, multiple address families
  - Aggregation/failure domains may not coincide
  - IPv6 domains must be contiguous within the deployment

Agenda

- Introduction
- IPv6 in the Enterprise
- Routing Considerations
- Security for IPv6
- First Hop Security
- Unified Communications
- Multicast
- DNS
- Deployment and Operation Considerations

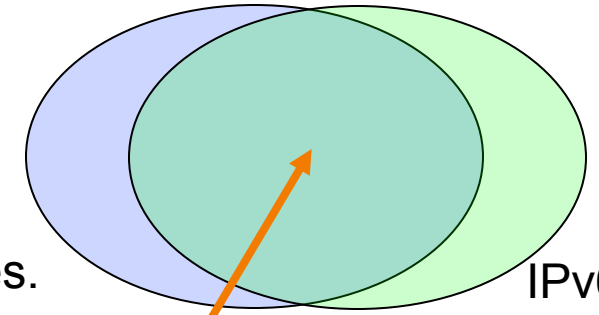
IPv6 – Security

Session Objectives

- IPv6 vs. to IPv4 from a threat and mitigation perspective
- Advanced IPv6 security topics like transition options and dual stack environments
- Requirements: basic knowledge of the IPv6 and IPSec protocols as well as IPv4 security best practices
- The BRKSEC-2003 IPv6 Security Threats & Mitigation is more detailed version of this part

IPv6 Security - Agenda

- Issues shared by IPv4 and IPv6
- Issues specific to IPv6
  - IPsec everywhere, dual-stack, tunnels and 6VPE
- Enforcing a Security Policy in IPv6
  - ACL, Firewalls and IPS
- Enterprise Secure Deployment
  - Secure IPv6 transport over public network
- IPv6 Security “Best Common Practice”



IPv4 Vulnerabilities.

IPv6 Vulnerabilities.

Shared Issues

Security Issues Shared by IPv4 and IPv6

Reconnaissance in IPv6
Subnet Size Difference

- Default subnets in IPv6 have 2^{64} addresses

  10 Mpps = more than 50 000 years

- NMAP doesn't even support ping sweeps on IPv6 networks

Reconnaissance in IPv6
Scanning Methods Are Likely to Change

- Public servers will still need to be DNS reachable

  ⇒More information collected by Google...

- Increased deployment/reliance on dynamic DNS

  ⇒More information will be in DNS

- Using peer-to-peer clients gives IPv6 addresses of peers
- Administrators may adopt easy-to-remember addresses (:: 10,::20,::F00D, ::C5C0 or simply IPv4 last octet for dual stack)
- By compromising hosts in a network, an attacker can learn new addresses to scan
- Transition techniques (see further) derive IPv6 address from IPv4 address

  ⇒ can scan again

Scanning Made Bad for CPU

- Potential router CPU attacks if aggressive scanning
  - Router will do Neighbor Discovery... And waste CPU and memory
  - Built-in rate limiter but no option to tune it
- Using a /64 on point-to-point links => a lot of addresses to scan!
- Using infrastructure ACL prevents this scanning
  - iACL: edge ACL denying packets addressed to your routers
  - Easy with IPv6 because new addressing scheme can be done ☺

Viruses and Worms in IPv6

- Viruses and email, IM worms: IPv6 brings no change
- Other worms:

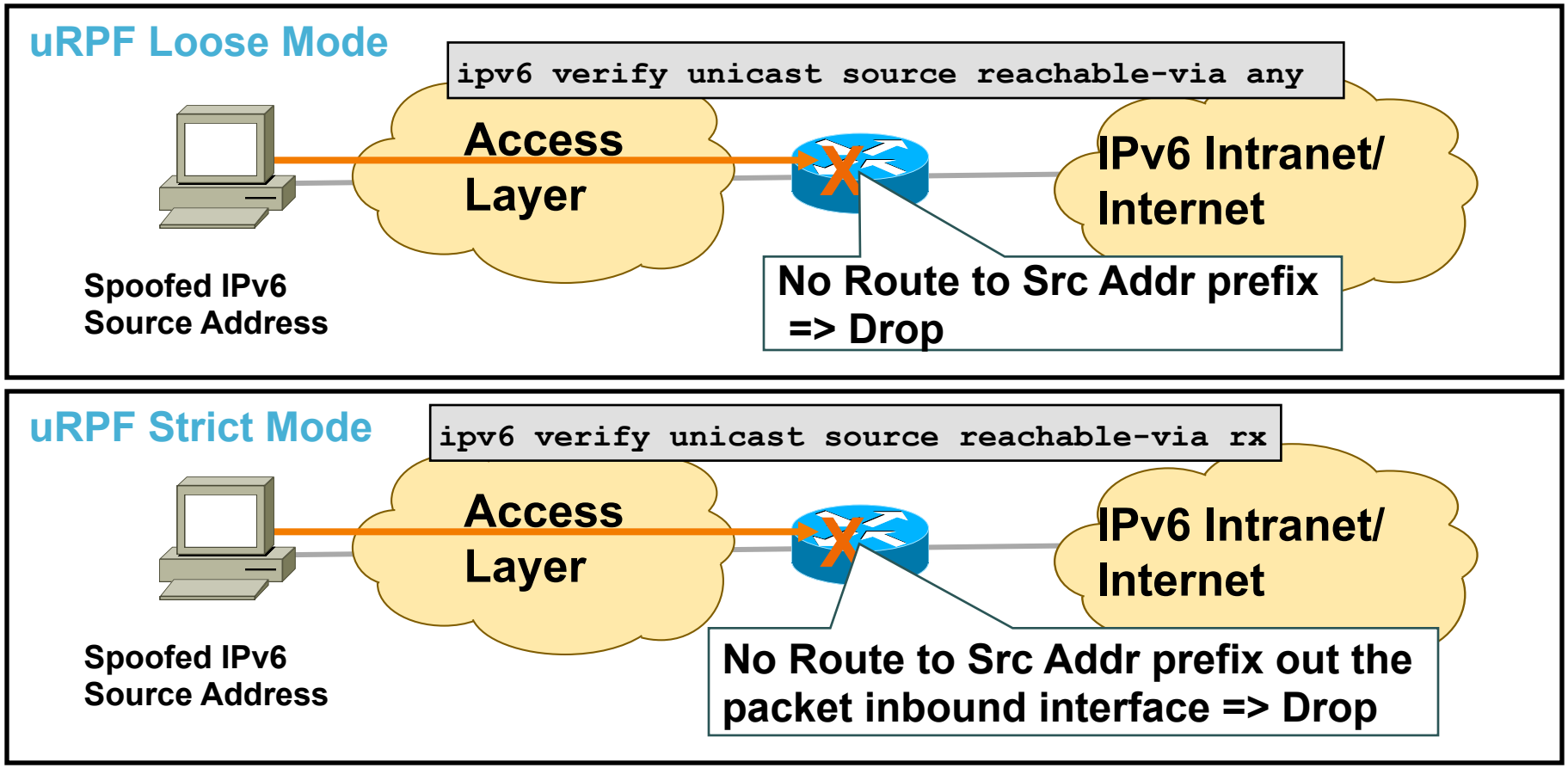
  IPv4: reliance on network scanning

  IPv6: not so easy (see reconnaissance) => will use alternative techniques

- Worm developers will adapt to IPv6
- IPv4 best practices around worm detection and mitigation remain valid

L3 Spoofing in IPv6

uRPF Remains the Primary Tool for Protecting Against L3 Spoofing



IP Source Guard does not exist yet (see further slides)

IPv6 uRPF and Cisco Devices The Theory-Practice Gap

- Supported everywhere except:
  - 7600 & Cat 6K: no IPv6 uRPF at all
    - AFAIK: will require next Supervisor...
  - Cat 3750: no uRPF at all
  - GSR only strict mode with E5 (else not supported) in 12.0 (31)S
  - ASR 9K (software limitation)

Preventing Routing Header Attacks

- Apply same policy for IPv6 as for Ipv4:
  - Block Routing Header type 0
- Prevent processing at the intermediate nodes
  - no ipv6 source-route
  - Windows, Linux, Mac OS: default setting
- At the edge
  - With an ACL blocking routing header
- RFC 5095 (Dec 2007) RH0 is deprecated
  - Default IOS changed in 12.4(15)T to ignore and drop RH0

ARP Spoofing is now NDP Spoofing: Threats

- ARP is replaced by Neighbor Discovery Protocol
  - Nothing authenticated
  - Static entries overwritten by dynamic ones
- Stateless Address Autoconfiguration
  - rogue RA (malicious or not)
  - All nodes badly configured
    - DoS
    - Traffic interception (Man In the Middle Attack)
- Attack tools exist (from THC – The Hacker Choice)
  - Parasit6
  - Fakerouter6
  - ...

The Hacker's Choice

ICMPv4 vs. ICMPv6

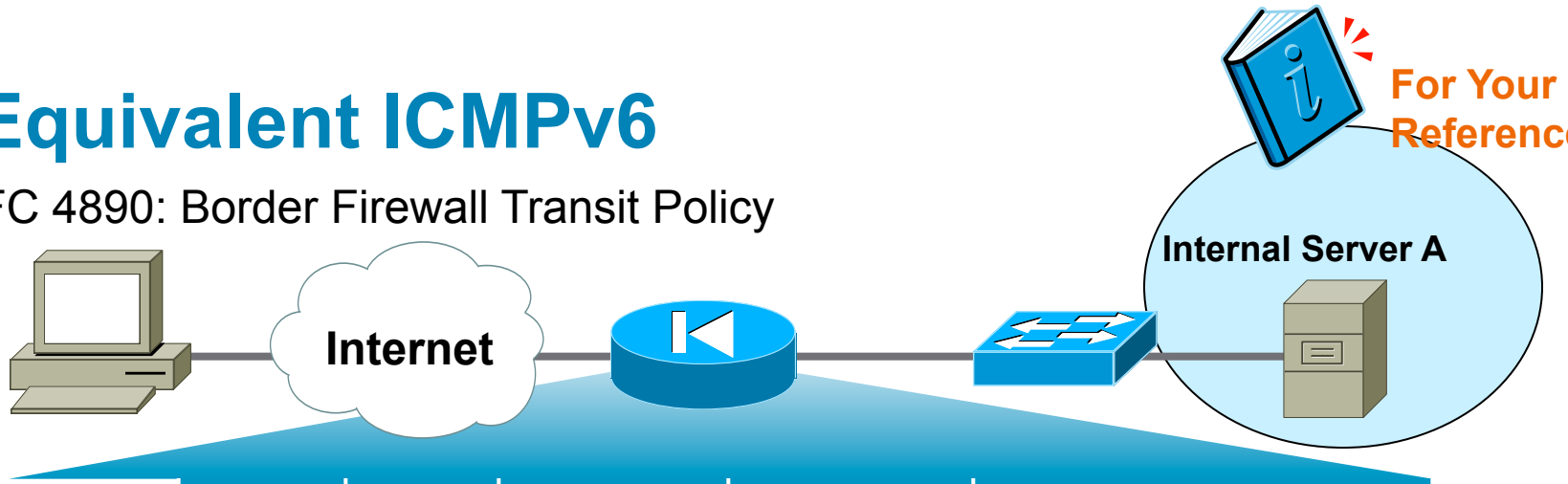
- Significant changes
- More relied upon

ICMP Message Type	ICMPv4	ICMPv6
Connectivity Checks	X	X
Informational/Error Messaging	X	X
Fragmentation Needed Notification	X	X
Address Assignment		X
Address Resolution		X
Router Discovery		X
Multicast Group Management		X
Mobile IPv6 Support		X

- => ICMP policy on firewalls needs to change

Equivalent ICMPv6

RFC 4890: Border Firewall Transit Policy

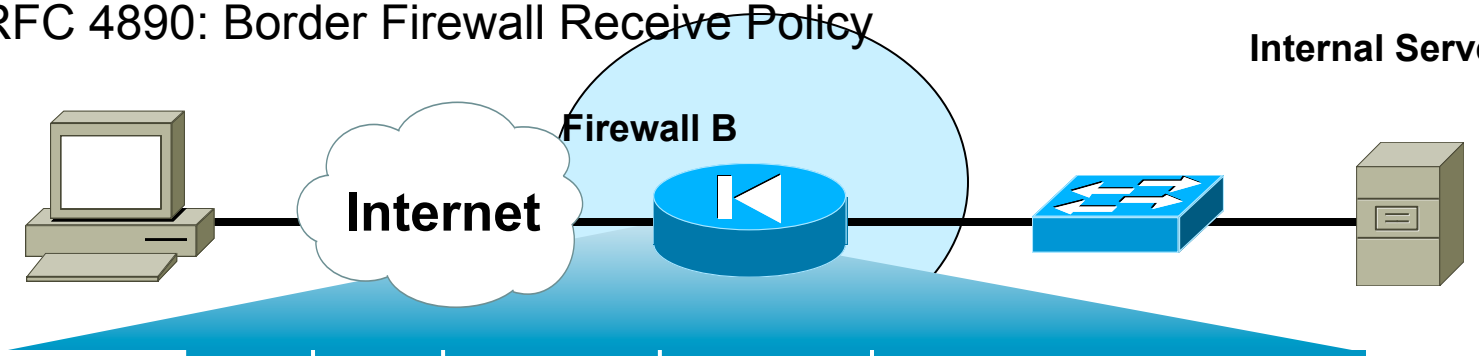


Action	Src	Dst	ICMPv6 Type	ICMPv6 Code	Name
Permit	Any	A	128	0	Echo Reply
Permit	Any	A	129	0	Echo Request
Permit	Any	A	1	0	No Route to Dst.
Permit	Any	A	2	0	Packet Too Big
Permit	Any	A	3	0	Time Exceeded—TTL Exceeded
Permit	Any	A	4	0	Parameter Problem

Potential Additional ICMPv6

For Your Reference

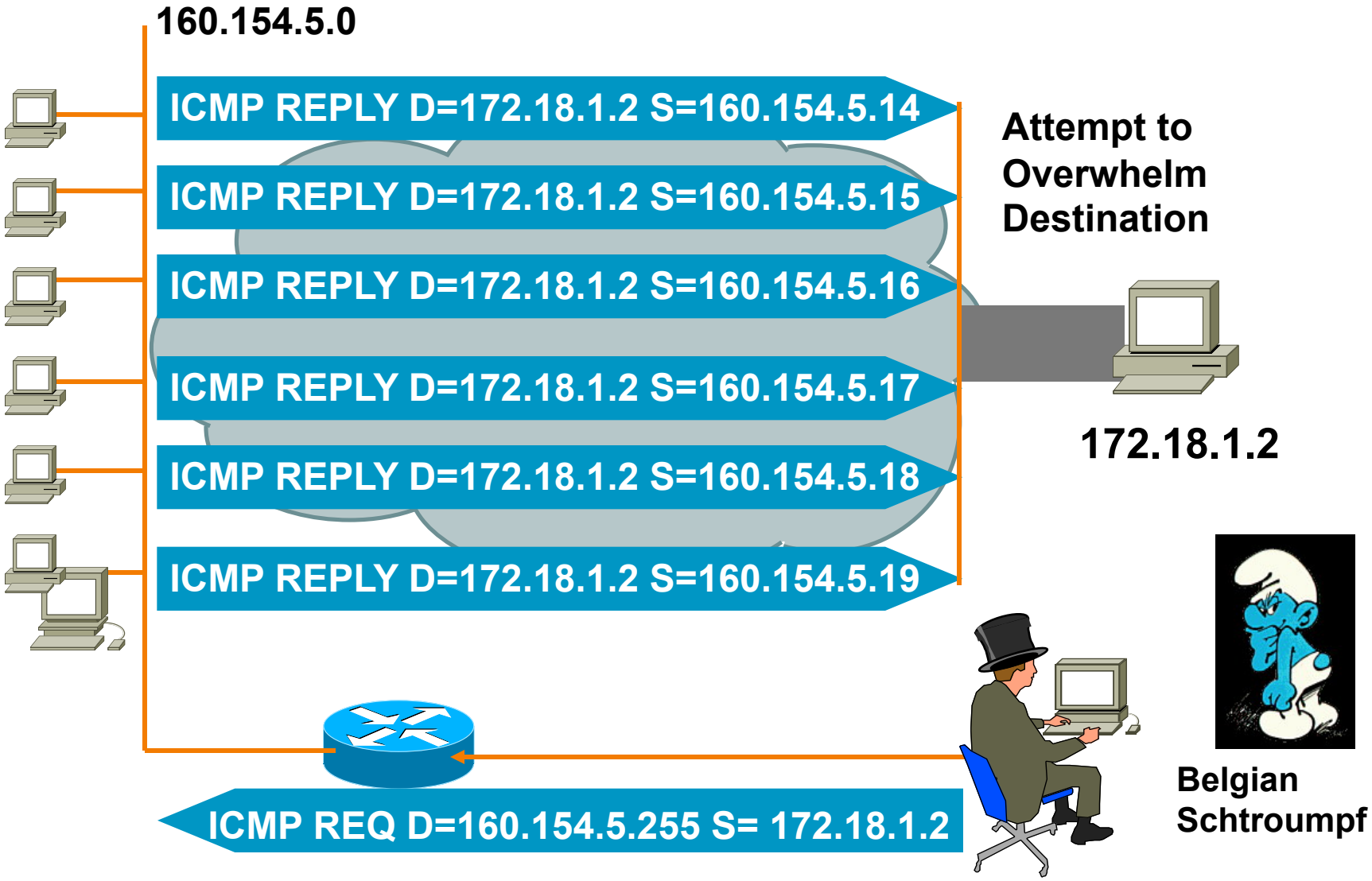
RFC 4890: Border Firewall Receive Policy



Action	Src	Dst	ICMPv6 Type	ICMPv6 Code	Name
Permit	Any	B	2	0	Packet too Big
Permit	Any	B	4	0	Parameter Problem
Permit	Any	B	130–132	0	Multicast Listener
Permit	Any	B	133/134	0	Neighbor Solicitation and Advertisement
Deny	Any	Any			

For locally generated traffic

Quick Reminder
IPv4 Broadcast Amplification: Smurf



IPv6 and Broadcasts

- There are no broadcast addresses in IPv6
- Broadcast address functionality is replaced with appropriate link local multicast addresses
  - Link Local All Nodes Multicast—FF02::1
  - Link Local All Routers Multicast—FF02::2
  - Link Local All mDNS Multicast—FF02::FB

Note: anti-spoofing also blocks amplification attacks because a remote attacker cannot masquerade as his victim

http://iana.org/assignments/ipv6-multicast-addresses/

IPv6 and Other Amplification Vectors

- IOS implements correctly RFC 4443 ICMPv6

  No ping-pong on a physical point-to-point link *Section 3.1*

  No ICMP error message should be generated in response to a packet with a multicast destination address *Section 2.4 (e.3)*

  Exceptions for *Section 2.4 (e.3)*

  – packet too big message

  – the parameter problem message

•Rate Limit egress ICMP Packets

•Rate limit ICMP messages generation

•Secure the multicast network (source specific multicast)

•Note: Implement Ingress Filtering of Packets with IPv6 Multicast Source Addresses

Preventing IPv6 Routing Attacks Protocol Authentication

- BGP, ISIS, EIGRP no change:

  An MD5 authentication of the routing update

- OSPFv3 has changed and pulled MD5 authentication from the protocol and instead is supposed to rely on transport mode IPSec
- RIPng, PIM also rely on IPSec
- IPv6 routing attack best practices

  Use traditional authentication mechanisms on BGP and IS-IS

  Use IPSec to secure protocols such as OSPFv3 and RIPng

OSPF or EIGRP Authentication

For Your Reference

```
interface Ethernet0/0
 ipv6 ospf 1 area 0
 ipv6 ospf authentication ipsec spi 500 md5
  1234567890ABCDEF1234567890ABCDEF
```

```
interface Ethernet0/0
 ipv6 authentication mode eigrp 100 md5
 ipv6 authentication key-chain eigrp 100 MYCHAIN

key chain MYCHAIN
 key 1
key-string 1234567890ABCDEF1234567890ABCDEF
accept-lifetime local 12:00:00 Dec 31 2006
  12:00:00 Jan 1 2008
send-lifetime local 00:00:00 Jan 1 2007 23:59:59
  Dec 31 2007
```

IPv6 Attacks with Strong IPv4 Similarities

- Sniffing

  IPv6 is no more or less likely to fall victim to a sniffing attack than IPv4

- Application layer attacks

  The majority of vulnerabilities on the Internet today are at the application layer, something that IPSec will do nothing to prevent

- Rogue devices

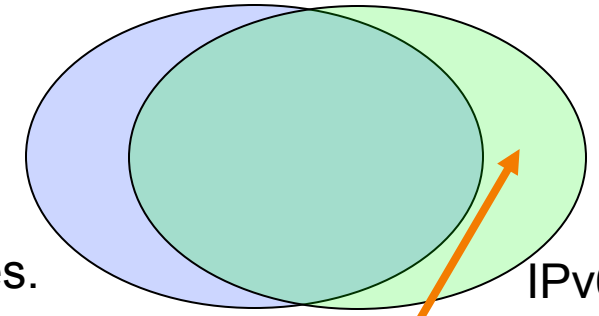
  Rogue devices will be as easy to insert into an IPv6 network as in IPv4

- Man-in-the-Middle Attacks (MITM)

  Without strong mutual authentication, any attacks utilizing MITM will have the same likelihood in IPv6 as in IPv4

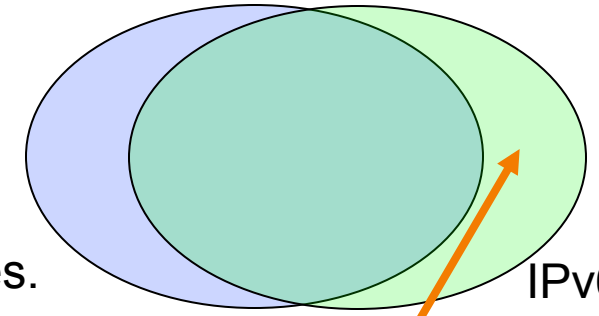
- Flooding

  Flooding attacks are identical between IPv4 and IPv6



Specific IPv6 Issues

Issues Applicable only to IPv6

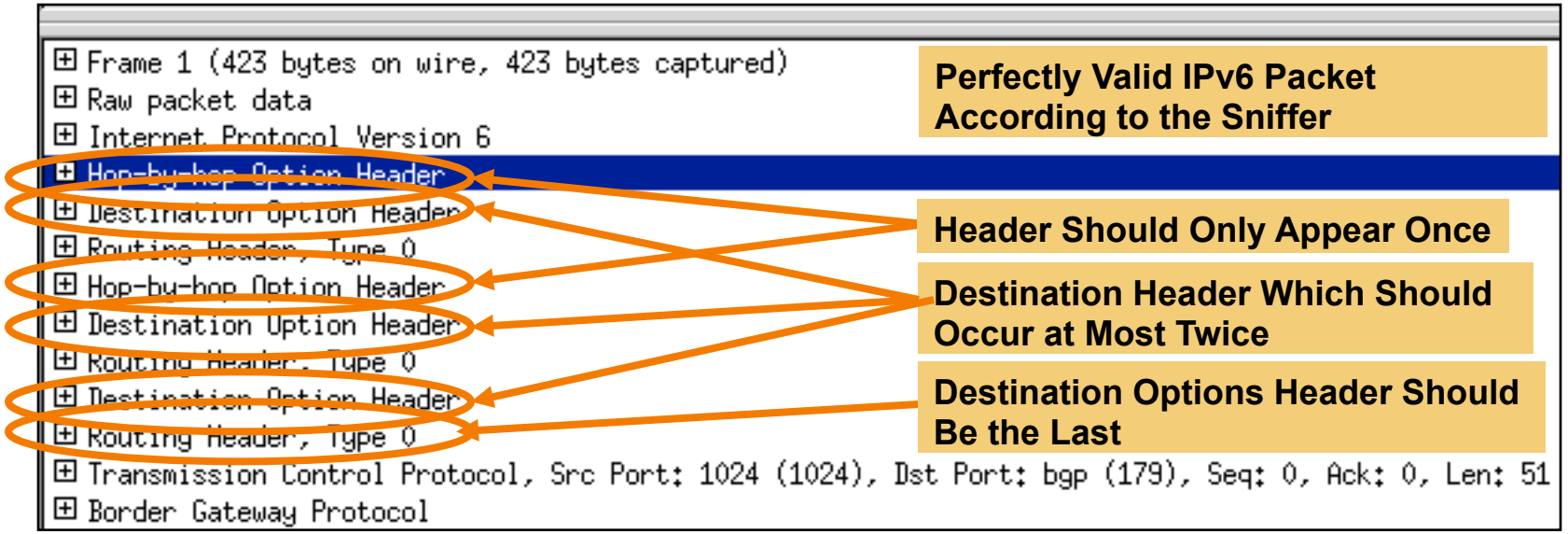


Specific IPv6 Issues

Issues Applicable only to IPv6

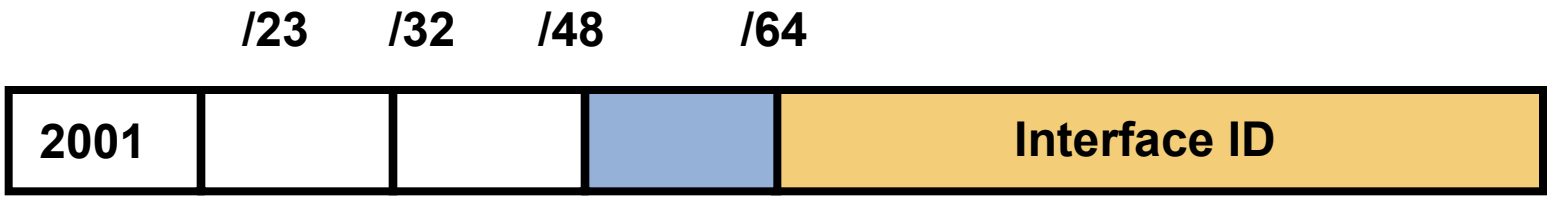
IPv6 Header Manipulation

- Unlimited size of header chain (spec-wise) can make filtering difficult
- Potential DoS with poor IPv6 stack implementations
  - More boundary conditions to exploit
  - Can I overrun buffers with a lot of extension headers?



See also: http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html

IPv6 Privacy Extensions (RFC 3041)

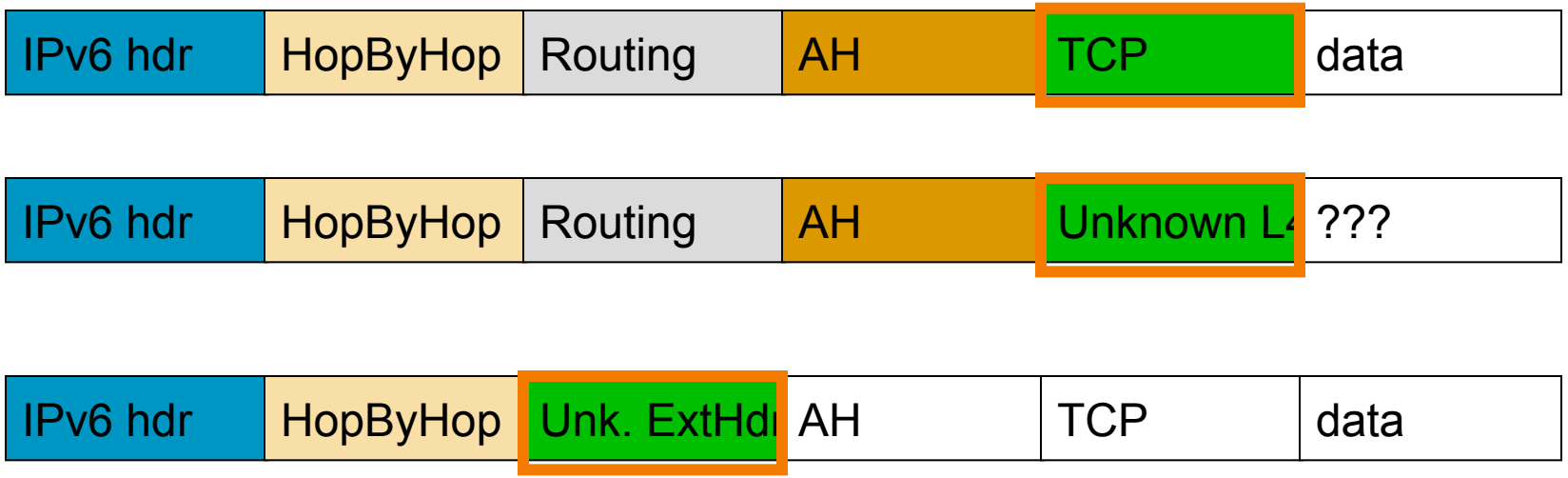


- Temporary addresses for IPv6 host client application, e.g. web browser
  - Inhibit device/user tracking
  - Random 64 bit interface ID, then run Duplicate Address Detection before using it
  - Rate of change based on local policy

Recommendation: Use Privacy Extensions for External Communication but not for Internal Networks (Troubleshooting and Attack Trace Back)

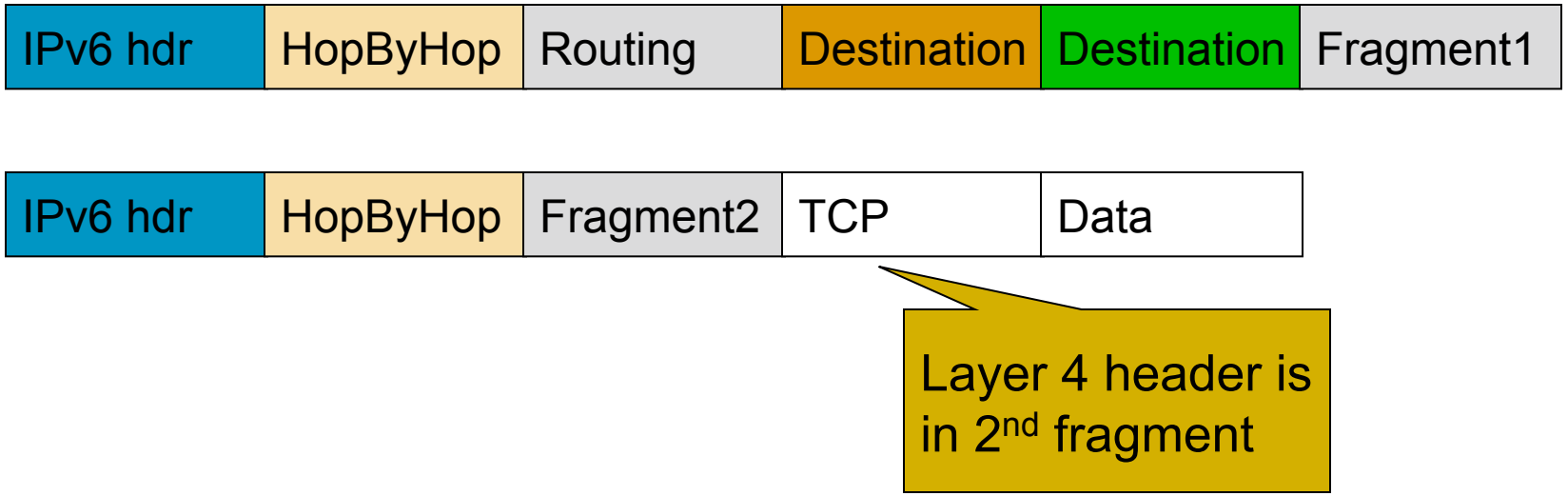
Parsing the Extension Header Chain

- Finding the layer 4 information is not trivial in IPv6
  - Skip all known extension header
  - Until either known layer 4 header found =>**SUCCESS**
  - Or unknown extension header/layer 4 header found... =>**FAILURE**



Parsing the Extension Header Chain Fragmentation Matters!

- Extension headers chain can be so large that it is fragmented!
- Finding the layer 4 information is not trivial in IPv6
  - Skip all known extension header
  - Until either known layer 4 header found =>**SUCCESS**
  - Or unknown extension header/layer 4 header found... =>**FAILURE**
  - Or end of extension header => **FAILURE**



IPv6 Fragmentation & IOS ACL Fragment Keyword

- This makes matching against the first fragment non-deterministic:
  - layer 4 header might not be there but in a later fragment
  - ⇒Need for stateful inspection
- `fragment` keyword matches
  - Non-initial fragments (same as IPv4)
  - And the first fragment if the L4 protocol cannot be determined
- `Undetermined-transport` keyword matches
  - Only for deny ACE
  - first fragment if the L4 protocol cannot be determined

The IPsec Myth: IPsec End-to-End will Save the World

- IPv6 mandates the implementation of IPsec
- IPv6 does not require the use of IPsec
- Some organizations believe that IPsec should be used to secure all flows...
  - Interesting **scalability** issue (n^2 issue with IPsec)
  - Need to **trust endpoints and end-users** because the network cannot secure the traffic: no IPS, no ACL, no firewall
    - IOS 12.4(20)T can parse the AH
  - Network **telemetry is blinded**: NetFlow of little use
  - Network **services hindered**: what about QoS?

Recommendation: do not use IPsec end to end within an administrative domain.
Suggestion: Reserve IPsec for residential or hostile environment or high profile targets.

IPv4 to IPv6 Transition Challenges

- 16+ methods, possibly in combination
- Dual stack
  - Consider security for both protocols
  - Cross v4/v6 abuse
  - Resiliency (shared resources)
- Tunnels
  - Bypass firewalls (protocol 41 or UDP)
  - Can cause asymmetric traffic (hence breaking stateful firewalls)

Dual Stack Host Considerations

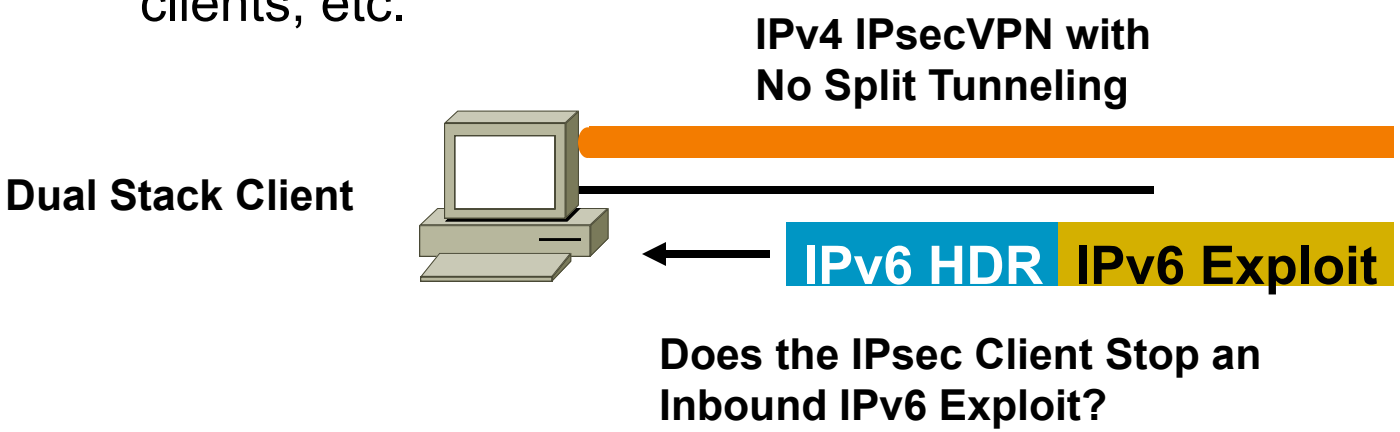
- Host security on a dual-stack device

  Applications can be subject to attack on both IPv6 and IPv4

  Fate sharing: as secure as the least secure stack...

- Host security controls should block and inspect traffic from both IP versions

  Host intrusion prevention, personal firewalls, VPN clients, etc.

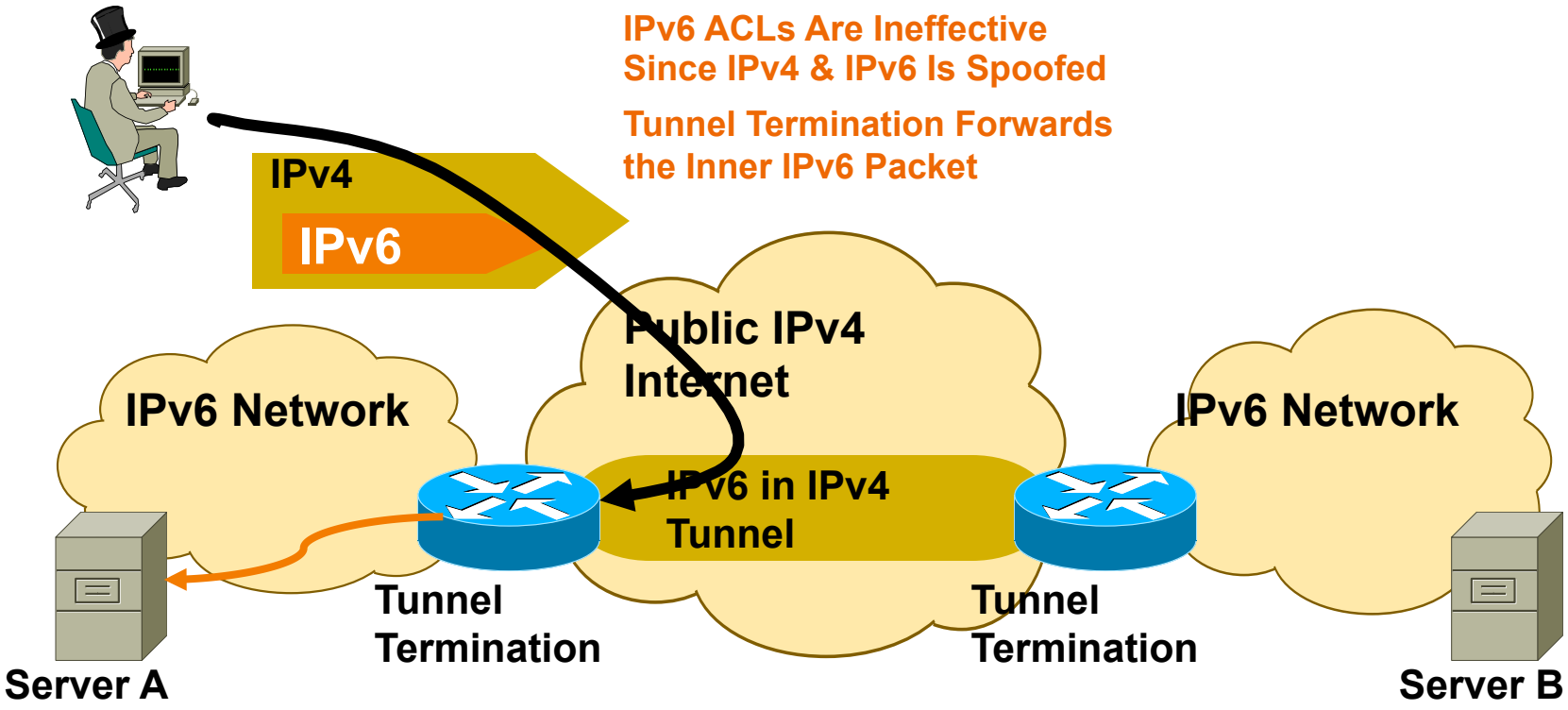


Dual Stack with Enabled IPv6 by Default

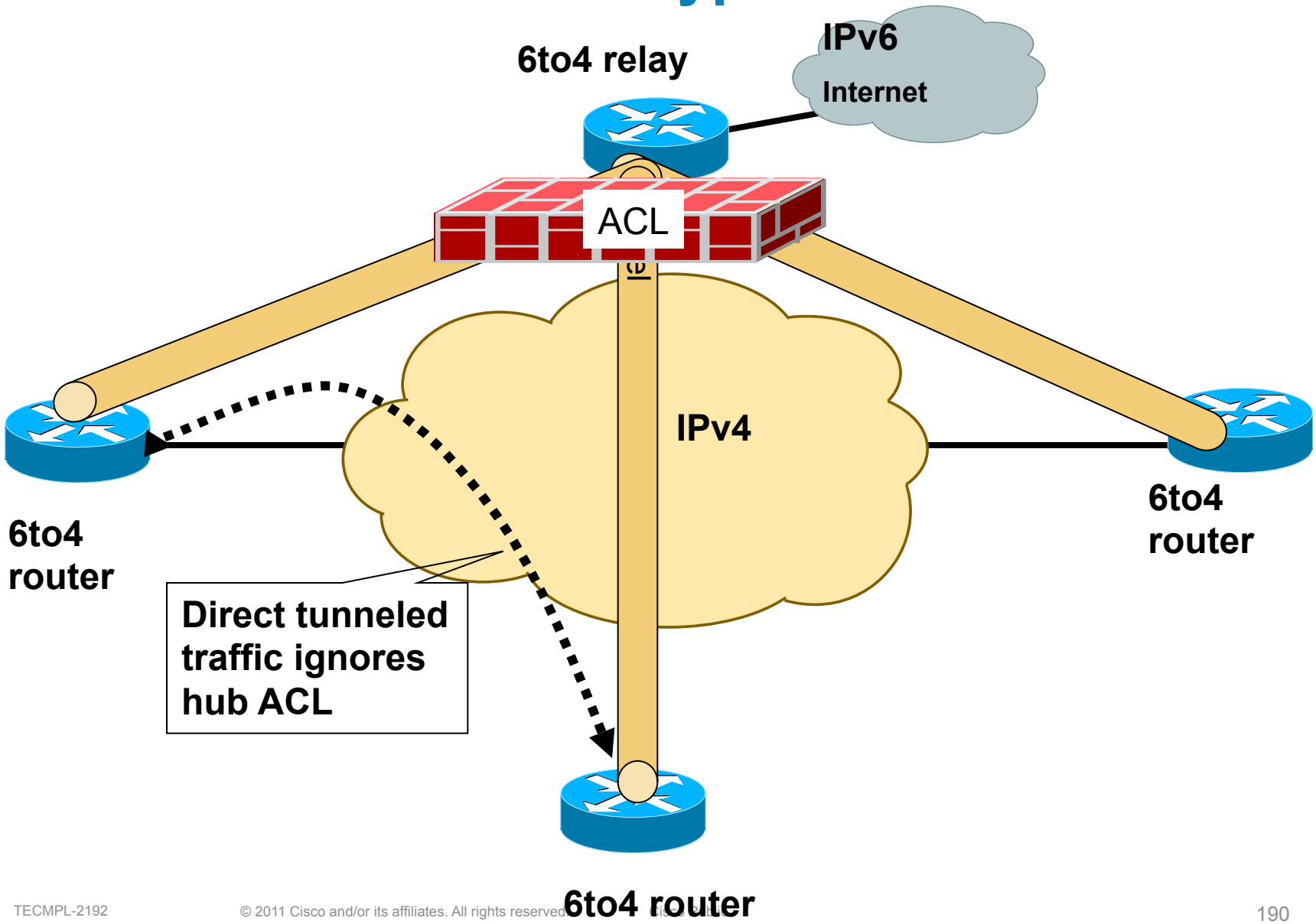
- Your host:
  - IPv4 is protected by your favorite personal firewall...
  - IPv6 is enabled by default (Vista, Linux, Mac OS/X, ...)
- Your network:
  - Does not run IPv6
- Your assumption:
  - I'm safe
- Reality
  - You are **not** safe
  - Attacker sends Router Advertisements
  - Your host silently configures to IPv6
  - You are now under IPv6 attack
- => Probably time to think about IPv6 in your network

L3-L4 Spoofing in IPv6 When Using IPv6 over IPv4 Tunnels

- Most IPv4/IPv6 transition mechanisms have no authentication built in
- => an IPv4 attacker can inject traffic if spoofing on IPv4 and IPv6 addresses



ISATAP/6to4 Tunnels Bypass ACL



Looping Attack Between 2 ISATAP routers

1. Spoofed IPv6 packet
S: 2001:db8:2::200:5efe:c000:201
D: 2001:db8:1::200:5efe:c000:202

ISATAP router 1
Prefix 2001:db8:1::/64
192.0.2.1

ISATAP router 2
Prefix 2001:db8:2::/64
192.0.2.2

2. IPv4 ISATAP packet containing
S: 2001:db8:2::200:5efe:c000:201
D: 2001:db8:1::200:5efe:c000:202

3 IPv6 packet
S: 2001:db8:2::200:5efe:c000:201
D: 2001:db8:1::200:5efe:c000:202

Repeat until Hop Limit == 0

- Root cause
  - ISATAP routers ignore each other
- ISATAP router:
  - accepts native IPv6 packets
  - forwards it inside its ISATAP tunnel
  - Other ISATAP router decaps and forward as native IPv6

Mitigation:
- IPv6 anti-spoofing everywhere
- ACL on ISATAP routers accepting IPv4 from valid clients only
- Within an enterprise, block IPv4 ISATAP traffic between ISATAP routers
- Within an enterprise block IPv6 packets between ISATAP routers

http://www.usenix.org/events/woot09/tech/full_papers/nakibly.pdf

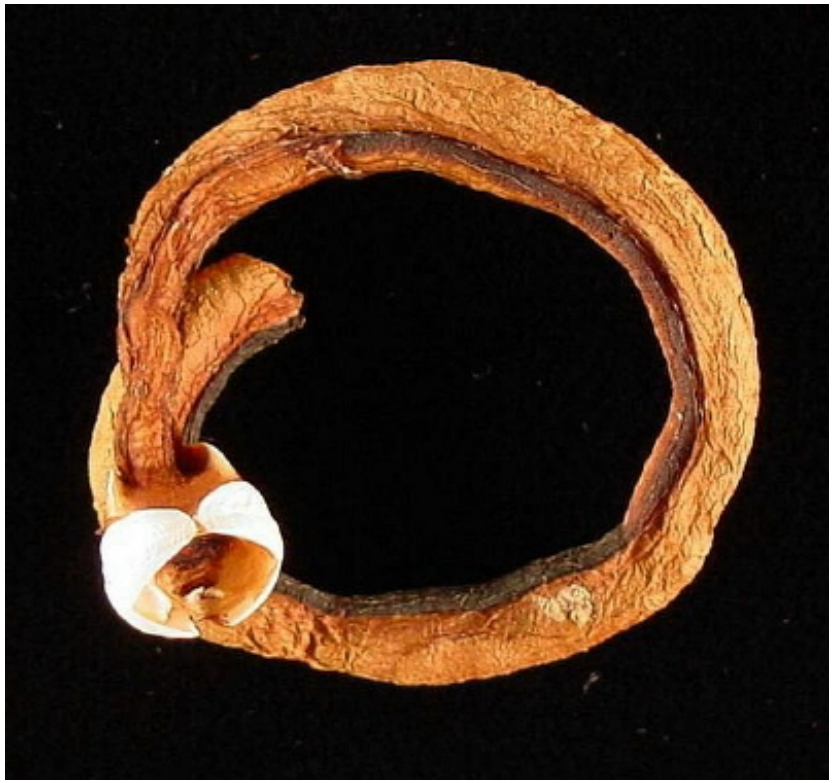
TEREDO?

- Teredo navalis

  A shipworm drilling holes in boat hulls

- Teredo Microsoftis

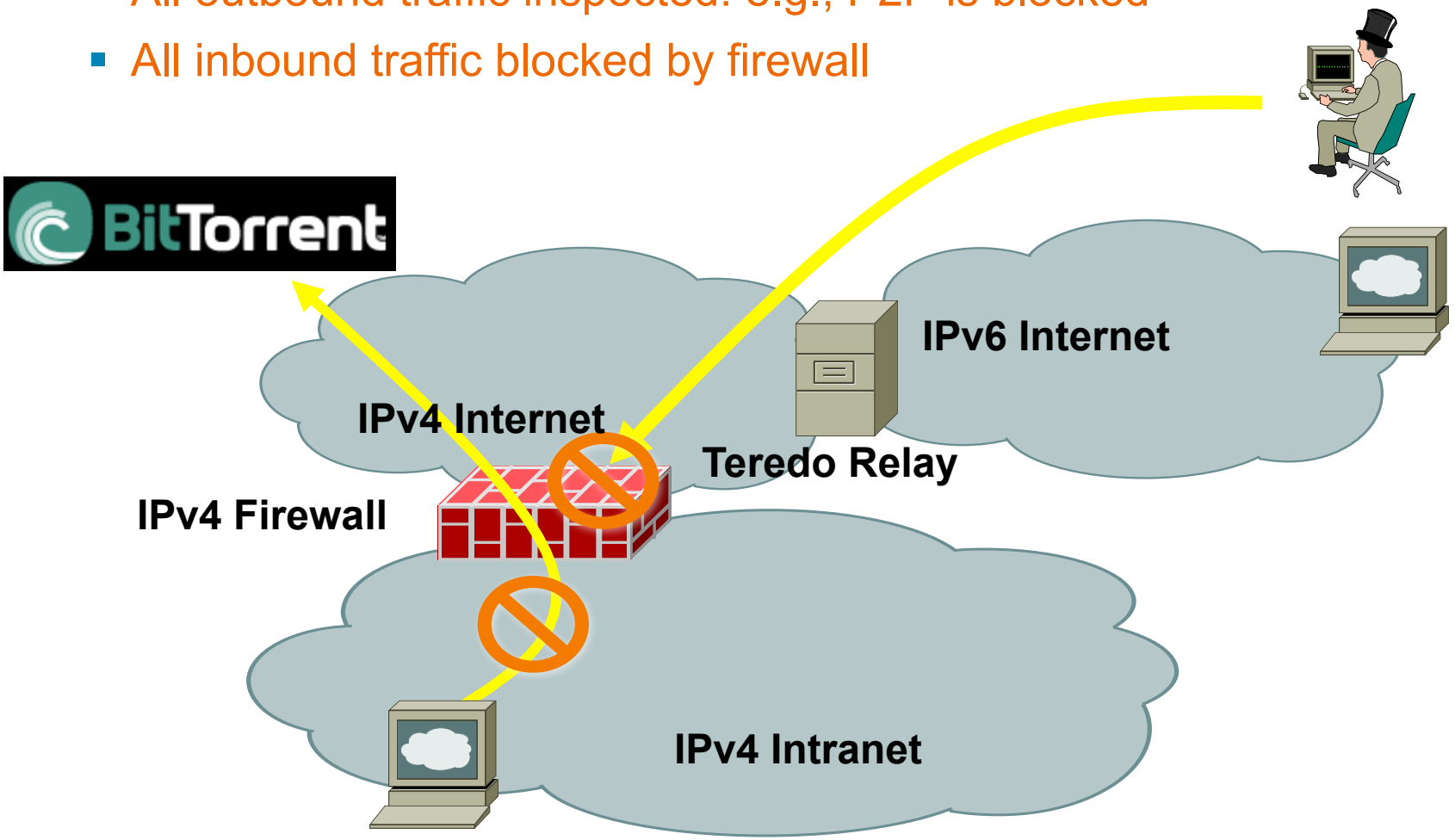
  IPv6 in IPv4 punching holes in NAT devices



Source: United States Geological Survey

Teredo Tunnels (1/3)
Without Teredo: Controls Are in Place

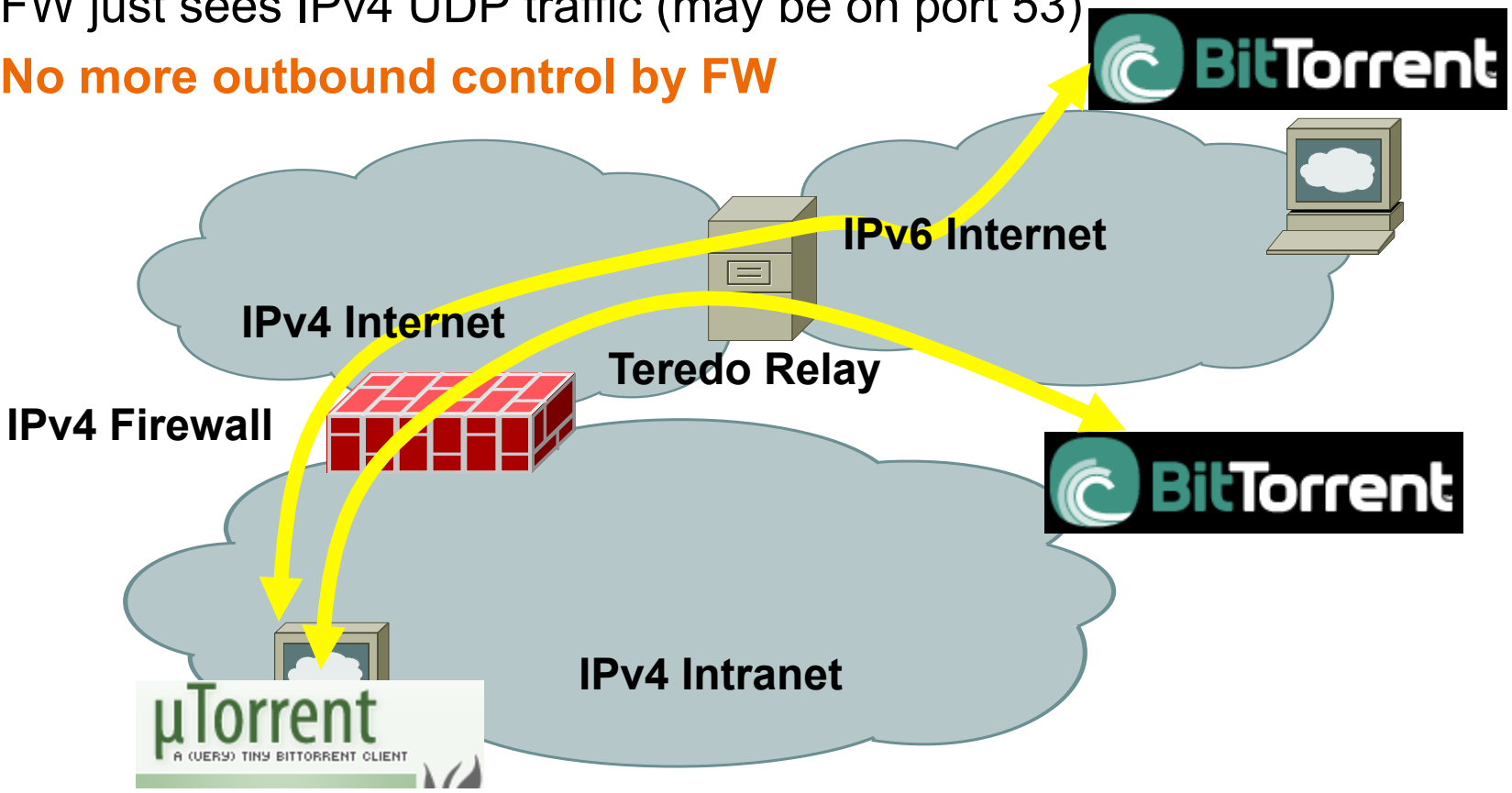
- All outbound traffic inspected: e.g., P2P is blocked
- All inbound traffic blocked by firewall



Teredo Tunnels (2/3)
No More Outbound Control

Teredo threats—IPv6 over UDP (port 3544)

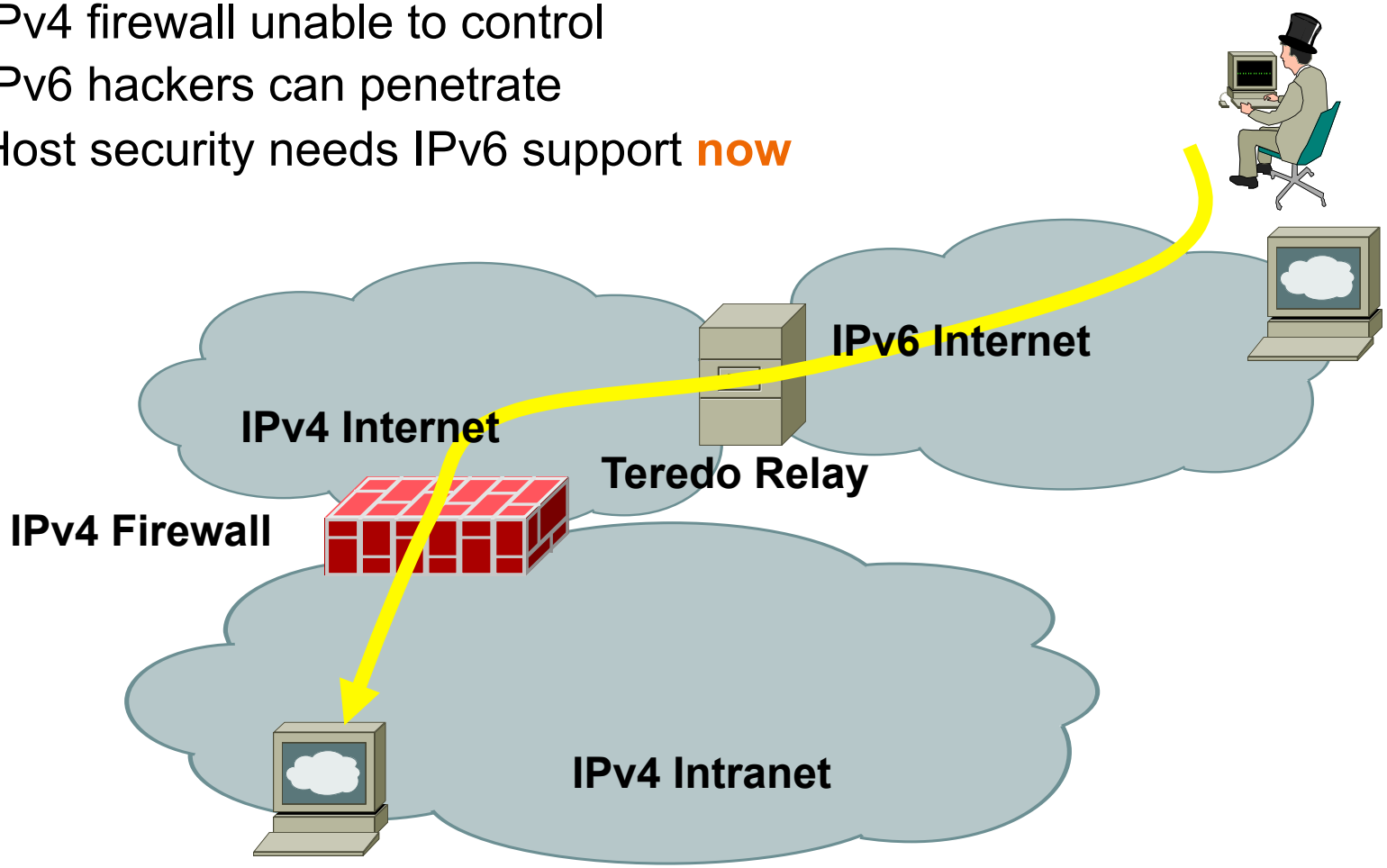
- Internal users wants to get P2P over IPv6
- Configure the Teredo tunnel (already enabled by default!)
- FW just sees IPv4 UDP traffic (may be on port 53)
- **No more outbound control by FW**



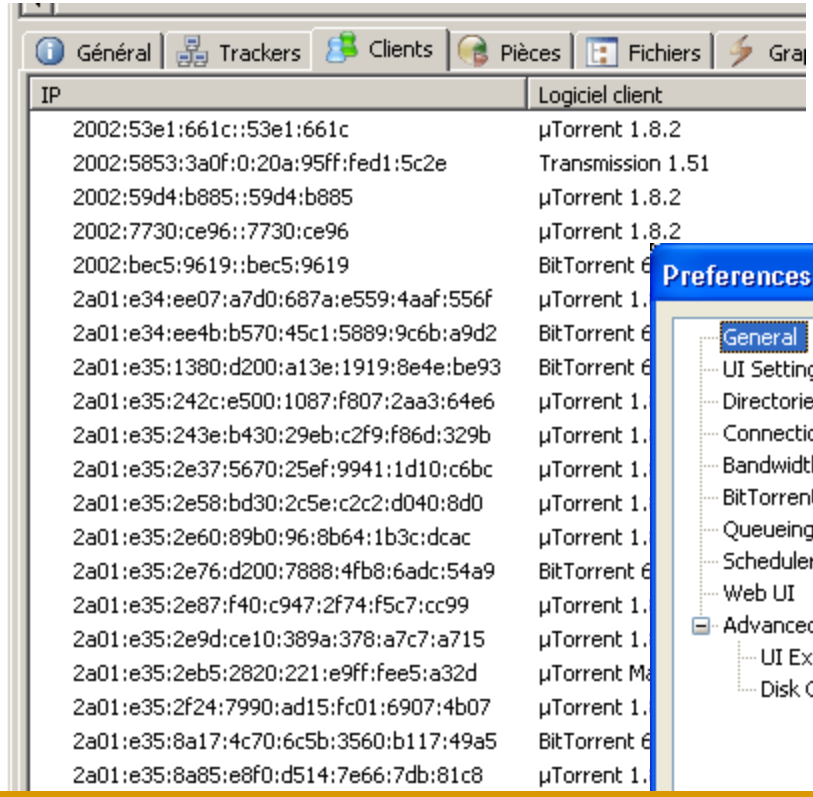
Teredo Tunnels (3/3)
No More Outbound Control

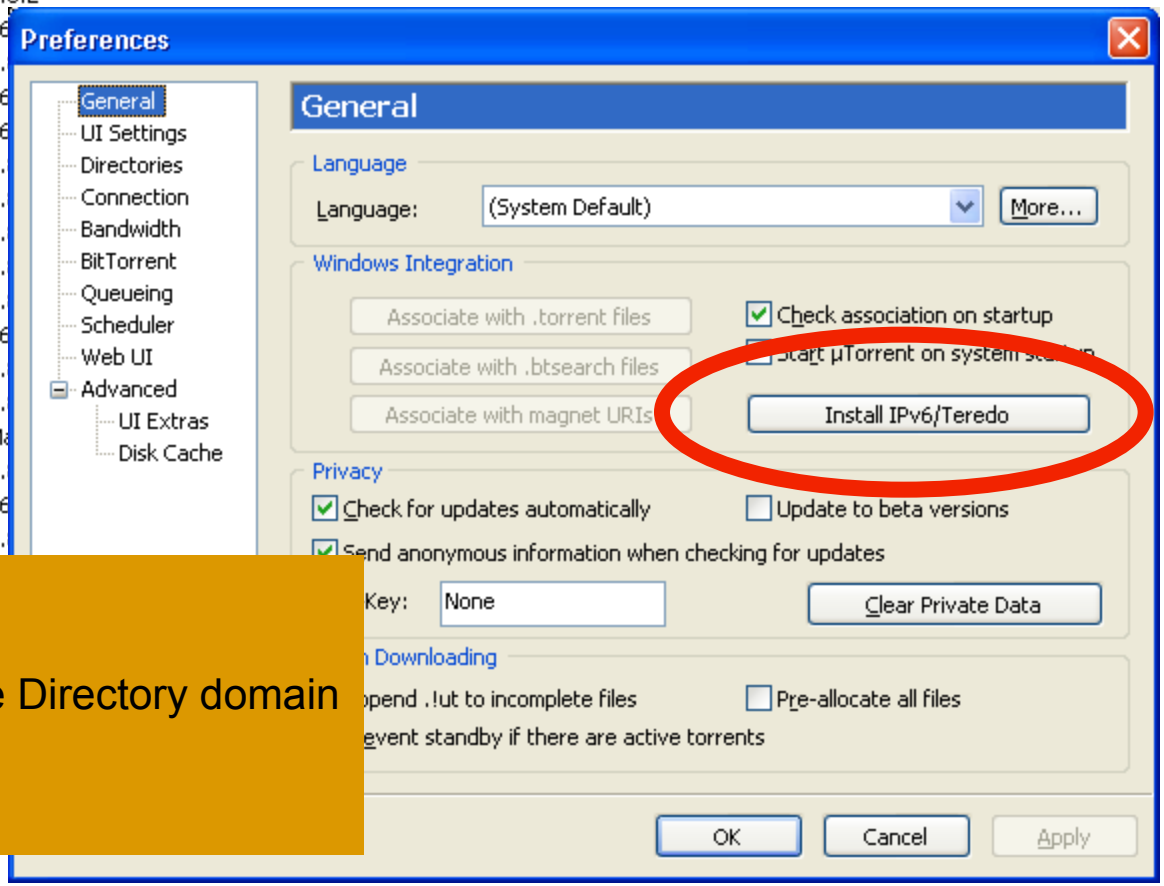
Once Teredo Configured

- **Inbound** connections are allowed
- IPv4 firewall unable to control
- IPv6 hackers can penetrate
- Host security needs IPv6 support **now**



Is it real?
May be uTorrrent 1.8 (released Aug 08)

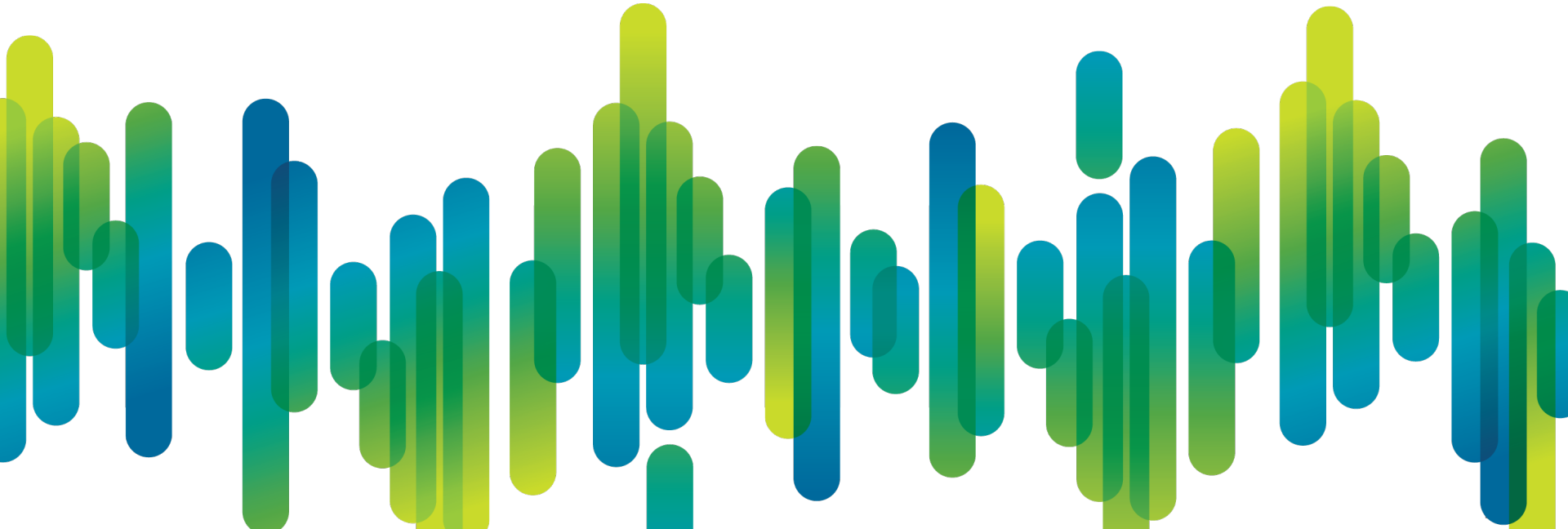




Note: on Windows Teredo is:
-Disabled when firewall is disabled
-Disabled when PC is part of Active Directory domain
-Else enabled

-User can override this protection

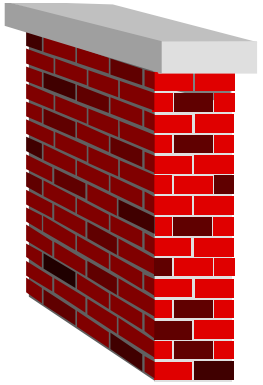
Enforcing a Policy



Cisco IOS IPv6 Extended Access Control Lists

- Very much like in IPv4
  - Filter traffic based on
    - Source and destination addresses
    - Next header presence
    - Layer 4 information
  - Implicit deny all at the end of ACL
  - Empty ACL means traffic allowed
  - Reflexive and time based ACL
- Known extension headers (HbH, AH, RH, MH, destination, fragment) are scanned until:
  - Layer 4 header found
  - Unknown extension header is found
- Side note for 7600 & other switches:
  - No VLAN ACL on the roadmap
  - Port ACL on Nexus-7000, Cat 3750 (12.2(46)SE not in base image), Cat 4K (12.2(54)SG), Cat 6K (12.3(33)SXI4)

IOS IPv6 Extended ACL



- Can match on
  - Upper layers: TCP, UDP, SCTP port numbers
  - TCP flags SYN, ACK, FIN, PUSH, URG, RST
  - ICMPv6 code and type
  - Traffic class (only six bits/8) = DSCP
  - Flow label (0-0xFFFFF)
- IPv6 extension header
  - `routing` matches any RH, `routing-type` matches specific RH
  - `mobility` matches any MH, `mobility-type` matches specific MH
  - `dest-option` matches any, `dest-option-type` matches specific destination options
  - `auth` matches AH
  - Can skip AH (but not ESP) since IOS 12.4(20)T
- `fragments` keyword matches
  - Non-initial fragments (same as IPv4)
  - And the first fragment if the L4 protocol cannot be determined
- `undetermined-transport` keyword matches (only for deny)
  - Any packet whose L4 protocol cannot be determined: fragmented or unknown extension header

IPv6 ACL Implicit Rules RFC 4890

- Implicit entries exist at the end of each IPv6 ACL to allow neighbor discovery:

```
permit icmp any any nd-na
permit icmp any any nd-ns
deny ipv6 any any
```

- Nexus 7000 also allows RS &RA

Example: RFC 4890 ICMP ACL

```
ipv6 access-list RFC4890
    permit icmp any any echo-reply
    permit icmp any any echo-request
    permit icmp any any 1 3
    permit icmp any any 1 4
    permit icmp any any packet-too-big
    permit icmp any any time-exceeded
    permit icmp any any parameter-problem
    permit icmp any any mld-query
    permit icmp any any mld-reduction
    permit icmp any any mld-report
    permit icmp any any nd-na
    permit icmp any any nd-ns
    permit icmp any any router-solicitation
```

IPv6 ACL to Protect VTY

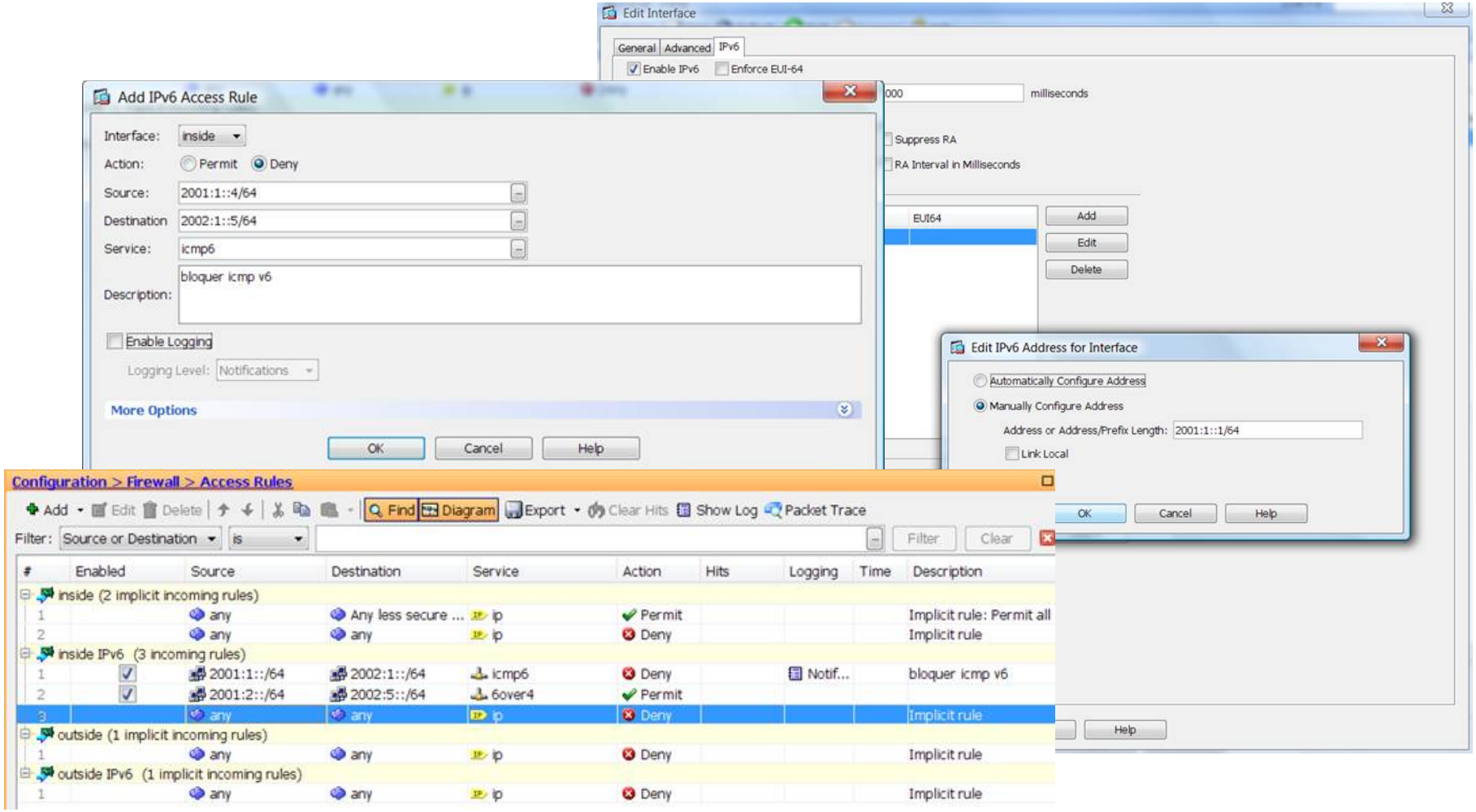
For Your Reference

```
ipv6 access-list VTY
  permit ipv6 2001:db8:0:1::/64 any


line vty 0 4
  ipv6 access-class VTY in
```

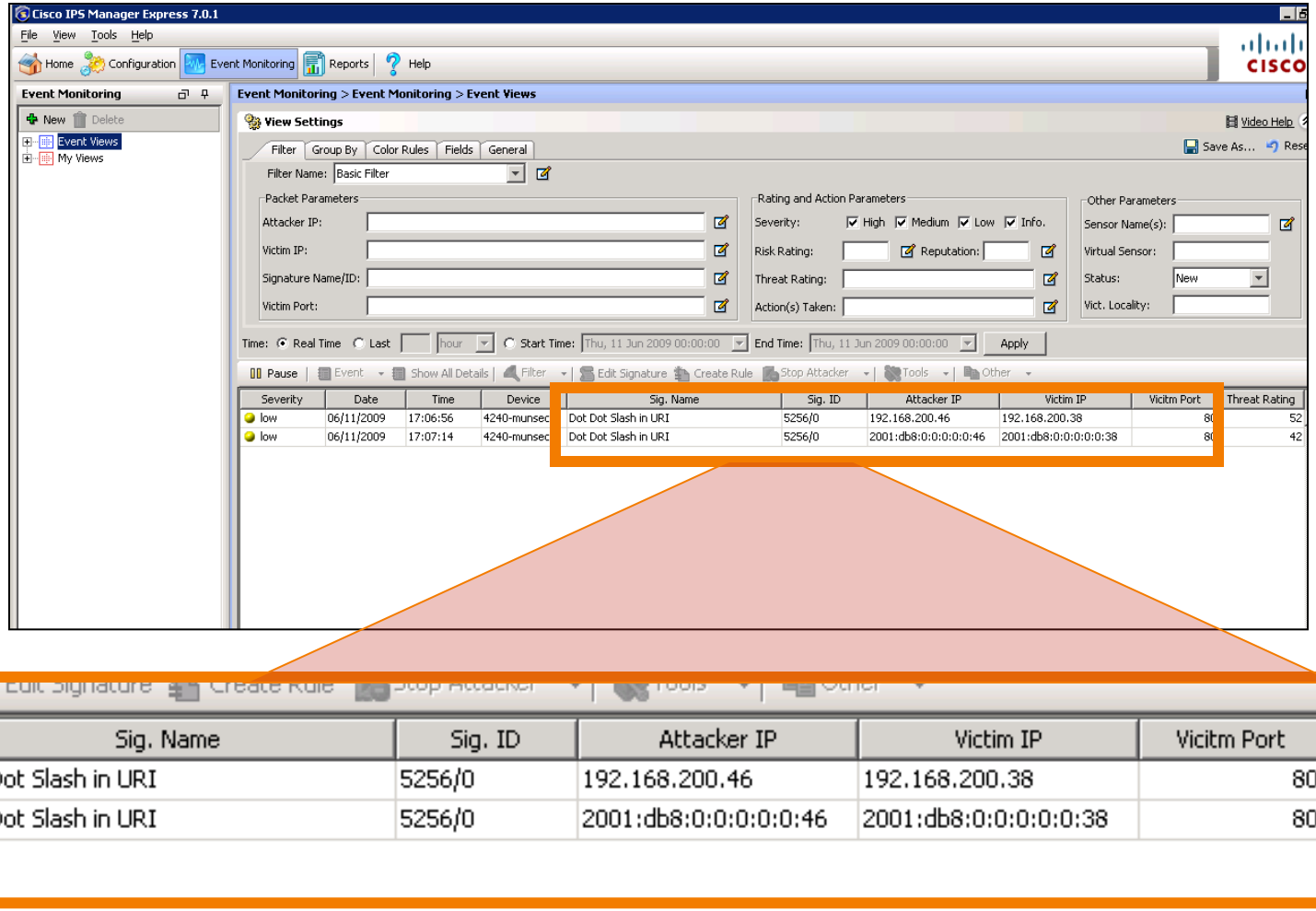
ASA Firewall IPv6 Support

- Since version 7.0 (April 2005)
- Dual-stack, IPv6 only, IPv4 only
- Extended IP ACL with stateful inspection
- Application awareness
  - HTTP, FTP, telnet, SMTP, TCP, SSH, UDP
- uRPF and v6 Frag guard
- IPv6 header security checks
  - Always block routing-header (type 0 and 2)
- Management access via IPv6
  - Telnet, SSH, HTTPS
- ASDM support (ASA 8.2)
- Routed & transparent mode (ASA 8.2)
- Fail-over support (ASA 8.2.2)
- **Caveats:**
  - **Cannot block specific extension headers**

ASA Firewall IPv6 Support

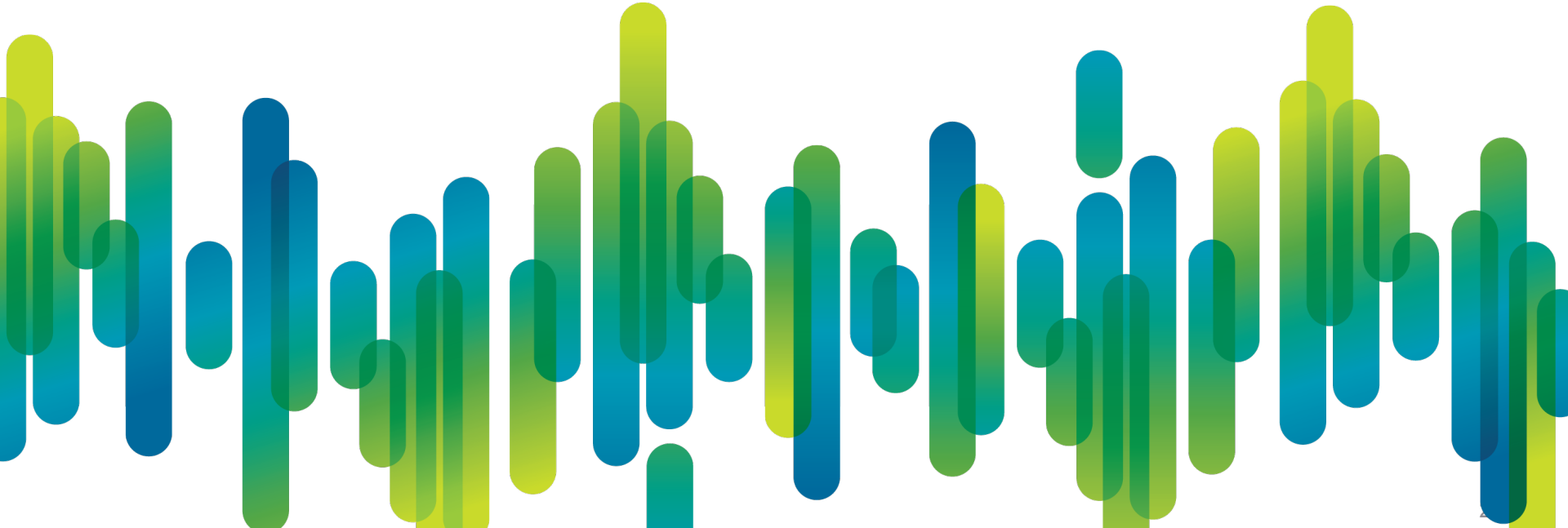


Dual-Stack IPS Engines
Service HTTP



Enterprise Deployment: Secure IPv6 Connectivity

How to Secure IPv6 over the WAN

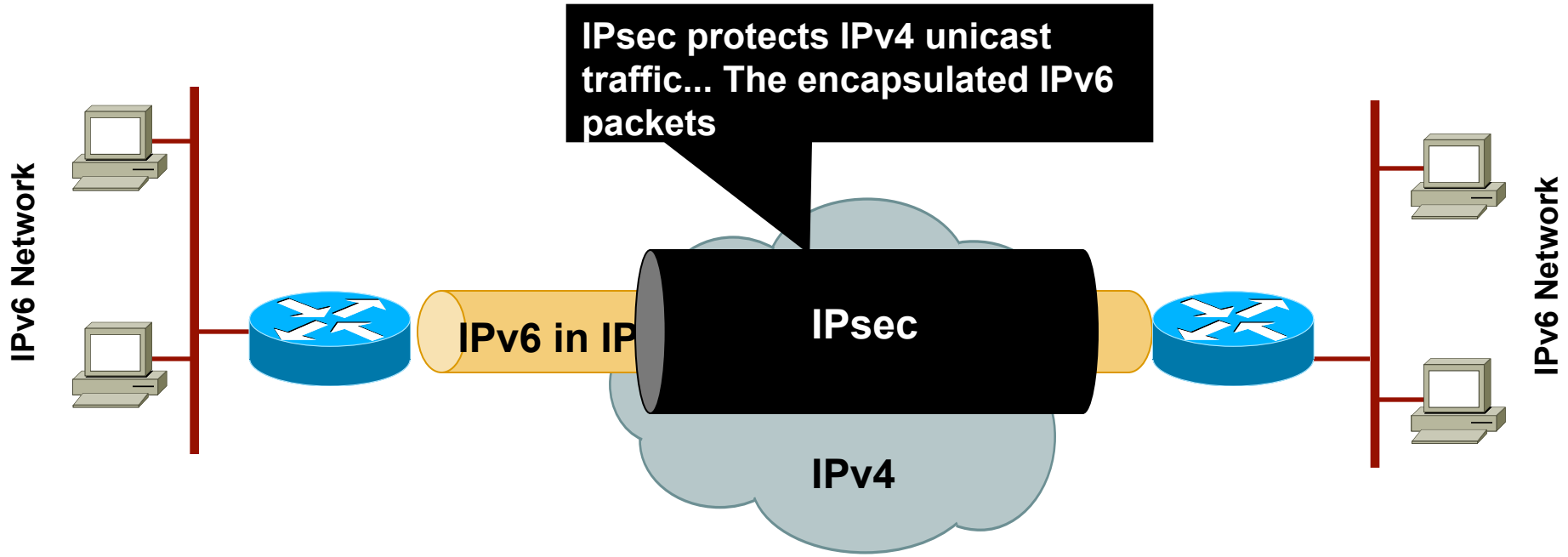


Secure IPv6 over IPv4/6 Public Internet

- No traffic sniffing
- No traffic injection
- No service theft

Public Network	Site 2 Site	Remote Access
IPv4	▪6in4/GRE Tunnels Protected by IPsec ▪DMVPN 12.4(20)T	▪ ISATAP Protected by RA IPsec ▪ SSL VPN Client AnyConnect
IPv6	IPsec VTI 12.4(6)T	N/A

Secure Site to Site IPv6 Traffic over IPv4 Public Network with GRE IPsec



GRE tunnel can be used to transport both IPv4 and IPv6 in the same tunnel

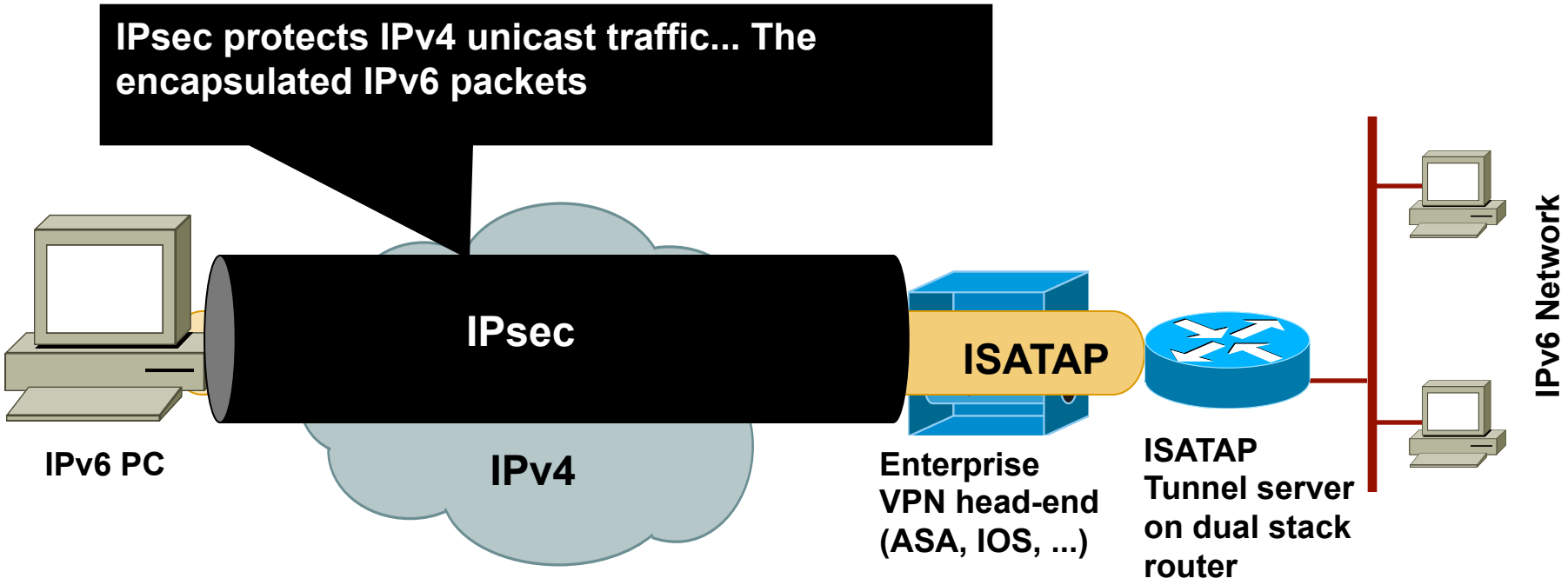
Secure Site to Site IPv6 Traffic over IPv4 Public Network with DMVPN

- IPv6 packets over DMVPN IPv4 tunnels
  - In IOS release 12.4(20)T (July 2008)
  - IPv6 and/or IPv4 data packets over same GRE tunnel
- Complete set of NHRP commands
  - network-id, holdtime, authentication, map, etc.
- NHRP registers two addresses
  - Link-local for routing protocol (Automatic or Manual)
  - Global for packet forwarding (Mandatory)

IPv6 for Remote Devices Solutions

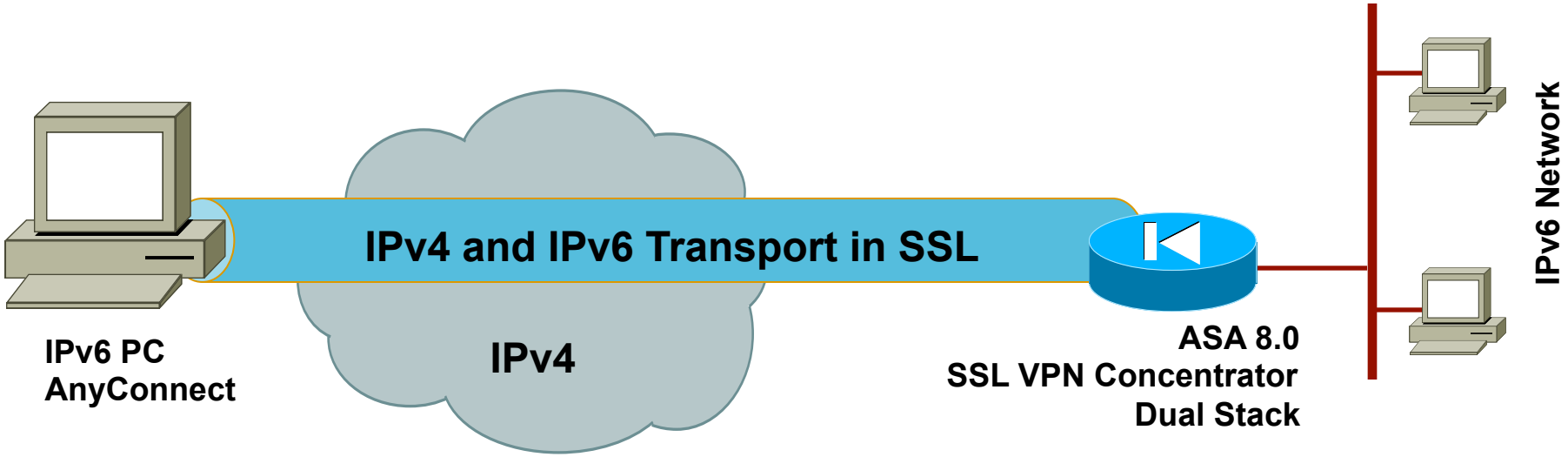
- Enabling IPv6 traffic inside the Cisco VPN Client tunnel
  - NAT and Firewall traversal support
  - Allow remote host to establish a v6-in-v4 tunnel either automatically or manually
    - ISATAP—Intra Site Automatic Tunnel Addressing Protocol
    - Fixed IPv6 address enables server's side of any application to be configured on an IPv6 host that could roam over the world
- Use of ASA 8.0 and SSL VPN Client AnyConnect
  - Can transfer IPv6 traffic over public IPv4

Secure RA IPv6 Traffic over IPv4 Public Network: ISATAP in IPSec

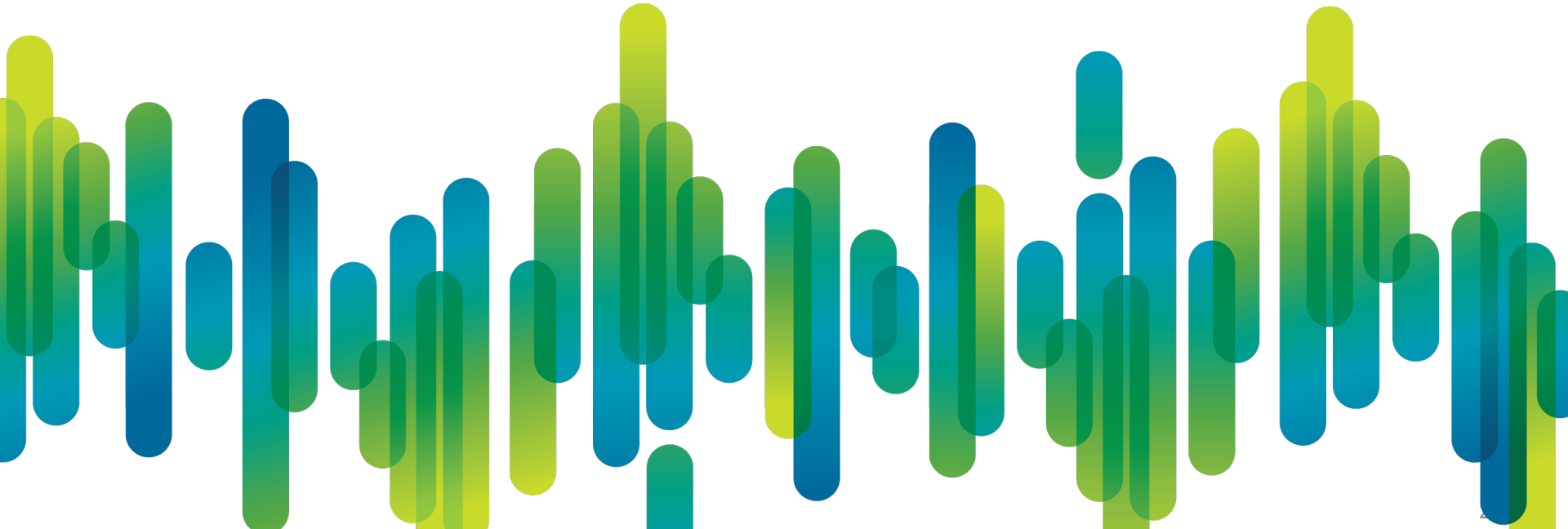


IPsec with NAT-T can traverse NAT
ISATAP encapsulates IPv6 into IPv4

Secure RA IPv6 Traffic over IPv4 Public Network: AnyConnect SSL VPN Client



Conclusion

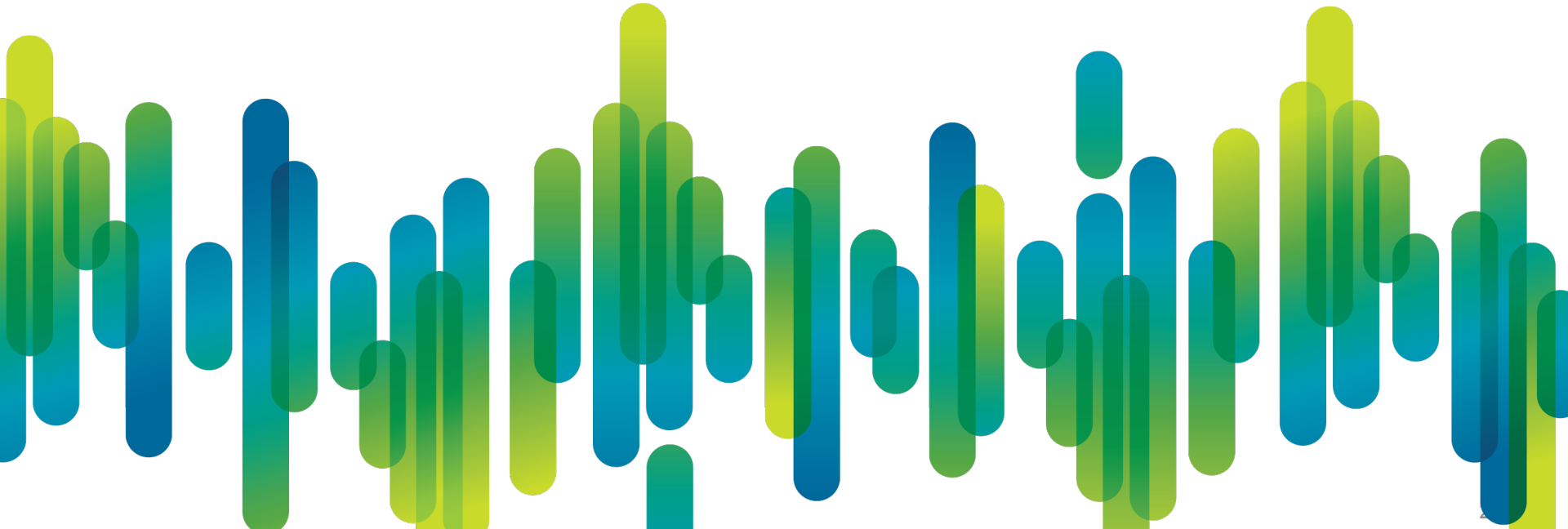


Key Take Away

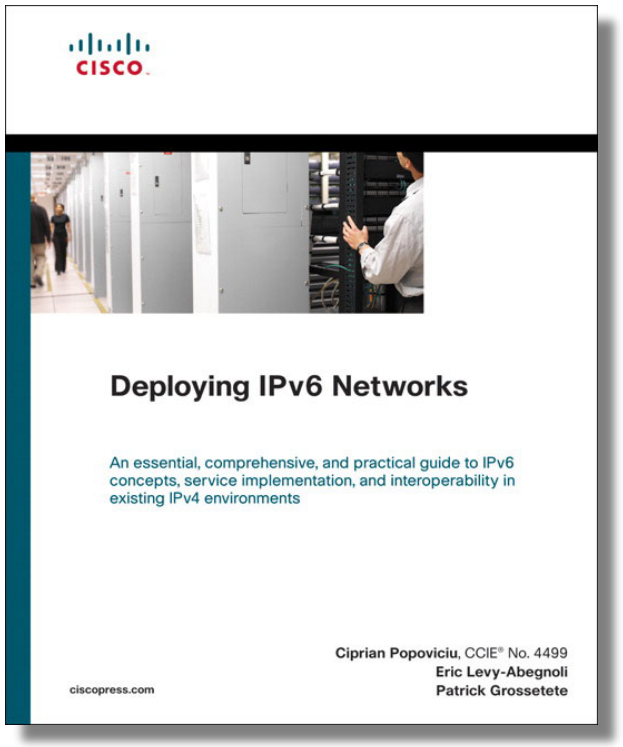
- So, nothing really new in IPv6
- Lack of operation experience may hinder security for a while: **training is required**
- Security enforcement is possible

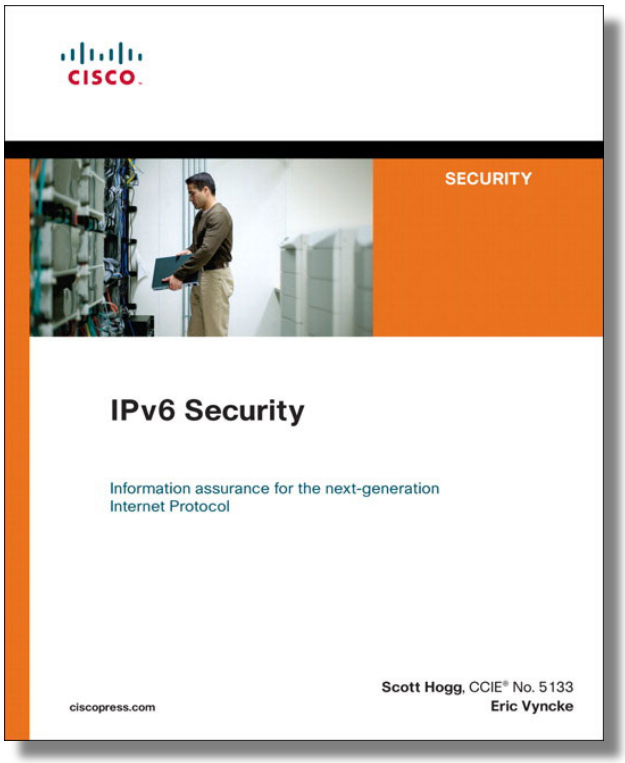
  Control your IPv6 traffic as you do for IPv4
- Leverage IPsec to secure IPv6 when suitable

Q & A



Recommended Reading





Source: Cisco Press

Agenda

- Introduction
- IPv6 in the Enterprise
- Routing Considerations
- Security for IPv6
- First Hop Security
- Unified Communications
- Multicast
- DNS
- Deployment and Operation Considerations

IPv6 – First Hop Security

Agenda

- **Terminology and other high level considerations**
- Neighbor Discovery Protocol overview and vulnerabilities
- Distributed security :
  - SEcure Neighbor Discovery overview
  - SeND deployment challenges and pitfalls
- Centralized security:
  - IPv6 first-hop security overview
  - Deep Dive on ten most wanted First-Hop features
  - Deployment challenges and pitfalls
- IETF update
- Demo

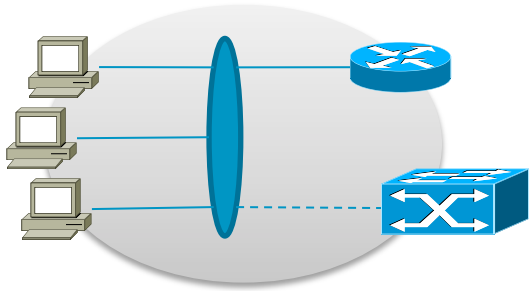
What Threats?

- Focus on threats related to link-operations
- By the nature of IPv6, this encompass:
  - Address operations
  - Neighbors discovery
  - Router discovery
- Threats which can be mitigated by knowledge acquired during link operations

What are link operations?

Operations contained within the link boundaries, necessary for a node to communicate with its neighbors, including the link exit points.

- **It encompass:**
  - Address configuration parameters
  - Address initialization
  - Address resolution
  - Default gateway discovery
  - Local network configuration
  - Neighbor reachability tracking



"A link"

Why Securing Link-operations?

End-nodes exposed to many threats:

- Address configuration parameters : Trickery on configuration parameters
- Address initialization: Denial of address insertion
- Address resolution: Address stealing
- Default gateway discovery: Rogues routers
- Local network configuration: Trickery on configuration parameters
- Neighbor reachability tracking: Trickery on neighbor status

Malicious nodes can hide on the link

- To disrupt link-operations
- To poison neighbor caches
- To attack on-link or off-link victims
- To highjack key roles such as router or dhcp server

Malicious nodes can sit anywhere in the network

- To launch DoS attacks on last-router and exploit link-operations security caveats

What is different with IPv6?

Threats are very much tight up to the topology: what is specific to IPv6 from topology standpoint?

- **More addresses!**
  - More end-nodes allowed on the link (up to 2^{64} !)
  - Bigger neighbor cache on end-nodes an on default-router
  - May lead to some dramatic topology evolution.
  - Creates new opportunities for DoS attacks

Threats are also tight up to the protocols in use: what is different?

- **More distributed and more autonomous operations**
  - Nodes discover automatically their default router.
  - Nodes auto-configure their addresses
  - Nodes defend themselves (SeND)
  - Distributed address assignment creates true challenges for controlling address misuse

Agenda

- Terminology and other high level considerations
- **Neighbor Discovery Protocol overview and vulnerabilities**
- Distributed security :
  - SEcure Neighbor Discovery overview
  - SeND deployment challenges and pitfalls
- Centralized security:
  - IPv6 first-hop security overview
  - Deep Dive on ten most wanted First-Hop features
  - Deployment challenges and pitfalls
- IETF update
- Demo

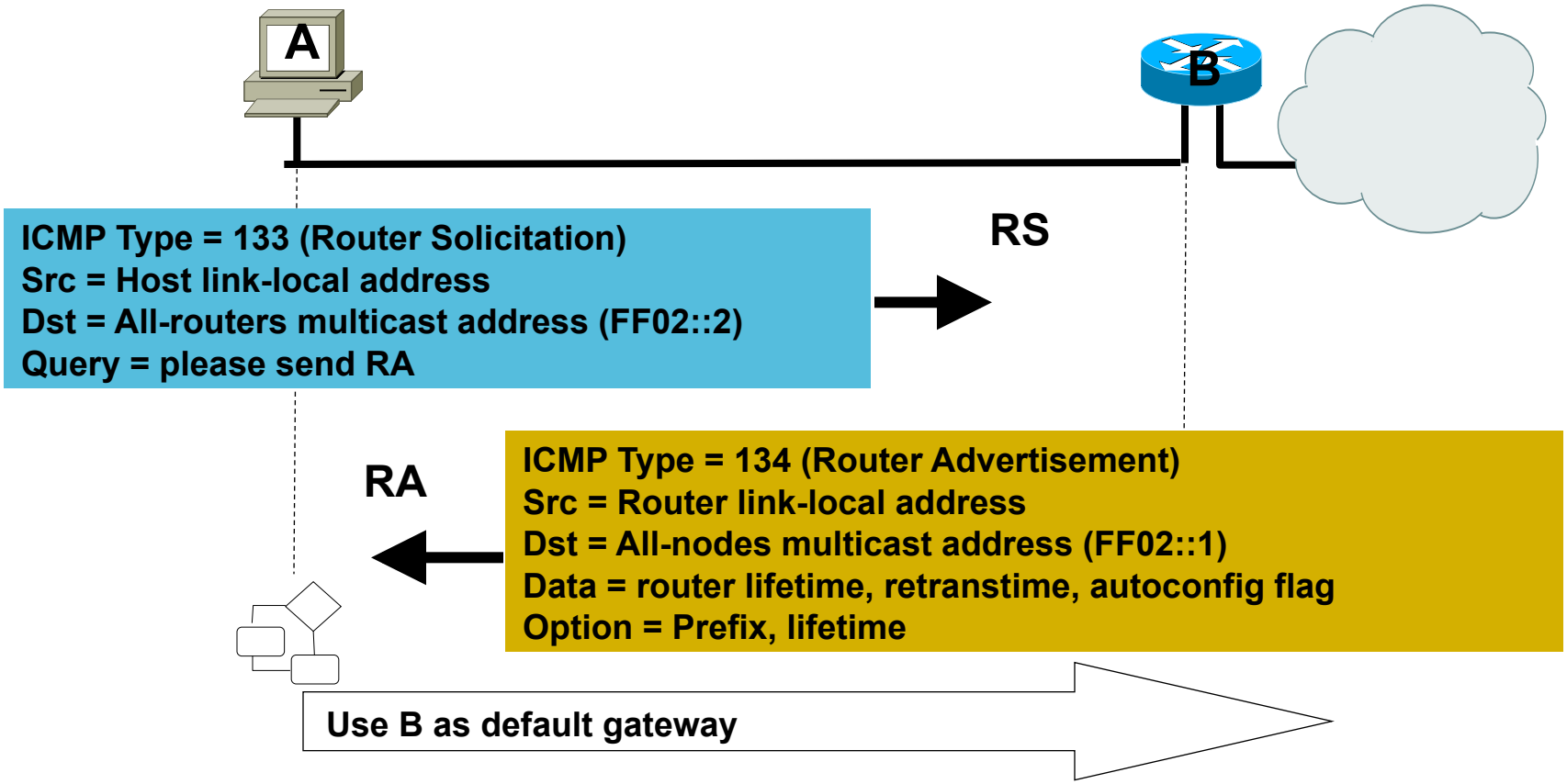
Fundamentals On Neighbor Discovery

- Defined in RFC 4861, “Neighbor Discovery for IP Version 6 (IPv6)” and RFC 4862 (“IPv6 Stateless Address Autoconfiguration”)
- Used for:
  - Router discovery
  - Autoconfiguration of addresses (SLAAC)
  - IPv6 address resolution (replaces ARP)
  - Neighbor reachability (NUD)
  - Duplicate Address Detection (DAD)
  - Redirection
- Operates above ICMPv6
  - Rely heavily on multicast (including L2-multicast)
- Works with icmp messages and messages “options”

Router Discovery

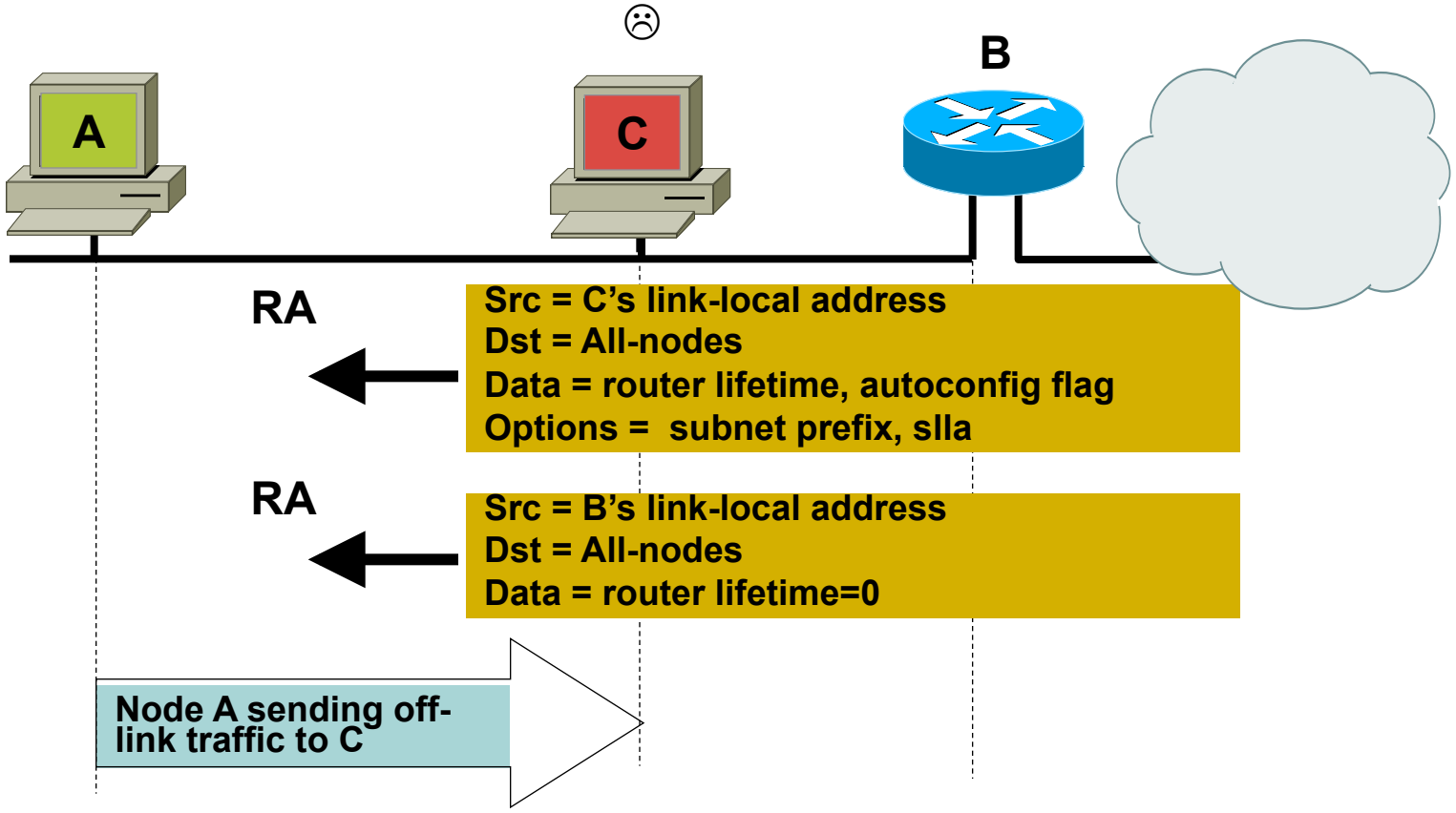
- Find default/first-hop routers
- Discover on-link prefixes => which destinations are neighbors

  → Messages: Router Advertisements, Router Solicitations



Attack On Router Discovery

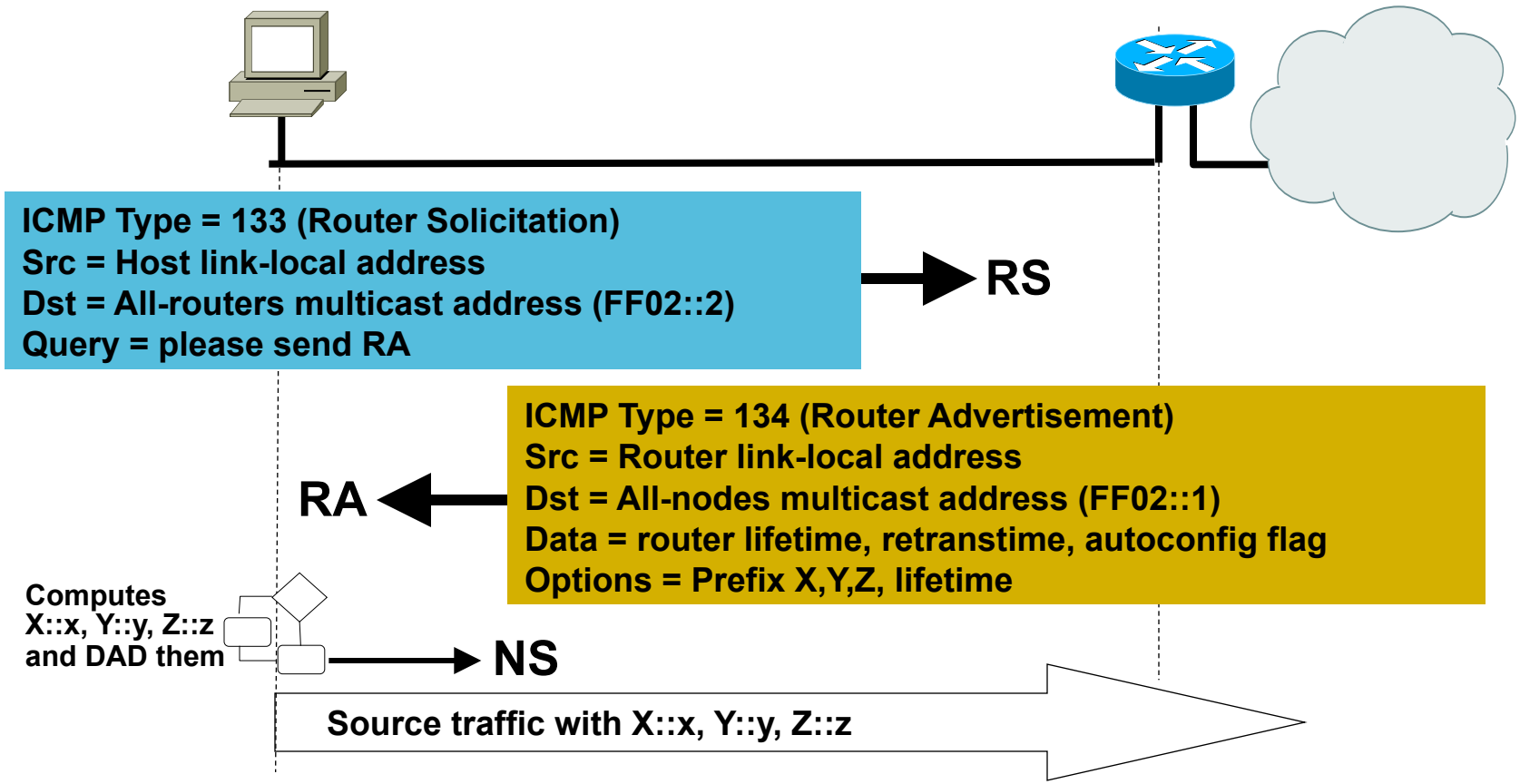
- Attacker tricks victim into accepting itself as default router
- Based on spoofed Router Advertisements
- The most frequent threat by non-malicious user



Stateless Auto-Configuration

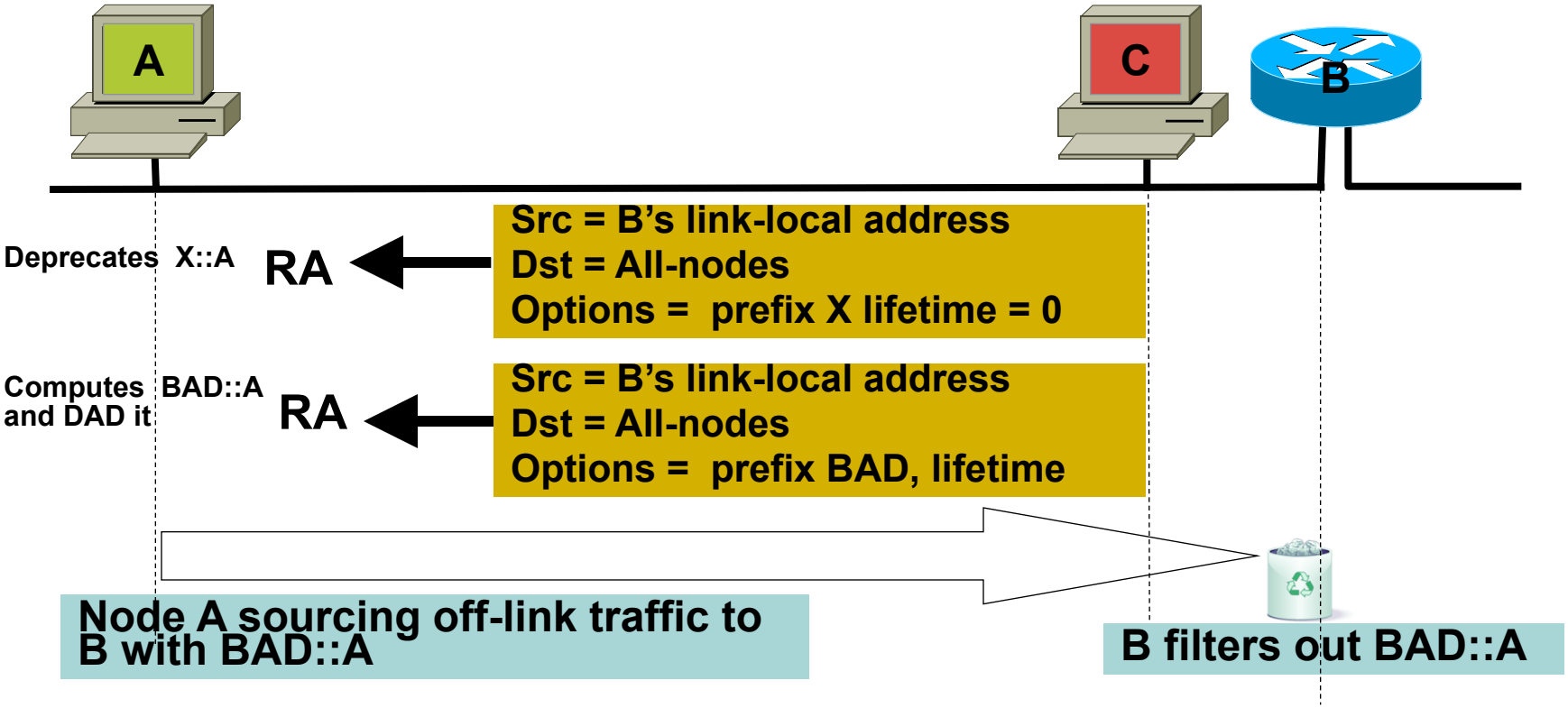
- Stateless, based on prefix information delivered in Router Advertisements

  → Messages: Router Advertisements , Router Solicitations



Attack on Address Configuration

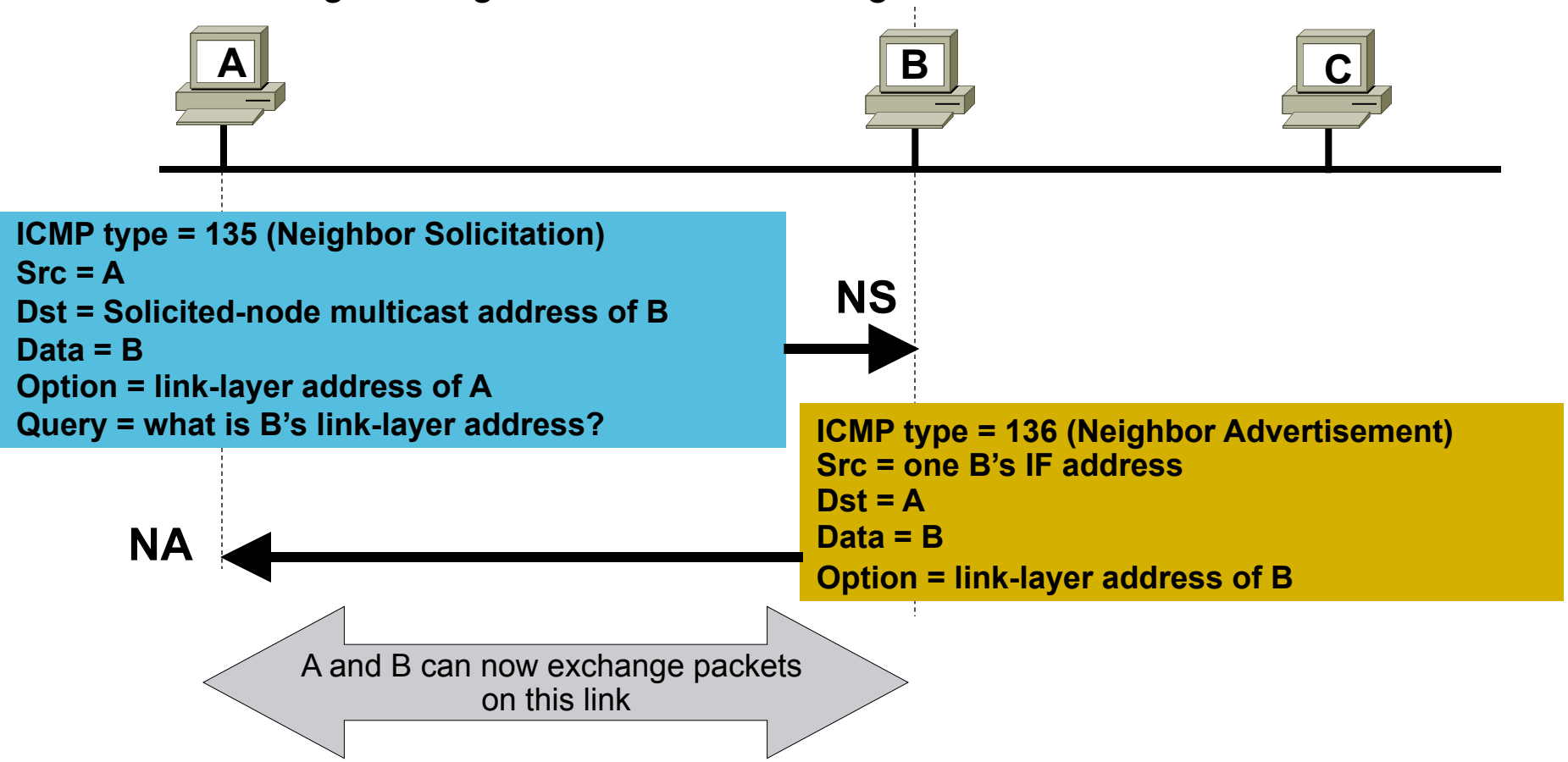
- Attacker spoofs Router Advertisement with false on-link prefix
- Victim generates IP address with this prefix
- Access router drops outgoing packets from victim (ingress filtering)
- Incoming packets can't reach victim ☹



Address Resolution

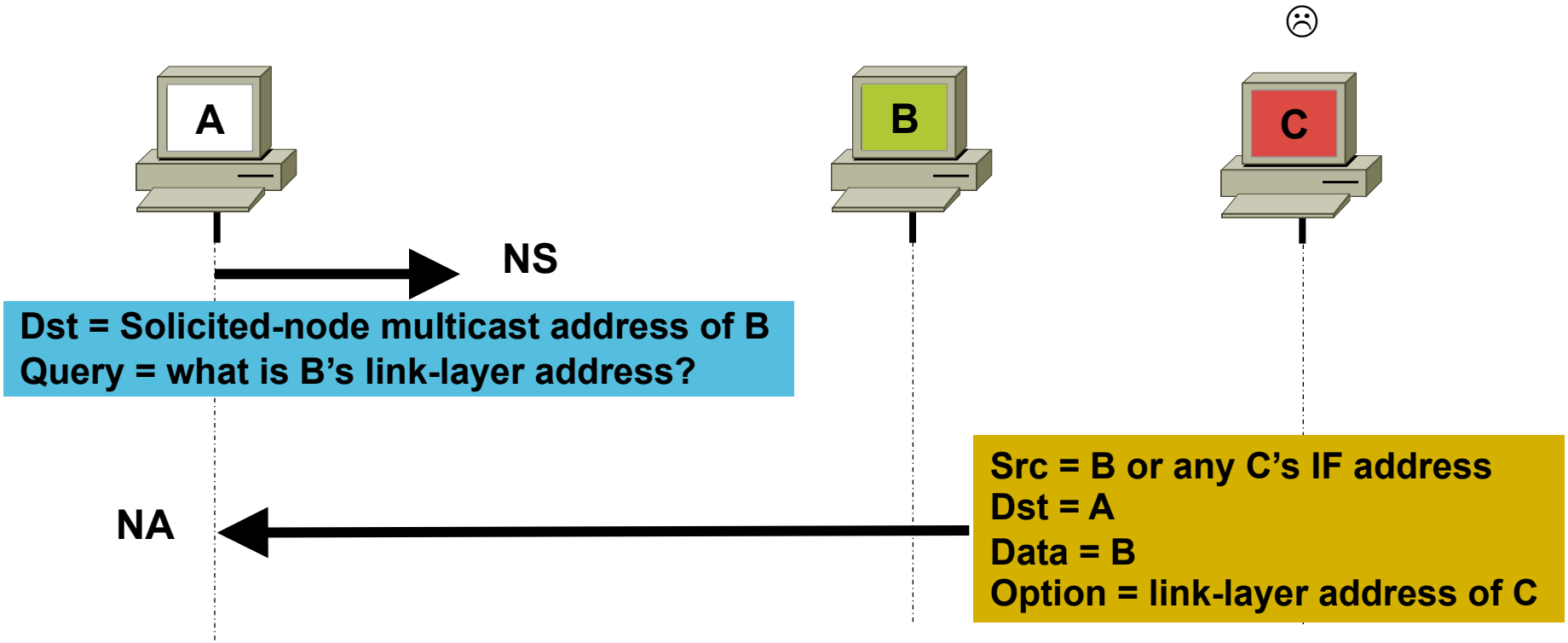
- Resolves IP address into MAC address
- Creates neighbor cache entry

  → Messages: Neighbor Solicitation, Neighbor Advertisement



Attack On Address Resolution

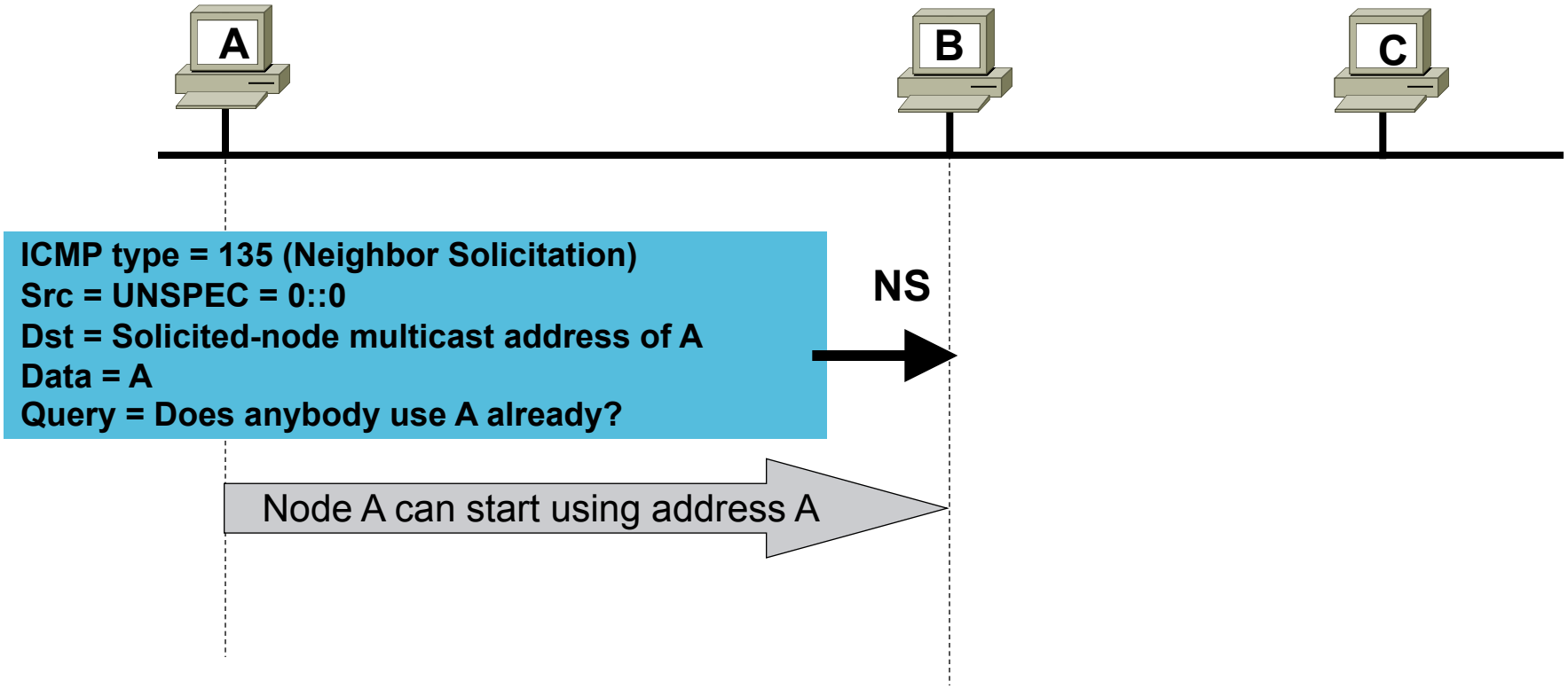
- Attacker can claim victim's IP address



NDP Features: Duplicate Address Detection

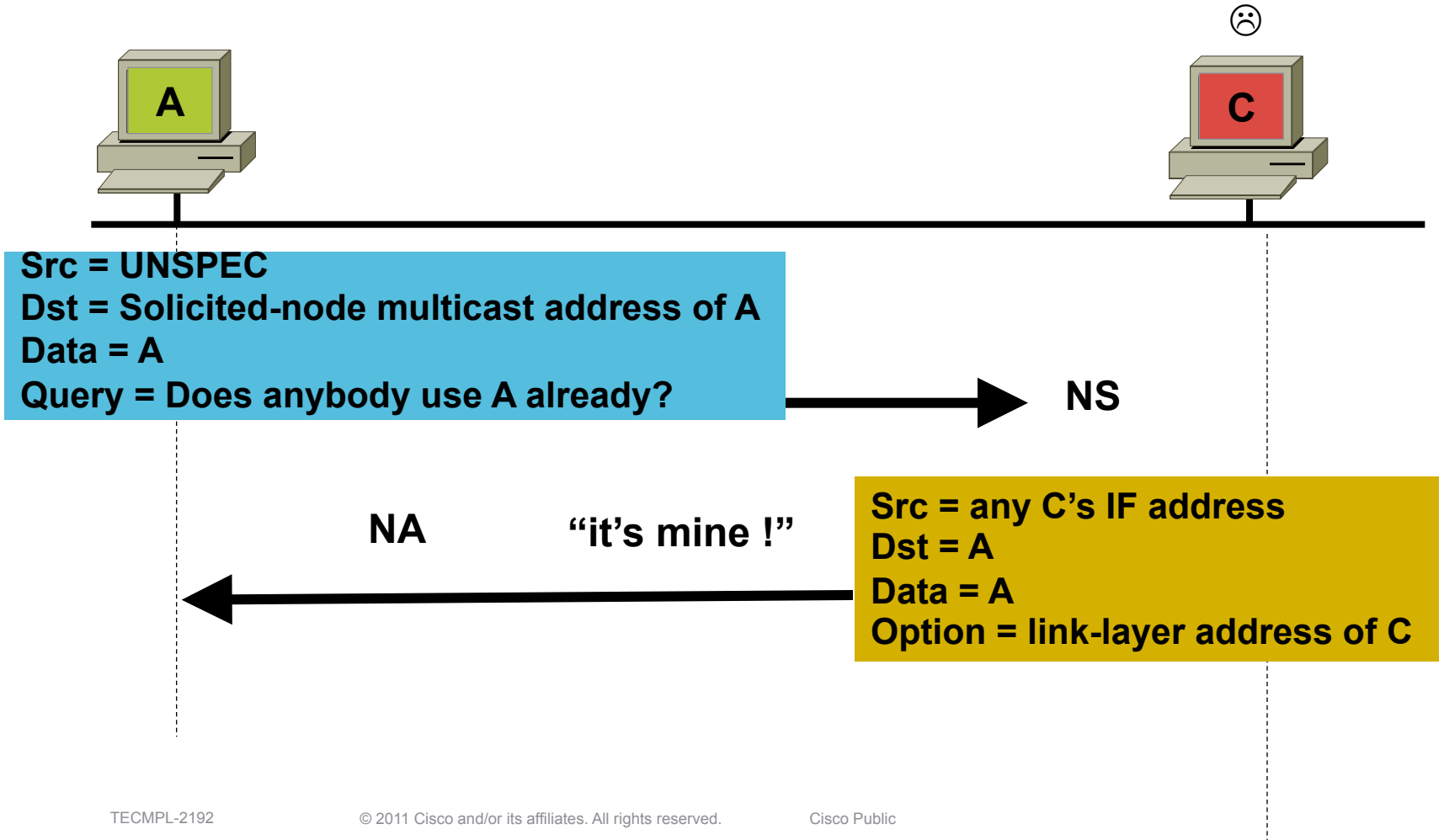
- Verify address uniqueness
- Probe neighbors to verify nobody claims the address

  → Messages: Neighbor Solicitation, Neighbor Advertisement



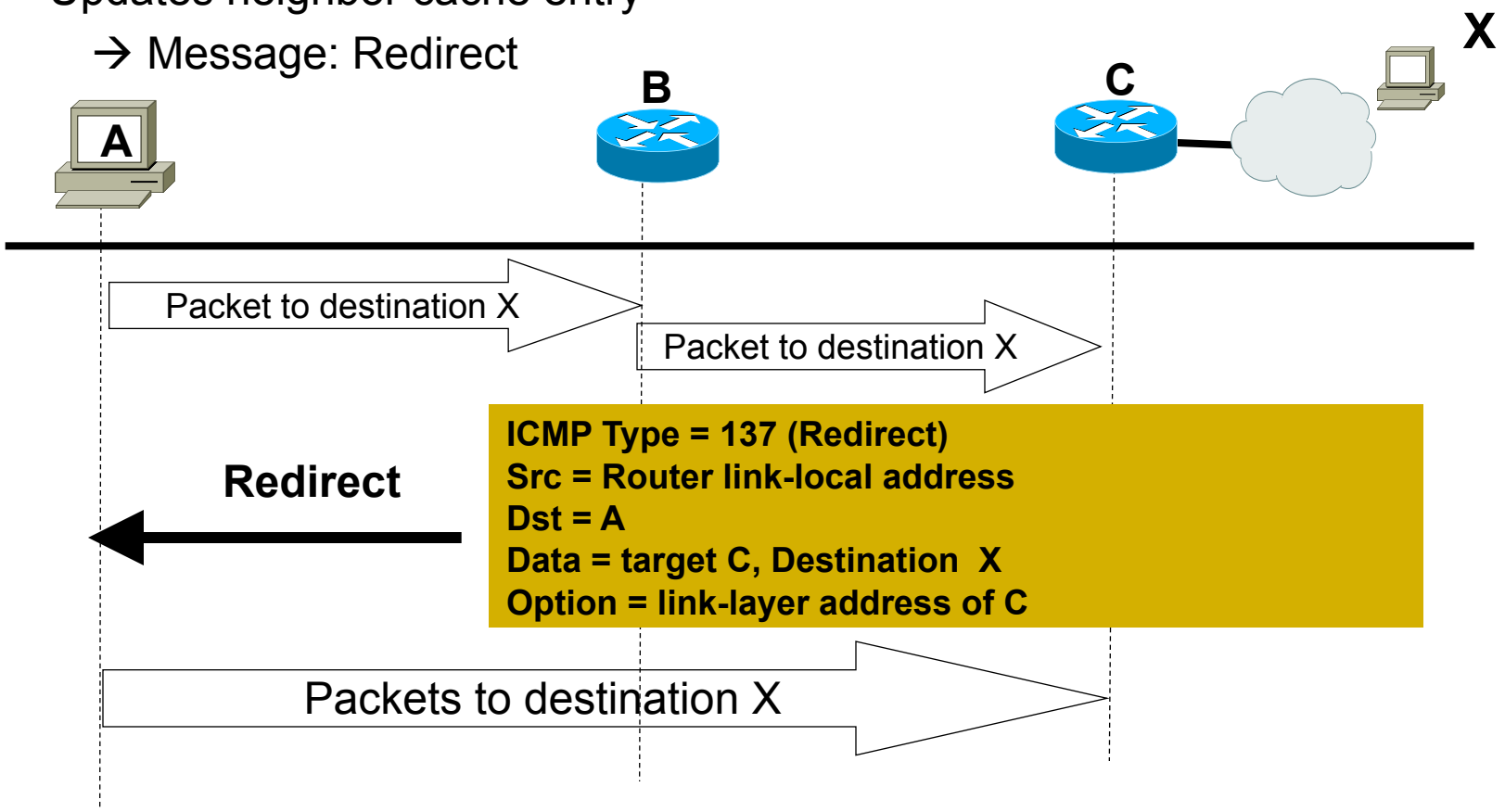
Attack On DAD

- Attacker hacks any victim's DAD attempts
- Victim can't configure IP address and can't communicate



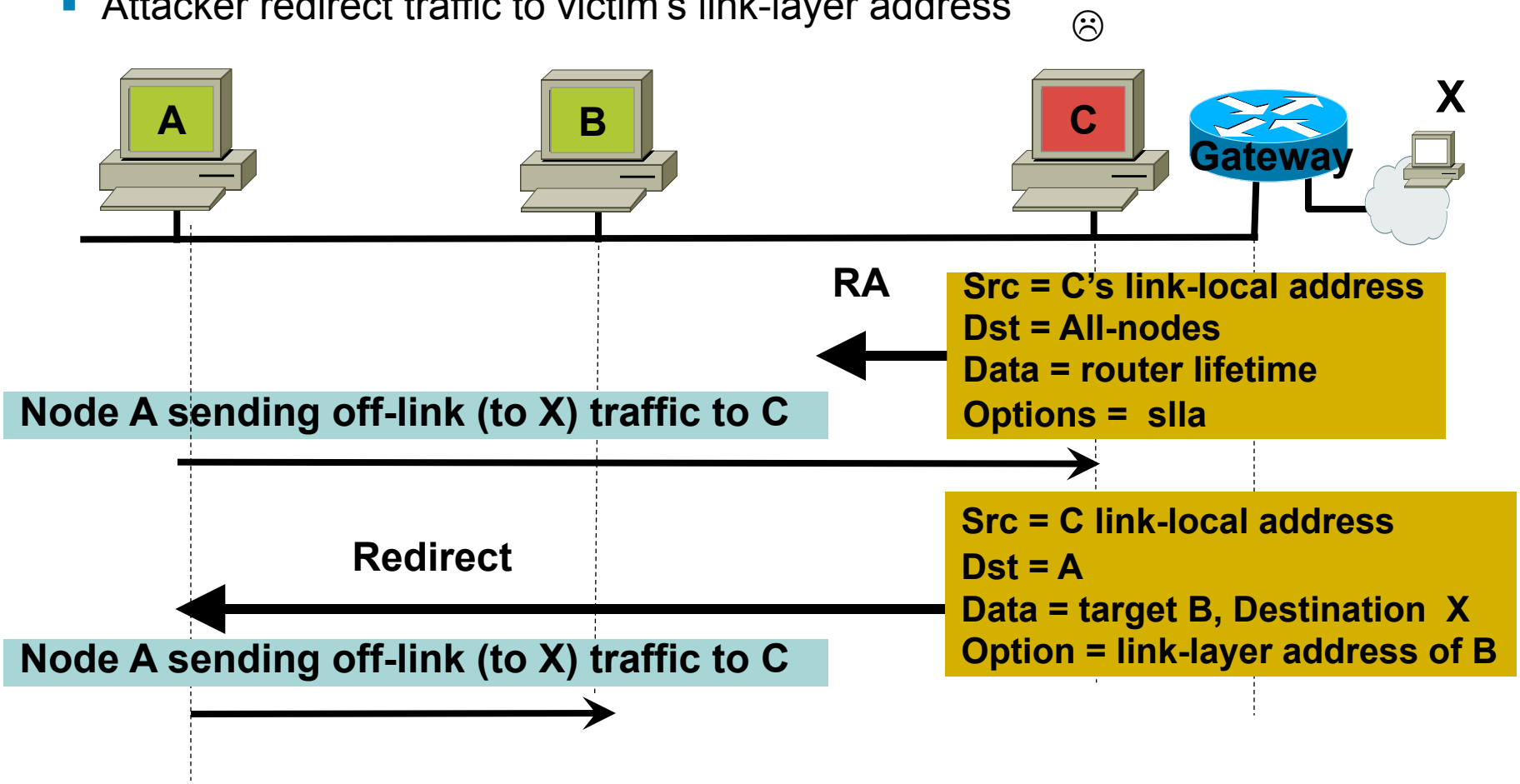
Redirect

- Redirect host to better router
- Redirect host (from first-hop router) to neighbor
- Updates neighbor cache entry
  → Message: Redirect

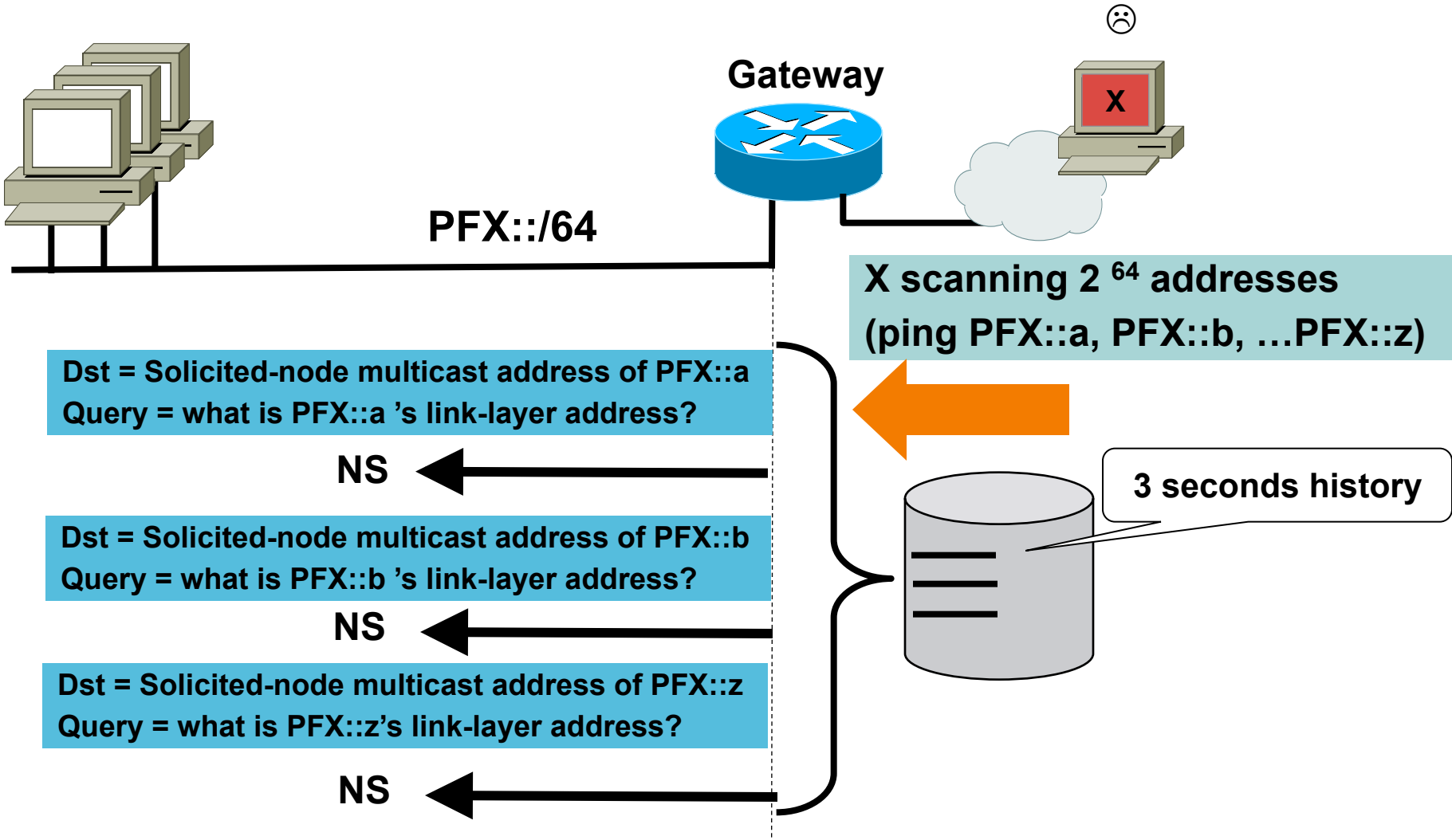


Redirect Attack

- Attacker tricks nodes on the link into accepting itself as default router
- Attacker redirect traffic to victim's link-layer address



DoS Attacks On Neighbor Cache



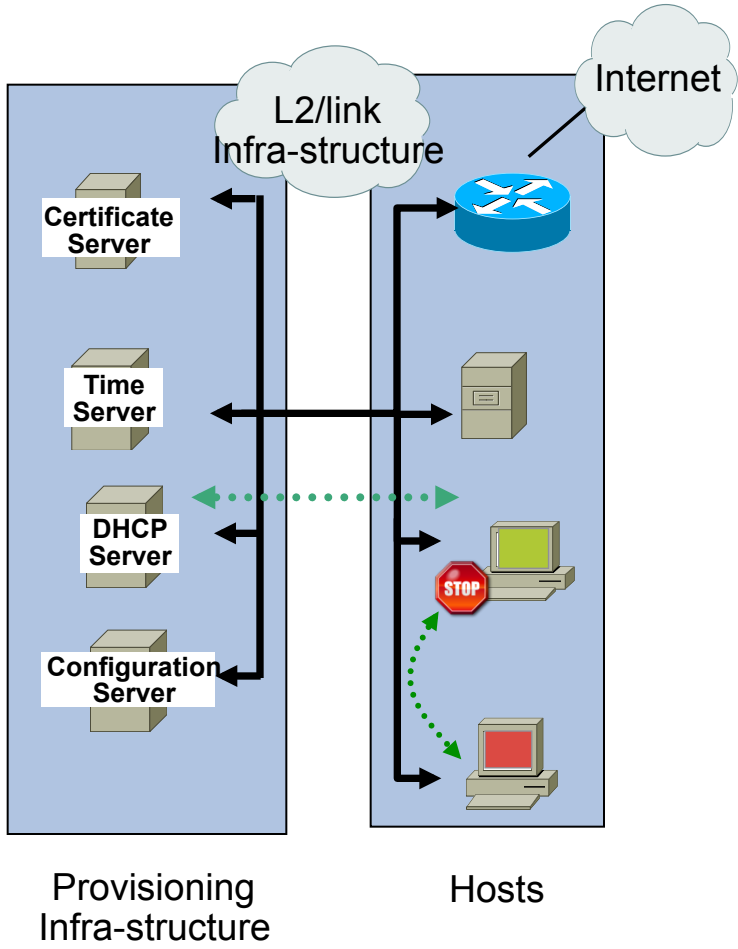
Agenda

- Terminology and other high level considerations
- Neighbor Discovery Protocol overview and vulnerabilities
- **Distributed security :**
  - SEcure Neighbor Discovery overview
  - SeND deployment challenges and pitfalls
- Centralized security:
  - IPv6 first-hop security overview
  - Deep Dive on ten most wanted First-Hop features
  - Deployment challenges and pitfalls
- IETF update
- Demo

Distributed Security:
Securing Link-operations On End-nodes

- **Advantages**
  - No central administration, no central operation
  - No bottleneck, no single-point of failure
  - Intrinsic part of the link-operations
  - No tying up to the L2 infra
  - Load distribution

- **Disadvantages**
  - Heavy provisioning of end-nodes
  - Only provisioned end-nodes are protected
  - Tied up to nodes capability
  - Bootstrapping issue
  - Complexity spread all over the domain.



Distributed Security ≡ Secure Neighbor Discovery

DOES

- Each node on the link takes care of its own security
- Verifies router legitimacy
- Verifies address ownership

DOES NOT

- It does not verify other key role legitimacy (DHCP server, NTP, etc.)
- It only applies to link operations
- It does not provide end-to-end security

What Is SeND?

- Provides Address ownership proof and Router authorization
- SeND is NOT a new protocol
- SeND is “just” an extension to NDP
- Therefore ND+SeND remains a protocol operating on the link
- **SeND is a distributed mitigation mechanism**
- SeND does not provide any “end-to-end” security
- SeND specified in RFC3971 and RFC3972

Address Ownership Proof

- Problem:

  Unlike IPv6, IPv6 ND favors a distributed model for allocating addresses, with no or very incomplete central police capabilities.

  Worse: ND cache policy is a last-come first-serve model!

  It's easy to steal addresses on the link

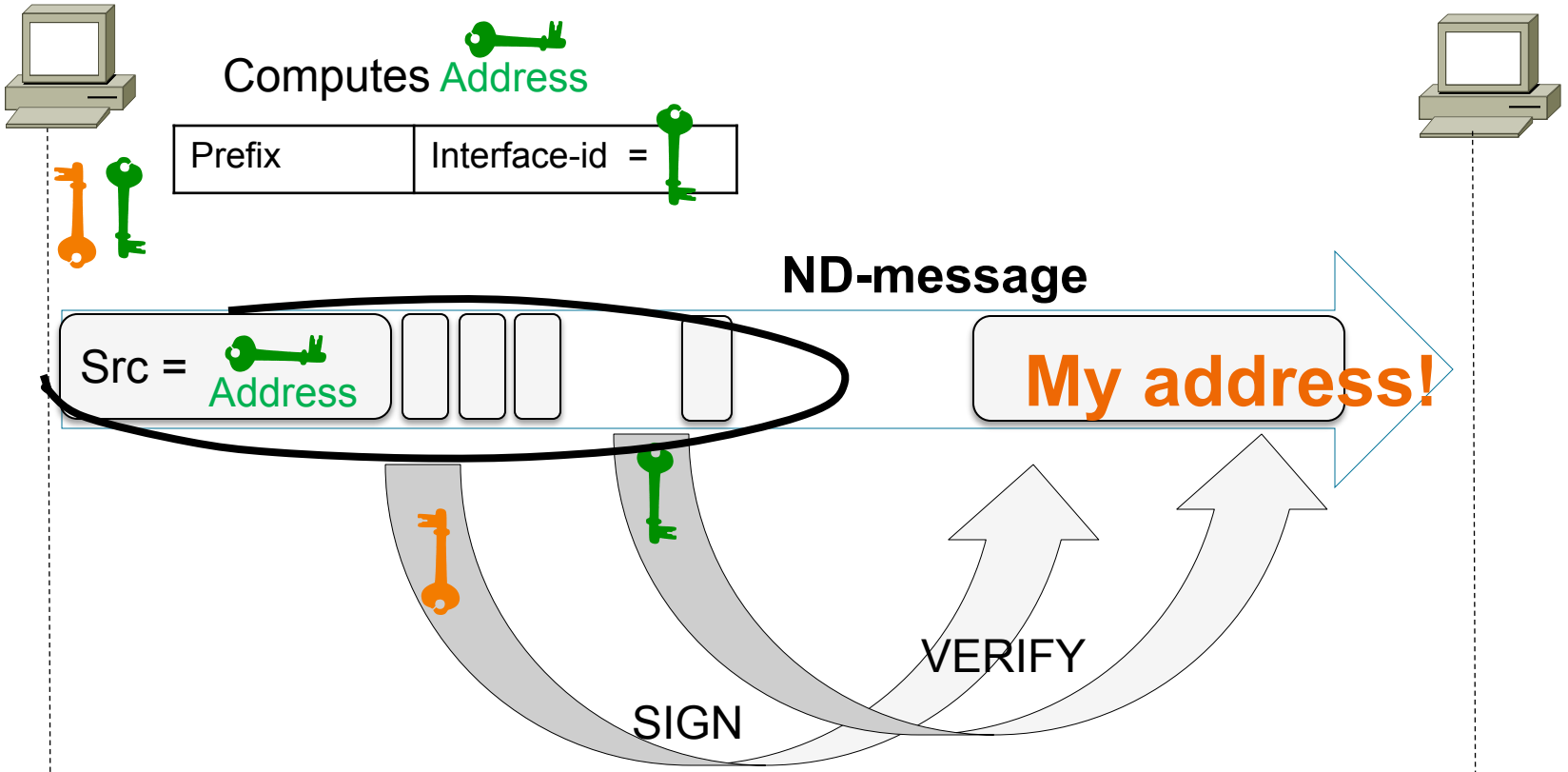
  ND does not verify address ownership

- Objectives for Address ownership:

  Verify that and address claimed **in NDP** is owned by the claimer

  Link with the Source Address Validation system?

Address Ownership Proof for dummies



Router Authorization Overview

- Problem:

  ND enables node to automatically configure itself and address and pick up its default gateway

  It's easy to configure a "rogue" router on an unsecured link

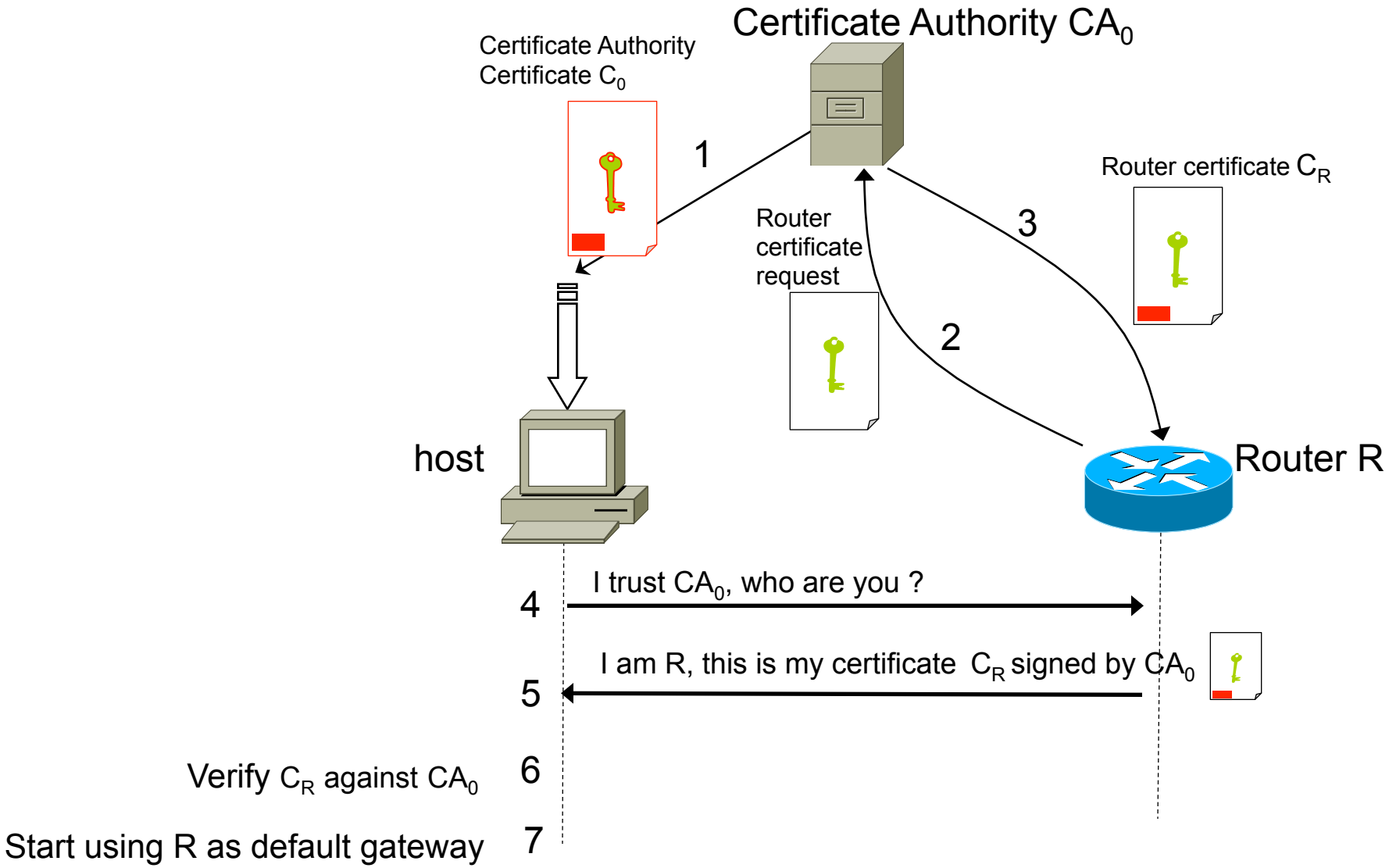
  It's difficult for a node to distinguish valid and invalid source of information

- Objectives for Router authorization:

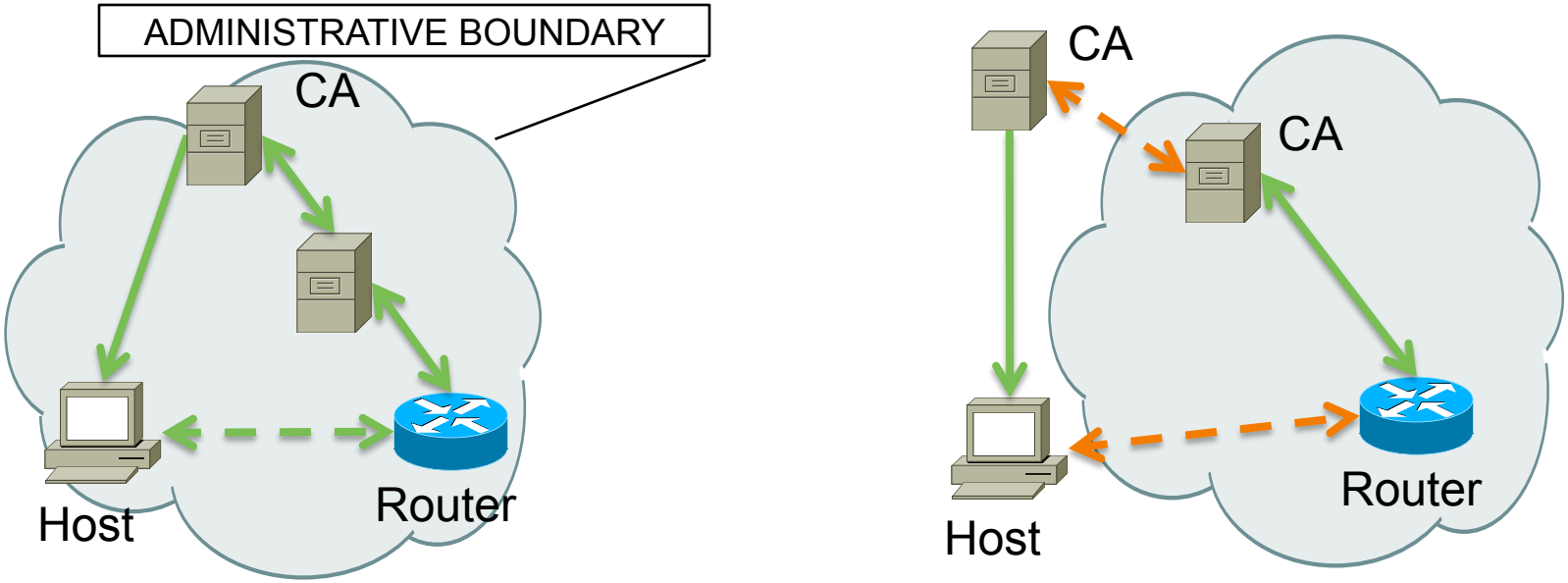
  Authorize routers to forward packets

  Authorize routers to advertise certain prefixes

Router Authorization for dummies



Deployment challenges



→ A chain of trust is “easy” to establish within the administrative boundaries, but very hard outside

→ To benefit fully from SeND, nodes must be:

- → Provisioned with CA certificate(s)
- → Time synchronized/have access to the NTP server
- → Have access to a CRL server

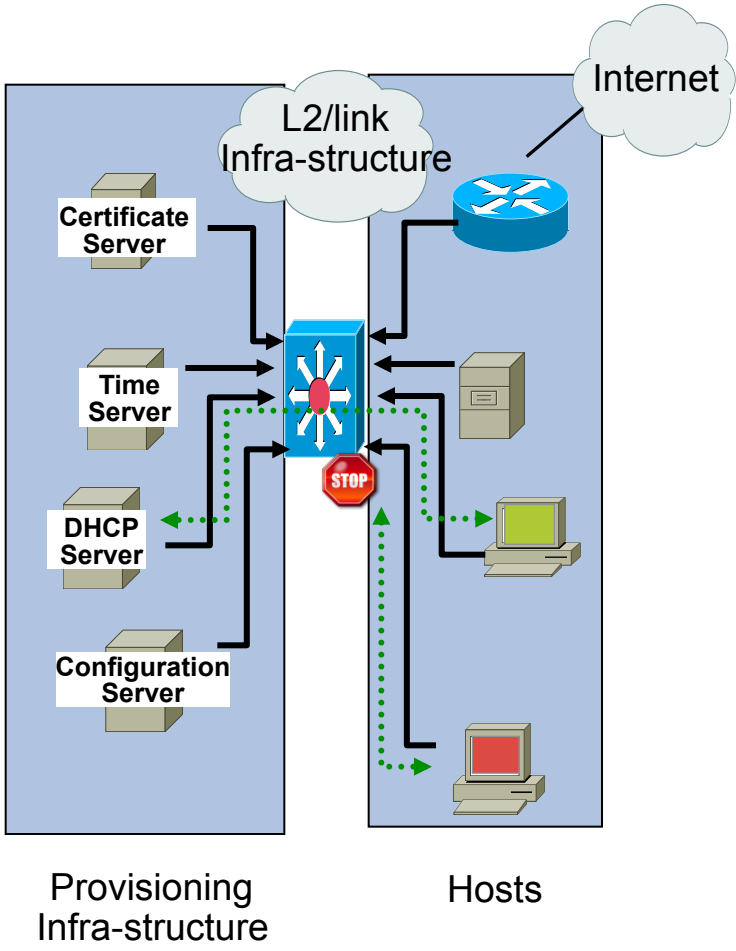
Agenda

- Terminology and other high level considerations
- Neighbor Discovery Protocol overview and vulnerabilities
- Distributed security :
  - SEcure Neighbor Discovery overview
  - SeND deployment challenges and pitfalls
- **Centralized security:**
  - IPv6 first-hop security overview
  - Deep Dive on ten most wanted First-Hop features
  - Deployment challenges and pitfalls
- IETF update
- Demo

Securing Link-operations In L2-infrastructure

- **Advantages**
  - central administration, central operation
  - Complexity and provisioning limited to first hop
  - All nodes protected
  - Transitioning lot easier

- **Disadvantages**
  - Applicable only to certain topologies
  - Requires first-hop to learn about end-nodes
  - First-hop can be a bottleneck and single-point of failure



Centralized Security ≡ smart switch

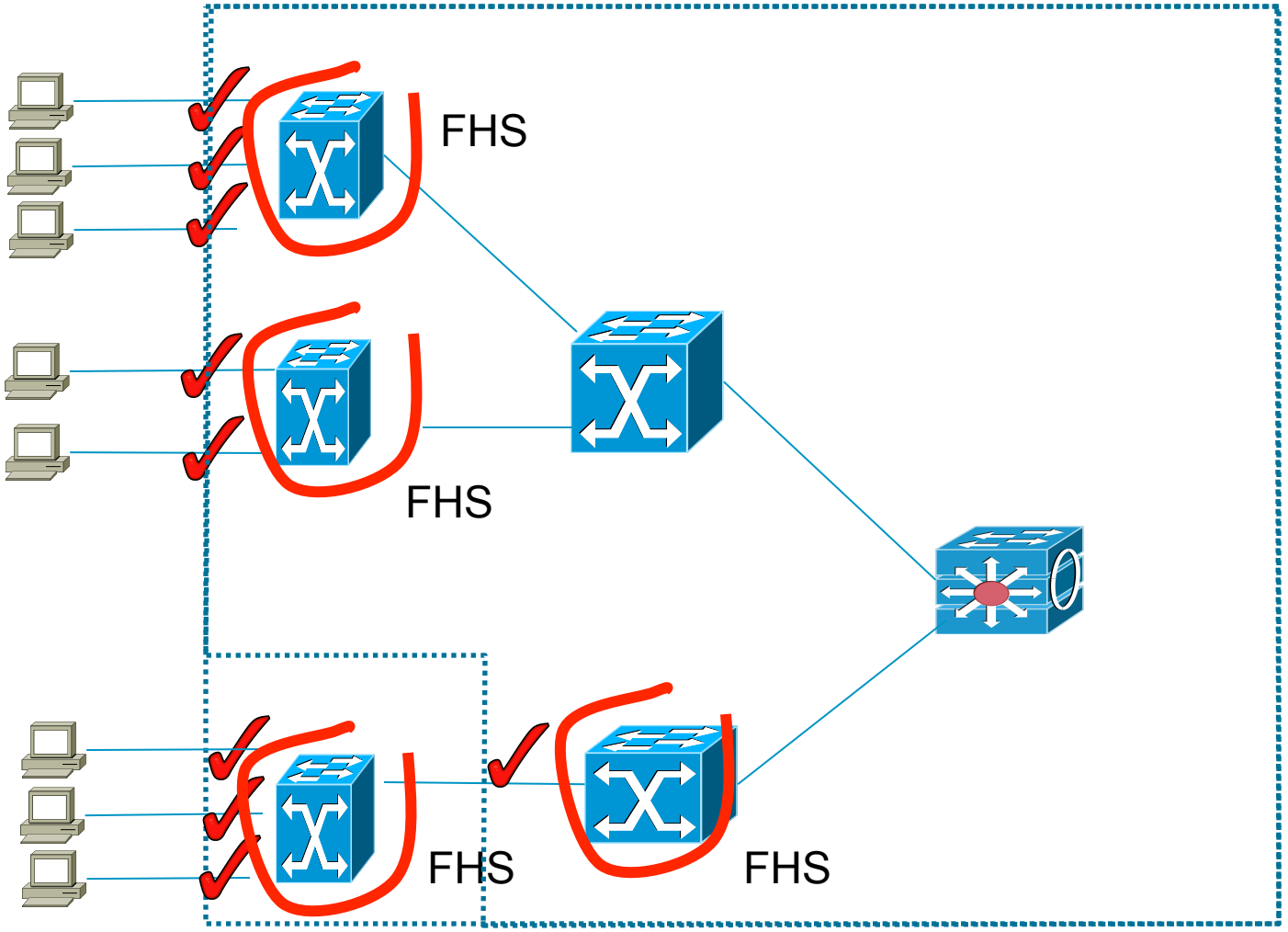
DOES

- Takes care of all nodes security, primarily from a link-operations standpoint
- With some incursions outside link-security
- Leverage information gleaned by snooping link-operations
- Arbitrage between different address assignment methods, different protocols, different nodes, different ports, etc.

REQUIRES

- Must be “in the centre” or
- Part of the security perimeter
- Required some provisioning
- Must be versatile (NDP, SeND, DHCP, MLD, etc.)

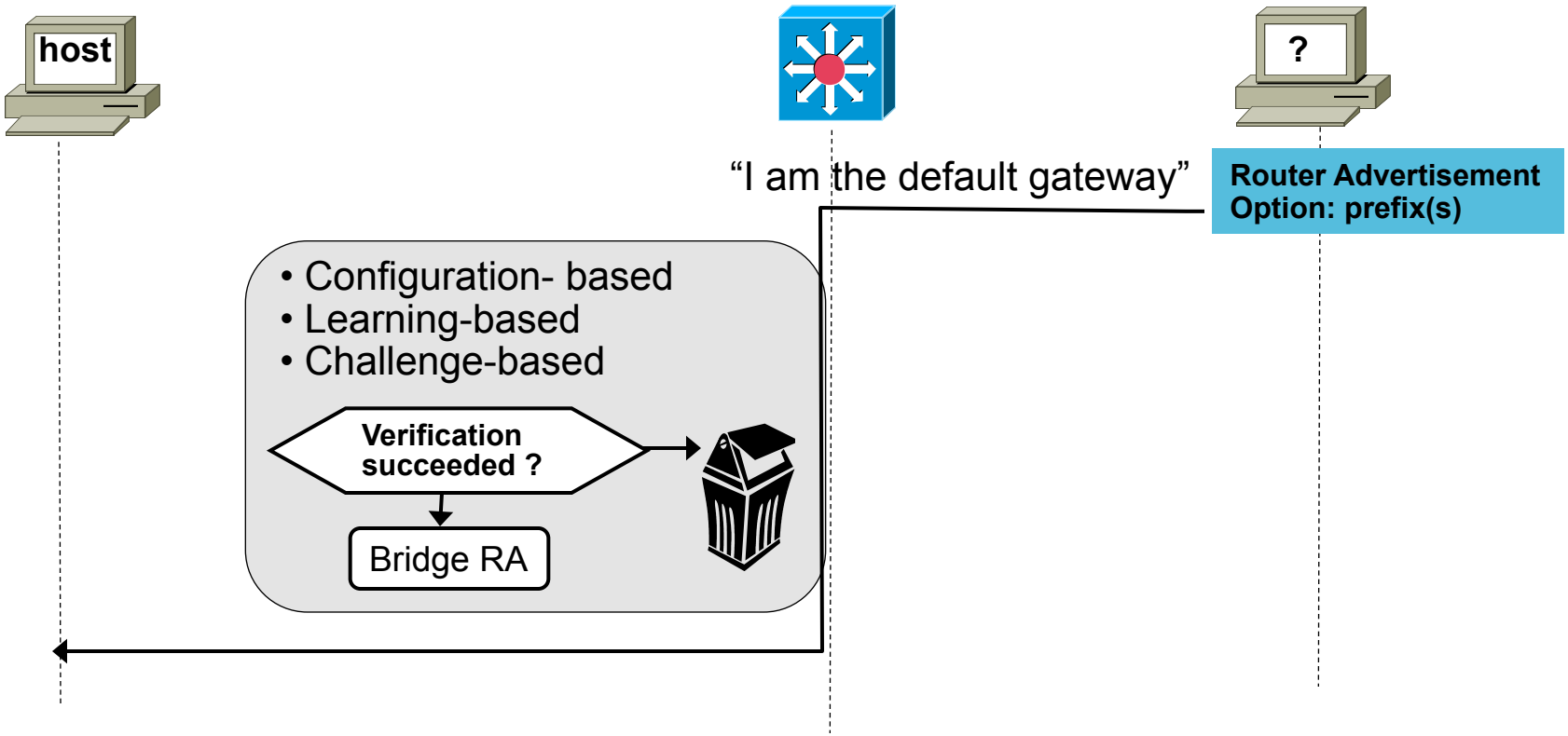
Security perimeter



10 most wanted features in IPv6 FHS

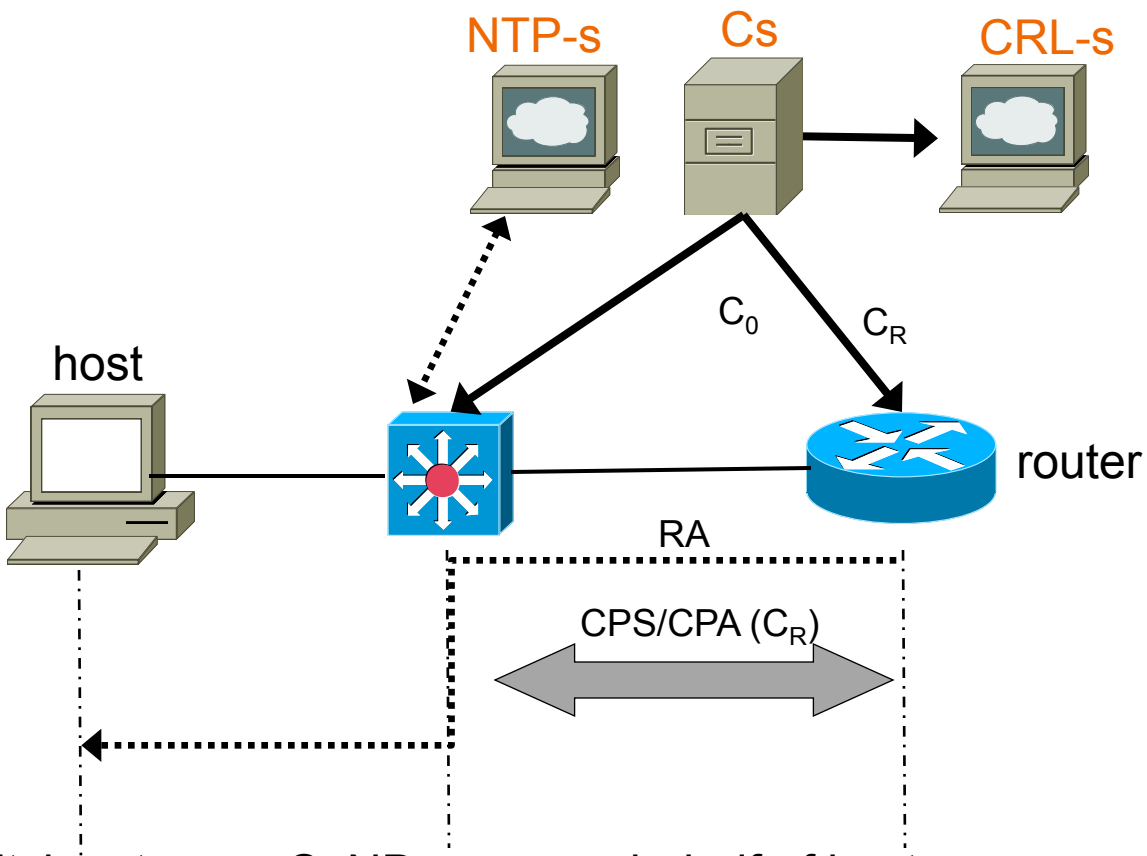
- The switch does/will integrate a set of monitoring, inspection and guard features for a variety of security-centric purposes:
  1. RA-guard
  2. NDP address glean/ inspection
  3. Address watch/ownership enforcement
  4. Device Tracking
  5. DHCP-guard
  6. Address Glean (NDP + DHCP + data)
  7. DAD/Resolution proxy
  8. Source-guard (SAVI)
  9. Destination-guard
  10. DHCP L2 relay
- It can leverage SeND for accrued security
- Can provide network “optimization” such as ND-suppress, RA-throttling or DAD-proxy

1 -RA-Guard



- Switch selectively accepts or rejects RAs based on various criteria's
- Can be ACL based, learning based or challenge (SeND) based.
- Hosts see only allowed RAs, and RAs with allowed content
- Stateful or stateless on the switch depending on the selection criteria's

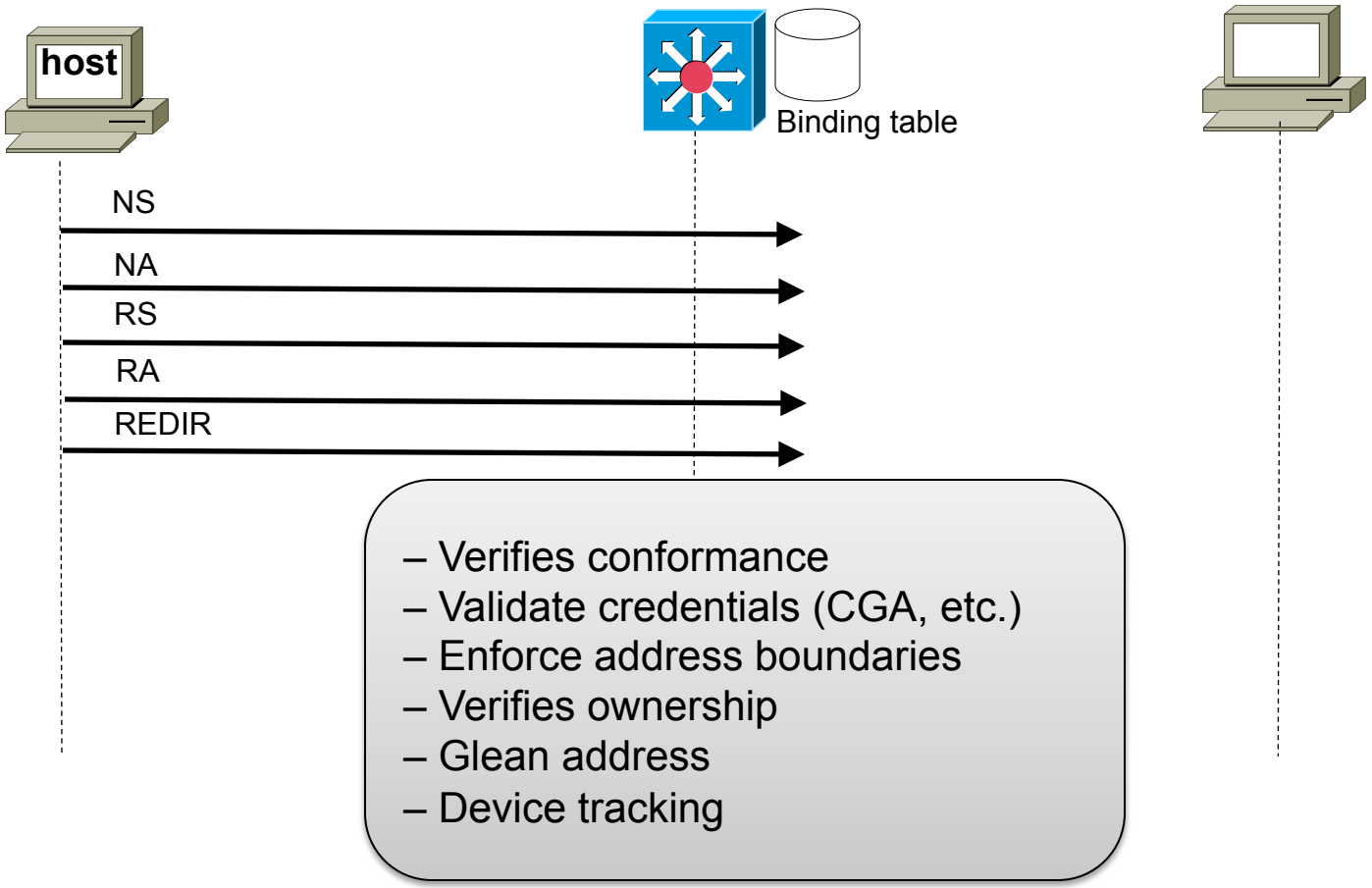
1- RA-guard Based On SeND (*)



- L2 switch acts as a SeND-proxy on behalf of hosts
- Transparent to the host
- Configuration/provisioning applies only to the switch
- Trust established at layer3 and above: no dependency on the topology
- Applies regardless on the router location (access port, trunk port, etc.)

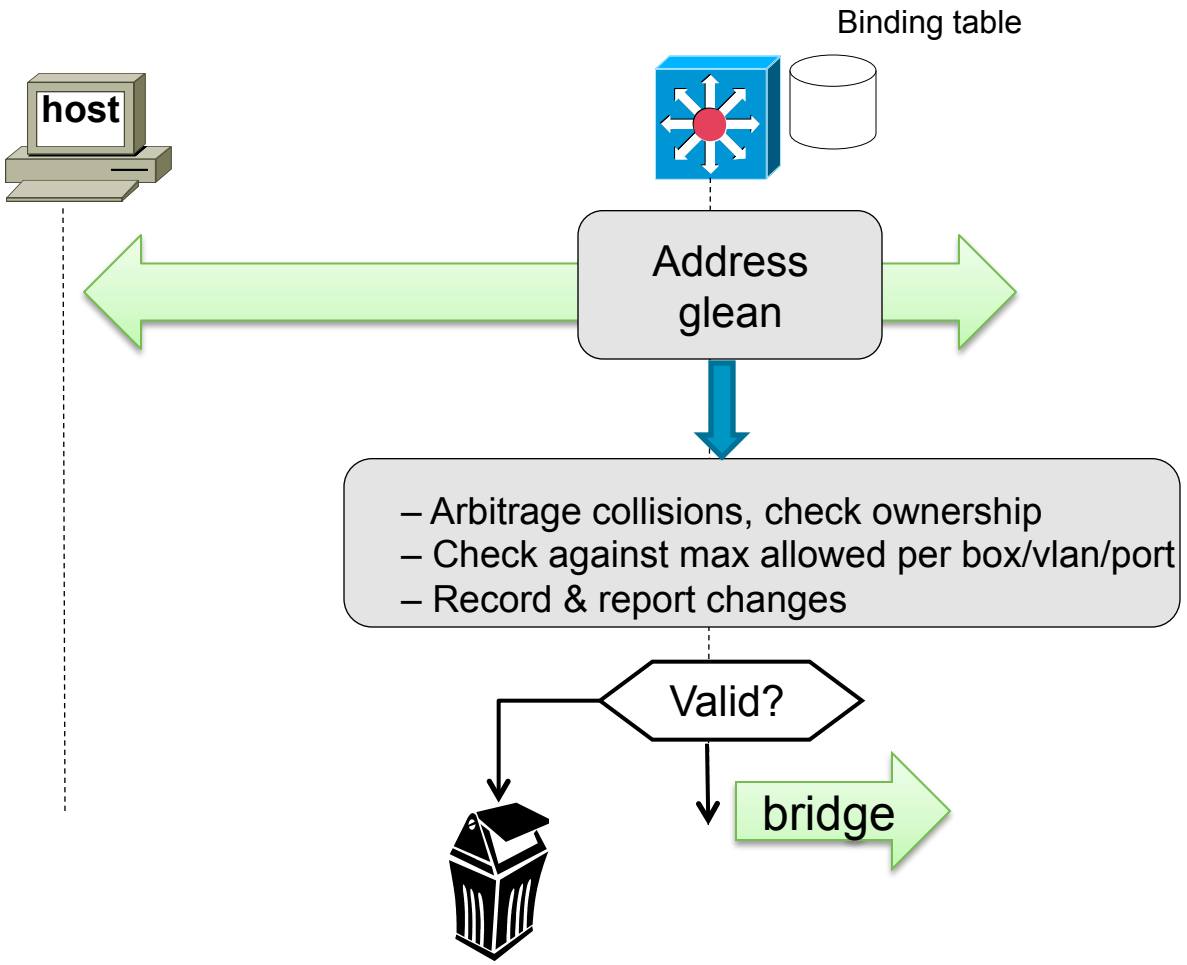
*Radar

2 - NDP address glean/inspection

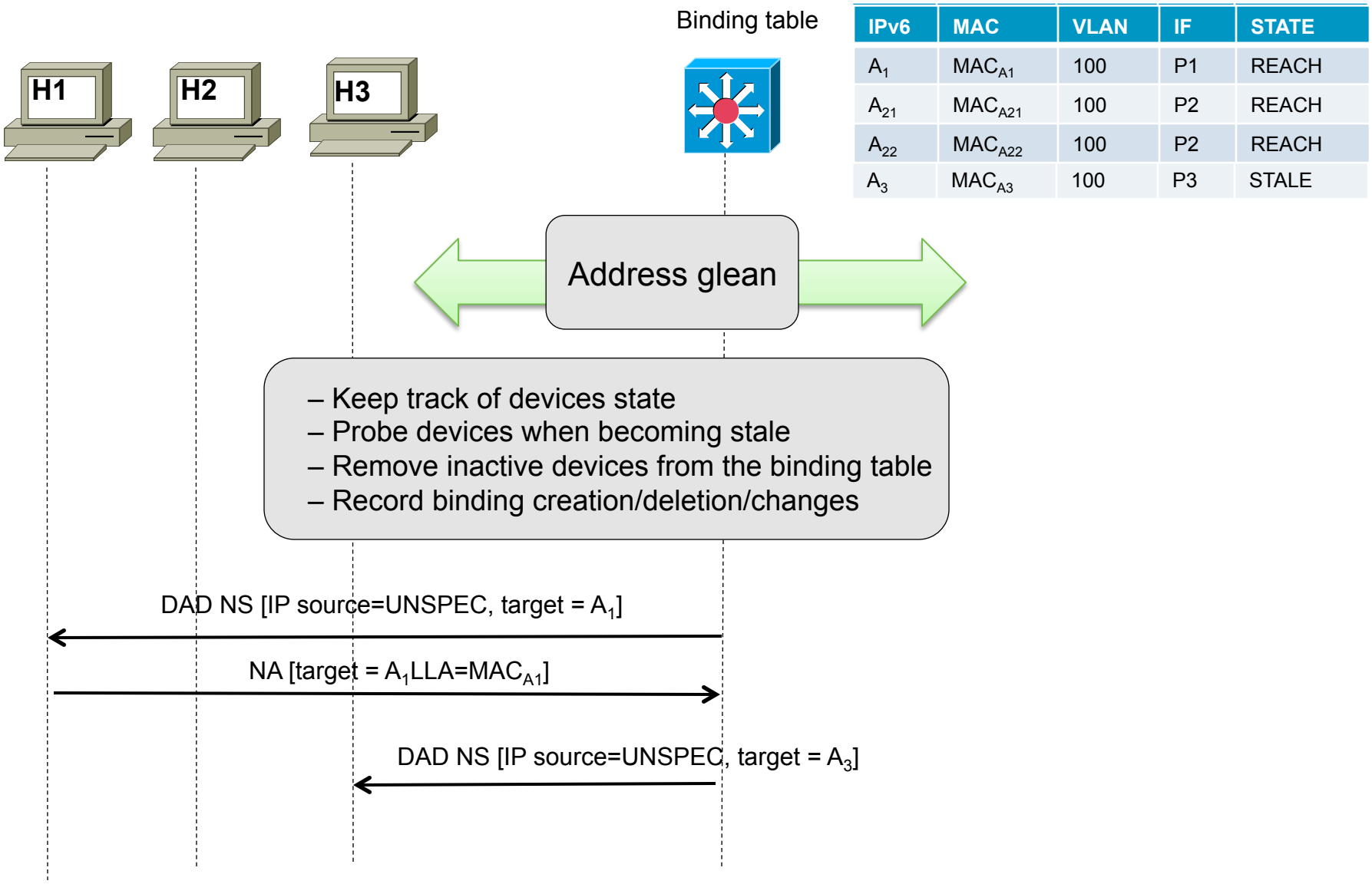


IT'S A BUNDLE !

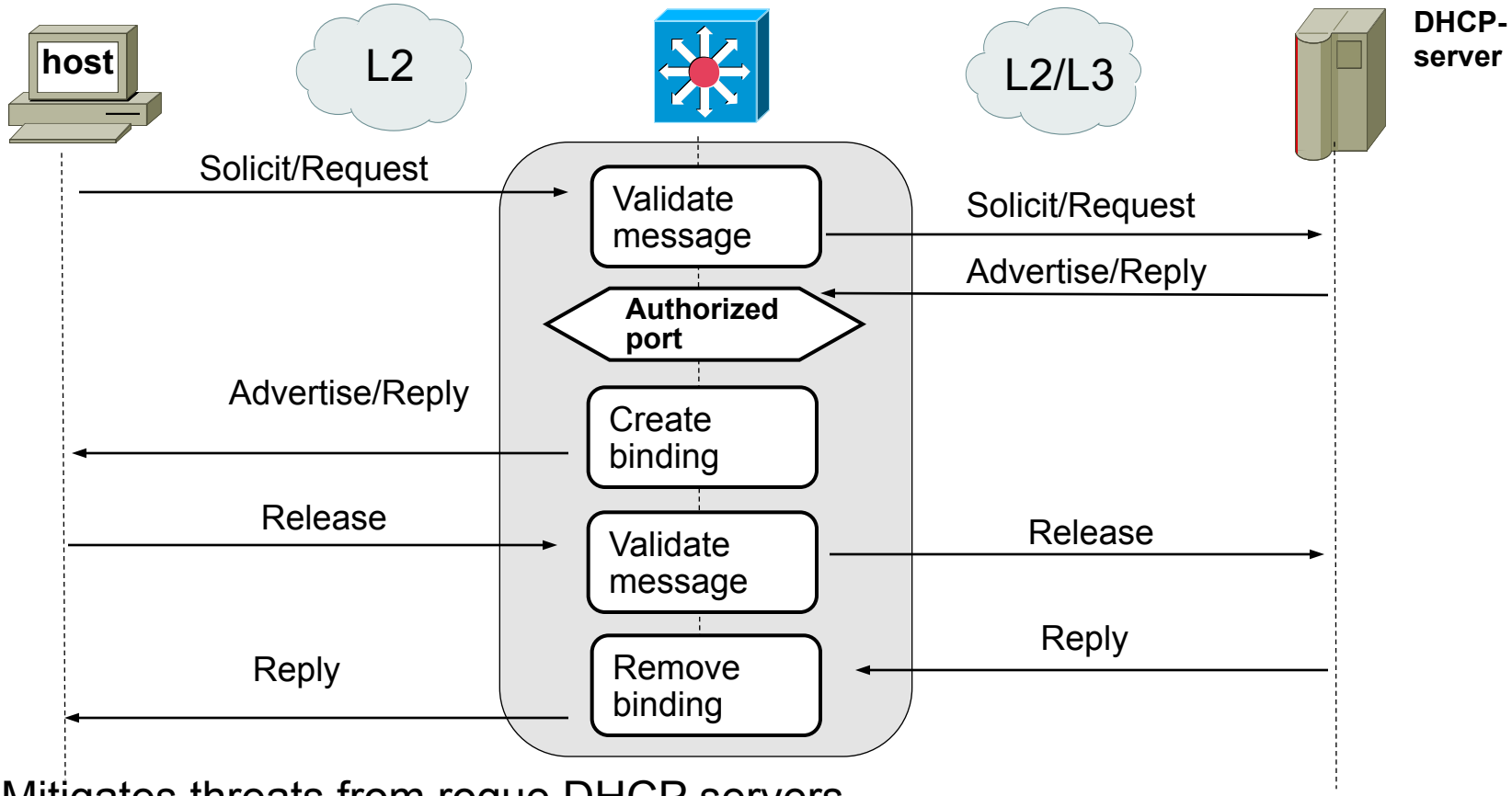
3 - Address-watch



4 - Device tracking

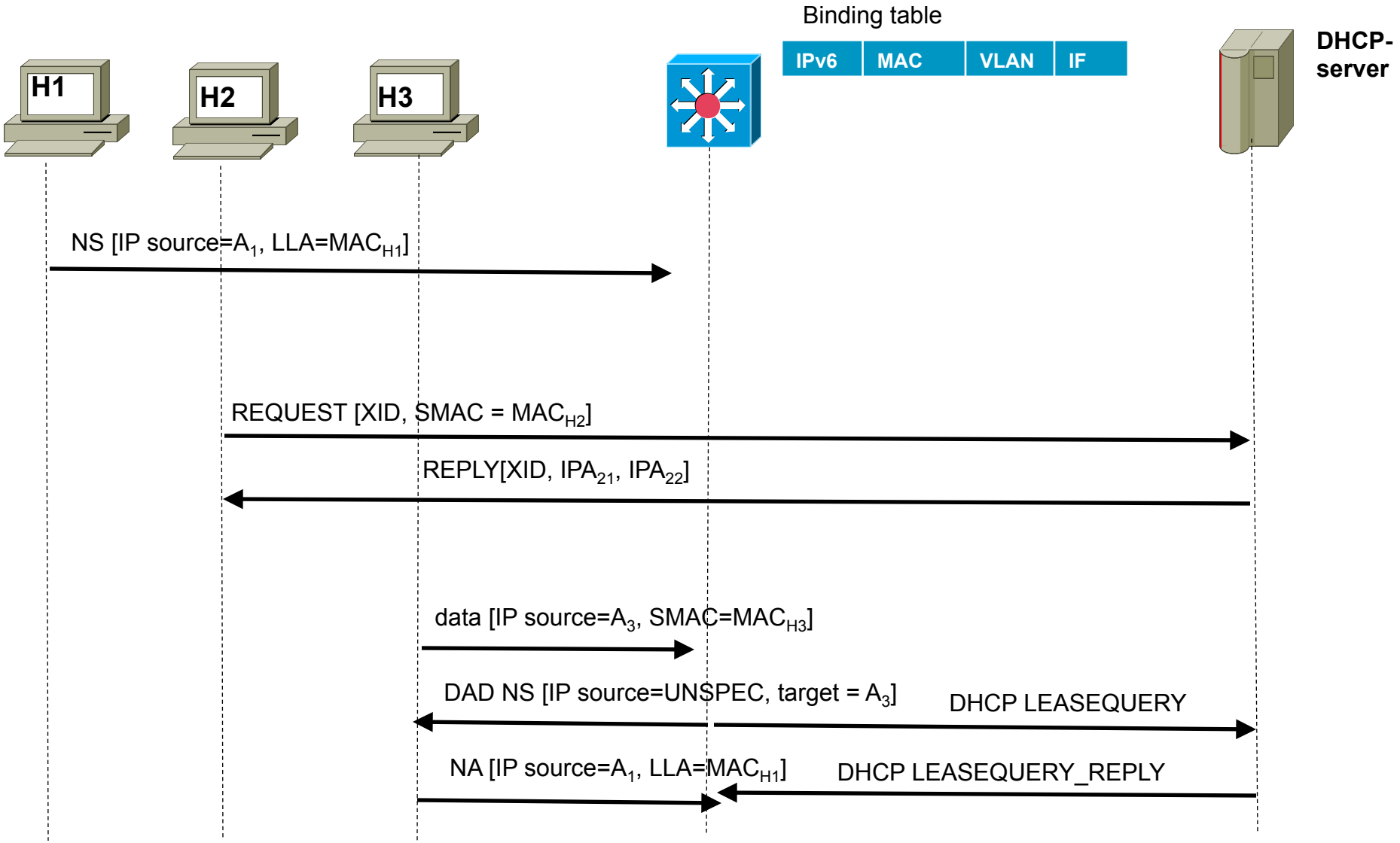


5- DHCP Guard

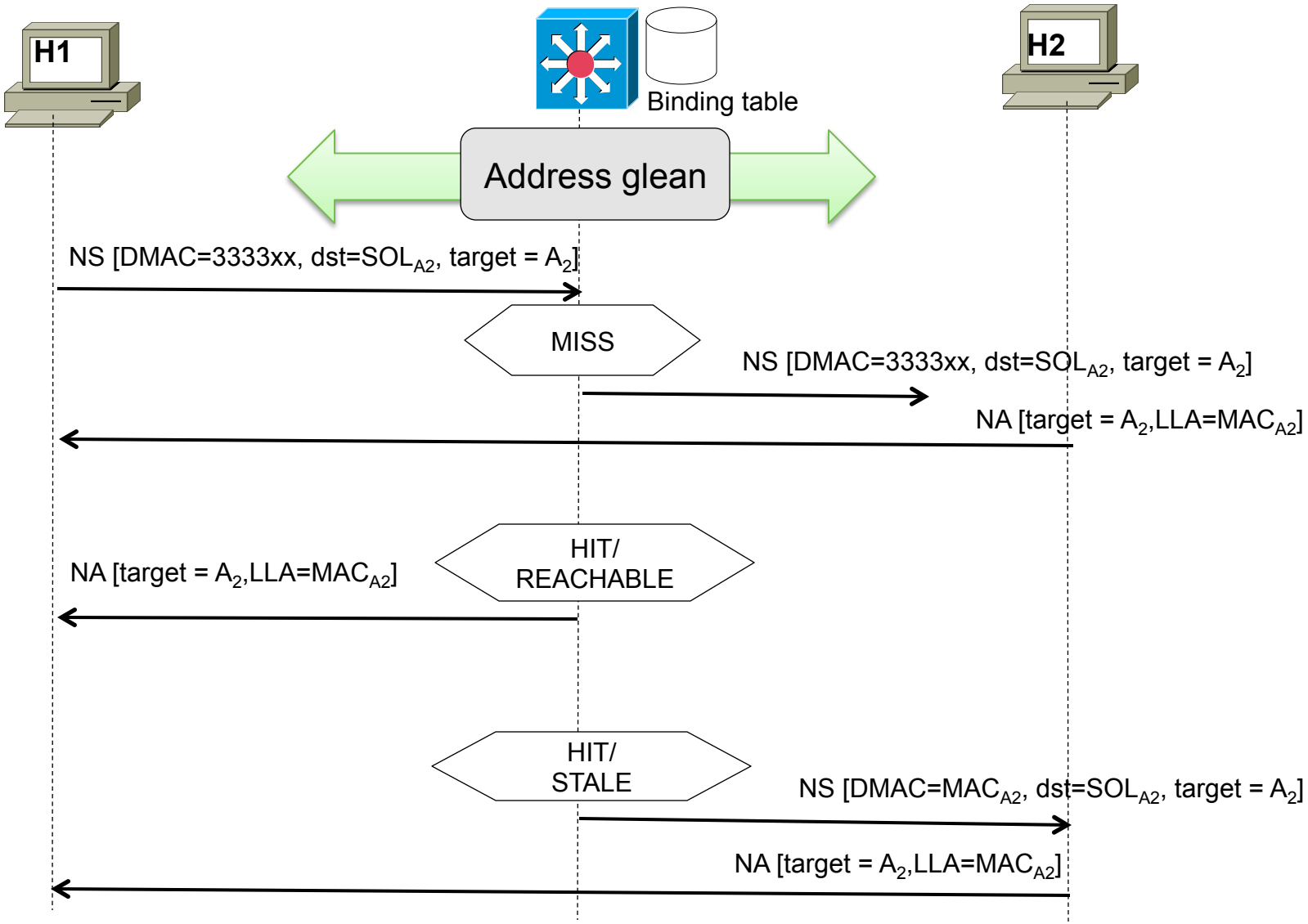


- Mitigates threats from rogue DHCP servers
- Learns and secures bindings for Stateful DHCP assigned addresses
- Switch intercepts DHCP messages, validate and filters invalid messages
- Limit broadcast of messages to select ports only
- Insert DHCP options to influence address allocation by servers
- Secure Port ←→LLA ←→ IPA binding in binding table

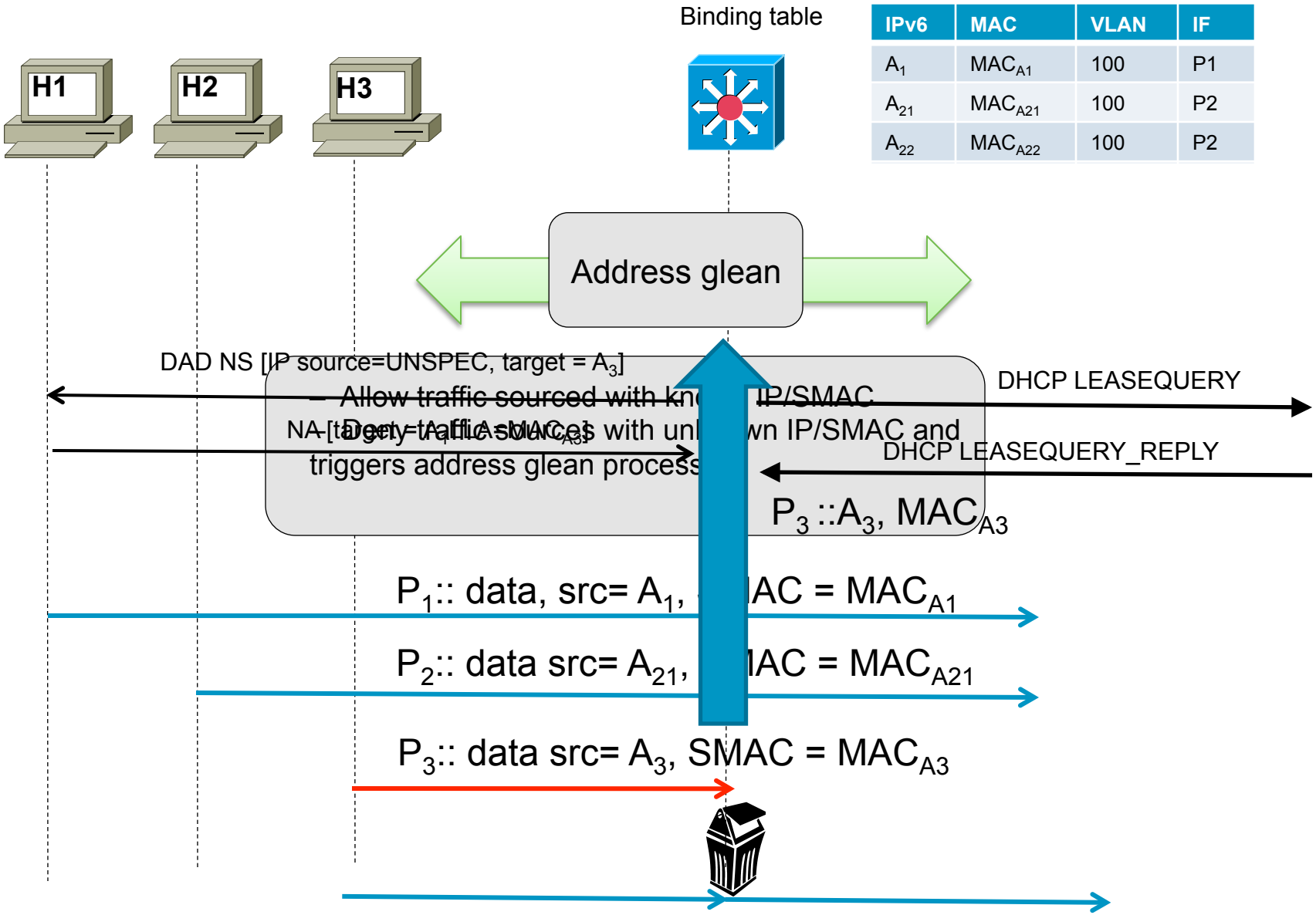
6 - Address GLEAN



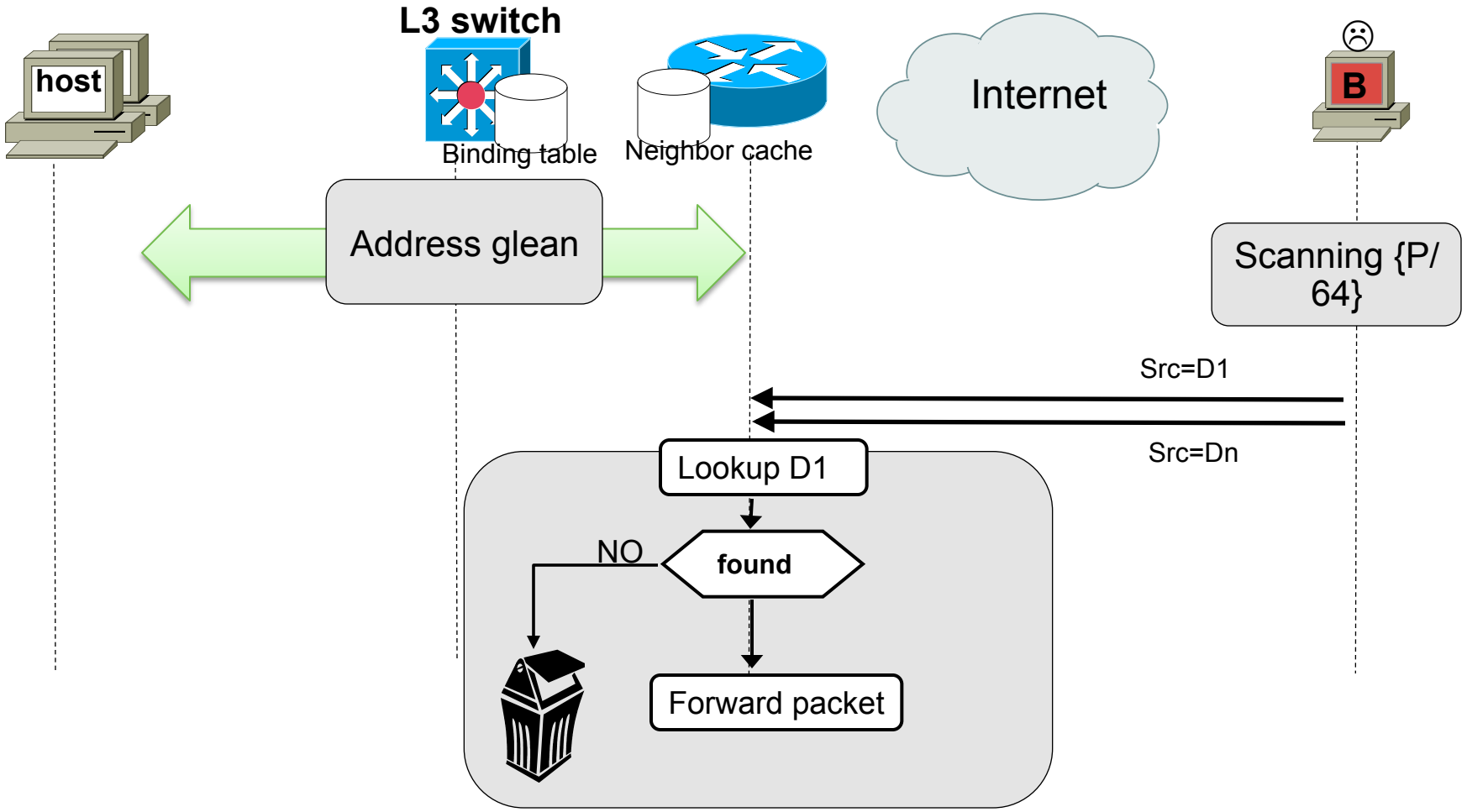
7– DAD/Resolution proxy



8- IP-Source Guard

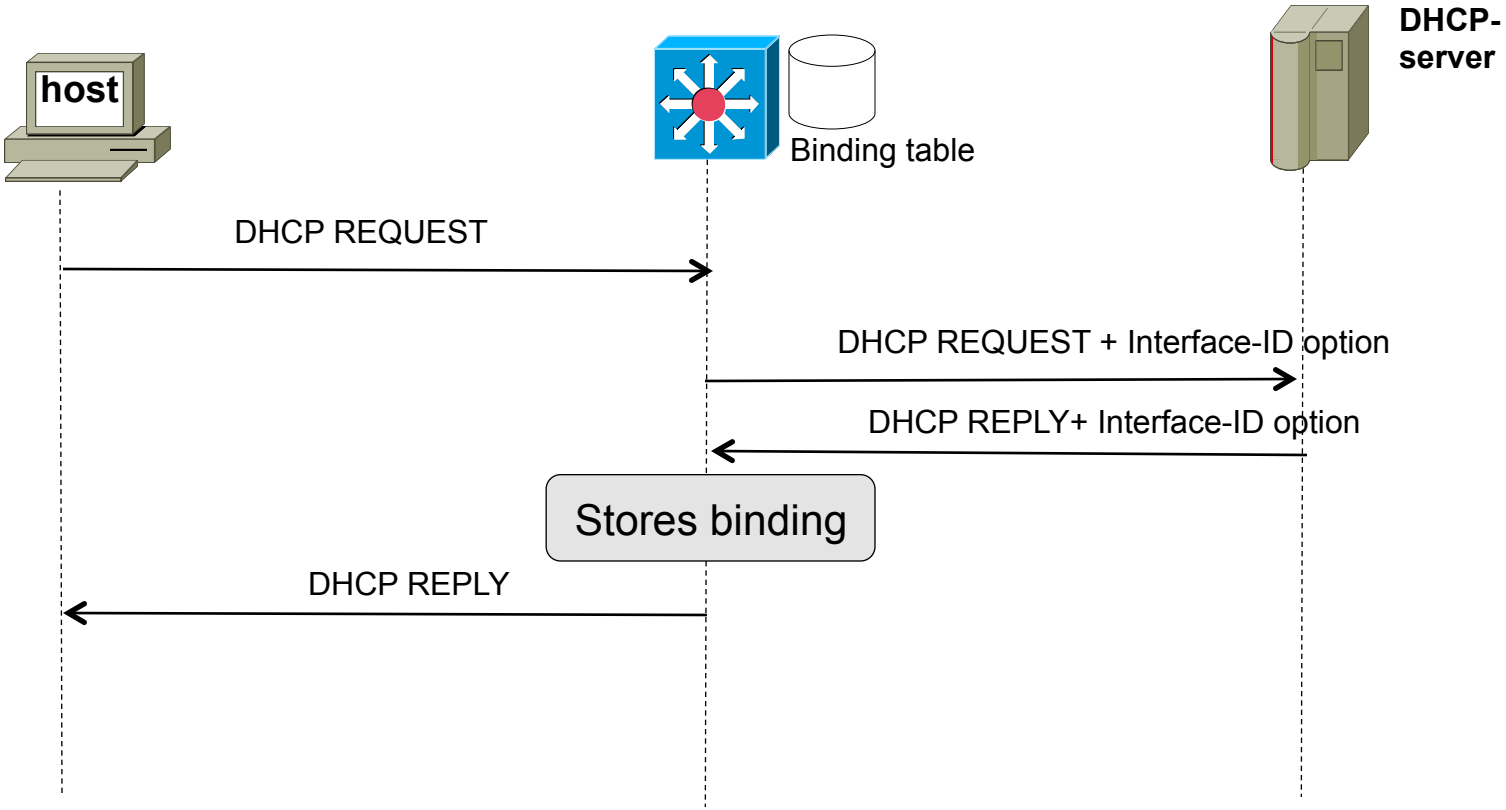


9- IP-Destination Guard



- Mitigate prefix-scanning attacks and Protect ND cache
- Useful at last-hop router and L3 distribution switch
- Drops packets for destinations without a binding entry

10- DHCPv6 L2 relay



Agenda

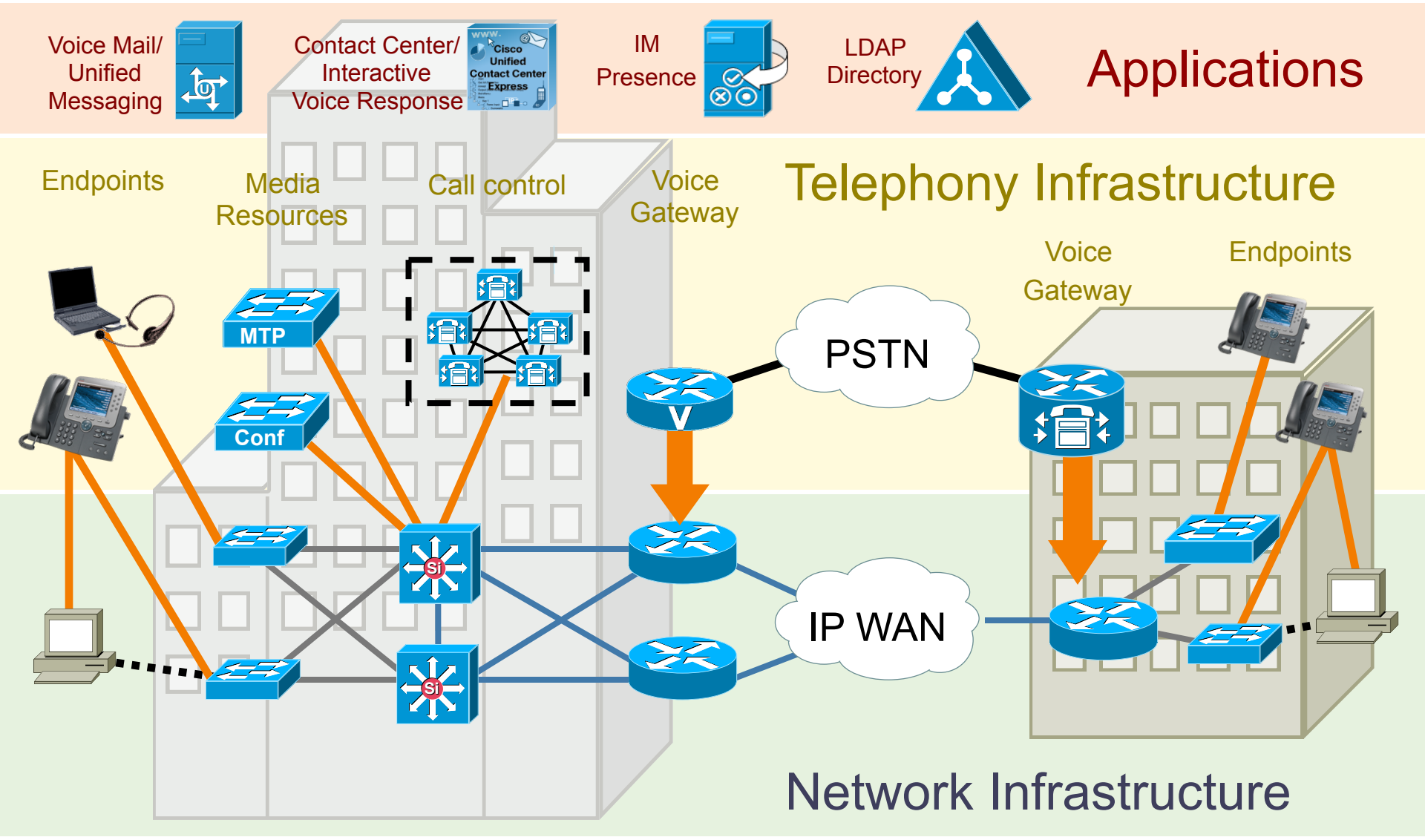
- Introduction
- IPv6 in the Enterprise
- Routing Considerations
- Security for IPv6
- First Hop Security
- Unified Communications
- Multicast
- DNS
- Deployment and Operation Considerations

IPv6 – Unified Communications

Agenda

- Intro UC
- IPv6 and UC features summary
- IPv6 Addressing and Cisco UC devices
- CUCM IPv6 Device Configuration and Media Handling
- Other IPv6 Design Considerations
- Summary

Unified Communications Network



Glossary

- **CUCM**: Cisco Unified Communications Manager; multi-protocol call-control agent (SIP, h.323, SCCP, MGCP, …)
- **CARS**: Common Application Run-time Service. CARS is a very thin, very secure, appliance container built on a x86_64 Linux kernel from a CentOS base. It provides a Cisco IOS-like CLI shell. Since 2005 CARS has been the foundation of several Cisco UC products.
- **MTP**: Media Termination Point. Used to terminate and re-initiate media legs; for example receives media in IPv4 and re-sends in IPv6
- **ANAT :** Alternative Network Address Types (RFC 4091)
- **SBC**: Session Border controller. Used to separate UC networks into logical domain.
- **SCCP**: Skinny Call-control Protocol; Cisco's client server call signaling
- **AXL**: AVVID XML Layer API. It's a mechanism for inserting, retrieving, updating, and removing data from the database using an XML/SOAP interface
- **CTI**: Computer Telephony Integration
- **MOH**: Music on hold

Icons & Terminology

IPv4 Only

Device communicates with and understands IPv4 addresses only

IPv6 Only

Device communicates with and understands IPv6 addresses only

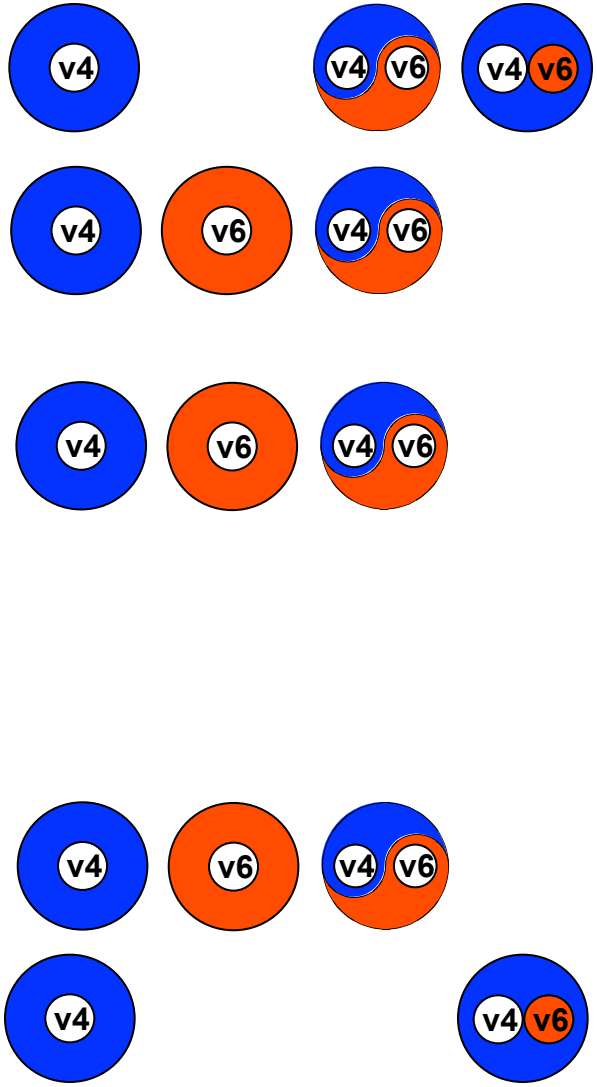
Dual Stack – IPv4 and IPv6

Device communicates with and understands both IPv4 and IPv6 addresses

IPv6 Aware

Device communicates with IPv4 addresses, but can receive and understand IPv6 addresses embedded in Application PDUs – Typically used by applications which use IPv4 to transport IPv6 information

IPv4 and IPv6 for UC support



- **Cisco Unified Communications Manager 7.1(2)** and above
- **The following Cisco IP Phones with SCCP firmware**

  7906G, 7911G, 7931G, 7941G, 7941GE 7942G, 7945G, 7961G, 7961GE 7962G, 7965G, 7970G, 7971G-GE, 7975G

  Support with SIP firmware will be extended by the end of 2011 (with UCM 9.0)
- **Gateways**

  SIP Gateways (ISR 28XX & 38XX, ISR 29XX & 39XX, ASR1k, AS5400)

  VG224 SCCP Analogue Gateway

  SCCP FXS ports on ISR routers

  IOS MTPs for IPv4 - IPv6 RTP Media conversion

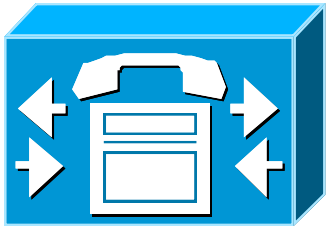
  Cisco Unified Border Element (SBC)
- **CUCM SIP Trunks**
- **Applications**

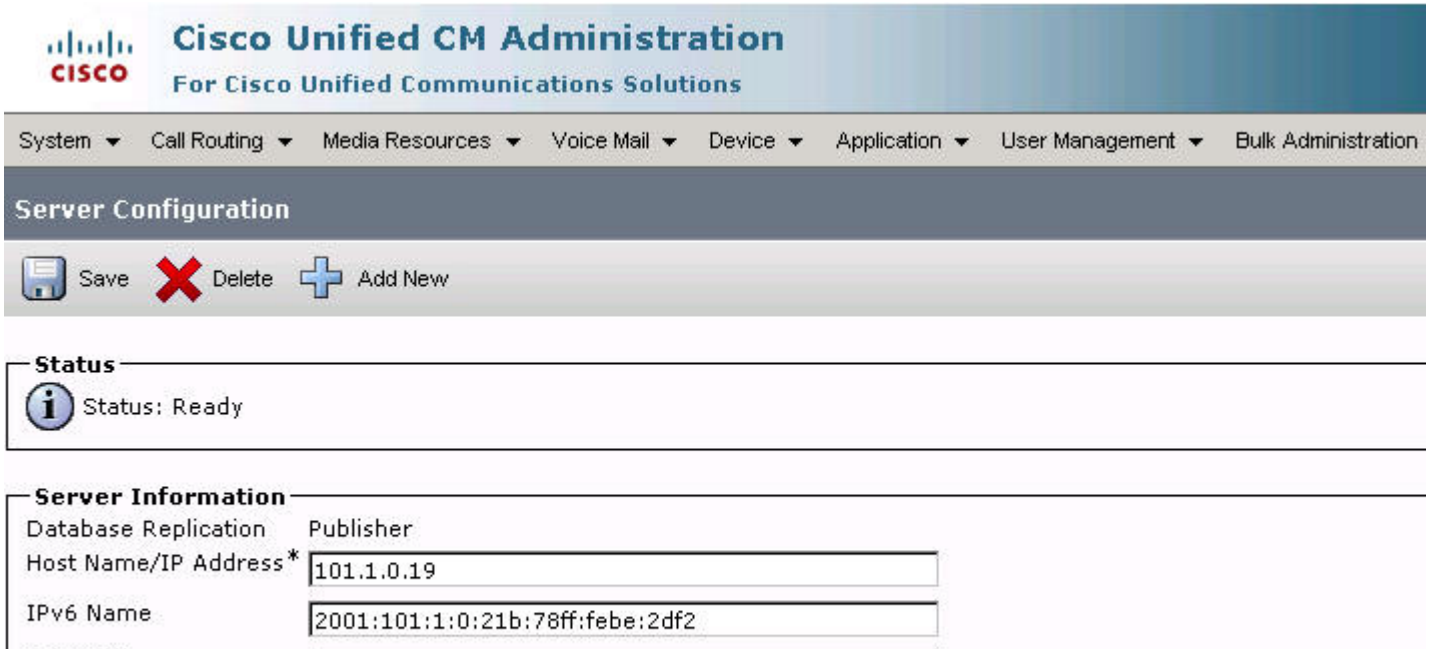
  CUCM : CTI, AXL/SOAP, SNMP - IPv6 aware

  Unity Connection 8.5(1) and above

Cisco Unified Communications Manager IPv6 Addressing

- CUCM can support :
  - One Link Local Address and
  - One Unique Local Address or
  - One Global Address
  - (and an IPv4 address)





IP Phone – IPv6 Addressing

- IP Phones can support :
  - One Link Local Address and
  - Multiple Unique Local Addresses
  - Multiple Global Addresses
  - (and an IPv4 address)
- IP Phone will use one IPv6 address (Global or Unique Local) for signaling and media.

IP Phone – IPv6 Addressing

Additional information

- IP Phones can support a combination of up to 20 Addresses (Global or Unique Local)
- IP Phone Address selection priority :
  1) If configured, use the address that has been manually configured via the Phone's UI
  2) If an address has not been manually configured, use DHCPv6 to assign an address
  3) If neither a DHCPv6, nor a manually configured address is available, and Auto Configuration (SLAAC) is enabled for the Phone (CUCM default = On) - The phone will use SLAAC to create an IPv6 address. Router RA "O" bit should be set.
- A Link Local address will never be sent to CUCM as a signaling and media address
- If the phone has both Unique Local and Global addresses, the Global Addresses take precedence over Unique Local Addresses.
- If multiple Unique Local or multiple Global addresses exist - the first address configured will be used as the signaling and media address sent to CUCM

CUCM Configuration for IPv6

- Server Platform IPv6 Address configuration
- UC server IPv6 Address configuration
- CUCM IPv6 Cluster wide configuration
- IPv6 Device Specific configuration parameters
- Common Device configuration
- SIP Trunk configuration
  - SIP ANAT and CUCM Trunk Operation

UC Server Ethernet Port IPv6 address Configuration

To allow IPv6 based call processing – IPv6 must first be enabled throughout the cluster.

This involves two steps:

1) Configuring IPv6 via the OS CLI or CUCM **OS** GUI on each server in the cluster
2) Configuring IPv6 via the CUCM GUI Server Configuration (next slide)

Server OS Admin CLI commands :

To enable IPv6 :

```
set network ipv6 service enable"
```

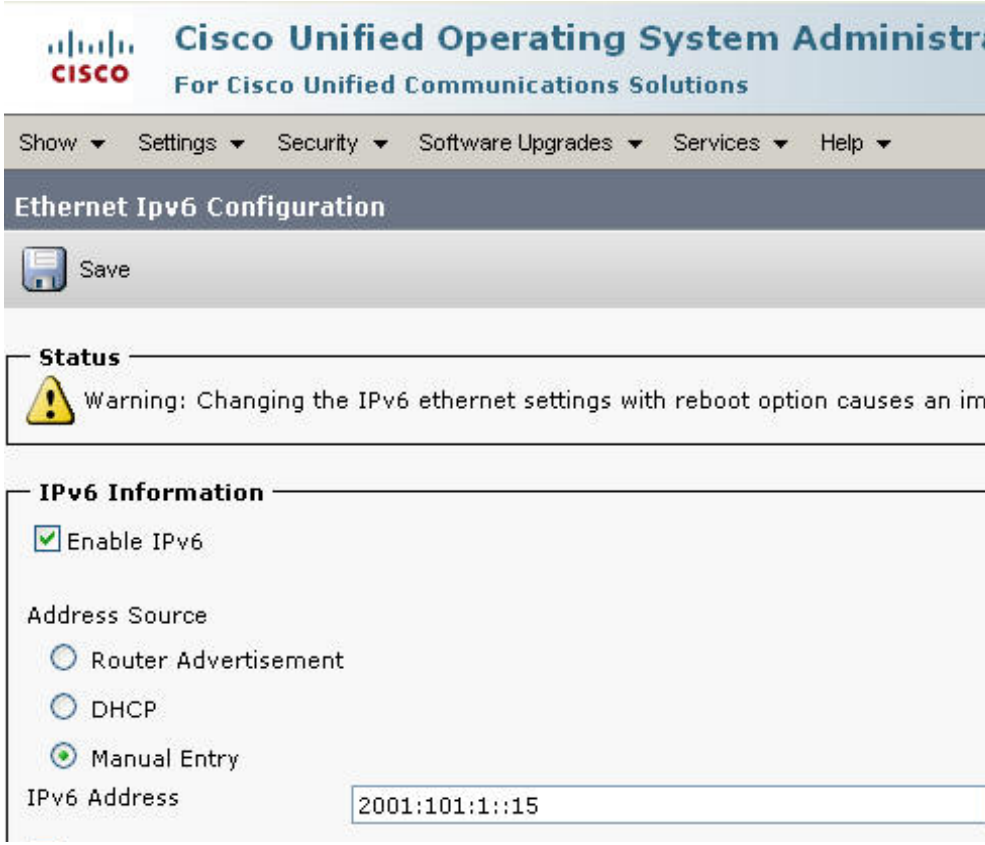
To set a static IPv6 server address :

```
set network ipv6 static_address <addr> <mask>
```

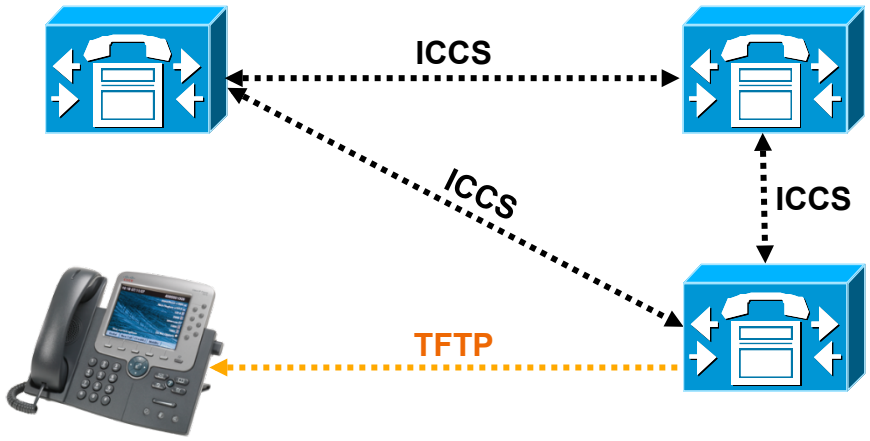
To view IPv6 address settings :

```
show network ipv6 settings
```

Static IPv6 addressing is recommended.



CUCM Server - IPv6 Address Configuration

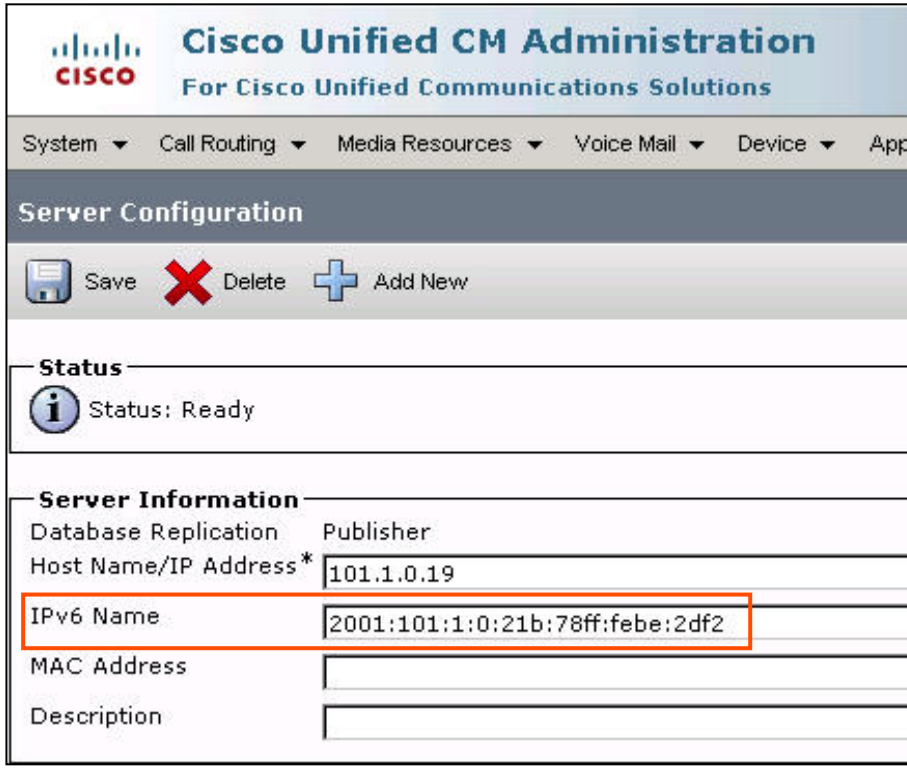


Configure an IPv6 address or name

If a name is used, DNSv6 is required

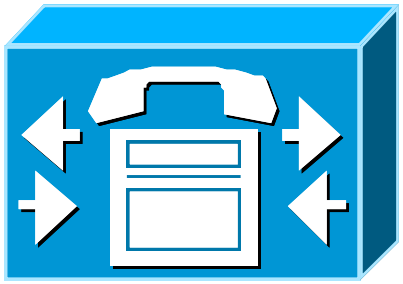
The IPv6 address is used by the TFTP server in the configuration files that are sent to devices.
The address is used by these devices for CUCM registration.

Between servers in the cluster, the addresses are used for ICCS (Intra-Cluster Communication Signaling)

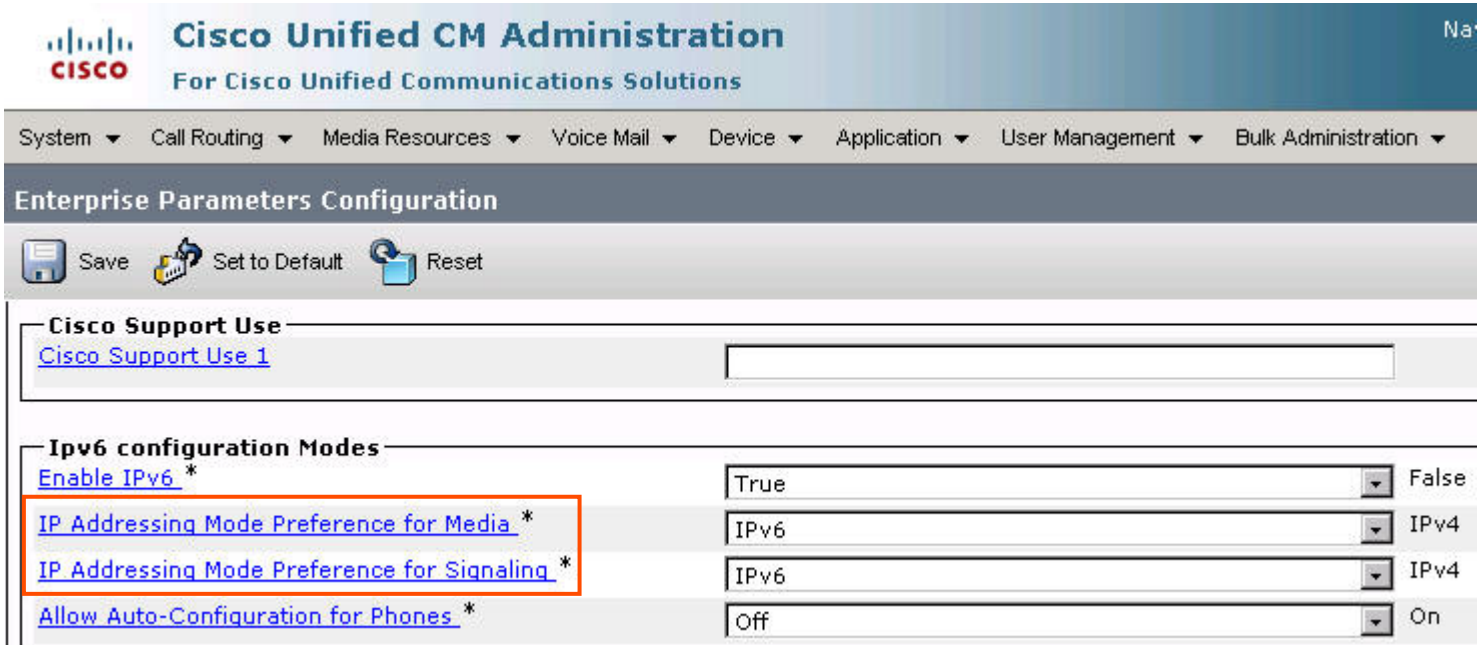


CUCM Enterprise Parameters for IPv6

Enable IPv6 Cluster-wide via CUCM GUI



Configure Cluster-wide :
IP Addressing Mode Preference for Media
IP Addressing Mode Preference for Signalling
Allow Auto-Configuration for Phones (SLAAC)



Signalling Preference and Phone Auto Configuration settings are also configurable at the device (or group of device) level – Device setting takes precedence

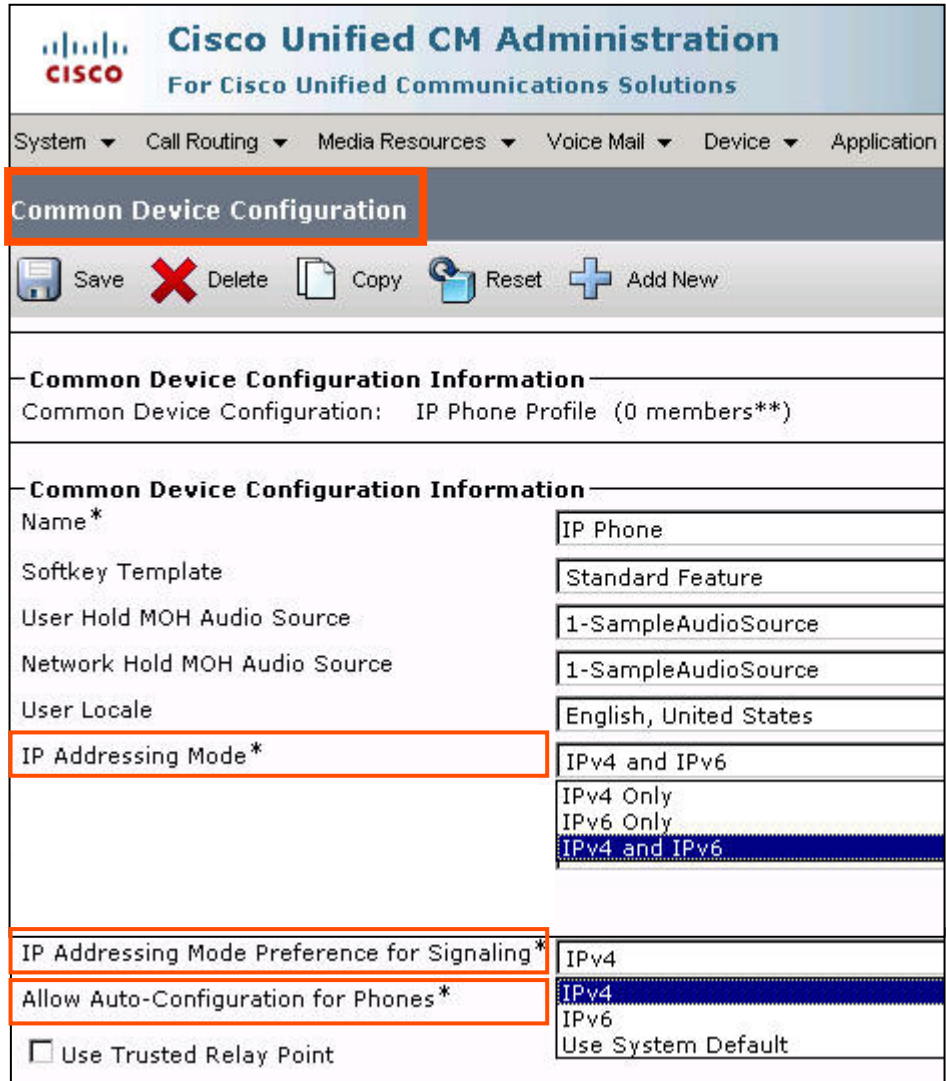
CUCM Common Device Configuration

The Common Device Configuration is a configuration template that can be applied to Phones and Trunks.

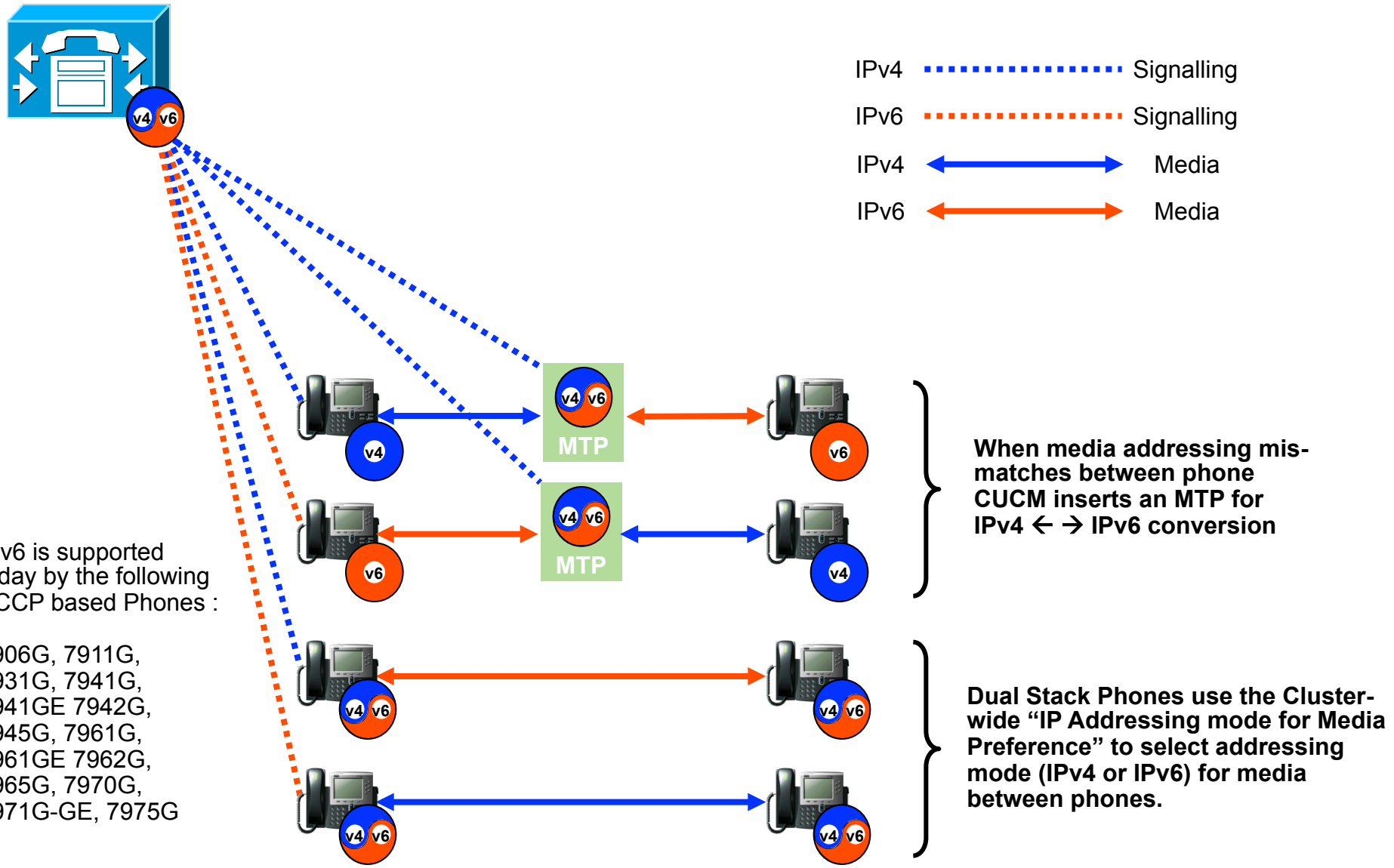
IP Addressing Mode:
IPv4 Only - Device uses one IPv4 address only
IPv6 Only - Device uses one IPv6 address only
IPv4 and IP6 - Device uses one IPv4 address and one IPv6 address

IP Addressing Mode Preference for Signalling:
IPv4 only
IPv6 only
System Default

Allow Auto Configuration For Phones :
On
Off
Default



CUCM Phone Signaling and Media Options



IPv6 is supported today by the following SCCP based Phones :

7906G, 7911G, 7931G, 7941G, 7941GE 7942G, 7945G, 7961G, 7961GE 7962G, 7965G, 7970G, 7971G-GE, 7975G

CUCM SIP Trunk Configuration

Common Device Configuration – Applies Addressing Mode and Signalling preference settings

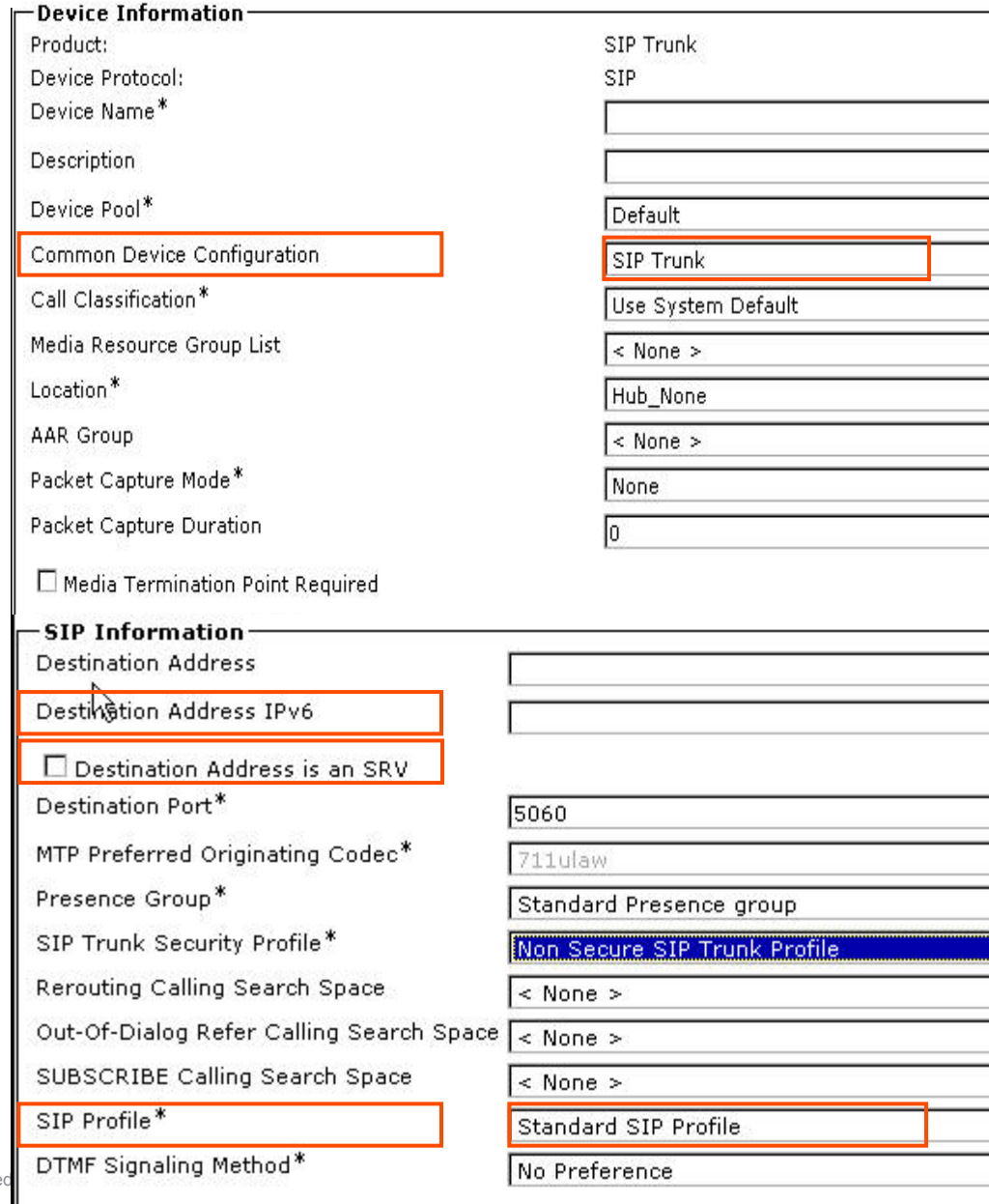
Recommended Addressing Mode : IPv4 and IPv6

SIP Early Offer or Delayed Offer with ANAT or without ANAT

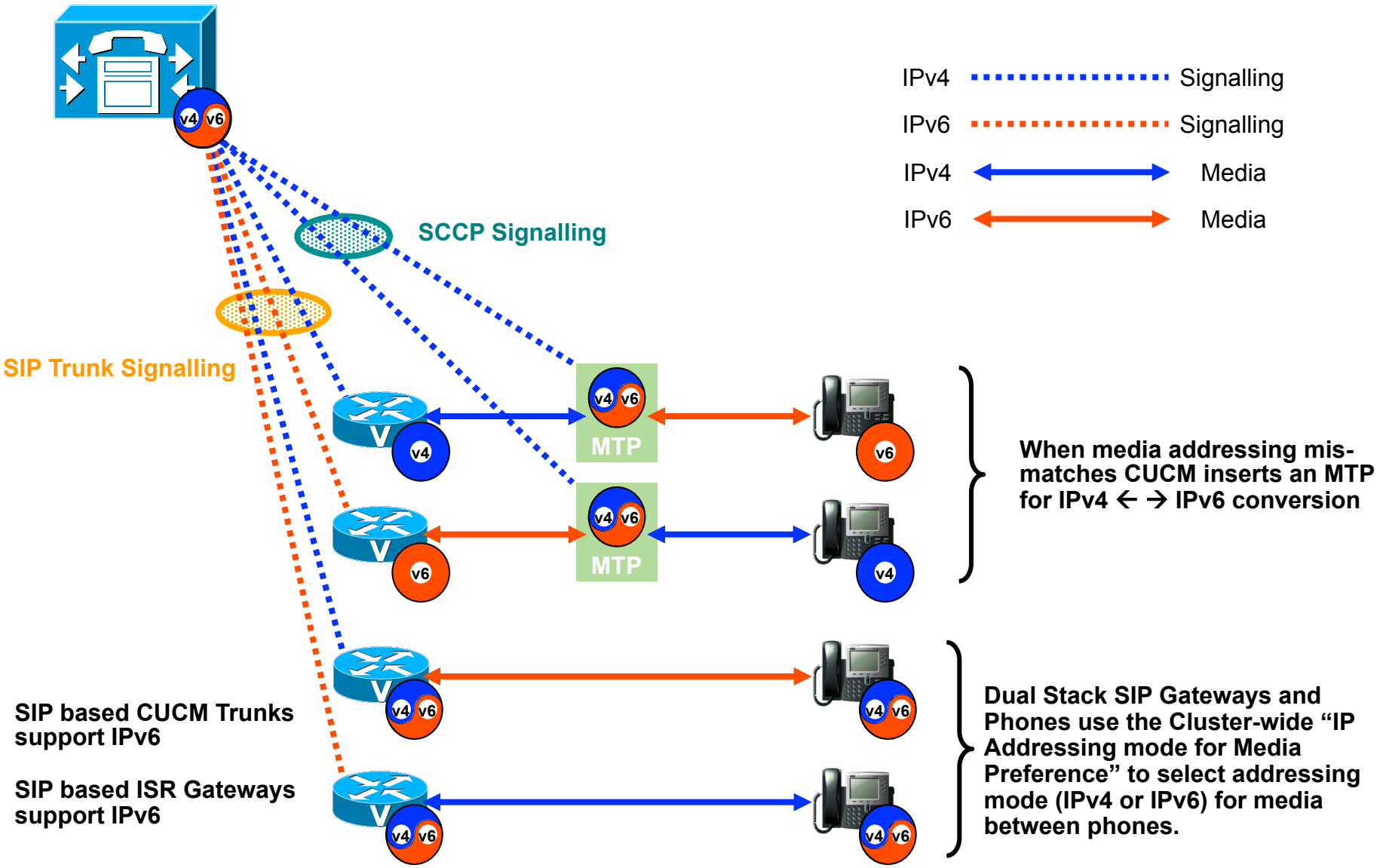
IPv6 Destination Addresses

If IPv6 Destination Address is an SRV – cluster wide DNSv6 address must be configured

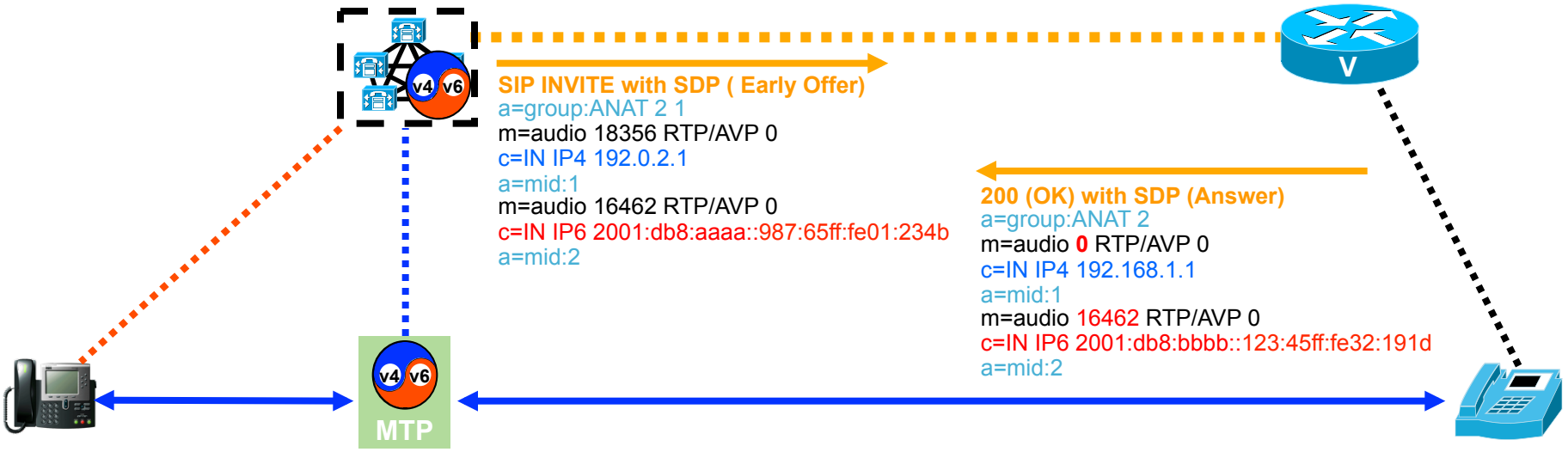
SIP Profile – Applies ANAT setting



CUCM SIP Trunks Signaling and Media Options



SIP Gateways and Trunks
Alternative Network Address Types (ANAT)

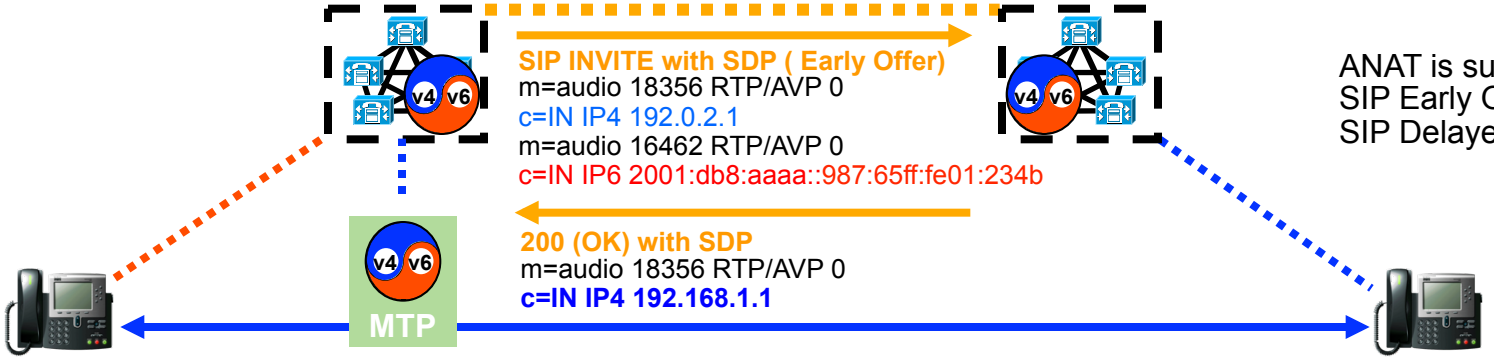


ANAT allows both IPv4 and IPv6 addresses to be exchanged in the SIP Offer and SIP Answer
The Options field of the SIP Invite can indicate whether ANAT is Required or Supported

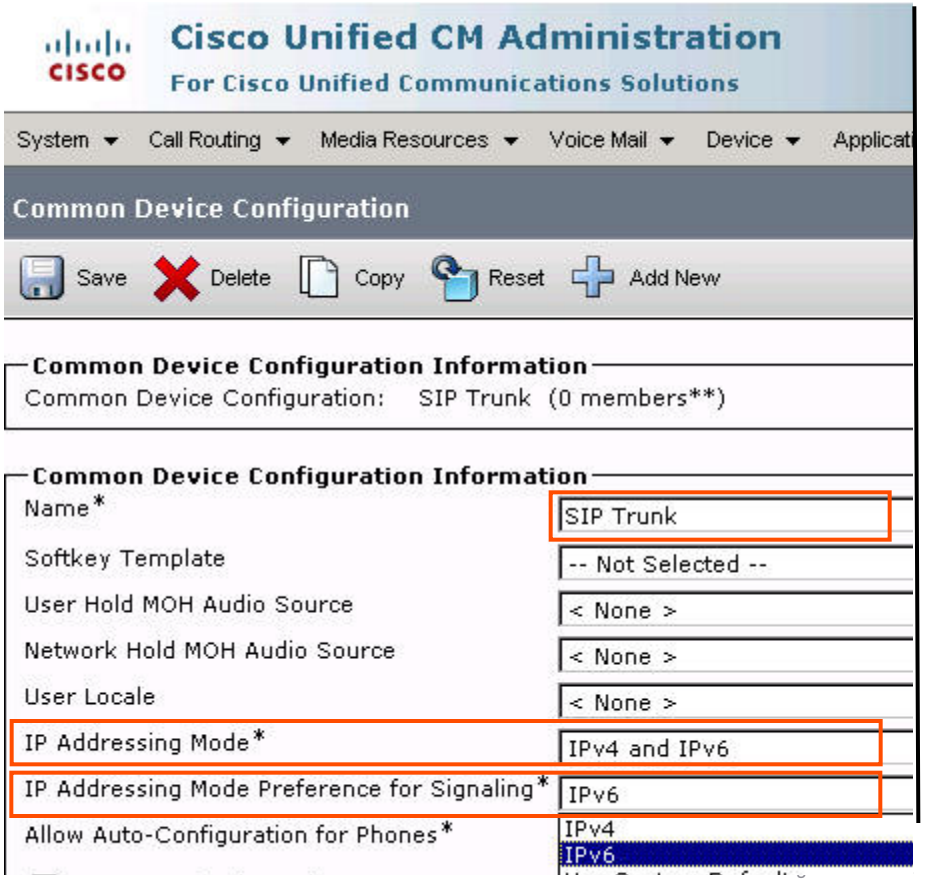
The SDP Body of the SIP Offer can contain both an IPv4 and IPv6 address – preference is indicated in the a=group:ANAT field (using the a=mid: values associated with each address)

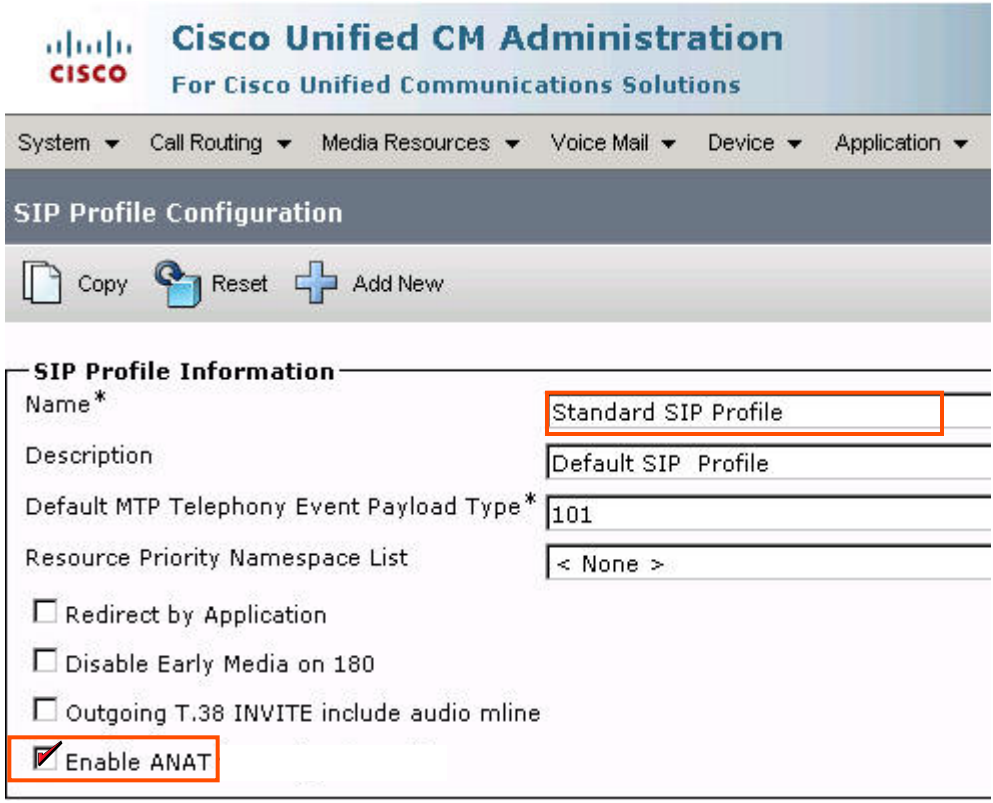
The SDP Body of the SIP Answer can contain both an IPv4 and IPv6 address – the selected address is indicated in the a=group:ANAT field (using the a=mid: values associated with each address). The UDP port number of the non-preferred IP address is set to 0

IPv6 SIP Trunks – Configuring IPv6 and ANAT



ANAT is supported for SIP Early Offer and SIP Delayed Offer calls





IPv6 – CUCM SIP Trunks Deployment Recommendations

<u>IPv4 Only</u> – Standard Configuration

<u>IPv6 Only</u>
IPv6 Enabled
Addressing Mode - IPv6 Only
Signalling Mode Preference – IPv6
No ANAT
IPv6 Trunk destination address or server name (for signalling)
SIP Early Offer (MTP Required) or Delayed Offer

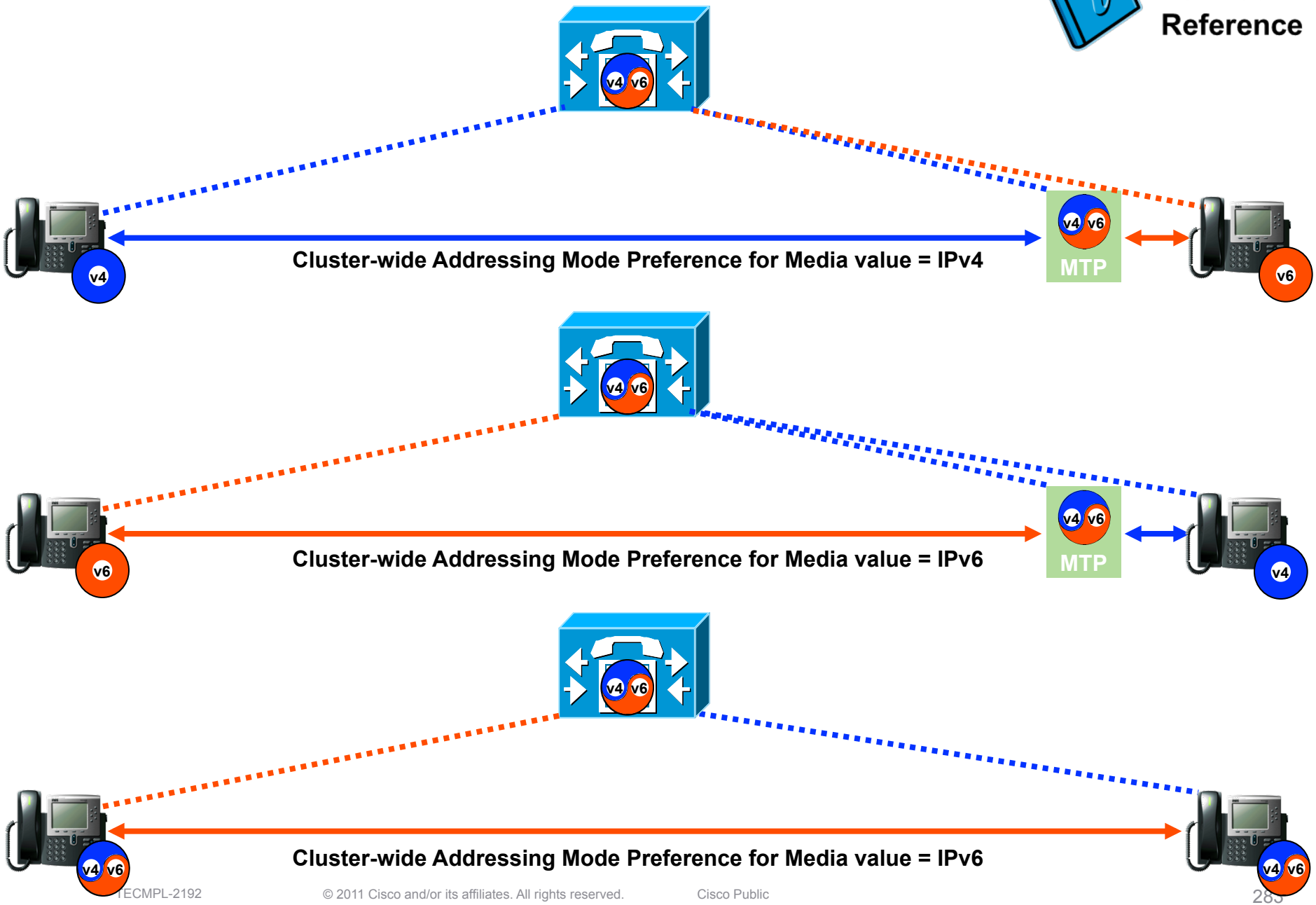
<u>Dual Stack with ANAT</u>
IPv6 Enabled
Addressing Mode - IPv4 and IPv6
Signalling Mode Preference – IPv4 or IPv6
ANAT Enabled
IPv4 or IPv6 Trunk destination address or server name
SIP Early Offer (MTP Required) or Delayed Offer

In all cases - Determine the far end Trunk device's capabilities :
e.g. IOS Gateways :
Always send SIP Early Offer - Can accept SIP Early and Delayed Offer calls
Once the IOS SIP stack is configured as Dual Stack - ANAT is automatically enabled

See IOS IPv6 VOIP implementation Guide at :
www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6_voip.pdf

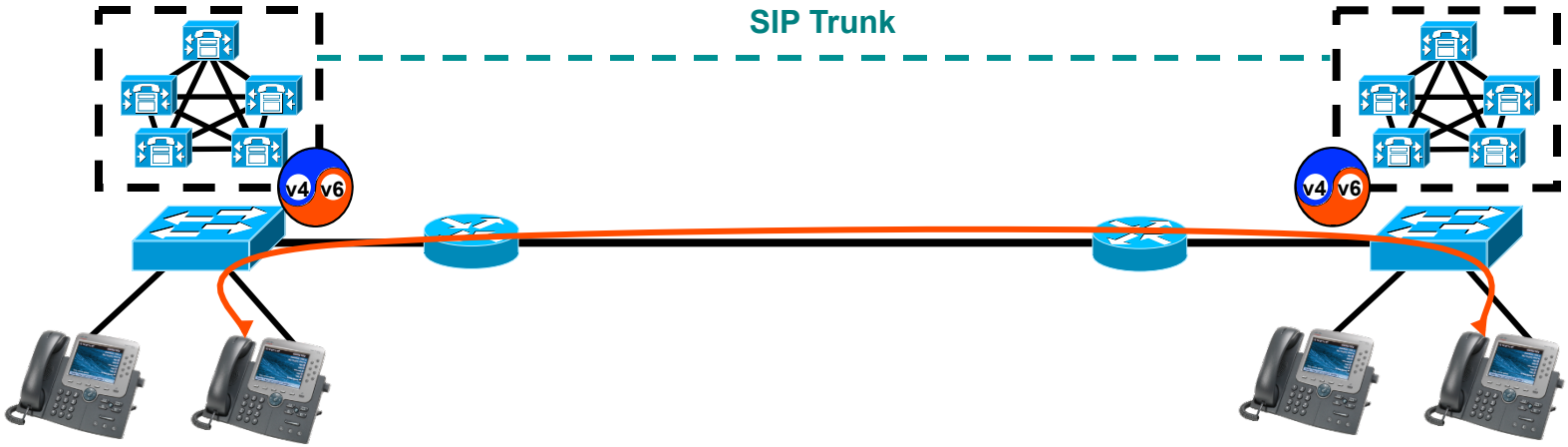
Effect of IPv6 Enterprise Parameter on MTP selection

For Your Reference



CUCM and Call Admission Control

For Your Reference



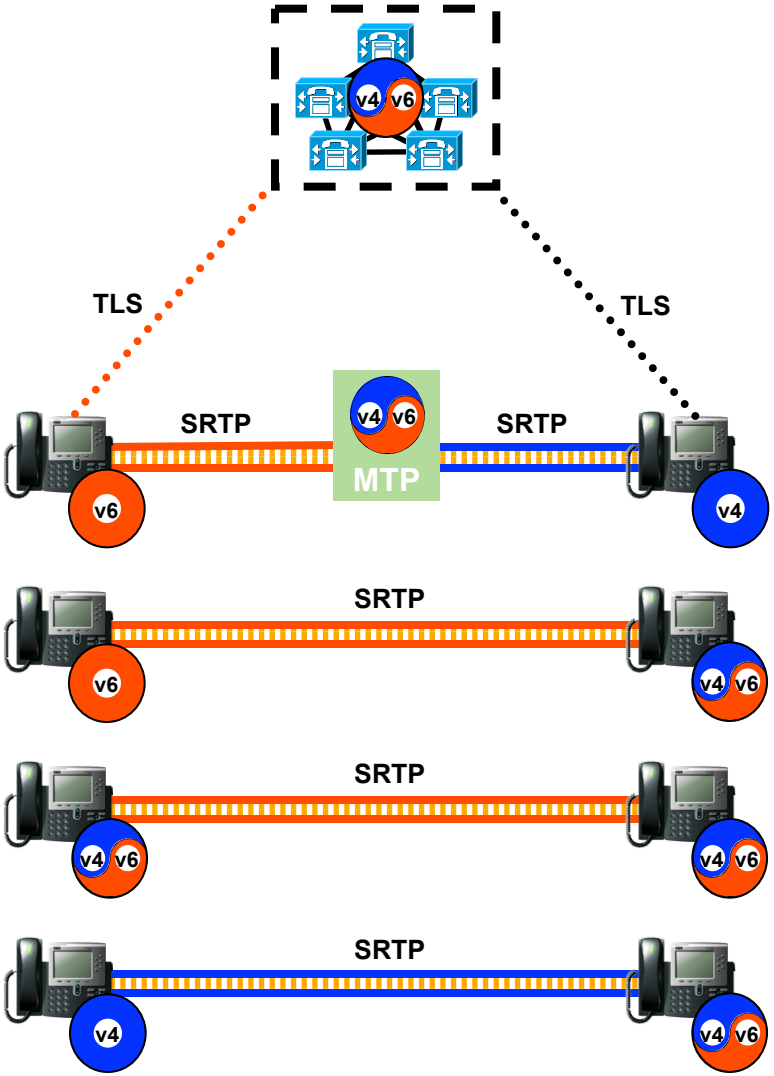
Call Admission Control (CAC)

- Use CUCM Locations based CAC
- Locations based CAC accounts for IPv6 bandwidth overhead (20 additional bytes per packet)
- No Support for RSVP CAC today

Dual Stack Deployment Models

- Single Site Call Processing
- Multiple Site Distributed Call Processing
- Multiple Site Centralized Call Processing
- SRST Supports IPv4 only today – Dual Stack Phones fail-over to IPv4 for SRST

IPv6 UC and Security



- CUCM supports Encrypted calls between IP Phones, Gateways and over CUCM Trunks.
- IPv6 capable IP Phones, SIP Trunks SIP/SCCP Gateways and use TLS and SRTP
- IPv4 based H323 and MGCP gateway connections use IPSec.
- MTPs can be dynamically inserted for IPv4 <-> IPv6 conversion of encrypted voice media. MTPs use the pass-through codec to transparently pass SRTP streams.
- For IPv6 UC environments SRTP is used as SRTP is specifically crafted for UDP based RTP traffic and has a lower packet overhead.
- Majority of UC vendors have adopted SRTP

In Summary

- IPv6 features are available from CUCM 7.1(2), that is since April 2009.
- Some UC IPv6 deployment include: US DoD, AT&T, Sony and 10+

- **Related reading**

  SRND: Deploying IPv6 in Unified Communications Networks

  http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/ipv6/ipv6srnd.html

  IOS IPv6 VOIP implementation Guide

  http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6_voip.pdf

- **Cisco Live session** (with more detailled configuration examples)

  BRKUCC-2061 IPv6 in Enterprise Unified Communications Networks

- We are interest in your feedback at http://www.myciscocommunity.com/message/47414

  What are your views on IPv6 for UC ?

  Are you considering deploying IPv6 in you UC network in the near future ?

  What are your drivers for deploying IPv6 for UC ? e.g. Address Exhaustion? Network Readiness ? Corporate Compliance ? etc.

  Do you require an IPv6 connection to your Service Provider for IP PSTN connectivity ?

  Based on the IPv6 capabilities of Cisco UC products today - What IPv6 features would you like to see Cisco developing in future releases ?

Agenda

- Introduction
- IPv6 in the Enterprise
- Routing Considerations
- Security for IPv6
- First Hop Security
- Unified Communications
- Multicast
- DNS
- Deployment and Operation Considerations

IPv6 – Multicast

Agenda

- Fundamentals
- Multicast receivers – Multicast Listener Discovery (MLD)
- RPF Mechanics
- Tree Building (PIM)
- Rendezvous Points
- Source Specific Multicast (SSM)
- Conclusions

IPv6 Multicast Fundamentals

Elements of Multicast Technology

- Protocols to build multicast distribution trees:
  - PIM
- Protocols for receivers to “signal” to the network which multicast group/source they want to receive:
  - IGMP, MLD
- Protocols and mechanisms for receivers to discover sources:
  - ASM - RP, SSM
- Protocols for source / receiver to discover ASM RP:
  - BSR, static, embedded
- Mechanism for multicast forwarding with loop avoidance:
  - RPF

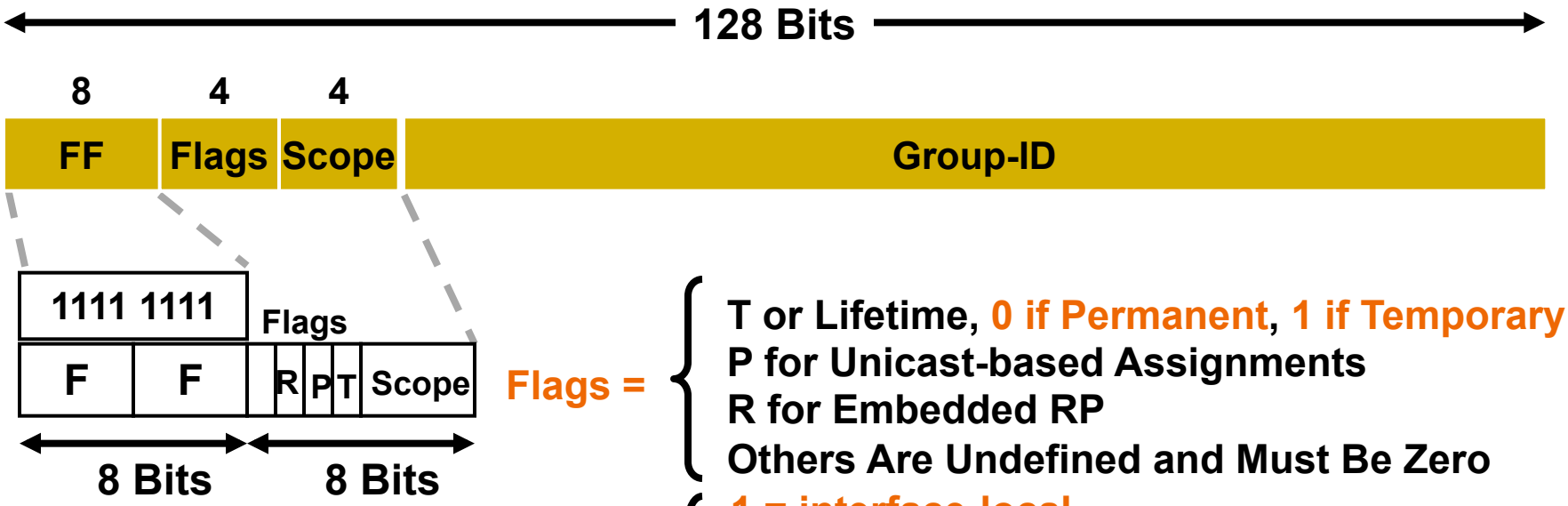
IPv4 and IPv6 Multicast Comparison

Service	IPv4 component	IPv6 component
Addressing Range	32-bit, Class D	128-bit (112-bit Group)
Routing	Protocol Independent, All IGPs and MBGP	Protocol Independent, All IGPs and MBGP with v6 mcast SAFI
Forwarding	PIM-DM, PIM-SM, PIM-SSM, PIM-bidir, PIM-BSR	~~PIM-DM~~, PIM-SM, PIM-SSM, PIM-bidir, PIM-BSR
Group Management	IGMPv1, v2, v3	MLDv1, v2
Domain Control	Administrative boundary	Scope boundary
Interdomain Solutions	MSDP Across Independent PIM Domains	SSM or Single RP Within Globally Shared Domains

IPv6 Addresses

- 128 bits (IPv6) vs. 32 bits (IPv4)
  - 2001:0DB8:0000:130F:0000:0000:087C:140B or
  - 2001:DB8:0:130F::87C:140B (same address)
- Prefix representation – the same
  - 2001:DB8:10::/48
- Interfaces have multiple addresses (Global, Link Local, ULA, Multicast)! These addresses have scope associated
- No broadcast address!
- Routing protocols – pretty much the same as in IPv4
- Use of multicast is ubiquitous
  - Neighbor discovery (L2 address resolution, router discovery)

IPv6 Multicast Addresses - RFC 4291



Flags =

- T or Lifetime, 0 if Permanent, 1 if Temporary
- P for Unicast-based Assignments
- R for Embedded RP
- Others Are Undefined and Must Be Zero

Scope =

- 1 = interface-local
- 2 = link
- 4 = admin-local
- 5 = site
- 8 = organization
- E = global
- 0, 3, F = reserved

Note: other scopes (6, 7, 9-D) are unassigned but can be used

Unicast-Based Multicast Addresses - RFC 3306

- RFC 3306—unicast-based multicast addresses

  Similar to IPv4 GLOP addressing (233/8 + ASN = 256 group addresses)

  Solves IPv6 global address allocation problem (2^32 multicast group addresses per (up to /64) unicast prefix you own)

  Flags = 00PT: P = 1, T = 1 →Unicast-based multicast address

- Example

  Content provider's unicast prefix

  1234:5678:9abc::/48

  Multicast address

  FF3E:0030:1234:5678:9abc::1 (hex "30" is 48 bits)

Source Specific Multicast (SSM) Addresses - RFC 3306

- Based on unicast-based multicast addresses (RFC 3306)
- Flags = 00PT: P=T=1
- Scope = any valid address scope value (>=3)
- Plen = 0
- Network-Prefix = 0
- Range = FF3x::/32
  (x = any valid address scope value)
- SSM ranges are hardcoded

```
R1#show ipv6 pim range-list
Static SSM Exp: never Learnt
from : ::
  FF33::/32 Up: 1d02h
  FF34::/32 Up: 1d02h
  FF35::/32 Up: 1d02h
  FF36::/32 Up: 1d02h
  FF37::/32 Up: 1d02h
  FF38::/32 Up: 1d02h
  FF39::/32 Up: 1d02h
  FF3A::/32 Up: 1d02h
  FF3B::/32 Up: 1d02h
  FF3C::/32 Up: 1d02h
  FF3D::/32 Up: 1d02h
  FF3E::/32 Up: 1d02h
  FF3F::/32 Up: 1d02h
```

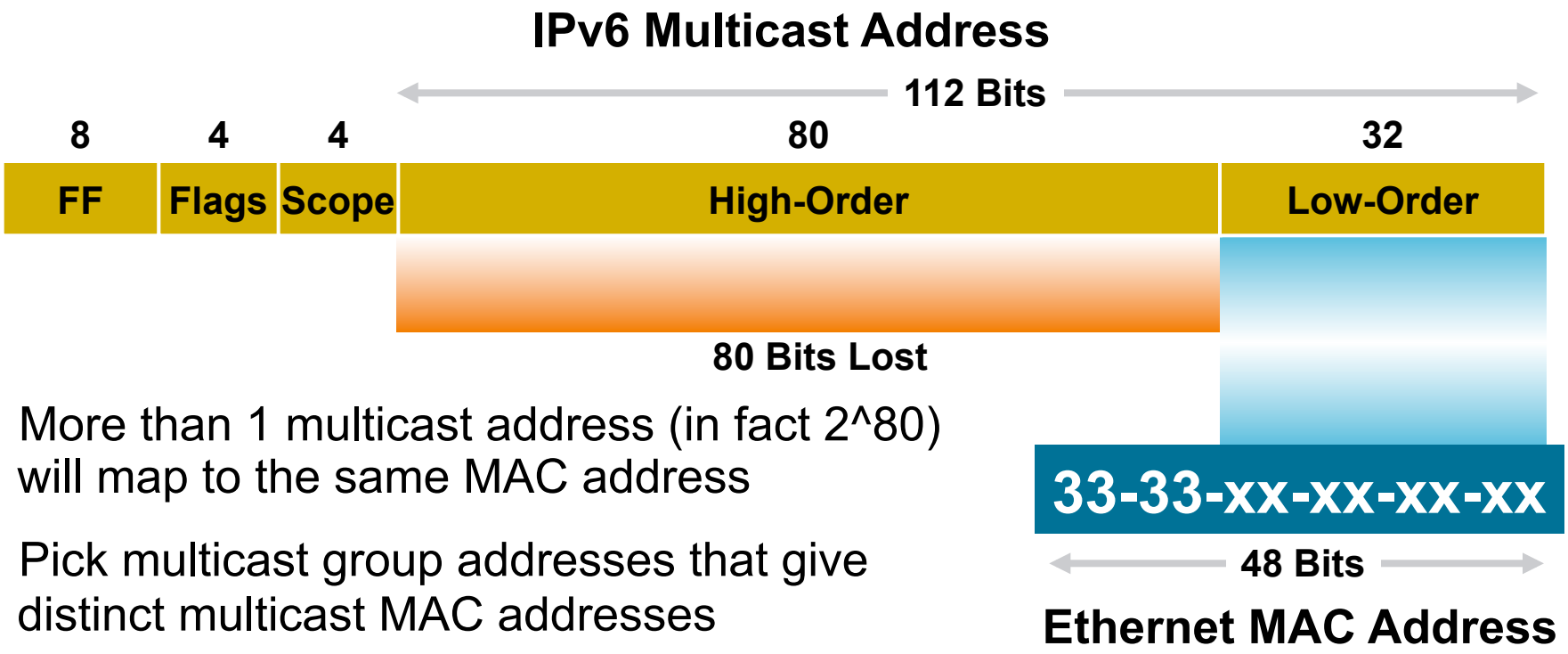
Embedded RP Addressing – RFC 3956

- Based on unicast-based multicast addresses (RFC 3306)
- RP address is embedded in multicast address
- Flag bits = 0RPT

  R = 1, P = 1, T = 1 → Embedded RP address
- RP address = Network-Prefix::RPadr
- Range = FF70::/12
- For each unicast prefix (up to /64) you own, you now also own:

  16 RPs for each of the 16 multicast scopes (256 total) with 2^32 multicast groups assigned to each RP (2^40 total)
- Deployment choices: network-prefix is max. 64 bits but can be smaller → RPs per /64, per /48, etc…

IPv6 Layer 2 Multicast Addressing Mapping – RFC 2464

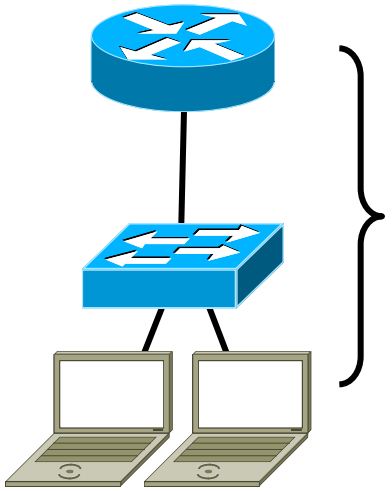


- More than 1 multicast address (in fact 2^80) will map to the same MAC address
- Pick multicast group addresses that give distinct multicast MAC addresses
- For example: FF02::1 → 33-33-00-00-00-01
  FF3E::1 → 33-33-00-00-00-01
- Similar to IPv4: 5 bits are lost (28 significant L3 multicast bits are mapped into 23 L2 MAC bits)

Multicast Listener Discovery - MLD

Multicast Listener Discovery – MLD
Multicast Host Membership Control

- MLD specified in RFC's 2710 and 3810
- MLD is equivalent to IGMP in IPv4
- MLD messages transported over ICMPv6
- MLD uses link local source addresses
- MLD packets use "Router Alert" option in IPv6 Hop-by-Hop extension header (RFC 2711) with Hop Limit =1



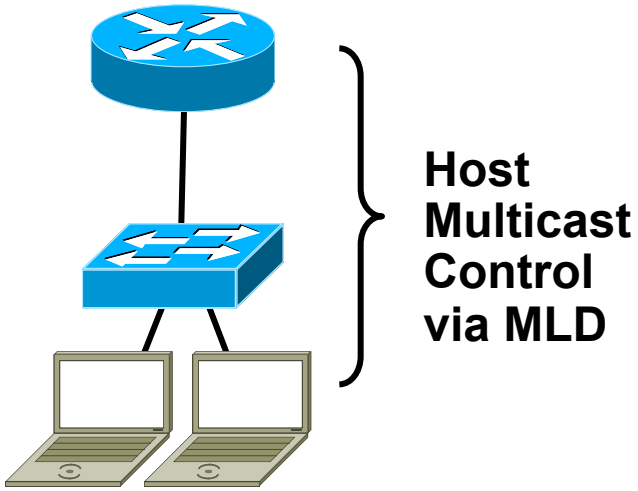
Multicast Listener Discovery – MLD
Multicast Host Membership Control

- Version number “confusion”:

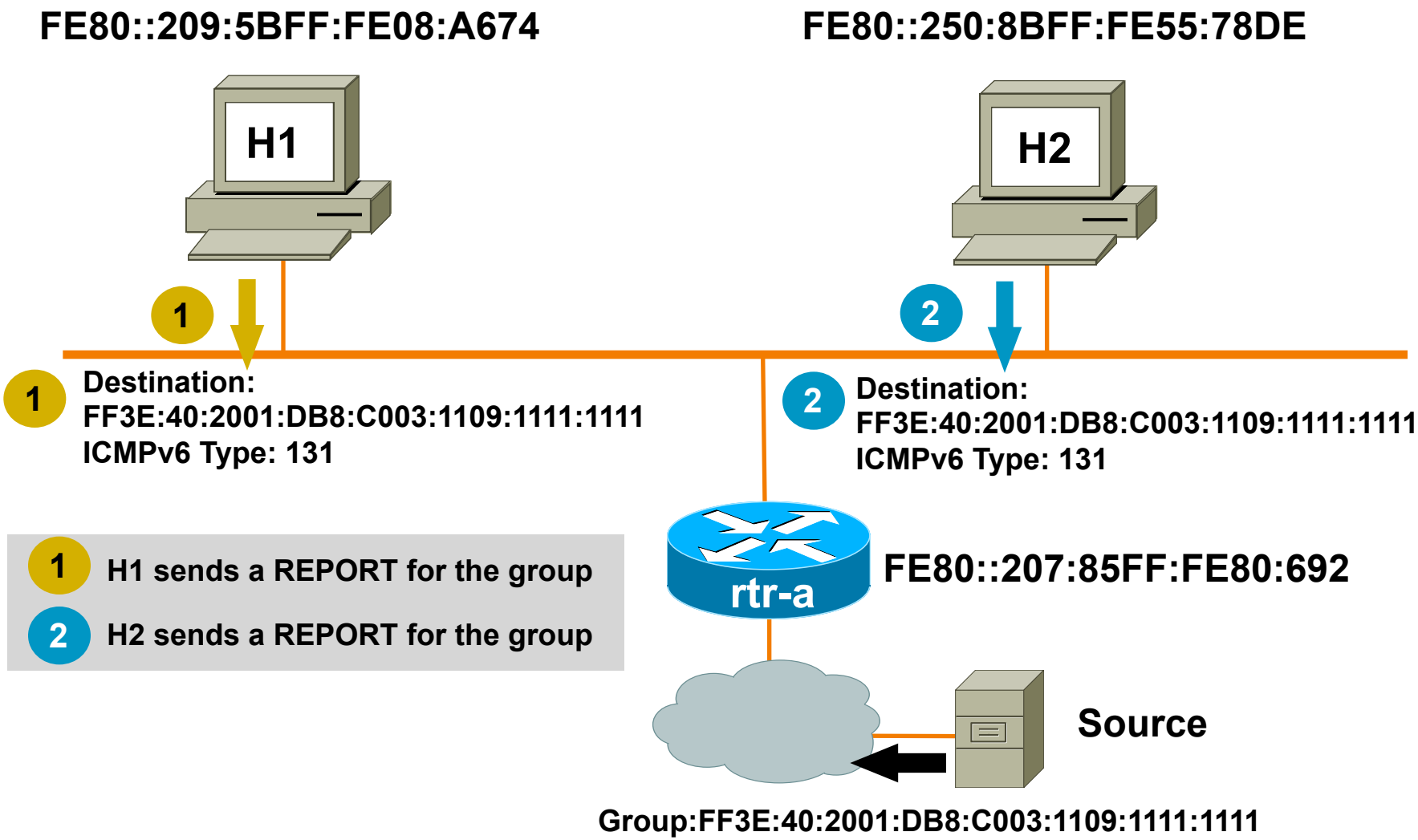
  MLDv1 (RFC 2710) ~ IGMPv2

  MLDv2 (RFC 3810) ~ IGMPv3

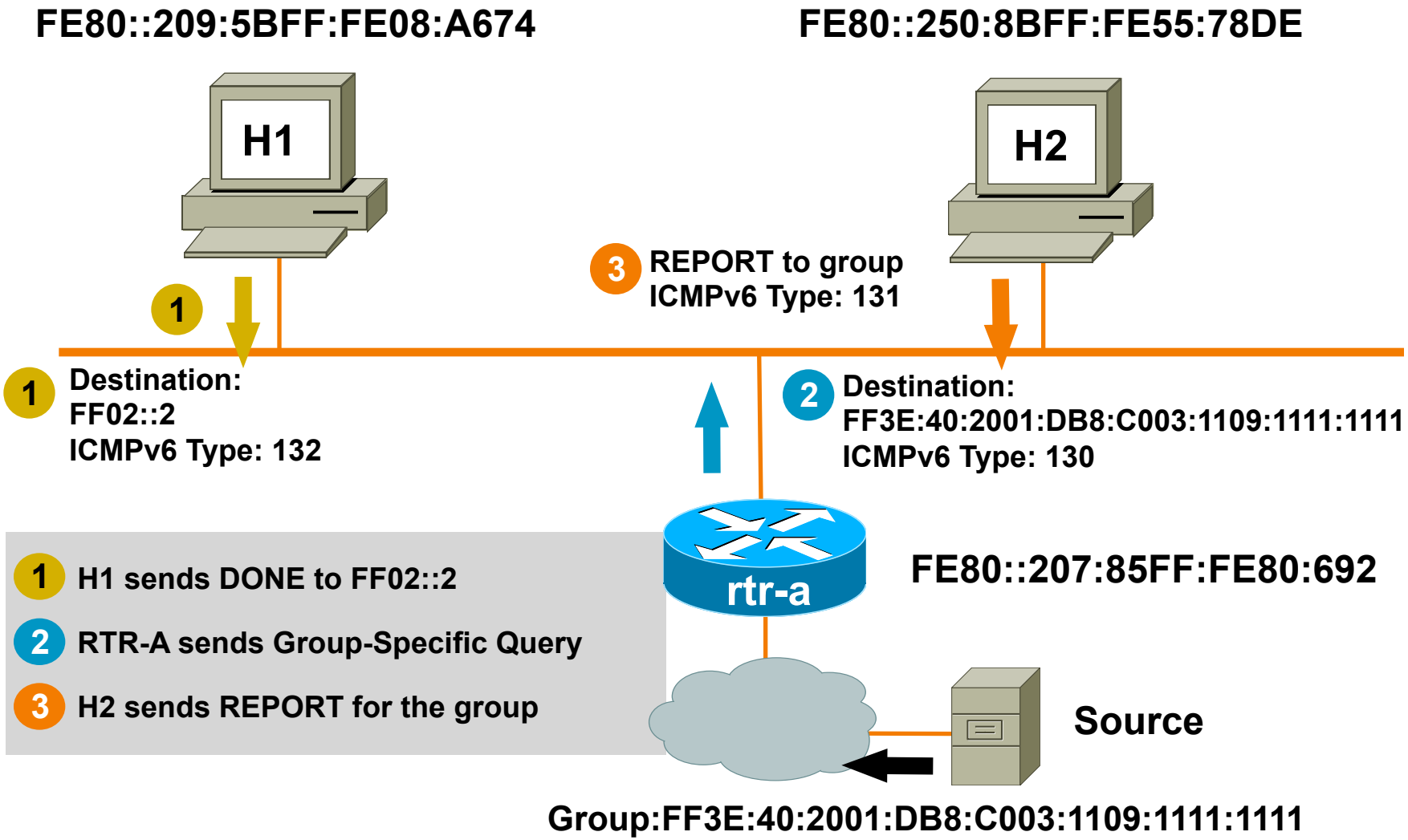
- MLDv2 router compatible with MLDv1 hosts
- SSM transition through SSM mapping for MLDv1 messages – static or DNS
- MLD snooping



MLDv1: Joining a Group (REPORT)



MLDv1: Host Management
(Group-Specific Query)



Other MLD Operations

- Leave/DONE
  - Last host leaves—sends DONE (Type 132)
  - Router will respond with group-specific query (Type 130)
  - Router will use the last member query response interval (Default=1 sec) for each query
  - Query is sent twice and if no reports occur then entry is removed (2 seconds)
- General Query (Type 130)
  - Sent to learn of listeners on the attached link
  - Sets the multicast address field to zero
  - Sent every 125 seconds (configurable) to FF02::1 (All Nodes)

MLDv2

- MLDv2 enables a host to join a specific multicast source
- Supports SSM deployment model
- 2 message types: Report (Type 143) and Query (Type 130)
- Capabilities of Report Message (Type 143) include a concatenated set of “Multicast Address Records” detailing the multicast sources in which the receiver is/is not interested
- Report Message sent to “All-MLDv2 Routers” multicast address (FF02::16) (facilitates MLD snooping on L2 switches)
- Report Message (Type 143) also performs function of MLDv1 Done message (Type 132)
- MLDv2 is backwards compatible and interoperable with MLDv1and therefore also supports the MLDv1 messages Type 131 (Report) and Type 132 (Done)

Enabling / managing MLD - IOS

- MLD is automatically enabled on all interfaces with:

```
ipv6 multicast-routing
```

- Routers implement MLDv2 with MLDv1 compatibility mode for MLDv1 hosts. The compatibility mode is maintained based on the multicast group address.
- MLD can be disabled on a per interface basis (e.g. for core interfaces or access interfaces without receivers) by:

```
no ipv6 mld router
```

- MLD ACLs allow access only to specific multicast groups and/or sources using:

```
ipv6 mld access-group
```

- SSM transition through SSM mapping for MLDv1 messages – static or DNS

IPv6 RPF Mechanics

IPv6 RPF – Sources of Information

- IPv6Unicast RIB: all IPv6IGPs (ISIS, OSPFv3, EIGRPv6, RIPng, static)
- IPv6 Static Multicast Routes

  ipv6 route*ipv6-prefix*/*prefix-length* {*ipv6-address* | *interface-type interface-number* [*ipv6-address*]} [*administrative-distance*] [***administrative-multicast-distance***| **unicast** | **multicast**] [**tag***tag*]

  Same behaviour as IPv4 static routes (**except for new options**)

  Unicast-only static routes

  Equal or less configuration lines than in IPv4 (“ip route” / “ipmroute”)
- IPv6 Multicast BGP Table (AFI=2, SAFI=2) – see next slide (but NOT IPv6UnicastBGP Table)

IPv6 RPF – Sources of Information

- Multiprotocol Extensions for BGP-4: RFC 2545 / RFC 4760 (obsoletes RFC 2858)

  New BGP-4 attributes: MP_REACH_NLRI (attribute 14), MP_UNREACH_NLRI (attribute 15)

  AFI=1 (IPv4), AFI=2 (IPv6), SAFI=1 (unicast), SAFI=2 (multicast). See IANA: http://www.iana.org/assignments/safi-namespace

- IPv6 Multicast BGP Table (AFI=2, SAFI=2) used as an IPv6 RPF check source. This is a route only usable for IPv6 multicast, NOT for IPv6 unicast.

- SAFI=2 must be used in transit ISP scenarios (peering neighbor does not know BGP route is really usable for multicast or not)

IPv6 RPF Algorithm

- Select route with longest-prefix match from the following sources
  1. IPv6 Static Multicast Routes
  2. IPv6 Multicast BGP Table
  3. IPv6Unicast RIB (all IGPs, NOT IPv6UnicastBGP)
- If multiple longest-prefix matches exist, select the the route with the lowest administrative distance
- If multiple routes still exist, select according to the order above
- Essentially the same as unicast route selection with the difference that the “Multicast RIB” result is “virtual”, while for unicast the selected routes are merged in a “real” RIB.
- BGPIPv6Unicast routes are NOT used in the RPF selection process

  IOS, command to override:

  ```
  ipv6 multicast rpf use-bgp
  ```

  Not recommended

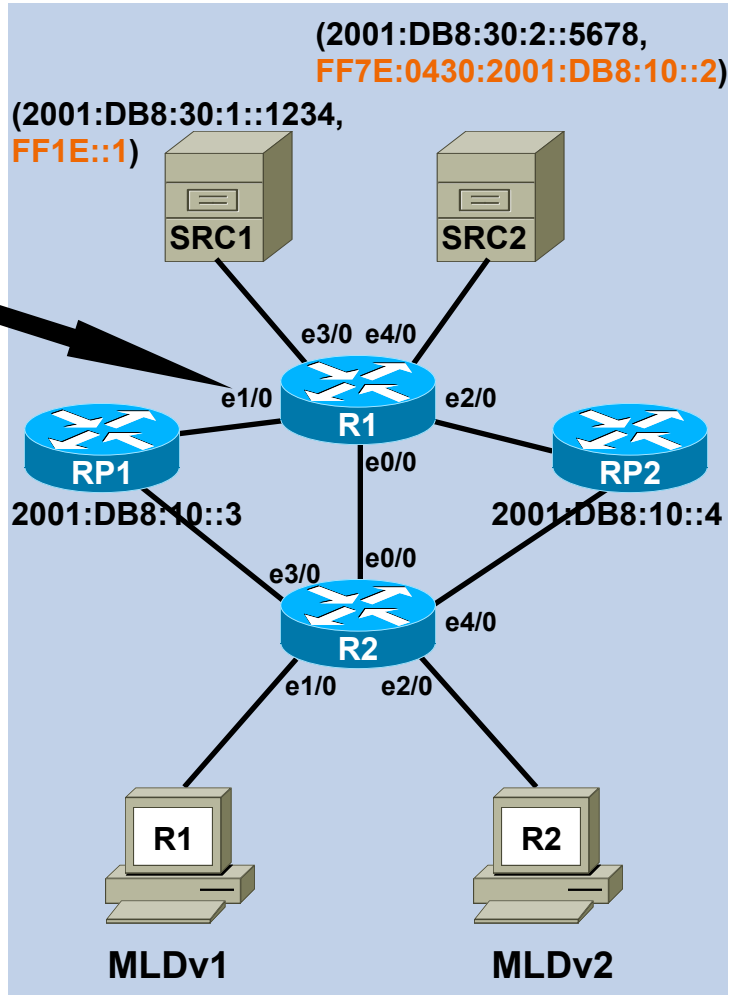
RPF Interface vs. Neighbor (RFC 4601)

- RPF Interface: chosen by the RPF algorithm (MRIB) to reach the multicast source (SPT) or RP (shared tree)
- RPFNeighbor: PIM neighbor residing on the RPF Interface towards the multicast source (SPT) or RP (shared tree). PIM J/P messages can ONLY be sent to the RPFneighbor.
- Note: existence of an RPF Interface (but without an actual RPF Neighbour) is NOT enough to forward PIM J/P messages over that interface and a multicast distribution tree to be built

Multicast Tree Building – PIM

IPv6 Multicast Configuration - Basic

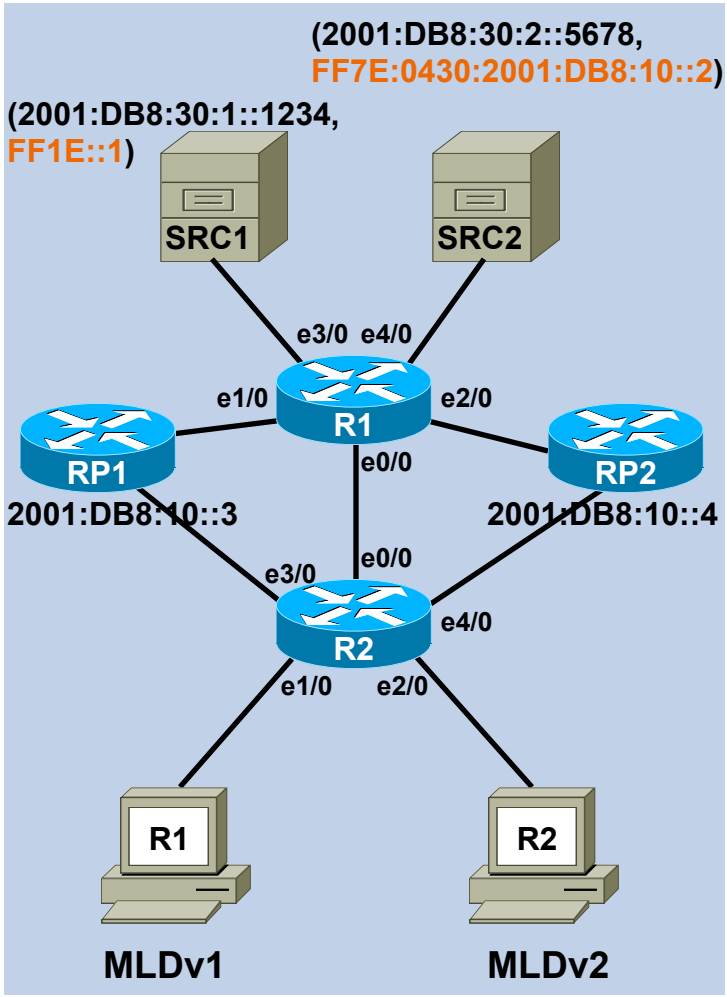
```
!
ipv6 unicast-routing
ipv6 cef
ipv6 multicast-routing
!
interface Loopback0
 no ip address
 ipv6 address 2001:DB8:10::1/128
 ipv6 ospf 1 area 0
!
interface Ethernet0/0
 no ip address
 ipv6 address
2001:DB8:20:1::1/64
 ipv6 ospf 1 area 0
…
!
ipv6 router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
 passive-interface Ethernet3/0
 passive-interface Ethernet4/0
 passive-interface Loopback0
!
ipv6 pimrp-address
2001:DB8:10::3
!
```



- With SSM or Embedded RP, only "IPv6 multicast-routing is required

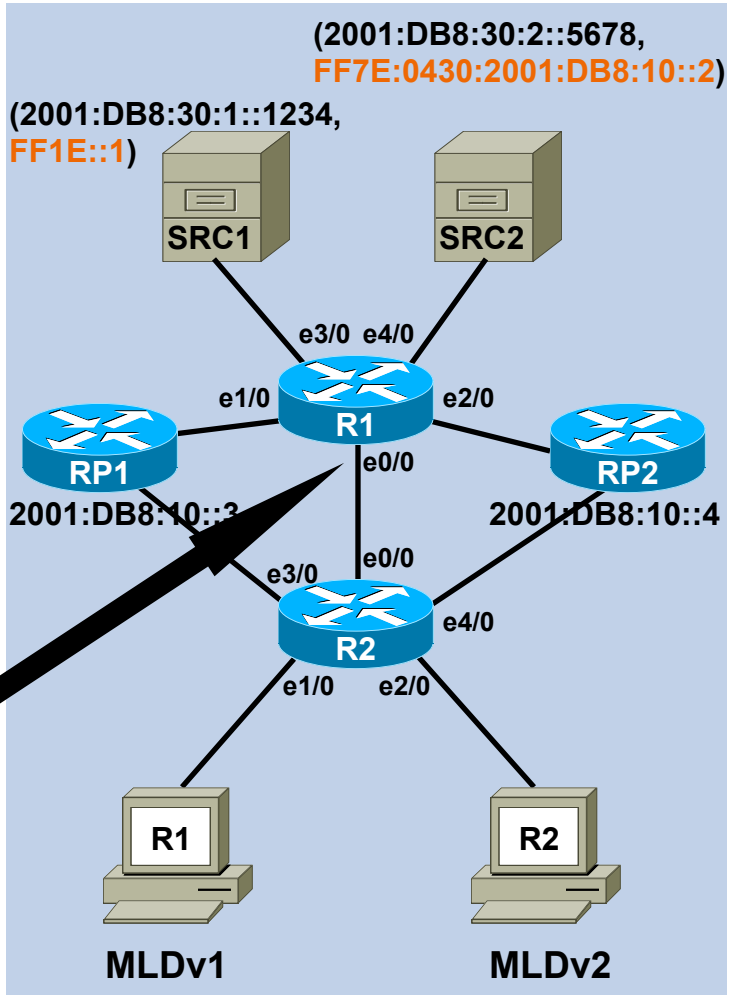
Enabling PIM for IPv6 Multicast

- "ipv6 multicast-routing" enables PIM on all interfaces (←→IPv4)
- "ipv6 multicast-routing" enables MLDv2 on all interfaces (←→IPv4)
- PIM / MLDv2 can be turned off on per interface basis
  - "no ipv6 pim"
  - "no ipv6 mld router"
- PIM neighbor discovery and PIM hellos use link local addresses only. PIM hellos are sent to a link local multicast address FF02::D



PIM Neighbors

- PIM neighbors are identified through link-local addresses

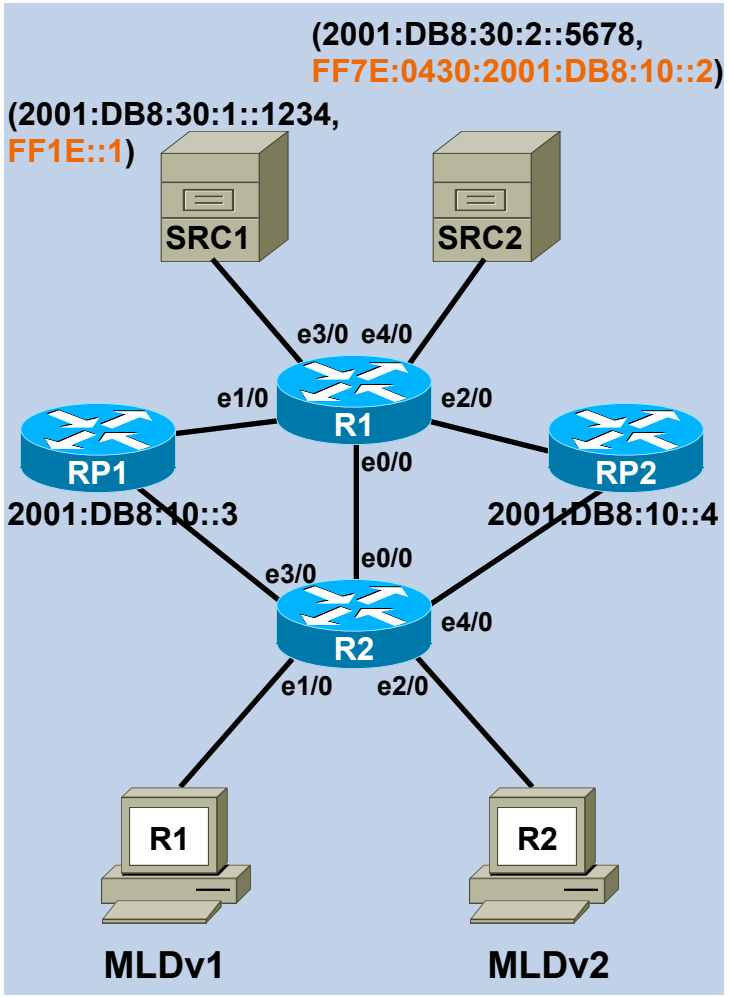



```
R1#sh ipv6 pim interface ethernet 0/0
Interface            PIM   Nbr    Hello   DR
                           Count  Intvl   Prior

Ethernet0/0          on    130      1
    Address: FE80::A8BB:CCFF:FE00:6500
    DR     : FE80::A8BB:CCFF:FE00:6600
```

```
R1#sh ipv6 pim neighbor ethernet 0/0
Neighbor Address              Interface          Uptime    Expires DR pri Bidir

FE80::A8BB:CCFF:FE00:6600     Ethernet0/0        00:35:56  00:01:31 1 (DR) B
```

Multicast Interface Groups

```
R1#show ipv6 interface ethernet 0/0
Ethernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::A8BB:CCFF:FE00:6500
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:20:1::1, subnet is 2001:DB8:20:1::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::5
    FF02::6
    FF02::D
    FF02::16
    FF02::1:FF00:1
    FF02::1:FF00:6500
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```



- FF02::D → All PIM routers
- FF02::16 → All MLDv2 routers

PIM Topology Information - OILs

- New in the updated RFC 4601 (vs. RFC 2362)
- PIM States have Outgoing Interface Lists (OILs)
- Immediate OIL: Built directly from the state of the relevant type

  For example, immediate OIL for (S,G) state is the OIL that would be built if the router only had (S,G) state and no (*,G) or (S,G,rpt) state. This requires explicit PIM Joins / MLD Reports.

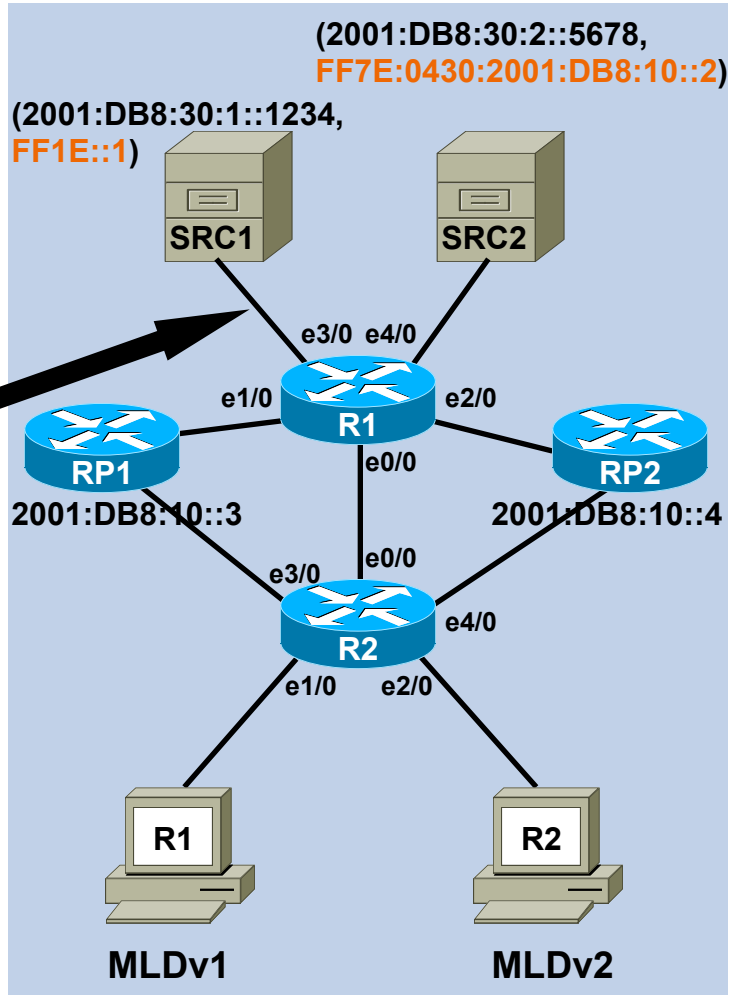
  "show ipv6pim topology"
- Inherited OIL: Inherits state from other state types

  For example, immediate OIL of parent (*,G) state is copied to inherited OIL for (S,G) state

  "show ipv6mrib route" ("show ipv6mroute")
- Generally speaking, Inherited OILs are used for forwarding, Immediate OILs are used to make decisions about state maintenance

PIM Topology Information - OILs

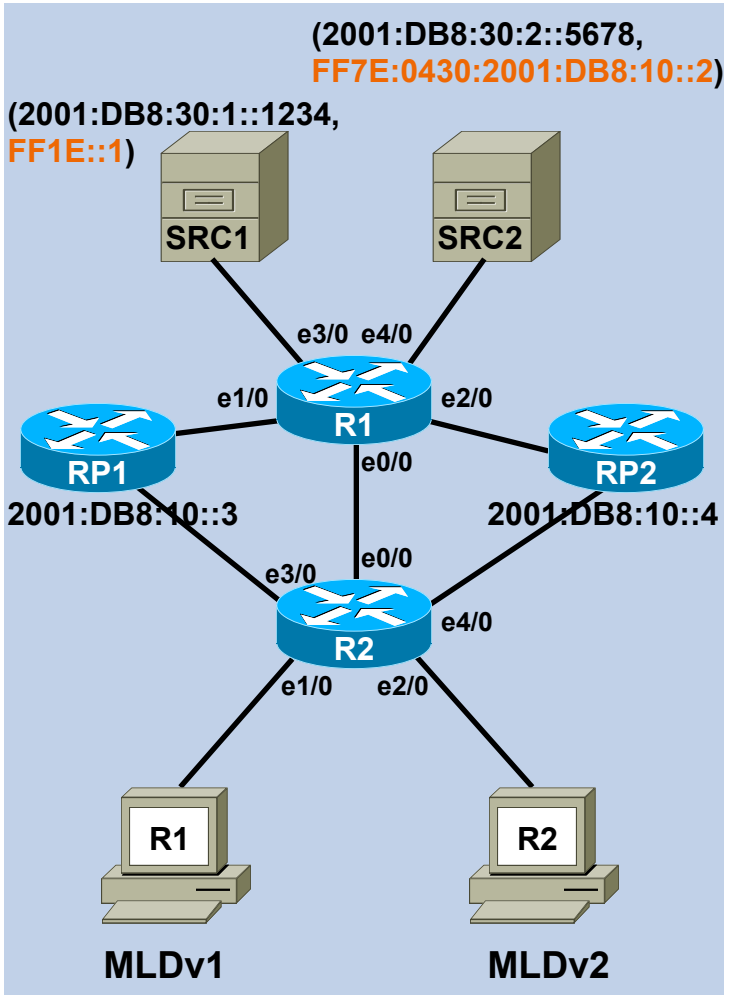
```
R1#show ipv6 pim topology FF1E::1
IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe
Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR - Sending Registers, E - MSDP
External,
    DCC - Don't Check Connected
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Disinterest,
    II - Internal Interest, ID - Internal Disinterest,
    LH - Last Hop, AS - Assert, AB - Admin Boundary

(2001:DB8:30:1::1234,FF1E::1)
SM SPT UP: 1d00h JP: Join(never) Flags: KAT(00:01:31) RA
RPF: Ethernet3/0,2001:DB8:30:1::1234*
Ethernet0/0          18:40:01   fwd Join(00:02:32)
```




```
R1#show ipv6 mrib route FF1E::1
IP Multicast Routing Information Base
e
Entry flags: L - Domain-Local Source, E - External Source to the
Domain,
    C - Directly-Connected Check, S - Signal, IA - Inherit Accept,
    K - Keepalive
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local
Interest,
    LD - Local Disinterest

(2001:DB8:30:1::1234,FF1E::1) RPF nbr: 2001:DB8:30:1::1234 Flags:
  Ethernet3/0 Flags: A
  Ethernet0/0 Flags: F NS
```

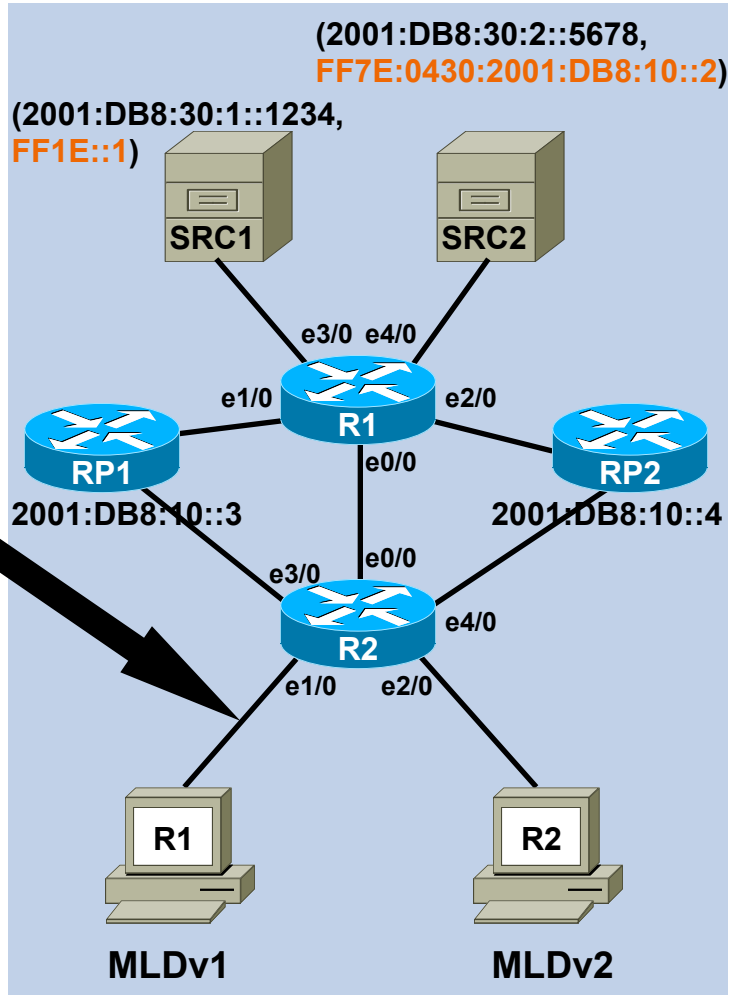
PIM Topology Information - OILs

```
R1#show ipv6 mroute FF1E::1
Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host
Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit
set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State

(2001:DB8:30:1::1234, FF1E::1), 1d00h/00:02:18, flags: SFT
Incoming interface: Ethernet3/0
  RPF nbr: 2001:DB8:30:1::1234
Immediate Outgoing interface list:
    Ethernet0/0, Forward, 18:39:15/00:03:19
```



PIM Topology Information - OILs

```
R2#show ipv6 mld groups FF1E::1 detail
Interface:      Ethernet1/0
Group:          FF1E::1
Uptime:         1d00h
Router mode:    EXCLUDE (Expires: 00:0[illegible]32)
Host mode:      INCLUDE
Last reporter:  FE80::A8BB:CCFF:FE00:CA00
Source list is empty
```

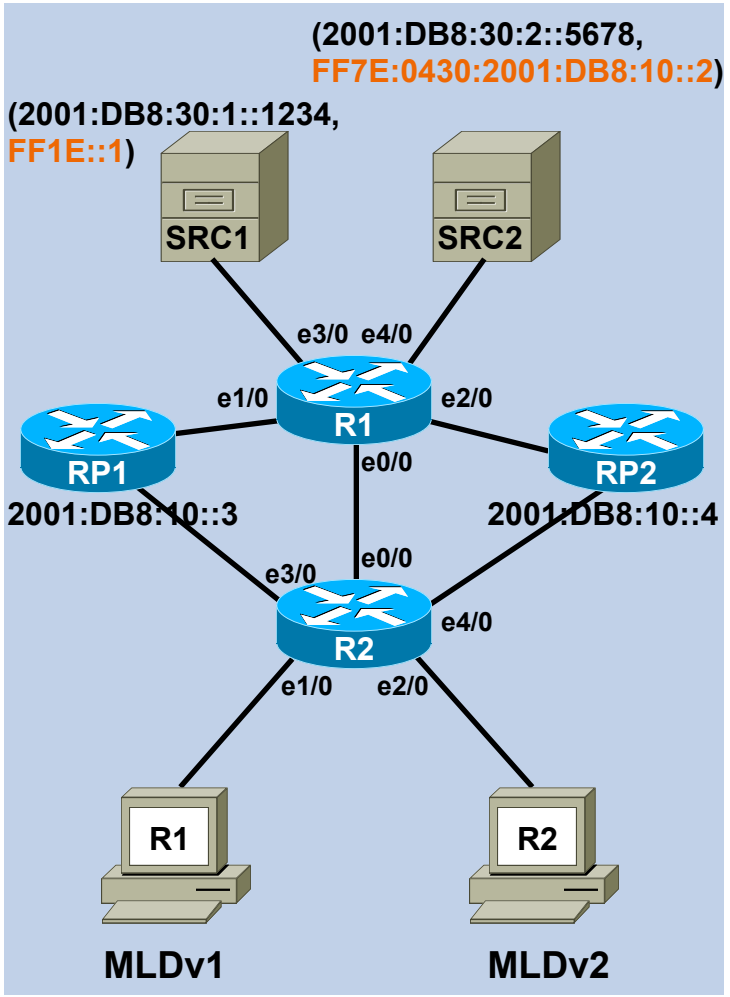


- On R2: only MLDv1 client (R1) active at the moment → no source-specific MLDv2 Reports
- No Immediate OIL created for (S,G) state

PIM Topology Information - OILs

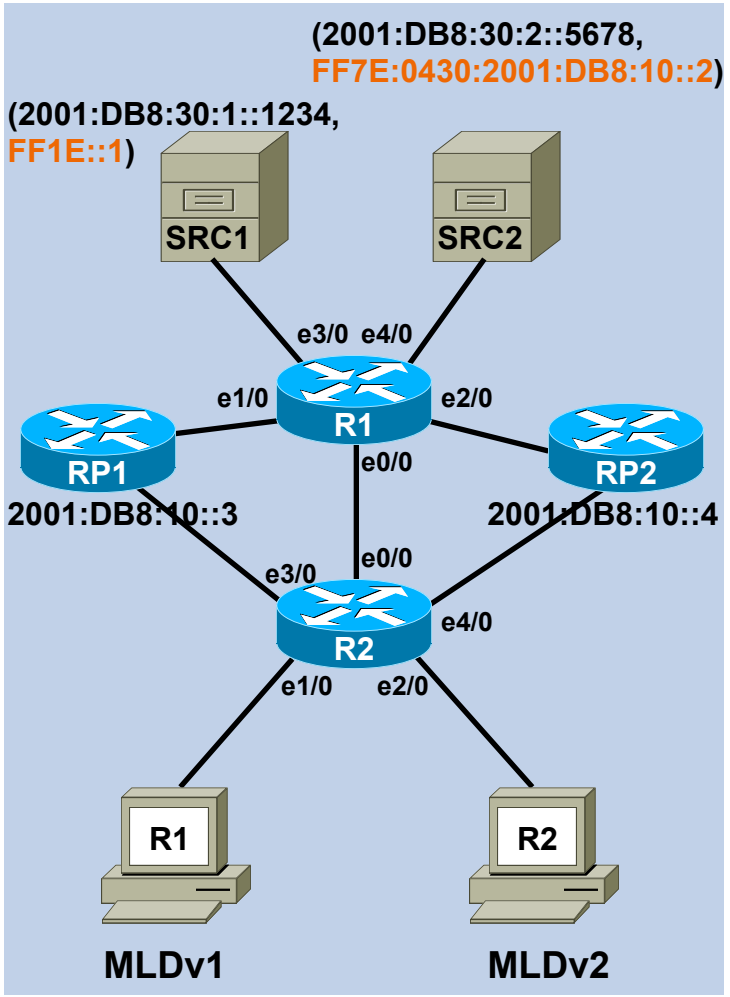
```
R2#show ipv6 pim topology FF1E::1
IP PIM Multicast Topology Table
…
(output truncated)
…
(*,FF1E::1)
SM UP: 23:28:23 JP: Join(00:00:21) Flags: LH
RP: 2001:DB8:10::3
RPF: Ethernet3/0,FE80::A8BB:CCFF:FE00:6703
Ethernet1/0         23:28:23  fwd LI LH

(2001:DB8:30:1::1234,FF1E::1)
SM SPT UP: 18:39:12 JP: Join(00:00:01) Flags: KAT(00:03:16) RA
RPF: Ethernet0/0,FE80::A8BB:CCFF:FE00:6500
No interfaces in immediate olist
```

```
R2#show ipv6 mrib route FF1E::1
IP Multicast Routing Information Base
…
(output truncated)
…
(*,FF1E::1) RPF nbr: FE80::A8BB:CCFF:FE00:6703 Flags: C
Ethernet1/0 Flags: F LI NS
Ethernet3/0 Flags: A NS

(2001:DB8:30:1::1234,FF1E::1) RPF nbr: FE80::A8BB:CCFF:FE00:6500
Flags:
  Ethernet0/0 Flags: A
  Ethernet1/0 Flags: F NS
```



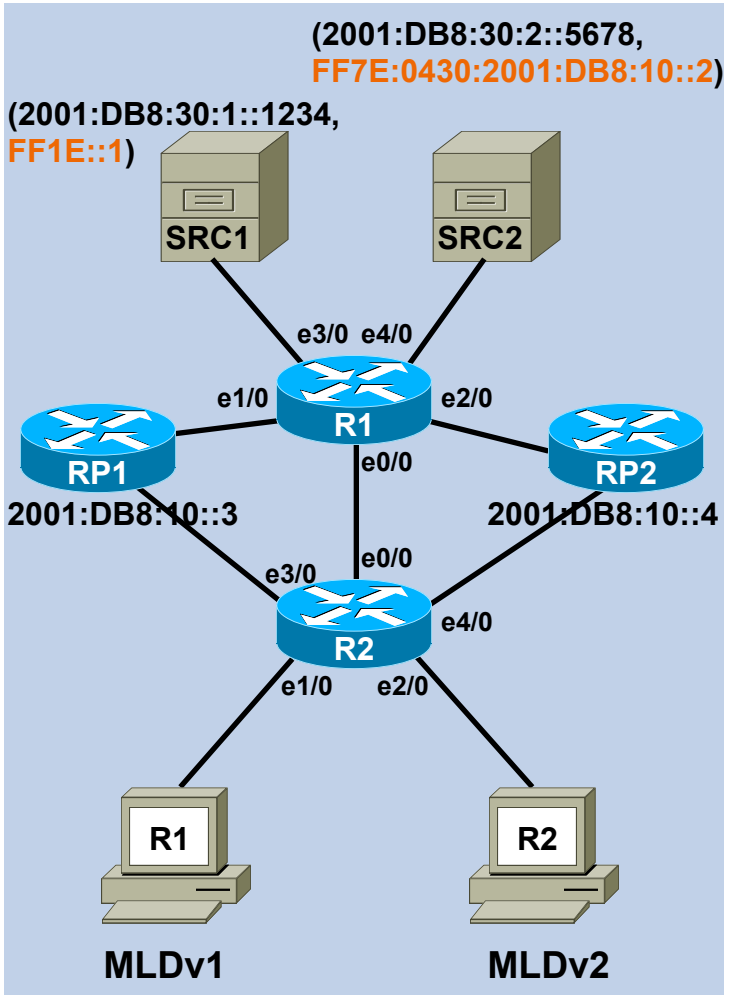
PIM Topology Information - OILs

```
R2#show ipv6 mroute FF1E::1
Multicast Routing Table
…
(output truncated)
…
(*, FF1E::1), 23:31:28/never, RP 2001:DB8:10::3, flags: SCJ
Incoming interface: Ethernet3/0
  RPF nbr: FE80::A8BB:CCFF:FE00:6703
Immediate Outgoing interface list:
Ethernet1/0, Forward, 23:31:28/never

(2001:DB8:30:1::1234, FF1E::1), 18:42:17/00:00:11, flags: SJT
  Incoming interface: Ethernet0/0
  RPF nbr: FE80::A8BB:CCFF:FE00:6500
  Inherited Outgoing interface list:
Ethernet1/0, Forward, 23:31:28/never
```



PIM Topology Information - OILs

```
R2#show ipv6 mld groups FF1E::1 detail
Interface:      Ethernet1/0
Group:          FF1E::1
Uptime:         00:02:26
Router mode:    EXCLUDE (Expires: 00:03:22)
Host mode:      INCLUDE
Last reporter:  FE80::A8BB:CCFF:FE00:CA00
Source list is empty
Interface:      Ethernet2/0
Group:          FF1E::1
Uptime:         00:02:25
Router mode:    INCLUDE
Host mode:      INCLUDE
Last reporter:  FE80::A8BB:CCFF:FE00:CA01
Group source list:
Source Address                          Uptime    Expires   Fwd
Flags
2001:DB8:30:1::1234                     00:02:25  00:03:27  Yes
Remote 4
```

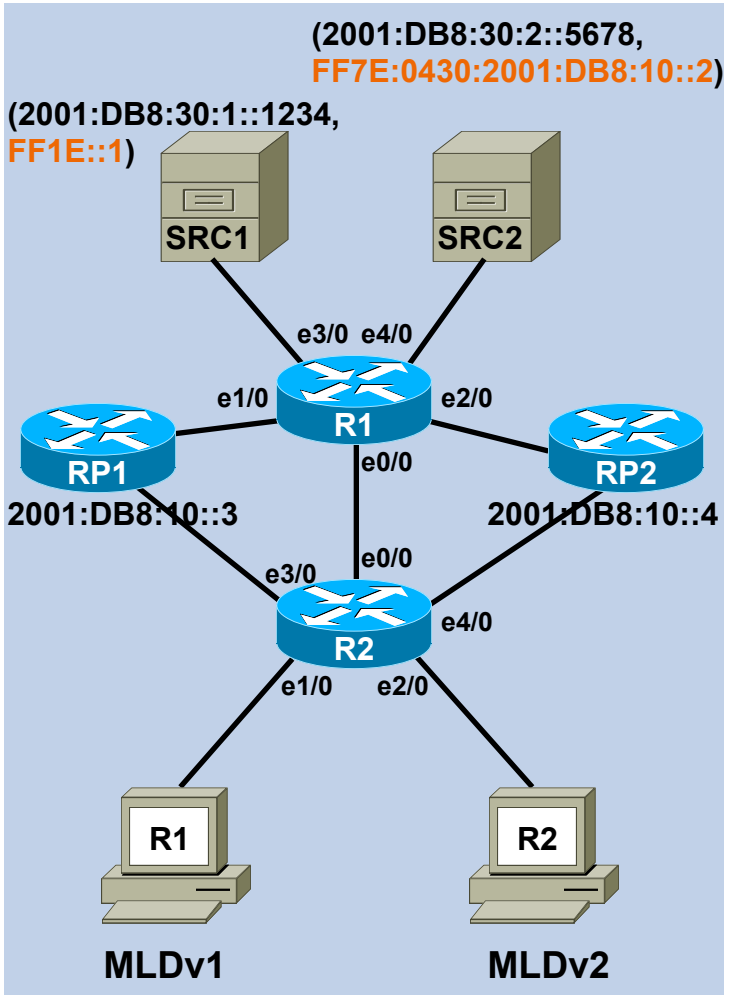


- On R2: both MLDv1 (R1) and MLDv2 (R2) clients active at the moment → source-specific MLD Reports
- Immediate OIL created for (S,G) state

PIM Topology Information - OILs

```
R2#show ipv6 pim topology FF1E::1
IP PIM Multicast Topology Table
…
(output truncated)
…
(2001:DB8:30:1::1234,FF1E::1)
SM SPT UP: 00:04:27 JP: Join(00:00:20) Flags:
RPF: Ethernet0/0,FE80::A8BB:CCFF:FE00:6500
Ethernet2/0          00:04:26  fwd LI LH
```

```
R2#show ipv6 mroute FF1E::1
Multicast Routing Table
…
(output truncated)
…
(2001:DB8:30:1::1234, FF1E::1), 00:07:23/never, flags:
STI
  Incoming interface: Ethernet0/0
  RPF nbr: FE80::A8BB:CCFF:FE00:6500
Immediate Outgoing interface list:
    Ethernet2/0, Forward, 00:07:22/never
Inherited Outgoing interface list:
    Ethernet1/0, Forward, 00:07:23/never
```



Rendezvous Points

IPv6 Multicast RP Mapping Mechanisms

- Static RP
- Embedded RP
- BootStrap Router (BSR)

Static RP Configuration

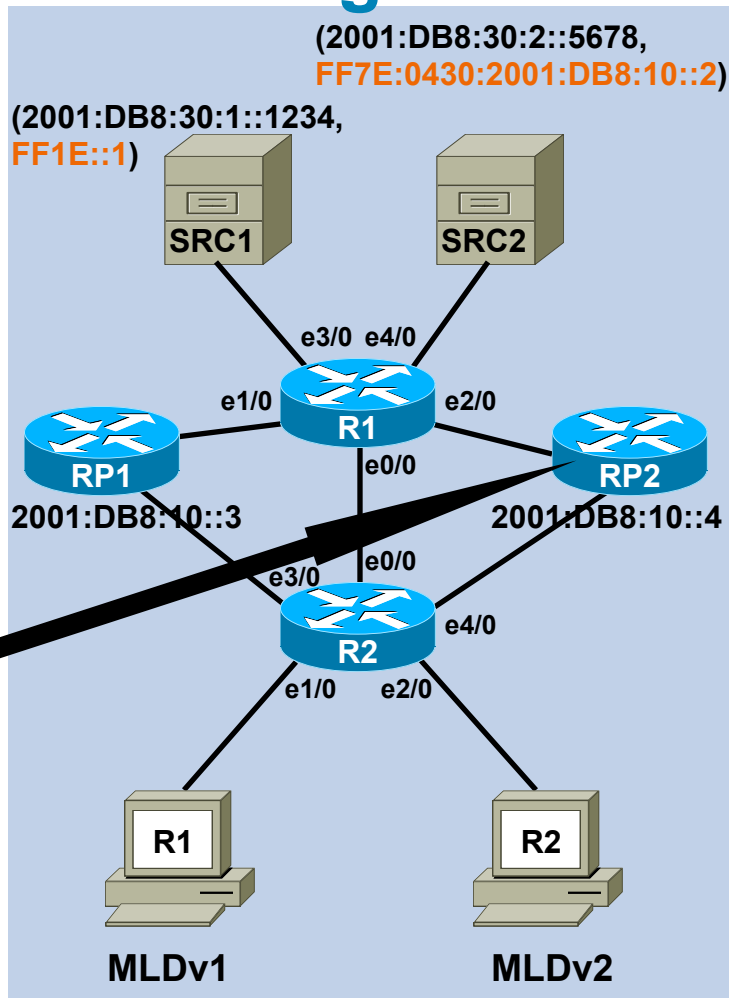
- Hard-configured RP address
  - RP assigned to a loopback (Lo1) on the RP router
  - Same static RP configuration must be on all routers
  - RP can be relocated to another router through configuration
    - Set loopback of “new” RP to the domains RP address
- Command:

```
ipv6 pimrp-address ipv6-address [ group-access-list ]
[ bidir ]
```

  - Optional group list specifies group range
  - bidirkeyword enables a BiDir RP

IPv6 Multicast – Embedded RP Configuration

```
!
ipv6 unicast-routing
ipv6 cef
ipv6 multicast-routing
!
interface Loopback0
 no ip address
 ipv6 address 2001:DB8:10::4/128
 ipv6 ospf 1 area 0
!
ipv6 router ospf 1
 router-id 4.4.4.4
 log-adjacency-changes
 passive-interface Loopback0
!
ipv6 pimrp-address 2001:DB8:10::3
ipv6 pimrp-address 2001:DB8:10::4 ERP
!
ipv6 access-list ERP
 permit ipv6 any FF7E:430:2001:DB8:10::/80
!
```

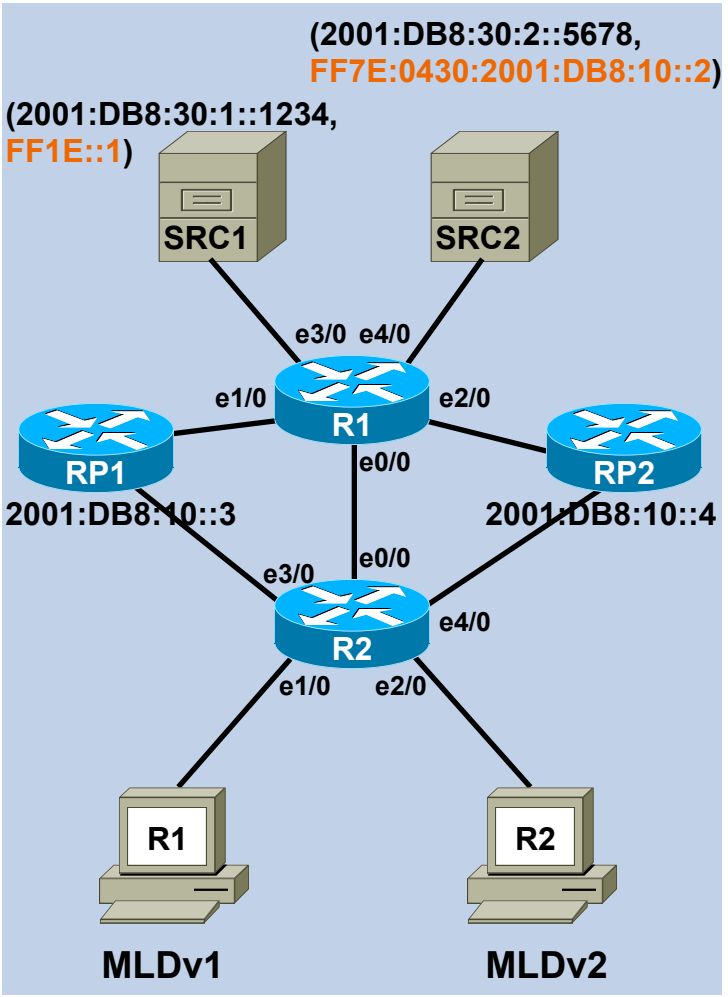


- RP to be used as Embedded RP needs to be configured with address group range
- Other non-RP routers require no special configuration
- Embedded RP does not yet support PIM-Bidir

Embedded RP - display group Mode/ Range/RP Information

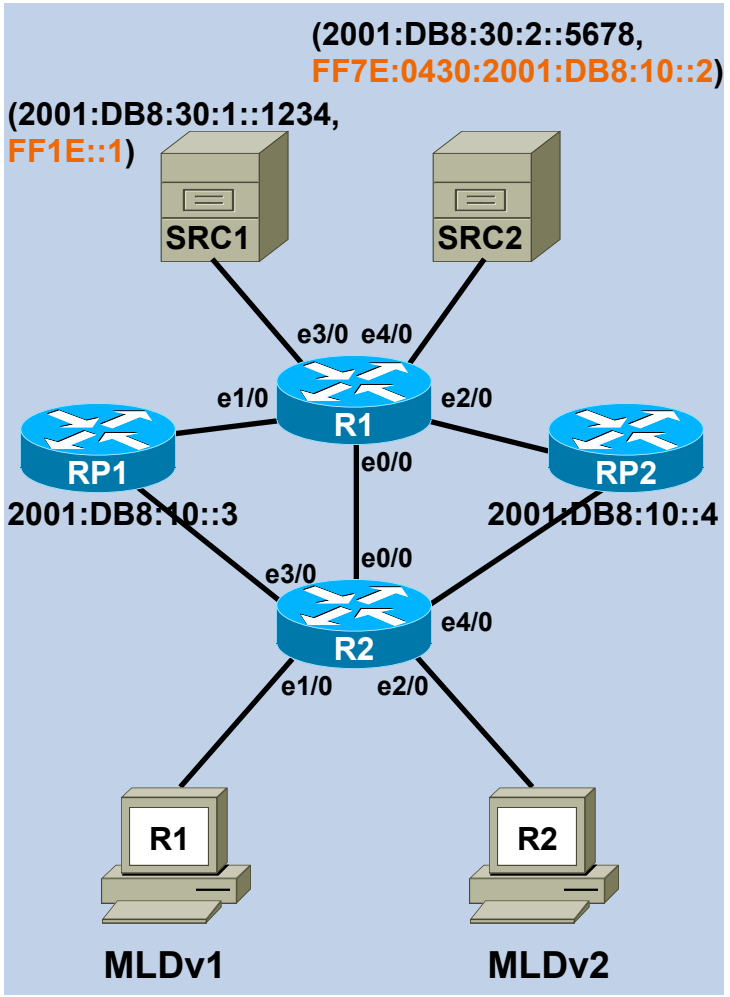
```
R1#show ipv6 pim range-list
Static SSM Exp: never Learnt from : ::
  FF33::/32 Up: 01:04:42
  FF34::/32 Up: 01:04:42
  FF35::/32 Up: 01:04:42
  FF36::/32 Up: 01:04:42
  FF37::/32 Up: 01:04:42
  FF38::/32 Up: 01:04:42
  FF39::/32 Up: 01:04:42
  FF3A::/32 Up: 01:04:42
  FF3B::/32 Up: 01:04:42
  FF3C::/32 Up: 01:04:42
  FF3D::/32 Up: 01:04:42
  FF3E::/32 Up: 01:04:42
  FF3F::/32 Up: 01:04:42
Static SM RP: 2001:DB8:10::3 Exp: never Learnt from : ::
  FF00::/8 Up: 01:04:41
Embedded SM RP: 2001:DB8:10::4 Exp: never Learnt
from : ::
FF7E:430:2001:DB8:10::/80 Up: 01:00:35
```

- No configuration for embedded RP (RP2) on R1
- R1 has learned the embedded RP from SRC2 transmitting to an Embedded RP Group Address (learned through actual data, PIM / MLD joins)



Embedded RP - display Group to RP Mappings

```
R1#show ipv6 pim group-map
IP PIM Group Mapping Table
(* indicates group mappings being used)

FF7E:430:2001:DB8:10::/80*
SM, RP: 2001:DB8:10::4
     RPF: Et2/0,FE80::A8BB:CCFF:FE00:6802
     Info source: Embedded
     Uptime: 01:01:21, Groups: 1
FF33::/32*
SSM
     Info source: Static
     Uptime: 3d01h, Groups: 0
FF34::/32*
     SSM
     Info source: Static
     Uptime: 3d01h, Groups: 0
…
FF00::/8*
     SM, RP: 2001:DB8:10::3
     RPF: Et1/0,FE80::A8BB:CCFF:FE00:6701
     Info source: Static
     Uptime: 3d01h, Groups: 1
…
```



BootStrap Router (BSR) - overview

- Multiple candidate BSRs (C-BSR), single BSR is elected from C-BSR announcements, other C-BSR are backup
  - Uses BSR priority (highest=best), IP address as tie breaker (higher=best), pre-emptive
  - BootStrap messages (BSMs) flooded hop-by-hop to FF02::D (All-PIM routers) controlled by RPF check
- Multiple candidate RPs (C-RP) send unicast announcements to BSR, BSR stores all C-RP announcements in “RP-Set”
- “RP-Set” flooded hop-by-hop to FF02::D (All-PIM routers) controlled by RPF check
- BSM filtering at border through

```
ipv6 pimbsr border
```

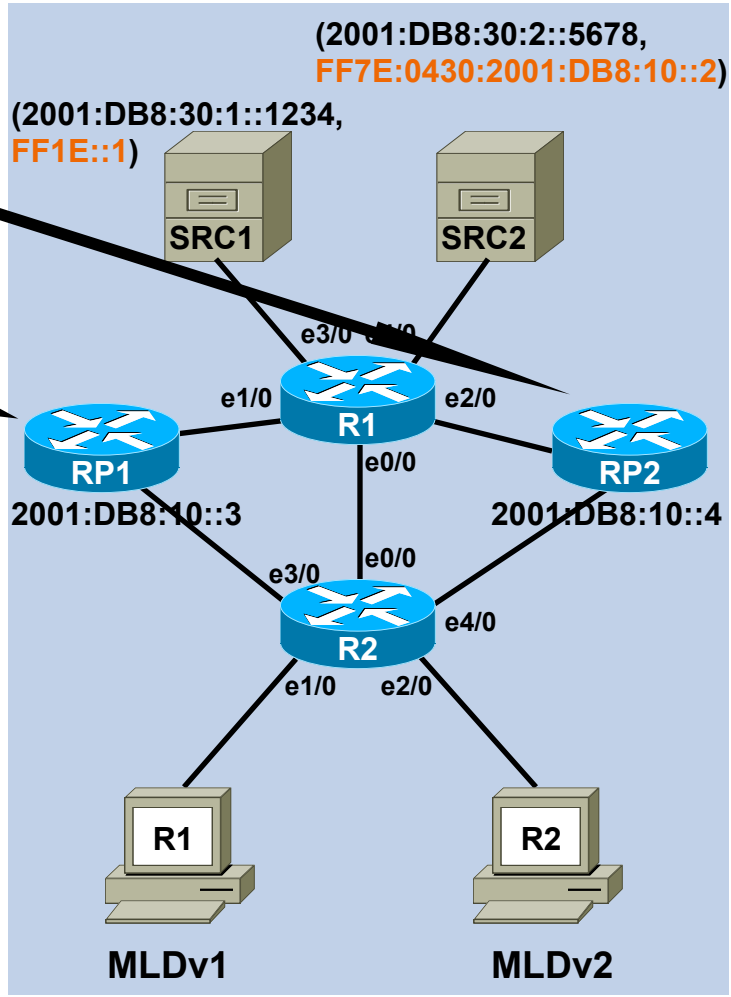
- All routers select RP from the RP-Set, using same algorithm
  - Ensures consistency
  - Uses C-RP priority (lowest=best), hash function value (highest=best) and IP address as tie breaker (highest=best)

BootStrap Router - configuration

```
RP2#show run | i bsr
ipv6 pim bsr candidate bsr 2001:DB8:10::4 priority 20
ipv6 pim bsr candidate rp 2001:DB8:10::4 priority 20
```

```
RP1#show run | ibsr
ipv6 pimbsr candidate bsr 2001:DB8:10::3 priority 10
ipv6 pimbsr candidate rp 2001:DB8:10::3 priority 10
```

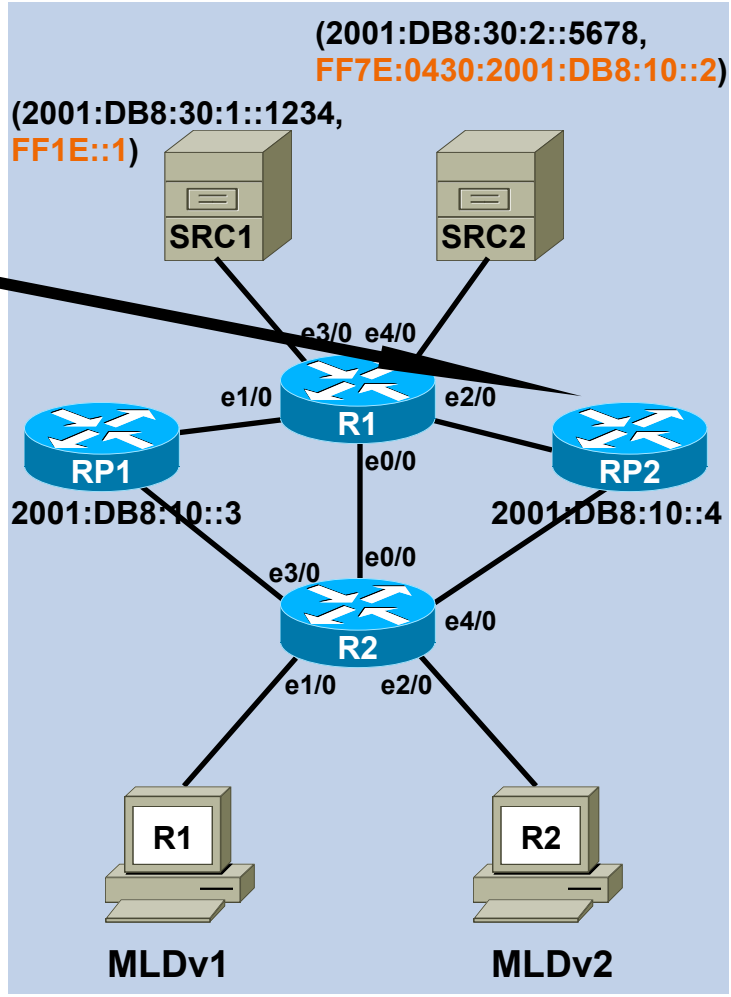
- RP2 will become the BSR



BootStrap Router - Operation

```
RP2#show ipv6 pimbsr election
PIMv2 BSR information

BSR Election Information
  Scope Range List: ff00::/8
  This system is the Bootstrap Router (BSR)
BSR Address: 2001:DB8:10::4
     Uptime: 00:07:18, BSR Priority: 20, Hash mask length: 126
     RPF: FE80::A8BB:CCFF:FE00:6800,Loopback0
     BS Timer: 00:00:43
  This system is candidate BSR
     Candidate BSR address: 2001:DB8:10::4, priority: 20, hash mask
length: 126
```

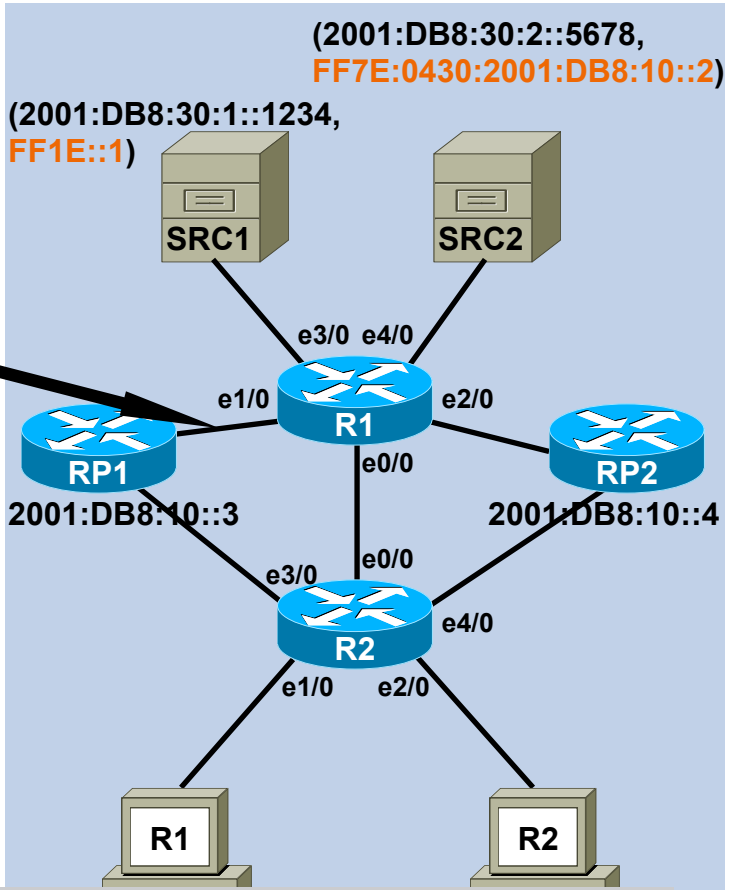
```
RP2#show ipv6 pimbsrrp-cache
PIMv2 BSR C-RP Cache

BSR Candidate RP Cache

Group(s) FF00::/8, RP count 2
RP 2001:DB8:10::3 SM
Priority 10, Holdtime 150
    Uptime: 00:08:34, expires:
00:01:57
RP 2001:DB8:10::4 SM
Priority 20, Holdtime 150
    Uptime: 00:08:34, expires:
00:01:57
```




```
IPv6 BSR: Received C-RP Advertisement from 2001:DB8:10::3, priority 10
holdtime 150, prefix count 1
IPv6 BSR: Updating C-RP cache for 2001:DB8:10::4
IPv6 BSR: Updated received range FF00::/8, mode Sparse
IPv6 BSR: Originating BSM for 2001:DB8:10::4, priority 20 hash mask length
126
IPv6 BSR: Adding Group prefix FF00::/8, RP count 2, Frag RP count 2
IPv6 BSR: Adding RP 2001:DB8:10::3, Priority 10, Holdtime 150
IPv6 BSR: Adding RP 2001:DB8:10::4, Priority 20, Holdtime 150
IPv6 BSR: Sending BSR message on interface Ethernet2/0
IPv6 BSR: Sending BSR message on interface Ethernet4/0
```

BootStrap Router - Operation

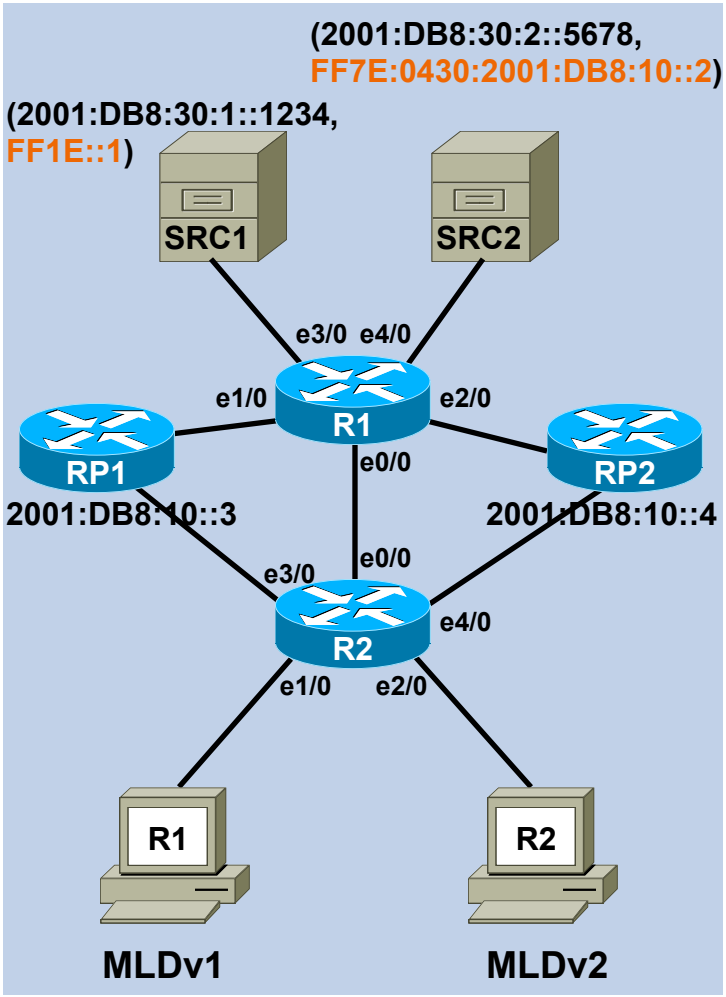
```
R1#show ipv6 pim group-map info-source bsr
IP PIM Group Mapping Table
(* indicates group mappings being used)

FF00::/8*
     SM, RP: 2001:DB8:10::3
     RPF: Et1/0,FE80::A8BB:CCFF:FE00:6701
     Info source: BSR From: 2001:DB8:10::4(00:02:09),
Priority: 10
     Uptime: 00:10:22, Groups: 1
FF00::/8
     SM, RP: 2001:DB8:10::4
     RPF: ,::
     Info source: BSR From: 2001:DB8:10::4(00:02:09),
Priority: 20
     Uptime: 00:10:22, Groups: 0
```




```
IPv6 BSR: Received BSR message from FE80::A8BB:CCFF:FE00:6802 for 2001:DB8:10::4, BSR priority 20
hash mask length 126
IPv6 BSR: Recieved Group range FF00::/8, RP count 2 Fragment RP count2
IPv6 BSR: Update RP 2001:DB8:10::3, Holdtime 150, Priority 10
IPv6 BSR: Update RP 2001:DB8:10::4, Holdtime 150, Priority 20
IPv6 BSR: Received BSR message from FE80::A8BB:CCFF:FE00:6600 for 2001:DB8:10::4, BSR priority 20
hash mask length 126
IPv6 BSR: BSR message from FE80::A8BB:CCFF:FE00:6600/Ethernet0/0 for 2001:DB8:10::4 RPF failed,
dropped
IPv6 BSR: Received BSR message from FE80::A8BB:CCFF:FE00:6701 for 2001:DB8:10::4, BSR priority 20
hash mask length 126
IPv6 BSR: BSR message from FE80::A8BB:CCFF:FE00:6701/Ethernet1/0 for 2001:DB8:10::4 RPF failed,
dropped
```

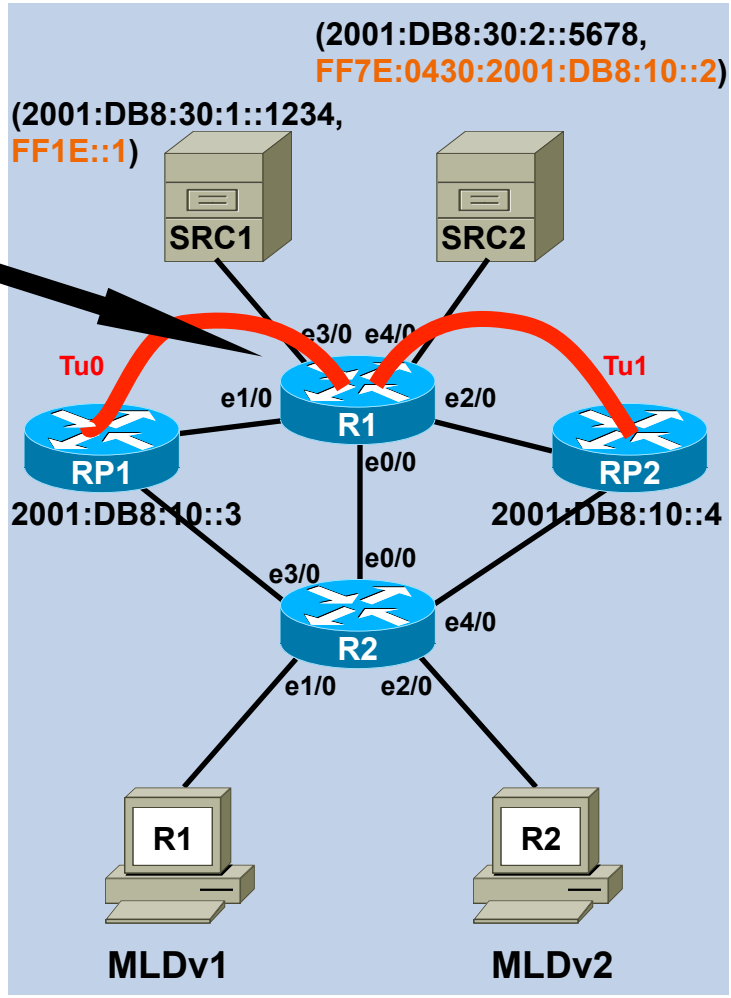
Source Registering – DR

- Automatically creates unidirectional virtual tunnel interfaces
- One virtual tunnel for each active RP in the network
- IOS maintains tunnel as long as RP is known
- Virtual tunnel interface is UP automatically, line protocol is UP only when a valid RPF interface to the RP exists
- PIM Register messages are sent through tunnel. PIM Register-Stop messages are sent directly (NOT through tunnel)



Source Registering – DR

```
R1#show ipv6 pim tunnel
Tunnel0*
  Type   : PIM Encap
  RP     : 2001:DB8:10::3
  Source: 2001:DB8:10::1
Tunnel1*
  Type   : PIM Encap
  RP     : Embedded RP Tunnel
  Source: 2001:DB8:10::1
```

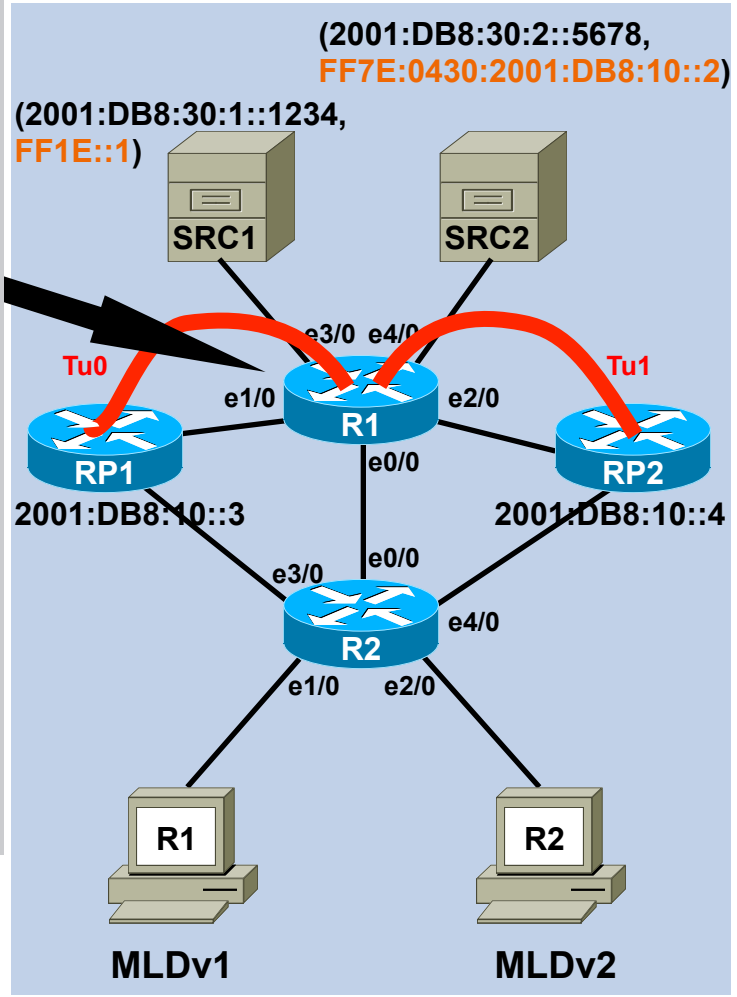


- Tunnel0: statically-defined RP
- Tunnel1: for all embedded RPs (multipoint)

Source Registering – DR

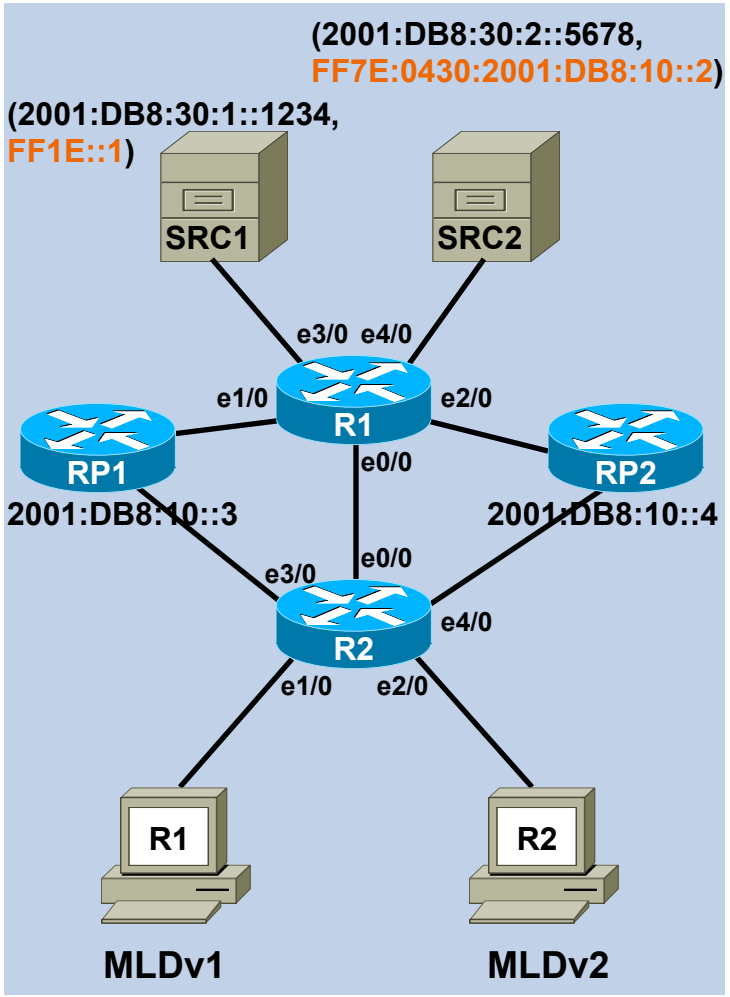
```
R1#show interfaces tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  MTU 1514 bytes, BW 9 Kbit/sec, DLY 500000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
Tunnel source 2001:DB8:10::1 (Loopback0), destination 2001:DB8:10::3
  Tunnel protocol/transport PIM/IPv6
  Tunnel TTL 255
  Tunnel is transmit only
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input never, output 3d02h, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     1 packets output, 88 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

- Unidirectional transmit-only tunnel



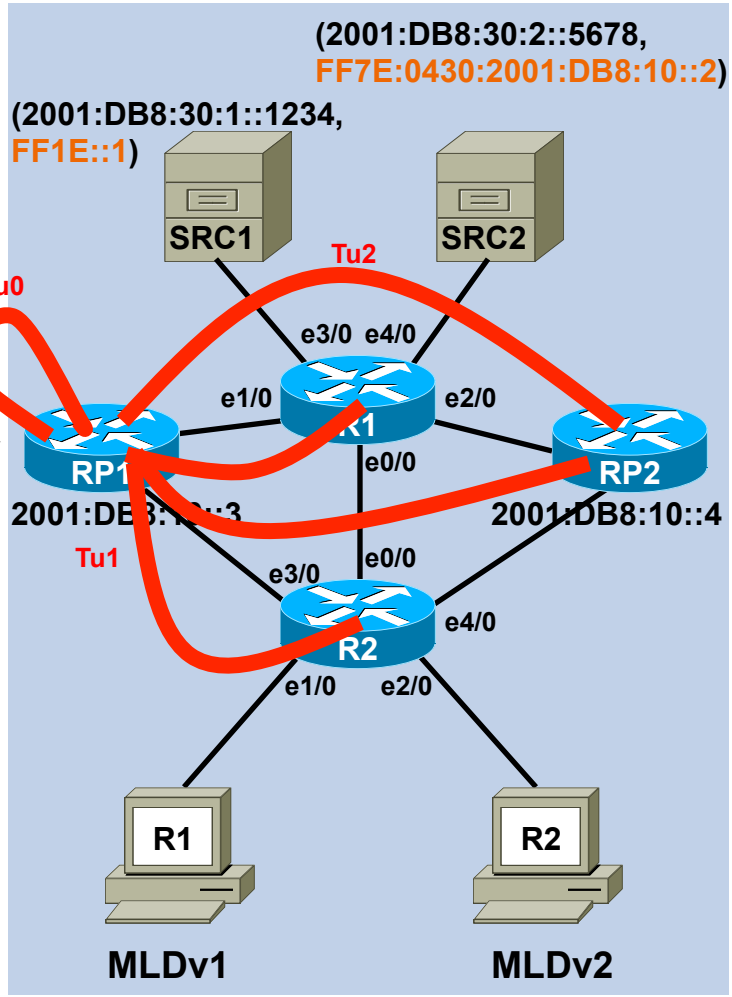
Source Registration

- Automatically creates at least 2 unidirectional virtual tunnel interfaces on the RP
- First is a transmit-only tunnel used for registering sources locally connected to the RP
- Second is a receive-only tunnel used for decapsulating PIM Register messages from all DRs
- There is only a single PIM Decap tunnel to decapsulate ALL PIM Register messages from ALL DRs



Source Registration - tunnels

```
RP1#show ipv6 pim tunnel
Tunnel0*
  Type   : PIM Encap
  RP     : 2001:DB8:10::3*
  Source: 2001:DB8:10::3
Tunnel2*
  Type   : PIM Encap
  RP     : Embedded RP Tunnel
  Source: 2001:DB8:10::3
Tunnel1*
  Type   : PIM Decap
  RP     : 2001:DB8:10::3*
  Source:  -
```



- Tunnel 0: for sending Register messages for locally attached sources to itself (transmit-only)
- Tunnel 2: for sending Register messages to all embedded RPs (1 multipoint tunnel, transmit-only)
- Tunnel 1: for receiving Register messages from all DRs (single, receive-only)
- PIM registers can be restricted at RP through **`ipv6 pim accept-register`**

RP Redundancy options

- RP is single point of failure therefore redundancy is required
- MSDP-Anycast-RP impossible (no MSDP for IPv6)
- Prefixlength-Anycast-RP (aka PriorityCast-RP)
  - 2 (or more) RPs with same IPv6 address, but different masks
  - PIM Registers and (*,G) Joins forwarded to RP with longest-prefix match
  - Slower convergence due to periodic register messages
  - Topology considerations (RP-on-a-stick)
- PIM-Anycast-RP (RFC 4610)
  - Anycast-RP (without MSDP0 by extending PIM Register mechanism
  - Cisco implementation planned
- BSR provides RP redundancy
  - Slower convergence than MSDP-anycast-RP
  - Active protocol operations required in all routers

Source Specific Multicast (SSM)

Source Specific Multicast

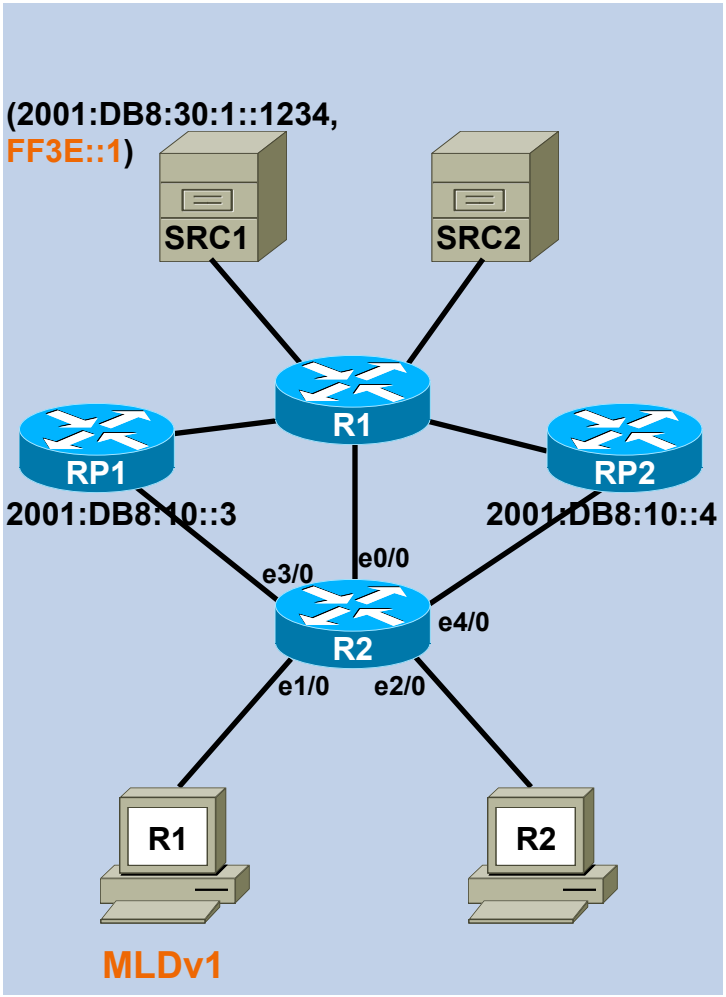
- PIM SSM is just a subset of PIM SM
- PIM, Topology Table, MRIB, MFIB all apply to SSM
- Only required configuration:

```
ipv6 multicast-routing
```

- Requires MLDv2 on receiver

SSM Source Mapping

- SSM transition through SSM Mapping for MLDv1 messages – static or DNS
  - When MLDv2 is not available on the endpoint
  - SSM Mapping will map MLDv1 Reports to a multicast source
  - Mapping can be done statically or though DNS (default)

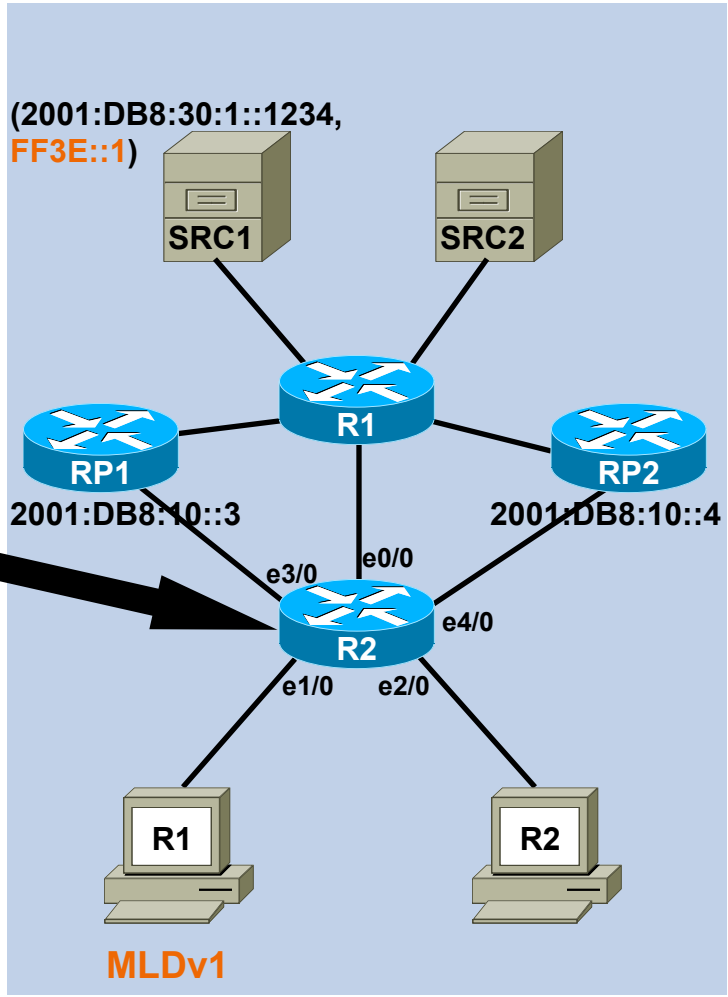



```
!
ipv6 mld ssm-map enable
ipv6 mld ssm-map static SSM_MAP 2001:DB8:30:1::1234
no ipv6 mld ssm-map query dns
!
ipv6 access-list SSM_MAP
 permit ipv6 any host FF3E::1
!
```

SSM Source Mapping

```
R2#show ipv6 pim topology FF3E::1
IP PIM Multicast Topology Table
…
(output truncated)
…
(2001:DB8:30:1::1234,FF3E::1)
SSM SPT UP: 05:38:16 JP: Join(00:00:28) Flags:
RPF: Ethernet0/0,FE80::A8BB:CCFF:FE00:6500
  Ethernet1/0          05:38:16   fwd LI LH
```

```
R2#show ipv6 pim group-map FF3E::1
IP PIM Group Mapping Table
(* indicates group mappings being used)

FF3E::/32*
SSM
    Info source: Static
    Uptime: 05:44:46, Groups: 1
```



- No (*,G) state

Inter Domain IPv6 Multicast - options

- Problem: how to allow receivers to discover sources?
- Option 1: SSM

  Clients require MLDv2 or use SSM Source Mapping

  (S,G) discovery required
- Option 2: ASM with Embedded RP

  Requires all routers in the path to support Embedded RP mechanism
- Option 3: ASM with single shared RP between multicast domains

  Not really practical (requires co-ordination between multicast domains)
- No Multicast Source Discovery Protocol (MSDP) which (in IPv4 multicast) provides “Source Active” announcements between RPs

Conclusions

Conclusions

- IPv6 multicast technology advantages
  - Large address space / “owned” multicast address space
  - Built-in scope
  - Embedded RP
  - No NAT required
- Innovative production IPv6 multicast services exist
  - Hikari-TV (NTT): TV broadcast (SD/HD), 10000+ VoDs, 13000+ karaoke titles
  - Earthquake Early Warning System (NTT Communications): estimated earthquake intensity, #seconds countdown based on location. Estimated 1 sec reaction time.
- Widely deployed in NRENs, GEANT, Internet2, TEIN2, CERNET, etc…

IPv6 Multicast Based Multimedia Services (NTT-East)

- NTT-East rolled out native IPv6 multicast services instead of IPv4 offering IPTV, music and games:

  http://www.ipv6style.jp/en/action/20040902/index.shtml

  http://www.networkworld.com/news/2009/010809-ntt-ipv6-tv.html

Deployment References

- NTT

  http://www.afrinic.net/meeting/afrinic-7/presentations/26/AFRINIC7_JPNIC%20IPv6_Deployment.pdf

- CESNET

  http://www.cesnet.cz/doc/techzpravy/2007/cesnet-ipv6-multicast/

- JANET

  http://www.ja.net/documents/publications/technical-guides/ipv6-multicast-web.pdf

References

- CCO:

  http://www.cisco.com/ipv6

- IOS:

  http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-roadmap.html

- IOS-XR:

  http://www.cisco.com/en/US/docs/routers/crs/software/crs_r3.9/multicast/configuration/guide/mc39mcst.html

- IPv6 Multicast and MPLS

  http://www.computer.org/portal/web/csdl/doi/10.1109/ICCGI.2006.65

  http://ieeexplore.ieee.org/xpl/RecentCon.jsp?punumber=4124012

Agenda

- Introduction
- IPv6 in the Enterprise
- Routing Considerations
- Security for IPv6
- First Hop Security
- Unified Communications
- Multicast
- DNS
- Deployment and Operation Considerations

IPv6 – DNS

What You Will Learn

- To use IPv6 with DNS, you need to perform a series of tasks, explained here
- We will also explain some DNS-specific terms and processes, but you are expected to already have a working DNS set up for IPv4 and a basic knowledge of DNS
- For more information about DNS, see the For More Information section at the end of this document

Basic Steps - 1

- Add AAAA records in your DNS server for the hostnames of the devices that can be reached through the IPv6 protocol.
- Add pointer (PTR) records in your DNS server for the IP addresses of the devices that can be reached through the IPv6 protocol.
- Enable IPv6 access to the authoritative DNS servers. Be sure that TCP/53 and UDP/53 can be accessed through IPv6.
- Enable IPv6 connectivity to the external full-service resolvers that send DNS queries to authoritative servers in the world.

Basic Steps - 2

- Make sure that the full-service resolver is configured with both IPv4 and IPv6 glue for the root servers in the world.
- Enable IPv6 on the recursive resolver so that it responds to DNS requests over IPv6 as well as IPv4.
- Enable IPv6 on the node that sends queries so that it can send DNS requests to the recursive resolver.
- Configure the stub resolver on the node that sends queries so that it uses IPv6 to send DNS queries, either statically or using Dynamic Host Configuration Protocol Version 6 (DHCPv6).
- Review policies for flows and make sure that both TCP/53 and UDP/53 can be accessed over IPv4 and IPv6

DNS Basics and Terminology Used

- The Domain Name System, or DNS, is both the namespace and database
- DNS involves three hosts:

  the client that runs an application that needs the address for given a hostname

  the intermediary server that responds to this query and acts as a proxy

  the authoritative server that holds the authoritative data

Queries - Recursion

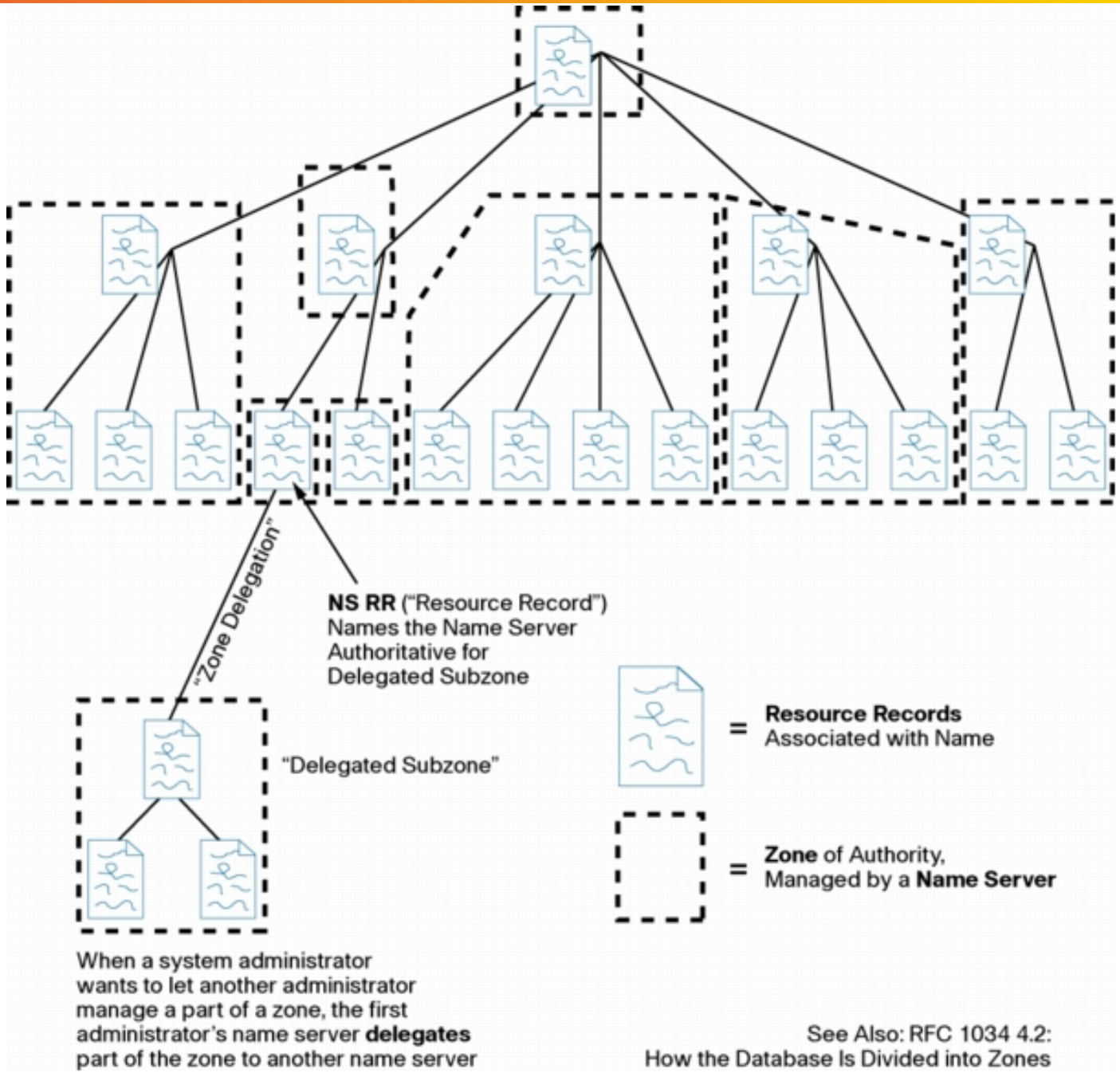
- Queries can be sent either with a request from the client that the server provide recursion, or without such a request
- If recursion is requested, the server can choose to deny this request
- A client that runs an application the needs responses normally runs a resolver, which always requests recursion
- An intermediary server can use a forwarder, in turn using another intermediary server for all its queries

Responses

- When a name server record (NS) is sent back to, and received by the client, the client must look up the IP address to which the hostname refers

  This is because the next query is to be sent to the host which the NS record refers to

- If the hostname is in the delegated zone, a difficulty occurs: only the server the IP address refers to knows the answer to the query regarding hostname to IP address mapping
- In this special case, the server that returned the name server records, in addition to the name server records that refer to the hostname, also includes the IP addresses of the hostnames that are in the delegated zone – glue records



Introduction to DNS and IPv6

- When you introduce IPv6, you will use both IPv4 and IPv6 addresses in your network
- Therefore, you need to add mappings from names to IPv6 addresses in parallel with the existing mapping from names to IPv4 addresses
- One example of such a mapping, using the AAAA resource record type, is shown here:

  www.ipv6.cisco.com. 86400 IN AAAA 2001:420:80:1::5

- Mapping from a name to an IPv6 address is performed using an AAAA resource record, with the IPv6 address given as a hexadecimal address (RFC 3596)

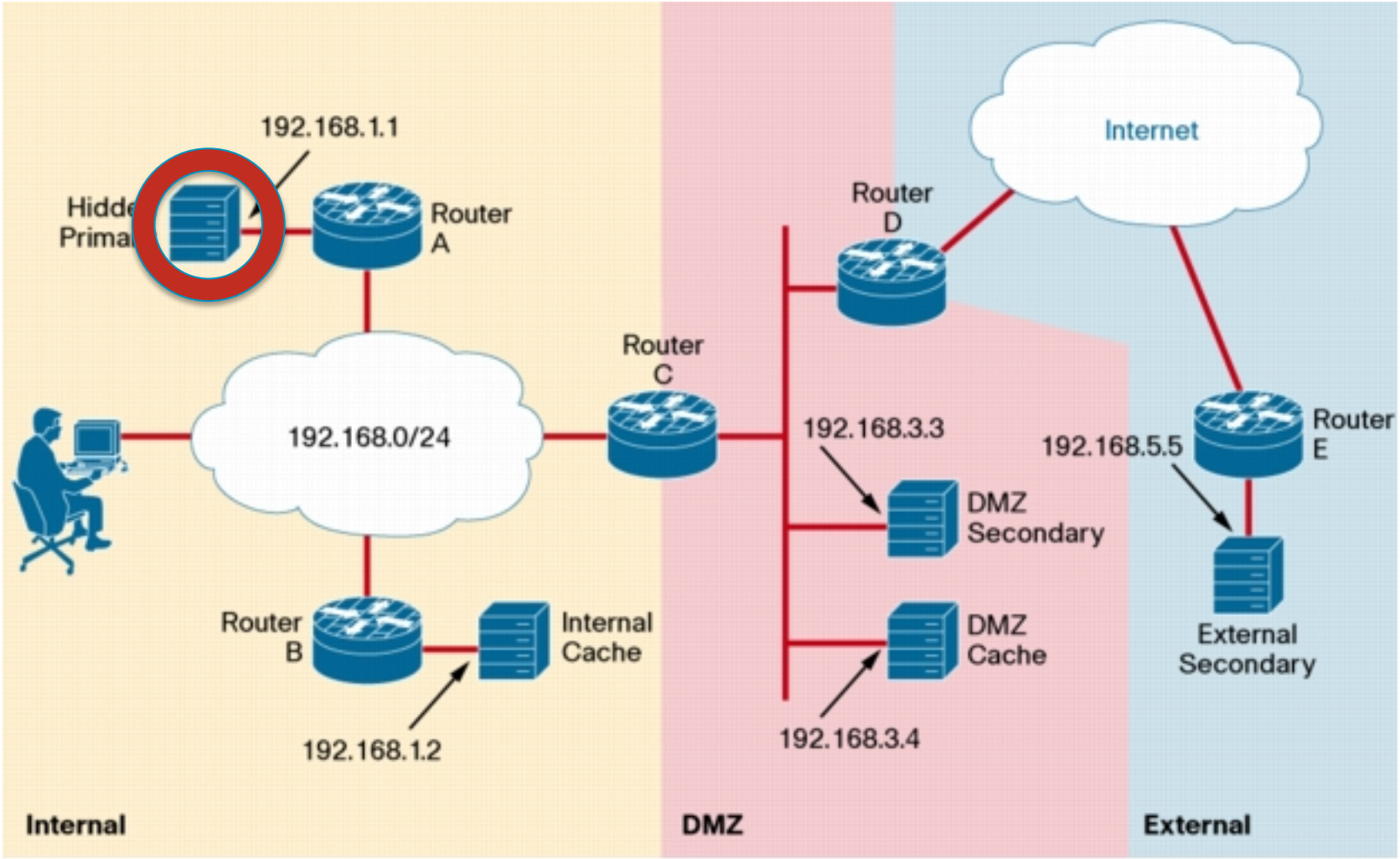
Task 1

- Add AAAA records in your DNS server for the hostnames of the devices that can be reached through the IPv6 protocol

5.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.0.8.0.0.0.2.4.0.1.0.0.2.ip6.arpa.
900 IN PTR www.ipv6.cisco.com.

Task 2

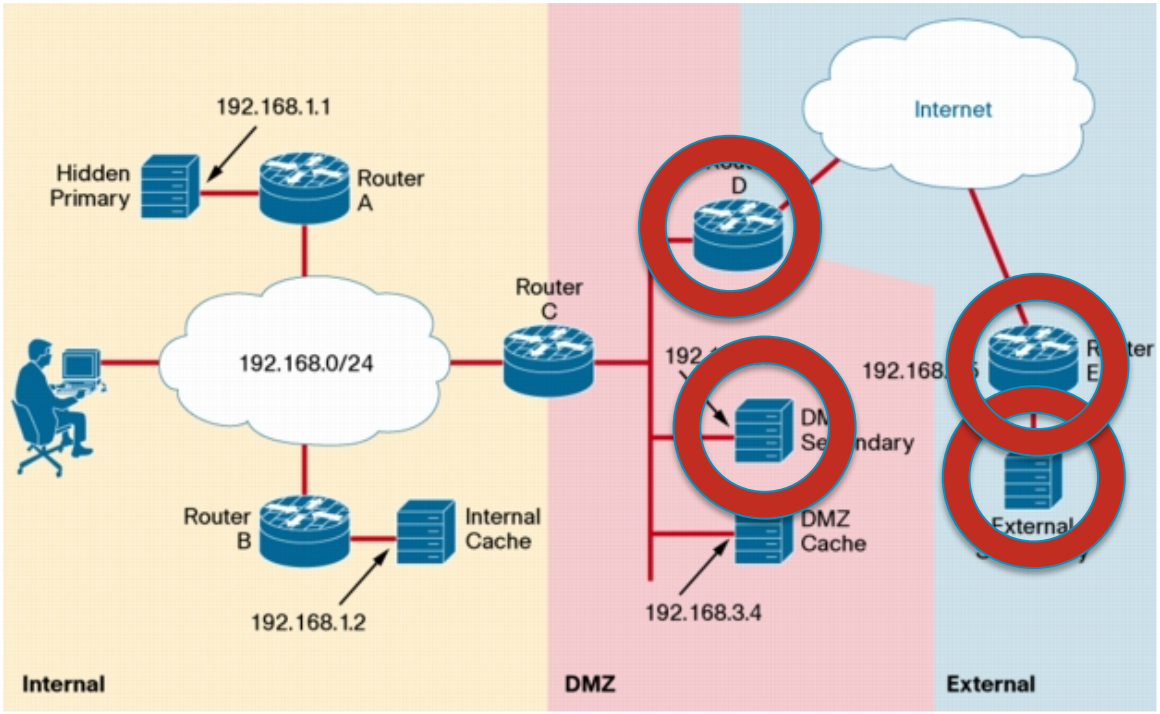
- Add PTR records in your DNS server for the IP addresses of the devices that can be reached through the IPv6 protocol
- Having data in the namespace is not enough for successful DNS deployment in an IPv6 environment because that data is accessible only using the IPv4 protocol
- This step is needed to start the use of IPv6 as a transport for the DNS protocol



Task 3

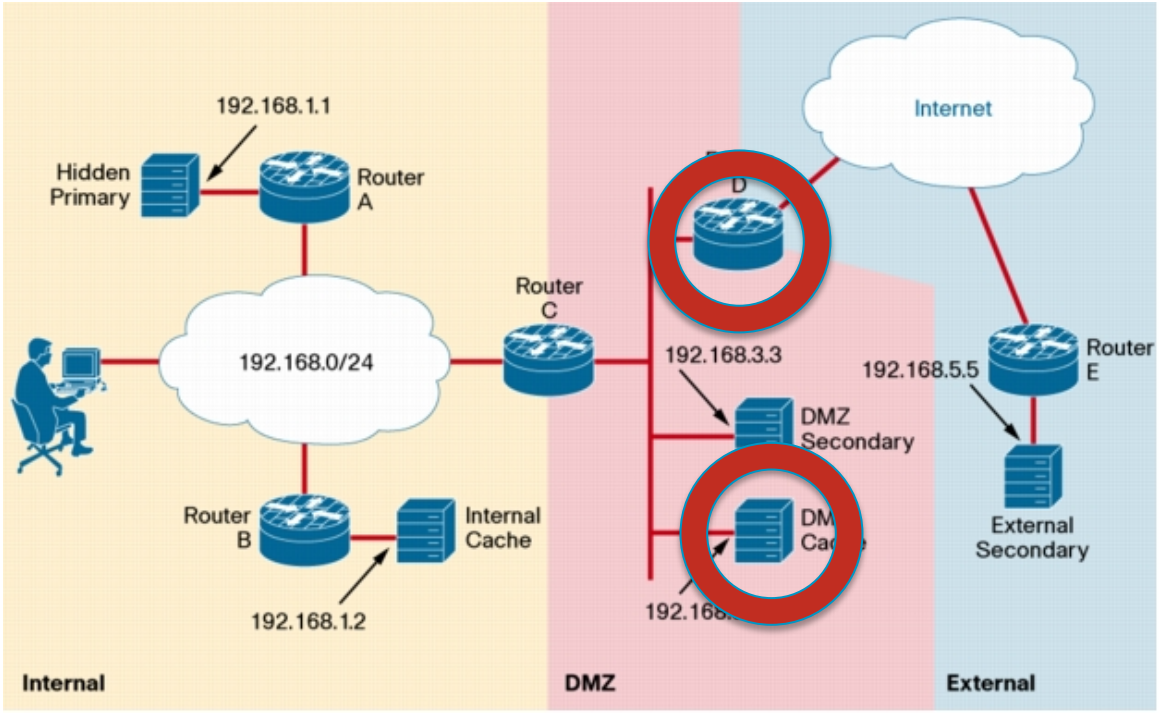
- Enable IPv6 access to the authoritative DNS servers

  Be sure that TCP/53 and UDP/53 can be accessed through IPv6



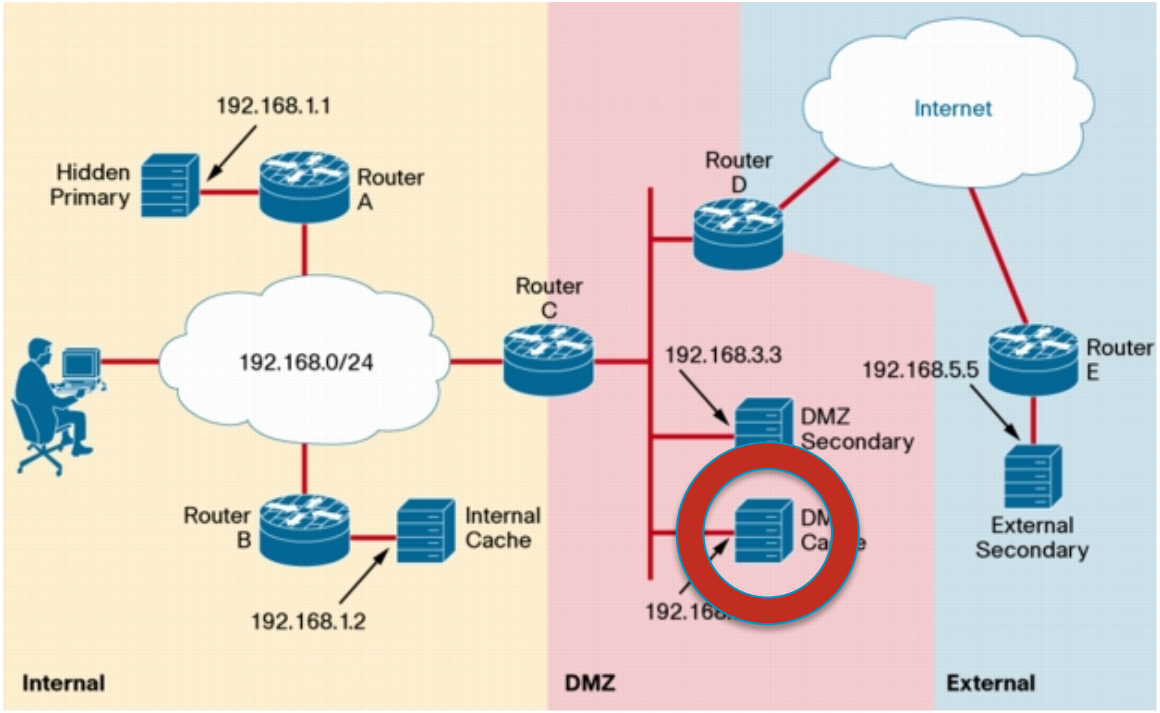
Task 4

- Enable IPv6 connectivity to the external full-service resolvers that send DNS queries to authoritative servers in the world



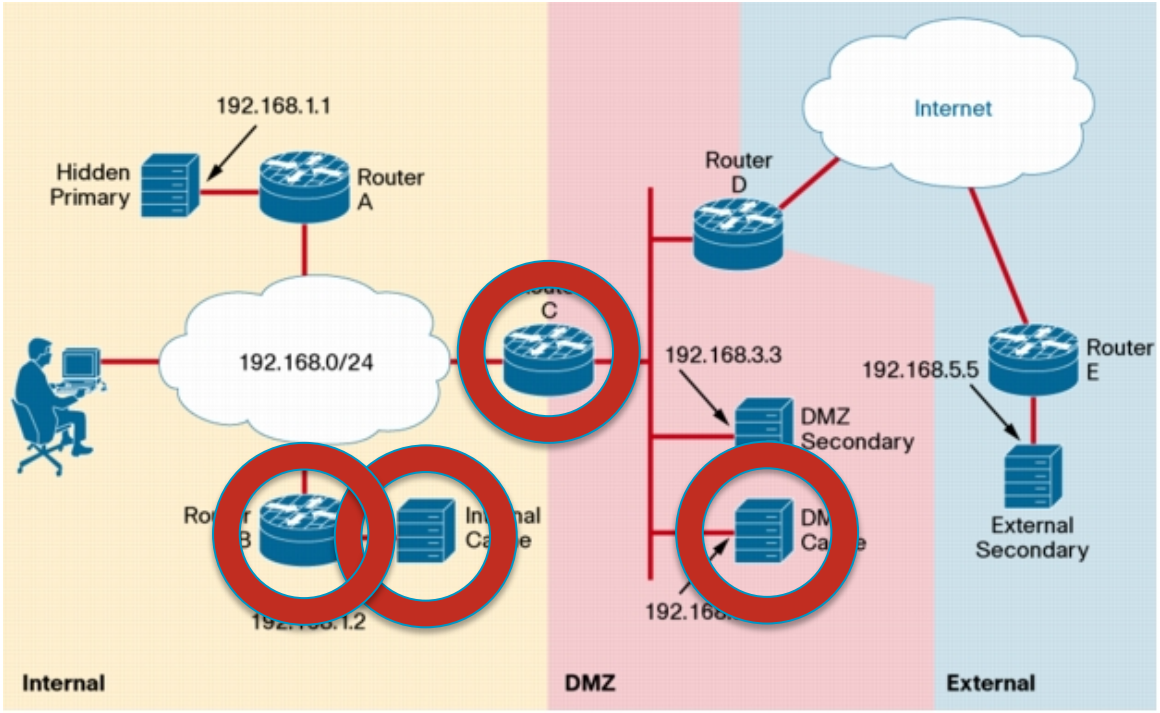
Task 5

- Make sure that the full-service resolver is configured with both IPv4 and IPv6 glue for the root servers in the world



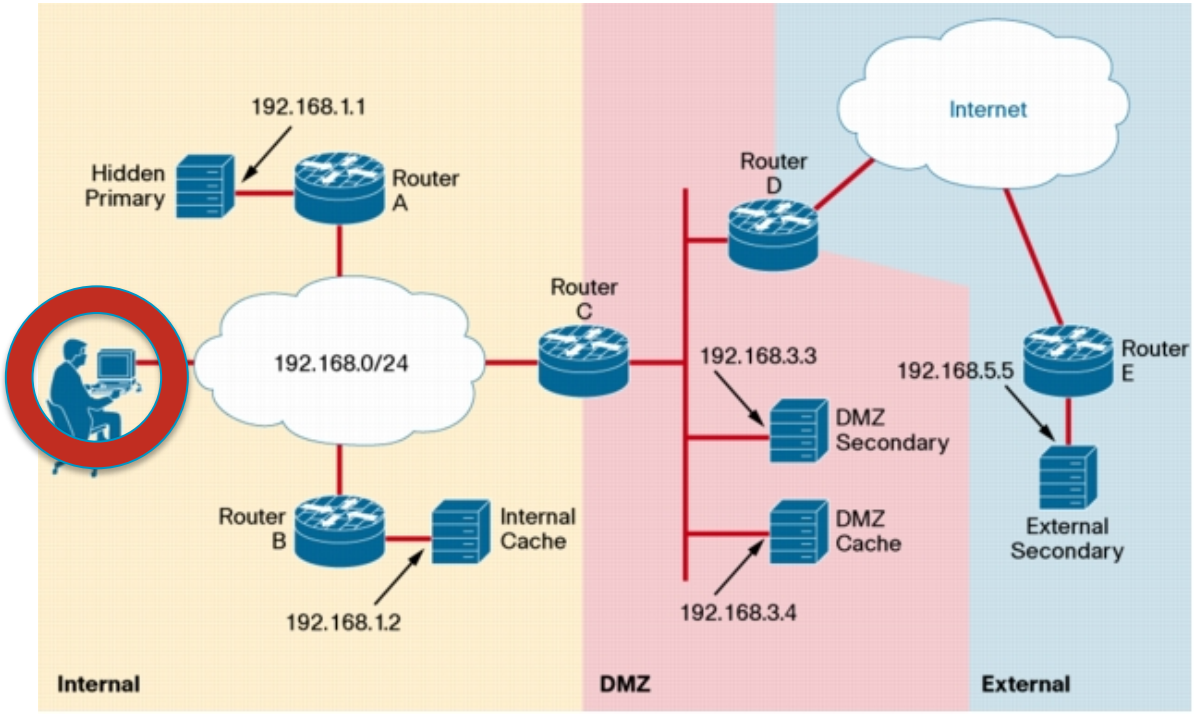
Task 6

- Enable IPv6 on the recursive resolver so that it responds to DNS requests over IPv6 as well as IPv4



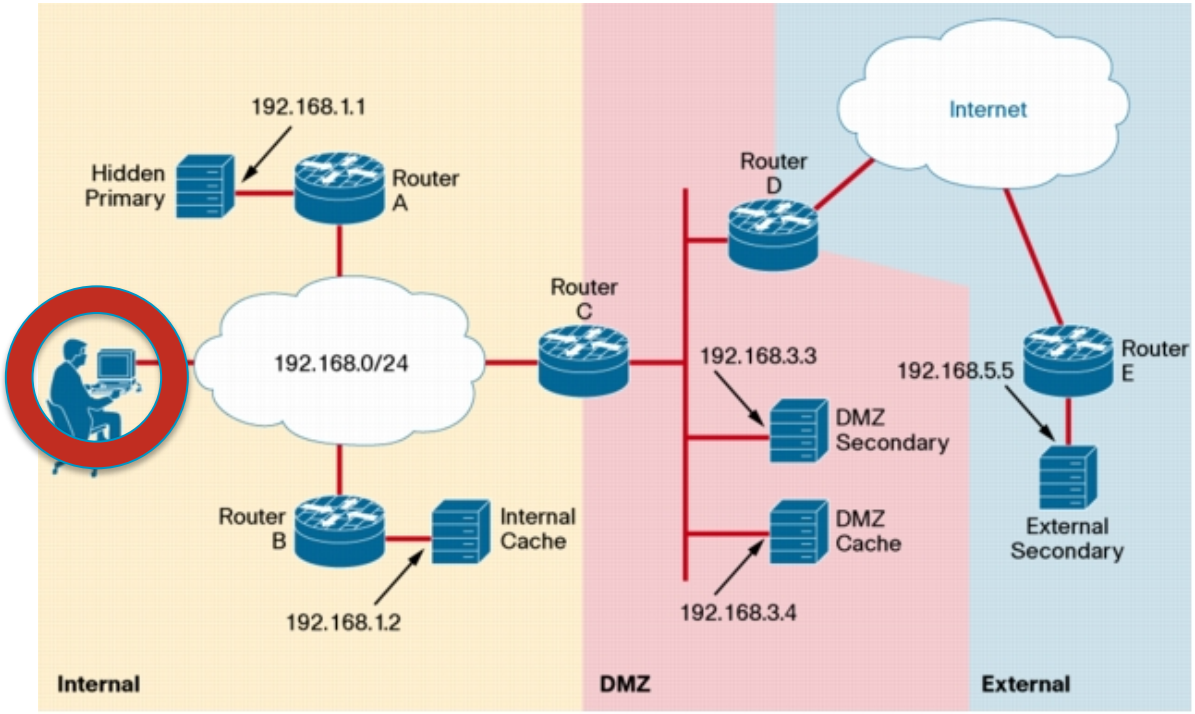
Task 7

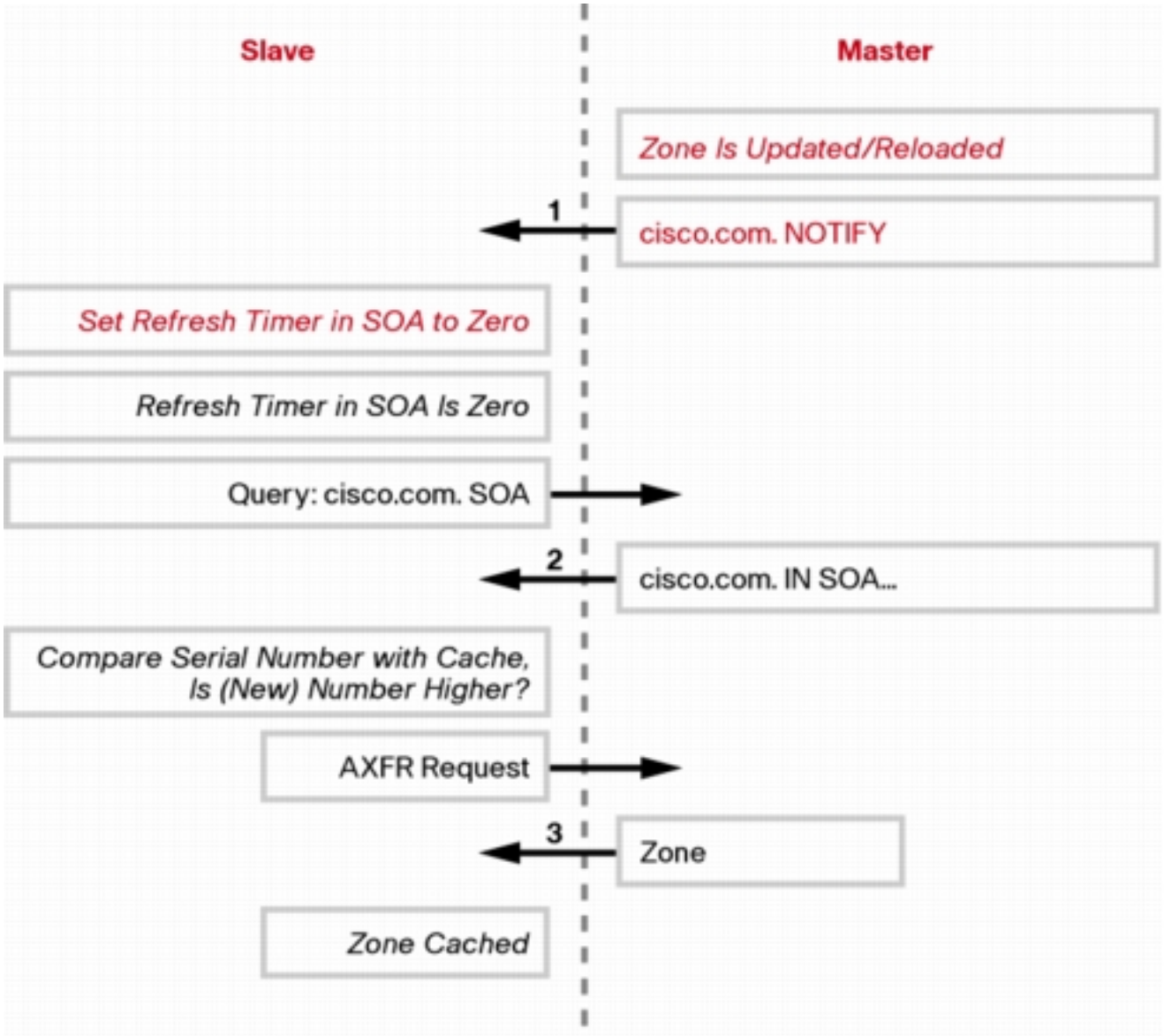
- Enable IPv6 on the node that sends queries so that it can send DNS requests to the recursive resolver



Task 8

- Configure the stub resolver on the node that sends queries so that it uses IPv6 to send DNS queries, either statically or using DHCPv6





Task 9

- Review policies for flows and make sure that both TCP/53 and UDP/53 can be accessed over IPv4 and IPv6

References

- *DNS and BIND, 5th Edition,* by Cricket Liu and Paul Albitz, O'Reilly Media, May 2006
- RFC 3596: DNS Extensions to Support IP Version 6, by S. Thomson, C. Huitema, V. Ksinant, and M. Souissi, October 2003 (format: TXT=14093 bytes) (obsoletes RFC 3152 and RFC 1886) (status: Draft Standard)

Agenda

- Introduction
- IPv6 in the Enterprise
- Routing Considerations
- Security for IPv6
- First Hop Security
- Unified Communications
- Multicast
- DNS
- Deployment and Operation Considerations

Deployment and Operation Considerations

Deployment and Operation Considerations Agenda

- How to get started
- Enterprise Adoption Phases
- Deployment Considerations
- Network and Application Assessment
- Network Management Operations Considerations
- Cisco IT Strategy
- Phased IPv6 Approach
- Summary

How to get Started

How Do we Get There from Here?

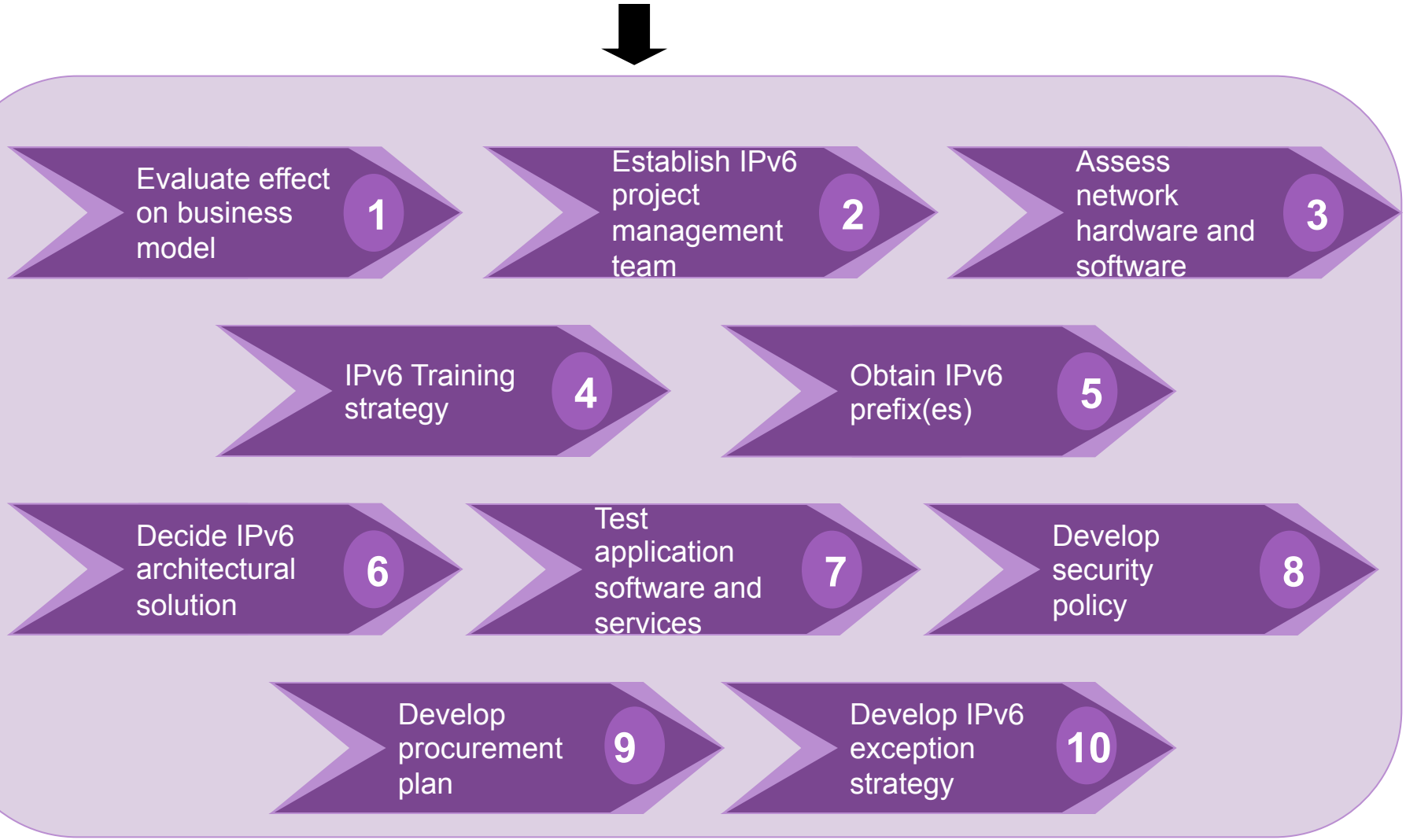
- IPv4 & IPv6 will coexist for the foreseeable future
  - No D-Day / Flag Day.
- Education & Careful Planning are crucial.
  - How long does it take in your environment?
  - What impacts are there to the existing network?
- IPv4 & IPv6 implementations must be scalable, reliable, secure and feature rich.

Strategy that reflects this …

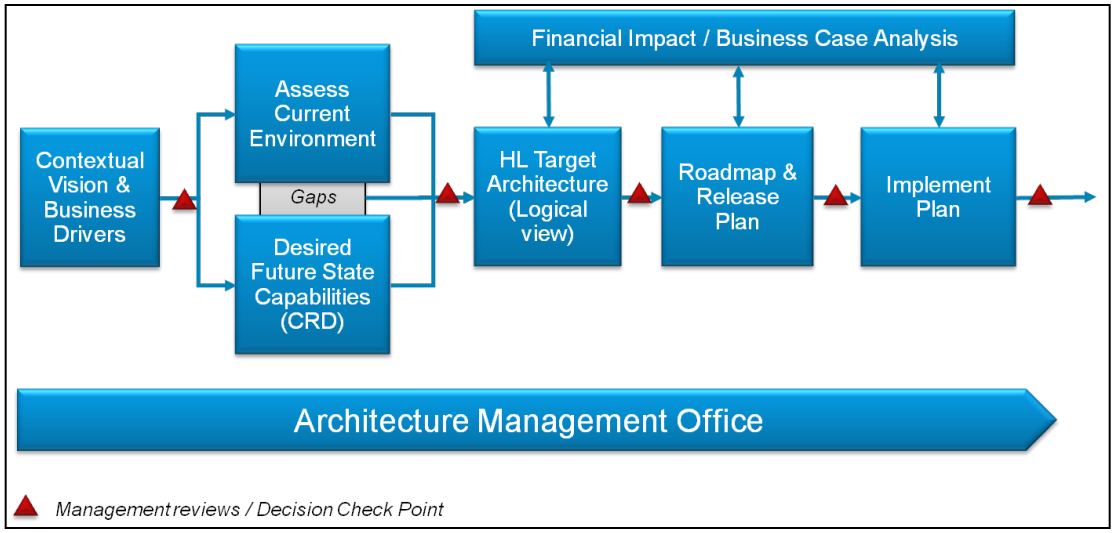
Starting with Edge upgrades enable IPv6 service offerings now

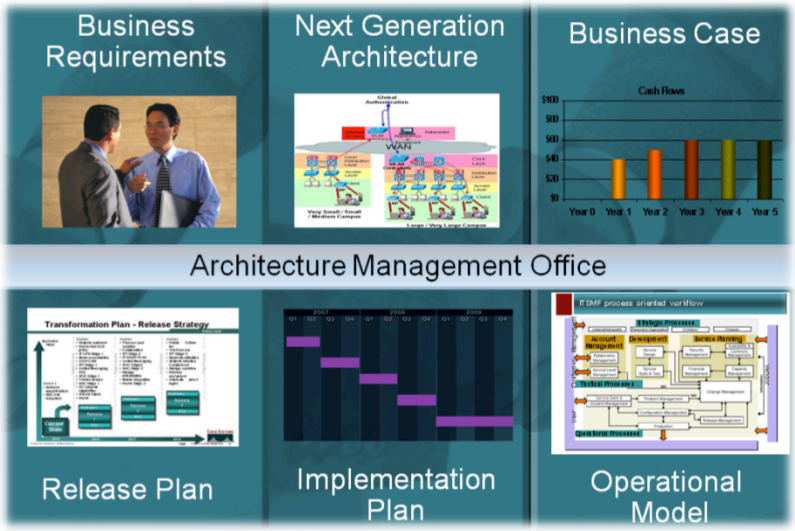
IPv6 Planning Steps

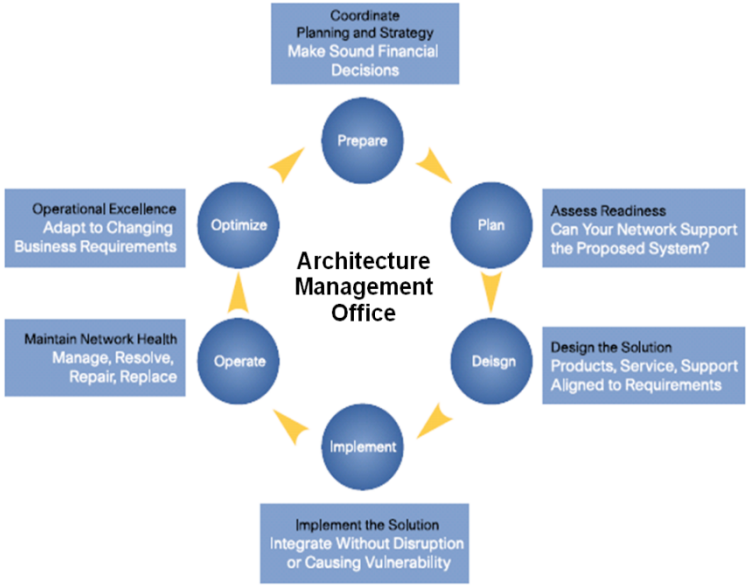
Business Case Identified/Justified



A life Cycle approach that delivers a full transformation journey ...





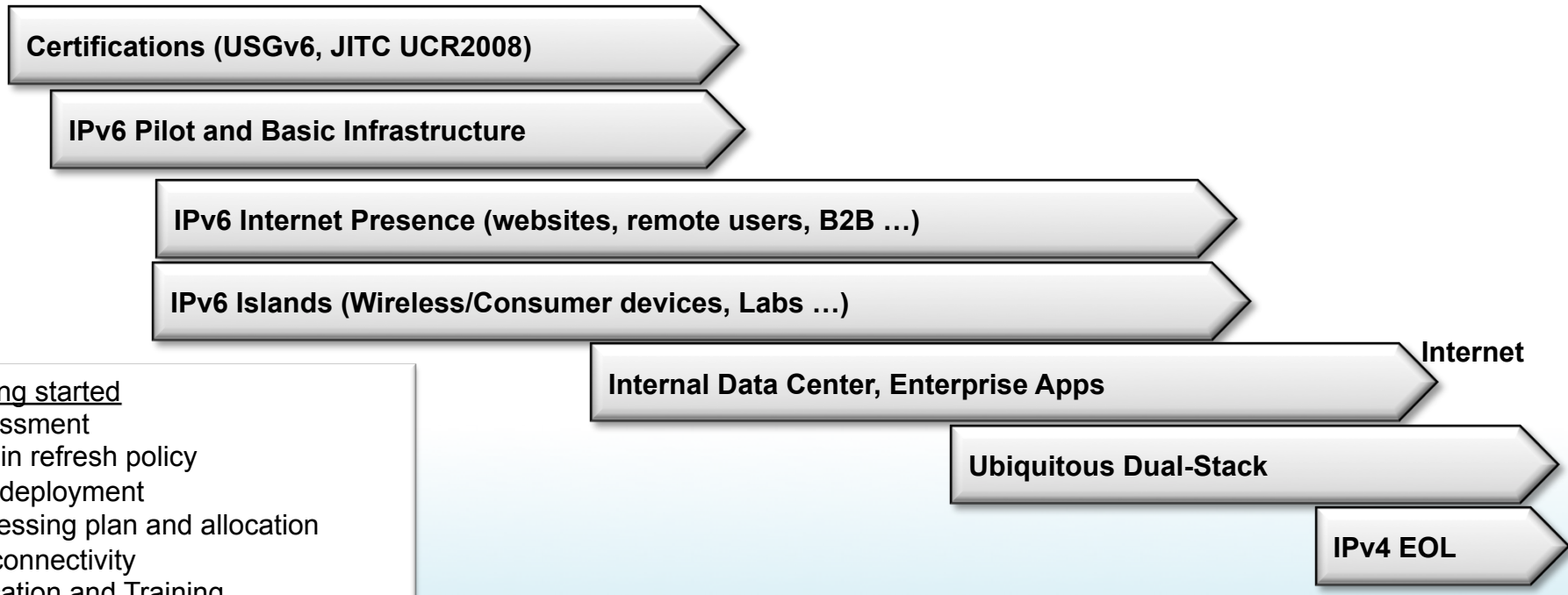


Process is Critical

- If you think it is just about technology, you are mistaken
- If you think it is just about the services, you are mistaken
- It is about active support throughout the organization
  - From executive to individual contributor level
  - From purchasing to development
  - From design to deployment
  - From network infrastructure to Application deployment
- The process focus helps minimize costs, properly orchestrate alongside inflight projects, achieve goals
- Create a virtual team of IT representatives from every area of IT to ensure coverage for OS, Apps, Network and Operations/Management

Enterprise Adoption Phase

Enterprise Adoption Stages and Considerations



Getting started
Assessment
IPv6 in refresh policy
Pilot deployment
Addressing plan and allocation
ISP connectivity
Education and Training

Network Design Choices and Deployment

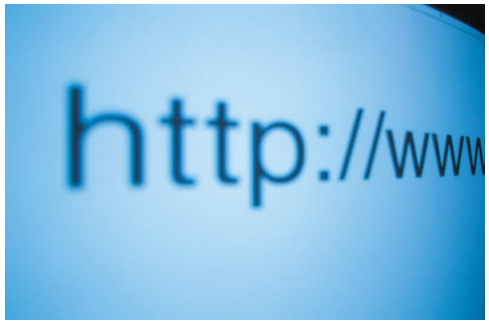
Host configuration (DHCPv6 vs. SLAAC)
Routing (OSPFv3, IS-IS, EIGRP)
DNS (ipv6.company.com vs. www.company.com)
Tunneling and Overlay networks (GRE, ISATAP, etc)
Native or dual stack
NAT
Security (Firewalls, Antispoofing)
Peering/Transit
Network Management

Applications

Web applications
Collaboration (Voice, Video, etc)
Enterprise Software
Custom Applications
IPv6-Only Applications

Why Should an Enterprise Add an IPv6 Internet Presence?

- To be ready for IPv6
- Regulations or incentives
- To keep applications running
- Unique IP address per user
- Customers having only IPv6 connectivity
- Competitive Advantage
- Do not get left behind
- Business Growth
- New areas of expansion Smart Grid, Smart and Connected communities



Enterprise Deployment Considerations

Requirements for any IPv6 Transition Strategy

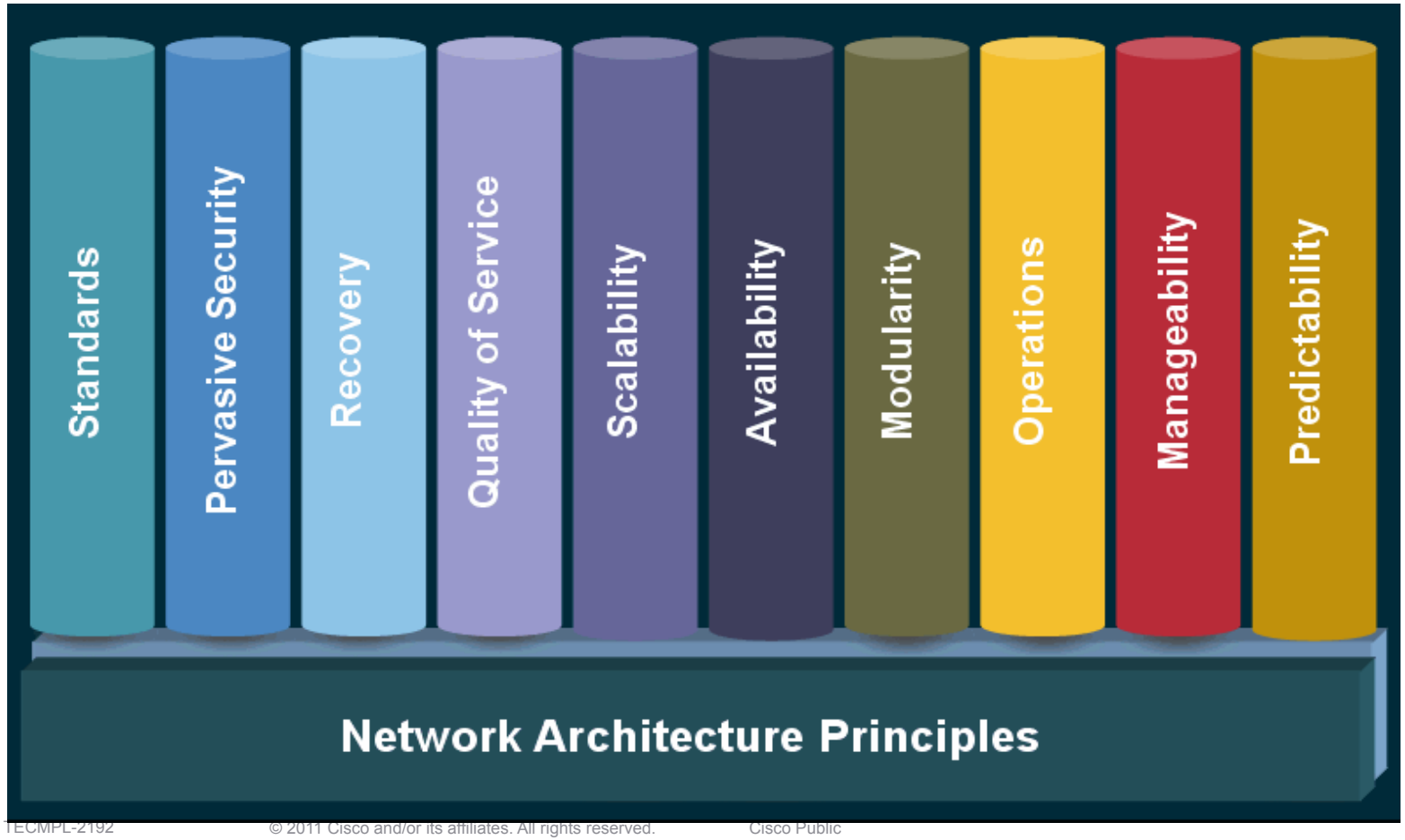
- Must be low-cost and low-risk
- Must co-exist with existing IPv4 infrastructure
- Must allow access to public IPv4 Internet
- Must be incrementally deployable
- Must understand the cost of adding a new services
- Must not impact existing services.
- Nobody should know the integration occurred (seamless)

Issues for the IT Organization

- Cost
- Staff training
- Develop an addressing plan
- Certify hardware & software configurations
- Enable Routing
- Internal infrastructure services (DNS, NTP, DHCP, …)
- Network management infrastructure
- Security
- Operational experience
- Deploy some IPv6-only systems to find the IPv4-dependencies
- Peering
- Develop a plan for encouraging a migration over time
  - Costs for maintaining IPv4 will skyrocket due to space fragmentation
- Enable public facing services

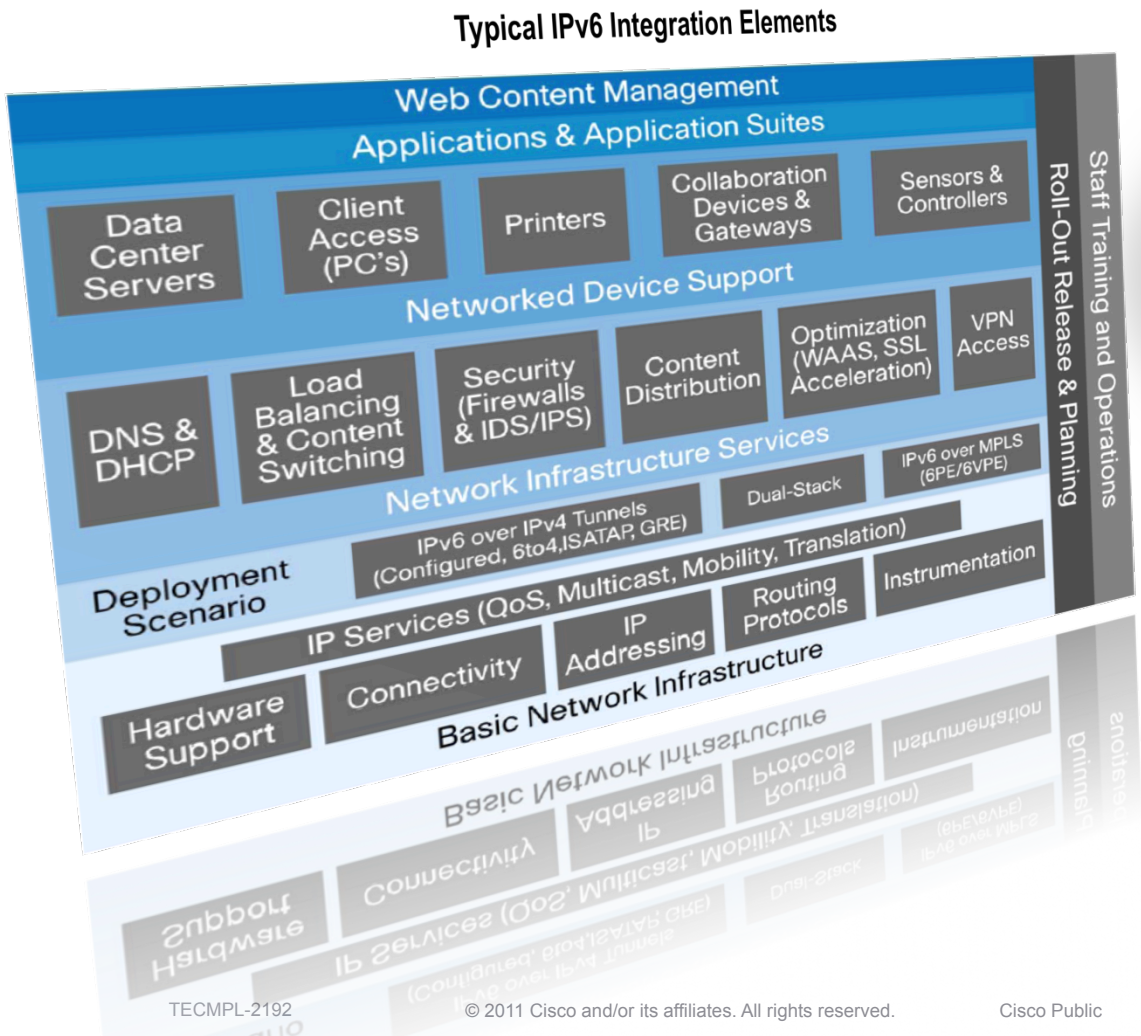
Core Design Factors

Service Mapping	Topology & Attachment	Control Plane	Data Plane	Management Plane



IPv6 integration should be managed from a broad architectural / ‘systems-wide’ perspective…

IPv6 integration is not ‘just a network upgrade’ but complex endeavour, involving many elements and capabilities which evolve over time, rather than changing all at once.



Planning and coordination is required from many across the organisation, including …

- ✓ Network engineers & operators
- ✓ Security engineers
- ✓ Application developers
- ✓ Desktop (Office Automation) / Server engineers
- ✓ Web hosting / content developers
- ✓ Business development managers
- ✓ …

Moreover, **training will be required** for all involved in supporting the various IPv6 based network services

IPv6 in the Data Center
Biggest Challenges Today

- Network services above L3
  - SLB, SSL-Offload, application monitoring (probes)
  - Application Optimization (WAAS)
  - High-speed security inspection/perimeter protection
- Application support for IPv6
  - 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
- Growing DC complexity
  - Virtualization should make large 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

IPv6 Address Considerations

- Develop an addressing plan and corresponding network architecture
- Understand IPv6 addressing at micro level (subnet assignment)
- Take into consideration aggregation/summarization for scalability. Design network prefixes as it were native/dual stack environment
- Establish policies for using the IPv6 prefix and decide which mechanisms to use to assign addresses
  - Dynamic Host Configuration Protocol v6 (DHCPv6)
  - Stateless Auto Configuration (SLAAC)
  - cryptographically generated addresses (CGA).
  - Interface assignment format ?? MAC address based etc ?
  - Some might use multiple mechanisms – for example, manually assigning addresses to critical servers and networking devices and using DHCPv6 to assign addresses to others.
  - Cisco IPv6 Addressing White paper:
    - http://www.cisco.com/web/strategy/docs/gov/IPv6_WP.pdf

IPv6 Routing Protocol Considerations Question to ask yourself

- Are the topologies going to be congruent?
- Separate routing process or the same ?

  EIGRP, OSPF, RIPng Separate Proccess

  ISIS one process today supports Multi-Topology (what is the impact to flooding in your network)
- What are the High Availability requirements
- What are the fast convergence needs i.e application needs, network convergence fast hello's, iSPF, BFD etc Does the protocol support it yet ?
- If both IPv4 and IPv6 timers are tweaked what are the affects on convergence and the Platforms.
- BGP peering consideration

  separate peers, route-maps separate policies,

  Link local peering for EBGP ? Or global,

  Route Reflector design separate RR's,

Understanding co-existence implications

- Resources considerations

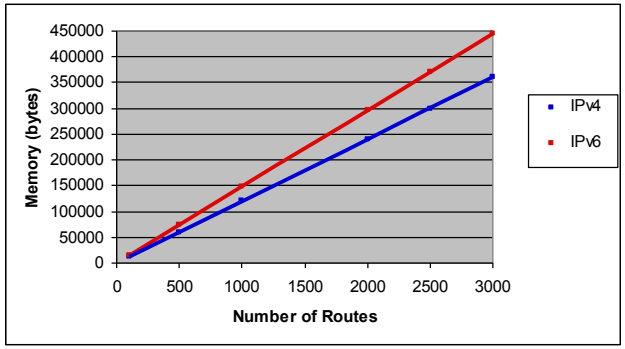
  - Memory (storing the same amount of IPv6 routes requires less memory than might be expected)
  - CPU (insignificant increase in the case of HW platforms, additive in the case of SW platforms)

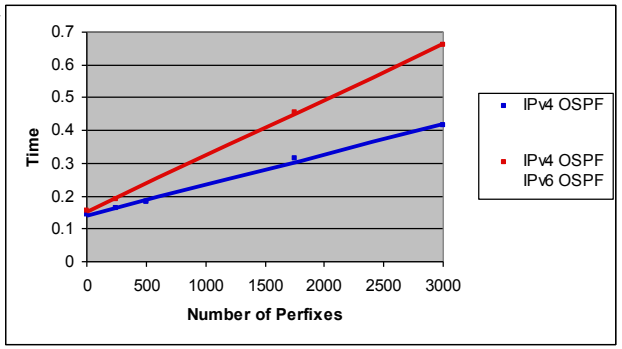
- Control plane considerations

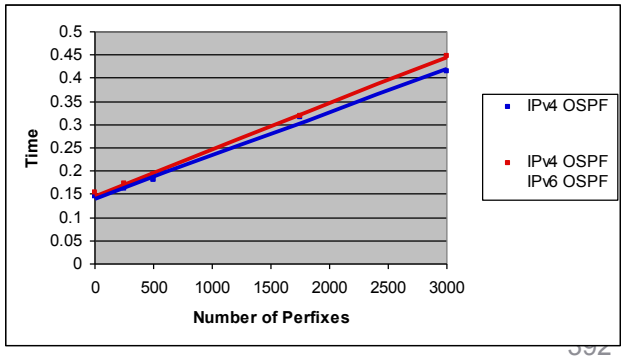
  Balance between IPv4/IPv6 control plane separation and scalability of the number of sessions

- Performance considerations

  - Forwarding in the presence of advanced features
  - Convergence of IPv4 routing protocols when IPv6 is enabled



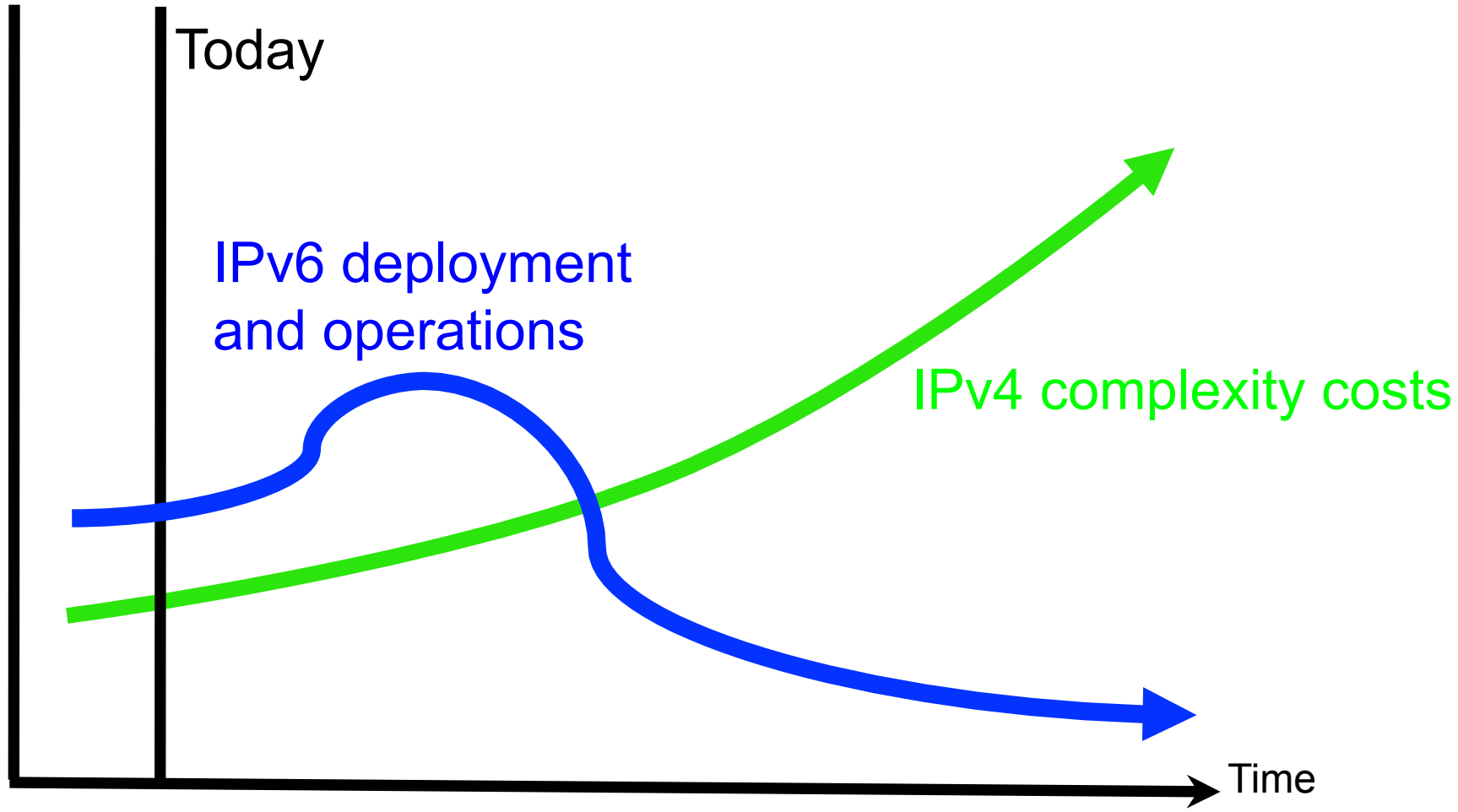




IPv6 Testing Considerations

- Test/identify application software and services
  - •Establish a lab for testing applications and services
  - •Should IPv6 RA's be disabled how do devices re-act to that ?
  - •IPv6 routing protocol design, convergence,
  - •IPv6 QOS and Security features
  - •IPv6 integration/solution techniques and how it fits it in the bigger picture
  - • Test Co-existence IPv4 and IPv6. Based off IPv4 base line i.e take worst case IPv4 scenarios and built IPv6 on top of that.
  - •DHCPv6, DHCPv6-prefix delegation, NMS polling.
  - •How do devices re-act with A and AAAA DNS records
  - •Does application being used implement SAS(Source address algorithm) correctly

IPv6 vs. IPv4 costs over time



Service Provider Connectivity Considerations Question to ask

- **SP Deployment Type**
  - Dual Stack, Native or Overlay (if so what kind of overlay)
  - What kind of SLA are provided for the services
- **What kind of services are offered**
  - Internet Services
  - Layer 2 or Layer 3 VPN's
  - IPv6 Multicast support or plans ?
- **Visibility and footprint to the IPv6 internet.**
  - Understanding Peering arrangements
- **Understand Addressing Policy and acceptance**
  - Prefix length acceptance
  - Provider Independent or Provider Assigned acceptance
- **Provisioning**
  - Is there a self service portal ?
  - Routing add and deletes
- **Charging model do you charge for IPv6 ?**
- **NAT services do you have any ?**
- **Hosting Services ?**

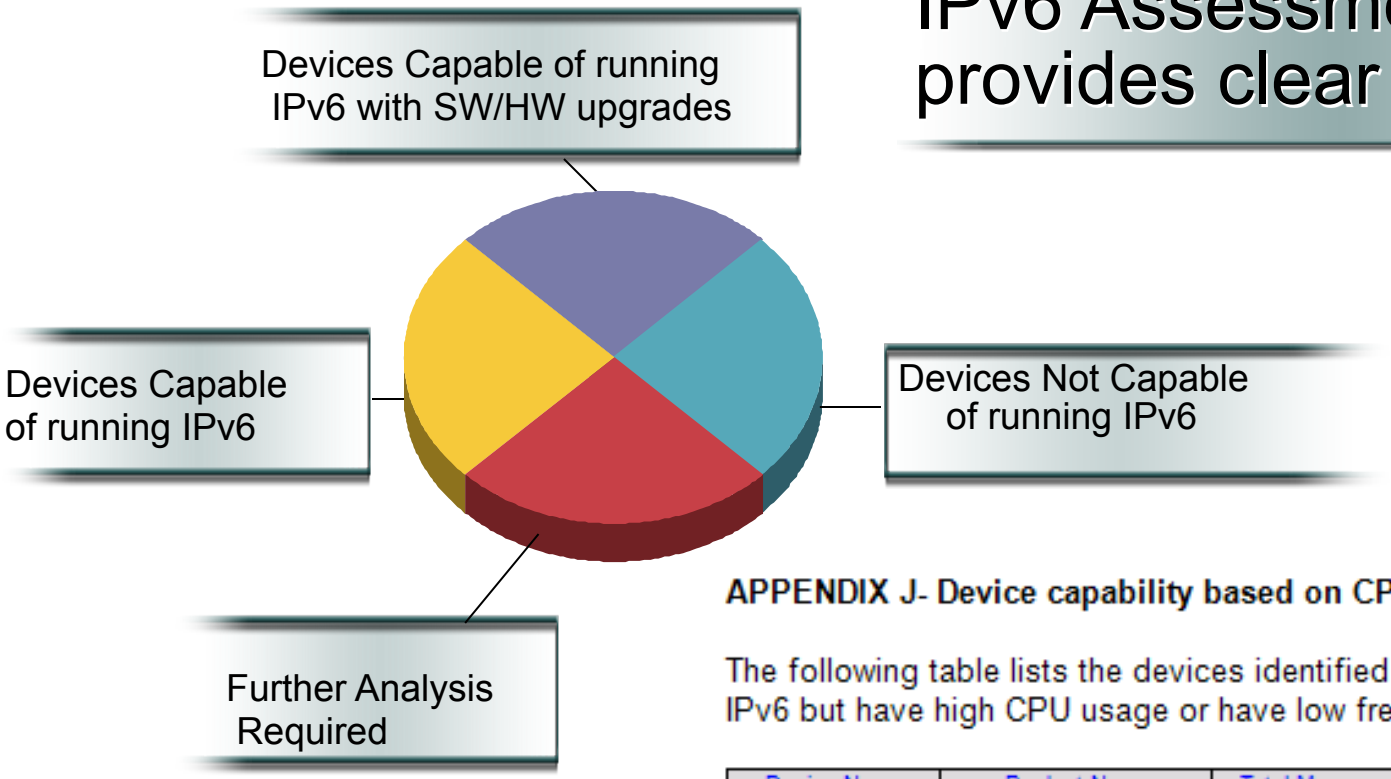
Network and Application Assessment

Network Assessment

- A key and mandatory step to evaluate the impact of IPv6 integration
- May be split in several phases
  - Infrastructure – networking devices
  - Hosts, Servers and applications
- Must be as complete as possible to allow upgrade costs evaluation and planning
  - Hardware type, memory size, interfaces, CPU load,…
  - Software version, features enabled, license type,…
- Difficult to complete if a set of features is not defined per device's category for a specific environment
  - IPv6-capable definition, knowledge of the environment and applications, design goals

Is my network IPv6 ready ?

IPv6 Assessment Tool provides clear answer



APPENDIX J- Device capability based on CPU and Memory

The following table lists the devices identified as capable to support IPv6 but have high CPU usage or have low free memory.

Device Name	Product Name	Total Memory	Free Memory	CPU usage
Device60	CHAS-7507=	264	43	15
Device61	GSR10/200-AC	2048	928	72
Device62	CISCO7609	1024	100	22
Device63	GSR10/200-AC	2048	200	32
Device64	GSR10/200-AC	2048	800	52

IPv6 Network Management and Operations

IPv6 Transition: Network Management Considerations

Introduction of IPv6 creates new network management challenges:

1. Designing the IPv6 deployment
2. Planning the transition process
3. Requirements for institutional knowledge of IPv6
4. Managing network element transitions to IPv6 operation
5. Management and design strategies for IPv6 addressing model, policies and operation
6. Introduction of extended IP services: DHCP, DNS, IPAM
7. Managing security infrastructures: Firewall, IDS, NAC, AAA
8. Tool visibility, insight and analysis of IPv6 traffic Netflow, IPSLA
9. Troubleshooting, IPv4-IPv6 interaction

IPv6 impacts 4 areas of Network Management

1. Instrumentation (MIBs, Netflow, IPSLA,…)
   Updated IP MIBs, RFC 4001 compliancy,…

2. Management protocols running over IPv6 (SNMP, TFTP, Syslog, Telnet, SSH, NTP, Radius/Tacacs, DNS, CDP, ..)

3. Instrumentation running over IPv6 (CNS Agents, Config logger, HTTP, Netconf, SOAP, TCL …)

4. Network Management tools and applications:

   Ciscoworks LMS, Network Analysis Module (NAM), Cisco Network Registar (CNR)

Operations Considerations

Type of Tool	Examples
Traffic Monitoring	Management Information Base (MIB) for IPv6, NetFlow IPv6 records, IPv6 Service Level Agreement (SLA)
Network Services	DHCPv6 Server and Relay, Domain Name Server (DNS), Network Time Protocol (NTP)
Network Management Systems	Network management Applications specific to the IPv6 environment such as an IPv6 topology mapping, IPv6 user's tracking
Other Management Applications	Secure Shell (SSH), Simple Network Management Protocol (SNMP), Syslog
Troubleshooting Documentation	Troubleshooting Guides

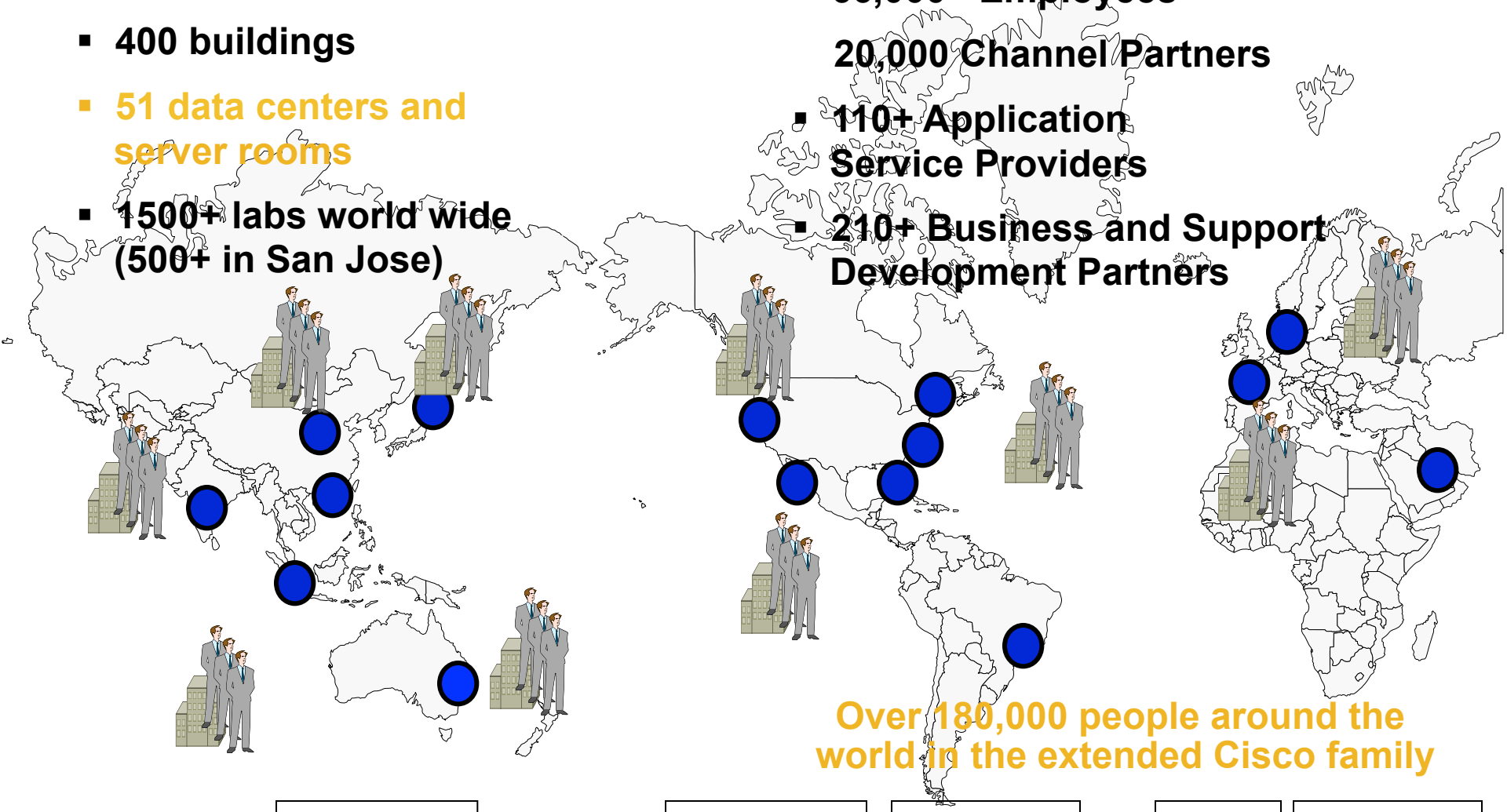
Cisco IT – IPv6 Integration Strategy

Drivers and Goals

- Business Drivers
  1. IPv6 leadership and mindshare
  2. IPv6 product and solution readiness
- IT Drivers
  1. Corporate Growth (Possible IPv4 Address Depletion in the future)
  2. Enable IPv6 Infrastructure for development and testing
  3. Cisco on Cisco
- Goals
  1. cisco.com IPv6 Internet presence
  2. Enable ubiquitous IPv6-enabled user access in the network
  3. End to end IPv6 (Dual Stack)

Information about Cisco

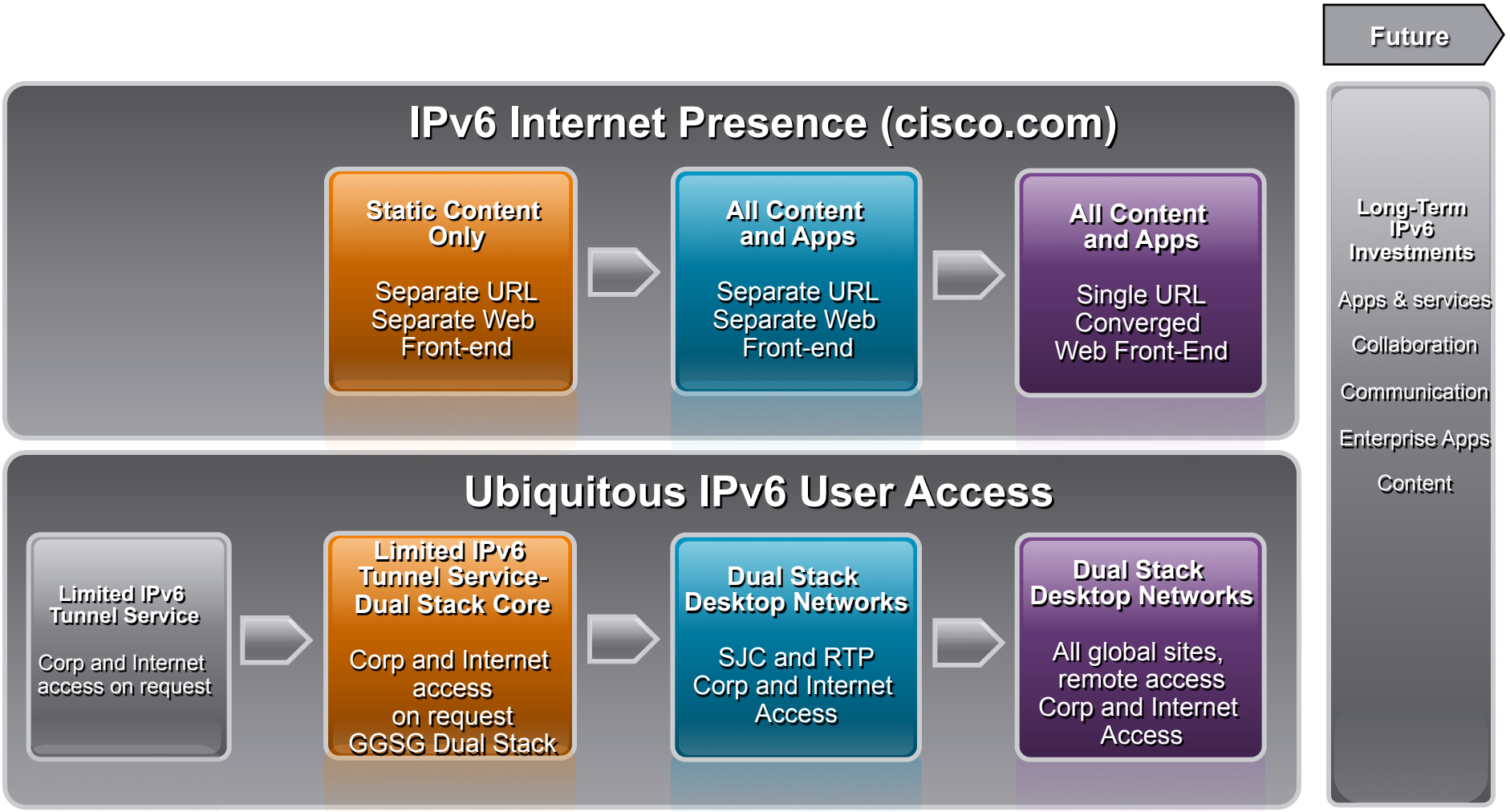
- 300 locations in 90 countries
- 400 buildings
- 51 data centers and server rooms
- 1500+ labs world wide (500+ in San Jose)
- 66,000+ Employees
  20,000 Channel Partners
- 110+ Application Service Providers
- 210+ Business and Support Development Partners



Over 180,000 people around the world in the extended Cisco family

ASIAPAC | N. America | S. America | Europe | Middle East

Cisco IT's IPv6 Strategy

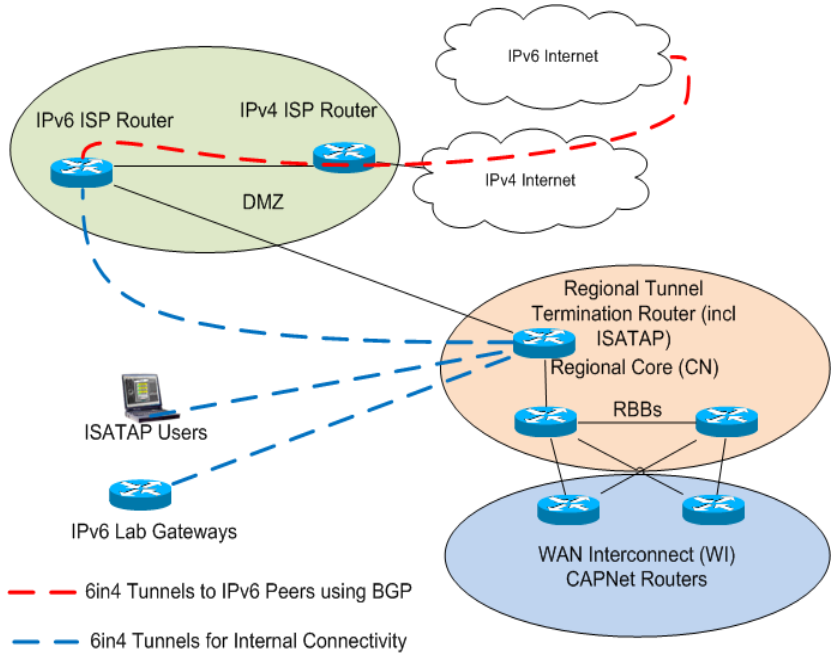


IPv6 Address Planning Highlights

1. Comply with current IP addressing policy
2. Mirror current IPv4 Regional Allocations
3. Proportional to usage and expected growth
4. Hierarchical Model (Global, Region, Sub-Region and Site)
5. Template addressing at Sub-Regional, Site and PIN (Places in the Network) Levels
6. Holding adequate spares at EACH level of the hierarchy
7. Global Infrastructure and Mobility Allocations

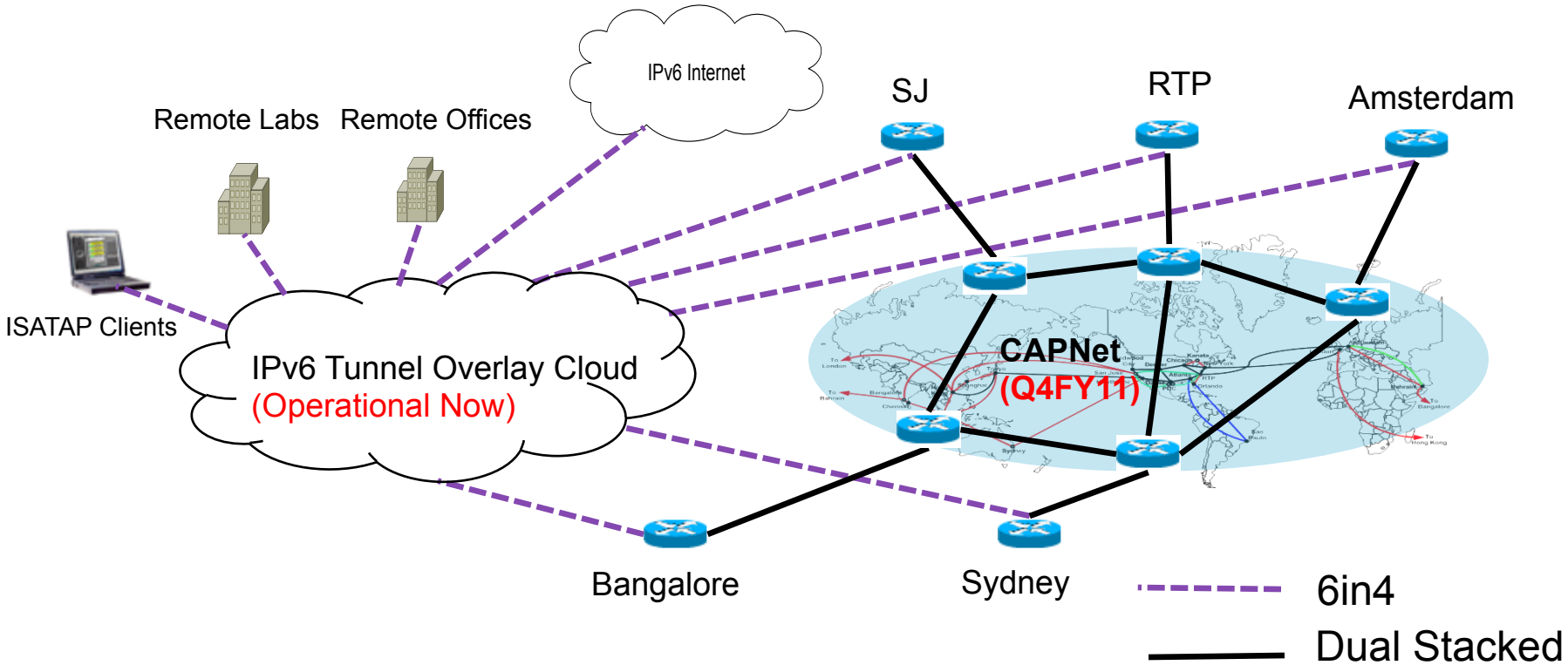
Cisco IT IPv6 Tunnelling Infrastructure – Pilot Phase

- Tunnelled Internet connectivity to IPv6 Internet only through SJ
- No regional Tunnel Head Ends
- High latency between intra-regional labs / users due to back hauling
- Single point of failure
- No IPv6 DMZ to host content on IPv6 internet



IPv6 Deployment (DS Core – Initial Phase)

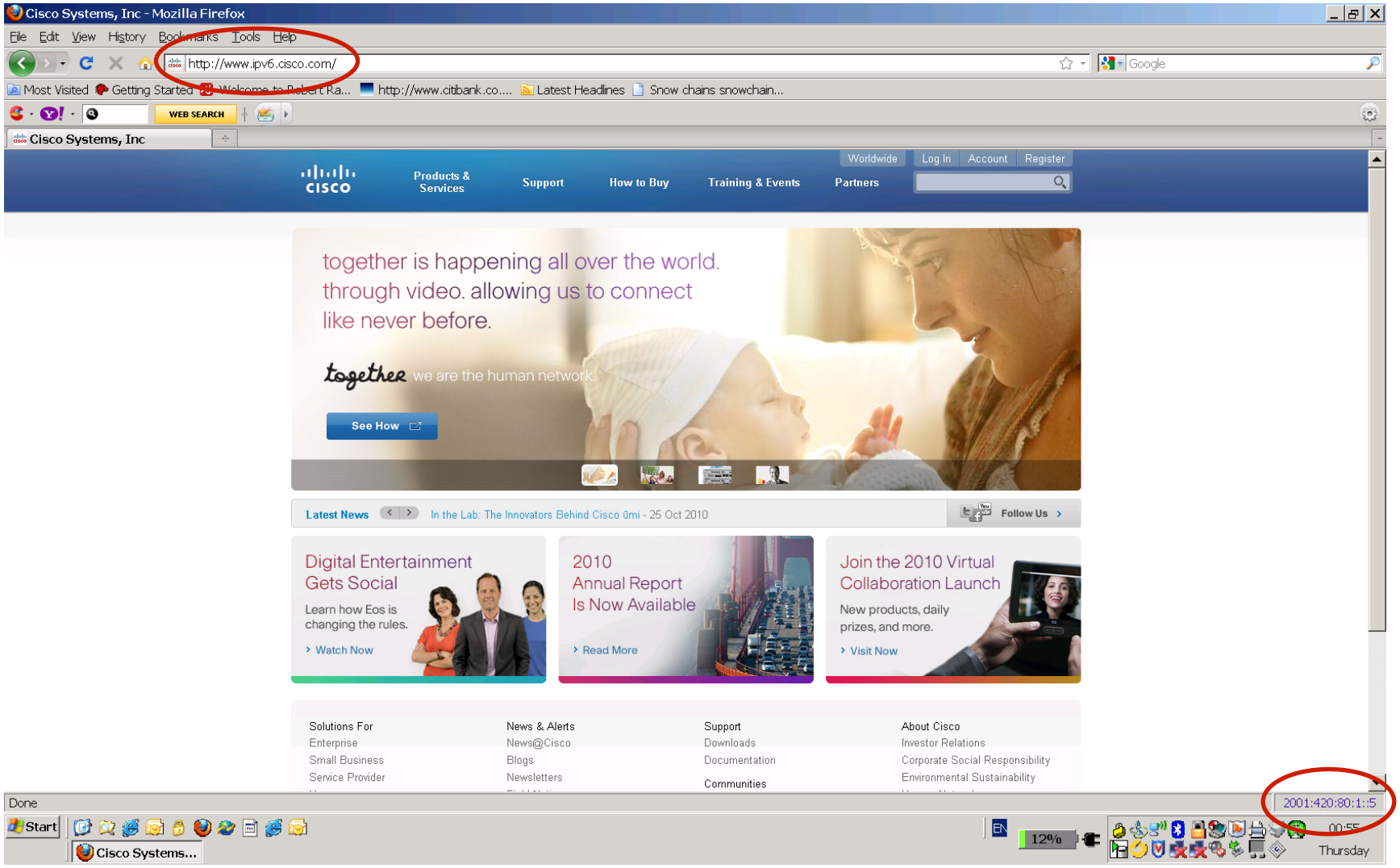
- Five Regional Tunnel Head Ends offering 6in4 and Anycast based ISATAP
- 6in4 Tunnels will gradually be migrated to dual stacked links extending from the core outwards
- Tunnel Overlay will remain to aid rapid enablement of remote sites and ease migration to IPv6 while infrastructure catches up



Cisco.com Phase I Solution Overview

- Replication
  - Replicate “static content” to v6 environment
  - Directories with secure content in them will not be replicated
  - 200G of content is replicated to IPv6 environment
- Content Delivery
  - AAAA record for www.ipv6.cisco.com served from DNS
  - “Static Content” served locally
  - Dynamic Content redirected to WWW

www.ipv6.cisco.com – 2001:420:80:1::5



Phased IPv6 Approach

A Phased, Iterative Approach to Successful IPv6 Adoption

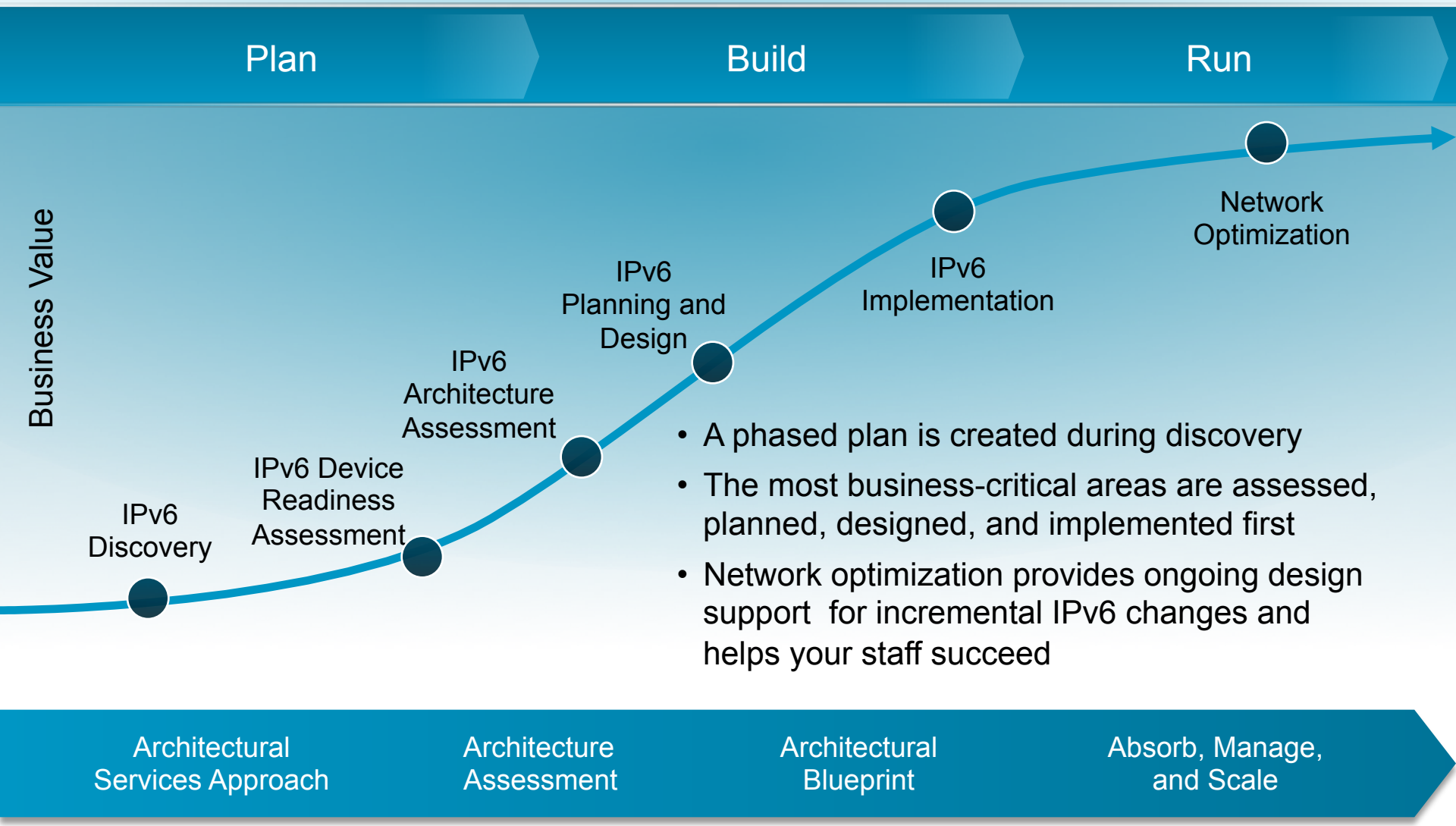
Start with a Phased Plan Aligned with Your Business Strategy

1. Identify the highest priority IPv6-critical areas in your network
2. Perform IPv6 Assessment on highest-priority areas to determine scope of design
3. Develop an IPv6 design that enables IPv6 to be introduced without disrupting your IPv4 network
4. Begin IPv6 testing and implementation in pilot mode, then extend over time into production deployment

Repeat for the Next IPv6-Critical Area in Your Network

An Iterative Approach to IPv6 Adoption

Addressing Critical Areas in Priority Order



- A phased plan is created during discovery
- The most business-critical areas are assessed, planned, designed, and implemented first
- Network optimization provides ongoing design support for incremental IPv6 changes and helps your staff succeed

Architectural Services Approach | Architecture Assessment | Architectural Blueprint | Absorb, Manage, and Scale

Summary

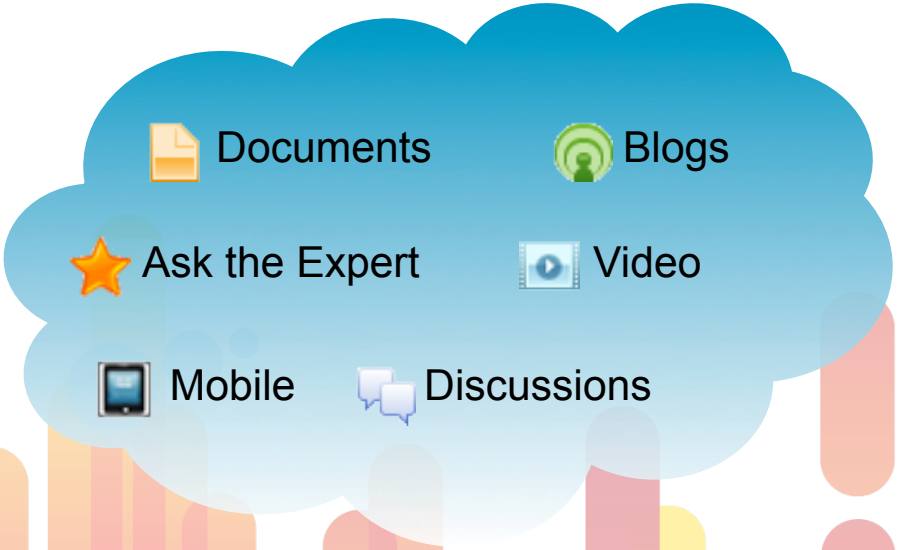
- IPv4 exhaust is about business continuity
- IPv6 has some winning economic, technical and service arguments
- IPv6 architecture choices will define business opportunities for many years
- Expect innovation in applications as characteristics of IPv6 are understood
- Create a plan and Strategy with time lines
- Put IPv6 into your procurement process for tech refresh cycles
- Understand Network Readiness today
- Don’t get left behind

IPv6 Enterprise Techtorial
Conclusion

Join Cisco Support Communities!

- **Free** for anyone with Cisco.com registration
- Get **timely** answers to your technical questions
- Find **relevant** technical documentation
- Engage with over 200,000 **top technical experts**
- **Seamless** transition from discussion to TAC Service Request *(Cisco customers and partners only)*
- Visit the Cisco Support Community booth in the World of Solutions for more information

IPv6 Support Community
Coming Soon!



supportforums.cisco.com
supportforums.cisco.mobi

The Cisco Support Community is your one-stop community destination from Cisco for sharing current, real-world technical support knowledge with peers and experts.

Reference Materials

- New/Updated IPv6 Cisco Sites

  http://www.cisco.com/ipv6

  http://www.cisco.com/go/ipv6

  http://www.cisco.gom/go/entipv6

- IPv6 Addressing Guide

  http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Smart_Business_Architecture/BN_Enterprise_IPv6_Addressing_Guide_H2CY10.pdf

- Cisco Smart Business Architecture (SBA Enterprise):

  http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns982/landing_sBus_archit.html

- Deploying IPv6 in Campus Networks:

  http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/CampIPv6.html

- Deploying IPv6 in Branch Networks:

  http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns816/landing_br_ipv6.html

Reference Materials

- SRND: Deploying IPv6 in Unified Communications Networks

  http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/ipv6/ipv6srnd.html

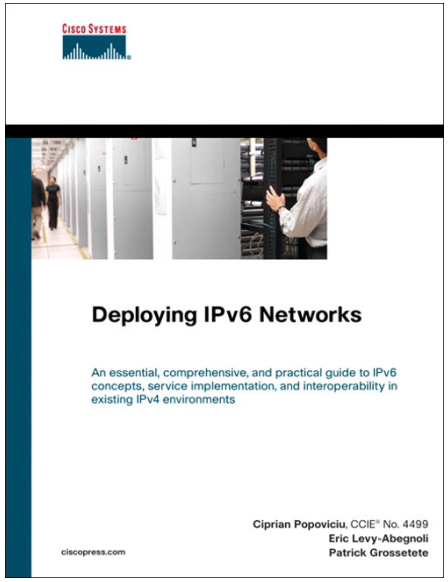
- IOS IPv6 VOIP implementation Guide

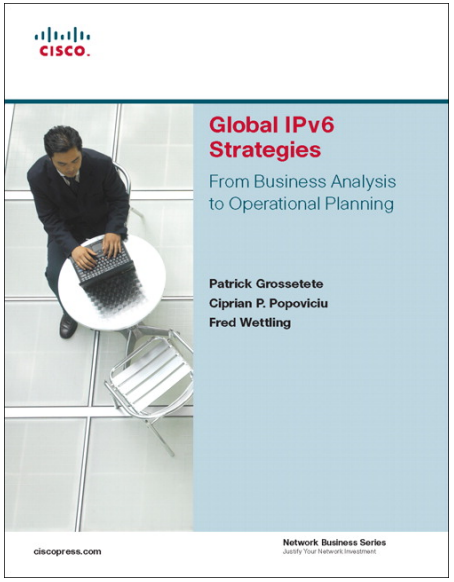
  http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6_voip.pdf

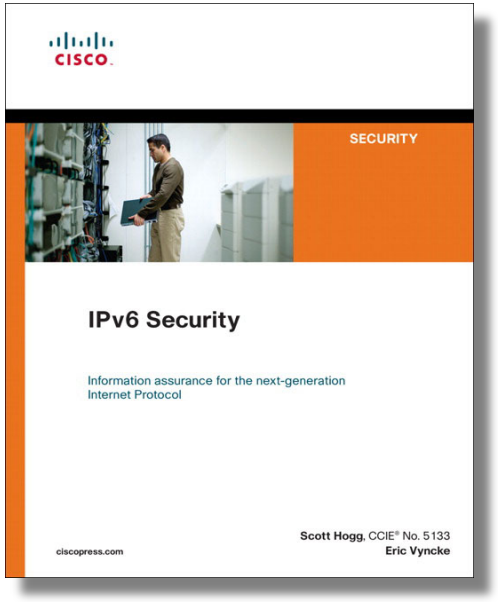
- DNS and BIND, 5th Edition, by Cricket Liu and Paul Albitz, O'Reilly Media, May 2006

- RFC 3596: DNS Extensions to Support IP Version 6, by S. Thomson, C. Huitema, V. Ksinant, and M. Souissi, October 2003 (format: TXT=14093 bytes)(obsoletes RFC 3152 and RFC 1886) (status: Draft Standard)

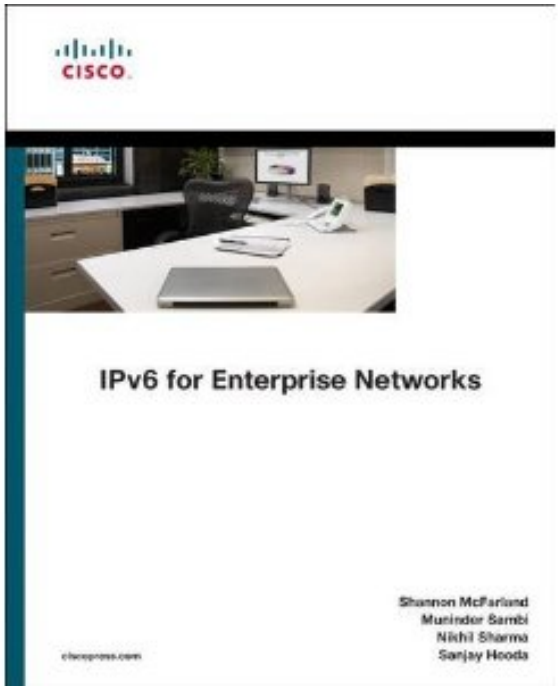
Recommended Reading







Recommended Reading



Coming Soon!!

Deploying IPv6 in Broadband Networks
Adeel Ahmed, Salman Asadullah
ISBN0470193387,
John Wiley & Sons Publications®