IPv6 for Dummies

Janne Östling

janoz@cisco.com

Agenda

- General Concepts
  - Addressing
  - Routing
  - QoS
  - Tunnels
  - NAT
- Infrastructure Deployment

  Campus/Data Center

  WAN/Branch

  Remote Access
- Planning and Deployment Summary
- Appendix & Hidden slides — for Reference Only!

  (240 slides total so far…)

Preamble

A Need for IPv6?

- IETF IPv6 WG began in early 90s, to solve addressing growth issues, but

  CIDR, NAT,…were developed

- IPv4 32 bit address = 4 billion hosts

  ~40% of the IPv4 address space is still unused which is different from unallocated

  The rising of Internet connected device and appliance will eventually deplete the IPv4 address space

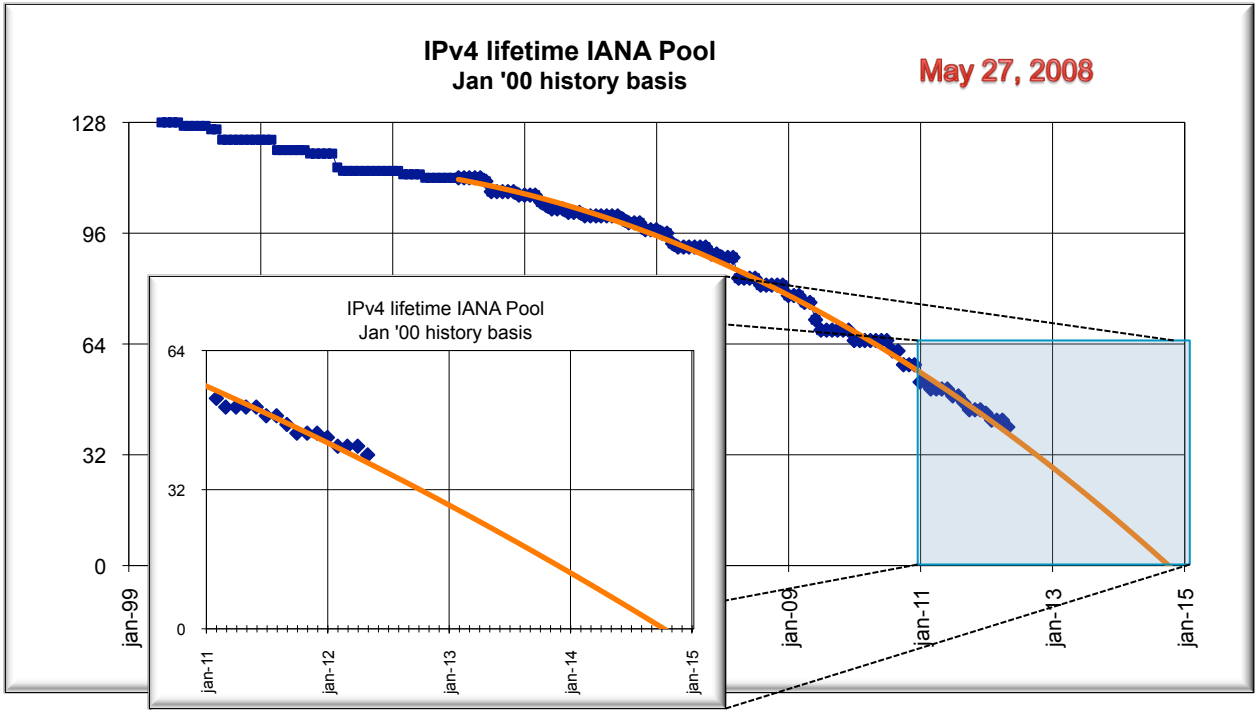
- IP is everywhere

  Data, voice, audio and video integration is a reality

  Regional registries apply a strict allocation control

- So, only compelling reason: More IP addresses

Reflection - Denial



Update to: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_8-3/ipj_8-3.pdf Tony Hain

Whatever happens, today's IPv4 Internet will continue to run – It just stops growing (OECD report http://www.oecd.org/dataoecd/7/1/40605942.pdf)

Day 2011-12-24 Last RIR depleted

Make your own IPv4 exhaustion estimate.

Developed by Stephan Lagerholm

http://www.lagerholm.com/~stephan/cgi-bin/ipv6/predict.cgi

http://www.infoweapons.com/pdfs/When_Will_IPv4_Addresses_Run_Out_ver00_rev06.pdf

Monitoring Market Drivers

Address space depletion

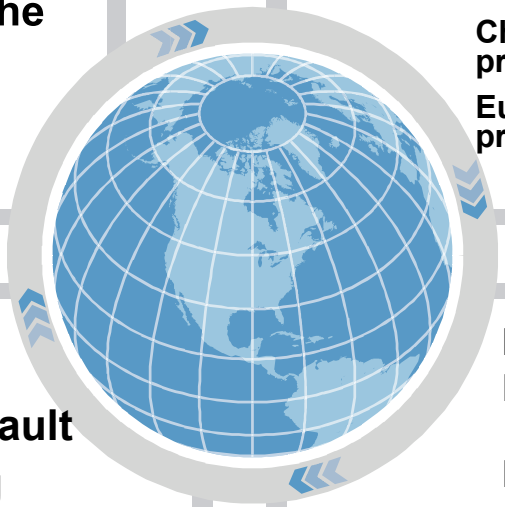
http://www.potaroo.net/tools/ipv4/

Impact being a slow down of the Internet growth and market penetration

National IT Strategy

U.S. Federal Mandate

- IPv6 Task Force and promotion councils: Africa, India, Japan, Korea,…
- China Next Generation Internet (CNGI) project
- European Commission sponsored projects



MSFT Vista & Server 2008

IPv6 "on" & "preferred" by default

Applications only running over IPv6 (P2P framework)

Infrastructure Evolution

- IP NGN
- DOCSIS 3.0, FTTH, HDTV, Quad Play
- Mobile SP – 3G, WiMax, PWLAN
- Networks in Motion
- Networked Sensors, ie: AIRS
- NAT Overlap – M&A

Why Not NAT

- It was created as a temp solution
- NAT breaks the end-to-end model
- Growth of NAT has slowed down growth of transparent applications
- No easy way to maintain states of NAT in case of node failures
- NAT break security
- NAT complicates mergers, double NATing is needed for devices to communicate with each other

Operating System Support

- Every major OS supports IPv6 today
- Top-to-bottom TCP/IP stack re-design
- IPv6 is on by default and preferred over IPv4 (considering network/DNS/application support)
- Tunnels will be used before IPv4 if required by IPv6-enabled application

  ISATAP, Teredo, 6to4, Configured
- All applications and services that ship with Vista/Server 2008 support IPv4 and IPv6 (IPv6-only is supported)

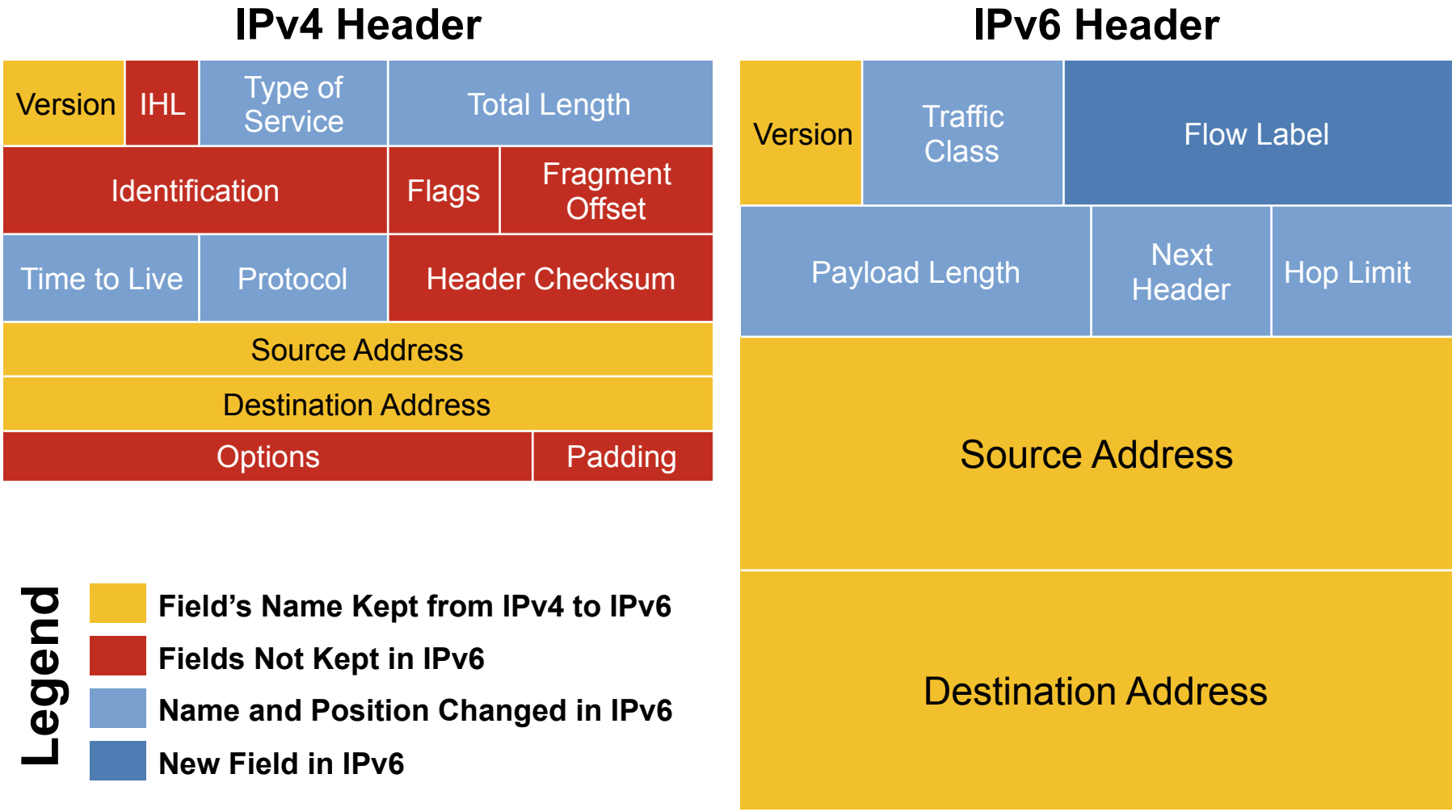
  Active Directory, IIS, File/Print/Fax, WINS/DNS/DHCP/LDAP, Windows Media Services, Terminal Services, Network Access Services – Remote Access (VPN/Dial-up), Network Access Protection (NAP), Windows Deployment Service, Certificate Services, SharePoint services, Network Load-Balancing, Internet Authentication Server, Server Clustering, etc…
- http://www.microsoft.com/technet/network/ipv6/default.mspx

Header

(General Concepts)

IPv6 Addressing

IPv4 and IPv6 Header Comparison

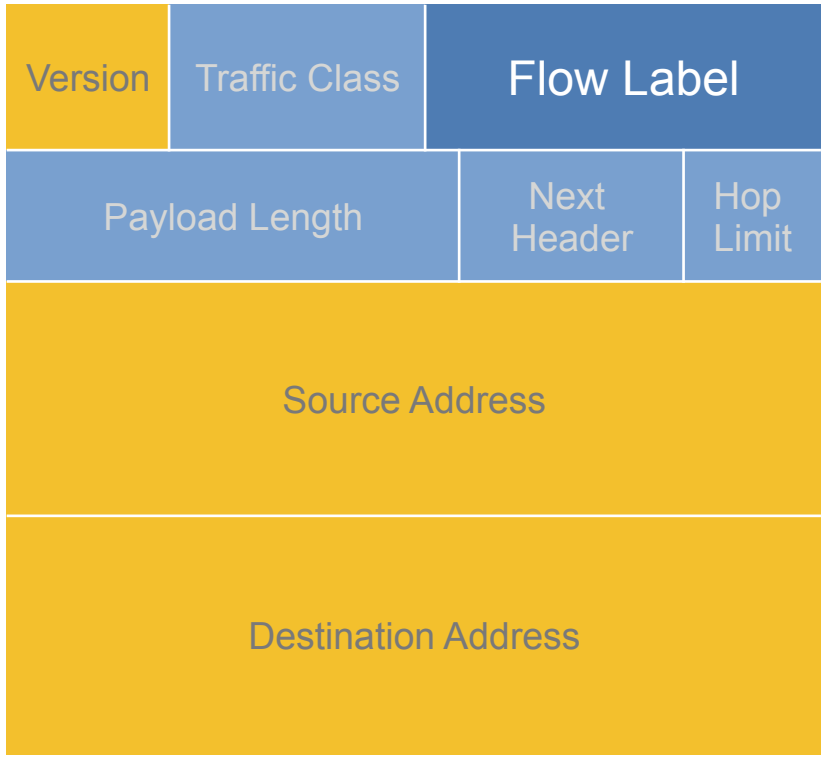


IPv6 Header New Field—Flow Label (RFC3697)

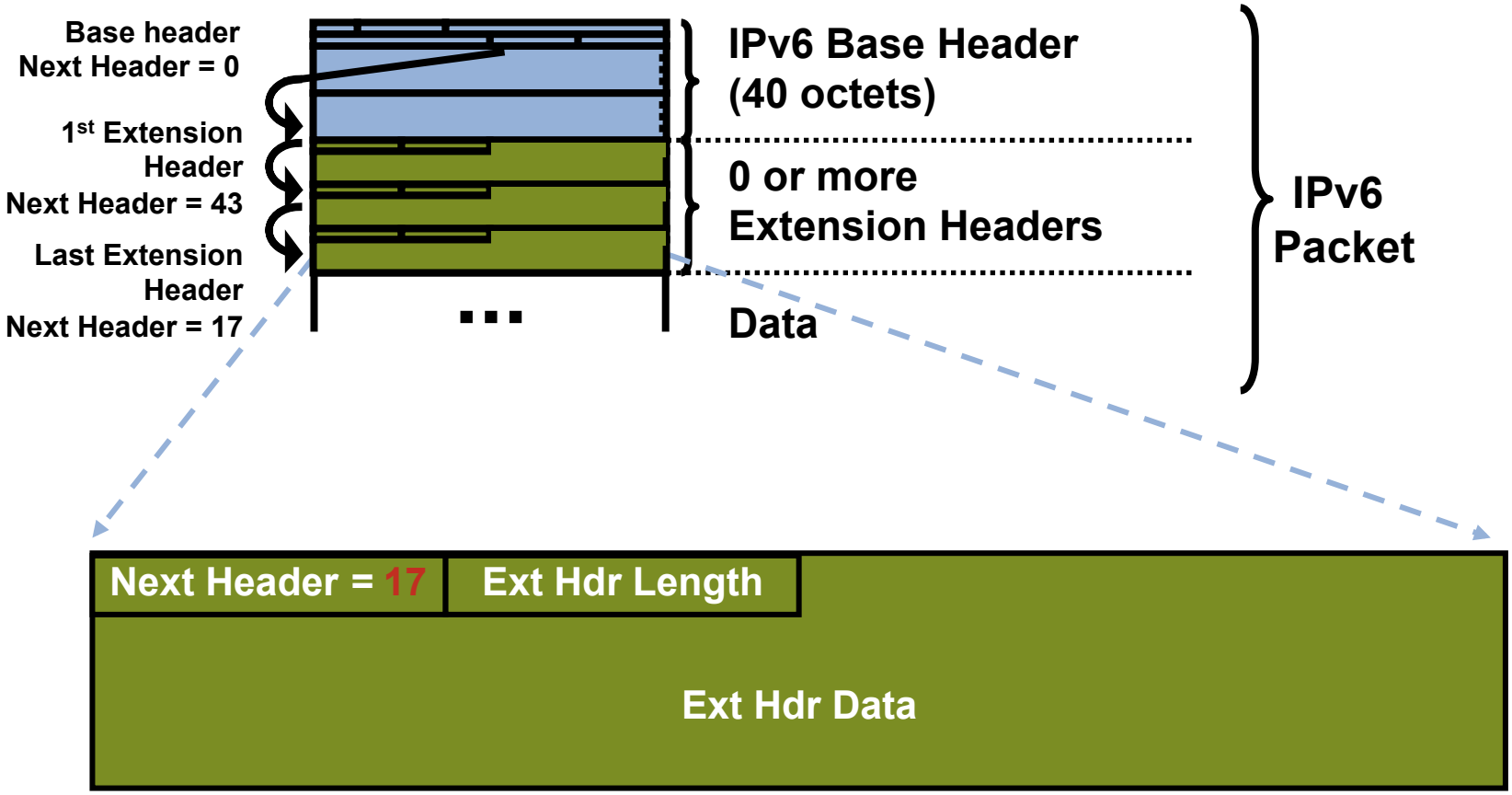
20-Bit Flow Label Field to Identify Specific Flows Needing Special QoS

- Flow classifiers had been based on 5-tuple: Source/destination address, protocol type and port numbers of transport
- Some of these fields may be unavailable due to fragmentation, encryption or locating them past extension headers
- With flow label, each source chooses its own flow label values; routers use source addr + flow label to identify distinct flows
- Flow label value of 0 used when no special QoS requested (the common case today)

IPv6 Header



Extension Headers



Extension Header Order

Extension Headers Should Be Constructed in the Following Sequence and Should Be Sequenced in this Order:

Hop-by-Hop header	(0)
Destination options header (w/ routing header)	(60)
Routing header	(43)
Fragment header	(44)
Authentication header	(51)
ESP header	(50)
Mobility header	(135)
Destination options header	(60)
ICMPv6	(58)
No Next header	(59)
Upper-layer header	(Varies—TCP=6, UDP=17)

MTU Issues

- Minimum link MTU for IPv6 is 1280 octets (vs. 68 octets for IPv4)

  => on links with MTU < 1280, link-specific fragmentation and reassembly must be used

- Implementations are expected to perform path MTU discovery to send packets bigger than 1280
- Minimal implementation can omit PMTU discovery as long as all packets kept ≤ 1280 octets
- A hop-by-hop option supports transmission of “jumbograms” with up to 232 octets of payload; payload is normally 216

Addressing Format

Representation

- 16-bit hexadecimal numbers
- Numbers are separated by (:)
- Hex numbers are not case sensitive
- Abbreviations are possible

  Leading zeros in contiguous block could be represented by (::)

  Example:

  2001:0db8:0000:130F:0000:0000:087C:140B

  2001:0db8:0:130F::87C:140B

  Double colon only appears once in the address

Addressing

Prefix Representation

- Representation of prefix is just like CIDR
- In this representation you attach the prefix length
- Like v4 address:

  198.10.0.0/16

- V6 address is represented the same way:

  2001:db8:12::/48

- Only leading zeros are omitted. Trailing zeros are not omitted

  2001:0db8:0012::/48 = 2001:db8:12::/48

  2001:db8:**1200**::/48 ≠ 2001:db8:12::/48

IPv6 Address Representation

- Loopback address representation

  0:0:0:0:0:0:0:1=> ::1

  Same as 127.0.0.1 in IPv4

  Identifies self

- Unspecified address representation

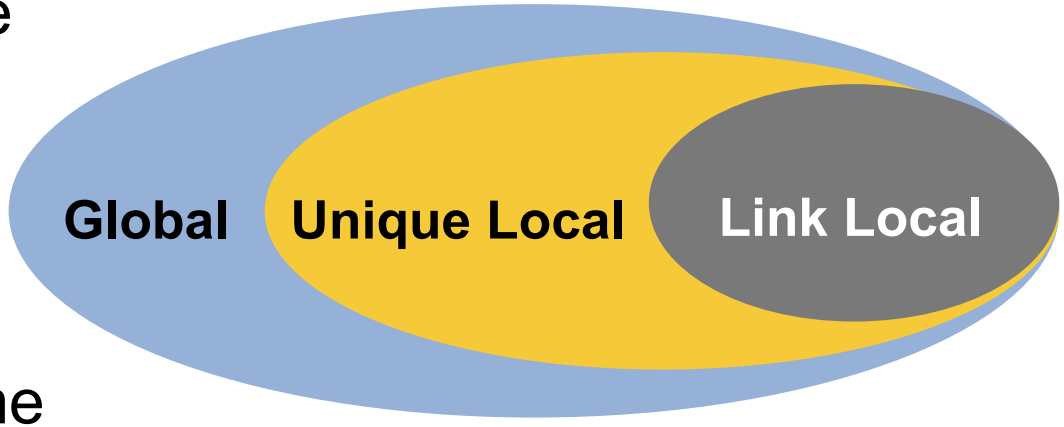
  0:0:0:0:0:0:0:0=> ::

  Used as a placeholder when no address available

  (Initial DHCP request, Duplicate Address Detection DAD)

IPv6—Addressing Model

- Addresses are assigned to interfaces
  - Change from IPv4 mode:
- 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

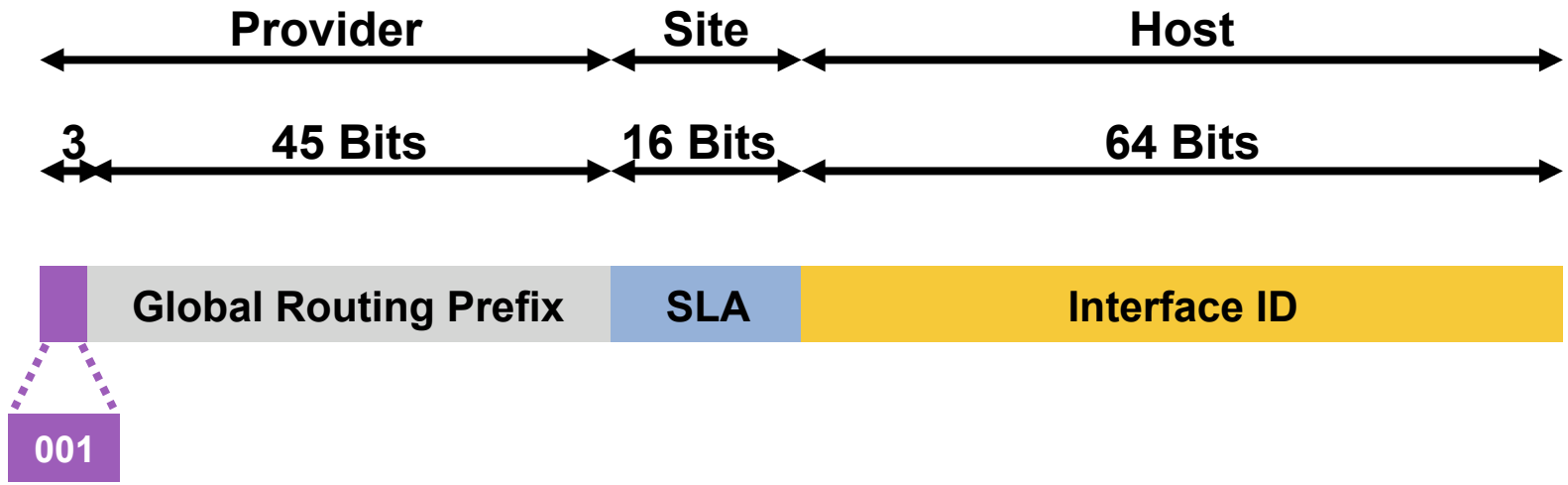
- No more broadcast addresses

Addressing

Some Special Addresses

Type	Binary	Hex
Aggregatable Global Unicast Address	001	2xxx or 3xxx
Link Local Unicast Address	1111 1110 10	FE80::/10
Unique Local Unicast Address	1111 1100 1111 1101	FC00::/7 FC00::/8(registry) FD00::/8 (no registry)
Multicast Address	1111 1111	FF00::/8

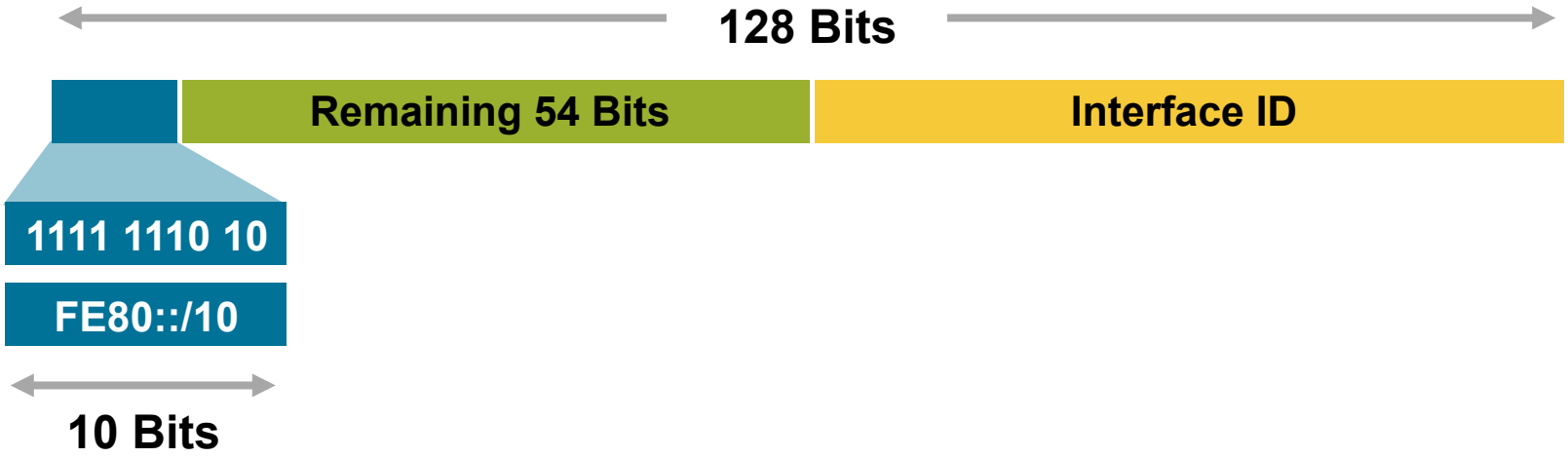
Aggregatable Global Unicast Addresses



Aggregatable Global Unicast Addresses Are:

- Addresses for generic use of IPv6
- Structured as a hierarchy to keep the aggregation

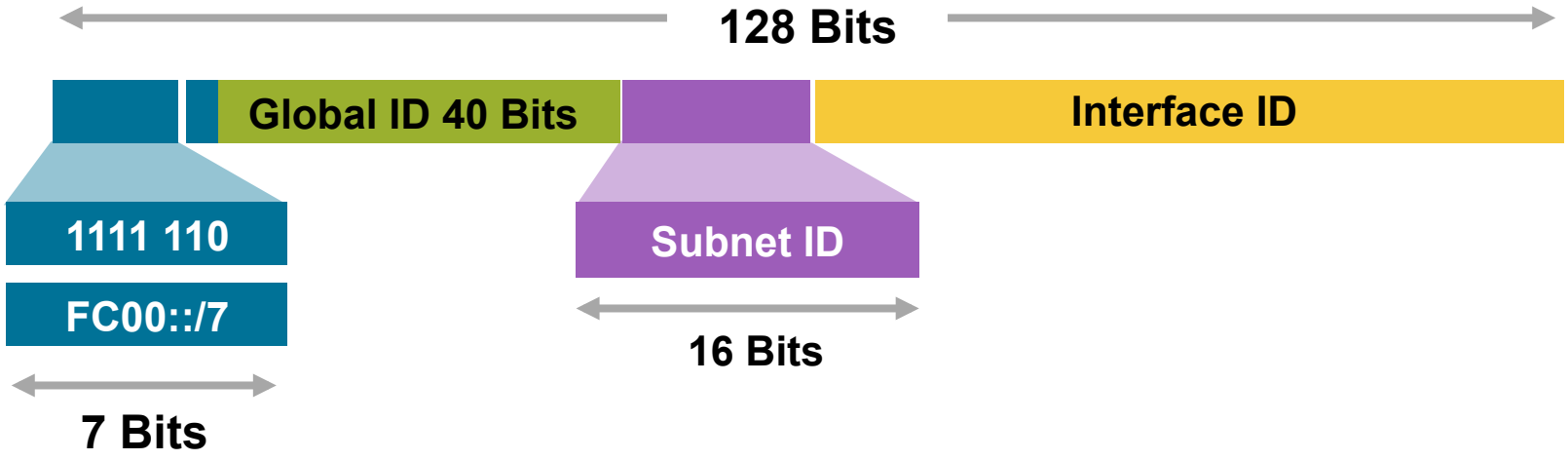
Link-Local



Link-Local Addresses Used for:

- Mandatory Address for Communication between two IPv6 device (like ARP but at Layer 3)
- Automatically assigned by Router as soon as IPv6 is enabled
- Also used for Next-Hop calculation in Routing Protocols
- Only Link Specific scope
- Remaining 54 bits could be Zero or any manual configured value

Unique-Local



Unique-Local Addresses Used for:

- Local communications
- Inter-site VPNs
- Not routable on the Internet

IPv6 Multicast Address

- IP multicast address has a prefix FF00::/8 (1111 1111); the second octet defines the lifetime and scope of the multicast address

8-bit	4-bit	4-bit	112-bit
1111 1111	Lifetime	Scope	Group-ID

Lifetime	
0	If Permanent
1	If Temporary

Scope	
1	Node
2	Link
5	Site
8	Organization
E	Global

Some Well Known Multicast Addresses

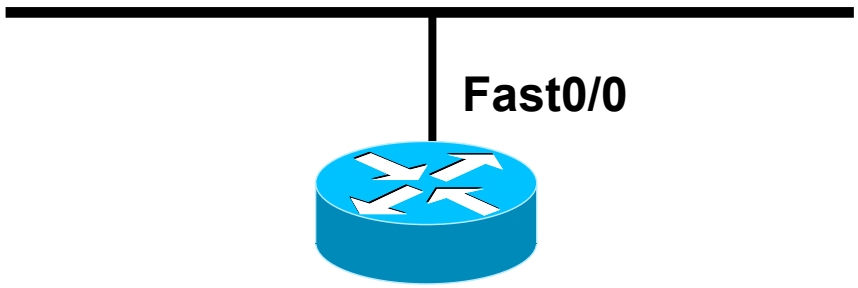
Address	Scope	Meaning
FF01::1	Node-Local	All Nodes
FF02::1	Link-Local	All Nodes
FF01::2	Node-Local	All Routers
FF02::2	Link-Local	All Routers
FF05::2	Site-Local	All Routers
FF02::1:FFXX:XXXX	Link-Local	Solicited-Node

- Note that 02 means that this is a permanent address and has link scope
- More details at http://www.iana.org/assignments/ipv6-multicast-addresses

IPv6 Configurations

IOS IPv6 Addressing Examples (1)

Manual Interface Identifier




```
ipv6 unicast-routing
!
interface FastEthernet0/0
 ip address 10.151.1.1 255.255.255.0
 ip pim sparse-mode
 duplex auto
 speed auto
 ipv6 address 2006:1::1/64
 ipv6 enable
 ipv6 nd ra-interval 30
 ipv6 nd prefix 2006:1::/64 300 300
!
```

IOS IPv6 Addressing Examples (1)

Manual Interface Identifier

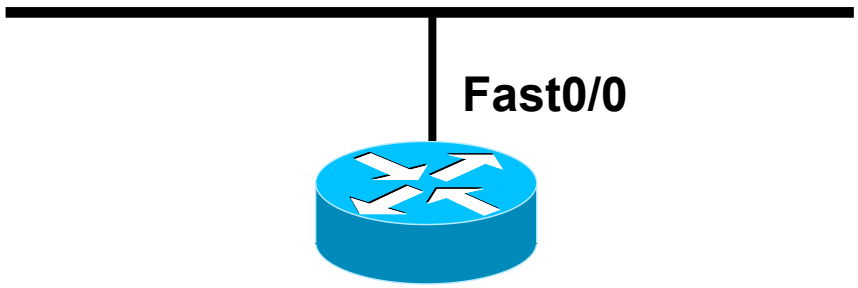
```
r1#sh ipv6 int fast0/0
FastEthernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::207:50FF:FE5E:9460
  Global unicast address(es):
    2006:1::1, subnet is 2006:1::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
    FF02::1:FF5E:9460
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND
  ND
  ND
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 30 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
r1#
```

MAC Address : 0007.505e.9460

```
r1#sh int fast0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is AmdFE, address is 0007.505e.9460 (bia 0007.505e.9460)
```

IOS IPv6 Addressing Examples (2)

EUI-64 Interface Identifier




```
ipv6 unicast-routing
!
interface FastEthernet0/0
 ip address 10.151.1.1 255.255.255.0
 ip pim sparse-mode
 duplex auto
 speed auto
 ipv6 address 2006:1::/64 eui-64
 ipv6 enable
 ipv6 nd ra-interval 30
 ipv6 nd prefix 2006:1::/64 300 300
!
```

IOS IPv6 Addressing Examples (2)

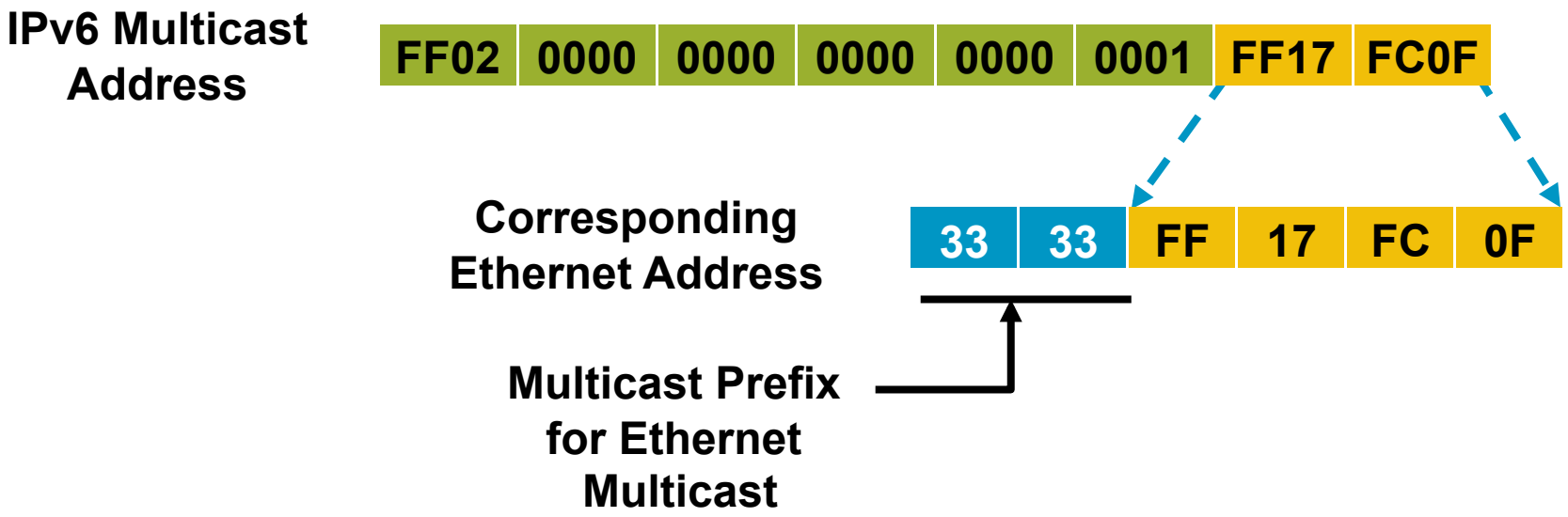
EUI-64 Interface Identifier

```
r1#sh ipv6 int fast0/0
FastEthernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::207:50FF:FE5E:9460
  Global unicast address(es):
    2006:1::207:50FF:FE5E:9460, subnet is 2006:1::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF5E:9460
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  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 30 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
r1#
```

MAC Address : 0007.505e.9460

```
r1#sh int fast0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is AmdFE, address is 0007.505e.9460 (bia 0007.505e.9460)
```

Multicast Mapping over Ethernet

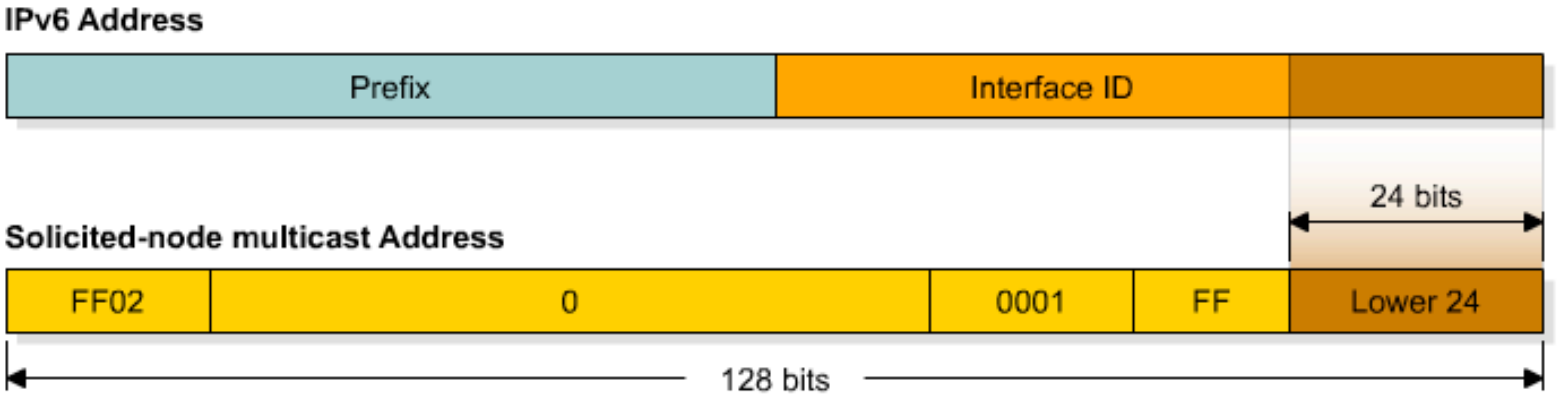


Mapping of IPv6 multicast address to Ethernet address is:

33:33:<last 32 bits of the IPv6 multicast address>

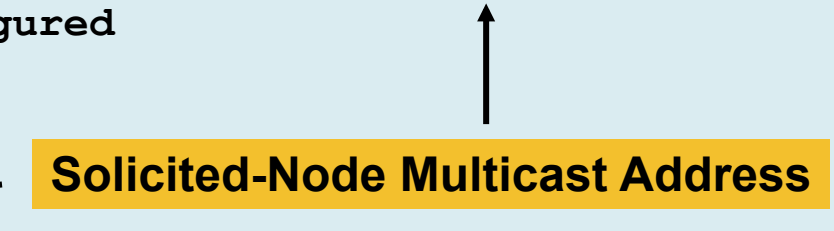
Solicited-Node Multicast Address

- For each unicast and anycast address configured there is a corresponding solicited-node multicast
- This is specially used for two purpose, for the replacement of ARP, and DAD
- Used in neighbor solicitation messages
- Multicast address with a link-local scope
- Solicited-node multicast consists of prefix + lower 24 bits from unicast, FF02::1:FF:



Router Interface

```
R1#sh ipv6 int e0
Ethernet0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::200:CFF:FE3A:8B18
  No global unicast address is configured
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF3A:8B18
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  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
  Hosts use stateless autoconfig for addresses.
R1#
```



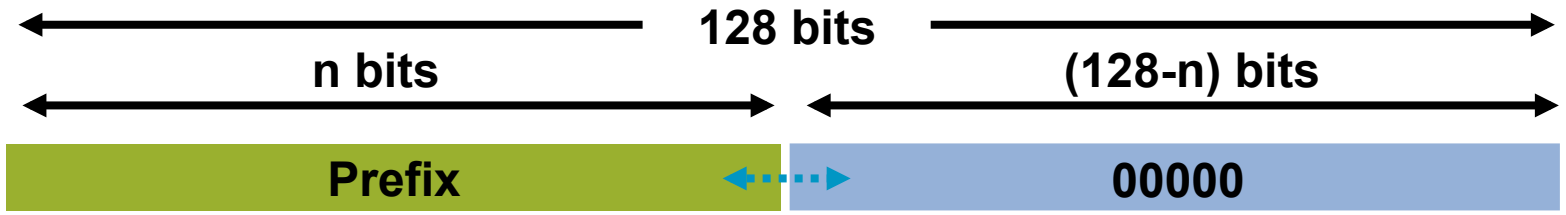
Anycast

Anycast Address Assignment

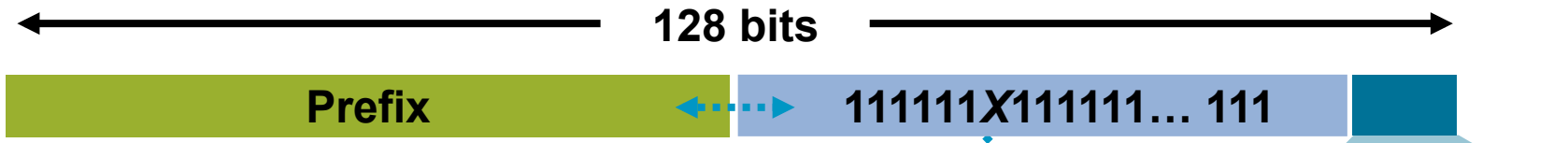
- Anycast allows a source node to transmit IP datagrams to a single destination node out of a group destination nodes with same subnet id based on the routing metrics
- Only routers should respond to anycast addresses
- Routers along the path to the destination just process the packets based on network prefix
- Routers configured to respond to anycast packets will do so when they receive a packet send to the anycast address

Anycast Address

Subnet Router Anycast Address (RFC 4291)

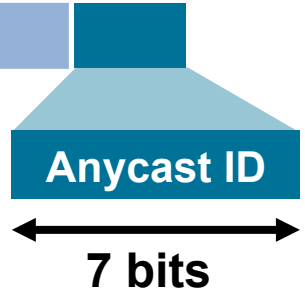


Reserved Subnet Anycast Address (RFC 2526)



- Syntactical the same as a Unicast address
- Is one-to-nearest type of address
- Has a current limited use

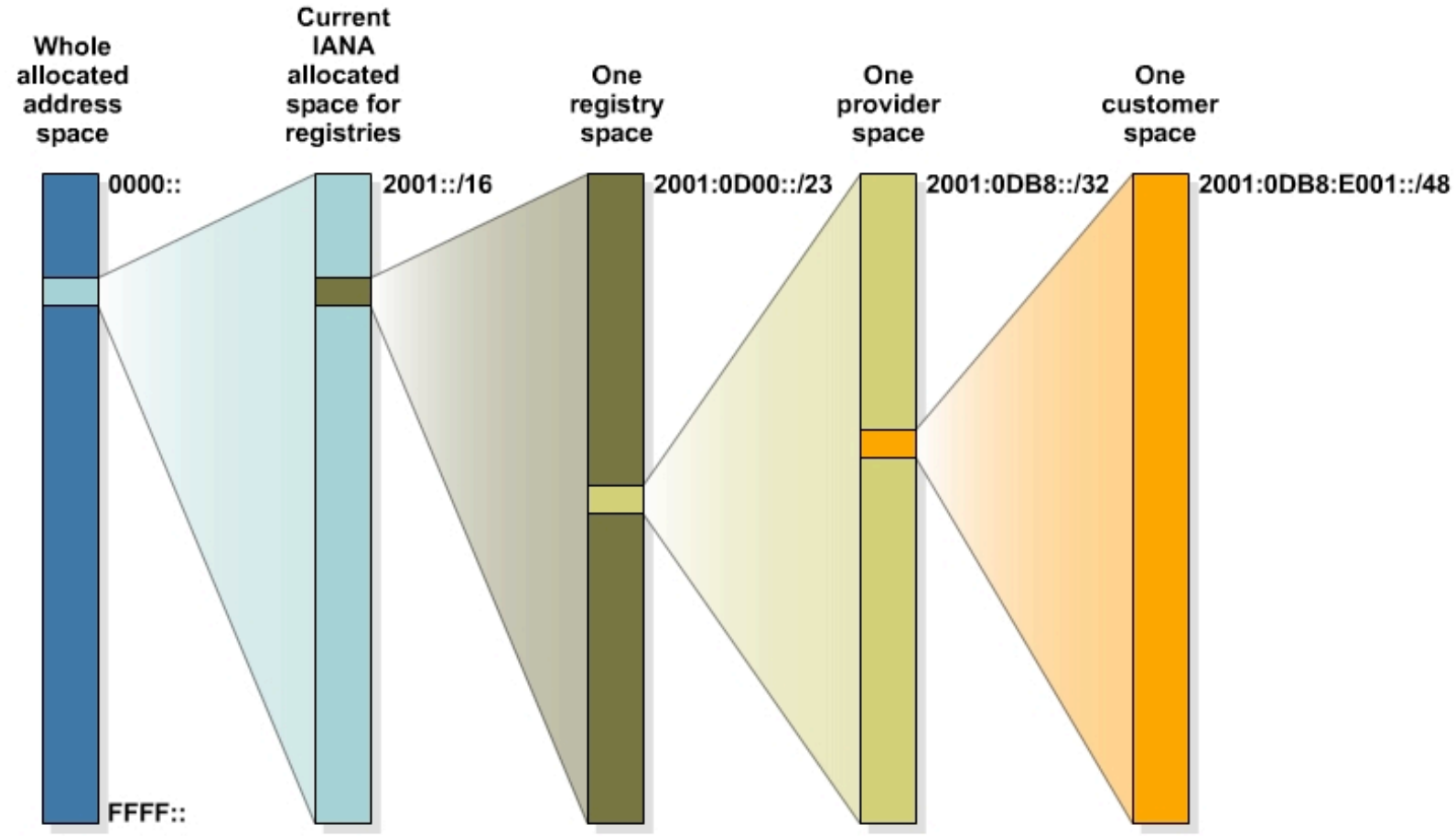
X = { 0 If EUI-64 Format; 1 If Non-EUI-64 Format }



- Use Example: Mobile IPv6 Home-Agent Anycast Address

IPv6 Address Allocation Process

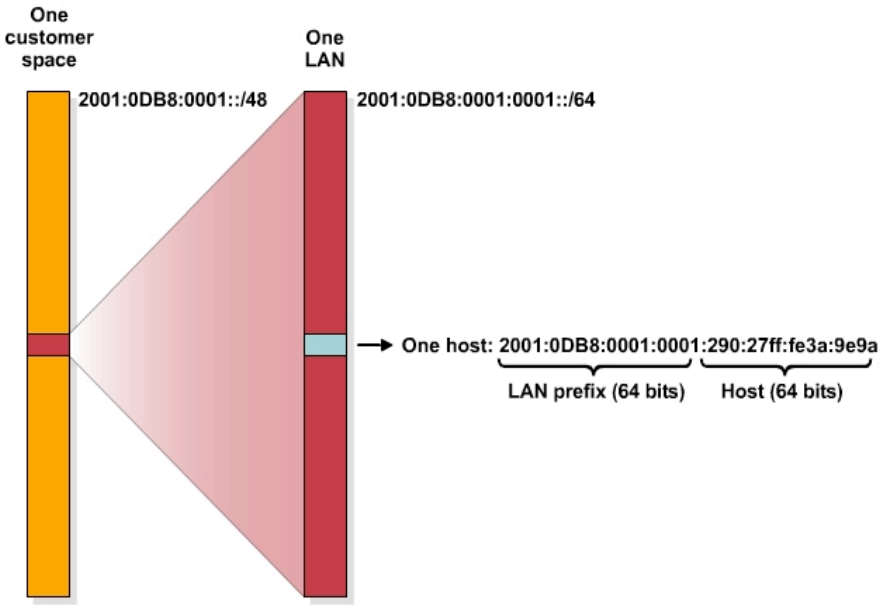
Partition of Allocated IPv6 Address Space



IPv6 Address Allocation Process

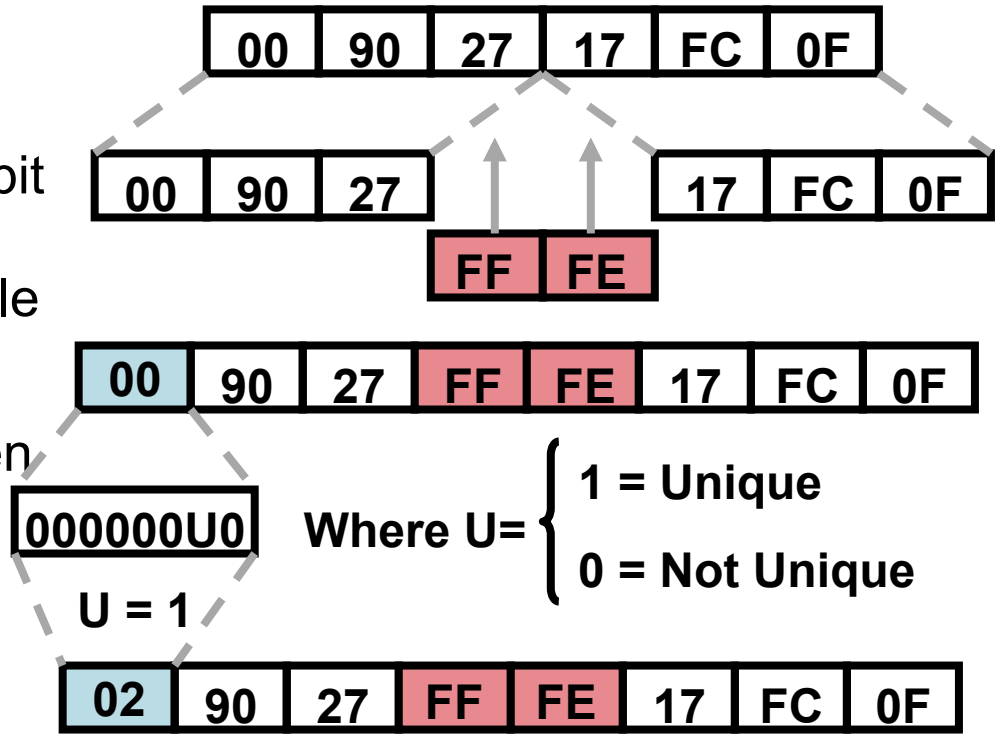
Partition of Allocated IPv6 Address Space (Cont.)

- Lowest-Order 64-bit field of unicast address may be assigned in several different ways:
  - Auto-configured from a 64-bit EUI-64, or expanded from a 48-bit MAC address (e.g., Ethernet address)
  - Auto-generated pseudo-random number (to address privacy concerns)
  - Assigned via DHCP
  - Manually configured

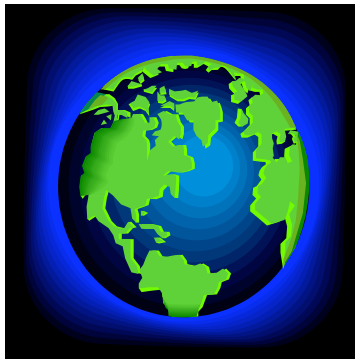


IPv6 Interface Identifier

- Cisco uses 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



IPv6 Addressing



World's population is approximately 6.5 billion

$$\frac{2^{128}}{6.5 \text{ Billion}}$$

$= 5{,}23 * 10^{28}$
= 52 thousand trillion trillion per person

Lots of addresses it is…

Milky way ~ 200 to 400 Billion stars…

ICMP, ND, dhcp, dns, routing, acl…

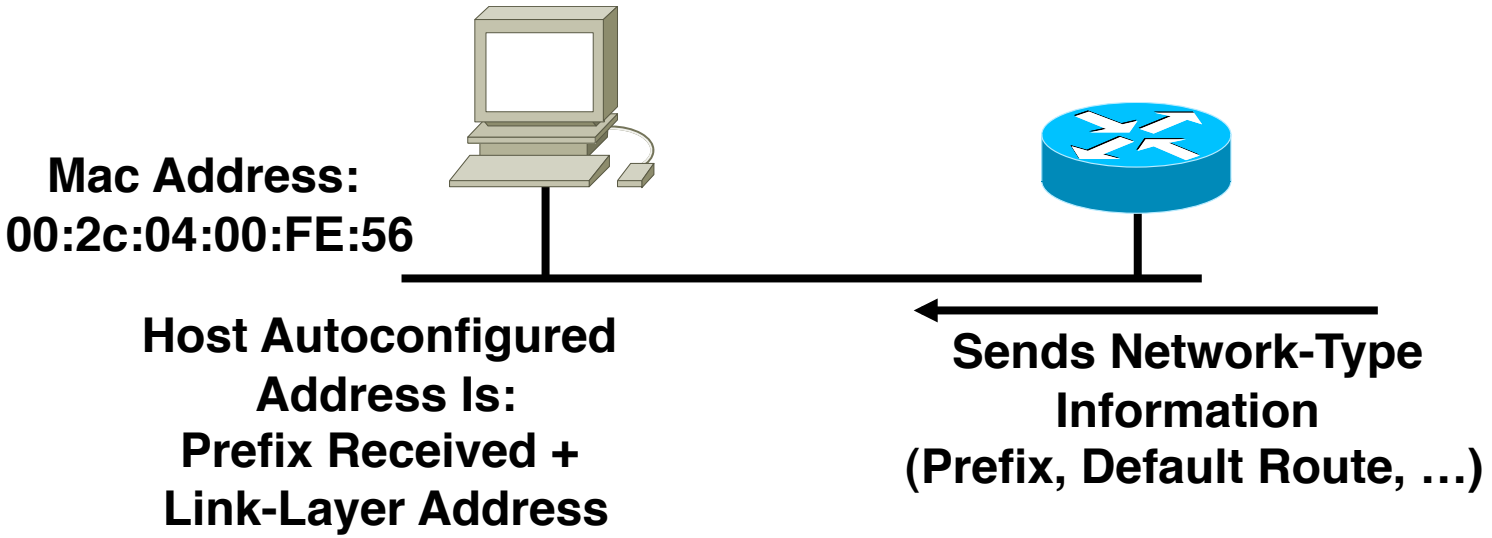
ICMPv6

- Internet Control Message Protocol version 6
- RFC 2463
- Modification of ICMP from IPv4
- Message types are similar (but different types/codes)
  - Destination unreachable (type 1)
  - Packet too big (type 2)
  - Time exceeded (type 3)
  - Parameter problem (type 4)
  - Echo request/reply (type 128 and 129)

ICMPv6 Message Fields

- Type—identifies the message or action needed
- Code—is a type-specific sub-identifier. For example, Destination Unreachable can mean no route, port unreachable, administratively prohibited, etc.
- Checksum—computed over the entire ICMPv6 message and prepended with a pseudo-header containing a single-octet
- Next Header in ipv6 will have a value of 58 for icmp

Autoconfiguration



Larger Address Space Enables:

- The use of link-layer addresses inside the address space
- Autoconfiguration with “no collisions”
- Offers “plug and play”

Renumbering

Mac Address:
00:2c:04:00:FE:56

Host Autoconfigured Address Is:
New Prefix Received
+ Link-Layer Address

Sends New Network-Type Information
(Prefix, Default Route, …)
Data = Two prefixes:
- Current prefix (to be deprecated), with short lifetimes
- New prefix (to be used), with normal lifetimes

Larger Address Space Enables:

- Renumbering, using autoconfiguration and multiple addresses

Renumbering (Cont.)

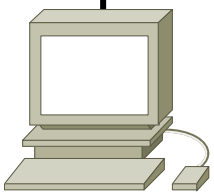
Router Configuration after Renumbering:

```
interface Ethernet0
  ipv6 nd prefix 2001:db8:c18:1::/64 43200 0
  ipv6 nd prefix 2001:db8:c18:2::/64 43200 43200
```

or:

```
interface Ethernet0
  ipv6 nd prefix 2001:db8:c18:1::/64 at Jul 31 2008 23:59 Jul 20 2008 23:59
  ipv6 nd prefix 2001:db8:c18:2::/64 43200 43200
```

New Network Prefix: 2001:db8:c18:2::/64
Deprecated Prefix: 2001:db8:c18:1::/64



Router Advertisements

Autoconfiguring IPv6 Hosts

Host Configuration:

```
deprecated address 2001:db8:c18:1:260:8ff:fede:8fbe
preferred address 2001:db8:c18:2:260:8ff:fede:8fbe
```

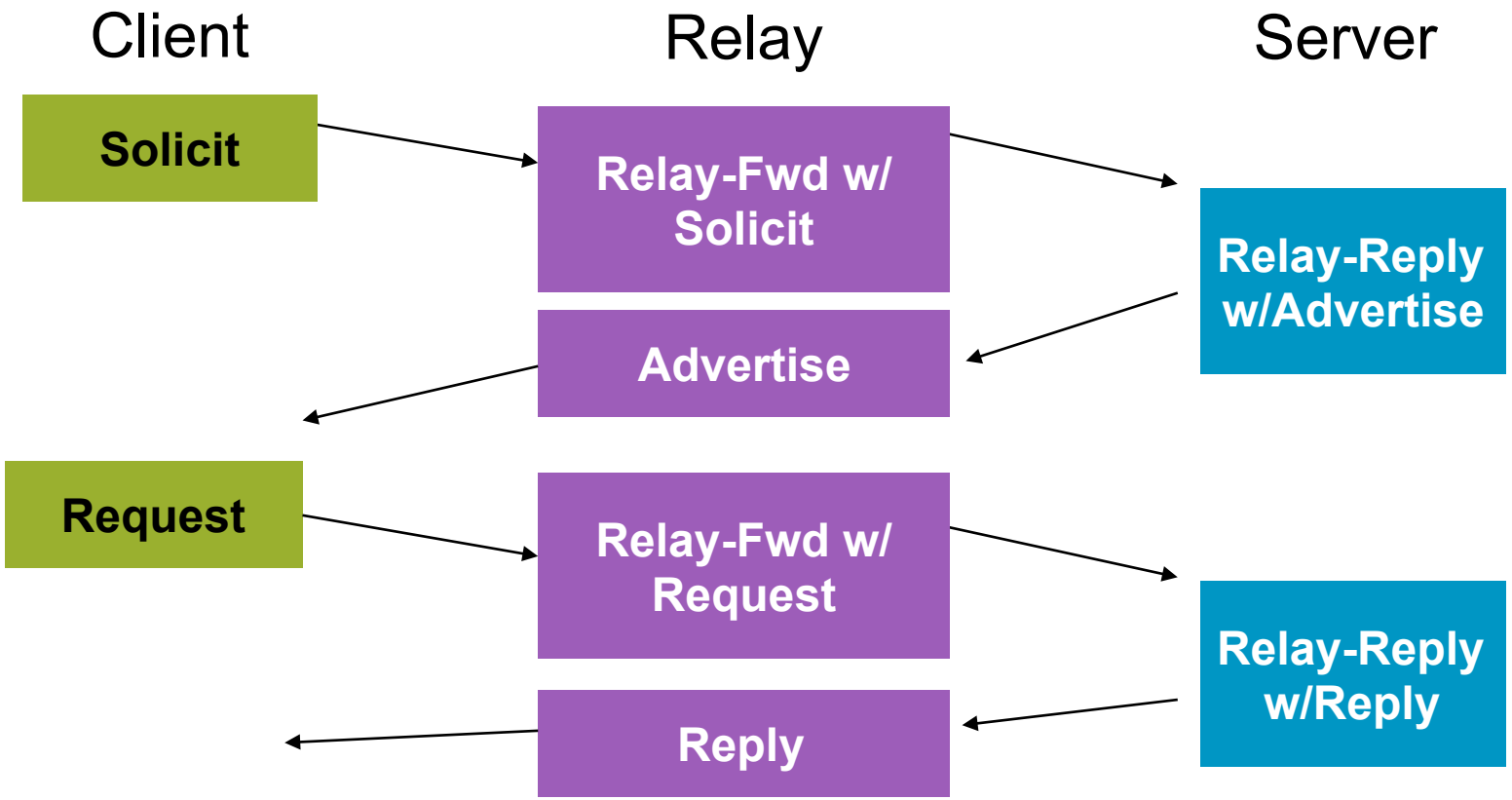
DHCPv6

- Updated version of DHCP for IPv4
- Client detects the presence of routers on the link
- If found, then examines router advertisements to determine if DHCP can or should be used
- If no router found or if DHCP can be used, then

  DHCP Solicit message is sent to the All-DHCP-Agents multicast address

  Using the link-local address as the source address

DHCPv6 Operation



- All_DHCP_Relay_Agents_and_Servers (FF02::1:2)
- All_DHCP_Servers (FF05::1:3)
- DHCP Messages: Clients listen UDP port 546; servers and relay agents listen on UDP port 547

Stateful/Stateless DHCPv6

- Stateful and Stateless DHCPv6 Server

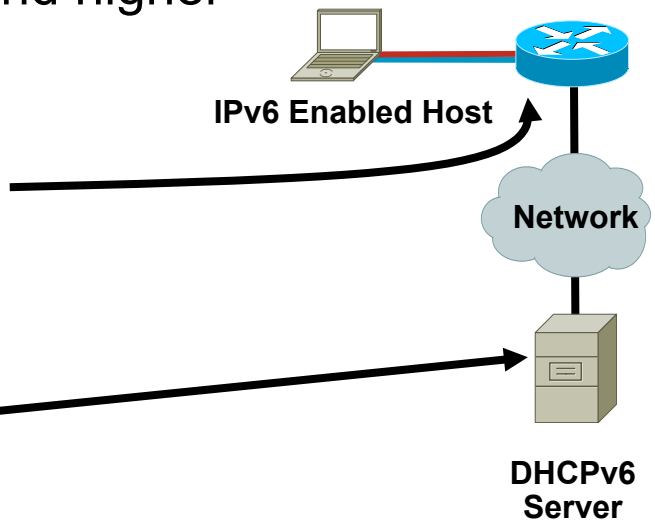
  Cisco Network Registrar:
  http://www.cisco.com/en/US/products/sw/netmgtsw/ps1982/

  Microsoft Windows Server 2008:
  http://technet2.microsoft.com/windowsserver2008/en/library/bab0f1a1-54aa-4cef-9164-139e8bcc44751033.mspx?mfr=true

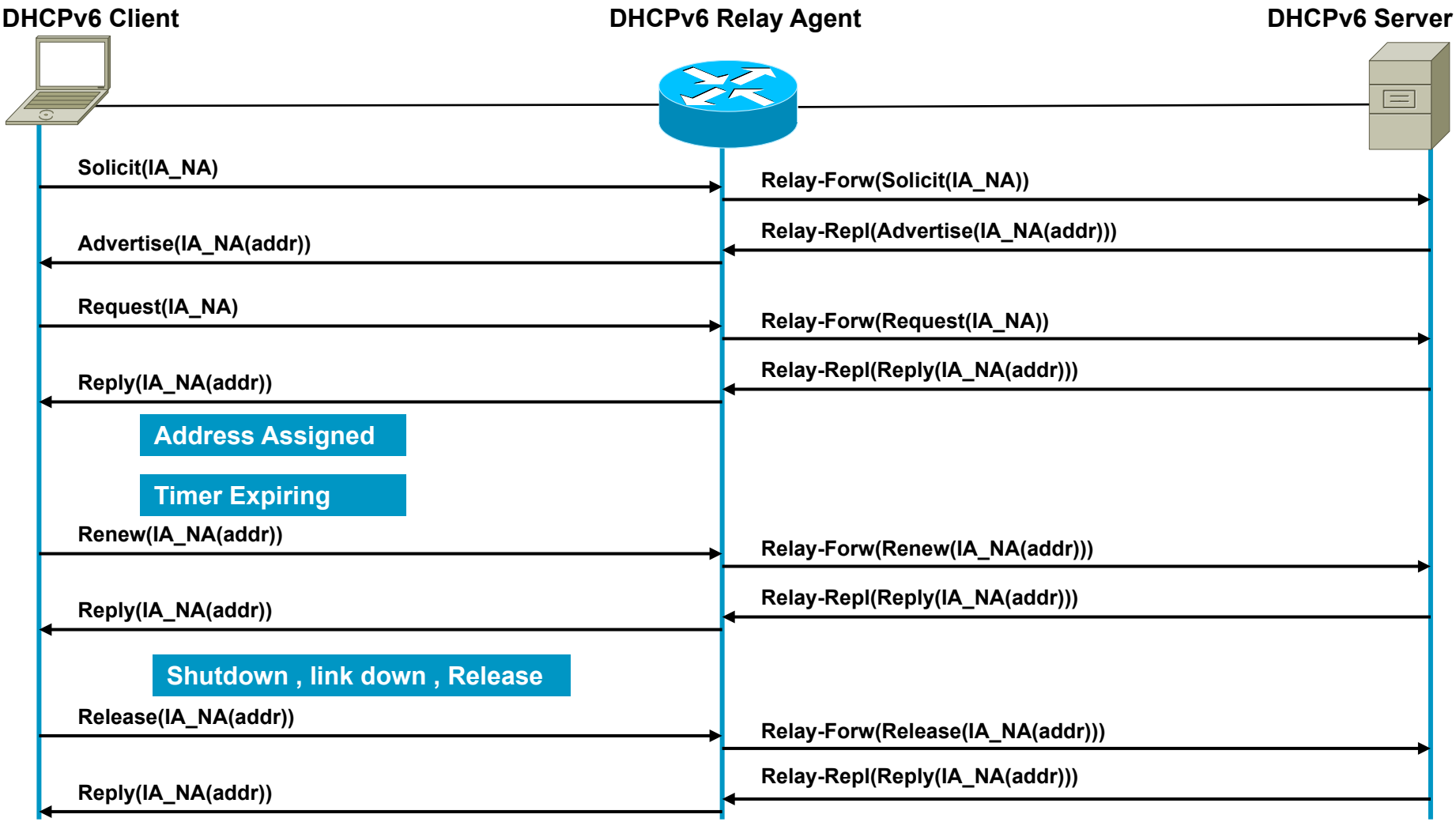
  Dibbler: http://klub.com.pl/dhcpv6/

- DHCPv6 Relay—12.3(11)T/12.2(28)SB and higher

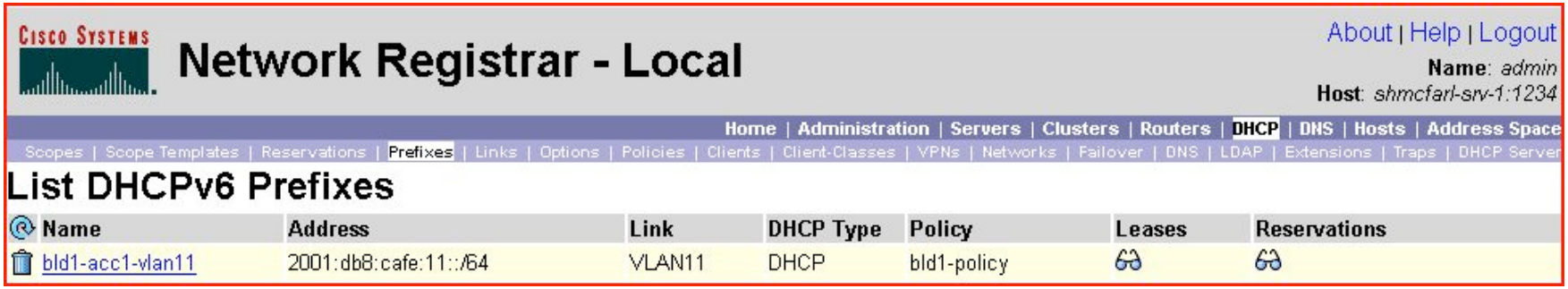
```
interface FastEthernet0/1
 description CLIENT LINK
 ipv6 address 2001:DB8:CAFE:11::1/64
 ipv6 nd prefix 2001:DB8:CAFE:11::/64 no-advertise
 ipv6 nd managed-config-flag
 ipv6 nd other-config-flag
 ipv6 dhcp relay destination 2001:DB8:CAFE:10::2
```

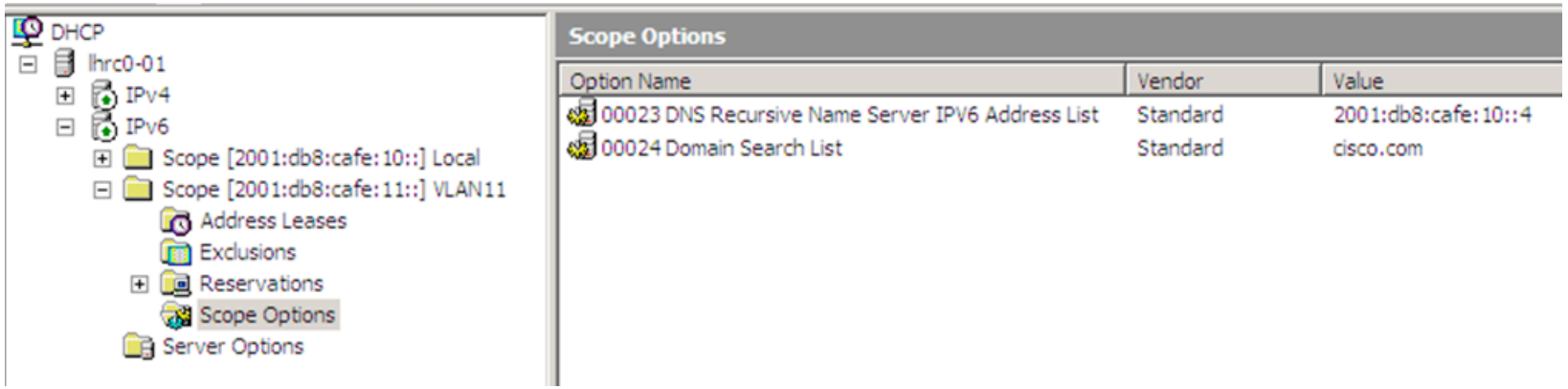


Basic DHCPv6 Message Exchange



CNR/W2K8—DHCPv6





IPv6 General Prefix

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

  "ESE ::11:0:0:0:1" = 2001:db8:cafe:11::1/64

```
ipv6 unicast-routing
ipv6 cef
ipv6 general-prefix ESE 2001:DB8:CAFE::/48
!
interface GigabitEthernet3/2
ipv6 address ESE ::2/126
ipv6 cef
!
interface GigabitEthernet1/2
ipv6 address ESE ::E/126
ipv6 cef
```

```
interface Vlan11
 ipv6 address ESE ::11:0:0:0:1/64
 ipv6 cef
!
interface Vlan12
 ipv6 address ESE ::12:0:0:0:1/64
 ipv6 cef
```

```
Global unicast address(es):
  2001:DB8:CAFE:11::1, subnet is 2001:DB8:CAFE:11::/64
```

Neighbor Discovery

- Replaces ARP, ICMP (redirects, router discovery)
- Reachability of neighbors
- Hosts use it to discover routers, auto configuration of addresses
- Duplicate Address Detection (DAD)

Neighbor Discovery

- Neighbor discovery uses ICMPv6 messages, originated from node on link local with hop limit of 255
- Consists of IPv6 header, ICMPv6 header, neighbor discovery header, and neighbor discovery options
- Five neighbor discovery messages
  1. Router solicitation (ICMPv6 type 133)
  2. Router advertisement (ICMPv6 type 134)
  3. Neighbor solicitation (ICMPv6 type 135)
  4. Neighbor advertisement (ICMPv6 type 136)
  5. Redirect (ICMPV6 type 137)

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

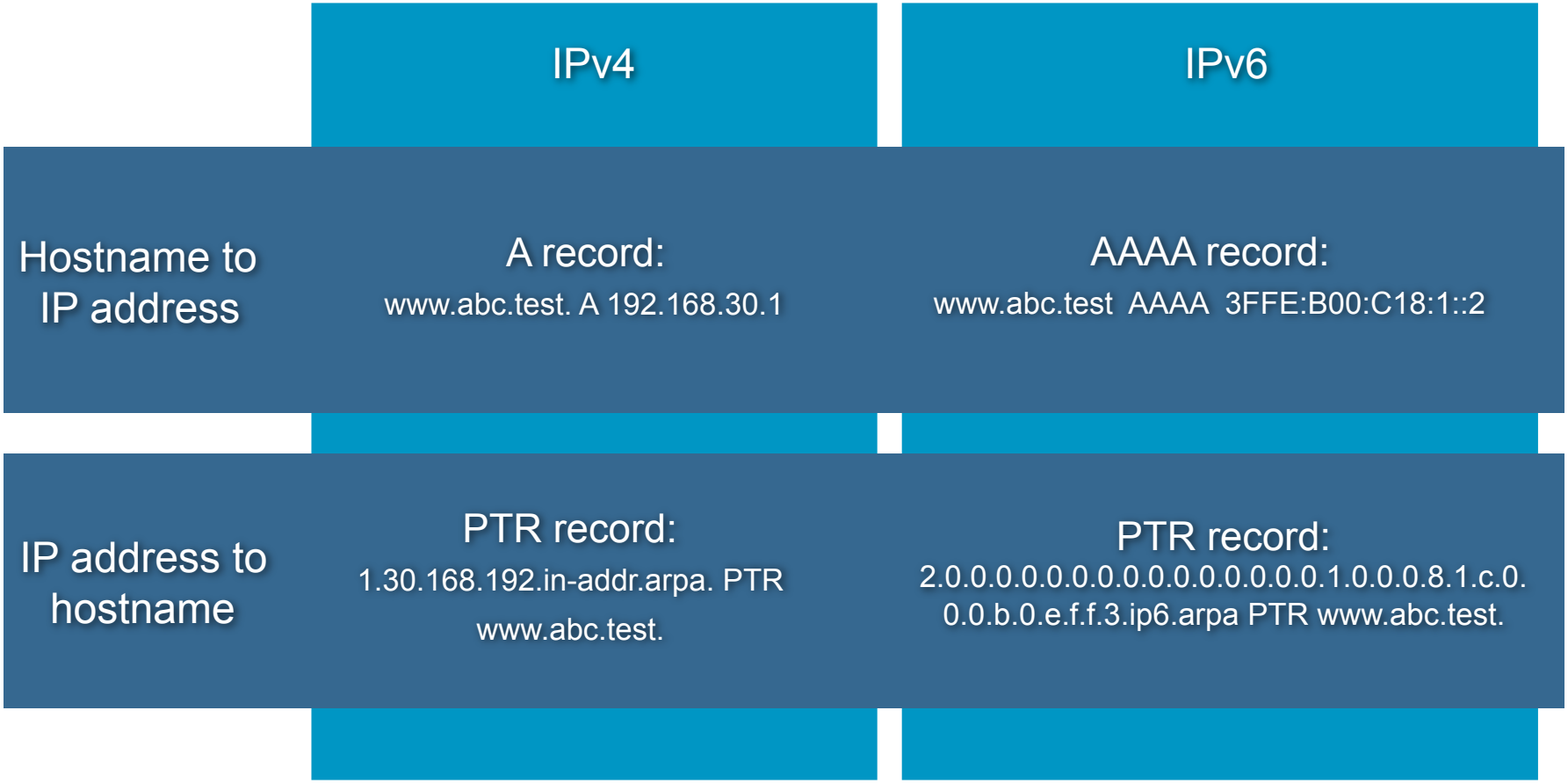
Neighbor Solicitation
ICMP type = 135

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

IPv6 and DNS



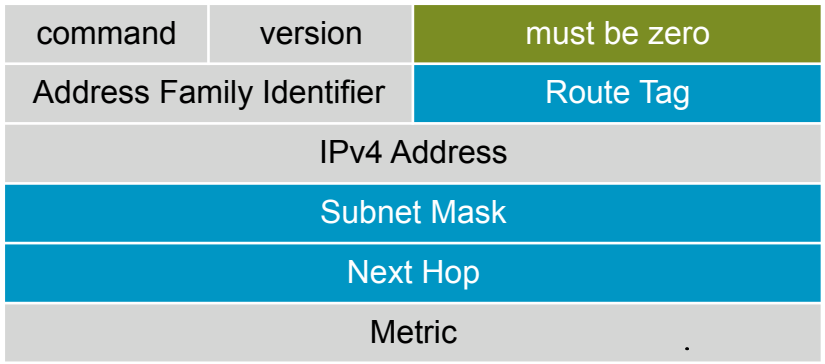
Routing: The IPv4 – IPv6 Parallel slalom

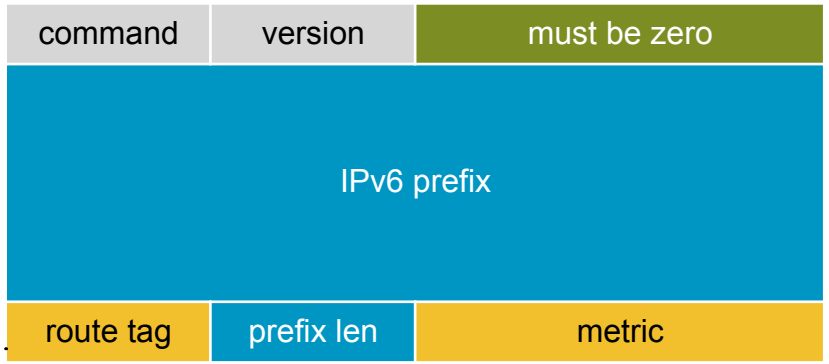
RIP	RIPv2 for IPv4 RIPng for IPv6 Distinct but similar protocols with RIPng taking advantage of IPv6 specificities
OSPF	OSPFv2 for IPv4 OSPFv3 for IPv6 Distinct but similar protocols with OSPFv3 being a cleaner implementation that takes advantage of IPv6 specificities
IS-IS	Extended to support IPv6 Natural 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

RIPng (RFC 2080)

Enhanced Routing Protocol Support RIPng Overview RFC 2080





- Similar characteristics as IPv4

  Distance-vector, hop limit of 15, split-horizon, multicast based (FF02::9), UDP port (521) etc.

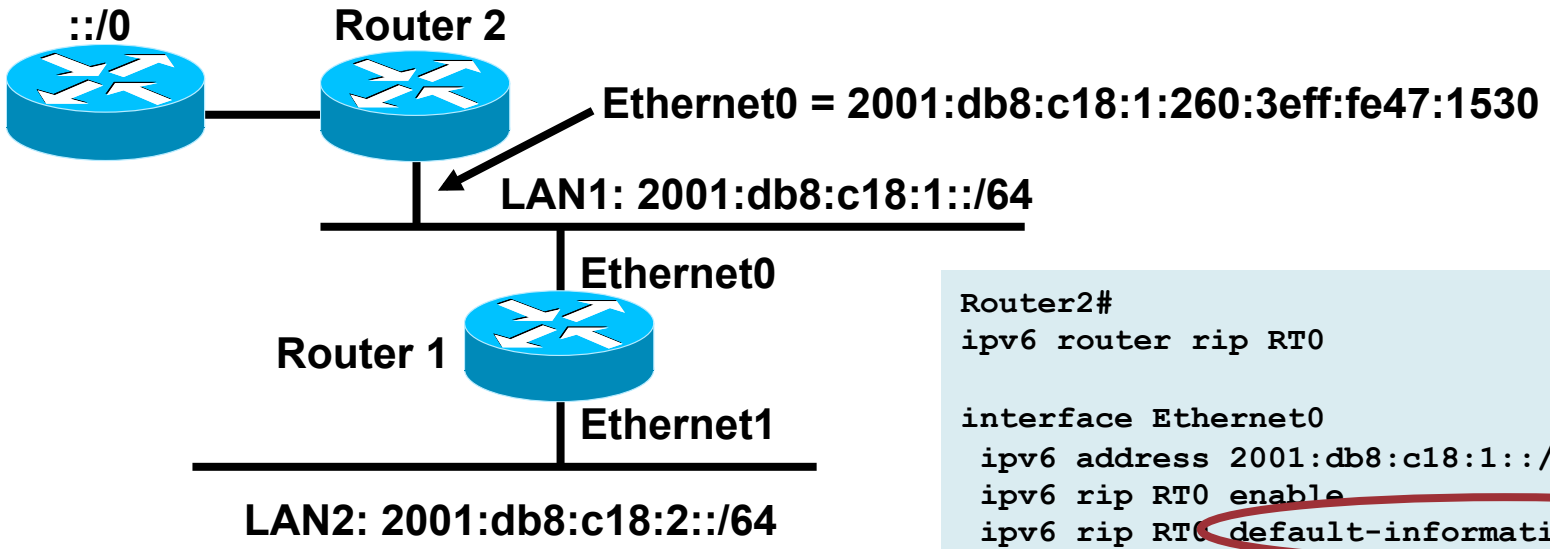
- Updated features for IPv6

  IPv6 prefix & prefix len

- Special Handling for the NH

  Route tag and prefix len for NH is all 0. Metric will have 0xFF; NH must be link local

Enhanced Routing Protocol Support RIPng Configuration and Display




```
Router2#
ipv6 router rip RT0

interface Ethernet0
 ipv6 address 2001:db8:c18:1::/64 eui-64
 ipv6 rip RT0 enable
 ipv6 rip RT0 default-information originate
```

```
Router1#
ipv6 router rip RT0

interface Ethernet0
 ipv6 address 2001:db8:c18:1::/64 eui-64
 ipv6 rip RT0 enable
 Interface Ethernet1
 ipv6 address 2001:db8:c18:2::/64 eui-64
 ipv6 rip RT0 enable
```

```
Router2# debug ipv6 rip
RIPng: Sending multicast update on Ethernet0 for RT0
       src=FE80::260:3eff:fe47:1530
       dst=FF02::9 (Ethernet0)
       sport=521, dport=521, length=32
       command=2, version=1, mbz=0, #rte=1
       tag=0, metric=1, prefix=::/0
```

Multicast All RIP-Routers

Link-Local src Address

Access Lists

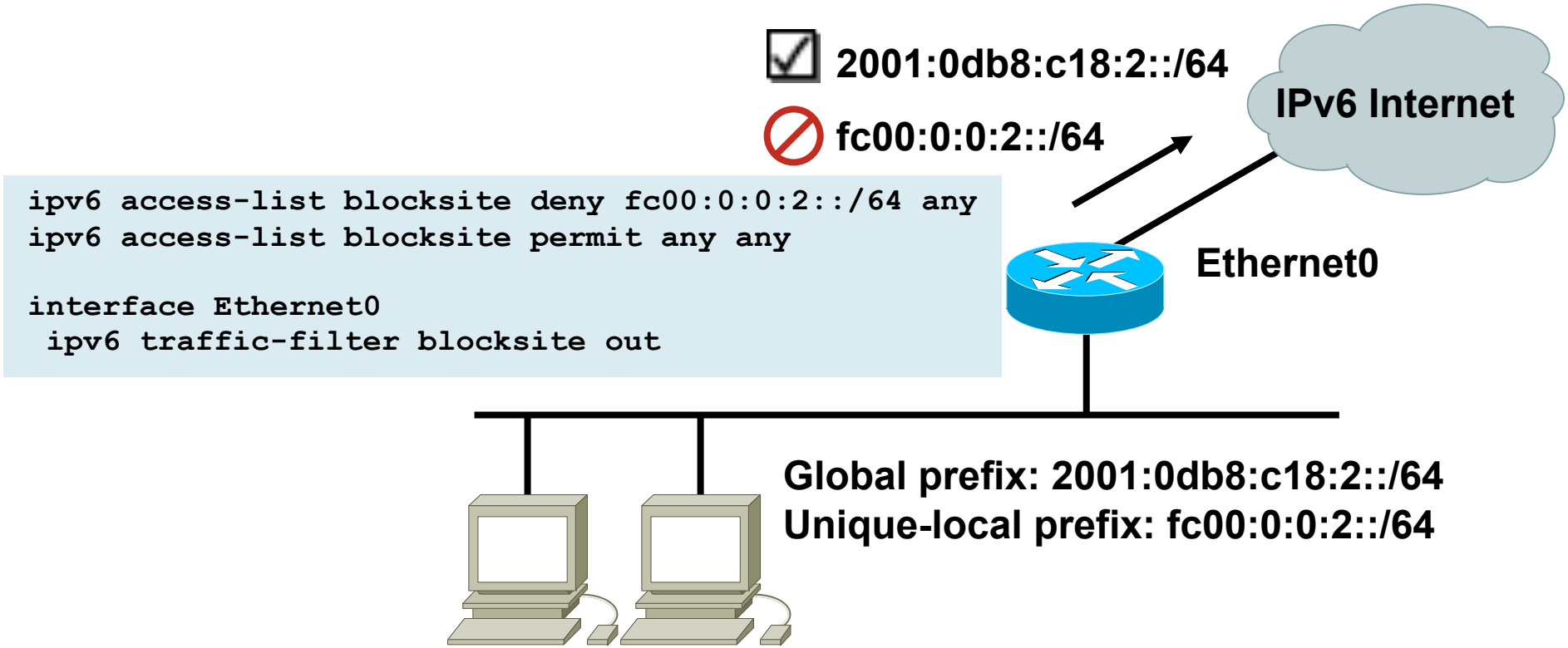
Cisco IOS Standard Access Lists

When Used for Traffic Filtering, IPv6 Standard Access Control Lists (ACL) Offers the Following Functions:

- Can filter traffic based on source and destination address
- Can filter traffic inbound or outbound on a specific interface
- Can add priority to the ACL
- Implicit “deny all” at the end of access list

IPv6 Access-List Example

- Filtering outgoing traffic from unique-local source addresses

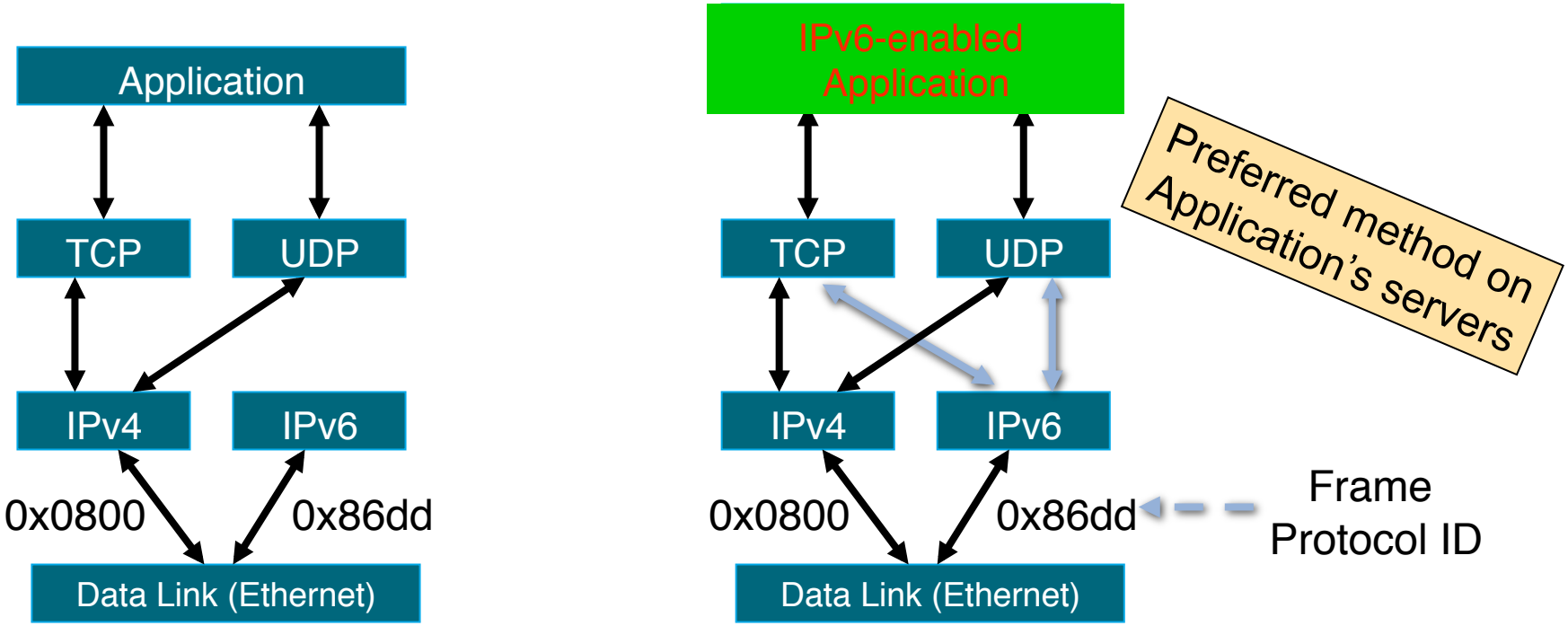


Coexistence

IPv4-IPv6 Transition/Coexistence

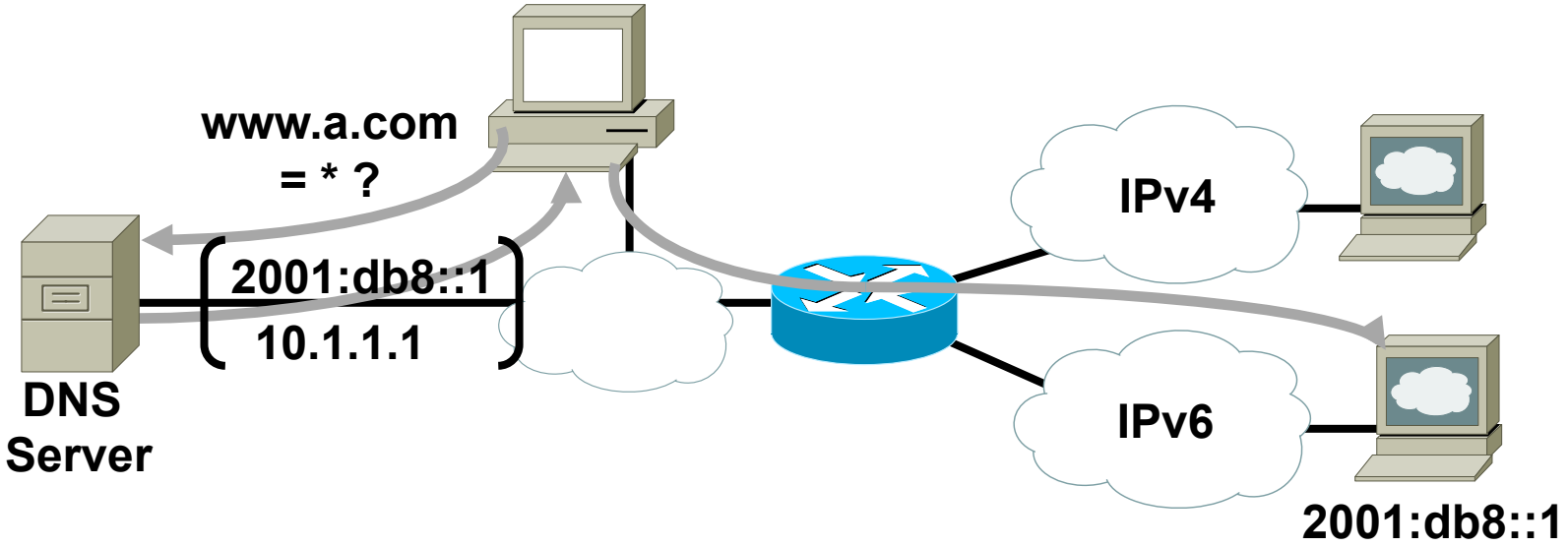
- A wide range of techniques have been identified and implemented, basically falling into three categories:
  1. Dual-stack techniques, to allow IPv4 and IPv6 to co-exist in the same devices and networks
  2. Tunneling techniques, to avoid order dependencies when upgrading hosts, routers, or regions
  3. Translation techniques, to allow IPv6-only devices to communicate with IPv4-only devices
- Expect all of these to be used, in combination

Dual Stack Approach



- Dual stack node means:
  - –Both IPv4 and IPv6 stacks enabled
  - –Applications can talk to both
  - –Choice of the IP version is based on name lookup and application preference

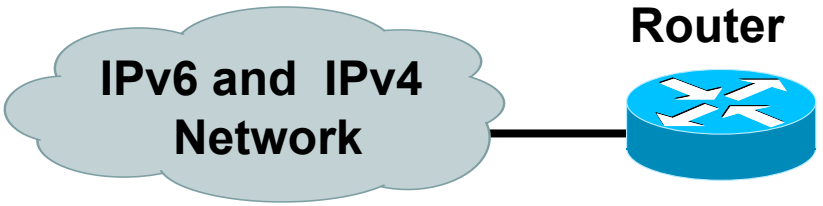
Host Running Dual Stack



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

Cisco IOS Dual Stack Configuration




```
router#
ipv6 unicast-routing

interface Ethernet0
 ip address 192.168.99.1 255.255.255.0
 ipv6 address 2001:db8:213:1::/64 eui-64
```

IPv4: 192.168.99.1

IPv6: 2001:db8:213:1::/64 eui-64

Cisco IOS® Is IPv6-Enable:

- If IPv4 and IPv6 are configured on one interface, the router is dual-stacked
- Telnet, Ping, Traceroute, SSH, DNS client, TFTP, etc.

Tunneling

Tunneling

Many Ways to Do Tunneling

- Some ideas same as before

  GRE, MPLS, IP

- Native IP over data link layers

  ATM PVC, dWDM Lambda, Frame Relay PVC, Serial, Sonet/ SDH, Ethernet

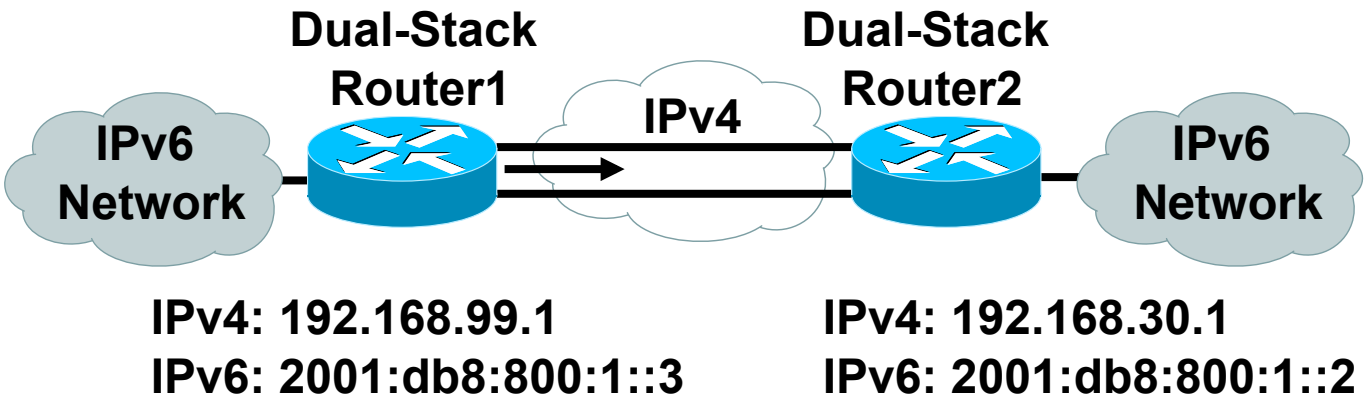
- Some new techniques

  Automatic tunnels using IPv4 , compatible IPv6 address, 6to4, ISATAP

Using Tunnels for IPv6 Deployment

- Many techniques are available to establish a tunnel:
  - –Manually configured
    - •Manual Tunnel (RFC 2893)
    - •GRE (RFC 2473)
  - –Automatic
    - •Compatible IPv4 (RFC 2893): Deprecated
    - •6to4 (RFC 3056)
    - •6over4: Deprecated
    - •ISATAP (RFC 4214)
    - •Teredo (RFC 4380)

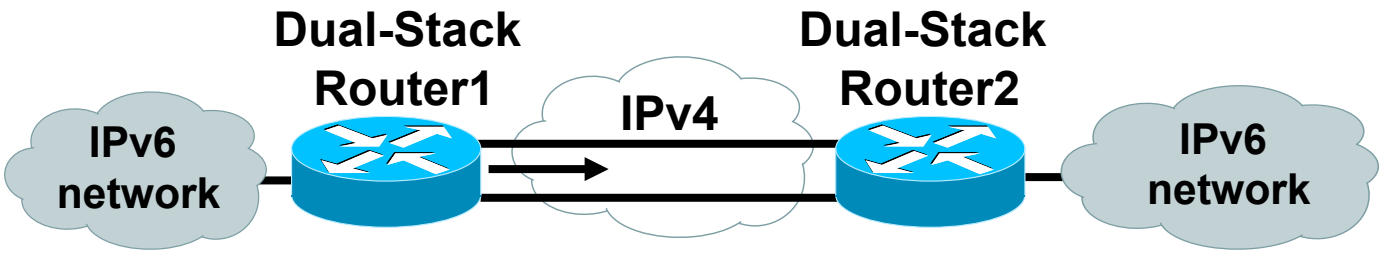
Manually Configured GRE Tunnel




```
router1#

interface Tunnel0
 ipv6 enable
 ipv6 address 2001:db8:c18:1::3/128
 tunnel source 192.168.99.1
 tunnel destination 192.168.30.1
 tunnel mode gre ipv6
```

```
router2#

interface Tunnel0
 ipv6 enable
 ipv6 address 2001:db8:c18:1::2/128
 tunnel source 192.168.30.1
 tunnel destination 192.168.99.1
 tunnel mode gre ipv6
```

Manually Configured IPv6 over IPv4 Tunnel



IPv4: 192.168.99.1
IPv6: 2001:db8:800:1::3

IPv4: 192.168.30.1
IPv6: 2001:db8:800:1::2

```
router1#

interface Tunnel0
 ipv6 enable
 ipv6 address
2001:db8:c18:1::3/127
 tunnel source 192.168.99.1
 tunnel destination 192.168.30.1
 tunnel mode ipv6ip
```

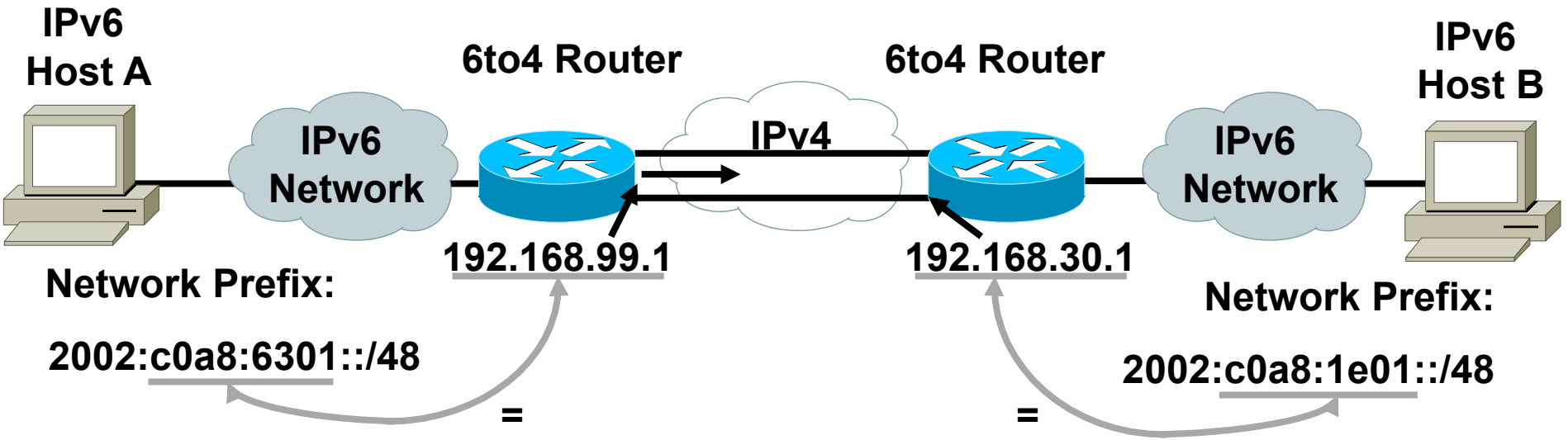
```
router2#

interface Tunnel0
 ipv6 enable
 ipv6 address 2001:db8:c18:1::2/127
 tunnel source 192.168.30.1
 tunnel destination 192.168.99.1
 tunnel mode ipv6ip
```

6to4 Tunneling

Automatic 6to4 Tunnels

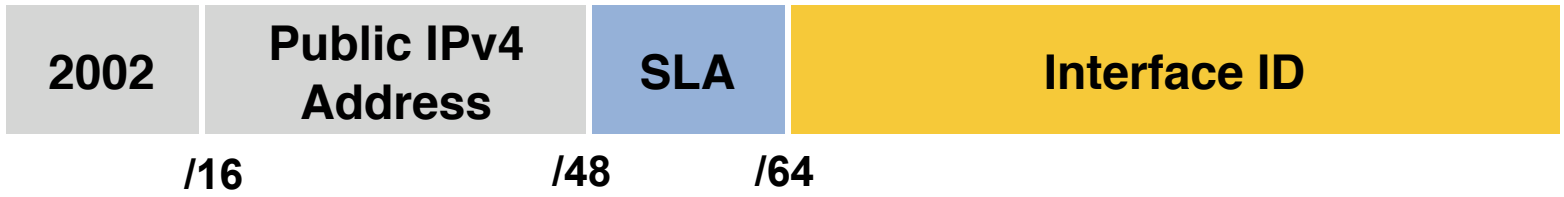
- Automatic 6to4 tunnel allows isolated IPv6 domains to connect over an IPv4 network
- Unlike the manual 6to4 the tunnels are not point-to-point, they are multipoint tunnels
- IPv4 is embedded in the IPv6 address is used to find the other end of the tunnel
- Address format is 2002:IPv4 address::

Automatic 6to4 Tunnel (RFC 3056)

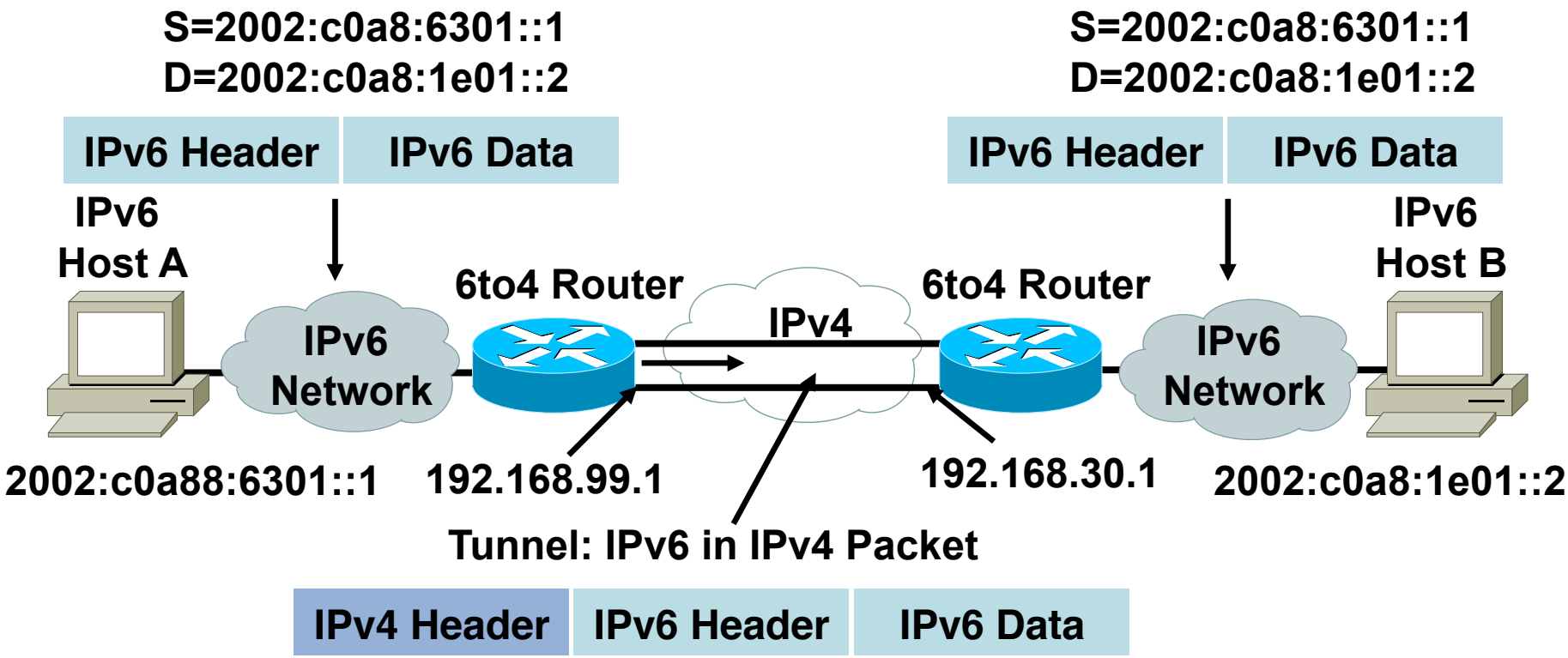


6to4:

- Is an automatic tunnel method
- Gives a prefix to the attached IPv6 network

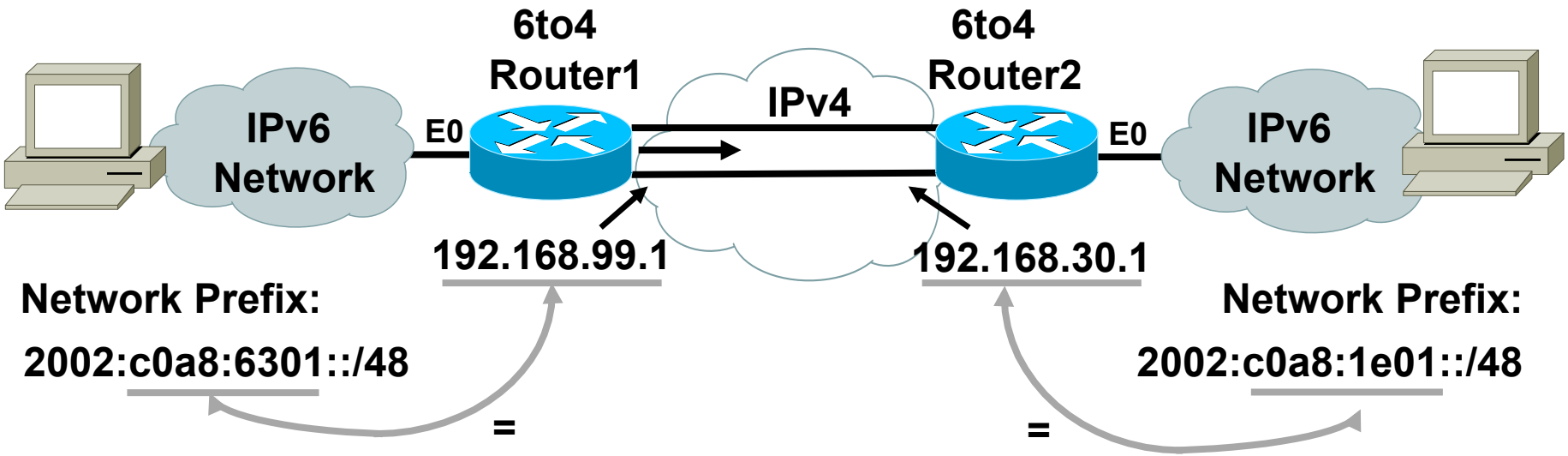


Automatic 6to4 Tunnel (RFC 3056)



S(v4)=192.168.99.1
D(v4)=192.168.30.1
S(v6)=2002:c0a8:6301::1
D(v6)=2002:c0a8:1e01::2

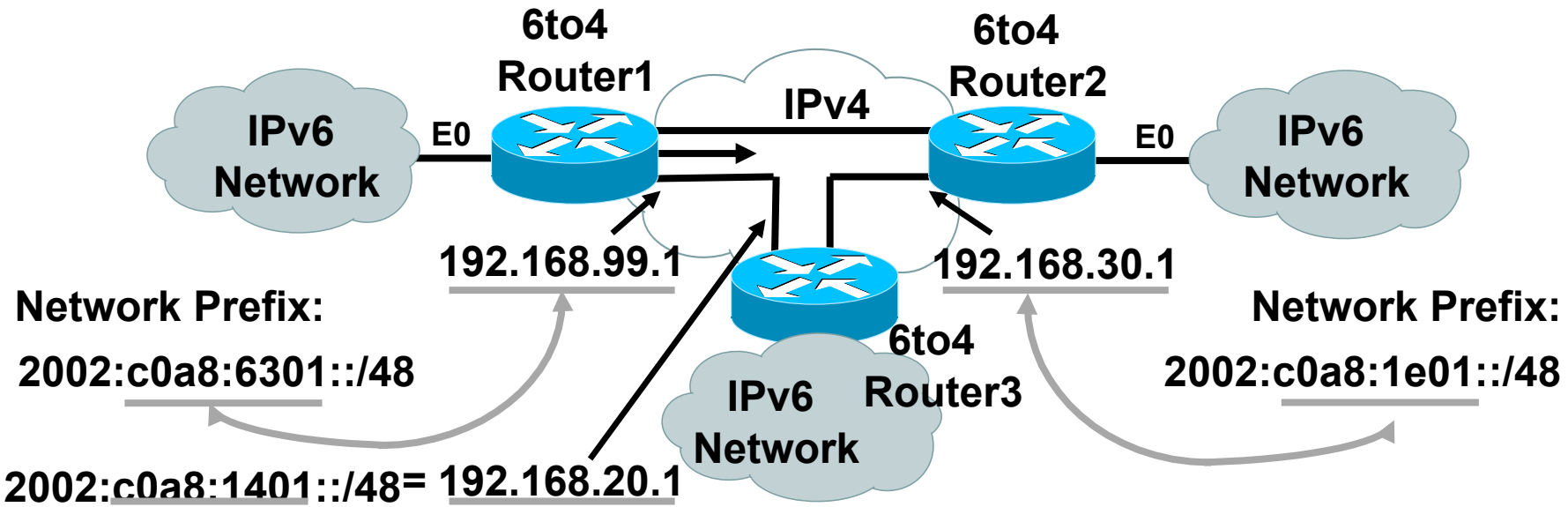
Automatic 6to4 Configuration




```
router1#
interface Ethernet0
 ipv6 address 2002:c0a8:6301:1::/64 eui-64
Interface Ethernet1
  ip address 192.168.99.1 255.255.0.0
interface Tunnel0
 ipv6 unnumbered Ethernet0
 tunnel source Ethernet1
 tunnel mode ipv6ip 6to4

ipv6 route 2002::/16 Tunnel0
```

```
router2#
interface Ethernet0
 ipv6 address 2002:c0a8:1e01:1::/64 eui-64
Interface Ethernet1
 ip address 192.168.30.1 255.255.0.0
interface Tunnel0
 ipv6 unnumbered Ethernet0
 tunnel source Ethernet1
 tunnel mode ipv6ip 6to4

ipv6 route 2002::/16 Tunnel0
```

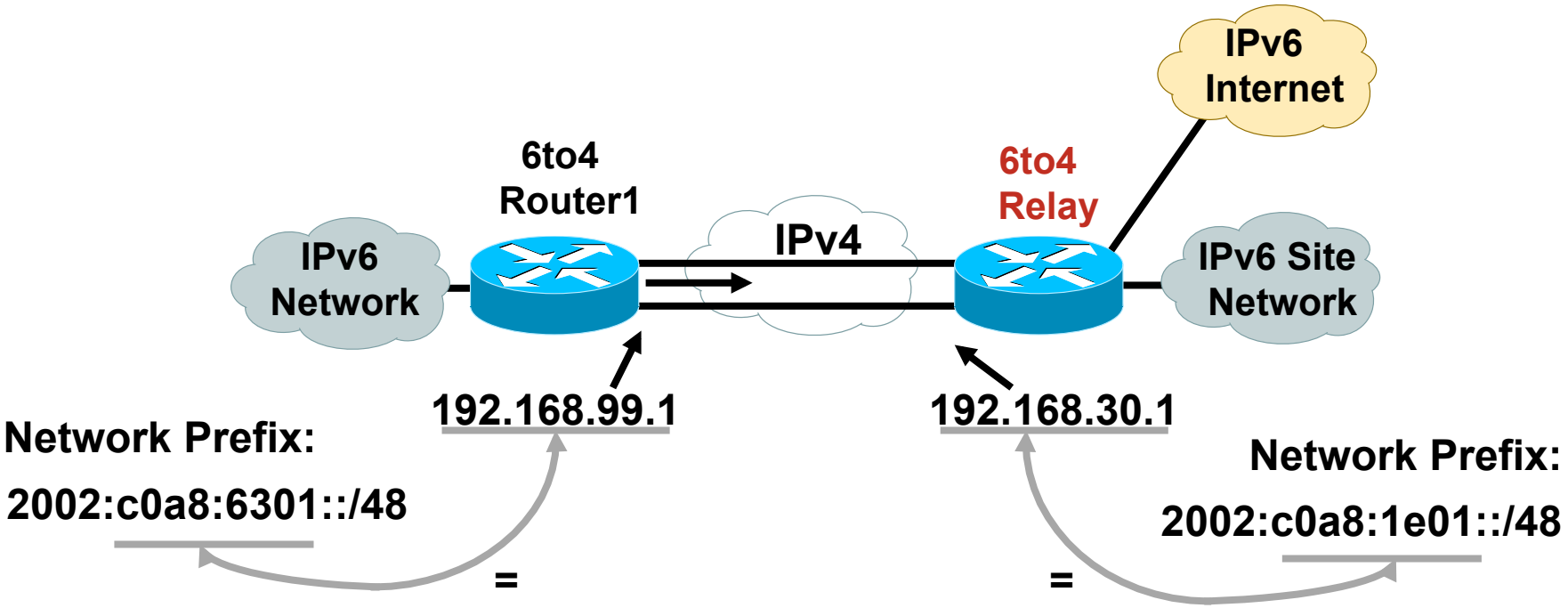
Automatic 6to4 Configuration




```
router1#
interface Ethernet0
 ipv6 address 2002:c0a8:6301:1::/64 eui-64
Interface Ethernet1
  ip address 192.168.99.1 255.255.0.0
interface Tunnel0
 ipv6 unnumbered Ethernet0
 tunnel source Ethernet1
 tunnel mode ipv6ip 6to4

ipv6 route 2002::/16 Tunnel0
```

```
router3#
interface Ethernet0
 ipv6 address 2002:c0a8:1401:1::/64 eui-64
Interface Ethernet1
 ip address 192.168.20.1 255.255.0.0
interface Tunnel0
 ipv6 unnumbered Ethernet0
 tunnel source Ethernet1
 tunnel mode ipv6ip 6to4

ipv6 route 2002::/16 Tunnel0
```

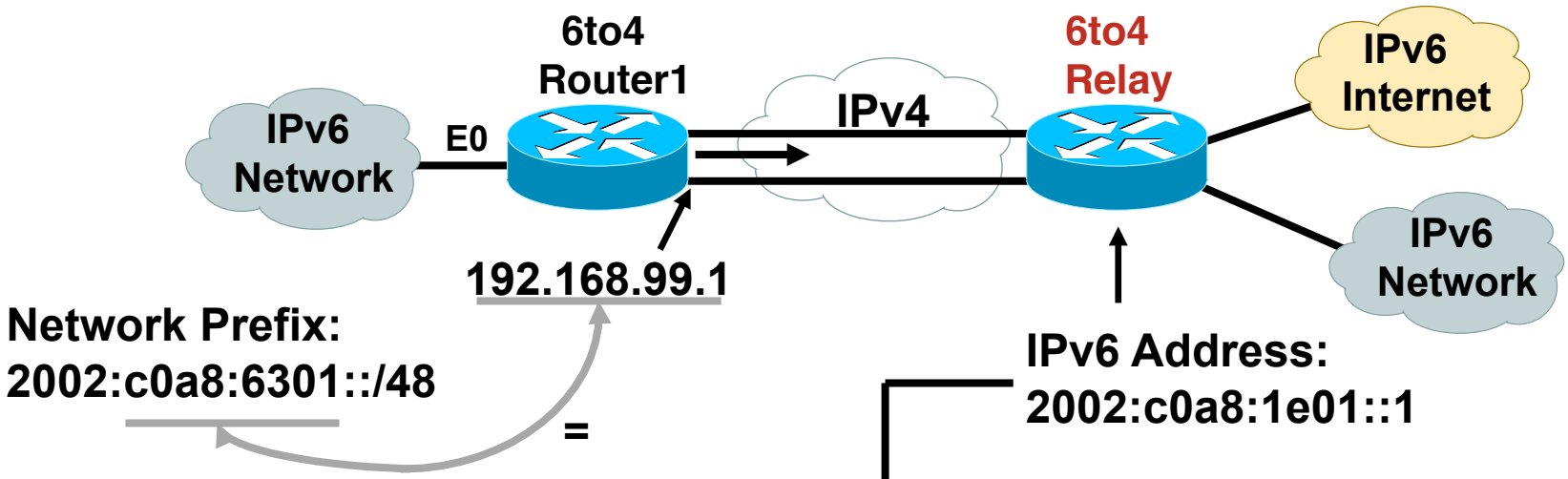
Automatic 6to4 Relay



6to4 Relay:

- Is a gateway to the rest of the IPv6 Internet
- Is a default router

Automatic 6to4 Relay Configuration




```
router1#
interface Ethernet0
 ipv6 address 2002:c0a8:6301:1::/64 eui-64
Interface Ethernet1
  ip address 192.168.99.1 255.255.0.0
interface Tunnel0
 no ip address
 ipv6 unnumbered Ethernet0
 tunnel source Ethernet1
 tunnel mode ipv6ip 6to4

ipv6 route 2002::/16 Tunnel0
ipv6 route ::/0 2002:c0a8:1e01::1
```

Automatic 6to4 Tunnels

Requirements for 6to4

- Border router must be dual stack with a global IPv4 address
- Interior routing protocol for IPv6 is required
- DNS for IPv6

ISATAP Tunneling

Intrasite Automatic Tunnel Address Protocol

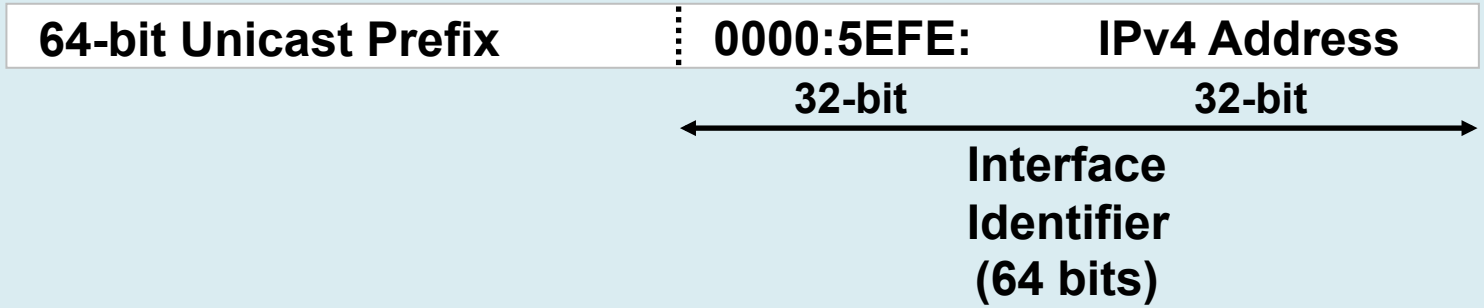
- RFC 4214
- This is for enterprise networks such as corporate and academic networks
- Scalable approach for incremental deployment
- ISATAP makes your IPv4 infratructure as transport (NBMA) network

Intrasite Automatic Tunnel Address Protocol

- RFC 4214
- To deploy a router is identified that carries ISATAP services
- ISATAP routers need to have at least one IPv4 interface and 0 or more IPv6 interface
- DNS entries are created for each of the ISATAP routers IPv4 addresses
- Hosts will automatically discover ISATAP routers and can get access to global IPv6 network
- Host can apply the ISATAP service before all this operation but its interface will only have a link local v6 address until the first router appears

Intrasite Automatic Tunnel Address Protocol

Use IANA's OUI 00-00-5E and Encode IPv4 Address as Part of EUI-64



- ISATAP is used to tunnel IPv4 within as administrative domain (a site) to create a virtual IPv6 network over a IPv4 network
- Supported in Windows XP Pro SP1 and others

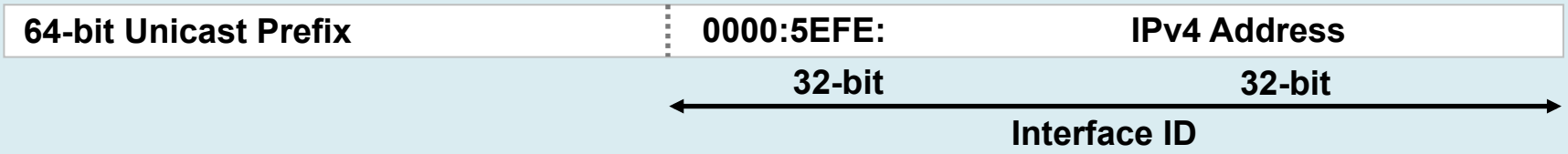
IPv6 Campus ISATAP Configuration

- Supported in Windows XP Pro SP1 and others
- ISATAP connections look like one flat network
- Create DNS “A” record for “ISATAP” = 10.1.1.1
- Use Static Config if DNS use is not desired:

```
C:\>netsh interface ipv6 isatap set
router 10.1.1.1
```

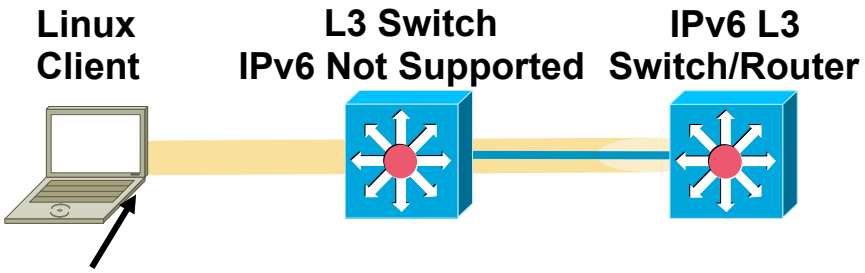
- Currently ISATAP does not support multicast!!

ISATAP Address Format:



2001:DB8:C003:111F:0:5EFE:10.1.2.100

Client Configuration (Linux): ISATAP Tunnels

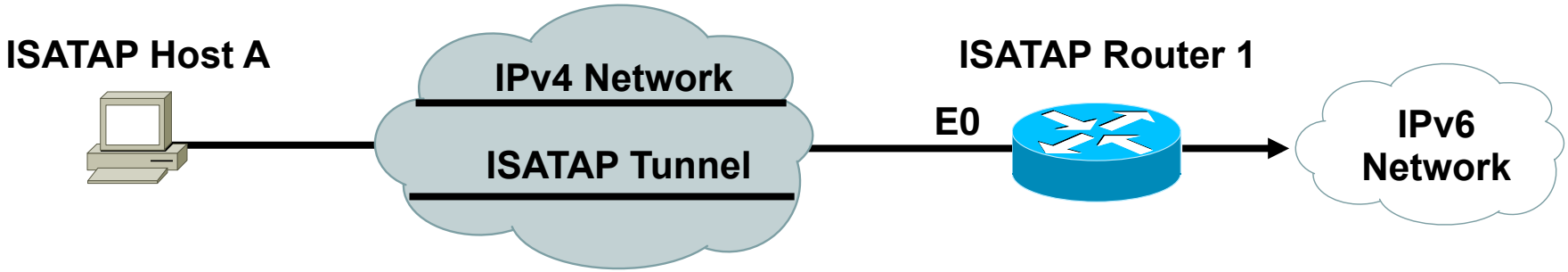


- IPv6-enabled
- Requires Kernel support for ISATAP—USAGI
- Modified IProute package—USAGI
- Must configure ISATAP router —not automatic

Host IP Router IP

```
# ip tunnel add is0 mode isatap 10.1.1.100 v4any 30.1.1.1 ttl 64
# ip link set is0 up
```

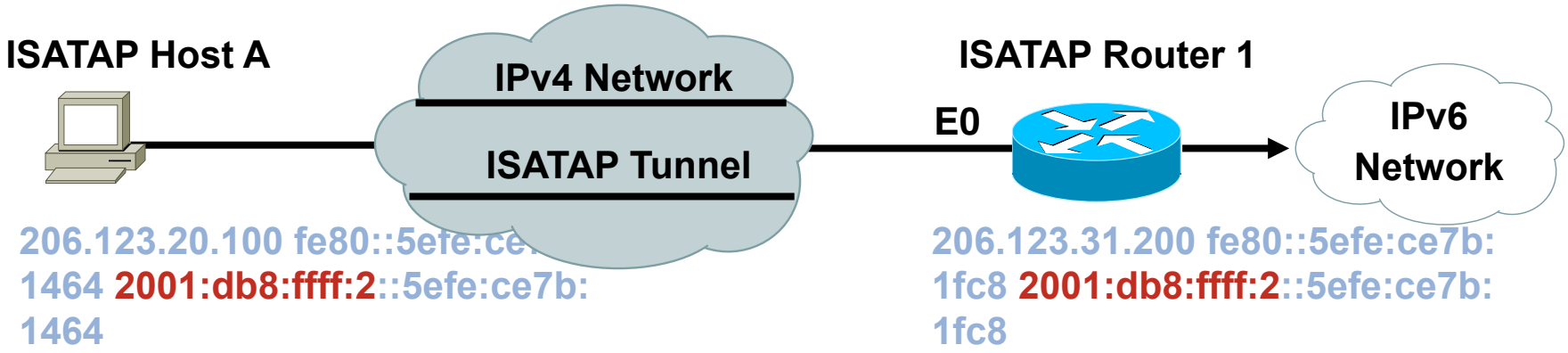
Automatic Advertisement of ISATAP Prefix



ICMPv6 Type 133 (RS)
IPv4 Source: 206.123.20.100
IPv4 Destination: 206.123.31.200
IPv6 Source: fe80::5efe:ce7b:1464
IPv6 Destination: fe80::5efe:ce7b:1fc8
Send me ISATAP Prefix

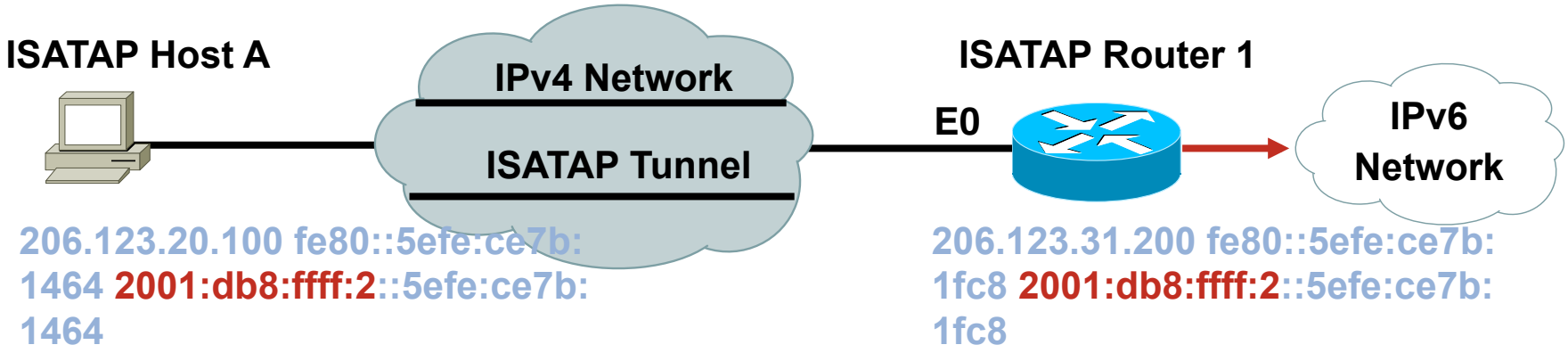
ICMPv6 Type 134 (RA)
IPv4 Source: 206.123.31.200
IPv4 Destination: 206.123.20.100
IPv6 Source: fe80::5efe:ce7b:1fc8
IPv6 Destination: fe80::5efe:ce7b:1464
ISATAP Prefix: 2001:db8:ffff :2::/64

Automatic Address Assignment of Host and Router



- ISATAP host A receives the ISATAP prefix 2001:db8:ffff:2::/64 from ISATAP Router 1
- When ISATAP host A wants to send IPv6 packets to 2001:db8:ffff:2::5efe:ce7b:1fc8, ISATAP host A encapsulates IPv6 packets in IPv4. The IPv4 packets of the IPv6 encapsulated packets use IPv4 source and destination address.

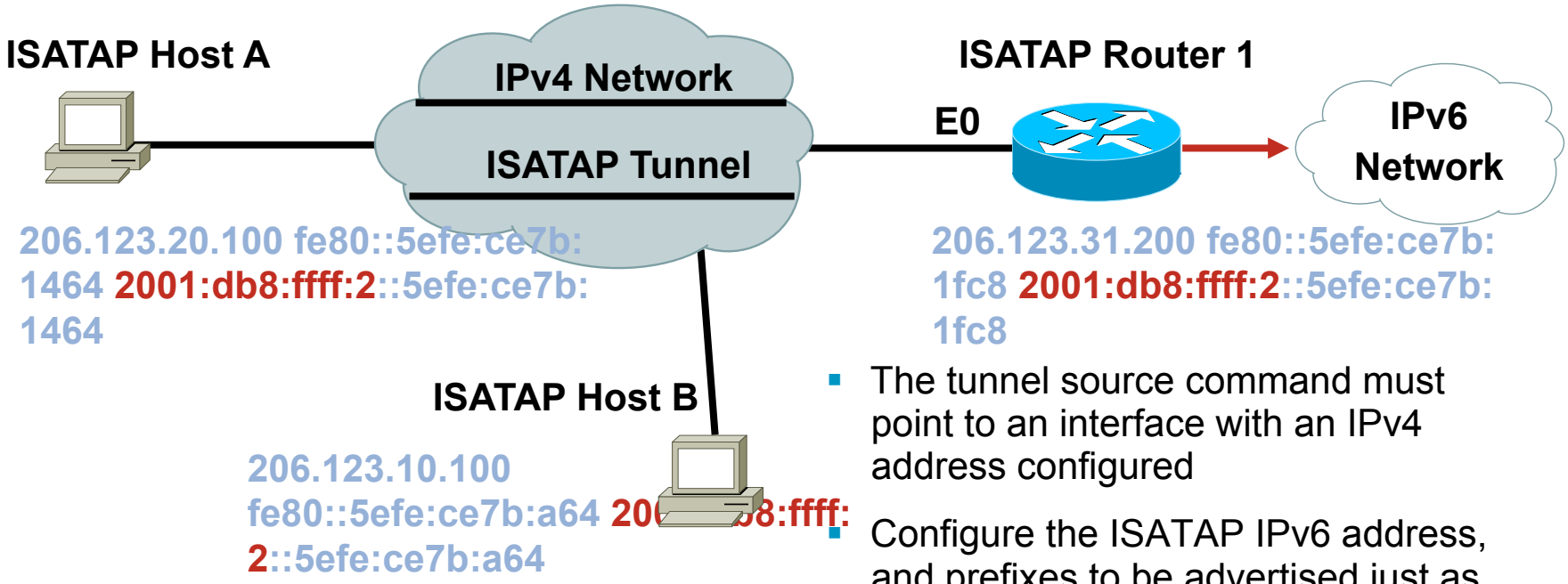
Automatic Configuring ISATAP




```
ISATAP-router1#
!
interface Ethernet0
 ip address 206.123.31.200 255.255.255.0
!
interface Tunnel0
 ipv6 address 2001:db8:ffff:2::/64 eui-64
 no ipv6 nd suppress-ra
 tunnel source Ethernet0
 tunnel mode ipv6ip isatap
```

- The tunnel source command must point to an interface with an IPv4 address configured
- Configure the ISATAP IPv6 address, and prefixes to be advertised just as you would with a native IPv6 interface
- The IPv6 address has to be configured as an EUI-64 address since the last 32 bits in the interface identifier is used as the IPv4 destination address

Automatic Configuring ISATAP




```
ISATAP-router1#
!
interface Ethernet0
 ip address 206.123.31.200 255.255.255.0
!
interface Tunnel0
 ipv6 address 2001:db8:ffff:2::/64 eui-64
 no ipv6 nd suppress-ra
 tunnel source Ethernet0
 tunnel mode ipv6ip isatap
```

- The tunnel source command must point to an interface with an IPv4 address configured
- Configure the ISATAP IPv6 address, and prefixes to be advertised just as you would with a native IPv6 interface
- The IPv6 address has to be configured as an EUI-64 address since the last 32 bits in the interface identifier is used as the IPv4 destination address

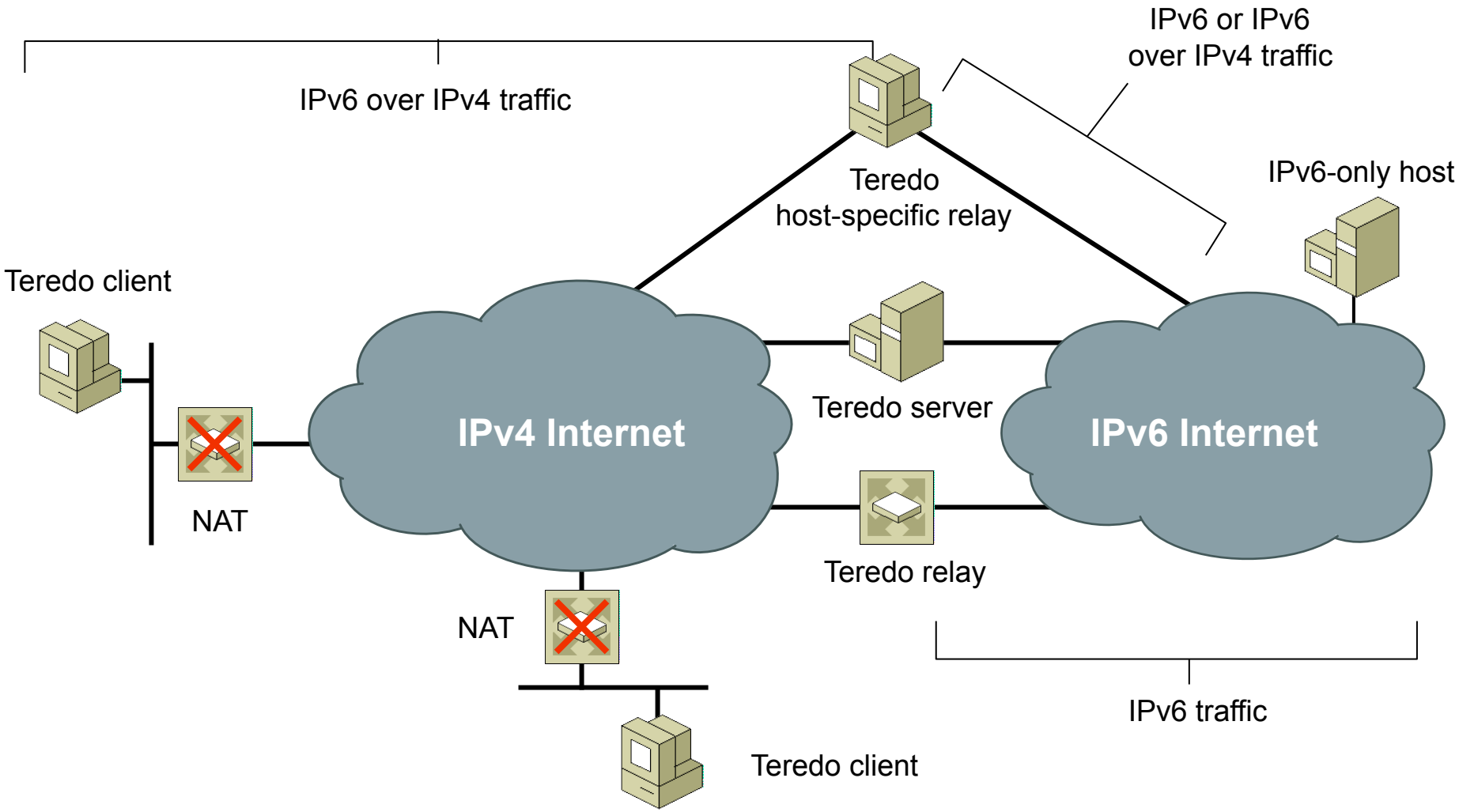
What Is Teredo?

- RFC4380
- Tunnel IPv6 through NATs (NAT types defined in RFC3489)
  - Full Cone NATs (aka one-to-one)—Supported by Teredo
  - Restricted NATs—Supported by Teredo
  - Symmetric NATs—Supported by Teredo with Vista/Server 2008 if only one Teredo client is behind a Symmetric NATs
- Uses UDP port 3544
- Is complex—many sequences for communication and has several attack vectors
- Available on:
  - Microsoft Windows XP SP1 w/Advanced Networking Pack
  - Microsoft Windows Server 2003 SP1
  - Microsoft Windows Vista (enabled by default—inactive until application requires it)
  - Microsoft Server 2008
    http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/teredo.mspx
  - Linux, BSD and Mac OS X—“Miredo”
    http://www.simphalempin.com/dev/miredo/

Teredo Components

- Teredo Client—Dual-stack node that supports Teredo tunneling to other Teredo clients or IPv6 nodes (via a relay)
- Teredo Server—Dual-stack node connected to IPv4 Internet and IPv6 Internet. Assists in addressing of Teredo clients and initial communication between clients and/or IPv6-only hosts—Listens on UDP port 3544
- Teredo Relay—Dual-stack router that forwards packets between Teredo clients and IPv6-only hosts
- Teredo Host-Specific Relay—Dual-stack node that is connected to IPv4 Internet and IPv6 Internet and can communicate with Teredo Clients without the need for a Teredo Relay

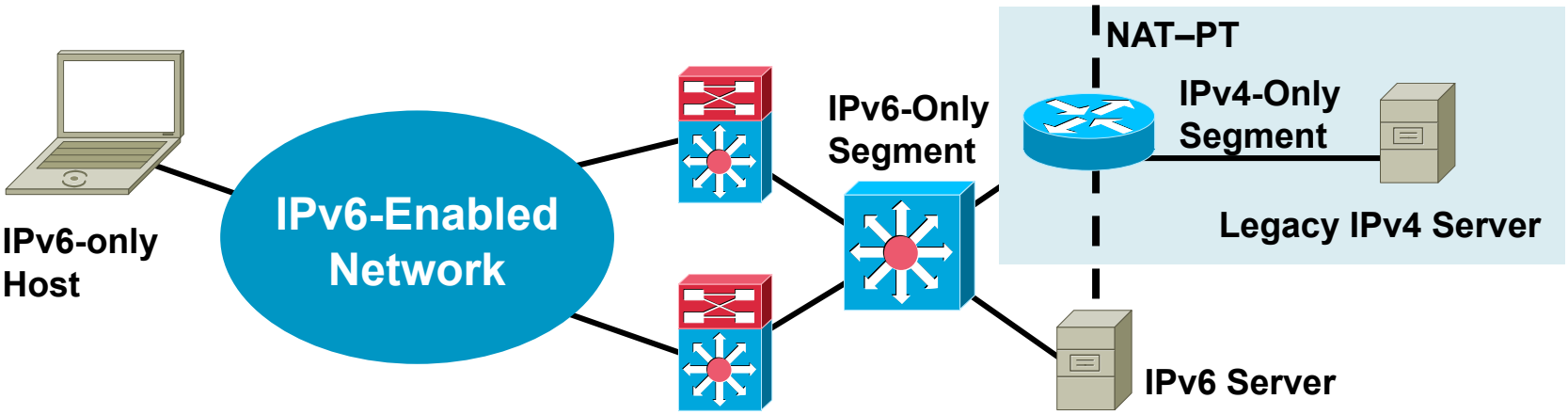
Teredo Overview



*From Microsoft “Teredo Overview” paper

Translation, redundancy, mld

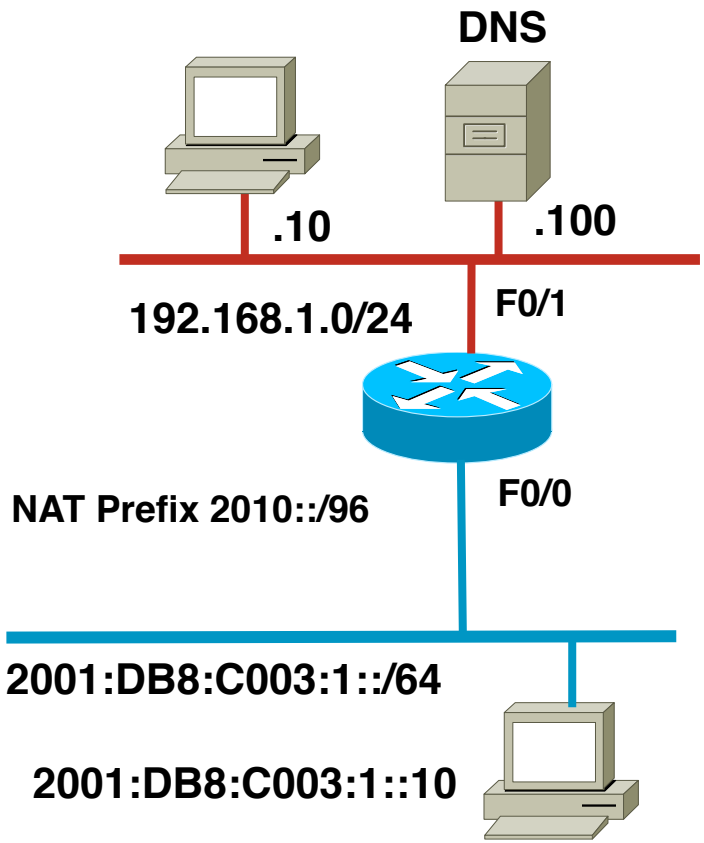
Legacy Services (IPv4 Only)



- Many of the non-routing/switching products do not yet support IPv6 (i.e., content switching modules)
- NAT-PT (Network Address Translation–Protocol Translation) as an option to front-end IPv4-only server—Note: NAT-PT IS being moved to experimental
- Place NAT-PT box as close to IPv4 only server as possible
- Be very aware of performance and manageability issues

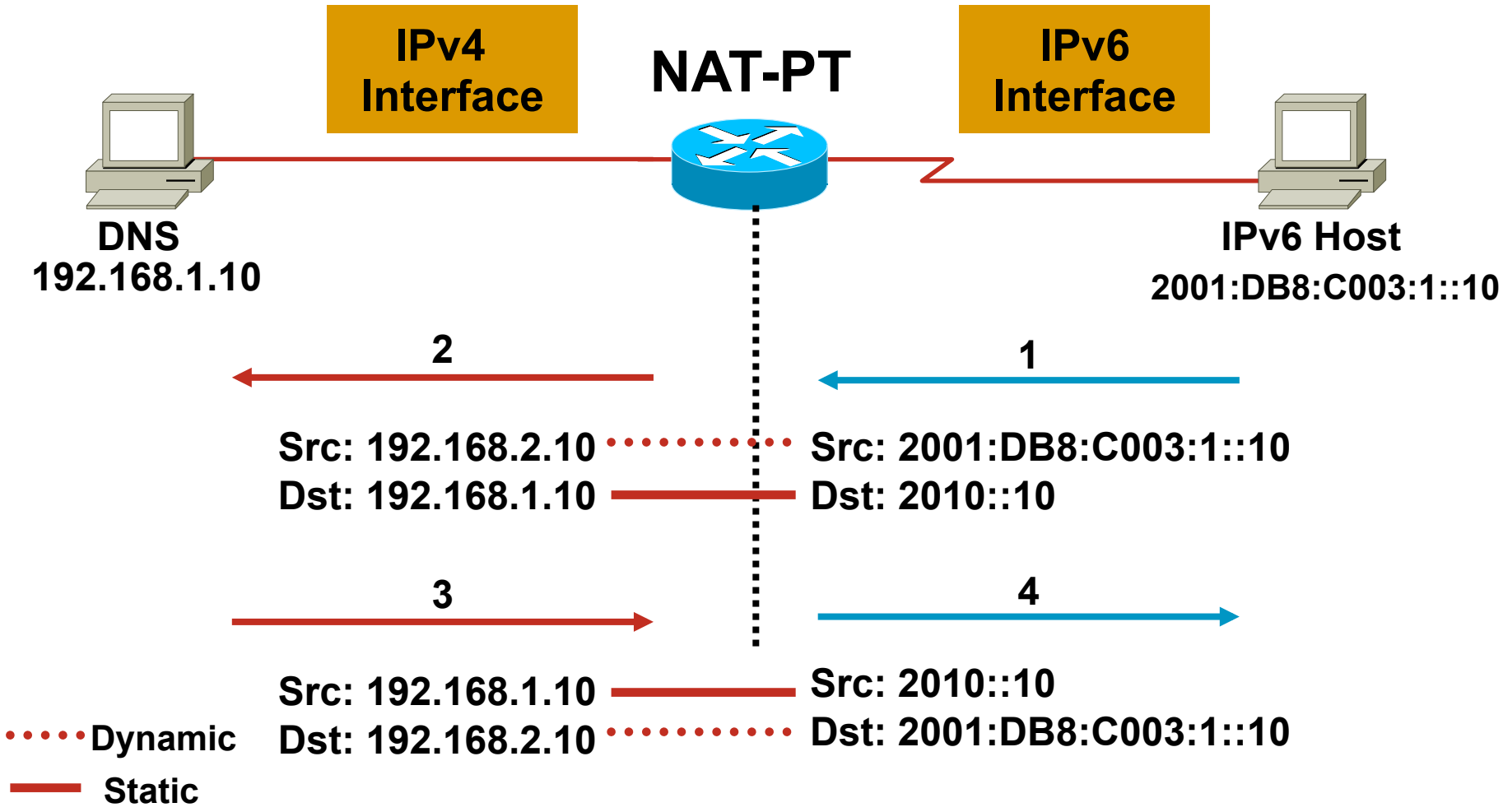
Configuring Cisco IOS NAT-PT

- NAT-PT enables communication between IPv6-only and IPv4-only nodes
- CEF switching in 12.3(14)T

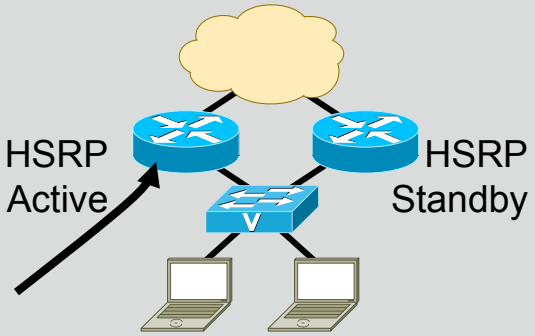



```
interface FastEthernet0/0
   ipv6 address 2001:DB8:C003:1::1/64
   ipv6 cef
   ipv6 nat
!
interface FastEthernet0/1
   ip address 192.168.1.1 255.255.255.0
   ipv6 nat prefix 2010::/96
   ipv6 nat
!
ipv6 nat v4v6 source 192.168.1.100 2010::100
ipv6 nat v4v6 source 192.168.1.10  2010::10
!
ipv6 nat v6v4 source route-map MAP1 pool V4POOL
ipv6 nat v6v4 pool V4POOL 192.168.2.1
192.168.2.10 prefix-length 24
!
route-map MAP1 permit 10
 match interface FastEthernet0/0
```

NAT-PT Packet Flow

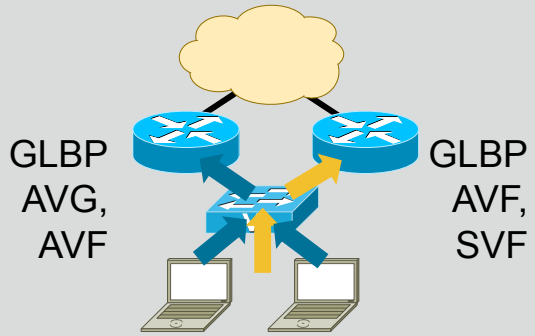


First-Hop Router Redundancy



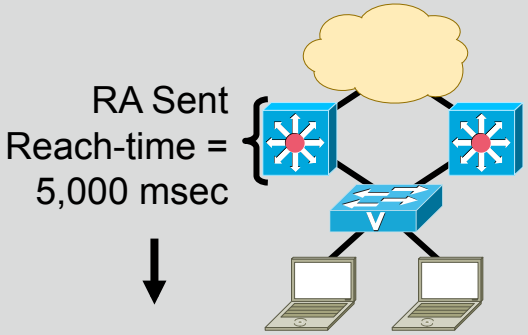
HSRP for v6

- 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)

First-Hop Redundancy

- When HSRP,GLBP and VRRP for IPv6 are not available
- NUD can be used for rudimentary HA at the first-hop (today this only applies to the Campus/DC…HSRP is available on routers)

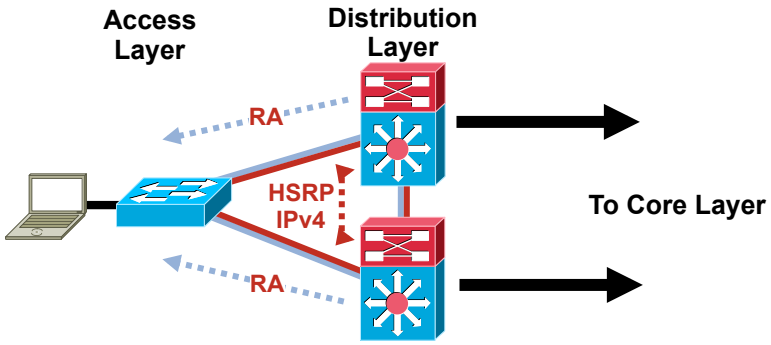
```
(config-if)#ipv6 nd reachable-time 5000
```

- Hosts use NUD “reachable time” to cycle to next known default gateway (30 seconds by default)
- Can be combined with default router preference to determine primary gw:

```
(config-if)#ipv6 nd router-preference {high | medium | low}
```

```
Default Gateway . . . . . . . . . . : 10.121.10.1
                                      fe80::211:bcff:fec0:d000%4
                                      fe80::211:bcff:fec0:c800%4
```

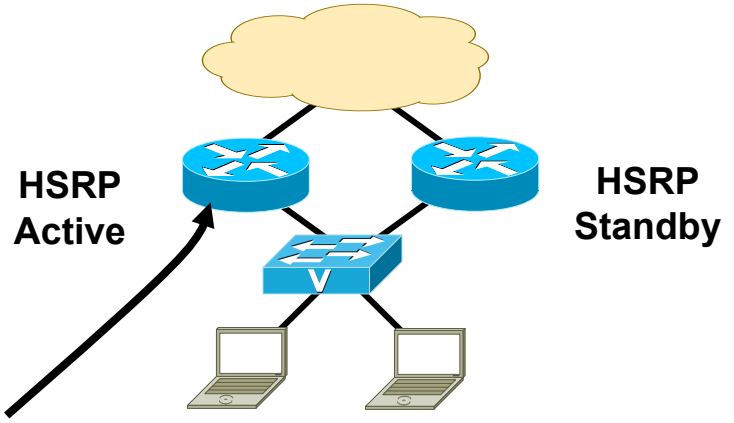
```
Reachable Time              : 6s
Base Reachable Time         : 5s
```



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

HSRP for IPv6

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



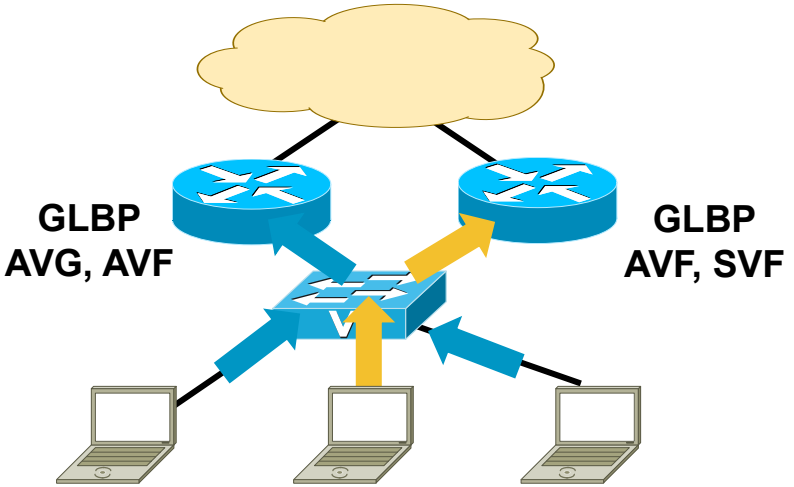

```
interface FastEthernet0/1
 ipv6 address 2001:DB8:66:67::2/64
 ipv6 cef
 standby version 2
 standby 1 ipv6 autoconfig
 standby 1 timers msec 250 msec 800
 standby 1 preempt
 standby 1 preempt delay minimum 180
 standby 1 authentication md5 key-string cisco
 standby 1 track FastEthernet0/0
```

Host with GW of Virtual IP

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

GLBP for IPv6

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

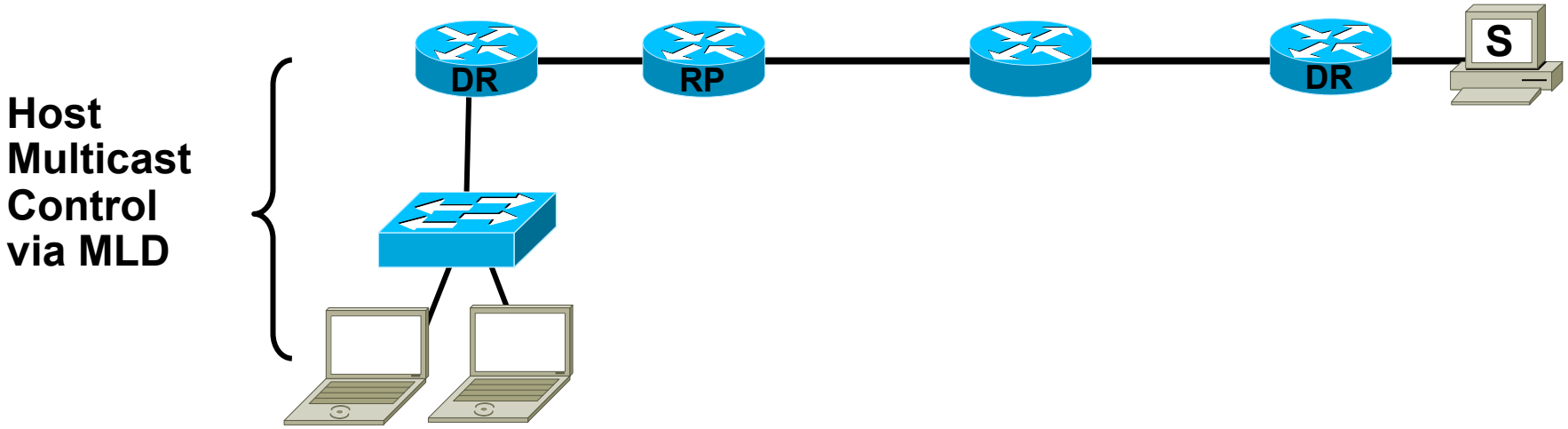



```
interface FastEthernet0/0
 ipv6 address 2001:DB8:1::1/64
 ipv6 cef
 glbp 1 ipv6 autoconfig
 glbp 1 timers msec 250 msec 750
 glbp 1 preempt delay minimum 180
 glbp 1 authentication md5 key-string cisco
```

AVG=Active Virtual Gateway
AVF=Active Virtual Forwarder
SVF=Standby Virtual Forwarder

IPv6 Multicast Availability

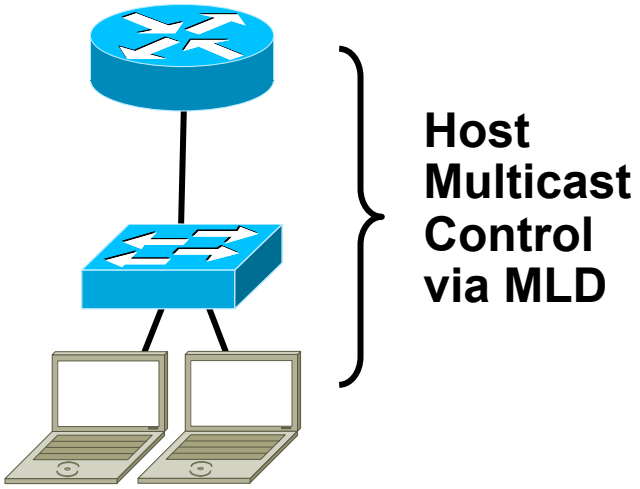
- Multicast Listener Discovery (MLD)
  – Equivalent to IGMP
- PIM Group Modes: Sparse Mode, Bidirectional and Source Specific Multicast
- RP Deployment: Static, Embedded
  – NO Anycast-RP Yet



Multicast Listener Discovery: MLD

Multicast Host Membership Control

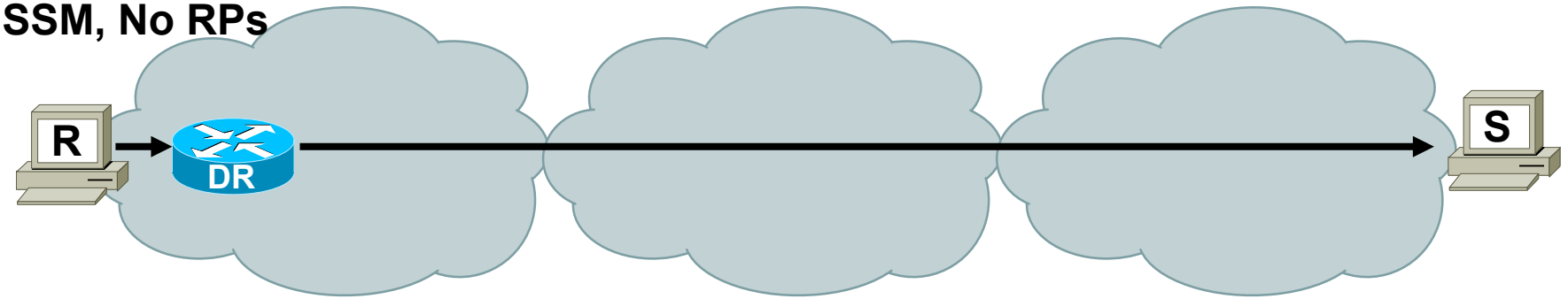
- MLD is equivalent to IGMP in IPv4
- MLD messages are transported over ICMPv6
- MLD uses link local source addresses
- MLD packets use “Router Alert” in extension header (RFC2711)
- Version number confusion:
  - MLDv1 (RFC2710) like IGMPv2 (RFC2236)
  - MLDv2 (RFC3810) like IGMPv3 (RFC3376)
- MLD snooping



Multicast Deployment Options

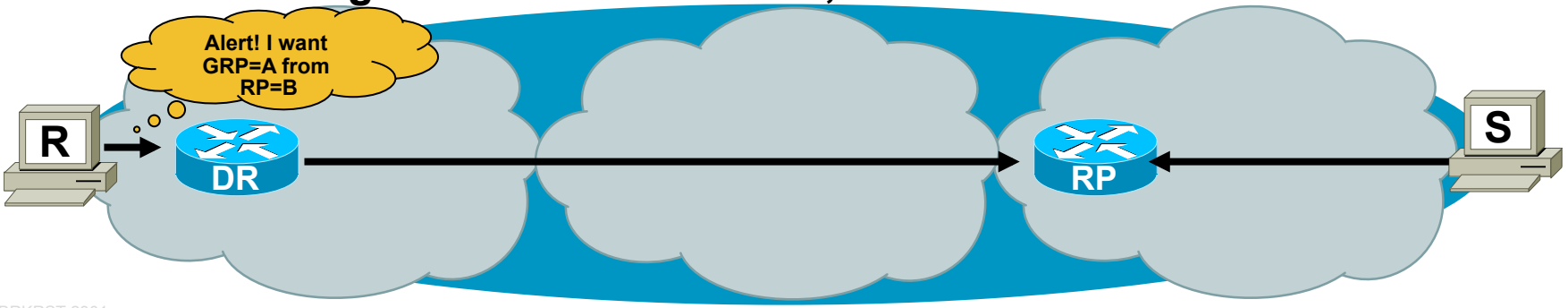
With and Without Rendezvous Points (RP)

SSM, No RPs



ASM Single RP—Static definitions

ASM Across Single Shared PIM Domain, One RP—Embedded-RP



IPv6 QoS: Header Fields

- IPv6 traffic class

  Exactly the same as TOS field in IPv4

- IPv6 Flow Label (RFC 3697)

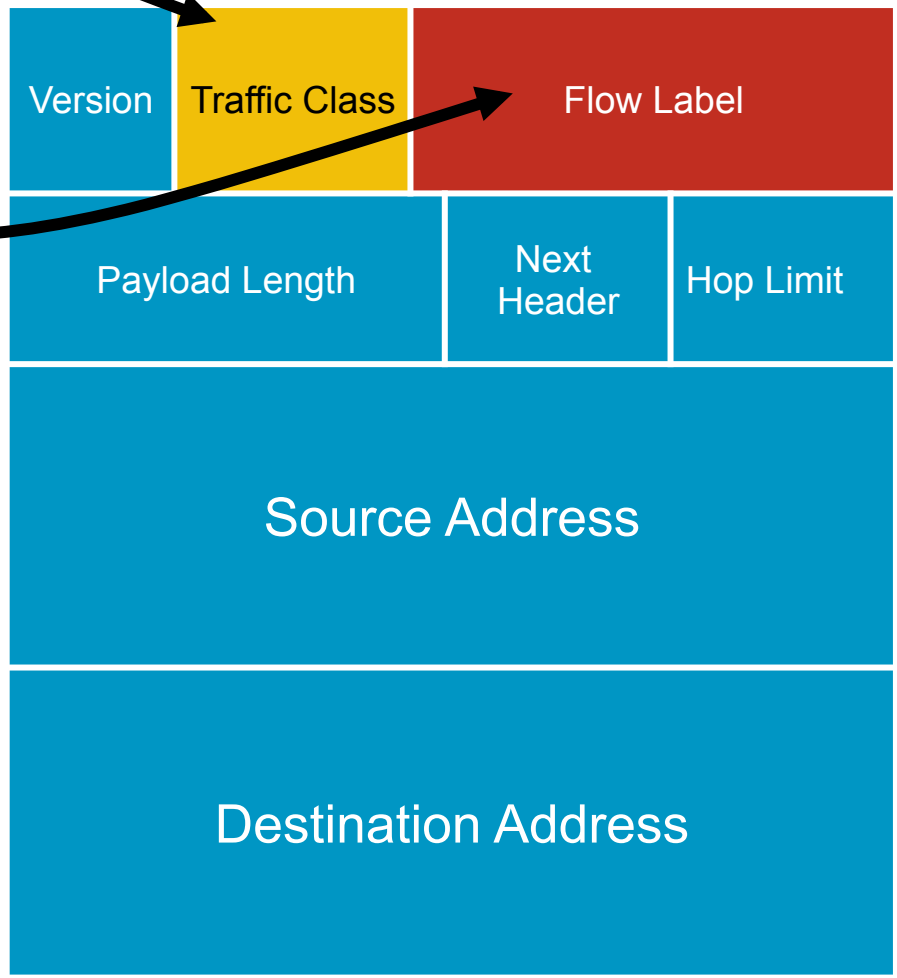
  A new 20-bit field in the IPv6 basic header which:

  Labels packets belonging to particular flows

  Can be used for special sender requests

  Per RFC, Flow Label must not be modified by intermediate routers

- Keep an eye out for work being doing to leverage the flow label



IPv6 QoS Syntax Changes

- IPv4 syntax has used “ip” following match/set statements

  Example: `match ip dscp, set ip dscp`

- Modification in QoS syntax to support IPv6 and IPv4

```
New match criteria
  match dscp – Match DSCP in v4/v6
  match precedence – Match Precedence in v4/v6
New set criteria
  set dscp – Set DSCP in v4/v6
  set precedence – Set Precedence in v4/v6
```

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

  Example—WRED

Scalability and Performance

- IPv6 Neighbor Cache = ARP for IPv4

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

  ARP entry for host in the campus distribution layer:

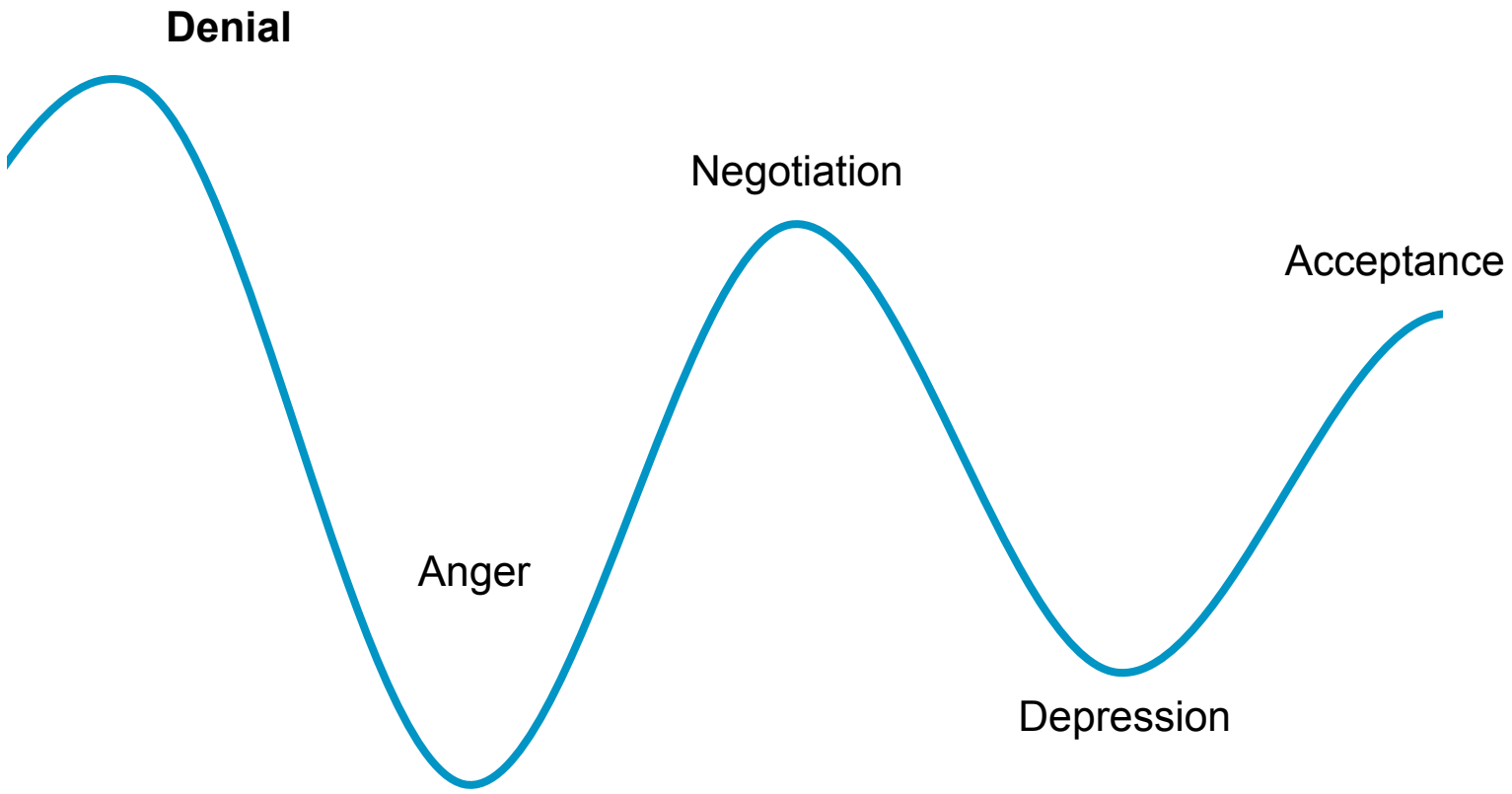
```
Internet  10.120.2.200                    2   000d.6084.2c7a  ARPA  Vlan2
```

  IPv6 Neighbor Cache entry:

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

- Full Internet route tables—ensure to account for TCAM/Memory requirements for both IPv4/IPv6—Not all vendors can properly support both
- Multiple routing protocols—IPv4 and IPv6 will have separate routing protocols. Ensure enough CPU/Memory is present
- Control Plane impact when using tunnels—Terminate ISATAP/configured tunnels in HW platforms when attempting large scale deployments (hundreds/ thousands of tunnels)

IPv4 to IPv6 transition and the stages of grief

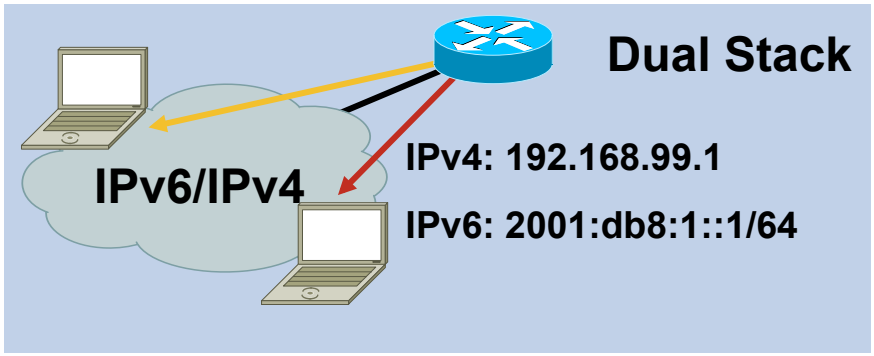


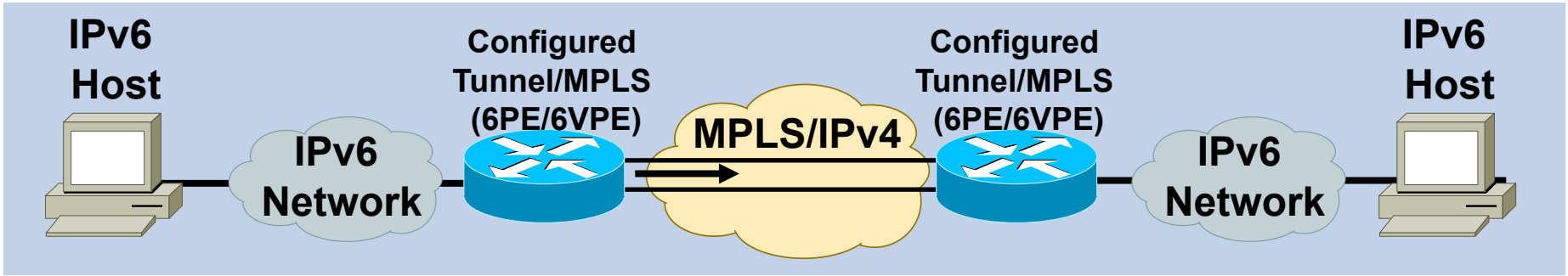
Data

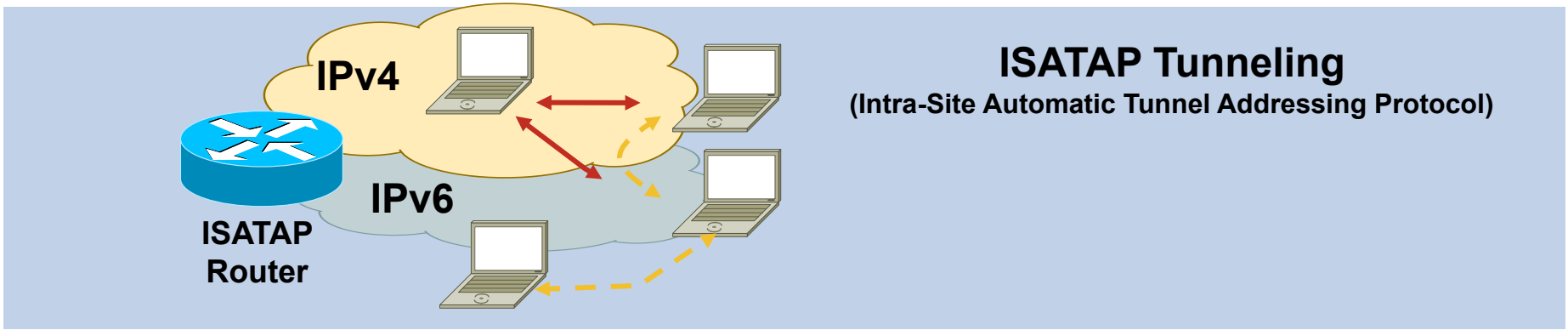
(Infrastructure Deployment)

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 Coexistence







TCP

(Campus/Data Center)

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

ESE Campus Design and Implementation Guides:
http://www.cisco.com/en/US/netsol/ns656/networking_solutions_design_guidances_list.html#anchor2

Campus IPv6 Deployment

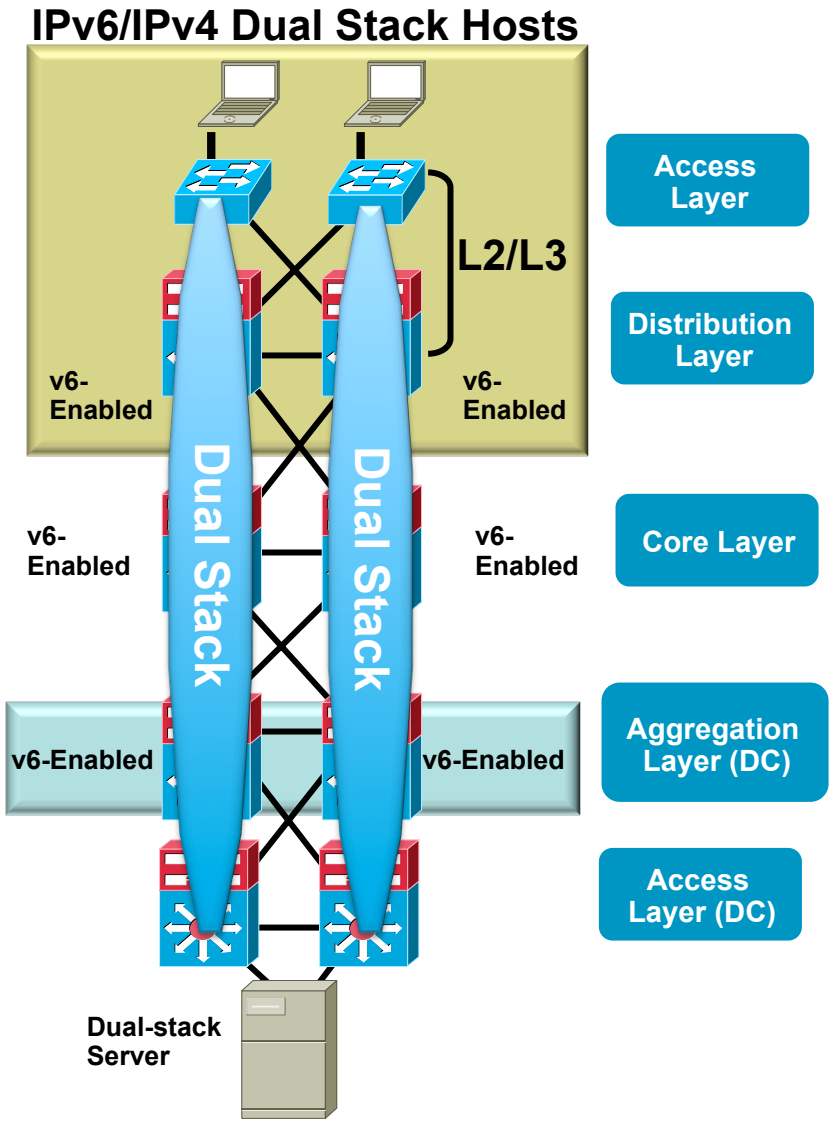
Three Major Options

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

Campus IPv6 Deployment Options

Dual-stack IPv4/IPv6

- #1 requirement - switching/routing platforms must support hardware based forwarding for IPv6
- IPv6 is transparent on L2 switches but…
  - L2 multicast - MLD snooping
  - IPv6 management —Telnet/SSH/HTTP/SNMP
  - Intelligent IP services on WLAN
- Expect to run the same IGPs as with IPv4
- Keep feature expectations simple



Access Layer: Dual Stack (Layer 2 Access)

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

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

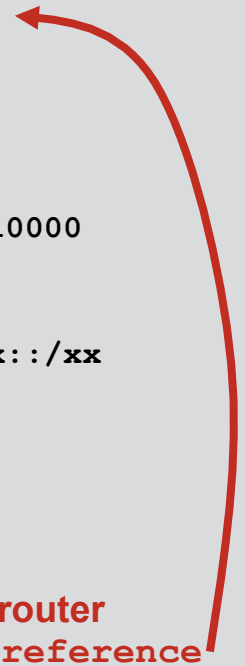
- If using a traditional Layer-2 access design, the only thing that needs to be enabled on the access switch (management/security discussed later) is MLD snooping:

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

Distribution Layer: Dual Stack (Layer 2 Access)

```
ipv6 unicast-routing
ipv6 multicast-routing
ipv6 cef distributed
!
interface GigabitEthernet1/1
 description To 6k-core-right
 ipv6 address 2001:DB8:CAFE:1105::A001:1010/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 ospf network point-to-point
 ipv6 ospf 1 area 0
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
!
interface GigabitEthernet1/2
 description To 6k-core-left
 ipv6 address 2001:DB8:CAFE:1106::A001:1010/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 ospf network point-to-point
 ipv6 ospf 1 area 0
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
```

```
interface Vlan2
 description Data VLAN for Access
 ipv6 address 2001:DB8:CAFE:2::A001:1010/64
 ipv6 nd reachable-time 5000
 ipv6 nd router-preference high
 no ipv6 redirects
 ipv6 ospf 1 area 1
!
ipv6 router ospf 1
 auto-cost reference-bandwidth 10000
 router-id 10.122.0.25
 log-adjacency-changes
 area 2 range 2001:DB8:CAFE:xxxx::/xx
 timers spf 1 5
```



May optionally configure default router preference—`ipv6 nd router-preference {high | medium | low}`—12.2(33)SXG

Access Layer: Dual Stack (Routed Access)

```
ipv6 unicast-routing
ipv6 cef
!
interface GigabitEthernet1/0/25
 description To 6k-dist-1
 ipv6 address 2001:DB8:CAFE:1100::CAC1:3750/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 ospf network point-to-point
 ipv6 ospf 1 area 2
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 cef
!
interface GigabitEthernet1/0/26
 description To 6k-dist-2
 ipv6 address 2001:DB8:CAFE:1101::CAC1:3750/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 ospf network point-to-point
 ipv6 ospf 1 area 2
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 cef
```

```
interface Vlan2
 description Data VLAN for Access
 ipv6 address 2001:DB8:CAFE:2::CAC1:3750/64
 ipv6 ospf 1 area 2
 ipv6 cef
!
ipv6 router ospf 1
 router-id 10.120.2.1
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 area 2 stub no-summary
 passive-interface Vlan2
 timers spf 1 5
```

Distribution Layer: Dual Stack (Routed Access)

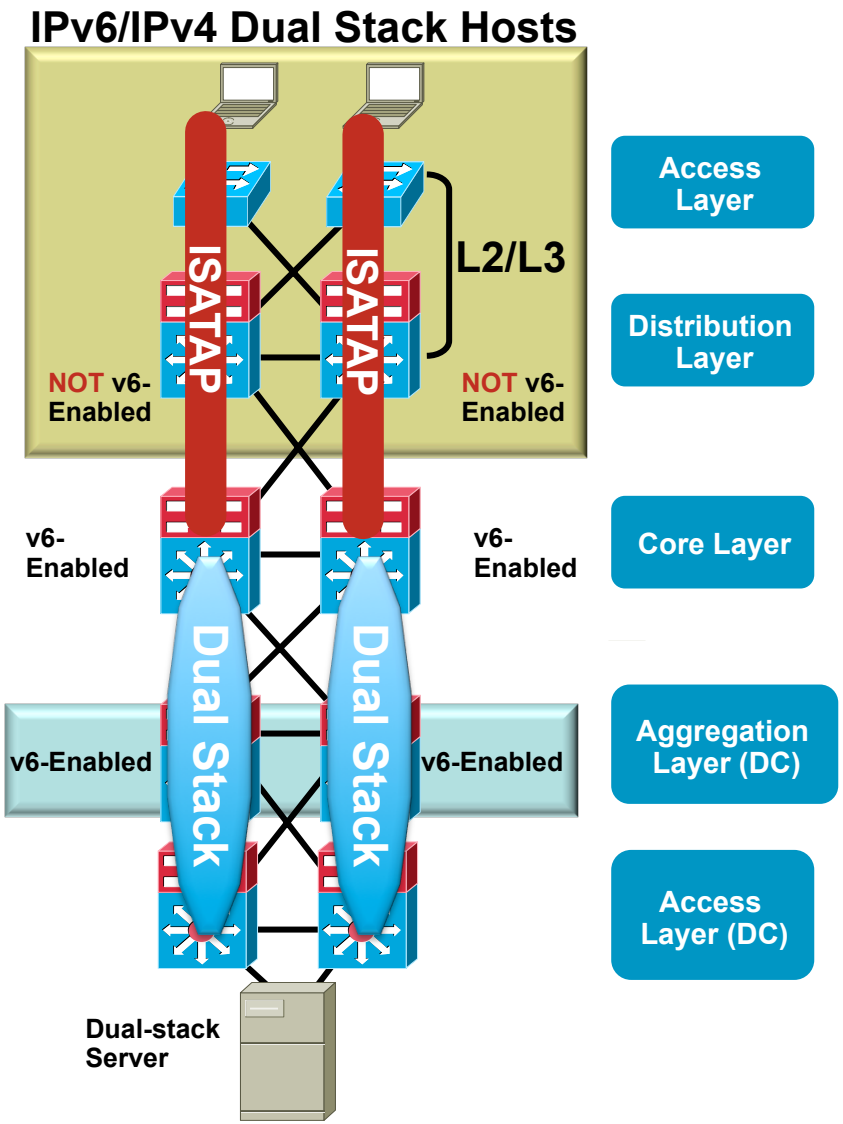
```
ipv6 unicast-routing
ipv6 multicast-routing
ipv6 cef distributed
!
interface GigabitEthernet3/1
 description To 3750-acc-1
 ipv6 address 2001:DB8:CAFE:1100::A001:1010/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 ospf network point-to-point
 ipv6 ospf 1 area 2
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 cef
!
interface GigabitEthernet1/2
 description To 3750-acc-2
 ipv6 address 2001:DB8:CAFE:1103::A001:1010/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 ospf network point-to-point
 ipv6 ospf 1 area 2
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 cef
```

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

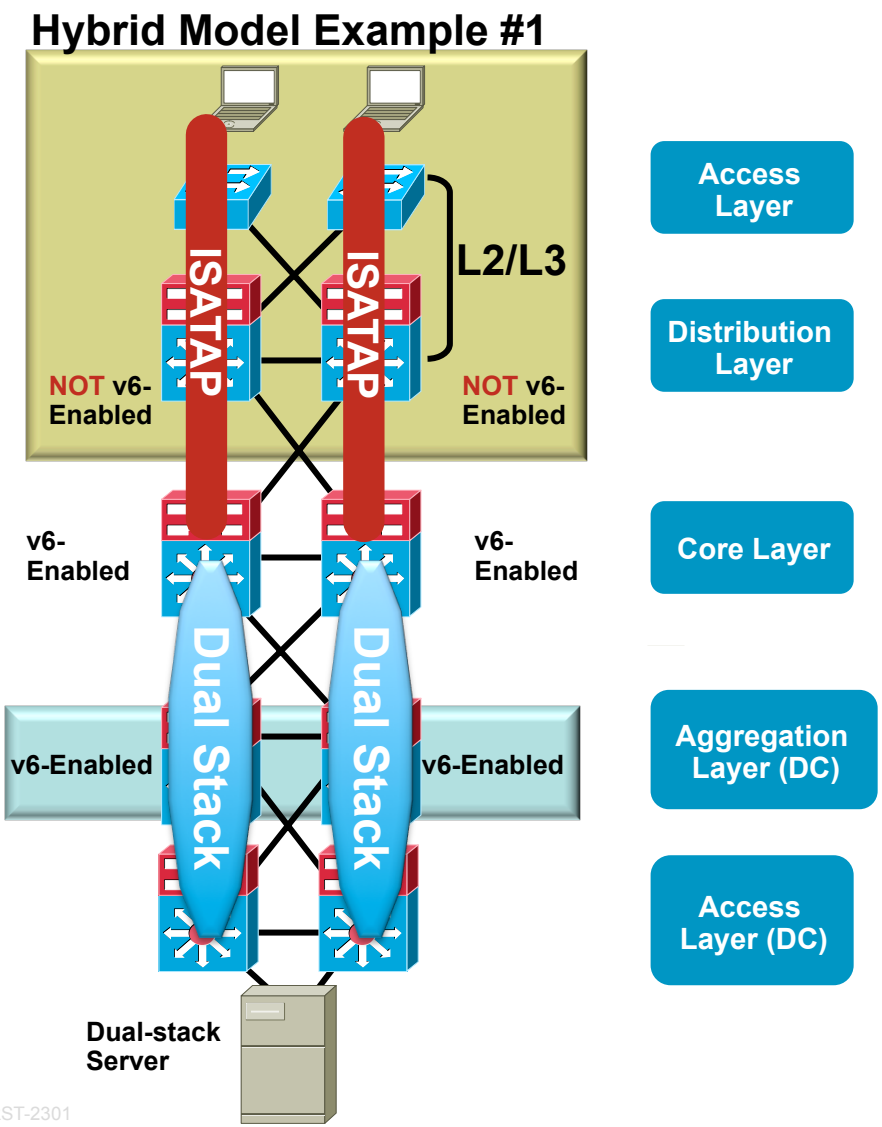
Campus IPv6 Deployment Options

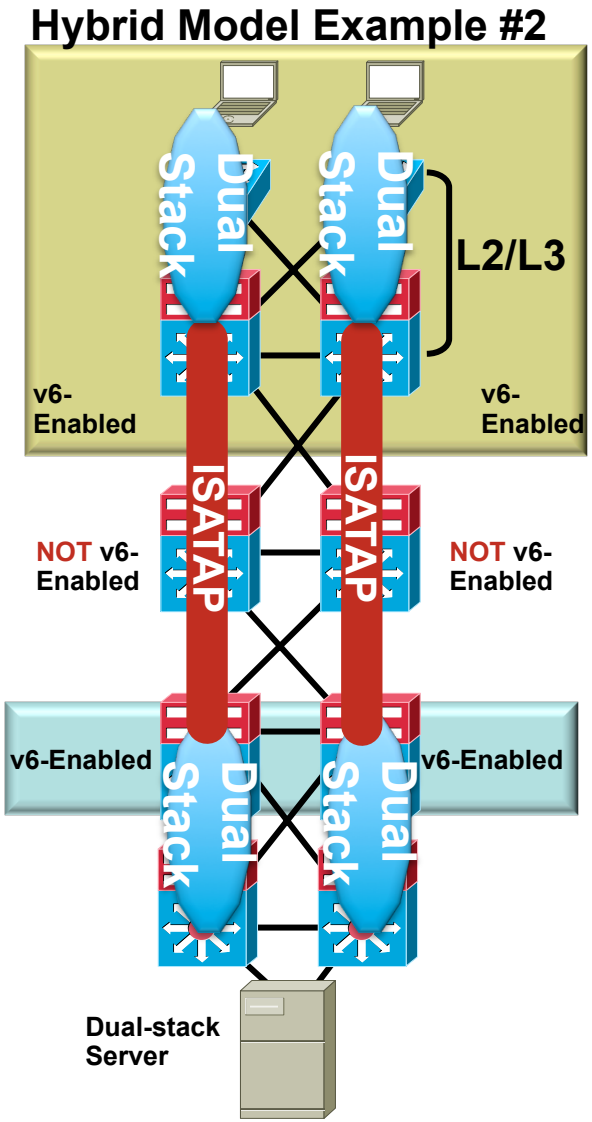
Hybrid Model

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



Hybrid Model Examples





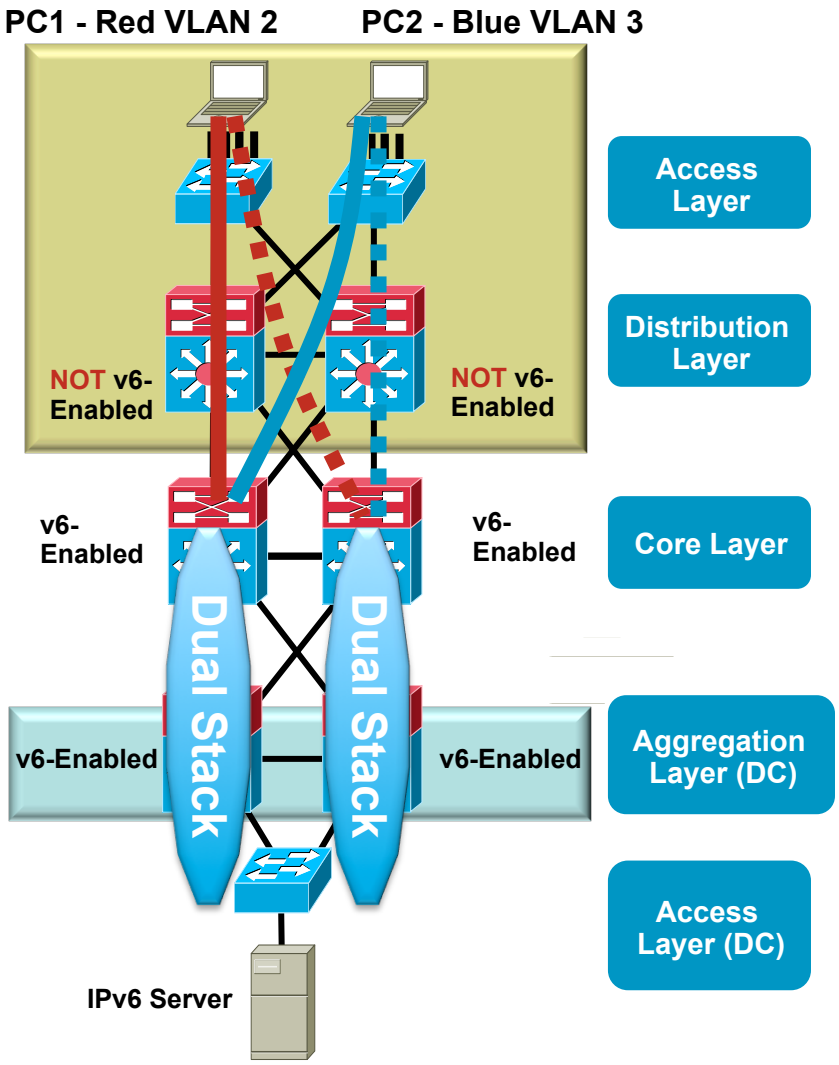
IPv6 ISATAP Implementation

ISATAP Host Considerations

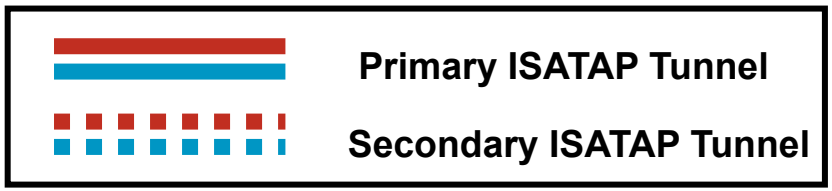
- ISATAP is available on Windows XP, Windows 2003, Vista/Server 2008, port for Linux
- If Windows host does not detect IPv6 capabilities on the physical interface then an effort to use ISATAP is started
- Can learn of ISATAP routers via DNS “A” record lookup “isatap” or via static configuration
  - If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

Highly Available ISATAP Design

Topology



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



IPv6 Campus ISATAP Configuration

Redundant Tunnels

ISATAP Primary

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

ISATAP Secondary

```
interface Tunnel2
 ipv6 address 2001:DB8:CAFE:2::/64 eui-64
 no ipv6 nd suppress-ra
 ipv6 ospf 1 area 2
 ipv6 ospf cost 10
 tunnel source Loopback2
 tunnel mode ipv6ip isatap
!
interface Tunnel3
 ipv6 address 2001:DB8:CAFE:3::/64 eui-64
 no ipv6 nd suppress-ra
 ipv6 ospf 1 area 2
 ipv6 ospf cost 10
 tunnel source Loopback3
 tunnel mode ipv6ip isatap
!
interface Loopback2
 ip address 10.122.10.102 255.255.255.255
 delay 1000
!
interface Loopback3
 ip address 10.122.10.103 255.255.255.255
 delay 1000
```

IPv6 Campus ISATAP Configuration

IPv4 and IPv6 Routing—Options

ISATAP Secondary—Bandwidth adjustment

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

ISATAP Primary—Longest-match adjustment

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

ISATAP Secondary—Longest-match adjustment

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

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

IPv4—EIGRP

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

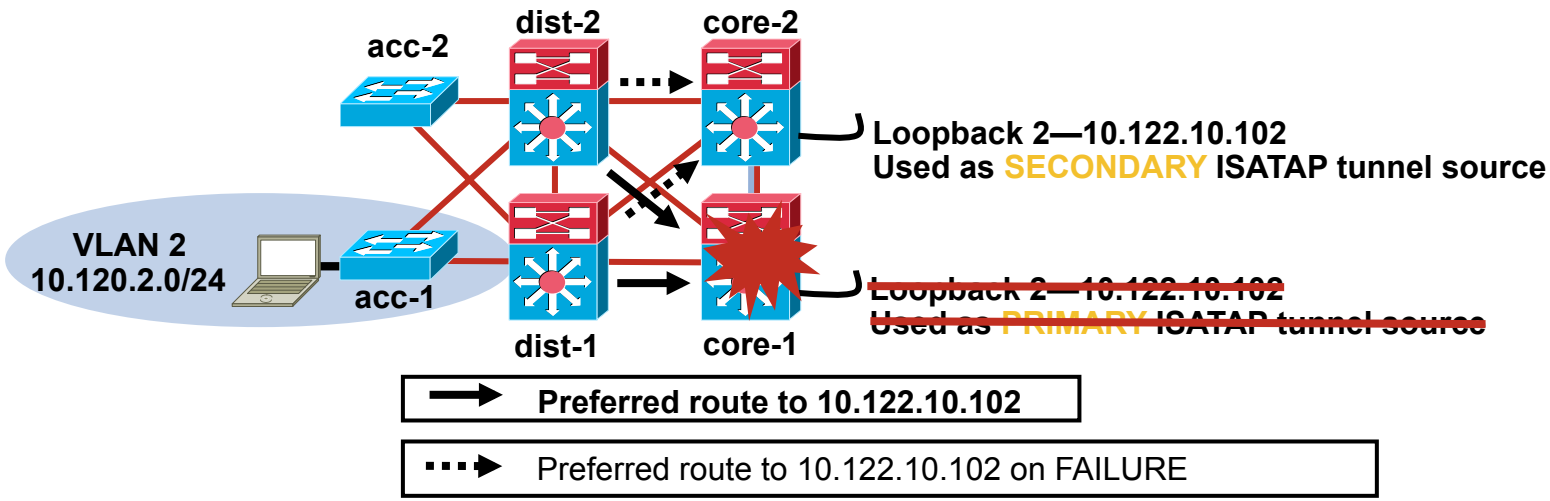
IPv6—OSPFv3

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

Set RID to ensure redundant loopback addresses do not cause duplicate RID issues

Distribution Layer Routes

Primary/Secondary Paths to ISATAP Tunnel Sources



Before Failure

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

After Failure

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

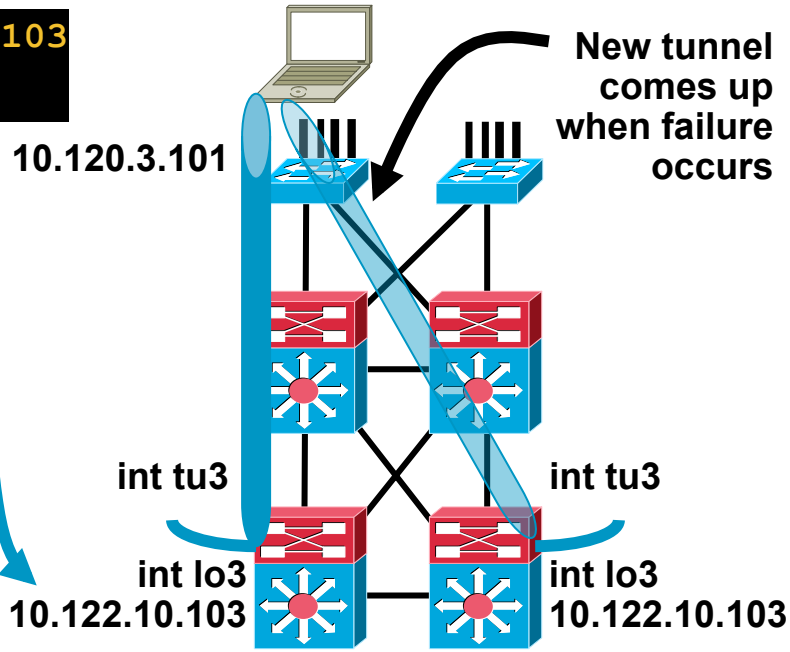
IPv6 Campus ISATAP Configuration

ISATAP Client Configuration

Windows XP/Vista Host

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

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

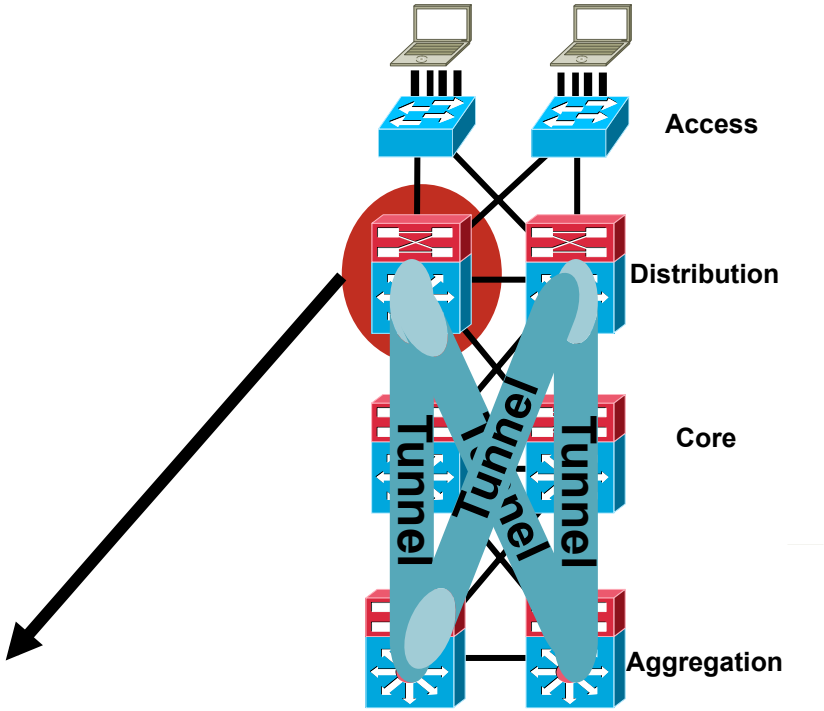



```
Tunnel adapter Automatic Tunneling Pseudo-Interface:
Connection-specific DNS Suffix  . :
IP Address. . . . . . . . . . . . : 2001:db8:cafe:3:0:5efe:10.120.3.101
IP Address. . . . . . . . . . . . : fe80::5efe:10.120.3.101%2
Default Gateway . . . . . . . . . : fe80::5efe:10.122.10.103%2
```

IPv6 Configured Tunnels

Think GRE or IP-in-IP Tunnels

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

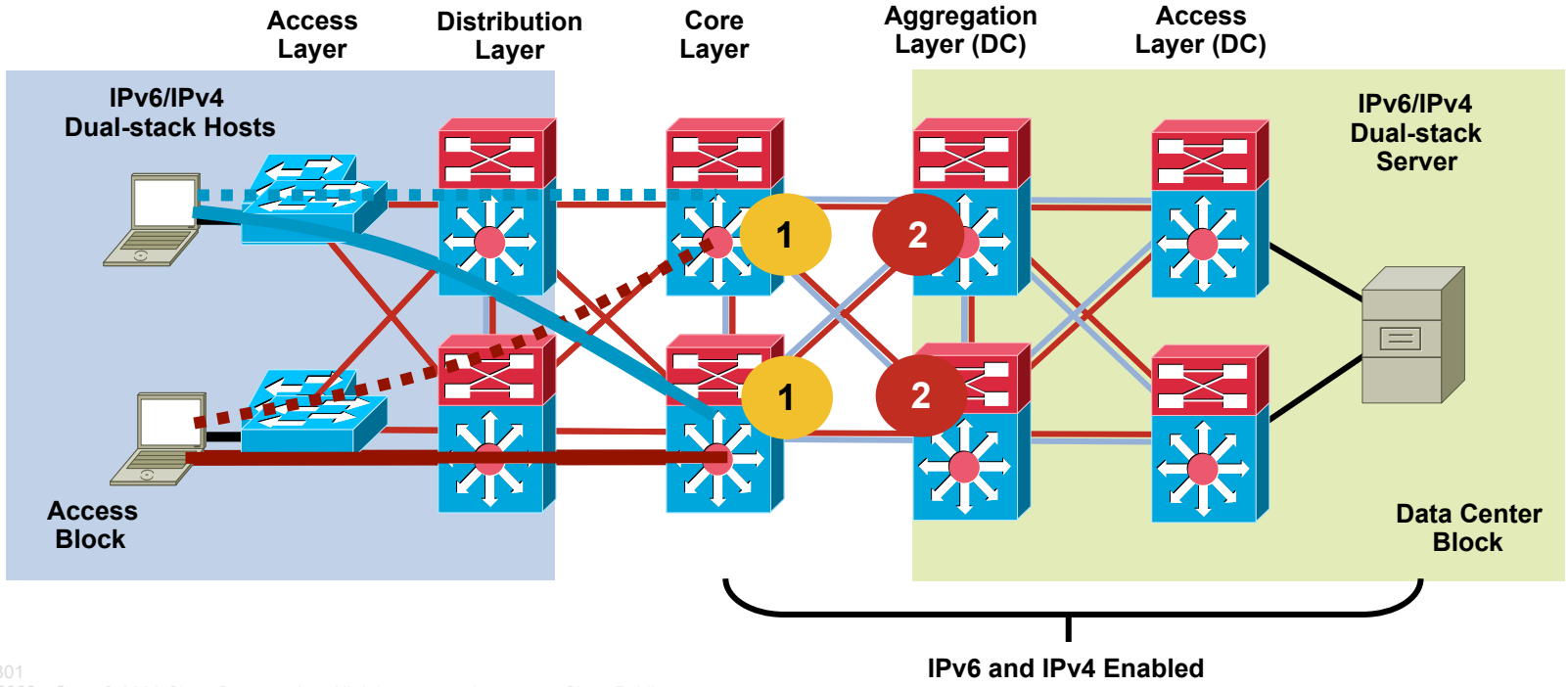



```
interface Tunnel0
 ipv6 cef
 ipv6 address 2001:DB8:CAFE:13::1/127
 ipv6 ospf 1 area 0
 tunnel source Loopback3
 tunnel destination 172.16.2.1
 tunnel mode ipv6ip
```

```
interface GigabitEthernet1/1
 ipv6 address 2001:DB8:CAFE:13::4/127
 ipv6 ospf 1 area 0
 ipv6 cef
!
interface Loopback3
 ip address 172.16.1.1 255.255.255.252
```

Campus Hybrid Model 1
QoS

1. Classification and marking of IPv6 is done on the egress interfaces on the core layer switches because packets have been tunneled until this point - QoS policies for classification and marking cannot be applied to the ISATAP tunnels on ingress
2. The classified and marked IPv6 packets can now be examined by upstream switches (e.g. aggregation layer switches) and the appropriate QoS policies can be applied on ingress. These polices may include trust (ingress), policing (ingress) and queuing (egress).



Campus Hybrid Model 1

QoS Configuration Sample—Core Layer

```
mls qos
!
class-map match-all CAMPUS-BULK-DATA
  match access-group name BULK-APPS
class-map match-all CAMPUS-TRANSACTIONAL-DATA
  match access-group name TRANSACTIONAL-APPS
!
policy-map IPv6-ISATAP-MARK
  class CAMPUS-BULK-DATA
   set dscp af11
  class CAMPUS-TRANSACTIONAL-DATA
   set dscp af21
  class class-default
   set dscp default
!
ipv6 access-list BULK-APPS
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
!
ipv6 access-list TRANSACTIONAL-APPS
 permit tcp any any eq telnet
 permit tcp any any eq 22
```

```
ipv6 access-list BULK-APPS
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
!
ipv6 access-list TRANSACTIONAL-APPS
 permit tcp any any eq telnet
 permit tcp any any eq 22
!
interface GigabitEthernet2/1
 description to 6k-agg-1
 mls qos trust dscp
 service-policy output IPv6-ISATAP-MARK
!
interface GigabitEthernet2/2
 description to 6k-agg-2
 mls qos trust dscp
 service-policy output IPv6-ISATAP-MARK
!
interface GigabitEthernet2/3
 description to 6k-core-1
 mls qos trust dscp
 service-policy output IPv6-ISATAP-MARK
```

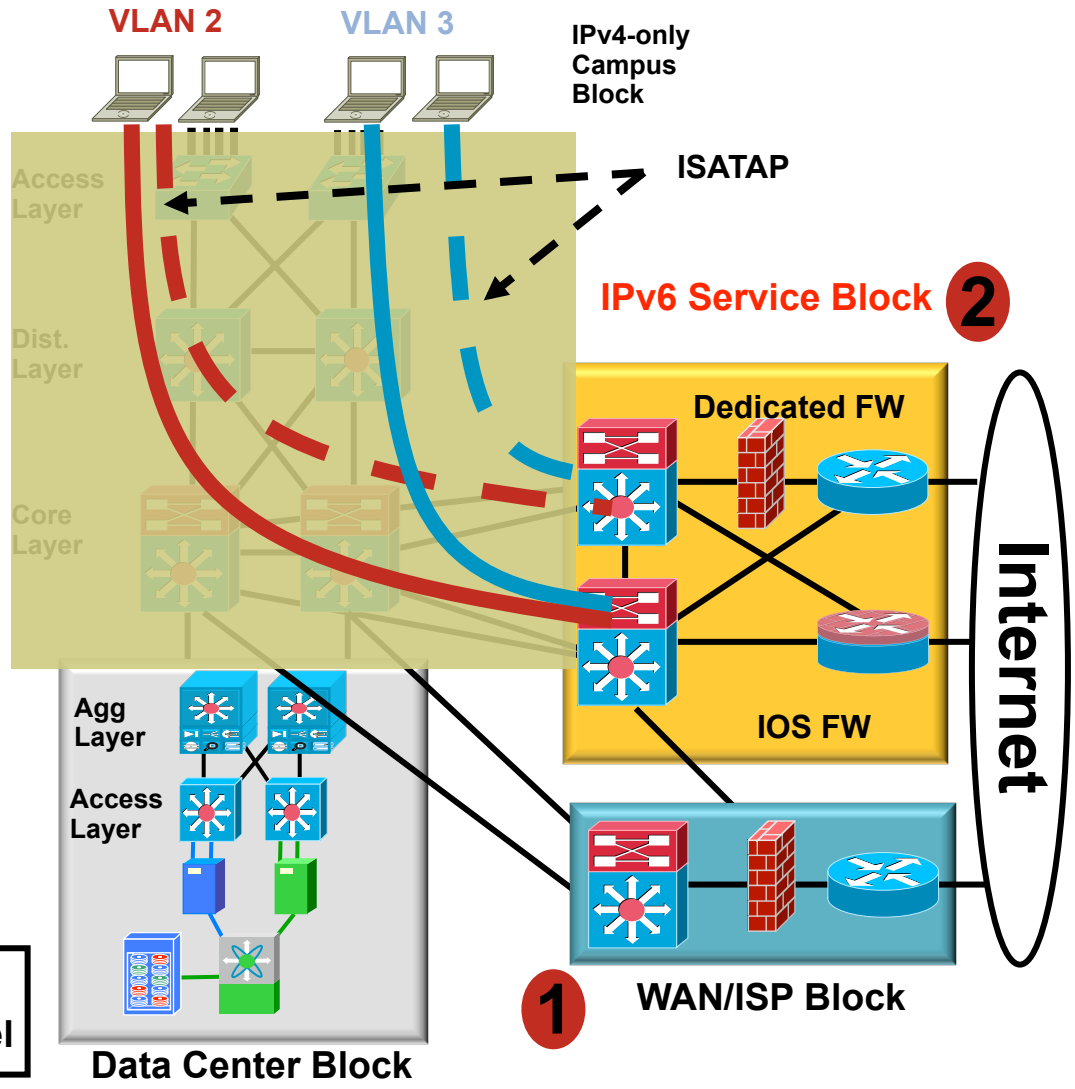
Campus IPv6 Deployment Options

IPv6 Service Block – An Interim Approach

- Provides ability to rapidly deploy IPv6 services without touching existing network
- Provides tight control of where IPv6 is deployed and where the traffic flows (maintain separation of groups/locations)
- Offers the same advantages as Hybrid Model without the alteration to existing code/configurations
- Configurations are very similar to the Hybrid Model

  ISATAP tunnels from PCs in Access layer to Service Block switches (instead of core layer – Hybrid)

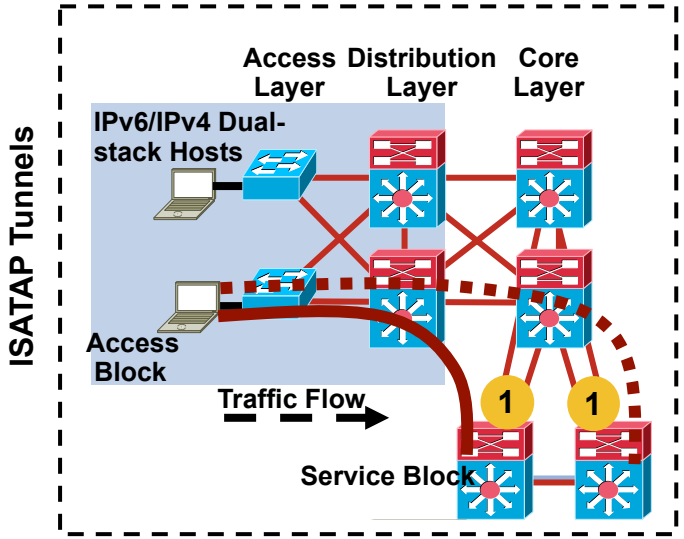
- 1) Leverage existing ISP block for both IPv4 and IPv6 access
- 2) Use dedicated ISP connection just for IPv6 – Can use IOS FW or PIX/ASA appliance

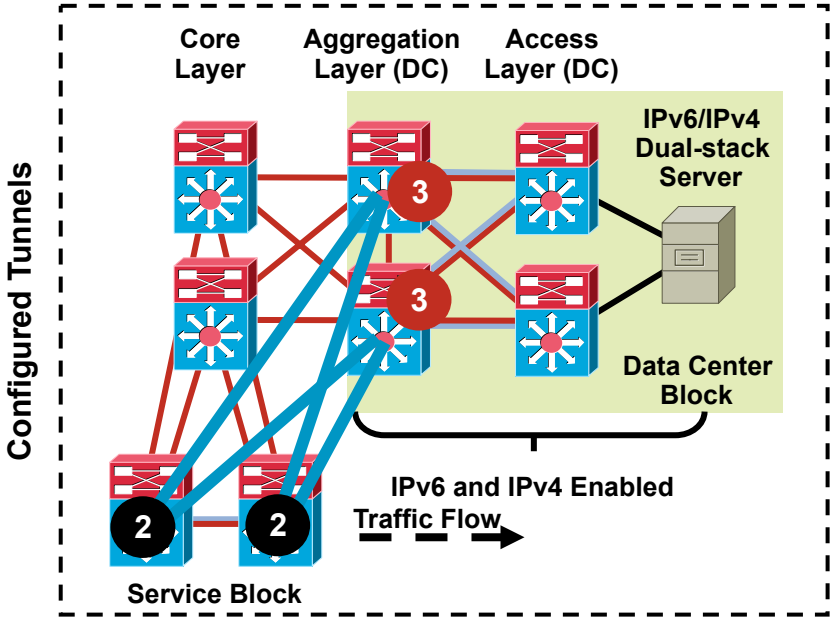


Campus Service Block

QoS From Access Layer

1. Same policy design as Hybrid Model—The first place to implement classification and marking from the access layer is after decapsulation (ISATAP) which is on the egress interfaces on the Service Block switches
2. IPv6 packets received from ISATAP interfaces will have egress policies (classification/marking) applied on the configured tunnel interfaces
3. Aggregation/Access switches can apply egress/ingress policies (trust, policing, queuing) to IPv6 packets headed for DC services





ISATAP Scalability Testing Result

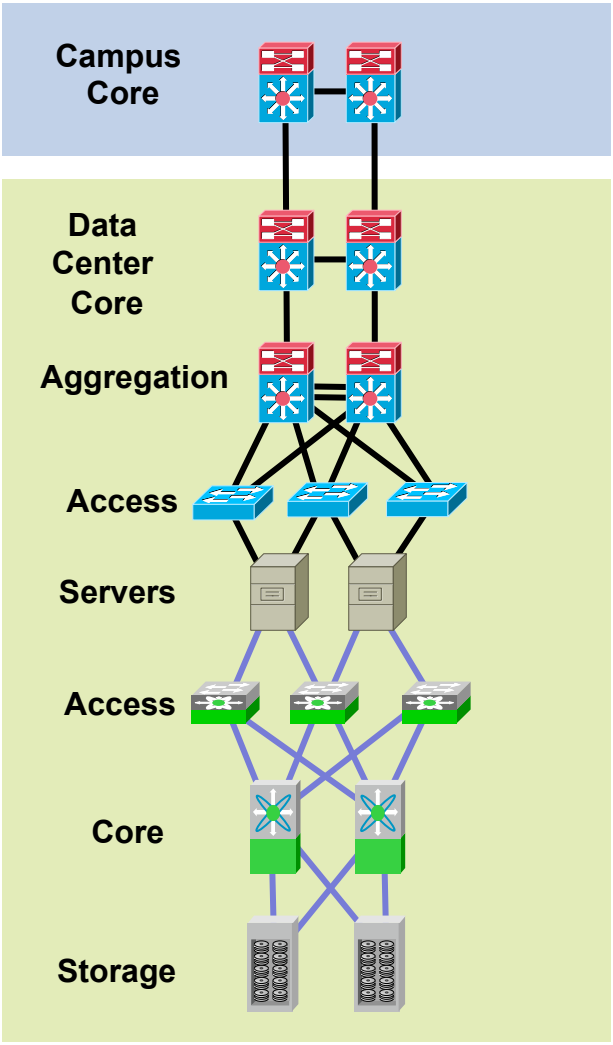
- CPU and memory utilization during scale of ISATAP tunnels

# of Tunnels	1 min. CPU %		Free Memory
	Before	After	
100 tunnel	2	2	845246288
200 tunnel	2	2	839256168
500 tunnel	2	4	8278904

- Traffic convergence for each tunnel

# of Tunnel	Convergence for upstream (ms)		Convergence for downstream (ms)		Convergence for Recovery (ms)	
	Client to Server	Avg. Client to Server	Server to Client	Avg. Server to Client	upstream	downstream
100 tunnel	**208~369**	**350**	**353~532**	**443**	**0**	**0**
500 tunnel	**365~780**	**603**	**389~1261**	**828**	**0~33**	**11~43**

IPv6 Data Center Integration



- The single most overlooked and, potentially, complicated area for IPv6 deployment
- Front-end design will be similar to Campus based on feature, platform and connectivity similarities
- IPv6 for SAN is supported in SAN-OS 3.0
- Major issue in DC with IPv6 today—NIC Teaming (missing in some NIC/Server vendor implementations)
- Watch status of IPv6 support from App, Grid, DB vendors, DC management
  - Get granular—e.g. iLO
  - Impact on clusters—Microsoft Server 2008 failover clusters fully support IPv6 (and L3)
- Your favorite appliance/module may not be ready today

Cisco IPv6 Storage Networking

SAN-OS 3.x

Core (Host Implementation)

- IPv6 (RFC 2460)
- ICMPv6 (RFC 2463)
- Neighbor Discovery (RFC 2461)
- Stateless Auto-configuration
- VRRP for IPv6 for application redundancy (IETF Draft)

Applications and Mgmt

- Telnet, TFTP, FTP, SCP, DNS Resolver, HTTP, Ping, Traceroute, SSH
- Cisco IP, IP-Forwarding and VRRP MIBs
- SNMP over IPv6

Security

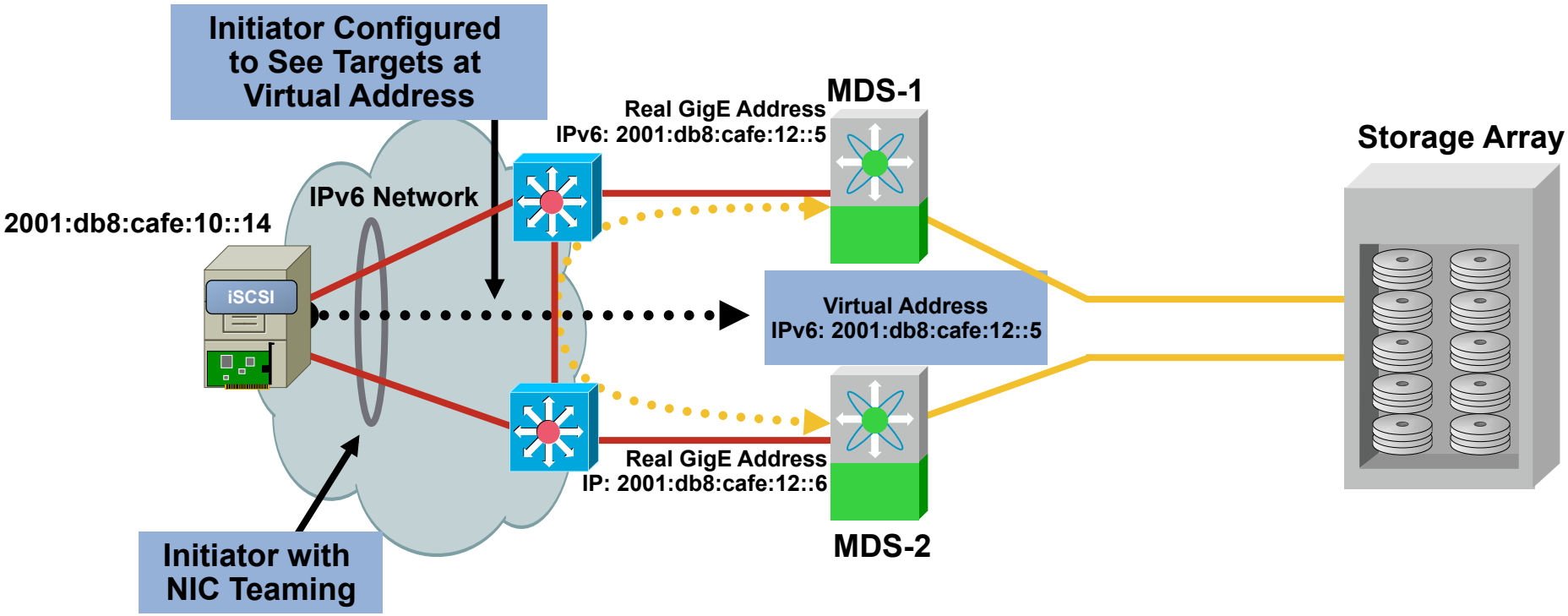
- IPv6 Access Control lists
- IPv6 IPsec (3.2)

SAN Applications

- IP Storage—iSCSI, ISNS, and FCIP
- Zone Server, FC Name Server
- IPv6 over FC
- Other modules—eg. NTP, fc-tunnel etc.

MDS 9500 Family

iSCSI/VRRP for IPv6



- Same configuration requirements and operation as with IPv4
- Can use automatic preemption—configure VR address to be the same as physical interface of “primary”
- Host-side HA uses NIC teaming (see slides for NIC teaming)
- SAN-OS 3.2 will support iSCSI with IPsec

iSCSI IPv6 Example—MDS

Initiator/Target

```
iscsi virtual-target name iscsi-atto-target
  pWWN 21:00:00:10:86:10:46:9c
  initiator iqn.1991-05.com.microsoft:w2k8-svr-01.cisco.com permit
iscsi initiator name iqn.1991-05.com.microsoft:w2k8-svr-01.cisco.com
  static pWWN 24:01:00:0d:ec:24:7c:42
  vsan 1
zone default-zone permit vsan 1
zone name iscsi-zone vsan 1
    member symbolic-nodename iqn.1991-05.com.microsoft:w2k8-svr-01.cisco.com
    member pwwn 21:00:00:10:86:10:46:9c
    member pwwn 24:01:00:0d:ec:24:7c:42
    member symbolic-nodename iscsi-atto-target
zone name Generic vsan 1
    member pwwn 21:00:00:10:86:10:46:9c
zoneset name iscsi_zoneset vsan 1
    member iscsi-zone
zoneset name Generic vsan 1
    member Generic
```

iSCSI/VRRP IPv6 Example—MDS

Interface

MDS-1

```
interface GigabitEthernet2/1
  ipv6 address 2001:db8:cafe:12::5/64
  no shutdown
  vrrp ipv6 1
    address 2001:db8:cafe:12::5
    no shutdown
```

MDS-2

```
interface GigabitEthernet2/1
  ipv6 address 2001:db8:cafe:12::6/64
  no shutdown
  vrrp ipv6 1
    address 2001:db8:cafe:12::5
    no shutdown
```

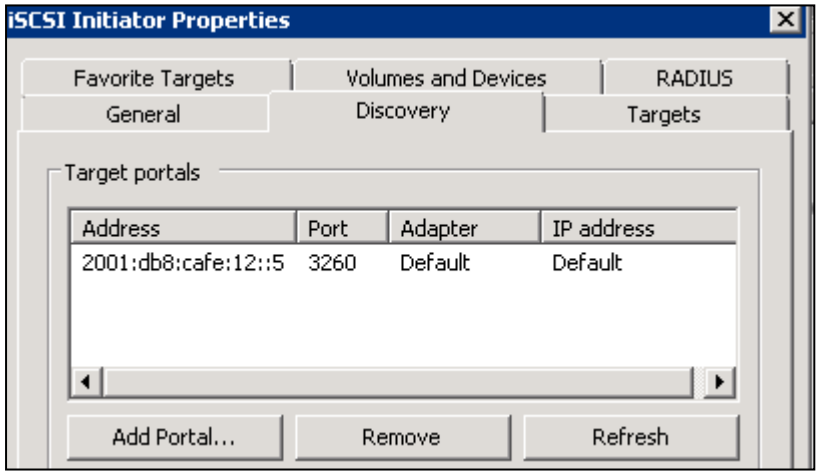
```
mds-1# show vrrp ipv6 vr 1
Interface  VR IpVersion Pri   Time Pre State   VR IP addr
---------------------------------------------------------------------
  GigE2/1   1   IPv6    255  100cs     master  2001:db8:cafe:12::5
```

```
mds-2# show vrrp ipv6 vr 1
Interface  VR IpVersion Pri   Time Pre State   VR IP addr
---------------------------------------------------------------------
  GigE2/1   1   IPv6    100  100cs     backup  2001:db8:cafe:12::5
```

iSCSI Initiator Example—W2K8 IPv6

1

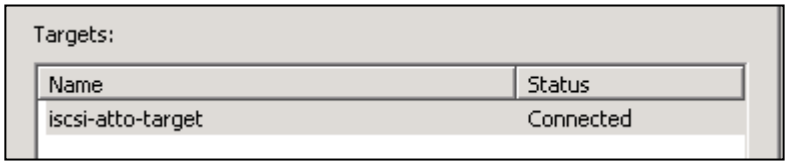
```
iscsi initiator name iqn.1991-05.com.microsoft:w2k8-svr-01.cisco.com
```



2

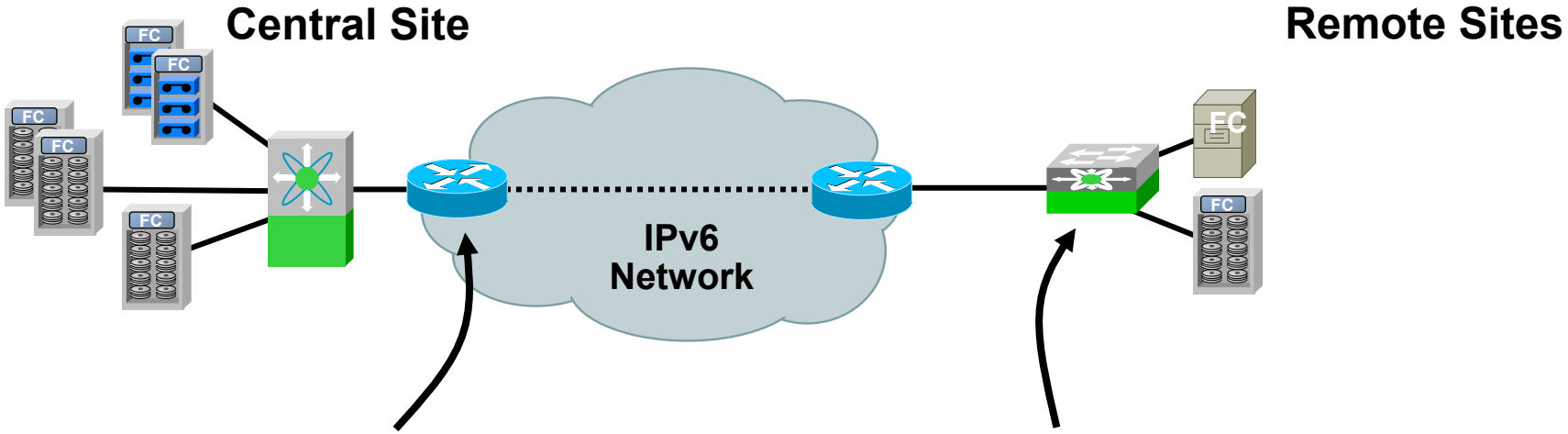
```
interface GigabitEthernet2/1
  ipv6 address 2001:db8:cafe:12::5/64
```

3




```
mds9216-1# show fcns database vsan 1
VSAN 1:
--------------------------------------------------------------------------
FCID      TYPE  PWWN                    (VENDOR)  FC4-TYPE:FEATURE
--------------------------------------------------------------------------
0x670400  N     21:00:00:10:86:10:46:9c           scsi-fcp:target
0x670405  N     24:01:00:0d:ec:24:7c:42 (Cisco)   scsi-fcp:init isc..w
```

SAN-OS 3.x—FCIP(v6)




```
fcip profile 100
  ip address 2001:db8:cafe:50::1
  tcp max-bandwidth-mbps 800 min-available-
bandwidth-mbps 500  round-trip-time-us 84
!
interface fcip100
  use-profile 100
  peer-info ipaddr 2001:db8:cafe:50::2
!
interface GigabitEthernet2/2
  ipv6 address 2001:db8:cafe:50::1/64
```

```
fcip profile 100
  ip address 2001:db8:cafe:50::2
  tcp max-bandwidth-mbps 800 min-available-
bandwidth-mbps 500  round-trip-time-us 84
!
interface fcip100
  use-profile 100
  peer-info ipaddr 2001:db8:cafe:50::1
!
interface GigabitEthernet2/2
  ipv6 address 2001:db8:cafe:50::2/64
```

Data Center NIC Teaming Issue

What Happens if IPv6 is Unsupported?

Auto-configuration

```
Interface 10: Local Area Connection #VIRTUAL TEAM INTERFACE

Addr Type  DAD State  Valid Life   Pref. Life   Address
---------  ---------- ------------ ------------ ----------------------------
Public     Preferred  29d23h58m41s  6d23h58m41 2001:db8:cafe:10:20d:9dff:fe93:b25d
```

Static configuration

```
netsh interface ipv6> add address "Local Area Connection" 2001:db8:cafe:10::7
Ok.

netsh interface ipv6>sh add
Querying active state...
Interface 10: Local Area Connection
Addr Type  DAD State  Valid Life   Pref. Life   Address
---------  ---------- ------------ ------------ ----------------------------
Manual     Duplicate      infinite     infinite 2001:db8:cafe:10::7
Public     Preferred  29d23h59m21s  6d23h59m21s 2001:db8:cafe:10:20d:9dff:fe93:b25d
```

Note: Same Issue Applies to Linux

Intel ANS NIC Teaming for IPv6

- Intel IPv6 NIC Q&A—Product support
- http://www.intel.com/support/network/sb/cs-009090.htm
- Intel now supports IPv6 with Express, ALB, and AFT deployments

  Intel statement of support for RLB—“Receive Load Balancing (RLB) is not supported on IPv6 network connections. If a team has a mix of IPv4 and IPv6 connections, RLB will work on the IPv4 connections but not on the IPv6 connections. All other teaming features will work on the IPv6 connections.”

Interim Hack for Unsupported NICs

- Main issue for NICs with no IPv6 teaming support is DAD—Causes duplicate checks on Team and Physical even though the physical is not used for addressing
- Set DAD on Team interface to “0”—Understand what you are doing ☺
- Microsoft Vista/Server 2008 allows for a command line change to reduce the “DAD transmits” value from 1 to 0

```
netsh interface ipv6 set interface 19 dadtransmits=0
```

- Microsoft Windows 2003—Value is changed via a creation in the registry

```
\\HKLM\System\CurrentControlSet\Services\Tcpip6\Parameters
\Interfaces\(InterfaceGUID)\DupAddrDetectTransmits - Value “0”
```

- Linux

```
# sysctl -w net/ipv6/conf/bond0/dad_transmits=0
net.ipv6.conf.eth0.dad_transmits = 0
```

Intel NIC Teaming—IPv6 (Pre Team)

```
Ethernet adapter Local Area Connection 3:
   Connection-specific DNS Suffix  . :
   Autoconfiguration IP Address. . . : 169.254.25.192
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   IP Address. . . . . . . . . . . . : fe80::204:23ff:fec7:b0d7%11
   Default Gateway . . . . . . . . . : fe80::212:d9ff:fe92:de76%11

Ethernet adapter LAN:
   Connection-specific DNS Suffix  . :
   IP Address. . . . . . . . . . . . : 10.89.4.230
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   IP Address. . . . . . . . . . . . : 2001:db8:cafe:1::2
   IP Address. . . . . . . . . . . . : fe80::204:23ff:fec7:b0d6%12
   Default Gateway . . . . . . . . . : fe80::212:d9ff:fe92:de76%12
```

Intel NIC Teaming—IPv6 (Post Team)

```
Ethernet adapter TEAM-1:
   Connection-specific DNS Suffix  . :
   IP Address. . . . . . . . . . . . : 10.89.4.230
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   IP Address. . . . . . . . . . . . : 2001:db8:cafe:1::2
   IP Address. . . . . . . . . . . . : fe80::204:23ff:fec7:b0d6%13
   Default Gateway . . . . . . . . . : fe80::212:d9ff:fe92:de76%13
```

```
Interface 13: TEAM-1

Addr Type  DAD State  Valid Life   Pref. Life   Address
---------  ---------- ------------ ------------ ----------------------------
Public     Preferred         4m11s        4m11s 2001:db8:cafe:1::2
Link       Preferred      infinite     infinite fe80::204:23ff:fec7:b0d6
```

Data Center—IPv6 on FWSM

Transparent Firewall Mode—Example

```
FWSM Version 3.1(3) <context>
!
firewall transparent
hostname WEBAPP
!
interface inside
 nameif inside
 bridge-group 1
 security-level 100
!
interface outside
 nameif outside
 bridge-group 1
 security-level 0
!
interface BVI1
 ip address 10.121.10.254 255.255.255.0
!
access-list BRIDGE_TRAFFIC ethertype permit bpdu
access-list BRIDGE_TRAFFIC ethertype permit 86dd
!
access-group BRIDGE_TRAFFIC in interface inside
access-group BRIDGE_TRAFFIC in interface outside
```

- Today, IPv6 inspection is supported in the routed firewall mode.
- Transparent mode can allow IPv6 traffic to be bridged (no inspection)

Permit ethertype 0x86dd (IPv6 ethertype)

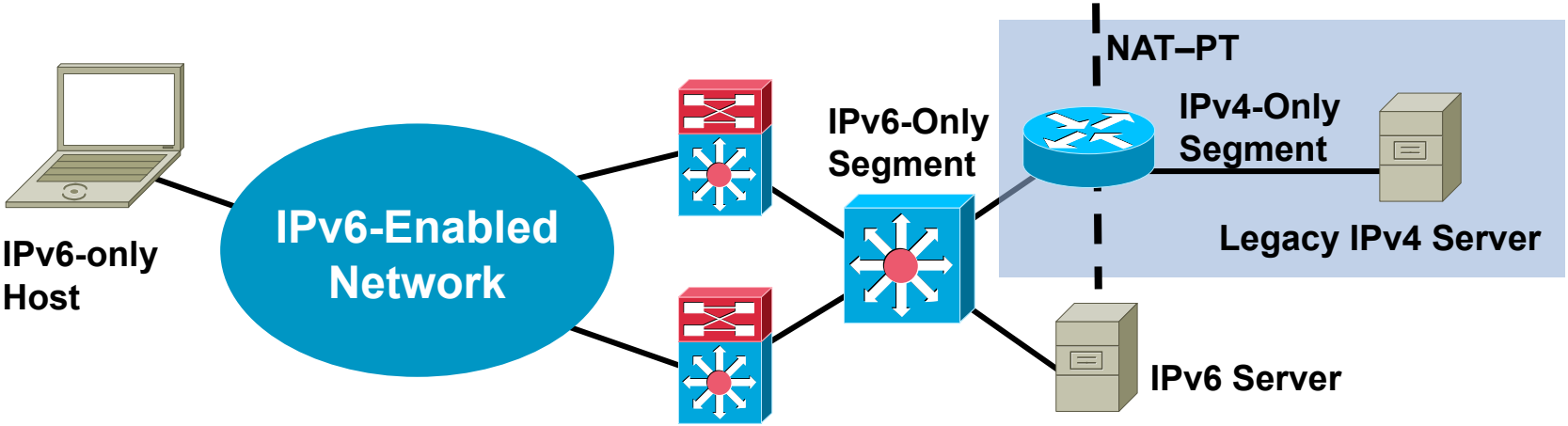
Data Center—IPv6 on FWSM

Routed Firewall Mode—Example

```
FWSM Version 3.1(3) <context>
!
hostname WEBAPP
!
interface inside
 nameif inside
 security-level 100
 ipv6 address 2001:db8:cafe:10::f00d:1/64
!
interface outside
 nameif outside
 security-level 0
 ipv6 address 2001:db8:cafe:101::f00d:1/64
!
ipv6 route outside ::/0 2001:db8:cafe:101::1
ipv6 access-list IPv6_1 permit icmp6 any 2001:db8:cafe:10::/64
ipv6 access-list IPv6_1 permit tcp 2001:db8:cafe:2::/64 host 2001:db8:cafe:10::7 eq www
access-group IPv6_1 in interface outside
```

GW to MSFC outside VLAN intf.

Legacy Services (IPv4 Only)



- There will be many in-house developed applications that will never support IPv6—Move them to a legacy VLAN or server farm
- NAT-PT (Network Address Translation–Protocol Translation) as an option to front-end IPv4-only Server—Note: NAT-PT has been moved to experimental
- Place NAT-PT box as close to IPv4 only server as possible
- Be VERY aware of performance and manageability issues

Still TCP…

(WAN/Branch)

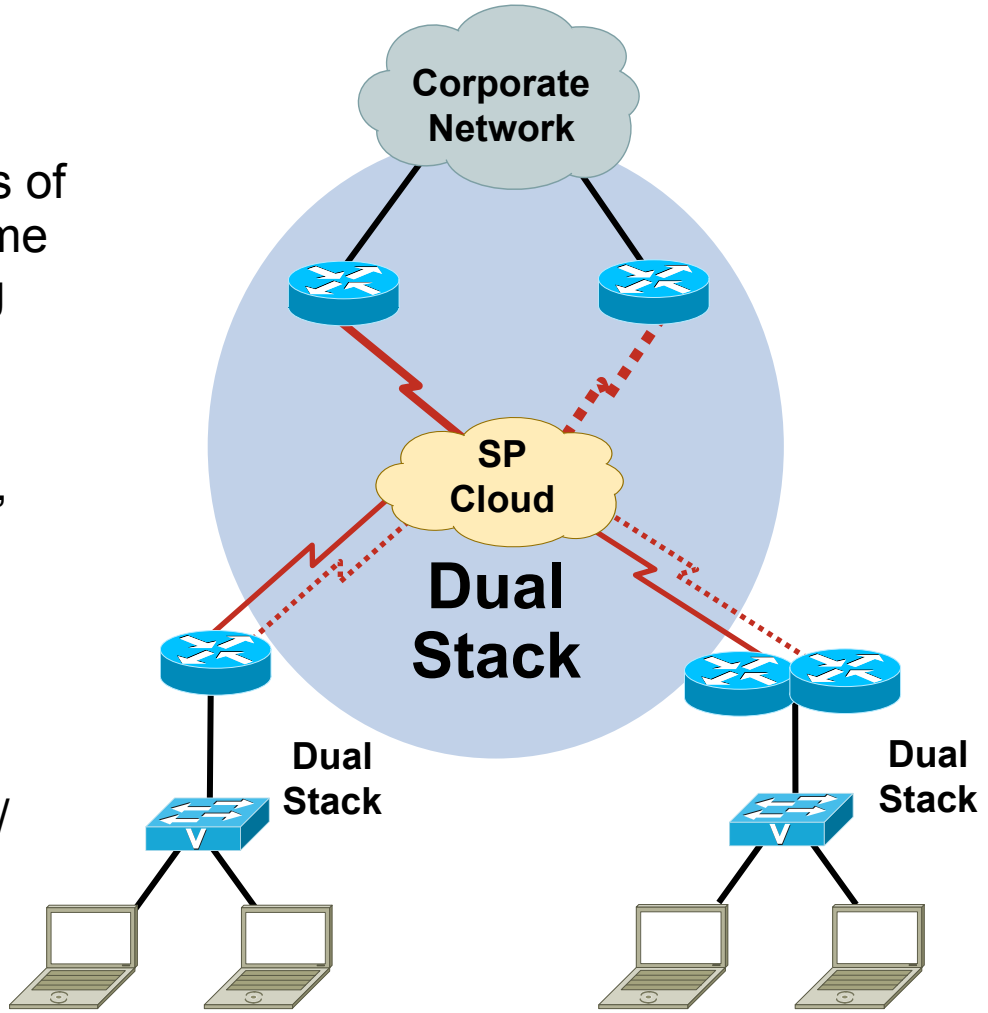
Deploying IPv6 in Branch Networks:
http://www.cisco.com/univercd/cc/td/doc/solution/brchipv6.pdf

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

http://www.cisco.com/en/US/netsol/ns656/networking_solutions_design_guidances_list.html#anchor10

WAN/Branch Deployment

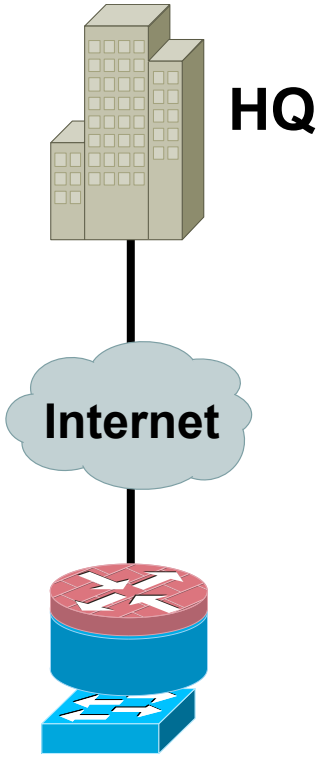
- Cisco routers have supported IPv6 for a long time
- Dual-stack should be the focus of your implementation…but, some situations still call for tunneling
- Support for every media/WAN type you want to use (Frame Relay, leased-line, broadband, MPLS, etc…)
- Don't assume all features for every technology are IPv6-enabled
- Better feature support in WAN/ Branch than in Campus/DC



IPv6 Enabled Branch

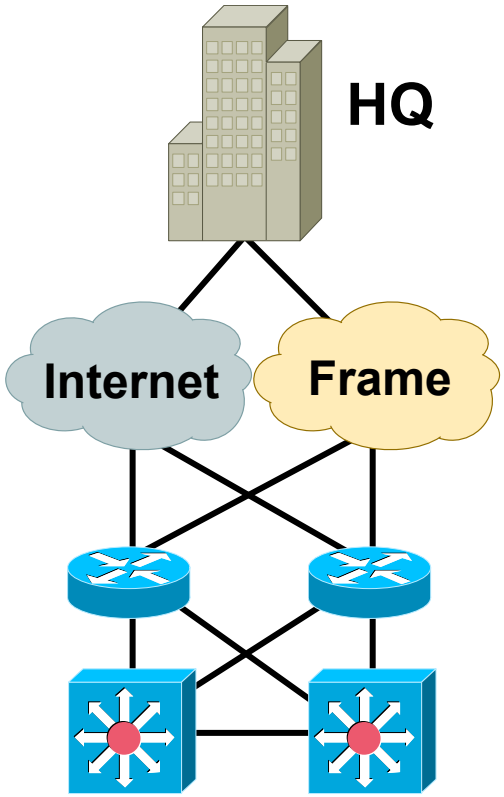
Take Your Pick—Mix-and-Match

Branch Single Tier



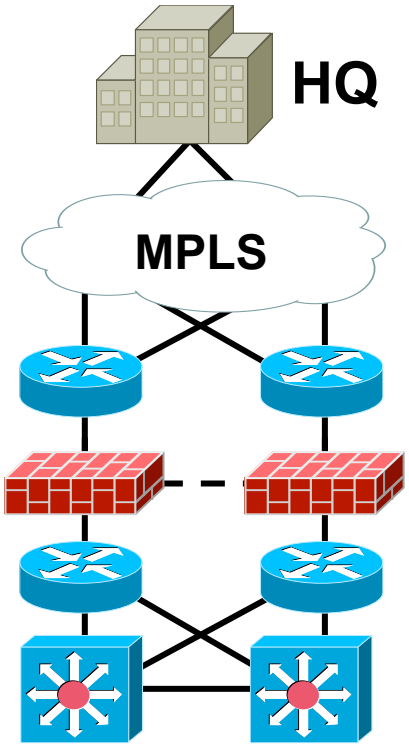
Dual-Stack
IPSec VPN (IPv4/IPv6)
IOS Firewall (IPv4/IPv6)
Integrated Switch
(MLD-snooping)

Branch Dual Tier



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

Branch Multi-Tier



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

DMVPN with IPv6—12.4(20)T Feature

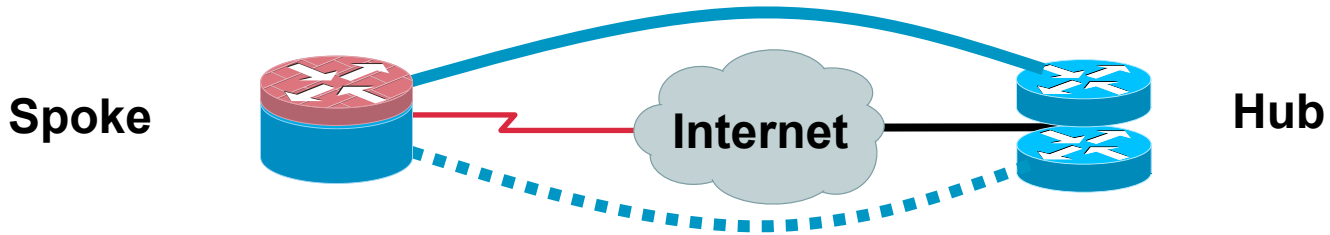
Example Tunnel Configuration

Spoke Router

```
interface Tunnel0
 ipv6 address 2001:DB8:CAFE:1261::2/64
 ipv6 enable
 ipv6 mtu 1400
 ipv6 eigrp 1
 ipv6 nhrp authentication ESE
 ipv6 nhrp map multicast 172.17.1.3
 ipv6 nhrp map 2001:DB8:CAFE:1261::1/128 172.17.1.3
 ipv6 nhrp network-id 100000
 ipv6 nhrp holdtime 600
 ipv6 nhrp nhs 2001:DB8:CAFE:1261::1
 ipv6 nhrp cache non-authoritative
 tunnel source 172.16.1.2
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile SPOKE
```

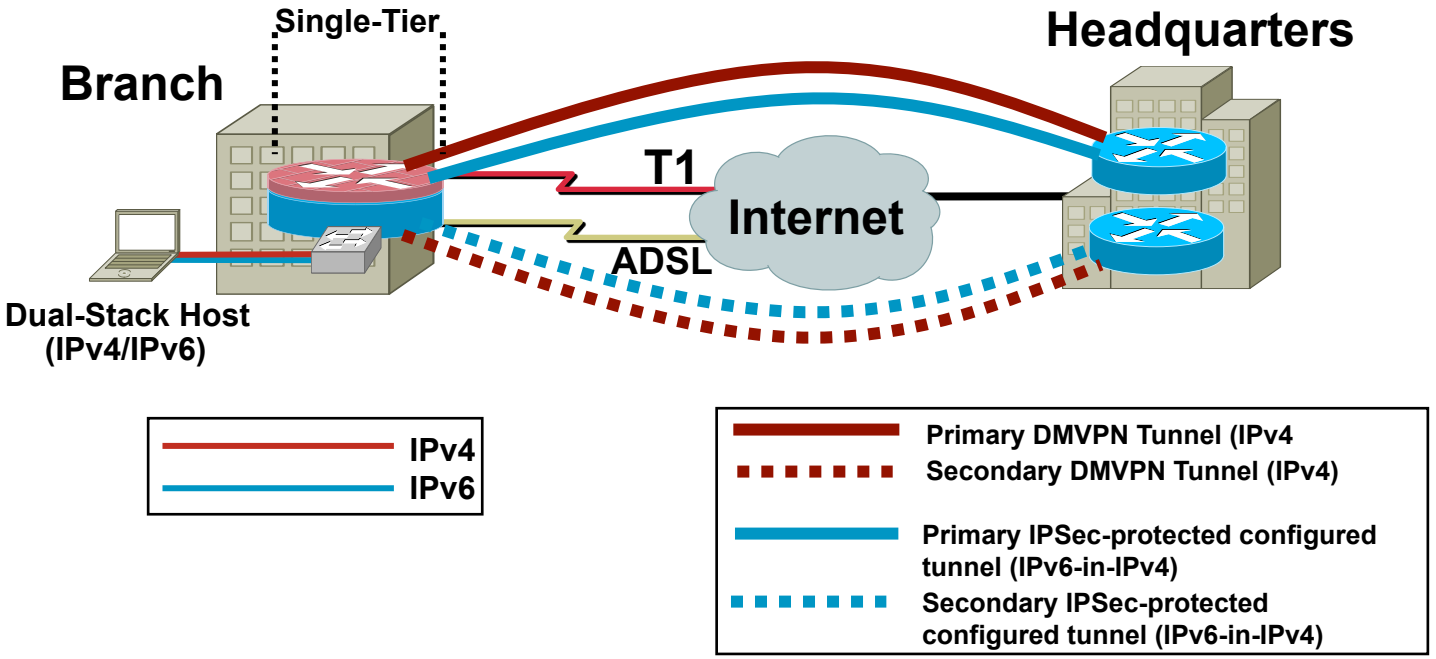
Hub Router

```
interface Tunnel0
 ipv6 address 2001:DB8:CAFE:1261::1/64
 ipv6 enable
 ipv6 mtu 1400
 ipv6 eigrp 1
 no ipv6 split-horizon eigrp 1
 ipv6 hold-time eigrp 1 35
 no ipv6 next-hop-self eigrp 1
 ipv6 nhrp authentication ESE
 ipv6 nhrp map multicast dynamic
 ipv6 nhrp network-id 100000
 ipv6 nhrp holdtime 600
 ipv6 nhrp cache non-authoritative
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile HUB
```



Single-Tier Profile

- Totally integrated solution – Branch router and integrated EtherSwitch module – IOS FW and VPN for IPv6 and IPv4
- When SP does not offer IPv6 services, use IPv4 IPSec VPNs for manually configured tunnels (IPv6-in-IPv4) or DMVPN for IPv6
- When SP does offer IPv6 services, use IPv6 IPSec VPNs (Latest AIM/VAM supports IPv6 IPSec)

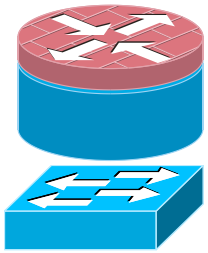


Single-Tier Profile

LAN Configuration

```
ipv6 unicast-routing
ipv6 multicast-routing
ipv6 cef
!
ipv6 dhcp pool DATA_VISTA
 dns-server 2001:DB8:CAFE:10:20D:9DFF:FE93:B25D
 domain-name cisco.com
!
interface GigabitEthernet1/0.100
 description DATA VLAN for Computers
 encapsulation dot1Q 100
 ipv6 address 2001:DB8:CAFE:1100::BAD1:A001/64
 ipv6 nd other-config-flag
 ipv6 dhcp server DATA_VISTA
```

Router



Obtain “other” info

Enable DHCP

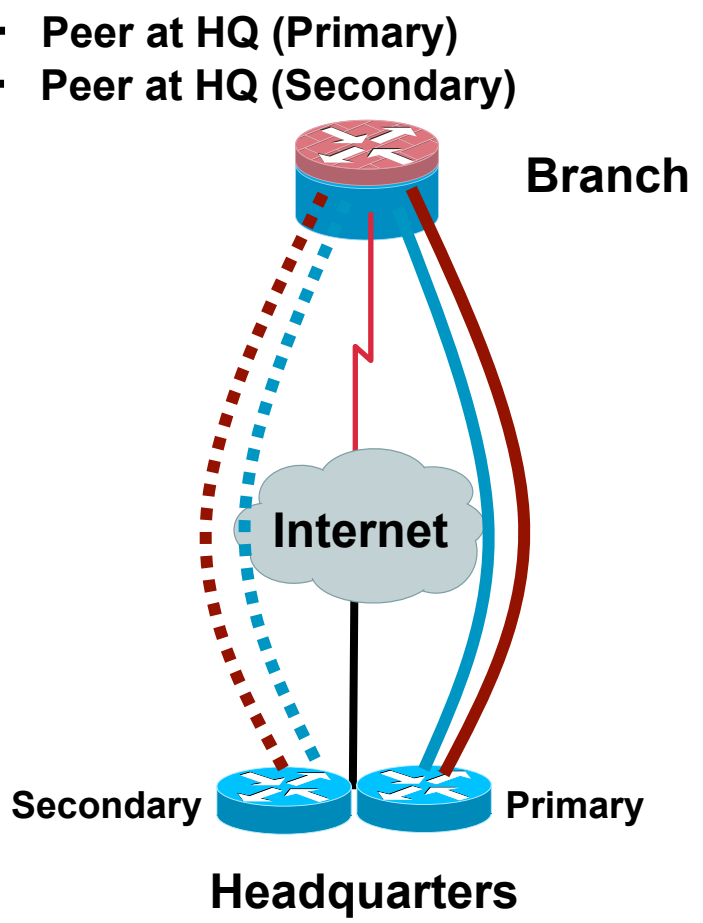
```
ipv6 mld snooping
!
interface Vlan100
 description VLAN100 for PCs and Switch management
 ipv6 address 2001:DB8:CAFE:1100::BAD2:F126/64
```

EtherSwitch Module

Single-Tier Profile

IPSec Configuration—1

```
crypto isakmp policy 1
 encr 3des
 authentication pre-share
crypto isakmp key CISCO address 172.17.1.3
crypto isakmp key SYSTEMS address 172.17.1.4
crypto isakmp keepalive 10
!
crypto ipsec transform-set HE1 esp-3des esp-sha-hmac
crypto ipsec transform-set HE2 esp-3des esp-sha-hmac
!
crypto map IPv6-HE1 local-address Serial0/0/0
crypto map IPv6-HE1 1 ipsec-isakmp
 set peer 172.17.1.3
 set transform-set HE1
 match address VPN-TO-HE1
!
crypto map IPv6-HE2 local-address Loopback0
crypto map IPv6-HE2 1 ipsec-isakmp
 set peer 172.17.1.4
 set transform-set HE2
 match address VPN-TO-HE2
```



Single-Tier Profile

IPSec Configuration—2

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

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

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

Single-Tier Profile
Routing

```
ipv6 unicast-routing
ipv6 cef
!
key chain ESE
 key 1
  key-string 7 111B180B101719
!
interface Tunnel3
 description IPv6 tunnel to HQ Head-end 1
 delay 500
 ipv6 eigrp 1
 ipv6 hold-time eigrp 1 35
 ipv6 authentication mode eigrp 1 md5
 ipv6 authentication key-chain eigrp 1 ESE
!
interface Tunnel4
 description IPv6 tunnel to HQ Head-end 2
 delay 2000
 ipv6 eigrp 1
 ipv6 hold-time eigrp 1 35
 ipv6 authentication mode eigrp 1 md5
 ipv6 authentication key-chain eigrp 1 ESE
```

```
interface Loopback0
 ipv6 eigrp 1
!
interface GigabitEthernet1/0.100
 description DATA VLAN for Computers
 ipv6 eigrp 1
!
ipv6 router eigrp 1
 router-id 10.124.100.1
 stub connected summary
 no shutdown
 passive-interface GigabitEthernet1/0.100
 passive-interface GigabitEthernet1/0.200
 passive-interface GigabitEthernet1/0.300
 passive-interface Loopback0
```

EtherSwitch Module

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

Single-Tier Profile

Security—1

```
ipv6 inspect name v6FW tcp
ipv6 inspect name v6FW icmp
ipv6 inspect name v6FW ftp
ipv6 inspect name v6FW udp
!
interface Tunnel3
 ipv6 traffic-filter INET-WAN-v6 in
 no ipv6 redirects
 no ipv6 unreachables
 ipv6 inspect v6FW out
 ipv6 virtual-reassembly
!
interface GigabitEthernet1/0.100
ipv6 traffic-filter DATA_LAN-v6 in
!
line vty 0 4
ipv6 access-class MGMT-IN in
```

Inspection profile for TCP, ICMP, FTP and UDP

ACL used by IOS FW for dynamic entries

Apply firewall inspection For egress traffic

Used by firewall to create dynamic ACLs and protect against various fragmentation attacks

Apply LAN ACL (next slide)

ACL used to restrict management access

Single-Tier Profile

Security—2

Sample Only

```
ipv6 access-list MGMT-IN
 remark permit mgmt only to loopback
 permit tcp 2001:DB8:CAFE::/48 host 2001:DB8:CAFE:1000::BAD1:A001
 deny ipv6 any any log-input
!
ipv6 access-list DATA_LAN-v6
remark PERMIT ICMPv6 PACKETS FROM HOSTS WITH PREFIX CAFE:1100::/64
permit icmp 2001:DB8:CAFE:1100::/64 any
remark PERMIT IPv6 PACKETS FROM HOSTS WITH PREFIX CAFE:1100::64
permit ipv6 2001:DB8:CAFE:1100::/64 any
remark PERMIT ALL ICMPv6 PACKETS SOURCED BY HOSTS USING THE LINK-LOCAL PREFIX
permit icmp FE80::/10 any
remark PERMIT DHCPv6 ALL-DHCP-AGENTS REQUESTS FROM HOSTS
permit udp any eq 546 any eq 547
remark DENY ALL OTHER IPv6 PACKETS AND LOG
deny ipv6 any any log-input
```

Single-Tier Profile

Security—3

Sample Only

```
ipv6 access-list INET-WAN-v6
 remark PERMIT EIGRP for IPv6
 permit 88 any any
 remark PERMIT PIM for IPv6
 permit 103 any any
 remark PERMIT ALL ICMPv6 PACKETS SOURCED USING THE LINK-LOCAL PREFIX
 permit icmp FE80::/10 any
 remark PERMIT SSH TO LOCAL LOOPBACK
 permit tcp any host 2001:DB8:CAFE:1000::BAD1:A001 eq 22
 remark PERMIT ALL ICMPv6 PACKETS TO LOCAL LOOPBACK,VPN tunnels,VLANs
 permit icmp any host 2001:DB8:CAFE:1000::BAD1:A001
 permit icmp any host 2001:DB8:CAFE:1261::BAD1:A001
 permit icmp any host 2001:DB8:CAFE:1271::BAD1:A001
 permit icmp any 2001:DB8:CAFE:1100::/64
 permit icmp any 2001:DB8:CAFE:1200::/64
 permit icmp any 2001:DB8:CAFE:1300::/64
 remark PERMIT ALL IPv6 PACKETS TO VLANs
 permit ipv6 any 2001:DB8:CAFE:1100::/64
 permit ipv6 any 2001:DB8:CAFE:1200::/64
 permit ipv6 any 2001:DB8:CAFE:1300::/64
 deny ipv6 any any log
```

Single-Tier Profile
QoS

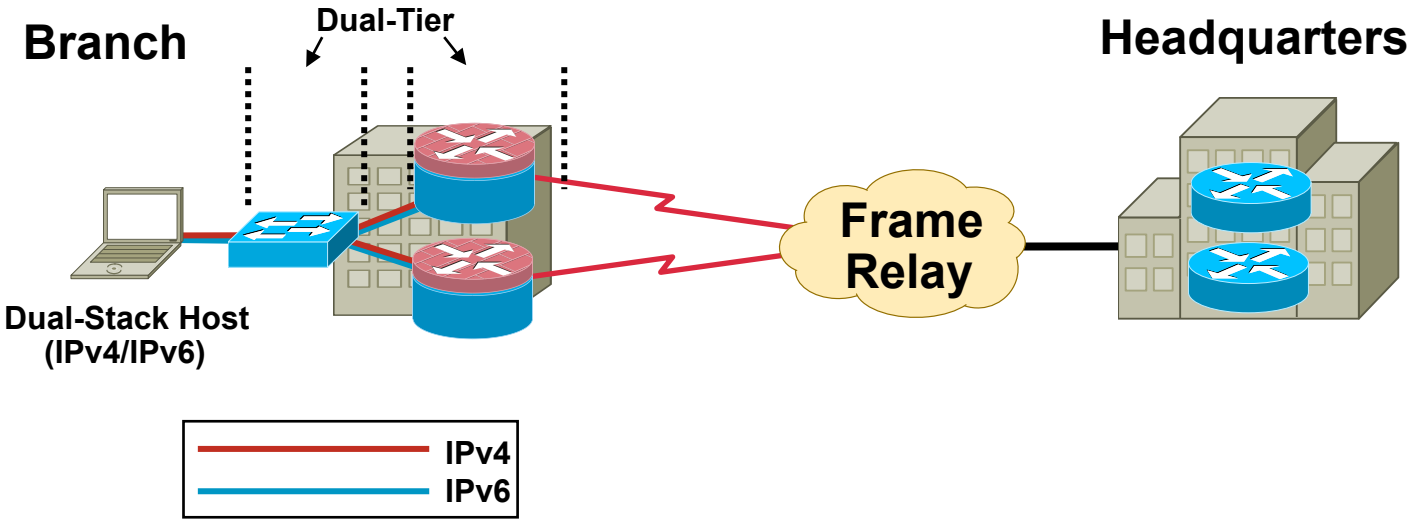
```
class-map match-any BRANCH-TRANSACTIONAL-DATA
 match protocol citrix
 match protocol ldap
 match protocol sqlnet
 match protocol http url "*cisco.com"
 match access-group name BRANCH-TRANSACTIONAL-V6
!
policy-map BRANCH-WAN-EDGE
 class TRANSACTIONAL-DATA
  bandwidth percent 12
  random-detect dscp-based
!
policy-map BRANCH-LAN-EDGE-IN
 class BRANCH-TRANSACTIONAL-DATA
  set dscp af21
!
ipv6 access-list BRANCH-TRANSACTIONAL-V6
 remark Microsoft RDP traffic-mark dscp af21
 permit tcp any any eq 3389
 permit udp any any eq 3389
```

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

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

Dual-Tier Profile

- Redundant set of branch routers—Separate branch switch (multiple switches can use StackWise technology)
- Each branch router uses a single frame-relay connection
- All dual-stack (branch LAN and WAN)—no tunnels needed



Dual-Tier Profile

Configuration

Branch Router 1

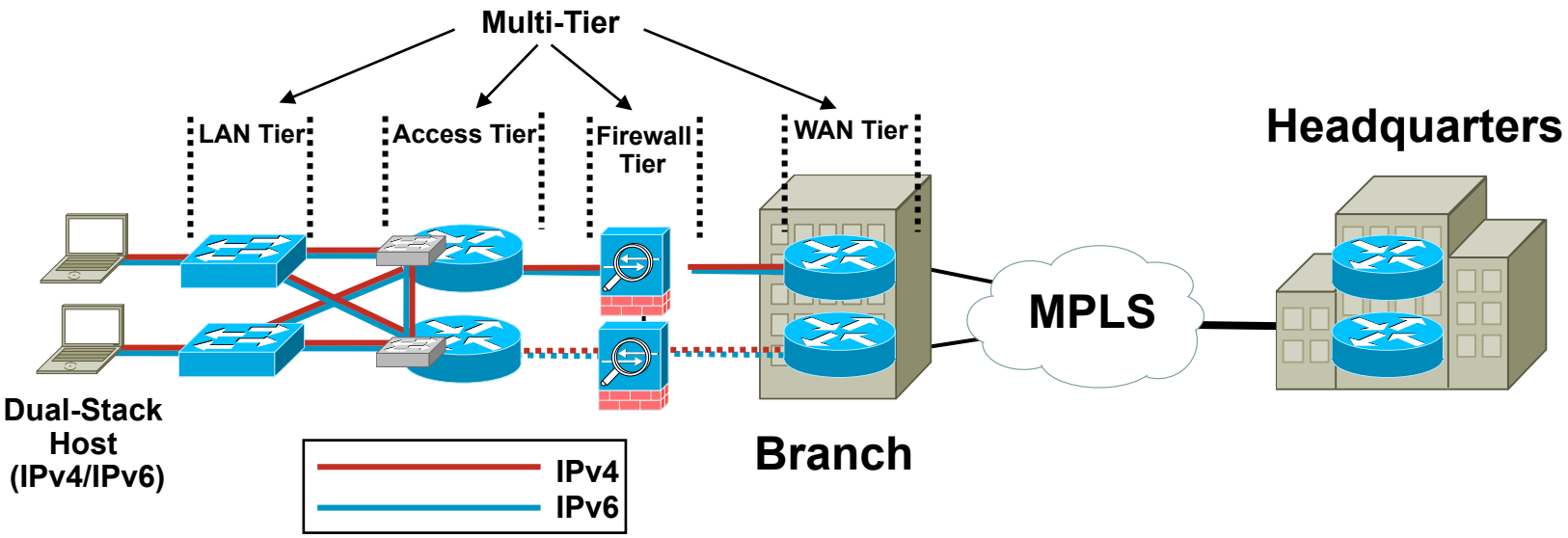
```
interface Serial0/1/0.17 point-to-point
 description TO FRAME-RELAY PROVIDER
 ipv6 address 2001:DB8:CAFE:1262::BAD1:1010/64
 ipv6 eigrp 1
 ipv6 hold-time eigrp 1 35
 ipv6 authentication mode eigrp 1 md5
 ipv6 authentication key-chain eigrp 1 ESE
 frame-relay interface-dlci 17
  class QOS-BR2-MAP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

Branch Router 2

```
interface Serial0/2/0.18 point-to-point
 description TO FRAME-RELAY PROVIDER
 ipv6 address 2001:DB8:CAFE:1272::BAD1:1020/64
 ipv6 eigrp 1
 ipv6 hold-time eigrp 1 35
 ipv6 authentication mode eigrp 1 md5
 ipv6 authentication key-chain eigrp 1 ESE
 frame-relay interface-dlci 18
  class QOS-BR2-MAP
!
interface FastEthernet0/0.100
 ipv6 address 2001:DB8:CAFE:2100::BAD1:1020/64
 ipv6 traffic-filter DATA_LAN-v6 in
 ipv6 nd other-config-flag
 ipv6 eigrp 1
 standby version 2
 standby 201 ipv6 autoconfig
 standby 201 preempt
 standby 201 authentication ese
```

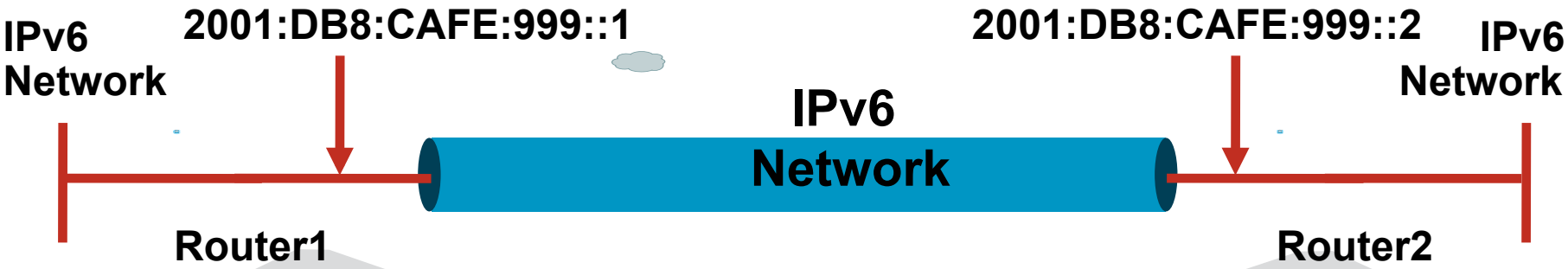
Multi-Tier Profile

- All branch elements are redundant and separate
  - WAN Tier—WAN connections—Can be anything (Frame/IPSec)—MPLS shown here
  - Firewall Tier—Redundant ASA Firewalls
  - Access Tier—Internal services routers (like a campus distribution layer)
  - LAN Tier—Access switches (like a campus access layer
- Dual-stack is used on every tier—If SP provides IPv6 services via MPLS. If not, tunnels can be used from WAN tier to HQ site



IPv6 IPSec Example

IKE/IPSec Policies

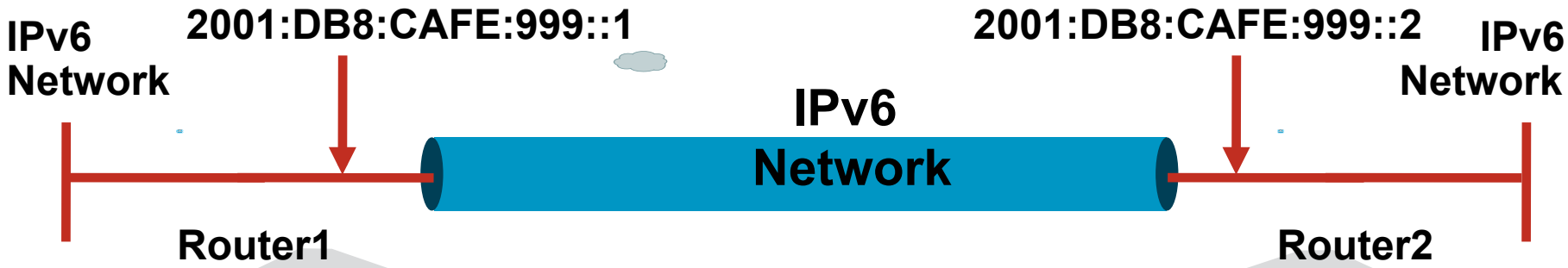



```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key CISCOKEY address ipv6
2001:DB8:CAFE:999::2/128
crypto isakmp keepalive 10 2
!
crypto ipsec transform-set v6STRONG
esp-3des esp-sha-hmac
!
crypto ipsec profile v6PRO
 set transform-set v6STRONG
```

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key CISCOKEY address ipv6
2001:DB8:CAFE:999::1/128
crypto isakmp keepalive 10 2
!
crypto ipsec transform-set v6STRONG
esp-3des esp-sha-hmac
!
crypto ipsec profile v6PRO
 set transform-set v6STRONG
```

IPv6 IPSec Example

Tunnels

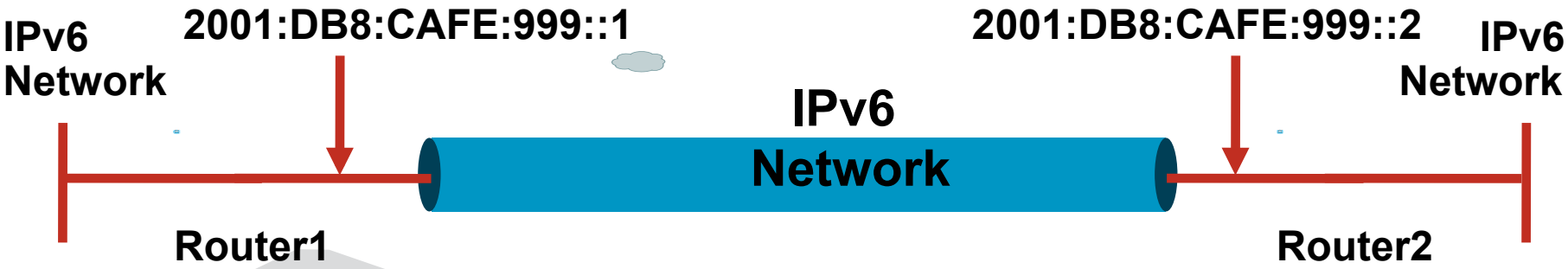



```
interface Tunnel0
 ipv6 address 2001:DB8:CAFE:F00D::1/127
 ipv6 eigrp 1
 ipv6 mtu 1400
 tunnel source Serial2/0
 tunnel destination 2001:DB8:CAFE:
999::2
 tunnel mode ipsec ipv6
 tunnel protection ipsec profile v6PRO
!
interface Ethernet0/0
 ipv6 address 2001:DB8:CAFE:100::1/64
 ipv6 eigrp 1
!
interface Serial2/0
 ipv6 address 2001:DB8:CAFE:999::1/127
```

```
interface Tunnel0
 ipv6 address 2001:DB8:CAFE:F00D::2/127
 ipv6 eigrp 1
 ipv6 mtu 1400
 tunnel source Serial2/0
 tunnel destination 2001:DB8:CAFE:
999::1
 tunnel mode ipsec ipv6
 tunnel protection ipsec profile v6PRO
!
interface Ethernet0/0
 ipv6 address 2001:DB8:CAFE:200::1/64
 ipv6 eigrp 1
!
interface Serial2/0
 ipv6 address 2001:DB8:CAFE:999::2/127
```

IPv6 IPSec Example

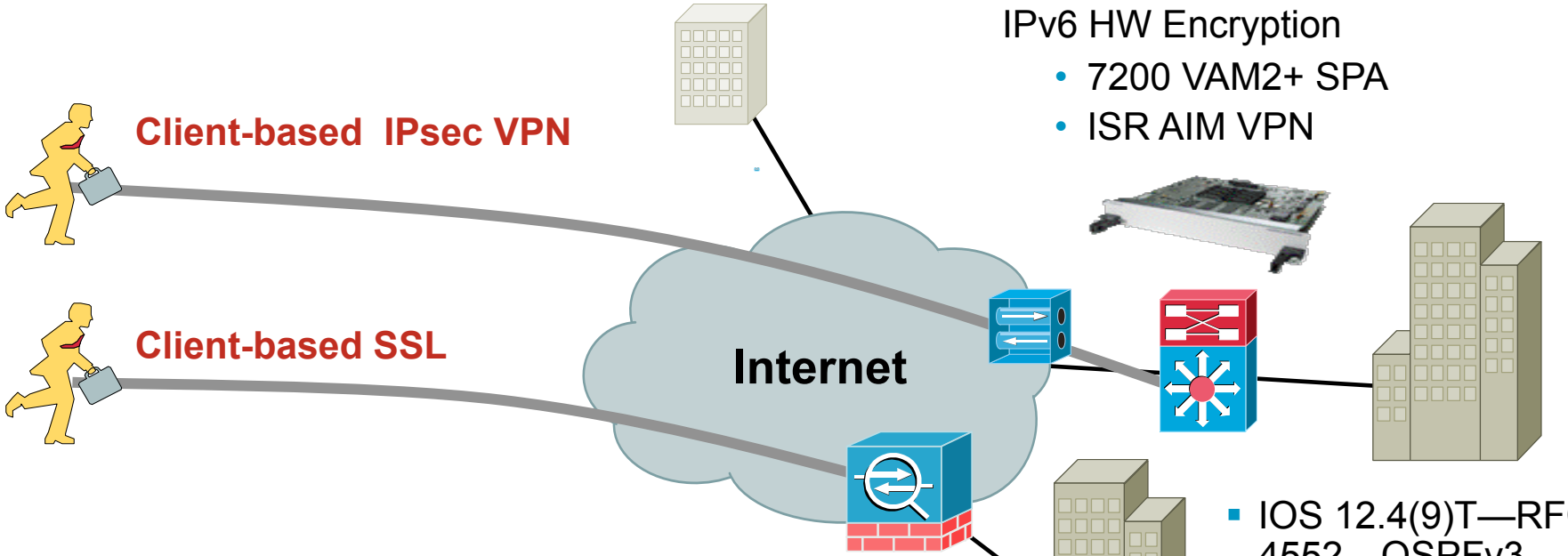
Show Output




```
Router1#show crypto engine connections active
Crypto Engine Connections
   ID Intfc  Type  Algorithm           Encrypt  Decrypt IP-Address
    3 Tu0    ipsec 3DES+SHA                 0       17 2001:DB8:CAFE:999::1
    4 Tu0    ipsec 3DES+SHA                16        0 2001:DB8:CAFE:999::1
 1006 Tu0    IKE   SHA+DES                  0        0 2001:DB8:CAFE:999::1

Router1#show crypto sessions
Crypto session current status
Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 2001:DB8:CAFE:999::2 port 500
  IKE SA: local 2001:DB8:CAFE:999::1/500
          remote 2001:DB8:CAFE:999::2/500 Active
  ipsec FLOW: permit 41 ::/0 ::/0
        Active SAs: 2, origin: crypto map
```

Remote Access

Cisco IPv6 Security



IPv6 IPSec Tunnels
- IOS 12.4(4)T

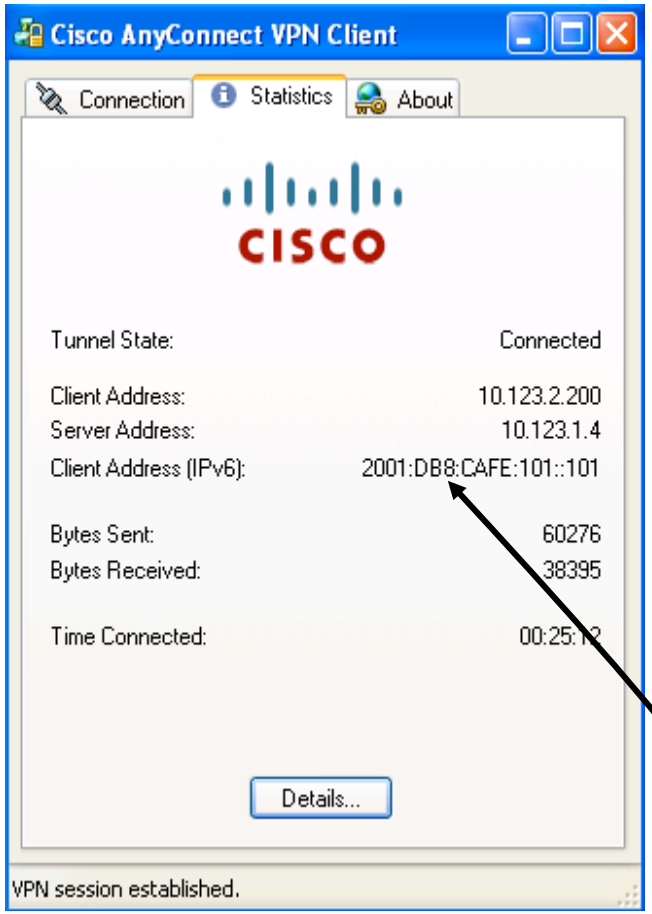
IPv6 HW Encryption
- 7200 VAM2+ SPA
- ISR AIM VPN

- 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.

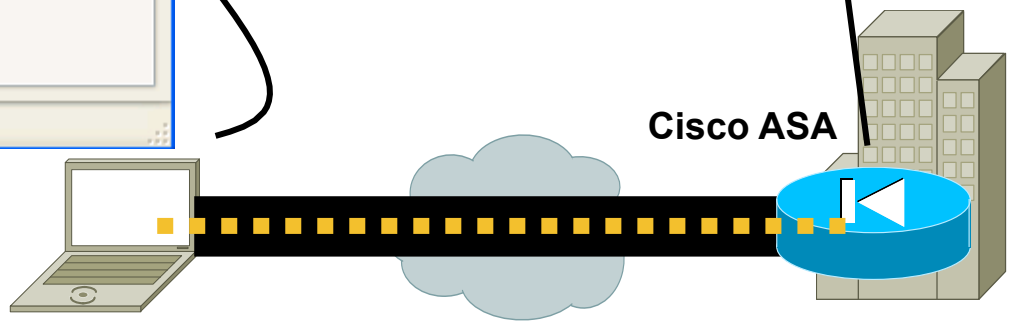
- IOS 12.4(9)T—RFC 4552—OSPFv3 Authentication
- All IOS—packet filtering e-ACL
- IPv6 over DMVPN

IPv6 Firewall
- IOS Firewall 12.3T, 12.4, 12.4T
- FWSM 3.x
- PIX 7.x +, including ASA 5500 series

AnyConnect 2.x—SSL VPN



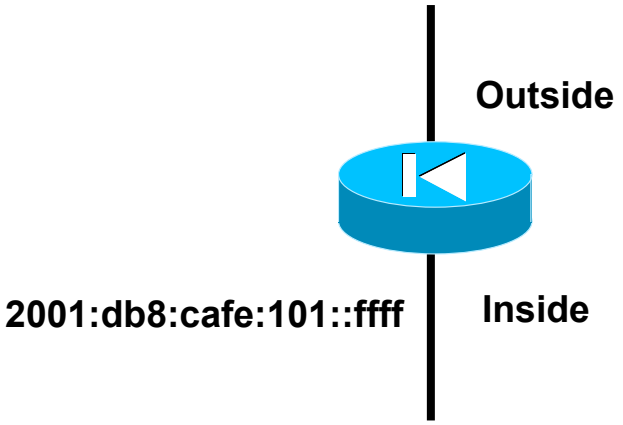

```
asa-edge-1#show vpn-sessiondb svc
Session Type: SVC
Username     : ciscoese                Index        : 14
Assigned IP  : 10.123.2.200            Public IP    : 10.124.2.18
Assigned IPv6: 2001:db8:cafe:101::101
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
License      : SSL VPN
Encryption   : 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

AnyConnect 2.x—Summary Configuration

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.123.1.4 255.255.255.0
 ipv6 enable
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.123.2.4 255.255.255.0
 ipv6 address 2001:db8:cafe:101::ffff/64
!
ipv6 local pool ANYv6POOL 2001:db8:cafe:101::101/64 200
```



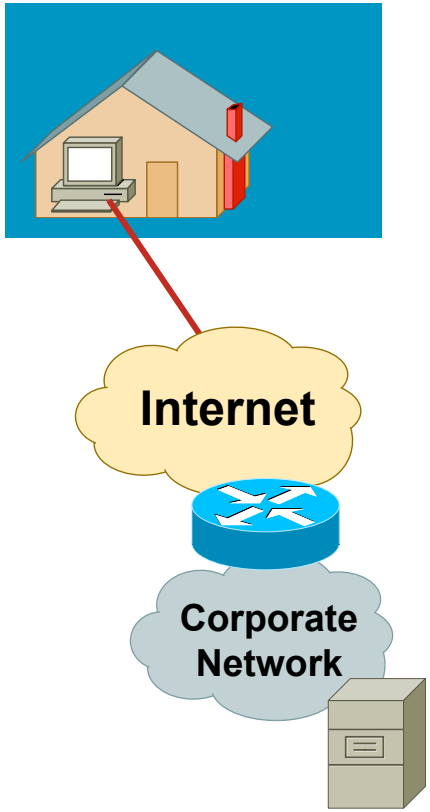

```
webvpn
 enable outside
 svc enable
 tunnel-group-list enable
group-policy AnyGrpPolicy internal
group-policy AnyGrpPolicy attributes
 vpn-tunnel-protocol svc
 default-domain value cisco.com
 address-pools value AnyPool
tunnel-group ANYCONNECT type remote-access
tunnel-group ANYCONNECT general-attributes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

```
crypto ca trustpoint ASDM_TrustPoint0
 enrollment self
 fqdn asa-edge-1.cisco.com
 subject-name CN=asa-edge-1
 keypair esevpnkeypair
 no client-types
 crl configure
ssl trust-point ASDM_TrustPoint0 outside
```

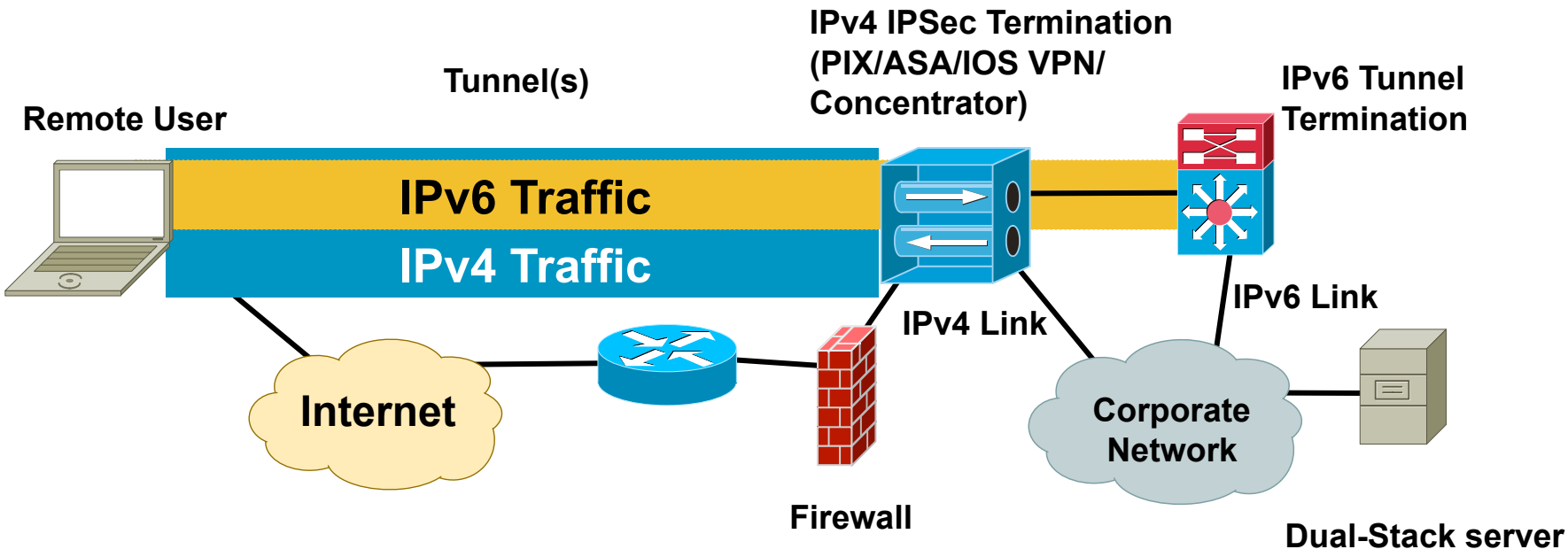
http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect20/administrative/guide/admin6.html#wp1002258

IPv6 for Remote Devices

- Remote hosts can use a VPN client or router to establish connectivity back to enterprise
- Possible over IPv4 today, not possible over IPv6…yet
- How you allow access to IPv6 services at central site or Internet in a secure fashion?
  - Enabling IPv6 traffic inside the Cisco VPN client tunnel
  - Allow remote host to establish a v6-in-v4 tunnel either automatically or manually
    - ISATAP—Intra Site Automatic Tunnel Addressing Protocol
    - Configured—Static configuration for each side of tunnel
  - Same split-tunneling issues exists



IPv6-in-IPv4 Tunnel Example—Cisco VPN Client

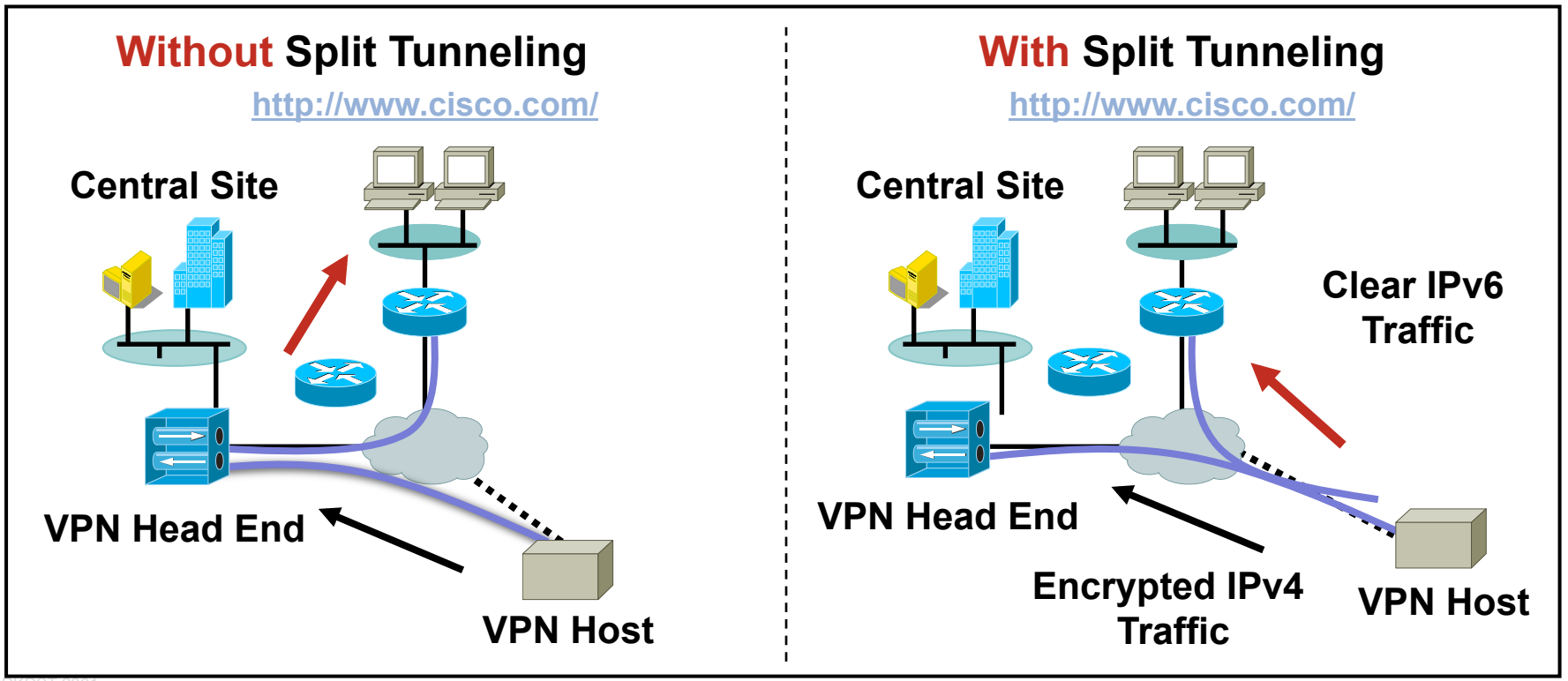


Considerations

- Cisco IOS® version supporting IPv6 configured/ ISATAP tunnels
  - Configured—12.3(1)M/12.3(2)T/12.2(14)S and above (12.4M/12.4T)
  - ISATAP—12.3(1)M, 12.3(2)T, 12.2(14)S and above (12.4M/12.4T)
  - Catalyst® 6500 with Sup720/32—12.2(17a)SX1—HW forwarding
- Be aware of the security issues if split-tunneling is used
  - Attacker can come in IPv6 interface and jump on the IPv4 interface (encrypted to enterprise)
  - In Windows Firewall—default policy is to DENY packets from one interface to another
- Remember that the IPv6 tunneled traffic is still encapsulated as a tunnel WHEN it leaves the VPN device
- Allow IPv6 tunneled traffic across access lists (Protocol 41)

Split Tunneling

- Ensure that the IPv6 traffic is properly routed through the IPv4 IPSec tunnel
- IPv6 traffic MAY take a path via the clear (unencrypted) route
- This is bad if **you are unaware that it is happening**



Required Stuff: Client Side

- Client operating system with IPv6

  Microsoft Windows XP SP1/2003 and Vista/Server 2008 (Supports Configured/ISATAP)

  Linux (7.3 or higher)—USAGI port required for ISATAP

  Mac OS X (10.2 or higher)—Currently need a VPN device on client network

  SunOS (8 or higher)—Currently need a VPN device on client network

  See reference slide for links/OS listing

- Cisco VPN Client 4.0.1 and higher for configured/ISATAP

IPv6 Using Cisco VPN Client

Example: Client Configuration (Windows XP): ISATAP

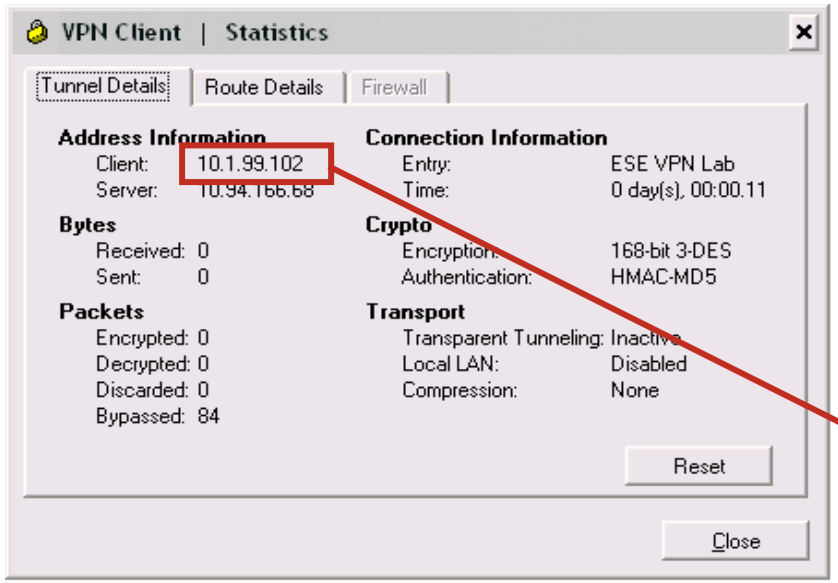
- Microsoft Windows XP (SP1 or higher)
- IPv6 must be installed
- XP will automatically attempt to resolve the name “ISATAP”
  - Local host name
  - Hosts file—SystemRoot\system32\drivers\etc
  - DNS name query
  - NetBIOS and Lmhosts
- Manual ISATAP router entry can be made

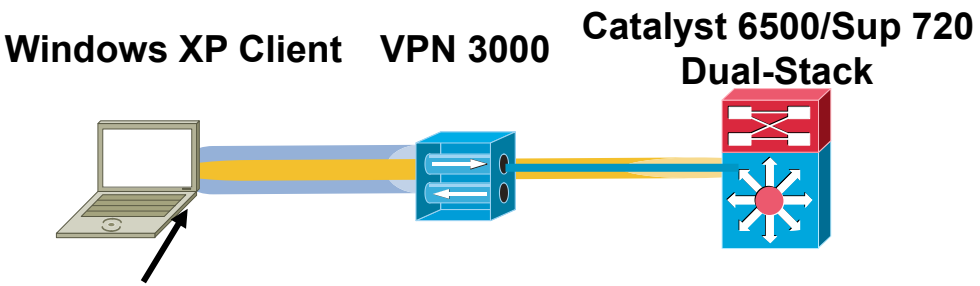
```
netsh interface ipv6 isatap set router 20.1.1.1
```

- Key fact here is that NO additional configuration on the client is needed again!
- Use previous ISATAP configurations shown for router-side

Note: ISATAP is supported on some versions of Linux/BSD (manual router entry is required)

Does It Work?





10.1.99.102—VPN Address

2001:DB8:c003:1101:0:5efe:10.1.99.102—IPv6 address

```
Interface 2: Automatic Tunneling Pseudo-Interface

Addr Type  DAD State  Valid Life    Pref. Life    Address
---------  ---------- ------------ ------------ ----------------------------
Public     Preferred   29d23h56m5s  6d23h56m5s 2001:db8:c003:1101:0:5efe:10.1.99.102
Link       Preferred   infinite     infinite   fe80::5efe:10.1.99.102
```

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

Publish  Type       Met  Prefix                    Idx  Gateway/Interface Name
-------  --------  ----  ------------------------  ---  --------------------
no       Autoconf     9  2001:db8:c003:1101::/64     2  Automatic Tunneling Pseudo-Interface
no       Manual       1  ::/0                        2  fe80::5efe:20.1.1.1
```

Checksum

(Planning and Deployment Summary)

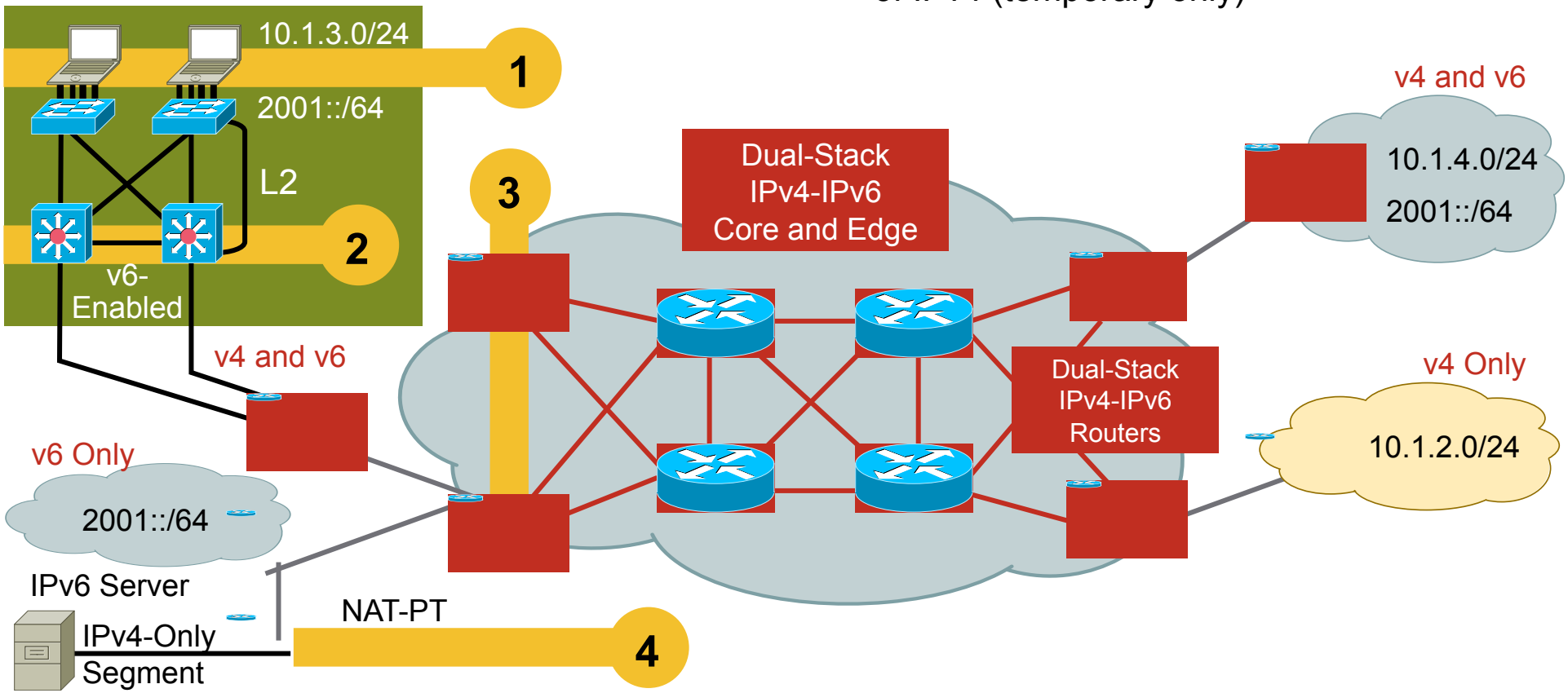
IPv6 Integration Outline

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

Integration/Coexistence Starting Points

Example: Integration Demarc/Start Points in Campus/WAN

1. Start dual-stack on hosts/OS
2. Start dual-stack in campus distribution layer (details follow)
3. Start dual-stack on the WAN/campus core/edge routers
4. NAT-PT for servers/apps only capable of IPv4 (temporary only)



Pre-Deployment Checklist

Other Critical Network Planning Requirements

- ✓ **Establish starting point, network assessment, security guidelines**
- ✓ **Acquire IPv6 address block and create IPv6 addressing scheme**
- ✓ Create and budget for an IPv6 lab that closely emulates all network elements (routers, switches, hosts, OS)
- ✓ Upgrade DNS server to support IPv6
- ✓ Establish network management considerations (hardware, MIBs required for v6, etc.)
- ✓ Routing and multicast protocol and selection/evaluation process (align with IPv4 choice is possible)
- ✓ Consider options for centralized ISATAP router (see campus example)
- ✓ Evaluate IPv6-capable transport services available from current Service Provider (SP)
  - Link support to timeline needed, not before
  - Does L3 VPN service support QoS? Dual-homing? Security at NAP?

Transport Deployment Options for Integration

Applied to Campus, WAN, Branch, and Other

- Campus (also applies to Data Center)
  - Dual-stack (IPv4/v6 enabled on all L3 devices—core/distr/access)
  - Hybrid (combination dual-stack, tunnels, ISATAP)
  - Services block (dedicated for IPv6 ISATAP tunnel termination)
- WAN (used for core or branch interconnect)
  - Dual-stack core/edge
  - WAN L2 transport (IPv4/v6 over ATM/FR, PPP/HDLC, T1/T3, OC-x)
  - Metro Service (Ethernet, point-to-point, point-to-multipoint)
- VPN/transport considerations
  - Self-deployed MPLS VPNs: PE to PE (VPN or non-VPN service)
  - SP Offering L3 VPN service: CE to CE (encryption? QoS? multicast?)
  - Overlay 6 over 4 IPSec: site-to-site, VPN client-based using ISATAP
  - IPv6 over WiFi (802.1x is not required to be supported over IPv6)
- Other service options
  - Broadband, internet (as transport), remote access supporting IPv6

General IPv6 Requirements

Considered in Each Place in the Network

- General Coexistence
  - IPv4 and IPv6 coexist with no impact on performance
  - Flexible integration tools
- Routing
  - High-performance IPv6-aware routing protocols
- QoS
  - Identify and prioritize traffic based upon a wide-variety of criteria
  - Contiguous over campus, WAN, branch
  - SP offered
- IP Multicast
  - Optimize traffic utilization with a broad range of deployment types
- Security
  - User-based policy enforcement
  - Stress Host-based features
  - Privacy extensions
  - Monitoring and reporting
- Mobility
  - Access to applications and services while in motion
  - Design into core infrastructure for IPv4 and IPv6

Each Category Applied to Campus, WAN, Branch, Other

Industry's Broadest Platform Support

Cisco IOS 12.0S

Cisco 12000 Series Routers

Cisco 10720 Series

Cisco IOS 12.4/12.4T

Cisco 800 Series Routers

Cisco 1700 Series Routers

Cisco 1800 Series Routers

Cisco 2600 Series Routers

Cisco 2800 Series Routers

Cisco 3600 Series Routers

Cisco 3700 Series Routers

Cisco 3800 Series Routers

Cisco 7200 Series Routers

Cisco 7301 Series Routers

Cisco 7500 Series Routers (EoL)

Cisco IOS-XR

CRS-1, Cisco 12000

Cisco IOS 12.2S family

Cisco ASR1000 series

Cisco 72/7300 Series Routers

Cisco 75/7600 Series Routers

Cisco 10000 Series Routers

Catalyst 3750/3560/2960 Series

Catalyst 4500 Series

Catalyst 6500 Series

Cisco Product Portfolio

ASA Firewall (7.x), FWSM 3.1,

LMS 2.5, CNR 6.2, NFC 5.x, NAM 3.x,

MDS9500 series, Nexus 7000, GGSN 7.0

High Capacity Forwarding
Cisco IPv6 Solutions

- Cisco CRS-1

OC-768, OC-48, 10GE and GE line cards

- Cisco 12000 series

Internet Service Engine 3 – up to 3.8Mpps per LC

Internet Service Engine 5 – Up to 16Mpps per LC

- Cisco 10000 PRE2/PRE3/PRE4
- Cisco ASR 1000 series
- Cisco 7600 and Catalyst 6500 series

Sup. Engine 720, 720-3BXL, 32W, 32/PISA, RSP720 – up to 200Mpps (EANTC report)

IPv6 tunneling—Configured, Automatic, 6to4 and ISATAP tunnels in hardware

- Nexus 7000 series, MDS 9500 series
- Catalyst 4500 series

Supervisor Engine 6E

- Catalyst 3750/3560 & 3750E/3560E series

Other Security Products

- ASA Firewall
  - Since version 7.0
  - Dual stack, IPv6 only,
  - No header extension parsing, no stateful-failover (coming)
- FWSM
  - IPv6 in software...
- Cisco Security Agent
  - Needs CSA 6.0 for IPv6 network protection
- IPS
  - Needs 6.2 (not yet FCS...)

Cisco IPv6 compliance

- Conformance tests + Interoperability tests
  - IPv6 Ready Logo – www.ipv6ready.org
  - US DoD JITC conformance - http://jitc.fhu.disa.mil/apl/ipv6.html
  - Cable Labs DOCSIS 3.0 conformance
  - Microsoft Vista/Server 2008 interoperability – *Vista logo*
- Cisco IOS Release certification
  - Cisco IOS 12.4(11)T, C7600, C6500, C4500, IOS Firewall achieved JITC certification
  - Cisco IOS 12.3, 12.3T, 12.2SX, 12.0S and XR (3.2) are compliant with the IPv6 Ready Logo Phase I
  - Cisco IOS 12.4(9)T is compliant with IPv6 Ready Logo Phase II core specs
  - DOCSIS 3.0 Bronze qualified

Issues for success

Focus on Business Value…

Most early success has been in closed environments.

Dual stack simplifies the overall task of transition by allowing graceful one-application-at-a-time deployments, ***BUT*** that can't happen without IPv4.

There will be a panic in the press once the IPv4 pool is depleted.

Carriers will be required to support IPv4 until their customers move. The current retail rate is ~$1/day/address, and the cost of scarce commodities generally does not go down…

Conclusion

- Start learning now—Books, presentations, your own pilot lab
- 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 and Server 2008 will have IPv6 enabled by default—Understand what impact any OS has on the network
- Things to consider:

  Full parity between IPv4 and IPv6 is the goal, but not a reality today

  Watch the standards and policies

More Information

- CCO IPv6

  http://www.cisco.com/ipv6

- The ABC of IPv6

  http://www.cisco.com/en/US/products/sw/iosswrel/products_abc_ios_overview.html

- IPv6 e-Learning [requires CCO username/password]

  http://www.cisco.com/warp/customer/732/Tech/ipv6/elearning/

- IPv6 Access Services

  http://www.cisco.com/warp/public/732/Tech/ipv6/docs/ipv6_access_wp_v2.pdf

- ICMPv6 Packet Types and Codes TechNote

  http://www.cisco.com/warp/customer/105/icmpv6codes.html

- Cisco IOS IPv6 Product Manager

  pgrosset@cisco.com

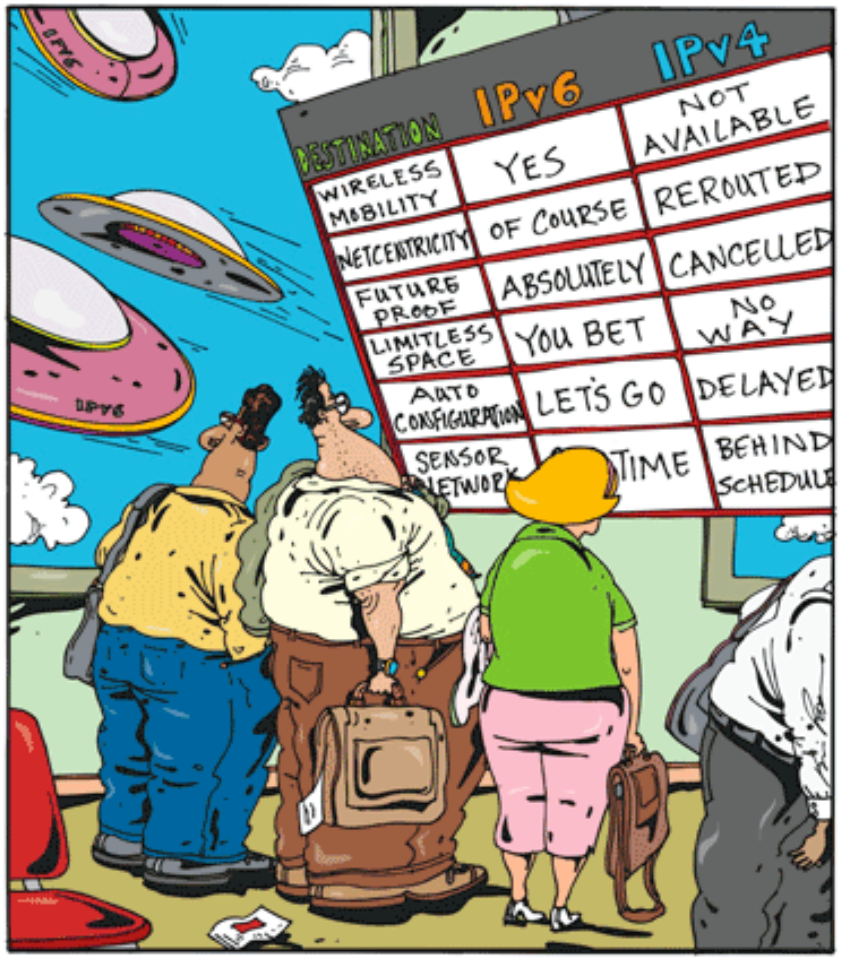
Reference Materials

Speaker Recommended!!

"Deploying IPv6 Networks" by Ciprian Popoviciu, Eric Levy-Abegnoli, Patrick Grossetete—Cisco Press (ISBN: 1587052105)

- Deploying IPv6 in Campus Networks: http://www.cisco.com/univercd/cc/td/doc/solution/campipv6.pdf
- Deploying IPv6 in Branch Networks: http://www.cisco.com/univercd/cc/td/doc/solution/brchipv6.pdf
- CCO IPv6 Main Page: http://www.cisco.com/go/ipv6
- Cisco Network Designs: http://www.cisco.com/go/srnd

Famous last words…



Suddenly, it dawned on Ronald that he needed to be on the right flight plan and IPv6 seemed to be just the ticket.

Appendix Slides
For Reference Only

Appendix: Microsoft Windows Vista/Server 2008

Understand the Behavior of Vista

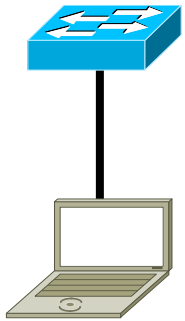
- IPv6 is preferred over IPv4
  - Vista sends IPv6 NA/NS/RS upon link-up
    - Attempts DHCP for IPv6
    - If no DHCP or local RA received with Global or ULA, then try ISATAP
    - If no ISATAP, then try Teredo
- Become familiar with Teredo http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/teredo.mspx
- ANY application built on the Peer-to-Peer Framework REQUIRES IPv6 and will NOT function over IPv4 - http://www.microsoft.com/technet/network/p2p/default.mspx

In More Detail—Vista on Link-Up

No Network Services

No.	Time	Source	Destination	Protocol	Info
1	0.000000	::	ff02::1:ffae:4361	ICMPv6	Neighbor solicitation
2	0.000030	fe80::80aa:fd5:f7ae:4361	ff02::2	ICMPv6	Router solicitation
3	0.000080	fe80::80aa:fd5:f7ae:4361	ff02::16	ICMPv6	Multicast Listener Report Message v2
4	1.155917	fe80::80aa:fd5:f7ae:4361	ff02::1:3	UDP	Source port: 49722 Destination port: 5355
5	1.156683	169.254.67.97	224.0.0.252	UDP	Source port: 49723 Destination port: 5355
6	3.484709	169.254.67.97	169.254.255.255	NBNS	Name query NB **ISATAP**<00>
7	126.409530	fe80::80aa:fd5:f7ae:4361	ff02::1:2	DHCPv6	Information-request
8	128.886397	0.0.0.0	255.255.255.255	DHCP	DHCP Discover—Transaction ID 0x6c8d6efa

1. Unspecified address :: → Solicited node address NS/DAD
2. Looking for a local router → ff02::2 RS
3. Looking for MLD enabled routers → ff02::16 MLDv2 report
4. LLMNR for IPv6—ff02::1:3—advertise hostname
5. LLMNR for IPv4—224.0.0.252 from RFC 3927 address
6. No global or ULA received via step 1/2—Try ISATAP
7. Try DHCP for IPv6—ff02::1:2
8. Try DHCP for IPv4

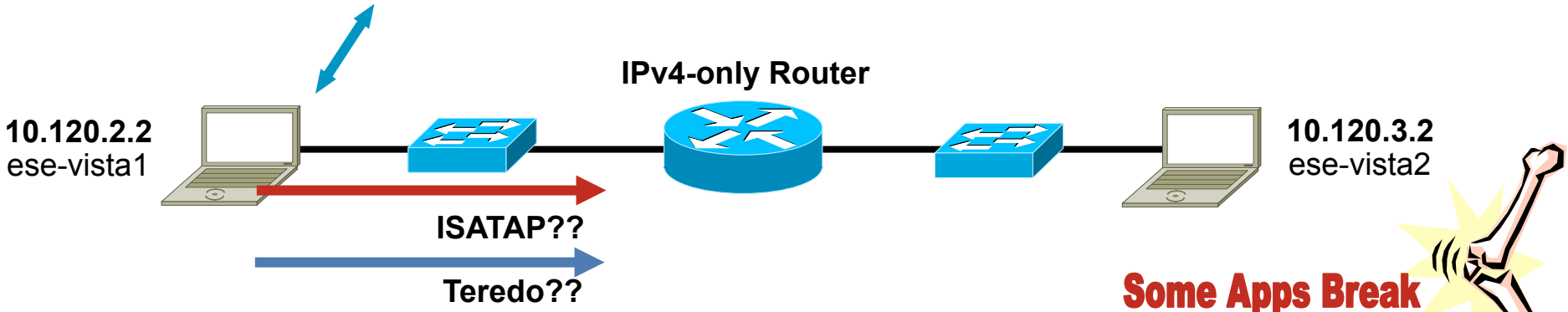


fe80::80aa:fd5:f7ae:4361
ese-vista1

IPv4 Network—No IPv6 Network Services

What Does Vista Try to Do?

```
No.     Time       Source          Destination     Protocol Info
  13 8.813509    10.120.2.1        10.120.2.2       DHCP    DHCP ACK      - Transaction ID 0x2b8af443
....
Bootstrap Protocol
    ...
    Your (client) IP address: 10.120.2.2 (10.120.2.2)
    ...
    Option: (t=3,l=4) Router = 10.120.2.1
    Option: (t=6,l=4) Domain Name Server = 10.121.11.4
    Option: (t=15,l=9) Domain Name = "cisco.com"
    ..

No.     Time       Source          Destination     Protocol Info
    70 13.360756   10.120.2.2        10.121.11.4       DNS     Standard query A isatap.cisco.com

No.     Time       Source          Destination     Protocol Info
   138 25.362181   10.120.2.2        10.121.11.4       DNS     Standard query A teredo.ipv6.microsoft.com

No.     Time       Source          Destination     Protocol Info
   580 296.686197  10.120.2.2      10.120.3.2        TCP     49211 > epmap [SYN] Seq=0 Len=0 MSS=1460 WS=8
   581 296.687721  10.120.3.2      10.120.2.2        TCP     epmap > 49211 [SYN, ACK] Seq=0 Ack=1 Win=2097152
   582 296.687794  10.120.2.2      10.120.3.2        TCP     49211 > epmap [ACK] Seq=1 Ack=1 Win=65536 Len=0
   583 296.687913  10.120.2.2      10.120.3.2        DCERPC  Bind: call_id: 1, 2 context items, 1st IOXIDResolver V0.0
```



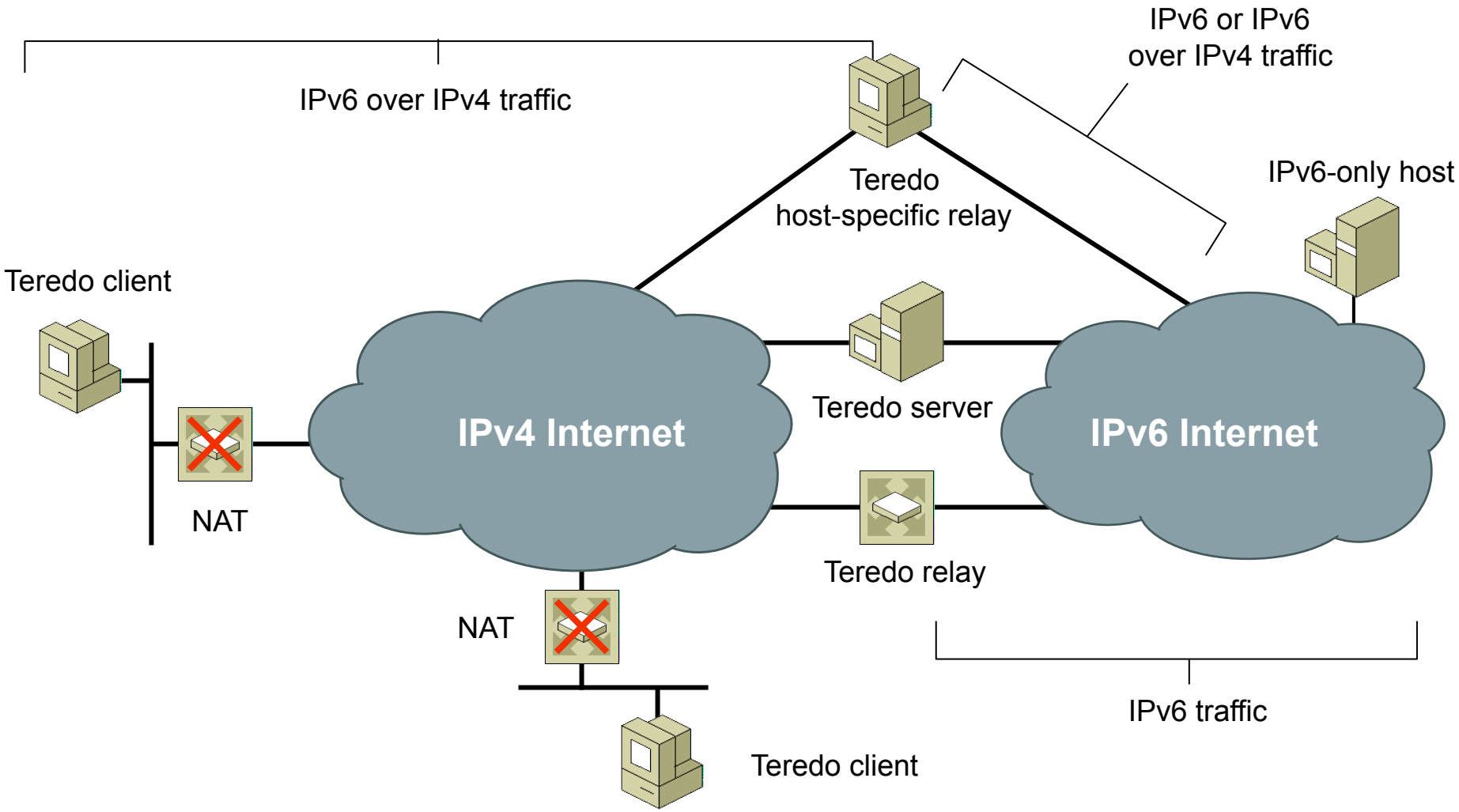
What Is Teredo?

- RFC4380
- Tunnel IPv6 through NATs (NAT types defined in RFC3489)
  - Full Cone NATs (aka one-to-one)—Supported by Teredo
  - Restricted NATs—Supported by Teredo
  - Symmetric NATs—Supported by Teredo with Vista/Server 2008 if only one Teredo client is behind a Symmetric NATs
- Uses UDP port 3544
- Is complex—many sequences for communication and has several attack vectors
- Available on:
  - Microsoft Windows XP SP1 w/Advanced Networking Pack
  - Microsoft Windows Server 2003 SP1
  - Microsoft Windows Vista (enabled by default—inactive until application requires it)
  - Microsoft Server 2008
    http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/teredo.mspx
  - Linux, BSD and Mac OS X—“Miredo”
    http://www.simphalempin.com/dev/miredo/

Teredo Components

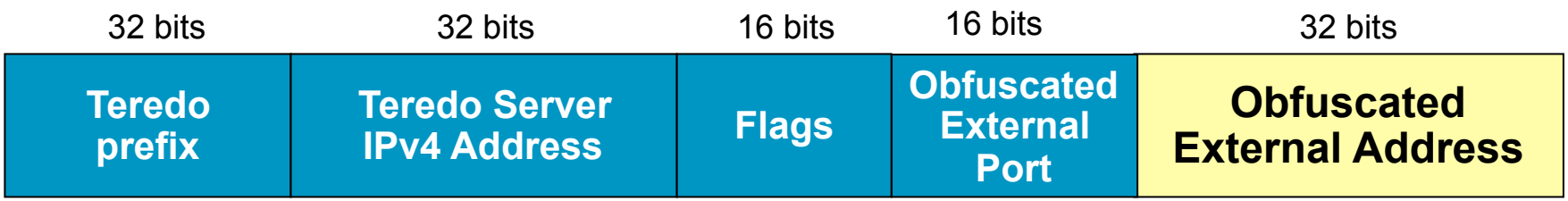
- Teredo Client—Dual-stack node that supports Teredo tunneling to other Teredo clients or IPv6 nodes (via a relay)
- Teredo Server—Dual-stack node connected to IPv4 Internet and IPv6 Internet. Assists in addressing of Teredo clients and initial communication between clients and/or IPv6-only hosts—Listens on UDP port 3544
- Teredo Relay—Dual-stack router that forwards packets between Teredo clients and IPv6-only hosts
- Teredo Host-Specific Relay—Dual-stack node that is connected to IPv4 Internet and IPv6 Internet and can communicate with Teredo Clients without the need for a Teredo Relay

Teredo Overview



*From Microsoft “Teredo Overview” paper

Teredo Address



- Teredo IPv6 prefix (2001::/32—previously was 3FFE:831F::/32)
- Teredo Server IPv4 address: global address of the server
- Flags: defines NAT type (e.g. Cone NAT)
- Obfuscated External Port: UDP port number to be used with the IPv4 address
- Obfuscated External Address: contains the global address of the NAT

Initial Configuration for Client

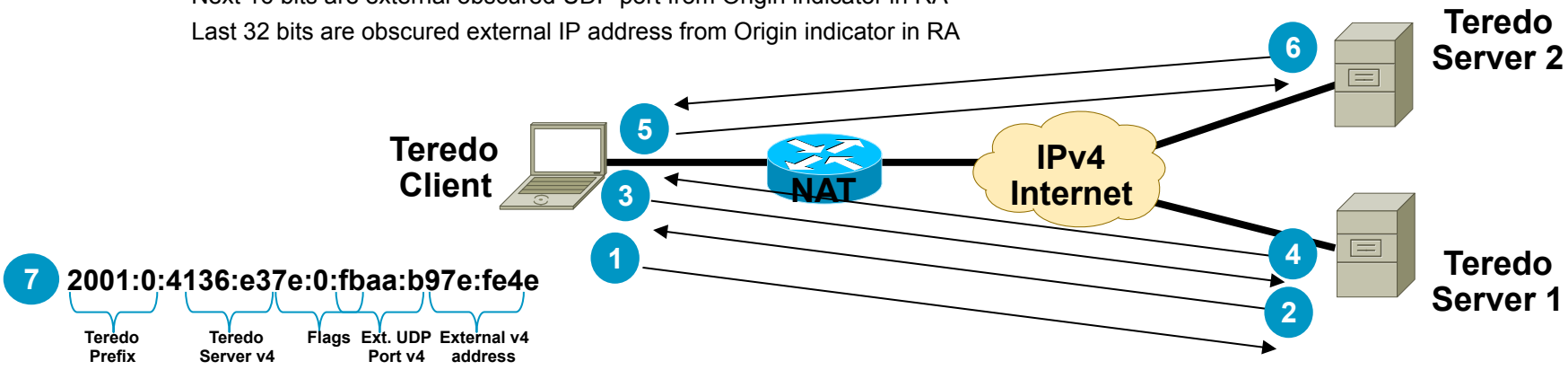
1. RS message sent from Teredo client to server—RS from LL address with Cone flag set
2. Server responds with RA—RS has Cone flag set—server sends RA from alternate v4 address —if client receives the RA, client is behind cone NAT
3. If RA is not received by client, client sends another RA with Cone flag not set
4. Server responds with RA from v4 address = destination v4 address from RS—if client receives the RA, client is behind restricted NAT
5. To ensure client is not behind symmetric NAT, client sends another RS to secondary server
6. 2nd server sends an RA to client—client compares mapped address and UDP ports in the Origin indicators of the RA received by both servers. If different, then the NAT is mapping same internal address/port to different external address/port and NAT is a symmetric NAT
7. Client constructs Teredo address from RA

   First 64 bits are the value from prefix received in RA (32 bits for IPv6 Teredo prefix + 32 bits of hex representation of IPv4 Teredo server address)

   Next 16 bits are the Flags field (0x0000 = Restricted NAT, 0x8000 = Cone NAT)

   Next 16 bits are external obscured UDP port from Origin indicator in RA

   Last 32 bits are obscured external IP address from Origin indicator in RA



What Happens on the Wire—1

No.	Time	Source	Destination	Protocol	Info
15	25.468050	172.16.1.103	151.164.11.201	DNS	Standard query A **teredo.ipv6.microsoft.com**

No.	Time	Source	Destination	Protocol	Info
16	25.481609	151.164.11.201	172.16.1.103	DNS	Standard query response A **65.54.227.126** A 65.54.227.127 A 65.54.227.120 A 65.54.227.124

```
netsh interface ipv6>sh teredo
Teredo Parameters
---------------------------------------------
Type                                    : client
Server Name                             : teredo.ipv6.microsoft.com
Client Refresh Interval                 : default
Client Port                             : default
State                                   : probe(cone)
Type                                    : teredo client
Network                                 : unmanaged
NAT                                     : cone
```

```
netsh interface ipv6>sh teredo
Teredo Parameters
---------------------------------------------
Type                                    : client
Server Name                             : teredo.ipv6.microsoft.com
Client Refresh Interval                 : default
Client Port                             : default
State                                   : qualified
Type                                    : teredo client
Network                                 : unmanaged
NAT                                     : restricted
```

What Happens on the Wire—2

No. Time Source Destination Protocol Info
28 33.595460 **fe80::8000:ffff:ffff:fffd** **ff02::2** ICMPv6 **Router solicitation**
Internet Protocol, Src: **172.16.1.103** (172.16.1.103), Dst: **65.54.227.126** (65.54.227.126)
User Datagram Protocol, Src Port: 1109 (1109), Dst Port: **3544** (3544)

No. Time Source Destination Protocol Info
29 37.593598 **fe80::8000:ffff:ffff:fffd** **ff02::2** ICMPv6 **Router solicitation**
Internet Protocol, Src: **172.16.1.103** (172.16.1.103), Dst: **65.54.227.126** (65.54.227.126)

No. Time Source Destination Protocol Info
31 45.546052 **fe80::ffff:ffff:fffd** **ff02::2** ICMPv6 **Router solicitation**
Internet Protocol, Src: **172.16.1.103** (172.16.1.103), Dst: **65.54.227.127** (65.54.227.127)
User Datagram Protocol, Src Port: 1109 (1109), Dst Port: 3544 (3544)

No. Time Source Destination Protocol Info
32 46.039706 **fe80::8000:f227:bec9:1c81** **fe80::ffff:ffff:fffd** ICMPv6 **Router advertisement**
Internet Protocol, Src: **65.54.227.127** (65.54.227.127), Dst: **172.16.1.103** (172.16.1.103)
User Datagram Protocol, Src Port: 3544 (3544), Dst Port: 1109 (1109)
Teredo Origin Indication header
Origin UDP port: **1109**
Origin IPv4 address: **70.120.2.1** (70.120.2.1)
Prefix: **2001:0:4136:e37e::**

No. Time Source Destination Protocol Info
33 46.093832 **fe80::ffff:ffff:fffd** **ff02::2** ICMPv6 **Router solicitation**
Internet Protocol, Src: **172.16.1.103** (172.16.1.103), Dst: **65.54.227.126** (65.54.227.126)
User Datagram Protocol, Src Port: 1109 (1109), Dst Port: 3544 (3544)

No. Time Source Destination Protocol Info
34 46.398745 **fe80::8000:f227:bec9:1c81** **fe80::ffff:ffff:fffd** ICMPv6 **Router advertisement**
Internet Protocol, Src: **65.54.227.126** (65.54.227.126), Dst: **172.16.1.103** (172.16.1.103)
Teredo Origin Indication header
Origin UDP port: **1109**
Origin IPv4 address: **70.120.2.1** (70.120.2.1)
Prefix: **2001:0:4136:e37e::**

Send RS Cone Flag=1 (Cone NAT), every 4 seconds

If no reply, send Flag=0 (restricted NAT)

Receive RA with Origin header and prefix

Send RS to 2nd server to check for symmetric NAT

Compare 2nd RA—Origin port/address from 2nd server

What Happens on the Wire—3

No. Time Source Destination Protocol Info
82 139.258206 172.16.1.103 151.164.11.201 DNS **Standard query AAAA www.kame.net**

No. Time Source Destination Protocol Info
83 139.530547 151.164.11.201 172.16.1.103 DNS **Standard query response AAAA 2001:200:0:8002:203:47ff:fea5:3085**

No. Time Source Destination Protocol Info
96 148.960607 **2001:0:4136:e37e:0:fbaa:b97e:fe4e 2001:200:0:8002:203:47ff:fea5:3085 ICMPv6 Echo request**
Internet Protocol, Src: **172.16.1.103** (172.16.1.103), Dst: 6**5.54.227.126** (65.54.227.126)
User Datagram Protocol, Src Port: **1109** (1109), Dst Port: **3544** (3544)

No. Time Source Destination Protocol Info
97 149.405579 **fe80::8000:5445:5245:444f 2001:0:4136:e37e:0:fbaa:b97e:fe4e** IPv6 **IPv6 no next header**

Internet Protocol, Src: **65.54.227.126** (65.54.227.126), Dst: **172.16.1.103** (172.16.1.103)
Teredo IPv6 over UDP tunneling
Teredo Origin Indication header
Origin UDP port: **50206**
Origin IPv4 address: **66.117.47.227** (66.117.47.227)

No. Time Source Destination Protocol Info
98 149.405916 **172.16.1.103 66.117.47.227** UDP Source port: 1109 Destination port: 50206

No. Time Source Destination Protocol Info
99 149.463719 **66.117.47.227 172.16.1.103** UDP Source port: 50206 Destination port: 1109

No. Time Source Destination Protocol Info
100 149.464100 **172.16.1.103 66.117.47.227** UDP Source port: 1109 Destination port: 50206

No. Time Source Destination Protocol Info
101 149.789493 **66.117.47.227 172.16.1.103** UDP Source port: 50206 Destination port: 1109

DNS lookup

Response

ICMP to host via Teredo Server

Relay sends Bubble packet to client via server—client receives relay address-port

Packets to/ from IPv6 host and client traverse relay

……

According to MSFT, if Teredo is the only IPv6 path, AAAA query should not be sent—being researched:
http://msdn2.microsoft.com/en-us/library/aa965910.aspx

What Happens on the Wire—3 (Cont.)

```
Interface 7: Teredo Tunneling Pseudo-Interface

Addr Type  DAD State  Valid Life    Pref. Life   Address
---------  ---------- ------------ ------------ ----------------------------
Public     Preferred      infinite     infinite 2001:0:4136:e37e:0:fbaa:b97e:fe4e
Link       Preferred      infinite     infinite fe80::ffff:ffff:fffd
```

```
C:\>ping www.kame.net

Pinging www.kame.net [2001:200:0:8002:203:47ff:fea5:3085] with 32 bytes of data


Reply from 2001:200:0:8002:203:47ff:fea5:3085: time=829ms
Reply from 2001:200:0:8002:203:47ff:fea5:3085: time=453ms
Reply from 2001:200:0:8002:203:47ff:fea5:3085: time=288ms
Reply from 2001:200:0:8002:203:47ff:fea5:3085: time=438ms
```

Maintaining NAT Mapping

- Every 30 seconds (adjustable) clients send a single bubble packet to Teredo server to refresh NAT state

  Bubble packet = Used to create and maintain NAT mapping and consists of an IPv6 header with no IPv6 payload (Payload 59—No next header)

```
No.     Time        Source                                  Destination     Protocol Info
 35 46.399072   2001:0:4136:e37e:0:fbaa:b97e:fe4e        ff02::1         IPv6     IPv6 no next header

Frame 35 (82 bytes on wire, 82 bytes captured)
Ethernet II, Src: Foxconn_2d:a1:4e (00:15:58:2d:a1:4e), Dst: 01:00:5e:00:00:fd (01:00:5e:00:00:fd)
Internet Protocol, Src: 172.16.1.103 (172.16.1.103), Dst: 224.0.0.253 (224.0.0.253)
User Datagram Protocol, Src Port: 1109 (1109), Dst Port: 3544 (3544)
Teredo IPv6 over UDP tunneling
Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 0
    Next header: IPv6 no next header (0x3b)
    Hop limit: 21
    Source address: 2001:0:4136:e37e:0:fbaa:b97e:fe4e
    Destination address: ff02::1
```

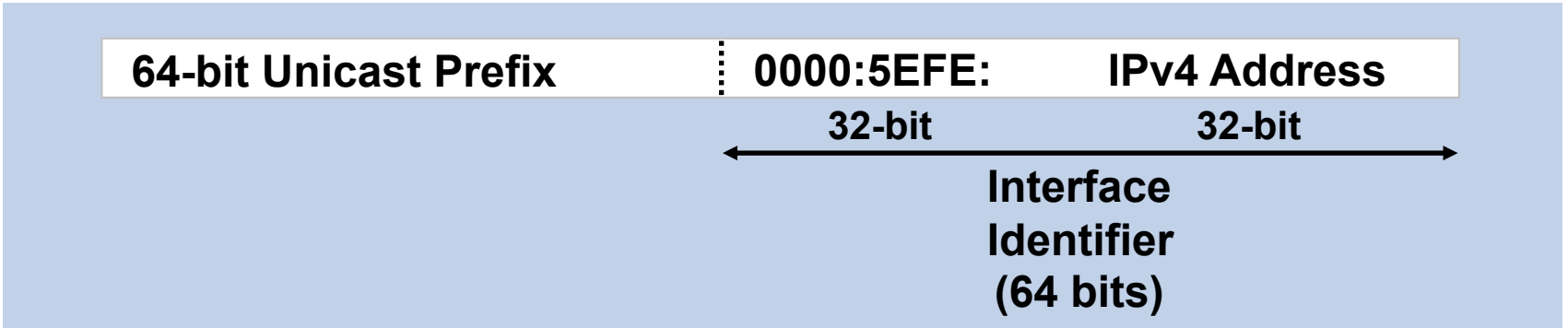
Appendix: ISATAP Overview

Intrasite Automatic Tunnel Address Protocol

- RFC 4214
- This is for enterprise networks such as corporate and academic networks
- Scalable approach for incremental deployment
- ISATAP makes your IPv4 infratructure as transport (NBMA) network

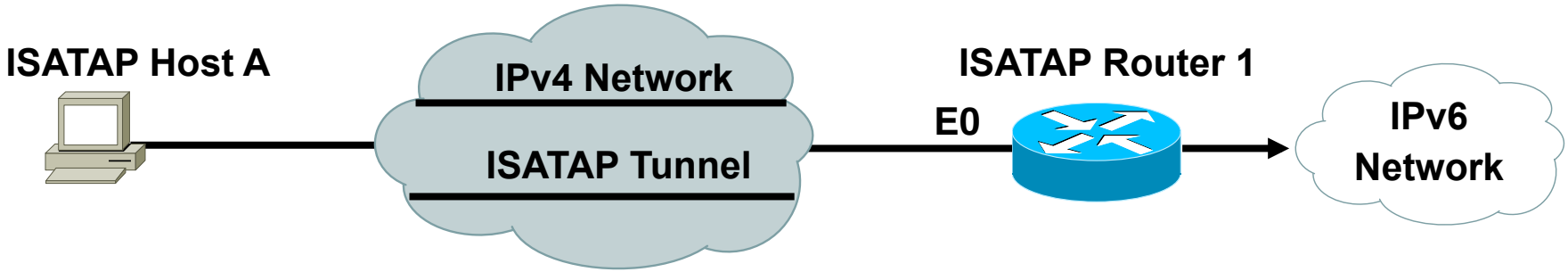
Intrasite Automatic Tunnel Address Protocol

Use IANA's OUI 00-00-5E and
Encode IPv4 Address as Part of EUI-64



- ISATAP is used to tunnel IPv4 within as administrative domain (a site) to create a virtual IPv6 network over a IPv4 network
- Supported in Windows XP Pro SP1 and others

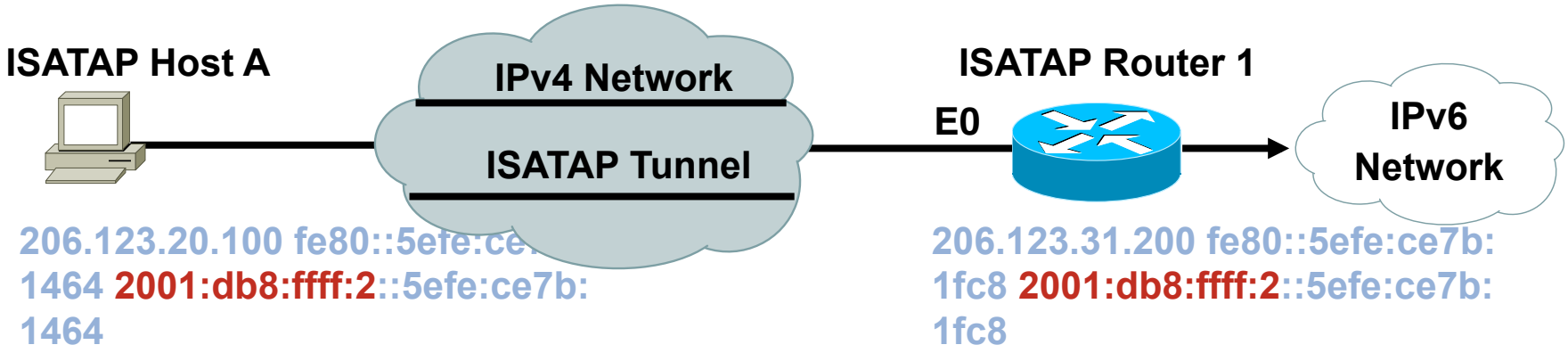
Automatic Advertisement of ISATAP Prefix



ICMPv6 Type 133 (RS)
IPv4 Source: 206.123.20.100
IPv4 Destination: 206.123.31.200
IPv6 Source: fe80::5efe:ce7b:1464
IPv6 Destination: fe80::5efe:ce7b:1fc8
Send me ISATAP Prefix

ICMPv6 Type 134 (RA)
IPv4 Source: 206.123.31.200
IPv4 Destination: 206.123.20.100
IPv6 Source: fe80::5efe:ce7b:1fc8
IPv6 Destination: fe80::5efe:ce7b:1464
ISATAP Prefix: 2001:db8:ffff :2::/64

Automatic Address Assignment of Host and Router



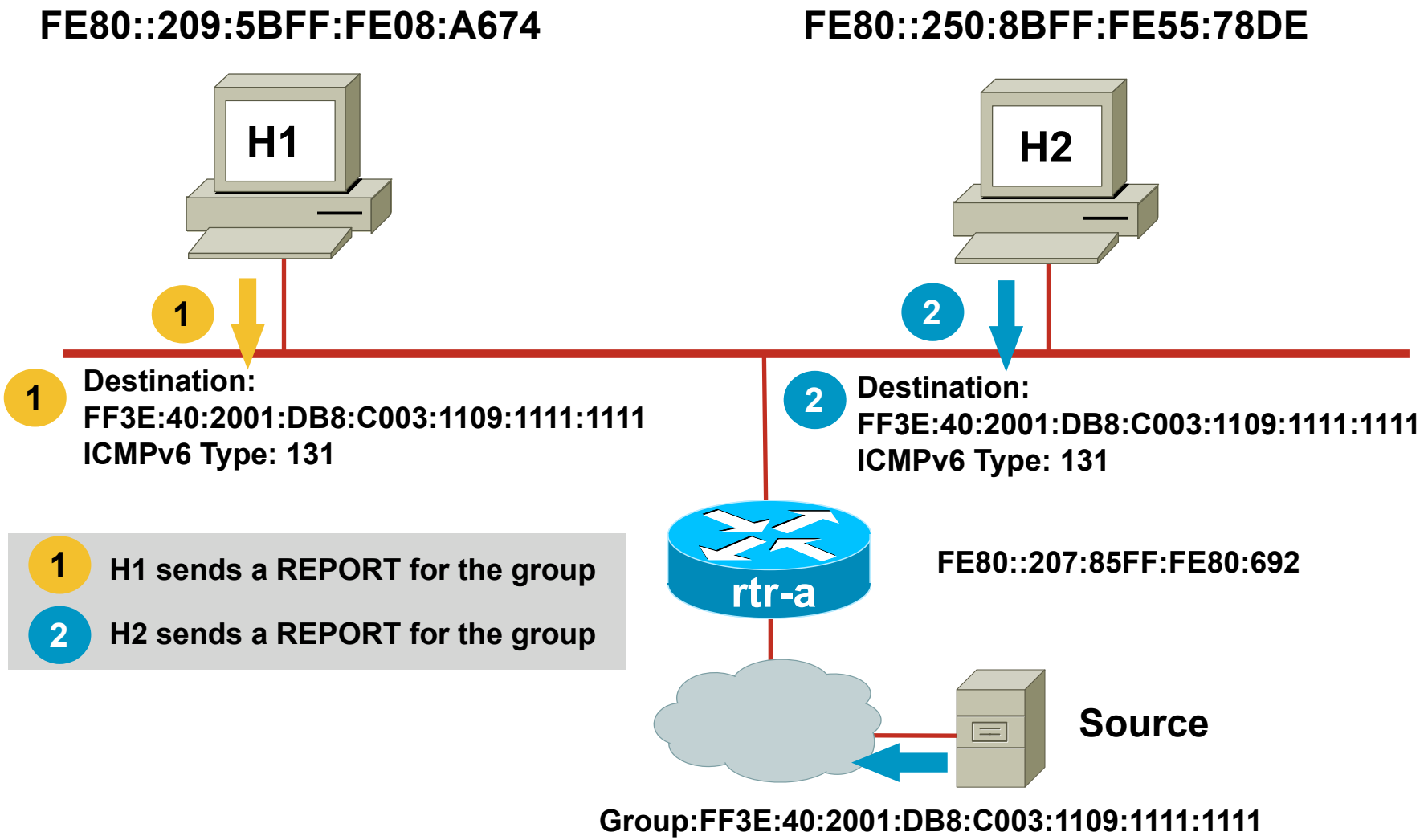
- ISATAP host A receives the ISATAP prefix 2001:db8:ffff:2::/64 from ISATAP Router 1
- When ISATAP host A wants to send IPv6 packets to 2001:db8:ffff:2::5efe:ce7b:1fc8, ISATAP host A encapsulates IPv6 packets in IPv4. The IPv4 packets of the IPv6 encapsulated packets use IPv4 source and destination address.

Appendix: Multicast

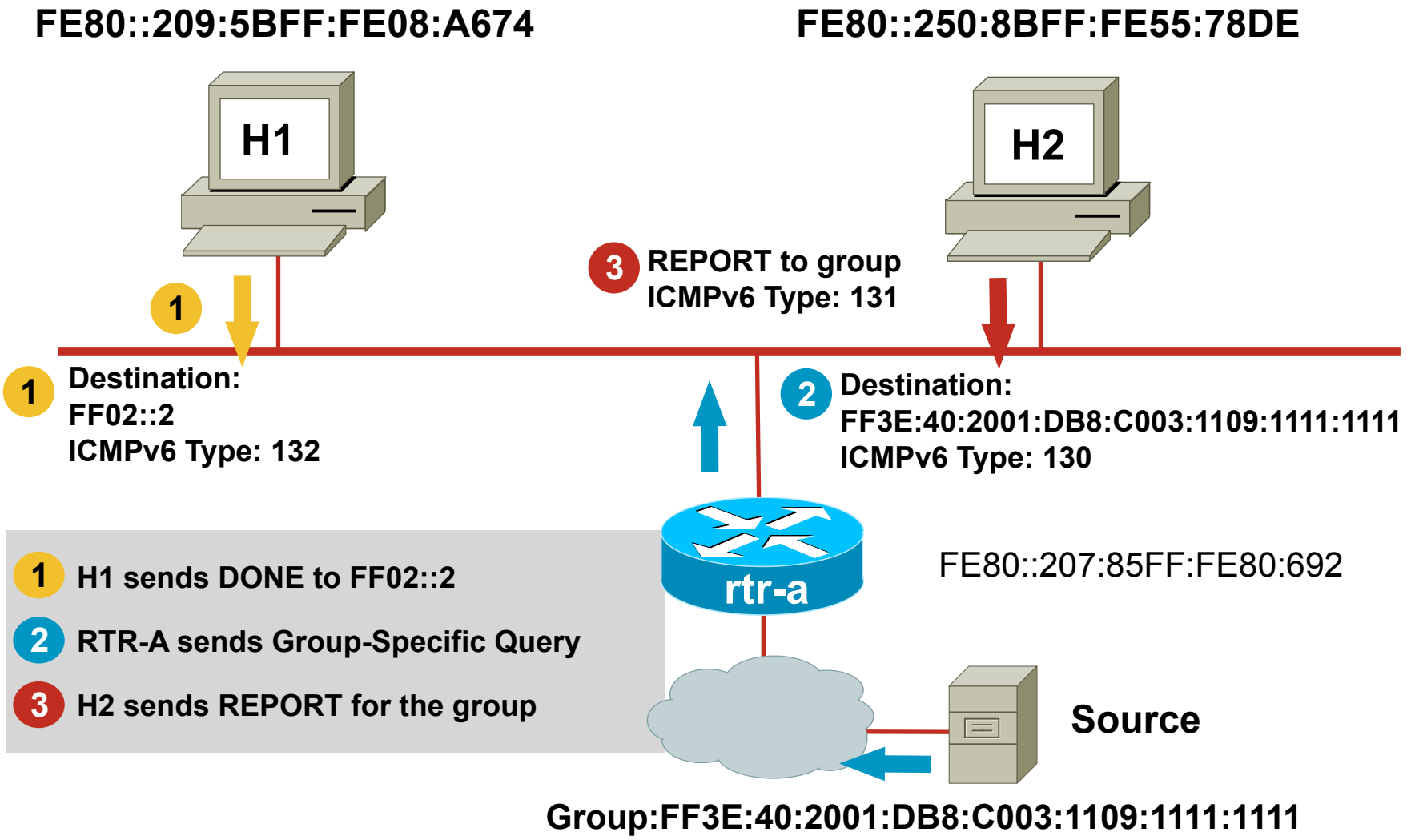
IPv4 and IPv6 Multicast Comparison

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

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)

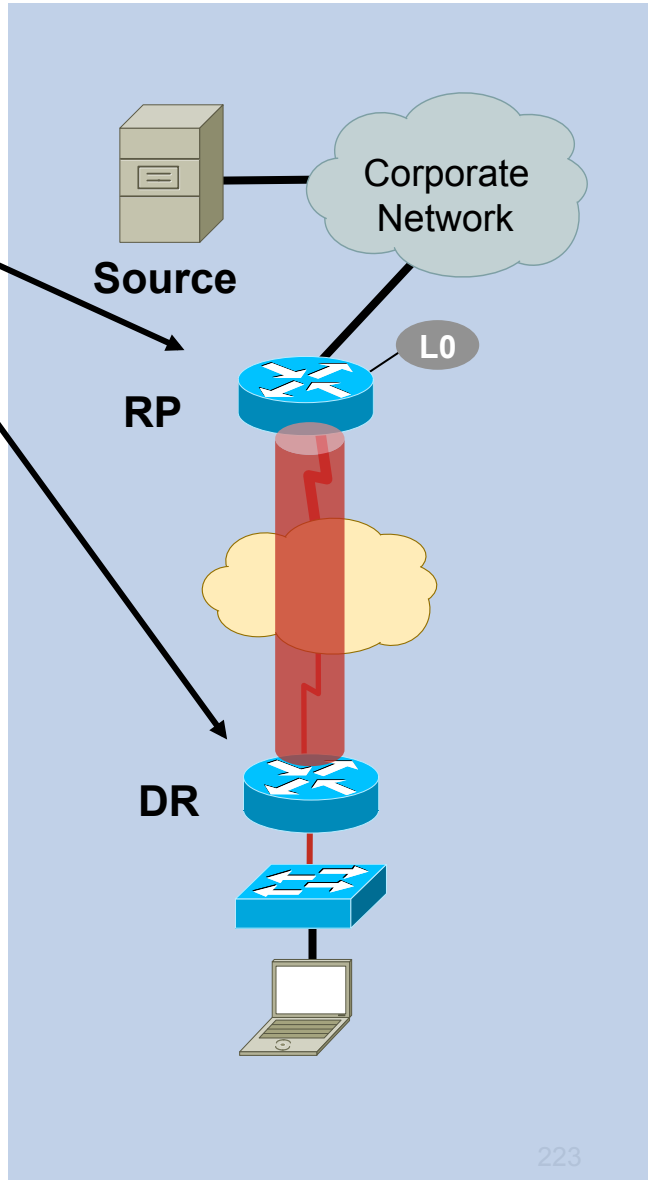
A Few Notes on Tunnels…

- PIM uses tunnels when RPs/sources are known
- Source registering (on first-hop router)
  - Uses virtual tunnel interface (appear in OIL for [S,G])
  - Created automatically on first-hop router when RP is known
  - Cisco IOS® keeps tunnel as long as RP is known
  - Unidirectional (transmit only) tunnels
  - PIM Register-Stop messages are sent directly from RP to registering router (not through tunnel!)

PIM Tunnels (DR-to-RP)

```
branch#show ipv6 pim tunnel
Tunnel1*
  Type   : PIM Encap
  RP     : 2001:DB8:C003:1116::2
  Source: 2001:DB8:C003:111E::2
```

```
branch#show interface tunnel 1
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 2001:DB8:C003:111E::2 (Serial0/2),
destination 2001:DB8:C003:1116::2
  Tunnel protocol/transport PIM/IPv6, key disabled,
sequencing disabled
  Checksumming of packets disabled
  Tunnel is transmit only
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
… output truncated…
```



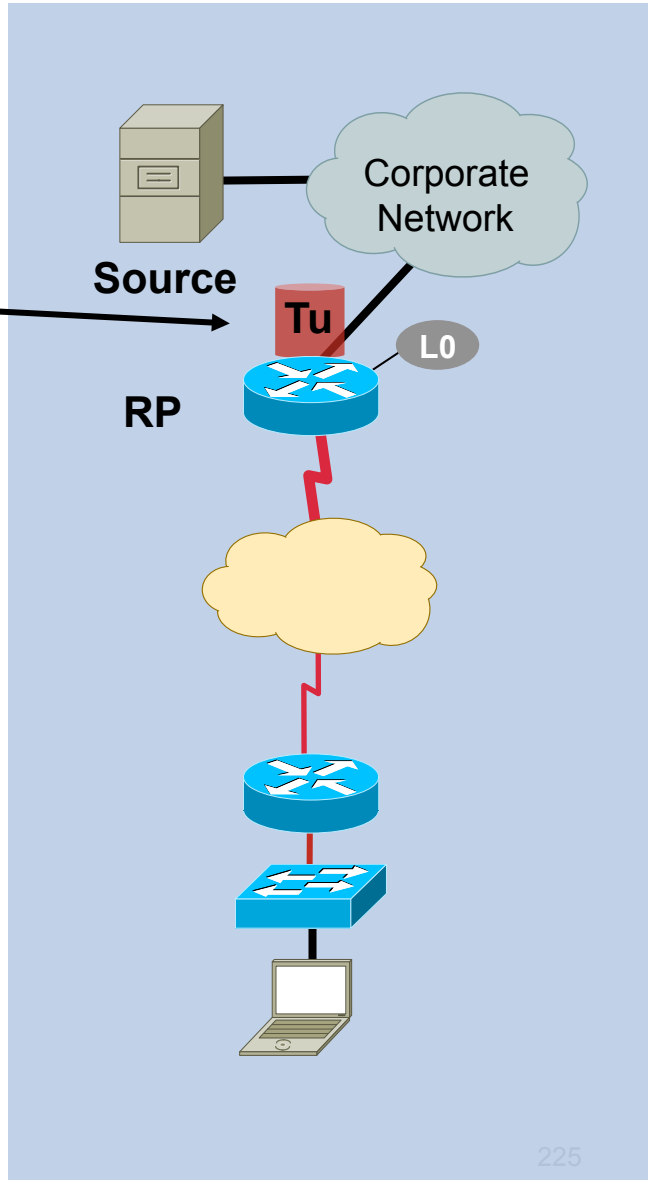
PIM Tunnels (RP)

- Source registering (on RP) → two virtual tunnels are created
  - One transmit only for registering sources locally connected to the RP
  - One receive only for decapsulation of incoming registers from remote designated routers
  - No one-to-one relationship between virtual tunnels on designated routers and RP!

PIM Tunnels (RP-for-Source)

```
RP-router#show ipv6 pim tunnel
Tunnel0*
  Type   : PIM Encap
  RP     : 2001:DB8:C003:1116::2
  Source: 2001:DB8:C003:1116::2
Tunnel1*
  Type   : PIM Decap
  RP     : 2001:DB8:C003:1116::2
  Source:  -
```

```
RP-router#show interface tunnel 1
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 2001:DB8:C003:1116::2
(FastEthernet0/0), destination 2001:DB8:C003:1116::2
  Tunnel protocol/transport PIM/IPv6, key disabled,
sequencing disabled
  Checksumming of packets disabled
  Tunnel is receive only

… output truncated…
```



Tunneling v6 Multicast

v6 in v4

- v6 in v4 most widely used

```
tunnel mode ipv6ip <----- IS-IS cannot traverse
```

- v6 in v4 GRE (IS-IS can traverse)

```
tunnel mode gre ip
```

- ISATAP/6to4 do not support IPv6 multicast

v6 in v6

- v6 in v6

```
tunnel mode ipv6
```

- v6 in v6 GRE

```
tunnel mode gre ipv6
```

Source Specific Multicast (SSM)

- **No** configuration required other than enabling

```
ipv6 multicast-routing
```

- SSM group ranges are automatically defined
- Requires MLDv2 on host or SSM Mapping feature

```
router#show ipv6 pim range-list
config SSM Exp: never Learnt from : ::
  FF33::/32 Up: 1d00h
  FF34::/32 Up: 1d00h
  FF35::/32 Up: 1d00h
  FF36::/32 Up: 1d00h
  FF37::/32 Up: 1d00h
  FF38::/32 Up: 1d00h
  FF39::/32 Up: 1d00h
  FF3A::/32 Up: 1d00h
  FF3B::/32 Up: 1d00h
  FF3C::/32 Up: 1d00h
  FF3D::/32 Up: 1d00h
  FF3E::/32 Up: 1d00h
  FF3F::/32 Up: 1d00h
```

SSM-Mapping

- Delay in SSM deployment (both IPv4 and IPv6) is based mainly on lack of IGMPv3 and MLDv2 availability on the endpoints
- SSM-Mapping allows for the deployment of SSM in the network infrastructure without requiring MLDv2 (for IPv6) on the endpoint
- SSM-Mapping enabled router will map MLDv1 reports to a source (which do not natively include the source like with MLDv2)
  - Range of groups can be statically defined or used with DNS
  - Wildcards can be used to define range of groups

SSM-Mapping

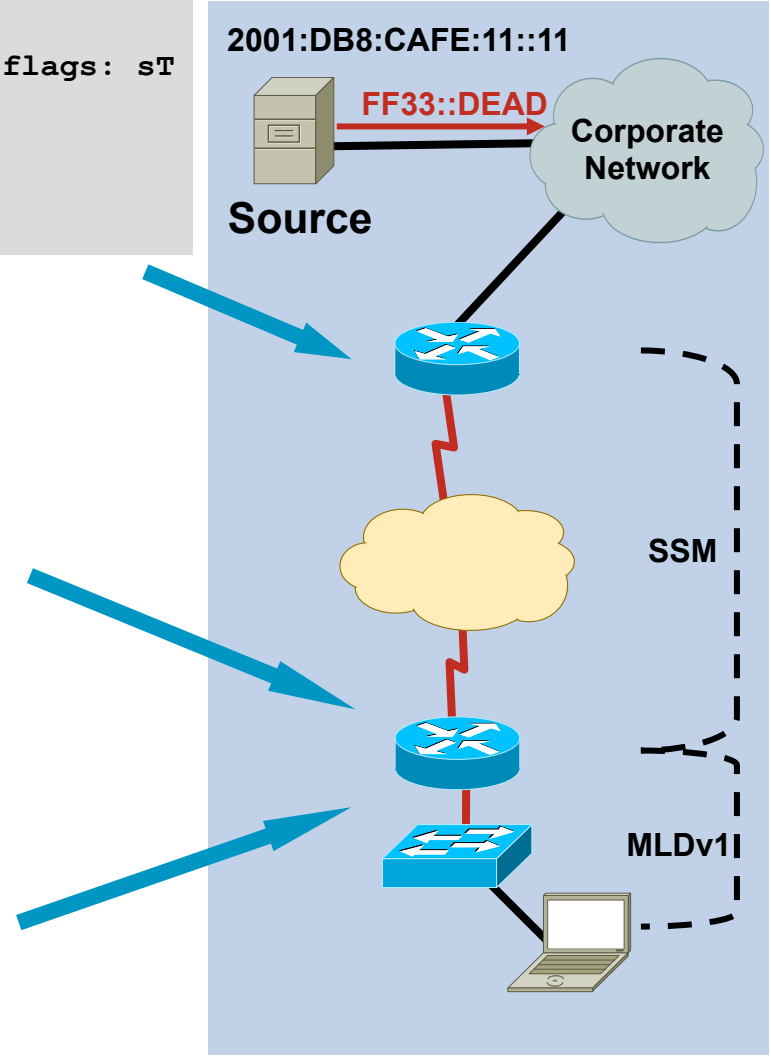
```
core-1#show ipv6 mroute | begin 2001:DB8:CAFE:11::11
(2001:DB8:CAFE:11::11, FF33::DEAD), 00:01:20/00:03:06, flags: sT
  Incoming interface: GigabitEthernet3/3
  RPF nbr: FE80::20E:39FF:FEAD:9B00
  Immediate Outgoing interface list:
    GigabitEthernet5/1, Forward, 00:01:20/00:03:06
```

Static Mapping:

```
ipv6 multicast-routing
!
ipv6 mld ssm-map enable
ipv6 mld ssm-map static MAP 2001:DB8:CAFE:11::11
no ipv6 mld ssm-map query dns
!
ipv6 access-list MAP
 permit ipv6 any host FF33::DEAD
```

DNS Mapping (the default):

```
ipv6 multicast-routing
!
ipv6 mld ssm-map enable
!
ip domain multicast ssm-map.cisco.com
ip name-server 10.1.1.1
```

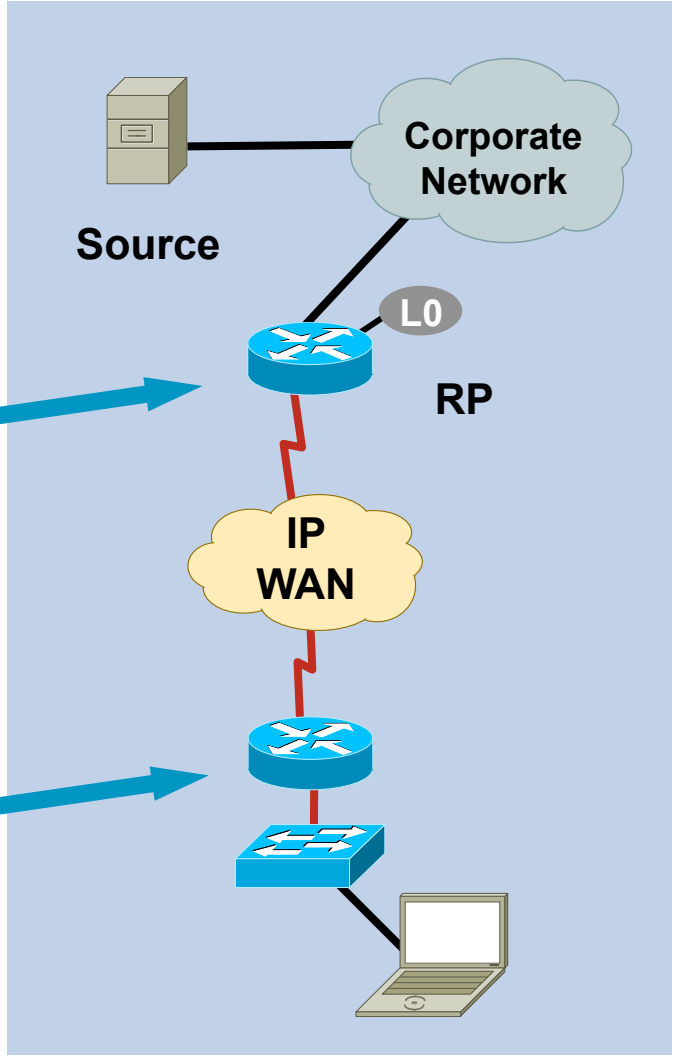


IPv6 Multicast Static RP

- Easier than before as PIM is auto-enabled on every interface

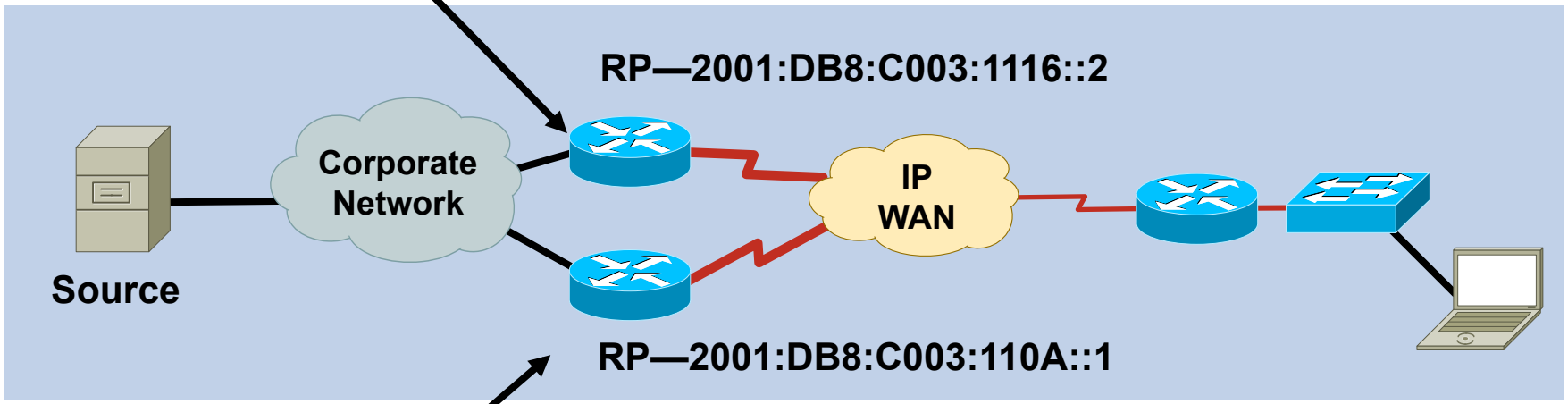
```
ipv6 multicast-routing
!
interface Loopback0
 description IPV6 IPmc RP
 no ip address
 ipv6 address 2001:DB8:C003:110A::1/64
!
ipv6 pim rp-address 2001:DB8:C003:110A::1/64
```

```
ipv6 multicast-routing
!
ipv6 pim rp-address 2001:DB8:C003:110A::1/64
```



IPv6 Multicast PIM BSR: Configuration

```
wan-top#sh run | incl ipv6 pim bsr

ipv6 pim bsr candidate-bsr 2001:DB8:C003:1116::2
ipv6 pim bsr candidate-rp 2001:DB8:C003:1116::2
```




```
wan-bottom#sh run | incl ipv6 pim bsr

ipv6 pim bsr candidate-bsr 2001:DB8:C003:110A::1
ipv6 pim bsr candidate-rp 2001:DB8:C003:110A::1
```

Bidirectional PIM (Bidir)

- The same many-to-many model as before
- Configure Bidir RP and range via the usual `ip pim rp-address` syntax with the optional `bidir` keyword

```
!
ipv6 pim rp-address 2001:DB8:C003:110A::1 bidir
!
#show ipv6 pim range | include BD

Static BD RP: 2001:DB8:C003:110A::1 Exp: never Learnt from : ::
```

Embedded-RP Addressing Overview

- RFC 3956
- Relies on a subset of RFC3306—IPv6 unicast-prefix-based multicast group addresses with special encoding rules:

  Group address carries the RP address for the group!

8	4	4	4	4	8	64	32
FF	Flags	Scope	Rsvd	RPaddr	Plen	Network Prefix	Group ID

New Address format defined :

Flags = 0RPT, R = 1, P = 1, T = 1=> RP address embedded

(0111 = 7)

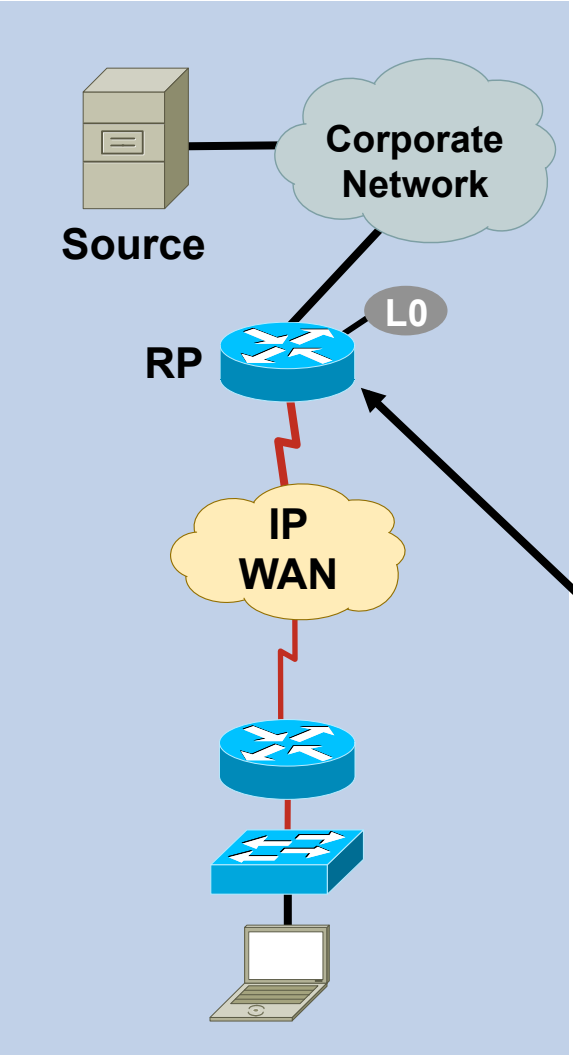
Example Group: FF7E:0140:2001:0DB8:C003:111D:0000:1112

Embedded RP: 2001:0DB8:C003:111D::1

Embedded-RP

- PIM-SM protocol operations with embedded-RP:
  - Intradomain transition into embedded-RP is easy:
    - Non-supporting routers simply need to be configured statically or via BSR for the embedded-RPs!
- Embedded-RP is just a method to learn ONE RP address for a multicast group:
  - It can not replace RP-redundancy as possible with BSR or MSDP/Anycast-RP
- Embedded-RP does not (yet) support Bidir-PIM
  - Simply extending the mapping function to define Bidir-PIM RPs is not sufficient:
    - In Bidir-PIM routers carry per-RP state (DF per interface) prior to any data packet arriving; this would need to be changed in Bidir-PIM if Embedded-RP was to be supported

Embedded-RP Configuration Example



- RP to be used as an Embedded-RP needs to be configured with address/ group range
- All other non-RP routers require no special configuration

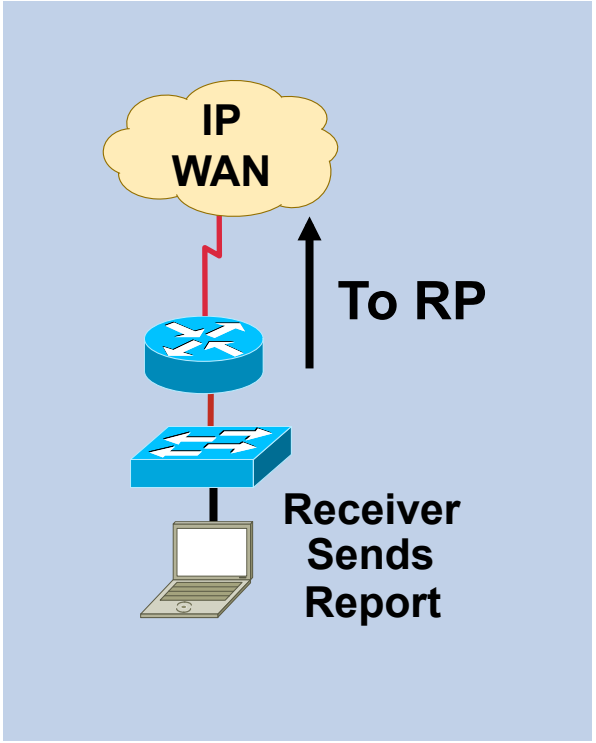
```
ipv6 pim rp-address 2001:DB8:C003:111D::1 ERP
!
ipv6 access-list ERP
 permit ipv6 any FF7E:140:2001:DB8:C003:111D::/96
```

Embedded RP—Does It Work?

```
branch#show ipv6 pim group

FF7E:140:2001:DB8:C003:111D ::/96*
    RP       : 2001:DB8:C003:111D::1
    Protocol: SM
    Client   : Embedded
    Groups   : 1
    Info     : RPF: Se0/0.1,FE80::210:7FF:FEDD:40
```

```
branch#show ipv6 mroute active

Active IPv6 Multicast Sources - sending >= 4 kbps
Group: FF7E:140:2001:DB8:C003:111D:0:1112
  Source: 2001:DB8:C003:1109::2
    Rate: 21 pps/122 kbps(1sec), 124 kbps(last 100 sec)
```

```
branch#show ipv6 pim range | include Embedded

Embedded SM RP: 2001:DB8:C003:111D::1 Exp: never Learnt from : ::

 FF7E:140:2001:DB8:C003:111D::/96 Up: 00:00:24
```



Multicast Applications

- Microsoft Windows Media Server/Player (9 -11)
  http://www.microsoft.com/windows/windowsmedia/default.aspx
- VideoLAN
  www.videolan.org
- DVTS (Digital Video Transport System)
  http://www.sfc.wide.ad.jp/DVTS/http://www.dvts.jp/en/dvts.html
- Internet radio stations over IPv6
  http://www.ipv6.ecs.soton.ac.uk/virginradio/

  Supported on iTunes 4.5, Windows Media Player, XMMS 1.2.8, etc…
- Many more applications…Google is your friend :-)

Appendix: QoS

IPv6 QoS: Header Fields

- IPv6 traffic class

  Exactly the same as TOS field in IPv4

- IPv6 Flow Label (RFC 3697)

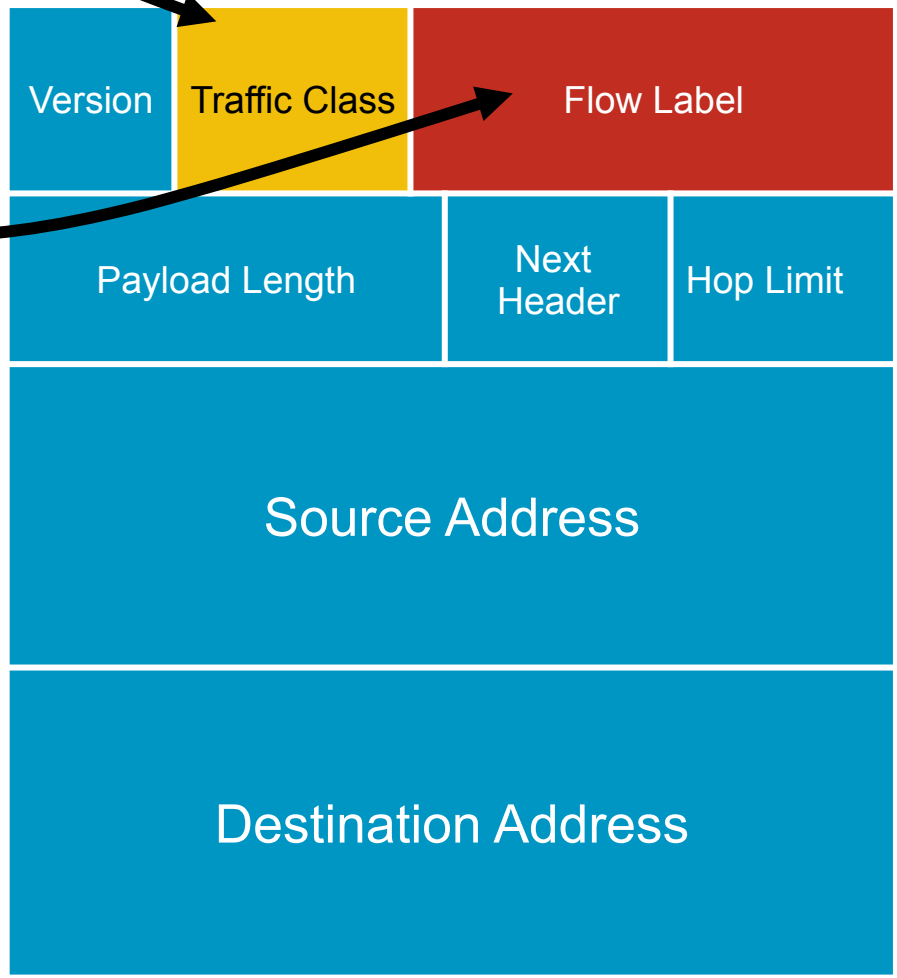
  A new 20-bit field in the IPv6 basic header which:

  Labels packets belonging to particular flows

  Can be used for special sender requests

  Per RFC, Flow Label must not be modified by intermediate routers

- Keep an eye out for work being doing to leverage the flow label

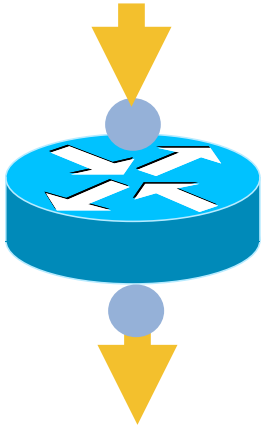


Simple QoS Example: IPv4 and IPv6

```
class-map match-any BRANCH-BULK-DATA
 match access-group name BULK-DATA-IPV6
 match access-group name BULK-DATA
class-map match-all BULK-DATA
 match  dscp af11
!
policy-map RBR-WAN-EDGE
 class BULK-DATA
  bandwidth percent 4
  random-detect
!
policy-map RBR-LAN-EDGE-IN
 class BRANCH-BULK-DATA
  set dscp af11
!
ip access-list extended BULK-DATA
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
!
ipv6 access-list BULK-DATA-IPV6
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
```

ACL Match To Set DSCP (If Packets Are Not Already Marked)

```
service-policy input RBR-LAN-EDGE-IN
```



```
service-policy output RBR-WAN-EDGE
```

ACLs to Match for Both IPv4 and IPv6 Packets