IPv6 Concepts

RST-1300

Why IPv6?

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

A Need for IPv6?

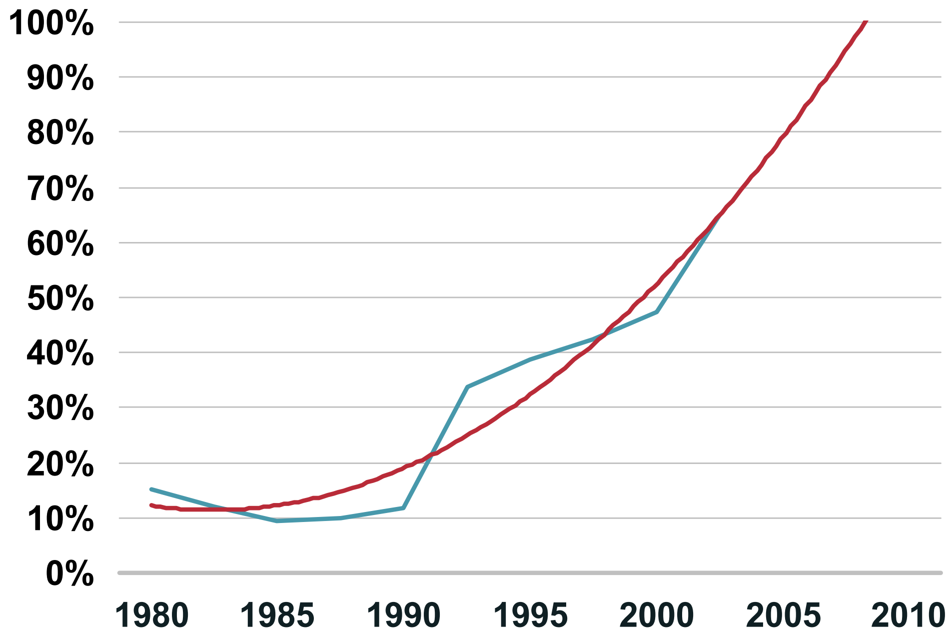
- **Internet population**
  - ~600M users in Q4 CY'01, ~945M by end CY'04—only 10–15% of the total population
  - How to address the future worldwide population? (~9B in CY'50)
  - Emerging Internet countries need address space, e.g.,
    - China uses nearly two class A (11/2001), ~20 class A needed if every student (320M) has to get an IP address
- **Mobile Internet introduces new generation of Internet devices**
  - PDA (~20M in 2004), mobile phones (~1.5B in 2003), tablet PC
  - Enable through several technologies, e.g., 3G, 802.11, etc.
- **Consumer, home and industrial appliances**

A Need for IPv6?

- **Transportation—mobile networks**
  - 1B automobiles forecast for 2008—begin now on vertical markets
  - Internet access on planes, e.g. Lufthansa—train, e.g. Narita express
- **Travelers flying on Lufthansa from Frankfurt, Germany to Washington, DC were among the first to try high-speed Internet access at 35,000 feet. The Boeing 747-400 jet equipped with a broadband network is esteemed to be the model for commercial airline travel in the future.**

IP Address Allocation History

1981	~ IPv4 Protocol Published
1985	~ 1/16 of Total Space
1990	~ 1/8 of Total Space
1995	~ 1/3 of Total Space
2000	~ 1/2 of Total Space
2001.5	~ 2/3 of Total Space



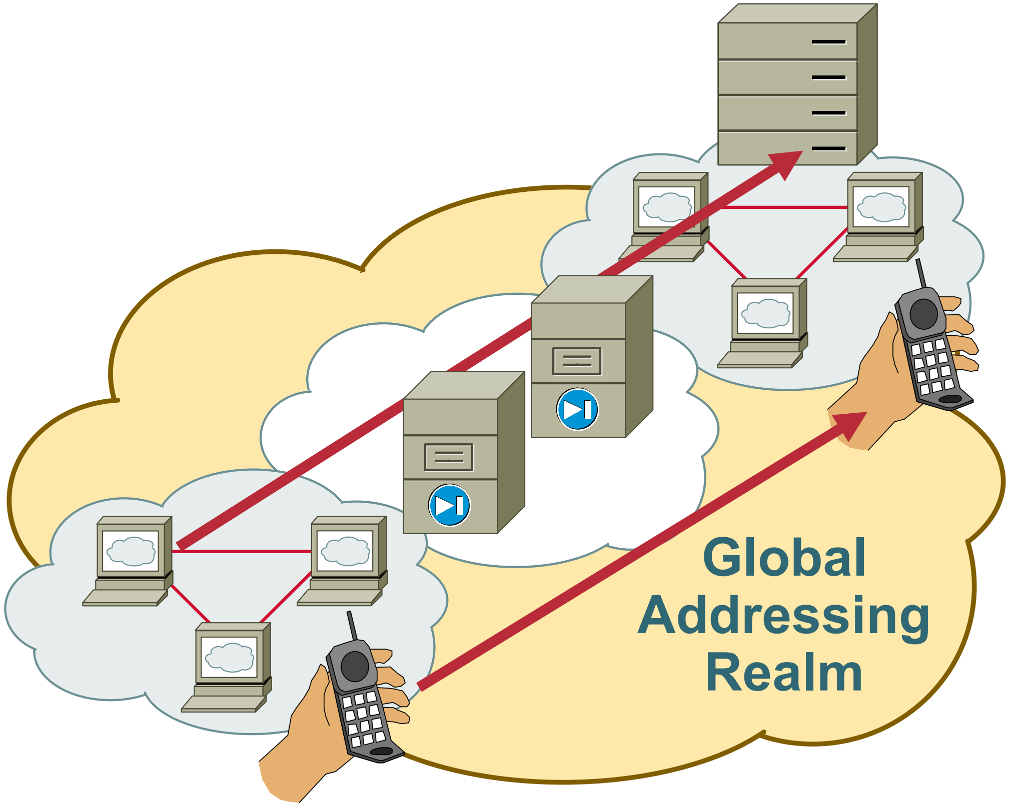
- **This despite increasingly intense conservation efforts**
  - PPP/DHCP address sharing
  - CIDR (classless inter-domain routing
  - NAT (network address translation)
  - plus some address reclamation
- **Theoretical limit of 32-bit space: ~4 billion devices**
  Practical limit of 32-bit space: ~250 million devices (RFC 3194)

Coming Back to an End-to-End Architecture

New Technologies/Applications for Home Users

"Always-On"—Cable, DSL, Ethernet-to-the-Home, Wireless, etc.

- Internet started with end-to-end connectivity for any applications
- Today, NAT and Application-Layer Gateways connect disparate networks
- Always-on devices need an address when you call them:
  - Mobile phones
  - Gaming
  - Residential Voice over IP gateway
  - IP fax



Why Not NAT

- Exhaustion of address space
- 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

IP—The Application's Convergence Layer

With Millions of New Devices Becoming IP Aware, the Need for Increased Addressing and Plug-and-Play Networking Is Only Met with the Implementation of IPv6

IPv6 Technology

IPv6 Features

- **Larger address space enabling:**

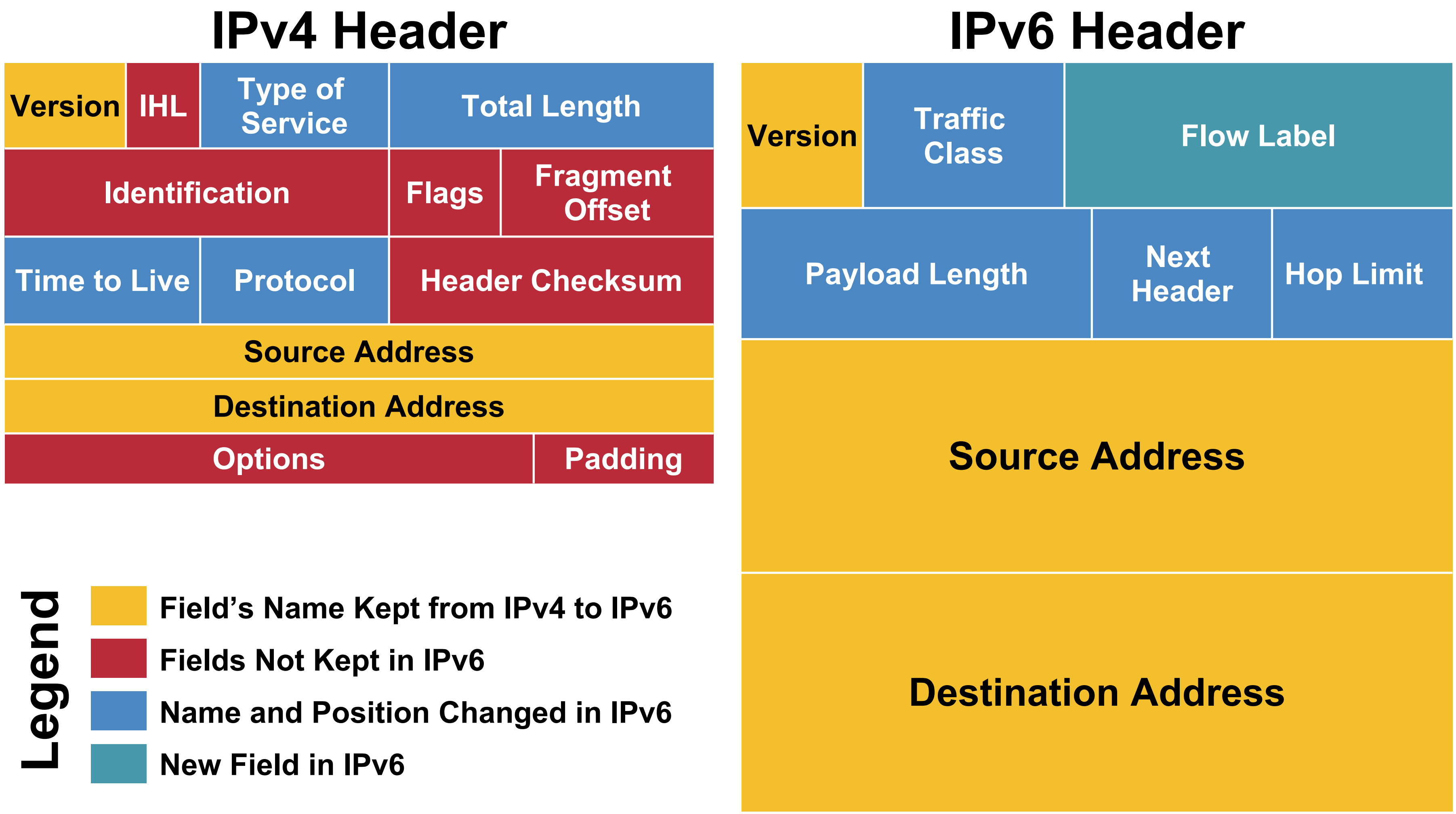
  Global reachability, flexibility, aggregation, multihoming, autoconfiguration, "plug and play" and renumbering

- **Simpler header enabling:**

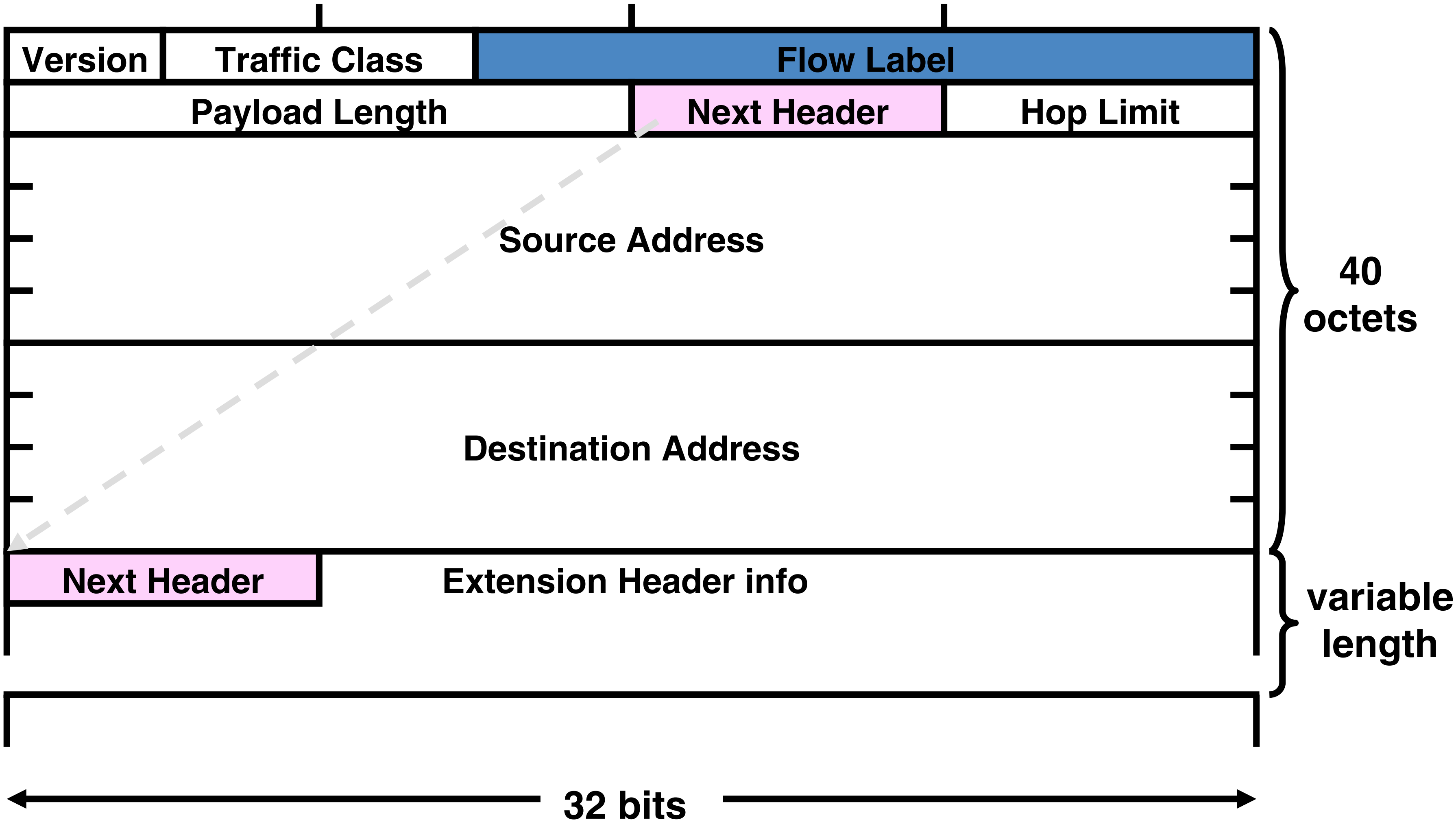
  Routing efficiency, performance and forwarding rate scalability

- **Improved option support**
- **Mandated security (global key yet to be defined)**
- **Transition richness**

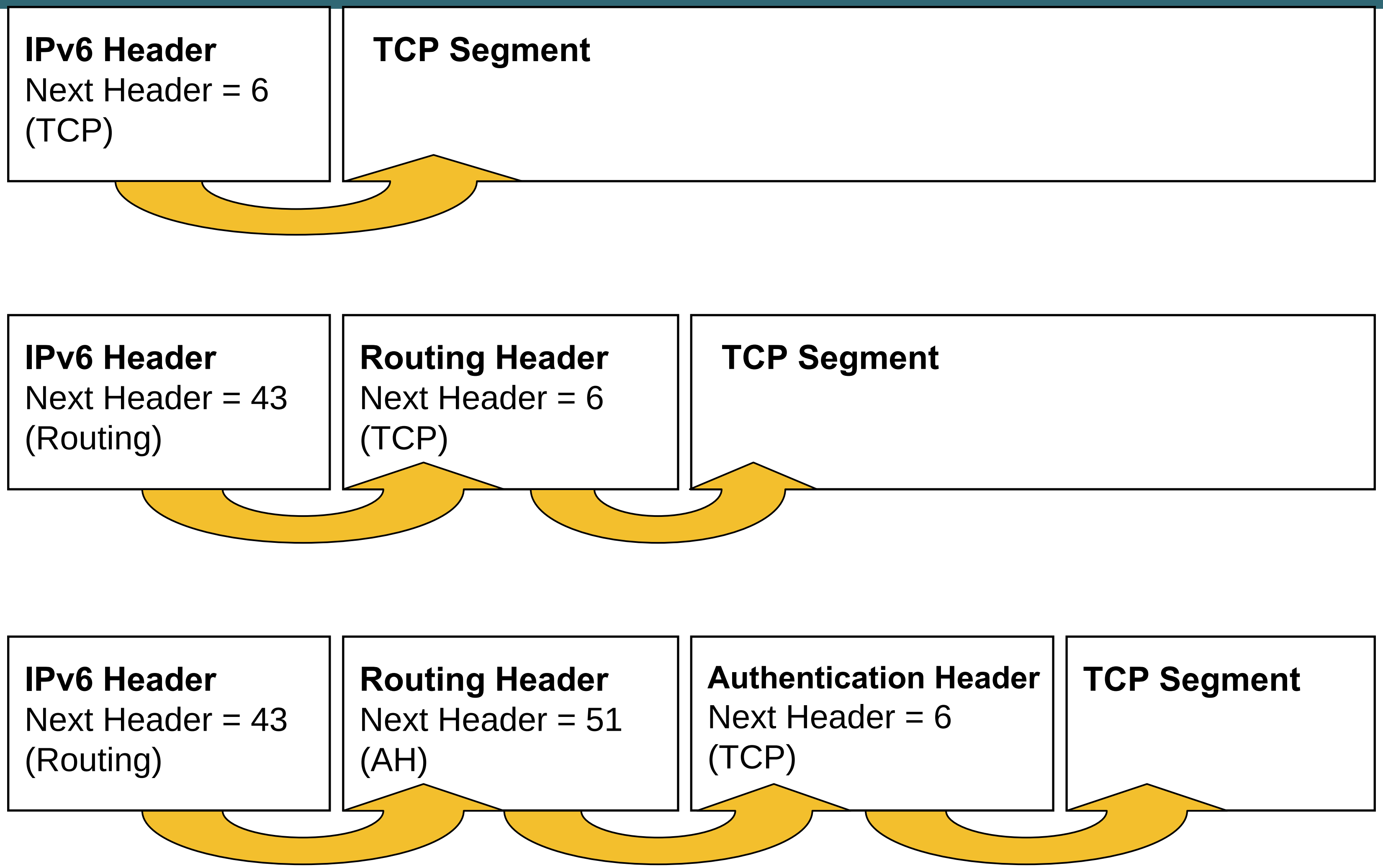
IPv4 and IPv6 Header Comparison



IPv6 Header Format



The Chain of Pointers Formed by the Next Header Field



IPv6 Protocol

- New field
- Flow label (RFC3697)

  Sequence of packets for which a source desires to label a flow

  Flow classifiers have 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.

  In IPv6: Only 3 tuple, flow label, source/destination address

MTU Issues

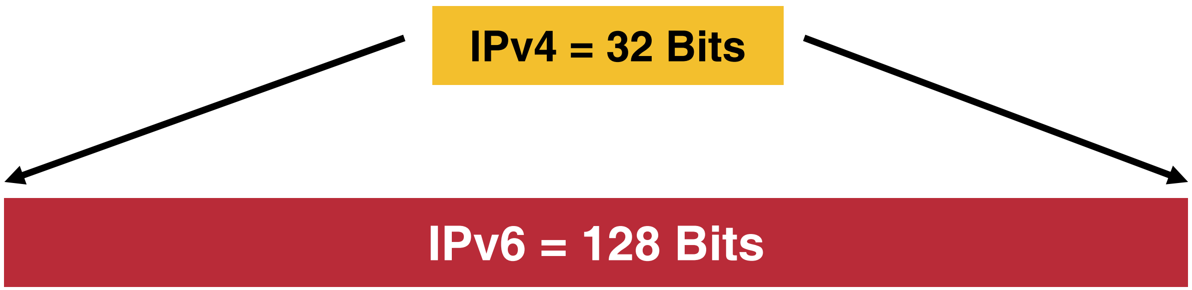
- **Minimum link MTU for IPv6 is 1280 octets (vs. 68 octets for IPv4)**

  => 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 2^{32} octets of payload**

Addressing

Larger Address Space



- **IPv4**

  32 bits

  =~ 4,200,000,000 possible addressable nodes

- **IPv6**

  128 bits

  = 340,282,366,920,938,463,463,374,607,431,768,211,456 nodes

Addressing

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:

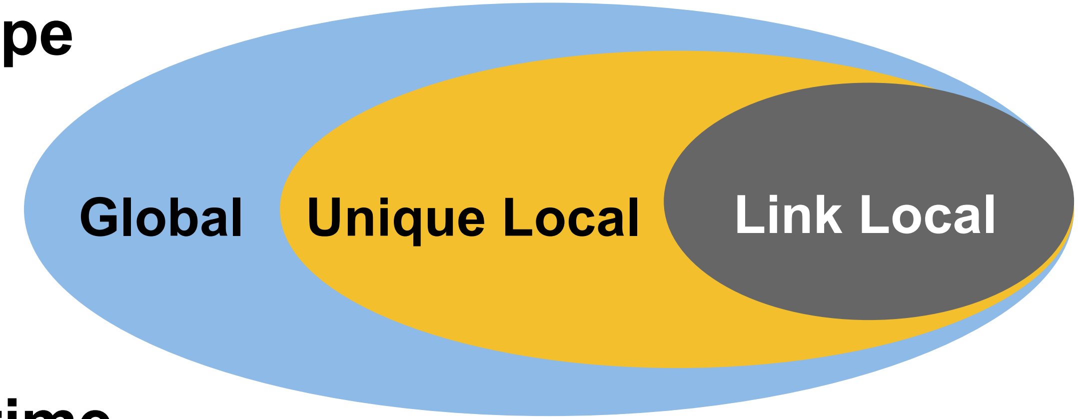
  198.10.0.0/16

- V6 address is represented the same way:

  2001:db8:12::/40

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**

Addressing

- **Some special addresses**

Type	Binary	Hex
Aggregatable Global Unicast Address	0010	2
Link Local Unicast Address	1111 1110 10	FE80::/10
Unique Local Unicast Address	1111 1100 1111 1101	FC00::/8 FD00::/8
Multicast Address	1111 1111	FF00::/16

Types of IPv6 Addresses

- **Unicast**

  Address of a single interface. One-to-one delivery to single interface

- **Multicast**

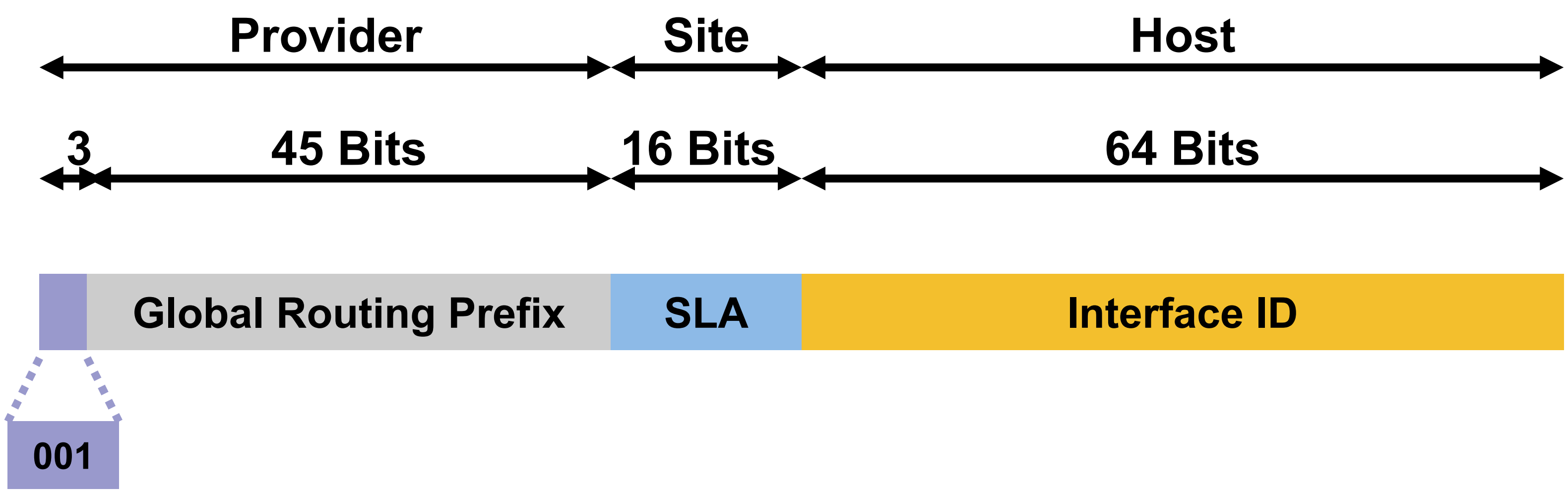
  Address of a set of interfaces. One-to-many delivery to all interfaces in the set

- **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**

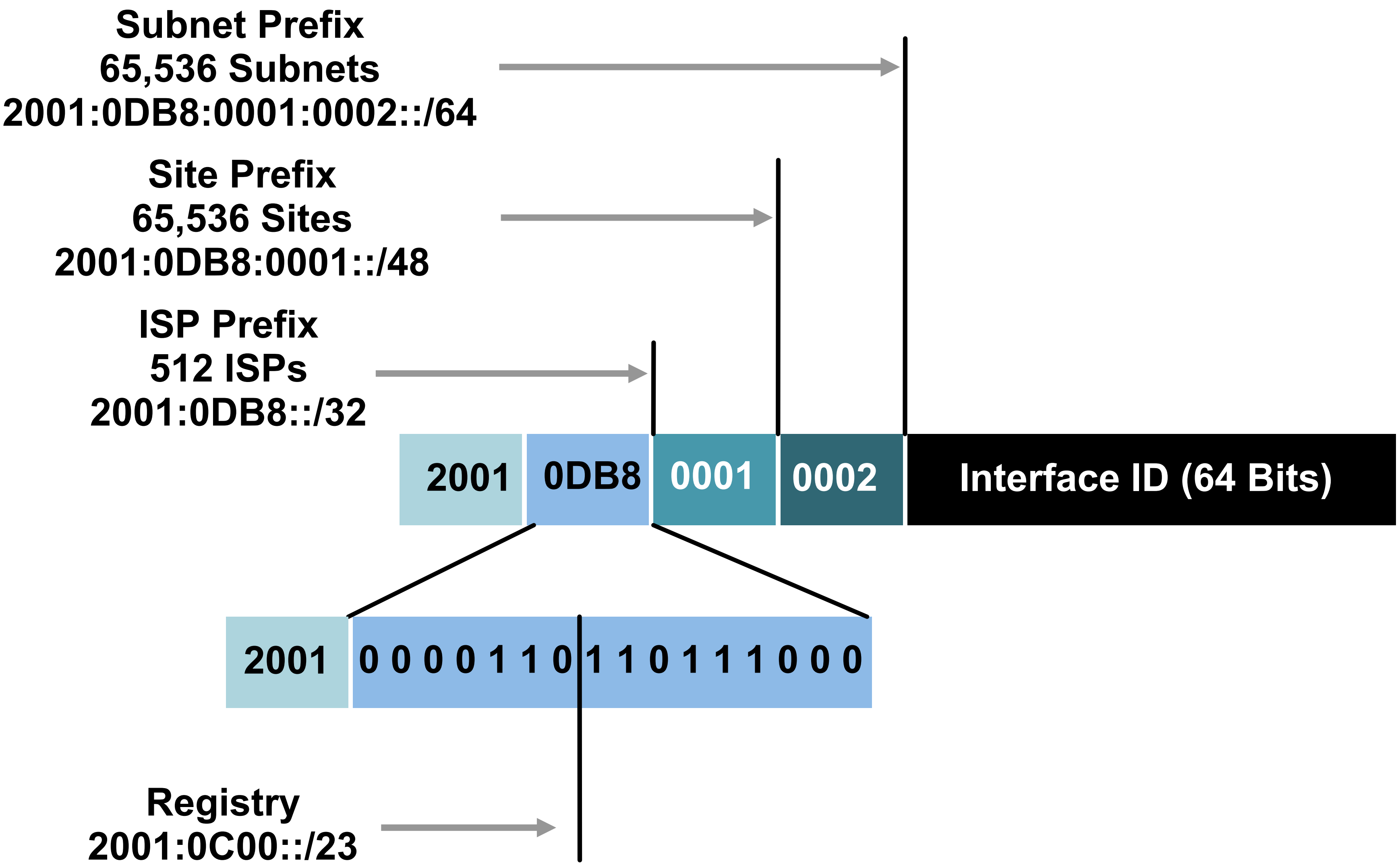
Aggregatable Global Unicast Addresses



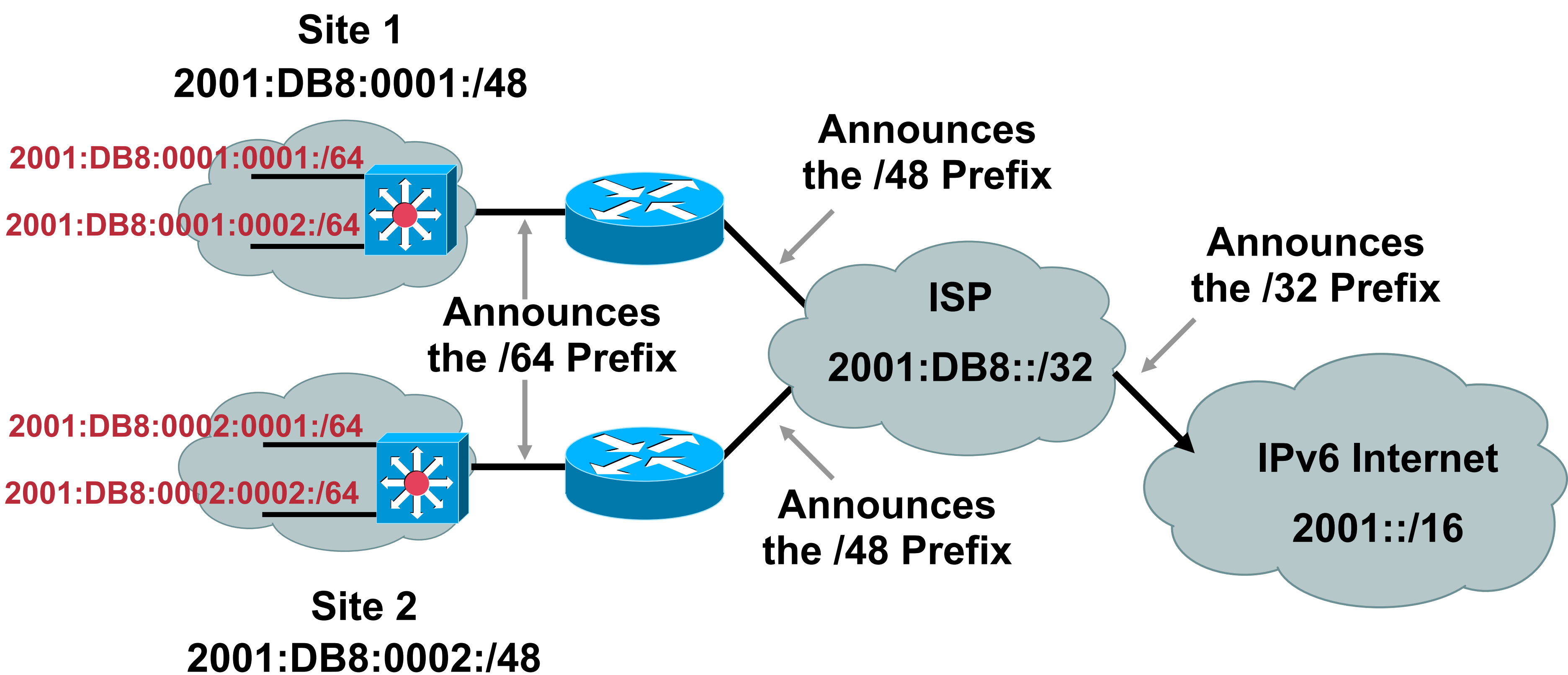
Aggregatable Global Unicast Addresses Are:

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

Hierarchical Addressing and Aggregation



Hierarchical Addressing and Aggregation



IPv6 Interface Identifier

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

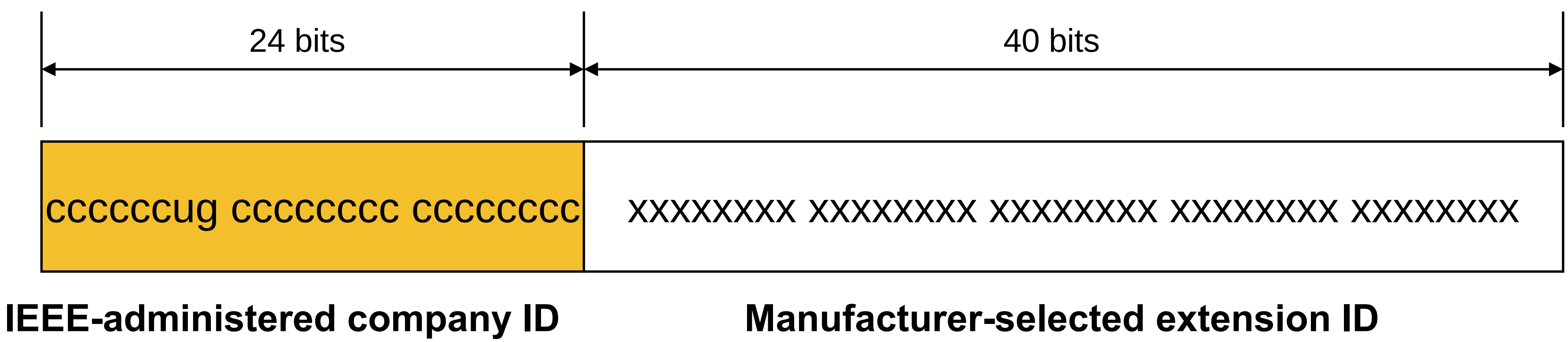
- **Cisco uses the EUI-64 format to do stateless auto-configuration**
- **This format expands the 48 bit MAC address to 64 bits by inserting FFFE into the middle 16 bits**
- **To make sure that the chosen address is from a unique Ethernet MAC address, the universal/local ("u" bit) is set to 1 for global scope and 0 for local scope**

IEEE EUI-64 Addresses

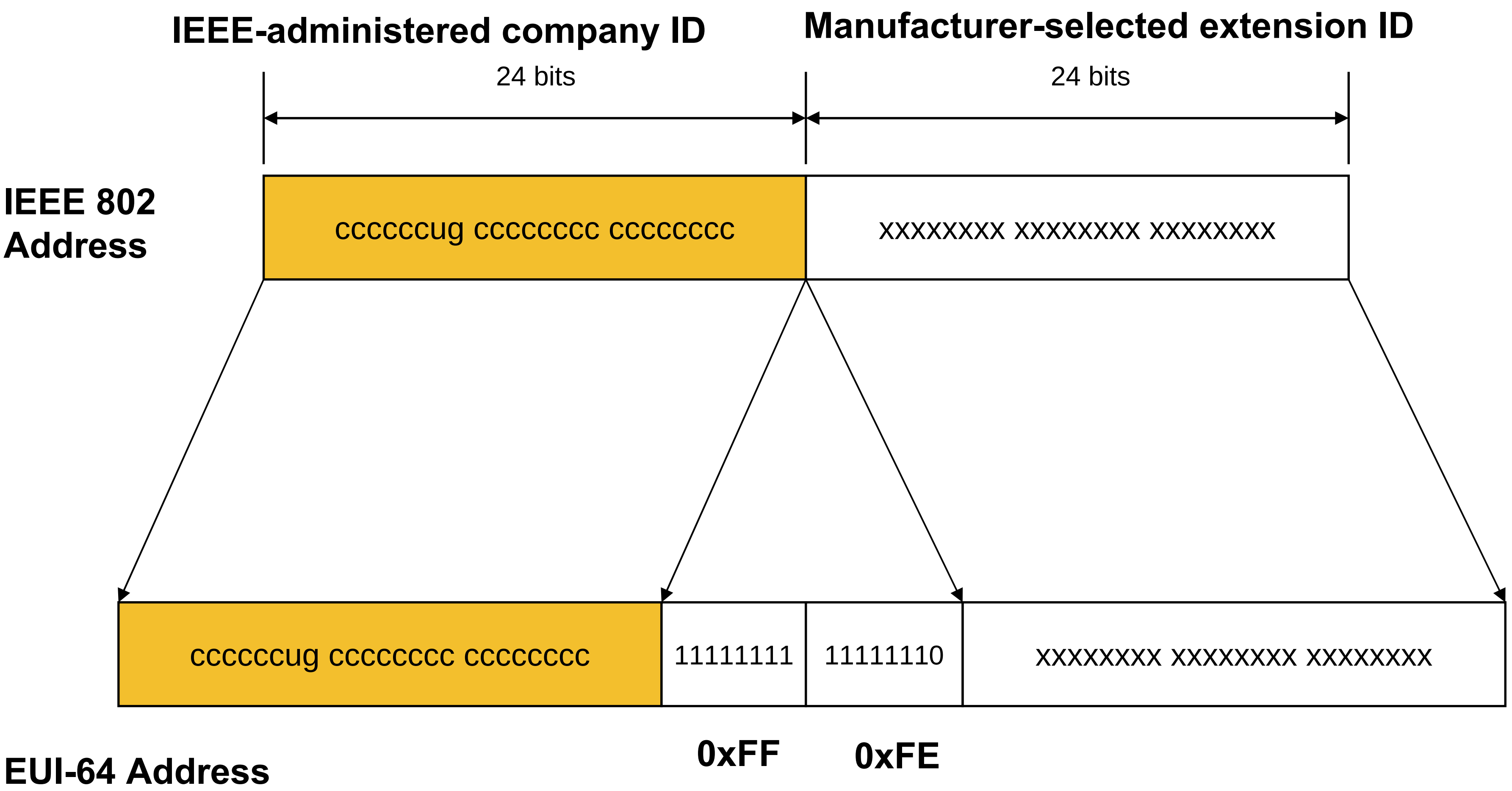
- **Extended Unique Identifier (EUI)**
- **Company ID - Extension ID**
- **U/L bit (u)**

  Universally (=0)/Locally (=1) Administered
- **U/G bit (g)**

  Unicast (=0)/Group (=1) Address



Conversion of an IEEE 802 Address to an EUI-64 Address



Aggregatable Global Unicast Addresses

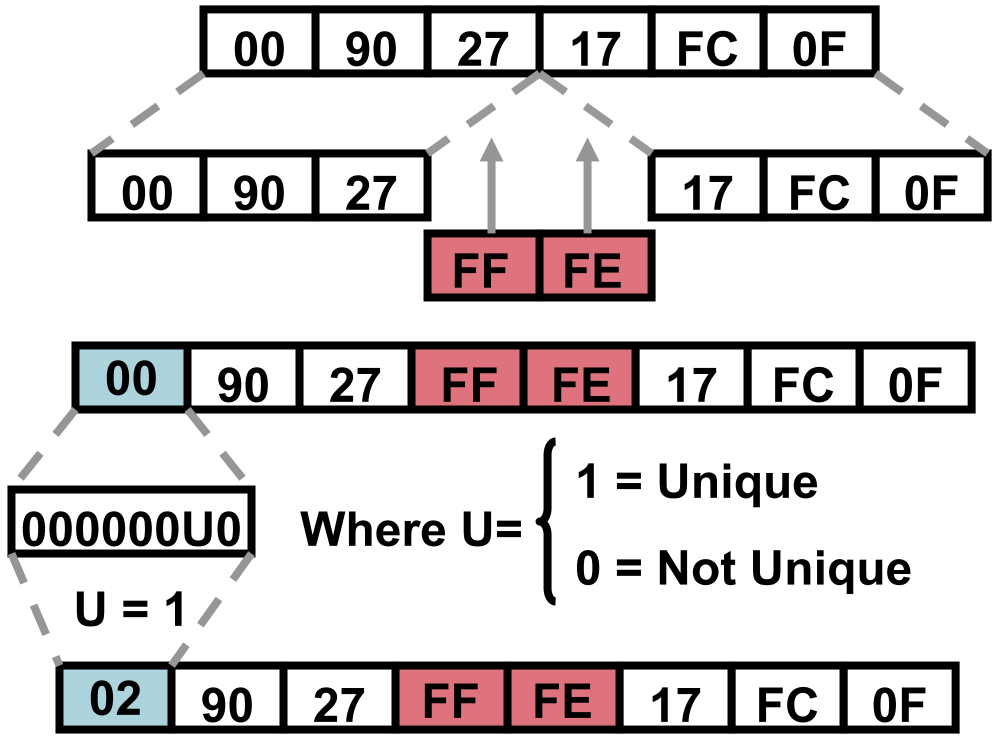
EUI-64

Ethernet MAC Address
(48 Bits)

64-Bits Version

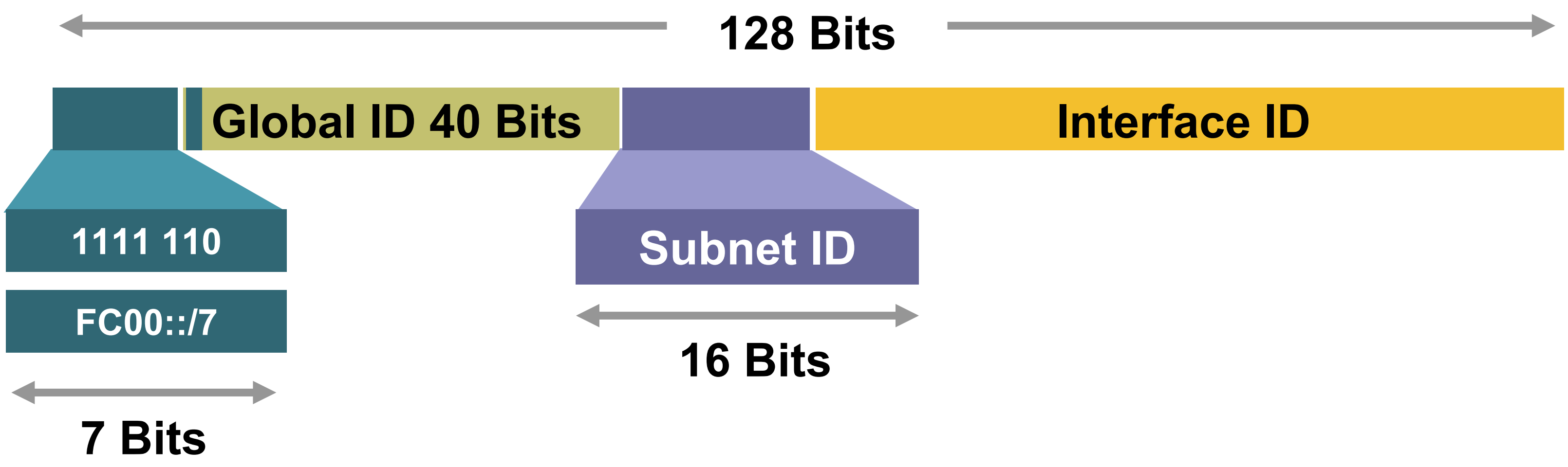
Uniqueness of the MAC

Eui-64 Address



- Eui-64 address: Insert “FFFE” in middle
- Invert ‘U’ bit to identify uniqueness of MAC

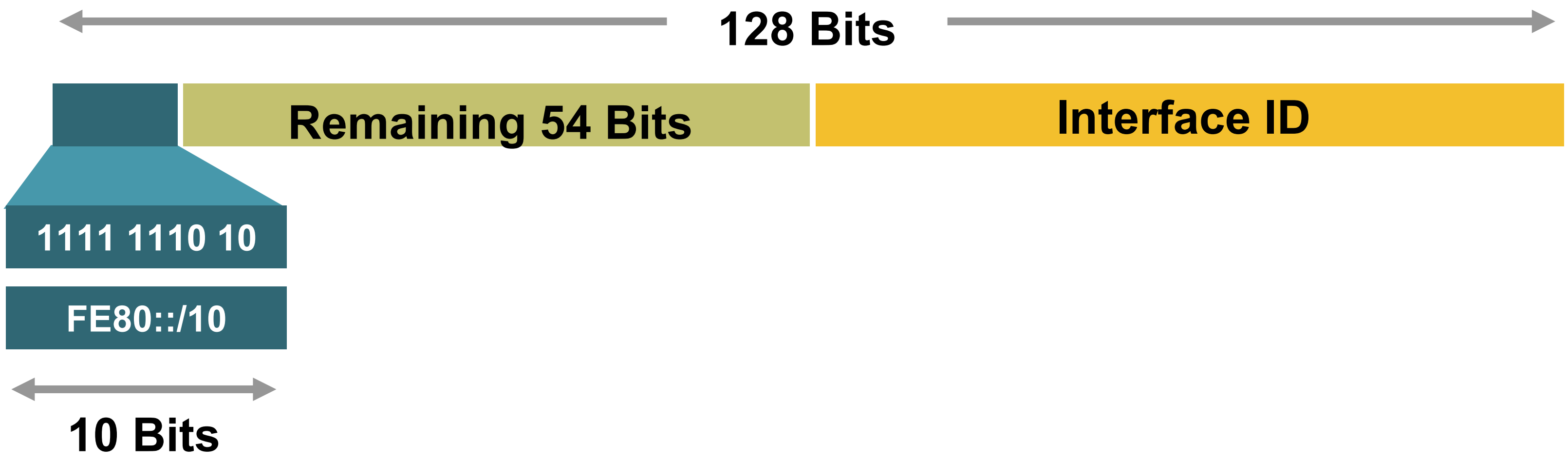
Unique-Local



Unique-Local Addresses Used For:

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

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

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

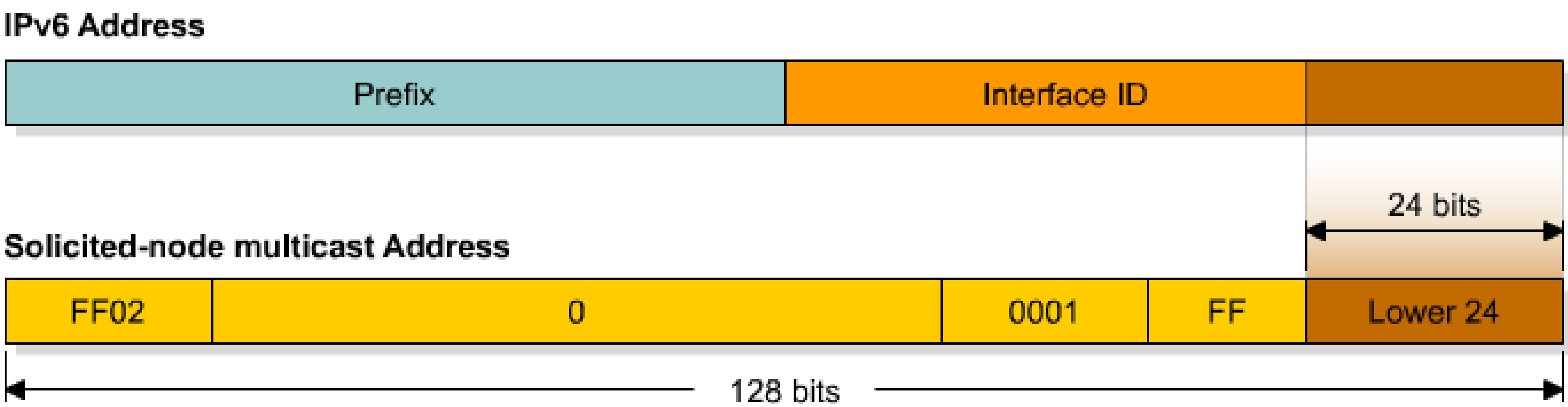
IPv6 Multicast Address

- The multicast address AllSPFRouters is FF02::5 note that 02 means that this is a permanent address and has link scope
- The multicast address ALLDRouters is FF02::6

Solicited-Node Multicast Address

- For each unicast and anycast address configured there is a corresponding solicited-node multicast
- This address is link local significance only
- This is specially used for two purpose, for the replacement of ARP, and DAD

Solicited-Node Multicast Address



- 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#
```

Solicited-Node Multicast Address

Anycast

Anycast Address Assignment

- 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 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

ICMPv6 and Neighbor Discovery

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** value of 58

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)

Neighbor Discovery

Router Solicitation

- Host send to inquire about presence of a router on the link
- Send to all routers multicast address of FF02::2 (all routers multicast address)
- Source IP address is either link local address or unspecified IPv6 address (::)

Router Solicitation and Advertisement

1—ICMP Type = 133 (RS)

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

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

Query = please send RA

2—ICMP Type = 134 (RA)

Src = link-local address (FE80::/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**

Neighbor Solicitation

- **Send to discover link layer address of IPv6 node**
- **For Layer 2 it is set to multicast for address resolution, unicast for node reachability**
- **IPv6 header, source address is set to unicast address of sending node, or :: for DAD**
- **Destination address is set to the unicast address for reachability and solicited node multicast for DAD**

Neighbor Advertisement

- **Response to neighbor solicitation message**
- **Also send to inform change of link layer address**

Neighbor Solicitation and Advertisement

Neighbor Solicitation:
ICMP type = 135
Src = A
Dst = Solicited-node multicast address of B
Data = link-layer address of A
Query = what is your link-layer 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

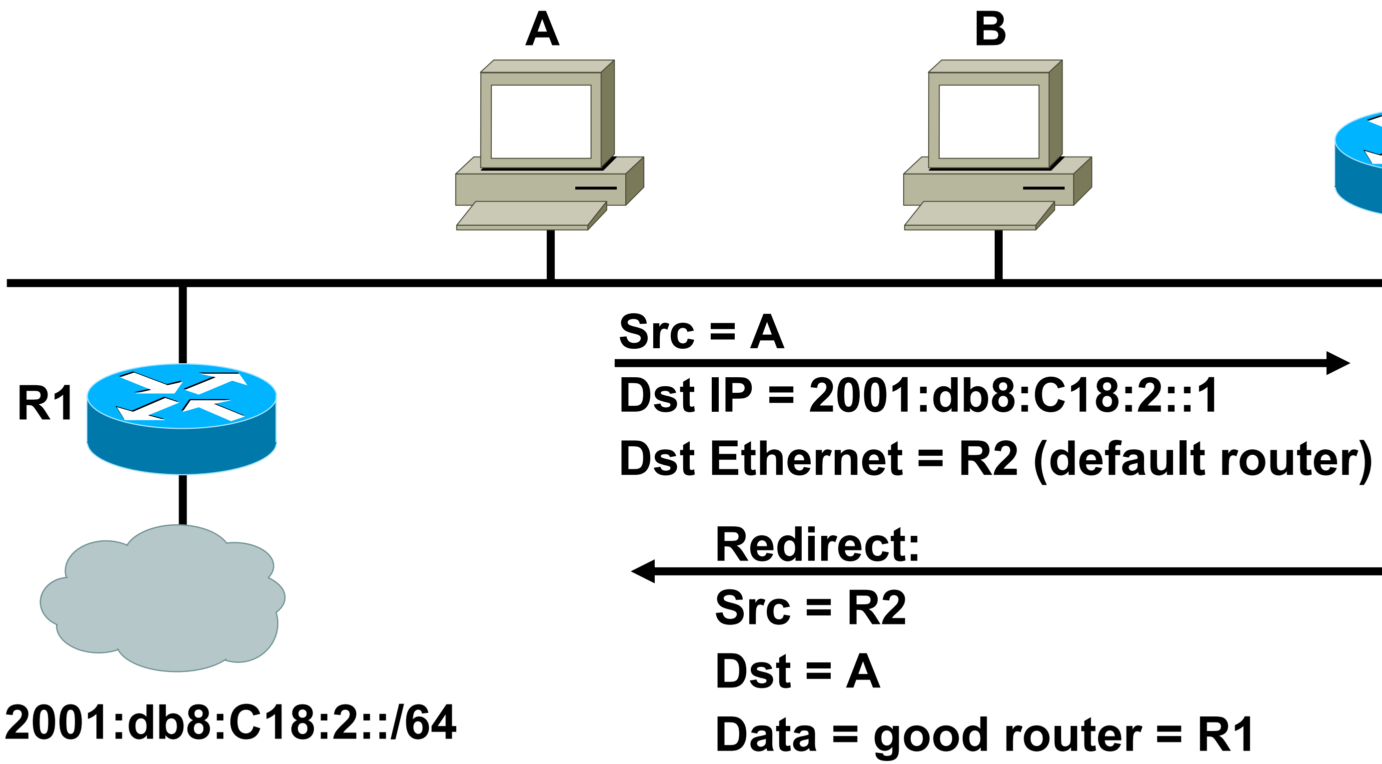
Viewing Neighbors in the Cache

```
R1#sho ipv6 neighbors
IPv6 Address                              Age Link-layer Addr State Interface
FE80::A8BB:CCFF:FE00:7800                   0 aabb.cc00.7800  STALE Et0/0
FE80::A8BB:CCFF:FE00:7A00                  50 aabb.cc00.7a00  STALE Et0/0
```

Neighbors are only considered “reachable” for 30-seconds. “Stale” indicates that, before we contact this neighbor, we will need to send a ND packet.

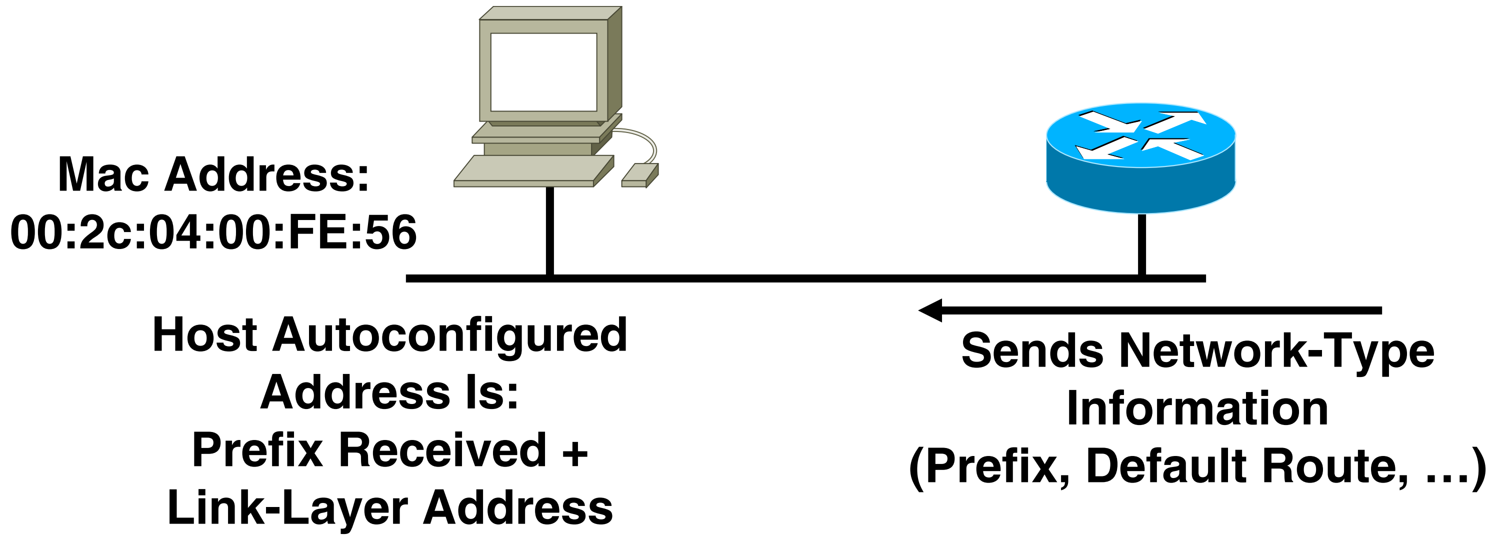
```
R1#ping ipv6
Target IPv6 address: FE80::A8BB:CCFF:FE00:7A00
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands? [no]:
Output Interface: Ethernet0/0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FE80::A8BB:CCFF:FE00:7A00, timeout is 2 second
s:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/24/32 ms
R1#sho ipv6 neighbors
IPv6 Address                              Age Link-layer Addr State Interface
FE80::A8BB:CCFF:FE00:7800                   3 aabb.cc00.7800  STALE Et0/0
FE80::A8BB:CCFF:FE00:7A00                   0 aabb.cc00.7a00  REACH Et0/0
```

Redirect



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

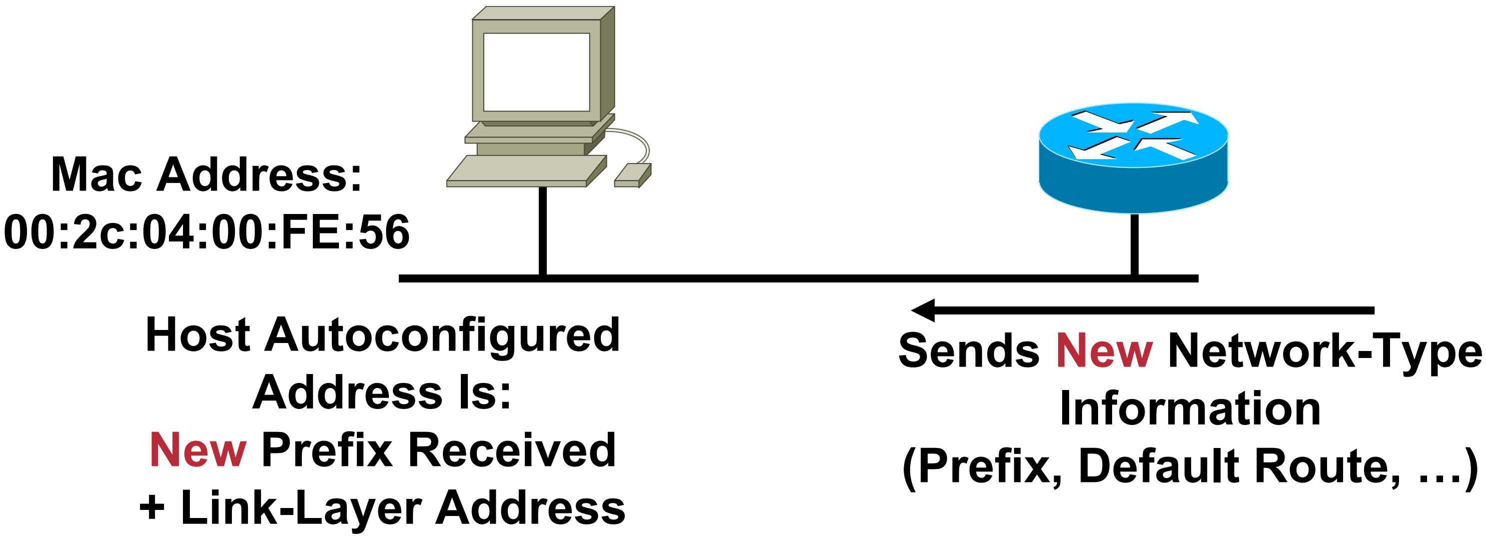
Autoconfiguration



Larger Address Space Enables:

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

Renumbering



Larger Address Space Enables:

- **Renumbering, using autoconfiguration and multiple addresses**

IPv6 Configurations

IPv6 Configuration

- In order to enable IPv6 the following global command should be entered

  Router(config) # ipv6 unicast-routing

- To configure a global IPv6 or unique local IPv6 the following command should be entered

  Router (config-if)# ipv6 address X:X::/prefix

- Note that by configuring an IPV6 address you will have a global or unique-local IPv6 address and a link-local IPv6 address which is

  FE80::interface-id

IPv6 Configuration

- The local-link IPv6 address is constructed automatically by concatenating FE80 with Interface ID as soon as IPv6 is enabled on the interface either by assigning an IPv6 address or simply by entering the command

  Router(config-if)# ipv6 enable

IPv6 Configuration

```
Router#conf t
Router(config)#int fastEthernet 0/0
Router(config-if)#ipv6 enable

Router#show ipv6 interface fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::205:5FFF:FED3:6808
  No global unicast address is configured
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FFD3:6808
  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.
```

IPv6 Configuration

```
R1E#sh ipv6 interface
Ethernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::A8BB:CCFF:FE00:1E00
  Global unicast address(es):
    2001:DB8::A8BB:CCFF:FE00:1E00, subnet is 2001:DB8::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1E00
  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.
```

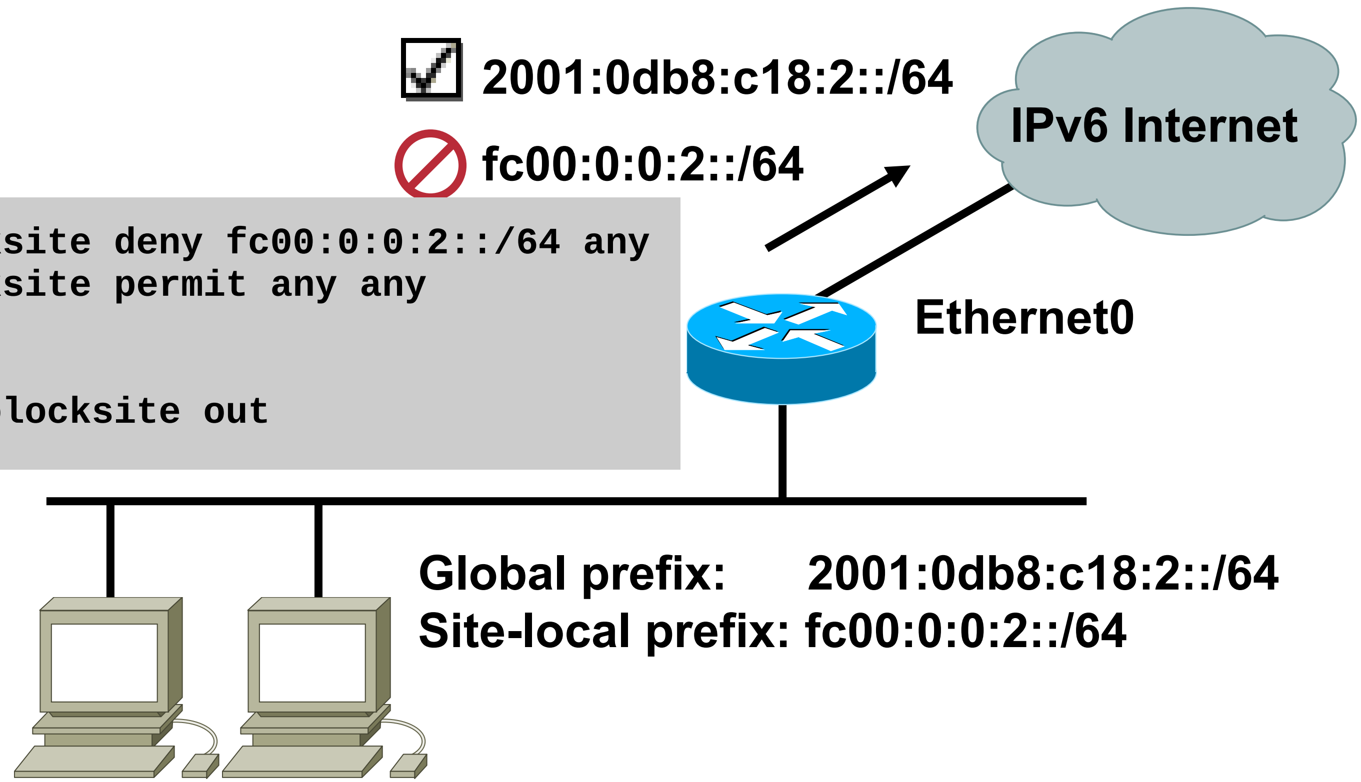
Cisco IOS Standard Access Lists

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 site-local source addresses**




```
ipv6 access-list blocksite deny fc00:0:0:2::/64 any
ipv6 access-list blocksite permit any any

interface Ethernet0
 ipv6 traffic-filter blocksite out
```

Troubleshooting Access-Lists

```
Router# show ipv6 access-list

ipv6 access-list florida
  deny 2001:db8::/64 any priority 10
  permit 2001::/64 any priority 20
  permit any any priority 30
```

```
Router#debug ipv6 packet
IPv6 unicast packet debugging is on
3d22h: IPV6: source FE80::210:7BFF:FEC7:38C0 (local)
3d22h:       dest FF02::1 (Ethernet0/0)
3d22h:       traffic class 112, flow 0x0, len 96+1404, prot 58, hops 255, originating

Router#debug ipv6 nd
ICMP Neighbor Discovery events debugging is on
3d22h: ICMPv6-ND: Sending RA to FF02::1 on Ethernet0/0
3d22h: ICMPv6-ND:     prefix = 2001:ABCD:ABCD:1::/64 onlink autoconfig
3d22h: ICMPv6-ND: Received RA from FE80::210:7BFF:FEC7:3440 on Ethernet0/0
```

Routing

Static Routing

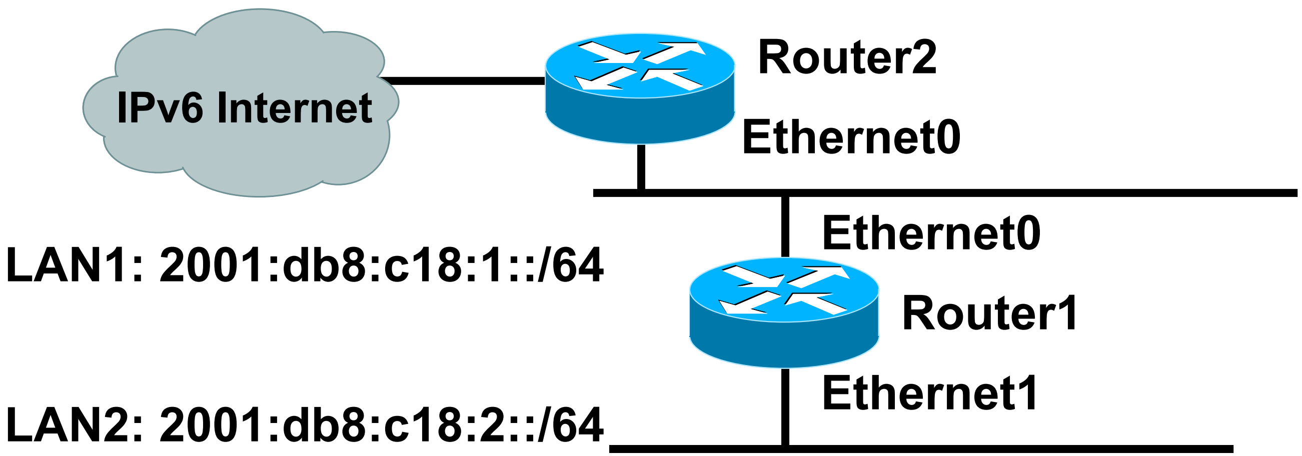
Static Routing

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

```
Router(config)# ipv6 route 7fff::0/32 2001:1100:0:CC00::1 110
```

- **The following example routes packets for network 7fff::0/32 to a networking device at 2001:1100:0:CC00::1 with an administrative distance of 110:**

Default Routing Example




```
ipv6 unicast-routing

interface Ethernet0
 ipv6 address 2001:db8:c18:1::a/64
 ipv6 nd prefix-advertisement 2001:db8:c18:1::/64
43200 43200 onlink autoconfig

interface Ethernet1
 ipv6 address 2001:db8:c18:2::a/64
 ipv6 nd prefix-advertisement 2001:db8:c18:2::/64
43200 43200 onlink autoconfig

ipv6 route ::/0 <address of R2 ethernet0>
```

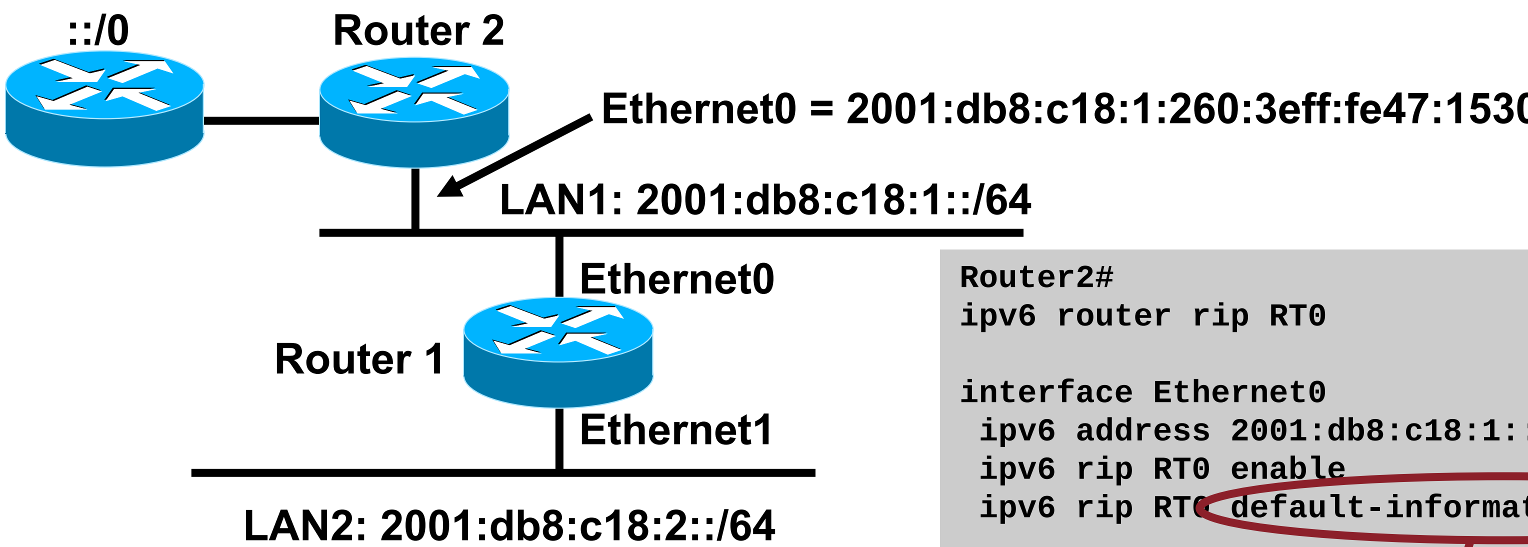
Default Route to Router2

RIPng (RFC 2080)

Enhanced Routing Protocol Support
RIPng Overview

- **RIPng for IPv6, RFC 2080**
- **Same as IPv4:**
  - **Distance-vector, radius of 15 hops, split-horizon and etc.**
  - **Based on RIPv2**
- **Updated features for IPv6**
  - **IPv6 prefix, next-hop IPv6 address**
  - **Uses the multicast group FF02::9, the all-rip-routers multicast group, as the destination address for RIP updates**
  - **Uses IPv6 for transport**

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

Deployment

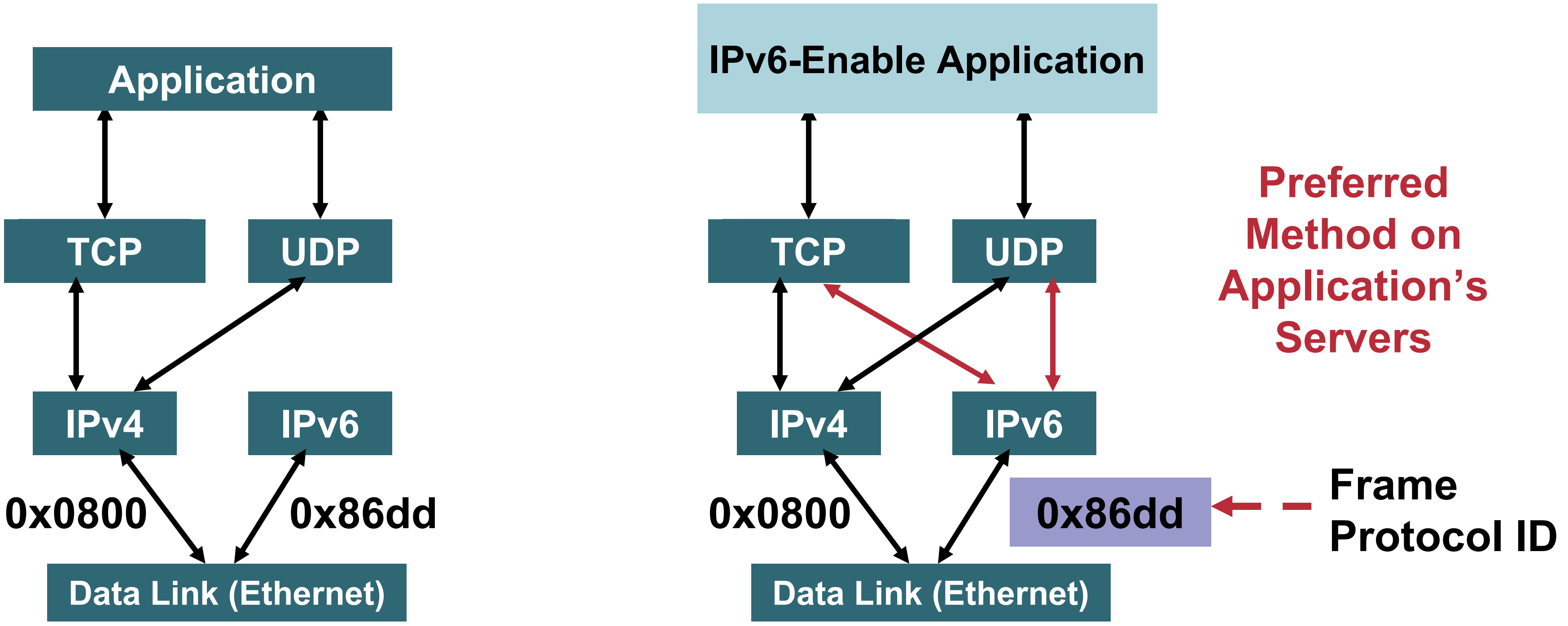
IPv4-IPv6 Transition/Coexistence

- **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**

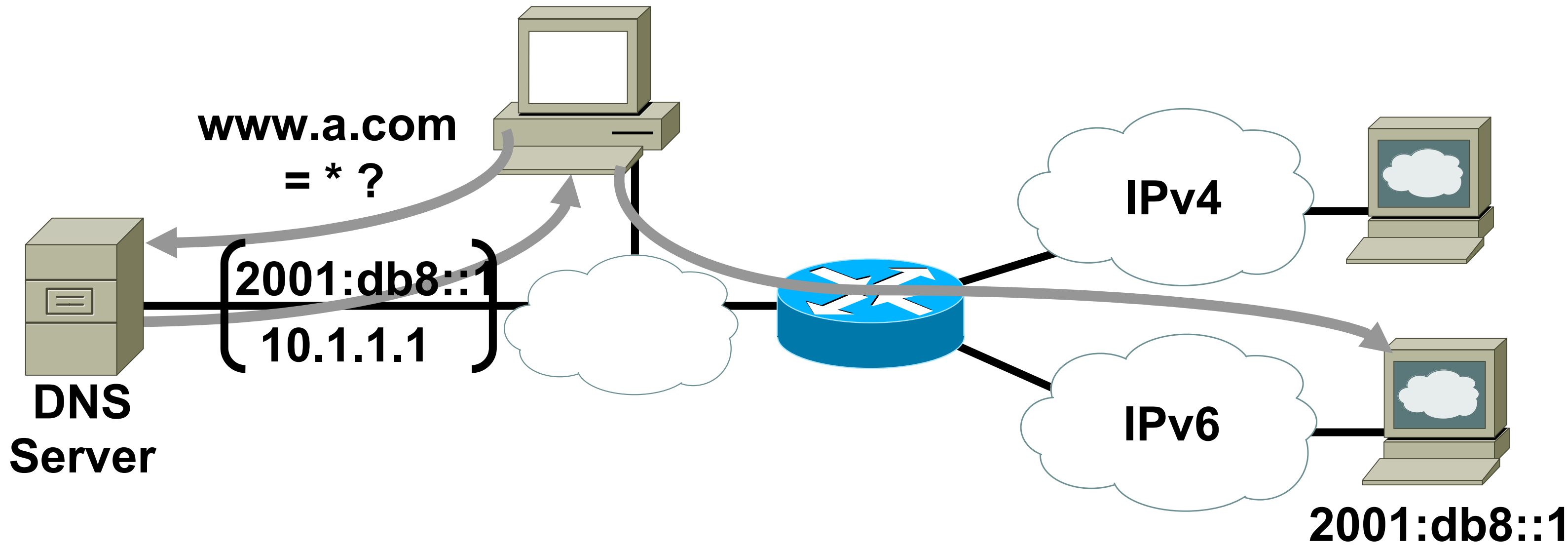
Dual Stack Approach



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

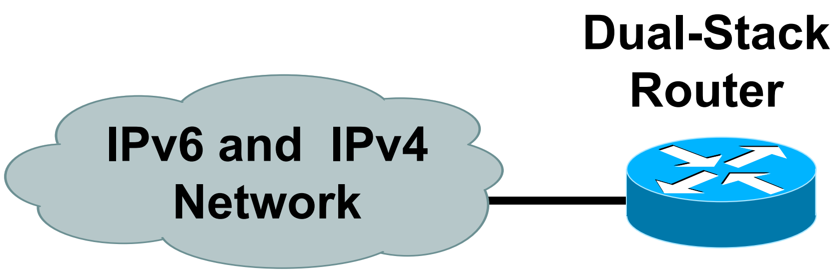
Host Running Dual Stack



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

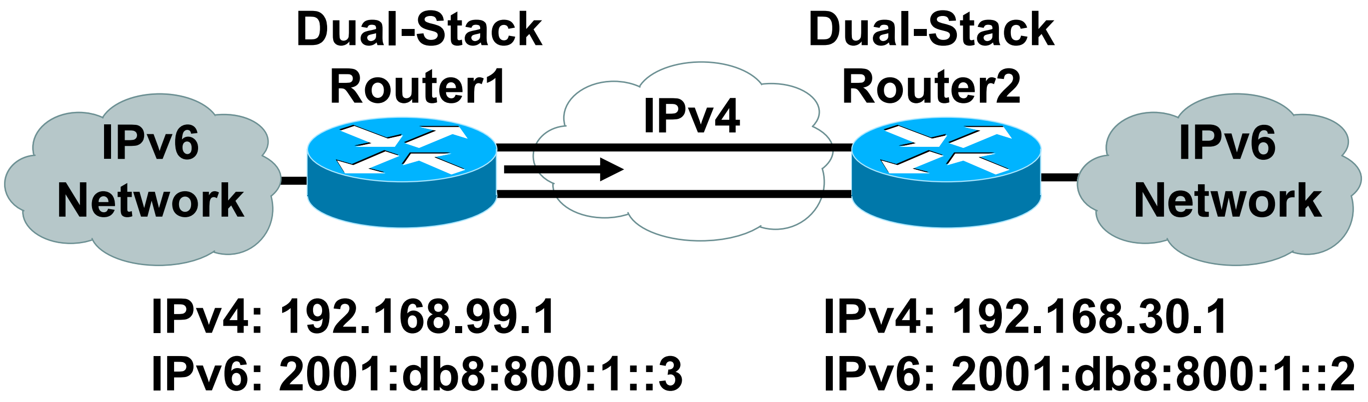
- **Native IP over data link layers**

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

- **Some new techniques**

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

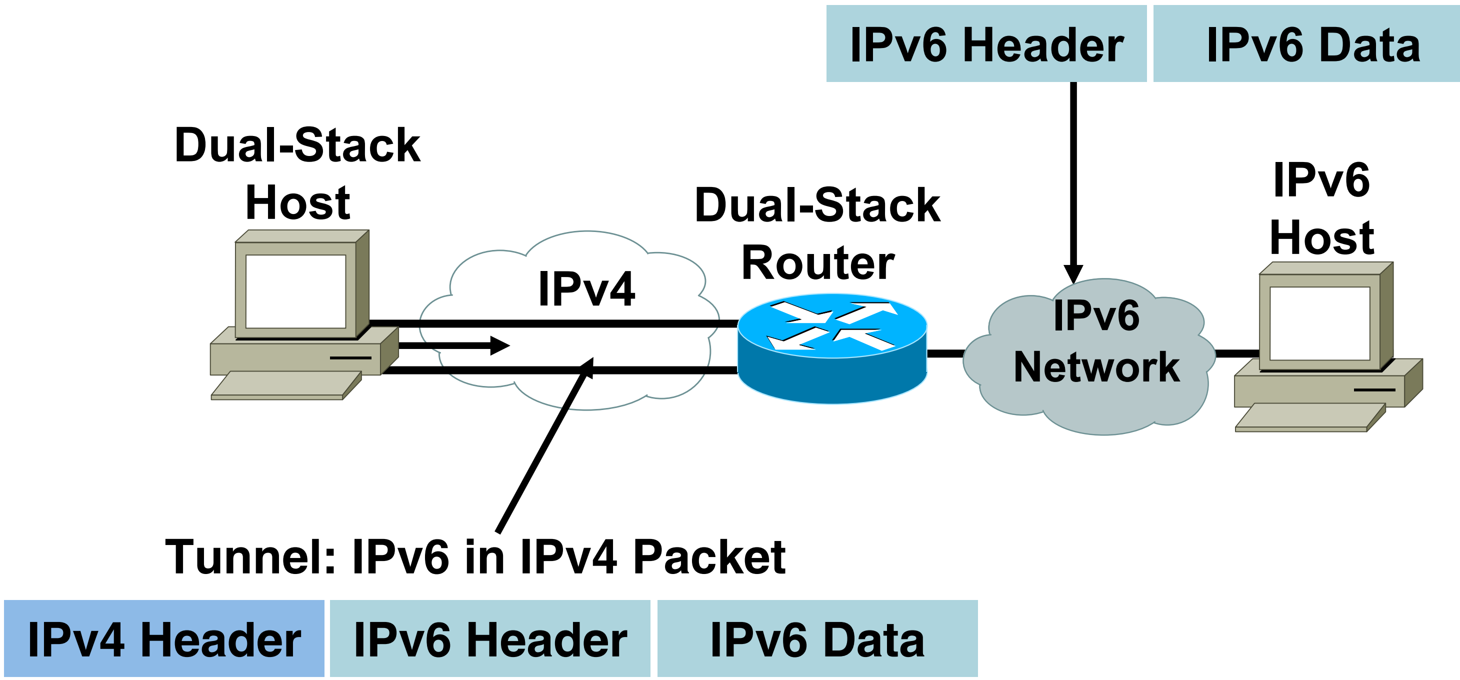
Manually Configured GRE Tunnel Configuration




```
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
```

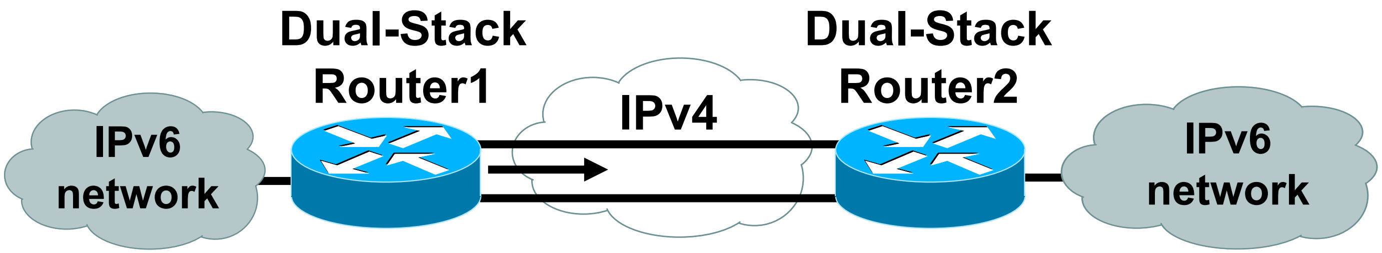
```
router2#

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
```

IPv6 over IPv4 Tunnels



- **Tunneling can be used by routers and hosts**

Manually Configured Manual Tunnel Configuration



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

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

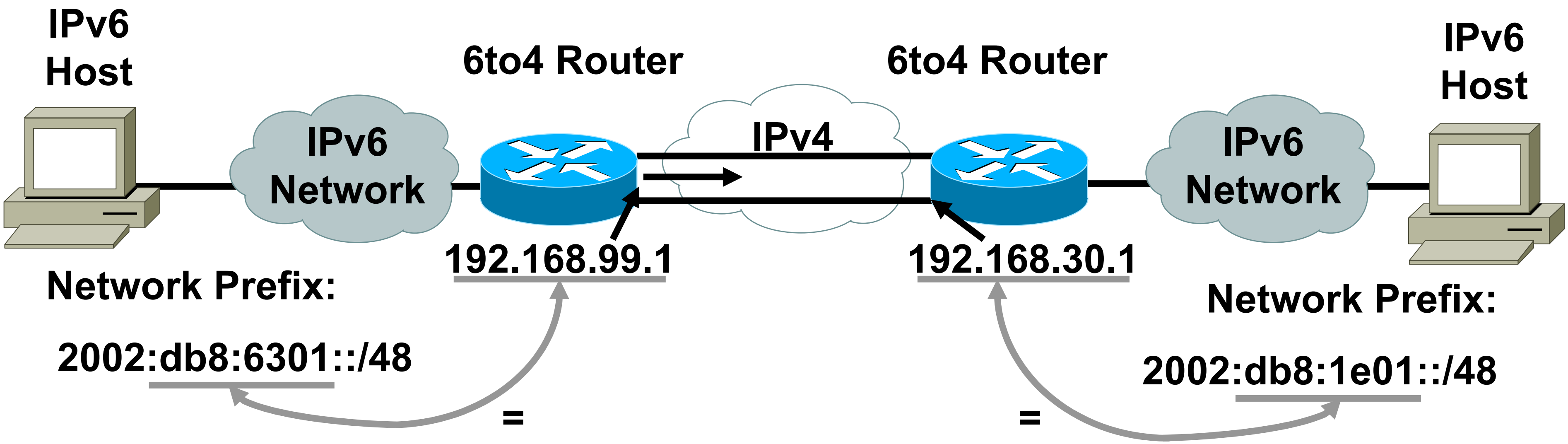
```
router1#

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
```

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 network is treated like a virtual NBMA network
- 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)

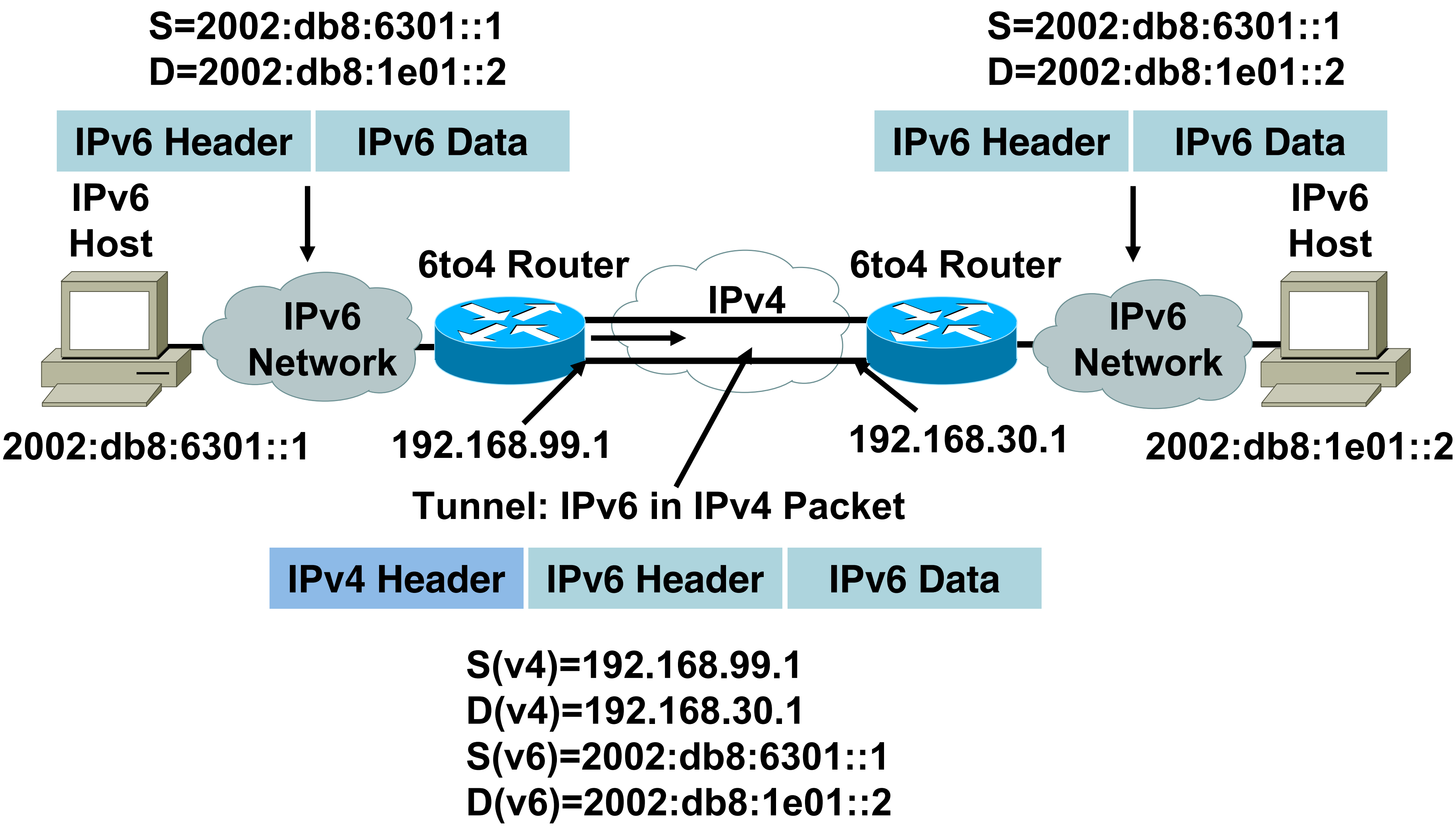


6to4:

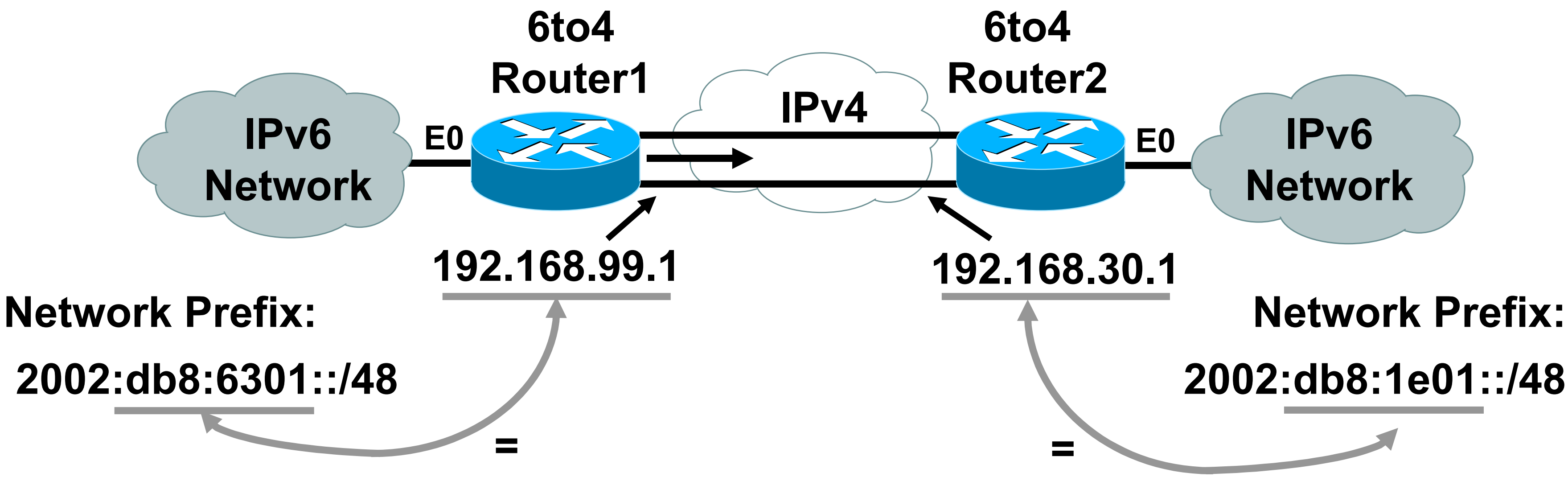
- Is an automatic tunnel method
- Gives a prefix to the attached IPv6 network

2002	Public IPv4 Address	SLA	Interface ID
/16	/48	/64	

Automatic 6to4 Tunnel (RFC 3056)



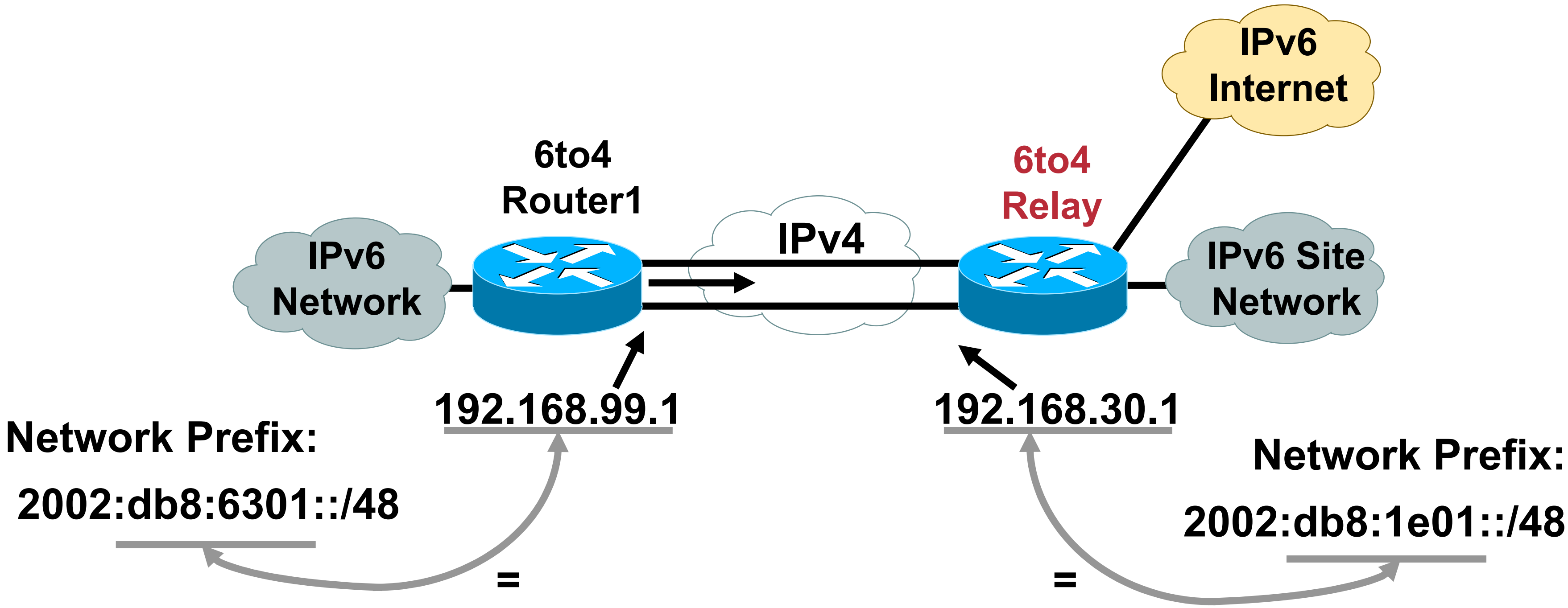
Automatic 6to4 Configuration




```
router1#
interface Ethernet0
 ipv6 address 2002:db8:6301:1::/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:db8:1e01:1::/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
```

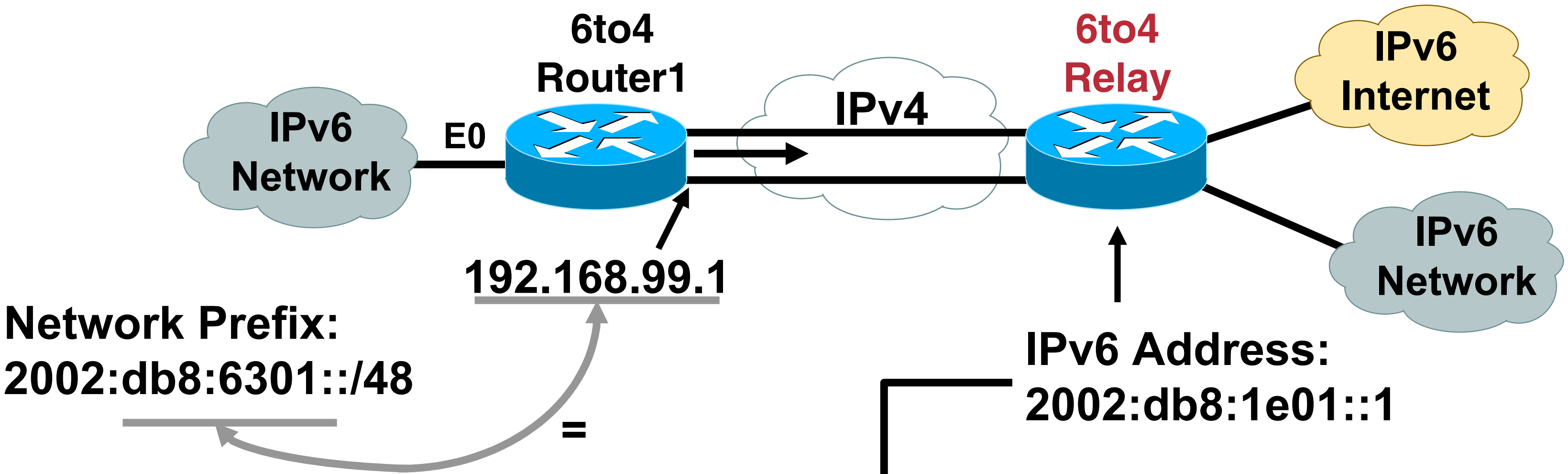
Automatic 6to4 Relay



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:db8:6301:1::/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 2001:db8:1e01::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

Intrasite Automatic Tunnel Address Protocol

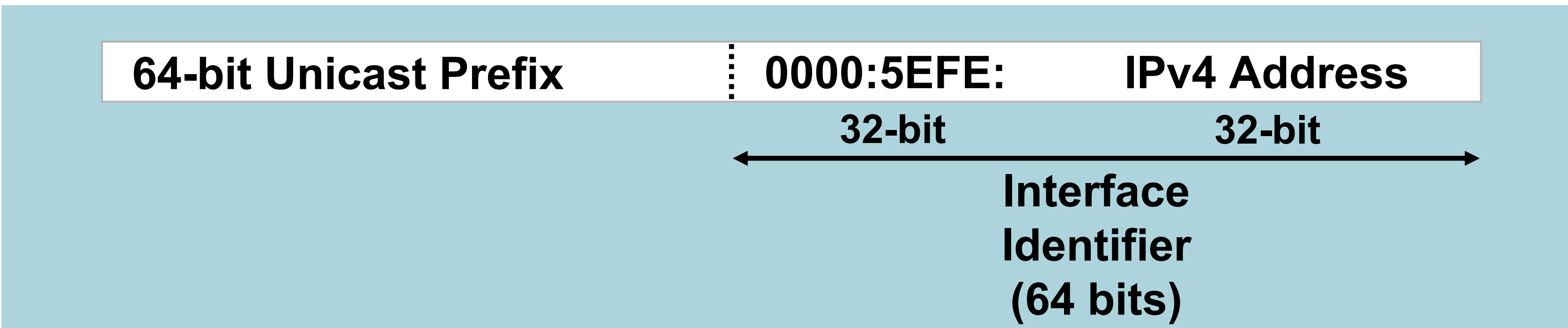
- RFC 4214
- This is for enterprise networks such as corporate and academic networks
- Scalable approach for incremental deployment
- ISATAP makes your IPv4 infratructure as transport (NBMA) network

Intrasite Automatic Tunnel Address Protocol

- 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 there interface will only have a link local v6 address until the first router appears

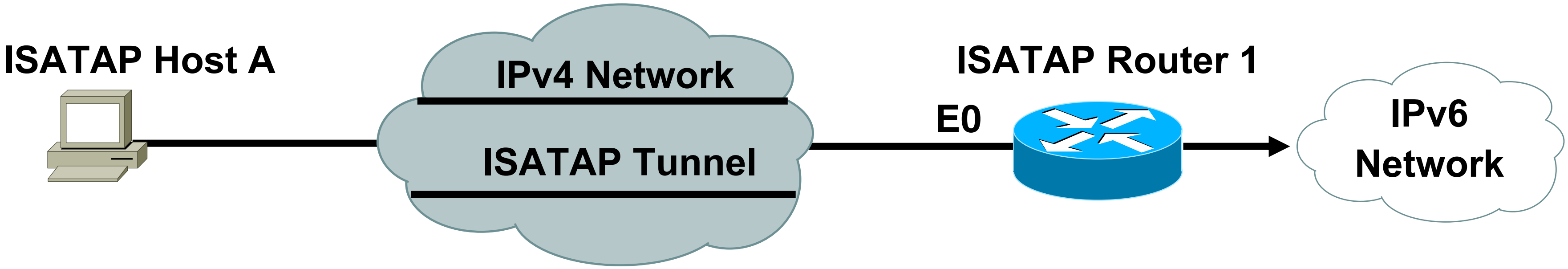
Intrasite Automatic Tunnel Address Protocol

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**

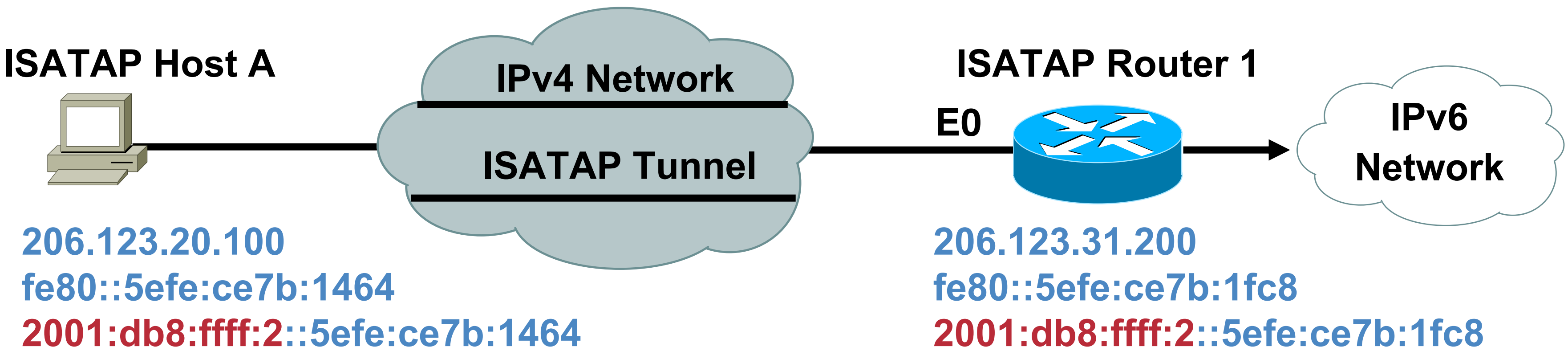
Automatic Advertisement of ISATAP Prefix



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

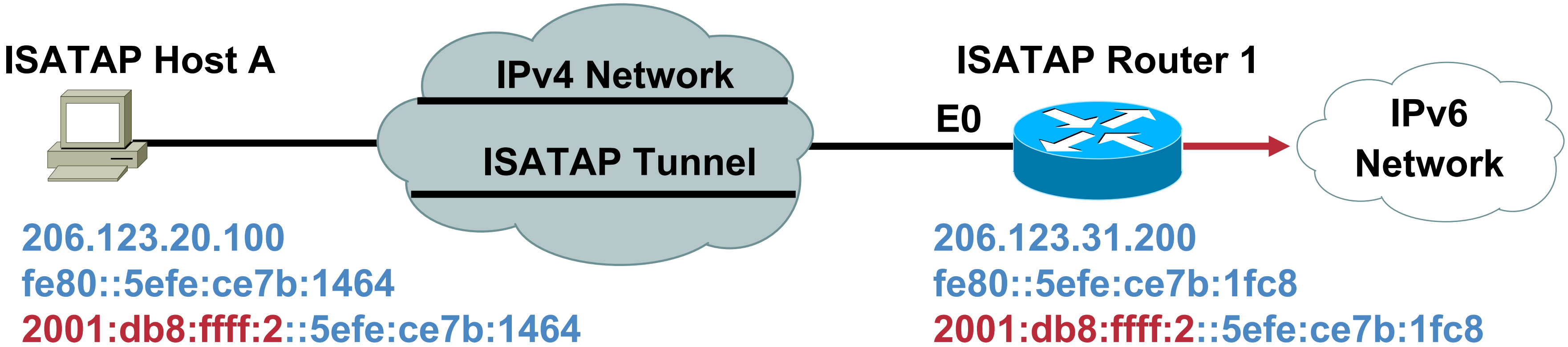
ICMPv6 Type 134 (RA)
IPv4 Source: 206.123.31.200
IPv4 Destination: 206.123.20.100
IPv6 Source: fe80::5efe:ce7b:1fc8
IPv6 Destination: fe80::5efe:ce7b:1464
ISATAP Prefix: 2001:db8:ffff :2::/64

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**

Conclusion

- IPv6 is real!
- Start now rather than later
  - Purchase for the future
  - Start moving legacy application towards IPv6 support
- Integration can be done per application (dual stack or tunneled)
- Know what is still under development:
  - EIGRP for IPv6—Feb. 2006
  - IPv6 HSRP—available for most platforms except Catalyst® OS
  - Enterprise products/features—(Voice, CDN, Advanced Security)
  - Full-scale management of IPv6
  - Key management for IPSec (prevents scalable IPv6 IPSec deployment with clients)
  - ISP multihoming solutions

Q and A

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]

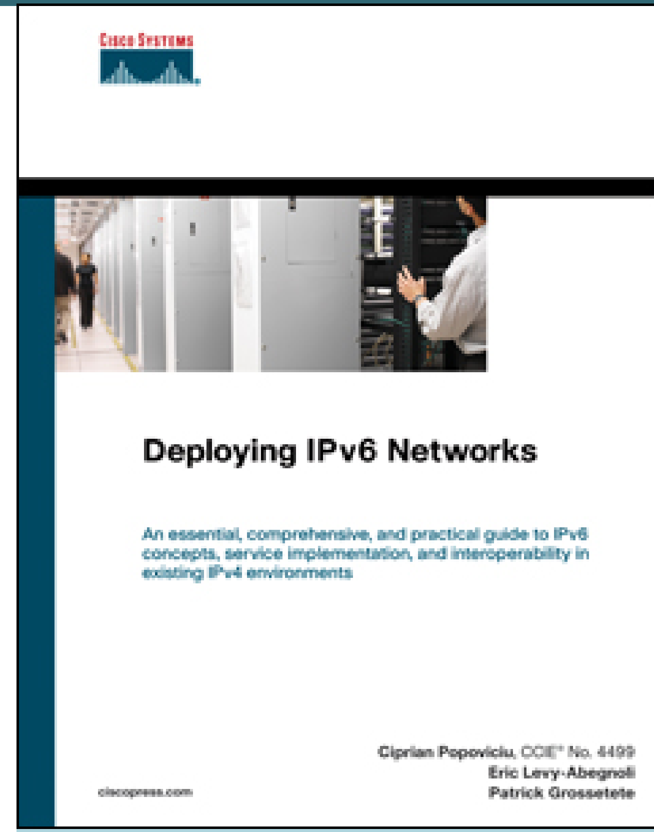
  http://www.cisco.com/warp/customer/732/Tech/ipv6/elearning/
- IPv6 Access Services

  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

Recommended Reading

- Continue your Cisco Networkers learning experience with further reading from Cisco Press
- Check the Recommended Reading flyer for suggested books



Available Onsite at the Cisco Company Store

Complete Your Online Session Evaluation

- **Win fabulous prizes; Give us your feedback**
- **Receive ten Passport Points for each session evaluation you complete**
- **Go to the Internet stations located throughout the Convention Center to complete your session evaluation**
- **Drawings will be held in the World of Solutions**

  Tuesday, June 20 at 12:15 p.m.

  Wednesday, June 21 at 12:15 p.m.

  Thursday, June 22 at 12:15 p.m. and 2:00 p.m.