IPv6 Workshop

Majid Siddiq : majsiddi@cisco.com
15th April, 2015

Agenda

Day 1:

- IPv6 Business Drivers
- IPv6 Addressing, Header, and Basics
- IPv6 Address Allocation & Configuration
- Labs 1: Addressing & 2: Neighbor Discovery

Day 2:

- Lab 3: Static Routing
- IPv6 Services
- IPv6 Routing
- Labs 4: OSPFv3 & 5: BGP

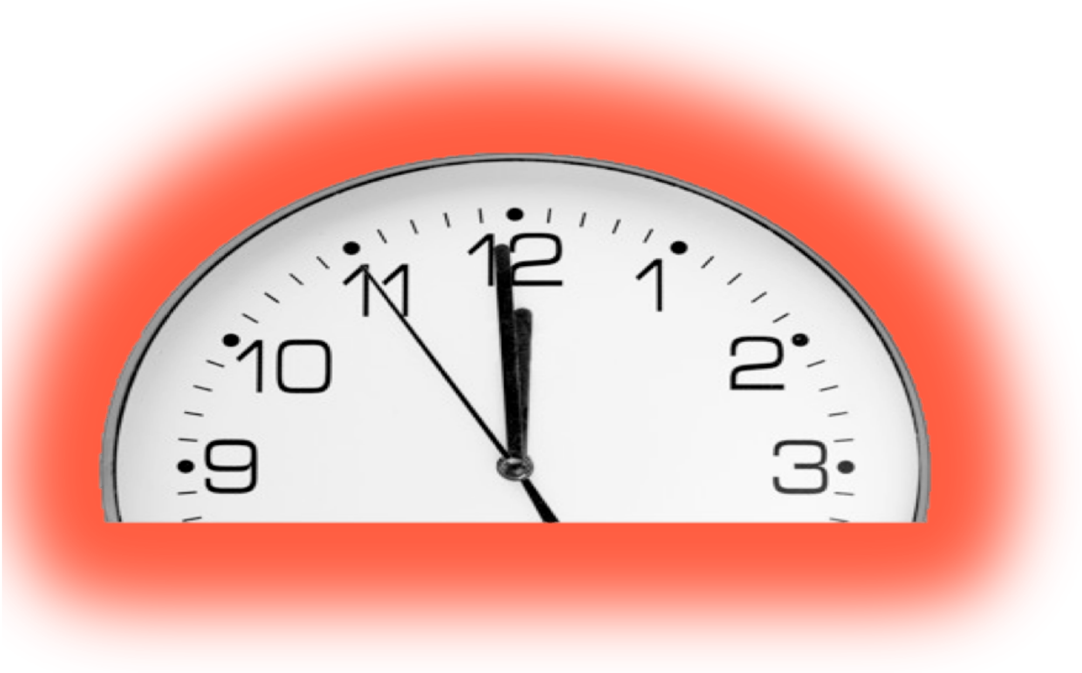
Day 3:

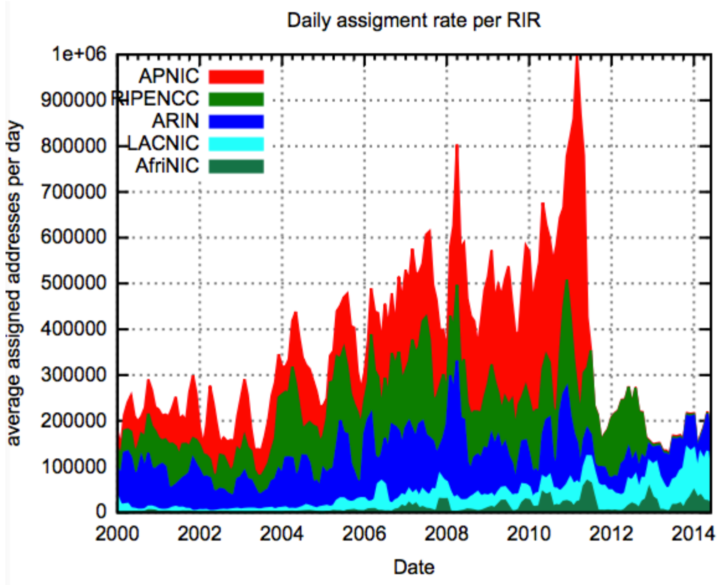
- IPv6 Deployment
- Labs 6: Manual Tunnel & 7: Automatic Tunnel
- IPv6 Security

IPv6 Business Drivers

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

IPv4 Address Depletion





Time’s Up

No more IPv4 addresses left with IANA or APNIC

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Where Did All the IPv4 Go?

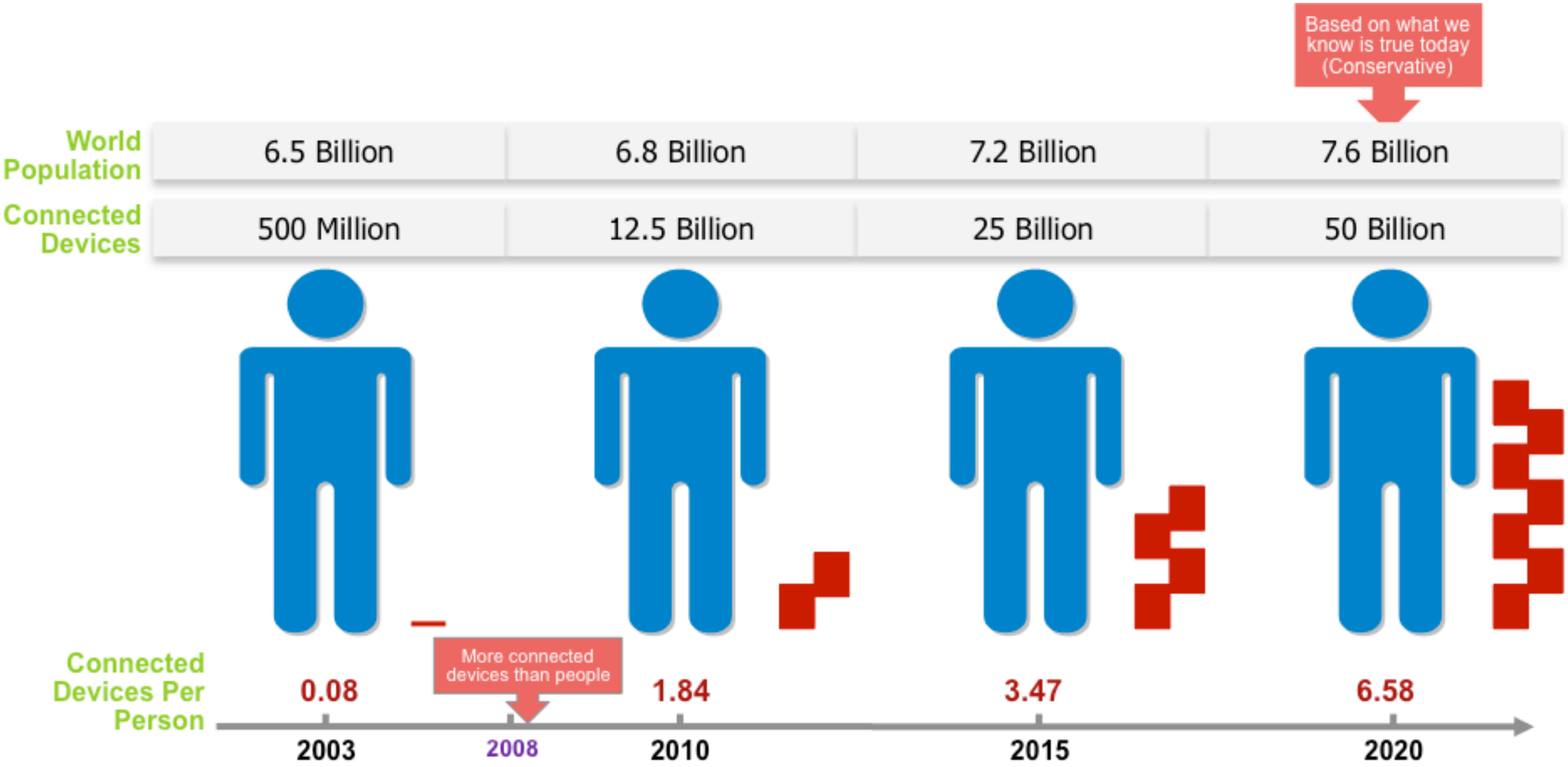
Fractal map: Layout by Randall Munroe, Time Sequence by Tony Hain, Highlighted by Jeff Apcar

000 IANA	001 APNIC	014 PDN	015 HP	016 DEC	019 Ford	020 CsC	021 US DoD	234 Multicast	235 Multicast	236 Multicast	239 Multicast	240 Class E	241 Class E	254 Class E	255 Class E
003 GE	002 RIPE	013 Xerox	012 AT&T	017 Apple	018 MIT	023 Next	022 US DoD	233 Multicast	232 Multicast	237 Multicast	238 Multicast	243 Class E	242 Class E	253 Class E	252 Class E
004 L3	007 ARIN	008 L3	011 US DoD	030 US DoD	029 US DoD	024 Cable	025 UK Defense	230 Multicast	231 Multicast	226 Multicast	225 Multicast	244 Class E	247 Class E	248 Class E	251 Class E
005 RIPE	006 US DoD	009 IBM	010 RFC1918	031 RIPE	028 US DoD	027 APNIC	026 US DoD	229 Multicast	228 Multicast	227 Multicast	224 Multicast	245 Class E	246 Class E	249 Class E	250 Class E
058 APNIC	057 SITA	054 Merck	053 Cap Debis	032 AT&T	035 MERIT	036 APNIC	037 RIPE	218 APNIC	219 APNIC	220 APNIC	223 APNIC	202 APNIC	201 LACNIC	198 Legacy	197 AFRINic
059 APNIC	056 US Postal	055 US DoD	052 El duPONT	033 US DoD	034 Haliburton	039 APNIC	038 PSI	217 RIPE	216 ARIN	221 APNIC	222 APNIC	203 APNIC	200 LACNIC	199 ARIN	196 AfriNIC
060 APNIC	061 APNIC	050 ARIN	051 UK DSS	046 RIPE	045 ARIN	040 Eli Lily	041 AfriNIC	214 US DoD	215 US DoD	210 APNIC	209 ARIN	204 ARIN	205 ARIN	194 RIPE	195 RIPE
063 ARIN	062 RIPE	049 APNIC	048 Prudential	047 Bell North	044 Radio	043 Inet	042 APNIC	213 RIPE	212 RIPE	211 APNIC	208 ARIN	207 ARIN	206 ARIN	192 RIPE	192 Legacy
064 ARIN	067 ARIN	068 ARIN	069 ARIN	122 APNIC	123 APNIC	124 APNIC	127 Loopback	128 Legacy	131 Legacy	132 Legacy	133 Legacy	186 LACNIC	187 LACNIC	188 Legacy	191 Legacy
065 ARIN	066 ARIN	071 ARIN	070 ARIN	121 APNIC	120 APNIC	125 APNIC	126 APNIC	129 Legacy	130 Legacy	135 Legacy	134 Legacy	185 RIPE	184 ARIN	189 LACNIC	190 LACNIC
078 RIPE	077 RIPE	072 ARIN	073 ARIN	118 APNIC	119 APNIC	114 APNIC	113 APNIC	142 Legacy	141 Legacy	136 Legacy	137 Legacy	182 APNIC	183 APNIC	178 RIPE	177 LACNIC
079 RIPE	076 ARIN	075 ARIN	074 ARIN	117 APNIC	116 APNIC	115 APNIC	112 APNIC	143 Legacy	140 Legacy	139 Legacy	138 Legacy	181 LACNIC	180 APNIC	179 LACNIC	176 RIPE
080 RIPE	081 RIPE	094 RIPE	095 RIPE	096 ARIN	097 ARIN	110 APNIC	111 APNIC	144 Legacy	145 Legacy	158 Legacy	159 Legacy	160 Legacy	161 Legacy	174 ARIN	175 APNIC
083 RIPE	082 RIPE	093 RIPE	092 RIPE	099 ARIN	098 ARIN	109 RIPE	108 ARIN	147 Legacy	146 Legacy	157 Legacy	156 Legacy	163 Legacy	162 Legacy	173 ARIN	172 Legacy
084 RIPE	087 RIPE	088 RIPE	091 RIPE	100 ARIN	103 APNIC	104 ARIN	107 ARIN	148 Legacy	151 Legacy	152 Legacy	155 Legacy	164 Legacy	167 Legacy	168 Legacy	171 Legacy
085 RIPE	086 RIPE	089 RIPE	090 RIPE	101 APNIC	102 AfriNIC	105 AfriNIC	106 APNIC	149 Legacy	150 Legacy	153 Legacy	154 Legacy	165 Legacy	166 Legacy	169 Legacy	170 Legacy

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Growth of Connected Devices



Source: Cisco IBSG, April 2011

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Worldwide Internet Population

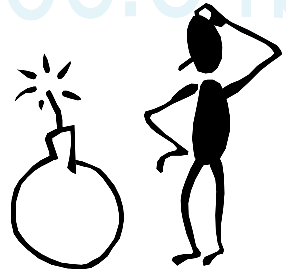
	Population	Internet Users (Dec, 2000)	Internet Users (Latest Data)	Penetration %
Africa	1,125,721,038	4,514,400	297,885,898	26.50%
Asia	3,996,408,007	114,304,000	1,386,188,112	34.70%
Europe	825,824,883	105,096,093	582,441,059	70.50%
Middle East	231,588,580	3,284,800	111,809,510	48.30%
North America	353,860,227	108,096,800	310,322,257	87.70%
Latin America / Caribbean	612,279,181	18,068,919	320,312,562	52.30%
Oceania / Australia	36,724,649	7,620,480	26,789,942	72.90%
WORLD TOTAL	7,182,406,565	360,985,492	3,035,749,340	42.30%

Source: http://www.internetworldstats.com/stats.htm June 2014

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Global Internet Challenges



- Depletion of IPv4 address space
- Growing size of the Internet routing table

	Current Size January 2011	Increase from January 2008
IPv4 BGP Entries	511,702	165%
IPv6 BGP Entries	20,388	900%

Source: telnet://route-views.oregon-ix.net Dec 2014

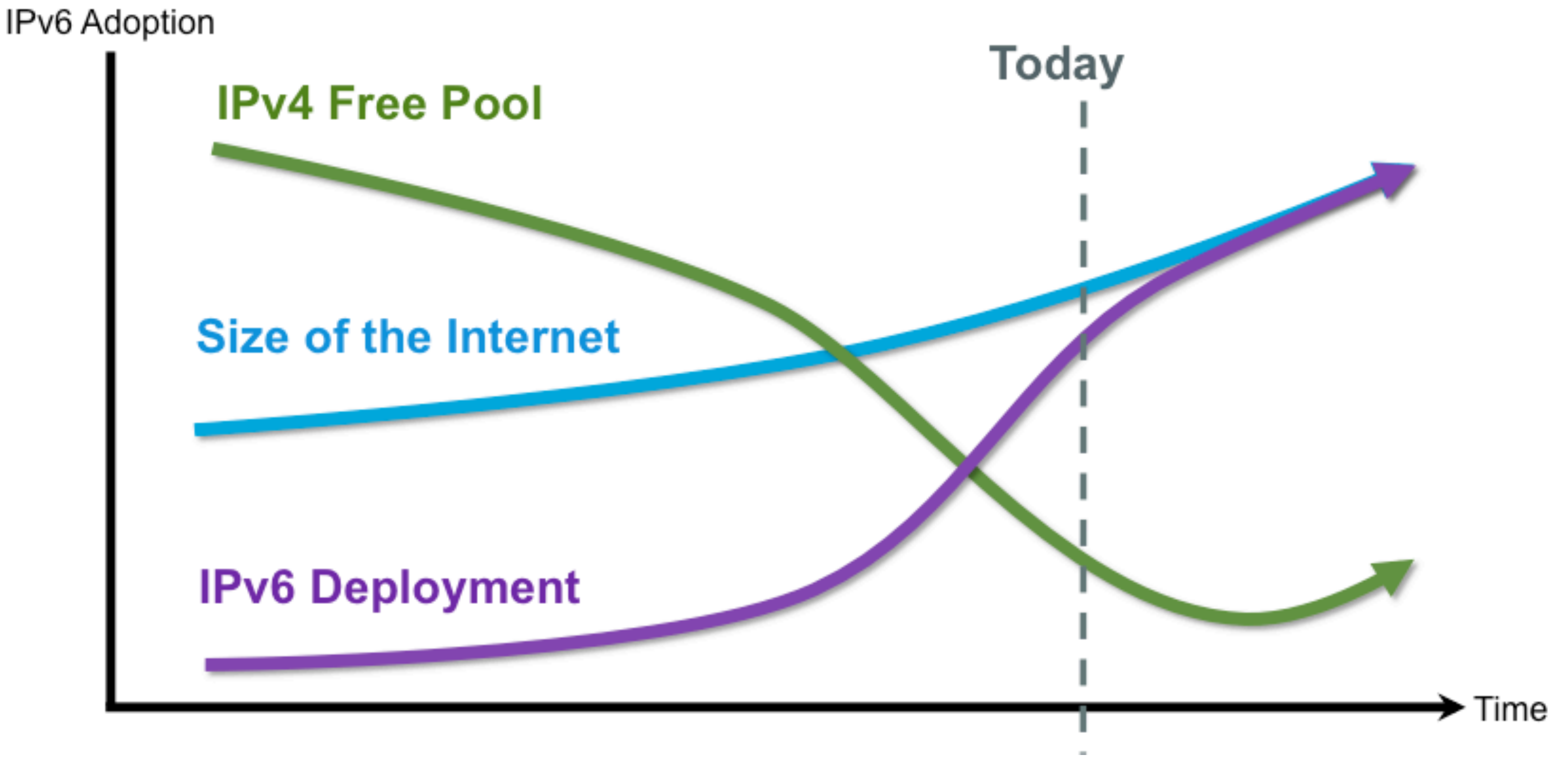
2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Need for More IP Addresses

- **Omnipresent IP**
  - Integration of Data, Voice, and Video
  - Explosion of mobile devices
  - SmartGrid and Smart Connected Community
- **NAT and CIDR**
  - Developed to ease the global Internet challenges
  - Not to entirely solve the issues
- **IETF IPv6 WG** began in early 90s
  - IPv4 32-bit address = ~ 4 billion addresses ($4x10^9$)
  - IPv6 128-bit address = ~ 340 undecillion addresses ($340x10^{36}$)
- One Compelling Reason for IPv6 is "More IP Addresses"

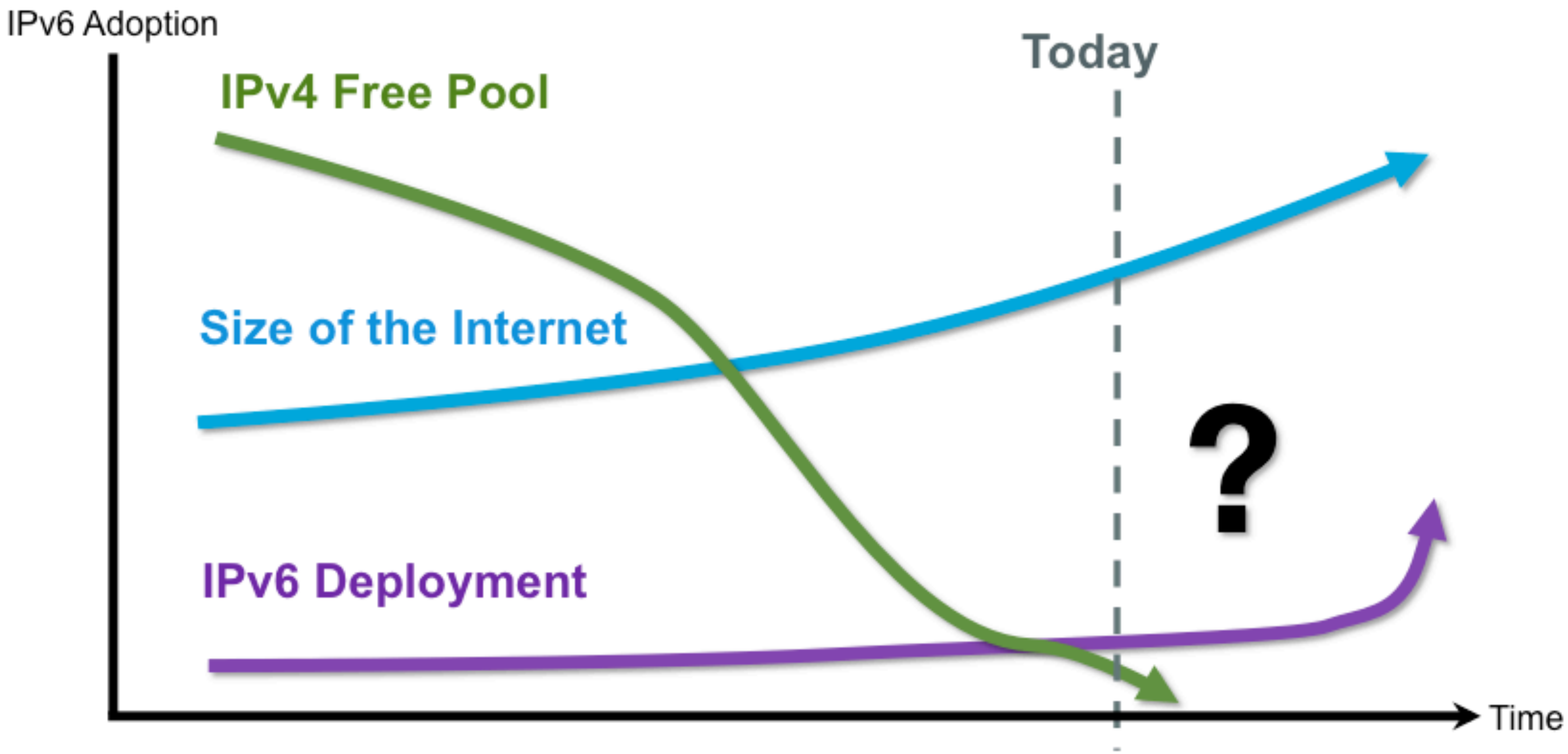
2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

The Plan



2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

The Reality


IPv6 Adoption
IPv4 Free Pool
Today
Size of the Internet
?
IPv6 Deployment
Time

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

6th June 2012

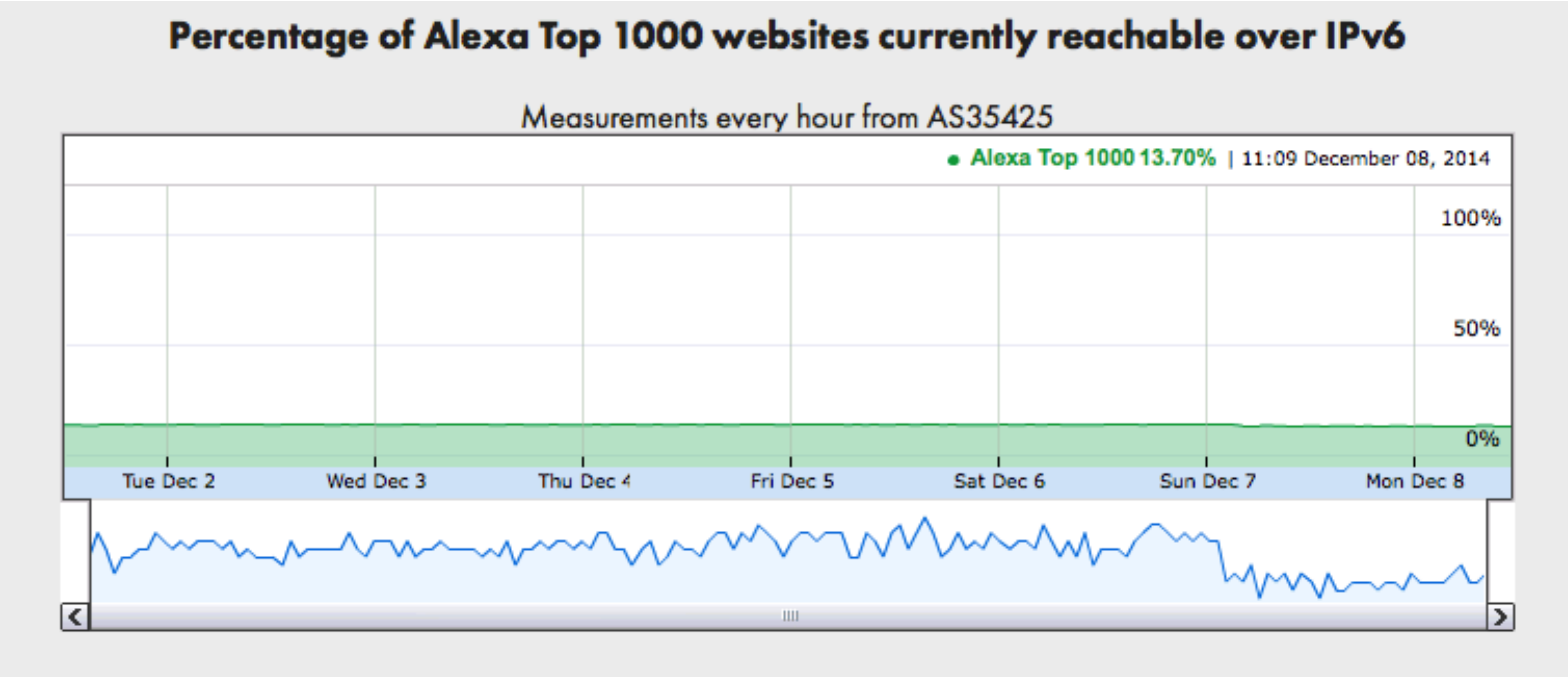
Turn it on. WORLD IPv6 LAUNCH **Leave it on.**

http://www.worldipv6launch.org

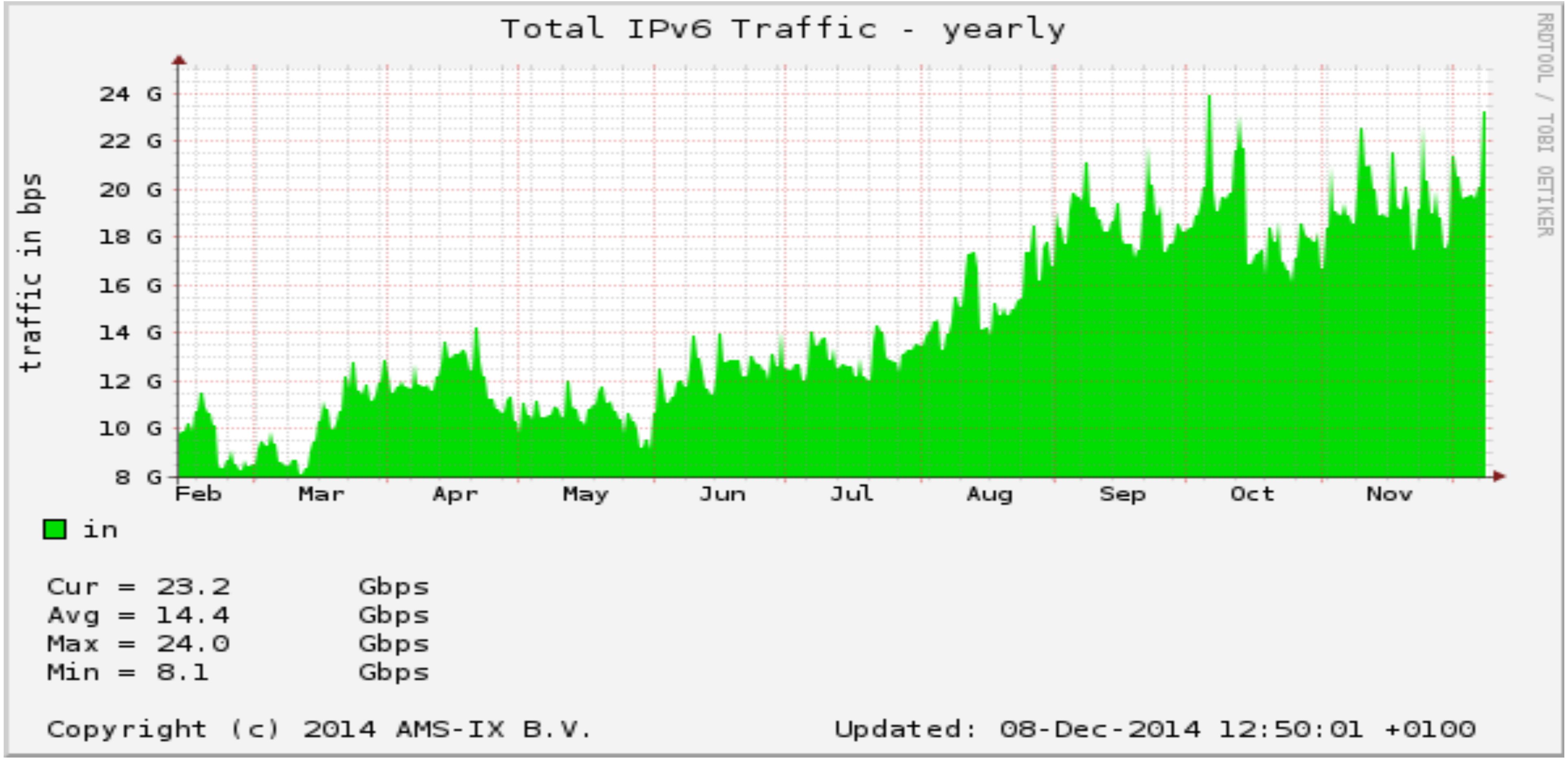
2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

World IPv6 Launch: Working Towards New Internet Protocol

World IPv6 Launch - Measurements



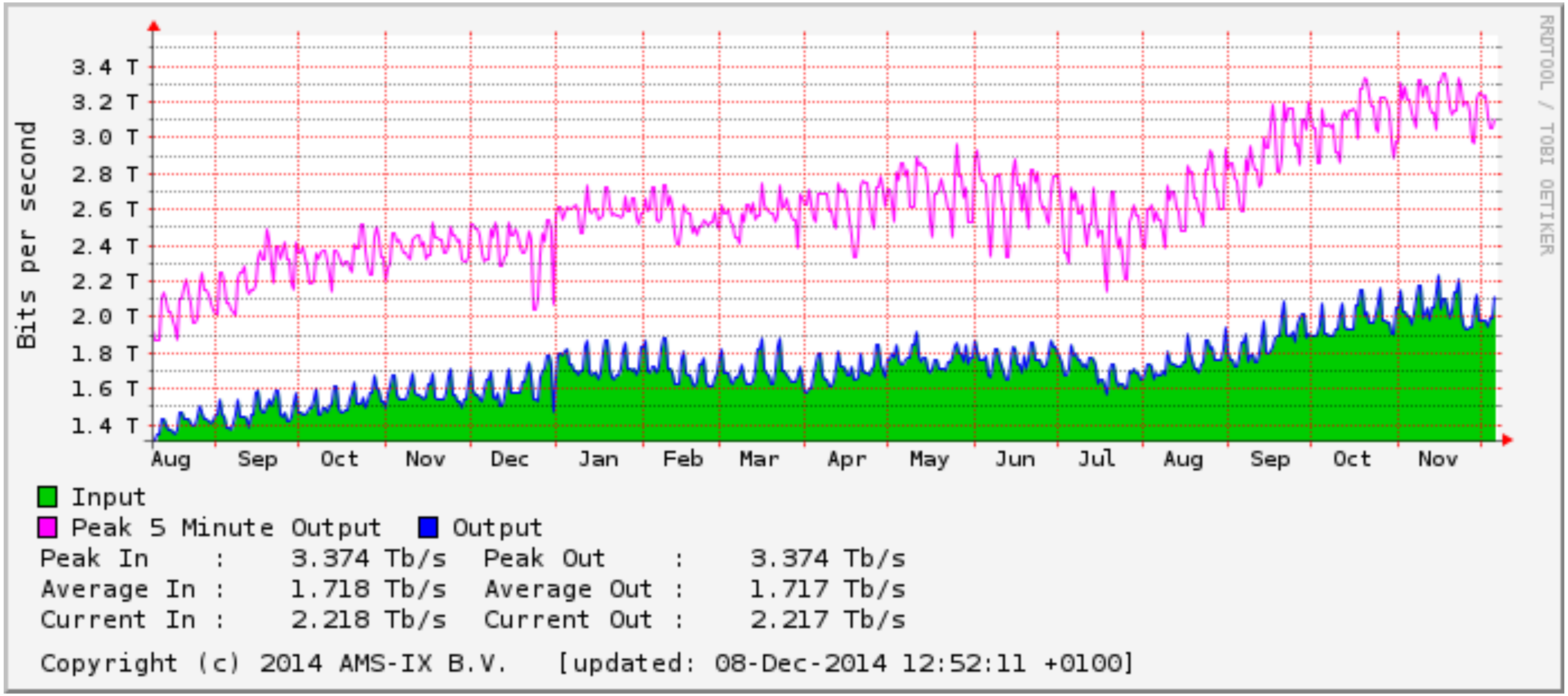
IPv6 Traffic



2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

IPv4 Traffic ☺



2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

John Chambers on Cisco IPv6 Strategy

"…if we don't overcome the challenges of IPv4 (...) we will slow down the growth of the Internet and loose momentum as an industry"

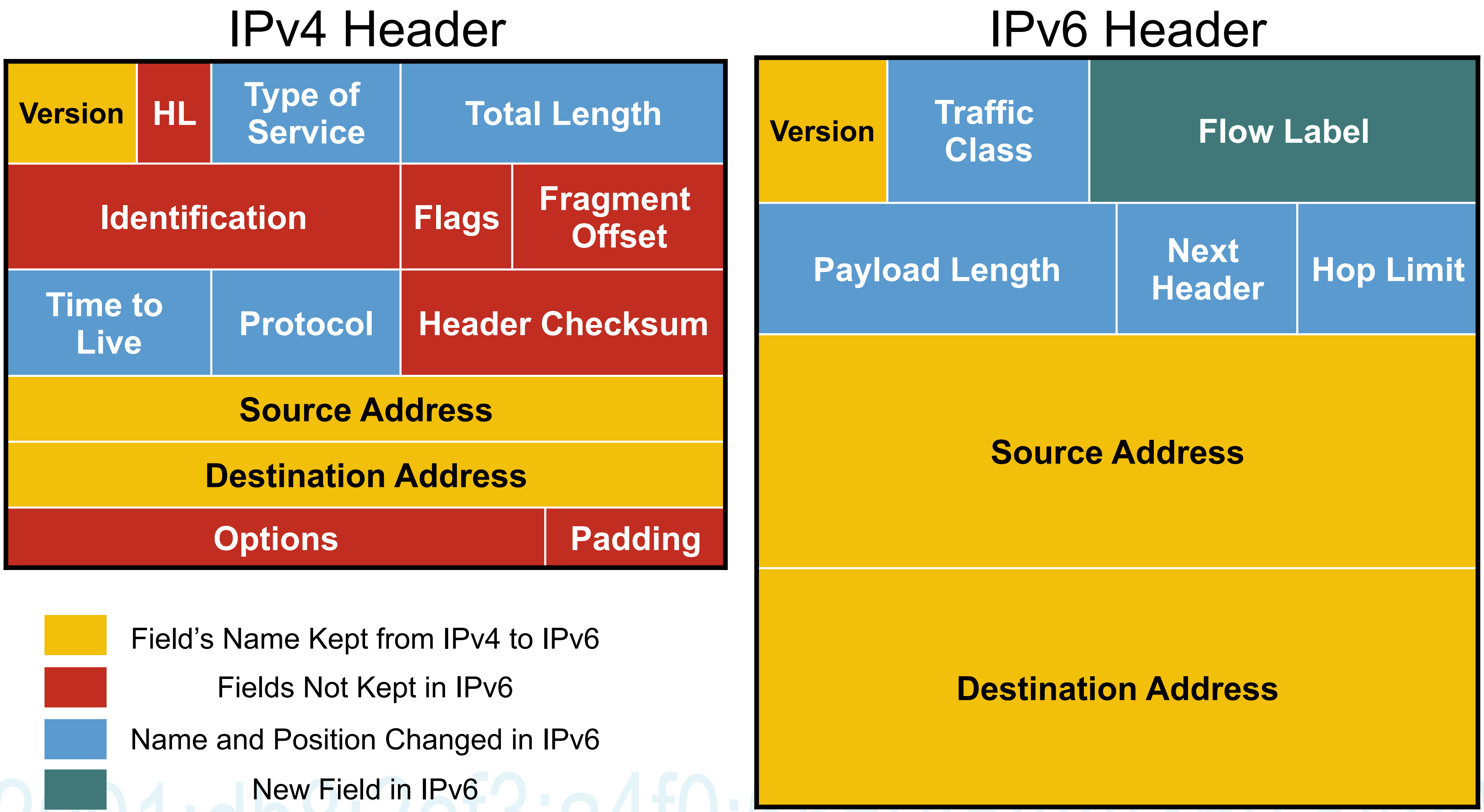
"IPv6 is important to all of us (…) to everyone around the world, It is crucial to our ability to tie together everyone and every device."

"At Cisco we are commited architecturally to IPv6 across the board: All of our devices, all of our applications and all of our services."

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

IPv6 Packet Header

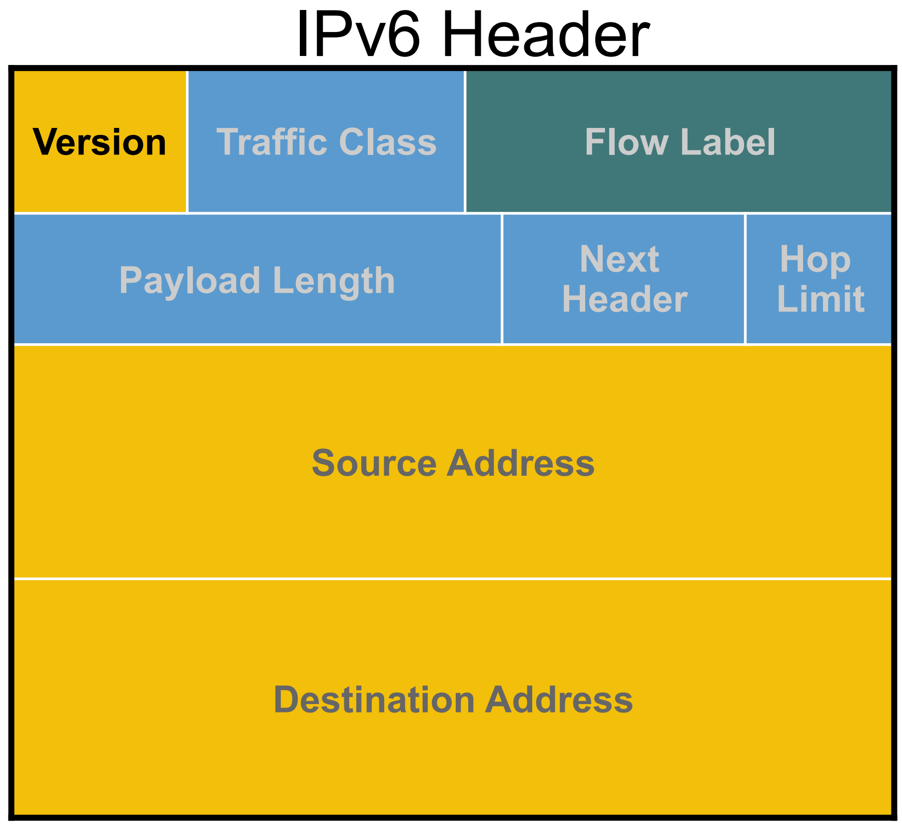
IPv4 and IPv6 Header Comparison



2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

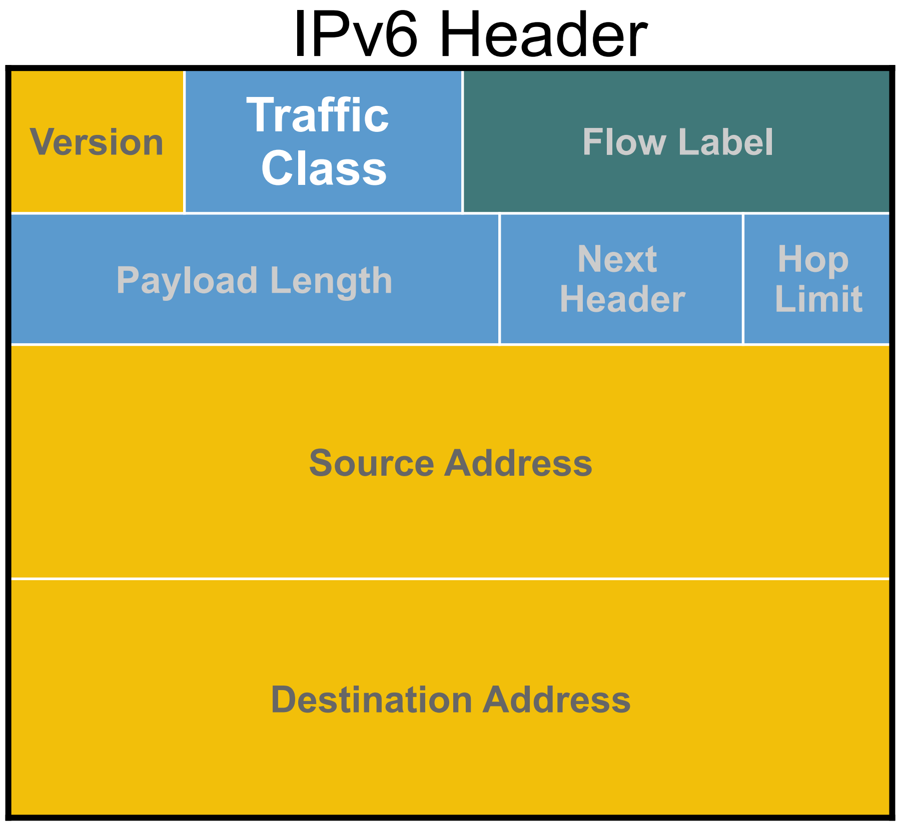
IPv4 and IPv6 Header Comparison

- Version: a 4-bit field that contains the number 6 instead of 4



IPv4 and IPv6 Header Comparison
Fields Renamed

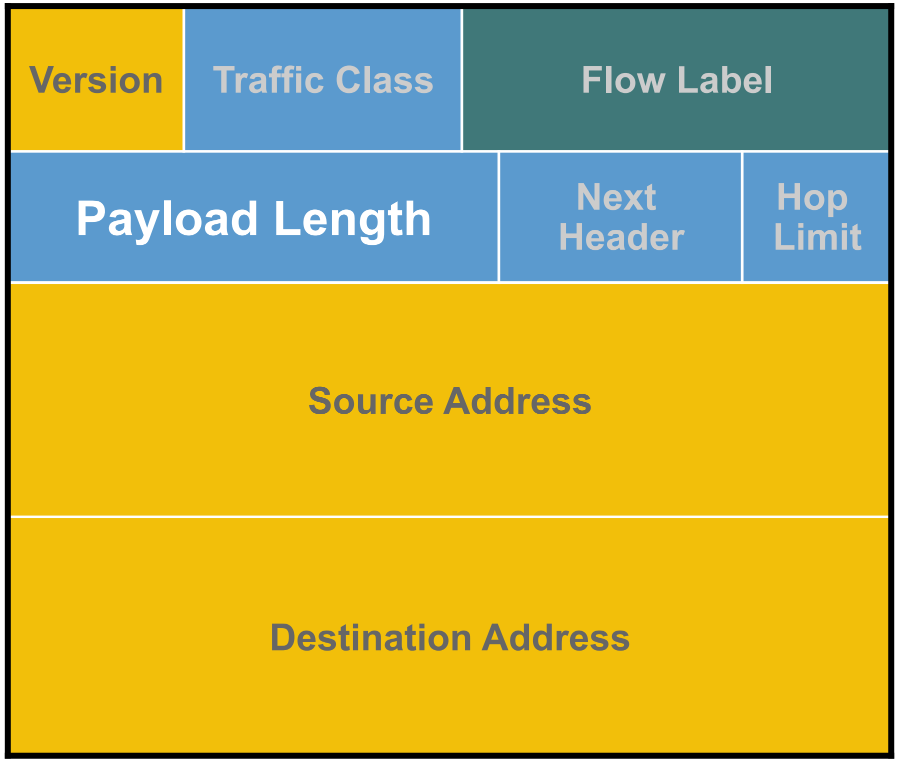
- Traffic class: an 8-bit field that is similar to the TOS field in IPv4
- It tags the packet with a traffic class that can be used in differentiated services
- These functionalities are the same as in IPv4



IPv4 and IPv6 Header Comparison
Fields Renamed

- Payload length: this is similar to the total length in IPv4, except it does not include the 40-byte header

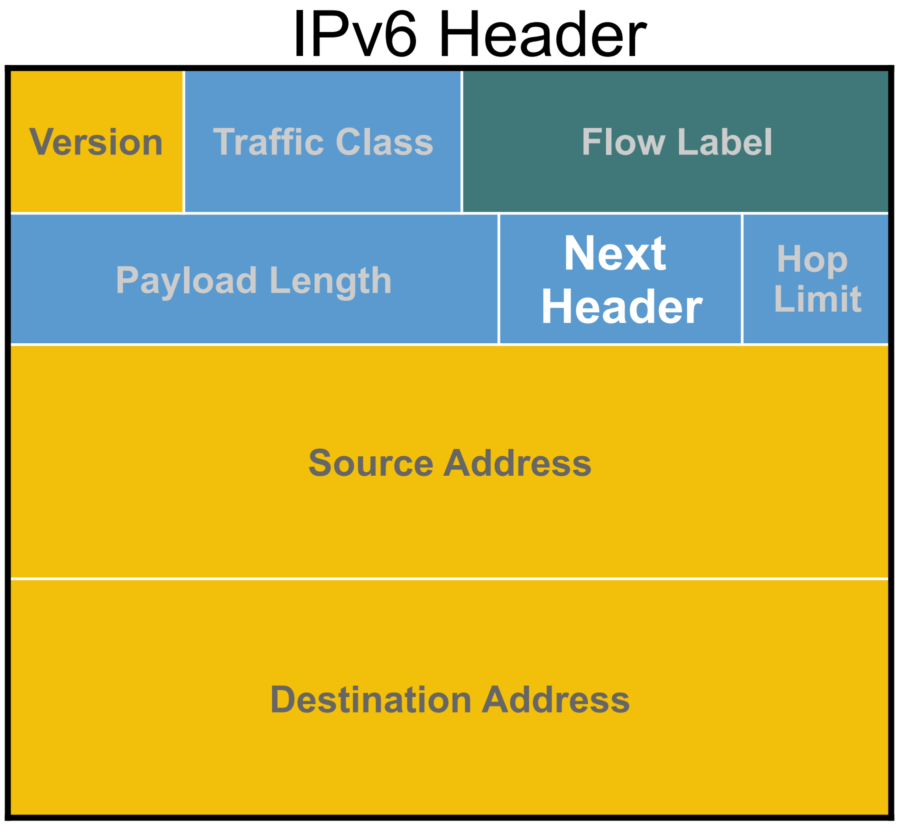
IPv6 Header



IPv4 and IPv6 Header Comparison
Fields Renamed

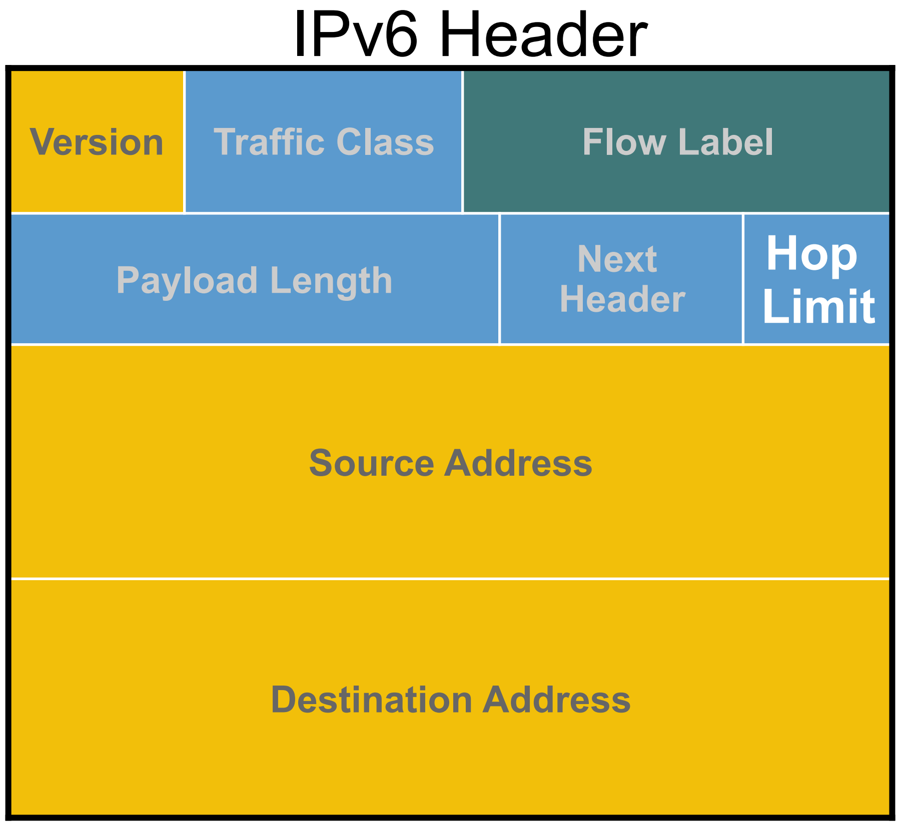
- Next header: similar to the protocol field in IPv4
- The value in this field tells you what type of information follows

  E.g. TCP, UDP, extension header



IPv4 and IPv6 Header Comparison Fields Renamed

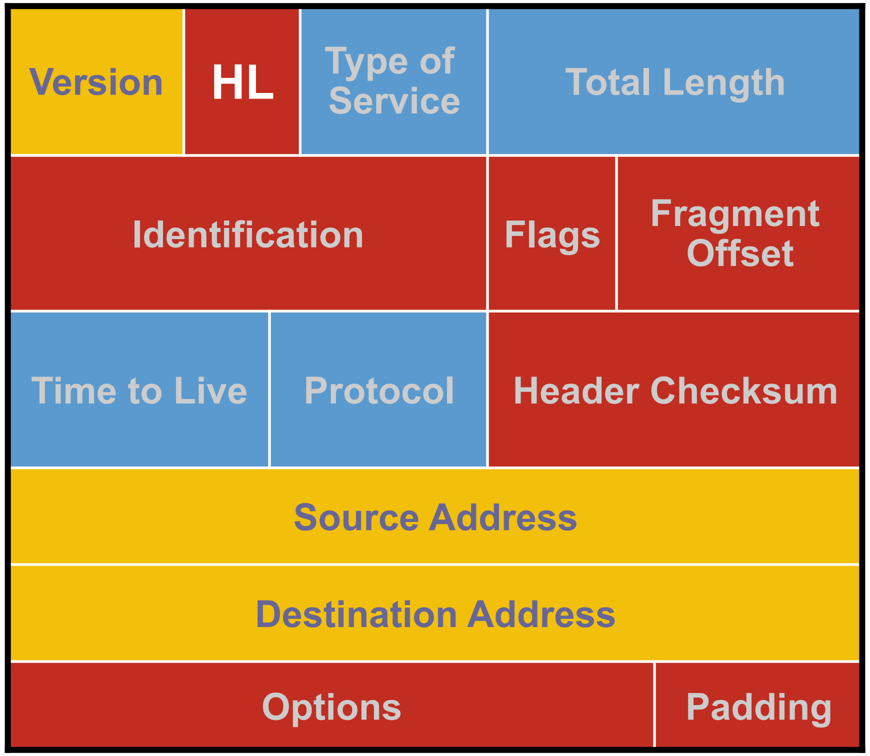
- Hop limit: like TTL field, decrements by one for each router



IPv4 and IPv6 Header Comparison
Fields Removed

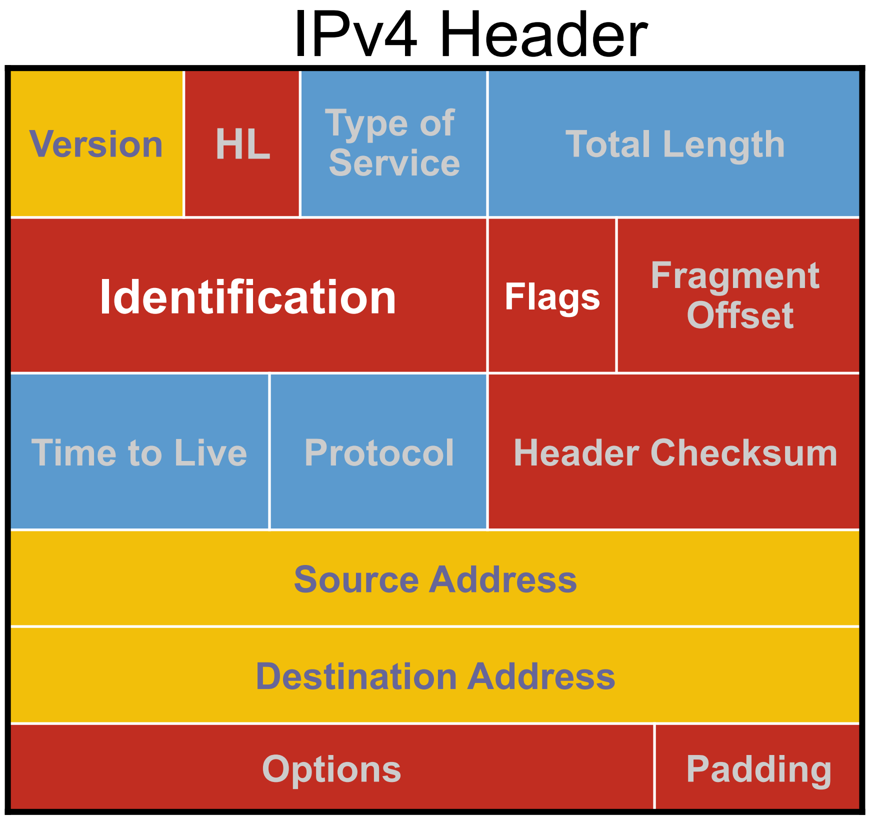
- Header length: IPv6 has a fixed header length (40 bytes)

IPv4 Header



IPv4 and IPv6 Header Comparison
Fields Removed

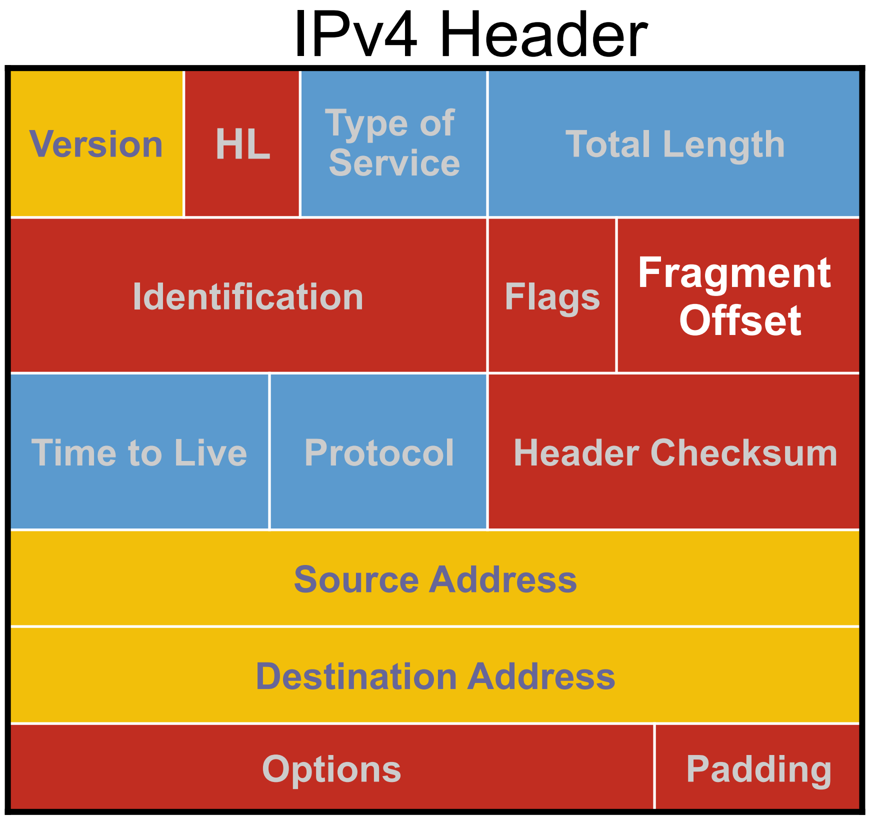
- Identification: used to identify the datagram from the source
- No fragmentation is done in IPv6 so no need for identification, also no need for flags



2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

IPv4 and IPv6 Header Comparison Fields Removed

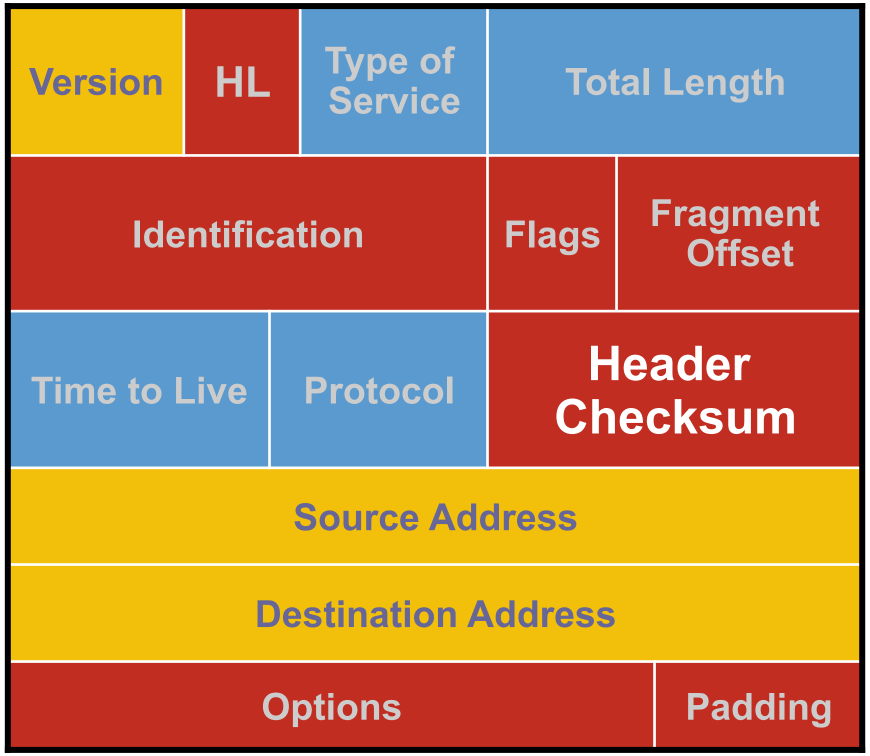
- Fragmentation: IPv6 does not do fragmentation
- If a sending host wants to do fragmentation, it will do it through extension headers



IPv4 and IPv6 Header Comparison Fields Removed

- Checksum not needed because both media access and upper layer protocol (UDP and TCP) have the checksum; IP is best-effort, plus removing checksum helps expedite *Packet* processing

IPv4 Header

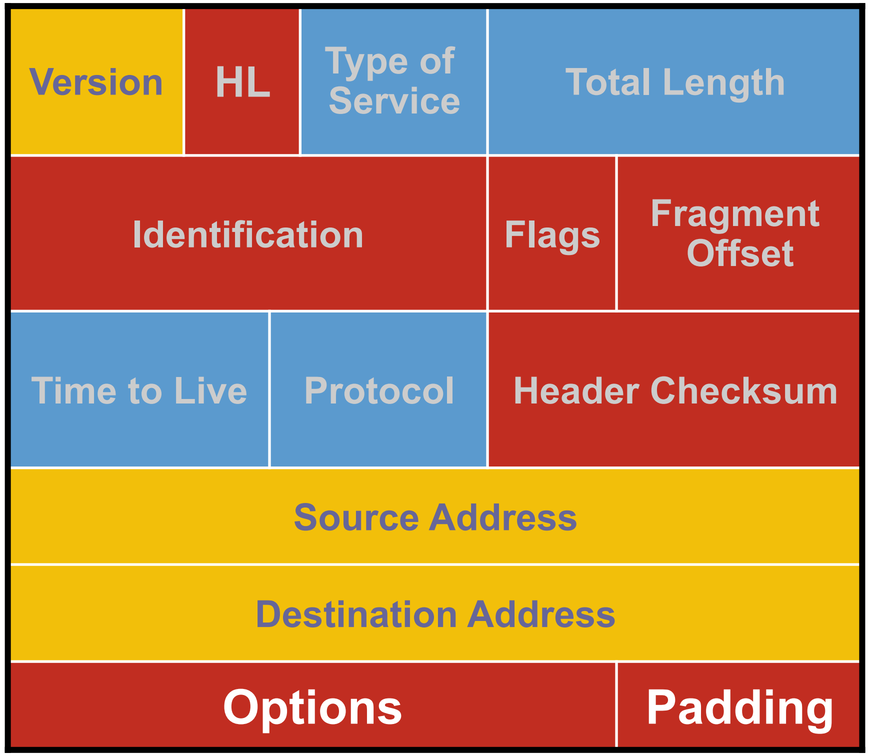


2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

IPv4 and IPv6 Header Comparison
Fields Removed

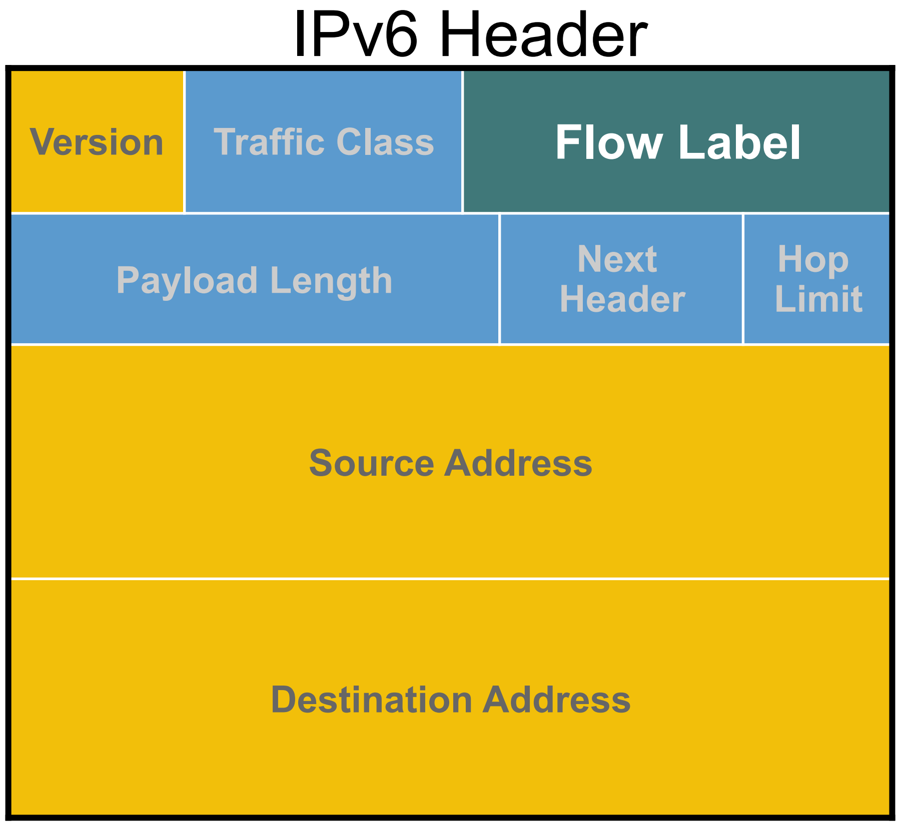
- Options removed since it is normally disabled by SPs

IPv4 Header



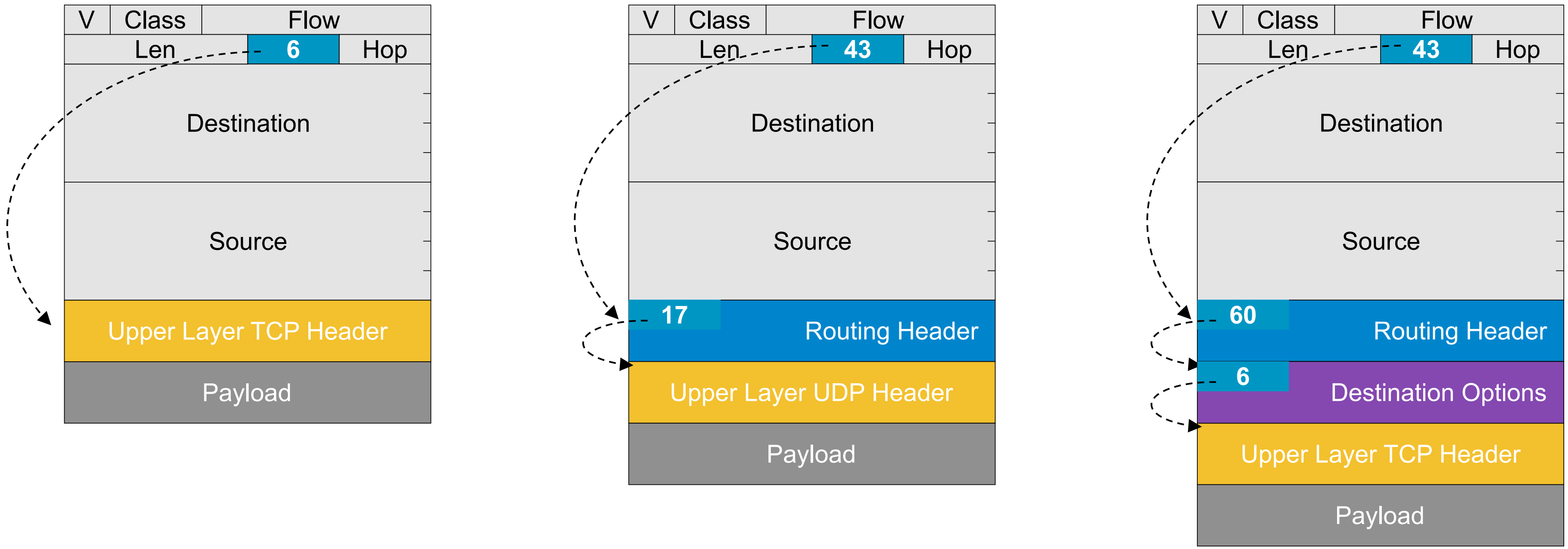
IPv4 and IPv6 Header Comparison Fields Added

- 20-bit flow label field to identify specific flows needing special QoS
  - 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)



RFC 3697

Extension Headers



- Extension Headers Are Daisy Chained

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

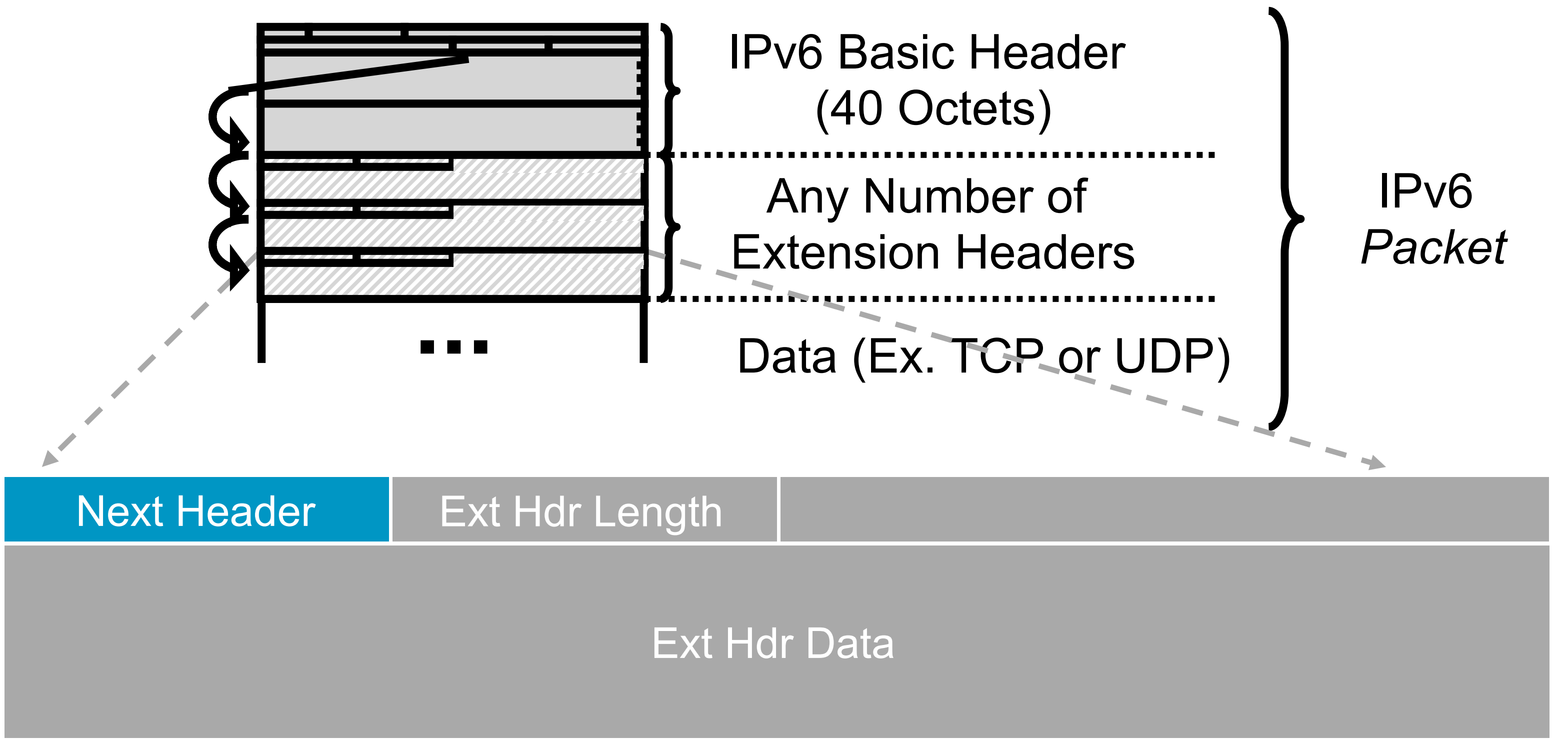
Header Format Simplification
IPv6 Extension Headers

- Extension headers must be in the following sequence

Order	Header Type	Header Code
1	Basic IPv6 Header	-
2	Hop-by-Hop Options	0
3	Dest Options (with Routing options)	60
4	Routing Header	43
5	Fragment Header	44
6	Authentication Header	51
7	ESP Header	50
8	Destination Options	60
9	Mobility Header	135
-	No Next Header	59
Upper Layer	TCP	6
Upper Layer	UDP	17
Upper Layer	ICMPv6	58

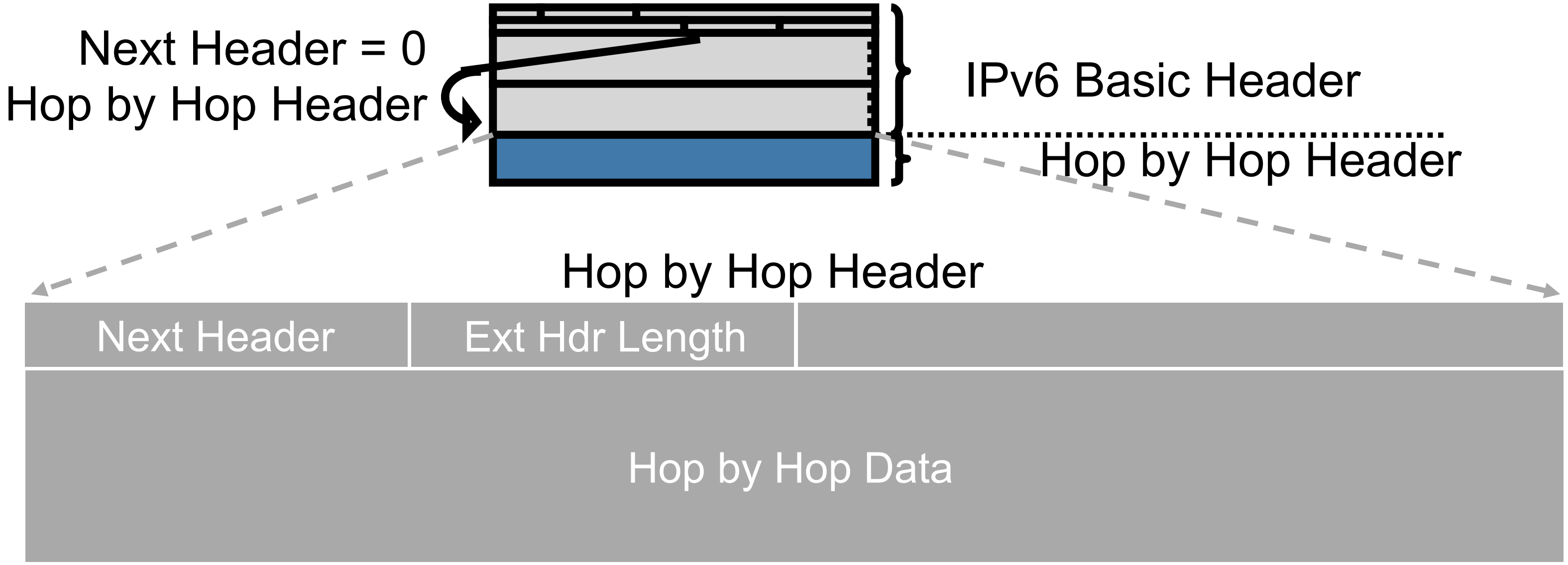
2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Extension Header Order



- Next header = TCP/UDP or extension header
- Extension headers are optional following the IPv6 basic header
- Each extension header is 8 octets (64 bits) aligned

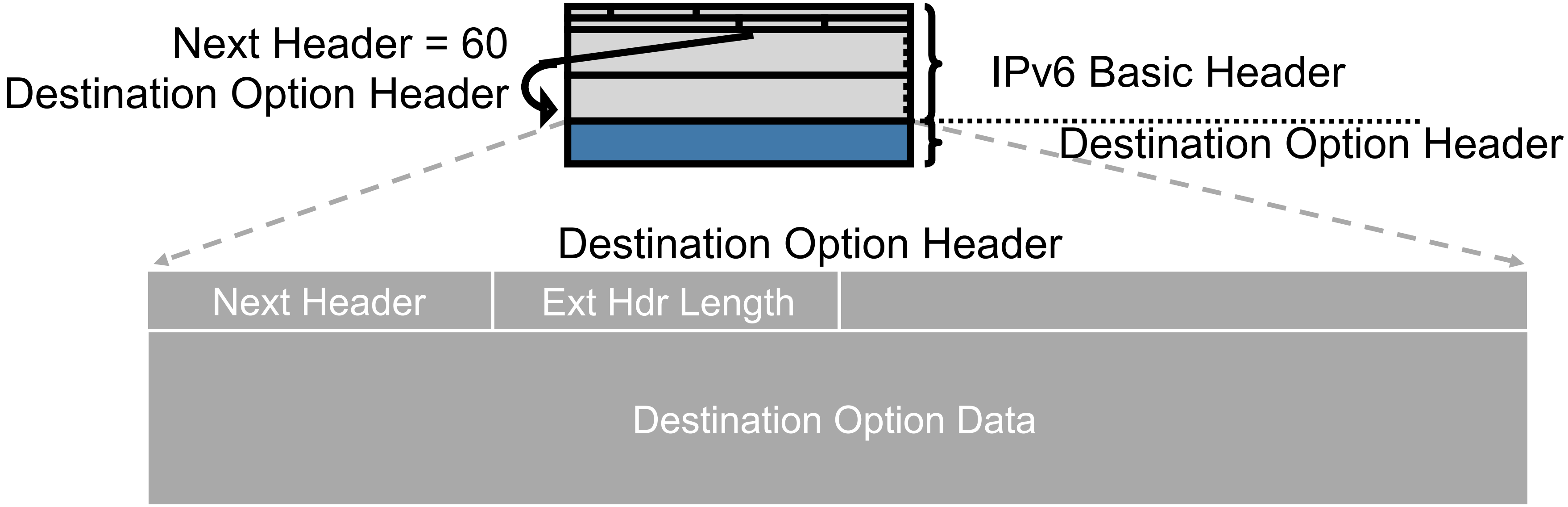
IPv6 Extension Header Types
Hop by Hop Header (Protocol 0)



- Read and processed by every node and router along the delivery path
- When present, follows immediately after the basic IPv6 *Packet* header
- Used for router alerts; an example of applying this option would be RSVP, because each router needs to look at it

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

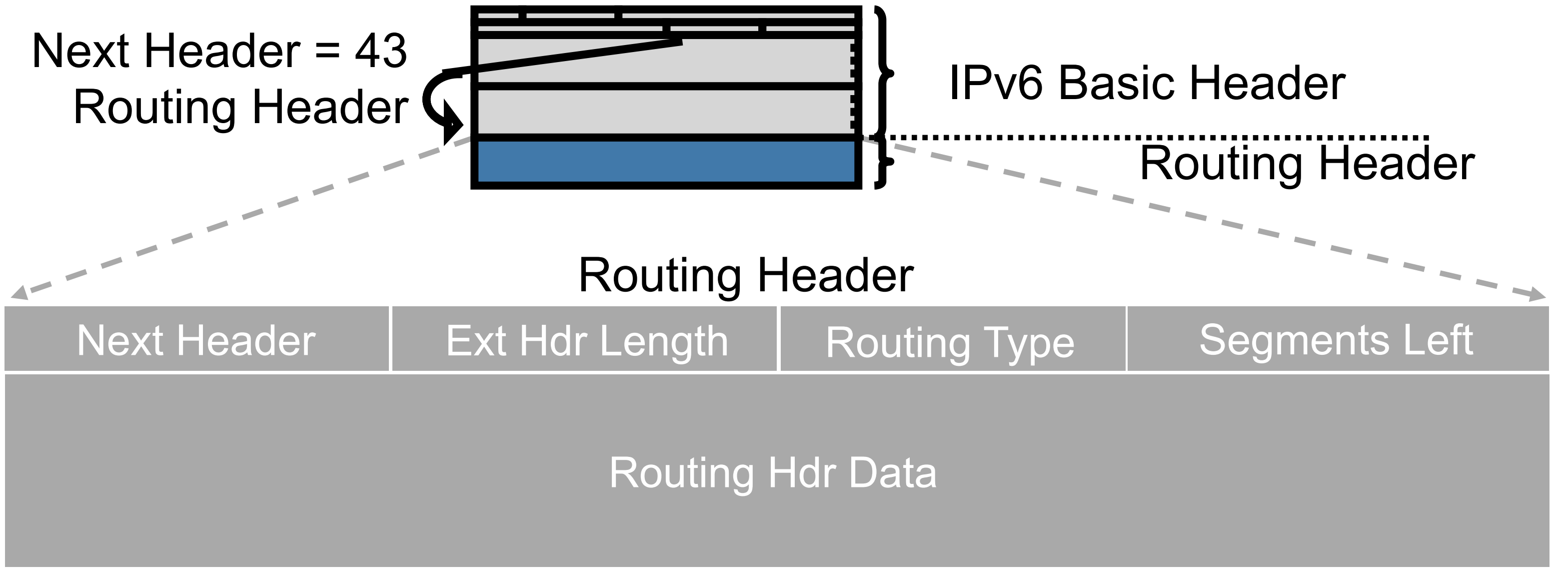
IPv6 Extension Header Types
Destination Option Header (Protocol 60)



- Carries optional information that is specifically targeted to *Packet*' s destination address
- The Mobile IPv6 uses this option to exchange registration messages between mobile nodes and the home agent

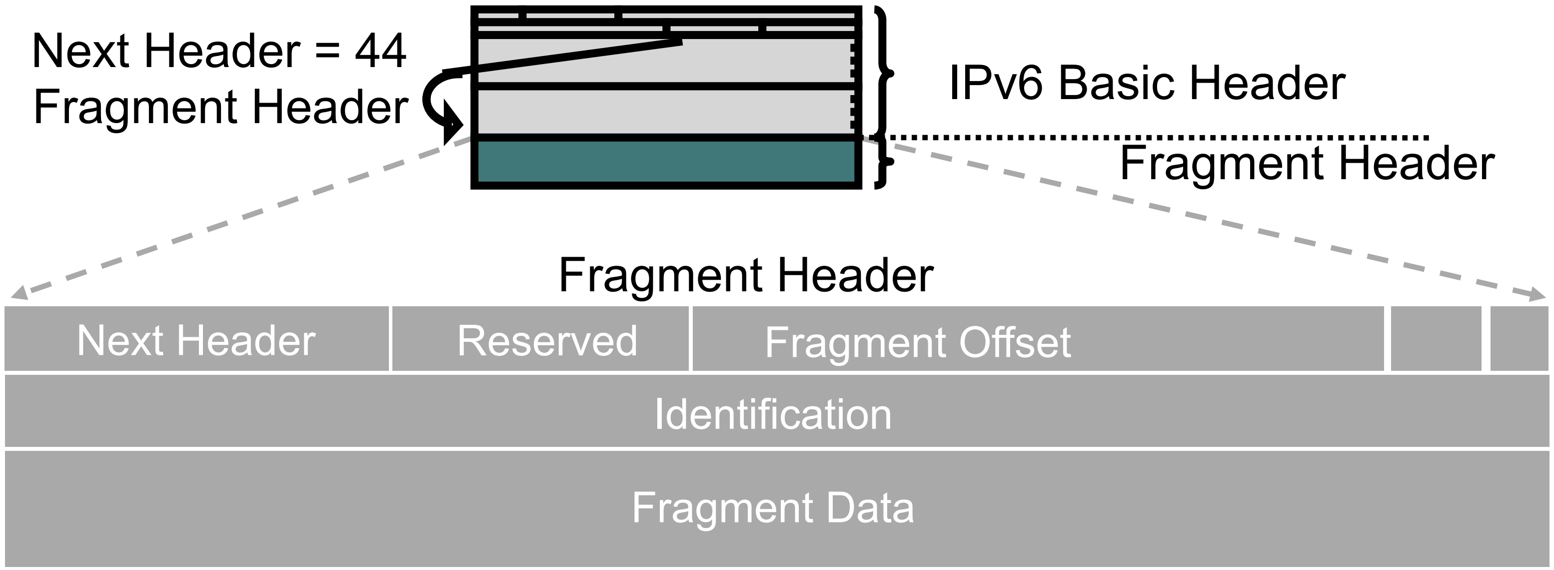
2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

IPv6 Extension Header Types
Routing Header (Protocol 43)



- Routing header forces the routing through a list of intermediate routers
- This is similar to the "loose source route" option in IPv4

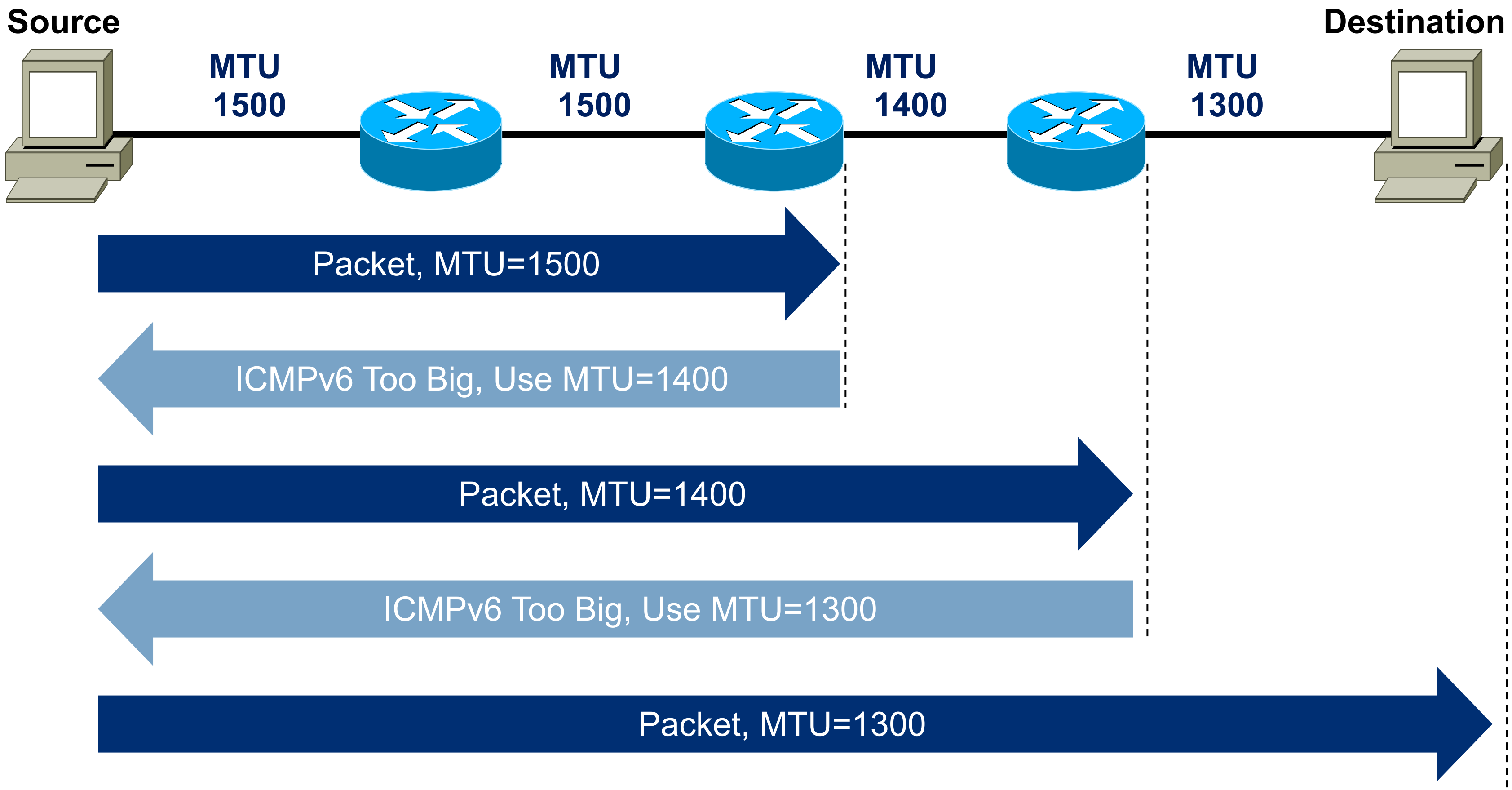
IPv6 Extension Header Types
Fragment Header (Protocol 44)



- Used by source when *Packet* is fragmented
- Fragment header is used in each fragmented *Packet*
- Fragment offset: identifies the position of the specific fragment in the full original *Packet*
- Identification: a number to identify fragments of the same original *Packet*
- Fragment data: used by destination node to reassemble the *Packet* in its original form

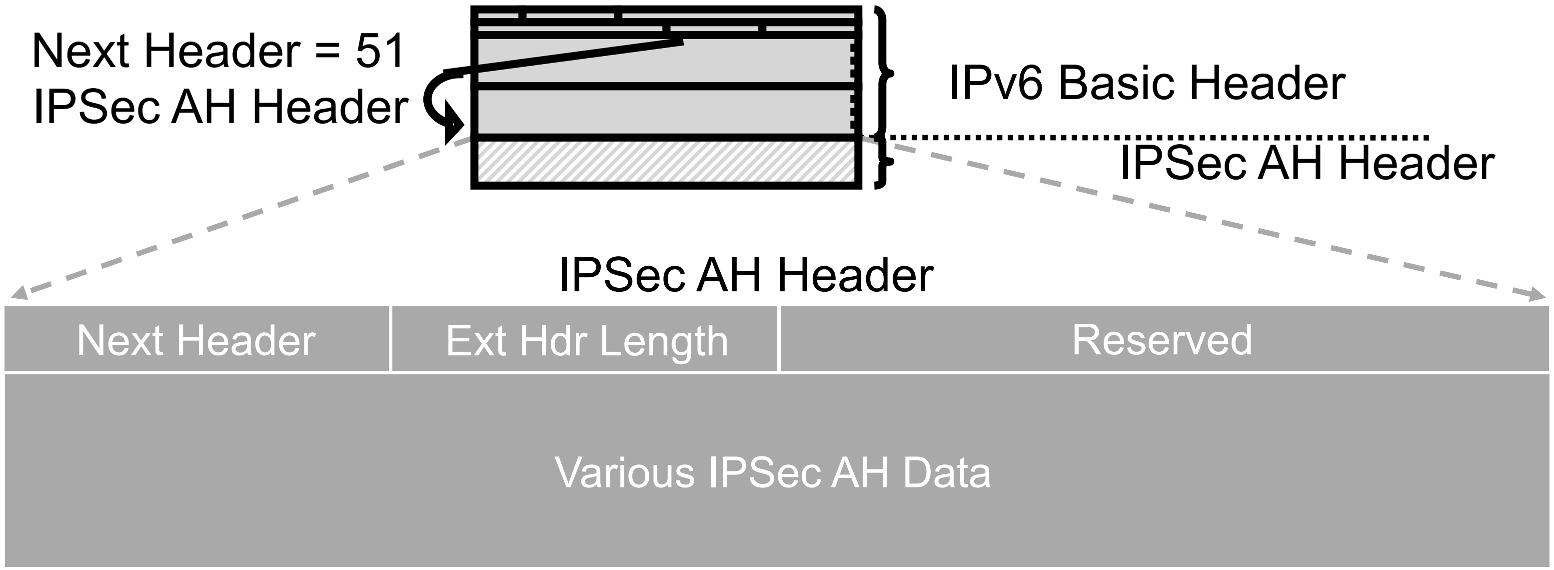
2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Path MTU Discovery



- Store PMTU per destination (if received)
- Age out PMTU (10 mins), reset to first link MTU

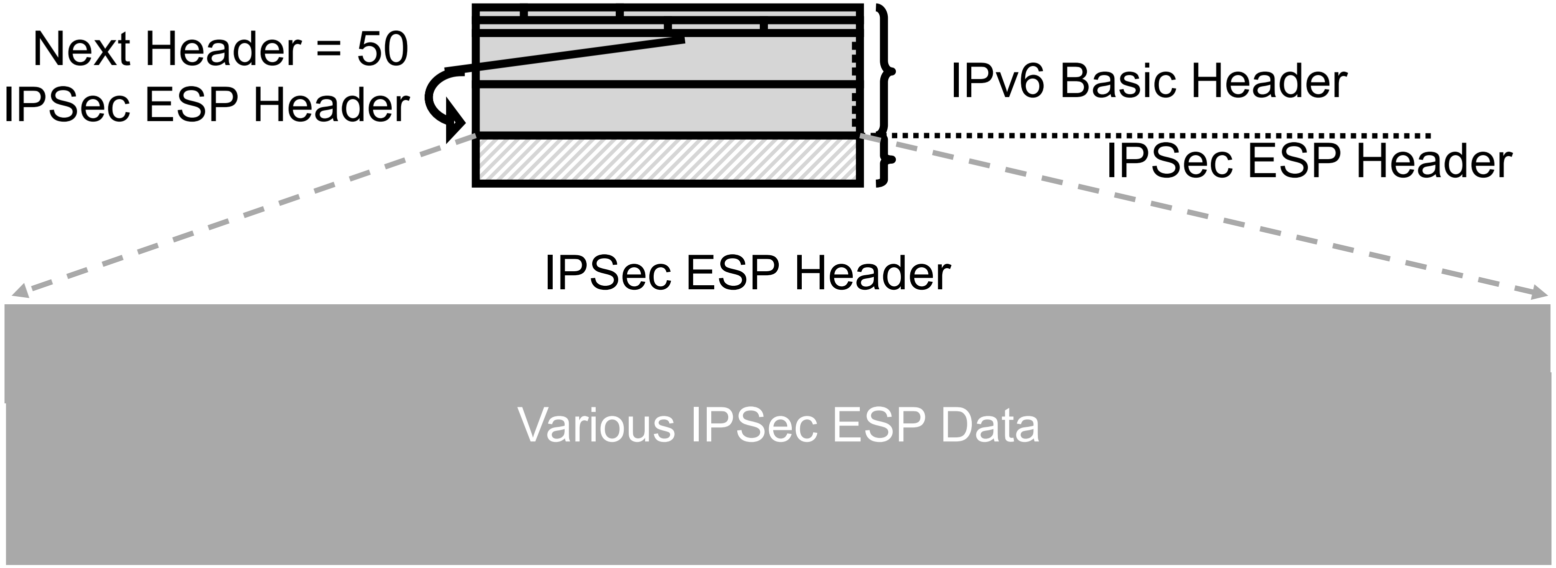
IPv6 Extension Header Types
IPSec Authentication Header (Protocol 51)



- IPSec Authentication Header (AH) provides:
  - Integrity
  - Authentication of the source

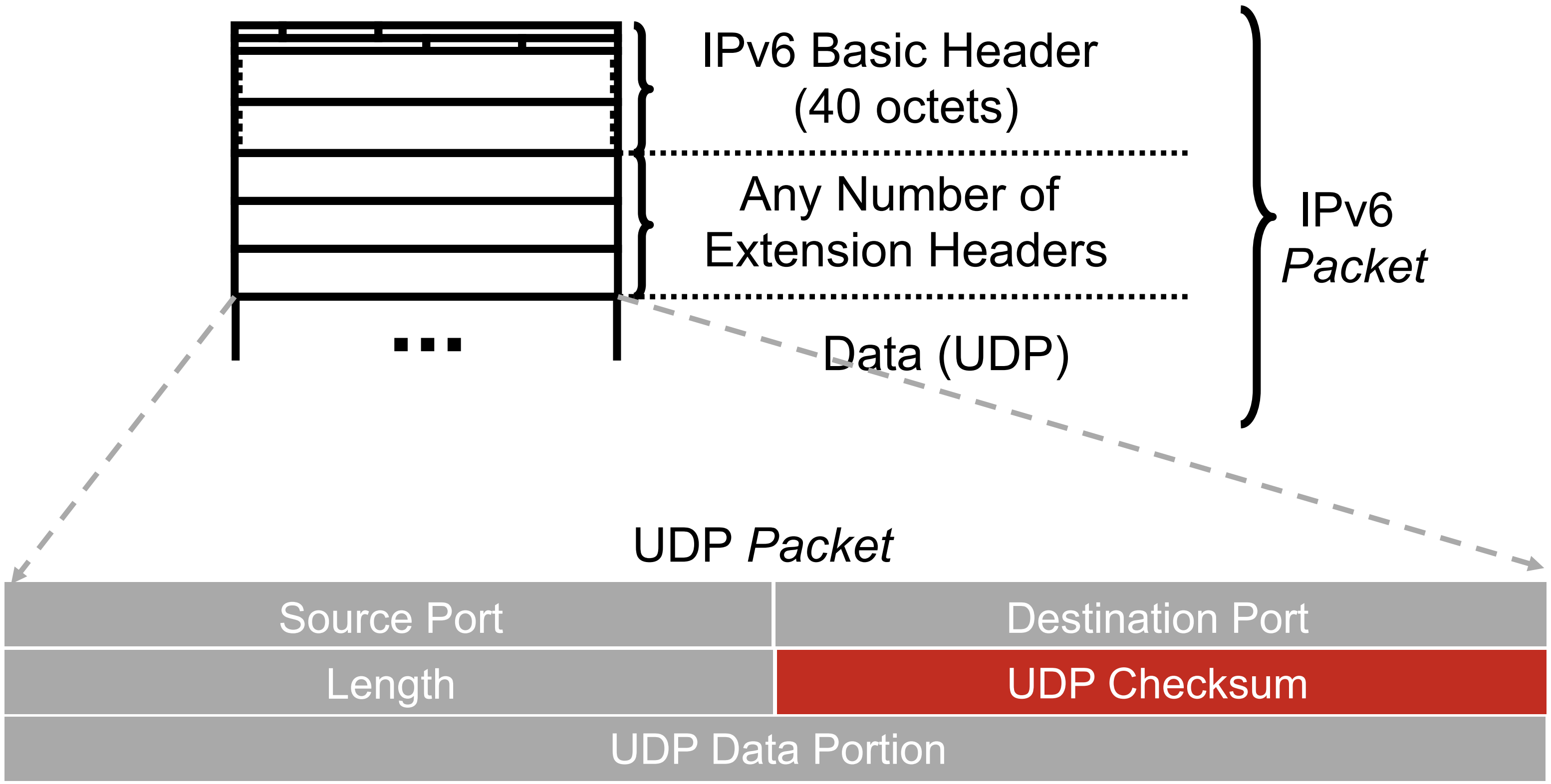
2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

IPv6 Extension Header Types
IPSec ESP (Protocol 50)



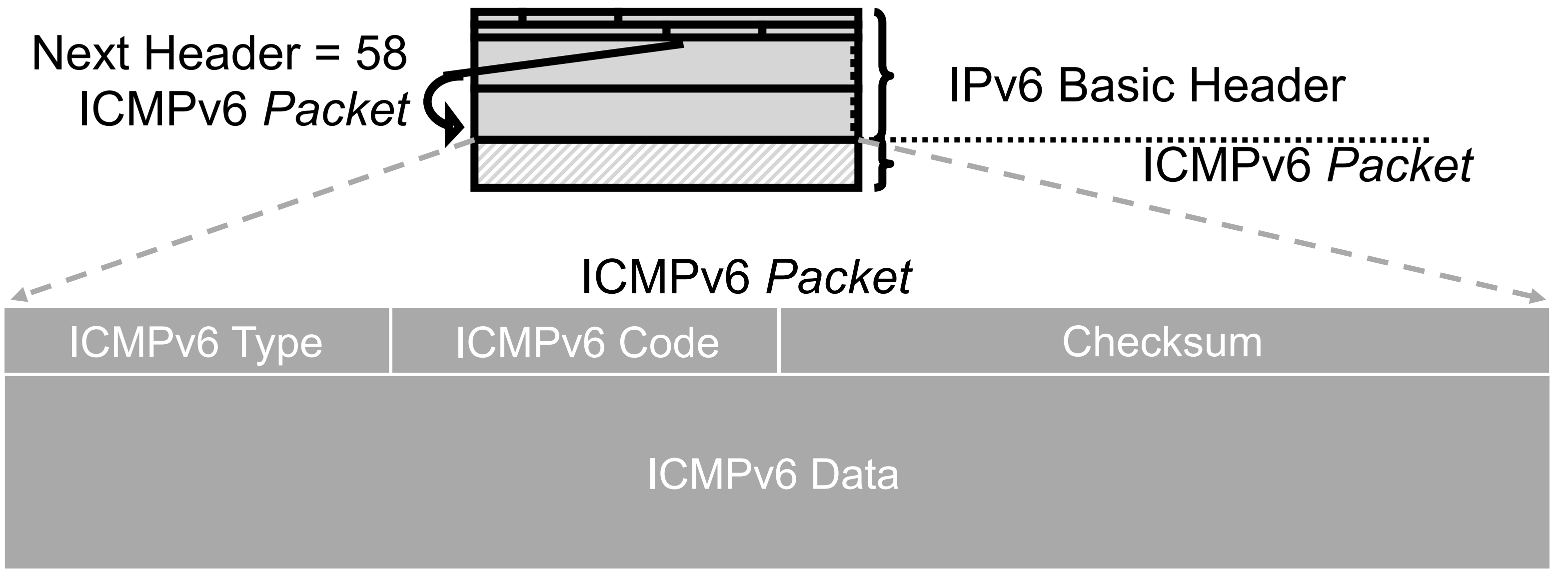
- IPSec Encapsulating Security Payload (ESP) provides:
  - Confidentiality
  - Integrity
  - Authentication of the source

Upper Layer Header
User Datagram Protocol (Protocol 17)



- Upper layer (UDP, TCP, ICMPv6) checksum must be computed
- These are the typical headers used inside a *Packet* to transport data
- This could be UDP (Protocol 17), TCP (Protocol 6), or ICMPv6 (Protocol 58)

Upper Layer Header
ICMPv6 (Protocol 58)



- ICMPv6 is similar to IPv4: provides diagnostic and error messages
- Additionally, it’s used for neighbor discovery, path MTU discovery

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

IPv6 Addressing

IPv6 Addressing

IPv4 32-bits

IPv6 128-bits

$2^{32} = 4{,}294{,}967{,}296$

$2^{128} = 340{,}282{,}366{,}920{,}938{,}463{,}463{,}374{,}607{,}431{,}768{,}211{,}456$

$2^{128} = 2^{32} * 2^{96}$

2^{96} = 79,228,162,514,264,337,593,543,950,336 times the number of possible IPv4 Addresses
(79 trillion trillion)

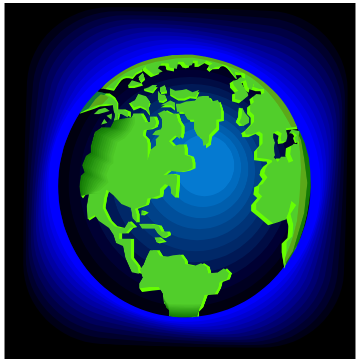
2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

IPv4 / IPv6 Technology Comparison

Service	IPv4	IPv6
Addressing Range	32-bit, NAT	128-bit, Multiple Scopes
IP Provisioning	DHCP	SLAAC, Renumbering, DHCP
Security	IPSec	IPSec
Mobility	Mobile IP	Mobile IP with Direct Routing
Quality-of-Service	Differentiated Service, Integrated Service	Differentiated Service, Integrated Service
Multicast	IGMP/PIM/MBGP	MLD/PIM/MBGP, Scope Identifier

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

IPv6 Addressing



World's population is approximately 6.5 billion

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

= 52 Trillion Trillion IPv6 addresses per person

Typical brain has ~100 billion brain cells (your count may vary)

$$\frac{52 \text{ Trillion Trillion}}{100 \text{ Billion}}$$

= 523 Quadrillion (523 thousand trillion) IPv6 addresses for every human brain cell on the planet!

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

IPv6 Addressing

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

  2003:0000:130F:0000:0000:087C:876B:140B

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

IPv6 Address Representation

- 16-bit fields in colon hexadecimal representation

  2031:0000:130F:0000:0000:09C0:876A:130B

- Leading zeros in a field are optional

  2031:0:130F:0:0:9C0:876A:130B

- Successive fields of 0 represented as (::), but only once in an address

  2031:0:130F::9C0:876A:130B

  2031::130F::9C0:876A:130B not valid!

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

IPv6 Prefix Representation

- Representation of prefix is just like CIDR
- In this representation you attach the prefix length
- IPv4 address: 198.10.0.0/16
- IPv6 address: 3ef8:ca62:12FE::/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

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

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)

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

IPv6 Addressing Model

- Addresses are assigned to interfaces
- Interface “expected” to have multiple addresses
- Addresses have scope
  - Link Local
  - Unique Local
  - Global
- Addresses have lifetime
  - Valid and preferred lifetime

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

IPv6 Addressing Type

Type	Binary	Hex
Global Unicast Address	001	2 or 3
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::/16
Solicited Node Multicast		FF02::1:FF/104

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Type 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

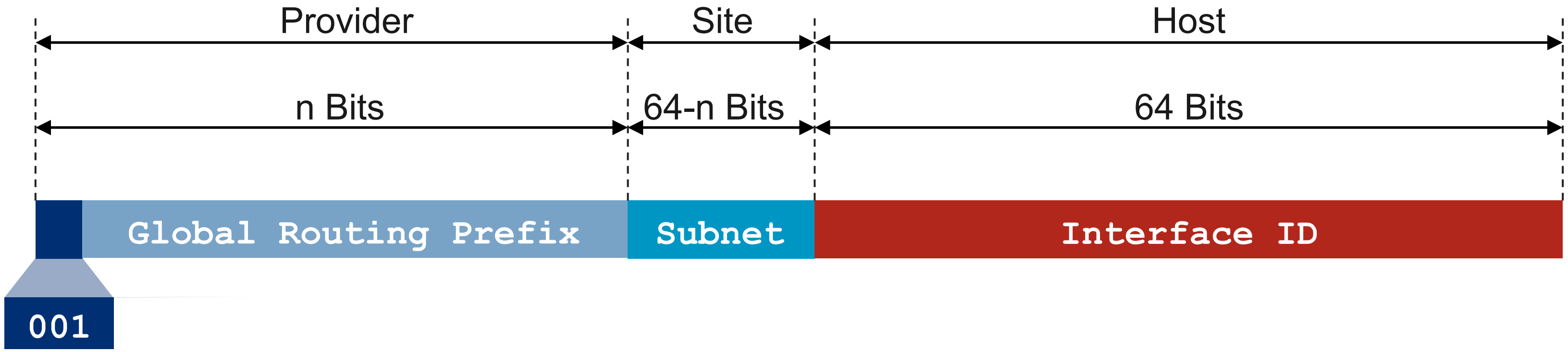
2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Interface Address Set

- An interface can have many addresses allocated to it

Address Type	Requirement	Comment
Link Local	Required	Required on all interfaces
Unique Local	Optional	Valid only within an Administrative Domain
Global Unicast	Optional	Globally routed prefix
Auto-Config 6to4	Optional	Used for 2002:: 6to4 tunnelling
Solicited Node Multicast	Required	Neighbour Discovery and Duplicate Detection (DAD)
All Nodes Multicast	Required	For ICMPv6 messages

Aggregatable Global Unicast Addresses

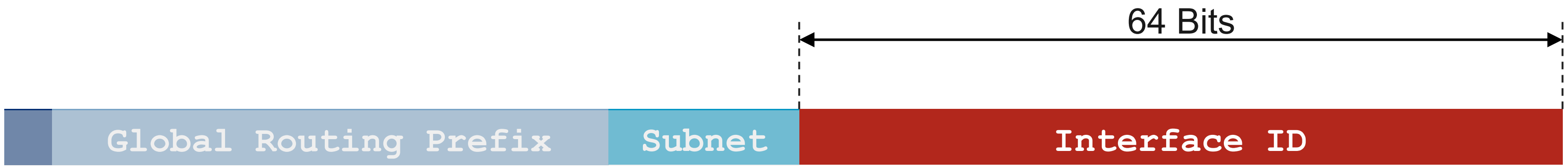


- Aggregatable global unicast addresses are:
  - Addresses for generic use of IPv6
  - Structured as a hierarchy to keep the aggregation
- See RFC 3513

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Interface ID

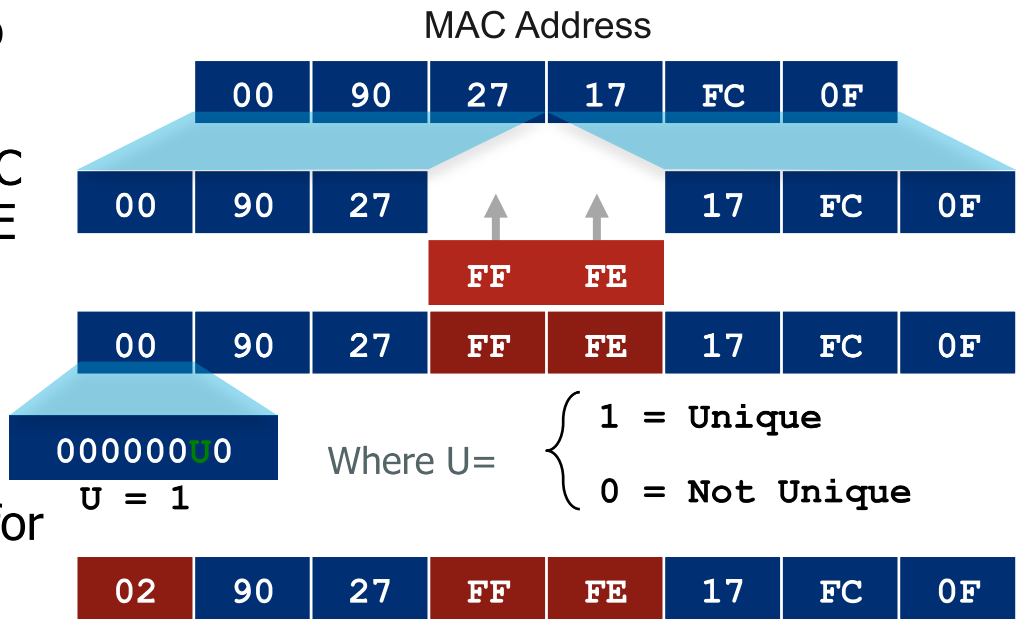
- Interface ID unicast address may be assigned in different ways
  - Auto-configured from a 64-bit EUI-64 or expanded from a 48-bit MAC
  - Auto-generated pseudo-random number (to address privacy concerns)
  - Assigned via DHCP
  - Manually configured
- EUI-64 format to do stateless auto-configuration
  - Expands the 48 bit MAC address to 64 bits by inserting FFFE into the middle
  - To ensure 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



2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

IPv6 Interface ID (EUI-64)

- 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
- Cisco devices 'bit-flip' the 7th bit



2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

IPv6 over Ethernet

- IPv6 uses Ethernet Protocol ID (0x86DD)

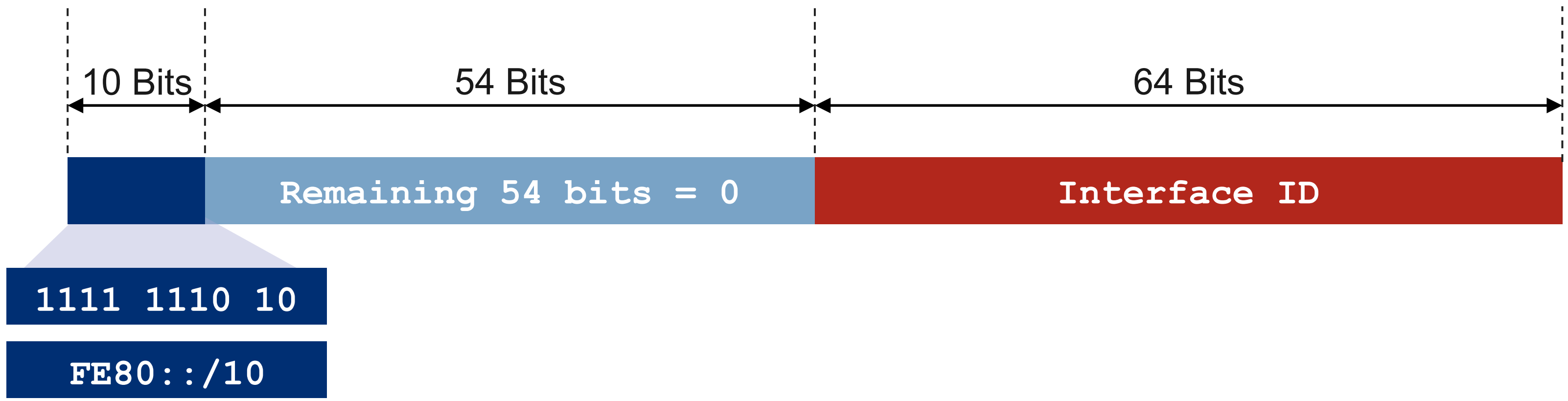
Dest MAC	Source MAC	0x86DD	IPv6 Header and Payload

- IPv4 uses Ethernet Protocol ID (0x0800)

Dest MAC	Source MAC	0x0800	IPv4 Header and Payload

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

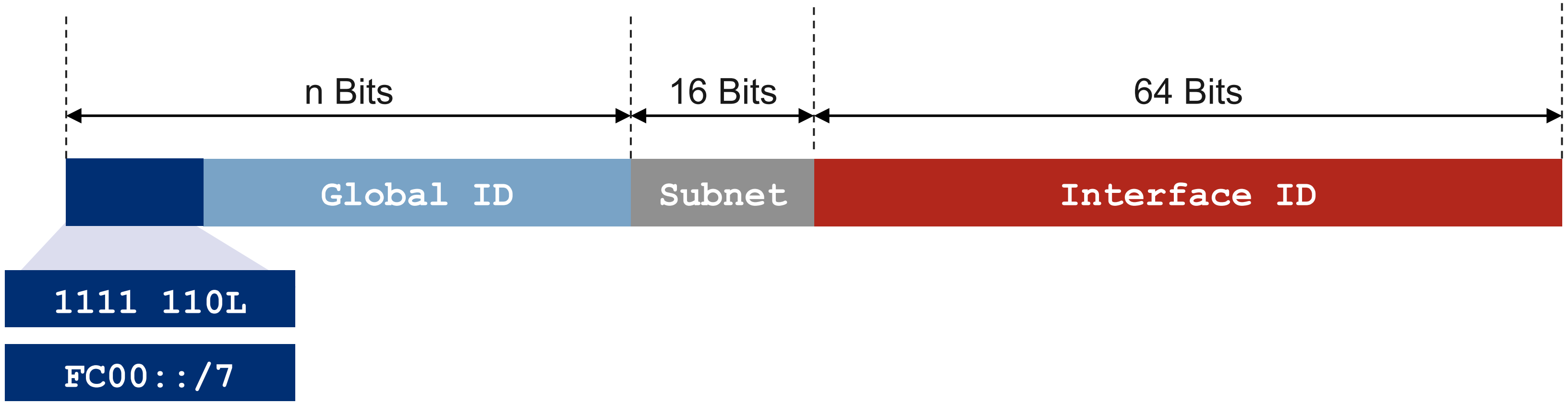
Link-Local



- Link-local addresses:
  - Only Link Specific scope
  - Automatically assigned by Router as soon as IPv6 is enabled
  - Also used for Next-Hop calculation in Routing Protocols

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Unique-Local Addresses



- ULA are “like” RFC 1918 – not routable on Internet
- ULA uses include
  - Local communications
  - Inter-site VPNs (Mergers and Acquisitions)
- FC00::/8 is Registry Assigned (L bit = 0), FD00::/8 is self generated (L bit = 1)
  - Registries not yet assigning ULA space, http://www.sixxs.net/tools/grh/ula/
- Global ID can be generated using an algorithm
  - Low order 40 bits result of SHA-1 Digest {EUI-64 && Time}

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

IPv6 Multicast Address (RFC 4291)

- An IPv6 multicast address has the prefix FF00::/8 (1111 1111)
  Second octet defines lifetime and scope

8Bits	4 Bits	4 Bits	112 Bits
1111 1111	0 R P T	Scope	Variable Format

(RFC 4291)

Flags	
R = 0 R = 1	No embedded RP Embedded RP
P = 0 P = 1	Not based on unicast Based on unicast
T = 0 T = 1	Permanent address (IANA assigned) Temporary address (local assigned)

Scope	
1	Node
2	Link
3	Subnet
4	Admin
5	Site
8	Organization
E	Global

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Well Known Multicast Addresses

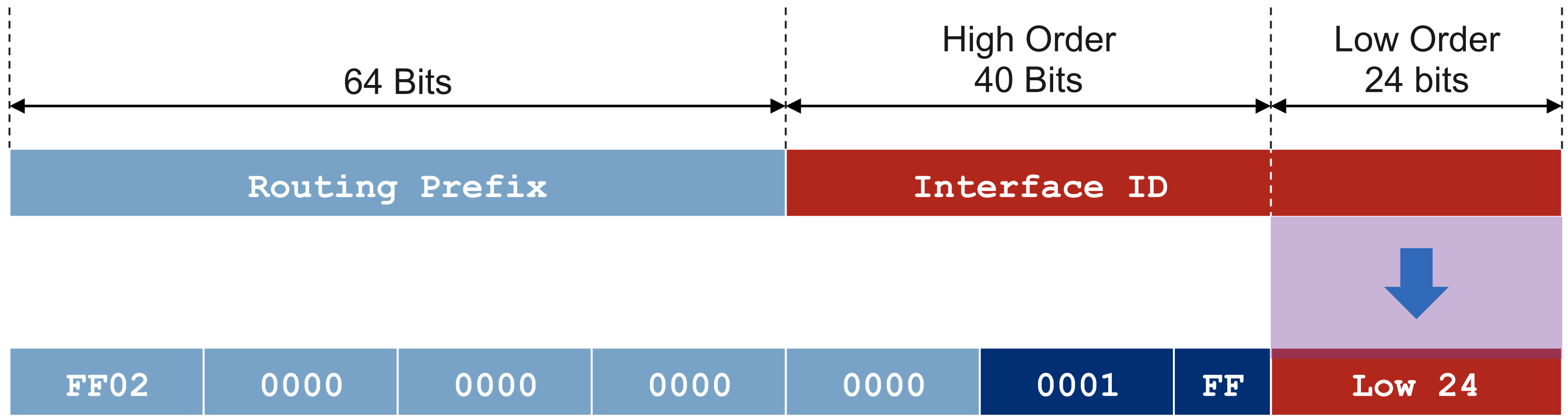
Address	Scope	Meaning
FF01::1	Node-Local	All Nodes
FF01::2	Node-Local	All Routers
FF02::1	Link-Local	All Nodes
FF02::2	Link-Local	All Routers
FF02::5	Link-Local	OSPFv3 Routers
FF02::6	Link-Local	OSPFv3 DR Routers
FF02::1:FFXX:XXXX	Link-Local	Solicited-Node

- "02" means that this is a permanent address (t = 0) and has link scope (2)
- http://www.iana.org/assignments/ipv6-multicast-addresses

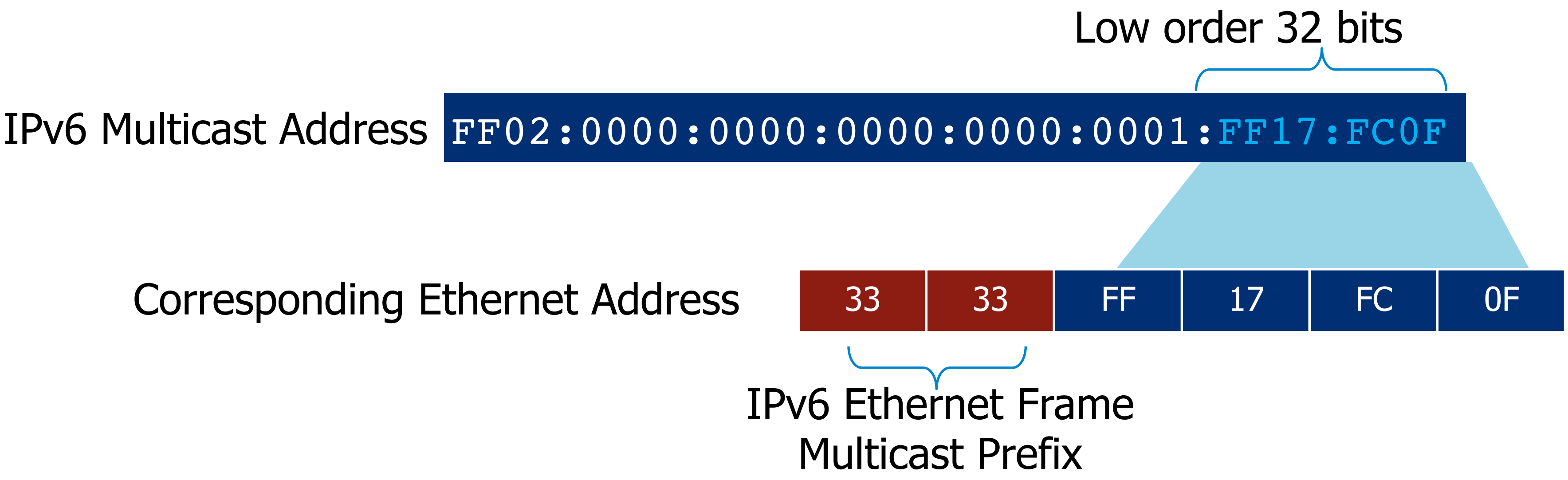
Solicited-Node Multicast Address

- For each Unicast and Anycast address configured there is a corresponding solicited-node multicast (Layer 3 address)
- Used in neighbor solicitation (NS) messages
- Multicast address with a link-local scope
- Solicited-node multicast consists of

  FF02::1:FF & {lower 24 bits from IPv6 Unicast interface ID}



Multicast Mapping over Ethernet (RFC 2464)

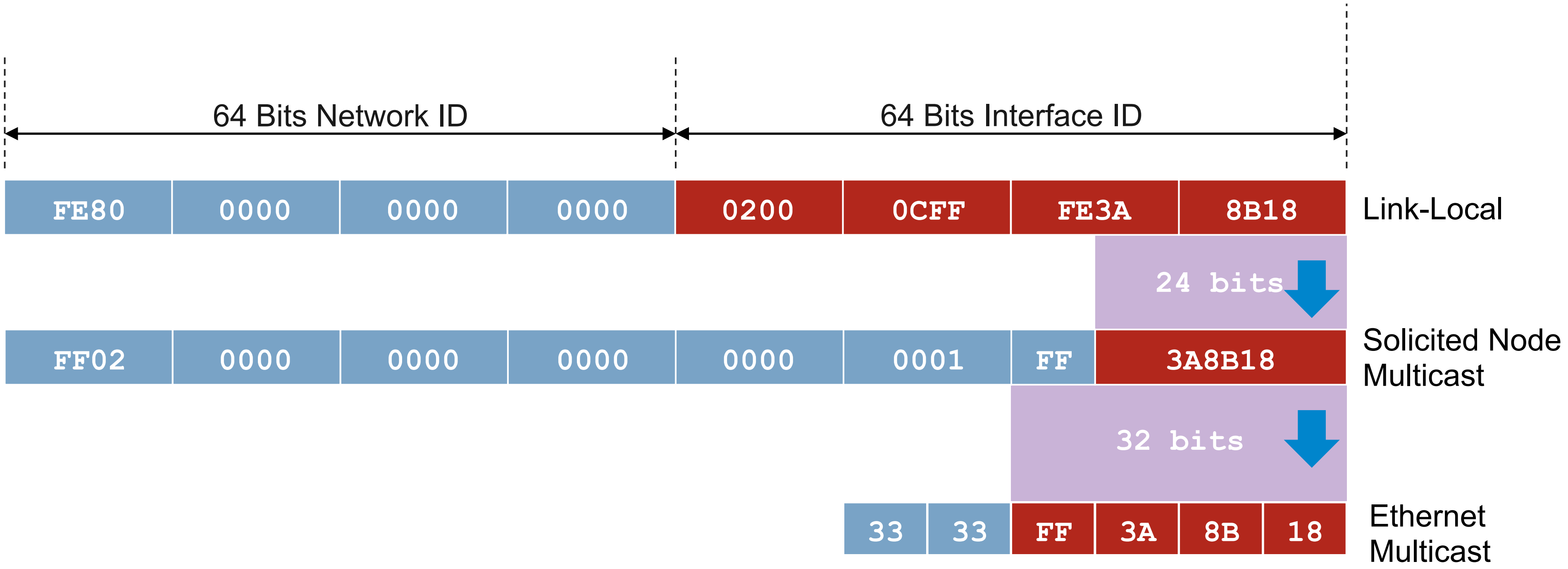


- IPv6 multicast address to Ethernet mapping

  33:33:{Low Order 32 bits of the IPv6 multicast address}

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Solicited Node Multicast Address Example



2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

IPv6 Interface Example

```
R1#show ipv6 interface 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#
```

Link-local address (FE80::)

All Nodes

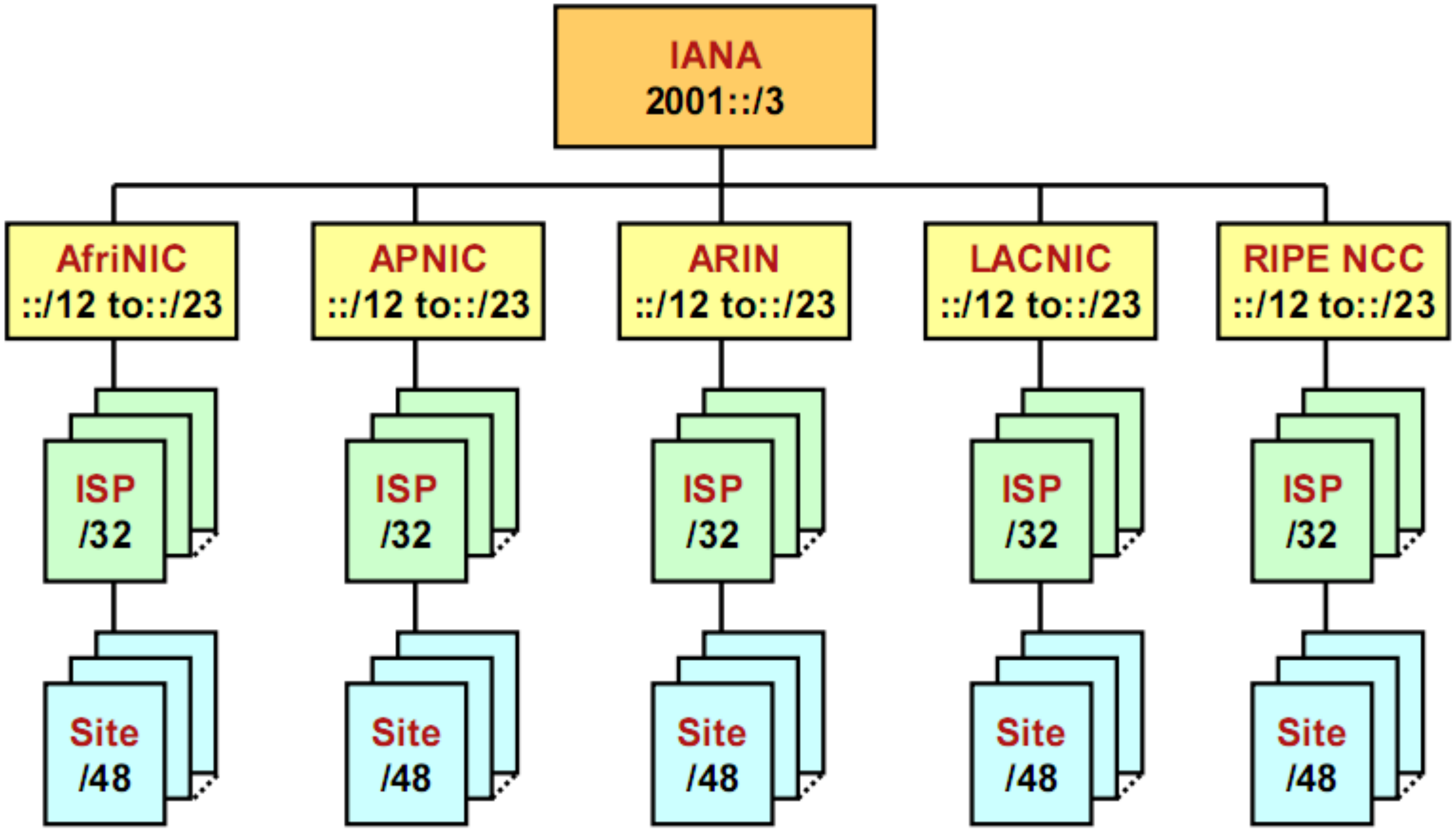
All Routers

Solicited Node Multicast Address

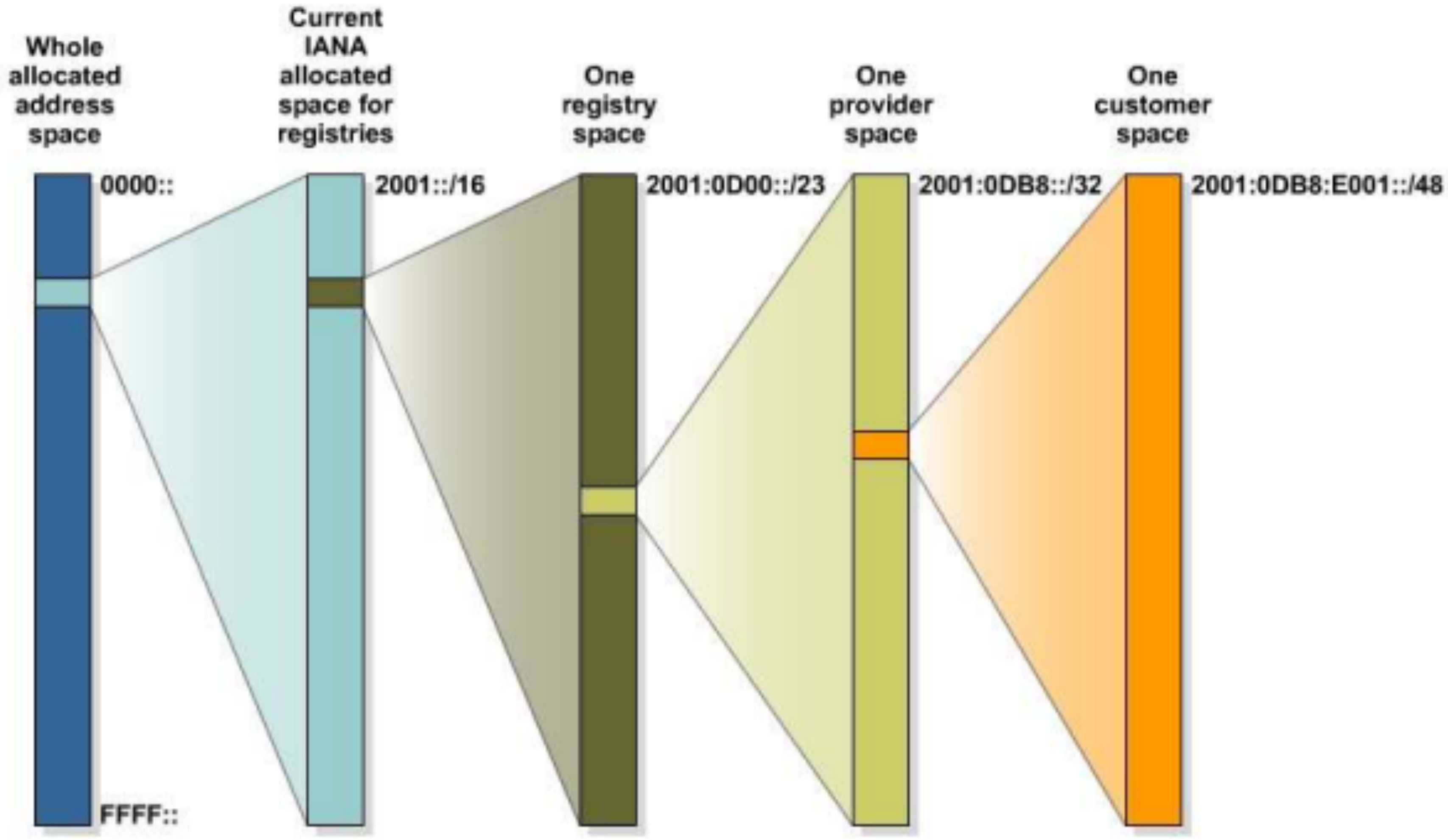
2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

IPv6 Address Allocation Process

IPv6 Prefix Allocation Hierarchy

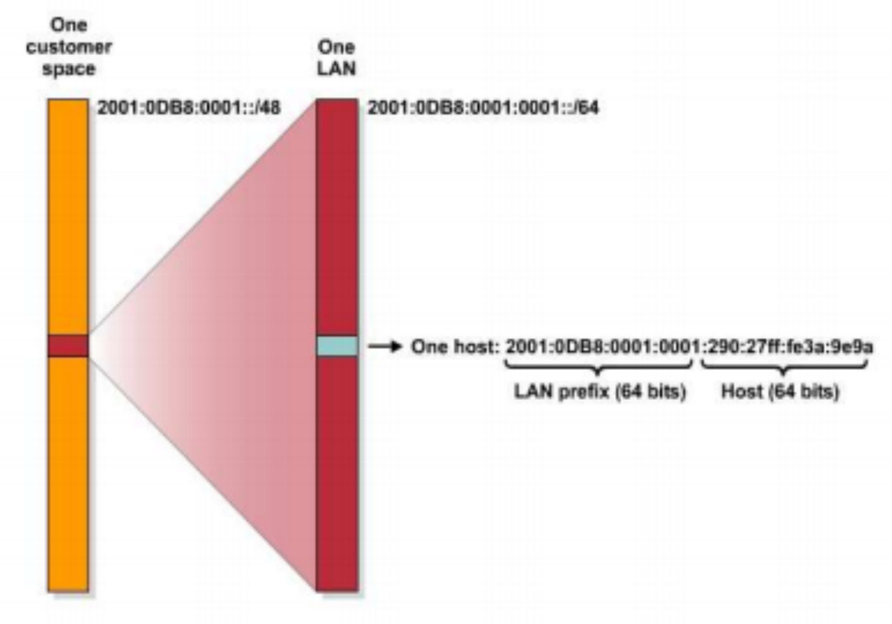


IPv6 Address Allocation Process



IPv6 Address Allocation Process (contd.)

- 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

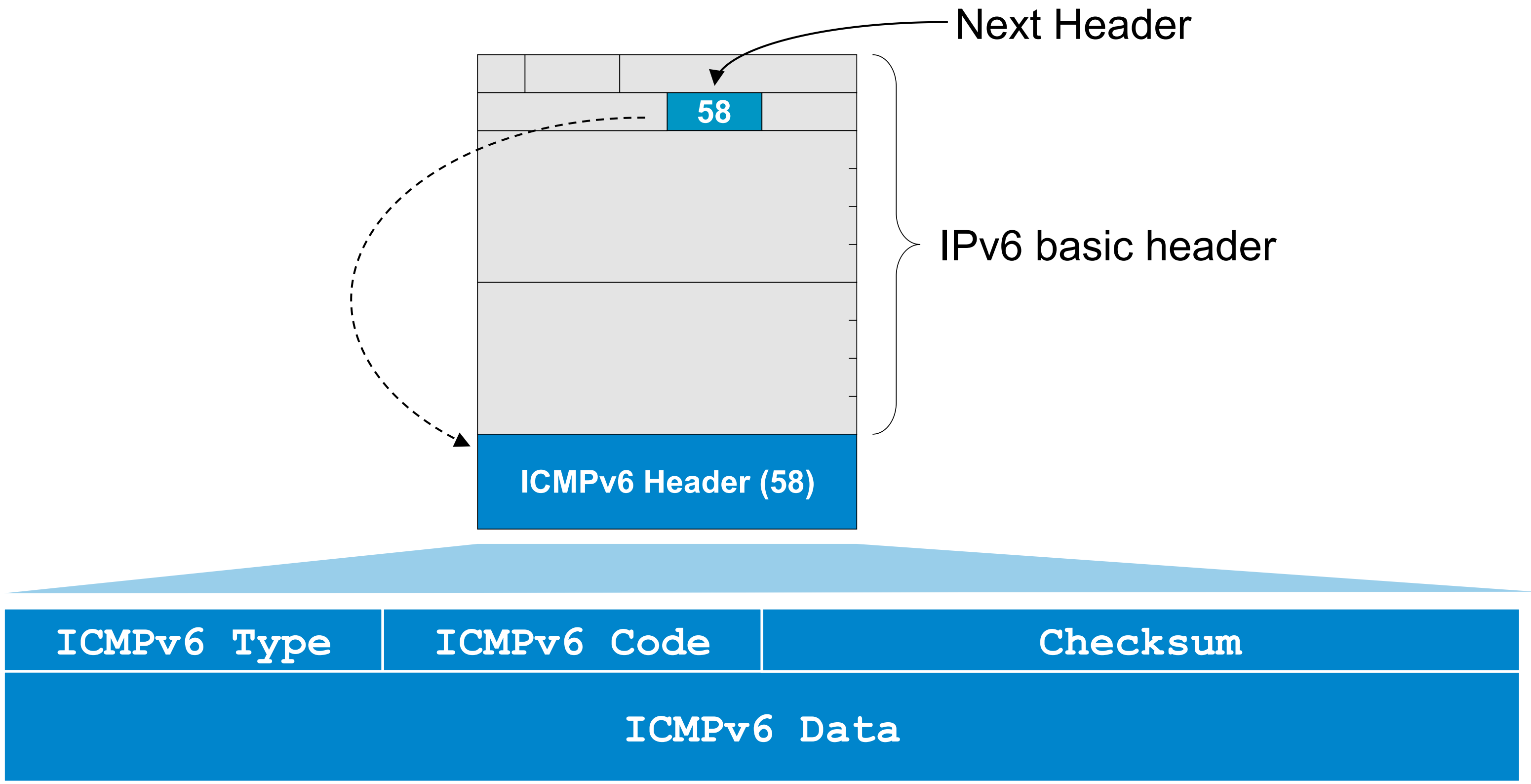


ICMPv6 (RFC 2463)

- Internet Control Message Protocol version 6
- Combines several IPv4 functions
  - ICMPv4, IGMP and ARP
- Message types are similar to ICMPv4
  - Destination unreachable (type 1)
  - Packet too big (type 2)
  - Time exceeded (type 3)
  - Parameter problem (type 4)
  - Echo request/reply (type 128 and 129)

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

ICMPv6 Header



- Also used for Neighbor Discovery, Path MTU discovery and Mcast listener discovery (MLD)

  Type - identifies the message or action needed

  Code – is a type-specific sub-identifier.

  Checksum – computed over the entire ICMPv6

Neighbor Discovery Messages (ND)

- ND uses ICMPv6 messages
  - Originated from node on link local with a hop limit of 255
  - Receivers checks hop limit is still 255 (has not passed a router)
- Consists of IPv6 header, ICMPv6 header, neighbor discovery header, and neighbor discovery options
- Five neighbor discovery messages

Message	Purpose	ICMP Code	Sender	Target
Router Solicitation (RS)	Prompt routers to send RA	133	Nodes	All routers
Router Advertisement (RA)	Advertise default router, prefixes Operational parameters	134	Routers	Sender of RS All routers
Neighbor Solicitation (NS)	Request link-layer of target	135	Node	Solicited Node Target Node
Neighbor Advertisement (NA)	Response to NS (solicited) Advertise link-layer address change (Unsolicited)	136	Nodes	
Redirect	Inform hosts of a better first hop	137	Routers	

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

ICMPv6 Neighbor Discovery (RFC 4861)

- Replaces ARP, ICMP (redirects, router discovery)
- Uses ICMPv6 header
- Reachability of neighbours
- Hosts use it to discover routers, auto configuration of addresses (SLAAC)
- Duplicate Address Detection (DAD)

IPv4/IPv6 Provisioning Comparison

Function	IPv4	IPv6
Address Assignment	DHCPv4	DHCPv6, SLAAC, Reconfiguration
Address Resolution	ARP RARP	ICMPv6 NS, NA Not Used
Router Discovery	ICMP Router Discovery	ICMPv6 RS, RA
Name Resolution	DNS	DNS

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Router Solicitation and Advertisement (RS & RA)

Router Solicitation	
ICMP Type	133
IPv6 Source	A Link Local (FE80::1)
IPv6 Destination	All Routers Multicast (FF02::2)
Query	Please send RA

Router Advertisement	
ICMP Type	134
IPv6 Source	A Link Local (FE80::2)
IPv6 Destination	All Nodes Multicast (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

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Neighbor Solicitation & Advertisement

- Neighbor Solicitation (NS)

  Used to discover link layer address of IPv6 node

NS Function	Source	Destination
Address resolution	Unicast	Solicited Node Multicast
Node reachability	Unicast	Unicast
Duplicate Address Detection	::0	Solicited Node Multicast

- Neighbor Advertisement (NA)

  Response to neighbor solicitation (NS) message

  A node may also send unsolicited Neighbor Advertisements to announce a link-layer address change.

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Neighbor Solicitation & Advertisement (NS & NA)

Neighbour Solicitation	
ICMP Type	135
IPv6 Source	A Unicast
IPv6 Destination	B Solicited Node Multicast
Data	FE80:: address of A
Query	What is B link layer address?

Neighbour Advertisment	
ICMP Type	136
IPv6 Source	B Unicast
IPv6 Destination	A Unicast
Data	FE80:: address of B, MAC Address

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Viewing Neighbors in the Cache

- Neighbors are only considered "reachable" for 30-seconds
- "Stale" indicates that ND packet must be sent again

```
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
```

Entry STALE due to no contact for > 30 secs (Age 50 secs)

```
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
```

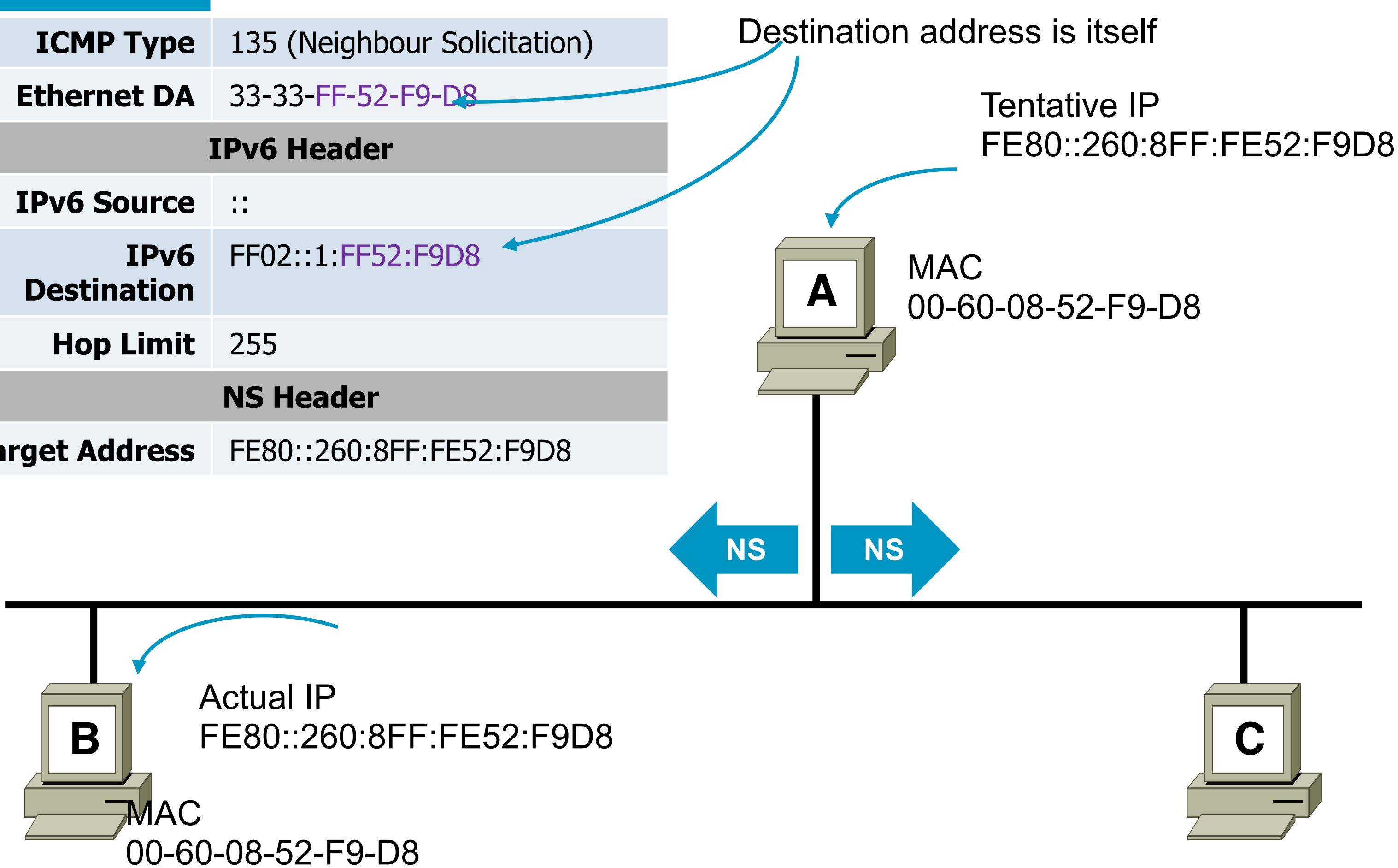
After PING entry now reachable again (Age 0 secs)

Neighbor Unreachability Detection

- Neighbor is declared reachable if
  - The connection is making forward progress
  - Previously sent data is known to have been delivered correctly
  - Source receives an NA in response to NS
- If neighbour status unknown then send NS
- Defined in RFC 4861 Section 7.3

Duplicate Address Detection (DAD)

Neighbour Solicitation	
ICMP Type	135 (Neighbour Solicitation)
Ethernet DA	33-33-FF-52-F9-D8
IPv6 Header	
IPv6 Source	::
IPv6 Destination	FF02::1:FF52:F9D8
Hop Limit	255
NS Header	
Target Address	FE80::260:8FF:FE52:F9D8

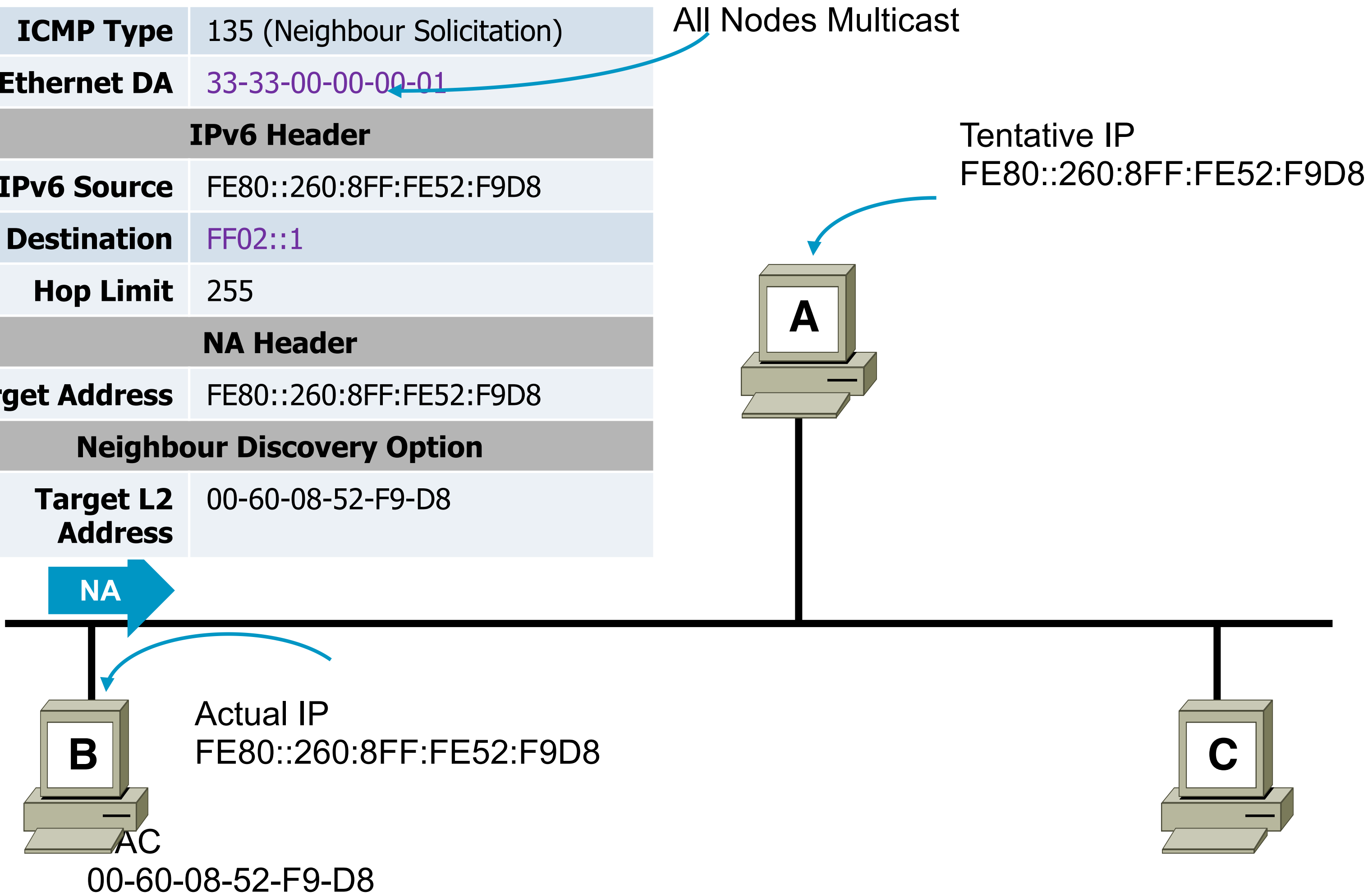


2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Duplicate Address Detection Response

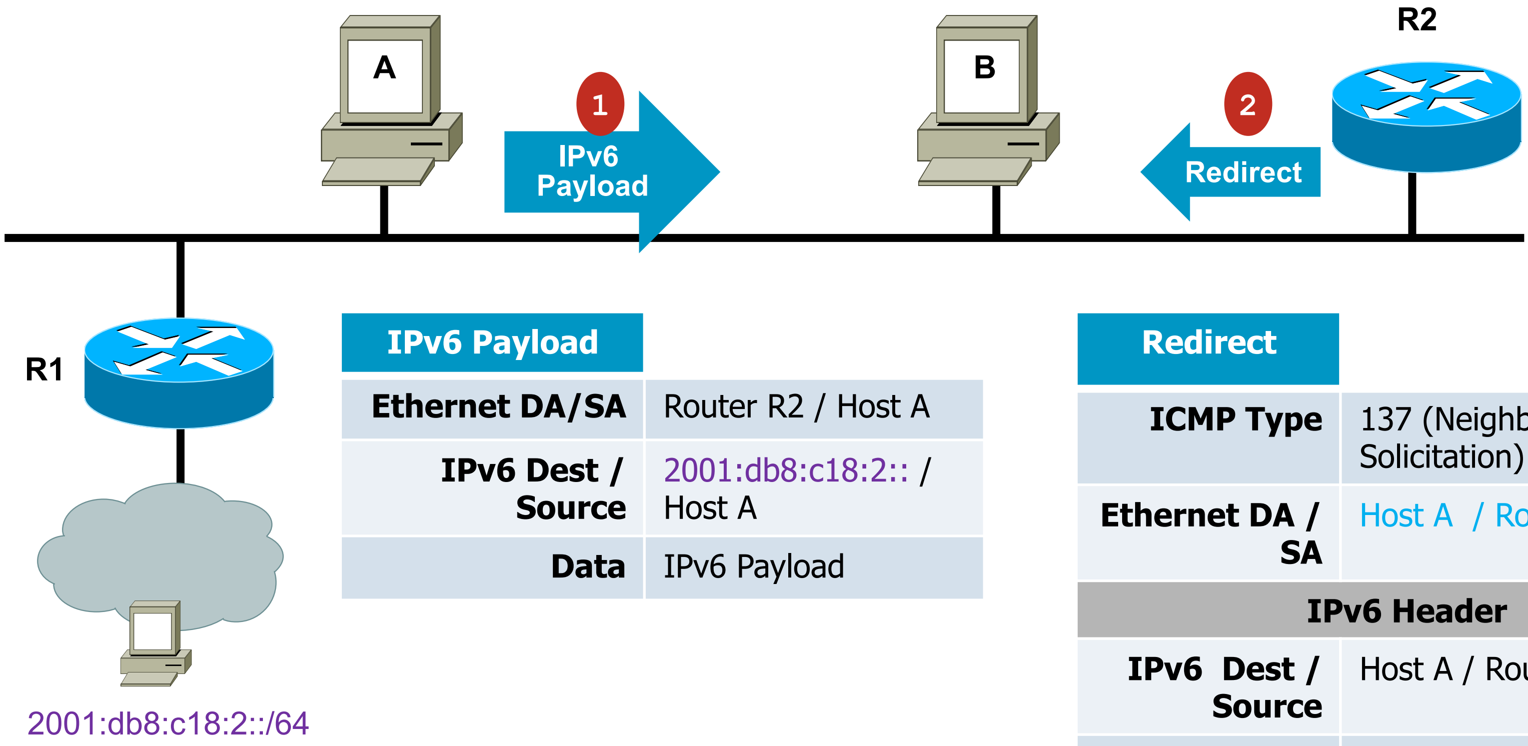
Neighbour Solicitation	
ICMP Type	135 (Neighbour Solicitation)
Ethernet DA	33-33-00-00-00-01
IPv6 Header	
IPv6 Source	FE80::260:8FF:FE52:F9D8
IPv6 Destination	FF02::1
Hop Limit	255
NA Header	
Target Address	FE80::260:8FF:FE52:F9D8
Neighbour Discovery Option	
Target L2 Address	00-60-08-52-F9-D8



2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

ICMPv6 Redirection

- Redirect is used by a router to informs hosts of a better first hop

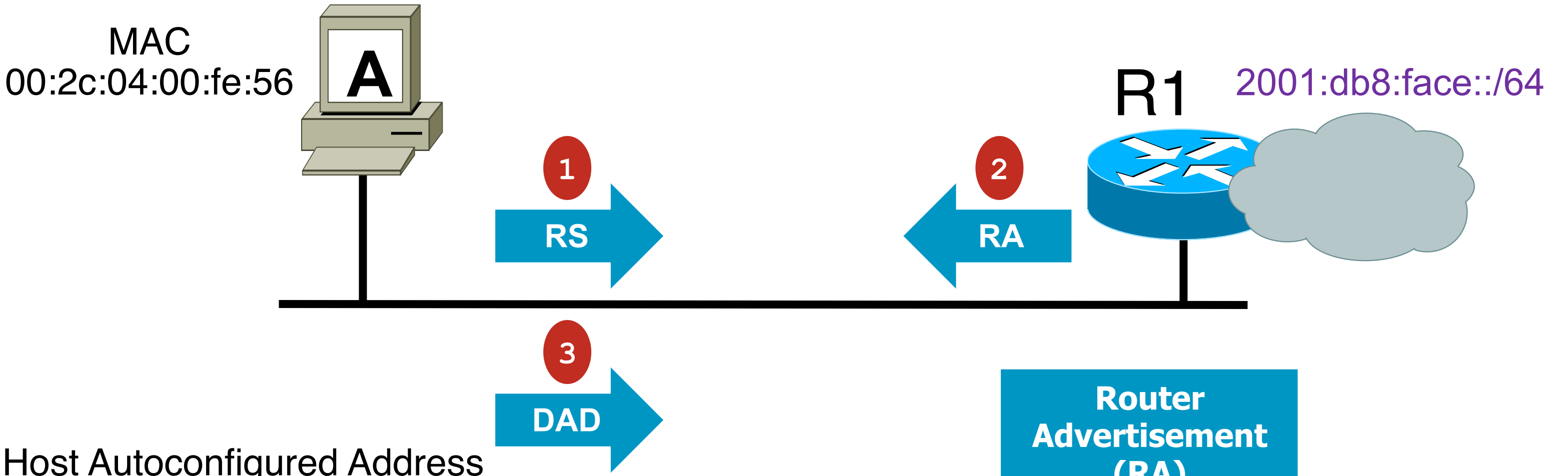


IPv6 Payload	
Ethernet DA/SA	Router R2 / Host A
IPv6 Dest / Source	2001:db8:c18:2:: / Host A
Data	IPv6 Payload

Redirect	
ICMP Type	137 (Neighbour Solicitation)
Ethernet DA / SA	Host A / Router R2
IPv6 Header	
IPv6 Dest / Source	Host A / Router R2
Hop Limit	255
Redirect Data	
Target Address	Router R1
Redirected Prefix	2001:db8:c18:2::/64

Stateless Address Autoconfiguration (RFC4862)

- Autoconfiguration is used to automatically assigned an address to a host “plug and play”
  - Generating a link-local address,
  - Generating global addresses via stateless address autoconfiguration
  - Duplicate Address Detection procedure to verify the uniqueness of the addresses on a link



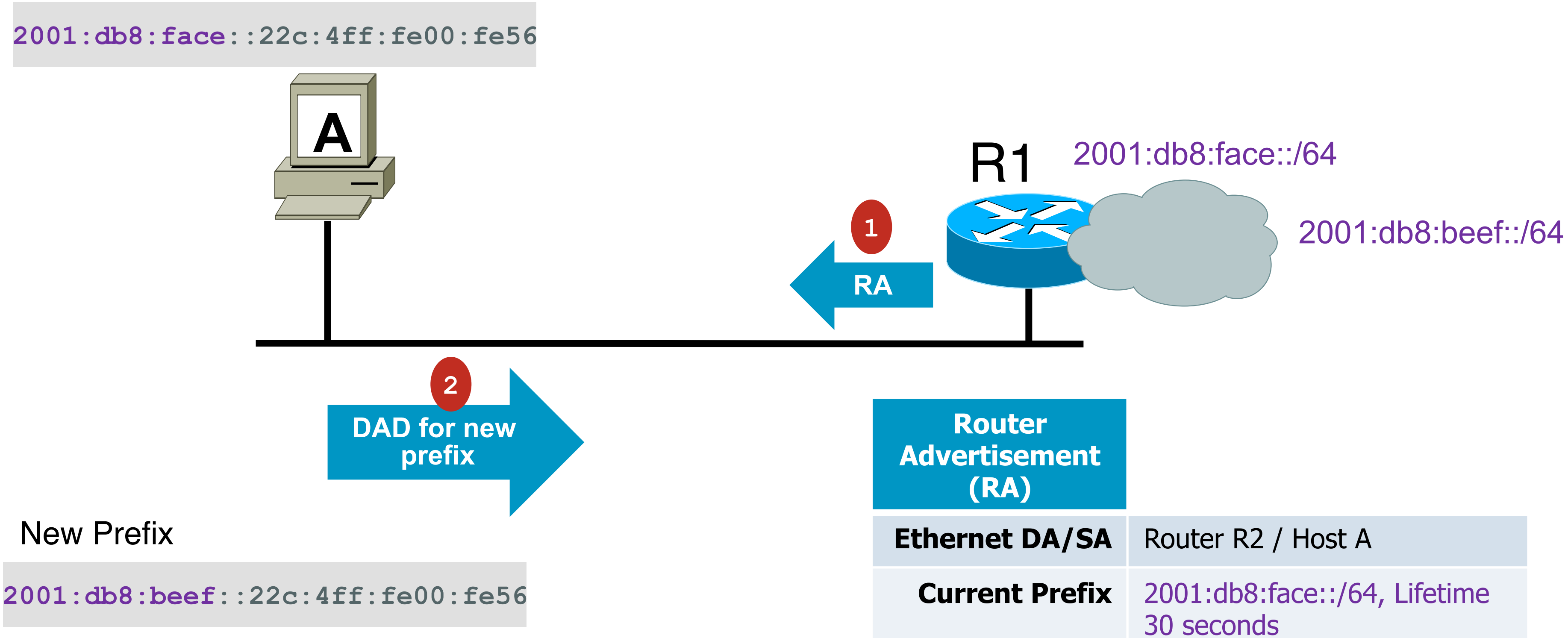
Host Autoconfigured Address comprises
Prefix Received + Link-Layer Address if DAD check passes

`2001:db8:face::22c:4ff:fe00:fe56`

Router Advertisement (RA)	
Ethernet DA/SA	Router R2 / Host A
Prefix Information	2001:db8:face::/64
Default Router	Router R1

Prefix Renumbering

- Prefixes can be given a lifetime in RA messages
- Allows seamless transition for renumbering to a new prefix



Router Advertisement (RA)	
Ethernet DA/SA	Router R2 / Host A
Current Prefix	2001:db8:face::/64, Lifetime 30 seconds
New Prefix	2001:db8:beef::/64, Lifetime 30 seconds

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Renumbering (contd.)

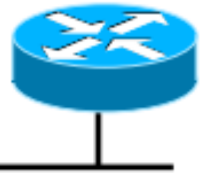
Router Configuration after Renumbering:

```
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 2010 23:59 Jul 1 2010 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
```

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Review Questions

Question 1

- What type of is

`2001:0ba0:0000:0000:0000:0000:0000:1234`

A. Link Local ✘ Incorrect link-local begin with FE80::/10

B. Multicast ✘ Multicast addresses begin with FF00::/8

C. Global Unicast ✓

D. Unique Local ✘ Unique-local begin with FC00::/7

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Question 2

- Which of the following is a valid abbreviation for

  2001:0ba0:0000:0000:0000:0000:0000:1234

A. **2001:0ba0::1234** ✓

B. **2001:ba0:0:0:0:0:0:1234** ✓

C. **2001:0ba::1234** ✗ Incorrect because 0ba0 not equal to 0ba (only leading zeros can be omitted)

D. **2001:0ba0::0:0:0::1234** ✗ Incorrect :: cannot be used more than once

Question 3

- Which of the following is a valid EUI-64 address for an interface with the MAC address

  `58:b0:35:fe:7e:4a`

A. `2001::5ab0:35ff:fefe:7e4a` ✓

B. `2001::58b0:35ff:fffe:7e4a` ✗ Incorrect FFFE should be inserted in the middle not FFFF

C. `2001::58b0:35ff:feff:7e4a` ✗ Incorrect FE in the MAC address should not be changed to FF

D. `2001::58b0:35ff:fefe:7e4a` ✗ Incorrect because bit 7 was not flipped in EUI-6 interface ID

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Question 4

- Which well known multicast addresses are mandatory to have on an interface?

A. Node-Local “All Nodes”, Link-Local “All Nodes” and Link-Local “Solicited-Node”

B. Link-Local “All Nodes” and Link-Local “Solicited Node”

C. Link-Local “All Nodes” only

D. Node-Local “All Nodes” only

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Question 5

- Which type of request does a node use to learn if another node has the same address?

A. Unicast DAD

B. Neighbour Solicitation (NS)
With src = Unicast, dst = solicited node multicast

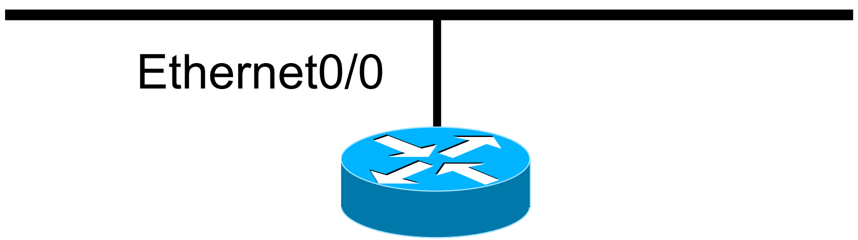
C. Router Solicitation (RS)

D. Neighbour Solicitation (NS)
With src = ::, dst = solicited node multicast

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Configuring IPv6

IPv6 Address Configuration: Link Local




```
r1#show interface ethernet 0/0
Ethernet0/0 is up, line protocol is up
  Hardware is AmdP2, address is 0004.9aac.7d80
(bia 0004.9aac.7d80)
```

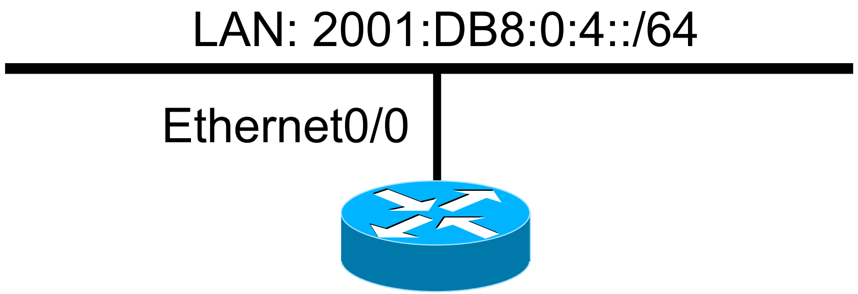
```
ipv6 unicast-routing

interface Ethernet0/0
 ipv6 enable
```

MAC address: 0004:9AAC:7D80

```
router#show ipv6 interface Ethernet 0/0
Ethernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::204:9AFF:FEAC:7D80
  No global unicast address is configured
  Joined group address(es):
    FF02::1 (All Nodes Link Local)
    FF02::2 (All Routers Link Local)
    FF02::1:FFAC:7D80 (Solicited-Node Multicast)
  MTU is 1500 bytes
```

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

IPv6 Address Configuration: Ethernet EUI-64




```
ipv6 unicast-routing

interface Ethernet0/0
 ipv6 address 2001:DB8:0:4::/64 eui-64
```

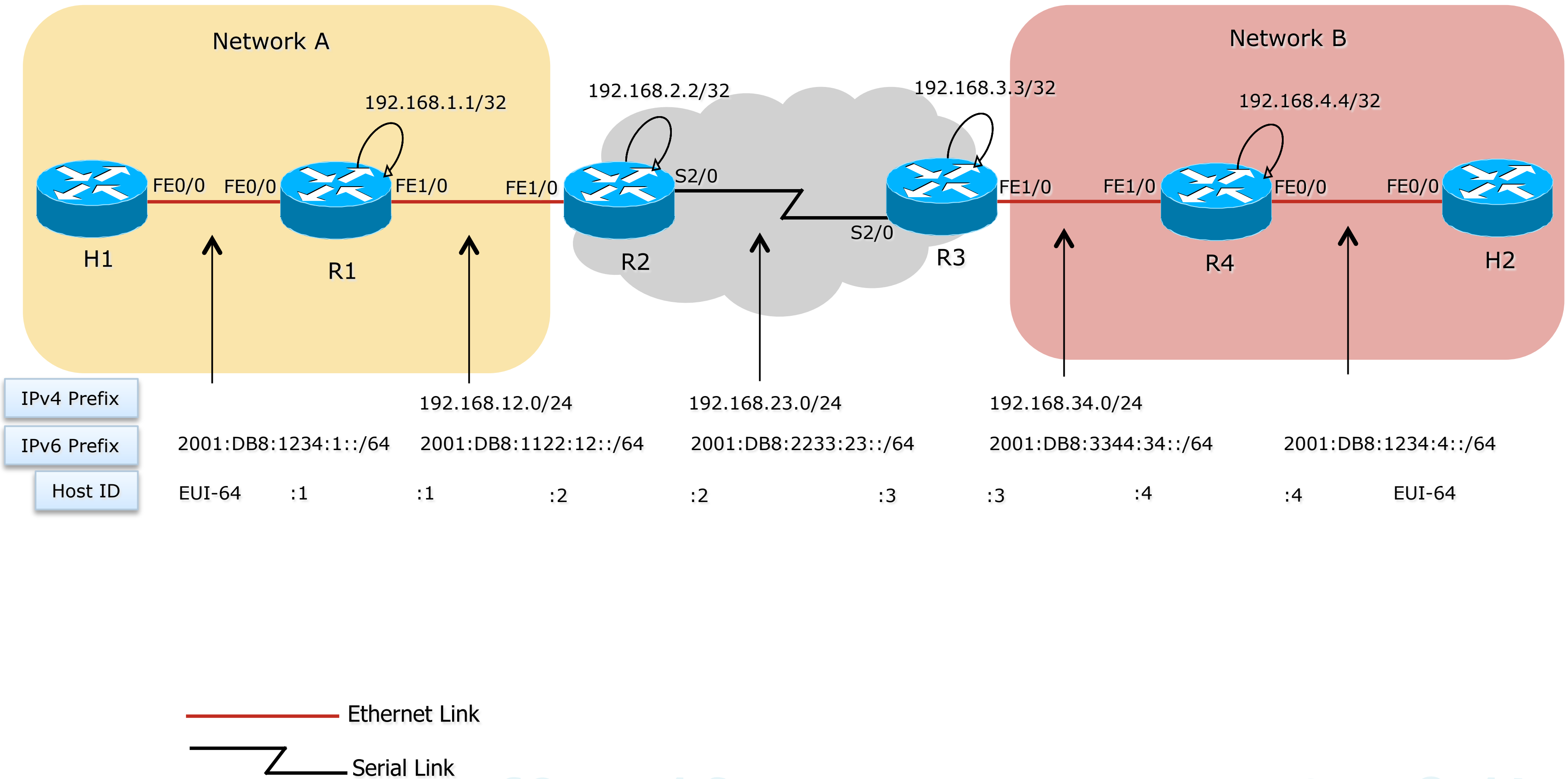
MAC address: 0004:9AAC:7D80

```
router# show ipv6 interface Ethernet0/0
Ethernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::204:9AFF:FEAC:7D80
  Global unicast address(es):
    2001:DB8:0:4:204:9AFF:FEAC:7D80, subnet is 2001:DB8:0:4::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FFAC:7D80
  MTU is 1500 bytes
```

LAB 1: IPv6 Addressing

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

IPv6 LAB Topology



2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

LAB 2: IPv6 Neighbor Discovery

Default & Static Route

- Similar to IPv4. Need to define the next hop / interface.
- Default route denoted as ::/0
- Examples:

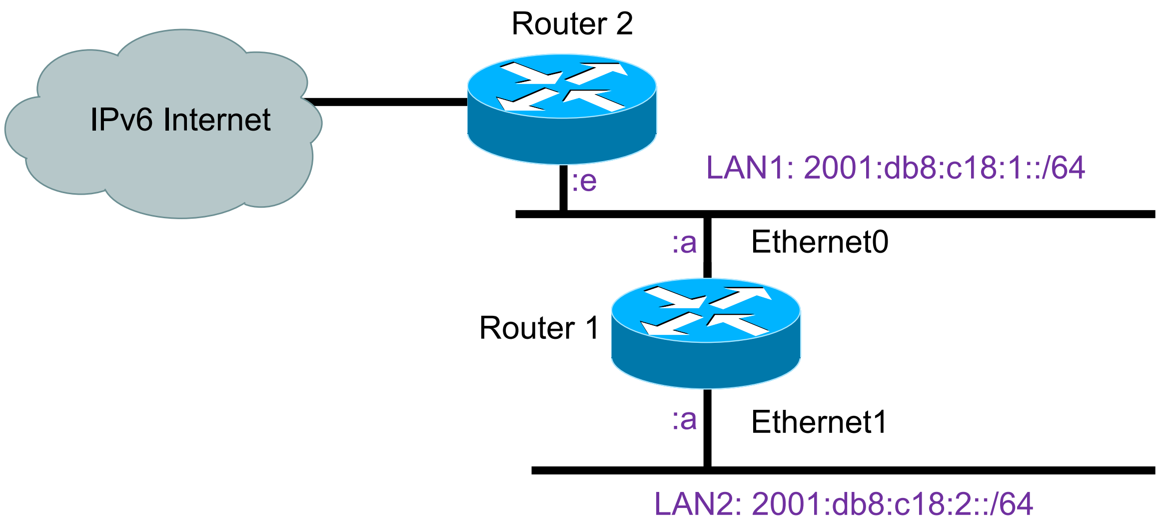
Forward packets for network 2001:DB8::0/32 through 2001:DB8:1:1::1 with an administrative distance of 10

```
Router(config)# ipv6 route 2001:DB8::0/32 2001:DB8:1:1::1 10
```

Default route to 2001:DB8:1:1::1

```
Router(config)# ipv6 route ::/0 2001:DB8:1:1::1
```

Default Routing Example




```
router 1#config term
ipv6 unicast-routing
!
interface Ethernet0
 ipv6 address 2001:db8:c18:1::a/64
!
interface Ethernet1
 ipv6 address 2001:db8:c18:2::a/64
!
ipv6 route ::/0 2001:db8:c18:1::e
```

Default router to Router 2

Lab 3 : IPv6 Static Routing

IPv6 Services

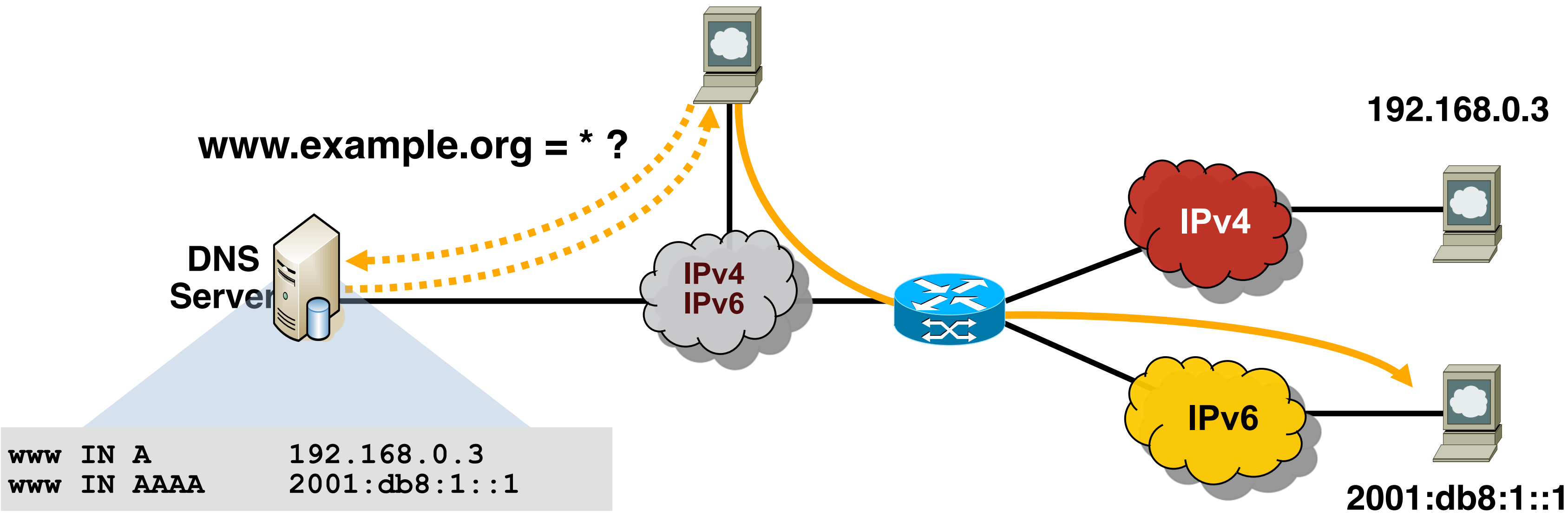
DNS Basics

- DNS is a database managing Resource Records (RR)
  - Storage of RR for various types—IPv4 and IPv6:
    - Start of Authority (SoA)
    - Name Server
    - Address—A and AAAA
    - Pointer—PTR
- DNS is an IP application
  - Uses either UDP or TCP on top of IPv4 or IPv6
- References
  - RFC3596: DNS Extensions to Support IP Version 6
  - RFC3363: Representing Internet Protocol Version 6 Addresses in Domain Name system (DNS)
  - RFC3364: Tradeoffs in Domain Name System (DNS) Support for Internet Protocol version 6 (IPv6)

IPv6 and DNS Entries

Function	IPv4	IPv6
Hostname to IP Address	A Record www.abc.test. IN A 92.168.30.1	AAAA Record (Quad A) www.abc.test. IN AAAA 2001:db8:C18:1::2
IP Address To Hostname	PTR Record 1.30.168.192.in-addr.arpa. IN PTR www.abc.test.	PTR Record 2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.8.1.c.0.8.b.d.0.1.0.0.2.ip6.arpa IN PTR www.abc.test.

Dual Stack Approach & DNS



- In a dual stack case an application that:
  - Is IPv4 and IPv6-enabled
  - Can query the DNS for IPv4 and/or IPv6 records (A) or (AAAA) records
  - Chooses one address and, for example, connects to the IPv6 address

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

IPv6 Host Address Assignment Methods

- Manual Assignment
  - Statically configured by human operator
- Stateless Address Autoconfiguration (SLAAC RFC 4862)
  - Allows auto assignment of address through Router Advertisements
- Stateful DHCPv6 (RFC 3315)
  - Allows DHCPv6 to allocate IPv6 address plus other configuration parameters (DNS, NTP etc…)
- Stateless DHCPv6 (RFC 3736)
  - Combination of SLAAC for host address allocation
  - DHCPv6 for additional parameters such as DNS Servers and NTP

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

DHCPv6

- Updated version of DHCP for IPv4 to supports new addressing
- Can be used for renumbering
- DHCP Process is same as in IPv4, but,
  - Client first detects the presence of routers on the link
  - If found, then examines router advertisements (RA) to determine if DHCPv6 can be used
  - If no router found or if DHCPv6 can be used, then
    - DHCPv6 Solicit message is sent to the All-DHCP-Agents multicast address using link-local as source
- Multicast addresses used
  - FF02::1:2 = All DHCP Agents (servers or relays, Link-local scope)
  - FF05::1:3 = All DHCP Servers (Site-local scope)
  - DHCP Messages: Clients listen UDP port 546; servers and relay agents listen on UDP port 547

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

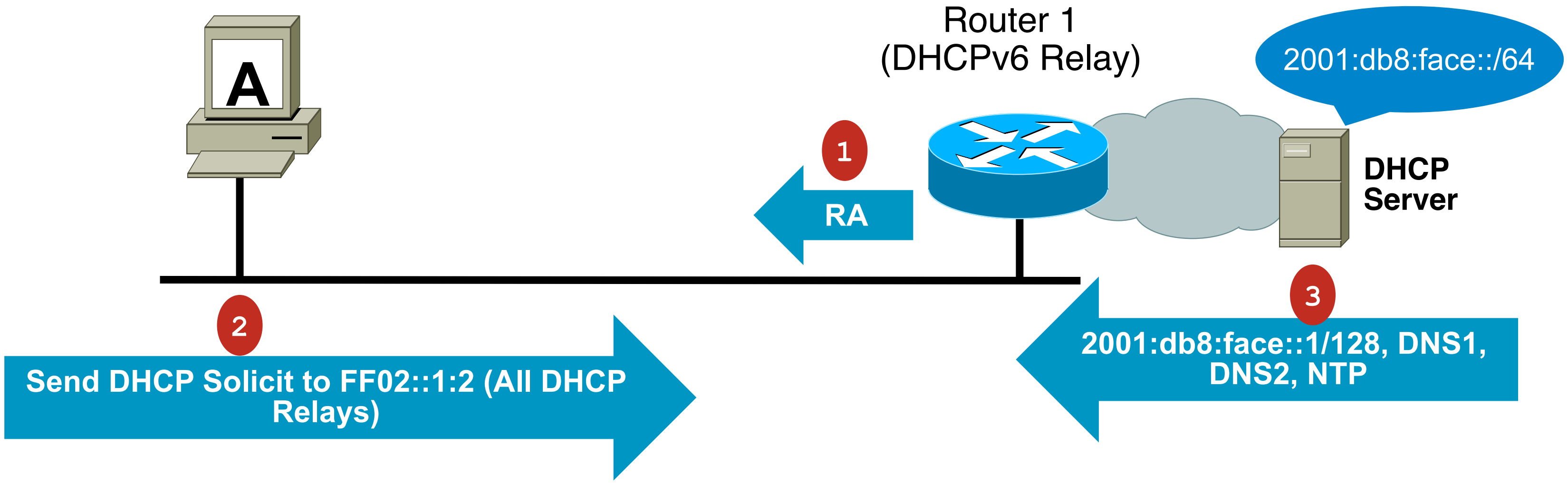
DHCPv4/DHCPv6 Protocol Comparison

DHCP Messages	IPv4	IPv6
Initial Message Exchange	4-way handshake	4-way handshake
Message Types	Broadcast, Unicast	Multicast, Unicast
Client → Server (1)	DISCOVER	SOLICIT
Server → Client (2)	OFFER	ADVERTISE
Client → Server (3)	REQUEST	REQUEST
Server → Client (4)	ACK	REPLY

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Router Advertisement for Stateful DHCPv6

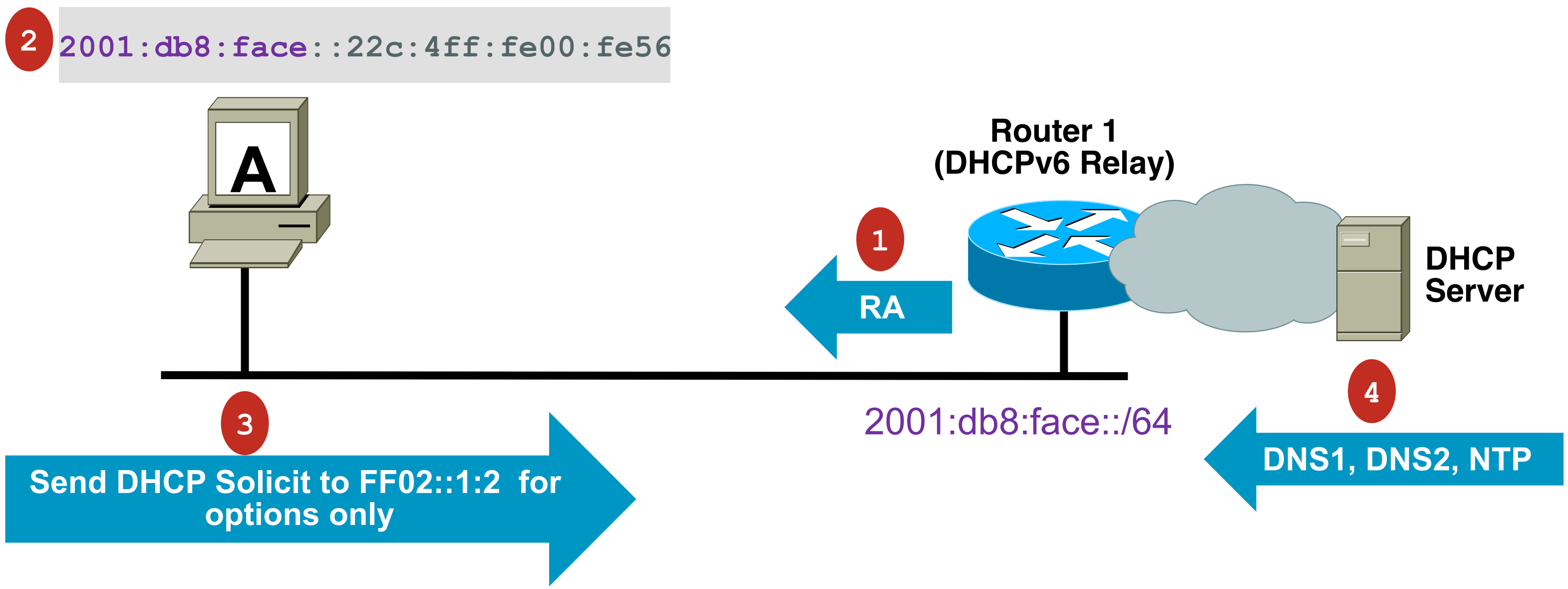
- RA message contain flags that indicate address allocation combination (A, M and O bits)
  - Use SLAAC only, Use DHCPv6 stateful, Use SLAAC and DHCPv6 for other options



Router Advertisement (RA)	
A bit (Address config flag)	Set to **0** - Do not use SLAAC for host config
M bit (Managed address configuration flag)	Set to **1** - Use DHCPv6 for host IPv6 address
O bit (Other configuration flag)	Set to **1** - Use DHCPv6 for additional info (DNS, NTP)

Router Advertisement for Stateless DHCPv6

- RA message contain flags that indicate address allocation combination (A, M and O bits)
  - Use SLAAC only, Use DHCPv6 stateful, Use SLAAC and DHCPv6 for other options



Router Advertisement (RA)	
A bit (Address config flag)	Set to **1** - Use SLAAC for host address config
On-link Prefix	2001:db8:face::/64
M bit (Managed address configuration flag)	Set to **0** - Do not use DHCPv6 for IPv6 address
O bit (Other configuration flag)	Set to **1** - Use DHCPv6 for additional info (DNS, NTP)

DHCPv6 Configuration options
Setting the bits

- Config options on Router interface

A bit (default) just use SLAAC

```
int e0/0
 ipv6 address 2001:db8:1000::1/64
```

Host gets address and other SLAAC options. Nothing else

M bit & O bit (Stateful DHCP)

```
int e0/0
 ipv6 address 2001:db8:1000::1/64
 ipv6 nd managed-config-flag
 ipv6 nd other-config-flag
 ipv6 dhcp relay destination
2001:db8::10
```

Host gets full stateful config from DHCP server (2001:db8::10)

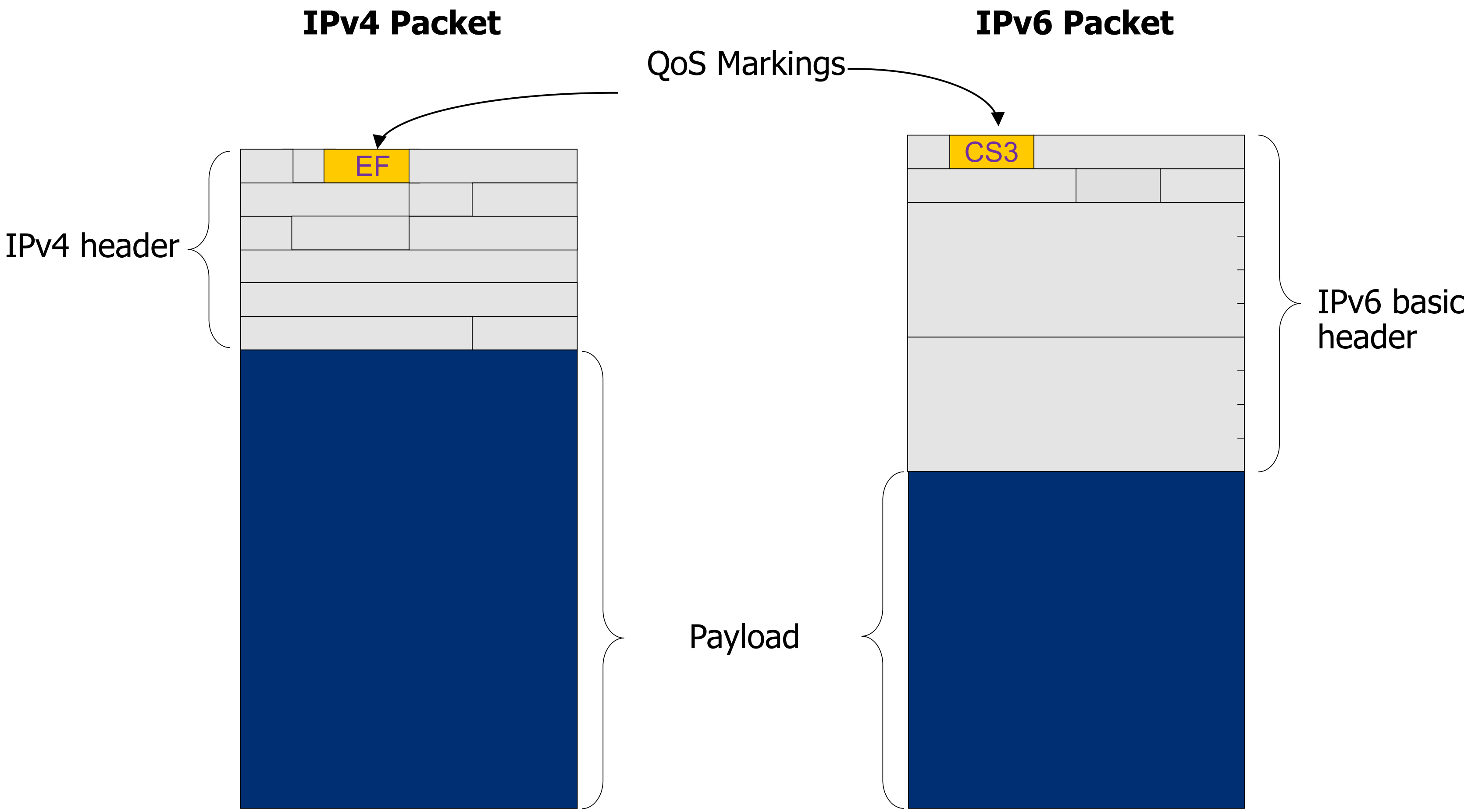
A bit & O bit (Stateless DHCP)

```
int e0/0
 ipv6 address 2001:db8:1000::1/64
 ipv6 nd other-config-flag
 ipv6 dhcp relay destination
2001:db8::10
```

Host get address from SLAAC and other config from DHCP server (2001:db8::10)

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

QoS
It is the same



- IOS MQC can match DSCP or Precedence (ToS)

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

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 → "**BOB ::11:0:0:0:1**" = **2001:db8:cafe:11::1/64**

```
ipv6 general-prefix BOB 2001:db8:cafe::/48
!
interface GigabitEthernet3/2
 ipv6 address BOB ::1/127
!
interface Vlan11
 ipv6 address BOB ::11:0:0:0:1/64
!
```

```
#show ipv6 route
<snip>
Global unicast address(es):
    2001:DB8:CAFE:11::1, subnet is 2001:DB8:CAFE:
11::/64
```

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Telnet & SSH

- Telnet supported by default once an IPv6 address (GUA / UL / LL) is defined
- Treat VTY security the same as you would for IPv4

```
line vty 0 4
 password <password>
 login
```

- TACACS+ and RADIUS user authentication mechanisms are not currently supported over IPv6 Transport
  - IPv4 transport needs to be supported if SSH with TACACS or RADIUS is to be enabled

```
hostname router1
domain-name example.com
crypto key generate rsa
ip ssh time-out 60
ip ssh authentication-retries 2
line vty 0 4
 transport input ssh
```

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

TFTP & FTP

- IPv6 supports TFTP & FTP file downloading and uploading using the copy command. The copy command accepts a destination IPv6 address or IPv6 hostname as an argument.

```
copy running-config tftp://[2001:db8:1000::1]/running-config
```

```
copy ftp: disk0:
 Address or name of remote host [2001:db8:1000::2]?
 Source filename []? IOS_image_12.2SE6
 Destination filename []? IOS_image_12.2SE6
 Accessing ftp://2001:db8:1000::2/IOS_image_12.2SE6
 !!!!!!
```

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

DNS

- Supports IPv6 transport and VRF support

```
ip name-server 2001:db8:2000::53
ip name-server 192.0.2.53
ip name-server vrf Mgmt-intf 2001:db8:2000::53
```

- Up to 6 name-servers can be defined
  - Can be all IPv4, all IPv6, or combination

```
R1(config)#ip name-server 2001:db8:1000::57
% Name-server table is full; 2001:DB8:1000::57 not
added
```

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

SNMP

- SNMP supports IPv6 Transport

```
snmp-server community public
snmp-server enable traps bgp
snmp-server host 172.16.1.27 version 2c public
snmp-server host 172.16.1.111 version 1 public
snmp-server host 2001:db8:1000::3 public
```

- SNMP support for IPv6 MIBs is however slowly being implemented

MIB	Comment
CISCO-CONFIG-COPY-MIB	Supports IPv6 addressing when either TFTP, remote copy protocol (rcp), or FTP is used.
CISCO-CONFIG-MAN-MIB	
CISCO-DATA-COLLECTION-MIB	
CISCO-FLASH-MIB	Supports IPv6 addressing when either TFTP, remote copy protocol (rcp), or FTP is used.
IP-FORWARD-MIB	IP-FORWARD-MIB updated to support RFC 4292.
IP-MIB	IP-MIB updated to support RFC 4293.
ENTITY-MIB	
NOTIFICATION-LOG-MIB	
SNMP-TARGET-MIB	
CISCO-SNMP-TARGET-EXT-MIB	This MIB was added for the IPv6 over SNMP support feature

VRF Support

- VRFs (MPLS / VRF-Lite) are IPv6 transport capable
- Management VRFs also support IPv6 Transport
- VRF syntax needs to be upgraded

```
ip vrf GREEN
 rd 200:1
  route-target export 200:1
  route-target import 200:1
!
interface Ethernet0/1
 ip vrf forwarding GREEN
```

```
vrf upgrade-cli multi-af-mode
{common-policies | non-common-
policies} [vrf <name>]
```

```
vrf definition GREEN
 rd 200:1
 address-family ipv4
  route-target export 200:1
  route-target import 200:1
 exit-address-family
 !
 address-family ipv6
  route-target export 200:1
  route-target import 200:1
 exit-address-family
!
interface Ethernet0/1
 vrf forwarding GREEN
```

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Syslog Support & HTTP

- Syslog is supported over IPv6 Transport

```
logging buffered informational
logging host ipv6 2001:DB8:1000::14
logging host 172.16.1.1
```

- The Cisco IOS HTTP server supports IPv6 transport

```
ip http server
```

- The syntax supports both IPv4 and IPv6 HTTP server
- Access Classes can only be applied in IPv4
- IPv6 Security needs other means (Traffic ACL)
- Not Best Practice to use HTTP server

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Not yet Supported

- LDPv6
- RADIUS or TACACS+
- Some feature limitations
  - e.g. no Access Class for HTTP server
    - Limited IPv6 QoS support based on IOS / Platform (no priority queue support, no NBAR)
    - No OSPFv3 support for VRFs
- Release Notes for Hardware and Software is the source of truth for support
  - http://www.cisco.com/go/support

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Review Questions

- Q1: Will there be IPv6 client to Server traffic just by enabling IPv6 on the network?

  No, The application needs to be IPv6 capable, and there needs to be a quad-A record in the DNS

- Q2: What is Stateful DHCP?

  Host receives RA to tell host to use DHCP for full configuration (M & O bit set)

- Q3: What is Stateless DHCP?

  Host receives RA from which it does SLAAC, then gets other settings from DHCP (DNS, NTP, etc). (A & O bit set)

- Q4: Are there differences in QoS config and behaviour for IPv6 ?

  QoS config has changed to support, IPv4, IPv6, or IPv4 & IPv6

  QoS behaviour has not changed

- Q5: What IOS management functions exist in IPv6

  Telnet, SSH, SNMP, FTP, TFTP, HTTP, DNS, VRF Support, Syslog

- Q6: What functions are not yet supported in IPv6

  LDP, TACACS transport, RADIUS Transport, and some features

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Routing in IPv6

Routing in IPv6

- As in IPv4, IPv6 has 2 families of routing protocols: IGP and EGP, and still uses the longest-prefix match routing algorithm
- IGP
  - RIPng (RFC 2080)
  - Cisco EIGRP for IPv6
  - Integrated IS-ISv6 (draft-ietf-isis-ipv6-02)
  - OSPFv3 (RFC 2740)
- EGP : MP-BGP4 (RFC 2858 and RFC 2545)
- Cisco IOS supports all of them
  - Pick one that meets your objectives

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

RIPng

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

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

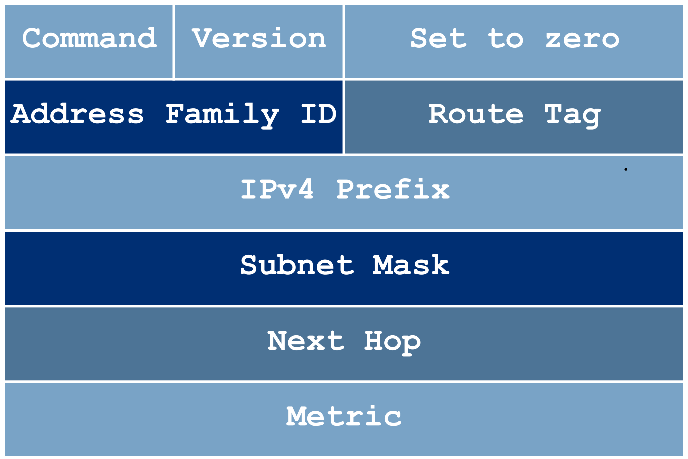
RIPng Overview

Legend

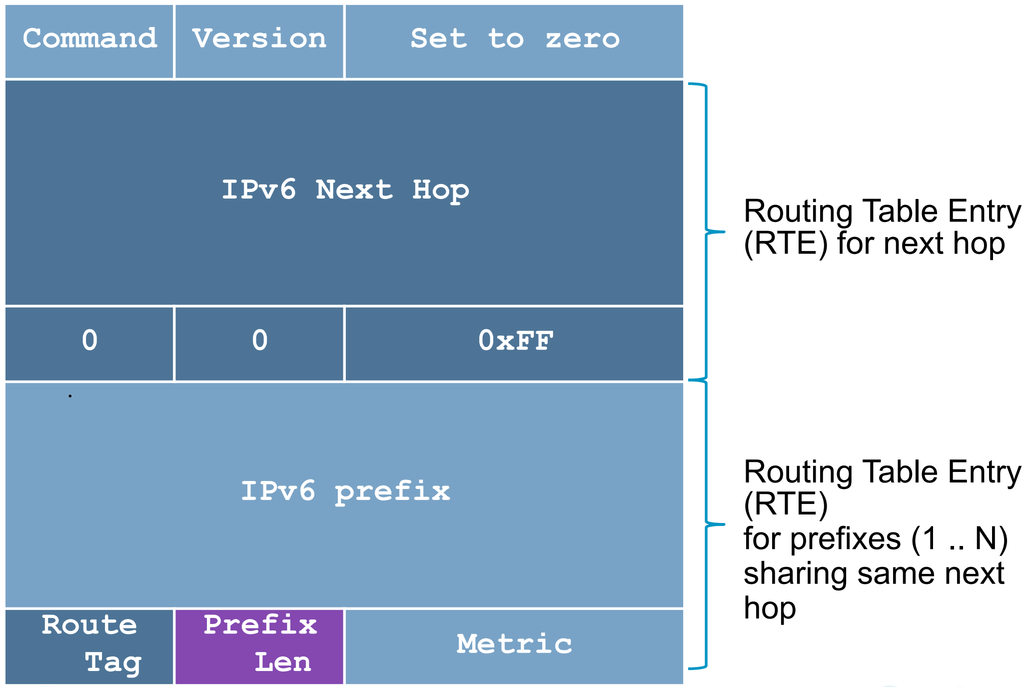
- Field's Name kept from IPv4 to IPv6
- Fields not kept in IPv6
- Name and/or position changed in IPv6
- New Field in IPv6

- Similar to RIPv2
  - Distance-vector, Hop limit of 15, split-horizon, All RIP routers is FF02::9, UDP port (521)
- Updated features for IPv6
  - Prefix length added, address-family and subnet mask fields removed
- Special Handling for the NH
  - One NH entry per group of prefixes

RIP header

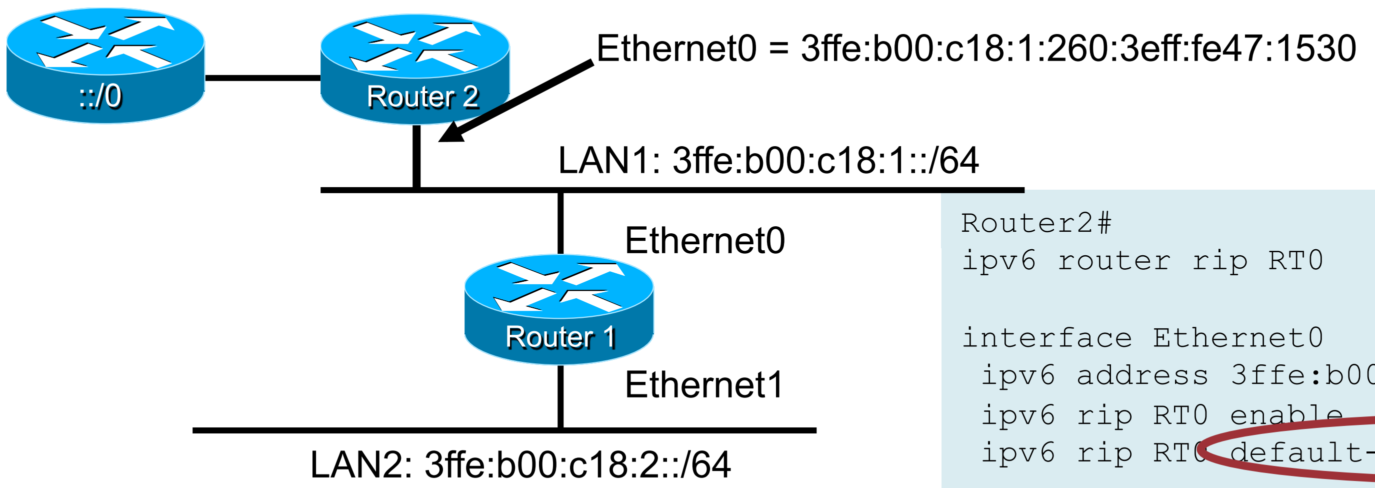


RIPng header



2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

RIPng Configuration and Display




```
Router2#
ipv6 router rip RT0

interface Ethernet0
 ipv6 address 3ffe:b00:c18:1::/64 eui-64
 ipv6 rip RT0 enable
 ipv6 rip RT0 default-information originate
```

```
Router1#
ipv6 router rip RT0

interface Ethernet0
 ipv6 address 3ffe:b00:c18:1::/64 eui-64
 ipv6 rip RT0 enable
 Interface Ethernet1
 ipv6 address 3ffe:b00: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

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

RIPng Routing Entries

```
R1# show ipv6 route
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS -
ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 -
OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
C   2001:DB8:1::/64 [0/0]
     via ::, Loopback1
L   2001:DB8:1:0:A8BB:CCFF:FE00:100/128 [0/0]
     via ::, Loopback1
R   2001:DB8:2::/64 [120/2]
     via FE80::A8BB:CCFF:FE00:200, Serial2/0
R   2001:DB8:3::/64 [120/3]
     via FE80::A8BB:CCFF:FE00:200, Serial2/0
C   2001:DB8:12::/64 [0/0]
     via ::, Serial2/0
L   2001:DB8:12:0:A8BB:CCFF:FE00:100/128 [0/0]
     via ::, Serial2/0
R   2001:DB8:23::/64 [120/2]
     via FE80::A8BB:CCFF:FE00:200, Serial2/0
L   FF00::/8 [0/0]
     via ::, Null0
```

Note all RIP next hops are link-local addresses (FE80::)

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

OSPFv3
(RFC 2740)

OSPFv3 Overview

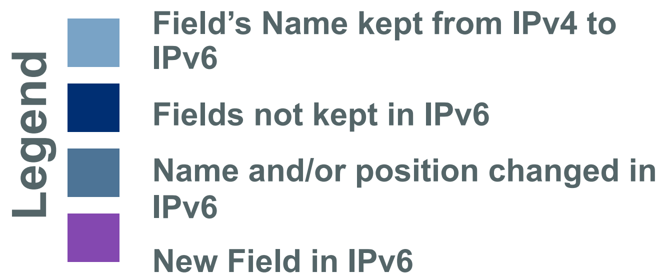
- OSPFv3 is OSPF for IPv6 (RFC 5340)
- Based on OSPFv2 with enhancements
- Distributes IPv6 prefixes only
- Runs directly over IPv6
- Ships-in-the-night with OSPFv2

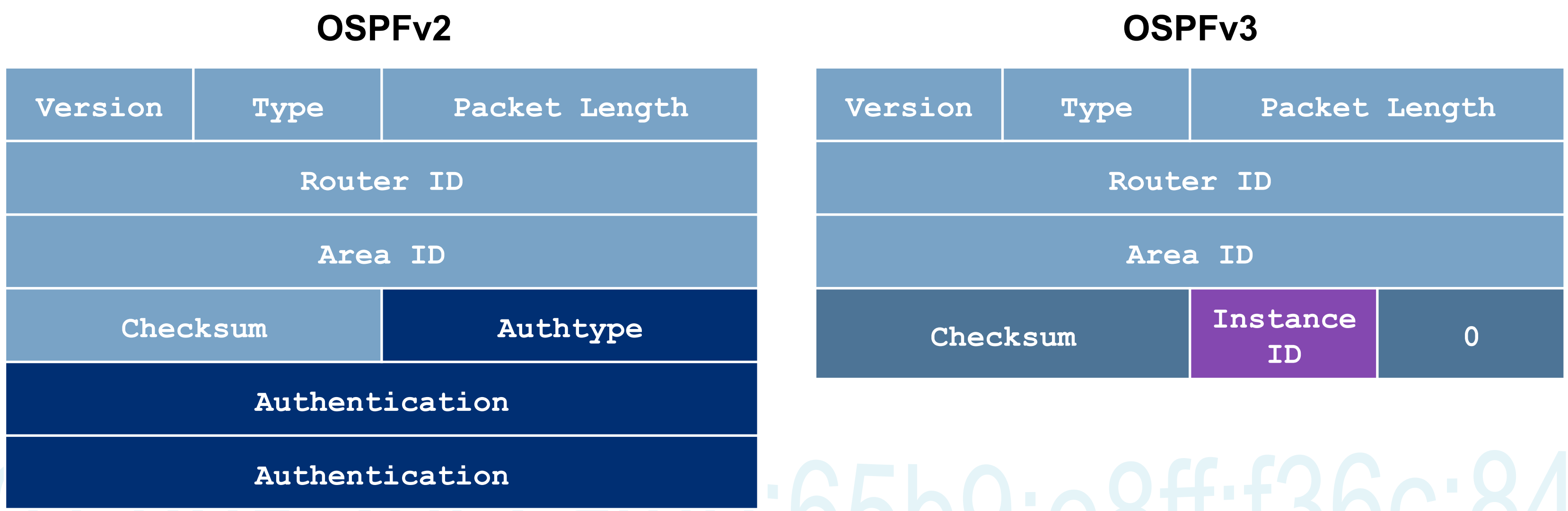
2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

OSPFv3 Differences from OSPFv2

- OSPFv3 has same 5 packet types some fields have been changed
- OSPFv3 packets have a 16 byte header verses the 24 byte header in OSPFv2

Packet Type	Description
1	Hello
2	Database description
3	Link state request
4	Link state update
5	Link state acknowledgement





2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

OSPFv3 Differences from OSPFv2

- Uses link local addresses
  - To identify the OSPFv3 adjacency neighbors
- Two New LSA Types
  - Link-LSA (LSA Type 0x0008)
  - There is one Link-LSA per link. This LSA advertises the router's link-local address, list of all IPv6 prefixes and options associated with the link to all other routers attached to the link
  - Intra-Area-Prefix-LSA (LSA Type 0x2009)
  - Carries all IPv6 prefix information that in IPv4 is included in Router-LSAs and Network-LSAs
- Two LSAs are renamed
  - Type-3 summary-LSAs, renamed to "Inter-Area-Prefix-LSAs"
  - Type-4 summary LSAs, renamed to "Inter-Area-Router-LSAs"

OSPFv3 Differences from OSPFv2

- Multicast Addresses
  - FF02::5 – Represents all SPF routers on the link local scope, Equivalent to 224.0.0.5 in OSPFv2
  - FF02::6 – Represents all DR routers on the link local scope, Equivalent to 224.0.0.6 in OSPFv2
- Removal of Address Semantics
  - IPv6 addresses are no longer present in OSPF packet header (Part of payload information)
  - Router LSA, Network LSA do not carry IPv6 addresses
  - Router ID, Area ID and Link State ID remains at 32 bits
  - DR and BDR are now identified by their Router ID and no longer by their IP address
- Security
  - OSPFv3 uses IPv6 AH & ESP extension headers instead of variety of mechanisms defined in OSPFv2

OSPFv3 LSA Types

LSA Description	LSA Code	LSA Type	Bits Set=1
Router LSA	1	0x2001	S1
Network LSA	2	0x2002	S1
Inter-Area-Prefix-LSA	3	0x2003	S1
Inter-Area-Router-LSA	4	0x2004	S1
AS-External-LSA	5	0x4005	S2
Deprecated	6	0x2006	S1
NSSA-LSA	7	0x2007	S1
Link-LSA	8	0x0008	
Intra-Area-Prefix-LSA	9	0x2009	S1

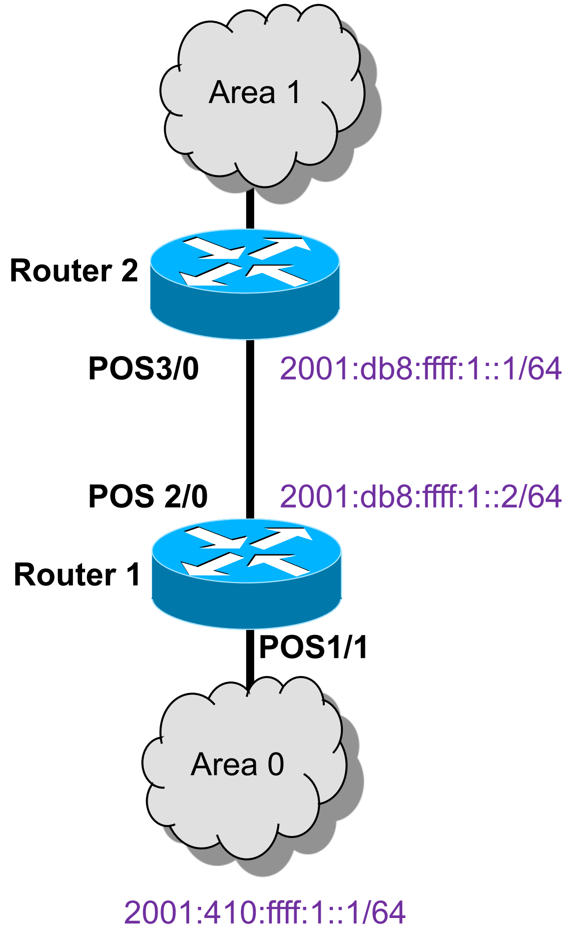
U Bit	LSA Handling
0	Treat the LSA as if it had link-local flooding scope
1	Store and flood the LSA as if the type is understood

S2	S1	Flooding Scope
0	0	Link-Local Scoping - Flooded only on originating link
0	1	Area Scoping - Flooded only in originating area
1	0	AS Scoping - Flooded throughout AS
1	1	Reserved

LSA Type Format

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

OSPFv3 Configuration Example




```
Router1#
interface POS1/1
 ipv6 address 2001:410:FFFF:1::1/64
 ipv6 ospf 100 area 0
!
interface POS2/0
 ipv6 address 2001:db8:FFFF:1::2/64
 ipv6 ospf 100 area 0
!
ipv6 router ospf 100
   router-id 10.1.1.3

Router2#
interface POS3/0
 ipv6 address 2001:db8:FFFF:1::1/64
 ipv6 ospf 100 area 0
!
ipv6 router ospf 100
   router-id 10.1.1.4
```

Enables IPv6 facing Area 0

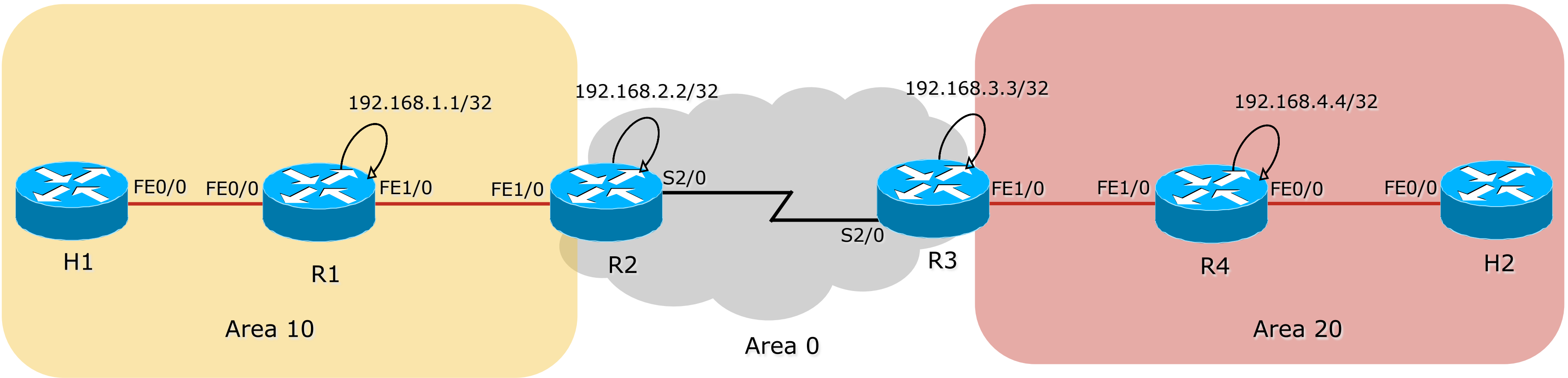
Interlink connection (could use link-lc

32 bit ID specified in dotted decimal notation

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Lab 4 : Routing with OSPFv3

OSPFv3 Configuration Example



BGP-4 Extensions for IPv6 (RFC 2545)

BGP-4 Extensions for IPv6 (MP-BGP)

- BGP-4 carries only 3 pieces of IPv4 specific information
  - NLRI in the UPDATE message contains an IPv4 prefix
  - NEXT_HOP path attribute in the UPDATE message contains a IPv4 address
  - BGP Identifier in the OPEN message & AGGREGATOR attribute
- RFC 4760 defines multi-protocol extensions for BGP-4 to support protocols other than IPv4
  - New BGP-4 optional and non-transitive attributes:
    - MP_REACH_NLRI
    - MP_UNREACH_NLRI
  - Protocol independent NEXT_HOP attribute
  - Protocol independent NLRI attribute

MP-BGP IPv6 Support

- Optional and non-transitive BGP attributes
  - MP_REACH_NLRI (Attribute code: 14)
    - "Carry the set of reachable destinations together with the next-hop information to be used for forwarding to these destinations" (RFC4760)
  - MP_UNREACH_NLRI (Attribute code: 15)
    - Carry the set of unreachable destinations
- Attribute 14 and 15 contains one or more triples
  - Address Family Information (AFI), Sub AFI (SAFI)
  - Next-Hop Information (must be of the same address family)
  - NLRI

AFI	Meaning
1	IPv4
2	IPv6

SAFI	Meaning
1	NLRI used for unicast
2	NLRI used for multicast
3	NLRI used for unicast and multicast
4	NLRI with MPLS labels
64	Tunnel SAFI
65	VPLS
66	BGP MDT
128	MPLS-labeled VPN address (VPNv4, VPNv6)

Source: http://www.iana.org/assignments/safi-namespace/safi-namespace.xml

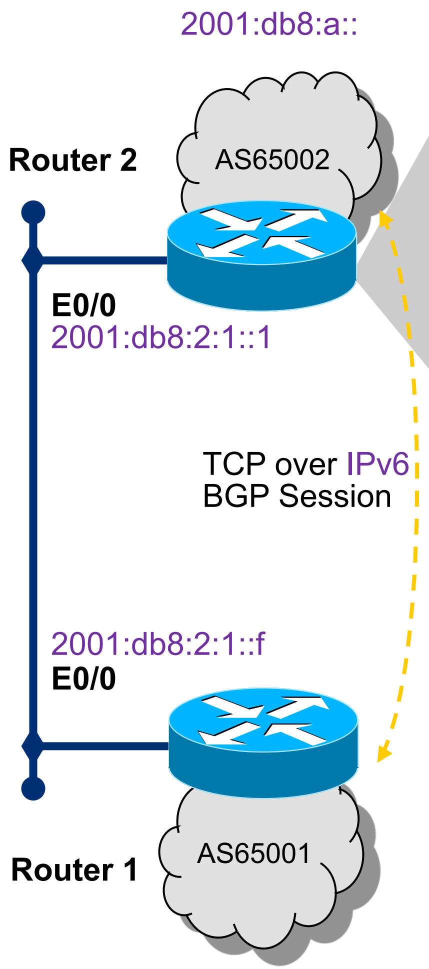
MP-BGP for IPv6 Considerations

- TCP Interaction
  - BGP-4 runs over a TCP (179) session using IPv4 or IPv6
  - The NLRI BGP carried (IPv4, IPv6, MPLS) is agnostic of the session protocol
- Router ID
  - If IPv4 session is not used, a BGP router-id must still exist in a 32 bit dotted decimal notation
  - The RID does not have to be in valid IPv4 format. For example, 0.0.0.1 is valid
  - The sole purpose of RID is for identification
  - In BGP it is used as a tie breaker and is sent within the OPEN message
- Next-hop contains a global IPv6 address (or potentially a link local address)

BGP Peering Address

- Two options are available for configuring BGP peering
- Using link local addressing
  - ISP uses FE80:: addressing for BGP neighbours
  - Deployable but not recommended
    - There are plenty of IPv6 addresses
    - Unnecessary configuration complexity
- Using global unicast addresses
  - As with IPv4
  - Recommended option

BGP IPv6 Configuration Global Address Peering




```
Router2#
!
interface Ethernet0/0
 ipv6 address 2001:db8:2:1::1/64
!
router bgp 65002
 bgp router-id 10.10.10.1
 no bgp default ipv4-unicast
 neighbor 2001:db8:2:1::f remote-as
65001
 address-family ipv6
  neighbor 2001:db8:c18:2:1::f activate
  network 2001:db8:a::/48
  exit-address-family
```

Router ID in dotted decimal notation

Disable IPv4 prefix exchange

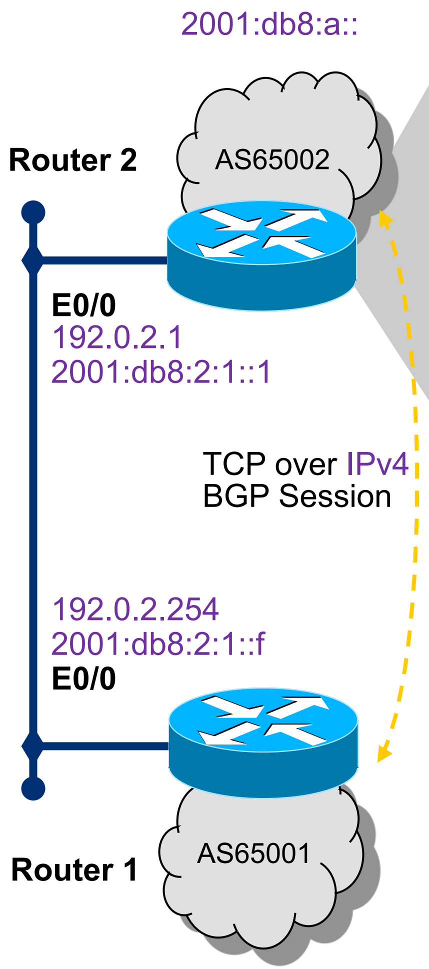
Only use IPv6 address family

Activate IPv6 session with neighb

IPv6 prefix to be advertised

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

BGP IPv6 NLRI Configuration over IPv4 Peer




```
Router2#
!
router bgp 65002
 bgp router-id 192.168.30.1
 neighbor 192.0.2.254 remote-as
65001
 !
 address-family ipv6
 neighbor 192.0.2.254 activate
 neighbor 192.0.2.254 route-map
SETNH out
 network 2001:db8:a::/48
!
route-map SETNH permit 10
 set ipv6 next-hop 2001:db8:2:1:1
```

Allow IPv6 AFI to be passed in NLRI

Enable BGP session over IPv4 to carry IPv6 pref

IPv6 prefix to be advertised

Ensure IPv6 NLRI has a suitable next-hop

- This configuration sets up an IPv4 neighbour session
- IPv4 session transports IPv6 prefixes (NLRI)
- Rewrites the next hop to a valid IPv6 address in the update
  - Inbound or Outbound route-maps can be used
- Next hop needs to be set to correct IPv6 address

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

BGP Configuration IPv4 and IPv6

```
router bgp 65000
 no bgp default ipv4-unicast
 neighbor 2001:db8:1:1019::1 remote-as 65001
 neighbor 172.16.1.2 remote-as 65002
!
 address-family ipv4
 neighbor 172.16.1.2 activate
 neighbor 172.16.1.2 prefix-list ipv4-ebgp in
 neighbor 172.16.1.2 prefix-list v4out out
 network 172.16.0.0
 exit-address-family
!
 address-family ipv6
 neighbor 2001:db8:1:1019::1 activate
 neighbor 2001:db8:1:1019::1 prefix-list
ipv6-ebgp in
 neighbor 2001:db8:1:1019::1 prefix-list
v6out out
 network 2001:db8::/32
 exit-address-family
!
ip prefix-list ipv4-ebgp permit 0.0.0.0/0 le
32
ip prefix-list v4out permit 172.16.0.0/16
ipv6 prefix-list ipv6-ebgp permit ::/0 le 128
ipv6 prefix-list v6out permit 2001:db8::/32
```

Common configuration section

Enable IPv4 specifics

Enable separate IPv4 BGP session

Enable IPv6 specifics

Enable separate IPv6 BGP session

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

BGP Status Commands

- IPv6 BGP show commands take ipv6 as argument

```
show bgp ipv6 unicast <parameter>
Router1#show bgp ipv6 unicast 2001:db8::/32
BGP routing table entry for 2001:db8::/32, version 11
Paths: (1 available, best #1)
Local
2001:db8:c18:2:1::1 from 2001:db8:c18:2:1::1 (10.10.20.2)
Origin incomplete, localpref 100, valid, internal, best
```

- IPv4 BGP show commands can also use this format

```
show bgp ipv4 unicast <parameter>
```

BGP Status Commands

- Display summary information regarding the state of the BGP neighbours

  show bgp ipv6 unicast summary

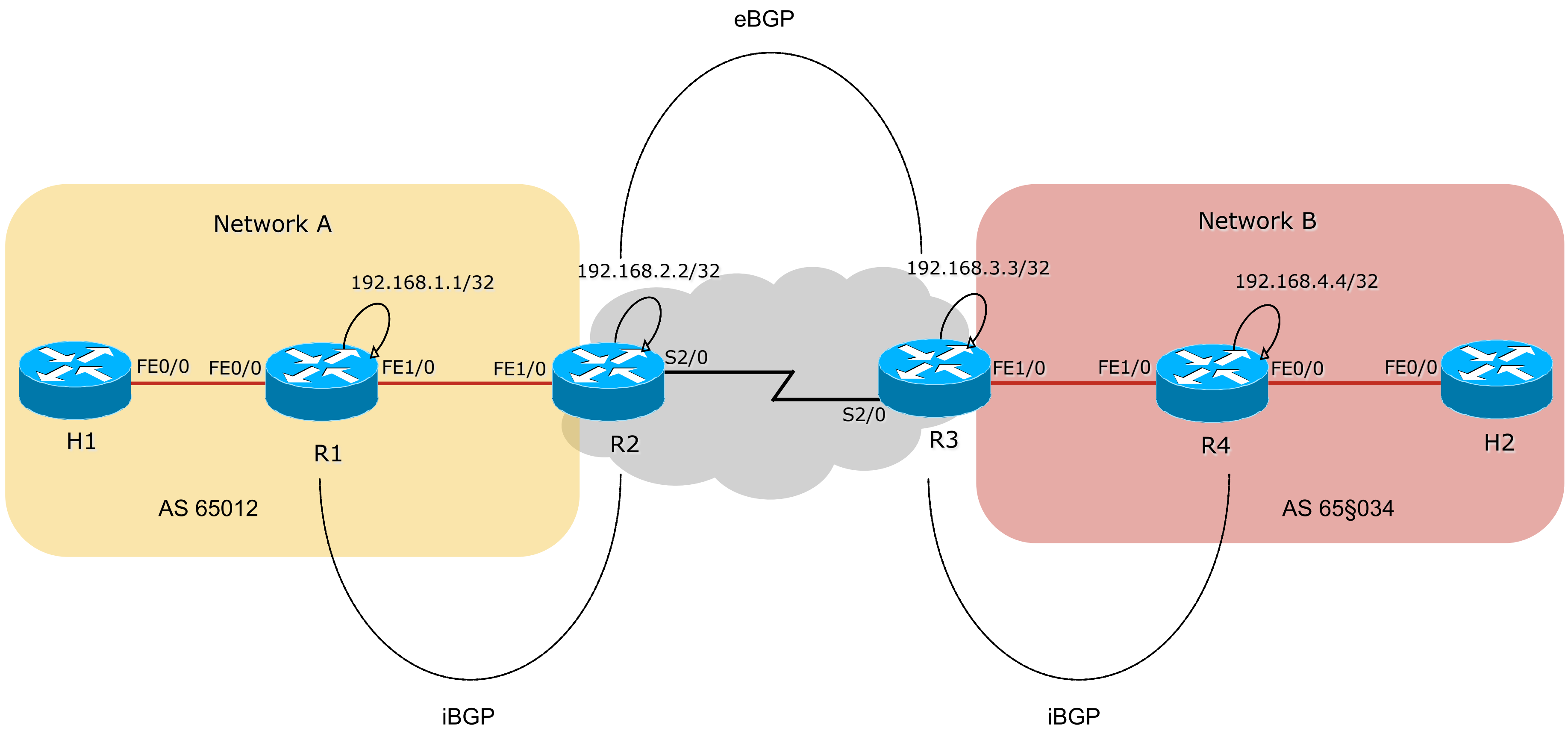
```
BGP router identifier 192.0.2.37, local AS number 65000
BGP table version is 400386, main routing table version 400386
585 network entries using 78390 bytes of memory
9365 path entries using 674280 bytes of memory
16604 BGP path attribute entries using 930384 bytes of memory
8238 BGP AS-PATH entries using 228072 bytes of memory
42 BGP community entries using 1008 bytes of memory
9451 BGP route-map cache entries using 302432 bytes of memory
584 BGP filter-list cache entries using 7008 bytes of memory
BGP using 2221574 total bytes of memory
2 received paths for inbound soft reconfiguration
BGP activity 63094/62437 prefixes, 1887496/1878059 paths, scan interval
60secs

Neighbor        V    AS  MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
2001:1458:C000::64B:4:1
                4  65001 1294728  460213   400386    0    0 3d11h
498
```

Neighbour Information

Prefixes Received

Lab 5 : Routing with BGP

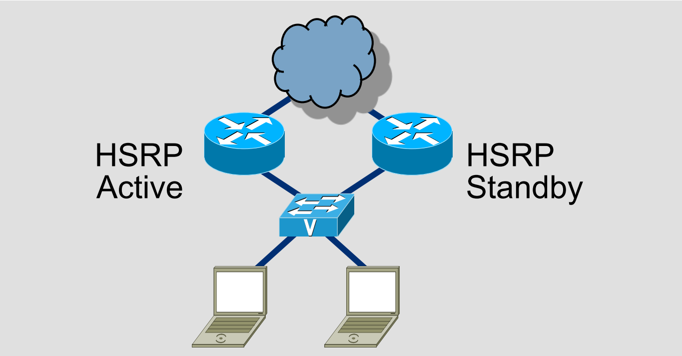
BGP Configuration Example



2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

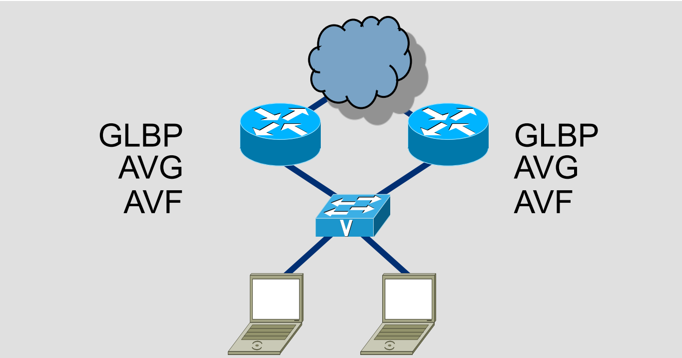
First Hop Redundnacy Protocol

First Hop Router Redundancy Options



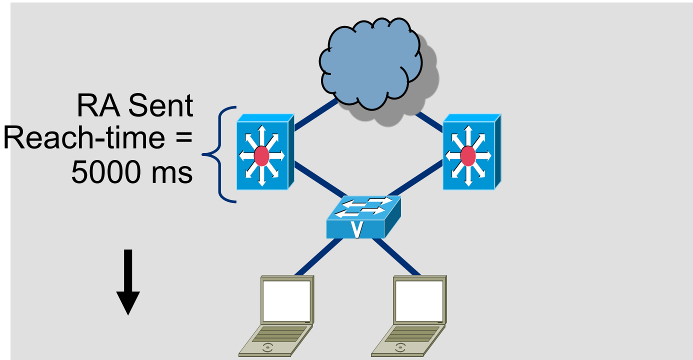
HSRP for IPv6

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



GLBP for IPv6

- Modification to Neighbor Advertisement, Router Advertisement Gateway 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)

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

First-Hop Redundancy using NUD

- NUD as last resort, when HSRP, GLBP or VRRP for IPv6 are not available
- NUD can be used for rudimentary HA at the first-hop

  This only applies to the L3 devices not supported HSRP

  ```
  ipv6 nd reachable-time 5000
  ```

  Decreasing timers increases traffic and processing

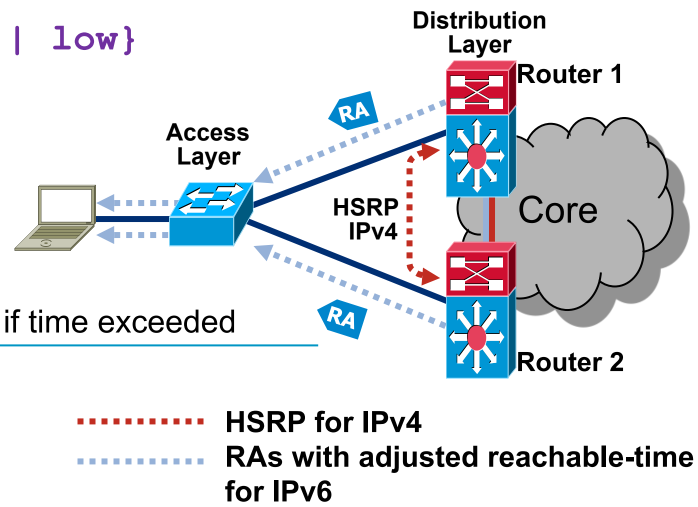
- Hosts use NUD "reachable time" to cycle to next known default gateway (30 seconds by default)
- Can be combined with default router preference to determine primary gateway

  ```
  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
```

Switch to other gateway if time exceeded



2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

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 (4096 addresses)

  0005.73a0.0000 - 0005.73a0.0FFF
- HSRP IPv6 UDP Port Number 2029

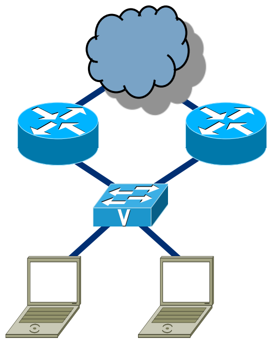
2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

HSRP for IPv6 Configuration

```
Router 1#config term
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
```

Mandatory before HSRPv6 can be activated

Generate link-local using virtual MAC & group ID



Note V-MAC converted into EUI-64

Host with GW of Virtual IP

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

HSRP link-local with Virtual MAC & group ID

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

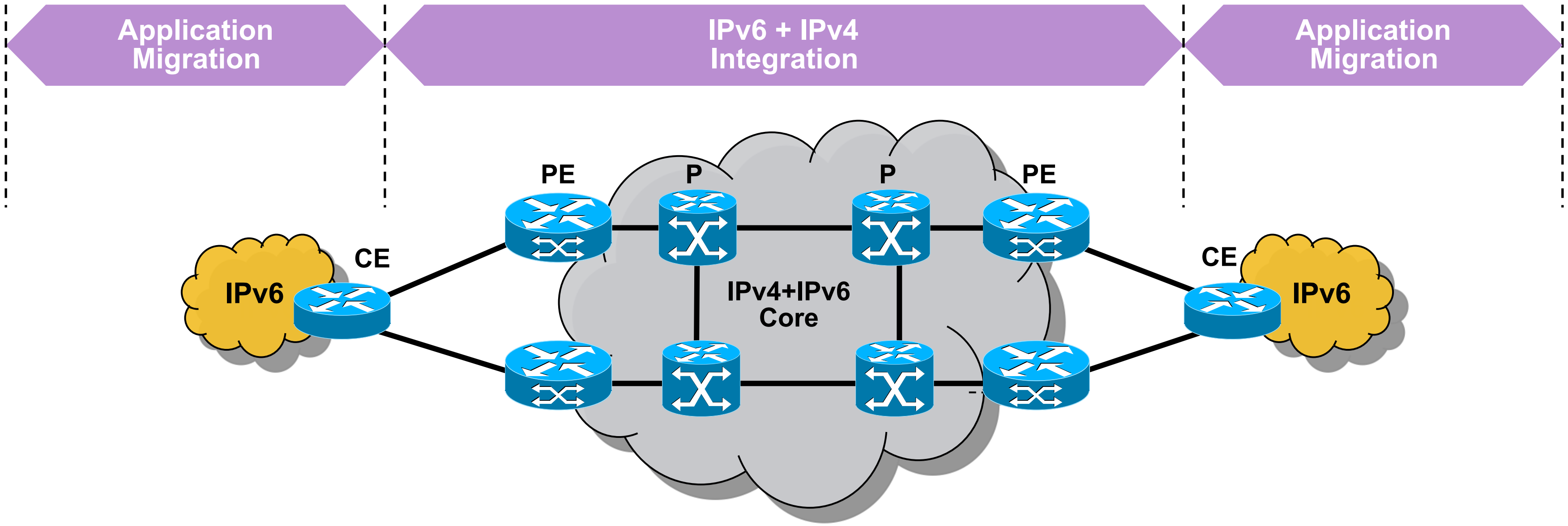
Review Questions

- Q1: What format is the Router-ID in IPv6 routing protocols
  32 bit integer in dotted decimal notation (a.b.c.d) - looks like IPv4 but is not!
- Q2: What next-hop do IPv6 dynamic protocols use?
  Dynamic routing protocols always use the link-local address of the next-hop
- Q3: How does BGP carry an IPv6 address?
  It uses a special IPv6 address family in multi-protocol BGP
- Q4: Name two protocols that provide first hop redundancy
  HSRP, GLBP and NUD (Neighbour Unreachability Detection)

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

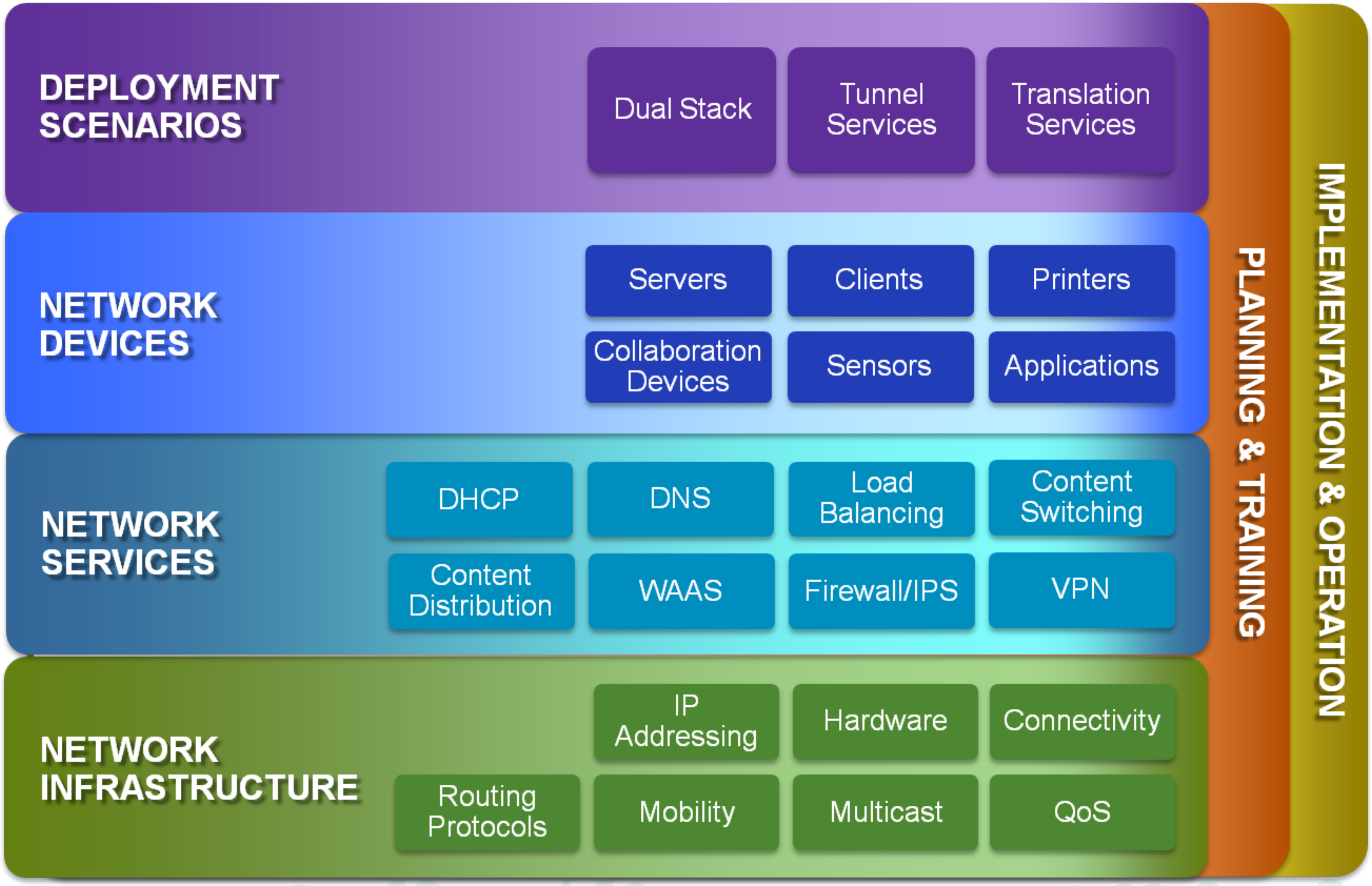
IPv6 Deployment

Integration or Migration?



- Some applications at the edge will MIGRATE to IPv6
- Network infrastructures will INTEGRATE IPv6
    - IPv4 will be around for a very long time
    - Networks will support both protocols
    - Many hardware components will be dual-stack capable (IPv4+IPv6)
    - IPv6 is a gradual and controlled process of INTEGRATION

Architectural Scope of IPv6 Deployment

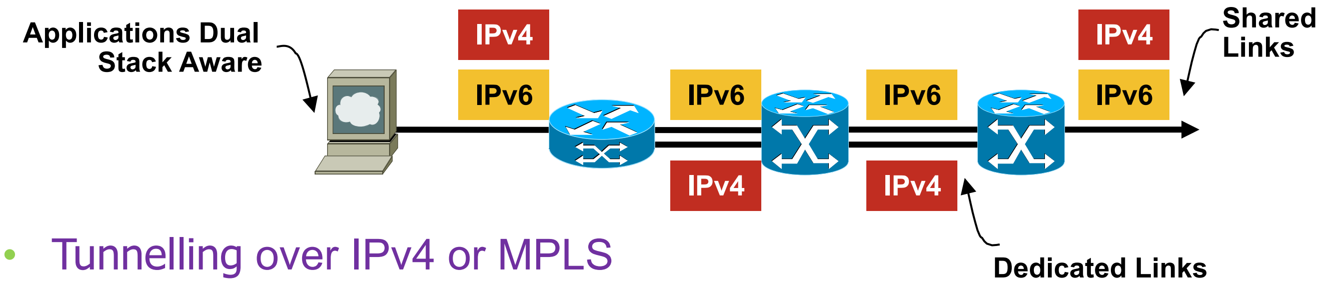


2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

IPv6 Deployment Options

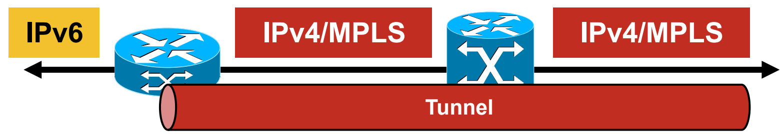
- Dual Stack (in devices/hosts and networks)

  IPv4 and IPv6 operate in tandem over shared or dedicated links



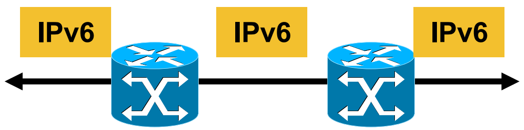
- Tunnelling over IPv4 or MPLS

  IPv6 confined to the edge of the IPv4 / MPLS core



- IPv6 Only

  IPv6 is the only protocol operating in the network



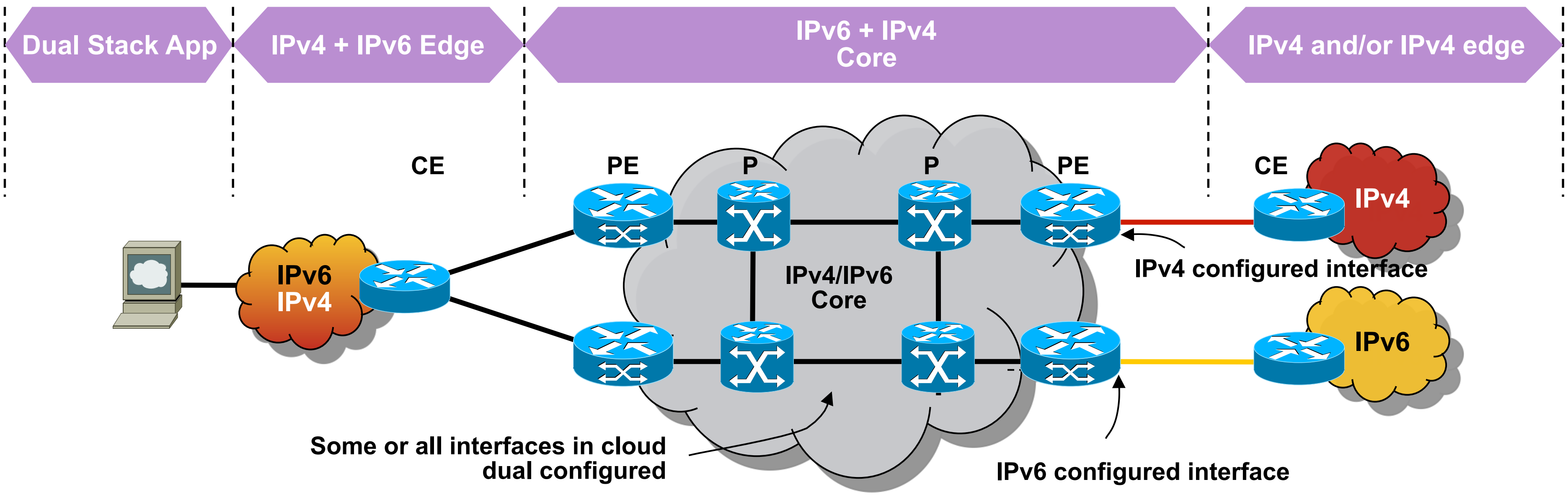
- 6to4 Protocol Translation

  Allow IPv6-only devices to communicate with IPv4-only devices

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Dual Stack Technique

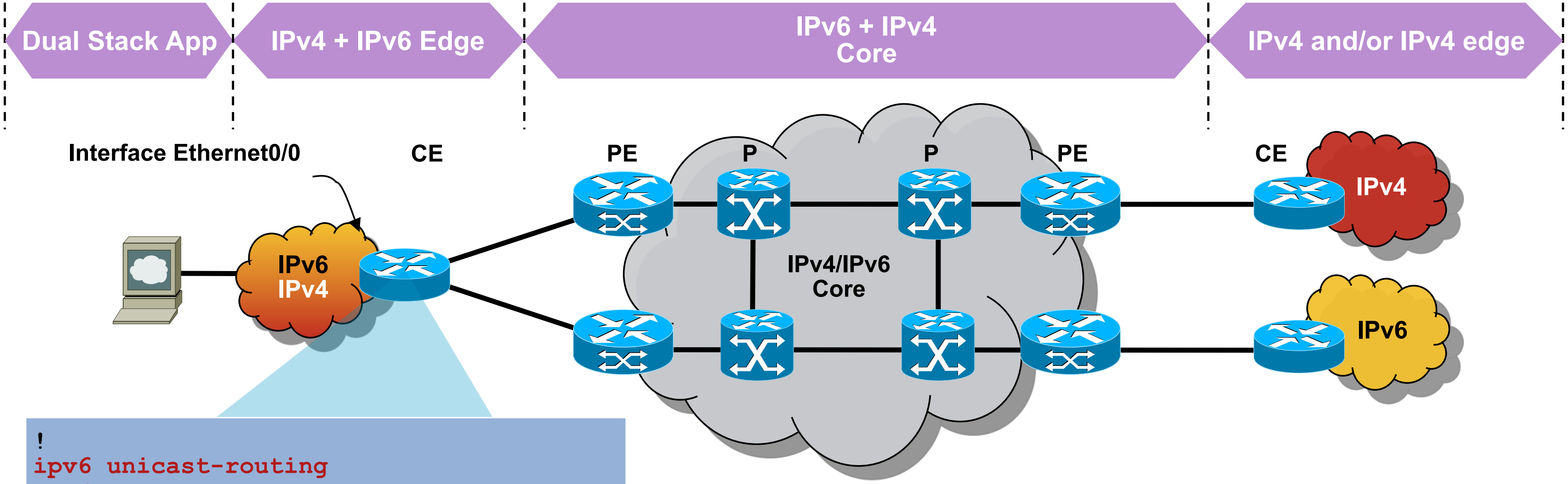
IPv6 using Dual Stack Backbone



- All P + PE routers are capable of IPv4+IPv6 support
- Two IGPs supporting IPv4 and IPv6
- Memory considerations for larger routing tables
- Native IPv6 multicast support
- All IPv6 traffic routed in global space
- Good for content distribution and global services (Internet)

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Dual Stack Configuration
The Basics

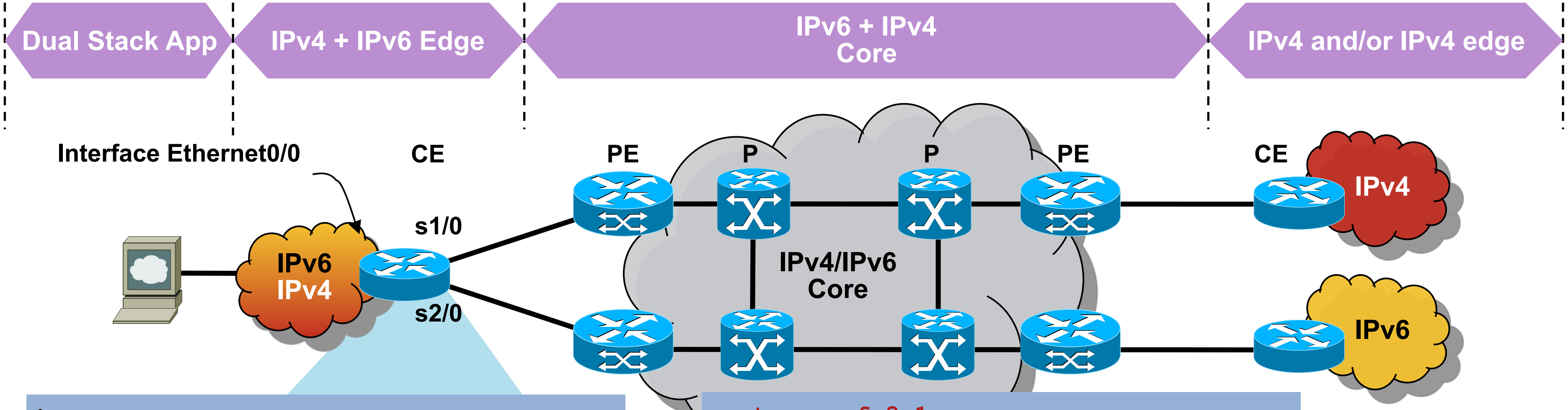



```
!
ipv6 unicast-routing
ipv6 cef
!
interface Ethernet0/0
 ip address 192.168.99.1 255.255.255.0
 ipv6 address 2001:db8:213:1::1/64
!
```

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Dual Stack Configuration

More Realistic

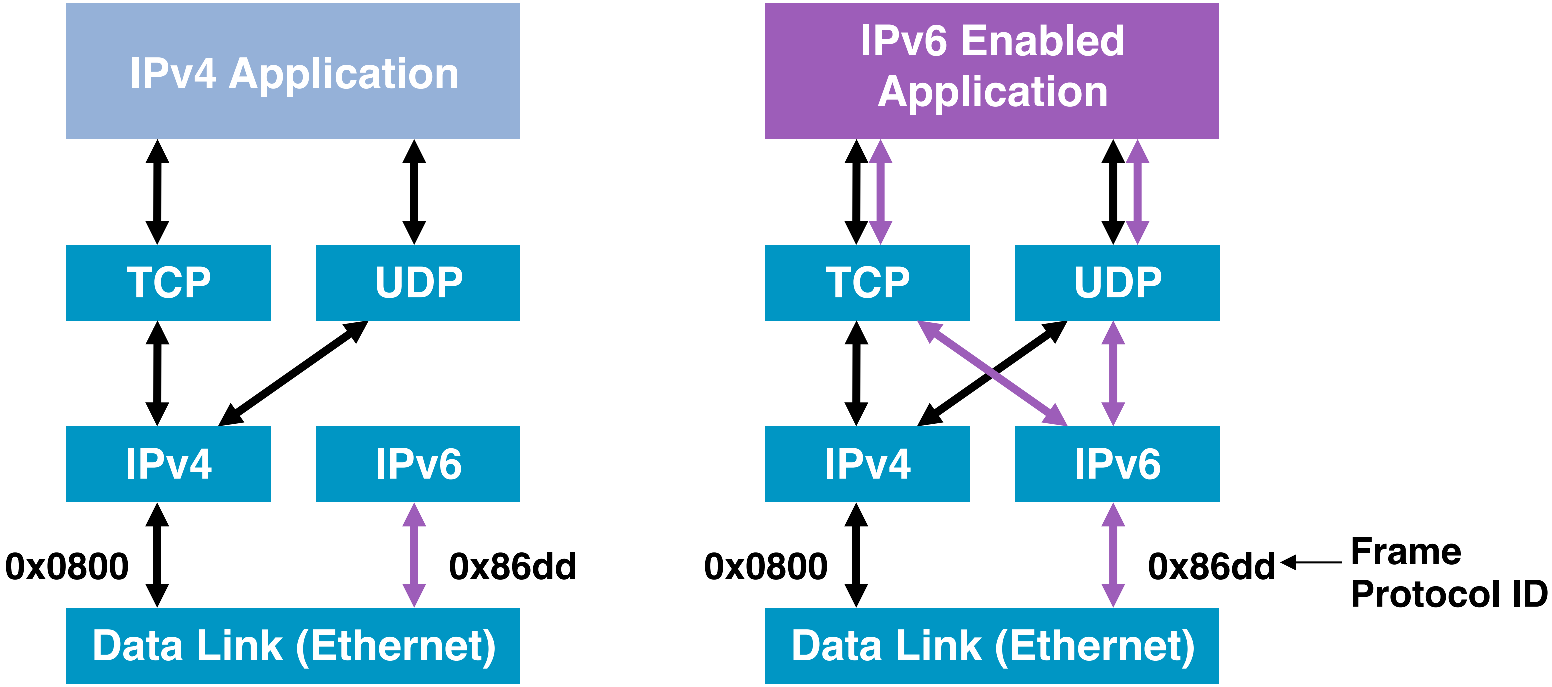



```
!
interface Ethernet0/0
 ip address 192.168.99.1 255.255.255.0
 ipv6 address 2001:db8:213:1::1/64
 ospfv3 1 area 0 ipv6
!
interface Serial 1/0
 ip address 192.0.2.1 255.255.255.252
 ipv6 address 2001:db8:ffff:1::1/64
!
interface Serial 2/0
 ip address 192.0.2.5 255.255.255.252
 ipv6 address 2001:db8:ffff:2::1/64
!
```

```
router ospfv3 1
 address-family ipv6 unicast
 exit-address-family
!
router bgp 65000
...
address-family ipv4
neighbor 192.0.2.2 activate
neighbor 192.0.2.6 activate
!
address-family ipv6
neighbor 2001:db8:ffff:1::2 activate
neighbor 2001:db8:ffff:2::2 activate
...
```

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

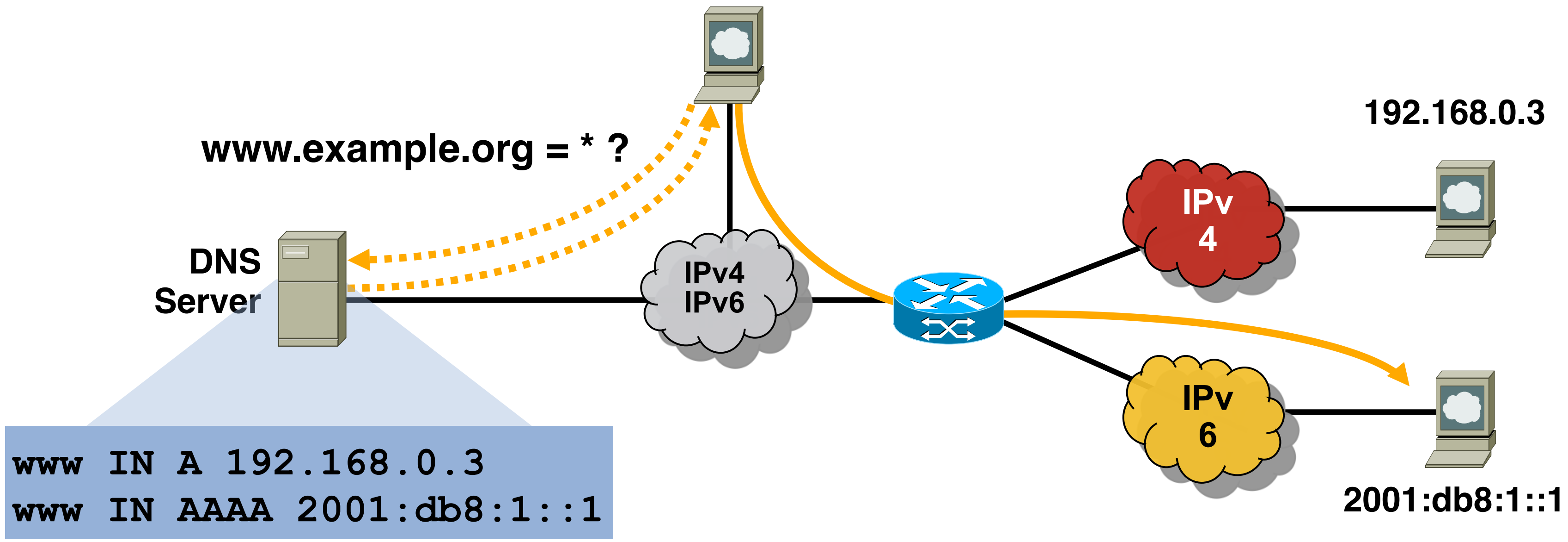
Application Dual Stack Approach



- Dual stack in a device means
  - Both IPv4 and IPv6 stacks enabled
  - Applications can talk to both
  - Choice of the IP version is based on DNS and application preference
- Dual stack at edge does not necessarily mean dual stack backbone

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

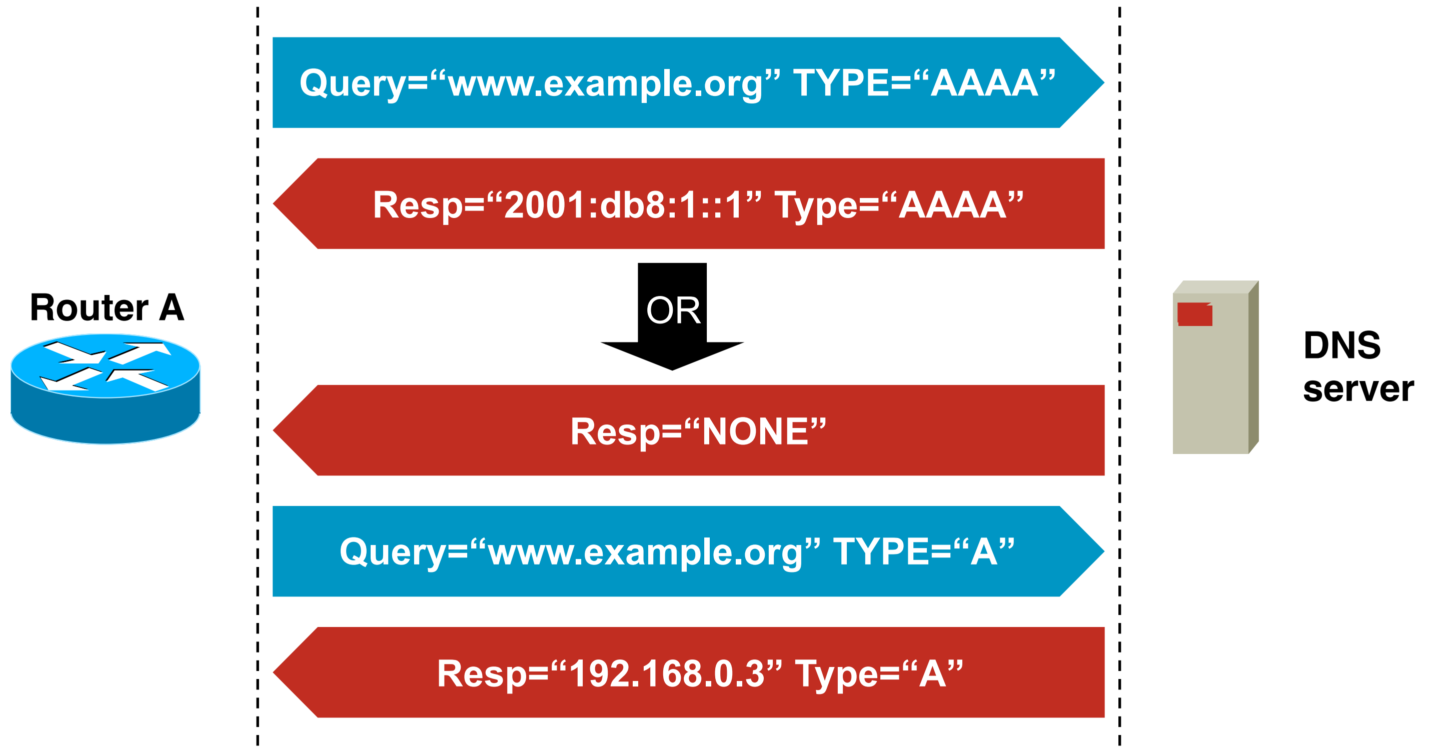
Dual Stack Approach & DNS



- In a dual stack network an application that is IPv4 and IPv6-enabled:
  - Can query the DNS for IPv4 records (A) and/or IPv6 (AAAA) records
  - The transport used for the lookup is not related to the resource record required.
    - e.g. Use IPv4 transport to ask for AAAA records
  - Chooses one address and, for example, connects to the IPv6 address

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

DNS query in IOS

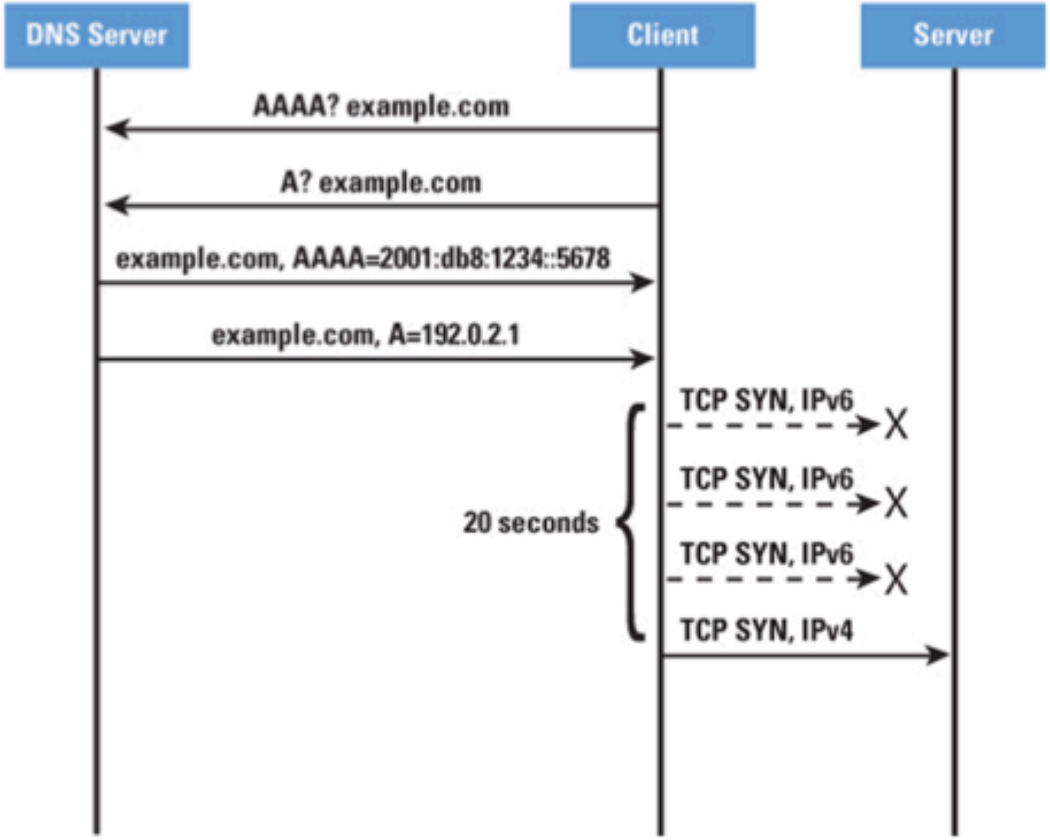


- DNS resolver picks IPv6 AAAA record first
- IPv6 stacks on Windows XP, W7, Linux, FreeBSD, MacOS etc also pick IPv6 address before IPv4 address if both exist

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Improving User Experience with Happy Eyeballs

Behaviour of a typical Web-Browser

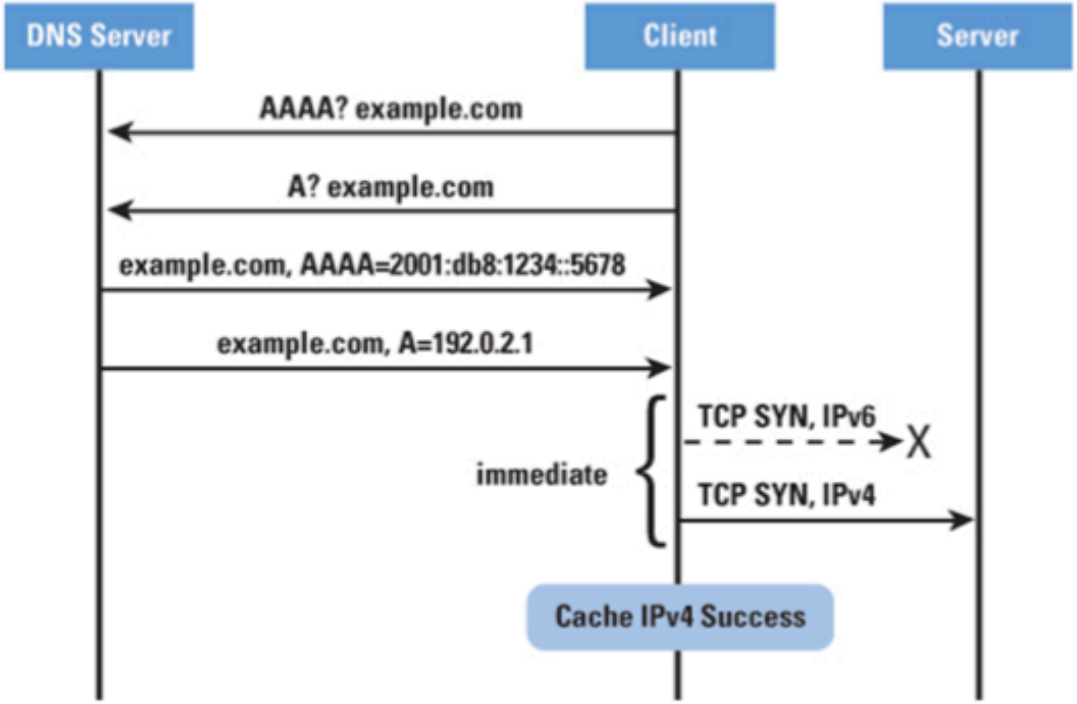


draft-ietf-v6ops-happy-eyeballs
http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_13-3/133_he.html

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Improving User Experience with Happy Eyeballs

Dual-Stack Web-Browser implementing Happy Eyeballs



draft-ietf-v6ops-happy-eyeballs
http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_13-3/133_he.html

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

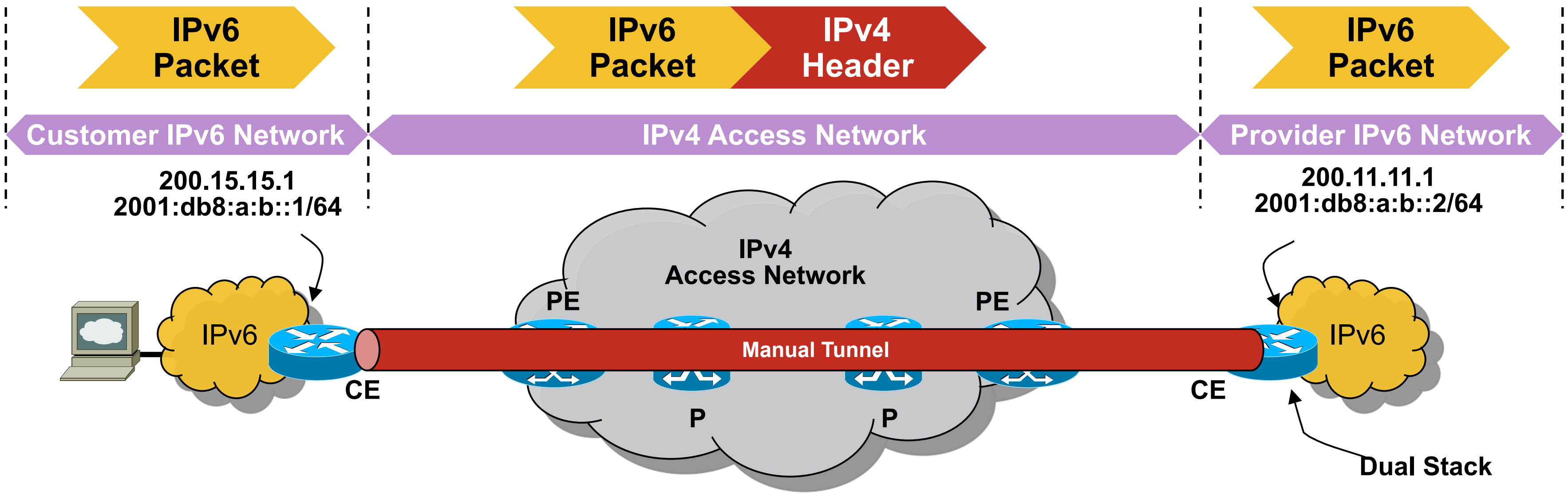
Tunnel Technique

Using Tunnels for IPv6 Deployments

- Tunnelling encapsulates an IPv6 packet into an IPv4 packet
  - Host to Router, Router to Router, Router to Host, or Host to Host
- Manually configured tunnels
  - Manual Tunnel (RFC 2893)
  - IPv6 over GRE (RFC 2473)
- Semi-automated tunnels
  - Tunnel broker (RFC 3053)
- Automatic tunnels
  - 6to4 (RFC 3056)
  - ISATAP (RFC 5214)
  - Dynamic Multipoint VPN
  - 6rd (RFC5969)

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

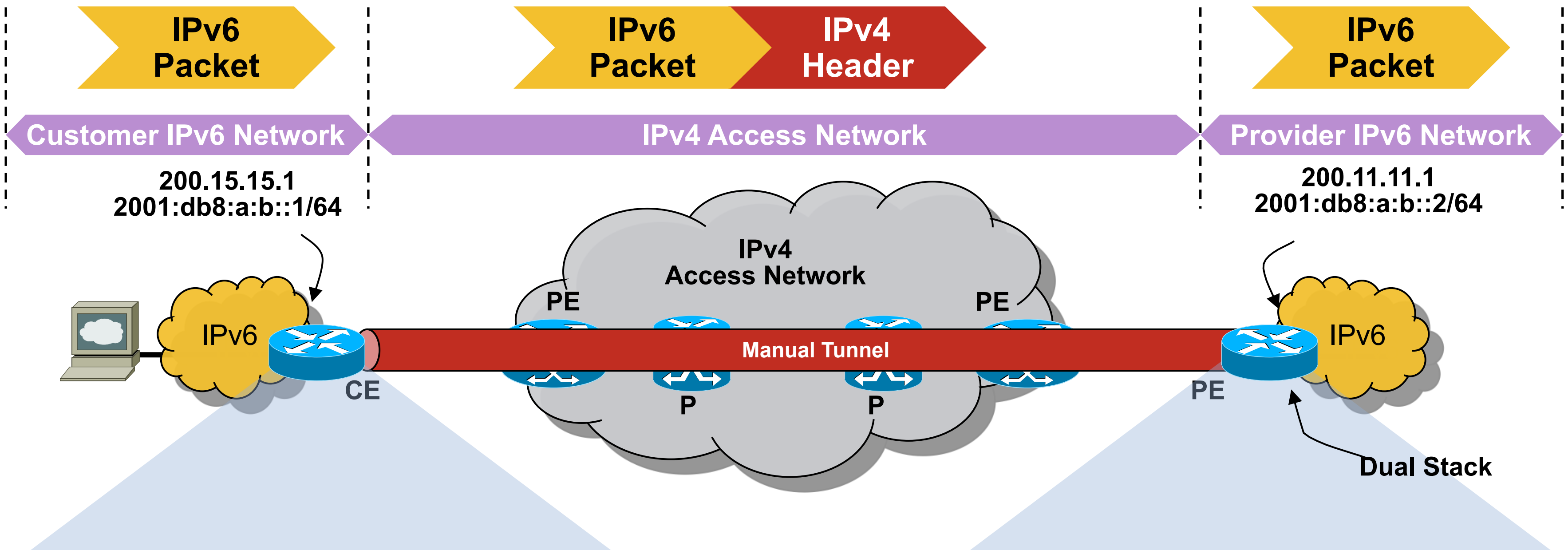
Manual Tunnel (RFC 2893)



- One of the first transition mechanisms developed for IPv6
  - Static P2P tunnel, IP protocol type = 41, no additional header, NAT breaks
- Terminates on dual stack end points
  - IPv4 end point address must be routable
  - IPv6 prefix configured on tunnel interface
- Difficult to scale and manage
  - For link few sites in fixed long term topology
  - Use across IPv4 access network to reach IPv6 Provider

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Manual Tunnel Configuration



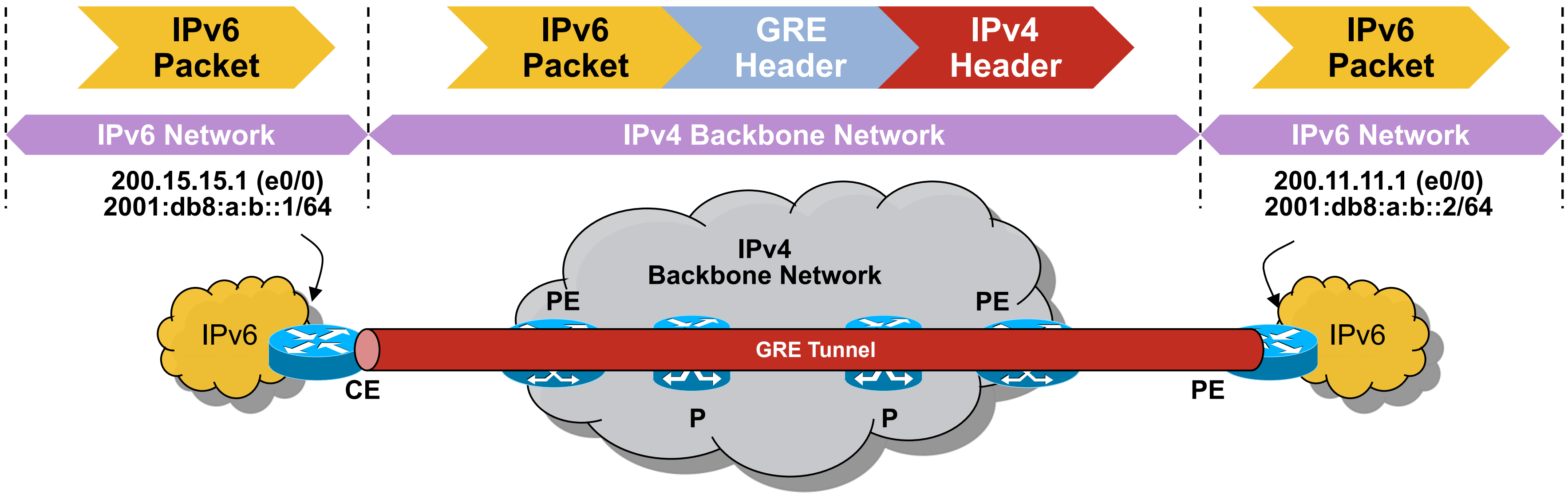

```
interface tunnel 100
 ipv6 address 2001:db8:a:b::1/64
 tunnel source 200.15.15.1
 tunnel destination 200.11.11.1
 tunnel mode ipv6ip
```

```
interface tunnel 100
 ipv6 address 2001:db8:a:b::2/64
 tunnel source 200.11.11.1
 tunnel destination 200.15.15.1
 tunnel mode ipv6ip
```

- Only supports routing protocols that use IP encapsulation
  - ISIS is itself a network layer protocol (not dependant upon IP)
  - Therefore will not work over IP Protocol-Type=41

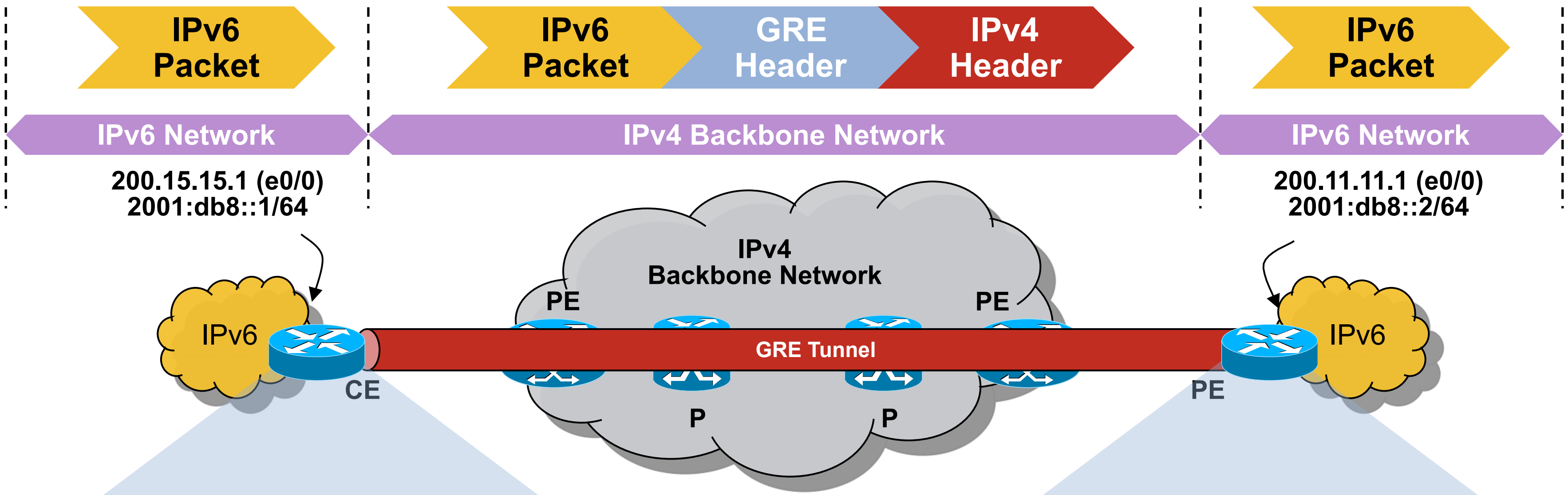
2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

IPv6 over GRE Tunnel



- Similar to Manual Tunnel (RFC 2893)
  - But can transport non IP packets
  - Hence can be used to support ISIS across the tunnel
- GRE header uses 0x86DD to identify IPv6 payload
- Similar scale and management issues
- L2TPv3 is another tunnelling option

IPv6 over GRE Tunnel Configuration

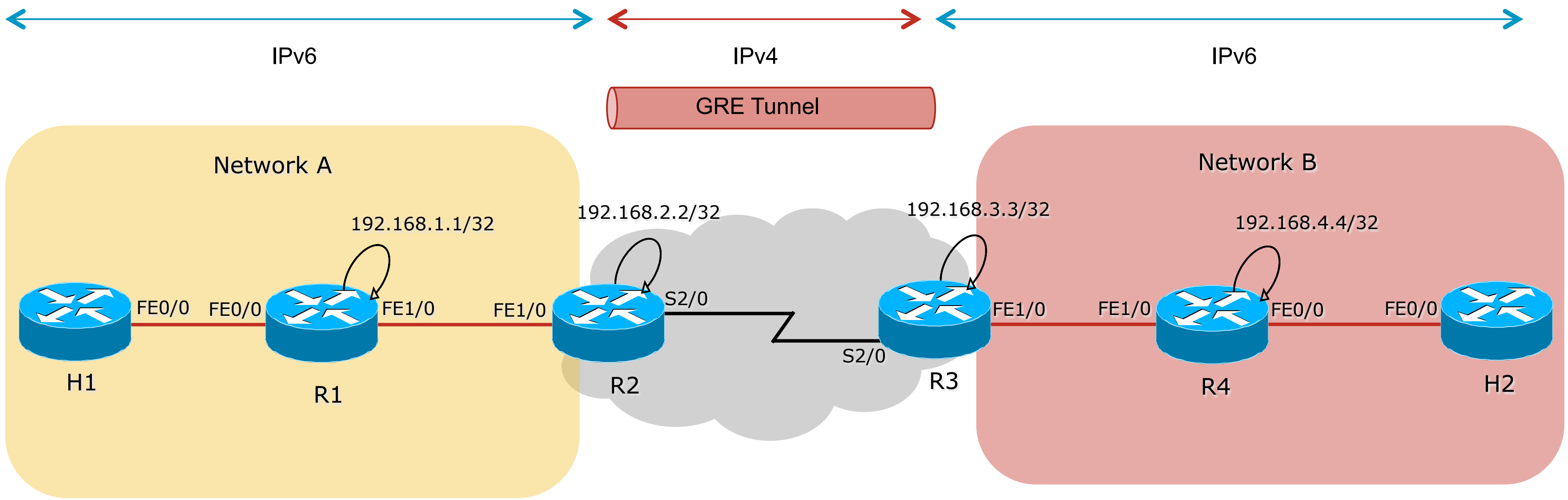



```
interface tunnel 100
 ipv6 address 2001:db8:a:b::1/64
 tunnel source e0/0
 tunnel destination 200.11.11.1
 tunnel mode gre ip
 ipv6 router isis
```

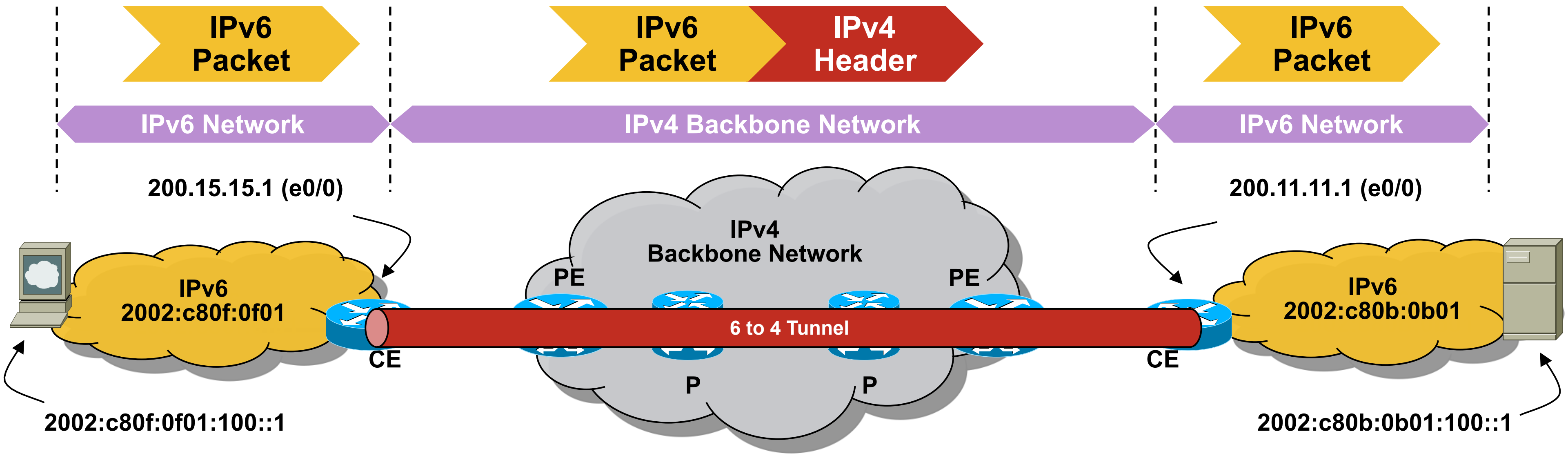
```
interface tunnel 100
 ipv6 address 2001:db8:a:b::2/64
 tunnel source e0/0
 tunnel destination 200.15.15.1
 tunnel mode gre ip
 ipv6 router isis
```

Lab 6 : Manual Tunneling in IPv6

Manual Tunnel Configuration Example



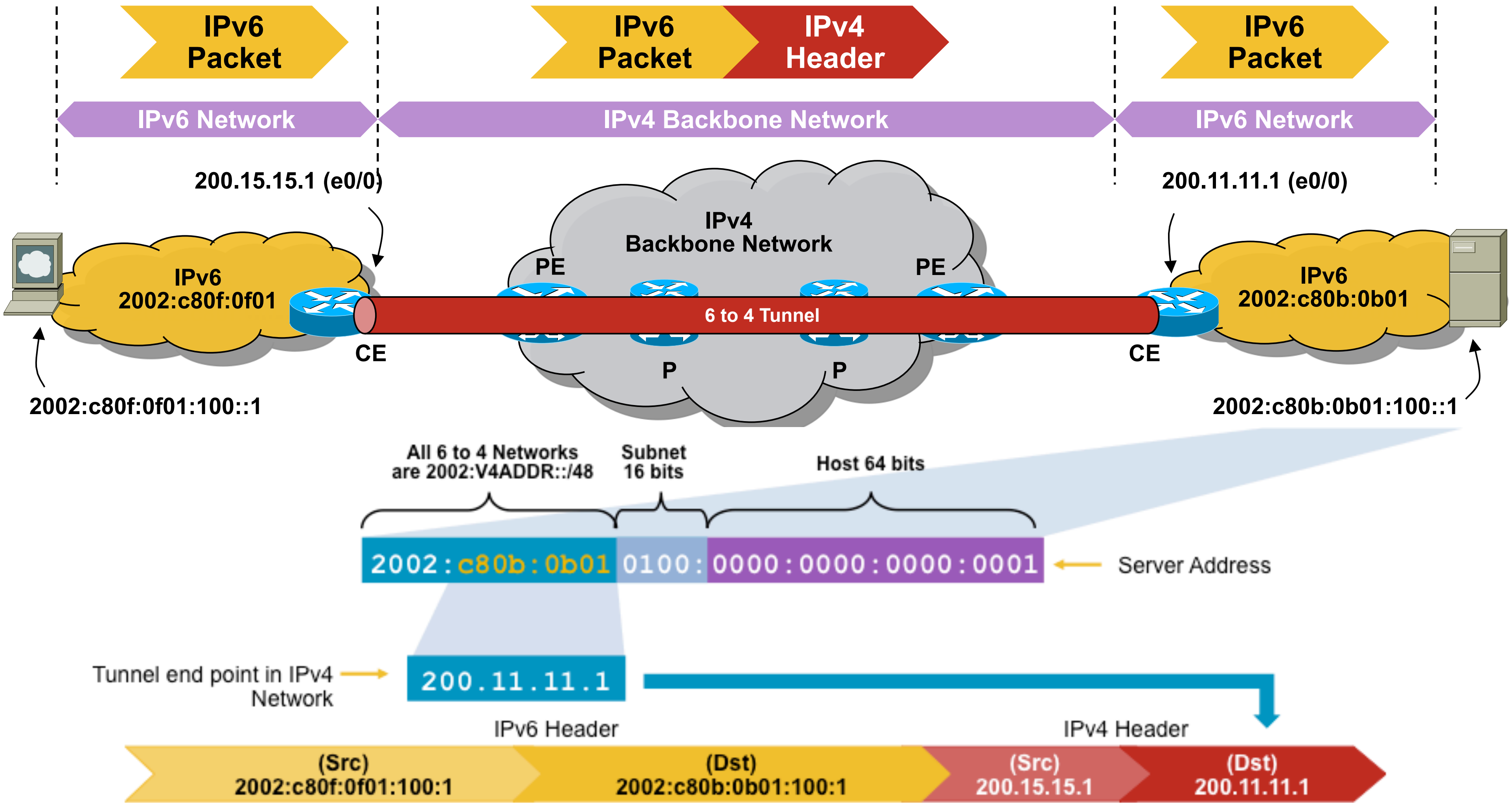
6 to 4 Tunnels (RFC 3056)



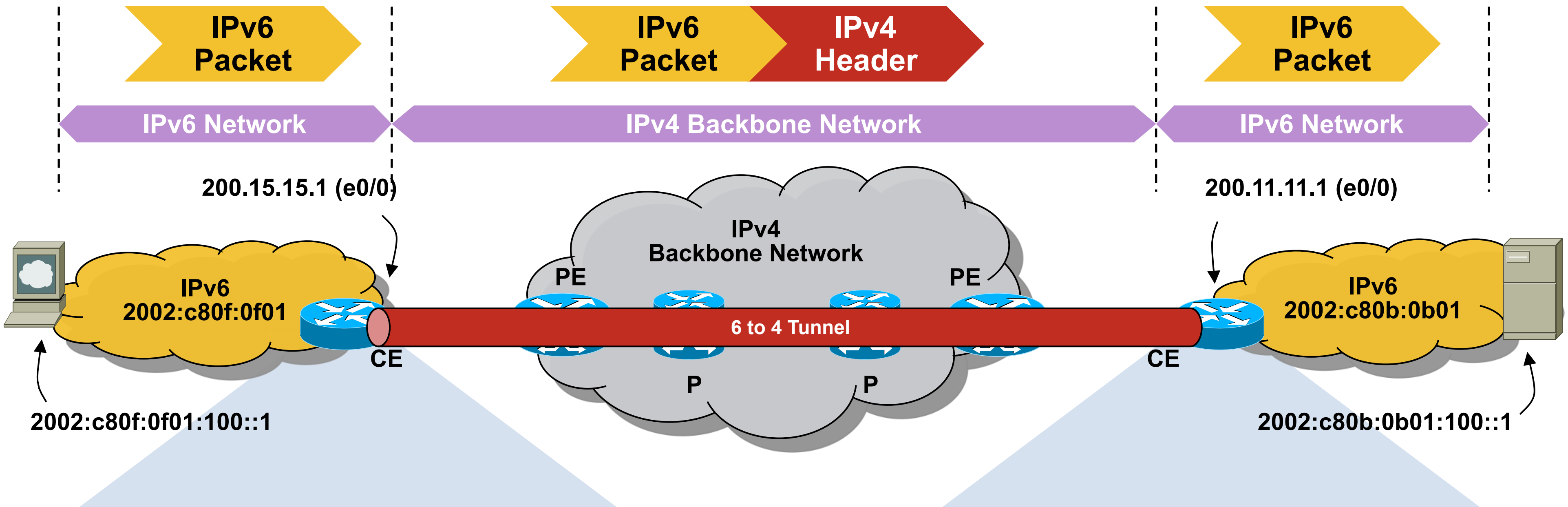
- Automatic tunnel method using 2002:IPv4::/48 IPv6 range
  IPv4 embedded in IPv6 format eg. `2002:c80f:0f01::` = `200.15.15.1`
- No impact on existing IPv4 or MPLS Core (IPv6 unaware)
- Tunnel endpoints have to be IPv6 and IPv4 aware (Dual stack)
- Transition technology – not for long term use
- No multicast support, Static Routing
- Intrinsic linkage between destination IPv6 Subnet and IPv4 gateway interface
  IPv4 Gateway = Tunnel End point

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Destination Dynamically Computed



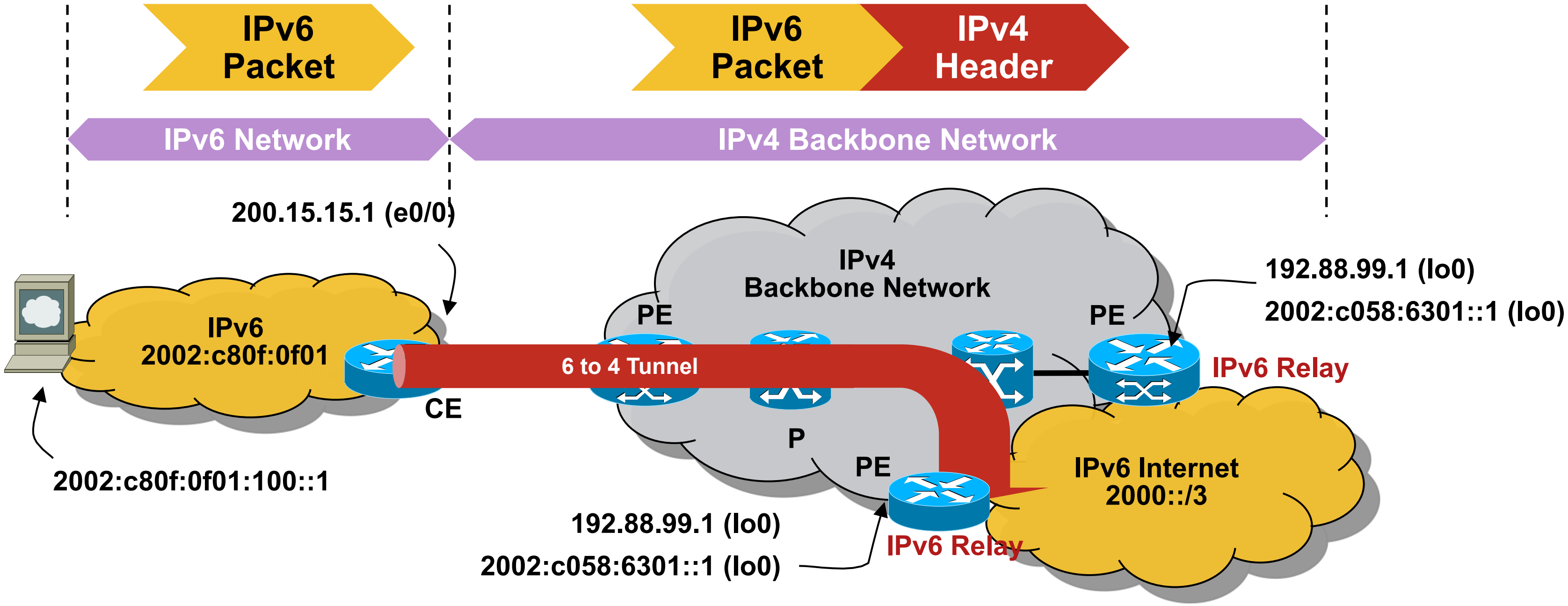
6 to 4 Configuration




```
interface tunnel 2002
 ipv6 address 2002:c80f:0f01::1/128
 tunnel source ethernet0/0
 tunnel mode ipv6ip 6to4

interface ethernet 0/0
 ip address 200.15.15.1 255.255.255.0

interface ethernet 1/0
 ipv6 address 2002:c80f:0f01:100::2/64

ipv6 route 2002::/16 tunnel2002
```

```
interface tunnel 2002
 ipv6 address 2002:c80b:0b01::1/128
 tunnel source ethernet0/0
 tunnel mode ipv6ip 6to4

interface ethernet 0/0
 ip address 200.11.11.1 255.255.255.0

interface ethernet 1/0
 ipv6 address 2002:c80b:0b01:100::2/64

ipv6 route 2002::/16 tunnel2002
```

6 to 4 Relay Service

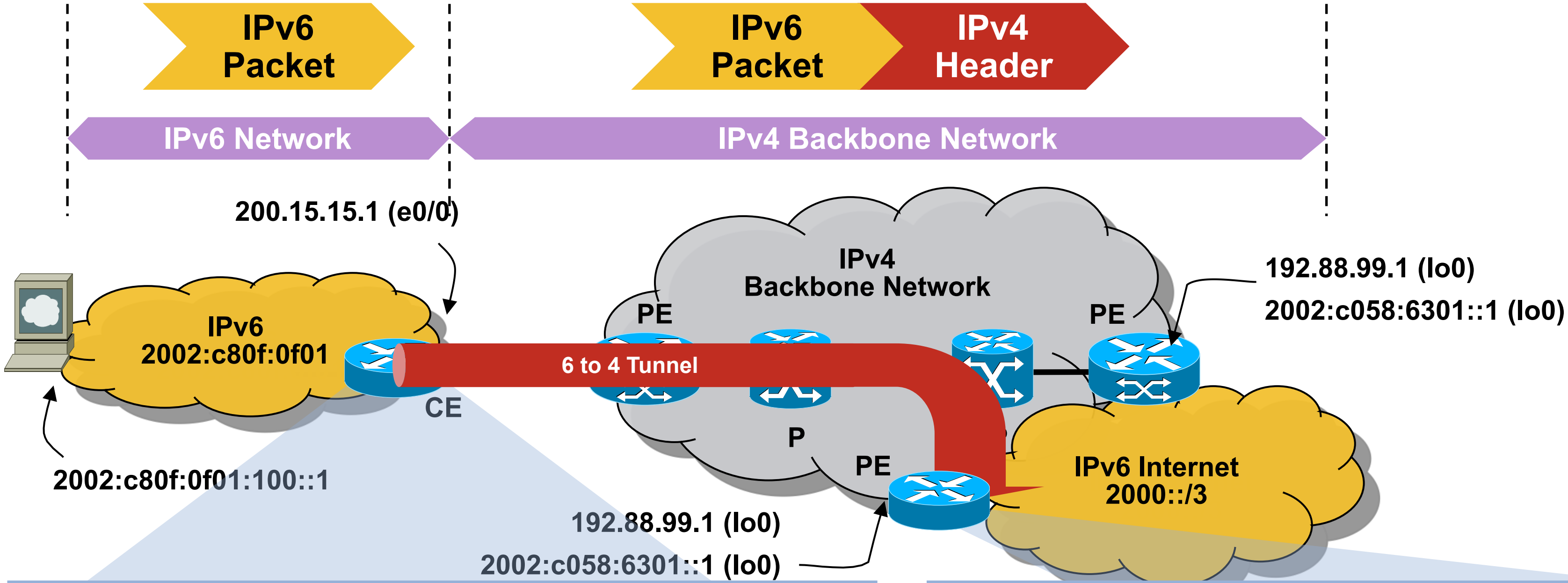


- 6 to 4 relay allows access to IPv6 global network
- Can use tunnel Anycast address 192.88.99.1
  - 6 to 4 router finds closest 6-to-4 relay router
  - Return path could be asymmetric
- Default route to IPv6 Internet
  - BGP can also be used to select particular 6 to 4 relay based on prefix
  - Allows more granular routing policy

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

6 to 4 Relay Configuration



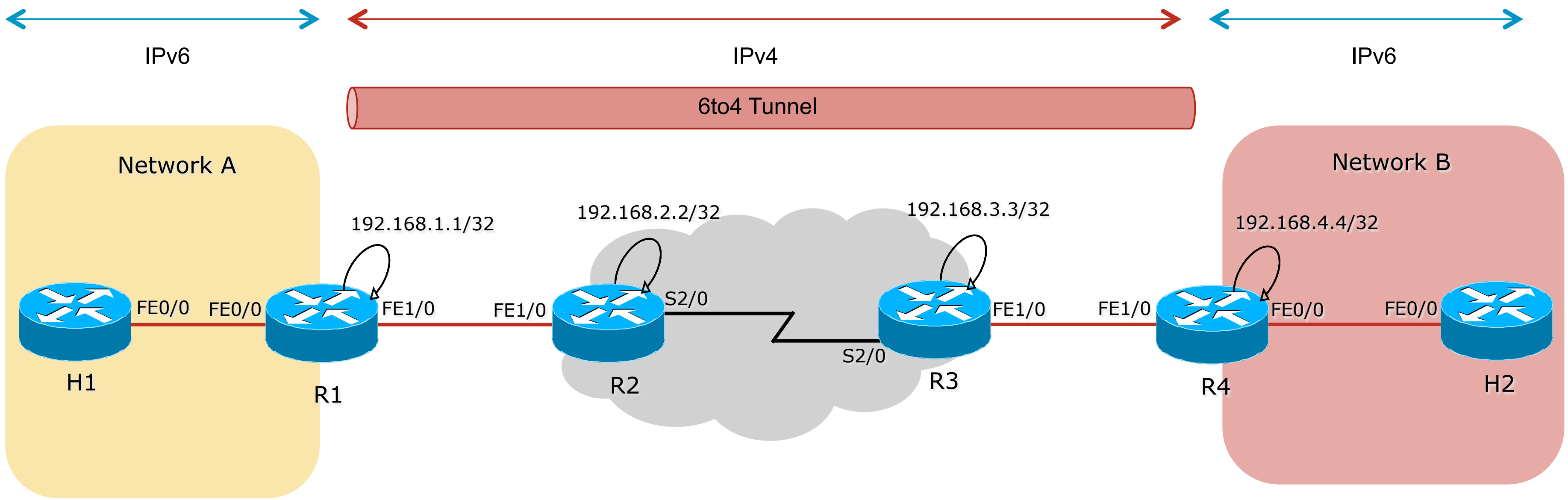

```
interface tunnel 2002
 ipv6 address 2002:c80f:0f01::1/128
 tunnel source ethernet0/0
 tunnel mode ipv6ip 6to4

interface ethernet 0/0
 ip address 200.15.15.1 255.255.255.0

interface ethernet 1/0
 ipv6 address 2002:c80f:0f01:100::2/64

ipv6 route 2002::/16 tunnel2002
ip route ::/0 2002:c058:6301::1
```

```
interface Loopback0
  ip address 192.88.99.1 255.255.255.0
  ipv6 address 2002:c058:6301::1/128
!
interface Tunnel2002
  ipv6 unnumbered Loopback2
  tunnel source Loopback2
  tunnel mode ipv6ip 6to4
!
ipv6 route 2002::/16 Tunnel2002
```

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Lab 7 : Automatic Tunneling in IPv6

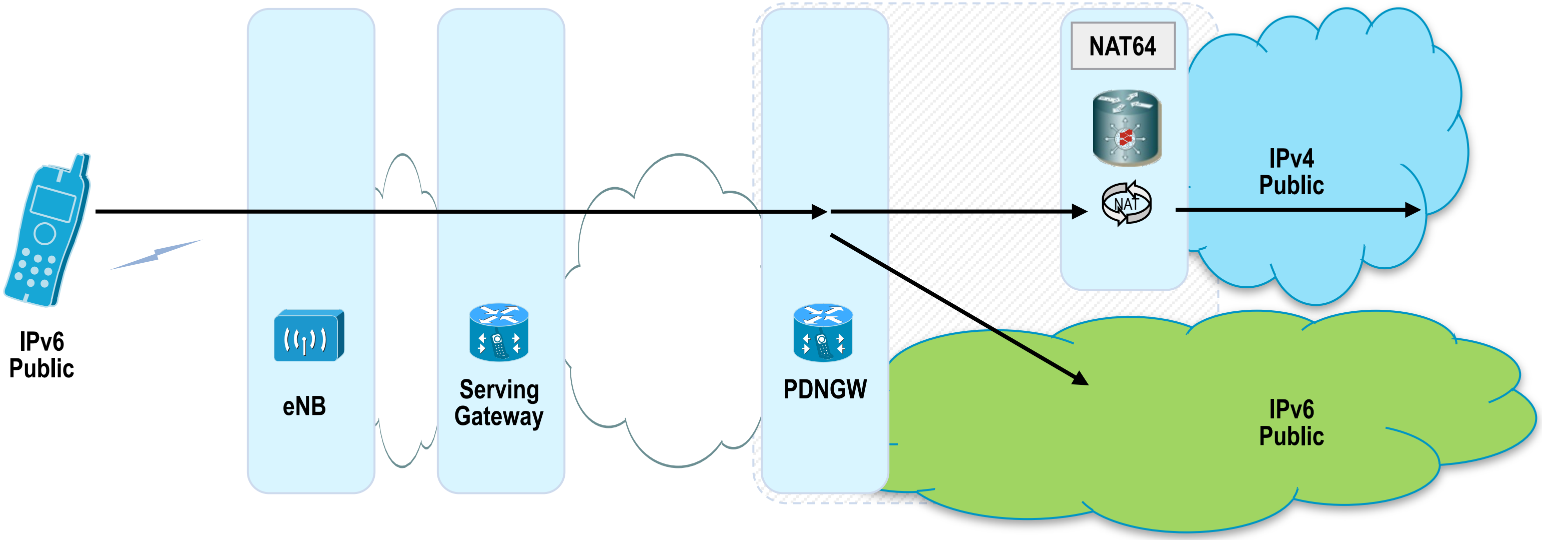
Automatic Tunnel Configuration Example



IPv6 Translation
NAT64

IPv6 and NAT64

- NAT64 technology is required in cases where there are IPv6 *only* end-points that need to communicate with IPv4 *only* end-points.
- NAT64 represents translating from IPv6 to IPv4.



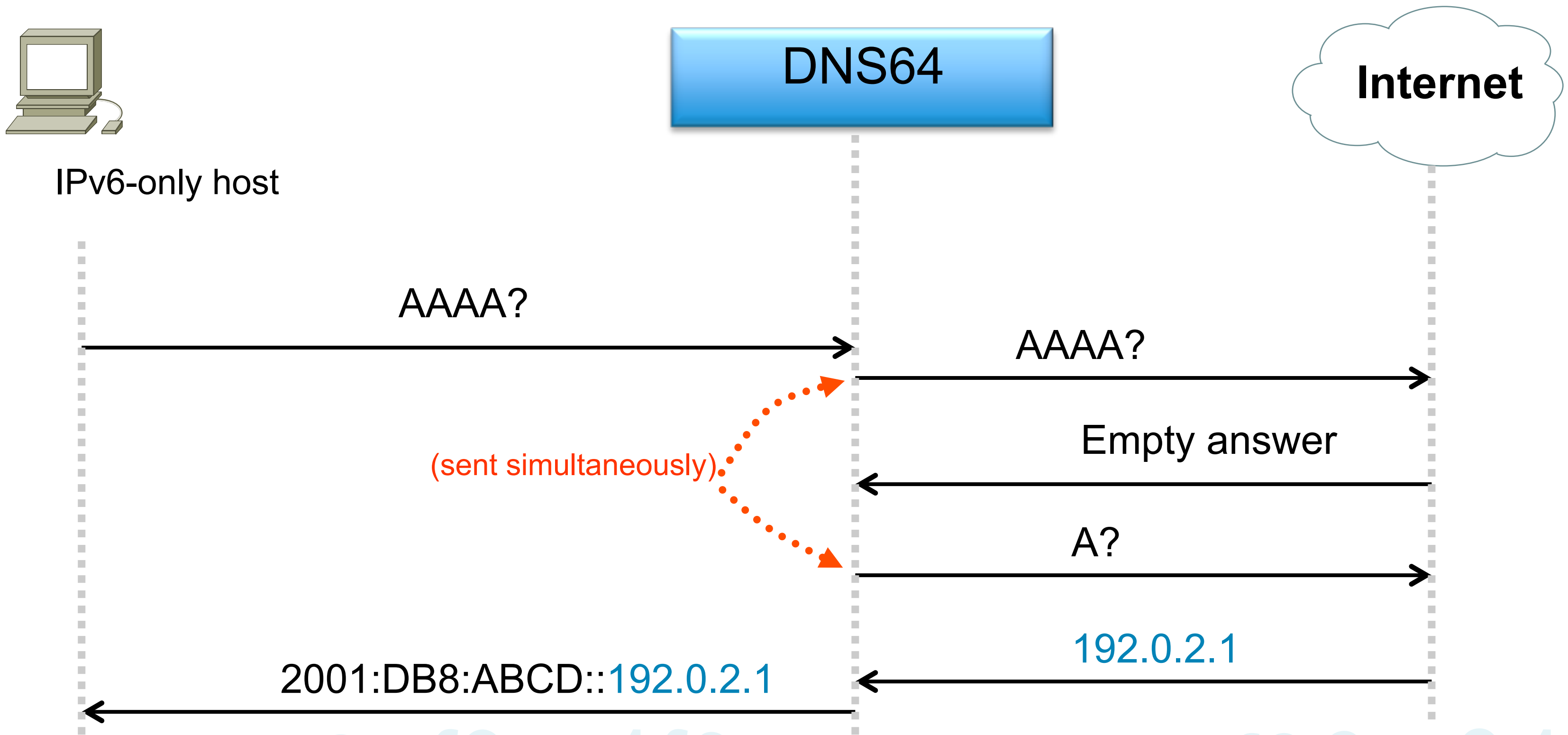
- NAT64:= "stateful" or "stateless" v6 to v4 translation

NAT64 Translation Framework Terminology

- Stateful
  - Each flow creates state in the translator. Supports only IPv6 host initiated communication
  - Amount of state based on O(of translations)
  - N:1 mappings (like NAPT with NAT44) (1:1 Mappings are also of course possible)
- Stateless
  - Flow DOES NOT create any state in the translator
  - Algorithmic operation performed on packet headers that carry embedded public IPv4 addressing
  - 1:1 mappings (one IPv4 address used for each translation to an IPv6 host). Recent proposal allows for semi-stateless translation
  - For internet access public IPv4 address pool is required for each IPv6 host.
  - Supports both IPv6 and IPv4 host initiated communication

DNS64

- Required when using NAT64 with IPv6-only end-hosts.
- Synthesizes AAAA records when not present
  - With IPv6 prefix of NAT64 translator

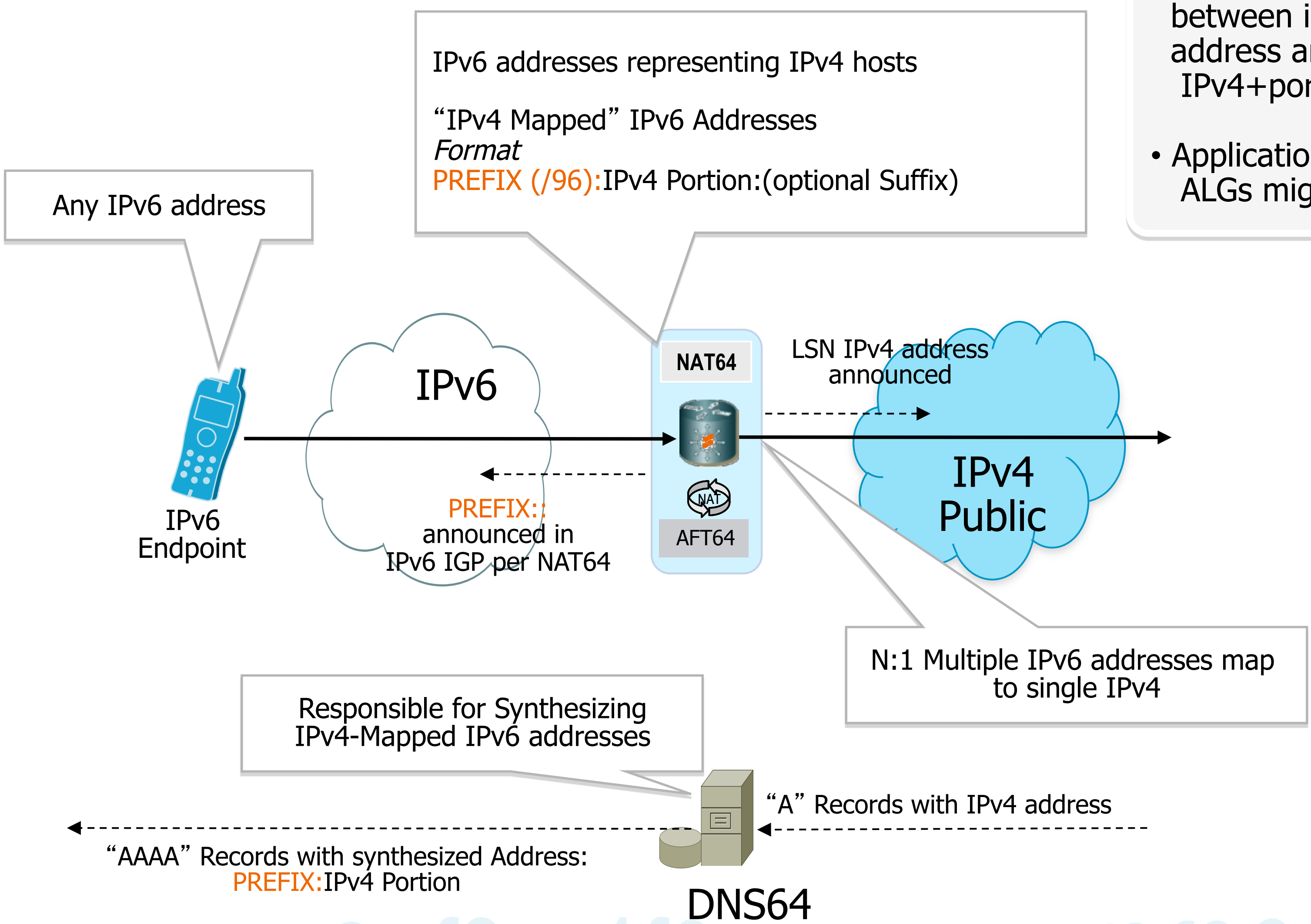


2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

AFT64 Stateful Translators

Stateful AFT64

- AFT keeps binding state between inner IPv6 address and outer IPv4+port (full-cone)
- Application dependent, ALGs might be required*



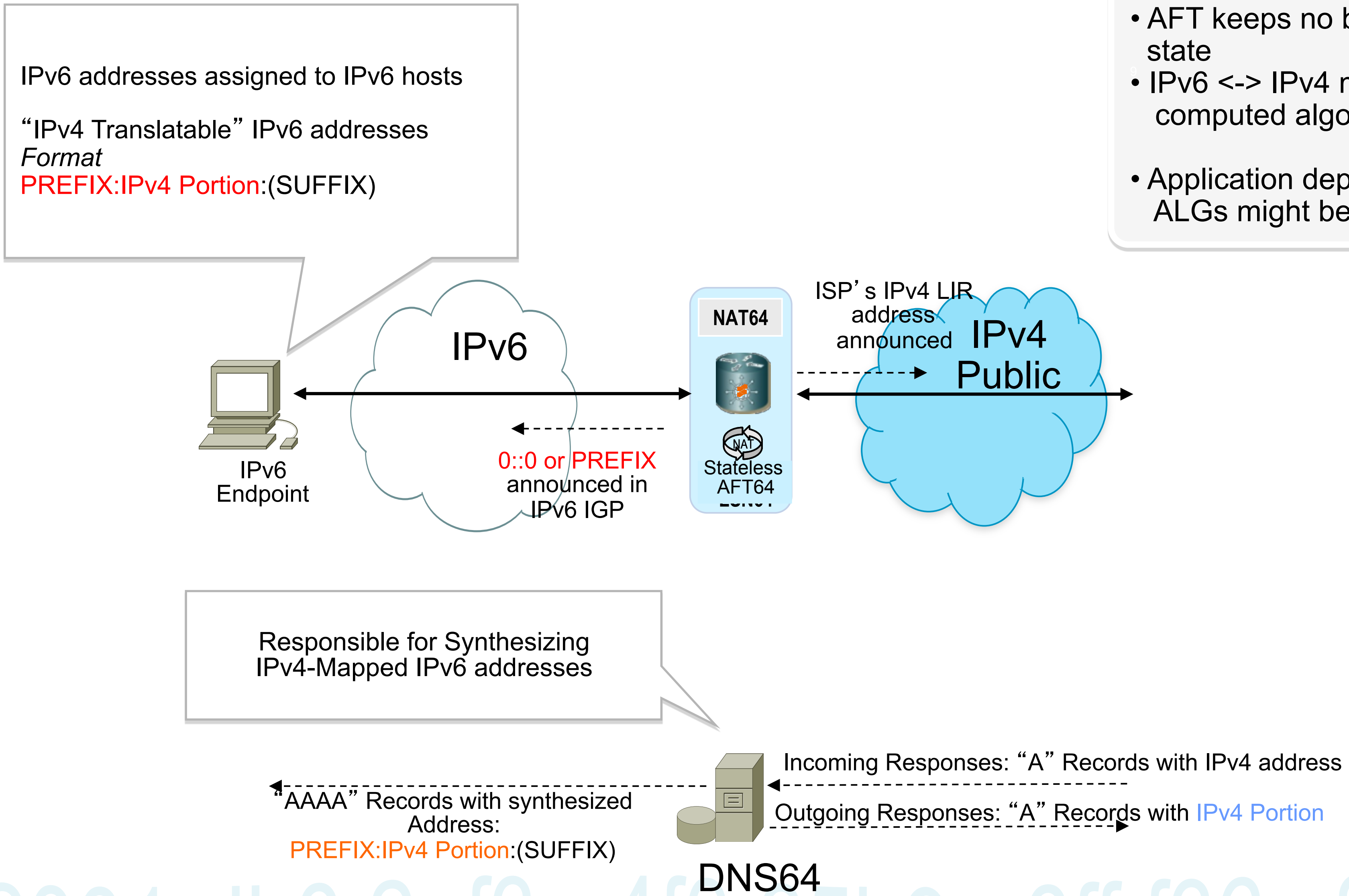
*Note: ALGs for NAT64 and NAT44 not necessarily the same (think FTP)

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

AFT64 Stateless Translators

Stateless AFT64

- AFT keeps no binding state
- IPv6 <-> IPv4 mapping computed algorithmically
- Application dependent, ALGs might be required*



*Note: ALGs for NAT64 and NAT44 not necessarily the same (think FTP)

IPv6 Security

Is IPv6 more secure than IPv4 ?

Reconnaissance in IPv6
Subnet Size Difference

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

  10 Mpps = more than 58 000 years
- NMAP doesn't even support ping sweeps on IPv6 networks
- reconnaissance attacks will NOT go away in an IPv6 environment, rather the tactics will be modified
- passive techniques such as DNS name server resolution, to identify victim networks for more targeted exploitation
- Neighbour discovery-based attacks will also replace counterparts on IPv4 such as ARP spoofing

18,446,744,073,709,551,616
addresses
/
10,000,000 pps
=
1,844,674,407,370 seconds
=
21,350,398 days
=
58,494 years

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Reconnaissance in IPv6

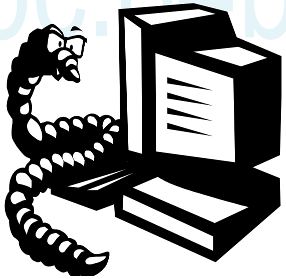
- Public servers will still need to be DNS reachable
  - ⇒ More information collected by Google...
- Increased deployment/reliance on dynamic DNS
  - ⇒ More information will be in DNS
- Using peer-to-peer clients gives IPv6 addresses of peers
- Administrators may adopt easy-to-remember addresses (::10,::20,::F00D, ::C5C0 or simply IPv4 last octet for dual stack)
- By compromising hosts in a network, an attacker can learn new addresses to scan
- Transition techniques (see further) derive IPv6 address from IPv4 address
  - ⇒ Can scan again

Scanning Made Bad for CPU

- Potential router CPU attacks if aggressive scanning
  - Router will do Neighbor Discovery... And waste CPU and memory
  - Built-in rate limiter but no option to tune it
- Using a /64 on point-to-point links => a lot of addresses to scan!
  - Using /127 could help (RFC 6164)
- Using infrastructure ACL prevents this scanning
  - iACL: edge ACL denying packets addressed to your routers
  - Easy with IPv6 because new addressing scheme can be done

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Viruses and Worms in IPv6



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

  IPv4: reliance on network scanning

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

Worm developers will adapt to IPv6

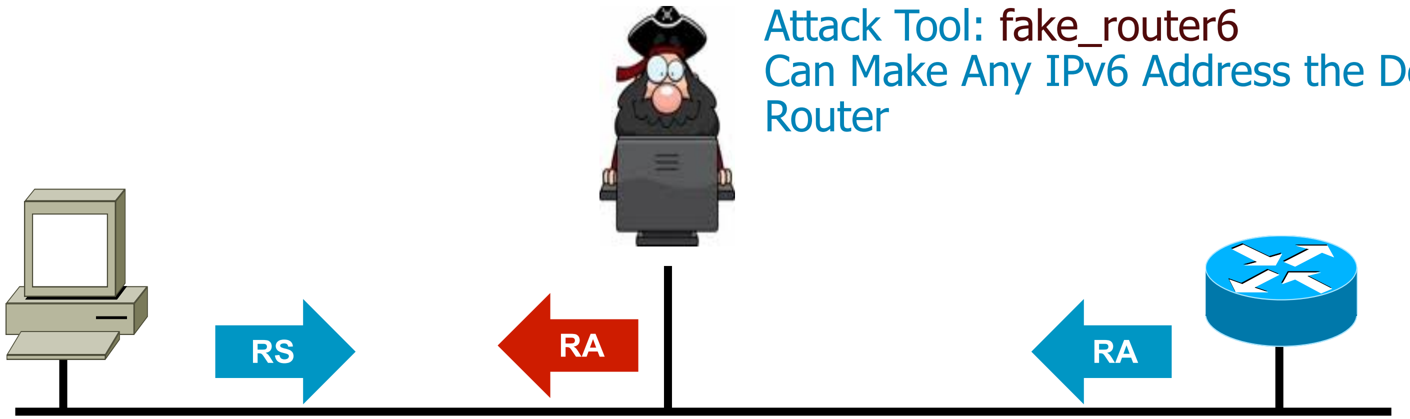
IPv4 best practices around worm detection and mitigation remain valid

Neighbor Discovery Issue#1
Stateless Autoconfiguration

Router Solicitations Are Sent by Booting Nodes to Request Router Advertisements for Stateless Address Auto-Configuring

RA/RS w/o Any Authentication Gives Exactly Same Level of Security as ARP for IPv4 (None)

Attack Tool: fake_router6
Can Make Any IPv6 Address the Default Router



Router Solicitation	
ICMP Type	133
IPv6 Source	A Link Local (FE80::1)
IPv6 Destination	All Routers Multicast (FF02::2)
Query	Please send RA

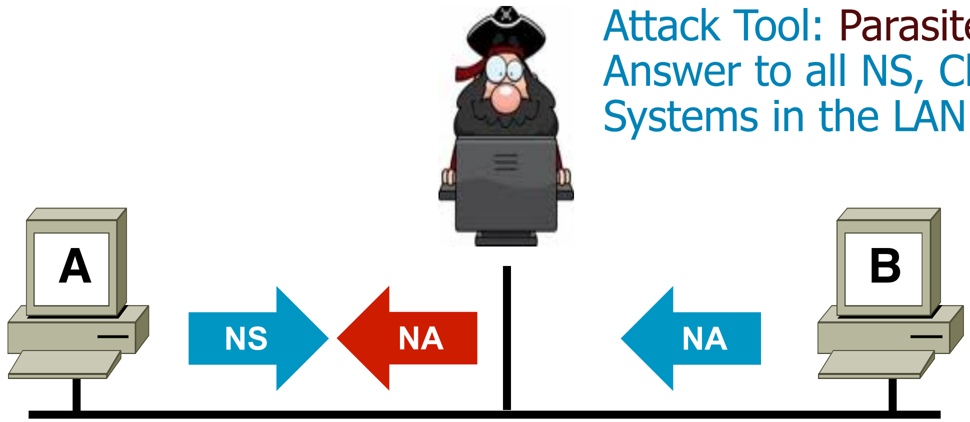
Router Advertisement	
ICMP Type	134
IPv6 Source	A Link Local (FE80::2)
IPv6 Destination	All Nodes Multicast (FF02::1)
Data	Options, subnet prefix, lifetime, autoconfig flag

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Neighbor Discovery Issue#2
Neighbor Solicitation

No Security Mechanisms Built into Discovery Protocol therefore very similar to ARP

Attack Tool: Parasite6
Answer to all NS, Claiming to Be All Systems in the LAN...



Neighbour Solicitation	
ICMP Type	135
IPv6 Source	A Unicast
IPv6 Destination	B Solicited Node Multicast
Data	FE80:: address of A
Query	What is B link layer address?

Neighbour Advertisement	
ICMP Type	136
IPv6 Source	B Unicast
IPv6 Destination	A Unicast
Data	FE80:: address of B

ARP Spoofing is now NDP Spoofing:
Mitigation

- **SEMI-BAD NEWS**: nothing yet like dynamic ARP inspection for IPv6
  - First phase (Port ACL & RA Guard) have been available since September 2010
  - http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-first_hop_security.html
- **GOOD NEWS**: Secure Neighbor Discovery
  - SEND = NDP + crypto
  - IOS 12.4(24)T
  - But not in Windows Vista, 2008 and 7
  - Crypto means slower...
- More **GOOD NEWS**:
  - Private VLAN works with IPv6
  - Port security works with IPv6
  - 801.x works with IPv6

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Secure Neighbor Discovery: Caveats

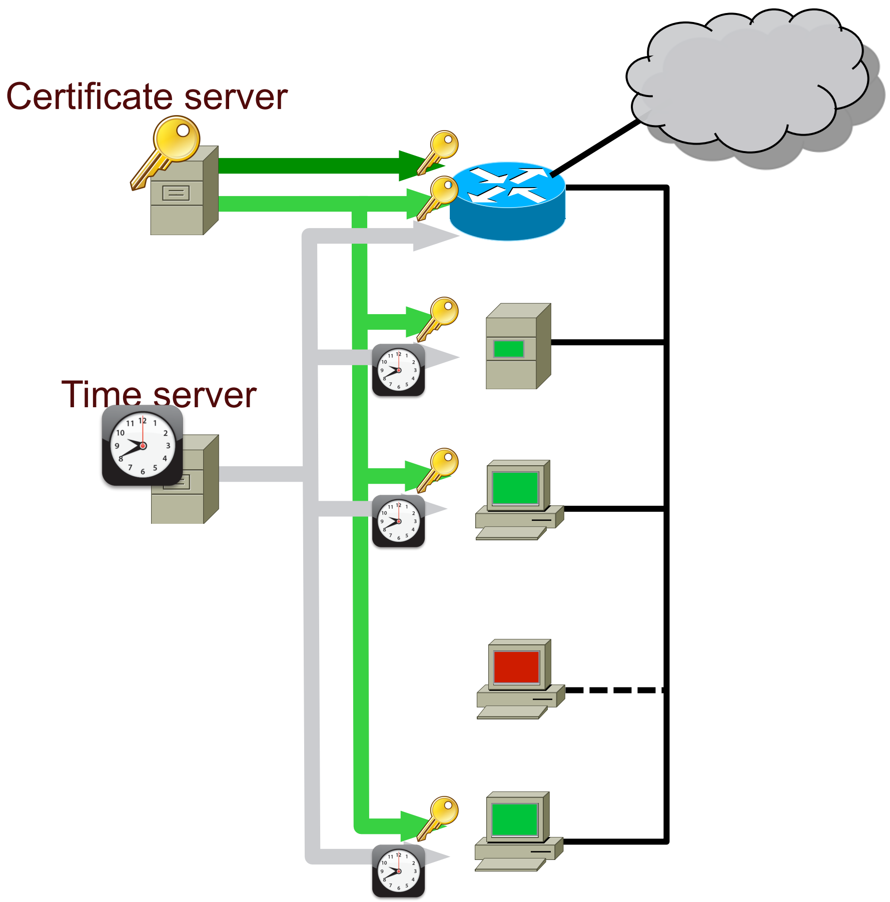
- Private/public key pair on all devices for CGA
- Overhead introduced
  - Routers have to do many public/private key calculation (some may be done in advance of use)
    - => Potential DoS target
  - Routers need to keep more state
- Available:
  - Unix (DoCoMo)
  - Cisco IOS 12.4(24)T
- Microsoft:
  - no support in Vista, Windows 2008 and Windows7

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Securing Link Operations:
on Nodes?

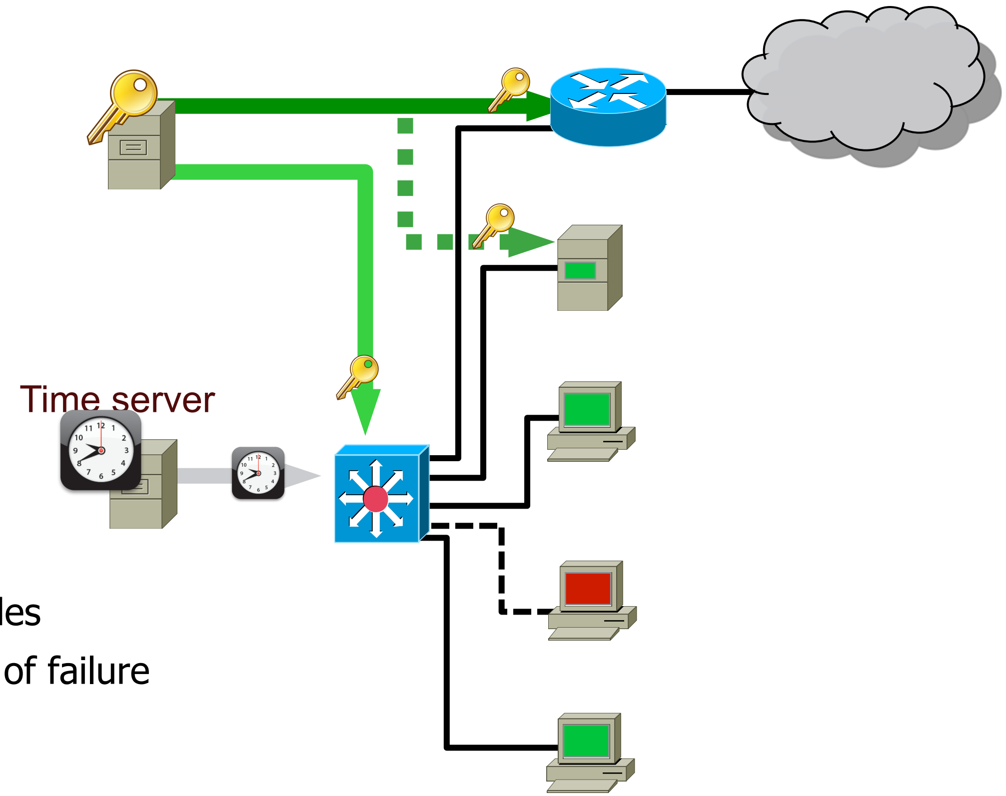
- **Advantages**
  - No central administration, no central operation
  - No bottleneck, no single-point of failure
  - Intrinsic part of the link-operations
  - Efficient for threats coming from the link

- **Disadvantages**
  - Heavy provisioning of end-nodes
  - Poor for threats coming from outside the link
  - Bootstrapping issue
  - Complexity spread all over the domain.
  - Transitioning quite painful



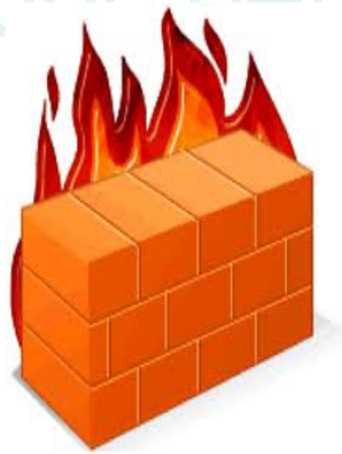
Securing Link Operations:
First Hop Trusted Device

- **Advantages**
  - Central administration, central operation
  - Complexity limited to first hop
  - Transitioning lot easier
  - Efficient for threats coming from the link
  - Efficient for threats coming from outside



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

IOS IPv6 Extended ACL



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

IPv6 ACL Implicit Rules
RFC 4890

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

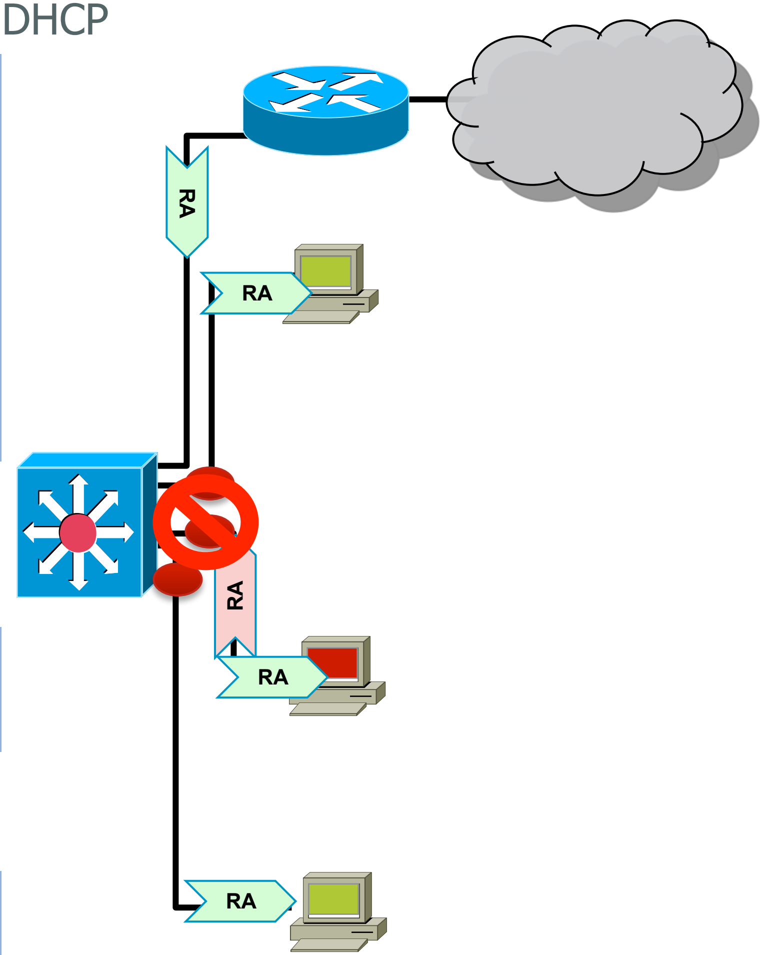
```
permit icmp any any nd-na
permit icmp any any nd-ns
deny ipv6 any any
```

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Rogue RA & DHCP Port ACL

- Switch Based Port ACL to protect against Rogue RAs & DHCP

```
ipv6 access-list ACCESS_PORT
    remark Block all traffic DHCP server -> client
    deny udp any eq 547 any eq 546
    remark Block Router Advertisements
    deny icmp any any router-advertisement
    permit any any

Interface gigabitethernet 1/0/1
    switchport
    ipv6 traffic-filter ACCESS_PORT in
```



- Cat6k and 4k have a system macro for RA Guard

```
interface gigabitethernet 1/0/1
switchport
ipv6 nd raguard
```

- Port ACL replaces Router ACL

```
interface gigabitethernet 1/0/1
switchport
access-group mode prefer port
```

Nexus-7000, Cat 3750 12.2(46)SE, Cat 4500 12.2(54)SG and Cat 6500 12.2(33)SXI4

IPv6 ACL to Protect VTY

- Protect VTY access to devices like you would with IPv4

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

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

- Assess if IPv6 access is required in the management plane.
- Some NMS still IPv4 only
- Low priority change for existing networks

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Control Plane Policing for IPv6
Protecting the Router CPU

- Against DoS with NDP, Hop-by-Hop, Hop Limit Expiration...
- Software routers (ISR, 7200): works with CoPPr (CEF exceptions)

```
policy-map COPPr
 class ICMP6_CLASS
   police 8000
 class OSPF_CLASS
   police 200000
 class class-default
   police 8000
!
control-plane cef-exception
 service-policy input COPPr
```

- Cat 6K & 7600

  IPv6 shares mls rate-limit with IPv4 for NDP & HL expiration

```
mls rate-limit all ttl-failure 1000
mls rate-limit unicast cef glean 1000
```

ICMPv4 vs. ICMPv6

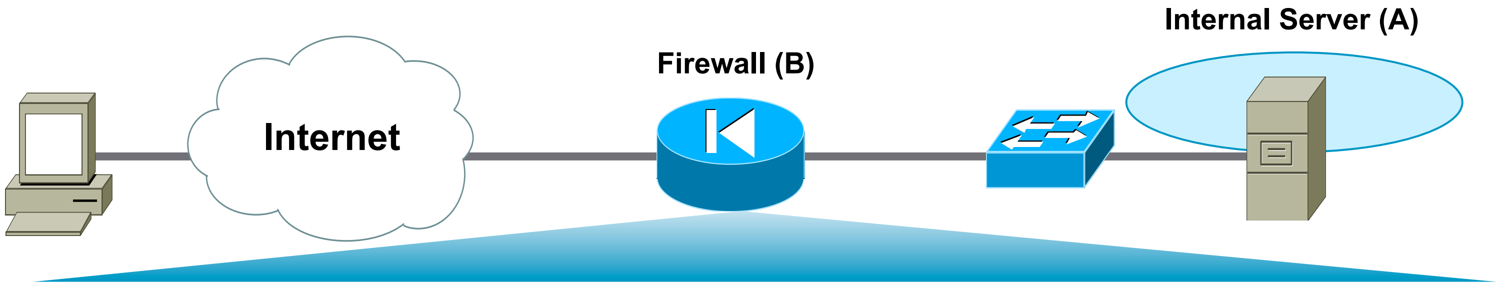
- Significant changes
- More relied upon

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

- ICMP policy on firewalls needs to change to support IPv6

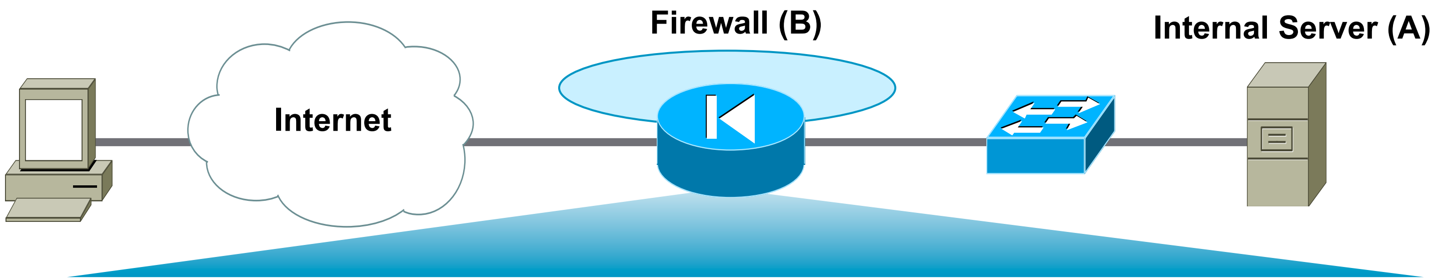
2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Equivalent ICMPv6
RFC 4890: Border Firewall Transit Policy



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

Potential Additional ICMPv6
RFC 4890: Border Firewall Receive Policy



Action	Src	Dst	ICMPv6 Type	ICMPv6 Code	Name
Permit	Any	B	2	0	Packet too Big
Permit	Any	B	4	0	Parameter Problem
Permit	Any	B	130–132	0	Multicast Listener
Permit	Any	B	133/134	0	NS & NA
Deny	Any	Any			

For locally generated traffic

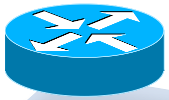
2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Preventing IPv6 Routing Attacks
Protocol Authentication

- BGP, ISIS, EIGRP no change:
  - An MD5 authentication of the routing update
- OSPFv3 has changed and pulled MD5 authentication from the protocol and instead is supposed to rely on transport mode IPSec
- RIPng, PIM also rely on IPSec
- IPv6 routing attack best practices
  - Use traditional authentication mechanisms on BGP and IS-IS
  - Use IPSec to secure protocols such as OSPFv3 and RIPng

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

OSPF Authentication



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

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

IPv6 Attacks with Strong IPv4 Similarities

- Sniffing

  IPv6 is no more or less likely to fall victim to a sniffing attack than IPv4
- Application layer attacks

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

  Rogue devices will be as easy to insert into an IPv6 network as in IPv4
- Man-in-the-Middle Attacks (MITM)

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

  Flooding attacks are identical between IPv4 and IPv6

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

IPv6 Stack Vulnerabilities

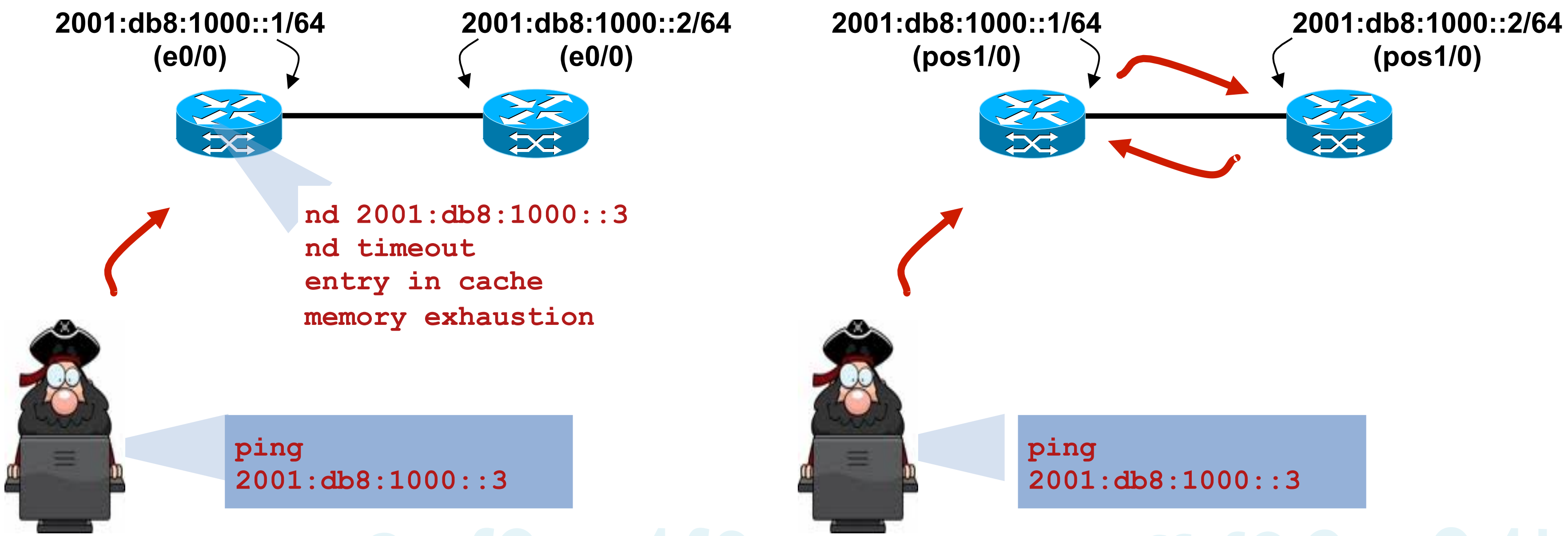
- IPv6 stacks were new and could be buggy
- Some examples

CVE	Date	OS	Issue
CVE-2009-2208	Jun 2009	FreeBSD OpenBSD NetBSD and others	Local users can disable IPv6 without privileges
CVE-2010-1188	Mar 2010	Linux	DoS for socket() manipulation
CVE-2010-4684	Jan 2011	IOS	IPv6 TFTP crashes when debugging
CVE-2008-1576	Jun 2008	Apple Mac OS X	Buffer overflow in Mail over IPv6
CVE-2010-4669	Jan 2011	Microsoft	Flood of forged RA DoS

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

DoS Example
Ping-Pong over Physical Point-to-Point

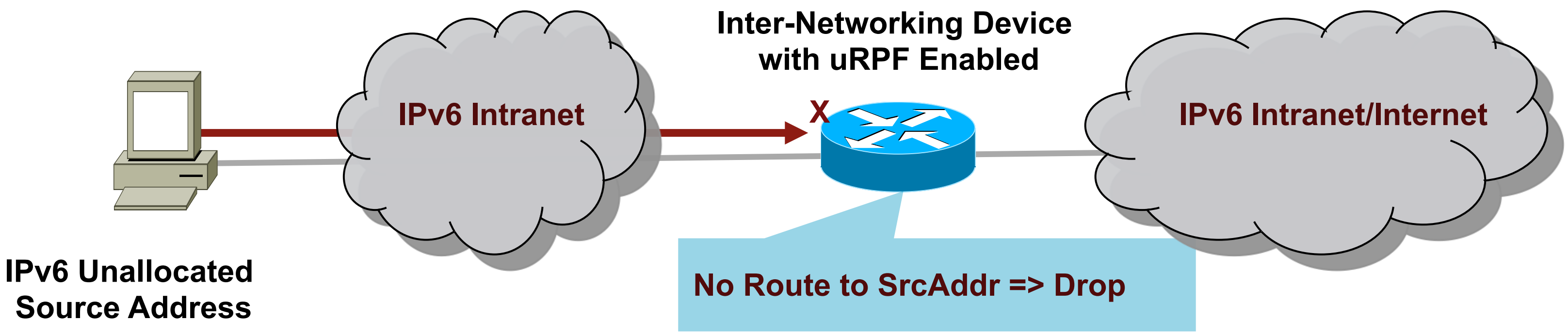
- IOS implements RFC 4443 so this is not a threat
- Neighbour Discovery still exploitable
- Else use /127 on P2P link (see also RFC 3627)
- Same as in IPv4, on real P2P, if not for me then send it on the other side...
  Could produce looping traffic



2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

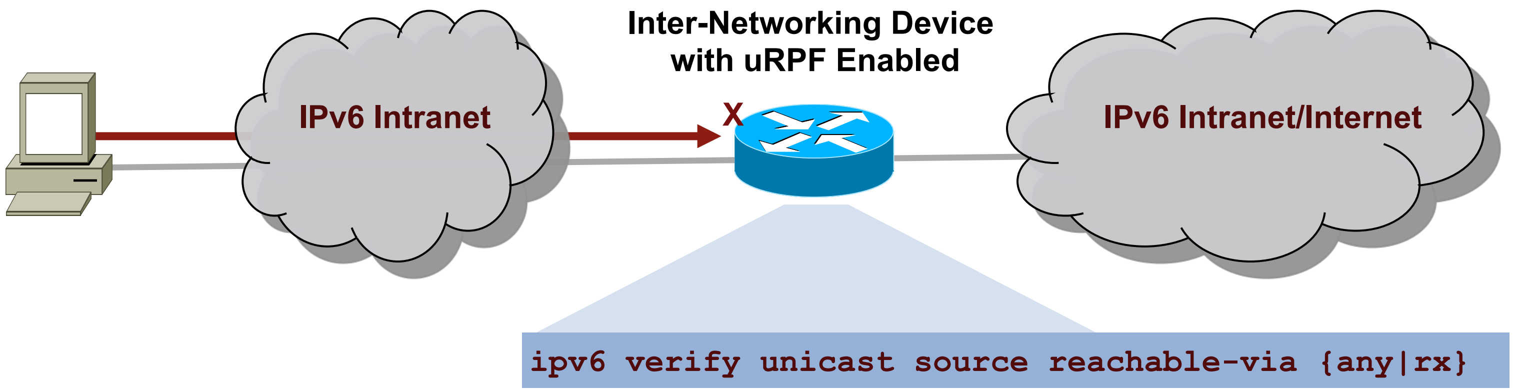
IPv6 Bogon Filtering & Anti-Spoofing

- In IPv4 it is easier to block bogons than to permit non-bogons
- In IPv6, in the beginning when a small amount of top-level aggregation identifiers (TLAs) has been allocated
  - Easier to permit non-bogons
  - Now, more complex: http://www.cymru.com/Bogons/ipv6.txt
- Now IPv6 is in a similar situation as IPv4
  - Same technique = uRPF



IPv6 uRPF and Cisco Devices
The Theory-Practice Gap

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

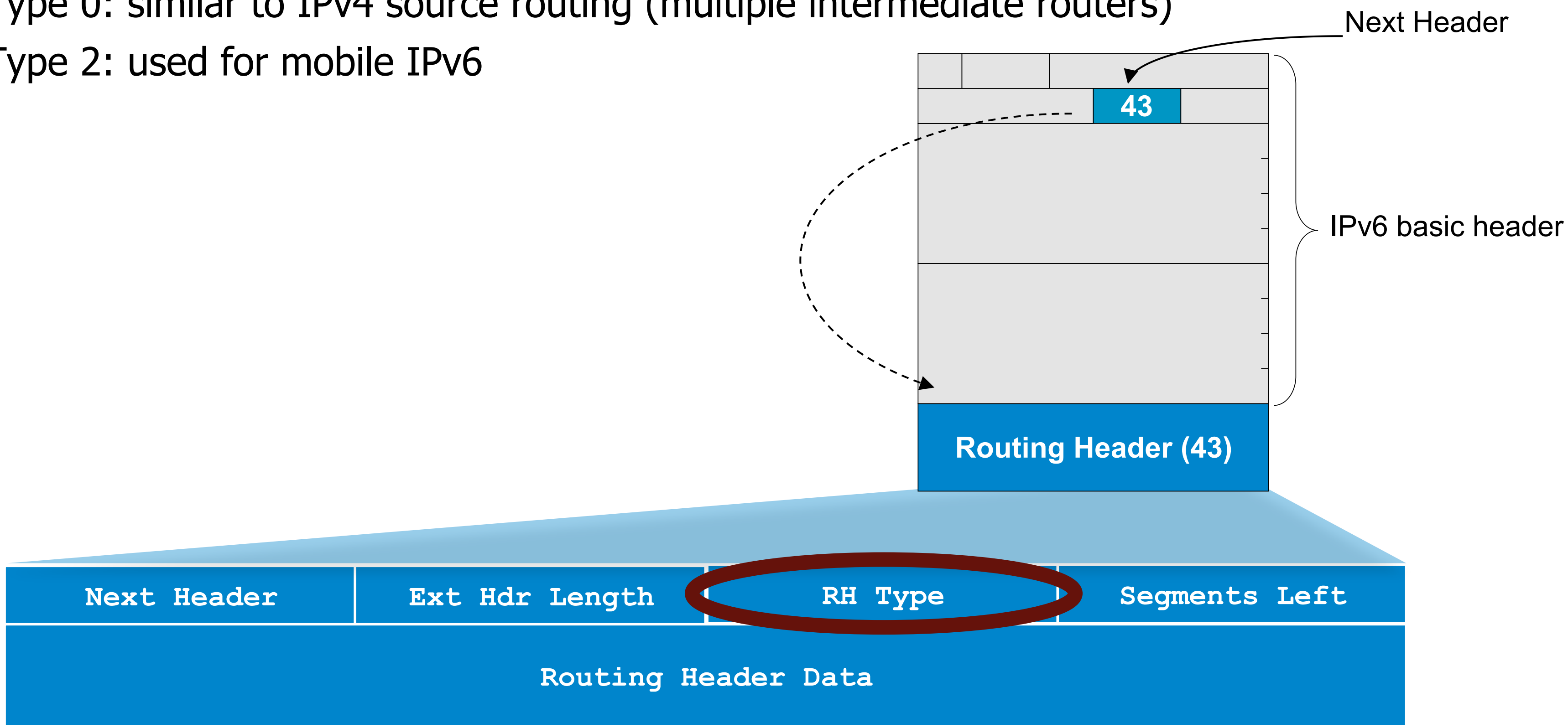


IPv6 Routing Header

- An extension header
- Processed by the listed intermediate routers
- Two types

  Type 0: similar to IPv4 source routing (multiple intermediate routers)

  Type 2: used for mobile IPv6



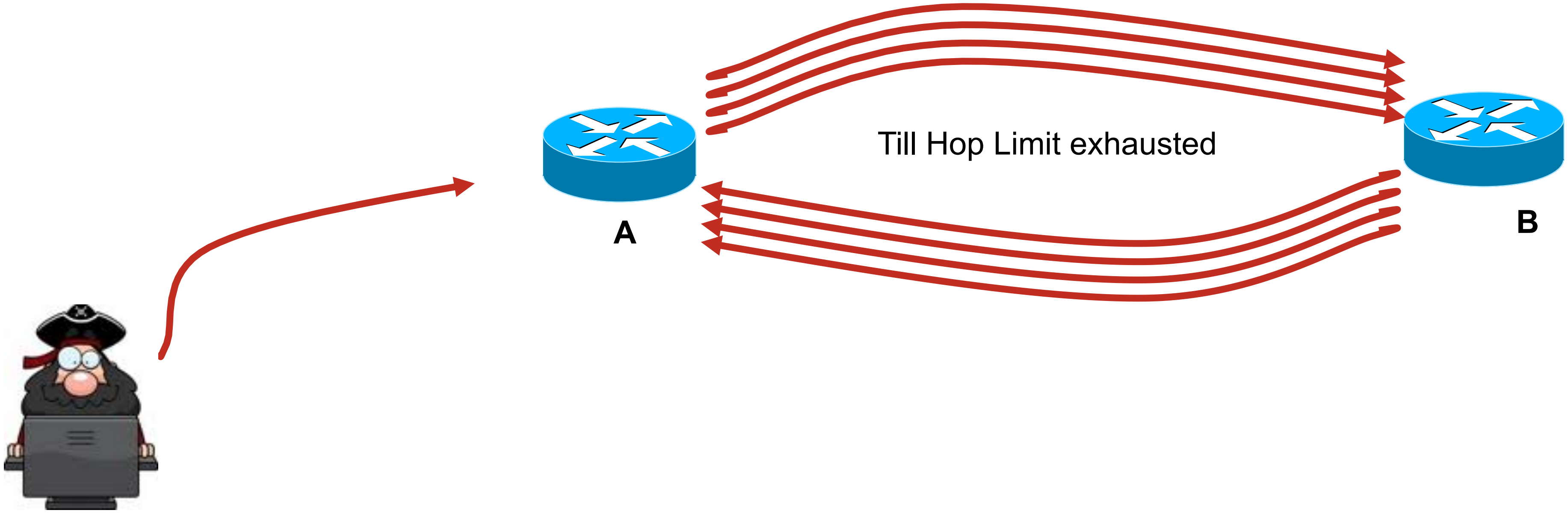
2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Type 0 Routing Header
Issue: Amplification Attack

- What if attacker sends a packet with RH containing

  A -> B -> A -> B -> A -> B -> A -> B -> A ....

- Packet will loop multiple time on the link A-B
- An amplification attack!



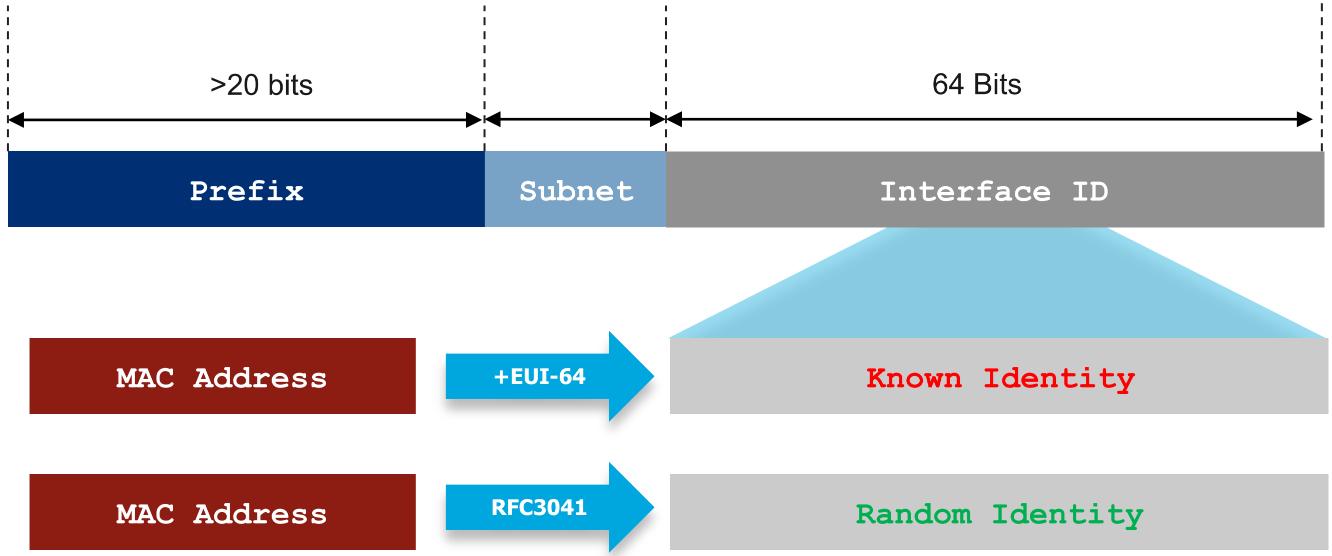
2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Preventing Routing Header Attacks

- Apply same policy for IPv6 as for Ipv4:
  - Block Routing Header type 0
- Prevent processing at the intermediate nodes
  - no ipv6 source-route (in IOS only)
  - Windows, Linux, Mac OS: default setting
- At the edge
  - With an ACL blocking routing header, specifically type 0
- RFC 5095 (Dec 2007) RH0 is deprecated
  - Default IOS changed in 12.4(15)T to ignore and drop RH0
  - No need to configure 'no ipv6 source-route'

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

IPv6 Privacy Extensions (RFC 3041)



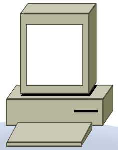
- Temporary addresses for IPv6 host client application, e.g. web browser
  - Inhibit device/user tracking
  - Random 64 bit interface ID, then run Duplicate Address Detection before using it
  - Rate of change based on local policy

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

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Disabling Privacy Extension
Windows XP,2003,Vista,7,2008

- Microsoft Windows
  - Deploy a Group Policy Object (GPO), or
  - Disable with ‘netsh’ CLI

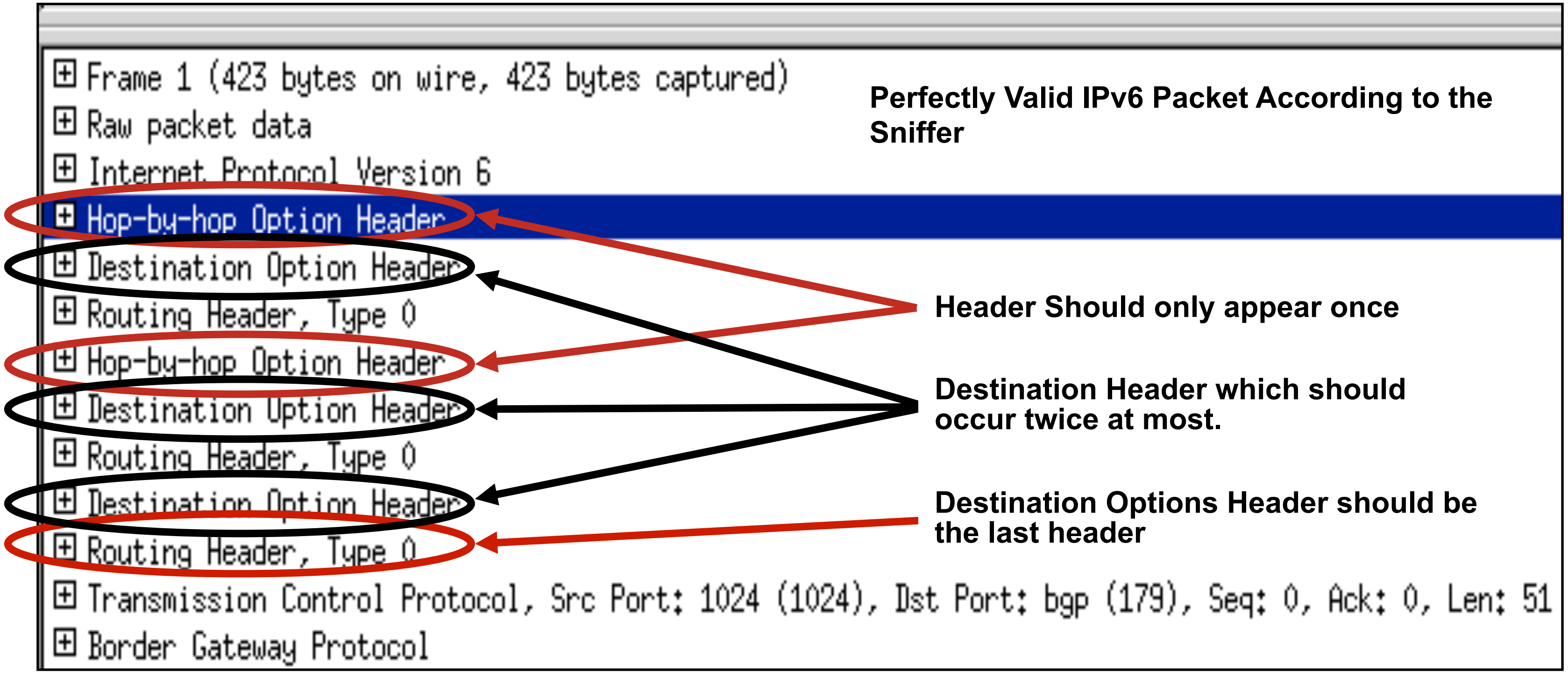


```
netsh interface ipv6 set global randomizeidentifiers=disabled
netsh interface ipv6 set global randomizeidentifiers=disabled
store=persistent
netsh interface ipv6 set privacy state=disabled store=persistent
```

- Alternatively
  - Use DHCP (see later) to a specific pool
  - Ingress filtering allowing only this pool

IPv6 Header Manipulation

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



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

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Parsing the Extension Header Chain

- Finding the layer 4 information is not trivial in IPv6
  - Skip all known extension header
  - Until either known layer 4 header found meaning **SUCCESS, or**
  - until unknown Extension Header or Layer 4 Header is found meaning **FAILURE**

IPv6 hdr	HopByHop	Routing	AH	TCP	Data
IPv6 hdr	HopByHop	Routing	AH	Unknown L4	???
IPv6 hdr	HopByHop	Unknown EH	???	???	???

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

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

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

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

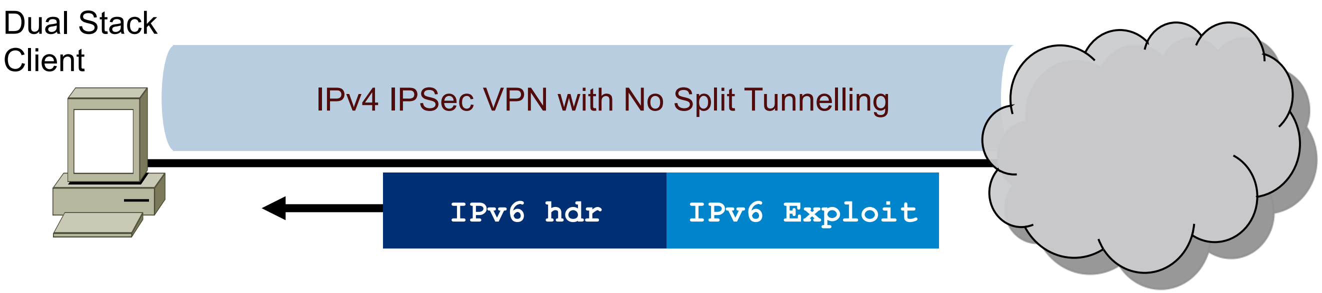
IPv4 to IPv6 Transition Challenges

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

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Dual Stack Host Considerations

- Host security on a dual-stack device
  - Applications can be subject to attack on both IPv6 and IPv4
  - **Fate sharing**: as secure as the least secure stack...
- Host security controls should block and inspect traffic from both IP versions
  - Host intrusion prevention, personal firewalls, VPN clients, etc.

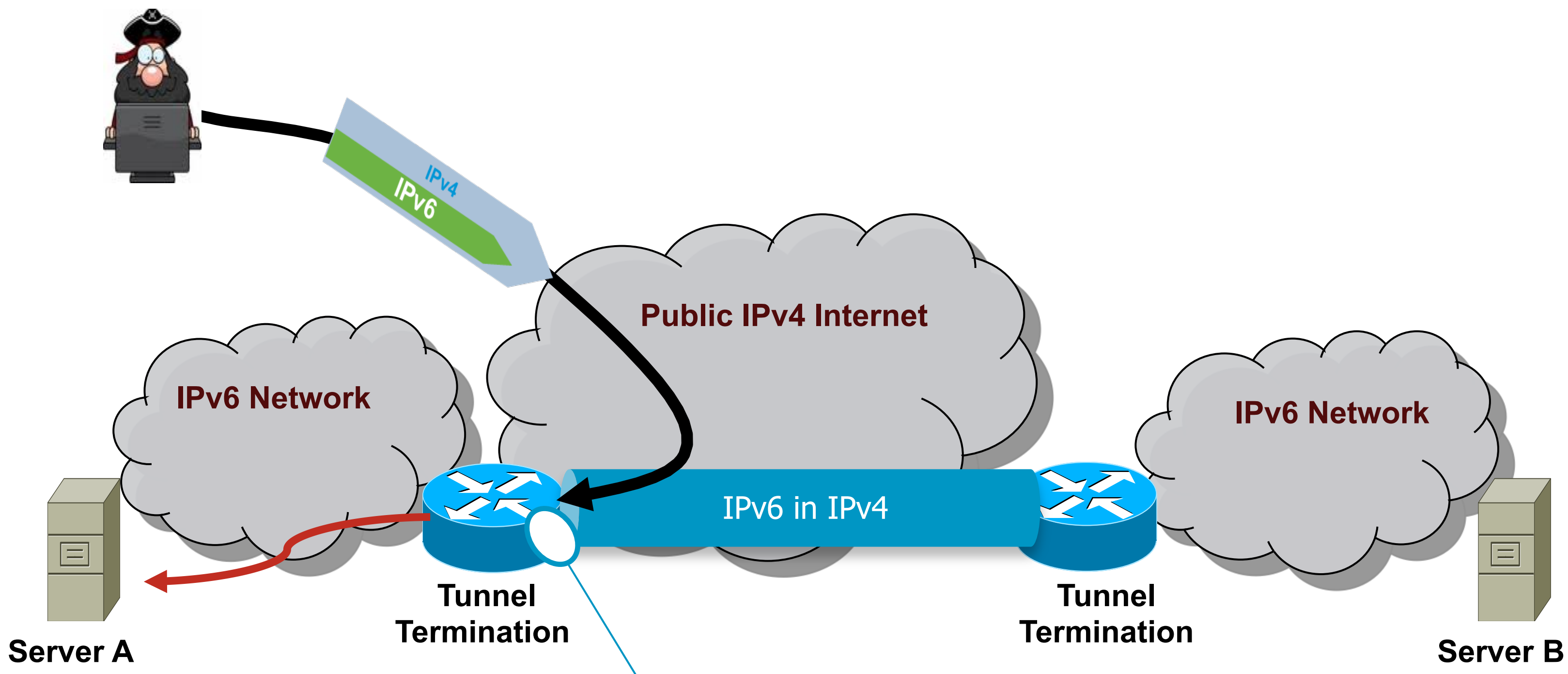


- Does the IPsec Client Stop an Inbound IPv6 Exploit?

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

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

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



IPv6 ACLs Are Ineffective Since IPv4 & IPv6 Is Spoofed

Tunnel Termination Forwards the Inner IPv6 Packet

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

ASA Firewall IPv6 Support

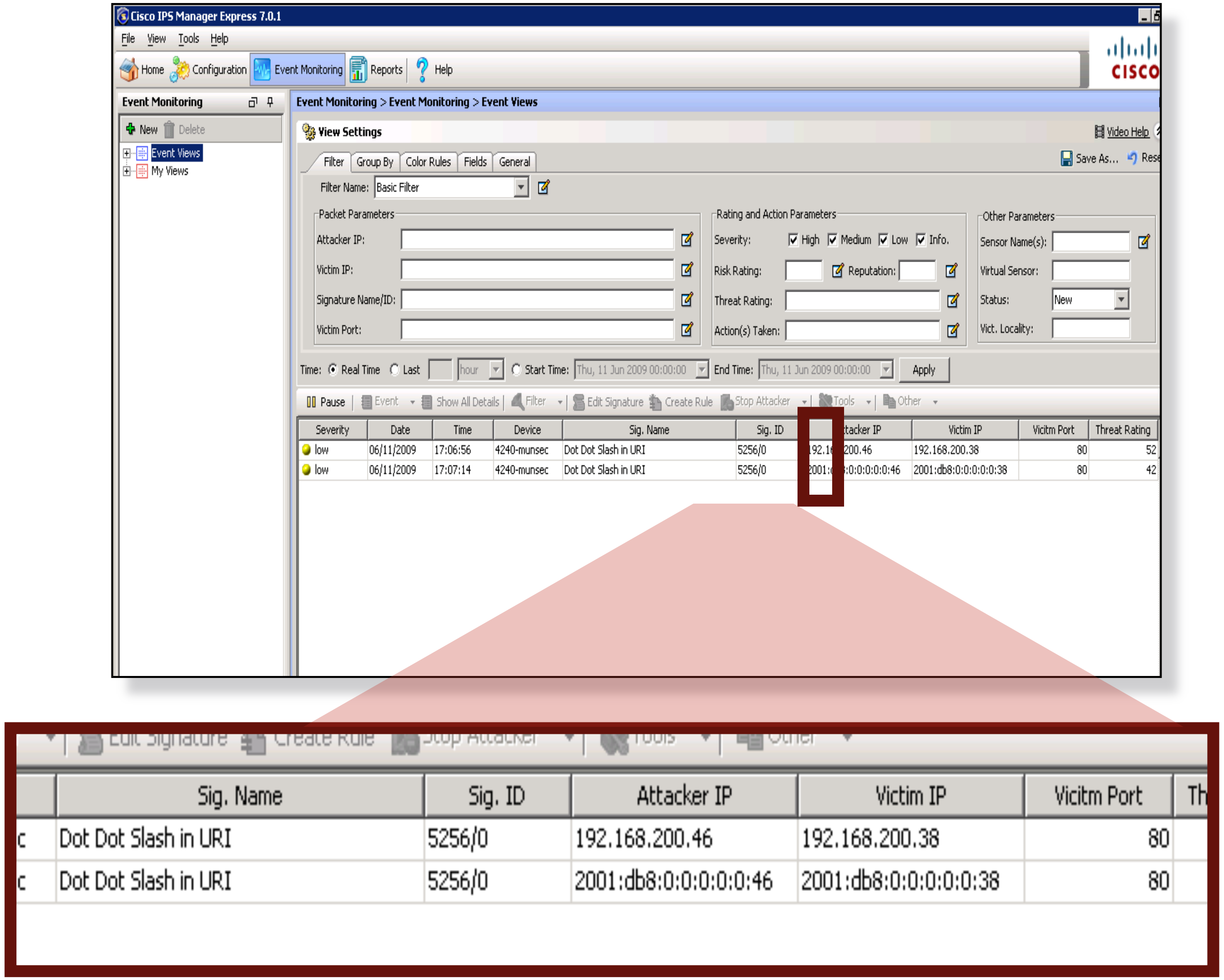
- Since version 7.0 (April 2005)
- Dual-stack, IPv6 only, IPv4 only
- Extended IP ACL with stateful inspection
- Application awareness
  - HTTP, FTP, telnet, SMTP, TCP, SSH, UDP
- uRPF and v6 Frag guard
- IPv6 header security checks
  - Always block routing-header (type 0 and 2)
  - Selective Extension Header blocking (ASA 8.4.2)
- Management access via IPv6
  - Telnet, SSH, HTTPS
- ASDM support (ASA 8.2)
- Routed & transparent mode (ASA 8.2)
- Fail-over support (ASA 8.2.2)

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

Dual-Stack IPS Engines

Service HTTP



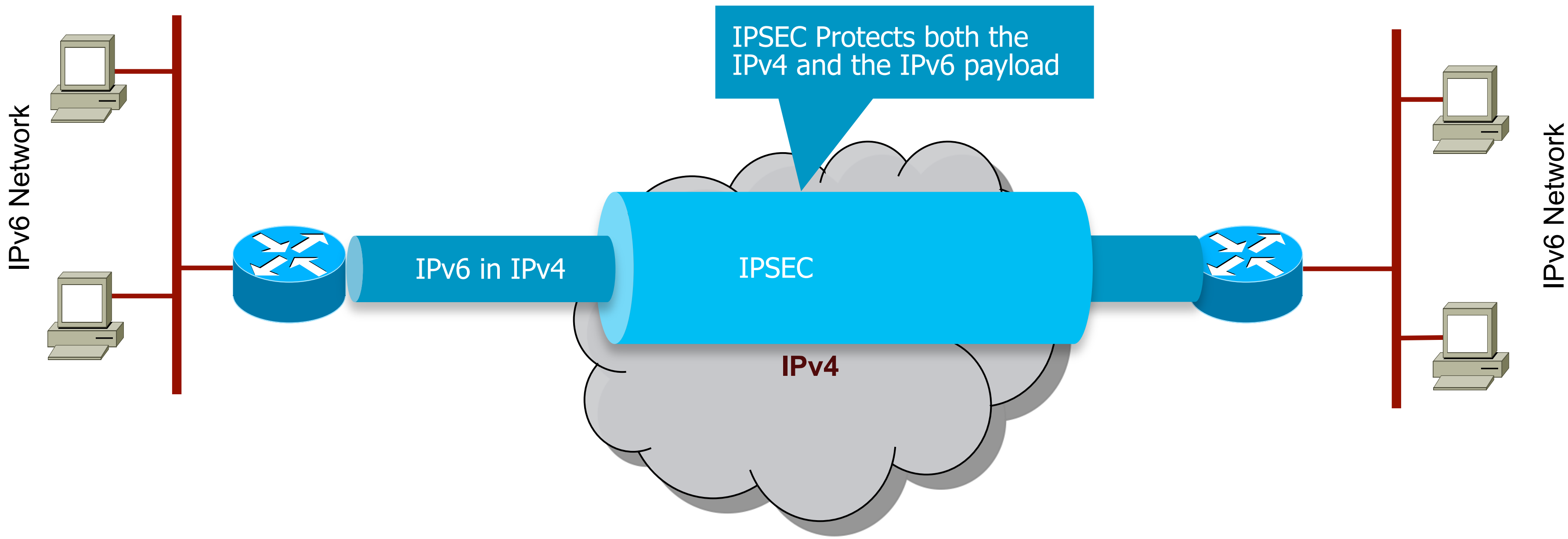
2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

IPv6 for Remote Devices

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

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

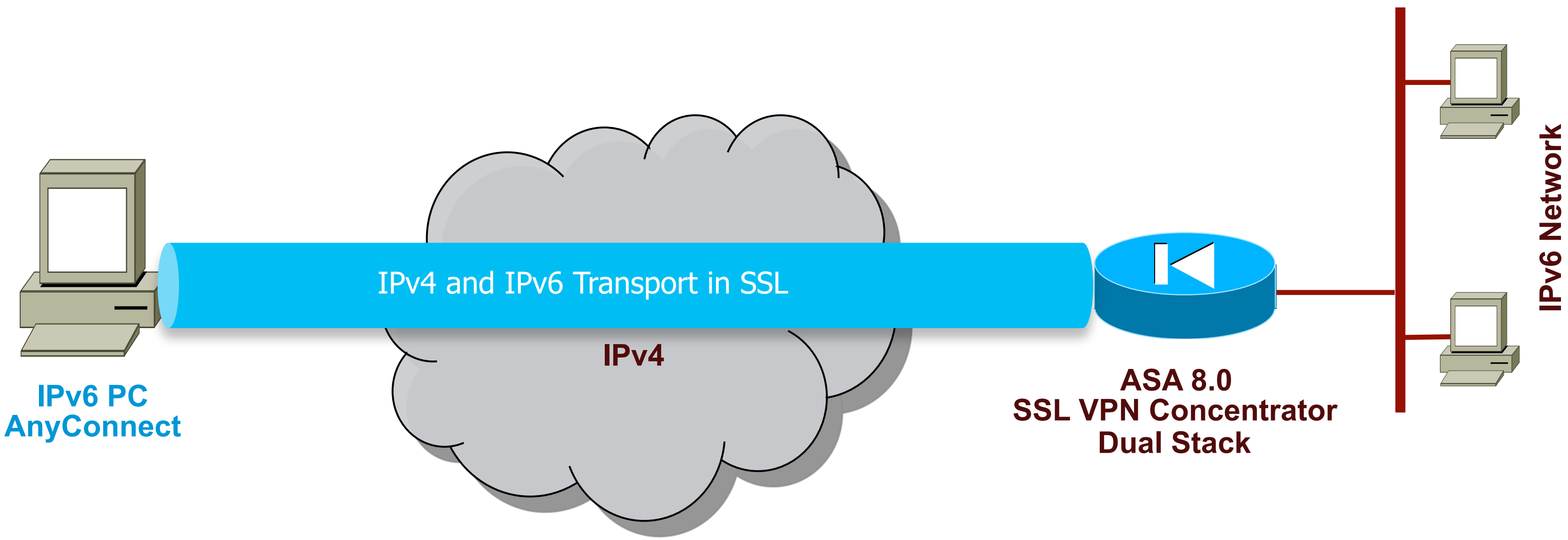
Secure Site to Site IPv6 Traffic over IPv4 Public Network with GRE IPsec



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

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

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



Key Take Away

- So, nothing really new in IPv6
  - Reconnaissance: address enumeration replaced by DNS enumeration
  - Spoofing & bogons: uRPF is our IP-agnostic friend
  - NDP spoofing: RA guard and more feature coming
  - ICMPv6 firewalls need to change policy to allow NDP
  - Extension headers: firewall & ACL can process them
  - Amplification attacks by multicast mostly impossible
  - Potential loops between tunnel endpoints: ACL must be used
- Lack of operation experience may hinder security for a while: **training is required**
- Security enforcement is possible
  - Control your IPv6 traffic as you do for IPv4
- Leverage IPsec to secure IPv6 when suitable

Review Questions

- Q1: Are there IPv6 Unique security threats ?
  Yes, IPv6 introduces new Layer 2 mechanisms (NS/ND & RS/RA) that can be exploited
- Q2: Is network address scanning viable in IPv6 ?
  No, scanning a /64 at 10Mpps would take 58,000 years
- Q3: What are some of the protection mechanisms available in IPv6 ?
  IPv6 Access Lists
  RA Guard
  IPv6 Firewall Policy
  Control Plane Policing

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0

2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0
2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0
2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0
2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0
2001:db8:2ef3:a4f0:65b9:e8ff:f36c:84b0