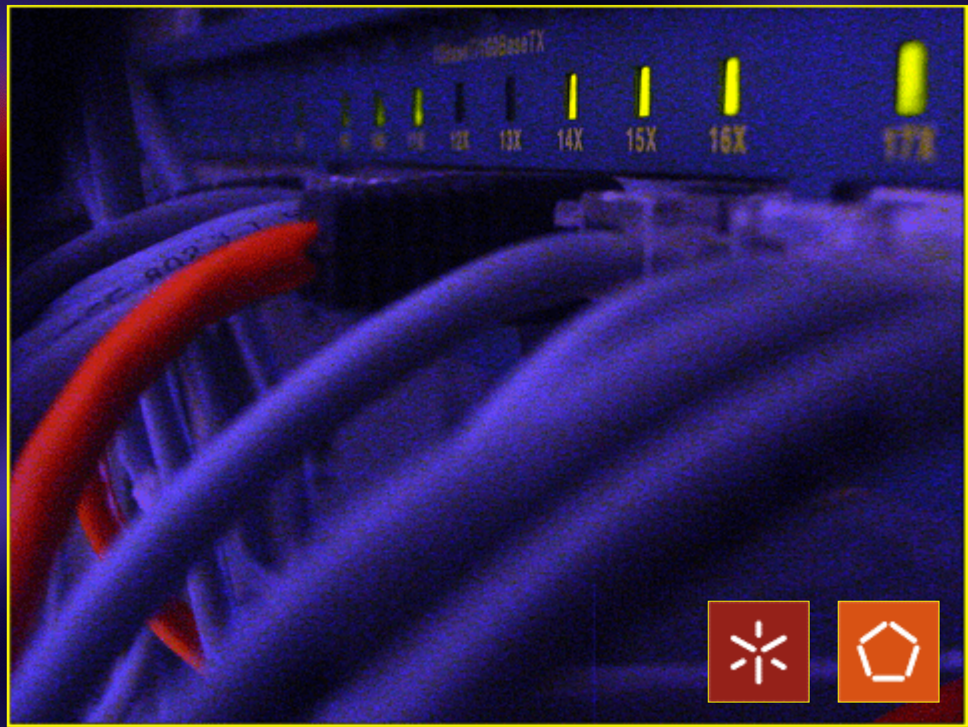
Advanced Computer Networks - ACN

MAP-I 2010/2011



Alexandre Santos
COMPUTER COMMUNICATIONS GROUP
INFORMATICS DEPARTAMENT
ENGiNEERING SCHOOL   UNIVERSITY OF MINHO

MATERIAL SOURCES:

- IPv6 Tutorial, 1st Pacific IPv6 Summit, APNIC, 2007
- IPv6 Tutorial, SANOG V, Cisco Systems, 2005
- IPV6 Tutorial, VIAGENIE, 2010

- IPv6 in Canada: Final Report and Recommendations of the ISACC IPv6 Task Group (IITG), IITG Final Report to ISACC, March 2010

  http://www.viagenie.ca/publications/2010-05-13-isacc-ipv6-task-group-report.pdf

- Mobile Internet kick starts IPv6, Zhang Chi, Communicate, 51, Sep 2009

  http://www.huawei.com/file/download.do?f=6434

Why IPv6 ?

Problems with IPv4

- IPv4 has been designed early in the 70s
- Many « add-ons» to the protocol :
  - Mobileip
  - QoS
  - Security (IPsec)
  - Others
- Using one « add-ons » -> easy
- Using two at the same time -> difficult
- Using three or more -> acrobatic !!!!

Why IPv6 ?

Problems with IPv4

- During the 80s, addresses delegation without optimisation and without aggregation

Possible solution : IP renumbering and unused address space redistribution

Consequences :

- Large routing table on the backbone
- Unthinkable for some sites

Why IPv6 ?

IPv4 address shortage (current situation)

- Some ISP in these countries are providing private addresses to their clients (Suedish ISP using NAT)
- Internet users move from PPP connectivity to xDSL/cable modem (ratio users by IP address is changing from 10:1 to 1:1)
- ISP are delegating only few address space to their corporate client s
- Temporary solution --> NAT (but unfortunatly permanent)

Why IPv6 ?

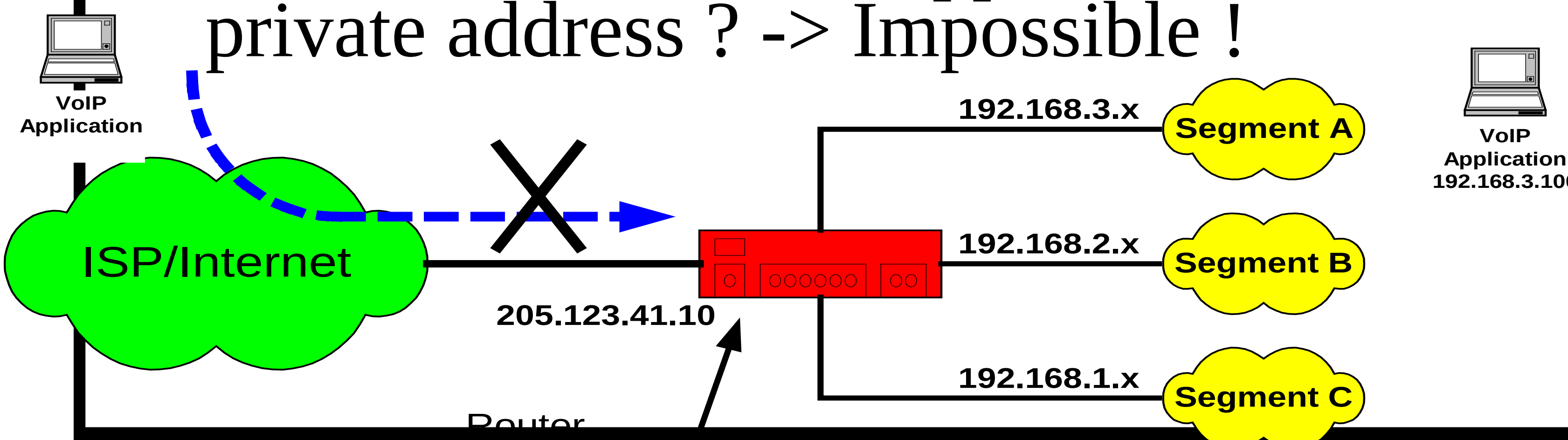
IPv4 address shortage in the future

- Internet growth in some regions :
  - Asia (2.5 billions people)
  - Eastern Europe (250 millions)
  - Africa (800 millions)
  - South and Central America (500 millions)
- Growth of the applications that need IP addresses globally scoped, unique and routable (VoIP, videoconferencing, games)

Why IPv6 ?

NAT « hinders » Internet applications deployment

- Unidirectionnal concept (from Intranets to Internet)
- How to reach a VoIP application with a private address ? -> Impossible !

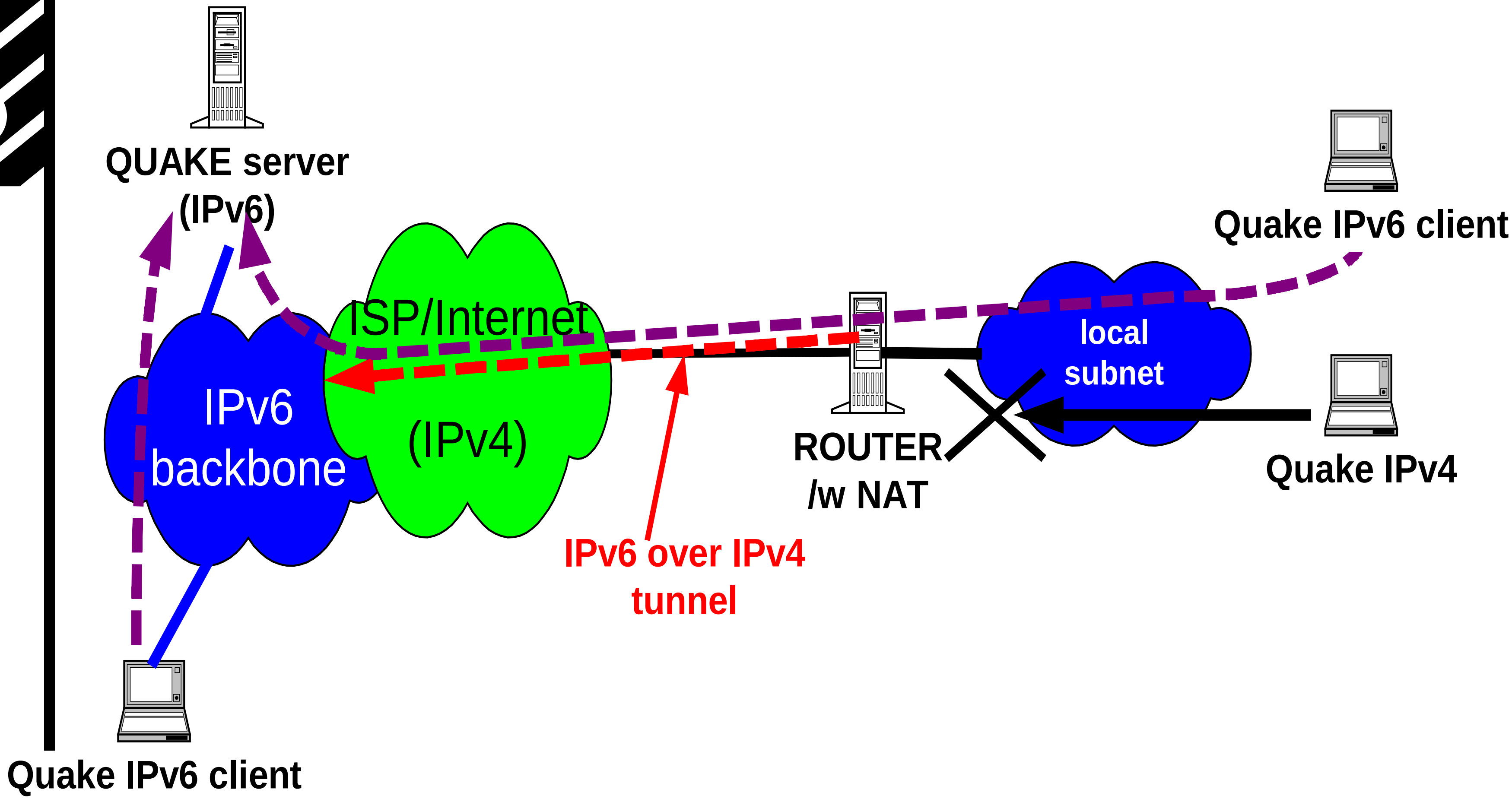


Why IPv6 ?

NAT « hinders » Internet applications deployment

- Comunication, security and game applications need bidirectionnel support
  - VoIP (RTP/RTCP)
  - Videoconferencing (RTP/RTCP)
  - IPsec
  - Network game (Quake multiplayer)
- RFC 2775 about *Internet Transparency* by Brian Carpenter

Home gaming IPv6 setup



Why IPv6 ?

NAT « hinders » Internet applications deployment

- Several protocols don ’t pass throught NAT
  - IPsec -> NAT changes address in the packet header -> lost of integrity
  - Kerboros -> NAT changes address in the packet header -> K needs the source address
  - RTP/RTCP -> use UDP with dynamic ports assignation -> NAT is not able to support this translation during a session (except proxy)
  - Multicast is not easy to set-up !!!

Why IPv6 ?

Communications technologies need permanent addresses to get connected to the Internet

- Cellulars (500 millions)
- Standard phones (900 millions)
- Radio/TV (++ hundred millions)
- Industrials devices (billions of IP addresses)
- Any electronics device (walkman to download MP3 files, bulgar alarm to send e-mail to the police station …)

Why IPv6 ?

CONCLUSION :

The true question is not :

« *Do we need and do we believe in IPv6* ? »

Not, the right one is :

« Are we interested in a network that allows any IP electronic devices to communicate transparently to each other regarless its location on THE global net ? »

- Viagénie

IPv6 @ Google IPv6 Implementors Conference

- Vint Cerf Opening Remaks

http://www.youtube.com/watch?feature=player_embedded&v=lSsbJj4TVPM

http://www.youtube.com/watch?feature=player_embedded&v=lSsbJj4TVPM

A need for IPv6?

- IETF IPv6 WG began in early 1990s, to solve addressing growth issues, but
  - CIDR, NAT, PPP, DHCP were developed
  - Some address reclamation
  - The RIR system was introduced
  - → Brakes were put on IPv4 address consumption
- IPv4 32 bit address = 4 billion hosts
  - 38.1% address space still unallocated (09/2004)

A need for IPv6?

- **General perception is that "*IPv6 has not yet taken hold strongly*"**
  - **IPv4 Address shortage is not upon us yet**
  - **Private sector requires a business case**
  - **Data on Wireless infrastructure emerges recently**
- **But reality looks far better for the coming years! IPv6 needed to sustain the *Internet growth***
- **Only compelling reason for IPv6:**
  - **LARGER ADDRESS SPACE**
  - **HD Ratio (RFC3194) limits IPv4 to 250 million hosts**

Do we really need a larger address space?

- **Internet population**

  ~600 million users in Q4 CY2002

  ~945M by end CY 2004 – only 10-15%

  How to address the future Worldwide population? (~9B in CY 2050)

- **Emerging Internet countries need address space, e.g.:**

  China uses more than a /7 today

  China would need more than a /4 of IPv4 address space if every student (320M) is to get an IPv4 address

Do we really need a larger address space?

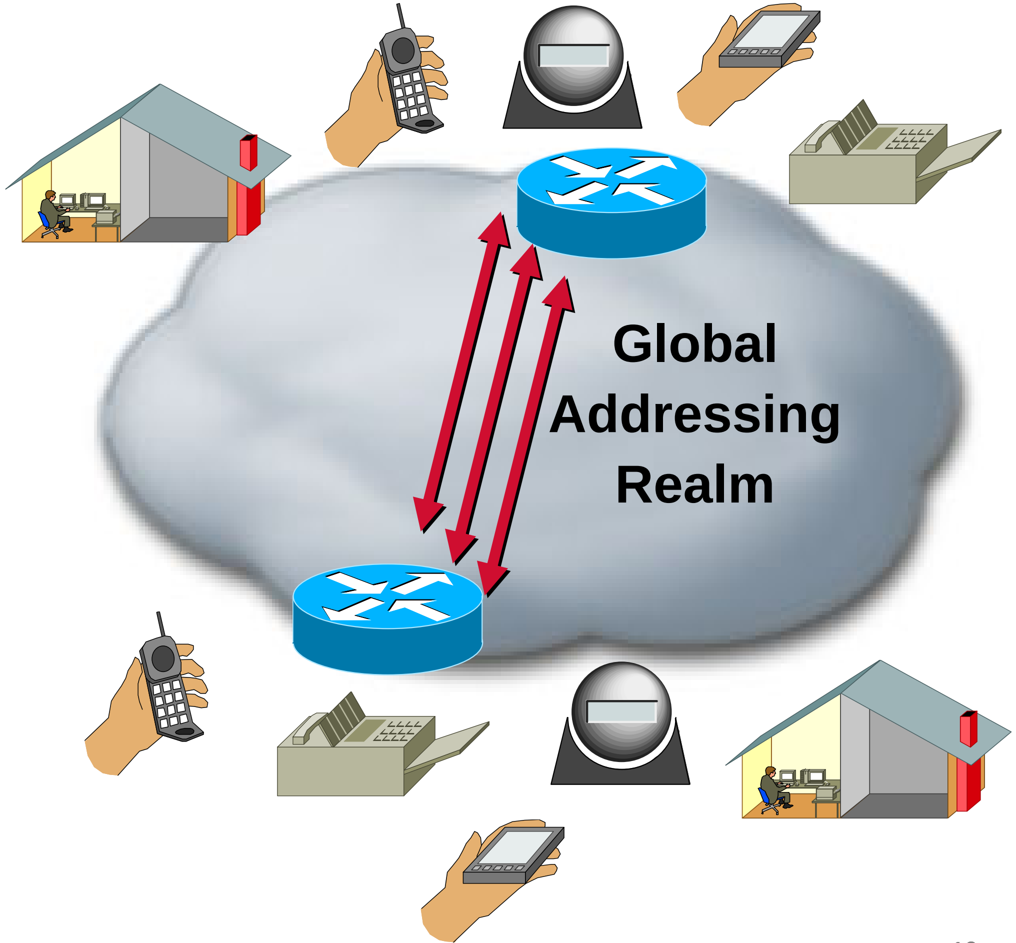
- Mobile Internet introduces new generation of Internet devices
  - PDA (~20M in 2004), Mobile Phones (~1.5B in 2003), Tablet PC
  - Enable through several technologies, eg: 3G, 802.11,…
- Transportation – Mobile Networks
  - 1B automobiles forecast for 2008 – Begin now on vertical markets
  - Internet access on planes, e.g. Connexion/Boeing
  - Internet access on trains, e.g. Narita express
- Consumer, Home and Industrial Appliances

Restoring an End-to-End Architecture

New Technologies/Applications for Home Users

'Always-on'—Cable, DSL, Ethernet-to-the-Home, Wireless,…

- Internet started with end-to-end connectivity for any applications
  - Replacing ALG such as Decnet/SNA gateway
- Today, NAT and Application-Layer Gateways connect disparate networks
- Peer-to-Peer or Server-to-Client applications mean global adresses when you connect to
  - IP Telephony, Fax, Video Conf
    Mobile, Residential,…
  - Distributed Gaming
  - Remote Monitoring
  - Instant Messaging



IPv6 Markets

- National Research & Education Networks (NREN) & Academia
- Geographies & Politics
- Wireless (PDA, 3G Mobile Phone networks, Car,...)
- Home Networking
  - Set-top box/Cable/xDSL/Ethernet-to-the-home
  - e.g. Japan Home Information Services initiative
  - Distributed Gaming
  - Consumer Devices
- Enterprise
  - Requires full IPv6 support on O.S. & Applications
- Service Providers

IPv6 Features

- Larger Address Space
- Aggregation-based address hierarchy
  - Efficient backbone routing
- Efficient and Extensible IP datagram
  - No fragmentation by routers
  - 64 bits field alignement
  - Simpler basic header
- Autoconfiguration
- Security
- IP Renumbering part of the protocol

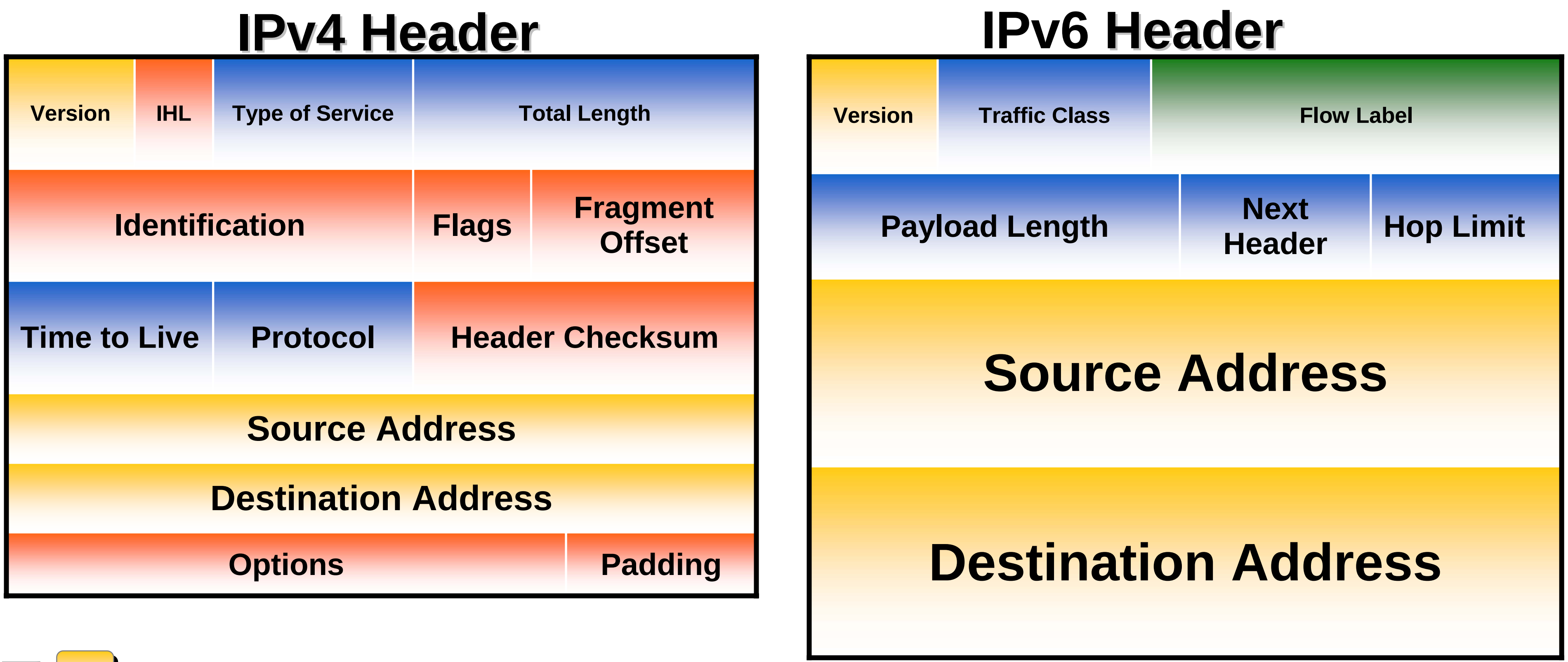
Design criterias for IPv6

- Number of addresses
- Efficiency in routers low and very high bandwidth (100G/bytes++)
- Security
- Mobility
- Autoconfig
- Seamless transition
  – Don't require a day X for switching to IPv6
  – No need to change hardware

So what's really changed?

- Expanded address space
  - Address length quadrupled to 16 bytes
- Header Format Simplification
  - Fixed length, optional headers are daisy-chained
  - IPv6 header is twice as long (40 bytes) as IPv4 header without options (20 bytes)
- No checksum at the IP network layer
- No hop-by-hop segmentation
  - Path MTU discovery
- 64 bits aligned
- Authentication and Privacy Capabilities
  - IPsec is mandated
- No more broadcast

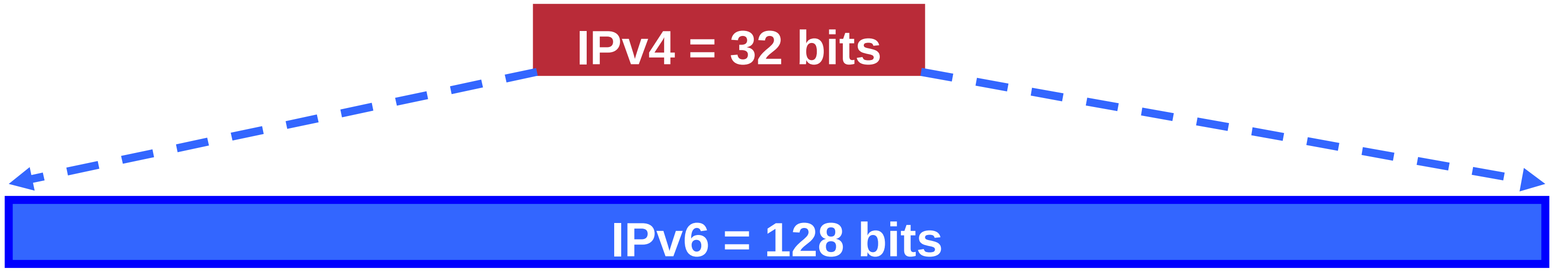
IPv4 & IPv6 Header Comparison



Legend

- Field's name kept from IPv4 to IPv6
- Fields not kept in IPv6
- Name & position changed in IPv6
- New field in IPv6

Larger Address Space



IPv4

- 32 bits
- = 4,294,967,296 possible addressable devices

IPv6

- 128 bits: 4 times the size in bits
- = 3.4 x 10^{38} possible addressable devices
- = 340,282,366,920,938,463,463,374,607,431,768,211,456
- ~ 5 x 10^{28} addresses per person on the planet

How Was The IPv6 Address Size Chosen?

- **Some wanted fixed-length, 64-bit addresses**

  Easily good for 10^{12} sites, 10^{15} nodes, at .0001 allocation efficiency (3 orders of magnitude more than IPv6 requirement)

  Minimizes growth of per-packet header overhead

  Efficient for software processing

- **Some wanted variable-length, up to 160 bits**

  Compatible with OSI NSAP addressing plans

  Big enough for auto-configuration using IEEE 802 addresses

  Could start with addresses shorter than 64 bits & grow later

- **Settled on fixed-length, 128-bit addresses**

Basic specifications

- Version (4 bits)
  - 6 for IPv6
- Traffic Class (8 bits)
  - ~= TOS in IPv4
  - Identifies and distinguishes between different classes or priorities (diffserv)
- Flow Label (20 bits)
  - Experimental
  - Used by a source node to label sequences of packets
- Payload Length
  - ~= Total length in IPv4

Basic specifications

- Next Header (8 bits)
  - Used for extension headers
  - ~= Protocol field in IPv4
  - Most not processed by routers in the path
  - Hop-by-hop options (0)
    - information that must be examined by every node along the path
  - Routing (43)
    - similar to IPv4's Loose Source and Record Route option
  - Fragment (44)
    - used by source node (routers don’t fragment anymore !)

Basic specifications

- Next Header (8 bits) cont.
  - Destination options (60)
    - used to carry optional information that need to be examined only by a packet's destination node(s)
  - Authentication (IPsec)
  - ESP (IPsec)
- Hop Limit ~= TTL in IPv4
- MTU must be at least 1280 bytes (1500+ recommended). Nodes should use Path MTU discovery.
- UDP checksum required

IPv6 Address Representation

- 16 bit fields in case insensitive 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 is ok

  2031::130F::9C0:876A:130B is NOT ok

  0:0:0:0:0:0:0:1 → ::1 (loopback address)

  0:0:0:0:0:0:0:0 → :: (unspecified address)

IPv6 Address Representation

- **IPv4-compatible (not used any more)**

  0:0:0:0:0:0:192.168.30.1

  = ::192.168.30.1

  = ::C0A8:1E01

- **In a URL, it is enclosed in brackets (RFC2732)**

  http://[2001:1:4F3A::206:AE14]:8080/index.html

  Cumbersome for users

  Mostly for diagnostic purposes

  Use fully qualified domain names (FQDN)

- **⇒ The DNS has to work!!**

IPv6 Addressing

- **IPv6 Addressing rules are covered by multiples RFC's**

  Architecture defined by RFC 3513

- **Address Types are :**

  Unicast : One to One (Global, Link local)

  Anycast : One to Nearest (Allocated from Unicast)

  Multicast : One to Many

- **A single interface may be assigned multiple IPv6 addresses of any type (unicast, anycast, multicast)**

  No Broadcast Address → Use Multicast

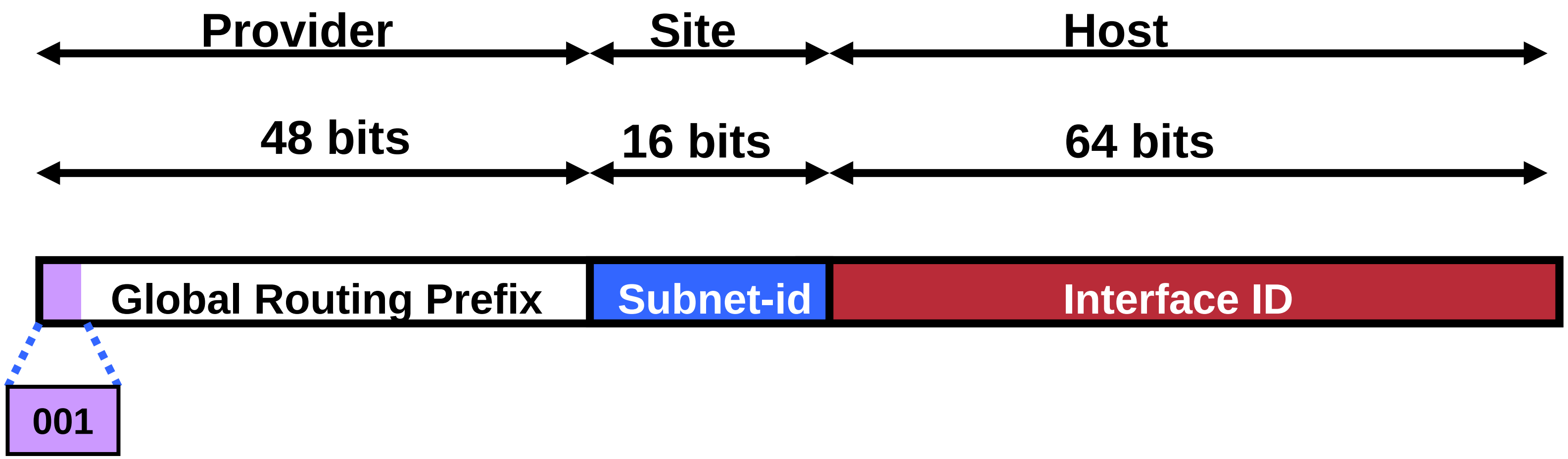
Address type identification

- **Address type identification**

Unspecified	00..0 (128 bits)	::/128
Loopback	00..1 (128 bits)	::1/128
Link Local	1111 1110 10	FE80::/10
Multicast	1111 1111	FF00::/8
Global Unicast	everything else	

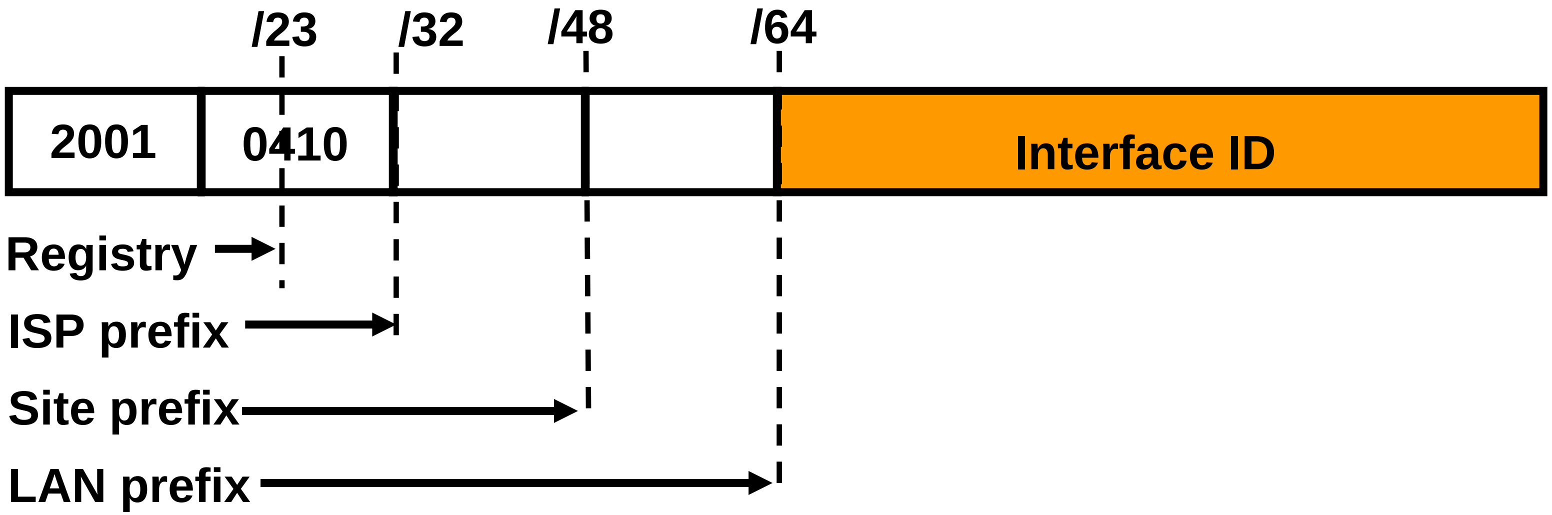
- **All address types have to support EUI-64 bits Interface ID setting**
  - Except for multicast

IPv6 Global Unicast Addresses



- **IPv6 Global Unicast addresses are:**
  - **Addresses for generic use of IPv6**
  - **Structured as a hierarchy to keep the aggregation**
- **First 3 bits 001 (2000::/3) is first allocation to IANA for use for IPv6 Unicast**

IPv6 Address Allocation



- **The allocation process is:**

  The IANA has allocated 2001::/16 for initial IPv6 unicast use

  Each registry gets /23 prefixes from the IANA

  Registry allocates a /32 prefix to an IPv6 ISP

  Policy is that an ISP allocates a /48 prefix to each end customer

IPv6 address representation

- Format is **x:x:x:x:x:x:x:x**
  - x is a 16 bit hexadecimal field
  - **FEDC:BA98:7654:3210:FEDC:BA98:7654:3210**
- Leading zeros in a field are optional
- **::** can be used to represent multiple groups of 16 bits of zero
  - **::** can only be used once in an address
  - **FF01:0:0:0:0:0:0:101 = FF01::101**
  - **0:0:0:0:0:0:0:1 = ::1**
  - **0:0:0:0:0:0:0:0 = ::**

IPv6 addressing

- Unicast address
  - FE80::/10 Link-Local Unicast Address
    - scope limited to local network
    - automatically configured on all nodes using interface identifiers
    - FE80::<interface id>
    - used for neighbor discovery and router discovery.
    - can also be used as a non-globally-routed IPv6 local network

IPv6 addressing

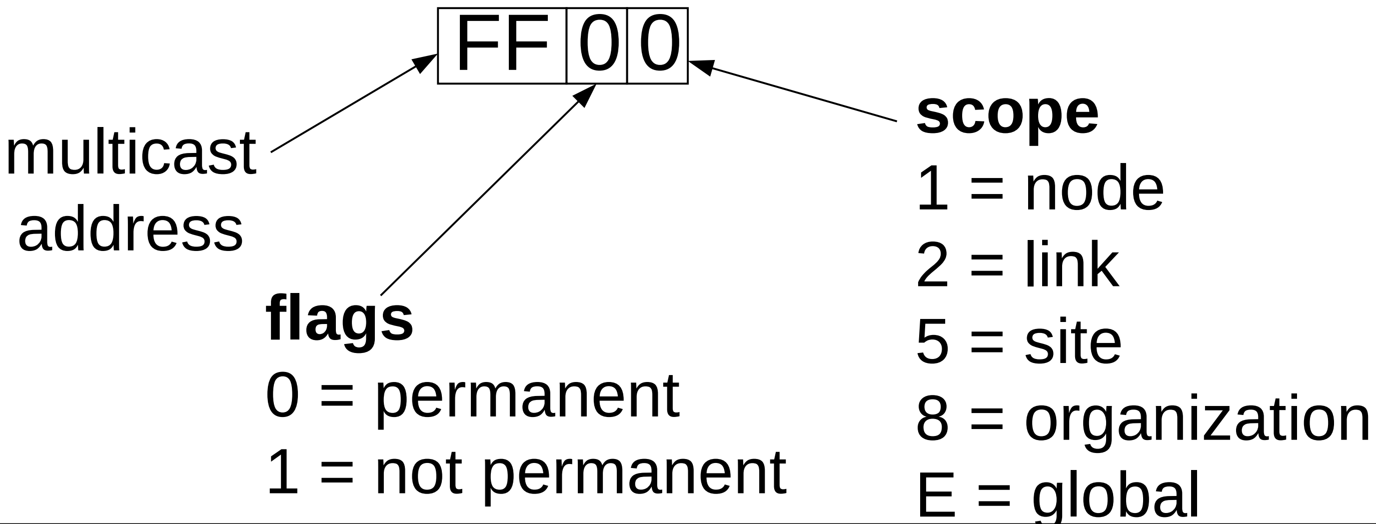
- Unicast address
  - FEC0::/10 Site-Local Unicast Address
    - confined to local site or organization
    - configured using interface identifier and a pre-defined 16 bits subnet ID
    - FEC0::<subnet id>:<interface id>
    - what is a site??? (few drafts: draft-haberman-ipv6-site-route-00.txt, draft-ietf-ipngwg-site-prefixes-02.txt)

IPv6 Addressing

- **`::1`**
  - Loopback address (like 127.0.0.1 in IPv4)
- **`::`**
  - Unspecified address
- **`::<IPv4 address>`**
  - IPv4 compatible address
  - Auto-tunnels (IPv6 over IPv4)
- **`::FFFF:<IPv4 address>`**
  - IPv4 mapped address (used by resolver library)
  - IPv6 representation of an IPv4 node
  - 206.123.31.101 is mapped as ::FFFF:206.123.31.101

Multicast address

- RFC2375 IPv6 Multicast Address Assignments
- FF00::/8
  - FF02::1 all nodes on the local network
  - FF02::2 all routers on the local network



Solicited-Node multicast address

- Solicited-Node multicast address
  - **FF02:0:0:0:0:1:FF00::/104**
    - address formed by appending the lower 24 bits of the IPv6 address
    - a node is required to join for every unicast and anycast address it is assigned

3FFE:0B00:0C18:0001:0290:27FF:FE17:FC0F

Global unicast address

FF02:0000:0000:0000:0000:0001:FF17:FC0F

Solicited multicast address

Anycast address

- Address assigned to more than one interface and/or node
- Packet sent to anycast address is routed to "closest" interface

subnet prefix	11111111111	ID
n bits	121-n bits	7 bits anycast ID

Example: **`3FFE:B00:C18:1:FDFF:FFFF:FFFF:FFFE`**

RFC2526: Reserved IPv6 Subnet Anycast Addresses

Required Node Addresses

- Link-Local Address for each interface
- Assigned Unicast Addresses
- Loopback Address
- All-Nodes Multicast Addresses
- Solicited-Node Multicast Address for each of its assigned unicast and anycast addresses
- Multicast Addresses of all other groups to which the host belongs

Interface IDs

- **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

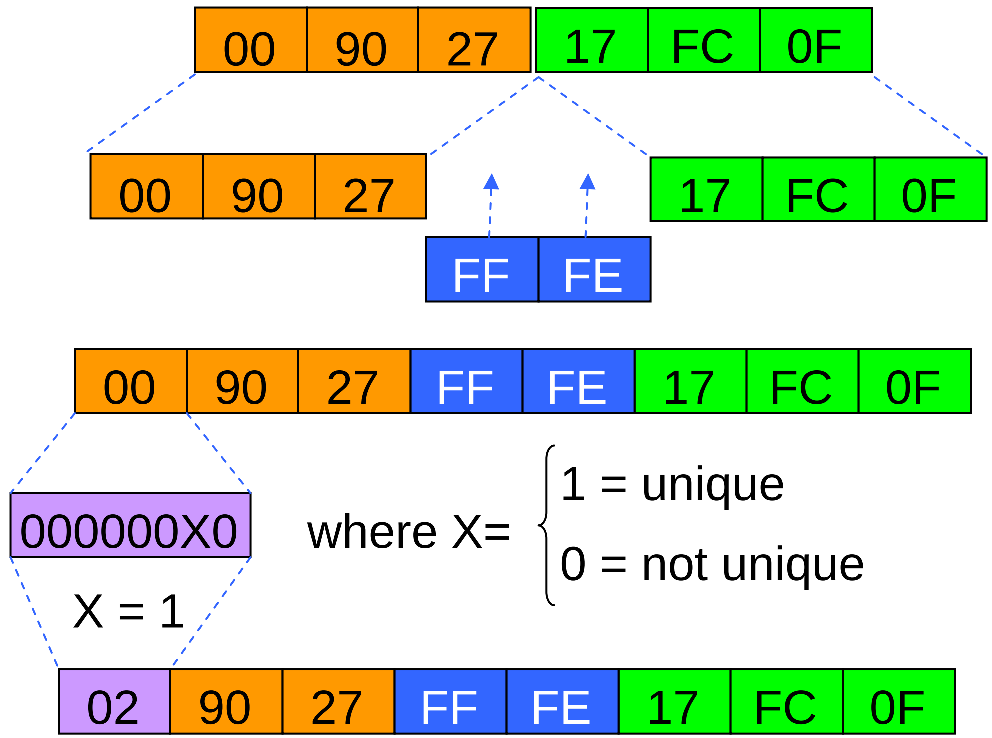
EUI-64

Ethernet MAC address (48 bits)

64 bits version

Uniqueness of the MAC

Eui-64 address

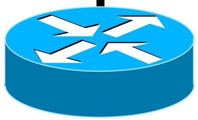


- **EUI-64 address is formed by inserting FFFE and OR'ing a bit identifying the uniqueness of the MAC address**

IPv6 Addressing Examples

LAN: 2001:410:213:1::/64

Ethernet0

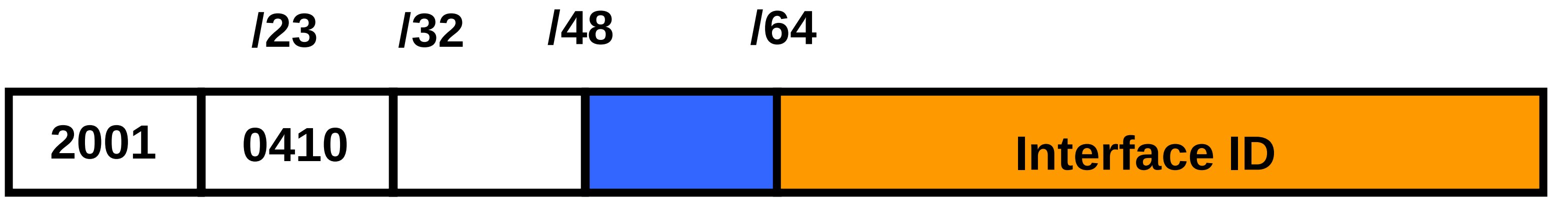


```
interface Ethernet0
 ipv6 address 2001:410:213:1::/64 eui-64
```

MAC address: 0060.3e47.1530

```
router# show ipv6 interface Ethernet0
Ethernet0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::260:3EFF:FE47:1530
Global unicast address(es):
    2001:410:213:1:260:3EFF:FE47:1530, subnet is 2001:410:213:1::/64
  Joined group address(es):
    FF02::1:FF47:1530
    FF02::1
    FF02::2
  MTU is 1500 bytes
```

IPv6 Address Privacy (RFC 3041)



- **Temporary addresses for IPv6 host client application, e.g. Web browser**
  - **Inhibit device/user tracking but is also a potential issue**
    - **More difficult to scan all IP addresses on a subnet but port scan is identical when an address is known**
  - **Random 64 bit interface ID, run DAD before using it**
  - **Rate of change based on local policy**
  - **Implemented on Microsoft Windows XP**
  - **From RFC 3041: "…interface identifier …facilitates the tracking of individual devices (and thus potentially users)…"**

Required Router Addresses

- All the required node addresses
- The Subnet-Router anycast addresses for the interfaces it is configured to act as a router on
- All other Anycast addresses which the router has been configured with
- All-Routers Multicast Addresses

ICMPv6

- RFC2463
- Protocol ICMPv6 (IPv6 Next Header 58)

IPv6 header		
Type	**Code**	**Checksum**
Message body		

← 32 bits →

ICMPv6 error messages

- Type 1: Destination Unreachable
  - Code 0: no route to destination
  - Code 1: communication administratively prohibited
  - Code 3: address unreachable
  - Code 4: port unreachable
- Type 2: Packet Too Big
  - Message contains MTU

ICMPv6 error messages

- Type 3: Time Exceeded
  - Code 0: hop limit exceeded
  - Code 1: fragment reassembly time exceeded
- Type 4: Parameter Problem
  - Code 0: erroneous header field
  - Code 1: unrecognized Next Header type
  - Code 2: unrecognized IPv6 option

ICMPv6 informational messages

- Type 128: Echo request
  - Message contains Identifier and Sequence number
- Type 129: Echo reply
  - Message contains Identifier and Sequence number
- ICMP “who are you”
  - draft-ietf-ipngwg-icmp-name-lookups-05.txt
  - Gets FQDN of remote node
  - Defines new ICMPv6 types for query and reply

Neighbor Discovery

- RFC2461
- ~= ARP in IPv4
- Uses ICMPv6 messages
- Used to:
  - Find link-layer address of neighbor
  - Find neighboring routers
  - Actively keep track of neighbor reachability
- Protocol used for host autoconfiguration
- All ND messages must have Hop Limit=255
  - Must originate from same link

Neighbor Discovery messages

- Router Solicitation
  - ICMP type 133
  - Host request routers to send Router Advertisement immediately

Neighbor Discovery messages

- Router Advertisement
  - ICMP type 134
  - Routers advertise periodically
    - max. time between advertisements can be in the range from 4 and 1800 seconds
  - Contains one or more prefixes
  - Prefixes have a lifetime
  - Specifies if stateful or stateless autoconfiguration is to be used
- Plays a key role in site renumbering

Neighbor Discovery messages

- Neighbor Advertisement
  - ICMP type 136
  - Response to a Neighbor Solicitation
- Neighbor Solicitation
  - ICMP type 135
  - Sent by node to determine link-layer address of a neighbor
- Route change, Redirect
  - Router send better hop for a destination
  - ~= ICMP redirect

IPv6 autoconfiguration

- Stateful autoconfiguration
  - Manual IP configuration
  - DHCP configuration (draft-ietf-dhc-dhcpv6-14.txt)

- Stateless Address Autoconfiguration (RFC2462)
  - Applies to hosts only (not to routers)
  - No manual configuration required, but does not specify the DNS servers, the prefix, lifetime and a default route
  - Assumes interface has unique identifier
  - Assumes multicast capable link
  - Uses Duplicate Address Detection

IPv6 autoconfiguration

- Duplicate Address Detection
  - Join all-nodes multicast address (FF02::1)
  - Join solicited-node multicast address of the tentative address
    - FF02:0:0:0:0:1:FF00: ...
  - Send Neighbor Solicitation on solicited-node multicast address
  - If no Neighbor Advertisement is received, address is ok

IPv6 Auto-Configuration

- **Stateless (RFC2462)**

  Host autonomously configures its own Link-Local address

  Router solicitation are sent by booting nodes to request RAs for configuring the interfaces.

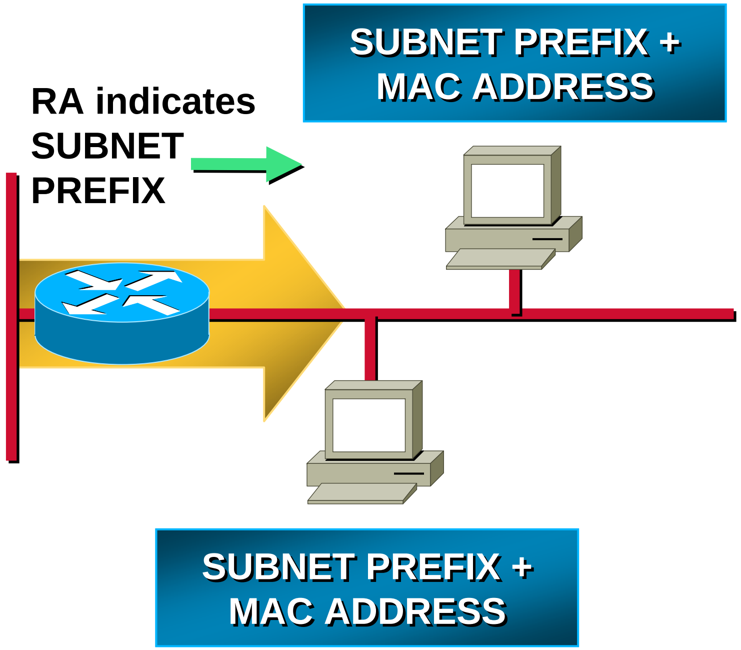
- **Stateful**

  DHCPv6 – required by most enterprises

- **Renumbering**

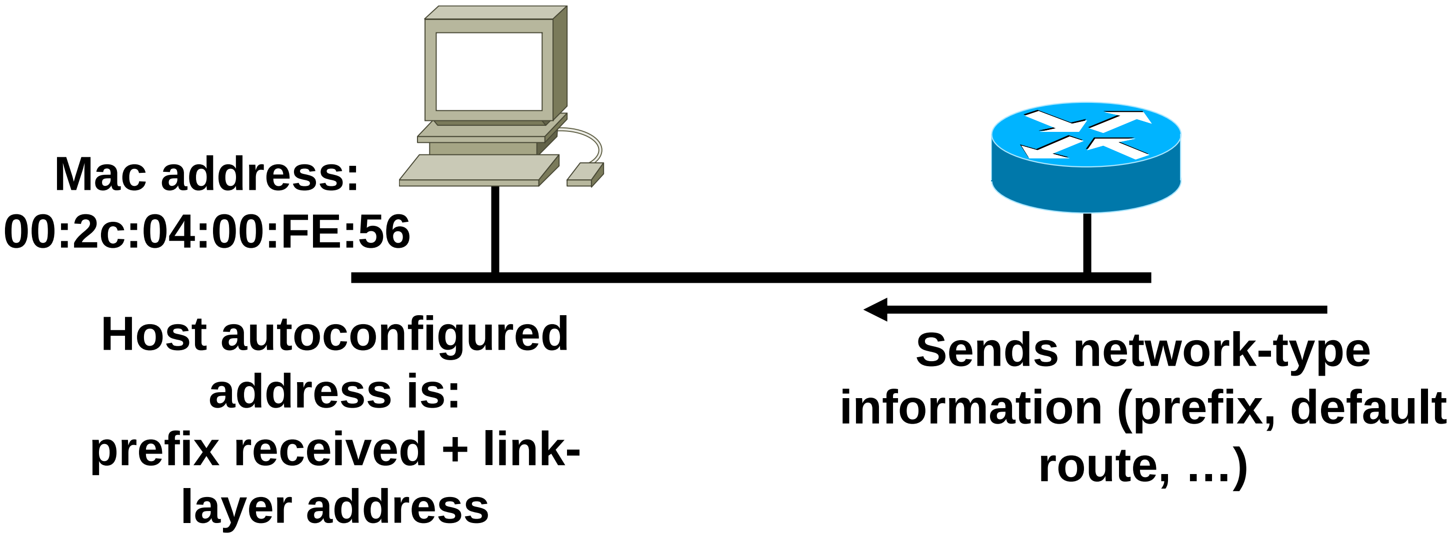
  Hosts renumbering is done by modifying the RA to announce the old prefix with a short lifetime and the new prefix

  Router renumbering protocol (RFC 2894), to allow domain-interior routers to learn of prefix introduction / withdrawal



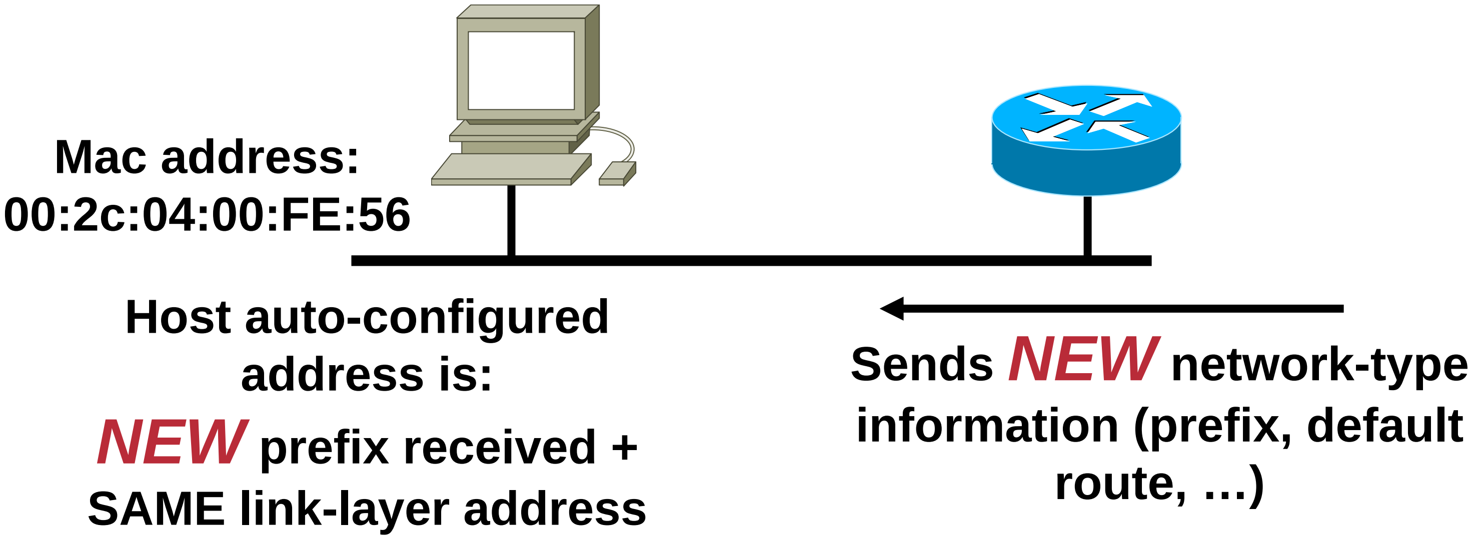
At boot time, an IPv6 host build a Link-Local address, then its global IPv6 address(es) from RA

Auto-configuration



- **Larger address space enables:**
  - **The use of link-layer addresses inside the address space**
  - **Auto-configuration with "no collisions“**
  - **Offers "Plug and play"**

Renumbering



- **Larger address space enables:**

  Renumbering, using auto-configuration and multiple addresses

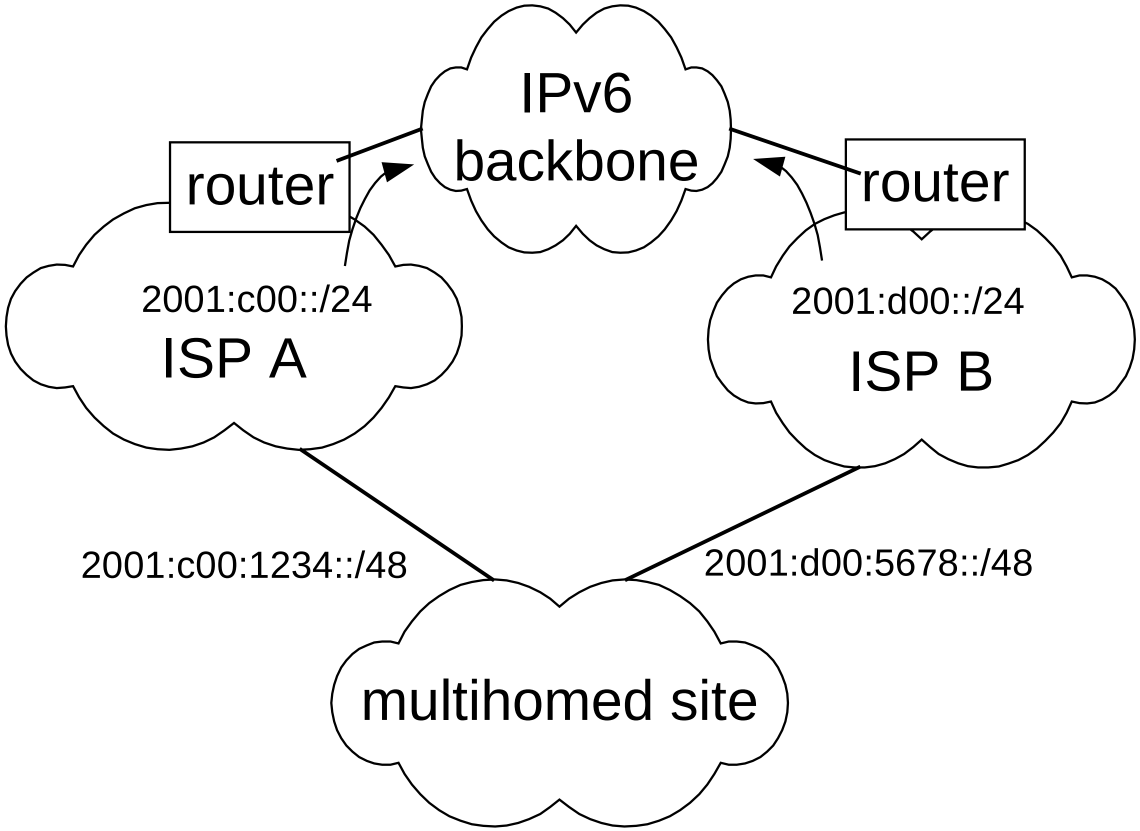
Renumbering

- Site Renumbering: hosts
  - Decrease the lifetime of the prefix in the router advertisement
- Router Renumbering
  - Protocol to renumber routers within a site
  - Defines new ICMPv6 messages
  - draft-ietf-ipngwg-router-renum-09.txt (work in progress)

Multihoming

- The IPv6 address assignment and allocation mechanism is fully hierarchical
  - A site uses its ISP prefix
- A multihomed site will have more than one prefix
- How does the hosts know which source address to use ?

Multihoming



Multihoming

- Default Address Selection for IPv6
  - draft-ietf-ipngwg-default-addr-select-00.txt

- IPv6 Multihoming with Route Aggregation
  - draft-ietf-ipngwg-ipv6multihome-with-aggr-00.txt

- Multihomed routing domain issues for IPv6 aggregatable scheme
  - draft-ietf-ipngwg-multi-isp-00.txt

IPv6 Standards

- **Core IPv6 specifications are IETF Draft Standards → well-tested & stable**

  IPv6 base spec, ICMPv6, Neighbor Discovery, PMTU Discovery,...

- **Other important specs are further behind on the standards track, but in good shape**

  mobile IPv6, header compression,...

  for up-to-date status: playground.sun.com/ipv6

- **3GPP UMTS Rel. 5 cellular wireless standards mandate IPv6; also being considered by 3GPP2**

IPv6 Status – Standardisation

- **Several key components on standards track…**

Specification (RFC2460)	Neighbour Discovery (RFC2461)
ICMPv6 (RFC2463)	IPv6 Addresses (RFC3513/3587)
RIP (RFC2080)	BGP (RFC2545)
IGMPv6 (RFC2710)	OSPF (RFC2740)
Router Alert (RFC2711)	Jumbograms (RFC2675)
Autoconfiguration (RFC2462)	Radius (RFC3162)
DHCPv6 (RFC3315)	Flow Label (RFC3697)
IPv6 Mobility (RFC3775)	GRE Tunnelling (RFC2473)

- **IPv6 available over:**

PPP (RFC2023)	Ethernet (RFC2464)
FDDI (RFC2467)	Token Ring (RFC2470)
NBMA (RFC2491)	ATM (RFC2492)
Frame Relay (RFC2590)	ARCnet (RFC2497)
IEEE1394 (RFC3146)	FibreChannel (RFC3831)

Recent IPv6 "Hot Topics" in the IETF

- Multi-homing
- Address selection
- Address allocation
- DNS discovery
- 3GPP usage of IPv6
- Anycast addressing
- Scoped address architecture
- Flow-label semantics
- API issues

  (flow label, traffic class, PMTU discovery, scoping,…)

- Enhanced router-to-host info
- Site renumbering procedures
- Inter-domain multicast routing
- Address propagation and AAA issues of different access scenarios
- End-to-end security vs. firewalls
- And, of course, transition / co-existence / interoperability with IPv4 (a bewildering array of transition tools and techniques)

Note: this indicates vitality, not incompleteness, of IPv6!

IPv6 and DNS

	IPv4	IPv6
Hostname to IP address	**A record:** www.abc.test. A 192.168.30.1	**AAAA record:** www.abc.test AAAA 3FFE:B00:C18:1::2
IP address to hostname	**PTR record:** 1.30.168.192.in-addr.arpa. PTR www.abc.test.	**PTR record:** 2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.8.1.c.0. 0.0.b.0.e.f.f.3.ip6.arpa PTR www.abc.test.

Overview

- Putting IPv6 data into DNS
  - Forward zone
  - Reverse zone
- Configuring BIND for IPv6 data
  - Zone file syntax for AAAA record
  - Naming convention for ip6.arpa sub-zone
- Putting a DNS server on a IPv6 network
  - Operational considerations
- Configuring BIND to run on IPv6
  - named.conf statements for controlling process on IPv6
  - Strategies for adding servers to IPv6
  - Migrating IPv6 service into an IPv4 network
  - Maintaining service for IPv4 clients

RFC4472

- DNS
  - To present a single, globally unique name space
  - The IP version used for querying resources records is independent of the protocol version of the resource records
    - AAAA records can be queried over IPv4
    - A records can be queried over IPv6

IPv6 support in BIND

- BIND above 9 answers DNS queries on IPv6 sockets
  - http://www.isc.org/index.pl?/sw/bind/bind9.php
- Newest version as of Aug 2007
  - BIND 9.4.1 – P1
- BIND expects an A record's record-specific data to be a 32-bit address (in dotted-octet format)
  - Various extensions were made to cope with a 128-bit address
    - AAAA
    - ip6.arpa

Putting IPv6 data into DNS - Forward lookup

- Multiple Resource Records (RR) for names to numbers
- AAAA (Similar to A RR for IPv4, pronounced quad-A)
- Can assign A records and AAAA records to a given name/domain
- Can also assign separate domains for IPv6 and IPv4

Forward lookup zone file

- Adding an IPv6 address to the DNS
  - A straight-forward matter
  - No need to a special zone for IPv6 in the forward space
  - You can add the AAAA record to existing zones and existing names
- If you can afford:
  - Maybe a good idea to keep some service servers IPv4 only, mixed, and some IPv6 only
    - To cope with immature IPv6 routing fabric
    - Older applications often do not fall back to IPv4 automatically

Forward zone file – sample

FQDN

```
; File: db.example.com
;
example.com.        IN      SOA     ns.example.com.
        hostmaster.example.com. (
                                20061101; serial
                                28800     ; refresh 8h
                                7200      ; retry 2h
                                604800    ; expiry 7days
                                86400 )   ; TTL 1day
                    IN      NS      ns.example.com.
                    IN      NS      ns2.example.com.

; Host addresses
;
ns.example.com      IN      A       10.11.12.13
ns2.example.com     IN      A       192.0.2.6
www.example.com     IN      A       10.11.12.15
                    IN      AAAA    2001:db8::3210
```

Reference:IPv6 Networking Administration

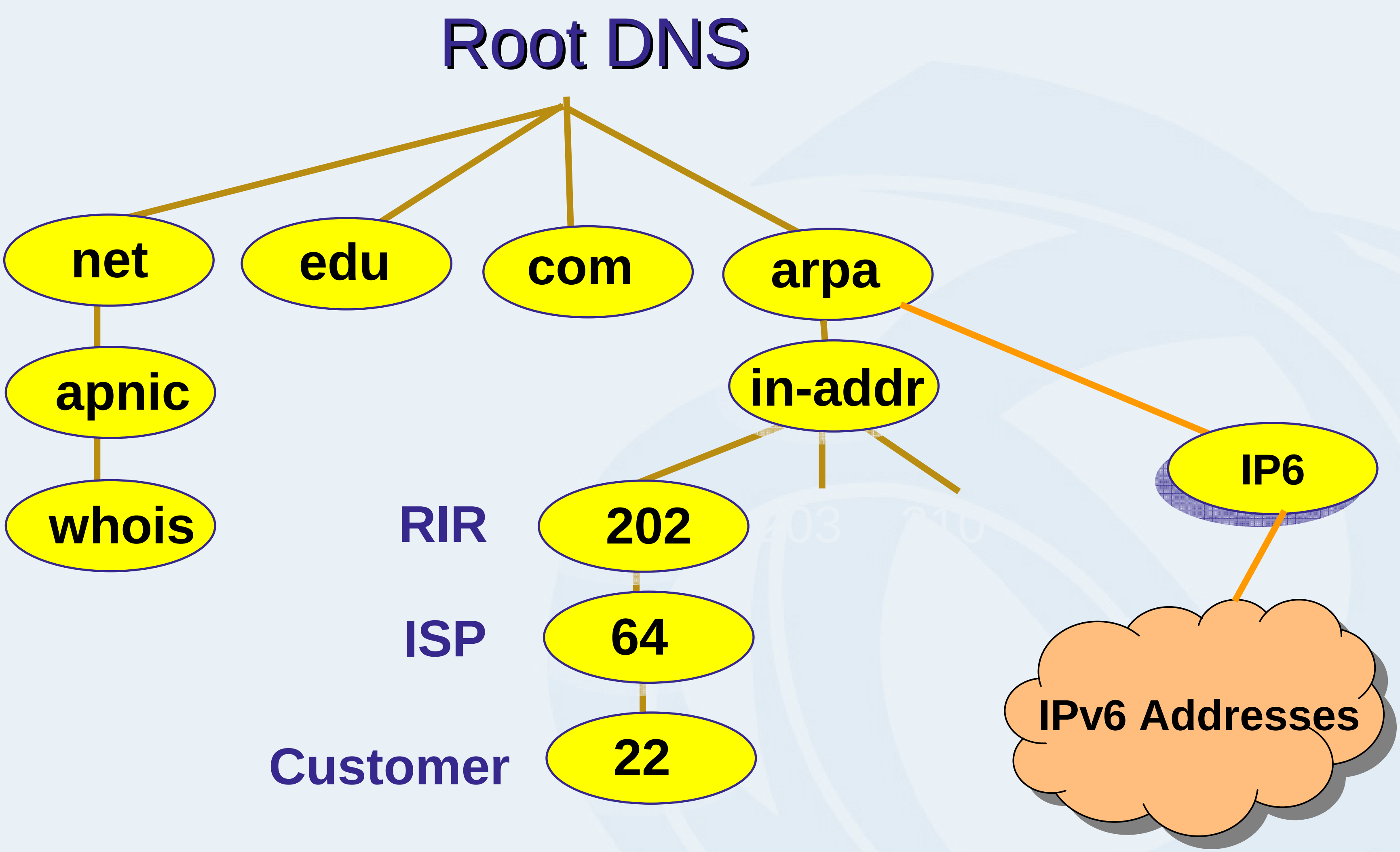
Putting IPv6 data into DNS – Reverse zone

- Why reverse mapping?
- RFC4472 (Operational Considerations and Issues with IPv6 DNS)
  - Some applications use reverse DNS
    - to look up some hints about the topological information associated with an address
    - E.g., resolving web server access logs
  - Weak form of a security
    - Did the network zone administrator authorise the domain name claim the address?
  - To weed out the majority of unauthorised users
    - By ensuring the reverse and forward DNS contents match

Reverse delegation

- Delegation
  - process of assigning responsibility for a zone to a particular set of servers
- You need to make a request to your provider
  - To get the appropriate reverse zone under ip6.arpa delegated to your nameserver
- In case you can not get the zone corresponding to your address space delegated:
  - You can run a nameserver for the zone without delegation
  - The records will only be visible to hosts directly querying your nameserver
    - But this may be sufficient for internal needs

The reverse DNS tree – with IPv6



IPv6 representation in the reverse DNS

- Reverse nibble format for zone ip6.arpa

- E.g., reverse lookup domain name corresponding to the address 4321:0:1:2:3:4:567:89ab
  - **b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.0.1.2.3.4.ip6.arpa.**

IPv6 reverse lookups - PTR records

- Example: reverse name lookup for a host with address 4321:8050:201:1860:42::1

```
1.0.0.0.0.0.0.0.0.0.0.0.2.4.0.0.0.6.8.1.1.0.2.0.0.5.0.8.1.2.3.4.ip6.arpa.
                                        IN      PTR     www.example.com.
```

```
$ORIGIN 0.6.8.1.1.0.2.0.0.5.0.8.1.2.3.4.ip6.arpa.
1.0.0.0.0.0.0.0.0.0.0.0.2.4.0.0         IN      PTR     www.example.com.
```

Reverse zone file - sample

```
; File: db.0000.0000.8bd0.1002
; IPv6 reverse lookup zone for 2001:db8::/64
; zone file for 0.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.ipv6.arpa
;
0.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa.        IN   SOA   ns.ipv6domail.com   root.ipv6domain.com. (
                                20061101; serial
                                28800        ; refresh 8h
                                7200         ; retry 2h
                                604800       ; expiry 7days
                                86400 )      ; TTL 1day
                                         IN   NS    ns.example.com.
                                         IN   NS    ns2.example.com.
0.1.2.3.0.0.0.0.0.0.0.0.0.0.0.0          IN   PTR   www.example.com.
```

Reference:IPv6 Networking Administration

named.conf file - sample

```
Zone “example.com” {
        type master;
        file “example.com.fwd”;
        allow-transfer { 192.0.2.6; }
};
Zone “0.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa” {
        type master;
        file “example.com.6rev”;
        allow-transfer { 192.0.2.6; }
};
```

Reference:IPv6 Networking Administration

IPv6 transport

- How to get DNS running over IPv6?
  - Firstly, make sure that your DNS server can answer queries over IPv6
    - May require a configuration option or
    - A patch to the software
    - E.g., BIND: “listen-on-v6” must be given in the named.conf
  - Then advertise your IPv6 capable DNS server
    - Add AAAA records listed as NS records for your zone, e.g.,

```
ns      IN    A       10.11.12.13
        IN    AAAA    2001:db8::32111
```

Routing in IPv6

- Routing in IPv6 is unchanged from IPv4:
  - IPv6 has 2 types of routing protocols: IGP and EGP
  - IPv6 still uses the longest-prefix match routing algorithm
- IGP
  - RIPng (RFC 2080)
  - Cisco EIGRP for IPv6
  - OSPFv3 (RFC 2740)
  - Integrated IS-ISv6 (draft-ietf-isis-ipv6-05)
- EGP : MP-BGP4 (RFC 2858 and RFC 2545)

RIPng

- **For the ISP industry, simply don't go here**
- **ISPs do not use RIP in any form unless there is absolutely no alternative**

  And there usually is
- **RIPng was used in the early days of the IPv6 test network**

  Sensible routing protocols such as OSPF and BGP rapidly replaced RIPng when they became available

EIGRP for IPv6

- Cisco EIGRP has had IPv6 protocol support added
- Uses similar CLI to existing IPv4 protocol support
- Easy deployment path for existing IPv4 EIGRP users
- In EFT images, coming soon to 12.3T

OSPFv3 overview

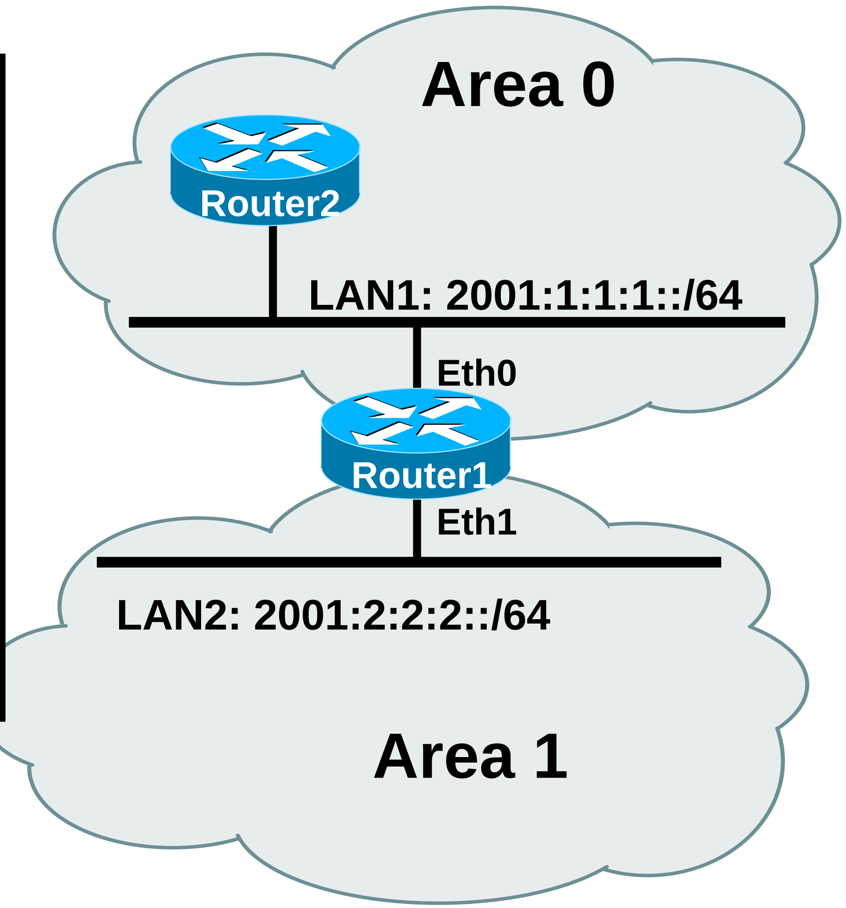
- OSPFv3 is OSPF for IPv6 (RFC 2740)
- Based on OSPFv2, with enhancements
- Distributes IPv6 prefixes
- Runs directly over IPv6
- Ships-in-the-night with OSPFv2

Differences from OSPFv2

- Runs over a link, not a subnet
    - Multiple instances per link
- Topology not IPv6 specific
    - Router ID
    - Link ID
- Standard authentication mechanisms
- Uses link local addresses
- Generalized flooding scope
- Two new LSA types

OSPFv3 configuration example

```
Router1#
 interface Ethernet0
  ipv6 address 2001:1:1:1::1/64
  ipv6 ospf 1 area 0

 interface Ethernet1
  ipv6 address 2001:2:2:2::2/64
  ipv6 ospf 1 area 1

 ipv6 router ospf 1
  router-id 1.1.1.1
  area 1 range 2001:2:2::/48
```



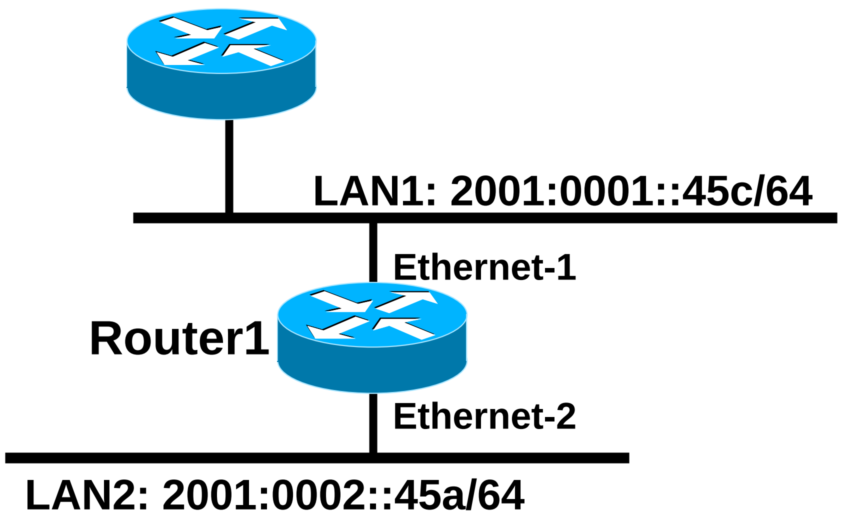
ISIS Standards History

- IETF ISIS for Internets Working Group
- ISO 10589 specifies OSI IS-IS routing protocol for CLNS traffic
  - Tag/Length/Value (TLV) options to enhance the protocol
  - A Link State protocol with a 2 level hierarchical architecture.
- RFC 1195 added IP support, also known as Integrated IS-IS (I/IS-IS)
  - I/IS-IS runs on top of the Data Link Layer
  - Requires CLNP to be configured
- Internet Draft defines how to add IPv6 address family support to IS-IS
  - www.ietf.org/internet-drafts/draft-ietf-isis-ipv6-06.txt
- Internet Draft introduces Multi-Topology concept for IS-IS
  - www.ietf.org/internet-drafts/draft-ietf-isis-wg-multi-topology-07.txt

IS-IS for IPv6

- 2 Tag/Length/Values added to introduce IPv6 routing
- IPv6 Reachability TLV (0xEC)
  - External bit
  - Equivalent to IP Internal/External Reachability TLV's
- IPv6 Interface Address TLV (0xE8)
  - For Hello PDUs, must contain the Link-Local address
  - For LSP, must only contain the non-Link Local address
- IPv6 NLPID (0x8E) is advertised by IPv6 enabled routers

Cisco IOS IS-IS dual IP configuration




```
Router1#
interface ethernet-1
 ip address 10.1.1.1 255.255.255.0
 ipv6 address 2001:0001::45c/64
 ip router isis
 ipv6 router isis

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

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

Dual IPv4/IPv6 configuration.
Redistributing both IPv6 static routes and IPv4 static routes.

Multi-Topology IS-IS extensions

- **New TLVs attributes for Multi-Topology extensions.**

  ***Multi-topology TLV*: contains one or more multi-topology ID in which the router participates. It is theoretically possible to advertise an infinite number of topologies. This TLV is included in IIH and the first fragment of a LSP.**

  ***MT Intermediate Systems TLV*: this TLV appears as many times as the number of topologies a node supports. A MT ID is added to the extended IS reachability TLV type 22.**

  ***Multi-Topology Reachable IPv4 Prefixes TLV*: this TLV appears as many times as the number of IPv4 announced by an IS for a give n MT ID. Its structure is aligned with the extended IS Reachability TLV Type 236 and add a MT ID.**

  ***Multi-Topology Reachable IPv6 Prefixes TLV*: this TLV appears as many times as the number of IPv6 announced by an IS for a given MT ID. Its structure is aligned with the extended IS Reachability TLV Type 236 and add a MT ID.**

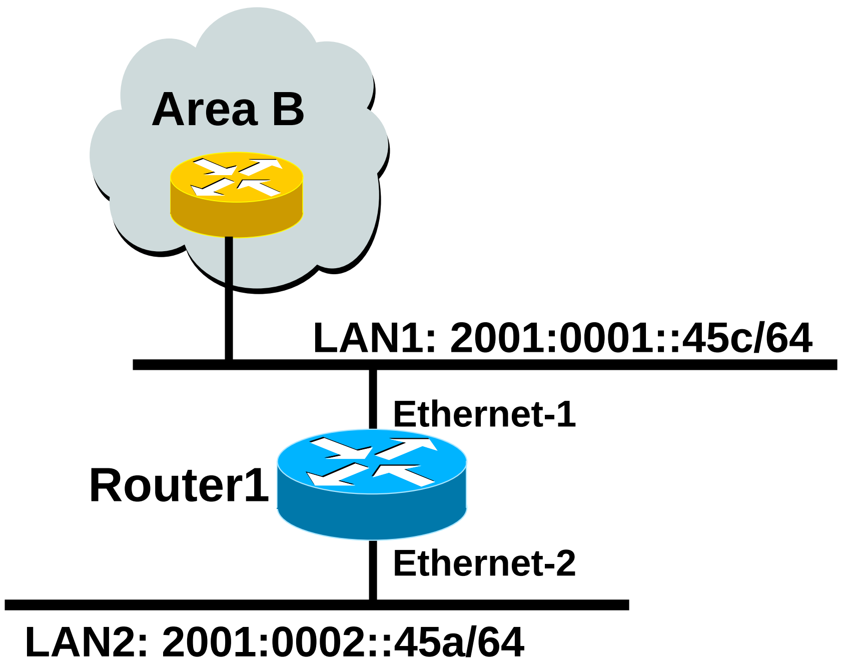
- **Multi-Topology ID Values**

  Multi-Topology ID (MT ID) standardized and in use in Cisco IOS:

  MT ID #0 – "standard" topology for IPv4/CLNS

  MT ID #2 – IPv6 Routing Topology.

Cisco IOS Multi-Topology ISIS configuration example



- The optional keyword *transition* may be used for transitioning existing IS-IS IPv6 single SPF mode to MT IS-IS
- Wide metric is mandated for Multi-Topology to work

```
Router1#
interface ethernet-1
 ip address 10.1.1.1 255.255.255.0
 ipv6 address 2001:0001::45c/64
 ip router isis
 ipv6 router isis
 isis ipv6 metric 20

interface ethernet-2
 ip address 10.2.1.1 255.255.255.0
 ipv6 address 2001:0002::45a/64
 ip router isis
 ipv6 router isis
 isis ipv6 metric 20

router isis
 net 49.0000.0100.0000.0000.0500
 metric-style wide
 !
 address-family ipv6
  multi-topology
 exit-address-family
```

Multi-Protocol BGP for IPv6 – RFC2545

- **IPv6 specific extensions**

  Scoped addresses: Next-hop contains a global IPv6 address and/or potentially a link-local address

  NEXT_HOP and NLRI are expressed as IPv6 addresses and prefix

  Address Family Information (AFI) = 2 (IPv6)

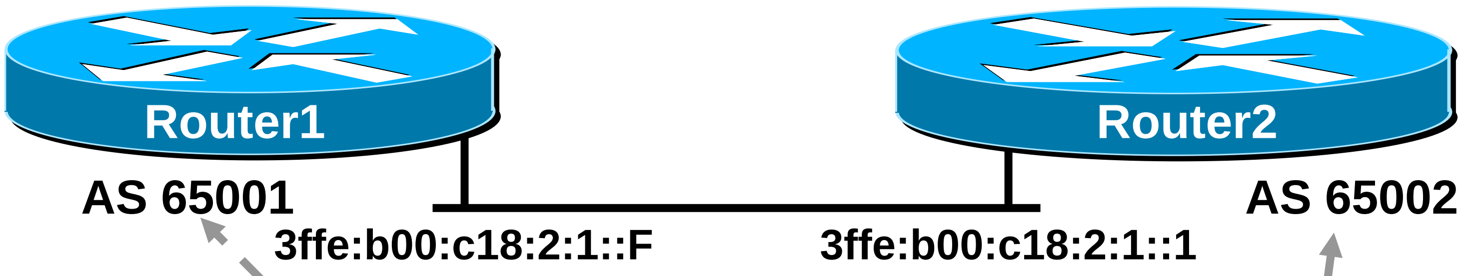
    Sub-AFI = 1 (NLRI is used for unicast)

    Sub-AFI = 2 (NLRI is used for multicast RPF check)

    Sub-AFI = 3 (NLRI is used for both unicast and multicast RPF check)

    Sub-AFI = 4 (label)

A Simple MP-BGP Session




```
Router1#
interface Ethernet0
 ipv6 address 3FFE:B00:C18:2:1::F/64
!
router bgp 65001
 bgp router-id 10.10.10.1
 no bgp default ipv4-unicast
 neighbor 3FFE:B00:C18:2:1::1 remote-as 65002
 address-family ipv6
  neighbor 3FFE:B00:C18:2:1::1 activate
  neighbor 3FFE:B00:C18:2:1::1 prefix-list bgp65002in in
  neighbor 3FFE:B00:C18:2:1::1 prefix-list bgp65002out out
  exit-address-family
```

Routing Protocols for IPv6 Summary

- Support for IPv6 in the major routing protocols
- More details for OSPF and BGP in following slides

OSPF for IPv6

OSPFv2

- April 1998 was the most recent revision (RFC 2328)
- OSPF uses a 2-level hierarchical model
- SPF calculation is performed independently for each area
- Typically faster convergence than DVRPs
- Relatively low, steady state bandwidth requirements

OSPFv3 overview

- OSPF for IPv6
- Based on OSPFv2, with enhancements
- Distributes IPv6 prefixes
- Runs directly over IPv6
- Ships-in-the-night with OSPFv2

OSPFv3 / OSPFv2 Similarities

- **Basic packet types**

  Hello, DBD, LSR, LSU, LSA

- **Mechanisms for neighbor discovery and adjacency formation**
- **Interface types**

  P2P, P2MP, Broadcast, NBMA, Virtual

- **LSA flooding and aging**
- **Nearly identical LSA types**

OSPFv3 / OSPFv2 Differences

- OSPFv3 runs over a link, rather than a subnet
- Multiple instances per link
- OSPFv2 topology not IPv6-specific
  - Router ID
  - Link ID
- Standard authentication mechanisms
- Uses link-local addresses
- Generalized flooding scope
- Two new LSA types

LSA Type Review

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

Link LSA

- A link LSA per link
- Link local scope flooding on the link with which they are associated
- Provide router link local address
- List all IPv6 prefixes attached to the link
- Assert a collection of option bit for the Router-LSA

Inter-Area Prefix LSA

- Describes the destination outside the area but still in the AS
- Summary is created for one area, which is flooded out in all other areas
- Originated by an ABR
- Only intra-area routes are advertised into the backbone
- Link State ID simply serves to distinguish inter-area-prefix-LSAs originated by the same router
- Link-local addresses must never be advertised in inter-area- prefix-LSAs

Configuring OSPFv3 in Cisco IOS® Software

- **Similar to OSPFv2**
  - **Prefixing existing Interface and Exec mode commands with “ipv6”**
- **Interfaces configured directly**
  - **Replaces `network` command**
- **“Native” IPv6 router mode**
  - **Not a sub-mode of `router ospf`**

Configuration Modes in OSPFv3

- **Entering router mode**

  [no] ipv6 router ospf <process ID>

- **Entering interface mode**

  [no] ipv6 ospf <process ID> area <area ID>

- **Exec mode**

  [no] show ipv6 ospf [<process ID>]

  clear ipv6 ospf [<process ID>]

Cisco IOS OSPFv3 Specific Attributes

- **Configuring area range**

  [no] area <area ID> range <prefix>/<prefix length>

- **Showing new LSA**

  show ipv6 ospf [<process ID>] database link

  show ipv6 ospf [<process ID>] database prefix

OSPFv3 Debug Commands

- **Adjacency is not appearing**

  [no] debug ipv6 ospf adj

  [no] debug ipv6 ospf hello

- **SPF is running constantly**

  [no] debug ipv6 ospf spf

  [no] debug ipv6 ospf flooding

  [no] debug ipv6 ospf events

  [no] debug ipv6 ospf lsa-generation

  [no] debug ipv6 ospf database-timer

- **General purpose**

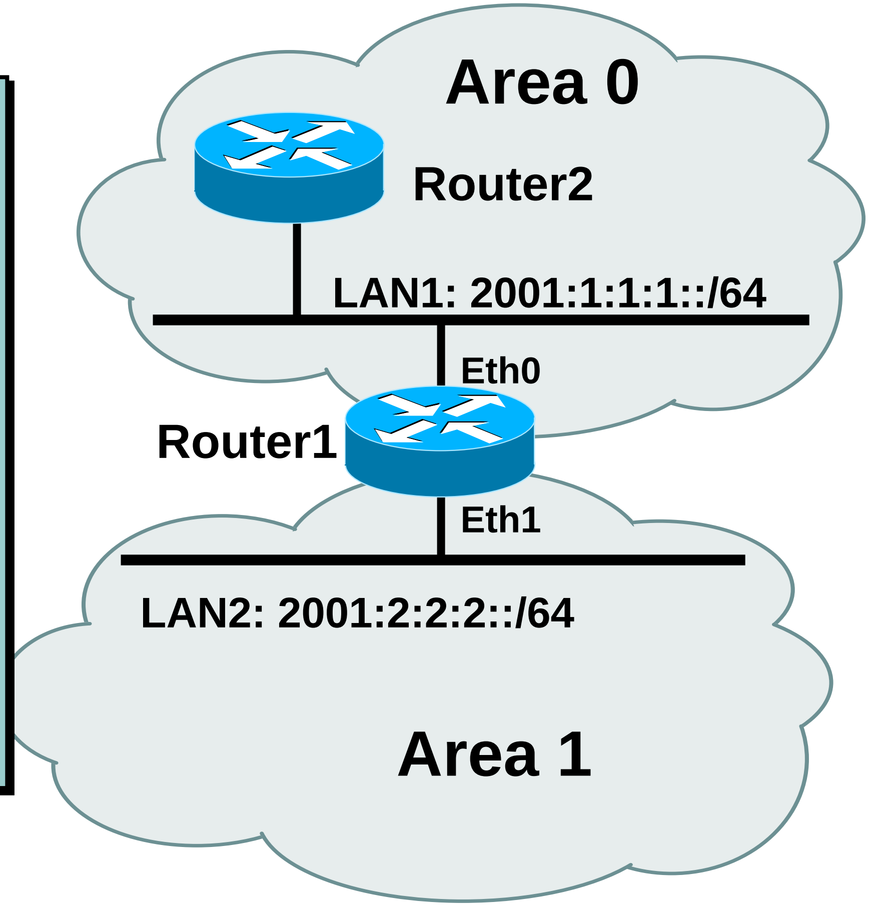
  [no] debug ipv6 ospf packets

  [no] debug ipv6 ospf retransmission

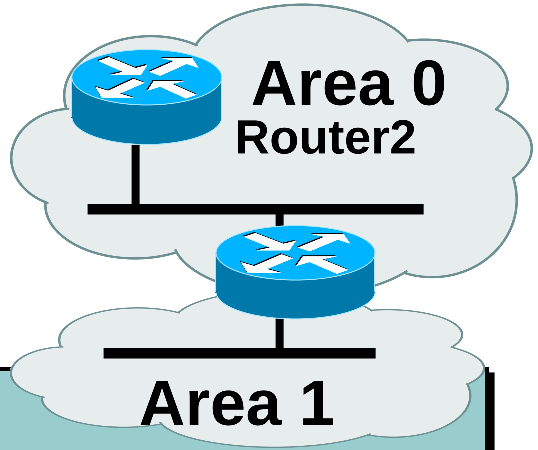
  [no] debug ipv6 ospf tree

OSPFv3 configuration example

```
Router1#
 interface Ethernet0
  ipv6 address 2001:1:1:1::1/64
  ipv6 ospf 1 area 0

 interface Ethernet1
  ipv6 address 2001:2:2:2::2/64
  ipv6 ospf 1 area 1

 ipv6 router ospf 1
  router-id 1.1.1.1
  area 1 range 2001:2:2::/48
```



Cisco IOS OSPFv3 Display




```
Router 2# show ipv6 route ospf
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
O   2001:1:1:2::1/128 [110/1]
     via FE80::205:5FFF:FEAF:2C38, Ethernet0
OI  2001:2:2::/48 [110/2]
     via FE80::205:5FFF:FEAF:2C38, Ethernet0
```

Cisco IOS OSPFv3 Database Display

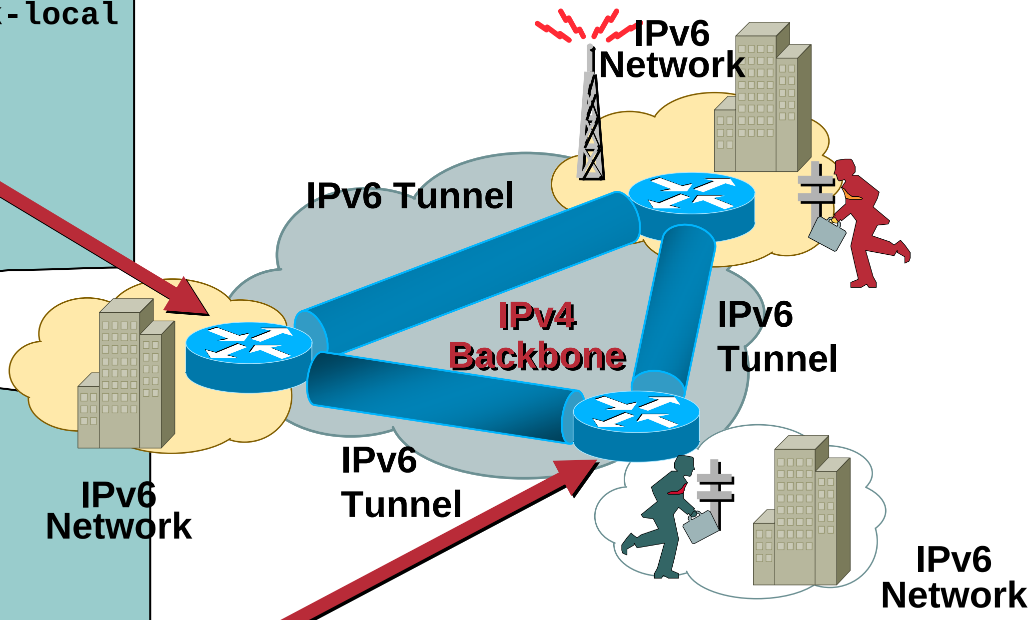
```
Router2# show ipv6 ospf database

OSPF Router with ID (3.3.3.3) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
0               1.1.1.1         2009        0x8000000A 0x2DB1   1
0               3.3.3.3         501         0x80000007 0xF3E6   1

                Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
7               1.1.1.1         480         0x80000006 0x3BAD

                Inter Area Prefix Link States (Area 0)

ADV Router      Age         Seq#        Prefix
1.1.1.1         1761        0x80000005  2001:2:2:2::/64
1.1.1.1         982         0x80000005  2001:2:2:4::2/128

                Link (Type-8) Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Interface
11              3.3.3.3         245         0x80000006 0xF3DC   Lo0
7               1.1.1.1         236         0x80000008 0x68F    Fa2/0
7               3.3.3.3         501         0x80000008 0xE7BC   Fa2/0

                Intra Area Prefix Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Ref lstype
0               1.1.1.1         480         0x80000008 0xD670   0x2001
107             1.1.1.1         236         0x80000008 0xC05F   0x2002
0               3.3.3.3         245         0x80000006 0x3FF7   0x2001
```

Cisco IOS OSPFv3 Detailed LSA Display

```
show ipv6 ospf 1 database inter-area prefix

  LS age: 1714
  LS Type: Inter Area Prefix Links
  Link State ID: 0
  Advertising Router: 1.1.1.1
  LS Seq Number: 80000006
  Checksum: 0x25A0
  Length: 36
  Metric: 1
  Prefix Address: 2001:2:2:2::
  Prefix Length: 64, Options: None

 show ipv6 ospf 1 database link

  LS age: 283
  Options: (IPv6 Router, Transit Router, E-Bit, No Type 7-to-5, DC)
  LS Type: Link-LSA (Interface: Loopback0)
  Link State ID: 11 (Interface ID)
  Advertising Router: 3.3.3.3
  LS Seq Number: 80000007
  Checksum: 0xF1DD
  Length: 60
  Router Priority: 1
  Link Local Address: FE80::205:5FFF:FEAC:1808
  Number of Prefixes: 2
  Prefix Address: 2001:1:1:3::
  Prefix Length: 64, Options: None
  Prefix Address: 2001:1:1:3::
  Prefix Length: 64, Options: None
```

OSPFv3 on IPv6 Tunnels over IPv4

```
interface Tunnel0
 no ip address
 ipv6 address 2001:0001::45A/64
 ipv6 address FE80::10:7BC2:ACC9:10 link-local
 ipv6 router ospf 1 area 0
 tunnel source Ethernet1
 tunnel destination 10.42.2.1
 tunnel mode ipv6ip
!
ipv6 router ospf 1
```




```
interface Tunnel0
 no ip address
 ipv6 address 2001:0001::45C/64
 ipv6 address FE80::10:7BC2:B280:11 link-local
 ipv6 router ospf 1 area 0
 tunnel source Ethernet2
 tunnel destination 10.42.1.1
 tunnel mode ipv6ip
!
ipv6 router ospf 1
```

Conclusion

- **Based on existing OSPFv2 implementation**
- **Similar CLI and functionality**
- **Cisco IOS Software availability:**

  Release 12.2(15)T and 12.3

  Release 12.2(18)S for Cisco 7000 Series Routers and Cisco Catalyst 6000 Series Switches

  Release 12.0(24)S the Cisco 12000 Series Internet Routers

BGP Enhancements for IPv6

Adding IPv6 to BGP…

- **RFC2858**

  Defines *Multi-protocol Extensions for BGP4*

  Enables BGP to carry routing information of protocols other than IPv4

  - **e.g. MPLS, IPv6, Multicast etc**

  Exchange of multiprotocol NLRI must be negotiated at session startup

- **RFC2545**

  Use of BGP Multiprotocol Extensions for IPv6 Inter-Domain Routing

Adding IPv6 to BGP…

- **New 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 (RFC2858)

  MP_UNREACH_NLRI (Attribute code: 15)

  Carry the set of unreachable destinations

- **Attribute contains one or more Triples:**

  AFI Address Family Information

  Next-Hop Information (must be of the same address family)

  NLRI Network Layer Reachability Information

Adding IPv6 to BGP…

- **Address Family Information (AFI) for IPv6**

  AFI = 2 (RFC 1700)

Sub-AFI = 1	**Unicast**
Sub-AFI = 2	**Multicast for RPF check**
Sub-AFI = 3	**for both Unicast and Multicast**
Sub-AFI = 4	**Label**
Sub-AFI = 128	**VPN**

BGP Considerations

- **Rules for constructing the NEXTHOP attribute:**

  When two peers share a common subnet the NEXTHOP information is formed by a global address and a link local address

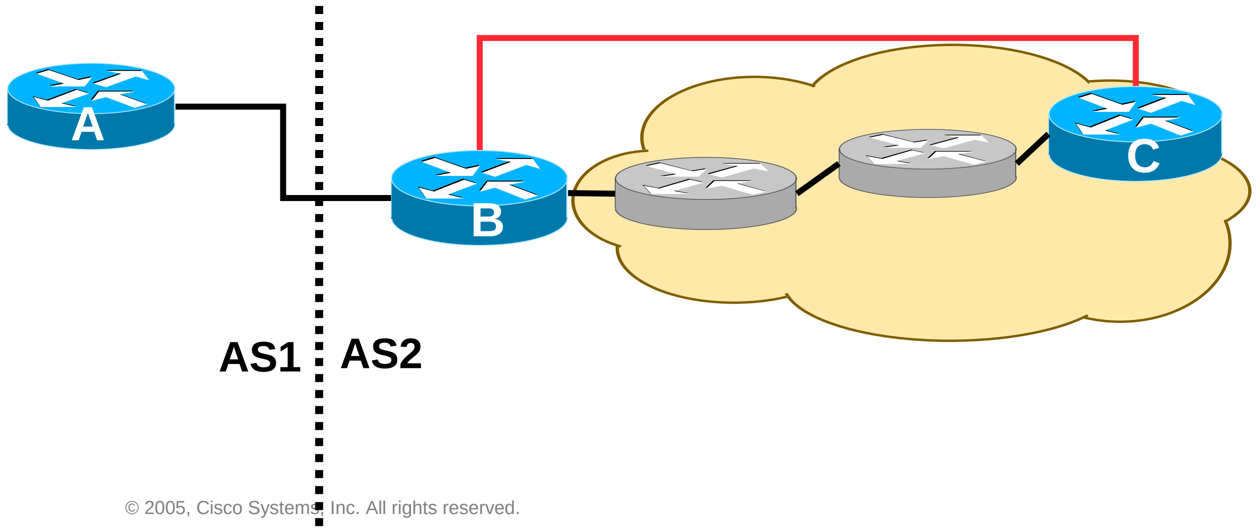
  Redirects in IPv6 are restricted to the usage of link local addresses

Routing Information

- **Independent operation**
  - **One RIB per protocol**
    - **e.g. IPv6 has its own BGP table**
  - **Distinct policies per protocol**
- **Peering sessions can be shared when the topology is congruent**

BGP next-hop attribute

- Next-hop contains a global IPv6 address (or potentially a link local address)
- Link local address as a next-hop is only set if the BGP peer shares the subnet with both routers (advertising and advertised)



More BGP considerations

- **TCP Interaction**

  BGP runs on top of TCP

  This connection could be set up either over IPv4 or IPv6

- **Router ID**

  When no IPv4 is configured, an explicit bgp router-id needs to be configured

  BGP identifier is a 32 bit integer currently generated from the router identifier – which is generated from an IPv4 address on the router

  This is needed as a BGP identifier, this is used as a tie breaker, and is send within the OPEN message

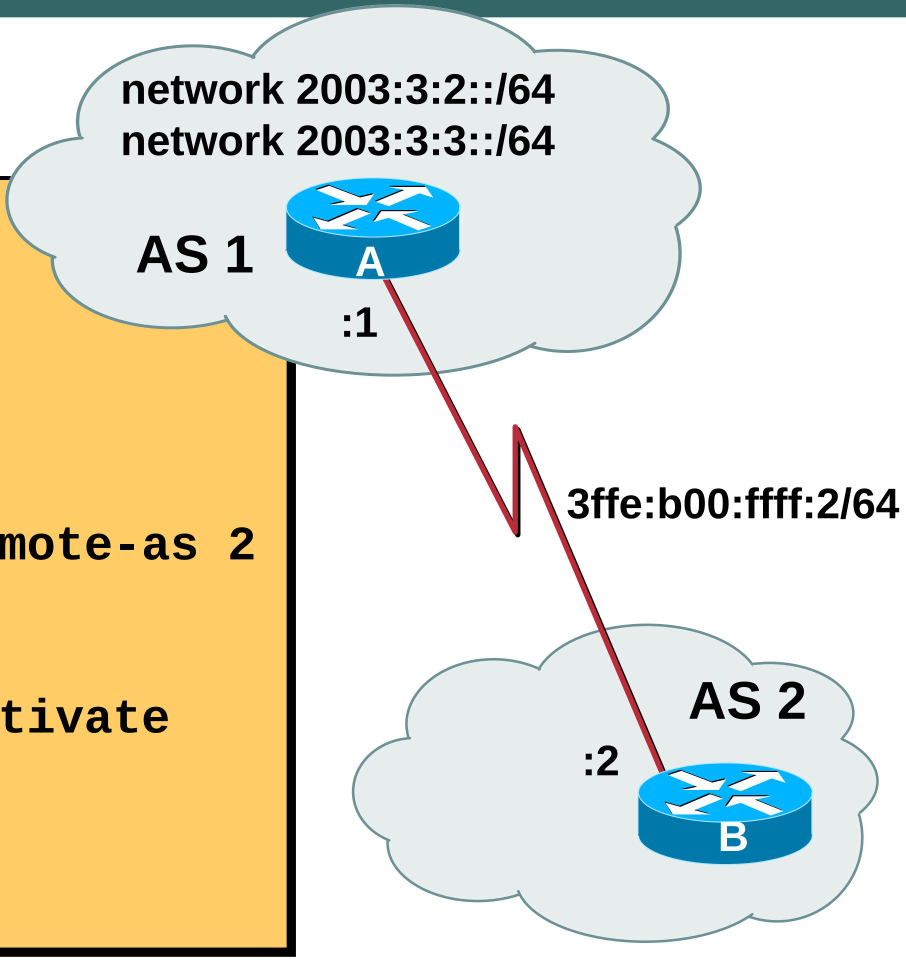
BGP Configuration

- Two options for configuring iBGP peering
- Using link local addressing
  - ISP uses FE80:: addressing for iBGP neighbours
  - NOT RECOMMENDED
    - There are plenty of IPv6 addresses
    - Configuration complexity
- Using global unicast addresses
  - As with IPv4
  - RECOMMENDED

BGP Configurations
Non Link Local Peering

Router A

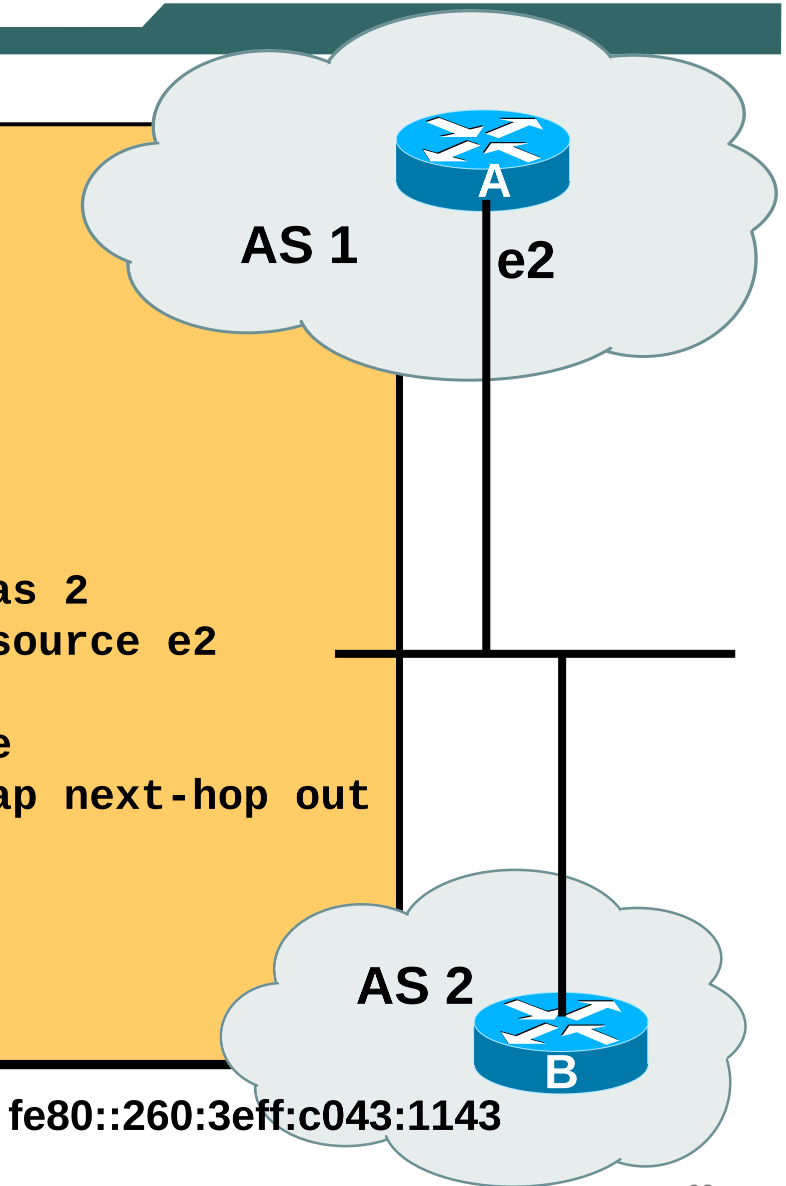
```
router bgp 1
 no bgp default ipv4 unicast
 bgp router-id 1.1.1.1
 neighbor 3ffe:b00:ffff:2::2 remote-as 2
!
 address-family ipv6
 neighbor 3ffe:b00:ffff:2::2 activate
 network 2003:3:2::/64
 network 2003:3:3::/64
!
```



BGP Configurations
Link Local Peering

Router A

```
interface e2
 ipv6 address 2001:412:ffco:1::1/64
!
router bgp 1
 no bgp default ipv4 unicast
 bgp router-id 1.1.1.1
 neighbor fe80::260:3eff:c043:1143 remote-as 2
 neighbor fe80::260:3eff:c043:1143 update source e2
address-family ipv6
 neighbor fe80::260:3eff:c043:1143 activate
 neighbor fe80::260:3eff:c043:1143 route-map next-hop out
!
route-map next-hop permit 5
 set ipv6 next-hop 2001:412:ffco:1::1
!
```



BGP Configuration
Filtering Prefixes

- **IOS Prefix-list is used for filtering prefixes in IPv4**
  - **And for IPv6 too!**
- **Example:**

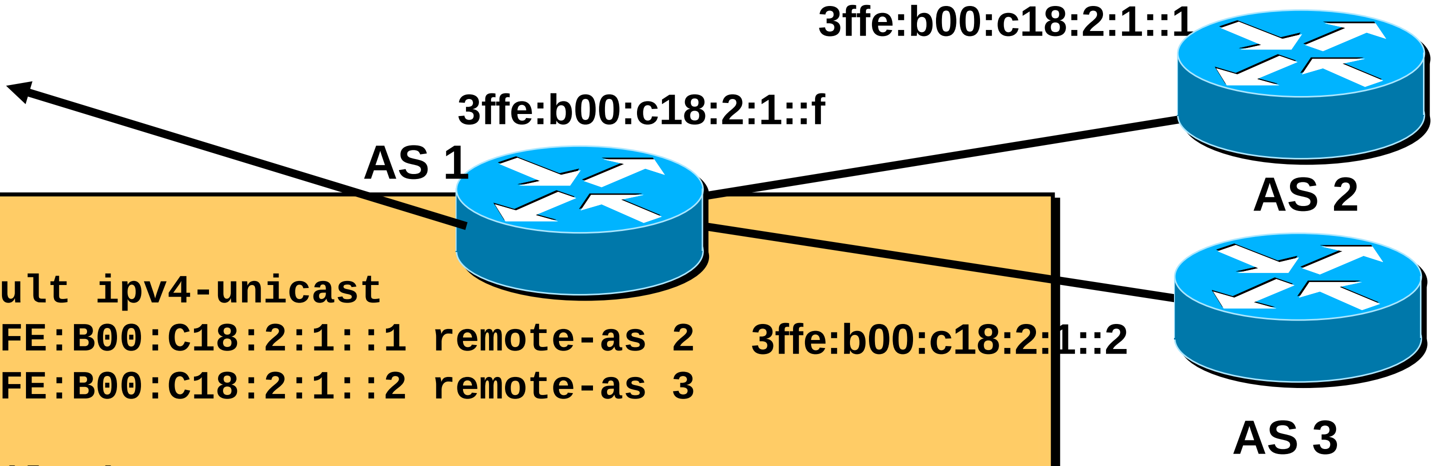
```
ipv6 prefix-list in-filter seq 5 permit 3ffe::/16 le 32
ipv6 prefix-list in-filter seq 6 permit 2001::/16 le 48
```

- **Apply to the BGP neighbor:**

```
router bgp 1
 no bgp default ipv4 unicast
 bgp router-id 1.1.1.1
 neighbor 3ffe:b00:ffff:2::2 remote-as 2
address-family ipv6
 neighbor 3ffe:b00:ffff:2::2 activate
 neighbor 3ffe:b00:ffff:2::2 prefix-list in-filter in
```

BGP Configuration
Manipulating Attributes

- **Prefer routes from AS 2 (local preference)**




```
router bgp 1
 no bgp default ipv4-unicast
 neighbor 3FFE:B00:C18:2:1::1 remote-as 2
 neighbor 3FFE:B00:C18:2:1::2 remote-as 3
!
 address-family ipv6
 neighbor 3FFE:B00:C18:2:1::1 activate
 neighbor 3FFE:B00:C18:2:1::1 prefix-list in-filter in
 neighbor 3FFE:B00:C18:2:1::1 route-map fromAS2 in
 neighbor 3FFE:B00:C18:2:1::2 activate
 neighbor 3FFE:B00:C18:2:1::2 prefix-list in-filter in
 network 3FFE:B00::/24
 exit-address-family
!
route-map fromAS2 permit 10
 set local-preference 120
```

BGP Configuration
Carrying IPv4 inside IPv6 peering

- **IPv4 prefixes can be carried inside an IPv6 peering**
  - **Note that we need to "fix" the next-hop**

- **Example**

```
router bgp 1
 neighbor 3ffe:b00:ffff:2::2 remote-as 2
!
address-family ipv4
 neighbor 3ffe:b00:ffff:2::2 activate
 neighbor 3ffe:b00:ffff:2::2 route-map ipv4 in
!
route-map ipv4 permit 10
 set ip next-hop 131.108.1.1
```

BGP Status Commands

- IPv6 BGP show commands take *ipv6* as argument

  show bgp ipv6 unicast *parameter*

```
Router1#show bgp ipv6 unicast 2017::/96
BGP routing table entry for 2017::/96, version 11
Paths: (1 available, best #1)
Local
    3FFE:B00:C18:2:1::1 from 3FFE:B00:C18:2:1::1 (10.10.20.2)
      Origin incomplete, localpref 100, valid, internal, best
```

BGP Status Commands

Display summary information regarding the state of the BGP neighbours

show bgp ipv6 unicast summary

```
BGP router identifier 128.107.240.254, local AS number 109
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
Dampening enabled. 3 history paths, 11 dampened paths
2 received paths for inbound soft reconfiguration
BGP activity 63094/62437 prefixes, 1887496/1878059 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:1458:C000::64B:4:1
                4   513 1294728  460213   400386    0    0 3d11h         498
```

Neighbour Information **BGP Messages Activity**

Conclusion

- BGP extended to support multiple protocols
  - IPv6 is but one more address family
- Operators experienced with IPv4 BGP should have no trouble adapting
  - Configuration concepts and CLI is familiar format

IPv4-IPv6 Co-existence/Transition

- **A wide range of techniques have been identified and implemented, basically falling into three categories:**

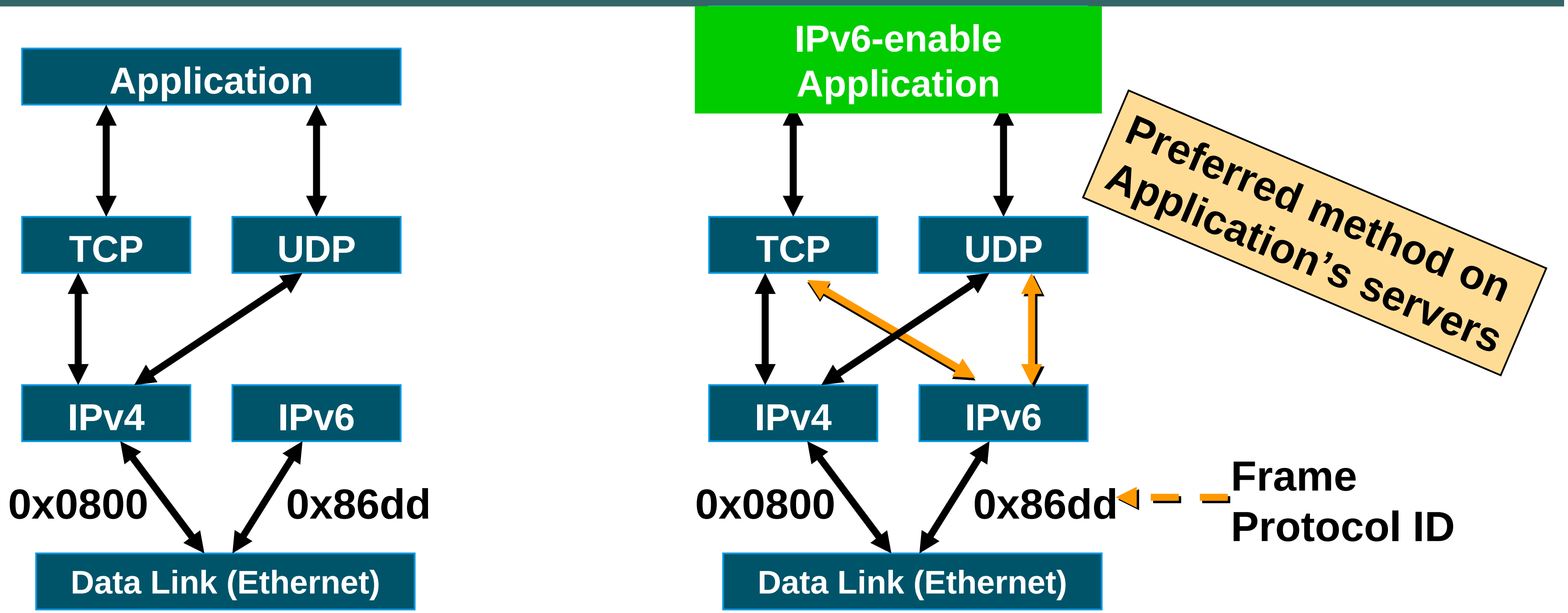
  (1) Dual-stack techniques, to allow IPv4 and IPv6 to co-exist in the same devices and networks

  (2) Tunneling techniques, to avoid order dependencies when upgrading hosts, routers, or regions

  (3) Translation techniques, to allow IPv6-only devices to communicate with IPv4-only devices

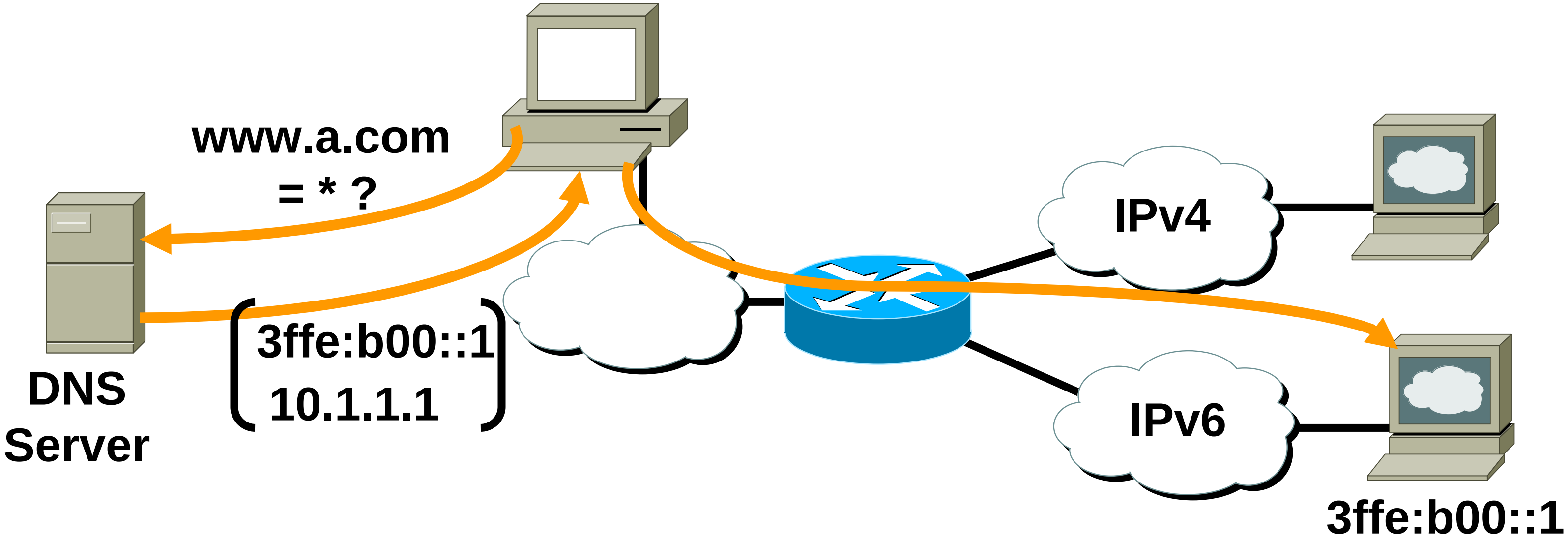
- **Expect all of these to be used, in combination**

Dual Stack Approach



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

Dual Stack Approach & DNS



- **In a dual stack case, an application that:**

  Is IPv4 and IPv6-enabled

  Asks the DNS for all types of addresses

  Chooses one address and, for example, connects to the IPv6 address

IOS IPv6 DNS Client Support

- IOS supports IPv6 DNS client
- Queries DNS servers for IPv6/IPv4:

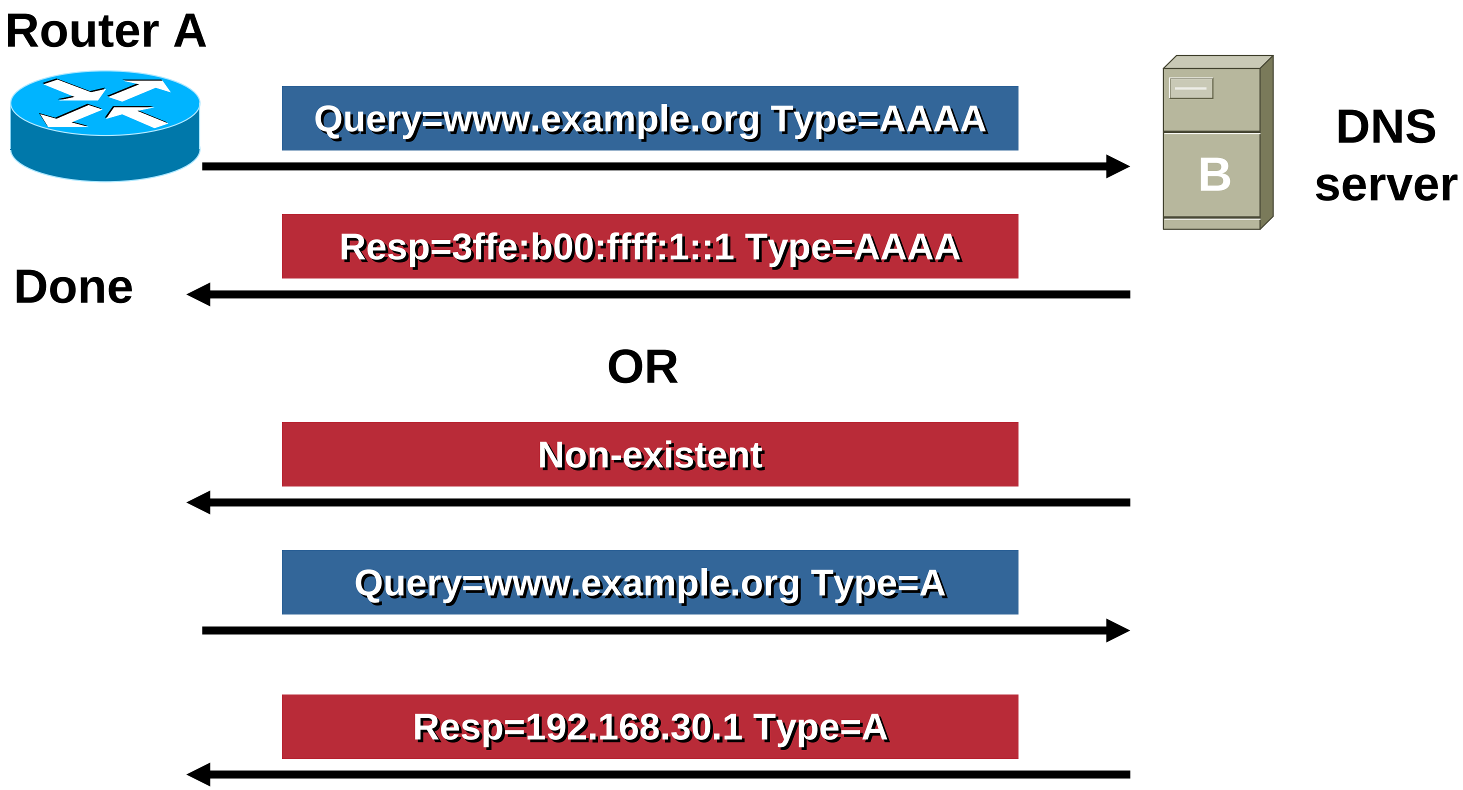
  First tries queries for an IPv6 address (AAAA record)

  If no IPv6 address exists, then query for an IPv4 address (A record)

  When both IPv6 and IPv4 records exists, the IPv6 address is picked first
- Static hostname to IPv6 address can also be configured
- Note: IPv6 stacks on Windows XP, Linux, FreeBSD, etc also pick IPv6 address before IPv4 address if both exist

  Check out www.kame.net for example

Example of DNS query



- DNS resolver picks IPv6 AAAA record first

IOS DNS configuration

- **DNS commands for IPv6**

  Define static name for IPv6 addresses

  ipv6 host <name> [<port>] <ipv6addr> [<ipv6addr> ...]

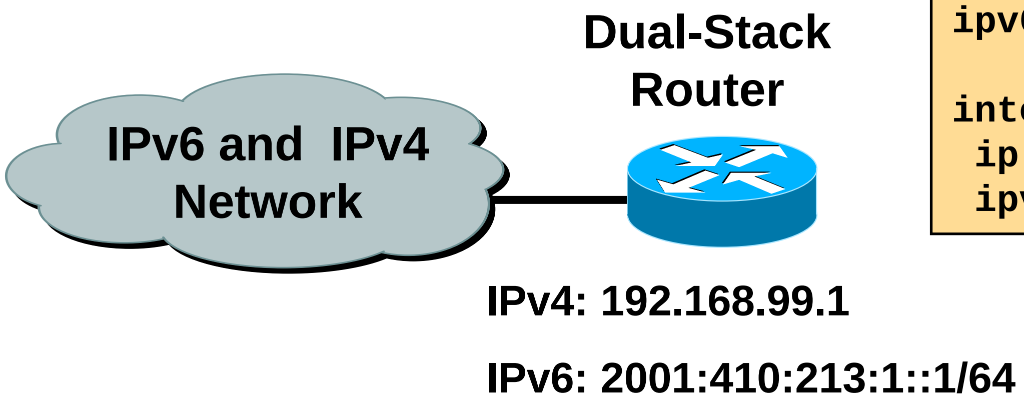
  Example: ipv6 host router1 3ffe:b00:ffff:b::1

  Configuring DNS servers to query

  ip name-server <address>

  Example: ip name-server 3ffe:b00:ffff:1::10

A Dual Stack Configuration




```
router#
ipv6 unicast-routing

interface Ethernet0
 ip address 192.168.99.1 255.255.255.0
 ipv6 address 2001:410:213:1::1/64
```

- **IPv6-enable router**

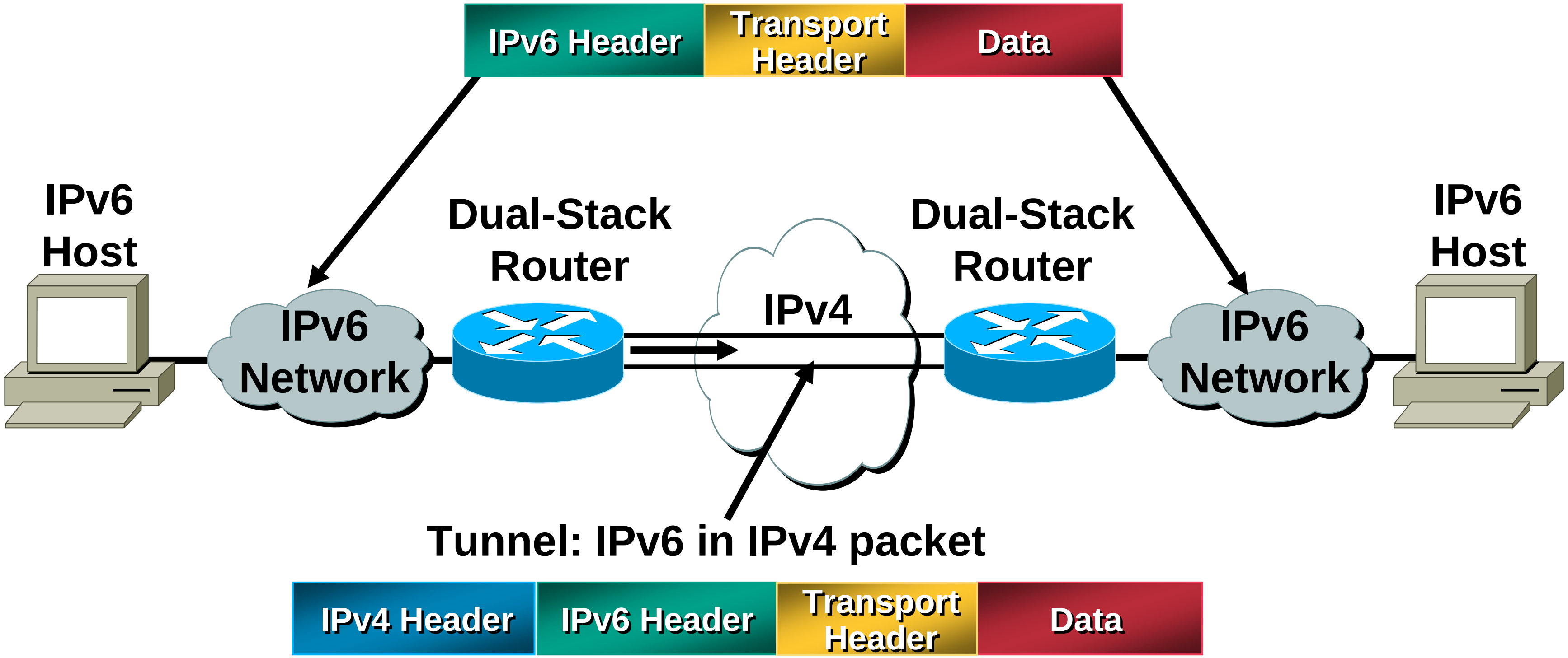
  If IPv4 and IPv6 are configured on one interface, the router is dual-stacked

  Telnet, Ping, Traceroute, SSH, DNS client, TFTP,…

Using Tunnels for IPv6 Deployment

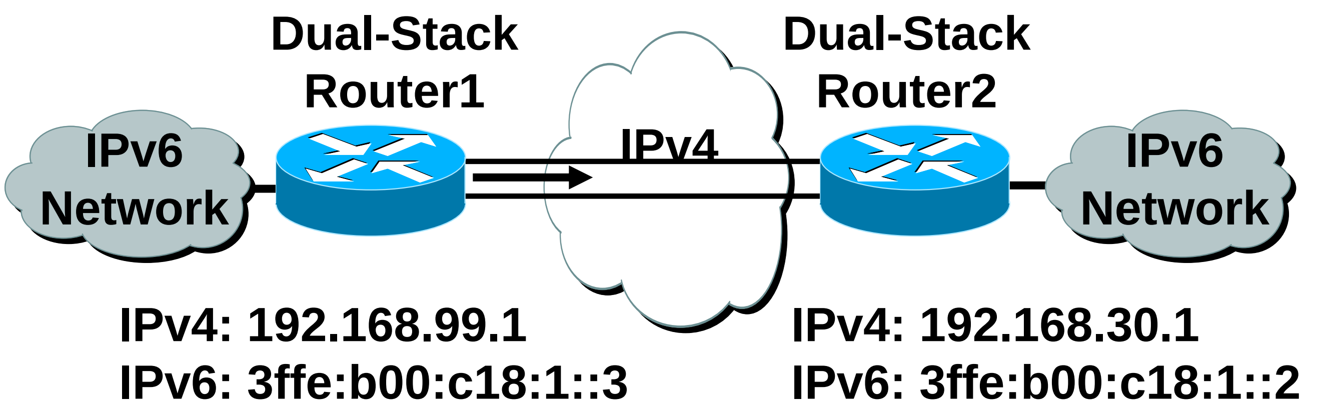
- **Many techniques are available to establish a tunnel:**
  - **Manually configured**
    - **Manual Tunnel (RFC 2893)**
    - **GRE (RFC 2473)**
  - **Semi-automated**
    - **Tunnel broker**
  - **Automatic**
    - **Compatible IPv4 (RFC 2893) : Deprecated**
    - **6to4 (RFC 3056)**
    - **6over4: Deprecated**
    - **ISATAP**

IPv6 over IPv4 Tunnels



- Tunneling is encapsulating the IPv6 packet in the IPv4 packet
- Tunneling can be used by routers and hosts

Manually Configured Tunnel (RFC2893)

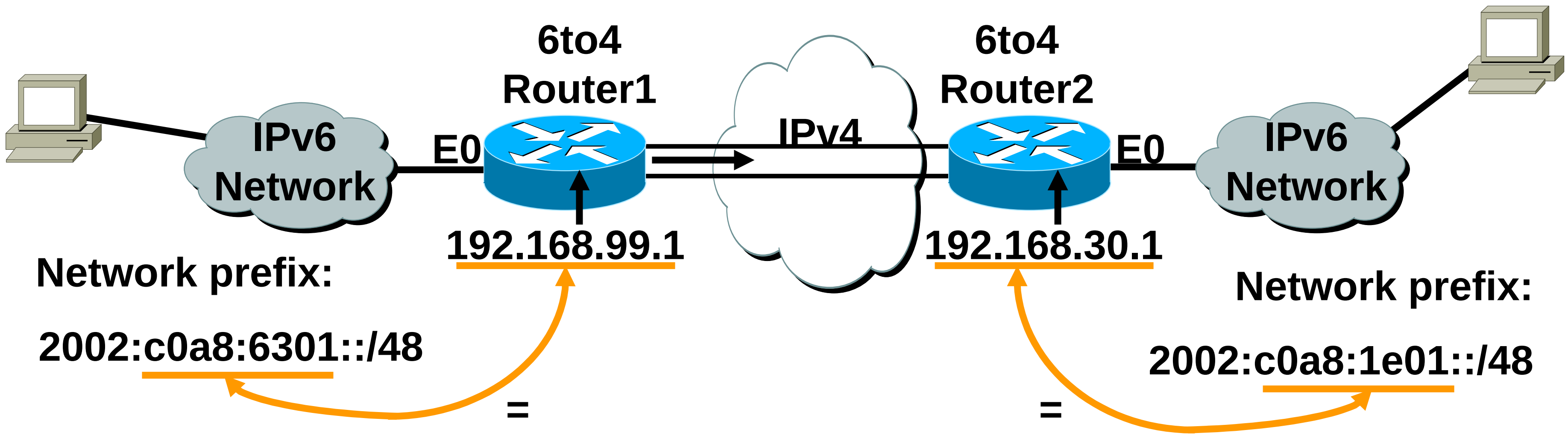



```
router1#

interface Tunnel0
 ipv6 address 3ffe:b00:c18:1::3/64
 tunnel source 192.168.99.1
 tunnel destination 192.168.30.1
 tunnel mode ipv6ip
```

```
router2#

interface Tunnel0
 ipv6 address 3ffe:b00:c18:1::2/64
 tunnel source 192.168.30.1
 tunnel destination 192.168.99.1
 tunnel mode ipv6ip
```

- **Manually Configured tunnels require:**
  - **Dual stack end points**
  - **Both IPv4 and IPv6 addresses configured at each end**

6to4 Tunnel (RFC 3056)



- **6to4 Tunnel:**

  Is an automatic tunnel method

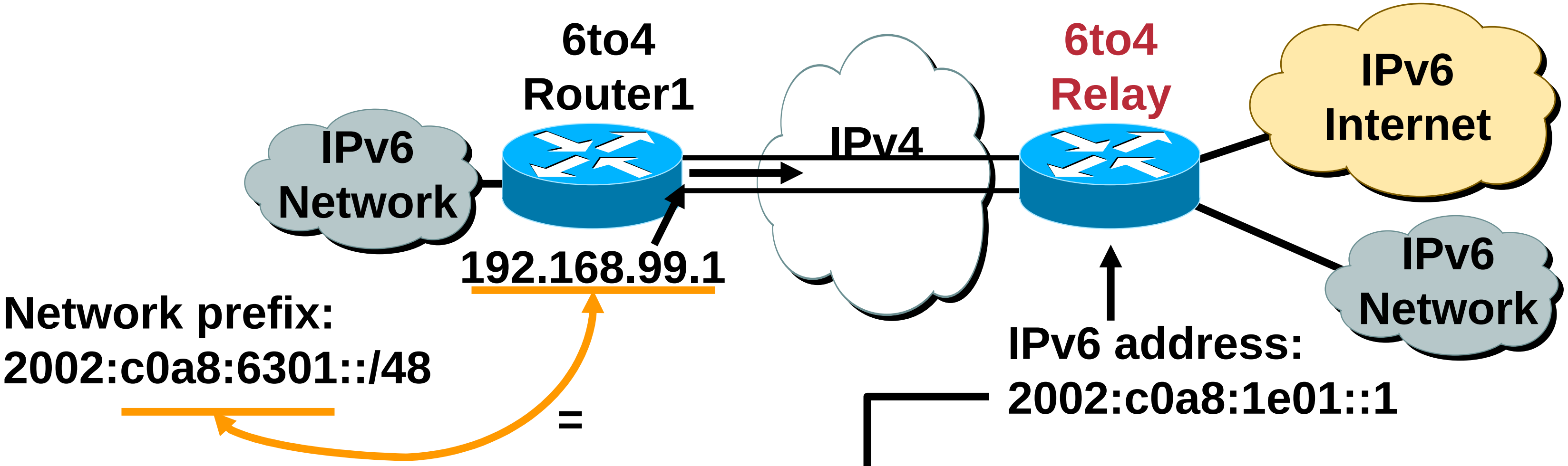
  Gives a prefix to the attached IPv6 network

  2002::/16 assigned to 6to4

  Requires one global IPv4 address on each Ingress/Egress site

```
router2#
interface Loopback0
 ip address 192.168.30.1 255.255.255.0
 ipv6 address 2002:c0a8:1e01:1::/64 eui-64
interface Tunnel0
 no ip address
 ipv6 unnumbered Ethernet0
 tunnel source Loopback0
 tunnel mode ipv6ip 6to4

ipv6 route 2002::/16 Tunnel0
```

6to4 Relay




```
router1#
interface Loopback0
 ip address 192.168.99.1 255.255.255.0
 ipv6 address 2002:c0a8:6301:1::/64 eui-64
interface Tunnel0
 no ip address
 ipv6 unnumbered Ethernet0
 tunnel source Loopback0
 tunnel mode ipv6ip 6to4

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

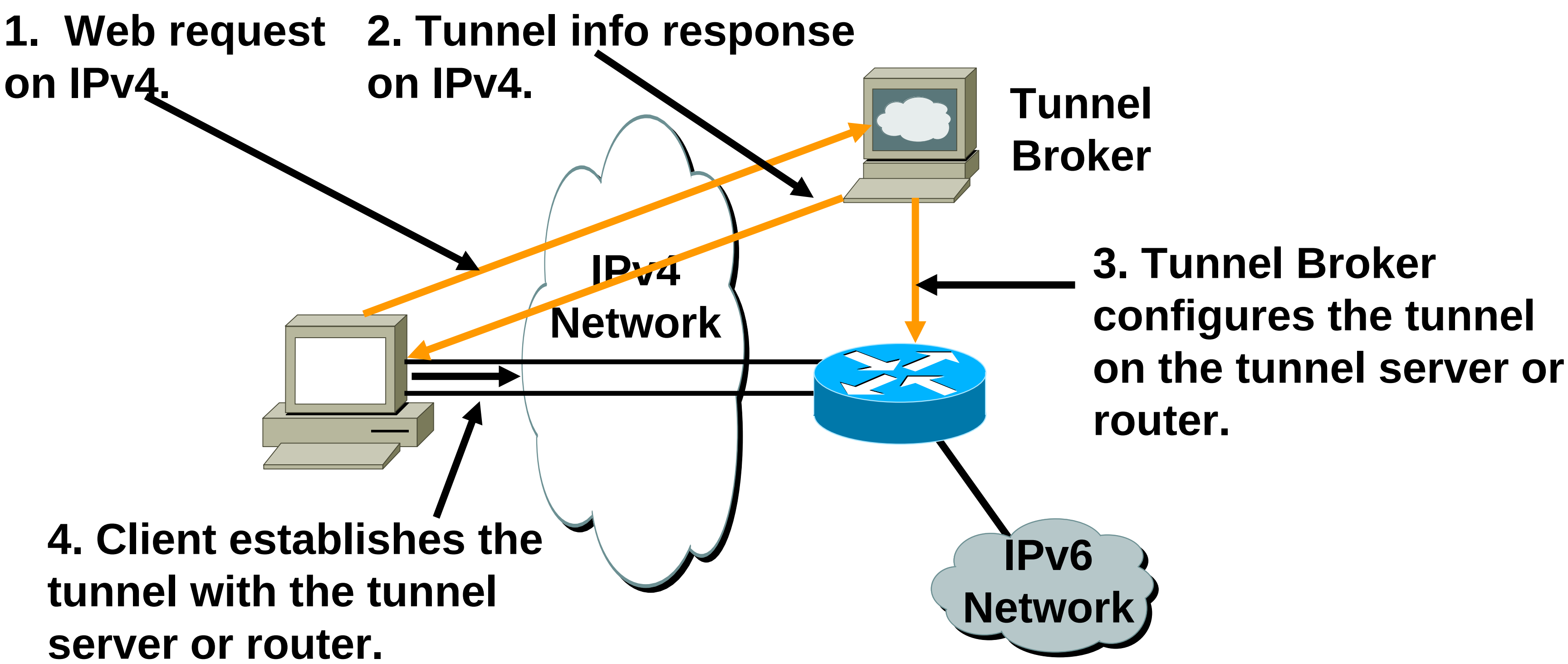
- **6to4 relay:**

  Is a gateway to the rest of the IPv6 Internet

  Default router

  Anycast address (RFC 3068) for multiple 6to4 Relay

Tunnel Broker

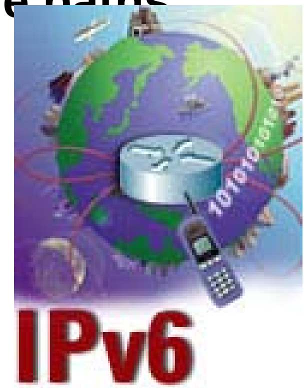


- **Tunnel broker:**

  Tunnel information is sent via http-ipv4

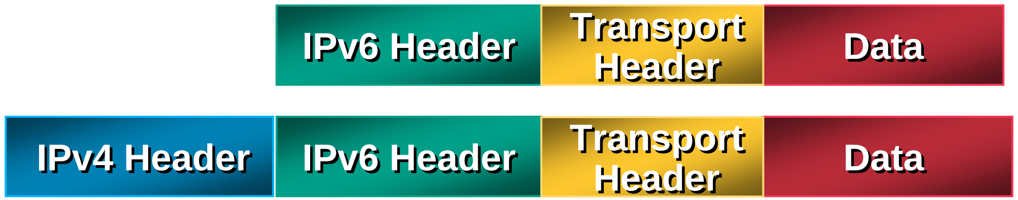
IPv6 Deployment Scenarios

- **Many ways to deliver IPv6 services to End Users**
  - **End-to-end IPv6 traffic forwarding is the Key feature**
  - **Minimize operational upgrade costs**
- **Service Providers and Enterprises may have different deployment needs**
  - **Incremental Upgrade/Deployment**
  - **ISP's differentiate Core and Edge infrastructures upgrade**
  - **Enterprise Campus and WAN may have separate upgrade paths**
- **IPv6 over IPv4 tunnels**
- **Dedicated Data Link layers for native IPv6**
- **Dual stack Networks**
  - **IPv6 over MPLS or IPv4-IPv6 Dual Stack Routers**



IPv6 over IPv4 Tunnels

- **Several Tunnelling mechanisms defined by IETF**
  - **Apply to ISP and Enterprise WAN networks**
    - **GRE, Configured Tunnels, Automatic Tunnels using IPv4 compatible IPv6 Address, 6to4**
  - **Apply to Campus**
    - **ISATAP**
- **Leverages 6Bone experience**
- **No impact on Core infrastructure**
  - **Either IPv4 or MPLS**



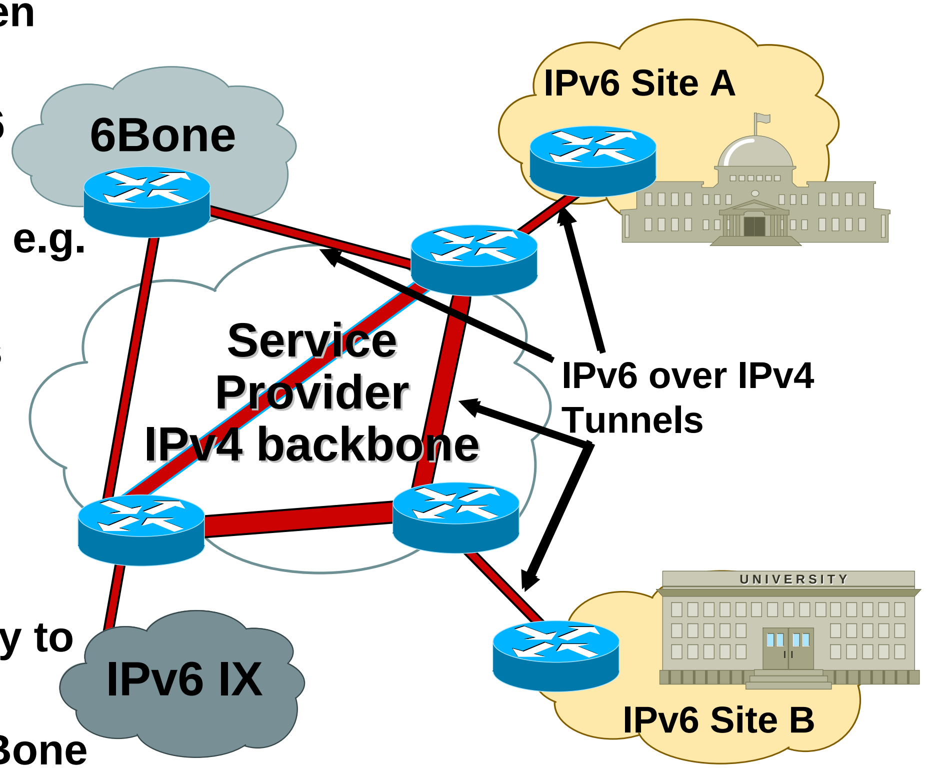
Native IPv6 over Dedicated Data Links

- **Native IPv6 links over dedicated infrastructures**
  - **ATM PVC, dWDM Lambda, Frame Relay PVC, Serial, Sonet/SDH, Ethernet**
- **No impact on existing IPv4 infrastructures**
  - **Only upgrade the appropriate network paths**
  - **IPv4 traffic (and revenues) can be separated from IPv6**
- **Network Management done through IPv4**

IPv6 Tunnels & Native Case Study

- ISP scenario
  - Configured Tunnels or Native IPv6 between IPv6 Core Routers
  - Configured Tunnels or Native IPv6 to IPv6 Enterprise's Customers
  - Tunnels for specific access technologies, e.g. Cable
  - MP-BGP4 Peering with other 6Bone users
  - Connection to an IPv6 IX
  - 6to4 relay service
- Enterprise/Home scenario
  - 6to4 tunnels between sites, use 6to4 Relay to connect to the IPv6 Internet
  - Configured tunnels between sites or to 6Bone users
  - ISATAP tunnels or Native IPv6 on a Campus

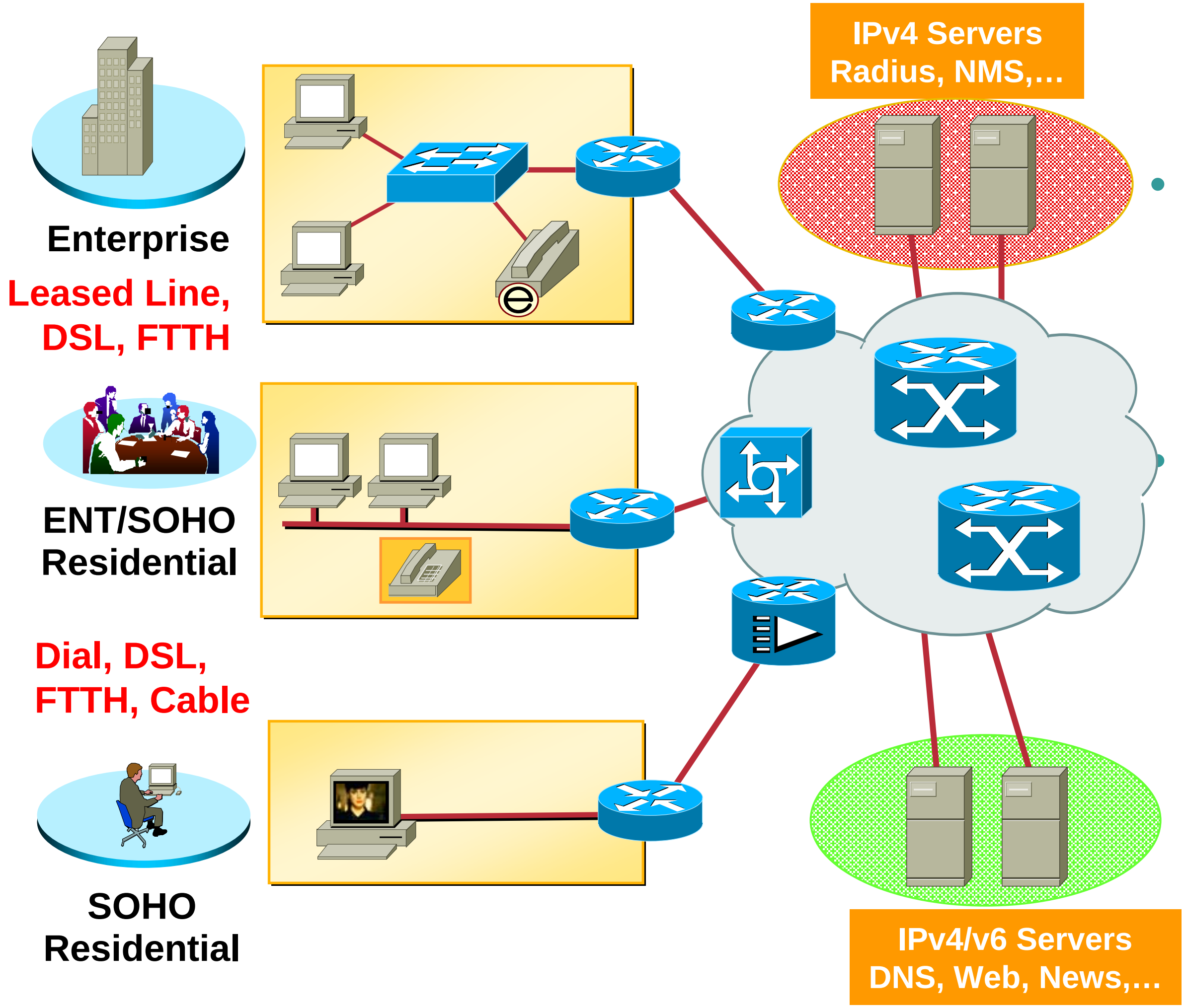
Use the most appropriate



Dual Stack IPv4-IPv6 Infrastructure

- It is generally a long term goal when IPv6 traffic and users will be rapidly increasing
- May be easier on network's portion such as Campus or Access networks
- Theoretically possible but the network design phase has to be well planned
  - Memory size to handle the growth for both IPv4 & IPv6 routing tables
  - IGP options & its management: Integrated versus "Ships in the Night"
  - Full network upgrade impact
- IPv4 and IPv6 Control & Data planes should not impact each other
  - Feedback, requirements & experiments are welcome

Dual Stack IPv4-IPv6 Case Study



- Campus scenario

  Upgrade all layer 3 devices to allow IPv6 hosts deployment anywhere, similar to IPX/IP environment

- ISP

  Access technologies may have IPv4 dependencies, eg. for User's management

  Transparent IPv4-IPv6 access services

  Core may not go dual-stack before sometimes to avoid a full network upgrade

IPv6 over MPLS Infrastructure

- **Service Providers have already deployed MPLS in their IPv4 backbone for various reasons**

  MPLS/VPN, MPLS/QoS, MPLS/TE, ATM + IP switching

- **Several IPv6 over MPLS scenarios**

  IPv6 Tunnels configured on CE (no impact on MPLS)

  IPv6 over Circuit_over_MPLS (no impact on IPv6)

  IPv6 Provider Edge Router (6PE) over MPLS (no impact on MPLS core)

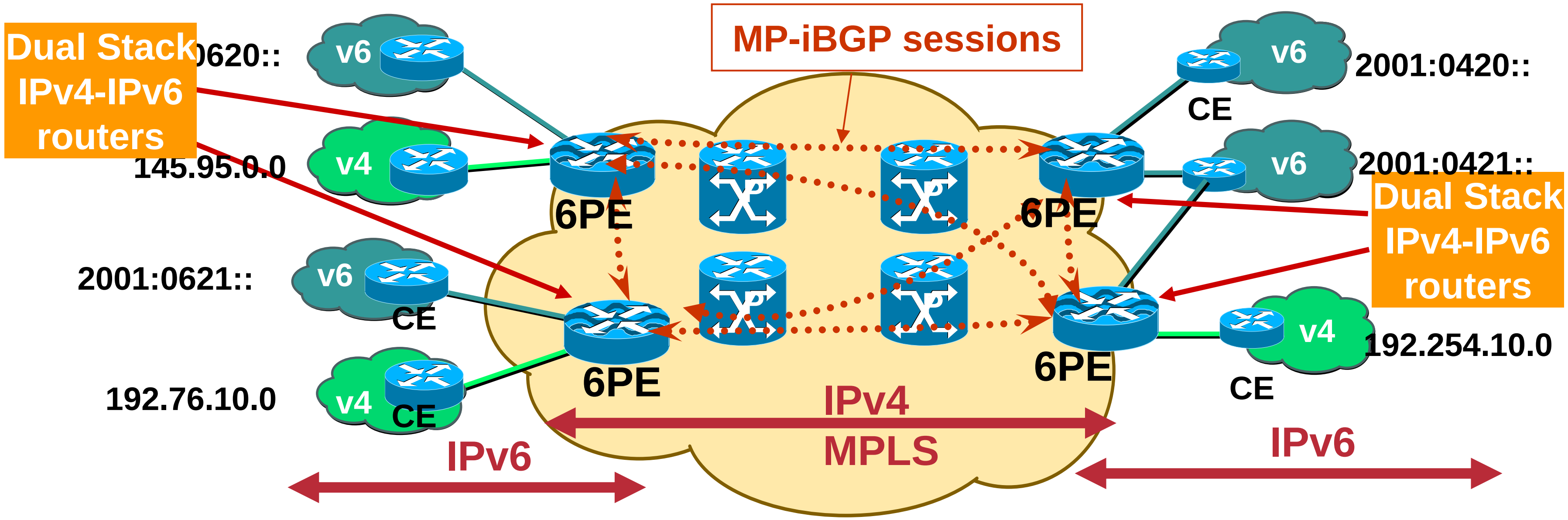
  Native IPv6 MPLS (require full network upgrade)

- **Upgrading software to IPv6 Provider Edge Router (6PE)**

  Low cost and risk as only the required Edge routers are upgraded or installed

  Allows IPv6 Prefix delegation by ISP

IPv6 Provider Edge Router (6PE) over MPLS



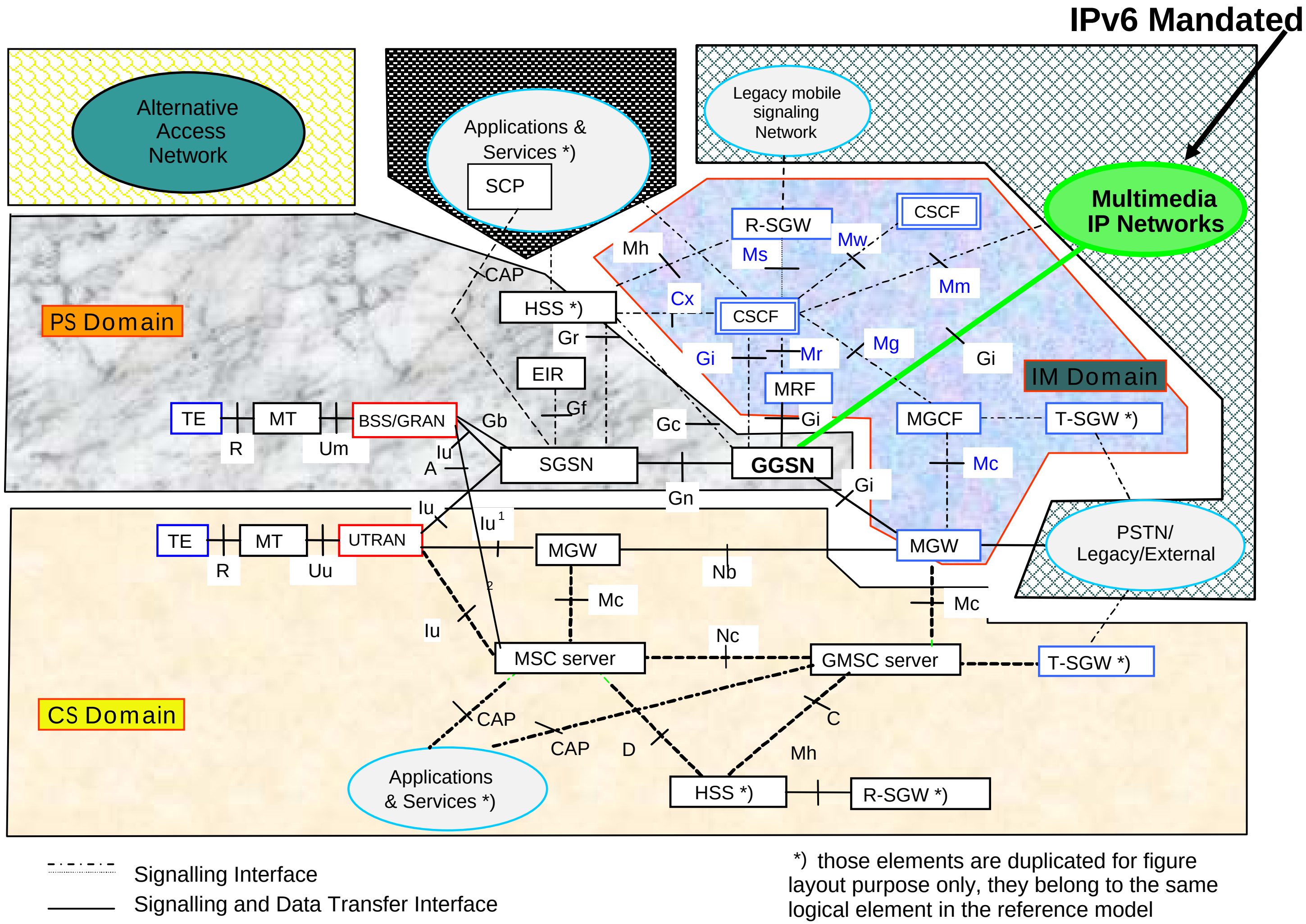
- IPv4 or MPLS core infrastructure is IPv6-unaware
- PEs are updated to support Dual Stack/6PE
- IPv6 reachability exchanged among 6PEs via iBGP
- IPv6 packets transported from 6PE to 6PE inside MPLS

3GPP/UMTS Release 5: a 6PE Application

GPRS Access Network

MPLS offers ATM + IP + IPv6 switching

MS Circuit Switch Access Network



Signalling Interface

Signalling and Data Transfer Interface

*) those elements are duplicated for figure layout purpose only, they belong to the same logical element in the reference model

IM Domain is now a sub-set of the PS Domain

Native IPv6-only Infrastructure?

- **Application's focus**

  When will the IPv6 traffic be important enough?

- **Requires**

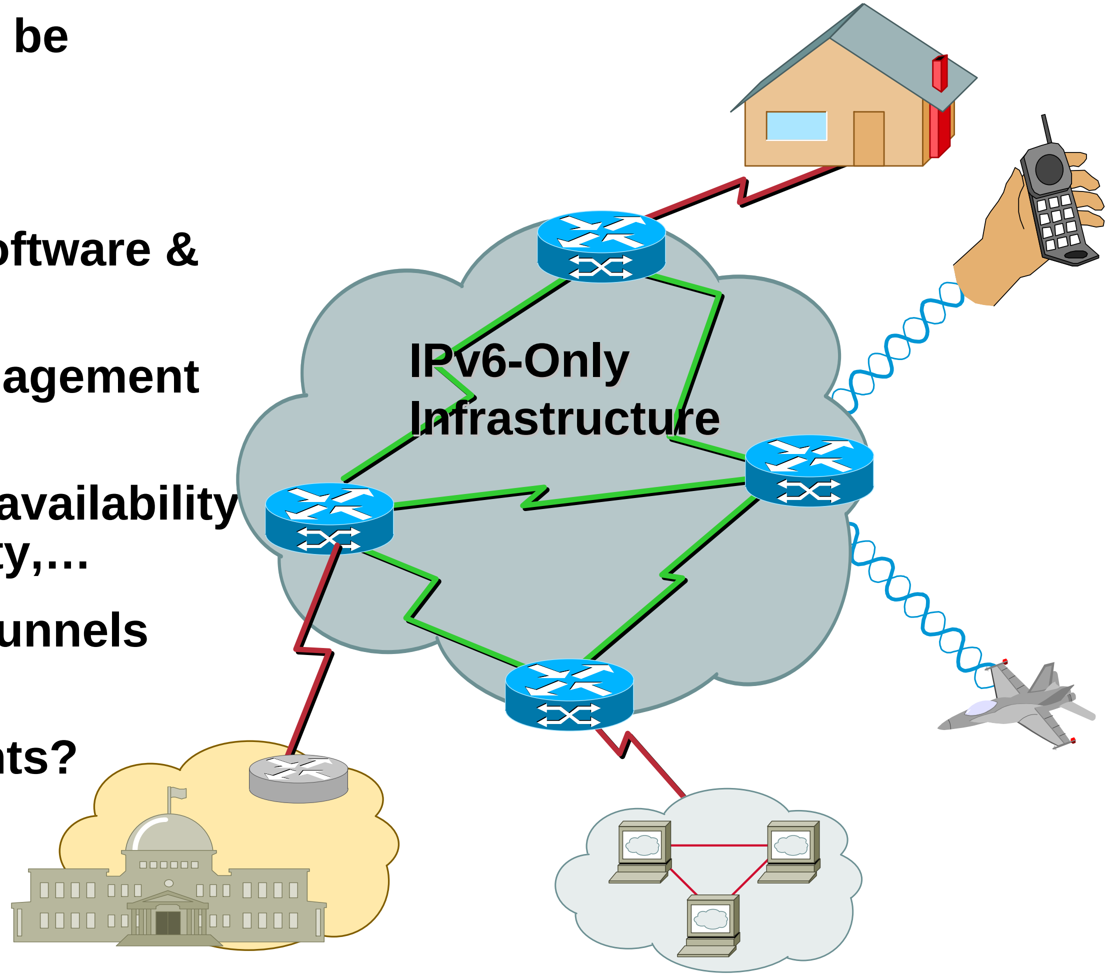
  Full Network upgrade (software & potentially hardware)

  Native IPv6 Network Management Solutions

  Enhanced IPv6 services availability
  Multicast, QoS, security,…

  Transport IPv4 through tunnels over IPv6

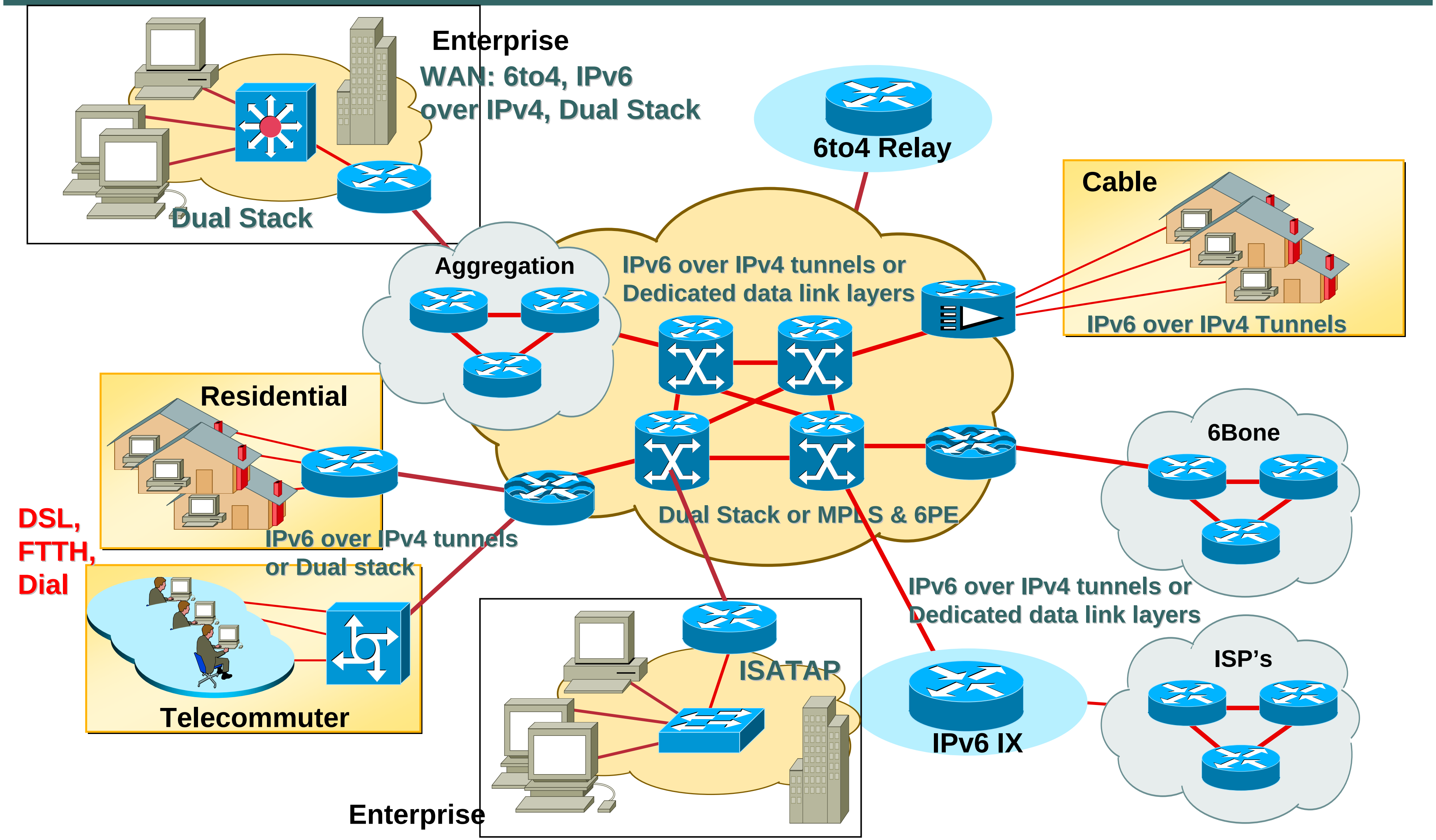
  IPv4 traffic requirements?



IPv6 Deployment Phases

Phases	Benefits
IPv6 Tunnels over IPv4	Low cost, low risk to offer IPv6 services. No infrastructure change. Has to evolve when many IPv6 clients get connected
Dedicated Data Link layers for Native IPv6	Natural evolution when connecting many IPv6 customers. Require a physical infrastructure to share between IPv4 and IPv6 but allow separate operations
MPLS 6PE	Low cost, low risk , it requires MPLS and MP-BGP4. No need to upgrade the Core devices , keep all MPLS features (TE, IPv4-VPN)
Dual stack	Requires a major upgrade. Valid on Campus or Access networks as IPv6 hosts may be located anywhere
IPv6-Only	Requires upgrading all devices. Valid when IPv6 traffic will become predominant

Moving IPv6 to Production



Recent IPv6 "Hot Topics" in the IETF

- Multi-homing
- Address selection
- Address allocation
- DNS discovery
- 3GPP usage of IPv6
- Anycast addressing
- Scoped address architecture
- Flow-label semantics
- API issues

  (flow label, traffic class, PMTU discovery, scoping,…)

- Enhanced router-to-host info
- Site renumbering procedures
- Inter-domain multicast routing
- Address propagation and AAA issues of different access scenarios
- End-to-end security vs. firewalls
- And, of course, transition / co-existence / interoperability with IPv4 (a bewildering array of transition tools and techniques)

Note: this indicates vitality, not incompleteness, of IPv6!