

Chapter 2

Internet Protocol Overview

By Pavan Poudel

Overview

1. TCP/IP and the IP Layer overview
2. IPv4 and IPv6 Address Types and Formats
3. IPv4 and IPv6 Header Structure
4. Internet RFCs

TCP/IP Reference Model

- The The U.S. Department of Defense (DoD) created the TCP/IP reference model, because it wanted to design a network that could survive any conditions, including a nuclear war.
- In a world connected by different types of communication media such as copper wires, microwaves, optical fibres and satellite links, the DoD wanted transmission of packets every time and under any conditions.
- This very difficult design problem brought about the creation of the TCP/IP model.
- TCP/IP was developed as an open standard. This meant that anyone was free to use TCP/IP. This helped speed up the development of TCP/IP as a standard.
- The TCP/IP model has the following four layers:
 - Application layer
 - Transport layer
 - Internet layer
 - Network access layer /Host-to-network layer

TCP/IP Reference Model



Network Access/ Host to Network (Layer 1)

- Network Access Layer is the first layer of the four layer TCP/IP model.
- Network Access layer defines details of how data is physically sent through the network, including how bits are electrically or optically signalled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fibre, or twisted pair copper wire.
- The protocols included in Network Access layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.
- The most popular LAN architecture among those listed above is Ethernet.
- Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to access the media. An Access Method determines how a host will place data on the medium.

The Internet Layer (Layer 2)

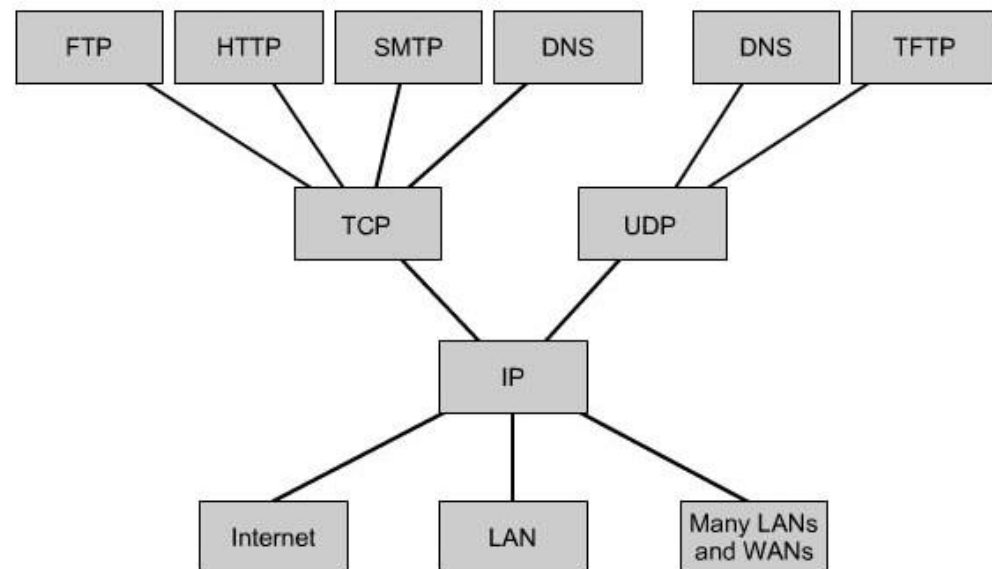
- Network address
- Best path determination
- Data transmission between the subnet
- Protocol Data Unit(PDU): Datagram / Packet

Transport Layer (Layer 3)

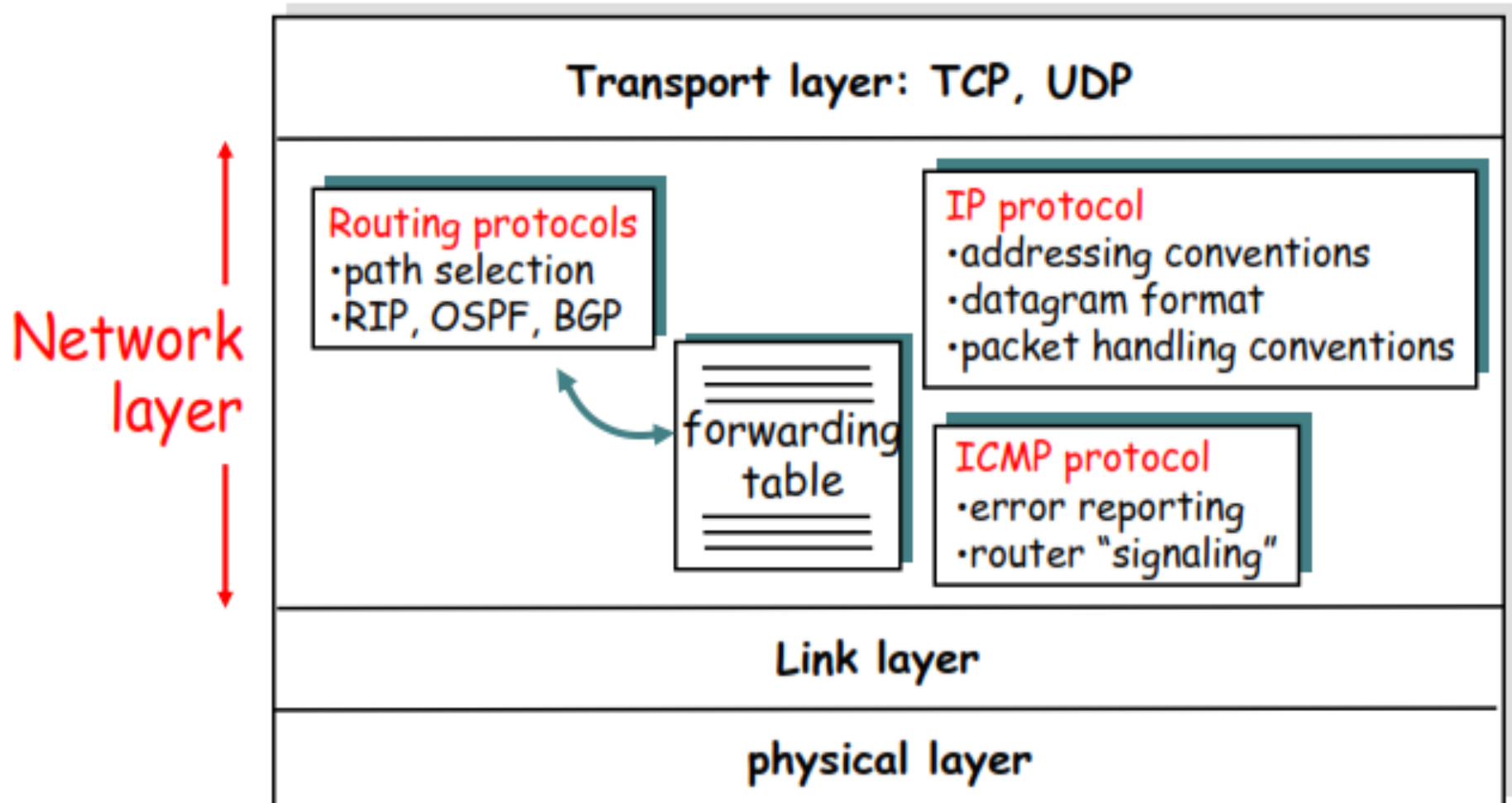
- End to end connection
- Process are addressed
- Transportation issue between the host
- Reliable data transfer between the host
- Establish connection between the host
- Flow control and congestion control
- Error detection and recovery
- Protocol Data Unit (PDU): Segment

Application Layer (Layer 4)

- Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol), DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.
- Application for the user for network use
- Provide the different network services to the user
- Protocol Data Unit (PDU): Data



IP Layer Overview



IPv4 Address Notation

- IP v4 is 32 bits long.
- Thus a total of 2^{32} (4,294,967,296 i.e. nearly 4 billion) IP address is possible in IPv4.
- These address are typically written in so called dotted-decimal notation.
 - e.g. 202.70.91.200
 - $(202)_{10} = (11001010)_2$
- Each interface on every host and router in the global Internet must have an IP address that is globally Unique.
- IPv4 Supported Address Types:
 - Unicast Address
 - Multicast Address
 - Broadcast Address

IPv4 Addressing

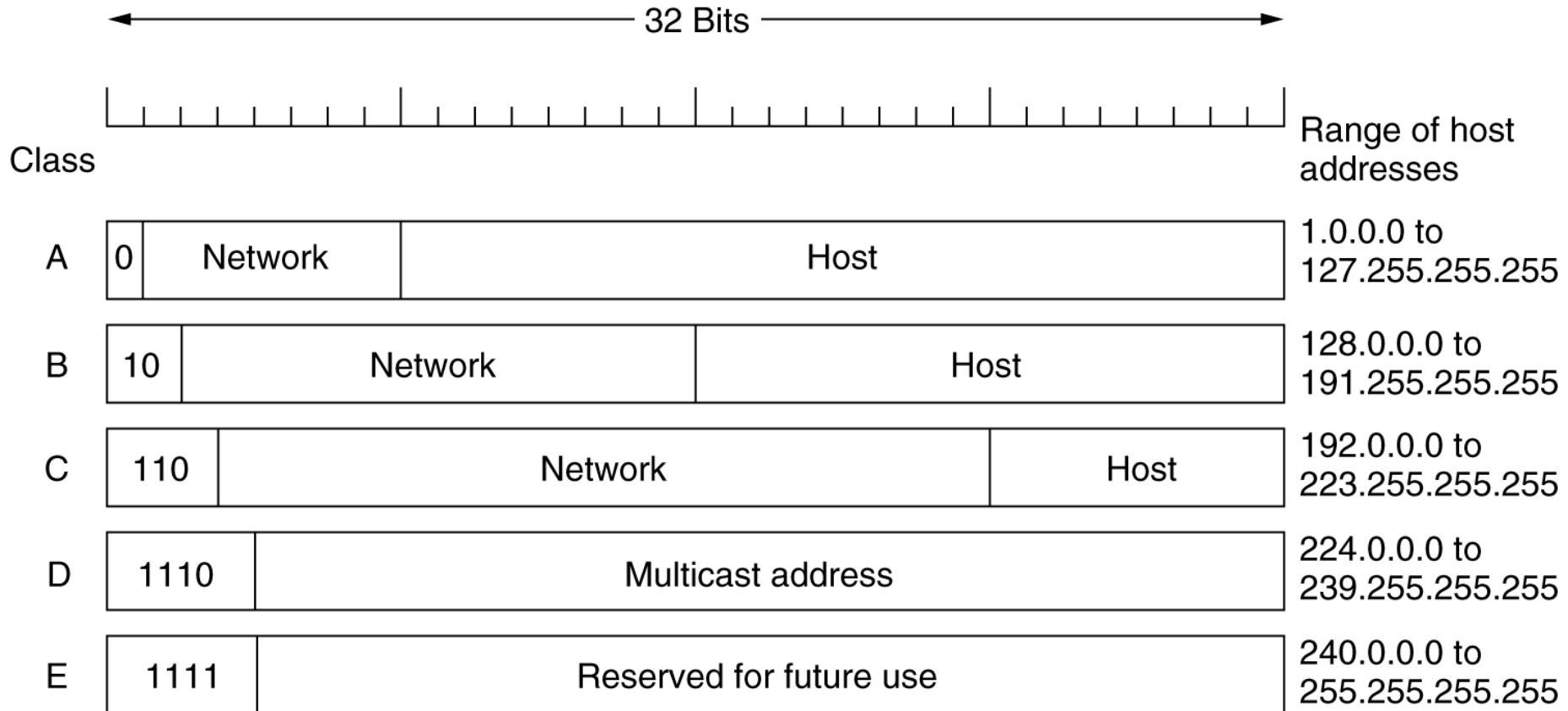
- 32 bits of IP address is divided into network and host portion.

Network

Host

- Classes
 - A (8 bits is used for networks and rest 24 bits for host)
 - B (16 bits is used for networks and rest 16 bits for host)
 - C (24 bits is used for networks and rest 8 bits for host)
 - D (Used for Multicasting)
 - E (For Future Use)

Class-full IPv4 Address



IPV4 Address Class

- **Class A**

- Range : 0 – 127
- So total of 126 (2^8-2) Networks are possible and total host = 2^{24} in each Network.
- Default subnet mask is 255.0.0.0

- **Class B**

- Range : 128 – 191
- So total of $2^{16}-2$ Networks are possible and total host = 2^{16} in each Network.
- Default subnet mask is 255.255.0.0

IPv4 Address Class

- **Class C**
 - Range : 192 – 223
 - So total of $2^{24}-3$ Networks are possible and total host = 2^8 in each Network.
 - Default subnet mask is 255.255.255.0
- **Class D**
 - Range : 224 – 239
 - Used for Multicasting
 - E.g. 224.0.0.1 (group)
- **Class E**
 - Range 240-255
 - Not used (for future use)

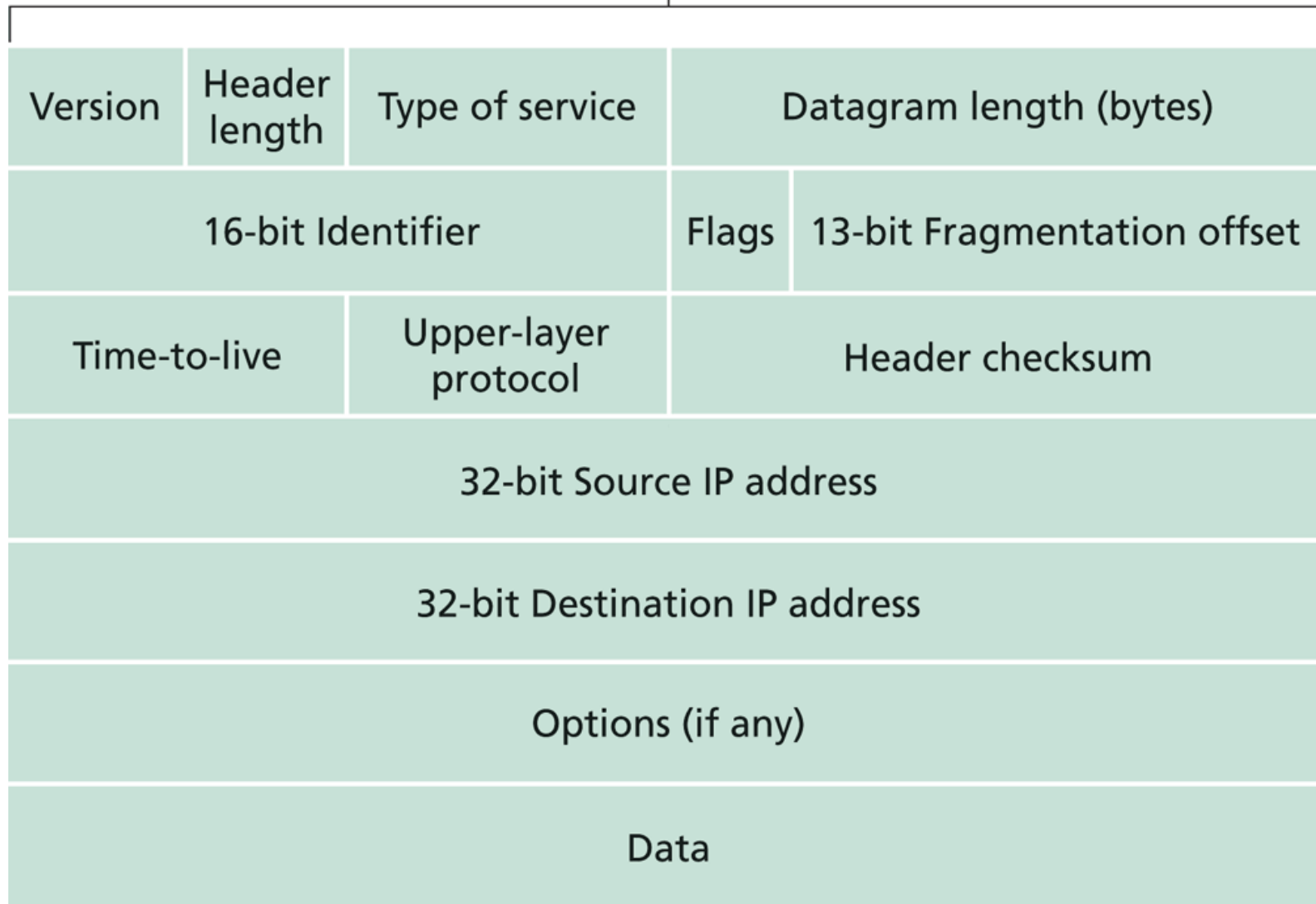
Public and Private IP Address

- Public IP globally Unique
 - e.g. 202.70.91.7
- Visible to public, people can access your device.
- Private IP significant in Local Sites only.
- Private IP are commonly used when the public IP couldn't be obtained for all devices.
- Private IP address Range:

IP Classes	Private IP Address Range
Class A	10.0.0.0 – 10.255.255.255
Class B	172.16.0.0 – 172.31.255.255
Class C	192.168.0.0 – 192.168.255.255

IPv4 Datagram Format

32 bits



IPv4 Datagram Format

- ***Version (4 bits)***: Specify the IP Protocol version of Datagram
- ***Header Length (4 bits)***: Because an IPV4 datagram can contain a variable number of options these four bits are needed to determine where in the IP datagram the data actually begins(minimum HLEN = 20 bytes).
- ***Type of Service (8 bits)***: TOS is included in the IPv4 header to allow different types of IP datagram(e.g. datagram particularly requiring low delay, high throughput , or reliability) to be distinguished from other. Eg. Realtime data requires fast delivery, file transfer requires reliability.
- ***Datagram Length(16 bits)***: contains the total length of datagram (Header+ Datagram)

IPv4 Datagram Format

- ***Identifier, flag and Fragmentation offset*** : used for IP fragmentation.
 - *Identification (16 bits)* : Datagram identification for fragments
 - *DF* : Don't Fragment
 - *MF* : More Fragments
 - *Fragment Offset (13 bits)*: location of current frame in datagram
- ***Time to Live (8 bits)*** : to ensure that the datagram don't circulate forever in the network. Limits Packet Life. In practice, just counts hops. Each router decrements the TTL and upon hitting 0, packet is discarded.
- ***Upper layer Protocol(8bits)***: These 8 bits are used to identify the next level protocol above the IP that is to receive the datagram. TCP or UDP

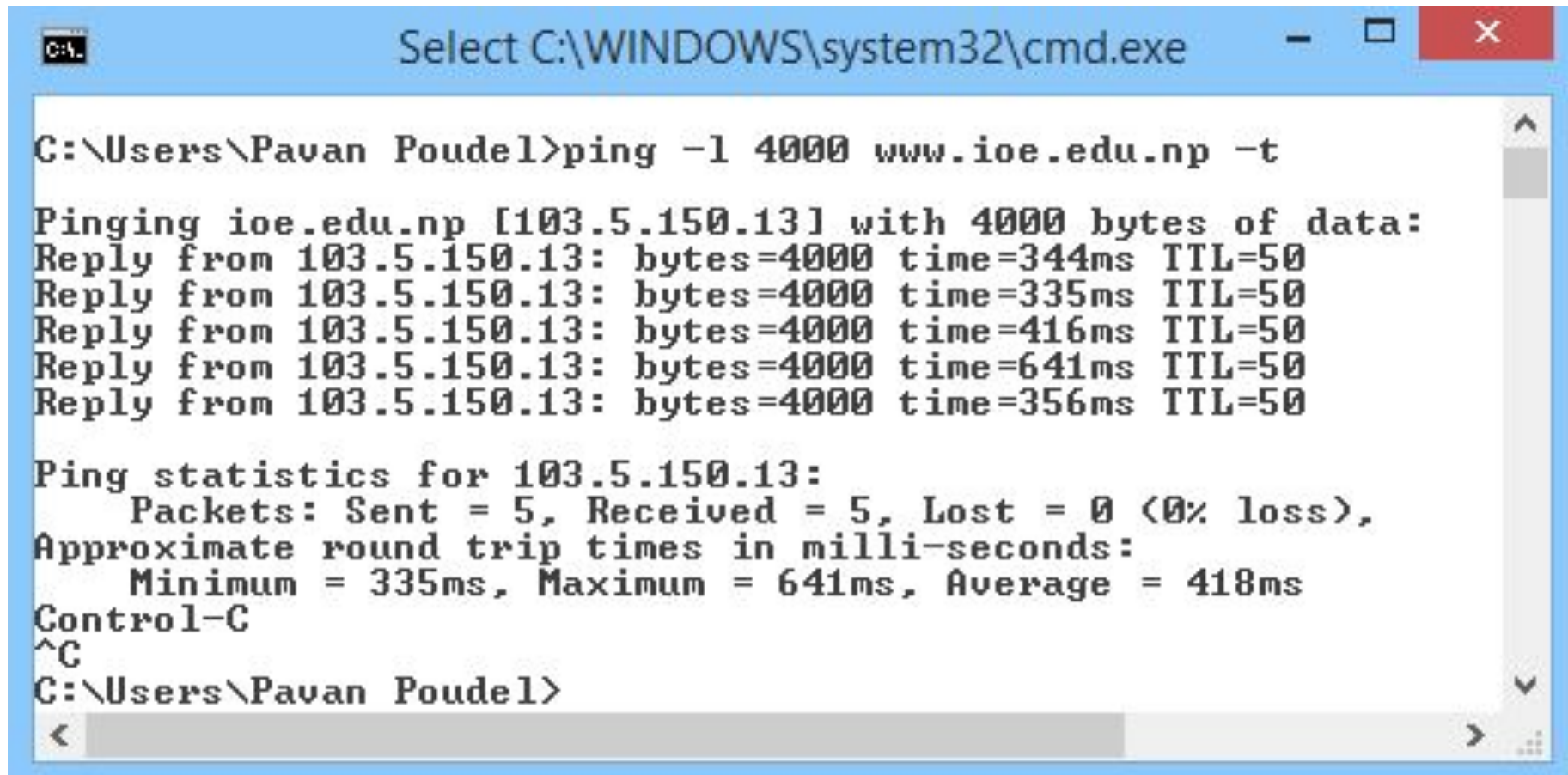
IPv4 Datagram Format

- ***Header Check sum (16 bits):*** used to detect a error that may occur in the header
- ***Source and Destination address:*** Carries 32 bit source and destination address
- ***Options:*** used to identify several additional services, not used in every datagram
- ***Data:*** contains the user data

Datagram Fragmentation and Re-assembly

- MTU(Maximum Transfer Unit) is defined for a network link. Eg. MTU for Ethernet packet is usually 1500 bytes
- So, if data size is greater than MTU, it must be fragmented into smaller packet before transmitting to the link and re-assembled at receiver side to get original packet.
- In case of IPv4, Fragmentation is done at router just before the link with smaller MTU (where as, in case of IPv6, it must be done by the sender)
- For each Fragment, Header must be attached with Datagram ID, offset and Flag.

Datagram Fragmentation and Re-assembly

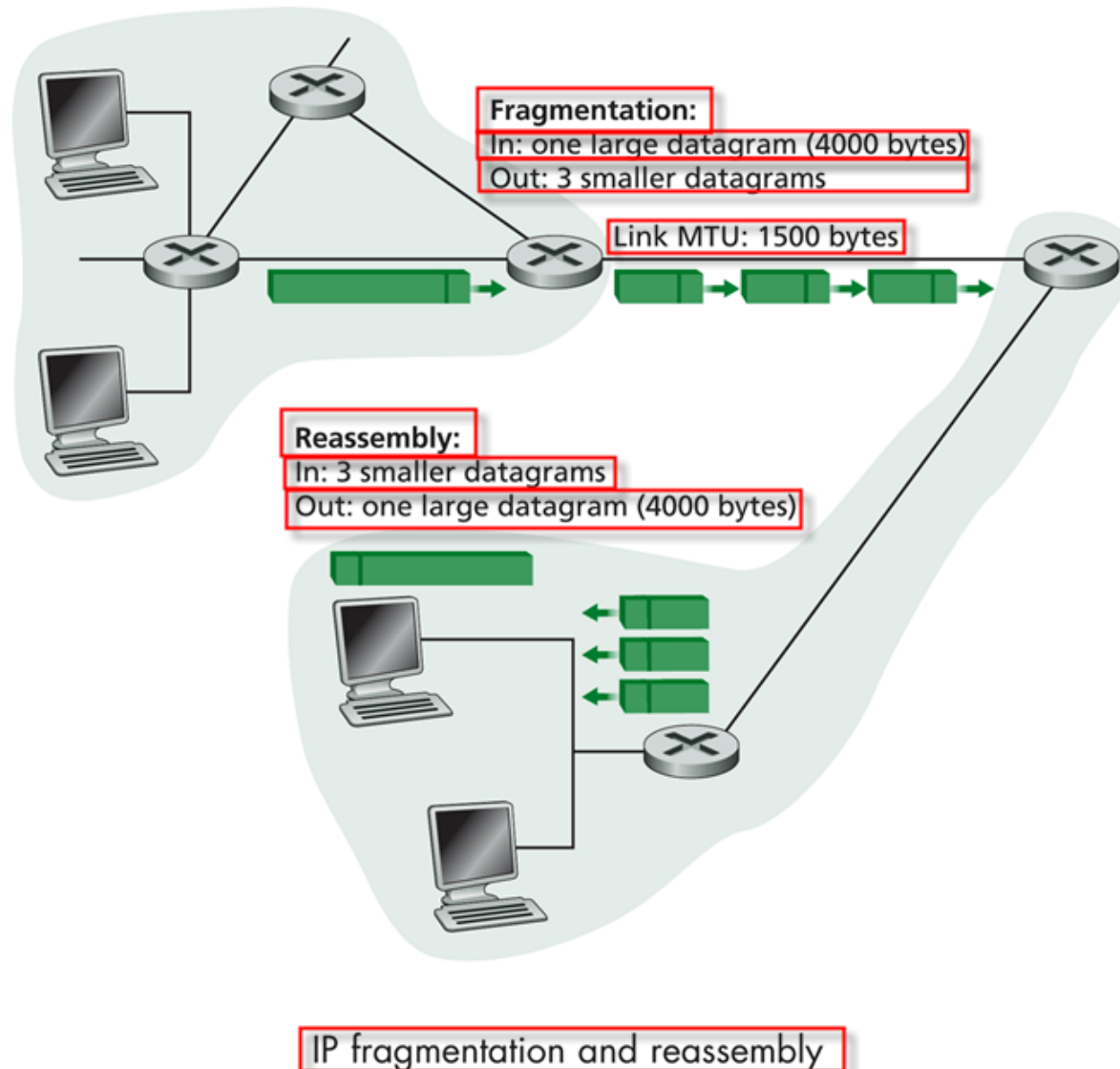


```
C:\Users\Pavan Poudel>ping -l 4000 www.ioe.edu.np -t

Pinging ioe.edu.np [103.5.150.13] with 4000 bytes of data:
Reply from 103.5.150.13: bytes=4000 time=344ms TTL=50
Reply from 103.5.150.13: bytes=4000 time=335ms TTL=50
Reply from 103.5.150.13: bytes=4000 time=416ms TTL=50
Reply from 103.5.150.13: bytes=4000 time=641ms TTL=50
Reply from 103.5.150.13: bytes=4000 time=356ms TTL=50

Ping statistics for 103.5.150.13:
    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 335ms, Maximum = 641ms, Average = 418ms
Control-C
^C
C:\Users\Pavan Poudel>
```

Datagram Fragmentation and Re-assembly



Datagram Fragmentation and Re-assembly

Datagram Size = 4000

Actual data size = 4000-20
= 3980 bytes

MTU = 1500 including 20 byte header

So fragmented packet size:

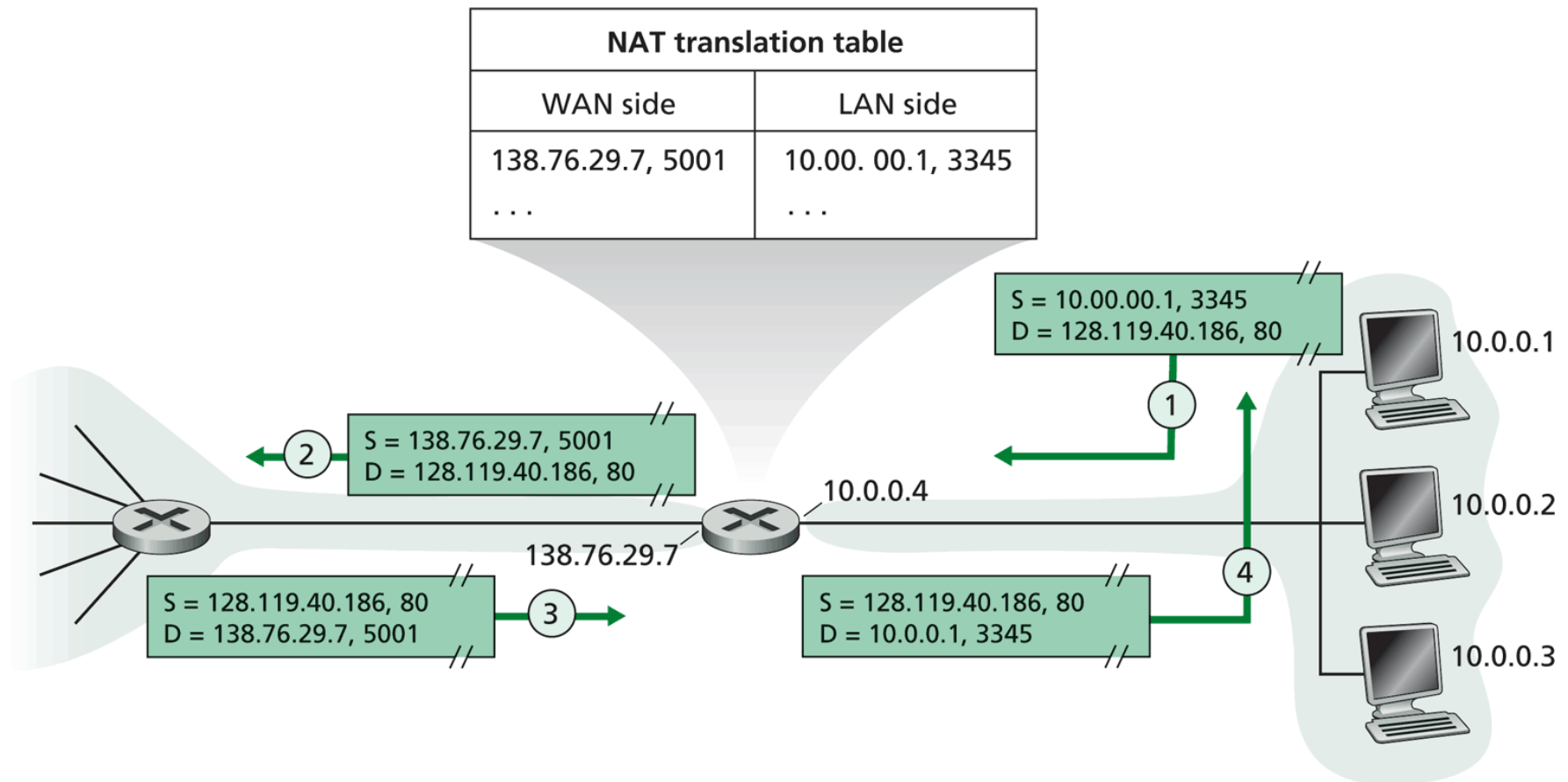
1st frag. : 1480 + 20 (Header)

2nd frag. : 1480 + 20 (Header)

3rd frag. : 1020 + 20 (Header)

Fragment	Bytes	ID	Offset	Flag (MF)
1st Fragment	1480 bytes in data field of IP Datagram	777 (eg.)	Offset = 0 (Beginning part)	MF = 1 (more fragments)
2st Fragment	1480 bytes in data field of IP Datagram	777	Offset = 1480 (beginning at byte 1480)	MF = 1 (more fragments)
3st Fragment	1020 bytes in data field of IP Datagram	777	Offset = 2960 (beginning at byte 2960)	MF = 0 (no more fragments)

Network Address Translation (NAT)



ICMP (Internet Control Message Protocol)

- Used to test the Internet
- ICMP is one of the core protocols of the Internet Protocol Suite.
- It is used by the operating systems of networked computers to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached.
- ICMP can also be used to relay query messages.
- ICMP differs from transport protocols such as TCP and UDP in that it is not typically used to exchange data between systems, nor is it regularly employed by end-user network applications (with the exception of some diagnostic tools like ping and traceroute).
- Most Typical Use of ICMP is for error reporting.

ICMP (Internet Control Message Protocol)

Message type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach a router about geography
Echo request	Ask a machine if it is alive
Echo reply	Yes, I am alive
Timestamp request	Same as Echo request, but with timestamp
Timestamp reply	Same as Echo reply, but with timestamp

ICMP (Internet Control Message Protocol)

<u>Type</u>	<u>Code</u>	<u>description</u>
0	0	echo reply (ping)
3	0	dest. network unreachable
3	1	dest host unreachable
3	2	dest protocol unreachable
3	3	dest port unreachable
3	6	dest network unknown
3	7	dest host unknown
4	0	source quench (congestion control - not used)
8	0	echo request (ping)
9	0	route advertisement
10	0	router discovery
11	0	TTL expired
12	0	bad IP header

IPv6

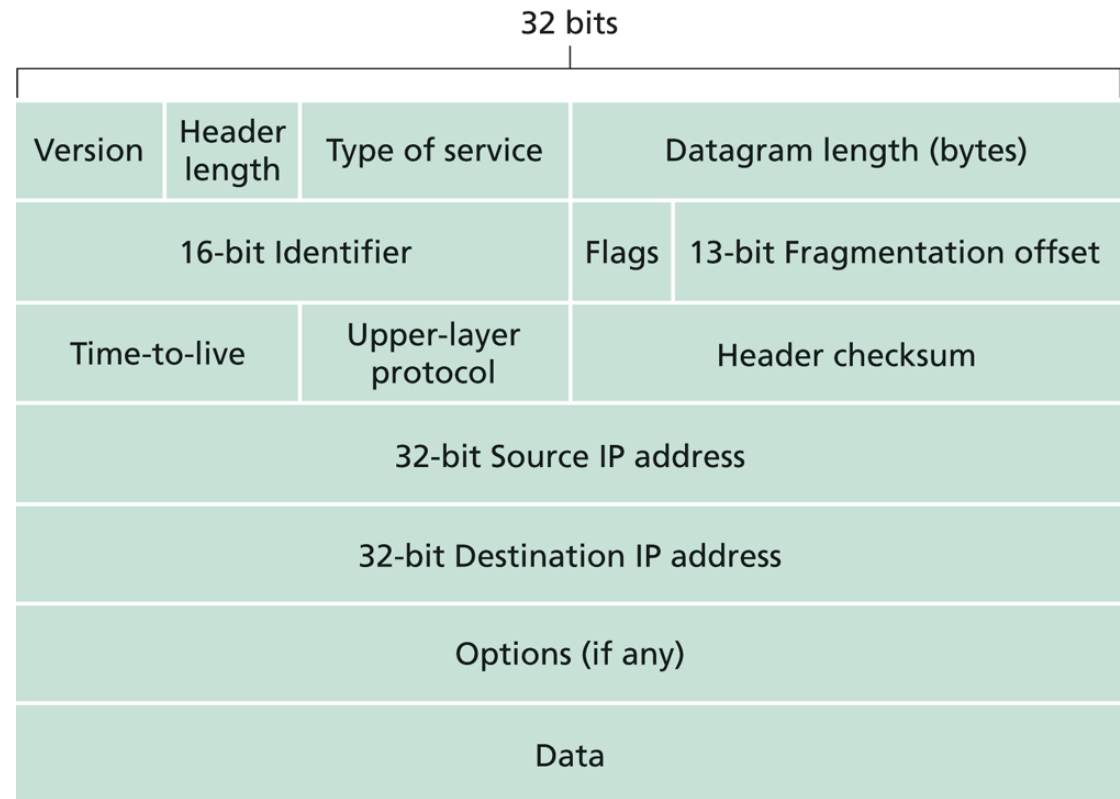
- The huge growth in Internet use has not only led to increased demand for better, faster technology, but has also increased the demand for addresses from which to send and receive information.
- This is especially true for developing countries where people are only really starting to use the Internet.
- IPv6 deployment can solve the problem.

IPv6

- Each device on the Internet, such as a computer or mobile telephone, must be assigned an IP address in order to communicate with other devices.
- With the ever-increasing number of new devices being connected to the Internet, there is a need for more addresses than IPv4 can accommodate.
- IPv6 uses 128-bit addresses, allowing for 2^{128} , or approximately 3.4×10^{38} addresses. IPv4 uses 32-bit addresses, allowing for only 4,294,967,296 unique addresses worldwide.
- IPv6 addresses, as commonly displayed to users, consist of eight groups of four hexadecimal digits separated by colons, for example 2001:0db8:85a3:0042:0000:8a2e:0370:7334.

Unforeseen limitations of IPv4

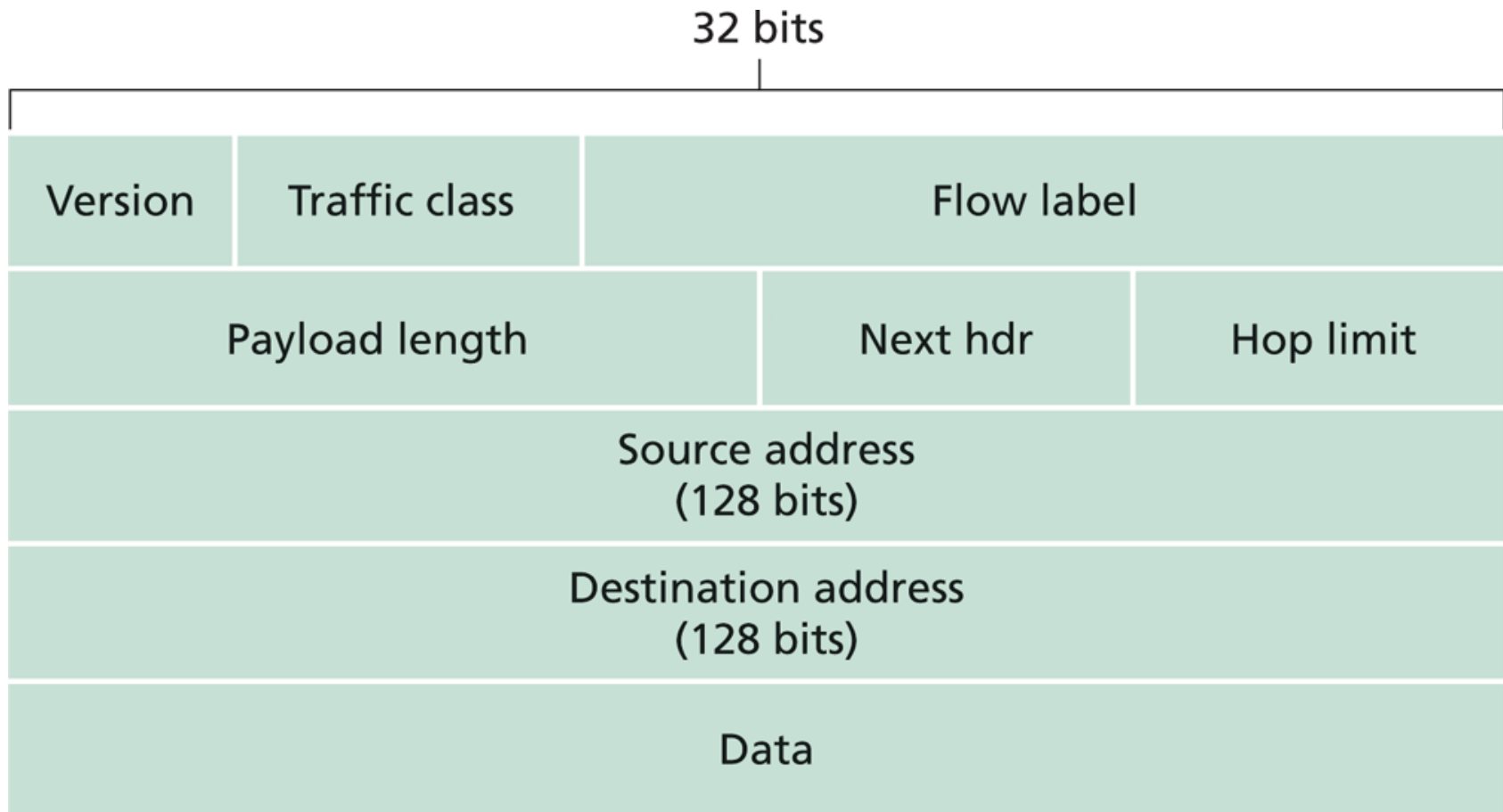
- Address Space
- Various unnecessary header fields
- Variable header fields
- Fragmentation in Router
- Addressing Model
- NAT
- Broadcast Versus Multicast
- Quality of Service



Advantages of IPv6

- Very large address space: 128-bit address $\Rightarrow 2^{128} \sim 3$ Trillion trillion trillion
 - “Every grain of sand on earth can get Unique IPv6 address”
- Reduce end-to-end delay : Processing delay reduces due to fixed header size and no header checksum
- A streamlined 40 bytes header : Allows faster processing of the IP datagram
 - Optional headers are daisy-chained
- Flow labelling and priority
 - Has an elusive definition of flow (according to quality of service or real time service e.g. audio and video transfer)
- Higher level of security
 - Mandatory IPsec
- Mobility - Keep same IP address regardless of the network
- No fragmentation by routers
 - reduces fragmentation / reassembly overhead
- Aid multicasting by allowing scopes to be specified.

IPv6 Header Format



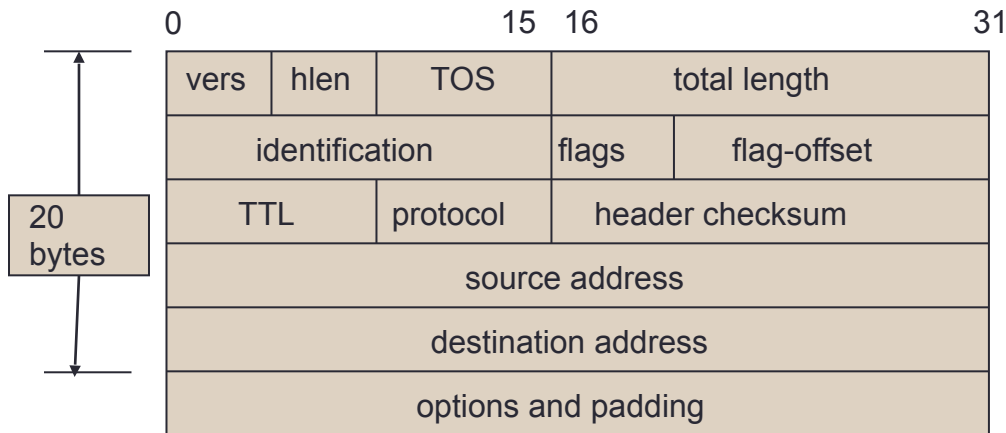
IPv6 Header Format

- **Version (4 bits)** - 4 bits are used to indicate the version of IP and is set to 6
- **Traffic Class (8 bits)** - Same function as the Type of Service field in the IPv4, distinguish different real-time delivery requirement
- **Flow Label (20 bits)**
 - Identifies a flow and it is intended to enable the router to identify packets that should be treated in a similar way without the need for deep lookups within those packets.
 - Set by the source and should not be changed by routers along the path to destination.
- **Payload Length (16 bits)** – Only the length of the payload (Header length is fixed to 40 bytes)

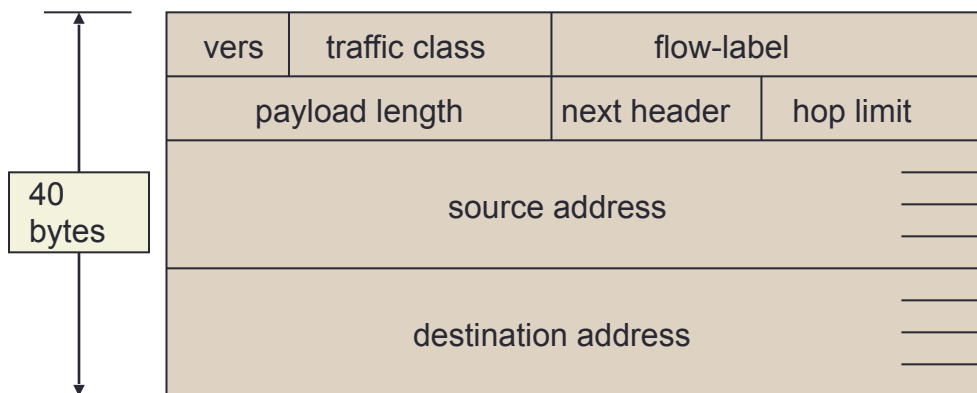
IPv6 Header Format

- **Next Header (8 bits)** - Indicates either the first extension header (if present) or the protocol in the upper layer PDU (such as TCP, UDP, or ICMPv6).
- **Hop Limit (8 bits)** - IPv4 TTL was appropriately renamed Hop Limit because it is a variable that is decremented at each hop, and it does not have a temporal dimension.
- **Source Address (128 bits)** - Stores the IPv6 address of the originating host.
- **Destination Address (128 bits)** - Stores the IPv6 address of the current destination host.

Header Comparison



IPv4



IPv6

Removed (6)

- ID, flags, flag offset
- TOS, hlen
- header checksum

Changed (3)

- total length => payload
- protocol => next header
- TTL => hop limit

Added (2)

- traffic class
- flow label

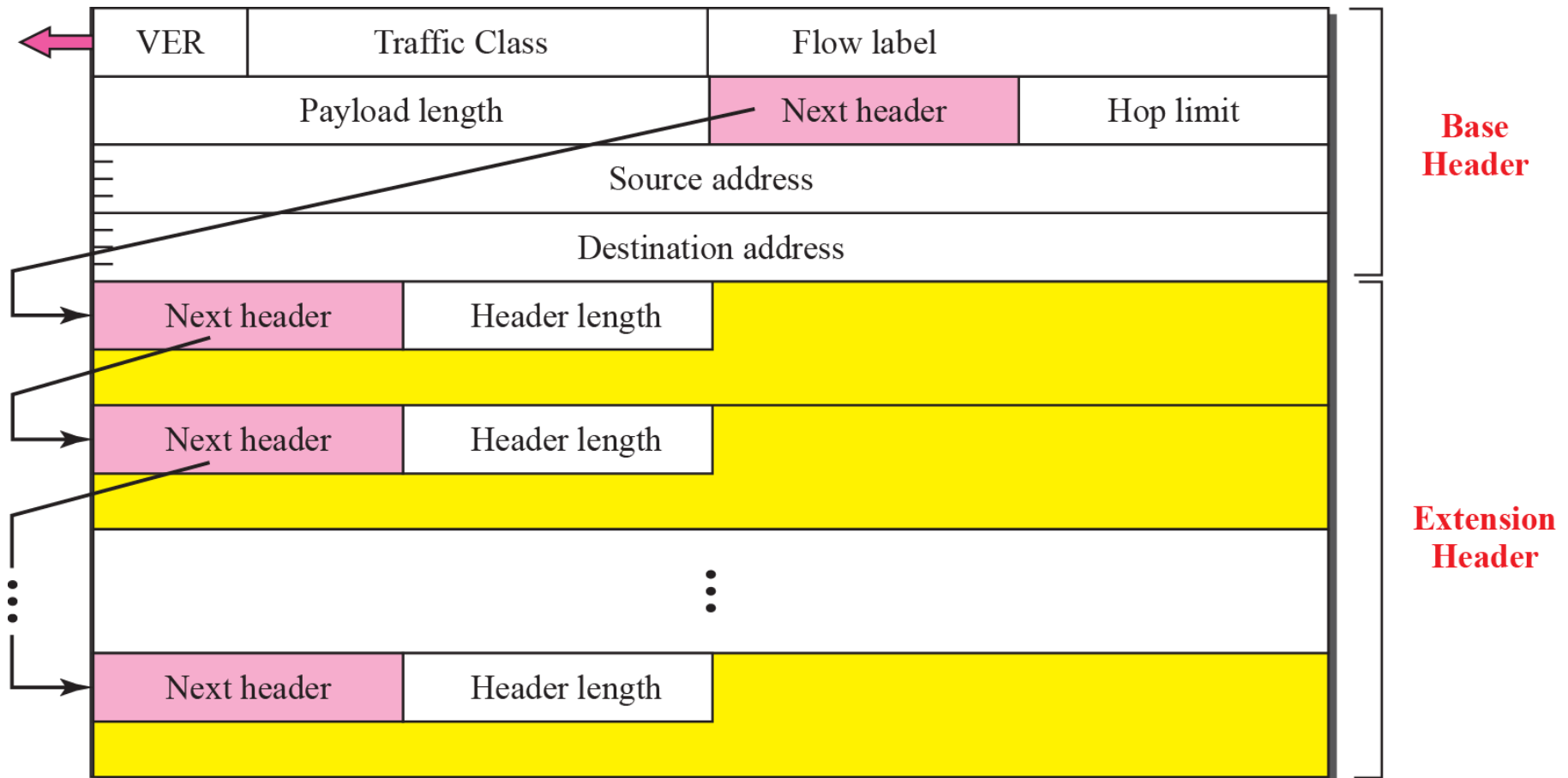
Expanded

- address 32 to 128 bits

Extension Headers

- The length of base header is 40 bytes.
- However in IPv6 header can be followed by upto 6 extension headers
- This is to give more functionality to IP datagram
- **Extension headers of variable size contain a Header Extension Length field** and must use padding as needed to ensure that their size is a multiple of 8 bytes.
- Next Header field in the IPv6 header and zero or more extension headers form a chain of pointers.
- Each pointer indicates the type of header that comes after the immediate header until the upper layer protocol is ultimately identified.
- Extension headers must be processed strictly in the order they appear in the packet.

IPv6 Extension Headers



Types of Extension Headers

- **Hop-by-Hop Options Header :**
 - Special options that require hop-by-hop processing
- **Destination Options Header :**
 - Used to carry optional information for destination node
- **Routing Options Header :**
 - Lists one or more IPv6 node to be “visited” on the way to a packet destination.
- **Fragmentation Options Header :**
 - Fragmentation and reassembly
 - Only source node can fragment a packet in IPv6
- **Authentication Options Header :**
 - Provide Integrity and authentication, security
- **Encapsulating Security Payload:**
 - Provides Encryption Security, Confidentiality

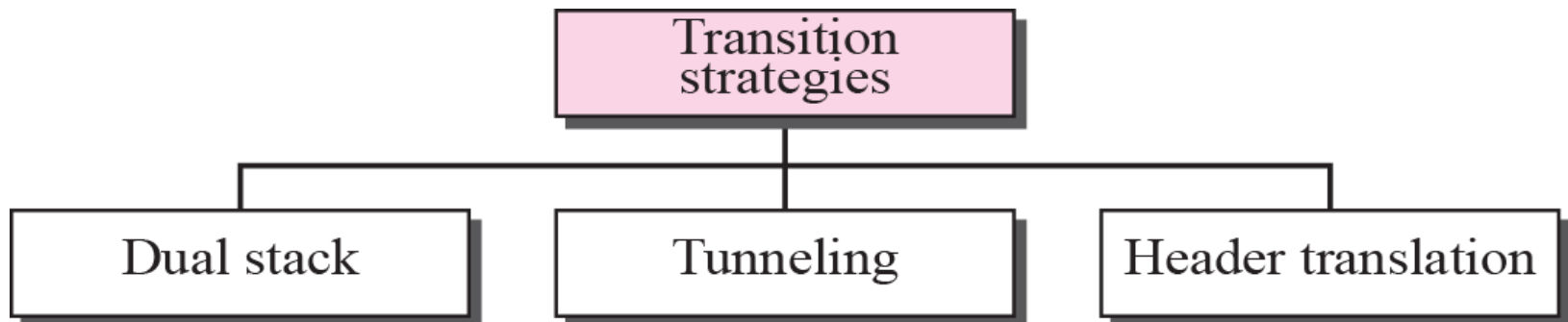
Extension Header Codes

<i>Code</i>	<i>Next Header</i>	<i>Code</i>	<i>Next Header</i>
0	Hop-by-hop option	44	Fragmentation
2	ICMP	50	Encrypted security payload
6	TCP	51	Authentication
17	UDP	59	Null (No next header)
43	Source routing	60	Destination option

Fig. Next Header Code

IPv4 to IPv6 Transition

- Because of the huge number of systems on the Internet, the transition from IPv4 to IPv6 cannot happen suddenly.
- Flag Day is not Possible
- The transition must be smooth to prevent any problems between IPv4 and IPv6 systems.
- Three strategies to help the transition :



Fragmentation in IPv6

- IPv6 routers do not support fragmentation or the Don't Fragment option.
- For IPv6, Path MTU Discovery works by initially assuming the path MTU is the same as the MTU on the link layer interface through which the traffic is being sent.
- Then, similar to IPv4, any device along the path whose MTU is smaller than the packet will drop the packet and send back an ICMPv6 Packet Too Big (Type 2) message containing its MTU, allowing the source host to reduce its Path MTU appropriately.
- The process is repeated until the MTU is small enough to traverse the entire path without fragmentation.

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 (Zero Suppression):
 - 2031:0:130F:0:0:9C0:876A:130B
- Successive fields of 0 represented as :: (Zero Compression), 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

- :: representation
 - RFC5952 recommends that the rightmost set of :0: be replaced with :: for consistency
 - 2001:db8:0:2f::5 rather than 2001:db8::2f:0:0:0:5
- 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 (RFC3986)
 - [http://\[2001:db8:4f3a::206:ae14\]:8080/index.html](http://[2001:db8:4f3a::206:ae14]:8080/index.html)
 - Cumbersome for users, mostly for diagnostic purposes
 - Use fully qualified domain names (FQDN)
 - ⇒ The DNS has to work!!

IPv6 Address Representation

- Like IPv4 classless addresses , IP v6 addresses are fundamentally divided into a number of network ID bits followed by a number of host ID bits.
- The network identifier is called the prefix, and the number of bits used is the prefix length.
- 805B:2D9D:DC28::FC57:D4C8:1FFF/48

□ Prefix Representation

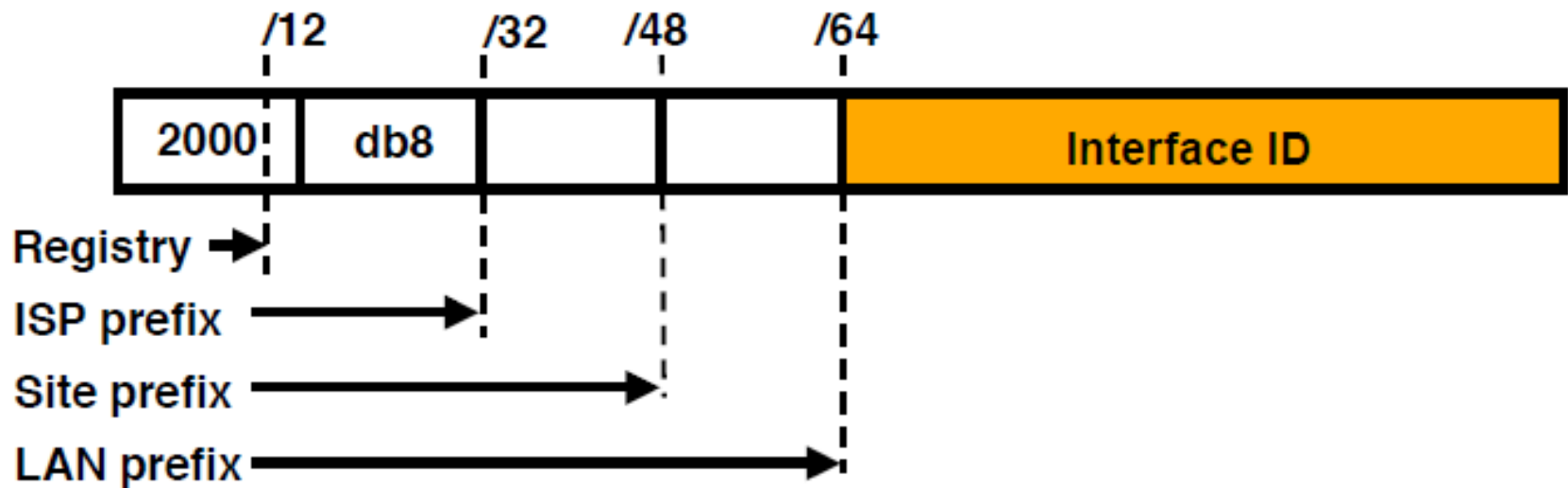
- Representation of prefix is just like IPv4 CIDR
- In this representation you attach the prefix length
- Like IPv4 address:
 - 198.10.0.0/16
- IPv6 address is represented in the same way:
 - 2001:db8:12::/40

IPv6 Addressing

- IPv6 Addressing rules are covered by multiple RFCs
 - Architecture defined by RFC 4291
- Address Types are :
 - Unicast : One to One (Global, Unique Local, 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

IPv6 Address Allocation

- The allocation process is:
 - The IANA is allocating out of 2000::/3 for initial IPv6 unicast use
 - Each registry gets a /12 prefix from the IANA
 - Registry allocates a /32 prefix (or larger) to an IPv6 ISP
 - Policy is that an ISP allocates a /48 prefix to each end customer



IPv6 Addressing Scope

- 64 bits reserved for the interface ID
 - Possibility of 2^{64} hosts on one network LAN
 - Arrangement to accommodate MAC addresses within the IPv6 address
- 16 bits reserved for the end site
 - Possibility of 2^{16} networks at each end-site
 - 65536 subnets equivalent to a /12 in IPv4 (assuming a /28 or 16 hosts per IPv4 subnet)
- 16 bits reserved for each service provider
 - Possibility of 2^{16} end-sites per service provider
 - 65536 possible customers: equivalent to each service provider receiving a /8 in IPv4 (assuming a /24 address block per customer)
- 29 bits reserved for all service providers
 - Possibility of 2^{29} service providers i.e. 536,870,912 discrete service provider networks
 - Although some service providers already are justifying more than a /32

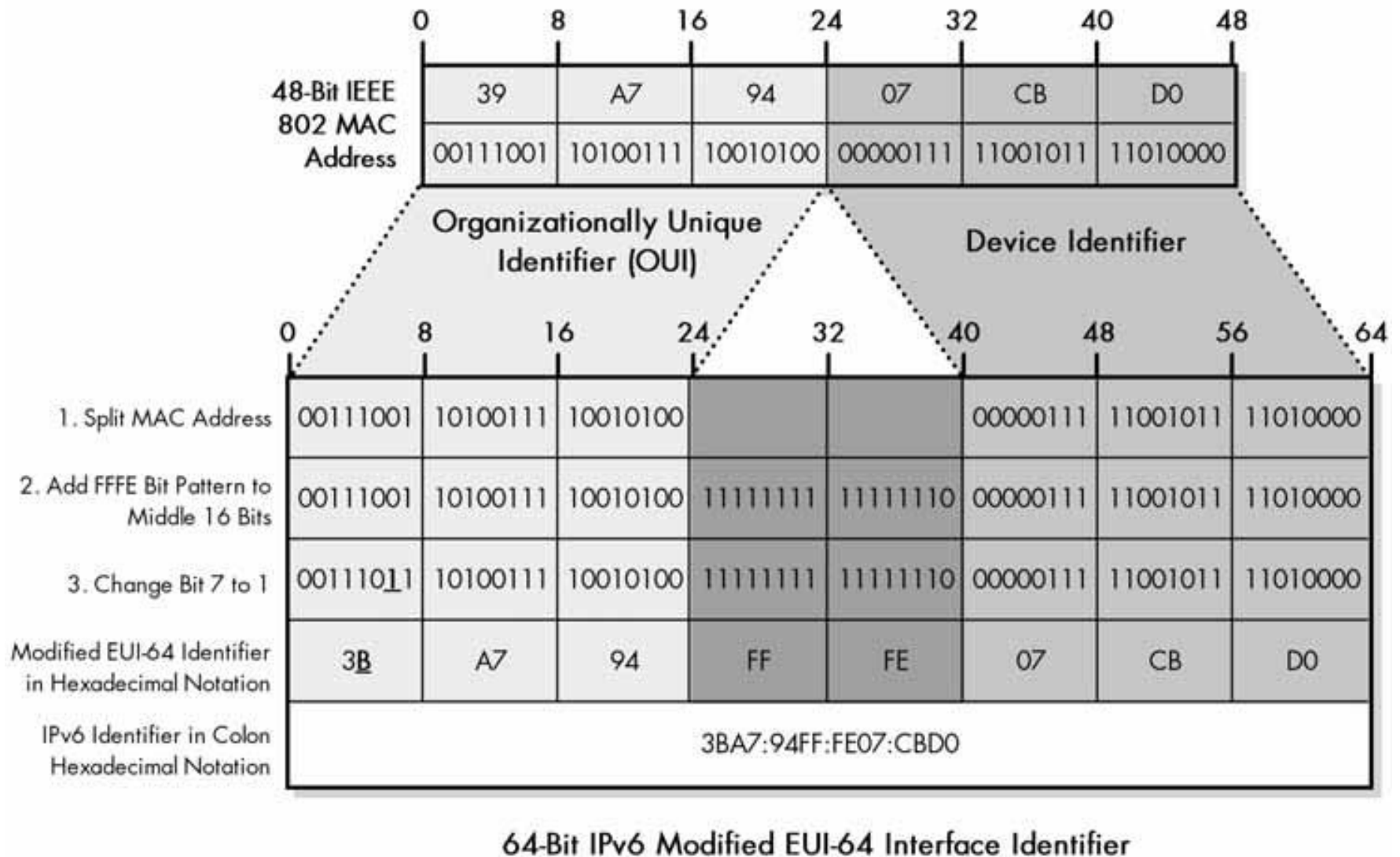
Interface IDs

- 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

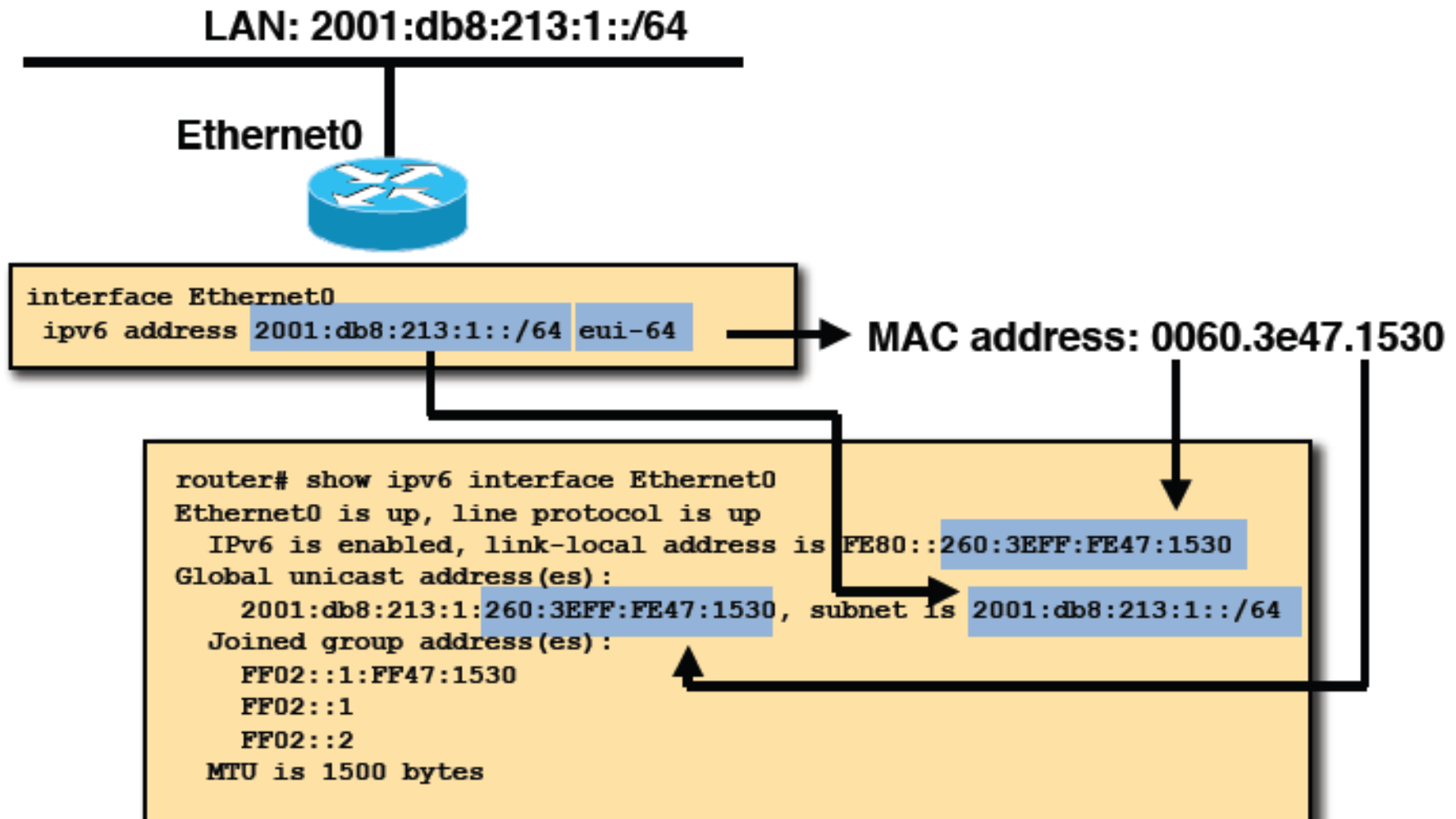
IPv6 Interface Identifier and Physical Address Mapping

- 48 bit network prefix, 16 bit subnet ID , we have still 64 bits to use for the interface identifier (Interface ID)
- Process of Generating Unicast Address Using MAC address
 - Take the 24-bit OUI portion, the leftmost 24 bits of the Ethernet address, and put them into the leftmost 24 bits of the interface ID.
 - Take the 24-bit local portion(the rightmost 24 bits of the Ethernet address) and put it into the rightmost 24 bits of the interface ID.
 - In the remaining 16 bits in the middle of the interface ID, put the value 11111111 11111110, FFFE in hexadecimal.
 - The address is now in EUI-64 form. Change the universal/local bit (bit 7 from the left, shown in bold in Figure 25-5) from a 0 to a 1.
 - This gives the modified EUI-64 interface ID.

IPv6 Interface Identifier and Physical Address Mapping



IPv6 Addressing Example



IPv6 Addressing

Type	Binary	Hex
Unspecified	000...0	::/128
Loopback	000...1	::1/128
Global Unicast Address	0010	2000::/3
Link Local Unicast Address	1111 1110 10	FE80::/10
Unique Local Unicast Address	1111 1100 1111 1101	FC00::/7
Multicast Address	1111 1111	FF00::/8

Reserved Address

- A portion of the address space is set aside as reserved for various uses by the IETF, both present and future
- The reserved block in IPv6 is at the “top” of the address space, beginning with 0000 0000
- This represents $1/256$ th of the total address space

Unspecified Address

- In IPv4, an IP address of all zeros has a special meaning.
- It refers to the host itself and is used when a device doesn't know its own address.
- In IPv6, this concept has been formalized, and the all-zeros address (0:0:0:0:0:0:0:0) is named the unspecified address.
- It must never be assigned to any node. It indicates the absence of an address.
- One example of its use is in the Source Address field of any IPv6 packets sent by an initializing host before it has learned its own address.
- The unspecified address must not be used as the destination address of IPv6 packets or in IPv6 Routing headers.
- An IPv6 packet with a source address of unspecified must never be forwarded by an IPv6 router.

The Loopback Address

- The unicast address 0:0:0:0:0:0:0:1 is called the loopback address.
- It may be used by a node to send an IPv6 packet to itself. It must not be assigned to any physical interface. It is treated as having Link-Local scope, and may be thought of as the Link-Local unicast address of a virtual interface (typically called the "loopback interface") to an imaginary link that goes nowhere.
- The loopback address must not be used as the source address in IPv6 packets that are sent outside of a single node.
- An IPv6 packet with a destination address of loopback must never be sent outside of a single node and must never be forwarded by an IPv6 router.
- A packet received on an interface with a destination address of loopback must be dropped.

IPv6 Global Unicast Address

- 1/8th of total address are Global Unicast address, which are indicated by 001 in the first three bits of the address.
- Divided into three section :

Field Name	Size (Bits)	Description
Prefix	48 (n)	Global Routing Prefix: The network ID or prefix of the address that's used for routing. The first three bits are 001 to indicate a unicast address.
Subnet ID	16(m)	Subnet Identifier: A number that identifies a subnet within the site.
Interface ID	64 (128-n-m)	Interface ID: The unique identifier for a particular interface (host or other device). It is unique within the specific prefix and subnet.

IPv6 Global Unicast Address

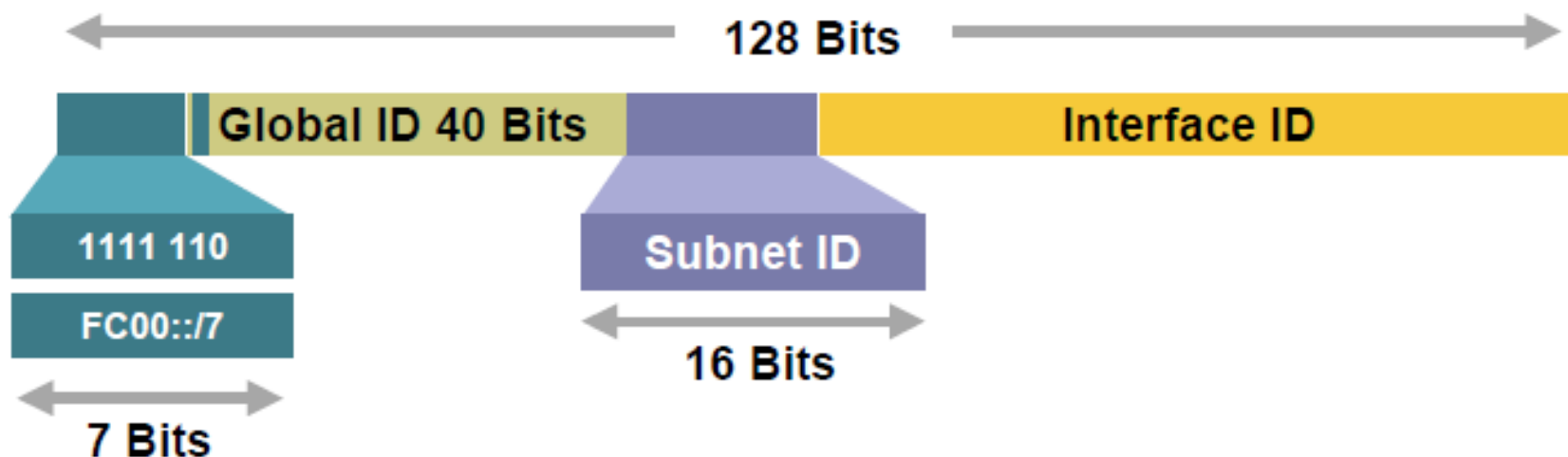
- The 16 bits of subnet ID allow each site considerable flexibility in creating subnets that reflect the site's network structure. Here are some example uses of the 16 bits:
 - A smaller organization can just set all the bits in the subnet ID to zero and have a flat internal structure.
 - A medium-sized organization could use all the bits in the subnet ID to perform the equivalent of straight subnetting under IPv4, thereby assigning a different subnet ID to each subnet. There are 16 bits here, and this allows a whopping 65,536 subnets!
 - A larger organization can use the bits to create a multiple-level hierarchy of subnets, exactly like IPv4's Variable Length Subnet Masking (VLSM). For example, the company could use two bits to create four subnets. It could then take the next three bits to create eight sub-subnets in some or all of the four subnets. There would still be 11 more bits to create sub-sub-subnets, and so forth.

Unregistered / No routable Address

- These addresses are local only to a particular link or site and, therefore, are never routed outside a particular company's network.
- Types based on scope :
 - site-local / unique local
 - link-local

Site-Local/Unique Local Unicast Addresses

- These addresses have the scope of an entire site or organization.
- They allow addressing within an organization without having to use a public prefix.
- Routers will forward datagrams using site-local addresses within the site, but not addresses outside it to the public Internet.
- Begin with 1111 1100 , (FC00::/7 in HEX).



Site-Local/Unique Local Unicast Addresses

- Unique-Local Addresses Used For:
 - Local communications & inter-site VPNs
 - Local devices such as printers, telephones, etc
 - Site Network Management systems connectivity
- Not routable on the Internet
- Reinvention of the deprecated site-local?

Link local unicast address

- Link-Local addresses are for use on a single link. Link-Local addresses have the following format:

10 bits	54 bits	64 bits
1111 1110 10 (FE80::/10)	0	Interface ID

- Link-Local addresses are designed to be used for addressing on a single link for purposes such as automatic address configuration, neighbour discovery, or when no routers are present.
- Routers must not forward any packets with Link-Local source or destination addresses to other links.
- Link-Local Addresses Used For:
 - Communication between two IPv6 devices (like ARP but at Layer 3)
 - Next-Hop calculation in Routing Protocols
- Automatically assigned by Router as soon as IPv6 is enabled

Anycast Addresses

- An IPv6 anycast address is an address that is assigned to more than one interface (typically belonging to different nodes), with the property that a packet sent to an anycast address is routed to the "nearest" interface having that address, according to the routing protocols' measure of distance.
- Anycast addresses are allocated from the unicast address space, using any of the defined unicast address formats. Thus, anycast addresses are syntactically indistinguishable from unicast addresses.
- When a unicast address is assigned to more than one interface, thus turning it into an anycast address, the nodes to which the address is assigned must be explicitly configured to know that it is an anycast address.

IPv6 Multicast Address

- Multicasting is used to allow a single device to send a datagram to a group of recipients.
- This is 1/256th of the address space, and it consists of all addresses that begin with 1111 1111.
- i.e. Ipv6 multicast address has a prefix FF00::/8 .
- The second octet defines the lifetime and scope of the multicast address.

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

Lifetime	
0	If Permanent
1	If Temporary

Scope	
1	Node
2	Link
5	Site
8	Organisation
E	Global

IPv6 Multicast Address

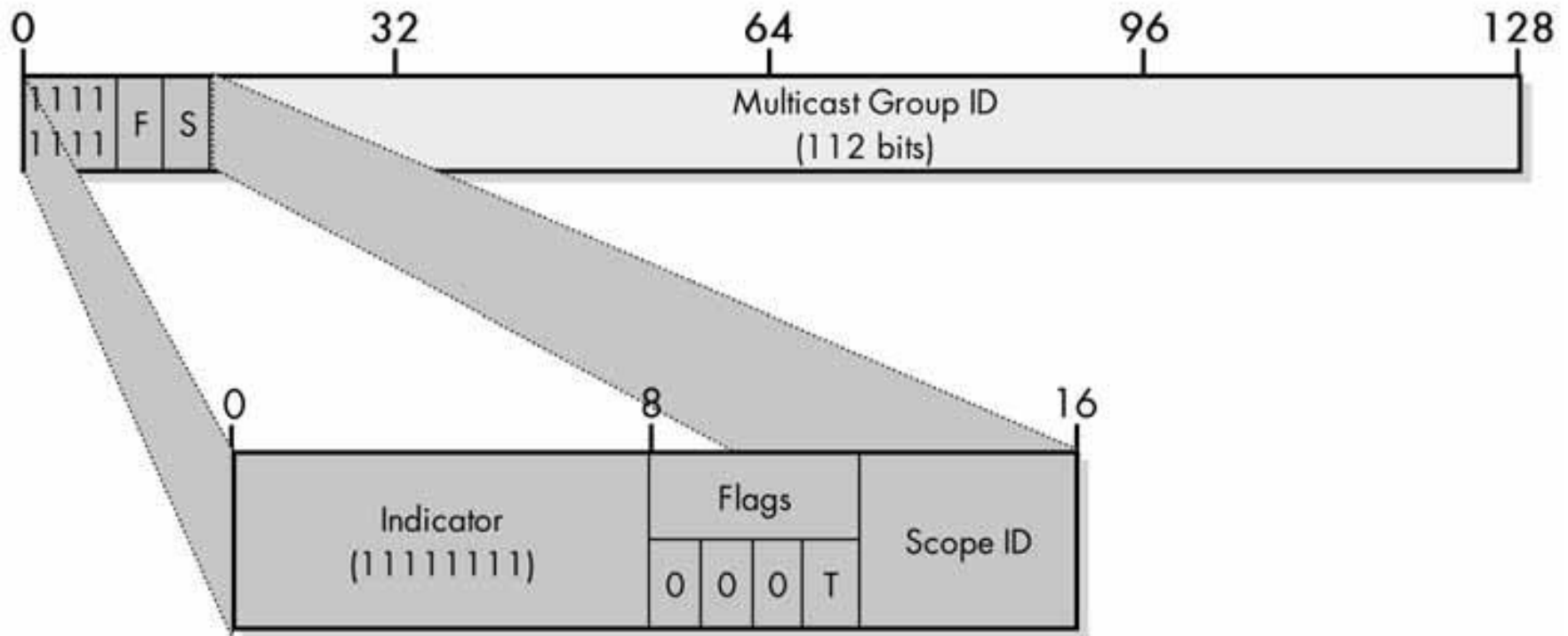


Fig. IPv6 multicast address format

IPv6 Multicast Address

Field Name	Size(bits)	Description
(Indicator)	8	The first eight bits are always 1111 1111, which indicates a multicast address. This used to be called the format prefix before the term was dropped (as explained in the section about IPv6 address space allocation earlier in this chapter). The field now has no name.
Flags	4	Four bits are reserved for flags that can be used to indicate the nature of certain multicast addresses. Currently, the first three of these are unused and set to zero. The fourth is the T (Transient) flag. If left as zero , this marks the multicast address as a permanently assigned, well-known multicast address, as you will see shortly. If set to one , this means this is a transient multicast address, meaning that it is not permanently assigned.

IPv6 Multicast Address

Field Name	Size(bits)	Description
Scope ID	4	<p>These four bits are used to define the scope of the multicast address; 16 different values from 0 to 15 are possible. This field allows creation of multicast addresses that are global to the entire Internet, or restricted to smaller spheres of influence such as a specific organization, site, or link. The currently defined values (in decimal) are as follows:</p> <ul style="list-style-type: none">0 = Reserved1 = Node-Local Scope2 = Link-Local Scope5 = Site-Local Scope8 = Organization-Local Scope14 = Global Scope15 = Reserved
Group ID	112	Defines a particular group within each scope level.

Multicast Scopes

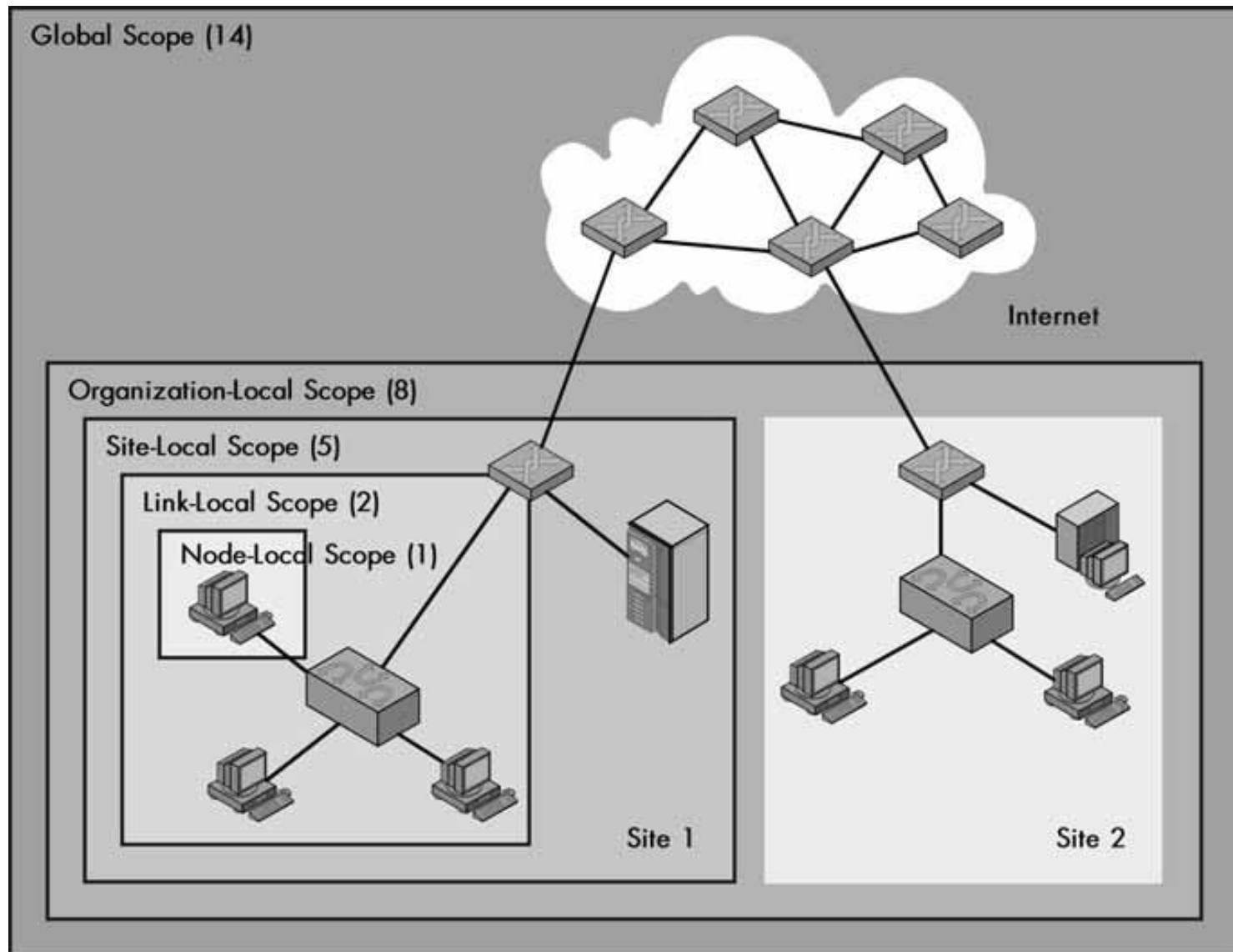


Fig. IPv6 multicast scope

IPv6 Multicasting Examples

- RIPng
 - The multicast address AllRIPRouters is FF02::9
 - Note that 02 means that this is a permanent address and has link scope
- OSPFv3
 - The multicast address AllSPFRouters is FF02::5
 - The multicast address AllDRouters is FF02::6
- EIGRP
 - The multicast address AllEIGRPRouters is FF02::A

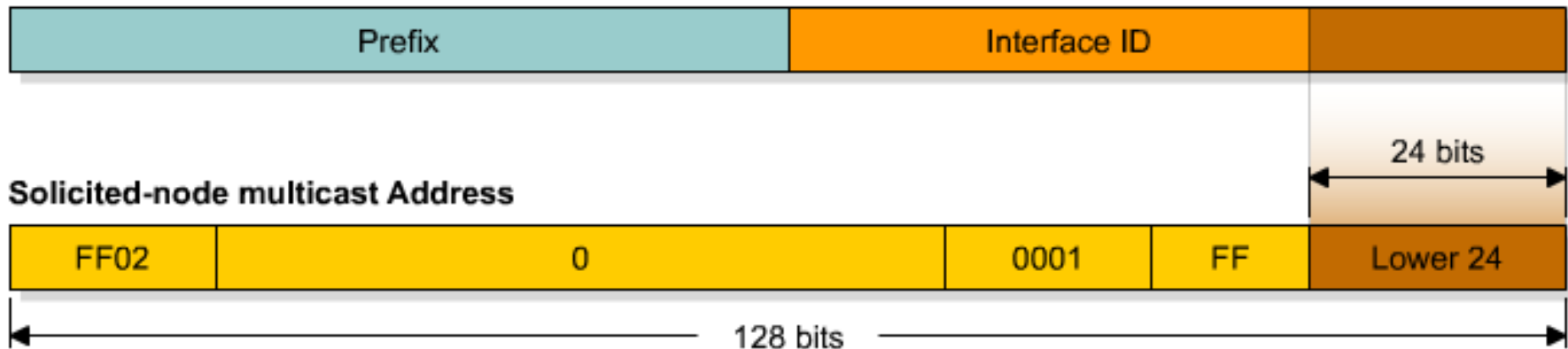
Solicited-Node Multicast

- Solicited-Node Multicast is used for Duplicate Address Detection
 - Part of the Neighbour Discovery process
 - Replaces ARP
 - Duplicate IPv6 Addresses are rare, but still have to be tested for
- For each unicast and anycast address configured there is a corresponding solicited-node multicast address
 - This address is only significant for the local link

Solicited-node multicast address

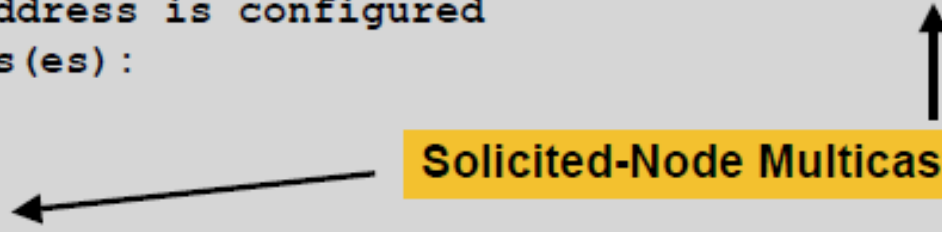
- Solicited-node multicast address consists of FF02:0:0:0:0:1:FF::/104 prefix joined with the lower 24 bits from the unicast or anycast IPv6 address.

IPv6 Address



Solicited-node multicast address

```
R1#sh ipv6 int e0
Ethernet0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::200:CFF:FE3A:8B18
  No global unicast address is configured
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF3A:8B18
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
R1#
```



The diagram illustrates the mapping from the link-local address `FE80::200:CFF:FE3A:8B18` to the solicited-node multicast address `FF02::1:FF3A:8B18`. An upward arrow points from the `FE3A:8B18` portion of the link-local address to a yellow box labeled "Solicited-Node Multicast Address". A leftward arrow points from this box to the `FF3A:8B18` portion of the multicast address `FF02::1:FF3A:8B18`.

Internet RFCs

- In computer network engineering, a *Request for Comments (RFC)* is a memorandum, usually published by the RFC Editor on behalf of the Internet Engineering Task Force (IETF), **describing methods, behaviors, research, or innovations applicable to the working of the Internet and Internet connected systems.**
- Through the Internet Society, engineers and computer scientists may publish discourse in the form of an RFC, either for peer review or simply to convey new concepts, information, or (occasionally) engineering humor. The IETF adopts some of the proposals published as RFCs as Internet standards.
- Request For Comments documents were invented by Steve Crocker in 1969 to help record unofficial notes on the development of the ARPANET. They have since become the official record for Internet **specifications, protocols, procedures, and events.**

Internet RFCs

- The RFC Editor assigns each RFC a unique serial number. Once assigned a number and published, an RFC is never rescinded or modified; if the document requires amendments, the authors publish a revised document. Therefore, some RFCs supersede others; the superseded RFCs are said to be *deprecated*, *obsolete*, or *obsoleted* by the superseding RFC. Together, the serialized RFCs compose a continuous historical record of the evolution of Internet standards and practices.
- The official source for RFCs on the World Wide Web is the RFC Editor. Almost any individual published RFC, for example RFC 5000, can be retrieved via the URL: <http://www.rfceditor.org/rfc/rfc5000.txt>
- **For more details about RFCs and the RFC process, see RFC 2026, "The Internet Standards Process, Revision 3"**

Internet RFCs

- The RFC production process differs from the standardization process of formal standards organizations such as ISO. Internet technology experts may submit an Internet Draft without support from an external institution. Standards-track RFCs are published with approval from the IETF, and are usually produced by experts participating in working groups, which first publish an Internet Draft.
- This approach facilitates initial rounds of peer review before documents mature into RFCs.
- The RFC series contains three sub-series for IETF RFCs:
 - BCP: *Best Current Practice*; mandatory IETF RFCs not on standards track
 - FYI: *For Your Information*; informational RFCs promoted by the IETF as specified in RFC 1150
 - (FYI 1). In 2011, RFC 6360 obsoleted FYI 1 and concluded this sub-series.
 - STD: *Standard*; this used to be the third and highest maturity level of the IETF standards track specified in RFC 2026 (BCP 9)

RFC: Example

Network Working Group

Request for Comments: 1149

1 April 1990

A Standard for the Transmission of IP Datagrams on Avian Carriers

Status of this Memo

D. Waitzman

BBN STC

This memo describes an experimental method for the encapsulation of IP datagrams in avian carriers. This specification is primarily useful in Metropolitan Area Networks. This is an experimental, not recommended standard. ...

Overview and Rational

Avian carriers can provide high delay, low throughput, and low altitude service. The connection topology is limited to a single point-to-point path for each carrier, used with standard carriers, but many carriers can be used without significant interference with each other, outside of early spring. This is because of the 3D ether space available to the carriers, in contrast to the 1D ether used by IEEE802.3. The carriers have an intrinsic collision avoidance system, which increases

Frame Format

The IP datagram is printed, on a small scroll of paper, in hexadecimal, with each octet separated by whitestuff and blackstuff. The scroll of paper is wrapped around one leg of the avian carrier. A band of duct tape is used to secure the datagram's edges. The bandwidth is limited to the leg length.

Thank You !!!