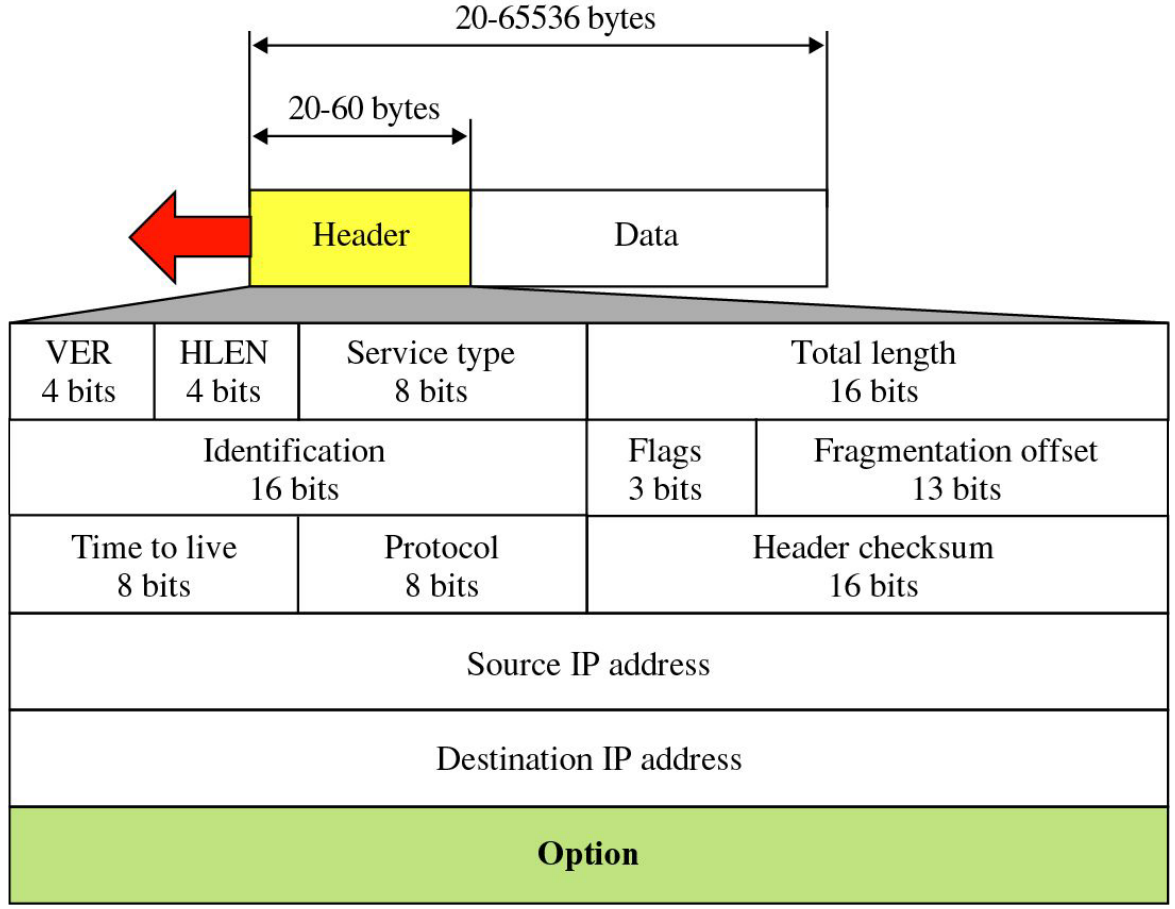
Computer Network(CSC 503)

Shilpa Ingoley

Lecture 26

MU Question

- A IP header from an IP packet received at destination 4500003c1c4640004006b1 e6ac100a63ac100 a 0c. Map these values to IP header and explain all bits.



Contd…

Sr. No	IP Header Fields	Explanation of bits
1	Version (4 bits)	4 (0100)
2	IHL(Internet Header Length)(4 bits)	5 (0101)When no options is specified, the header length is 20 bytes, and the value of this field is 5 (5 x 4 = 20).
3	Type of Service (8 bits)	00
4	Total length (16 bits)	003c (header + data) =60bytes Header length = 20 bytes, Length of data = 40bytes
5	Identification (16 bits)	1c46
6	Flags and Fragment offset(16 bits)	‘4000’ can be divided into two bytes. These two bytes (divided into 3 bits and 13 bits respectively) correspond to the flags and fragment offset of IP header fields
7	TTL and Protocol(16 bits)	‘4006’ can be divided into TTL and Protocol bits respectively i.e. ’40’ and ’06’. The first byte ’40’ corresponds to the TTL field. The byte ’06’ corresponds to the protocol field of the IP header. ’06’ indicates that the protocol is TCP.
8	Checksum(16 bits)	‘be16’ represents to the checksum, which is set at the source side. This field will be set to zero while computing the checksum at destination end.
9	Source IP Address	‘ac10 0a63’
10	Destination, IP Address	‘ac10 0a0c’

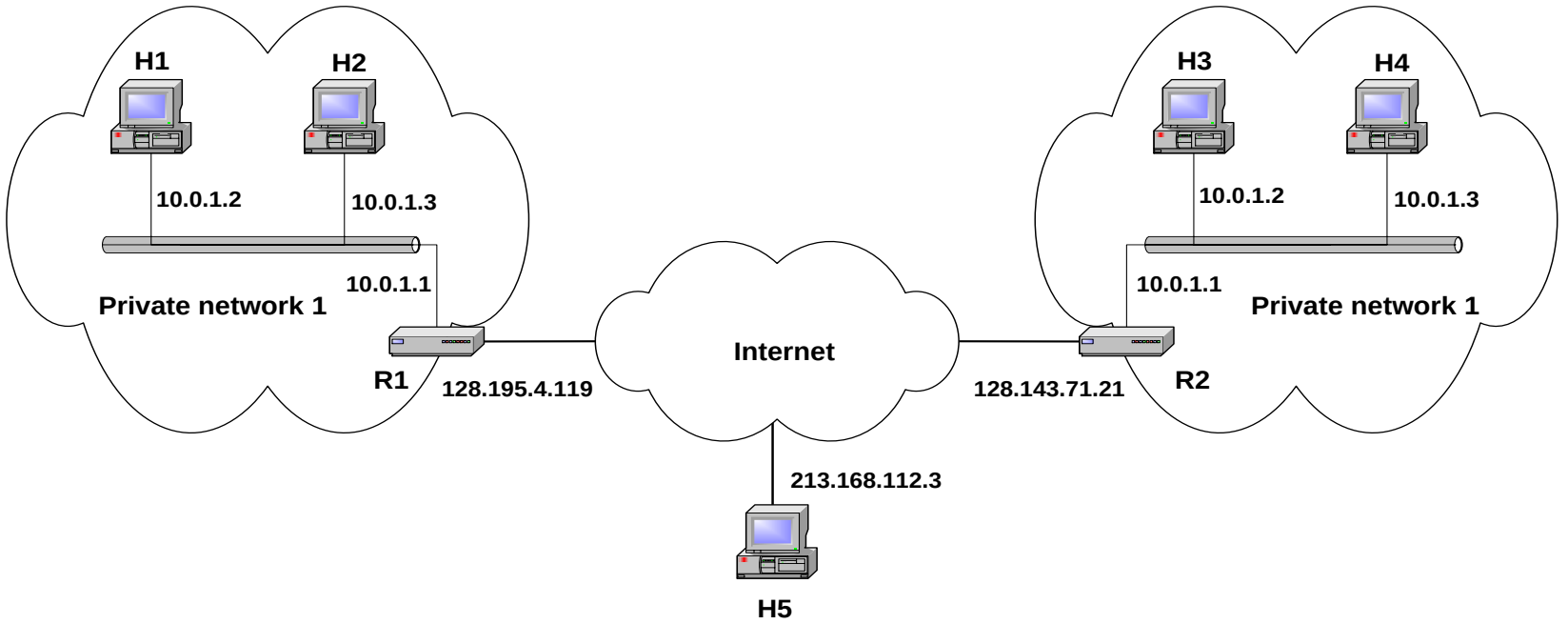
Private Network

- *Private IP* network is an IP network that is not directly connected to the Internet
- IP addresses in a private network can be assigned arbitrarily.
  - Not registered and not guaranteed to be globally unique
- Private networks use addresses from the following address ranges :
  - 10.0.0.0 – 10.255.255.255/8 (16,777,216 hosts)
  - 172.16.0.0 – 172.31.255.255/12 (1,048,576 hosts)
  - 192.168.0.0 – 192.168.255.255/16 (65,536 hosts)
- To make this scheme possible, three ranges of IP addresses have been declared as private.

➢Companies may use them internally as they wish.

➢ The only rule is that no packets containing these addresses may appear on the Internet itself.

Private Addresses



Network Address Translation (NAT)

- A short term solution to the problem of the depletion of IP addresses
  - Long term solution is IP v6
  - CIDR (Classless InterDomain Routing) is a possible short term solution
  - NAT is another

- NAT is a way to conserve IP addresses
  - Can be used to hide a number of hosts behind a single IP address
  - Uses private addresses:
    - 10.0.0.0-10.255.255.255,
    - 172.16.0.0-172.32.255.255 or
    - 192.168.0.0-192.168.255.255

Network Address Translation (NAT)

- NAT is a router function where IP addresses (and possibly port numbers) of IP datagrams are replaced at the boundary of a private network

- NAT is a method that enables hosts on private networks to communicate with hosts on the Internet

- NAT is run on routers that connect private networks to the public Internet, to replace the IP address-port pair of an IP packet with another IP address-port pair.

NAT-Network Address Translation

- With the growing number of internet users, it might be possible that we might be running out of IP addresses
- NAT solves the problem
- The basic idea behind NAT is to assign each company a small number of IP addresses
- Within the company, every computer gets a unique IP address, which is used for routing internal traffic.
- But when a packet exits the company and goes to the ISP, an address translation takes place.
- The NAT box is often combined in a single device with a firewall, which provides security by

Contd…

- In most situations, only a portion of computers in a small network need access to the Internet simultaneously. A technology that can provide the mapping between the private and universal addresses, and at the same time support virtual private networks, which, is Network Address Translation (NAT). The technology allows a site to use a set of private addresses for internal communication and a set of global Internet addresses (at least one) for communication with the rest of the world.

Contd...

- Within the company premises, every machine has a unique address of the form 10.x.y.z.
- When a packet leaves the company premises, it passes through a NAT box that converts the internal IP source address, 10.0.0.1 to the company's true IP address, 198.60.42.12
- The TCP Source port field is replaced by an index into the NAT box's entry translation table
- This table entry contains the original IP address and the original source port.
- Finally, both the IP and TCP header checksums are recomputed and inserted into the packet.

Contd...

- It is necessary to replace the Source port because connections from machines 10.0.0.1 and 10.0.0.2 may both happen to use port 5000. So the Source port alone is not enough to identify the sending process.
- When a packet arrives at the NAT box from the ISP, the Source port in the TCP header is extracted and used as an index into the NAT box's mapping table.
- From the entry located, the internal IP address and original TCP Source port are extracted and inserted into the packet.
- Then both the IP and TCP checksums are

Figure : ***NAT***

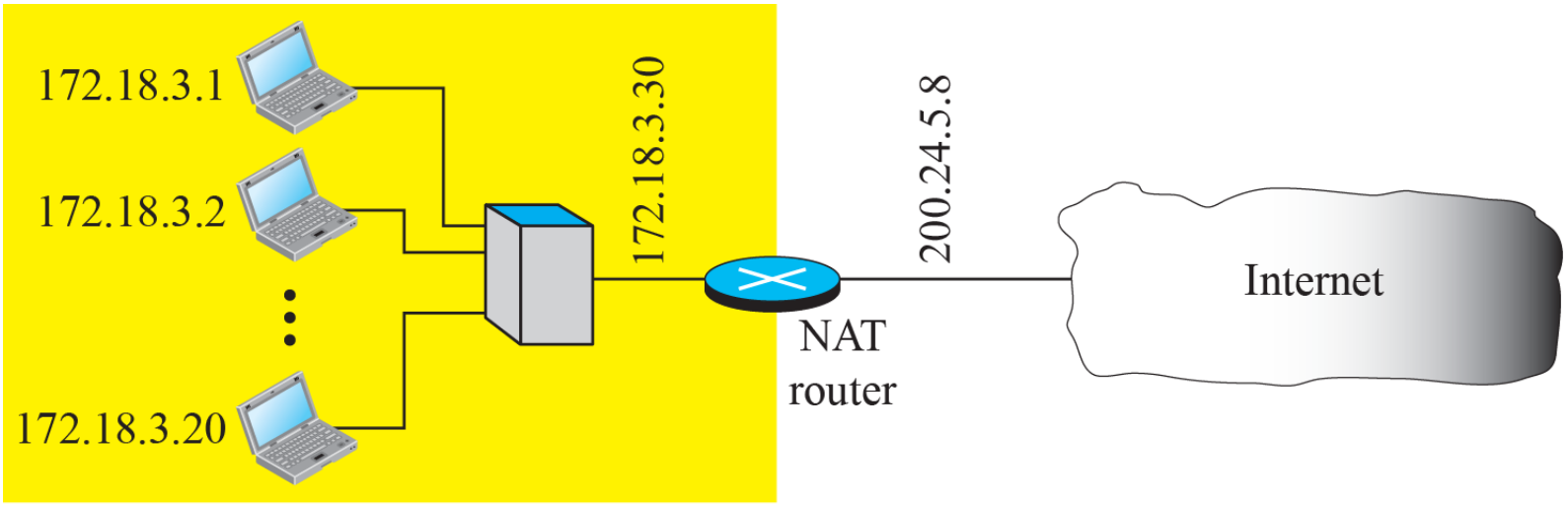

172.18.3.1
172.18.3.2
172.18.3.20
172.18.3.30
200.24.5.8
NAT
router
Internet
Site using private addresses

Figure : ***Address translation***

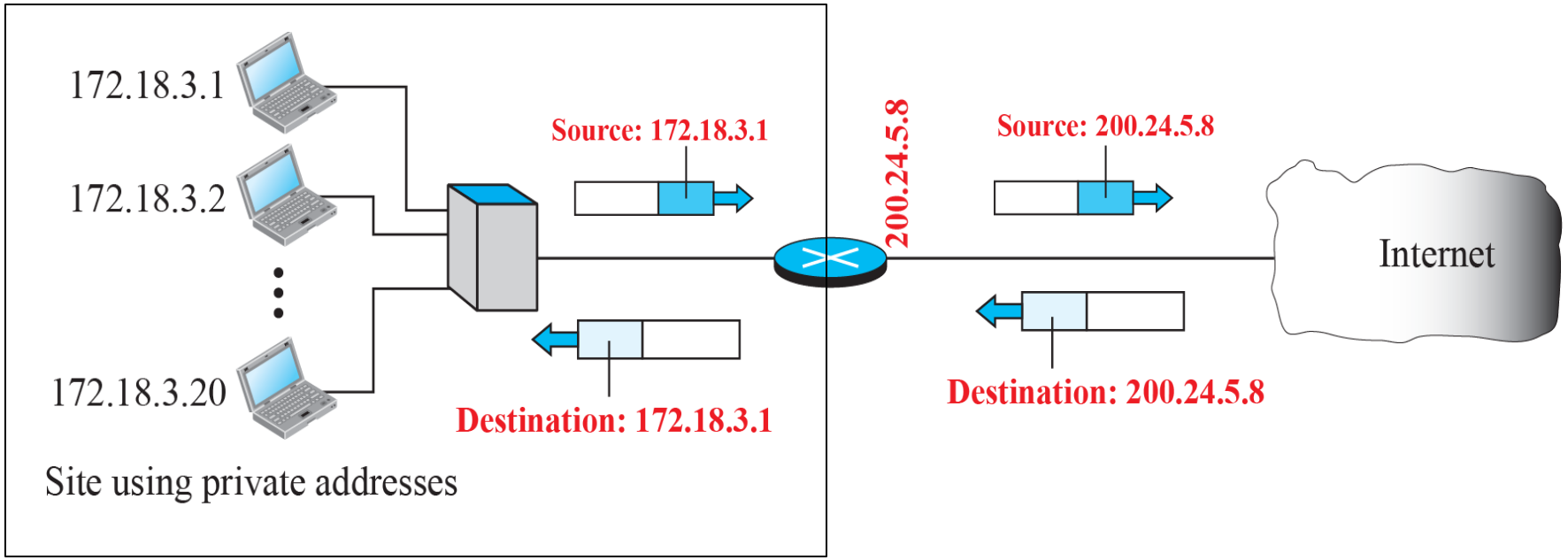


Figure : Translation

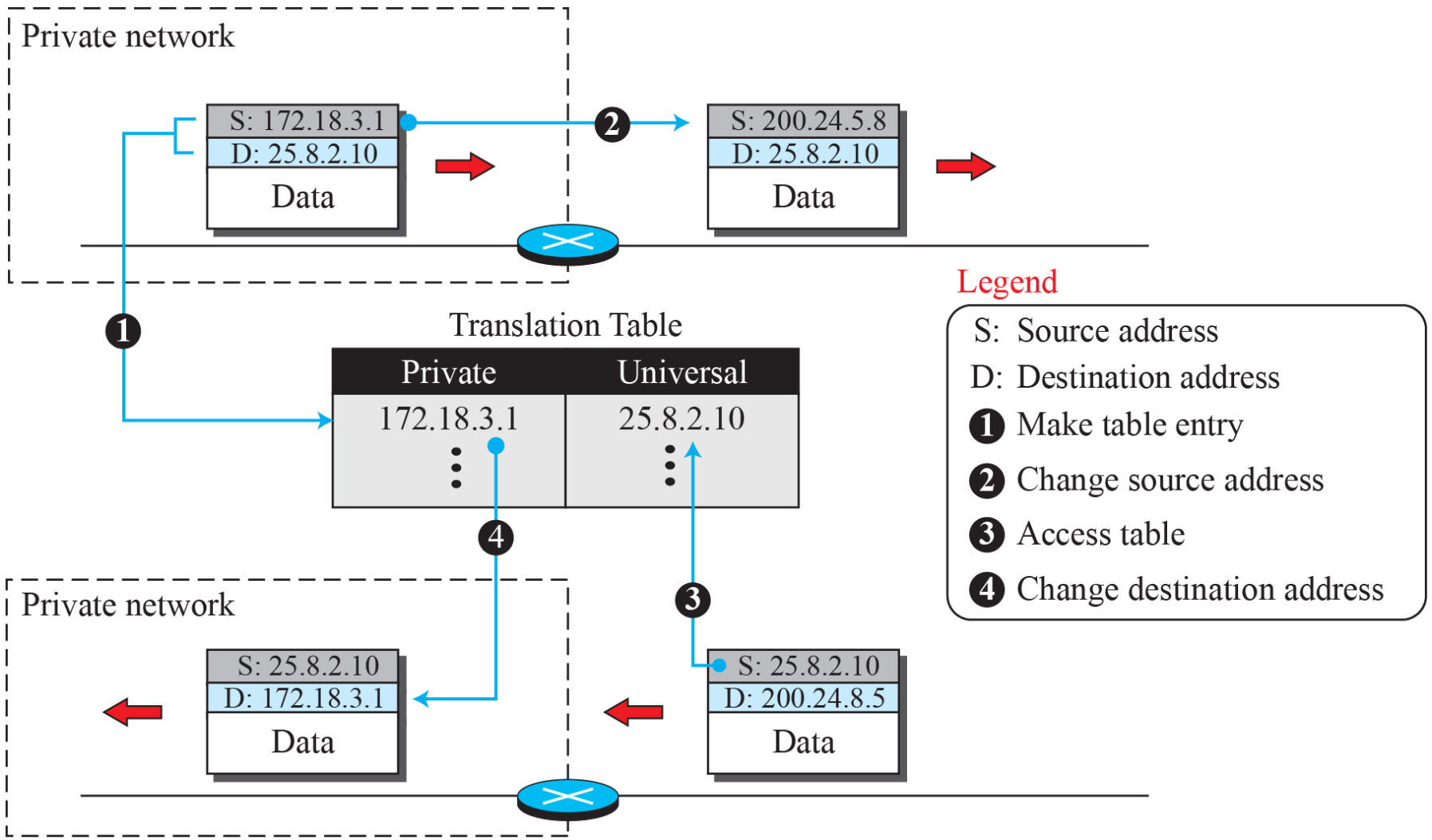
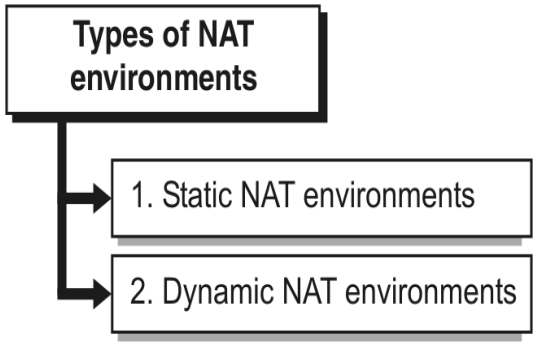


Table : Five-column translation table

Private address	*Private port*	*External address*	*External port*	*Transport protocol*
172.18.3.1	1400	25.8.3.2	80	TCP
172.18.3.2	1401	25.8.3.2	80	TCP
⋮	⋮	⋮	⋮	⋮

Type of NAT



- **1. Static:** In a static NAT environment, the NAT router maps private and public addresses on a one-to-one basis, that is, the private address of a given device always maps to the same public address.
- This type of NAT environment is commonly used for devices that need to be accessible to the public network
- **2. Dynamic:** In a dynamic NAT environment, the NAT router dynamically allocates public IP addresses, from a group of addresses, to devices on the private network that wish to communicate with the public network.
- **3. (PAT):** PAT (Port Address Translation), maps multiple private addresses to the same public address using different ports.

Contd…

Advantages of NAT –

- NAT conserves legally registered IP addresses.
- It provides privacy as the device’s IP address, sending and receiving the traffic, will be hidden.
- Eliminates address renumbering when a network evolves.

IPv6 ADDRESSES

Despite all short-term solutions, address depletion is still a long-term problem for the Internet. This and other problems in the IP protocol itself have been the motivation for IPv6.

It is also called IP new generation (IPng) protocol

IETF (Internet Engineering Task Force) has developed IPv6 with the very old problem regarding IPv4 address exhaustion.

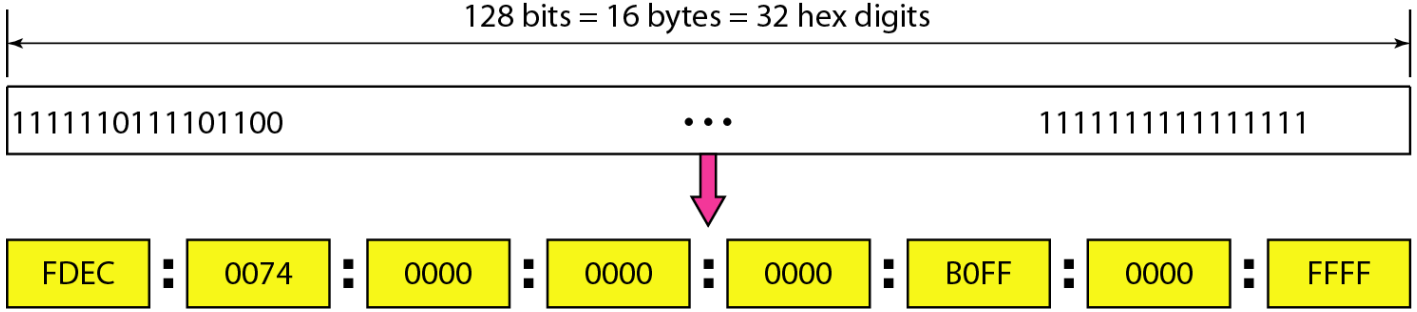
With drastic growth of the Internet, it became necessary that there is requirement of far more addresses for connecting devices than the existing IPv4 address space had available. 128-bit addresses are used by the IPv6, hypothetically allowing 2^128

Compare between IPv4 and IPv6

Parameter	IPv4	IPv6
Length	IPv4 has 32-bit address length	IPv6 has 128-bit address length
Address Configuration	Has support for Manual and DHCP configuration.	Has support for Auto-configuration and renumbering
Fragmentation	Fragmentation is implemented by sender and forwarding routers.	Fragmentation is implemented only by sender.
Addresses	Availability of maximum of 4.3 billion addresses.	Nearly limitless number of IP addresses available.
Checksum field	Available	Not available
Security features	Security is dependent on application.	For security purpose IPSEC is inbuilt in the IPv6 protocol.
Address Representation	Decimal form	Hexadecimal form
Option fields	Available	Not available but IPv6 Extension headers are available.
Message Transmission Scheme	Broadcasting	Multicasting and Anycasting
Packet flow identification	Not Available	Available
Encryption and Authentication	Not Provided	Provided

IPv6 Address

- An IPv6 address is 128 bits long (16-byte).
- Hexadecimal Colon Notation



- Abbreviation

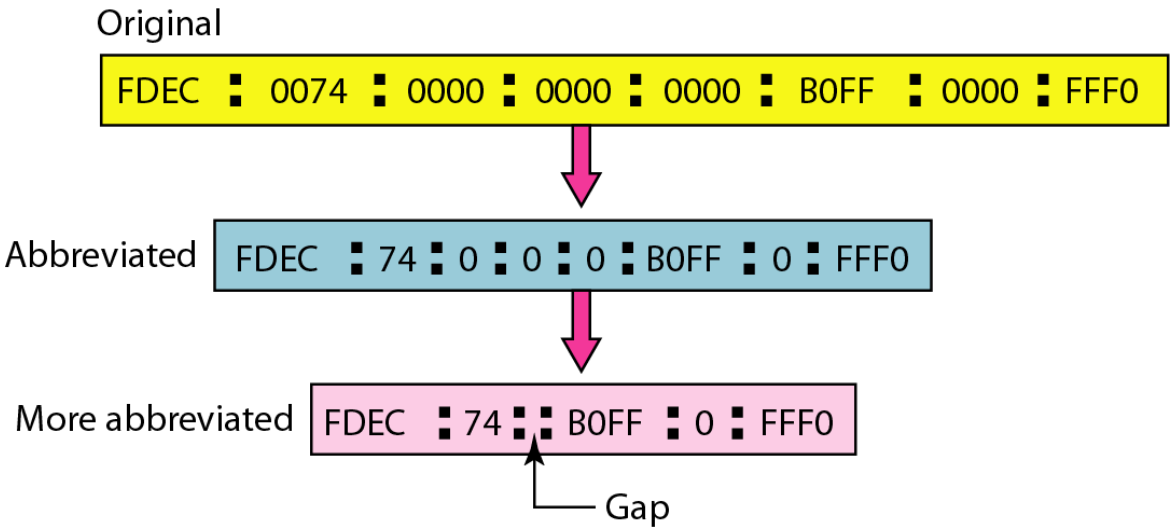
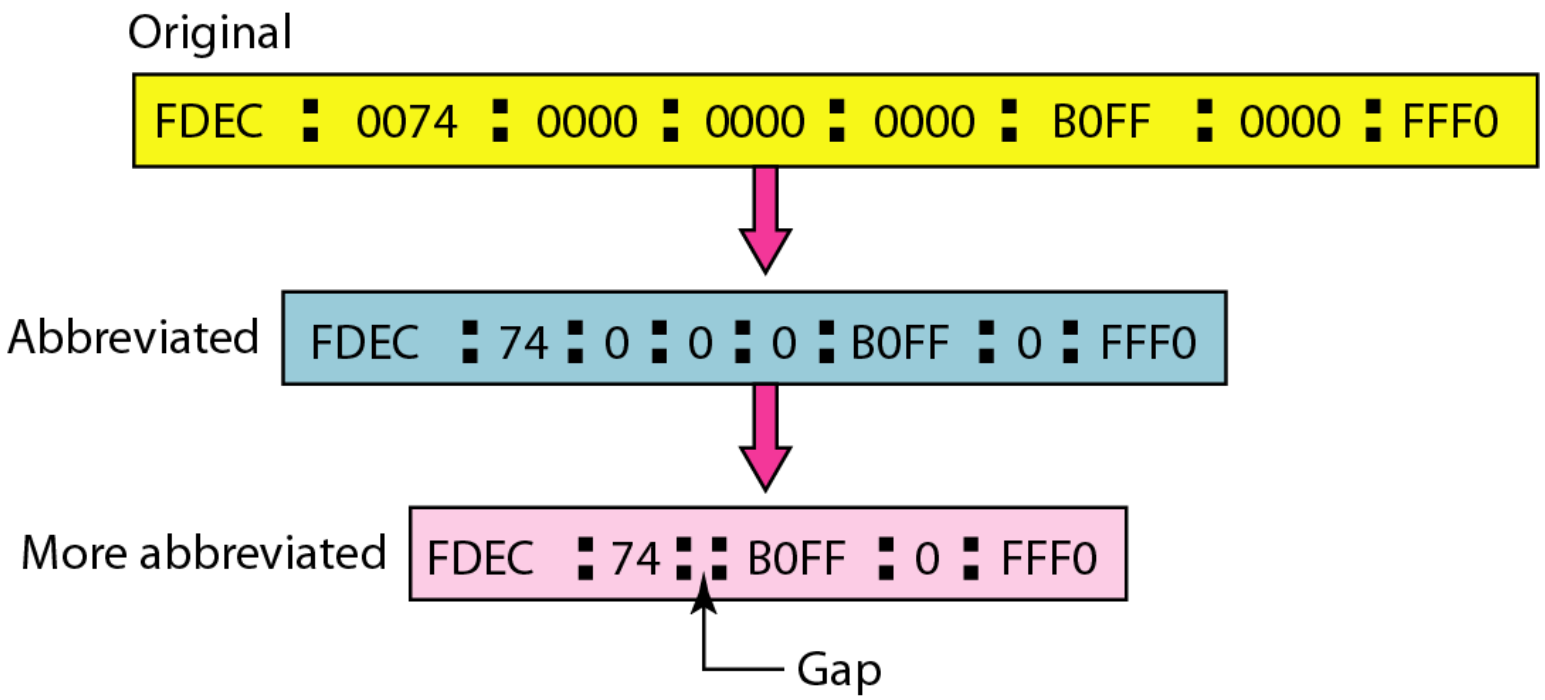


Figure: *Abbreviated IPv6 addresses*



Example 1

Expand the address 0:15::1:12:1213 to its original.

Solution

We first need to align the left side of the double colon to the left of the original pattern and the right side of the double colon to the right of the original pattern to find how many 0s we need to replace the double colon.

```
xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
  0:   15:                   :    1:   12:1213
```

This means that the original address is.

```
0000:0015:0000:0000:0000:0001:0012:1213
```

Structure of IPv6 Address

- Type prefix
  - For categorization,
  - Variable length,
  - No partial conflict among the different prefix

Type prefixes for IPv6 addresses

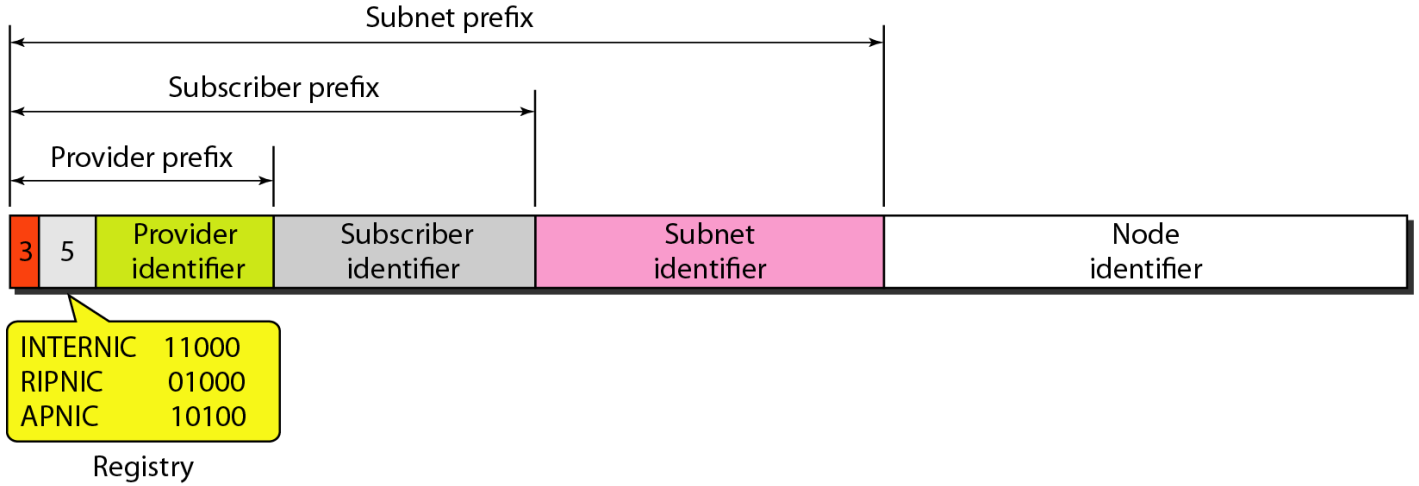
Type Prefix	*Type*	*Fraction*
0000 0000	Reserved	1/256
0000 0001	Unassigned	1/256
0000 001	ISO network addresses	1/128
0000 010	IPX (Novell) network addresses	1/128
0000 011	Unassigned	1/128
0000 1	Unassigned	1/32
0001	Reserved	1/16
001	Reserved	1/8
010	**Provider-based unicast addresses**	**1/8**

Type prefixes for IPv6 addresses

Type Prefix	*Type*	*Fraction*
011	Unassigned	1/8
100	Geographic-based unicast addresses	1/8
101	Unassigned	1/8
110	Unassigned	1/8
1110	Unassigned	1/16
1111 0	Unassigned	1/32
1111 10	Unassigned	1/64
1111 110	Unassigned	1/128
1111 1110 0	Unassigned	1/512
1111 1110 10	Link local addresses	1/1024
1111 1110 11	Site local addresses	1/1024
1111 1111	Multicast addresses	1/256

Unicast

- For a single computer
- Two types of unicast addresses
  - Geographically based
  - Provider-based
- Fields
  - Type ID (3-bit), Registry ID (5-bit), Provider ID (16-bit), Subscriber ID (24-bit), Subnet ID (32-bit), Node ID (48-bit)



Multicast address in IPv6

- For a group of hosts
- To deliver packets to each member

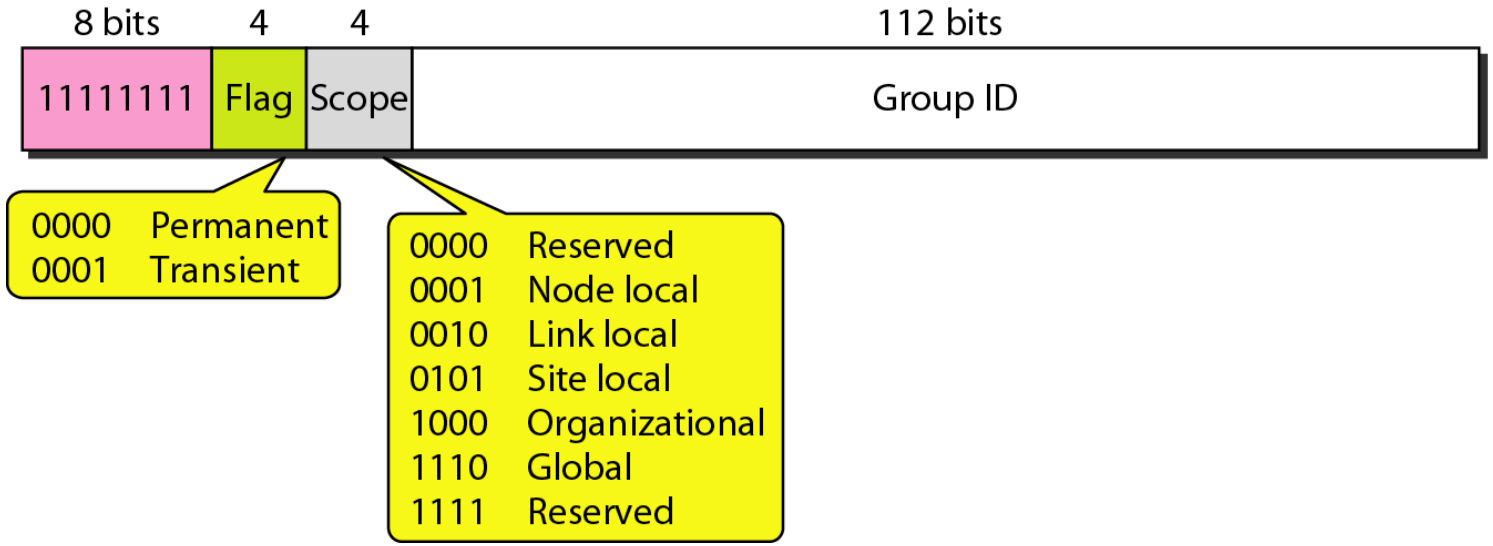
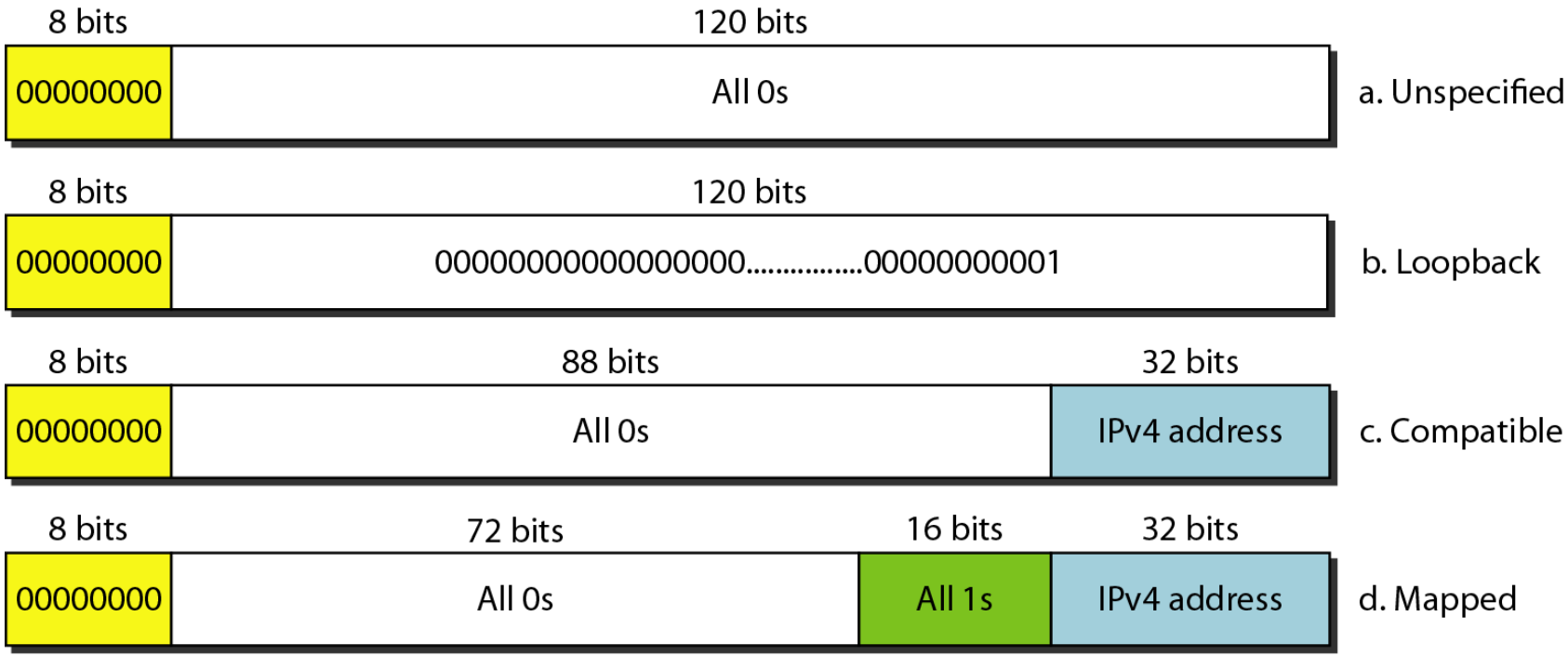
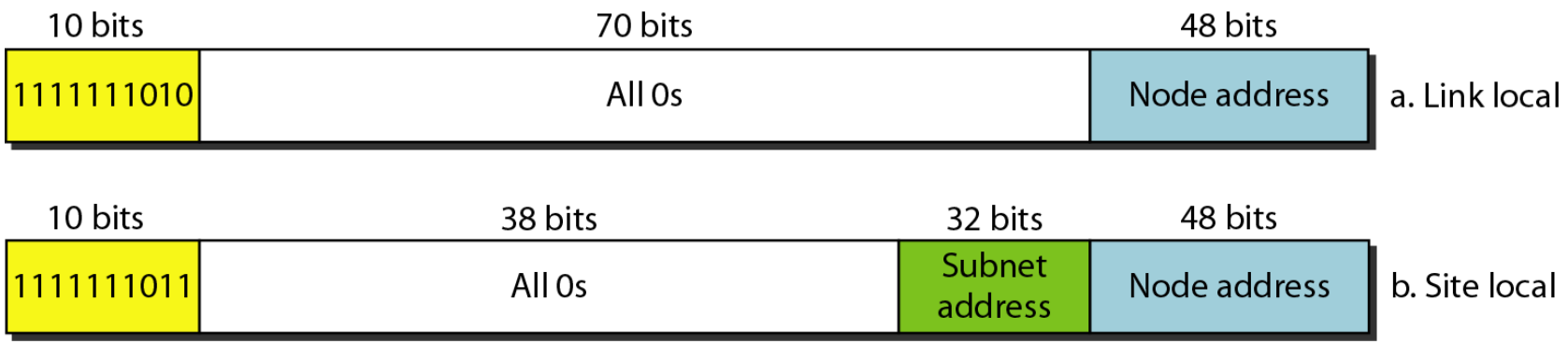


Figure *Reserved addresses in IPv6*



Local addresses in IPv6

- To use IPv6 without connecting to the global Internet.



Transition from IPV4 to IPV6

- To have smooth transition from IPv4 to IPv6. People should stop using Ipv4 and should start using IPv6.
- Following strategies used to handle the transition from IPv4 to IPV6
  - 1. Dual stack
  - 2. Tunneling
  - 3. Header translation

IPv6 Header

- IPv6 fixed header starts an IPv6 packet and has a size of 40 octets (320 bits).It has the following format :

Offsets Octet	Octet Bit	0								1								2								3							
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				Traffic Class								Flow Label																			
4	32	Payload Length																Next Header								Hop Limit							
8	64	Source Address																															
12	96																																
16	128																																
20	160																																
24	192	Destination Address																															
28	224																																
32	256																																
36	288																																

Contd...

- **Traffic Class(8 bits)**

– This field represents the class or priority of the IPv6 packet. Its size is eight bits. The Traffic Class field has same functionality as of the Service field of IPv4.

- **Flow Label (20 bits)**

– The use of Flow Label is for non-default quality of service connections, for example those required by real-time data (voice and video).

– For the purpose of default router handling, the value of Flow Label is set as 0.

- **Payload Length (16 bits)**

– This field represents the length of the IPv6 payload. This field has size of 16 bits. This field contains the extension headers as well as the upper layer PDU (Protocol Data Unit).

– If payload length is greater than 65,535 bytes, then the value of Payload Length field is set to 0 and the Jumbo Payload option comes in picture in the Hop-by-Hop Options extension header.

- **Next Header (8 bits)**

– Specifies the type of the next header. This field usually specifies the transport layer protocol used by a packet's payload.

– When extension headers are present in the packet this field indicates which extension header follows.

- **Hop Limit(8 bits)**

– Replaces the time to live field of IPv4. This value is decremented by one at each forwarding node and packet discarded if it becomes 0.

– **Source Address (128 bits) :** The IPv6 address of the sending node.

- **Destination Address (128 bits) :** The IPv6 address of the destination node(s).