Subject Name: Computer Networks

Module 4 : Network Layer

Faculty Name : Dr. Savita R. Bhosale
Dr. Ashwini Naik
Dr. Dhananjay Dakhane
Ms. Shweta Ashtekar
Ms. Jyoti Vengurlekar
Ms. Krupali Kanekar
Mr. Dayanand Dhongade

Index

Unit No: 4 Unit name: Network Layer

Lecture No: 22
Internet Protocol (IP)

IP Address

What is an IP Address?

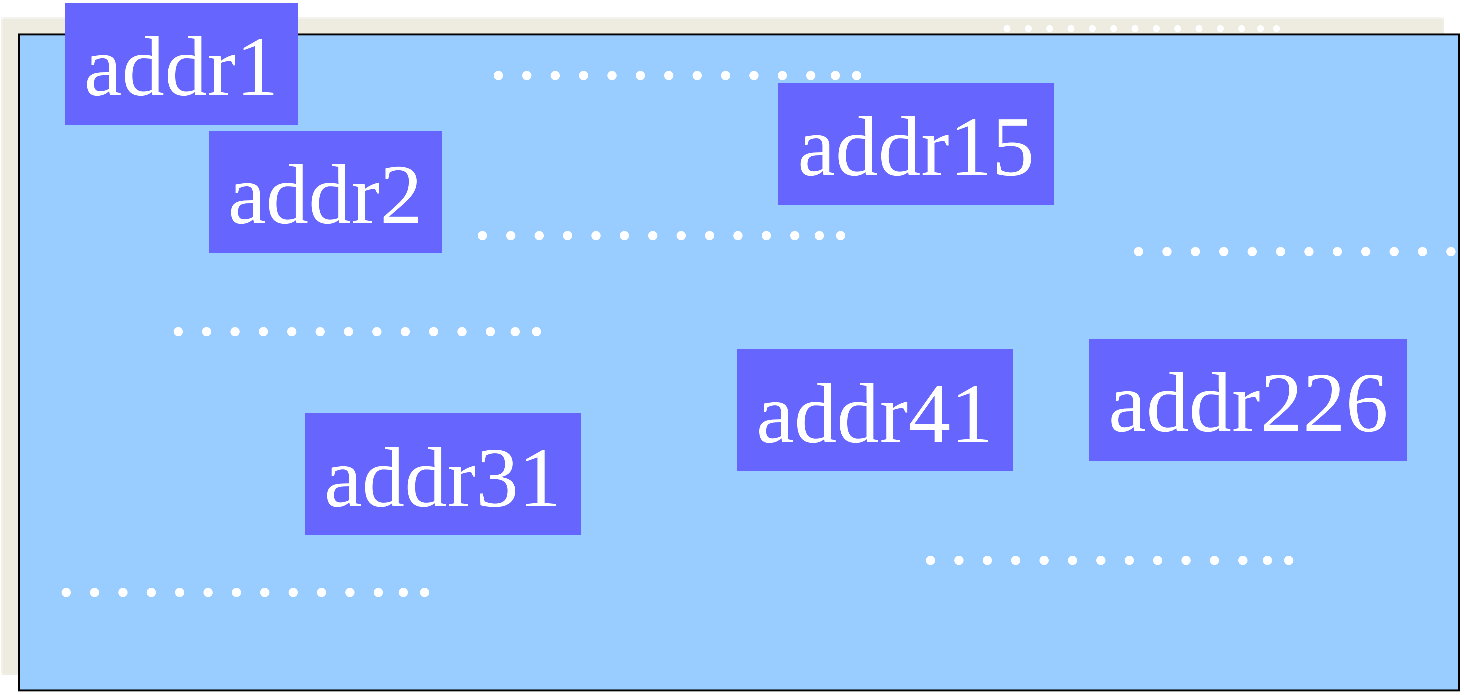
An IP address is a 32-bit address.

Note

The IP addresses are unique.

IP Address

Address Space



D Y PATIL DEEMED TO BE UNIVERSITY RAMRAO ADIK INSTITUTE OF TECHNOLOGY NAVI MUMBAI

Address space rule

The address space in a protocol That uses N-bits to define an Address is:

$$2^N$$

D Y PATIL DEEMED TO BE UNIVERSITY RAMRAO ADIK INSTITUTE OF TECHNOLOGY NAVI MUMBAI

IPv4 address space

The address space of IPv4 is

2^{32}

or

4,294,967,296.

IP Address

Binary Notation

01110101 10010101 00011101 11101010

IP Address

Dotted-decimal notation

10000000 00001011 00000011 00011111

128.11.3.31

Hexadecimal Notation

0111 0101 1001 0101 0001 1101 1110 1010

75 95 1D EA

0x75951DEA

D Y PATIL
DEEMED TO BE
UNIVERSITY
RAMRAO ADIK
INSTITUTE OF TECHNOLOGY
NAVI MUMBAI

IP Address Example

- Change the following IP address from binary notation to dotted-decimal notation.
- 10000001 00001011 00001011 11101111

Solution

129.11.11.239

IP Address Example

Change the following IP address from dotted-decimal notation to binary notation:

111.56.45.78

Solution

01101111 00111000 00101101 01001110

IP Address Example

Find the error in the following IP Address
111.56.045.78

Solution

There are no leading zeroes in
Dotted-decimal notation (045)

IP Address Example

Find the error in the following IP Address
75.45.301.14

Solution

In decimal notation each number <= 255
301 is out of the range

IP Address Example

Change the following binary IP address Hexadecimal notation

10000001 00001011 00001011 11101111

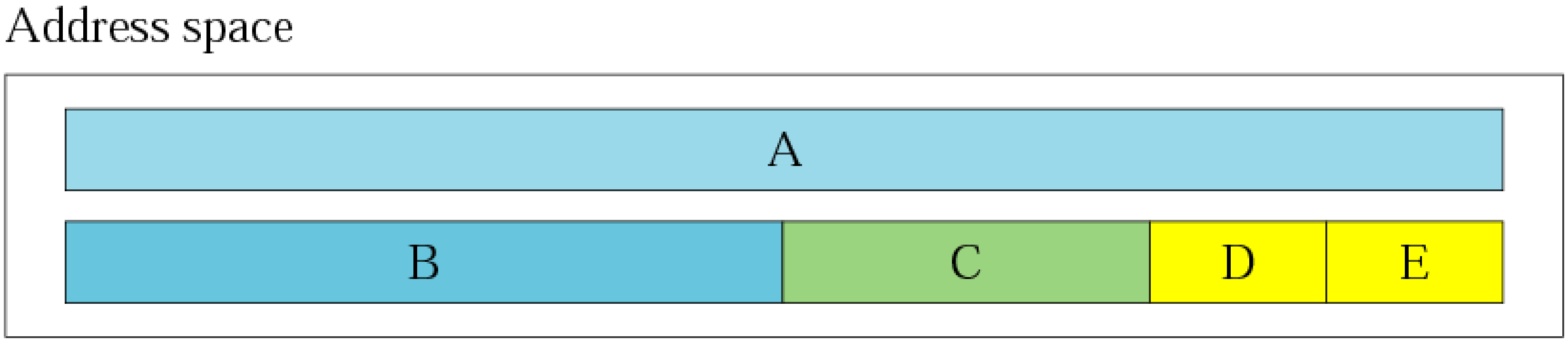
Solution

0X810B0BEF or 810B0BEF16

IP Address

CLASSFUL ADDRESSING

Occupation of the address space



IP Address (Classful Addressing)

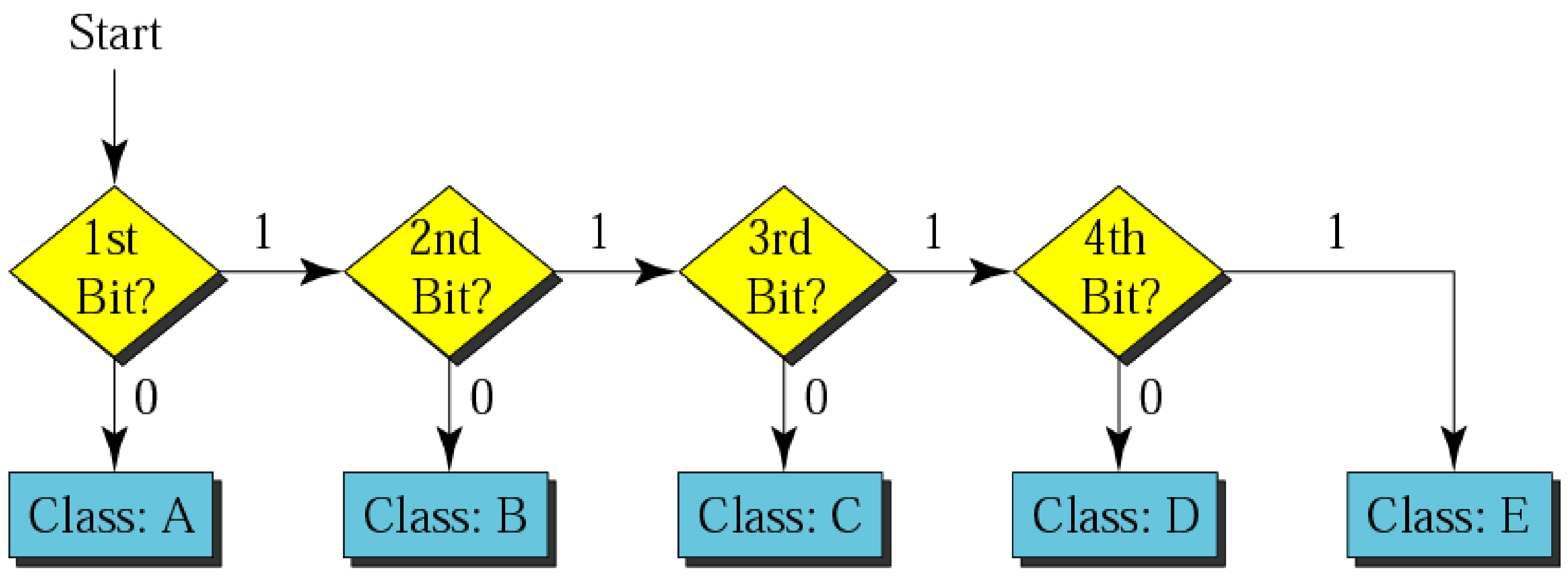
In classful addressing the address space is divided into 5 classes:

A, B, C, D, and E.

Finding the class in binary notation

	First byte	Second byte	Third byte	Fourth byte
Class A	**0**			
Class B	**10**			
Class C	**110**			
Class D	**1110**			
Class E	**1111**			

Finding the address class



IP Address (Classful Addressing)

Show that Class A has
231 = 2,147,483,648 addresses

D Y PATIL DEEMED TO BE UNIVERSITY
RAMRAO ADIK INSTITUTE OF TECHNOLOGY
NAVI MUMBAI

IP Address (Classful Addressing)

Find the class of the following IP addresses
00000001 00001011 00001011 11101111
11000001 00001011 00001011 11101111

Solution

00000001 00001011 00001011 11101111
1st is 0, hence it is Class A
11000001 00001011 00001011 11101111
1st and 2nd bits are 1, and 3rd bit is 0 hence, Class C

IP Address (Classful Addressing)

Finding the class in decimal notation

	First byte	Second byte	Third byte	Fourth byte
Class A	**0 to 127**			
Class B	**128 to 191**			
Class C	**192 to 223**			
Class D	**224 to 239**			
Class E	**240 to 255**			

IP Address (Classful Addressing)

Find the class of the following addresses
158.223.1.108
227.13.14.88

Solution

158.223.1.108
1st byte = 158 (128<158<191) class B
227.13.14.88
1st byte = 227 (224<227<239) class D

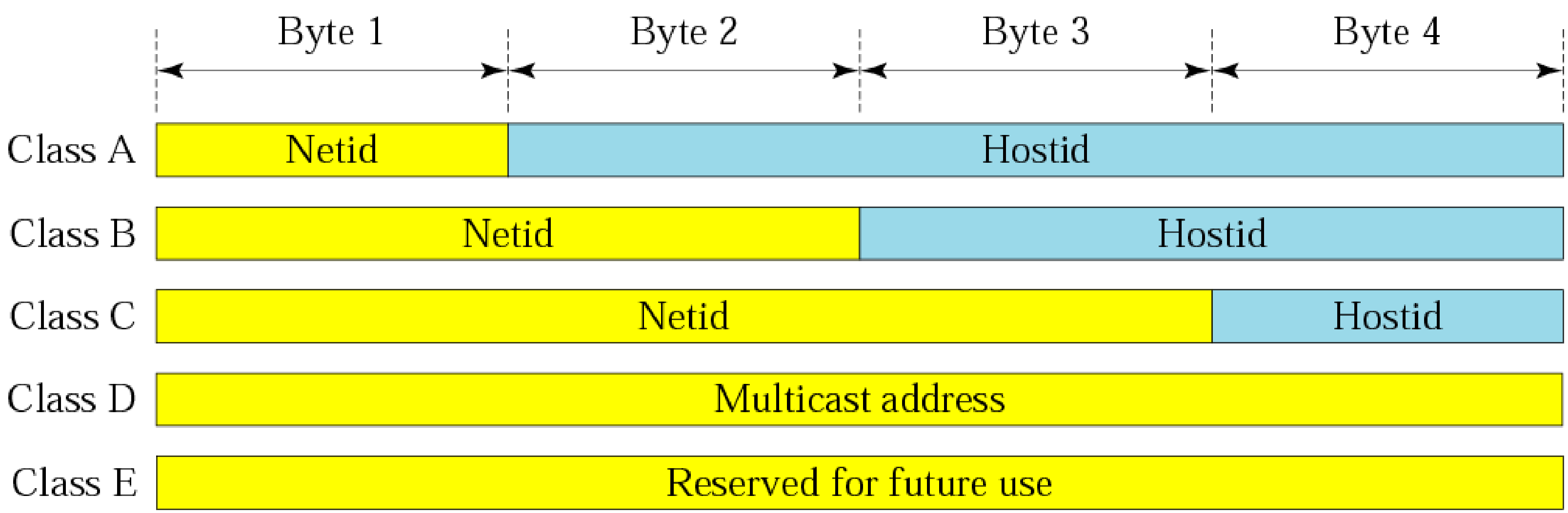
D Y PATIL
DEEMED TO BE UNIVERSITY
RAMRAO ADIK INSTITUTE OF TECHNOLOGY
NAVI MUMBAI

IP address with appending port number

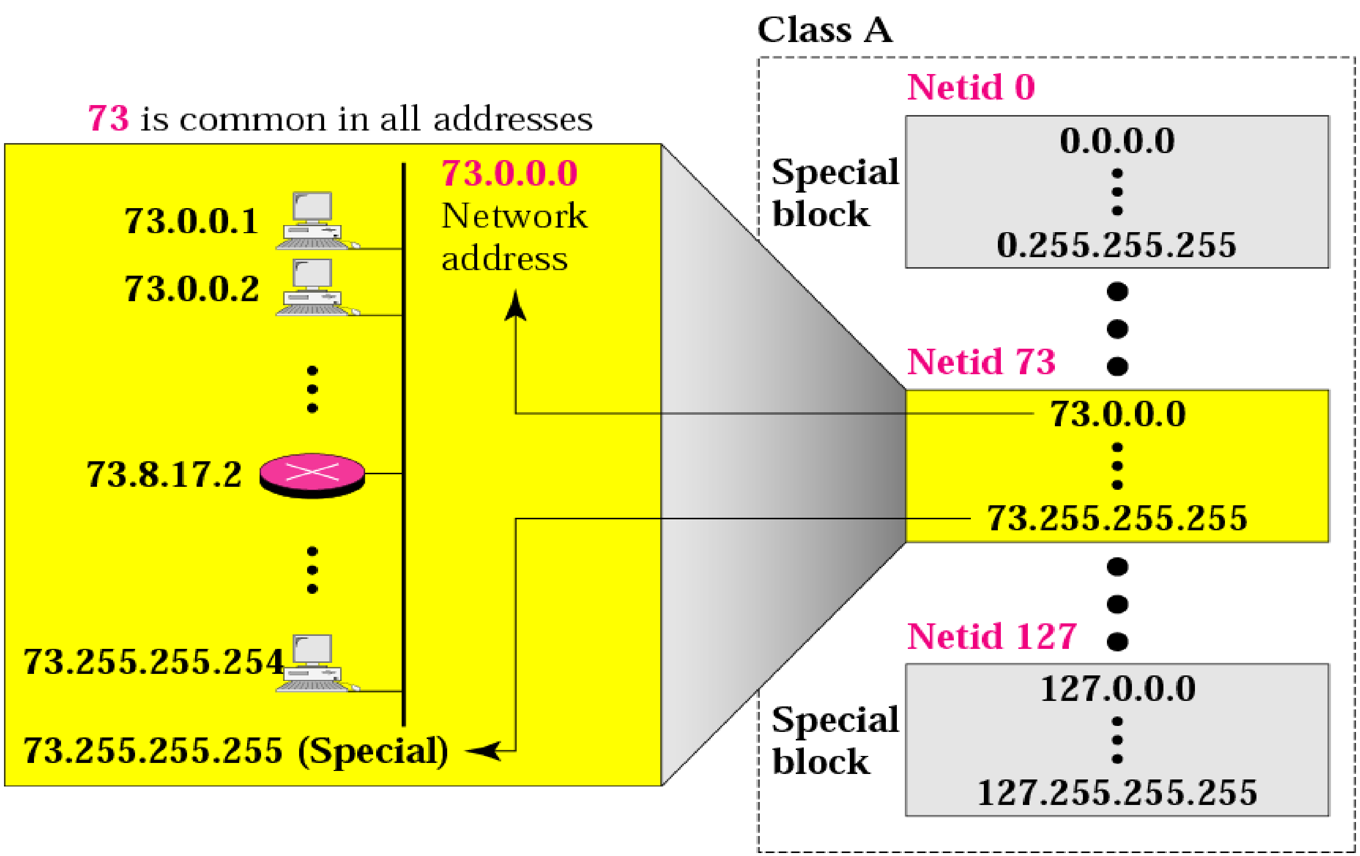
- 158.128.1.108:25
- the for octet before colon is the IP address
- The number of colon (25) is the port number

IP Address (Classful Addressing)

Netid and hostid



Blocks in class A

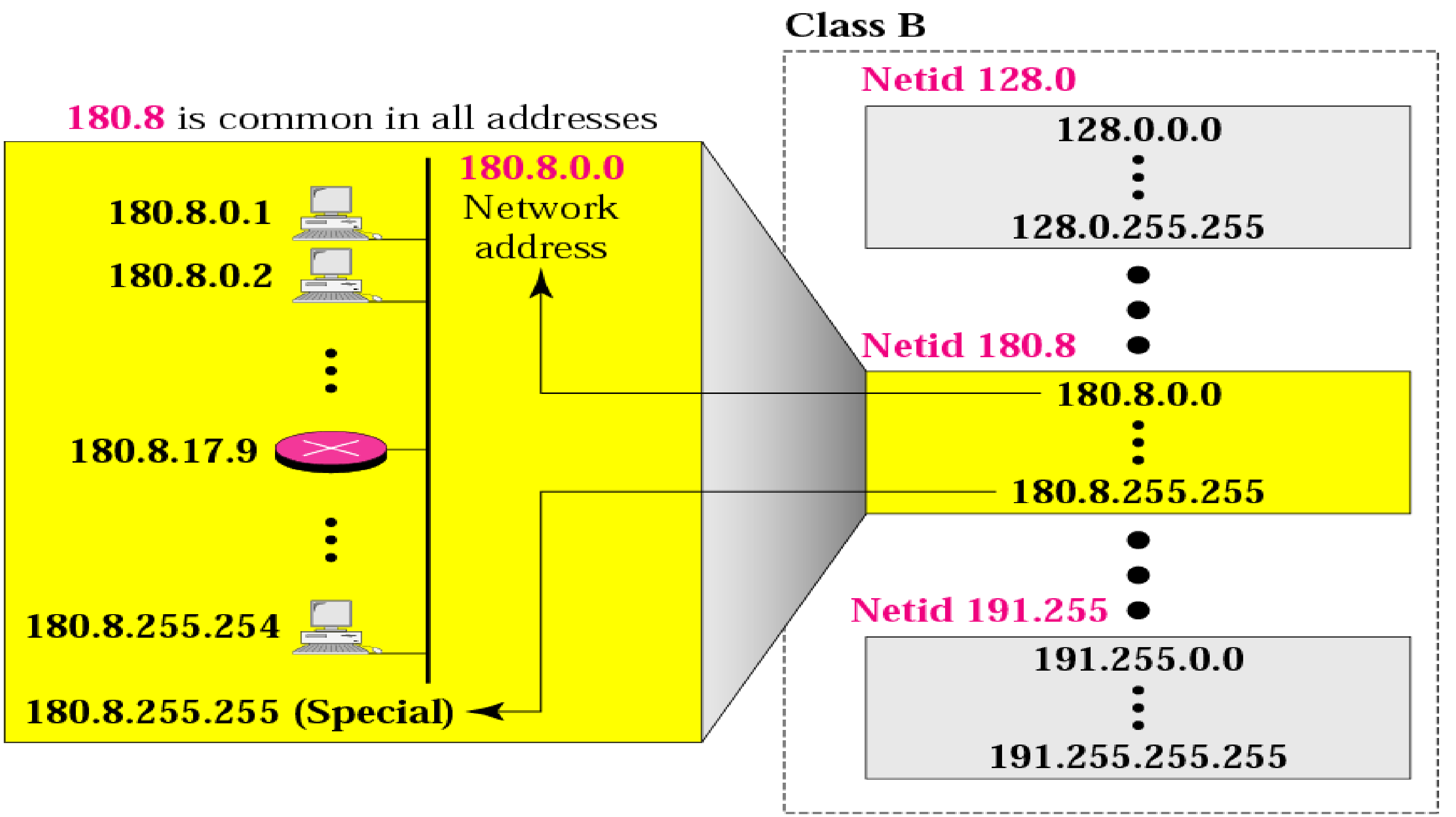


128 blocks: 16,777,216 addresses in each block

Blocks in class A

Millions of class A addresses are wasted.

Blocks in class B

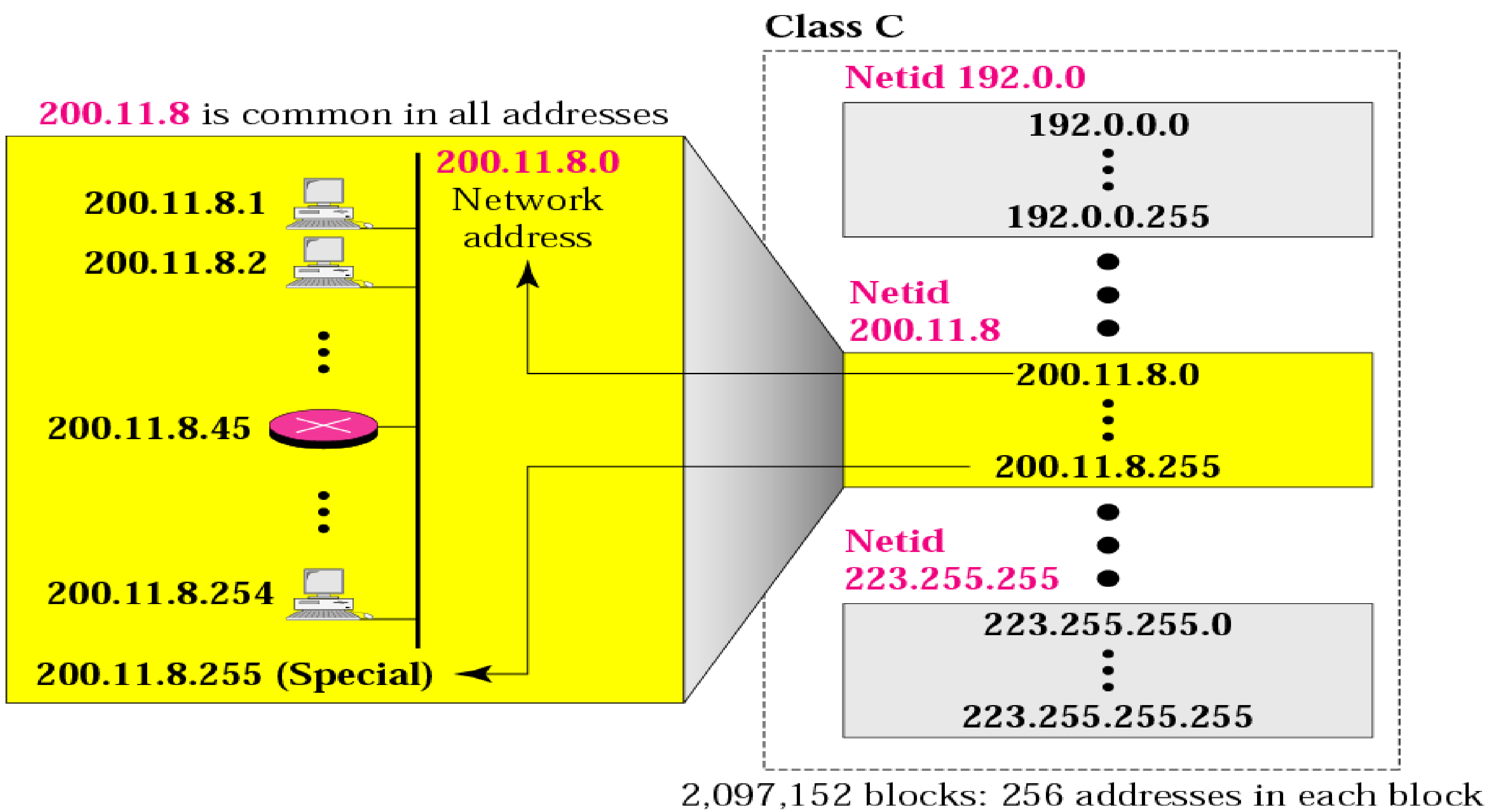


16,384 blocks: 65,536 addresses in each block

Blocks in class B

Many class B addresses are wasted.

Blocks in class C



Blocks in class C

The number of addresses in a class C block is smaller than the needs of most organizations.

Blocks in class D

Class D addresses are used for multicasting; there is only one block in this class.

Blocks in class E

Class E addresses are reserved for special purposes; most of the block is wasted.

NETWORK ADDRESS

The network address is the first address.

The network address defines the network to the rest of the Internet.

Given the network address, we can find the class of the address, the block, and the range of the addresses in the block

NETWORK ADDRESS

In classful addressing,
the network address
(the first address in the block)
is the one that is assigned
to the organization.

NETWORK ADDRESS

Given the network address 132.21.0.0, find the class, the block, and the range of the addresses

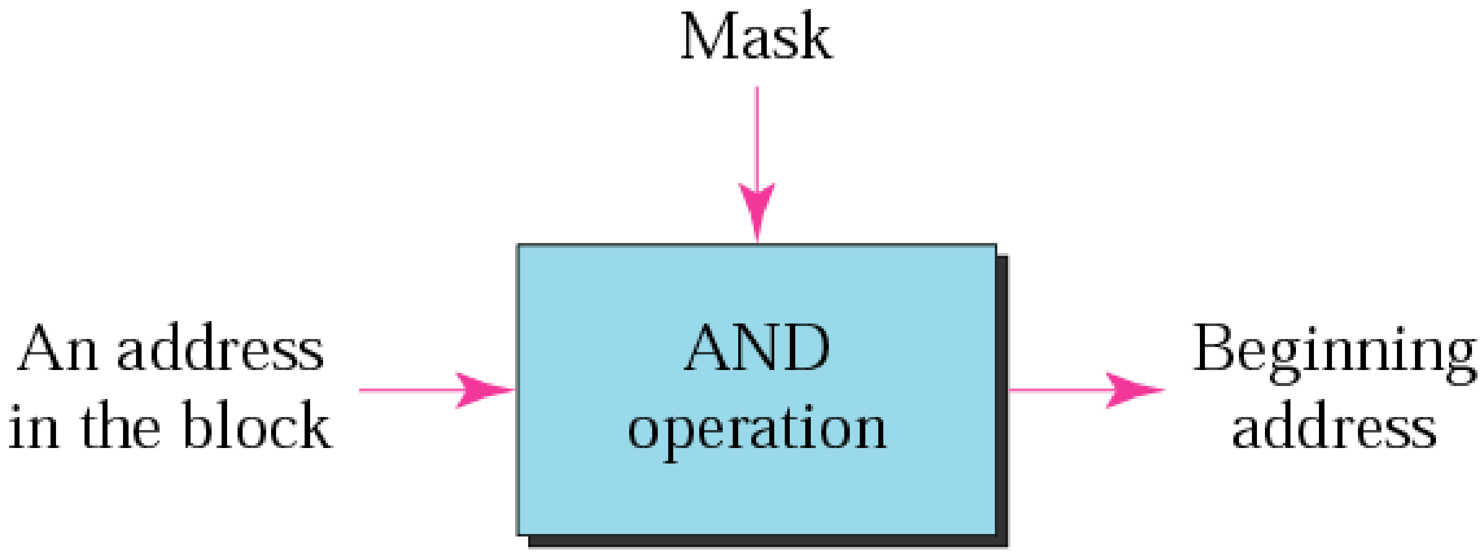
Solution

The 1st byte is between 128 and 191.
Hence, Class B
The block has a netid of 132.21.
The addresses range from
132.21.0.0 to 132.21.255.255.

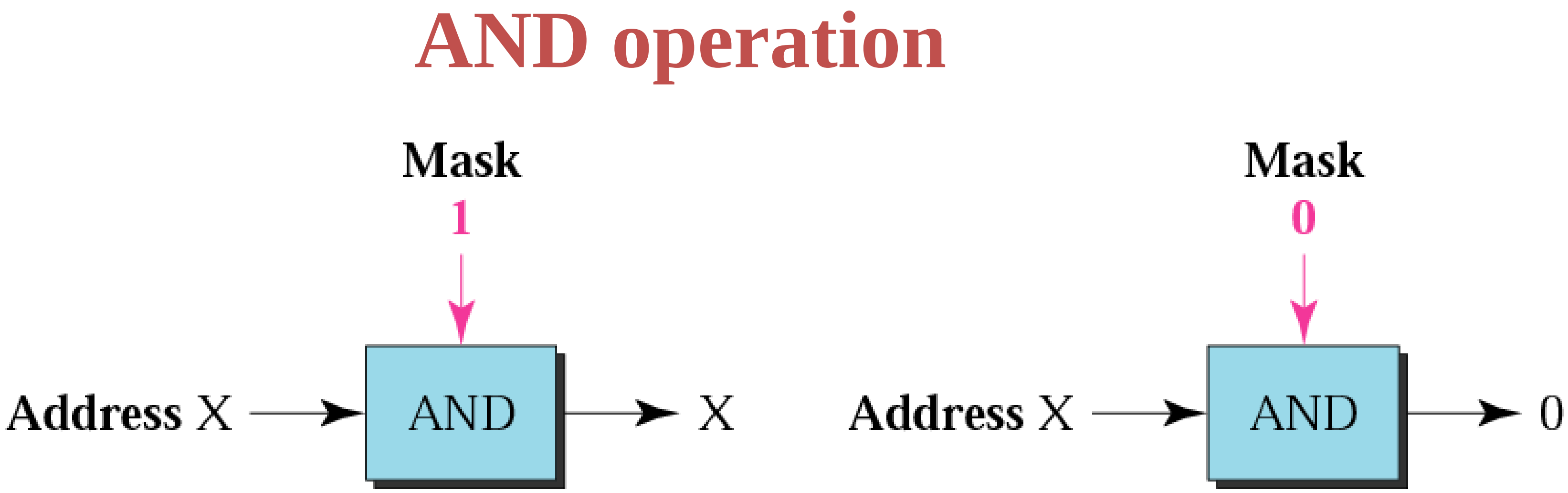
Mask

- A mask is a 32-bit binary number.
- The mask is ANDeD with IP address to get
  - The block address (Network address)
  - Mask And IP address = Block Address

Masking Concept



Masking Concept



Mask

The network address is the beginning address of each block.
It can be found by applying the default mask to any of the addresses in the block (including itself).
It retains the ***netid*** *of the block and sets the* ***hostid*** *to zero.*

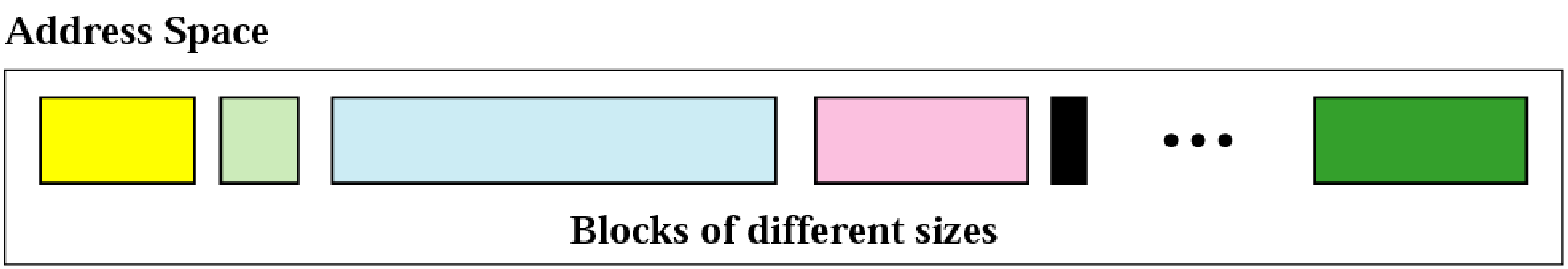
Default Mask

- Class A default mask is 255.0.0.0
- Class B default mask is 255.255.0.0
- Class C Default mask 255.255.255.0

Variable Length Blocks

In classless addressing variable-length blocks are assigned that belong to no class. In this architecture, the entire address space (232 addresses) is divided into blocks of different sizes.

Variable Length Blocks



Example

Which of the following can be the beginning address of a block that contains 16 addresses?

a. 205.16.37.32 *b.190.16.42.44*
c. 17.17.33.80 *d.123.45.24.52*

Solution

Only two are eligible (a and c). The address 205.16.37.32 is eligible because 32 is divisible by 16. The address 17.17.33.80 is eligible because 80 is divisible by 16.

Example

Which of the following can be the beginning address of a block that contains 256 addresses?

a.205.16.37.32 *b.190.16.42.0*
c.17.17.32.0 *d.123.45.24.52*

Solution

In this case, the right-most byte must be 0. As The IP addresses use base 256 arithmetic. When the right-most byte is 0, the total address is divisible by 256. Only two addresses are eligible (b and c).

D Y PATIL DEEMED TO BE UNIVERSITY RAMRAO ADIK INSTITUTE OF TECHNOLOGY NAVI MUMBAI

Example

Which of the following can be the beginning address of a block that contains 1024 addresses?

a. 205.16.37.32 *b.190.16.42.0*
c. 17.17.32.0 *d.123.45.24.52*

Solution

In this case, we need to check two bytes because 1024 = 4 × 256. The right-most byte must be divisible by 256. The second byte (from the right) must be divisible by 4. Only one address is eligible (c).

Format of classless addressing address

x.y.z.t/n

Format of classless addressing address

/n	Mask	/n	Mask	/n	Mask	/n	Mask
/1	128.0.0.0	/9	255.128.0.0	/17	255.255.128.0	/25	255.255.255.128
/2	192.0.0.0	/10	255.192.0.0	/18	255.255.192.0	/26	255.255.255.192
/3	224.0.0.0	/11	255.224.0.0	/19	255.255.224.0	/27	255.255.255.224
/4	240.0.0.0	/12	255.240.0.0	/20	255.255.240.0	/28	255.255.255.240
/5	248.0.0.0	/13	255.248.0.0	/21	255.255.248.0	/29	255.255.255.248
/6	252.0.0.0	/14	255.252.0.0	/22	255.255.252.0	/30	255.255.255.252
/7	254.0.0.0	/15	255.254.0.0	/23	255.255.254.0	/31	255.255.255.254
/8	255.0.0.0	/16	255.255.0.0	/24	255.255.255.0	/32	255.255.255.255

Classless Addressing

Classful addressing is a special case of classless addressing.

Example

What is the first address in the block if one of the addresses is 167.199.170.82/27?

Solution

The prefix length is 27, which means that we must keep the first 27 bits as it is and change the remaining bits (5) to 0s. The following shows the process:

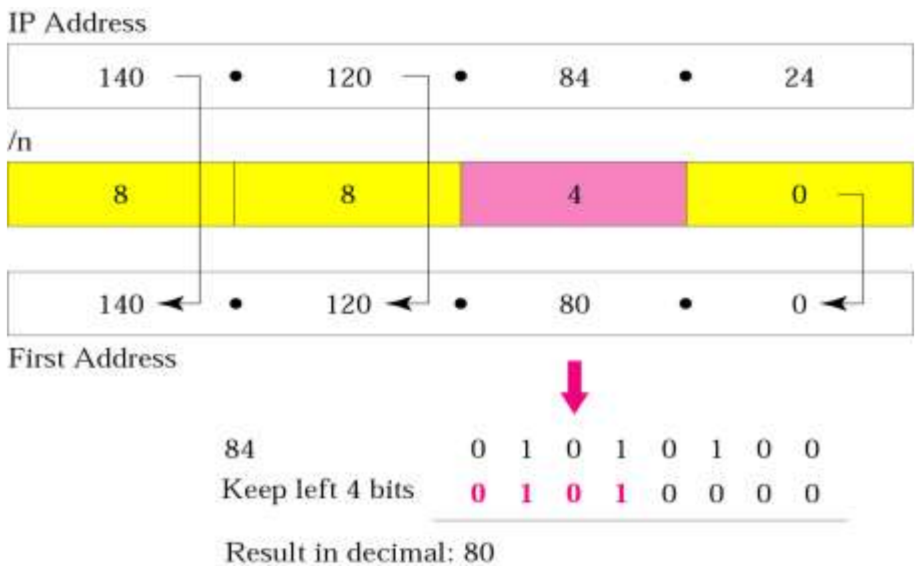
Address in binary: 10100111 11000111 10101010 01010010
Keep the left 27 bits: 10100111 11000111 10101010 01000000
Result in CIDR notation: 167.199.170.64/27

Example

What is the first address in the block if one of the addresses is 140.120.84.24/20?

Solution

Figure shows the solution. The first, second, and fourth bytes are easy; for the third byte we keep the bits corresponding to the number of 1s in that group. The first address is 140.120.80.0/20.



Example

Find the first address in the block if one of the addresses is 140.120.84.24/20.

Solution

The first, second, and fourth bytes are as defined in the previous example. To find the third byte, we write 84 as the sum of powers of 2 and select only the leftmost 4 (m is 4) as shown in Figure 5.4. The first address is 140.120.80.0/20.

	128	64	32	16	8	4	2	1
Write 84 as sum of:	0	64	0	16	0	4	0	0
Select only leftmost 4:	0	64	0	16				
Add to find the result:	80							

Example

Find the number of addresses in the block if one of the addresses is 140.120.84.24/20.

Solution

The prefix length is 20. The number of addresses in the block is 2^{32-20} *or* 2^{12} *or 4096. Note that this is a large block with 4096 addresses.*

Example

Using the first method, find the last address in the block if one of the addresses is 140.120.84.24/20.

Solution

We found in the previous examples that the first address is 140.120.80.0/20 and the number of addresses is 4096. To find the last address, we need to add 4095 (4096 − 1) to the first address.

Example

To keep the format in dotted-decimal notation, we need to represent 4095 in base 256 and do the calculation in base 256. We write 4095 as 15.255. We then add the first address to this number (in base 255) to obtain the last address as shown below:

```
140 . 120 .  80 .   0
              15  .  255
--------------------------
140 . 120 .  95 .  255
```

The last address is 140.120.95.255/20.

Example

Using the second method, find the last address in the block if one of the addresses is 140.120.84.24/20.

Solution

The mask has twenty 1s and twelve 0s. The complement of the mask has twenty 0s and twelve 1s. In other words, the mask complement is

00000000 00000000 00001111 11111111

or 0.0.15.255. We add the mask complement to the beginning address to find the last address.

Example

We add the mask complement to the beginning address to find the last address.

```
140 . 120 . 80 .   0
  0 .   0  . 15 . 255
-----------------------------
140 . 120 . 95 . 255
```

The last address is 140.120.95.255/20.

Example

Find the block if one of the addresses is 190.87.140.202/29.

Solution

We follow the procedure in the previous examples to find the first address, the number of addresses, and the last address. To find the first address, we notice that the mask (/29) has five 1s in the last byte. So we write the last byte as powers of 2 and retain only the leftmost five as shown below:

Example

202 → 128 + 64 + 0 + 0 + 8 + 0 + 2 + 0

The leftmost 5 numbers are → 128 + 64 + 0 + 0 + 8

The first address is 190.87.140.200/29

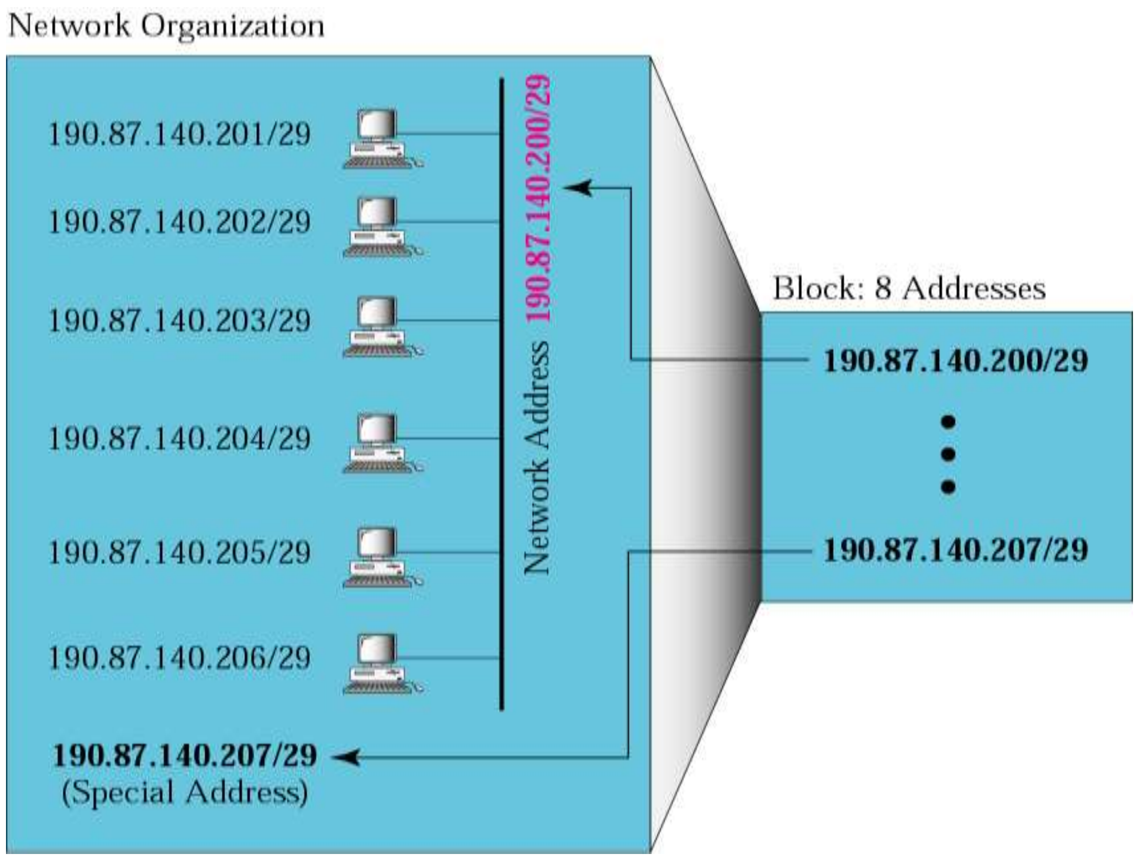
The number of addresses is 2^{32-29} or 8. To find the last address, we use the complement of the mask. The mask has twenty-nine 1s; the complement has three 1s. The complement is 0.0.0.7. If we add this to the first address, we get 190.87.140.207/29. In other words, the first address is 190.87.140.200/29, the last address is 190.87.140.207/20. There are only 8 addresses in this block.

Example

Show a network configuration for the block in the previous example.

Solution

The organization that is granted the block in the previous example can assign the addresses in the block to the hosts in its network. However, the first address needs to be used as the network address and the last address is kept as a special address (limited broadcast address). Figure 5.5 shows how the block can be used by an organization. Note that the last address ends with 207, which is different from the 255 seen in classful addressing.



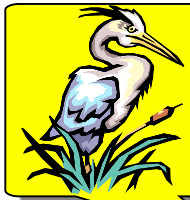
Network Organization
190.87.140.201/29
190.87.140.202/29
190.87.140.203/29
190.87.140.204/29
190.87.140.205/29
190.87.140.206/29
Network Address 190.87.140.200/29
190.87.140.207/29
(Special Address)
Block: 8 Addresses
190.87.140.200/29
190.87.140.207/29

Classless Addressing

Note:

In classless addressing, the last address in the block does not necessarily end in 255.

CIDR (Classless Inter-Domain Routing)



Note:

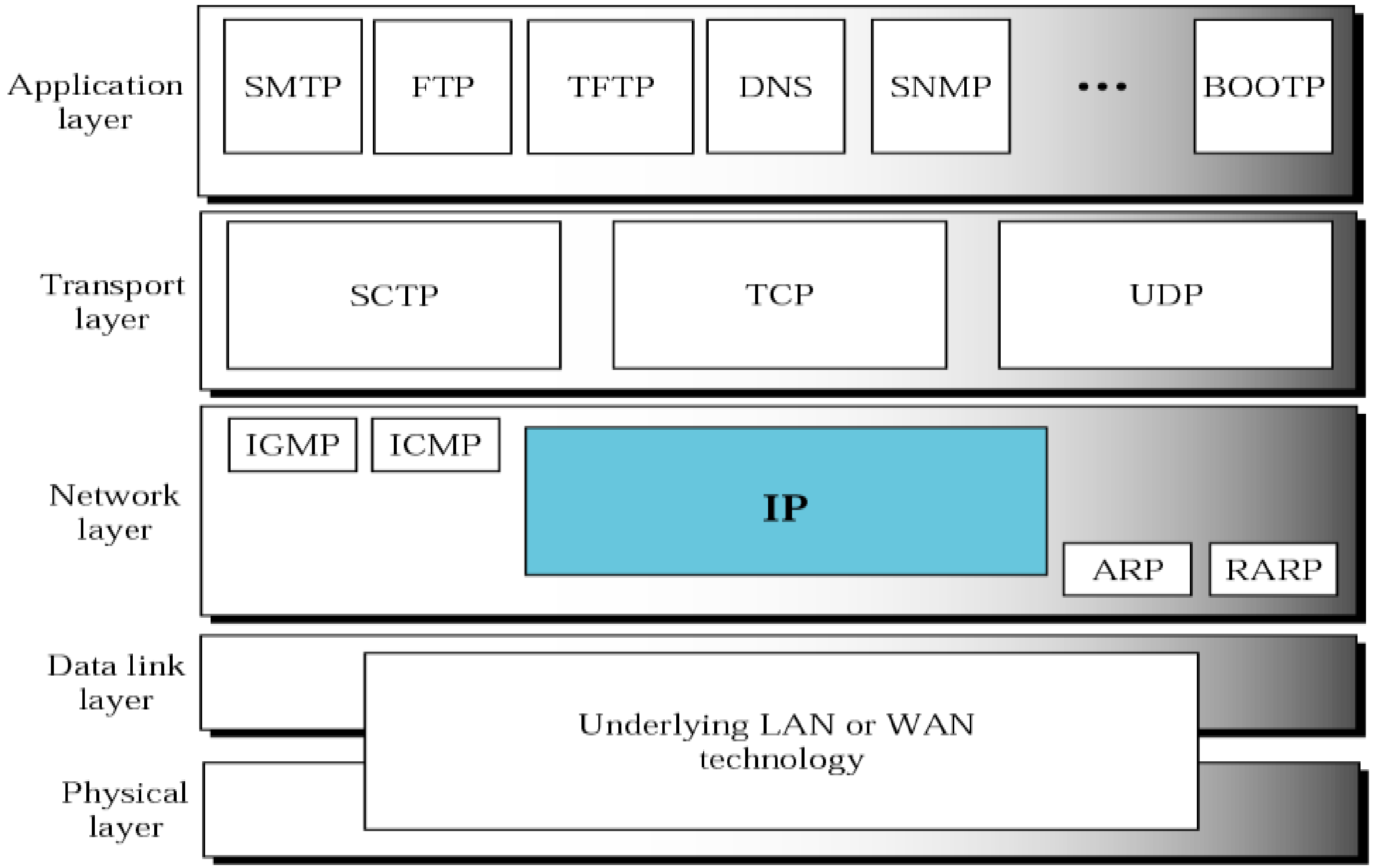
In CIDR notation, the block granted is defined by the first address and the prefix length.

Thank You

Unit No: 4 Unit name: Network Layer

Lecture No: 23
IPV6

Position of IP in TCP/IP protocol suite

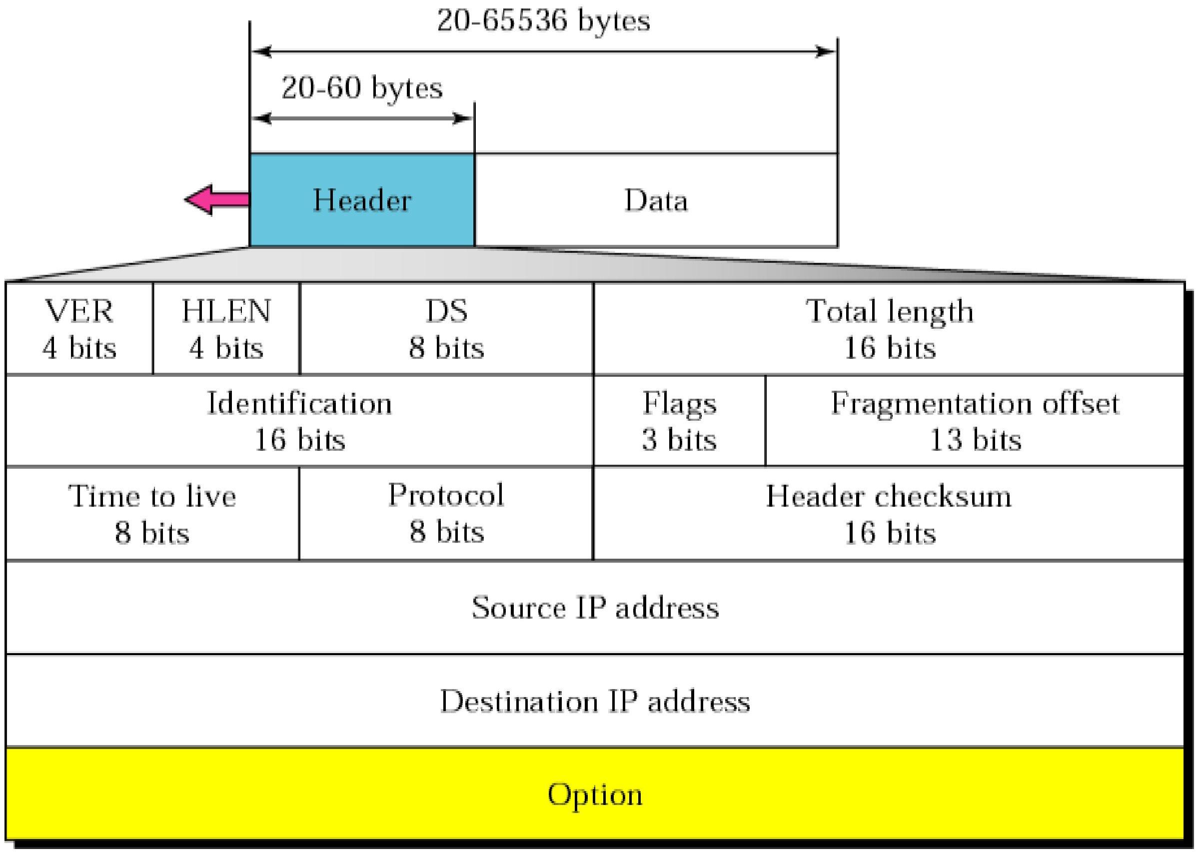


D Y PATIL DEEMED TO BE UNIVERSITY RAMRAO ADIK INSTITUTE OF TECHNOLOGY NAVI MUMBAI

IP (Internet Protocol)

A packet in the IP layer is called a datagram, a variable-length packet consisting of two parts: header and data. The header is 20 to 60 bytes in length and contains information essential to routing and delivery.

IP



20-65536 bytes
20-60 bytes
Header
Data
VER 4 bits
HLEN 4 bits
DS 8 bits
Total length 16 bits
Identification 16 bits
Flags 3 bits
Fragmentation offset 13 bits
Time to live 8 bits
Protocol 8 bits
Header checksum 16 bits
Source IP address
Destination IP address
Option

- **Question:** In which order are the bytes of an IP datagram transmitted?
- **Answer:**
    - Transmission is row by row
    - For each row:
        1. First transmit bits 0-7
        2. Then transmit bits 8-15
        3. Then transmit bits 16-23
        4. Then transmit bits 24-31
- This is called **network byte** order or **big endian** byte ordering.

Fields of the IP Header

- **Version (4 bits)**: current most widely used version is 4, IPv6 till not in wide use.
- **Header length (4 bits)**: length of IP header, in multiples of 4 bytes
- **DS field (1 byte)**
  - This field was previously called as Type-of-Service (TOS) field. The role of this field has been re-defined, but is "backwards compatible" to TOS interpretation
  - Differentiated Service (DS) (6 bits):
    - Used to specify service level (currently not supported in the Internet)

Fields of the IP Header

- **Identification (16 bits):** Unique identification number for each datagram set at host end.

- **Flags (3 bits):**
  - First bit always set to 0
  - DF bit (Do not fragment)
  - MF bit (More fragments)

  Will be explained later→ Fragmentation

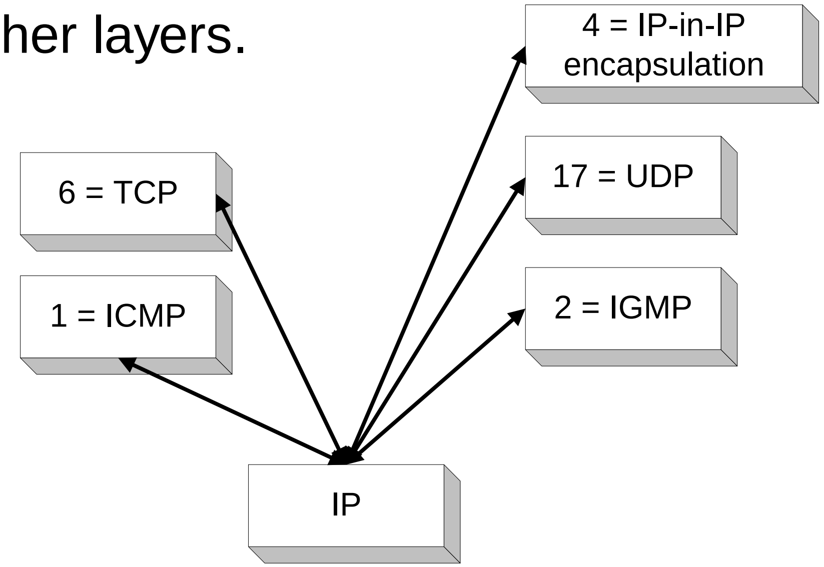
Fields of the IP Header

- **Time To Live (TTL) (1 byte):**
  - Specifies longest paths before datagram is dropped
  - Role of TTL field: Ensure that packet is eventually dropped when a routing loop occurs

  Used as follows:
  - Sender sets the value (e.g., 64)
  - Each router decrements the value by 1
  - When the value reaches 0, the datagram is dropped

Fields of the IP Header

- **Protocol (1 byte):**
  - Specifies the higher-layer protocol.
  - Used for de-multiplexing to higher layers.



- **Header checksum (2 bytes):** The IP checksum is a 16 bit 1's complement sum of all the 16 bit words in the IP header.

Fields of the IP Header

- **Options:**
    - Security restrictions
    - Record Route: each router that processes the packet adds its IP address to the header.
    - Timestamp: each router that processes the packet adds its IP address and time to the header.
    - (loose) Source Routing: specifies a list of routers that must be traversed.
    - (strict) Source Routing: specifies a list of the only routers that can be traversed.
- **Padding:** Padding bytes are added to ensure that header ends on a 4-byte boundary

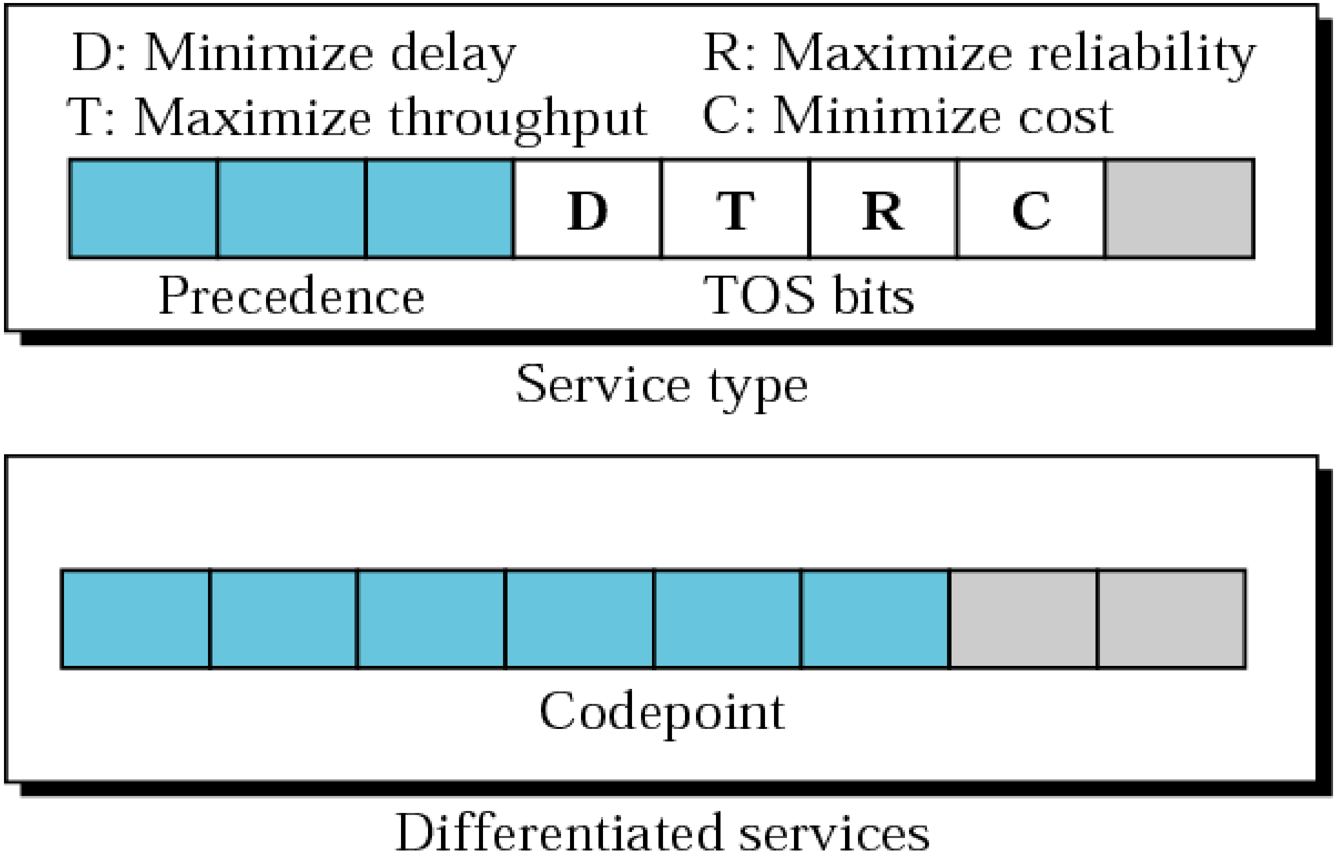
Maximum Transmission Unit

- Maximum size of IP datagram is 65535, but the data link layer protocol generally imposes a limit that is much smaller
- For example:
  - Ethernet frames have a maximum payload of 1500 bytes→
    IP datagrams encapsulated in Ethernet frame cannot be longer than 1500 bytes
- The limit on the maximum IP datagram size, imposed by the data link protocol is called **maximum transmission unit (MTU)**

- MTUs for various data link layers:

Ethernet:	1500	FDDI:	4352
802.3:	1492	ATM AAL5:	9180
802.5:	4464	PPP:	296

Differentiated Services



Types of Services

TOS Bits	*Description*
0000	Normal (default)
0001	Minimize cost
0010	Maximize reliability
0100	Maximize throughput
1000	Minimize delay

Default Types of Services

Protocol	*TOS Bits*	*Description*
ICMP	0000	Normal
BOOTP	0000	Normal
NNTP	0001	Minimize cost
IGP	0010	Maximize reliability
SNMP	0010	Maximize reliability
TELNET	1000	Minimize delay
FTP (data)	0100	Maximize throughput
FTP (control)	1000	Minimize delay
TFTP	1000	Minimize delay
SMTP (command)	1000	Minimize delay
SMTP (data)	0100	Maximize throughput
DNS (UDP query)	1000	Minimize delay
DNS (TCP query)	0000	Normal
DNS (zone)	0100	Maximize throughput

What's involved in Fragmentation?

- The following fields in the IP header are involved:

version	header length	DS	ECN	total length (in bytes)			
Identification				0	DF	MF	Fragment offset
time-to-live (TTL)		protocol		header checksum			

Identification When a datagram is fragmented, the identification is the same in all fragments

Flags

DF bit is set: Datagram cannot be fragmented and must be discarded if MTU is too small

MF bit set: This datagram is part of a fragment and an additional fragment follows this one

D Y PATIL DEEMED TO BE UNIVERSITY RAMRAO ADIK INSTITUTE OF TECHNOLOGY NAVI MUMBAI

What's involved in Fragmentation?

- The following fields in the IP header are involved:

version	header length	DS	ECN	total length (in bytes)			
Identification				0	DF	MF	Fragment offset
time-to-live (TTL)		protocol		header checksum			

Fragment offset Offset of the payload of the current fragment in the original datagram

Total length Total length of the current fragment

Note:

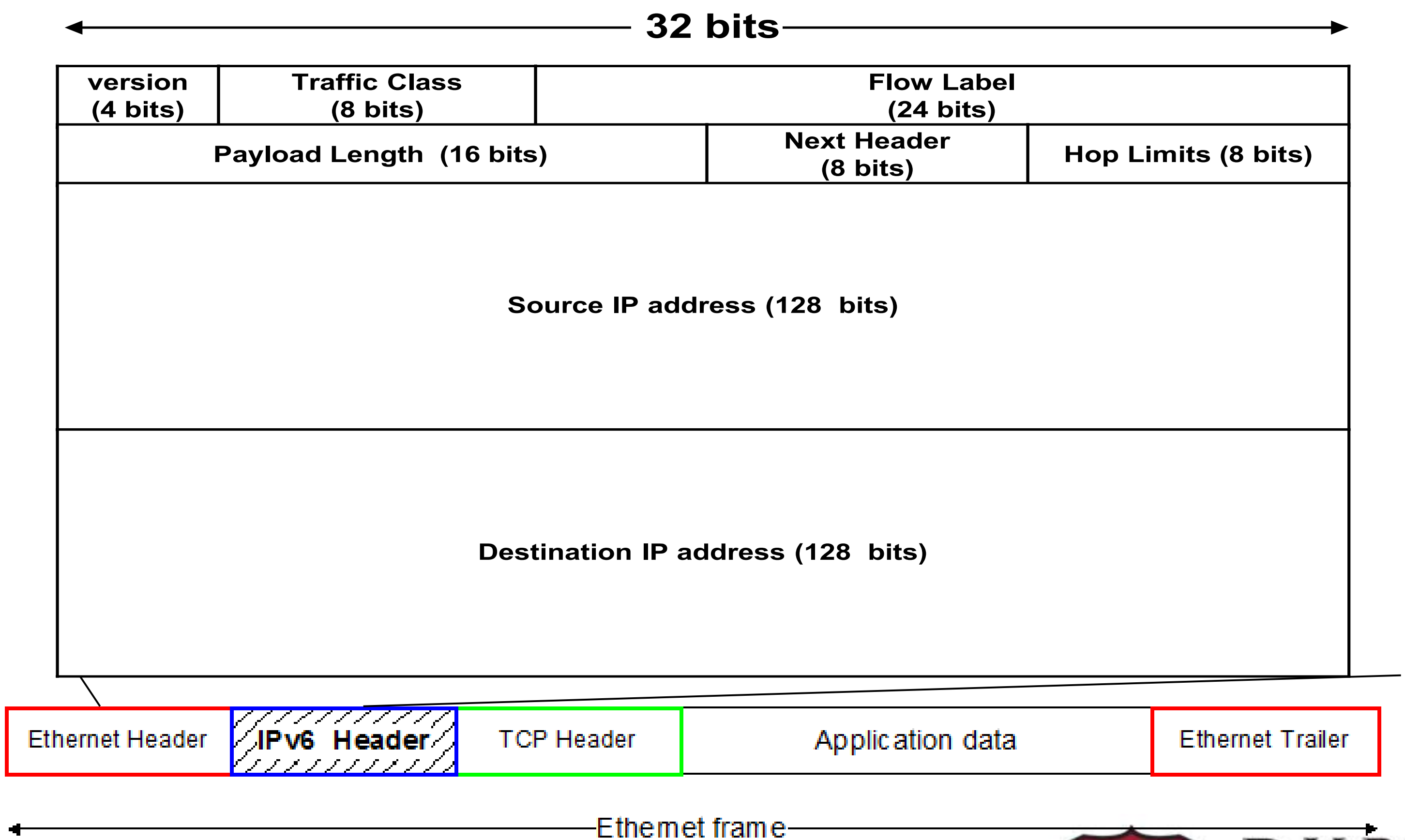
The ***total length*** *field defines the total length of the datagram including the header.*

IPv6 - IP Version 6

- **IP Version 6**
  - – Is the successor to the currently used IPv4
  - – Specification completed in 1994
  - – Makes improvements to IPv4 (no revolutionary changes)

- One (not the only !) feature of IPv6 is a significant increase in size of the IP address to **128 bits (16 bytes)**
  - IPv6 will solve – for the foreseeable future – the problems with IP addressing

IPv6 Header


32 bits
version
(4 bits)
Traffic Class
(8 bits)
Flow Label
(24 bits)
Payload Length (16 bits)
Next Header
(8 bits)
Hop Limits (8 bits)
Source IP address (128 bits)
Destination IP address (128 bits)
Ethernet Header
IPv6 Header
TCP Header
Application data
Ethernet Trailer
Ethernet frame

IPv6 vs. IPv4: Address Comparison

- **IPv4** has a maximum of

  $2^{32} \approx$ 4 billion addresses

- **IPv6** has a maximum of

  $2^{128} = (2^{32})^4 \approx$ **4 billion x 4 billion x 4 billion x 4 billion addresses**

Notation of IPv6 addresses

- **Convention**: The 128-bit IPv6 address is written as **eight 16-bit integers** (using hexadecimal digits for each integer)

  CEDF:BP76:3245:4464:FACE:2E50:3025:DF12

- **Short notation:**
- Abbreviations of leading zeroes:

  CEDF:BP76:0000:0000:009E:0000:3025:DF12
  → CEDF:BP76:0:0:9E
  :0:3025:DF12
- “:0000:0000” can be written as “::”

  CEDF:BP76:0:0:FACE:0:3025:DF12 →
  CEDF:BP76::FACE:0:3025:DF1
  2
- IPv6 addresses derived from IPv4 addresses have 96 leading zero bits. Convention allows to use IPv4 notation for the last 32 bits.

  ::80:8F:89:90 → ::128.143.137.144

IPv6 Provider-Based Addresses

- The first IPv6 addresses will be allocated to a provider-based plan

010	Registry ID	Provider ID	Subscriber ID	Subnetwork ID	Interface ID

The following fields have a variable length (recommeded length in "() ")

- Provider: Id of Internet access provider *(16 bits)*
- Subscriber: Id of the organization at provider *(24 bits)*
- Subnetwork: Id of subnet within organization *(32 bits)*
- Interface: identifies an interface at a node *(48 bits)*

More on IPv6 Addresses

- The provider-based addresses have a similar flavor as CIDR addresses
- IPv6 provides address formats for:
  – Unicast – identifies a single interface
  – Multicast – identifies a group. Datagrams sent to a multicast address are sent to all members of the group
  – Anycast – identifies a group. Datagrams sent to an anycast address are sent to one of the members in the group.

Thank You

Unit No: 4 Unit name: Network Layer

Lecture No: 24
ICMP

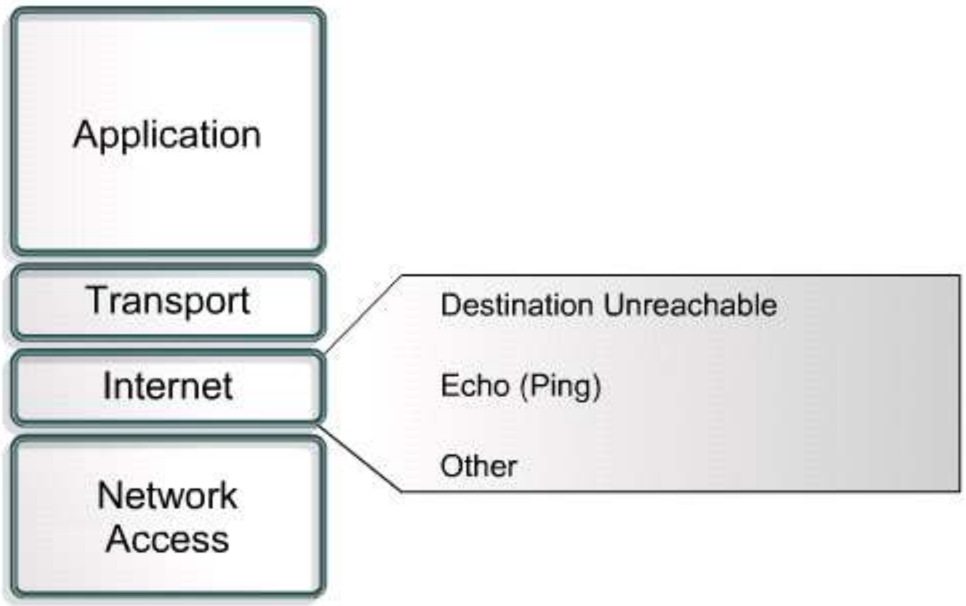
Internet Control Message Protocol (ICMP)

- IP is an unreliable method for delivery of network data.
- It has no built-in processes to ensure that data is delivered in the event that problems exist with network communication.
- If an intermediary device such as a router fails, or if a destination device is disconnected from the network, data cannot be delivered.
- Additionally, nothing in its basic design allows IP to notify the sender that a data transmission has failed.

Internet Control Message Protocol (ICMP)

- Internet Control Message Protocol (ICMP) is the component of the TCP/IP protocol stack that addresses this basic limitation of IP.
- ICMP does not overcome the unreliability issues in IP.
- Reliability must be provided by upper layer protocols if it is needed.

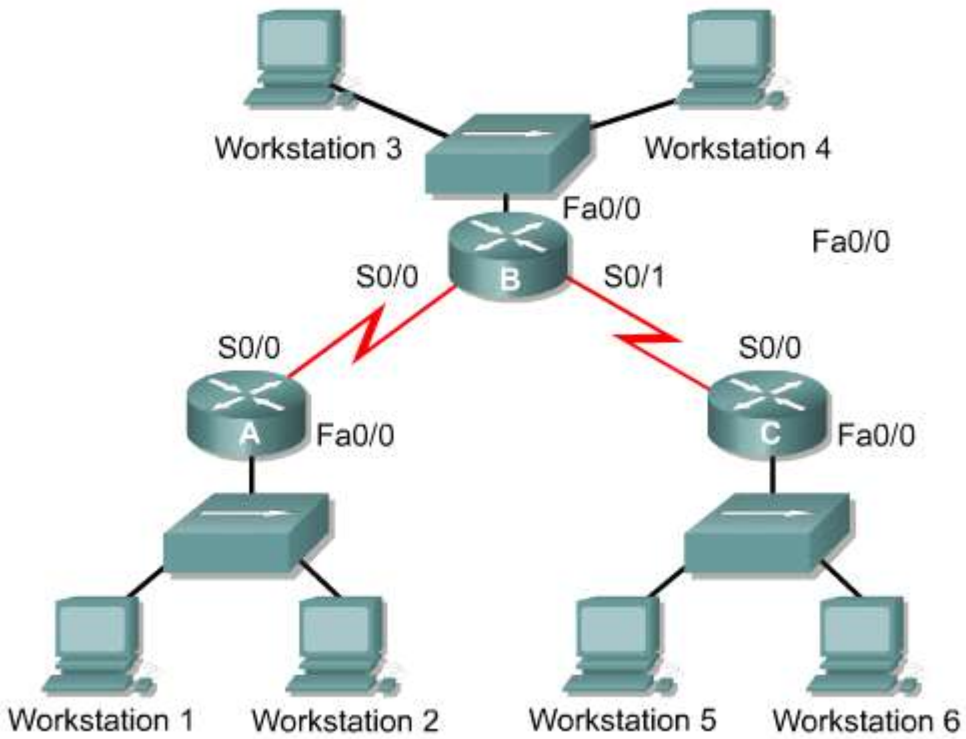
Internet Control Message Protocol (ICMP)



Error reporting and error correction

- ICMP is an error reporting protocol for IP.
- When datagram delivery errors occur, ICMP is used to report these errors back to the source of the datagram.
- ICMP does not correct the encountered network problem; it merely reports the problem.
- ICMP reports on the status of the delivered packet only to the source device.
- It does not propagate information about network changes to routers.

Error reporting and error correction



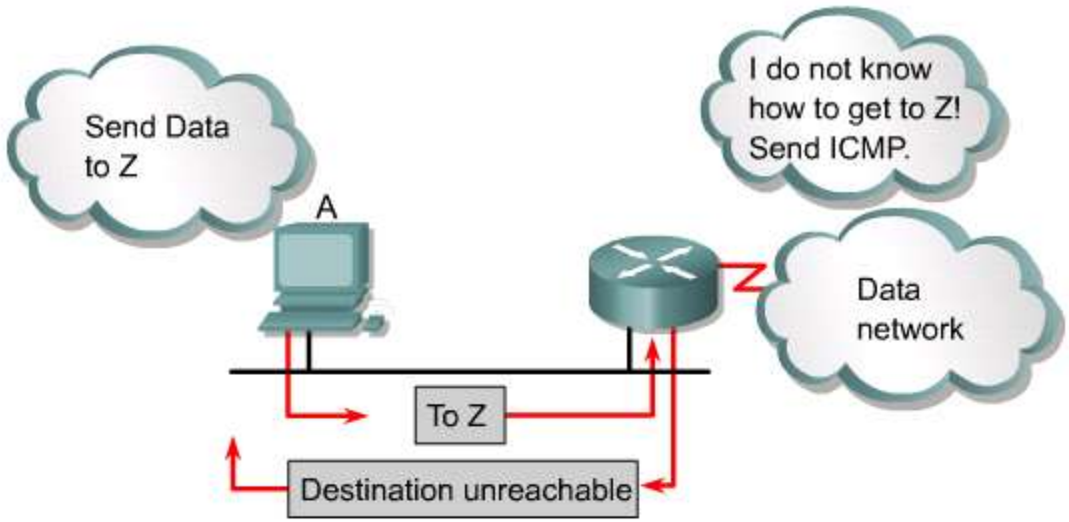
Unreachable networks

- Network communication depends upon certain basic conditions being met.
  - First, the sending and receiving devices must have the TCP/IP protocol stack properly configured.
  - Second, intermediary devices must be in place to route the datagram from the source device and its network to the destination network.

Unreachable networks

- For instance, the sending device may address the datagram to a non-existent IP address or to a destination device that is disconnected from its network.
- Routers can also be points of failure if a connecting interface is down or if the router does not have the information necessary to find the destination network.
- If a destination network is not accessible, it is said to be an unreachable network.

Unreachable networks



An ICMP destination unreachable meassage is sent if:

- Host or port unreachable
- Network unreachable

Introduction to control messages

- The Internet Control Message Protocol (ICMP) is an integral part of the TCP/IP protocol suite.
- Unlike error messages, control messages are not the results of lost packets or error conditions which occur during packet transmission.
- Instead, they are used to inform hosts of conditions such as network congestion or the existence of a better gateway to a remote network.

Internet Control Message Protocol (ICMP) : Control Messages

- Like all ICMP messages, ICMP control messages are encapsulated within an IP datagram.
- ICMP uses IP datagram in order to traverse multiple networks.
- Multiple types of control messages are used by ICMP.

Internet Control Message Protocol (ICMP) : Control Messages

ICMP Message Types	
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect/ Change Request
8	Echo Request
9	Router Advertisement
10	Router Selection
11	Time Exceeded
12	Parameter Problem
13	Timestamp Request
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply

ICMP redirect/change requests

- This type of message can only be initiated by a gateway.
- However, in some circumstances, a host connects to a segment that has two or more directly connected routers.
- In this case, the default gateway of the host may need to use a redirect/change request to inform the host of the best path to a certain network.

Congestion and flow control messages

- Dropped packets occur when there is too much congestion on a network.
- ICMP source-quench messages are used to reduce the amount of data lost.
- The source-quench message asks senders to reduce the rate at which they are transmitting packets.
- Most Cisco routers do not send source-quench messages by default, because the source-quench message may itself add to the network congestion.

D Y PATIL
DEEMED TO BE
UNIVERSITY
RAMRAO ADIK
INSTITUTE OF TECHNOLOGY
NAVI MUMBAI

Thank You