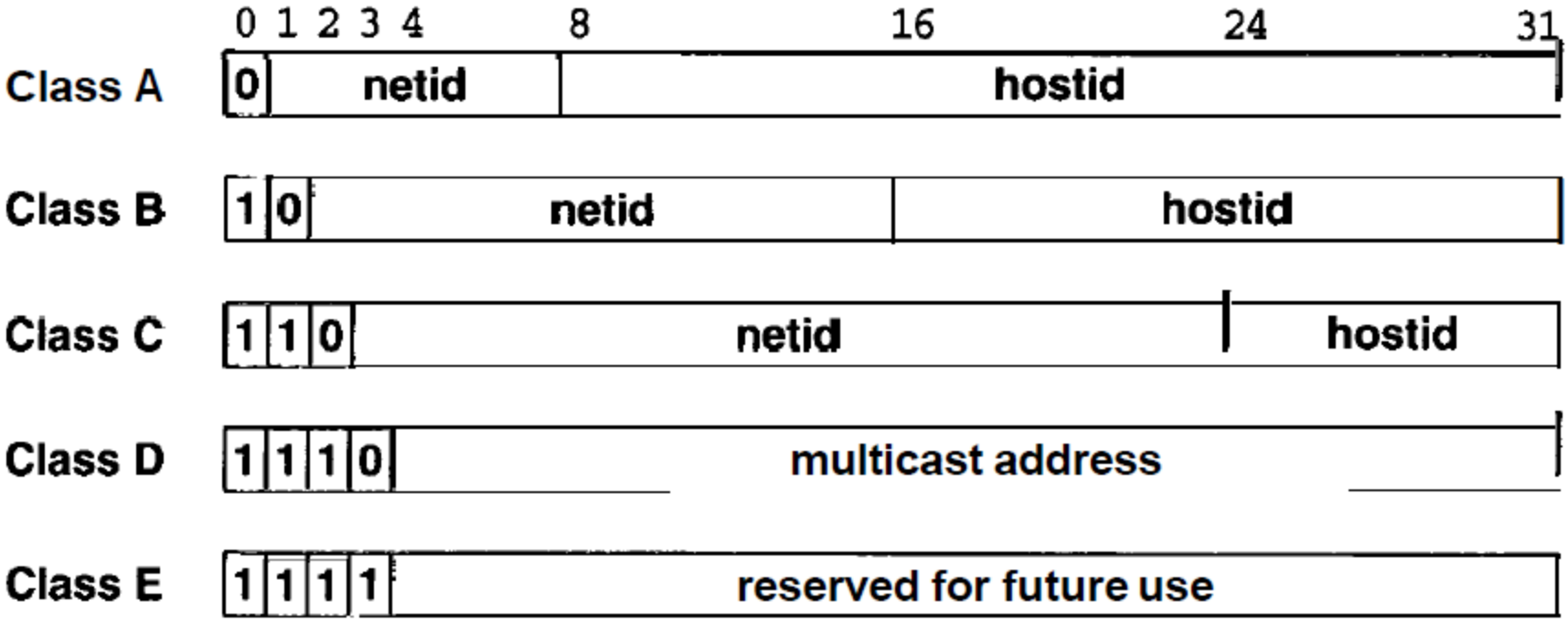
SRM
Institute of Science and Technology

21CSC302J-COMPUTER NETWORKS

Unit- II

Internet Protocol


0 1 2 3 4
8
16
24
31
Class A
0
netid
hostid
Class B
1 0
netid
hostid
Class C
1 1 0
netid
hostid
Class D
1 1 1 0
multicast address
Class E
1 1 1 1
reserved for future use

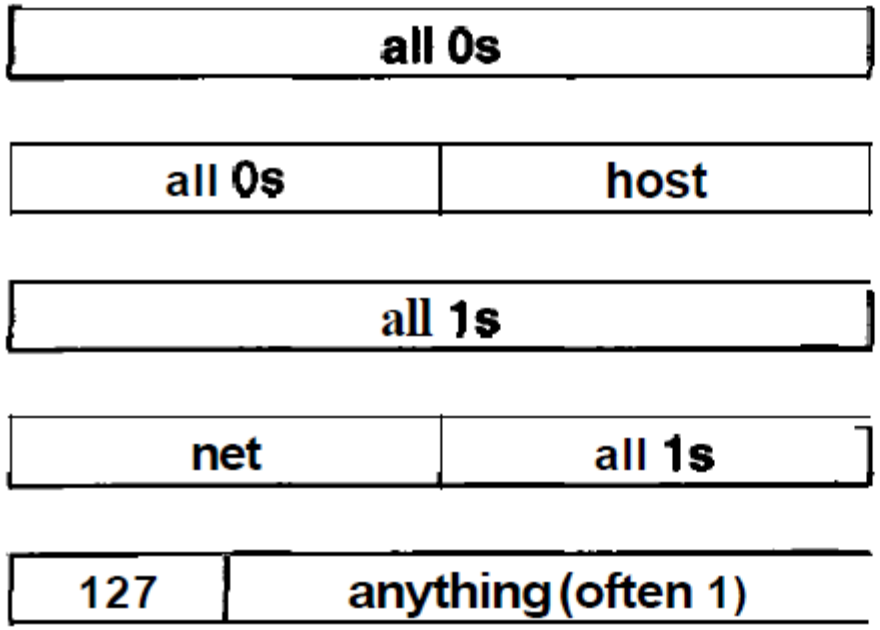
Because IP addresses encode both a network and a host on that network, they do not specify an individual computer, but a connection to a network.

Internet addresses can be used to refer to networks as well as individual hosts. By convention, an address that has all bits of the hostid equal to 0 is reserved to refer to the network.

In the 1980s as Local Area Network technologies became increasingly popular, it became apparent that requiring a unique prefix for each physical network would exhaust the address space quickly. Consequently, an addressing extension was developed to conserve network prefixes. Known as ***subnet addressing***, the scheme allows multiple physical networks to share a prefix

Class	Lowest Address	Highest Address
A	1.0.0.0	126.0.0.0
B	128.1.0.0	191.255.0.0
C	192.0.1.0	223.255.255.0
D	224.0.0.0	239.255.255.255
E	240.0.0.0	255.255.255.254

The range of dotted decimal values that correspond to each IP address class



Notes: [1] Allowed only at system startup and is never a valid destination address.
[2] Never a valid source address.
[3] Should never appear on a network.

Special forms of IP addresses

Class	Bits to Start	Size of Network ID Field	Size of Host ID Field	Number of Available Network Addresses	Number of Available Host Addresses per Network	Start Address	End Address
A	0	7	24	126	16,777,214	0.0.0.0	127.255.255.255
B	10	14	16	16,382	65,534	128.0.0.0	191.255.255.255
c	110	21	8	2,097,150	254	192.0.0.0	223.255.255.255
D	1110	N/A	N/A	N/A	N/A	224.0.0.0	239.255.255.255
E	1111	N/A	N/A	N/A	N/A	240.0.0.0	255.255.255.255

Comparison of IP addressing schemes

Class A Address

126 possible Class A network addresses and 16,777,216 possible local host addresses.

The first 8 bits contain the network address (always beginning with a zero). The remaining 24 bits contain the local host address.

The first octet of a Class A address is in the range 1 to 126.

Class B Address

a 16-bit network address and a 16-bit local or host address.

16,384 possible network addresses and 65,536 local host addresses.
The highest order bits are set to 1 and 0.

address is in the range 128 to 191.

Class C Address

24-bit network address and an 8-bit local host address.

2,097,152 possible network addresses and 256 possible local host addresses. The highest order bits are set to I-I-0.

address is in the range I92 to 223.

Class D Address

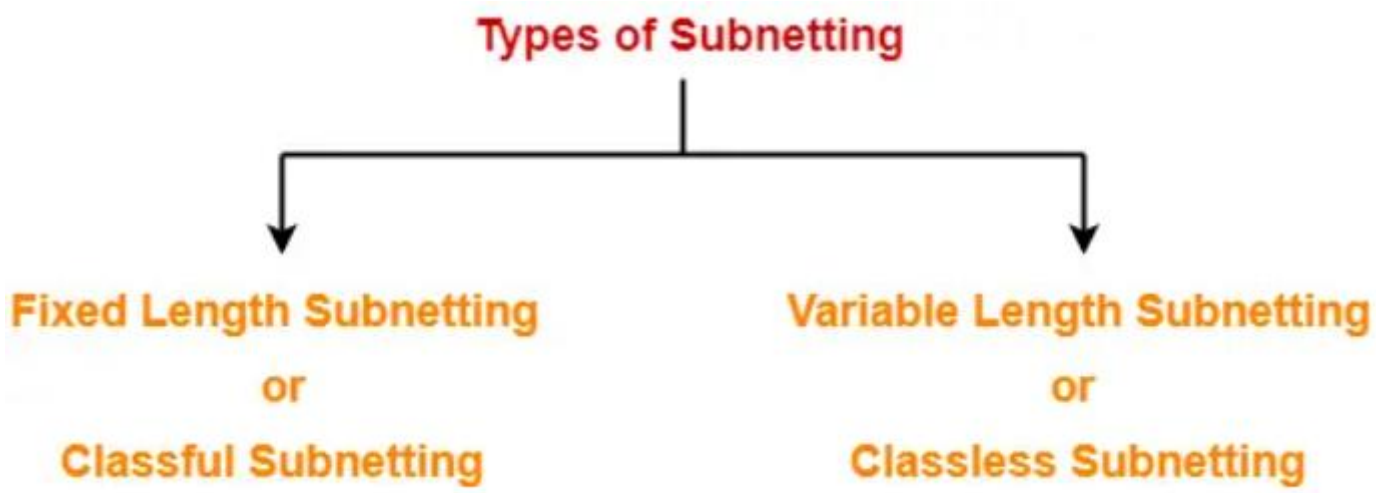
range of this class is from 224-239 and can't be allocated to hosts.

used for multicasting by various routing protocols.

224.0.0.5-Used by all OSPF routers, 224.0.0.6-Used by OSPF DRs (Designated Routers), 224.0.0.9-Used by RIP-2, 224.0.0.10-Used by EIGRP, 224.0.0.12-Used by DHCP Server/Relay Agent, 224.0.0.14-Used by RSVP encapsulation, 224.0.0.18-Used by VRRP, 224.0.0.22-Used by IGMP

Private Address

IPv4 Address Range
10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255


Types of Subnetting
Fixed Length Subnetting
or
Classful Subnetting
Variable Length Subnetting
or
Classless Subnetting

Fixed Length Subnetting

- Fixed length subnetting also called as classful subnetting divides the network into subnets where-

- ***All the subnets are of same size.***
- ***All the subnets have equal number of hosts.***
- ***All the subnets have same subnet mask.***

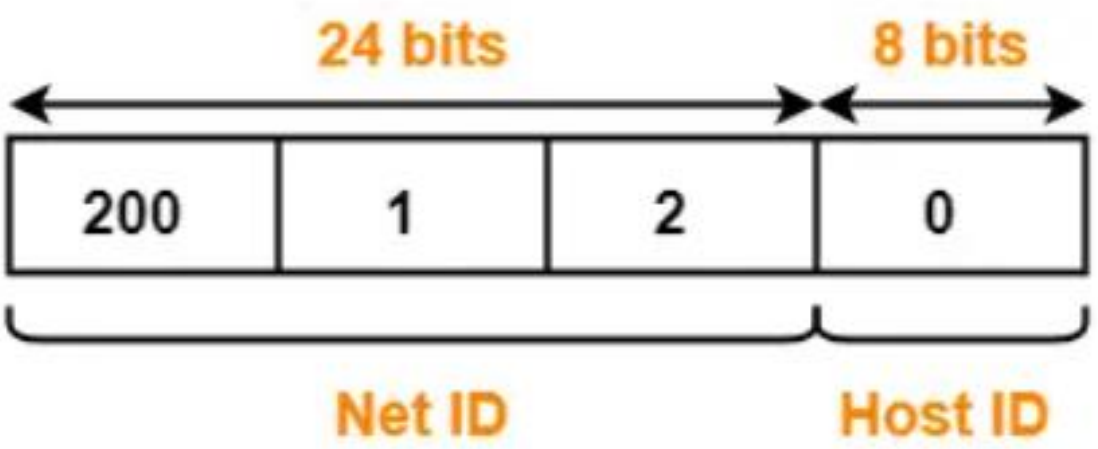
Variable Length Subnetting

- Variable length subnetting also called as classless subnetting divides the network into subnets where-

- ***All the subnets are not of same size.***
- ***All the subnets do not have equal number of hosts.***
- ***All the subnets do not have same subnet mask.***

Example-01

- Consider-
  - ***We have a big single network having IP Address 200.1.2.0.***
  - ***We want to do subnetting and divide this network into 2 subnets.***
  - ***Clearly, the given network belongs to class C.***

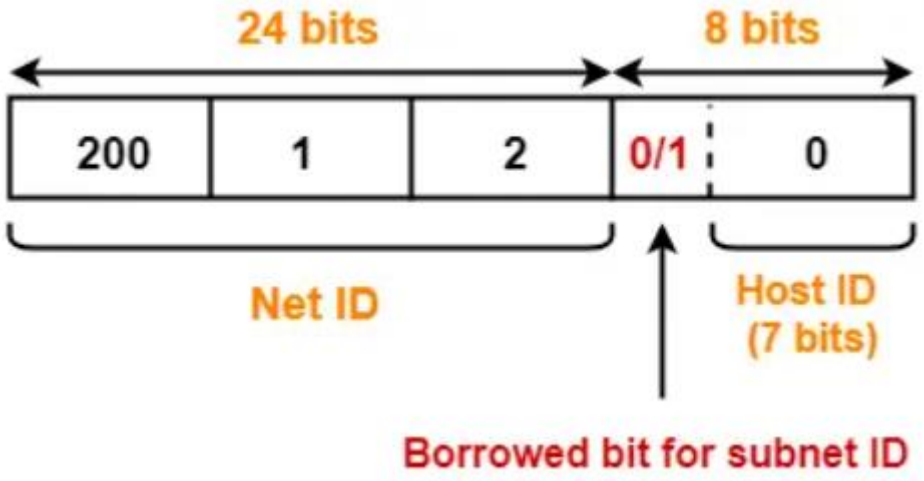


Example-01

- **For creating two subnets and to represent their subnet IDs, *we require 1 bit.***

- So,

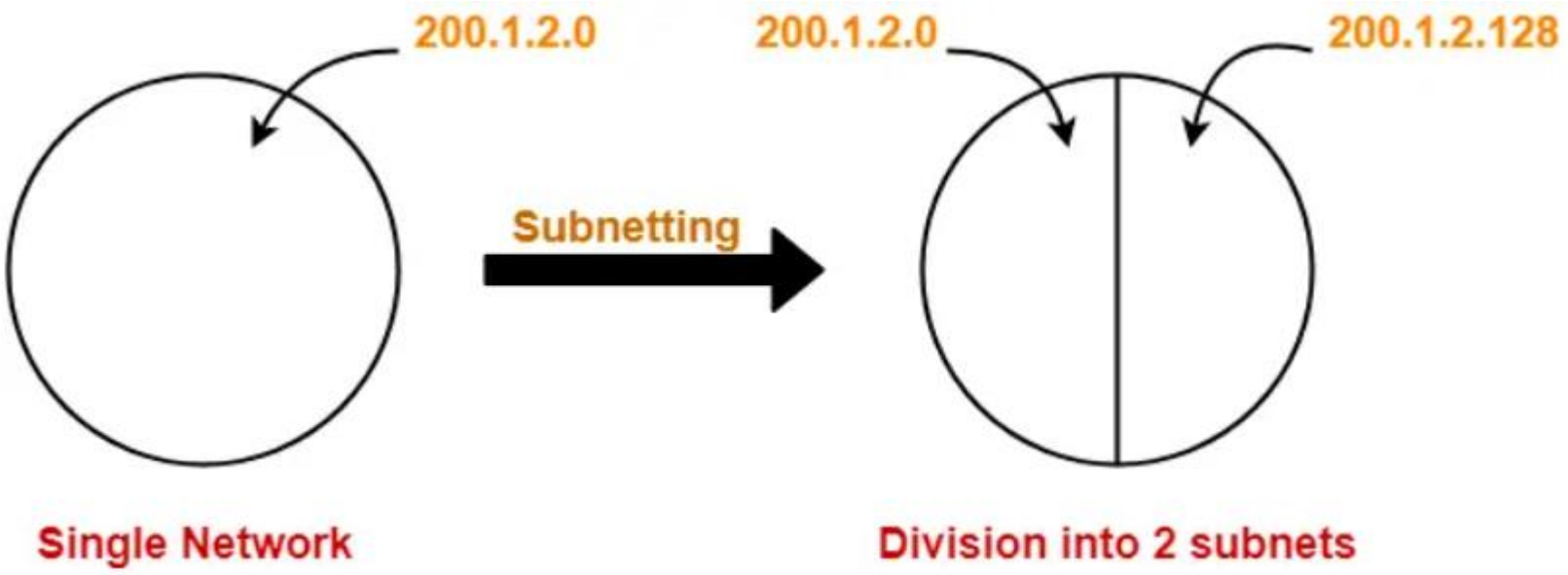
- **We borrow one bit from the Host ID part.**
- After borrowing one bit, **Host ID part remains with only 7 bits.**



Example-01

- IP Address of the two subnets are-

- ***200.1.2.00000000 = 200.1.2.0***
- ***200.1.2.10000000 = 200.1.2.128***



For 1st Subnet

- IP Address of the subnet = 200.1.2.0
- Total number of IP Addresses = 2^7 = 128
- Total number of hosts that can be configured = 128 – 2 = 126
- Range of IP Addresses = [200.1.2.00000000, 200.1.2.01111111] = [200.1.2.0, 200.1.2.127]
- Direct Broadcast Address = 200.1.2.01111111 = 200.1.2.127
- Limited Broadcast Address = 255.255.255.255

For 2nd Subnet

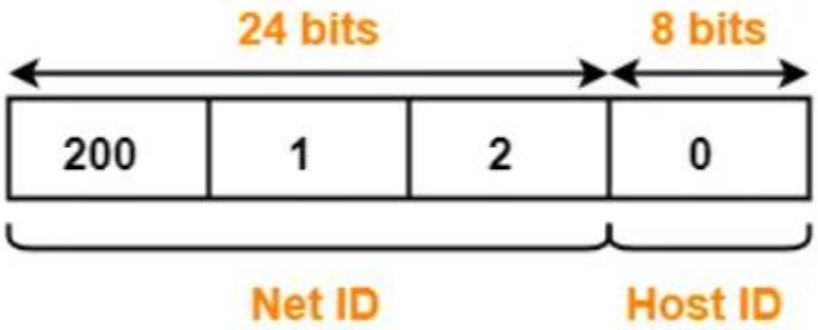
- IP Address of the subnet = 200.1.2.128
- Total number of IP Addresses = 2^7 = 128
- Total number of hosts that can be configured = 128 – 2 = 126
- Range of IP Addresses = [200.1.2.10000000, 200.1.2.11111111] = [200.1.2.128, 200.1.2.255]
- Direct Broadcast Address = 200.1.2.11111111 = 200.1.2.255
- Limited Broadcast Address = 255.255.255.255

Example-02

- Consider

- We have a big single network having IP Address 200.1.2.0.
- We want to do subnetting and divide this network into 4 subnets.

- Clearly, the given network belongs to class C.

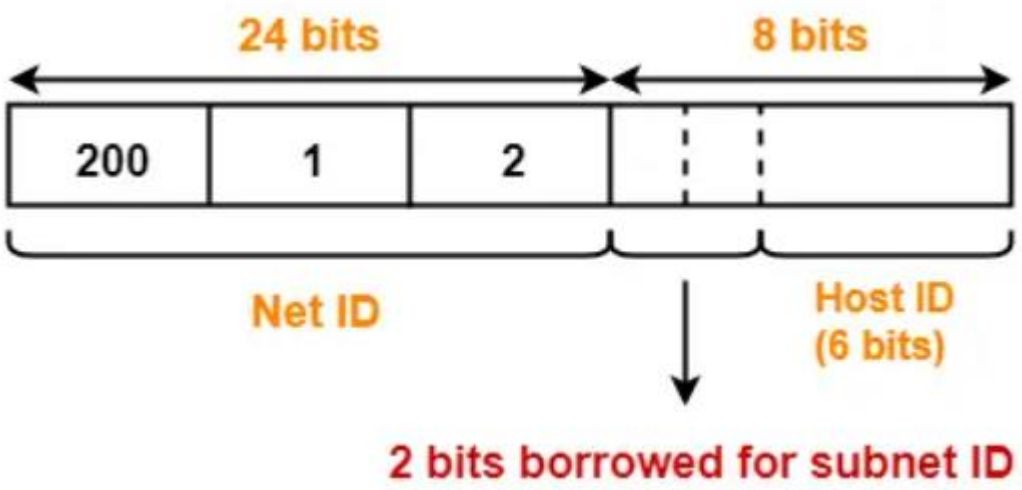


Example-02

- For creating four subnets and to represent their subnet IDs, we require 2 bits.

- So,

- We borrow two bits from the Host ID part.
- After borrowing two bits, Host ID part remains with only 6 bits.



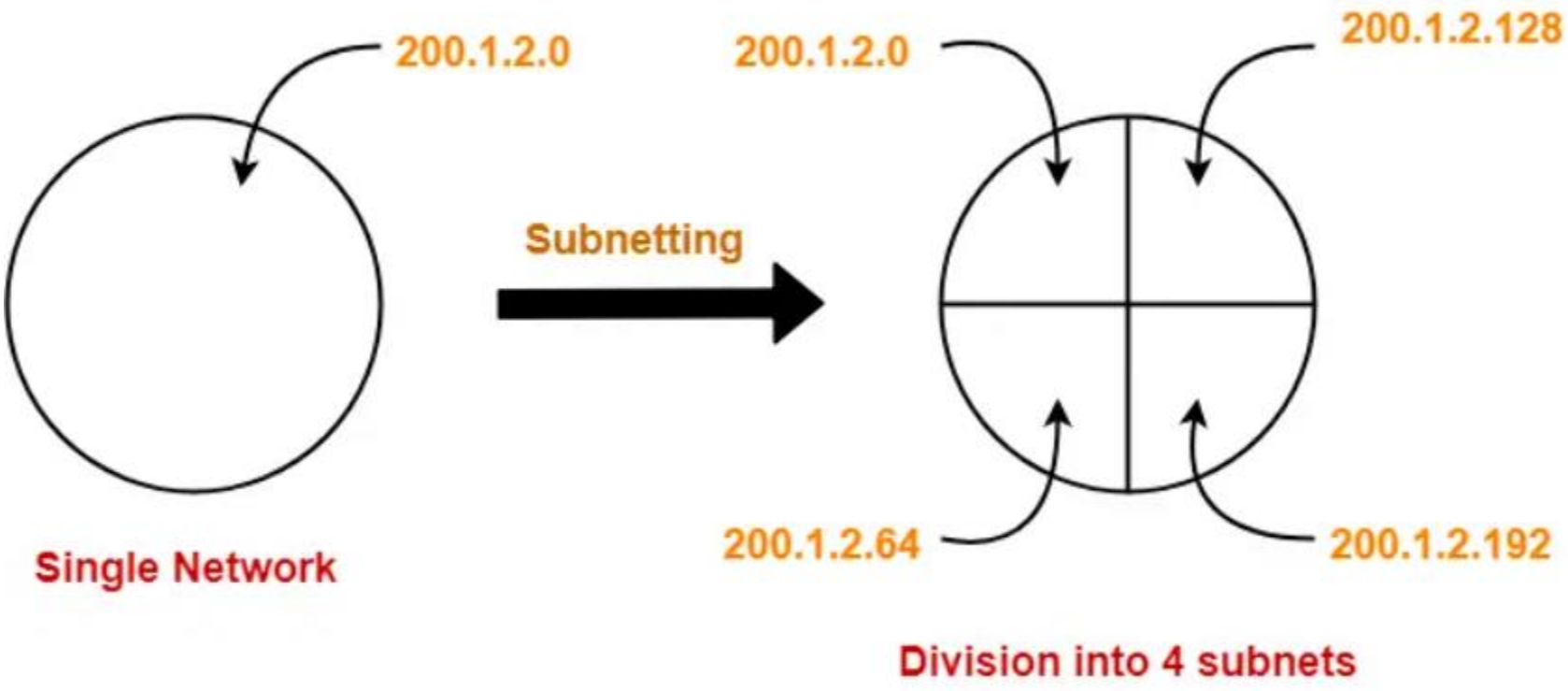
Example-02

- If borrowed bits = 00, then it represents the 1st subnet.
- If borrowed bits = 01, then it represents the 2nd subnet.
- If borrowed bits = 10, then it represents the 3rd subnet.
- If borrowed bits = 11, then it represents the 4th subnet.
-

- IP Address of the four subnets are-

- 200.1.2.00000000 = 200.1.2.0
- 200.1.2.01000000 = 200.1.2.64
- 200.1.2.10000000 = 200.1.2.128
- 200.1.2.11000000 = 200.1.2.192

Example-02


200.1.2.0
Single Network
Subnetting
200.1.2.0
200.1.2.128
200.1.2.64
200.1.2.192
Division into 4 subnets

For 1st Subnet

- IP Address of the subnet = 200.1.2.0
- Total number of IP Addresses = 26 = 64
- Total number of hosts that can be configured = 64 – 2 = 62
- Range of IP Addresses = [200.1.2.00000000, 200.1.2.00111111] = [200.1.2.0, 200.1.2.63]
- Direct Broadcast Address = 200.1.2.00111111 = 200.1.2.63
- Limited Broadcast Address = 255.255.255.255

For 2nd Subnet

- IP Address of the subnet = 200.1.2.64
- Total number of IP Addresses = 26 = 64
- Total number of hosts that can be configured = 64 – 2 = 62
- Range of IP Addresses = [200.1.2.01000000, 200.1.2.01111111] = [200.1.2.64, 200.1.2.127]
- Direct Broadcast Address = 200.1.2.01111111 = 200.1.2.127
- Limited Broadcast Address = 255.255.255.255

For 3rd Subnet

- IP Address of the subnet = 200.1.2.128
- Total number of IP Addresses = 26 = 64
- Total number of hosts that can be configured = 64 – 2 = 62
- Range of IP Addresses = [200.1.2.10000000, 200.1.2.10111111] = [200.1.2.128, 200.1.2.191]
- Direct Broadcast Address = 200.1.2.10111111 = 200.1.2.191
- Limited Broadcast Address = 255.255.255.255

For 4th Subnet

- IP Address of the subnet = 200.1.2.192
- Total number of IP Addresses = 26 = 64
- Total number of hosts that can be configured = 64 – 2 = 62
- Range of IP Addresses = [200.1.2.11000000, 200.1.2.11111111] = [200.1.2.192, 200.1.2.255]
- Direct Broadcast Address = 200.1.2.11111111 = 200.1.2.255
- Limited Broadcast Address = 255.255.255.255

Example-03

- Consider-

- We have a big single network having IP Address 200.1.2.0.
- We want to do subnetting and divide this network into 3 subnets.
-

- Here, the subnetting will be performed in two steps-

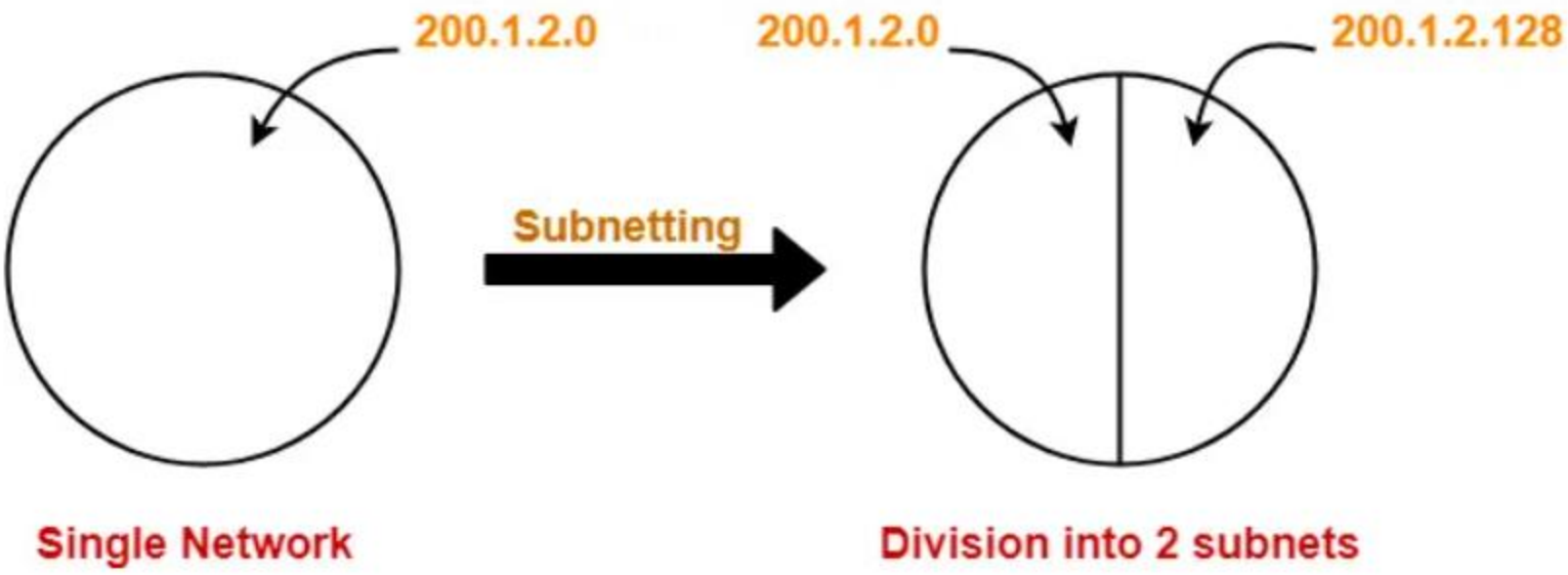
- Dividing the given network into 2 subnets
- Dividing one of the subnets further into 2 subnets

Example-03

- Step-01: Dividing Given Network into 2 Subnets-

- The subnetting will be performed exactly in the same way as performed in Example-01.

- After subnetting, we have



Example-03

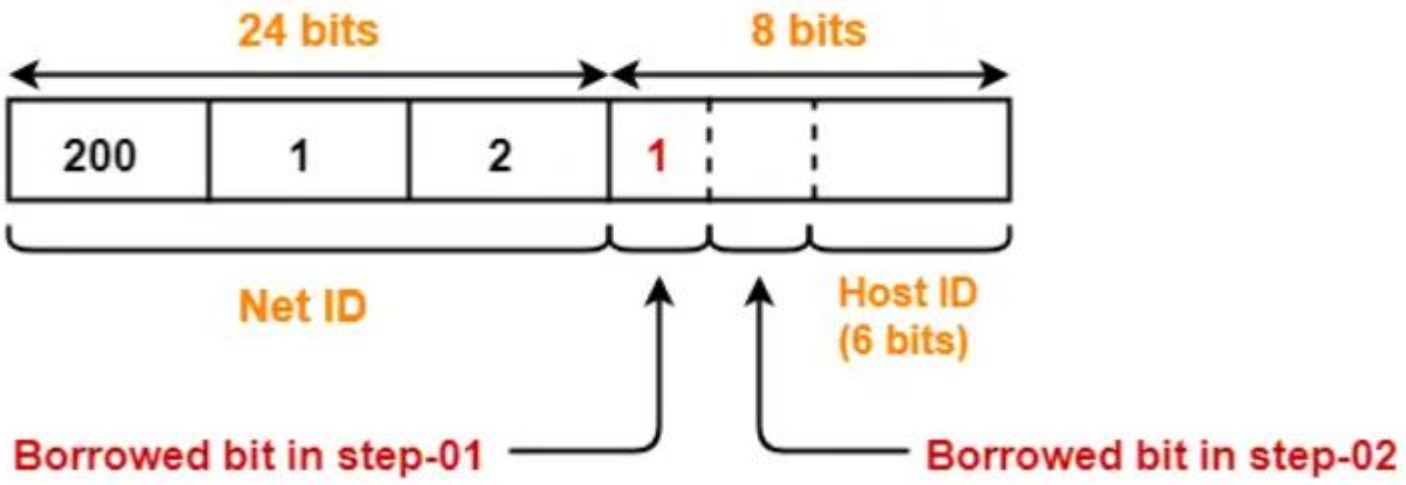
- Step-02: Dividing One Subnet into 2 Subnets-

- We perform the subnetting of one of the subnets further into 2 subnets.
- Consider we want to do subnetting of the 2nd subnet having IP Address 200.1.2.128.

- For creating two subnets and to represent their subnet IDs, we require 1 bit.

- So,
- We borrow one more bit from the Host ID part.
- After borrowing one bit, Host ID part remains with only 6 bits.

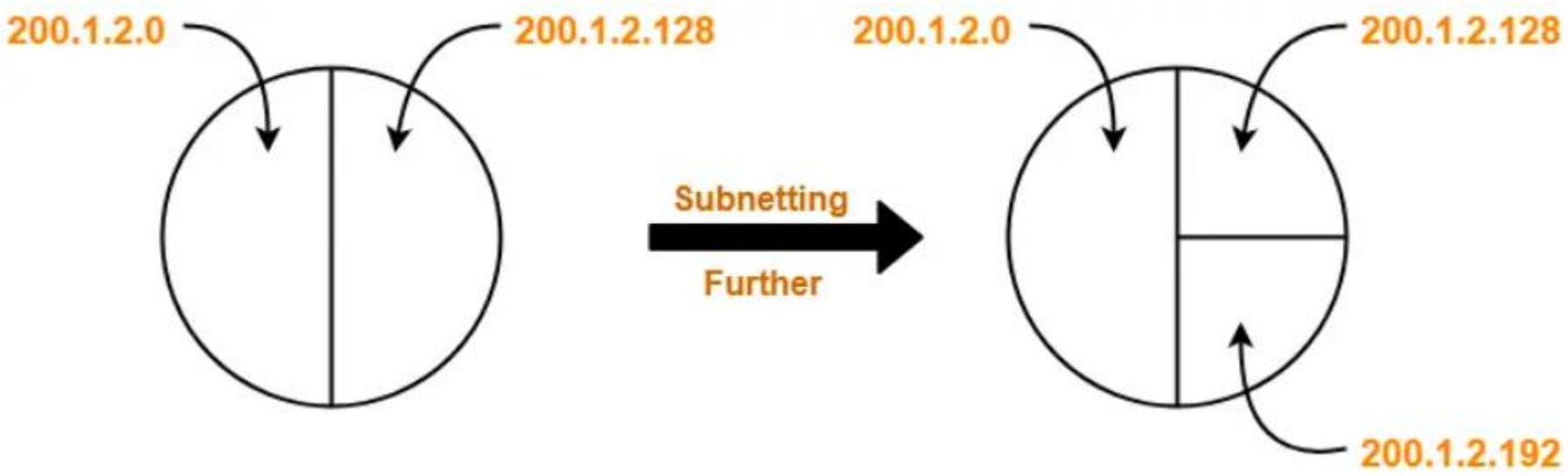
Example-03



- If 2nd borrowed bit = 0, then it represents one subnet.
- If 2nd borrowed bit = 1, then it represents the other subnet.

- IP Address of the two subnets are-
- 200.1.2.10000000 = 200.1.2.128
- 200.1.2.11000000 = 200.1.2.192

Example-03



- Finally, the given single network is divided into 3 subnets having IP Address-

- 200.1.2.0
- 200.1.2.128
- 200.1.2.192

Example-03

- Finally, the given single network is divided into 3 subnets having IP Address-

- 200.1.2.0
- 200.1.2.128
- 200.1.2.192

For 1st Subnet

- IP Address of the subnet = 200.1.2.0
- Total number of IP Addresses = 27 = 128
- Total number of hosts that can be configured = 128 – 2 = 126
- Range of IP Addresses = [200.1.2.00000000, 200.1.2.01111111] = [200.1.2.0, 200.1.2.127]
- Direct Broadcast Address = 200.1.2.01111111 = 200.1.2.127
- Limited Broadcast Address = 255.255.255.255

For 2nd Subnet

- IP Address of the subnet = 200.1.2.128
- Total number of IP Addresses = 26 = 64
- Total number of hosts that can be configured = 64 – 2 = 62
- Range of IP Addresses = [200.1.2.10000000, 200.1.2.10111111] = [200.1.2.128, 200.1.2.191]
- Direct Broadcast Address = 200.1.2.10111111 = 200.1.2.191
- Limited Broadcast Address = 255.255.255.255

For 3rd Subnet

- IP Address of the subnet = 200.1.2.192
- Total number of IP Addresses = 26 = 64
- Total number of hosts that can be configured = 64 – 2 = 62
- Range of IP Addresses = [200.1.2.11000000, 200.1.2.11111111] = [200.1.2.192, 200.1.2.255]
- Direct Broadcast Address = 200.1.2.11111111 = 200.1.2.255
- Limited Broadcast Address = 255.255.255.255

Exercise 04

- You have been allocated a class A network address of 29.0.0.0. You need to create at least 20 networks and each network will support a maximum of 160 hosts.

- Would the following two subnet masks work?
- 255.255.0.0 and 255.255.255.0

Default mask is 255.0.0.0

- Mask 255.255.0.0 has 8 bits for the subnet and 16 bits for the host
- 8 bits would accommodate 256 subnets
- 16 bits would accommodate over 64000 hosts
- Mask 255.255.255.0 has 16 bits for the subnet and 8 bits of the host
- Have possible 254 hosts whish is enough

Exercise 05

- You have been allocated a class B network address 135.1.0.0 and need to create 4 subnets each with around 200 hosts. What is the easiest mask to use to satisfy the criteria?

Default mask is 255.255.0.0

- Easiest is to sub net on a byte boundary which would mean a subnet mask of 255.255.255.0
- This would allocate 8 bits for the subnet and 8 bits for the host.
- We need to accommodate around 200 hosts which requires 8 bits which we have.
- We need 4 subnets which require 4 bits and we have 8 bits. So we have more than enough.

Exercise 05

- Write the IP address 222.1.1.20 mask 255.255.255.192 in CIDR notation.

Decimal 192 = 11000000 binary which means that 2 bits of this octet are used for the subnet.

Now add 24 bits 255.255.255 and we have 26 bits.

So we write

222.1.1.20/26

Exercise 06

- Subnet the class C IP Address 195.1.1.0. So that you have 10 subnets each with a maximum 12 hosts.

Current mask: 255.255.255.0

Bits needs for 10 subnets = 4 = 2^4 = 16
Bits need to 12 hosts = 4 = 2 ^ 4 = 16 – 2
So our mask in binary = 11110000 = 240 decimal

Final mask address is 255.255.255.240

Exercise 07

- Subnet the class C IP Address 205.11.2.0. So that you have 30 subnets. What is the subnet mask for the maximum of host.

- How many host can have in each subnet? What is the IP address of host 3 on subnet 2?

Current mask: 255.255.255.0

Bits needed for 30 subnets = 5 = 32 possible subnets
Bits left for hosts = 3 = 8 – 2 = 6 possible hosts.

So our mask in binary = 11111000 = 248
Final mask is 255.255.255.248

Exercise 07

Address of host 3 on subnet 2 is

Subnet 2 = 0001 0000 host 3 = 0000 0011

Add the two together = 0001 0011 = 19

Therefore IP address of host 3 on subnet 2 = 205.11.2.19

Exercise 08

- Subnet the class C IP Address 195.1.1.0. So that you have at least 2 subnets each subnet must have room for 48 hosts.

- What are the two possible subnet masks?

Current mask: 255.255.255.0

Bits needed for 48 hosts = 6 = 2 ^ 6 = 62 possible hosts
Bits needed for 2 subnets = 1 = 2 ^ 1= 2 possible subnets.

Total of 7 bits needed so therefore we can use either 1 bit or 2 bits for the subnet.

SRM INSTITUTE OF SCIENCE & TECHNOLOGY
Deemed to be University u/s 3 of UGC Act, 1956

Exercise 08

So we could have

1 bit for subnet 7 bits hosts or 2 bits subnet 6 bits host.

Masks are 1000 0000 and 1100 0000 = 128 decimal and 192 decimal

Final possible masks are:

255.255.255.128 and 255.255.255.192

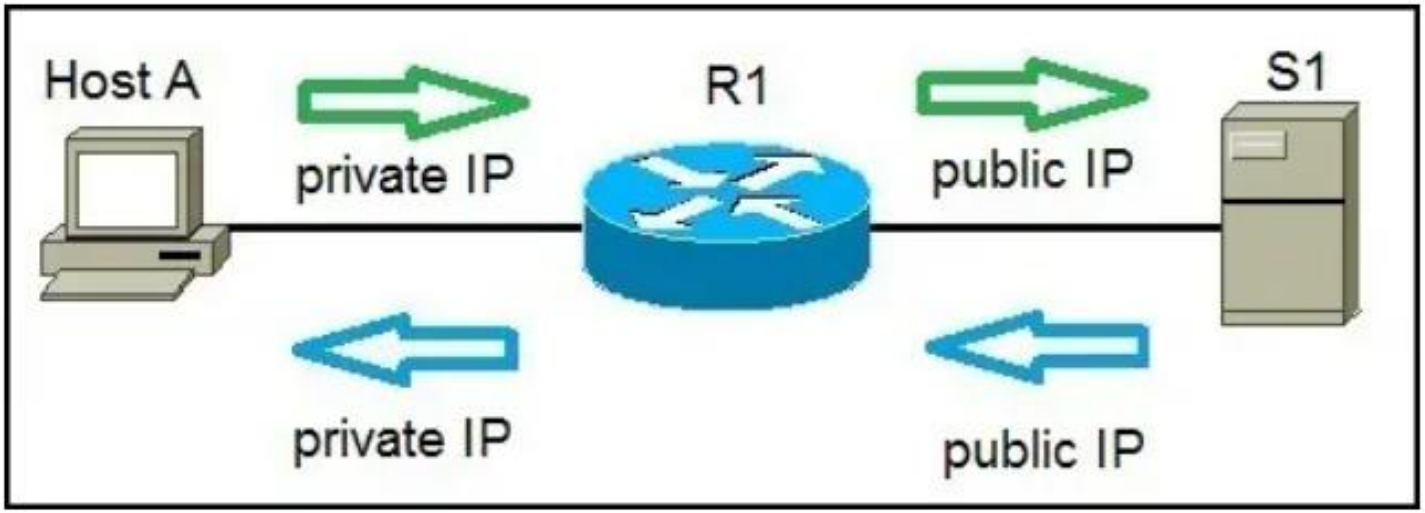
Network Address Translation

NAT

- **A process of *changing the source and destination IP addresses and ports.***

- Address translation
  - ***reduces the need for IPv4 public addresses and***
  - ***hides private network address ranges***.

- This process is usually done by routers or firewalls.



Network Address Translation

- **To access the Internet,**
  - ***one public IP address is needed,***
  - ***use a private IP address in our private network.***

- **The idea of NAT is *to allow multiple devices to access the Internet through a single public address.***

- To achieve this, the translation of a private IP address to a public IP address is required.

- **A process in which *one or more local IP address is translated into one or more Global IP address and vice versa* *in order to provide Internet access to the local hosts.***

- Also, it does the translation of port numbers
  - ***i.e. masks the port number of the host with another port number, in the packet that will be routed to the destination.***

- It ***makes the corresponding entries of IP address and port number in the NAT table.***

- There are three types of address translation:

- **Static NAT**
  - ***Translates one private IP address to a public one. The public IP address is always the same.***

- **Dynamic NAT**
  - ***Private IP addresses are mapped to the pool of public IP addresses.***

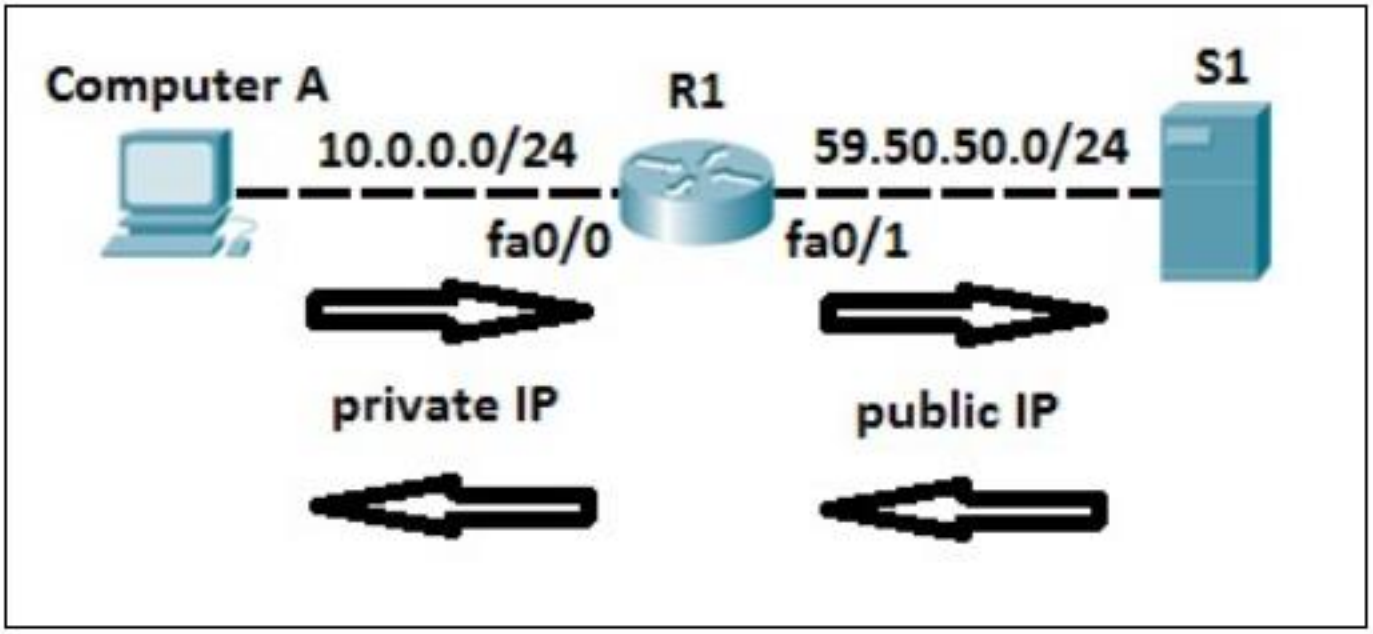
- **Port Address Translation (PAT)**
  - ***One public IP address is used for all internal devices, but a different port is assigned to each private IP address. Also known as NAT Overload.***

Static NAT

- **With static NAT, routers or firewalls *translate one private IP address to a single public IP address.***
- **Each private IP address is mapped *to a single public IP address.***
- Static NAT is not often used because it requires one public IP address for each private IP address.
- To configure static NAT, three steps are required:
  - ***configure private/public IP address mapping by using the "ip nat inside source static PRIVATE_IP PUBLIC_IP" command***
  - ***configure the router's inside interface using the "ip nat inside" command***

Static NAT

- To configure static NAT, three steps are required:
  - ***configure the router's outside interface using the "ip nat outside" command***



```
R1(config)#ip nat inside source static 10.0.0.2 59.50.50.1
R1(config)#interface fastEthernet 0/0
R1(config-if)#ip nat inside
R1(config-if)#interface fastEthernet 0/1
R1(config-if)#ip nat outside
```

```
R1#show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 59.50.50.1:9 10.0.0.2:9 59.50.50.2:9 59.50.50.2:9
--- 59.50.50.1 10.0.0.2 --- ---
```

Dynamic NAT

- **Does the mapping of a local address to a global address *happens dynamically.***
- **The router dynamically picks an address *from the global address pool that is not currently assigned.***
- The dynamic entry stays in the ***NAT translations table*** as long as the traffic is exchanged.
- **The entry times out after *a period of inactivity*** and the global IP address can be used for new translations.

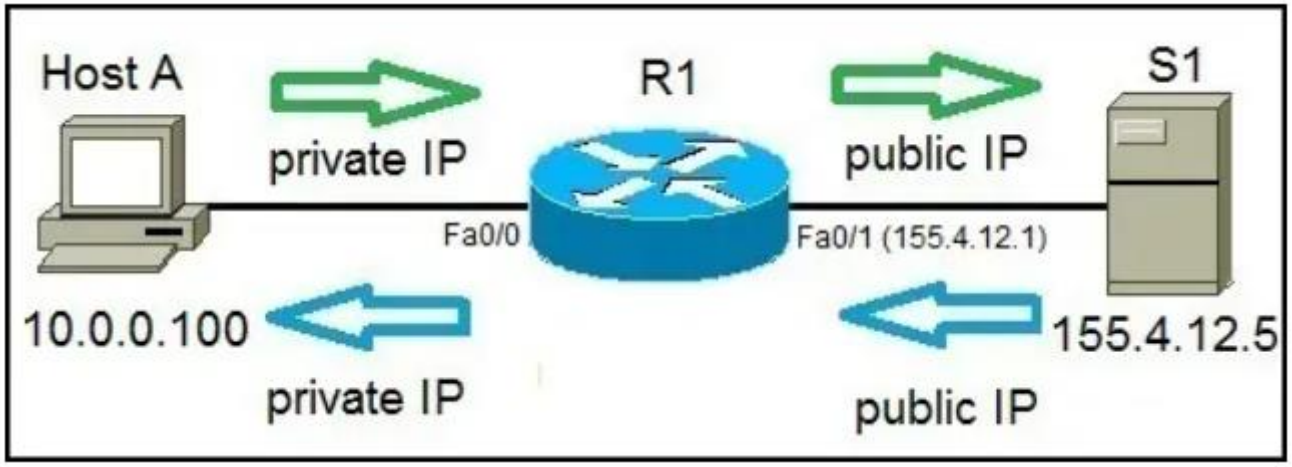
Dynamic NAT

- With dynamic NAT, you need to specify two sets of addresses on your Cisco router:
  - ***the inside addresses that will be translated***
  - ***a pool of global addresses***

- To configure dynamic NAT, the following steps are required:
  - ***configure the router's inside interface using the "ip nat inside" command***
  - ***configure the router's outside interface using the "ip nat outside" command***
  - ***configure an ACL that has a list of the inside source addresses that will be translated***

Dynamic NAT

- To configure dynamic NAT, the following steps are required:
  - ***configure a pool of global IP addresses using the "ip nat pool NAME FIRST_IP_ADDRESS LAST_IP_ADDRESS netmask SUBNET_MASK" command***
  - ***enable dynamic NAT with the "ip nat inside source list ACL_NUMBER pool NAME global configuration" command***



To configure dynamic NAT, the following commands are required on R1:

First we need to configure the router's inside and outside NAT interfaces:

```
R1(config)#int f0/0
R1(config-if)#ip nat inside
R1(config-if)#int f0/1
R1(config-if)#ip nat outside
```

Next, we need to configure an ACL that will include a list of the inside source addresses that will be translated. In this example we want to translate all inside hosts on the 10.0.0.0/24 network:

```
R1(config)#access-list 1 permit 10.0.0.0 0.0.0.255
```

To configure dynamic NAT, the following commands are required on R1:

We need to configure the pool of global (public) IP addresses available on the outside interface. The pool configured above consists of 3 addresses: 155.4.12.1, 155.4.12.2, and 155.4.12.3.

```
R1(config)#ip nat pool STUDY-CCNA_POOL 155.4.12.1 155.4.12.3 netmask 255.255.255.0
```

we need to enable dynamic NAT:

```
R1(config)#ip nat inside source list 1 pool STUDY-CCNA_POOL
```

The command above tells the router to translate all addresses specified in the access list 1 to the pool of global addresses named MY POOL.

You can list all NAT translations using the show ip nat translations command.

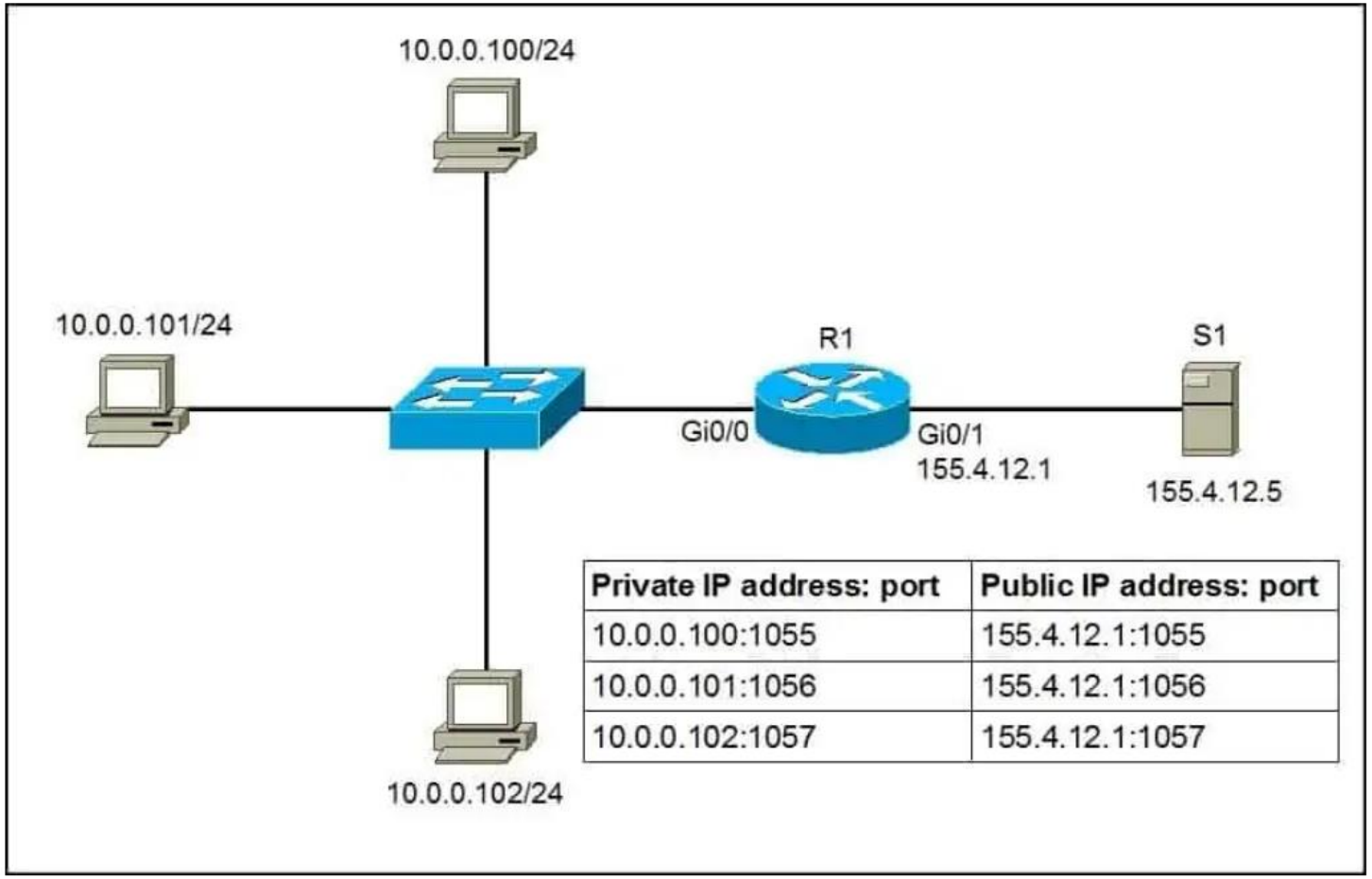
```
R1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 155.4.12.1:16     10.0.0.100:16      155.4.12.5:16      155.4.12.5:16
```

Port Address Translation (PAT)

- **A single public IP address is used for all internal private IP addresses, *but a different port is assigned to each private IP address.***
- ***Also known as NAT Overload*** and is the typical form of NAT used in today's networks.
- It is even supported by most consumer-grade routers.
- PAT ***allows you to support many hosts*** **with only few public IP addresses.**
- ***It works by creating dynamic NAT mapping***, in which **a global (public) IP address and a unique port number are selected.**

Port Address Translation (PAT)

- The router keeps a NAT table entry for every unique combination of the private IP address and port, with translation to the global address and a unique port number.



Private IP address: port	Public IP address: port
10.0.0.100:1055	155.4.12.1:1055
10.0.0.101:1056	155.4.12.1:1056
10.0.0.102:1057	155.4.12.1:1057

Port Address Translation (PAT)

- To configure PAT, the following commands are required:
  - ***configure the router's inside interface using the "ip nat inside" command.***
  - ***configure the router's outside interface using the "ip nat outside" command.***
  - ***configure an access list that includes a list of the inside source addresses that should be translated.***
  - ***enable PAT with the "ip nat inside source list ACL_NUMBER interface TYPE overload global configuration" command.***

Port Address Translation (PAT)

First, we will define the outside and inside interfaces on R1:

```
R1(config)#int Gi0/0
R1(config-if)#ip nat inside
R1(config-if)#int Gi0/1
R1(config-if)#ip nat outside
```

Next, we will define an access list that will include all private IP addresses we would like to translate:

```
R1(config-if)#access-list 1 permit 10.0.0.0 0.0.0.255
```

The access list defined above includes all IP addresses from the 10.0.0.0 – 10.0.0.255 range.

Port Address Translation (PAT)

we need to enable NAT and refer to the ACL created in the previous step and to the interface whose IP address will be used for translations:

```
R1(config)#ip nat inside source list 1 interface Gi0/1 overload
```

To verify the NAT translations, we can use the show ip nat translations command after hosts request a web resource from S1:

```
R1#show ip nat translations
Pro Inside global Inside local Outside local Outside global
tcp 155.4.12.1:1024 10.0.0.100:1025 155.4.12.5:80 155.4.12.5:80
tcp 155.4.12.1:1025 10.0.0.101:1025 155.4.12.5:80 155.4.12.5:80
tcp 155.4.12.1:1026 10.0.0.102:1025 155.4.12.5:80 155.4.12.5:80
```

Port Address Translation (PAT)

The same IP address (155.4.12.1) has been used to translate three private IP addresses (10.0.0.100, 10.0.0.101, and 10.0.0.102). The port number of the public IP address is unique for each connection. So when S1 responds to 155.4.12.1:1026, R1 look into its NAT translations table and forward the response to 10.0.0.102:1025

Networking Devices

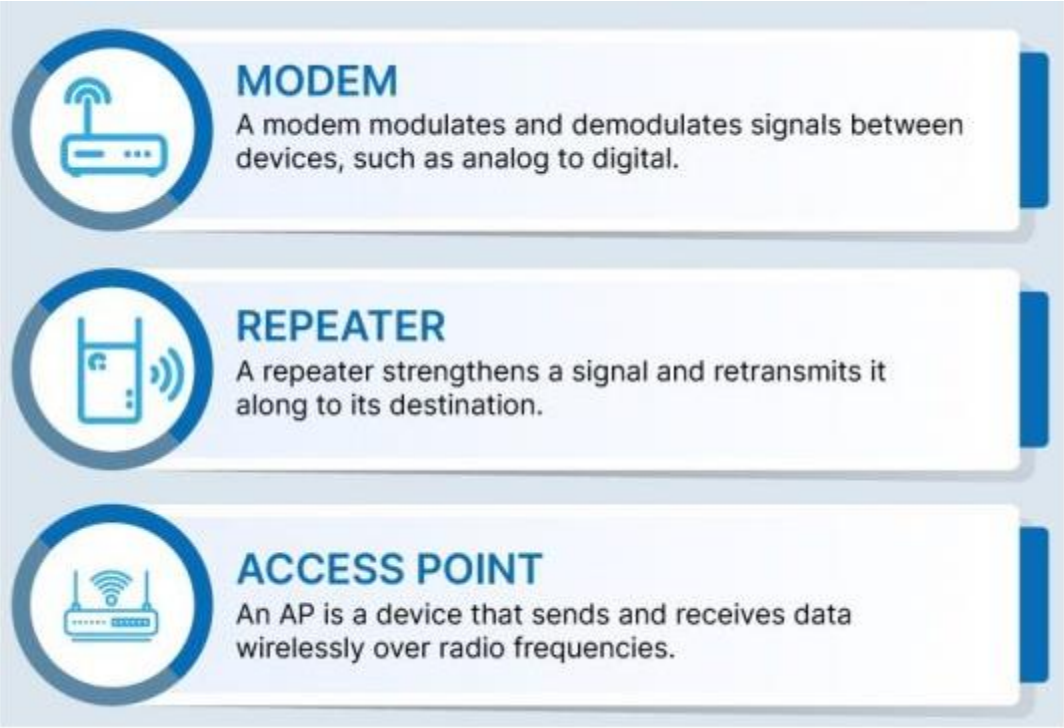
Network devices

- Physical devices that ***allow hardware on a computer network to interact and communicate with one another.***

- The devices that connect fax machines, computers, printers, and other electronic devices to the network.

- Some common examples of network devices in computer networks are
  - ***hub, router, switch, gateway, etc.***


TYPES OF NETWORK DEVICES
HUB
A hub joins multiple devices on the same LAN, broadcasting messages to all ports without examining frames.
SWITCH
A network switch forwards data to its proper destination, examining a packet's MAC address info to determine the intended device.
ROUTER
A router directs data requests from one network to another, using a packet's IP address to forward it to its destination.
BRIDGE
A network bridge acts as an interconnection between two LANs, creating a single network from separate LANS.
GATEWAY
A gateway connects discrete networks and translates packet data so it can travel between the systems.


MODEM
A modem modulates and demodulates signals between devices, such as analog to digital.
REPEATER
A repeater strengthens a signal and retransmits it along to its destination.
ACCESS POINT
An AP is a device that sends and receives data wirelessly over radio frequencies.

HUB

- **One of the simplest networking devices** that ***connects several computers or other network devices***
- **A hardware device** that ***allows multiple devices or connections to connect to a computer.***
- A USB hub, for example, allows multiple USB devices to connect with one computer, even if that computer only has one USB connection.
- Depending on the hub,
  - ***the number of ports on a USB hub can range from 4 to over 100, and***
  - ***it operates at the Physical layer***

HUB

- Also acts as a repeater
  - ***Amplifies signals that deteriorate after traveling long distances over connecting cables.***
- Used with both digital and analog data,
  - ***Settings have been configured to prepare for the formatting of the incoming data.***
- For example
  - ***if the incoming data is in digital format, the hub must pass it on as packets;***
  - ***if the incoming data is analog, then the hub passes it on in signal form.***
- **Do not perform *packet filtering or addressing functions***

HUB

- Send data packets to all connected devices.

- **There are two types of hubs**: ***simple and multiple port***

SRM INSTITUTE OF SCIENCE & TECHNOLOGY
Deemed to be University u/s 3 of UGC Act, 1956

HUB

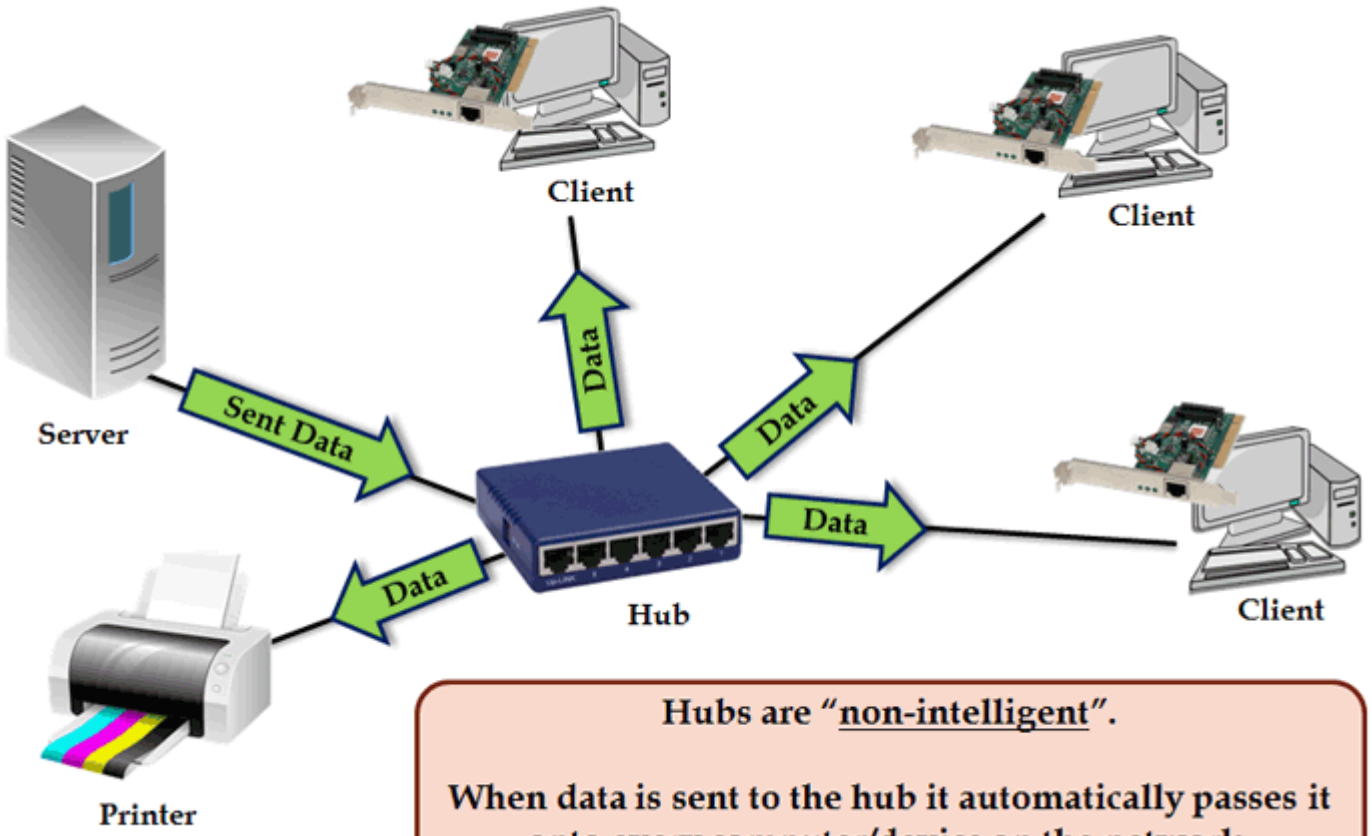
Advantages

- Easy to install
- Inexpensive
- does not affect the performance of the network seriously

Disadvantages

- Can not filter information
- can not reduce the network traffic
- Broadcast of the data happens to all the port

HUB



Hubs are "non-intelligent".

When data is sent to the hub it automatically passes it onto every computer/device on the network.

Switch

- *more intelligent role than hubs.*
- *A multiport device that improves network efficiency.*
- *Maintains limited routing information about nodes in the internal network*
- *Allows connections to systems like hubs or routers.*
- *Strands of LANs are usually connected using switches.*
- *Can read the hardware addresses of incoming packets to transmit them to the appropriate destination.*

Switch

- Switches also improve network security
  - ***The virtual circuits are more difficult to examine with network monitors.***

- A switch can work at either the Data Link layer or the Network layer of the OSI model.

- **A multilayer switch**
  - ***can operate at both layers,***
  - ***can operate as both a switch and a router.***
  - ***a high-performance device that supports the same routing protocols as routers.***

Switch

- Switches can be subject to distributed denial of service (DDoS) attacks; flood guards are used to prevent malicious traffic from bringing the switch to a halt.

- Switch port security is important so be sure to secure switches: Disable all unused ports and use DHCP snooping, ARP inspection and MAC address filtering.

Switch

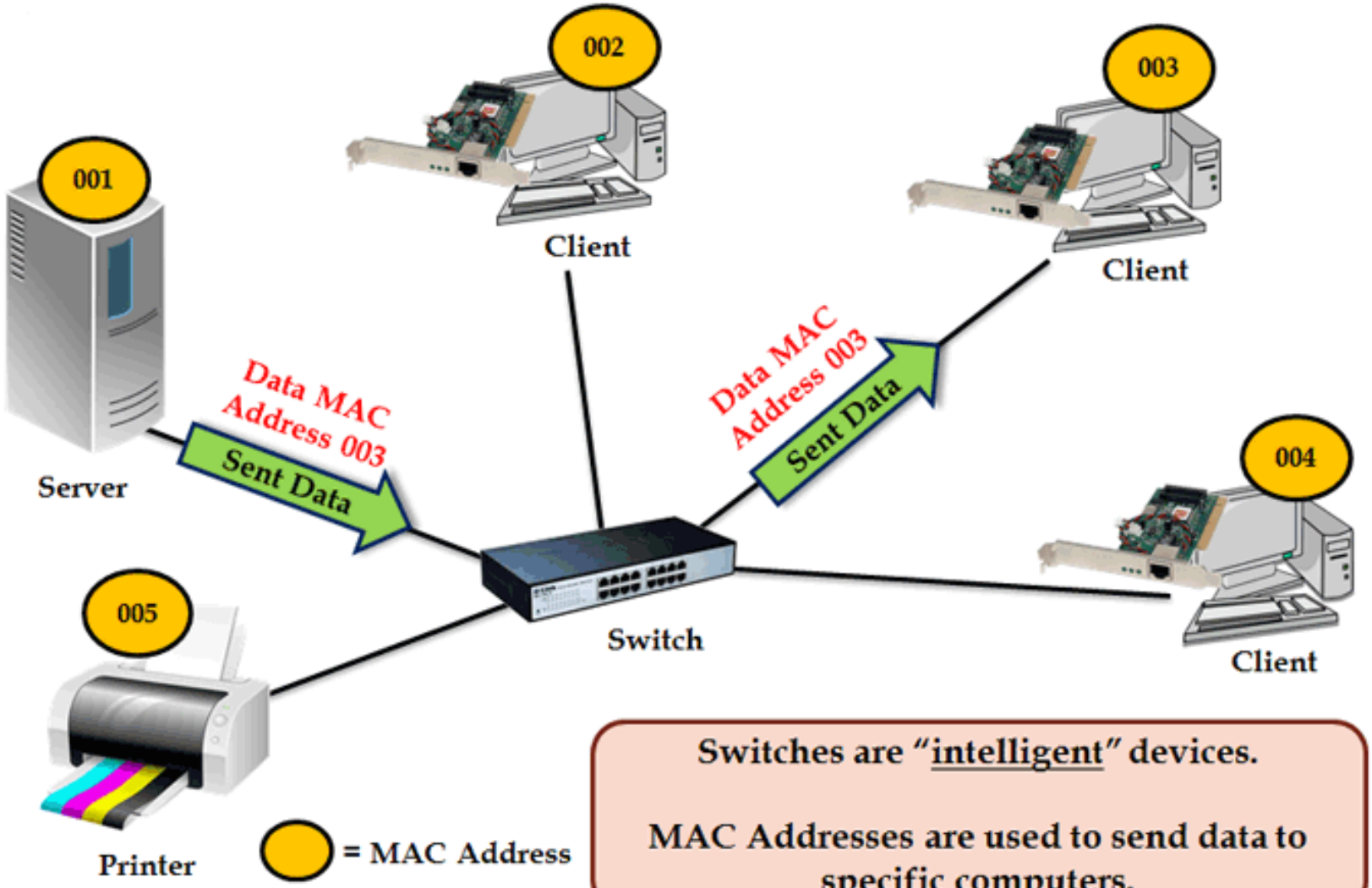
Advantages

- Increases the available bandwidth of the network.
- It helps in reducing the workload on individual host PCs
- Increases the performance of the network

Disadvantages

- They are more costly than network bridges.
- Broadcast traffic can be problematic.
- Network connectivity problems are challenging to track down via the network switch

Switch


001
002
003
004
005
Server
Client
Client
Client
Printer
Switch
Data MAC Address 003
Sent Data
Data MAC Address 003
Sent Data
= MAC Address
Switches are "intelligent" devices.
MAC Addresses are used to send data to specific computers.

Router

- Transmit packets to their destinations by charting a path through the sea of interconnected networking devices using different network topologies.

- **Routers are intelligent devices,** and ***store information about the networks they're connected to***.

- **Most routers can be configured *to operate as packet-filtering firewalls* *and use access control lists (ACLs).***

- Routers are ***also used to translate from LAN framing to WAN framing.***

Router

- This is needed because LANs and WANs use different network protocols.
- Such routers are known as border routers.
- They serve as the outside connection of a LAN to a WAN, and they operate at the border of your network.
- Router are also used to divide internal networks into two or more subnetworks.
- Routers can also be connected internally to other routers, creating zones that operate independently.

Router

- **Routers establish communication *by maintaining tables about destinations and local connections.***

- **A router contains**
  - ***information about the systems connected to it and***
  - ***where to send requests if the destination isn't known***.

- Routers usually communicate routing and other information using one of three standard protocols:
  - ***Routing Information Protocol (RIP),***
  - ***Border Gateway Protocol (BGP) or***
  - ***Open Shortest Path First (OSPF).***

Router

- ***Routers are the first line of defense***
- ***Must be configured to pass only traffic that is authorized by network administrators.***
- ***The routes themselves can be configured as static or dynamic.***
- **If they are static,** ***they can only be configured manually and stay that way until changed***.
- If they are dynamic, ***they learn of other routers around them and use information about those routers to build their routing tables.***

Router

- **Routers are general-purpose devices** that ***interconnect two or more heterogeneous networks.***

- They are usually dedicated to special-purpose computers, with separate input and output network interfaces for each connected network.

- **Routers and gateways are the backbone of large computer networks like the internet**, they have special features that give them the flexibility and the ability to cope with varying network addressing schemes and frame sizes through segmentation of big packets into smaller sizes that fit the new network components.

Router

- **Each router interface *has its***
  - ***own Address Resolution Protocol (ARP) module,***
  - ***own LAN address (network card address) and***
  - ***own Internet Protocol (IP) address.***

- The router, with the help of a routing table, has knowledge of routes a packet could take from its source to its destination.

- The routing table, grows dynamically.

- Upon receipt of a packet,
  - ***the router removes the packet headers and trailers and***
  - ***analyzes the IP header by determining the source and destination addresses and data type, and noting the arrival time.***

Router

- It also updates the router table with new addresses not already in the table.
- The IP header and arrival time information is entered in the routing table.
- Routers normally work at the Network layer of the OSI model.

Routers

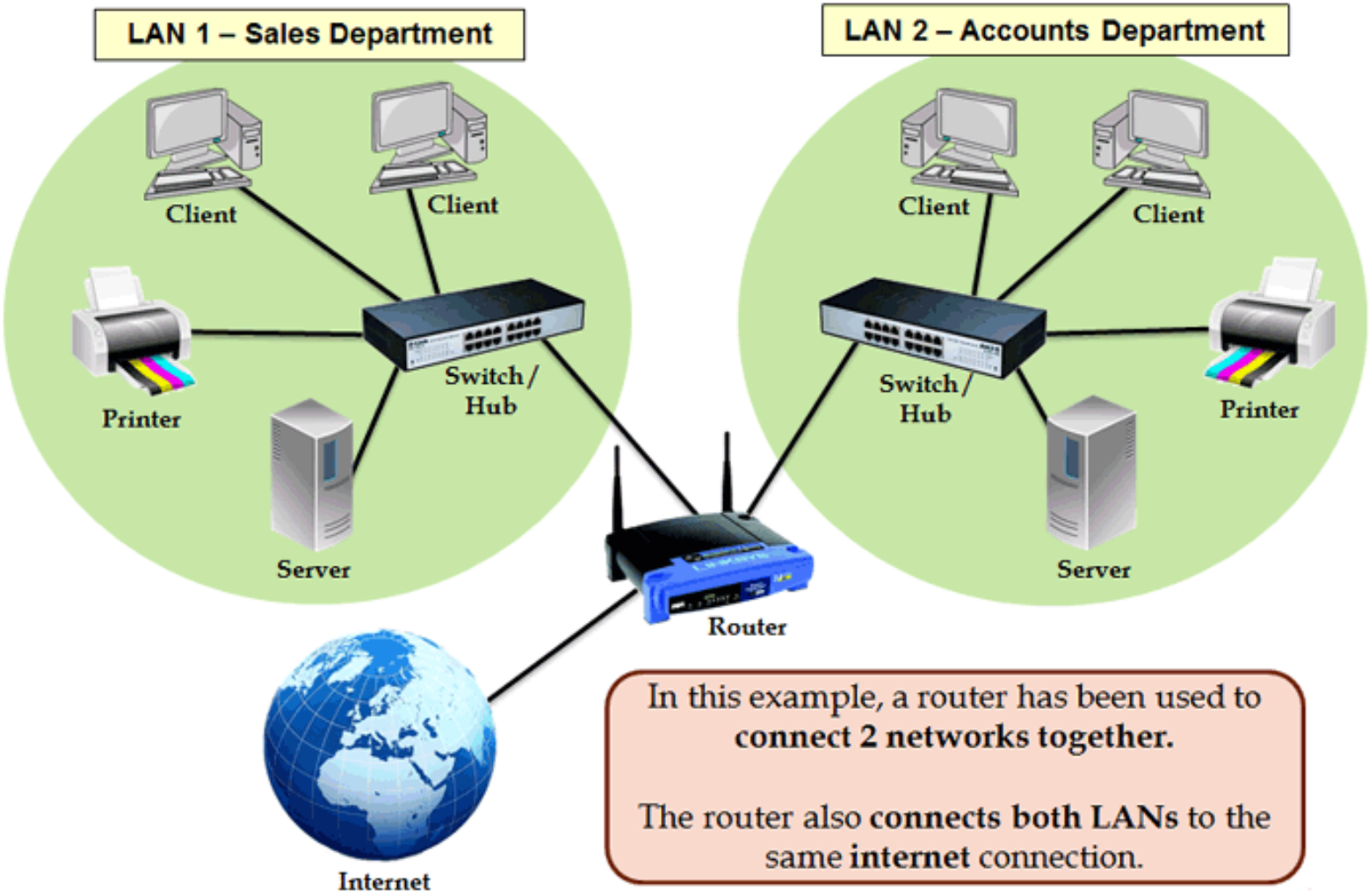
Advantages

- Connects various network architectures such as ethernet and token ring, among others.
- Reduces network traffic by establishing collision domains as well as broadcast domains.
- Chooses the best path across the internetwork using dynamic routing algorithms.

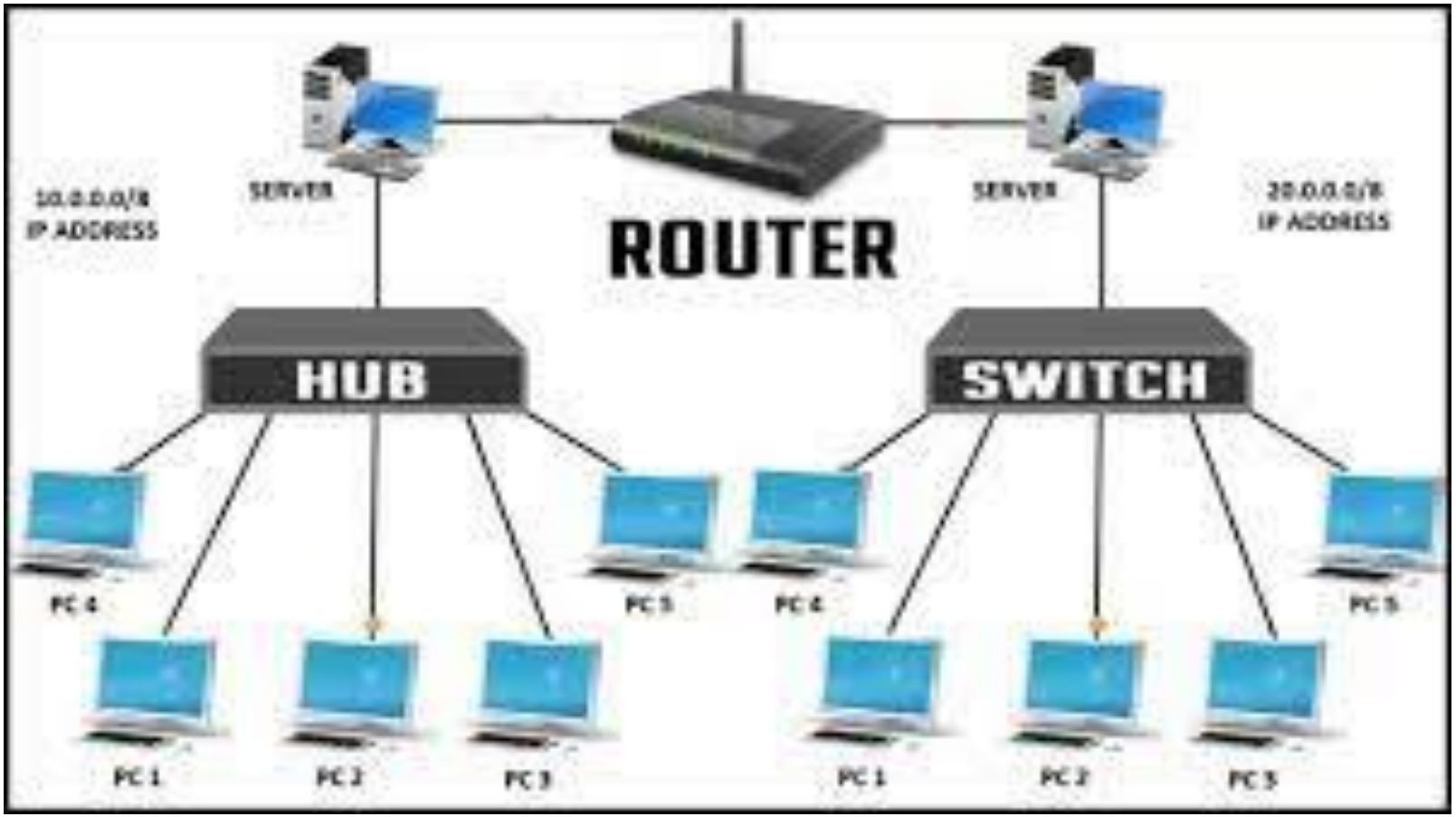
Disadvantages

- *They work with routable network protocols.*
- *More expensive than other network devices.*
- *They are slower because they must analyze data from layer 1 to layer 3.*

Router


LAN 1 – Sales Department
Client
Client
Printer
Switch / Hub
Server
LAN 2 – Accounts Department
Client
Client
Switch / Hub
Printer
Server
Router
Internet
In this example, a router has been used to **connect 2 networks together.**
The router also **connects both LANs** to the same **internet** connection.

Router


SERVER
SERVER
ROUTER
HUB
SWITCH
PC 1
PC 2
PC 3
PC 4
PC 5
PC 1
PC 2
PC 3
PC 4
PC 5

Bridge

- Bridges are used to connect two or more hosts or network segments together.
- **The basic role of bridges in network architecture *is storing and forwarding frames between the different segments that the bridge connects.***
- They use hardware Media Access Control (MAC) addresses for transferring frames.
- By looking at the MAC address of the devices connected to each segment, bridges can forward the data or block it from crossing.

Bridge

- Bridges can also be used to connect two physical LANs into a larger logical LAN.
- Bridges work only at the Physical and Data Link layers of the OSI model.
- Bridges are used to divide larger networks into smaller sections by sitting between two physical network segments and managing the flow of data between the two.
- Bridges are like hubs in many respects, including the fact that they connect LAN components with identical protocols.

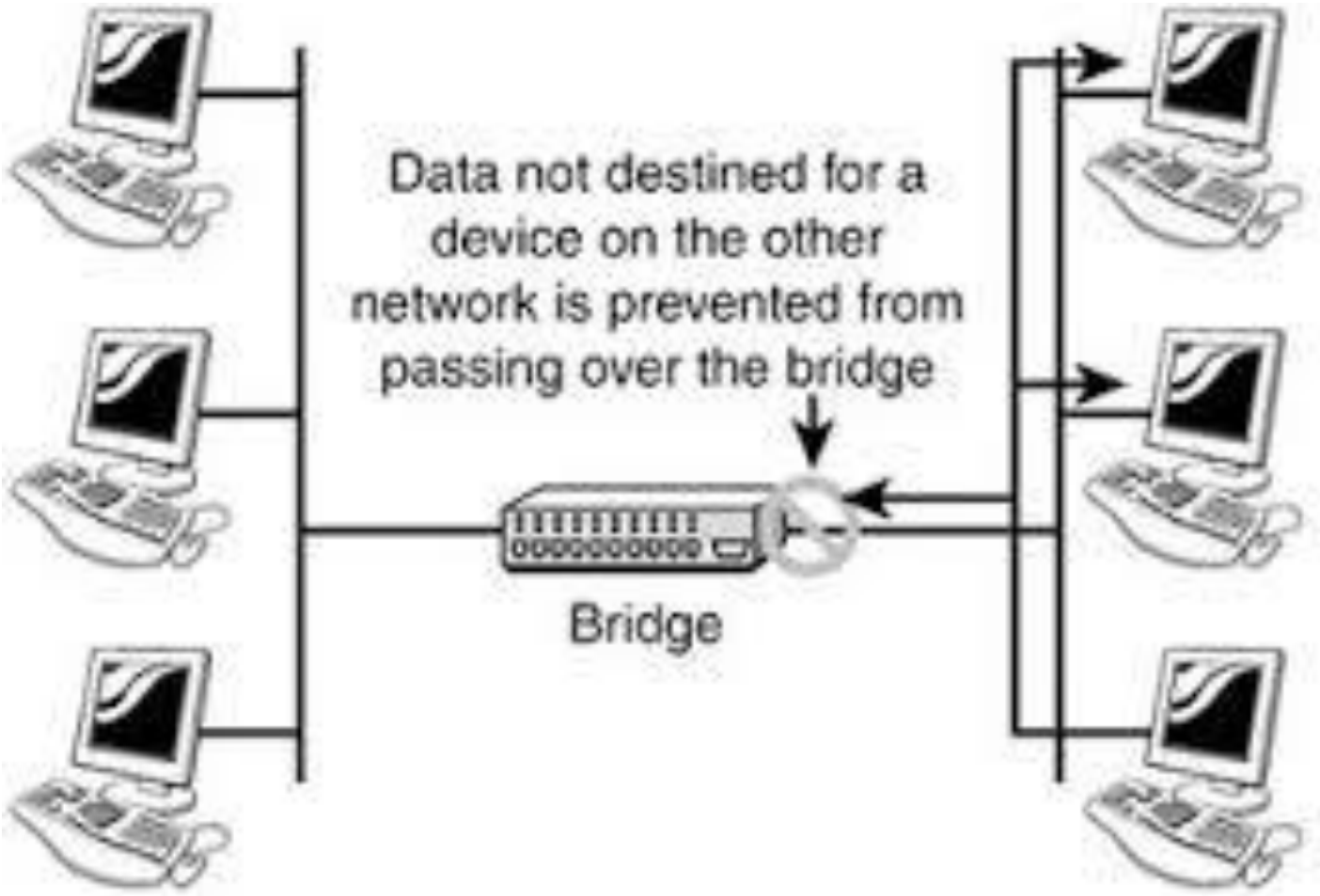
Bridge

- Bridges filter incoming data packets, known as frames, for addresses before they are forwarded.
- As it filters the data packets, the bridge makes no modifications to the format or content of the incoming data.
- The bridge filters and forwards frames on the network with the help of a dynamic bridge table.
- The bridge table, which is initially empty, maintains the LAN addresses for each computer in the LAN and the addresses of each bridge interface that connects the LAN to other LANs.

Bridge

- Bridges, like hubs, can be either simple or multiple port.
- Bridges have mostly fallen out of favor in recent years and have been replaced by switches, which offer more functionality.
- In fact, switches are sometimes referred to as “multiport bridges” because of how they operate.

Bridge


Data not destined for a device on the other network is prevented from passing over the bridge
Bridge

Routers

Advantages	Disadvantages
• Reduces collisions	• Does not filter broadcasts
• Reduces network traffic with minor segmentation	• More expensive compared to repeaters
• Connects similar network types with different cabling.	• Slower compare to repeaters due to the filtering process

Repeater

- A repeater is an electronic device that amplifies the signal it receives.
- receives a signal and retransmits it at a higher level or higher power so that the signal can cover longer distances, more than 100 meters for standard LAN cables.
- Repeaters work on the Physical layer.
- A repeater boosts the strength of a signal so that it can travel longer distances without losing quality.

Repeater

- These devices are commonly used in networks to help data reach further destinations.
- A range extender or wireless repeater, for example, is a repeater that extends the range and strength of a Wi-Fi signal.
- A repeater is effective in office buildings, schools, and factories where a single wireless router cannot reach all areas.
- A repeater operates at the OSI model's physical layer (Layer 1).

Repeater

Advantages	Disadvantages
• Repeaters are simple to set up and inexpensive.	• Repeaters are unable to connect disparate networks.
• Repeaters do not necessitate any additional processing.	• They are unable to distinguish between actual signals and noise.
• They can connect signals with various types of cables.	• They will not be able to reduce network traffic.

Thank You