KEMENTERIAN PENDIDIKAN MALAYSIA

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

FAKULTI TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

/ myftmk

http://ftmk.utem.edu.my

Chapter 5

by

Dr. Nazrul

nazrulazhar@utem.edu.my

NETWORK LAYER

INTERNET PROTOCOL VERSION 4

BITS 2343 | Computer Network

Learning Outcome

- Identify the role of the Network Layer, as it describes communication from one end device to another end device.
- Examine the most common Network Layer protocol, Internet Protocol (IP), and its features for providing connectionless and best-effort service.
- Understand the principles used to guide the division or grouping of devices into networks.

Outline

- IPv4
  - Network layer: Communication from host to host
  - IPv4: Example of network layer protocol
  - IPv4 packet header

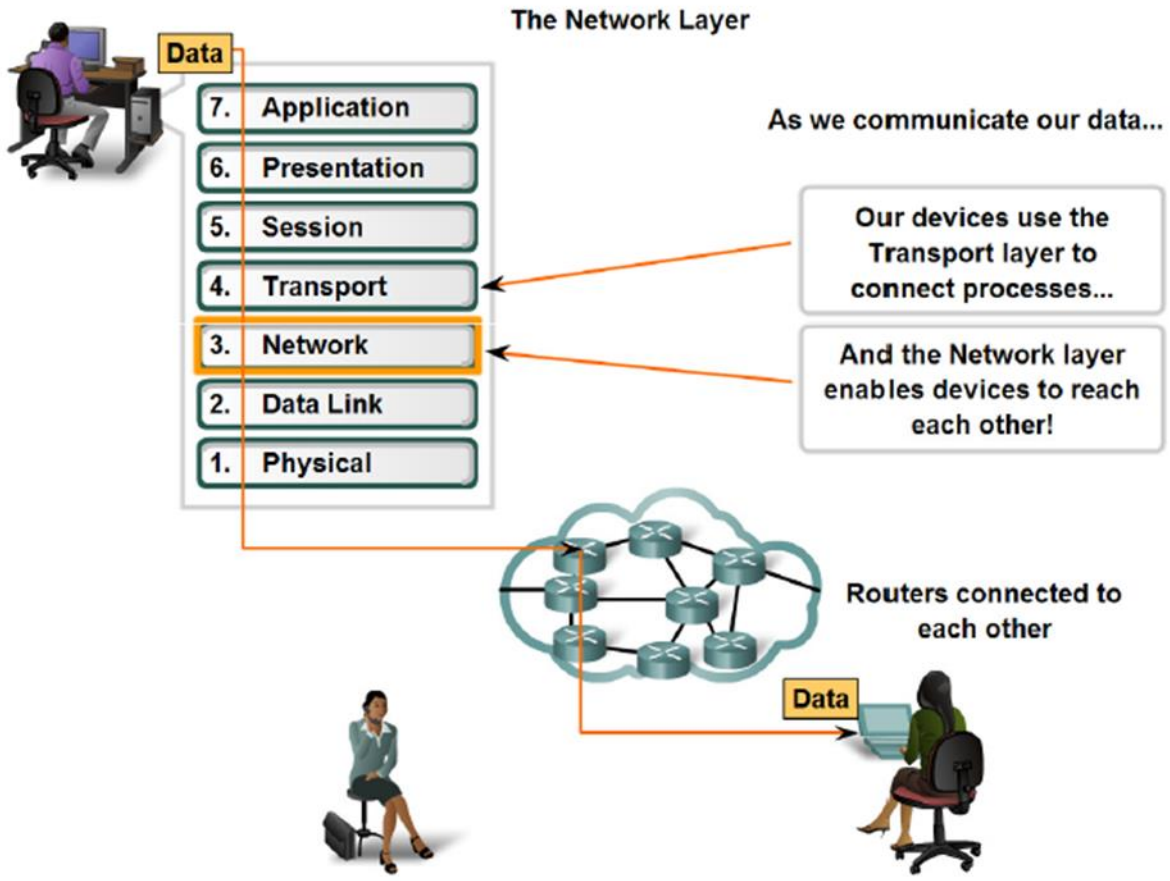
- Networks: Dividing hosts into groups
  - Creating common groups
  - Why separate hosts into networks
  - Dividing networks from networks

Internet Protocol (IP)

IPv4

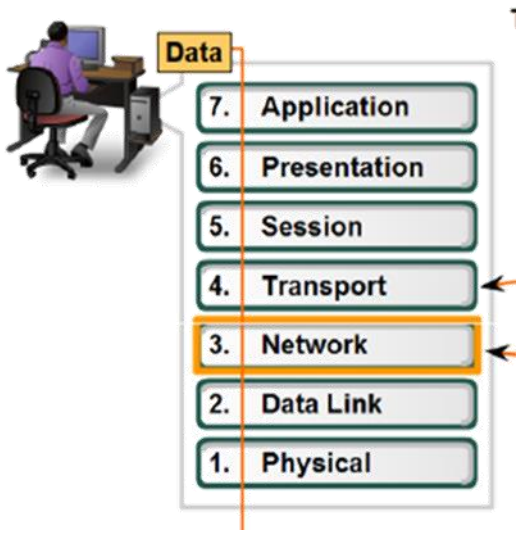
- The Network layer, or OSI layer 3, provides services to exchange the individual pieces of data over the network between identified end devices.
- To accomplished this end-to-end transport the segment (layer 4 PDU) will go through layer 3 processes:
  - To address the packet to the proper destination.
  - Encapsulate the packet with necessary data for delivery.
  - Route the packet through the web of connected network for delivery.
  - The destination host decapsulate the data for processing.
- The protocol used in the Internet's network layer is the called the Internet Protocol (IP).

Network layer: Communication from host to host



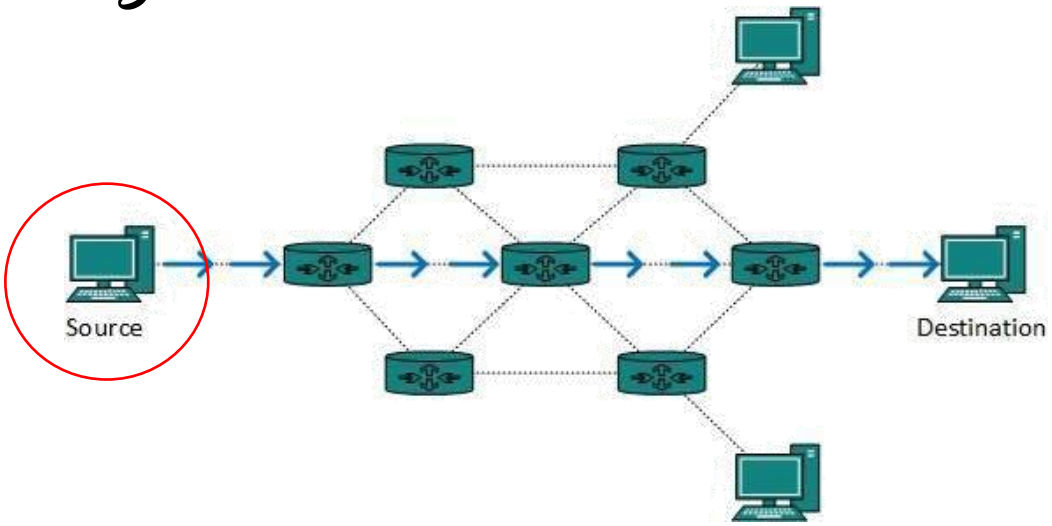
Network layer: Communication from host to host

- The network layer receives segments of data (PDU) from the transport layer.
  - Contains application data + transport header (either TCP or UDP).
- The network layer adds a header to the segment received:
  - Contains information to perform network-layer functions such as addressing.
  - The format of the header is defined by a network layer protocol such as IP.
- Four basic processes of network layer:
  i. Addressing
  ii. Encapsulation
  iii. Routing
  iv. Decapsulation



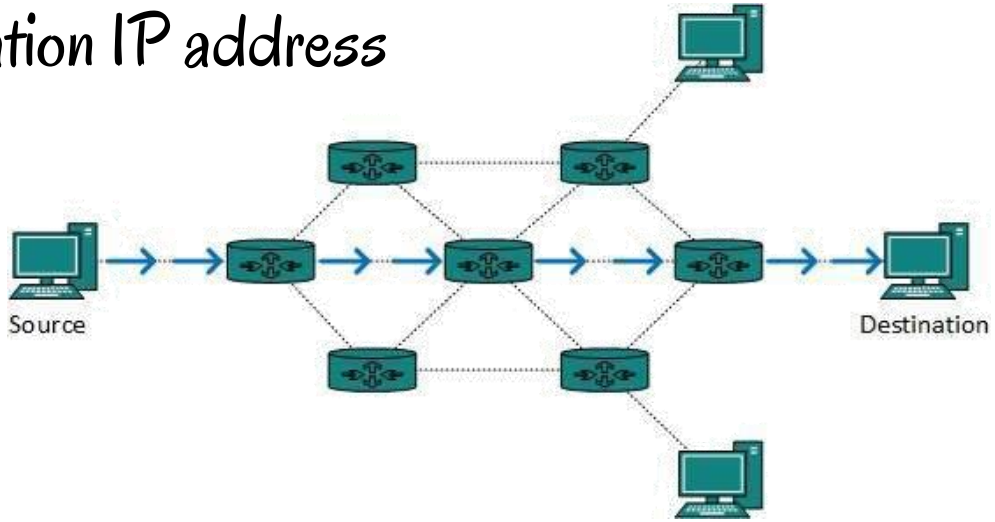
i. Addressing

- IP requires that each sending and receiving device / host to have a unique IP address.
- For a successful data transfer, both the source and destination IP addresses need to be specified.
  - Destination IP address enables the packet to be sent to the correct receiving host.
  - Source IP address enables the receiver to send a reply to the sending host.

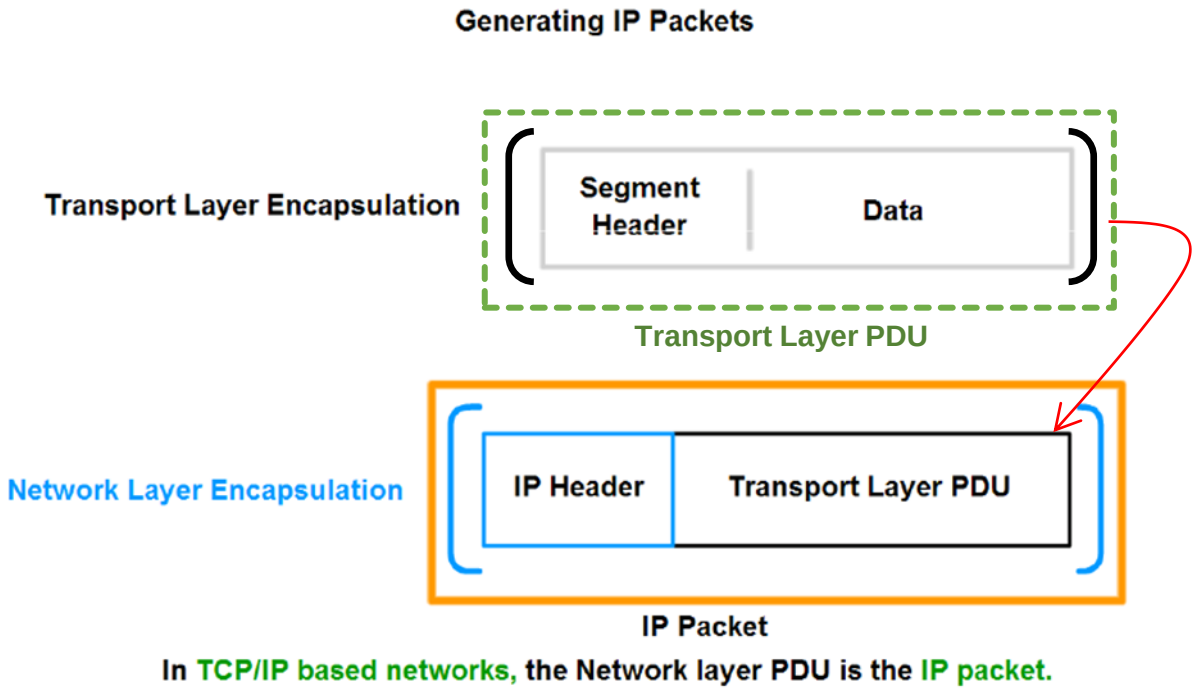


ii. Encapsulation

- Encapsulation refers to the process of adding an IP header to the segment received from the transport layer.
  - IP header + transport-layer PDU = network-layer PDU.
  - Network-layer PDU is also called a packet.
- Among others, the IP header contains:
  - Source IP address
  - Destination IP address

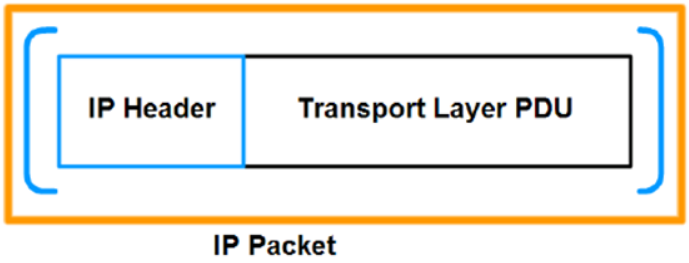


ii. Encapsulation



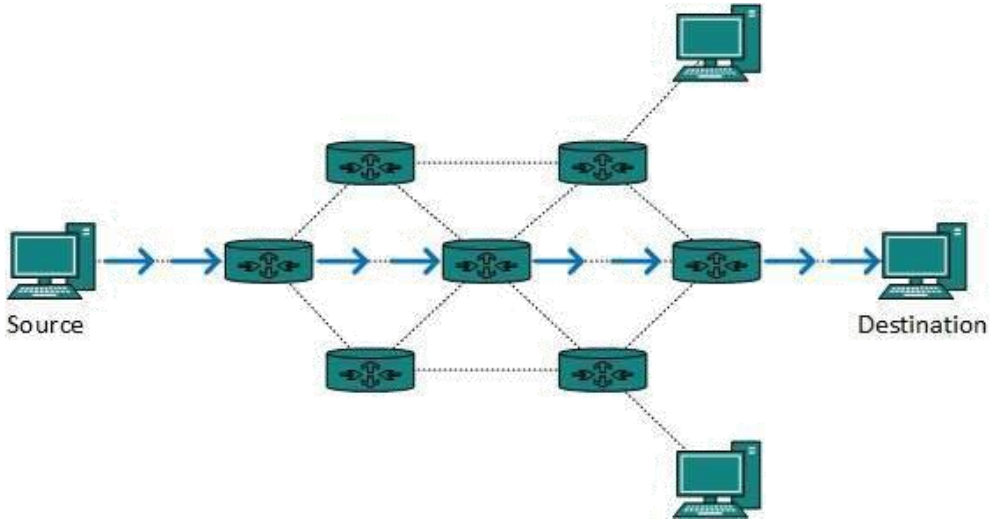
iii. Routing

- Routing refers to the process that a router performs when receiving a packet.
- This process involves:
  - Analyzing destination address information.
  - Using the address information to select a path for the packet.
  - Forwarding the packet to the next router.
- The packet header contains all the information required for the packet to travel through the network to the destination host.



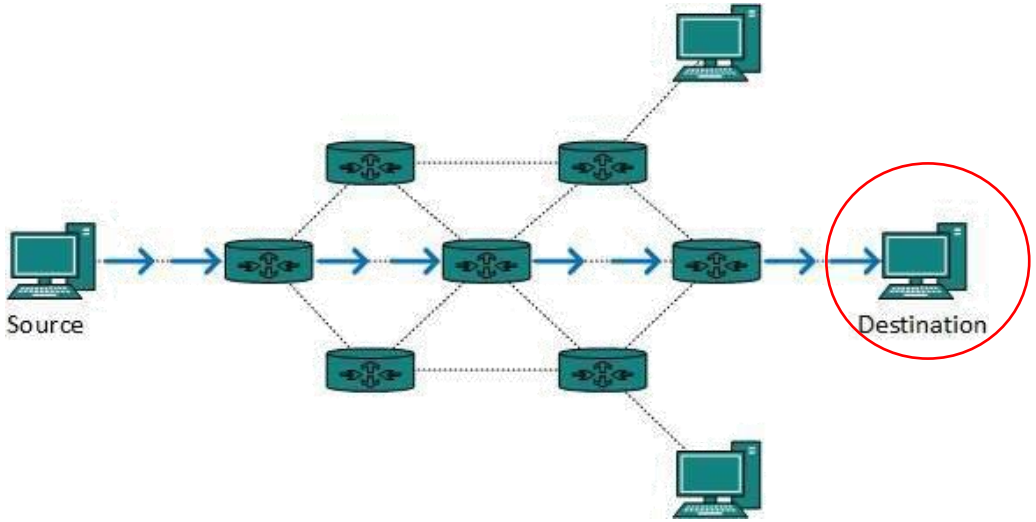
iii. Routing

- The path that the router chooses depend on the router configuration and information about the destination network.
  - Done by referring to the router's routing table.
- A packet may need to travel several hops before it reaches the receiving host.
  - A hop refers to the travel from one router to another router.
- The last router will then forward the packet to the destination host.



iv. Decapsulation

- When the receiving host receives the packet, it examines the destination address to verify that the packet was addressed to this device.
- If the address is correct, the packet is decapsulated.
  - Decapsulation refers to the process of taking off the IP header from the packet.
- The remaining segment (layer 4 PDU) is then passed to the appropriate service at the transport layer



Network Layer Protocols

Protocol	Description
Internet Protocol version 4 (IPv4)	Most widely used network protocol. Basic protocol of the Internet
Internet Protocol version 6 (IPv6)	Currently in use in some areas. Will work with IPv4 and likely to replace it
Novell IPX	Part of Novell NetWare, a widely popular internetworking protocol in the 1980s and 1990s
AppleTalk	Apple Computer's proprietary networking protocol
Connectionless Network Services (CLNS)	A protocol used in telecommunication networks that does not require established circuits

Example of Network Layer Protocol

- The network-layer protocol used in the Internet is the Internet Protocol (IP).
- The version of IP widely used in the Internet currently is IPv4.
- The next version of IP, which is IPv6 has already been developed and currently being used in certain areas.
  - IPv6 can operate alongside IPv4.
  - In the future, IPv6 is expected to replace IPv4 throughout the Internet.

Example of Network Layer Protocol

- IP was designed as a protocol with low overhead.
  - Provides only the functions that are necessary to deliver a packet from a source to a destination over an interconnected system of networks.
- IP was not designed to track and manage the flow of packets.
  - These functions are performed by other protocols in other layers.

Example of Network Layer Protocol

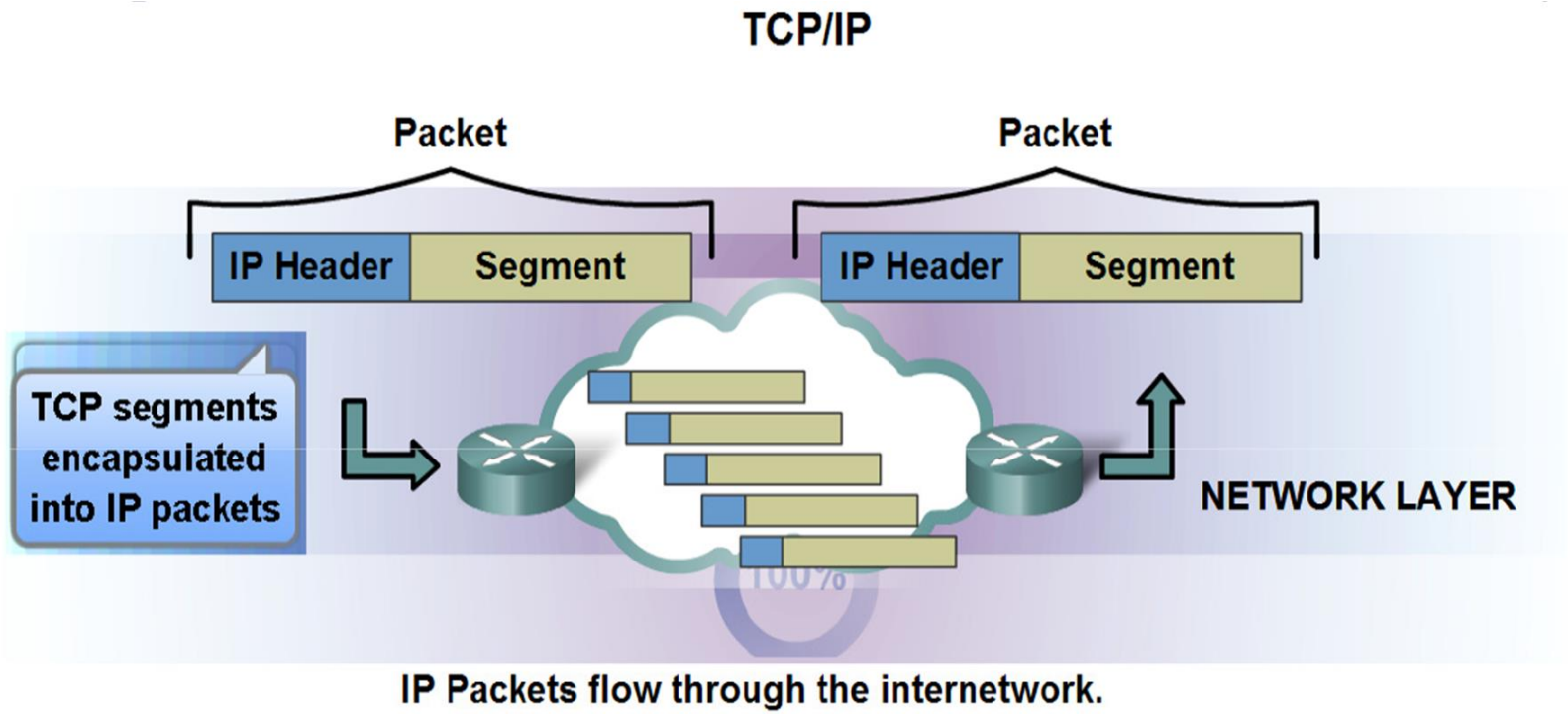
IPv4 characteristics:

i. Connectionless
   - No connection is established before sending data packet.

ii. Best effort (unreliable)
   - Does not guarantee data delivery.
   - This reduces the overhead at routers in terms of processing time and bandwidth usage.

iii. Media independent
   - Operates independently of the medium carrying the data.

Example of Network Layer Protocol



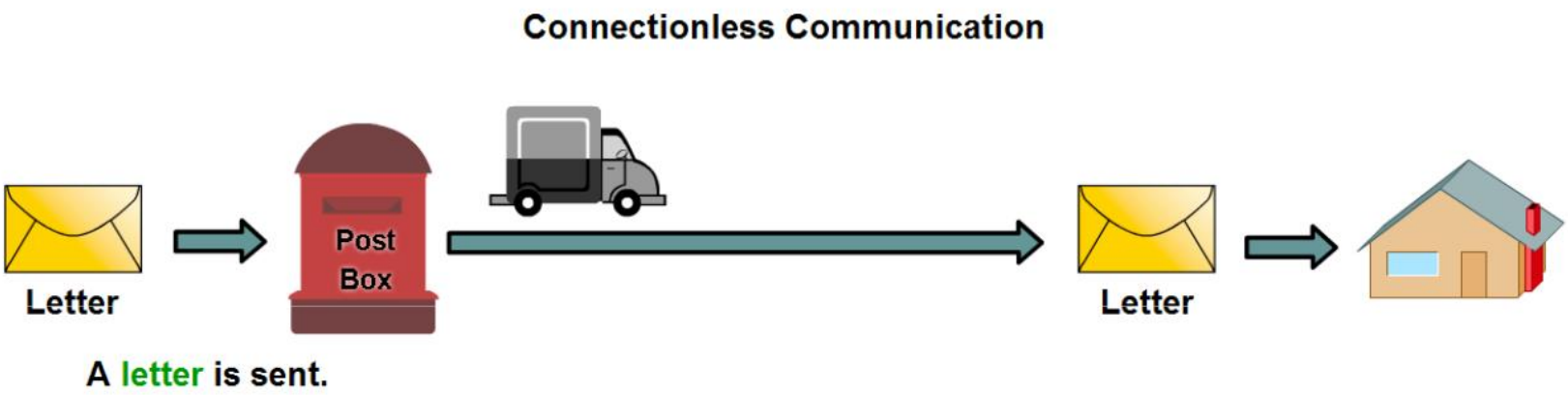
IP Packets flow through the internetwork.

i. Connectionless

- IP is connectionless:
  - No need to exchange control information to establish end to end connection before data transfer.
  - Does not require any field in the header to maintain connection.
  - This reduces the overhead of IP.

- Connectionless packet delivery may result in packets arriving at the destination out of sequence.
  - If out-of-order or missing packets create problems for the application using the data, then upper layer services will have to resolve these issues.

i. Connectionless



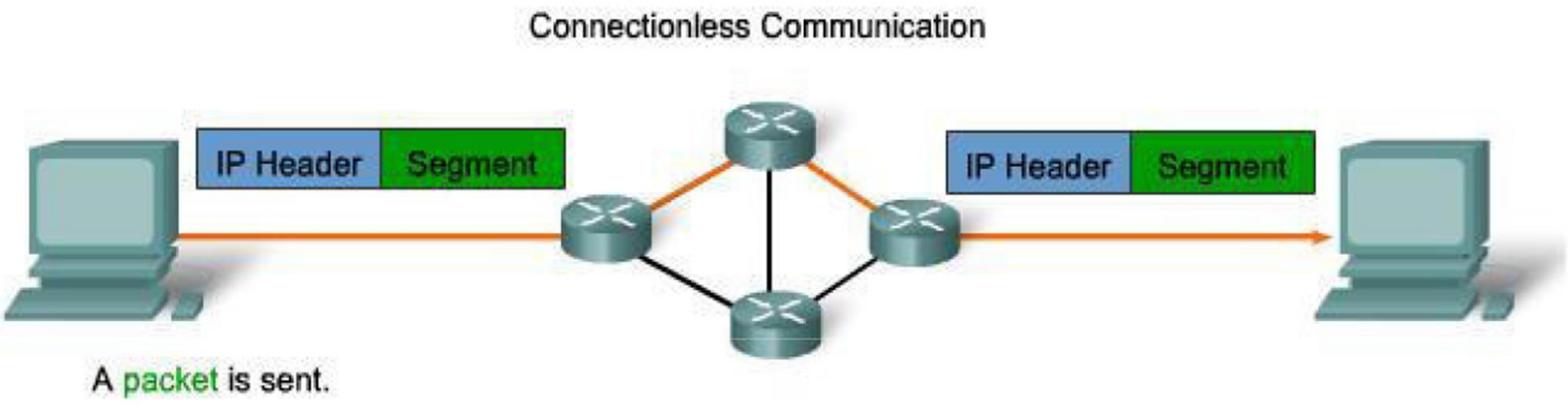
The sender doesn't know:

- if the receiver is present
- if the letter arrived
- if the receiver can read the letter

The receiver doesn't know:

- when it is coming

i. Connectionless



The sender doesn't know:

- if the receiver is present
- if the packet arrived
- if the receiver can read the packet

The receiver doesn't know:

- when it is coming

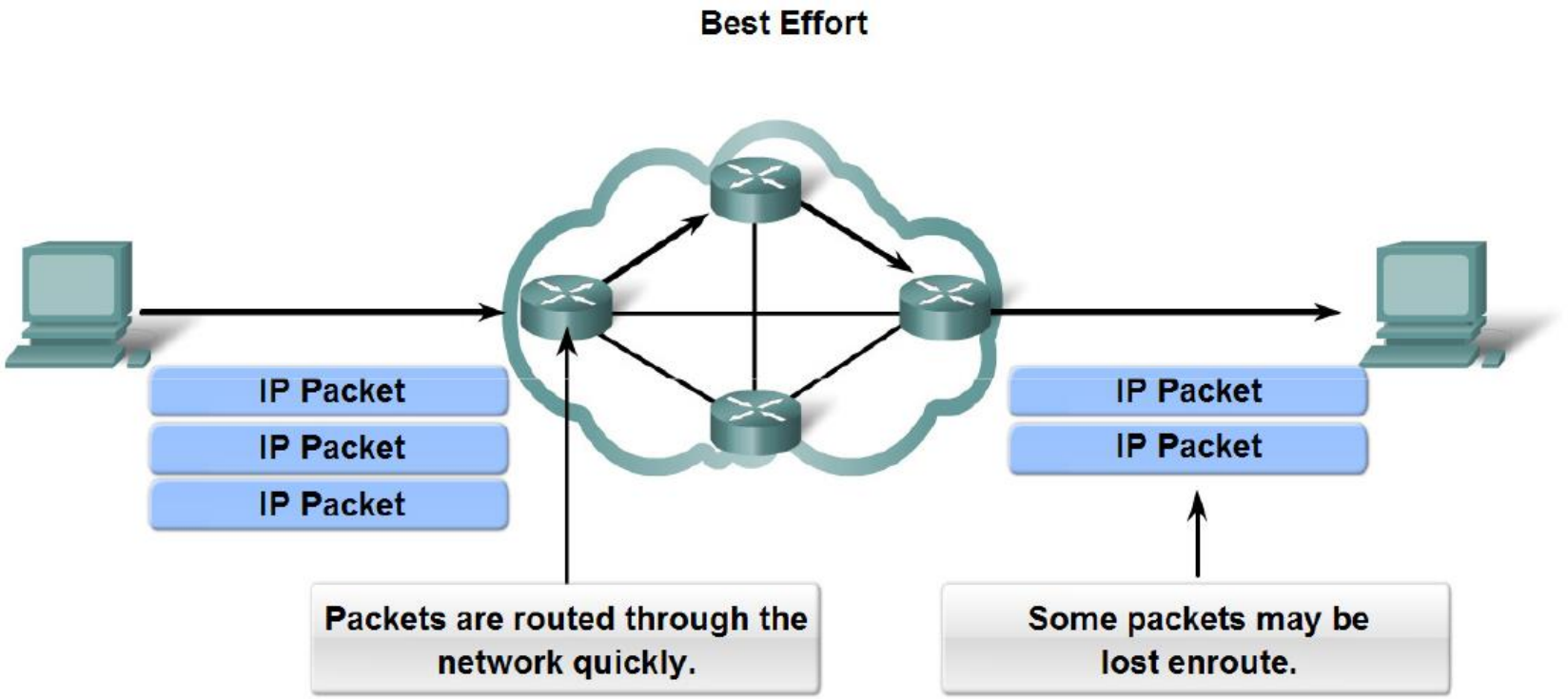
ii. Best Effort

- The IP protocol does not burden the IP service with providing reliability. It is an unreliable protocol.
  - Unreliable means that IP does not have the capability to manage, and recover from, undelivered or corrupt packets.

- Compared to a reliable protocol, the IP header is smaller.
  - Transporting these smaller headers requires less overhead.
  - Less overhead means less delay in delivery.

- Reliability will be managed by an upper layer protocol (such as TCP).

ii. Best Effort



As an unreliable Network layer protocol, IP does not guarantee that all sent packets will be received.

Other protocols manage the process of tracking packets and ensuring their delivery.

iii. Media Independent

- It does not matter whether IP packets are carried over what type of media.
  - The only difference between the different media is just how the bits are represented by the signals.

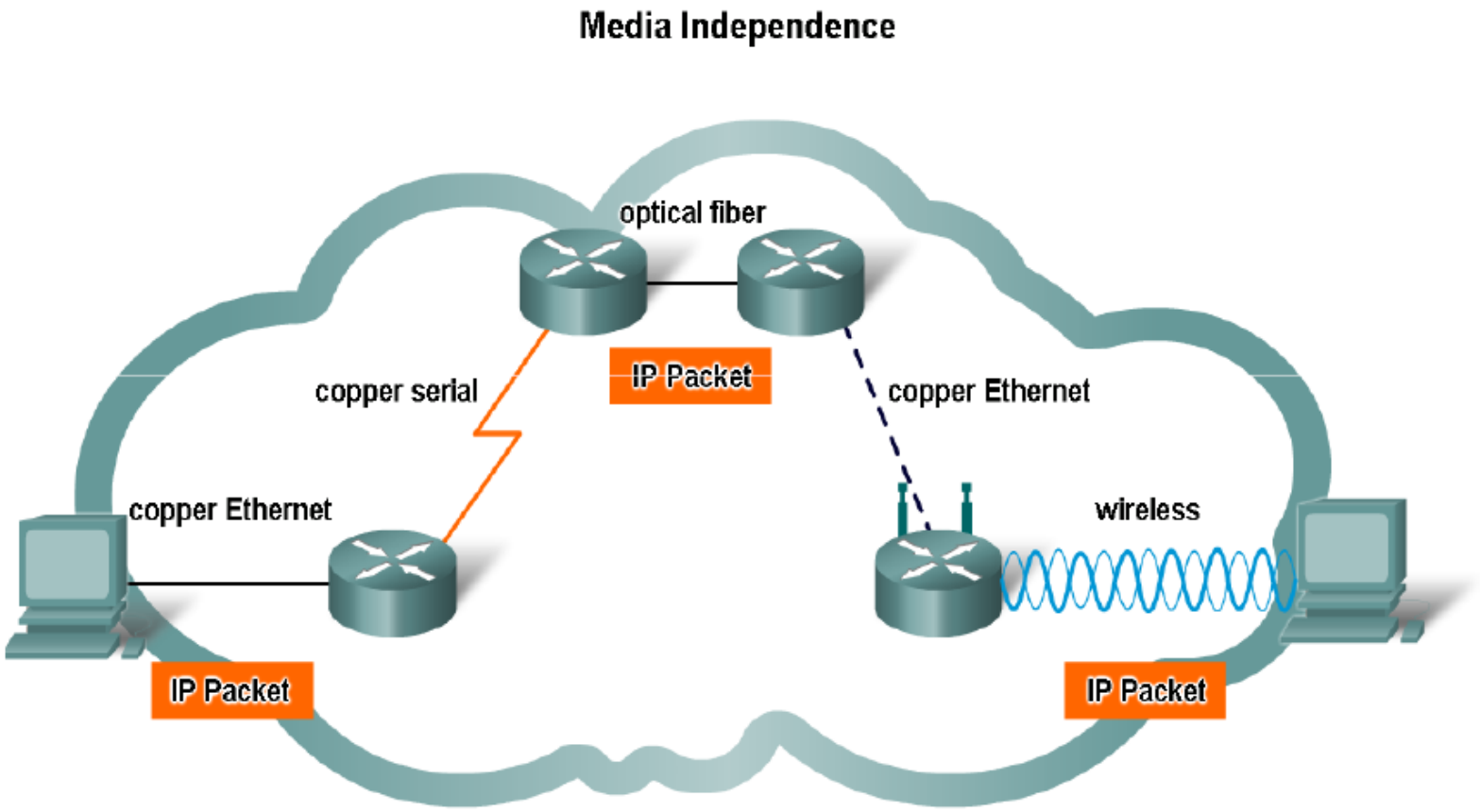
- The only issue that the network layer needs to consider is the maximum size of PDU that each medium can transport.
  - Different medium / link layer technology has its own maximum packet size.
  - This maximum size is called the maximum transfer unit (MTU).

iii. Media Independent

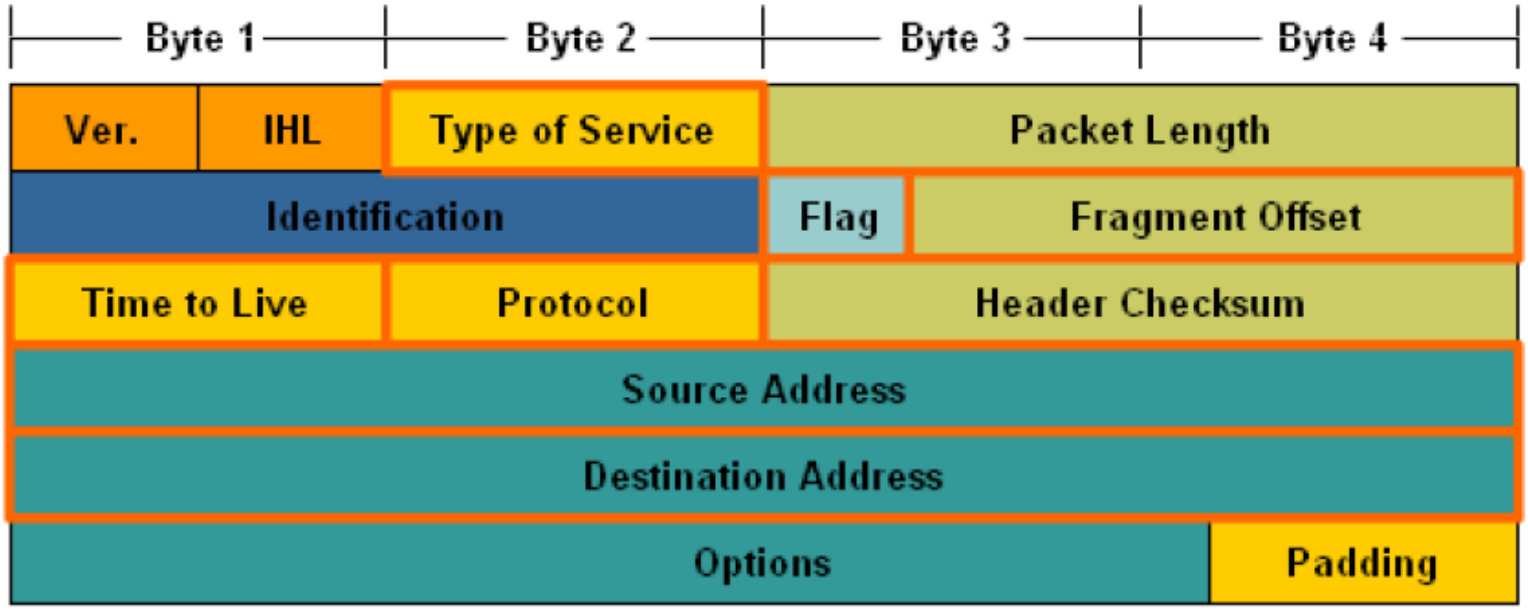
- The network layer must prepare the packets such that their size do not exceed the MTU.

- However, since a packet may go through different media along the path, it is still possible for a packet to be forwarded to a media with a smaller MTU than the packet size.
  - In this case, the router needs to fragment the packet into smaller packets.
  - This process is called fragmentation.

iii. Media Independent



IPv4 Packet Header



IPv4 Packet Header fields

IPv4 Packet Header

- Version
  - Indicates IP version, either 4 or 6.
- Internet Header Length (IHL)
  - Specifies the size of the packet header.
- Packet Length
  - Specifies the entire packet size (in bytes), including header and data.
- Identification, Flag and Fragmentation Offset
  - Used for fragmentation.
  - Enables fragmented IP packets to be reconstructed correctly by the receiving host.

IPv4 Packet Header

- Time to Live (TTL)
  - An 8 bit field that specifies the maximum hops the packet can take before it is considered lost or undeliverable.
  - The value is decreased by one each time the packet is processed by a router (that is, each hop).
  - When the value becomes zero, the router discards or drops the packet and it is removed from the network.
  - Prevents a packet from circulating forever in the network.

- Protocol
  - An 8-bit value that specifies the upper layer protocol that will receive this packet after decapsulation.

IPv4 Packet Header

- Header Checksum
  - Used for storing error checking code.
- Source Address
  - IP address of the sending host.
- Destination Address
  - IP address of the receiving host.
- Options
  - Additional fields to provide extra services.
  - Rarely used.
- Padding
  - Used to fill in bits when header data does not end on a 32-bit boundary.

Networks: Dividing hosts into groups

Networks: Dividing Hosts into Groups

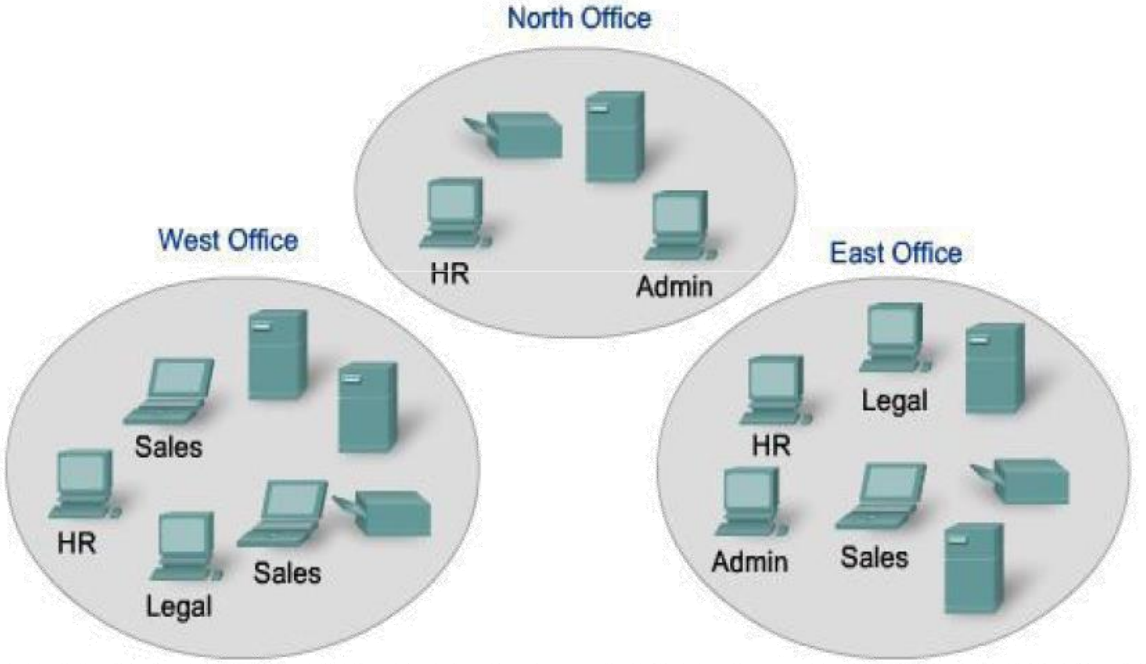
- Historically, IP-based network was managed as one large network.
  - As the network grew, so did the issues related to its growth.
  - To alleviate these issues, the large network is separated into smaller that were interconnected.
  - These smaller networks are called subnetworks or subnets.

- Dividing a network into subnets makes it easier to be managed.

Creating Common Groups

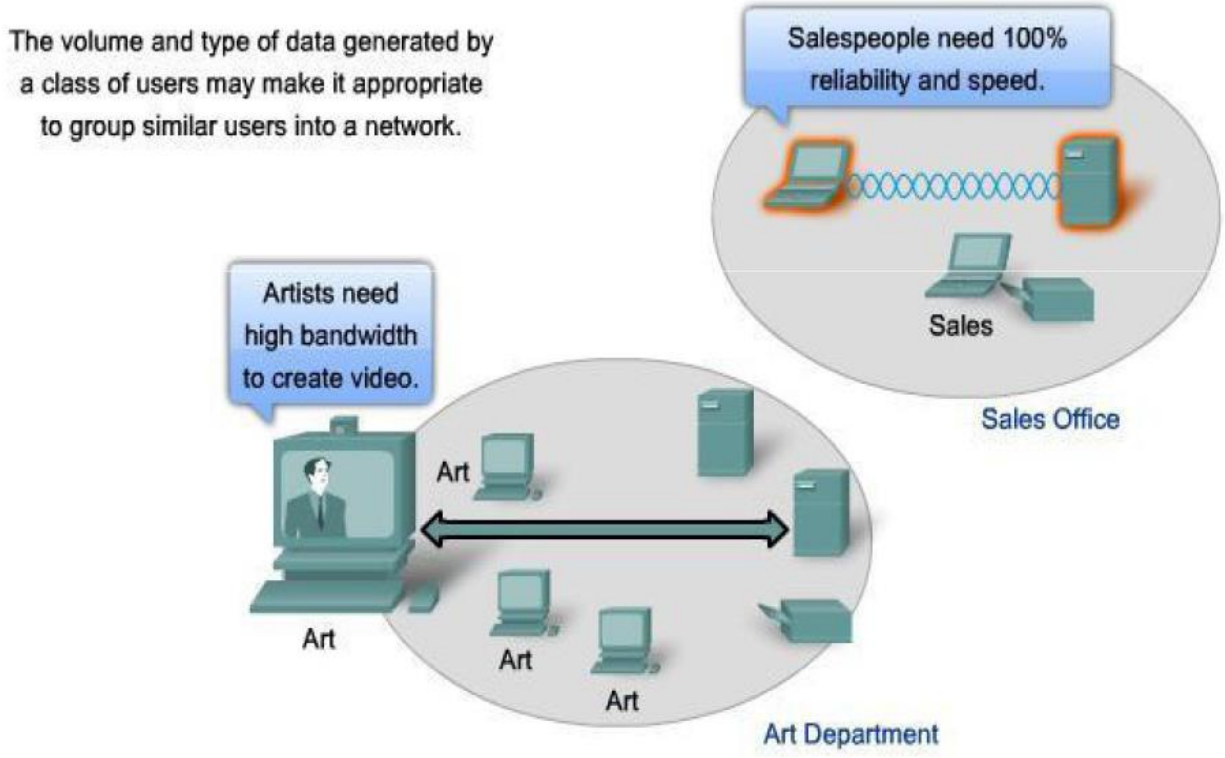
Hosts can be grouped:

- Geographically
  - Example: Grouping by office locations.

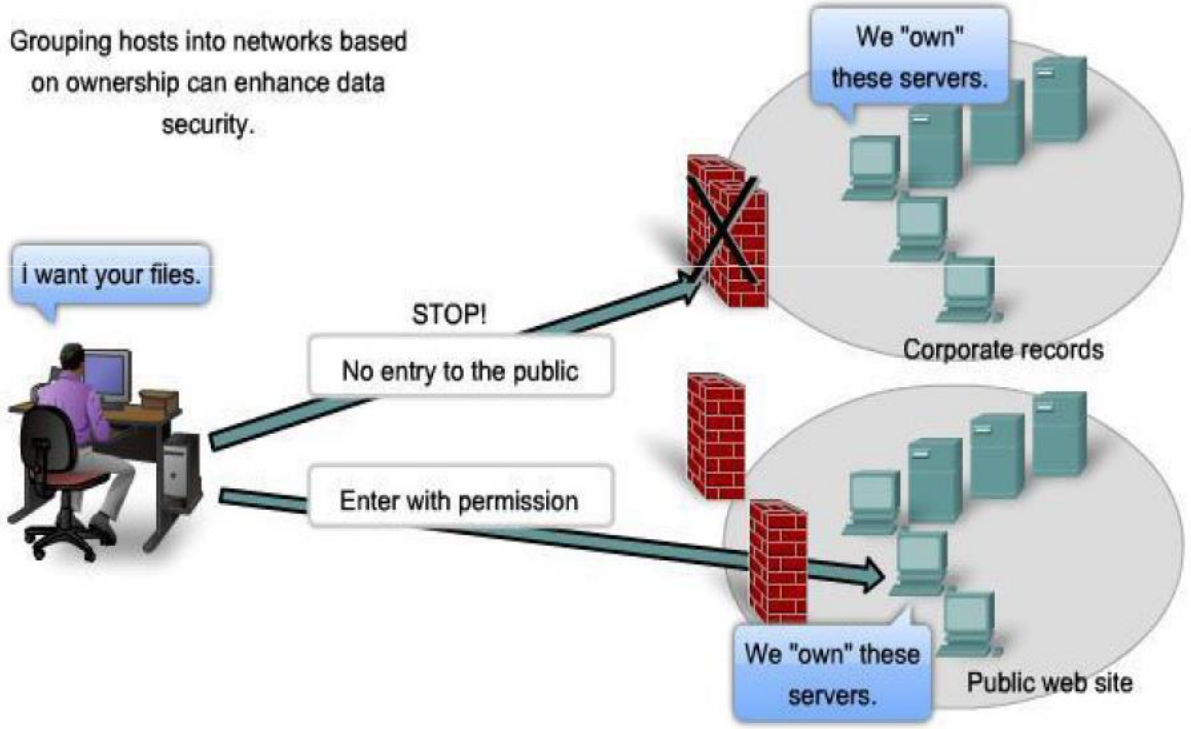


The simple fact of wiring together the physical network can make geographic location a logical place to start when segmenting a network.

- Based on a specific purpose
  - Example: Artists need high bandwidth to create video, but salesperson need 100% reliability and speed.
  - Allows network resources to be allocated accordingly.



- Based on ownership
  - Example: Certain network can only be accessed by a certain group of people.
  - Provides a boundary for security enforcement



Why Separate Hosts into Networks?

- As network gets larger, the following issues will arise:
  i. Performance degradation
  ii. Security issues
  iii. Address management

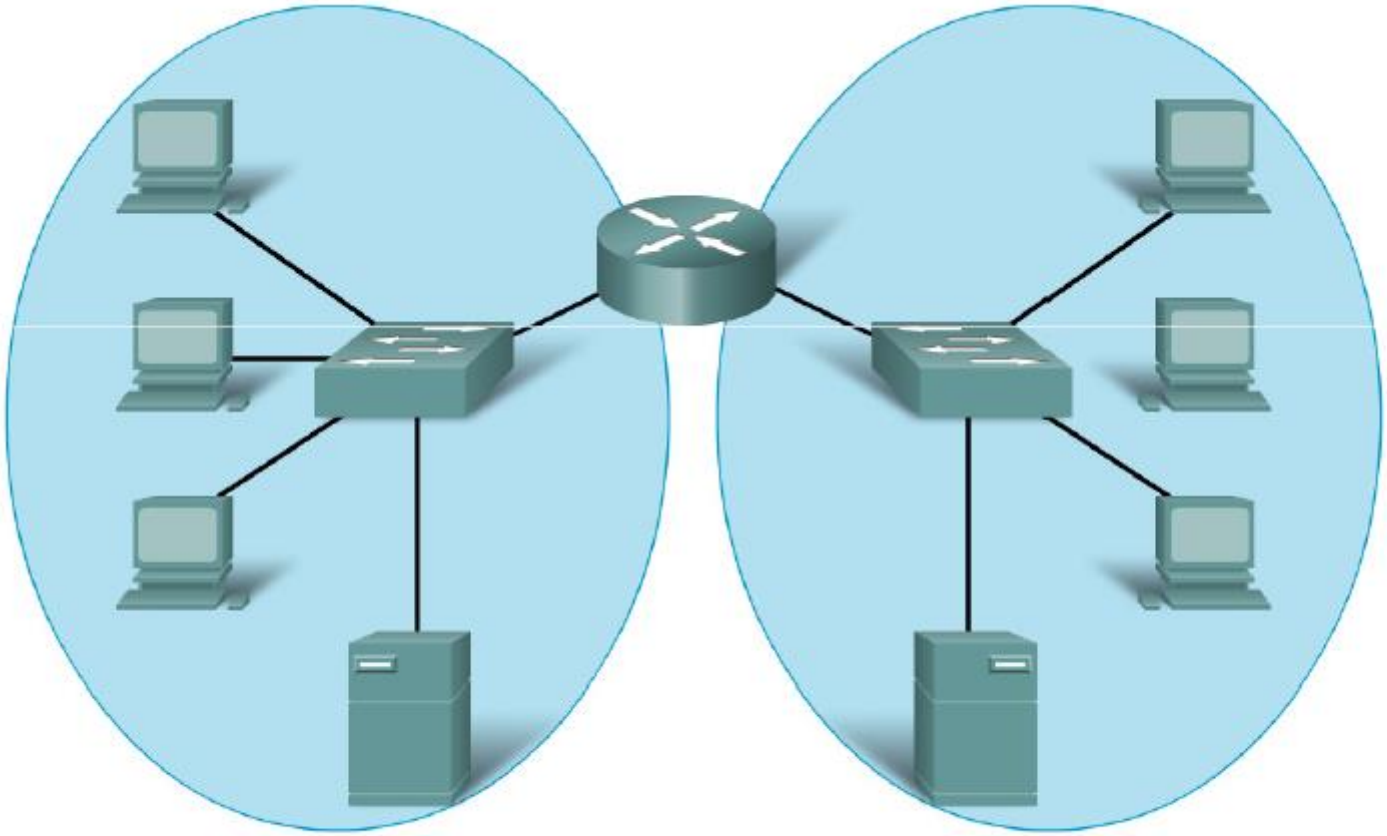
- Dividing a big network into smaller subnets can solve or reduce the issues above.

i. Performance Degradation

- Dividing a large network into smaller ones can reduce the broadcast domain.
  - A broadcast is a message sent from one host to all other hosts in the network.
    - Useful for certain applications such as DHCP.
  - A broadcast is sent to all hosts in the same network.
  - By having small networks, a broadcast sent by a host will only be sent to the other hosts in the sending host's network.

- Managing the size of broadcast domain ensures that network and host performances are not degraded to unacceptable levels.

i. Performance Degradation

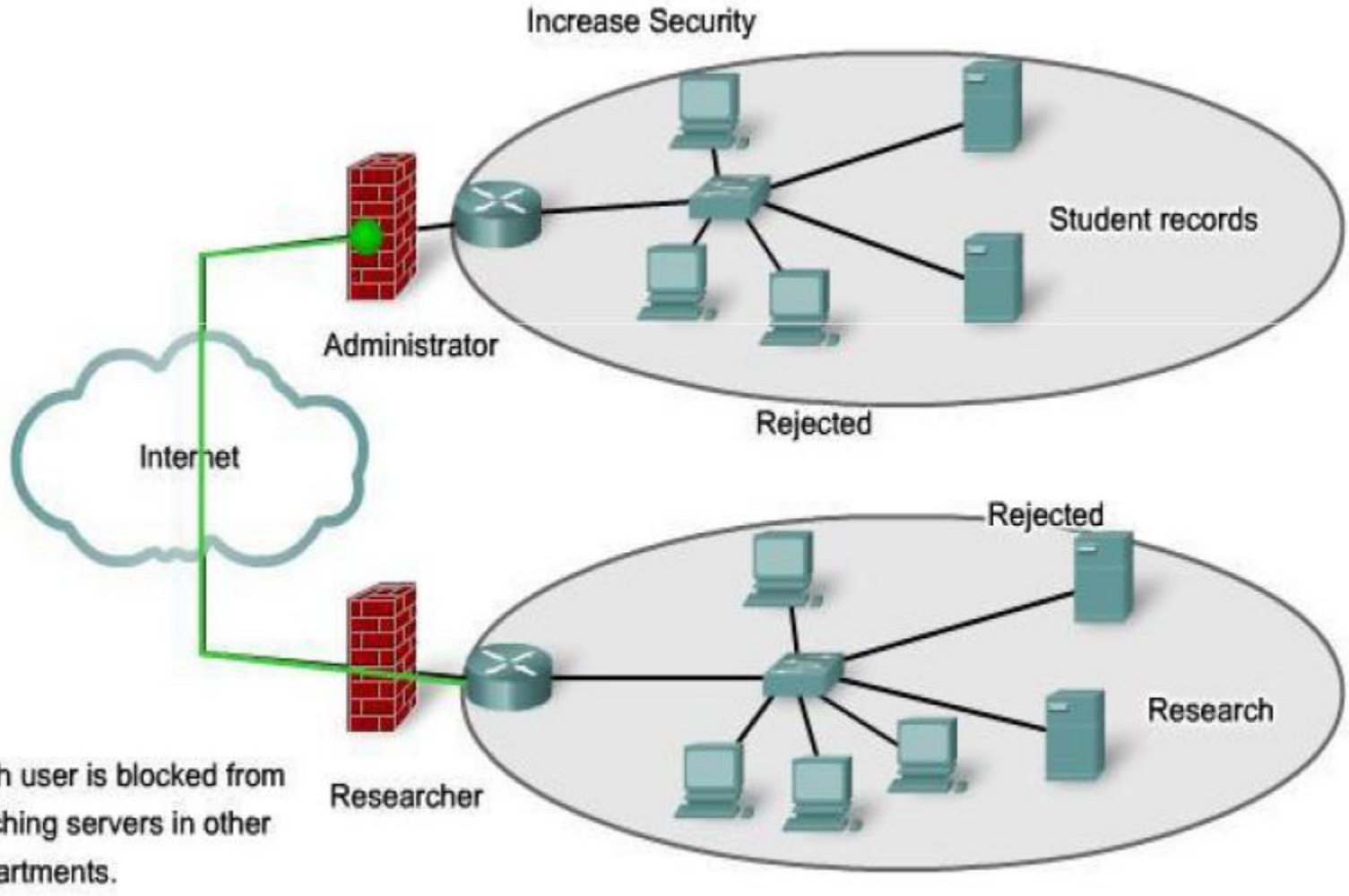


Replacing the middle switch with a router creates 2 IP subnets, hence, 2 distinct broadcast domains. All devices are connected but local broadcasts are contained.

ii. Security Issues

- Not all hosts in the network should be accessible by everybody.
- It is important for the network to provide a way to restrict user access.
  - To ensure that data cannot be accessed by unauthorized users.
- Security between networks is implemented using an intermediary device (a router or firewall) at the perimeter of the network.
  - Firewall is configured to permit only known, trusted user to access the network.
  - Enable all access to network resources to be prohibited, allowed or monitored.

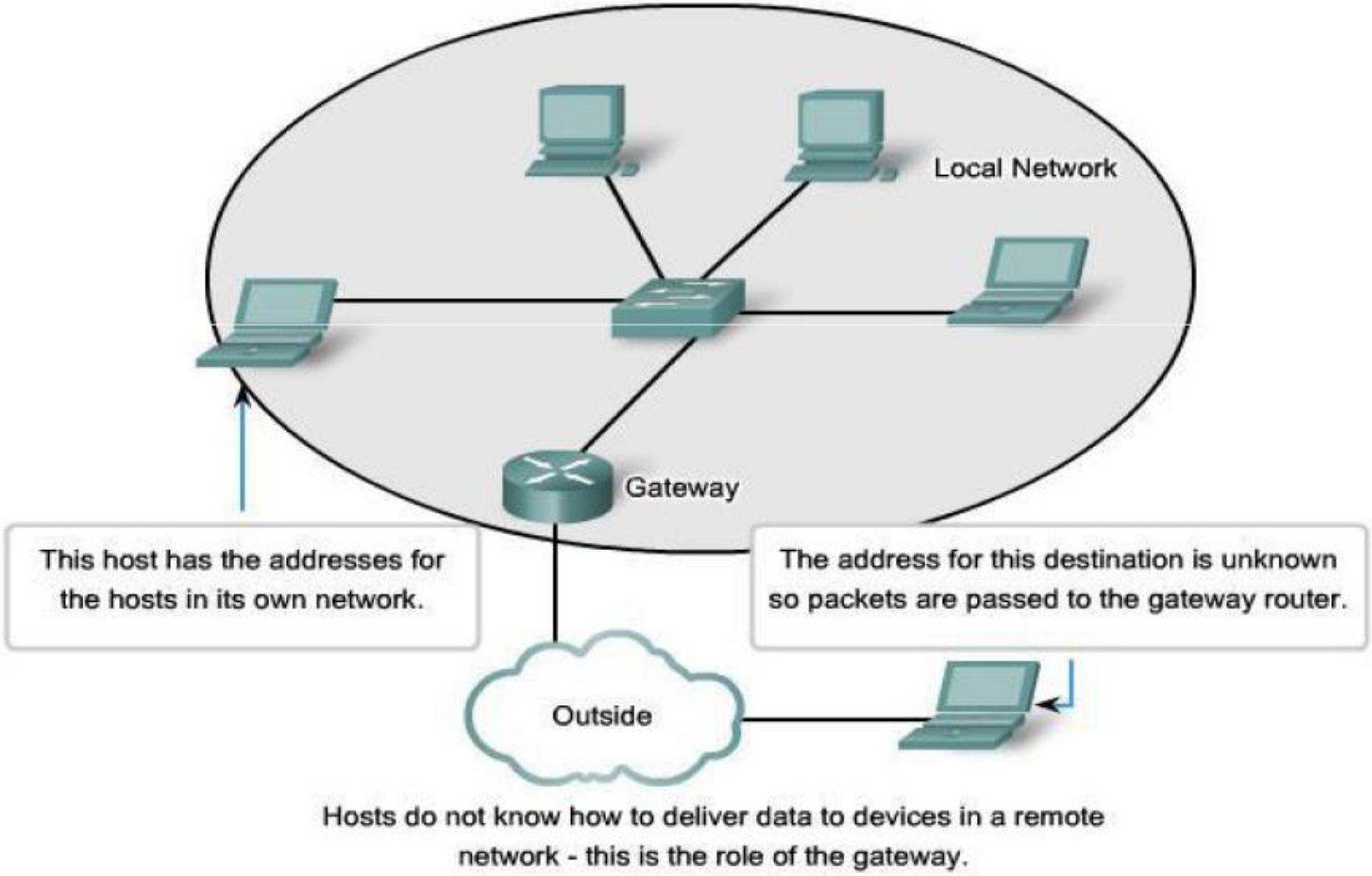
ii. Security Issues



iii. Address Management

- A host needs to know the address of the receiving host in order to send data.
- For a large network with many hosts, this can cause quite a lot of overhead (e.g. memory).
  - Since a host needs to store the addresses of all the other hosts.
- This can be solved by grouping hosts together.
  - A host only needs to store addresses of other hosts in the same group.
- For other destinations, the hosts only need to know the address of the gateway router.
  - A gateway is just a router that serves as an exit from a network.

iii. Address Management



KEMENTERIAN PENDIDIKAN MALAYSIA

UTeM
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

FTMK
FAKULTI TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

/ myftmk

http://ftmk.utem.edu.my