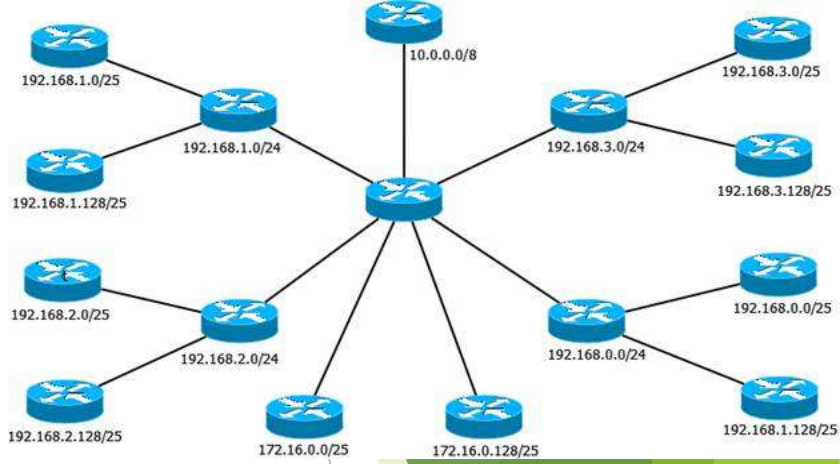
18CSE453T Network Routing Algorithms

PRESENTED BY:

Dr.S.Gnanavel M.E MISTE,MIANG,PhD.,

- Network Routing: An Introduction to Routing algorithms, Functions of Router
- IP addressing- Classful Addressing, Classless Addressing
- Protocol architecture stack – OSI Reference Model,IP Protocol Stack Architecture
- Network Topology Architecture, Network Management Architecture
- Public Switched Telephone Network
- Communication Technologies
- Standard Committees – International Telecommunication Union, Internet Engineering Task Force, MFA Forum
- Type Length Value, Network Protocol Analyzer

Networks



- Interconnection of Computers or Autonomous Systems or any electronic gadgets.
- LAN MAN WAN
- Applications – Resource sharing / Information Sharing / Communications / Distributed Processing / Remote Computing
- Star, Bus, Mesh, Tree, Hybrid topologies.
- Components involved – Sender, Receiver, Message, Medium and Protocol

Overview of Network Routing

- Network routing refers to the ability of an electronic communication network to send a unit of information from point A to point B by determining a path through the network, and by doing so efficiently and quickly.
- The determination of an efficient path depends on a number of factors
- We start with a key and necessary factor, known as addressing.
- In a communication network, addressing and how it is structured and used plays a critical role.
- In many ways, addressing in a communication network has similarities to postal addressing in the postal system.

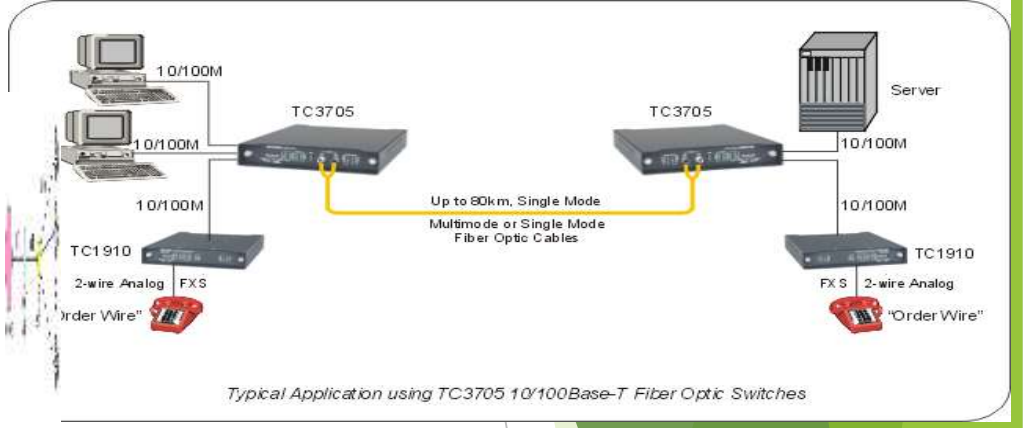
Addressing and Internet Services

- Internet addressing has similarities to the postal addressing system.
- The addressing in the Internet is referred to as Internet Protocol (IP) addressing.
- An IP address defines two parts: one part that is similar to the postal code and the other part that is similar to the house address; in Internet terminology, they are known as the netid and the hostid, to identify a network and a host address, respectively.
- Thus, a host is the end point of communication in the Internet and where a communication starts.
- A host is a generic term used for indicating many different entities; the most common ones are a web-server, an email server, and certainly the desktop, laptop, or any computer we use for accessing t he Internet.

Network Routing

- Cross-points in the Internet are known as routers
- A router's function is to read the destination address marked in an incoming IP packet, to consult its internal information to identify an outgoing link to which the packet is to be forwarded, and then forwards the packet.
- Similar to the number of lanes and the speed limit on a road, a network link that connects two routers is limited by how much data it can transfer per unit of time, commonly referred to as the bandwidth or capacity of a link; it is generally represented by a data rate, such as 1 megabits per second (Mbps).
- A network then carries traffic on its links and through its routers to the eventual destination;.

Network Routing : Overview



Typical Application using TC3705 10/100Base-T Fiber Optic Switches

- A communication network is made up of nodes and links.
- Depending on the type of the network, nodes have different names. For example, in an IP network, a node is called a router while in the telephone network a node is either an end (central) office or a toll switch. In an optical network, a node is an optical or electro-optical switch.
- A link connects two nodes; a link connecting two routers in an IP network is sometimes called an IP trunk or simply an IP link, while the end of a link outgoing from a router is called an interface. A link in a telephone network is called a trunkgroup, or an intermachine trunk (IMT), and sometimes simply a trunk

Routers

- A router is a common type of gateway.
- It is positioned where two or more networks meet at each point of presence on the internet.
- In the Open Systems Interconnection (OSI) model, routers are associated with the network layer (Layer 3).
- A router examines a packet header's destination IP address and compares it against a routing table to determine the packet's best next hop.
- Routing tables list directions for forwarding data to particular network destinations, sometimes in the context of other variables, like cost.
- They amount to an algorithmic set of rules that calculate the best way to transmit traffic toward any given IP address.

Types of Routers

- Core routers used by Internet Service Providers (ISPs) are the fastest and most powerful, sitting at the center of the internet and forwarding information along the main fiber optic backbone.

- Enterprise routers connect large organizations' networks to these core routers.

- An edge router, also known as an access router, is a lower-capacity device that resides at the boundary of a LAN and connects it to a the public internet or a private wide area network (WAN) and/or external local area network (LAN).

- Home and small office routers are considered subscriber edge routers.

Switches

- A switch is a device that is used at the Access or OSI Layer 2; a switch can be used to connect multiple hosts (PCs) to the network.
- Unlike a hub, a switch forwards a message to a specific host.
- When any host on the network or a switch sends a message to another host on the same network or same switch, the switch receives and decodes the frames to read the physical (MAC) address portion of the message.

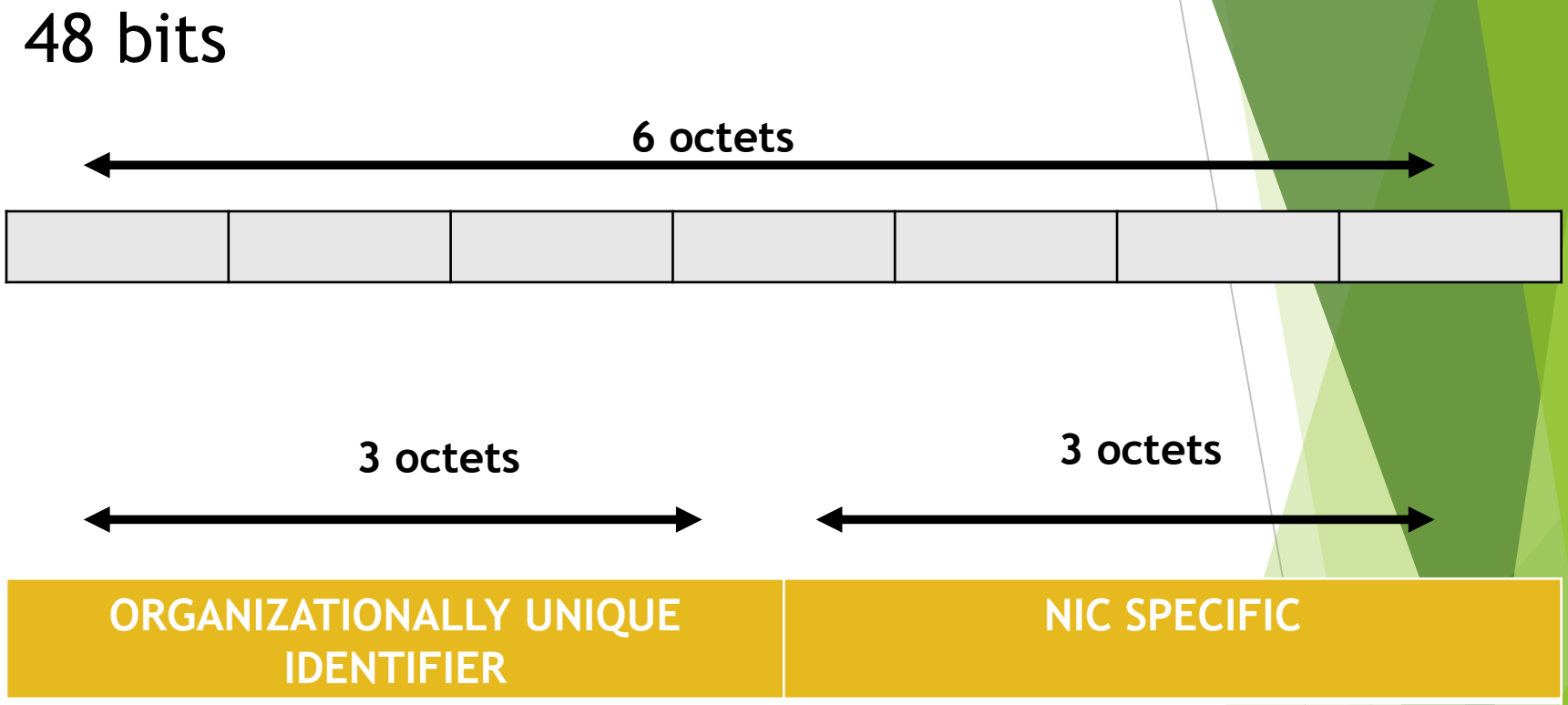
Routers vs Switches

S. No.	Key	Router	Switch
1	Objective	Router main objective is to connect various networks.	Switch main objective is to connect various devices in a network.
2	Layer	Router works in Network Layer.	Switch works in Data Link Layer.
3	Usage	Router is used in LAN and MAN.	Switch is used only in LAN.
4	Data Format	Router sends data in form of packets.	Switch sends data in form of packets and frames.
5	Mode of Transmission	Router follows duplex mode of transmission.	Switch also follows duplex mode of transmission.
6	Collision	Less collision in case of Router.	In full duplex mode, no collision happens in switch too.
7	NAT Compatability	Compatible with NAT.	Not compatible with NAT.
8	Type	Routing type is Adaptive and Non-adaptive routing.	Switching type is Circuit, Packet and Message switching.

IP ADDRESSING

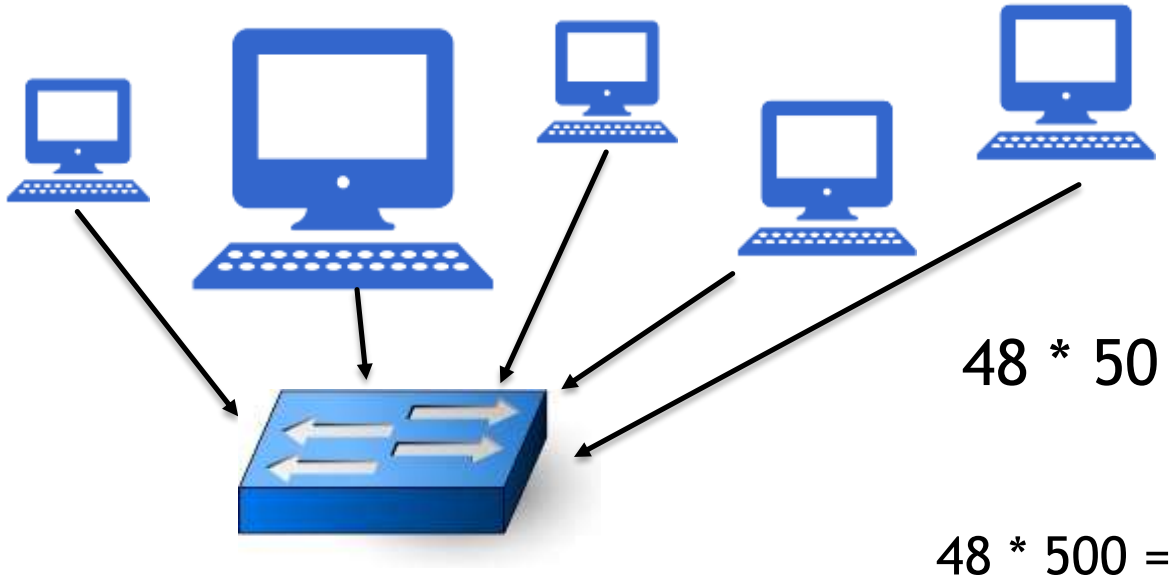
- MAC Address
- IP Address
- Port Address

MAC Address


48 bits
6 octets
3 octets
3 octets
ORGANIZATIONALLY UNIQUE IDENTIFIER
NIC SPECIFIC

For Routing?

MAC Address



48 * 50 = 2400 Bits

48 * 500 = 24000 Bits

48 * 5 = 240 Bits

48 * Number of devices in Internet = ???

Logical Addressing

- Two different versions of IP in TCP/IP: IPv4 and IPv6.
- IPv4 addresses are 32 bits in length.
- Broken into four bytes (called octets)

11111111	11111111	11111111	11111111

- X.X.X.X

IP Address

8	7	6	5	4	3	2	1
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

Binary to decimal conversion for byte values

1. Value of 11000001?

11111111.11111111.11111111.11111111

2. Value of 00110011?

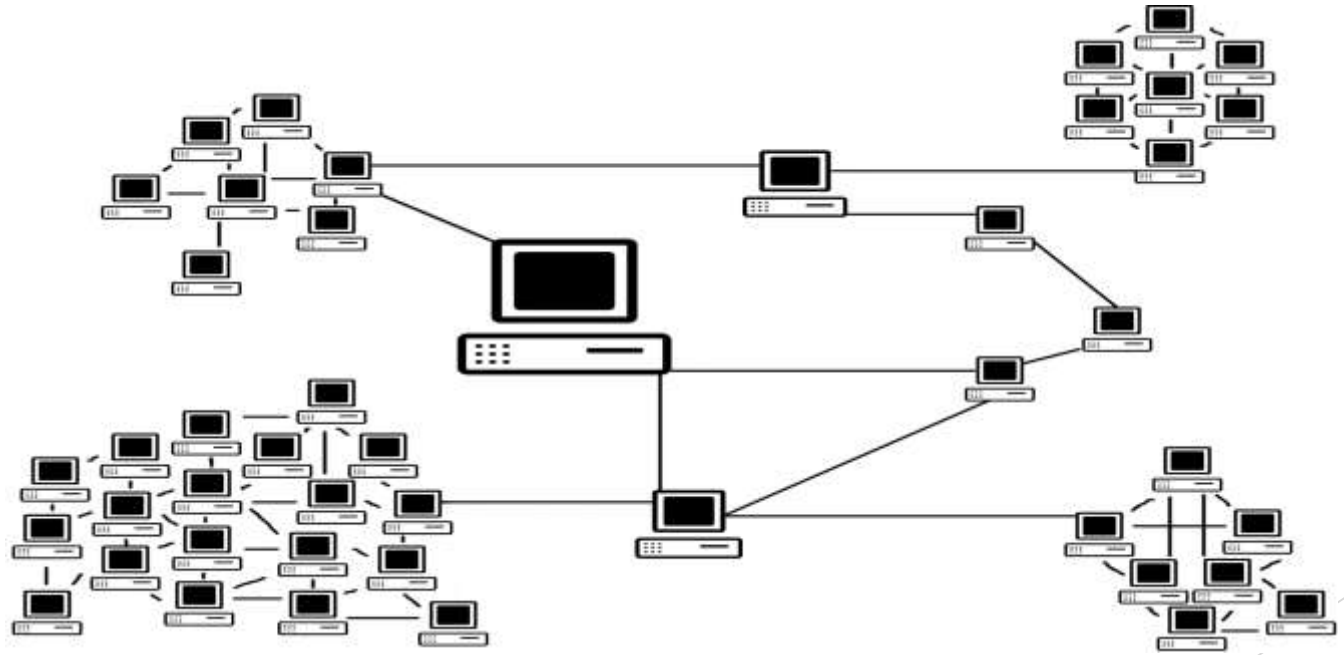
255.255.255.255

Classes of Addresses

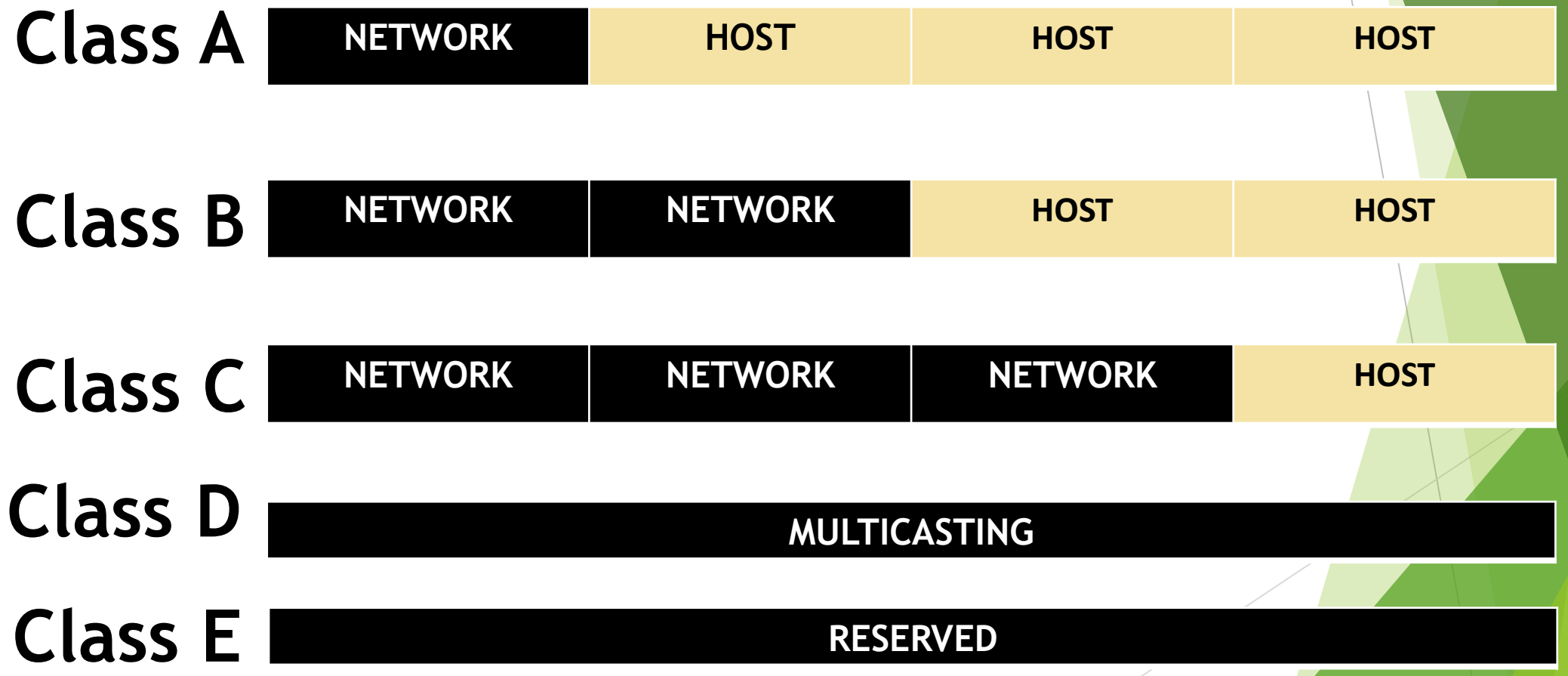
- Logical, or layer-3, or IP addresses, have two components:

Network Number	Host Number

- The network number uniquely identifies a segment in the network and a host number uniquely identifies a device on a segment.



Classes of Addresses



Distinguishing Between Classes of Addresses

- Class A addresses always begin with a “0” in the highest order bit

- Class B addresses always begin with “10” in the highest order bits

- Class C addresses always begin with “110” in the highest order bits

- Class D addresses always begin with “1110” in the highest order bits
- Class E addresses always begin with “11110” in the highest order bits

Network Numbers and Classes of Addresses

- Class A – First Bit is “0”
- Number of Network Bits = 8 Bits
- Number of Host Bits = 24

- Network starts from 00000000 to 01111111 i.e., 0 to 127
- 0 is reserved and represents all IP addresses; 127 is a reserved address and is used for testing, like a loopback on an interface: 00000001-01111111. (1 to 126)

Class B

- Class B – First two Bits are “ 10”
- Number of Network Bits = 16 Bits
- Number of Host Bits = 16

- Network starts from 10 000000 to 10 111111 i.e., 128 to 191

Class C

- Class C – First three Bits are “ 110”
- Number of Network Bits = 24 Bits
- Number of Host Bits = 8

- Network starts from 110 00000 to 110 11111 i.e., 192 to 223

Class D and Class E

- Class D addresses range from 224-239: 11100000-11101111.
- Class E addresses range from 240-254: 255 is a reserved address and is used for broadcasting purposes.

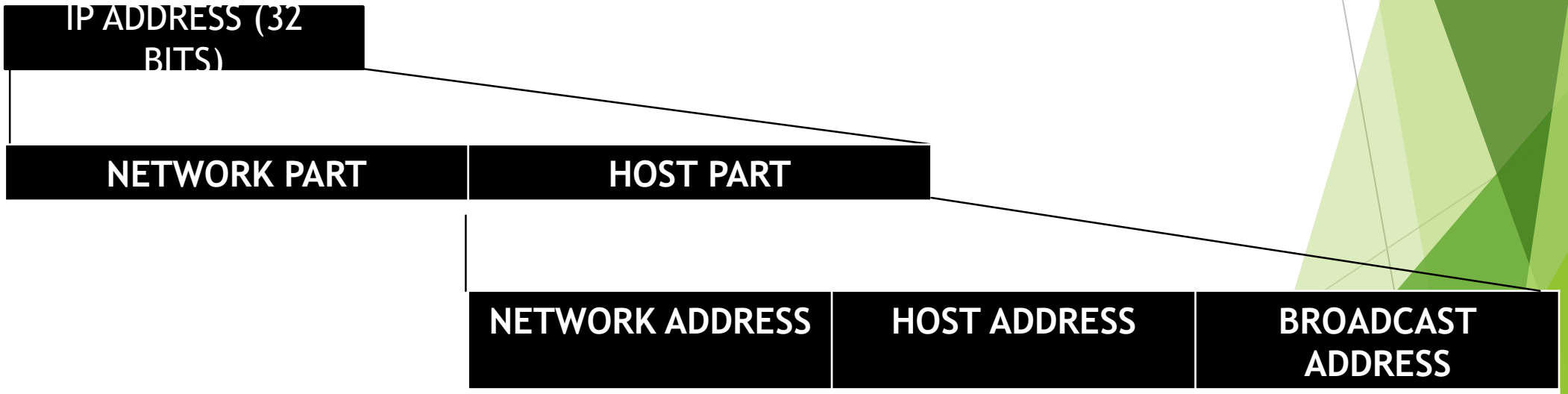
Private and Public Addresses

- When you are dealing with IP addresses, there are always two numbers reserved for a given network number: the first address in the network represents the network's address, and the last address in the network represents the broadcast address for this network, commonly called a directed broadcast.
- When you look at IP itself, there are two IP addresses reserved: 0.0.0.0 (the very first address), which represents all IP addresses, and 255.255.255.255 (the very last address), which is the local broadcast address (all devices should process this datagram).
- Within this range of addresses for Class A, B, and C addresses, there are some reserved addresses, commonly called Private Addresses. All the other addresses in these classes are called public addresses.

Remember the list of private networks, which cannot be used in public networks: 10.0.0.0, 172.16.0.0-172.31.0.0, and 192.168.0.0-192.168.255.0

IP Address Components

- Two components in IP addressing: network part and host part.
- The host portion is actually broken into three subcomponents: network address, host addresses, and directed broadcast address.



IP Address Components

- The very first address in a network number is called the network address, or wire number.
- The last address in the network number is called the directed broadcast address, and is used to represent all hosts on this network segment.
- Any address between the network address and the directed broadcast address is a host address for the segment.
- You use these middle addresses to assign to host devices on the segment, like PCs, servers, routers, and switches.

Class A Numbers

$2^1 = 2$	$2^9 = 512$	$2^{17} = 131,072$	$2^{25} = 33,554,432$
$2^2 = 4$	$2^{10} = 1,024$	$2^{18} = 262,144$	$2^{26} = 67,108,864$
$2^3 = 8$	$2^{11} = 2,048$	$2^{19} = 524,288$	$2^{27} = 134,217,728$
$2^4 = 16$	$2^{12} = 4,096$	$2^{20} = 1,048,576$	$2^{28} = 268,435,456$
$2^5 = 32$	$2^{13} = 8,192$	$2^{21} = 2,097,152$	$2^{29} = 536,870,912$
$2^6 = 64$	$2^{14} = 16,384$	$2^{22} = 4,194,304$	$2^{30} = 1,073,741,824$
$2^7 = 128$	$2^{15} = 32,768$	$2^{23} = 8,388,608$	$2^{31} = 2,147,483,648$
$2^8 = 256$	$2^{16} = 65,536$	$2^{24} = 16,777,216$	$2^{32} = 4,294,967,296$

- Number of Network Bits = 8 Bits (7 Bits) ➔ 2^7 Number of Networks
- i.e 127 Networks
- Number of Host Bits = 24 ➔ 2^{24} -2 Number of Hosts
- i.e 16,777,216 – 2 (16,777,214) Number of Hosts to each network

Class B Numbers

$2^1 = 2$	$2^9 = 512$	$2^{17} = 131,072$	$2^{25} = 33,554,432$
$2^2 = 4$	$2^{10} = 1,024$	$2^{18} = 262,144$	$2^{26} = 67,108,864$
$2^3 = 8$	$2^{11} = 2,048$	$2^{19} = 524,288$	$2^{27} = 134,217,728$
$2^4 = 16$	$2^{12} = 4,096$	$2^{20} = 1,048,576$	$2^{28} = 268,435,456$
$2^5 = 32$	$2^{13} = 8,192$	$2^{21} = 2,097,152$	$2^{29} = 536,870,912$
$2^6 = 64$	$2^{14} = 16,384$	$2^{22} = 4,194,304$	$2^{30} = 1,073,741,824$
$2^7 = 128$	$2^{15} = 32,768$	$2^{23} = 8,388,608$	$2^{31} = 2,147,483,648$
$2^8 = 256$	$2^{16} = 65,536$	$2^{24} = 16,777,216$	$2^{32} = 4,294,967,296$

- Number of Network Bits = 16 Bits (14 Bits) ➔ 2^{14} Number of Networks
- i.e 16,384 Networks
- Number of Host Bits = 16 ➔ 2^{16} -2 Number of Hosts
- i.e 65536 -2 (65534) Number of Hosts to each network

Class C Numbers

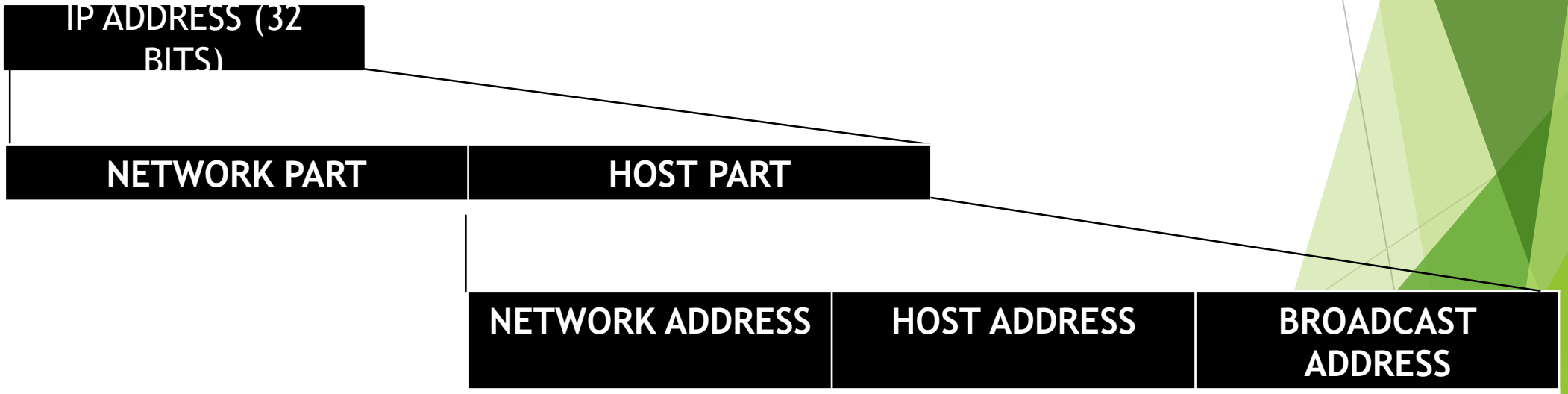
$2^1 = 2$	$2^9 = 512$	$2^{17} = 131,072$	$2^{25} = 33,554,432$
$2^2 = 4$	$2^{10} = 1,024$	$2^{18} = 262,144$	$2^{26} = 67,108,864$
$2^3 = 8$	$2^{11} = 2,048$	$2^{19} = 524,288$	$2^{27} = 134,217,728$
$2^4 = 16$	$2^{12} = 4,096$	$2^{20} = 1,048,576$	$2^{28} = 268,435,456$
$2^5 = 32$	$2^{13} = 8,192$	$2^{21} = 2,097,152$	$2^{29} = 536,870,912$
$2^6 = 64$	$2^{14} = 16,384$	$2^{22} = 4,194,304$	$2^{30} = 1,073,741,824$
$2^7 = 128$	$2^{15} = 32,768$	$2^{23} = 8,388,608$	$2^{31} = 2,147,483,648$
$2^8 = 256$	$2^{16} = 65,536$	$2^{24} = 16,777,216$	$2^{32} = 4,294,967,296$

- Number of Network Bits = 24 Bits (21 Bits) ➔ 2^{21} Number of Networks
- i.e 2,097,152 Networks
- Number of Host Bits = 8 ➔ 2^8 -2 Number of Hosts
- i.e 256 -2 (254) Number of Hosts to each network

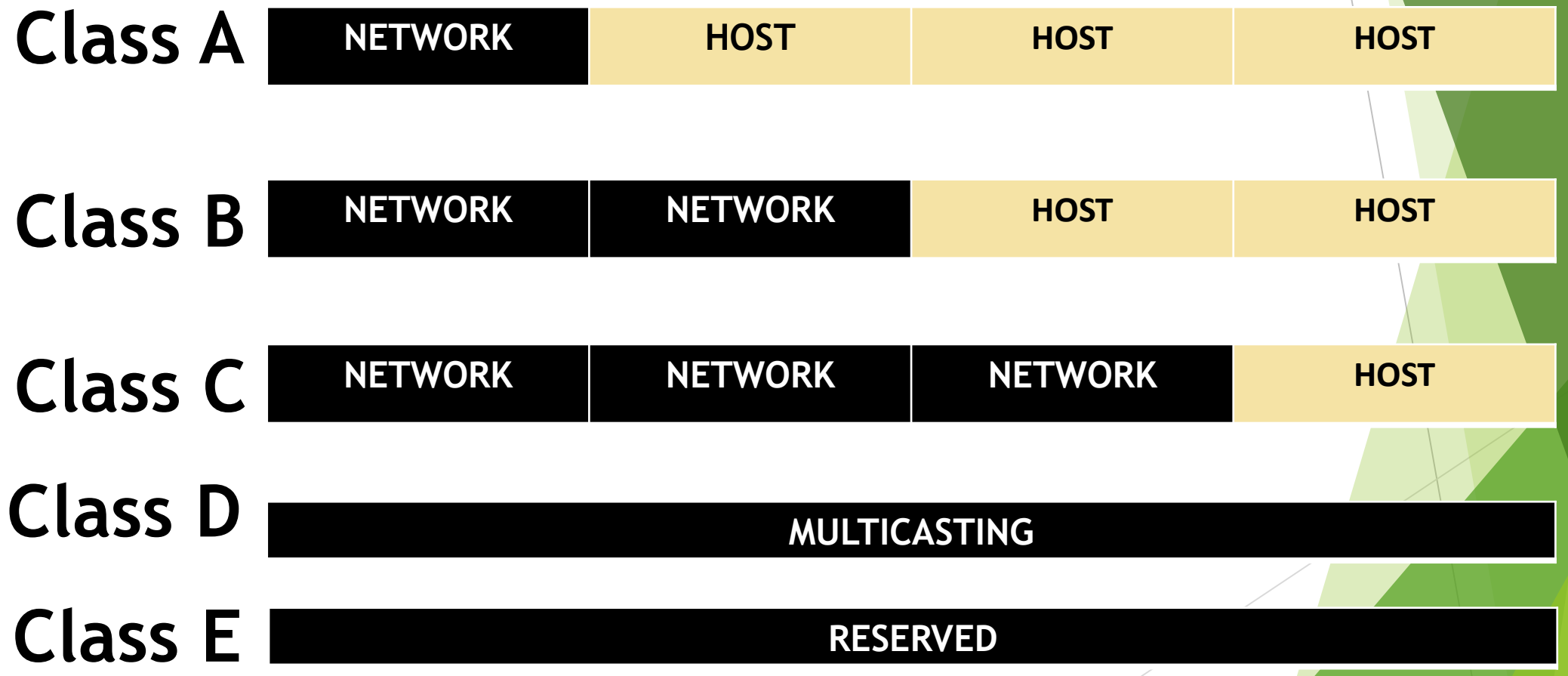
SUBNETTING

IP Address Components

- Two components in IP addressing: network part and host part.
- The host portion is actually broken into three subcomponents: network address, host addresses, and directed broadcast address.



Classes of Addresses



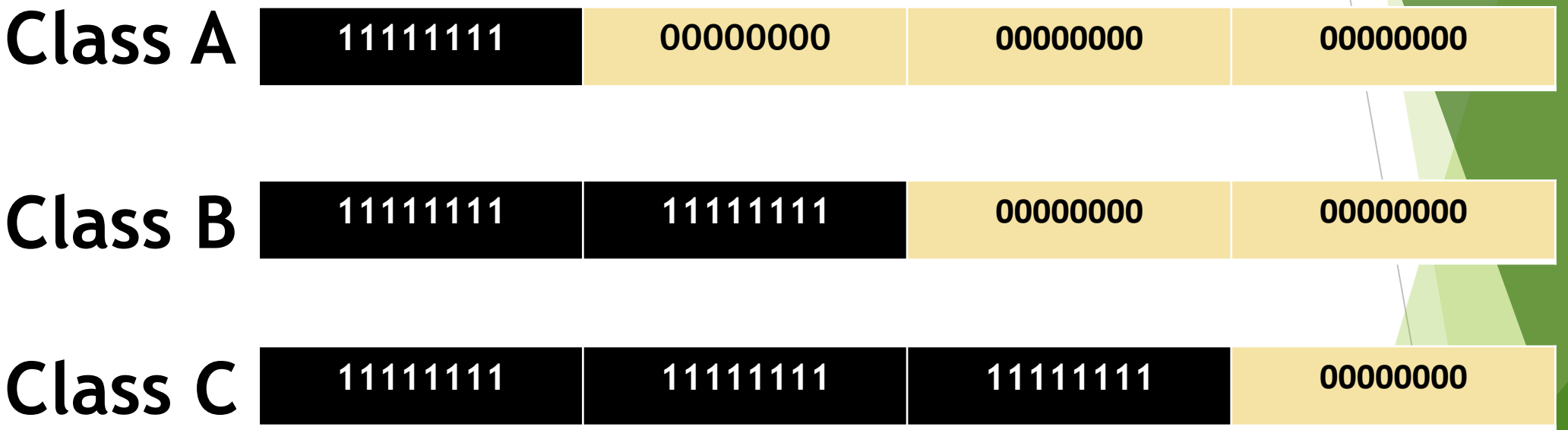
Subnet Mask

Subnet mask values, binary 1s and 0s, must be contiguous in order to be considered as a valid subnet mask.

When representing subnet masks, be very familiar with both the dotted decimal and number of networking bits nomenclature.

- There are actually three components to the address:
  - Network component
  - Host component
  - Subnet mask
- The function of the subnet mask is to differentiate between the network address, the host addresses, and the directed broadcast address.
- Like an IP address, the subnet mask is 32 bits long.
- In binary, a 1 in a bit position in the subnet mask represents a network component and a 0 in a bit position represents a host component.
- One restriction of subnet masks is that all the network bits (1s) must be contiguous and all the host bits (0s) are contiguous.

Default Subnet Masks



ADDRESSING EFFICIENCY ISSUES

Required Number of Hosts = 500

Prefer Class C?		
	0.0.0	.0
Networ Addr		
Broa Addre		55
Usable Addresses	68. to 192.168.0.254	192.168.1.1 to 192.168.1.254

2 Blocks needed in Class B

Prefer Class B?	
	1
Networ	
Broa addr	
Usable Addresses	0.1. to 128.0.255.254

65000 Addresses to be Wasted in Class B

SUBNETTING

- Subnetting allows you to take some of the higher-order host bits in a network number and use them to create more networks.
- In the process of creating more networks, each of these additional networks has a lesser number of hosts.
- These smaller networks are commonly called subnets.

Planning IP Addressing with Subnetting

1. Figure out network and host requirements
2. Satisfy host and network requirements
3. Figure out the subnet mask
4. Figure out the network addresses
5. Figure out the directed broadcasts for your networks
6. Figure out the host values for your networks

IP Addressing Exercise 1

- You are given a Class B network (172.16.0.0) and you have 490 segments in your network, where the largest segment needs 112 host addresses. What subnet mask should you use and what is the layout of your addresses?

IP Addressing Exercise 2

- You are given a Class A network (10.0.0.0) and you have 9,000 segments in your network, where the largest segment needs 560 host addresses. What subnet mask should you use and what is the layout of your addresses?

Architectural Facets of Networking

Architectures

- Network routing must account for each of the following architectural components.
- Some aspects of the architectures listed below are critical to routing issues:
  - Service Architecture
  - Protocol Stack Architecture
  - Router Architecture
  - Network Topology Architecture
  - Network Management Architecture

Service Architecture

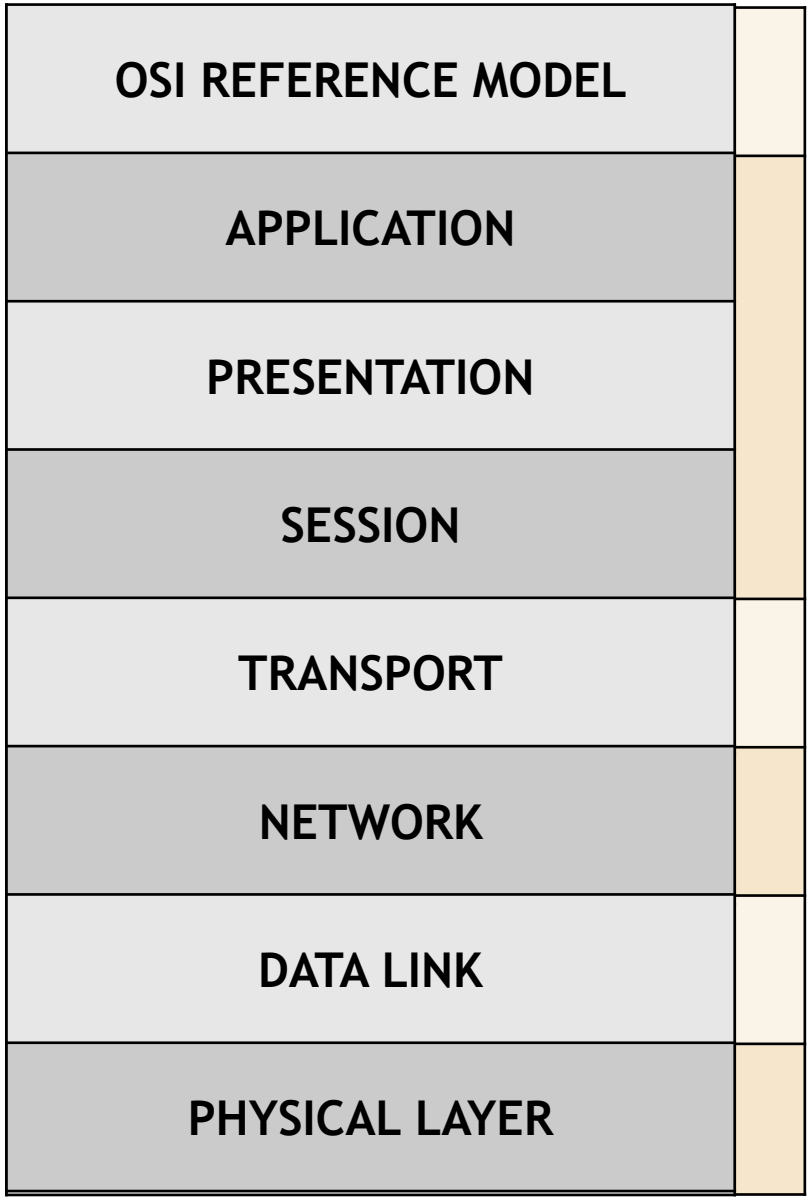
- An important aspect of a networking architecture is its service architecture.
- The service architecture depends partly also on the communication paradigm of its information units.
- Every networking environment has a service architecture, much like the postal delivery system.
- In the following, we focus on discussing three service models associated with IP networks.
  - BEST-EFFORT SERVICE ARCHITECTURE
  - INTEGRATED SERVICES ARCHITECTURE
  - DIFFERENTIATED SERVICES ARCHITECTURE

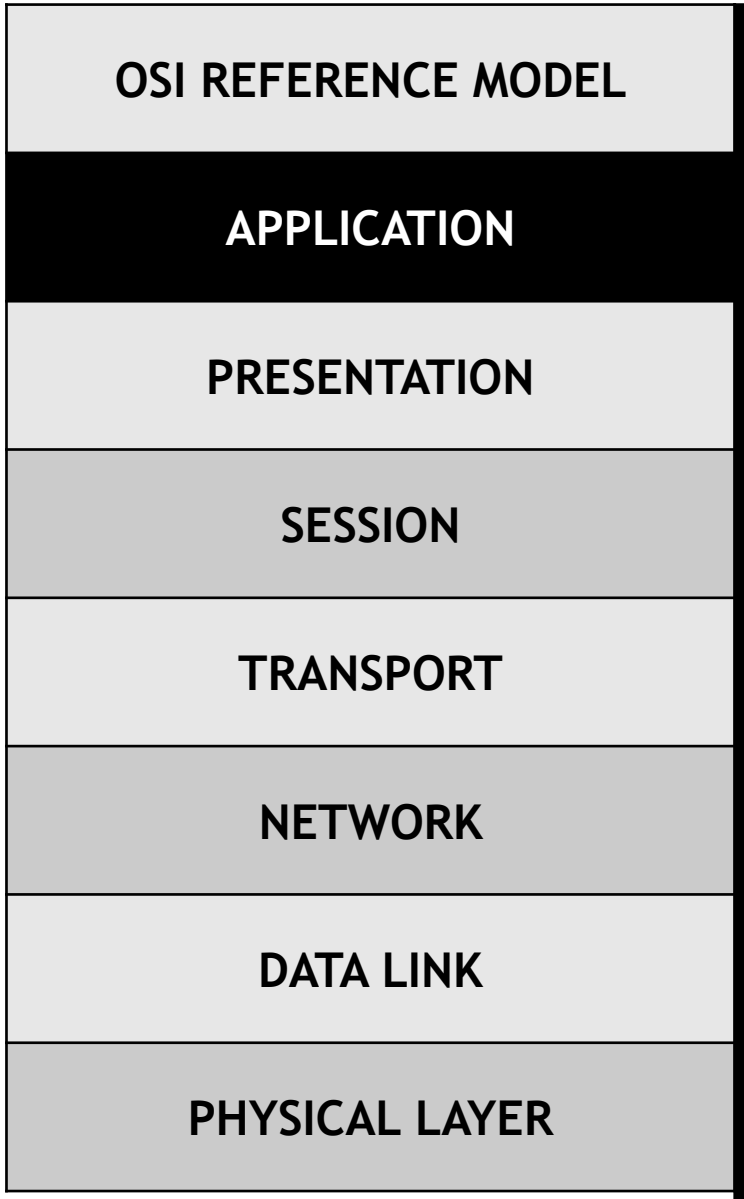
Service Architecture

- BEST-EFFORT SERVICE ARCHITECTURE
  - At the IP level, the packet forwarding function is provided without worrying about reliable delivery; in a sense, IP makes its best effort to deliver packets.
  - Because of this, the IP service paradigm is referred to as the best-effort service.
- INTEGRATED SERVICES ARCHITECTURE
  - The concept for integrated services (“int-serv”) architecture was developed in the early 1990s to allow functionalities for services that are real-time, interactive, and that can tolerate some loss, but require a bound on the delay.
  - Furthermore, each session or connection requires a well-defined bandwidth guarantee and a dedicated path.
  - For example, interactive voice and multimedia applications fall into this category.
- DIFFERENTIATED SERVICES ARCHITECTURE
  - The differentiated services (“diff-serv”) architecture was developed to provide prioritized service mechanisms without requiring connection-level information to be maintained at routers.
  - Specifically, this approach gives priority to services by marking IP packets with diffserv code points located in the IP header.

PROTOCOL STACK ARCHITECTURE
OSI REFERENCE MODEL

OSI REFERENCE MODEL
APPLICATION
PRESENTATION
SESSION
TRANSPORT
NETWORK
DATA LINK
PHYSICAL LAYER

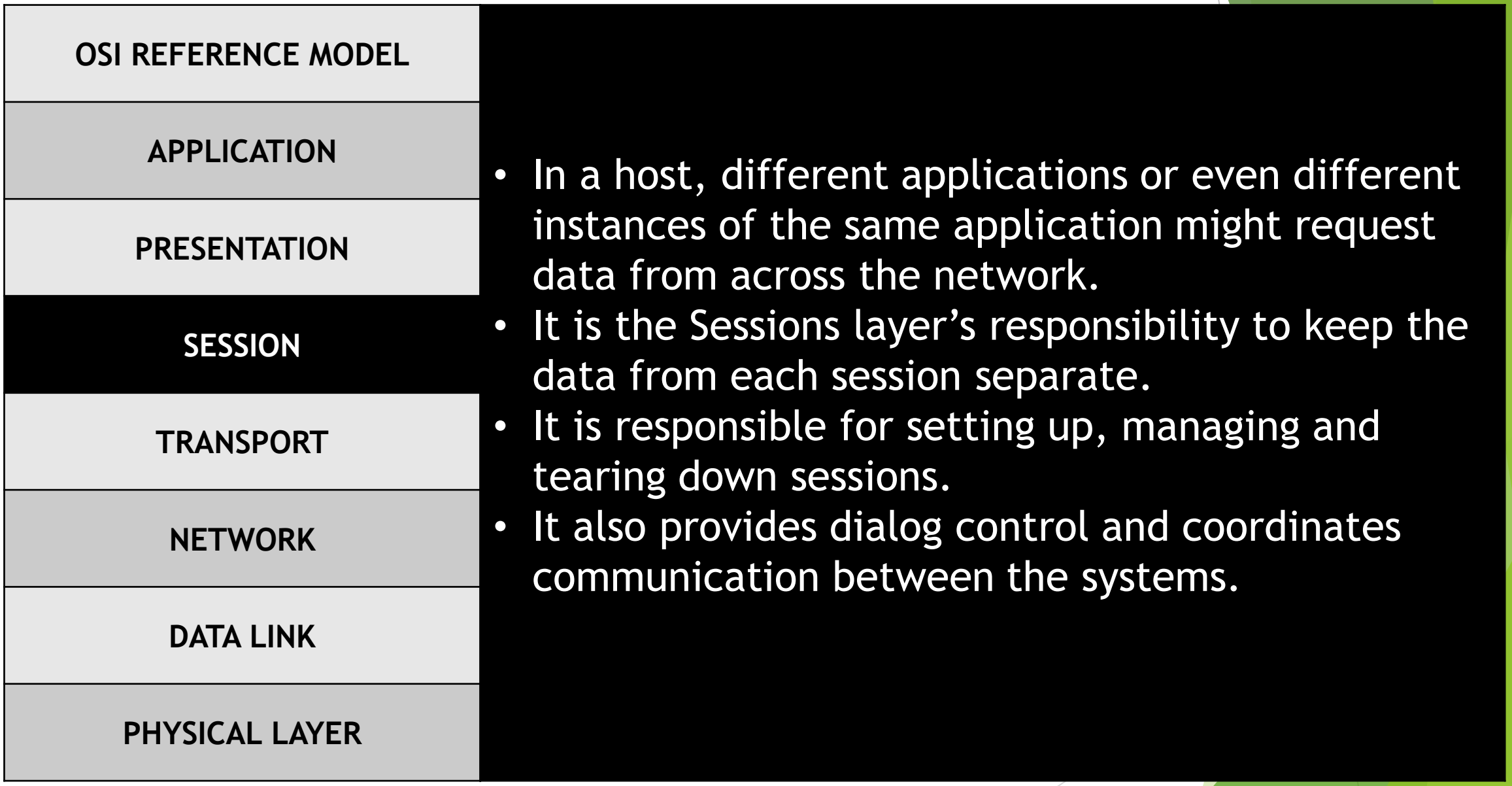

OSI REFERENCE MODEL
APPLICATION
PRESENTATION
SESSION
TRANSPORT
NETWORK
DATA LINK
PHYSICAL LAYER

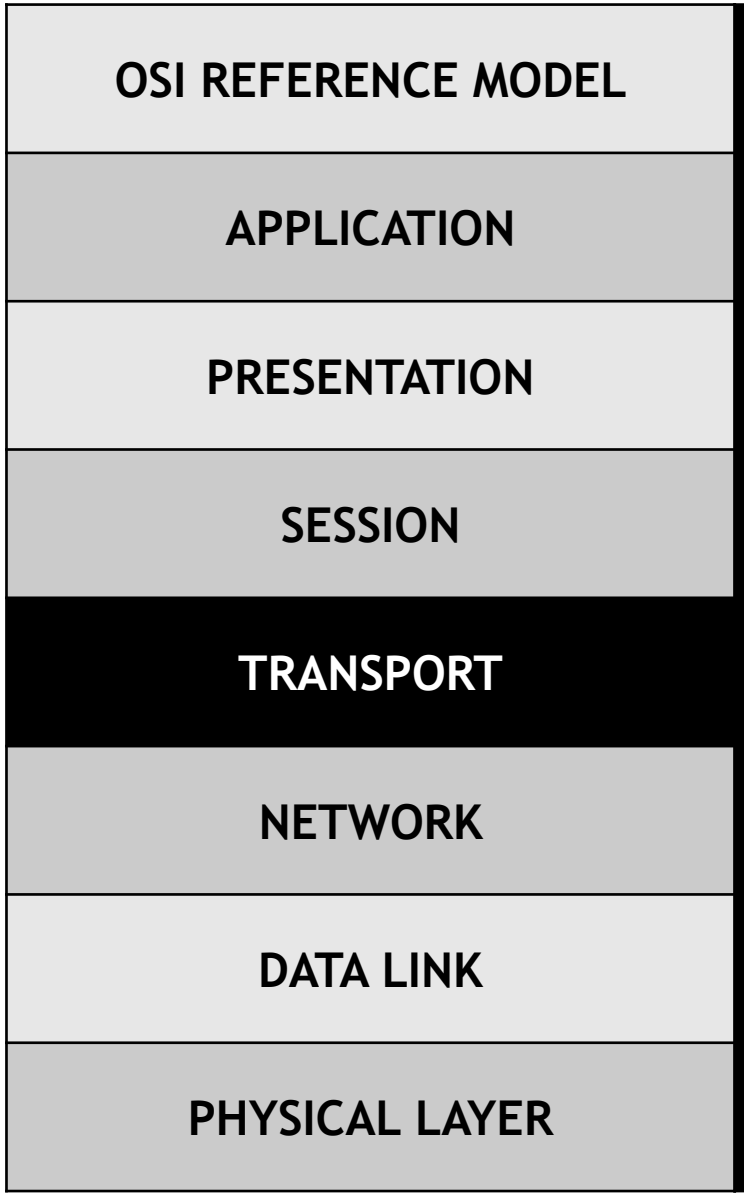


- The Application Layer provides the interface between the software application on a system and the network.
- Web Browser such as Internet Explorer or Firefox is the application.
- When it needs to fetch a webpage, it uses the **HTTP** protocol to send the request and receive the page contents.
- This protocol resides at the application layer and can be used by an application such as IE or FF to get webpages from web servers across the network.
- On the other side, the web server application such as Apache or IIS interacts with the HTTP protocol on the Application layer to receive the HTTP request and send the response back.

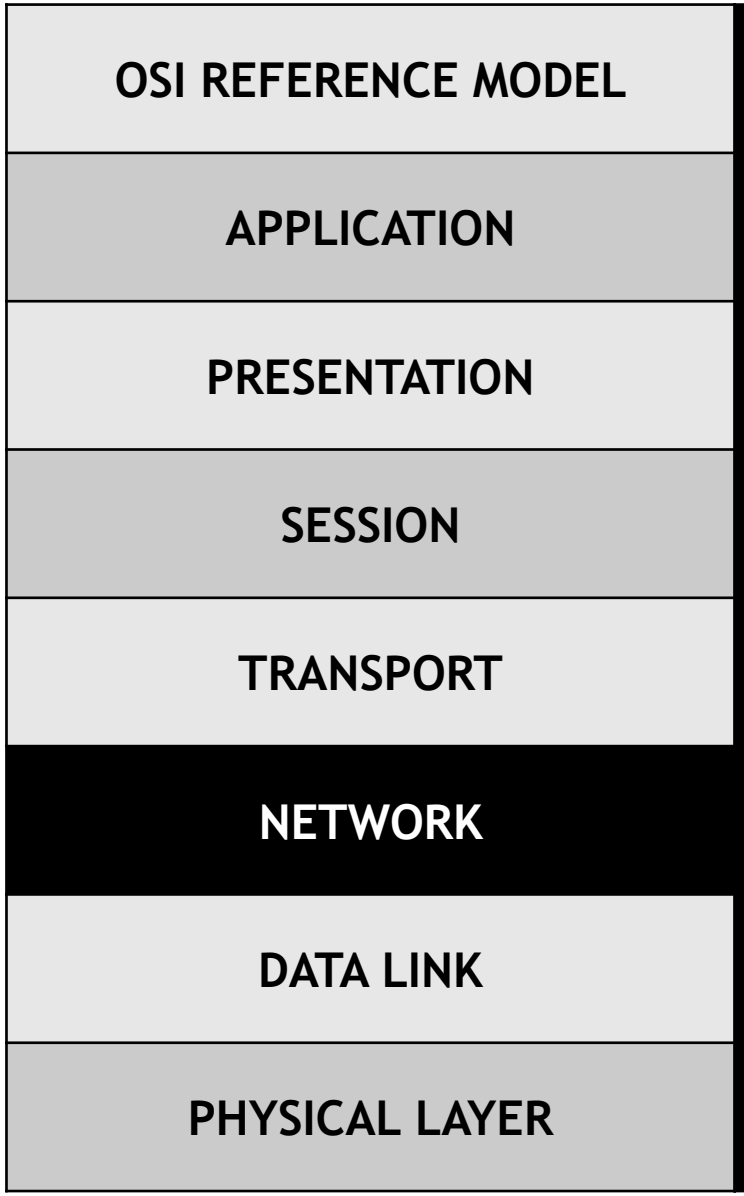
OSI REFERENCE MODEL
APPLICATION
PRESENTATION
SESSION
TRANSPORT
NETWORK
DATA LINK
PHYSICAL LAYER

- The Presentation Layer is responsible for data translation and encoding.
- It will take the data from the Application layer and translate it into a generic format for transfer across the network.
- At the receiving end the Presentation layer takes in generically formatted data and translates into the format recognized by the Application layer.
- An example of this is an **EBCDIC** to **ASCII** translation.
- The OSI model has protocol standards that define how data should be formatted.
- This layer is also involved in data compression, decompression, encryption, and decryption.

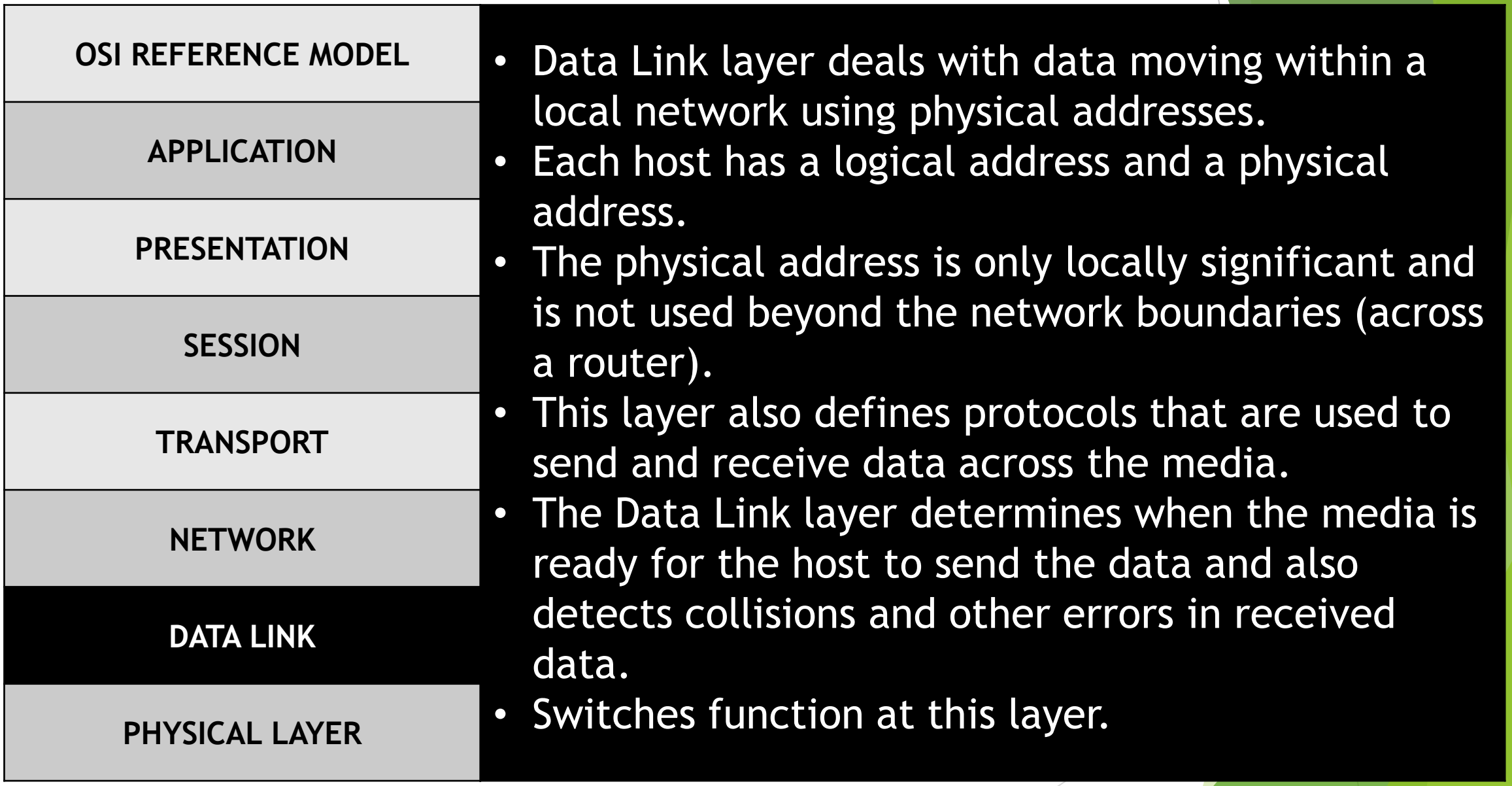

OSI REFERENCE MODEL
APPLICATION
PRESENTATION
SESSION
TRANSPORT
NETWORK
DATA LINK
PHYSICAL LAYER
• In a host, different applications or even different instances of the same application might request data from across the network.
• It is the Sessions layer's responsibility to keep the data from each session separate.
• It is responsible for setting up, managing and tearing down sessions.
• It also provides dialog control and coordinates communication between the systems.



- Where the upper layers are related to applications and data within the host, the transport layer is concerned with the actual end-to-end transfer of the data across the network.
- This layer establishes a logical connection between the two communicating hosts and provides reliable or unreliable data delivery and can provide flow control and error recovery.
- Although not developed under the OSI Reference Model and not strictly conforming to the OSI definition of the Transport Layer, typical examples of Layer 4 are the **Transmission Control Protocol (TCP)** and **User Datagram Protocol (UDP)**.



- Three functions – logical addressing, path determination and forwarding – are done at the Network Layer.
- Two types of protocols are used for these functions – **routed protocols** are used for logical addressing and forwarding while **routing protocols** are used for path determinations.
- Routers function at this layer. Remember that routers only care about the destination network. They do not care about the destination host itself.
- The task of delivery to the destination host lies on the Data Link Layer.


OSI REFERENCE MODEL
APPLICATION
PRESENTATION
SESSION
TRANSPORT
NETWORK
DATA LINK
PHYSICAL LAYER
• Data Link layer deals with data moving within a local network using physical addresses.
• Each host has a logical address and a physical address.
• The physical address is only locally significant and is not used beyond the network boundaries (across a router).
• This layer also defines protocols that are used to send and receive data across the media.
• The Data Link layer determines when the media is ready for the host to send the data and also detects collisions and other errors in received data.
• Switches function at this layer.

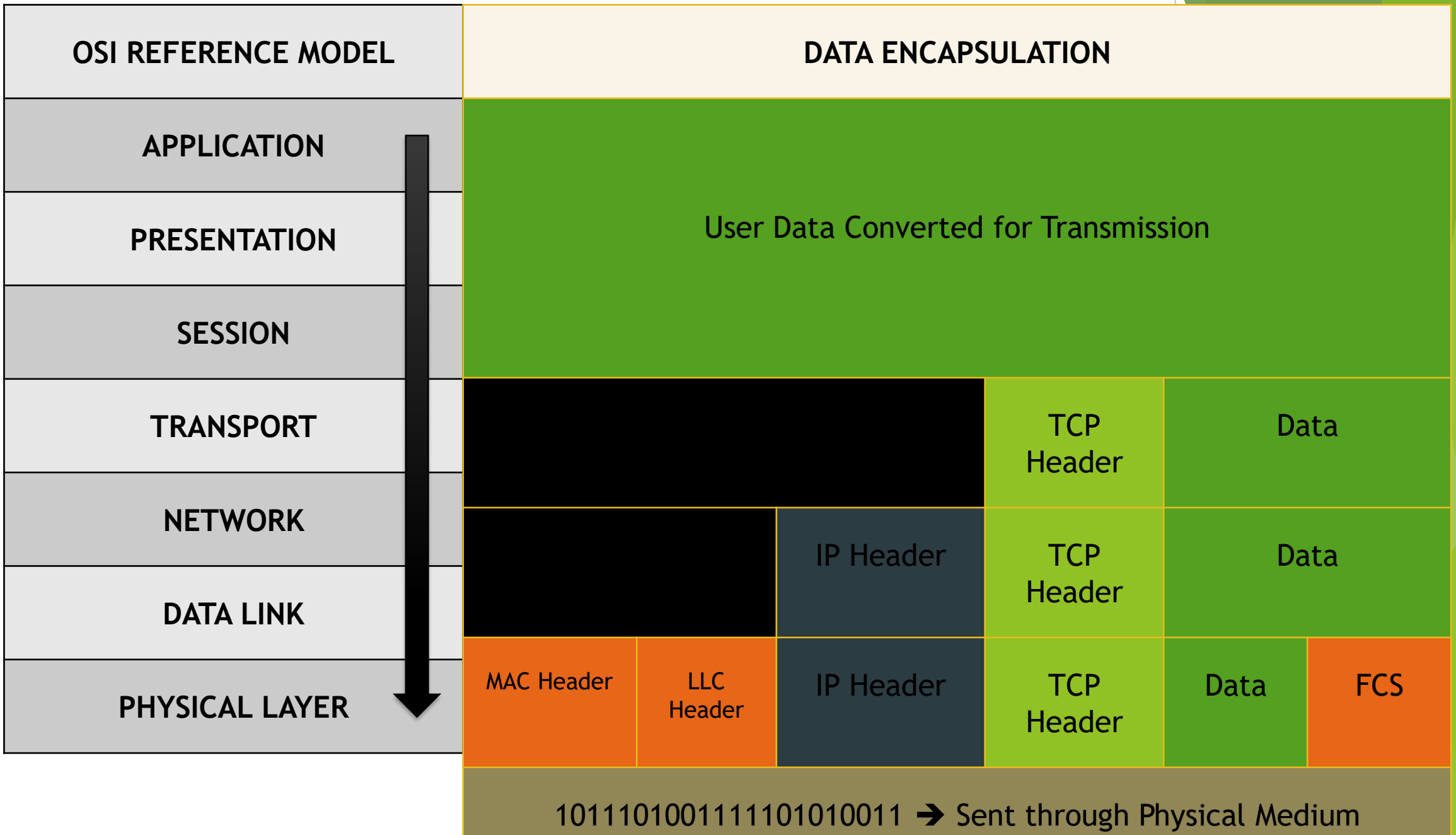
OSI REFERENCE MODEL
APPLICATION
PRESENTATION
SESSION
TRANSPORT
NETWORK
DATA LINK
PHYSICAL LAYER

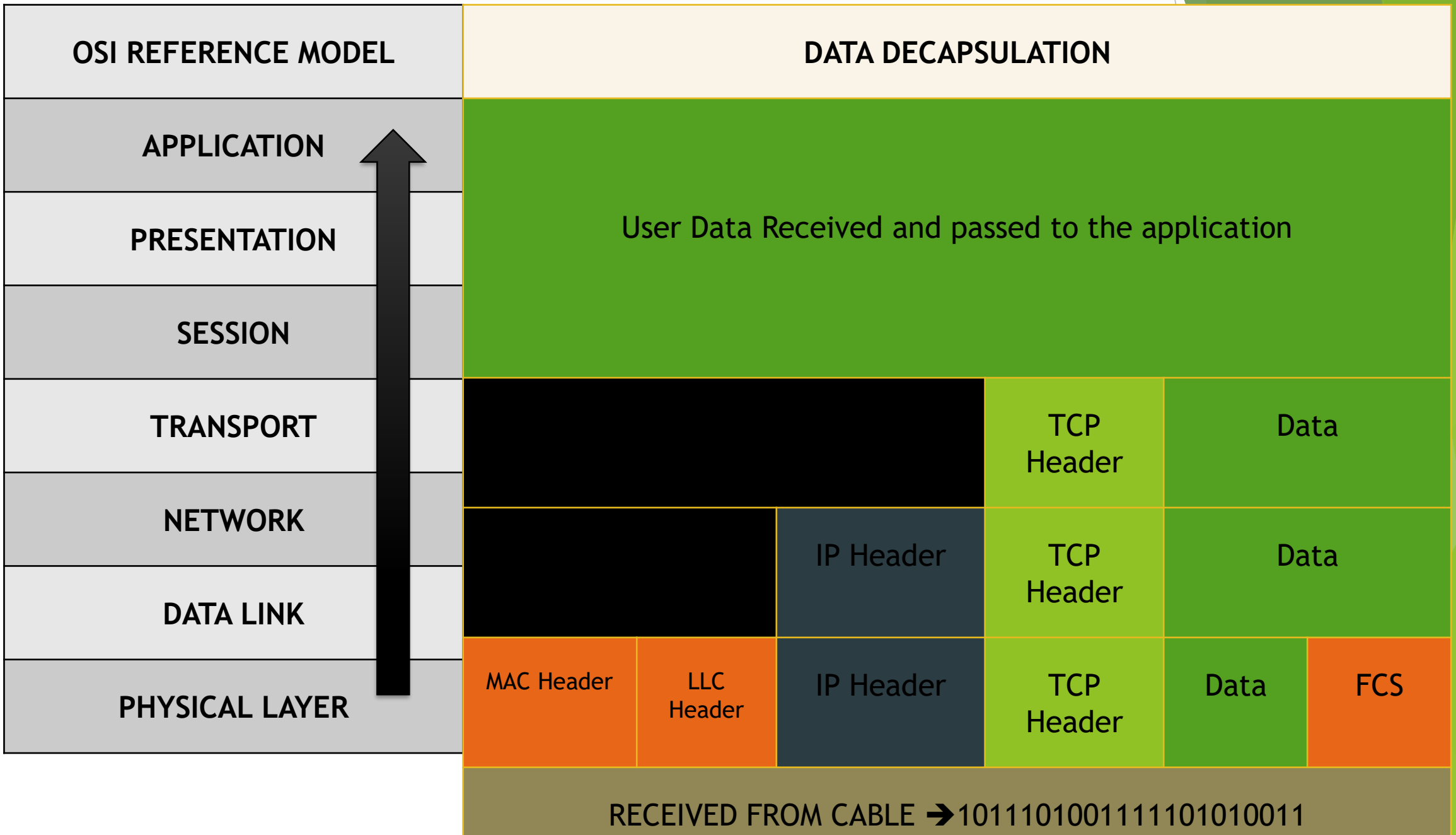
- This layer deals with the physical transmission medium itself.
- It activates, maintains and deactivates the physical link between systems (host and switch for example).
- This is where the connectors, pin-outs, cables, electrical currents etc. are defined.
- Essentially this layer puts the data on the physical media as bits and receives it in the same way.
- Hubs work at this layer.

OSI REFERENCE MODEL	FUNCTIONS
APPLICATION	Network Virtual Terminal, File transfer access and management, Mail Services, Directory Services
PRESENTATION	Translation, Encryption/ Decryption and Compression
SESSION	Session establishment, maintenance and termination, Dialog Control
TRANSPORT	Segmentation, Flow Control and Error Control, Service Point Addressing
NETWORK	Routing and Logical Addressing
DATA LINK	Framing, Physical addressing, Error control, Flow Control, Access control
PHYSICAL LAYER	Bit synchronization, Bit rate control, Physical topologies, Transmission mode

OSI REFERENCE MODEL	Components
APPLICATION	Computers, Servers, IP Phones, Smartphones and all the end devices
PRESENTATION	
SESSION	
TRANSPORT	Firewalls
NETWORK	Routers
DATA LINK	Switches, Access Points
PHYSICAL LAYER	Hubs, Cables and Patch Panels

OSI REFERENCE MODEL	Protocols
APPLICATION	HTTP, DNS, DHCP, Telnet, SMTP, POP, SIP
PRESENTATION	
SESSION	
TRANSPORT	TCP, UDP
NETWORK	IP, ARP, ICMP ,IPSec, OSPF, EIGRP
DATA LINK	PPP, CSMA and MAC Protocols, Ethernet (IEEE 802.3), 802.11
PHYSICAL LAYER	


OSI REFERENCE MODEL
DATA ENCAPSULATION
APPLICATION
PRESENTATION
SESSION
TRANSPORT
NETWORK
DATA LINK
PHYSICAL LAYER
User Data Converted for Transmission
TCP Header
Data
IP Header
TCP Header
Data
MAC Header
LLC Header
IP Header
TCP Header
Data
FCS
10111010011111010010011 ➔ Sent through Physical Medium


OSI REFERENCE MODEL
DATA DECAPSULATION
APPLICATION
PRESENTATION
SESSION
TRANSPORT
NETWORK
DATA LINK
PHYSICAL LAYER
User Data Received and passed to the application
TCP Header
Data
IP Header
TCP Header
Data
MAC Header
LLC Header
IP Header
TCP Header
Data
FCS
RECEIVED FROM CABLE ➔10111010011111010010011

IP Protocol Stack Architecture

- The IP architectural model can be classified into the following layers: the network interface, the IP layer, the transport layer, and the application layer.
- We can easily see that it does not exactly map into the seven-layer OSI reference model.
- Actual applications are considered on the top of the application layer, although the IP model does not strictly follow layering boundaries as in the OSI reference model

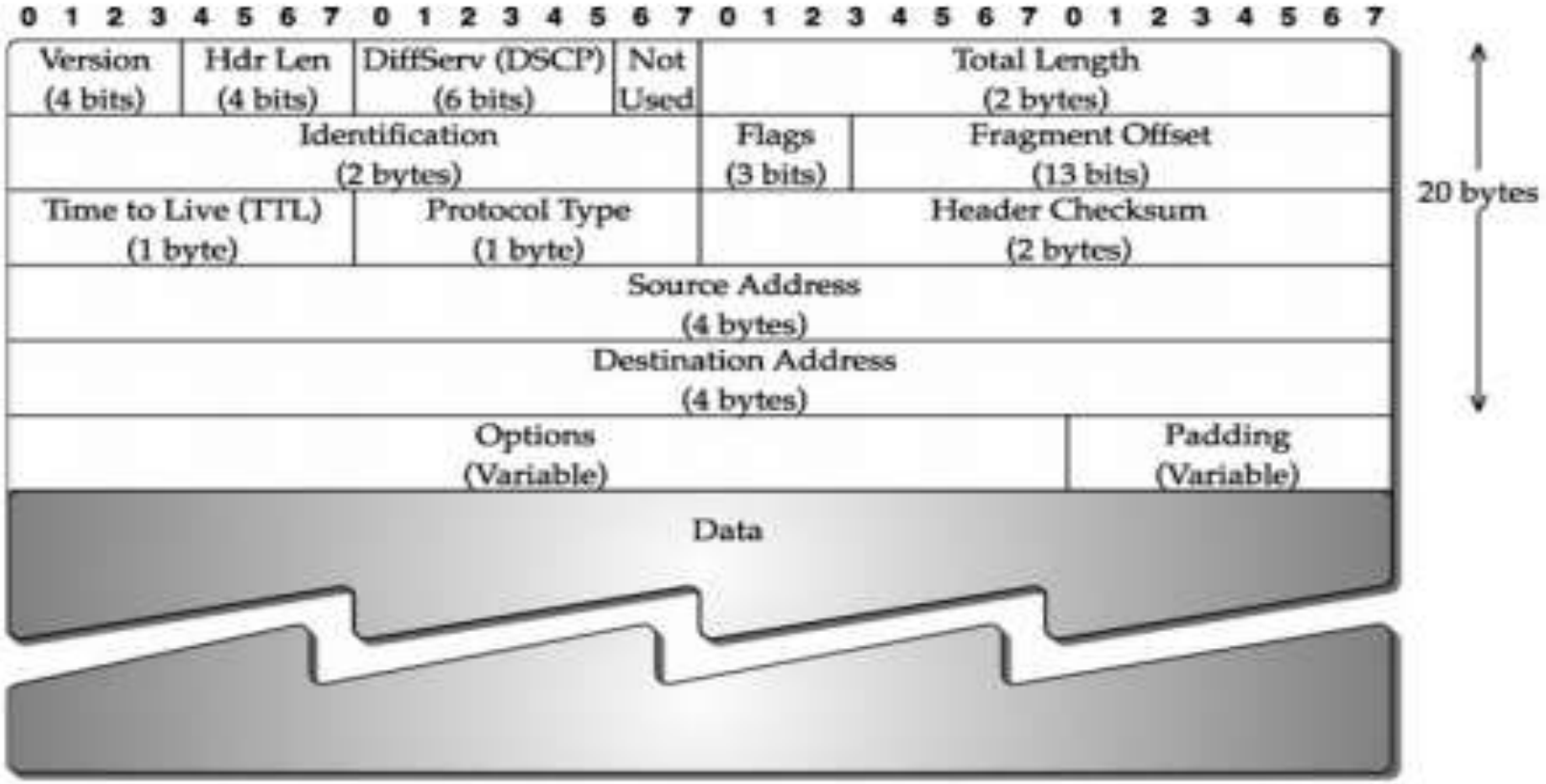
NETWORK AND TRANSPORT LAYER

- The IP addressing is defined at the IP layer, where the delivery mode is assumed to be unreliable.
- The transport layer that is above the IP layer provides transport services, which can be either reliable or unreliable.
- More important, the transport layer provides another form of addressing, commonly known as the port number. Port numbers are 16 bits long
- Both TCP and UDP are above IP, a field in the IP header, known as the protocol type field, is used to be able to distinguish them.
- That is, through five pieces of information consisting of the source and the destination IP addresses, the source and the destination port numbers, and the transport protocol type, a connection in the Internet can be uniquely defined. This is also known as a microflow

IP

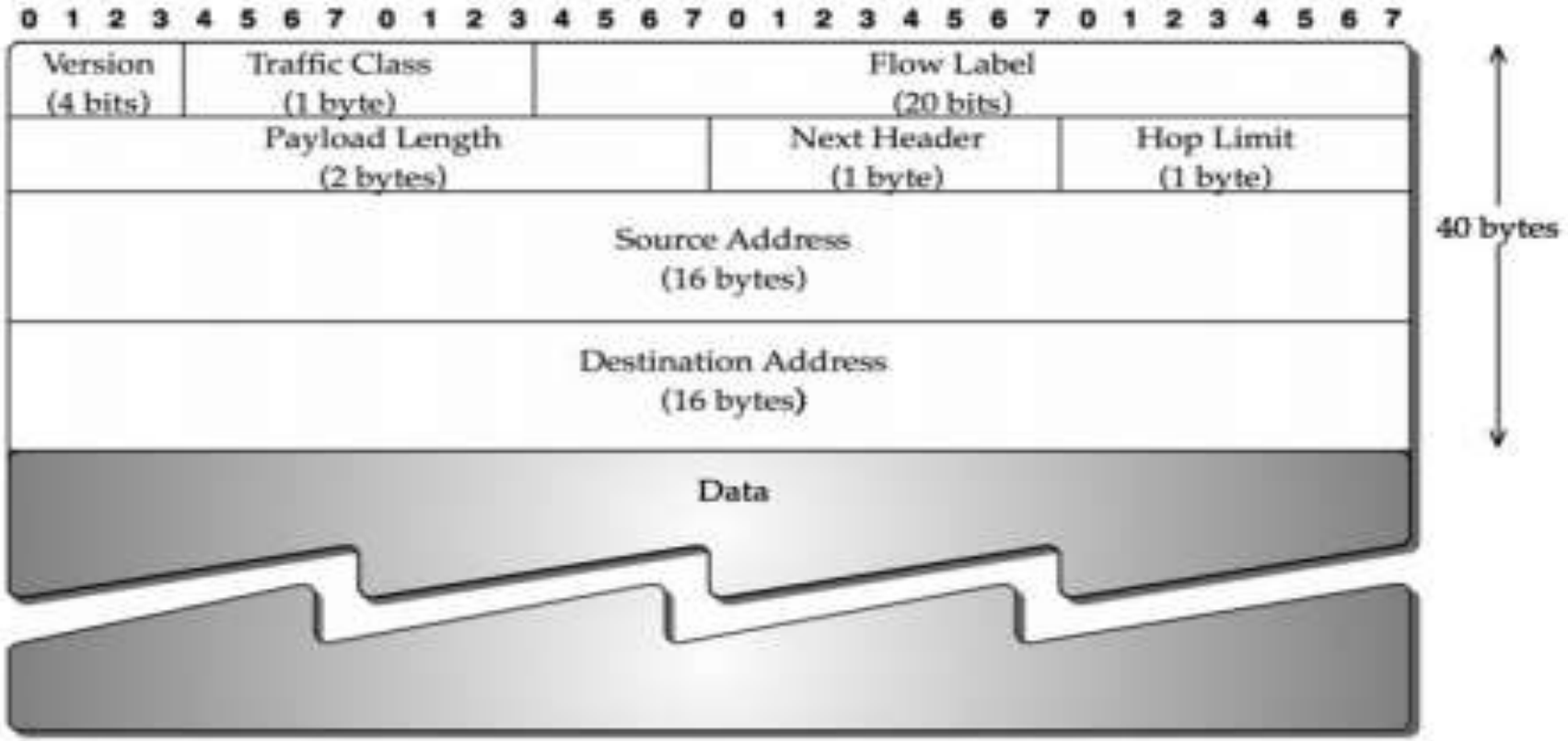
- Defines a uniform mechanism to access resources between internets
  - Enables networking across networks that are not connected at level 2 (data-link).
  - Defines IP addresses and how to route network packets to a destination address.
- IP v.4, addresses: 4 octets, organized hierarchically
  - Single host: 128.220.23.4 or 192.168.33.1
  - Class C network: 128.220.23.x, also written 128.220.23.0/24
  - Class B network: 192.168.x.x., also written 192.168.0.0/16
  - Class A network: 10.x.x.x, or 10.0.0.0/8

IPv4 Packet Format



(a) IPv4 packet

IPv6 Packet Format

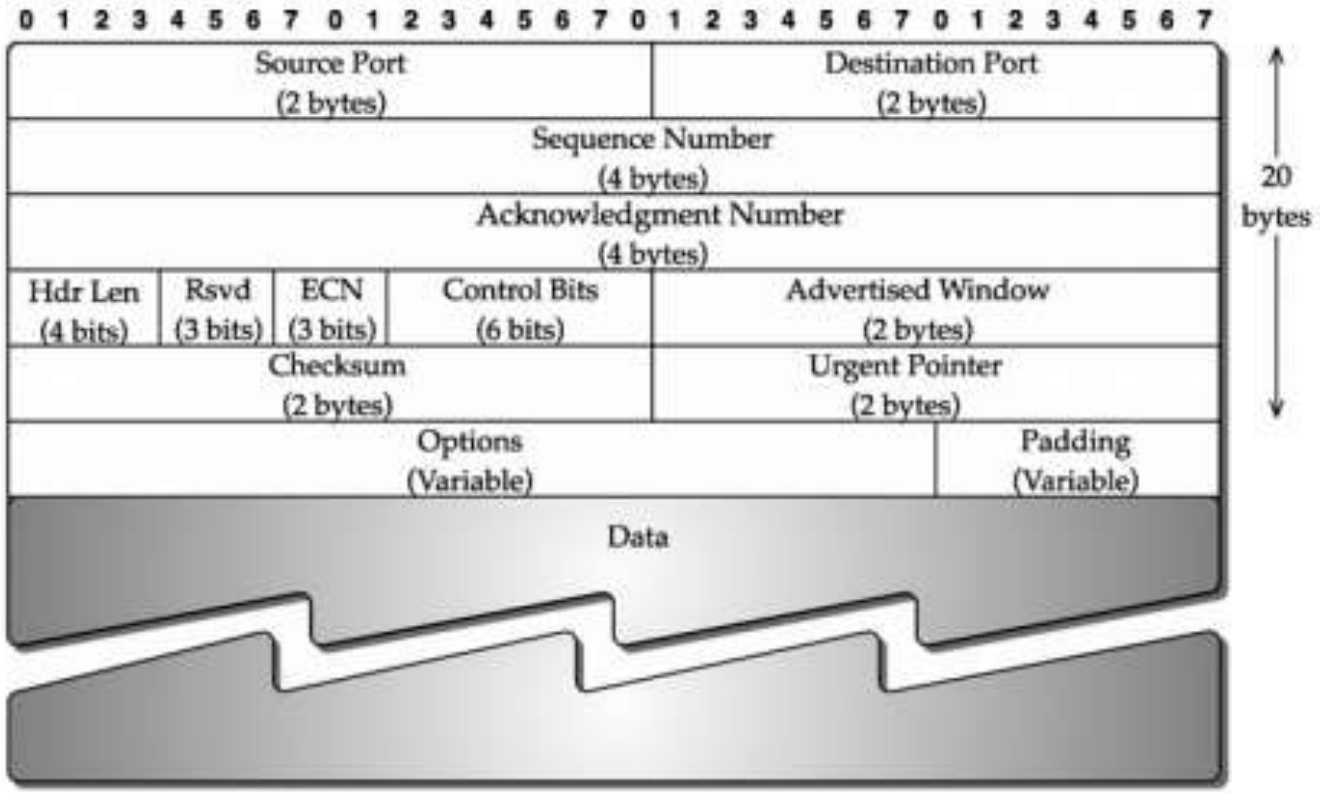


(b) IPv6 packet

TCP / UDP

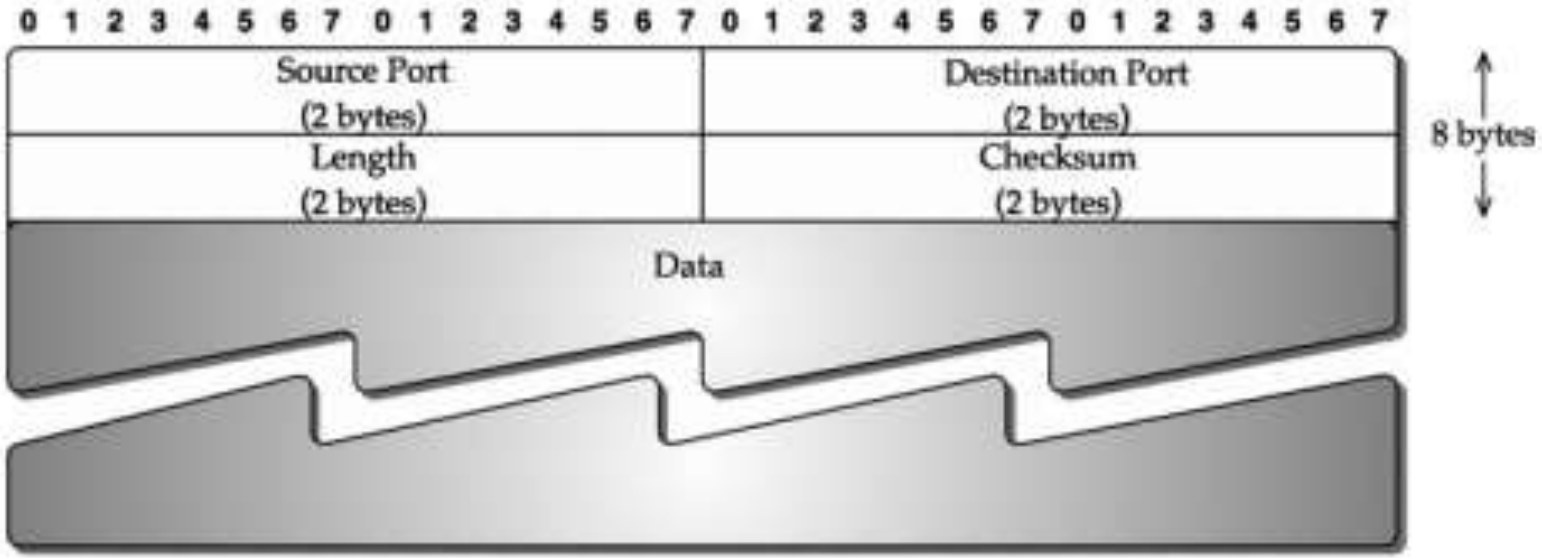
- Layer 4 (transport layer) protocols, run over IP
  - TCP and UDP packets are encapsulated into IP packets
- Use their own control information, stored in packet headers
  - Port numbers (indicate consuming program in the destination host)
- TCP is connection-oriented, and provides for reliable, order-preserving transmission of data
- UDP is not connection-oriented, does not guarantee data arrival, or proper ordering of arriving data

TCP Packet Format



(a) TCP packet

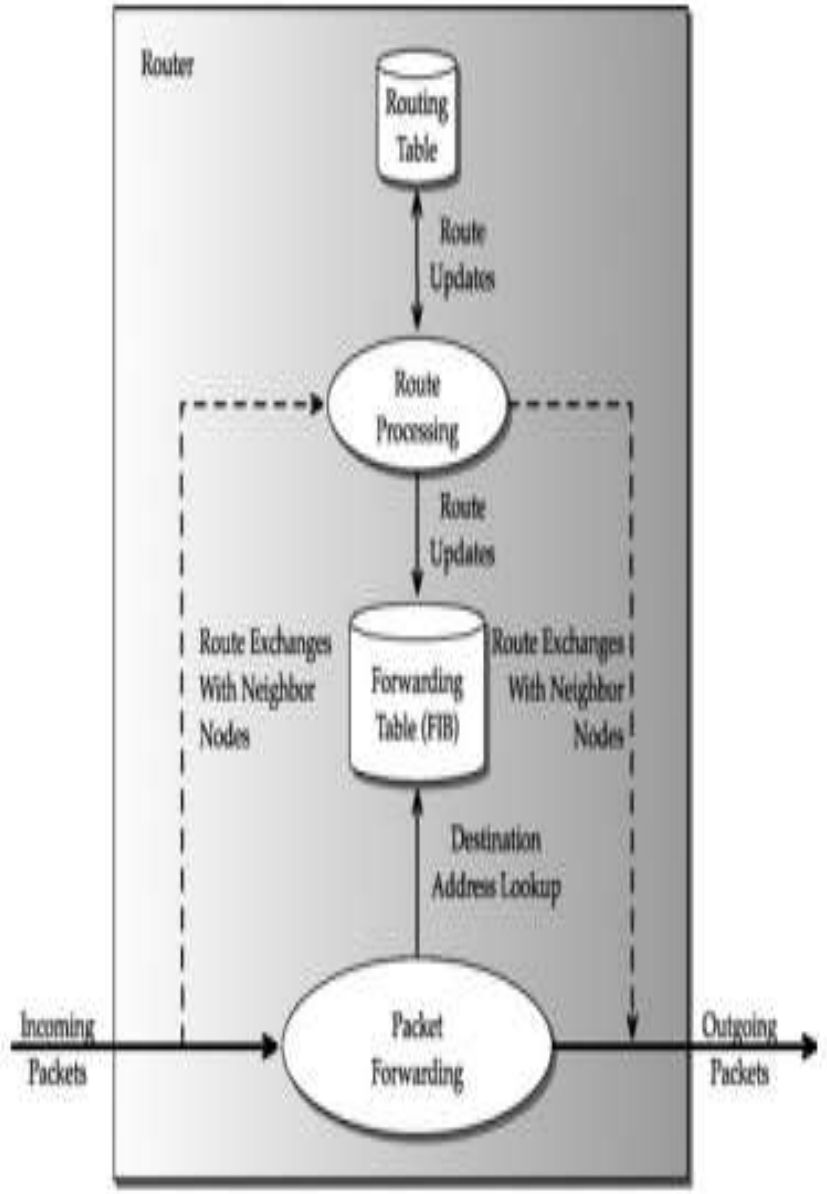
UDP Packet Format



(b) UDP packet

Router Architecture

- A router provides several important functions in order to ensure proper packet forwarding, and to do so in an efficient manner. A router is a specialized computer that handles three primary functions:
  - Packet Forwarding
  - Routing Protocol Message Processing
  - Specialized Services



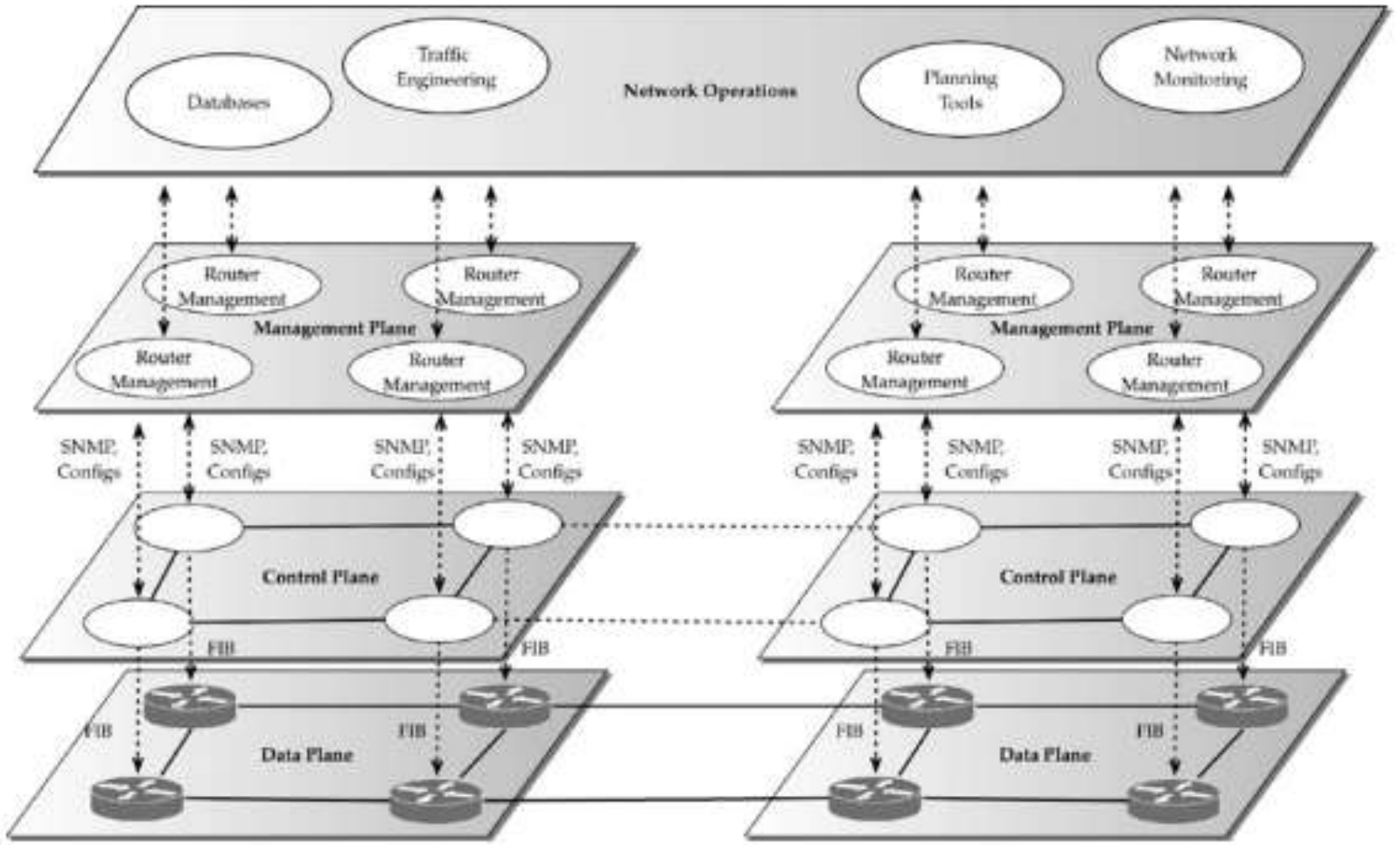
Router architecture: a functional view.

Network Topology Architecture

- The network topology architecture encompasses how a network is to be architected in an operational environment while accounting for future growth.
- The topological architecture then covers architecting a network topology that factors in economic issues, different technological capabilities, and limitations of devices to carry a certain volume of expected traffic and types of traffic, for an operational environment.
- Certainly, a network topology architecture needs to take into account routing capability, including any limitation or flexibility provided by a routing protocol.
- It is up to a network provider, also referred to as a network operator or a service provider, to determine the best topological architecture for the network.

Network Management Architecture

- For an operational network, it is important to have a network management architecture where various functions can be divided into “planes.”
- Specifically, we consider three different planes: the management plane, the control plane, and the data plane.
- The management plane addresses router configuration and collection of various statistics, such as packet throughput, on a link.
- The control plane exchanges control information between routers for management of a variety of functions, such as setting up a virtual link.
- The control plane is also involved in identifying the path to be taken between the endpoints of this virtual link, which relies on the routing information exchange.
- Routing-related functions are in the control plane, and the data transfers, such as the web or email, are in the data plane.



Network management architecture: data plane, control plane, and management plane.

Public Switched Telephone Network

- An information unit in the PSTN is a call.
- The PSTN has a global addressing scheme to uniquely identify an end device; an end device is commonly referred to as a telephone, while a more generic term is customer premise equipment (CPE).
- The global addressing scheme is known as E.164 addressing.
- It is a hierarchical addressing scheme that identifies the country code at the top level followed by the city or area code, and finally the number assigned to a subscriber.
- Nodes in the PSTN are called switches, which are connected by intermachine trunks (IMTs), also known as trunkgroups.
- From a protocol architecture point of view, and using the OSI reference model, PSTN can be simply summed up as consisting of application layer, network layer, and physical layer.

Communication Technologies

- Communication technologies provide transport services for both the Internet and PSTN.
- Note that the use of the term transport services is not to be confused with the term transport layer of the OSI reference model
- To provide transport services using communication technologies, a variety of transport network routing problems arises that need to take into account the capability of a particular communication technology and the “routing” device.
- Second, multilayered networking and multilayered routing can also be envisioned going from layer 3 down to layer 1 due to transport network routing.
- Third, new technologies for transport networking are being continually developed with new capabilities, creating new opportunities in transport network routing.
- Finally, traditionally, different transport networks had very little capability to communicate with each other and thus relied on manual configurations

Standards Committees

- There are two types of standards: de jure and de facto.
  - De jure standards are arrived at through consensus by national or international standards bodies; for example, ITU-T and IETF.
  - De facto standards are usually the result of an effort by one or more vendors to standardize a technology by forming a consortium.
- International Telecommunication Union
- Internet Engineering Task Force
- MPLS and Frame Relay Alliance (MFA) Forum

Type-Length-Value

- This concept is used in headers as well as the body of a packet, and by different layers of a networking architecture
- In many instances, the length may vary, or the type is preferred to be left open for future extensions of a protocol.
- To do that, the type and the length need to be explicitly declared along with the value—this notion is what is known as TLV.
- For example, a byte may be assigned to indicate the type (so that up to 256 different types can be defined), followed by two bytes for the length (to indicate through its 16 bits the length of value, that is counted in bytes), such that the value field can be up to 65,536 (=216) bytes.
- Because of the well-defined structure of TLV, the information content can be processed and another TLV can follow.
- Furthermore, a nested notion of TLV is also possible where the “V” part may include one or more TLV encoded sets of data.

Network Protocol Analyzer

- Network protocol analyzers are used to capture packets from live networks.
- By studying headers captured through such analyzers, it is often easier to understand a packet header, and more important, a protocol.
- Wireshark