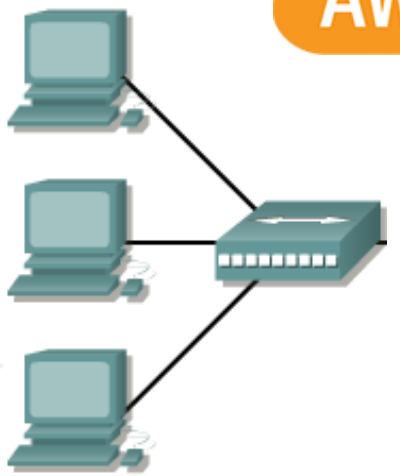
NETWORK COMPONENTS

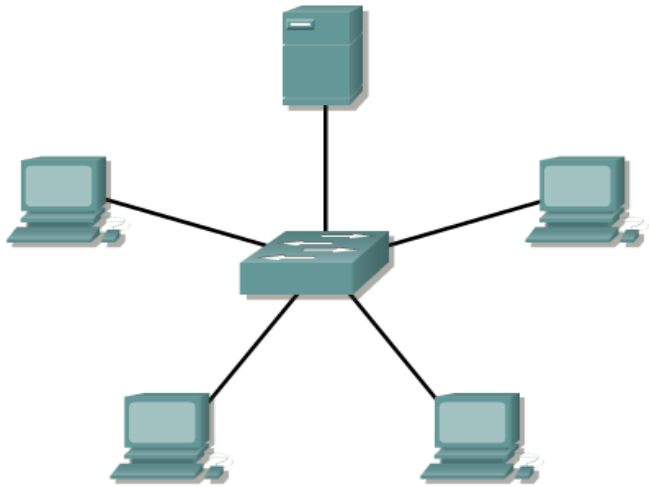
HUB

- ✓ Hub is Physical layer device which connects a group of Hosts.
- ✓ It will broadcasts the data to devices connected to it, if it is not aware of address of devices.
- ✓ Data's will be in the bits format(eg:100110)



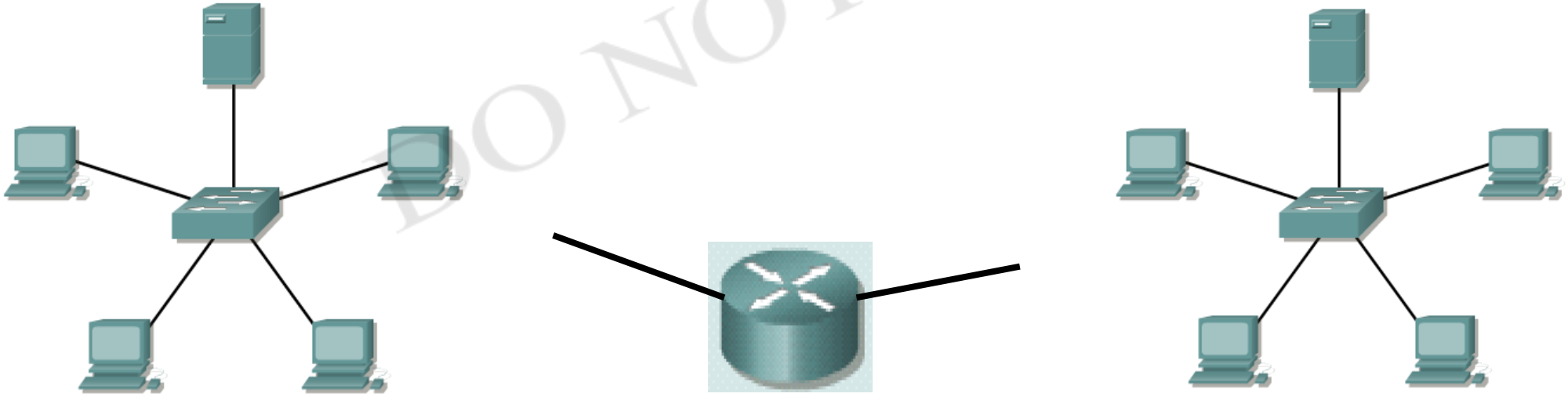
SWITCH

- ✓ Switches add more intelligence to data transfer management.
- ✓ It uses **physical device addresses (MAC)** in each incoming messages so that it can deliver the message to the right destination or port.
- ✓ Increases the speed of the network.



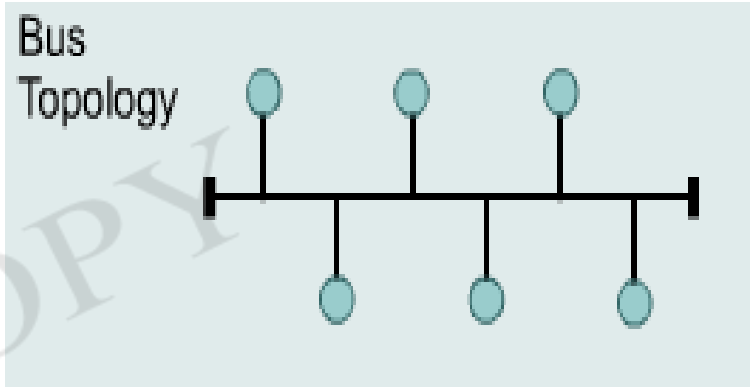
ROUTER

- ✓ Routers are used to connect networks together
- ✓ Route packets of data from one network to another
- ✓ Cisco became the de facto standard of routers because of their high-quality router products
- ✓ Routers, by default, break up a *broadcast domain*

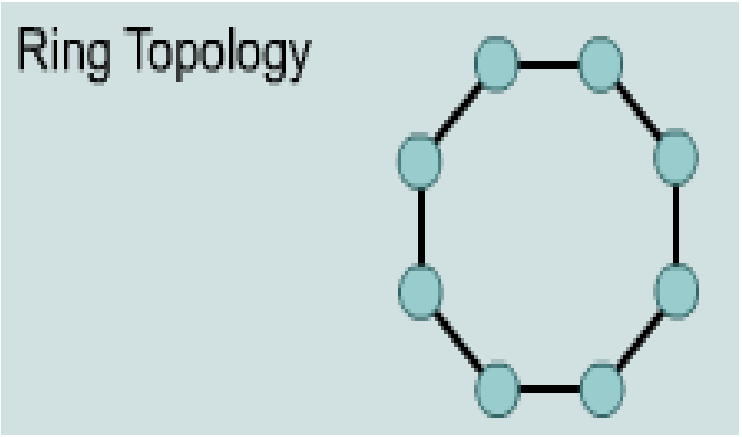


TOPOLOGY

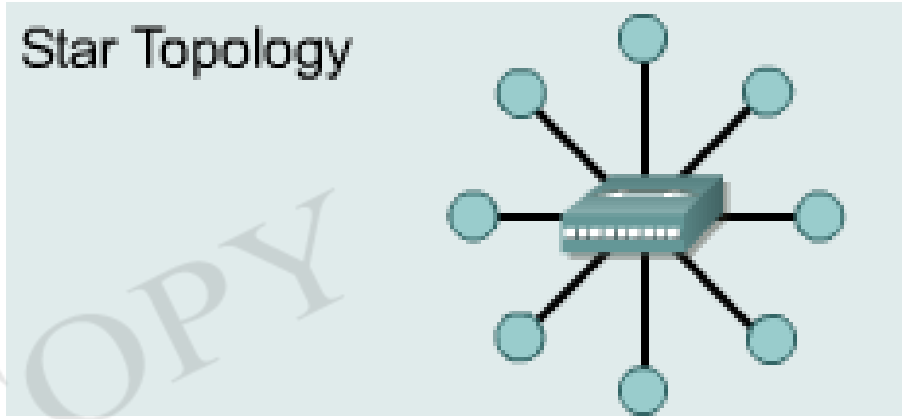
- ✓ A bus topology uses a single backbone cable that is terminated at both ends.
- ✓ All the hosts connect directly to this backbone.



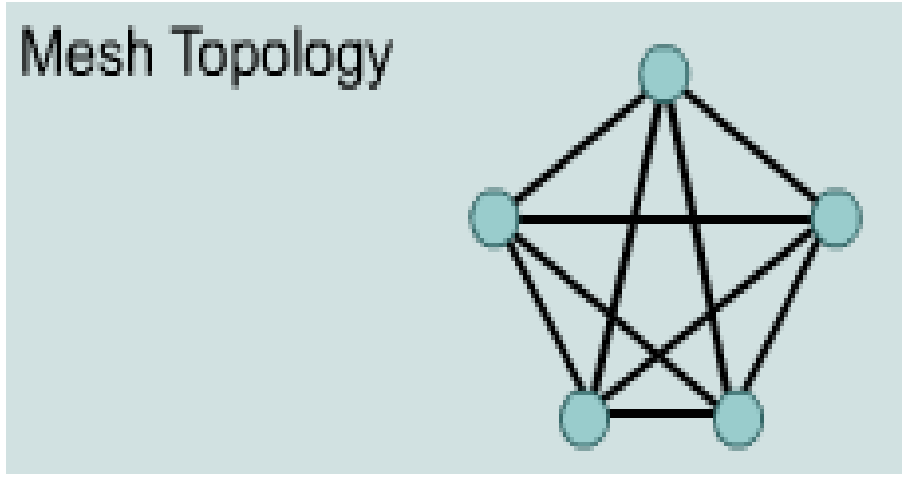
- ✓ A ring topology connects one host to the next and the last host to the first.
- ✓ This creates a physical ring of cable.



- ✓ A star topology connects all cables to a central point of concentration.

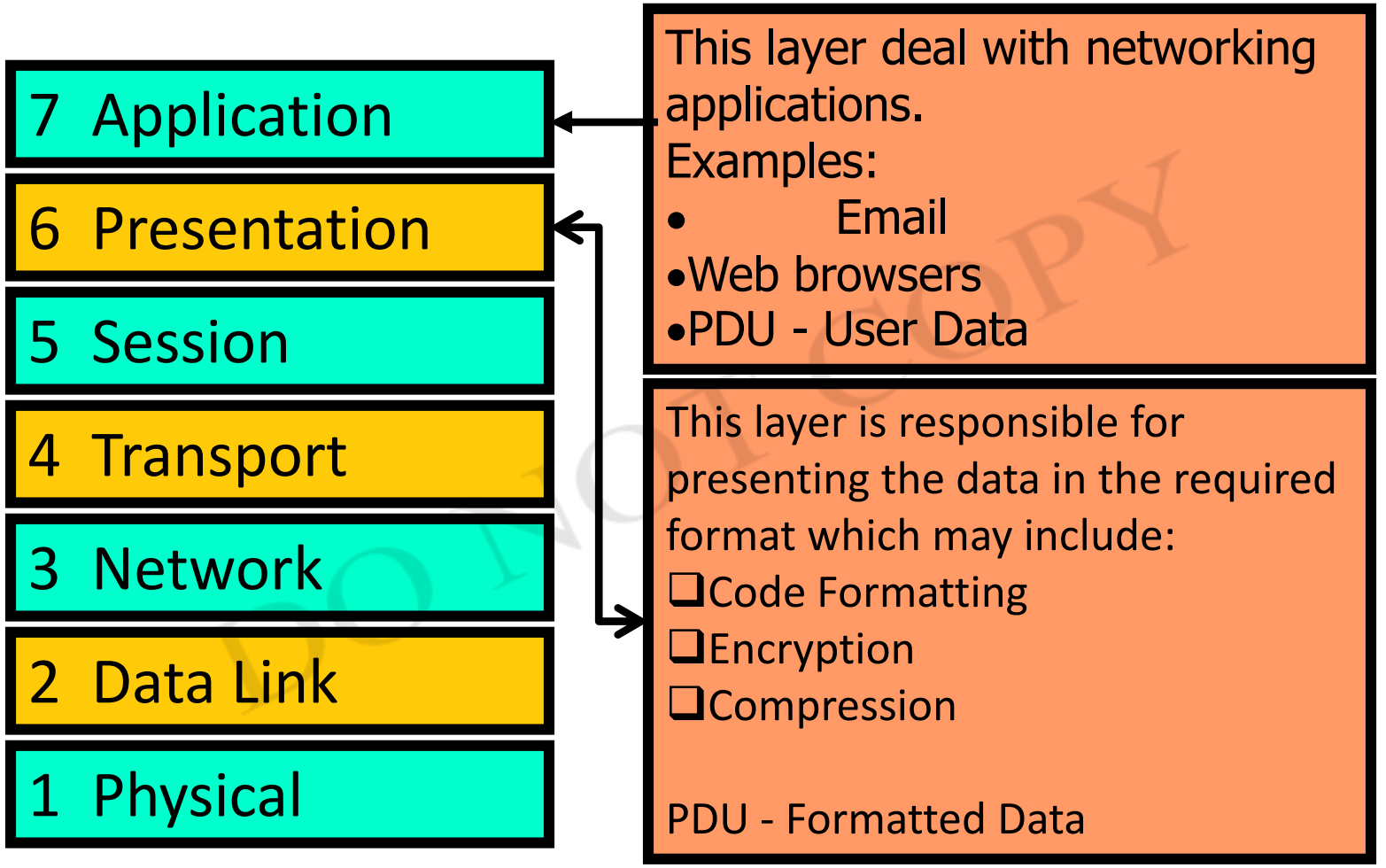


- ✓ A mesh topology is implemented to provide as much protection as possible from interruption of service.
- ✓ Each host has its own connections to all other hosts.
- ✓ Although the Internet has multiple paths to any one location, it does not adopt the full mesh topology.



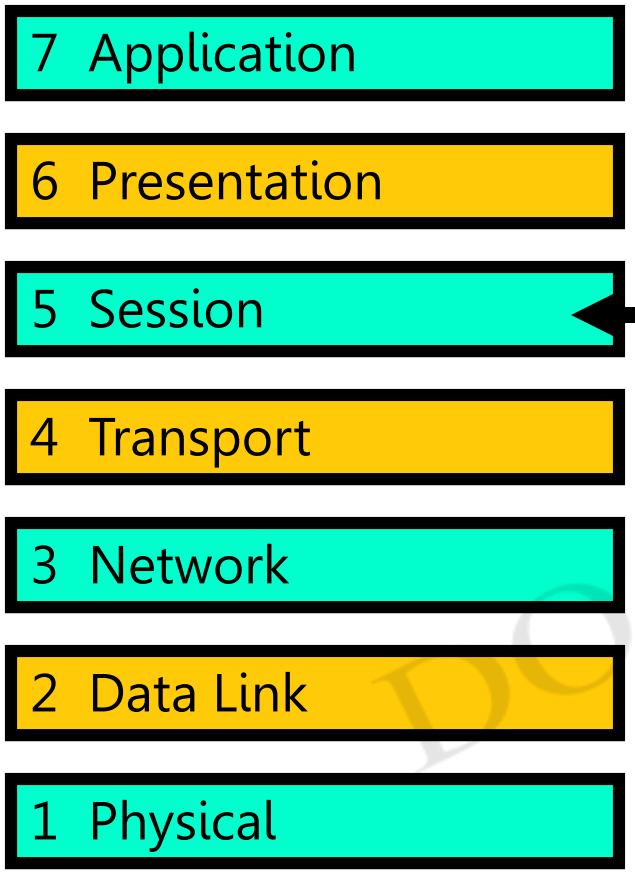
THE OSI MODEL

Layer 7 - The Application Layer



Each of the layers have Protocol Data Unit (PDU)

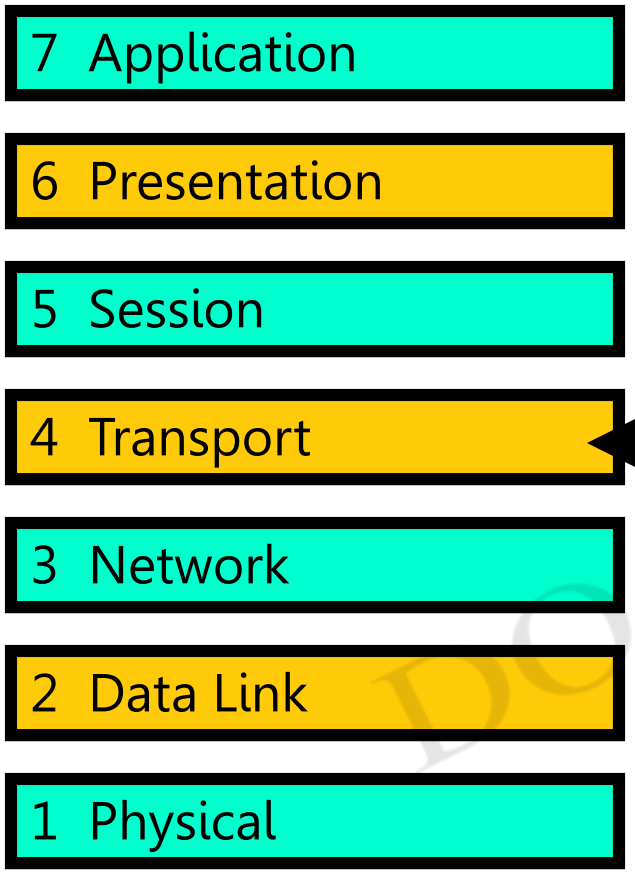
Layer 5 - The Session Layer



- ✓ This layer establishes, manages, and terminates sessions between two communicating hosts.
- ✓ Creates Virtual Circuit
- ✓ Coordinates communication between systems
- ✓ Organize their communication by offering three different modes
  - ✓ Simplex
  - ✓ Half Duplex
  - ✓ Full Duplex

Example:
Client Software (Used for logging in)
PDU - Formatted Data

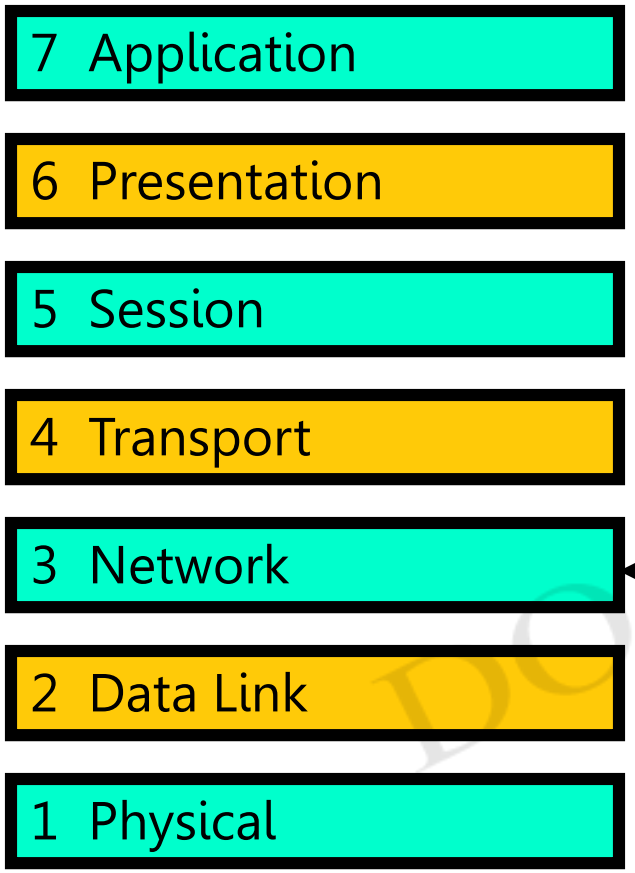
Layer 4 - The Transport Layer



- ✓ This layer breaks up the data from the sending host and then reassembles it in the receiver.
- ✓ It also is used to insure reliable data transport across the network.
- ✓ Can be reliable or unreliable
- ✓ Sequencing
- ✓ Acknowledgment
- ✓ Retransmission
- ✓ Flow Control

PDU - Segments

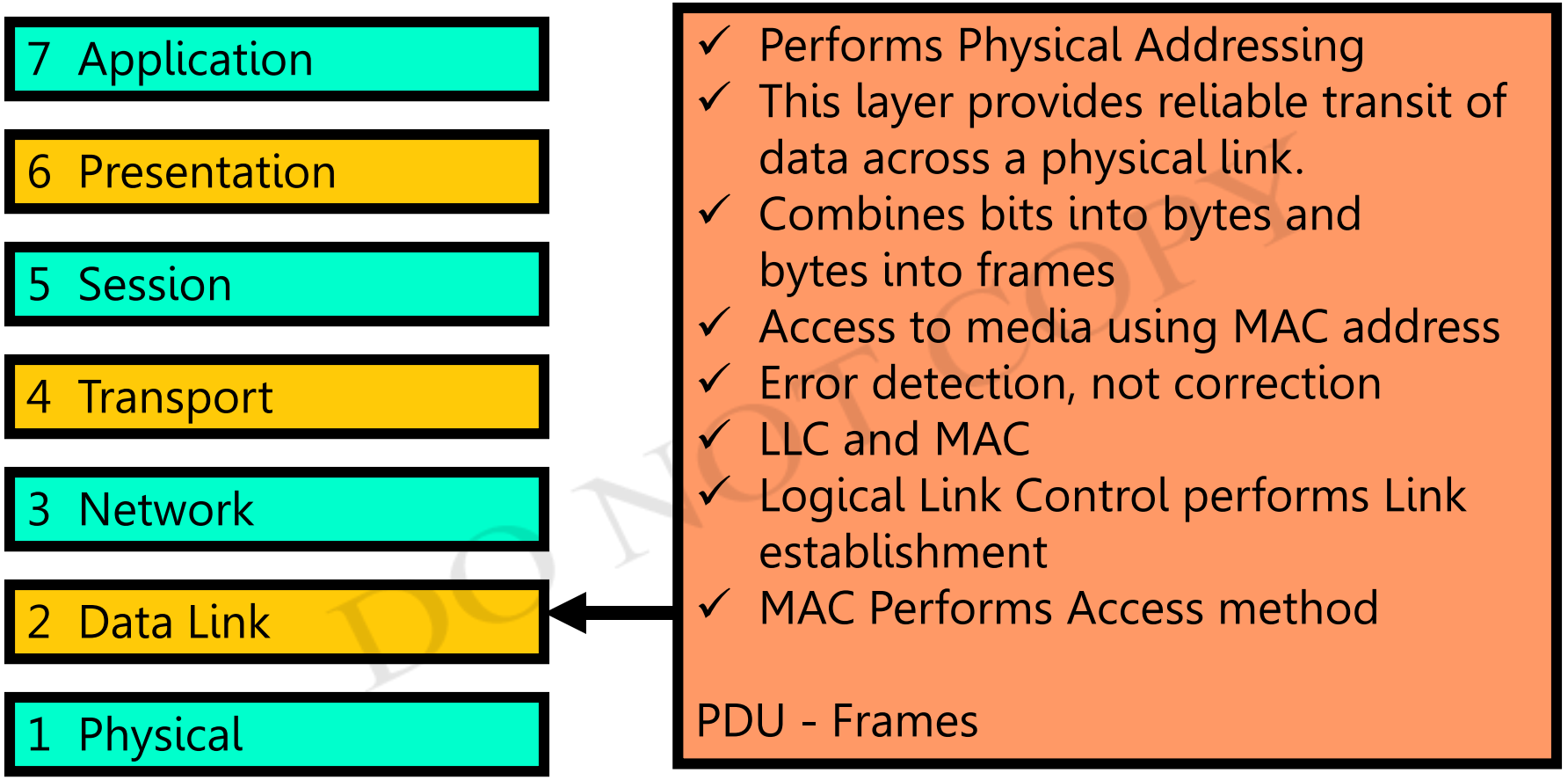
Layer 3 - The Network Layer



- ✓ Sometimes referred to as the "Cisco Layer".
- ✓ End to End Delivery
- ✓ Provide logical addressing that routers use for path determination
- ✓ Segments are encapsulated
- ✓ Internetwork Communication
- ✓ Packet forwarding
- ✓ Packet Filtering
- ✓ Makes "Best Path Determination"
- ✓ Fragmentation

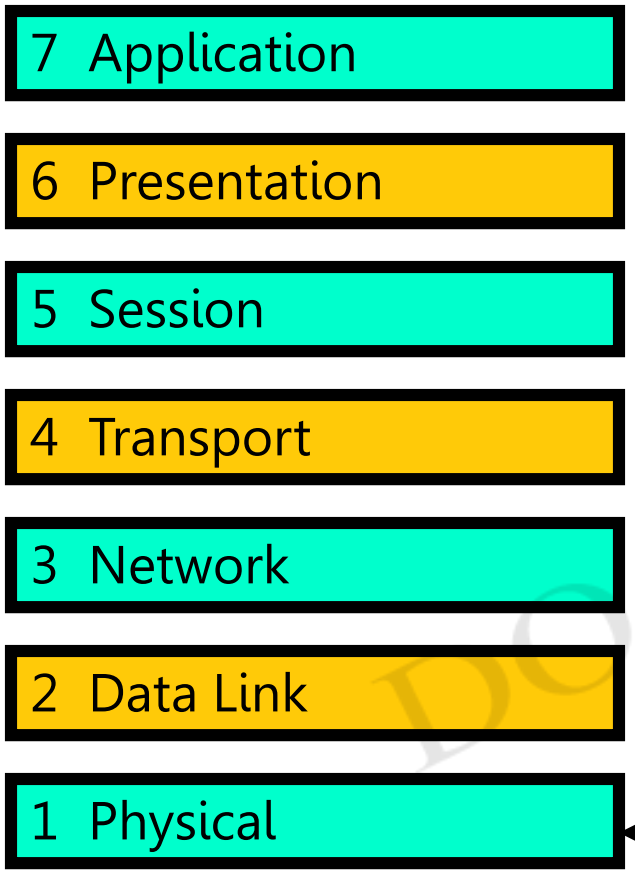
PDU – Packets – IP/IPX

Layer 2 - The Data Link Layer



Preamble	DMAC	SMAC	Data length	DATA	FCS

Layer 1 - The Physical Layer



- ✓ This is the physical media through which the data, represented as electronic signals, is sent from the source host to the destination host.
- ✓ Move bits between devices
- ✓ Encoding

PDU – Bits

IP Address Classes IPV4(32 bit) IPV6(128 bit)

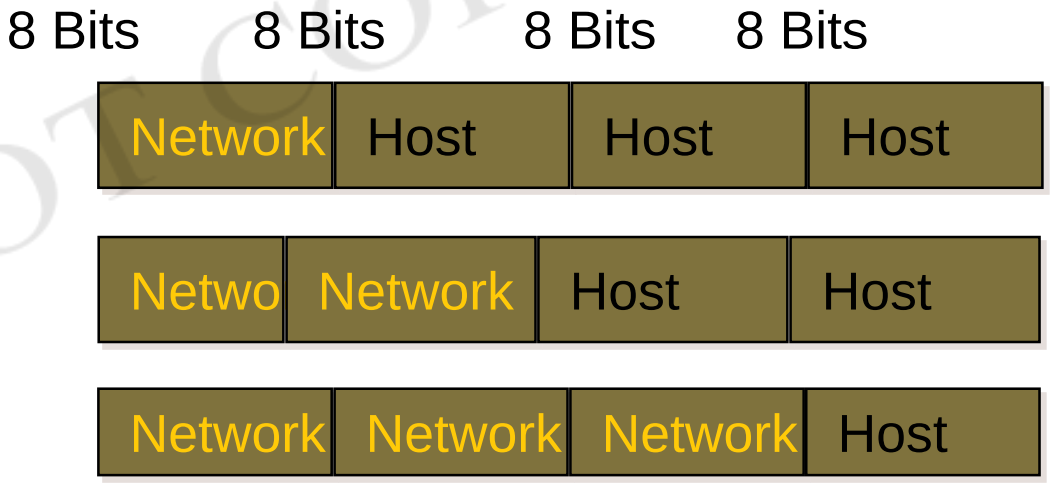
Class A: Range (1-126)

Class B: Range (128-191)

Class C: Range (192-223)

Class D: Range (224-239) Multicast

Class E: Range (240-255) Research



Public addresses are assigned by InterNIC and consist of class-based network IDs or blocks of CIDR-based addresses (called CIDR blocks) that are guaranteed to be globally unique to the Internet.

Private addresses are not reachable on the Internet. Private address range:

Class	Starting IP Address	Ending IP Address
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

Classless Inter-Domain Routing (CIDR)

Basically the method that ISPs (Internet Service Providers) use to allocate an amount of addresses to a company, a home

Ex : 192.168.10.32/28

The slash notation (/) means how many bits are turned on (1s)

Subnet Mask	CIDR Value
255.0.0.0	/8
255.128.0.0	/9
255.192.0.0	/10
255.224.0.0	/11
255.240.0.0	/12

Subnetting

Subnetting is logically dividing the network by extending the 1's used in SNM

Advantage

- ✓ Can divide network in smaller parts
- ✓ Restrict Broadcast traffic
- ✓ Security
- ✓ Simplified Administration

- ✓ Classful IP Addressing SNM are a set of 255's and 0's. In Binary it's contiguous 1's and 0's.
- ✓ SNM cannot be any value as it won't follow the rule of contiguous 1's and 0's.

Supernetting

	Network	Network	Network	Subnet
			16 8 4 2 1	
172.16.12.0	11000000	10101000	00001100	00000000
172.16.13.0	11000000	10101000	00001101	00000000
172.16.14.0	11000000	10101000	00001110	00000000
172.16.15.0	11000000	10101000	00001111	00000000
255.255.255.0	11111111	11111111	11111111	00000000

Supernetting

	Network	Network	Network	Subnet
			16 8 4 2 1	
172.16.12.0	11000000	10101000	00001100	00000000
172.16.13.0	11000000	10101000	00001101	00000000
172.16.14.0	11000000	10101000	00001110	00000000
172.16.15.0	11000000	10101000	00001111	00000000
255.255.252.0	11111111	11111111	11111100	00000000

172.16.12.0/24
172.16.13.0/24
172.16.14.0/24
172.16.15.0/24
} 172.16.12.0/22

VLAN's

- ✓ A VLAN is a logical grouping of network users and resources connected to administratively defined ports on a switch.
- ✓ Ability to create smaller broadcast domains within a layer 2 switched internetwork by assigning different ports on the switch to different subnetworks.
- ✓ Frames broadcast onto the network are only switched between the ports logically grouped within the same VLAN
- ✓ By default, no hosts in a specific VLAN can communicate with any other hosts that are members of another VLAN,
- ✓ For Inter VLAN communication you need routers

Types of Links

Access links

- ✓ This type of link is only part of one VLAN
- ✓ It's referred to as the *native VLAN* of the port.
- ✓ Any device attached to an *access link* is unaware of a VLAN
- ✓ Switches remove any VLAN information from the frame before it's sent to an access-link device.

Trunk links

- ✓ Trunks can carry multiple VLANs
- ✓ These carry the traffic of multiple VLANs
- ✓ A trunk link is a 100- or 1000Mbps point-to-point link between two switches, between a switch and router.

VLAN Trunking Protocol (VTP)

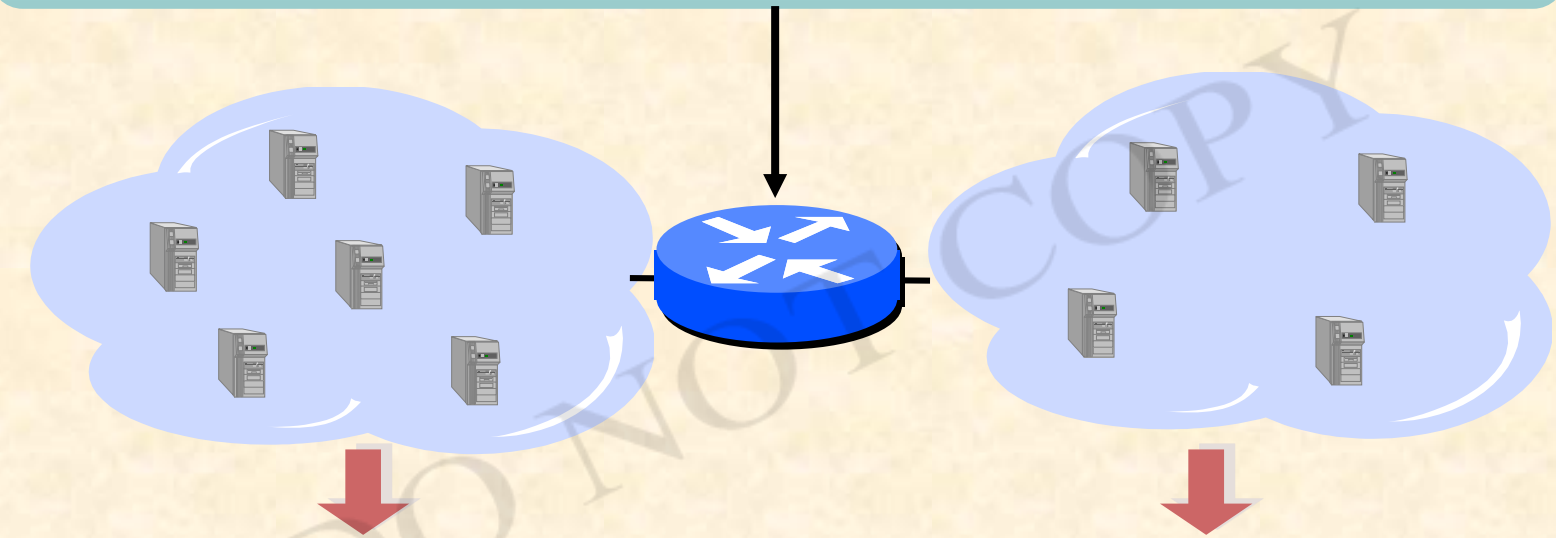
Benefits of VTP

- ✓ Consistent VLAN configuration across all switches in the network
- ✓ Accurate tracking and monitoring of VLANs
- ✓ Dynamic reporting of added VLANs to all switches in the VTP domain

NETWORK ADDRESS TRANSLATOR

NAT: Network Address Translator

- NAT
  - Translates between local addresses and public ones
  - Many private hosts share few global addresses



- Private Network
  - Uses private address range (local addresses)
  - Local addresses may not be used externally

- Public Network
  - Uses public addresses
  - Public addresses are globally unique

NAT Addressing Terms

Inside Local

The term “inside” refers to an address used for a host inside an enterprise. It is the actual IP address assigned to a host in the private enterprise network.

Inside Global

NAT uses an inside global address to represent the inside host as the packet is sent through the outside network, typically the Internet. A NAT router changes the source IP address of a packet sent by an inside host from an inside local address to an inside global address as the packet goes from the inside to the outside network.

Outside Global

The term “outside” refers to an address used for a host outside an enterprise, the Internet. An outside global is the actual IP address assigned to a host that resides in the outside network, typically the Internet.

Outside Local

NAT uses an outside local address to represent the outside host as the packet is sent through the private network. This address is outside private, outside host with a private address.

Types of NAT

There are different types of NAT that can be used, which are

- ✓ Static NAT
- ✓ Dynamic NAT
- ✓ Overloading NAT with PAT (NAPT)

- ✓ Static NAT - Mapping an unregistered IP address to a registered IP address on a one-to-one basis. Particularly useful when a device needs to be accessible from outside the network.
- ✓ In static NAT, the computer with the IP address of 192.168.32.10 will always translate to 213.18.123.110.

Dynamic NAT

Dynamic NAT - Maps an unregistered IP address to a registered IP address from a group of registered IP addresses.

In dynamic NAT, the computer with the IP address 192.168.32.10 will translate to the first available address in the range from 213.18.123.100 to 213.18.123.150. Dynamic NAT sets up a pool of possible inside global addresses and defines criteria for the set of inside local IP addresses whose traffic should be translated with NAT.

The dynamic entry in the NAT table stays in there as long as traffic flows occasionally.

If a new packet arrives, and it needs a NAT entry, but all the pooled IP addresses are in use, the router simply discards the packet

Overloading NAT with PAT (NAPT)

Overloading - A form of dynamic NAT that maps multiple unregistered IP addresses to a single registered IP address by using different ports. This is known also as PAT (Port Address Translation), single address NAT or port-level multiplexed NAT.

In overloading, each computer on the private network is translated to the same IP address (213.18.123.100), but with a different port number assignment.

LAN & WAN

A **LAN** (local area network) is a group of computers and network devices connected together, usually within the same building. By definition, the connections must be high speed and relatively inexpensive (e.g., token ring or Ethernet).

A LAN connection is a high-speed connection to a LAN. On the IUB campus, most connections are either Ethernet (10 Mbps) or Fast Ethernet (100 Mbps), and a few locations have Gigabit Ethernet (1000 Mbps) connections.

A **WAN** (wide area network), in comparison to a MAN, is not restricted to a geographical location, although it might be confined within the bounds of a state or country. A WAN connects several LANs, and may be limited to an enterprise (a corporation or an organization) or accessible to the public. The technology is high speed and relatively expensive. The Internet is an example of a worldwide public WAN.

Access Control Lists

Access Control Lists used to implement security in routers

powerful tool for network control

filter packets flow in or out of router interfaces

restrict network use by certain users or devices

deny or permit traffic

TYPES OF ACL

Standard IP Access Lists (1 - 99)
- – simpler address specifications
- – generally permits or denies entire protocol suite

Extended IP Access Lists (100 - 199)
- – more complex address specification
- – generally permits or denies specific protocols

Access Control List Syntax

Standard IP Access List Configuration Syntax

- access-list access-list-number {permit | deny} source {source-mask}
- ip access-group access-list-number {in | out}

Extended IP Access List Configuration Syntax

- access-list access-list-number {permit | deny} protocol source {source-mask} destination {destination-mask}
- ip access-group access-list-number {in | out}

Where To Place Access Control Lists

Place **Standard IP** access list close to **destination**

Place **Extended IP** access lists close to the **source** of the traffic you want to manage

THANK YOU