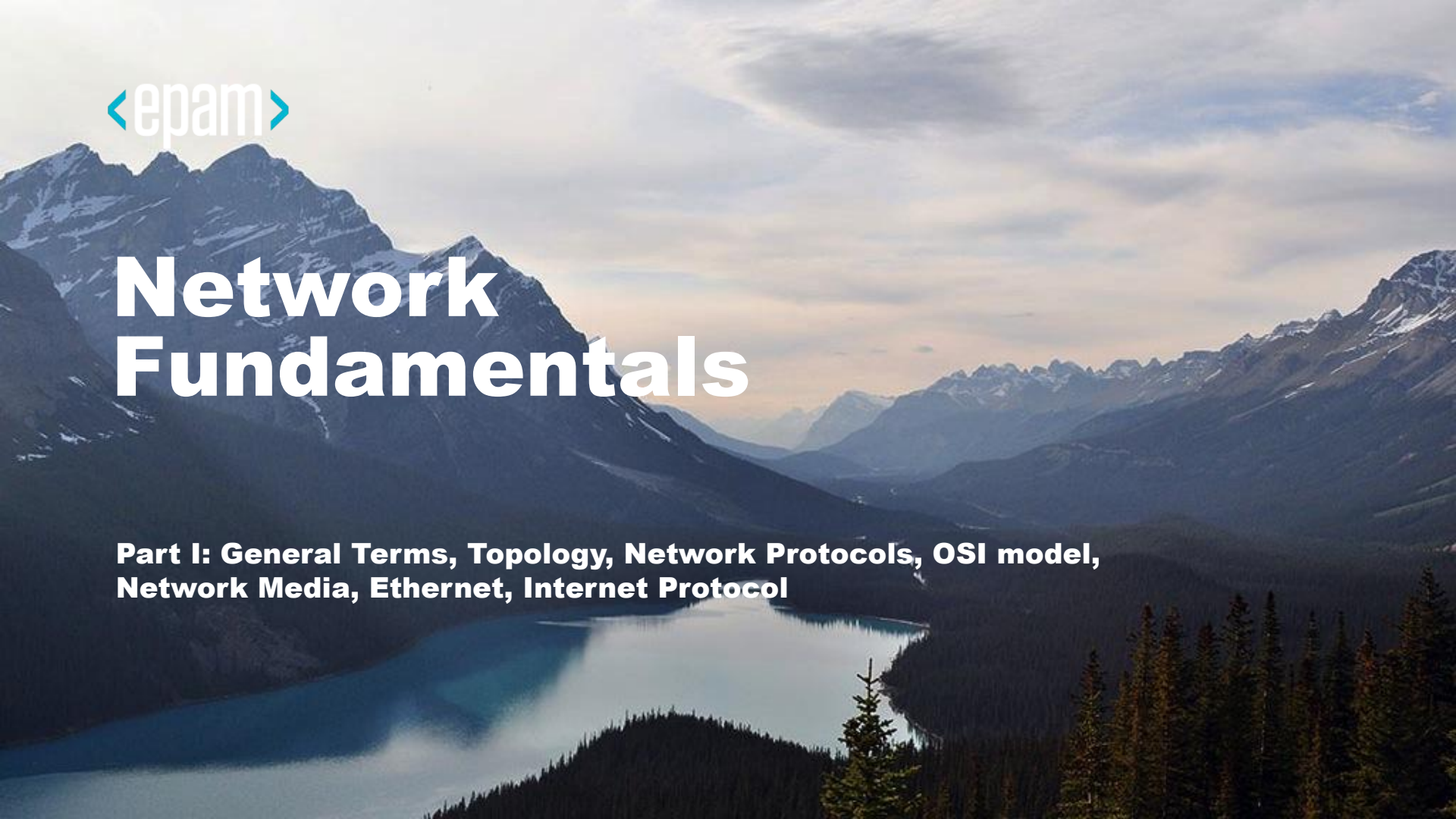


Network Fundamentals

Part I: General Terms, Topology, Network Protocols, OSI model, Network Media, Ethernet, Internet Protocol

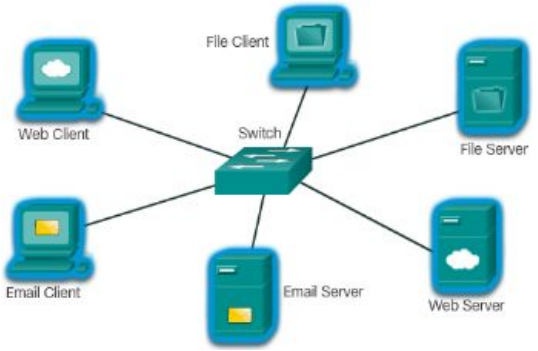
AGENDA

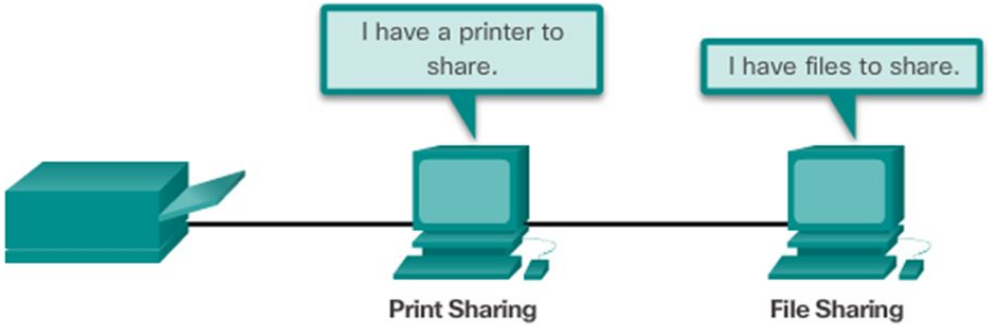
1. General terms
2. Topology
3. Network Protocols
4. OSI Model
5. Network Media
6. Ethernet
7. Internet Protocol

General Terms

Providing Resources in a Network

- Networks of Many Sizes
  - Small Home / Office Networks
  - Medium to Large Networks
  - World Wide Network
- Clients and Servers
  - Clients request and display information
  - Servers provide information to other devices on the network
- Peer-to-Peer
  - Computers can be both server and client at the same time.
  - What are the advantages?
  - What are the disadvantages?





Network Components

- End Devices
  - Either the source or destination of a message
  - Name some end devices
- Intermediary Network Devices
  - Connect multiple individual networks to form an internetwork
  - Connect the individual end devices to the network
  - Ensure data flows across the network
  - Provide connectivity
- Network Media
  - Provide the pathway for data transmission
  - Interconnect devices
  - Name the three types of media

Network Components

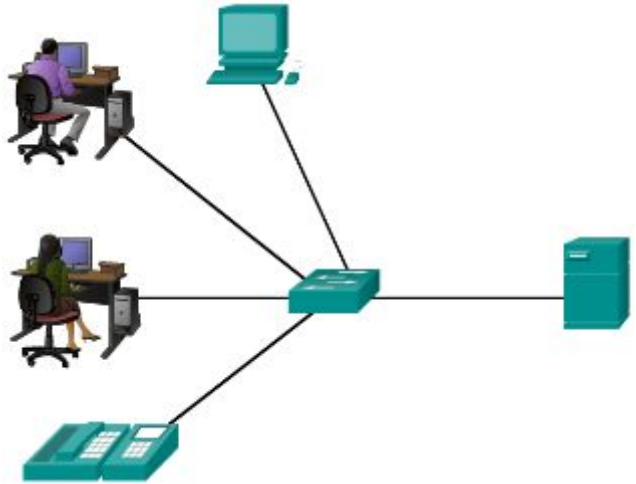
- Network Representations
  - What do the symbols represent?
- Topology Diagrams
  - Physical
  - Logical





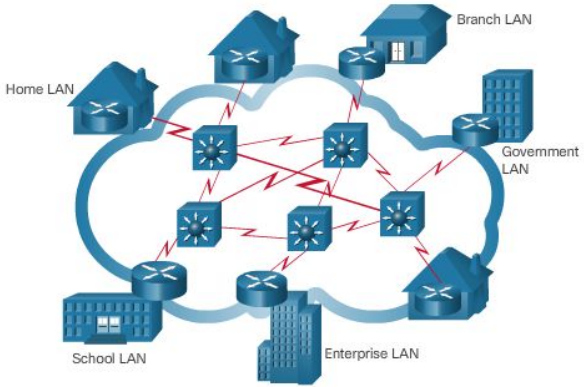

LANs and WANs

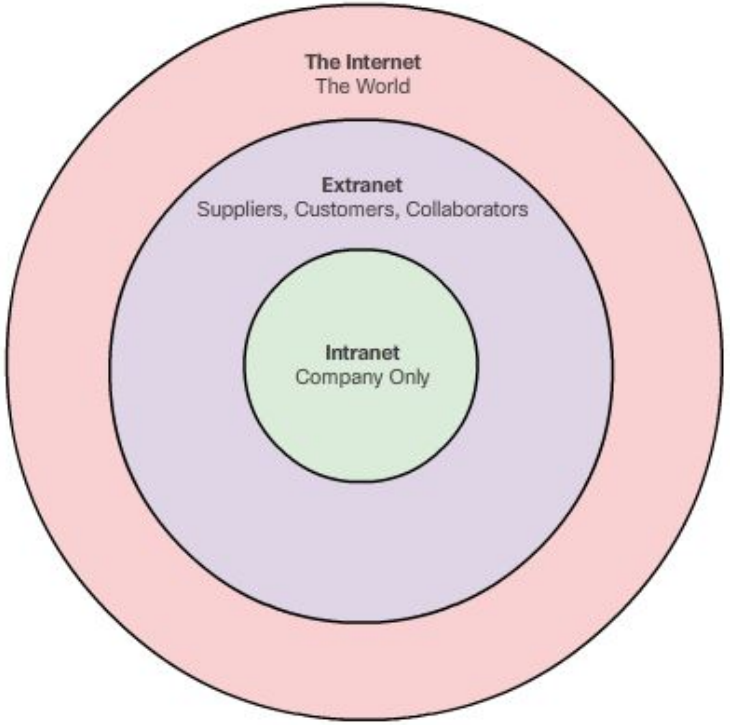
- Local Area Networks
  - Spans across small geographical area
  - Interconnects end devices
  - Administrated by a single organization
  - Provides high speed bandwidth to internal devices
- WAN Area Networks
  - Interconnects LAN
  - Administrated by multiple service providers
  - Provide slower speed links between LANS



The Internet, Intranets, and Extranets

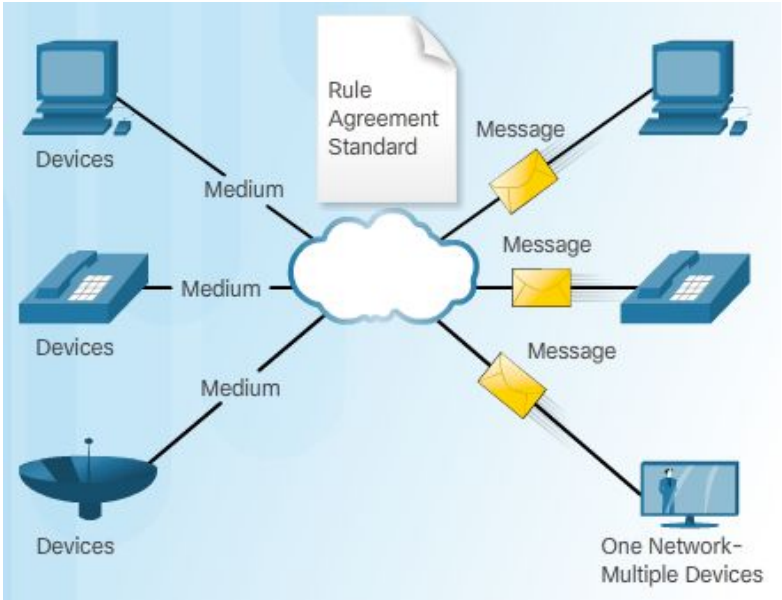
- The Internet
  - Worldwide collection of interconnected networks
  - Not owned by any individual or group
- Intranets and Extranets





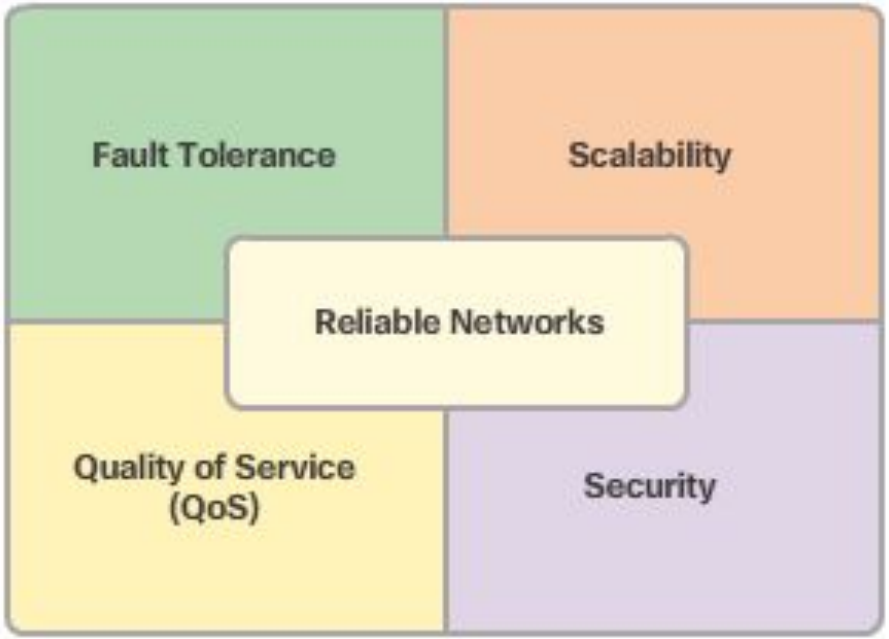
Converged Networks

- Traditional Separate Networks
  - Each network with its own rules and
- The Converging Network
  - Capable of delivering data, voice, and video over the same network infrastructure



Reliable Network

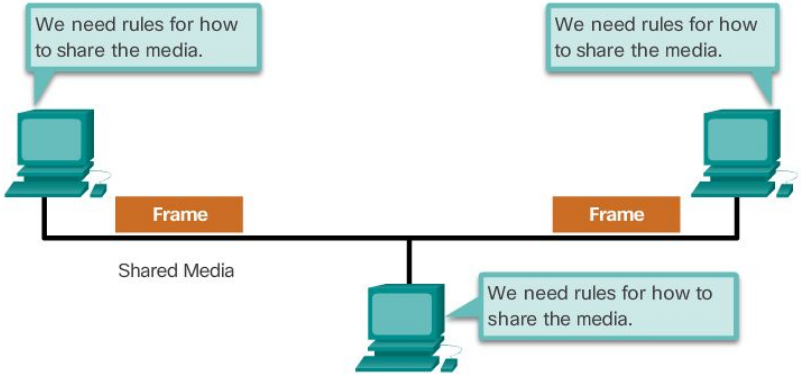
- Four Basic Characteristics of Network Architecture
  - Fault Tolerance
  - Scalability
  - Quality of Service (QoS)
  - Security



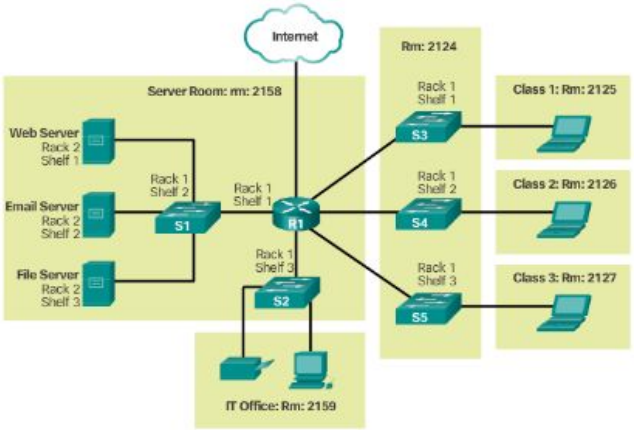
Network Topology

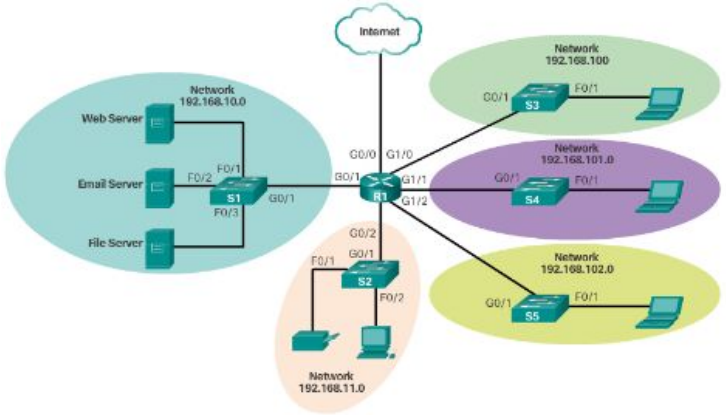
Topologies

Controlling Access to the Media



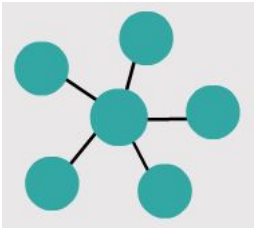
Physical and Logical Topologies

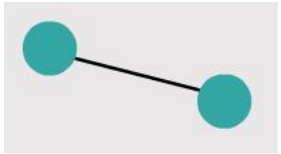


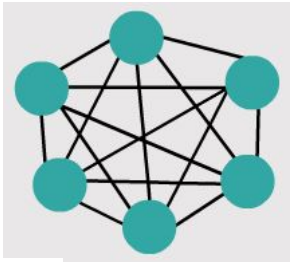


WAN Topologies

- Common Physical WAN Topologies
  - Point-to-point
  - Hub and spoke
  - Mesh
- Physical Point-to-Point Topology
- Logical Point-to-Point Topology

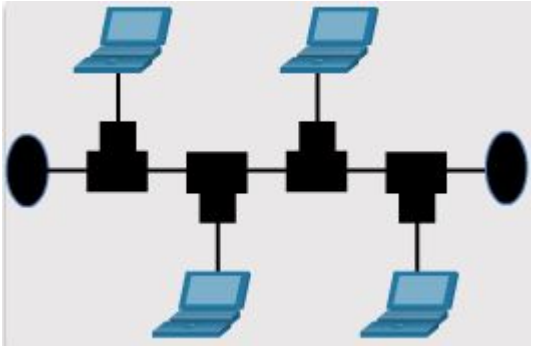


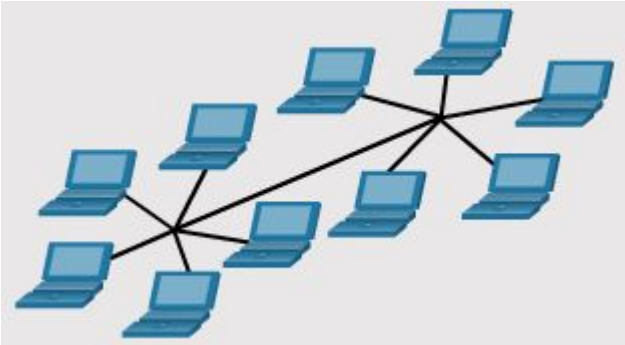




LAN Topologies

- Physical LAN Topologies
- Half and Full Duplex
- Media Access Control Methods
- Contention-Based Access
  - CSMA/CD vs. CSMA/CA

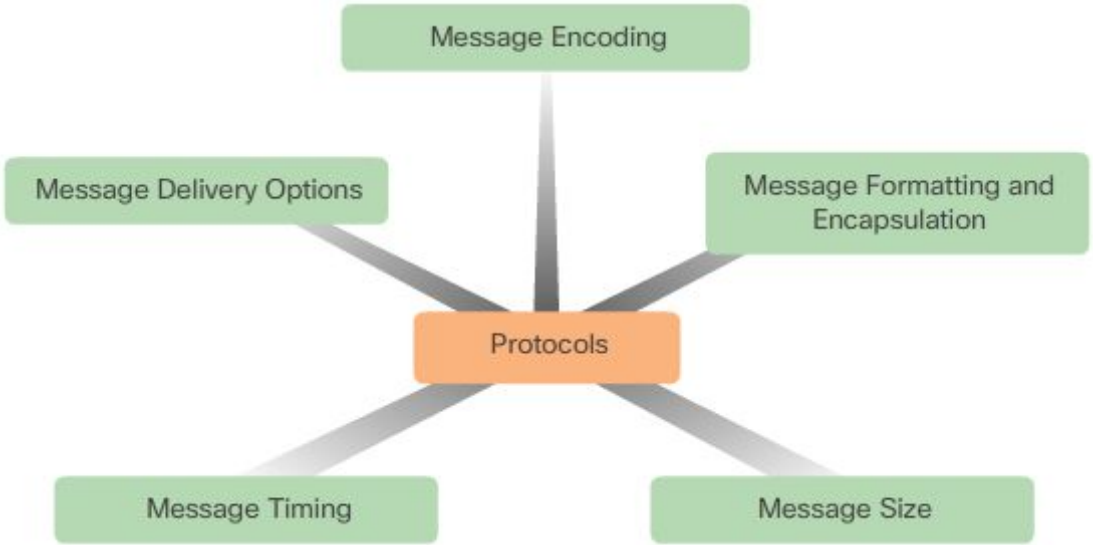




Network Protocols

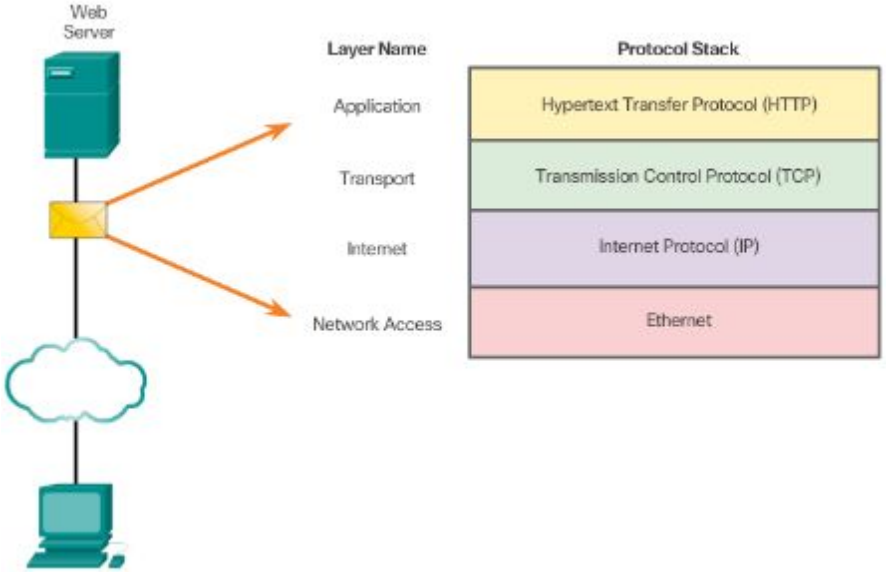
The Rules

- Rule Establishment
  - Identified sender and receiver
  - Common language and grammar
  - Speed and timing of delivery
  - Confirmation or acknowledgment requirements
- Message Encoding
  - Process of converting information into another acceptable form
- Message Formatting and Encapsulation
- Message Size
- Message Timing
  - Access method
  - Flow control
  - Response timeout
- Message Delivery Options
  - Unicast
  - Multicast
  - Broadcast



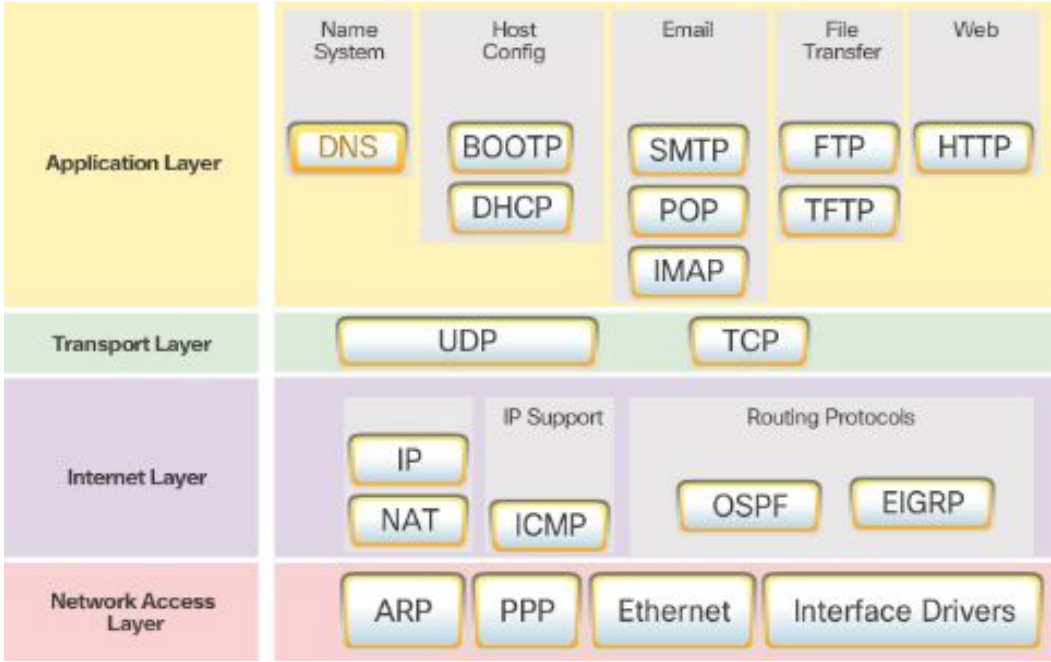
Protocols

- Rules that Govern Communications
- Network Protocols
  - The role of protocols
  - How the message is formatted or structured
  - The process by which networking devices share information about pathways with other networks
  - How and when error and system messages are passed between devices
  - The setup and termination of data transfer sessions
- Protocol Interaction
  - Example: web server and client



Protocol Suites

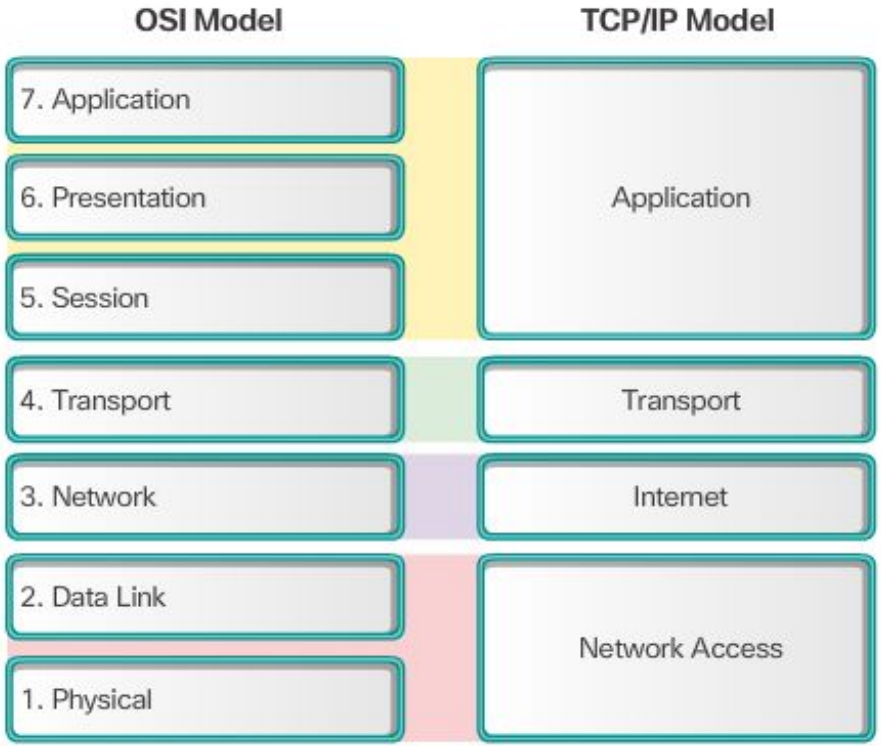
- Protocol Suites and Industry Standards
  - TCP/IP is an open standard
  - Can you name other protocol suites?
- TCP/IP Protocol Suites
  - Can you name some of the protocols from the TCP/IP protocol suite
- TCP/IP Communication Process
  - Can you describe the process?



OSI Model

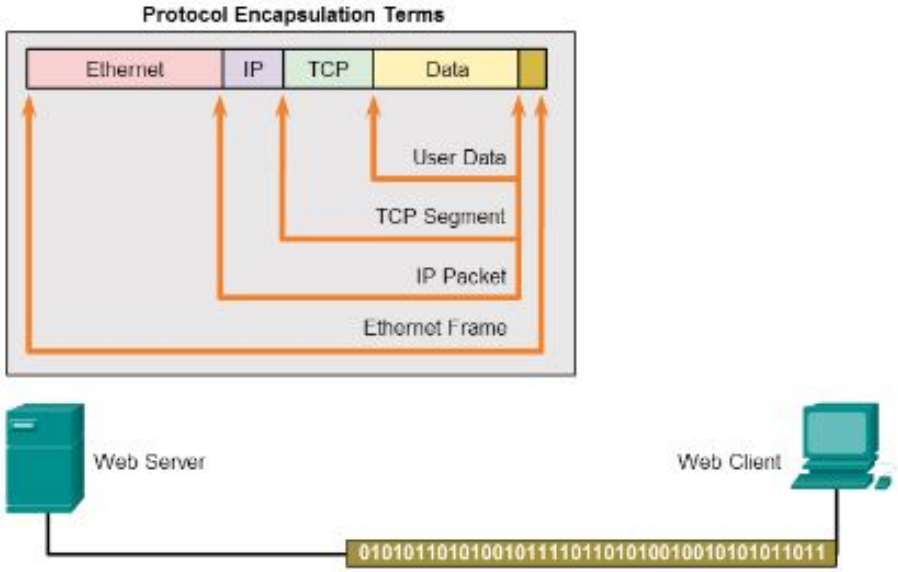
Reference Models

- The Benefits of Using a Layered Model
  - Name some benefits
- The OSI Reference Model
  - Provides list of functions
  - Describes interactions between layers
- OSI Model and TCP/IP Model Comparison
  - Similar: transport and network layers
  - Contrast: relationship between layers



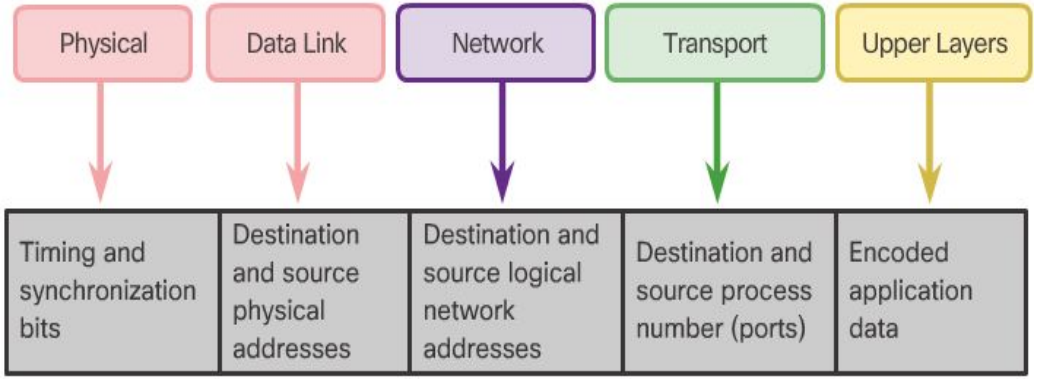
Data Encapsulation

- Message Segmentation
  - Segmentation - Break communication into pieces
  - Multiplexing – interleaving the pieces
- Protocol Data Units
  - What are PDUs called at each layer?
- Encapsulation and de-encapsulation process



Data Access

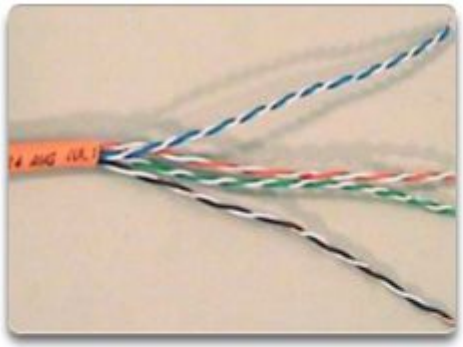
- Network Addresses
  - Source IP address
  - Destination IP address
  - Deliver the IP packet from the original source to the final destination, either on the same network or to a remote network
- Data Link Addresses
  - Source data link address
  - Destination data link address
  - Deliver the data link frame from one network interface card (NIC) to another NIC on the same network
- Devices on the Same Network
- Devices on a Remote Network



Network Media

Copper Cabling

- Characteristics of Copper Cabling
  - Inexpensive, easy to install, low resistance to electric current
  - Distance and signal interference
- Copper Media
- Unshielded Twisted-Pair Cable
- Shielded Twisted-Pair Cable
- Coaxial Cable
- Copper Media Safety
  - Fire and electrical hazards



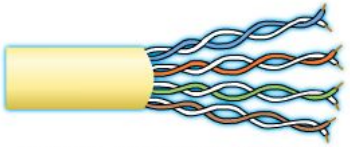
Unshielded Twisted-Pair (UTP) cable

Shielded Twisted-Pair (STP) cable

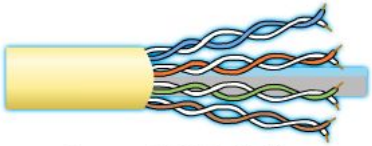
Coaxial cable

UTP Cabling

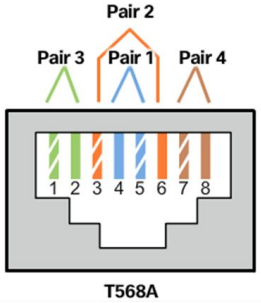
- Properties of UTP Cabling
  - Cancellation of EMI and RFI signals with twisted pairs
- UTP Cabling Standards
  - TIA/EIA-568
  - IEEE: Cat5, Cat5e, Cat6, Cat6e
- UTP Connectors
- Types of UTP Cable
  - Rollover
  - Crossover
  - Straight-through
- Testing UTP Cables
- Cable Pinouts

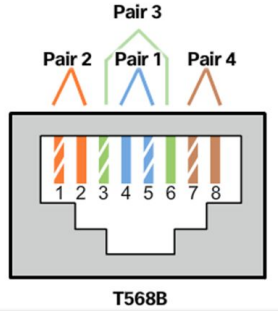


Category 5 and 5e Cable (UTP)



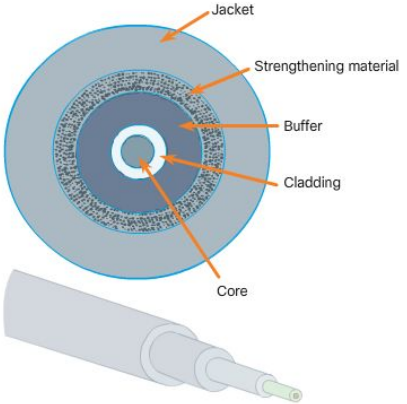
Category 6 Cable (UTP)





Fiber-Optic Cabling

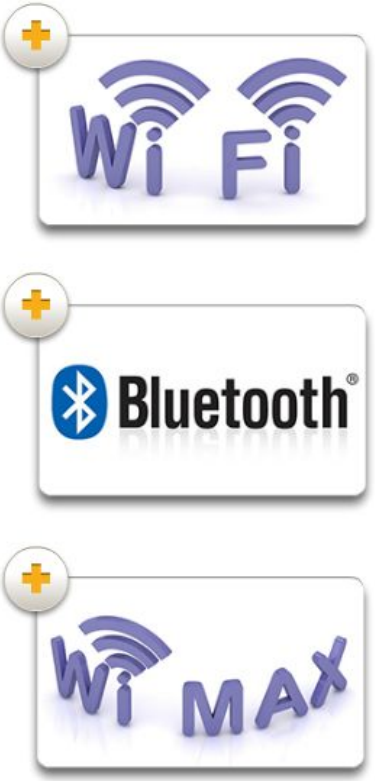
- Properties of Fiber-Optic Cabling
  - Transmits data over longer distances
  - Flexible, but thin strands of glass
  - Transmits with less attenuation
  - Immune to EMI and RFI
- Fiber Media Cable Design
- Types of Fiber Media
  - Single mode and multimode
- Fiber-Optic Connectors
- Testing Fiber Cables
- Fiber versus Copper



Implementation Issues	UTP Cabling	Fiber-optic Cabling
Bandwidth supported	10 Mb/s – 10 Gb/s	10 Mb/s – 100 Gb/s
Distance	Relatively short (1 – 100 meters)	Relatively high (1 – 100,000 meters)
Immunity to EMI and RFI	Low	High (Completely immune)
Immunity to electrical hazards	Low	High (Completely immune)
Media and connector costs	Lowest	Highest
Installation skills required	Lowest	Highest
Safety precautions	Lowest	Highest

Wireless Media

- Properties of Wireless Media
  - Data communications using radio or microwave frequencies
- Types of Wireless Media
  - Wi-Fi, Bluetooth, WiMax
- Wireless LAN
  - Wireless Access Point
  - Wireless NIC adapters



Wireless Media

Standard	Bandwidth	Frequency	Backward compatibility
802.11a	54 Mbps	5 GHz	No
802.11b	11 Mbps	2.4 GHz	No
802.11g	54 Mbps	2.4 GHz	802.11b
802.11n	600 Mbps	2.4 GHz or 5 GHz	802.11b/g
802.11ac	1.3 Gbps (1300 Mbps)	2.4 GHz and 5.5 GHz	802.11b/g/n
802.11ad	7 Gbps (7000 Mbps)	2.4 GHz, 5 GHz and 60 GHz	802.11b/g/n/ac

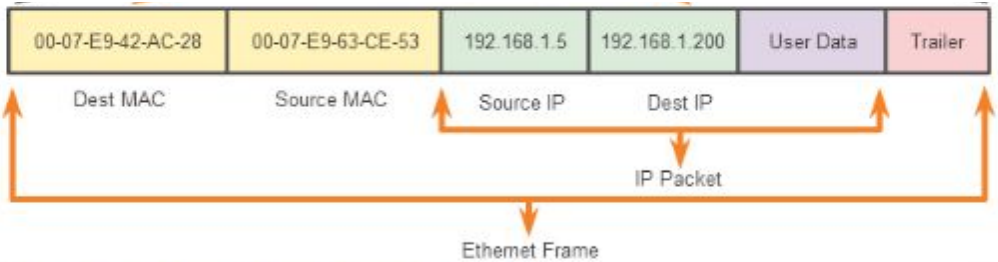
Ethernet

Ethernet MAC Addresses

- MAC Addresses and Hexadecimal
  - MAC address is 48-bit long and expressed as 12 hexadecimal digits
- MAC Addresses: Ethernet Identity
  - IEEE requires a vendor to follow two simple rules:
  - Must use that vendor's assigned OUI as the first three bytes
  - All MAC addresses with the same OUI must be assigned a unique value in the last three bytes
- Frame Processing
  - The NIC compares the destination MAC address in the frame with the device’s physical MAC address stored in RAM
  - If there is a match, the framed is passed up the OSI layers
  - If there is no match, the device discards the frame
- MAC Address Representations
  - MAC addresses can be represented with colons, dashes or dots and are case-insensitive
  - 00-60-2F-3A-07-BC, 00:60:2F:3A:07:BC, 0060.2F3A.07BC and 00-60-2f-3a-07-bc are all valid representations of the same MAC address

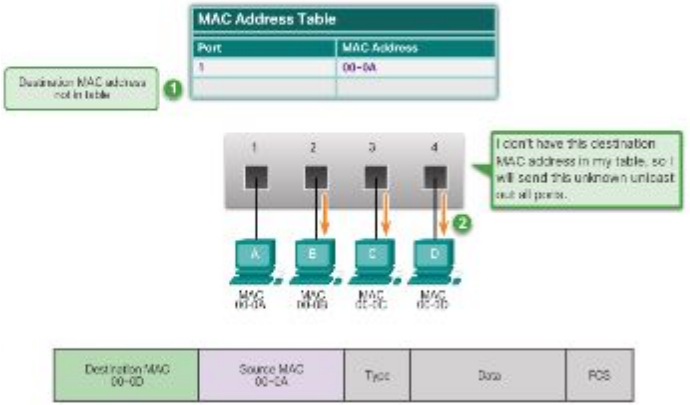
Ethernet MAC Addresses

- Unicast MAC Address
  - Unique address used when a frame is sent from a single transmitting device to a single destination device
  - The source MAC address must always be a unicast
- Broadcast MAC Address
  - Used to address all nodes in the segment
  - The destination MAC address is the address of FF-FF-FF-FF-FF-FF in hexadecimal (48 ones in binary)
- Multicast MAC Address
  - Used to address a group of nodes in the segment
  - The multicast MAC address is a special value that begins with 01-00-5E in hexadecimal
  - The remaining portion of the multicast MAC address is created by converting the lower 23 bits of the IP multicast group address into 6 hexadecimal characters



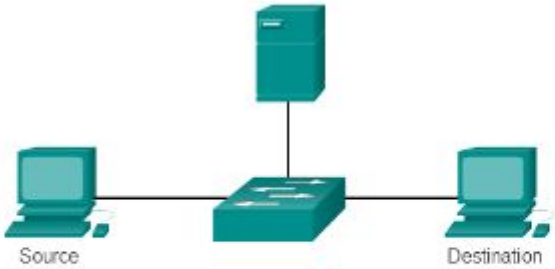
The MAC Address Table

- Switch Fundamentals
  - An Ethernet Switch is a Layer 2 device.
  - It uses MAC addresses to make forwarding decisions.
  - The MAC address table is sometimes referred to as a content addressable memory (CAM) table
- Learning MAC Addresses
  - Switches dynamically build the CAM by monitoring source MACs
  - Every frame that enters a switch is checked for new addresses
  - The frame is forwarded based on the CAM.
- Filtering Frames
  - Since the switch knows where to find a specific MAC address, it can filter the frames to that port only
  - Filtering is not done if the destination MAC is not present in the CAM



Switch Forwarding Methods

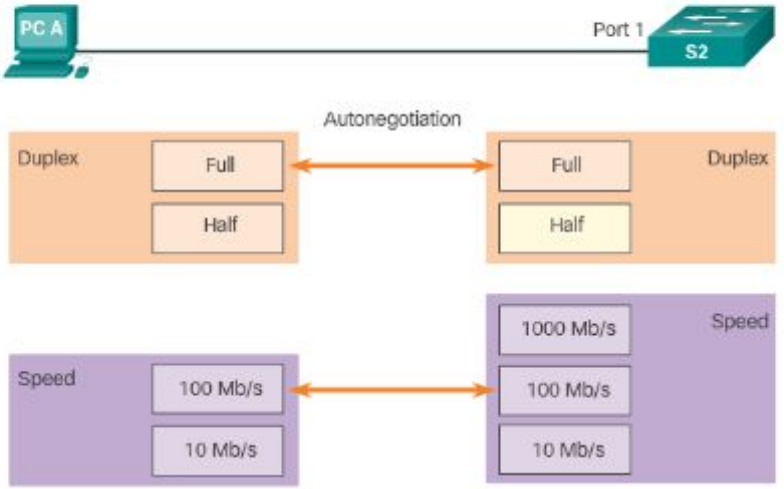
- Frame Forwarding Methods on Cisco Switches
  - Store-And-Forward
  - Cut-Through
- Cut-Through Switching
  - Fast-forward switching
    - Lowest level of latency immediately forwards a packet after reading the destination address
    - Typical cut-through method of switching
  - Fragment-free switching
    - Switch stores the first 64 bytes of the frame before forwarding
    - Most network errors and collisions occur during the first 64 bytes
- Memory Buffering on Switches
  - Port-based memory
  - Share memory



A cut-through switch forwards the frame before it is entirely received. At a minimum, the destination address of the frame must be read before the frame can be forwarded.

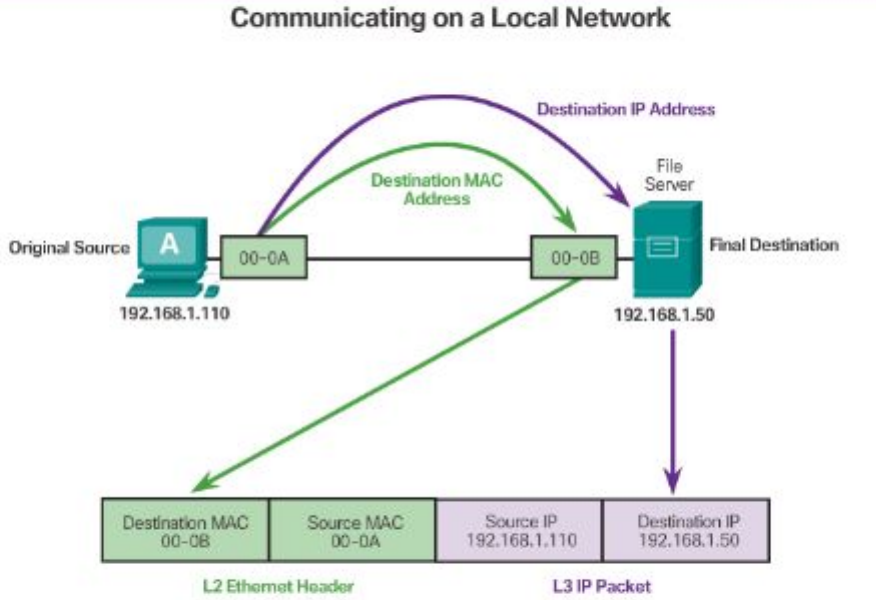
Switch Port Settings

- Duplex and Speed Settings
  - Full-duplex – Both ends of the connection can send and receive simultaneously
  - Half-duplex – Only one end of the connection can send at a time
  - A common cause of performance issues on Ethernet links is when one port on the link operates at half-duplex and the other on full-duplex
- Auto-MDX
  - Detects the type of connection required and configures the interface accordingly
  - Helps reducing configuration errors



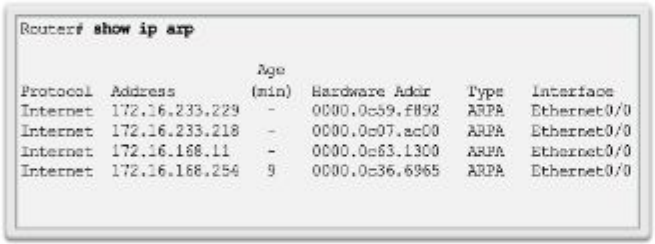
MAC and IP

- The combination of MAC and IP facilitate the End-to-End communication
- Layer 2 addresses are used to move the frame within the local network
- Layer 3 addresses are used to move the packets through remote networks
- Destination on Same Network
  - Physical address (MAC address) is used for Ethernet NIC to Ethernet NIC communications on the same network
- Destination on Remote Network
  - Logical address (IP address) is used to send the packet from the original source to the final destination



ARP

- Introduction to ARP
  - ARP allows the source to request the MAC address of the destination
  - The request is based upon the layer 3 address of the destination (known by the source)
- ARP Functions
  - Resolving IPv4 addresses to MAC addresses
  - Maintaining a table of mappings
  - ARP uses ARP Request and ARP Reply to perform its functions.
- Removing Entries from an ARP Table
  - Entries are removed from the device's ARP table when its cache timer expires
  - Cache timers are OS dependent
  - ARP entries can be manually removed via commands
- ARP Tables
  - On IOS: show ip arp
  - On Windows PCs: arp -a



Command Line Utilities

arp - is a utility for managing ARP table

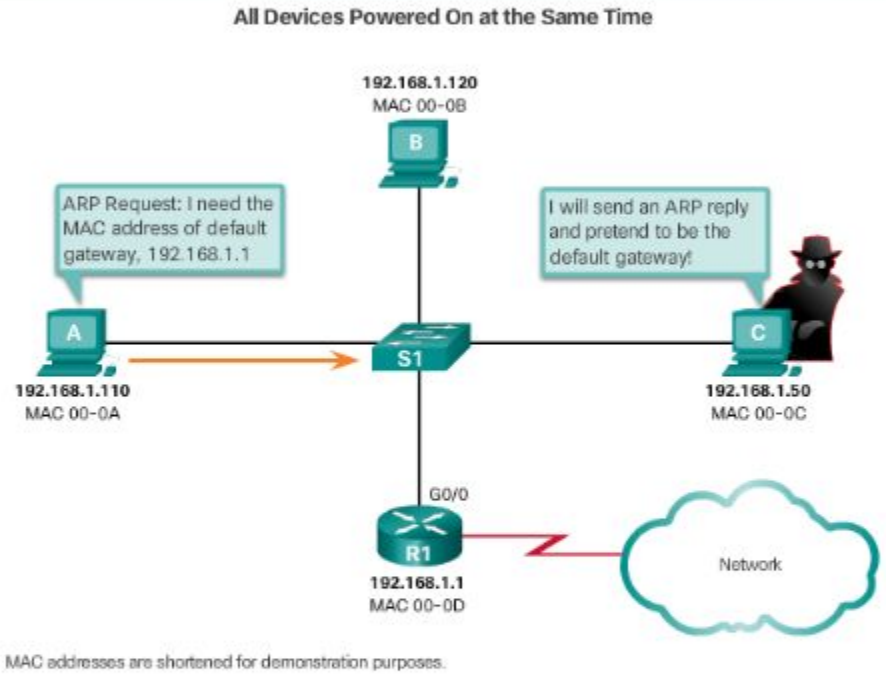
Parameters:

- /? - *help*
- -a - *show all records*
- -s - *add static record*
- -d - *delete record*

```
C:\Users\Parallels>arp /?

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

  -a            Displays current ARP entries by interrogating the current
                protocol data.  If inet_addr is specified, the IP and Physical
                addresses for only the specified computer are displayed.  If
                more than one network interface uses ARP, entries for each ARP
                table are displayed.
  -g            Same as -a.
  -v            Displays current ARP entries in verbose mode.  All invalid
                entries and entries on the loop-back interface will be shown.
  inet_addr     Specifies an internet address.
  -N if_addr    Displays the ARP entries for the network interface specified
                by if_addr.
  -d            Deletes the host specified by inet_addr. inet_addr may be
                wildcarded with * to delete all hosts.
  -s            Adds the host and associates the Internet address inet_addr
                with the Physical address eth_addr.  The Physical address is
                given as 6 hexadecimal bytes separated by hyphens. The entry
                is permanent.
  eth_addr      Specifies a physical address.
  if_addr       If present, this specifies the Internet address of the
                interface whose address translation table should be modified.
                If not present, the first applicable interface will be used.
Example:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Adds a static entry.
  > arp -a                                    .... Displays the arp table.
```

ARP Issues

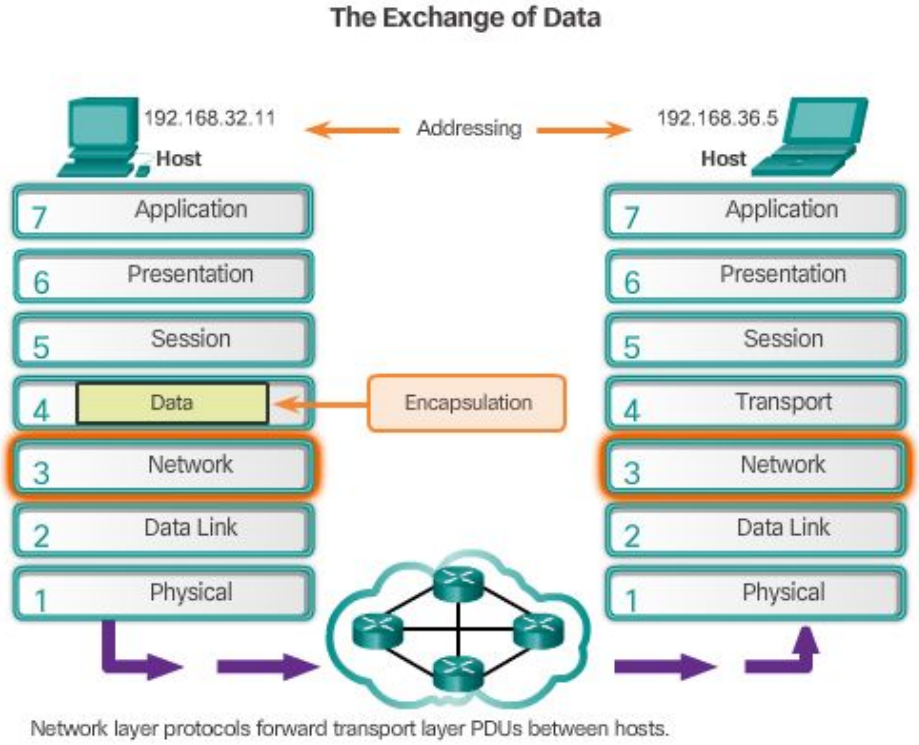
- ARP Broadcasts
  - ARP requests can flood the local segment
- ARP Spoofing
  - Attackers can respond to requests and pretend to be providers of services. Example: default gateway



Internet Protocol

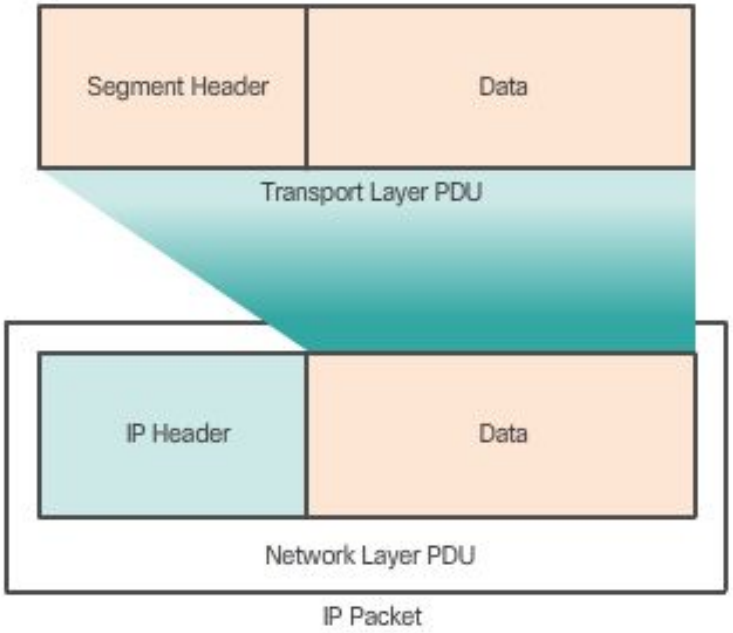
Network Layer in Communications

- The Network Layer
  - End to End Transport processes
  - Addressing end devices
  - Encapsulation
  - Routing
  - De-encapsulating
- Network Layer Protocols
  - IPv4
  - IPv6



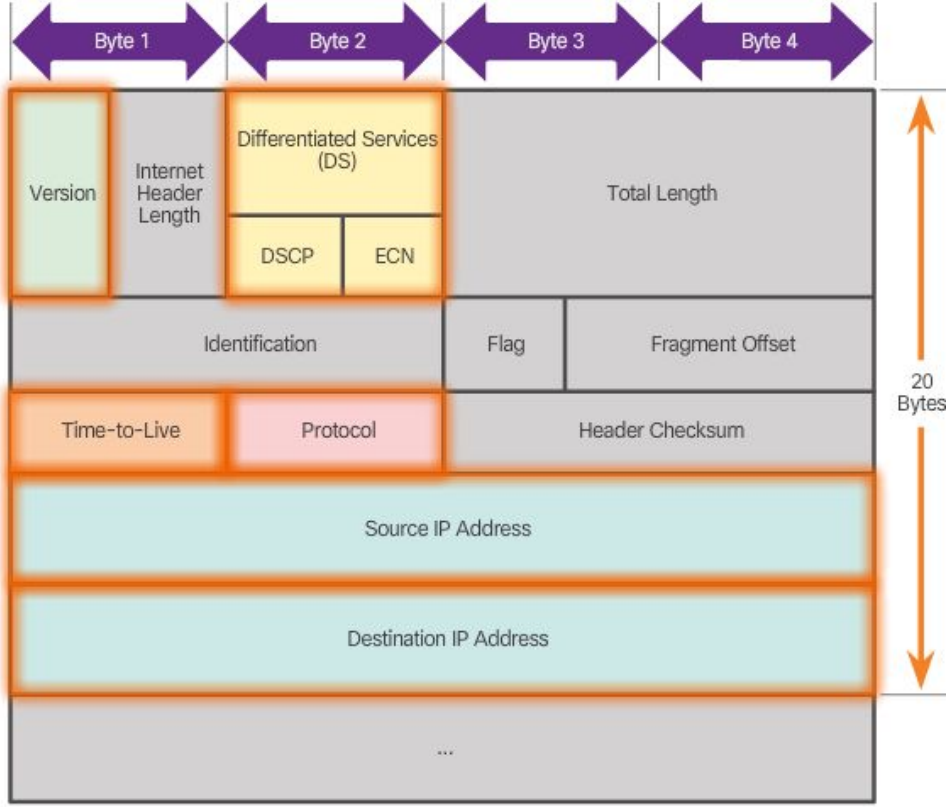
Characteristics of the IP Protocol

- Encapsulating IP
  - Segments are encapsulated into IP packets for transmission
  - The network layer adds a header so packets can be routed to the destination
- IP - Connectionless
  - Sender doesn't know if the receiver is listening or the message arrived on time.
  - Receiver doesn't know data is coming
- IP – Best Effort Delivery
  - No guarantees of delivery are made
- IP – Media Independent
  - IP can travel over different types of media



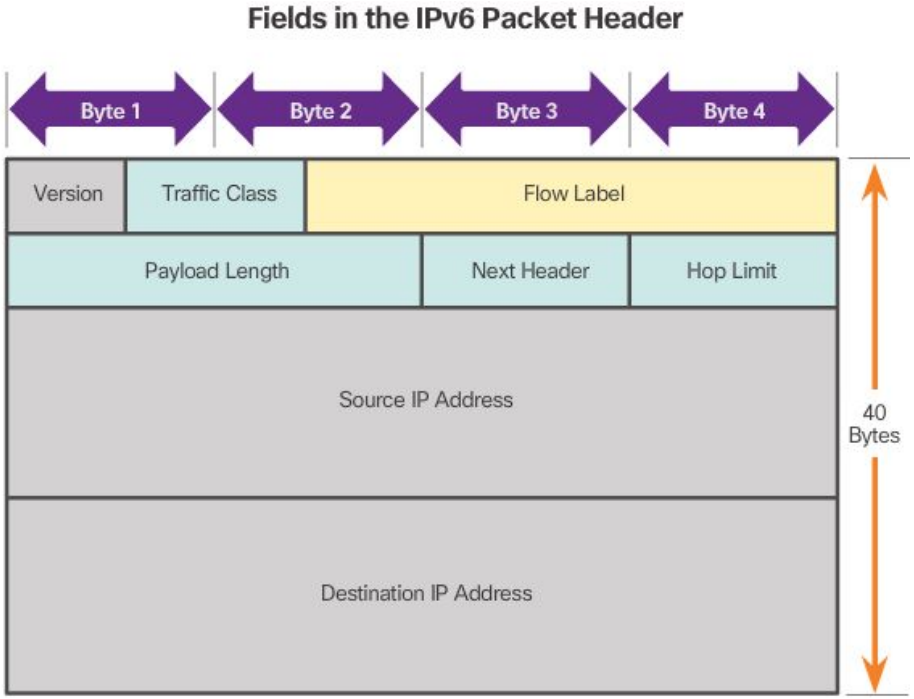
IPv4 Packet

- Version = 0100
- DS = Packet Priority
- TTL = Limits life of Packet
- Protocol = Upper layer protocol such as TCP
- Source IP Address = source of packet
- Destination IP Address = destination of packet



IPv6 Packet

- Limitations of IPv4
  - IP address depletion
  - Internet routing table expansion
  - Lack of end-to-end connectivity
- Introducing IPv6
  - Increased address space
  - Improved packet handling
  - Eliminates the need for NAT
- Encapsulating IPv6
  - Simplified header format
  - No checksum process requirement
  - More efficient Options Header mechanism
  - Flow Label field makes it more efficient
- IPv6 Packet Header
  - Version = 0110



Time for questions.

Thank You!

For more information, please contact:
Dmitry Lukashonok
Lead Software Testing Engineer
EPAM Systems, Inc.

Dmitry_lukashonok@epam.com