LAN Technologies

Lecture 3.2
Module 3. Networking Fundamentals

Serhii Zakharchenko

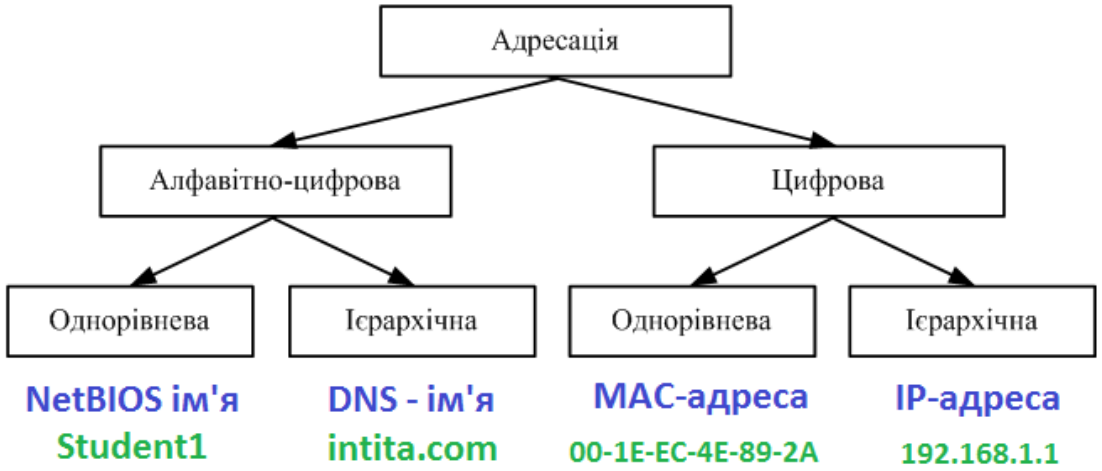
Agenda

- LAN addressing
- LAN technologies
- LAN devices
- Q&A

LAN addressing

Varieties of addresses in computer networks

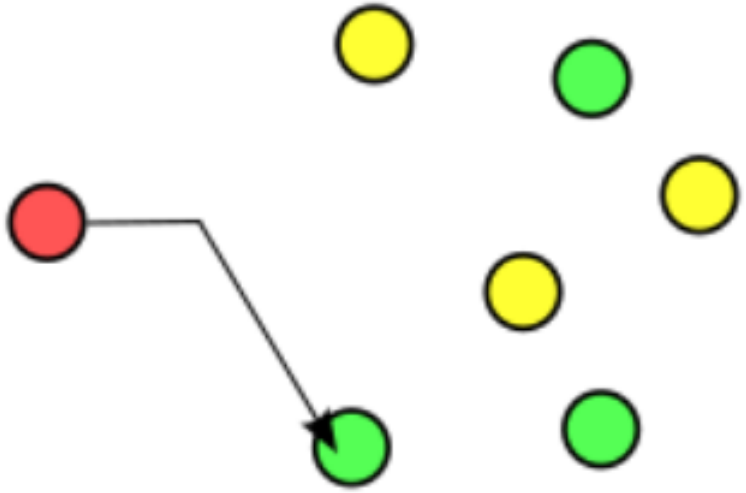
- **Single-level (flat) addresses** - used to deliver data on the local network. Example - physical address or MAC - address.
- **Hierarchical** - used to deliver data within a global network, such as the Internet. An example is an IP address.
- **Numeric addresses** - used by **equipment** to deliver data over the network. Examples: MAC address, IP address.
- **Alphanumeric** - used by **users** to access local or remote resources. Examples: NetBIOS names and DNS names.



- **Level 2 addresses** of the OSI model - are used by the equipment for data delivery in a local area network. Example: MAC address.
- **Level 3 addresses** of the OSI model - used by equipment to deliver data outside the local network. Example: IP address.
- OSI **Level 4 addresses** are used to identify programs that send or receive data over a network. Example: TCP and UDP ports.

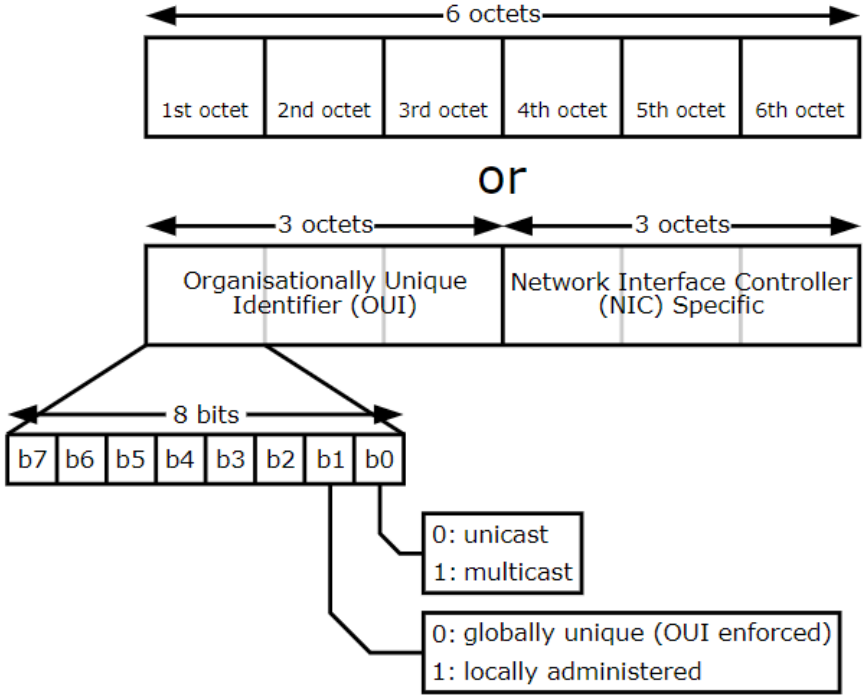
Message Delivery Address Classification

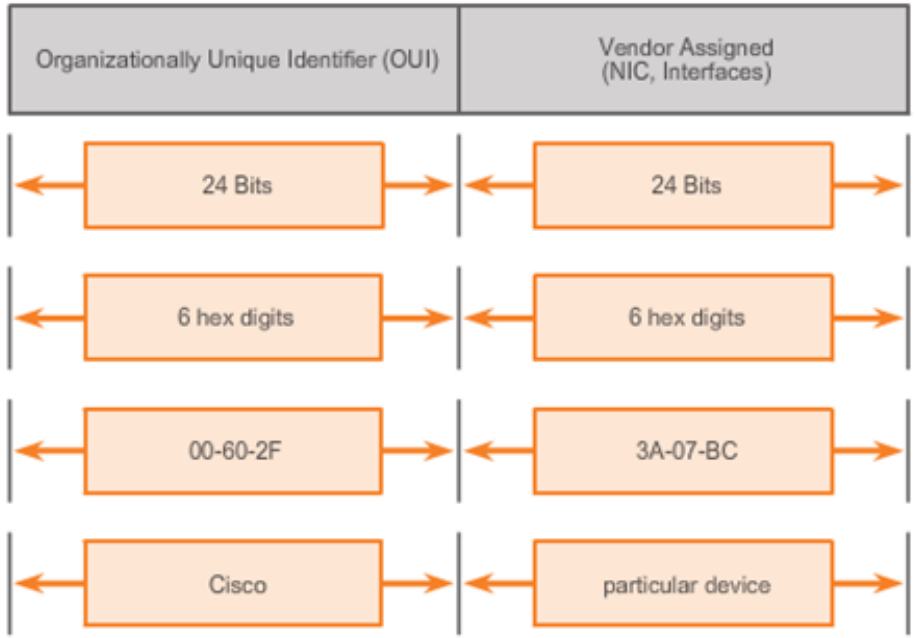
- Unicast
- Multicast
- Broadcast
- Anycast



MAC Address: LAN networking Identity

- Layer 2 MAC address is a 48-bit binary value expressed as 12 hexadecimal digits
- IEEE requires a vendor to follow two simple rules:
  - Must use that vendor's assigned OUI as the first 3 bytes
  - All MAC addresses with the same OUI must be assigned a unique value in the last 3 bytes





MAC Address Representations

```
C:\Users\Cep3a>getmac

Физический адрес    Имя транспорта
=================== ==========================================================
38-DE-AD-A1-B5-44   \Device\Tcpip_{6B7EC7A3-724C-4FB1-BCF4-AC9C10350BE9}
38-DE-AD-A1-B5-48   Носитель отключен
0A-00-27-00-00-05   \Device\Tcpip_{29E360BA-8F99-4563-94E3-F3BAC6101261}
```

```
C:\>ipconfig/all

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : example.com
   Description . . . . . . . . . . . : Intel(R) Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-21-CC-BA-44-C4
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.1.67(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Monday, November 26, 2012 12:14:48 PM
   Lease Expires . . . . . . . . . . : Saturday, December 01, 2012 12:15:02 AM
   Default Gateway . . . . . . . . . : 192.168.1.254
   DHCP Server . . . . . . . . . . . : 192.168.1.254
   DNS Servers . . . . . . . . . . . : 192.168.1.254
```

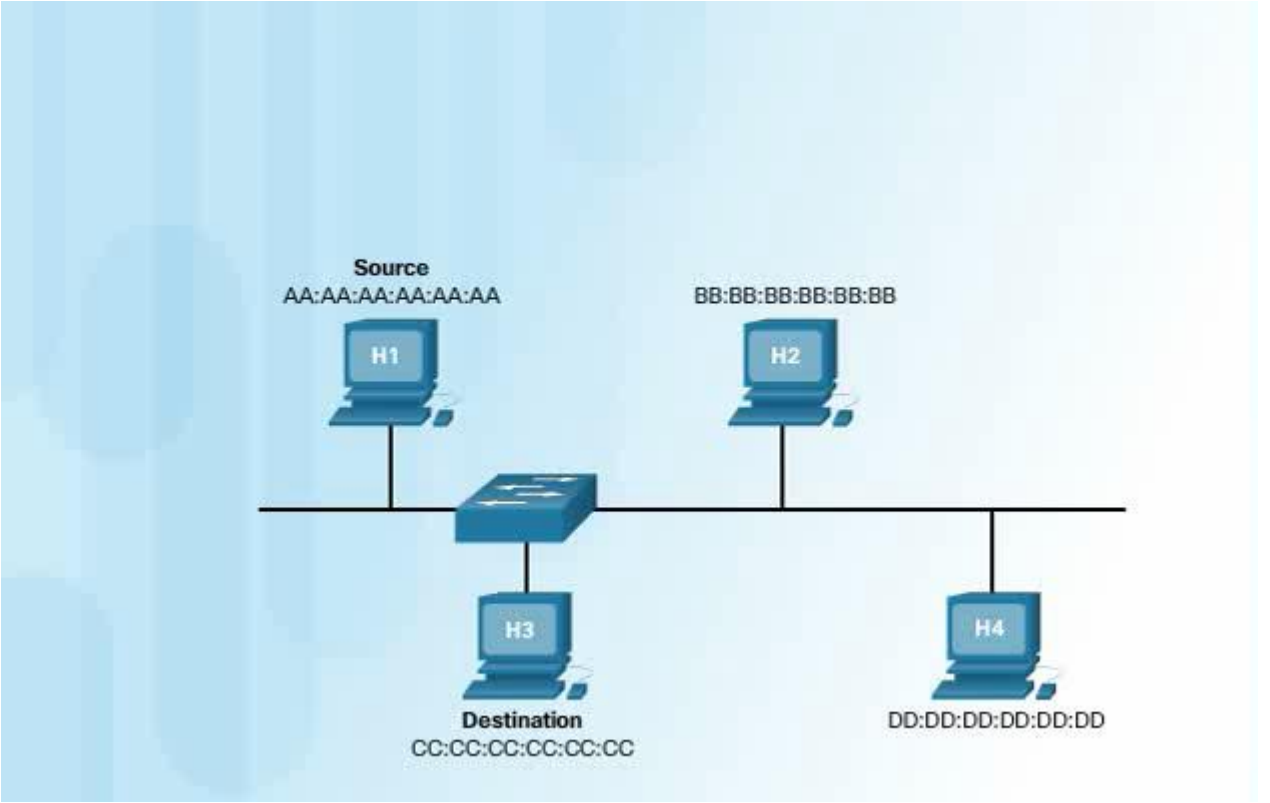
With Dashes 00-60-2F-3A-07-BC

With Colons 00:60:2F:3A:07:BC

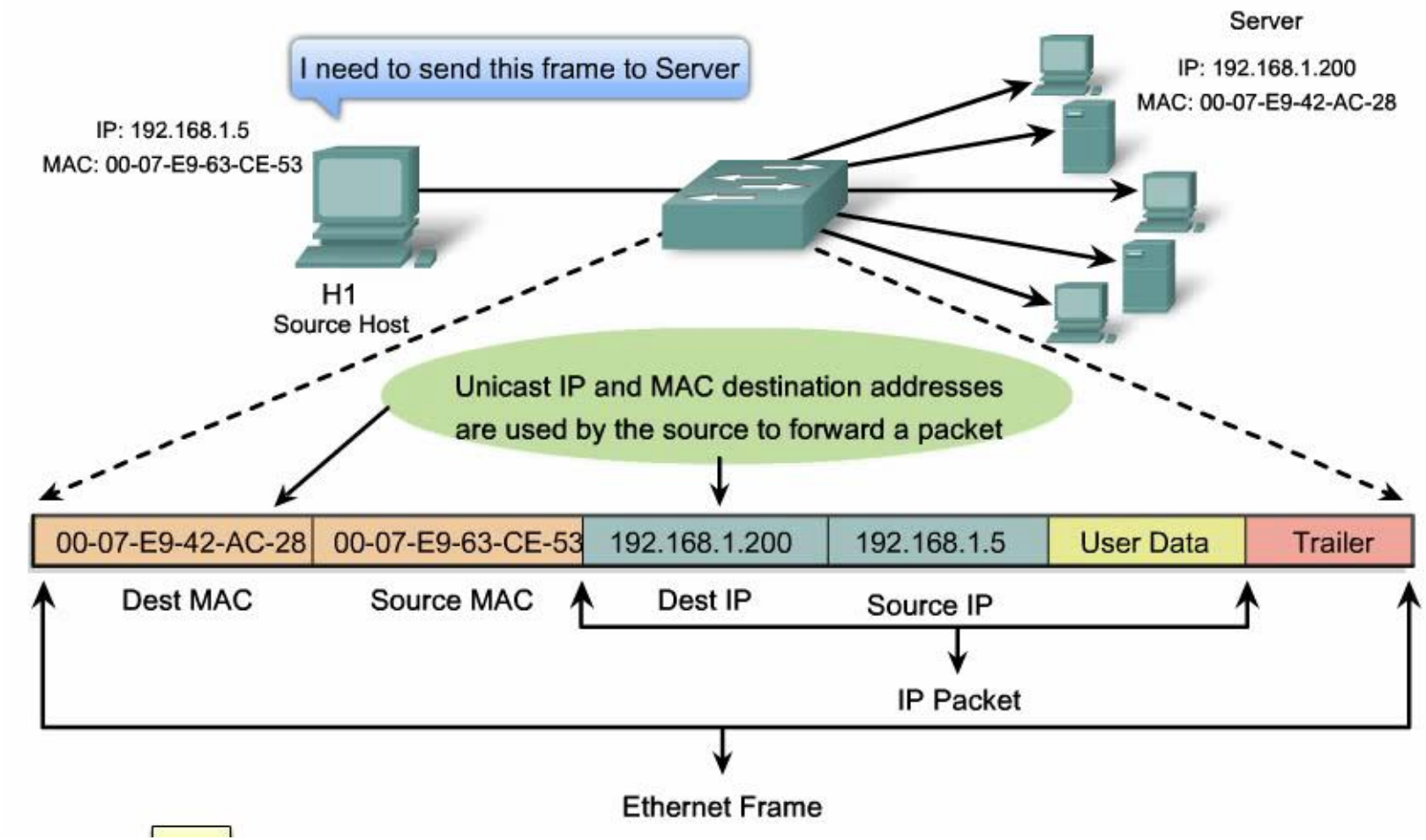
With Periods 0060.2F3A.07BC

Frame Processing

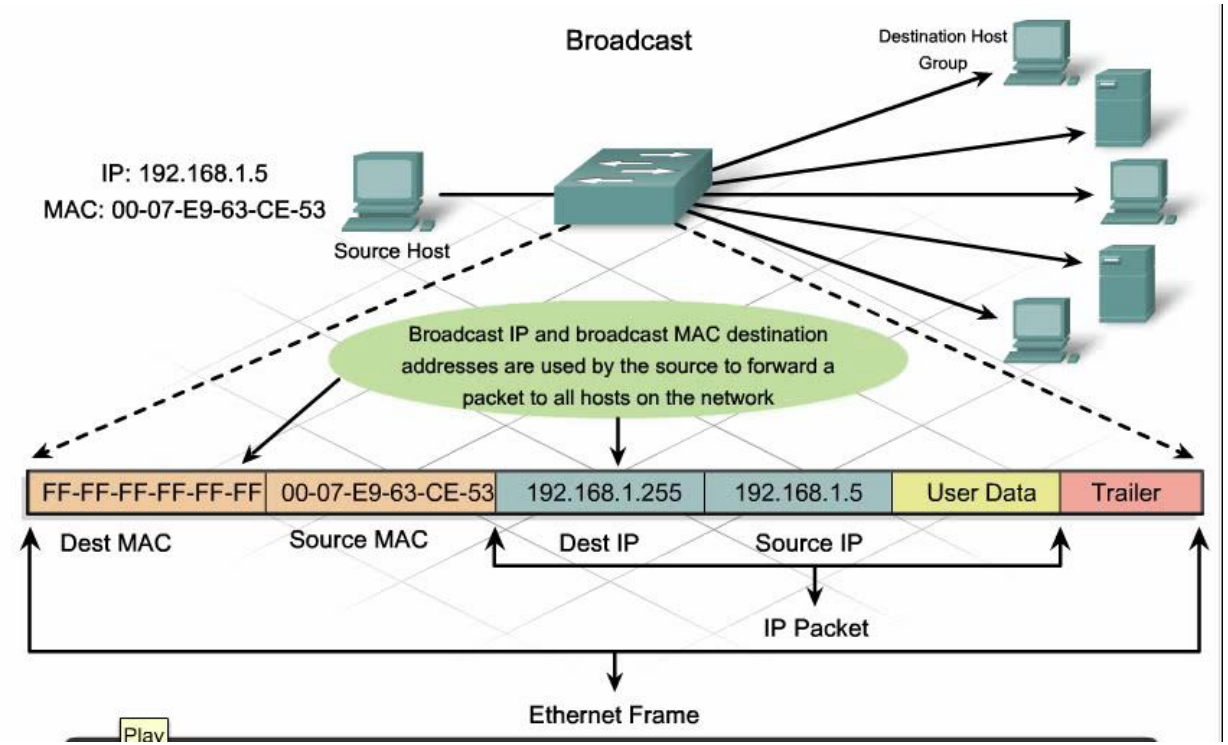
- MAC addresses assigned to workstations, servers, printers, switches, routers and other.
- Forwarded message to an LAN network, attaches header information to the packet, contains the source and destination MAC address
- Each NIC views information to see if the destination MAC address in the frame matches the device's physical MAC address stored in RAM
- No match, the device discards the frame
- Matches the destination MAC of the frame, the NIC passes the frame up the OSI layers, where the decapsulation process takes place

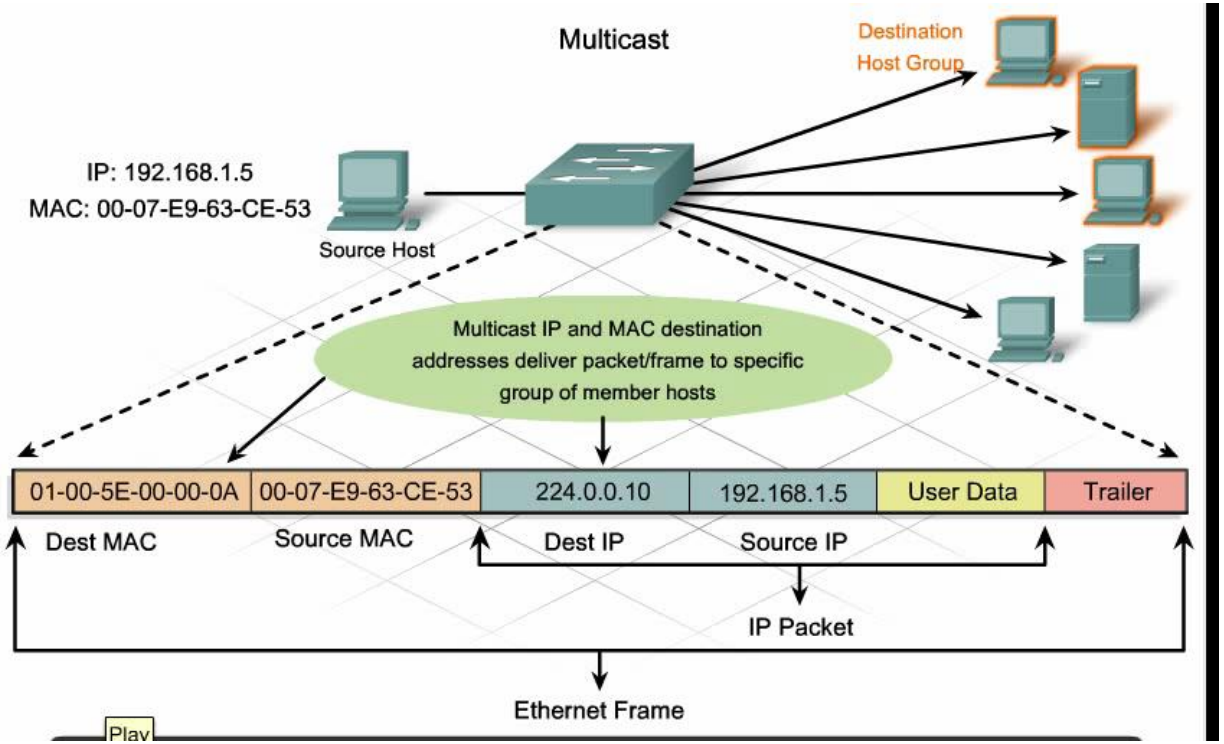


Ethernet Unicast



Ethernet Broadcast and Multicast





IP address (IPv4)

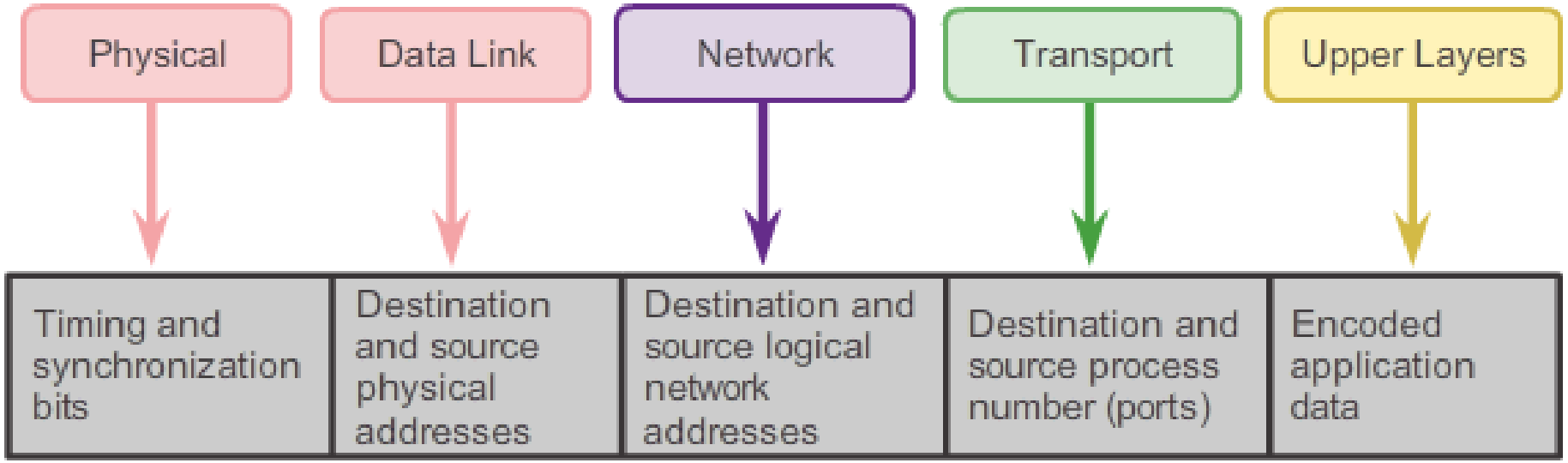
- Determined by the computer owner or Internet access provider
- Contains 4 bytes and is served in decimal or binary form
- Command to determine the IP address: **ipconfig**

192	.	168	.	10	.	1
11000000		10101000		00001010		00000001

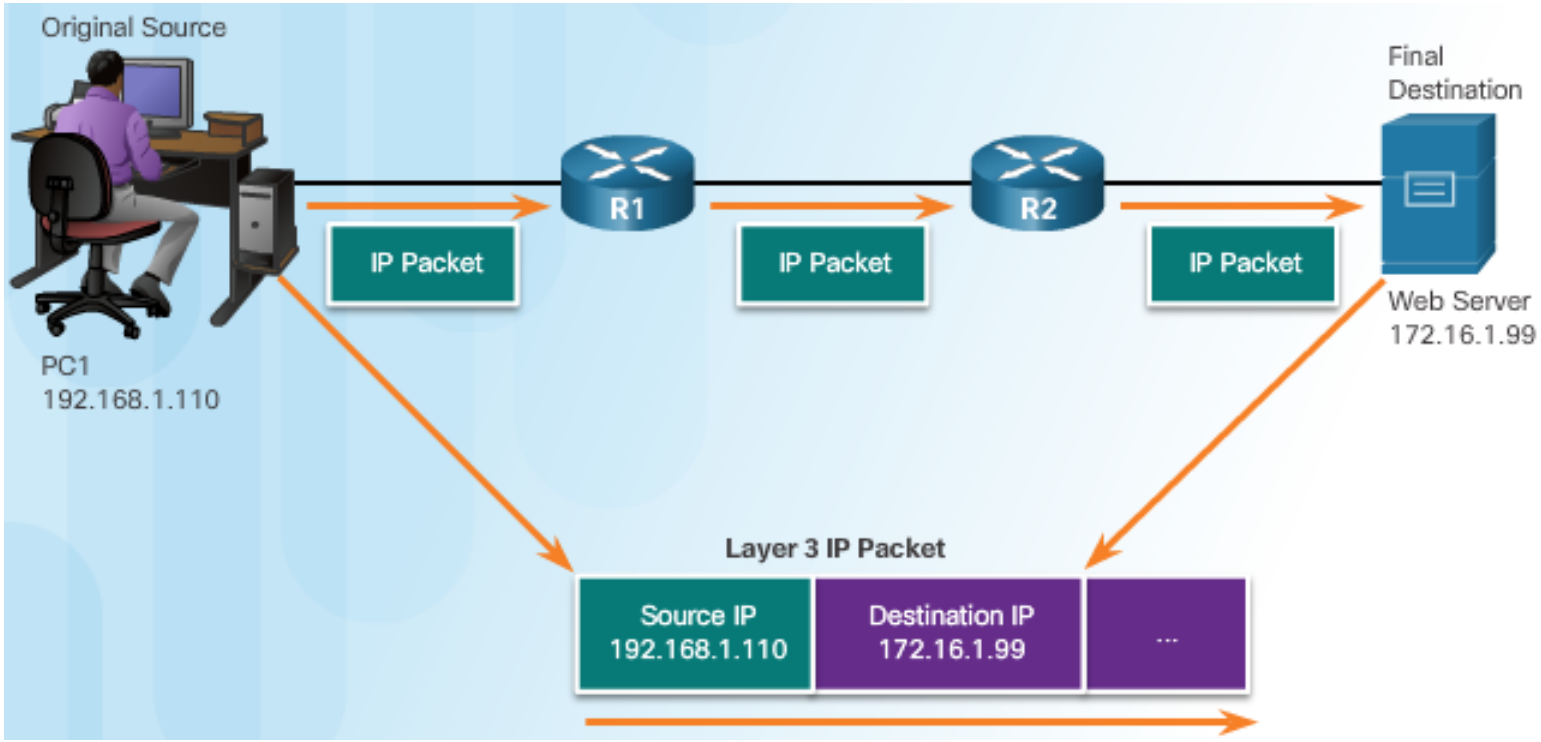
The computer using this IP address is on network 192.168.10.0.

Network addressing

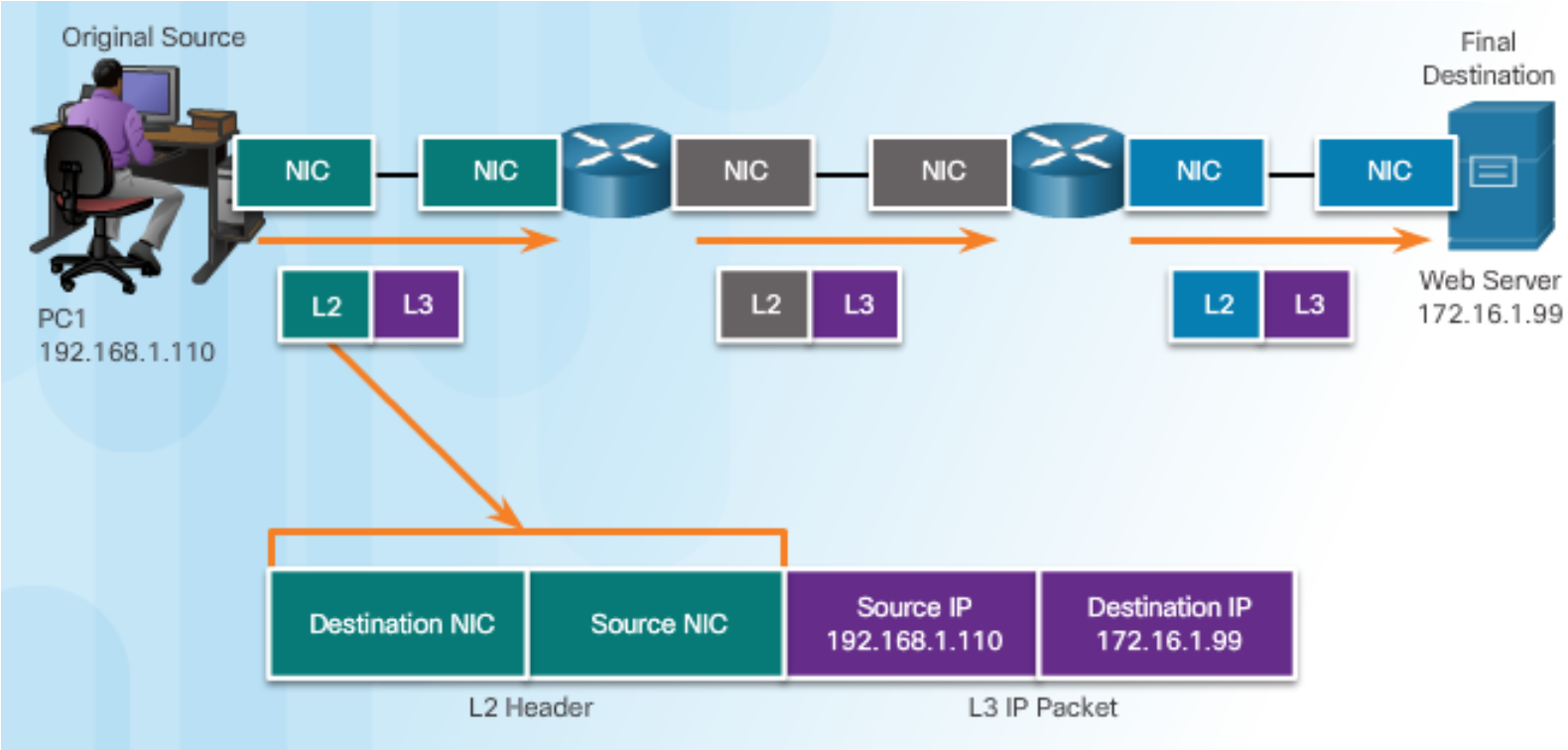
- The **network layer** and **data link layer** are responsible for delivering the data from the source device or sender, to the destination device or receiver.
- **Network layer source and destination addresses** - Responsible for delivering the IP packet from the original source to the final destination, either on the same network or to a remote network.
- **Data link layer source and destination addresses** – Responsible for delivering the data link frame from one network interface card (NIC) to another NIC on the same network.



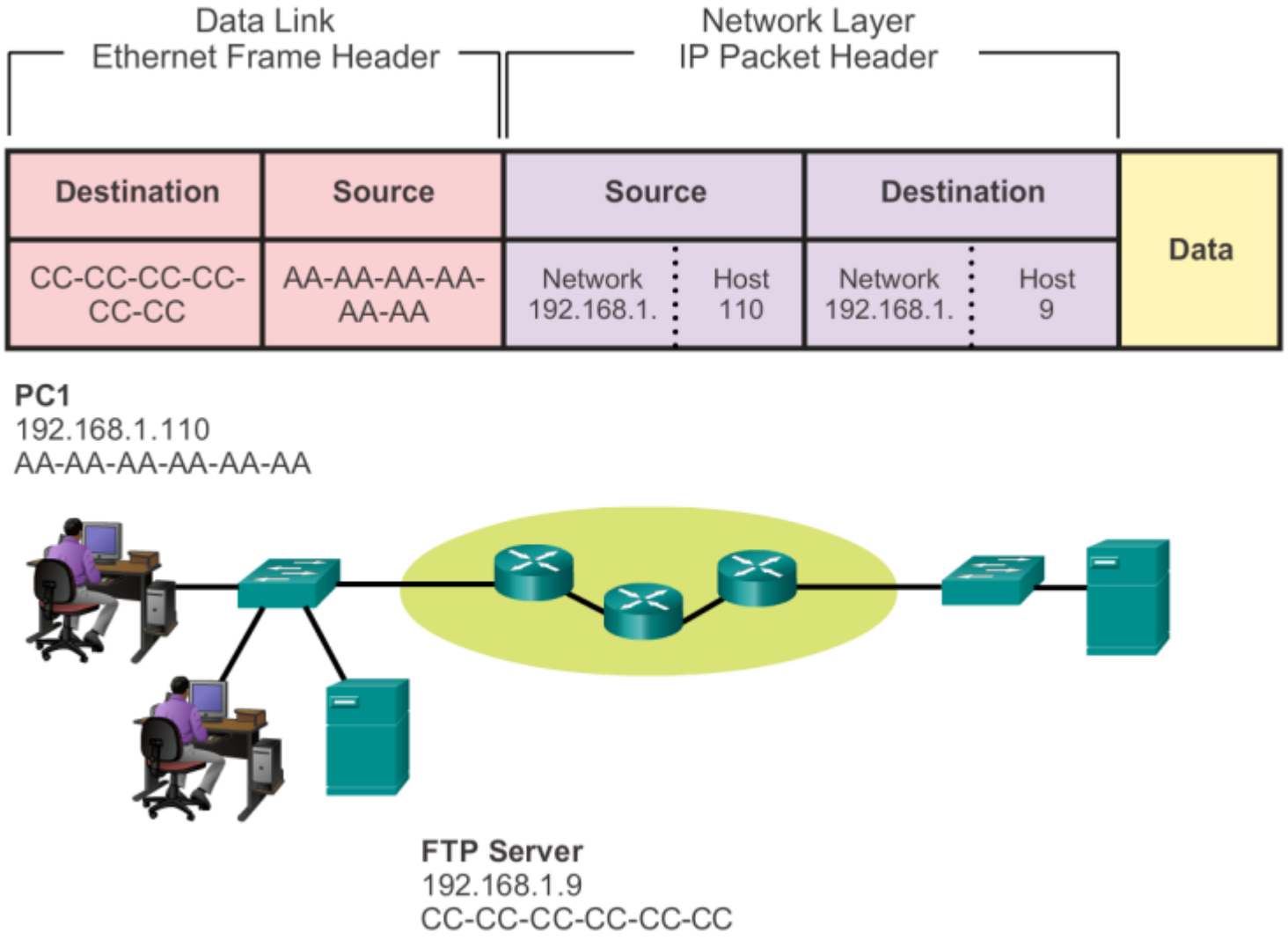
Network Layer Addresses



Data Link Layer Addresses

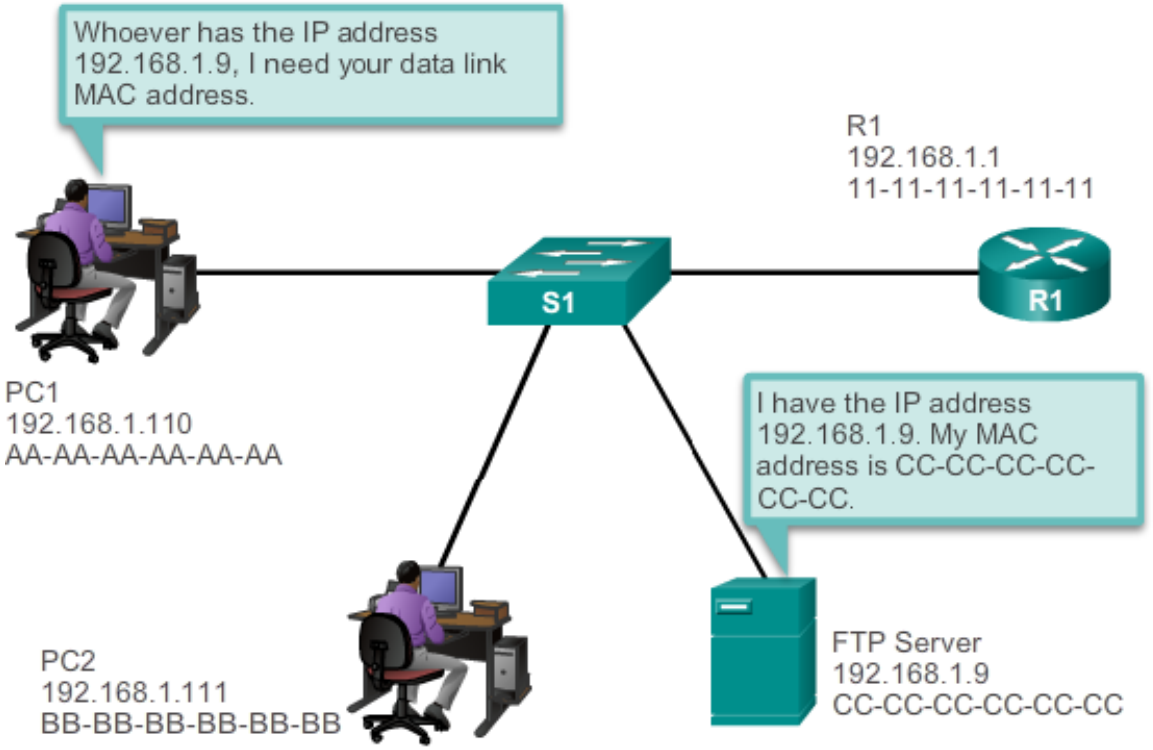


Communicating with Device / Same Network

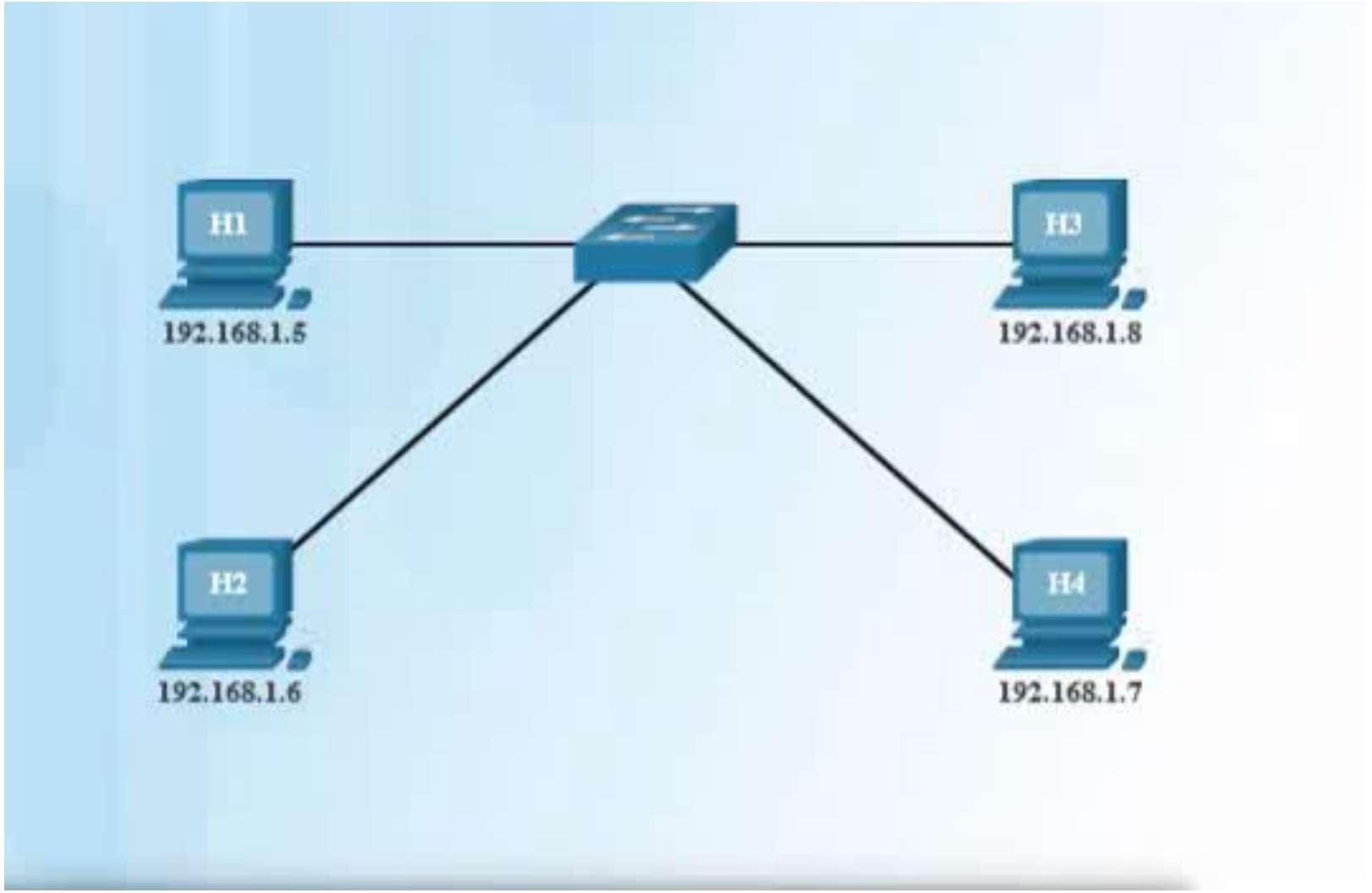


Address Resolution Protocol (ARP)

- Most network applications rely on the logical IP address of the destination to identify the location of the communicating hosts. The data link **MAC address is required** to deliver the encapsulated IP packet inside the Ethernet frame across the network to the destination.
- The sending host uses a protocol called **Address Resolution Protocol** (ARP) to discover the MAC address of any host on the same local network.
- The sending host sends an ARP Request message to the entire LAN in broadcast message.
- The ARP Request contains the IP address of the destination device.
- Only the device with the IP address contained in the ARP Request responds with an ARP Reply. The ARP Reply includes the MAC address

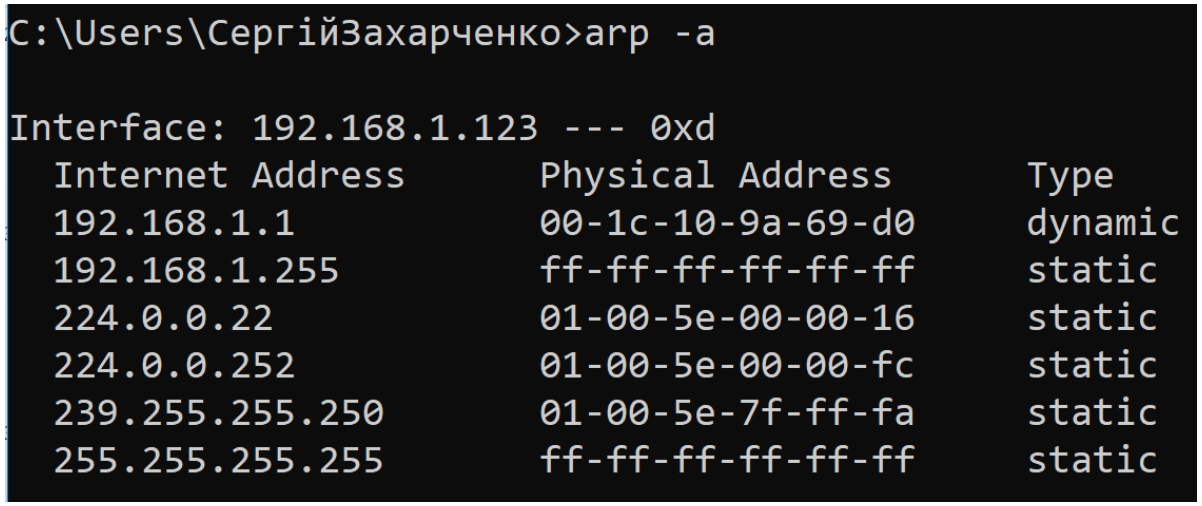


Introduction to ARP



ARP Cash

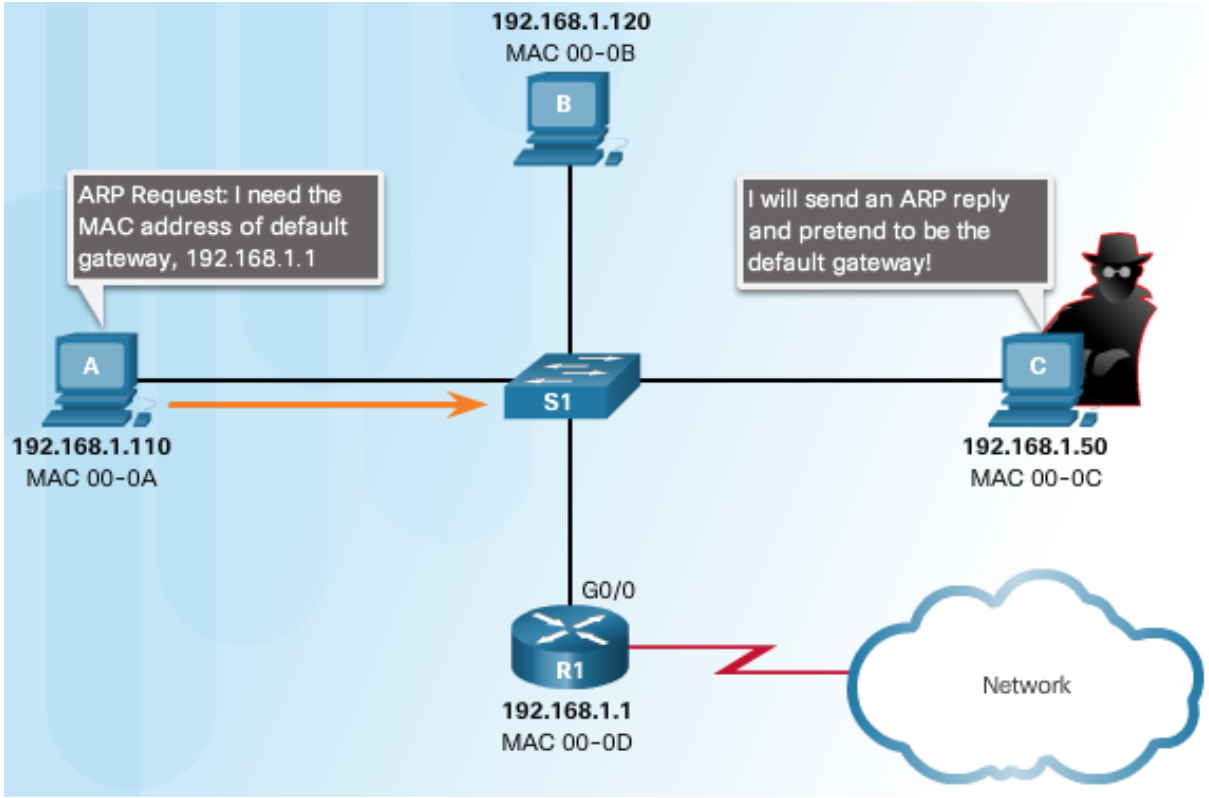
- ARP saves the results of requests in ARP cash. For review ARP cash in Windows cli command: **arp –a**. For ARP cash clearing: **arp –d**
- For each device, an ARP cache timer removes ARP entries that have not been used for a specified period of time. The times differ depending on the device's operating system. For example, some Windows operating systems store ARP cache entries for 2 minutes.
- Commands may also be used to manually remove all or some of the entries in the ARP table.
- After an entry has been removed, the process for sending an ARP request and receiving an ARP reply must occur again to enter the map in the ARP table.



How ARP Can Create Problems

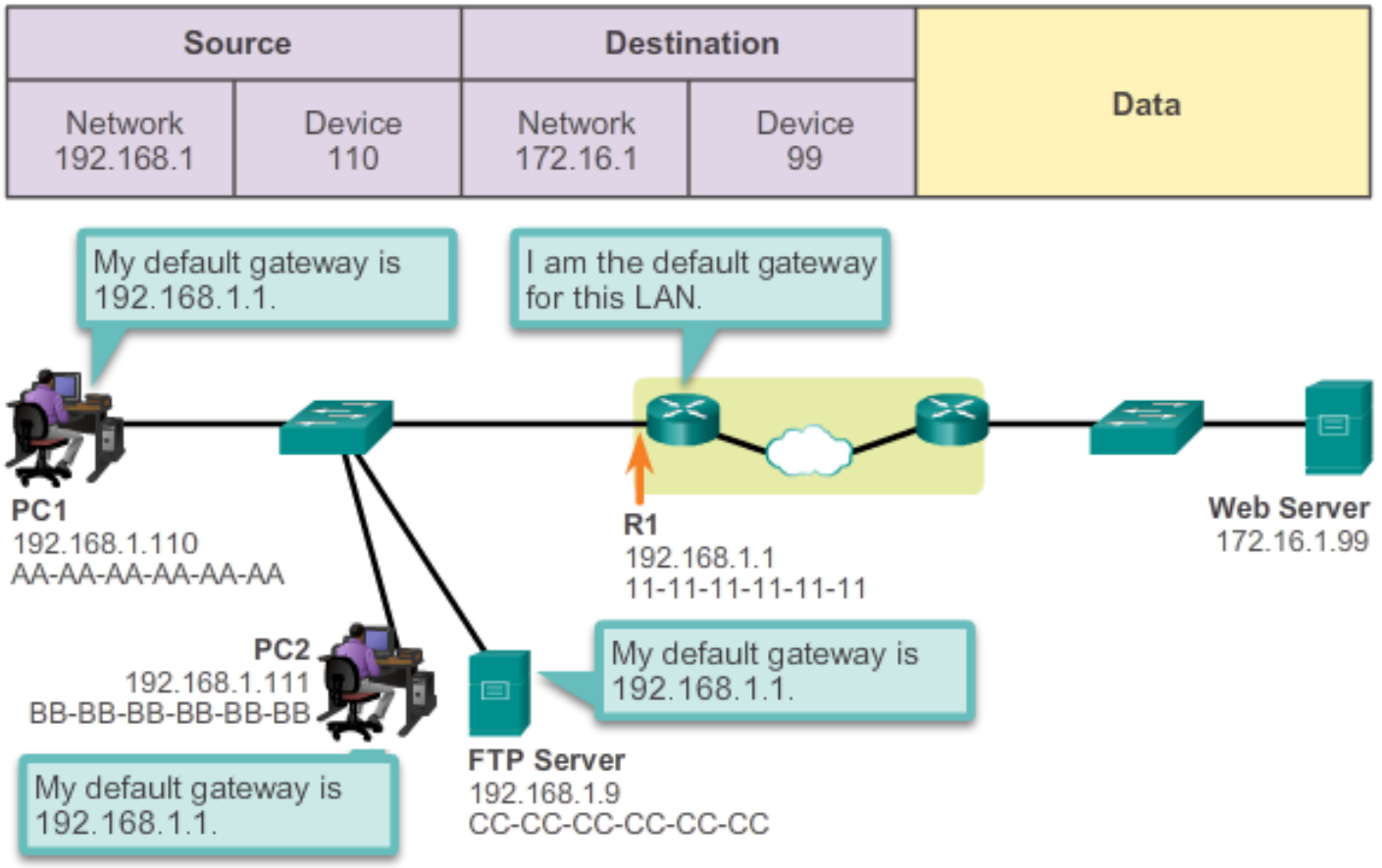
- **Overhead on the Media -** As a broadcast frame, an ARP request is received and processed by every device on the local network.
- **Security -** In some cases, the use of ARP can lead to a potential security risk. ARP spoofing, or ARP poisoning, is a technique used by an attacker to inject the wrong MAC address association into a network by issuing fake ARP requests.

- **ARP spoofing** technique used by an attacker to reply to an ARP request for an IPv4 address belonging to another device, such as the default gateway.
- The attacker sends an ARP reply with its own MAC address. The receiver of the ARP reply will add the wrong MAC address to its ARP table and send these packets to the attacker.

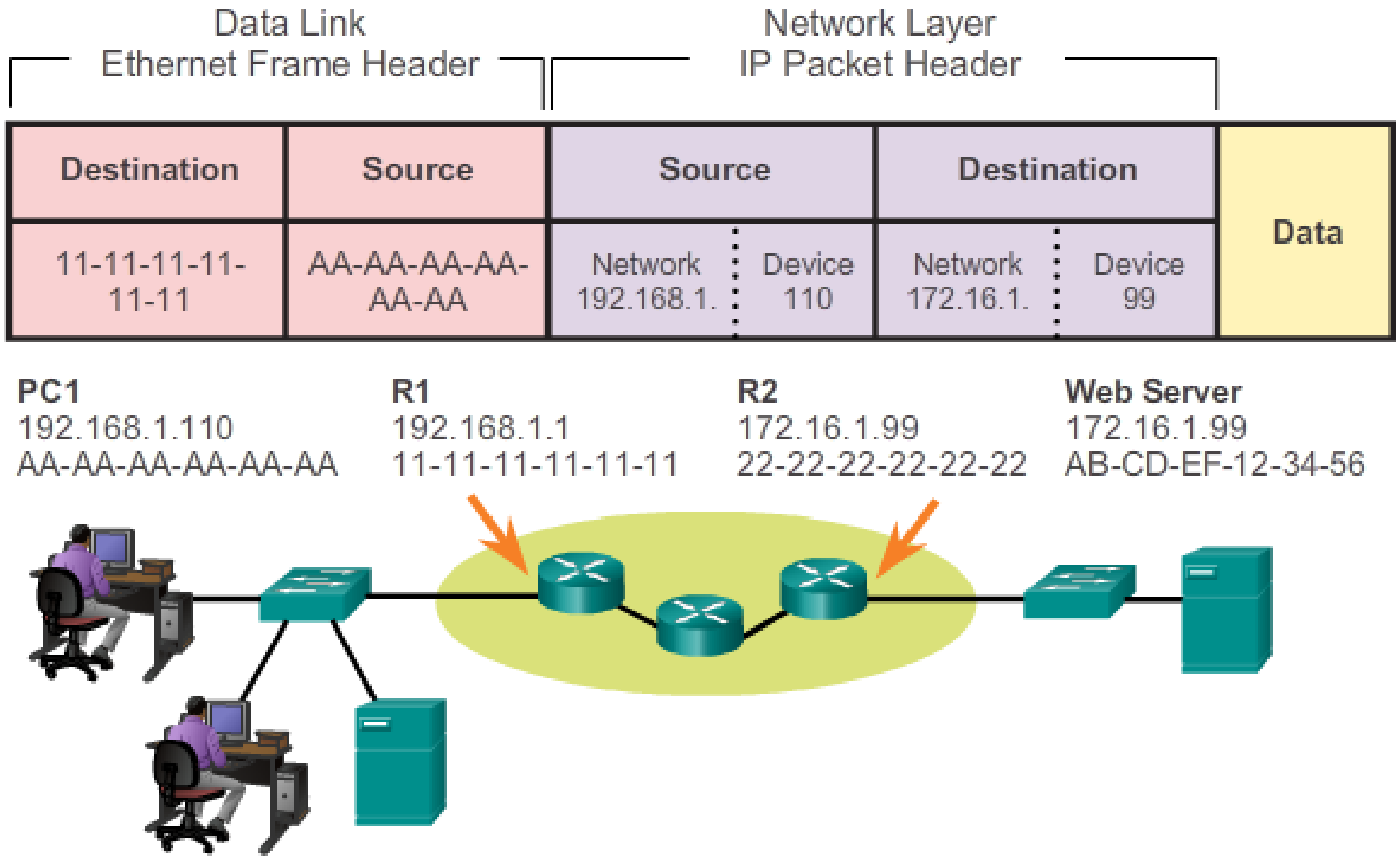


Accessing Remote Resources

- When a host needs to send a message to a remote network, it must use the router, also known as the **default gateway**. The default gateway is the IP address of an interface on a router on the same network as the sending host.
- It is important that the address of the **default gateway** be configured on **each host** on the local network. If no default gateway address is configured in the host TCP/IP settings, or if the wrong default gateway is specified, messages addressed to hosts on remote networks cannot be delivered.



Communicating Device / Remote Network



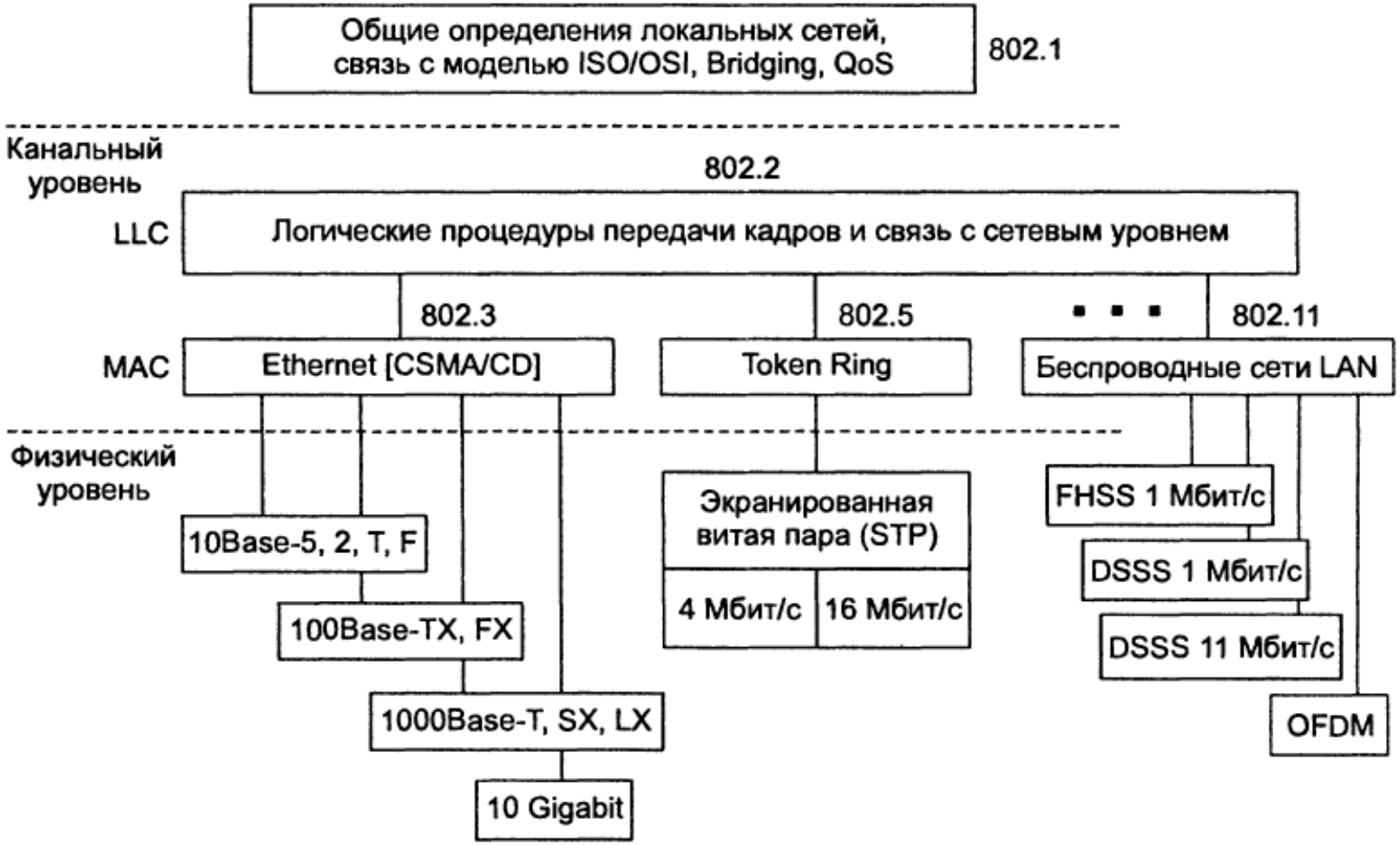
LAN technologies

IEEE 802 family standards

The IEEE 802 family of standards deals with local area networks and metropolitan area networks, including both wired and wireless:

- 802.1 Higher Layer LAN Protocols Working Group
- **802.3 Ethernet Working Group**
- **802.11 Wireless LAN Working Group**
- **802.15 Wireless Personal Area Network (WPAN) Working Group**
- 802.16 Broadband Wireless Access Working Group
- 802.18 Radio Regulatory TAG
- 802.22 Wireless Regional Area Networks
- 802.24 Smart Grid TAG

Standard 802.X



Ethernet

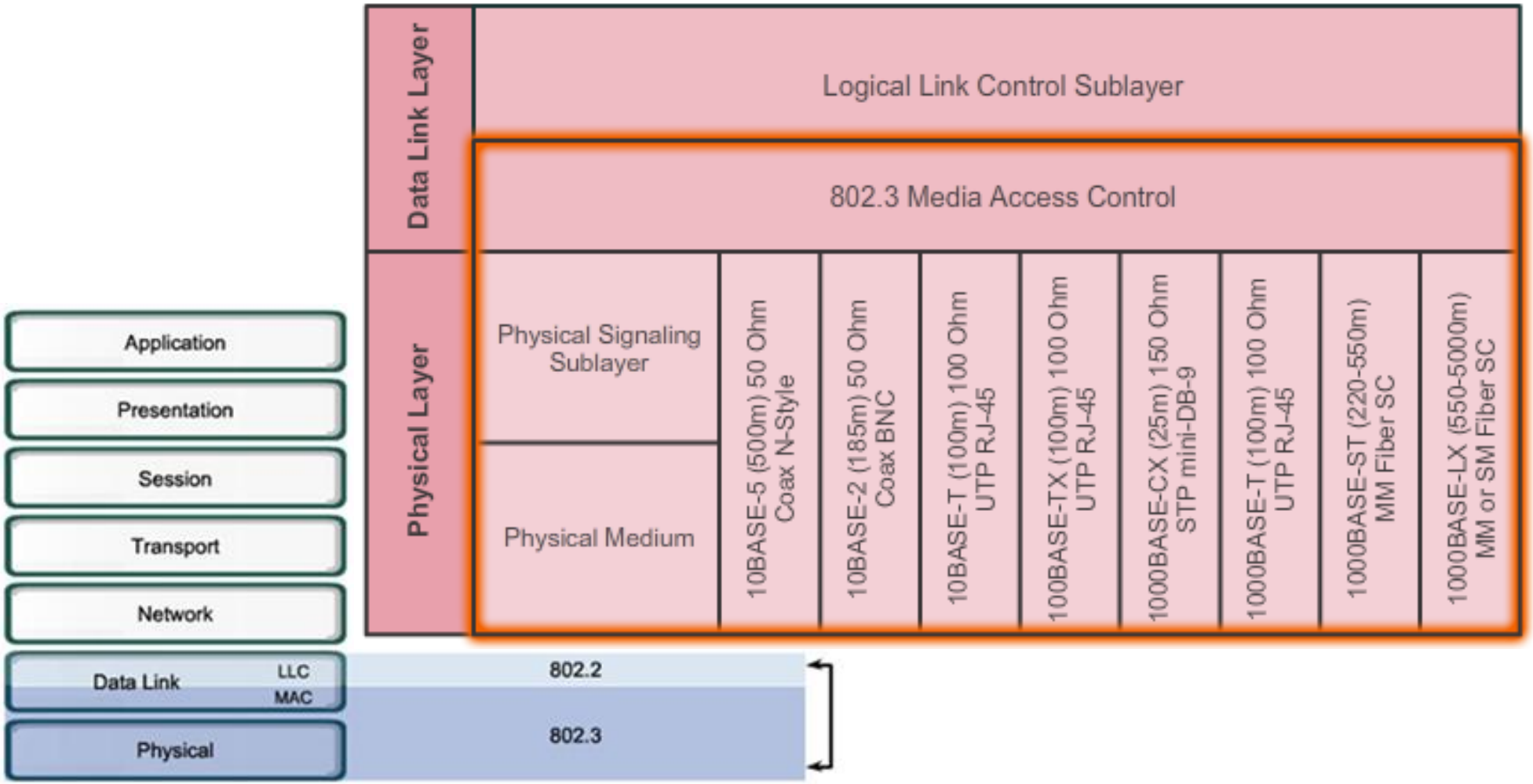
Ethernet –

- Most widely used LAN technology
- Operates in the data link layer and the physical layer
- Family of networking technologies that are defined in the IEEE 802.2 and 802.3 standards
- Supports data bandwidths of 10, 100, 1000, 10,000, 40,000, and 100,000 Mbps (100 Gbps)

Ethernet standards –

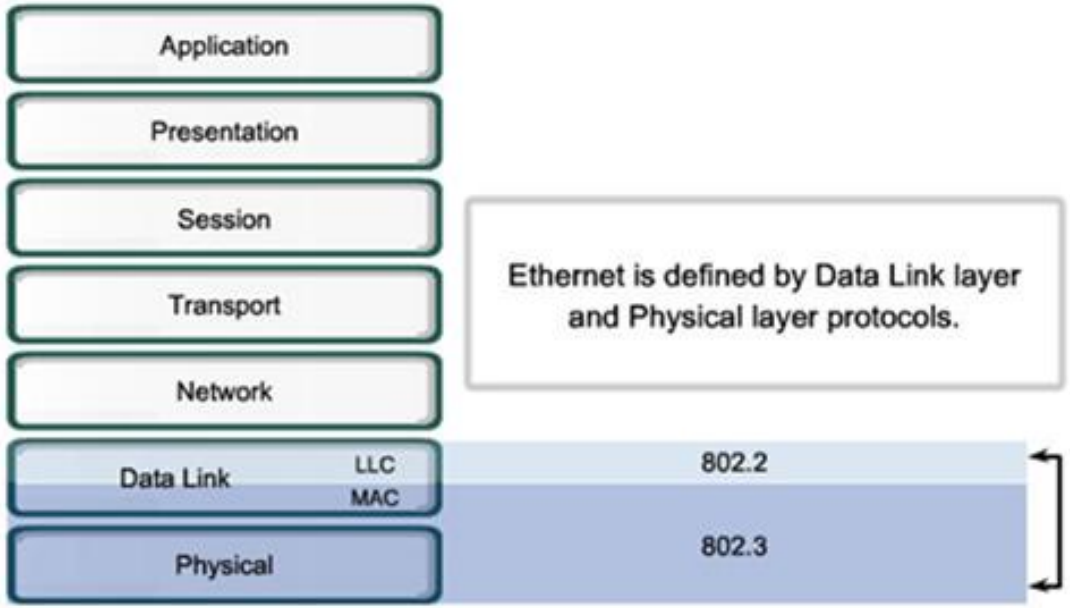
- Define Layer 2 protocols and Layer 1 technologies
- Two separate sub layers of the data link layer to operate - **Logical Link Control** (LLC) and the **Media Access Control** (MAC) sublayers

Ethernet


Data Link Layer
Logical Link Control Sublayer
802.3 Media Access Control
Physical Layer
Physical Signaling Sublayer
Physical Medium
10BASE-5 (500m) 50 Ohm Coax N-Style
10BASE-2 (185m) 50 Ohm Coax BNC
10BASE-T (100m) 100 Ohm UTP RJ-45
100BASE-TX (100m) 100 Ohm UTP RJ-45
1000BASE-CX (25m) 150 Ohm STP mini-DB-9
1000BASE-T (100m) 100 Ohm UTP RJ-45
1000BASE-ST (220-550m) MM Fiber SC
1000BASE-LX (550-5000m) MM or SM Fiber SC
Application
Presentation
Session
Transport
Network
Data Link
LLC
MAC
Physical
802.2
802.3

LLC and MAC Sublayers

- The Ethernet LLC sublayer handles the communication between the upper layers and the lower layers. This is typically between the networking software and the device hardware.
- The LLC sublayer takes the network protocol data, which is typically an IPv4 packet, and adds control information to help deliver the packet to the destination node.
- LLC is implemented in software, and its implementation is independent of the hardware. In a computer, the LLC can be considered the driver software for the NIC.



- MAC constitutes the lower sublayer of the data link layer.
- MAC is implemented by hardware, typically in the computer NIC.
- The specifics are specified in the IEEE 802.3 standards.

MAC Sublayer

Ethernet MAC sublayer has two primary responsibilities:

- **Data encapsulation**
  - Frame delimiting
  - Addressing
  - Error detection
- **Media access control**
  - Control of frame placement on and off the media
  - Media recovery

MAC Sublayer (Data encapsulation)

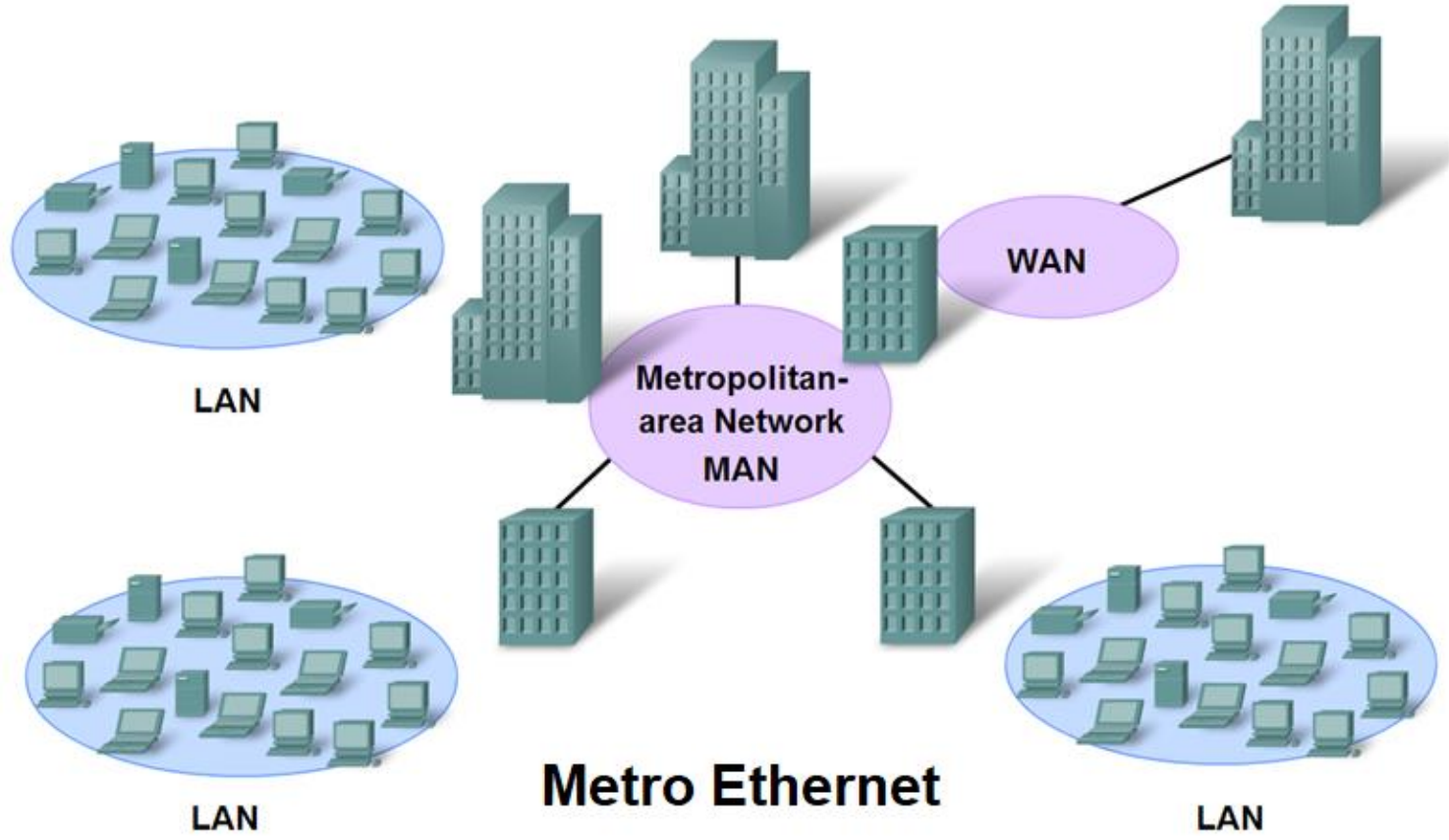
- **Frame delimiting** – identifies a group of bits that make up a frame, synchronization between the transmitting and receiving nodes
- **Addressing** – each Ethernet header added in the frame contains the physical address (MAC address) that enables a frame to be delivered to a destination node
- **Error detection** - each Ethernet frame contains a trailer with a cyclic redundancy check (CRC) of the frame contents

MAC Sublayer (Media Access Control)

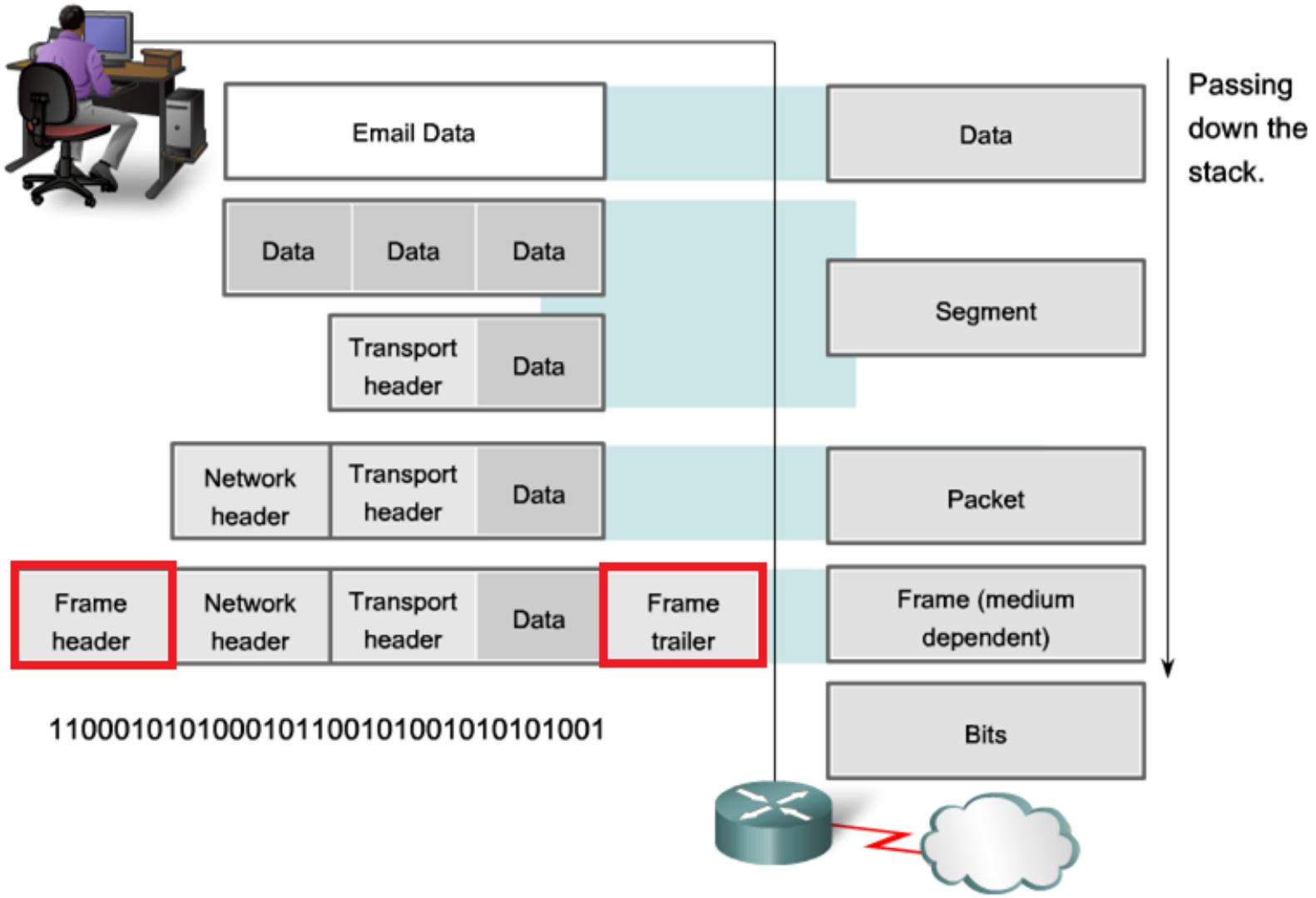
- Responsible for the placement of frames on the media and the removal of frames from the media
- Communicates directly with the physical layer
- If multiple devices on a single medium attempt to forward data simultaneously, the data will collide resulting in corrupted, unusable data
- Ethernet provides a method for controlling how the nodes share access through the use a **Carrier Sense Multiple Access** (CSMA) technology in **half-duplex** Ethernet LANs
- Today's Ethernet LANs use **full-duplex switches**, which allow multiple devices to send and receive simultaneously with no collisions.

Ethernet Evolution

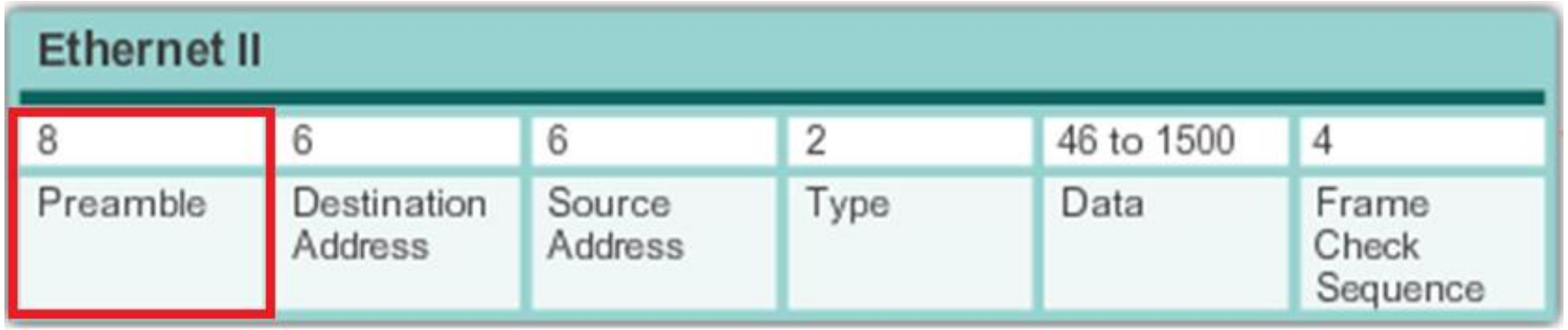
- Since the creation of Ethernet in **1973**, standards have evolved for specifying faster and more flexible versions of the technology.
- This ability for Ethernet to improve over time is one of the main reasons it has become so popular.
- Early versions of Ethernet were relatively slow at **10 Mbps**.
- The latest versions of Ethernet operate at **10 Gigabits** per second and faster.



Ethernet Encapsulation

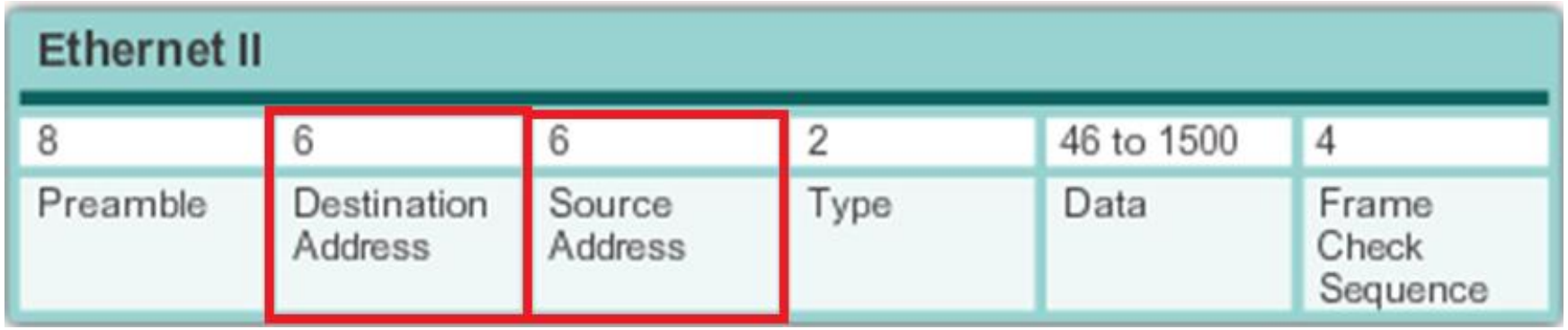


Ethernet Frame Fields



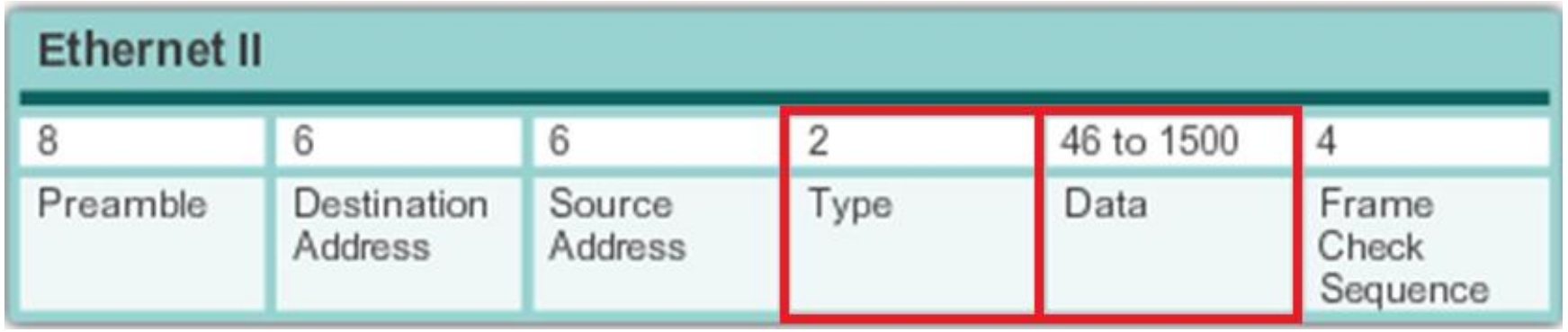
- The **Preamble** (7 bytes) and **Start Frame Delimiter** (SFD), also called the Start of Frame (1 byte), fields are used for synchronization between the sending and receiving devices.
- These first eight bytes of the frame are used to get the attention of the receiving nodes.
- Essentially, the first few bytes tell the receivers to get ready to receive a new frame.

Ethernet Frame Fields



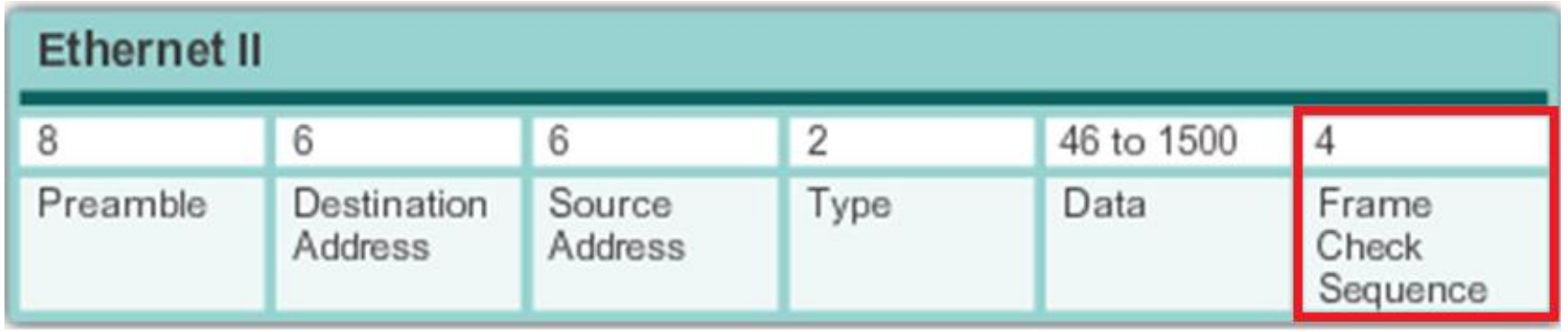
- **Destination MAC Address** - 6-byte field is the identifier for the intended recipient. This address is used by Layer 2 to assist devices in determining if a frame is addressed to them. The address in the frame is compared to the MAC address in the device. If there is a match, the device accepts the frame. Can be a **unicast**, **multicast** or **broadcast** address.
- **Source MAC Address** - 6-byte field identifies the frame's originating NIC or interface. Must be a **unicast** address.

Ethernet Frame Fields



- **Type** - 2-byte field identifies the upper layer protocol encapsulated in the Ethernet frame. Common values are, in hexadecimal, 0x800 for IPv4, 0x86DD for IPv6 and 0x806 for ARP.
- **Data** - This field (46 - 1500 bytes) contains the encapsulated data from a higher layer, which is a generic Layer 3 PDU, or more commonly, an IPv4 packet. All frames must be at least **64 bytes** long. If a small packet is encapsulated, additional bits called a pad are used to increase the size of the frame to this minimum size.

Ethernet Frame Fields



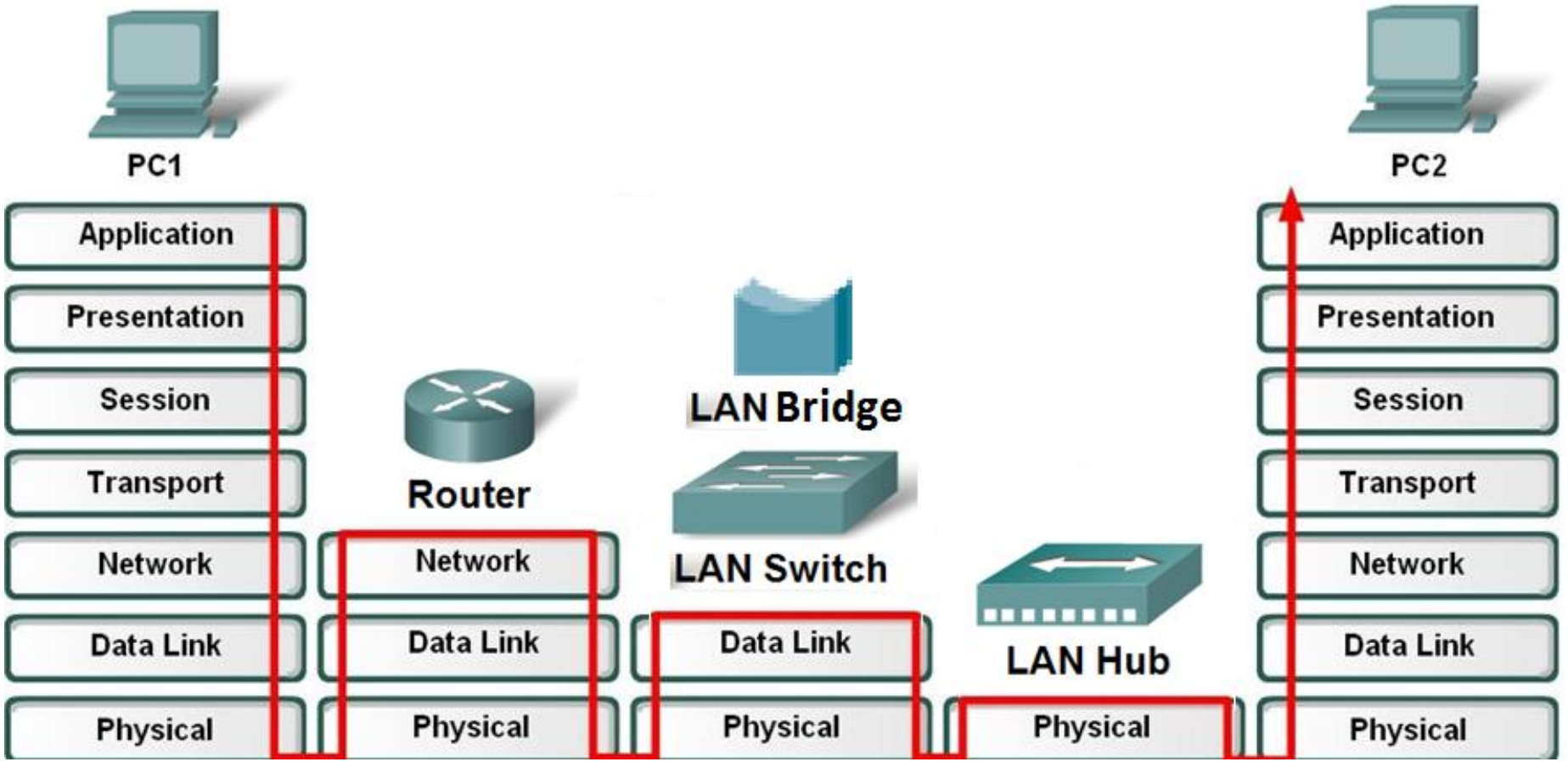
- The **Frame Check Sequence** (FCS) field (4 bytes) is used to detect errors in a frame. It uses a cyclic redundancy check (CRC).
- The sending device includes the results of a CRC in the FCS field of the frame.
- The receiving device receives the frame and generates a CRC to look for errors. If the calculations match, no error occurred. Calculations that do not match are an indication that the data has changed; therefore, the frame is dropped.

Ethernet Frame size

- The minimum Ethernet frame size is **64 bytes** and the maximum is **1518 bytes**. This includes all bytes from the Destination MAC Address field through the Frame Check Sequence (FCS) field. The Preamble field is not included when describing the size of a frame.
- Any frame less than 64 bytes in length is considered a “collision fragment” or “runt frame” and is automatically discarded by receiving stations. Frames with more than 1500 bytes of data are considered “jumbo” or “baby giant frames”.
- If the size of a transmitted frame is less than the minimum or greater than the maximum, the receiving device drops the frame. Dropped frames are likely to be the result of collisions or other unwanted signals and are therefore considered invalid.

LAN devices

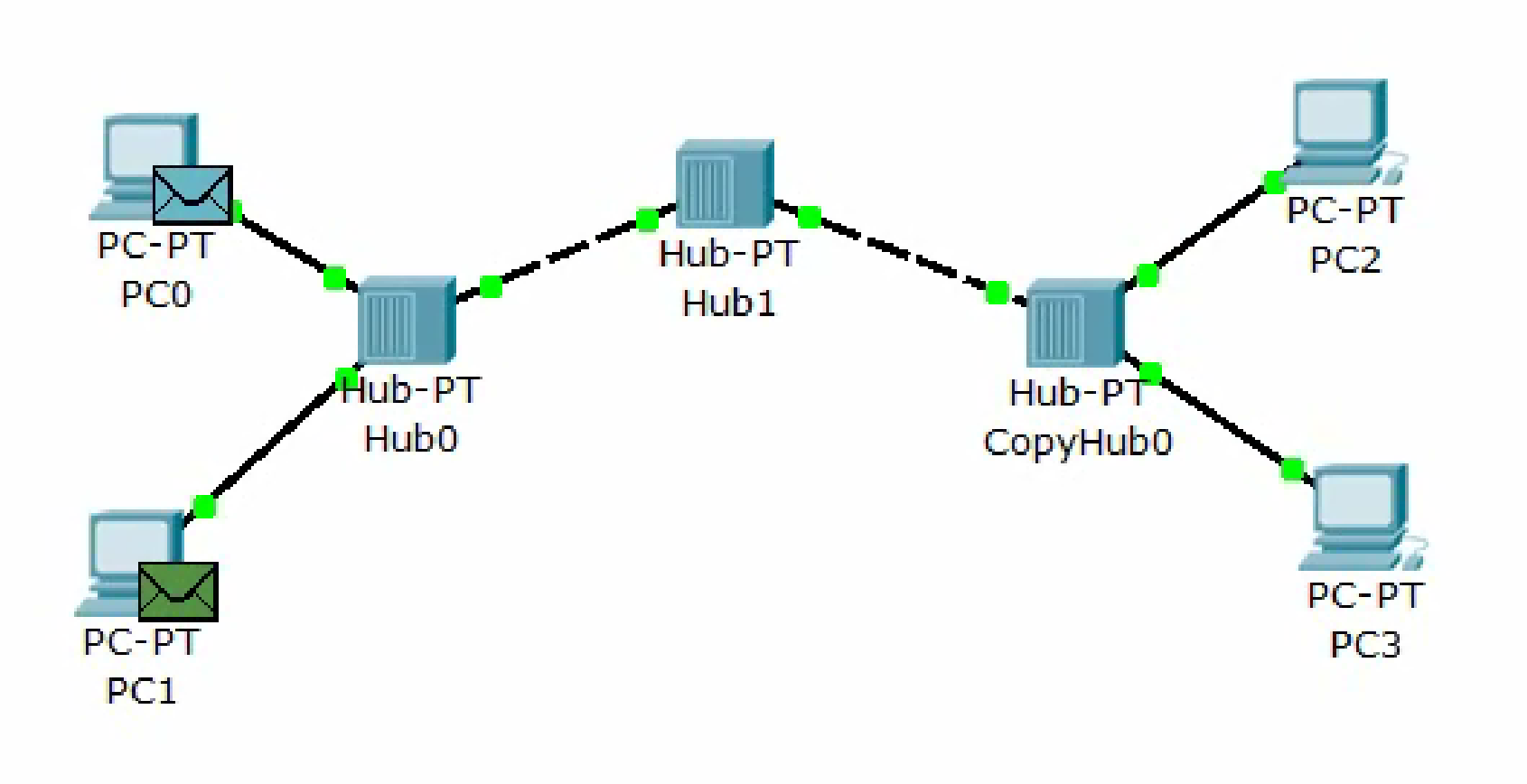
Network devices and OSI model



Hub

- The simplest device for connecting computers to a local area network
- Works at the physical level (restores the signal shape and transmits to all ports)
- Only one computer can transfer data through the hub at a time
- The bandwidth is shared between all users
- Low security - easy to listen to traffic
- If two or more devices connected to the hub simultaneously transmit data, there is a signal overlap - **collision**
- A network based on hubs forms a **collision domain**
- In a collision domain, only one station can transmit data at any one time
- It is a legacy device

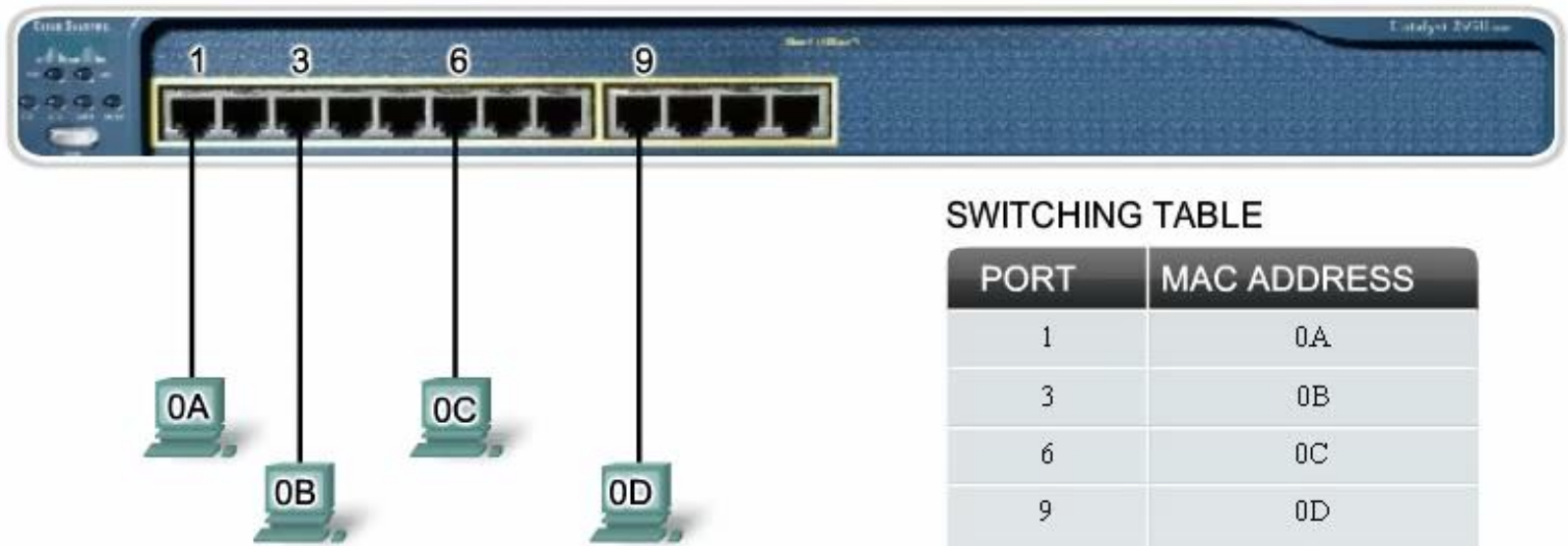
Collision distribution



Switching General Concept

- A Switch makes a decision based on **ingress port** and **destination address**.
- A LAN switch keeps a **table** that it uses to determine how to forward traffic through the switch.
- Cisco LAN switches forward Ethernet frames based on the **destination MAC address** of the frames.
- The only intelligence of the LAN switch is its ability to use its table to forward traffic based on the ingress port and the destination address of a message.
- Connects end devices to a central intermediate device on most Ethernet networks
- Builds a **MAC address table** that it uses to make forwarding decisions
- Depends on routers to pass data between IP subnetworks
- A switch is completely **transparent** to network protocols and user applications.

Switch Frame Forwarding



SWITCHING TABLE

PORT	MAC ADDRESS
1	0A
3	0B
6	0C
9	0D

FRAME 1

Preamble	Destination Address	Source Address	Type	Data	Pad	CRC
	0C	0A				

FRAME 2

Preamble	Destination Address	Source Address	Type	Data	Pad	CRC
	0C	0D				

Pause

Switch operation algorithm

Learn – Examining the Source MAC Address

Every frame that enters a switch is checked for new information to learn. It does this by examining the frame's source MAC address and port number where the frame entered the switch.

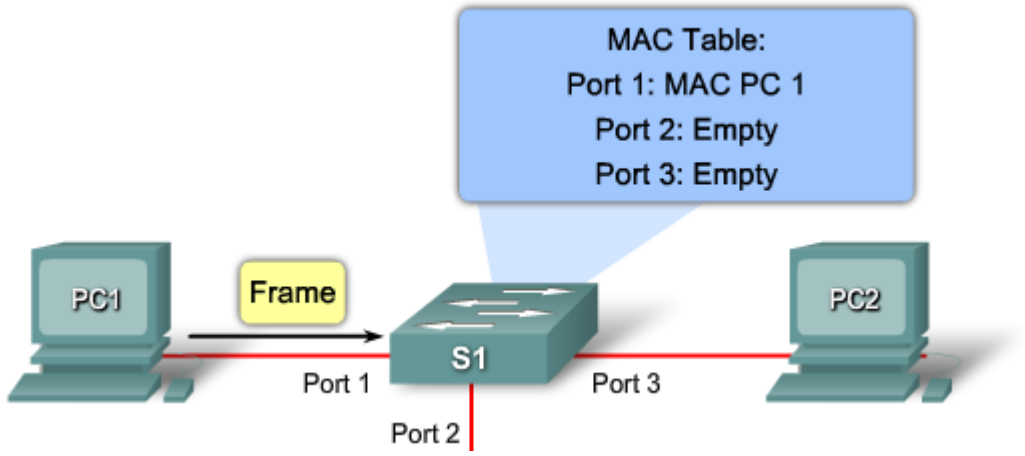
- If the source MAC address does **not exist**, it is added to the table along with the incoming port number.
- If the source MAC address does **exist**, the switch updates the refresh timer for that entry. By default, most Ethernet switches keep an entry in the table for 5 minutes.

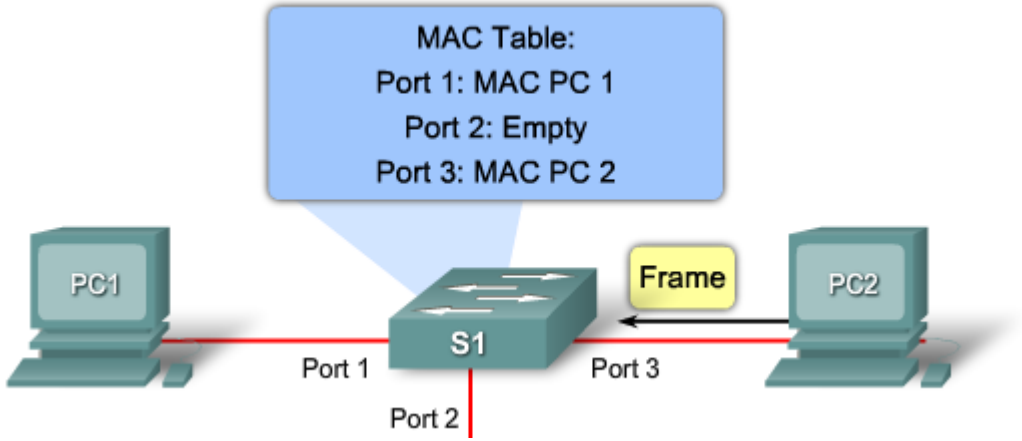
Forward – Examining the Destination MAC Address

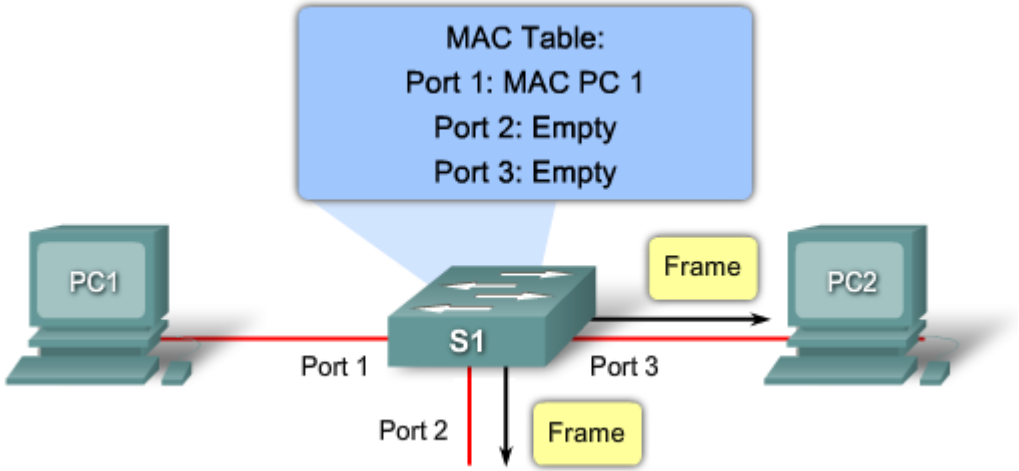
If the destination MAC address is a unicast address, the switch will look for a match between the destination MAC address of the frame and an entry in its MAC address table.

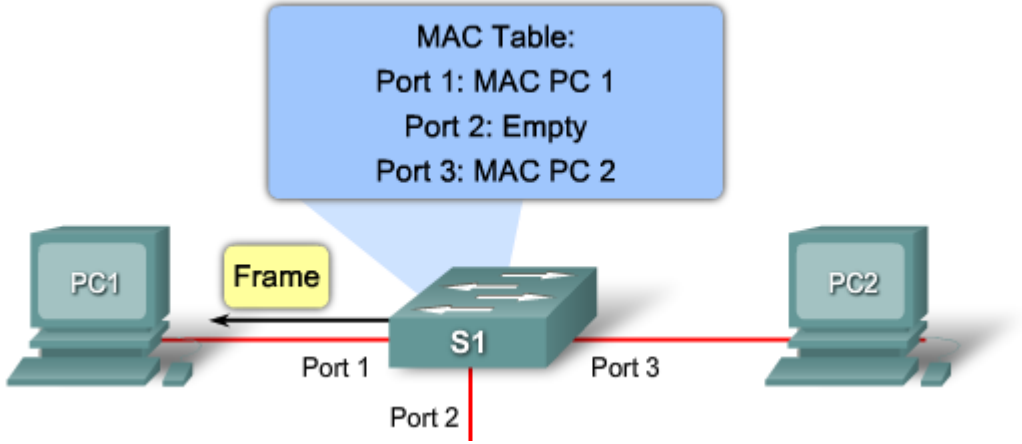
- If the destination MAC address is **in the table**, it will forward the frame out the specified port.
- If the destination MAC address is **not in the table**, the switch will forward the frame out all ports except the incoming port. This is known as an **unknown unicast**.

Switch operation steps









Dynamically Populating a Switch MAC Address Table

- A switch must first learn which devices exist on each port before it can transmit a frame
- It builds a table called a **MAC address**, or **content addressable memory** (CAM) table
- The mapping **device** to **port** is stored in the CAM table
- CAM is a special type of memory used in high-speed searching applications.
- The information in the MAC address table used to send frames
- When a switch receives an incoming frame with a MAC address that is not found in the CAM table, it **floods** it to all ports but not the one that received the frame.

Switch Forwarding Methods

Store-and-Forward

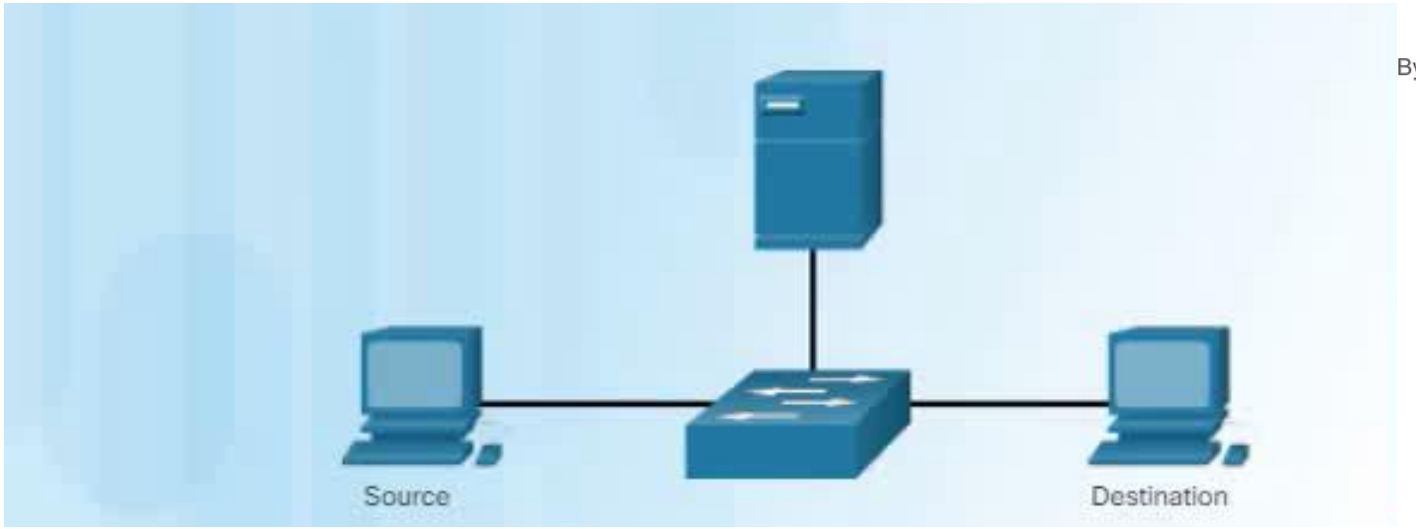
A store-and-forward switch receives the entire frame, and computes the CRC. If the CRC is valid, the switch looks up the destination address, which determines the outgoing interface. The frame is then forwarded out the correct port.

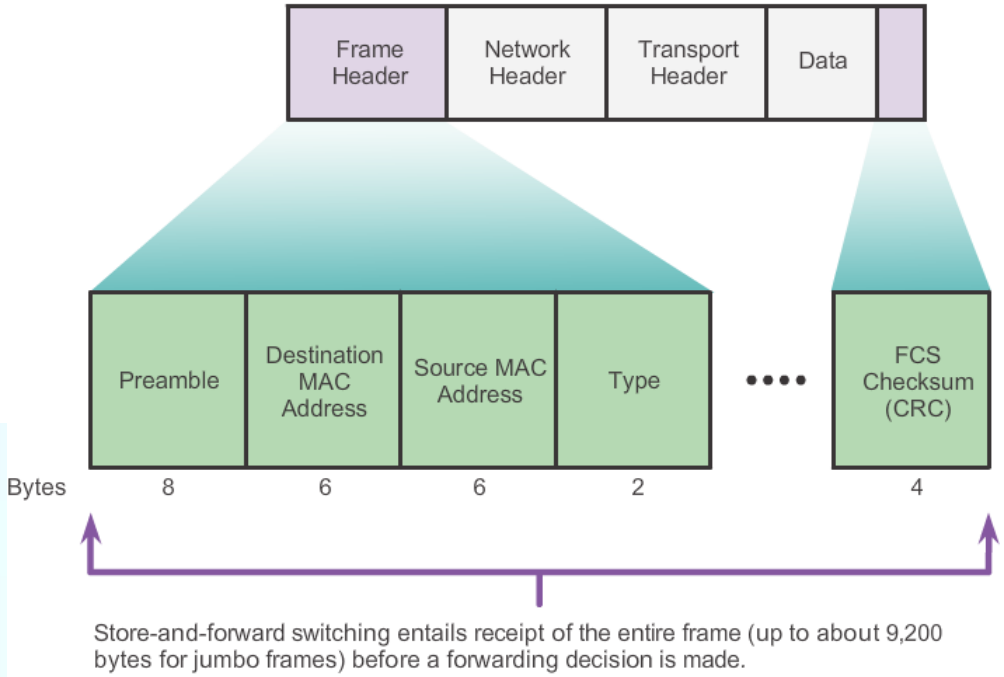
Cut-Through

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.

Store-and-Forward Switching

- Store-and-Forwarding allows the switch to:
  - Check for errors (via FCS check)
  - Perform Automatic Buffering
- Slower forwarding



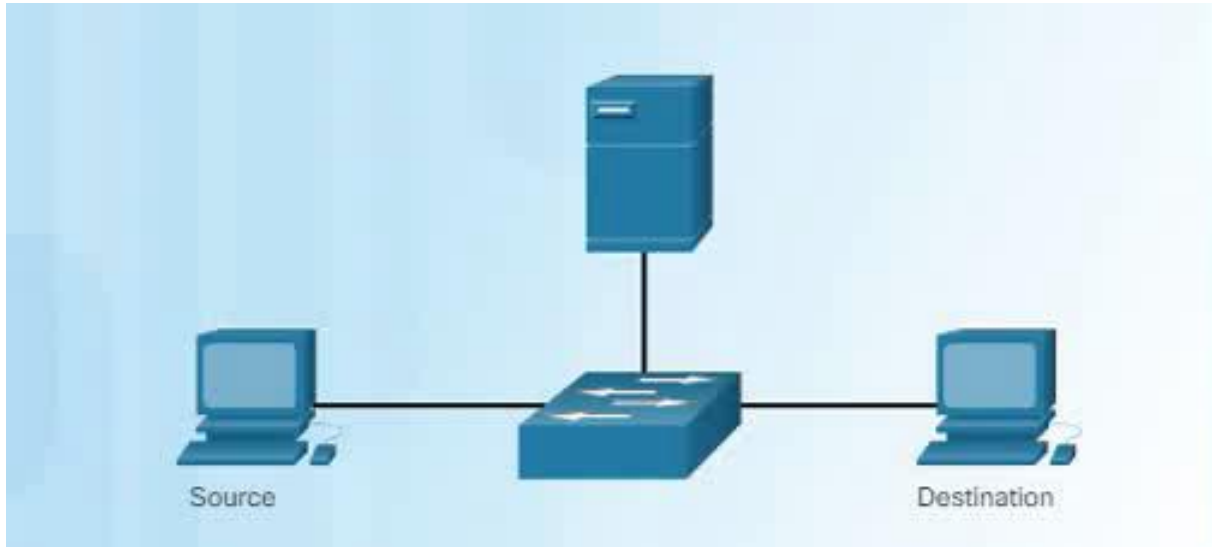


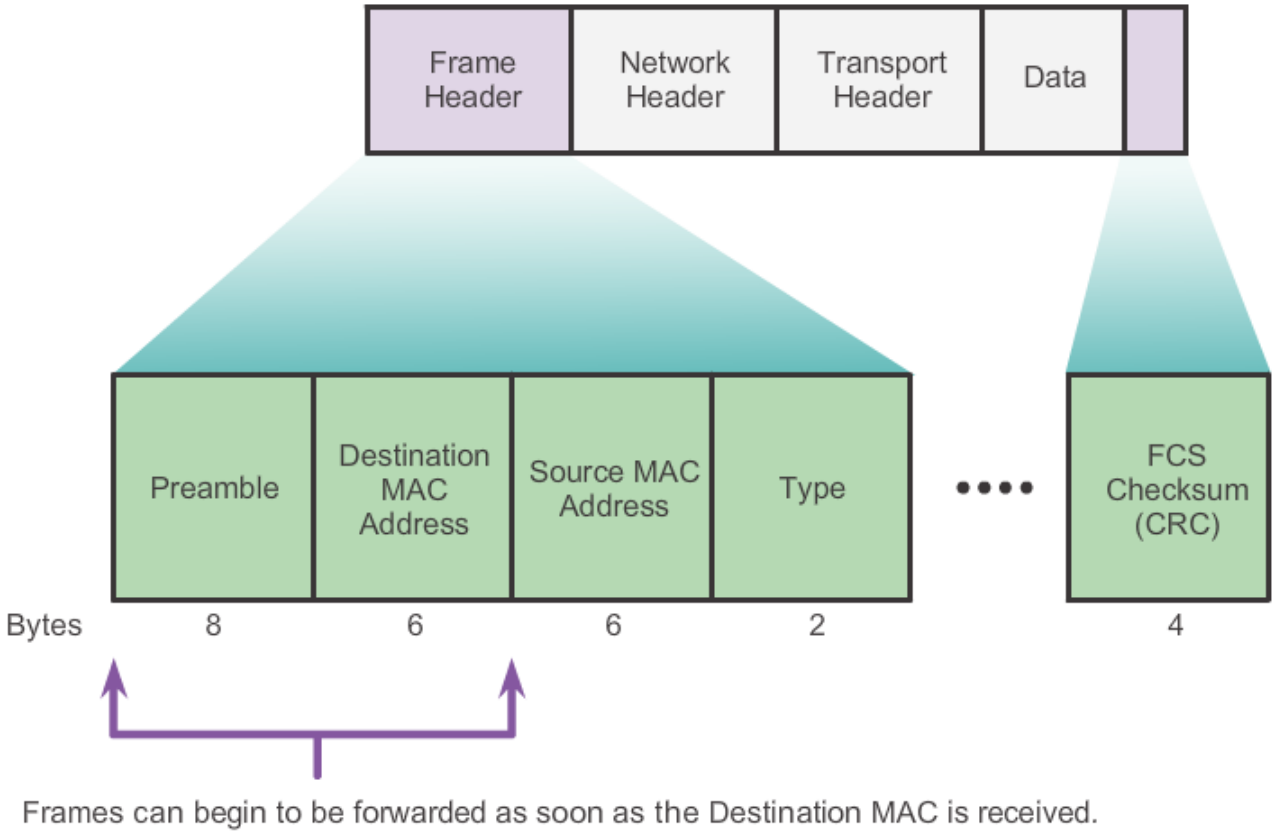
Cut-through Switching

- **Fast-forward switching** offers the lowest level of latency. Immediately forwards a packet after reading the destination address
- In **fragment-free switching**, the switch stores the **first 64 bytes** of the frame before forwarding. The reason fragment-free switching stores only the first 64 bytes of the frame is that most network errors and collisions occur during the first 64 bytes
- **Adaptive cut-through**. Cut-through switching on a per-port basis until a user-defined error threshold is reached and then they automatically change to store-and-forward.

Cut-Through Switching

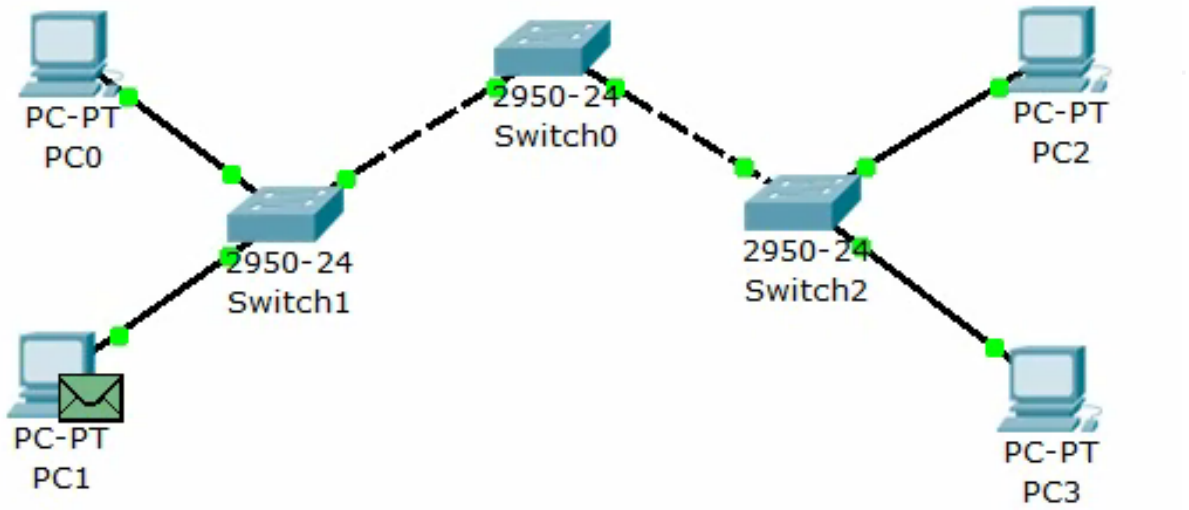
- Cut-Through allows the switch to start forwarding in about **10 microseconds**
- No FCS check
- No Automatic Buffering

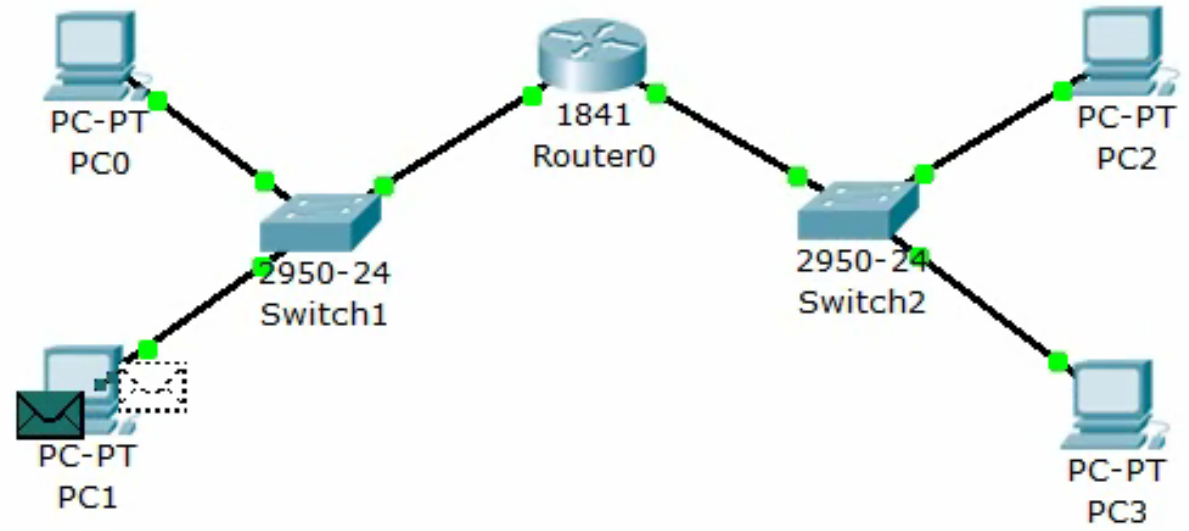




Broadcast Domains

- Broadcast domain is the extend of the network where a broadcast frame can be heard.
- Switches forward **broadcast** frames to **all port** Therefore switches don’t break broadcast domains.
- All ports of a switch (with its default configuration) belong to the **same** broadcast domain
- If two or more switches are connected, broadcasts will be **forward** to all ports of all switches (except for the port that originally received the broadcast)
- Only the **router** is a border of broadcast domai





Considerations of Switch Selection

- **Cost** - The cost of a switch will depend on the number and speed of the interfaces, supported features, and expansion capability.
- **Port Density** - Network switches must support the appropriate number of devices on the network.
- **Power** - It is now common to power access points, IP phones, and even compact switches using Power over Ethernet (PoE). Some chassis-based switches support redundant power supplies.
- **Reliability** - The switch should provide continuous access to the network.
- **Port Speed** - The speed of the network connection is of primary concern to end users.
- **Frame Buffers** - The ability of the switch to store frames is important in a network where there may be congested ports to servers or other areas of the network.
- **Scalability** - The number of users on a network typically grows over time; therefore, the switch should provide the opportunity for growth.

Switch Form Factor

- **Fixed configuration** switches **do not support** features or options beyond those that originally came with the switch

Features and options are limited to those that originally come with the switch.

- **Modular configuration** switches typically come with different sized chassis that allow for the installation of different numbers of modular **line cards.** The line cards actually contain the ports.

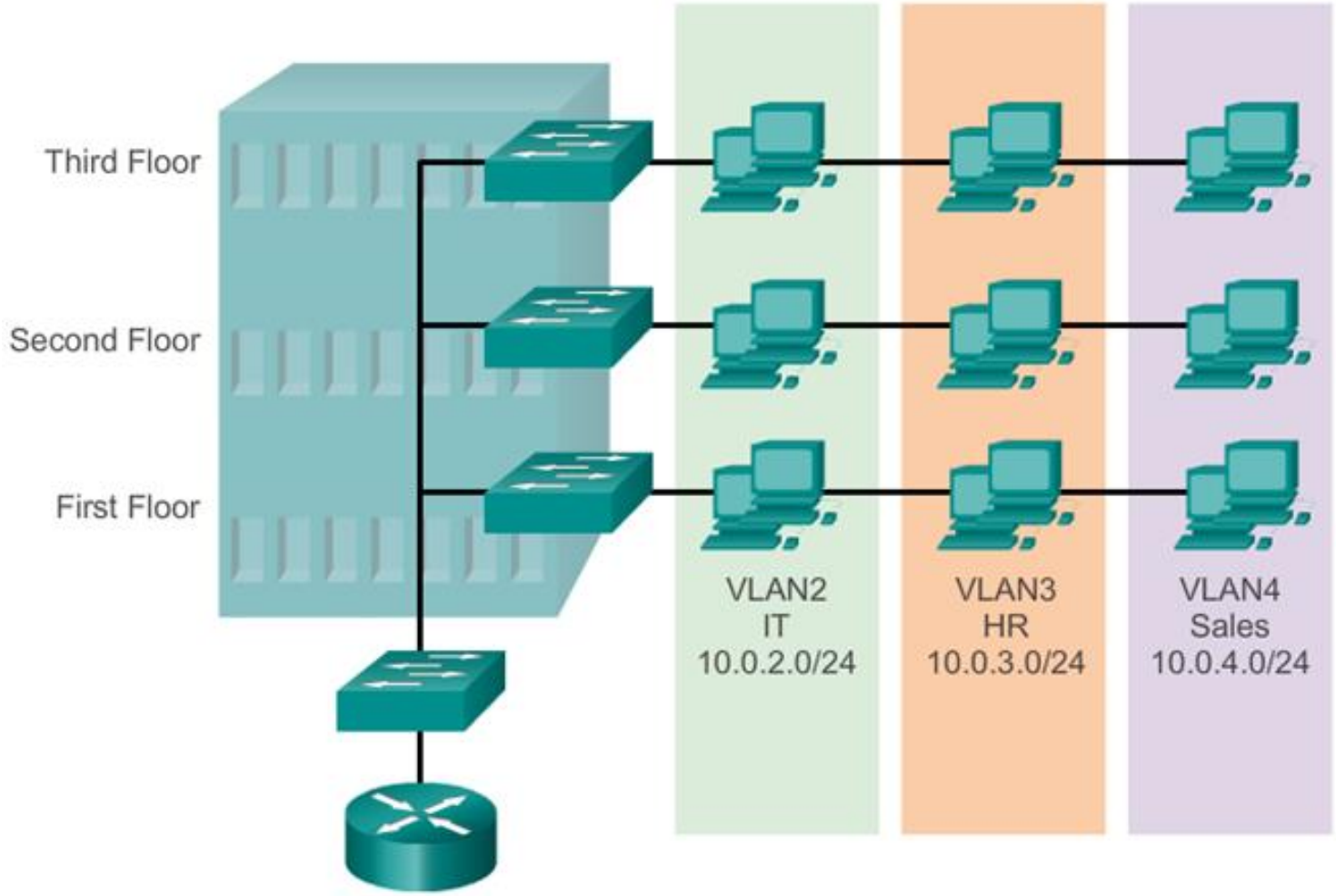
- **Stackable** configuration switches can be interconnected using a special cable that provides high-bandwidth throughput between the switches
- Cisco StackWise technology allows the interconnection of **up to nine** switches.

Stackable switches, connected by a special cable, effectively operate as one large switch.

VLAN Definitions

- VLAN (virtual LAN) is a **logical** partition of a layer 2 network
- Multiple partition can be created, allowing for multiple VLANs to co-exist
- Each VLAN is a **broadcast** domain, usually with its own IP network
- VLANS are mutually **isolated** and packets can only pass between them through a **router**
- The partitioning of the layer 2 network takes inside a layer 2 device, usually a switch.
- The hosts grouped within a VLAN are unaware of the VLAN's existence
- VLANs allow an administrator to segment networks based on factors such as **function**, **project team**, or **application**, without regard for the physical location of the user or device.
- VLANs enable the implementation of access and **security policies** according to specific groupings of users.
- Each switch port can be assigned to **only one VLAN** (with the exception of a port connected to an IP phone or to another switch).

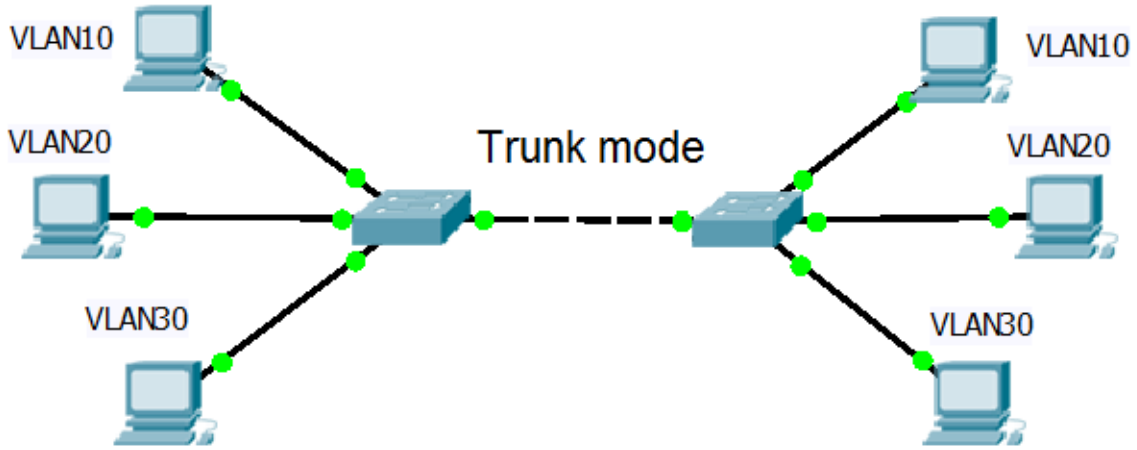
VLAN


Third Floor
Second Floor
First Floor
VLAN2
IT
10.0.2.0/24
VLAN3
HR
10.0.3.0/24
VLAN4
Sales
10.0.4.0/24

Types of VLAN

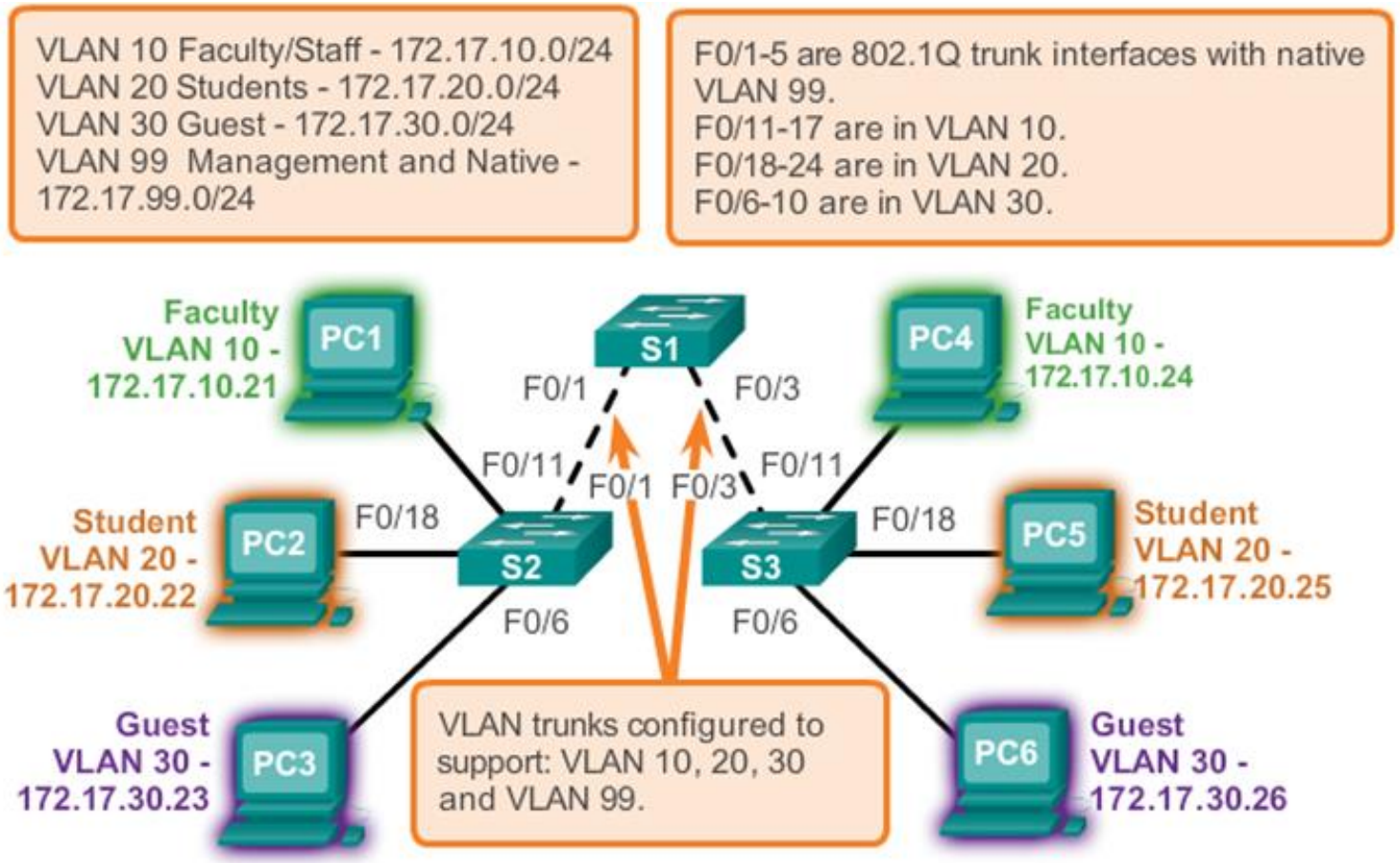
- A **data VLAN** is a VLAN that is configured to carry only user-generated traffic.
- All switch ports become a member of the **default VLAN** after the initial boot up of the switch.
- A **native VLAN** is assigned to an 802.1Q trunk port. An 802.1Q trunk port supports traffic coming from many VLANs (tagged traffic) as well as traffic that does not come from a VLAN (untagged traffic). The 802.1Q trunk port places untagged traffic on the native VLAN.
- A **management VLAN** is any VLAN you configure to access the management capabilities of a switch. VLAN 1 would serve as the management VLAN if you did not proactively define a unique VLAN to serve as the management VLAN.

Switch interconnection



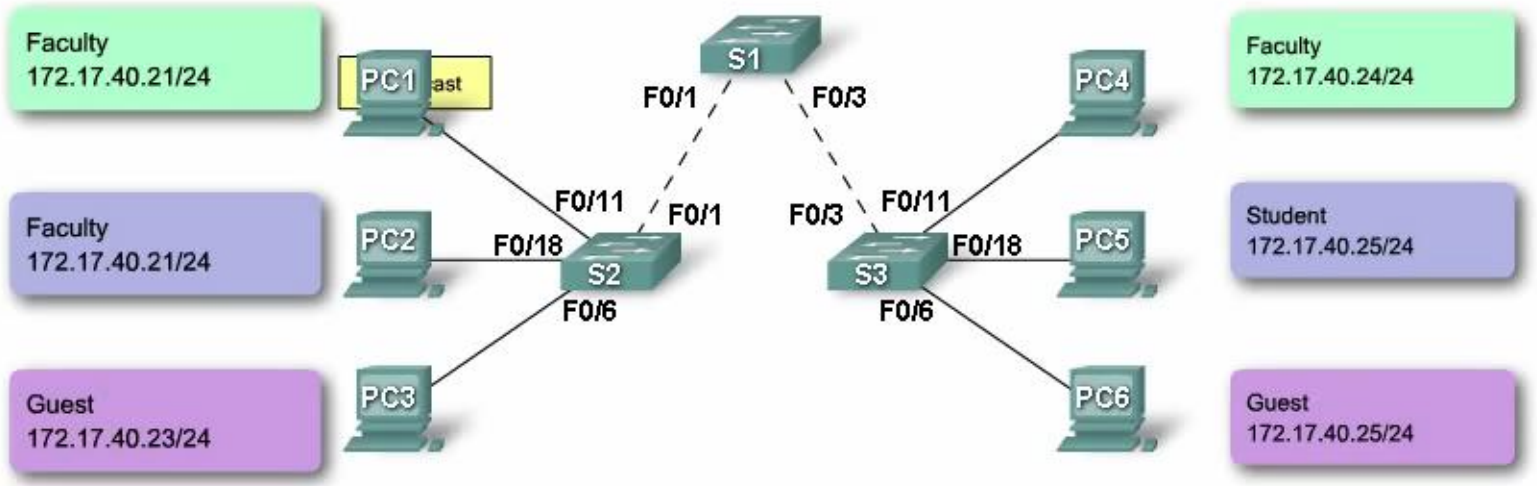
- A **VLAN trunk**, or trunk, is a point-to-point link between two network devices that carries more than one VLAN.
- Usually established **between switches** so same-VLAN devices can communicate even if physically connected to different switches
- A VLAN trunk **is not associated** to any VLANs. Neither is the trunk ports used to establish the trunk link
- **IEEE802.1q** is a popular VLAN trunk protocol

VLAN Trunks

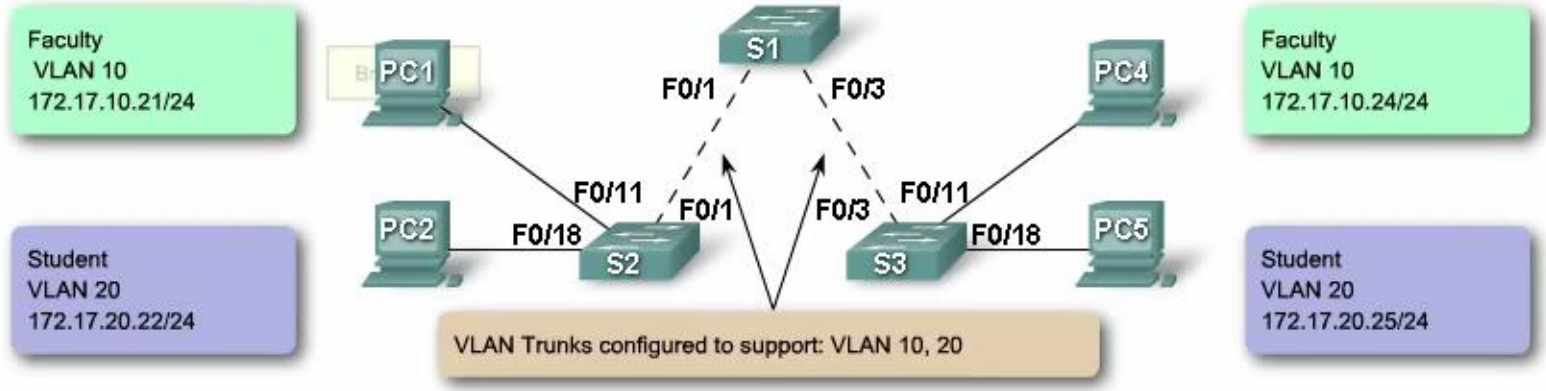

VLAN 10 Faculty/Staff - 172.17.10.0/24
VLAN 20 Students - 172.17.20.0/24
VLAN 30 Guest - 172.17.30.0/24
VLAN 99 Management and Native - 172.17.99.0/24
F0/1-5 are 802.1Q trunk interfaces with native VLAN 99.
F0/11-17 are in VLAN 10.
F0/18-24 are in VLAN 20.
F0/6-10 are in VLAN 30.
Faculty VLAN 10 - 172.17.10.21
PC1
S1
F0/1
F0/3
PC4
Faculty VLAN 10 - 172.17.10.24
F0/11
F0/1
F0/3
F0/11
Student VLAN 20 - 172.17.20.22
PC2
F0/18
S2
S3
F0/18
PC5
Student VLAN 20 - 172.17.20.25
F0/6
F0/6
Guest VLAN 30 - 172.17.30.23
PC3
VLAN trunks configured to support: VLAN 10, 20, 30 and VLAN 99.
PC6
Guest VLAN 30 - 172.17.30.26

Controlling broadcast domain with VLAN

Without VLAN segmentation



With VLAN segmentation



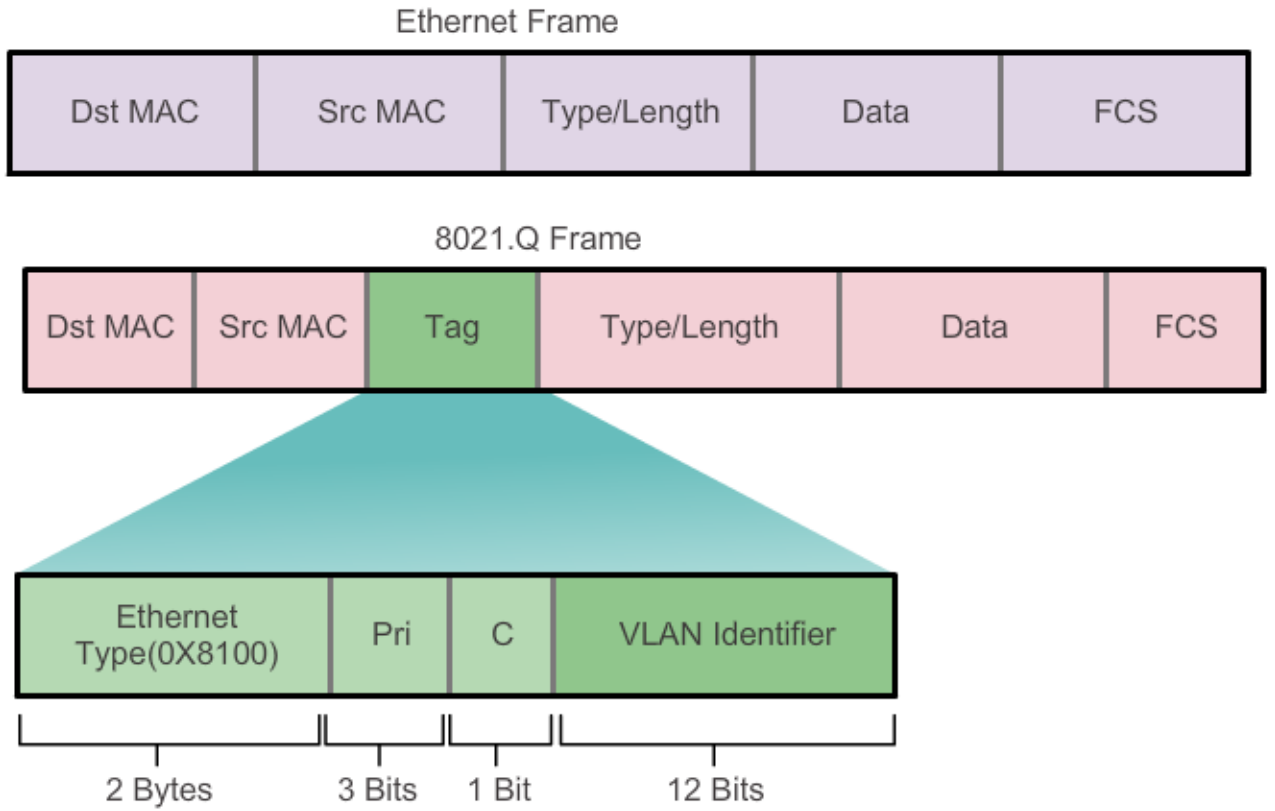
Tagging Ethernet Frames for VLAN Identification

- Frame tagging is used to **properly transmit** multiple VLAN frames through a **trunk** link
- Switches will **tag** frames to **identify** the VLAN they belong. Different tagging protocols exist, with **IEEE 802.1q** being a very popular one
- The protocol defines the structure of the tagging header added to the frame
- Switches will **add VLAN tags** to the frames before placing them into trunk links and remove the tags before forwarding frames through non-trunk ports
- Once properly tagged, the frames can transverse any number of switches via trunk links and still be forward within the correct VLAN at the destination

Tagging Ethernet Frames for VLAN Identification

IEEE 802.1q header

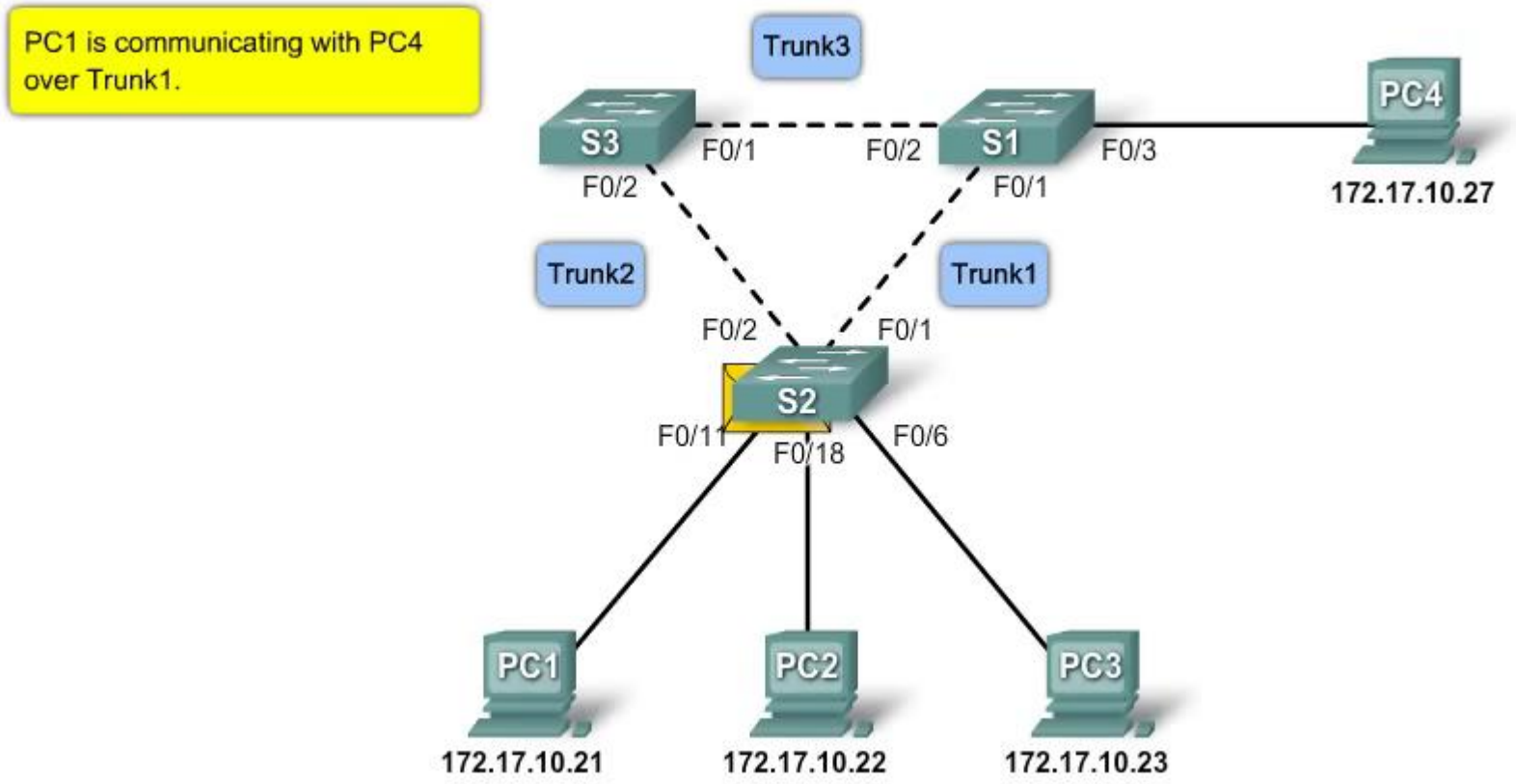
- **Type** - A 2-byte value called the tag protocol ID (TPID) value. For Ethernet, it is set to hexadecimal 0x8100.
- **User priority** - A 3-bit value that supports level or service implementation.
- **Canonical Format Identifier (CFI)** - A 1-bit identifier that enables Token Ring frames to be carried across Ethernet links.
- **VLAN ID (VID)** - A 12-bit VLAN identification number that supports up to 4096 VLAN IDs.



LAN Redundancy

Multiple cabled paths between switches:

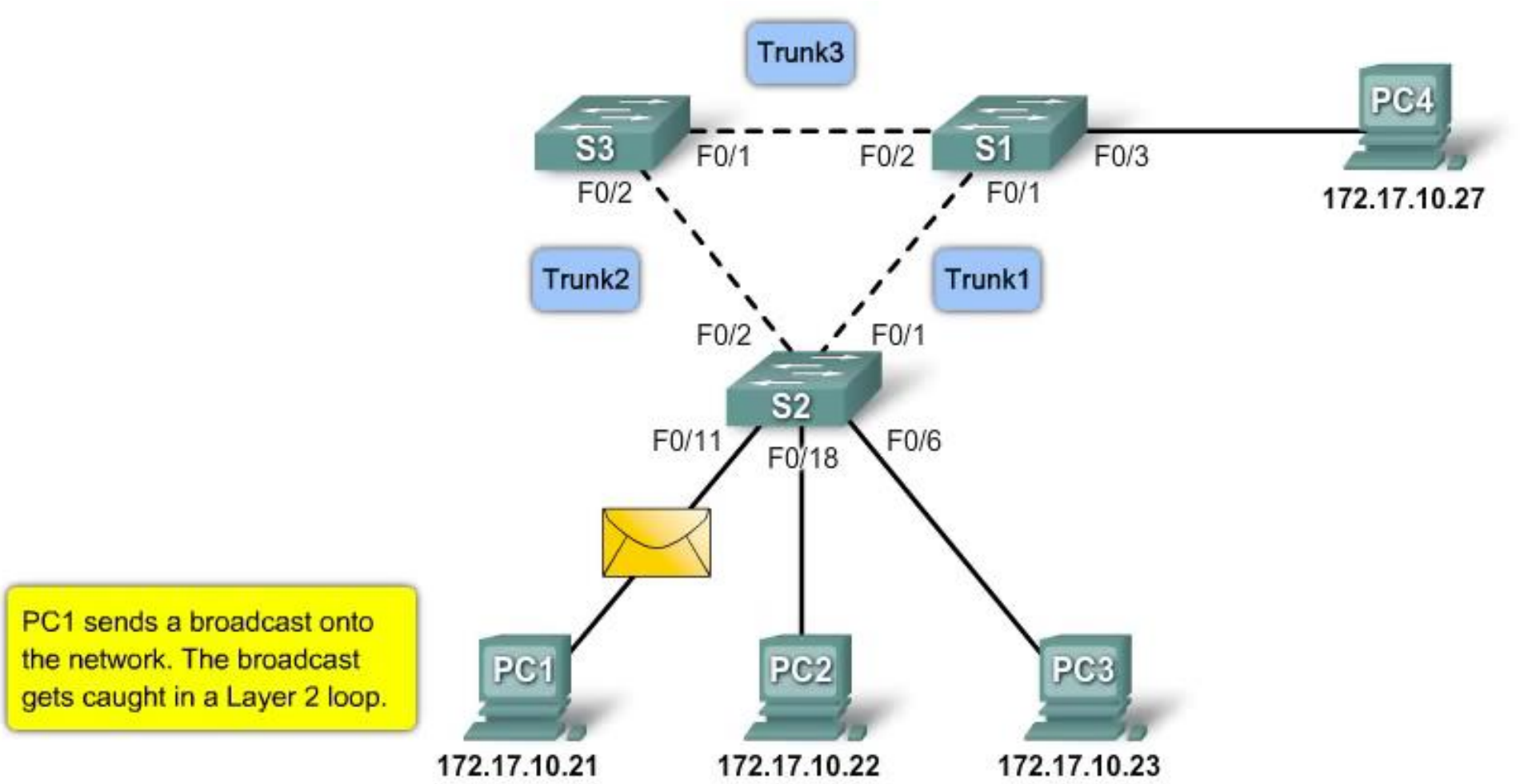
- Provide physical redundancy in a switched network.
- Improves the reliability and availability of the network.
- Enables users to access network resources, despite path disruption.



Layer 2 Redundancy Problems

- **MAC database instability -** Instability in the content of the MAC address table results from copies of the same frame being received on different ports of the switch. Data forwarding can be impaired when the switch consumes the resources that are coping with instability in the MAC address table.
- **Broadcast storms** - Without some loop-avoidance process, each switch may flood broadcasts endlessly (Ethernet frames do not have a time to live (TTL) attribute). This situation is commonly called a broadcast storm.
- **Multiple frame transmission -** Multiple copies of unicast frames may be delivered to destination stations. Many protocols expect to receive only a single copy of each transmission. Multiple copies of the same frame can cause unrecoverable errors.

Broadcast Storms

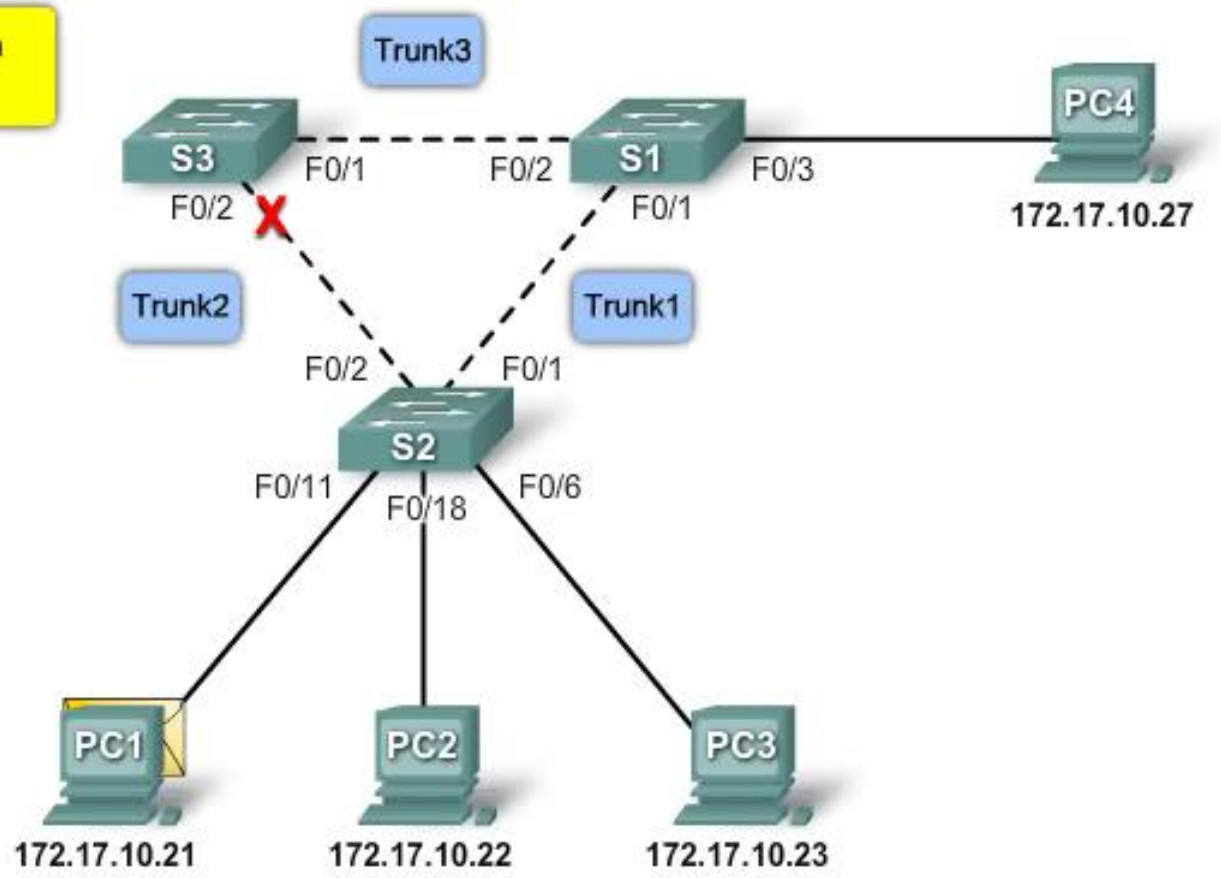


Spanning Tree Algorithm

- STP ensures that there is **only one** logical path between all destinations on the network by intentionally blocking redundant paths that could cause a loop.
- A port is considered blocked when user data is prevented from entering or leaving that port. This does not include bridge protocol data unit (BPDU) frames that are used by STP to prevent loops.
- The physical paths still exist to provide redundancy, but these paths are disabled to prevent the loops from occurring.
- If the path is ever needed to compensate for a network cable or switch failure, STP recalculates the paths and unblocks the necessary ports to allow the redundant path to become active.

Spanning Tree Algorithm

PC1 sends a broadcast to switch S2.



Q&A


Thank you!