CIS 81 Fundamentals of Networking
Chapter 5: Ethernet
Part 1 of 2

CCNA Introduction to Networking 5.0

Rick Graziani
Cabrillo College
graziani@cabrillo.edu

Fall 2015

Chapter 5: Objectives

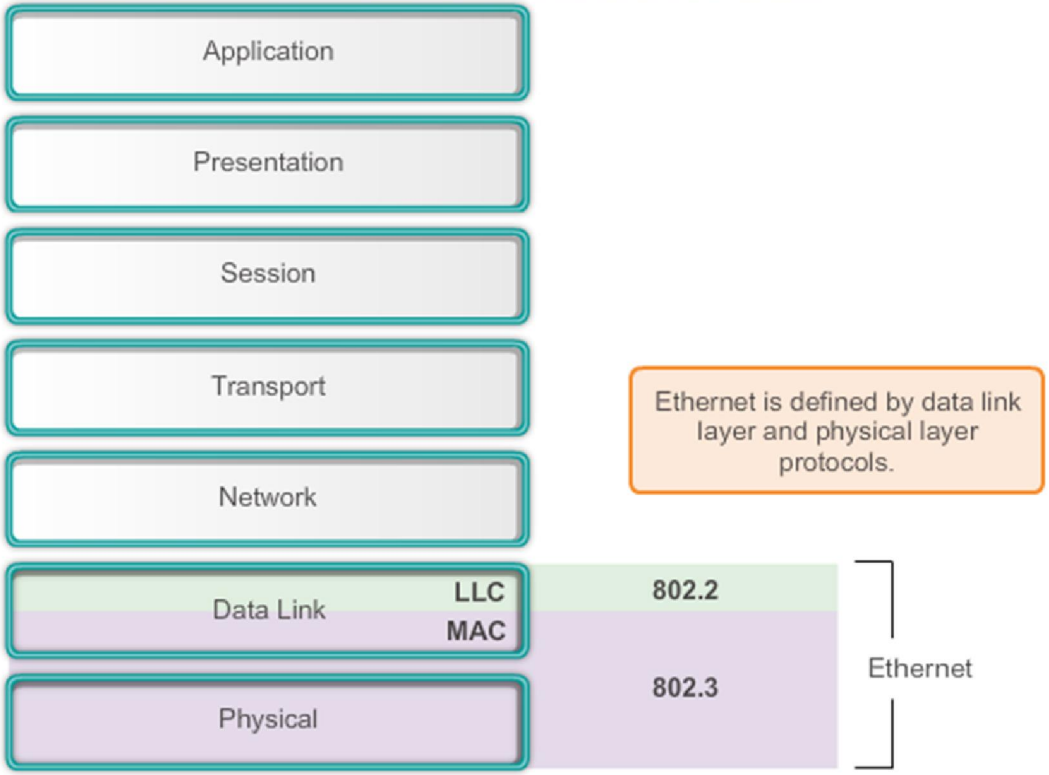
In this chapter, you will learn to:

- Describe the operation of the Ethernet sublayers.
- Identify the major fields of the Ethernet frame.
- Describe the purpose and characteristics of the Ethernet MAC address.
- Describe the purpose of ARP.
- Explain how ARP requests impact network and host performance.

Part 2

- Explain basic switching concepts.
- Compare fixed configuration and modular switches.
- Configure a Layer 3 switch.

Ethernet Protocol



- Ethernet – Most common LAN technology used today.
- Supports data bandwidths of 10, 100, 1000, 10,000, 40,000, and 100,000 Mbps (100 Gbps)
- Operates in the data link layer and the physical layer.
- Defined in the IEEE 802.2 and 802.3 standards.
- Ethernet relies on the two separate sublayers of the data link layer to operate:
- Logical Link Control (LLC)
- MAC

Reminder of encapsulation/decapsulation

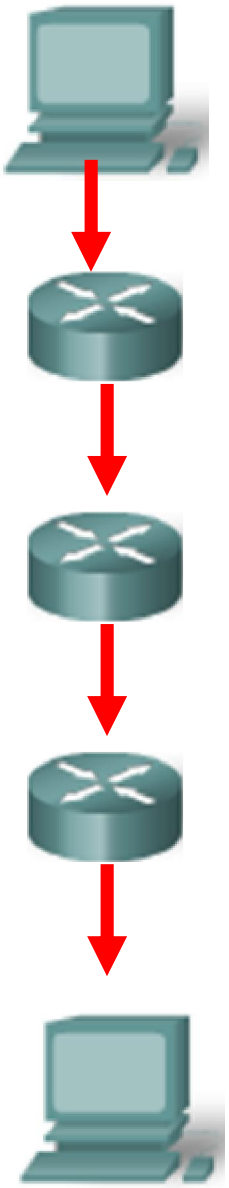
Data Link Header	IP Header	TCP Header	HTTP Header	Data	Data Link Trailer

Data Link Header	IP Packet	Data Link Trailer

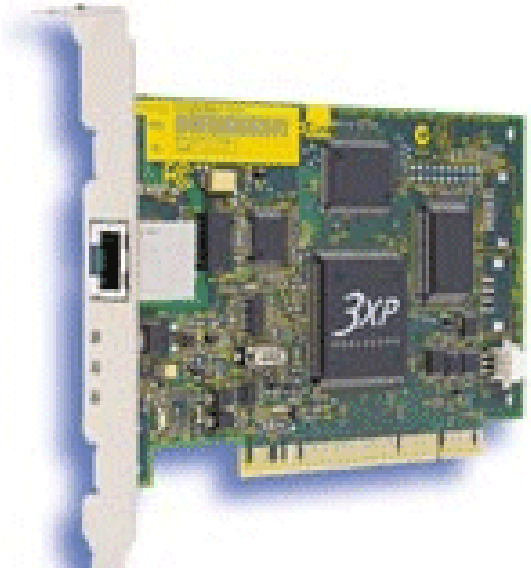
Data Link Header	IP Packet	Data Link Trailer

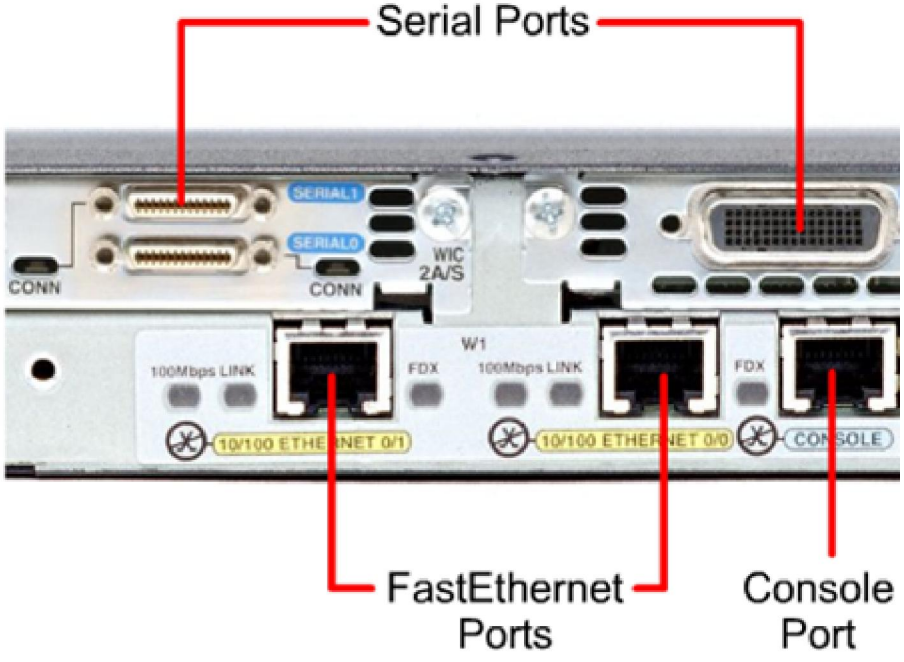
Data Link Header	IP Packet	Data Link Trailer

Data

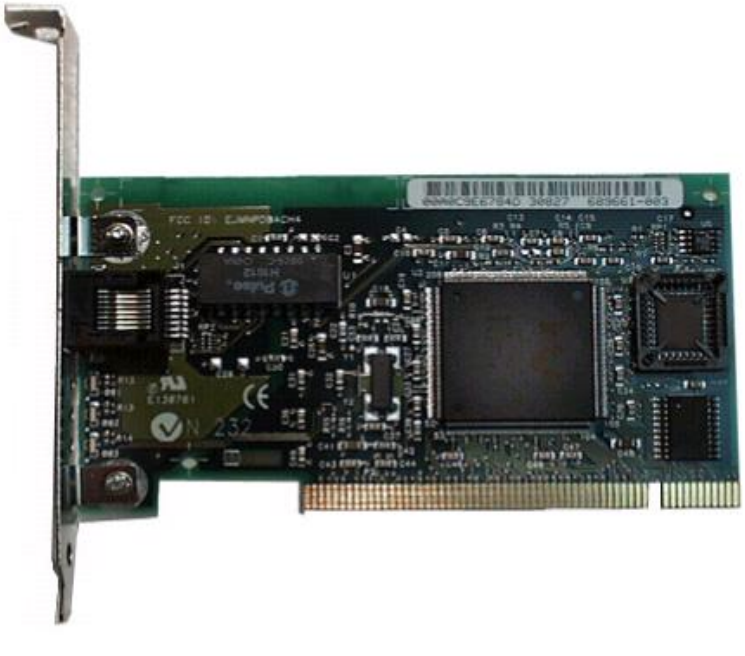


Network Interface Card (NIC)





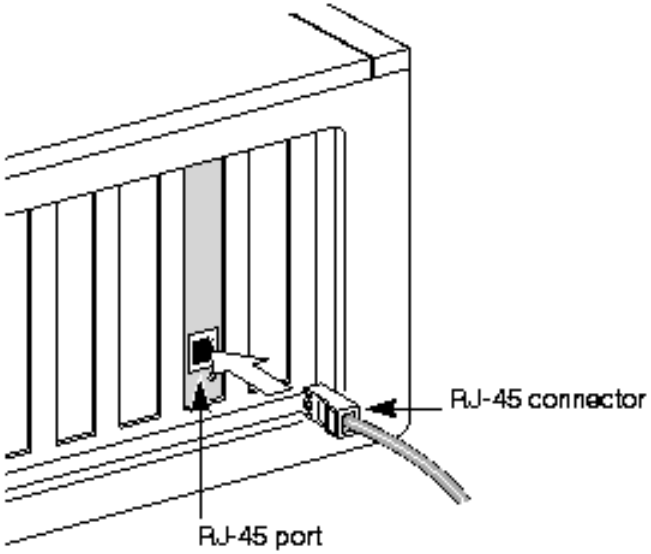
Network Interface Card (NIC)



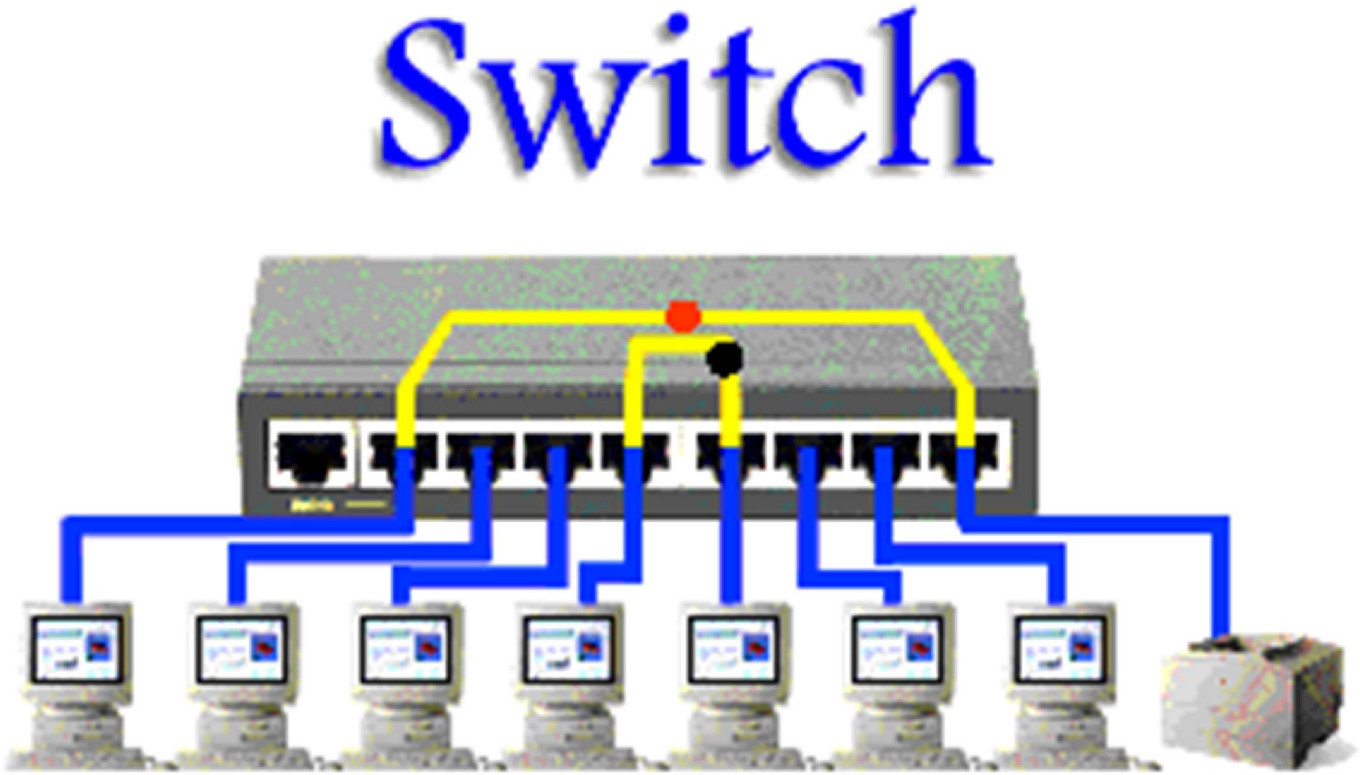
Network Interface Card (NIC)

- Layer 2, Data Link Layer, device
- Connects the device (computer) to the LAN
- Responsible for the local Layer 2 address (later)
- Common Layer 2 NICs:
  - Ethernet
  - Token Ring
- Common Bandwidth
  - 10 Mbps, 10/100 Mbps, 10/100/1000 Mbps

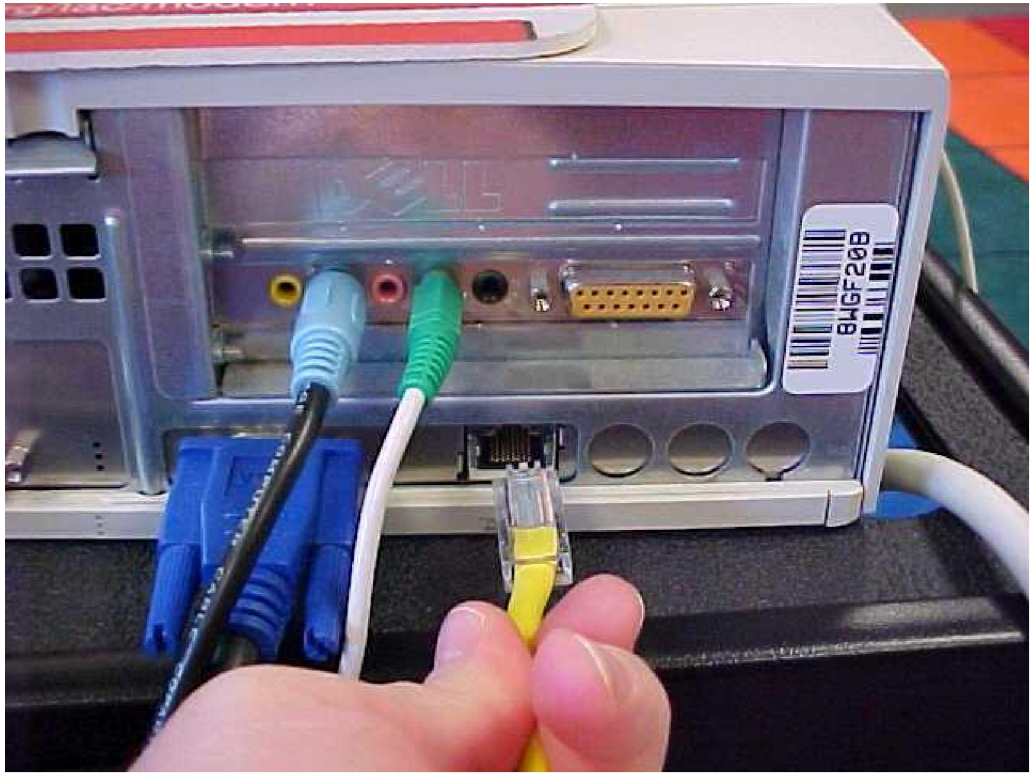
Tracing the Physical Connection
NIC (Network Interface Card)

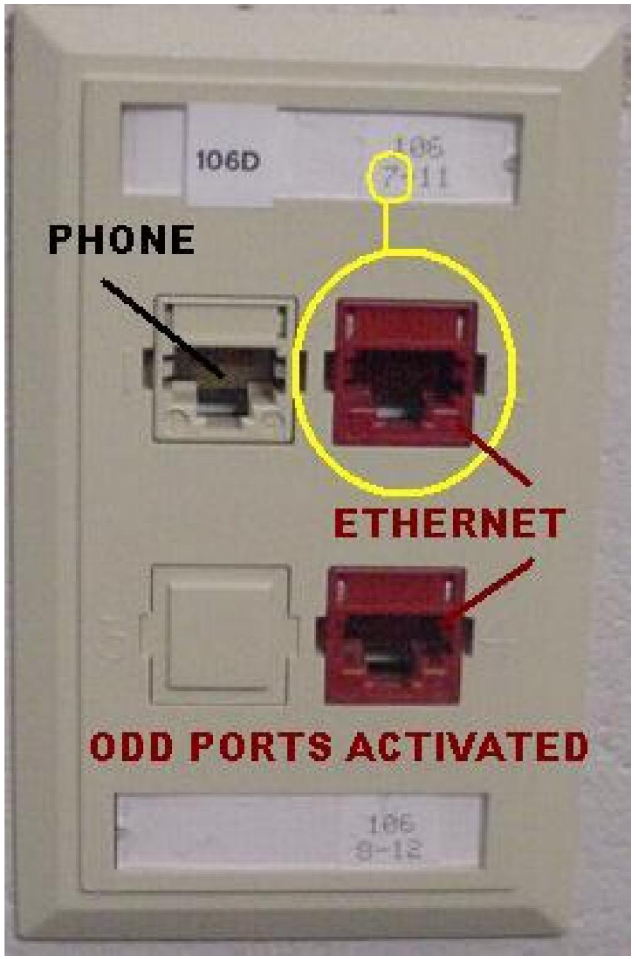


Connecting the NIC to Switch…



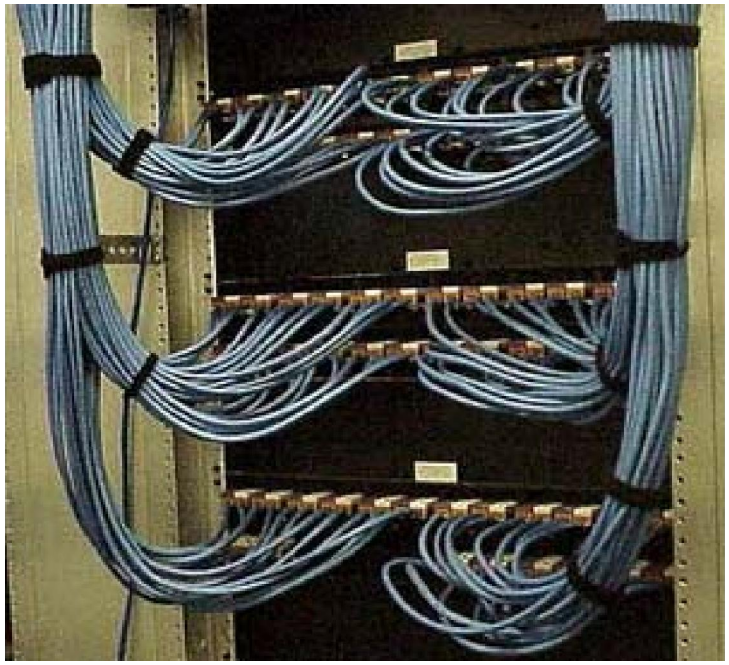
From PC to Ethernet Port…



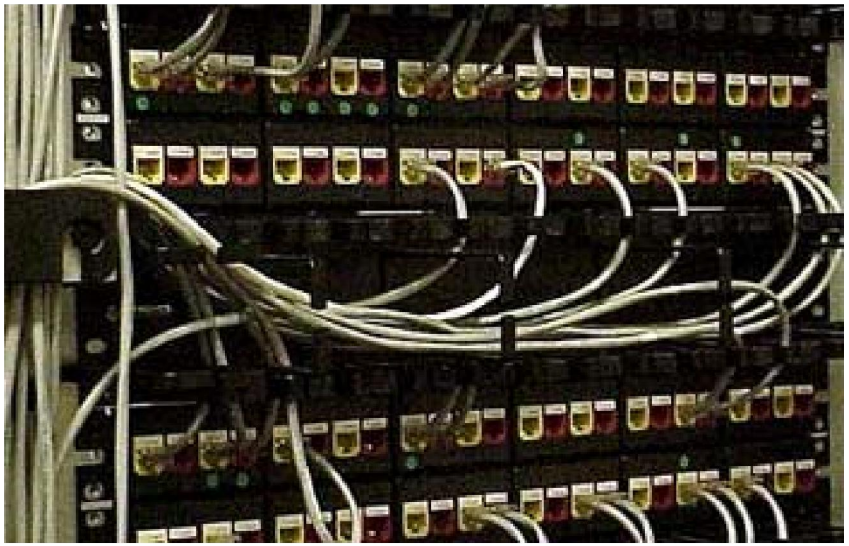


From Ethernet Port to Patch Panel…

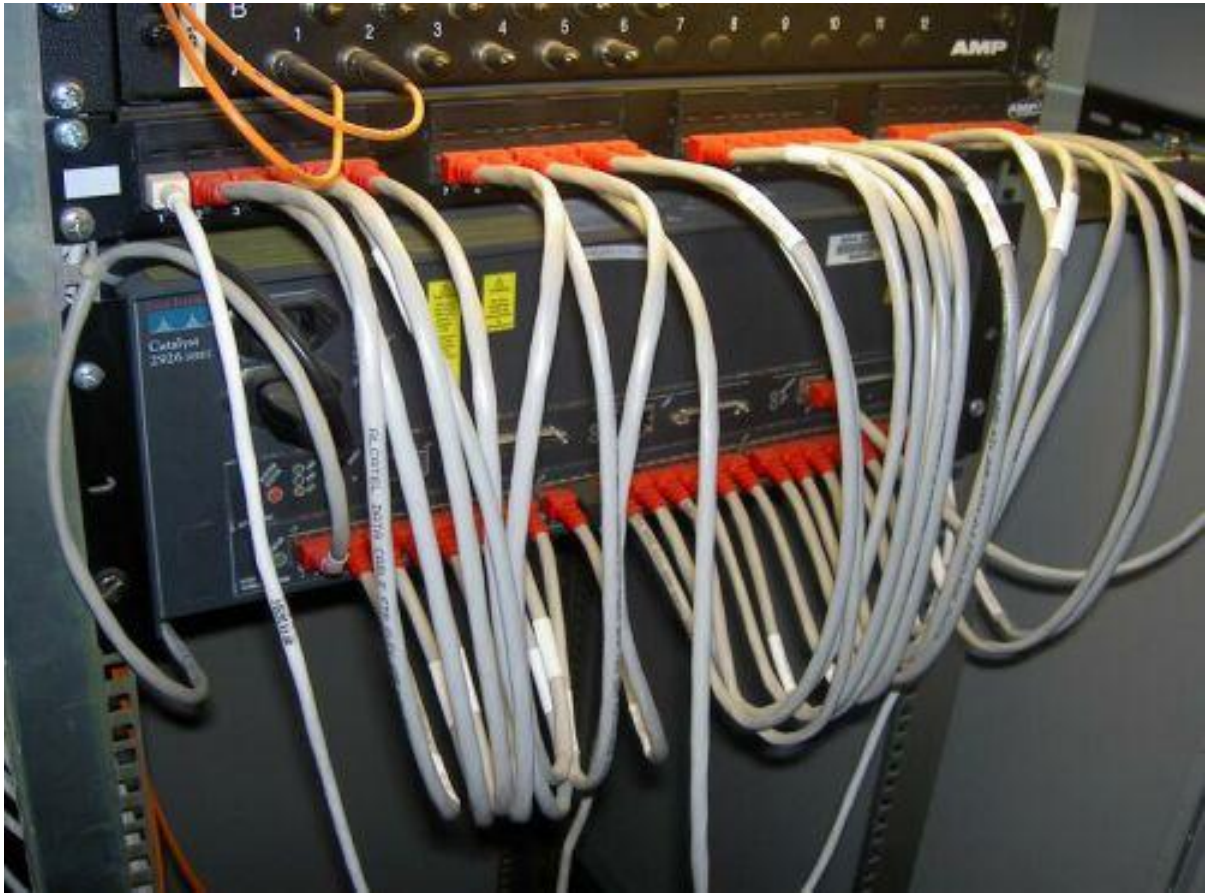
Back View



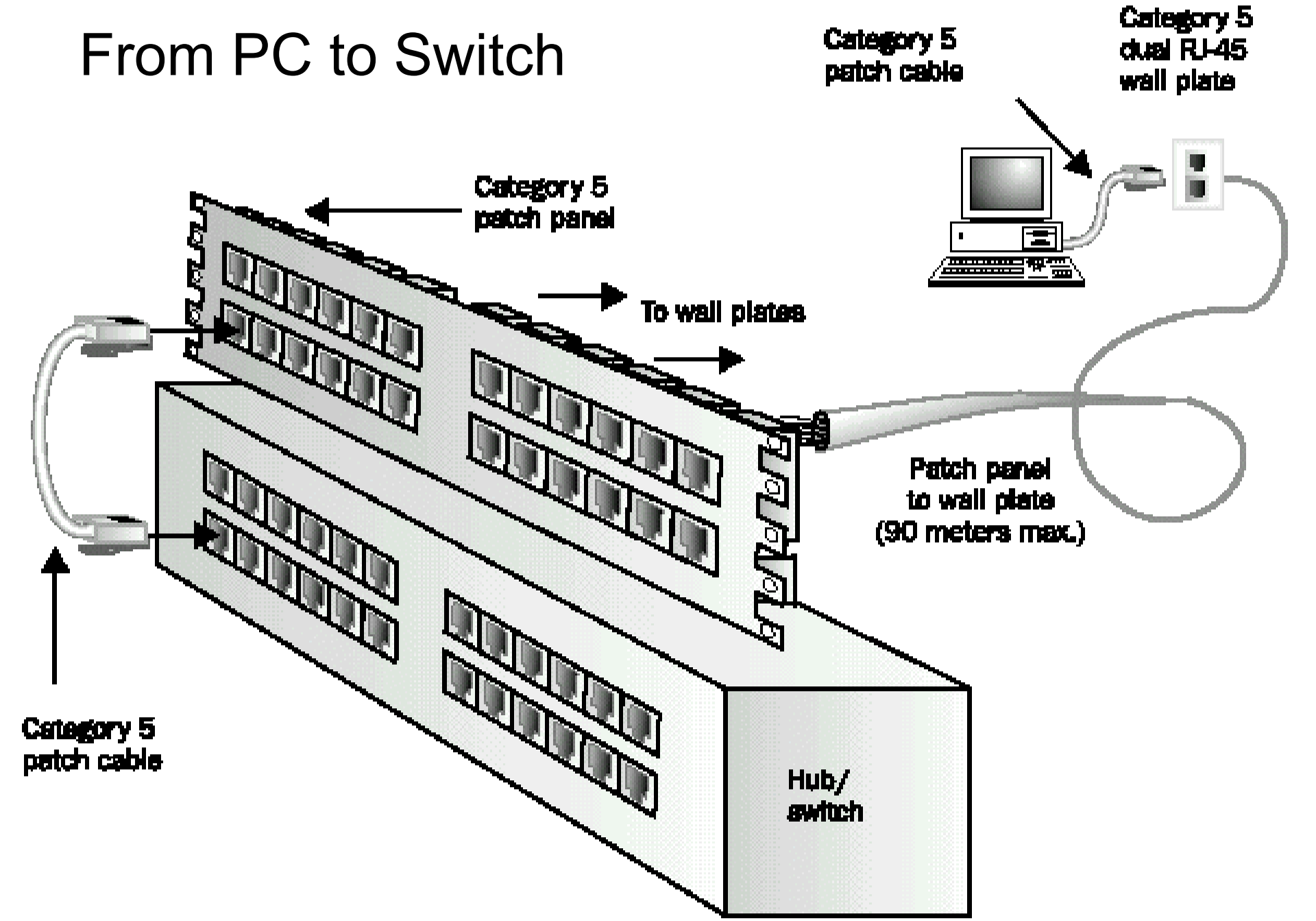
Front View



From Patch Panel to Switch (or hub)

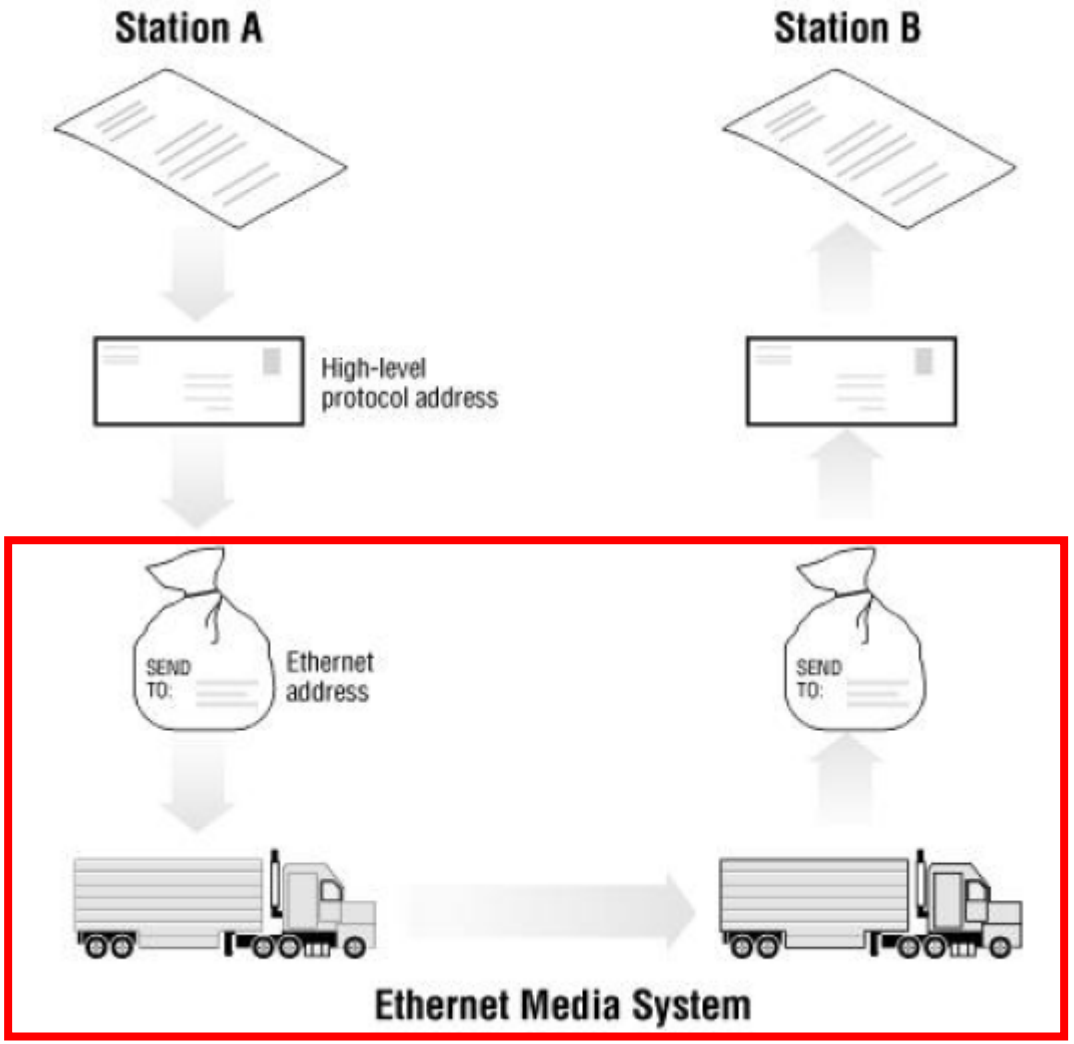


From PC to Switch

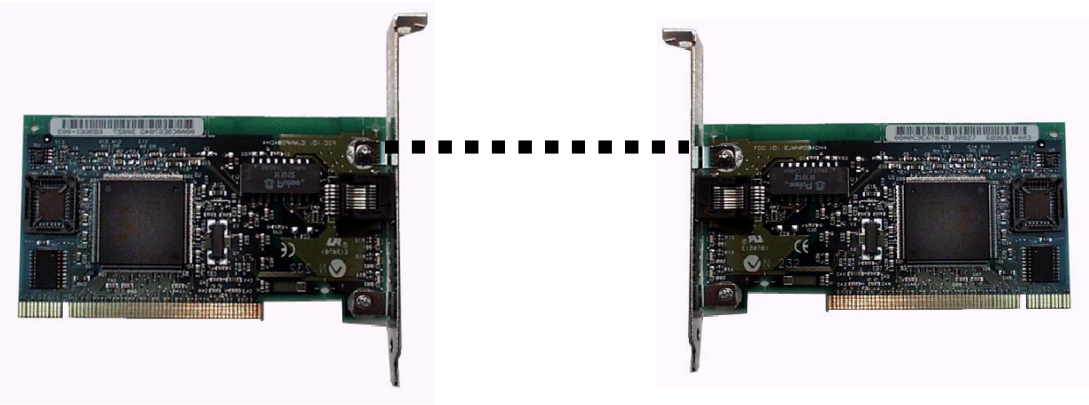


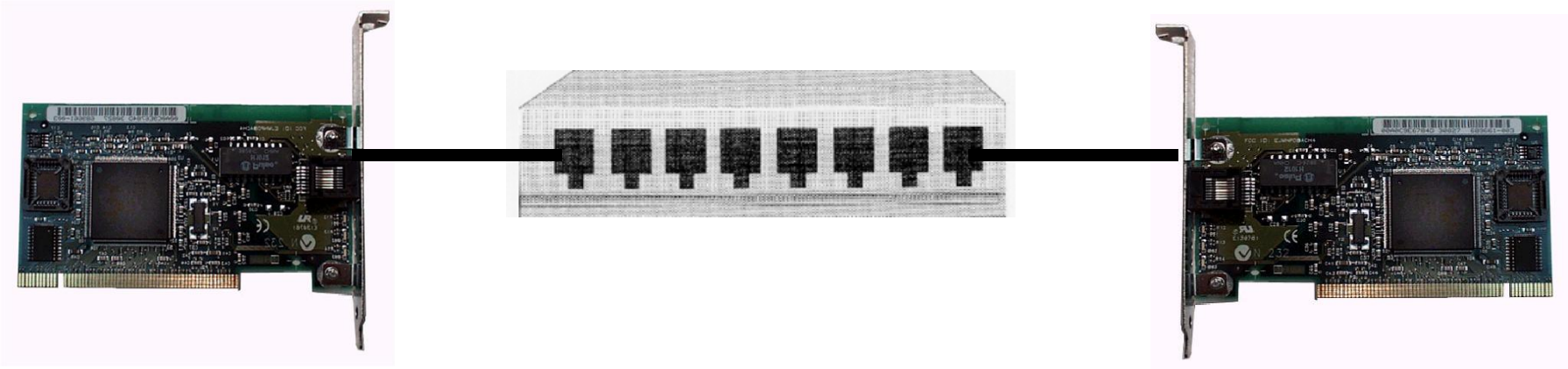
Ethernet is Best Effort Delivery

- Ethernet is best-effort delivery, no guarantee.
- Like a trucking service, it doesn't really know or care about the what it is carrying.

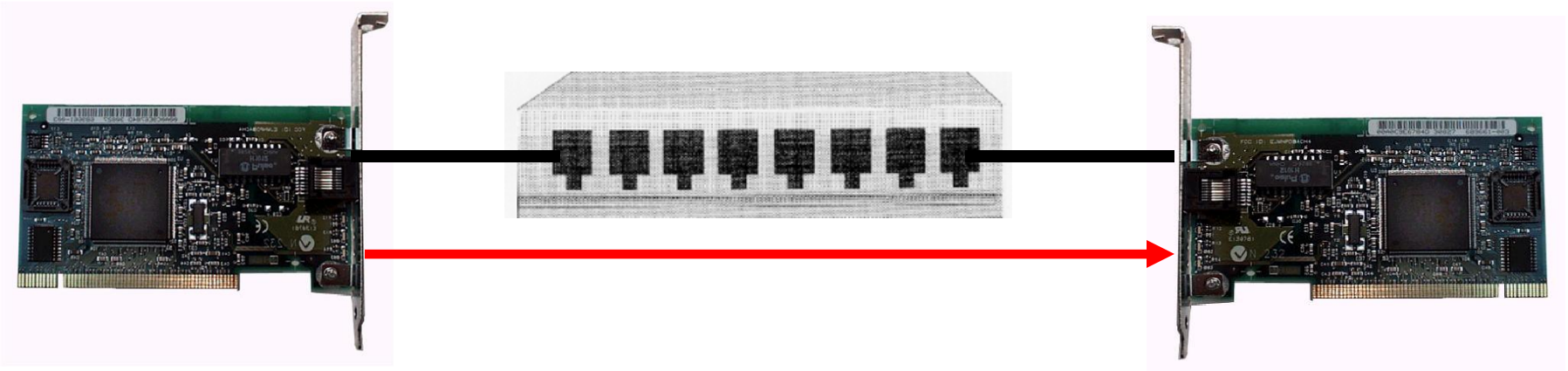


All of that is the same as these!



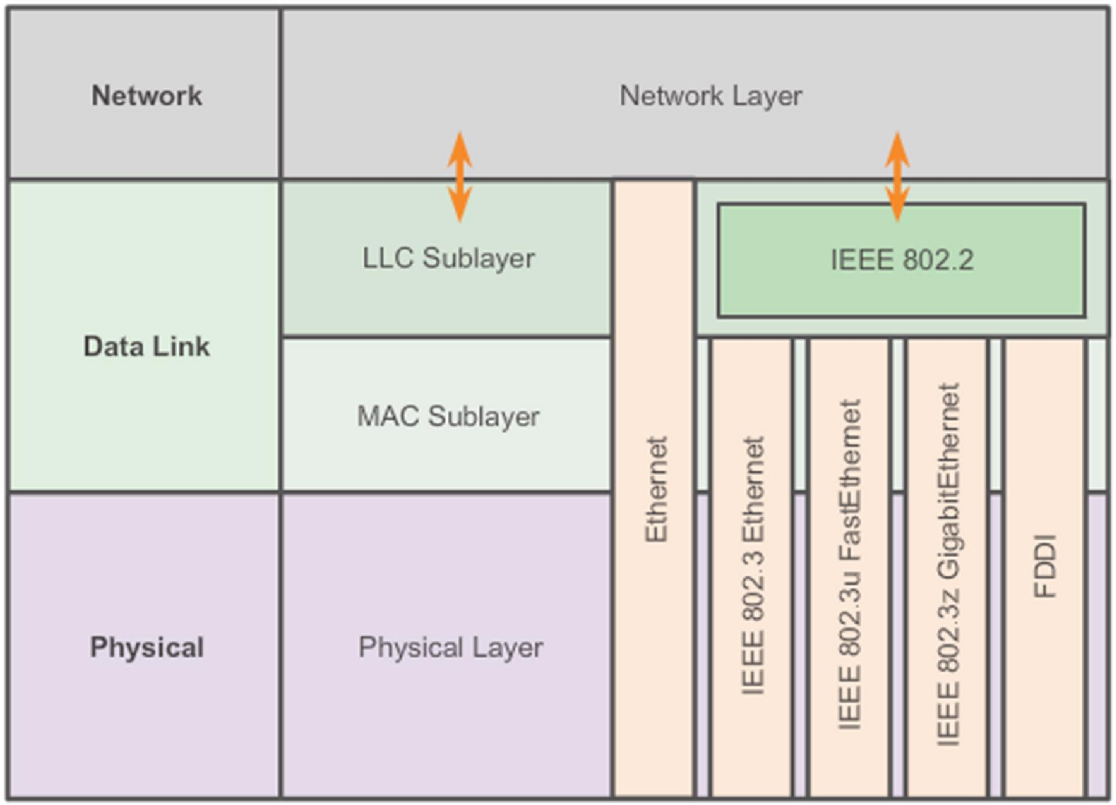


Our focus!



- Ethernet protocol is only concerned with how the information gets from one Ethernet NIC to another.

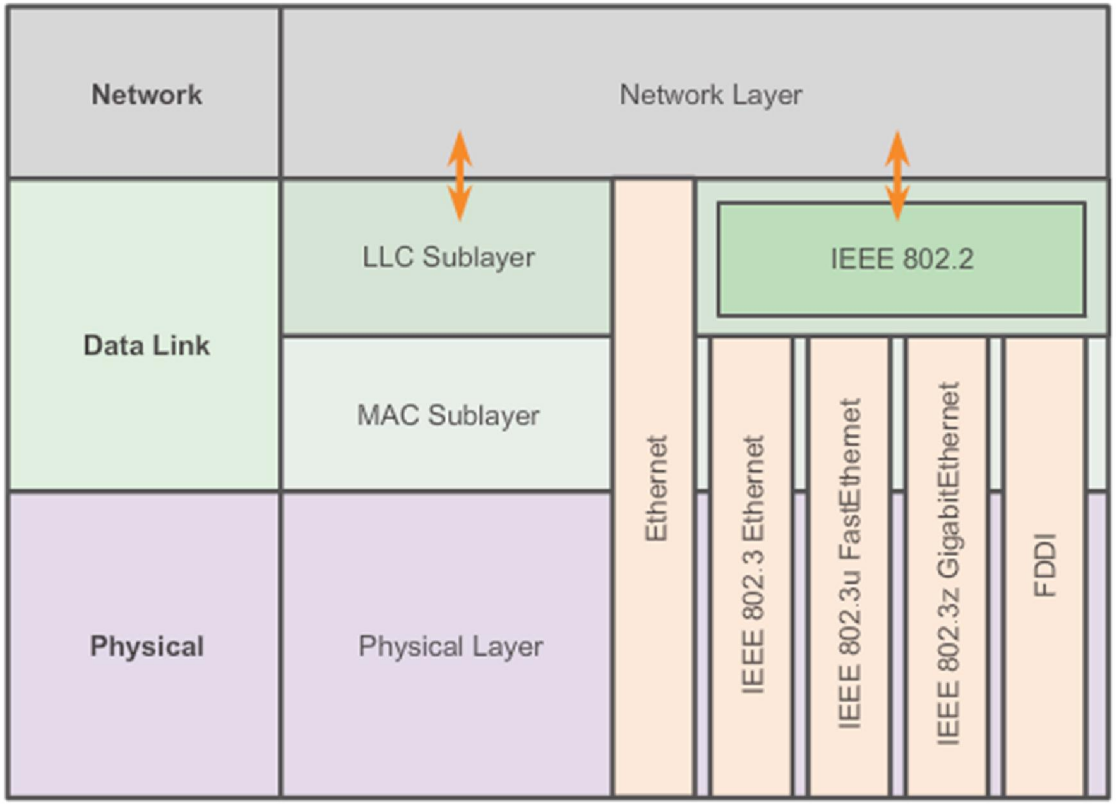
Ethernet Protocol



LLC

- Handles communication between upper and lower layers
- Takes the network protocol data and adds control information to help deliver the packet to the destination

Ethernet Protocol

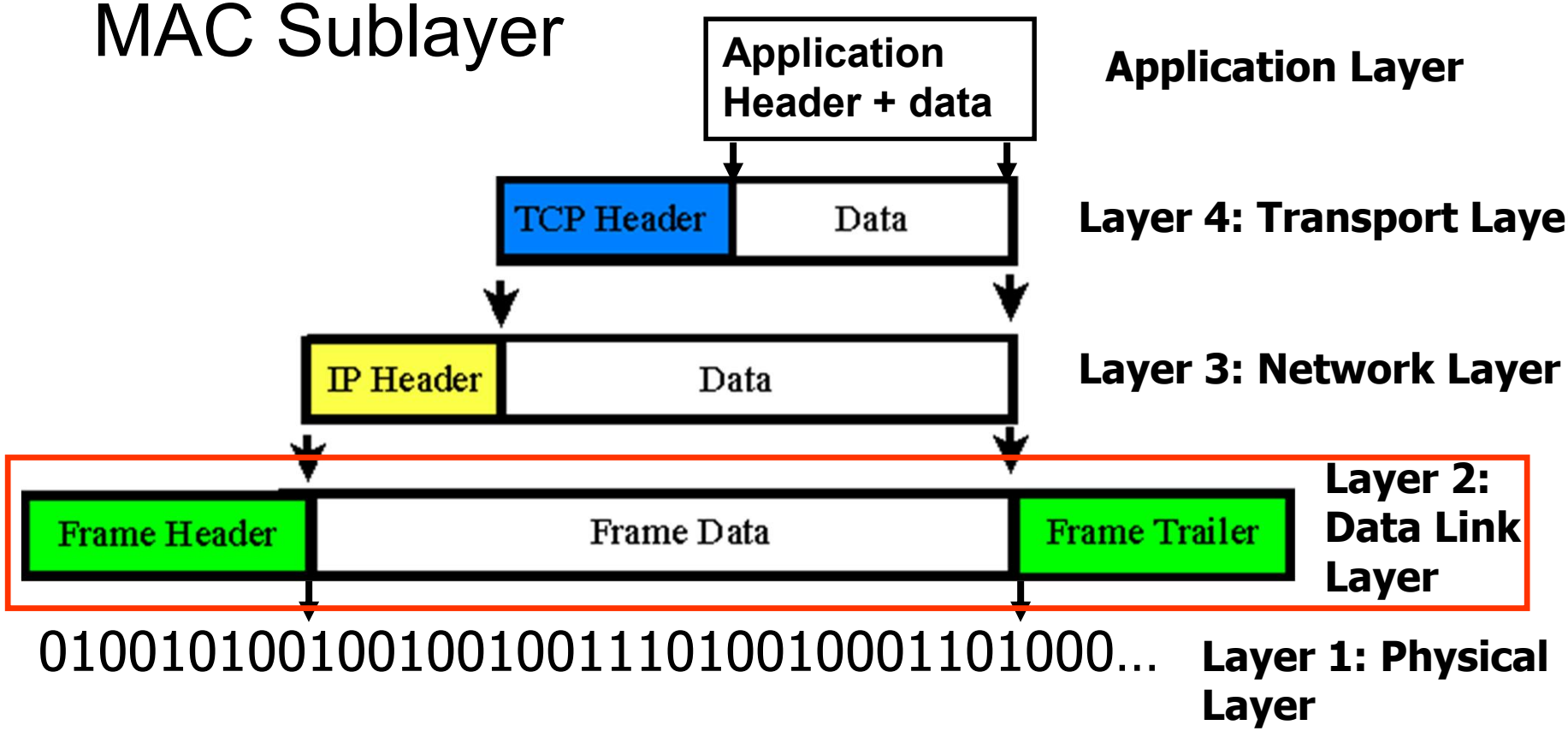


MAC

- Constitutes the lower sublayer of the data link layer
- Implemented by hardware, typically in the computer NIC
- Two primary responsibilities:
  - Data encapsulation
  - Media access control

Ethernet Operation

MAC Sublayer



Data encapsulation

- Frame assembly before transmission and frame disassembly upon reception of a frame
- MAC layer adds a header and trailer to the network layer PDU

Ethernet Operation

MAC Sublayer

Field Length, in Bytes

Ethernet

8	6	6	2	46-1500	4
Preamble	Destination Address	Source Address	Type	Data	FCS

Data encapsulation provides three primary functions:

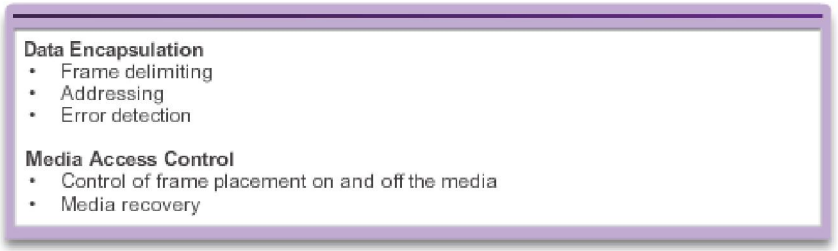
Frame delimiting – identifies a group of bits that make up a frame, synchronization between the transmitting and receiving nodes

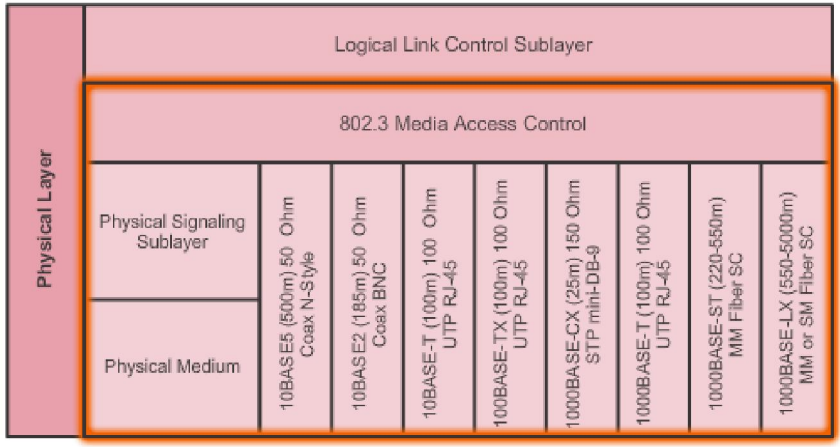
Addressing – each Ethernet header added in the frame contains the physical address (MAC address) that enables a frame to be delivered to a destination node

Error detection - each Ethernet frame contains a trailer with a cyclic redundancy check (CRC) of the frame contents

Ethernet Operation

MAC Sublayer



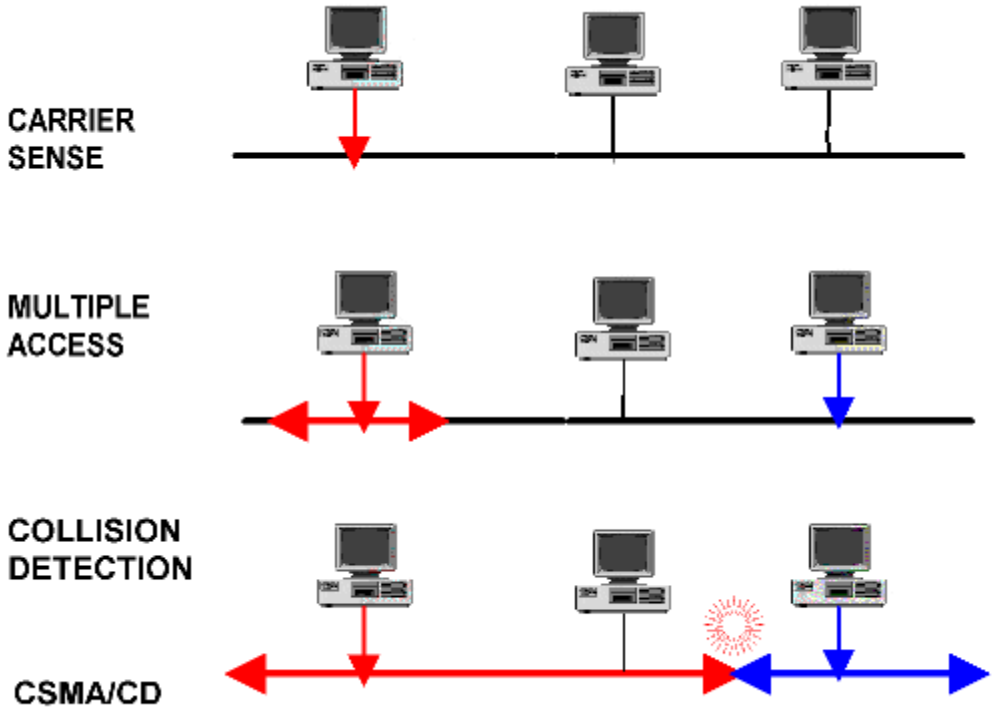


Media Access Control

- Responsible for the placement/removal of frames on 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

Ethernet Operation

Media Access Control



Carrier Sense Multiple Access (CSMA) process

- Used to first detect if the media is carrying a signal
- If no carrier signal is detected, the device transmits its data
- If two devices transmit at the same time - data collision

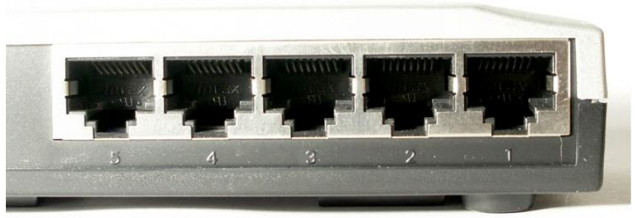
CSMA/CD and Collisions

CSMA/CD (Carrier Sense Multiple Access with Collision Detection)

- **Listens** to the network's shared media to see if any other users on "on the line" by trying to sense a neutral electrical signal or carrier.
- If no transmission is sensed, then *multiple access* **allows anyone onto the media** without any further permission required.
- If two PCs detect a neutral signal and access the shared media at the exact same time, a ***collision*** occurs and is *detected*.
- The PCs sense the collision by being unable to deliver the entire frame (coming soon) onto the network. *(This is why there are minimum frame lengths along with cable distance and speed limitations.)*
- When a collision occurs, a **jamming signal** is sent out by the first PC to detect the collision.
- Using either a **priority or random backoff scheme**, the PCs wait certain amount of time before retransmitting.
- If collisions continue to occur, the PCs random interval is doubled, lessening the chances of a collision.

Ethernet Operation

Media Access Control



CSMA/Collision Detection

- With today's intermediate devices (full-duplex switches), collisions do not occur
- Processes utilized by CSMA/CD are really unnecessary
- Wireless connections in a LAN environment still have to take collisions into account

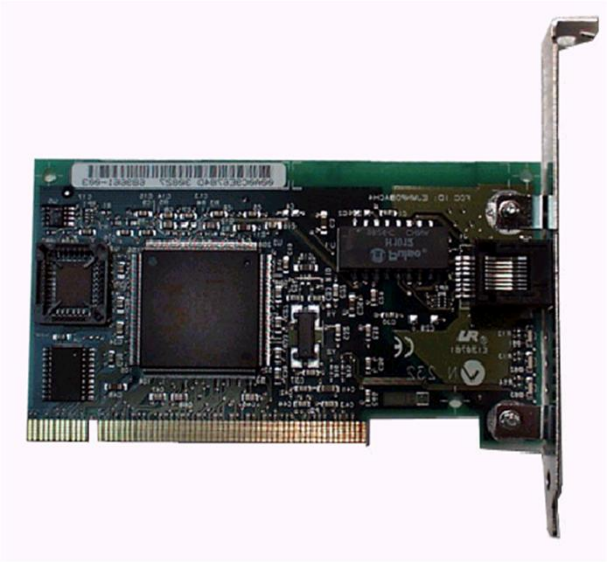
CSMA/Collision Avoidance (CSMA/CA) media access method

- Device examines the media for the presence of data signal - if the media is free, the device sends a notification across the media of its intent to use it
- The device then sends the data.
- Used by 802.11 wireless networking technologies

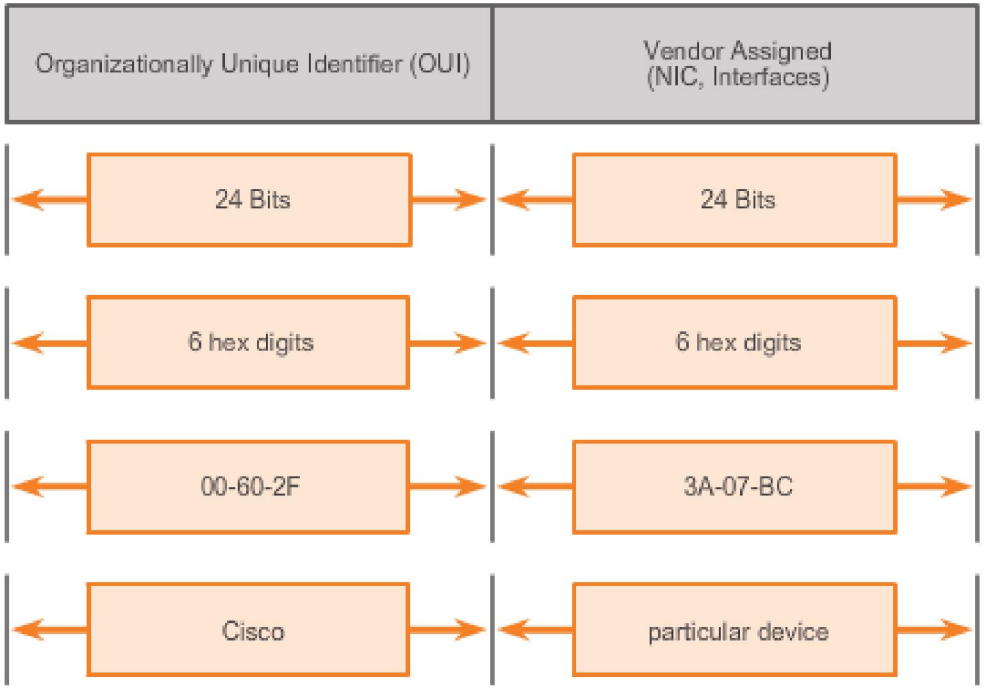
Ethernet Operation

MAC Address: Ethernet Identity

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

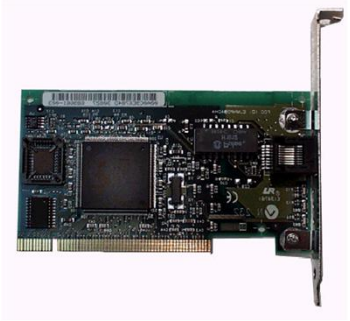


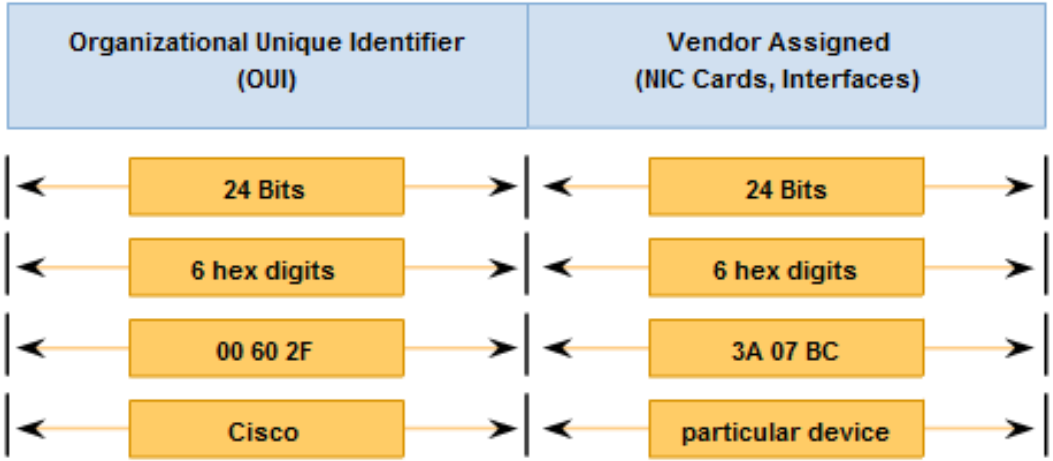
The Ethernet MAC Address Structure



Ethernet Operation

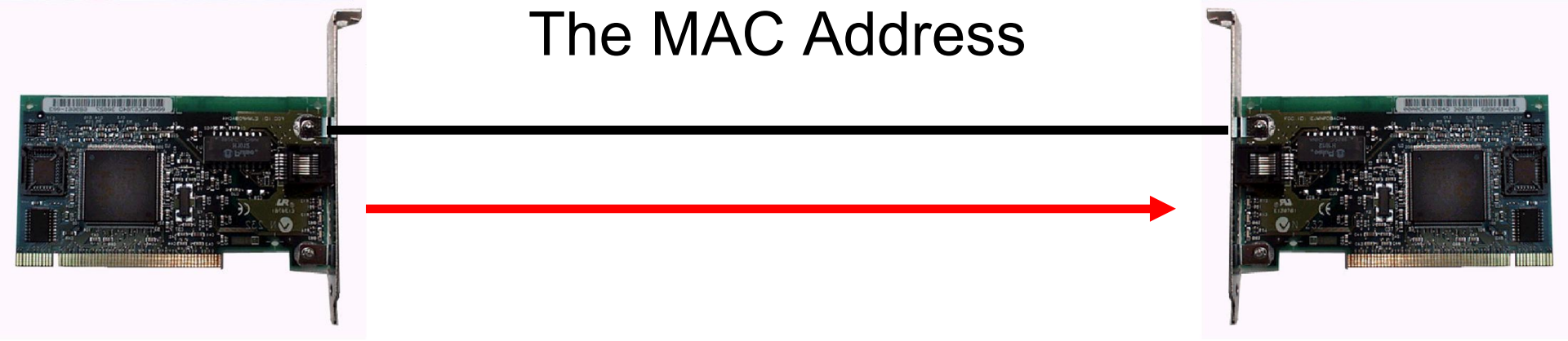
Frame Processing

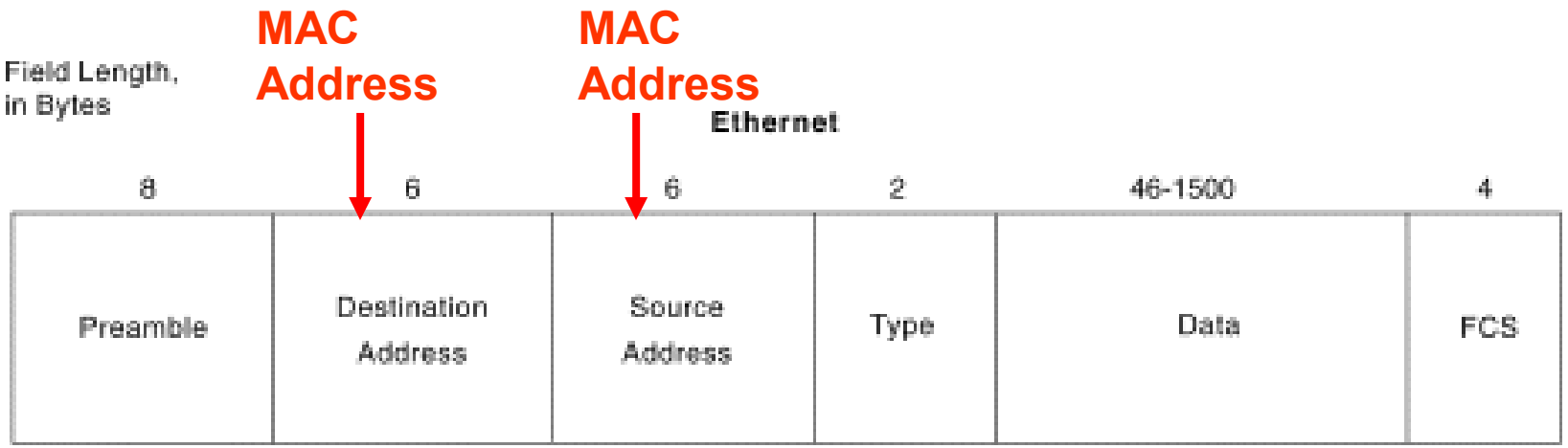




- Every device with an Ethernet NIC has a MAC addresses assigned:
  - workstations, servers, printers, switches, and routers
- MAC addresses are sometimes referred to as ***burned-in addresses (BIAs)***
- Examples: 00-05-9A-3C-78-00, 00:05:9A:3C:78:00, or 0005.9A3C.7800
- Ethernet header contains the 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

The MAC Address

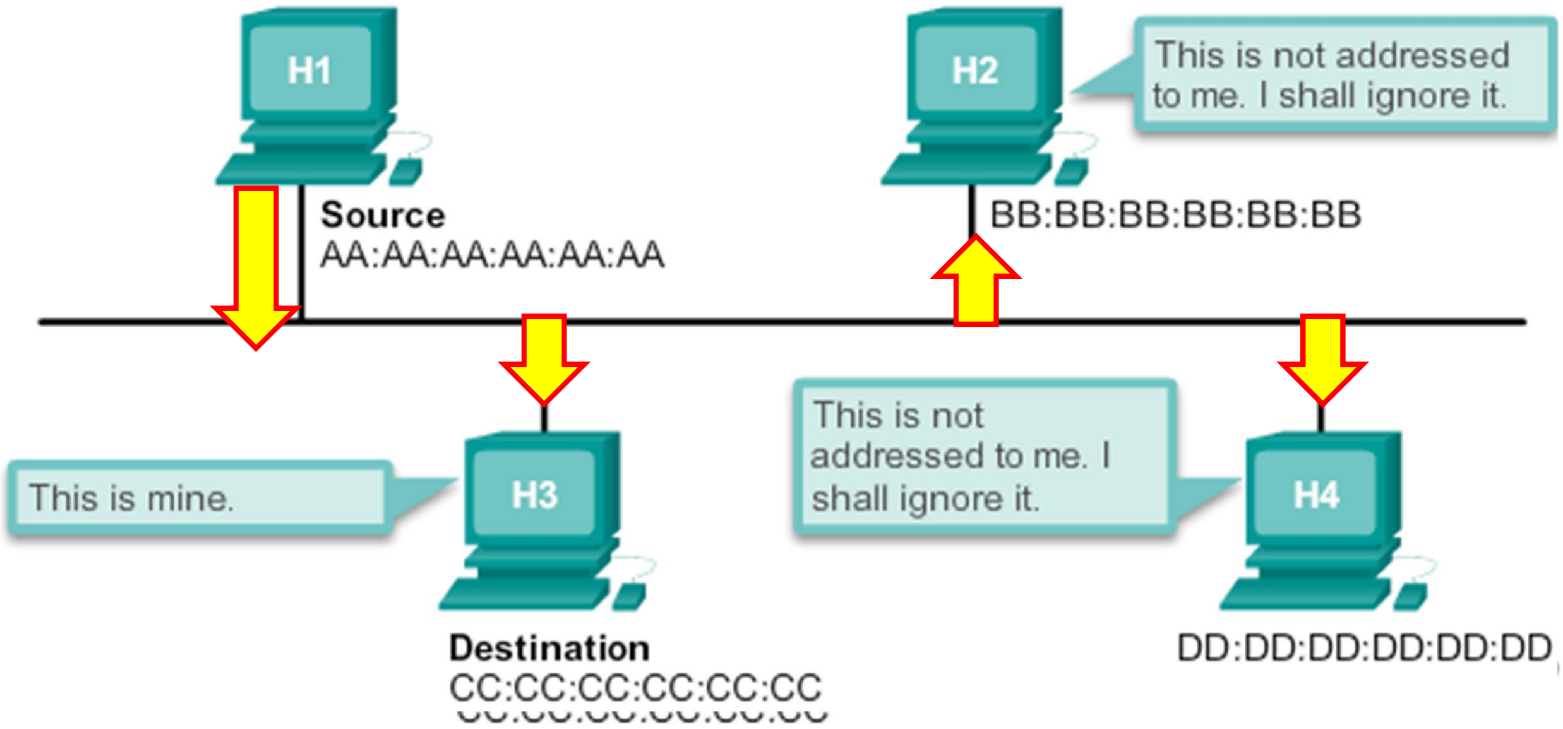




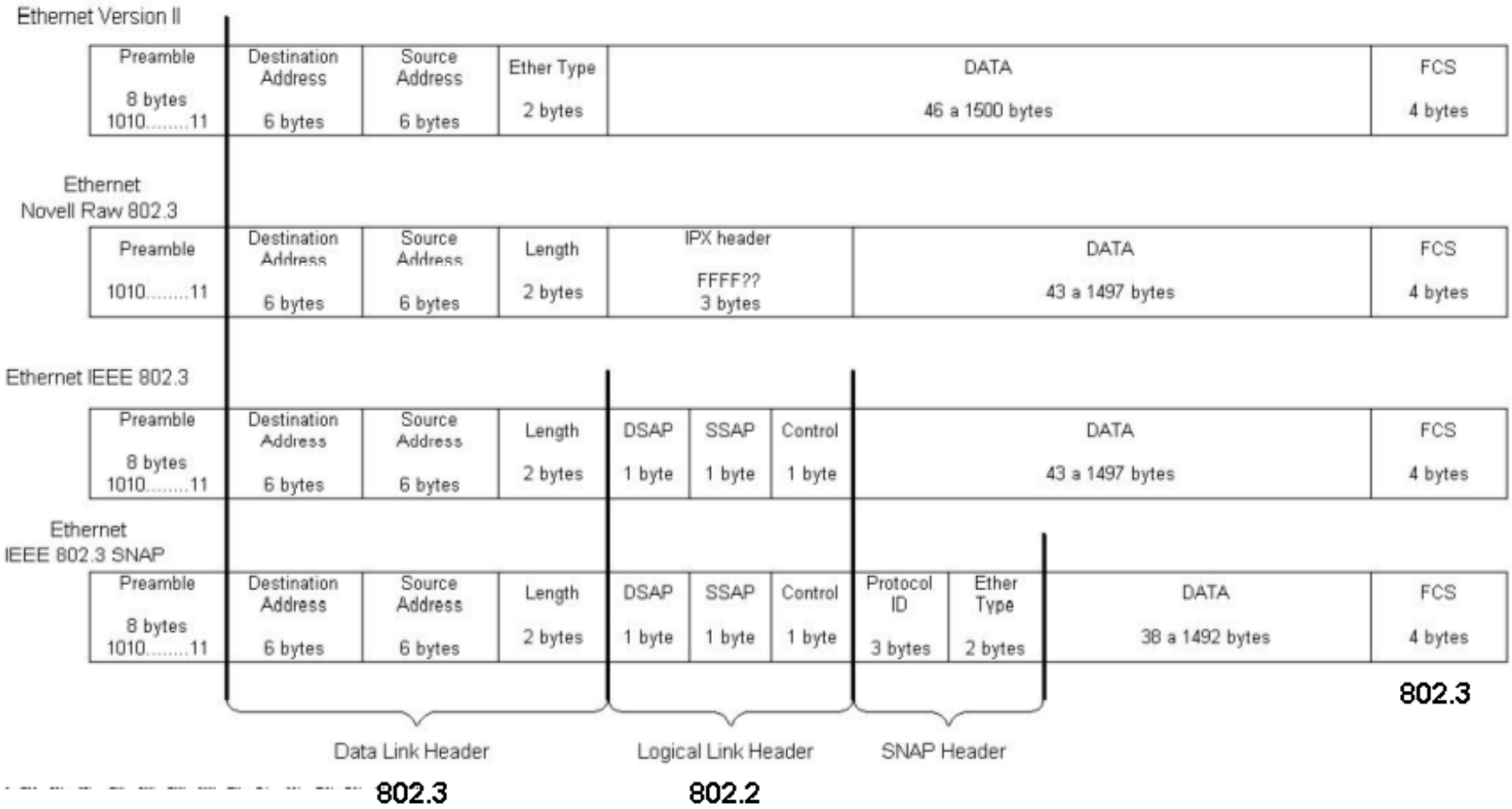
- The Ethernet protocol uses MAC addresses to identify the **source** of the Ethernet frame and the **destination** of the Ethernet frame.
- Whenever is computer sends an Ethernet frame, it includes the MAC address on its NIC as the Source “MAC” Address.
- We will learn later how it learns the Destination “MAC” Address.
- We will see how all of this works in a moment.

Frame Forwarding

Destination Address	Source Address	Data
CC:CC:CC:CC:CC:CC	AA:AA:AA:AA:AA:AA	Encapsulated data
Frame Addressing		



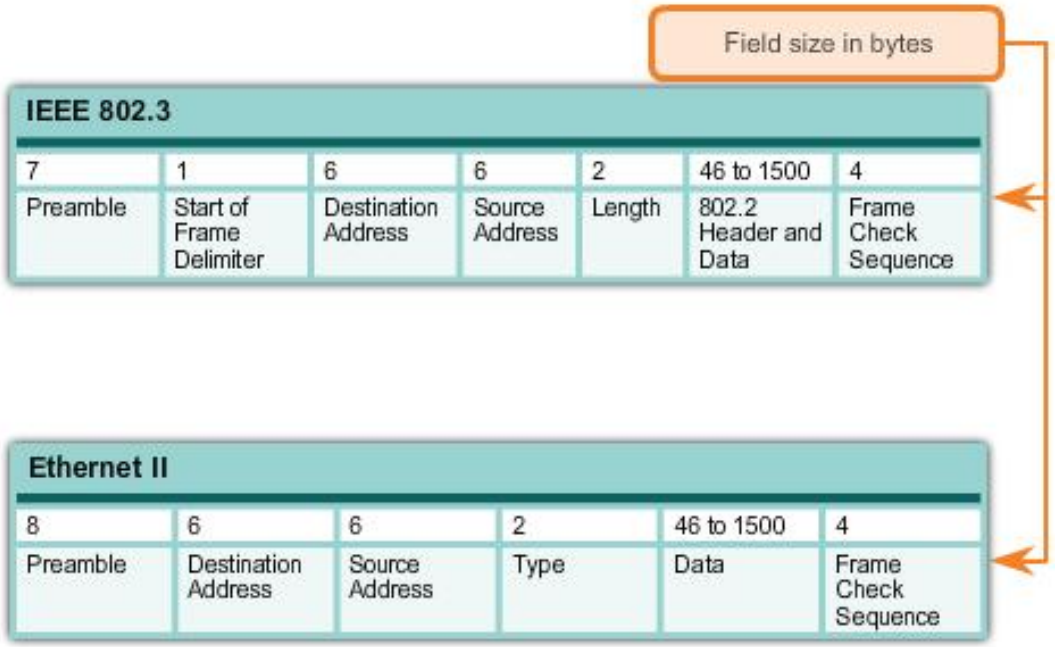
Ethernet Frame Attributes



Ethernet Frame Attributes

Ethernet Encapsulation

- Early versions of Ethernet were relatively slow at 10 Mbps
- Now operate at 10 Gigabits per second and faster
- Ethernet frame structure adds headers and trailers around the Layer 3 PDU to encapsulate the message being sent



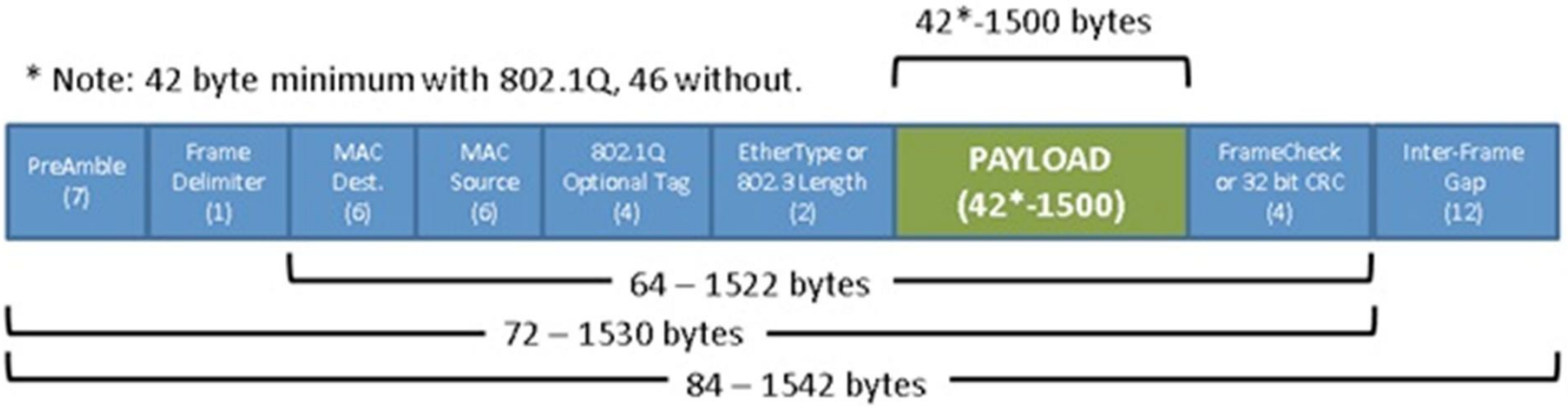
Ethernet II is the Ethernet frame format used in TCP/IP networks.

Evolution of the Ethernet Standard

- **1979** Bob Metcalfe developed Ethernet at XEROX PARC
- **1980** DEC-Intel-Xerox (DIX) publish first original 10 Mbps Ethernet Standard over thick coaxial cable
- **1985** IEEE 802.3 used DIX standard and published standard with the title *IEEE 802.3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications*
- **Supplements**
  - 1985 10BASE2 Thin Ethernet
  - 1990 10BASE-T Twisted-pair
  - 1995 100BASE-T Fast Ethernet and Autonegotiation
  - 1997 Full Duplex Standard
  - 1998 1000BASE-X Gigabit Ethernet

Ethernet Frame Attributes

Ethernet Frame Size

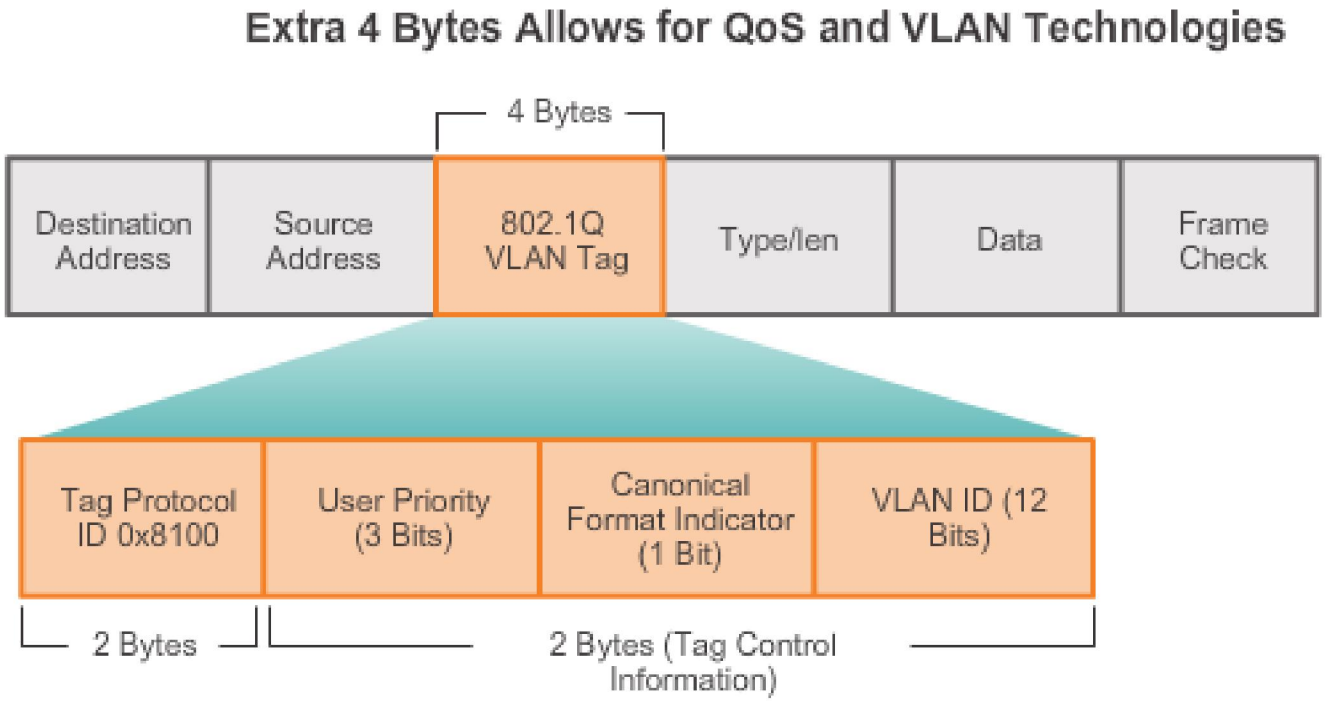


- Ethernet II and IEEE 802.3 standards define:
  - minimum frame size as 64 bytes
  - maximum as 1518 bytes
- "collision fragment" or "runt frame" – Frame less than 64 bytes
- If size of a transmitted frame is less than the minimum or greater than the maximum, the receiving device drops the frame
- At the physical layer, different versions of Ethernet vary in their method for detecting and placing data on the media

Ethernet Frame Attributes

Ethernet Frame Size

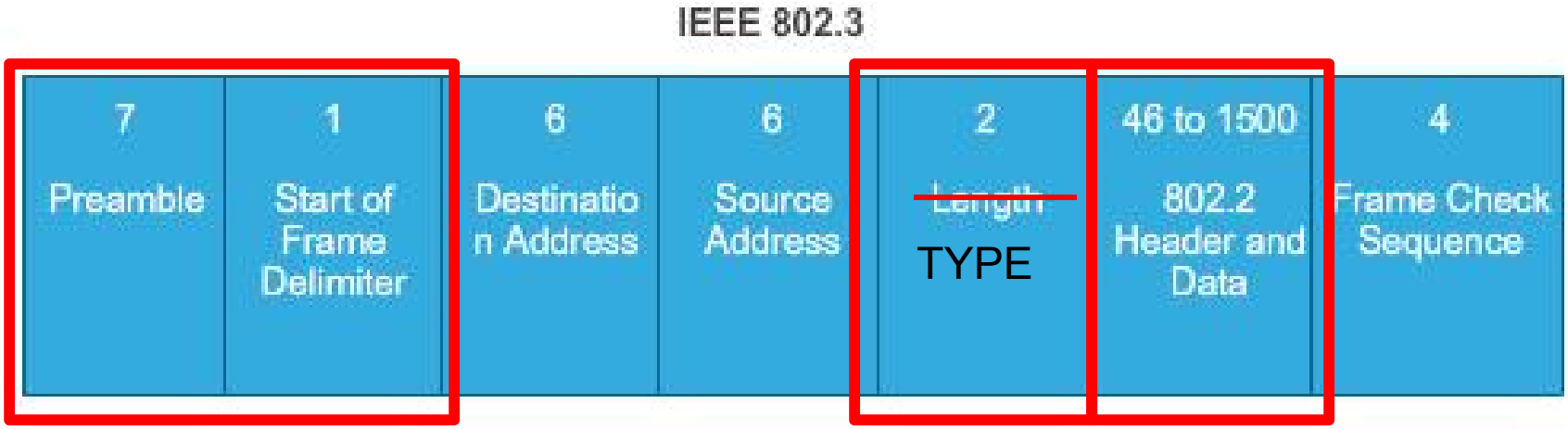
The figure displays the fields contained in the 802.1Q VLAN tag



- In 1998, IEEE 802.3ac standard extended the maximum allowable frame size to 1522 bytes.
- Increased to accommodate a technology called Virtual Local Area Network (VLAN).
- VLANs will be presented in a later course.

Ethernet Frame Attributes

Introduction to the Ethernet Frame



Preamble and Start Frame Delimiter Fields
Used for synchronization between the sending and receiving devices

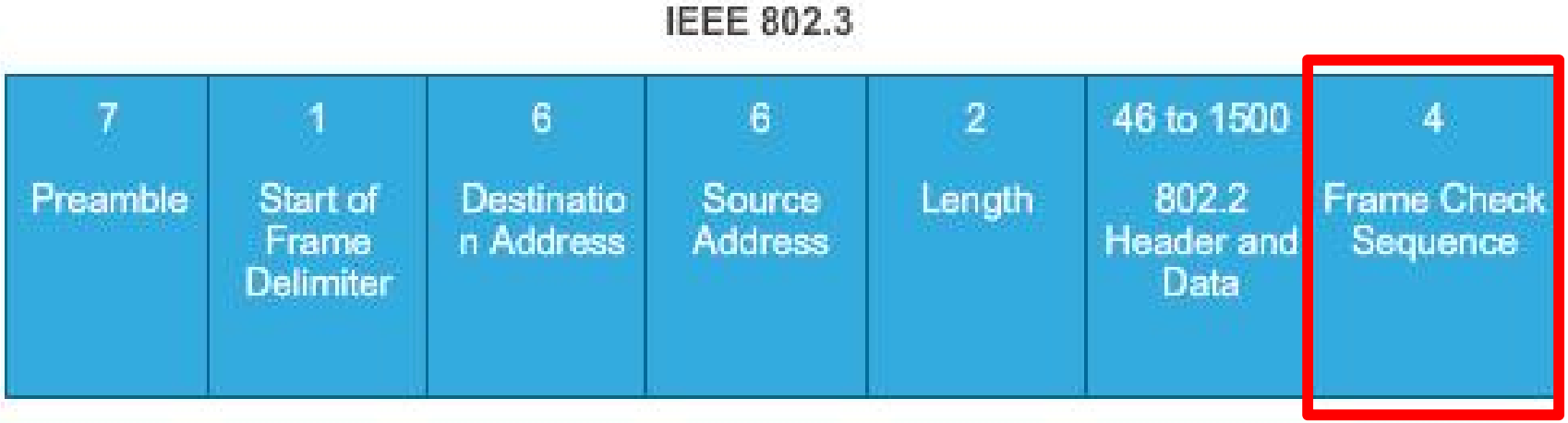
Length Field (Prior to 1997)
Defines the exact length of the frame's data field

Type Field
Describes which protocol is implemented

Data and Pad Fields
Contain the encapsulated data from a higher layer, an IPv4 packet

Ethernet Frame Attributes

Introduction to the Ethernet Frame



Frame Check Sequence Field
Used to detect errors in a frame with cyclic redundancy check (4 bytes), if calculations match at source and receiver, no error occurred.

Ethernet MAC

MAC Addresses and Hexadecimal

Decimal and Binary equivalents of 0 to F Hexadecimal

Decimal	Binary	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Selected Decimal, Binary and Hexadecimal equivalents

Decimal	Binary	Hexadecimal
0	0000 0000	00
1	0000 0001	01
2	0000 0010	02
3	0000 0011	03
4	0000 0100	04
5	0000 0101	05
6	0000 0110	06
7	0000 0111	07
8	0000 1000	08
10	0000 1010	0A
15	0000 1111	0F
16	0001 0000	10
32	0010 0000	20
64	0100 0000	40
128	1000 0000	80
192	1100 0000	C0
202	1100 1010	CA
240	1111 0000	F0
255	1111 1111	FF

Ethernet MAC

MAC Address Representations

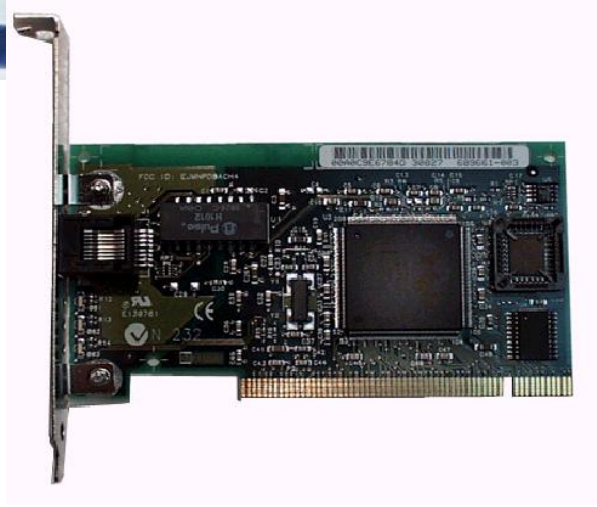
With Dashes 00-60-2F-3A-07-BC

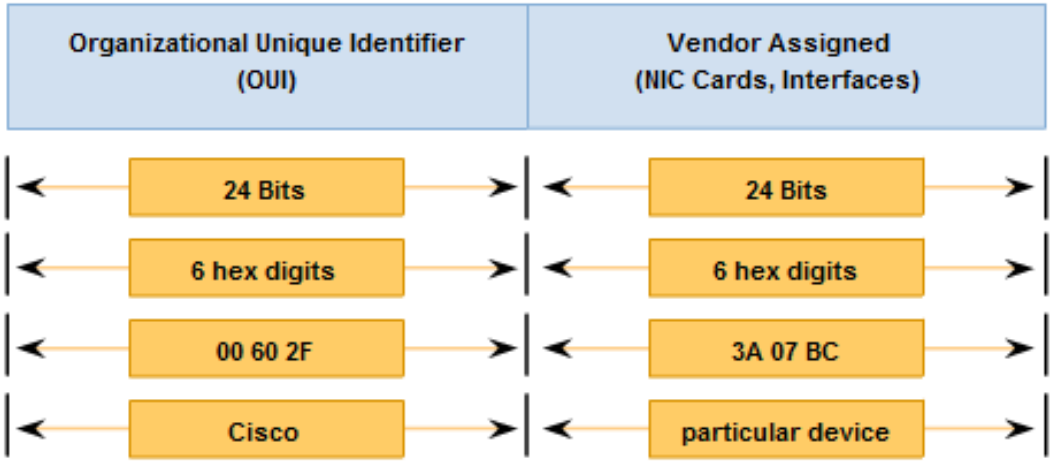
With Colons 00:60:2F:3A:07:BC

With Periods 0060.2F3A.07BC

```
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
```

MAC Address Format



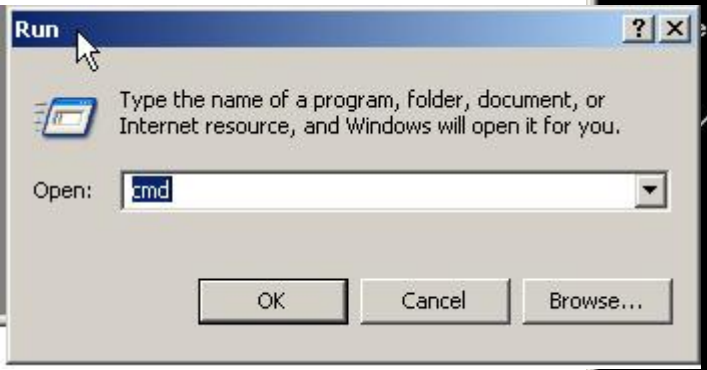


Dec	Bin	Hex	Dec	Bin	Hex
0	0000	0	8	1000	8
1	0001	1	9	1001	9
2	0010	2	10	1010	A
3	0011	3	11	1011	B
4	0100	4	12	1100	C
5	0101	5	13	1101	D
6	0110	6	14	1110	E
7	0111	7	15	1111	F

OUI **unique**

- An Intel MAC address: **00-21-CC-BA-44-C4**
- 0000 0000 - 0010 0001 – 1100 1100 - 1011 1010 – 0100 0100 – 1100 0100
- IEEE OUI FAQs: http://standards.ieee.org/faqs/OUI.html

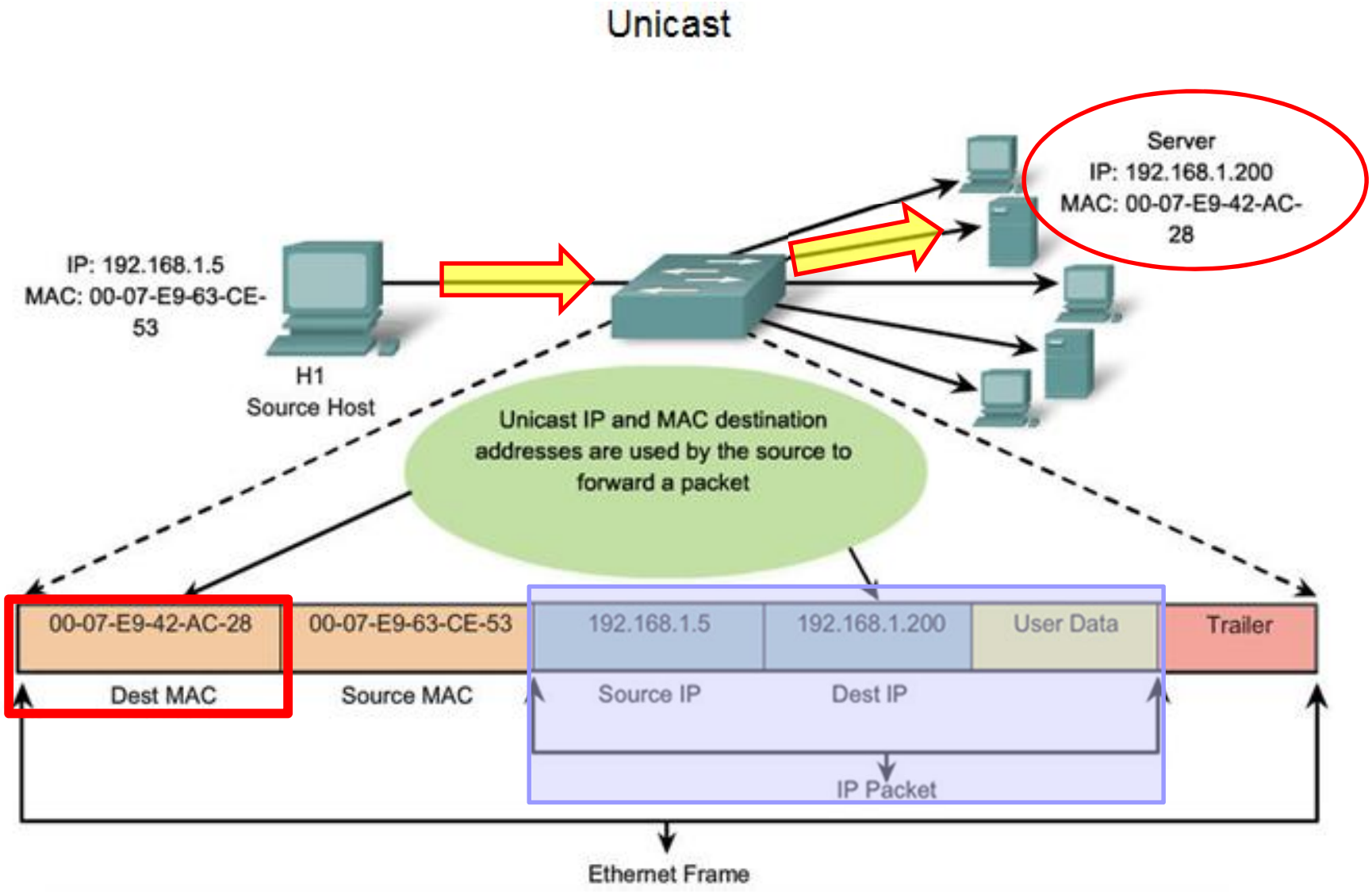
What is the Address on my NIC?




```
C:\WINNT\System32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : cabrillo.edu
        IP Address. . . . . . . . . . . . : 172.16.22.73
        Subnet Mask . . . . . . . . . . . : 255.255.224.0
        Default Gateway . . . . . . . . . : 172.16.1.1

C:\>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : RICK-GRAZIANI
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

t adapter Local Area Connection:

        Connection-specific DNS Suffix  . : cabrillo.edu
        Description . . . . . . . . . . . : Intel 8255x-based PCI Ethernet Adapt
100)
        Physical Address. . . . . . . . . : 00-20-E0-6B-17-62
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 172.16.22.73
        Subnet Mask . . . . . . . . . . . : 255.255.224.0
        Default Gateway . . . . . . . . . : 172.16.1.1
        DHCP Server . . . . . . . . . . . : 172.16.1.7
        DNS Servers . . . . . . . . . . . : 207.62.187.53
                                            207.62.187.54
        Primary WINS Server . . . . . . . : 171.69.2.87
        Secondary WINS Server . . . . . . : 171.68.235.228
        Lease Obtained. . . . . . . . . . : Wednesday, March 10, 2004 9:48:23 AM

        Lease Expires . . . . . . . . . . : Saturday, March 13, 2004 9:48:23 AM

C:\>_
```

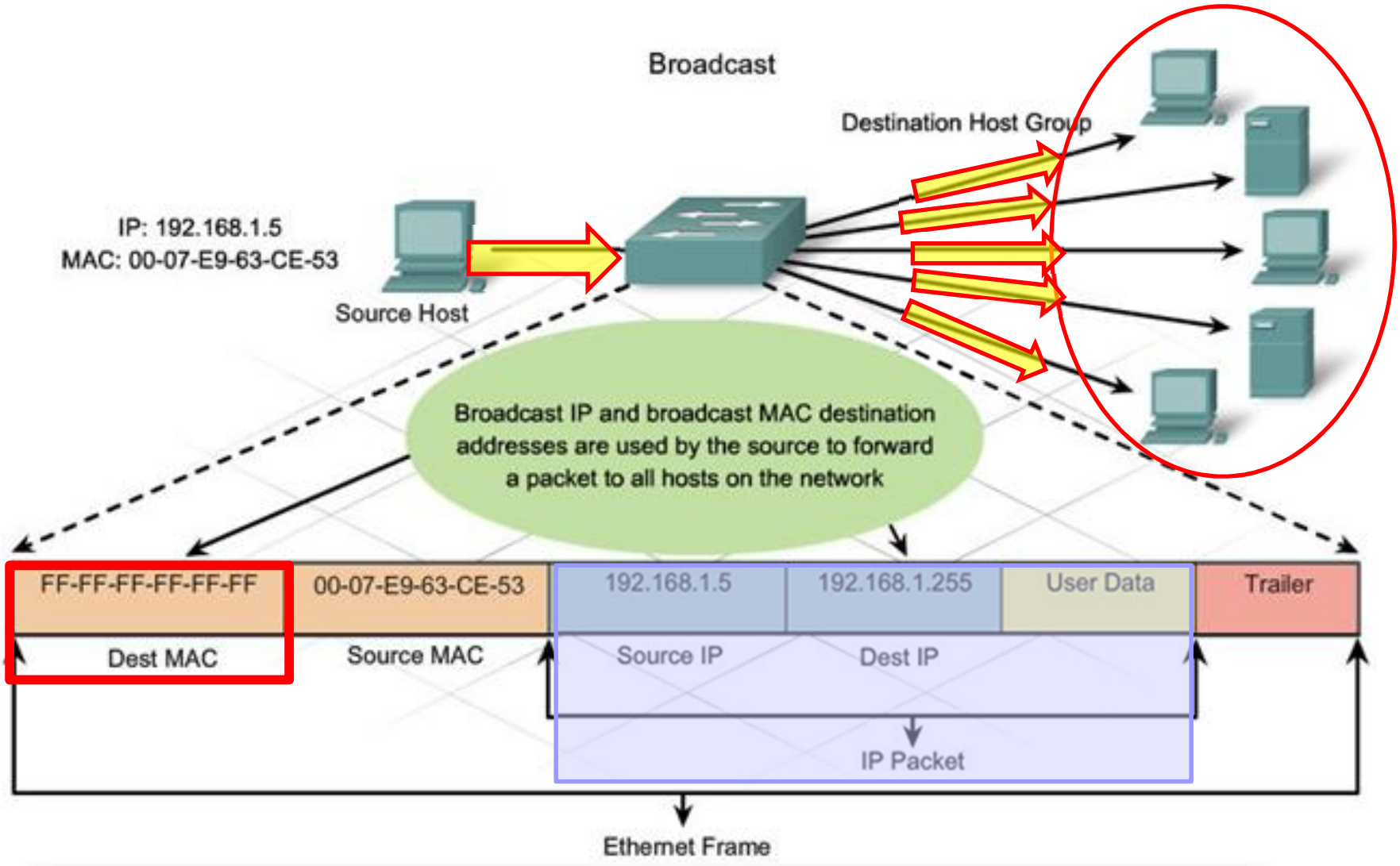
Ethernet MAC

Unicast MAC Address



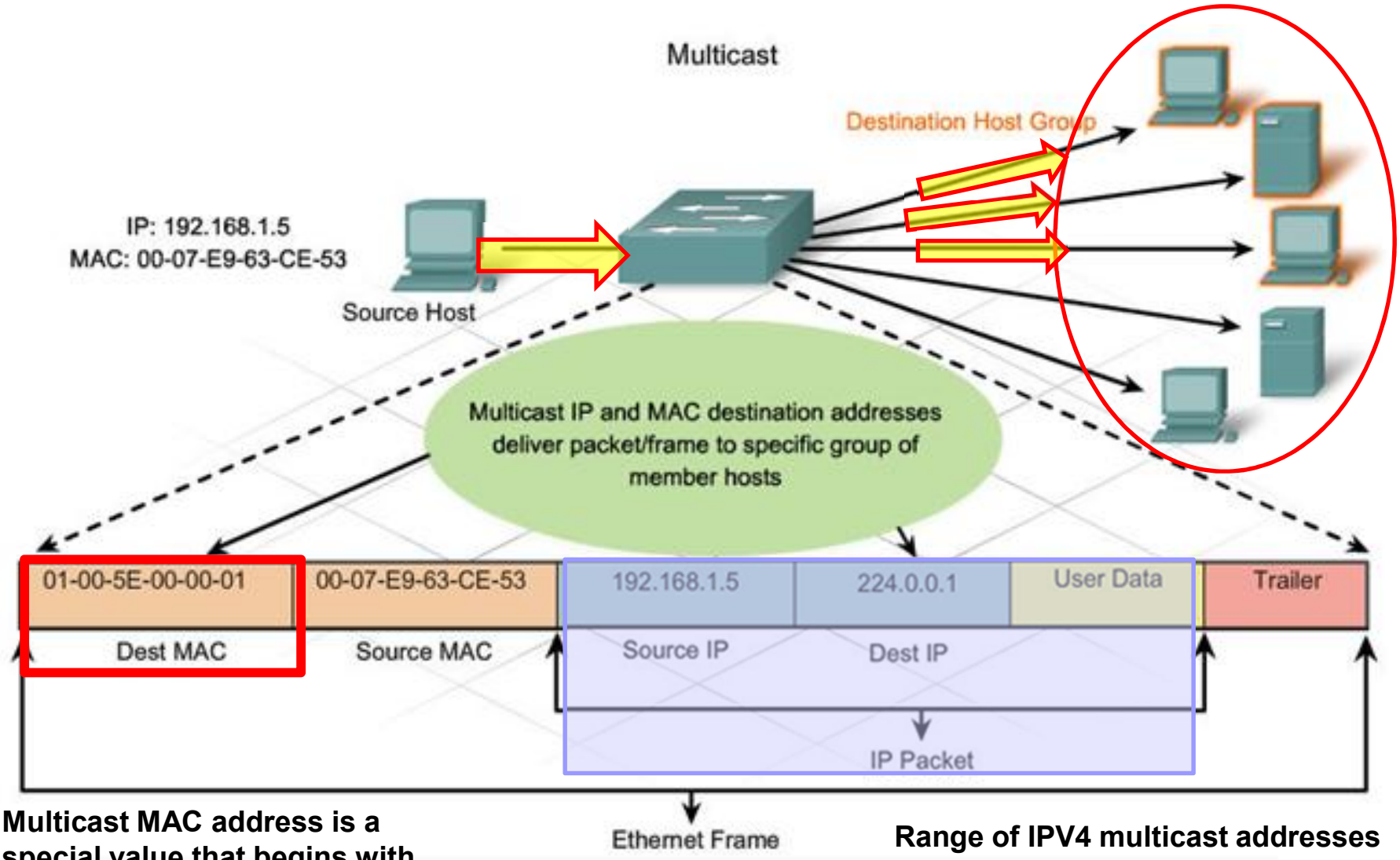
Ethernet MAC

Broadcast MAC Address



Ethernet MAC

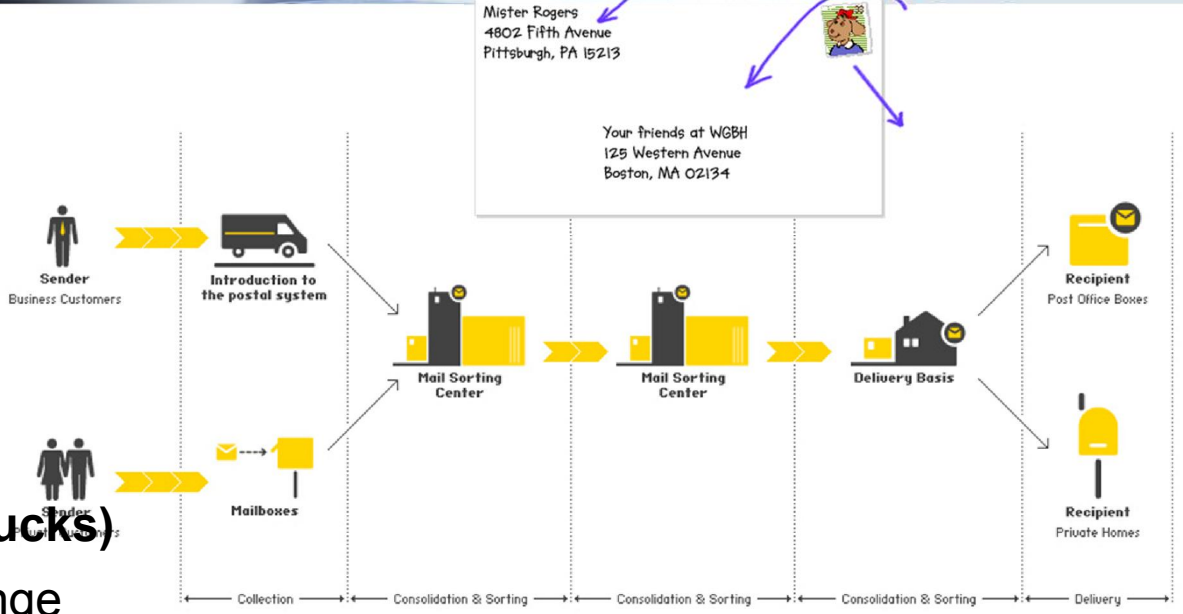
Multicast MAC Address



Multicast MAC address is a special value that begins with 01-00-5E in hexadecimal

Range of IPV4 multicast addresses is 224.0.0.0 to 239.255.255.255

MAC and IP



MAC address (Different Trucks)

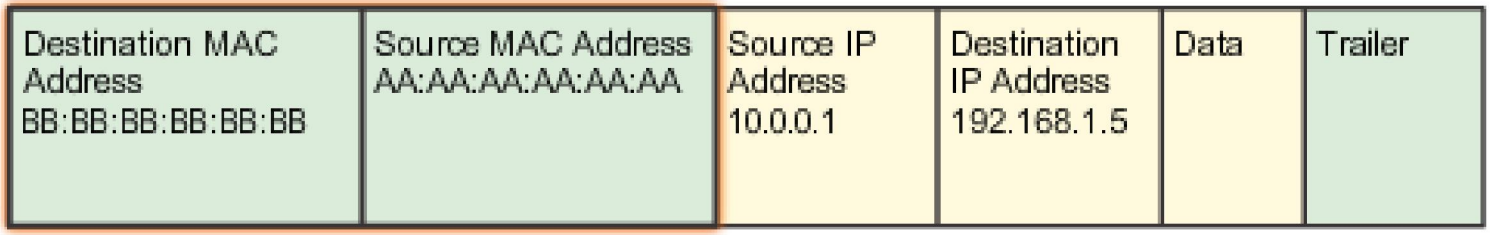
- This address does not change
- Similar to the name of a person
- Known as physical address because physically assigned to the host NIC

IP address (Mail Envelope)

- Similar to the address of a person
- Based on where the host is actually located
- Known as a logical address because assigned logically
- Assigned to each host by a network administrator

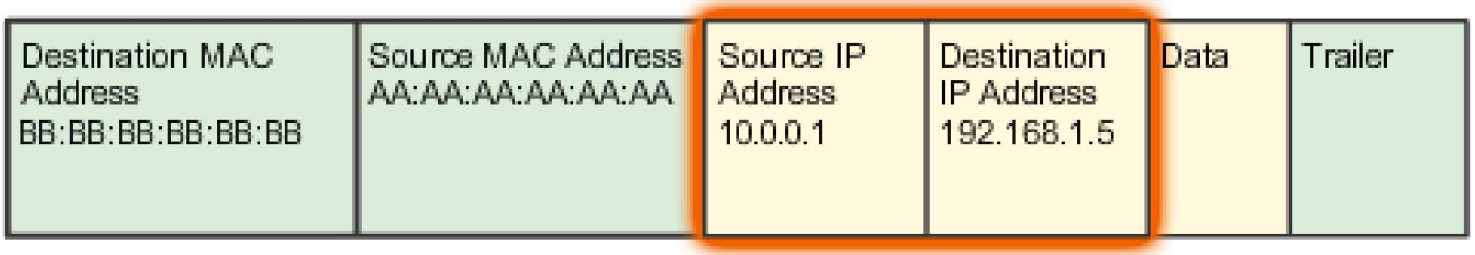
Both the physical MAC and logical IP addresses are required for a computer to communicate just like both the name and address of a person are required to send a letter

Ethernet MAC
NIC-to-NIC Connectivity (same network) - MAC



A switch examines MAC addresses.

End-to-End Connectivity (same or different network) – IP



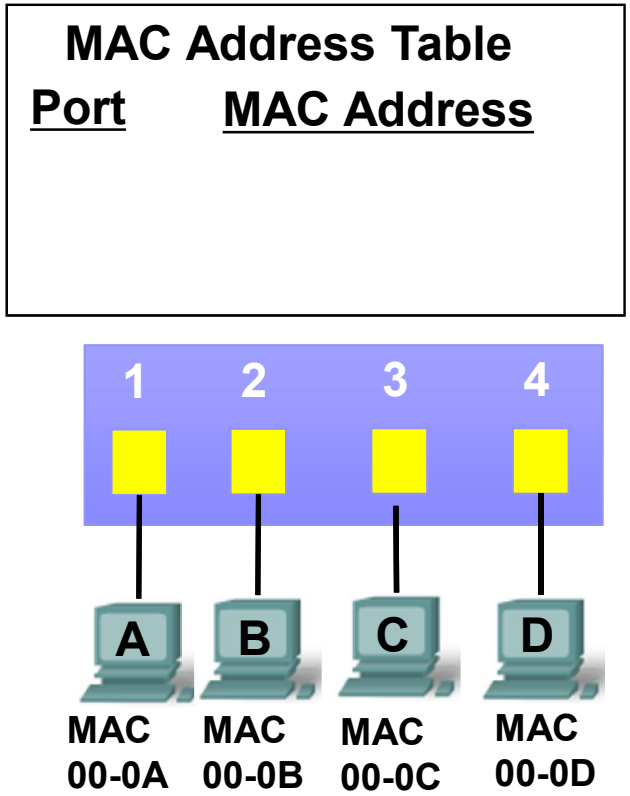
A router examines IP addresses

Switch Process

For every frame that enters a switch…

- Learning Stage (Building/Updating of SAT/MAC table)
  - Examines **Source MAC Address**:
    - If **Source MAC Address** is in the SAT/MAC table, update 5 minute timer
    - If **Source MAC Address** is NOT in the SAT/MAC table, add Source MAC Address and incoming port number to SAT/MAC table
- Forwarding Stage (Flood or Filter)
  - Examines **Destination MAC Address**:
    - If **Destination MAC Address** is in the SAT/MAC table, forward the frame only out that port (**Filter**), unless it is the outgoing port is the same as the incoming port (checks Source MAC Address)
    - If **Destination MAC Address** is NOT in the SAT/MAC table, forward the frame only out all ports except incoming port (**Flood**)

Learn: Examine Source MAC Address



MAC addresses are shortened for demonstration purposes.

Learn: Examine Source MAC Address

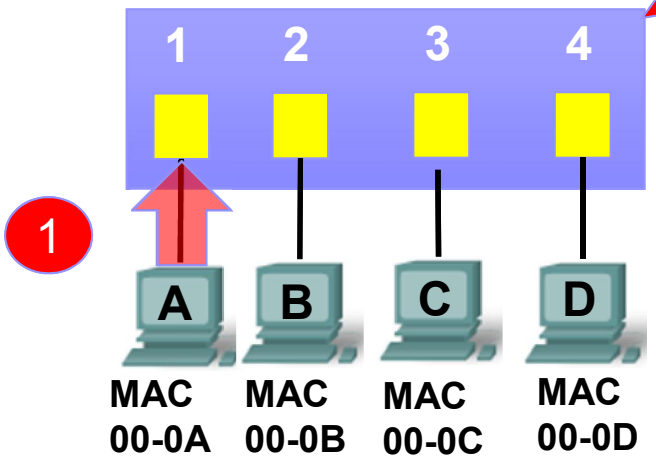
Port and Source MAC address added

2

MAC Address Table

Port	MAC Address
1	00-0A

I don't have this source MAC address and the incoming port in my table so I will add it.



1

2

Destination MAC 00-0D	Source MAC 00-0A	Type	Data	FCS

MAC addresses are shortened for demonstration purposes.

Forward: Examine Destination MAC Address

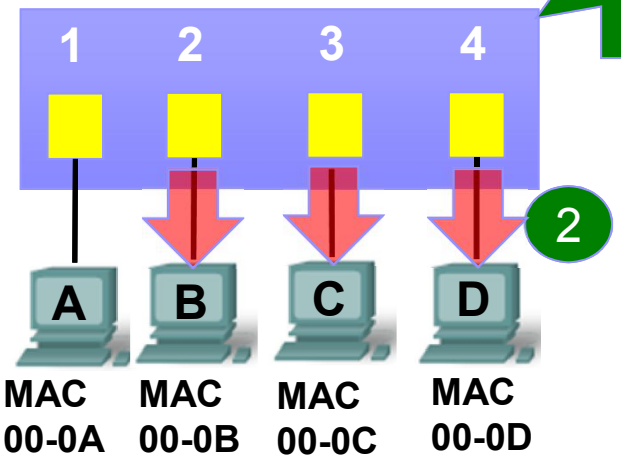
MAC Address Table

Port	MAC Address
1	00-0A

Destination MAC address not in table

1

I don't have this destination MAC address in my table so I will send this unknown unicast out all ports.



1

2

Destination MAC 00-0D	Source MAC 00-0A	Type	Data	FCS

MAC addresses are shortened for demonstration purposes.

Learn: Examine Source MAC Address

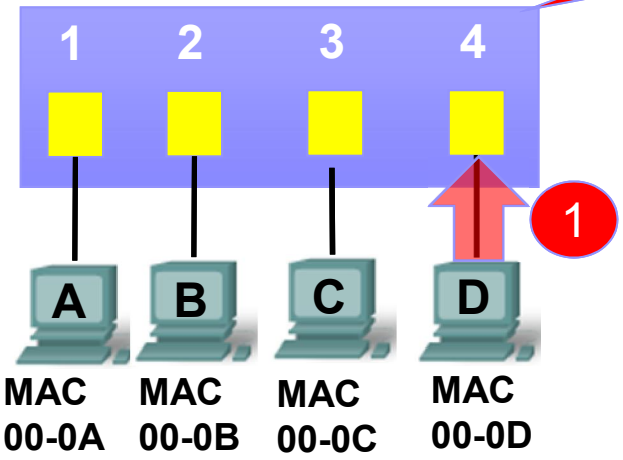
Port and Source MAC address added

1

MAC Address Table

Port	MAC Address
1	00-0A
4	00-0D

I don't have this source MAC address and the incoming port in my table so I will add it.



1

2

3

Destination MAC 00-0A	Source MAC 00-0D	Type	Data	FCS

MAC addresses are shortened for demonstration purposes.

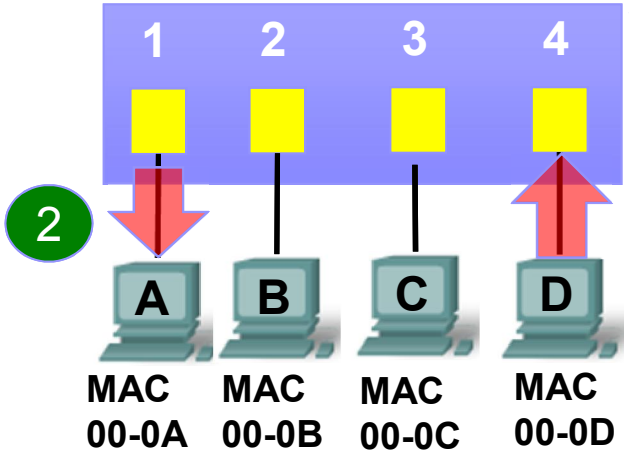
Forward: Examine Destination MAC Address

MAC Address Table

Port	MAC Address
1	00-0A
4	00-0D

2

I know the destination MAC address so I will only forward the frame out port 1.



1

2

3

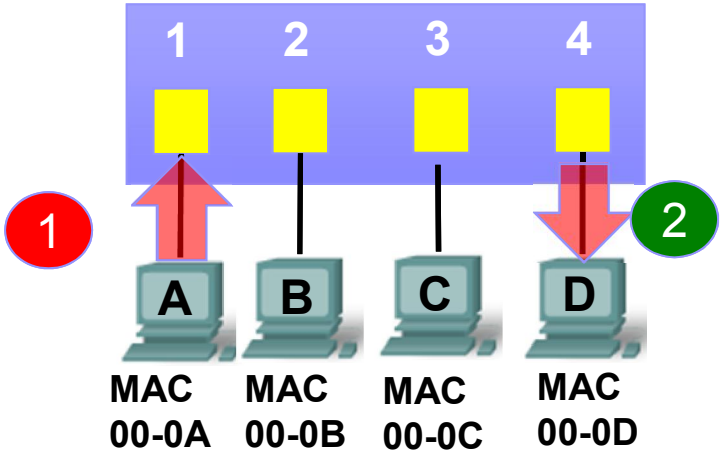
Destination MAC 00-0A	Source MAC 00-0D	Type	Data	FCS

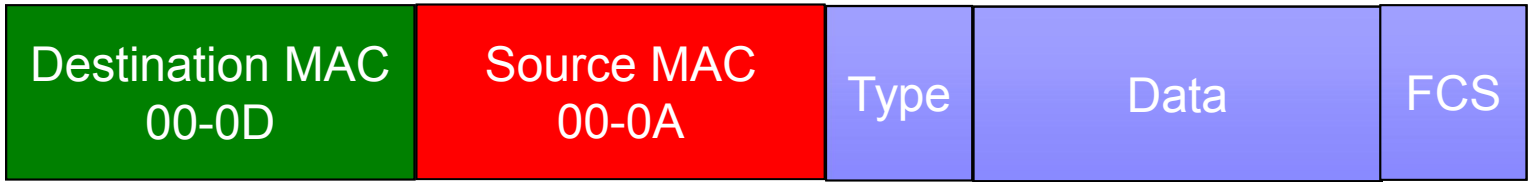
MAC addresses are shortened for demonstration purposes.

Learn: Examine Source MAC Address

MAC Address Table

Port	MAC Address
1	00-0A
4	00-0D



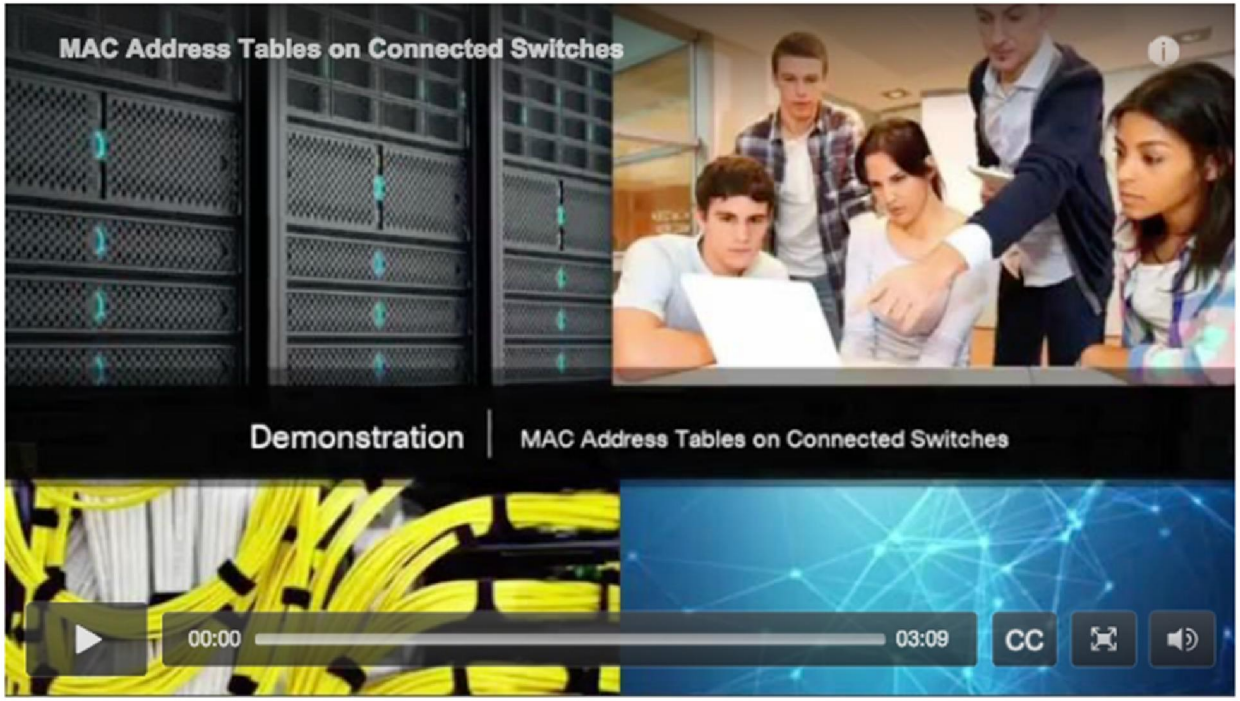


1

2

3

MAC addresses are shortened for demonstration purposes.



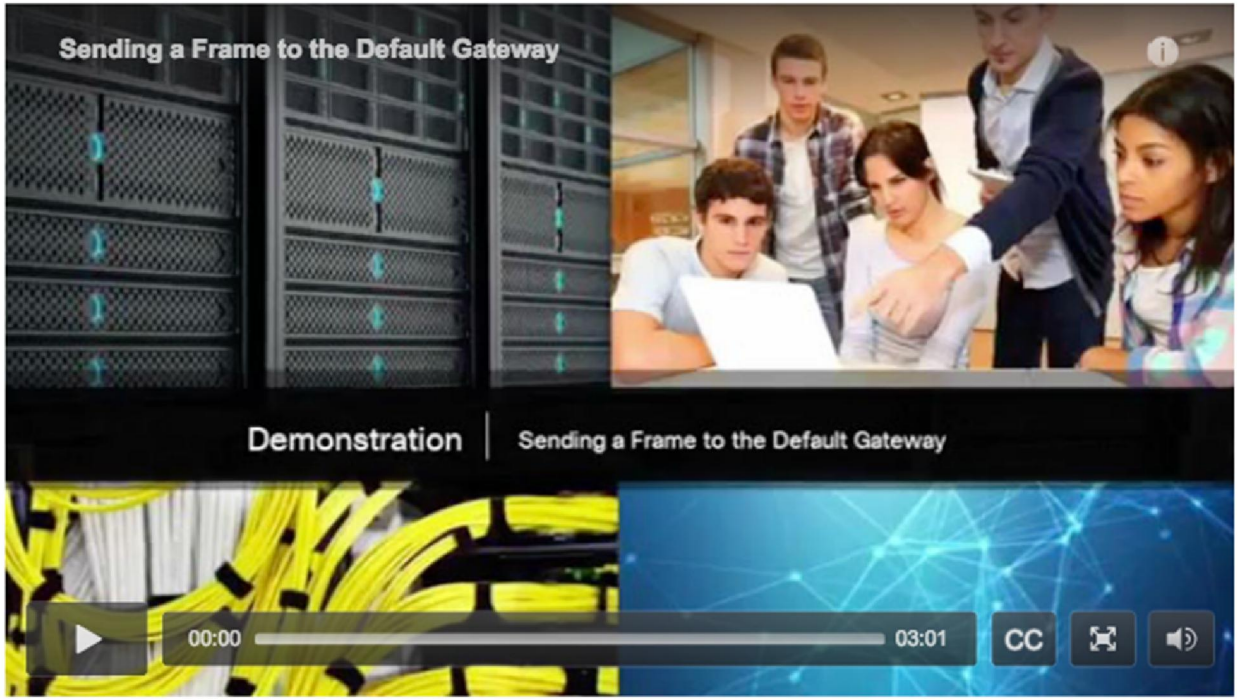
Video Demonstration - MAC Address Tables on Connected Switches

A switch can have multiple MAC addresses associated with a single port. This is common when the switch is connected to another switch. The switch will have a separate MAC address table entry for each frame received with a different source MAC address.

Click Play in the figure to view a demonstration of how two connected switches build MAC address tables.

Click here to download video slides from the demonstration.

Click here to read the transcript of this video.



Video Demonstration - Sending a Frame to the Default Gateway

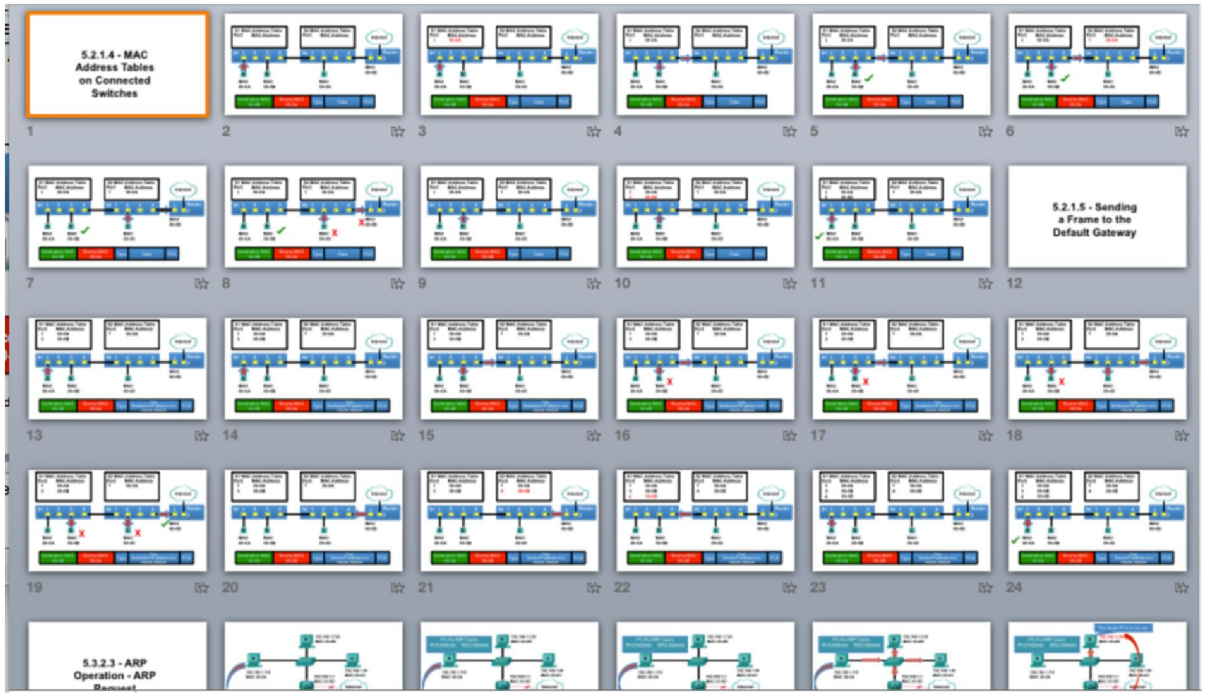
When a device has an IP address that is on a remote network, the Ethernet frame cannot be sent directly to the destination device. Instead, the Ethernet frame is sent to the MAC address of the default gateway, the router.

Click Play in the figure to view a demonstration of how PC-A communicates with its default gateway.

Note: In the video, the IP packet that is sent from PC-A to a destination on a remote network has a source IP address of PC-A and a destination IP address of the remote host. The returning IP packet will have the source IP address of remote host and the destination IP address will be that of PC-A.

Click here to download video slides from the demonstration.

For slides see my ‘Chapter 5 Ethernet Video Slides”

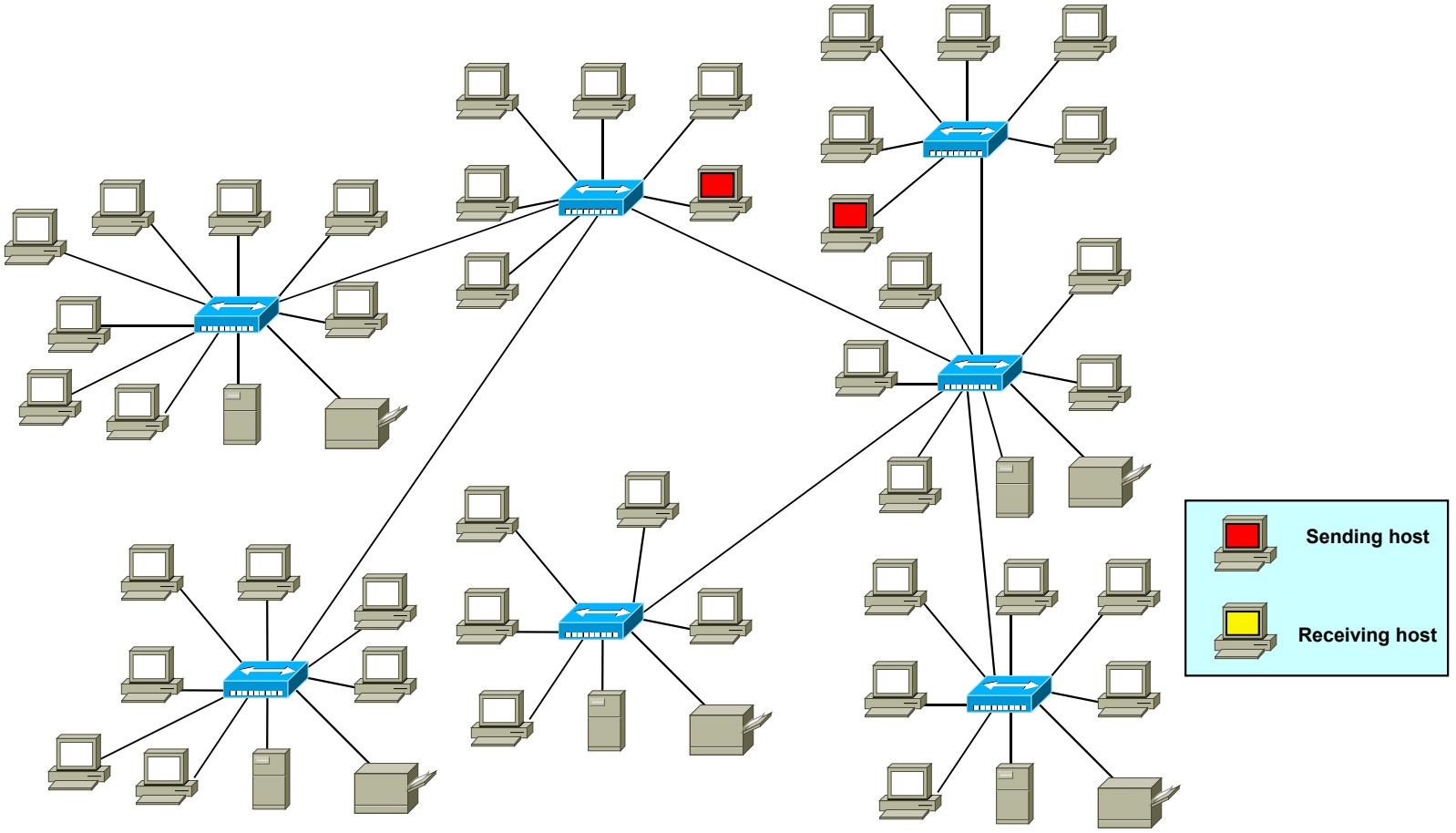


- **5.2.1.4 - MAC Address Tables on Connected Switches**
- **5.2.1.5 - Sending a Frame to the Default Gateway**

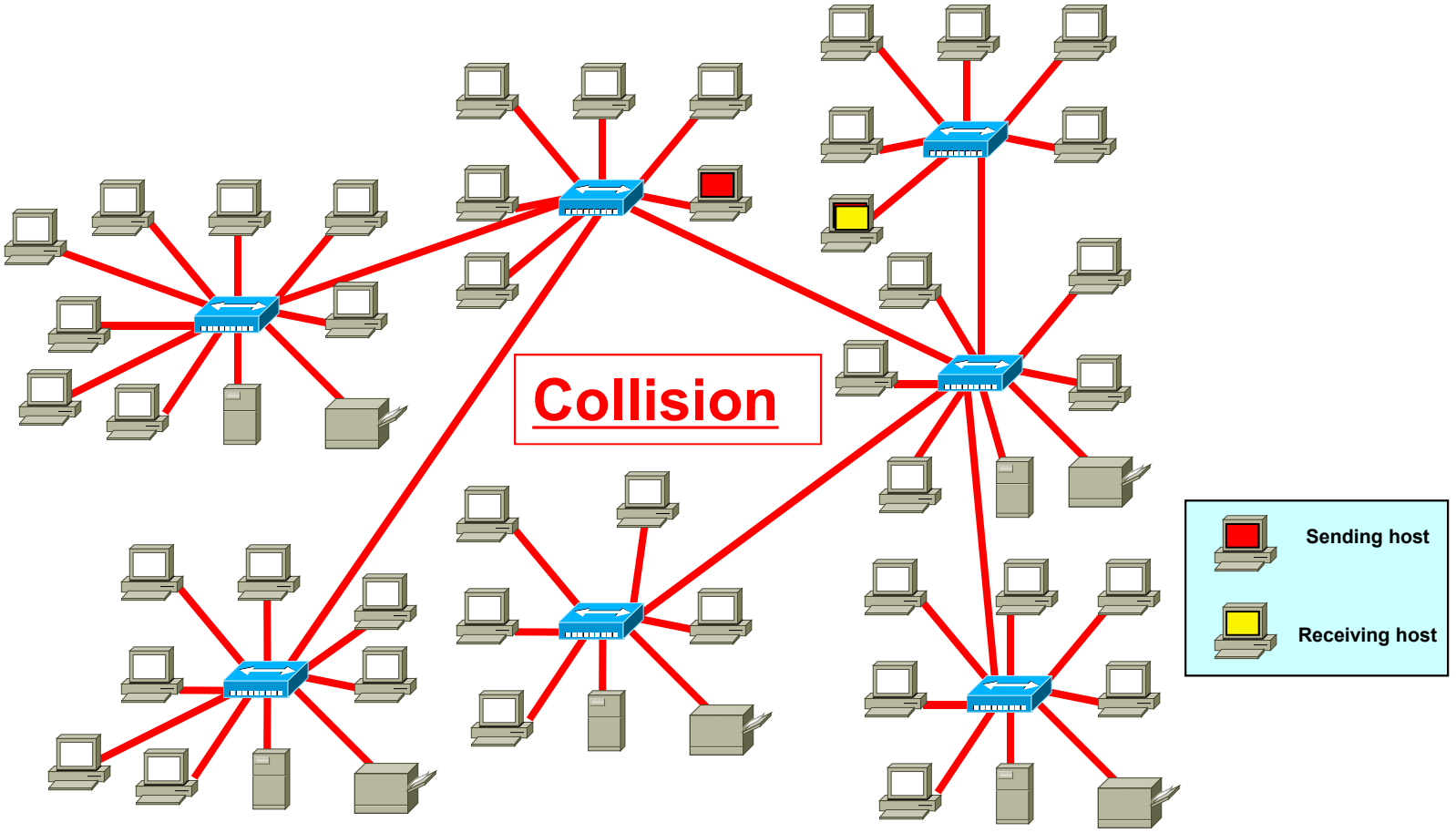
Ethernet Addresses Layer 1 Limitations

Layer 1 Limitations	Layer 2 Solutions
• Layer 1 cannot communicate with the upper-level layers.	• The (LLC) sublayer communicates with Layer 3.
• Layer 1 can only describe streams of bits.	• The MAC sublayer uses framing to control the placement of frames.
• Layer 1 cannot identify computers on a segment.	• The MAC sublayer uses MAC addresses to identify local hosts.
• Layer 1 is unable to decipher which computer will transmit binary data from a group of computers which are all trying to transmit at the same time.	• The MAC sublayer uses uses the CSMA/CD Media Access Control method.

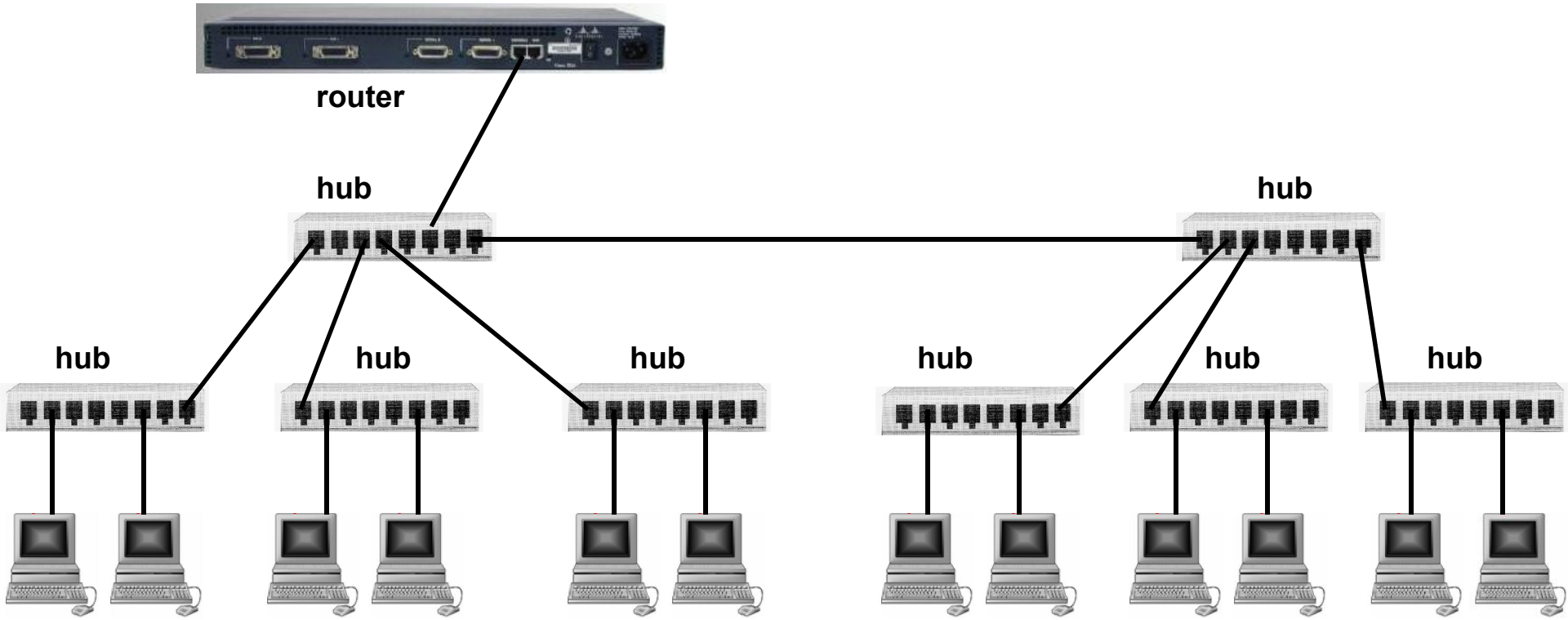
Hubs and Collision Domains



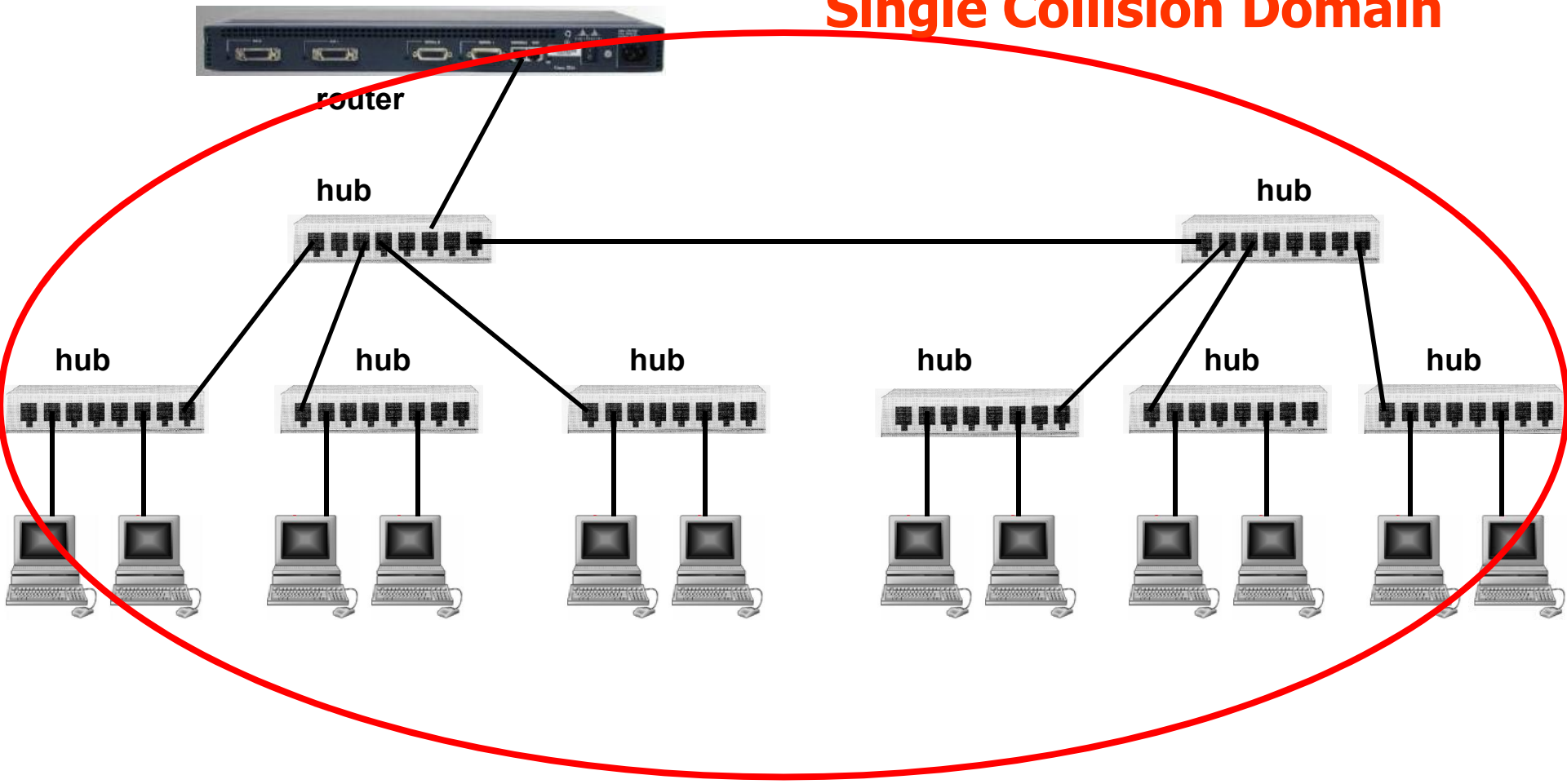
Hubs and Collision Domains



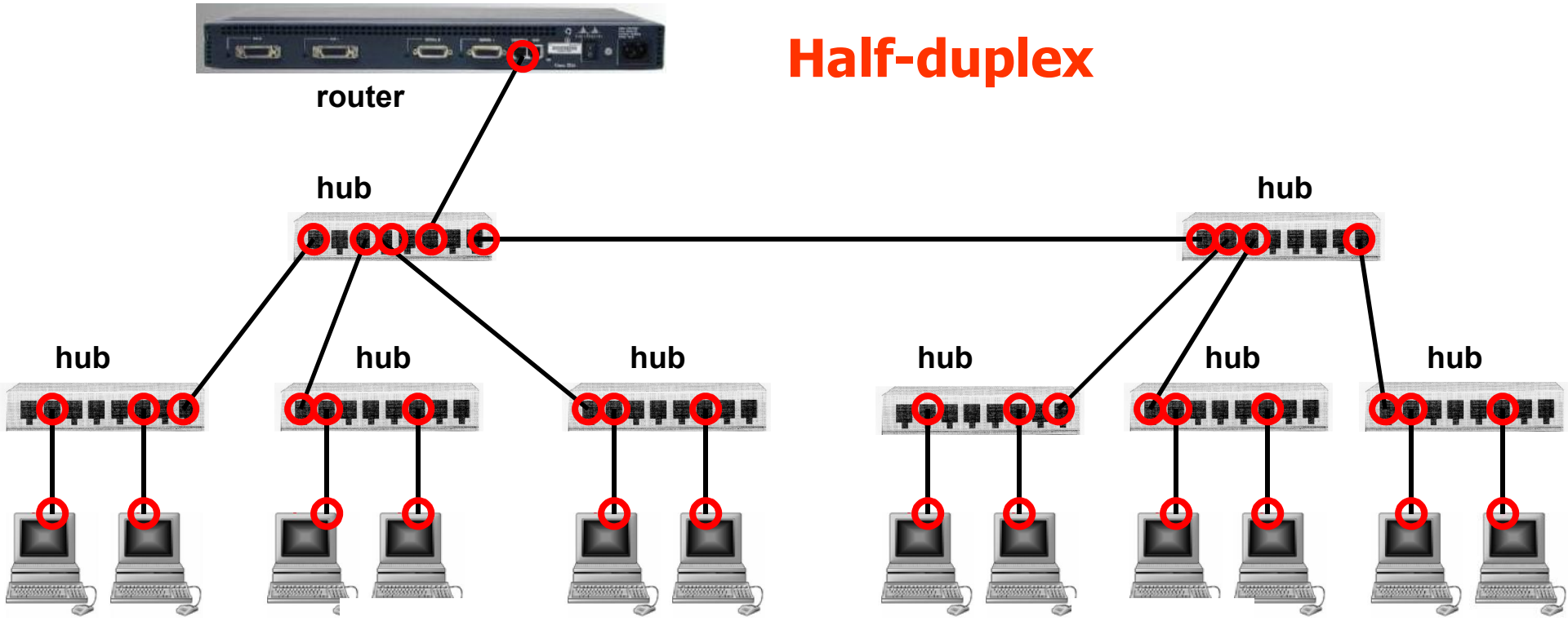
Where are the collision domains?
What would be the duplex settings?

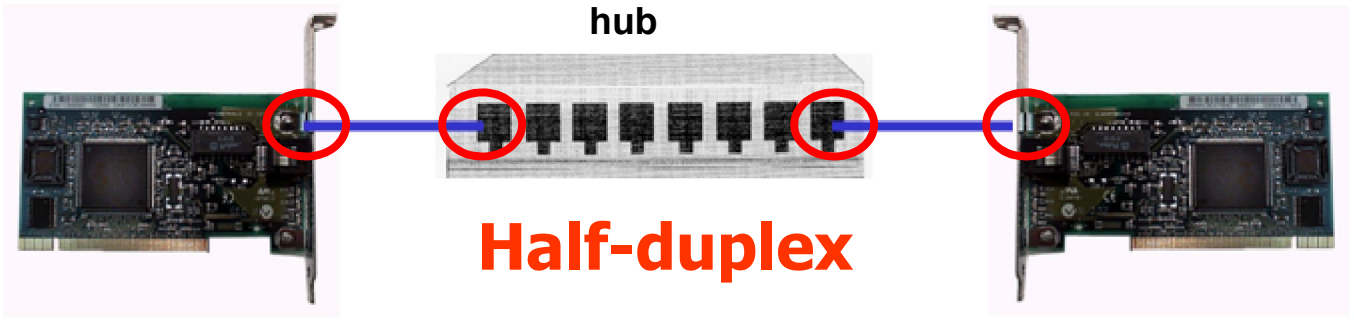


Where are the collision domains?

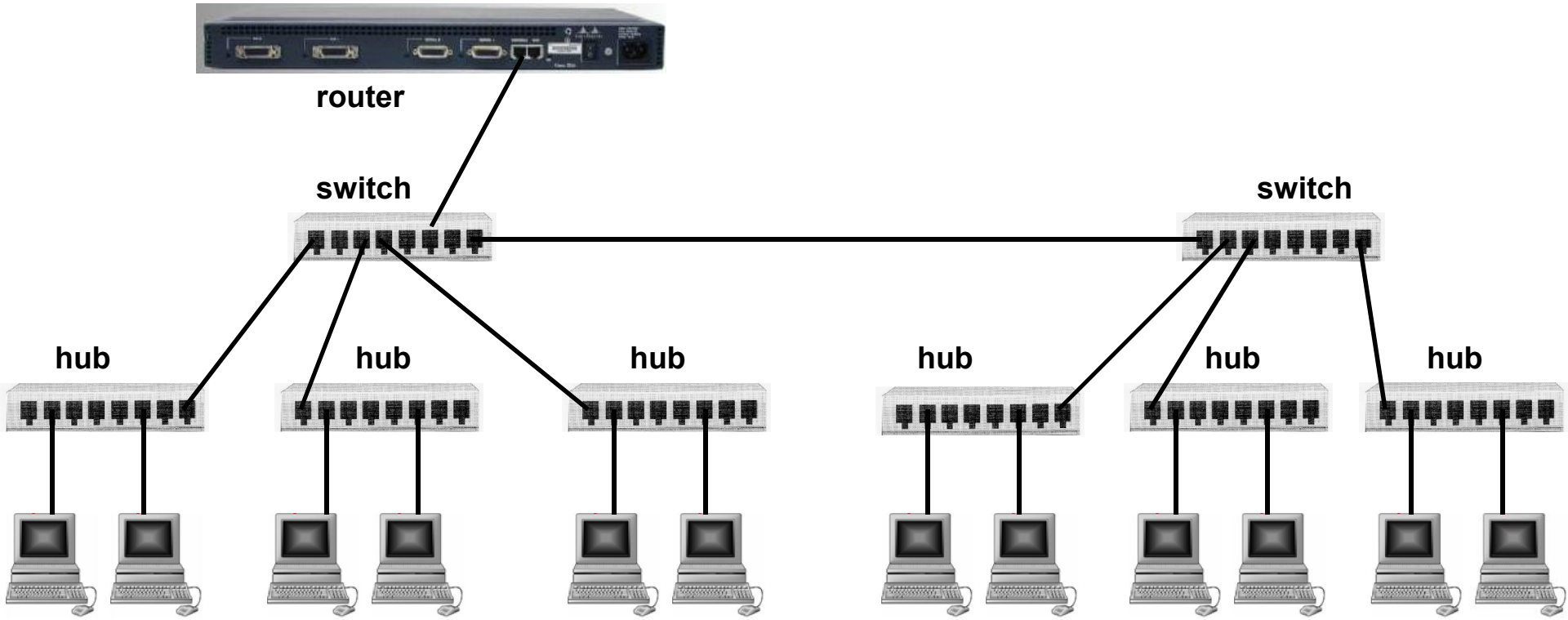


What would be the duplex settings?

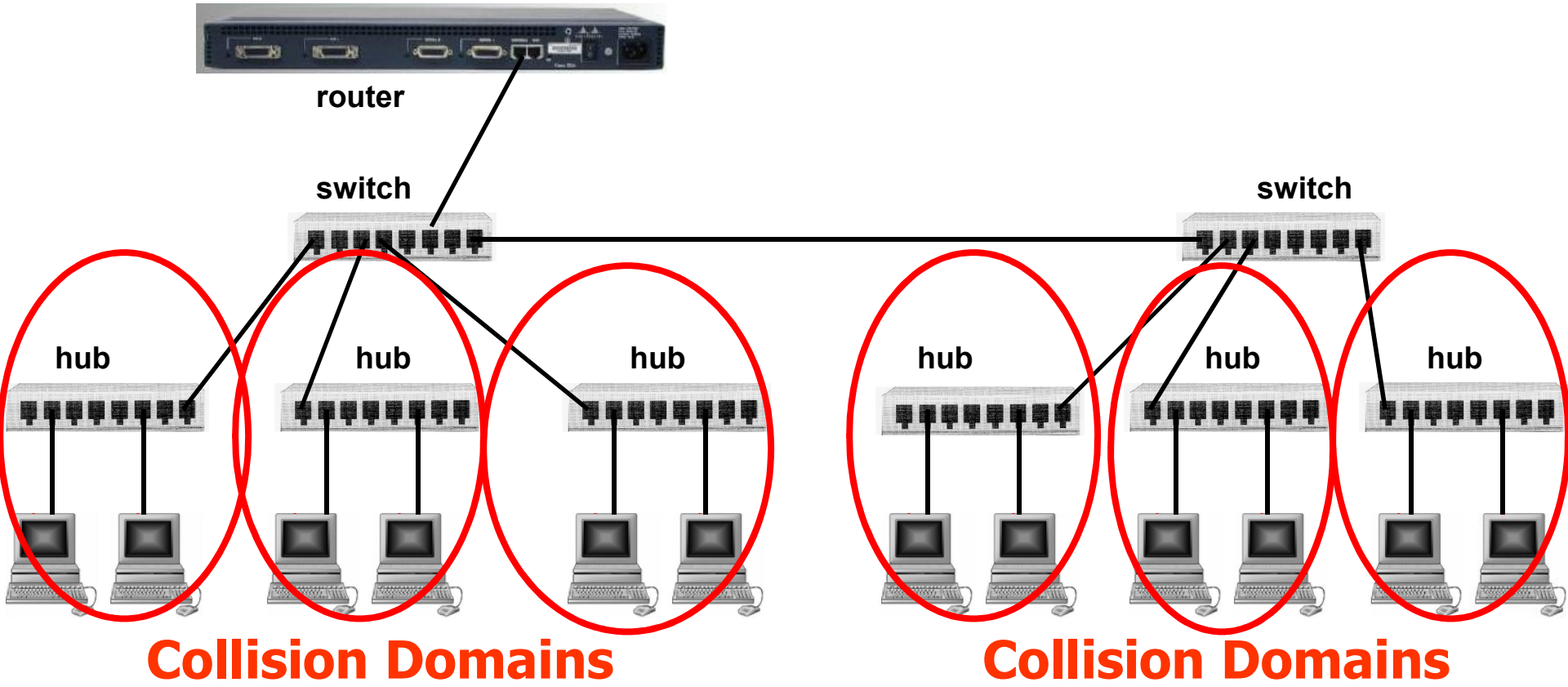




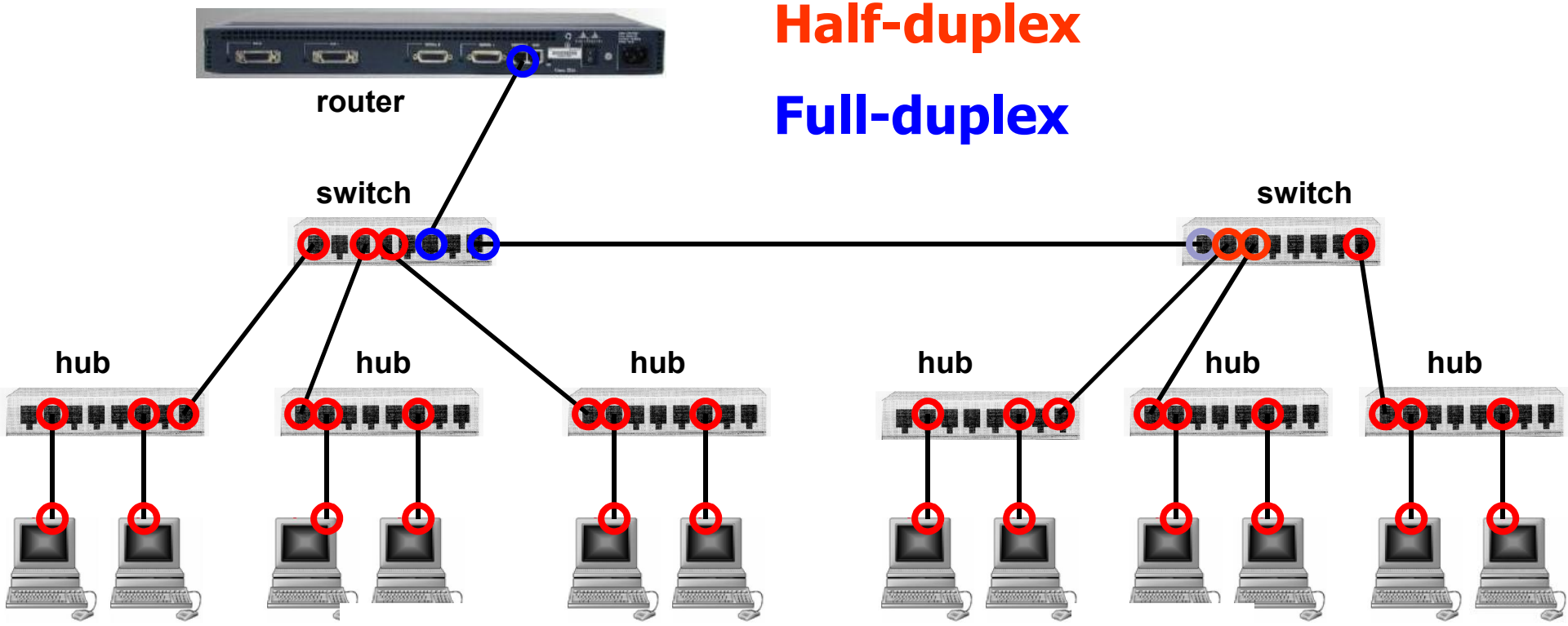
Where are the collision domains?
What would be the duplex settings?

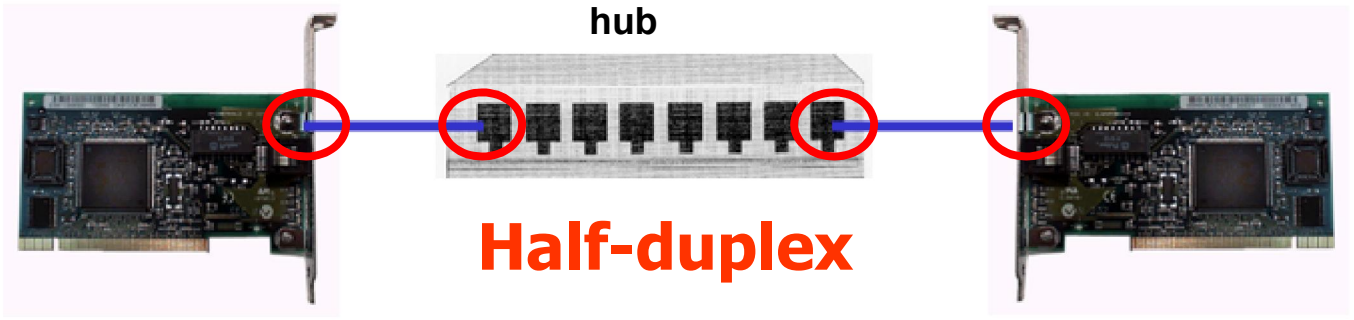


Where are the collision domains?
What would be the duplex settings?

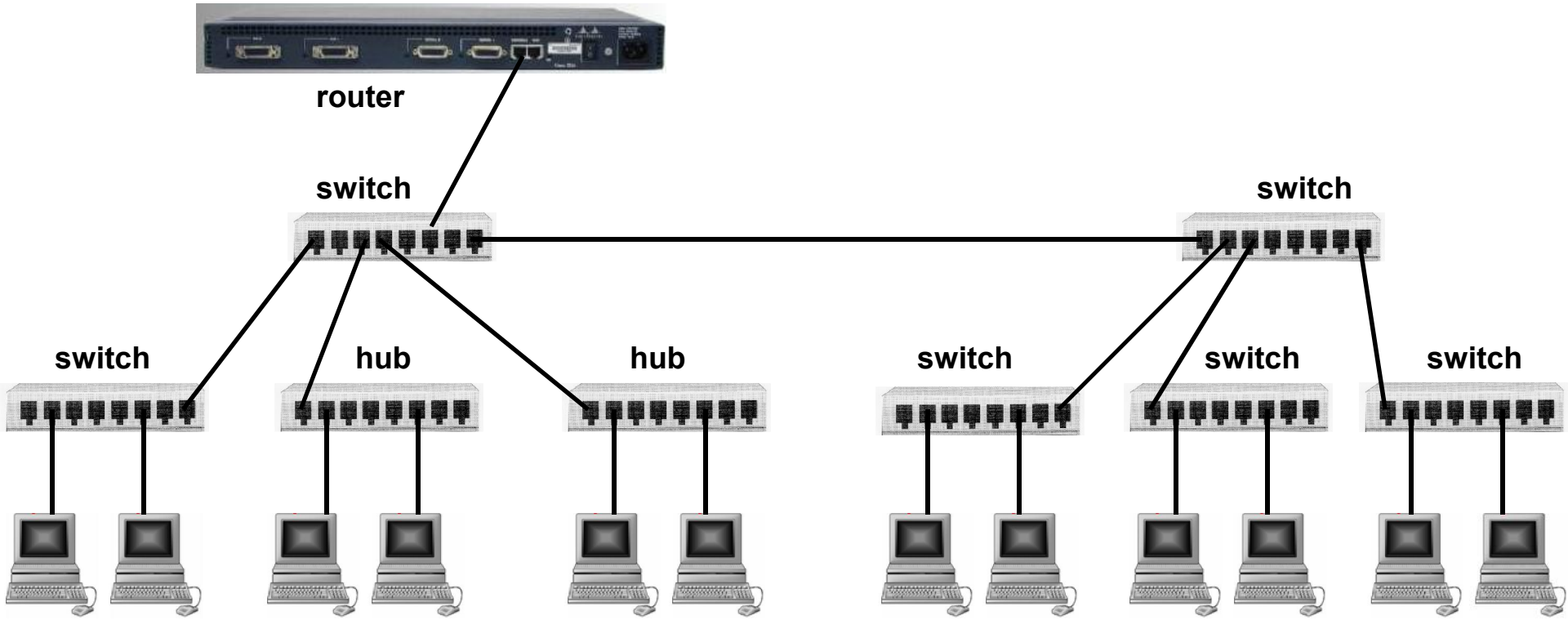


What would be the duplex settings?

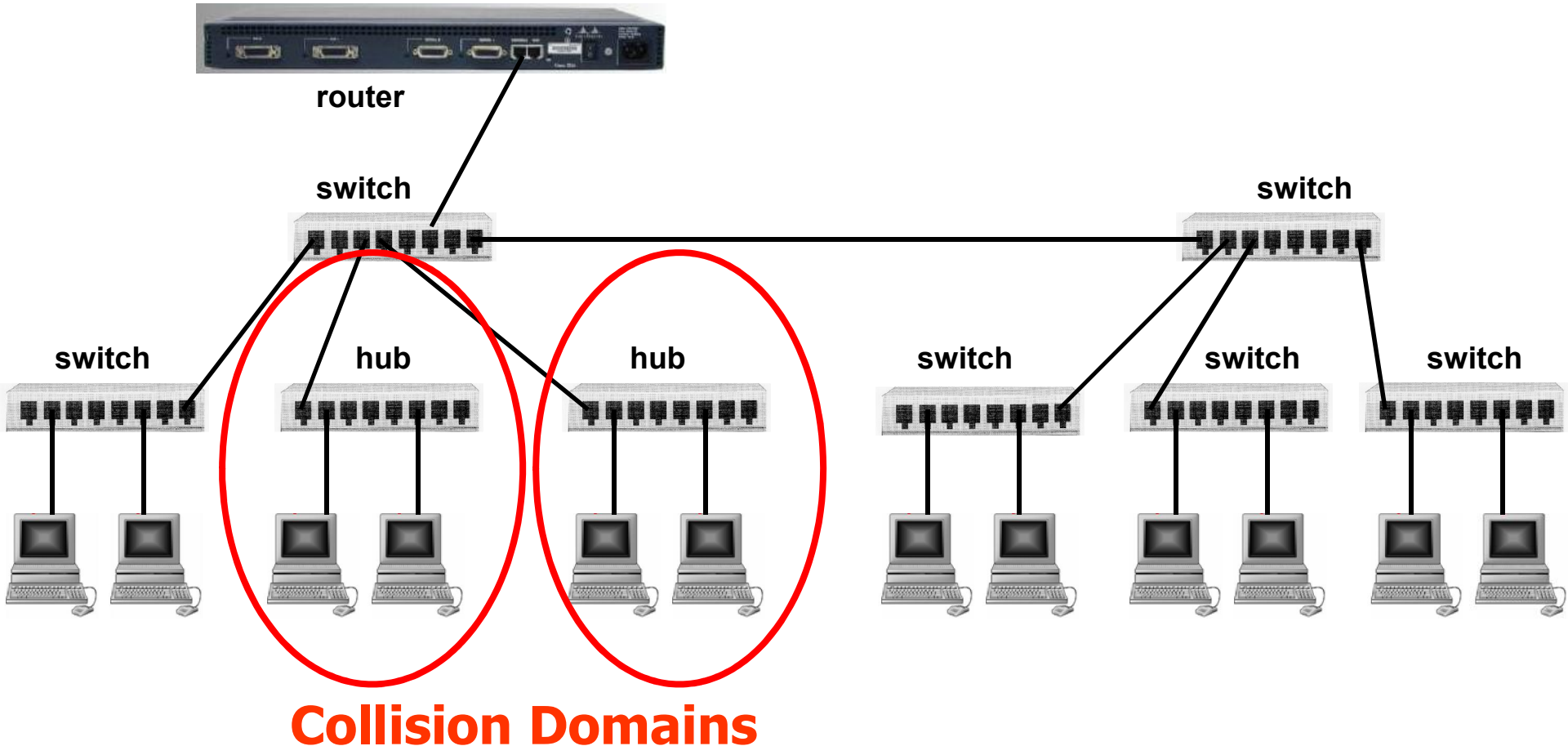




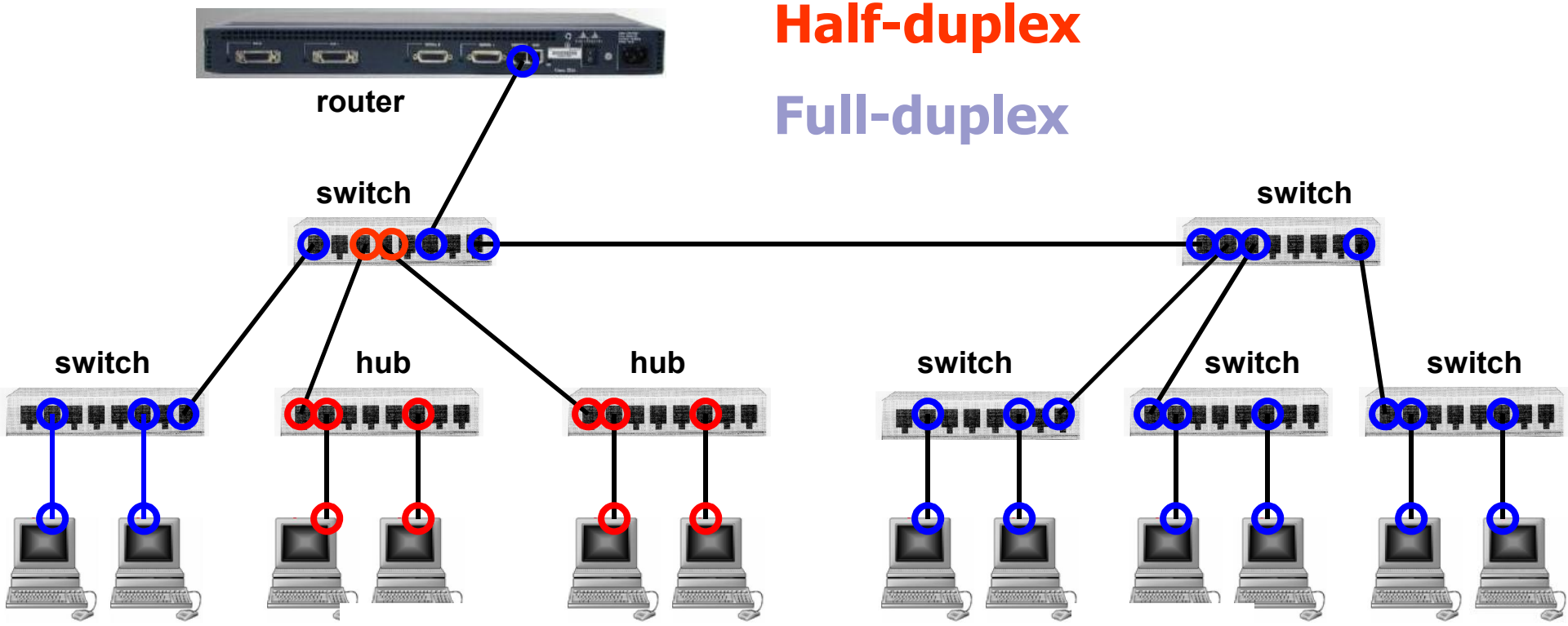
Where are the collision domains?
What would be the duplex settings?

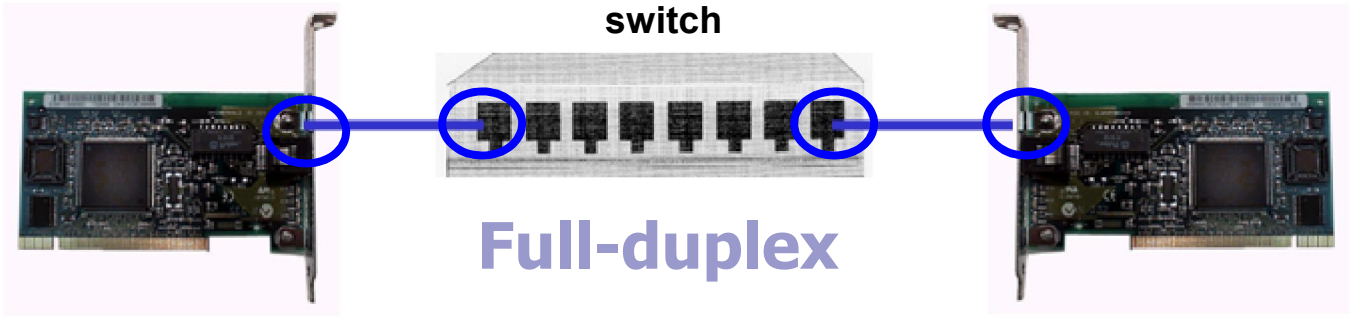


Where are the collision domains?

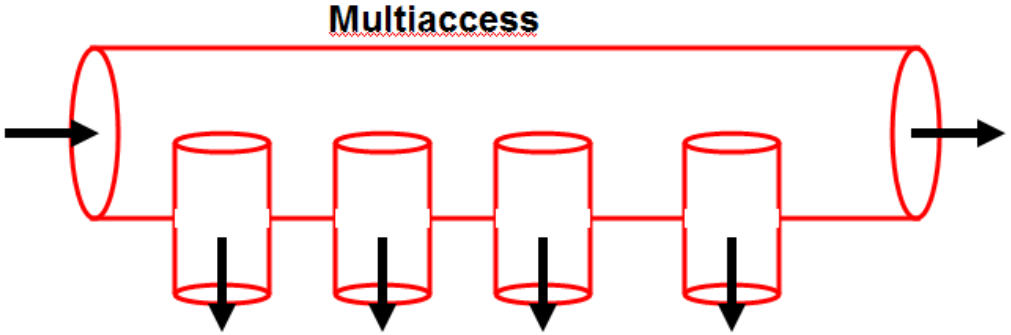


What would be the duplex settings?





All scenarios are multiaccess networks



router

switch

switch

switch

hub

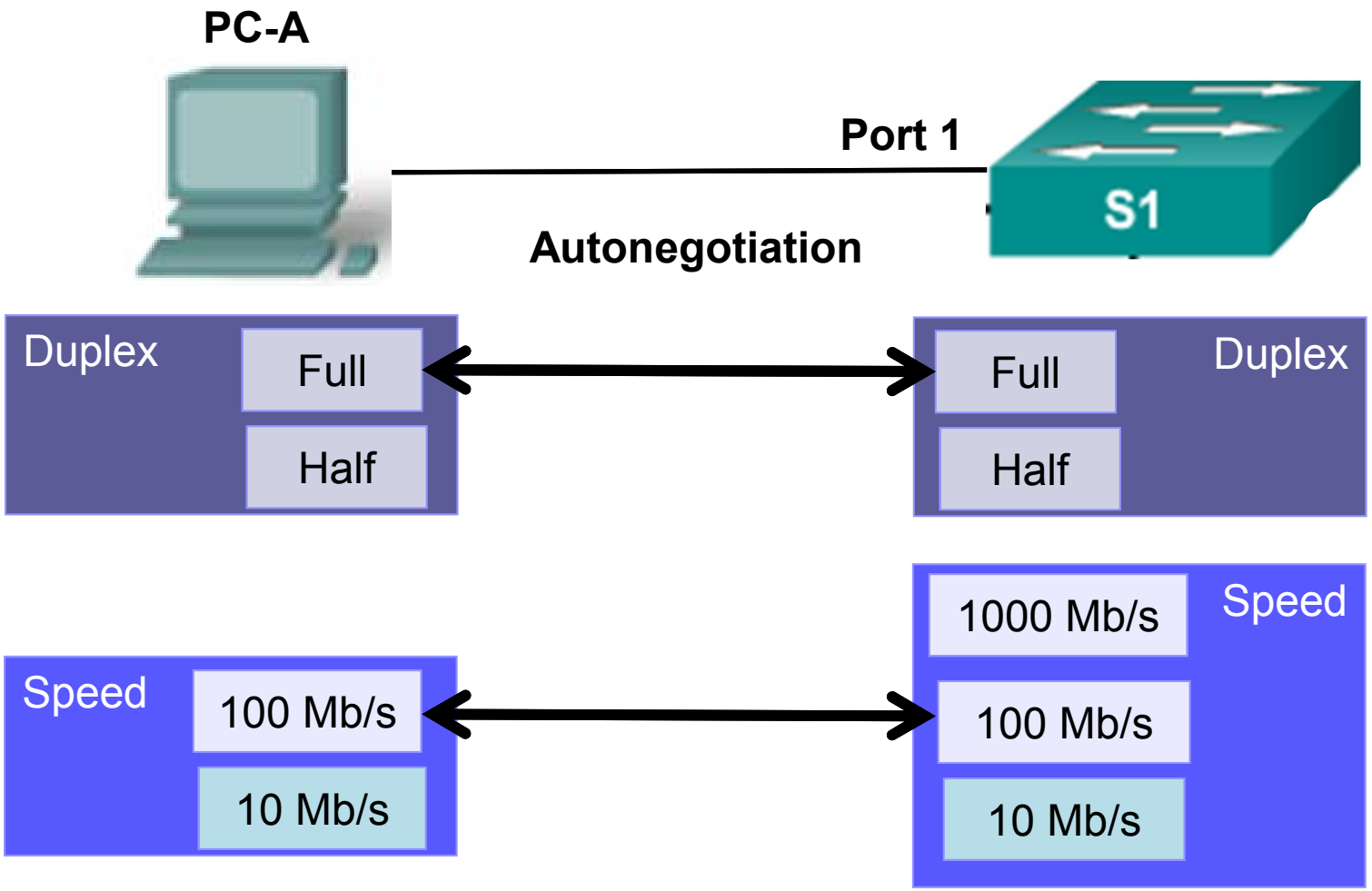
hub

switch

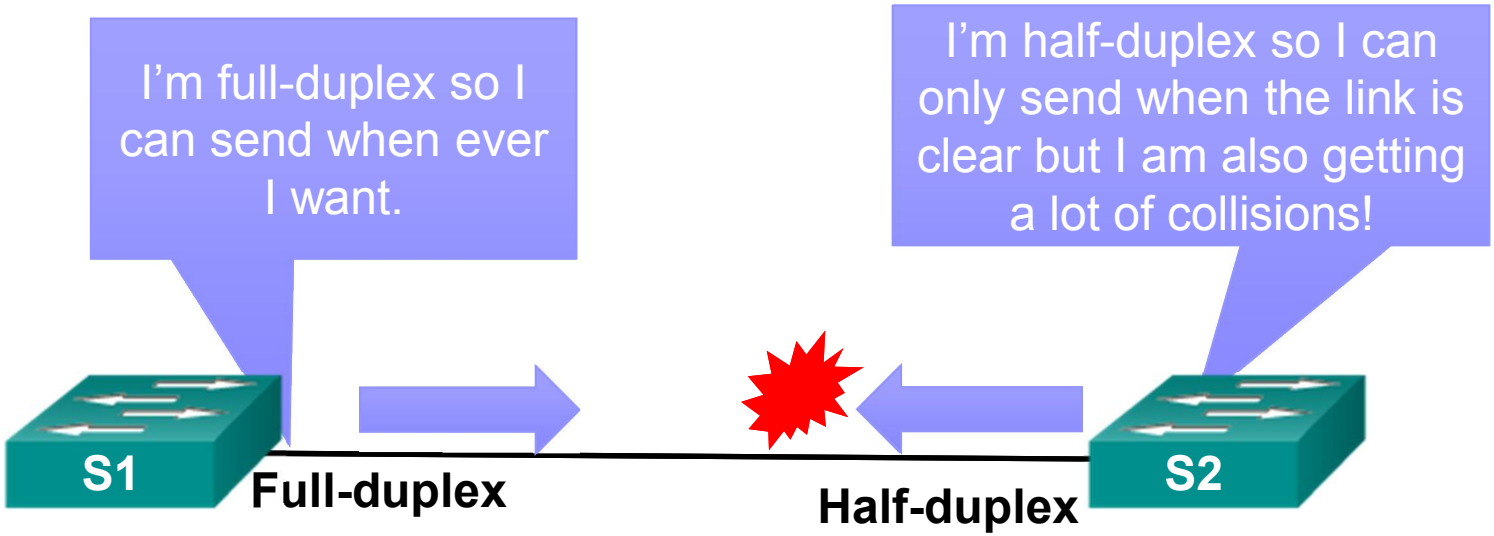
switch

switch

Duplex and Speed Seetings



Duplex Mismatch



S2 will continually experience collisions because S1 keeps sending frames any time it has something to send.

1

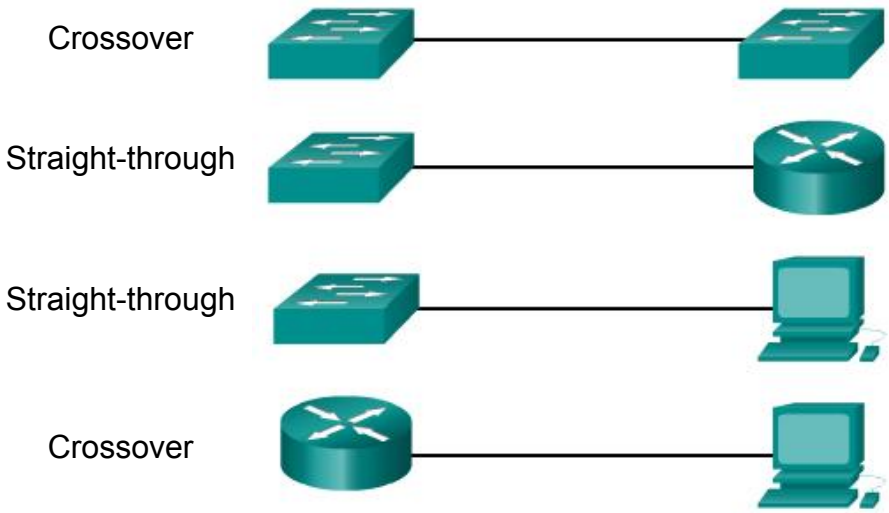
2

Full Duplex Operation

- A Cisco Catalyst switch supports three duplex settings:
  - The **full** option sets full-duplex mode.
  - The **half** option sets half-duplex mode.
  - The **auto** option sets autonegotiation of duplex mode which enables two ports to decide the best mode of operation.

- For Fast Ethernet and 10/100/1000 ports, the **default is auto**.
  - For 100BASE-FX ports, the default is full.
  - The 10/100/1000 ports operate in either half- or full-duplex mode when they are set to 10 or 100 Mb/s, but when set to 1,000 Mb/s, they operate only in full-duplex mode.

Auto-MDIX



- Connections between specific devices, such as switch-to-switch, switch-to-router, switch-to-host, and router-to-host device, once required the use of a specific cable types (crossover or straight-through).
- Modern Cisco switches support the **mdix auto** interface configuration command to enable the automatic medium-dependent interface crossover (auto-MDIX) feature.

Auto-MDIX

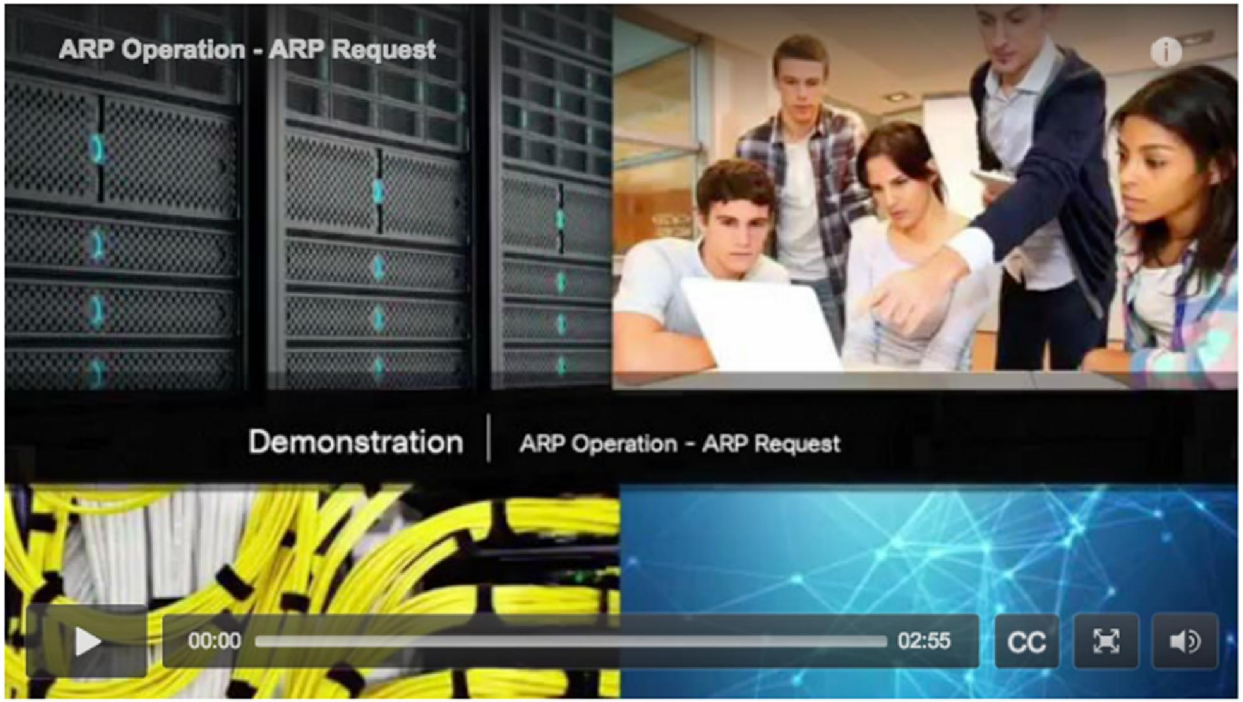
- What would happen if two new switches are interconnected with a straight-through cable?
  - The **auto-MDIX** feature is enabled by default, therefore a cable change is not needed.
    - Negotiate to work in full-duplex mode if capable.
    - Work at the fastest speed that is supported by both switches.

Address Resolution Protocol (ARP)

The primary purpose of ARP:

1. Resolving IPv4 addresses to MAC addresses
2. Maintaining a cache of mappings

- ARP is used to map known IP addresses to MAC addresses on the local network.
  - If the device is on a remote LAN segment, the host will send an ARP request for the MAC address of the default gateway.



Video Demonstration – ARP Request

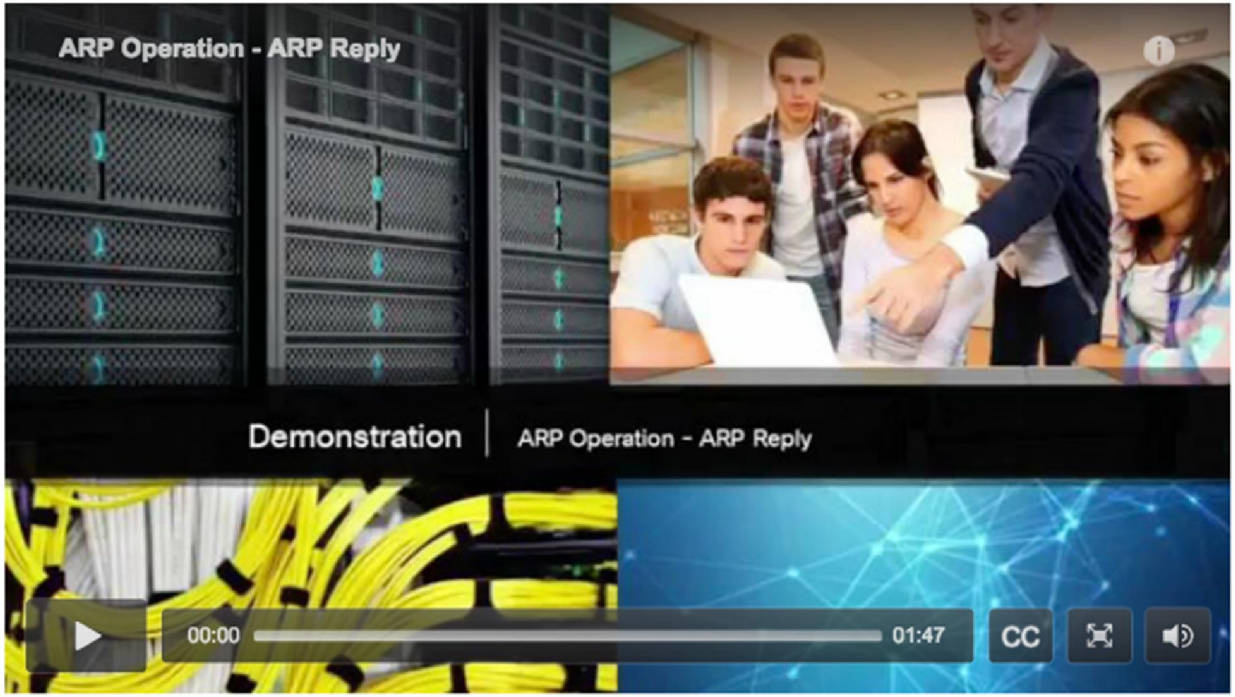
An ARP request is sent when a device needs a MAC address associated with an IPv4 address, and it does not have an entry for the IPv4 address in its ARP table.

ARP messages are encapsulated directly within an Ethernet frame. There is no IPv4 header. The ARP request message includes:

- Target IPv4 address – This is the IPv4 address that requires a corresponding MAC address.
- Target MAC address – This is the unknown MAC address and will be empty in the ARP request message.

The ARP request is encapsulated in an Ethernet frame using the following header information:

- Destination MAC address – This is a broadcast address requiring all Ethernet



Video Demonstration – ARP Reply

Only the device with an IPv4 address associated with the target IPv4 address in the ARP request will respond with an ARP reply. The ARP reply message includes:

- Sender's IPv4 address – This is the IPv4 address of the sender, the device whose MAC address was requested.
- Sender's MAC address – This is the MAC address of the sender, the MAC address needed by the sender of the ARP request.

The ARP reply is encapsulated in an Ethernet frame using the following header information:

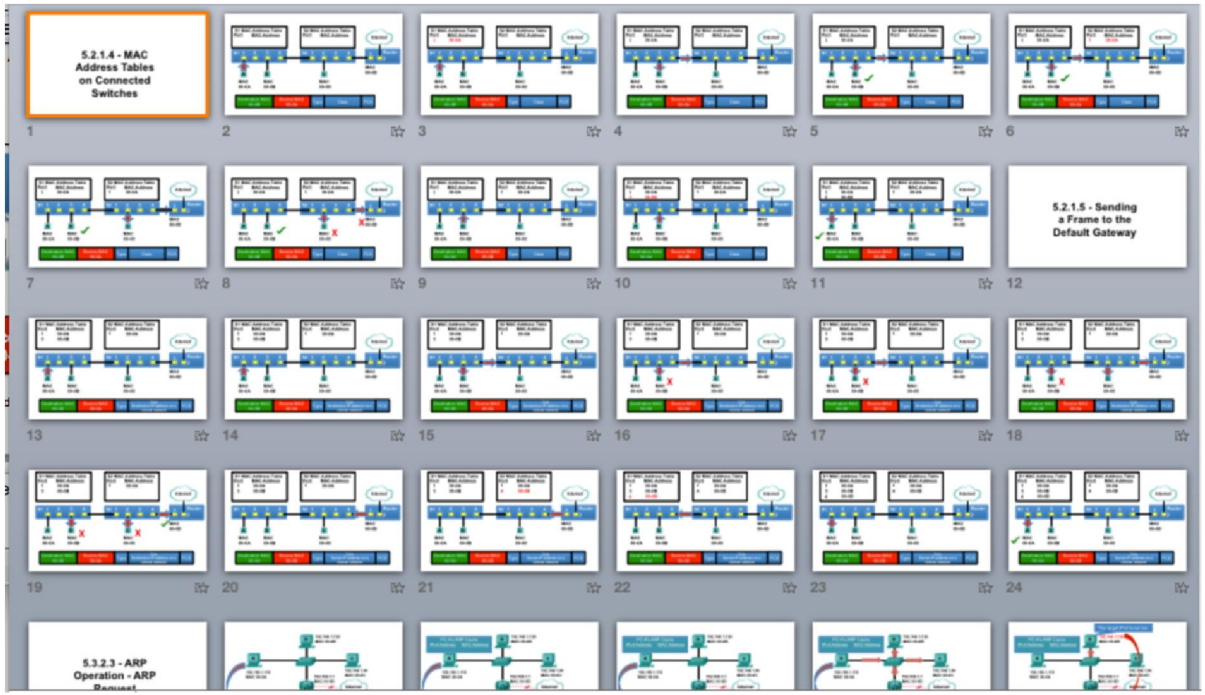
- Destination MAC address – This is the MAC address of the sender of the ARP request.
- Source MAC address – This is the sender of the ARP reply's MAC address.
- Type – ARP messages have a type field of

Video Demonstration – ARP Role in Remote Communication

When the destination IPv4 address is not on the same network as the source IPv4 address, the source device needs to send the frame to its default gateway. This is the interface of the local router. Whenever a source device has a packet with an IPv4 address on another network, it will encapsulate that packet in a frame using the destination MAC address of the router.

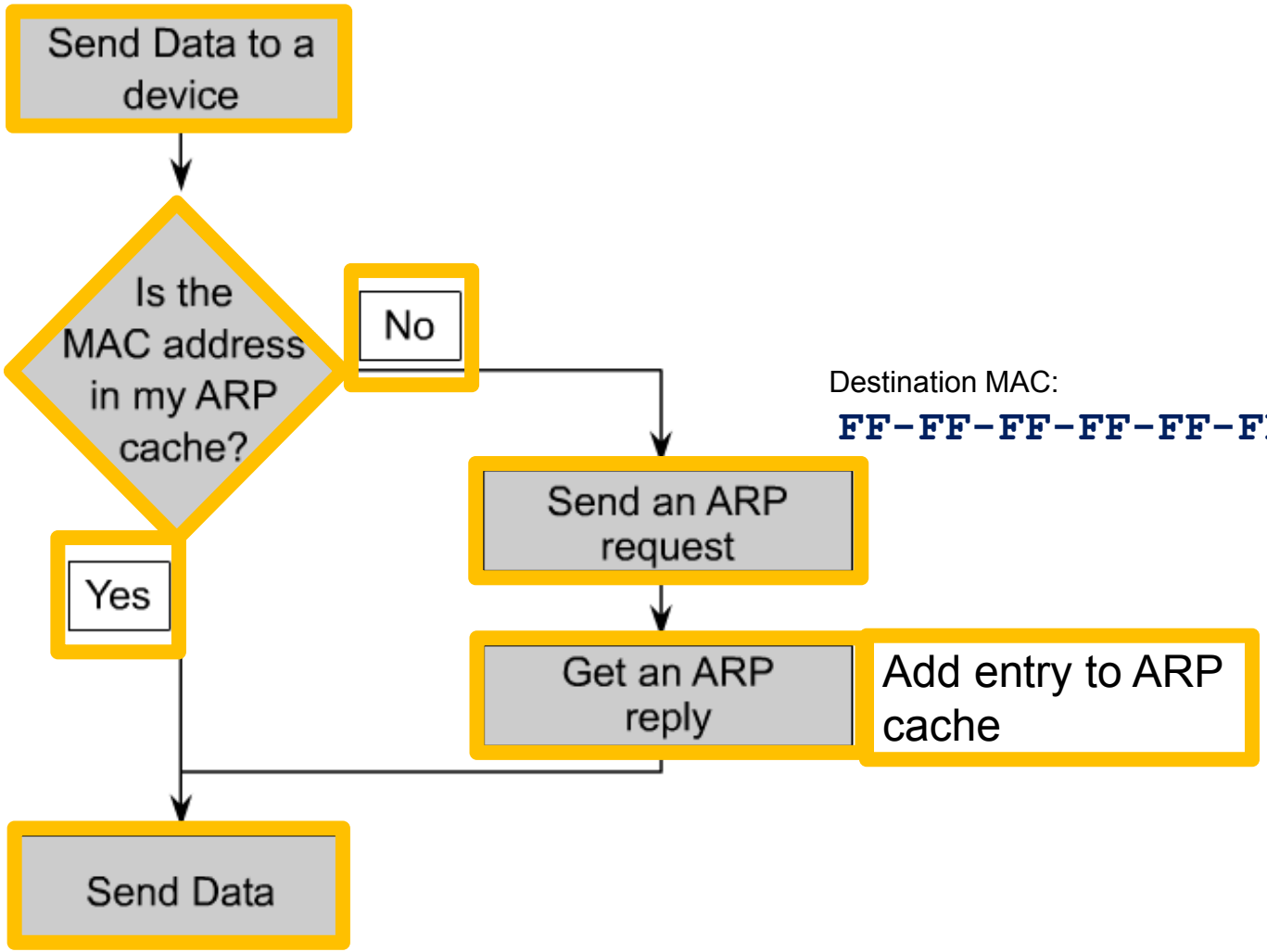
The IPv4 address of the default gateway address is stored in the IPv4 configuration of the hosts. When a host creates a packet for a destination, it compares the destination IPv4 address and its own IPv4 address to determine if the two IP addresses are located on the same Layer 3 network. If the destination host is not on its same network, the source checks its ARP table for an entry with the IPv4 address of the default gateway. If there is not an entry, it uses the ARP process to determine a MAC address

For slides see my ‘Chapter 5 Ethernet Video Slides”



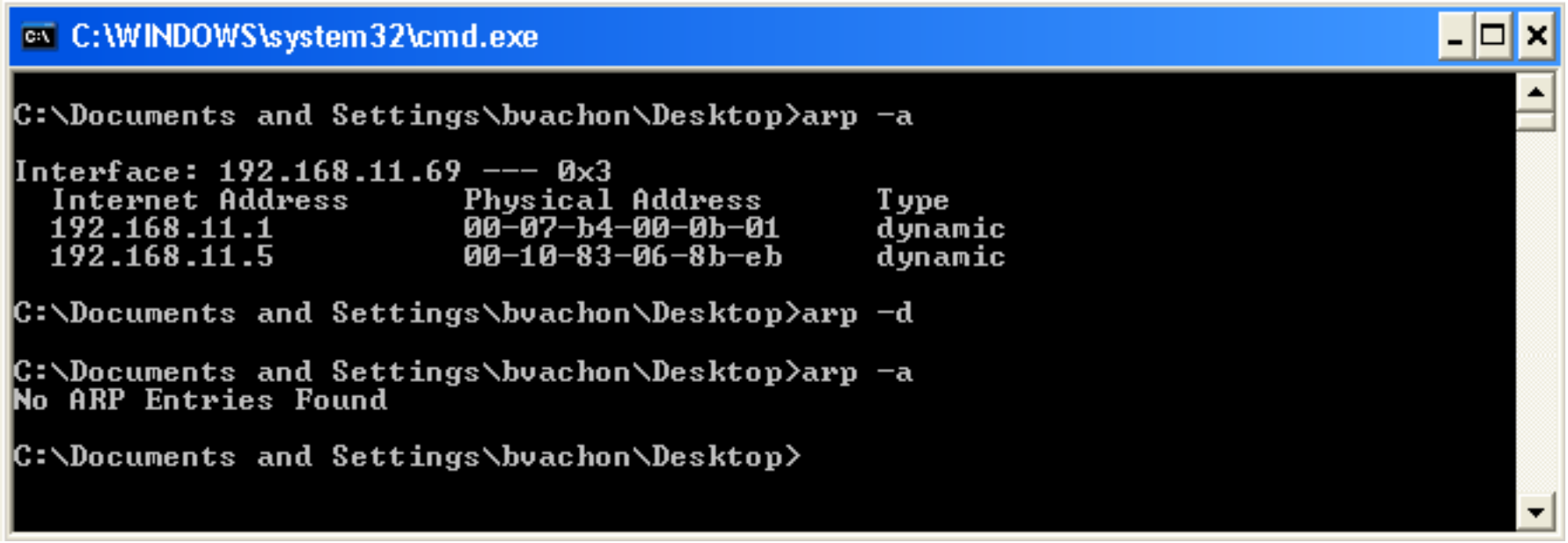
- **5.3.2.3 - ARP Operation - ARP Request**
- **5.3.2.4 - ARP Operation - ARP Reply**
- **5.3.2.5 - ARP Role in Remote Communication**

How Does ARP Work?



Viewing and Clearing the ARP Table

- To view the local ARP table in Windows DOS: **`arp -a`**



- On a Cisco router, use the **`show ip arp`**

The next 6 slides are of a Wireshark capture of a ping to 192.168.11.5 from 192.168.11.13.

Verify the ARP Cache and PING Target

```
C:\Users\Bob> arp -a

Interface: 192.168.11.13 --- 0xb
  Internet Address      Physical Address      Type
  192.168.11.1          00-07-b4-00-0b-01     dynamic
```

Start Wireshark

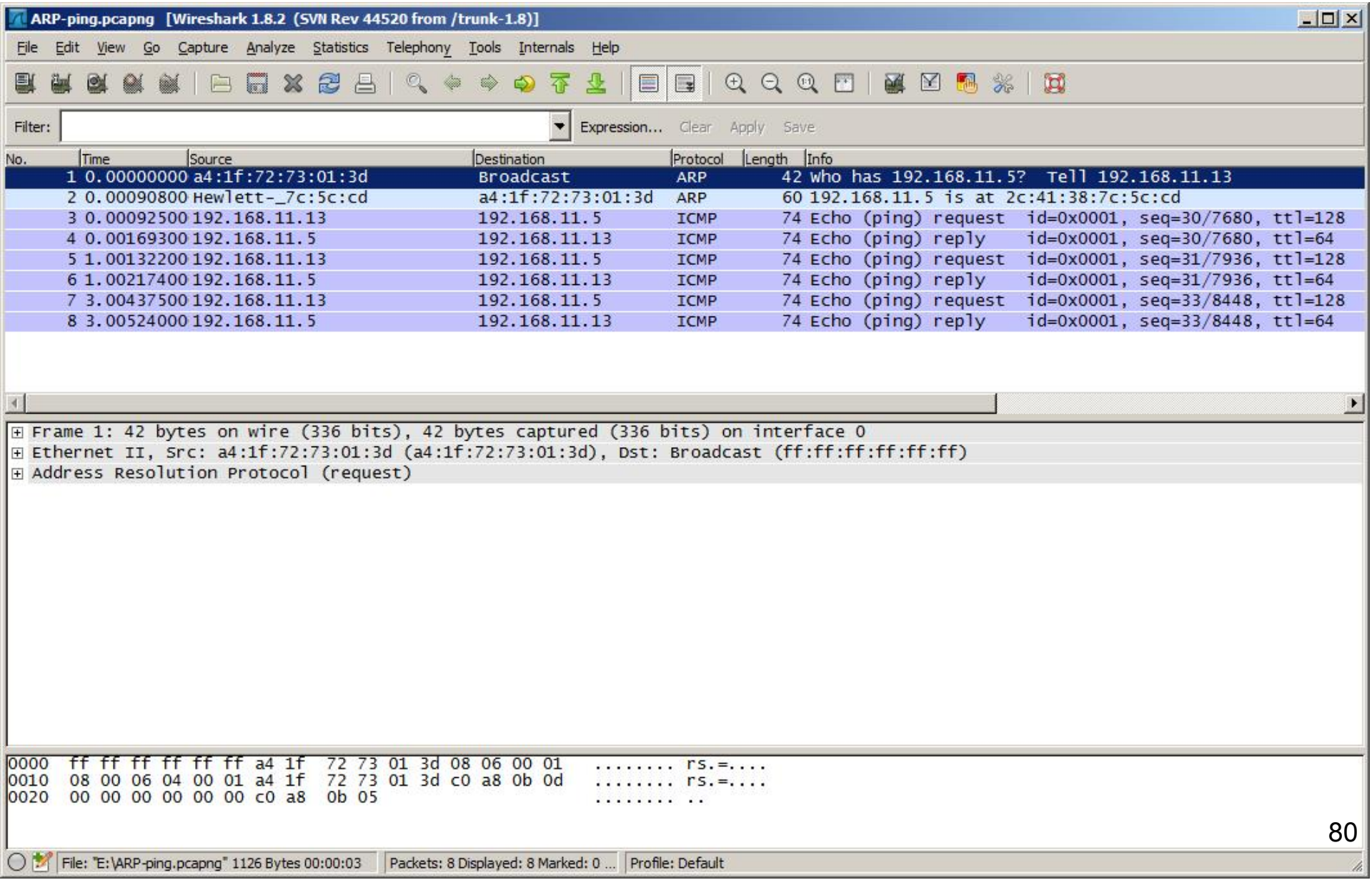
```
C:\Users\Bob>
C:\Users\Bob> ping 192.168.11.5

Pinging 192.168.11.5 with 32 bytes of data:
Reply from 192.168.11.5: bytes=32 time=1ms TTL=64
Reply from 192.168.11.5: bytes=32 time<1ms TTL=64
Reply from 192.168.11.5: bytes=32 time=1ms TTL=64
Reply from 192.168.11.5: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.11.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Stop Wireshark

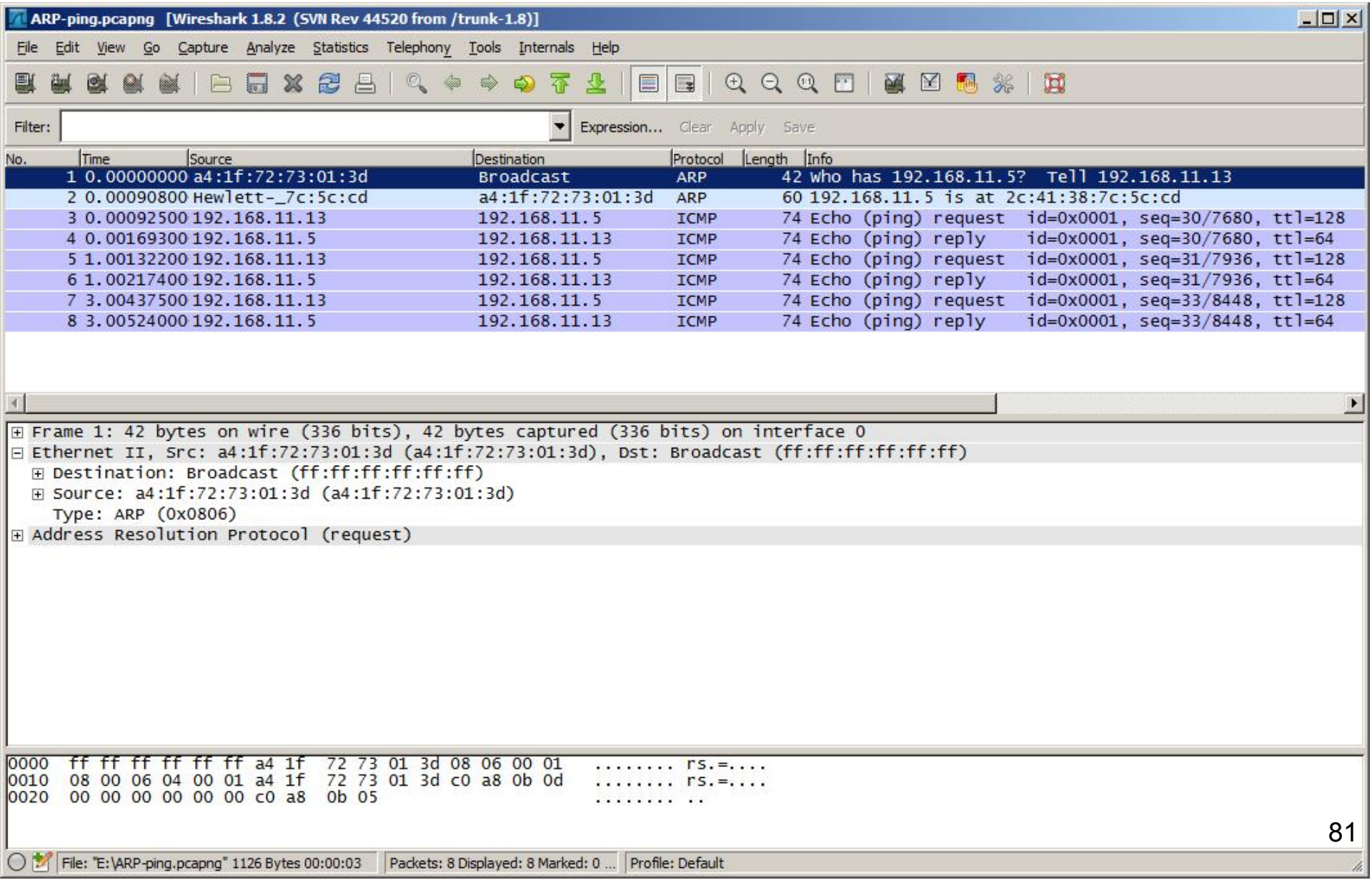
```
C:\Users\Bob>
```

Note: The Wireshark capture has been edited to display only packets of interest.

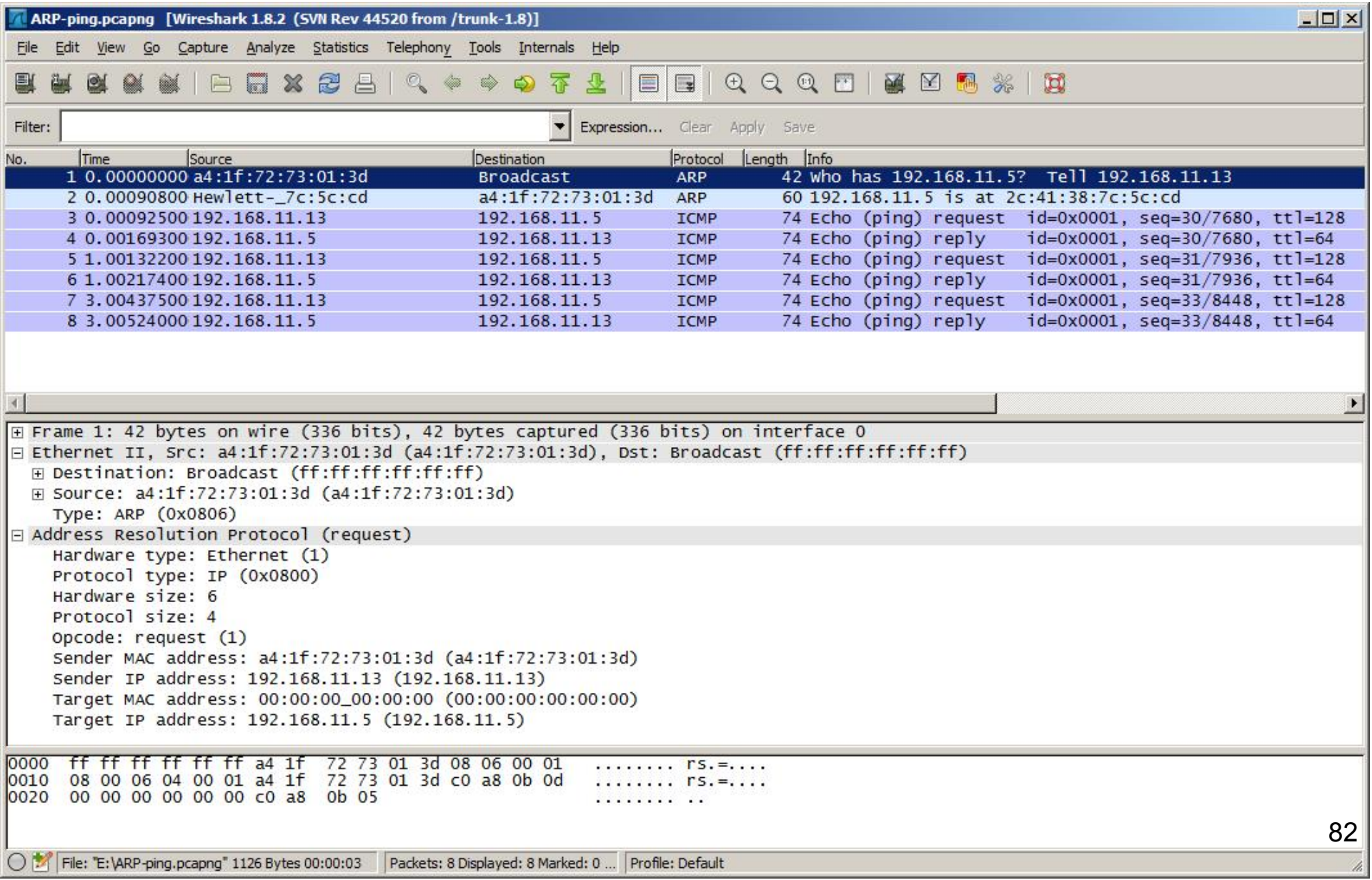
Wireshark ARP Capture



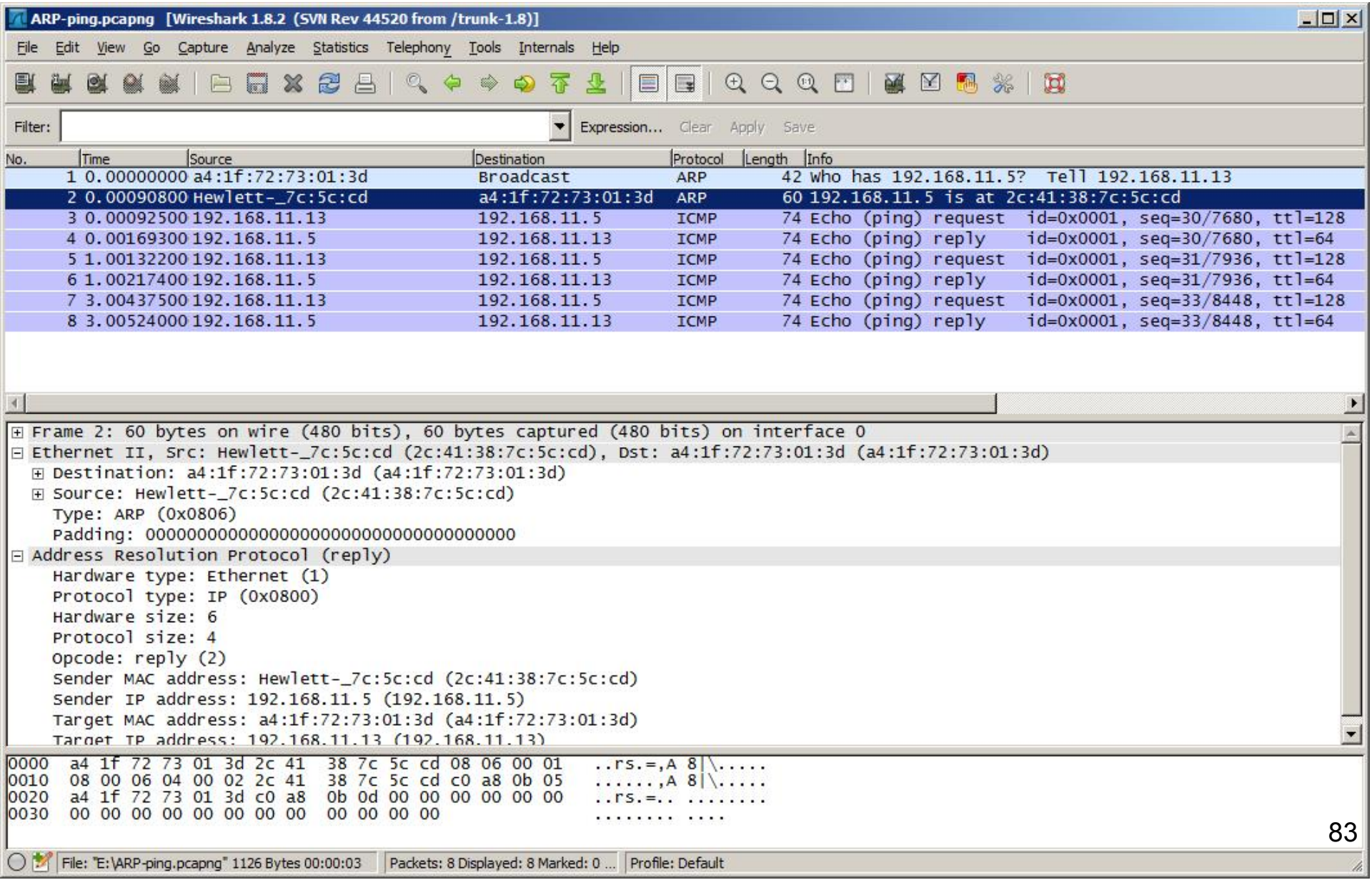
ARP Request Frame Information



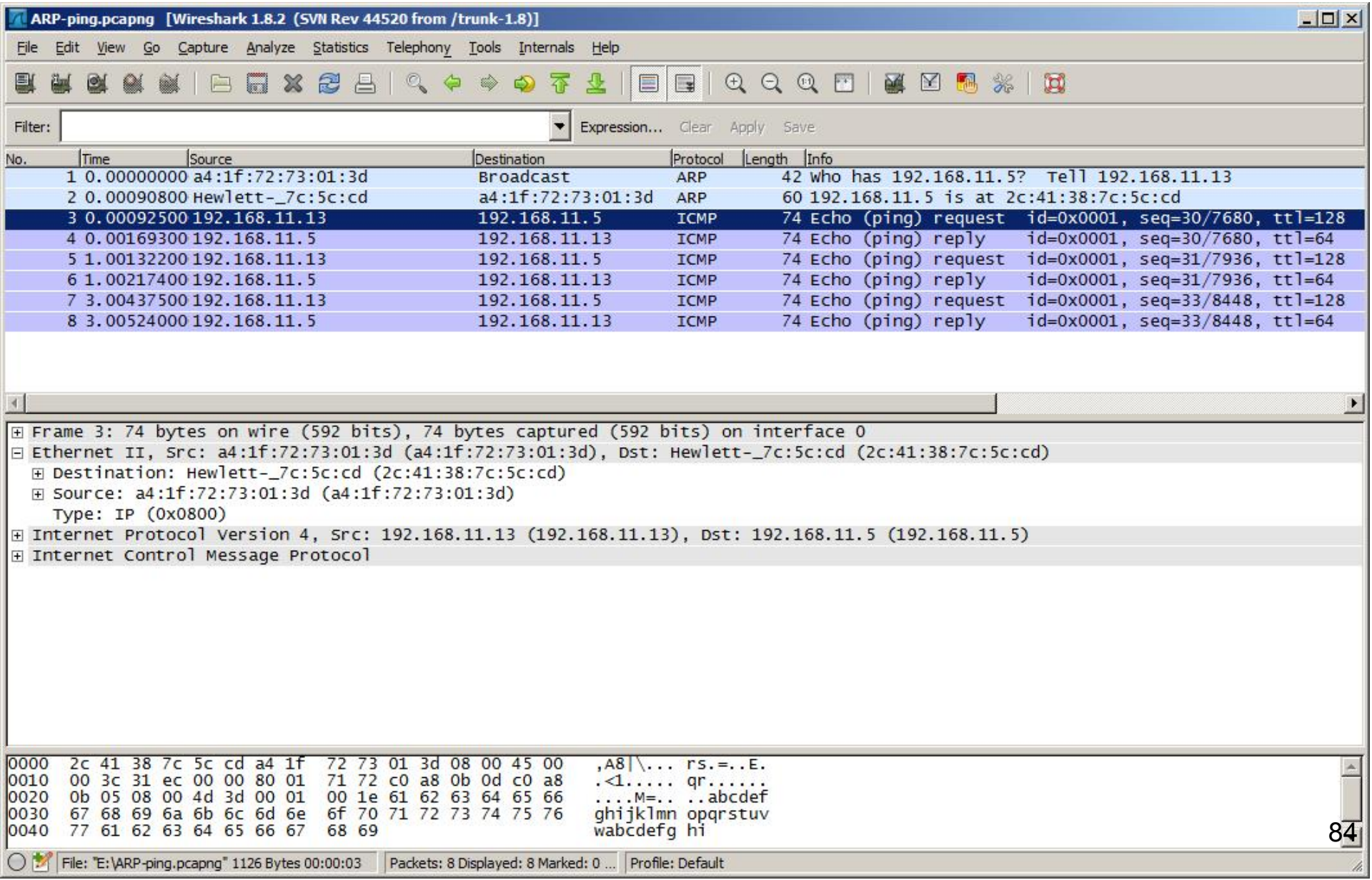
ARP Request Layer 3 Information



ARP Reply Information



PING Echo Request



PING Echo Reply

ARP-ping.pcapng [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	a4:1f:72:73:01:3d	Broadcast	ARP	42	Who has 192.168.11.5? Tell 192.168.11.13
2	0.00090800	Hewlett-_7c:5c:cd	a4:1f:72:73:01:3d	ARP	60	192.168.11.5 is at 2c:41:38:7c:5c:cd
3	0.00092500	192.168.11.13	192.168.11.5	ICMP	74	Echo (ping) request id=0x0001, seq=30/7680, ttl=128
4	0.00169300	192.168.11.5	192.168.11.13	ICMP	74	Echo (ping) reply id=0x0001, seq=30/7680, ttl=64
5	1.00132200	192.168.11.13	192.168.11.5	ICMP	74	Echo (ping) request id=0x0001, seq=31/7936, ttl=128
6	1.00217400	192.168.11.5	192.168.11.13	ICMP	74	Echo (ping) reply id=0x0001, seq=31/7936, ttl=64
7	3.00437500	192.168.11.13	192.168.11.5	ICMP	74	Echo (ping) request id=0x0001, seq=33/8448, ttl=128
8	3.00524000	192.168.11.5	192.168.11.13	ICMP	74	Echo (ping) reply id=0x0001, seq=33/8448, ttl=64

```
⊞ Frame 4: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
⊟ Ethernet II, Src: Hewlett-_7c:5c:cd (2c:41:38:7c:5c:cd), Dst: a4:1f:72:73:01:3d (a4:1f:72:73:01:3d)
  ⊞ Destination: a4:1f:72:73:01:3d (a4:1f:72:73:01:3d)
  ⊞ Source: Hewlett-_7c:5c:cd (2c:41:38:7c:5c:cd)
    Type: IP (0x0800)
⊞ Internet Protocol Version 4, Src: 192.168.11.5 (192.168.11.5), Dst: 192.168.11.13 (192.168.11.13)
⊞ Internet Control Message Protocol
```

```
0000  a4 1f 72 73 01 3d 2c 41  38 7c 5c cd 08 00 45 00   ..rs.=,A 8|\...E.
0010  00 3c b7 bf 00 00 40 01  2b 9f c0 a8 0b 05 c0 a8   .<....@. +.......
0020  0b 0d 00 00 55 3d 00 01  00 1e 61 62 63 64 65 66   ....U=.. ..abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                    wabcdefg hi
```

File: "E:\ARP-ping.pcapng" 1126 Bytes 00:00:03 | Packets: 8 Displayed: 8 Marked: 0 ... | Profile: Default

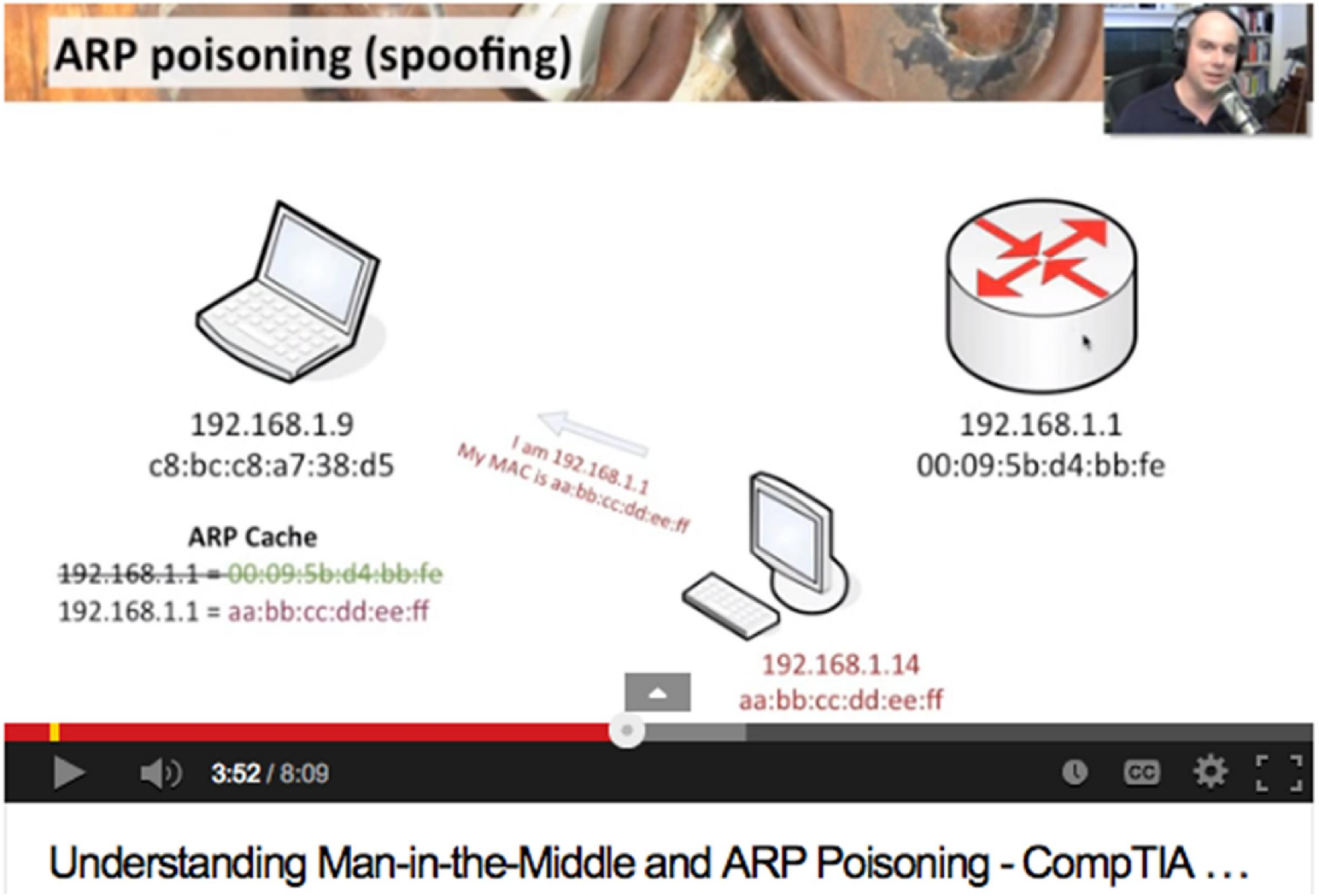
ARP-Ping.pcap

Verify the ARP Cache

```
C:\Users\Bob> arp -a

Interface: 192.168.11.13 --- 0xb
  Internet Address      Physical Address      Type
  192.168.11.1          00-07-b4-00-0b-01     dynamic
  192.168.11.5          2c-41-38-7c-5c-cd     dynamic

C:\Users\Bob>
```

ARP Issues

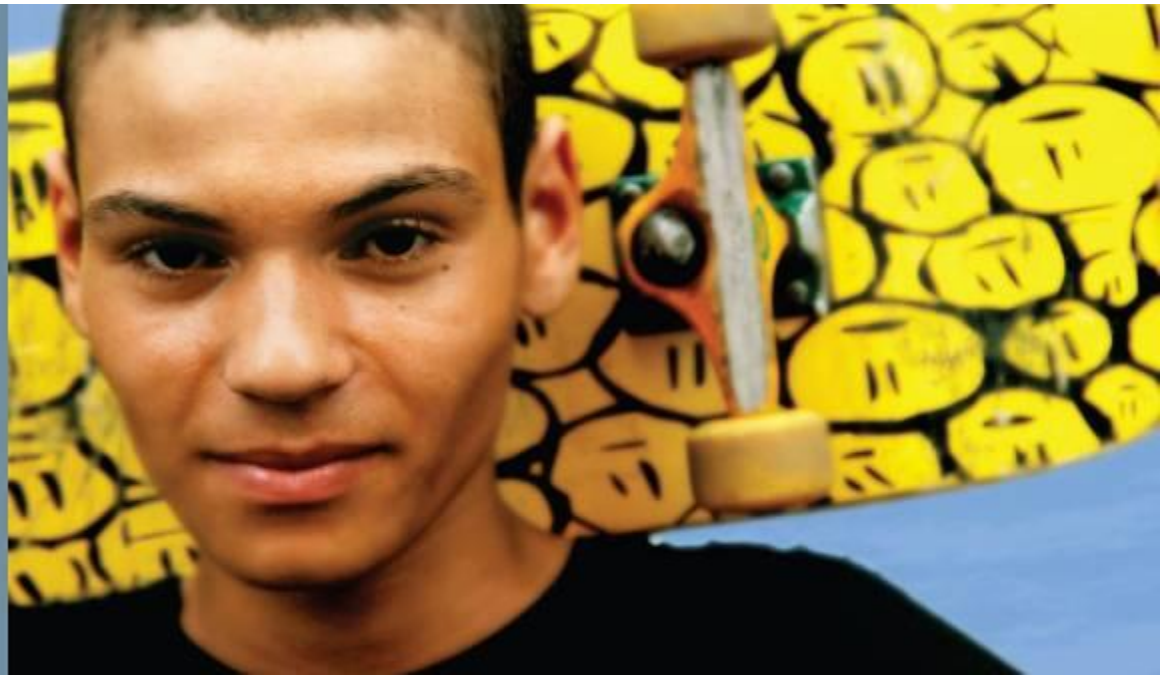
How ARP Can Create Problems



https://www.youtube.com/watch?v=2MBnX9-KIVU

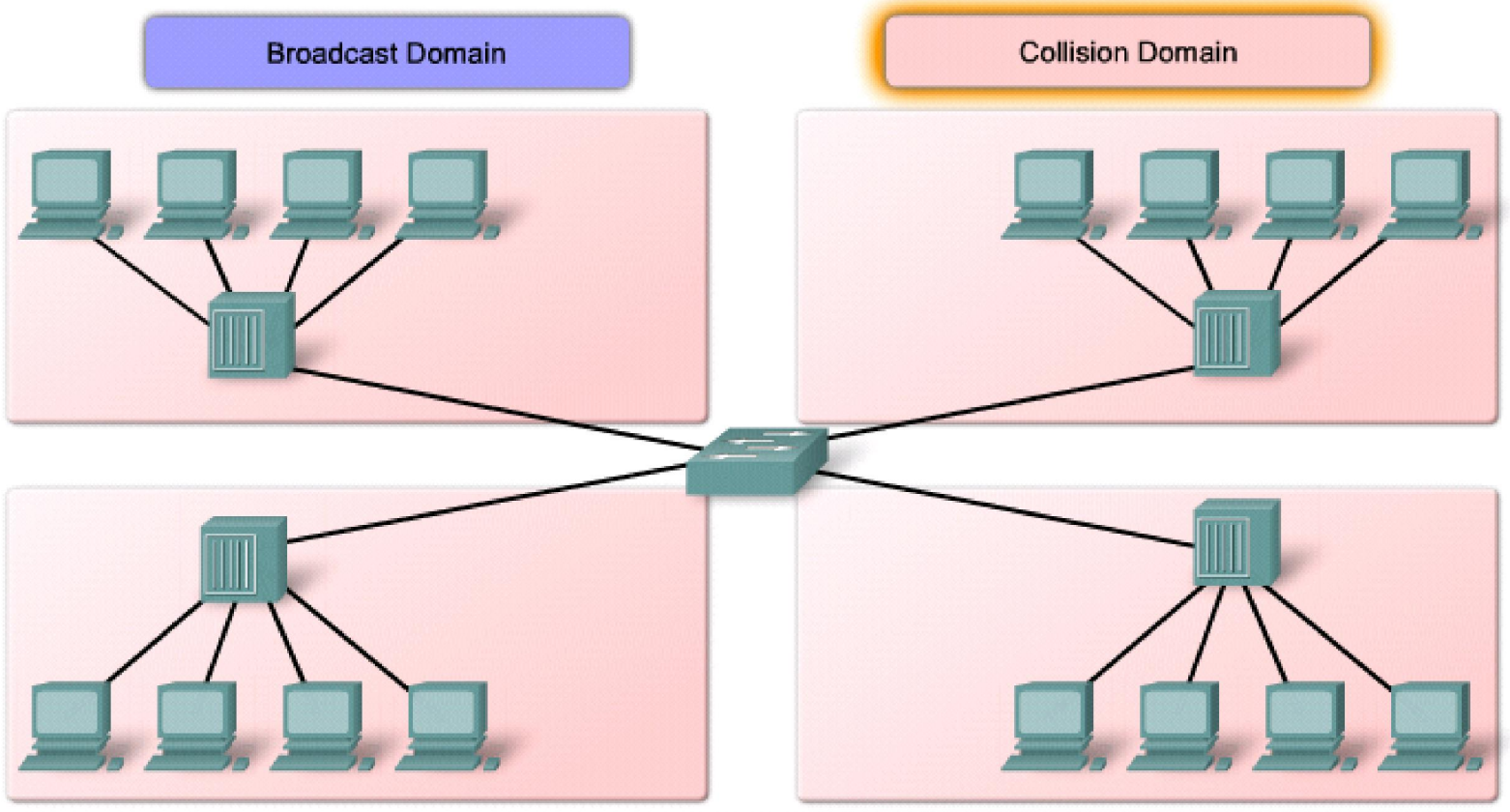
How a Switch Forwards Frames

(CAM Table)



Switches

- Switches separate collision domains.
  - They do not separate broadcast domains.
  - Only routers separate broadcast domains.



MAC Address Table

MAC Address Table

Port	Source MAC Add.	Port	Source MAC Add.
1	**1111**		

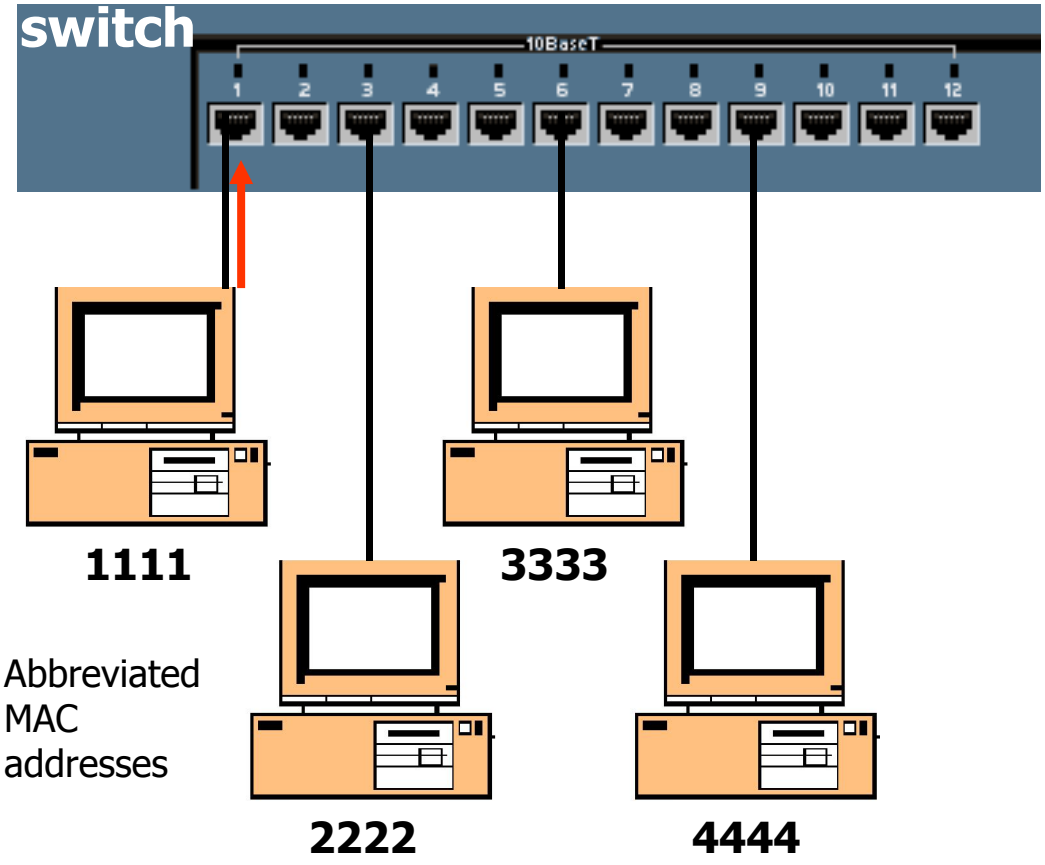
- Switches bind MAC addresses with switch ports and store the information in a MAC Address table.
  - Also known as a switch table, CAM table, or bridge table.

- The MAC address table is used to make forwarding decisions.

Learning Switches: Learns Source MAC Address

MAC Address Table

Port	Source MAC Add.	Port	Source MAC Add.
1	**1111**		



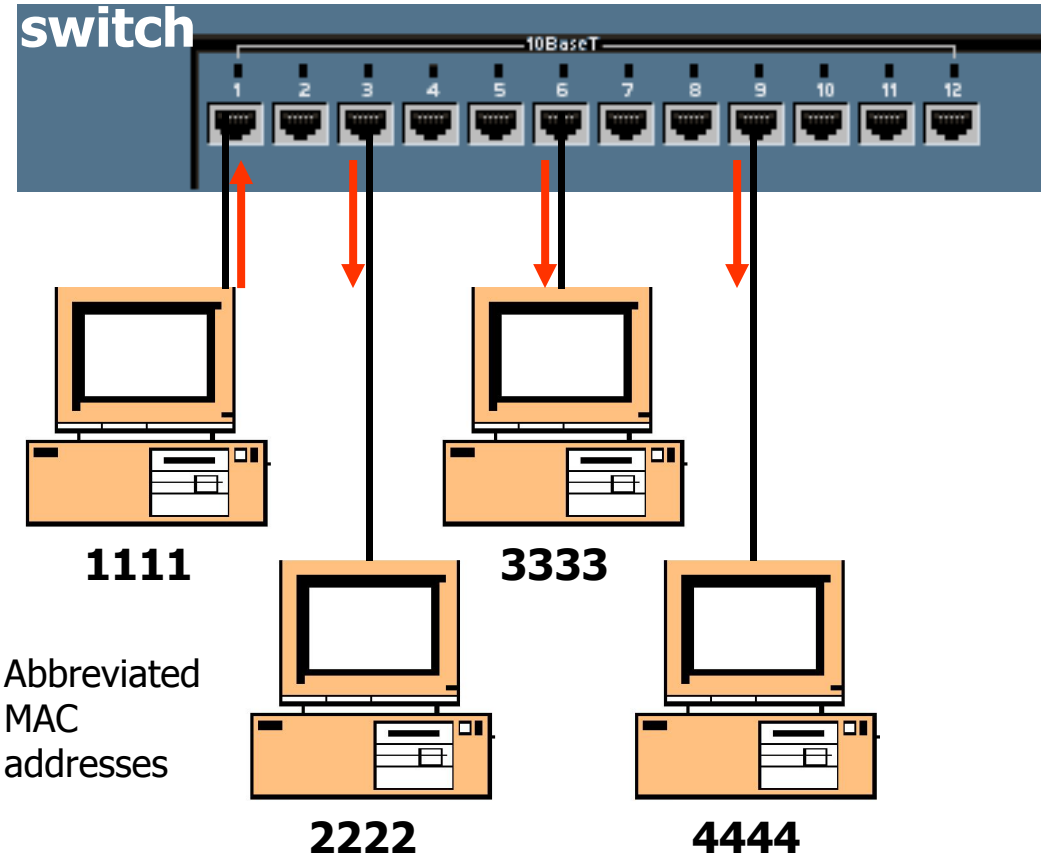
3333 1111

- Switches are also known as **learning bridges** or **learning switches**.
- A switch has a **source address table** (or **MAC Address Table**) in cache (RAM) where it stores a source MAC address after it learns about them.
- How does it learn source MAC addresses?
- Whenever a frame enters a switch, it will first see if the **Source Address** (1111) is in it's table.
  - If it is, it **resets the timer** (more in a moment).
  - If it is NOT in the table it **adds** it, with the port number.

Destination MAC Address: Filter or Flood

MAC Address Table

Port	Source MAC Add.	Port	Source MAC Add.
1	**1111**		



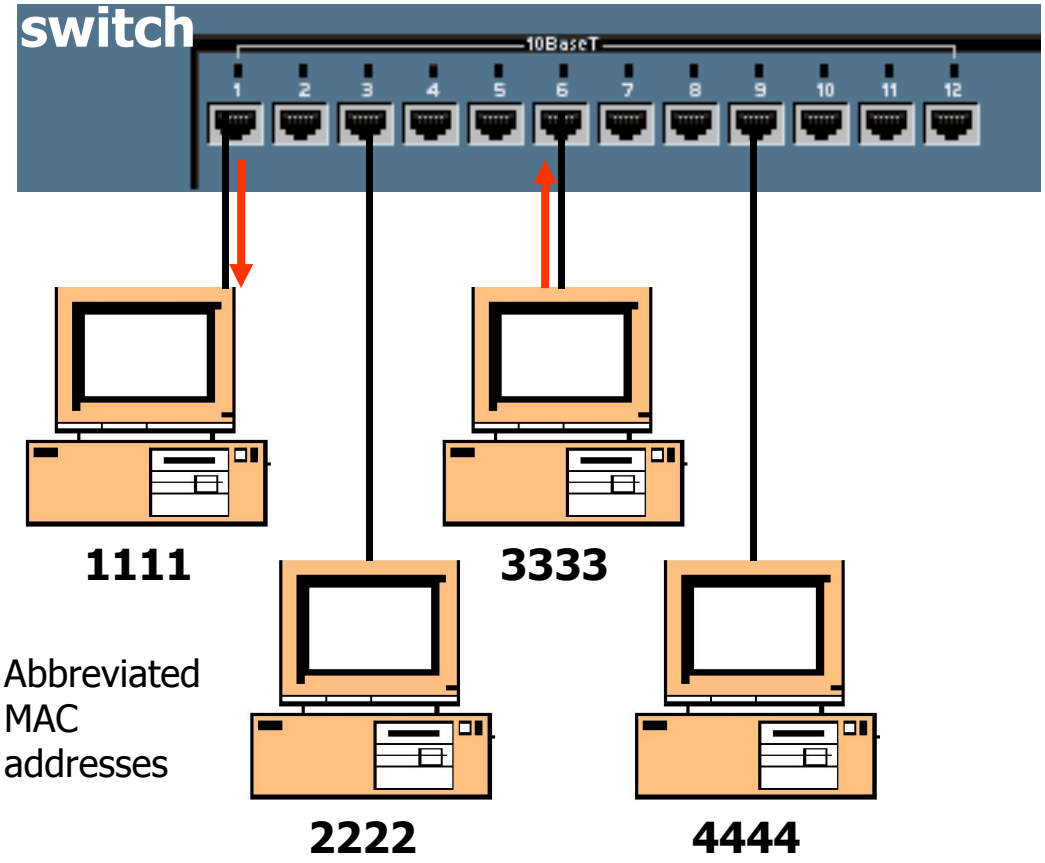
3333 1111

- Next, the switch examines the source address table for the **Destination MAC address**.
- If it finds a match, it **filters** the frame by only sending it out that port.
- If there is **not** a match if **floods** it out all ports.
- In this scenario, the switch will **flood** the frame out all other ports, because the **Destination Address** is **not** in the source address table.

Learning Switches: Learns, Filter or Flood

MAC Address Table

Port	Source MAC Add.	Port	Source MAC Add.
1	**1111**	**6**	**3333**



1111 3333

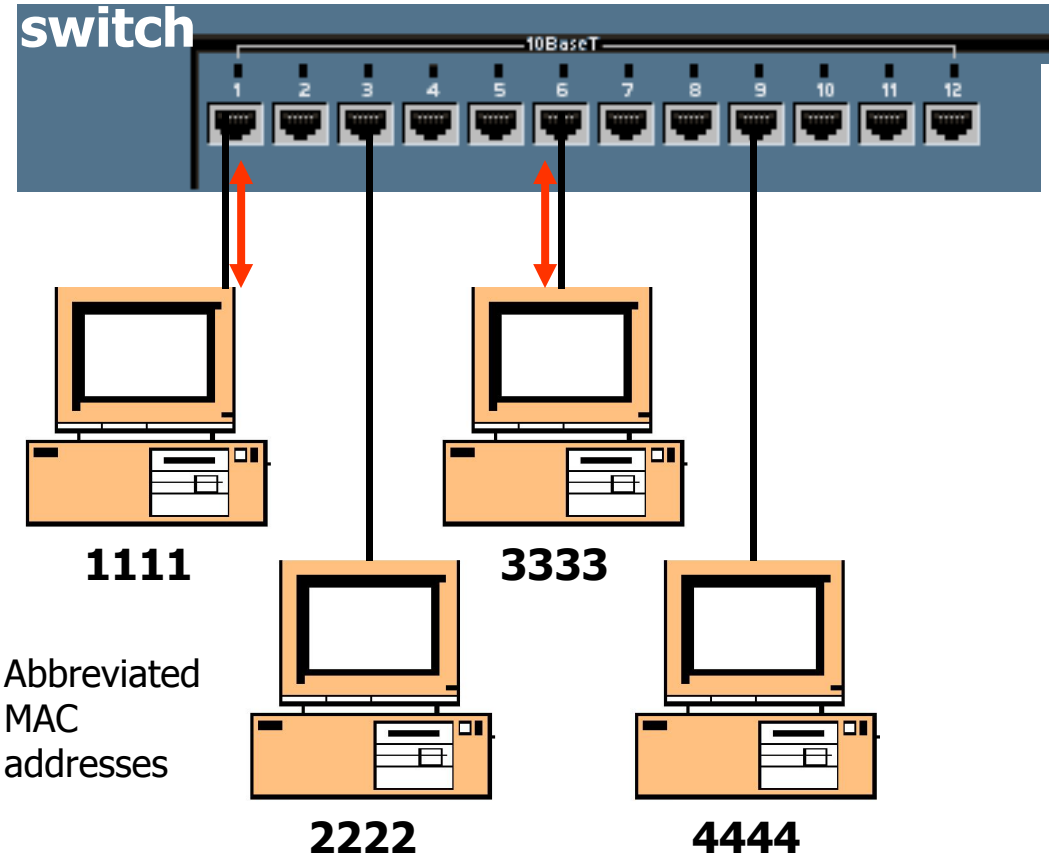
- Most communications involve some sort of **client-server relationship** or exchange of information. (You will understand this more as you learn about TCP/IP.)
- Now 3333 sends data back to 1111.
- The switch sees if it has the **Source Address** stored.
- It does **NOT** so it adds it. (This will help next time 1111 sends to 3333.)
- Next, it checks the **Destination Address** and in our case it can **filter** the frame, by sending it only out port 1.

Destination Address in table, Filter

MAC Address Table

Port	Source MAC Add.	Port	Source MAC Add.
1	**1111**	**6**	**3333**

Preamble	Destination Address	Source Address	Type	Data	Pad	CRC
	3333	**1111**				



1111 3333

- Now, because both MAC addresses are in the switch's table, any information exchanged between 1111 and 3333 can be sent (**filtered**) out the appropriate port.

- **What happens when two devices send to same destination?**
- **What if this was a hub?**
- **Where is (are) the collision domain(s) in this example?**

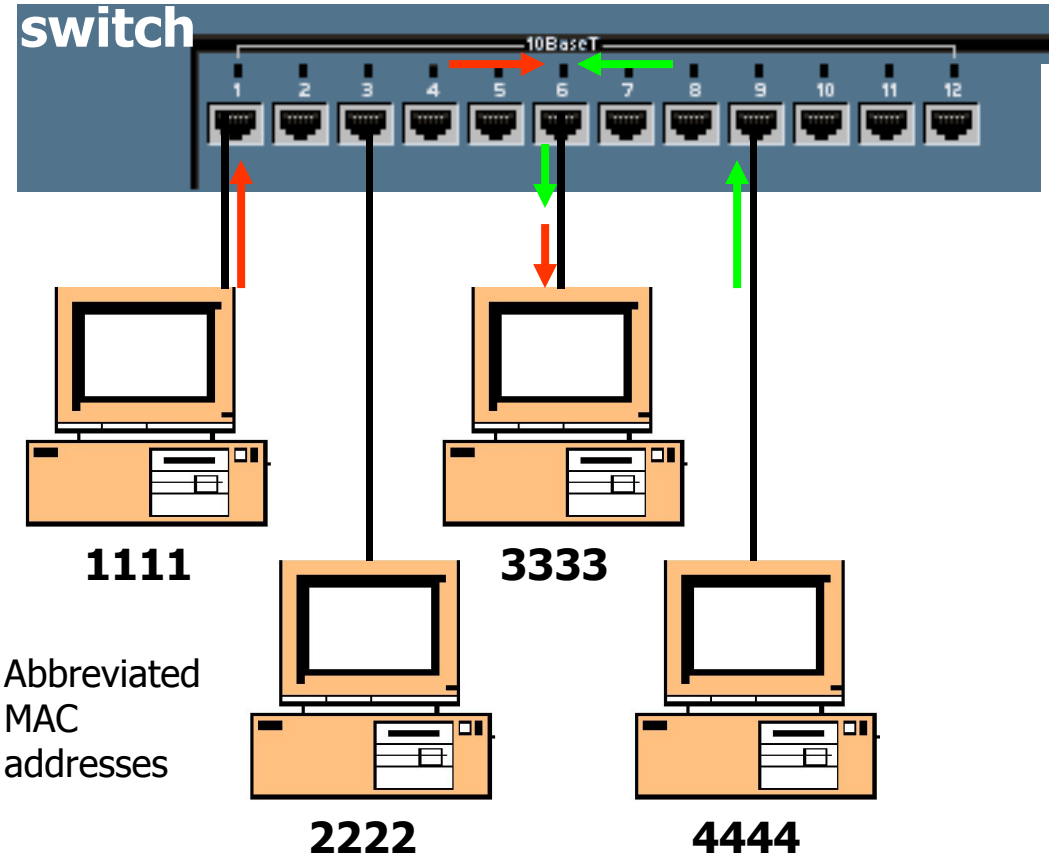
No Collisions in Switch, Buffering

MAC Address Table

Port	Source MAC Add.	Port	Source MAC Add.
1	1111	6	3333
9	4444		

Preamble	Destination Address	Source Address	Type	Data	Pad	CRC

3333 **1111**



3333 **4444**

- Unlike a hub, a **collision does NOT occur**, which would cause the two PCs to have to retransmit the frames.
- Collision domains end at the switch
- Instead the switch **buffers** the frames and sends them out port #6 one at a time.
- The sending PCs have no idea that their was another PC wanting to send to the same destination.

MAC Duplex – No collisions

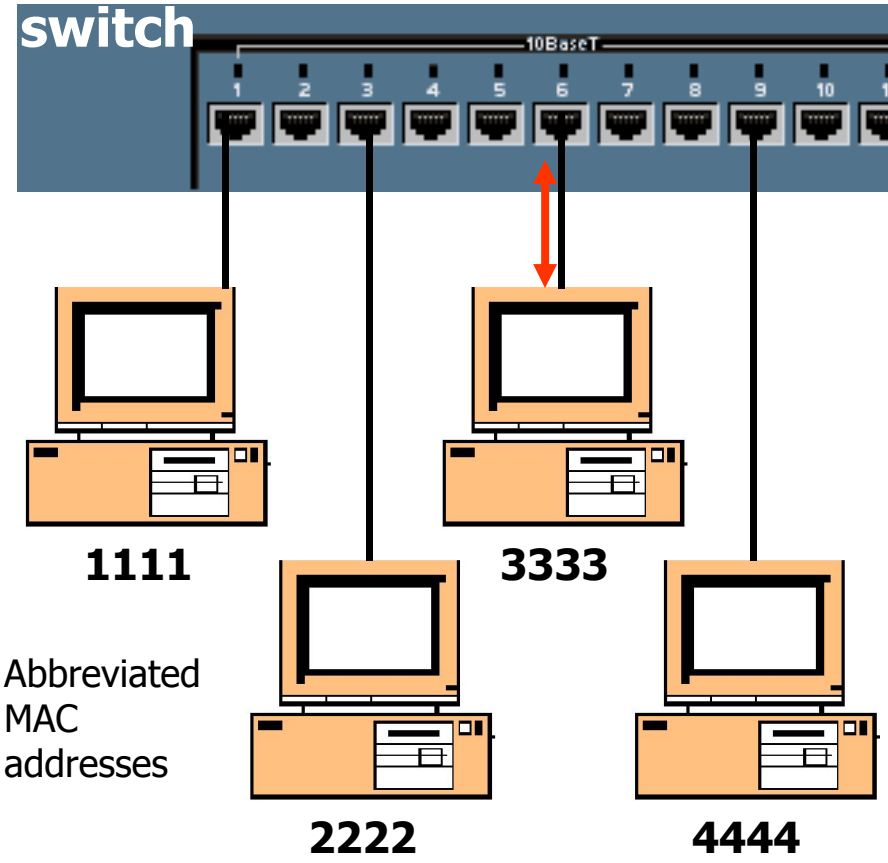
MAC Address Table

Port	Source MAC Add.	Port	Source MAC Add.
1	1111	6	3333
9	4444		

No Collision Domains

Preamble	Destination Address	Source Address	Type	Data	Pad	CRC

3333 **1111**



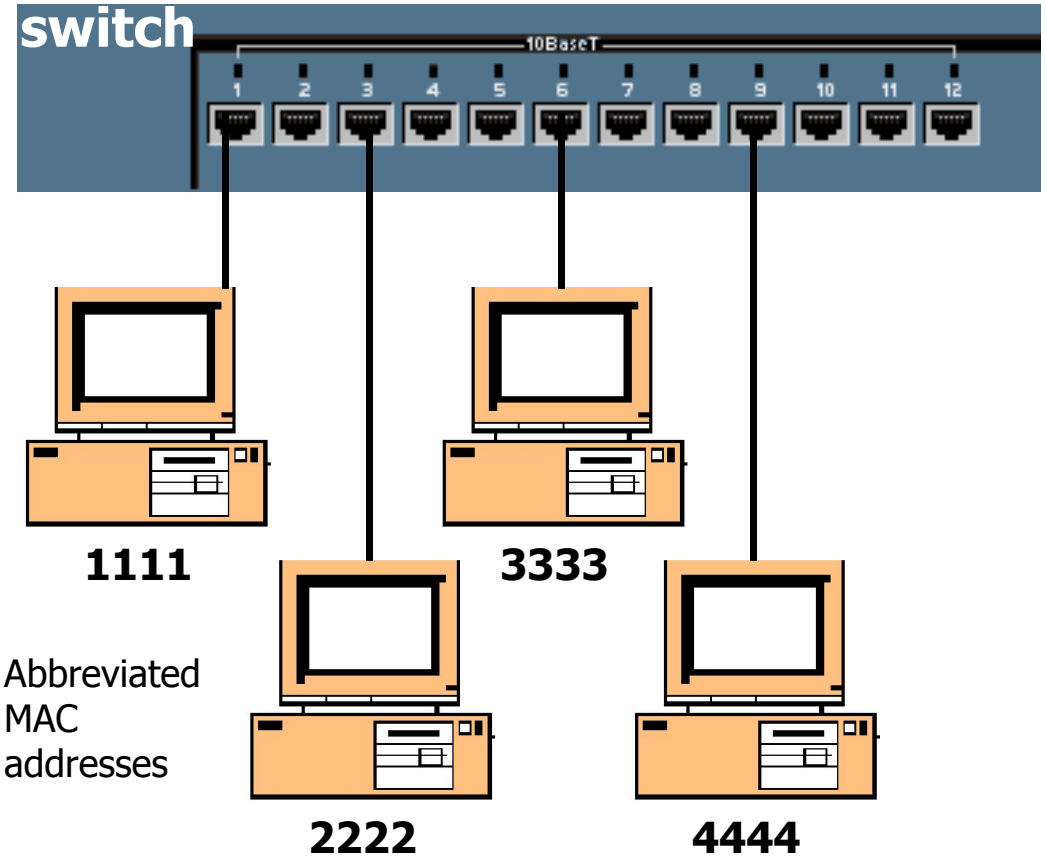
3333 **4444**

- When there is only one device on a switch port, the collision domain is only between the PC and the switch, which is non-existent with full-duplex.
- With a **full-duplex** PC and switch port, there will be no collision, since the devices and the medium can send and receive at the same time.

Other Information

MAC Address Table

Port	Source MAC Add.	Port	Source MAC Add.
1	**1111**	**6**	**3333**
9	**4444**		



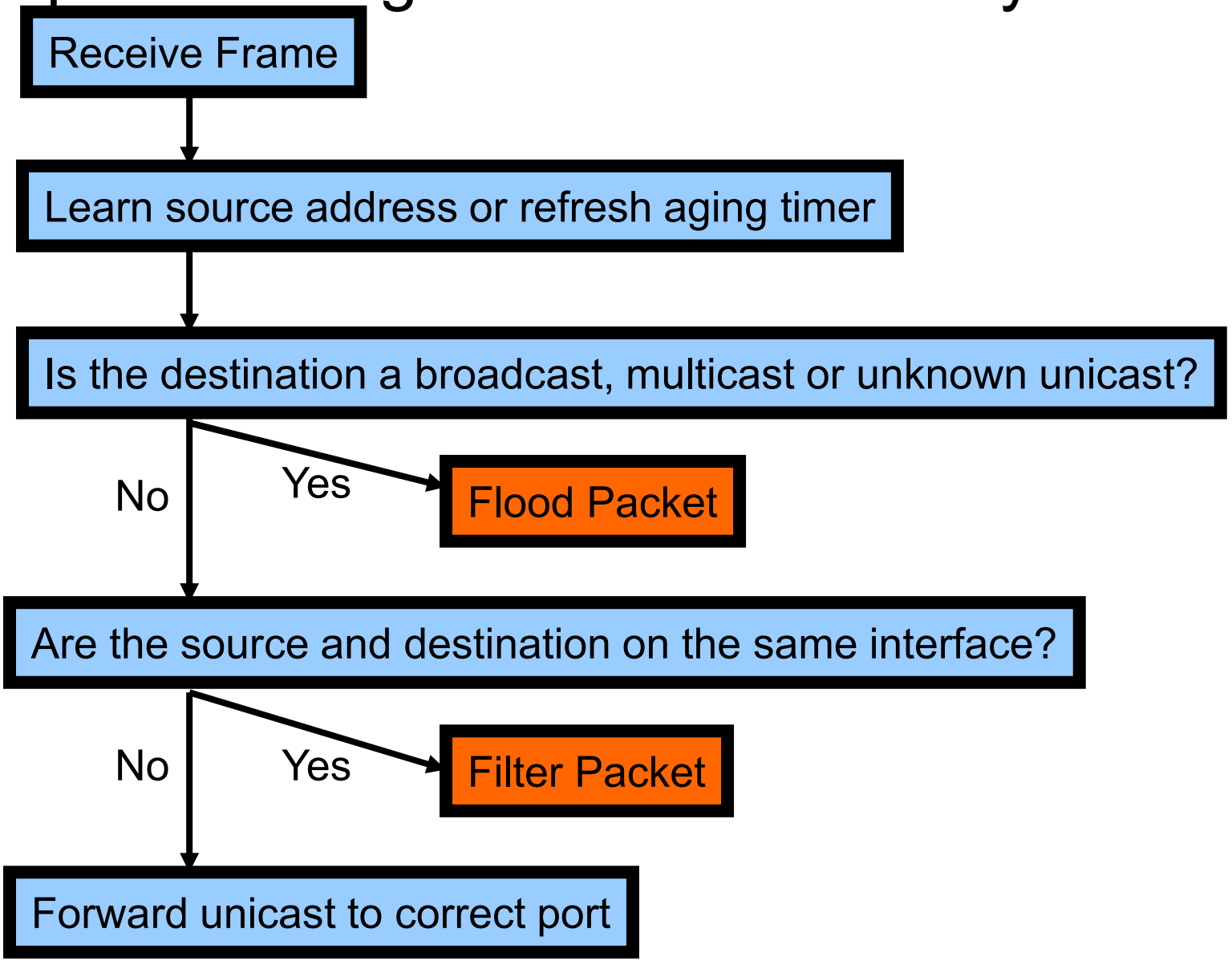
- How long are addresses kept in the Source Address Table?
  - **5 minutes** is common on most vendor switches.
- How do computers know the Destination MAC address?
  - **ARP Caches and ARP Requests** (later)
- How many addresses can be kept in the table?
  - Depends on the size of the cache, but 1,024 addresses is common.
- What about Layer 2 broadcasts?
  - Layer 2 broadcasts (**DA = all 1's) is flooded out all ports.**

Side Note - Transparent Bridging

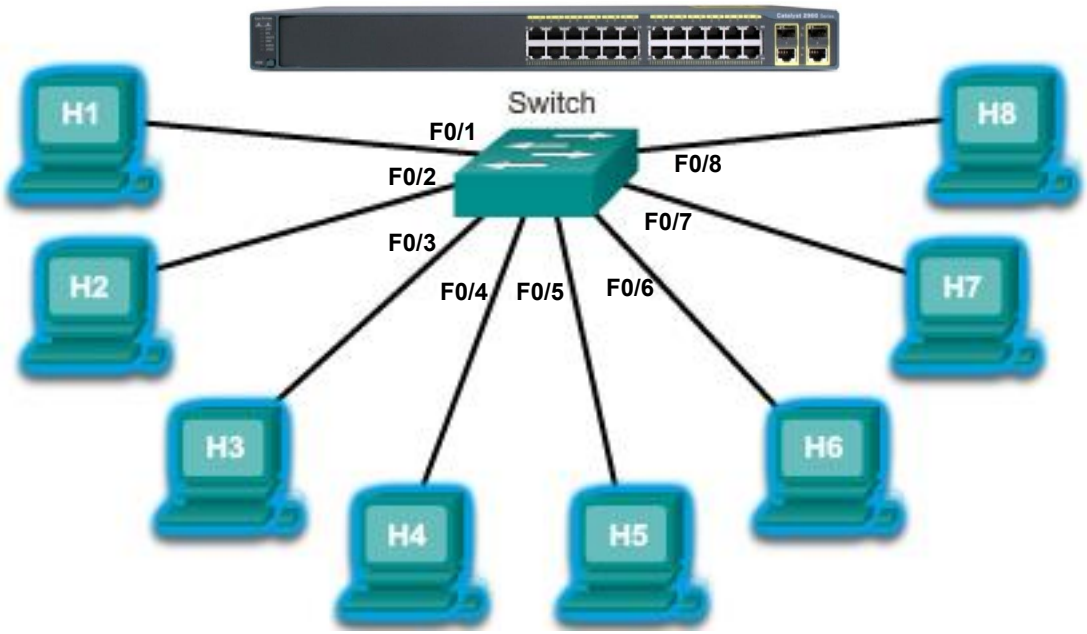
- Transparent bridging (normal switching process) is defined in IEEE 802.1D describing the five bridging processes of:
  - learning
  - flooding filtering
  - forwarding
  - aging

- These will be discussed further in STP (Spanning Tree Protocol), which is also part if IEEE 802.1D.

Transparent Bridge Process - Jeff Doyle



Switch Builds Its MAC Table



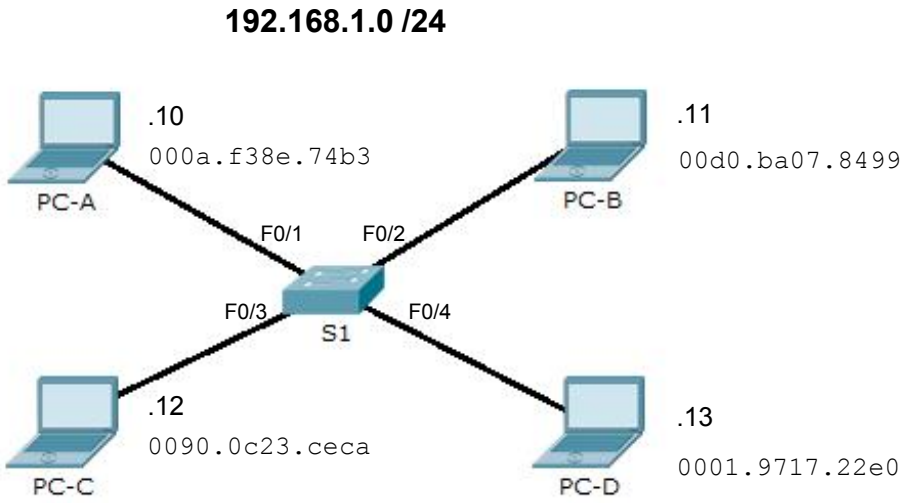
MAC Table

fa0/1	fa0/2	fa0/3	fa0/4
206d.8c01.0000	206d.8c01.1111	206d.8c01.2222	206d.8c01.3333
fa0/5	**fa0/6**	**fa0/7**	**fa0/8**
206d.8c01.4444	206d.8c01.5555	206d.8c01.6666	206d.8c01.7777

Layer 2 Switching #1

In this scenario, the switch has just rebooted.

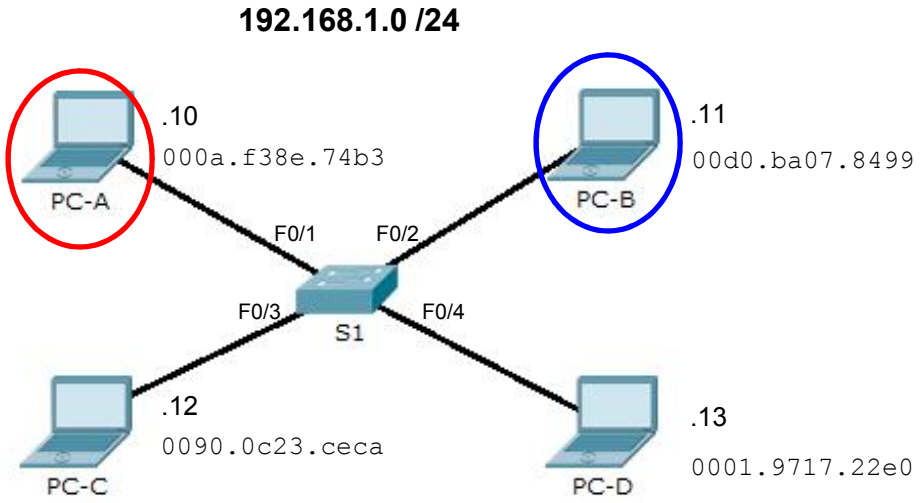
Verify the content of the MAC address table.




```
Sw1# show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

Sw1#
```

Packet Tracer Topology

Layer 2 Switching #1



PC-A pings PC-B.

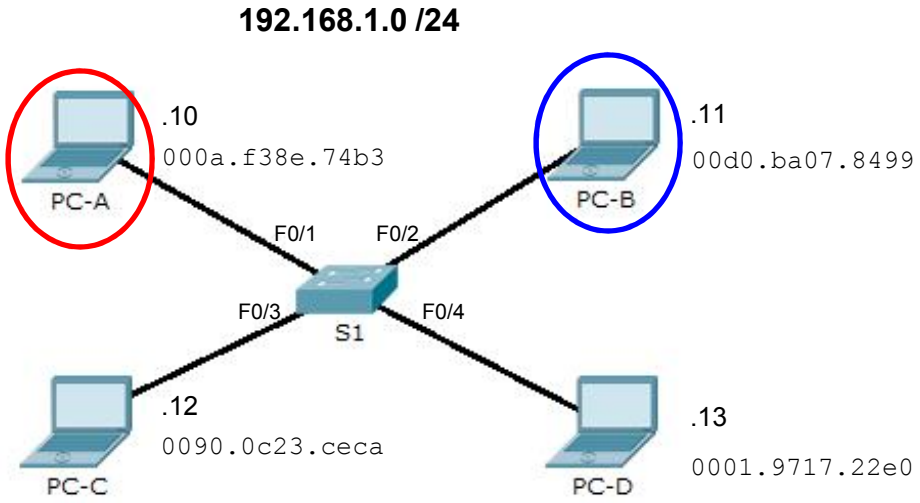
```
PC-A> ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:

Reply from 192.168.1.11: bytes=32 time=62ms TTL=128
Reply from 192.168.1.11: bytes=32 time=62ms TTL=128
Reply from 192.168.1.11: bytes=32 time=63ms TTL=128
Reply from 192.168.1.11: bytes=32 time=63ms TTL=128

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 62ms, Maximum = 63ms, Average = 62ms

PC-A>
```

Layer 2 Switching #1

Display the contents of the MAC table.

Notice how the switch has discovered that :
•PC-A's MAC address is connected to Fa0/1
•PC-B's MAC address is connected to Fa0/2.

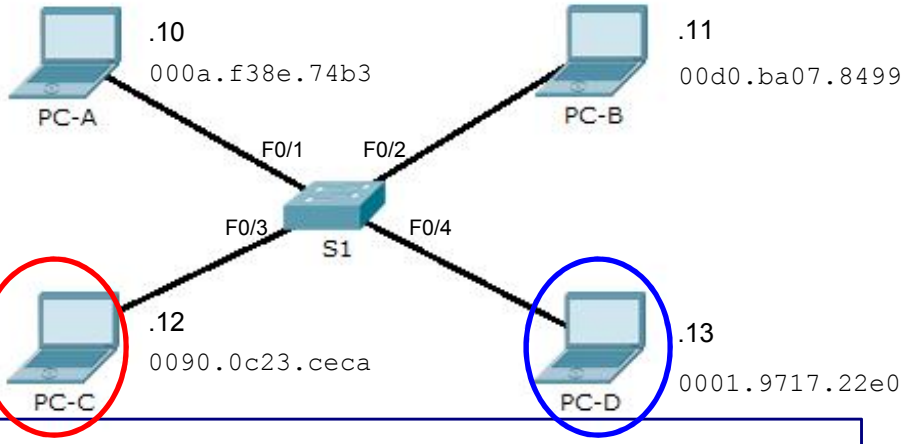
It used the source MAC address of the ARP Request and the source MAC address of the ARP Reply to add the entries in the MAC table.




```
Sw1# show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    000a.f38e.74b3    DYNAMIC     Fa0/1
   1    00d0.ba07.8499    DYNAMIC     Fa0/2
Sw1#
```

Layer 2 Switching #1

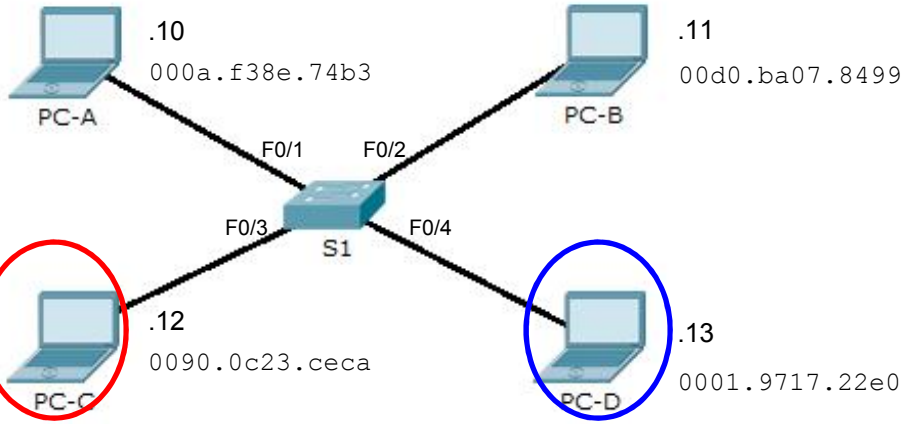
PC-C now pings PC-D.




```
PC-C> ping 192.168.1.13

Pinging 192.168.1.13 with 32 bytes of data:

Reply from 192.168.1.13: bytes=32 time=109ms TTL=128
Reply from 192.168.1.13: bytes=32 time=63ms TTL=128
Reply from 192.168.1.13: bytes=32 time=63ms TTL=128
Reply from 192.168.1.13: bytes=32 time=63ms TTL=128

Ping statistics for 192.168.1.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 63ms, Maximum = 109ms, Average = 74ms

PC-C>
```

Layer 2 Switching #1

192.168.1.0 /24



Notice how the switch has discovered that :
- PC-C's MAC address is connected to Fa0/3.
- PC-D's MAC address is connected to Fa0/4.

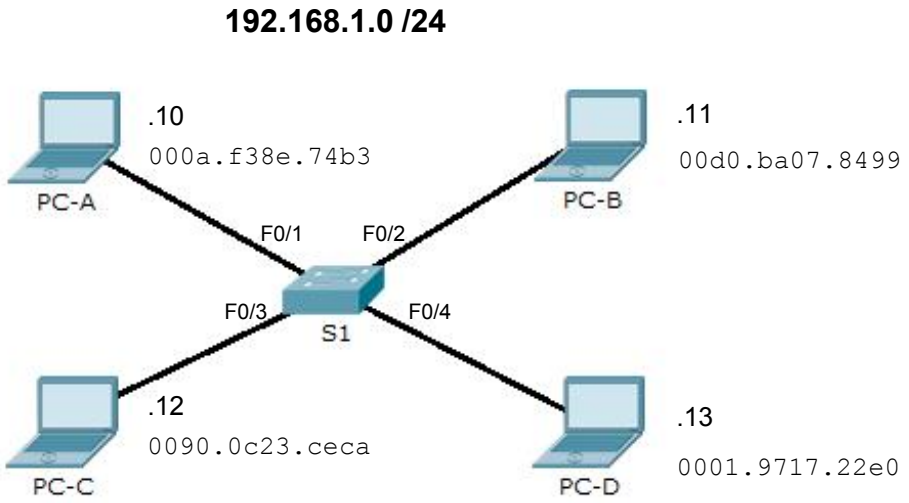
It used the source MAC address of the ARP Request and the source MAC address of the ARP Reply to add the entries in the MAC table.

Display the contents of the MAC table.

```
Sw1# show mac-address-table
Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.9717.22e0    DYNAMIC     Fa0/4
   1    000a.f38e.74b3    DYNAMIC     Fa0/1
   1    0090.0c23.ceca    DYNAMIC     Fa0/3
   1    00d0.ba07.8499    DYNAMIC     Fa0/2
Sw1#
```

Layer 2 Switching #1

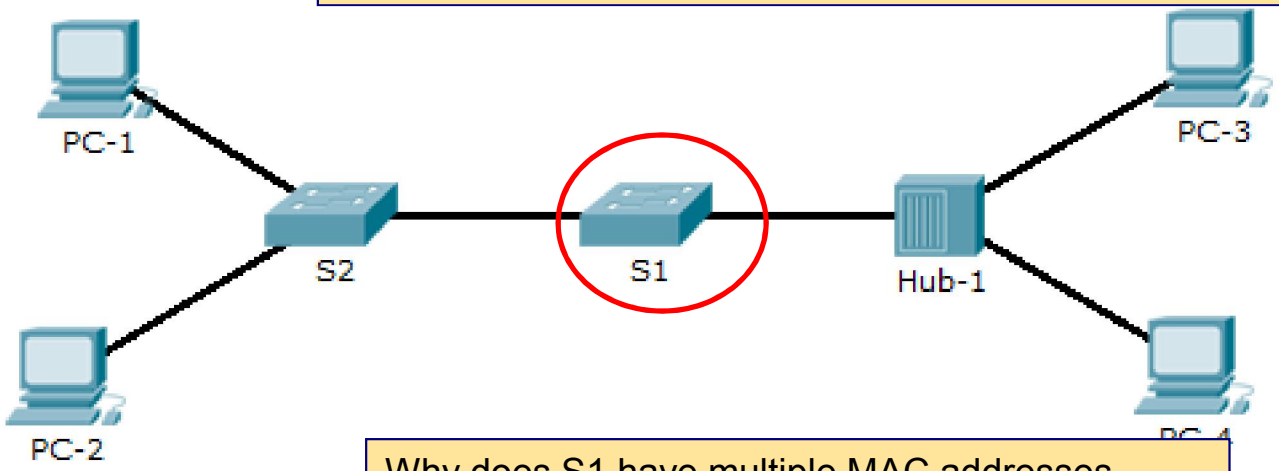
Clear and display the MAC table.




```
Sw1# clear mac-address-table
Sw1#
Sw1# show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

Sw1#
```

Layer 2 Switching #2

A switch records multiple entries for a single switch port in its MAC address table when another switch or hub is connected to the switch port.



Why does S1 have multiple MAC addresses assigned to Fa0/1 and Fa0/2?

```
S1# show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    000b.beea.03b6    DYNAMIC     Fa0/1
   1    0050.0f31.21b2    DYNAMIC     Fa0/1
   1    00d0.97e5.bc01    DYNAMIC     Fa0/1
   1    00e0.f7eb.6816    DYNAMIC     Fa0/2
   1    000d.bd8b.357d    DYNAMIC     Fa0/2
S1#
```

Basic Switch Operations

- All switches perform the following tasks:

Selective Forwarding

- A switch establishes a momentary logical point-to-point connection between the source and destination hosts.
  - Only long enough to forward a single frame.

- Switches can forward frames using 2 methods:
  - **Store and forward** (default on Cisco switches)
  - **Cut Through: Fast Forward or Fragment Free**

Selective Forwarding

Cut-Through

Lowest Latency

No error checking

Cut-Through

Fragment Free

Low Latency

Checks for collisions

(Filters most errors)

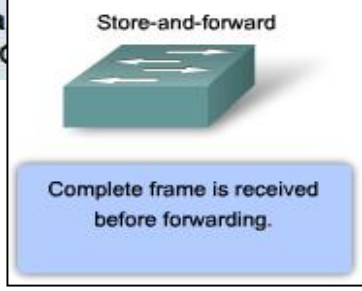
Store-and-Forward

Highest Latency

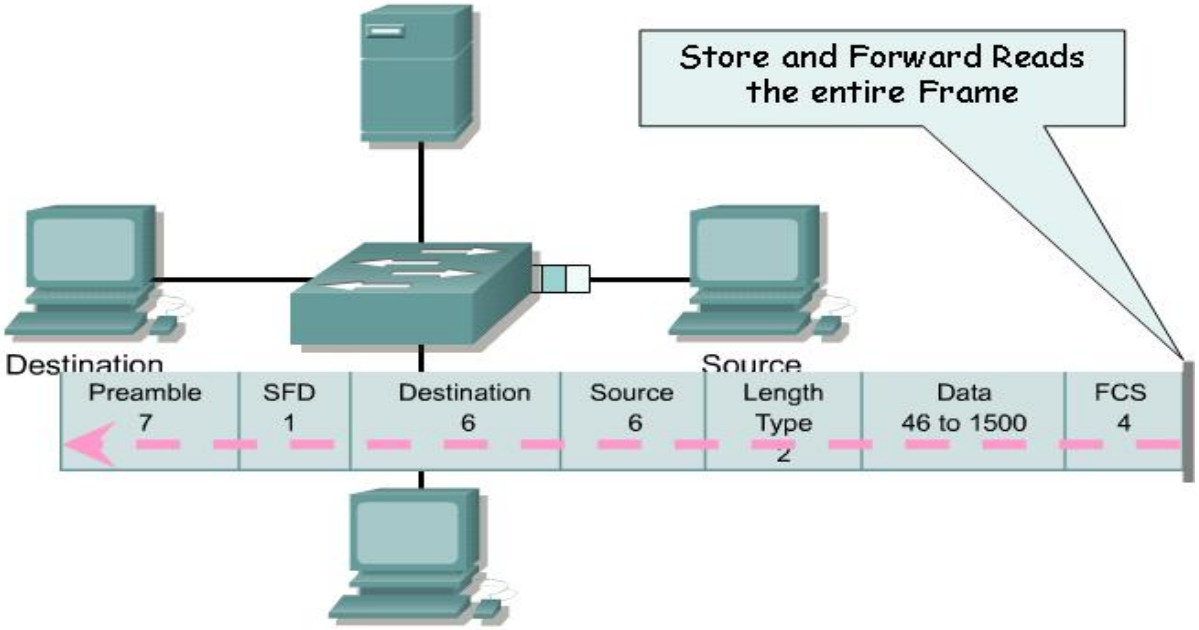
All errors filtered

Lowest Latency — **Highest Latency**

Less Error Checking — **More Error Checking**

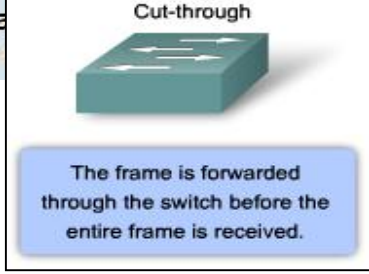


Store-and-Forward Switching

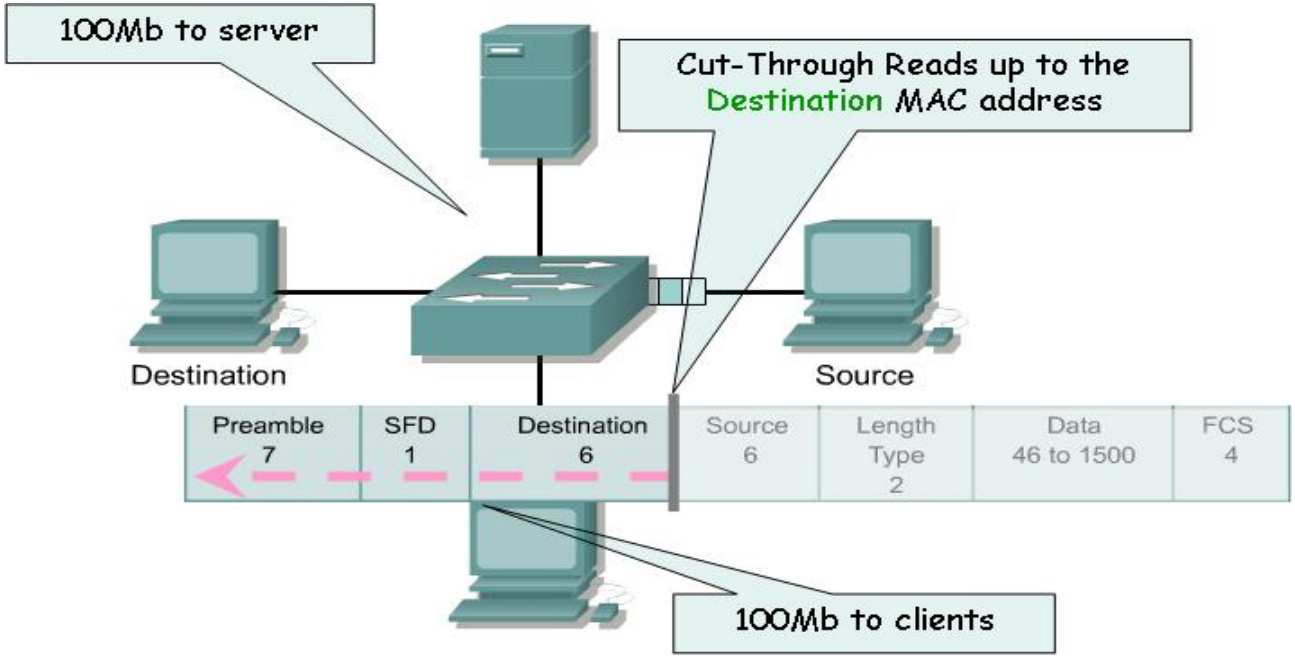


- Reads the entire frame:.
  - Discards any frames that are corrupt (runts/ too big)
  - Performs FCS using CRC and discards any frames with errors
  - Allows QoS checks

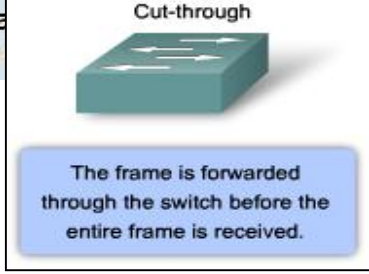
- Once the entire frame has been read and checked for errors, the switch then forwards it.
  - Allows entry and exit at different (asymmetric) bandwidths



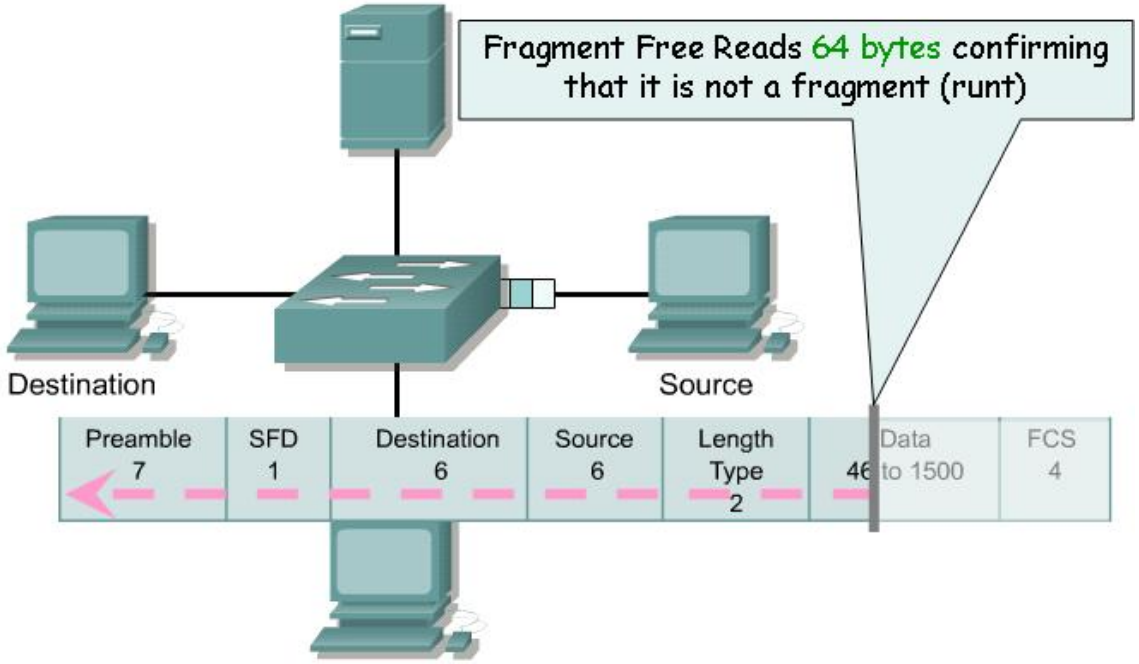
Cut Through – Fast Forward



- Reads up to the end of destination MAC address.
  - Then starts sending it out the designated port while remainder of frame is still coming in.
  - Lowest latency but no error control.
- Entry and exit must be same bandwidth



Cut Through – Fragment Free



- Reads up to the end of byte 64 and then:
  - Looks up port and start forwarding while remainder of frame (if any) is still coming in.
  - Discards collision fragments (too short) but other bad frames are forwarded
  - Compromise between low latency and checks
- Entry and exit must be same bandwidth

Symmetric and Asymmetric Switching

Port-Based and Shared Memory

- An Ethernet switch can use a buffering technique to store frames before forwarding them.
  - Buffering may also be used when the destination port is busy due to congestion and the switch stores the frame until it can be transmitted.

- Cisco switches can use two methods of memory buffering:
  - Port-based Memory Buffering
  - Shared Memory Buffering

Port-Based Buffering

- Each incoming port has its own queue.
- Frames stay in buffer until outgoing port is free.
- Frame destined for busy outgoing port can hold up all the others even if their outgoing ports are free.
- Each incoming port has a fixed and limited amount of memory.

Shared Memory Buffering

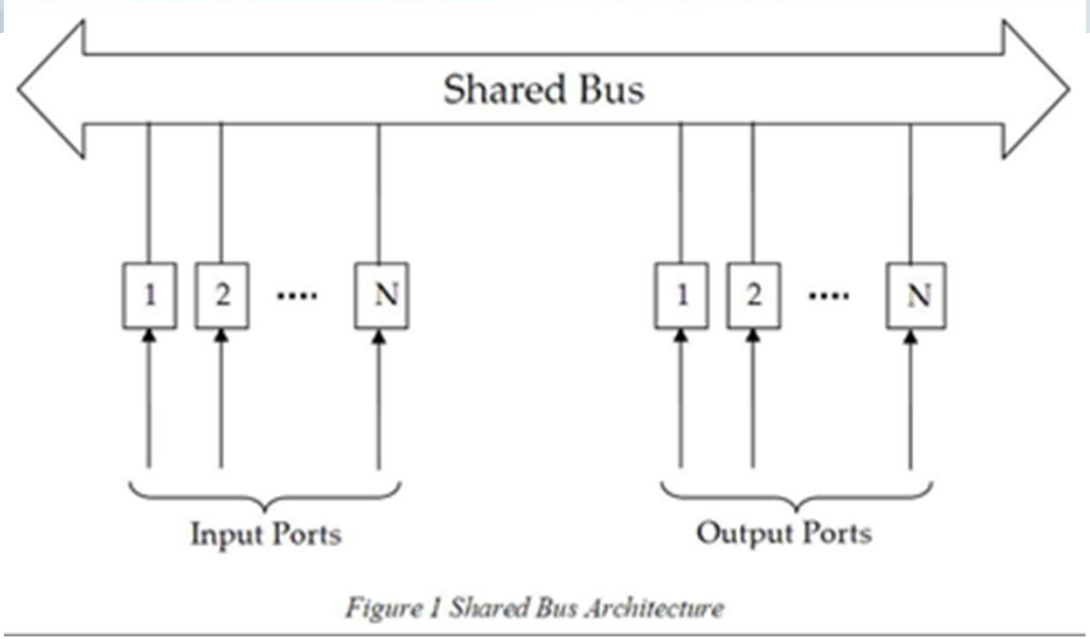
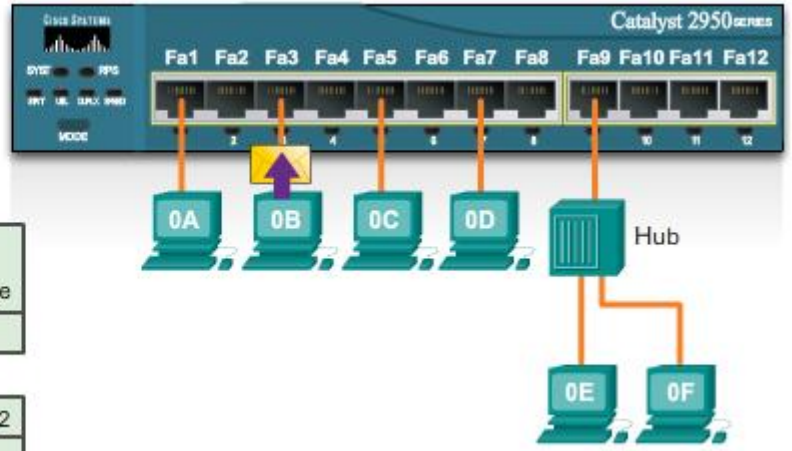


Figure 1 Shared Bus Architecture

- The number of frames stored in the buffer is restricted only by the size of the memory buffer and not to a port buffer.
  - Permits larger frames to be transmitted with fewer dropped frames.
- All incoming frames go in a common buffer.
  - Switch maps frame to destination port and forwards it when port is free.
  - Frames do not hold each other up.
- Shared memory buffers are required to support asymmetric switching.

5.3.1.9 -1

Activity
Determine how the switch forwards a frame based on the Source MAC and Destination MAC addresses and information in the switch MAC table.
Answer the questions below using the information provided.



Frame

Preamble	Destination MAC	Source MAC	Length Type	Encapsulated Data	End of Frame
	0A	**0B**			

MAC Table

Fa1	Fa2	Fa3	Fa4	Fa5	Fa6	Fa7	Fa8	Fa9		Fa10	Fa11	Fa12
0A				**0C**		**0D**		**0E**	**0F**			

Question 1 - Where will the switch forward the frame?

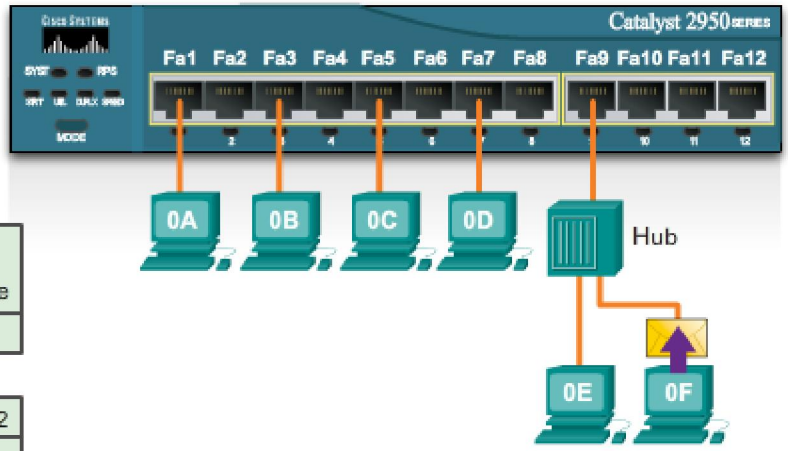
- [x] Fa1
- [ ] Fa2
- [ ] Fa3
- [ ] Fa4
- [ ] Fa5
- [ ] Fa6
- [ ] Fa7
- [ ] Fa8
- [ ] Fa9
- [ ] Fa10
- [ ] Fa11
- [ ] Fa12

Question 2 - When the switch forwards the frame, which statement(s) are true?

- [x] Switch adds the source MAC address to the MAC table.
- [ ] Frame is a broadcast frame and will be forwarded to all ports.
- [x] Frame is a unicast frame and will be sent to specific port only.
- [ ] Frame is a unicast frame and will be flooded to all ports.
- [ ] Frame is a unicast frame but it will be dropped at the switch.

5.3.1.9 -2

Activity
Determine how the switch forwards a frame based on the Source MAC and Destination MAC addresses and information in the switch MAC table.
Answer the questions below using the information provided.



Frame

Preamble	Destination MAC	Source MAC	Length Type	Encapsulated Data	End of Frame
	0D	0F			

MAC Table

Fa1	Fa2	Fa3	Fa4	Fa5	Fa6	Fa7	Fa8	Fa9	Fa10	Fa11	Fa12
		0B		0C							

Question 1 - Where will the switch forward the frame?

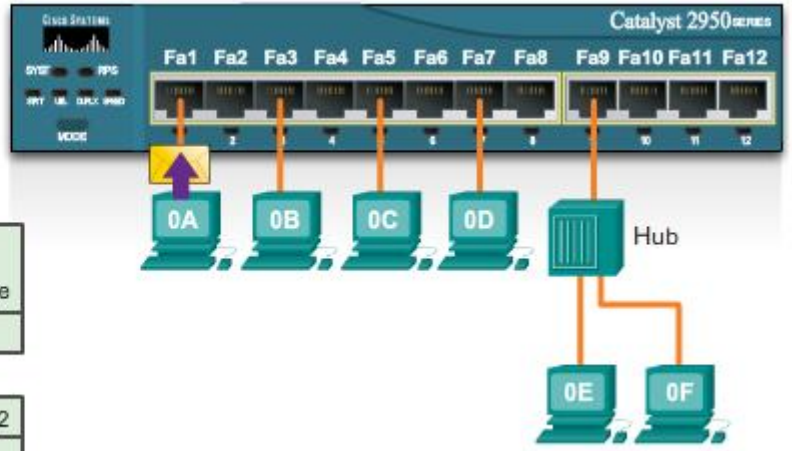
- [x] Fa1
- [ ] Fa2
- [x] Fa3
- [ ] Fa4
- [x] Fa5
- [ ] Fa6
- [x] Fa7
- [ ] Fa8
- [ ] Fa9
- [ ] Fa10
- [ ] Fa11
- [ ] Fa12

Question 2 - When the switch forwards the frame, which statement(s) are true?

- [x] Switch adds the source MAC address to the MAC table.
- [ ] Frame is a broadcast frame and will be forwarded to all ports.
- [ ] Frame is a unicast frame and will be sent to specific port only.
- [x] Frame is a unicast frame and will be flooded to all ports.
- [ ] Frame is a unicast frame but it will be dropped at the switch.

5.3.1.9 - 3

Activity
Determine how the switch forwards a frame based on the Source MAC and Destination MAC addresses and information in the switch MAC table.
Answer the questions below using the information provided.



Frame

Preamble	Destination MAC	Source MAC	Length Type	Encapsulated Data	End of Frame
	0D	**0A**			

MAC Table

Fa1	Fa2	Fa3	Fa4	Fa5	Fa6	Fa7	Fa8	Fa9	Fa10	Fa11	Fa12
0A		**0B**									

Question 1 - Where will the switch forward the frame?

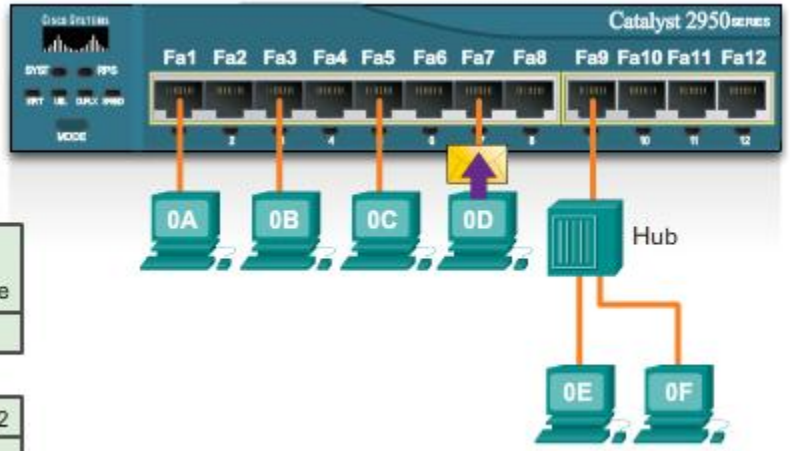
- [ ] Fa1
- [ ] Fa2
- [x] Fa3
- [ ] Fa4
- [x] Fa5
- [ ] Fa6
- [x] Fa7
- [ ] Fa8
- [x] Fa9
- [ ] Fa10
- [ ] Fa11
- [ ] Fa12

Question 2 - When the switch forwards the frame, which statement(s) are true?

- [ ] Switch adds the source MAC address to the MAC table.
- [ ] Frame is a broadcast frame and will be forwarded to all ports.
- [ ] Frame is a unicast frame and will be sent to specific port only.
- [x] Frame is a unicast frame and will be flooded to all ports.
- [ ] Frame is a unicast frame but it will be dropped at the switch.

5.3.1.9 - 4

Activity
Determine how the switch forwards a frame based on the Source MAC and Destination MAC addresses and information in the switch MAC table.
Answer the questions below using the information provided.



Frame

Preamble	Destination MAC	Source MAC	Length Type	Encapsulated Data	End of Frame
	FF	0D			

MAC Table

Fa1	Fa2	Fa3	Fa4	Fa5	Fa6	Fa7	Fa8	Fa9	Fa10	Fa11	Fa12
								0F			

Question 1 - Where will the switch forward the frame?

- [x] Fa1
- [ ] Fa2
- [x] Fa3
- [ ] Fa4
- [x] Fa5
- [ ] Fa6
- [ ] Fa7
- [ ] Fa8
- [x] Fa9
- [ ] Fa10
- [ ] Fa11
- [ ] Fa12

Question 2 - When the switch forwards the frame, which statement(s) are true?

- [x] Switch adds the source MAC address to the MAC table.
- [x] Frame is a broadcast frame and will be forwarded to all ports.
- [ ] Frame is a unicast frame and will be sent to specific port only.
- [ ] Frame is a unicast frame and will be flooded to all ports.
- [ ] Frame is a unicast frame but it will be dropped at the switch.

Fixed or Modular Switches

Enterprise Level Switches

Cisco Switches

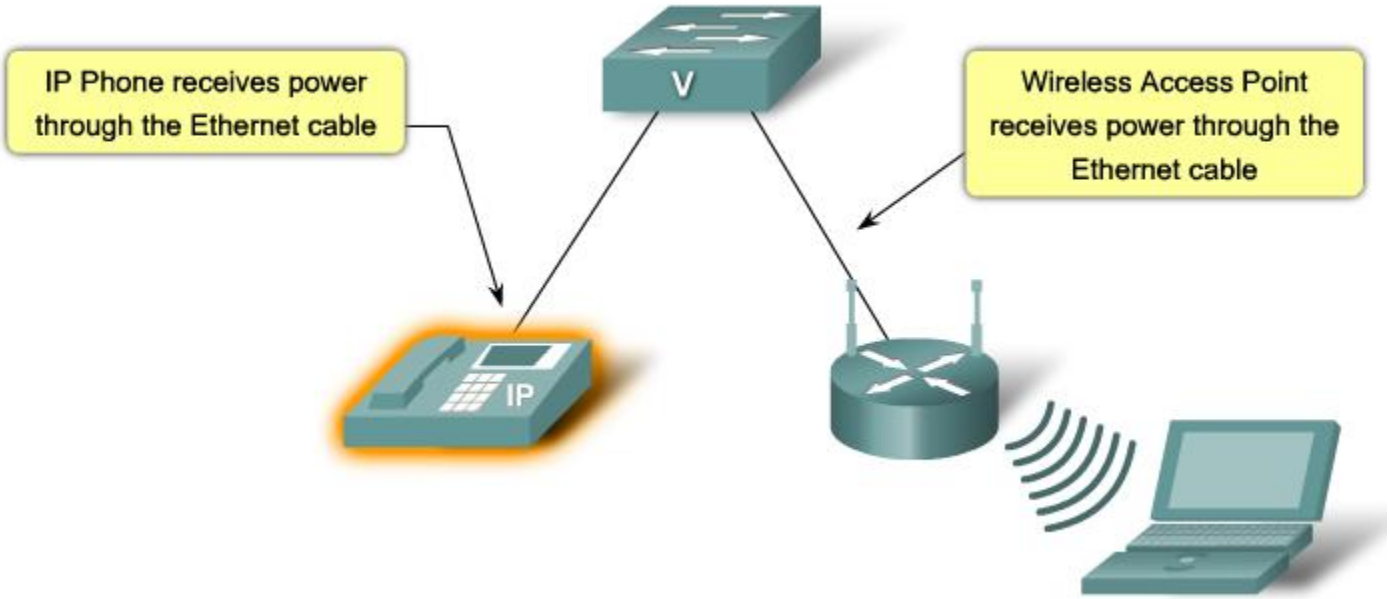
Switch Form Factors

Fixed Configuration Switches 	• Features and options are limited to those that originally come with the switch. • The number of ports cannot be increased. • Switch may be stackable. • Layer 2 switch: Catalyst 2960 • Layer 3 switch: Catalyst 3650
Modular Configuration Switches 	• Large enterprise class switches. • The chassis is totally customizable as different line cards can be used. • Adding additional line cards increases port density. • Catalyst 4500, 6500, 6800
Stackable Configuration Switches 	• Stackable switches, interconnected by a special cable and makes the combined group of switches operate as one large switch. • Catalyst 3750

Enterprise Level Switches

- Characteristics of enterprise level switches include:
  - **Port Density**: This is the number of ports available on a single switch.
  - **High Forwarding Rates**: Defines the processing capabilities of a switch by rating how much data the switch can process per second.
  - **Support for Link Aggregation**: Helps reduce traffic bottlenecks by allowing up to 8 switch ports to be bound and provide higher throughput.

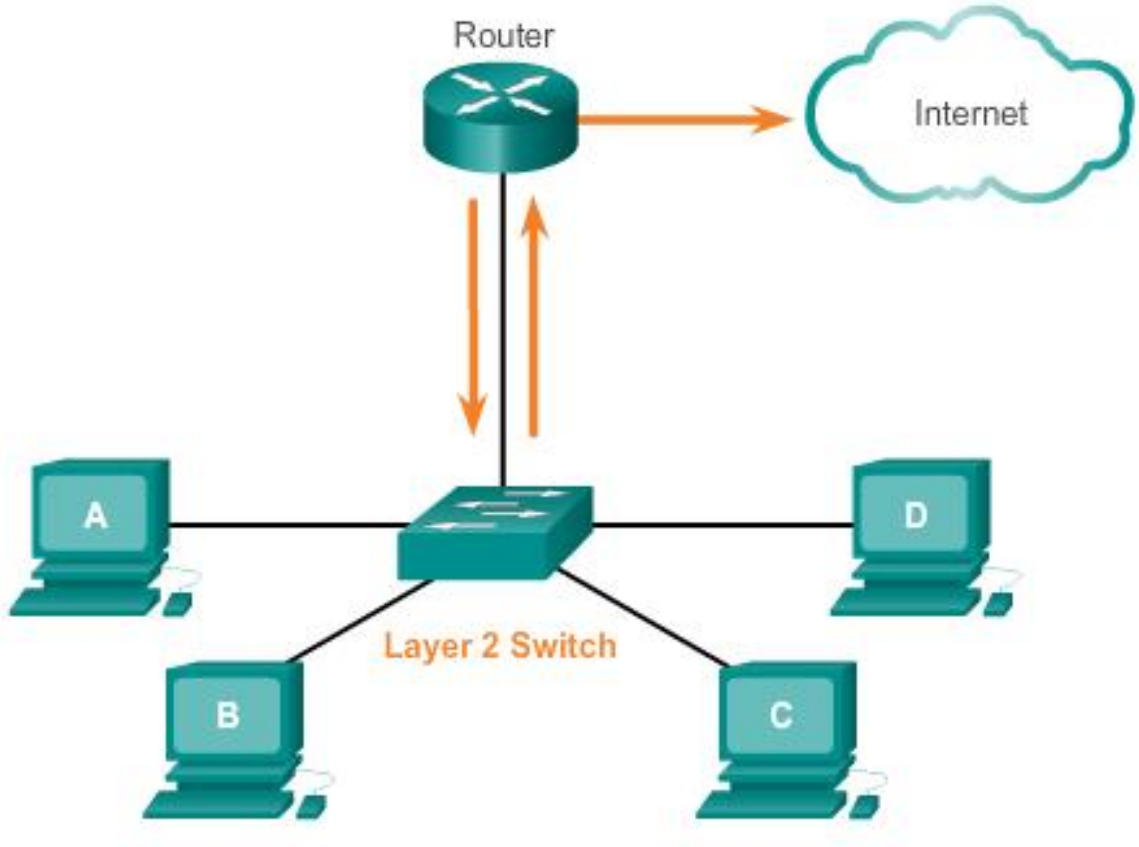
Power over Ethernet (PoE)



- Allows the switch to deliver power to a device over the existing Ethernet cabling.
- Can provide power to IP phones and wireless access points.

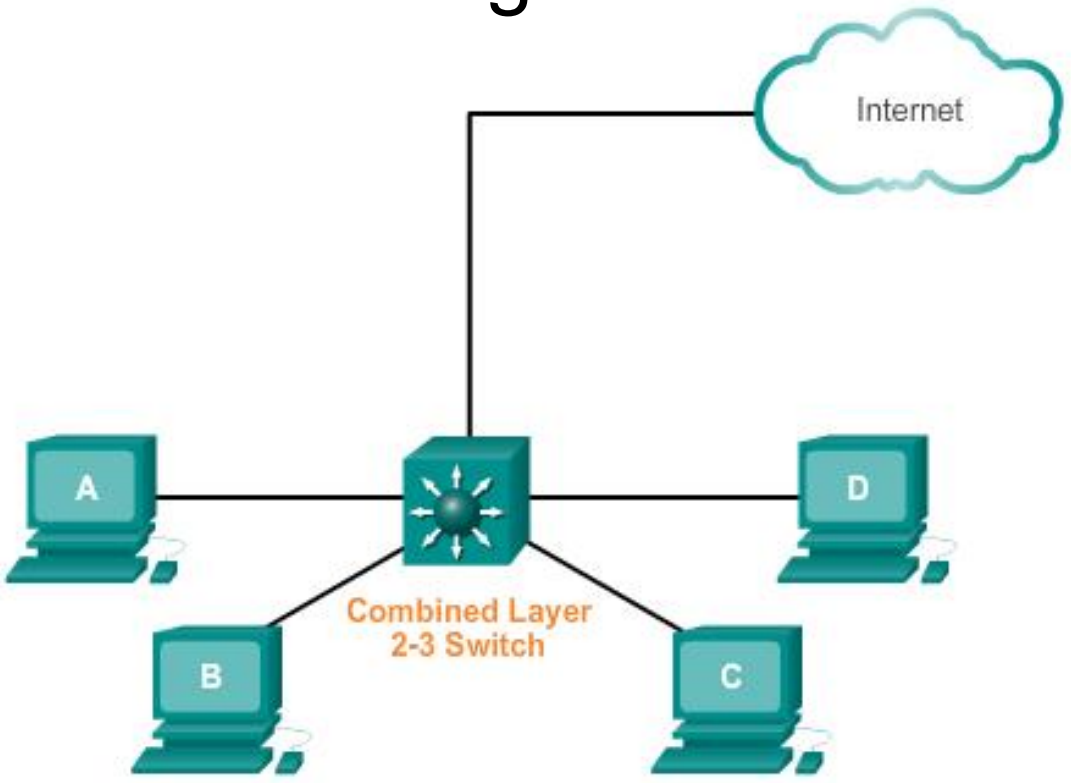
Layer 2 versus Layer 3 Switches

Layer 2 Functions



- Typically, switches operate at OSI Layer 2
  - It makes forwarding decisions based on the MAC addresses of devices connected to switch ports.

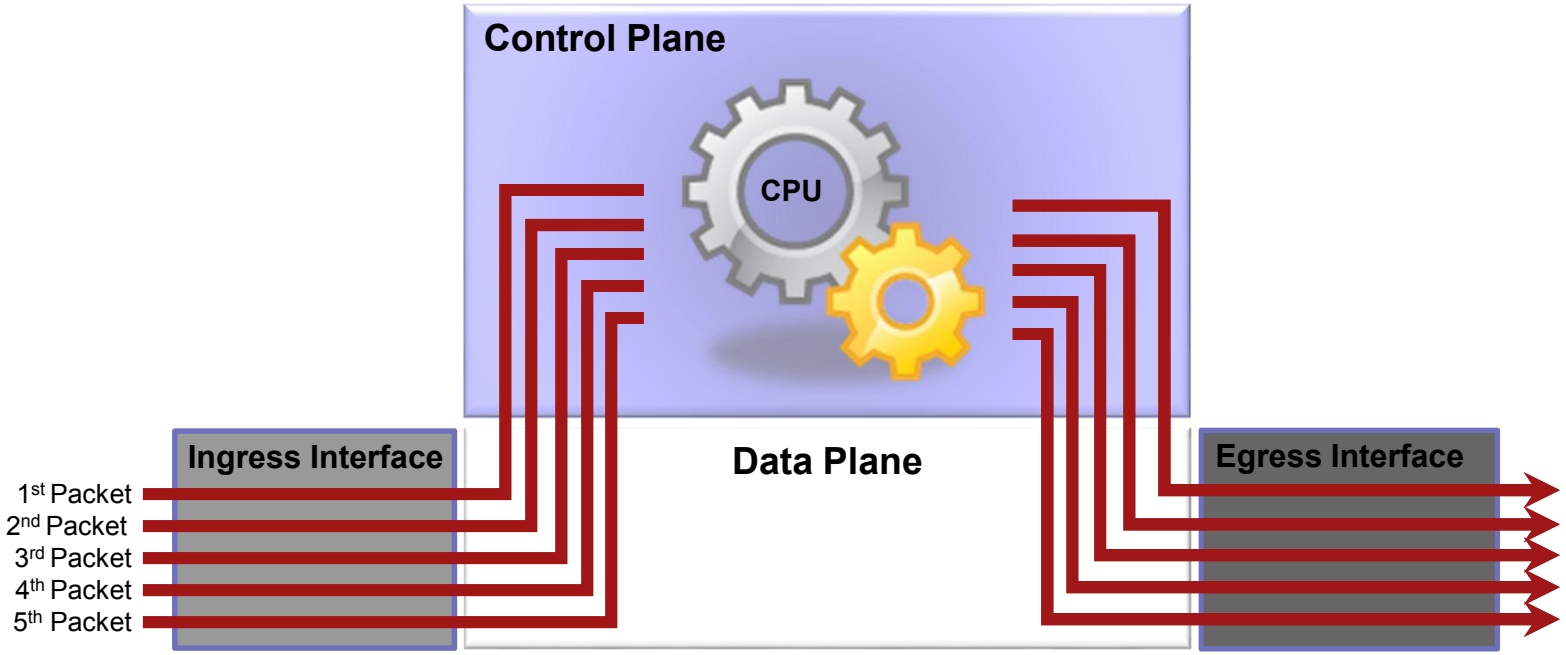
Layer 2 verses Layer 3 Switching



- Layer 3 switches (also known as multilayer switches) offer advanced functionality.
  - It makes forwarding decisions based on MAC and/or IP addresses of devices connected to switch ports.

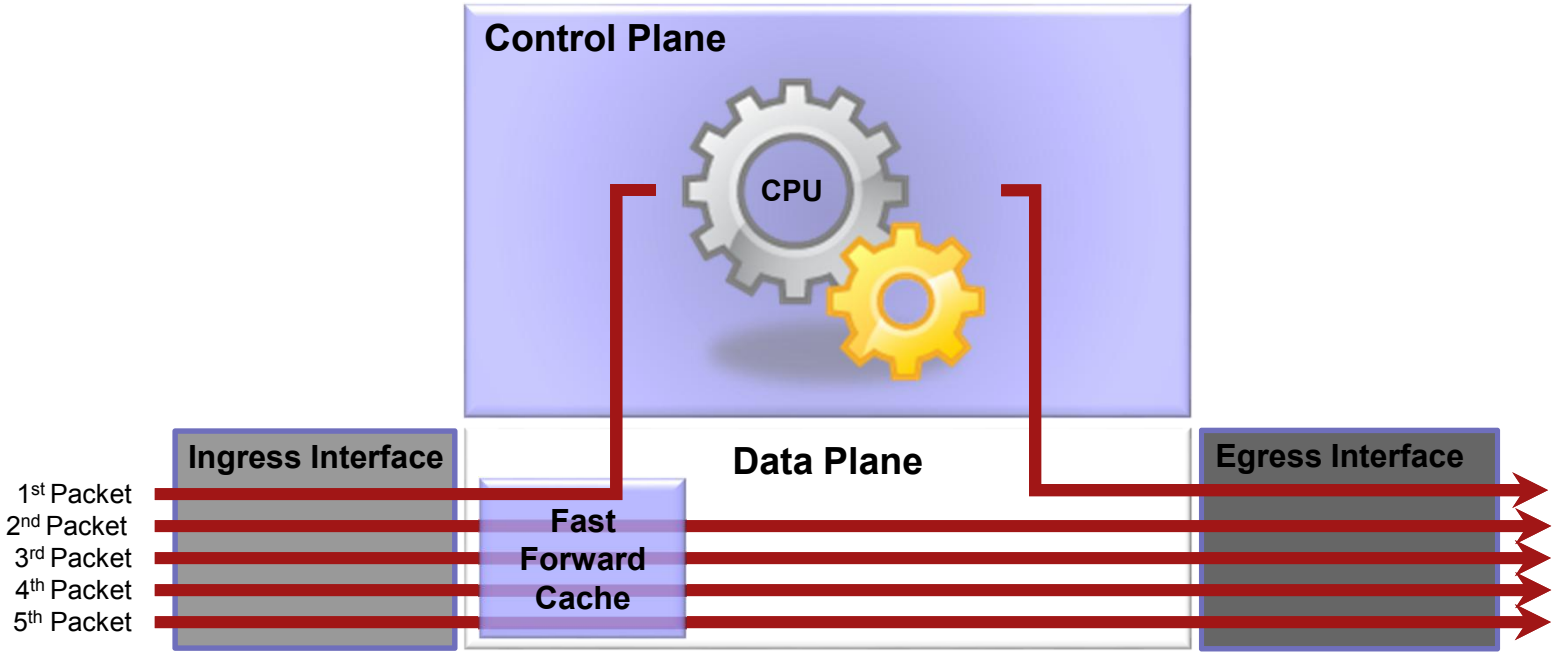
Process Switching

- Older method of switching where every packet is processed.



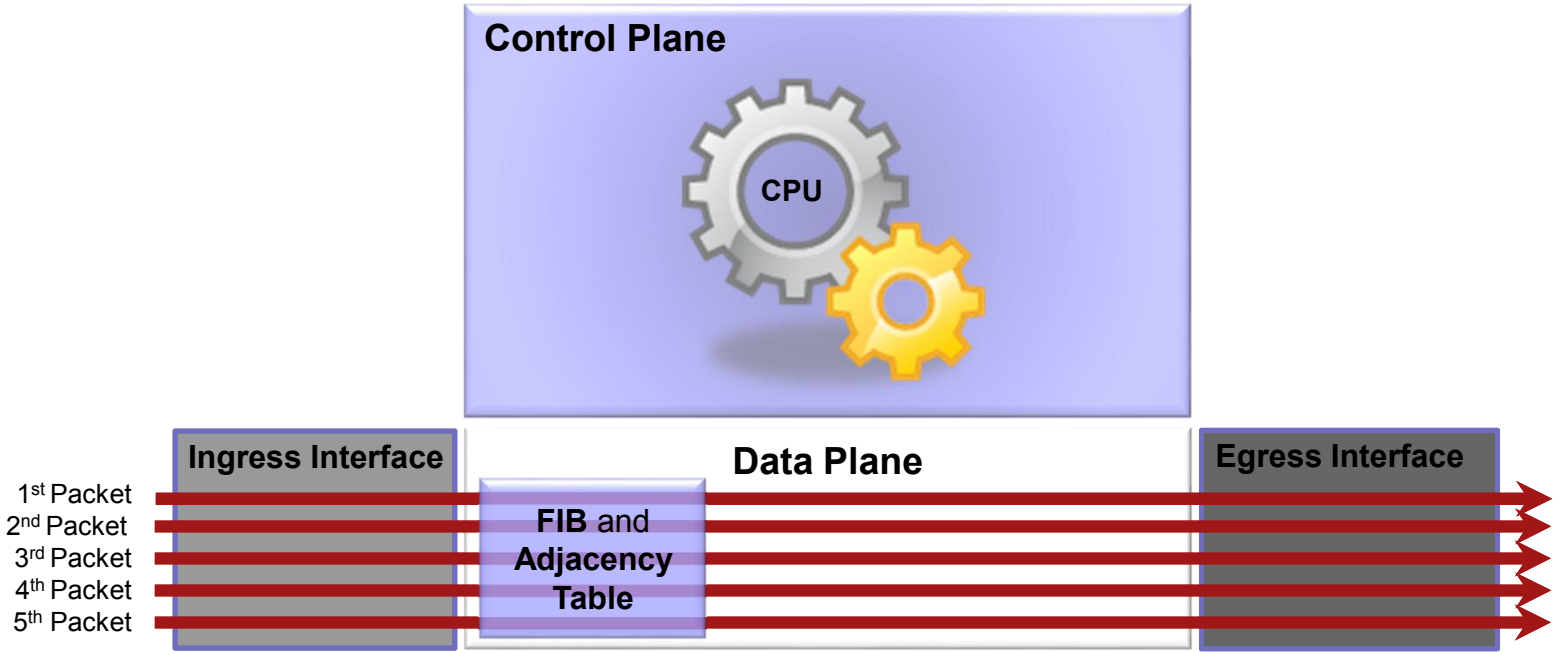
Fast Switching

- Better method of switching where it must process a packet once and then all subsequent packets from the same flow are fast forwarded out.



Cisco Express Forwarding

- Best packet switching method because a router / switch builds an adjacency table with Layer 2 information and then builds a FIB table based on the adjacency table and routing table.
  - It contains all possible routes scenarios.



Types of Layer 3 Interfaces

- The major types of configurable interfaces on Layer 3 switches:
  - **Switch Virtual Interface (SVI)**:
    - Logical interface on a switch associated with a virtual local area network (VLAN).
  - **Routed Port** :
    - Physical port on a Layer 3 switch configured to act as a router port.
    - Configure routed ports by putting the interface into Layer 3 mode with the **`no switchport`** interface configuration command.
  - **Layer 3 EtherChannel:**
    - Logical interface on a Cisco device associated with a bundle of routed ports.

Configuring a Routed Port on a Layer 3 Switch

```
Switch# conf t
Switch(config)# hostname S1
S1(config)#
S1(config)# interface fastEthernet 0/6
S1(config-if)# no switchport
S1(config-if)# ip address 192.168.200.1 255.255.255.0
S1(config-if)# no shut
S1(config-if)# end
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES unset  down                  down
FastEthernet0/2        unassigned      YES unset  down                  down
FastEthernet0/3        unassigned      YES unset  down                  down
FastEthernet0/4        unassigned      YES unset  down                  down
FastEthernet0/5        unassigned      YES unset  down                  down
FastEthernet0/6        192.168.200.1   YES manual up                    up
FastEthernet0/7        unassigned      YES unset  down                  down
FastEthernet0/8        unassigned      YES unset  down                  down
FastEthernet0/9        unassigned      YES unset  down                  down

<Output omitted>
```

CIS 81 Fundamentals of Networking
Chapter 5: Ethernet
Part 2 of 2

CCNA Introduction to Networking 5.0

Rick Graziani
Cabrillo College
graziani@cabrillo.edu

Fall 2013

Introduction to ARP

ARP Purpose

- Sending node needs a way to find the MAC address of the destination for a given Ethernet link

The ARP protocol provides two basic functions:

- Resolving IPv4 addresses to MAC addresses
- Maintaining a table of mappings

Next Week: Ethernet Part 2 - Switches

CIS 81 Fundamentals of Networking
Chapter 5: Ethernet
Part 1 of 2

CCNA Introduction to Networking 5.0

Rick Graziani
Cabrillo College
graziani@cabrillo.edu

Fall 2014