

## CASE STUDY

# 32524 LANs and Routing

(Autumn 2020)

### Due Date:

**IPv4 Addressing Milestone Submission (Tables A1, B and C):**

Before the start of your Week 7 lab class

**Individual Demonstration on Packet Tracer and viva:**

Week 10 lab class

## 1. Preamble

This Case Study provides an opportunity for students to practice their network design, implementation and troubleshooting skills gained mainly from studying the subject *LANs and Routing*.

The Case Study is organised to assist groups to complete the whole project **progressively** so that it can benefit students' learning experience. The *Scenario* describes your project in general terms and explains why the network is to be built. After that, the Case Study is broken into a number of tasks, each having detailed requirements guiding your group through several steps. It is important that you read and understand each requirement and complete tasks on a weekly basis as your study progresses.

## 2. Objectives and General Assessment Criteria

### Objectives

- Design hierarchical IPv4 and IPv6 addressing schemes to meet addressing requirements.
- Configure RIPv2 with simple route redistribution for IPv4
- Configure static, default static, summary static routing and floating static routing for IPv4.
- Configure floating default static routes for conditional redundancy at the ISP.
- Configure switching networks for management, VLANs, 802.1q trunking, inter-VLAN routing.
- Verify the functionality and troubleshoot the network when necessary.

### General Assessment Criteria

- Requirements met.
- Correctness of the design.
- Functionality of implementation.
- Justification of design and implementation
- Verification of functionality

## 3. Assessment

The Case Study is designed as a group activity, but it is mainly assessed individually, as:

### 1.1 Part A: IPv4 Addressing Milestone Submission (group submission, around 20%)

Each group as a team is required to submit their IPv4 **subnetting and addressing scheme**, i.e., **Tables A1, B and C** on Page 9 of this book, to your lab instructor via Email before the beginning of your **Week 7** lab. Feedback is expected to be given at the end of that class.

### 1.2 Part B: Packet Tracer based Demonstration and Oral Q&A (individual, around 80%)

During your scheduled lab session in Week 10, **individual** students will be required to implement, from scratch, the network that their group have designed on Packet Tracer, to demonstrate that their network meets all the requirements specified in this Case Study book. The network and its functionality will then be graded on site through testing and oral Q&A. Please refer to **Section 7 on Page 8** of this Case Study book for more details.

#### 4. Suggestions and General Requirements for Case Study Completion

It is expected that each student will spend in total **around 6 hours on this Case Study**.

It is suggested that Groups plan and complete the Case Study on a weekly basis, as the corresponding topics are covered in class (e.g., as suggested below) so that all tasks can be completed properly and students receive most benefit.

**Week 6:** complete Task One – IPv4 Subnetting (IPv4 Addressing due)

**Week 8:** complete Task Two – Static and RIP Routing

**Week 9:** complete Task Three – Switching

**Week 10 Lab:** Lab Demonstration

Leaving the Case Study to the very last week or day(s) will result in a poorly designed network and little benefit to your final assessments.

#### 5. Scenario

This Case Study presents a scenario in which a training organisation, the Arcadia Institute of Technology (AIT), has recently taken the ownership of another training centre and relocated its main site to the centre of the city. Hence AIT wishes to re-design and implement its whole network. AIT has hired your group as their ICT consultants to design and implement a new network for them. The solution will be evaluated by a demonstration of a prototype network using Packet Tracer.

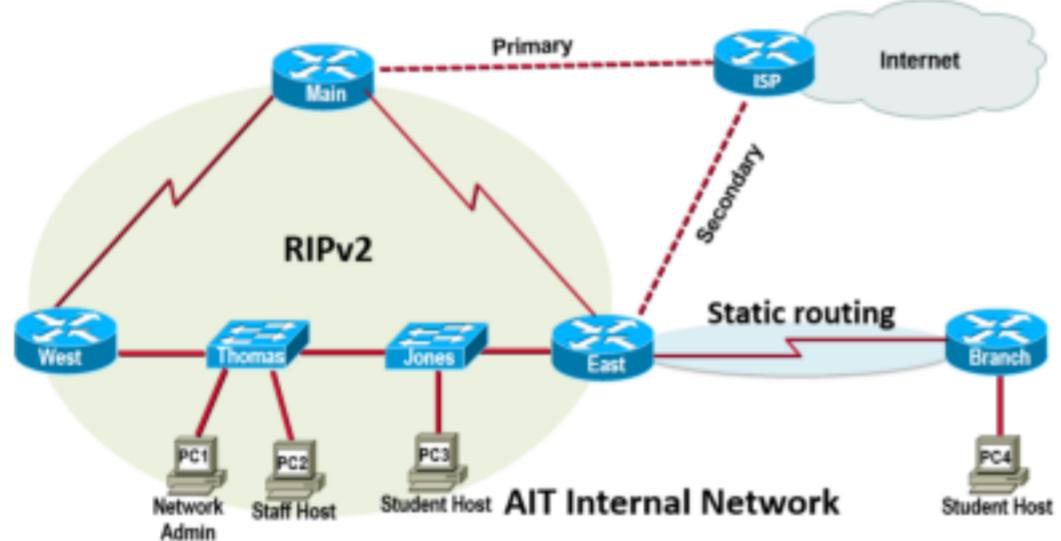
AIT is implementing an overall dual stack network, comprised of various networks. A partial logical Topology Diagram has been provided (see Fig. 1). The task is to design and implement the networks at the four sites (including a simulated ISP). AIT would like to see a prototype of the network built, before it is fully implemented, to verify that it will meet AIT's needs.

In order to help your group organise this Case Study, the scenario has been broken into **three tasks**. Detailed requirements are listed for each task. When all of the tasks are completed a prototype of the network is expected to be implemented using Packet Tracer to demonstrate its functionality..

As shown in Fig. 1, AIT for which you are to design a network, has locations in two campuses:

- On the **City Campus** there are three major sites in the **Main** building, **West Tower**, and **East Tower**, where the Main Building connects to the West Tower and East Tower sites using Leased Line serial connections.
  - The **West Tower** site is mainly for the AIT Teaching and Learning division. All user groups will each have users located in both of the buildings, i.e., Thomas and Jones. Because of the size and complexity of LANs, the company wants to create *VLANs* to control broadcasts, enhance security and logically organise user groups.
  - If the link from Thomas and Jones buildings loses its connection to West or to Main, all of the switching network traffic can exit from the alternative gateway via the **East Tower** router.
- The **Branch Campus** is located in a different suburb and, because of cost, will be connected via a leased line serial connection

AIT's internal network has **two exit links** for access to the Internet and external services. These exit links are on the City campus via the two border routers Main and East. The link from Main is the primary path and the secondary path through the East will only become used when the primary Main-ISP link becomes unavailable.



**Fig. 1. Basic network topology**

AIT has agreed to use **RIP version 2** for its internal networks, except for the Branch site, which will be routed using static routing. AIT also wants to use private IPv4 addresses for the entire IPv4 network. NAT for IPv4 may be implemented on the two border routers Main and East for all traffic leaving the company's network, but this is not compulsory for demonstrating your network.

Although private addresses will be used, the company appreciates efficiency and address conservation in their design. To minimise wasted address spaces, they have requested CIDR and hierarchical VLSM to be used whenever appropriate.

**IPv6** has been considered and at this stage, **dual-stacking** will be implemented everywhere to support both IPv4 and IPv6.

## 6. Requirements in Tasks

## Task One: Addressing the Network

### The ISP links:

The ISP has allocated **one of the following public IPv4 address spaces for your group**, which will need to be broken into two /30 address spaces for each of the two ISP links:

- Group A: **209.165.199.64/29**
- Group B: **209.165.199.72/29**
- Group C: **209.165.199.80/29**
- Group D: **209.165.199.88/29**
- Group E: **209.165.199.96/29**
- Group F: **209.165.199.104/29**

For IPv6, **2001:50:80:120::/64** and **2001:50:80:121::/64** are used to address the two ISP links.

### The Internal Network:

As part of the network redesign, the AIT has allocated **one of the following private address spaces for your group** and **2001:DB8:CA5E::/52** for addressing the internal network:

- Group A: **10.0.0.0/19**
- Group B: **10.0.32.0/19**
- Group C: **10.0.64.0/19**
- Group D: **10.0.96.0/19**
- Group E: **10.0.128.0/19**
- Group F: **10.0.160.0/19**

(PS. For demonstration, routing to private addresses is sufficient and NAT is not required.)

The expected numbers of users for each of the user groups (each on their unique IP networks) are:

For the **West** switching network (these will be implemented using *VLANs*):

- 200 hosts for Staff
- 3000 hosts for Students
- 500 hosts for Visitors

On the **Branch Campus site**:

- 600 hosts for Students (as shown in the Topology Diagram)
- 40 hosts for Staff (this will be simulated with a loopback interface)

The AIT requires that:

- The use of **hierarchical VLSM** design to maximise the use of IPv4 addresses, and account for CIDR and route aggregation between the main sites.
- All networking devices (including switches) must have IPv4 addresses** and the PC hosts' **gateways** will use the **first** usable address(es) in each subnet.
- Each of the ISP links will be allocated a **subnet mask of /30** for IPv4.
- All IPv6 addressed networks will have a network prefix of /64.
- The **Management VLAN** for the West switching network will have **two extra hosts** (one of which is referred to as the "Admin Host" as shown in the Topology Diagram) for network administration usage. The network administration hosts will have the **last usable** addresses on the Management VLAN subnet at the West site.

At this stage, AIT agrees that it is sufficient to assign all hosts with an IPv4 address statically.

### Milestone Submission: Tables A1, B and C

- 1) IPv4 Network subnetting **Table A1**, which shows possible subnets that meet the design requirements; Subnets that are not used are to be clearly identified in each table.
- 2) Detailed IPv4 addressing tables (**Tables B and C**) showing all networking devices' names and their interface details.

**Discussion Questions:** Consider how you do subnetting so as to meet each of the requirements.

## Task Two: Routing the Network

### Routing to and from ISP

The AIT network has purchased **two ISP links** to access the Internet and external services, i.e., via the Main and East router respectively. AIT's policy requires that the back-up East-ISP link is only used when the primary Main-ISP link becomes unavailable. Since the ISP also serves many other customers, routing to and from ISP will use only static routing, and a standard static route should be used on the ISP to only forward traffic to the AIT internal network when needed.

When correctly implemented, all hosts within the AIT network (incl. the Branch site) must be able to get to all external addresses, via the Main-ISP link, or the East-ISP link when the Main-ISP link is unavailable, in both directions.

Note that, for the demonstration purpose, use the loopback address, i.e., **11.11.11.11/32** for IPv4 and **2001:11:11:11::11/128** for IPv6, on ISP to simulate the Internet. Also, NAT at the border routers may be considered at a later stage.

### Routing the Internal Network

#### IPv4 Routing:

- AIT's policy is that RIP routing will be used internally for its IPv4 networks.
- The exception is that routing to and from the Branch site, where AIT wishes to use static routing because Branch is a stub network. Note that this static route will need to be propagated to all other internal routers.

#### IPv6 Routing:

- All IPv6 routing will use static, default, summary and/or floating static routing.

Your design and implementation of static routing should be in a most efficient manner.

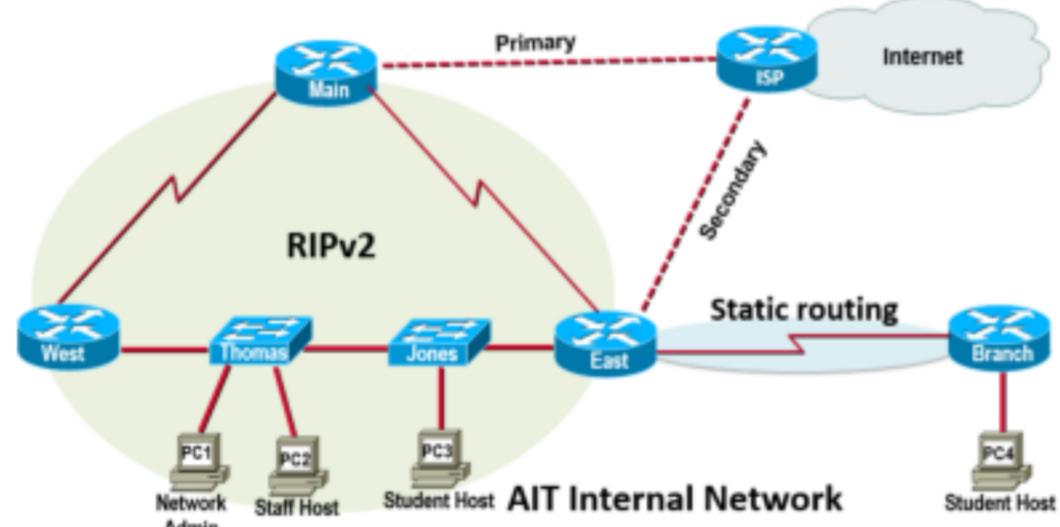


Fig. 2. Routing the network dynamically and statically

### Discussion Questions:

Consider how you **implement** and **verify** the following functions:

- 1) RIPv2 routing and static routing for the internal networks (including the networks at the Branch site).
- 2) Static routing and failover routing via the two ISP links.
- 3) Routing when the Thomas-West link fails.

### Task Three: Switching Network at the West Site

Because of the size and complexity of LANs at the **City** site, AIT wants to use VLAN technologies to control broadcasts, enhance security and logically organize its user groups. 802.1Q trunk-based Inter-VLAN routing for both IPv4 will have to be implemented to advertise all VLAN networks.

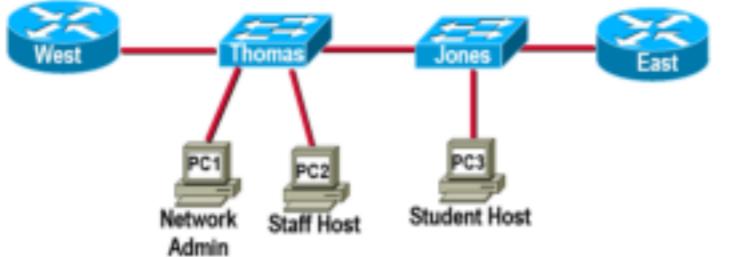


Fig. 3. The switching networks at the West Tower site.

#### The switching networks at the City site:

- Create the following VLAN IDs and Names for the required networks:
  - VLAN 10 – Staff
  - VLAN 20 – Students
  - VLAN 30 – Visitors
- All user groups will each have employees located in two adjoining buildings, i.e., connected via **Thomas** and **Jones** switches. For the purpose of demonstrating network functionality, allocate **five** ports to each *user* VLAN on each switch.
- Create **VLAN 77** as the Management VLAN and allocate **1** port to this VLAN on each switch. Use **VLAN 139** as the native VLAN ID.
- Do NOT allow traffic of the default VLAN 1 and unknown VLANs onto the trunk link(s).

#### Discussion Questions:

Consider, in detail, how you **implement** and **verify** the following functions:

- 1) Creating VLANs and assigning ports.
- 2) SVI configuration and verification.
- 3) Inter-VLAN routing configuration and verification.

## 7. Lab Demonstration

AIT now wants a demonstration of the complete network. To do this, you need to set up the network that you have designed and configure all devices Packet Tracer to demonstrate that your network functions as required.

The demonstration requires **basic settings on all routers and switches** including hostname, local passwords, MOTD banner, management address and SSH access, detailed as follows:

- Configure basic device settings:
  - Configure **hostnames** as per the partial Topology Diagram.
  - Configure password **cisco** for console connections.
  - Encrypt the privileged EXEC mode using password **class**.
  - Disable Domain Name Server (**DNS lookup**).
  - Enable **logging synchronous** for console connections and all virtual terminal lines.
  - Configure a Message of the Day (**MOTD banner**) warning against unauthorised access.
- Configure the interfaces of routers and hosts as per the Topology Diagram and your Addressing Tables B&C.
- Configure routing on all routers consistent with your design.
- Configure VLANs according to your Switch and VLAN tables.
- Configure Management VLAN SVI interface on the switch for TCP/IPv4 connectivity.
- Configure the following host PCs based on your addressing.
  - **PC1** as the network Admin Host on Management VLAN on the **Thomas** switch.
  - **PC2** as the Staff Host on the **Thomas** switch.
  - **PC3** as Student Host on the **Jones** switch.
  - **PC4** as the Student Host on the **Branch** router.

PS. AIT has a plan to implement DHCPv4 service and using ACLs to control network traffic. At this stage, statically assigning IPv4 addresses is sufficient for demonstration purpose.

AIT requires the following network verification to be assessed:

- Verification of the devices' basic configuration
- Verification of the correctness and functionality of the interface configuration
- Verification of dynamic routing for IPv4.
- Verification of static routing for both IPv4 and IPv6.
- Verification of the VLANs and inter-VLAN routing.
- Verifying end-to-end connectivity of all hosts to each other and the ISP's loopback addresses.

**Sample Partial Tables:****Table A1\*** - IPv4 Subnetting Table

Subnet Number	Subnet Address	Subnet Mask	Hosts Required	Maximum Hosts in Subnet	In Use (Yes or No)	Network Name

**Table A2** IPv6 Subnetting Table

Subnet Number	Subnet Address	Subnet Mask	Hosts Required	Maximum Hosts in Subnet	In Use (Yes or No)	Network Name

**Table B\*** Device Interface IP Addressing Table

Device	Interface	IPv4 address	Subnet Mask	IPv6 Address/Prefix Length
ISP				
Jones	Management (& Native) VLAN			N/A

**Table C\*** Host Addressing Table

Host	IPv4 Address	Subnet Mask	Gateway	IPv6 Address/Prefix Length

**Table D** Switch Table

Switch Name:

Switch Management IP Address:

Interface type & Port Number	Description of Purpose	Port Bandwidth	Network Name	Subnet Address	Subnet Mask	VLAN ID & Name	Switch Port Mode	Layer 2 Encapsulation

**Table E** VLAN Table

Switch Name	Number of Ports	Location	IP Address	Gateway	VLAN ID & Name



# Module 9: Address Resolution

Introduction to Networks v7.0  
(ITN)



# Module Objectives

**Module Title:** Address Resolution

**Module Objective:** Explain how ARP and ND enable communication on a network.

Topic Title	Topic Objective
MAC and IP	Compare the roles of the MAC address and the IP address.
ARP	Describe the purpose of ARP.
Neighbor Discovery	Describe the operation of IPv6 neighbor discovery.



# 9.1 MAC and IP

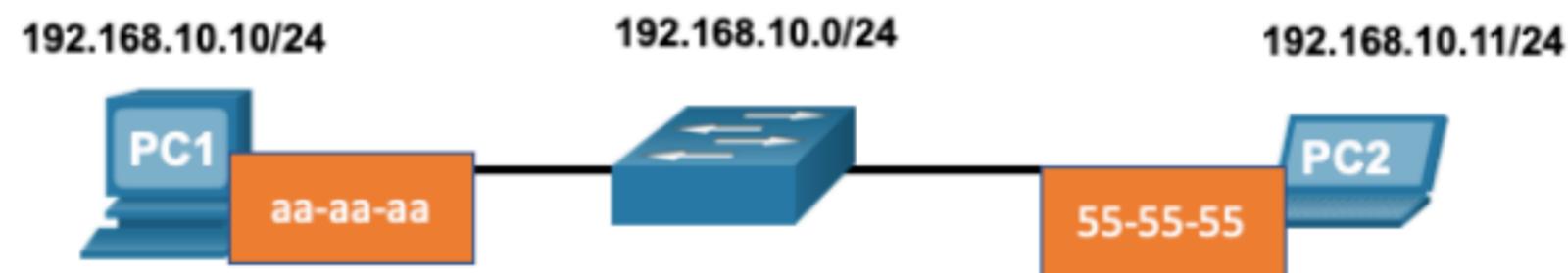


## MAC and IP Destination on Same Network

There are two primary addresses assigned to a device on an Ethernet LAN:

- **Layer 2 physical address (the MAC address)** – Used for NIC to NIC communications on the same Ethernet network.
- **Layer 3 logical address (the IP address)** – Used to send the packet from the source device to the destination device.

Layer 2 addresses are used to deliver frames from one NIC to another NIC on the same network. If a destination IP address is on the same network, the destination MAC address will be that of the destination device.

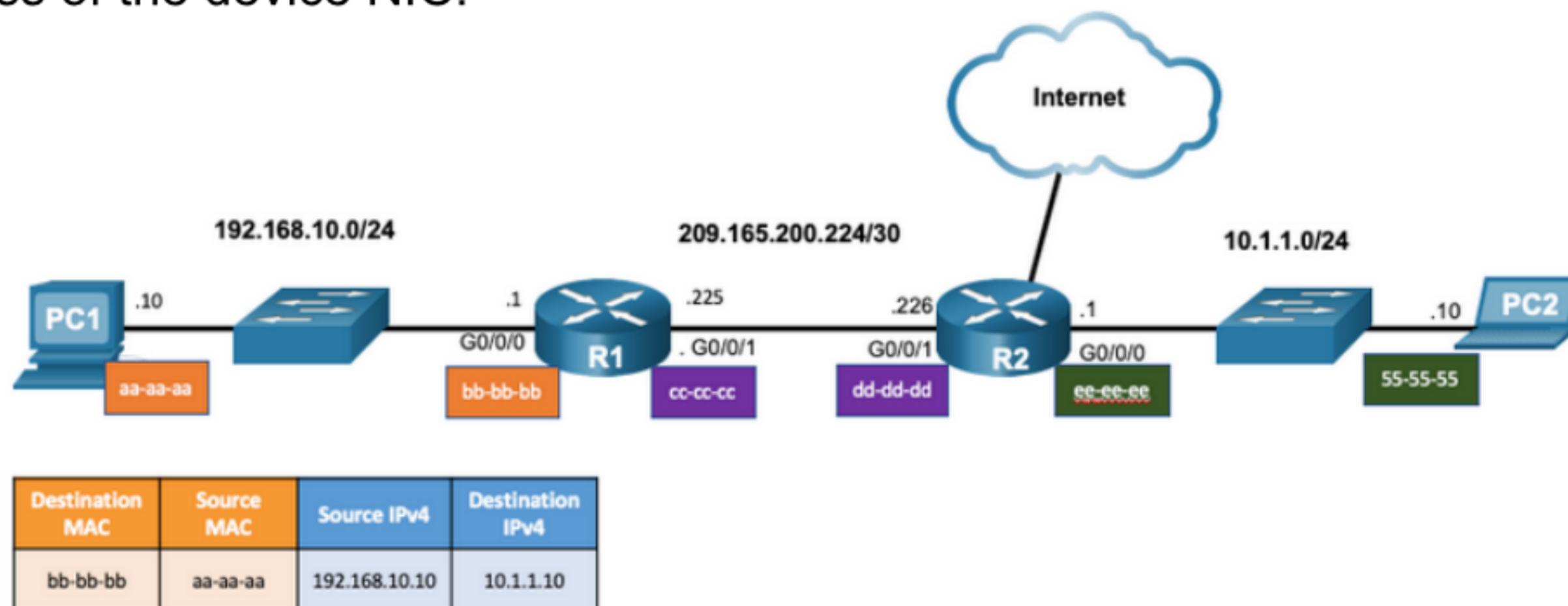


Destination MAC	Source MAC	Source IPv4	Destination IPv4
55-55-55	aa-aa-aa	192.168.10.10	192.168.10.11

# MAC and IP Destination on Remote Network

When the destination IP address is on a remote network, the destination MAC address is that of the default gateway.

- ARP is used by IPv4 to associate the IPv4 address of a device with the MAC address of the device NIC.
- ICMPv6 is used by IPv6 to associate the IPv6 address of a device with the MAC address of the device NIC.



MAC and IP

## Packet Tracer – Identify MAC and IP Addresses

In this Packet Tracer, you will complete the following objectives:

- Gather PDU Information for Local Network Communication
- Gather PDU Information for Remote Network Communication



# 9.2 ARP



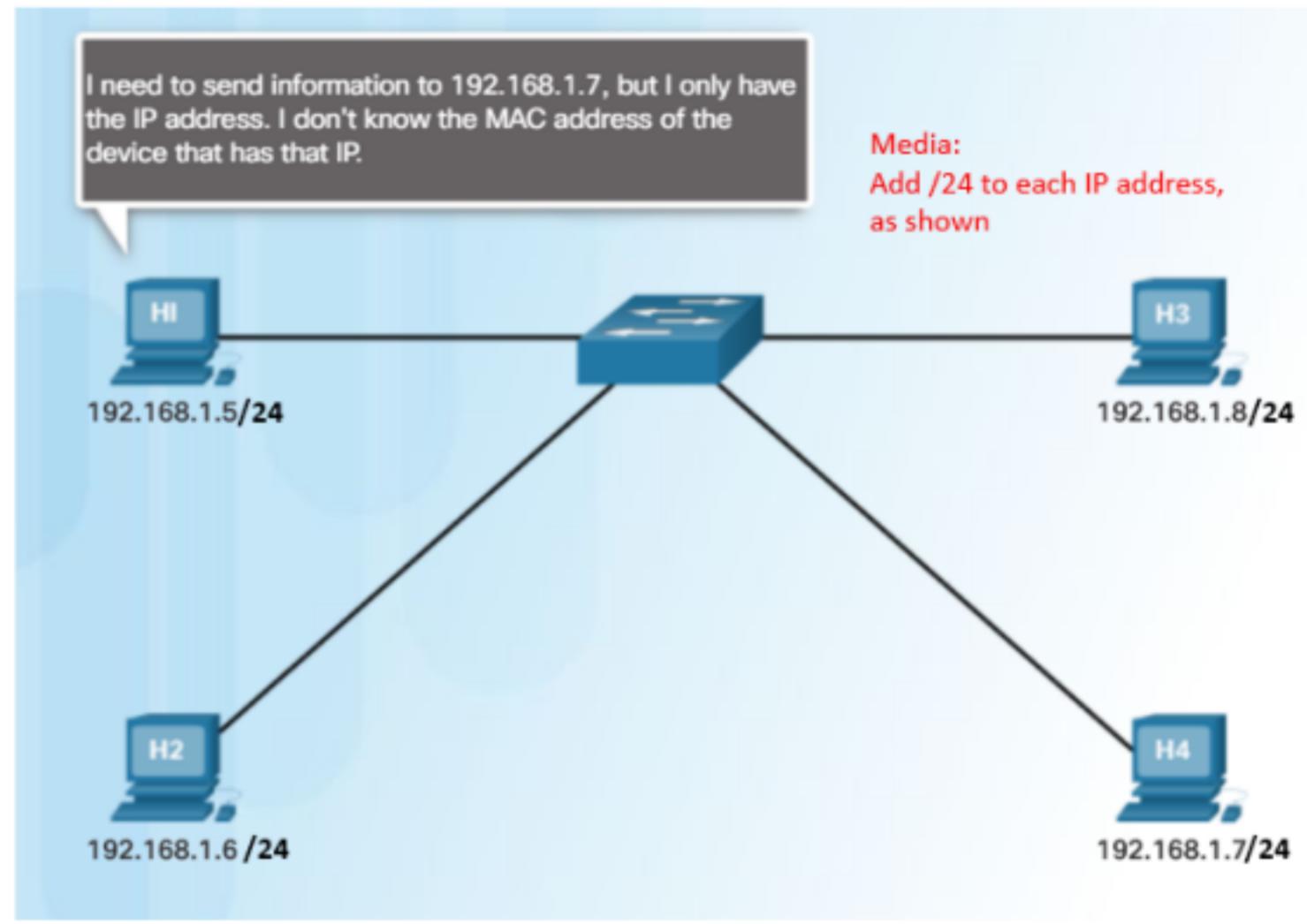
# ARP

## ARP Overview

A device uses ARP to determine the destination MAC address of a local device when it knows its IPv4 address.

ARP provides two basic functions:

- Resolving IPv4 addresses to MAC addresses
- Maintaining an ARP table of IPv4 to MAC address mappings



## ARP Functions

To send a frame, a device will search its ARP table for a destination IPv4 address and a corresponding MAC address.

- If the packet's destination IPv4 address is on the same network, the device will search the ARP table for the destination IPv4 address.
- If the destination IPv4 address is on a different network, the device will search the ARP table for the IPv4 address of the default gateway.
- If the device locates the IPv4 address, its corresponding MAC address is used as the destination MAC address in the frame.
- If there is no ARP table entry is found, then the device sends an ARP request.

# ARP Video - ARP Request

This video will cover an ARP request for a MAC address.



ARP

## Video – ARP Operation - ARP Reply

This video will cover an ARP reply in response to an ARP request.



ARP

## Video - ARP Role in Remote Communications

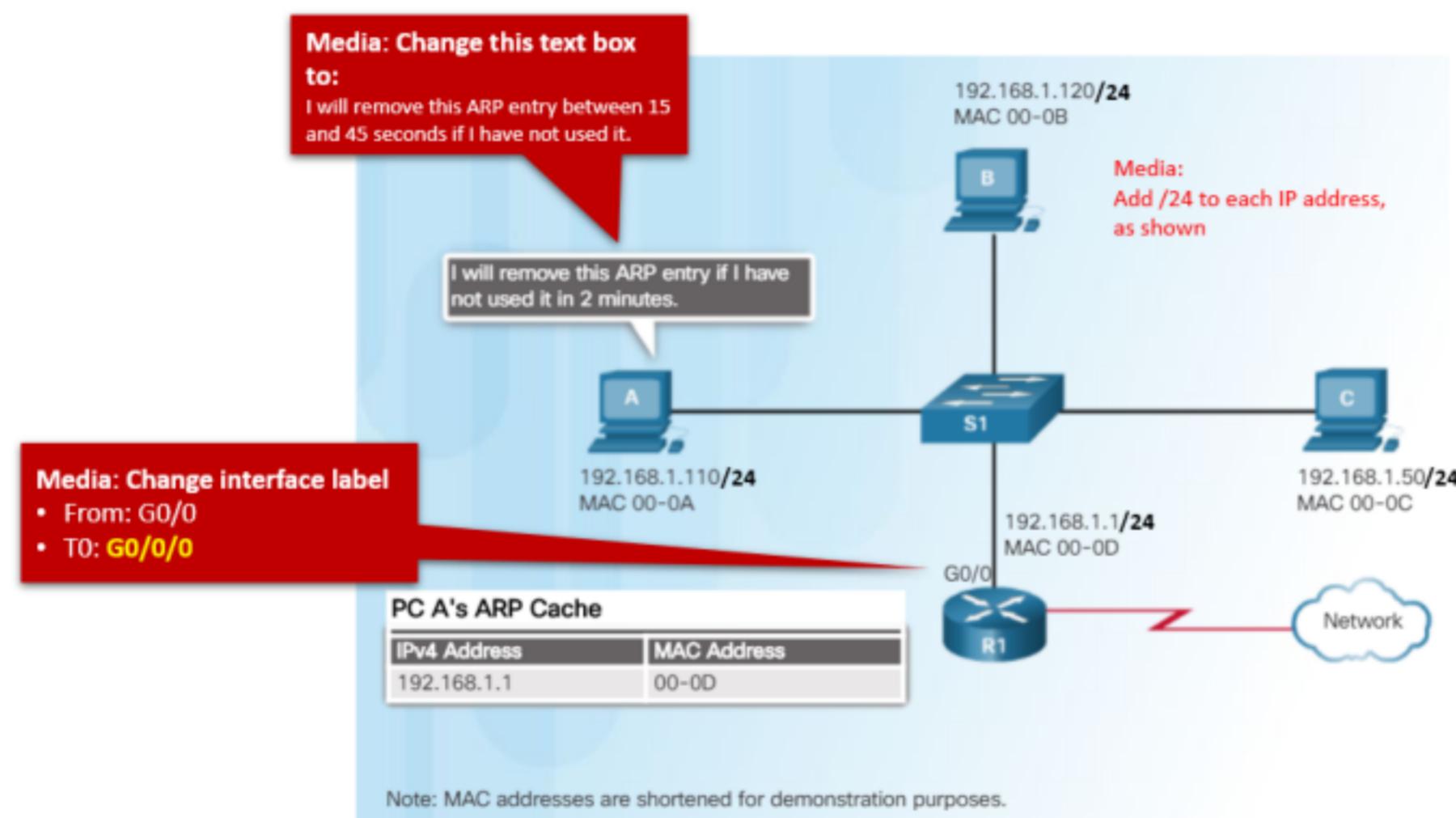
This video will cover how an ARP request will provide a host the MAC address of the default gateway.



## ARP

# Removing Entries from an ARP Table

- Entries in the ARP table are not permanent and are removed when an ARP cache timer expires after a specified period of time.
- The duration of the ARP cache timer differs depending on the operating system.
- ARP table entries can also be removed manually by the administrator.



## ARP

# ARP Tables on Networking Devices

- The **show ip arp** command displays the ARP table on a Cisco router.
- The **arp -a** command displays the ARP table on a Windows 10 PC.

```
R1# show ip arp
Protocol Address          Age (min)  Hardware Addr   Type      Interface
Internet 192.168.10.1        -         a0e0.af0d.e140  ARPA    GigabitEthernet0/0/0
```

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

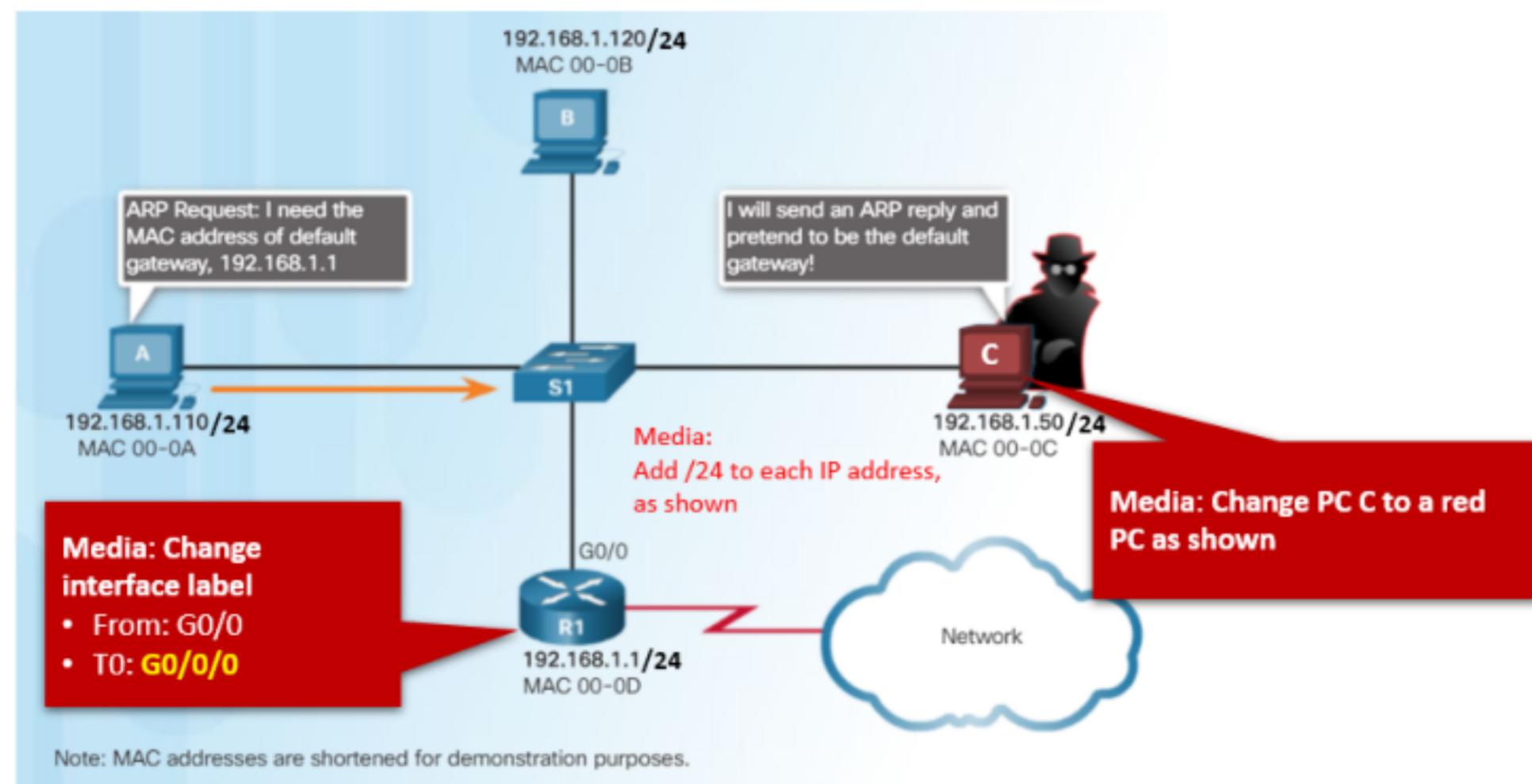
Interface: 192.168.1.124 --- 0x10
  Internet Address          Physical Address      Type
  192.168.1.1                c8-d7-19-cc-a0-86  dynamic
  192.168.1.101              08-3e-0c-f5-f7-77  dynamic
```



## ARP

# ARP Issues – ARP Broadcasting and ARP Spoofing

- ARP requests are received and processed by every device on the local network.
- Excessive ARP broadcasts can cause some reduction in performance.
- ARP replies can be spoofed by a threat actor to perform an ARP poisoning attack.
- Enterprise level switches include mitigation techniques to protect against ARP attacks.



ARP

## Packet Tracer – Examine the ARP Table

In this Packet Tracer, you will complete the following objectives:

- Examine an ARP Request
- Examine a Switch MAC Address Table
- Examine the ARP Process in Remote Communications



# 9.3 IPv6 Neighbor Discovery



IPv6 Neighbor Discovery

## Video – IPv6 Neighbor Discovery

This video will explain the process of how IPv6 performs address resolution using ICMPv6 neighbor solicitation and neighbor advertisement messages.



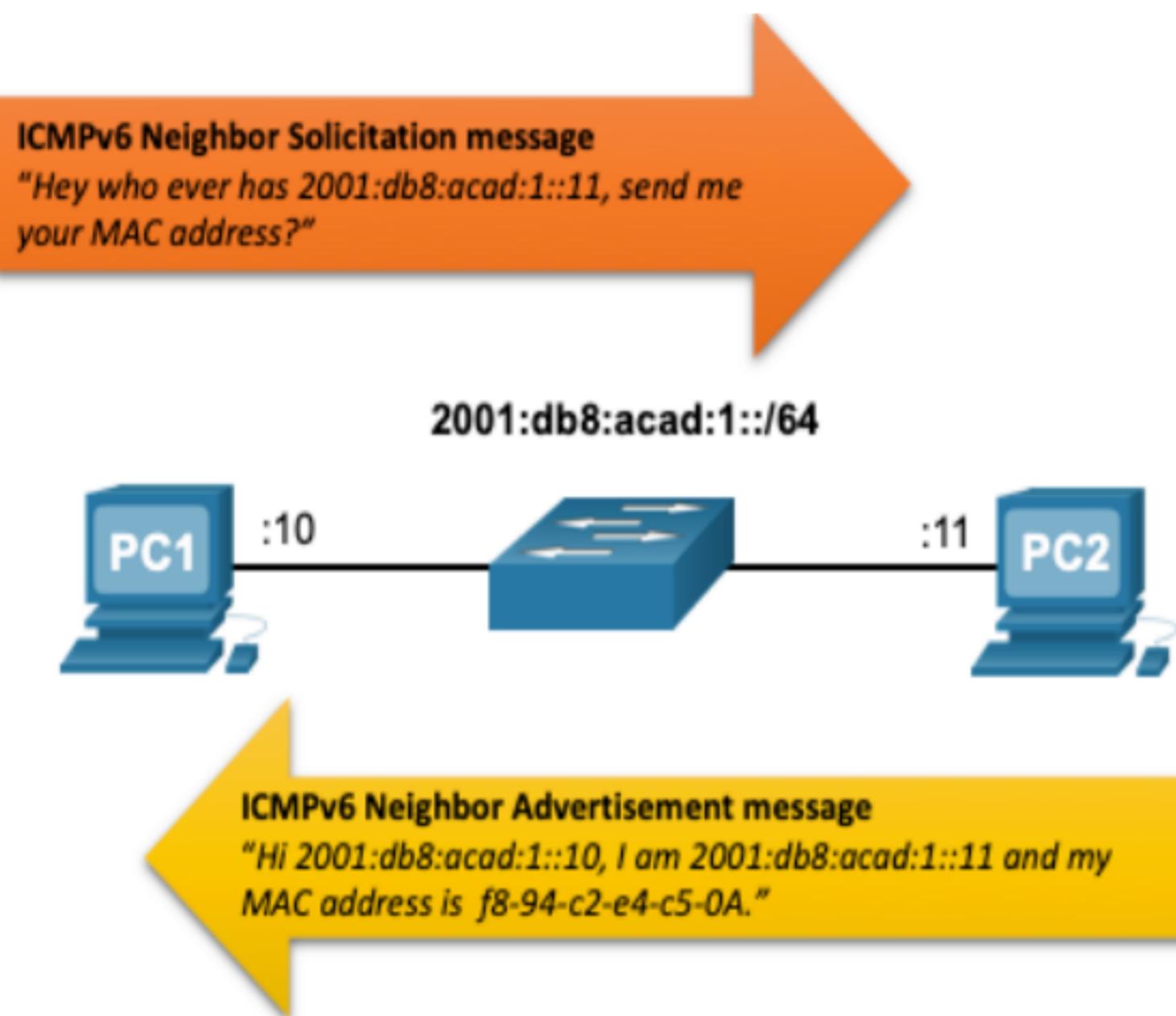
## IPv6 Neighbor Discovery Messages

IPv6 Neighbor Discovery (ND) protocol provides:

- Address resolution
- Router discovery
- Redirection services
- ICMPv6 Neighbor Solicitation (NS) and Neighbor Advertisement (NA) messages are used for device-to-device messaging such as address resolution.
- ICMPv6 Router Solicitation (RS) and Router Advertisement (RA) messages are used for messaging between devices and routers for router discovery.
- ICMPv6 redirect messages are used by routers for better next-hop selection.

## IPv6 Neighbor Discovery

# IPv6 Neighbor Discovery – Address Resolution



- IPv6 devices use ND to resolve the MAC address of a known IPv6 address.
- ICMPv6 Neighbor Solicitation messages are sent using special Ethernet and IPv6 multicast addresses.

## Packet Tracer – IPv6 Neighbor Discovery

In this Packet Tracer, you will complete the following objectives:

- Part 1: IPv6 Neighbor Discovery Local Network
- Part 2: IPv6 Neighbor discovery Remote Network

# 9.4 Module Practice and Quiz



## Module Practice and Quiz

# What did I learn in this module?

- Layer 2 physical addresses (i.e., Ethernet MAC addresses) are used to deliver the data link frame with the encapsulated IP packet from one NIC to another NIC on the same network.
- If the destination IP address is on the same network, the destination MAC address will be that of the destination device.
- When the destination IP address (IPv4 or IPv6) is on a remote network, the destination MAC address will be the address of the host default gateway (i.e., the router interface).
- An IPv4 device uses ARP to determine the destination MAC address of a local device when it knows its IPv4 address.
- ARP provides two basic functions: resolving IPv4 addresses to MAC addresses and maintaining a table of IPv4 to MAC address mappings.
- After the ARP reply is received, the device will add the IPv4 address and the corresponding MAC address to its ARP table.
- For each device, an ARP cache timer removes ARP entries that have not been used for a specified period of time.
- IPv6 does not use ARP, it uses the ND protocol to resolve MAC addresses.
- An IPv6 device uses ICMPv6 Neighbor Discovery to determine the destination MAC address of a local device when it knows its IPv6 address.



## New Terms and Commands

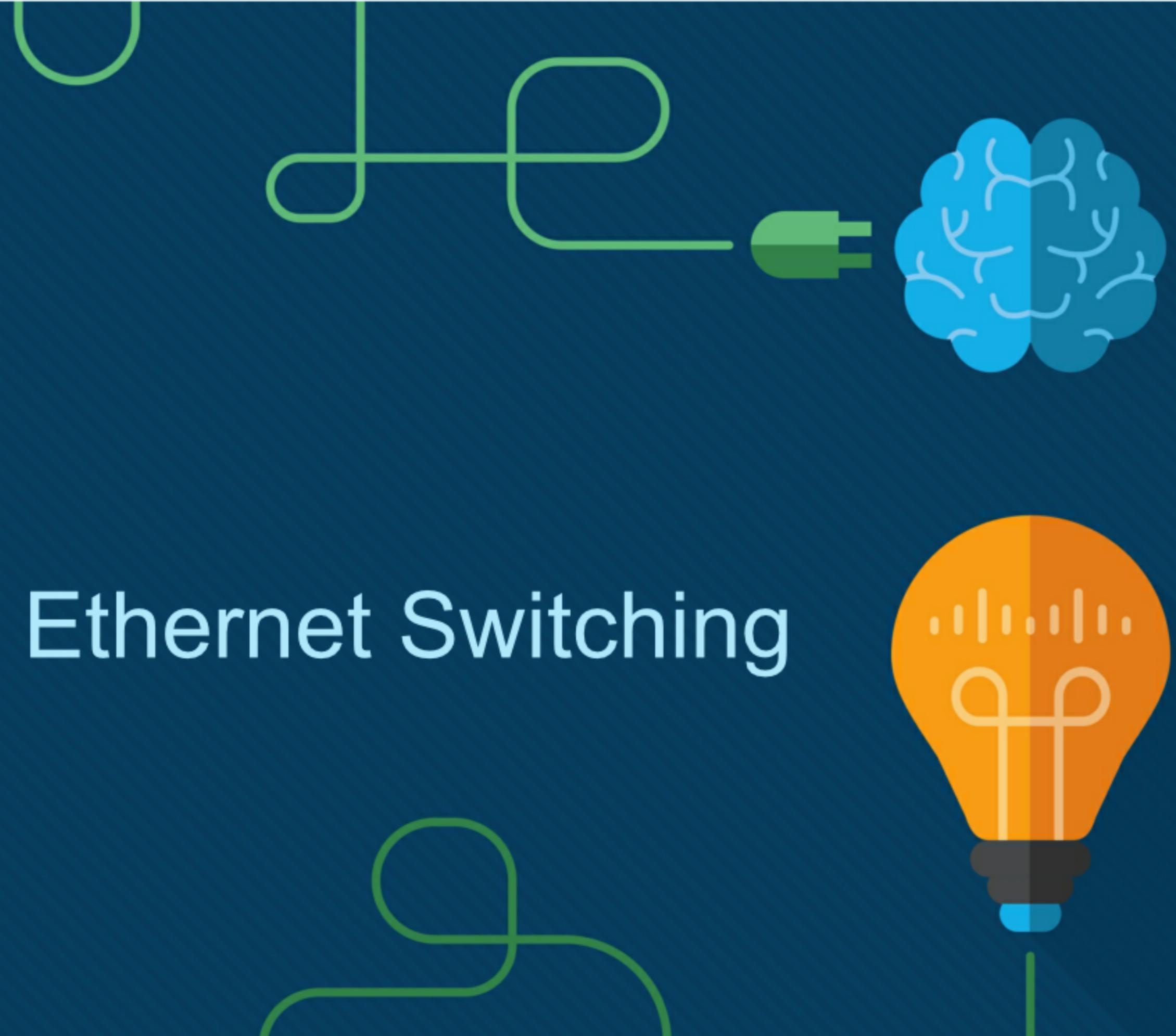
- Address Resolution Protocol (ARP)
- ARP table
- show ip arp
- arpr -a
- ICMPv6 Neighbor Discovery protocol (ND)
- ICMPv6 Neighbor Solicitation (NS)  
message
- ICMPv6 Neighbor Advertisement (NA)  
message
- ICMPv6 Router Solicitation (RS) message
- ICMPv6 Router Advertisement (RA)  
message
- ICMPv6 Redirect Message





# Module 7: Ethernet Switching

Introduction to Networks v7.0  
(ITN)



# Module Objectives

**Module Title:** Ethernet Switching

**Module Objective:** Explain how Ethernet works in a switched network.

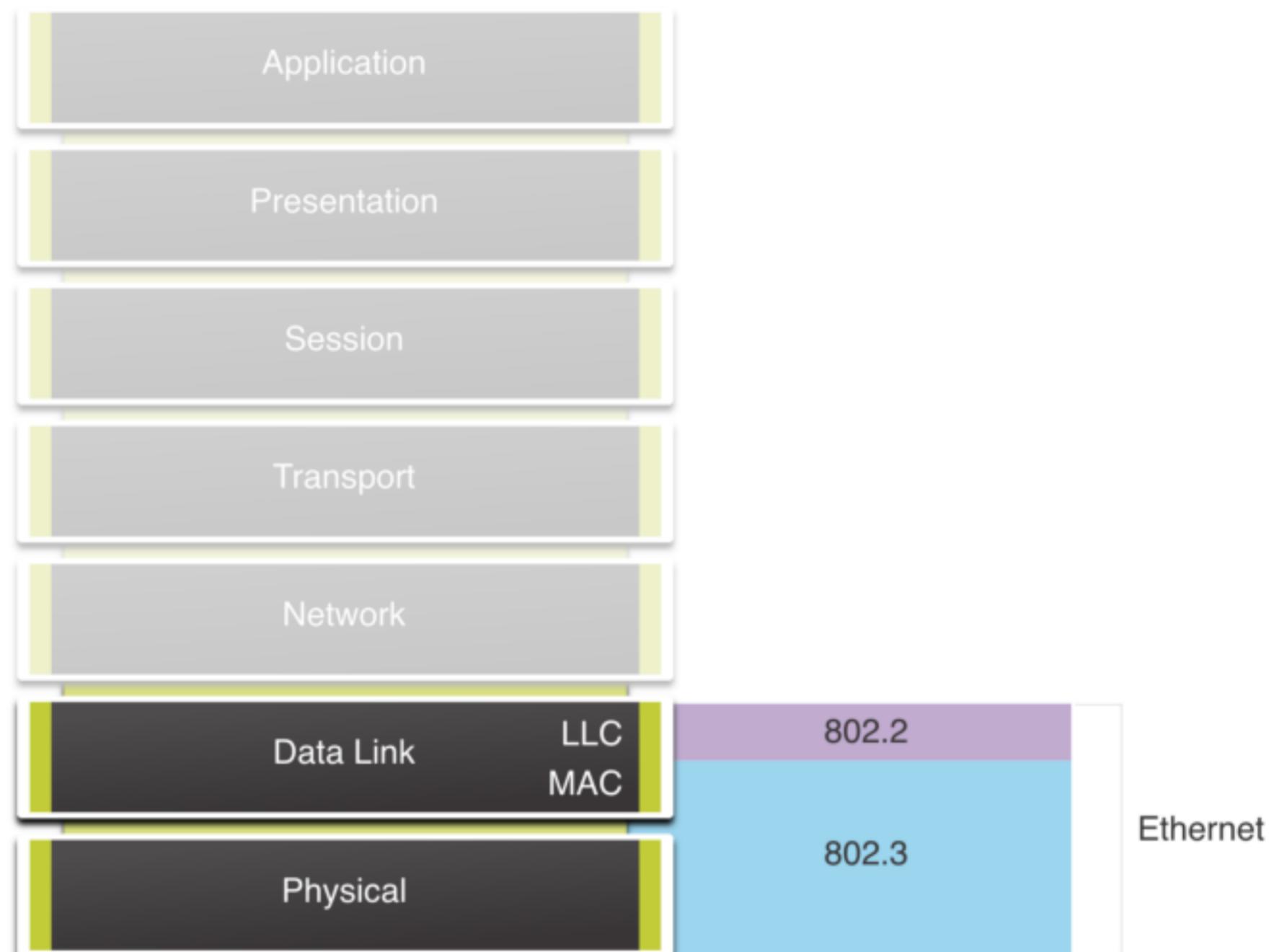
Topic Title	Topic Objective
Ethernet Frame	Explain how the Ethernet sublayers are related to the frame fields.
Ethernet MAC Address	Describe the Ethernet MAC address.
The MAC Address Table	Explain how a switch builds its MAC address table and forwards frames.
Switch Speeds and Forwarding Methods	Describe switch forwarding methods and port settings available on Layer 2 switch ports.

# 7.1 Ethernet Frames



## Ethernet Frames Ethernet Encapsulation

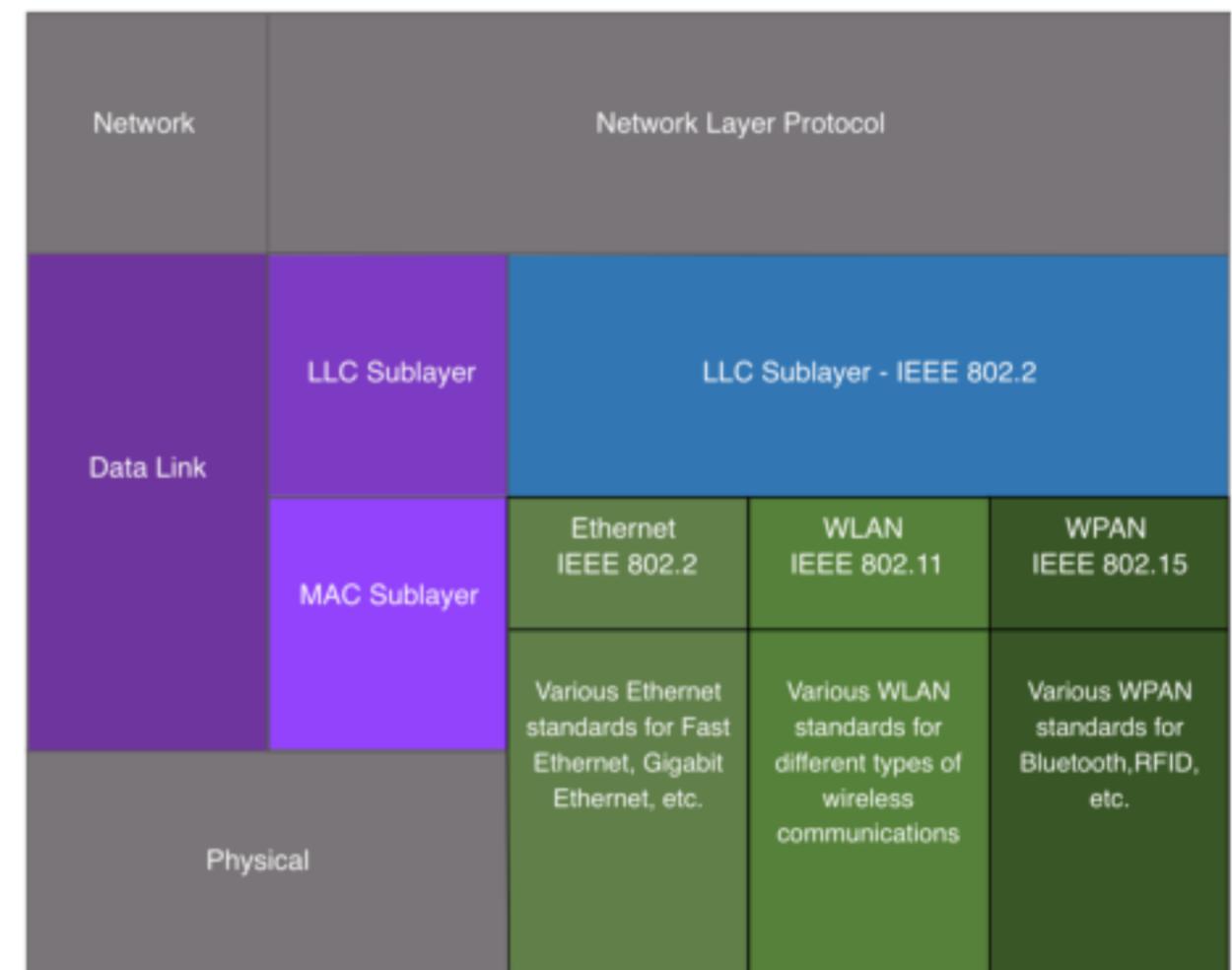
- Ethernet operates in the data link layer and the physical layer.
- It is a family of networking technologies defined in the IEEE 802.2 and 802.3 standards.



# Ethernet Frames Data Link Sublayers

The 802 LAN/MAN standards, including Ethernet, use two separate sublayers of the data link layer to operate:

- **LLC Sublayer:** (IEEE 802.2) Places information in the frame to identify which network layer protocol is used for the frame.
- **MAC Sublayer:** (IEEE 802.3, 802.11, or 802.15) Responsible for data encapsulation and media access control, and provides data link layer addressing.



# Ethernet Frames **MAC Sublayer**

The MAC sublayer is responsible for data encapsulation and accessing the media.

## Data Encapsulation

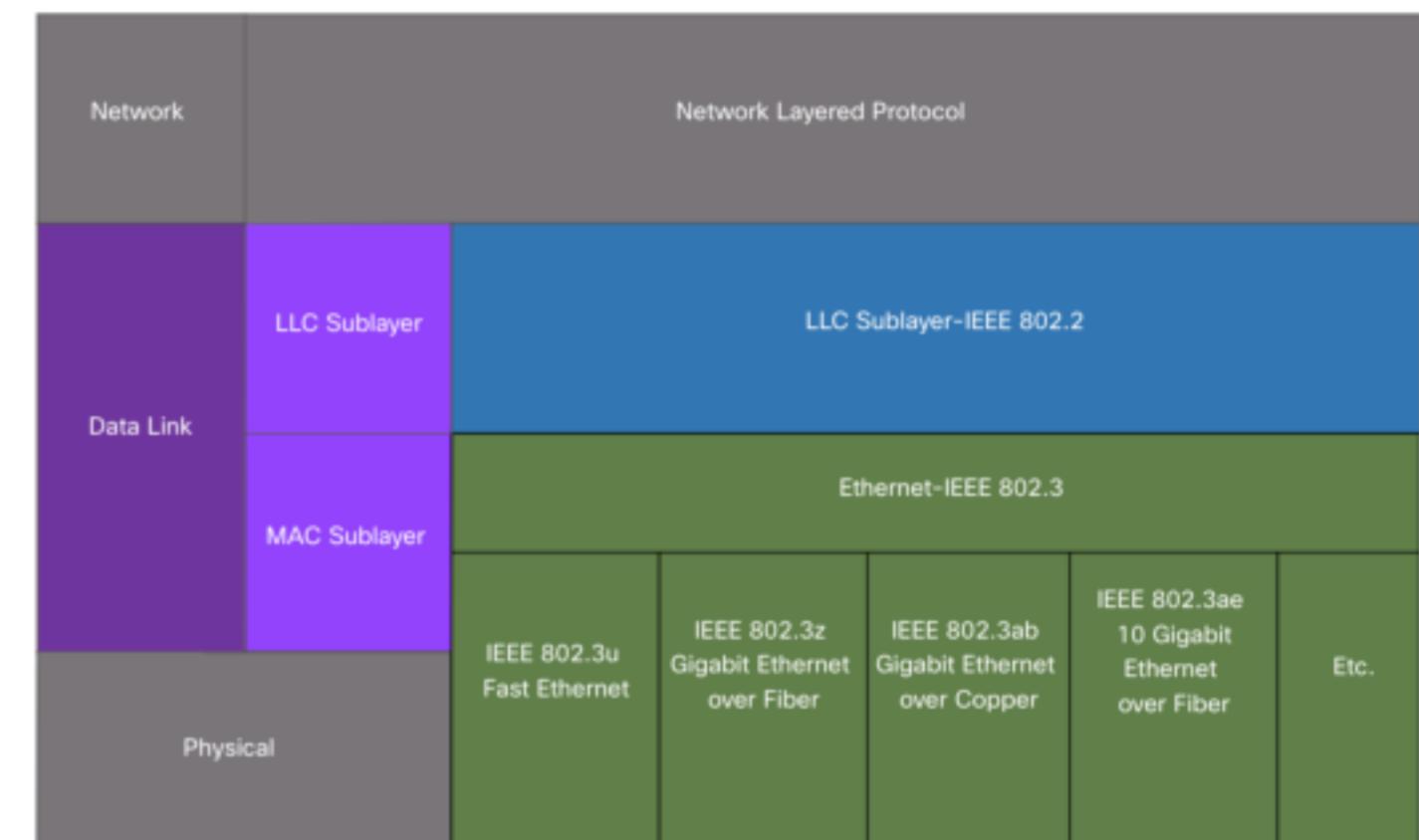
IEEE 802.3 data encapsulation includes the following:

1. **Ethernet frame** - This is the internal structure of the Ethernet frame.
2. **Ethernet Addressing** - The Ethernet frame includes both a source and destination MAC address to deliver the Ethernet frame from Ethernet NIC to Ethernet NIC on the same LAN.
3. **Ethernet Error detection** - The Ethernet frame includes a frame check sequence (FCS) trailer used for error detection.

# Ethernet Frames MAC Sublayer

## Media Access

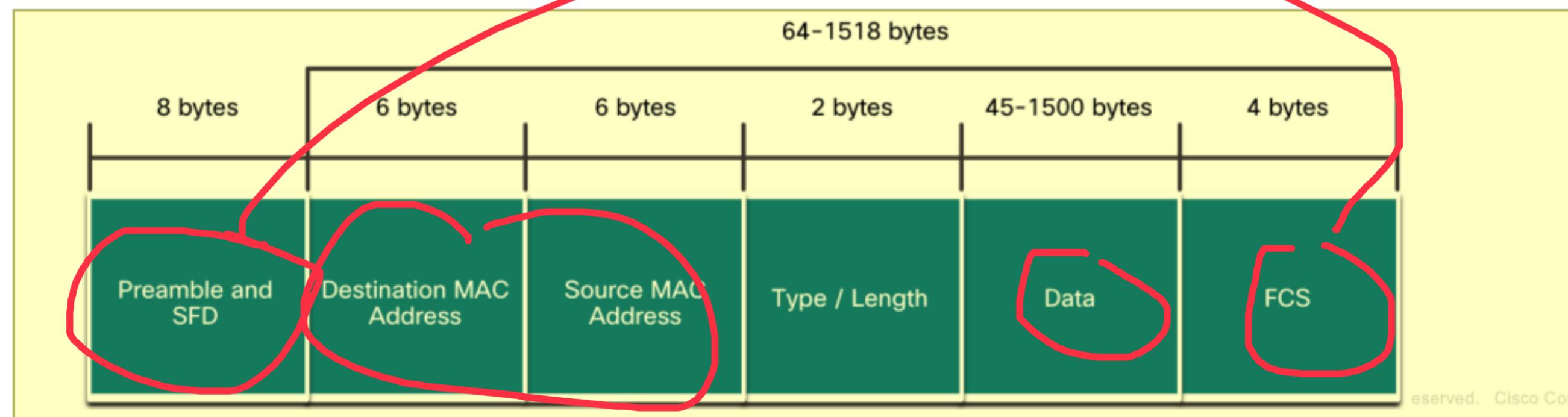
- The IEEE 802.3 MAC sublayer includes the specifications for different Ethernet communications standards over various types of media including copper and fiber.
- Legacy Ethernet using a bus topology or hubs, is a shared, half-duplex medium. Ethernet over a half-duplex medium uses a contention-based access method, carrier sense multiple access/collision detection (CSMA/CD).
- Ethernet LANs of today use switches that operate in full-duplex. Full-duplex communications with Ethernet switches do not require access control through CSMA/CD.



## Ethernet Frames

# Ethernet Frame Fields

- The minimum Ethernet frame size is 64 bytes and the maximum is 1518 bytes. The preamble field is not included when describing the size of the frame.
- Any frame less than 64 bytes in length is considered a “collision fragment” or “runt frame” and is automatically discarded. 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. They are considered invalid. Jumbo frames are usually supported by most Fast Ethernet and Gigabit Ethernet switches and NICs.



## Lab – Use Wireshark to Examine Ethernet Frames

In this lab, you will complete the following objectives:

- Part 1: Examine the Header Fields in an Ethernet II Frame
- Part 2: Use Wireshark to Capture and Analyze Ethernet Frames

# 7.2 Ethernet MAC Address



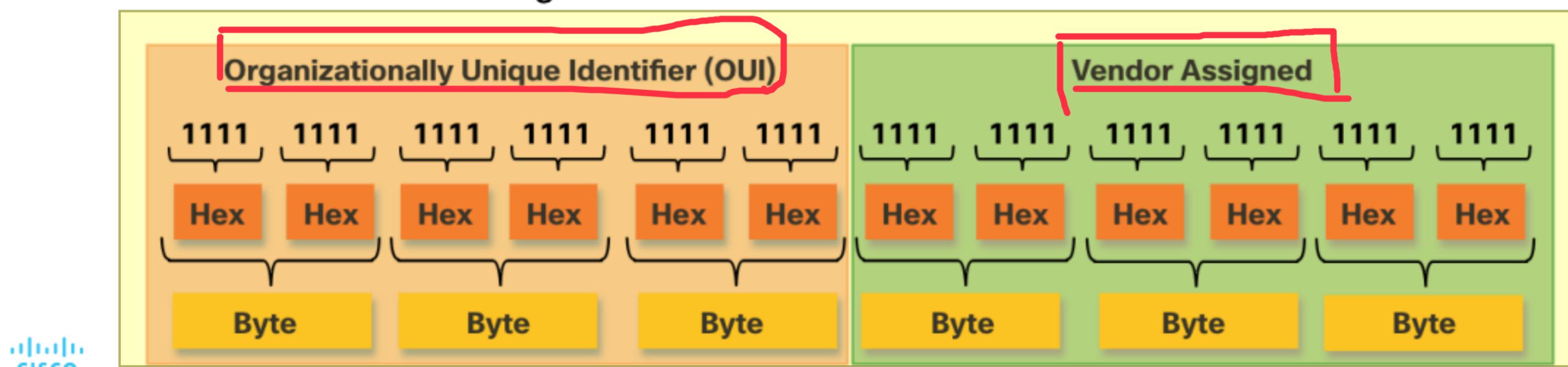
## MAC Address and Hexadecimal

- An Ethernet MAC address consists of a 48-bit binary value, expressed using 12 hexadecimal values.
- Given that 8 bits (one byte) is a common binary grouping, binary 00000000 to 11111111 can be represented in hexadecimal as the range 00 to FF,
- When using hexadecimal, leading zeroes are always displayed to complete the 8-bit representation. For example the binary value 0000 1010 is represented in hexadecimal as 0A.
- Hexadecimal numbers are often represented by the value preceded by **0x** (e.g., 0x73) to distinguish between decimal and hexadecimal values in documentation.
- Hexadecimal may also be represented by a subscript 16, or the hex number followed by an H (e.g., 73H).

## Ethernet MAC Addresses

# Ethernet MAC Address

- In an Ethernet LAN, every network device is connected to the same, shared media. MAC addressing provides a method for device identification at the data link layer of the OSI model.
- An Ethernet MAC address is a 48-bit address expressed using 12 hexadecimal digits. Because a byte equals 8 bits, we can also say that a MAC address is 6 bytes in length.
- All MAC addresses must be unique to the Ethernet device or Ethernet interface. To ensure this, all vendors that sell Ethernet devices must register with the IEEE to obtain a unique 6 hexadecimal (i.e., 24-bit or 3-byte) code called the organizationally unique identifier (OUI).
- An Ethernet MAC address consists of a 6 hexadecimal vendor OUI code followed by a 6 hexadecimal vendor-assigned value.



# Ethernet MAC Addresses Frame Processing

- When a device is forwarding a message to an Ethernet network, the Ethernet header include a Source MAC address and a Destination MAC address.
- When a NIC receives an Ethernet frame, it examines the destination MAC address to see if it matches the physical MAC address that is stored in RAM. If there is no match, the device discards the frame. If there is a match, it passes the frame up the OSI layers, where the de-encapsulation process takes place.

**Note:** Ethernet NICs will also accept frames if the destination MAC address is a broadcast or a multicast group of which the host is a member.

- Any device that is the source or destination of an Ethernet frame, will have an Ethernet NIC and therefore, a MAC address. This includes workstations, servers, printers, mobile devices, and routers.

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

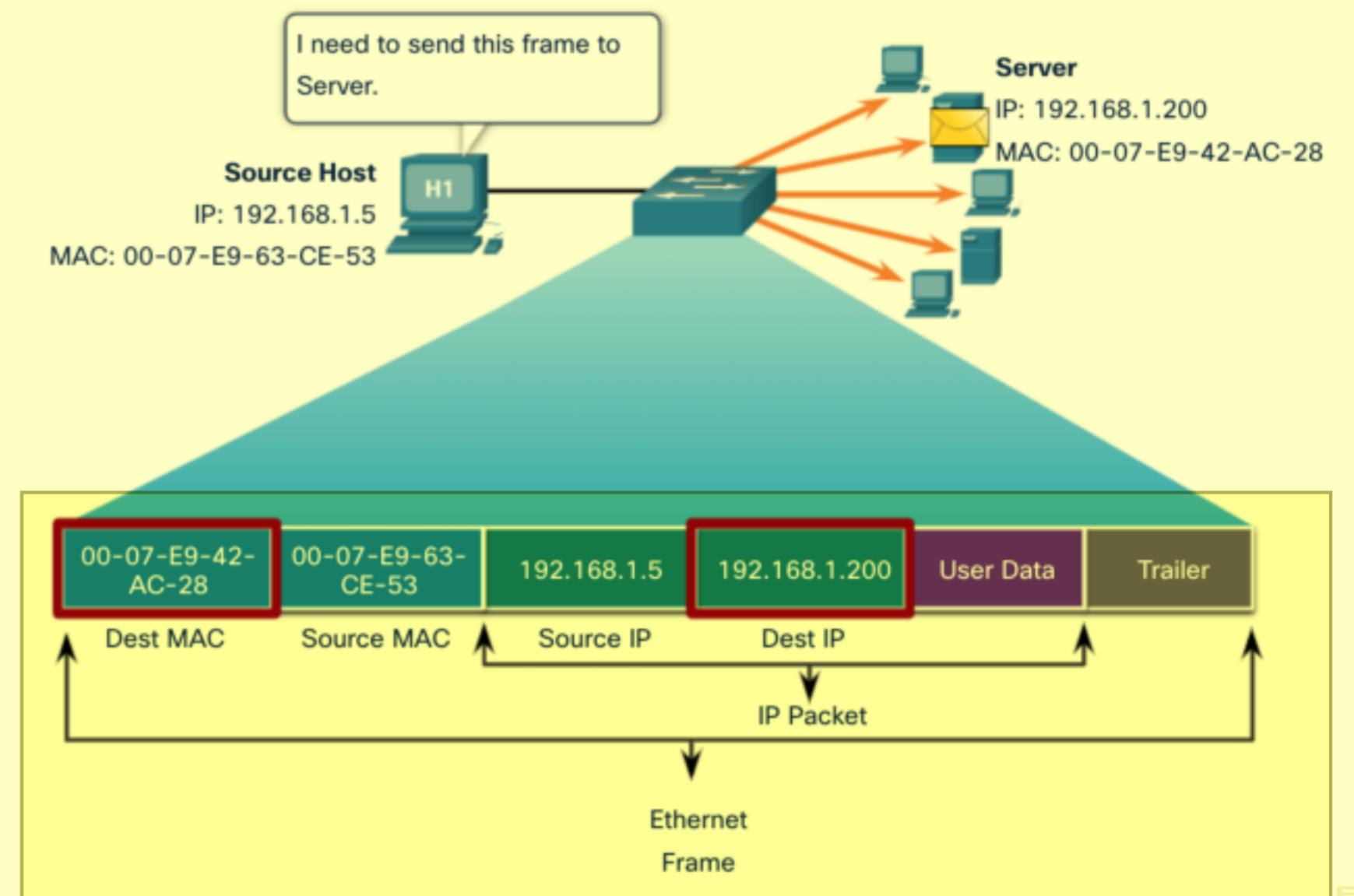


## Ethernet MAC Addresses Unicast MAC Address

In Ethernet, different MAC addresses are used for Layer 2 unicast, broadcast, and multicast communications.

- A unicast MAC address is the unique address that is used when a frame is sent from a single transmitting device to a single destination device.
- The process that a source host uses to determine the destination MAC address associated with an IPv4 address is known as Address Resolution Protocol (ARP). The process that a source host uses to determine the destination MAC address associated with an IPv6 address is known as Neighbor Discovery (ND).

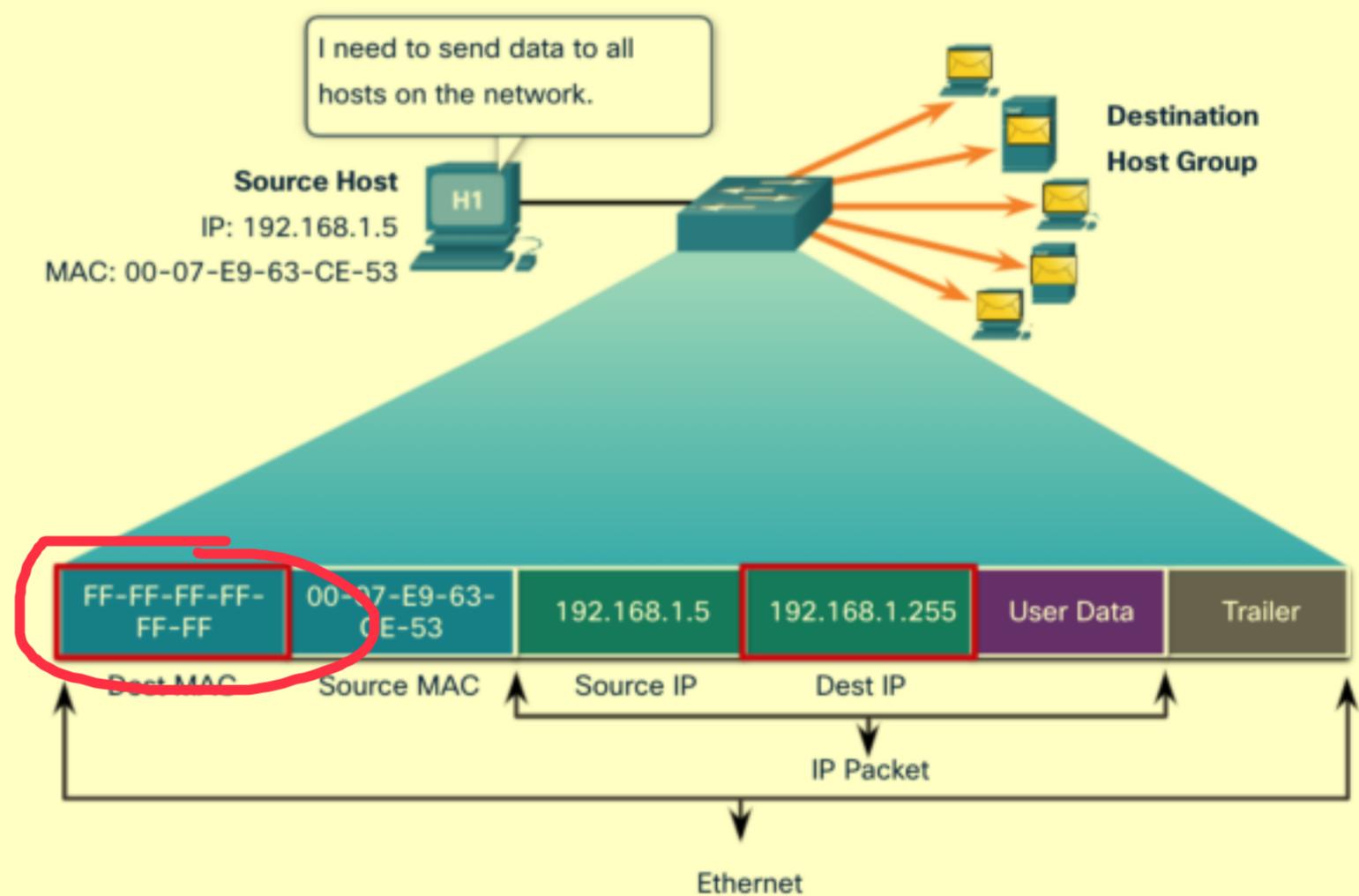
**Note:** The source MAC address must always be a unicast.



## Ethernet MAC Addresses Broadcast MAC Address

An Ethernet broadcast frame is received and processed by every device on the Ethernet LAN. The features of an Ethernet broadcast are as follows:

- It has a destination MAC address of FF-FF-FF-FF-FF-FF in hexadecimal (48 ones in binary).
- It is flooded out all Ethernet switch ports except the incoming port. It is not forwarded by a router.
- If the encapsulated data is an IPv4 broadcast packet, this means the packet contains a destination IPv4 address that has all ones (1s) in the host portion. This numbering in the address means that all hosts on that local network (broadcast domain) will receive and process the packet.

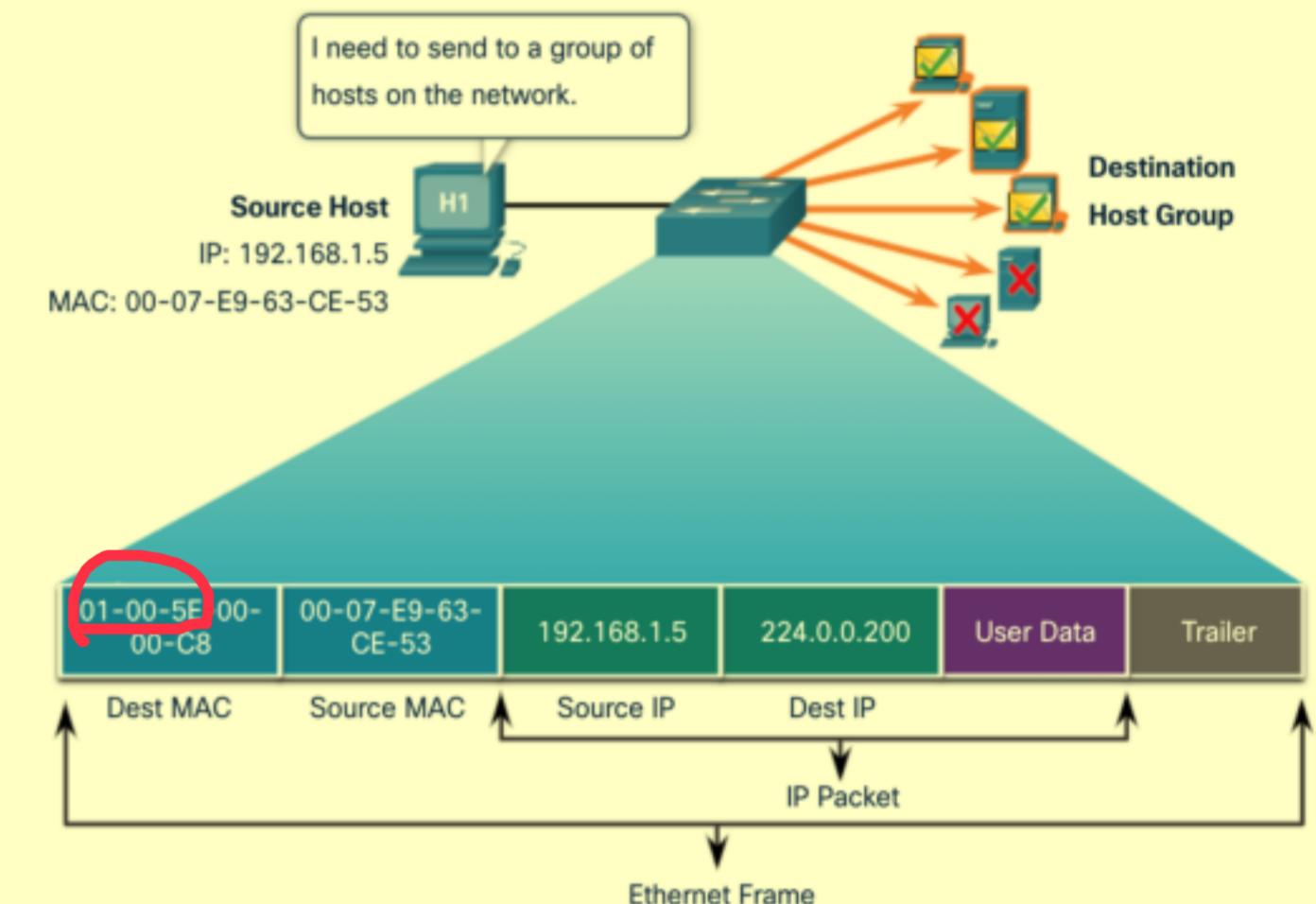


# Ethernet MAC Addresses

## Multicast MAC Address

An Ethernet multicast frame is received and processed by a group of devices that belong to the same multicast group.

- There is a destination MAC address of 01-00-5E when the encapsulated data is an IPv4 multicast packet and a destination MAC address of 33-33 when the encapsulated data is an IPv6 multicast packet.
- There are other reserved multicast destination MAC addresses for when the encapsulated data is not IP, such as Spanning Tree Protocol (STP).
- It is flooded out all Ethernet switch ports except the incoming port, unless the switch is configured for multicast snooping. It is not forwarded by a router, unless the router is configured to route multicast packets.
- Because multicast addresses represent a group of addresses (sometimes called a host group), they can only be used as the destination of a packet. The source will always be a unicast address.
- As with the unicast and broadcast addresses, the multicast IP address requires a corresponding multicast MAC address.



## Lab – View Network Device MAC Addresses

In this lab, you will complete the following objectives:

- Part 1: Set Up the Topology and Initialize Devices
- Part 2: Configure Devices and Verify Connectivity
- Part 3: Display, Describe, and Analyze Ethernet MAC Addresses

## 7.3 The MAC Address Table



## The MAC Address Table Switch Fundamentals

- A Layer 2 Ethernet switch uses Layer 2 MAC addresses to make forwarding decisions. It is completely unaware of the data (protocol) being carried in the data portion of the frame, such as an IPv4 packet, an ARP message, or an IPv6 ND packet. The switch makes its forwarding decisions based solely on the Layer 2 Ethernet MAC addresses.
- An Ethernet switch examines its MAC address table to make a forwarding decision for each frame, unlike legacy Ethernet hubs that repeat bits out all ports except the incoming port.
- When a switch is turned on, the MAC address table is empty.

**Note:** The MAC address table is sometimes referred to as a content addressable memory (CAM) table.

## The MAC Address Table Switch Learning and Forwarding

### Examine the Source MAC Address (Learn)

Every frame that enters a switch is checked for new information to learn. It does this by examining the source MAC address of the frame and the 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.

**Note:** If the source MAC address does exist in the table but on a different port, the switch treats this as a new entry. The entry is replaced using the same MAC address but with the more current port number.

## The MAC Address Table Switch Learning and Forwarding (Contd.)

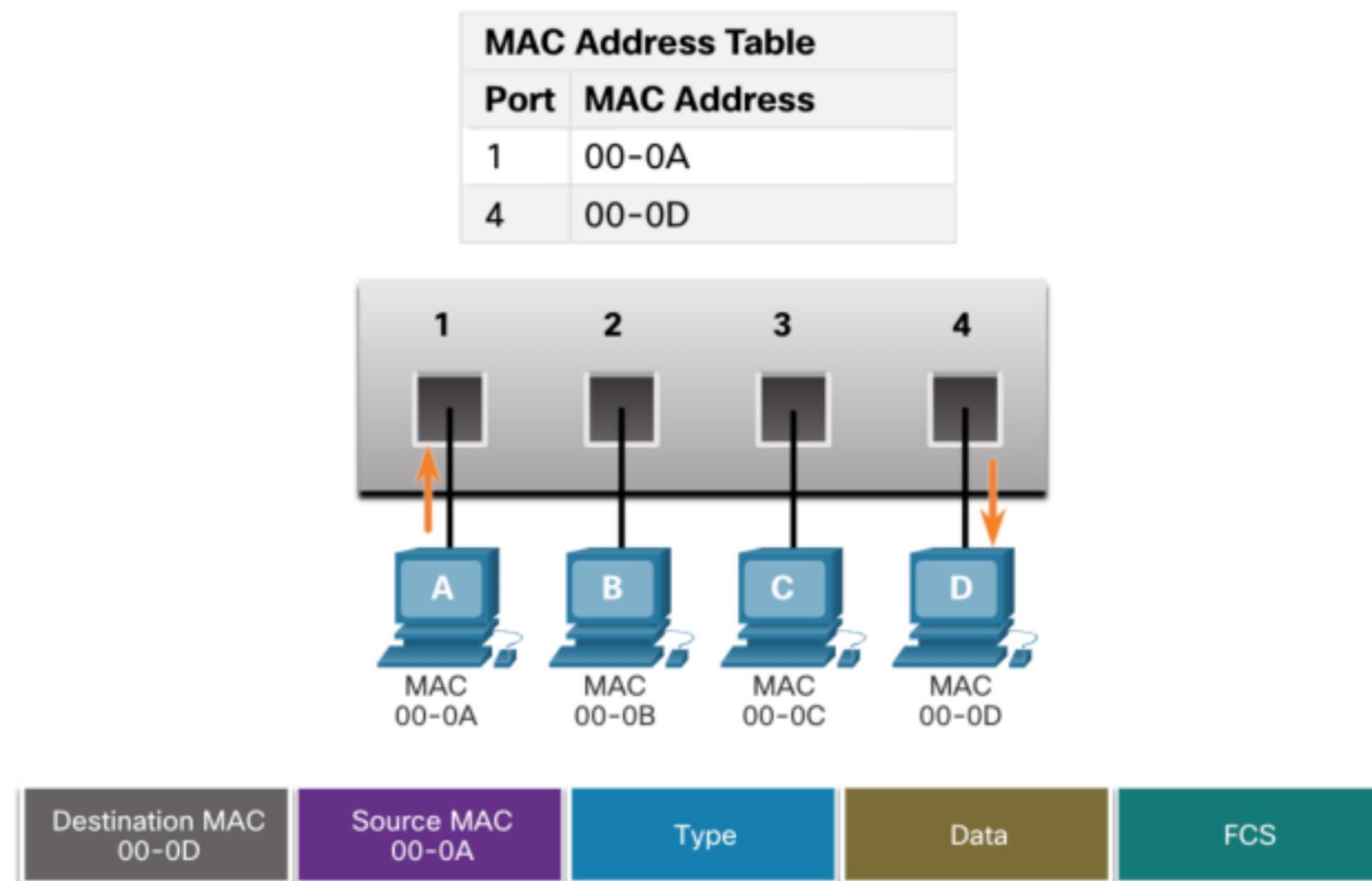
### **Find the Destination MAC Address (Forward)**

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 called an unknown unicast.

**Note:** If the destination MAC address is a broadcast or a multicast, the frame is also flooded out all ports except the incoming port.

## The MAC Address Table Filtering Frames

As a switch receives frames from different devices, it is able to populate its MAC address table by examining the source MAC address of every frame. When the MAC address table of the switch contains the destination MAC address, it is able to filter the frame and forward out a single port.



The MAC Address Table

## Video – MAC Address Tables on Connected Switches

This video will cover the following:

- How switches build MAC address tables
- How switches forward frames base on the content of their MAC address tables



## The MAC Address Table

# Video – Sending the Frame to the Default Gateway

This video will cover the following:

- What a switch does when the destination AMC address is not listed in the switch's MAC address table.
- What a switch does when the source AMC address is not listed in the switch's MAC address table



The MAC Address Table

## Lab – View the Switch MAC Address Table

In this lab, you will complete the following objectives:

- Part 1: Build and Configure the Network
- Part 2: Examine the Switch MAC Address Table



# 7.4 Switch Speeds and Forwarding Methods



## Switch Speeds and Forwarding Methods

# Frame Forwarding Methods on Cisco Switches

Switches use one of the following forwarding methods for switching data between network ports:

- **Store-and-forward switching** - This frame forwarding method 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. Then the frame is forwarded out of the correct port.
- **Cut-through switching** - This frame forwarding method 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.
- A big advantage of store-and-forward switching is that it determines if a frame has errors before propagating the frame. When an error is detected in a frame, the switch discards the frame. Discarding frames with errors reduces the amount of bandwidth consumed by corrupt data.
- Store-and-forward switching is required for quality of service (QoS) analysis on converged networks where frame classification for traffic prioritization is necessary. For example, voice over IP (VoIP) data streams need to have priority over web-browsing traffic.



## Switch Speeds and Forwarding Methods

# Cut-Through Switching

In cut-through switching, the switch acts upon the data as soon as it is received, even if the transmission is not complete. The switch buffers just enough of the frame to read the destination MAC address so that it can determine to which port it should forward out the data. The switch does not perform any error checking on the frame.

There are two variants of cut-through switching:

- **Fast-forward switching** - Offers the lowest level of latency by immediately forwarding a packet after reading the destination address. Because fast-forward switching starts forwarding before the entire packet has been received, there may be times when packets are relayed with errors. The destination NIC discards the faulty packet upon receipt. Fast-forward switching is the typical cut-through method of switching.
- **Fragment-free switching** - A compromise between the high latency and high integrity of store-and-forward switching and the low latency and reduced integrity of fast-forward switching, the switch stores and performs an error check on the first 64 bytes of the frame before forwarding. Because most network errors and collisions occur during the first 64 bytes, this ensures that a collision has not occurred before forwarding the frame.

## Switch Speeds and Forwarding Methods

# Memory Buffering on Switches

An Ethernet switch may use a buffering technique to store frames before forwarding them or when the destination port is busy because of congestion.

Method	Description
Port-based memory	<ul style="list-style-type: none"><li>• Frames are stored in queues that are linked to specific incoming and outgoing ports.</li><li>• A frame is transmitted to the outgoing port only when all the frames ahead in the queue have been successfully transmitted.</li><li>• It is possible for a single frame to delay the transmission of all the frames in memory because of a busy destination port.</li><li>• This delay occurs even if the other frames could be transmitted to open destination ports.</li></ul>
Shared memory	<ul style="list-style-type: none"><li>• Deposits all frames into a common memory buffer shared by all switch ports and the amount of buffer memory required by a port is dynamically allocated.</li><li>• The frames in the buffer are dynamically linked to the destination port enabling a packet to be received on one port and then transmitted on another port, without moving it to a different queue.</li></ul>

- Shared memory buffering also results in larger frames that can be transmitted with fewer dropped frames. This is important with asymmetric switching which allows for different data rates on different ports. Therefore, more bandwidth can be dedicated to certain ports (e.g., server port).



## Switch Speeds and Forwarding Methods

# Duplex and Speed Settings

Two of the most basic settings on a switch are the bandwidth (“speed”) and duplex settings for each individual switch port. It is critical that the duplex and bandwidth settings match between the switch port and the connected devices.

There are two types of duplex settings used for communications on an Ethernet network:

- **Full-duplex** - Both ends of the connection can send and receive simultaneously.
- **Half-duplex** - Only one end of the connection can send at a time.

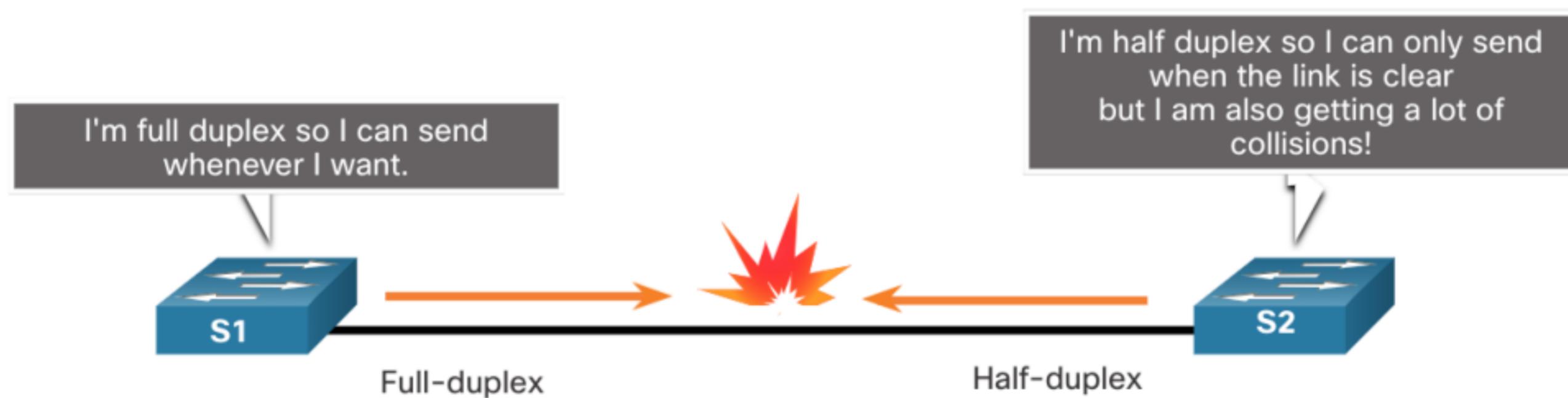
Autonegotiation is an optional function found on most Ethernet switches and NICs. It enables two devices to automatically negotiate the best speed and duplex capabilities.

**Note:** Gigabit Ethernet ports only operate in full-duplex.

## Switch Speeds and Forwarding Methods

# Duplex and Speed Settings

- Duplex mismatch is one of the most common causes of performance issues on 10/100 Mbps Ethernet links. It occurs when one port on the link operates at half-duplex while the other port operates at full-duplex.
- This can occur when one or both ports on a link are reset, and the autonegotiation process does not result in both link partners having the same configuration.
- It also can occur when users reconfigure one side of a link and forget to reconfigure the other. Both sides of a link should have autonegotiation on, or both sides should have it off. Best practice is to configure both Ethernet switch ports as full-duplex.



## Switch Speeds and Forwarding Methods

### Auto-MDIX

Connections between devices once required the use of either a crossover or straight-through cable. The type of cable required depended on the type of interconnecting devices.

**Note:** A direct connection between a router and a host requires a cross-over connection.

- Most switch devices now support the automatic medium-dependent interface crossover (auto-MDIX) feature. When enabled, the switch automatically detects the type of cable attached to the port and configures the interfaces accordingly.
- The auto-MDIX feature is enabled by default on switches running Cisco IOS Release 12.2(18)SE or later. However, the feature could be disabled. For this reason, you should always use the correct cable type and not rely on the auto-MDIX feature.
- Auto-MDIX can be re-enabled using the **mdix auto** interface configuration command.

# 7.5 Module Practice and Quiz



## Module Practice and Quiz

# What did I learn in this module?

- Ethernet operates in the data link layer and the physical layer. Ethernet standards define both the Layer 2 protocols and the Layer 1 technologies.
- Ethernet uses the LLC and MAC sublayers of the data link layer to operate.
- The Ethernet frame fields are: preamble and start frame delimiter, destination MAC address, source MAC address, EtherType, data, and FCS.
- MAC addressing provides a method for device identification at the data link layer of the OSI model.
- An Ethernet MAC address is a 48-bit address expressed using 12 hexadecimal digits, or 6 bytes.
- When a device is forwarding a message to an Ethernet network, the Ethernet header includes the source and destination MAC addresses. In Ethernet, different MAC addresses are used for Layer 2 unicast, broadcast, and multicast communications.

## Module Practice and Quiz

# What did I learn in this module? (Contd.)

- A Layer 2 Ethernet switch makes its forwarding decisions based solely on the Layer 2 Ethernet MAC addresses.
- The switch dynamically builds the MAC address table by examining the source MAC address of the frames received on a port.
- The switch forwards frames by searching for a match between the destination MAC address in the frame and an entry in the MAC address table.
- Switches use one of the following forwarding methods for switching data between network ports: store-and-forward switching or cut-through switching. Two variants of cut-through switching are fast-forward and fragment-free.
- Two methods of memory buffering are port-based memory and shared memory.
- There are two types of duplex settings used for communications on an Ethernet network: full-duplex and half-duplex.

## Module 7: Ethernet Switching

# New Terms and Commands

- Store-and-Forward Switching
- Cut-through Switching
- Fast-Forward Switching
- Fragment-free Switching
- OUI (Organizationally Unique Identifier)
- ARP (Address Resolution Protocol)
- ND (Neighbor Discovery)
- Port-based memory
- Shared memory
- Auto-MDIX

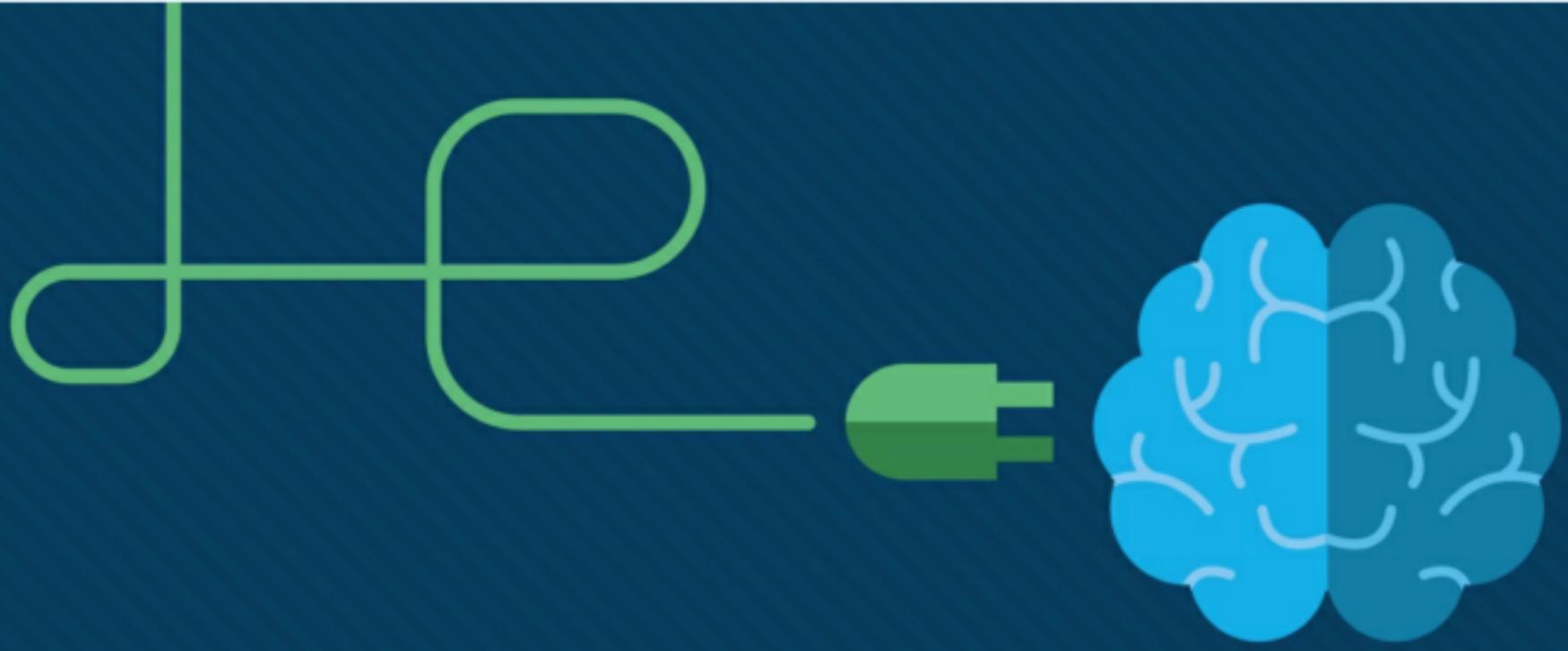






# Module 11: IPv4 Addressing

Introduction to Networks v7.0  
(ITN)



# Module Objectives

**Module Title:** IPv4 Addressing

**Module Objective:** Calculate an IPv4 subnetting scheme to efficiently segment your network.

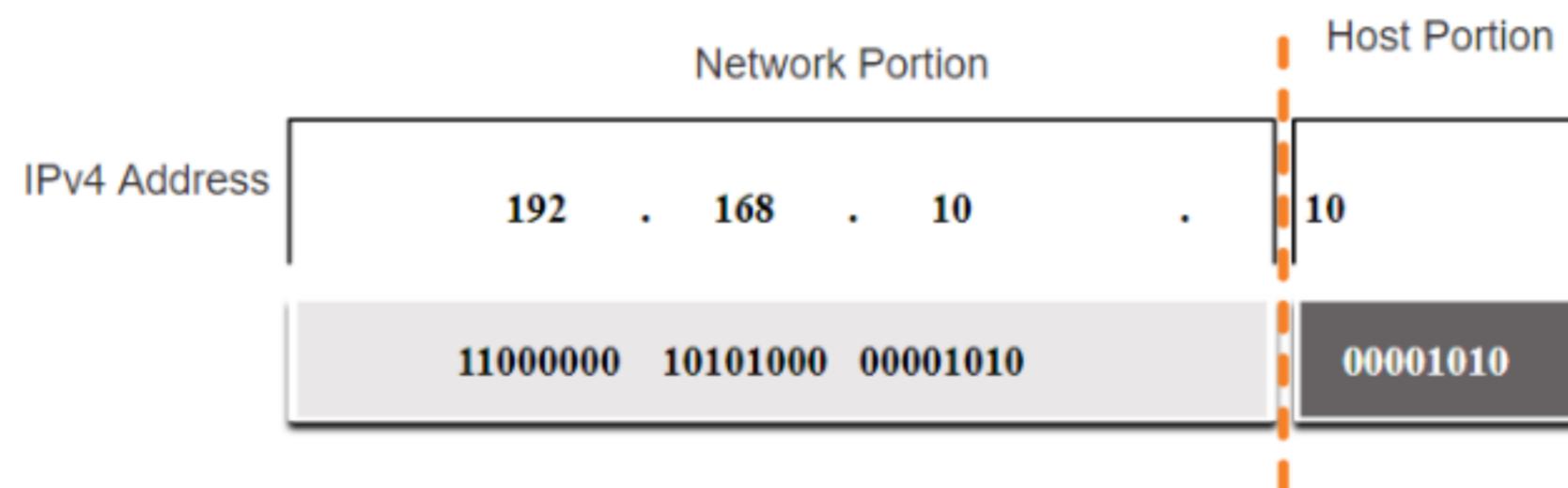
Topic Title	Topic Objective
IPv4 Address Structure	Describe the structure of an IPv4 address including the network portion, the host portion, and the subnet mask.
IPv4 Unicast, Broadcast, and Multicast	Compare the characteristics and uses of the unicast, broadcast and multicast IPv4 addresses.
Types of IPv4 Addresses	Explain public, private, and reserved IPv4 addresses.
Network Segmentation	Explain how subnetting segments a network to enable better communication.
Subnet an IPv4 Network	Calculate IPv4 subnets for a /24 prefix.

# 11.1 IPv4 Address Structure



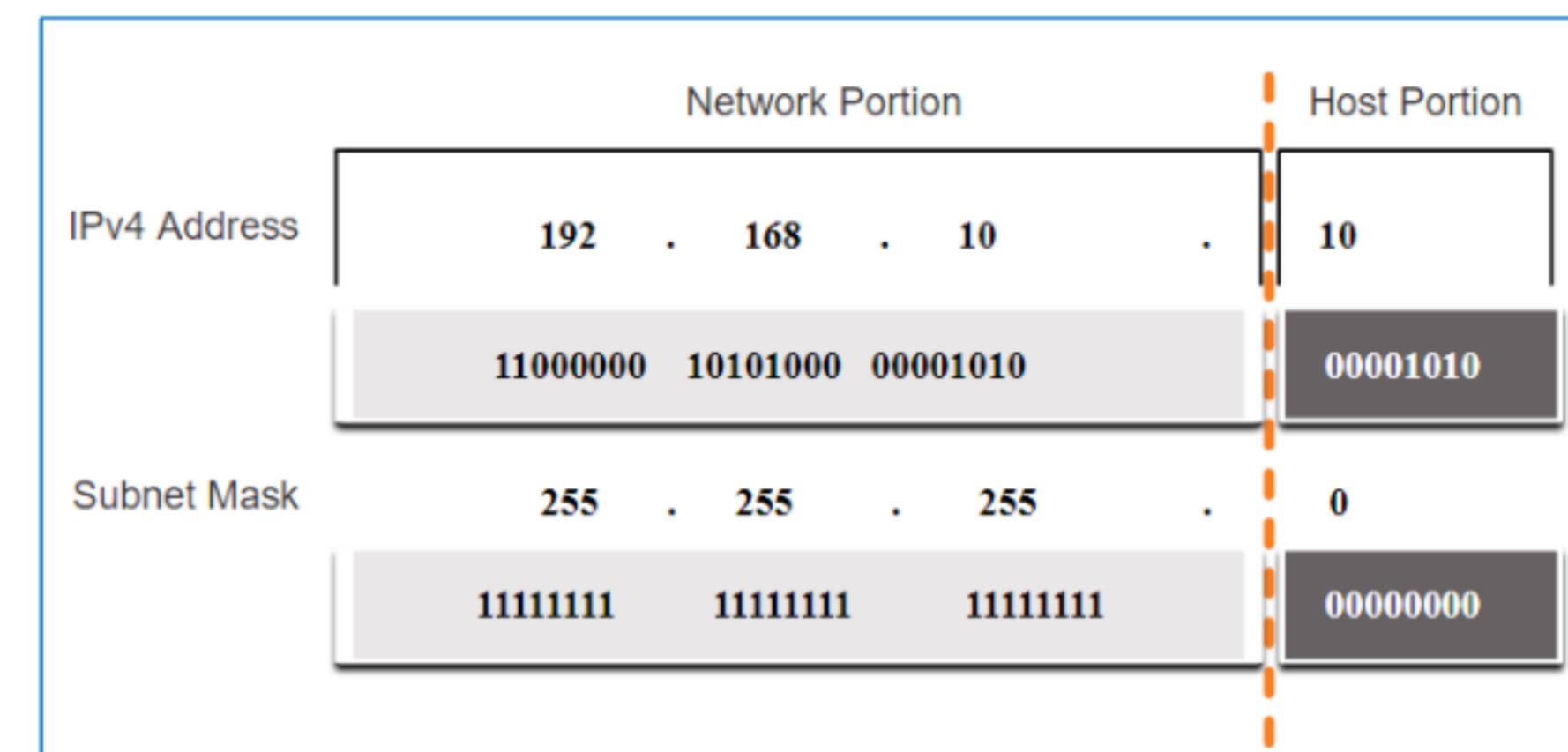
## IPv4 Address Structure Network and Host Portions

- An IPv4 address is a 32-bit hierarchical address that is made up of a network portion and a host portion.
- When determining the network portion versus the host portion, you must look at the 32-bit stream.
- A subnet mask



## IPv4 Address Structure The Subnet Mask

- To identify the network and host portions of an IPv4 address, the subnet mask is compared to the IPv4 address bit for bit, from left to right.
- The actual process used to identify the network and host portions is called ANDing.



## IPv4 Address Structure

# The Prefix Length

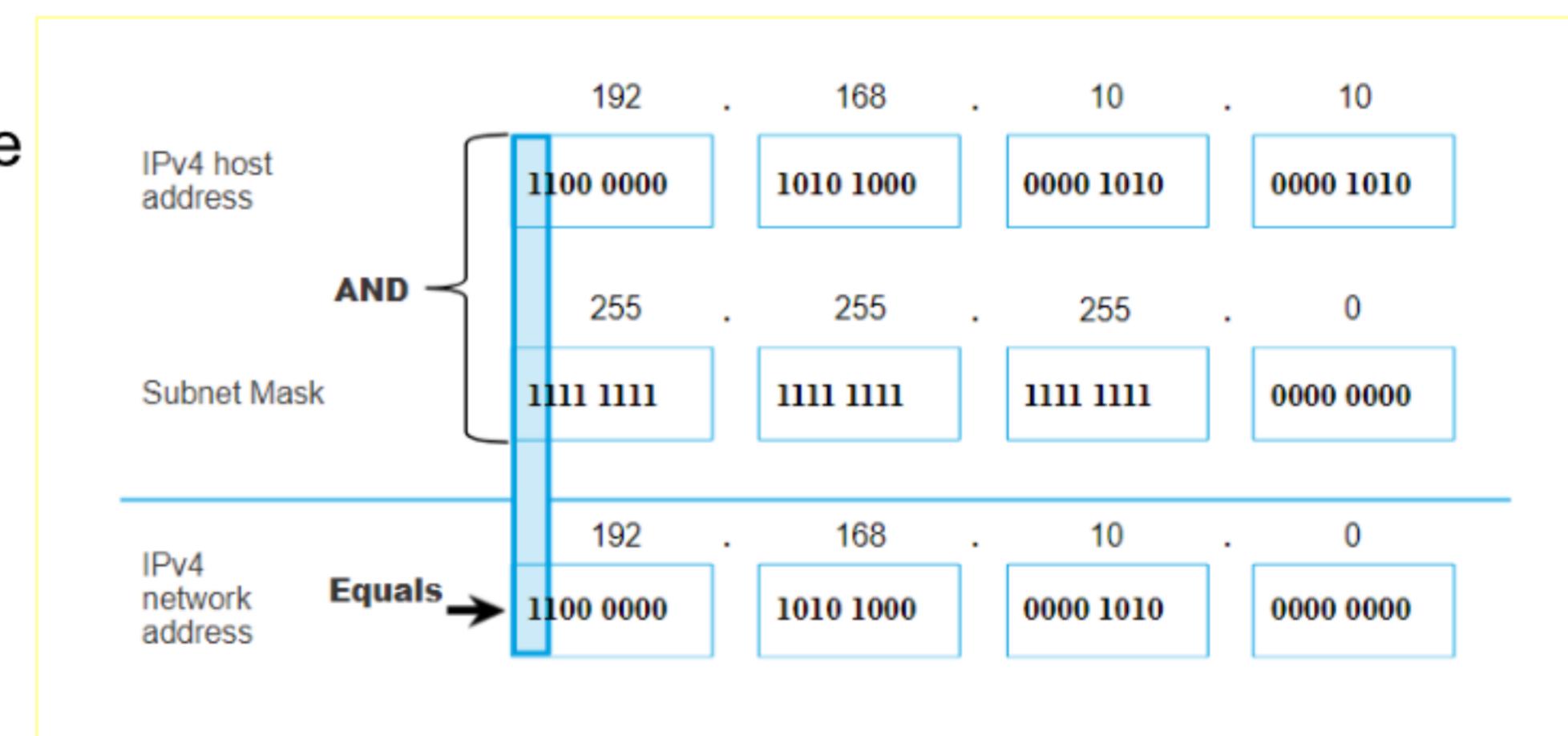
- A prefix length is a less cumbersome method used to identify a subnet mask address.
- The prefix length is the number of bits set to 1 in the subnet mask.
- It is written in “slash notation” therefore, count the number of bits in the subnet mask and prepend it with a slash.

Subnet Mask	32-bit Address	Prefix Length
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

## IPv4 Address Structure

# Determining the Network: Logical AND

- A logical AND Boolean operation is used in determining the network address.
- Logical AND is the comparison of two bits where only a 1 AND 1 produces a 1 and any other combination results in a 0.
- $1 \text{ AND } 1 = 1$ ,  $0 \text{ AND } 1 = 0$ ,  $1 \text{ AND } 0 = 0$ ,  $0 \text{ AND } 0 = 0$
- 1 = True and 0 = False
- To identify the network address, the host IPv4 address is logically ANDed, bit by bit, with the subnet mask to identify the network address.



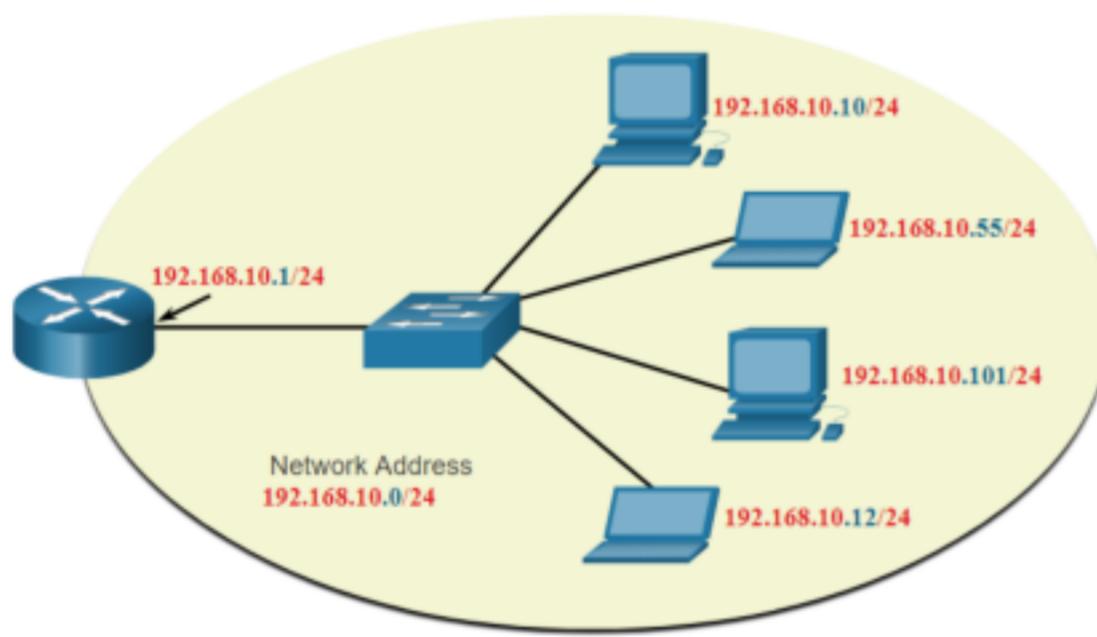
## Video – Network, Host and Broadcast Addresses

This video will cover the following:

- Network address
- Broadcast Address
- First usable host
- Last usable host

# IPv4 Address Structure Network, Host, and Broadcast Addresses

- Within each network are three types of IP addresses:
  - Network address
  - Host addresses
  - Broadcast address



	Network Portion			Host Portion	Host Bits
Subnet mask <b>255.255.255.0 or /24</b>	255 11111111	255 11111111	255 11111111	0 00000000	
Network address <b>192.168.10.0 or /24</b>	192 11000000	168 10100000	10 00001010	0 00000000	All 0s
First address <b>192.168.10.1 or /24</b>	192 11000000	168 10100000	10 00001010	1 00000001	All 0s and a 1
Last address <b>192.168.10.254 or /24</b>	192 11000000	168 10100000	10 00001010	254 11111110	All 1s and a 0
Broadcast address <b>192.168.10.255 or /24</b>	192 11000000	168 10100000	10 00001010	255 11111111	All 1s

# 11.2 IPv4 Unicast, Broadcast, and Multicast



## IPv4 Unicast, Broadcast, and Multicast

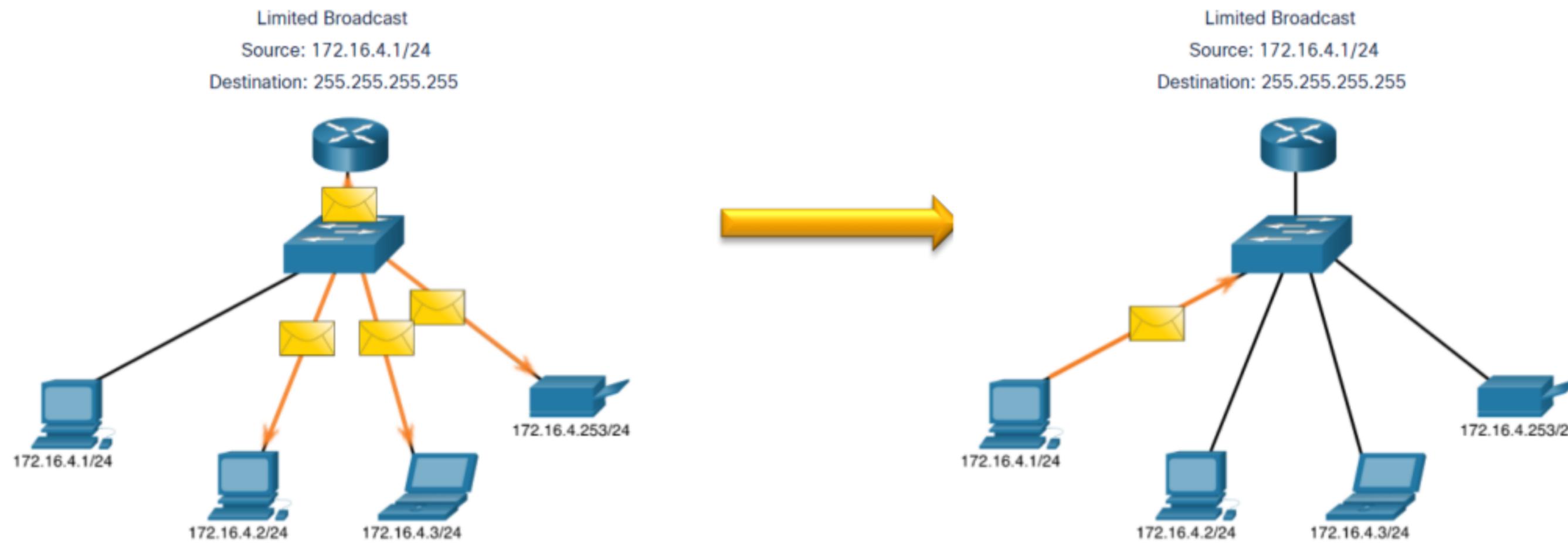
### Unicast

- Unicast transmission is sending a packet to one destination IP address.
- For example, the PC at 172.16.4.1 sends a unicast packet to the printer at 172.16.4.253.



## IPv4 Unicast, Broadcast, and Multicast Broadcast

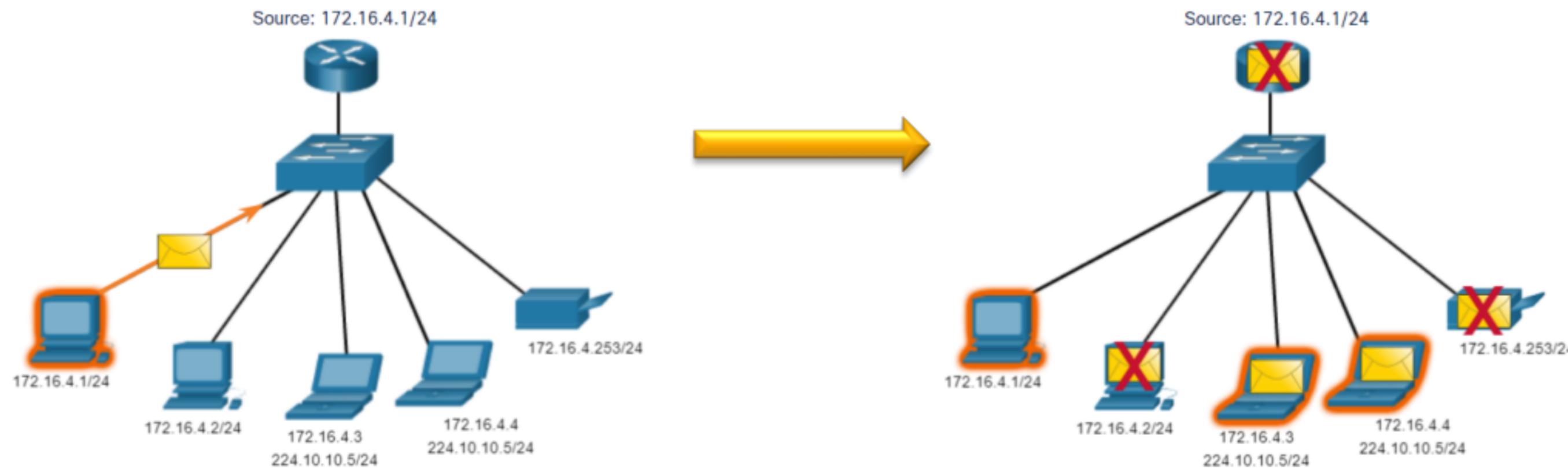
- Broadcast transmission is sending a packet to all other destination IP addresses.
- For example, the PC at 172.16.4.1 sends a broadcast packet to all IPv4 hosts.



## IPv4 Unicast, Broadcast, and Multicast

### Multicast

- Multicast transmission is sending a packet to a multicast address group.
- For example, the PC at 172.16.4.1 sends a multicast packet to the multicast group address 224.10.10.5.



# 11.3 Types of IPv4 Addresses



## Types of IPv4 Addresses

### Public and Private IPv4 Addresses

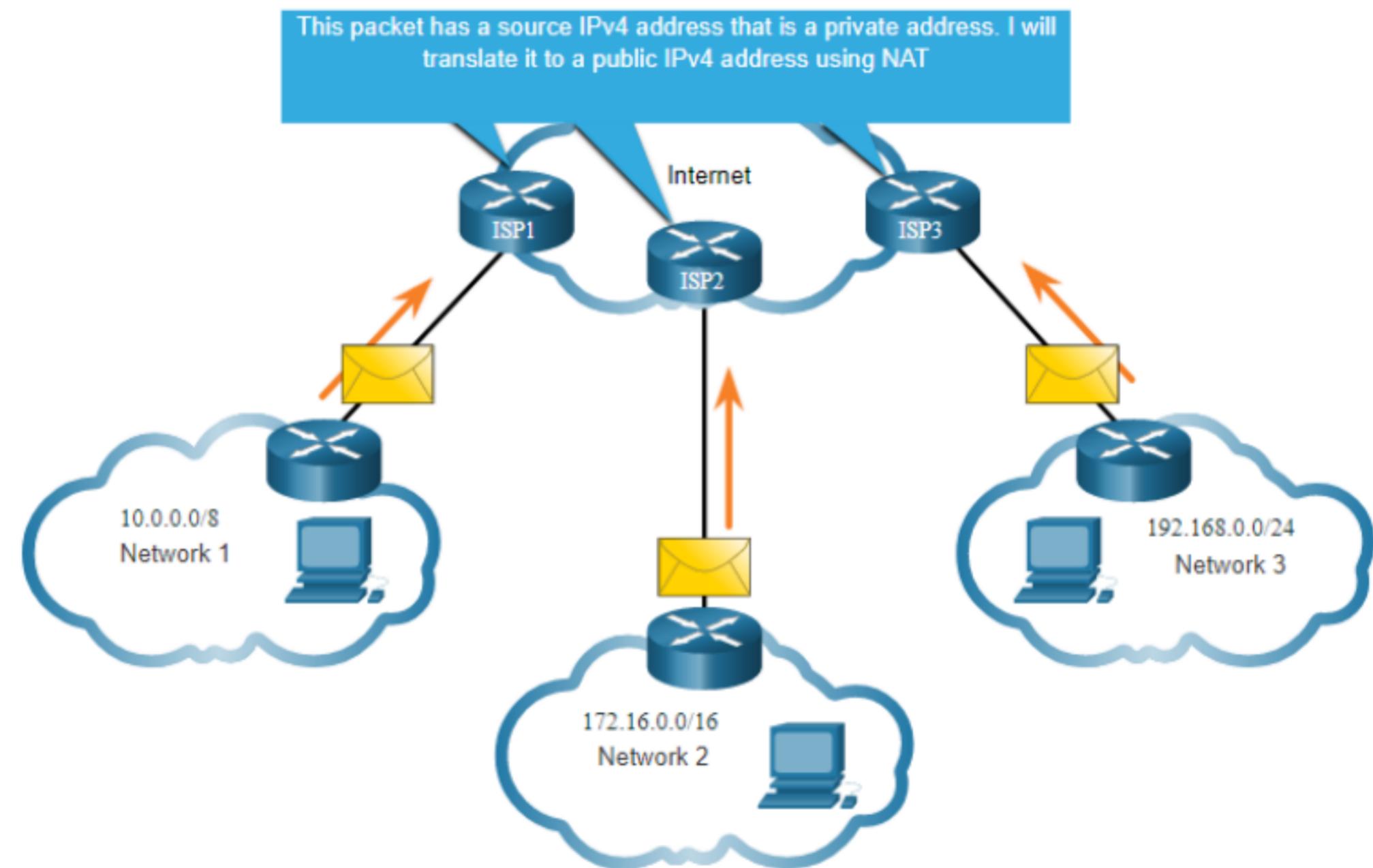
- As defined in RFC 1918, public IPv4 addresses are globally routed between internet service provider (ISP) routers.
- Private addresses are common blocks of addresses used by most organizations to assign IPv4 addresses to internal hosts.
- Private IPv4 addresses are not unique and can be used internally within any network.
- However, private addresses are not globally routable.

Network Address and Prefix	RFC 1918 Private Address Range
10.0.0.0/8	10.0.0.0 - 10.255.255.255
172.16.0.0/12	172.16.0.0 - 172.31.255.255
192.168.0.0/16	192.168.0.0 - 192.168.255.255

# Types of IPv4 Addresses

## Routing to the Internet

- Network Address Translation (NAT) translates private IPv4 addresses to public IPv4 addresses.
- NAT is typically enabled on the edge router connecting to the internet.
- It translates the internal private address to a public global IP address.



## Types of IPv4 Addresses

# Special Use IPv4 Addresses

## Loopback addresses

- 127.0.0.0 /8 (127.0.0.1 to 127.255.255.254)
- Commonly identified as only 127.0.0.1
- Used on a host to test if TCP/IP is operational.

```
C:\Users\NetAcad> ping 127.0.0.1
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
```

## Link-Local addresses

- 169.254.0.0 /16 (169.254.0.1 to 169.254.255.254)
- Commonly known as the Automatic Private IP Addressing (APIPA) addresses or self-assigned addresses.
- Used by Windows DHCP clients to self-configure when no DHCP servers are available.



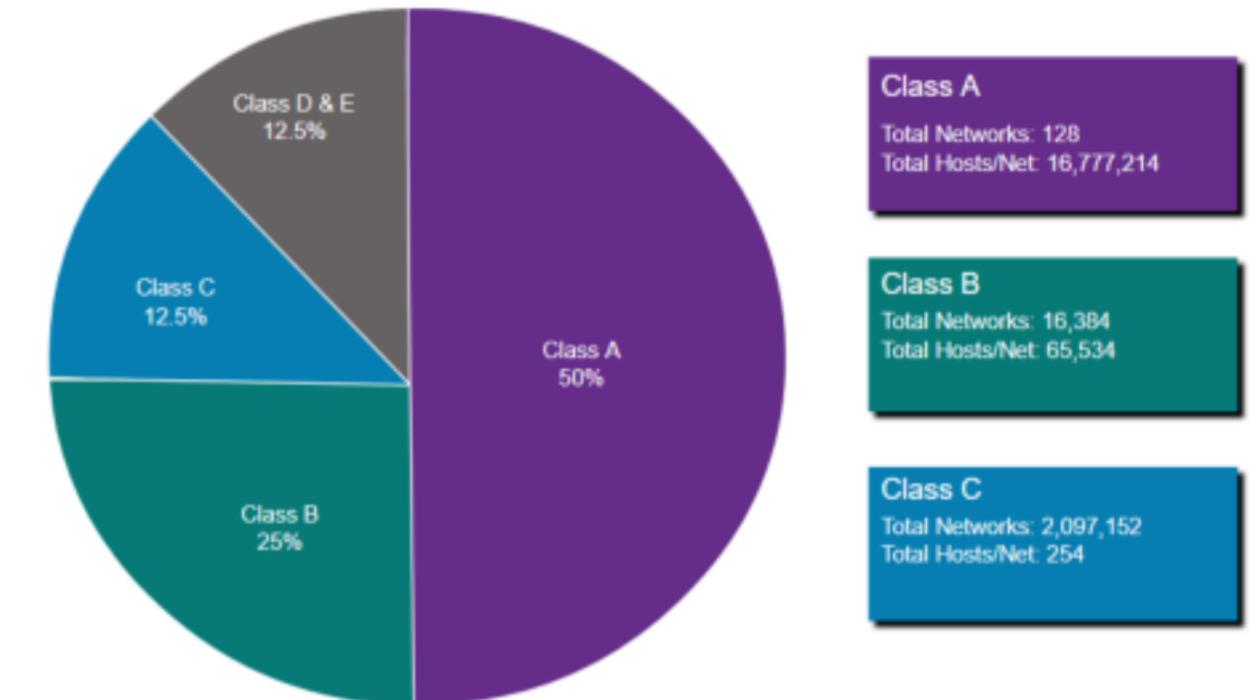
## Types of IPv4 Addresses

# Legacy Classful Addressing

RFC 790 (1981) allocated IPv4 addresses in classes

- Class A (0.0.0.0/8 to 127.0.0.0/8)
- Class B (128.0.0.0 /16 – 191.255.0.0 /16)
- Class C (192.0.0.0 /24 – 223.255.255.0 /24)
- Class D (224.0.0.0 to 239.0.0.0)
- Class E (240.0.0.0 – 255.0.0.0)
- Classful addressing wasted many IPv4 addresses.

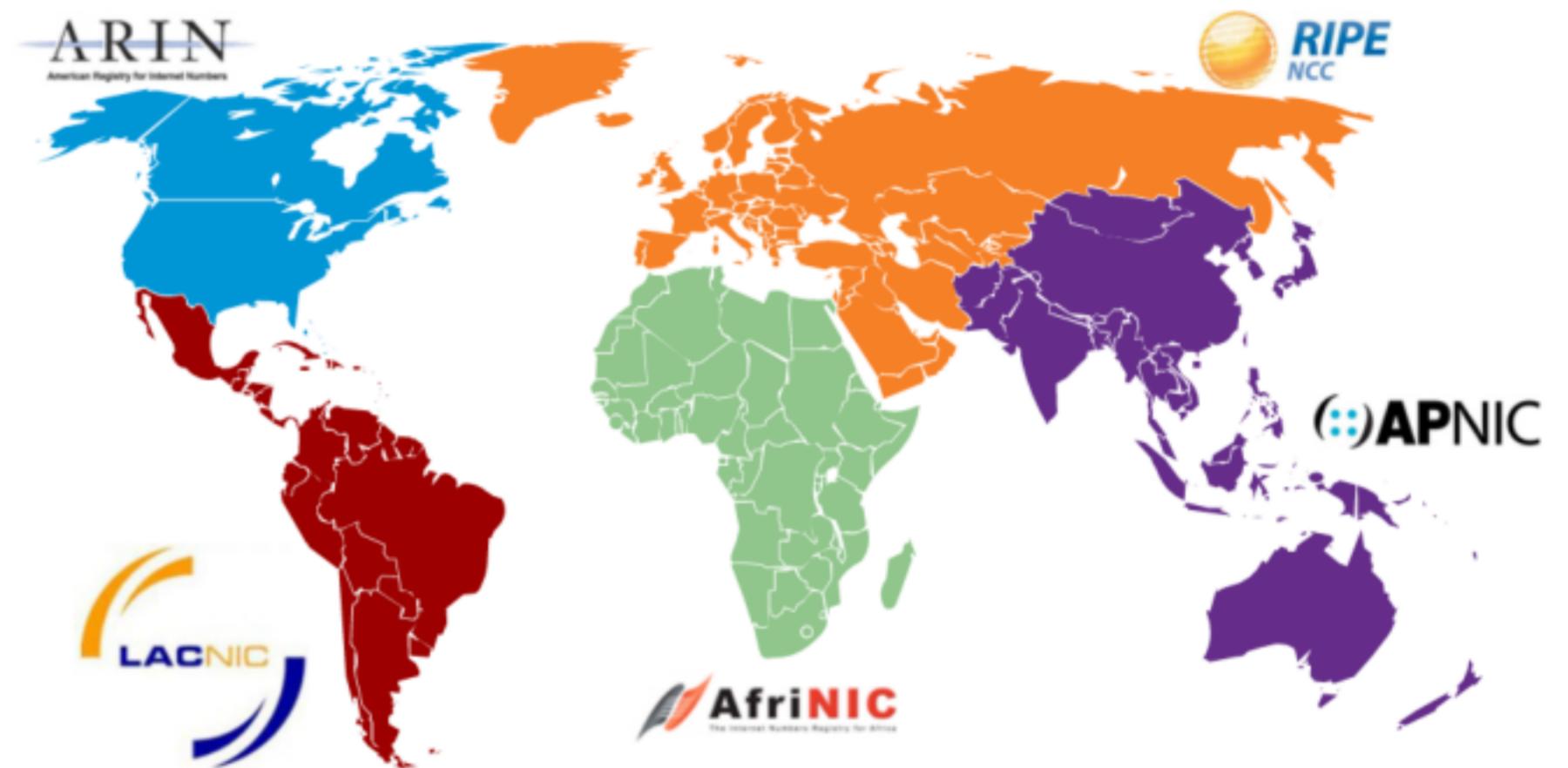
Classful address allocation was replaced with classless addressing which ignores the rules of classes (A, B, C).



## Types of IPv4 Addresses

# Assignment of IP Addresses

- The Internet Assigned Numbers Authority (IANA) manages and allocates blocks of IPv4 and IPv6 addresses to five Regional Internet Registries (RIRs).
- RIRs are responsible for allocating IP addresses to ISPs who provide IPv4 address blocks to smaller ISPs and organizations.

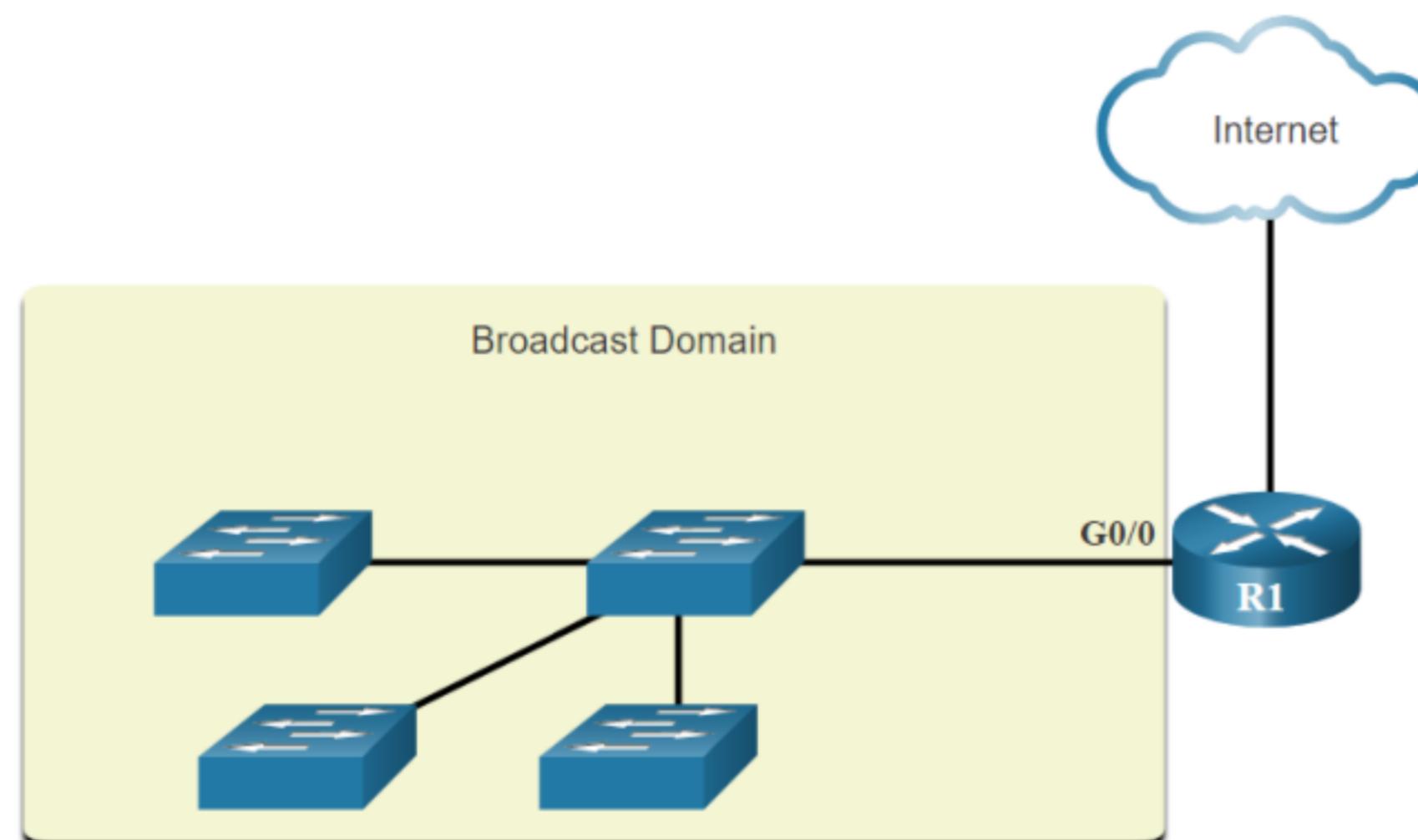


# 11.4 Network Segmentation



## Broadcast Domains and Segmentation

- Many protocols use broadcasts or multicasts (e.g., ARP use broadcasts to locate other devices, hosts send DHCP discover broadcasts to locate a DHCP server.)
- Switches propagate broadcasts out all interfaces except the interface on which it was received.

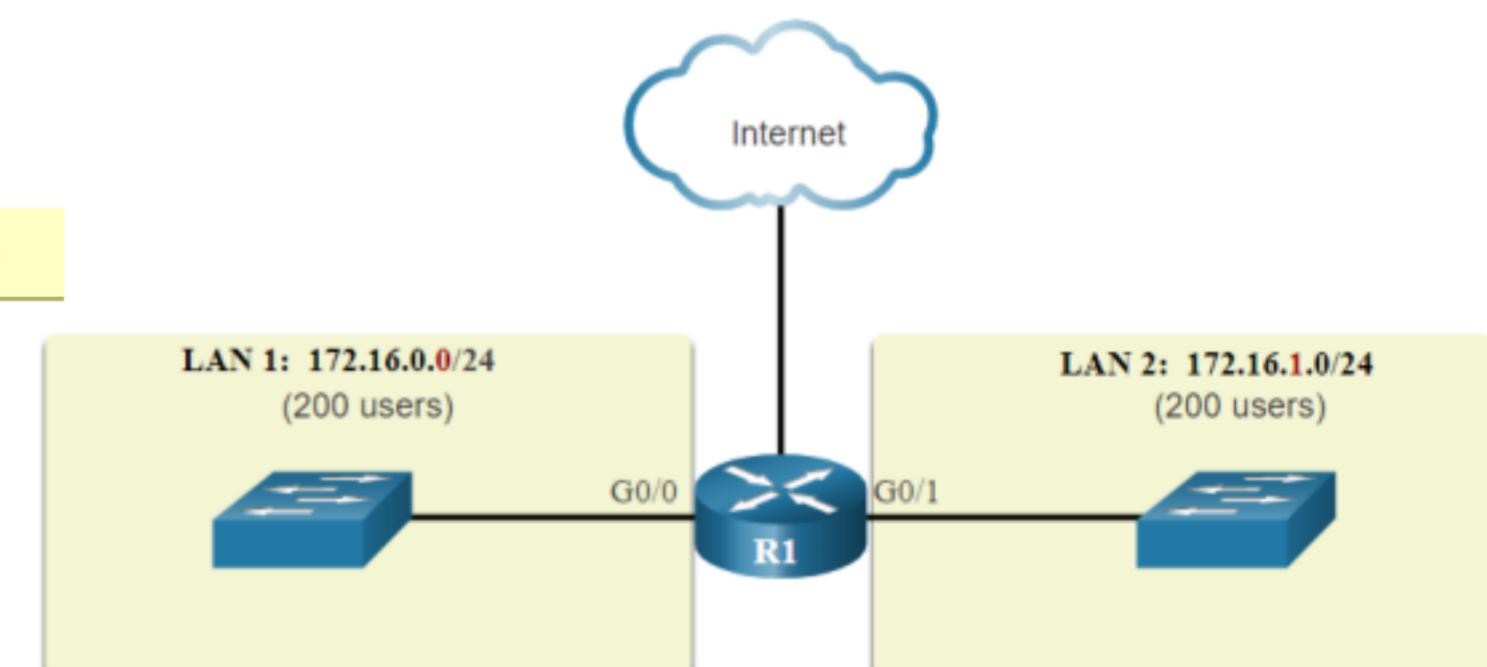
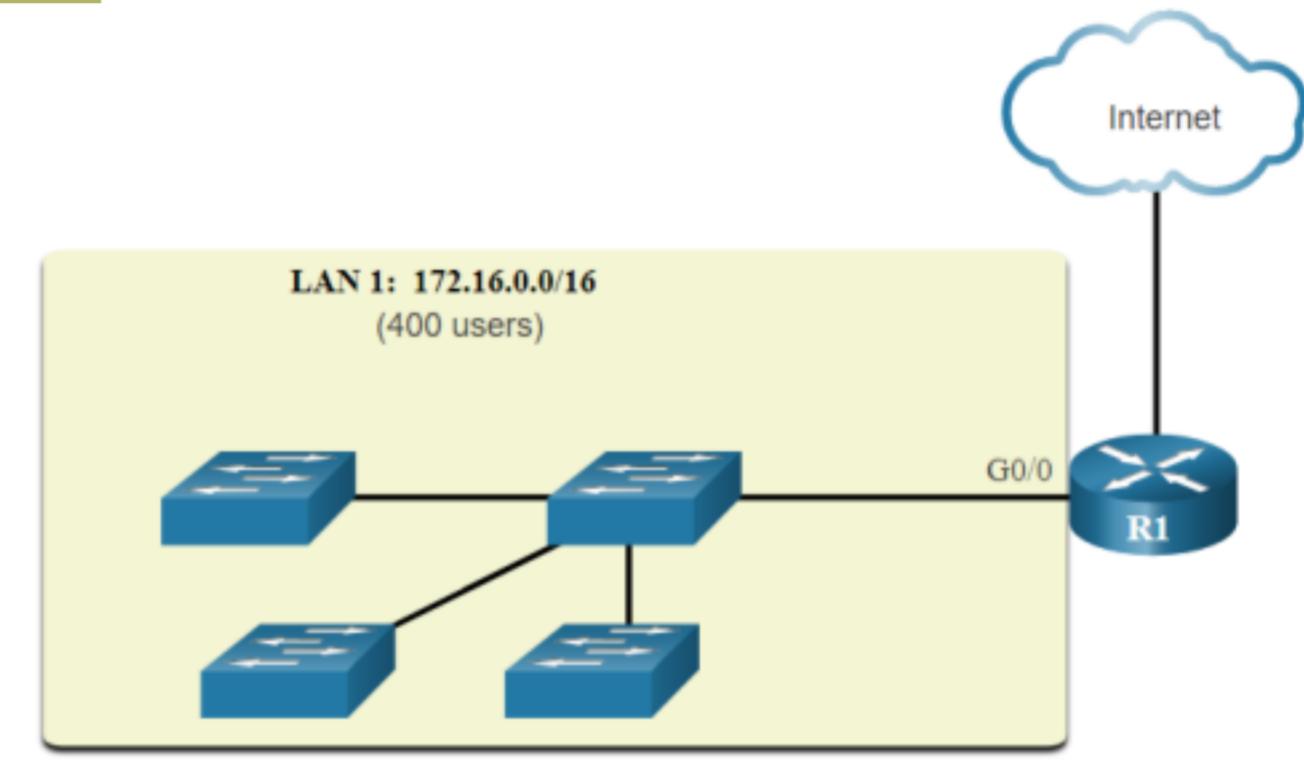


- The only device that stops broadcasts is a router.
- Routers do not propagate broadcasts.
- Each router interface connects to a broadcast domain and broadcasts are only propagated within that specific broadcast domain.

## Network Segmentation

# Problems with Large Broadcast Domains

- A problem with a large broadcast domain is that these hosts can generate excessive broadcasts and negatively affect the network.
- The solution is to reduce the size of the network to create smaller broadcast domains in a process called subnetting.
- Dividing the network address 172.16.0.0 /16 into two subnets of 200 users each: 172.16.0.0 /24 and 172.16.1.0 /24.
- Broadcasts are only propagated within the smaller broadcast domains.

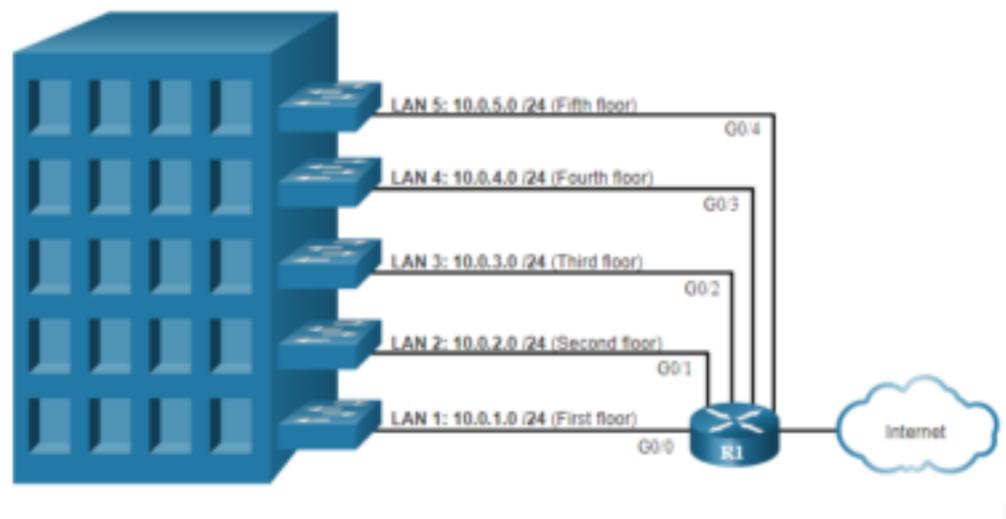


# Network Segmentation

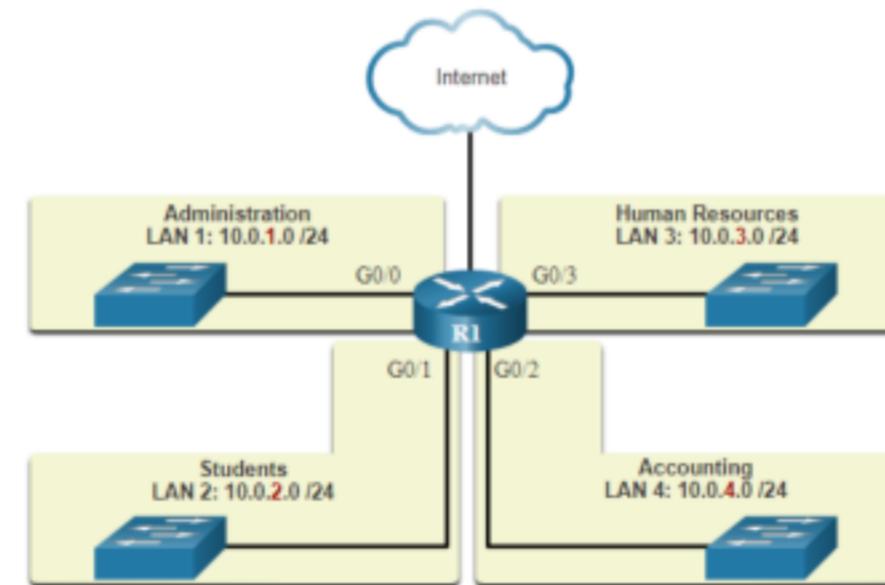
## Reasons for Segmenting Networks

- Subnetting reduces overall network traffic and improves network performance.
- It can be used to implement security policies between subnets.
- Subnetting reduces the number of devices affected by abnormal broadcast traffic.
- Subnets are used for a variety of reasons including by:

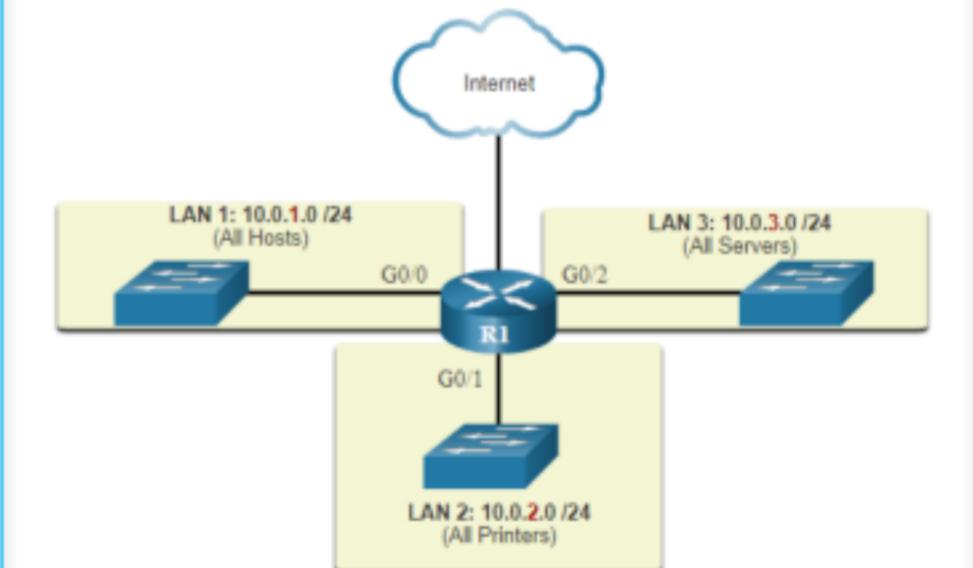
Location



Group or Function



Device Type



# 11.5 Subnet an IPv4 Network

## Subnet an IPv4 Network

### Subnet on an Octet Boundary

- Networks are most easily subnetted at the octet boundary of /8, /16, and /24.
- Notice that using longer prefix lengths decreases the number of hosts per subnet.

Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of hosts
/8	255.0.0.0	nnnnnnnn.hhhhhh.hhhhhh.hhhhhh 11111111.00000000.00000000.00000000	16,777,214
/16	255.255.0.0	nnnnnnnn.nnnnnnnn.hhhhhh.hhhhhh 11111111.11111111.00000000.00000000	65,534
/24	255.255.255.0	nnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhh 11111111.11111111.11111111.00000000	254

## Subnet an IPv4 Network

### Subnet on an Octet Boundary (Cont.)

- In the first table 10.0.0.0/8 is subnetted using /16 and in the second table, a /24 mask.

<b>Subnet Address</b> (256 Possible Subnets)	<b>Host Range</b> (65,534 possible hosts per subnet)	<b>Broadcast</b>
10.0.0.0/16	10.0.0.1 - 10.0.255.254	10.0.255.255
10.1.0.0/16	10.1.0.1 - 10.1.255.254	10.1.255.255
10.2.0.0/16	10.2.0.1 - 10.2.255.254	10.2.255.255
10.3.0.0/16	10.3.0.1 - 10.3.255.254	10.3.255.255
10.4.0.0/16	10.4.0.1 - 10.4.255.254	10.4.255.255
10.5.0.0/16	10.5.0.1 - 10.5.255.254	10.5.255.255
10.6.0.0/16	10.6.0.1 - 10.6.255.254	10.6.255.255
10.7.0.0/16	10.7.0.1 - 10.7.255.254	10.7.255.255
...	...	...
10.255.0.0/16	10.255.0.1 - 10.255.255.254	10.255.255.255

<b>Subnet Address</b> (65,536 Possible Subnets)	<b>Host Range</b> (254 possible hosts per subnet)	<b>Broadcast</b>
10.0.0.0/24	10.0.0.1 - 10.0.0.254	10.0.0.255
10.0.1.0/24	10.0.1.1 - 10.0.1.254	10.0.1.255
10.0.2.0/24	10.0.2.1 - 10.0.2.254	10.0.2.255
...	...	...
10.0.255.0/24	10.0.255.1 - 10.0.255.254	10.0.255.255
10.1.0.0/24	10.1.0.1 - 10.1.0.254	10.1.0.255
10.1.1.0/24	10.1.1.1 - 10.1.1.254	10.1.1.255
10.1.2.0/24	10.1.2.1 - 10.1.2.254	10.1.2.255
...	...	...
10.100.0.0/24	10.100.0.1 - 10.100.0.254	10.100.0.255
...	...	...
10.255.255.0/24	10.255.255.1 - 10.255.255.254	10.255.255.255



## Subnet an IPv4 Network

# Subnet within an Octet Boundary

- Refer to the table to see six ways to subnet a /24 network.

Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of subnets	# of hosts
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn. <b>n</b> hhhhhhh 11111111.11111111.11111111. <b>1</b> 0000000	2	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn. <b>nn</b> hhhhhh 11111111.11111111.11111111. <b>11</b> 000000	4	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn. <b>nnn</b> hhhh 11111111.11111111.11111111. <b>111</b> 00000	8	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn. <b>nnnn</b> hhh 11111111.11111111.11111111. <b>1111</b> 0000	16	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn. <b>nnnnn</b> hh 11111111.11111111.11111111. <b>11111</b> 000	32	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn. <b>nnnnnn</b> hh 11111111.11111111.11111111. <b>111111</b> 00	64	2

Subnet an IPv4 Network

## Video – The Subnet Mask

- This video will demonstrate the process of subnetting.



Subnet an IPv4 Network

## Video – Subnet with the Magic Number

- This video will demonstrate subnetting with the magic number.



## Packet Tracer – Subnet an IPv4 Network

In this Packet Tracer, you will do the following:

- Design an IPv4 Network Subnetting Scheme
- Configure the Devices
- Test and Troubleshoot the Network

# 11.6 Subnet a Slash 16 and a Slash 8 Prefix



## Subnet a Slash 16 and a Slash 8 Prefix Create Subnets with a Slash 16 prefix

- The table highlights all the possible scenarios for subnetting a /16 prefix.

Prefix Length	Subnet Mask	Network Address (n = network, h = host)	# of subnets	# of hosts
/17	255.255.128.0	nnnnnnnn.nnnnnnnn.nhhhhhhh.hhhhhhhh 11111111.11111111.10000000.00000000	2	32766
/18	255.255.192.0	nnnnnnnn.nnnnnnnn.nnhhhhhh.hhhhhhhh 11111111.11111111.11000000.00000000	4	16382
/19	255.255.224.0	nnnnnnnn.nnnnnnnn.nnnhhhhh.hhhhhhhh 11111111.11111111.11100000.00000000	8	8190
/20	255.255.240.0	nnnnnnnn.nnnnnnnn.nnnnhhhh.hhhhhhhh 11111111.11111111.11110000.00000000	16	4094
/21	255.255.248.0	nnnnnnnn.nnnnnnnn.nnnnnhhh.hhhhhhhh 11111111.11111111.11111000.00000000	32	2046
/22	255.255.252.0	nnnnnnnn.nnnnnnnn.nnnnnn hh.hhhhhhhh 11111111.11111111.11111100.00000000	64	1022
/23	255.255.254.0	nnnnnnnn.nnnnnnnn.nnnnnnnh.hhhhhhhh 11111111.11111111.11111110.00000000	128	510
/24	255.255.255.0	nnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh 11111111.11111111.11111111.00000000	256	254
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.nhhhhhhh 11111111.11111111.11111111.10000000	512	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnhhhhhhh 11111111.11111111.11111111.11000000	1024	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnhhhhh 11111111.11111111.11111111.11100000	2048	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnhhhh 11111111.11111111.11111111.11110000	4096	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnhhh 11111111.11111111.11111111.11111000	8192	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnn hh 11111111.11111111.11111111.11111100	16384	2



## Subnet a Slash 16 and a Slash 8 Prefix Create 100 Subnets with a Slash 16 prefix

Consider a large enterprise that requires at least 100 subnets and has chosen the private address 172.16.0.0/16 as its internal network address.

- The figure displays the number of subnets that can be created when borrowing bits from the third octet and the fourth octet.
- Notice there are now up to 14 host bits that can be borrowed (i.e., last two bits cannot be borrowed).

To satisfy the requirement of 100 subnets for the enterprise, 7 bits (i.e.,  $2^7 = 128$  subnets) would need to be borrowed (for a total of 128 subnets).

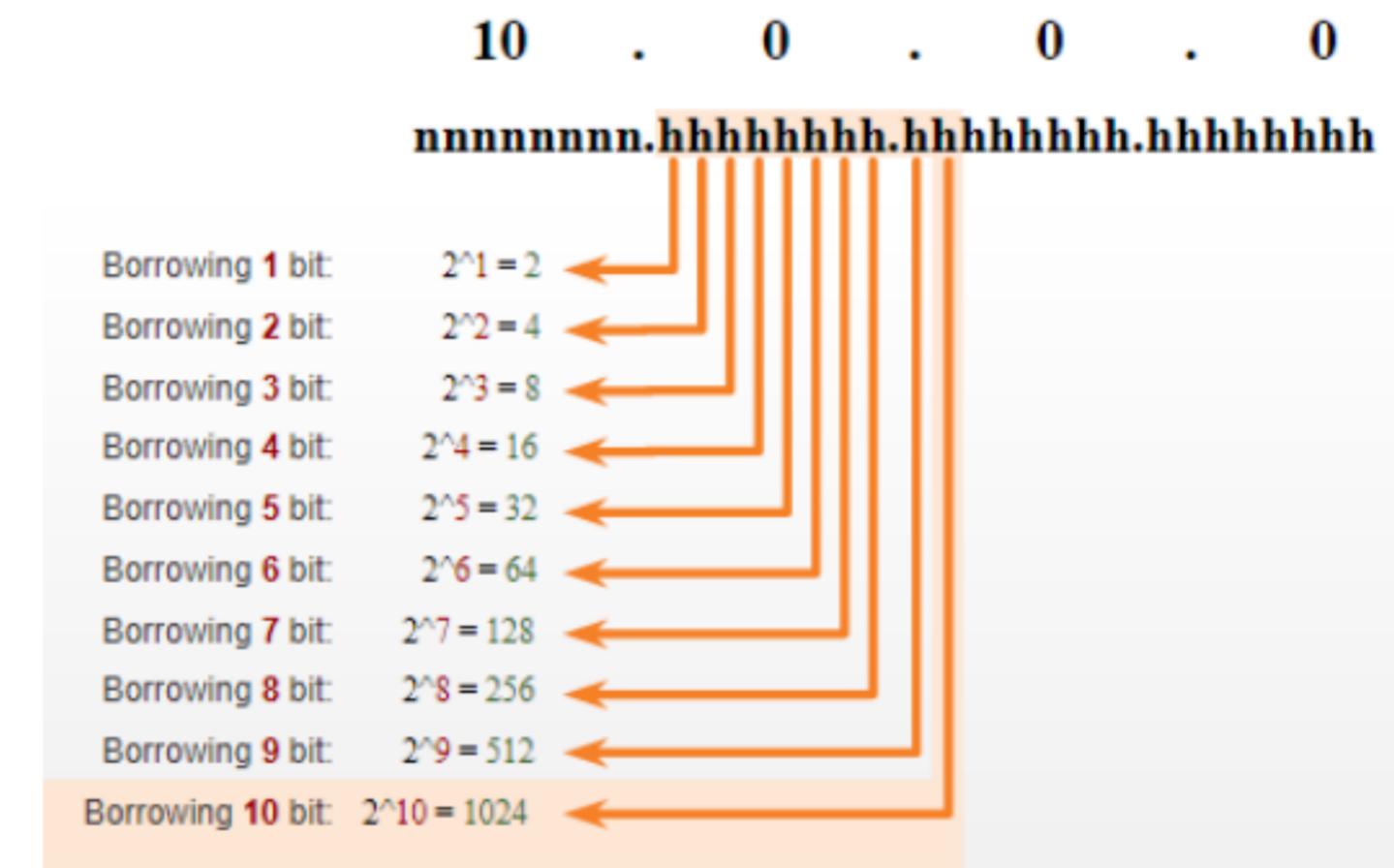


## Subnet a Slash 16 and a Slash 8 Prefix Create 1000 Subnets with a Slash 8 prefix

Consider a small ISP that requires 1000 subnets for its clients using network address 10.0.0.0/8 which means there are 8 bits in the network portion and 24 host bits available to borrow toward subnetting.

- The figure displays the number of subnets that can be created when borrowing bits from the second and third.
- Notice there are now up to 22 host bits that can be borrowed (i.e., last two bits cannot be borrowed).

To satisfy the requirement of 1000 subnets for the enterprise, 10 bits (i.e.,  $2^{10}=1024$  subnets) would need to be borrowed (for a total of 128 subnets)



Subnet a Slash 16 and a Slash 8 Prefix

## Video – Subnet Across Multiple Octets

This video will demonstrate creating subnets across multiple octets.



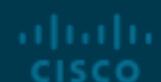
## Subnet a Slash 16 and a Slash 8 Prefix **Lab – Calculate IPv4 Subnets**

In this lab, you will complete the following objectives:

- Part 1: Determine IPv4 Address Subnetting
- Part 2: Calculate IPv4 Address Subnetting



# 11.7 Subnet to Meet Requirements

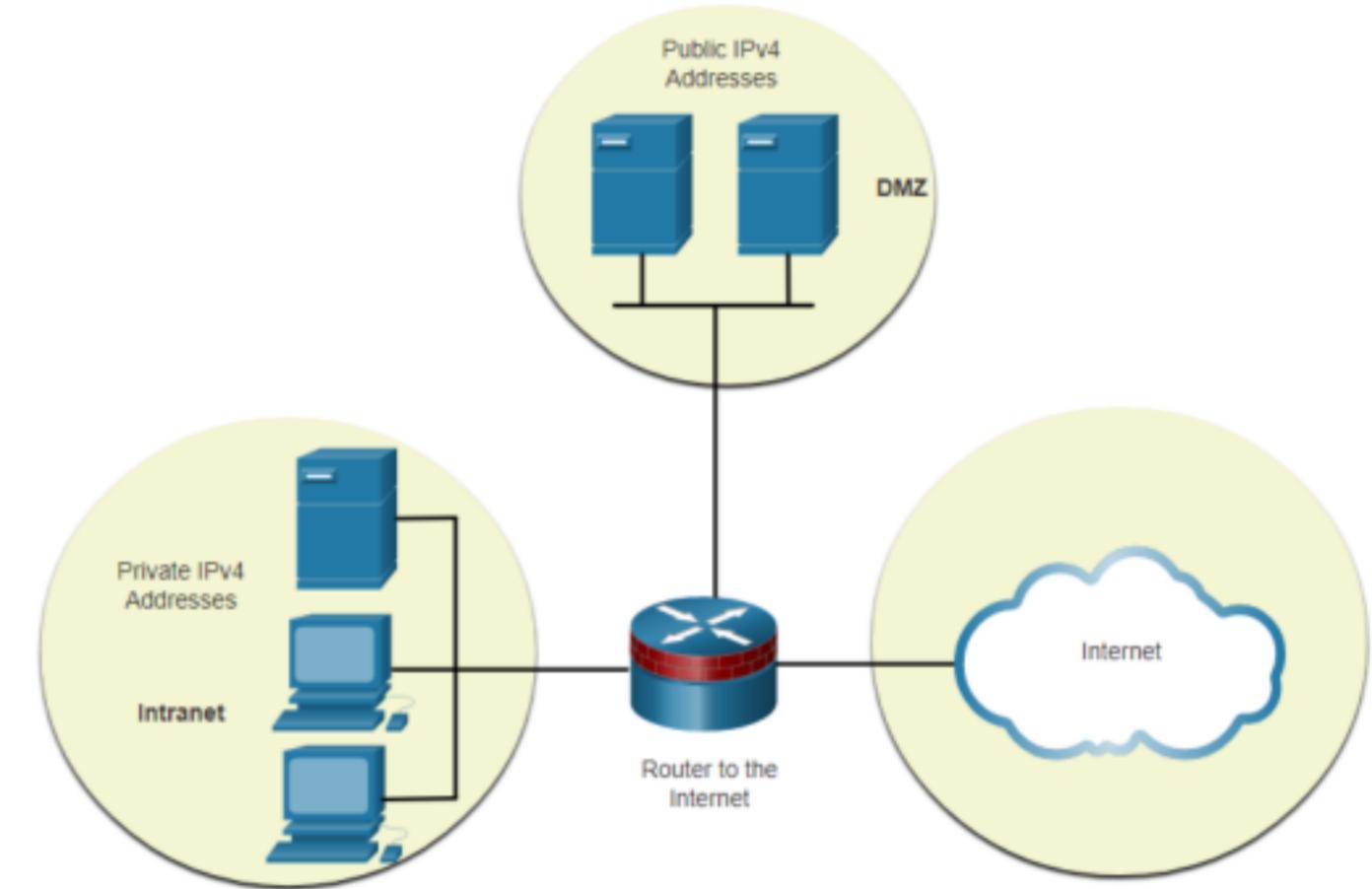


Subnet to Meet Requirements

## Subnet Private versus Public IPv4 Address Space

Enterprise networks will have an:

- Intranet - A company's internal network typically using private IPv4 addresses.
- DMZ – A companies internet facing servers. Devices in the DMZ use public IPv4 addresses.
- A company could use the 10.0.0.0/8 and subnet on the /16 or /24 network boundary.
- The DMZ devices would have to be configured with public IP addresses.



## Subnet to Meet Requirements

### Minimize Unused Host IPv4 Addresses and Maximize Subnets

There are two considerations when planning subnets:

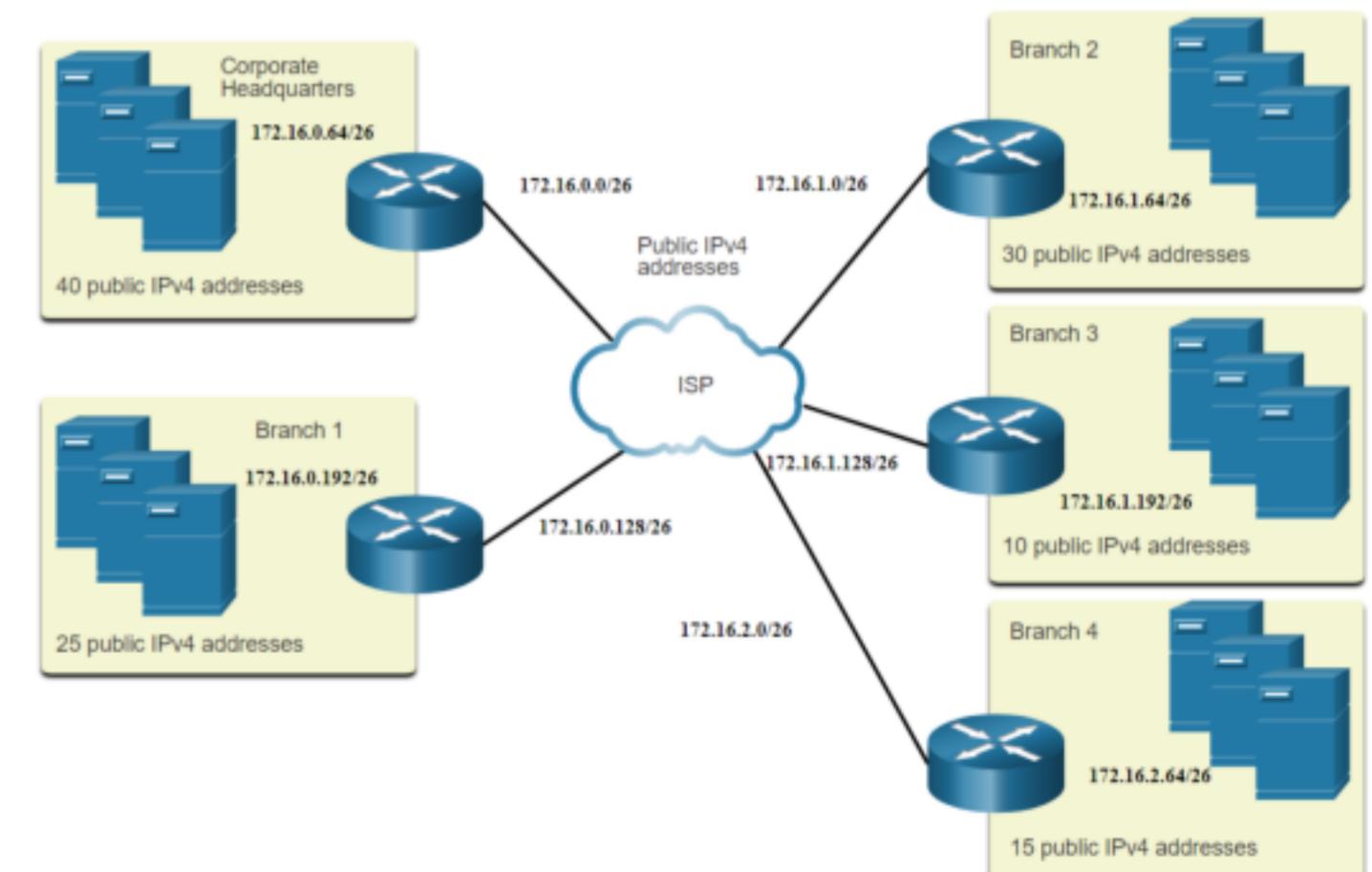
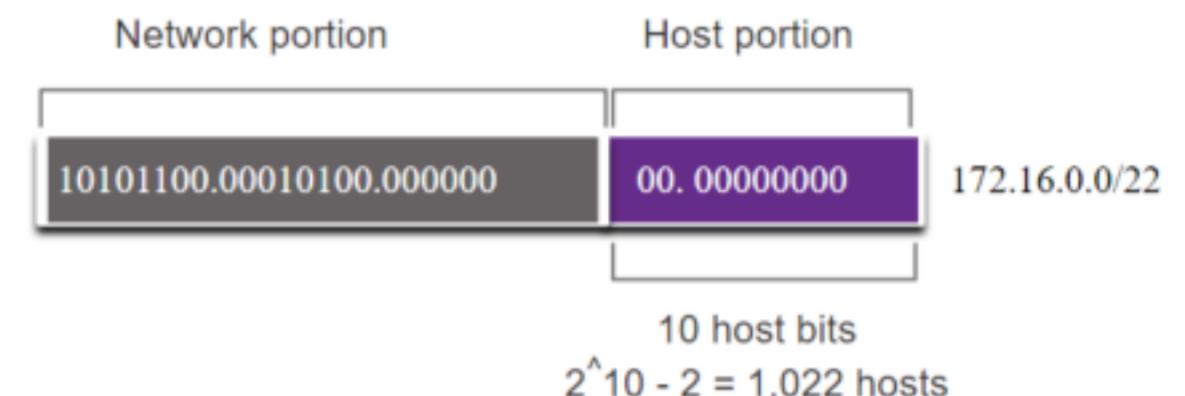
- The number of host addresses required for each network
- The number of individual subnets needed

Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of subnets	# of hosts
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn. <b>n</b> hhhhhhh 11111111.11111111.11111111. <b>1</b> 0000000	2	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn. <b>nn</b> hhhhhhh 11111111.11111111.11111111. <b>11</b> 000000	4	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn. <b>nnn</b> hhhhhhh 11111111.11111111.11111111. <b>111</b> 00000	8	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn. <b>nnnn</b> hhh 11111111.11111111.11111111. <b>1111</b> 0000	16	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn. <b>nnnnn</b> hh 11111111.11111111.11111111. <b>11111</b> 000	32	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn. <b>nnnnnn</b> hh 11111111.11111111.11111111. <b>111111</b> 00	64	2



## Subnet to Meet Requirements Example: Efficient IPv4 Subnetting

- In this example, corporate headquarters has been allocated a public network address of 172.16.0.0/22 (10 host bits) by its ISP providing 1,022 host addresses.
- There are five sites and therefore five internet connections which means the organization requires 10 subnets with the largest subnet requires 40 addresses.
- It allocated 10 subnets with a /26 (i.e., 255.255.255.192) subnet mask.



Subnet to Meet Requirements

## Packet Tracer – Subnetting Scenario

In this Packet Tracer, you will do the following:

- Design an IP Addressing Scheme
- Assign IP Addresses to Network Devices and Verify Connectivity



# 11.8 VLSM



# VLSM Video – VLSM Basics

- This video will explain VLSM basics.



# VLSM Video – VLSM Example

- This video will demonstrate creating subnets specific to the needs of the network.

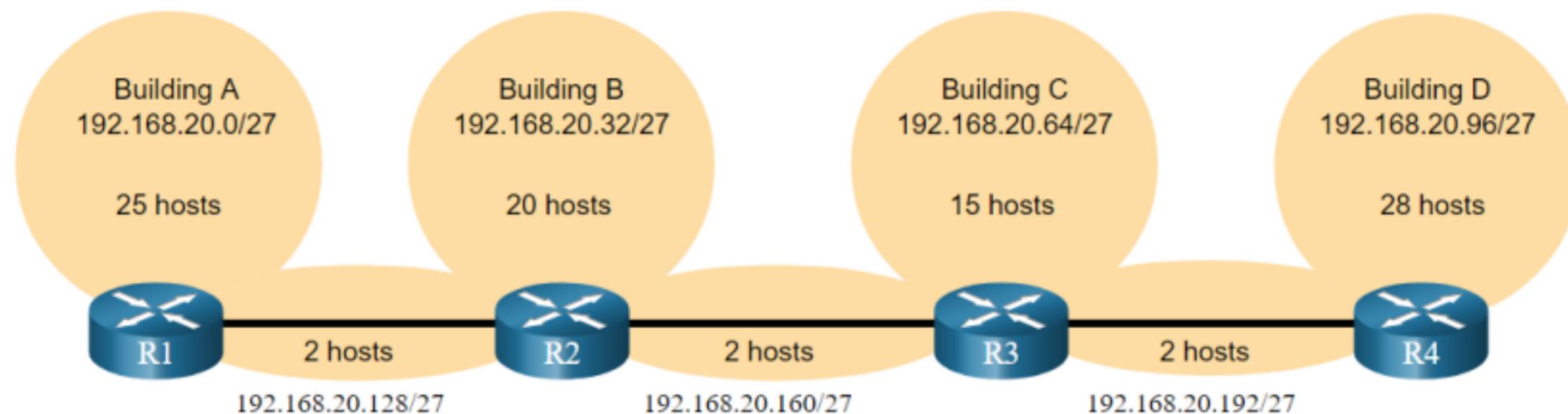


## VLSM

# IPv4 Address Conservation

Given the topology, 7 subnets are required (i.e, four LANs and three WAN links) and the largest number of host is in Building D with 28 hosts.

- A /27 mask would provide 8 subnets of 30 host IP addresses and therefore support this topology.

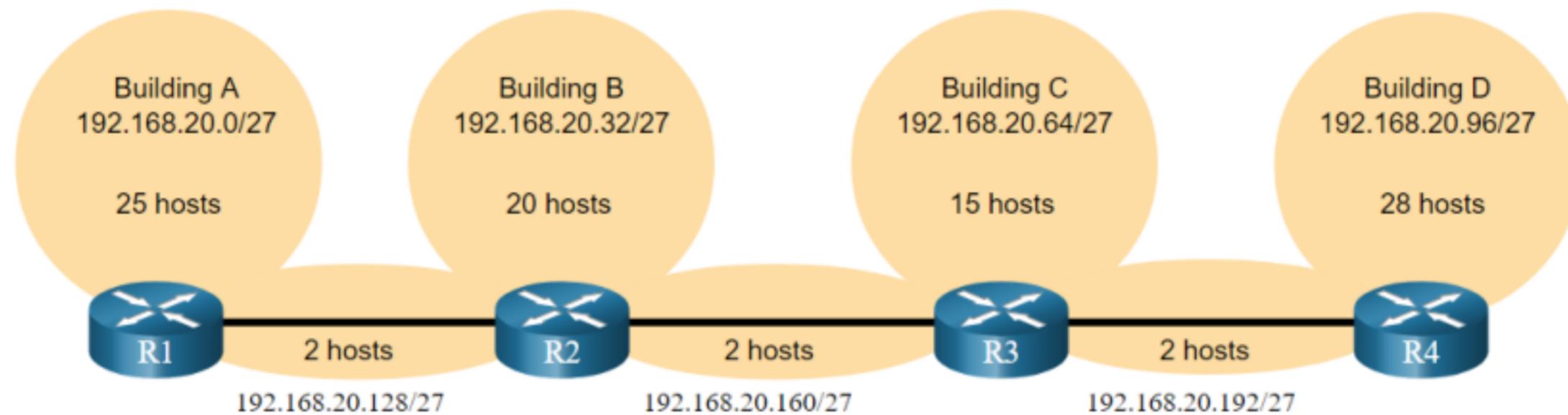


VLSM

## IPv4 Address Conservation (Cont.)

However, the point-to-point WAN links only require two addresses and therefore waste 28 addresses each for a total of 84 unused addresses.

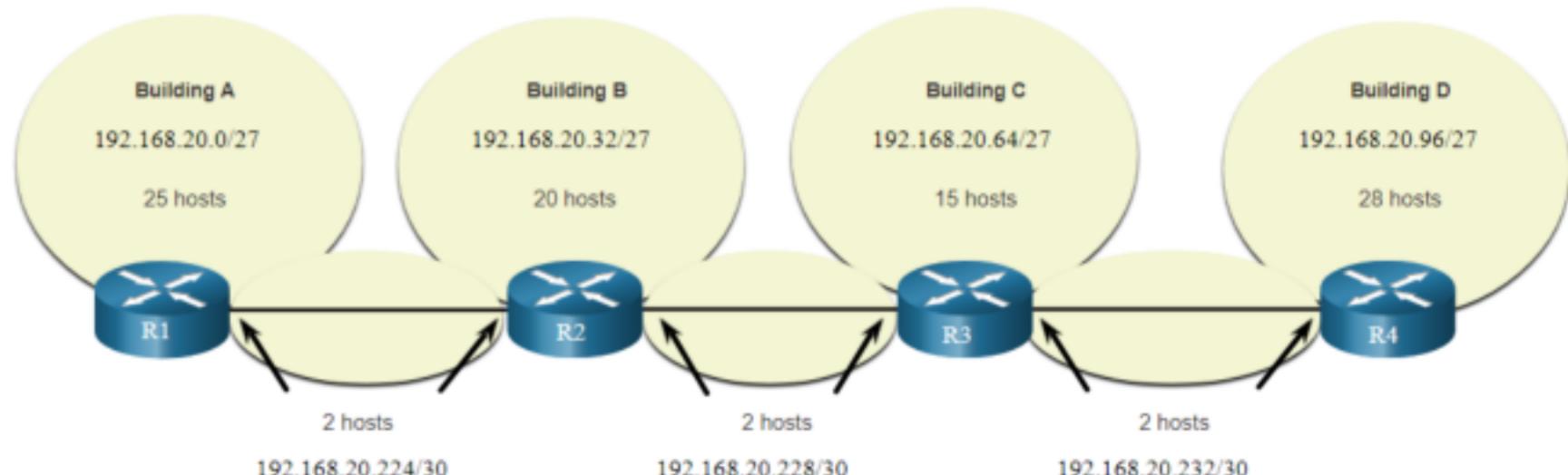
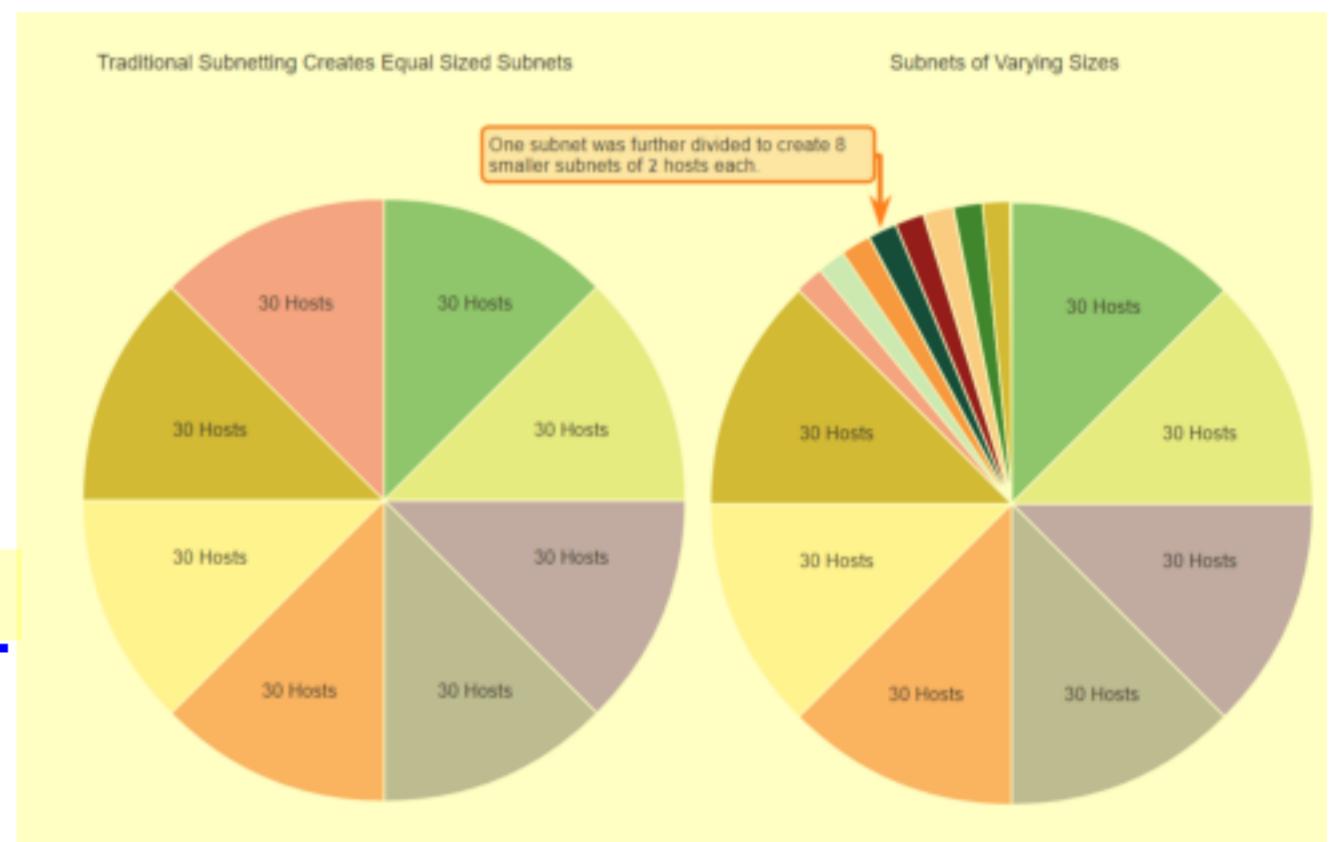
Host portion  
 $2^5 - 2 = 30$  host IP addresses per subnet  
 $30 - 2 = 28$   
Each WAN subnet wastes 28 addresses  
 $28 \times 3 = 84$   
84 addresses are unused



- Applying a traditional subnetting scheme to this scenario is not very efficient and is wasteful.
- VLSM was developed to avoid wasting addresses by enabling us to subnet a subnet.

# VLSM

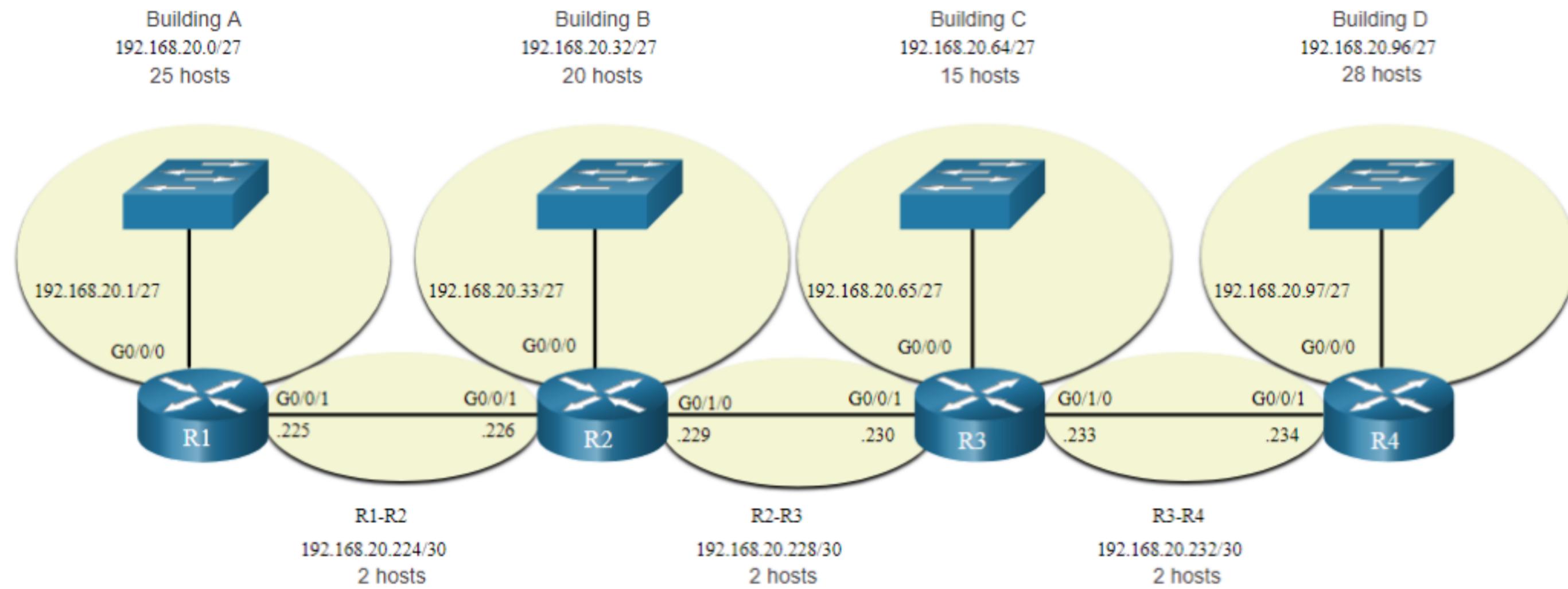
- The left side displays the traditional subnetting scheme (i.e., the same subnet mask) while the right side illustrates how VLSM can be used to subnet a subnet and divided the last subnet into eight /30 subnets.
- When using VLSM, always begin by satisfying the host requirements of the largest subnet and continue subnetting until the host requirements of the smallest subnet are satisfied.
- The resulting topology with VLSM applied.



## VLSM

# VLSM Topology Address Assignment

- Using VLSM subnets, the LAN and inter-router networks can be addressed without unnecessary waste as shown in the logical topology diagram.



# 11.9 Structured Design



## Structured Design

# IPv4 Network Address Planning

IP network planning is crucial to develop a scalable solution to an enterprise network.

- To develop an IPv4 network wide addressing scheme, you need to know how many subnets are needed, how many hosts a particular subnet requires, what devices are part of the subnet, which parts of your network use private addresses, and which use public, and many other determining factors.

Examine the needs of an organization's network usage and how the subnets will be structured.

- Perform a network requirement study by looking at the entire network to determine how each area will be segmented.
- Determine how many subnets are needed and how many hosts per subnet.
- Determine DHCP address pools and Layer 2 VLAN pools.

## Structured Design Device Address Assignment

Within a network, there are different types of devices that require addresses:

- **End user clients** – Most use DHCP to reduce errors and burden on network support staff. IPv6 clients can obtain address information using DHCPv6 or SLAAC.
- **Servers and peripherals** – These should have a predictable static IP address.
- **Servers that are accessible from the internet** – Servers must have a public IPv4 address, most often accessed using NAT.
- **Intermediary devices** – Devices are assigned addresses for network management, monitoring, and security.
- **Gateway** – Routers and firewall devices are gateway for the hosts in that network.

When developing an IP addressing scheme, it is generally recommended that you have a set pattern of how addresses are allocated to each type of device.

## Structured Design

# Packet Tracer – VLSM Design and Implementation Practice

In this Packet Tracer, you will do the following:

- Examine the Network Requirements
- Design the VLSM Addressing Scheme
- Assign IP Addresses to Devices and Verify Connectivity



# 11.10 Module Practice and Quiz



## Structured Design

# Packet Tracer – Design and Implement a VLSM Addressing Scheme

In this Packet Tracer, you will do the following:

- Design a VLSM IP addressing scheme given requirements
- Configure addressing on network devices and hosts
- Verify IP connectivity
- Troubleshoot connectivity issues as required.



## Structured Design

# Lab - Design and Implement a VLSM Addressing Scheme

In this lab, you will complete the following objectives:

- Examine Network Requirements
- Design the VLSM Address Scheme
- Cable and Configure the IPv4 Network



## Module Practice and Quiz

# What did I learn in this module?

- The IP addressing structure consists of a 32-bit hierarchical network address that identifies a network and a host portion. Network devices use a process called ANDing using the IP address and associated subnet mask to identify the network and host portions.
- Destination IPv4 packets can be unicast, broadcast, and multicast.
- There are globally routable IP addresses as assigned by the IANA and there are three ranges of private IP network addresses that cannot be routed globally but can be used on all internal private networks.
- Reduce large broadcast domains using subnets to create smaller broadcast domains, reduce overall network traffic, and improve network performance.
- Create IPv4 subnets using one or more of the host bits as network bits. However, networks are most easily subnetted at the octet boundary of /8, /16, and /24.
- Larger networks can be subnetted at the /8 or /16 boundaries.
- Use VLSM to reduce the number of unused host addresses per subnet.



## Module Practice and Quiz

# What did I learn in this module? (Cont.)

- VLSM allows a network space to be divided into unequal parts. Always begin by satisfying the host requirements of the largest subnet. Continue subnetting until the host requirements of the smallest subnet are satisfied.
- When designing a network addressing scheme, consider internal, DMZ, and external requirements. Use a consistent internal IP addressing scheme with a set pattern of how addresses are allocated to each type of device.



## New Terms and Commands

- prefix length
- logical AND
- network address
- broadcast address
- first usable address
- last usable address
- unicast, broadcast, and multicast transmissions
- private addresses
- public addresses
- Network Address Translation (NAT)
- loopback addresses
- Automatic Private IP Addressing (APIPA)  
addresses
- classful addressing (Class A, B, C, D, and E)

Internet Assigned Numbers Authority (IANA)  
Regional Internet Registries (RIRs)  
AfriNIC, APNIC, ARIN, LACNIC, and RIPE NCC  
broadcast domains  
subnets  
octet boundary  
variable-length subnet mask (VLSM)



## Lab – Converting IPv4 Addresses to Binary

### Objectives

- Part 1: Convert IPv4 Addresses from Dotted Decimal to Binary
- Part 2: Use Bitwise ANDing Operation to Determine Network Addresses
- Part 3: Apply Network Address Calculations

### Background / Scenario

Every IPv4 address is comprised of two parts: a network portion and a host portion. The network portion of an address is the same for all devices that reside in the same network. The host portion identifies a specific host within a given network. The subnet mask is used to determine the network portion of an IP address. Devices on the same network can communicate directly; devices on different networks require an intermediary Layer 3 device, such as a router, to communicate.

To understand the operation of devices on a network, we need to look at addresses the way devices do—in binary notation. To do this, we must convert the dotted decimal form of an IP address and its subnet mask to binary notation. After this has been done, we can use the bitwise ANDing operation to determine the network address.

This lab provides instructions on how to determine the network and host portion of IP addresses by converting addresses and subnet masks from dotted decimal to binary, and then using the bitwise ANDing operation. You will then apply this information to identify addresses in the network.

### Part 1: Convert IPv4 Addresses from Dotted Decimal to Binary

In Part 1, you will convert decimal numbers to their binary equivalent.

After you have mastered this activity, you will convert IPv4 addresses and subnet masks from dotted decimal to their binary form.

#### Step 1: Convert decimal numbers to their binary equivalent.

Fill in the following table by converting the decimal number to an 8-bit binary number. The first number has been completed for your reference. Recall that the eight binary bit values in an octet are based on the powers of 2, and from left to right are 128, 64, 32, 16, 8, 4, 2, and 1.

Decimal	Binary
192	11000000
168	
10	
255	
2	

## Lab – Converting IPv4 Addresses to Binary

---

### Step 2: Convert the IPv4 addresses to their binary equivalent.

An IPv4 address can be converted using the same technique you used above. Fill in the table below with the binary equivalent of the addresses provided. To make your answers easier to read, separate the binary octets with a period.

Decimal	Binary
192.168.10.10	11000000.10101000.00001010.00001010
209.165.200.229	
172.16.18.183	
10.86.252.17	
255.255.255.128	
255.255.192.0	

### Part 2: Use Bitwise ANDing Operation to Determine Network Addresses

In Part 2, you will use the bitwise ANDing operation to calculate the network address for the provided host addresses.

You will first need to convert an IPv4 decimal address and subnet mask to their binary equivalent. Once you have the binary form of the network address, convert it to its decimal form.

**Note:** The ANDing process compares the binary value in each bit position of the 32-bit host IP with the corresponding position in the 32-bit subnet mask. If there two 0s or a 0 and a 1, the ANDing result is 0. If there are two 1s, the result is a 1, as shown in the example here.

#### Example: Determine the number of bits to use to calculate the network address.

Description	Decimal	Binary
IP Address	192.168.10.131	11000000.10101000.00001010.10000011
Subnet Mask	255.255.255.192	11111111.11111111.11111111.11000000
Network Address	192.168.10.128	11000000.10101000.00001010.10000000

How do you determine what bits to use to calculate the network address?

Bit “1”

In the example above, how many bits are used to calculate the network address? 8+8+8+2

Lab – Converting IPv4 Addresses to Binary

---

**Step 1: Use the ANDing operation to determine the network address.**

- a. Enter the missing information into the table below:

Description	Decimal	Binary
IP Address	172.16.145.29	
Subnet Mask	255.255.0.0	
Network Address	172.16.0.0	

- b. Enter the missing information into the table below:

Description	Decimal	Binary
IP Address	192.168.10.10	
Subnet Mask	255.255.255.0	
Network Address		

- c. Enter the missing information into the table below:

Description	Decimal	Binary
IP Address	192.168.68.210	11010010
Subnet Mask	255.255.255.128	10000000
Network Address	192.168.68.128	1

- d. Enter the missing information into the table below:

Description	Decimal	Binary
IP Address	172.16.188.15	10111100
Subnet Mask	255.255.240.0	11110000
Network Address	172.16.176.0	10110000

Way 2

Divide into different subnetworks

So if the IP address is smaller than subnet

Description	Decimal	Binary
IP Address	10.172.2.8	10101
Subnet Mask	255.224.0.0 = /11	11100000
Network Address	10.	

/25

128/0

/26

0 64 128 192

### Part 3: Apply Network Address Calculations

In Part 3, you must calculate the network address for the given IP addresses and subnet masks. After you have the network address, you should be able to determine the responses needed to complete the lab.

#### Step 1: Determine whether IP addresses are on same network.

- a. You are configuring two PCs for your network. PC-A is given an IP address of 192.168.1.18, and PC-B is given an IP address of 192.168.1.33. Both PCs receive a subnet mask of 255.255.255.240.

What is the network address for PC-A? 192.168.1.16

What is the network address for PC-B? 192.168.1.32

Will these PCs be able to communicate directly with each other? No

What is the highest address that can be given to PC-B that allows it to be on the same network as PC-A?

192.168.1.30

- b. You are configuring two PCs for your network. PC-A is given an IP address of 10.0.0.16, and PC-B is given an IP address of 10.1.14.68. Both PCs receive a subnet mask of 255.254.0.0.

What is the network address for PC-A? \_\_\_\_\_

What is the network address for PC-B? \_\_\_\_\_

Will these PCs be able to communicate directly with each other? \_\_\_\_\_

What is the lowest address that can be given to PC-B that allows it to be on the same network as PC-A?

---

#### Step 2: Identify the default gateway address.

- a. Your company has a policy to use the **first** IP address in a network as the default gateway address. A host on the local-area network (LAN) has an IP address of 172.16.140.24 and a subnet mask of 255.255.192.0.

What is the network address for this network?

\_\_\_\_\_

What is the default gateway address for this host?

- b. Your company has a policy to use the **first** IP address in a network as the default gateway address. You have been instructed to configure a new server with an IP address of 192.168.184.227 and a subnet mask of 255.255.255.248.

What is the network address for this network?

\_\_\_\_\_

What is the default gateway for this server?

---

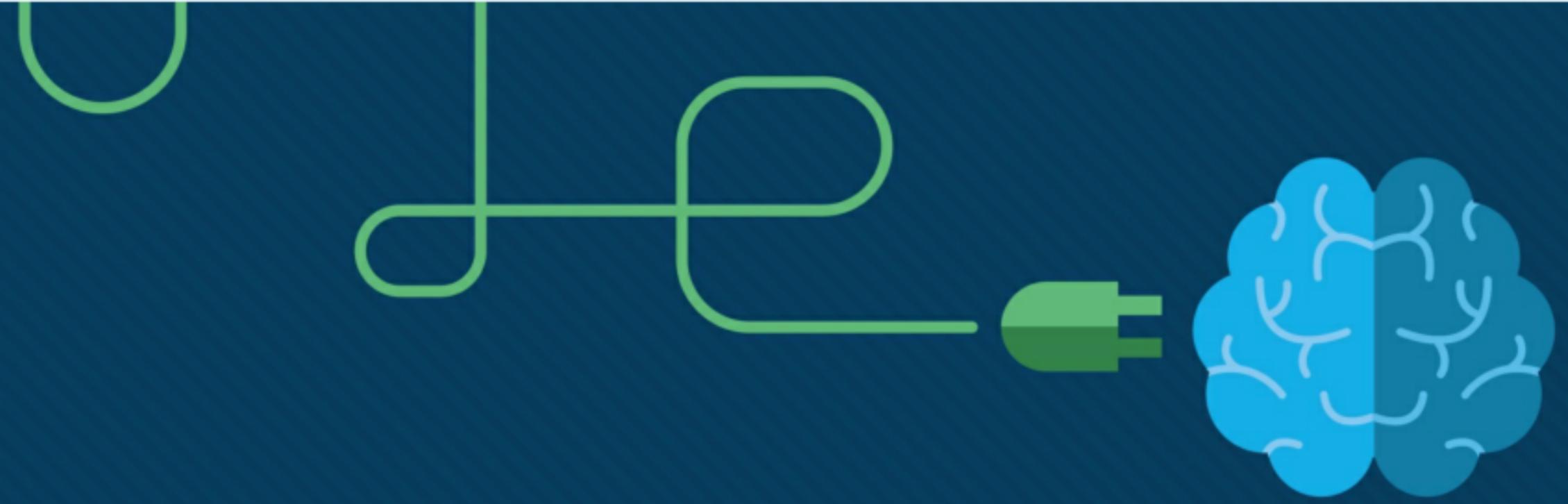
#### Reflection

Why is the subnet mask important in determining the network address?



# Module 6: Data Link Layer

Introduction to Networks v7.0  
(ITN)



# Module Objectives

**Module Title:** Data Link Layer

**Module Objective:** Explain how media access control in the data link layer supports communication across networks.

Topic Title	Topic Objective
Purpose of the Data Link Layer	Describe the purpose and function of the data link layer in preparing communication for transmission on specific media.
Topologies	Compare the characteristics of media access control methods on WAN and LAN topologies.
Data Link Frame	Describe the characteristics and functions of the data link frame.

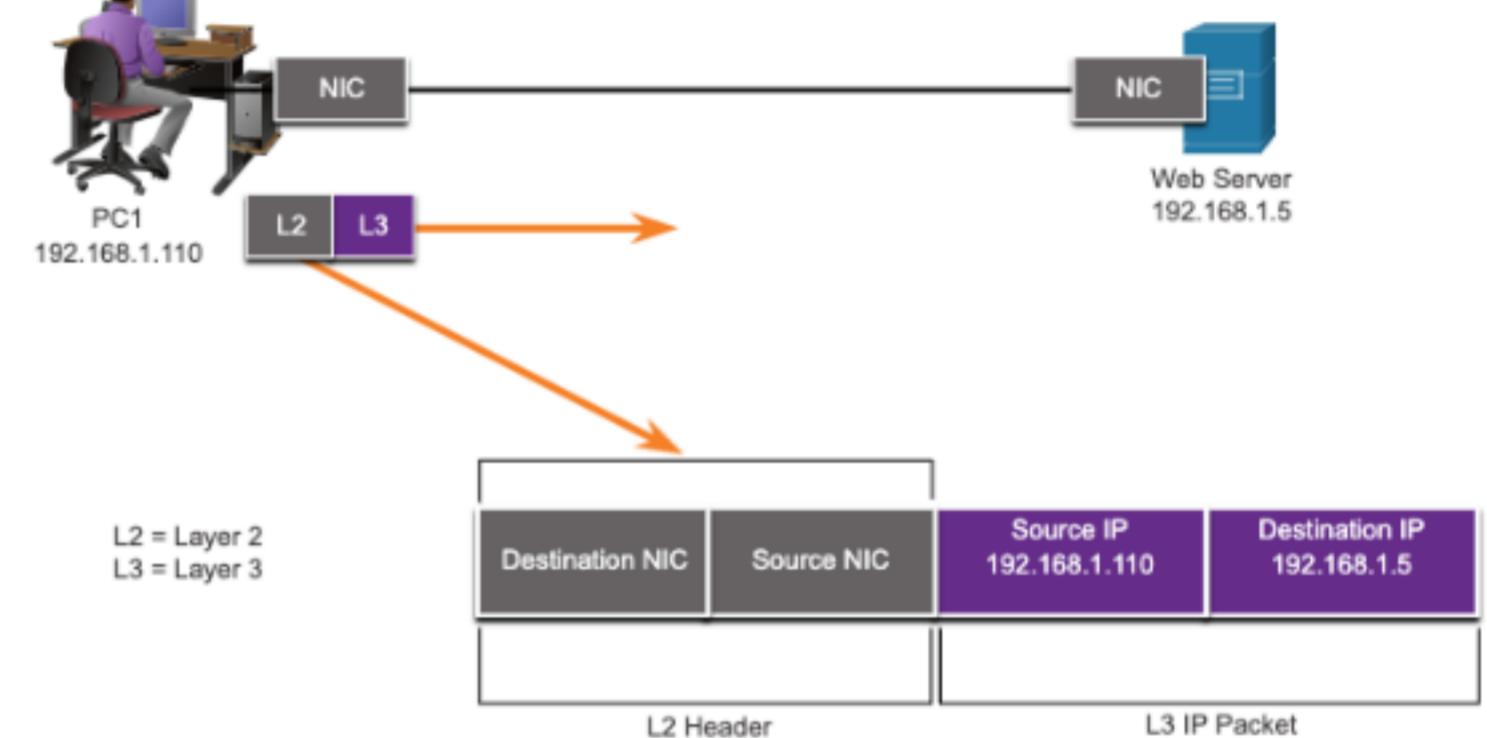
# 6.1 Purpose of the Data Link Layer



## Purpose of the Data Link Layer

# The Data Link Layer

- The Data Link layer is responsible for communications between end-device network interface cards.
- It allows upper layer protocols to access the physical layer media and encapsulates Layer 3 packets (IPv4 and IPv6) into Layer 2 Frames.
- It also performs error detection and rejects corrupts frames.



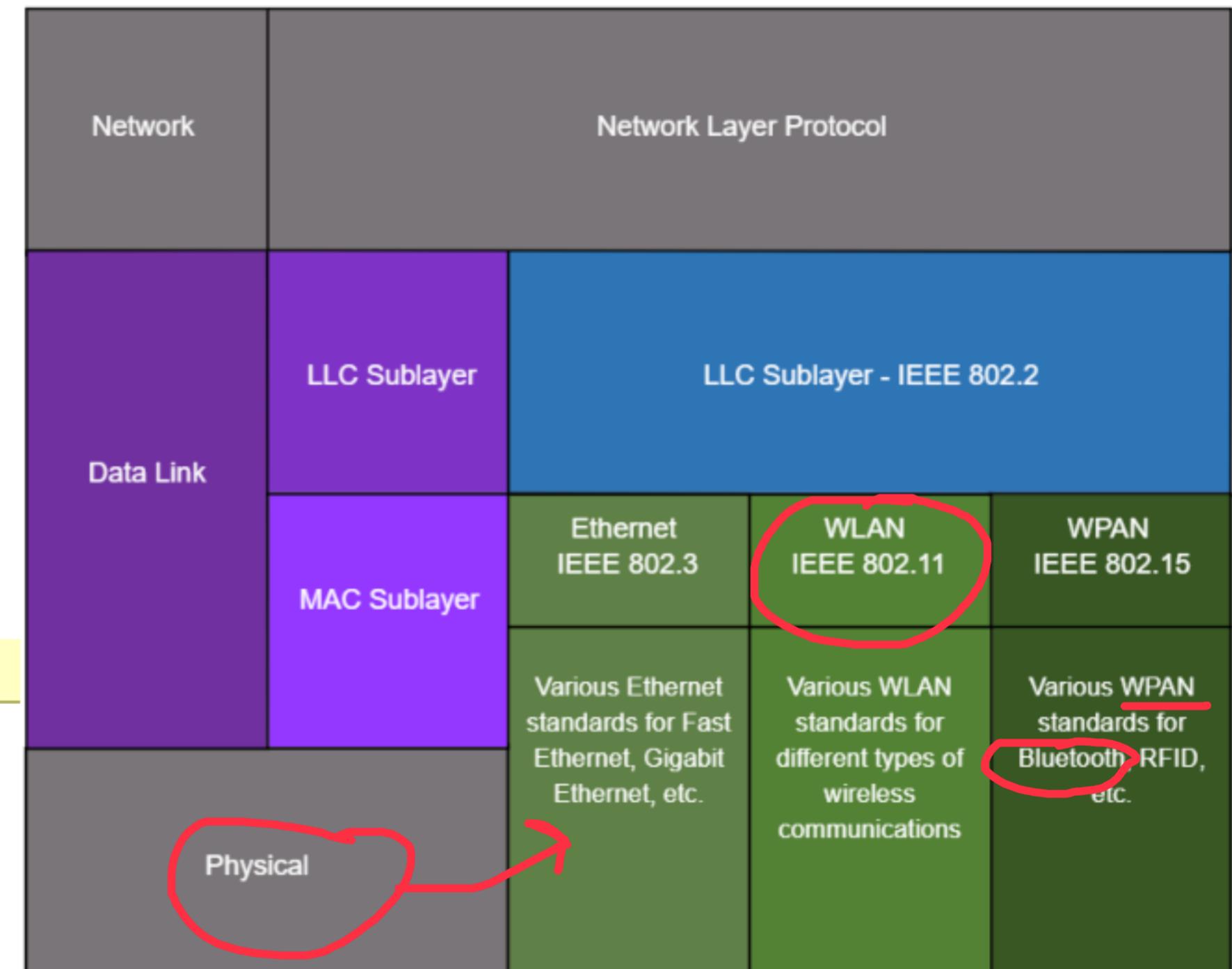
## Purpose of the Data Link Layer

# IEEE 802 LAN/MAN Data Link Sublayers

IEEE 802 LAN/MAN standards are specific to the type of network (Ethernet, WLAN, WPAN, etc).

The Data Link Layer consists of two sublayers. **Logical Link Control (LLC)** and **Media Access Control (MAC)**.

- The LLC sublayer communicates between the networking software at the upper layers and the device hardware at the lower layers.
- The MAC sublayer is responsible for data encapsulation and media access control.



## Purpose of the Data Link Layer Providing Access to Media

Packets exchanged between nodes may experience numerous data link layers and media transitions.

At each hop along the path, a router performs four basic Layer 2 functions:

- Accepts a frame from the network medium.
- De-encapsulates the frame to expose the encapsulated packet.
- Re-encapsulates the packet into a new frame.
- Forwards the new frame on the medium of the next network segment.

## Purpose of the Data Link Layer **Data Link Layer Standards**

Data link layer protocols are defined by engineering organizations:

- Institute for Electrical and Electronic Engineers (IEEE).
- International Telecommunications Union (ITU).
- International Organizations for Standardization (ISO).
- American National Standards Institute (ANSI).



# 6.2 Topologies



## Physical and Logical Topologies

The topology of a network is the arrangement and relationship of the network devices and the interconnections between them.

There are two types of topologies used when describing networks:

- **Physical topology** – shows physical connections and how devices are interconnected.
- **Logical topology** – identifies the virtual connections between devices using device interfaces and IP addressing schemes.

## Topologies WAN Topologies

There are three common physical WAN topologies:

- **Point-to-point** – the simplest and most common WAN topology. Consists of a permanent link between two endpoints.
- **Hub and spoke** – similar to a star topology where a central site interconnects branch sites through point-to-point links.
- **Mesh** – provides high availability but requires every end system to be connected to every other end system.

## Point-to-Point WAN Topology

- Physical point-to-point topologies directly connect two nodes.
- The nodes may not share the media with other hosts.
- Because all frames on the media can only travel to or from the two nodes, Point-to-Point WAN protocols can be very simple.



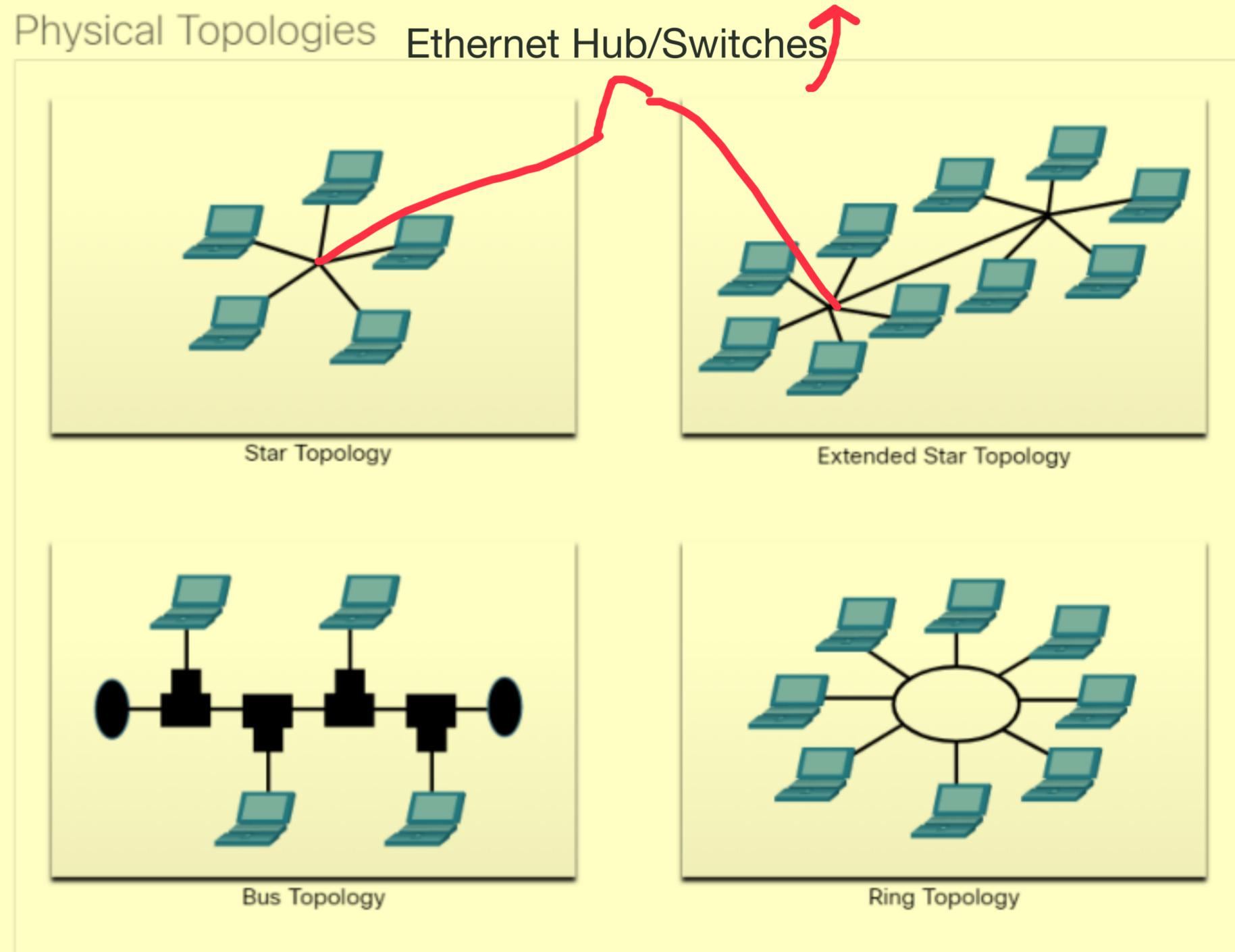
## Topologies

# LAN Topologies

End devices on LANs are typically interconnected using a star or extended star topology. Star and extended star topologies are easy to install, very scalable and easy to troubleshoot.

Early Ethernet and Legacy Token Ring technologies provide two additional topologies:

- **Bus** – All end systems chained together and terminated on each end.
- **Ring** – Each end system is connected to its respective neighbors to form a ring.



## Half and Full Duplex Communication



### Half-duplex communication

- Only allows one device to send or receive at a time on a shared medium.
- Used on WLANs and legacy bus topologies with Ethernet hubs.



### Full-duplex communication

- Allows both devices to simultaneously transmit and receive on a shared medium.
- Ethernet switches operate in full-duplex mode.



# Topologies Access Control Methods

## Contention-based access

All nodes operating in half-duplex, competing for use of the medium. Examples are:

- Carrier sense multiple access with collision detection (CSMA/CD) as used on legacy bus-topology Ethernet.
- Carrier sense multiple access with collision avoidance (CSMA/CA) as used on Wireless LANs.

## Controlled access

- Deterministic access where each node has its own time on the medium.
- Used on legacy networks such as Token Ring and ARCNET.

## Contention-Based Access – CSMA/CD

### CSMA/CD

- Used by legacy Ethernet LANs.
- Operates in half-duplex mode where only one device sends or receives at a time.
- Uses a collision detection process to govern when a device can send and what happens if multiple devices send at the same time.

### CSMA/CD collision detection process:

- Devices transmitting simultaneously will result in a signal collision on the shared media.
- Devices detect the collision.
- Devices wait a random period of time and retransmit data.

## Contention-Based Access – CSMA/CA

### CSMA/CA

- Used by IEEE 802.11 WLANs.
- Operates in half-duplex mode where only one device sends or receives at a time.
- Uses a collision avoidance process to govern when a device can send and what happens if multiple devices send at the same time.

### CSMA/CA collision avoidance process:

- When transmitting, devices also include the time duration needed for the transmission.
- Other devices on the shared medium receive the time duration information and know how long the medium will be unavailable.

# 6.3 Data Link Frame



## Data Link Frame The Frame

Data is encapsulated by the data link layer with a header and a trailer to form a frame.

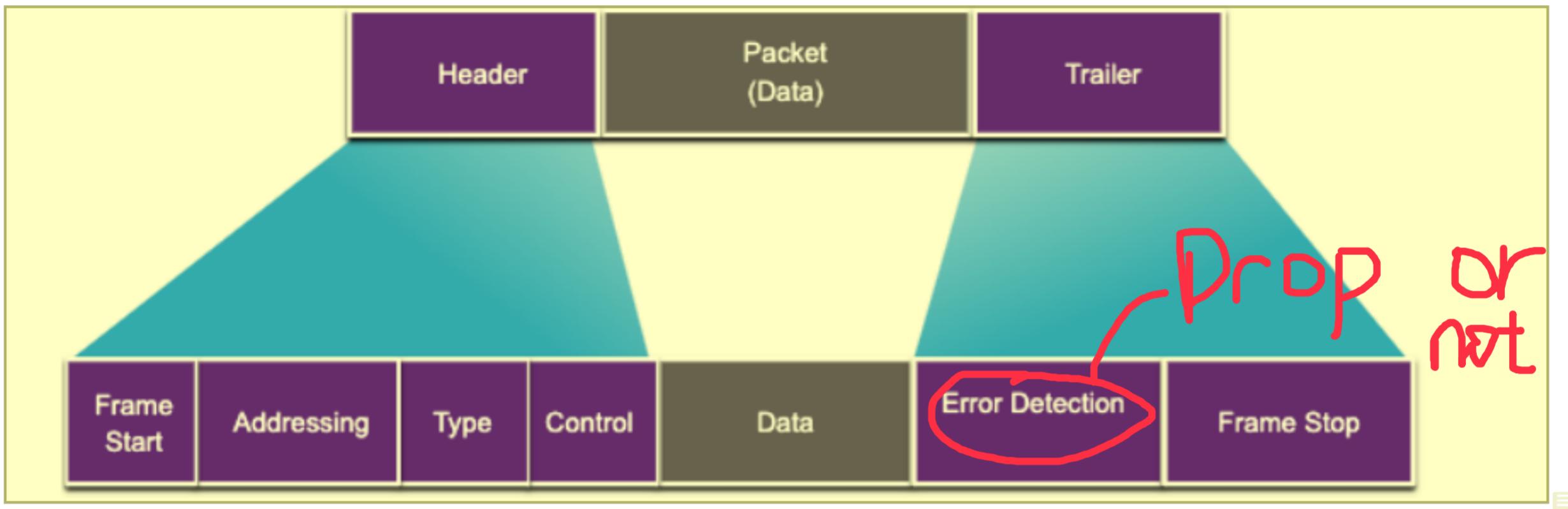
A data link frame has three parts:

- Header
- Data
- Trailer

The fields of the header and trailer vary according to data link layer protocol.

The amount of control information carried with in the frame varies according to access control information and logical topology.

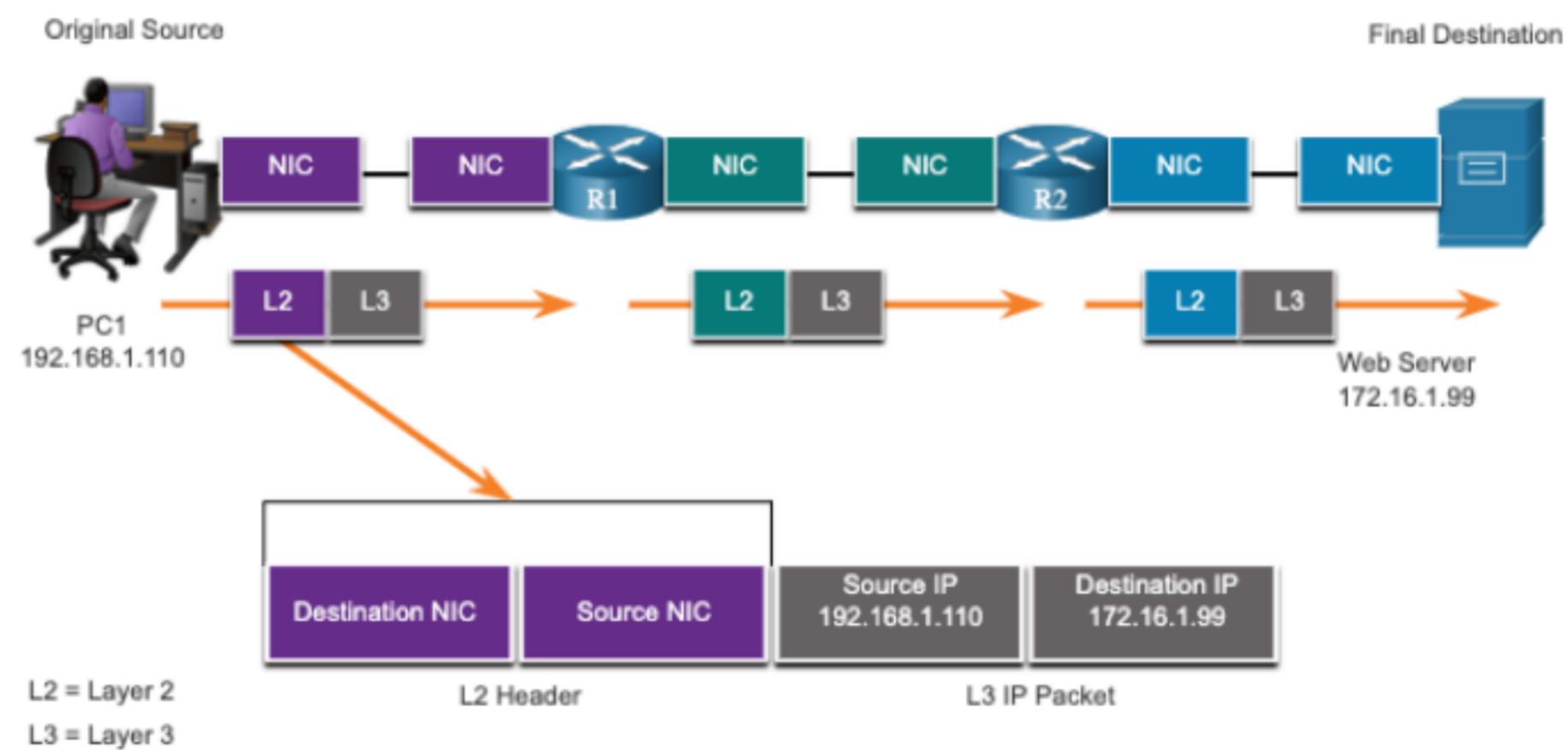
# Data Link Frame Frame Fields



Field	Description
Frame Start and Stop	Identifies beginning and end of frame
<u>Addressing</u>	<u>Indicates source and destination nodes</u>
<u>Type</u>	<u>Identifies encapsulated Layer 3 protocol</u>
Control	Identifies flow control services
Data	Contains the frame payload
Error Detection	Used for determine transmission errors

# Data Link Frame Layer 2 Addresses

- Also referred to as a physical address.
- Contained in the frame header.
- Used only for local delivery of a frame on the link.
- Updated by each device that forwards the frame.



## Data Link Frame LAN and WAN Frames

The logical topology and physical media determine the data link protocol used:

- Ethernet
- 802.11 Wireless
- Point-to-Point (PPP)
- High-Level Data Link Control (HDLC)
- Frame-Relay

Each protocol performs media access control for specified logical topologies.

# 6.4 Module Practice and Quiz



## Module Practice and Quiz

# What did I learn in this module?

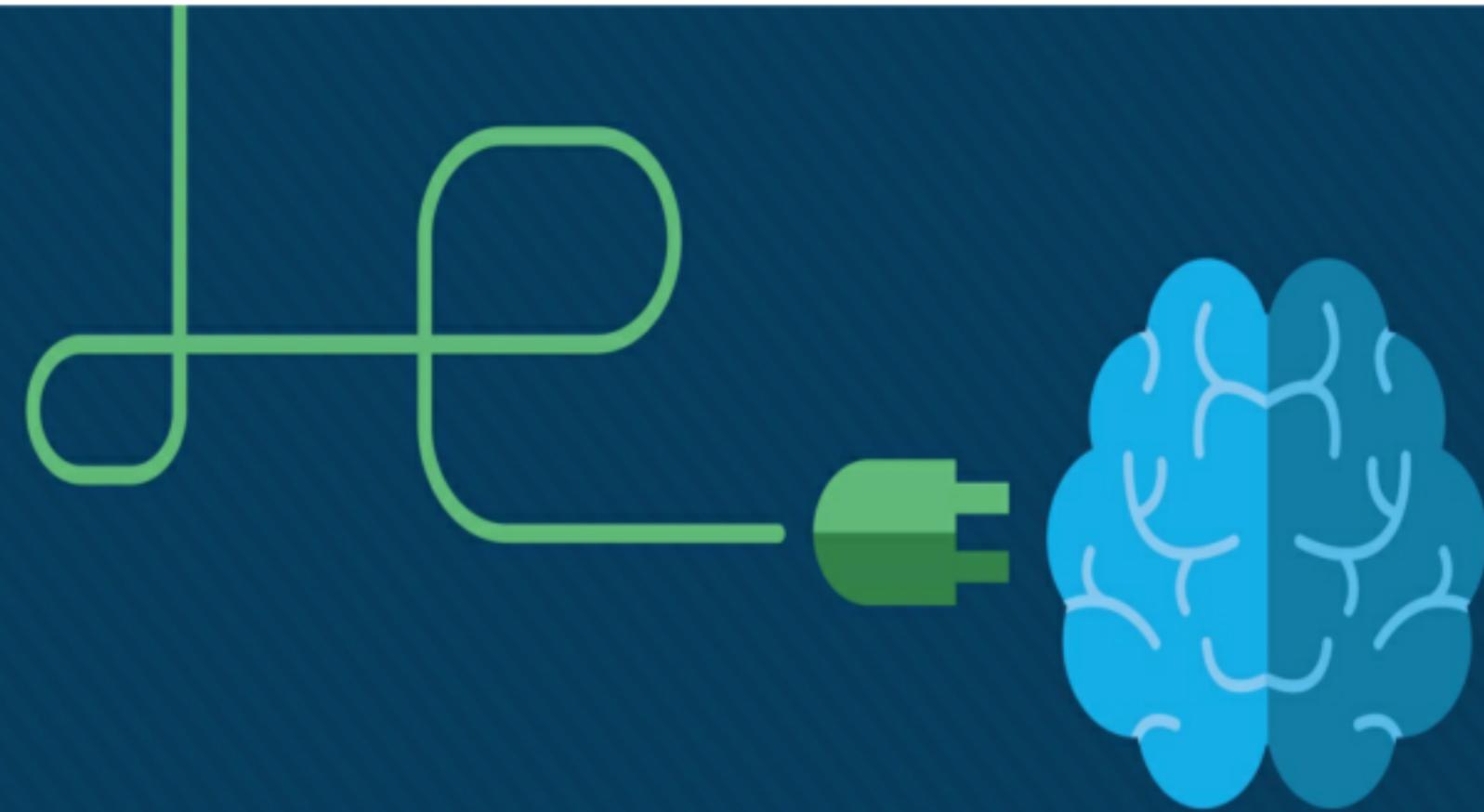
- The data link layer of the OSI model (Layer 2) prepares network data for the physical network.
- The data link layer is responsible for network interface card (NIC) to network interface card communications.
- The IEEE 802 LAN/MAN data link layer consists of the following two sublayers: LLC and MAC.
- The two types of topologies used in LAN and WAN networks are physical and logical.
- Three common types of physical WAN topologies are: point-to-point, hub and spoke, and mesh.
- Half-duplex communications exchange data in one direction at a time. Full-duplex sends and receives data simultaneously.
- In contention-based multi-access networks, all nodes are operating in half-duplex.
- Examples of contention-based access methods include: CSMA/CD for bus-topology Ethernet LANs and CSMA/CA for WLANs.
- The data link frame has three basic parts: header, data, and trailer.
- Frame fields include: frame start and stop indicator flags, addressing, type, control, data, and error detection.
- Data link addresses are also known as physical addresses.
- Data link addresses are only used for link local delivery of frames.



## New Terms and Commands

- |  |   |
|--|---|
| <ul style="list-style-type: none"><li>• Logical Link Control (LLC)</li><li>• Medial Access Control (MAC)</li><li>• Institute of Electrical and Electronic Engineers (IEEE)</li><li>• International Telecommunications Union (ITU)</li><li>• International Organization for Standardization (ISO)</li><li>• American National Standards Institute (ANSI)</li><li>• Physical Topology</li><li>• Logical Topology</li><li>• Half-duplex</li><li>• Full-duplex</li><li>• CSMA/CD</li><li>• CSMA/CA</li></ul> | <ul style="list-style-type: none"><li>• Cyclic Redundancy Check (CRC)</li><li>• Contention-based access</li><li>• Controlled access</li></ul> |
|--|---|





# Module 14: Routing Concepts

Switching, Routing, and Wireless Essentials v7.0  
(SRWE)

**“What does a router do with a packet received from one network and destined for another network?”**



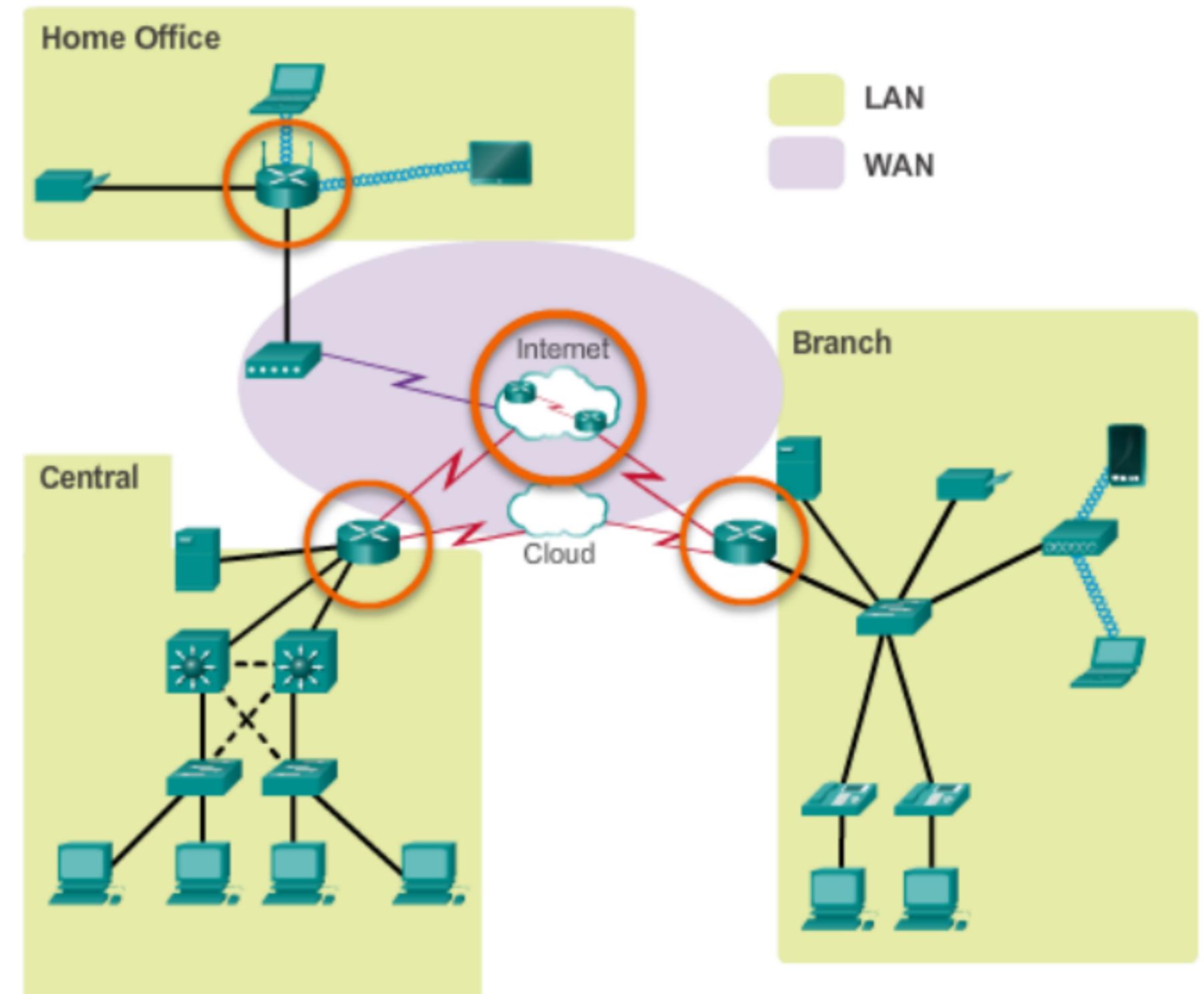


(recap)

# Routers Interconnect Networks

- **Routers connect multiple networks.**

Routers have multiple interfaces, each on a different IP network.



# “routing”



(recap)

## Routers Choose Best Paths

The primary functions of a router are to:

1. **Determine the best path to send packets**

Uses its **routing table** to determine path.

2. **Forward packets toward their destination**

**Forwards** packet to interface indicated in routing table.

**Encapsulates** the packet and forwards out toward destination.

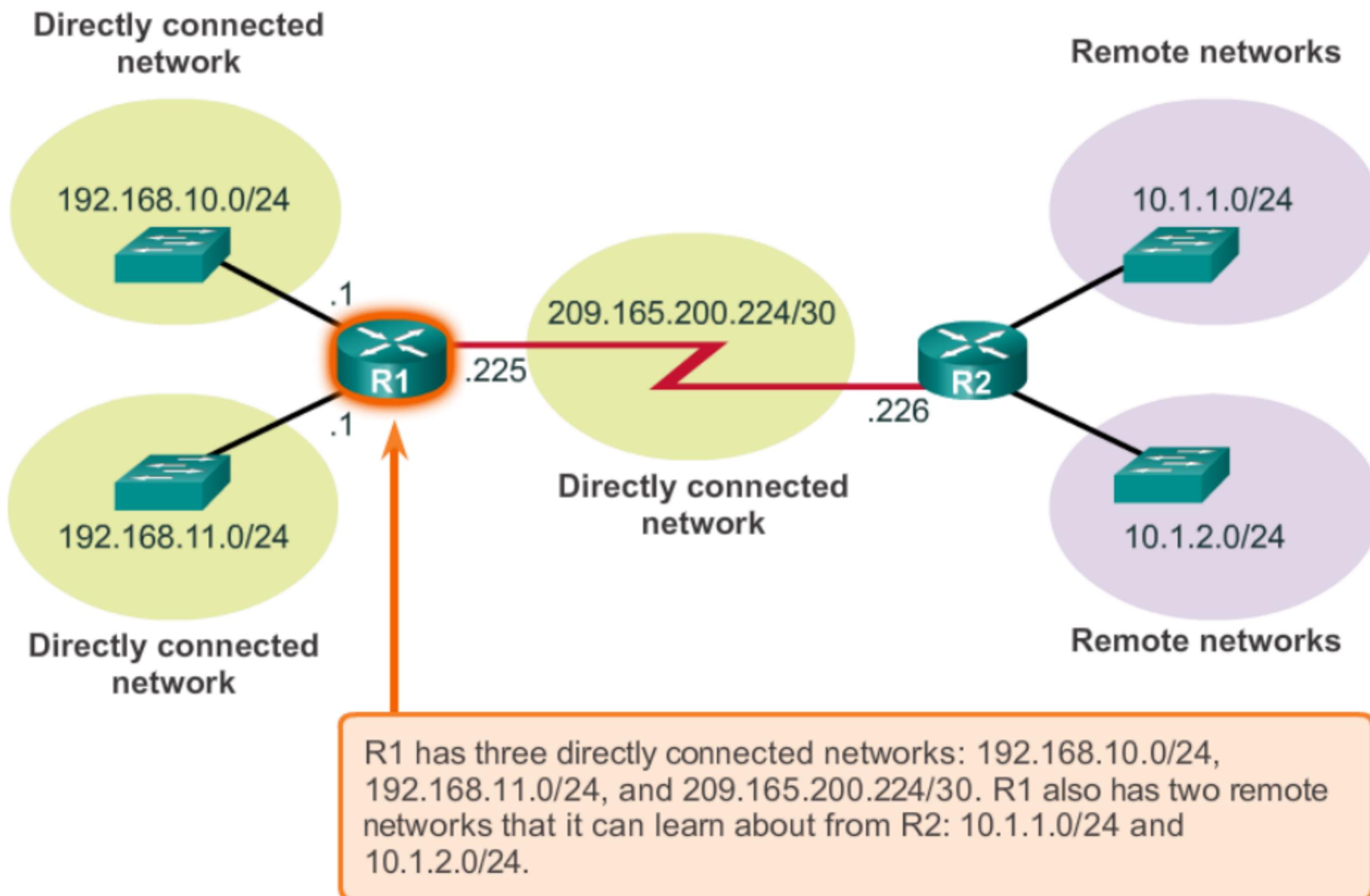
- Routers use **static routes** and **dynamic routing protocols** to learn about **remote** networks and build their routing tables.



(recap)

# Router Packet Forwarding Decision

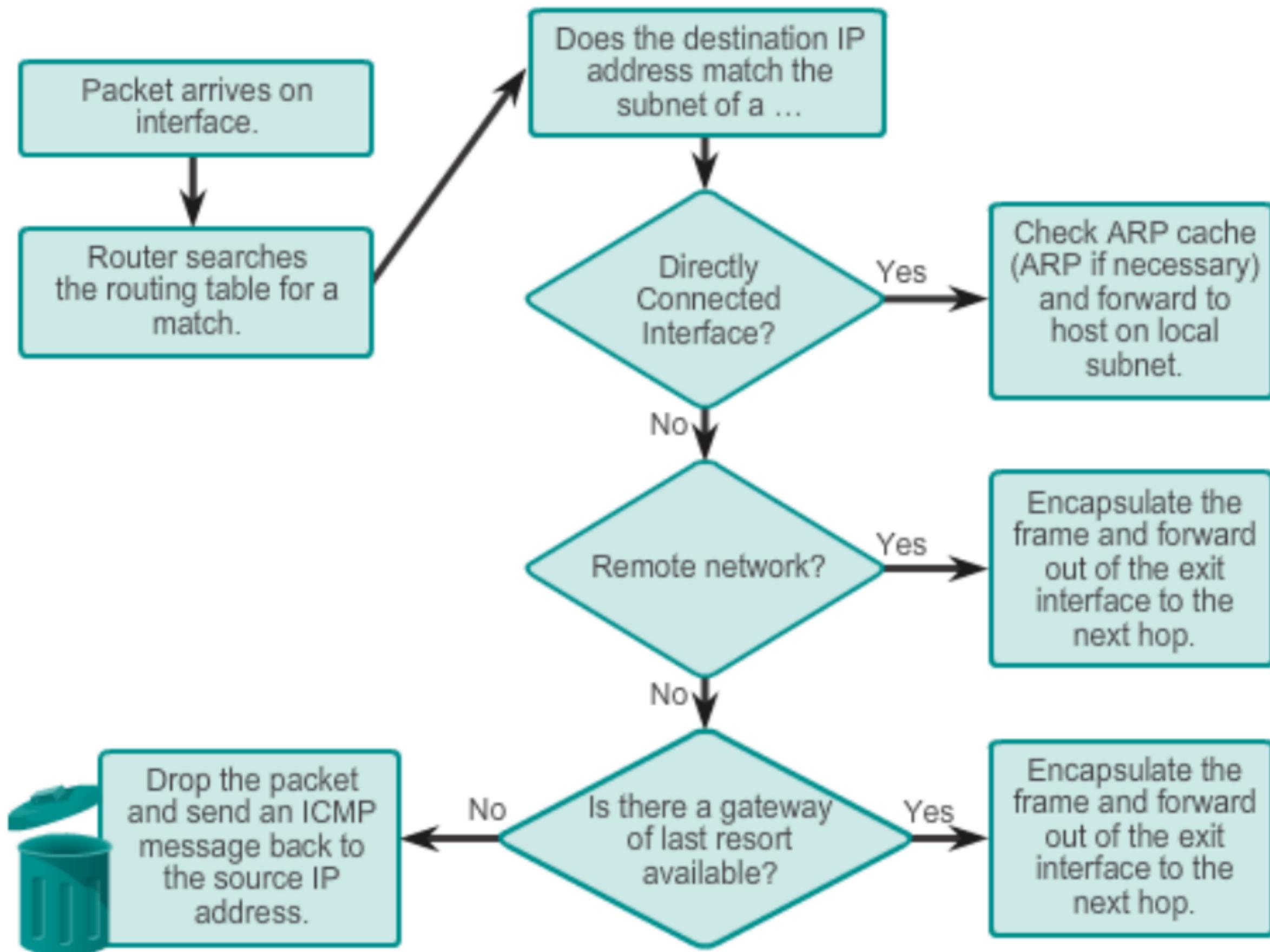
- **Directly-connected routes:** added automatically
- **Remote routes:** statically or dynamically





# Routing Decisions

## Packet Forwarding Decision Process





# “Best Path = Longest Match”

Matches for Packet Destined to 172.16.0.10

IP Packet Destination	172.16.0.10	10101100.00010000.00000000.00001010
Route 1	172.16.0.0/12	10101100.00010000.00000000.00000000
Route 2	172.16.0.0/18	10101100.00010000.00000000.00000000
Route 3	172.16.0.0/26	10101100.00010000.00000000.00000000

The **subnet mask** of the route in the routing table determines the **minimum number of far-left bits** that must **match**.

Longest Match to IP Packet Destination

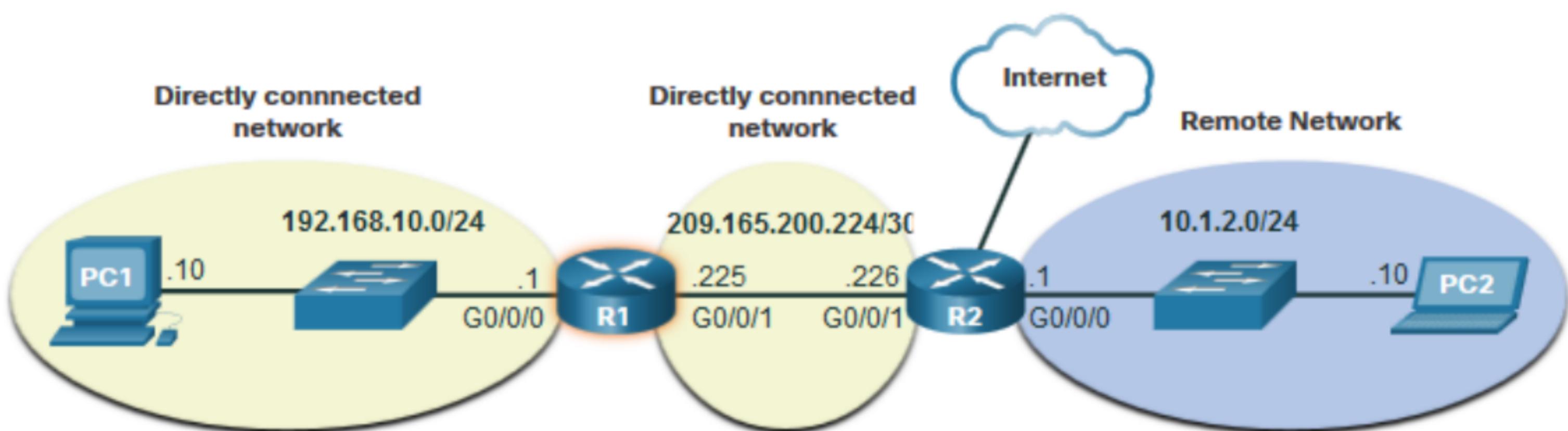
# 14.4 IP Routing Table



# Router Routing Table

There are three types of routes in a router's routing table:

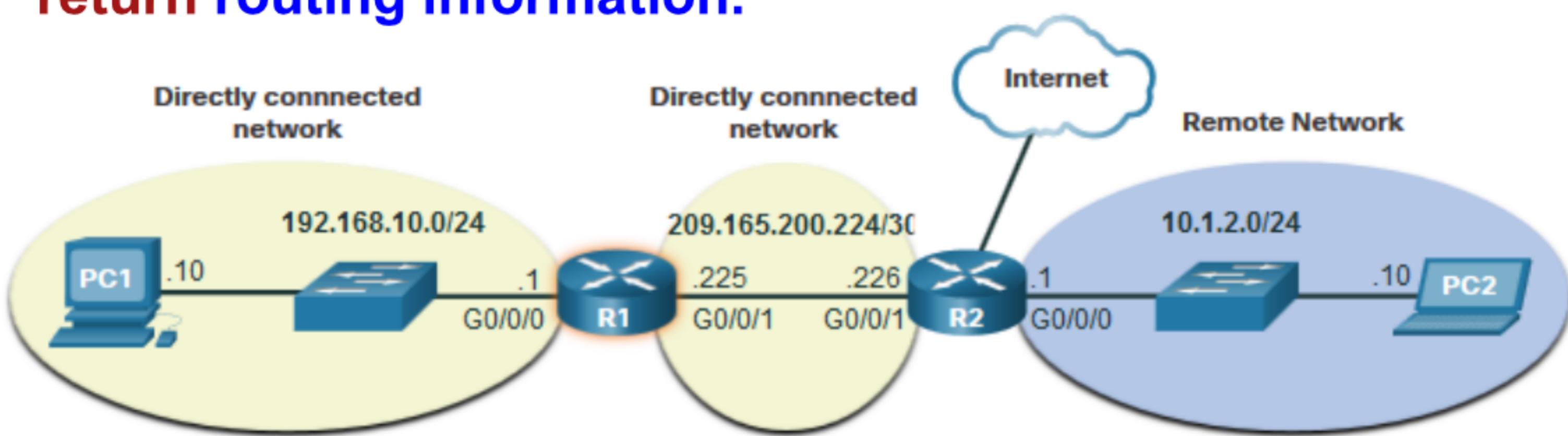
- **Directly Connected** – These routes are automatically added by the router, provided the interface is active and has addressing.
- **Remote** – These are the routes the router does not have a direct connection and may be learned:
  - **Manually** – with a static route
  - **Dynamically** – by using a routing protocol to have the routers share their information with each other
- **Default Route** – this forwards all traffic to a specific direction when there is not a match in the routing table





# Routing Table Principles

- Every router makes its decision alone, based on the information it has in its own routing table.
- The information in a routing table of one router does not necessarily match the routing table of another router.
- Routing information about a path does not provide return routing information.

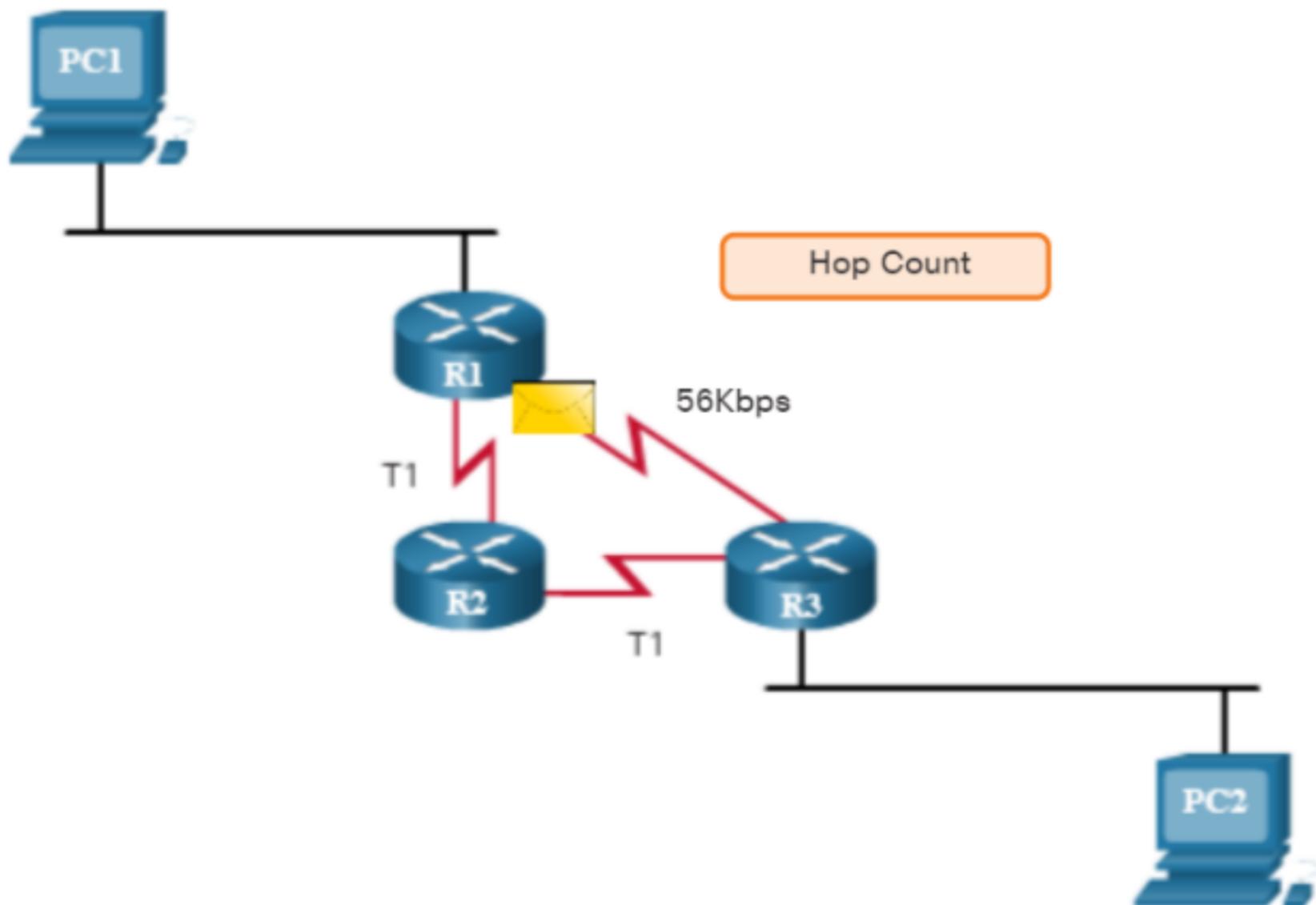




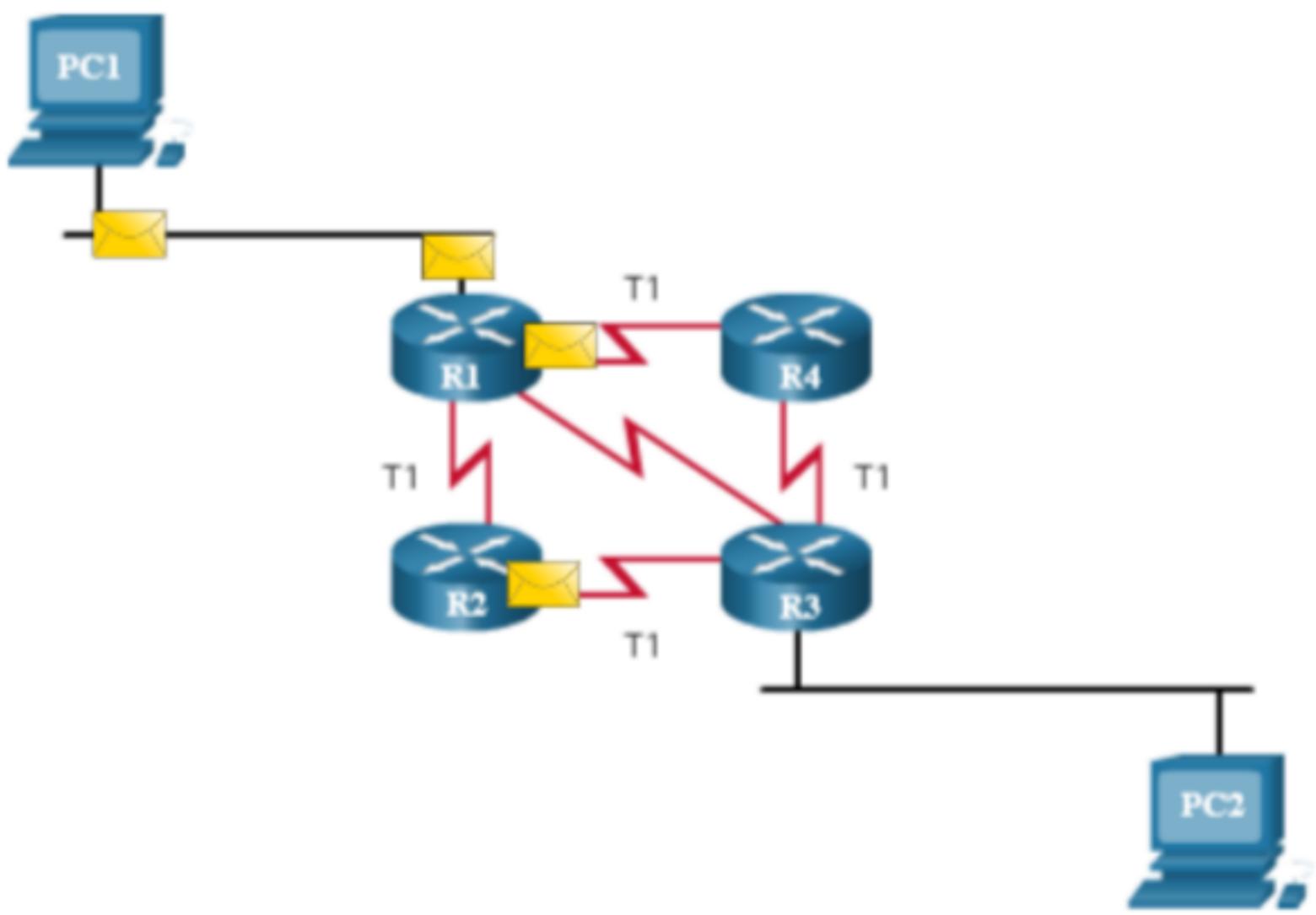
# Best Path? Metric

- A **metric** is the value used to measure the distance to a given network.
- **Best path** to a network is the path with the **lowest metric**.

Hop Count Versus Bandwidth as a Metric



Equal Cost Load Balancing





# “Administrative Distance (AD)”

- If multiple paths to a **same** destination are configured on a router, the path installed in the routing table is the one with the best (**lowest**) AD.
- AD is the “**trustworthiness**” of the route.
- The **lower** the AD, the more trustworthy the route source.

Default Administrative Distances

Route Source	Administrative Distance
Connected	0
Static	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
Internal BGP	200



## Module 4: Inter-VLAN Routing

Switching, Routing and Wireless  
Essentials v7.0 (SRWE)



# Module Objectives

**Module Title:** Inter-VLAN Routing

**Module Objective:** Troubleshoot inter-VLAN routing on Layer 3 devices

Topic Title	Topic Objective
Inter-VLAN Routing Operation	Describe options for configuring inter-VLAN routing.
Router-on-a-Stick Inter-VLAN Routing	Configure router-on-a-stick inter-VLAN routing.
Inter-VLAN Routing using Layer 3 Switches	Configure inter-VLAN routing using Layer 3 switching.
Troubleshoot Inter-VLAN Routing	Troubleshoot common inter-VLAN configuration issues.



# 4.1 Inter-VLAN Routing Operation



## What is Inter-VLAN Routing?

VLANs are used to segment switched Layer 2 networks for a variety of reasons. Regardless of the reason, hosts in one VLAN cannot communicate with hosts in another VLAN unless there is a router or a Layer 3 switch to provide routing services.

Inter-VLAN routing is the process of forwarding network traffic from one VLAN to another VLAN.

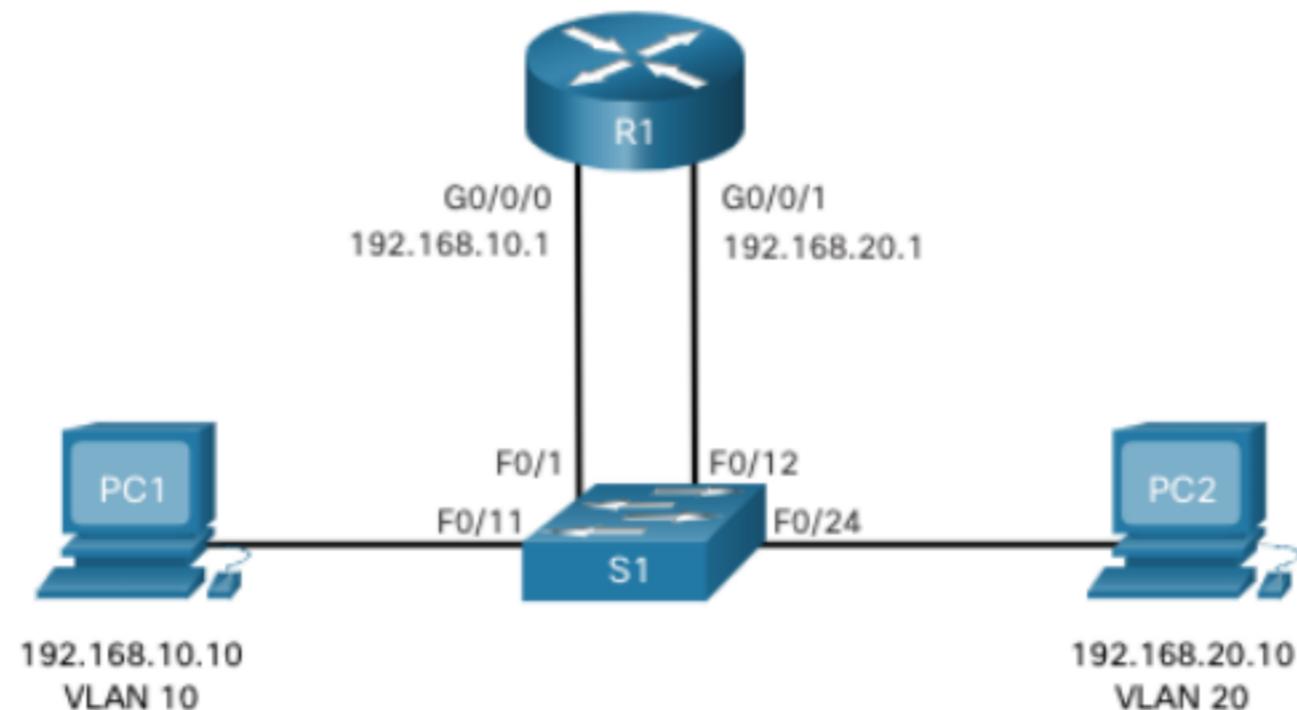
There are three inter-VLAN routing options:

- **Legacy Inter-VLAN routing** - This is a legacy solution. It does not scale well.
- **Router-on-a-Stick** - This is an acceptable solution for a small to medium-sized network.
- **Layer 3 switch using switched virtual interfaces (SVIs)** - This is the most scalable solution for medium to large organizations.

## Inter-VLAN Routing Operation

# Legacy Inter-VLAN Routing

- The first inter-VLAN routing solution relied on using a router with multiple Ethernet interfaces. Each router interface was connected to a switch port in different VLANs. The router interfaces served as the default gateways to the local hosts on the VLAN subnet.
- Legacy inter-VLAN routing using physical interfaces works, but it has a significant limitation. It is not reasonably scalable because routers have a limited number of physical interfaces. Requiring one physical router interface per VLAN quickly exhausts the physical interface capacity of a router.
- Note:** This method of inter-VLAN routing is no longer implemented in switched networks and is included for explanation purposes only.



## Inter-VLAN Routing Operation

# Router-on-a-Stick Inter-VLAN Routing

The ‘router-on-a-stick’ inter-VLAN routing method overcomes the limitation of the legacy inter-VLAN routing method. It only requires one physical Ethernet interface to route traffic between multiple VLANs on a network.

- A Cisco IOS router Ethernet interface is configured as an 802.1Q trunk and connected to a trunk port on a Layer 2 switch. Specifically, the router interface is configured using subinterfaces to identify routable VLANs.
- The configured subinterfaces are software-based virtual interfaces. Each is associated with a single physical Ethernet interface. Subinterfaces are configured in software on a router. Each subinterface is independently configured with an IP address and VLAN assignment. Subinterfaces are configured for different subnets that correspond to their VLAN assignment. This facilitates logical routing.
- When VLAN-tagged traffic enters the router interface, it is forwarded to the VLAN subinterface. After a routing decision is made based on the destination IP network address, the router determines the exit interface for the traffic. If the exit interface is configured as an 802.1q subinterface, the data frames are VLAN-tagged with the new VLAN and sent back out the physical interface

**Note:** The router-on-a-stick method of inter-VLAN routing does not scale beyond 50 VLANs.

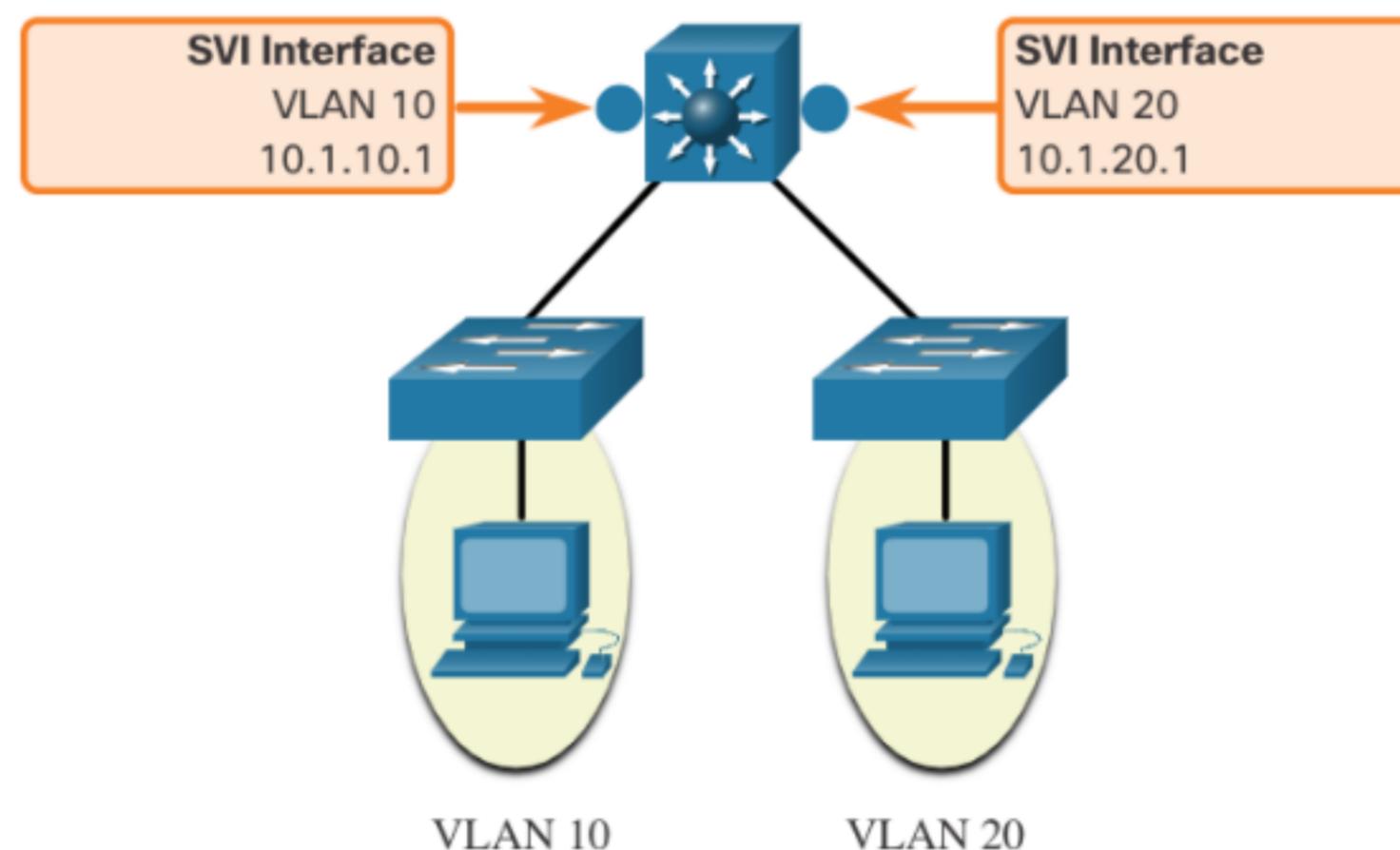


## Inter-VLAN Routing Operation

# Inter-VLAN Routing on a Layer 3 Switch

The modern method of performing inter-VLAN routing is to use Layer 3 switches and switched virtual interfaces (SVI). An SVI is a virtual interface that is configured on a Layer 3 switch, as shown in the figure.

**Note:** A Layer 3 switch is also called a multilayer switch as it operates at Layer 2 and Layer 3. However, in this course we use the term Layer 3 switch.



## Inter-VLAN Routing Operation

# Inter-VLAN Routing on a Layer 3 Switch (Cont.)

Inter-VLAN SVIs are created the same way that the management VLAN interface is configured. The SVI is created for a VLAN that exists on the switch. Although virtual, the SVI performs the same functions for the VLAN as a router interface would. Specifically, it provides Layer 3 processing for packets that are sent to or from all switch ports associated with that VLAN.

The following are advantages of using Layer 3 switches for inter-VLAN routing:

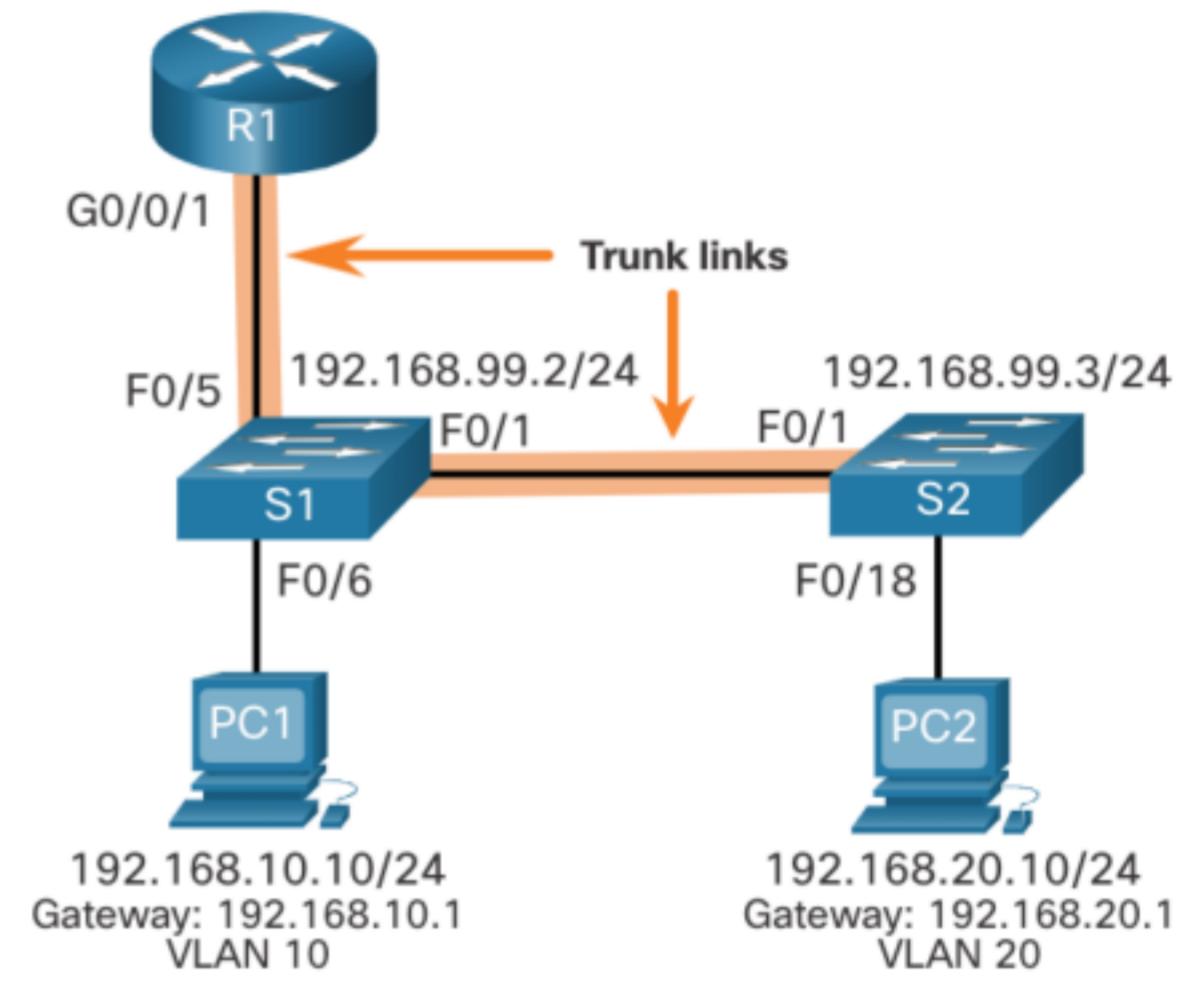
- They are much faster than router-on-a-stick because everything is hardware switched and routed.
- There is no need for external links from the switch to the router for routing.
- They are not limited to one link because Layer 2 EtherChannels can be used as trunk links between the switches to increase bandwidth.
- Latency is much lower because data does not need to leave the switch in order to be routed to a different network.
- They are more commonly deployed in a campus LAN than routers.
- The only disadvantage is that Layer 3 switches are more expensive.

# 4.2 Router-on-a-Stick Inter-VLAN Routing



## Router-on-a-Stick Inter-VLAN Routing Router-on-a-Stick Scenario

- In the figure, the R1 GigabitEthernet 0/0/1 interface is connected to the S1 FastEthernet 0/5 port. The S1 FastEthernet 0/1 port is connected to the S2 FastEthernet 0/1 port. These are trunk links that are required to forward traffic within and between VLANs.
- To route between VLANs, the R1 GigabitEthernet 0/0/1 interface is logically divided into three subinterfaces, as shown in the table. The table also shows the three VLANs that will be configured on the switches.
- Assume that R1, S1, and S2 have initial basic configurations. Currently, PC1 and PC2 cannot **ping** each other because they are on separate networks. Only S1 and S2 can **ping** each other, but they but are unreachable by PC1 or PC2 because they are also on different networks.
- To enable devices to ping each other, the switches must be configured with VLANs and trunking, and the router must be configured for inter-VLAN routing.



Subinterface	VLAN	IP Address
G0/0/1.10	10	192.168.10.1/24
G0/0/1.20	20	192.168.20.1/24
G0/0/1.30	99	192.168.99.1/24

## S1 VLAN and Trunking Configuration

Complete the following steps to configure S1 with VLANs and trunking:

- **Step 1.** Create and name the VLANs.
- **Step 2.** Create the management interface.
- **Step 3.** Configure access ports.
- **Step 4.** Configure trunking ports.

## Router-on-a-Stick Inter-VLAN Routing

# S2 VLAN and Trunking Configuration

The configuration for S2  
is similar to S1.

```
S2(config)# vlan 10
S2(config-vlan)# name LAN10
S2(config-vlan)# exit
S2(config)# vlan 20
S2(config-vlan)# name LAN20
S2(config-vlan)# exit
S2(config)# vlan 99
S2(config-vlan)# name Management
S2(config-vlan)# exit
S2(config)#
S2(config)# interface vlan 99
S2(config-if)# ip add 192.168.99.3 255.255.255.0
S2(config-if)# no shut
S2(config-if)# exit
S2(config)# ip default-gateway 192.168.99.1
S2(config)# interface fa0/18
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 20
S2(config-if)# no shut
S2(config-if)# exit
S2(config)# interface fa0/1
S2(config-if)# switchport mode trunk
S2(config-if)# no shut
S2(config-if)# exit
S2(config-if)# end
*Mar 1 00:23:52.137: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
```



## Router-on-a-Stick Inter-VLAN Routing R1 Subinterface Configuration

The router-on-a-stick method requires you to create a subinterface for each VLAN to be routed. A subinterface is created using the **interface interface\_id subinterface\_id** global configuration mode command. The subinterface syntax is the physical interface followed by a period and a subinterface number. Although not required, it is customary to match the subinterface number with the VLAN number.

Each subinterface is then configured with the following two commands:

- **encapsulation dot1q vlan\_id [native]** - This command configures the subinterface to respond to 802.1Q encapsulated traffic from the specified *vlan-id*. The **native** keyword option is only appended to set the native VLAN to something other than VLAN 1.
- **ip address ip-address subnet-mask** - This command configures the IPv4 address of the subinterface. This address typically serves as the default gateway for the identified VLAN.

Repeat the process for each VLAN to be routed. Each router subinterface must be assigned an IP address on a unique subnet for routing to occur. When all subinterfaces have been created, enable the physical interface using the **no shutdown** interface configuration command. If the physical interface is disabled, all subinterfaces are disabled.

## Router-on-a-Stick Inter-VLAN Routing R1 Subinterface Configuration (Cont.)

In the configuration, the R1 G0/0/1 subinterfaces are configured for VLANs 10, 20, and 99.

```
R1(config)# interface G0/0/1.10
R1(config-subif)# Description Default Gateway for VLAN 10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip add 192.168.10.1 255.255.255.0
R1(config-subif)# exit
R1(config)#
R1(config)# interface G0/0/1.20
R1(config-subif)# Description Default Gateway for VLAN 20
R1(config-subif)# encapsulation dot1Q 20
R1(config-subif)# ip add 192.168.20.1 255.255.255.0
R1(config-subif)# exit
R1(config)#
R1(config)# interface G0/0/1.99
R1(config-subif)# Description Default Gateway for VLAN 99
R1(config-subif)# encapsulation dot1Q 99
R1(config-subif)# ip add 192.168.99.1 255.255.255.0
R1(config-subif)# exit
R1(config)#
R1(config)# interface G0/0/1
R1(config-if)# Description Trunk link to S1
R1(config-if)# no shut
R1(config-if)# end
R1#
*Sep 15 19:08:47.015: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to down
*Sep 15 19:08:50.071: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to up
*Sep 15 19:08:51.071: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1,
changed state to up
R1#
```



## Router-on-a-Stick Inter-VLAN Routing Verify Connectivity Between PC1 and PC2

The router-on-a-stick configuration is complete after the switch trunk and the router subinterfaces have been configured. The configuration can be verified from the hosts, router, and switch.

From a host, verify connectivity to a host in another VLAN using the **ping** command. It is a good idea to first verify the current host IP configuration using the **ipconfig** Windows host command.

Next, use **ping** to verify connectivity with PC2 and S1, as shown in the figure. The **ping** output successfully confirms inter-VLAN routing is operating.

```
C:\Users\PC1> ping 192.168.20.10
Pinging 192.168.20.10 with 32 bytes of data:
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Ping statistics for 192.168.20.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss).
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\PC1>
C:\Users\PC1> ping 192.168.99.2
Pinging 192.168.99.2 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 192.168.99.2: bytes=32 time=2ms TTL=254
Reply from 192.168.99.2: bytes=32 time=1ms TTL=254
Ping statistics for 192.168.99.2:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss).
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\Users\PC1>
```



## Router-on-a-Stick Inter-VLAN Routing Verification

In addition to using **ping** between devices, the following **show** commands can be used to verify and troubleshoot the router-on-a-stick configuration.

- **show ip route**
- **show ip interface brief**
- **show interfaces**
- **show interfaces trunk**

Router-on-a-Stick Inter-VLAN Routing

## Packet Tracer– Configure Router-on-a-Stick Inter-VLAN Routing

In this Packet Tracer, you will complete the following objectives:

- Part 1: Add VLANs to a Switch
- Part 2: Configure Subinterfaces
- Part 3: Test connectivity with Inter-VLAN Routing



## Router-on-a-Stick Inter-VLAN Routing

# Lab – Configure Router-on-a-Stick Inter-VLAN Routing

In this lab, you will complete the following objectives:

- Part 1: Build the Network and Configure Basic Device Settings
- Part 2: Configure Switches with VLANs and Trunking
- Part 3: Configure Trunk-Based Inter-VLAN Routing



# 4.3 Inter-VLAN Routing using Layer 3 Switches



## Inter-VLAN Routing using Layer 3 Switches

# Layer 3 Switch Inter-VLAN Routing

Inter-VLAN routing using the router-on-a-stick method is simple to implement for a small to medium-sized organization. However, a large enterprise requires a faster, much more scalable method to provide inter-VLAN routing.

Enterprise campus LANs use Layer 3 switches to provide inter-VLAN routing. Layer 3 switches use hardware-based switching to achieve higher-packet processing rates than routers. Layer 3 switches are also commonly implemented in enterprise distribution layer wiring closets.

Capabilities of a Layer 3 switch include the ability to do the following:

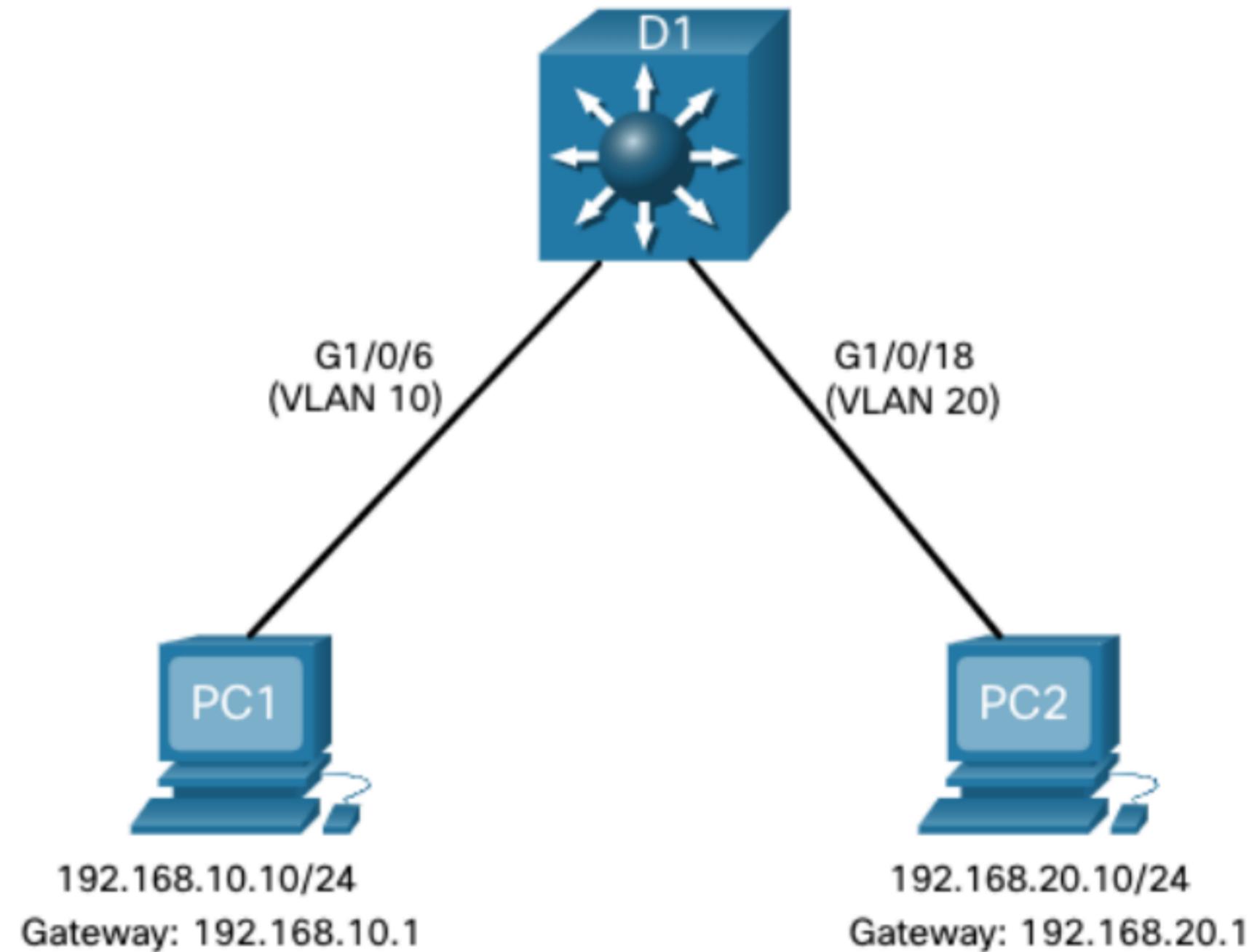
- Route from one VLAN to another using multiple switched virtual interfaces (SVIs).
- Convert a Layer 2 switchport to a Layer 3 interface (i.e., a routed port). A routed port is similar to a physical interface on a Cisco IOS router.
- To provide inter-VLAN routing, Layer 3 switches use SVIs. SVIs are configured using the same **interface vlan *vlan-id*** command used to create the management SVI on a Layer 2 switch. A Layer 3 SVI must be created for each of the routable VLANs.



## Inter-VLAN Routing using Layer 3 Switches

### Layer 3 Switch Scenario

In the figure, the Layer 3 switch, D1, is connected to two hosts on different VLANs. PC1 is in VLAN 10 and PC2 is in VLAN 20, as shown. The Layer 3 switch will provide inter-VLAN routing services to the two hosts.

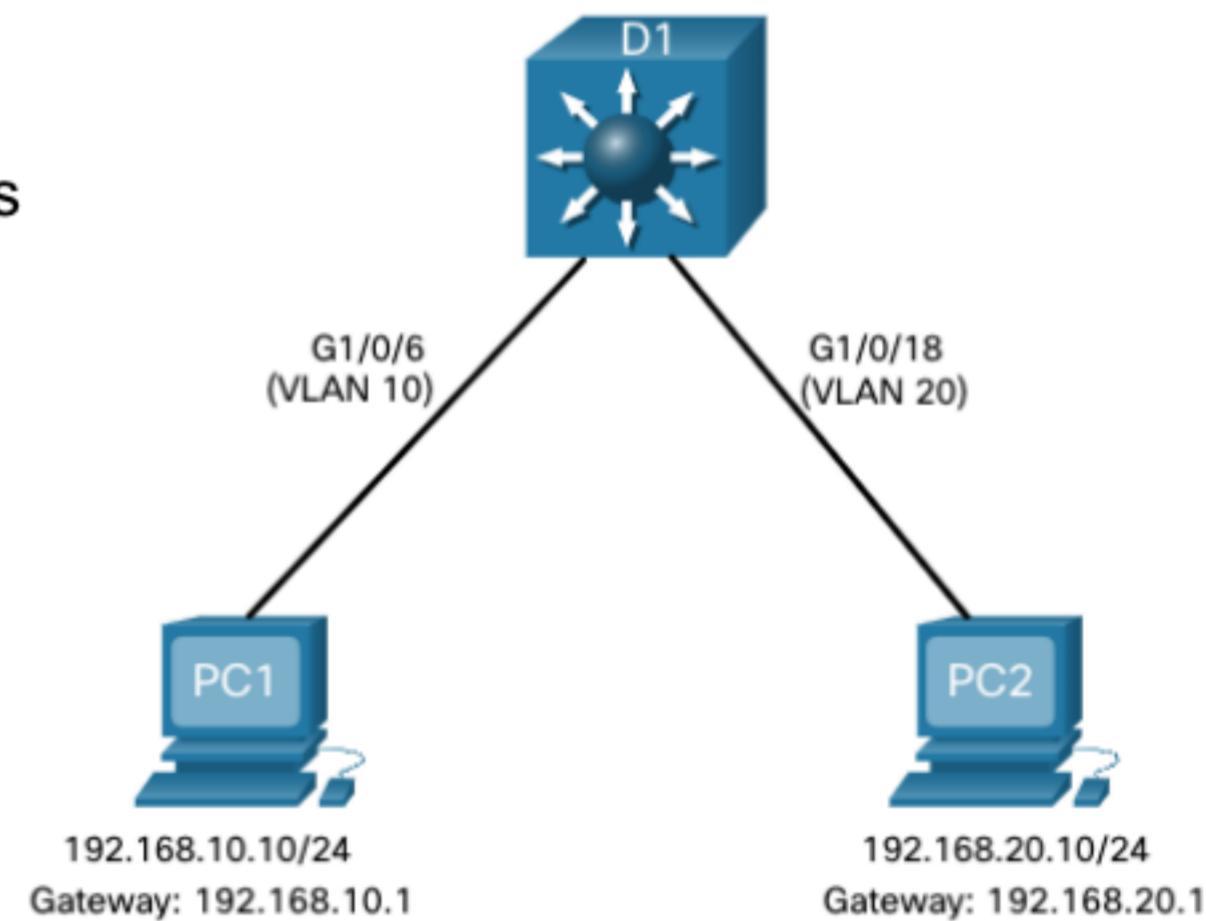


## Inter-VLAN Routing using Layer 3 Switches

### Layer 3 Switch Configuration

Complete the following steps to configure S1 with VLANs and trunking:

- **Step 1.** Create the VLANs. In the example, VLANs 10 and 20 are used.
- **Step 2.** Create the SVI VLAN interfaces. The IP address configured will serve as the default gateway for hosts in the respective VLAN.
- **Step 3.** Configure access ports. Assign the appropriate port to the required VLAN.
- **Step 4.** Enable IP routing. Issue the **ip routing** global configuration command to allow traffic to be exchanged between VLANs 10 and 20. This command must be configured to enable inter-VAN routing on a Layer 3 switch for IPv4.



## Layer 3 Switch Inter-VLAN Routing Verification

Inter-VLAN routing using a Layer 3 switch is simpler to configure than the router-on-a-stick method. After the configuration is complete, the configuration can be verified by testing connectivity between the hosts.

- From a host, verify connectivity to a host in another VLAN using the **ping** command. It is a good idea to first verify the current host IP configuration using the **ipconfig** Windows host command.
- Next, verify connectivity with PC2 using the **ping** Windows host command. The successful **ping** output confirms inter-VLAN routing is operating.

## Inter-VLAN Routing using Layer 3 Switches Routing on a Layer 3 Switch

If VLANs are to be reachable by other Layer 3 devices, then they must be advertised using static or dynamic routing. To enable routing on a Layer 3 switch, a routed port must be configured.

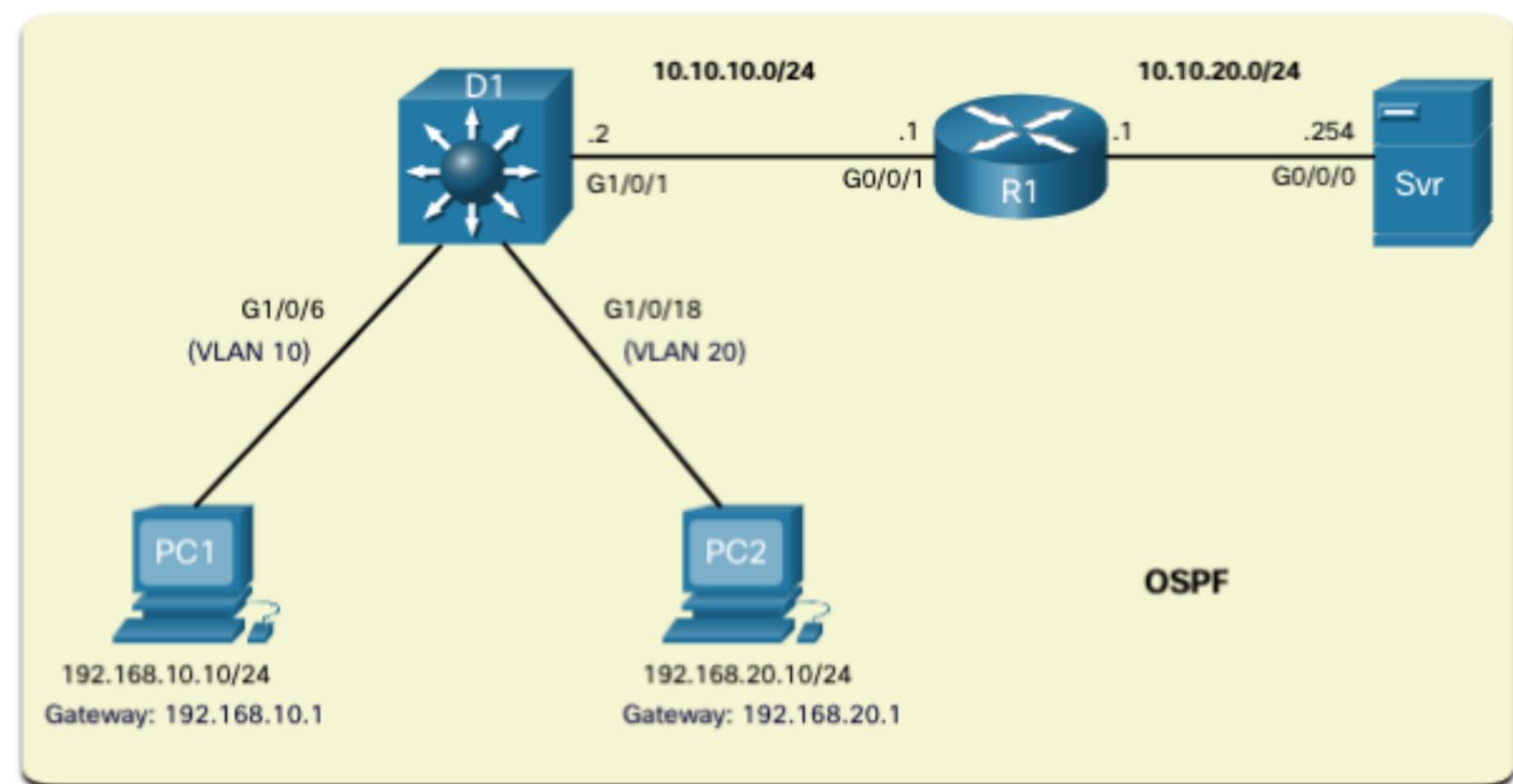
A routed port is created on a Layer 3 switch by disabling the switchport feature on a Layer 2 port that is connected to another Layer 3 device. Specifically, configuring the **no switchport** interface configuration command on a Layer 2 port converts it into a Layer 3 interface. Then the interface can be configured with an IPv4 configuration to connect to a router or another Layer 3 switch.



## Inter-VLAN Routing using Layer 3 Switches Routing Scenario on a Layer 3 Switch

In the figure, the previously configured D1 Layer 3 switch is now connected to R1. R1 and D1 are both in an Open Shortest Path First (OSPF) routing protocol domain. Assume inter-VLAN has been successfully implemented on D1. The G0/0/1 interface of R1 has also been configured and enabled. Additionally, R1 is using OSPF to advertise its two networks, 10.10.10.0/24 and 10.20.20.0/24.

**Note:** OSPF routing configuration is covered in another course. In this module, OSPF configuration commands will be given to you in all activities and assessments. It is not required that you understand the configuration in order to enable OSPF routing on the Layer 3 switch.



## Inter-VLAN Routing using Layer 3 Switches

# Routing Configuration on a Layer 3 Switch

Complete the following steps to configure D1 to route with R1:

- **Step 1.** Configure the routed port. Use the **no switchport** command to convert the port to a routed port, then assign an IP address and subnet mask. Enable the port.
- **Step 2.** Enable routing. Use the **ip routing** global configuration command to enable routing.
- **Step 3.** Configure routing. Use an appropriate routing method. In this example, Single-Area OSPFv2 is configured
- **Step 4.** Verify routing. Use the **show ip route** command.
- **Step 5.** Verify connectivity. Use the **ping** command to verify reachability.



Inter-VLAN Routing using Layer 3 Switches

## Packet Tracer – Configure Layer 3 Switching and inter-VLAN Routing

In this Packet Tracer, you will complete the following objectives:

- Part 1: Configure Layer 3 Switching
- Part 2: Configure Inter-VLAN Routing
- Part 3: Configure IPv6 Inter-VLAN Routing



# 4.4 Troubleshoot Inter-VLAN Routing



## Troubleshoot Inter-VLAN Routing Common Inter-VLAN Issues

There are a number of reasons why an inter-VAN configuration may not work. All are related to connectivity issues. First, check the physical layer to resolve any issues where a cable might be connected to the wrong port. If the connections are correct, then use the list in the table for other common reasons why inter-VLAN connectivity may fail.

Issue Type	How to Fix	How to Verify
Missing VLANs	<ul style="list-style-type: none"><li>Create (or re-create) the VLAN if it does not exist.</li><li>Ensure host port is assigned to the correct VLAN.</li></ul>	<b>show vlan [brief]</b> <b>show interfaces switchport</b> <b>ping</b>
Switch Trunk Port Issues	<ul style="list-style-type: none"><li>Ensure trunks are configured correctly.</li><li>Ensure port is a trunk port and enabled.</li></ul>	<b>show interface trunk</b> <b>show running-config</b>
Switch Access Port Issues	<ul style="list-style-type: none"><li>Assign correct VLAN to access port.</li><li>Ensure port is an access port and enabled.</li><li>Host is incorrectly configured in the wrong subnet.</li></ul>	<b>show interfaces switchport</b> <b>show running-config interface</b> <b>ipconfig</b>
Router Configuration Issues	<ul style="list-style-type: none"><li>Router subinterface IPv4 address is incorrectly configured.</li><li>Router subinterface is assigned to the VLAN ID.</li></ul>	<b>show ip interface brief</b> <b>show interfaces</b>



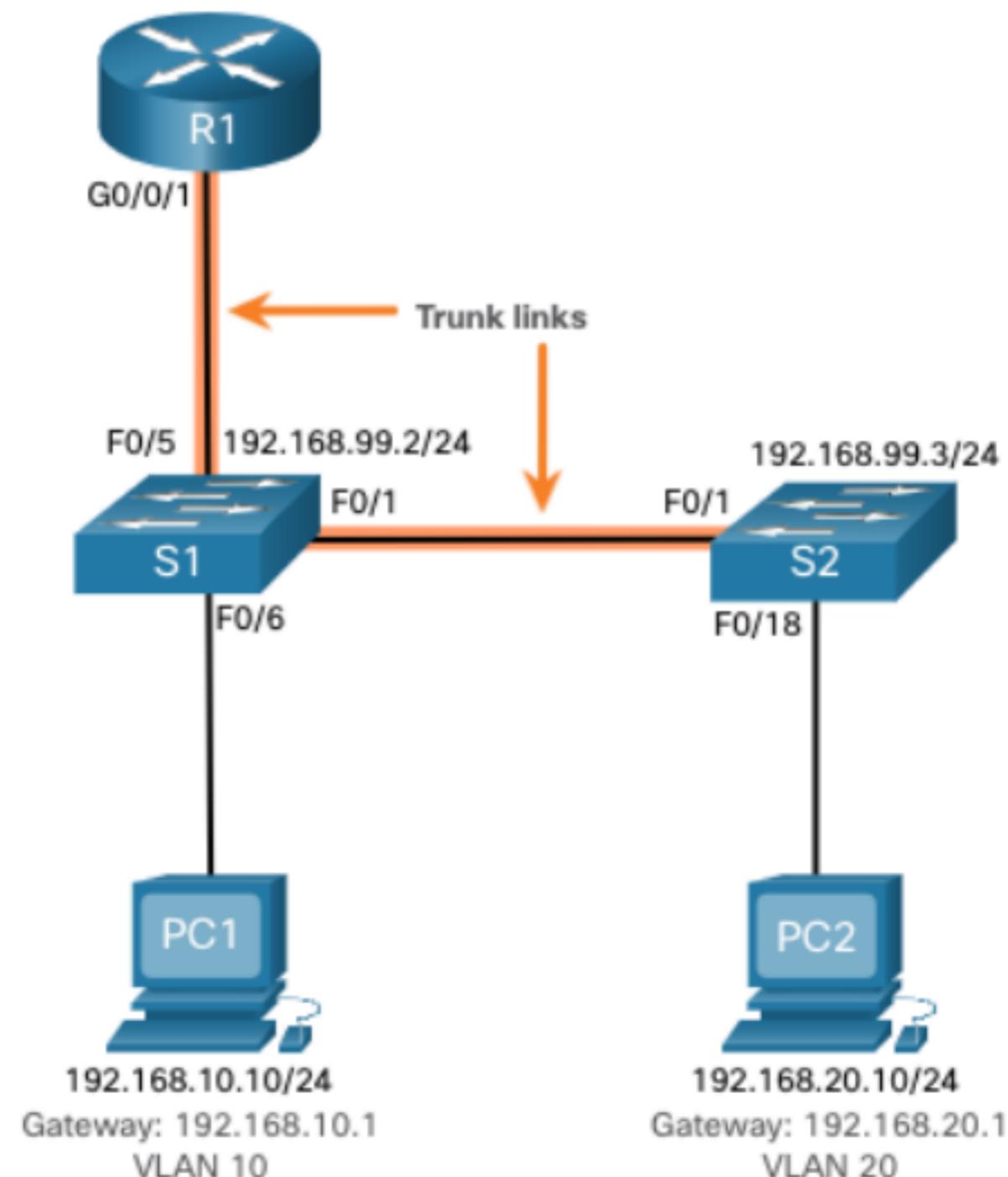
## Troubleshoot Inter-VLAN Routing

# Troubleshoot Inter-VLAN Routing Scenario

Examples of some of these inter-VLAN routing problems will now be covered in more detail.

This topology will be used for all of these issues.

Router R1 Subinterfaces		
Subinterface	VLAN	IP Address
G0/0/0.10	10	192.168.10.1/24
G0/0/0.20	20	192.168.20.1/24
G0/0/0.30	99	192.168.99.1/24



## Troubleshoot Inter-VLAN Routing Missing VLANs

An inter-VLAN connectivity issue could be caused by a missing VLAN. The VLAN could be missing if it was not created, it was accidentally deleted, or it is not allowed on the trunk link.

When a VLAN is deleted, any ports assigned to that VLAN become inactive. They remain associated with the VLAN (and thus inactive) until you assign them to a new VLAN or recreate the missing VLAN. Recreating the missing VLAN would automatically reassign the hosts to it.

Use the **show interface *interface-id* switchport** command to verify the VLAN membership of the port.

```
S1(config)# do show interface fa0/6 switchport
Name: Fa0/6
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (Inactive)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
(Output omitted)
```



## Troubleshoot Inter-VLAN Routing Switch Trunk Port Issues

Another issue for inter-VLAN routing includes misconfigured switch ports. In a legacy inter-VLAN solution, this could be caused when the connecting router port is not assigned to the correct VLAN.

However, with a router-on-a-stick solution, the most common cause is a misconfigured trunk port.

- Verify that the port connecting to the router is correctly configured as a trunk link using the **show interface trunk** command.
- If that port is missing from the output, examine the configuration of the port with the **show running-config interface X** command to see how the port is configured.

```
S1# show interface trunk
Port      Mode          Encapsulation  Status      Native vlan
Fa0/1    on           802.1q        trunking    1
Port      Vlans allowed on trunk
Fa0/1    1-4094
Port      Vlans allowed and active in management domain
Fa0/1    1,10,20,99
Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1    1,10,20,99
S1#
```



## Troubleshoot Inter-VLAN Routing Switch Access Port Issues

When a problem is suspected with a switch access port configuration, use verification commands to examine the configuration and identify the problem.

A common indicator of this issue is the PC having the correct address configuration (IP Address, Subnet Mask, Default Gateway), but being unable to ping its default gateway.

- Use the **show vlan brief**, **show interface X switchport** or **show running-config interface X** command to verify the interface VLAN assignment.

```
S1# show interface fa0/6 switchport
Name: Fa0/6
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
```



## Troubleshoot Inter-VLAN Routing Router Configuration Issues

Router-on-a-stick configuration problems are usually related to subinterface misconfigurations.

- Verify the subinterface status using the **show ip interface brief** command.
- Verify which VLANs each of the subinterfaces is on. To do so, the **show interfaces** command is useful but it generates a great deal of additional unrequired output. The command output can be reduced using IOS command filters. In this example, use the **include** keyword to identify that only lines containing the letters “Gig” or “802.1Q”

```
R1# show interfaces | include Gig|802.1Q
GigabitEthernet0/0/0 is administratively down, line protocol is down
GigabitEthernet0/0/1 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID  1., loopback not set
GigabitEthernet0/0/1.10 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID  100.
GigabitEthernet0/0/1.20 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID  20.
GigabitEthernet0/0/1.99 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID  99.
R1#
```



Troubleshoot Inter-VLAN Routing

## Packet Tracer – Troubleshoot Inter-VLAN Routing

In this Packet Tracer activity, you will complete the following objectives:

- Part 1: Locate Network Problems
- Part 2: Implement the Solution
- Part 3: Verify Network Connectivity



Troubleshoot Inter-VLAN Routing

## Lab – Troubleshoot Inter-VLAN Routing

In this lab, you will complete the following objectives:

- Part 1: Build the Network and Load Device Configurations
- Part 2: Troubleshoot the Inter-VLAN Routing Configuration
- Part 3: Verify VLAN Configuration, Port Assignment and Trunking
- Part 4: Test Layer 3 Connectivity



# 4.5 Module Practice and Quiz

Module Practice and Quiz

## Packet Tracer – Inter-VLAN Routing Challenge

In this Packet Tracer activity, you will demonstrate and reinforce your ability to implement inter-VLAN routing, including configuring IP addresses, VLANs, trunking, and subinterfaces.



## Module Practice and Quiz

# Lab– Implement Inter-VLAN Routing

In this lab, you will complete the following objectives:

- Part 1: Build the Network and Configure Basic Device Settings
- Part 2: Create VLANs and Assign Switch Ports
- Part 3: Configure an 802.1Q Trunk between the Switches
- Part 4: Configure Inter-VLAN Routing on the S1 Switch
- Part 5: Verify Inter-VLAN Routing is Working



## Module Practice and Quiz

# What Did I Learn In This Module?

- Inter-VLAN routing is the process of forwarding network traffic from one VLAN to another VLAN.
- Three options include legacy, router-on-a-stick, and Layer 3 switch using SVIs.
- To configure a switch with VLANs and trunking, complete the following steps: create and name the VLANs, create the management interface, configure access ports, and configure trunking ports.
- The router-on-a-stick method requires a subinterface to be created for each VLAN to be routed. A subinterface is created using the **interface interface\_id subinterface\_id** global configuration mode command.
- Each router subinterface must be assigned an IP address on a unique subnet for routing to occur. When all subinterfaces have been created, the physical interface must be enabled using the no shutdown interface configuration command.
- Enterprise campus LANs use Layer 3 switches to provide inter-VLAN routing. Layer 3 switches use hardware-based switching to achieve higher-packet processing rates than routers.
- Capabilities of a Layer 3 switch include routing from one VLAN to another using multiple switched virtual interfaces (SVIs) and converting a Layer 2 switchport to a Layer 3 interface (i.e., a routed port).
- To provide inter-VLAN routing, Layer 3 switches use SVIs. SVIs are configured using the same **interface vlan vlan-id** command used to create the management SVI on a Layer 2 switch.



## Module Practice and Quiz

# What Did I Learn In This Module? (Cont.)

- To configure a switch with VLANs and trunking, complete the following steps: create the VLANs, create the SVI VLAN interfaces, configure access ports, and enable IP routing.
- To enable routing on a Layer 3 switch, a routed port must be configured. A routed port is created on a Layer 3 switch by disabling the switchport feature on a Layer 2 port that is connected to another Layer 3 device. The interface can be configured with an IPv4 configuration to connect to a router or another Layer 3 switch.
- To configure a Layer 3 switch to route with a router, follow these steps: configure the routed port, enable routing, configure routing, verify routing, and verify connectivity.
- There are a number of reasons why an inter-VAN configuration may not work. All are related to connectivity issues such as missing VLANs, switch trunk port issues, switch access port issues, and router configuration issues.
- A VLAN could be missing if it was not created, it was accidentally deleted, or it is not allowed on the trunk link.
- Another issue for inter-VLAN routing includes misconfigured switch ports.
- In a legacy inter-VLAN solution, a misconfigured switch port could be caused when the connecting router port is not assigned to the correct VLAN.



## Module Practice and Quiz

# What Did I Learn In This Module? (Cont.)

- With a router-on-a-stick solution, the most common cause is a misconfigured trunk port.
- When a problem is suspected with a switch access port configuration, use **ping** and **show interfaces interface-id switchport** commands to identify the problem.
- Router configuration problems with router-on-a-stick configurations are usually related to subinterface misconfigurations. Verify the subinterface status using the **show ip interface brief** command.



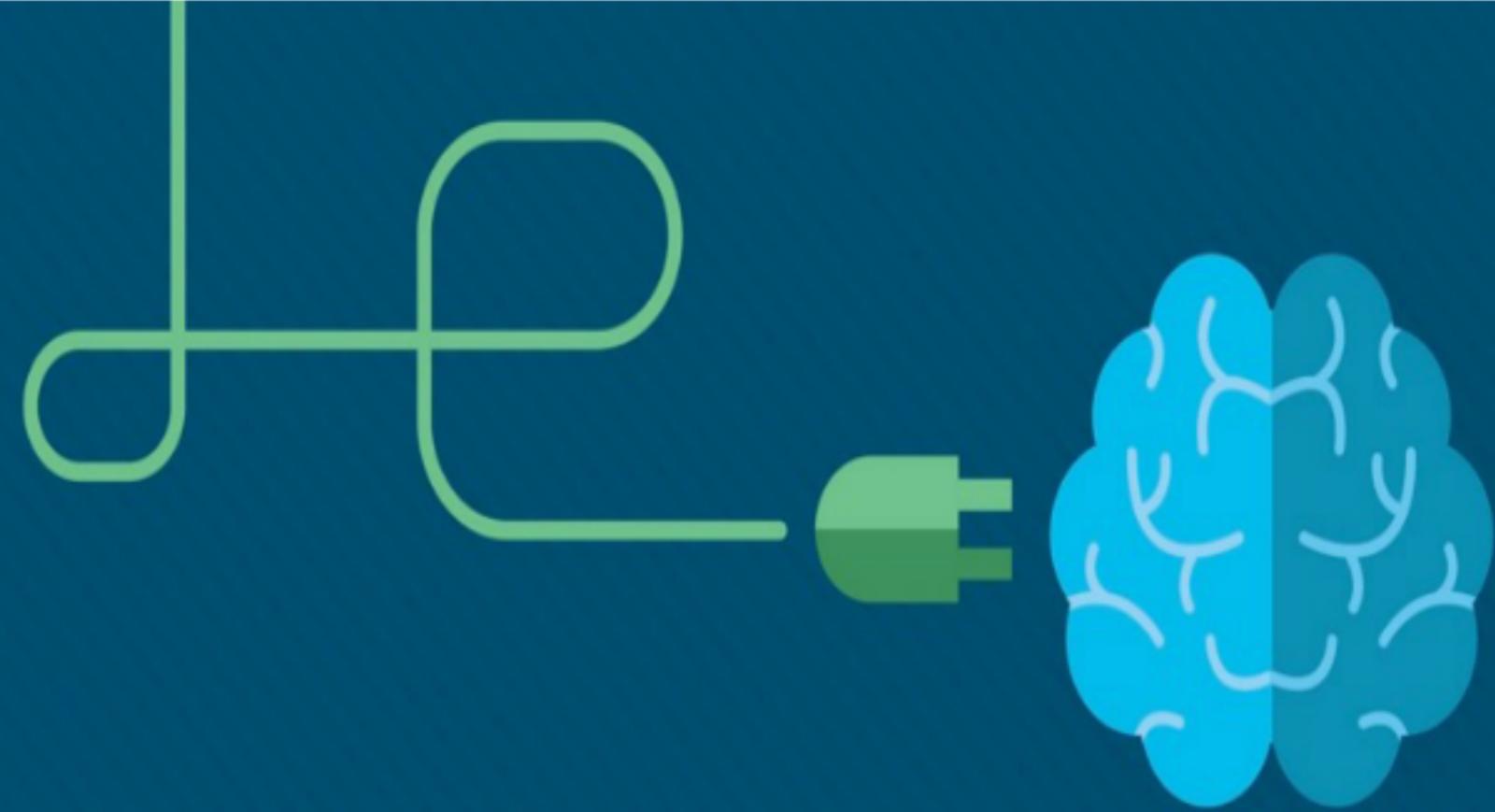
## Module 4: Basic Device Configuration

# New Terms and Commands

- Inter-VLAN Routing
- Router-on-a-Stick
- **encapsulation dot1q X [ native ]**
- **no switchport**
- **router ospf**
- **ip routing**







# Module 15: Application Layer

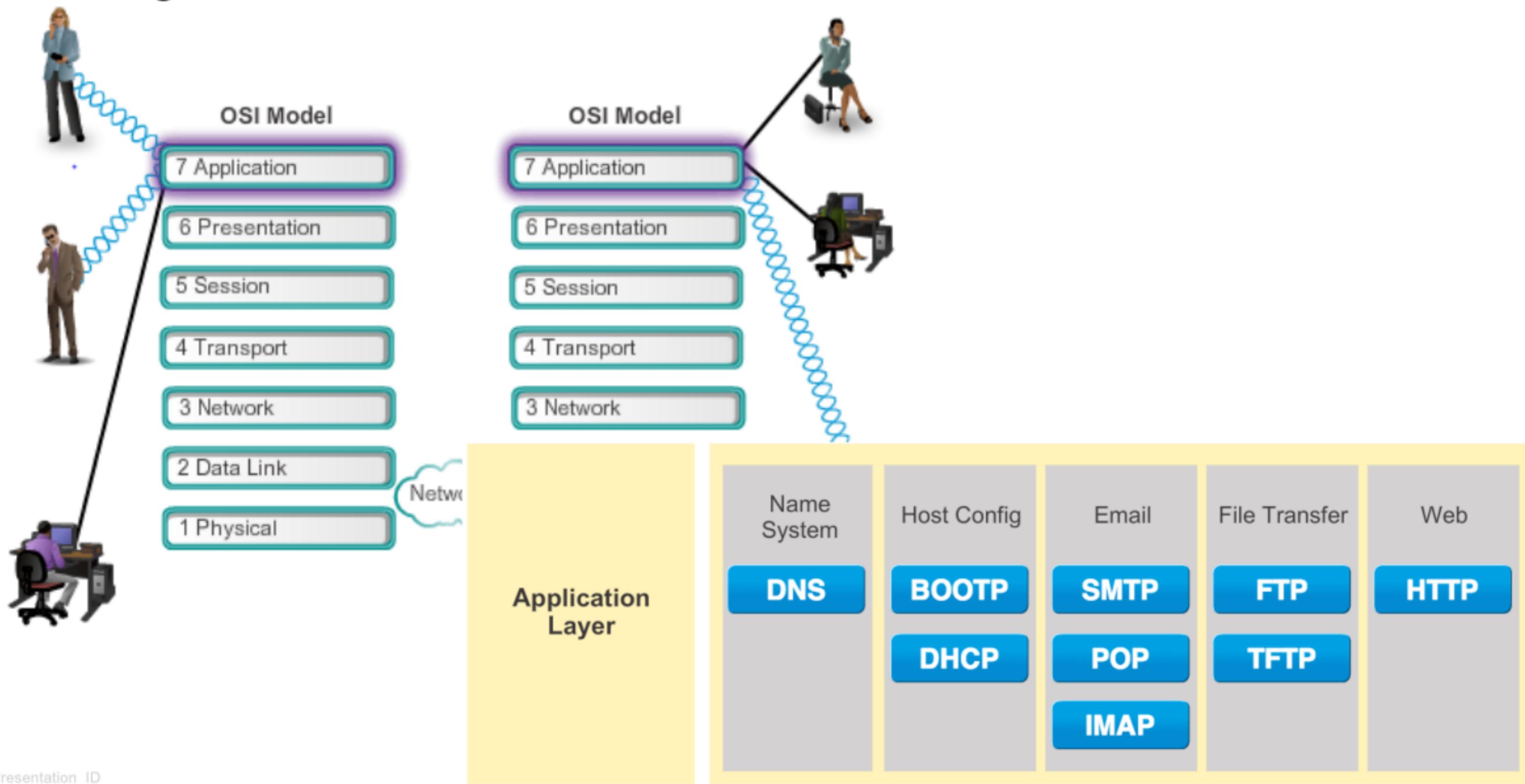
Introduction to Networks v7.0  
(ITN)





# Functions of the Application Layer

...provides the **interface between the applications** used to communicate, **and the underlying network** over which messages are transmitted.

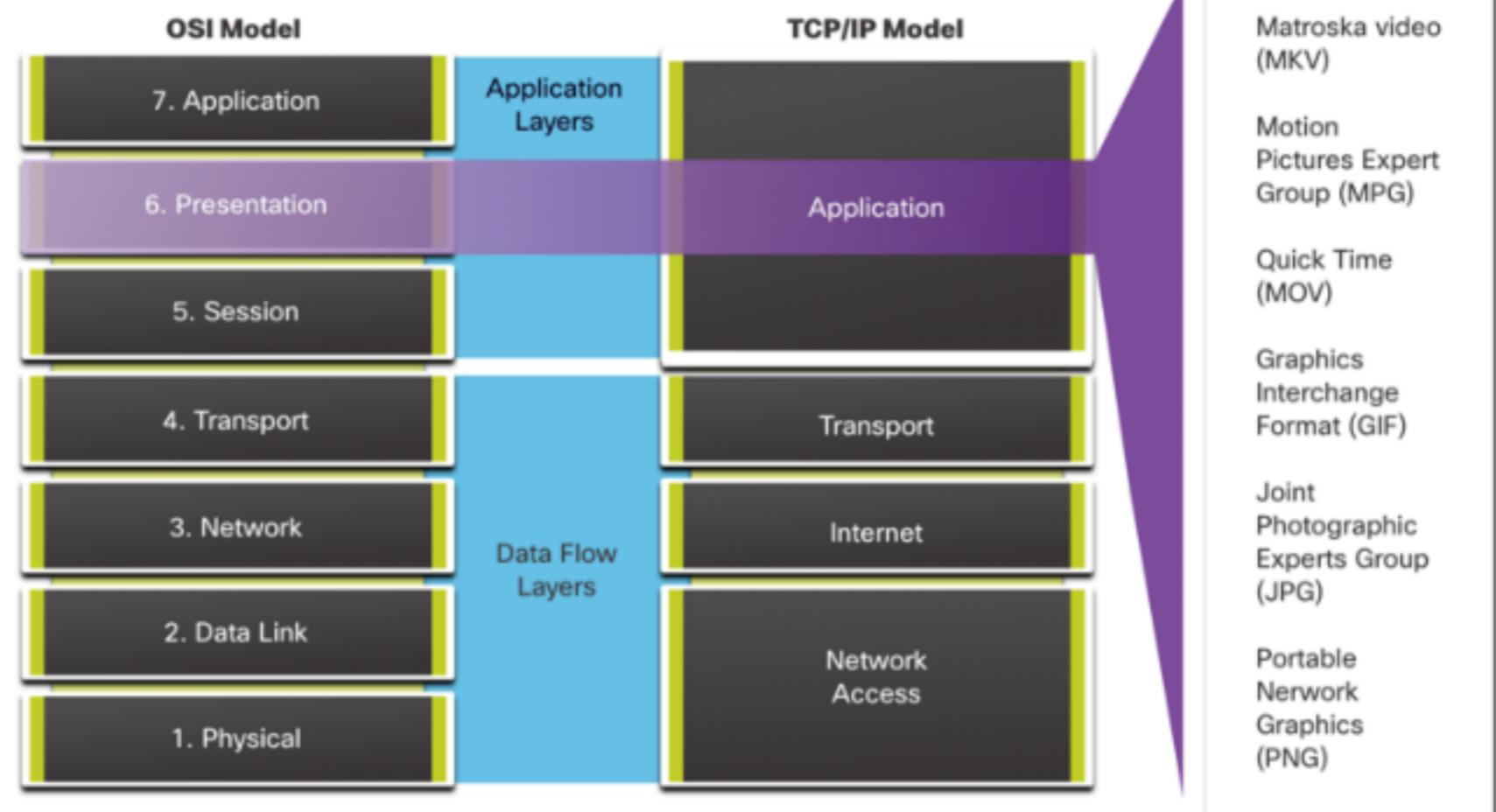




# Presentation and Session Layers

## Presentation layer primary functions:

- **Formatting (Presenting)**
- **Compressing**
- **Encrypting**



## Session Layer

- Functions **create and manage dialogs**
- Handles the **exchange of information** to initiate dialogs, keep them active, and to **restart sessions**

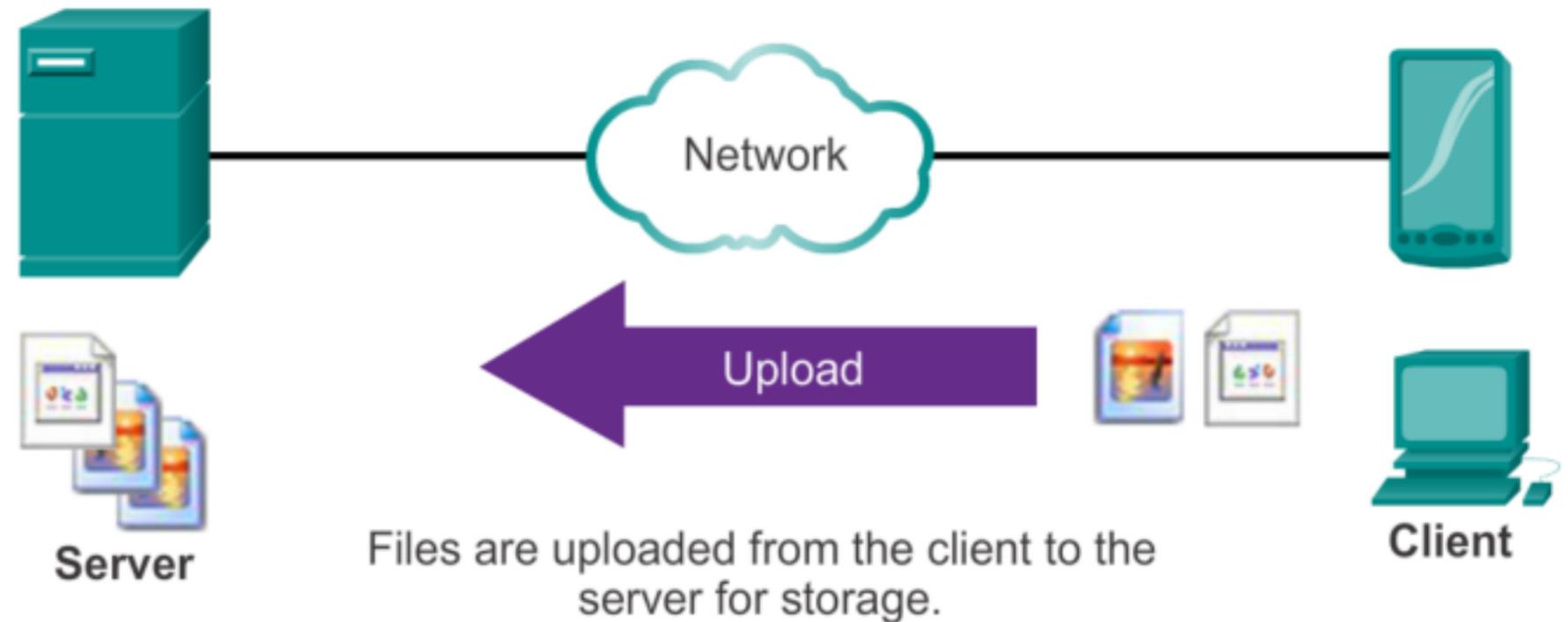


# How Application Protocols Interact with End-User Applications



Client

## Client/Server Model

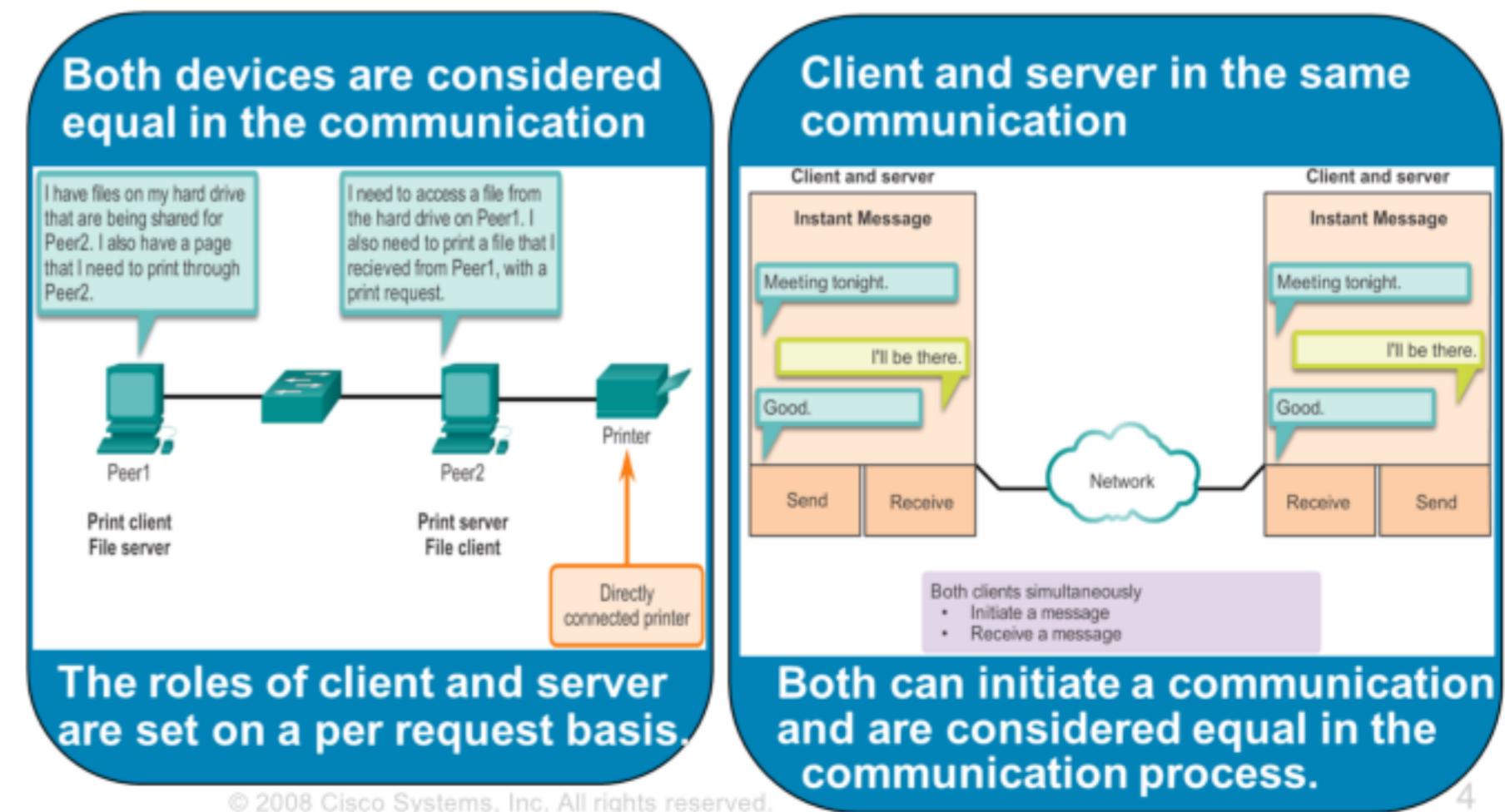


Files are uploaded from the client to the server for storage.

Resources are stored on the server.

A client is a hardware/software combination that people use directly.

## Peer-to-Peer Networks

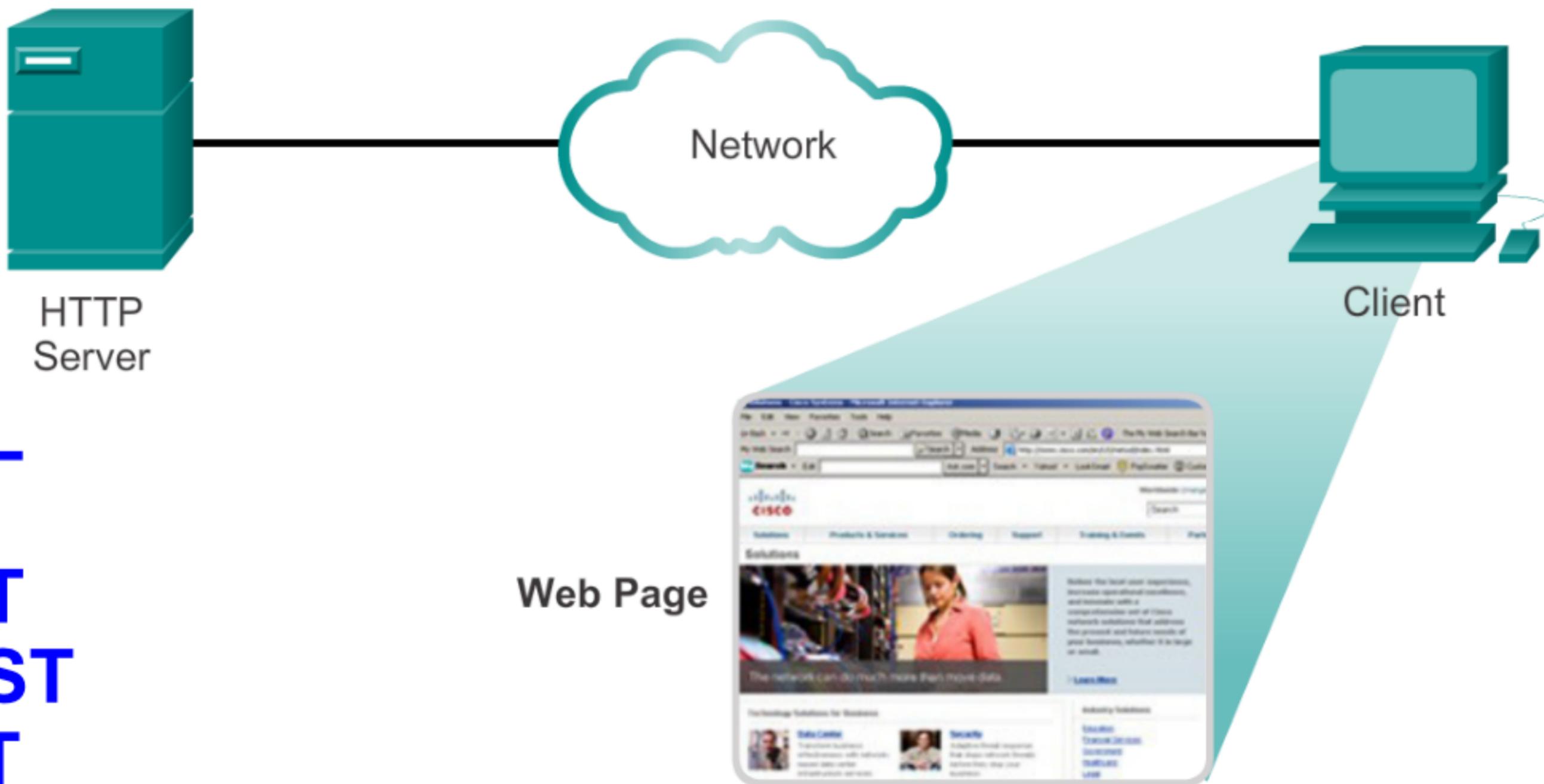


# 15.3 Web and Email Protocols



# HTTP and HTTPS – Publish and retrieve HTML pages

## HTTP Protocol Step 3



**URL**

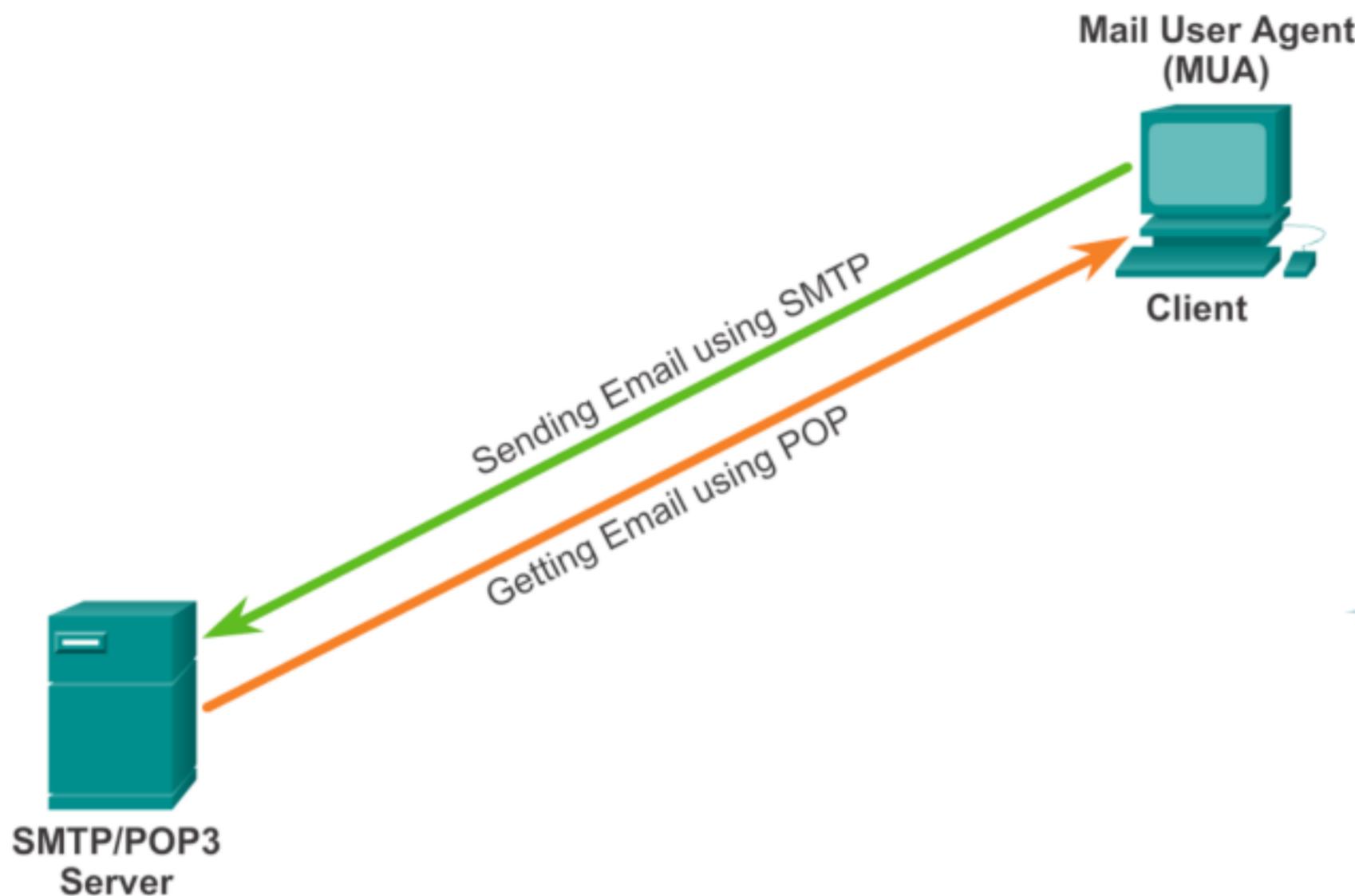
**GET  
POST  
PUT**

**Web Page**

**HTTPS**



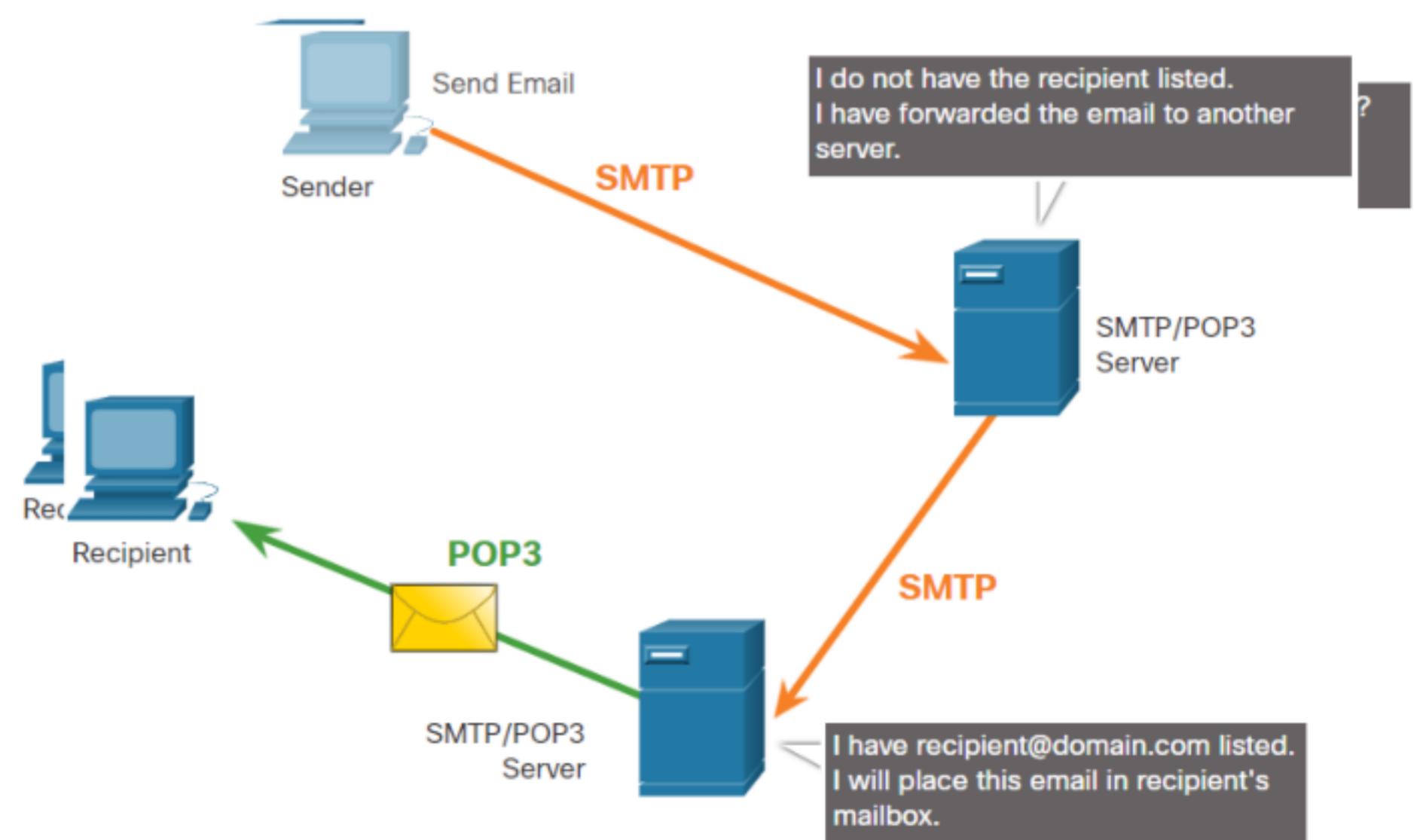
# SMTP, POP, and IMAP – send/receive Emails



**SMTP: send  
POP & IMAP: receive**

**Email clients communicate with mail servers to send & receive email.**

**Mail servers communicate with other mail servers to transport messages from one domain to another.**



# Domain Name Service (DNS) – resolve domain names

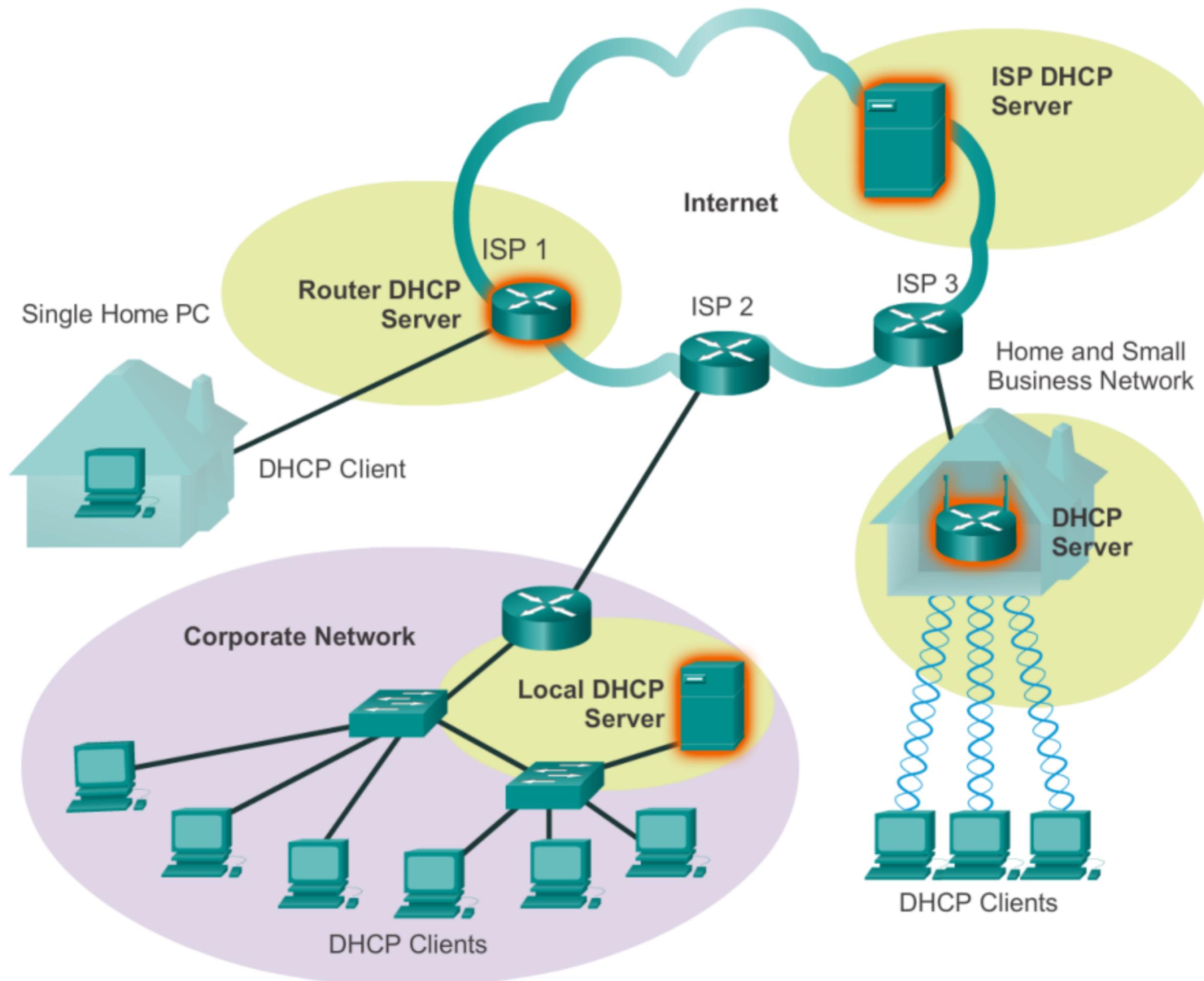
## Resolving DNS Addresses Step 5



**ipconfig /displaydns  
nslookup**

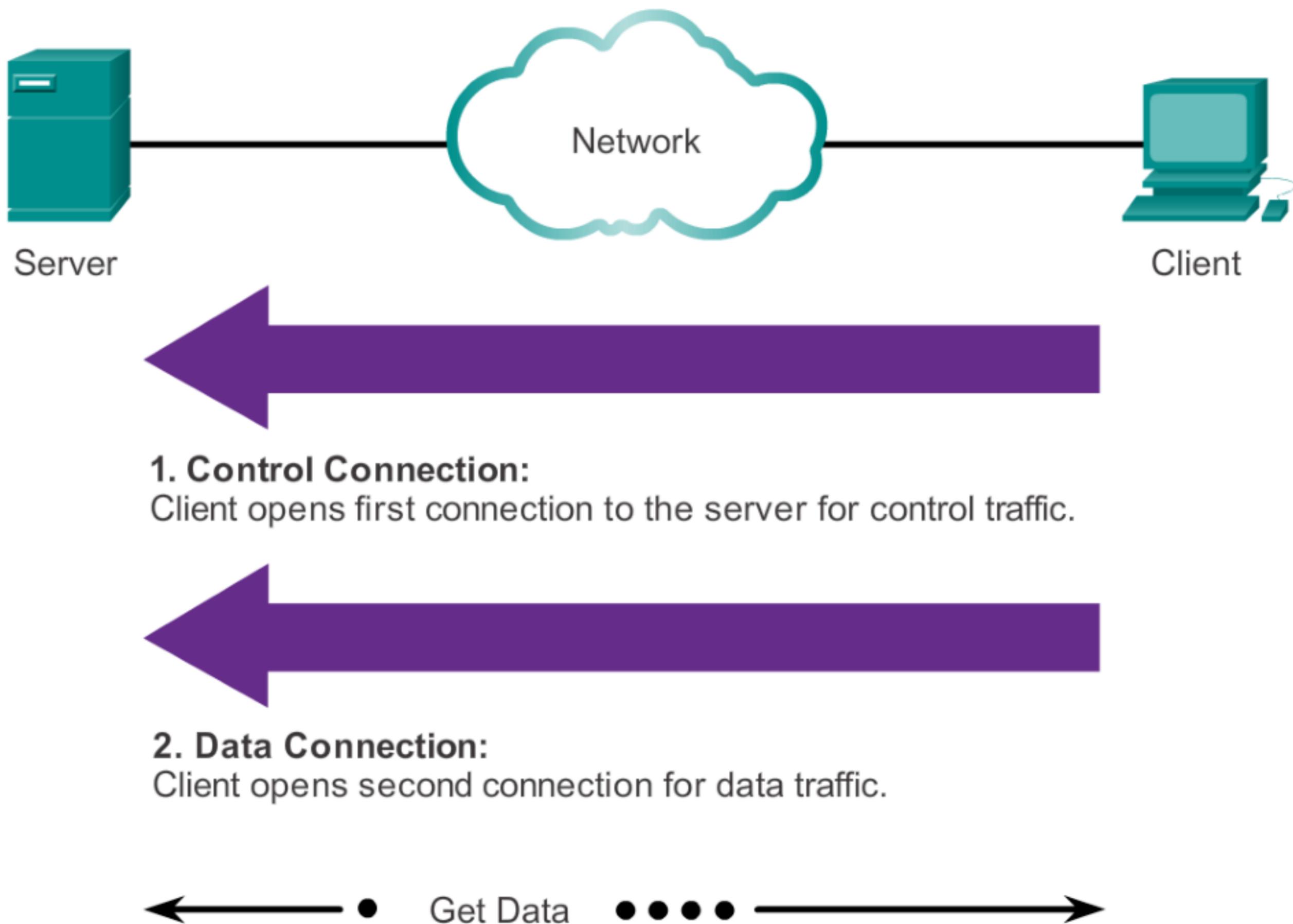


# Dynamic Host Configuration Protocol (DHCP)





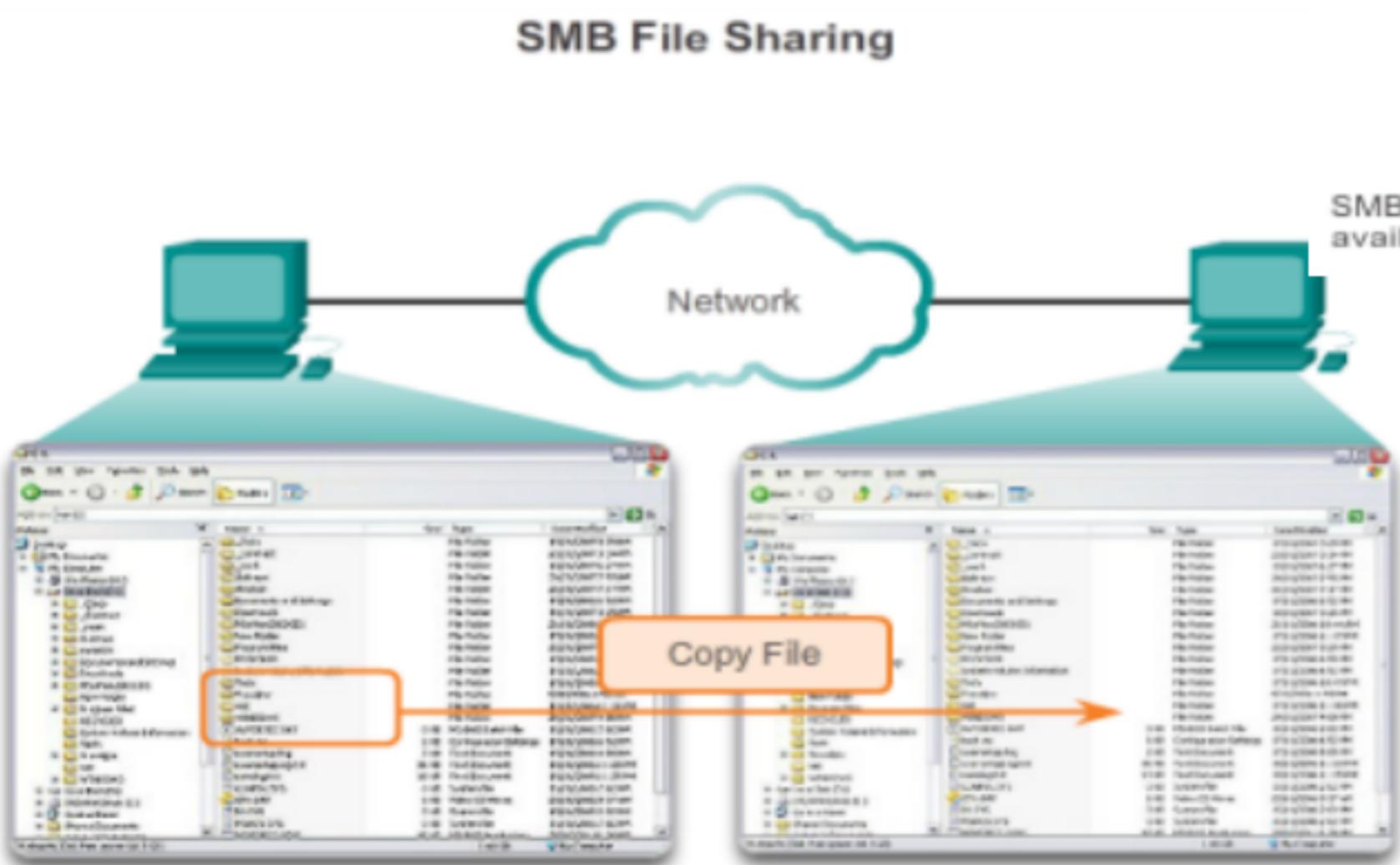
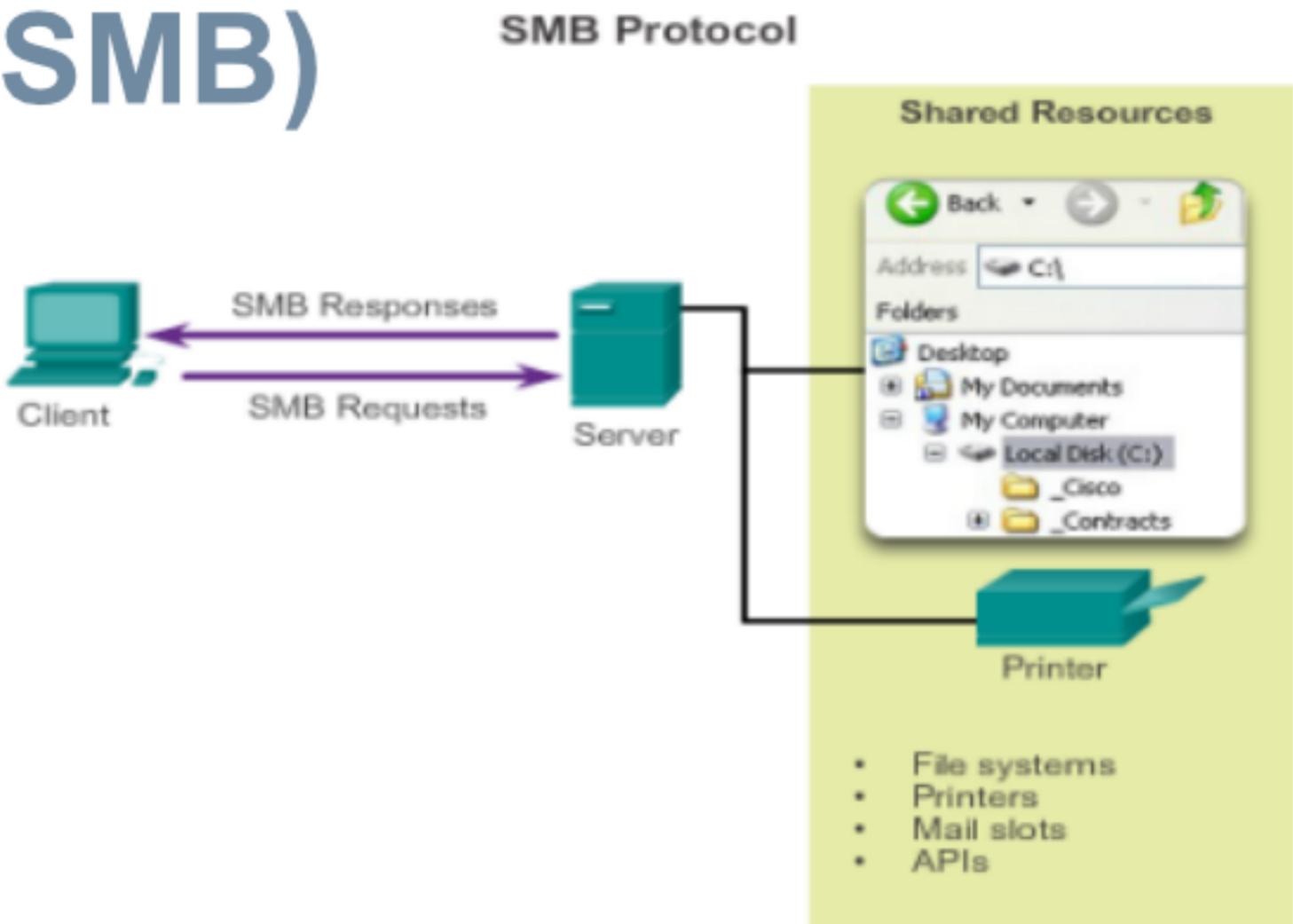
# File Transfer Protocol (FTP)





# Server Message Block (SMB)

- Clients establish a long term connection to servers.



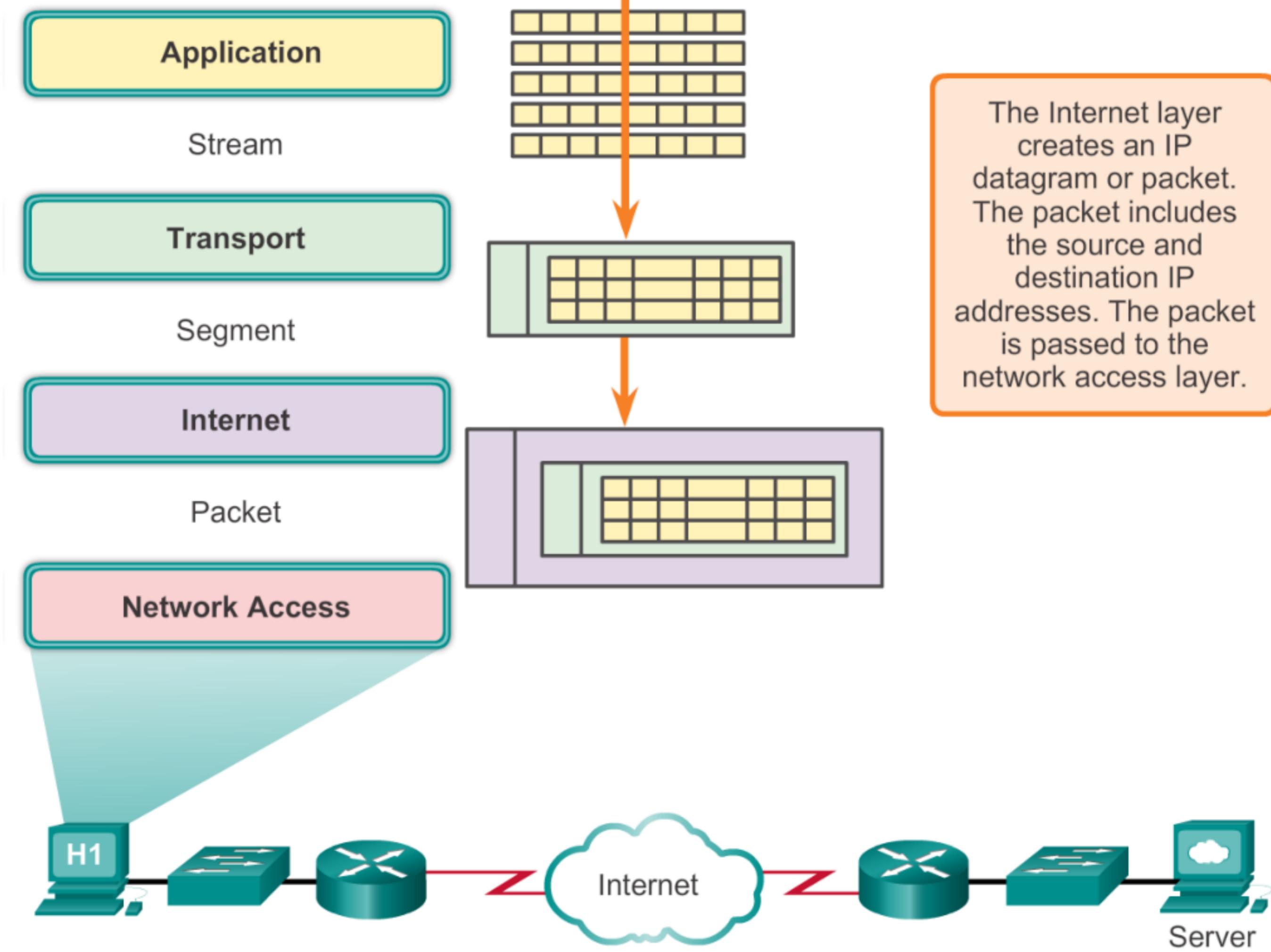
SMB is a client-server, request-response protocol. Servers can make their resources available to clients on the network.

- After the connection is established, the user can access the resources on the server as if the resource is local to the client host.

A file may be copied from PC to PC with Windows Explorer using the SMB protocol.



# Message Travels Through a Network





# Objectives

- Explain the **functions** of the application layer, session layer, and presentation layer.
- *Describe* how common application layer protocols interact with end user applications.
- *Describe*, at a high level, common application layer protocols that provide Internet services to end-users, including **WWW** services and **email**.
- *Describe* application layer protocols that provide IP addressing services, including **DNS** and **DHCP**.
- *Describe* the **features and operation of well-known application layer protocols** that allow for file sharing services, including: FTP, File Sharing Services, SMB protocol.
- Explain how data is moved across the network, from opening an application to receiving data.

## Lab – Identifying IPv4 Addresses

### Objectives

#### Part 1: Classify IPv4 Addresses

- Identify the type of address (network, host, multicast, or broadcast).
- Identify whether an address is public or private.
- Determine if an address assignment is a valid host address.

#### Part 2: Identify IPv4 Addresses

- Identify the network and host portion of an IP address.
- Identify the range of host addresses given a network/prefix mask pair.

### Background / Scenario

Addressing is an important function of network layer protocols because it enables data communication between hosts on the same network, or on different networks.

In this lab, you will examine the structure of Internet Protocol version 4 (IPv4) addresses. You will identify the various types of IPv4 addresses and the components that help comprise the address, such as network portion, host portion, and subnet mask. Types of addresses covered include public, private, unicast, and multicast.

### Part 1: Identify IPv4 Addresses

In Part 1, you will be given several examples of IPv4 addresses and will complete tables with appropriate information.

#### Step 1: Analyze the table shown below and identify the network portion and host portion of the given IPv4 addresses.

The first two rows show examples of how the table should be completed.

##### Key for table:

N = all 8 bits for an octet are in the network portion of the address  
n = a bit in the network portion of the address  
H = all 8 bits for an octet are in the host portion of the address  
h = a bit in the host portion of the address

IP Address/Prefix	Network/Host N,n = Network	Subnet Mask	Network Address
	H,h = Host		
192.168.10.10/24	N.N.H	255.255.255.0	192.168.10.0
10.101.99.17/23	N.N.nnnnnnnh.H	255.255.254.0	10.101.98.0
209.165.200.227/27	255.255.255.224		
172.31.45.252/24			
10.1.8.200/26	11110000	10.1.8.192	192
172.16.117.77/20		172.16.240.0	112.0
10.1.1.101/25		10.1.1.128	10.1.1.0
209.165.202.140/27		209.165.202.224	128
192.168.28.45/28	11110000	192.168.28.240	32

0001

**Step 2:** Analyze the table below and list the range of host and broadcast addresses given a network/prefix mask pair.

The first row shows an example of how the table should be completed.

IP Address/Prefix	First Host Address	Last Host Address	Broadcast Address
192.168.10.10/24	192.168.10.1	192.168.10.254	192.168.10.255
10.101.99.17/23			
209.165.200.227/27			
172.31.45.252/24			
10.1.8.200/26			
172.16.117.77/20			
10.1.1.101/25			
209.165.202.140/27			
192.168.28.45/28			

## Part 2: Classify IPv4 Addresses

In Part 2, you will identify and classify several examples of IPv4 addresses.

## Lab – Identifying IPv4 Addresses

---

**Step 1:** Analyze the table shown below and identify the type of address (network, host, multicast, or broadcast address).

The first row shows an example of how the table should be completed.

IP Address	Subnet Mask	Address Type
10.1.1.1	255.255.255.252	host
192.168.33.63	255.255.255.192	
239.192.1.100	255.252.0.0	
172.25.12.52	255.255.255.0	
10.255.0.0	255.0.0.0	
172.16.128.48	255.255.255.240	
209.165.202.159	255.255.255.224	
172.16.0.255	255.255.0.0	
224.10.1.11	255.255.255.0	

**Step 2:** Analyze the table shown below and identify the address as **public** or **private**.

IP Address/Prefix	Public or Private
209.165.201.30/27	
192.168.255.253/24	
10.100.11.103/16	
172.30.1.100/28	
192.31.7.11/24	
172.20.18.150/22	
128.107.10.1/16	
192.135.250.10/24	
64.104.0.11/16	

## Lab – Identifying IPv4 Addresses

---

**Step 3:** Analyze the table shown below and identify whether the address/prefix pair is a **valid host address**.

IP Address/Prefix	Valid Host Address?	Reason
127.1.0.10/24		
172.16.255.0/16		
241.19.10.100/24		
192.168.0.254/24		
192.31.7.255/24		
64.102.255.255/14		
224.0.0.5/16		
10.0.255.255/8		
198.133.219.8/24		

## Reflection

Why should we continue to study and learn about IPv4 addressing if the available IPv4 address space is depleted?

---

---

In the following questions, assume the following extract from a router's routing table:

```
172.16.0.0/16 is variably subnetted, 6 subnets, 4 masks
R    172.16.1.0/24 [120/1] via 172.16.2.1, 00:00:18, Serial 0/0
C    172.16.2.0/30 is directly connected, Serial 0/0
C    172.16.3.0/30 is directly connected, Serial 0/1
O    172.16.4.0/27 [110/128] via 172.16.2.1, 14:27:57, Serial 0/0
O    172.16.5.0/28 [110/65] via 172.16.3.2, 14:27:57, Serial 0/1
R    172.16.8.0/24 [120/2] via 172.16.2.1, 00:00:18, Serial 0/0
S    200.44.0.0/14 [1/0] via 192.168.2.2
C    192.168.2.0/24 is directly connected, FastEthernet 0/0
C    192.168.5.0/24 is directly connected, Loopback 0
```

- 1) What routing sources is/are this router using?
- 2) To which interface does the router send packets destined for **172.16.4.8**?
- 3) How did this router learn about the route to network **172.16.8.0 255.255.255.0**?
- 4) What are the useable addresses in the network attached to interface **Serial 0/0**?  
How are they being used?
- 5) How many **active physical interfaces** does this router have attached to it?  
What are they?
- 6) What is the address on the interface **Serial 0/1**?
- 7) Write the command(s) which would have caused the entry for **200.44.0.0** to be produced.  
What sort of network does this refer to?
- 8) Describe how the router deals with a packet destined for **200.44.22.5**.



# Module 2: Switching Concepts

Switching, Routing, and  
Wireless Essentials v7.0  
(SRWE)



# Module Objectives

**Module Title:** Switching Concepts

**Module Objective:** Explain how Layer 2 switches forward data.

Topic Title	Topic Objective
Frame Forwarding	Explain how frames are forwarded in a switched network.
Switching Domains	Compare a collision domain to a broadcast domain.



# 2.1 Frame Forwarding



## Frame Forwarding Switching in Networking

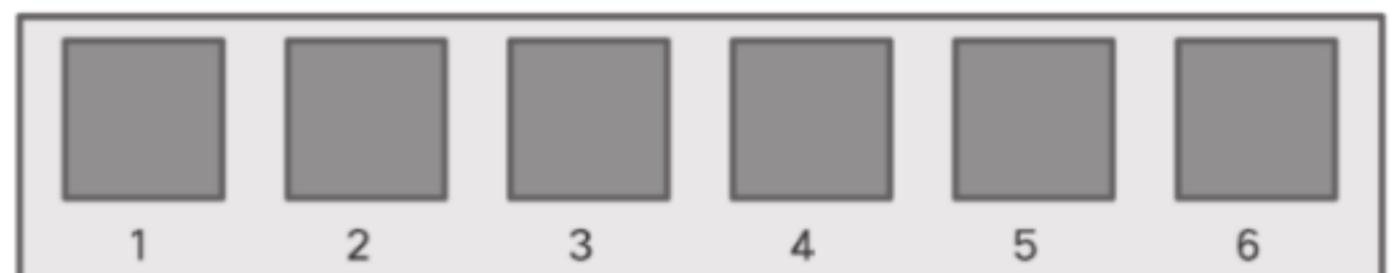
Two terms are associated with frames entering or leaving an interface:

- **Ingress** – entering the interface
- **Egress** – exiting the interface

A switch forwards based on the ingress interface and the destination MAC address.

A switch uses its MAC address table to make forwarding decisions.

**Note:** A switch will never allow traffic to be forwarded out the interface it received the traffic.



Port Table

Destination Addresses	Port
EE	1
AA	2
BA	3
EA	4
AC	5
AB	6

## Frame Forwarding

# The Switch MAC Address Table

A switch will use the destination MAC address to determine the egress interface.

Before a switch can make this decision it must learn what interface the destination is located.

A switch builds a MAC address table, also known as a Content Addressable Memory (CAM) table, by recording the source MAC address into the table along with the port it was received.



## Frame Forwarding

# The Switch Learn and Forward Method



The switch uses a two step process:

### **Step 1. Learn – Examines Source Address**

- Adds the source MAC if not in table
- Resets the time out setting back to 5 minutes if source is in the table

### **Step 2. Forward – Examines Destination Address**

- If the destination MAC is in the MAC address table it is forwarded out the specified port.
- If a destination MAC is not in the table, it is flooded out all interfaces except the one it was received.

## Frame Forwarding

# Video – MAC Address Tables on Connected Switches

This video will cover the following:

- How switches build MAC address tables
- How switches forward frames based on the content of their MAC address tables



## Frame Forwarding

# Switch Forwarding Methods

Switches use software on application-specific-integrated circuits (ASICs) to make very quick decisions.

A switch will use one of two methods to make forwarding decisions after it receives a frame:

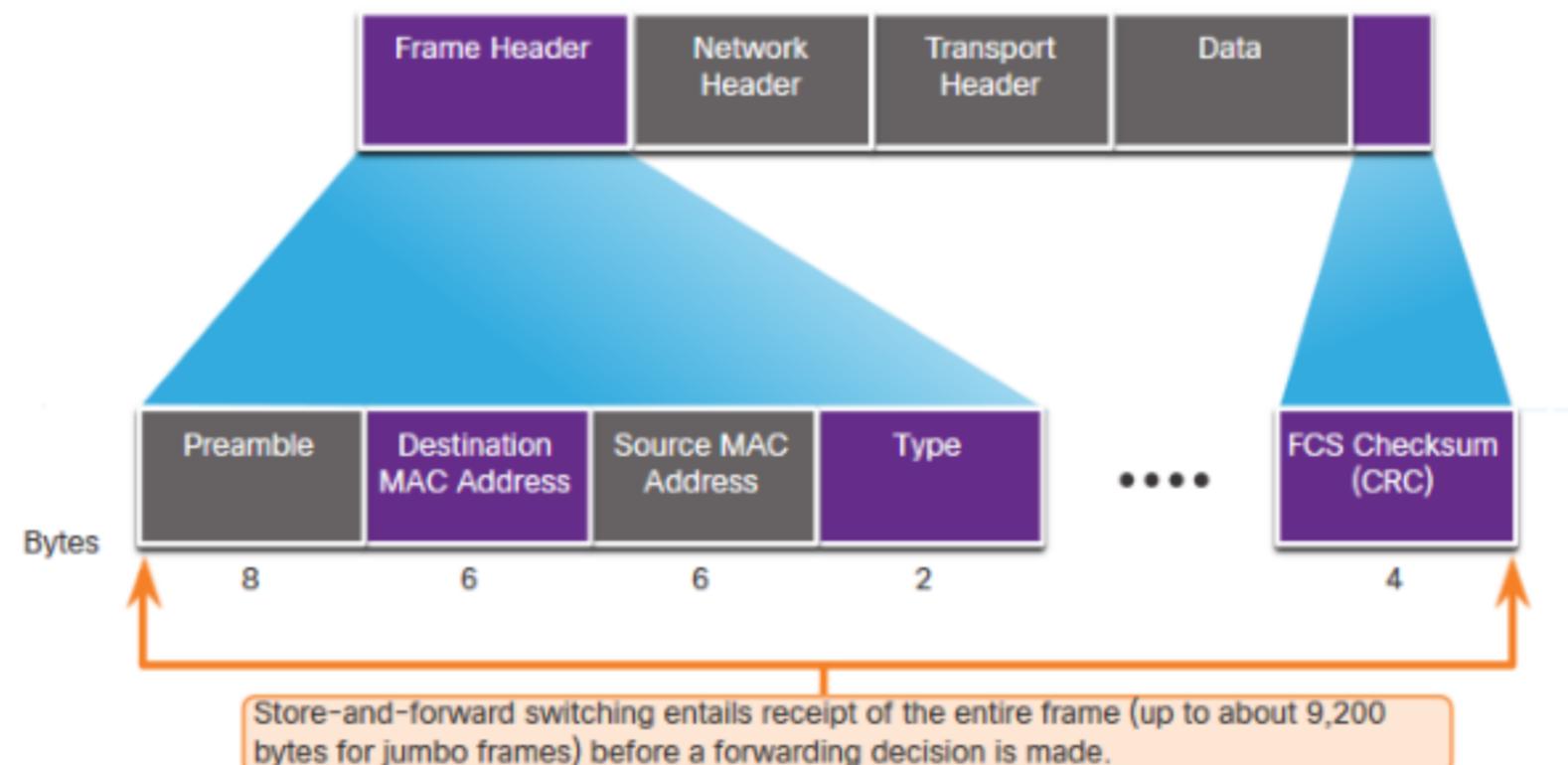
- **Store-and-forward switching** - Receives the entire frame and ensures the frame is valid. Store-and-forward switching is Cisco's preferred switching method.
- **Cut-through switching** – Forwards the frame immediately after determining the destination MAC address of an incoming frame and the egress port.

## Frame Forwarding

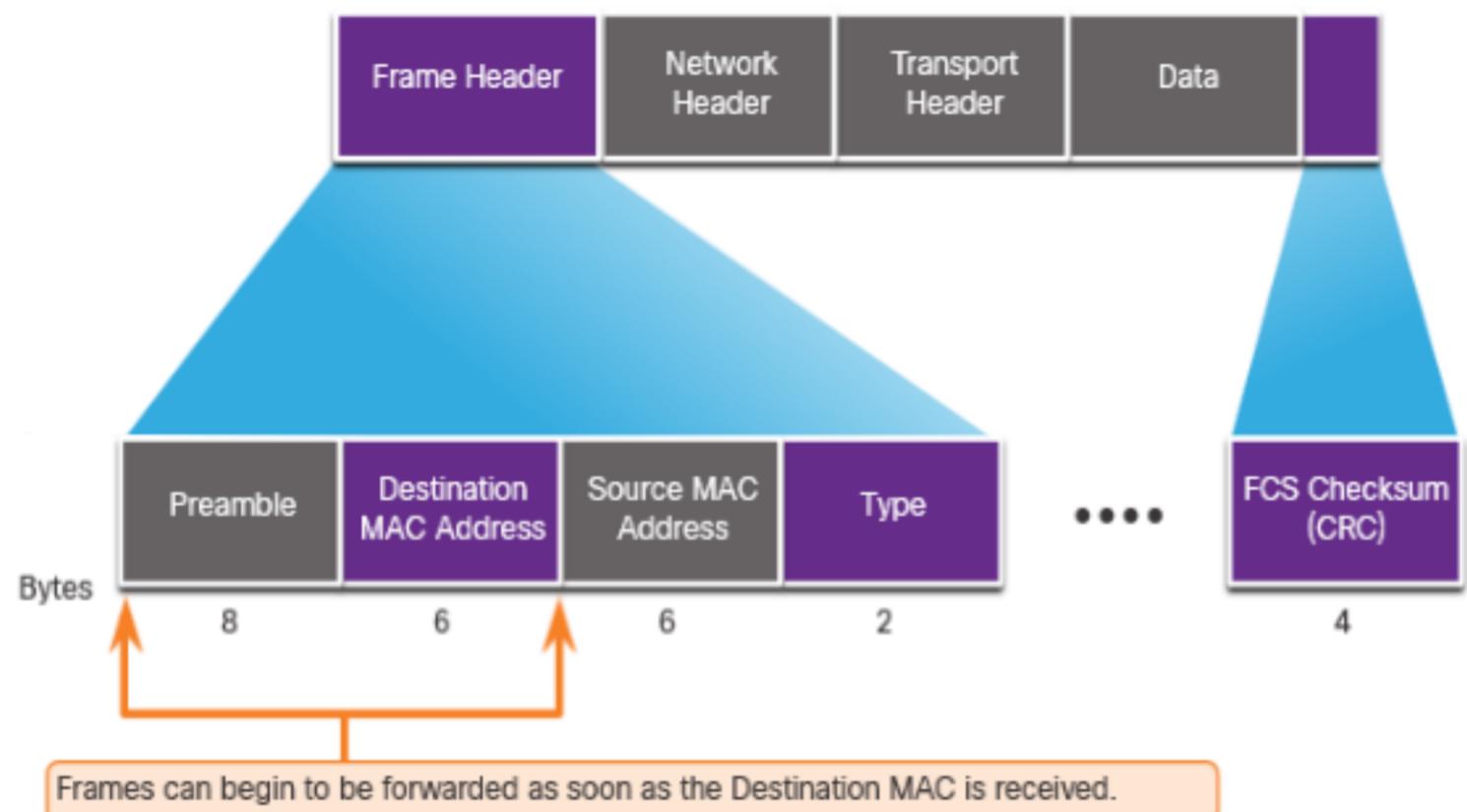
# Store-and-Forward Switching

Store-and-forward has two primary characteristics:

- Error Checking – The switch will check the Frame Check Sequence (FCS) for CRC errors. Bad frames will be discarded.
- Buffering – The ingress interface will buffer the frame while it checks the FCS. This also allows the switch to adjust to a potential difference in speeds between the ingress and egress ports.



# Frame Forwarding Cut-Through Switching



- Cut-through forwards the frame immediately after determining the destination MAC.
- Fragment (Frag) Free method will check the destination and ensure that the frame is at least 64 Bytes. This will eliminate runts.

Concepts of Cut-Through switching:

- Is appropriate for switches needing latency to be under 10 microseconds
- Does not check the FCS, so it can propagate errors
- May lead to bandwidth issues if the switch propagates too many errors
- Cannot support ports with differing speeds going from ingress to egress

## 2.2 Switching Domains

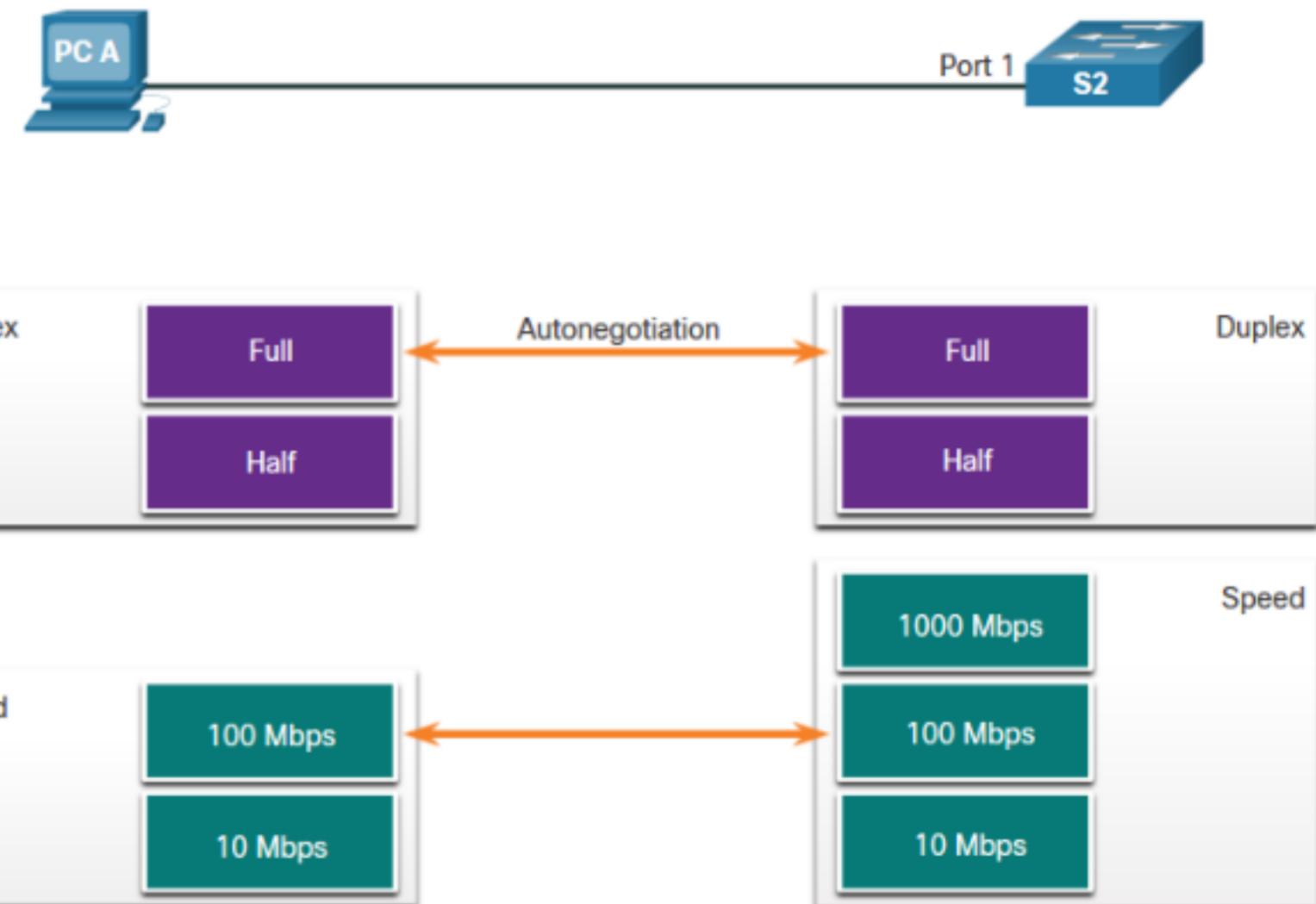


## Switching Domains

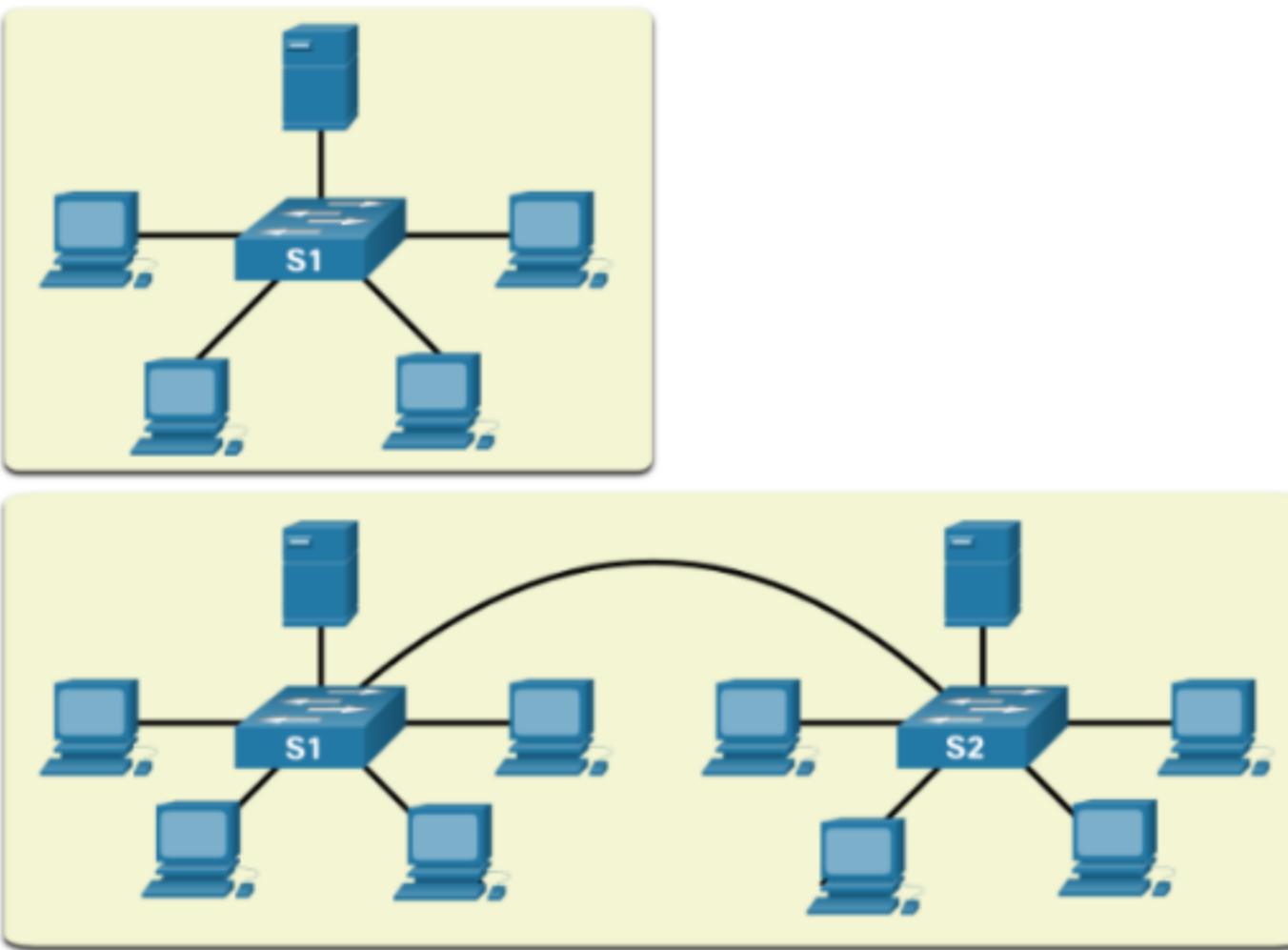
## Collision Domains

Switches eliminate collision domains and reduce congestion.

- When there is full duplex on the link the collision domains are eliminated.
- When there is one or more devices in half-duplex there will now be a collision domain.
  - There will now be contention for the bandwidth.
  - Collisions are now possible.
- Most devices, including Cisco and Microsoft use auto-negotiation as the default setting for duplex and speed.



## Switching Domains Broadcast Domains



- A broadcast domain extends across all Layer 1 or Layer 2 devices on a LAN.
  - Only a layer 3 device (router) will break the broadcast domain, also called a MAC broadcast domain.
  - The broadcast domain consists of all devices on the LAN that receive the broadcast traffic.
- When the layer 2 switch receives the broadcast it will flood it out all interfaces except for the ingress interface.
- Too many broadcasts may cause congestion and poor network performance.
- Increasing devices at Layer 1 or layer 2 will cause the broadcast domain to expand.

## Switching Domains

# Alleviated Network Congestion

Switches use the MAC address table and full-duplex to eliminate collisions and avoid congestion.

Features of the switch that alleviate congestion are as follows:

Protocol	Function
Fast Port Speeds	Depending on the model, switches may have up to 100Gbps port speeds.
Fast Internal Switching	This uses fast internal bus or shared memory to improve performance.
Large Frame Buffers	This allows for temporary storage while processing large quantities of frames.
High Port Density	This provides many ports for devices to be connected to LAN with less cost. This also provides for more local traffic with less congestion.



## 2.3 Module Practice and Quiz

## Module Practice and Quiz

# What did I learn in this module?

### Frame Forwarding

- Ingress is the entry port, egress is the exit port.
- The switch builds a MAC address table to forward frames on the LAN.
- The switch can use either the store-and-forward or cut-through method of switch forwarding.

### Switching Domains

- Ethernet ports in half-duplex will be a part of a collision domain.
- Full-duplex will eliminate collision domains.
- A switch will flood out all interfaces except the ingress port if the frame is a broadcast or if the unicast destination MAC is unknown.
- Broadcast domains may be broken up by a layer 3 device, like a router.
- Switches extend broadcast domains, but can eliminate collision domains and relieve congestion.



## New Terms and Commands

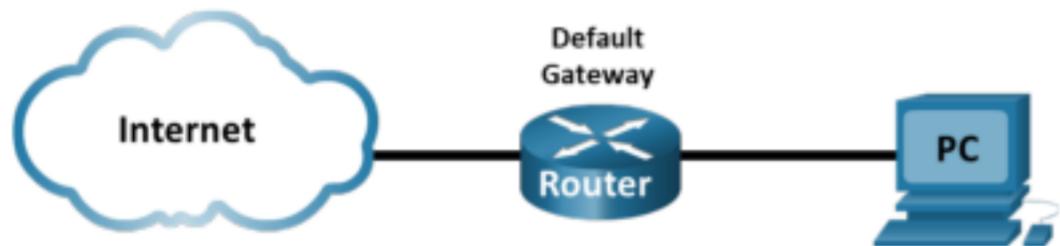
- content accessible memory (CAM)
- MAC address table
- store-and-forward switching
- cut-through switching
- automatic buffering
- fragment free switching
- collision domains
- broadcast domains





## Week 6 Lab.1 – Identifying IPv6 Addresses

### Topology



### Objectives

- Part 1: Practice IPv6 Address Abbreviation
- Part 2: Identify the Different Types of IPv6 Addresses
- Part 3: Examine a Host IPv6 Network Interface and Address

### Background / Scenario

With the depletion of the Internet Protocol version 4 (IPv4) network address space and the adoption and transition to IPv6, networking professionals must understand how both IPv4 and IPv6 networks function. Many devices and applications already support IPv6. This includes extensive Cisco device Internetwork Operating System (IOS) support and workstation/server operating system support, such as that found in Windows and Linux.

This lab focuses on IPv6 addresses and the components of the address. In Part 1, you will practice IPv6 address abbreviation, and in Part 2, you will identify the IPv6 address types. In Part 3, you will view the IPv6 settings on a PC.

### Part 1: Practice IPv6 Address Abbreviation

In Part 1, you will study and review rules for IPv6 address abbreviation to correctly compress and decompress IPv6 addresses.

#### Step 1: Study and review the rules for IPv6 address abbreviation.

**Rule 1:** In an IPv6 address, a string of four zeros (0s) in a hextet can be abbreviated as a single zero.

2001:0404:0001:1000:**0000:0000**:0EF0:BC00  
2001:0404:0001:1000:**0:0**EF0:BC00 (abbreviated with single zeros)

**Rule 2:** In an IPv6 address, the leading zeros in each hextet can be omitted, trailing zeros cannot be omitted.

2001:**0**404:**0001**:1000:0000:0000:0EF0:BC00  
2001:404:1:1000:0:0:EF0:BC00 (abbreviated with leading zeros omitted)

**Rule 3:** In an IPv6 address, a single continuous string of four or more zeros can be abbreviated as a double colon (::). The double colon abbreviation can only be used one time in an IP address.

2001:0404:0001:1000:**0000:0000**:0EF0:BC00  
2001:404:1:1000::EF0:BC00 (abbreviated with leading zeroes omitted and continuous zeros replaced with a double colon)

The image below illustrates these rules of IPv6 address abbreviation:

## Lab – Identifying IPv6 Addresses

---

FF01:0000:0000:0000:0000:0000:0000:1

= FF01:0:0:0:0:0:1

= FF01::1

E3D7:0000:0000:0000:51F4:00C8:C0A8:6420

= E3D7::51F4:C8:C0A8:6420

3FFE:0501:0008:0000:0260:97FF:FE40:EFAB

= 3FFE:501:8:0:260:97FF:FE40:EFAB

= 3FFE:501:8::260:97FF:FE40:EFAB

### Step 2: Practice compressing and decompressing IPv6 addresses.

Using the rules of IPv6 address abbreviation, either compress or decompress the following addresses:

1) 2002:0EC0:0200:0001:0000:04EB:44CE:08A2

2) FE80:0000:0000:0001:0000:60BB:008E:7402

3) FE80::7042:B3D7:3DEC:84B8

4) FF00::

5) 2001:0030:0001:ACAD:0000:330E:10C2:32BF

## Part 2: Identify the Different Types of IPv6 Addresses

In Part 2, you will review the characteristics of IPv6 addresses to identify the different types of IPv6 addresses.

### Step 1: Review the different types of IPv6 addresses.

An IPv6 address is 128 bits long. It is most often presented as 32 hexadecimal characters. Each hexadecimal character is the equivalent of 4 bits ( $4 \times 32 = 128$ ). A non-abbreviated IPv6 host address is shown here:

**2001:0DB8:0001:0000:0000:0000:0000:0001**

A hextet is the hexadecimal, IPv6 version of an IPv4 octet. An IPv4 address is 4 octets long, separated by dots. An IPv6 address is 8 hextets long, separated by colons.

An IPv4 address is 4 octets and is commonly written or displayed in decimal notation.

**255.255.255.255**

An IPv6 address is 8 hextets and is commonly written or displayed in hexadecimal notation.

**FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF**

In an IPv4 address, each individual octet is 8 binary digits (bits). Four octets equals one 32-bit IPv4 address.

## Lab – Identifying IPv6 Addresses

---

**11111111 = 255**

**11111111.11111111.11111111.11111111 = 255.255.255.255**

In an IPv6 address, each individual hextet is 16 bits long. Eight hextets equals one 128-bit IPv6 address.

**1111111111111111 = FFFF**

**1111111111111111.1111111111111111.1111111111111111.1111111111111111 =**

**1111111111111111.1111111111111111.1111111111111111.1111111111111111 =**

**FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF**

If we read an IPv6 address starting from the left, the first (or far left) hextet identifies the IPv6 address type. For example, if the IPv6 address has all zeros in the far left hextet, then the address is possibly a loopback address.

**0000:0000:0000:0000:0000:0000:0001 = loopback address**

**::1 = loopback address abbreviated**

As another example, if the IPv6 address has FE80 in the first hextet, then the address is a link-local address.

**FE80:0000:0000:0000:C5B7:CB51:3C00:D6CE = link-local address**

**FE80::C5B7:CB51:3C00:D6CE = link-local address abbreviated**

Study the chart below to help you identify the different types of IPv6 address based on the numbers in the first hextet.

First Hextet (Far Left)	Type of IPv6 Address
0000 to 00FF	Loopback address, any address, unspecified address, or IPv4-compatible
2000 to 3FFF	Global unicast address (a routable address in a range of addresses that is currently being handed out by the Internet Assigned Numbers Authority [IANA])
FE80 to FEBF	Link-local (a unicast address which identifies the host computer on the local network)
FC00 to FCFF	Unique-local (a unicast address which can be assigned to a host to identify it as being part of a specific subnet on the local network)
FF00 to FFFF	Multicast address

There are other IPv6 address types that are either not yet widely implemented, or have already become deprecated, and are no longer supported. For instance, an **anycast address** is new to IPv6 and can be used by routers to facilitate load sharing and provide alternate path flexibility if a router becomes unavailable. Only routers should respond to an anycast address. Alternatively, **site-local addresses** have been deprecated and replaced by unique-local addresses. Site-local addresses were identified by the numbers FEC0 in the initial hextet.

In IPv6 networks, there are no network (wire) addresses or broadcast addresses as there are in IPv4 networks.

### Step 2: Match the IPv6 address to its type.

Match the IPv6 addresses to their corresponding address type. Notice that the addresses have been compressed to their abbreviated notation and that the slash network prefix number is not shown. Some answer choices must be used more than once.

## Lab – Identifying IPv6 Addresses

---

IPv6 Address	Answer
2001:0DB8:1:ACAD::FE55:6789:B210	1. <u>B</u>
::1	2. <u>A</u>
FC00:22:A:2::CD4:23E4:76FA	3. <u>D</u>
2033:DB8:1:1:22:A33D:259A:21FE	4. <u>B</u>
FE80::3201:CC01:65B1	5. <u>C</u>
FF00::	6. <u>E</u>
FF00::DB7:4322:A231:67C	7. <u>E</u>
FF02::2	8. <u>E</u>

### Answer Choices

- a. Loopback address
- b. Global unicast address
- c. Link-local address
- d. Unique-local address
- e. Multicast address

## Part 3: Examine a Host IPv6 Network Interface and Address

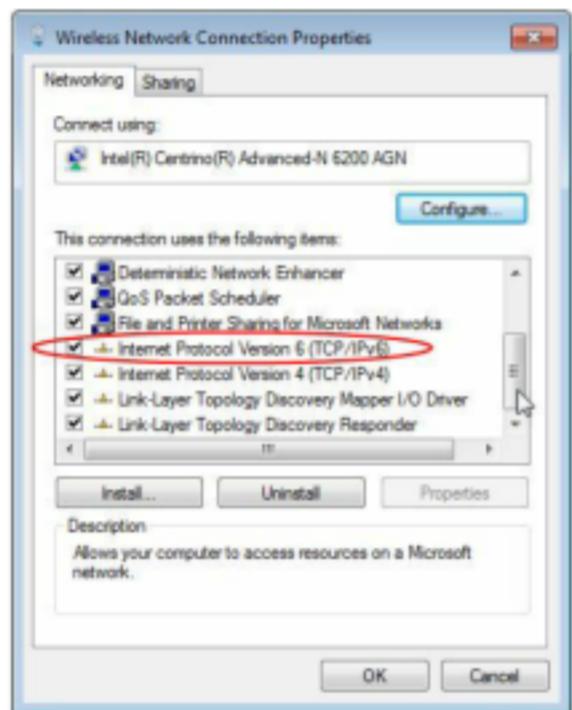
In Part 3, you will check the IPv6 network settings of your PC to identify your network interface IPv6 address.

### Step 1: Check your PC IPv6 network address settings.

- a. Verify that the IPv6 protocol is installed and active on your PC-A (check your Local Area Connection settings).
- b. Click the Windows **Start** button and then **Control Panel** and change **View by: Category** to **View by: Small icons**.
- c. Click the **Network and Sharing Center** icon.
- d. On the left side of the window, click **Change adapter settings**. You should now see icons representing your installed network adapters. Right-click your active network interface (it may be a **Local Area Connection** or a **Wireless Network Connection**), and then click **Properties**.

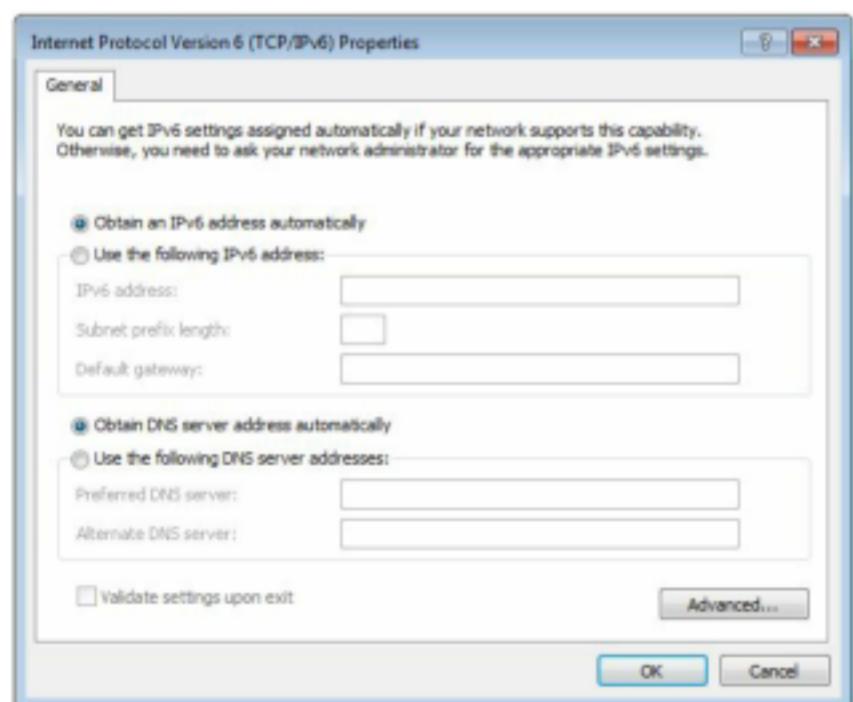
## Lab – Identifying IPv6 Addresses

- e. You should now see your Network Connection Properties window. Scroll through the list of items to determine whether IPv6 is present, which indicates that it is installed, and if it is also check marked, which indicates that it is active.



- f. Select the item **Internet Protocol Version 6 (TCP/IPv6)** and click **Properties**. You should see the IPv6 settings for your network interface. Your IPv6 properties window is likely set to **Obtain an IPv6 address automatically**. This does not mean that IPv6 relies on the Dynamic Host Configuration Protocol (DHCP). Instead of using DHCP, IPv6 looks to the local router for IPv6 network information and then auto-configures its own IPv6 addresses. To manually configure IPv6, you must provide the IPv6 address, the subnet prefix length, and the default gateway.

**Note:** The local router can refer host requests for IPv6 information, especially Domain Name System (DNS) information, to a DHCPv6 server on the network.



## Lab – Identifying IPv6 Addresses

---

- g. After you have verified that IPv6 is installed and active on your PC, you should check your IPv6 address information. To do this, click the **Start** button, type **cmd** in the *Search programs and files* form box, and press Enter. This opens a Windows command prompt window.

- h. Type **ipconfig /all** and press Enter. Your output should look similar to this:

```
C:\Users\user> ipconfig /all

Windows IP Configuration

<output omitted>

Wireless LAN adapter Wireless Network Connection:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) Centrino(R) Advanced-N 6200 AGN
Physical Address. . . . . : 02-37-10-41-FB-48
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . : fe80::8d4f:4f4d%3237:95e2%14 (Preferred)
IPv4 Address. . . . . : 192.168.2.106(PREFERRED)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Sunday, January 06, 2013 9:47:36 AM
Lease Expires . . . . . : Monday, January 07, 2013 9:47:38 AM
Default Gateway . . . . . : 192.168.2.1
DHCP Server . . . . . : 192.168.2.1
DHCPv6 IAID . . . . . : 335554320
DHCPv6 Client DUID. . . . . : 00-01-00-01-14-57-84-B1-C1-DE-91-C3-5D

DNS Servers . . . . . : 192.168.1.1
                           8.8.4.4
<output omitted>
```

- i. You can see from the output that the client PC has an IPv6 link-local address with a randomly generated interface ID. What does it indicate about the network regarding IPv6 global unicast address, IPv6 unique-local address, or IPv6 gateway address?
- 
- 

- j. What kind of IPv6 addresses did you find when using **ipconfig /all**?
- 
- 

## Reflection

1. How do you think you must support IPv6 in the future?

---

2. Do you think IPv4 networks continue on, or will everyone eventually switch over to IPv6? How long do you think it will take?

---

---



# Module 13: ICMP

Introduction of Networks v7.0  
(ITN)



# Module Objectives

**Module Title:** ICMP

**Module Objective:** Use various tools to test network connectivity.

Topic Title	Topic Objective
ICMP Messages	Explain how ICMP is used to test network connectivity.
Ping and Traceroute Testing	Use ping and traceroute utilities to test network connectivity.



# 13.1 ICMP Messages



## ICMP Messages

# ICMPv4 and ICMPv6 Messages

- Internet Control Message Protocol (ICMP) provides feedback about issues related to the processing of IP packets under certain conditions.
- ICMPv4 is the messaging protocol for IPv4. ICMPv6 is the messaging protocol for IPv6 and includes additional functionality.
- The ICMP messages common to both ICMPv4 and ICMPv6 include:
  - Host reachability
  - Destination or Service Unreachable
  - Time exceeded

Note: ICMPv4 messages are not required and are often not allowed within a network for security reasons.

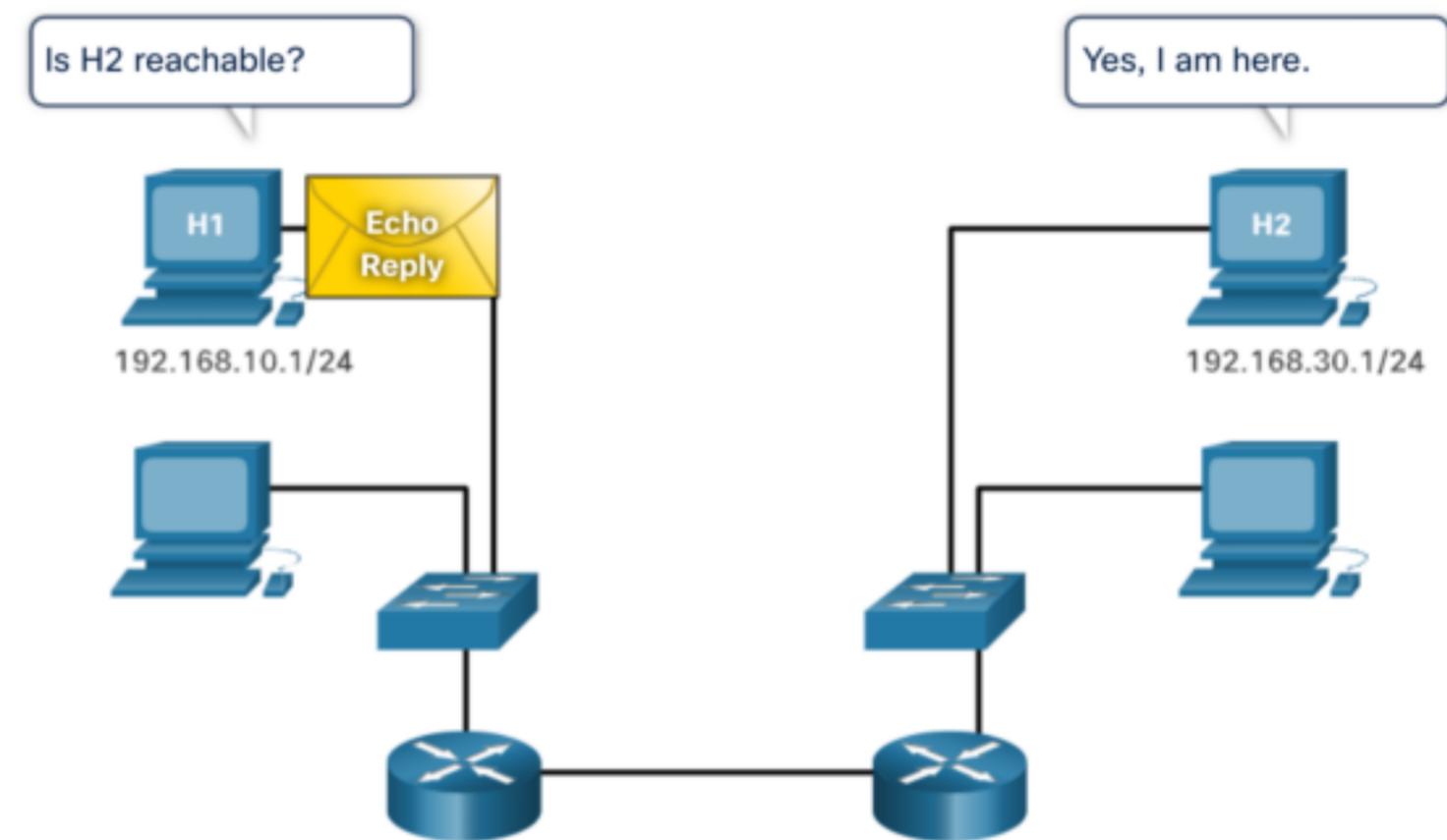
## ICMP Messages

# Host Reachability

ICMP Echo Message can be used to test the reachability of a host on an IP network.

In the example:

- The local host sends an ICMP Echo Request to a host.
- If the host is available, the destination host responds with an Echo Reply.



## ICMP Messages

### Destination or Service Unreachable

- An ICMP Destination Unreachable message can be used to notify the source that a destination or service is unreachable.
- The ICMP message will include a code indicating why the packet could not be delivered.

#### **A few Destination Unreachable codes for ICMPv4 are as follows:**

- 0 - Net unreachable
- 1 - Host unreachable
- 2 - Protocol unreachable
- 3 - Port unreachable

#### **A few Destination Unreachable codes for ICMPv6 are as follows:**

- 0 - No route to destination
- 1 - Communication with the destination is administratively prohibited (e.g., firewall)
- 2 – Beyond scope of the source address
- 3 - Address unreachable
- 4 - Port unreachable

**Note:** ICMPv6 has similar but slightly different codes for Destination Unreachable messages.



## ICMP Messages

### Time Exceeded

- When the Time to Live (TTL) field in a packet is decremented to 0, an ICMPv4 Time Exceeded message will be sent to the source host.
- ICMPv6 also sends a Time Exceeded message. Instead of the IPv4 TTL field, ICMPv6 uses the IPv6 Hop Limit field to determine if the packet has expired.

```
Pinging 8.8.8.8 with 32 bytes of data:  
Reply from 192.168.1.1: TTL expired in transit.  
  
Ping statistics for 8.8.8.8:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

**Note:** Time Exceeded messages are used by the **traceroute** tool.

## ICMP Messages

# ICMPv6 Messages

ICMPv6 has new features and improved functionality not found in ICMPv4, including four new protocols as part of the Neighbor Discovery Protocol (ND or NDP).

Messaging between an IPv6 router and an IPv6 device, including dynamic address allocation are as follows:

- Router Solicitation (RS) message
- Router Advertisement (RA) message

Messaging between IPv6 devices, including duplicate address detection and address resolution are as follows:

- Neighbor Solicitation (NS) message
- Neighbor Advertisement (NA) message

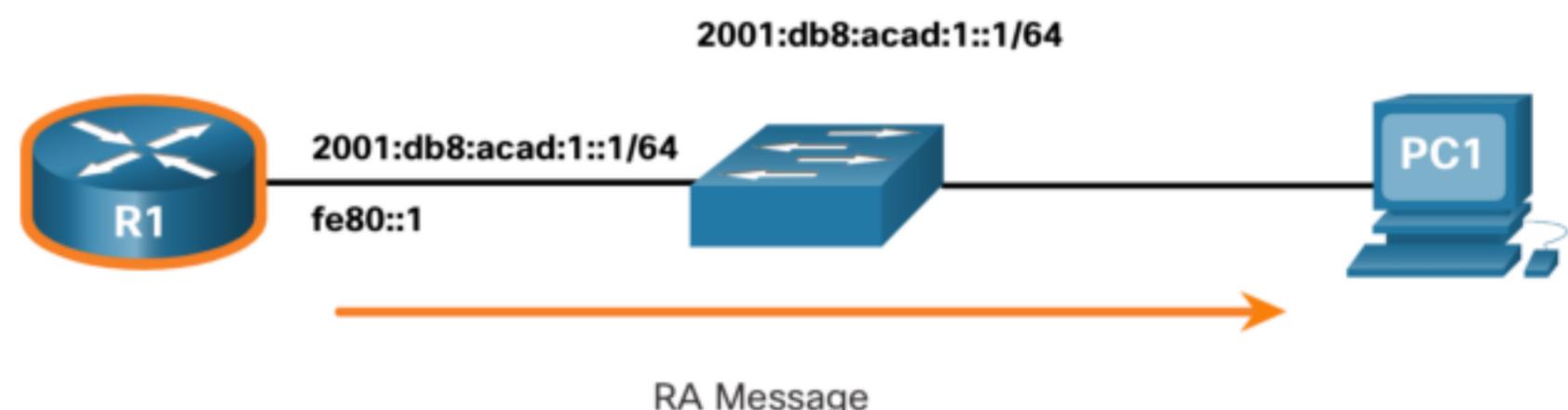
**Note:** ICMPv6 ND also includes the redirect message, which has a similar function to the redirect message used in ICMPv4.



## ICMP Messages

## ICMPv6 Messages (Cont.)

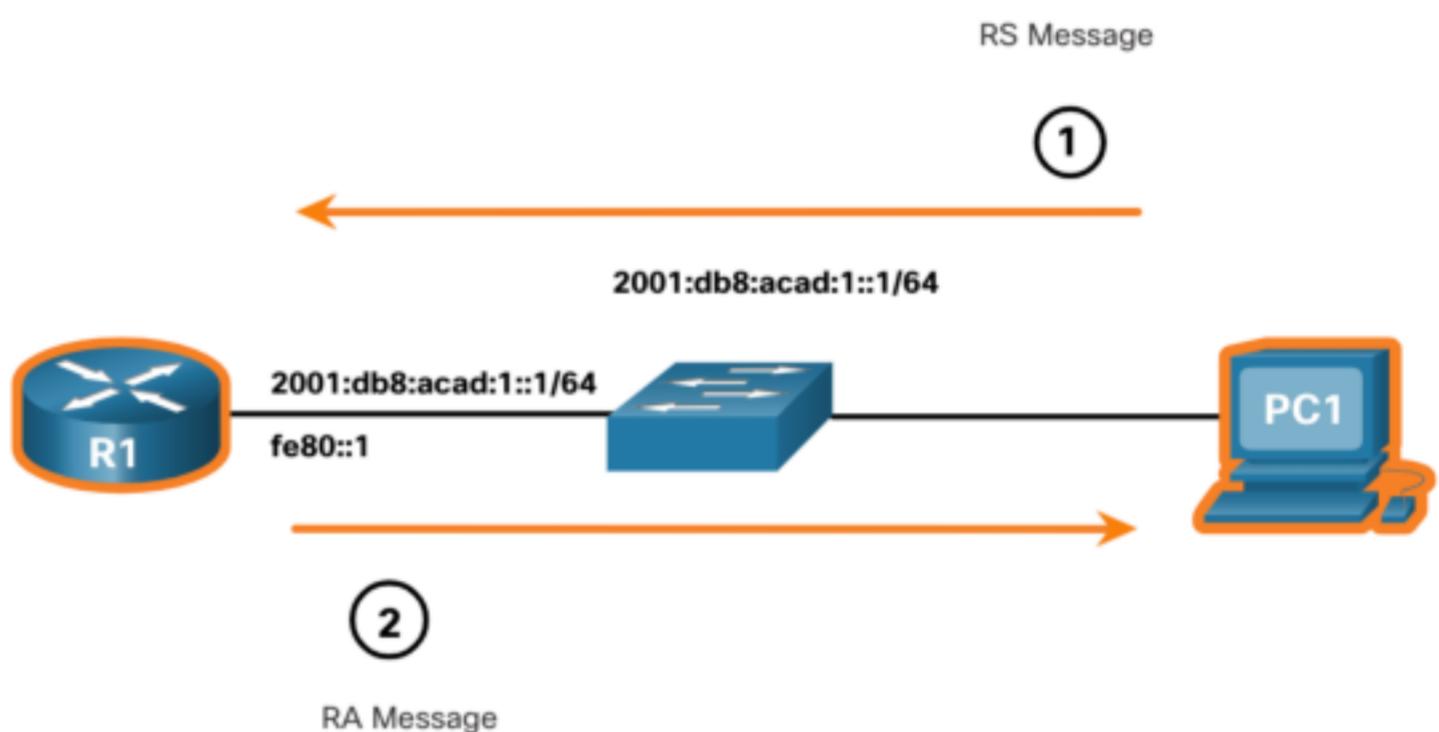
- RA messages are sent by IPv6-enabled routers every 200 seconds to provide addressing information to IPv6-enabled hosts.
- RA message can include addressing information for the host such as the prefix, prefix length, DNS address, and domain name.
- A host using Stateless Address Autoconfiguration (SLAAC) will set its default gateway to the link-local address of the router that sent the RA.



## ICMP Messages

## ICMPv6 Messages (Cont.)

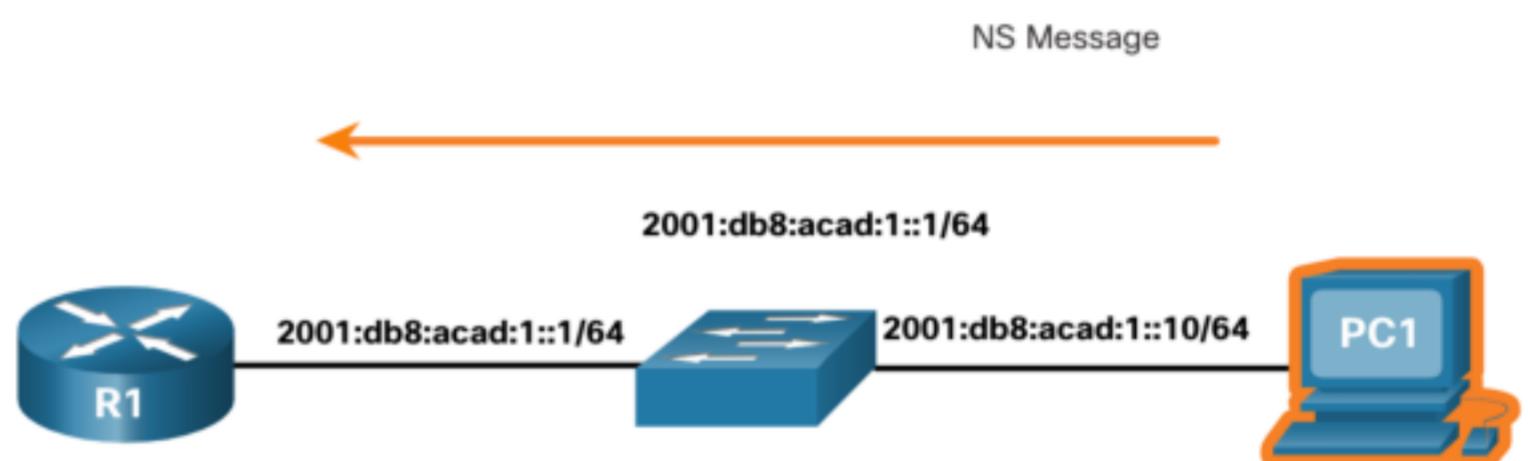
- An IPv6-enabled router will also send out an RA message in response to an RS message.
- In the figure, PC1 sends a RS message to determine how to receive its IPv6 address information dynamically.
  - R1 replies to the RS with an RA message.
  - PC1 sends an RS message, “Hi, I just booted up. Is there an IPv6 router on the network? I need to know how to get my IPv6 address information dynamically.”
  - R1 replies with an RA message. “Hi all IPv6-enabled devices. I’m R1 and you can use SLAAC to create an IPv6 global unicast address. The prefix is 2001:db8:acad:1::/64. By the way, use my link-local address fe80::1 as your default gateway.”



## ICMP Messages

### ICMPv6 Messages (Cont.)

- A device assigned a global IPv6 unicast or link-local unicast address, may perform duplicate address detection (DAD) to ensure that the IPv6 address is unique.
- To check the uniqueness of an address, the device will send an NS message with its own IPv6 address as the targeted IPv6 address.
- If another device on the network has this address, it will respond with an NA message notifying to the sending device that the address is in use.

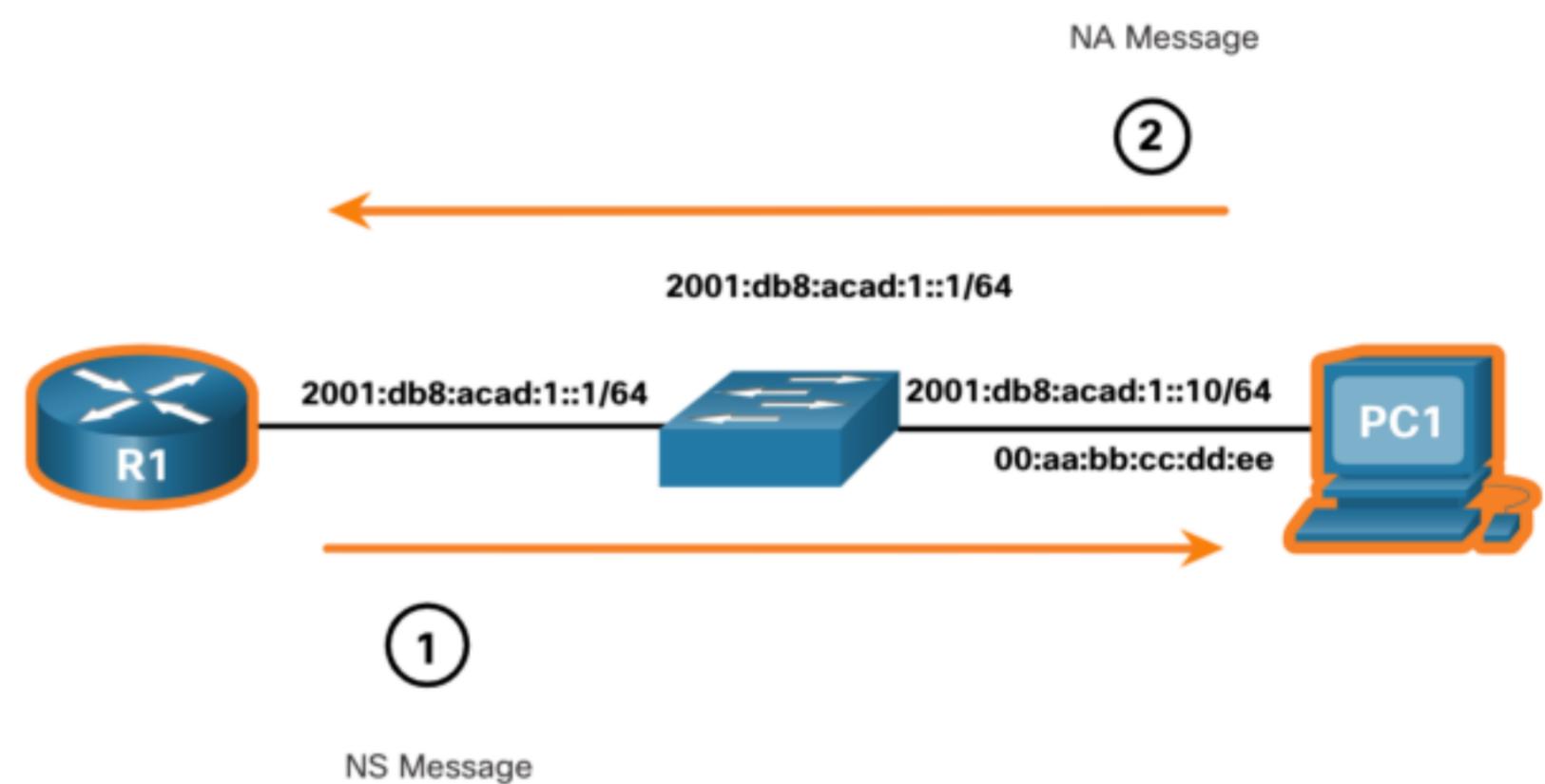


**Note:** DAD is not required, but RFC 4861 recommends that DAD is performed on unicast addresses.

## ICMP Messages

### ICMPv6 Messages (Cont.)

- To determine the MAC address for the destination, the device will send an NS message to the solicited node address.
- The message will include the known (targeted) IPv6 address. The device that has the targeted IPv6 address will respond with an NA message containing its Ethernet MAC address.
- In the figure, R1 sends a NS message to 2001:db8:acad:1::10 asking for its MAC address.



# 13.2 Ping and Traceroute Tests



## Ping and Traceroute Tests

# Ping – Test Connectivity

- The **ping** command is an IPv4 and IPv6 testing utility that uses ICMP echo request and echo reply messages to test connectivity between hosts and provides a summary that includes the success rate and average round-trip time to the destination.
- If a reply is not received within the timeout, ping provides a message indicating that a response was not received.
- It is common for the first ping to timeout if address resolution (ARP or ND) needs to be performed before sending the ICMP Echo Request.

```
S1#ping 192.168.20.2  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.168.20.2, timeout is 2 seconds:  
.!!!!  
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms
```

```
R1#ping 2001:db8:acad:1::2  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 2001:db8:acad:1::2, timeout is 2 seconds:  
.!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

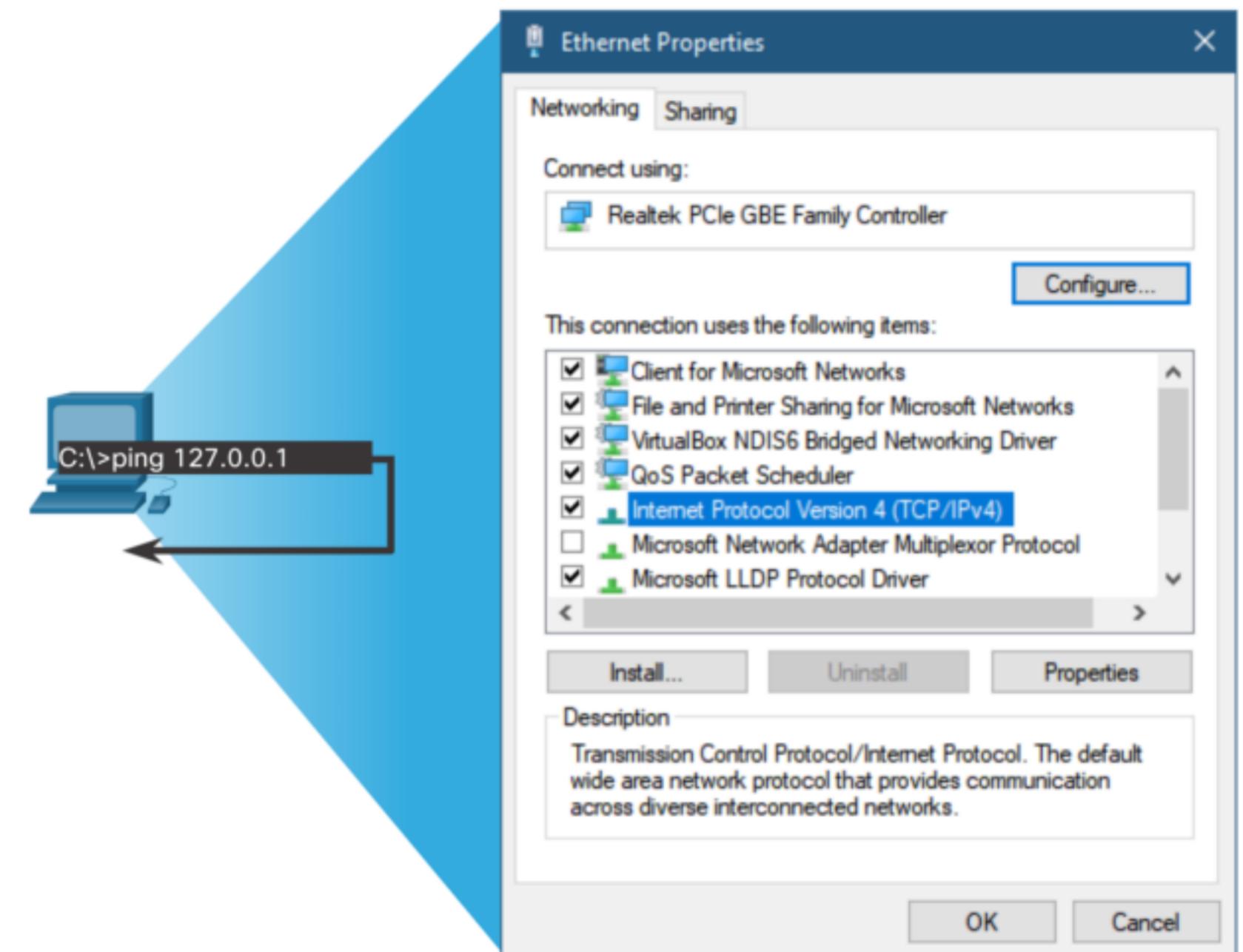


## Ping and Traceroute Tests

### Ping the Loopback

Ping can be used to test the internal configuration of IPv4 or IPv6 on the local host. To do this, **ping** the local loopback address of 127.0.0.1 for IPv4 (::1 for IPv6).

- A response from 127.0.0.1 for IPv4, or ::1 for IPv6, indicates that IP is properly installed on the host.
- An error message indicates that TCP/IP is not operational on the host.



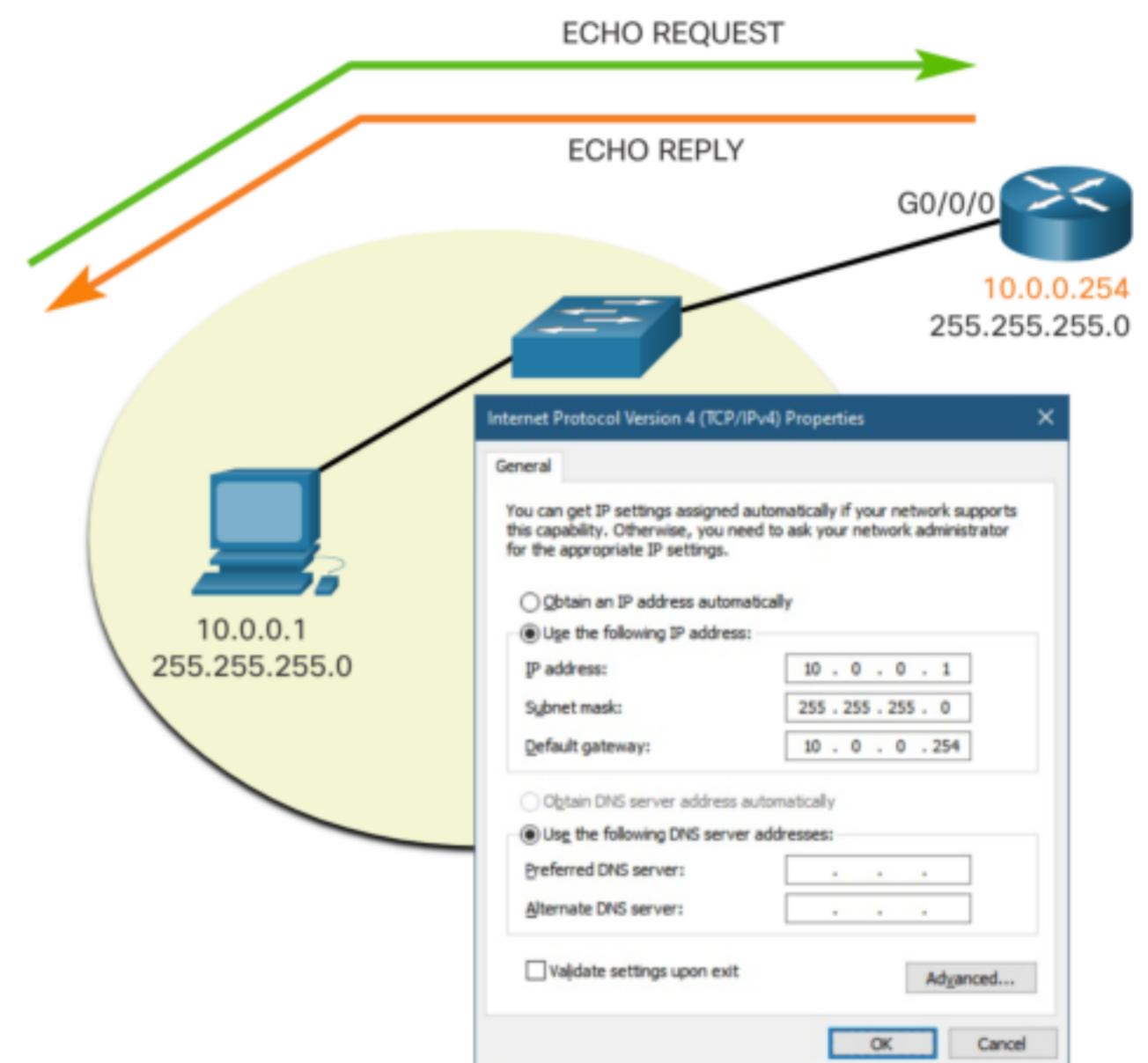
## Ping and Traceroute Tests

### Ping the Default Gateway

The **ping** command can be used to test the ability of a host to communicate on the local network.

The default gateway address is most often used because the router is normally always operational.

- A successful **ping** to the default gateway indicates that the host and the router interface serving as the default gateway are both operational on the local network.
- If the default gateway address does not respond, a **ping** can be sent to the IP address of another host on the local network that is known to be operational.



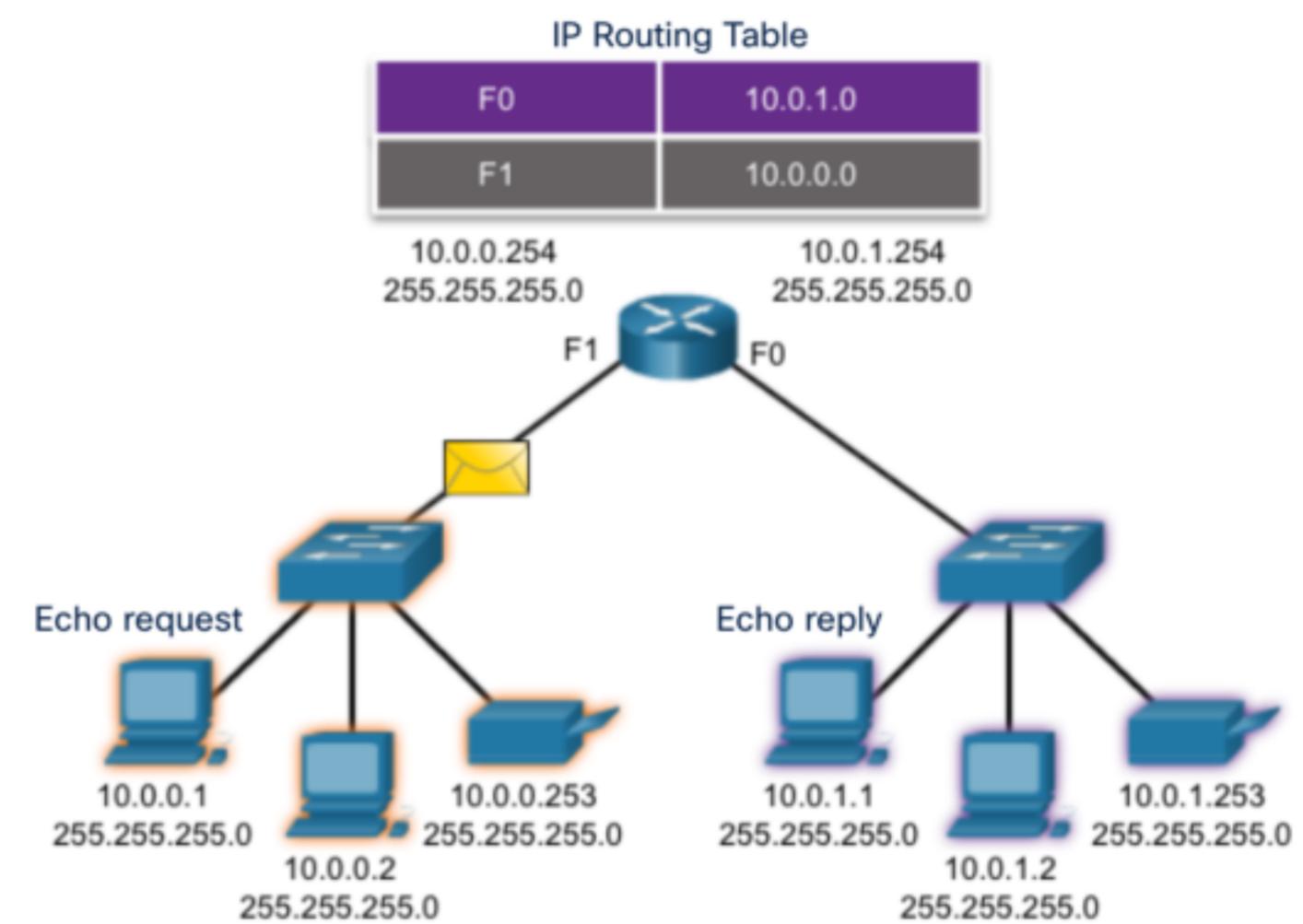
## Ping and Traceroute Tests

### Ping a Remote Host

Ping can also be used to test the ability of a local host to communicate across an internetwork.

A local host can ping a host on a remote network. A successful **ping** across the internetwork confirms communication on the local network.

**Note:** Many network administrators limit or prohibit the entry of ICMP messages therefore, the lack of a **ping** response could be due to security restrictions.



## Ping and Traceroute Tests

### Traceroute – Test the Path

- Traceroute (**tracert**) is a utility that is used to test the path between two hosts and provide a list of hops that were successfully reached along that path.
- Traceroute provides round-trip time for each hop along the path and indicates if a hop fails to respond. An asterisk (\*) is used to indicate a lost or unrepplied packet.
- This information can be used to locate a problematic router in the path or may indicate that the router is configured not to reply.

```
R1#traceroute 192.168.40.2
Type escape sequence to abort.
Tracing the route to 192.168.40.2
```

1	192.168.10.2	1 msec	0 msec	0 msec
2	192.168.20.2	2 msec	1 msec	0 msec
3	192.168.30.2	1 msec	0 msec	0 msec
4	192.168.40.2	0 msec	0 msec	0 msec

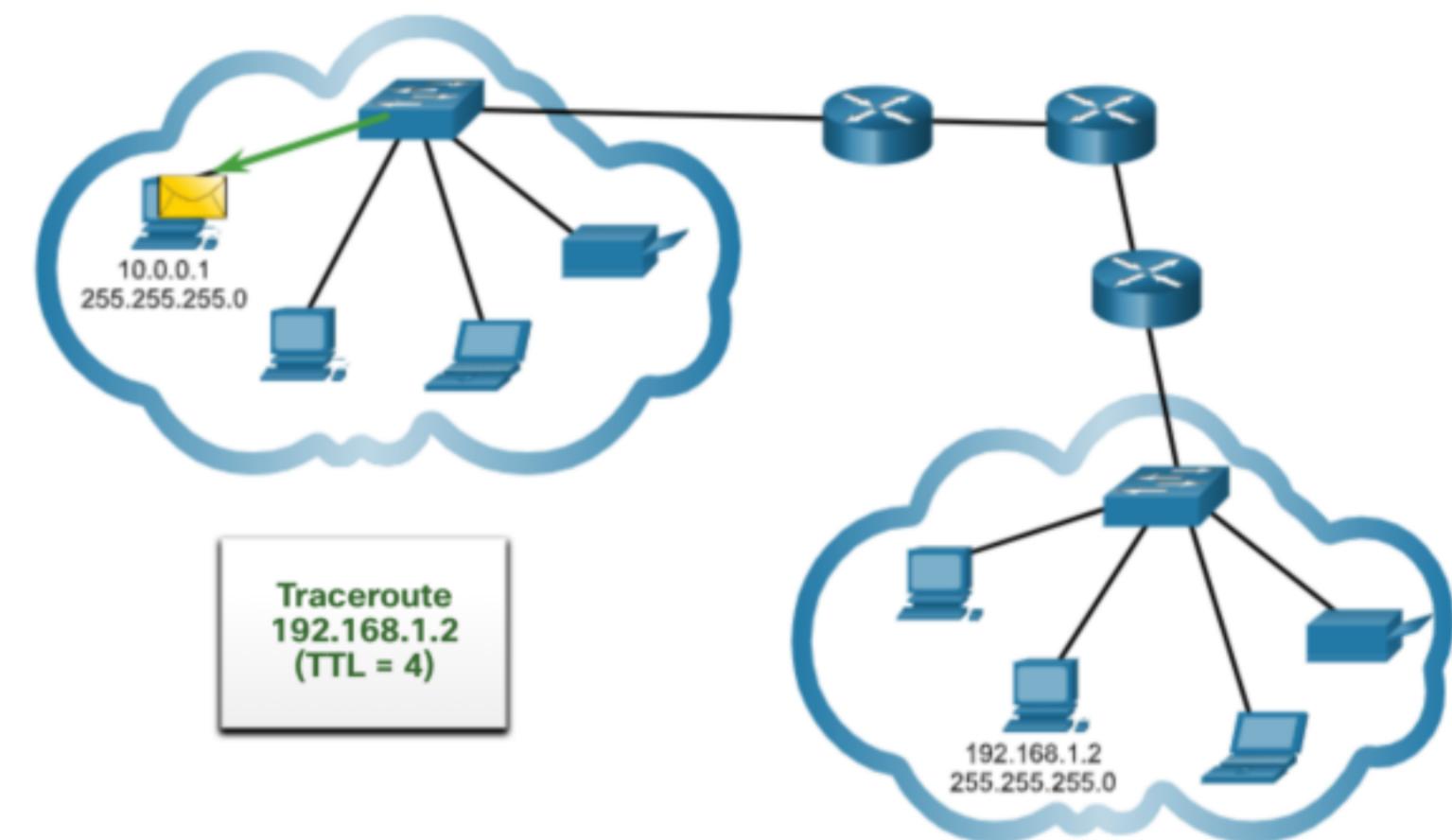
**Note:** Traceroute makes use of a function of the TTL field in IPv4 and the Hop Limit field in IPv6 in the Layer 3 headers, along with the ICMP Time Exceeded message.



## Ping and Traceroute Tests

### Traceroute – Test the Path (Cont.)

- The first message sent from traceroute will have a TTL field value of 1. This causes the TTL to time out at the first router. This router then responds with a ICMPv4 Time Exceeded message.
- Traceroute then progressively increments the TTL field (2, 3, 4...) for each sequence of messages. This provides the trace with the address of each hop as the packets time out further down the path.
- The TTL field continues to be increased until the destination is reached, or it is incremented to a predefined maximum.



## Ping and Traceroute Tests

# Packet Tracer – Verify IPv4 and IPv6 Addressing

In this Packet Tracer, you will do the following:

- Complete the Addressing Table Documentation
- Test Connectivity Using Ping
- Discover the Path by Tracing the Route



## Ping and Traceroute Tests

# Packet Tracer – Use Ping and Traceroute to Test Network Connectivity

In this Packet Tracer, you will do the following:

- Test and Restore IPv4 Connectivity
- Test and Restore IPv6 Connectivity



# 13.3 Module Practice and Quiz



## Module Practice and Quiz

# Packet Tracer – Use ICMP to Test and Correct Network Connectivity

In this Packet Tracer, you will do the following:

- Use ICMP to locate connectivity issues.
- Configure network devices to correct connectivity issues.



## Module Practice and Quiz

# Lab – Use Ping and Traceroute to Test Network Connectivity

In this lab, you complete the following objectives:

- Build and Configure the Network
- Use Ping Command for Basic Network Testing
- Use Tracert and Traceroute Commands for Basic Network Testing
- Troubleshoot the Topology



## Module Practice and Quiz

# What did I learn in this module?

- The purpose of ICMP messages is to provide feedback about issues related to the processing of IP packets under certain conditions.
- The ICMP messages common to both ICMPv4 and ICMPv6 are: Host reachability, Destination or Service Unreachable, and Time exceeded.
- The messages between an IPv6 router and an IPv6 device including dynamic address allocation include RS and RA. The messages between IPv6 devices include the redirect (similar to IPv4), NS and NA.
- Ping (used by IPv4 and IPv6) uses ICMP echo request and echo reply messages to test connectivity between hosts
- Ping can be used to test the internal configuration of IPv4 or IPv6 on the local host.
- Traceroute (tracert) generates a list of hops that were successfully reached along the path.



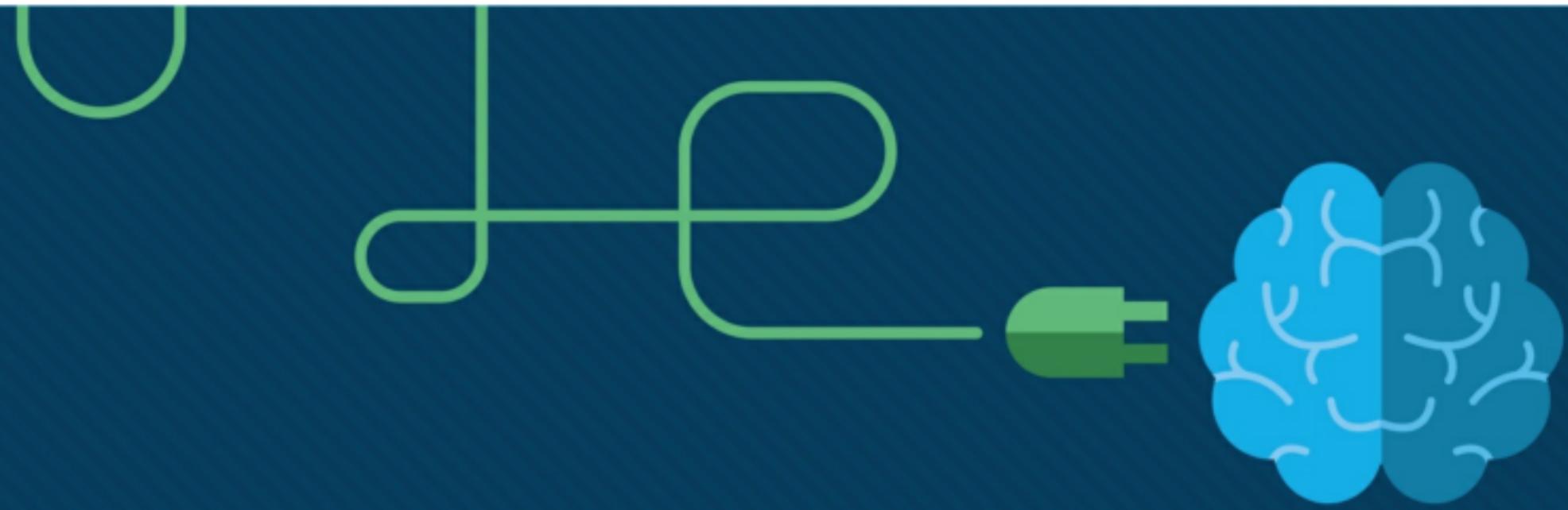
## Module 13 : ICMP

# New Terms and Commands

- ICMP
- ICMPv4
- ICMPv6
- ping
- traceroute
- tracert
- Network Discovery Protocol
- Router Solicitation (RS)
- Router Advertisement (RA)
- Neighbor Solicitation (NS)
- Neighbor Advertisement (NA)
- TTL







# Module 4: Physical Layer

Introduction to Networks v7.0  
(ITN)



# Module Objectives

## Module Title: Physical Layer

**Module Objective:** Explain how physical layer protocols, services, and network media support communications across data networks.

Topic Title	Topic Objective
Purpose of the Physical Layer	Describe the purpose and functions of the physical layer in the network.
Physical Layer Characteristics	Describe characteristics of the physical layer.
Copper Cabling	Identify the basic characteristics of copper cabling.
UTP Cabling	Explain how UTP cable is used in Ethernet networks.
Fiber-Optic Cabling	Describe fiber optic cabling and its main advantages over other media.
Wireless Media	Connect devices using wired and wireless media.

# 4.1 Purpose of the Physical Layer

## Purpose of the Physical Layer

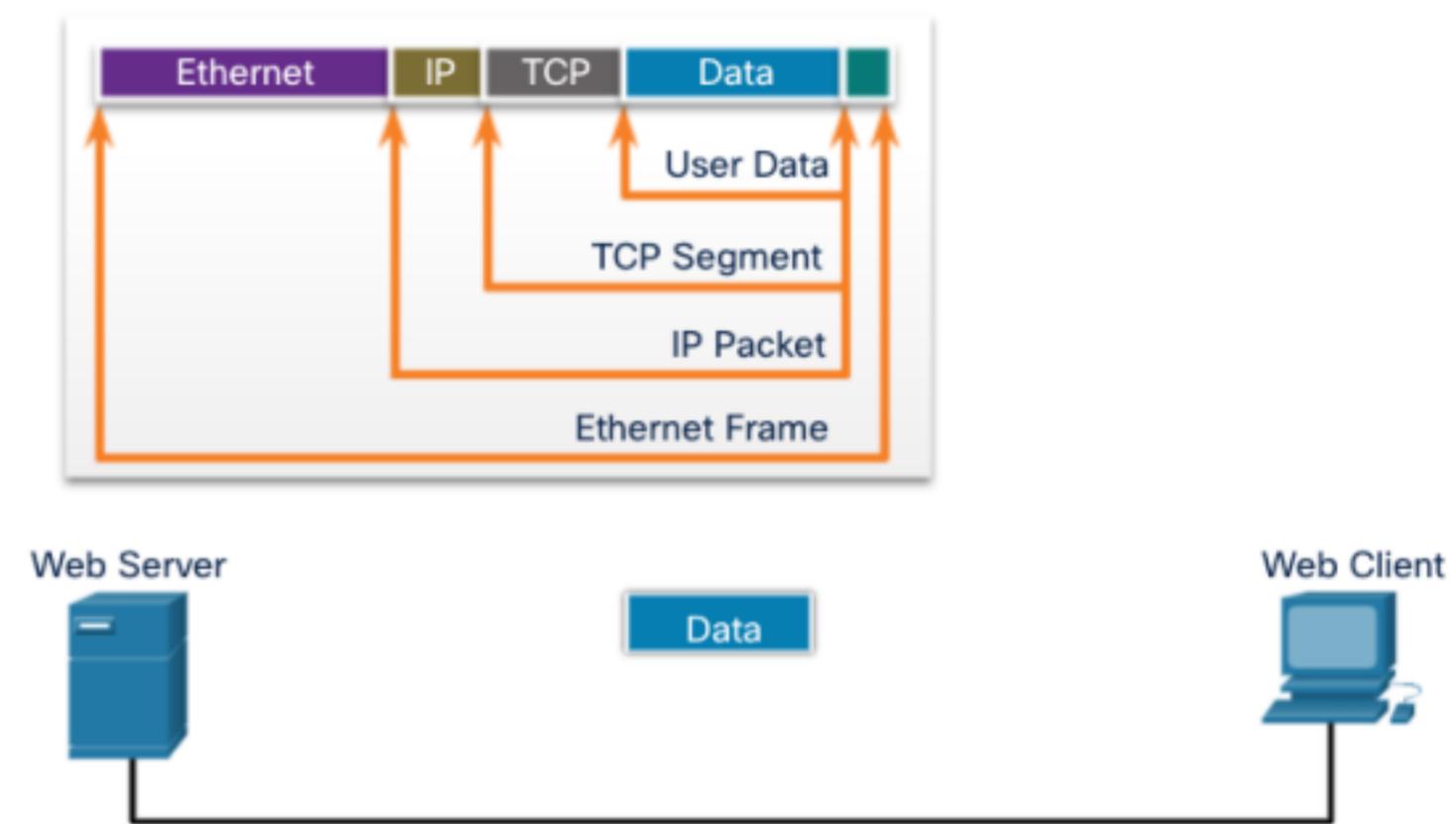
# The Physical Connection

- Before any network communications can occur, a physical connection to a local network must be established.
- This connection could be wired or wireless, depending on the setup of the network.
- This generally applies whether you are considering a corporate office or a home.
- A Network Interface Card (NIC) connects a device to the network.
- Some devices may have just one NIC, while others may have multiple NICs (Wired and/or Wireless, for example).
- Not all physical connections offer the same level of performance.

## Purpose of the Physical Layer

# The Physical Layer

- Transports bits across the network media
- Accepts a complete frame from the Data Link Layer and encodes it as a series of signals that are transmitted to the local media
- This is the last step in the encapsulation process.
- The next device in the path to the destination receives the bits and re-encapsulates the frame, then decides what to do with it.



# 4.2 Physical Layer Characteristics

## Physical Layer Characteristics

# Physical Layer Standards



The TCP/IP standards are implemented in software and governed by the IETF.

The physical layer standards are implemented in hardware and are governed by many organizations including:

- ISO
- EIA/TIA
- ITU-T
- ANSI
- IEEE

## Physical Layer Characteristics

# Physical Components

Physical Layer Standards address three functional areas:

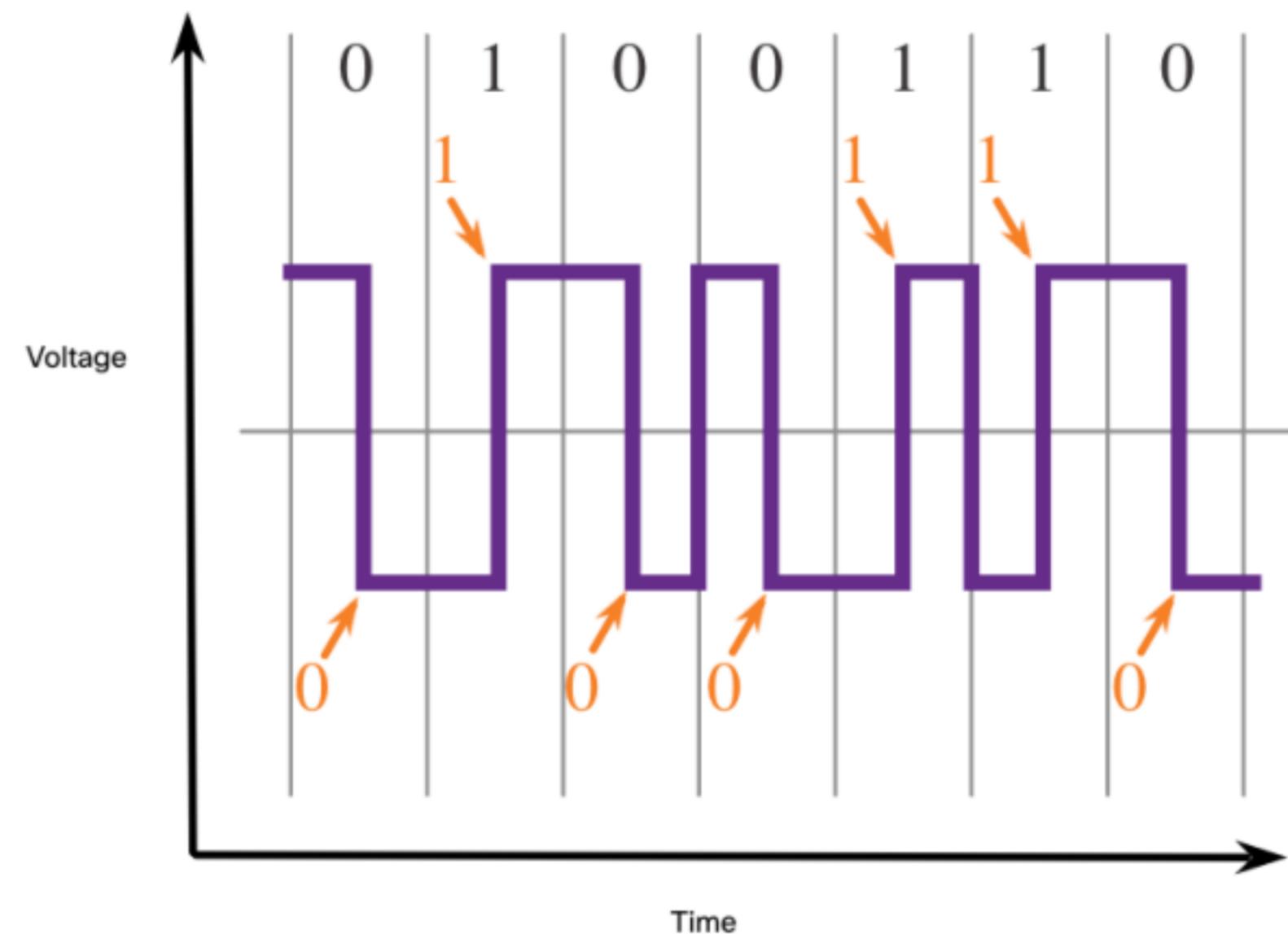
- Physical Components
- Encoding
- Signaling

The Physical Components are the hardware devices, media, and other connectors that transmit the signals that represent the bits.

- Hardware components like NICs, interfaces and connectors, cable materials, and cable designs are all specified in standards associated with the physical layer.

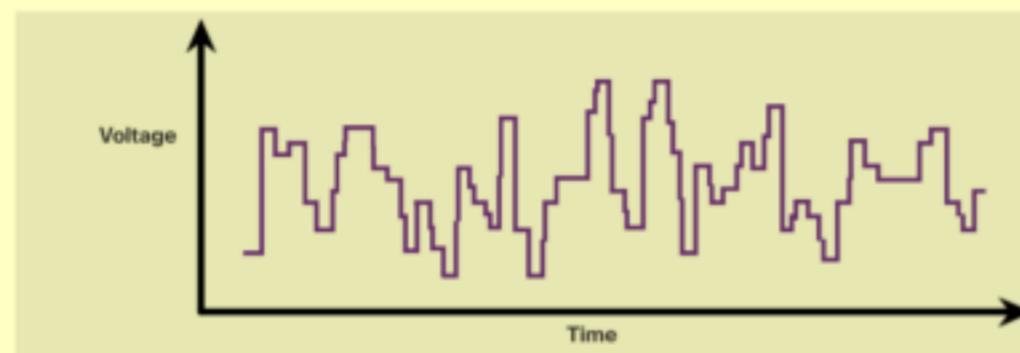
## Physical Layer Characteristics Encoding

- Encoding converts the stream of bits into a format recognizable by the next device in the network path.
- This ‘coding’ provides predictable patterns that can be recognized by the next device.
- Examples of encoding methods include Manchester (shown in the figure), 4B/5B, and 8B/10B.

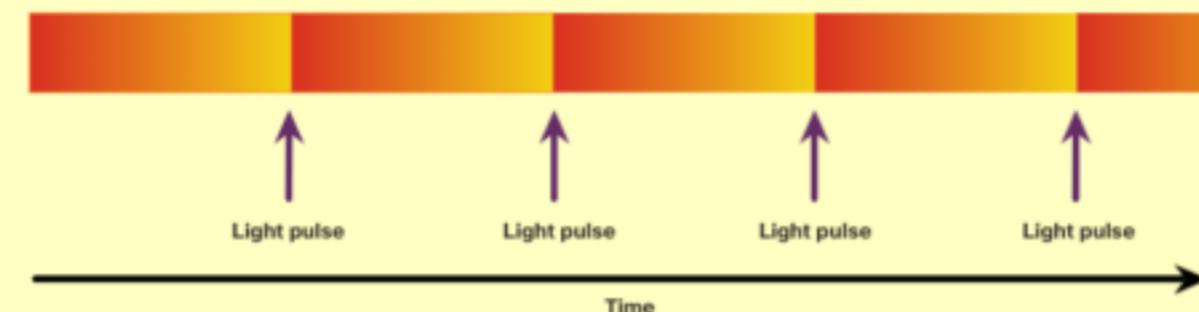


## Physical Layer Characteristics Signaling

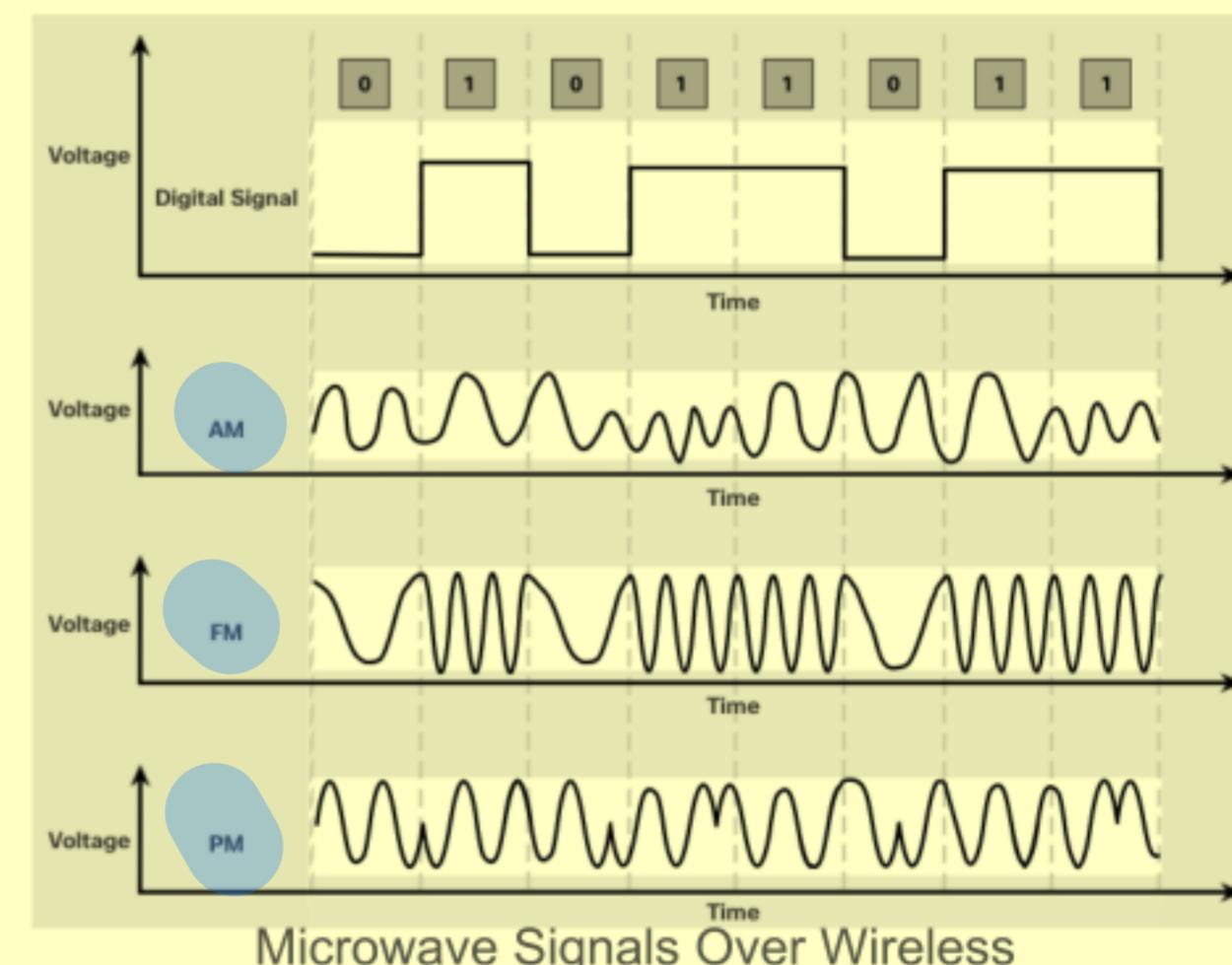
- The signaling method is how the bit values, “1” and “0” are represented on the physical medium.
- The method of signaling will vary based on the type of medium being used.



Electrical Signals Over Copper Cable



Light Pulses Over Fiber-Optic Cable



Microwave Signals Over Wireless

## Physical Layer Characteristics

### Bandwidth

- Bandwidth is the capacity at which a medium can carry data.
- Digital bandwidth measures the amount of data that can flow from one place to another in a given amount of time; how many bits can be transmitted in a second.
- Physical media properties, current technologies, and the laws of physics play a role in determining available bandwidth.

Unit of Bandwidth	Abbreviation	Equivalence
Bits per second	bps	1 bps = fundamental unit of bandwidth
Kilobits per second	Kbps	1 Kbps = 1,000 bps = $10^3$ bps
Megabits per second	Mbps	1 Mbps = 1,000,000 bps = $10^6$ bps
Gigabits per second	Gbps	1 Gbps – 1,000,000,000 bps = $10^9$ bps
Terabits per second	Tbps	1 Tbps = 1,000,000,000,000 bps = $10^{12}$ bps

## Physical Layer Characteristics

# Bandwidth Terminology

### Latency

- Amount of time, including delays, for data to travel from one given point to another

### Throughput

- The measure of the transfer of bits across the media over a given period of time

### Goodput

- The measure of usable data transferred over a given period of time
- $\text{Goodput} = \text{Throughput} - \text{traffic overhead}$



# 4.3 Copper Cabling

## Copper Cabling

# Characteristics of Copper Cabling

Copper cabling is the most common type of cabling used in networks today. It is inexpensive, easy to install, and has low resistance to electrical current flow.

### Limitations:

- Attenuation – the longer the electrical signals have to travel, the weaker they get.
- The electrical signal is susceptible to interference from two sources, which can distort and corrupt the data signals (Electromagnetic Interference (EMI) and Radio Frequency Interference (RFI) and Crosstalk).

### Mitigation:

- Strict adherence to cable length limits will mitigate attenuation.
- Some kinds of copper cable mitigate EMI and RFI by using metallic shielding and grounding.
- Some kinds of copper cable mitigate crosstalk by twisting opposing circuit pair wires together.

## Copper Cabling

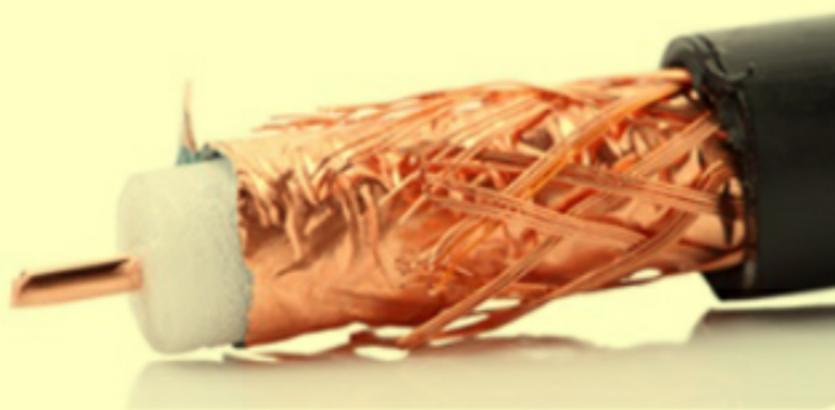
# Types of Copper Cabling



Unshielded Twisted-Pair (UTP) Cable

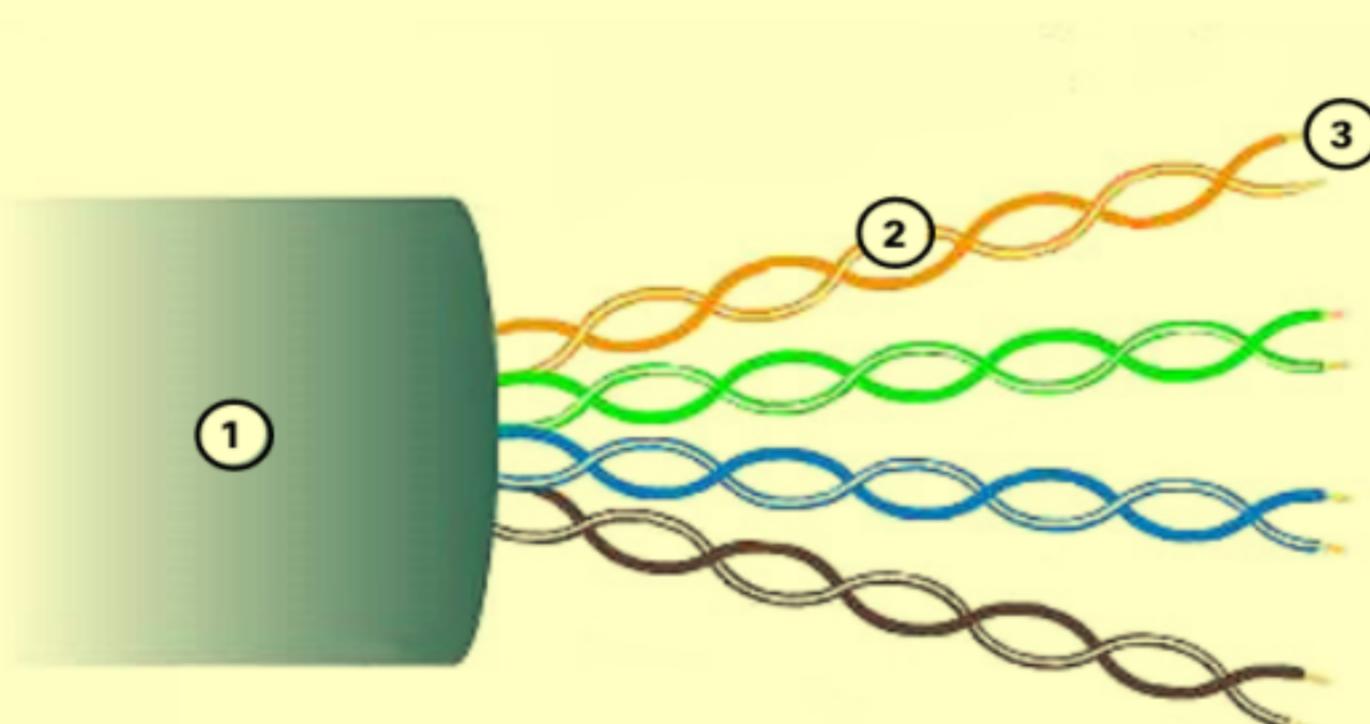


Shielded Twisted-Pair (STP) Cable



Coaxial Cable

## Copper Cabling Unshielded Twisted Pair (UTP)

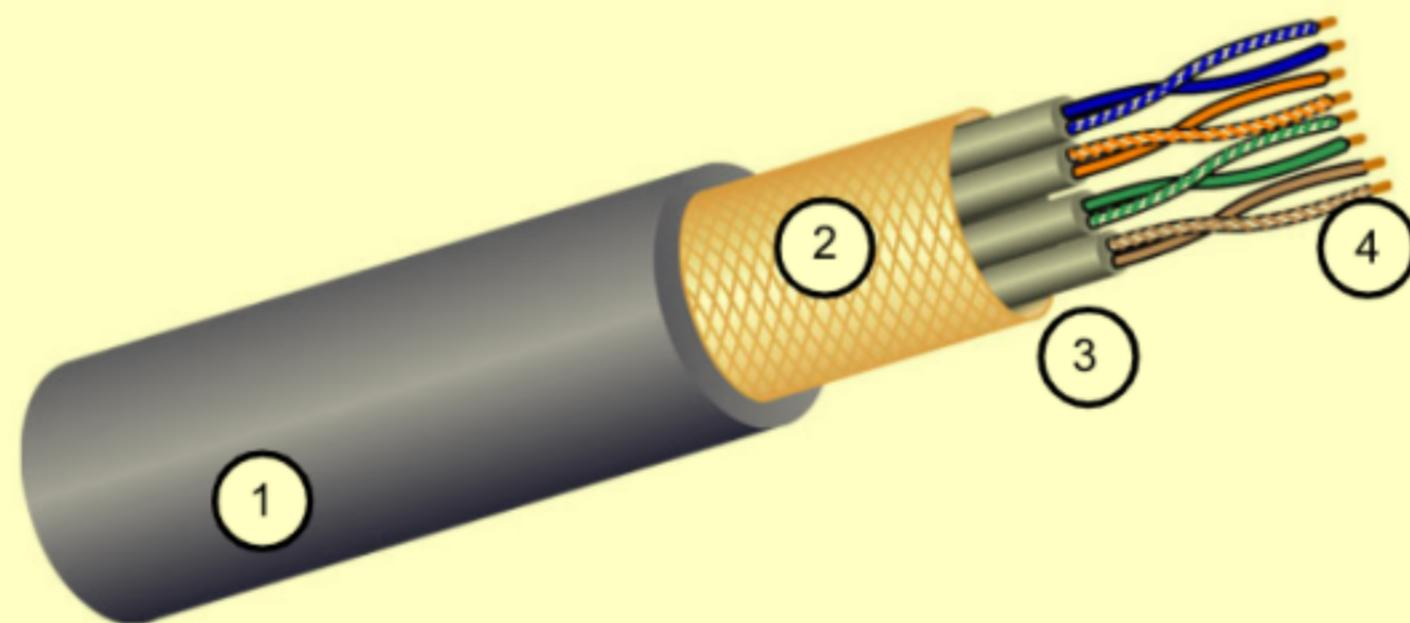


- UTP is the most common networking media.
- Terminated with RJ-45 connectors
- Interconnects hosts with intermediary network devices.

### Key Characteristics of UTP

1. The outer jacket protects the copper wires from physical damage.
2. Twisted pairs protect the signal from interference.
3. Color-coded plastic insulation electrically isolates the wires from each other and identifies each pair.

## Copper Cabling Shielded Twisted Pair (STP)



- Better noise protection than UTP
- More expensive than UTP
- Harder to install than UTP
- Terminated with RJ-45 connectors
- Interconnects hosts with intermediary network devices

### Key Characteristics of STP

1. The outer jacket protects the copper wires from physical damage
2. Braided or foil shield provides EMI/RFI protection
3. Foil shield for each pair of wires provides EMI/RFI protection
4. Color-coded plastic insulation electrically isolates the wires from each other and identifies each pair

## Copper Cabling Coaxial Cable

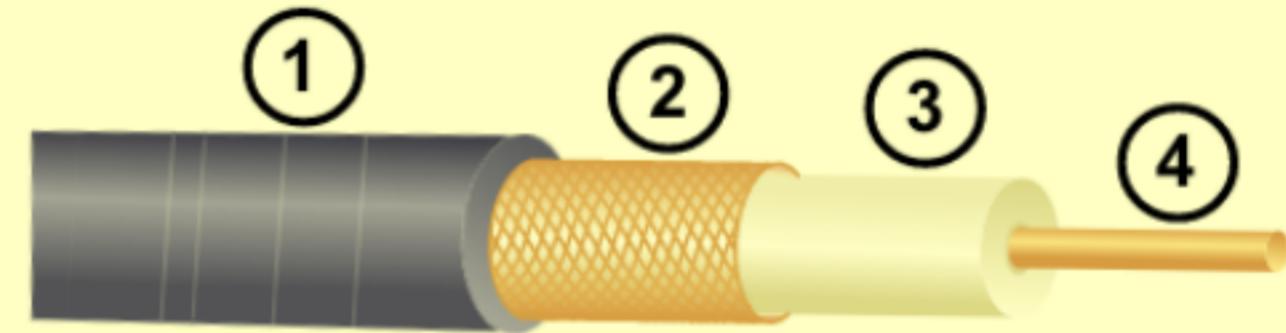
Consists of the following:

1. Outer cable jacket to prevent minor physical damage
2. A woven copper braid, or metallic foil, acts as the second wire in the circuit and as a shield for the inner conductor.
3. A layer of flexible plastic insulation
4. A copper conductor is used to transmit the electronic signals.

There are different types of connectors used with coax cable.

Commonly used in the following situations:

- Wireless installations - attach antennas to wireless devices
- Cable internet installations - customer premises wiring

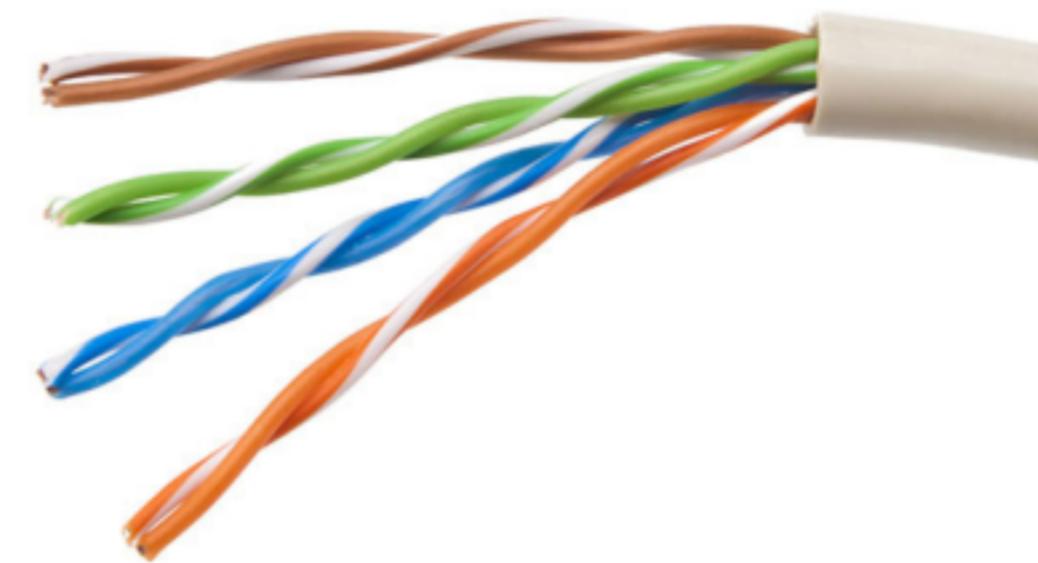


# 4.4 UTP Cabling

## UTP Cabling Properties of UTP Cabling

UTP has four pairs of color-coded copper wires twisted together and encased in a flexible plastic sheath. No shielding is used. UTP relies on the following properties to limit crosstalk:

- Cancellation - Each wire in a pair of wires uses opposite polarity. One wire is negative, the other wire is positive. They are twisted together and the magnetic fields effectively cancel each other and outside EMI/RFI.
- Variation in twists per foot in each wire - Each wire is twisted a different amount, which helps prevent crosstalk amongst the wires in the cable.



## UTP Cabling

# UTP Cabling Standards and Connectors

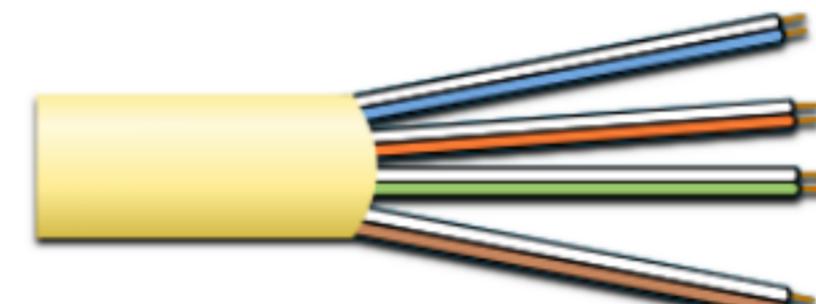
Standards for UTP are established by the TIA/EIA. TIA/EIA-568 standardizes elements like:

- Cable Types
- Cable Lengths
- Connectors
- Cable Termination
- Testing Methods

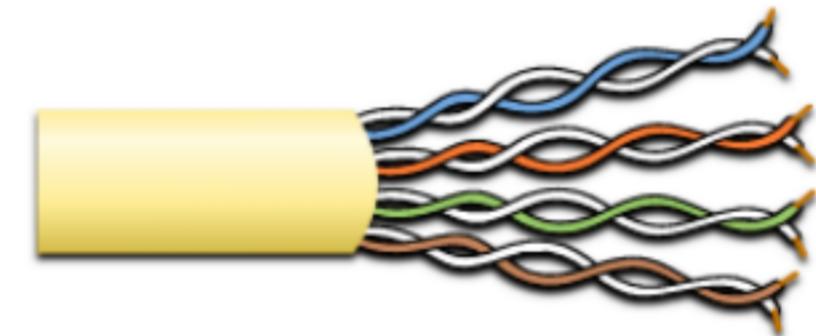
Electrical standards for copper cabling are established by the IEEE, which rates cable according to its performance.

Examples include:

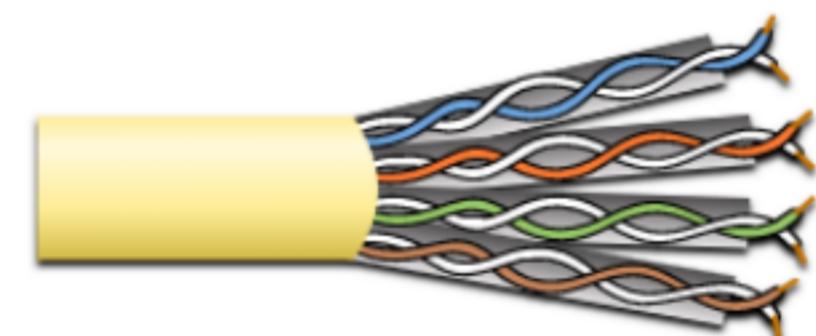
- Category 3
- Category 5 and 5e
- Category 6



Category 3 Cable (UTP)



Category 5 and 5e Cable (UTP)



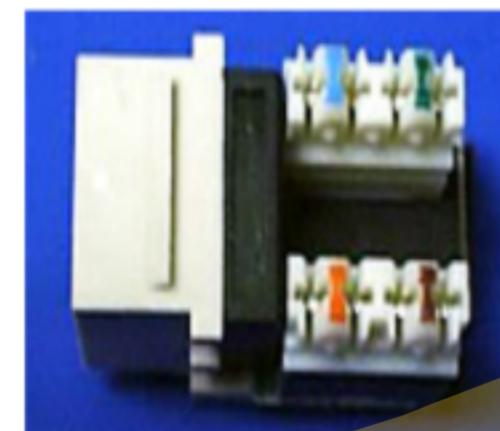
Category 6 Cable (UTP)

## UTP Cabling

# UTP Cabling Standards and Connectors (Cont.)



RJ-45 Connector



RJ-45 Socket

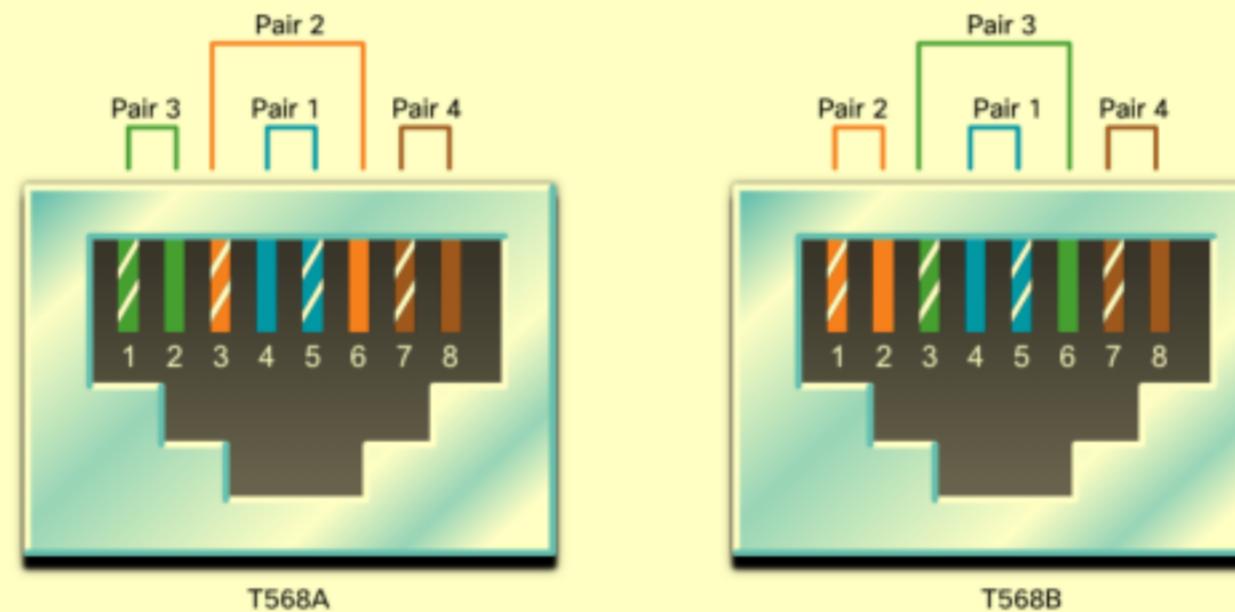


Poorly terminated UTP cable



Properly terminated UTP cable

## UTP Cabling Straight-through and Crossover UTP Cables



Cable Type	Standard	Application	
Ethernet Straight-through	Both ends T568A or T568B	Host to Network Device	Different devices
Ethernet Crossover *	One end T568A, other end T568B	Host-to-Host, Switch-to-Switch, Router-to-Router	
* Considered Legacy due to most NICs using Auto-MDIX to sense cable type and complete connection			
Rollover	Cisco Proprietary	Host serial port to Router or Switch Console Port, using an adapter	

# 4.5 Fiber-Optic Cabling

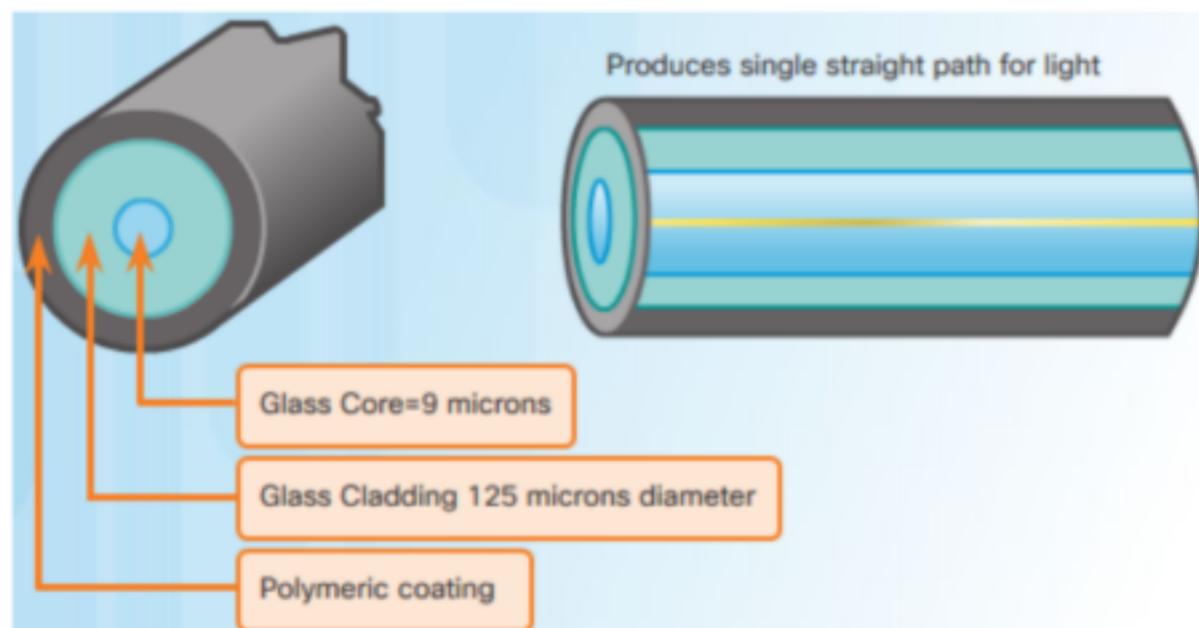
## Properties of Fiber-Optic Cabling

- Not as common as UTP because of the expense involved
- Ideal for some networking scenarios
- Transmits data over longer distances at higher bandwidth than any other networking media
- Less susceptible to attenuation, and completely immune to EMI/RFI
- Made of flexible, extremely thin strands of very pure glass
- Uses a laser or LED to encode bits as pulses of light
- The fiber-optic cable acts as a wave guide to transmit light between the two ends with minimal signal loss

# Fiber-Optic Cabling

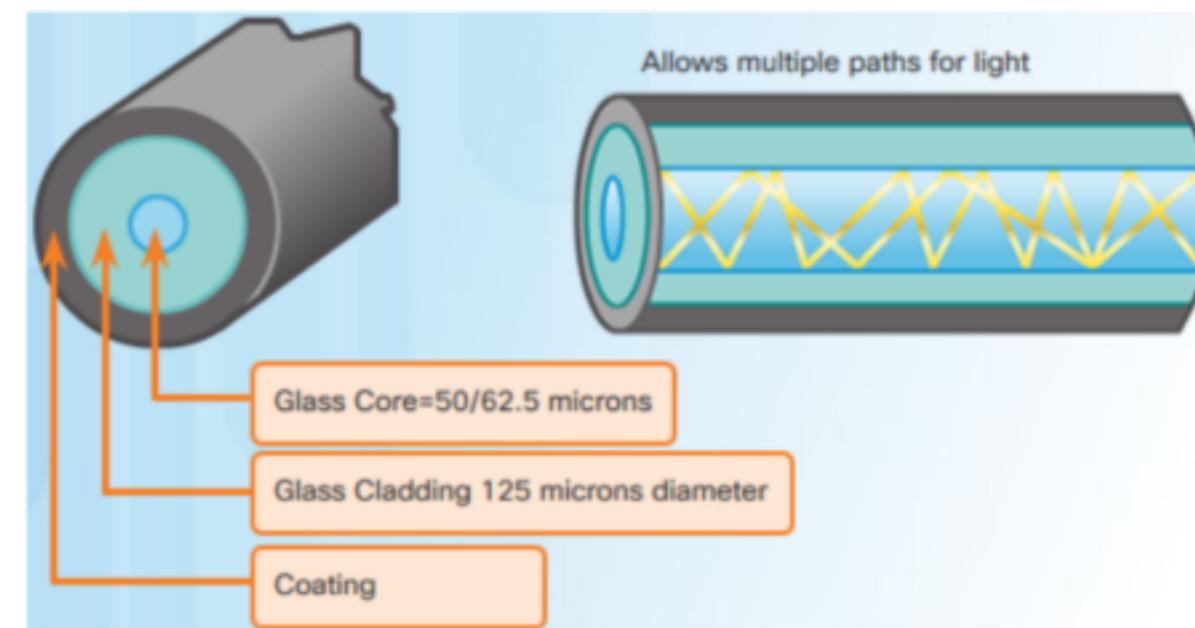
## Types of Fiber Media

Single-Mode Fiber



- Very small core
- Uses expensive lasers
- Long-distance applications

Multimode Fiber



- Larger core
- Uses less expensive LEDs
- LEDs transmit at different angles
- Up to 10 Gbps over 550 meters

Dispersion refers to the spreading out of a light pulse over time. Increased dispersion means increased loss of signal strength. MMF has greater dispersion than SMF, with a maximum cable distance for MMF is 550 meters.

## Fiber-Optic Cabling Usage

Fiber-optic cabling is now being used in four types of industry:

1. **Enterprise Networks** - Used for backbone cabling applications and interconnecting infrastructure devices
2. **Fiber-to-the-Home (FTTH)** - Used to provide always-on broadband services to homes and small businesses
3. **Long-Haul Networks** - Used by service providers to connect countries and cities
4. **Submarine Cable Networks** - Used to provide reliable high-speed, high-capacity solutions capable of surviving in harsh undersea environments at up to transoceanic distances.

Our focus in this course is the use of fiber within the enterprise.

## Fiber-Optic Cabling Fiber-Optic Connectors



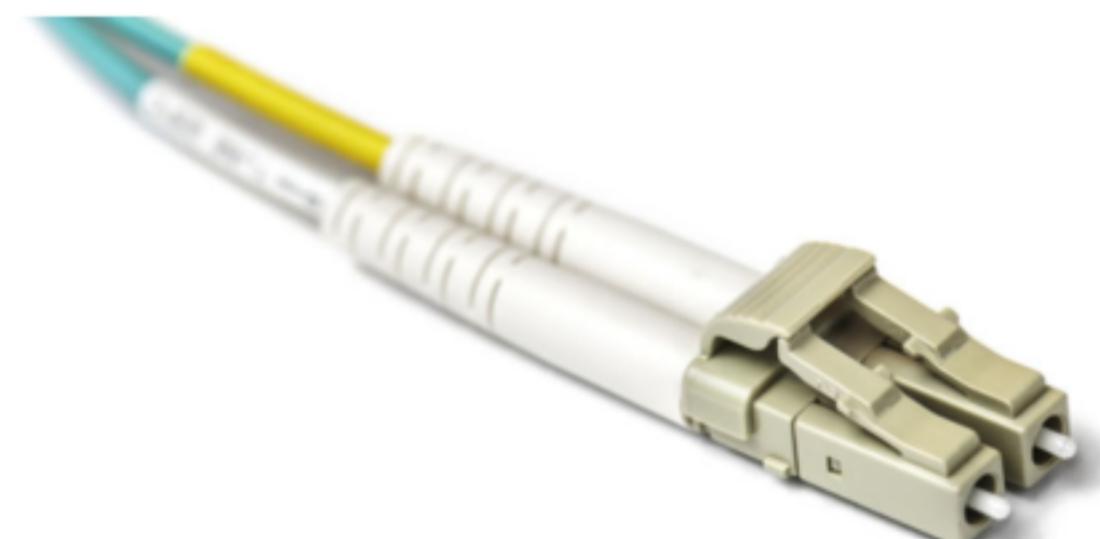
Straight-Tip (ST) Connectors



Lucent Connector (LC) Simplex Connectors

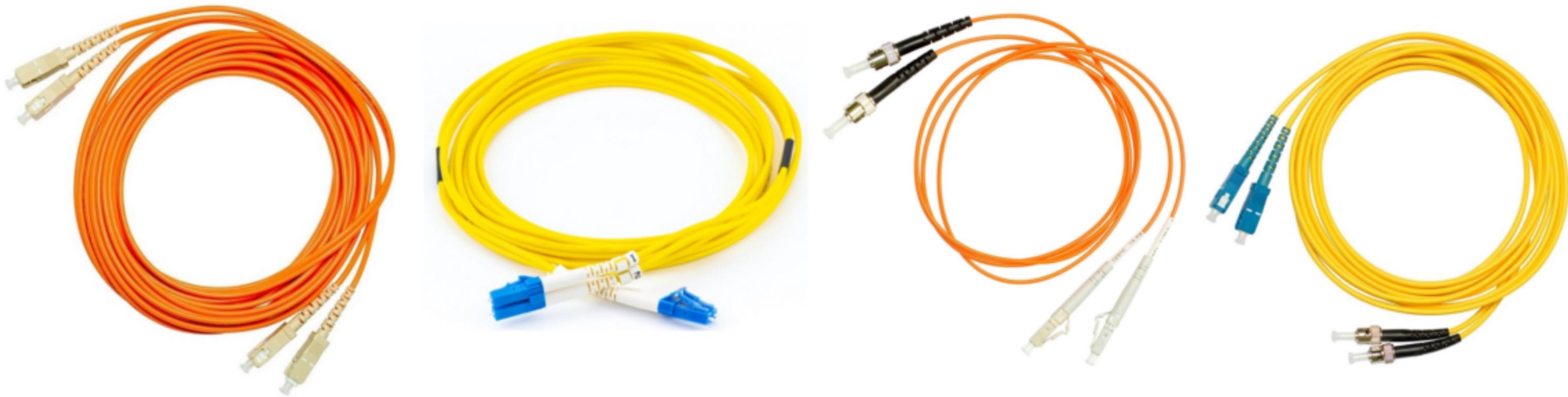


Subscriber Connector (SC) Connectors



Duplex Multimode LC Connectors

## Fiber-Optic Cabling Fiber Patch Cords



SC-SC MM Patch Cord

LC-LC SM Patch Cord

ST-LC MM Patch Cord

ST-SC SM Patch Cord

A yellow jacket is for single-mode fiber cables and orange (or aqua) for multimode fiber cables.

## Fiber-Optic Cabling Fiber versus Copper

Optical fiber is primarily used as backbone cabling for high-traffic, point-to-point connections between data distribution facilities and for the interconnection of buildings in multi-building campuses.

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

# 4.6 Wireless Media

## Wireless Media

# Properties of Wireless Media

It carries electromagnetic signals representing binary digits using radio or microwave frequencies. This provides the greatest mobility option. Wireless connection numbers continue to increase.

Some of the limitations of wireless:

- **Coverage area** - Effective coverage can be significantly impacted by the physical characteristics of the deployment location.
- **Interference** - Wireless is susceptible to interference and can be disrupted by many common devices.
- **Security** - Wireless communication coverage requires no access to a physical strand of media, so anyone can gain access to the transmission.
- **Shared medium** - WLANs operate in half-duplex, which means only one device can send or receive at a time. Many users accessing the WLAN simultaneously results in reduced bandwidth for each user.

## Wireless Media

# Types of Wireless Media

The IEEE and telecommunications industry standards for wireless data communications cover both the data link and physical layers. In each of these standards, physical layer specifications dictate:

- Data to radio signal encoding methods
- Frequency and power of transmission
- Signal reception and decoding requirements
- Antenna design and construction

### Wireless Standards:

- **Wi-Fi (IEEE 802.11)** - Wireless LAN (WLAN) technology
- **Bluetooth (IEEE 802.15)** - Wireless Personal Area network (WPAN) standard
- **WiMAX (IEEE 802.16)** - Uses a point-to-multipoint topology to provide broadband wireless access
- **Zigbee (IEEE 802.15.4)** - Low data-rate, low power-consumption communications, primarily for Internet of Things (IoT) applications



## Wireless Media

# Wireless LAN

In general, a Wireless LAN (WLAN) requires the following devices:

- **Wireless Access Point (AP)** - Concentrate wireless signals from users and connect to the existing copper-based network infrastructure
- **Wireless NIC Adapters** - Provide wireless communications capability to network hosts

There are a number of WLAN standards. When purchasing WLAN equipment, ensure compatibility, and interoperability.

Network Administrators must develop and apply stringent security policies and processes to protect WLANs from unauthorized access and damage.

## Packet Tracer – Connect a Wired and Wireless LAN

In this Packet Tracer, you will do the following:

- Connect to the Cloud
- Connect a Router
- Connect Remaining Devices
- Verify Connections
- Examine the Physical Topology

## Wireless Media

# Lab – View Wired and Wireless NIC Information

In this lab, you will complete the following objectives:

- Identify and Work with PC NICs
- Identify and Use the System Tray Network Icons



# 4.7 Module Practice and Quiz

## Module Practice and Quiz

# What did I learn in this module?

- Before any network communications can occur, a physical connection to a local network, either wired or wireless, must be established.
- The physical layer consists of electronic circuitry, media, and connectors developed by engineers.
- The physical layer standards address three functional areas: physical components, encoding, and signaling.
- Three types of copper cabling are: UTP, STP, and coaxial cable (coax).
- UTP cabling conforms to the standards established jointly by the TIA/EIA. The electrical characteristics of copper cabling are defined by the Institute of Electrical and Electronics Engineers (IEEE).
- The main cable types that are obtained by using specific wiring conventions are Ethernet Straight-through and Ethernet Crossover.

Module Practice and Quiz

## What did I learn in this module (Cont.)?

- Optical fiber cable transmits data over longer distances and at higher bandwidths than any other networking media.
- There are four types of fiber-optic connectors: ST, SC, LC, and duplex multimode LC.
- Fiber-optic patch cords include SC-SC multimode, LC-LC single-mode, ST-LC multimode, and SC-ST single-mode.
- Wireless media carry electromagnetic signals that represent the binary digits of data communications using radio or microwave frequencies. Wireless does have some limitations, including coverage area, interference, security, and the problems that occur with any shared medium.
- Wireless standards include the following: Wi-Fi (IEEE 802.11), Bluetooth (IEEE 802.15), WiMAX (IEEE 802.16), and Zigbee (IEEE 802.15.4).
- Wireless LAN (WLAN) requires a wireless AP and wireless NIC adapters.

# 4.8 Summary

Module Practice and Quiz

## Packet Tracer – Connect the Physical Layer

In this Packet Tracer, you will do the following:

- Identify Physical Characteristics of Internetworking Devices
- Select Correct Modules for Connectivity
- Connect Devices
- Check Connectivity



## Module 4: Physical Layer

# New Terms and Commands

- |   |   |
|---|---|
| <ul style="list-style-type: none"><li>• Telecommunications Industry Association/Electronic Industries Association (TIA/EIA)</li><li>• latency</li><li>• throughput</li><li>• goodput</li><li>• Electromagnetic interference (EMI)</li><li>• Radio frequency interference (RFI)</li><li>• Crosstalk</li><li>• Unshielded Twisted Pair (UTP)</li><li>• Shielded Twisted Pair (STP)</li><li>• Coaxial cable</li><li>• RJ-45</li><li>• Cancellation</li><li>• TIA/EIA-568</li></ul> | <ul style="list-style-type: none"><li>• Ethernet Straight-through</li><li>• Ethernet crossover</li><li>• Rollover</li><li>• Single-Mode Fiber (SMF)</li><li>• Multimode (MMF)</li><li>• Straight-tip (ST) Connectors</li><li>• Subscriber Connector (SC) Connectors</li><li>• Lucent Connector (LC) Simplex Connectors</li><li>• Duplex Multimode LC Connectors</li><li>• Bluetooth (IEEE 802.15)</li><li>• WiMAX (IEEE 802.16)</li><li>• Zigbee (IEEE 802.15.4)</li><li>• Wireless Access Point (AP)</li></ul> |
|---|---|





# Module 12: IPv6 Addressing

Introduction to Networks v7.0  
(ITN)



# Module Objectives

**Module Title:** IPv6 Addressing

**Module Objective:** Implement an IPv6 Addressing scheme.

Topic Title	Topic Objective
IPv4 Issues	Explain the need for IPv6 addressing.
IPv6 Address Representation	Explain how IPv6 addresses are represented.
IPv6 Address Types	Compare types of IPv6 network addresses.
GUA and LLA Static Configuration	Explain how to Configure static global unicast and link-local IPv6 network addresses.
Dynamic Addressing for IPv6 GUAs	Explain how to configure global unicast addresses dynamically.



## Module Objectives (Cont.)

**Module Title:** IPv6 Addressing

**Module Objective:** Implement an IPv6 Addressing scheme.

Topic Title	Topic Objective
Dynamic Addressing for IPv6 LLAs	Configure link-local addresses dynamically.
IPv6 Multicast Addresses	Identify IPv6 addresses.
Subnet an IPv6 Network	Implement a subnetted IPv6 addressing scheme.



# 12.1 IPv4 Issues



## IPv4 Issues Need for IPv6

- IPv4 is running out of addresses. IPv6 is the successor to IPv4. IPv6 has a much larger 128-bit address space.
- The development of IPv6 also included fixes for IPv4 limitations and other enhancements.
- With an increasing internet population, a limited IPv4 address space, issues with NAT and the IoT, the time has come to begin the transition to IPv6.



## IPv4 Issues

# IPv4 and IPv6 Coexistence

Both IPv4 and IPv6 will coexist in the near future and the transition will take several years.

The IETF has created various protocols and tools to help network administrators migrate their networks to IPv6. These migration techniques can be divided into three categories:

- **Dual stack** -The devices run both IPv4 and IPv6 protocol stacks simultaneously.
- **Tunneling** – A method of transporting an IPv6 packet over an IPv4 network. The IPv6 packet is encapsulated inside an IPv4 packet.
- **Translation** - Network Address Translation 64 (NAT64) allows IPv6-enabled devices to communicate with IPv4-enabled devices using a translation technique similar to NAT for IPv4.

**Note:** Tunneling and translation are for transitioning to native IPv6 and should only be used where needed. The goal should be native IPv6 communications from source to destination.



# 12.2 IPv6 Address Representation



## IPv6 Address Representation IPv6 Addressing Formats

- IPv6 addresses are 128 bits in length and written in hexadecimal.
- IPv6 addresses are not case-sensitive and can be written in either lowercase or uppercase.
- The preferred format for writing an IPv6 address is `x:x:x:x:x:x:x:x`, with each “x” consisting of four hexadecimal values.
- In IPv6, a hextet is the unofficial term used to refer to a segment of 16 bits, or four hexadecimal values.
- Examples of IPv6 addresses in the preferred format:

`2001:0db8:0000:1111:0000:0000:0000:0200`

`2001:0db8:0000:00a3:abcd:0000:0000:1234`



## IPv6 Address Representation Rule 1 – Omit Leading Zero

The first rule to help reduce the notation of IPv6 addresses is to omit any leading 0s (zeros).

### Examples:

- 01ab can be represented as 1ab
- 09f0 can be represented as 9f0
- 0a00 can be represented as a00
- 00ab can be represented as ab

**Note:** This rule only applies to leading 0s, NOT to trailing 0s, otherwise the address would be ambiguous.

Type	Format
Preferred	2001 : 0db8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200
No leading zeros	2001 : db8 : 0 : 1111 : 0 : 0 : 0 : 200



## IPv6 Address Representation Rule 2 – Double Colon

A double colon (:) can replace any single, contiguous string of one or more 16-bit hexets consisting of all zeros.

### Example:

- 2001:db8:cafe:1:0:0:0:1 (leading 0s omitted) could be represented as 2001:db8:cafe:1::1

**Note:** The double colon (:) can only be used once within an address, otherwise there would be more than one possible resulting address.

Type	Format
Preferred	2001 : 0db8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200
Compressed	2001:db8:0:1111::200



# 12.3 IPv6 Address Types



## IPv6 Address Types

# Unicast, Multicast, Anycast

There are three broad categories of IPv6 addresses:

- **Unicast** – Unicast uniquely identifies an interface on an IPv6-enabled device.
- **Multicast** – Multicast is used to send a single IPv6 packet to multiple destinations.
- **Anycast** – This is any IPv6 unicast address that can be assigned to multiple devices. A packet sent to an anycast address is routed to the nearest device having that address.

**Note:** Unlike IPv4, IPv6 does not have a broadcast address. However, there is an IPv6 all-nodes multicast address that essentially gives the same result.

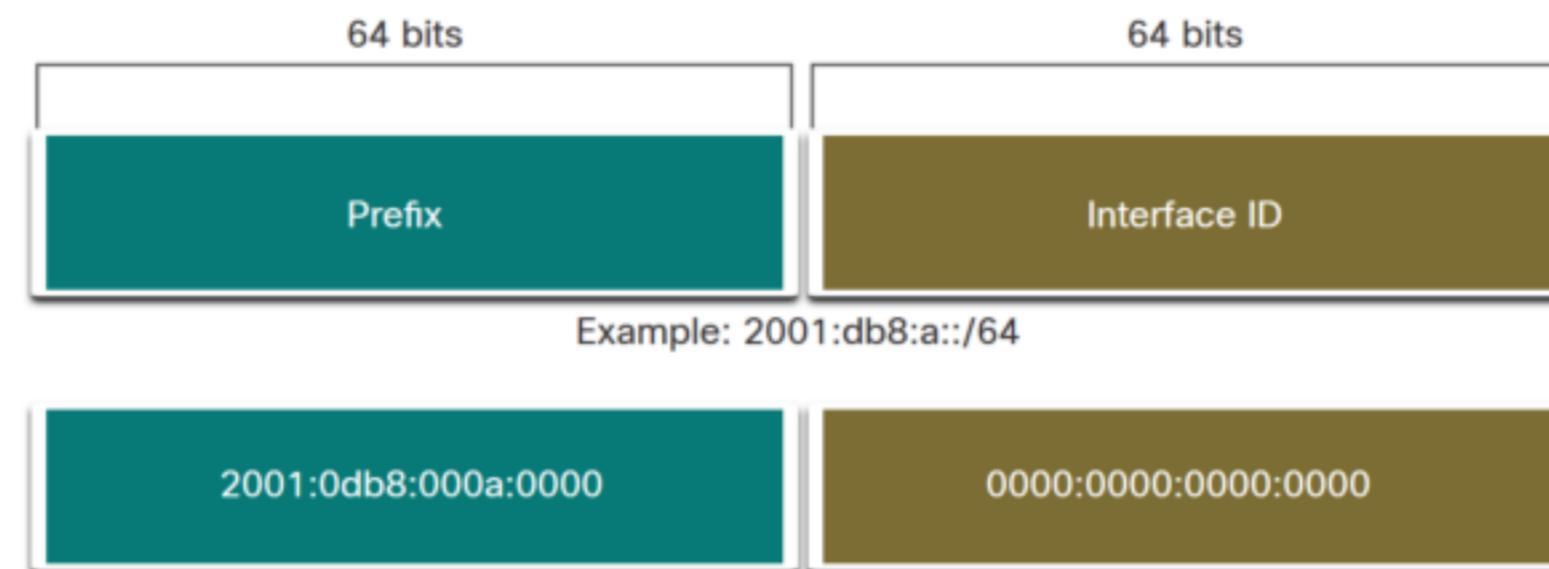


## IPv6 Address Types

### IPv6 Prefix Length

Prefix length is represented in slash notation and is used to indicate the network portion of an IPv6 address.

The IPv6 prefix length can range from 0 to 128. The recommended IPv6 prefix length for LANs and most other types of networks is /64.



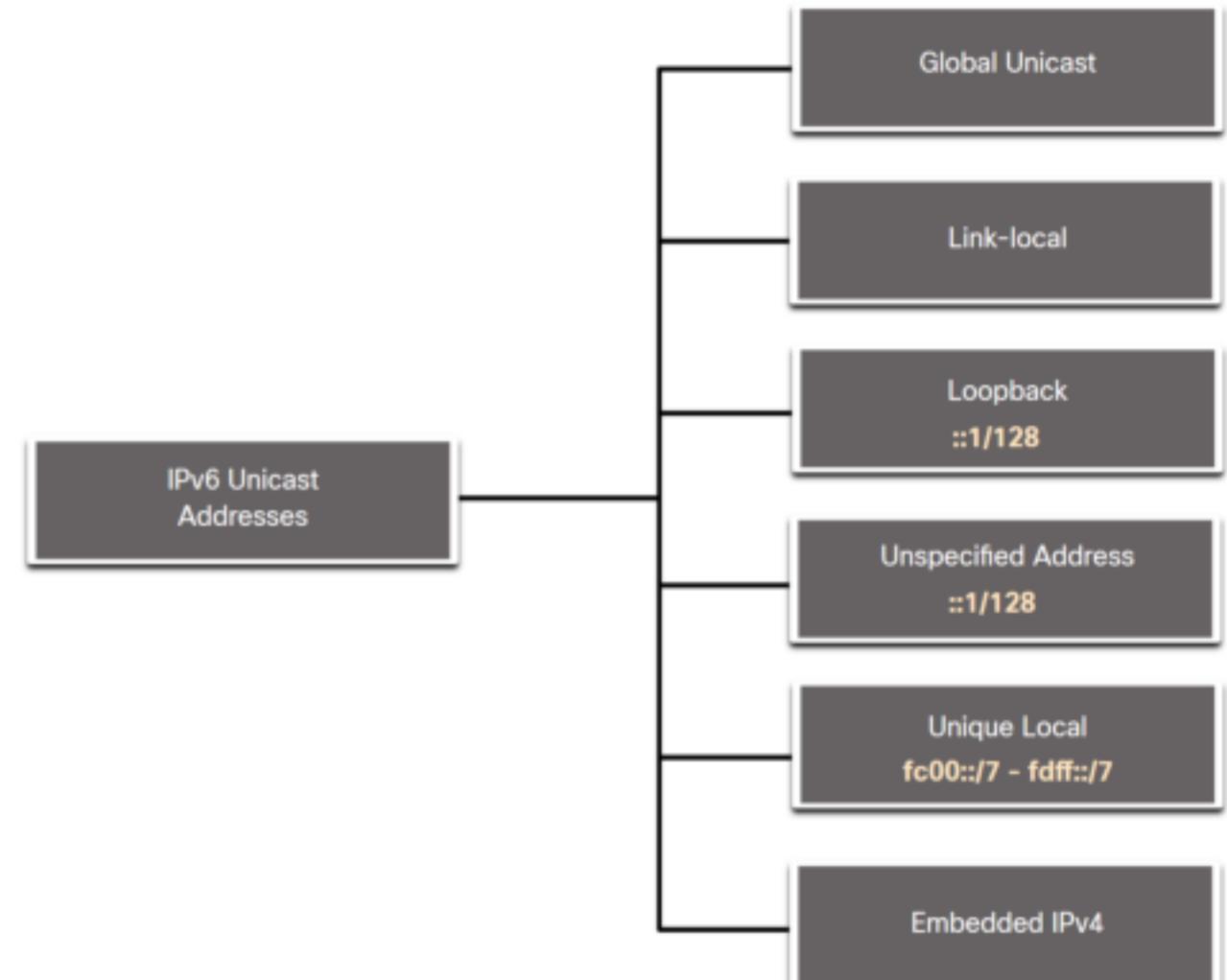
**Note:** It is strongly recommended to use a 64-bit Interface ID for most networks. This is because stateless address autoconfiguration (SLAAC) uses 64 bits for the Interface ID. It also makes subnetting easier to create and manage.

## IPv6 Address Types

# Types of IPv6 Unicast Addresses

Unlike IPv4 devices that have only a single address, IPv6 addresses typically have two unicast addresses:

- **Global Unicast Address (GUA)** – This is similar to a public IPv4 address. These are globally unique, internet-routable addresses.
- **Link-local Address (LLA)** - Required for every IPv6-enabled device and used to communicate with other devices on the same local link. LLAs are not routable and are confined to a single link.



## IPv6 Address Types

### A Note About the Unique Local Address

The IPv6 unique local addresses (range fc00::/7 to fdff::/7) have some similarity to RFC 1918 private addresses for IPv4, but there are significant differences:

- Unique local addresses are used for local addressing within a site or between a limited number of sites.
- Unique local addresses can be used for devices that will never need to access another network.
- Unique local addresses are not globally routed or translated to a global IPv6 address.

**Note:** Many sites use the private nature of RFC 1918 addresses to attempt to secure or hide their network from potential security risks. This was never the intended use of ULAs.

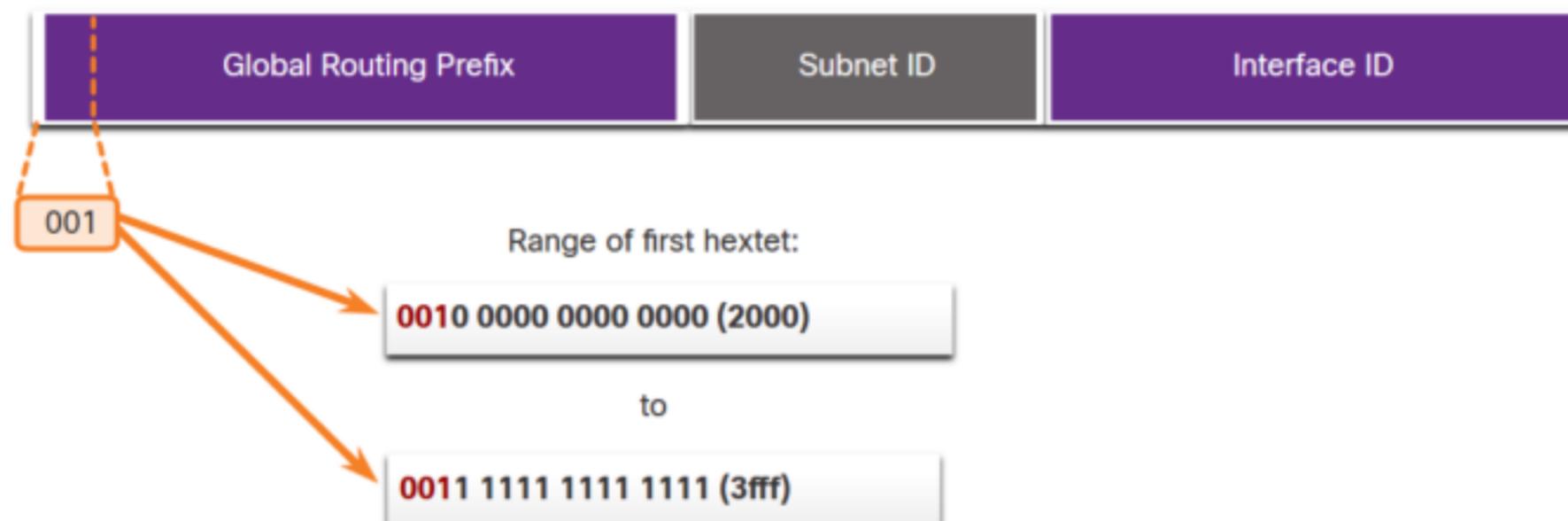


## IPv6 Address Types

### IPv6 GUA

IPv6 global unicast addresses (GUAs) are globally unique and routable on the IPv6 internet.

- Currently, only GUAs with the first three bits of 001 or 2000::/3 are being assigned.
- Currently available GUAs begins with a decimal 2 or a 3 (This is only 1/8th of the total available IPv6 address space).



## IPv6 Address Types

# IPv6 GUA Structure

### Global Routing Prefix:

- The global routing prefix is the prefix, or network, portion of the address that is assigned by the provider, such as an ISP, to a customer or site. The global routing prefix will vary depending on ISP policies.

### Subnet ID:

- The Subnet ID field is the area between the Global Routing Prefix and the Interface ID. The Subnet ID is used by an organization to identify subnets within its site.

### Interface ID:

- The IPv6 interface ID is equivalent to the host portion of an IPv4 address. It is strongly recommended that in most cases /64 subnets should be used, which creates a 64-bit interface ID.

**Note:** IPv6 allows the all-0s and all-1s host addresses can be assigned to a device. The all-0s address is reserved as a Subnet-Router anycast address, and should be assigned only to routers.

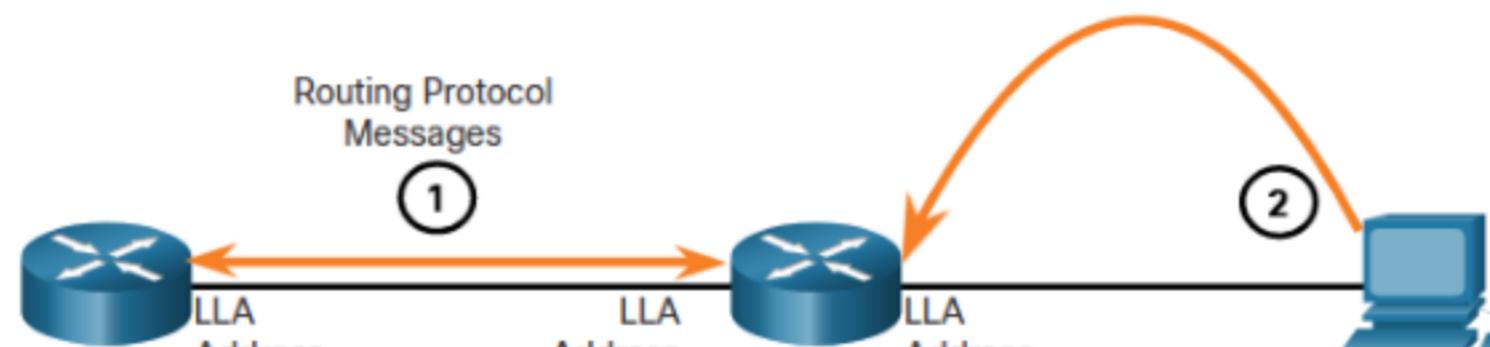


## IPv6 Address Types

### IPv6 LLA

An IPv6 link-local address (LLA) enables a device to communicate with other IPv6-enabled devices on the same link and only on that link (subnet).

- Packets with a source or destination LLA cannot be routed.
- Every IPv6-enabled network interface must have an LLA.
- If an LLA is not configured manually on an interface, the device will automatically create one.
- IPv6 LLAs are in the fe80::/10 range.



1. Routers use the LLA of neighbor routers to send routing updates.
2. Hosts use the LLA of a local router as the default-gateway.