Routing and Switching

Course Information

Dr. Fawaz Saleem Bokhari

Course Information

1. Network Fundamentals
2. Routing Protocols and Concepts
3. Switching Techniques

Course Material

Text Book/s

- Introduction to Networks by Cisco Press
- Routing and Switching Essentials, Companion Guide by Cisco Academy

Tools

- Packet Tracer

http://www.cabrillo.edu/~rgraziani/

Grading

Quiz: **15%**

Mid-Term: **35%**

Final-Term: **50%**

Tips

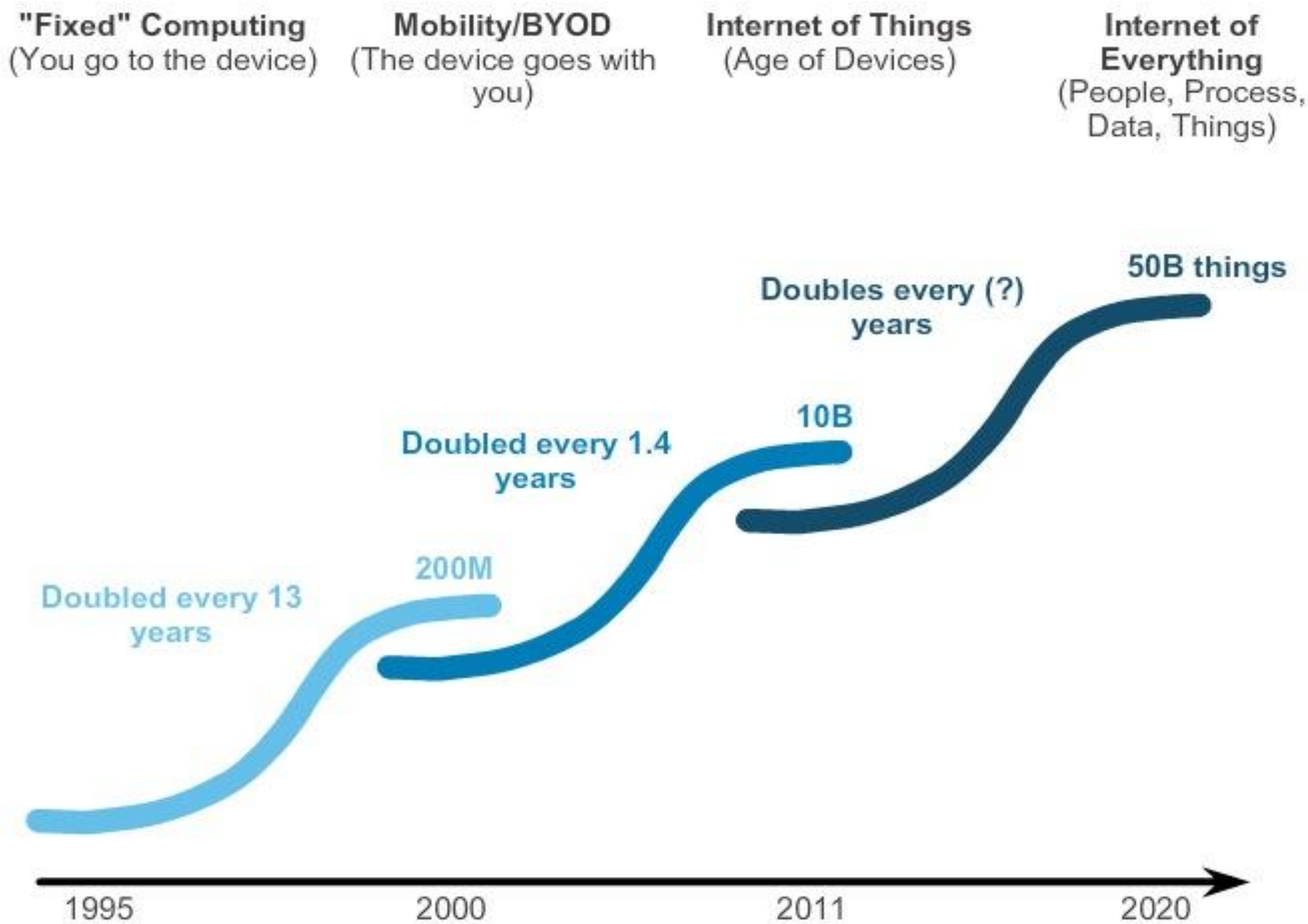
Succeeding in this course

- Find a quiet space
- Do not multitask
- Take notes on paper or in your book

Components of a Network

Technology
Then and Now

Technology Then and Now



Networks Support the Way We Learn

- Virtual Classrooms
- On-demand Video
- Collaborative Learning Spaces
- Mobile Learning

Networks Support the Way We Communicate

- Instant Messaging (IM)
- Social Media
- Weblogs
- Podcasting
- P2P File Sharing

Networks Support the Way We Play/Do Business

- Online Gaming
- Online Shopping
- Online Entertainment

Network Components - Clients and Servers

Hosts

- Client, Server, or both
- Software determines the role
- Run application programs

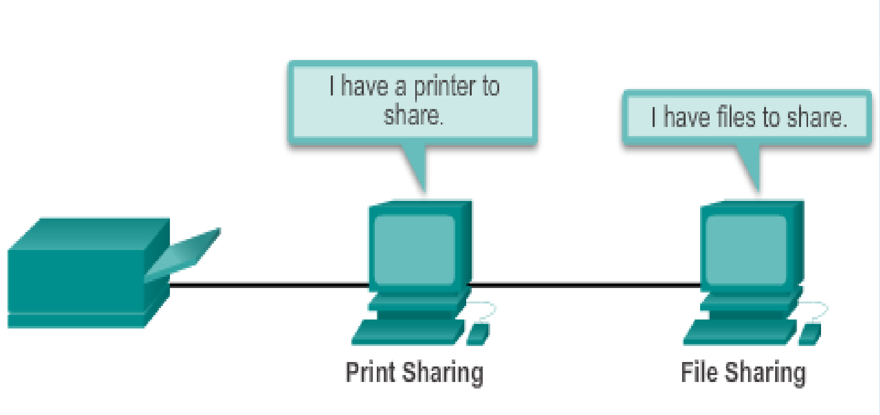
Servers

- Provide information and services to clients
- e-mail or web pages

Clients

- Request information from the server.

Peer to Peer



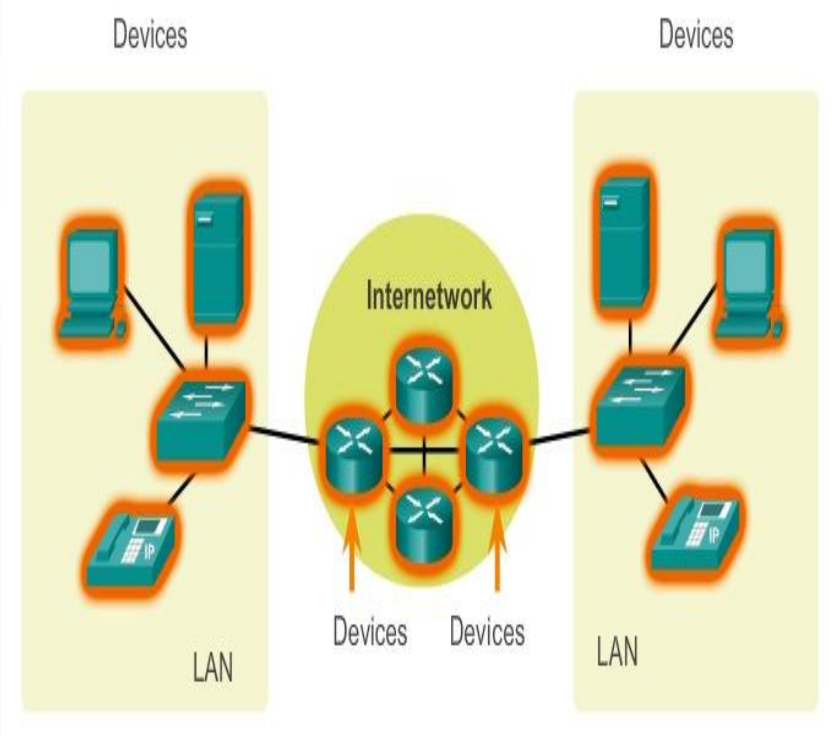
Advantages

- Easy to set up
- Less complexity
- Lower cost

Disadvantages

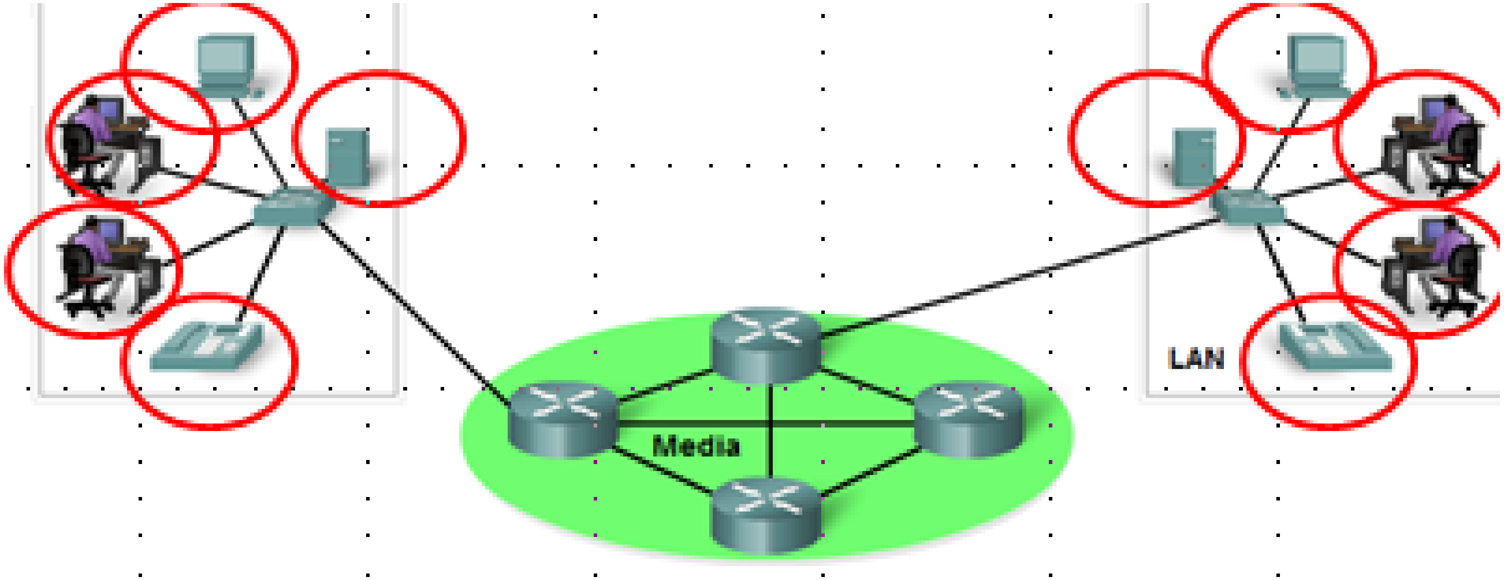
- No centralized administration
- Not so secure
- Not scalable

Network Components



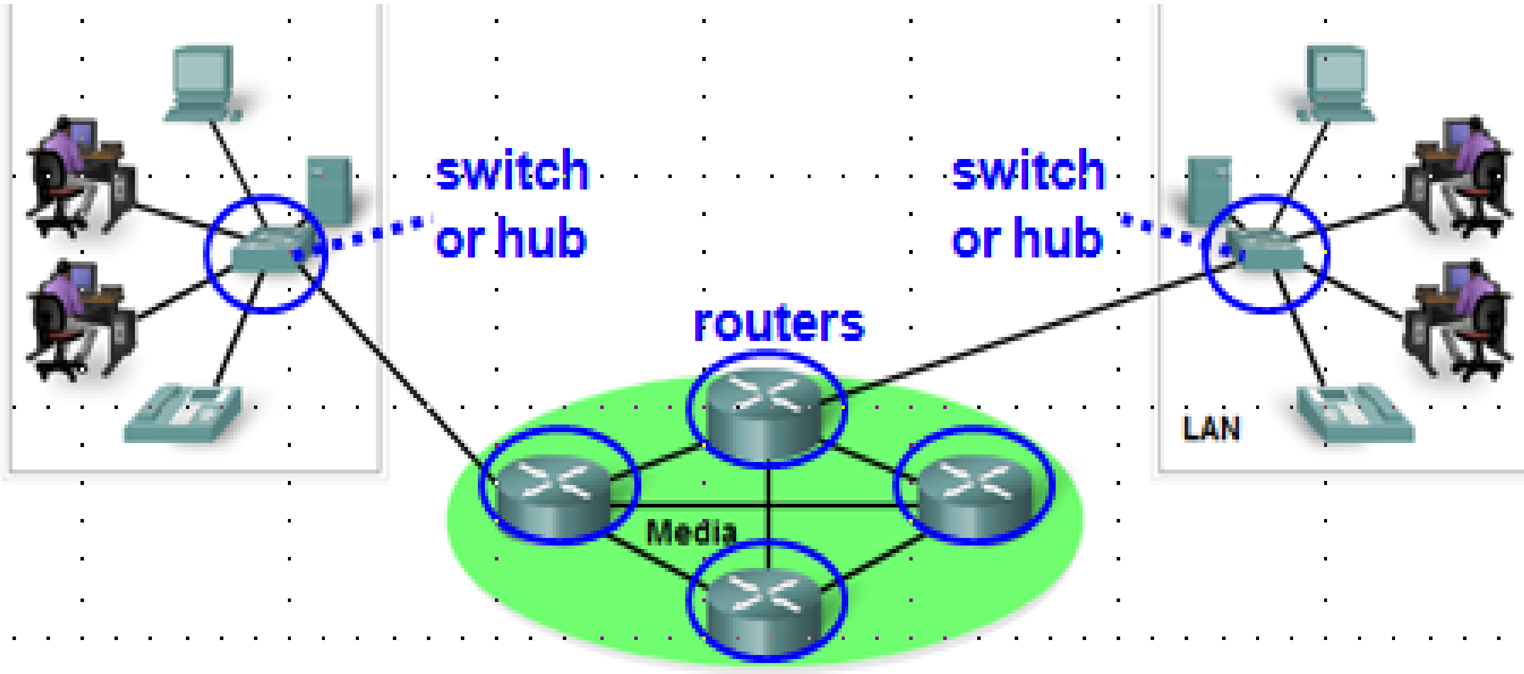
Devices
Media

End Devices



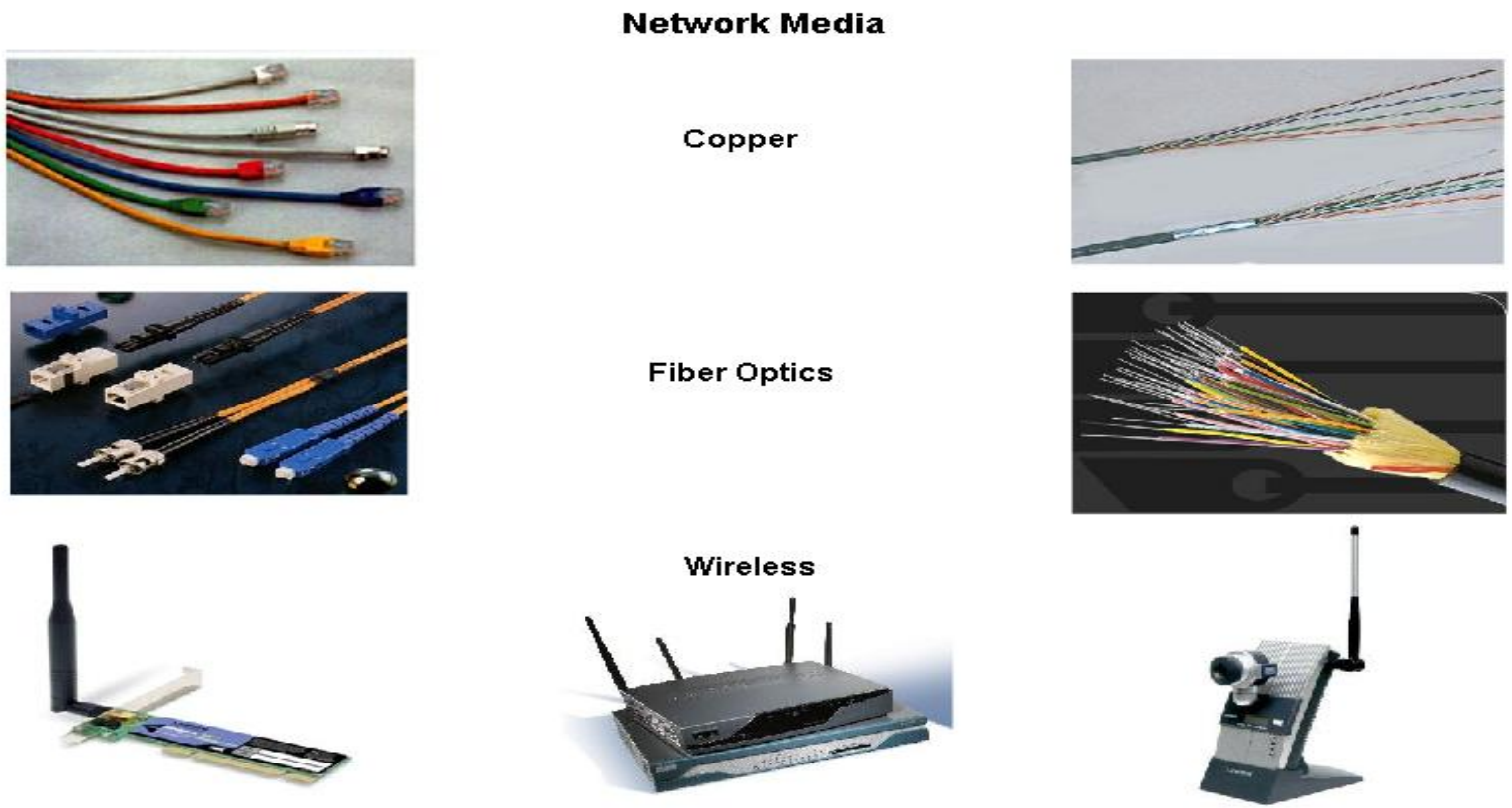
- Computers
- Printers
- VoIP Phones
- Security Cameras
- Mobile Handheld Devices

Intermediary Network Devices



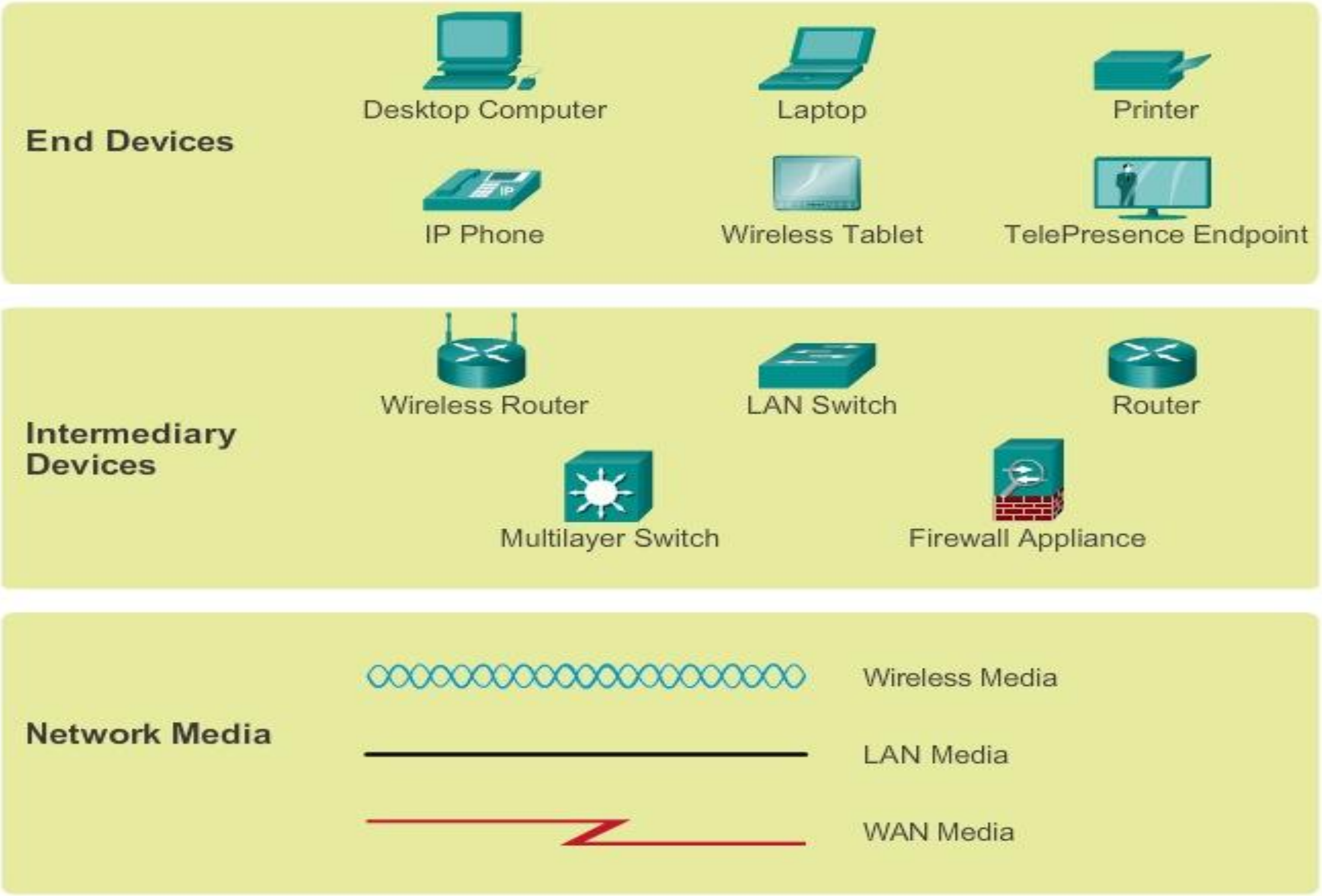
- Network Access (Switches and Wireless Access Points)
- Internetworking (Routers)
- Security (Firewalls)

Network Media



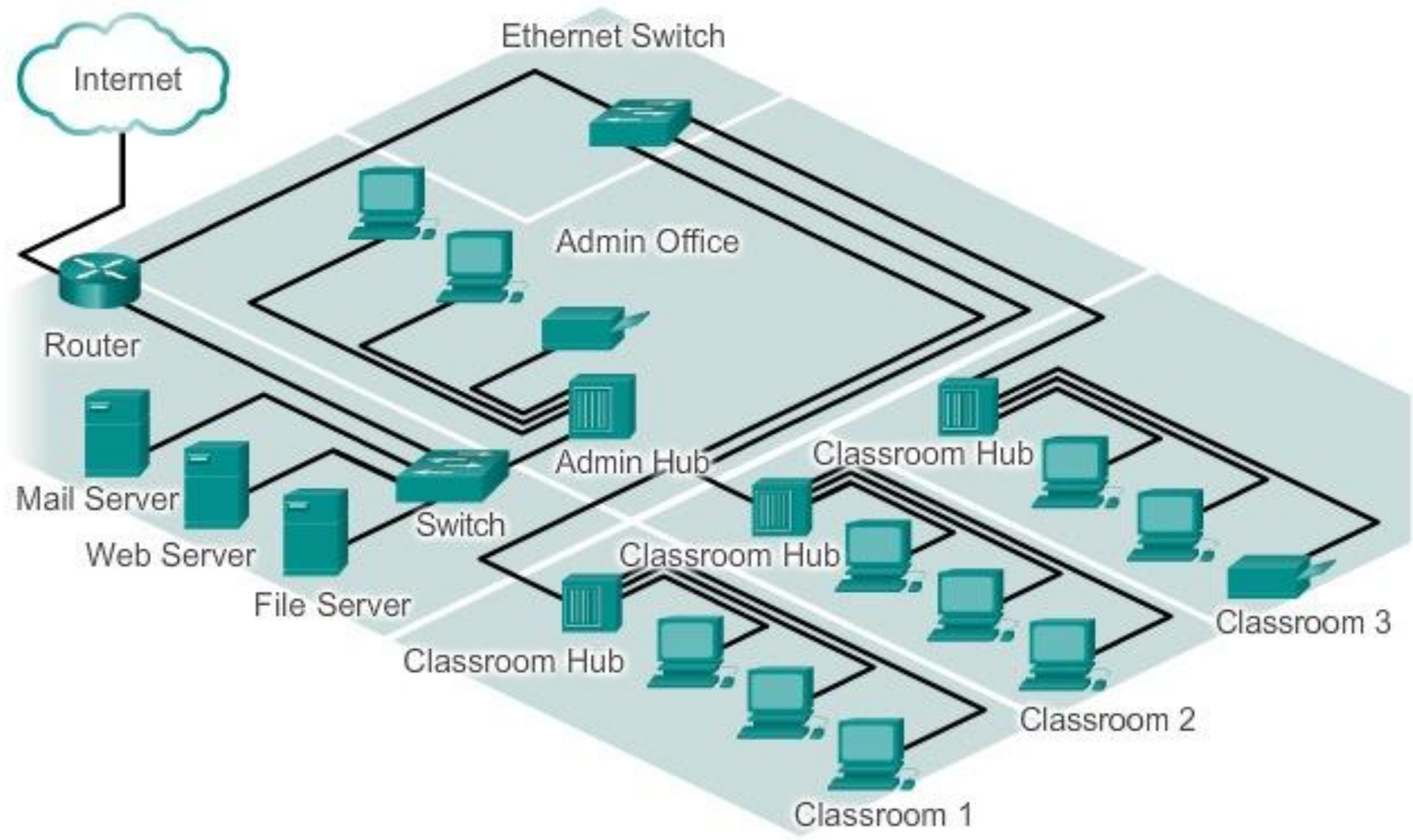
- Copper – Electronic pulses
- Fiber Optics – Pulses of light
- Wireless – Electromagnetic waves

Network Representations



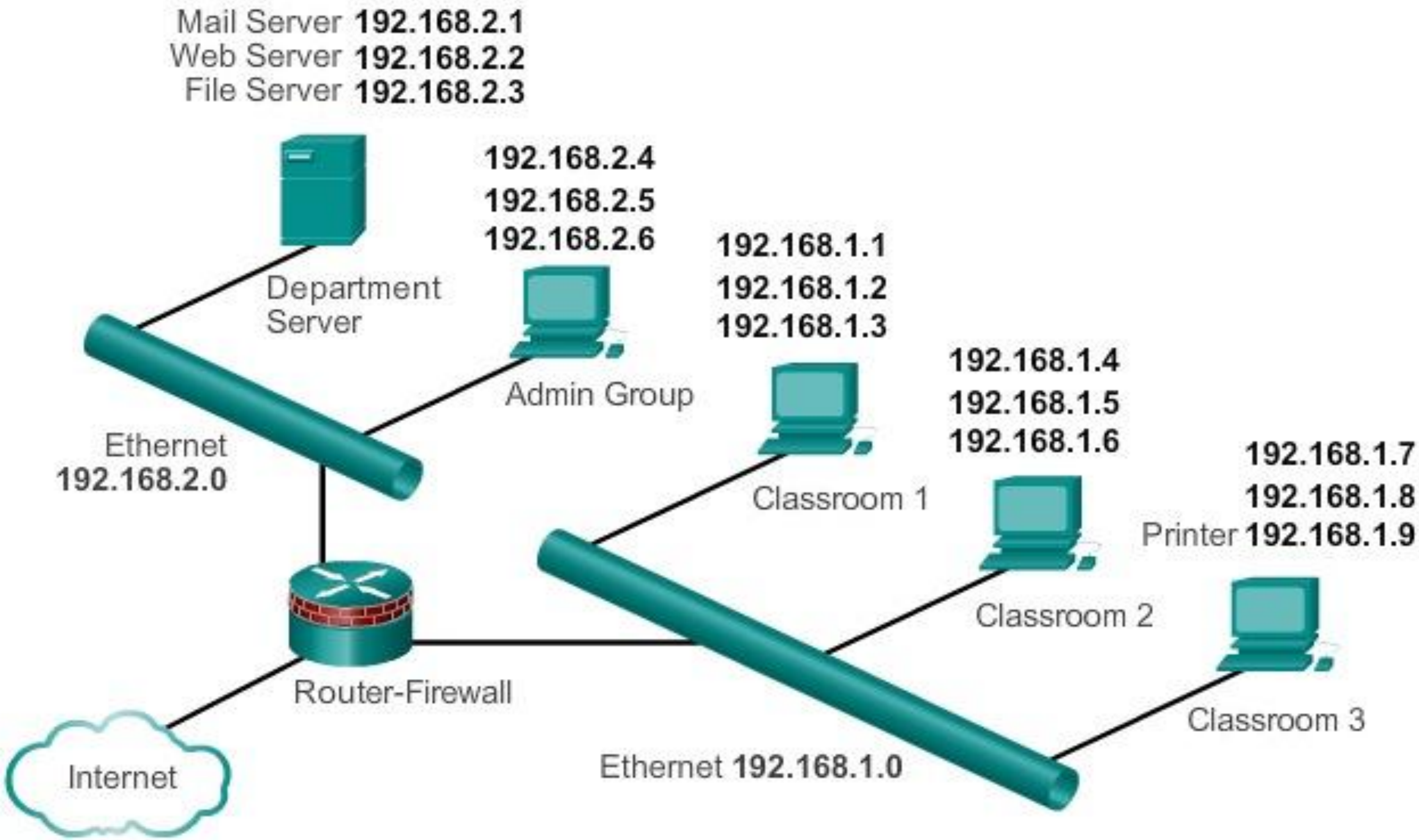
Topology Diagrams

Physical Topology



Topology Diagrams

Logical Topology



Topology Diagrams

Logical Topology

Physical Topology

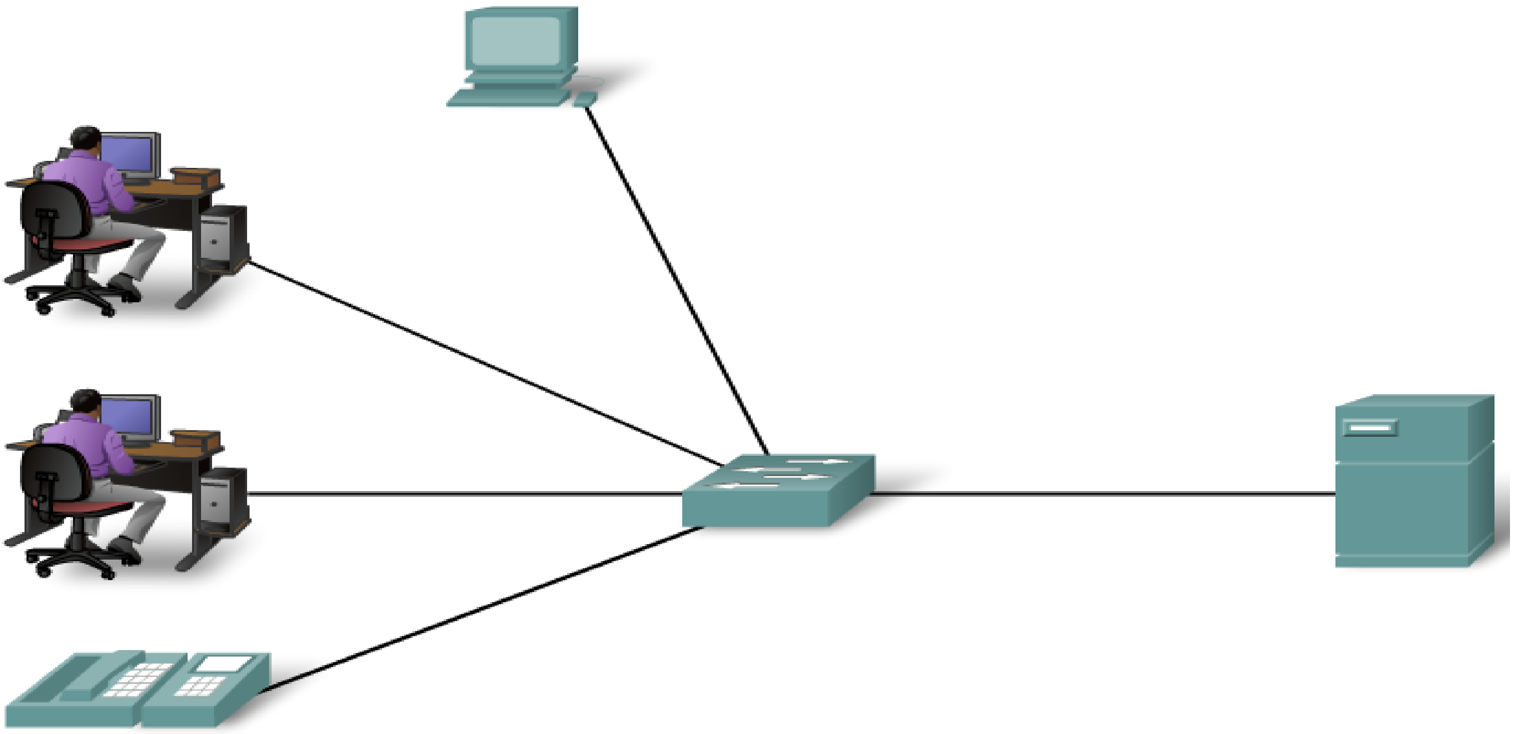
LANs, WANs and the Internet

Types of Networks

Types of Networks

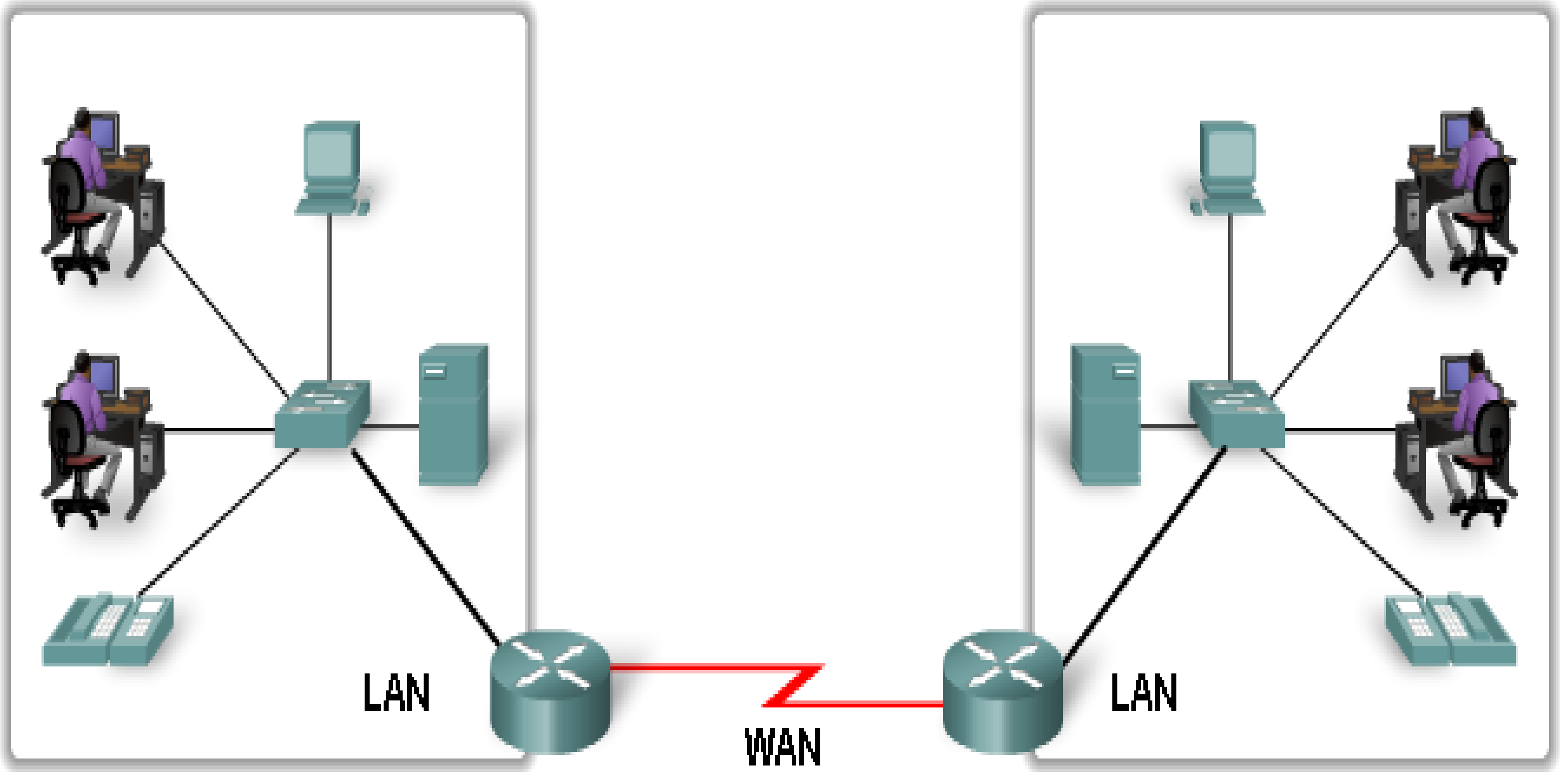
- Local Area Network (LAN)
- Wide Area Network (WAN)
- Metropolitan Area Network (MAN)
- Wireless LAN (WLAN)
- Storage Area Network (SAN)

Local Area Network (LAN)



- Interconnects devices in a limited area
- Administered by single organization/individual
- Provide high speed bandwidth

Wide Area Network (WAN)



- Interconnects LANs
- Administered by multiple service providers
- Slower speed links between LANs

MAN, WLAN, and SAN

MAN

- Greater than LAN but smaller than WAN

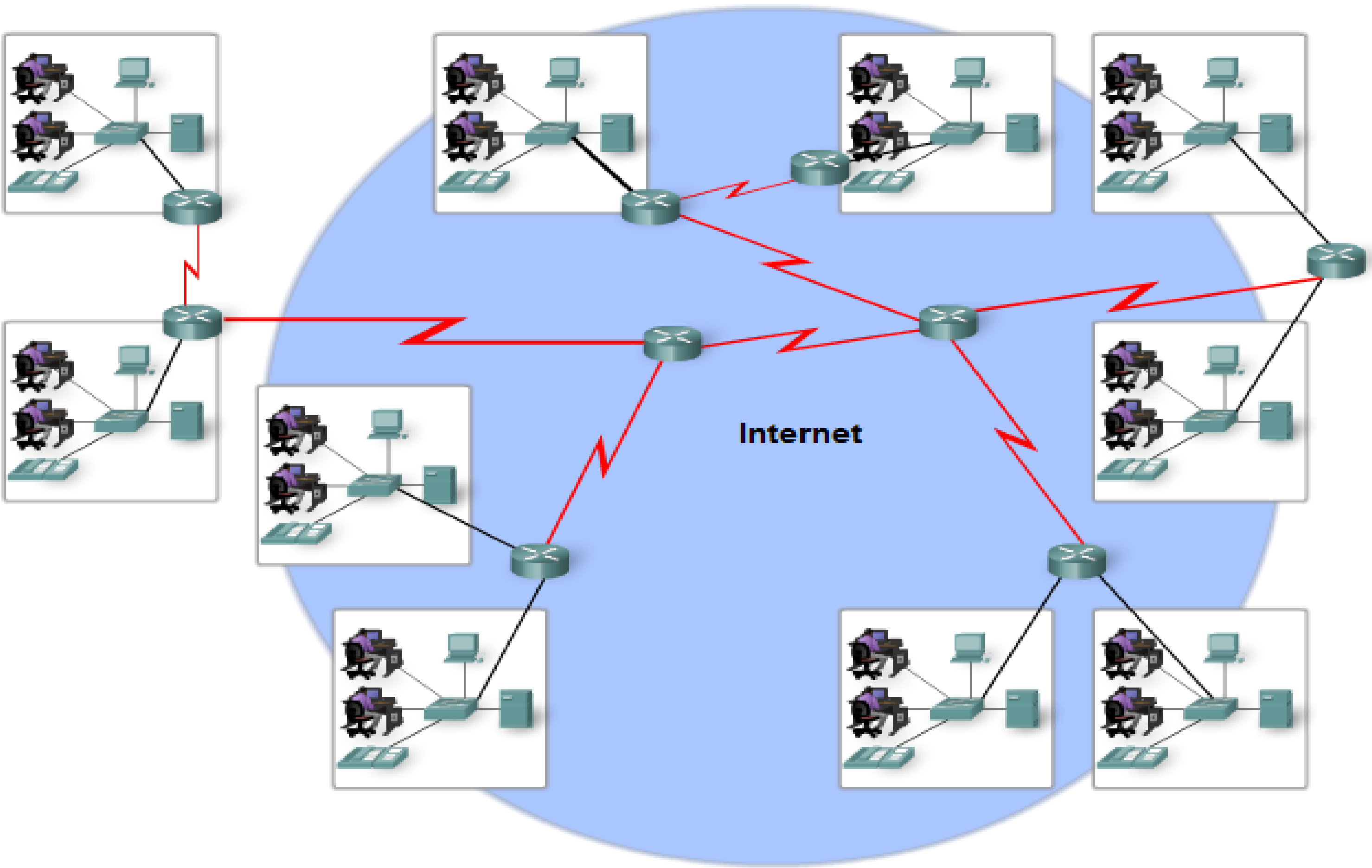
WLAN

- Similar to LAN but wireless

SAN

- Designed to support file servers, and provide data storage.

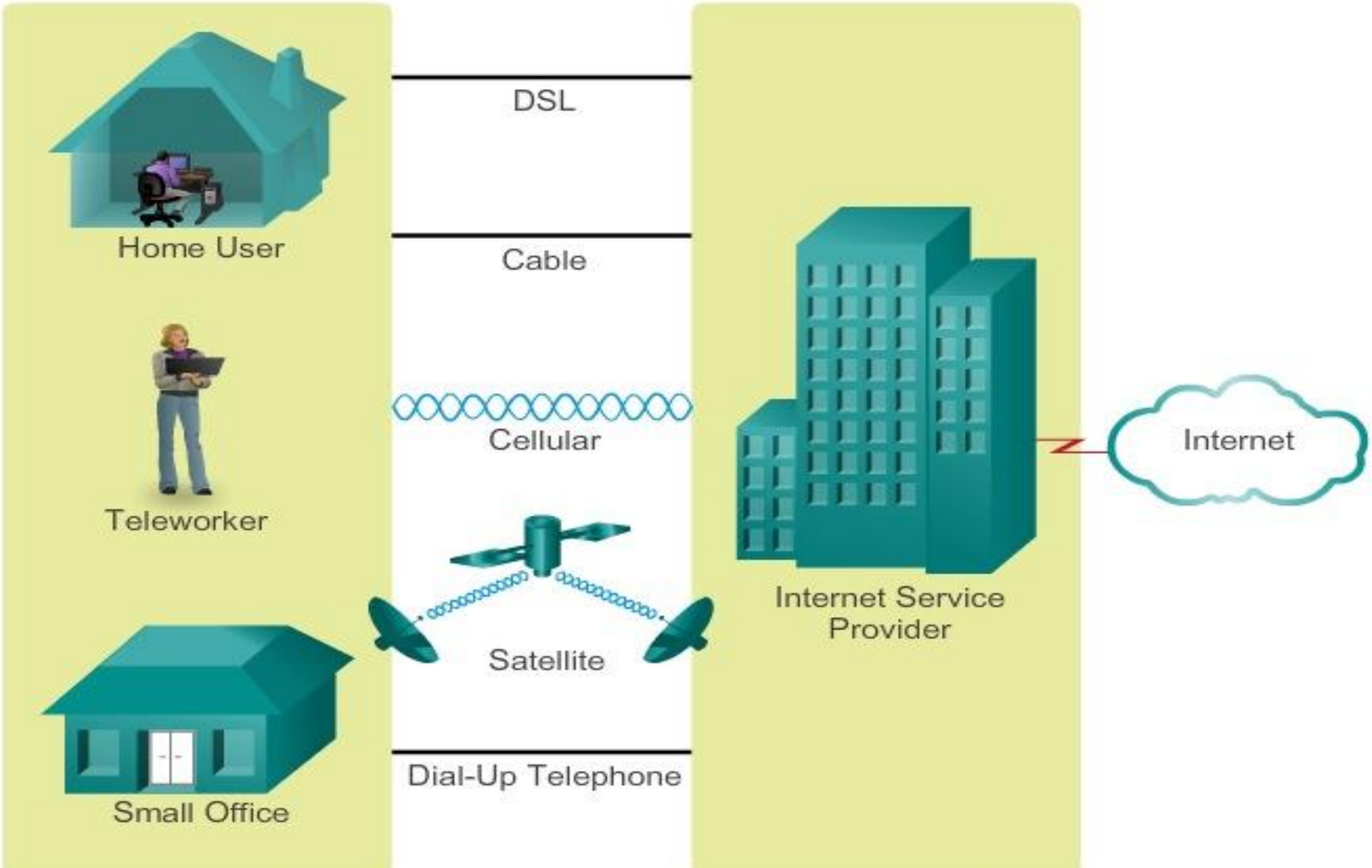
The Internet – A Network of Networks



Connecting to the Internet

Internet Access Technologies

Internet Access Technologies



Packet Tracer Basics: Part I

Part I

Packet Tracer Basics: Part II

Part II

Rules of Communication

Establishing Rules

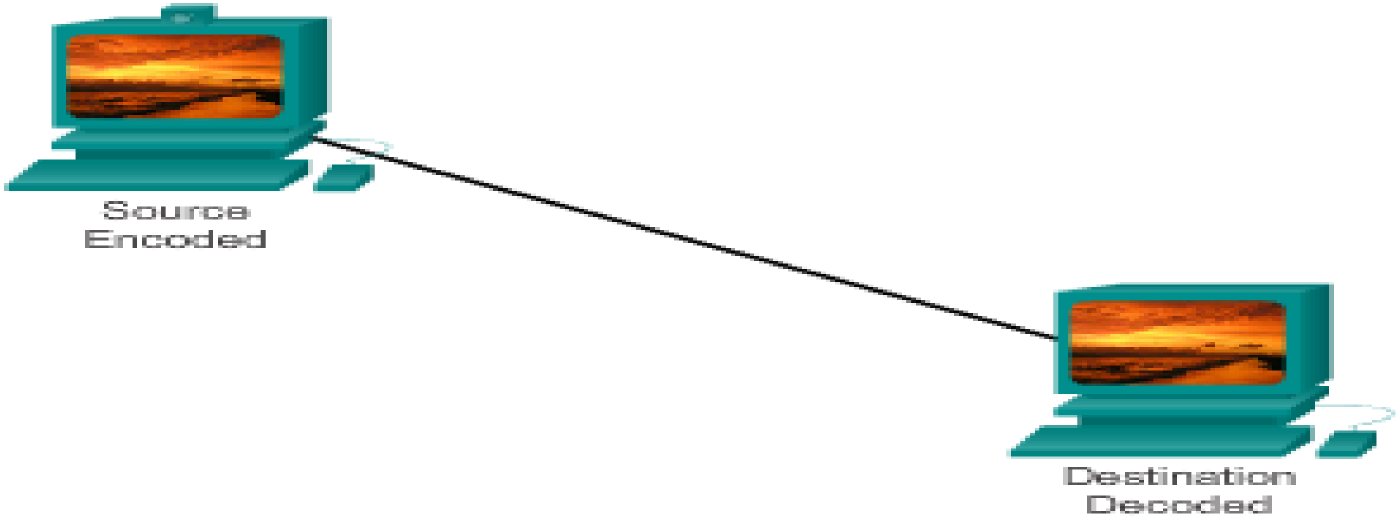
Establishing Rules

- Communication begins with a message, or information, that must be sent from a source to a destination

Protocol: Rules that govern communications
Protocol suite: A group of inter-related protocols

Example: TCP/IP

Message Encoding



Message Formatting and Encapsulation

Recipient (destination) Location address	Sender (source) Location address	Salutation (start of message indicator)	Recipient (destination) identifier	Content of Letter (encapsulated data)	Sender (source) identifier	End of Frame (End of message indicator)
Envelope Addressing		Encapsulated Letter				
1400 Main Street Canton, Ohio 44203	4085 SE Pine Street Ocala, Florida 34471	Dear	Jane	I just returned from my trip. I thought you might like to see my pictures.	John	

Message Size, Timing, Access Method

Message Size

- Breaks into smaller size or sentences

Timing

- When to speak, and how long to wait for a response

Access Method

- Determines when someone is able to send a message
- If two people talk at the same time, a collision occurs
- Hosts need an access method to know when to begin sending messages

Flow Control, Response Timeout

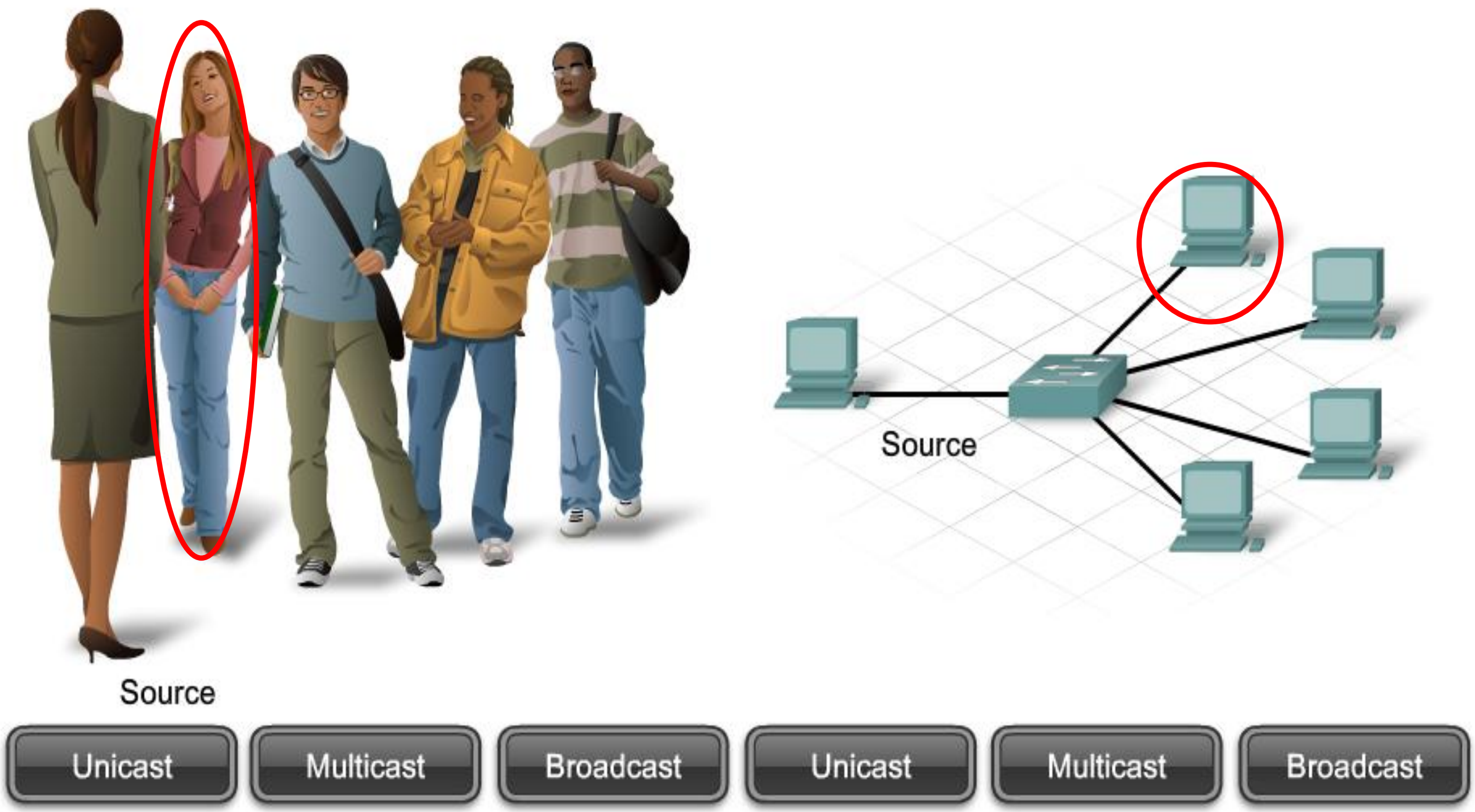
Flow Control

- How much information can be sent.
- Hosts use flow control to negotiate how much data can be sent/received

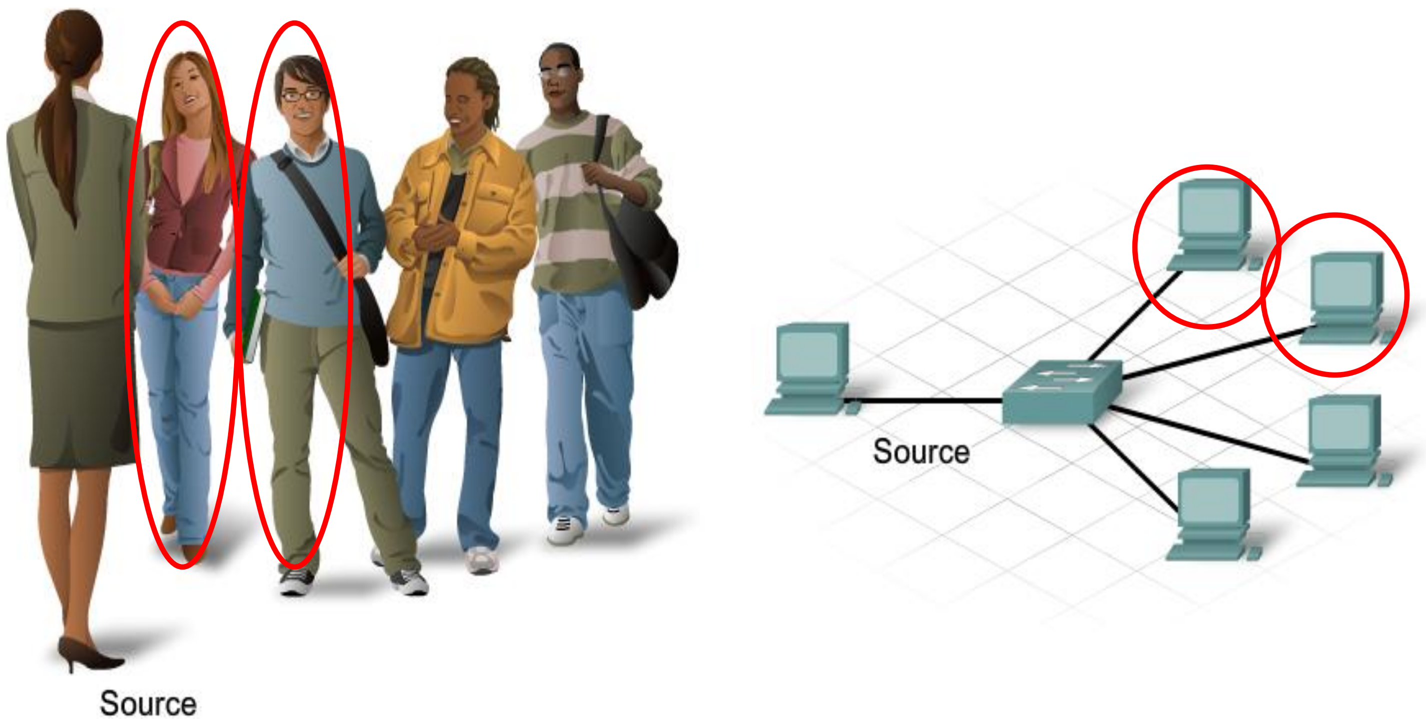
Response Timeout

- Hosts on the network also have rules that specify how long to wait for responses and what action to take if a response timeout occurs

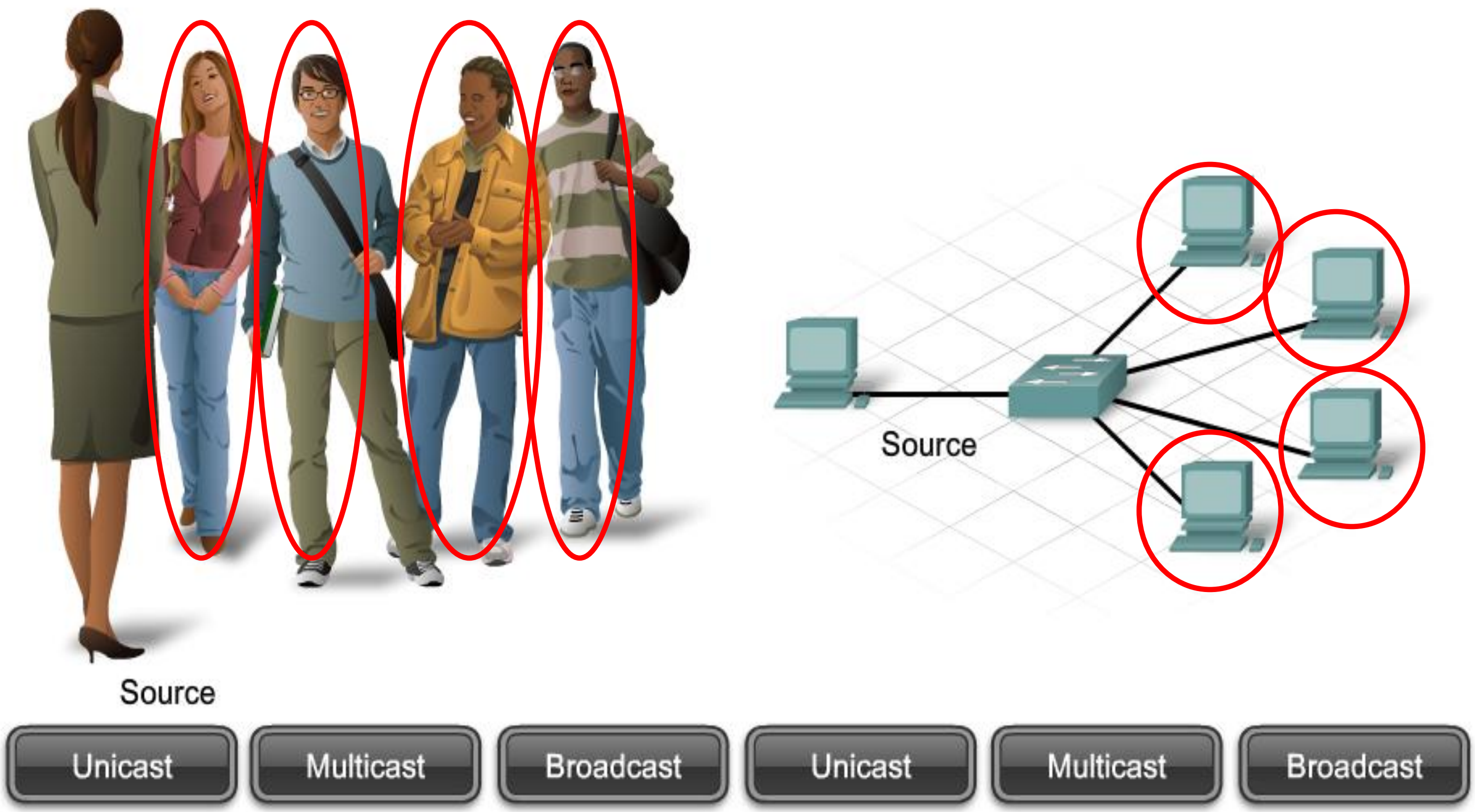
Message Delivery Options - Unicast



Message Delivery Options - Multicast



Message Delivery Options - Broadcast



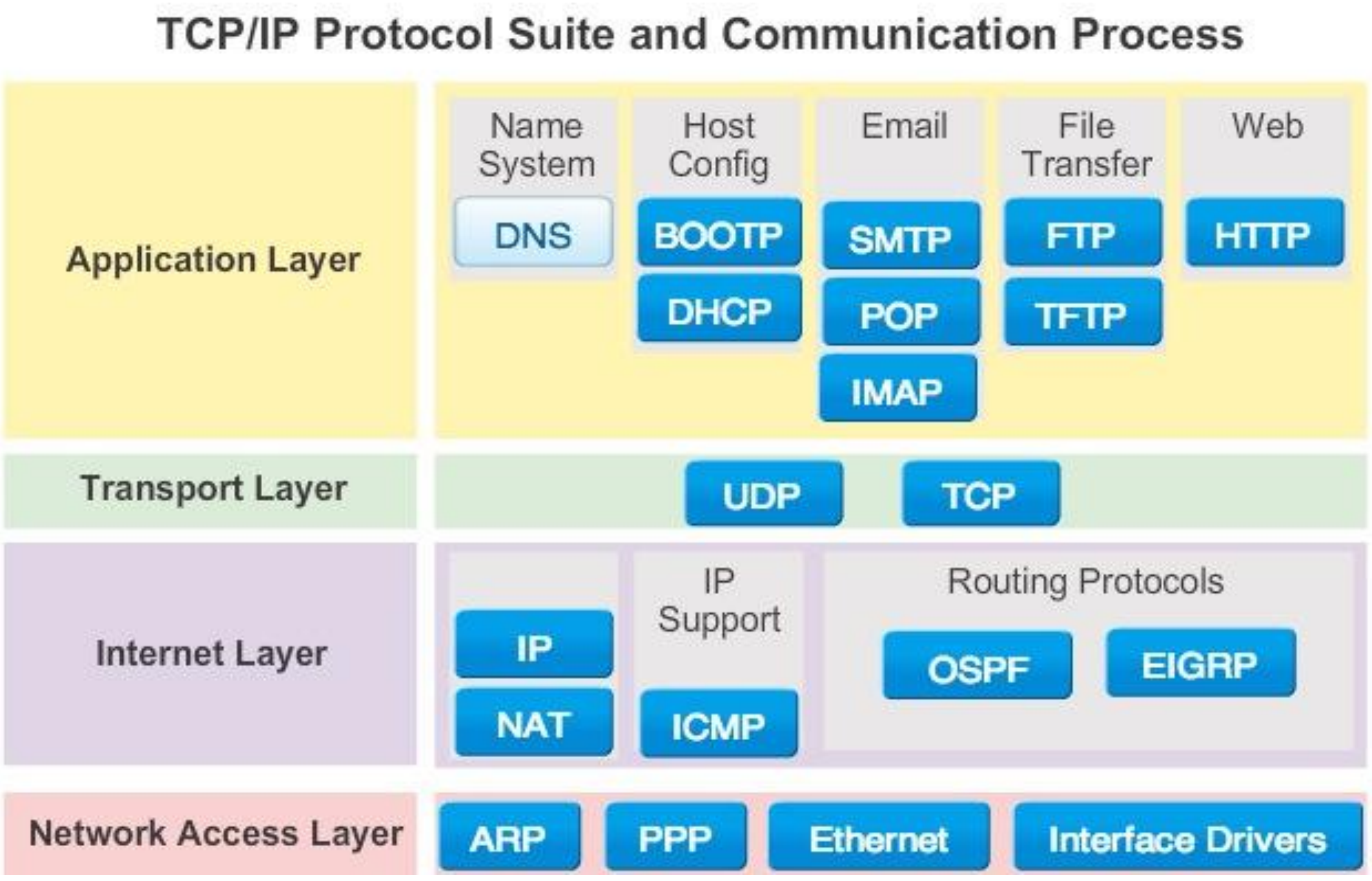
Message Delivery Options - Broadcast

- Unicast
- Multicast
- Broadcast

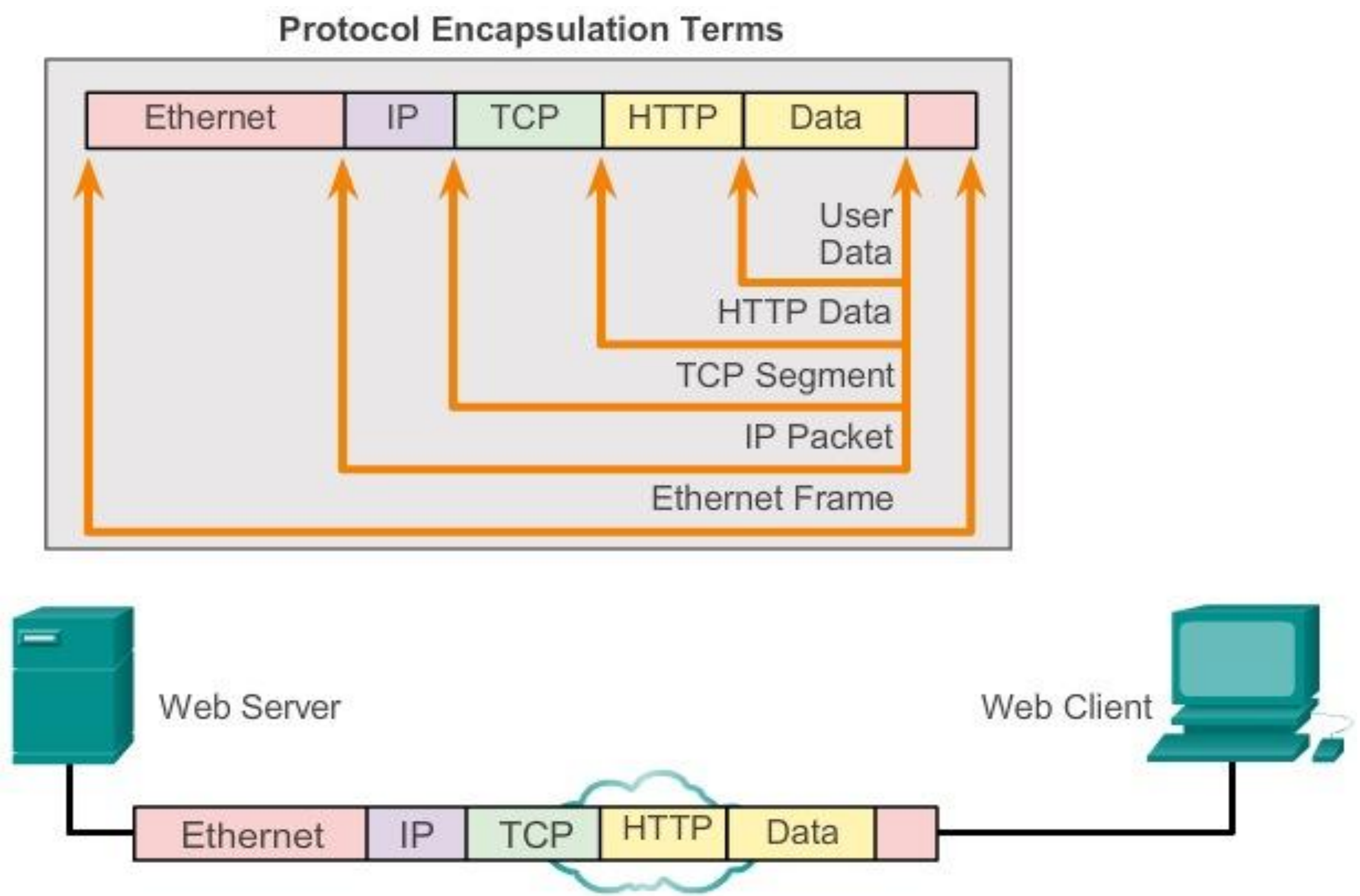
Protocol Suites

TCP/IP Protocol Suites

TCP/IP Protocol Suite



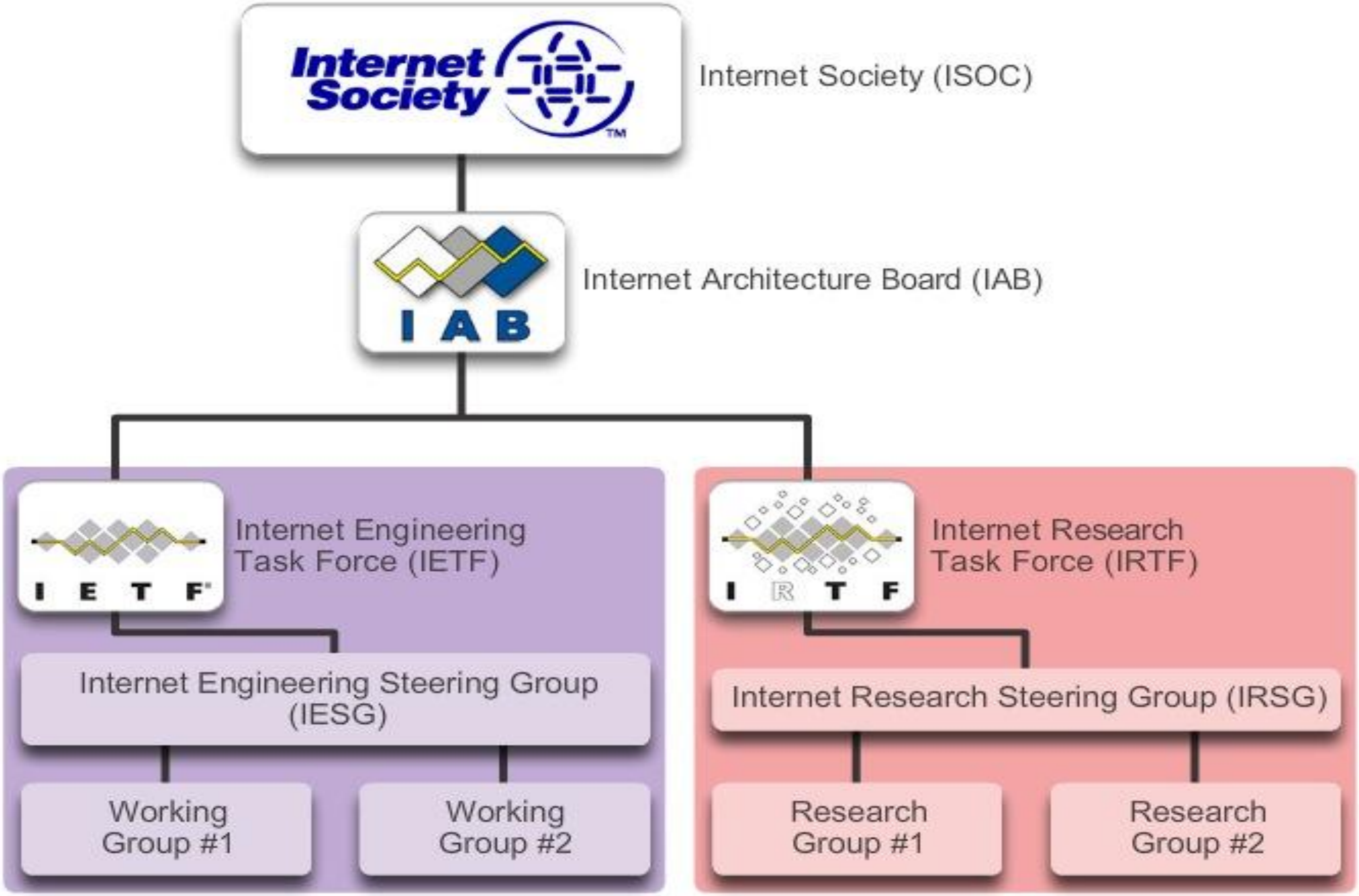
TCP/IP Protocol Suite



Standard Organizations

ISOC
IAB
IETF
IEEE
ISO

ISOC, IAB, IETF, & IRTF



IEEE

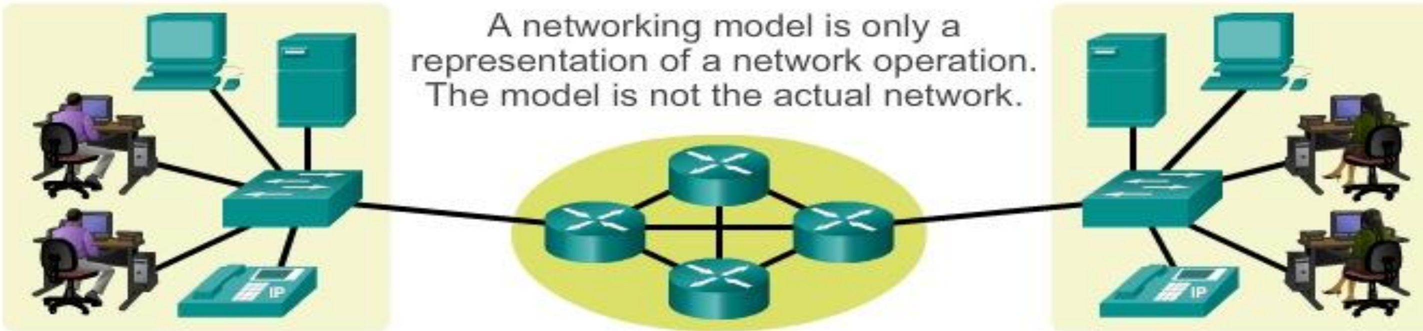
IEEE 802 Working Groups and Study Groups

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

Reference Models

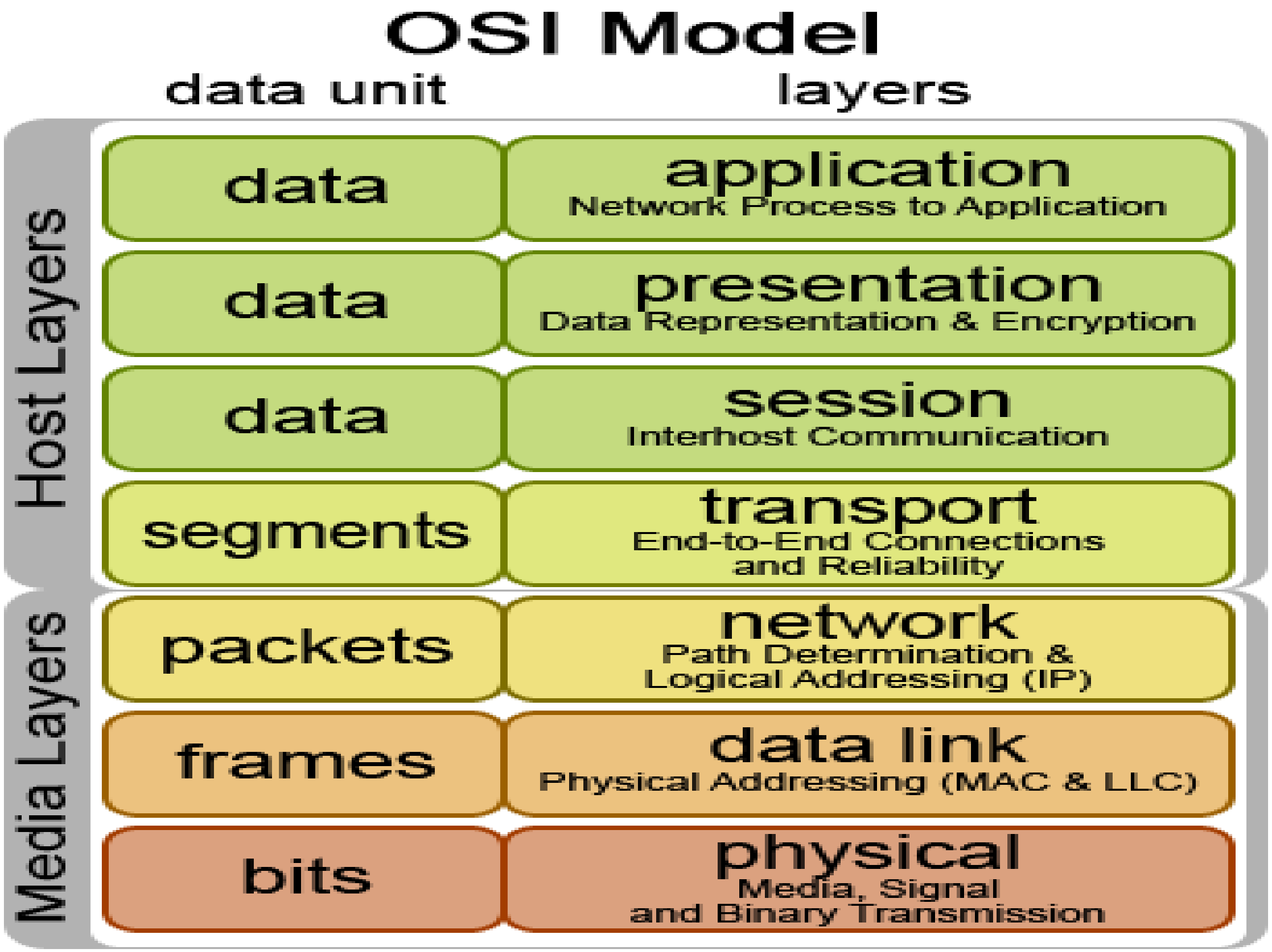
Benefits of Layered Model

Benefits of Layered Model



OSI Model	TCP/IP Protocol Suite	TCP/IP Model
Application	HTTP, DNS, DHCP, FTP	Application
Presentation		
Session		
Transport	TCP, UDP	Transport
Network	IPv4, IPv6, ICMPv4, ICMPv6	Internet
Data Link	PPP, Frame Relay, Ethernet	Network Access
Physical		

OSI Model


OSI Model
data unit
layers
Host Layers
Media Layers
data
application
Network Process to Application
data
presentation
Data Representation & Encryption
data
session
Interhost Communication
segments
transport
End-to-End Connections
and Reliability
packets
network
Path Determination &
Logical Addressing (IP)
frames
data link
Physical Addressing (MAC & LLC)
bits
physical
Media, Signal
and Binary Transmission

TCP/IP Model

TCP/IP Model

Application	Represents data to the user, plus encoding and dialog control.
Transport	Supports communication between diverse devices across diverse networks.
Internet	Determines the best path through the network.
Network Access	Controls the hardware devices and media that make up the network.

Internetwork Operating System (IOS)

Cisco IOS

Cisco IOS

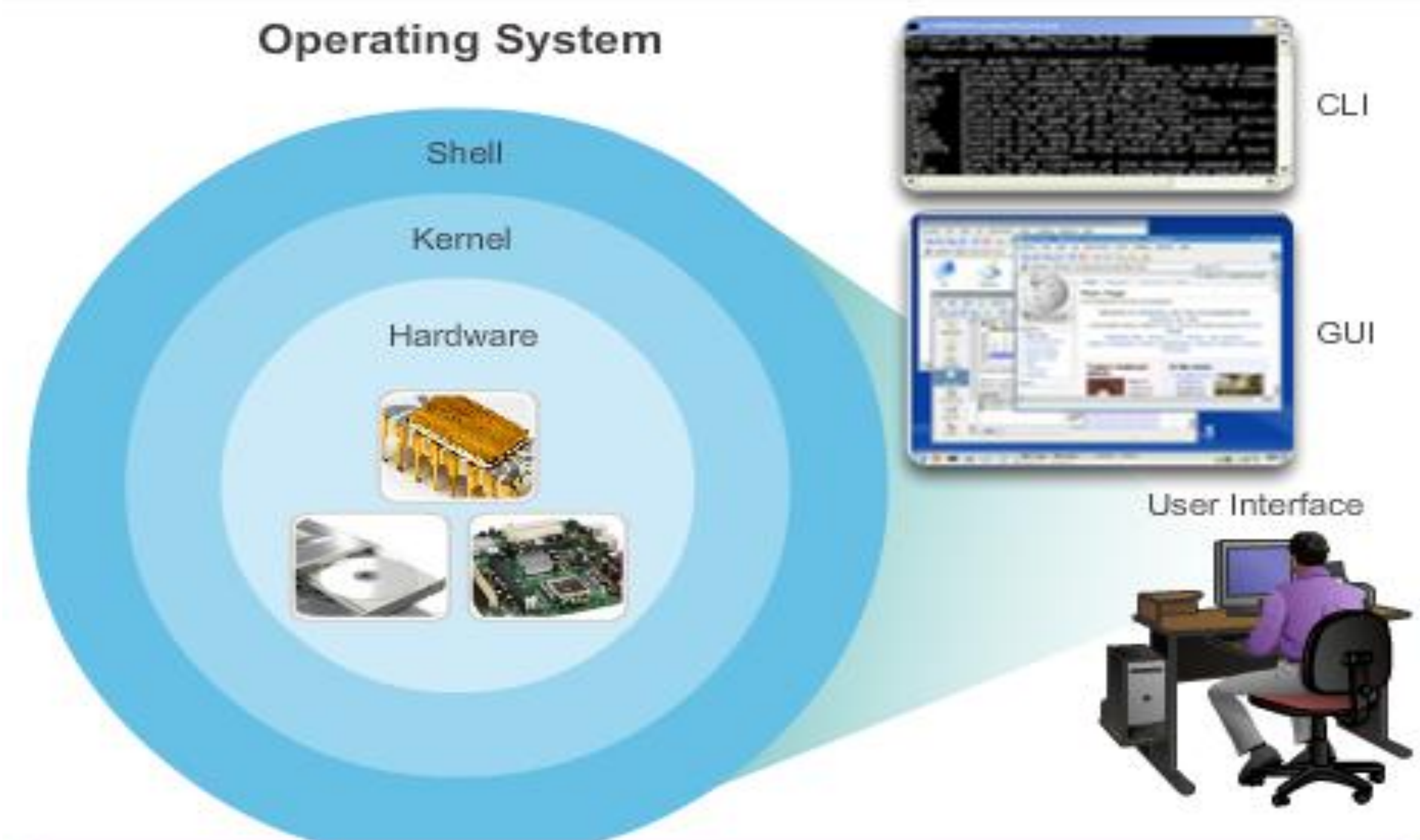
- All networking equipment depend on operating systems:

-End users
-Switches
-Routers
-Wireless access points
-Firewalls

Cisco Internetwork Operating System (IOS)

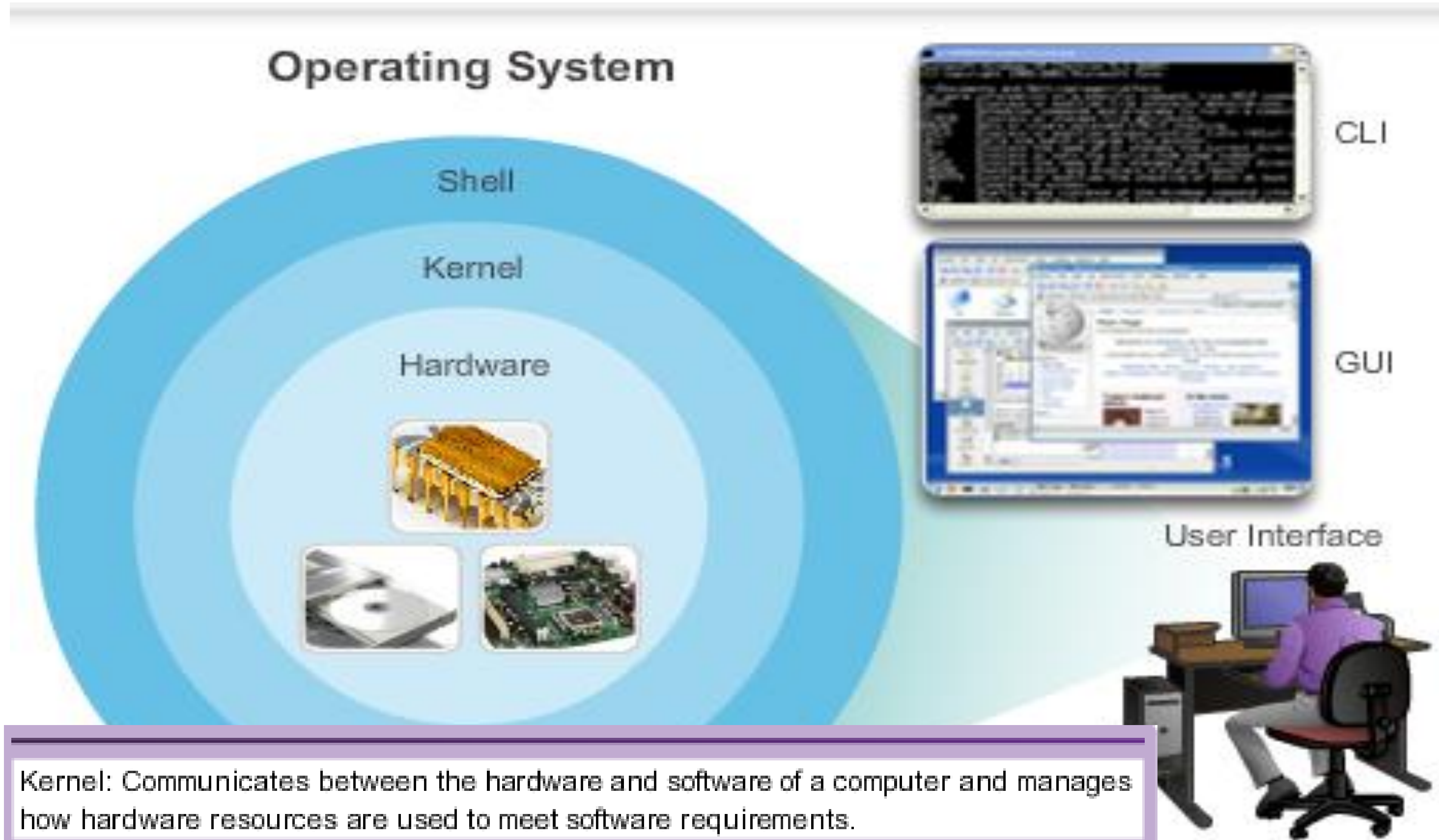
- Collection of network operating systems used on Cisco devices

Operating System



Shell: The user interface that allows users to request specific tasks from the computer. These requests can be made either through the CLI or GUI interfaces.

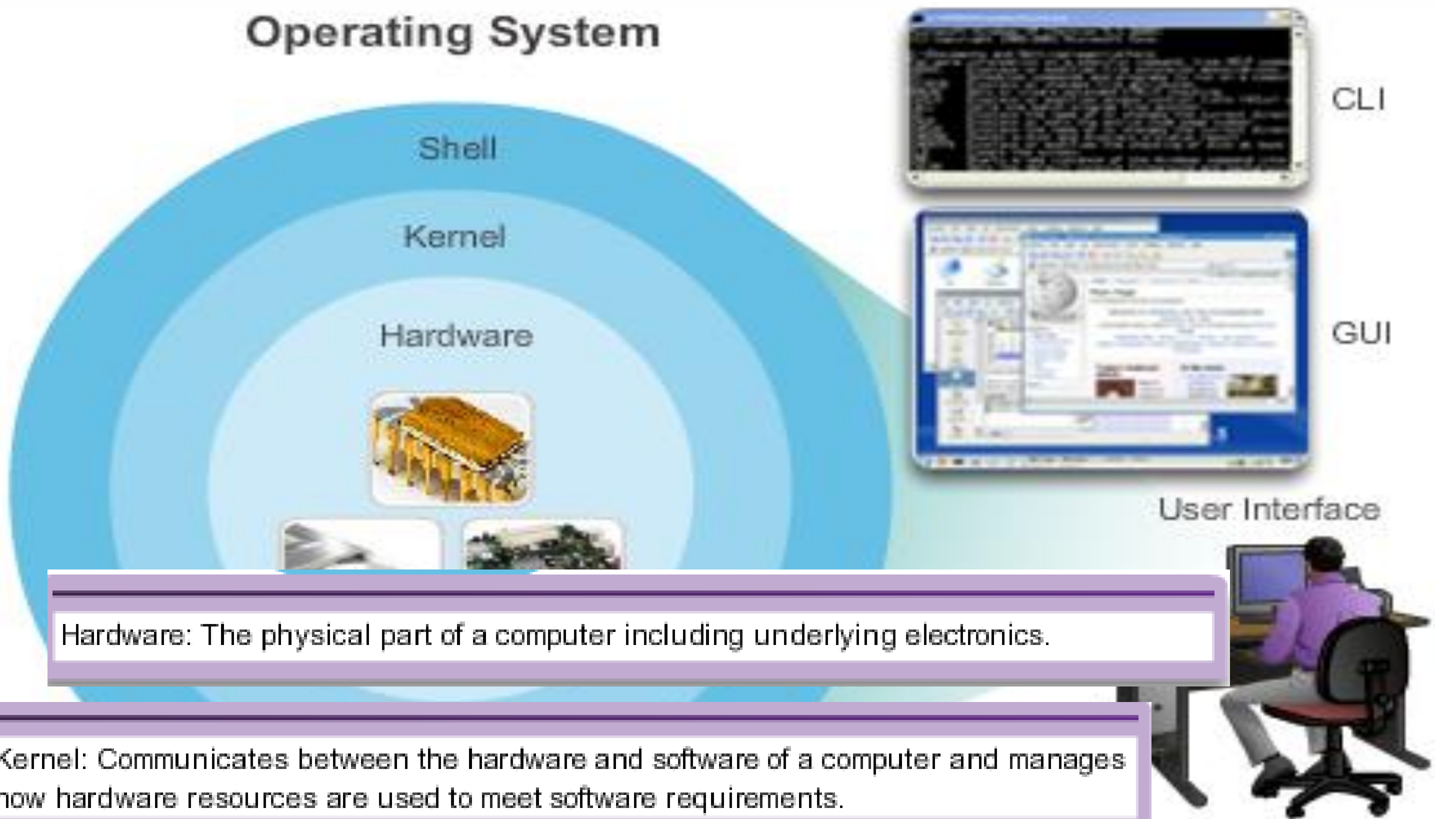
Operating System



Kernel: Communicates between the hardware and software of a computer and manages how hardware resources are used to meet software requirements.

Shell: The user interface that allows users to request specific tasks from the computer. These requests can be made either through the CLI or GUI interfaces.

Operating System



Hardware: The physical part of a computer including underlying electronics.

Kernel: Communicates between the hardware and software of a computer and manages how hardware resources are used to meet software requirements.

Shell: The user interface that allows users to request specific tasks from the computer. These requests can be made either through the CLI or GUI interfaces.

IOS Functions

Accessing an IOS Device

Console Access Methods

Console Access Methods

- Most common methods to access the Command Line Interface
  - Console
  - Telnet or SSH
  - AUX port

Console Port

- Device is accessible even **if no networking services** have been configured
- Need a special console cable (aka **rollover cable**)
- Allows configuration commands to be entered
- Should be configured with **passwords** to prevent unauthorized access
- Device should be **located in a secure room** so console port can not be easily accessed

Telnet, SSH, and AUX Methods

Telnet

- Method for **remotely accessing the CLI** over a network
- **Require active networking services** and one active interface that is configured

Secure Shell (SSH) – Preferred over Telnet

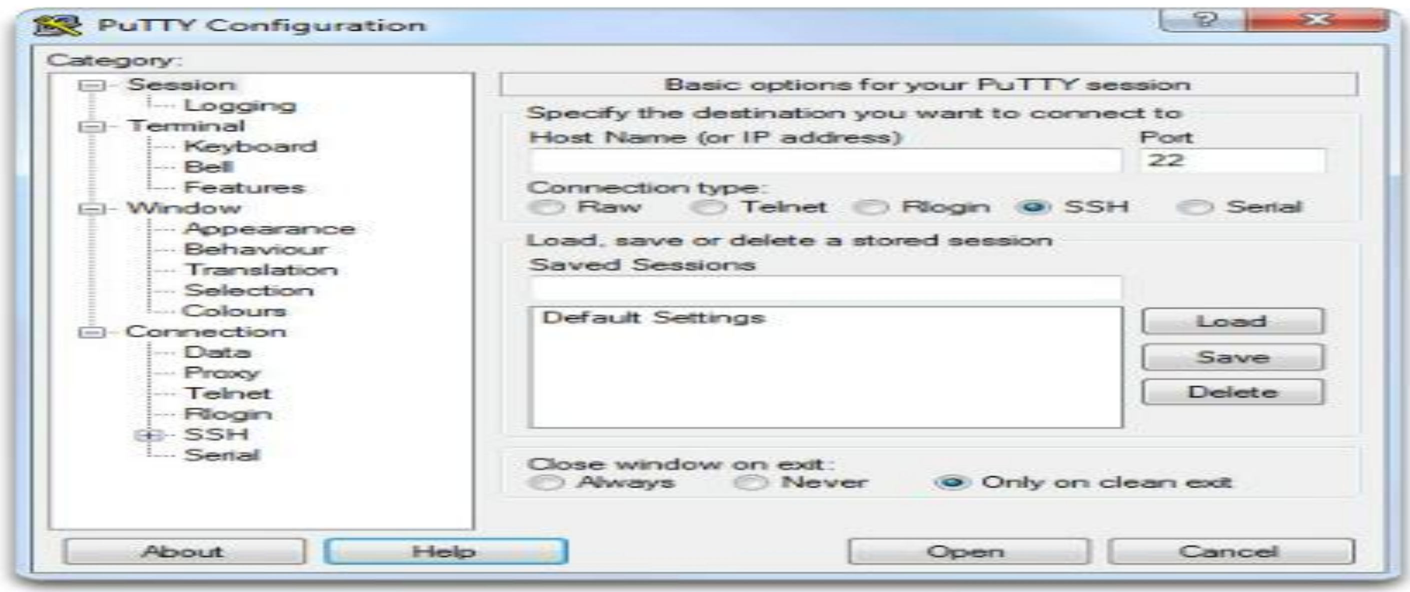
- Remote login similar to Telnet but utilizes **more security**
- Stronger password authentication
- Uses encryption when transporting data

Aux Port (not used too much)

- Out-of-band connection
- Uses telephone line
- Can be used like console port

Terminal Emulation Program

PuTTY



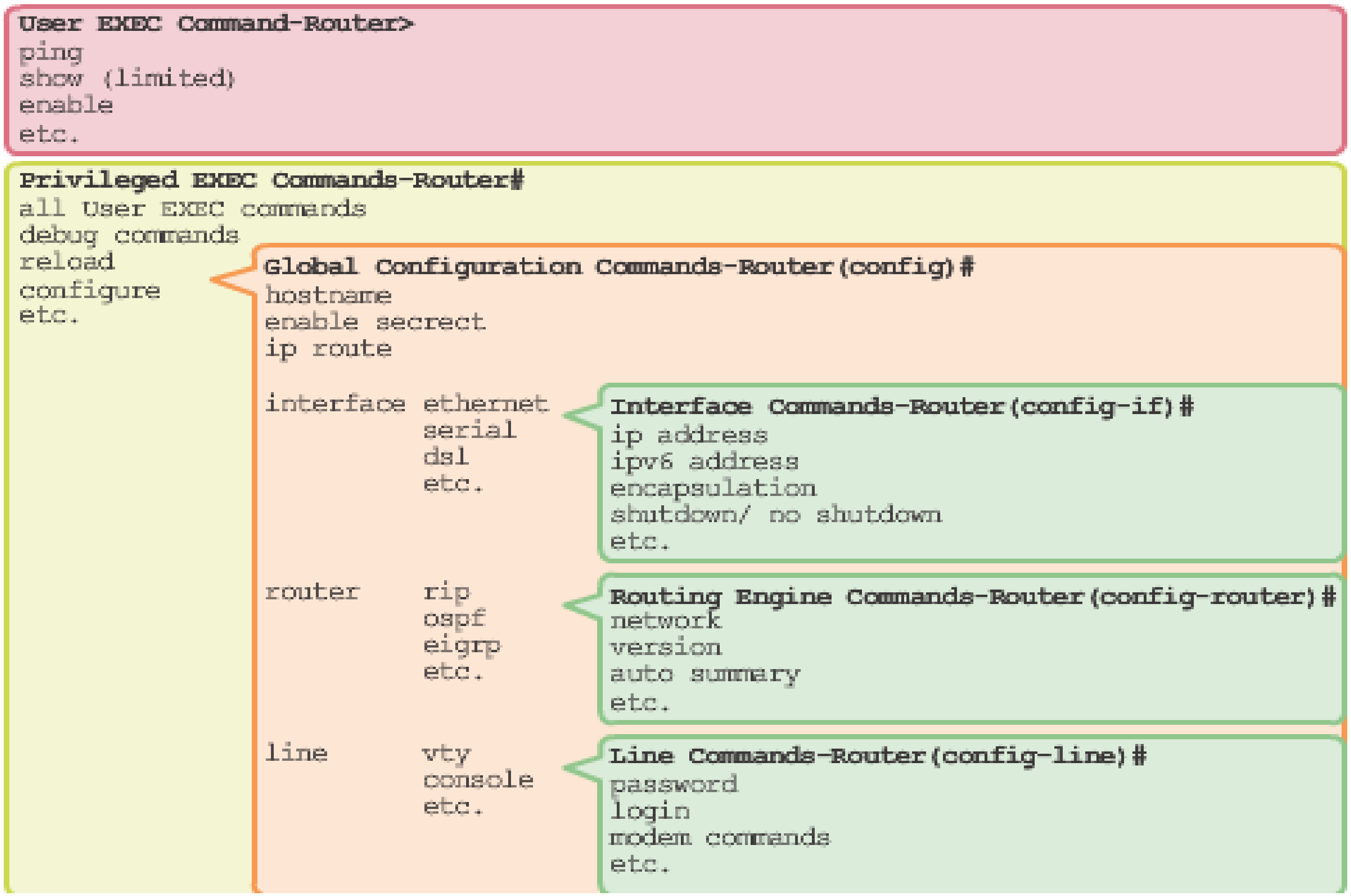
Software available for connecting to a networking device (usually same as terminal/serial/console connection):

- PuTTY
- Tera Term
- HyperTerminal
- OS X Terminal

IOS Modes of Operation

IOS Modes of Operation

IOS Mode Hierarchical Structure



Primary Modes

User EXEC Mode

Limited examination of router.
Remote access.

```
Switch>
Router>
```

The **User EXEC** mode allows only a limited number of basic monitoring commands and is often referred to as view-only mode.

Privileged EXEC Mode

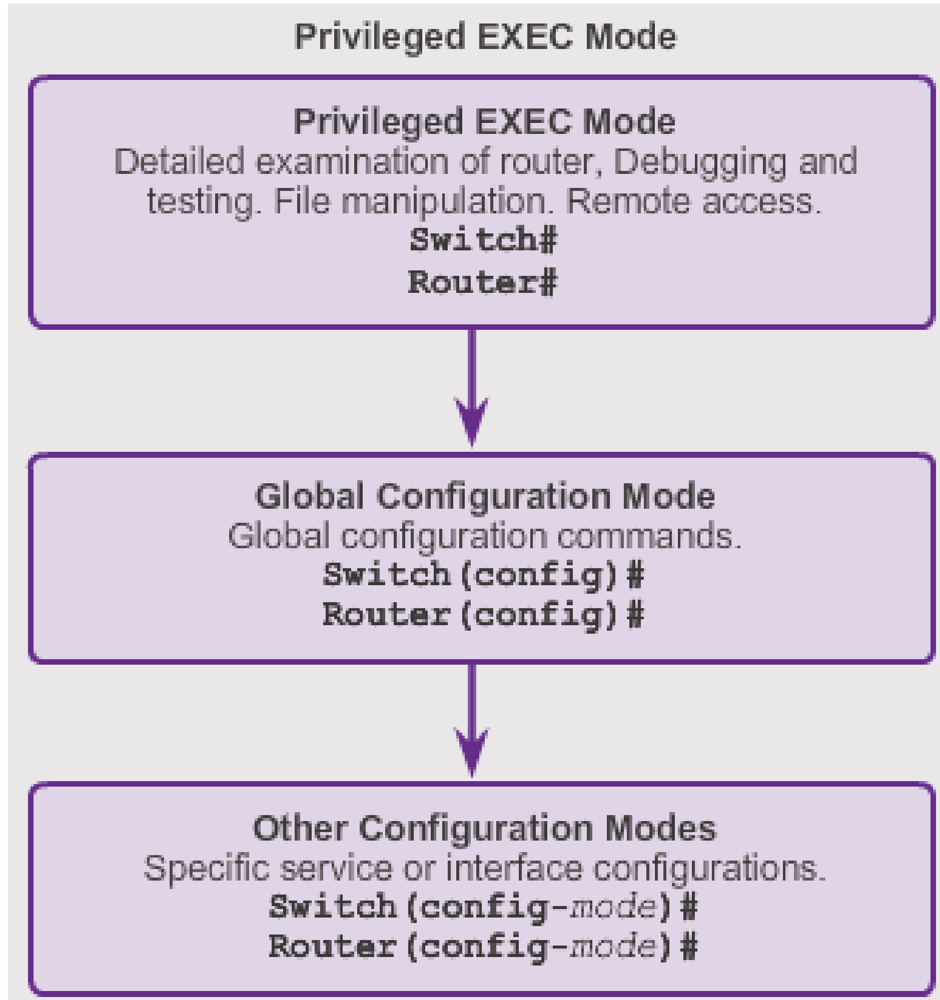
Detailed examination of router.
Debugging and testing. File manipulation.
Remote access.

```
Switch#
Router#
```

The **Privileged EXEC** mode, by default, allows all monitoring commands, as well as execution of configuration and management commands.

Global Configuration Mode and Submodes

Within Privileged EXEC mode, network administrators can access the global configuration mode and all other sub-configuration modes.



Global Configuration Mode and Submodes

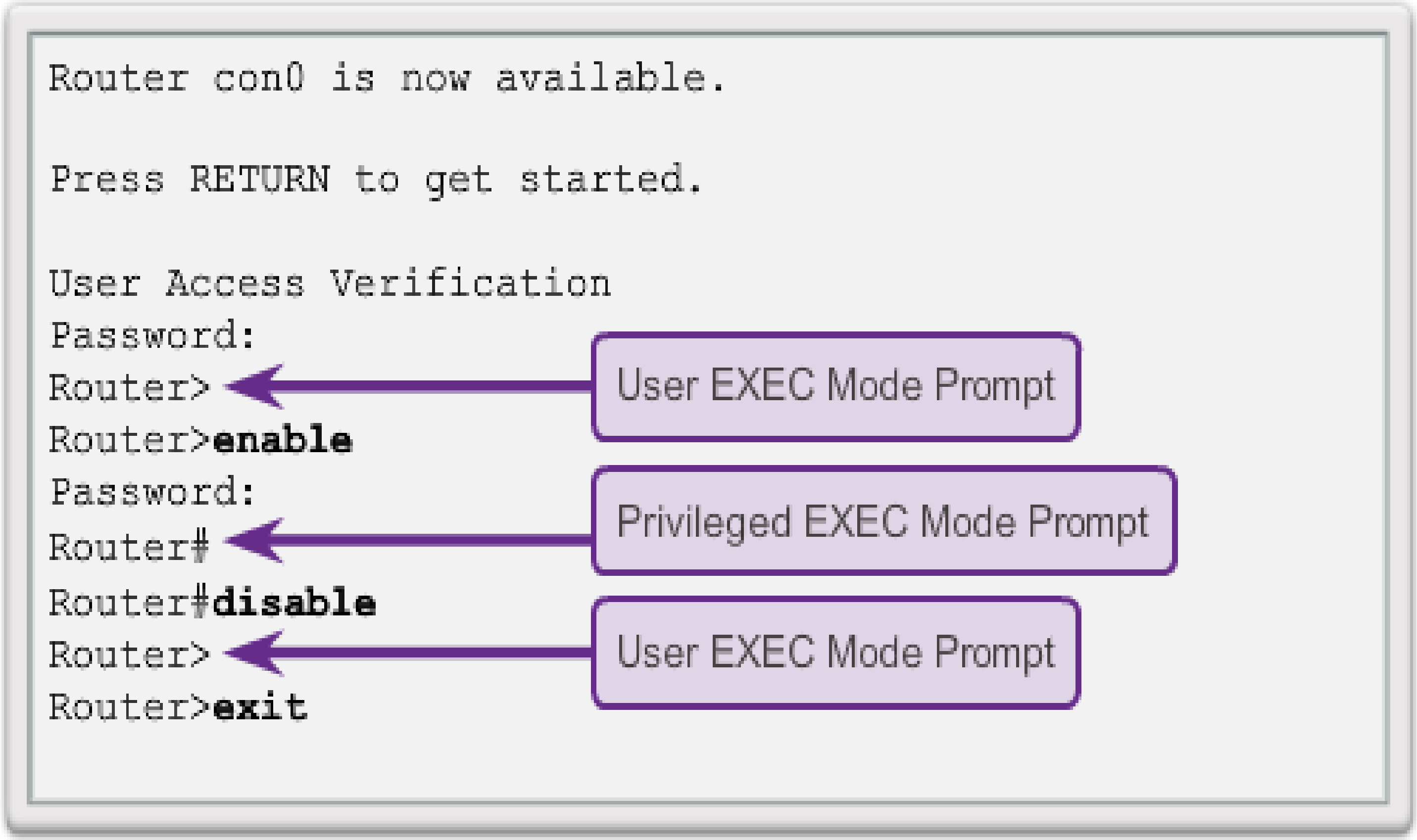
IOS Prompt Structure

```
Router>ping 192.168.10.5

Router#show running-config

Router(config)#Interface FastEthernet 0/0

Router(config-if)#ip address 192.168.10.1 255.255.255.0
```

The prompt changes to denote the current CLI mode.

```
Switch>ping 192.168.10.9

Switch#show running-config

Switch(config)#Interface FastEthernet 0/1

Switch(config-if)#Description connection to WEST LAN4
```

Navigating Between IOS Modes



Router

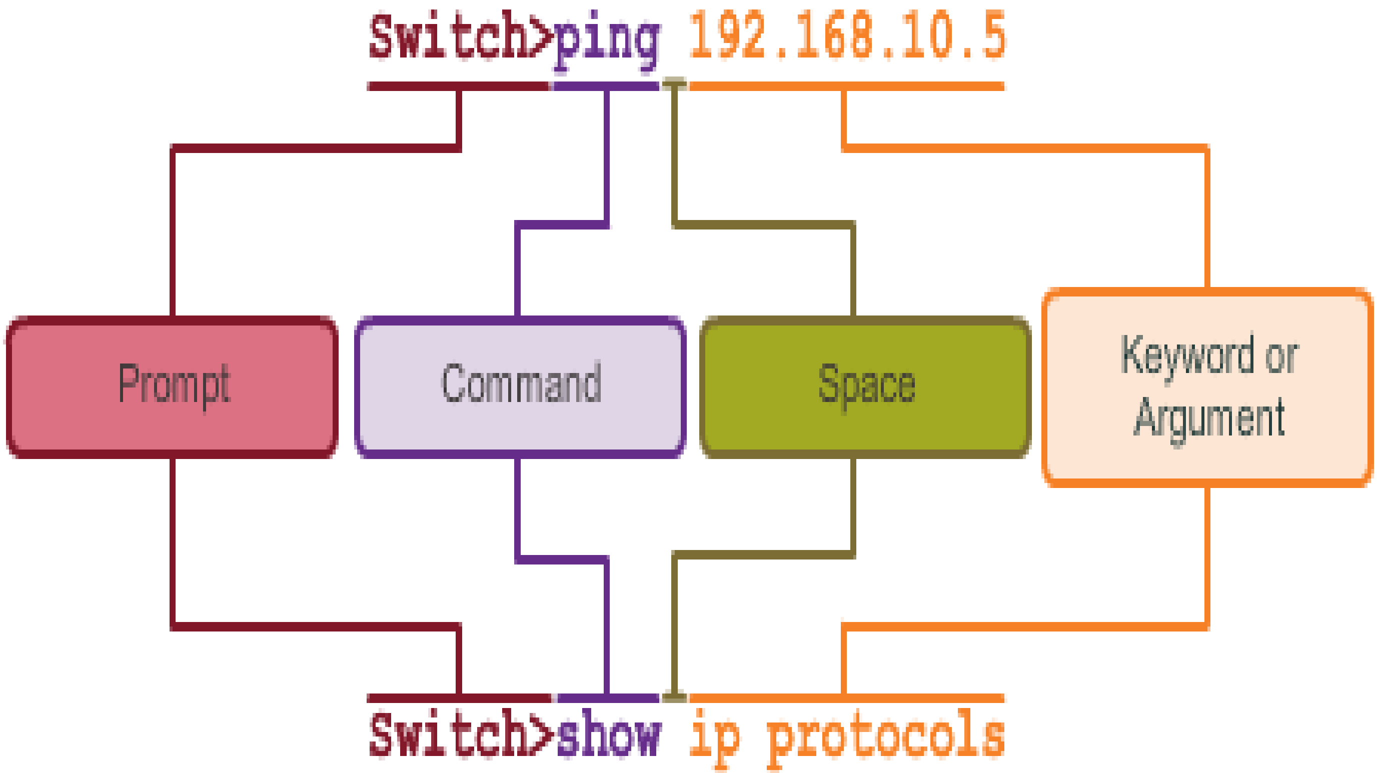
Navigating Between IOS Modes

- User Mode
- Privileged Mode
- Global
- Configuration Mode

The Command Structure

Basic IOS Command Structure

Basic IOS Command Structure



Cisco IOS Command Reference

- For the **ping** command:

  Switch> **ping** *IP-address*

  Switch> **ping 10.10.10.5**

  The command is **ping** and the user defined argument is the **10.10.10.5**.

- Similarly, the syntax for entering the **traceroute** command is:

  Switch> **traceroute** *IP-address*

  Switch> **traceroute 192.168.254.254**

  The command is **traceroute** and the user defined argument is the **192.168.254.254**.

Context-Sensitive Help

Context Sensitive Help

```
Switch#cl?
clear   clock

Switch#clock set ?
  hh:mm:ss   Current Time

Switch#clock set 19:50:00 ?
  <1-31>   Day of the month
  MONTH    Month of the year

Switch#clock set 19:50:00 25 June 2012
Switch#
```

Command options - display a list of commands or keywords that start with the characters **cl**

Command explanation - the IOS displays what command arguments or variables can be next, and provides an explanation of each

Command explanation with more than one argument or variable option

Command Syntax Check

```
Switch#>clock set
% Incomplete command.
Switch#clock set 19:50:00
% Incomplete command.
```

The IOS returns a help message indicating that required keywords or arguments were left off the end of the command.

```
Switch#c
% Ambiguous command:'c'
```

The IOS returns a help message to indicate that there were not enough characters entered for the command interpreter to recognize the command.

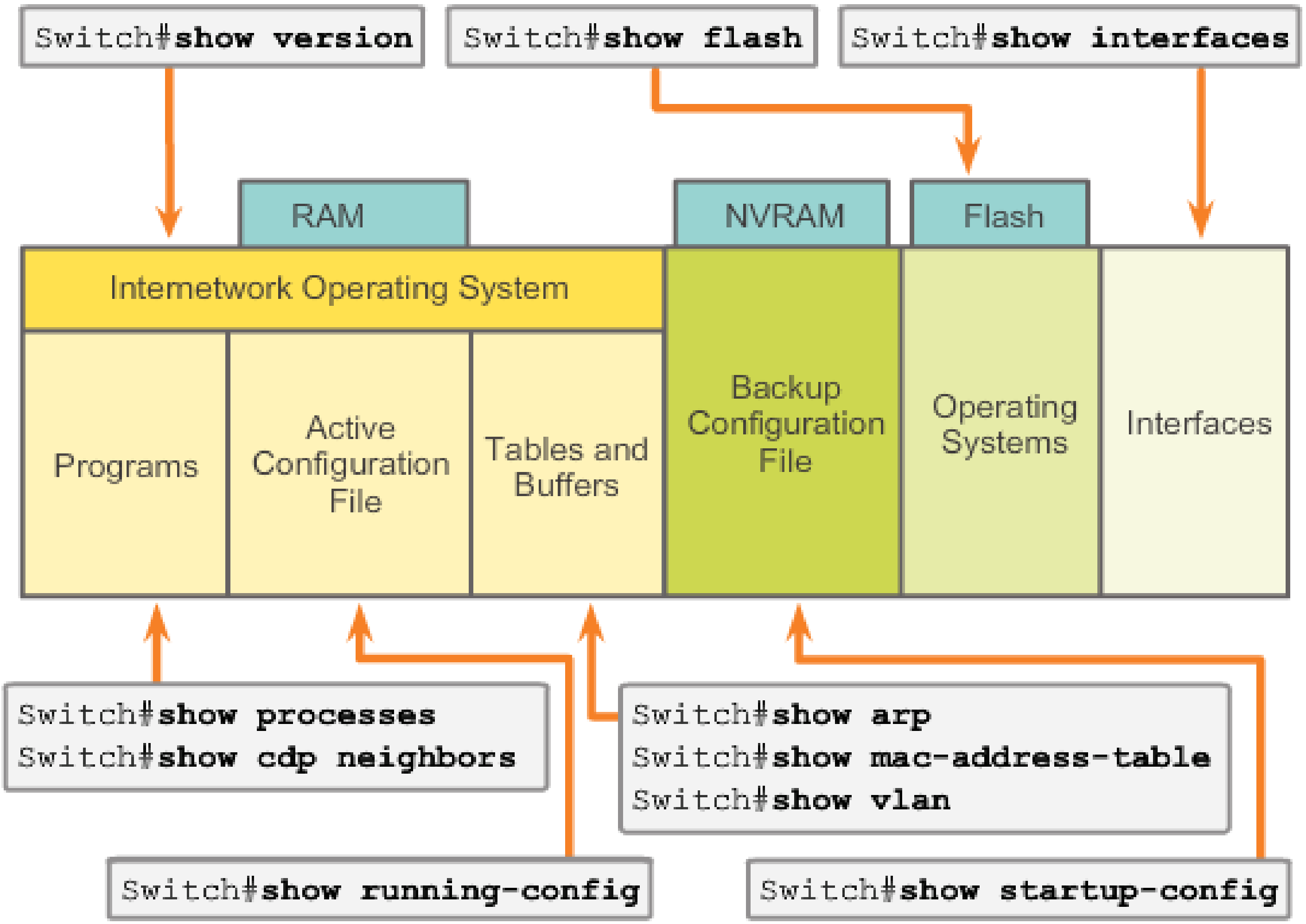
```
Switch#clock set 19:50:00 25 6
                             ^
% Invalid input detected at '^'
marker.
```

The IOS returns a **"^"** to indicate where the command interpreter can not decipher the command.

Hot Keys and Shortcuts

- **Tab** - Completes the remainder of a partially typed command or keyword
- **Ctrl-R** - Redisplays a line
- **Ctrl-A –** Moves cursor to the beginning of the line
- **Ctrl-Z** - Exits configuration mode and returns to user EXEC
- **Down Arrow** - Allows the user to scroll forward through former commands
- **Up Arrow** - Allows the user to scroll backward through former commands
- **Ctrl-Shift-6** - Allows the user to interrupt an IOS process such as **ping** or **traceroute.**
- **Ctrl-C** - Aborts the current command and exits the configuration mode

IOS Examination Commands



The “show version” Command

```
Router#show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version
15.2(4)M1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 26-Jul-12 19:34 by prod_rel_team

ROM: System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)

cisco1941 uptime is 41 minutes
System returned to ROM by power-on
System image file is ""flash0:c1900-universalk9-mz.SPA.152-
4.M1.bin""
Last reload type: Normal Reload
Last reload reason: power-on



This product contains cryptographic features and is subject to
United
States and local country laws governing import, export, transfer
and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use
encryption.
```

```
Router#show version
```

The Command Structure

- IOS Command Structure
- Context-Sensitvie Help
- Command Syntax Check
- Hot Keys and Shortcuts
- IOS Examination Commands

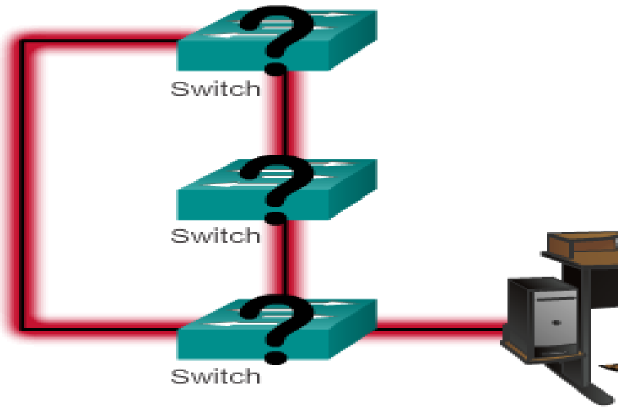
Packet Tracer – Navigating the IOS

Basic Connections
Accessing the CLI
Exploring EXEC Modes
Setting the Clock

Configuring Hostnames

Device
Names

Device Names



Hostnames allow devices to be identified by network administrators over a network or the Internet.

Some guidelines for naming conventions are that names should:

- Start with a letter
- Contain no spaces
- End with a letter or digit
- **Use only letters, digits, and dashes**
- Be less than 64 characters in length

Configuring Hostnames

Configure the switch hostname to be 'Sw-Floor-1'.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# hostname Sw-Floor-1
Sw-Floor-1(config)#
```

You successfully configured the switch hostname.

Limiting Access to Device Configurations

Securing Device Access

Securing Device Access

- Enable Password
- Enable Secret
- Console Password
- VTY Password

Securing Privilege EXEC Access

```
Sw-Floor-1>enable
Sw-Floor-1#
Sw-Floor-1#conf terminal
Sw-Floor-1(config)#enable secret class
Sw-Floor-1(config)#exit
Sw-Floor-1#
Sw-Floor-1#disable
Sw-Floor-1>enable
Password:
Sw-Floor-1#
```

- use the **enable secret** command, not the older **enable** password command
- **enable secret** provides greater security because the password is encrypted

Securing User EXEC Access

```
Sw-Floor-1(config)#line console 0
Sw-Floor-1(config-line)#password cisco
Sw-Floor-1(config-line)#login
Sw-Floor-1(config-line)#exit
Sw-Floor-1(config)#
Sw-Floor-1(config)#line vty 0 15
Sw-Floor-1(config-line)#password cisco
Sw-Floor-1(config-line)#login
Sw-Floor-1(config-line)#
```

- **Console port** must be secured
  - Reduces the chance of unauthorized personnel physically plugging a cable into the device and gaining device access
- **VTY lines** allow access to a Cisco device via Telnet

Securing Device Access

- Enable Password
- Enable Secret
- Console Password
- VTY Password

Packet Tracer – Configuring Initial Switch

Verify Default Switch Configuration

Configure a Basic Switch Configuration

Configure a MOTD Banner

Configure S2

Packet Tracer – Building a Simple Network

Set up the Network Topology
Configure PC Hosts
Configure and Verify Basic Switch Settings

Packet Tracer – Configuring Switch Management Address

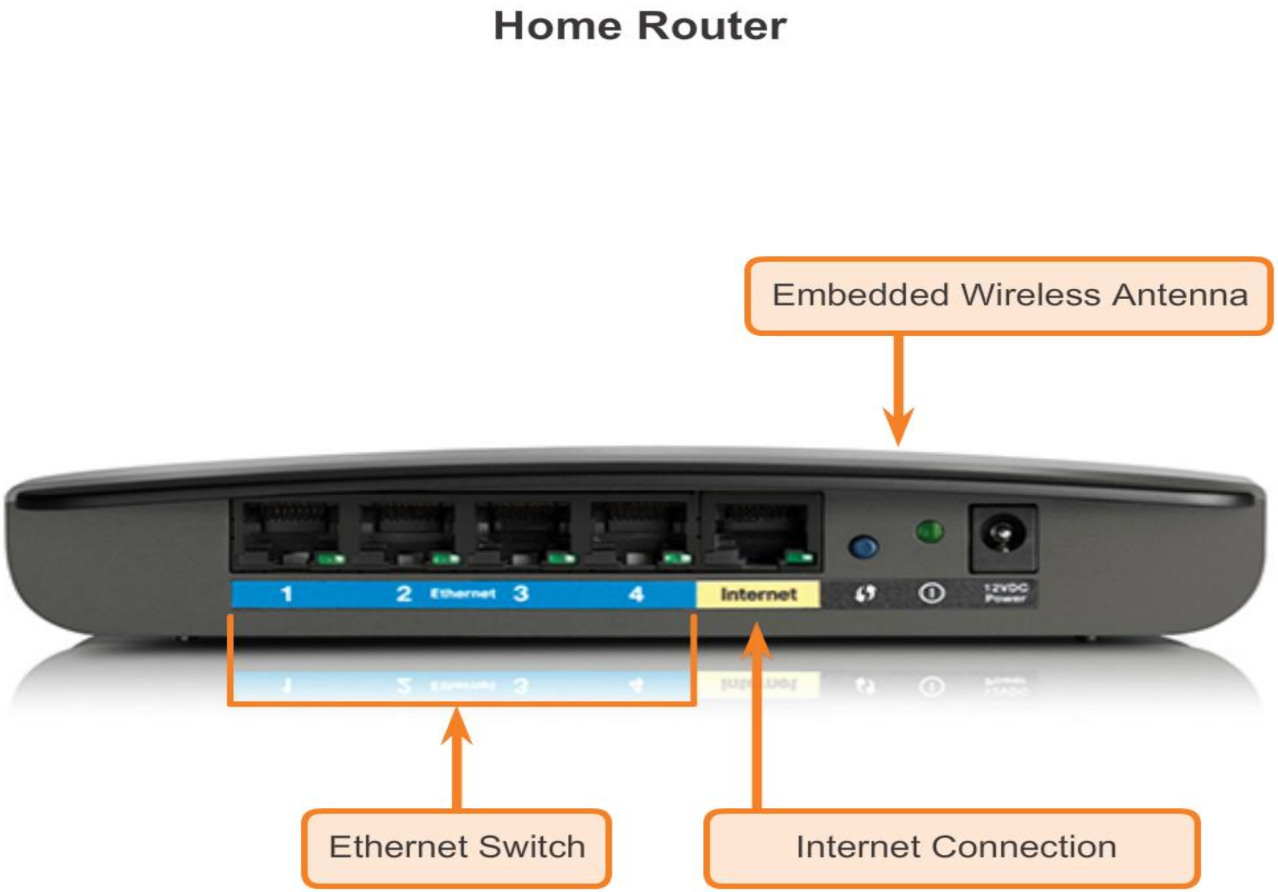
Configure a Basic Network Device

Verify and Test Network Connectivity

Physical Layer Protocols

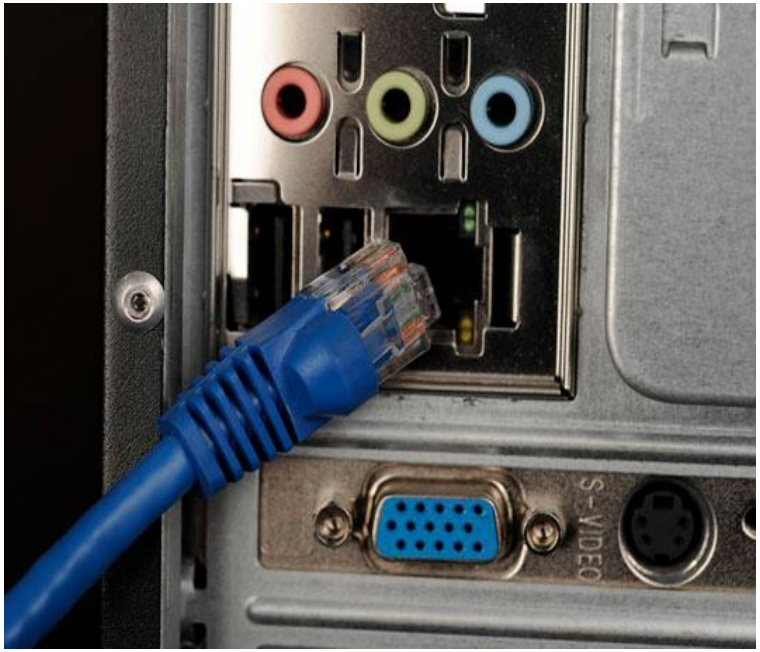
Connecting to the Network

Connecting to the Network



A physical connection can be a wired connection using a cable or a wireless connection using radio waves.

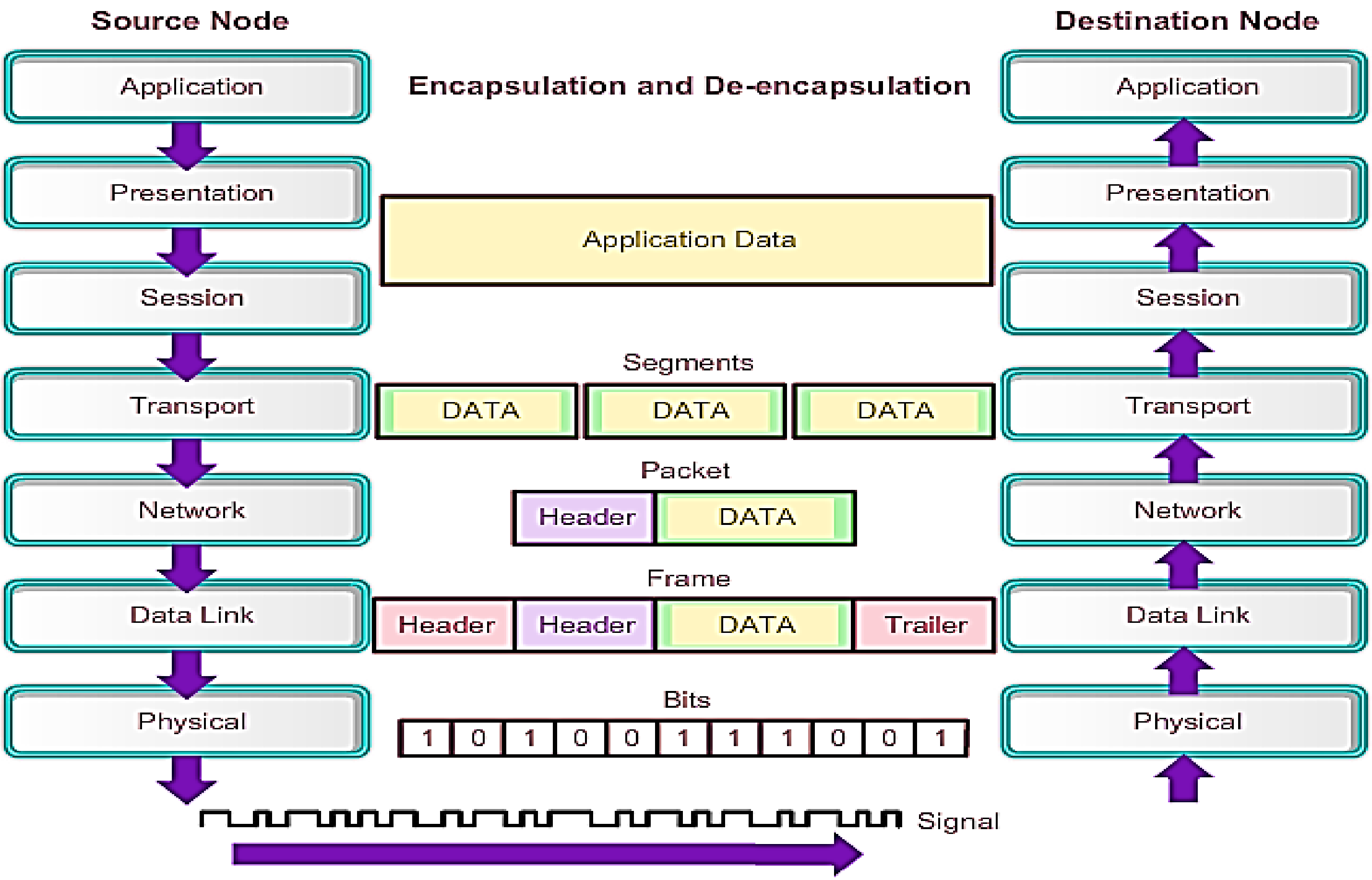
Network Interface Cards



•Network Interface Cards (NICs) connect a device to the network.

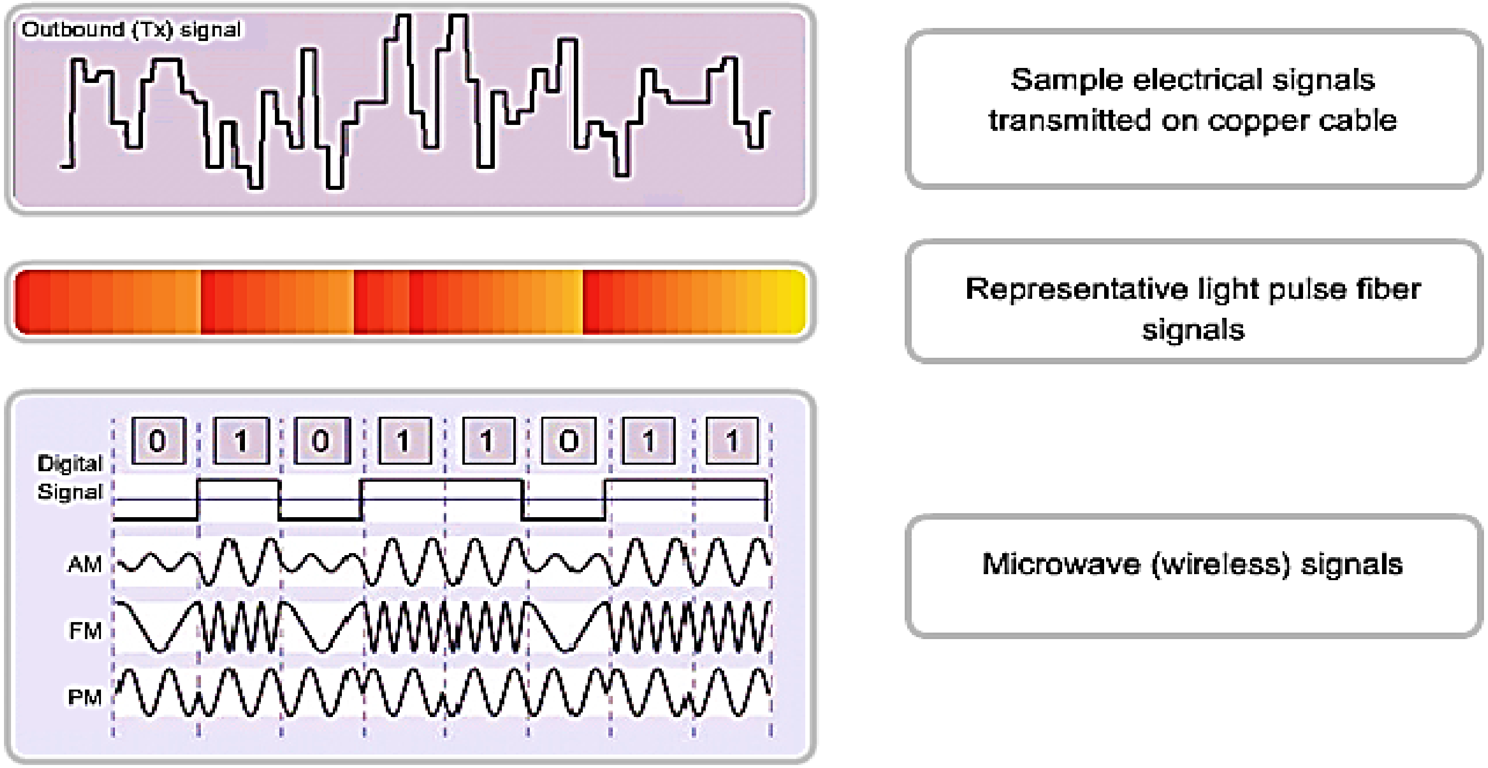
•Ethernet NICs are used for a wired connection whereas WLAN (Wireless Local Area Network) NICs are used for wireless.

Purpose of Physical Layer



The OSI physical layer provides the means to transport the bits that make up a data link layer frame across the network media.

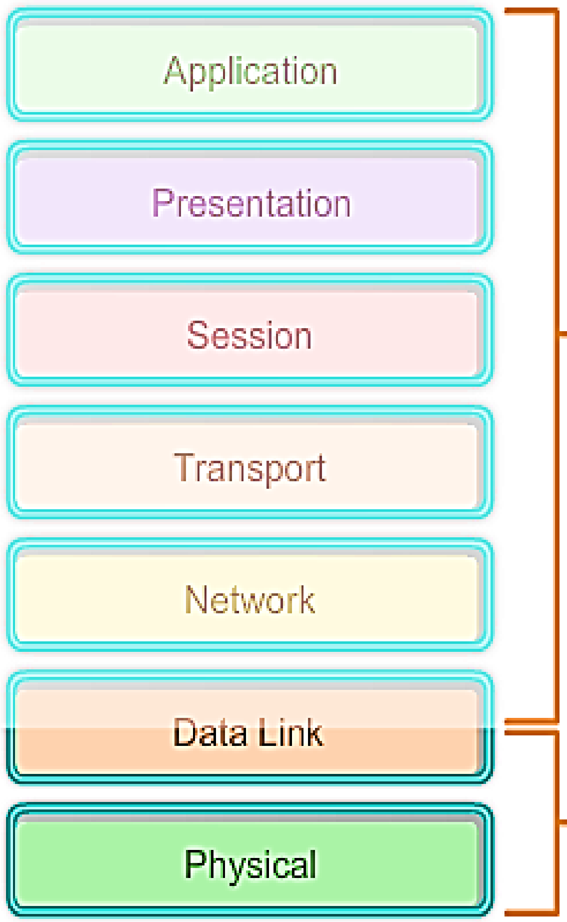
Physical Layer Media



The physical layer produces the representation and groupings of bits for each type of media as:

•**Copper cable**: The signals are patterns of electrical pulses.
•**Fiber-optic cable**: The signals are patterns of light.
•**Wireless**: The signals are patterns of microwave transmissions.

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 Fundamentals

Bandwidth
Throughput

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

Bandwidth is the capacity of a medium to carry data.
Typically measured in kilobits per second (kb/s) or megabits per second (Mb/s).

Throughput

- **Throughput** is the measure of the transfer of bits across the media over a given period of time.
- Due to a number of factors, throughput usually does not match the specified bandwidth in physical layer implementations.
- http://www.speedtest.net/
- http://ipv6-test.com/speedtest/

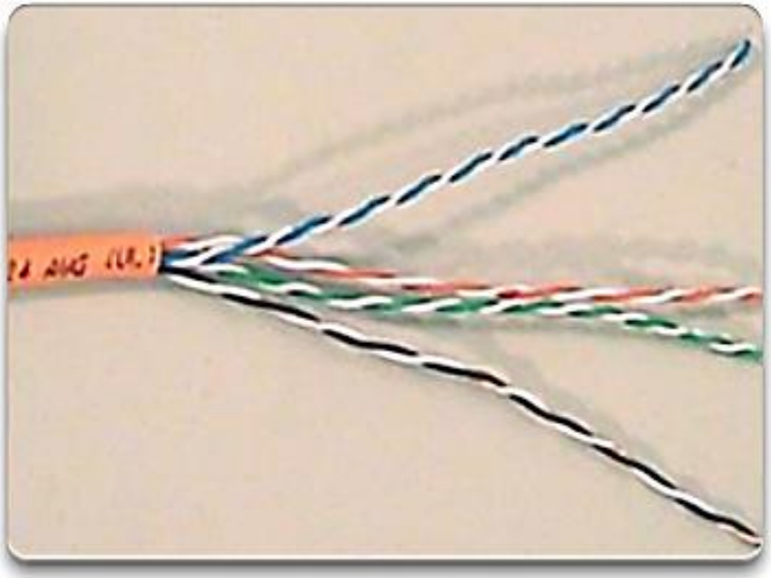
Physical Layer Protocols

NICs
Physical Layer
Media,
Standards,
Fundamentals

Network Media

Copper Cabling
UTP Cabling
Fiber Optic Cabling
Wireless Media

Copper Media

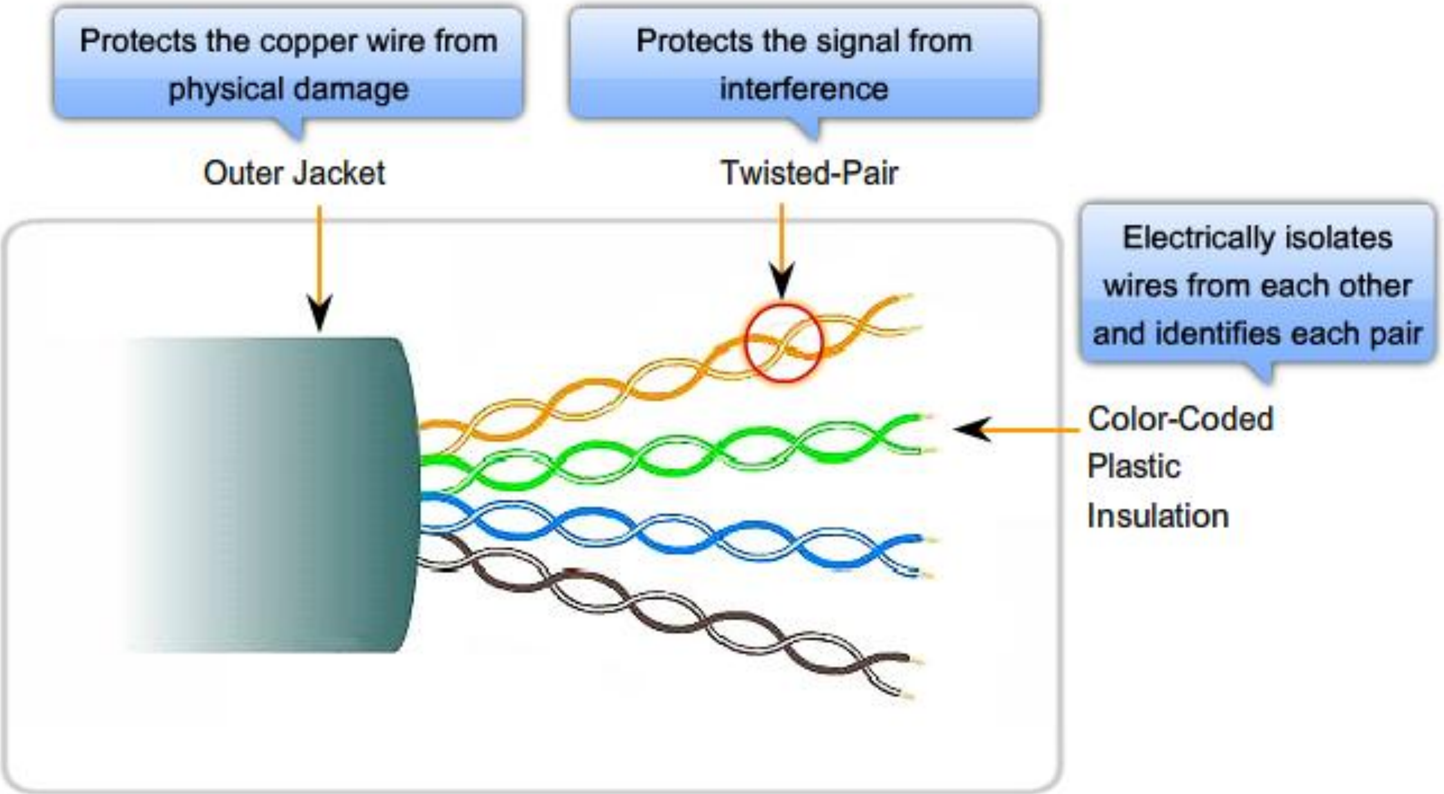


Unshielded Twisted-Pair (UTP) cable

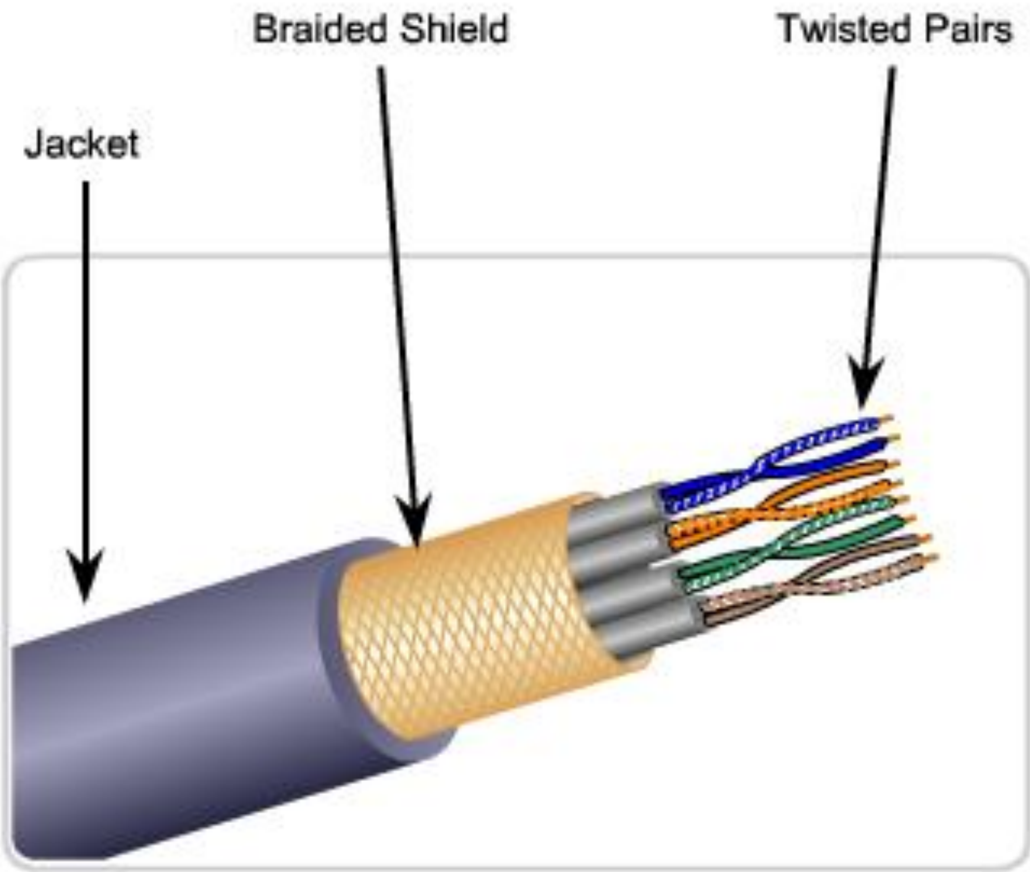
Shielded Twisted-Pair (STP) cable

Coaxial cable

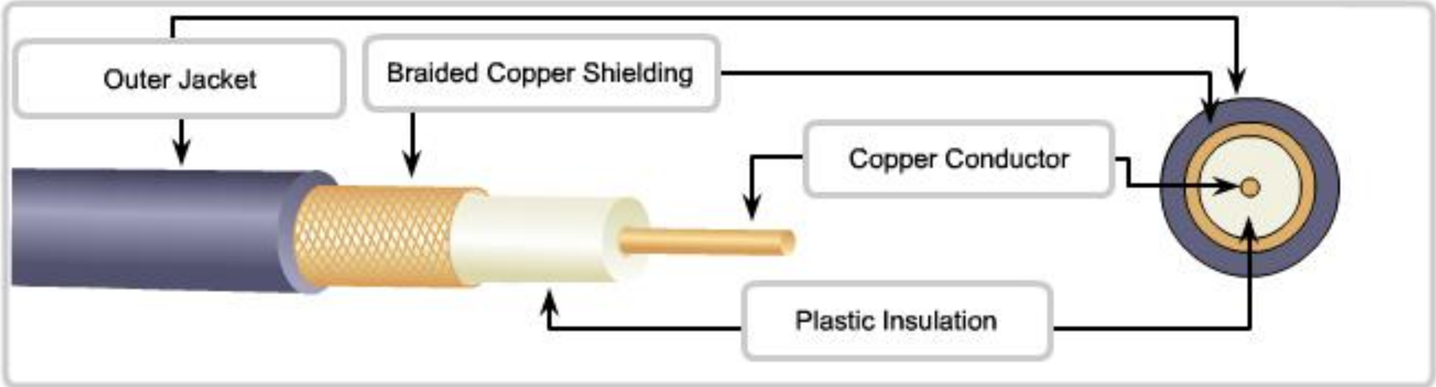
Unshielded Twisted-Pair Cable



Shielded Twisted-Pair Cable



Coaxial Cable

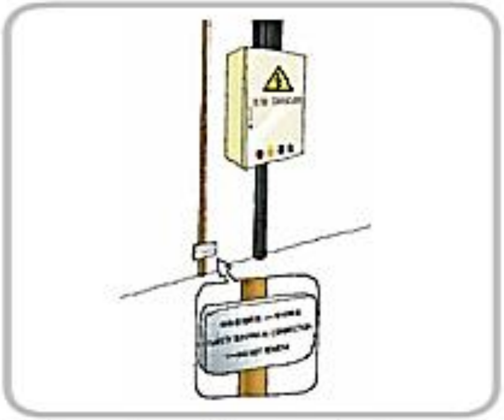


Copper Media Safety

The separation of data and electrical power cabling must comply with safety codes.

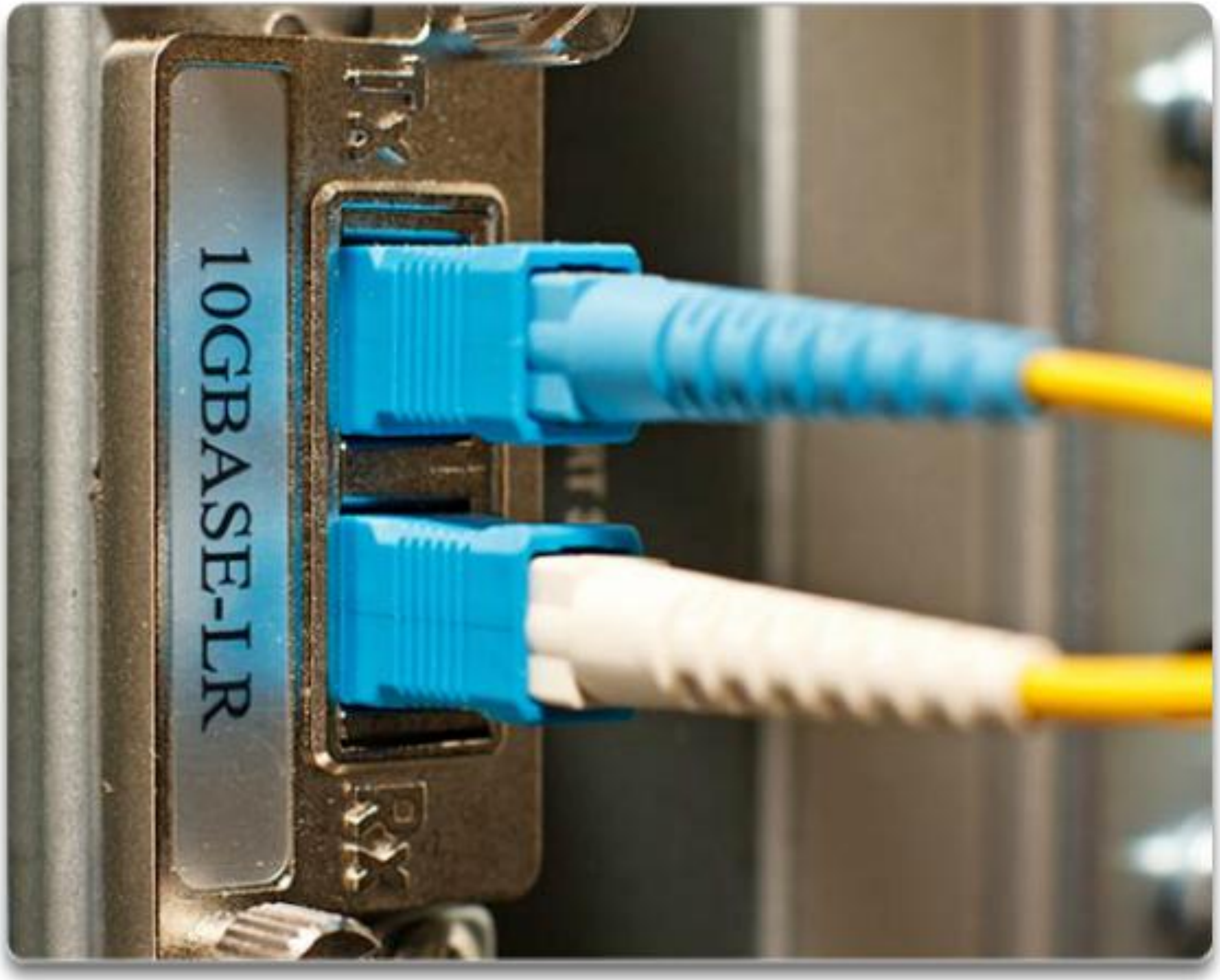
Cables must be connected correctly.

Installations must be inspected for damage.



Equipment must be grounded correctly.

Fiber Optic Cabling



Fiber vs. Copper

Implementation issues	Copper media	Fibre-optic
Bandwidth supported	10 Mbps – 10 Gbps	10 Mbps – 100 Gbps
Distance	Relatively short (1 – 100 meters)	Relatively High (1 – 100,000 meters)
Immunity to EMI and RFI	Low	High (Completely immune)
Immunity to electrical hazards	Low	High (Completely immune)
Media and connector costs	Lowest	Highest
Installation skills required	Lowest	Highest
Safety precautions	Lowest	Highest

Wireless Media

- IEEE 802.11 standards
- Commonly referred to as Wi-Fi
- Uses CSMA/CA
- Variations include:
  - 802.11a: 54 Mb/s, 5 GHz
  - 802.11b: 11 Mb/s, 2.4 GHz
  - 802.11g: 54 Mb/s, 2.4 GHz
  - 802.11n: 600 Mb/s, 2.4, and 5 GHz
  - 802.11ac: 1 Gb/s, 5 GHz
  - 802.11ad: 7 Gb/s, 2.4 GHz, 5 GHz, and 60 GHz

- IEEE 802.15 standard
- Supports speeds up to 3 Mb/s
- Provides device pairing over distances from 1 to 100 meters

- IEEE 802.16 standard
- Provides speeds up to 1 Gb/s
- Uses a point-to-multipoint topology to provide wireless broadband access

802.11 Wi-Fi Standards

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

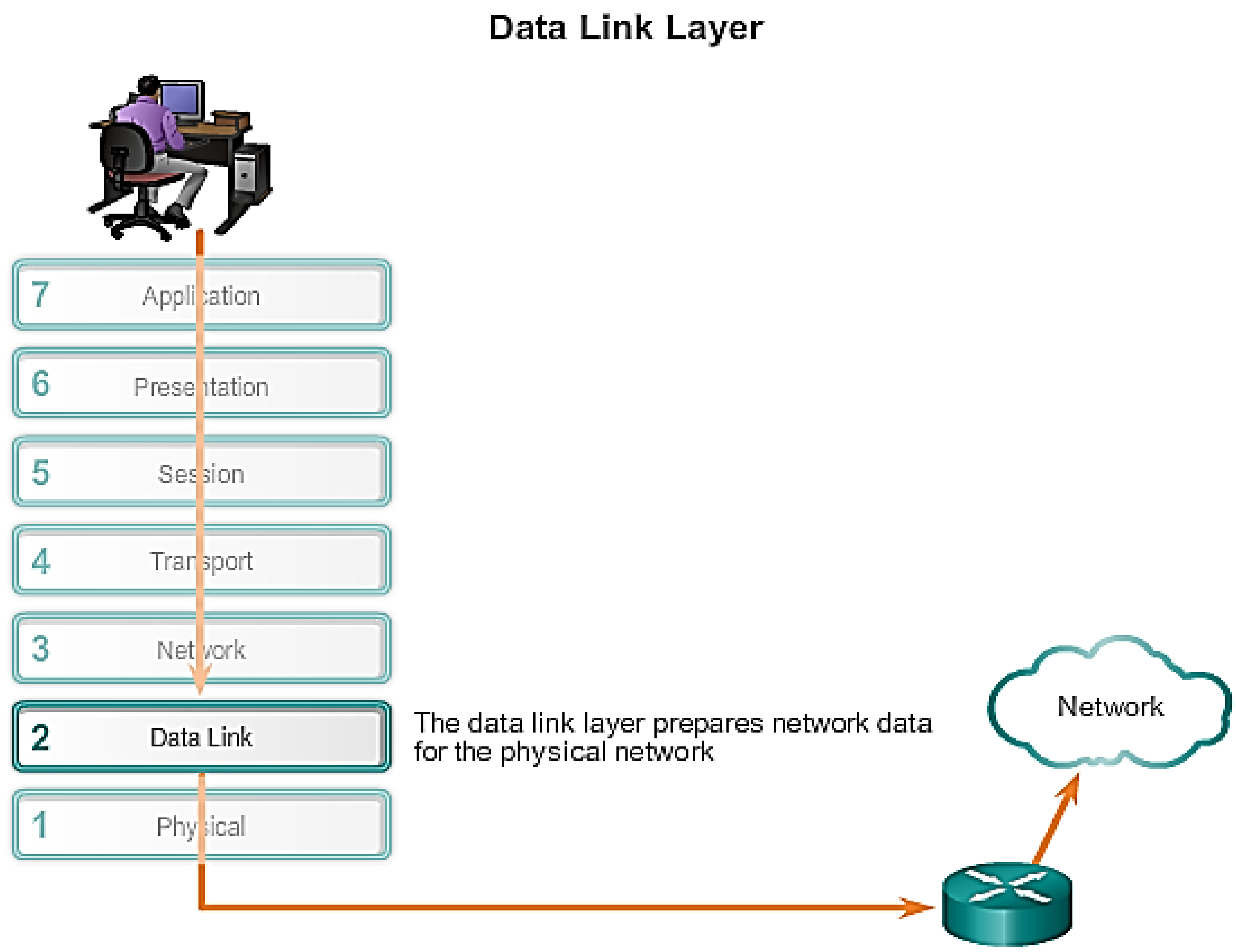
Network Media

Copper Cabling
UTP Cabling
Fiber Optic Calbing
Wireless Media

Data Link Layer Protocols

Purpose of the Data Link Layer

Purpose of the Data Link Layer



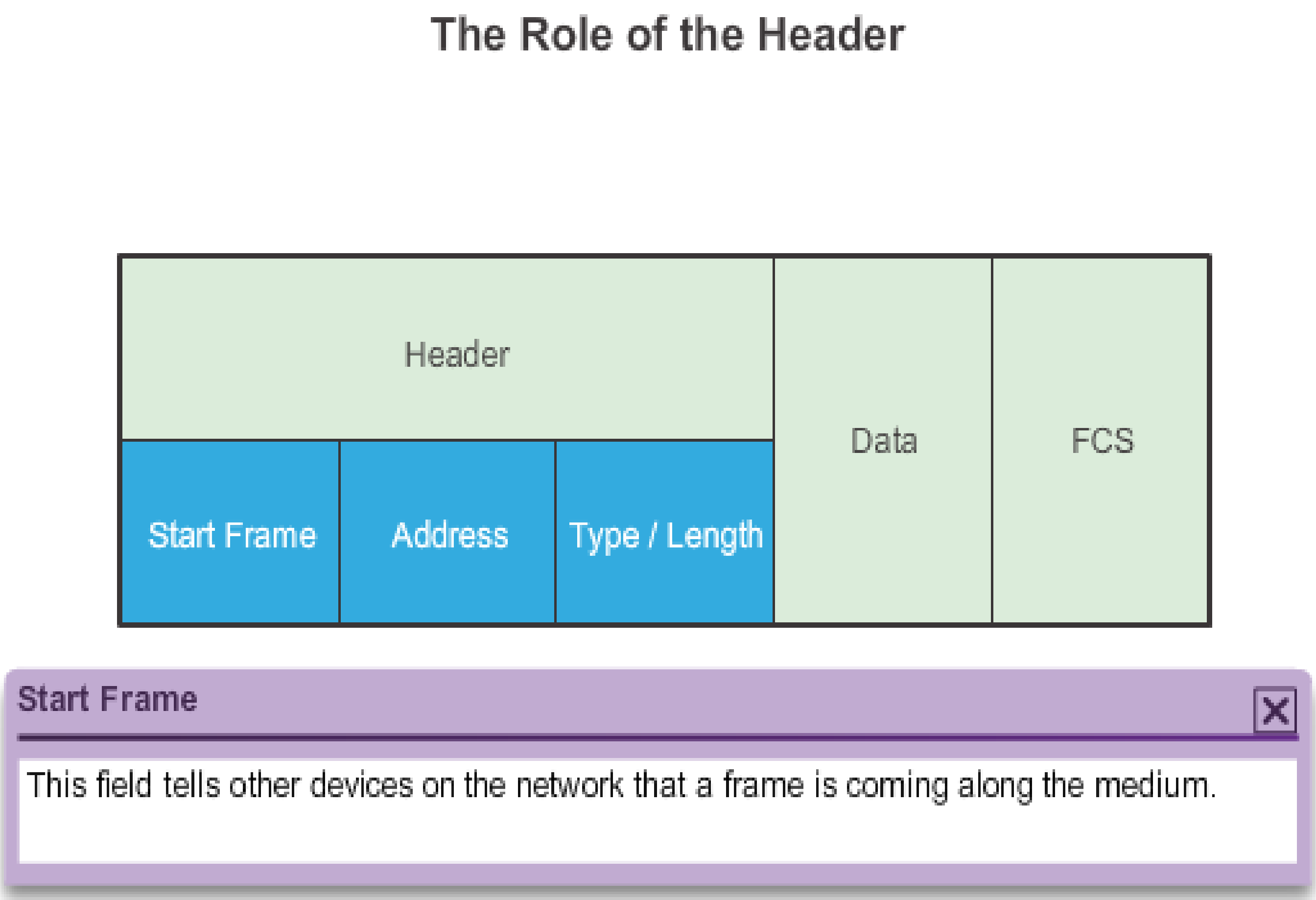
Data Link Sublayers

<table>
<tr><td>Network</td><td></td></tr>
<tr><td rowspan="2">Data Link</td><td>LLC Sublayer</td></tr>
<tr><td>MAC Sublayer</td></tr>
<tr><td>Physical</td><td></td></tr>
</table>

Data Link layer has **two sublayers** (sometimes):

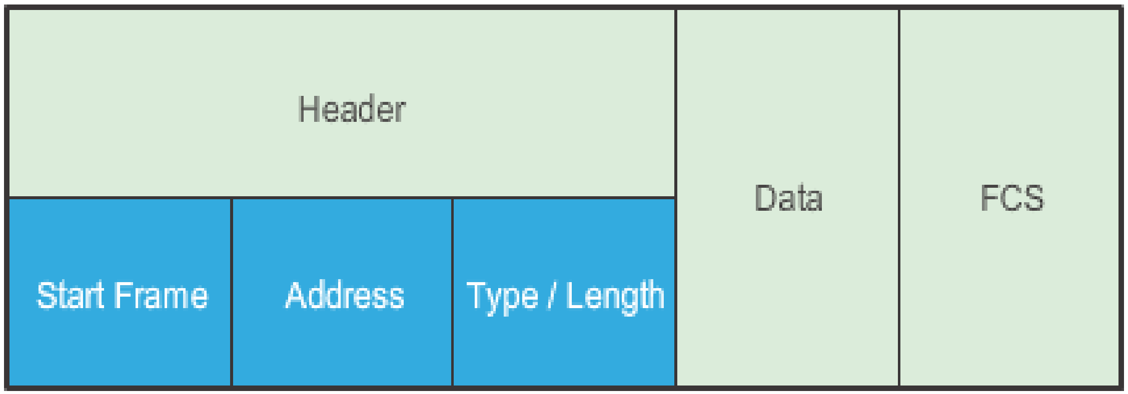
- **Logical Link Control (LLC)** – Software processes that provide services to the Network layer protocols.
- **Media Access Control (MAC)** - Media access processes performed by the hardware.
    - Provides Data Link layer addressing and framing of the data according to the protocol in use.

Data Link Frame Fields - Header



Data Link Frame Fields - Header

The Role of the Header

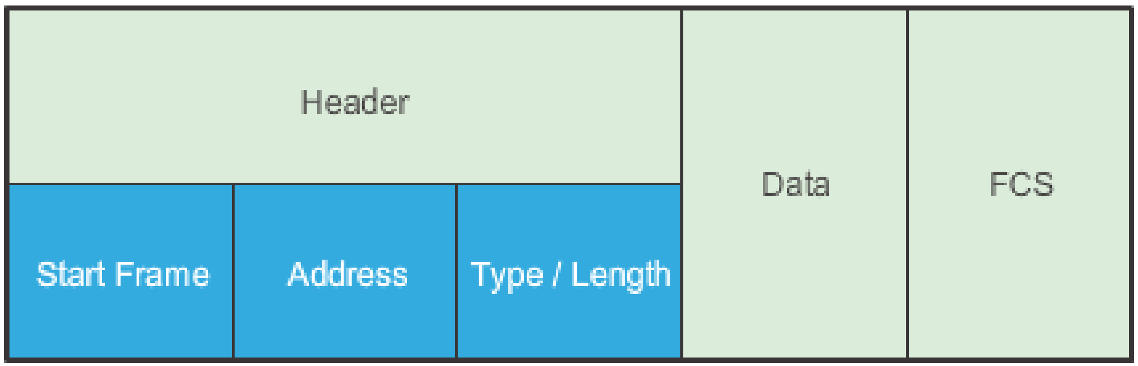


Address

This field stores the source and destination data link addresses.

Data Link Frame Fields - Header

The Role of the Header

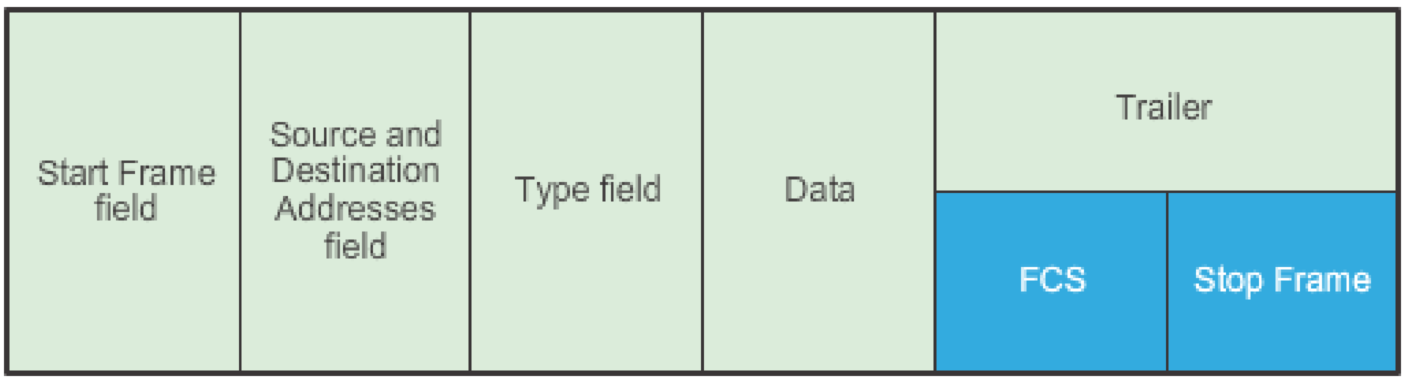


Type / Length

This field is an optional field used by some protocols to state either what type of data is coming or possibly the length of the frame.

Data Link Frame Fields – The Trailer

Frame Trailer



Frame Check Sequence

This field is used for error checking. The source calculates a number based on the frame's data and places that number in the FCS field. The destination then recalculates the data to see if the FCS matches. If they don't match, the destination deletes the frame.

Data Link Frame Fields – The Trailer

Frame Trailer

Start Frame field	Source and Destination Addresses field	Type field	Data	Trailer	
				FCS	Stop Frame

Stop Frame

This field, also called the Frame Trailer, is an optional field that is used when the length of the frame is not specified in the Type/Length field. It indicates the end of the frame when transmitted.

Ethernet Protocol for LANs

Frame

Preamble	Destination	Source	Type	Data	Frame Check Sequence
8 bytes	6 bytes	6 bytes	2 bytes	46 - 1500 bytes	4 bytes

Preamble - Used for synchronization; also contains a delimiter to mark the end of the timing information
Destination Address - 48-bit MAC address for the destination node
Source Address - 48-bit MAC address for the source node
Type - Value to indicate which upper layer protocol will receive the data after the Ethernet process is complete
Data or payload - This is the PDU, typically an IPv4 packet, that is to be transported over the media.
Frame Check Sequence (FCS) - A value used to check for damaged frames

Point-to-Point Protocol for WANs

Frame

Flag	Address	Control	Protocol	Data	FCS
1 byte	1 byte	1 byte	2 bytes	variable	2 or 4 bytes

Flag - A single byte that indicates the beginning or end of a frame. The flag field consists of the binary sequence 01111110.
Address - A single byte that contains the standard PPP broadcast address. PPP does not assign individual station addresses.
Control - A single byte that contains the binary sequence 00000011, which calls for transmission of user data in an unsequenced frame.
Protocol - Two bytes that identify the protocol encapsulated in the data field of the frame. The most up-to-date values of the protocol field are specified in the most recent Assigned Numbers Request For Comments (RFC).
Data - Zero or more bytes that contain the datagram for the protocol specified in the protocol field.
Frame Check Sequence (**FCS**) - Normally 16 bits (2 bytes). By prior agreement, consenting PPP implementations can use a 32-bit (4-byte) FCS for improved error detection.

Media Access Control – Data Link Frame

Data Link Frame
Ethernet Protocol
PPP Protocol

Data Link Layer Protocols

Link Layer Sublayers: LLC and MAC Frame Structure

The Network Layer

The Network Layer

- Provides services to allow end devices to exchange data across the network.
- Uses four basic processes:
    1. Addressing end devices
    2. Encapsulation
    3. Routing
    4. De-encapsulation

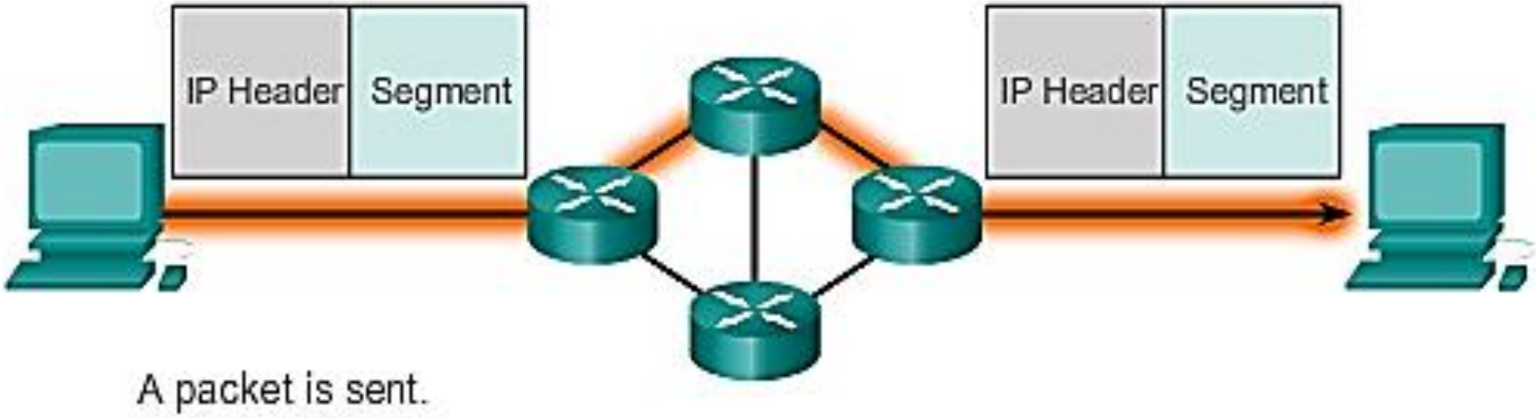
Network Layer Protocols

- Common Network Layer Protocols
  - IPv4
  - IPv6
- Legacy Network Layer Protocols
  - Novell Internetwork Packet Exchange (IPX)
  - AppleTalk
  - Connectionless Network Service (CLNS/DECNet)

Characteristics of IP Protocol

- **Connectionless**: No connection is established before sending data packets.
- **Best effort delivery:** No additional overhead is used to guarantee packet delivery.
- **Media independent:** Operates independently of the medium carrying the data.

Connectionless Service



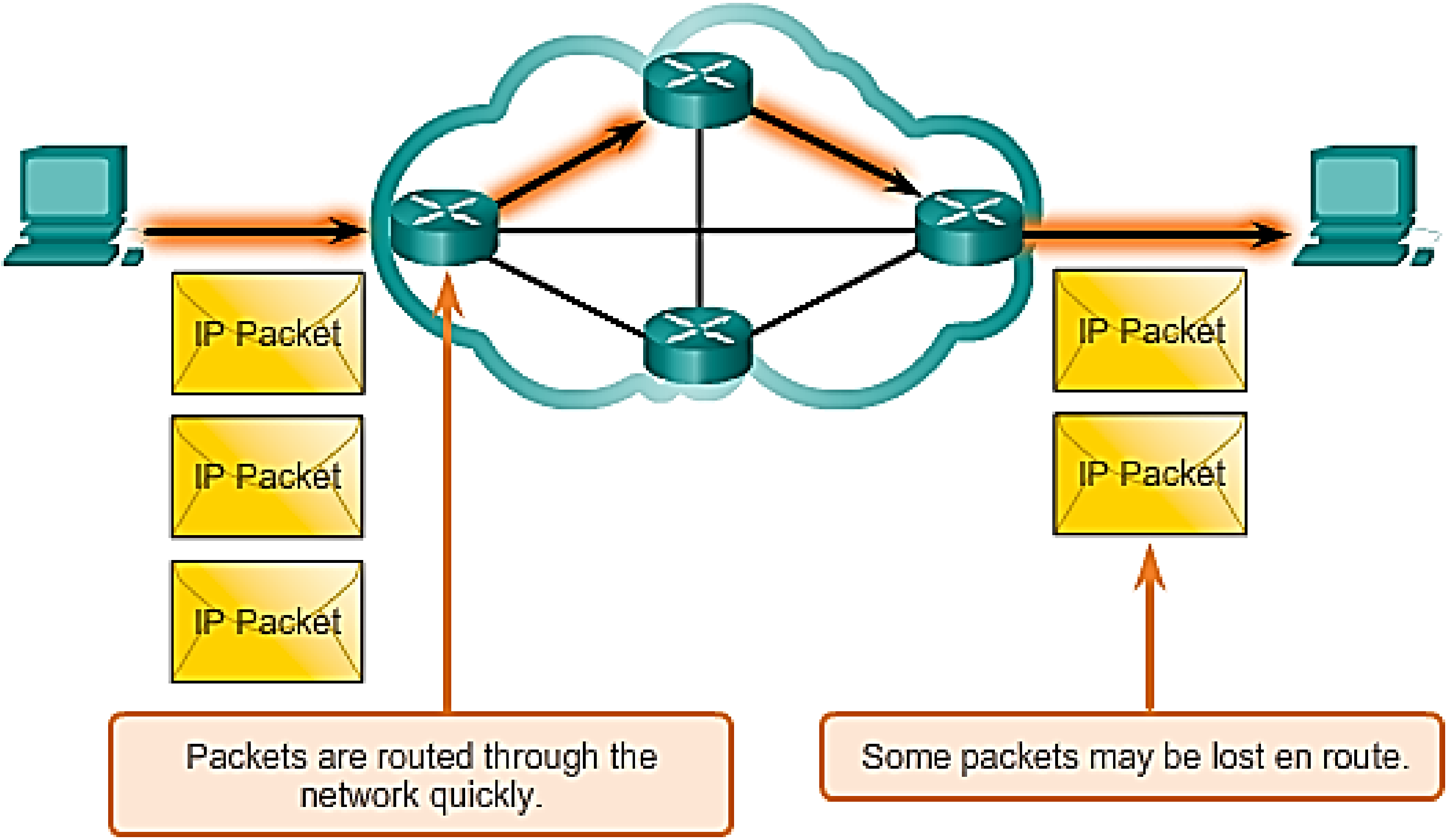
The sender doesn't know:

- if the receiver is present
- if the letter arrived
- if the receiver can read the letter

The receiver doesn't know:

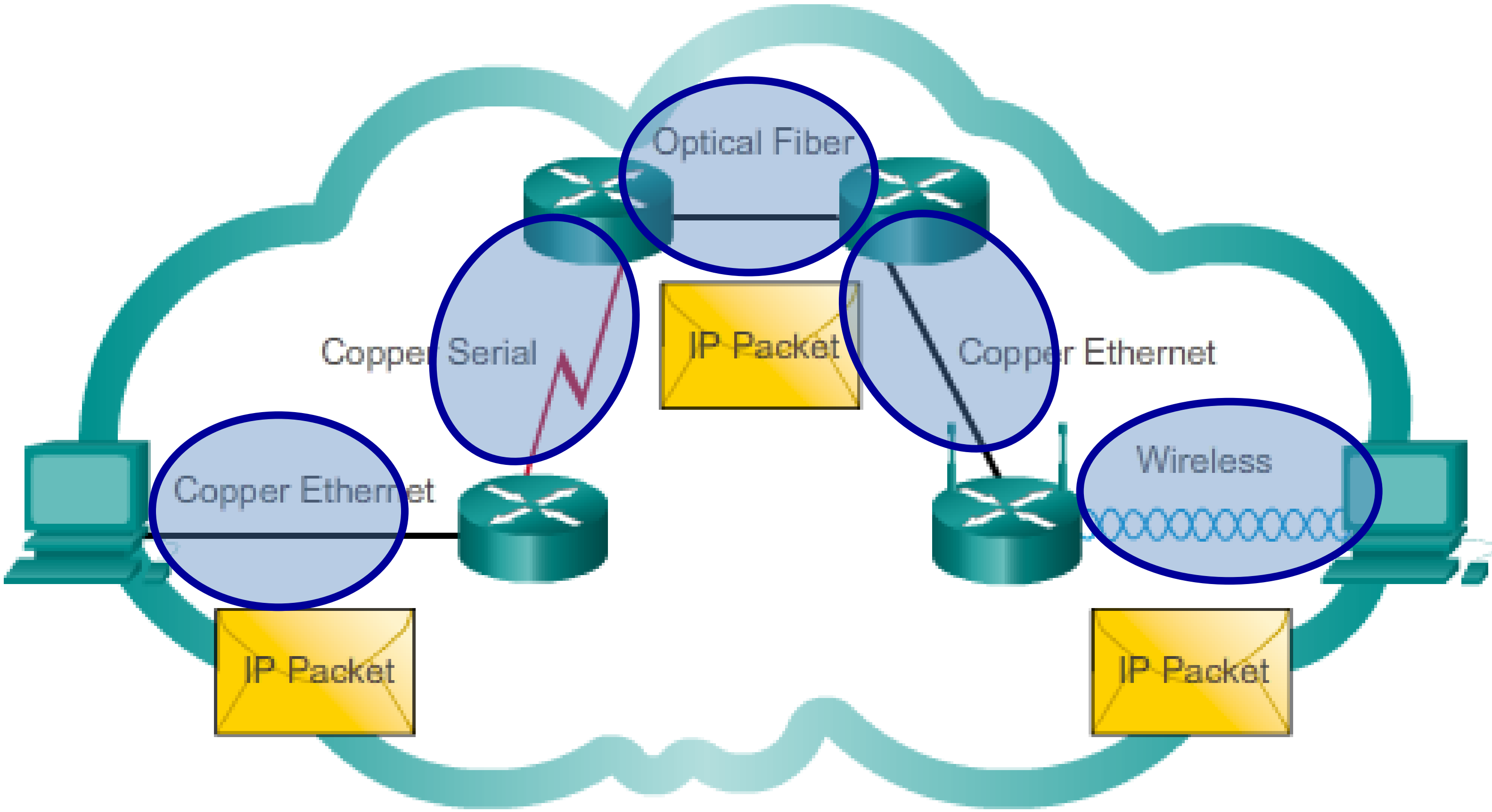
- when it is coming

Best Effort Delivery – Unreliable



As an unreliable network layer protocol, IP does not guarantee that all sent packets will be received. Other protocols manage the process of tracking packets and ensuring their delivery.

Media Independent



IP packets can travel over different media.

Network Layer Protocols

Network Layer Functions

IP Characteristics

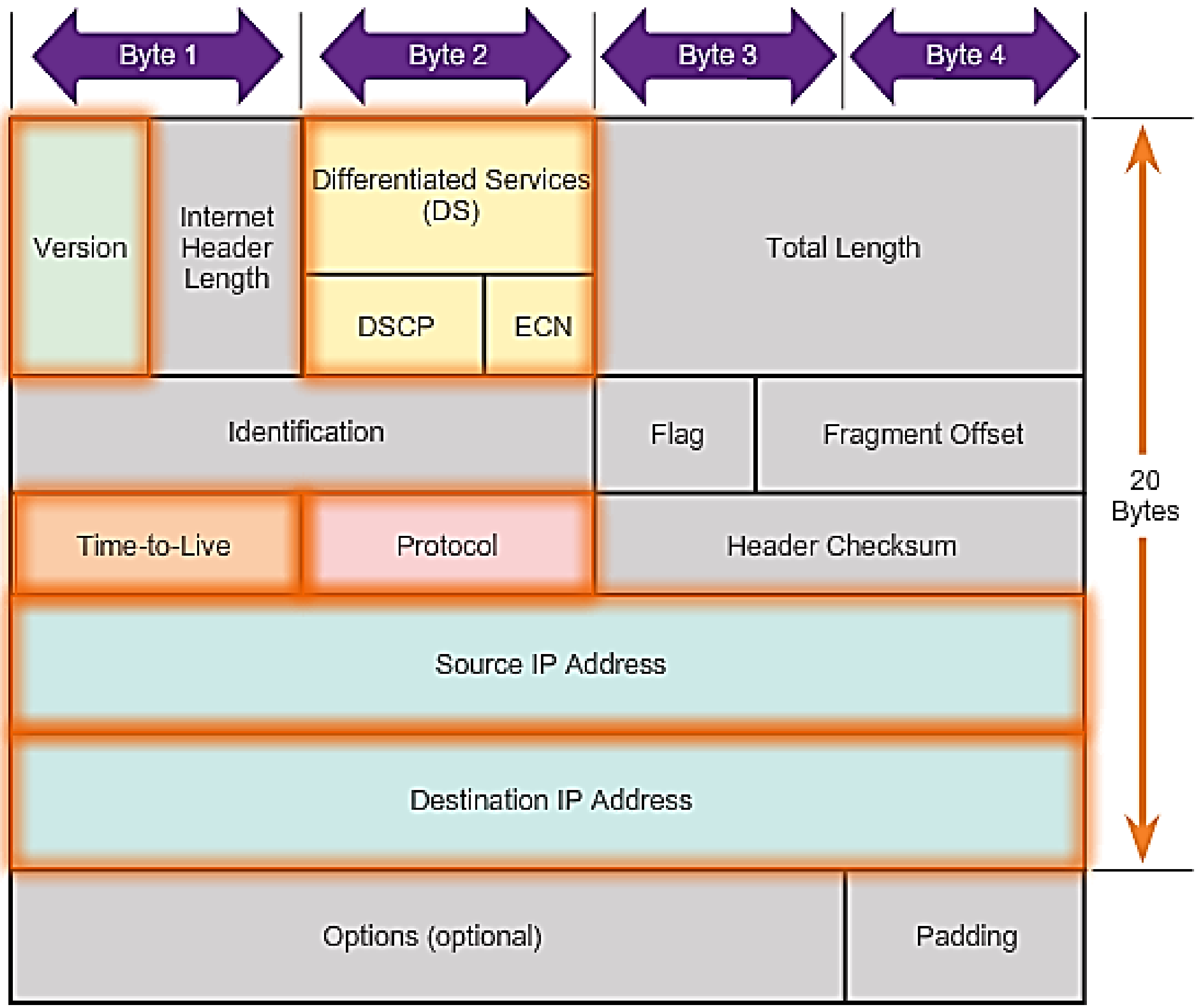
IPv4 Packet

IPv4 Packet Structure

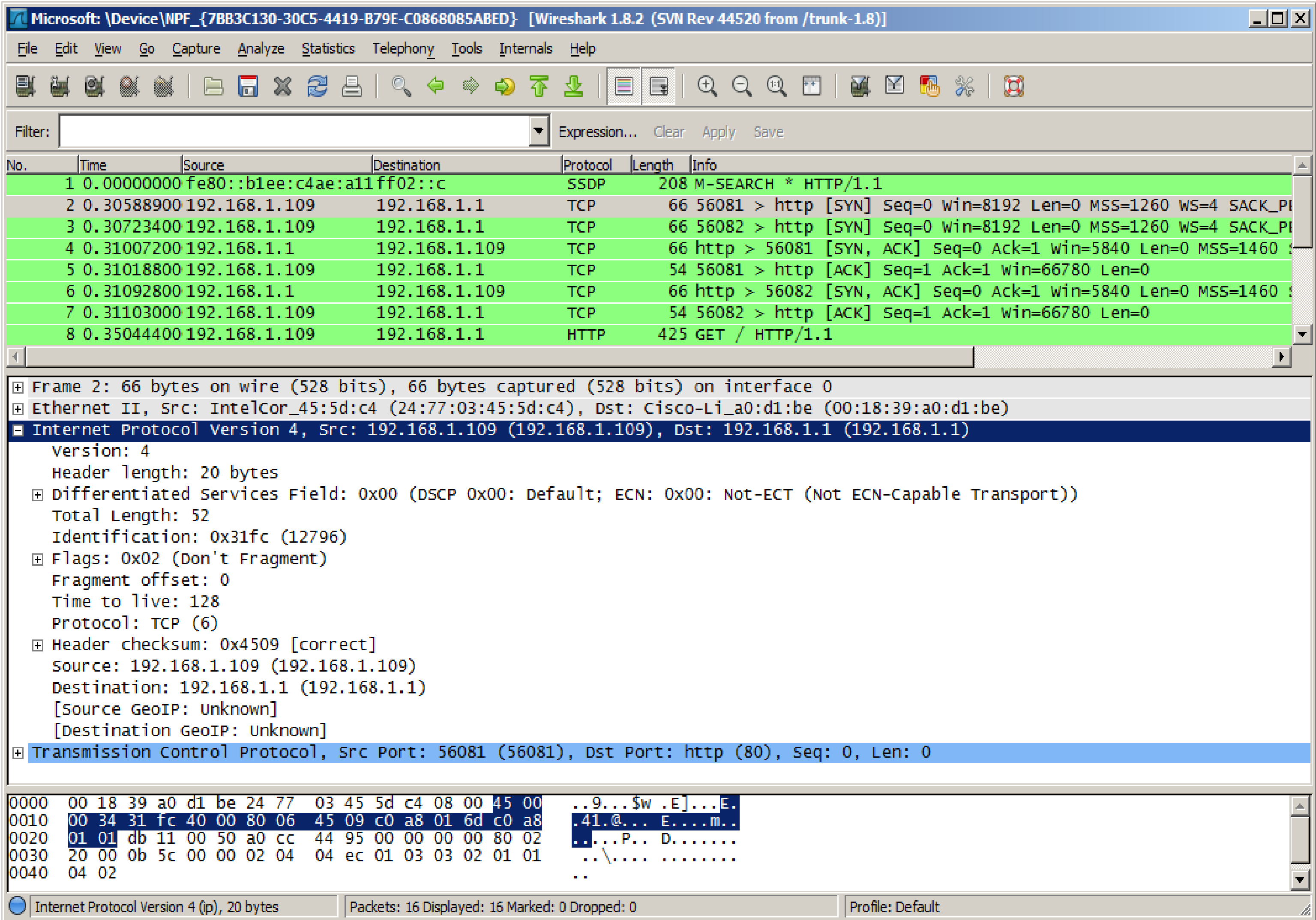
IPv4 Packet Structure

- An IPv4 packet has two parts:
  - **IP Header** - Identifies the packet characteristics.
  - **Payload** - Contains the Layer 4 segment information and the actual data.

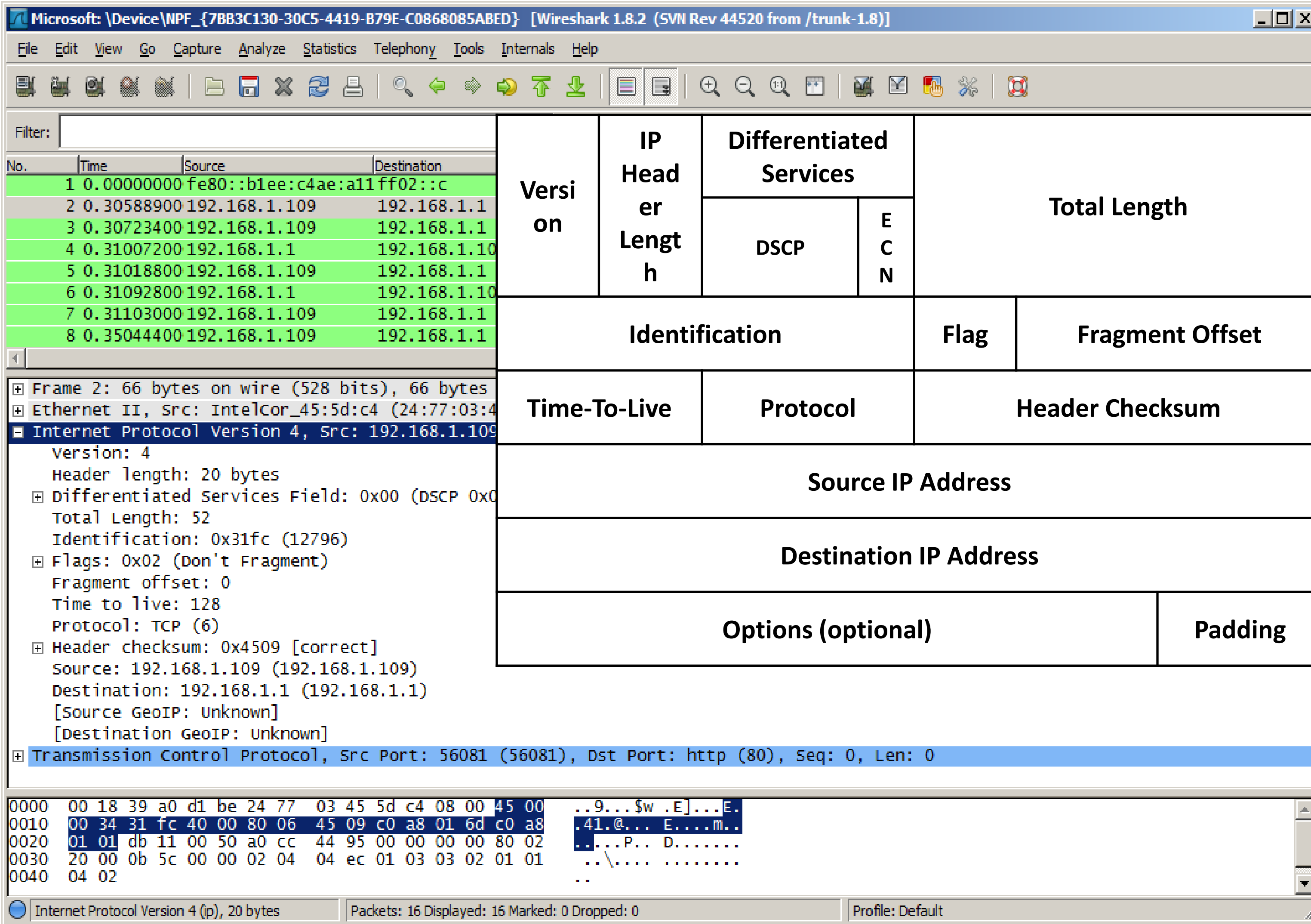
IPv4 Packet Header



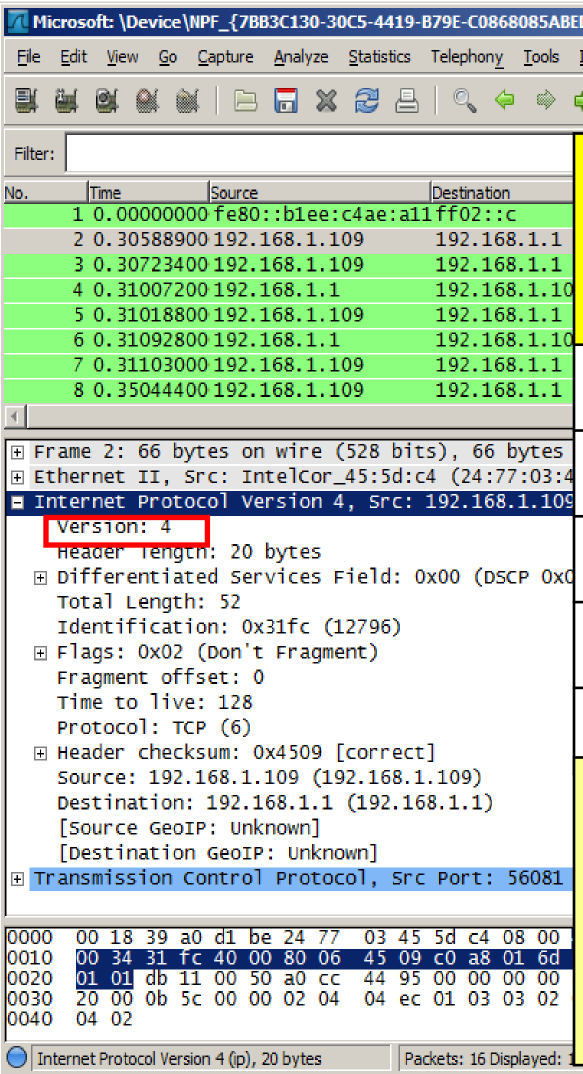
Sample IPv4 Packet



Sample IPv4 Packet



Sample IPv4 Packet

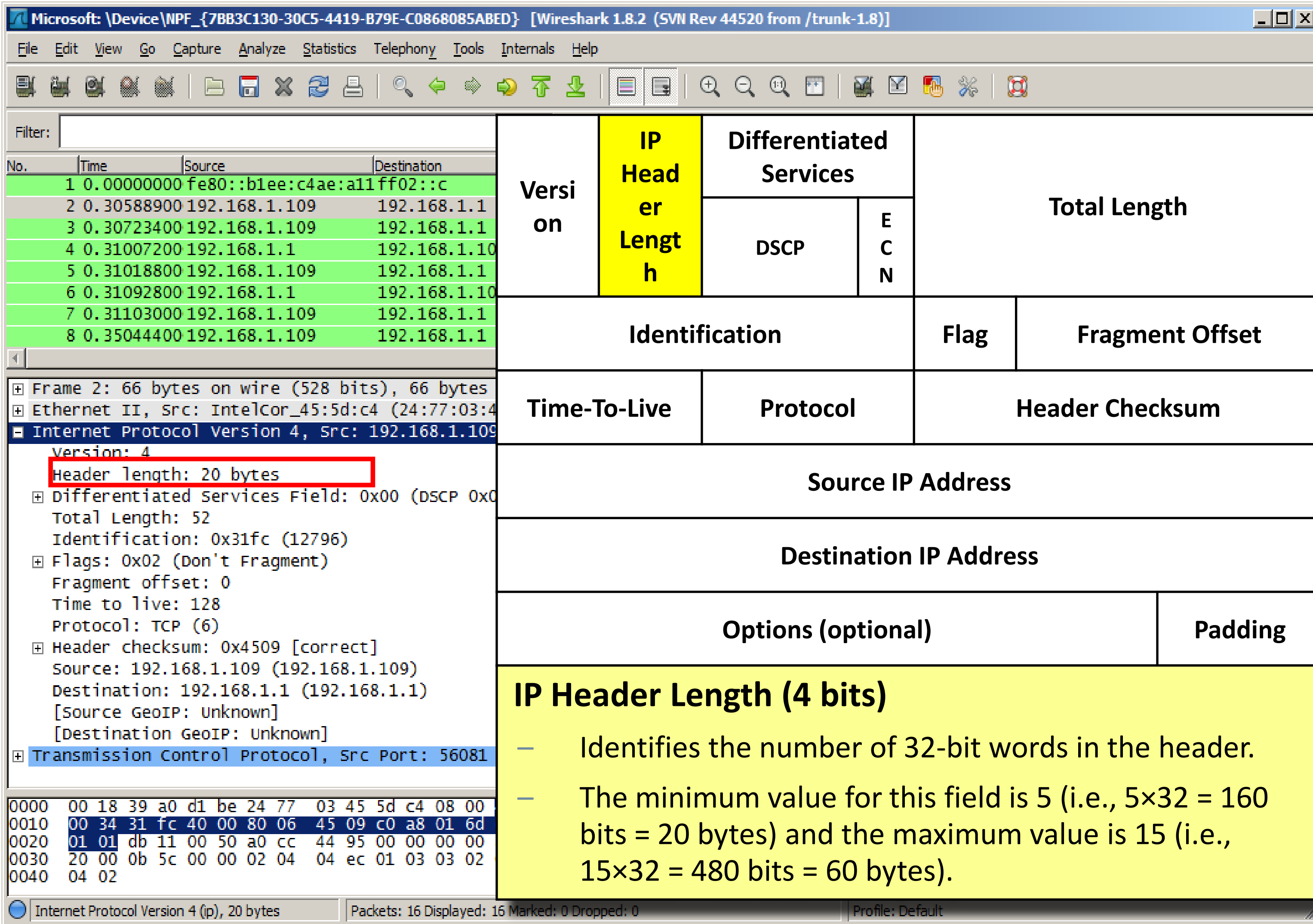


<table>
<tr><td rowspan="2">Version</td><td rowspan="2">IP Header Length</td><td colspan="2">Differentiated Services</td><td colspan="2" rowspan="2">Total Length</td></tr>
<tr><td>DSCP</td><td>ECN</td></tr>
<tr><td colspan="4">Identification</td><td>Flag</td><td>Fragment Offset</td></tr>
<tr><td colspan="2">Time-To-Live</td><td colspan="2">Protocol</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="6">Source IP Address</td></tr>
<tr><td colspan="6">Destination IP Address</td></tr>
<tr><td colspan="5">Options (optional)</td><td>Padding</td></tr>
</table>

Version (4 bits)

- Indicates the version of IP currently used.
- 0100 = 4 and therefore IPv4
- 0110 = 6 and therefore IPv6

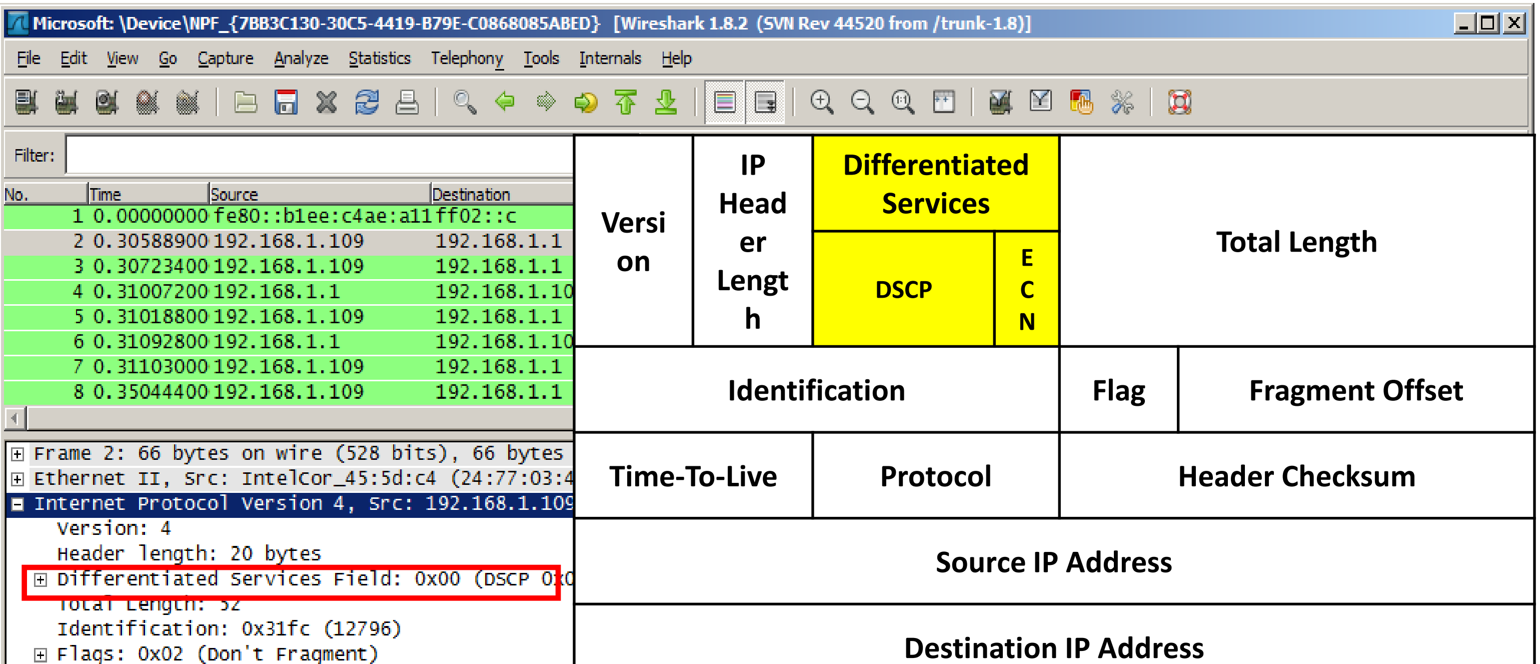
Sample IPv4 Packet



IP Header Length (4 bits)

- Identifies the number of 32-bit words in the header.
- The minimum value for this field is 5 (i.e., 5×32 = 160 bits = 20 bytes) and the maximum value is 15 (i.e., 15×32 = 480 bits = 60 bytes).

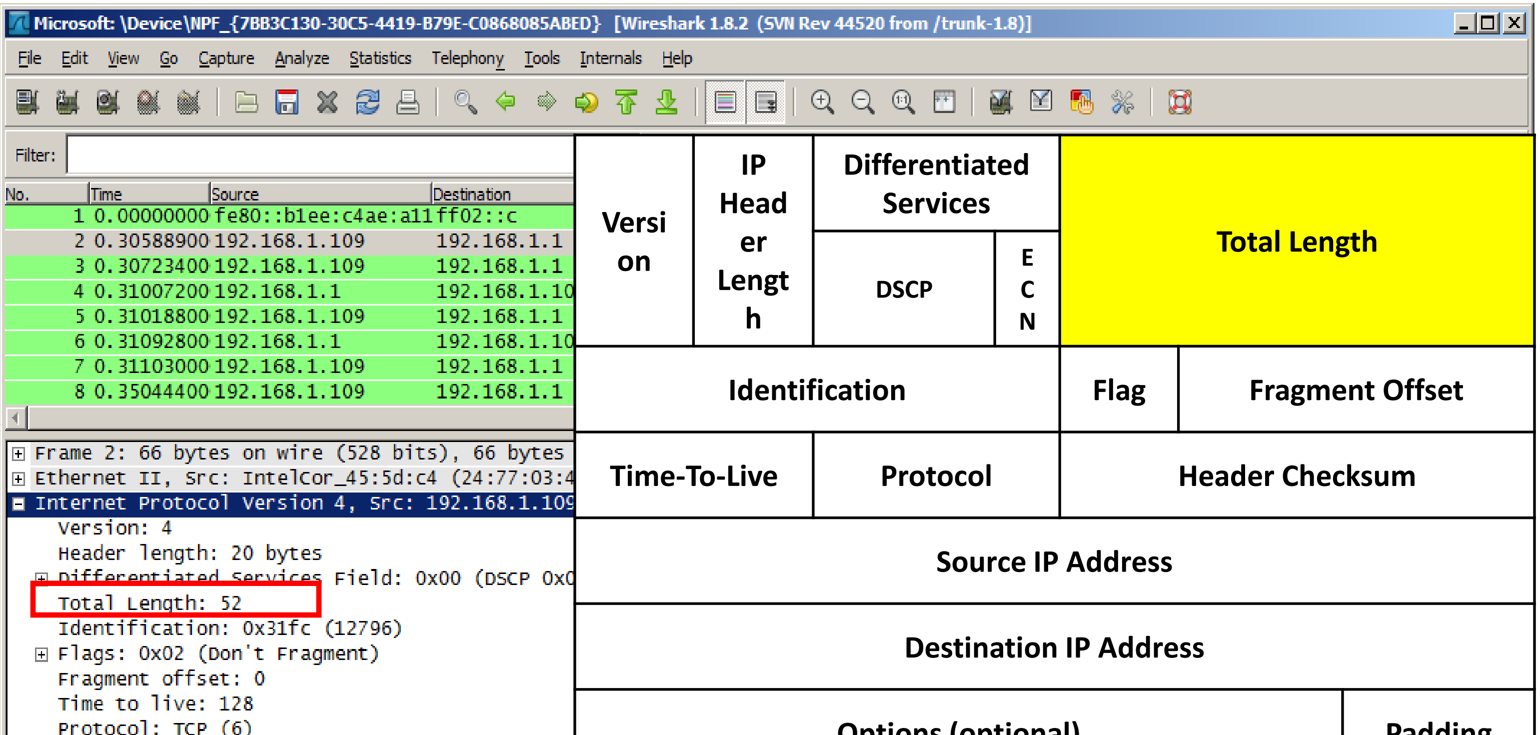
Sample IPv4 Packet



Differentiated Services (8 bits)

- Formerly called the Type of Service (ToS) field.
- The field is used to determine the priority of each packet.
- First 6 bits identify the Differentiated Services Code Point (DSCP) value for QoS.
- Last 2 bits identify the explicit congestion notification (ECN) value used to prevent dropped packets during times of network congestion.

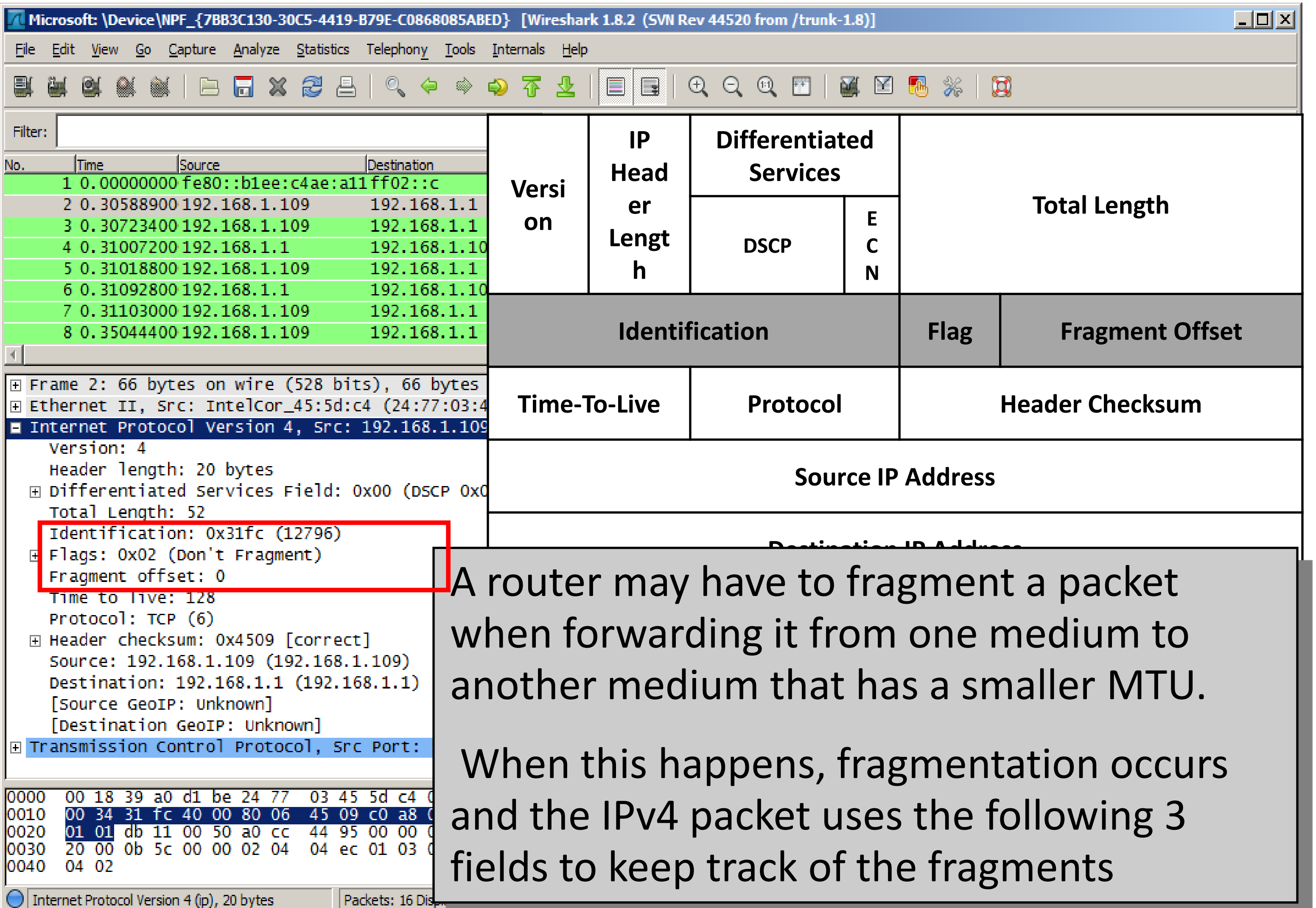
Sample IPv4 Packet



Total Length (16 bits)

- Sometimes referred to as the Packet Length.
- Defines the entire packet (fragment) size, including header and data, in bytes.
- The minimum length packet is 20 bytes (20-byte header + 0 bytes data) and the maximum is 65,535 bytes. .

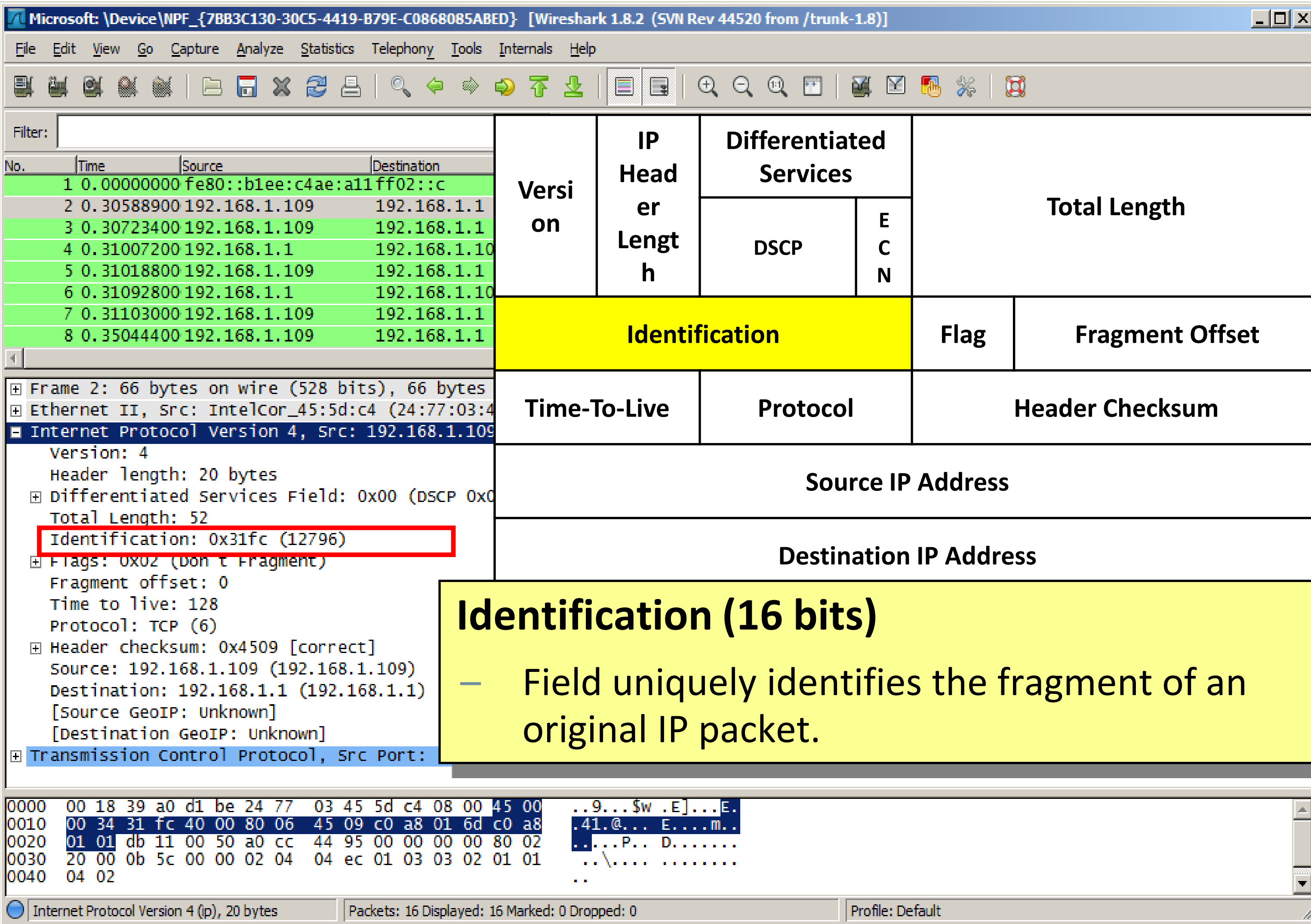
Sample IPv4 Packet



A router may have to fragment a packet when forwarding it from one medium to another medium that has a smaller MTU.

When this happens, fragmentation occurs and the IPv4 packet uses the following 3 fields to keep track of the fragments

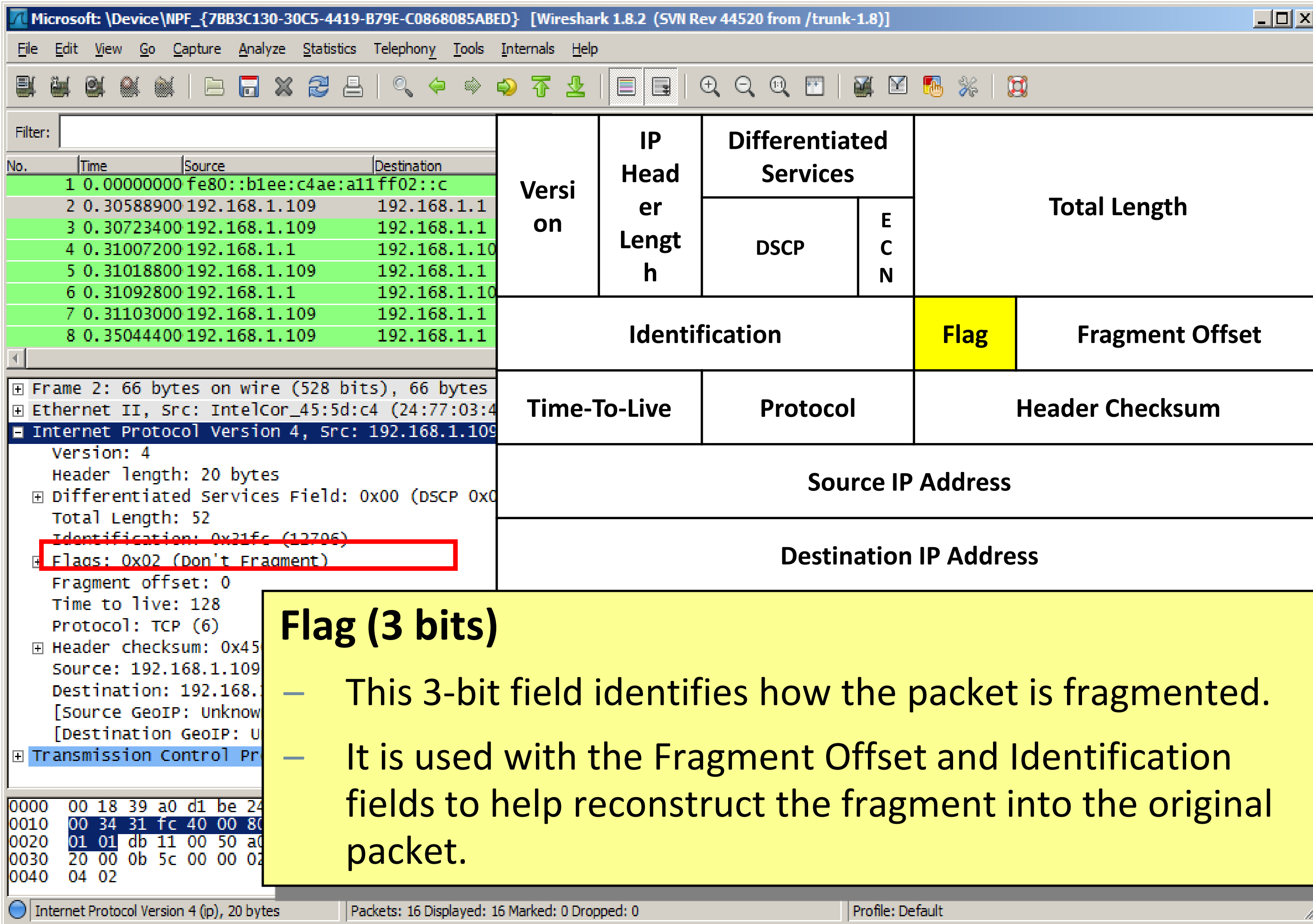
Sample IPv4 Packet



Identification (16 bits)

– Field uniquely identifies the fragment of an original IP packet.

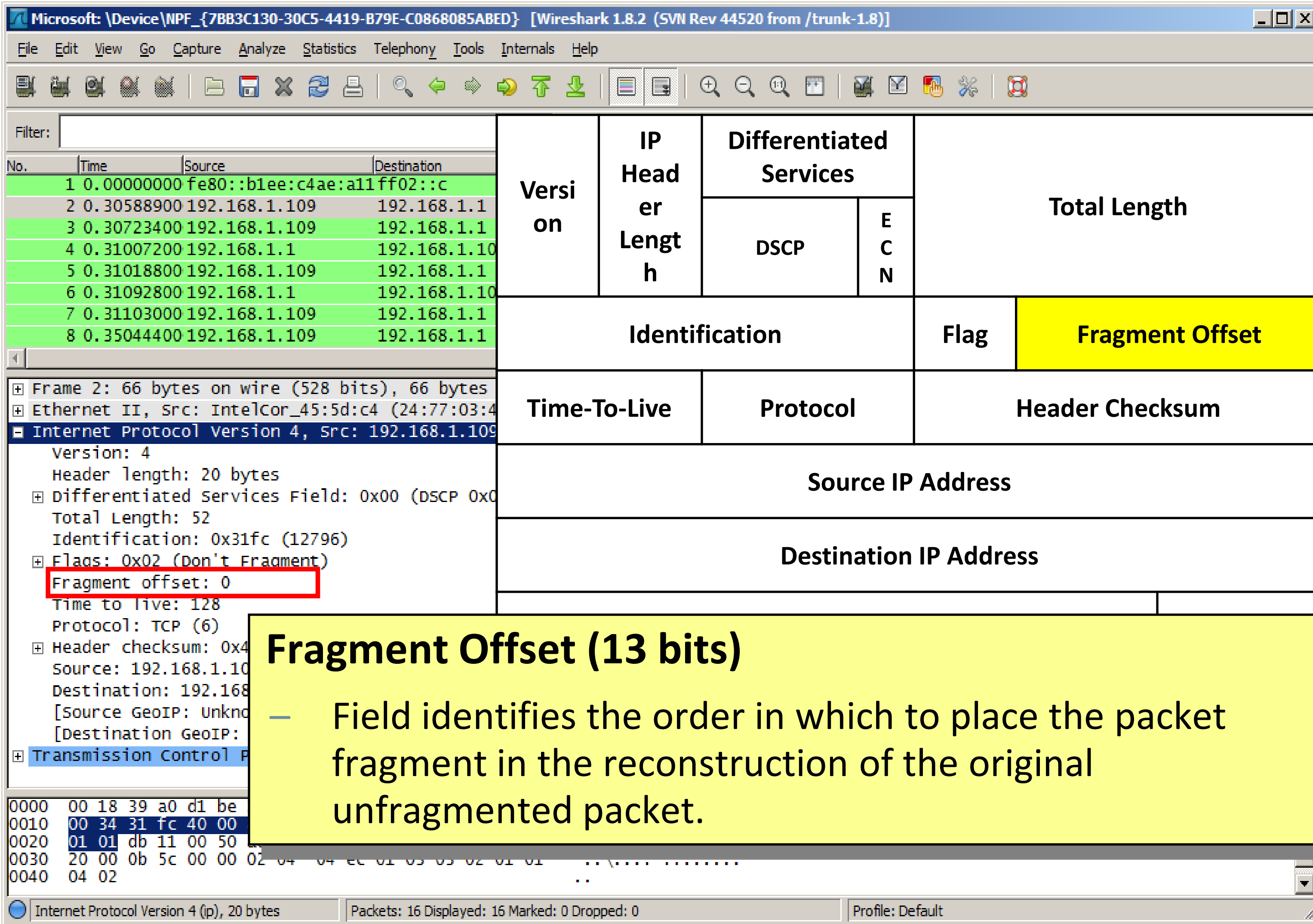
Sample IPv4 Packet



Flag (3 bits)

- This 3-bit field identifies how the packet is fragmented.
- It is used with the Fragment Offset and Identification fields to help reconstruct the fragment into the original packet.

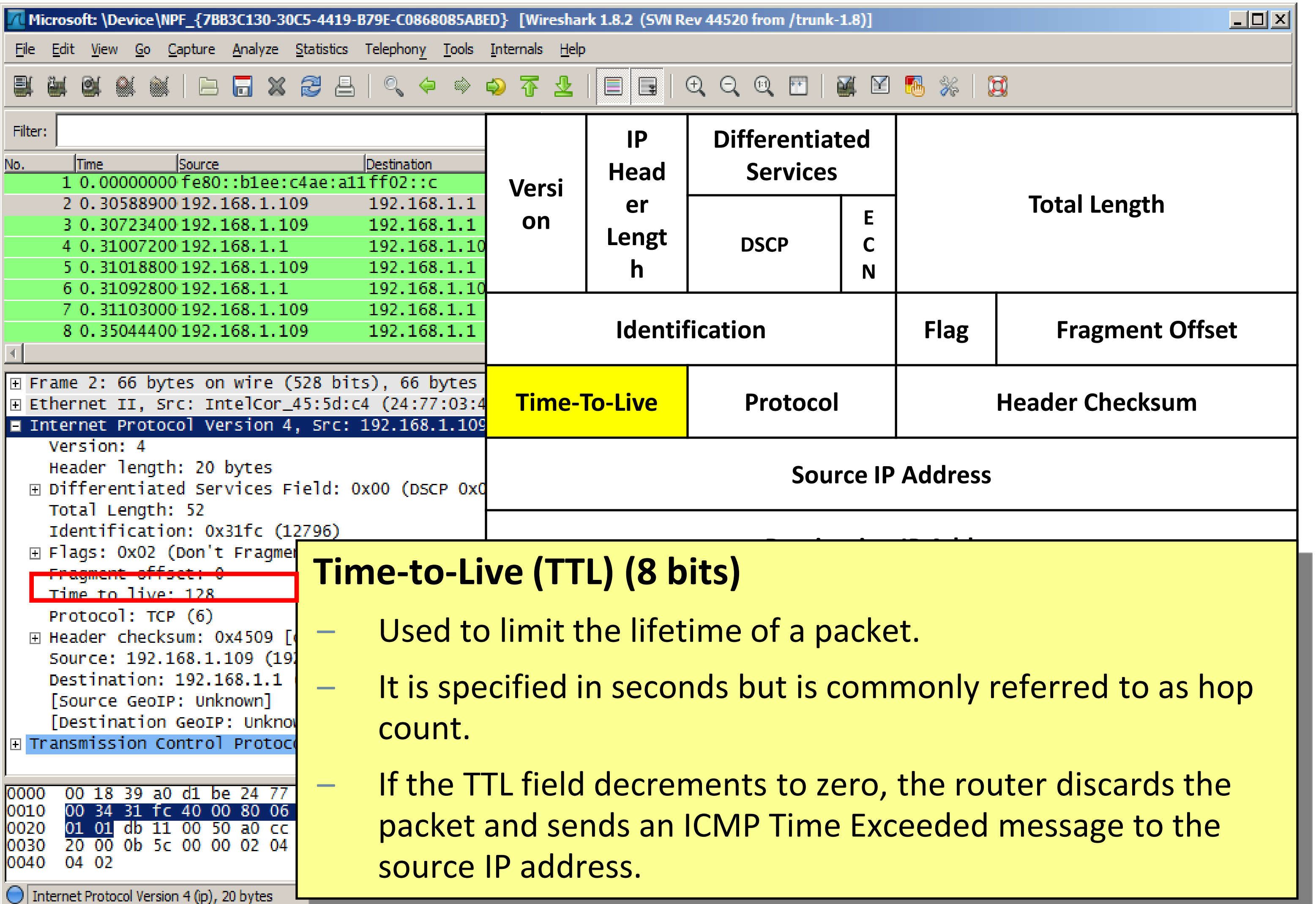
Sample IPv4 Packet



Fragment Offset (13 bits)

– Field identifies the order in which to place the packet fragment in the reconstruction of the original unfragmented packet.

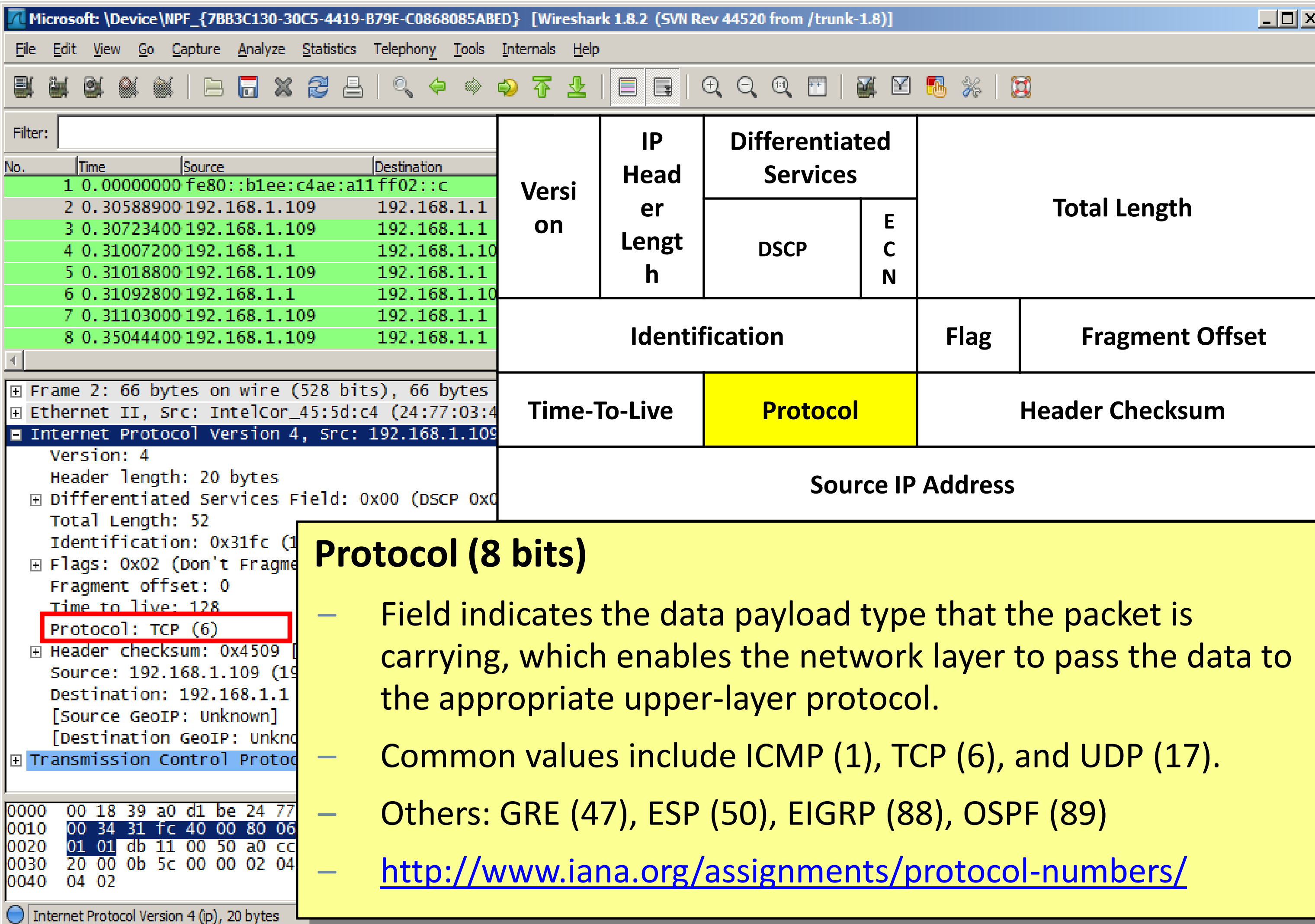
Sample IPv4 Packet



Time-to-Live (TTL) (8 bits)

- Used to limit the lifetime of a packet.
- It is specified in seconds but is commonly referred to as hop count.
- If the TTL field decrements to zero, the router discards the packet and sends an ICMP Time Exceeded message to the source IP address.

Sample IPv4 Packet

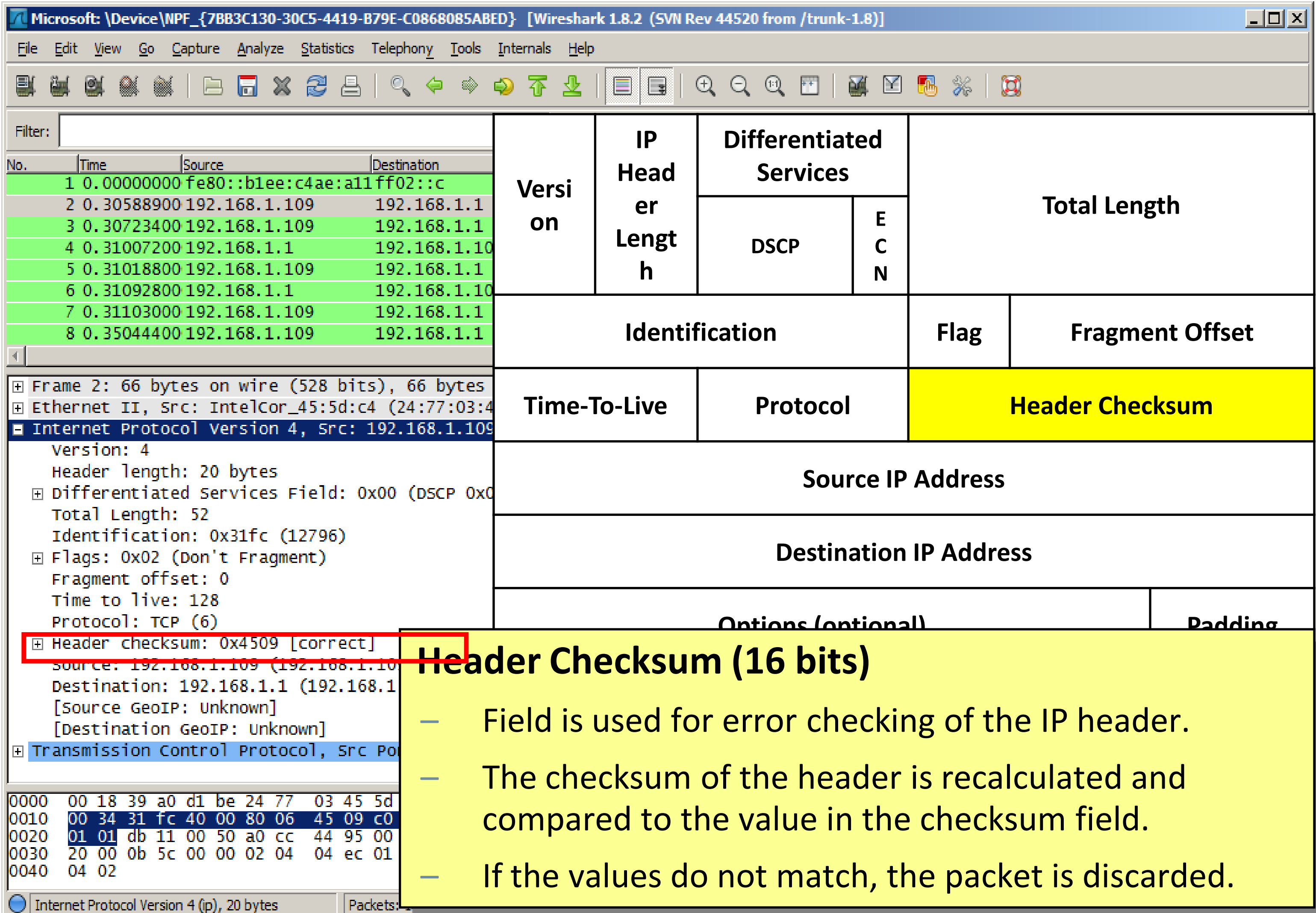


Version	IP Header Length	Differentiated Services		Total Length	
		DSCP	ECN		
Identification				Flag	Fragment Offset
Time-To-Live		Protocol		Header Checksum	
Source IP Address					

Protocol (8 bits)

- Field indicates the data payload type that the packet is carrying, which enables the network layer to pass the data to the appropriate upper-layer protocol.
- Common values include ICMP (1), TCP (6), and UDP (17).
- Others: GRE (47), ESP (50), EIGRP (88), OSPF (89)
- http://www.iana.org/assignments/protocol-numbers/

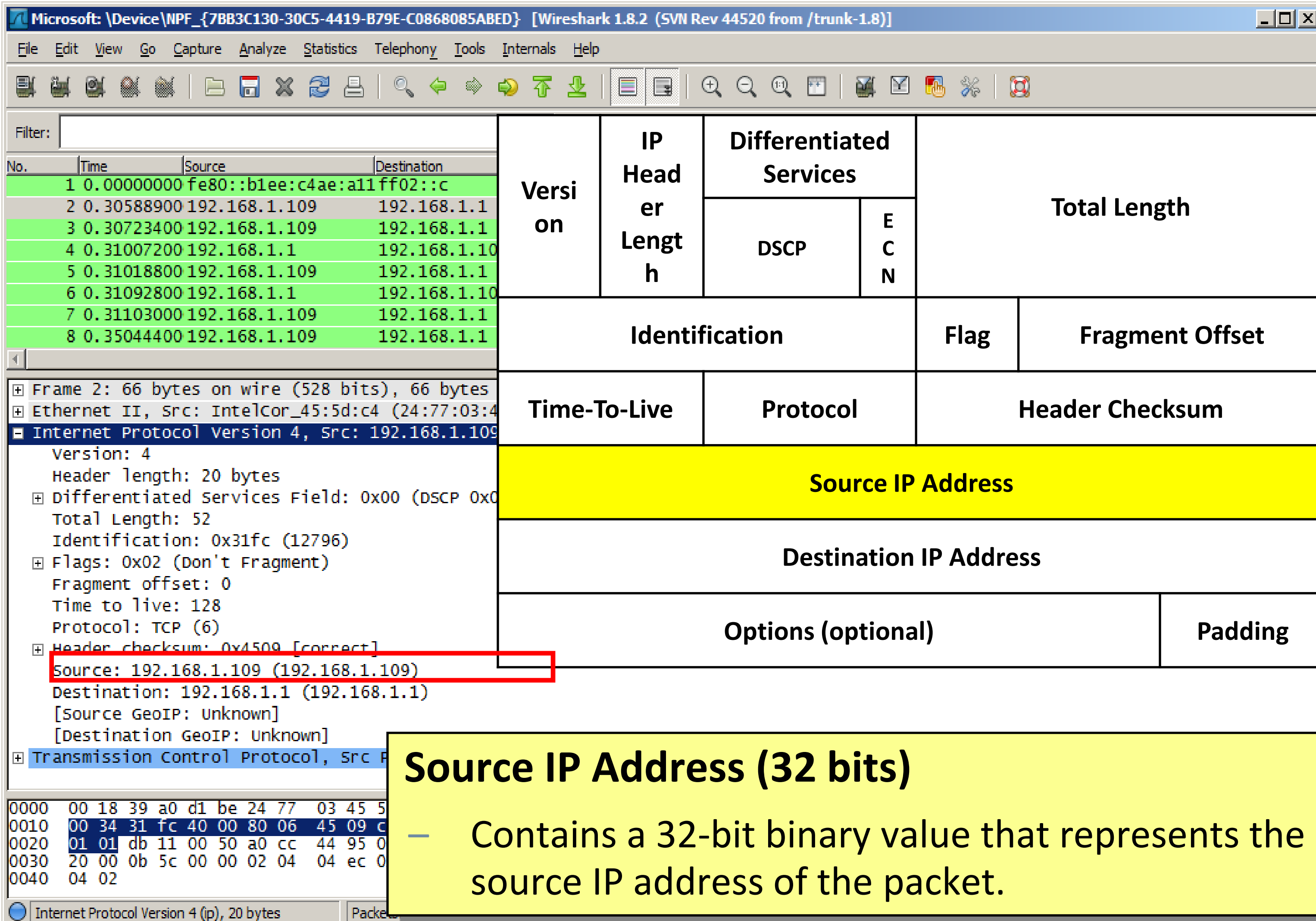
Sample IPv4 Packet



Header Checksum (16 bits)

- Field is used for error checking of the IP header.
- The checksum of the header is recalculated and compared to the value in the checksum field.
- If the values do not match, the packet is discarded.

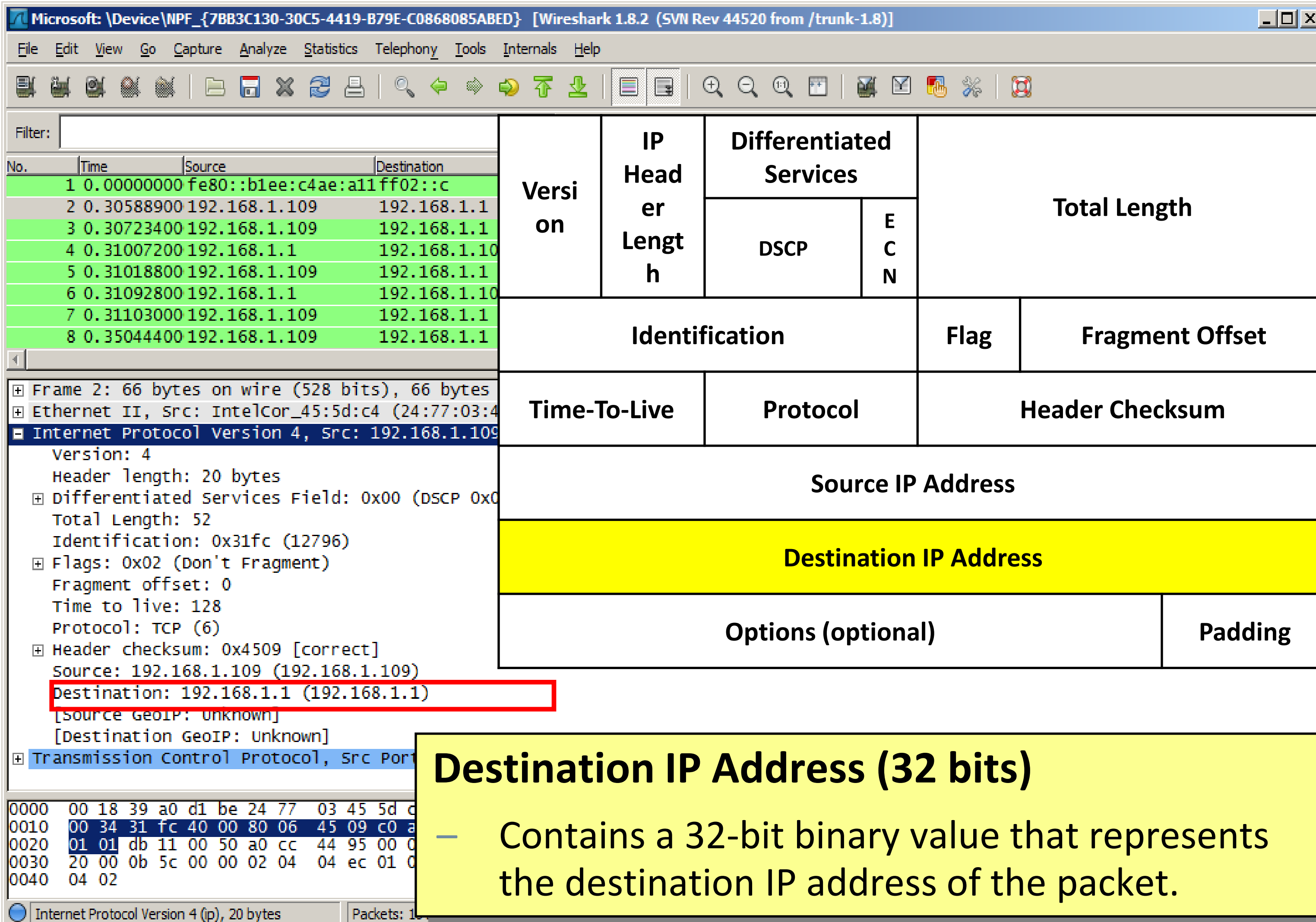
Sample IPv4 Packet



Source IP Address (32 bits)

- Contains a 32-bit binary value that represents the source IP address of the packet.

Sample IPv4 Packet



Destination IP Address (32 bits)

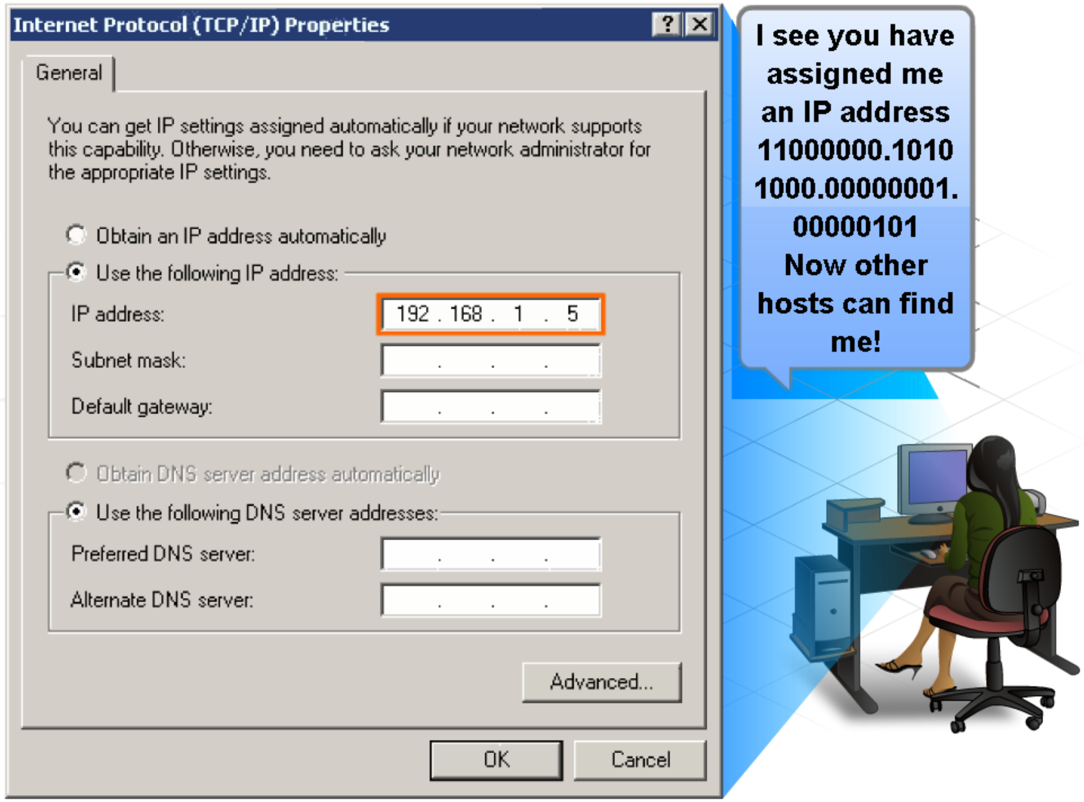
– Contains a 32-bit binary value that represents the destination IP address of the packet.

IPv4 Packet

IPv4 Packet
Header

IPv4 Address Structure

IPv4 Address Structure

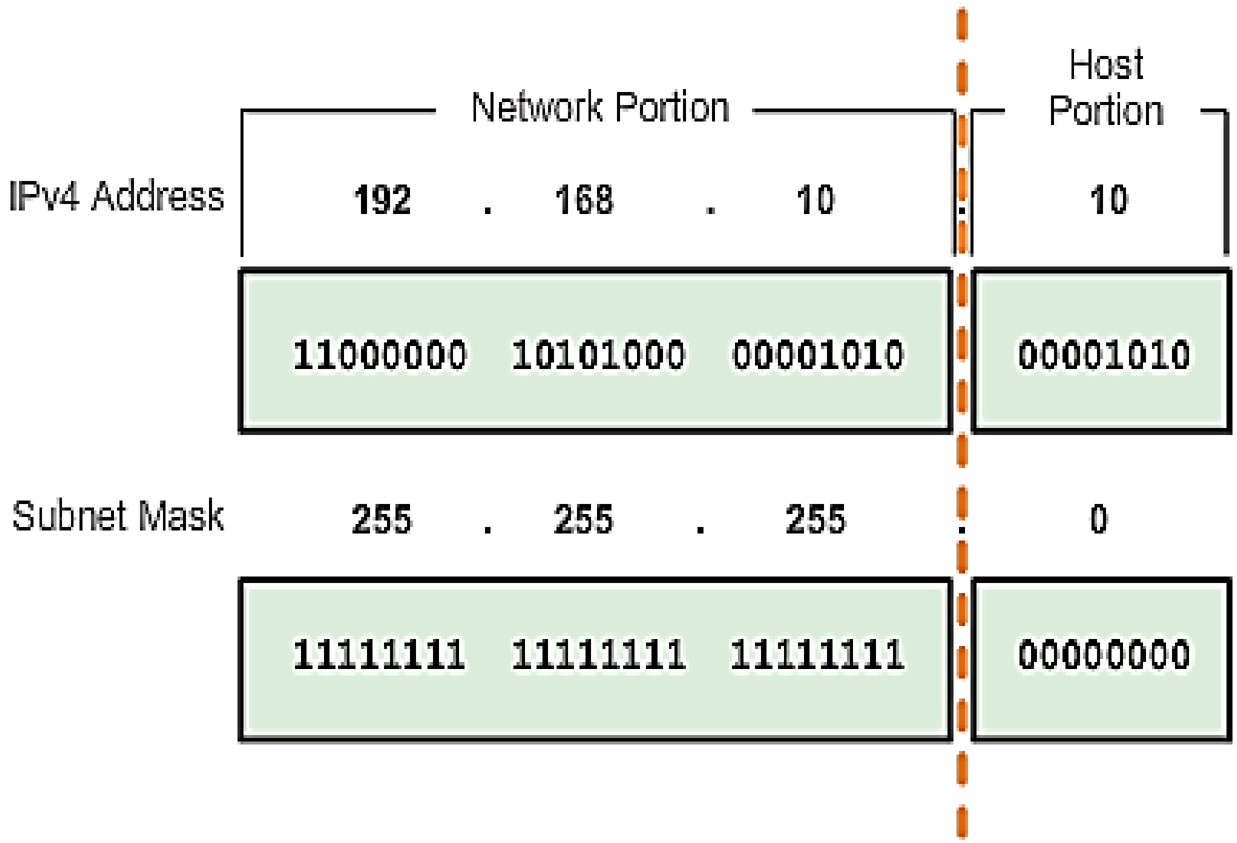


IP version 4 (IPv4) is the current form of addressing used on the Internet.

We look at IP addresses using the "*dotted decimal format*" but network devices only understand the binary format.

11000000 . 10101000 . 00000001 . 00000101

IPv4 Subnet Mask



Prefix Length

Subnet Mask: 192.168.11.10

255.255.255.0

192	168	11	10
255	255	255	0
11111111	11111111	11111111	00000000

The subnet mask identifies which part of the IP address refers to the network.

Network Portion			Host Portion
192	168	11	0

- The prefix length is the number of bits set to 1 in the subnet mask.
- For example:

  IP address: **192.168.11**.10 **255.255.255.0**

  Is the same as: **192.168.11**.10 **/24**

IPv4 Subnet Mask

So how do hosts figure out which part of the address is the network portion?

Hosts compare the IP address and the subnet mask.

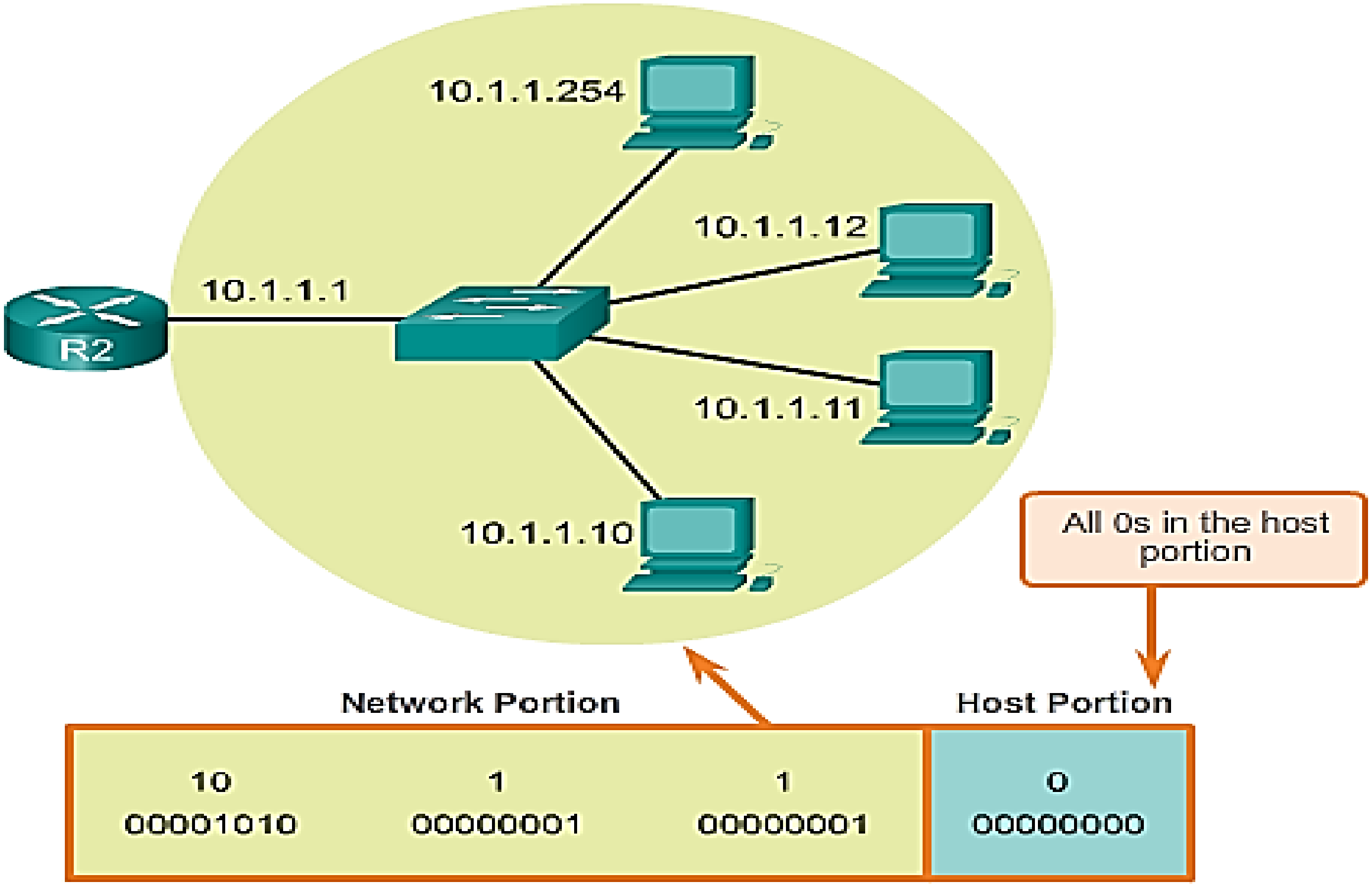
- "**1**" bits refer to the network portion.
- "**0**" bits refer to the host portion.

This tells them what network they belong to.

Types of Addresses in a Network

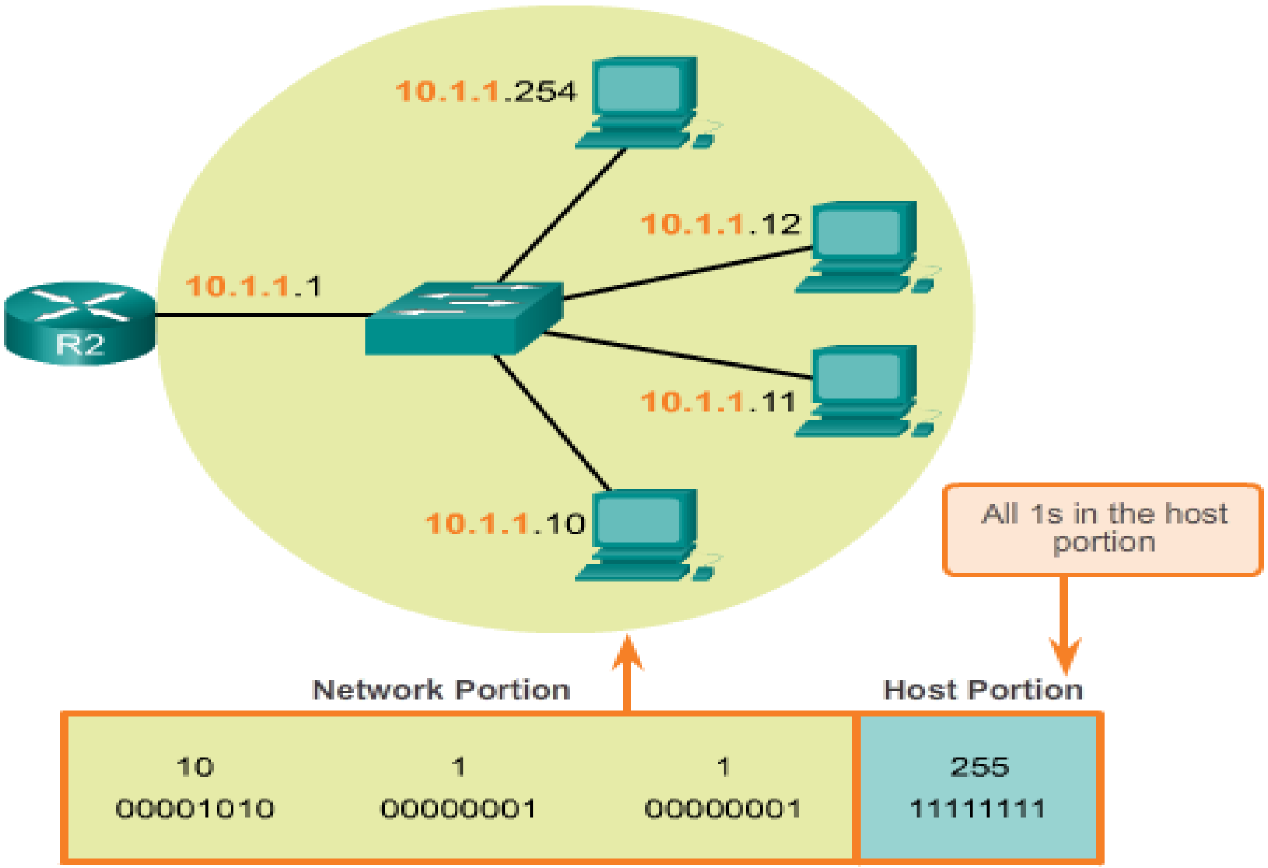
- Network Address
- Host Address
- Broadcast Address

Network Address 10.1.1.0/24



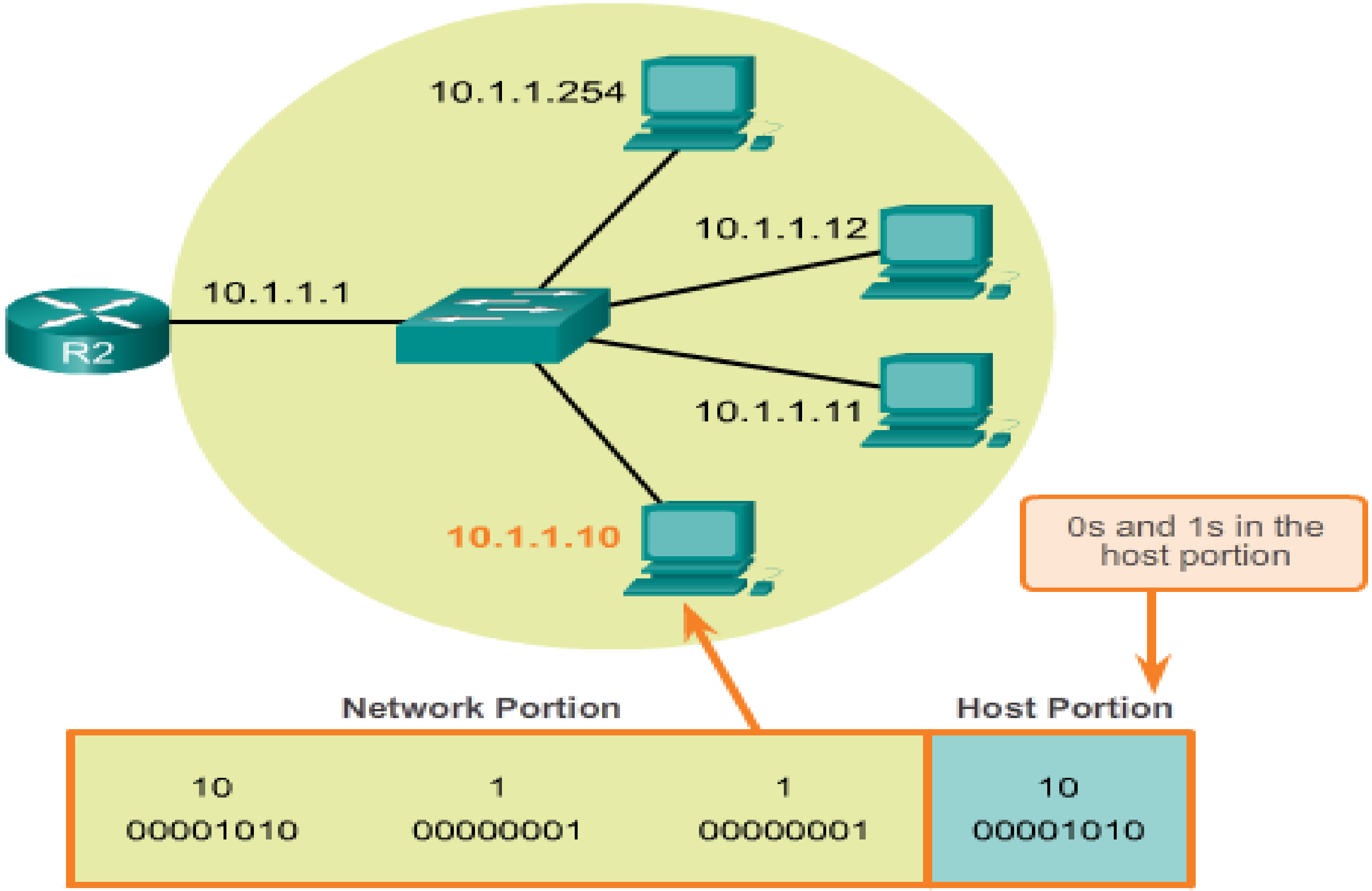
- All devices in the network have the same network bits.
  - ***The network address has all 0 bits in the host portion.***

Broadcast Address 10.1.1.255/24



- A broadcast address is used to send data to all hosts in the network.
  - ***The broadcast address has all 1 bits in the host portion.***

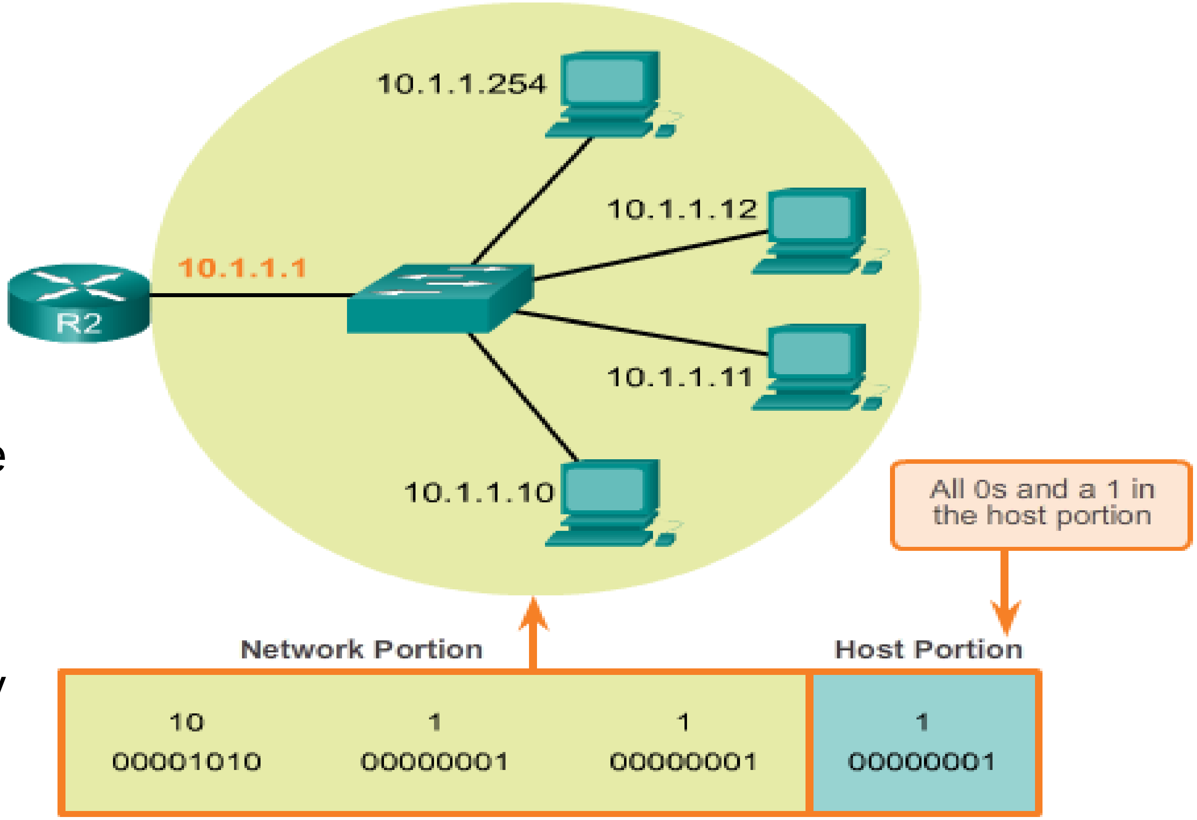
Host Address 10.1.1.10/24



- In IPv4 addresses, ***host addresses are the addresses between the network address and the broadcast address devices*** in that network.

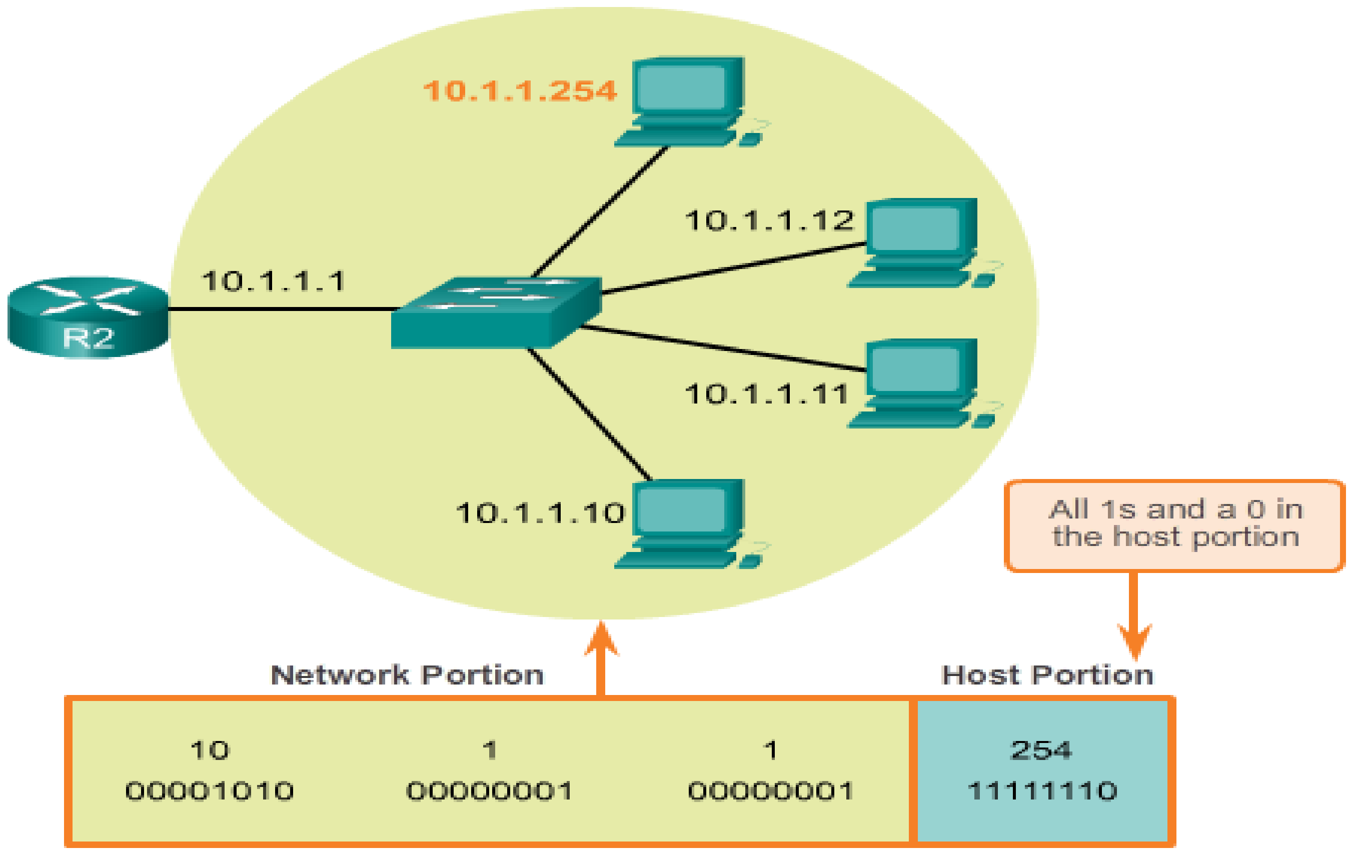
1st Host Address

NOTE:
It is common in many addressing schemes to use the first host address for the router or default gateway address.



- The host portion of the first host address will contain all 0 bits with a 1 bit for the lowest order or right-most bit. ("All 0's and a 1.")
  - For example the first host address is 10.1.1.1 /24.

Last Host Address

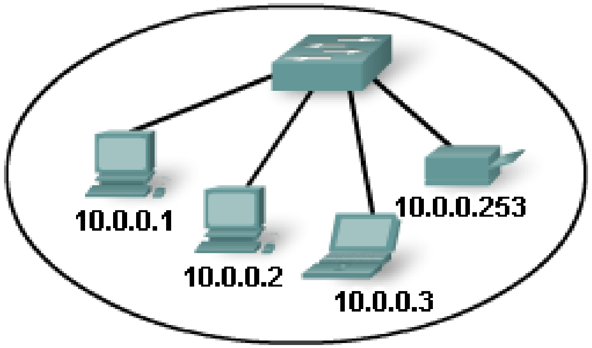


- The host portion of the last host address will contain all 1 bits with a 0 bit for the lowest order or right-most bit. (“All 1’s and a 0.”)
  - For example, the last host address is 10.1.1.254.

Bringing it Al together

	Network			Host
Network Address	10	0	0	0
	00001010	00000000	00000000	00000000
Broadcast Address	10	0	0	255
	00001010	00000000	00000000	11111111
Host Address	10	0	0	1
	00001010	00000000	00000000	00000001

Roll over to learn more.



IPv4 Address and Subnet Mask

- IPv4 Address
- Subnet Mask
- Types of Addresses

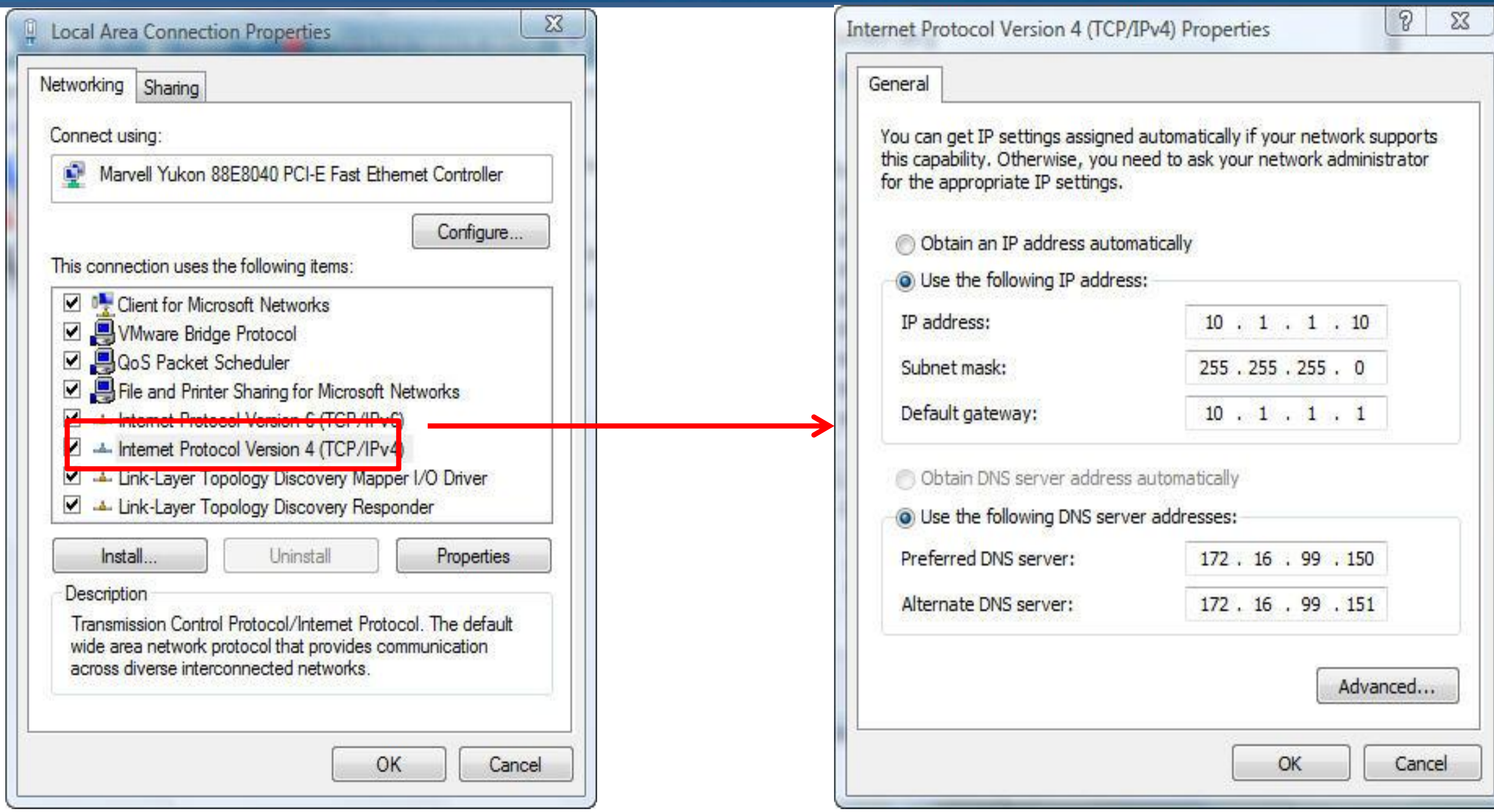
IPv4 Unicast, Broadcast, and Multicast

Addresses for User Devices

Addresses for User Devices

- Static Assignment
- Dynamic Assignment

Assigning a Static IPv4 Address to a Host



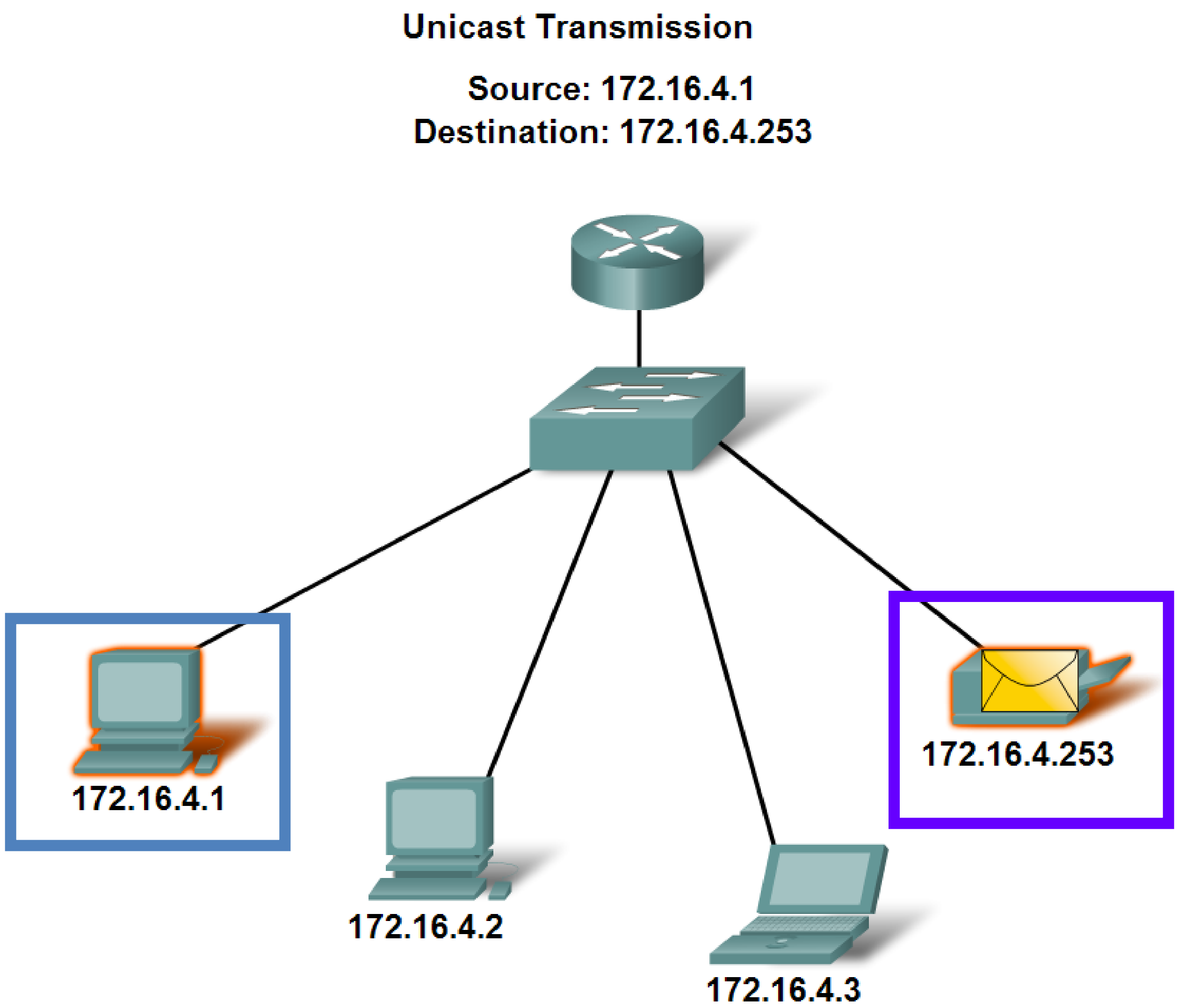
- Useful for printers, servers, and other networking devices that do not change location often and need to be accessible to clients on the network based on a fixed IP address.
- However, static addressing can be time-consuming to enter on each host.

Destination Unicasts, Broadcasts and Multicasts

Source IP Addresses are always unicast

- **Unicasts**:
  Packet travels from one host to another specific host.
- **Multicasts**:
  Packet travels from one host to a select number of other hosts.
  Supports voice and audio broadcasts, news feeds.
- **Broadcasts:**
  Packet travels from one host to all hosts on the local network.

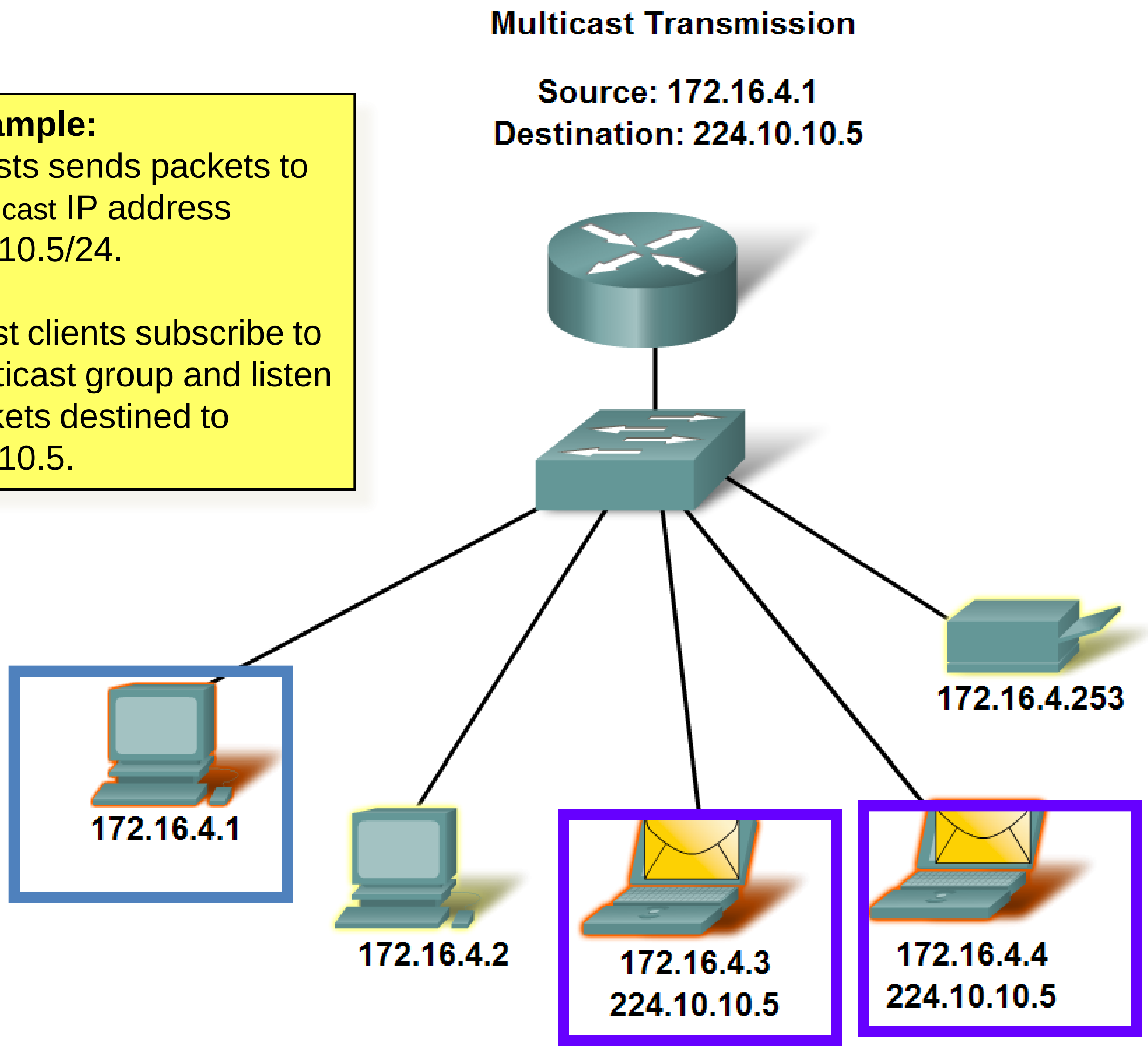
Unicast Addresses



Multicast Addresses

For example:
One hosts sends packets to the multicast IP address 224.10.10.5/24.

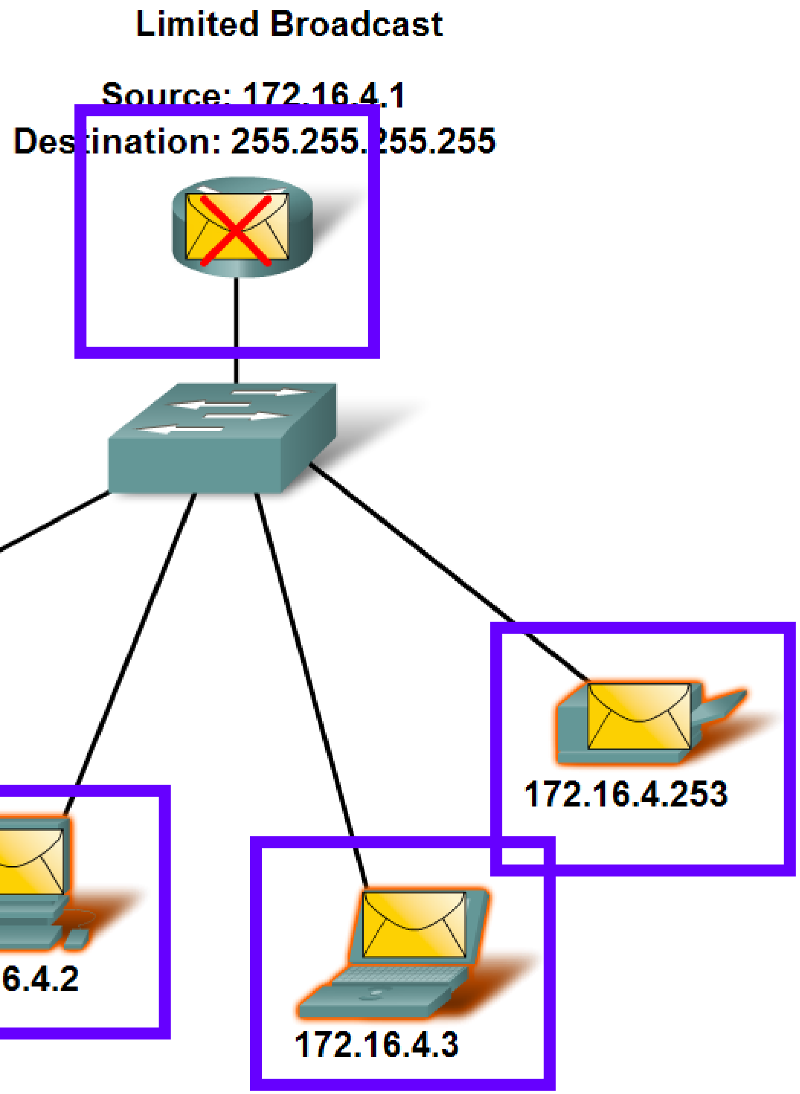
Multicast clients subscribe to the multicast group and listen for packets destined to 224.10.10.5.



Broadcast Addresses

Directed broadcast is sent to all hosts on a specific network. An example destination IPv4 address is 192.168.1.**255** /24.

Limited broadcast is to all hosts on the local network. These packets use a destination IPv4 address **255.255.255.255**.



IPv4 Unicast, Broadcast, and Multicast

Unicast
Broadcast
Multicast

Packet Tracer – Investigate Unicast, Broadcast and Multicast Traffic

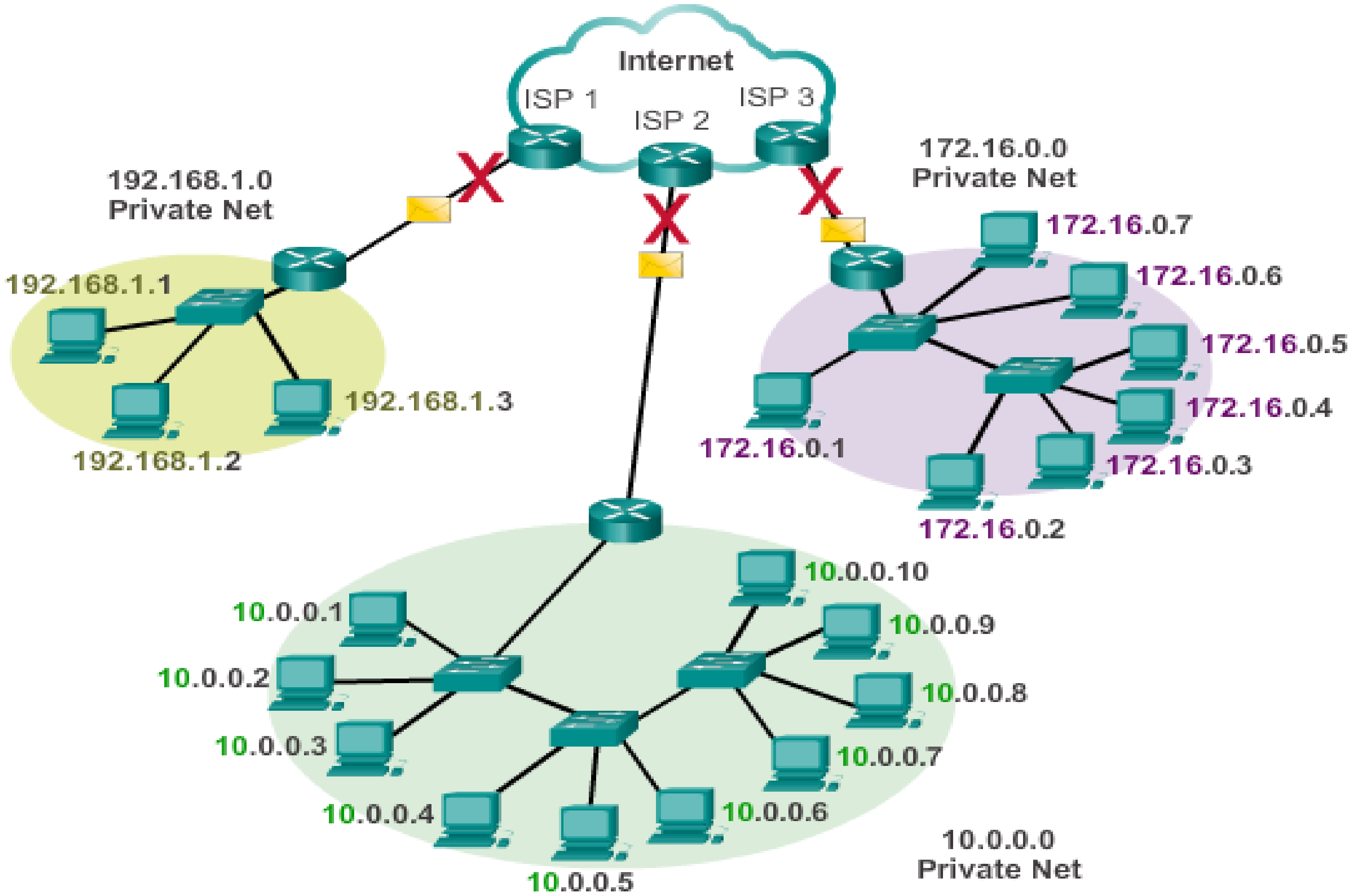
Generate Unicast Traffic
Generate Broadcast Traffic
Investigate Multicast Traffic

Types of IPv4 Addresses

Private vs.
Public
Addresses

Private vs. Public Addresses

Private addresses cannot be routed over the Internet



Special Use IPv4 Addresses

- Loopback address:
  - **127.0.0.1**
  - **127.0.0.0** – **127.255.255.255**
  - Hosts use to direct traffic to themselves.

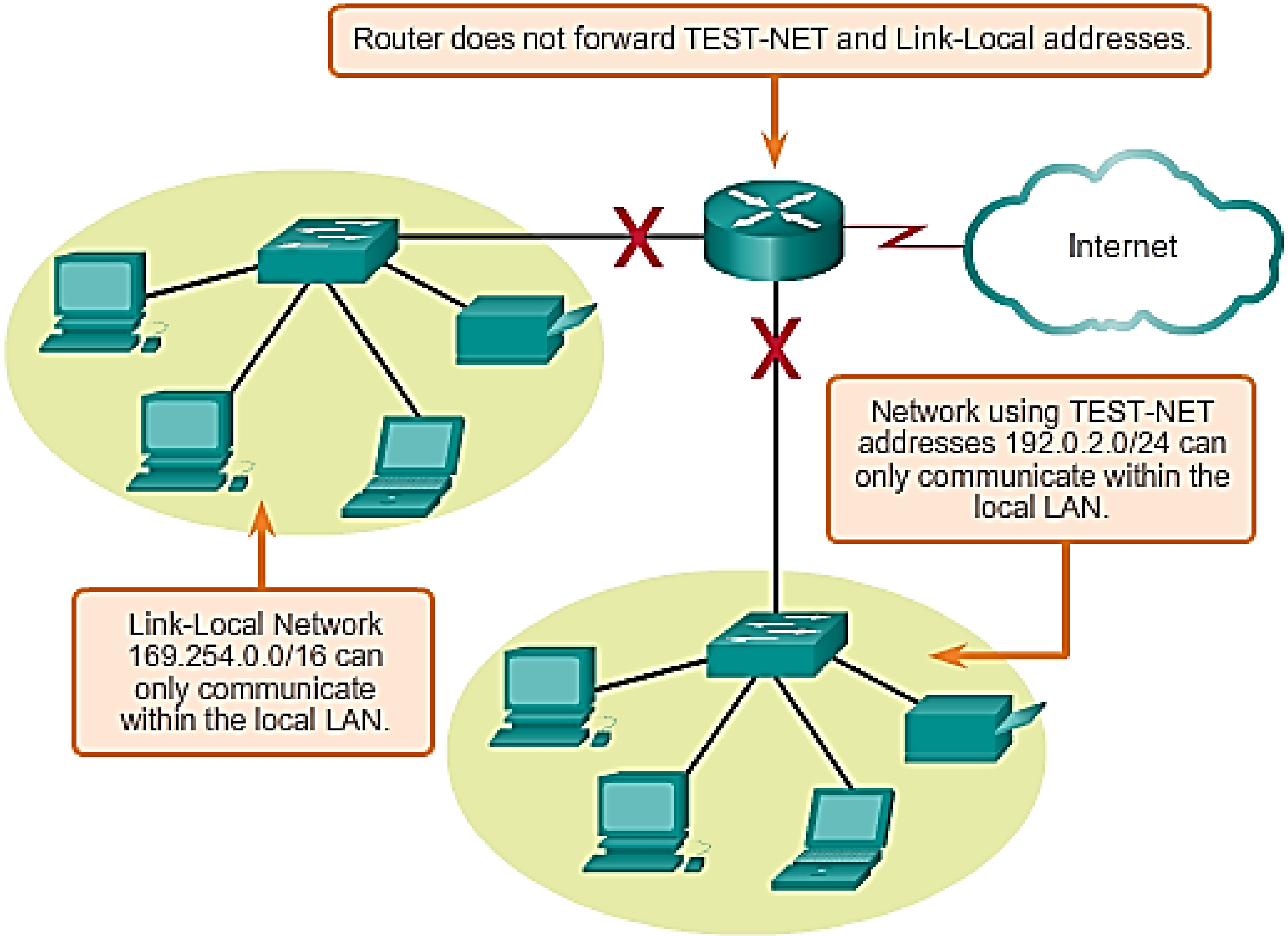
Link-Local addresses:

- **169.254.0.0/16**
- **169.254.0.0** – **169.254.255.255**
- Host can automatically assign itself an address if it has none.

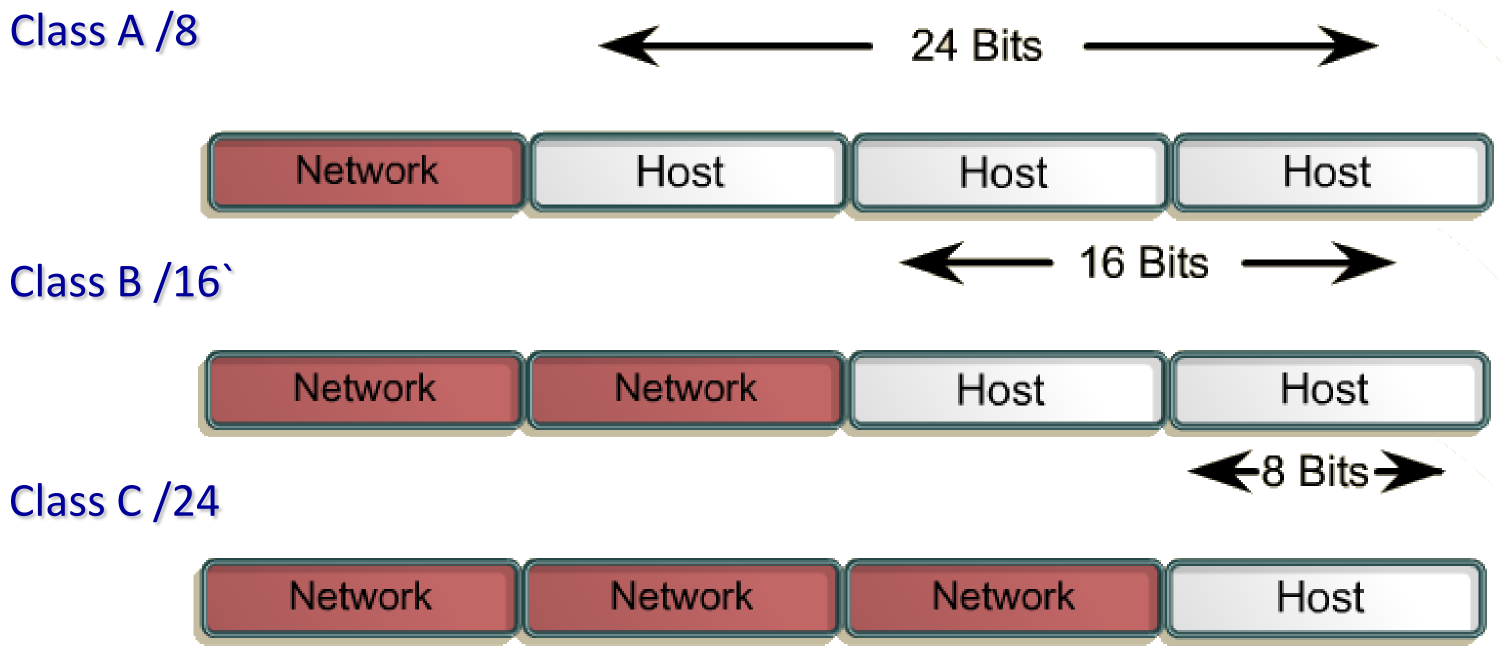
TEST-NET addresses:

- **192.0.2.0 to 192.0.2.255 (192.0.2.0 /24)**

Special Use IPv4 Addresses



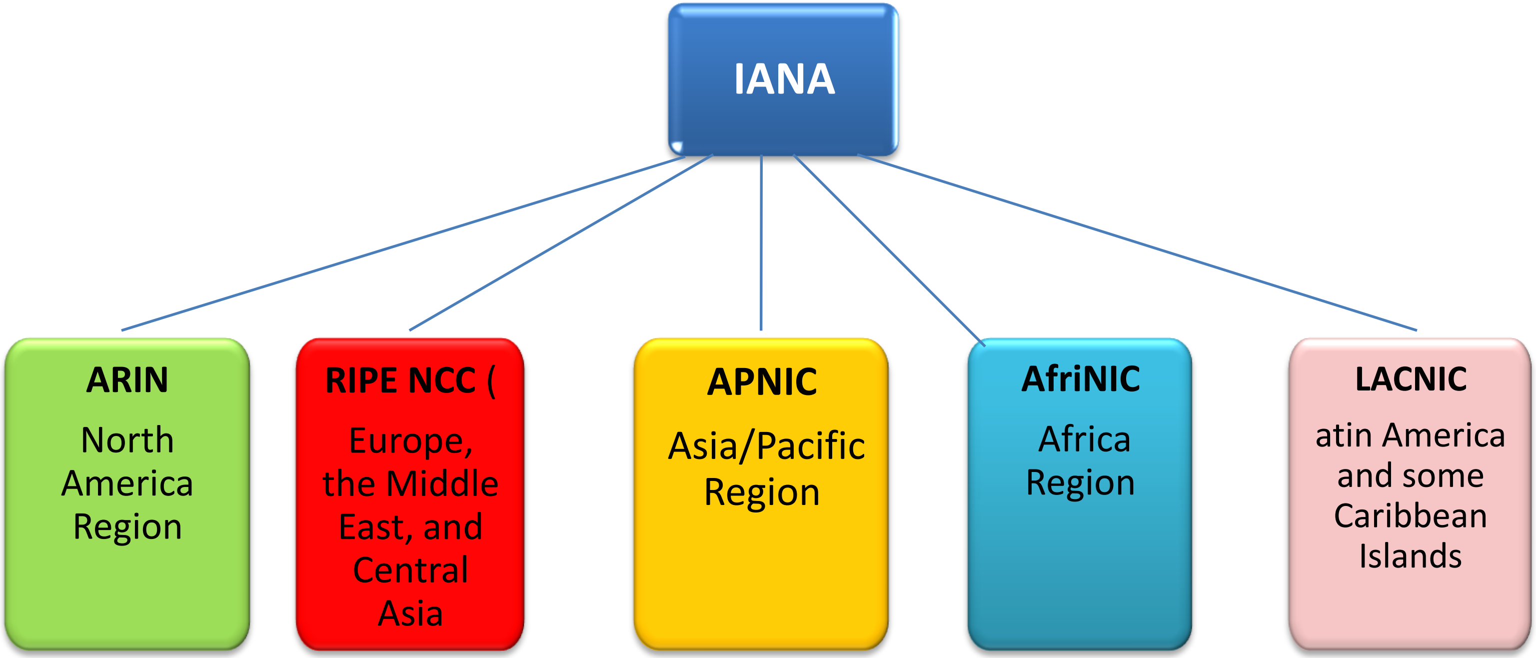
Legacy Classful Addresses



- **Class A, B, and C addresses**: **0.0.0.0** - **223.255.255.255**
- **Multicast addresses**: **224.0.0.0** - **239.255.255.255**
- **Experimental addresses**: **240.0.0.0** - **255.255.255.254**

Assignment of IP Addresses

- Internet Assigned Numbers Authority (IANA) manages the allocation of IPv4 and IPv6 addresses. IPv4 address space are allocated to various other registries to manage for particular purposes or for regional areas. These registration companies are called Regional Internet Registries (RIRs), as shown in the figure.



Types of IPv4 Addresses

Private vs. Public Assignment of IP Addresses

Using Windows Calculator with Network Addresses

Convert Between Numbering Systems

Converting IPv4 Addresses to Binary

Convert IPv4 Addresses from Dotted Decimal to Binary

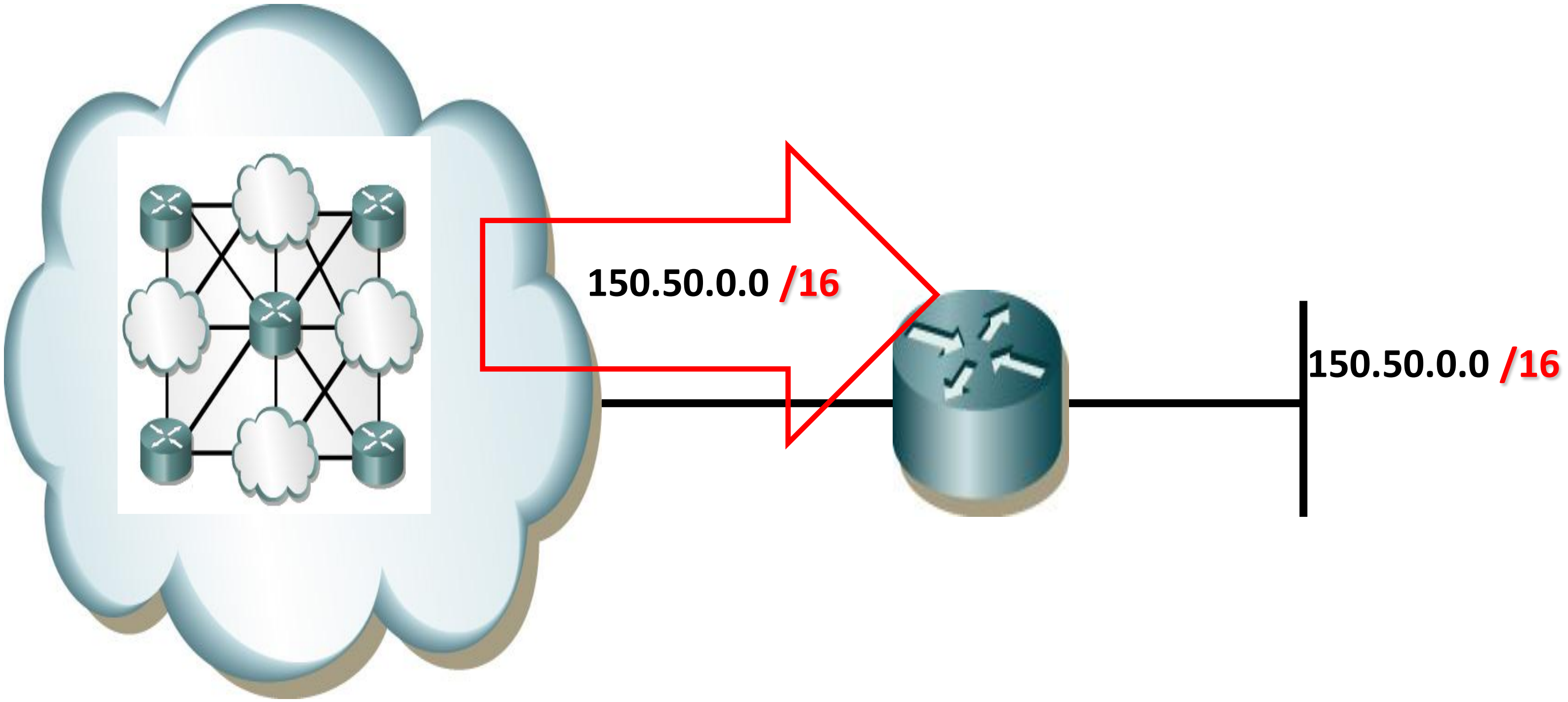
Bitwise ANDing

Network Address Calculation

Network Segmentation

Large Networks

Large Networks



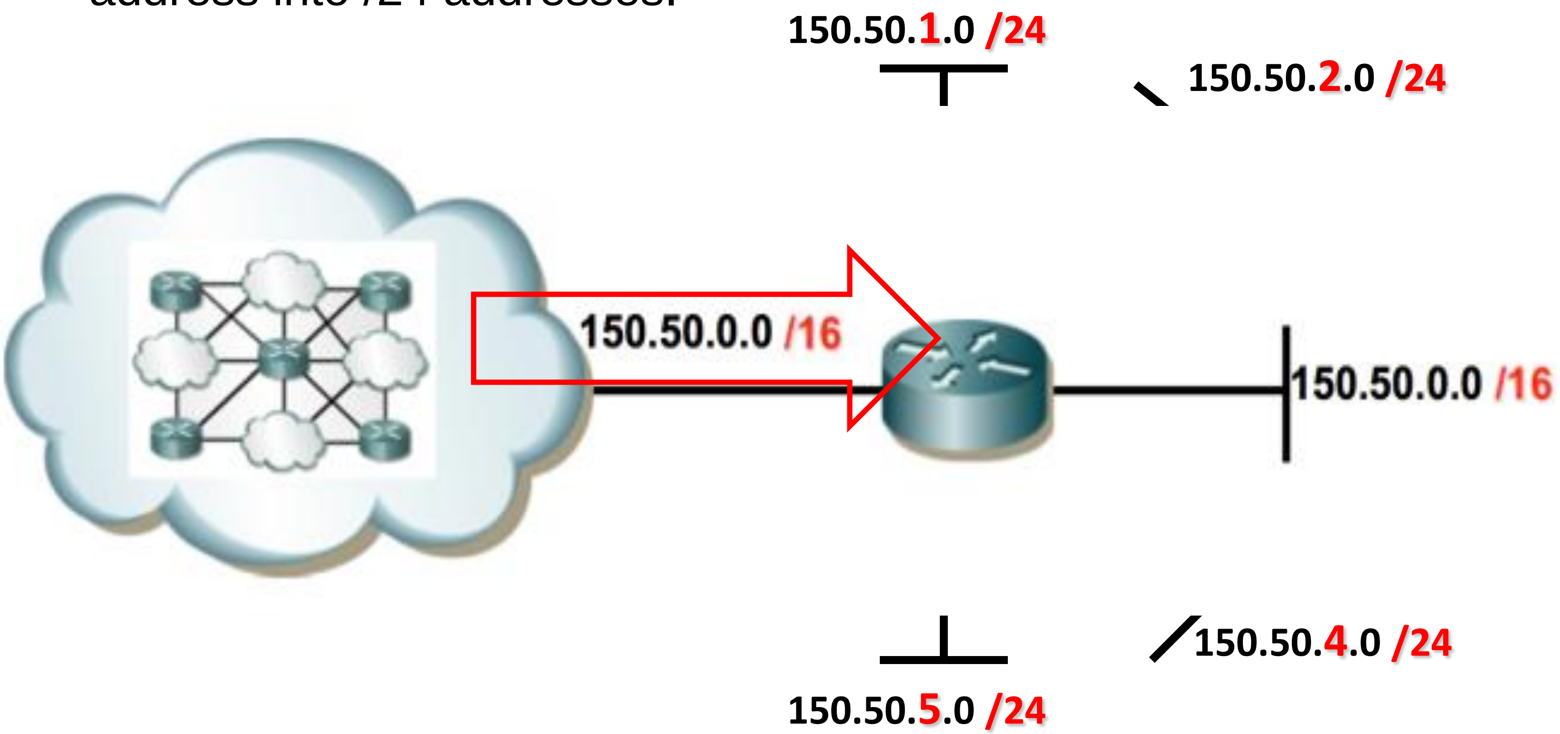
- In large networks, a flat network configuration creates major issues.
  - ❑Excessive broadcast traffic (e.g., DHCP, ARP) in one domain.
  - ❑Manageability and security

•As well, a network address with a /16 mask can support 65,534 host addresses on the same network.

- ❑What network would ever need to connect that many hosts on one network?

Subnetting

- Large networks need to be segmented into smaller sub-networks called "**Subnets**".
  - In the example, 5 subnets are created by subnetting the /16 network address into /24 addresses.



5 subnetworks capable of supporting 254 Hosts each.

Reasons for Subnetting

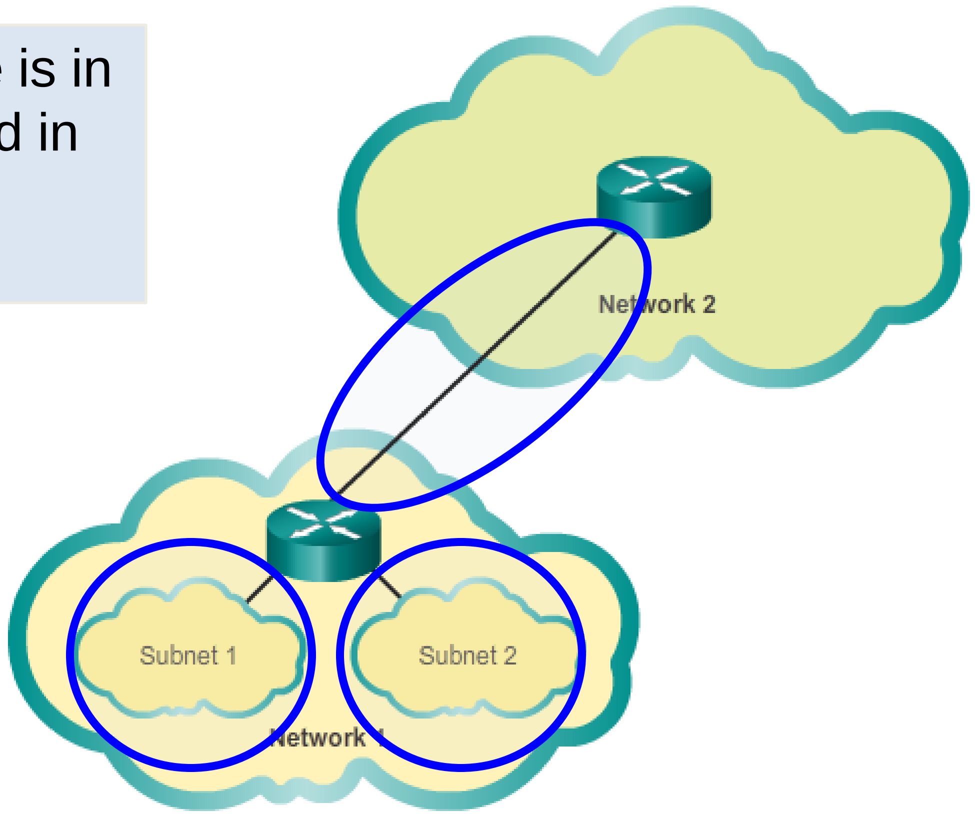
Segmenting networks in subnets creates smaller groups of devices and services in order to:

- Create smaller broadcast domains.
- Limit the amount of traffic on the other network segments.
- Provide low-level security.

Communication Between Subnets

- A router is required to subnet a network.
  - Each router interface is on a different subnet.
  - Devices on a subnet use the router interface as the default gateway.

Each router interface is in a different subnet and in its own broadcast domain.



Network Segmentation

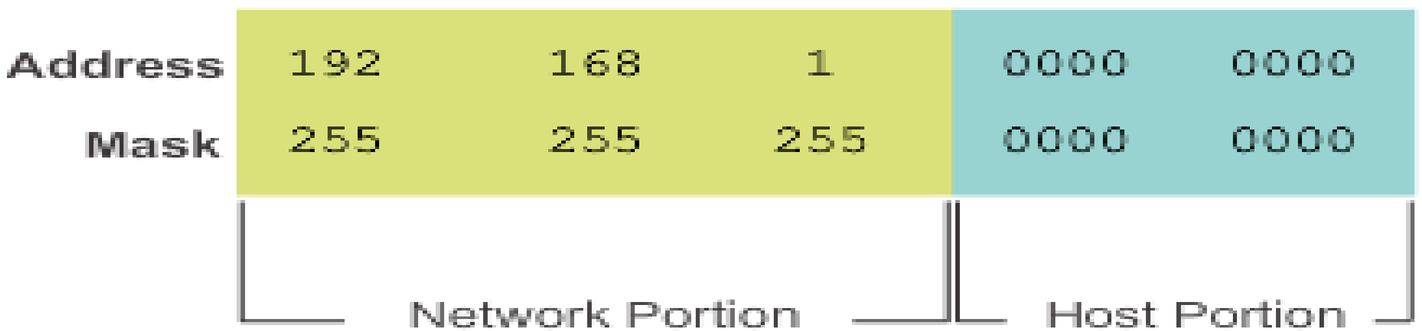
Reasons for Subnetting

Subnetting an IPv4 Network

Basic Subnetting

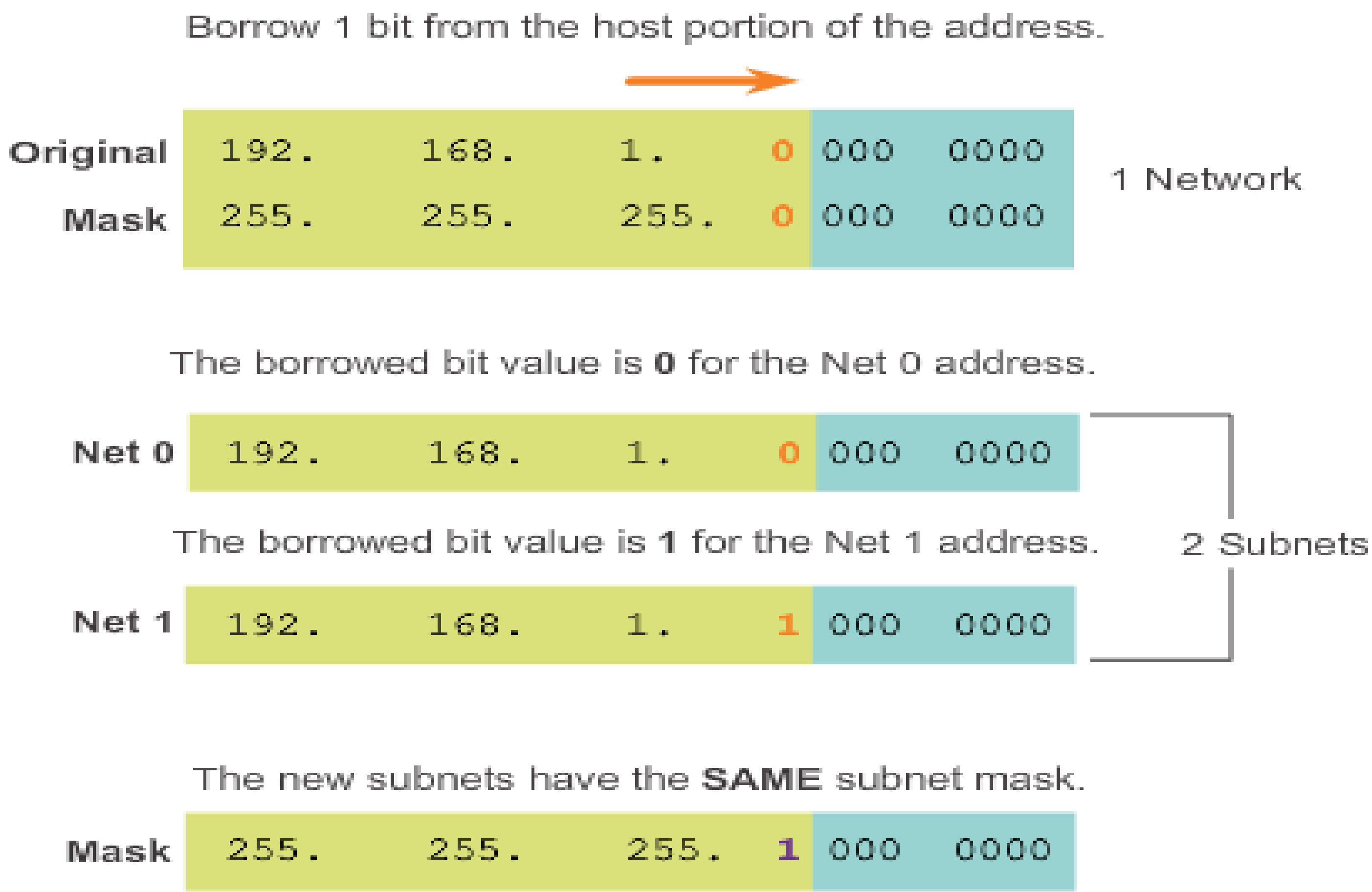
Basic Subnetting

192.168.1.0/24 Network



With no host bits borrowed, the host portion of both the network address and mask are all 0 bits.

Basic Subnetting



Basic Subnetting

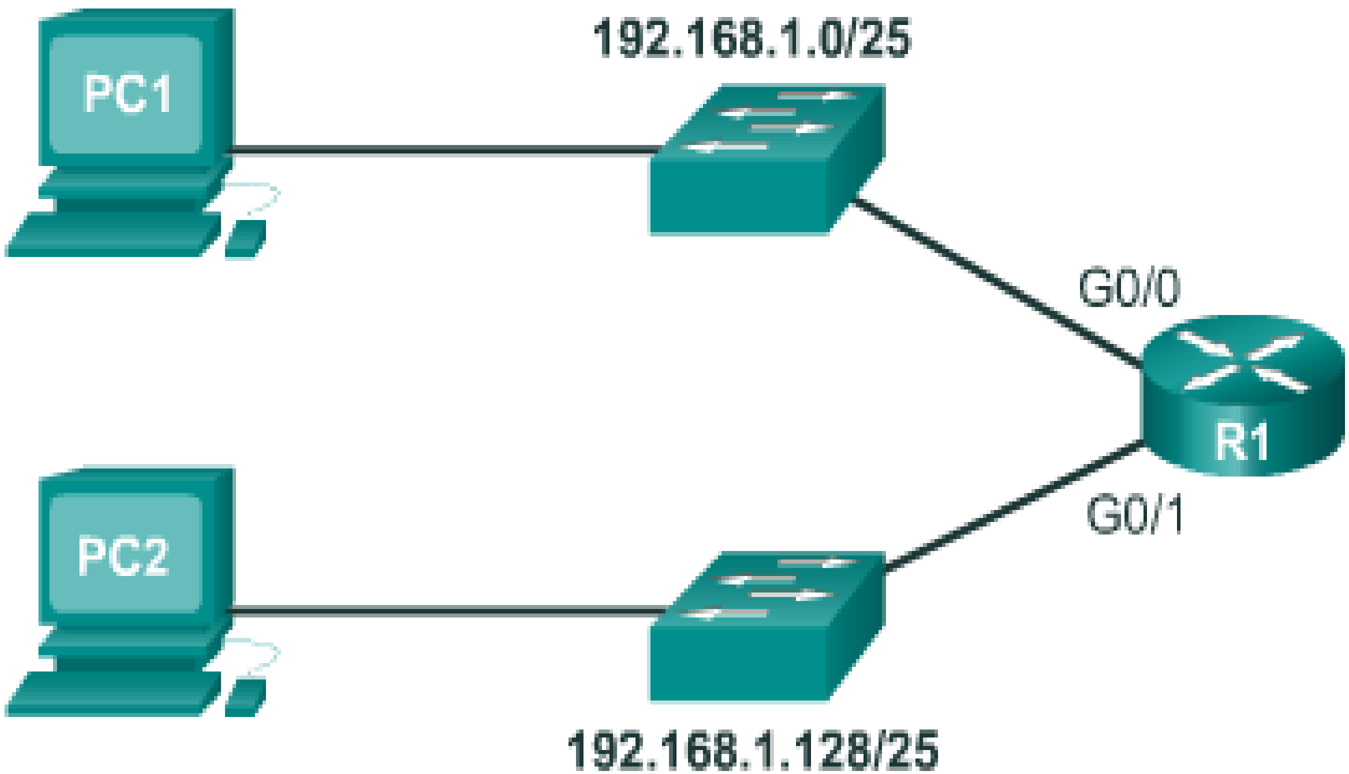
Decimal Representation

Original	192.	168.	1.	0	000	0000	Network: 192.168.1.0/24
Mask	255.	255.	255.	0	000	0000	Mask: 255.255.255.0

Borrowing 1 bit creates 2 subnets with the same mask.

Net 0	192.	168.	1.	0	000	0000	Network: 192.168.1.0/25
Mask	255.	255.	255.	1	000	0000	Mask: 255.255.255.128
Net 1	192.	168.	1.	1	000	0000	Network: 192.168.1.128/25
Mask	255.	255.	255.	1	000	0000	Mask: 255.255.255.128

Subnets in Use



Subnets in Use

Address Range for 192.168.1.0/25 Subnet

Network Address

192.	168.	1.	0	000	0000	=	192.168.1.0

First Host Address

192.	168.	1.	0	000	0001	=	192.168.1.1

Last Host Address

192.	168.	1.	0	111	1110	=	192.168.1.126

Broadcast Address

192.	168.	1.	0	111	1111	=	192.168.1.127

Subnets in Use

Address Range for 192.168.1.128/25 Subnet

Network Address

192.	168.	1.	1	000	0000	=	192.168.1.128

First Host Address

192.	168.	1.	1	000	0001	=	192.168.1.129

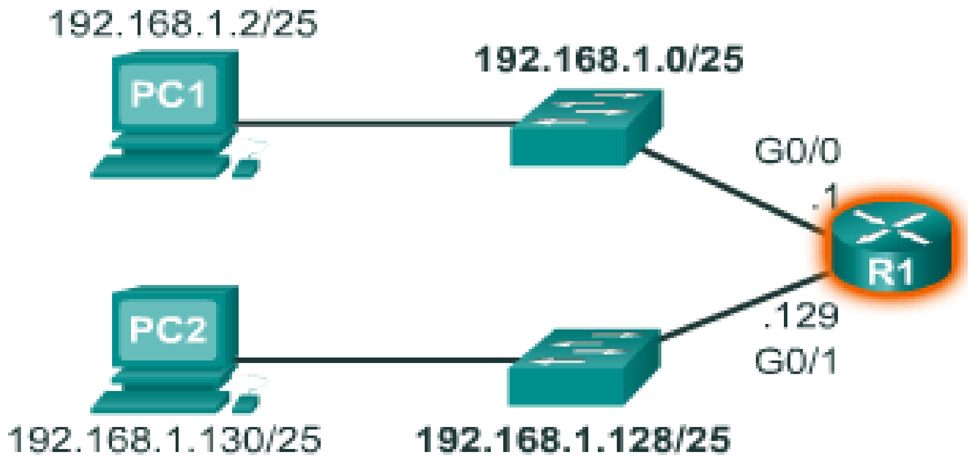
Last Host Address

192.	168.	1.	1	111	1110	=	192.168.1.254

Broadcast Address

192.	168.	1.	1	111	1111	=	192.168.1.255

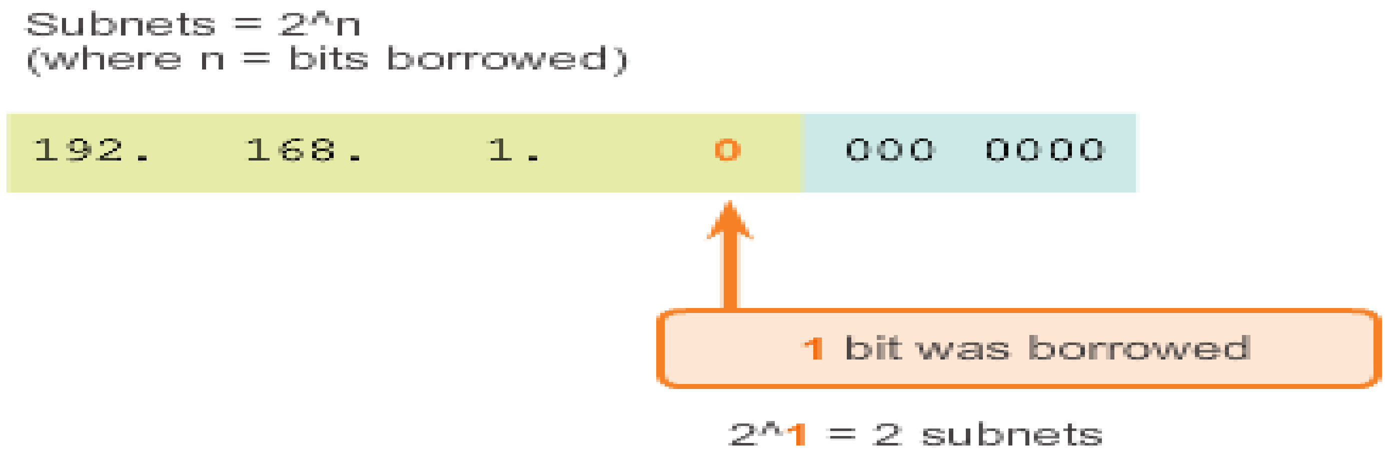
Subnets in Use



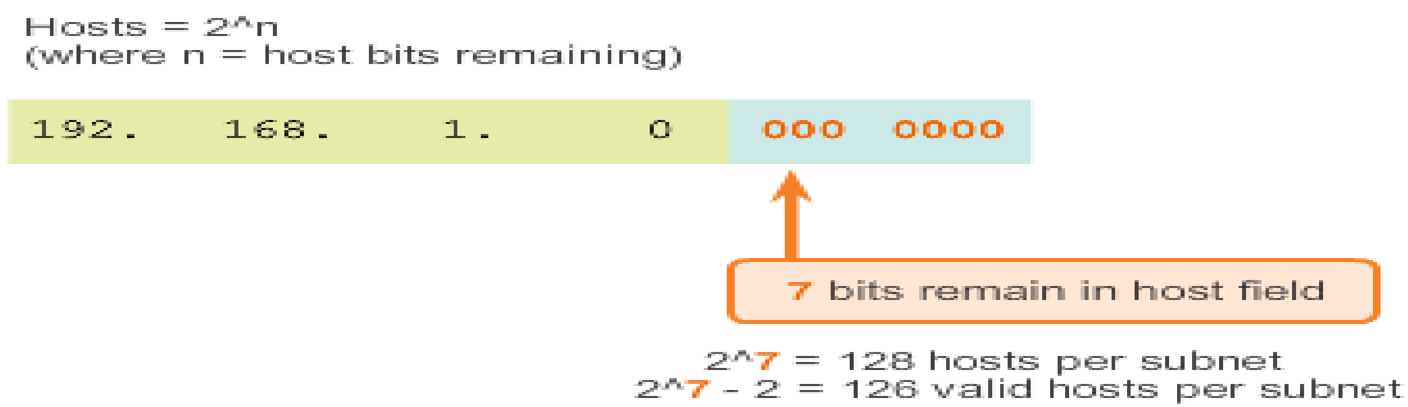

```
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.128
R1(config-if)#exit
R1(config)#interface gigabitethernet 0/1
R1(config-if)#ip address 192.168.1.129 255.255.255.128
```

Subnetting Formulas

- Calculate Number of Subnets



- Calculate Number of Hosts



Subnetting an IPv4 Network

Basic Subnetting

Calculating IPv4 Subnets

Calculate IPv4 Address Subnetting

Packet Tracer – Subnetting Scenario

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

Packet Tracer – Subnetting Scenario - 2

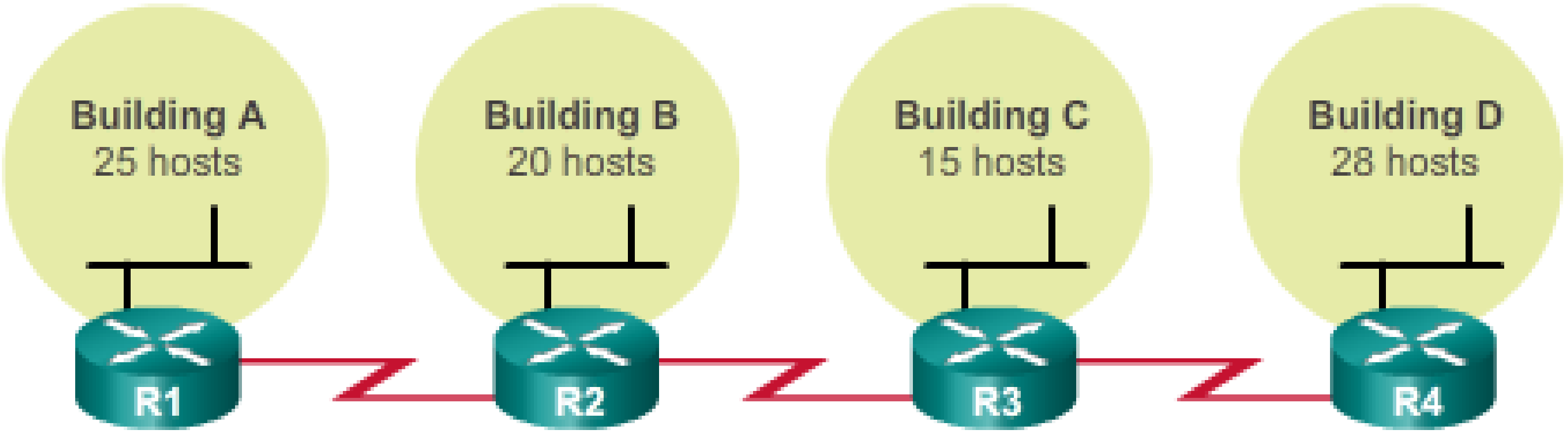
Design an IP Addressing Scheme
Assign IP Addresses to Network Devices and Verify

Variable Length Subnet Masking (VLSM)

Traditional Subnetting

Traditional Subnetting

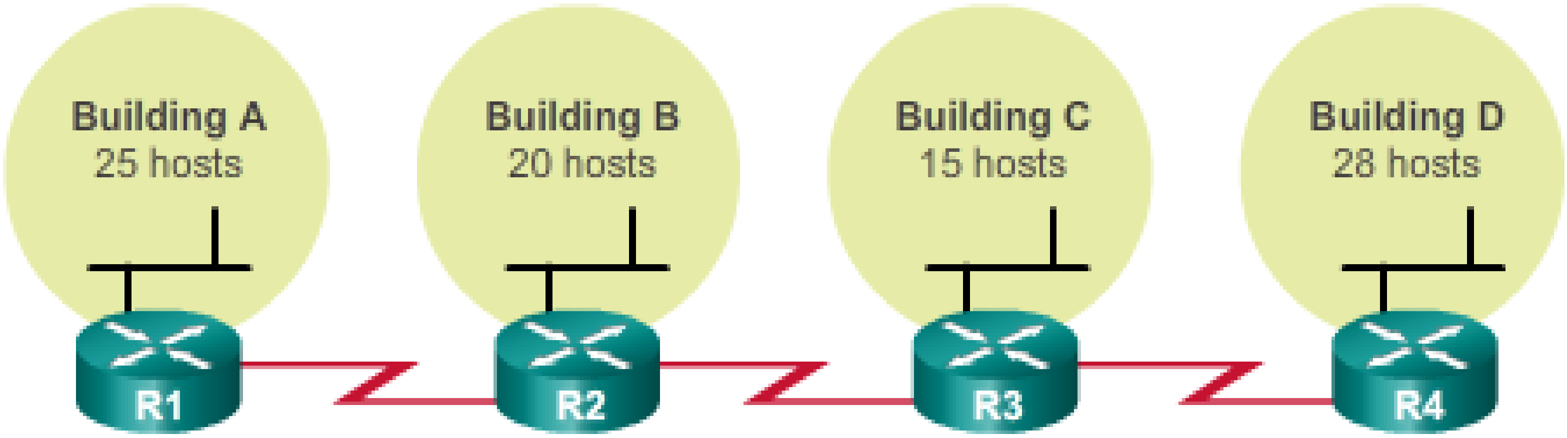
- So far, every subnet was the same size and all accommodated the same number of hosts.
  If all the subnets have the same requirements for the number of hosts, these fixed size address blocks would be efficient.



- For example, how many subnets are required?
  7 subnets of varying size.

Traditional Subnetting

- To meet the host requirement of the largest LAN we could borrow 3 bits (/27) to create 8 subnets of 30 hosts each.
  But it also wastes addresses on the point-to-point links and limits future growth by reducing the total number of subnets available.



- Solution:
  “Subnet a subnet” using **Variable Length Subnet Mask (VLSM)**.

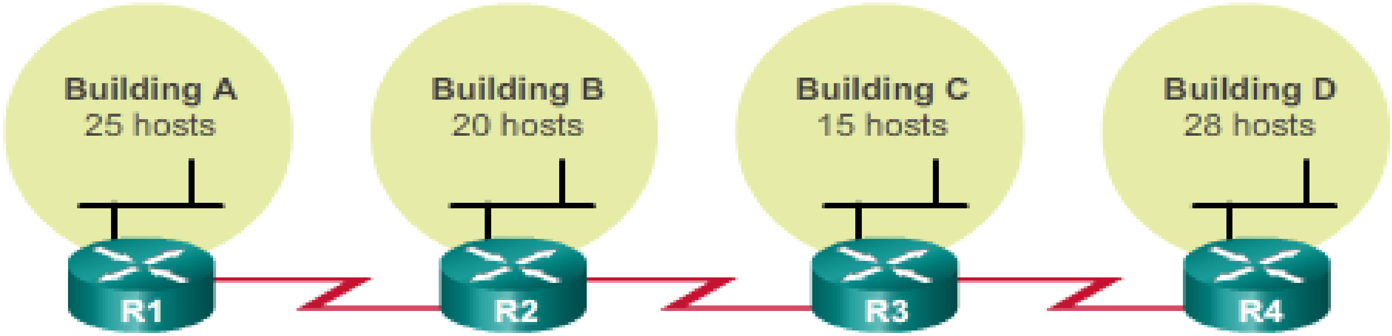
Special Use IPv4 Addresses

- VLSM allows a network space to be divided in unequal parts.
- With VLSM the subnet mask will vary depending on how many bits have been borrowed for a particular subnet, thus the “variable” part of the VLSM.
- VLSM enables a network number to be configured with different subnet masks on different interfaces.
- Allows for more hierarchical levels within an addressing plan.

  Allows for better route summarization.

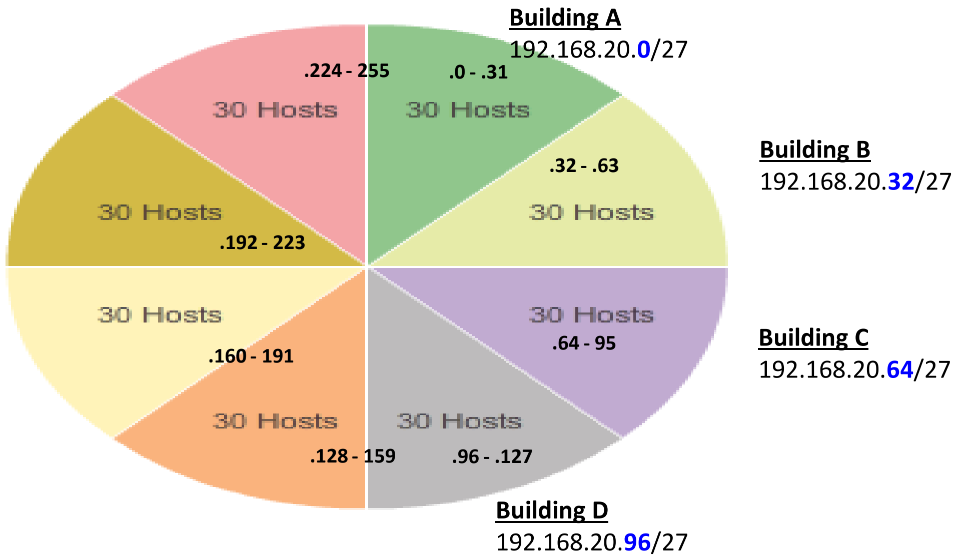
VLSM Example

The four LANs in our previous example can be accommodated using a /27 subnet mask.



VLSM Example

- This would create subnets with increments of 32, therefore:

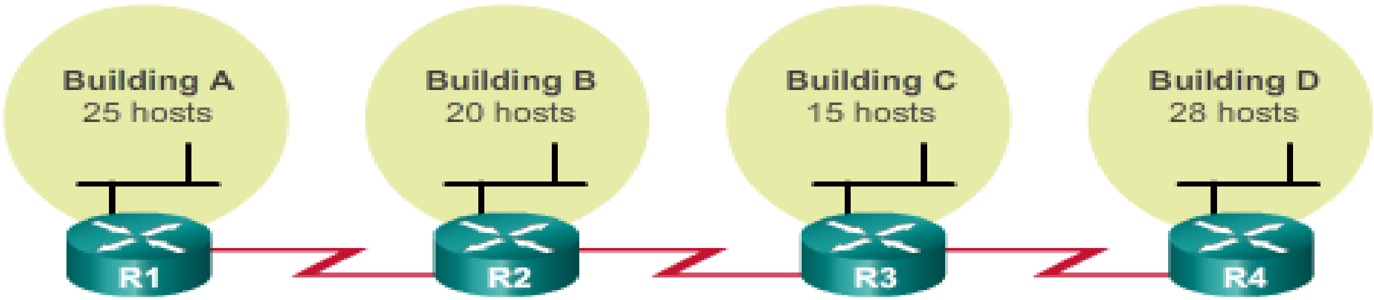


	11000000.10101000.00010100.00000000	192.168.20.0/24	
0	11000000.10101000.00010100.00000000	192.168.20.0/27	LANs A, B, C, D
1	11000000.10101000.00010100.00100000	192.168.20.32/27	
2	11000000.10101000.00010100.01000000	192.168.20.64/27	
3	11000000.10101000.00010100.01100000	192.168.20.96/27	
4	11000000.10101000.00010100.10000000	192.168.20.128/27	Unused / Available
5	11000000.10101000.00010100.10100000	192.168.20.160/27	
6	11000000.10101000.00010100.11000000	192.168.20.192/27	
7	11000000.10101000.00010100.11100000	192.168.20.224/27	

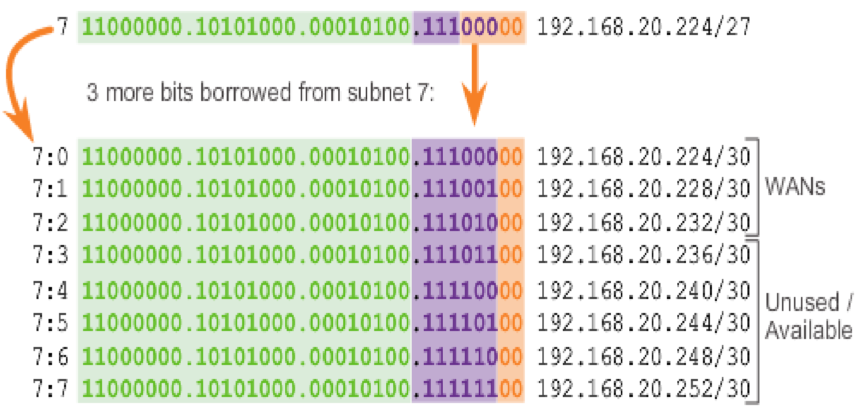
Basic subnets

VLSM Example

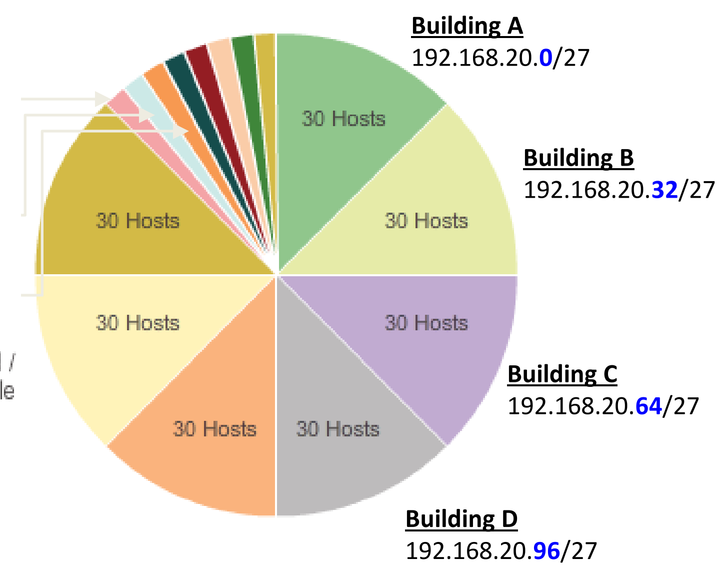
- The WAN interfaces of the routers are assigned the IP addresses and mask for the /30 subnets (2 hosts).



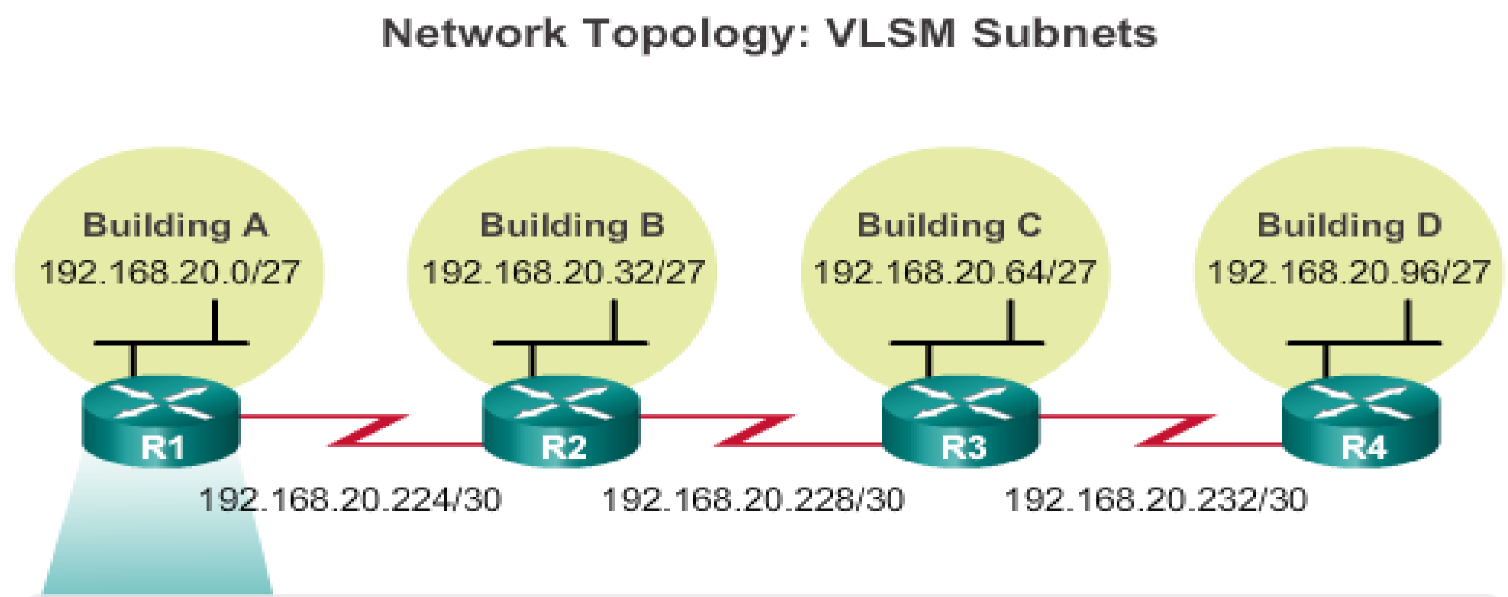
- In this example, the last subnet is subnetted into /30 subnets to accommodate WAN interfaces:



Subnetting a subnet

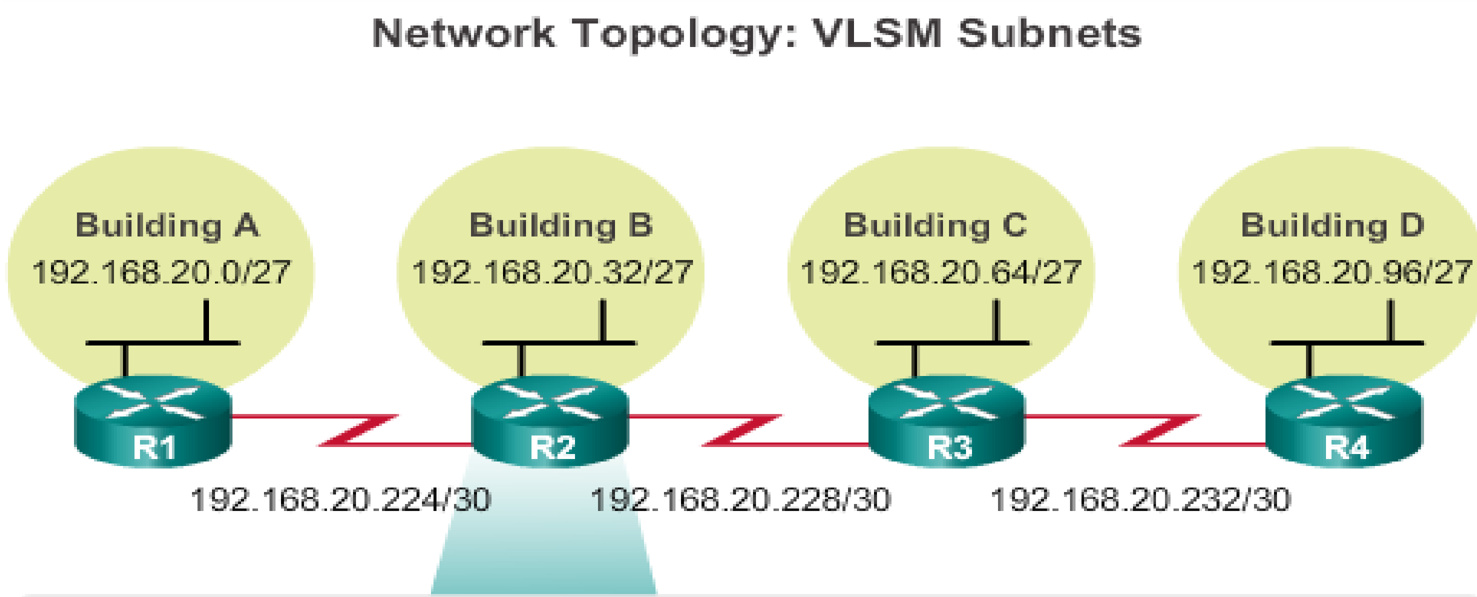


VLSM Example




```
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ip address 192.168.20.1 255.255.255.224
R1(config-if)#exit
R1(config)#interface serial 0/0/0
R1(config-if)#ip address 192.168.20.225 255.255.255.252
R1(config-if)#end
R1#
```

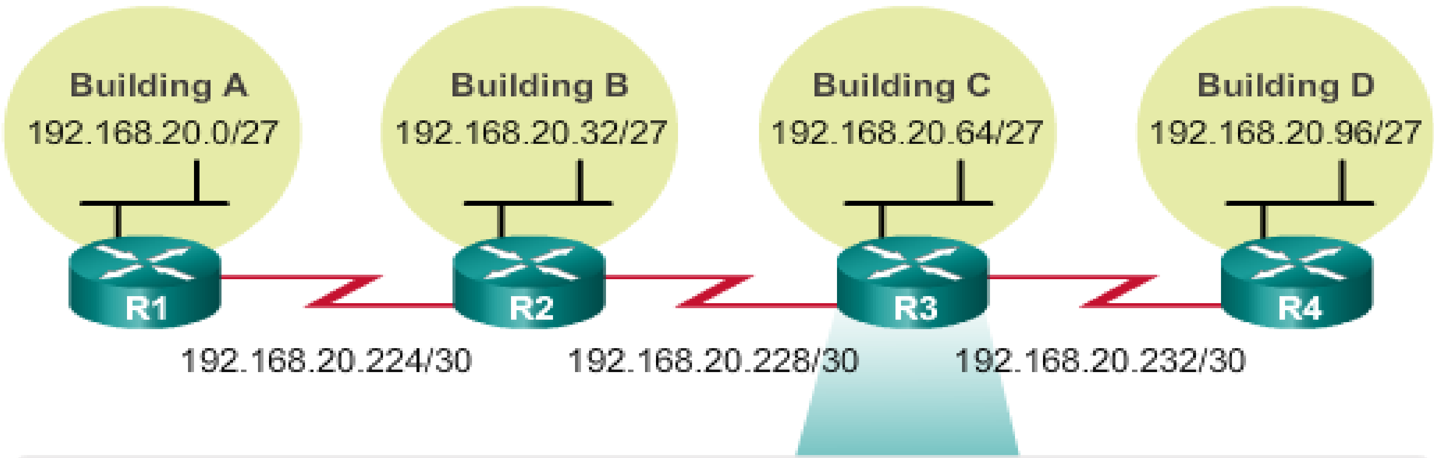
VLSM Example




```
R2(config)#interface gigabitethernet 0/0
R2(config-if)#ip address 192.168.20.33 255.255.255.224
R2(config-if)#exit
R2(config)#interface serial 0/0/0
R2(config-if)#ip address 192.168.20.226 255.255.255.252
R2(config-if)#exit
R2(config)#interface serial 0/0/1
R2(config)#ip address 192.168.20.229 255.255.255.252
R2(config-if)#end
R2#
```

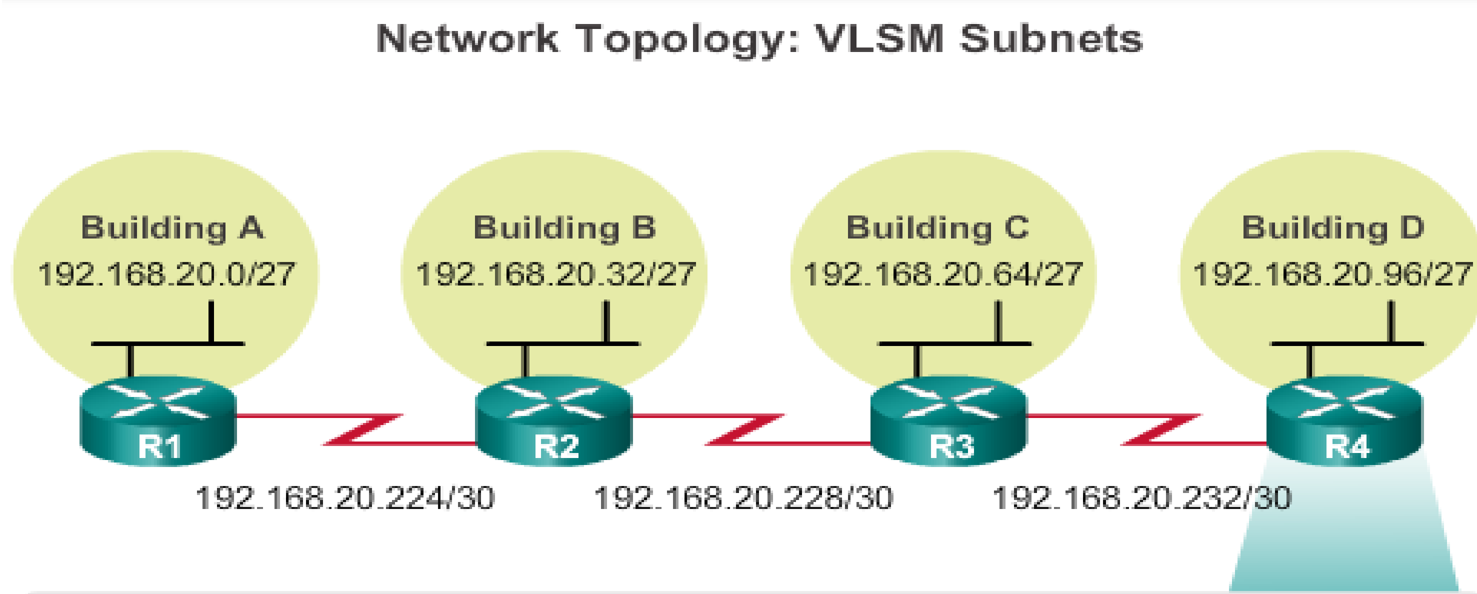
VLSM Example

Network Topology: VLSM Subnets




```
R3(config)#interface gigabitethernet 0/0
R3(config-if)#ip address 192.168.20.65 255.255.255.224
R3(config-if)#exit
R3(config)#interface serial 0/0/0
R3(config-if)#ip address 192.168.20.230 255.255.255.252
R3(config-if)#exit
R3(config)#interface serial 0/0/1
R3(config)#ip address 192.168.20.233 255.255.255.252
R3(config-if)#end
R3#
```

VLSM Example




```
R4(config)#interface gigabitethernet 0/0
R4(config-if)#ip address 192.168.20.97 255.255.255.224
R4(config-if)#exit
R4(config)#interface serial 0/0/0
R4(config-if)#ip address 192.168.20.234 255.255.255.252
R4(config-if)#end
R4#
```

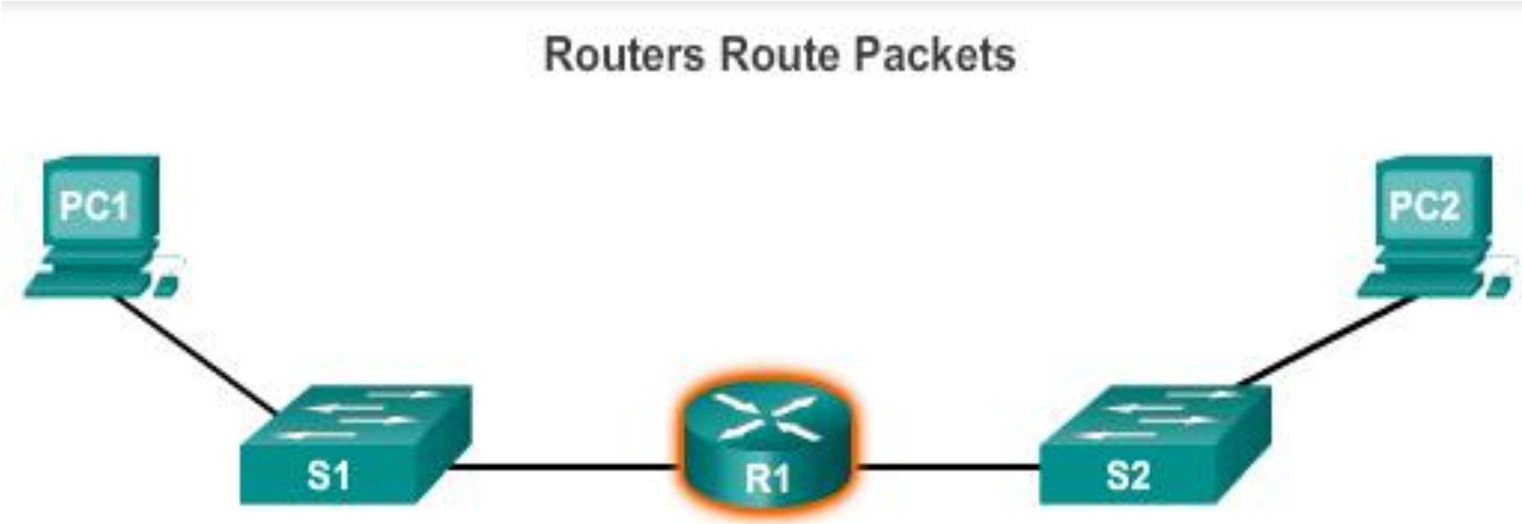
Variable Length Subnet Masking (VLSM)

VLSM Basics
VLSM in Practice

Anatomy of a Router

Why Routing

Why Routing



The router is responsible for the routing of traffic between networks

Functions of a Router

- Routers are computers
- Routers interconnects networks
- Routers choose best paths

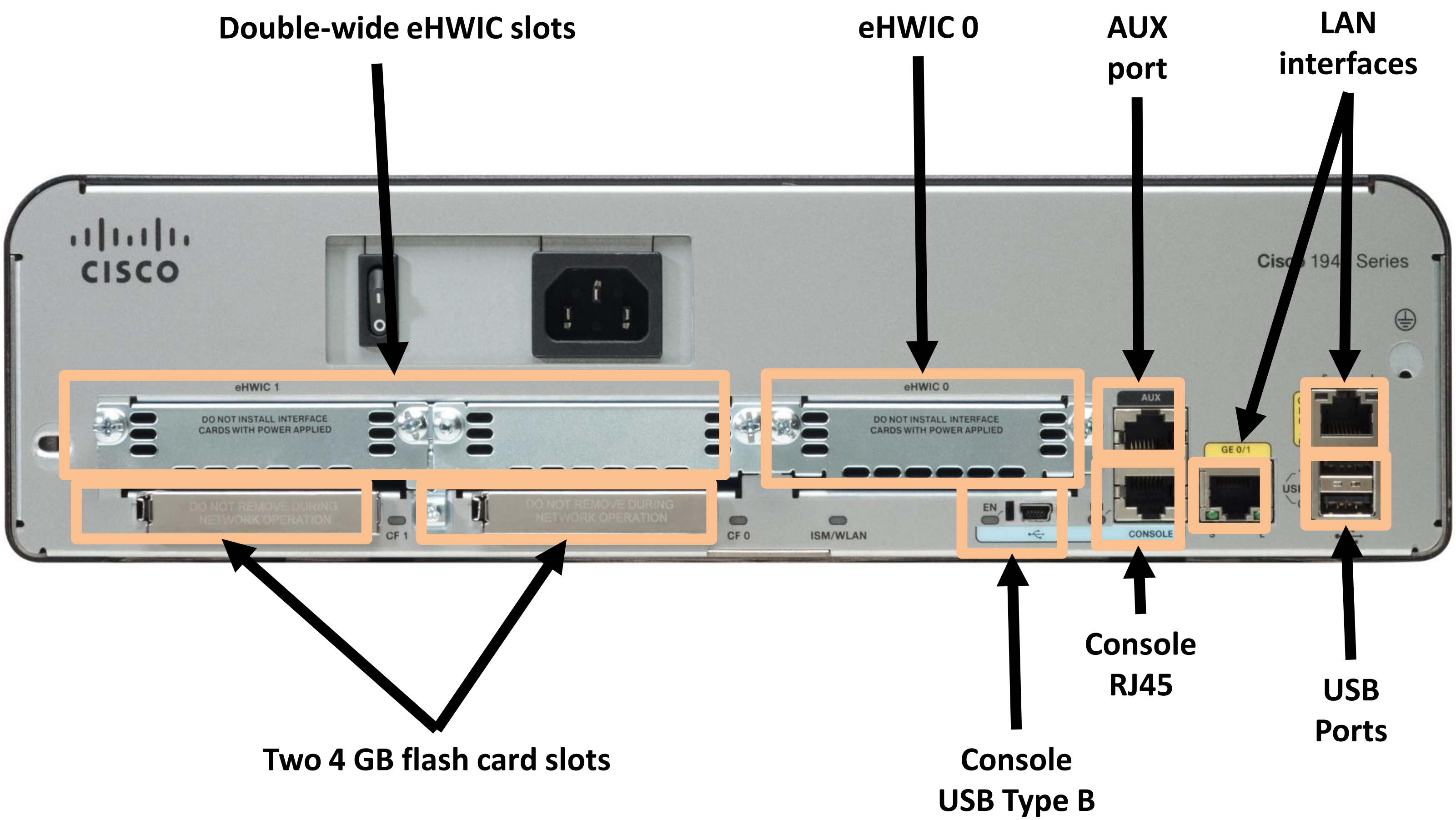
Router Components

- Routers are essentially computers and require:
  - ❑Operating systems (OS)
  - ❑Central processing units (CPU)
  - ❑Random-access memory (RAM)
  - ❑Read-only memory (ROM)
- Routers also have special memory that includes
  - ❑ Flash
  - ❑ Nonvolatile random-access memory (NVRAM).

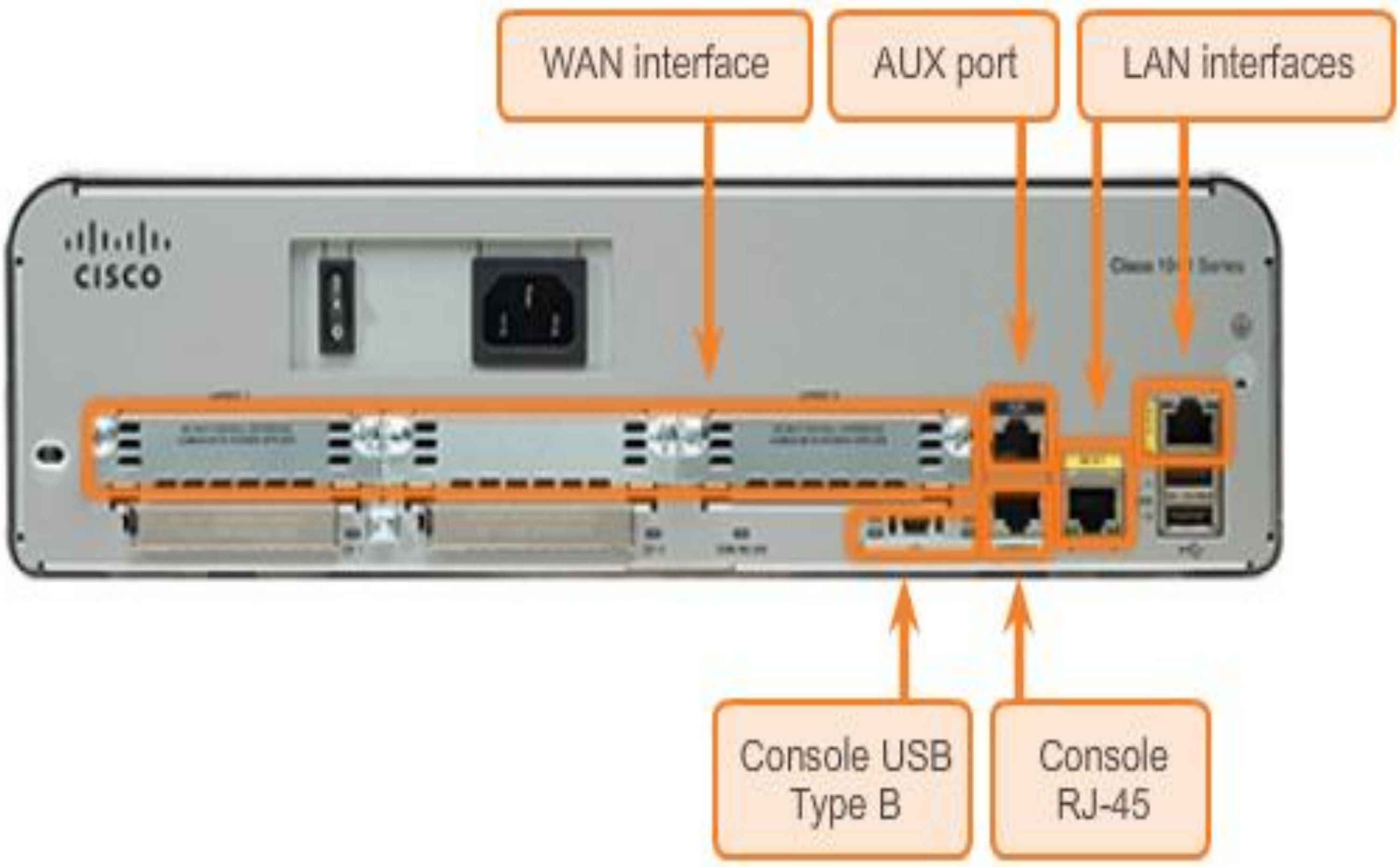
Router Memory

Memory	Volatile / Non-Volatile	Stores

Router Backplane



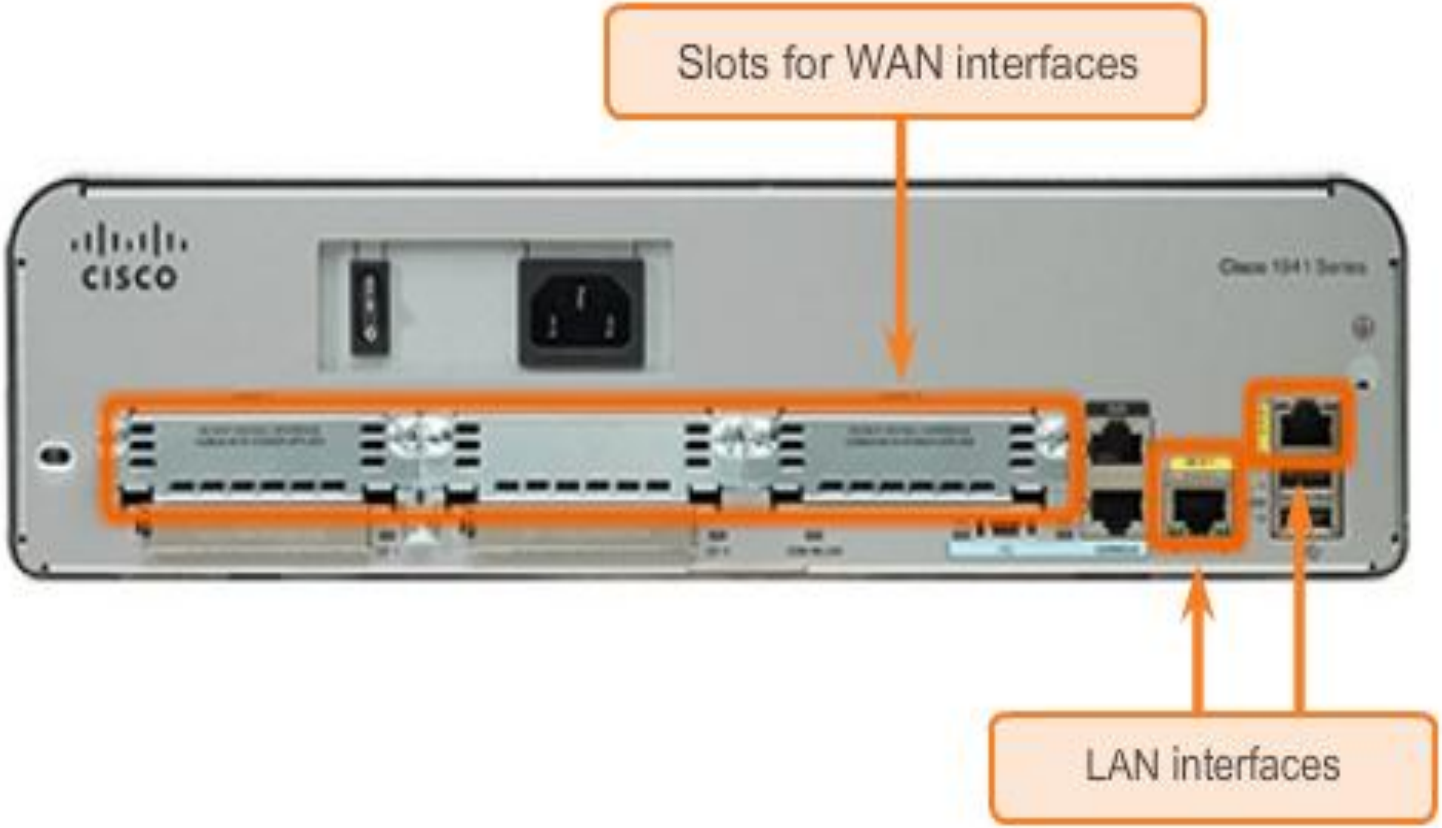
Connecting to a Router



Router Interfaces

- A router interface is a physical connector that enables a router to send or receive packets
- Types of router interfaces:
  - Ethernet
  - FastEthernet
  - Gigabit Ethernet
  - Serial
  - DSL
  - Cable
  - ISDN

LAN and WAN Interfaces



- Router interfaces can be grouped into two categories:
  - Ethernet LAN interfaces: Requires an IP address and enabled.
  - Serial WAN interfaces – Requires an IP address and enabled.

Anatomy of a Router

Functions of a Router
Router Components
Router Memory
Router Interfaces

Packet Tracer – Exploring Internetworking Devices

Identify Physical Characteristics of Internetworking Devices

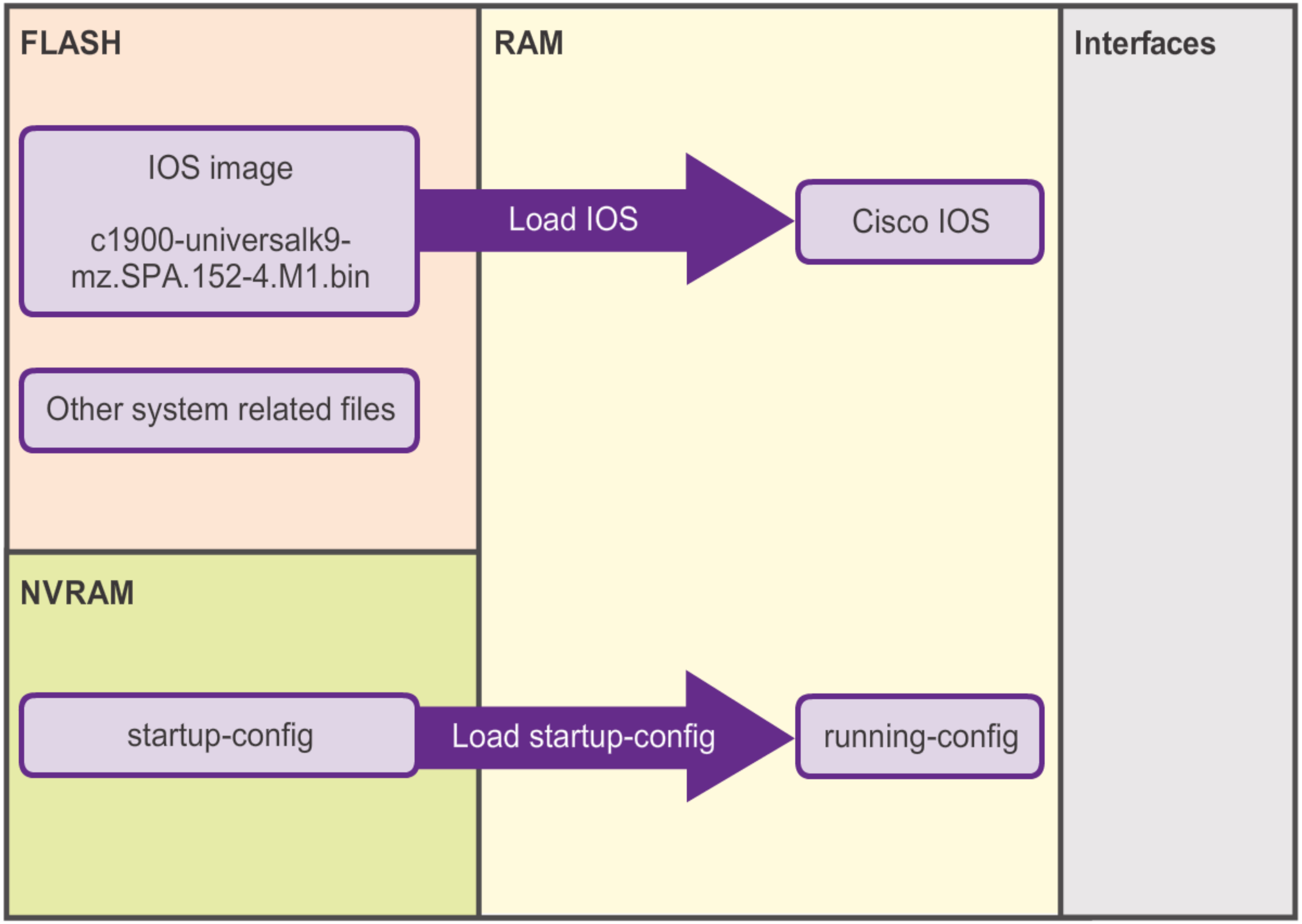
Select Correct Modules for Connectivity

Connect Devices

Router Bootup

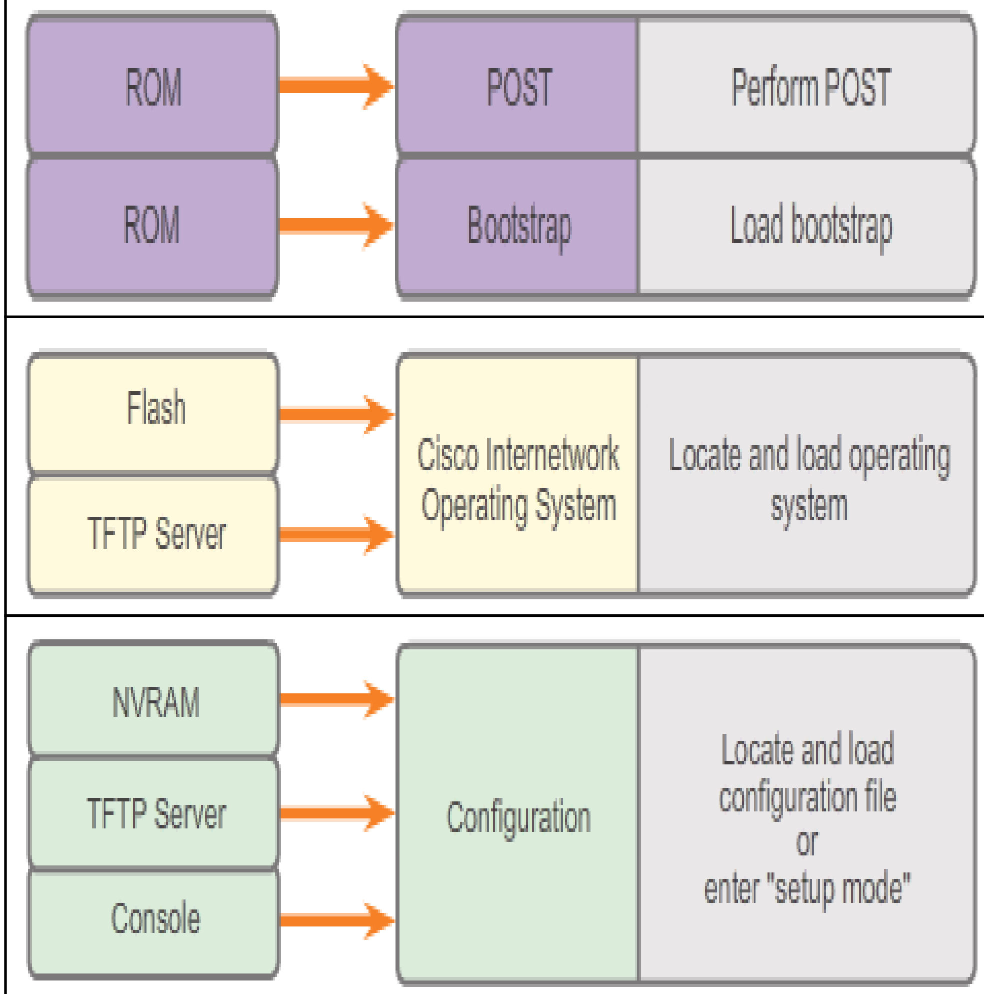
Cisco IOS

Cisco IOS



FLASH
RAM
Interfaces
IOS image
c1900-universalk9-
mz.SPA.152-4.M1.bin
Load IOS
Cisco IOS
Other system related files
NVRAM
startup-config
Load startup-config
running-config

Router Bootup Process



Router Bootup

Cisco IOS
Router Bootup
Process

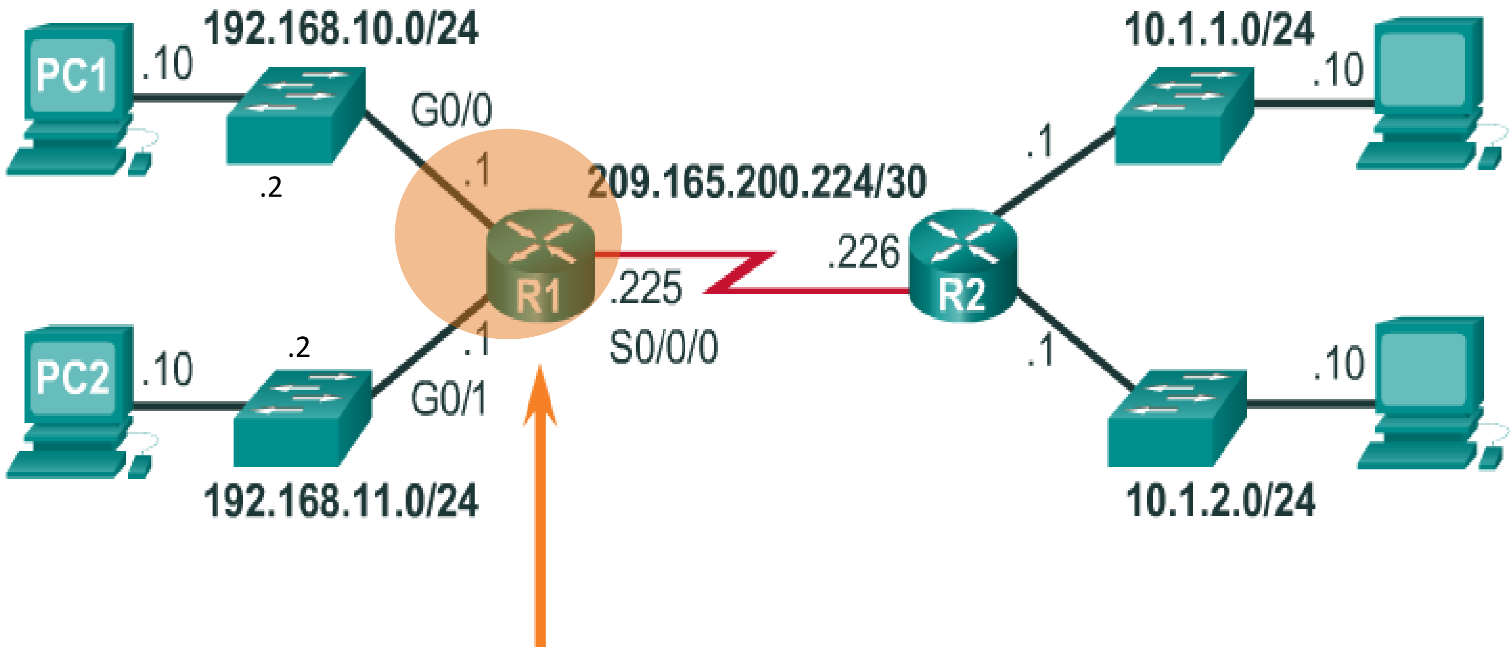
Configuring Routers

Basic Settings on a Router

Basic Settings on a Router

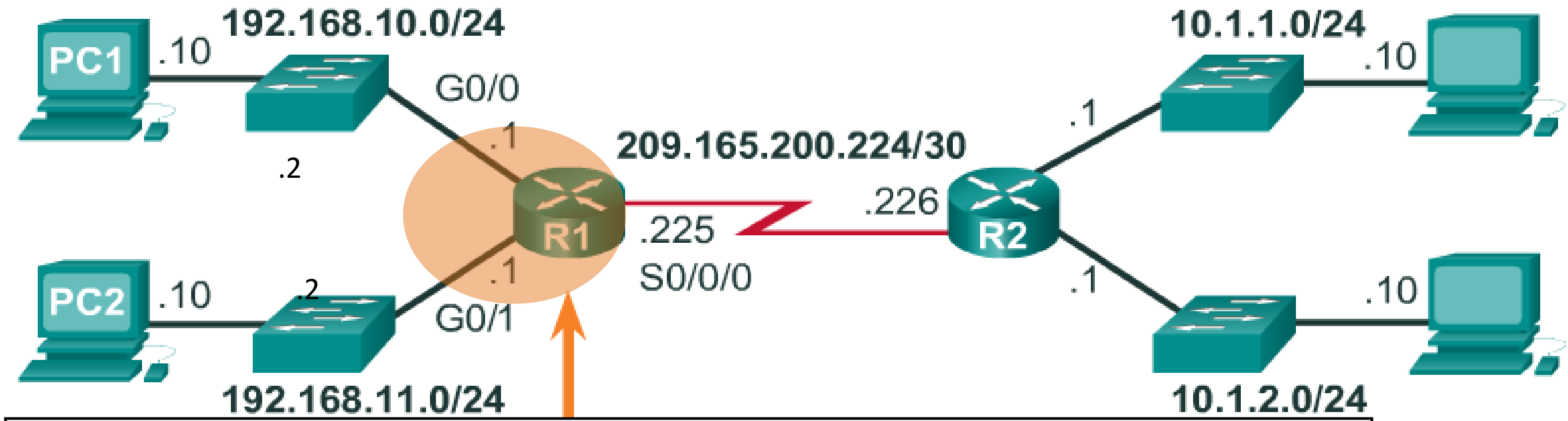
- Name the Device
- Secure Management Access
- Configure a Banner

Name the Device



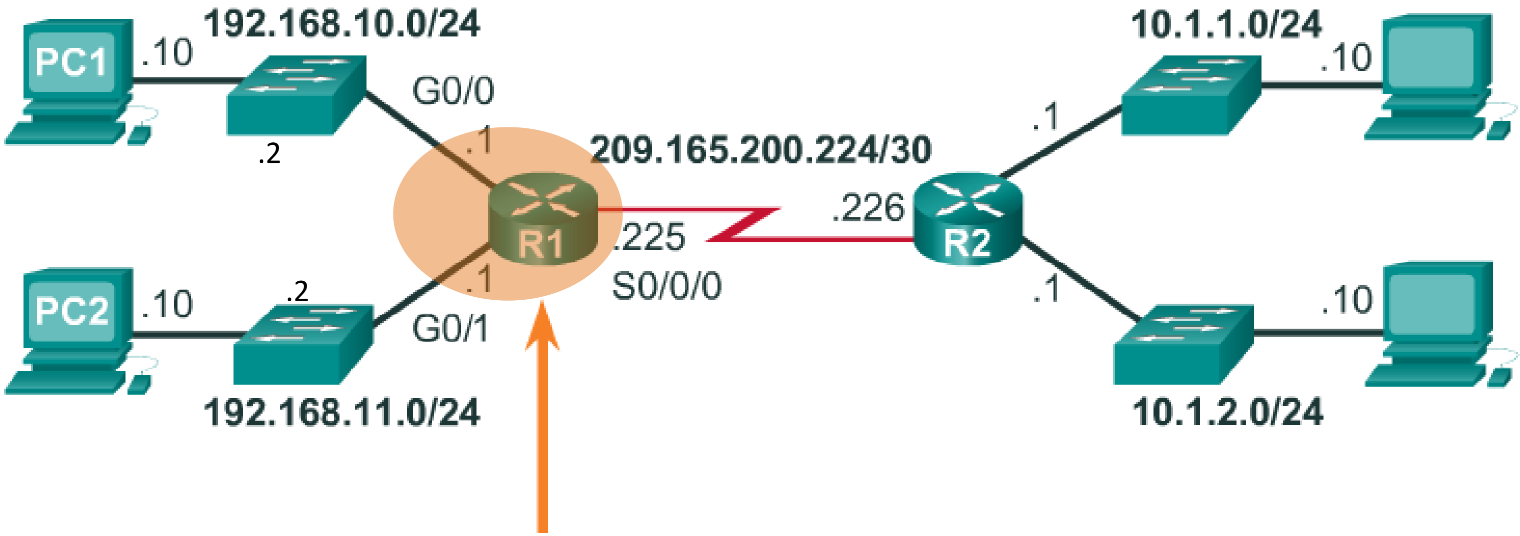

```
Router# configure terminal
Enter configuration commands, one per line.  End
with CNTL/Z.
Router(config)# hostname R1
R1(config)#
```

Secure Management Access




```
R1(config)# enable secret class
R1(config)# username admin secret class
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)# ip domain-name cisco.com
R1(config)# crypto key generate rsa 1024
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
R1(config-line)# login local
R1(config-line)# exit
R1(config)# service password-encryption
```

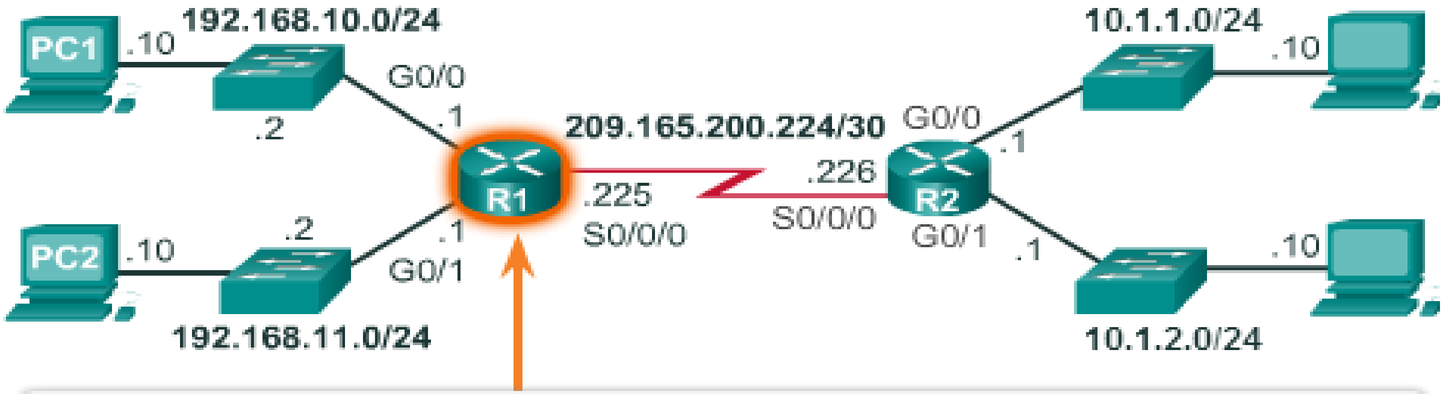
Configure a Banner




```
R1(config)# banner motd $ Authorized Access Only! $
R1(config)#
```

Configure an IPv4 Router Interface

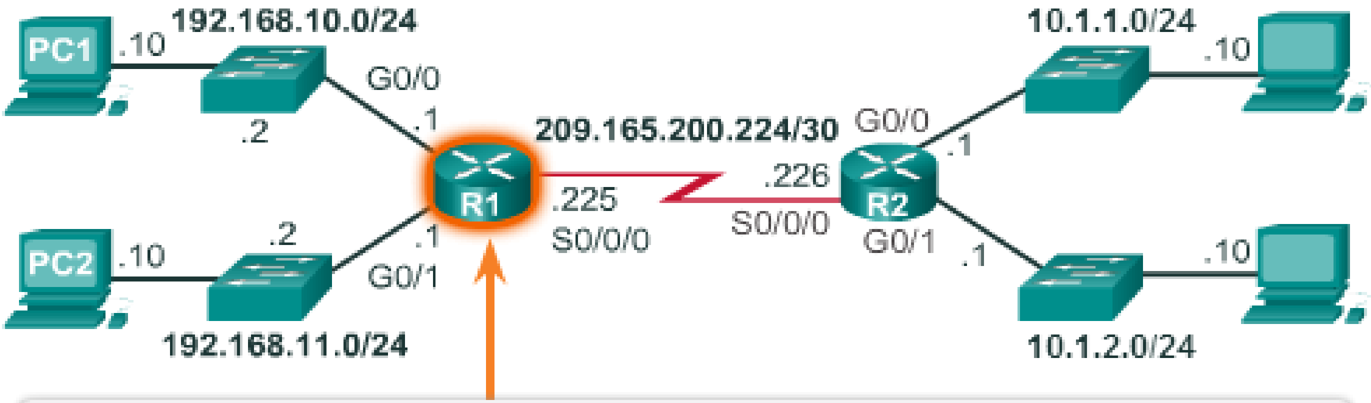
Configure the G0/0 Interface




```
R1(config)# interface gigabitethernet 0/0
R1(config-if)# description Link to LAN 1
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)#
*Jan 30 22:04:47.551: %LINK-3-UPDOWN: Interface
GigabitEthernet0/0, changed state to down
R1(config)#
*Jan 30 22:04:50.899: %LINK-3-UPDOWN: Interface
GigabitEthernet0/0, changed state to up
*Jan 30 22:04:51.899: %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet0/0, changed state to up
R1(config)#
```

Configure an IPv4 Router Interface

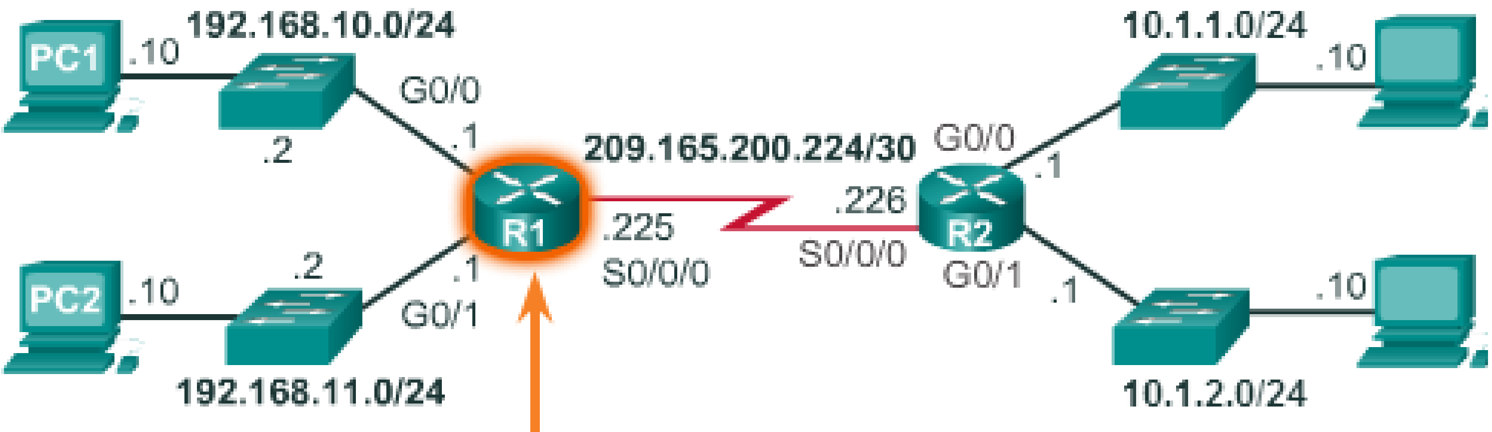
Configure the G0/1 Interface




```
R1(config)# interface gigabitethernet 0/1
R1(config-if)# description Link to LAN 2
R1(config-if)# ip address 192.168.11.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
*Jan 30 22:06:02.543: %LINK-3-UPDOWN: Interface
GigabitEthernet0/1, changed state to down
R1(config)#
*Jan 30 22:06:05.899: %LINK-3-UPDOWN: Interface
GigabitEthernet0/1, changed state to up
*Jan 30 22:06:06.899: %LINEPROTO-5-UPDOWN: Line
protocol on Interface GigabitEthernet0/1, changed state
to up
R1(config)#
```

Configure an IPv4 Router Interface

Configure the Serial 0/0/0 Interface




```
R1(config)# interface serial 0/0/0
R1(config-if)# description Link to R2
R1(config-if)# ip address 209.165.200.225 255.255.255.252
R1(config-if)# clockrate 128000
R1(config-if)# no shutdown
R1(config-if)# exit
*Jan 30 23:01:17.323: %LINK-3-UPDOWN: Interface Serial0/0/0,
changed state to down
R1(config)#
```

Configuring Routers

Basic Settings on a Router

Configuring IPv4 Router Interface

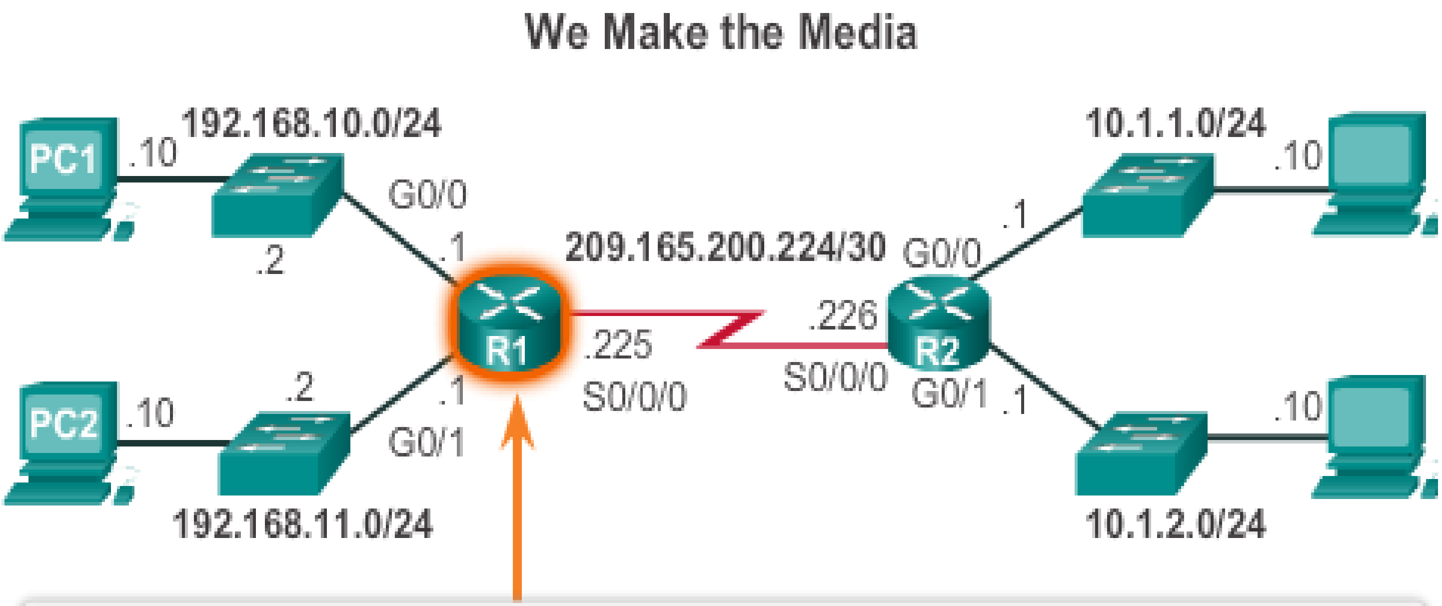
Packet Tracer – Configure Initial Router Settings

Verify the Default Router Configuration
Verify and Configure Initial Router Configuration
Save the Running Configuration File

Verify Connectivity of Directly Connected Networks

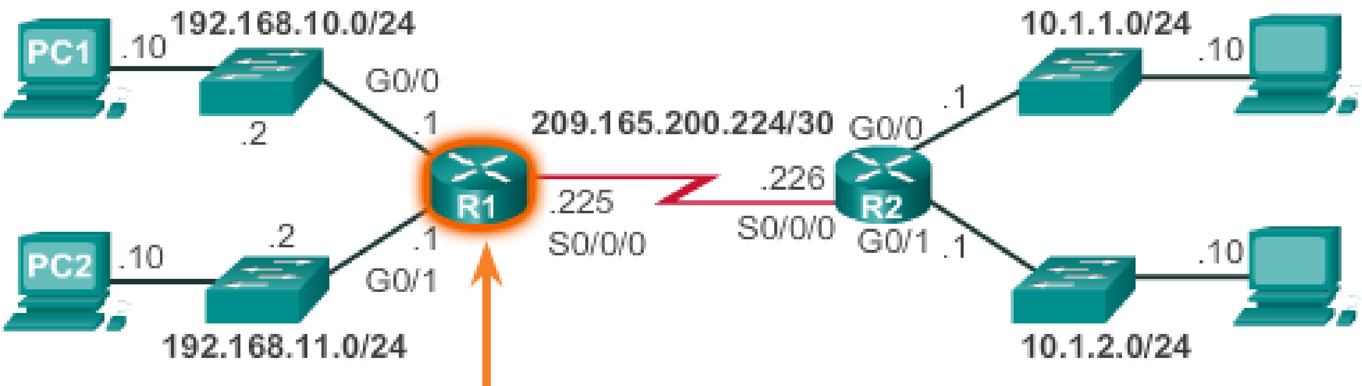
Verify Interface Settings

Verify Interface Settings




```
R1# show ip interface brief
Interface                  IP-Address      OK? Method Status
Embedded-Service-Engine0/0 unassigned      YES unset  administ
GigabitEthernet0/0         192.168.10.1    YES manual up
GigabitEthernet0/1         192.168.11.1    YES manual up
Serial0/0/0                209.165.200.225 YES manual up
Serial0/0/1                unassigned      YES unset  administ
R1#
```

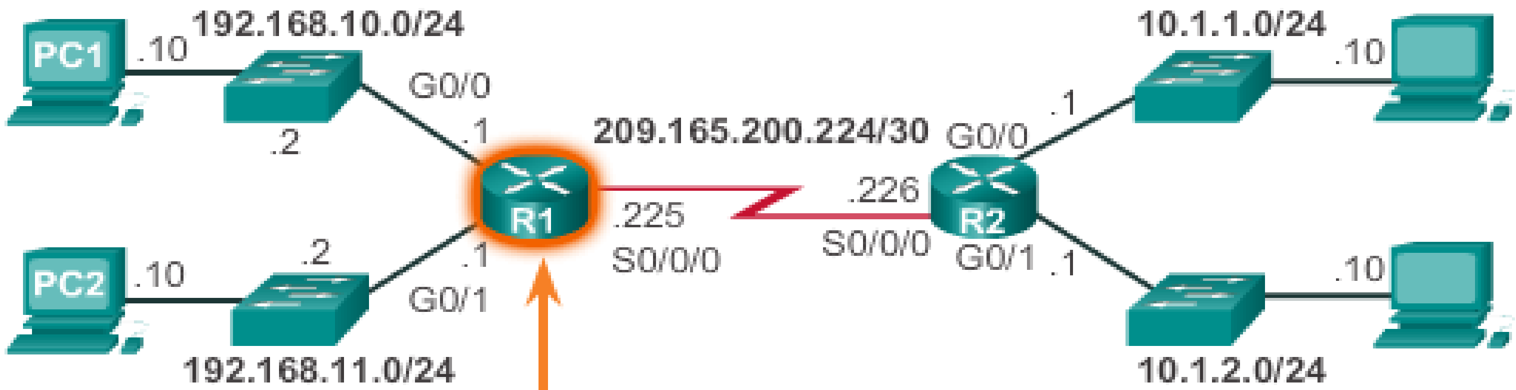
Verify Interface Settings




```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mo

<output omitted>

Gateway of last resort is not set

      192.168.10.0/24 is variably subnetted, 2 subnets, 2 ma
C        192.168.10.0/24 is directly connected, GigabitEther
L        192.168.10.1/32 is directly connected, GigabitEther
      192.168.11.0/24 is variably subnetted, 2 subnets, 2 ma
C        192.168.11.0/24 is directly connected, GigabitEther
L        192.168.11.1/32 is directly connected, GigabitEther
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 m
```

Verify Interface Settings

Verify an Interface Configuration




```
R1# show running-config interface gigabitEthernet 0/0
Building configuration...

Current configuration : 128 bytes
!
interface GigabitEthernet0/0
 description Link to LAN 1
 ip address 192.168.10.1 255.255.255.0
 duplex auto
 speed auto
end
```

Filter Show Command Output

```
R1# show running-config | section line vty
line vty 0 4
 password 7 030752180500
 login
 transport input all
R1#
```

Filter Show Command Output

```
R1# show ip interface brief
Interface                  IP-Address      OK? Method Status
Embedded-Service-Engine0/0 unassigned      YES unset  administ
GigabitEthernet0/0         192.168.10.1    YES manual up
GigabitEthernet0/1         192.168.11.1    YES manual up
Serial0/0/0                209.165.200.225 YES manual up
Serial0/0/1                unassigned      YES unset  administ
R1#
R1# show ip interface brief | include up
GigabitEthernet0/0         192.168.10.1    YES manual up
GigabitEthernet0/1         192.168.11.1    YES manual up
Serial0/0/0                209.165.200.225 YES manual up
R1#
```

Filter Show Command Output

```
R1# show ip interface brief
Interface                  IP-Address      OK? Method Status
Embedded-Service-Engine0/0 unassigned      YES unset  administ
GigabitEthernet0/0         192.168.10.1    YES manual up
GigabitEthernet0/1         192.168.11.1    YES manual up
Serial0/0/0                209.165.200.225 YES manual up
Serial0/0/1                unassigned      YES unset  administ

R1# show ip interface brief | exclude unassigned
Interface                  IP-Address      OK? Method Status
GigabitEthernet0/0         192.168.10.1    YES manual up
GigabitEthernet0/1         192.168.11.1    YES manual up
Serial0/0/0                209.165.200.225 YES manual up

R1#
```

Filter Show Command Output

```
R1# show ip route | begin Gateway
Gateway of last resort is not set

      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0
      192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.11.0/24 is directly connected, GigabitEthernet0/1
L        192.168.11.1/32 is directly connected, GigabitEthernet0/1
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.224/30 is directly connected, Serial0/0/0
L        209.165.200.225/32 is directly connected, Serial0/0/0
R1#
```

Command History Feature

```
R1# terminal history size 200
R1#
R1# show history
  show ip interface brief
  show interface g0/0
  show ip interface g0/1
  show ip route
  show ip route 209.165.200.224
  show running-config interface s0/0/0
  terminal history size 200
  show history
R1#
```

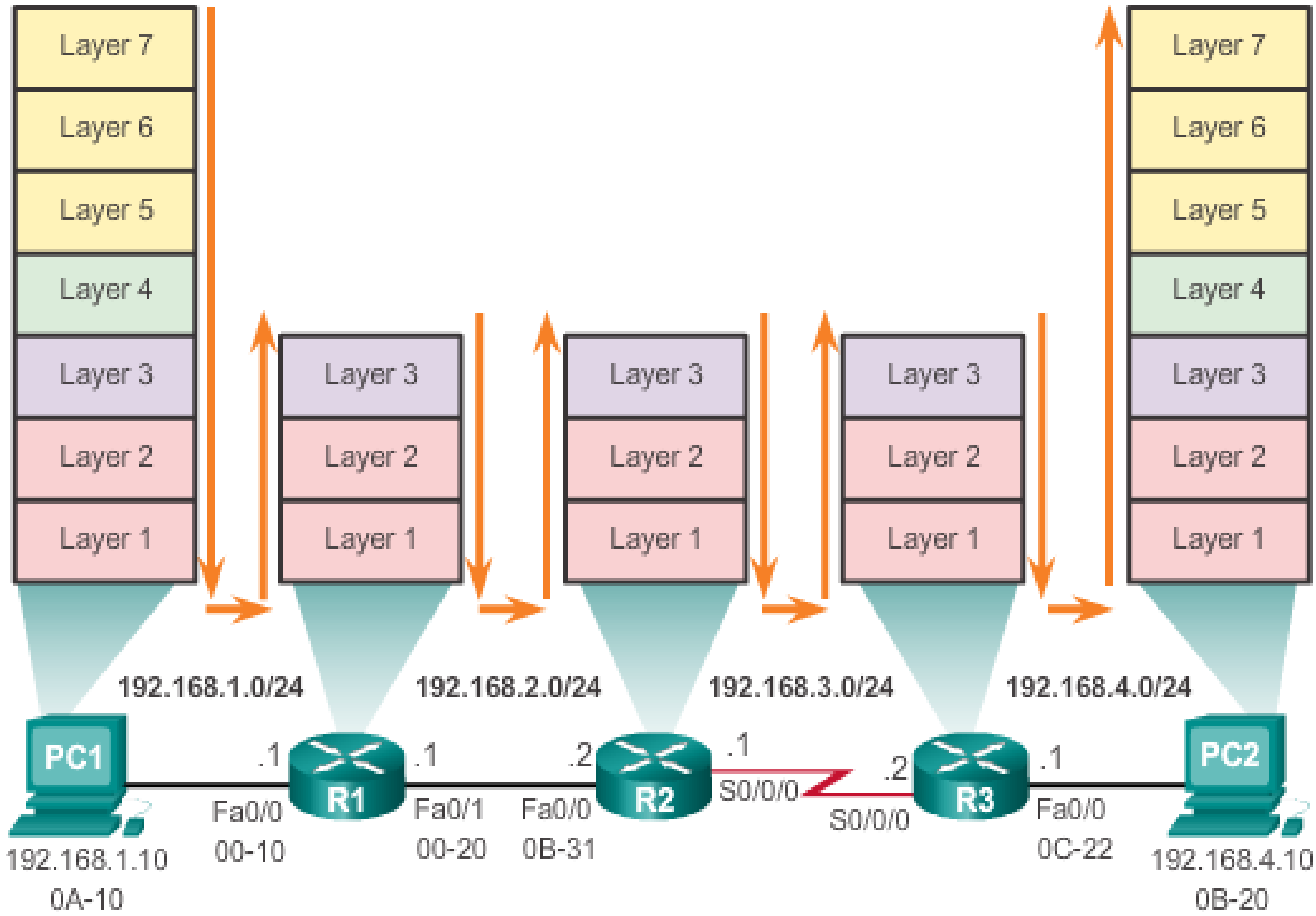
Configuring Routers

Verify Interface Settings
Filter Show Command Output
Command History Feature

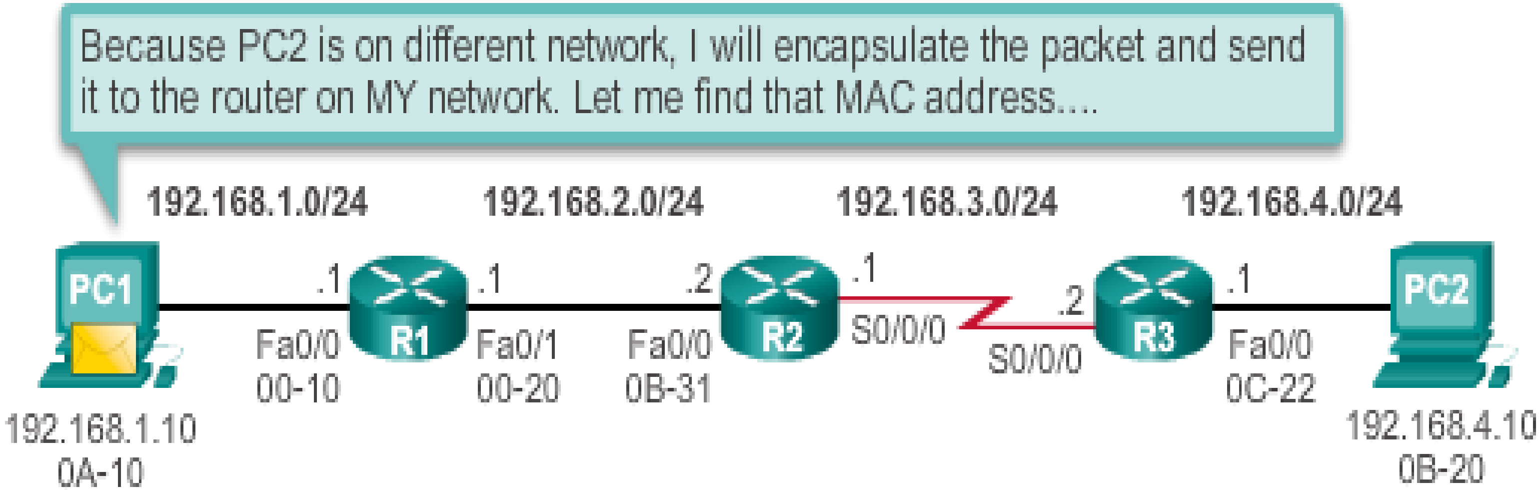
Switching Packets Between Networks

Router Switching Function

Router Switching Function



PC1 Sends a Packet to PC2



Layer 2 Data Link Frame

Packet's Layer 3 data

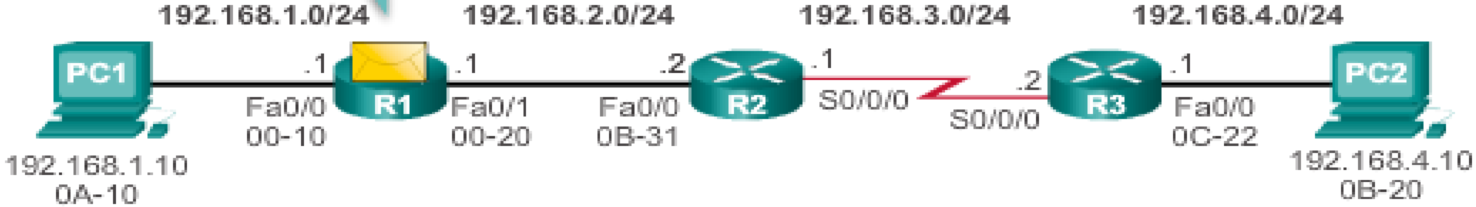
Dest. MAC 00-10	Source MAC 0A-10	Type 0x800	Source IP 192.168.1.10	Dest. IP 192.168.4.10	IP fields	Data	Trailer

PC1's ARP Cache for R1

IP Address	MAC Address
192.168.1.1	00-10

R1 Forwards the Packet to PC2

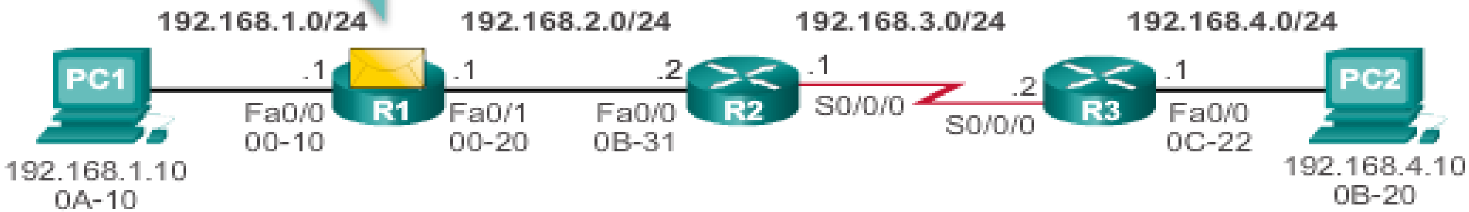
A frame was sent to me by MAC address 0A-10. Let me investigate further.



Layer 2 Data Link Frame — Packet's Layer 3 data

Dest. MAC	Source MAC		Source IP	Dest. IP			
00-10	0A-10	Type 0x800	192.168.1.10	192.168.4.10	IP fields	Data	Trailer

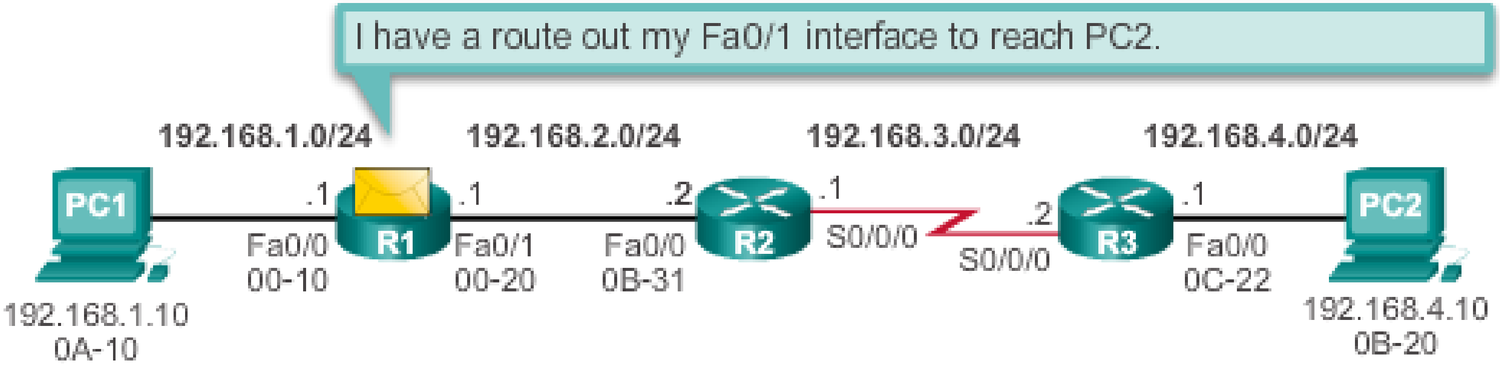
I can see from the type and destination IP address that this packet needs to be forwarded.



Layer 2 Data Link Frame — Packet's Layer 3 data

			Source IP	Dest. IP			
		Type 0x800	192.168.1.10	192.168.4.10	IP fields	Data	Trailer

R1 Forwards the Packet to PC2



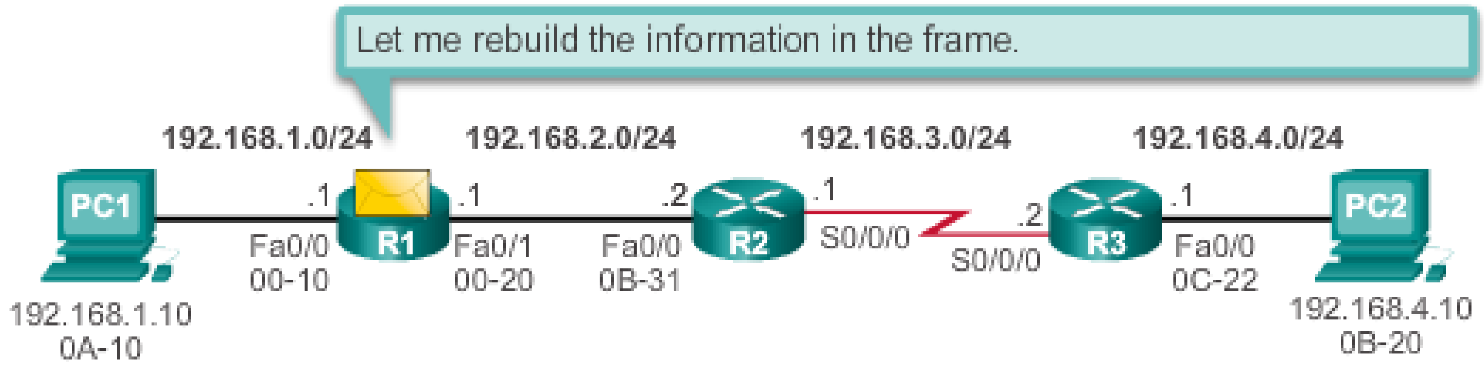
Layer 2 Data Link Frame **Packet's Layer 3 data**

		Type 0x800	Source IP 192.168.1.10	Dest. IP 192.168.4.10	IP fields	Data	Trailer

R1's Routing Table

Network	Hops	Next-hop-IP	Exit Interface
192.168.1.0/24	0	Dir. Connect.	Fa0/0
192.168.2.0/24	0	Dir. Connect.	Fa0/1
192.168.3.0/24	1	192.168.2.2	Fa0/1
192.168.4.0/24	**2**	**192.168.2.2**	**Fa0/1**

R1 Forwards the Packet to PC2



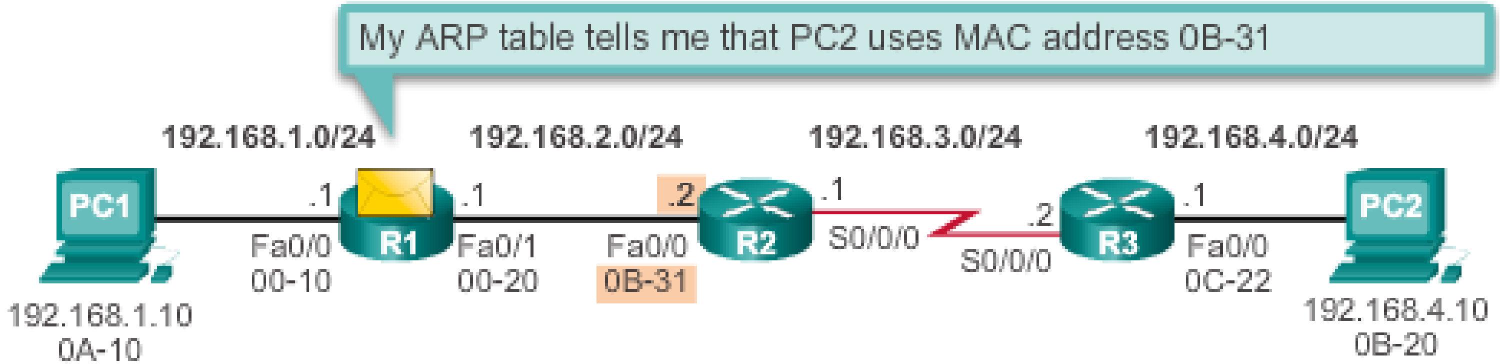
Layer 2 Data Link Frame | Packet's Layer 3 data

		Type 0x800	Source IP 192.168.1.10	Dest. IP 192.168.4.10	IP fields	Data	Trailer

R1's Routing Table

Network	Hops	Next-hop-IP	Exit Interface
192.168.1.0/24	0	Dir. Connect.	Fa0/0
192.168.2.0/24	0	Dir. Connect.	Fa0/1
192.168.3.0/24	1	192.168.2.2	Fa0/1
192.168.4.0/24	2	192.168.2.2	Fa0/1

R1 Forwards the Packet to PC2



Layer 2 Data Link Frame **Packet's Layer 3 data**

Dest. MAC 0B-31		Type 0x800	Source IP 192.168.1.10	Dest. IP 192.168.4.10	IP fields	Data	Trailer

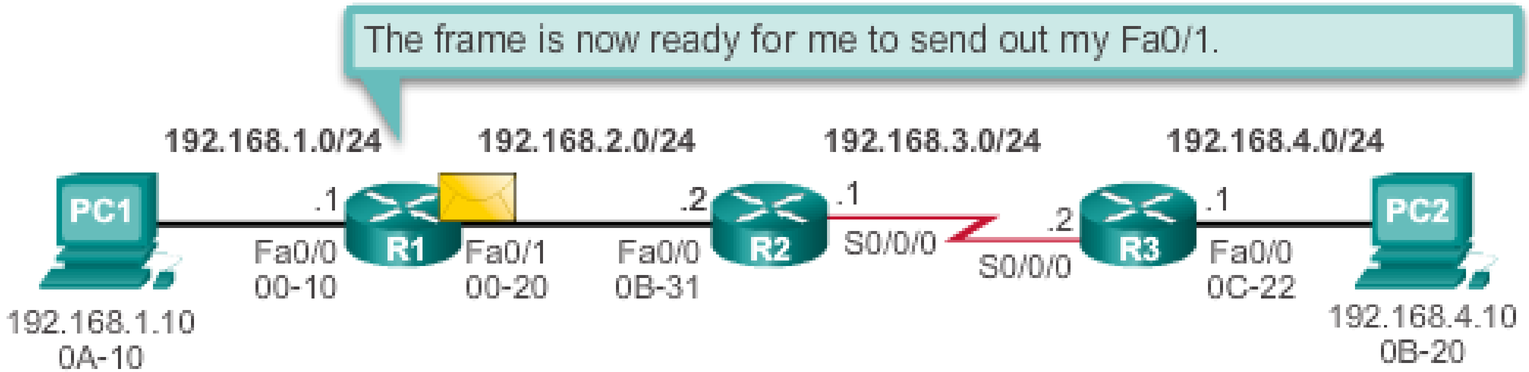
R1's ARP Cache

IP Address	MAC Address
192.168.2.2	0B-31

R1's Routing Table

Network	Hops	Next-hop-IP	Exit Interface
192.168.1.0/24	0	Dir. Connect.	Fa0/0
192.168.2.0/24	0	Dir. Connect.	Fa0/1
192.168.3.0/24	1	192.168.2.2	Fa0/1
192.168.4.0/24	2	192.168.2.2	Fa0/1

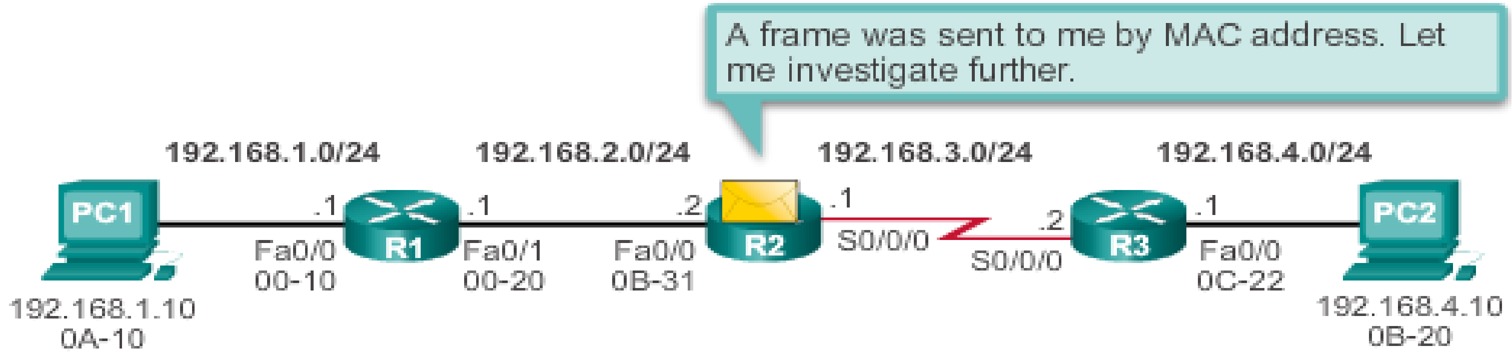
R1 Forwards the Packet to PC2



Layer 2 Data Link Frame   Packet's Layer 3 data

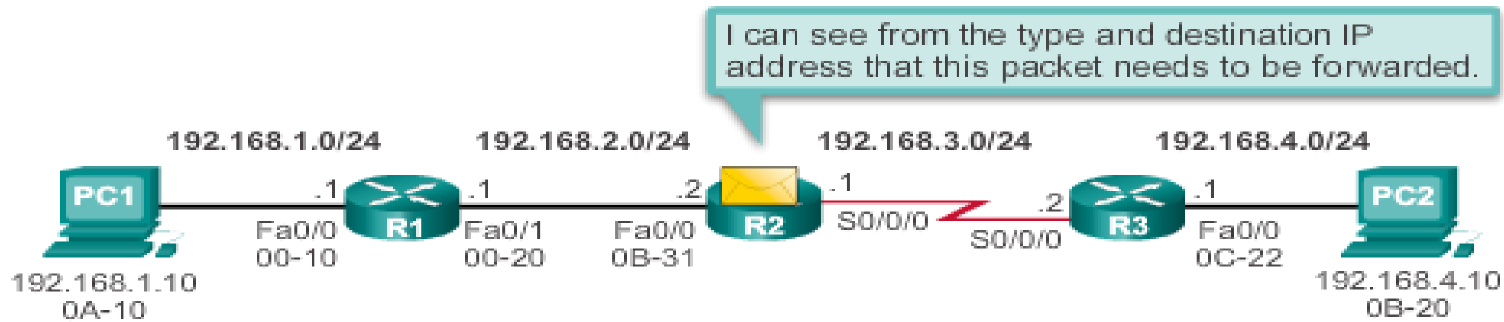
Dest. MAC 0B-31	Source MAC 00-20	Type 0x800	Source IP 192.168.1.10	Dest. IP 192.168.4.10	IP fields	Data	Trailer

Packet Routing – R2 Forwards the Packet to R3



Layer 2 Data Link Frame **Packet's Layer 3 data**

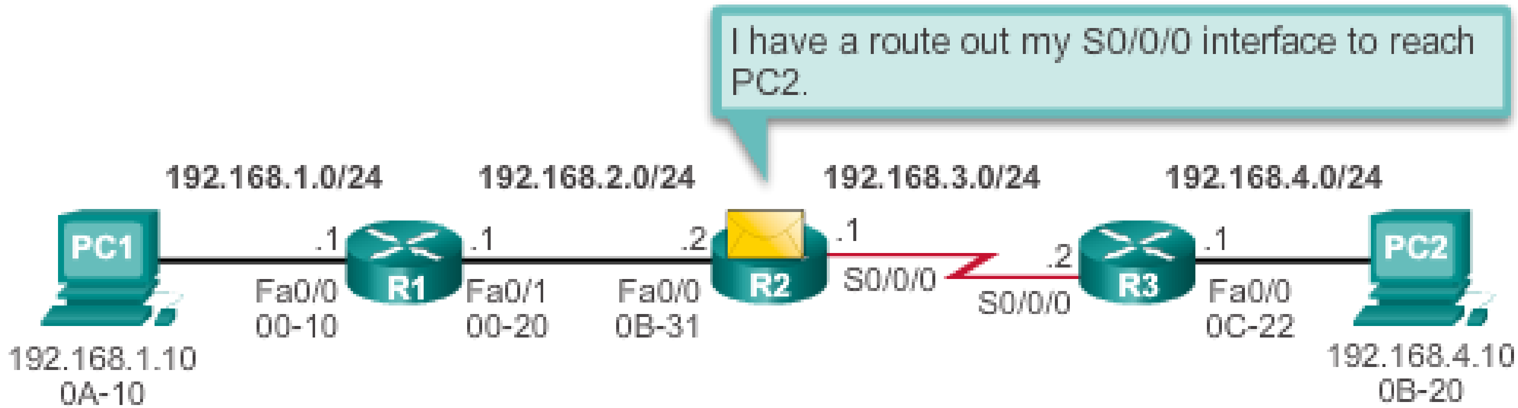
Dest MAC 0B-31	Source MAC 00-20	Type 0x800	Source IP 192.168.1.1 0	Dest. IP 192.168.4.1 0	IP fields	Data	Trailer



Layer 2 Data Link Frame **Packet's Layer 3 data**

		Type 0x800	Source IP 192.168.1.1 0	Dest. IP 192.168.4.1 0	IP fields	Data	Trailer

Packet Routing – R2 Forwards the Packet to R3



Layer 2 Data Link Frame

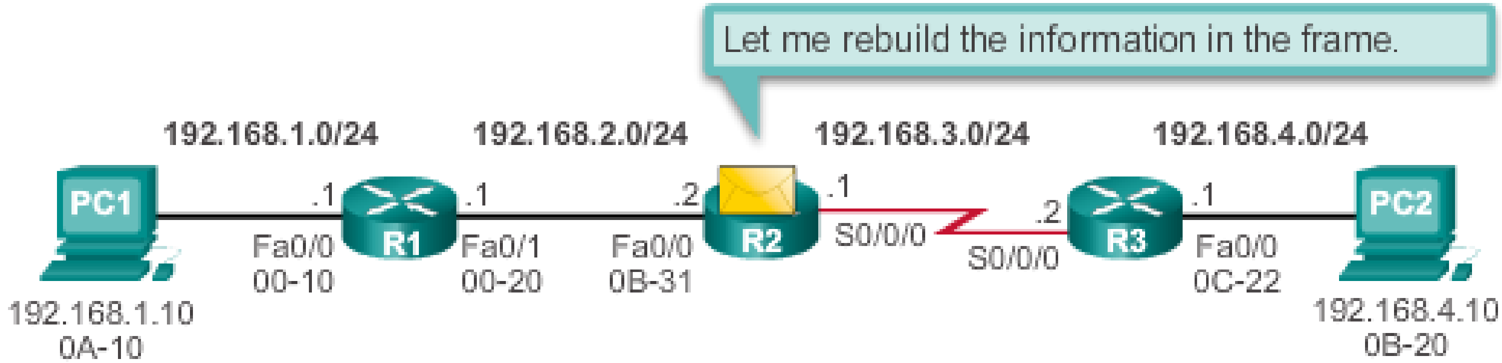
Packet's Layer 3 data

			Source IP 192.168.1.10	Dest. IP 192.168.4.10	IP fields	Data	Trailer

R2's Routing Table

Network	Hops	Next-hop-IP	Exit Interface
192.168.1.0/24	1	192.168.3.1	Fa/0/0
192.168.2.0/24	0	Dir. Connect.	Fa/0/0
192.168.3.0/24	0	Dir. Connect.	S0/0/0
192.168.4.0/24	**1**	**192.162.3.2**	**S0/0/0**

Packet Routing – R2 Forwards the Packet to R3



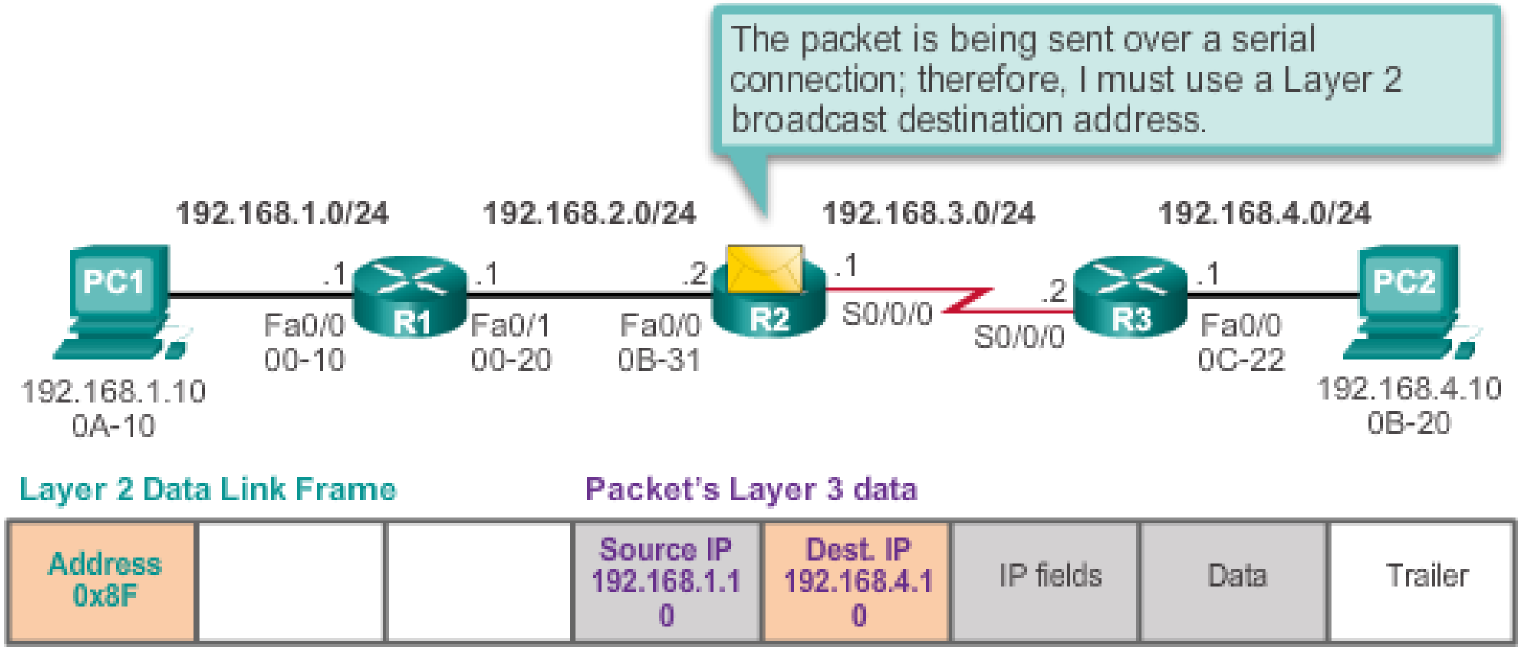
Layer 2 Data Link Frame **Packet's Layer 3 data**

			Source IP 192.168.1.10	Dest. IP 192.168.4.10	IP fields	Data	Trailer

R2's Routing Table

Network	Hops	Next-hop-IP	Exit Interface
192.168.1.0/24	1	192.168.3.1	Fa/0/0
192.168.2.0/24	0	Dir. Connect.	Fa/0/0
192.168.3.0/24	0	Dir. Connect.	S0/0/0
192.168.4.0/24	**1**	**192.162.3.2**	**S0/0/0**

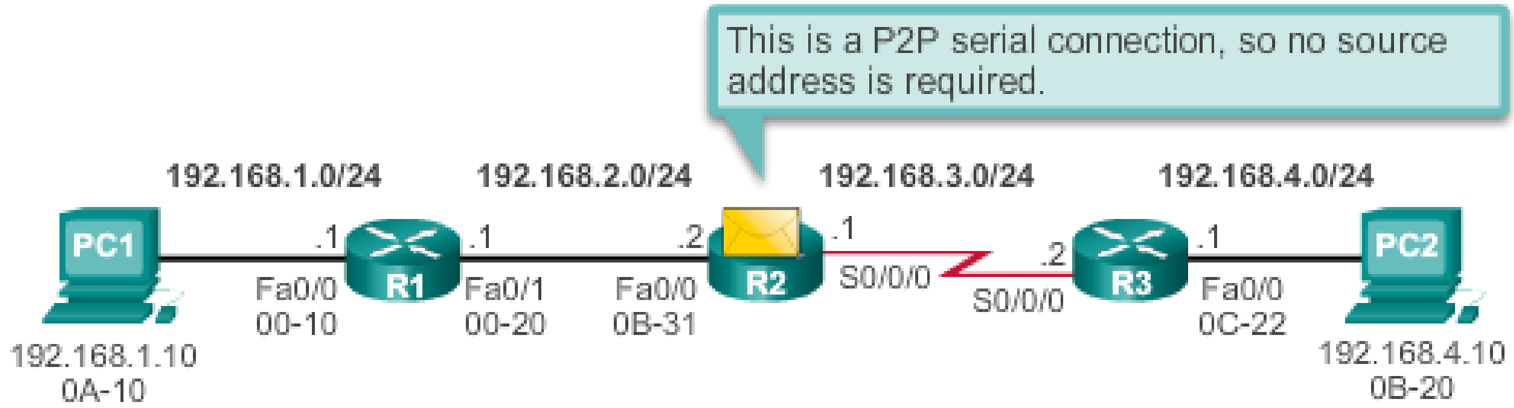
Packet Routing – R2 Forwards the Packet to R3



R2's Routing Table

Network	Hops	Next-hop-IP	Exit Interface
192.168.1.0/24	1	192.168.3.1	Fa/0/0
192.168.2.0/24	0	Dir. Connect.	Fa/0/0
192.168.3.0/24	0	Dir. Connect.	S0/0/0
192.168.4.0/24	**1**	**192.162.3.2**	**S0/0/0**

Packet Routing – R2 Forwards the Packet to R3



Layer 2 Data Link Frame | Packet's Layer 3 data

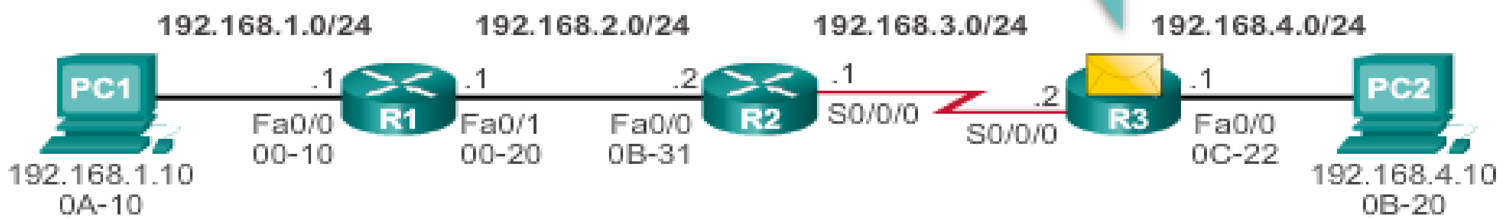
Address 0x8F	Control 0x00	Type 0x800	Source IP 192.168.1.10	Dest. IP 192.168.4.10	IP fields	Data	Trailer

R2's Routing Table

Network	Hops	Next-hop-IP	Exit Interface
192.168.1.0/24	1	192.168.3.1	Fa/0/0
192.168.2.0/24	0	Dir. Connect.	Fa/0/0
192.168.3.0/24	0	Dir. Connect.	S0/0/0
192.168.4.0/24	**1**	**192.162.3.2**	**S0/0/0**

Reach the Destination – R3 Forwards the Packet to PC2

A frame was sent to me across my point-to-point link. Let me investigate further.

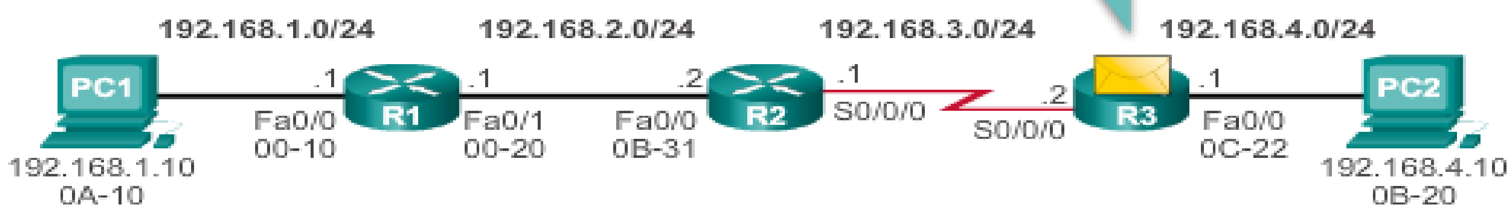


Layer 2 Data Link Frame

Packet's Layer 3 data

Address 0x8F	Control 0x00	Type 0x800	Source IP 192.168.10	Dest. IP 192.168.4.10	IP fields	Data	Trailer

I can see from the type and destination IP address that this packet needs to be forwarded.

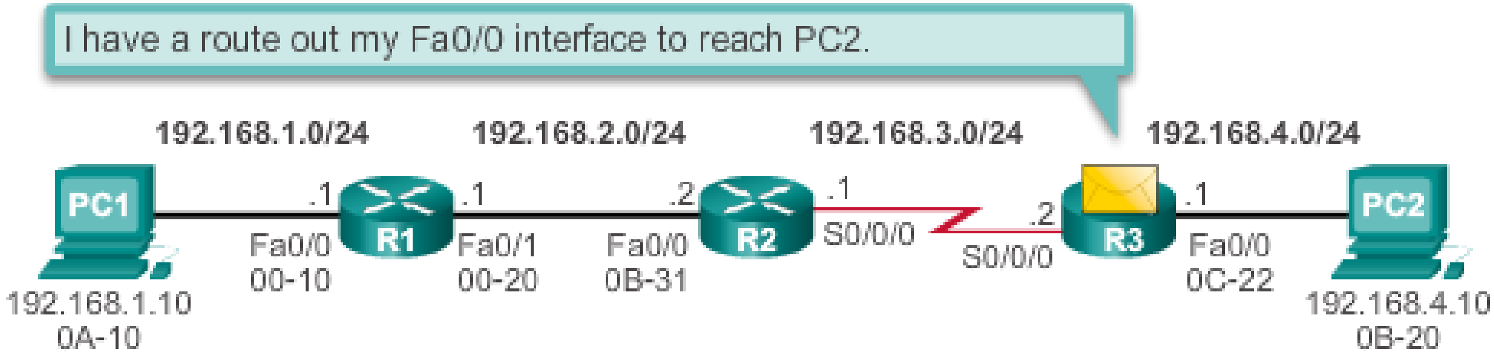


Layer 2 Data Link Frame

Packet's Layer 3 data

		Type 0x800	Source IP 192.168.10	Dest. IP 192.168.4.10	IP fields	Data	Trailer

Reach the Destination – R3 Forwards the Packet to PC2



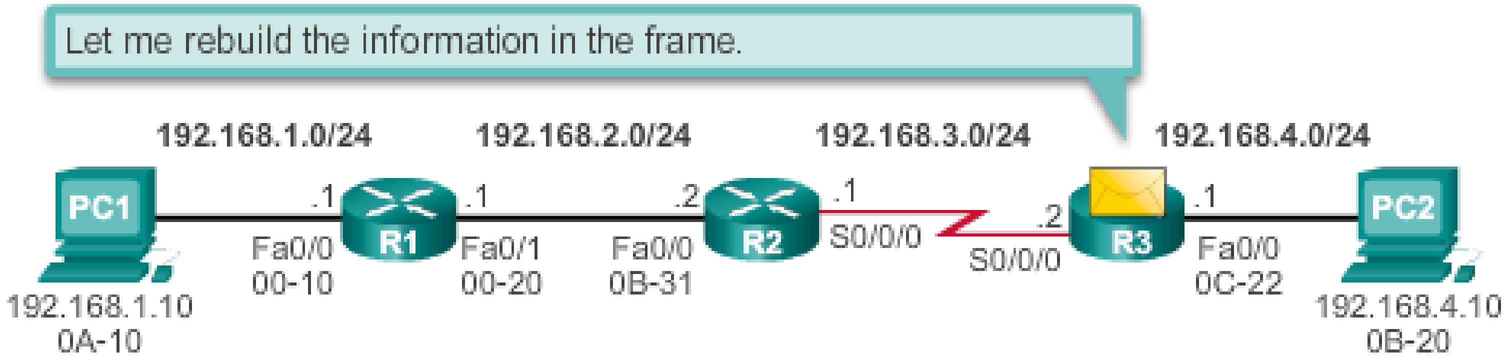
Layer 2 Data Link Frame | **Packet's Layer 3 data**

		Type 0x800	Source IP 192.168.1.10	Dest. IP 192.168.4.10	IP fields	Data	Trailer

R3's Routing Table

Network	Hops	Next-hop-IP	Exit Interface
192.168.1.0/24	2	192.168.3.1	S0/0/0
192.168.2.0/24	1	192.168.3.1	S0/0/0
192.168.3.0/24	0	Dir. Connect.	S0/0/0
192.168.4.0/24	**0**	Dir. Connect.	**Fa0/0**

Reach the Destination – R3 Forwards the Packet to PC2



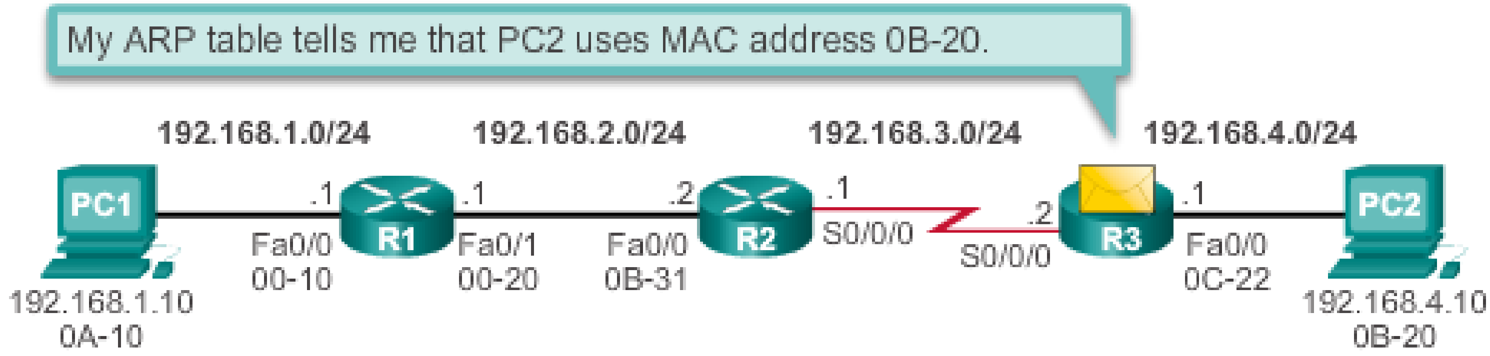
Layer 2 Data Link Frame — Packet's Layer 3 data

Dest. MAC 0B-20	Source MAC 0C-22	Type 0x800	Source IP 192.168.1.10	Dest. IP 192.168.4.10	IP fields	Data	Trailer

R3's Routing Table

Network	Hops	Next-hop-IP	Exit Interface
192.168.1.0/24	2	192.168.3.1	S0/0/0
192.168.2.0/24	1	192.168.3.1	S0/0/0
192.168.3.0/24	0	Dir. Connect.	S0/0/0
192.168.4.0/24	**0**	**Dir. Connect.**	**Fa0/0**

Reach the Destination – R3 Forwards the Packet to PC2



Layer 2 Data Link Frame — **Packet's Layer 3 data**

Dest. MAC 0B-20	Source MAC 0C-22	Type 0x800	Source IP 192.168.1.10	Dest. IP 192.168.4.10	IP fields	Data	Trailer

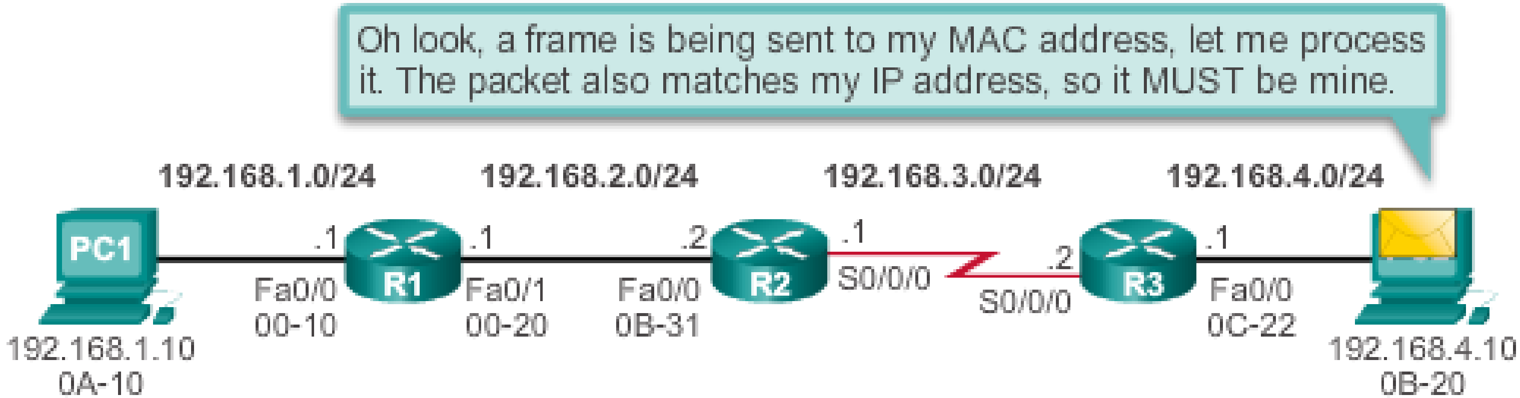
R3's ARP Cache

IP Address	MAC Address
192.168.4.10	0B-20

R3's Routing Table

Network	Hops	Next-hop-IP	Exit Interface
192.168.1.0/24	2	192.168.3.1	S0/0/0
192.168.2.0/24	1	192.168.3.1	S0/0/0
192.168.3.0/24	0	Dir. Connect.	S0/0/0
192.168.4.0/24	0	Dir. Connect.	Fa0/0

Reach the Destination – R3 Forwards the Packet to PC2



Layer 2 Data Link Frame **Packet's Layer 3 data**

Dest. MAC 0B-20	Source MAC 0C-22	Type 0x800	Source IP 192.168.1.10	Dest. IP 192.168.4.10	IP fields	Data	Trailer

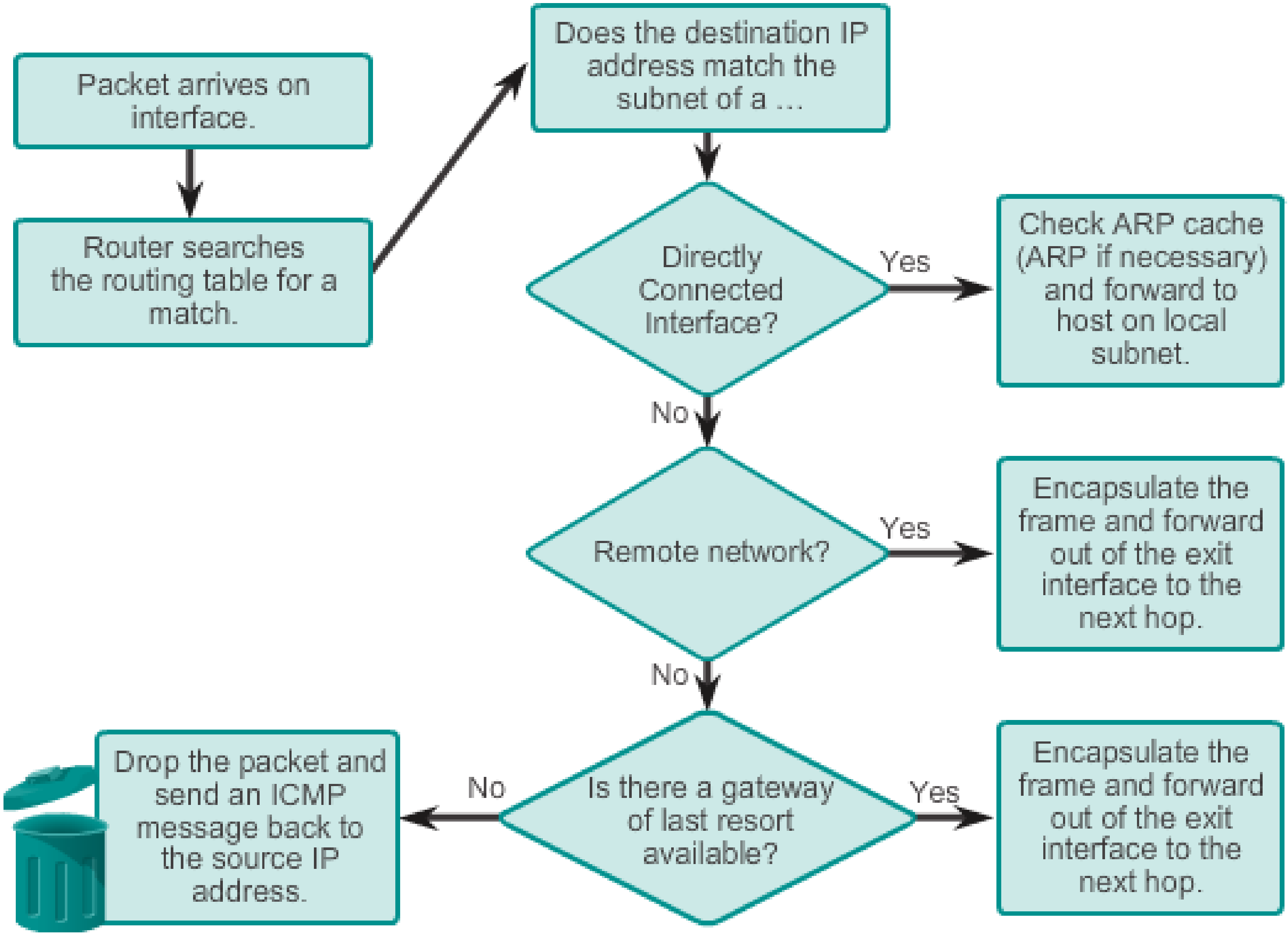
Switching Packets Between Networks

Router Switching Functions

Path Determination

Routing Decisions

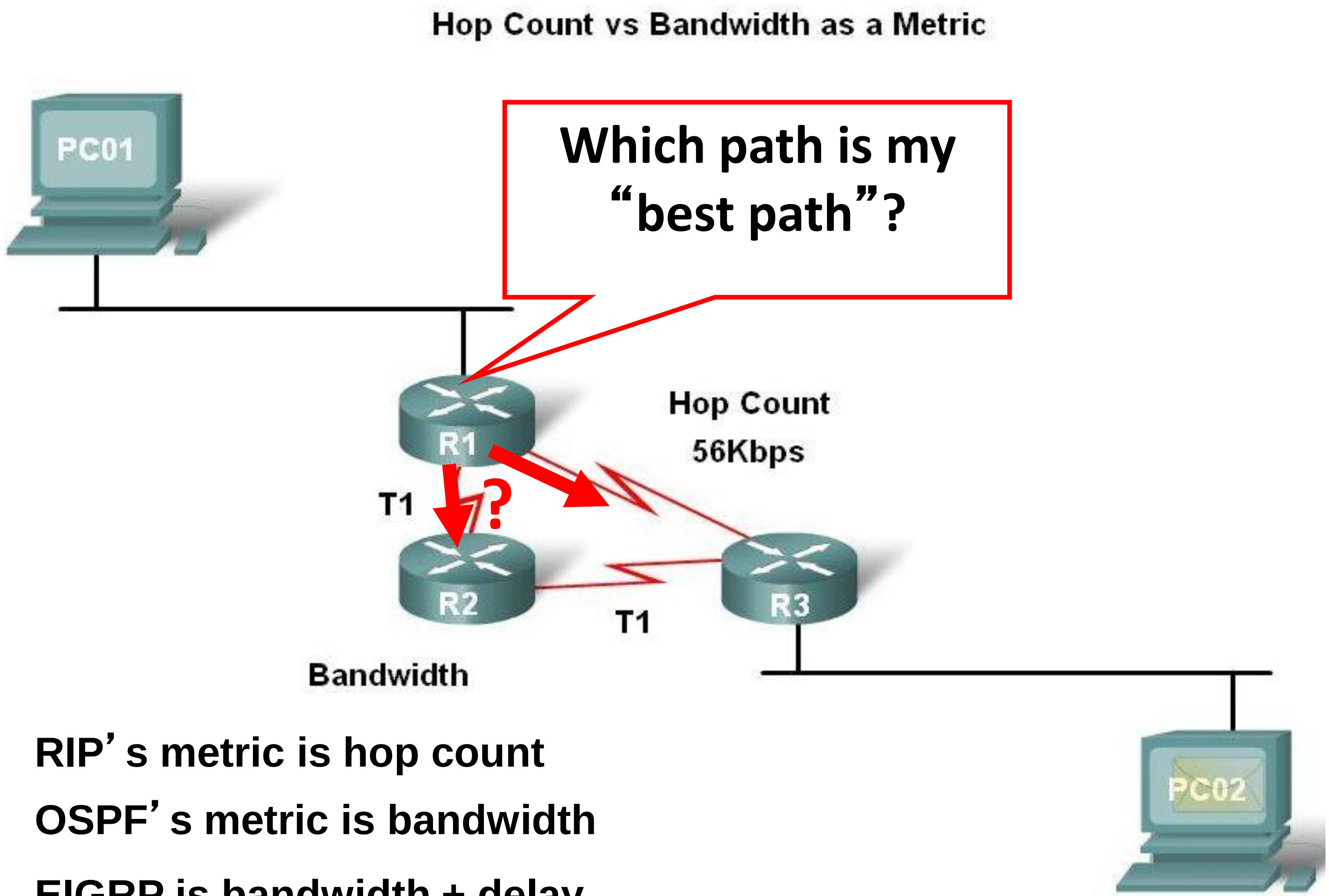
Routing Decisions



Best Path

- Router's determine best-path to a network:
  - •Depends on the **routing protocol**
  - •A protocol used between routers to determine **"best path"**
- Have own ***rules*** and ***metrics***.
  A metric:
  Quantitative value used to measure the distance to a given route.
- **Best path:**
  Path with the **lowest metric**.

Routing Metric

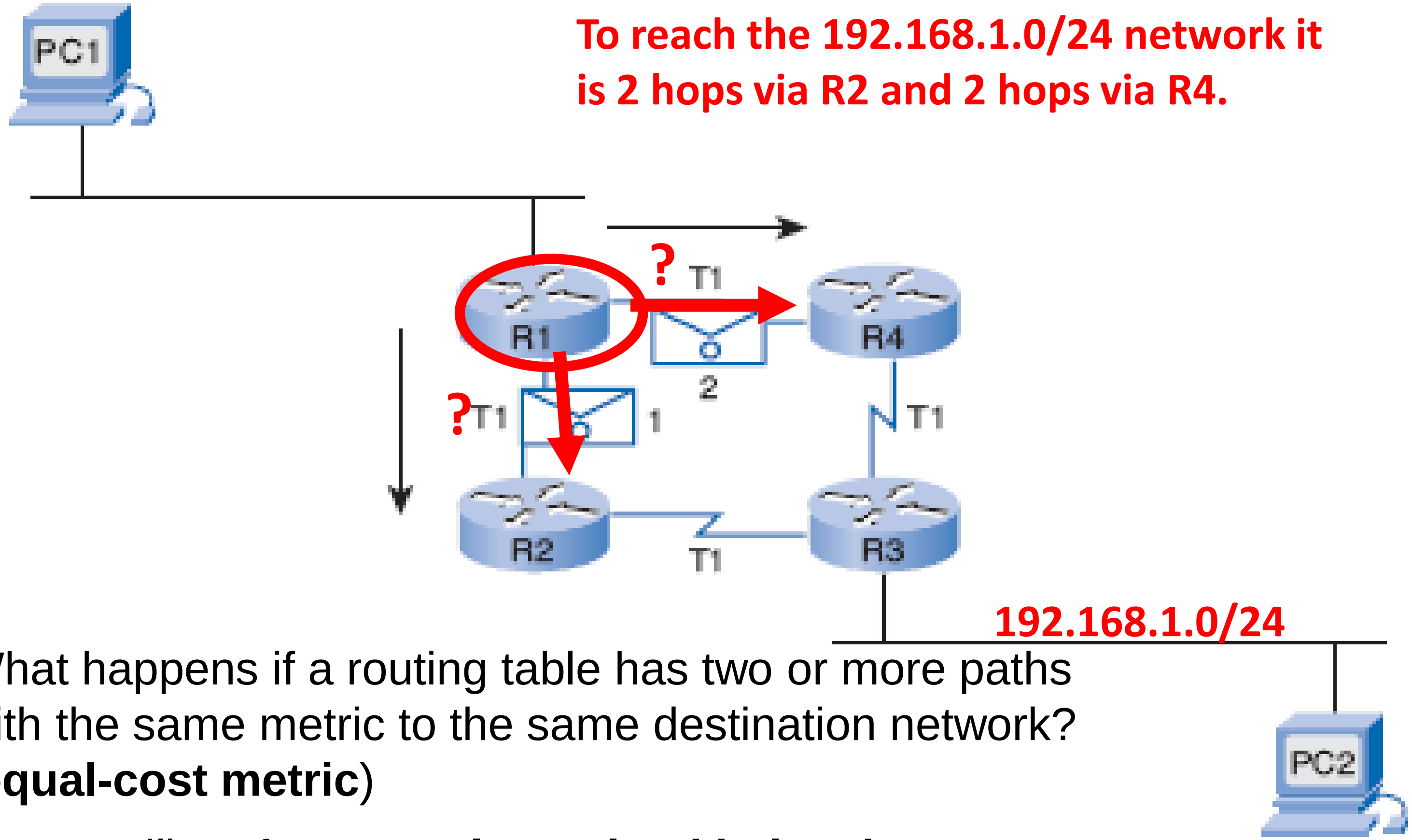


RIP's metric is hop count

OSPF's metric is bandwidth

EIGRP is bandwidth + delay

Load Balancing



What happens if a routing table has two or more paths with the same metric to the same destination network? (**equal-cost metric**)

Router will perform **equal-cost load balancing**.

All routing protocols (RIP, EIGRP, OSPF) support equal cost load balancing; EIGRP also supports unequal cost load balancing.

Path Determination

Routing Decisions
Best Path
Load Balancing

Analyze the Routing Table

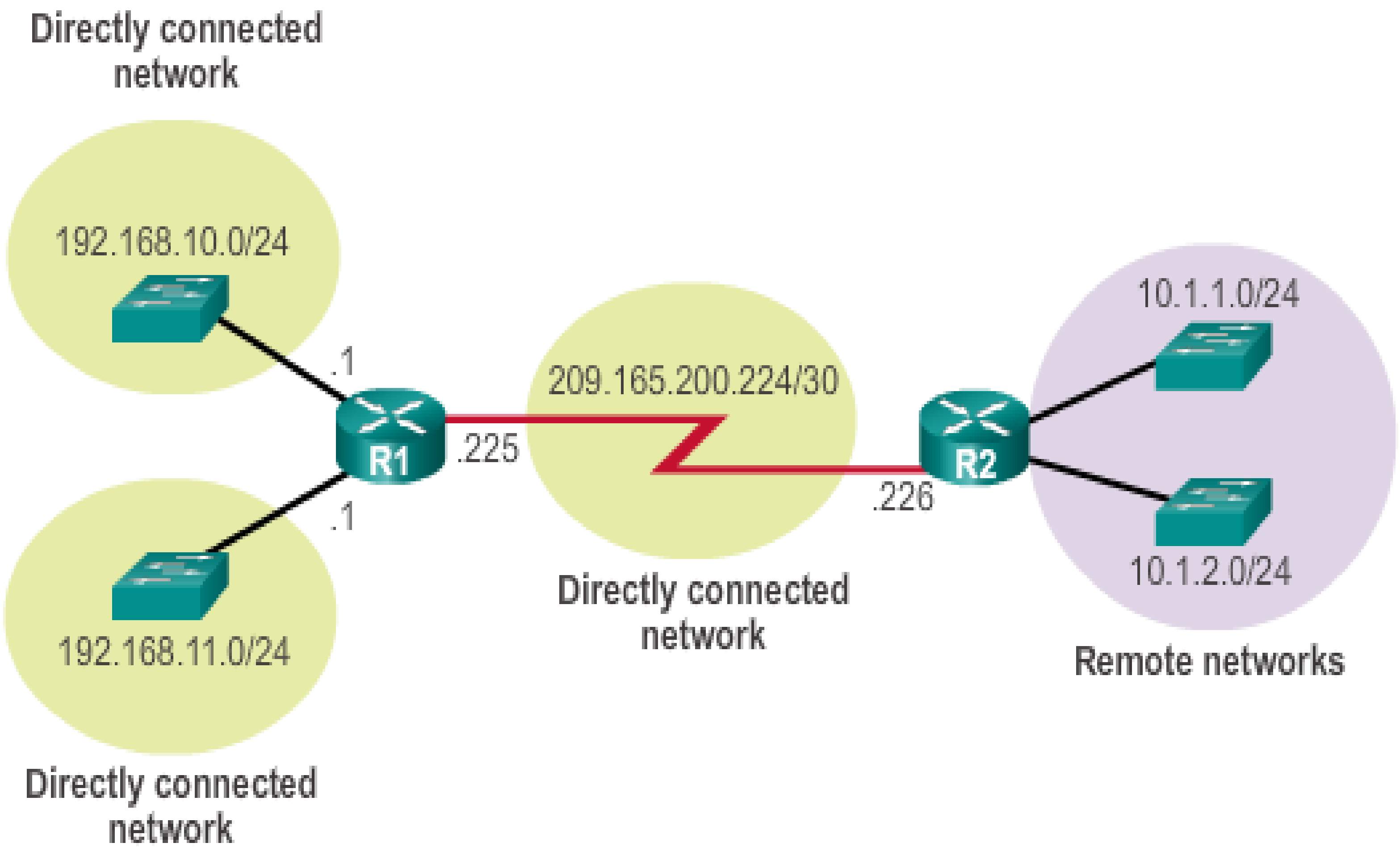
The Routing Table

The Routing Table

A routing table is a file stored in RAM that contains information about:

- Directly connected routes
- Remote routes
- Network or next hop associations

The Routing Table



Routing Table Sources

The **show ip route** commands are used to display the contents of the routing table:

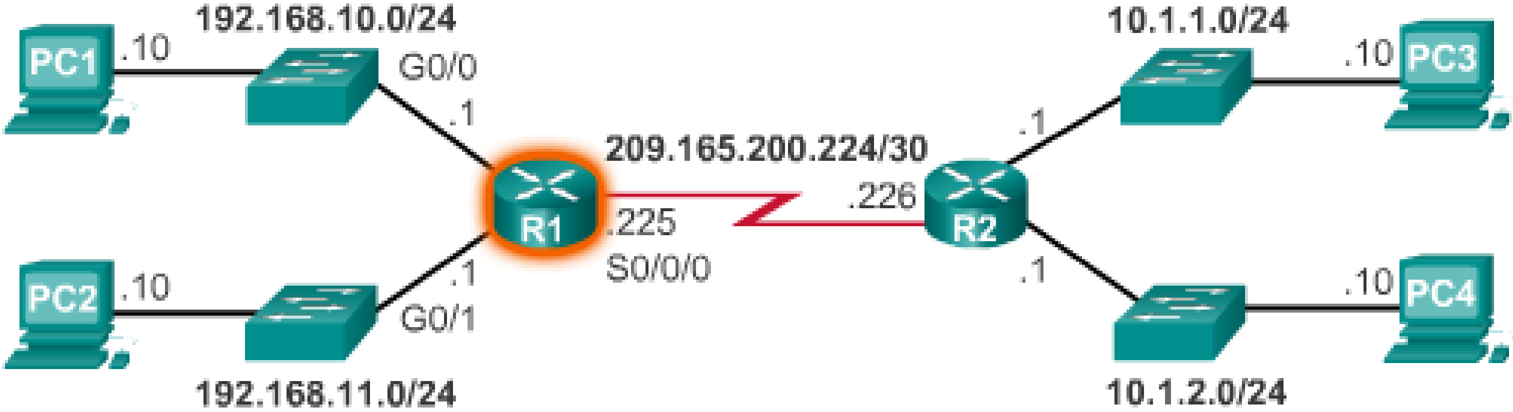
Local route interfaces - Added to the routing table when an interface is configured. (displayed in IOS 15 or newer)

Directly connected interfaces - Added to the routing table when an interface is configured and active.

Static routes - Added when a route is manually configured and the exit interface is active.

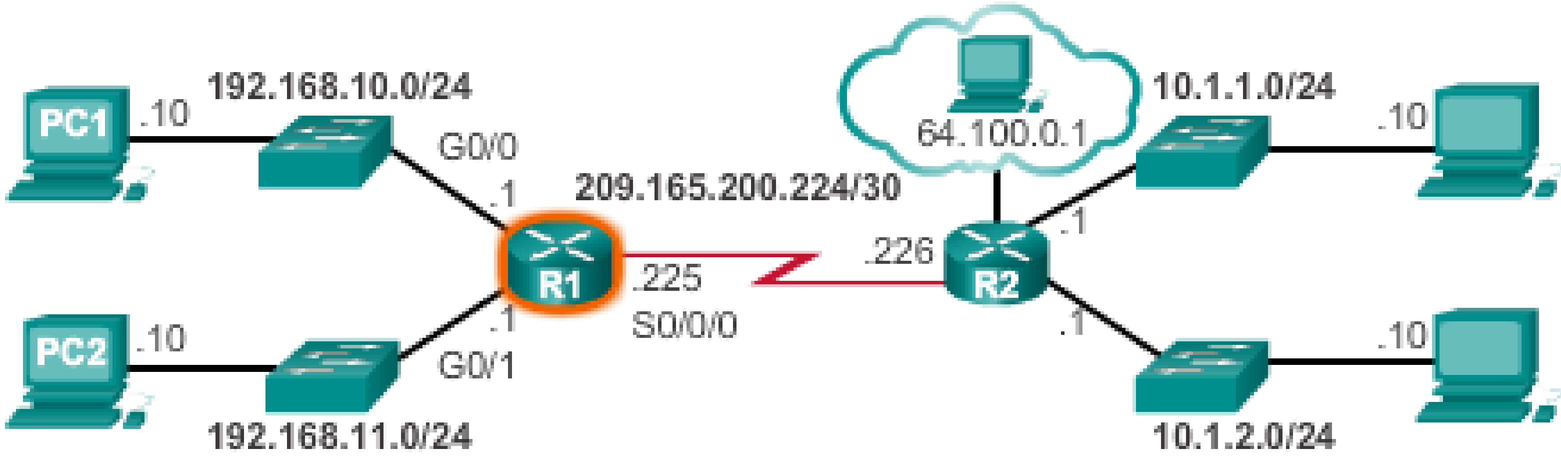
Dynamic routing protocol - Added when EIGRP or OSPF are implemented and networks are identified.

Routing Table for R1




```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
       IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D       10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05,
```

Remote Network Routing Entries



D 10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05, Serial0/0/0

Legend

- (green) - Identifies how the network was learned by the router.
- (pink) - Identifies the destination network.
- (orange) - Identifies the administrative distance (trustworthiness) of the route source.
- (purple) - Identifies the metric to reach the remote network.
- (peach) - Identifies the next-hop IP address to reach the remote network.
- (light green) - Identifies the amout of elapsed time since the network was discovered.
- (light yellow) - Identifies the outgoing interface on the router to reach the destination network.

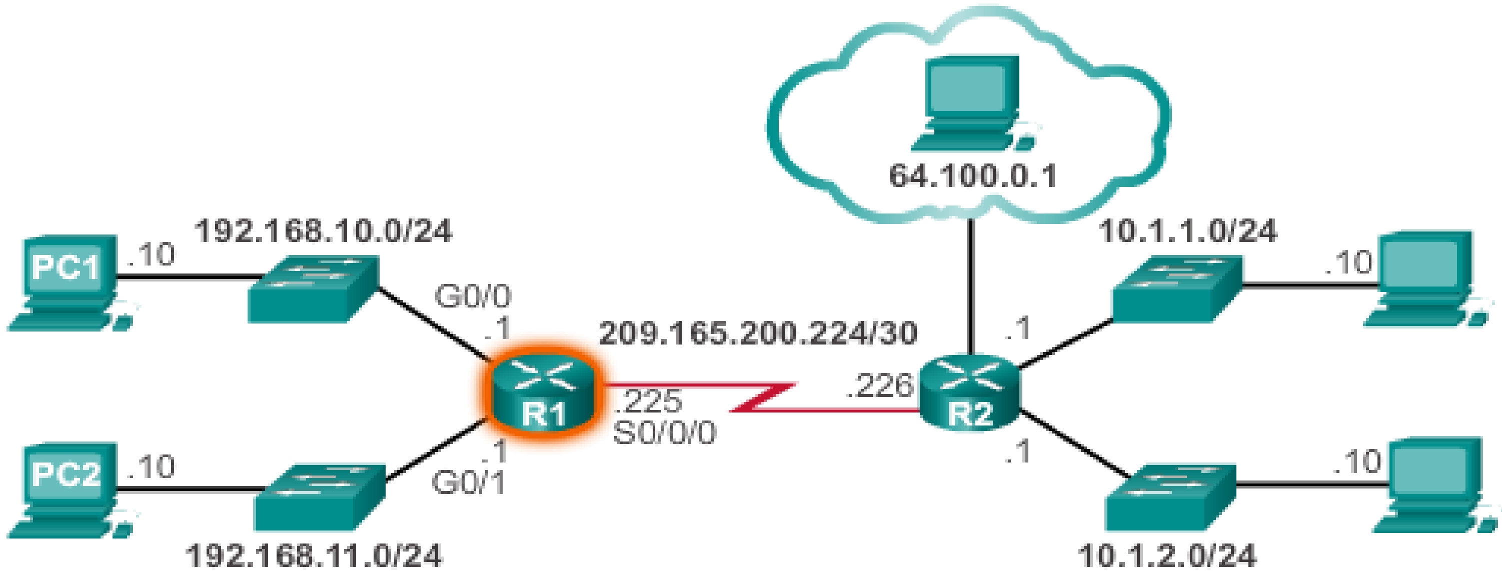
Analyze The Routing Table

The Routing Table
Routing Table Entries

Directly Connected/Static/Dynamic Routes

Directly Connected Routes

Directly Connected Routes

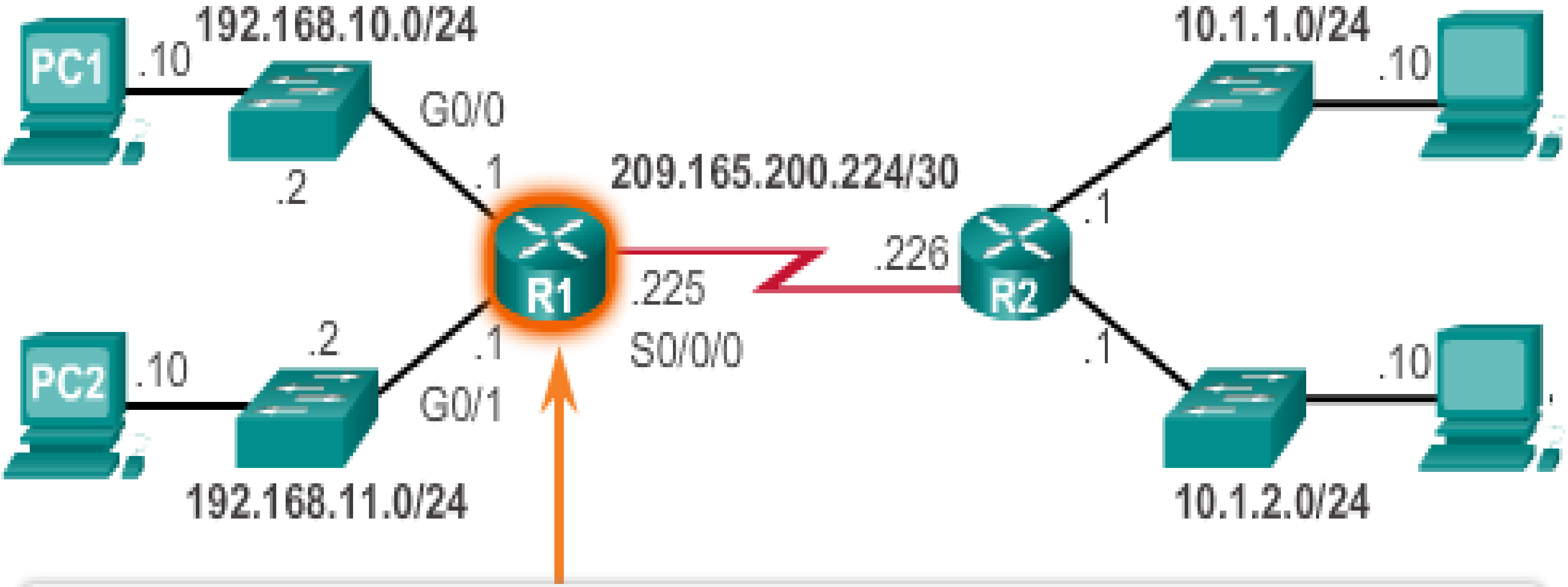


A	B	C
C	192.168.10.0/24 is directly connected,	GigabitEthernet0/0
L	192.168.10.1/32 is directly connected,	GigabitEthernet0/0

Legend

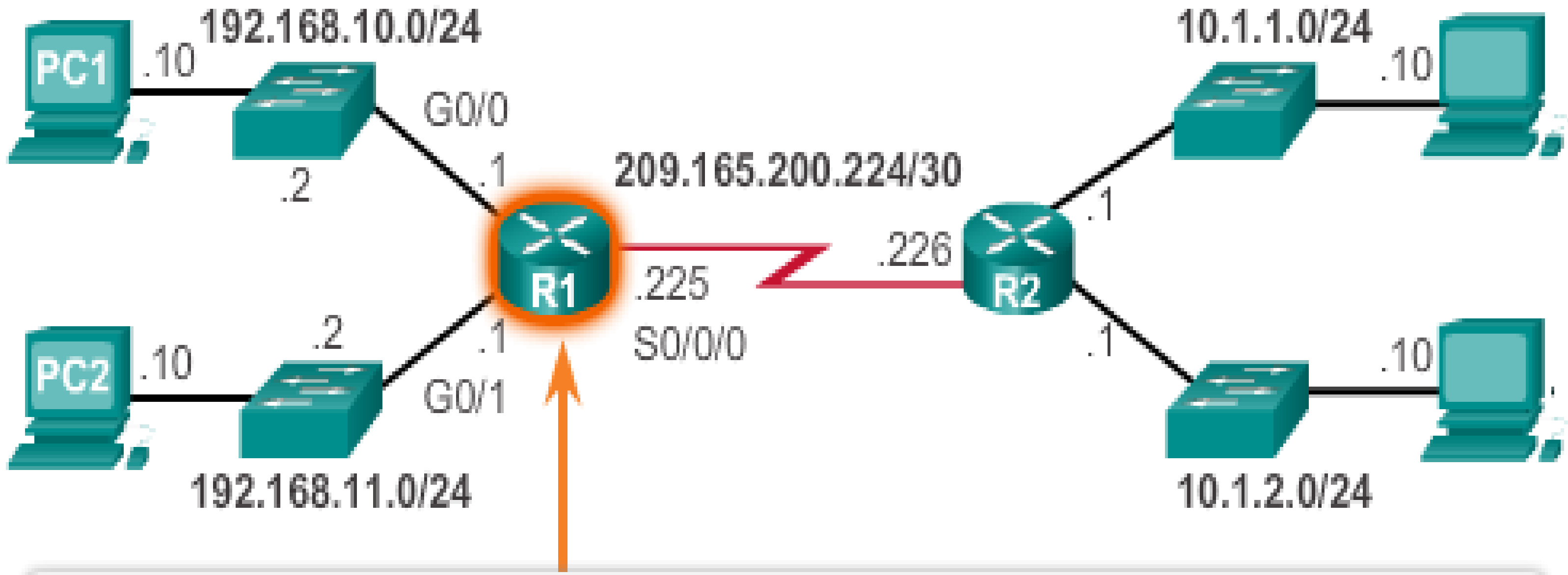
- (green) - Identifies how the network was learned by the router.
- (pink) - Identifies the destination network and how it is connected.
- (orange) - Identifies the interface on the router connected to the destination network.

Directly Connected Example



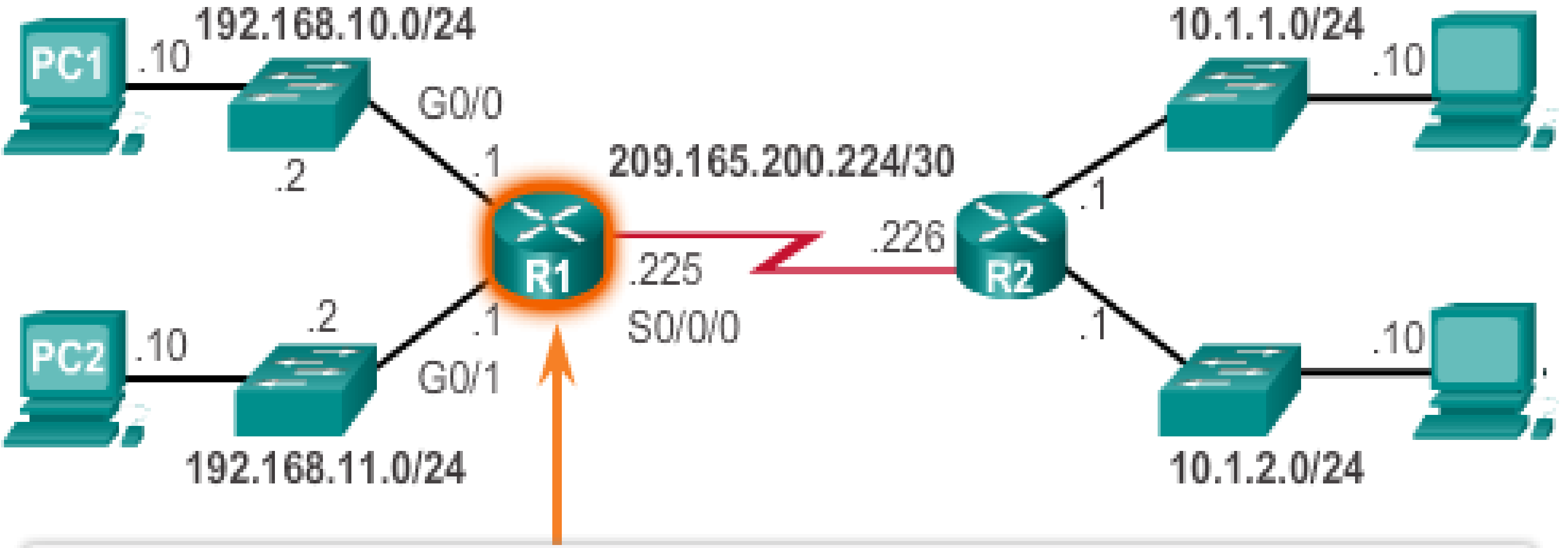

```
R1(config)# interface gigabitethernet 0/0
R1(config-if)# description Link to LAN 1
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)#
```

Directly Connected Example



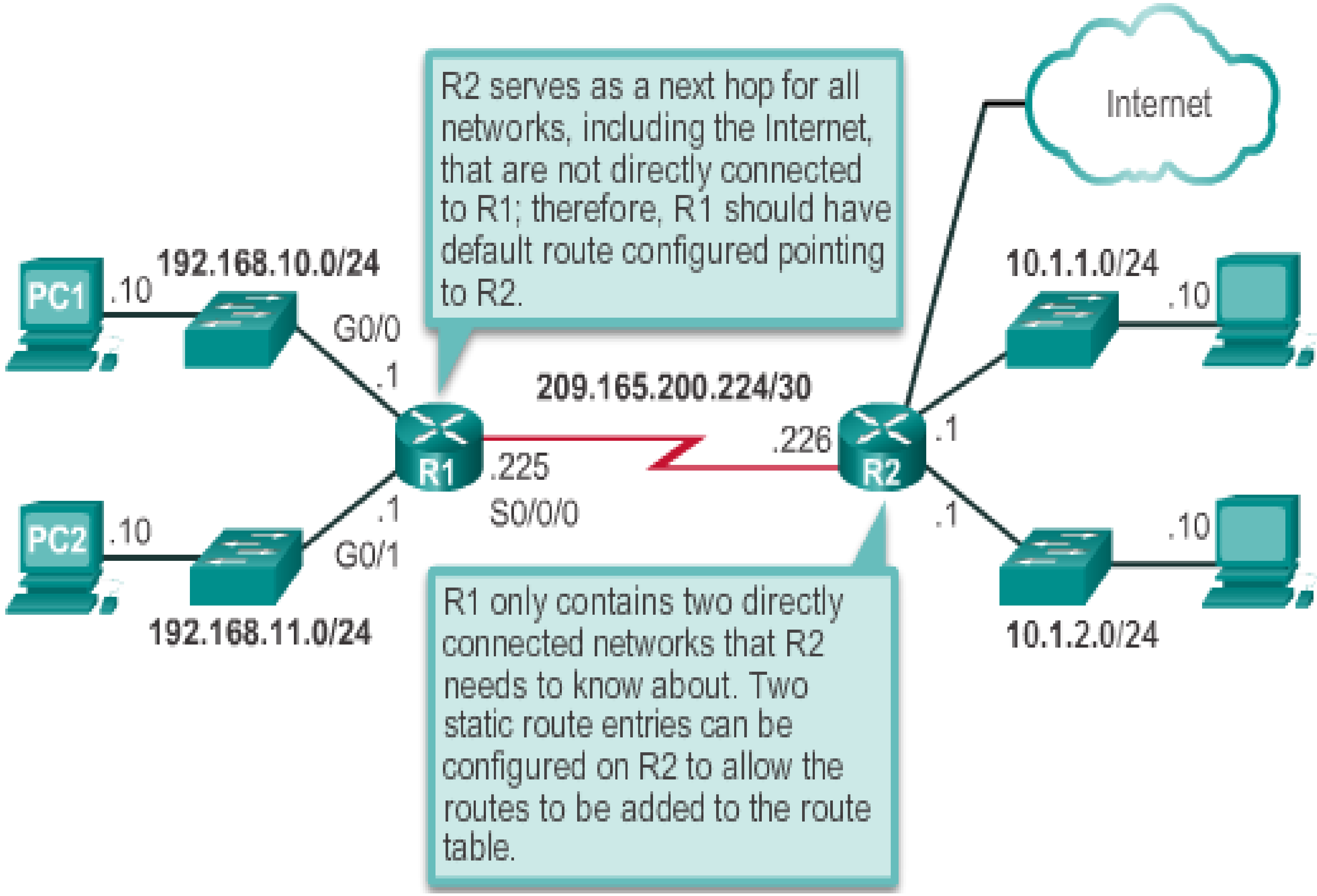

```
R1(config)# interface gigabitethernet 0/1
R1(config-if)# description Link to LAN 2
R1(config-if)# ip address 192.168.11.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)#
```

Directly Connected Example

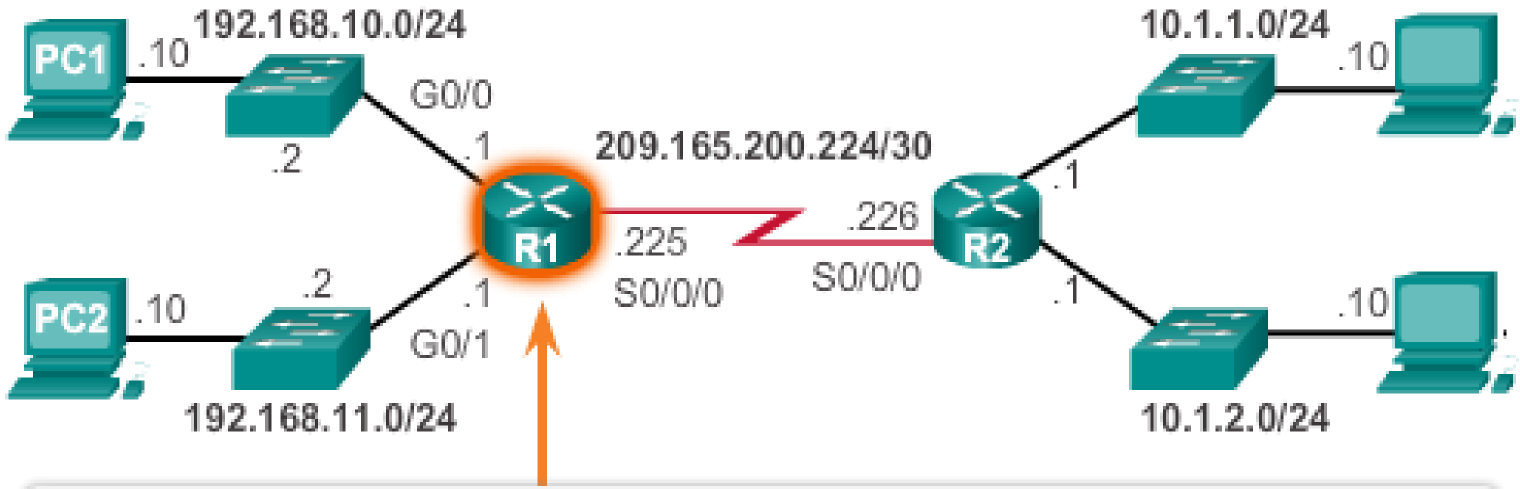



```
R1(config)# interface serial 0/0/0
R1(config-if)# description Link to R1
R1(config-if)# ip address 209.165.200.225 255.255.255.252
R1(config-if)# clock rate 128000
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)#
```

Statically Learned Routes

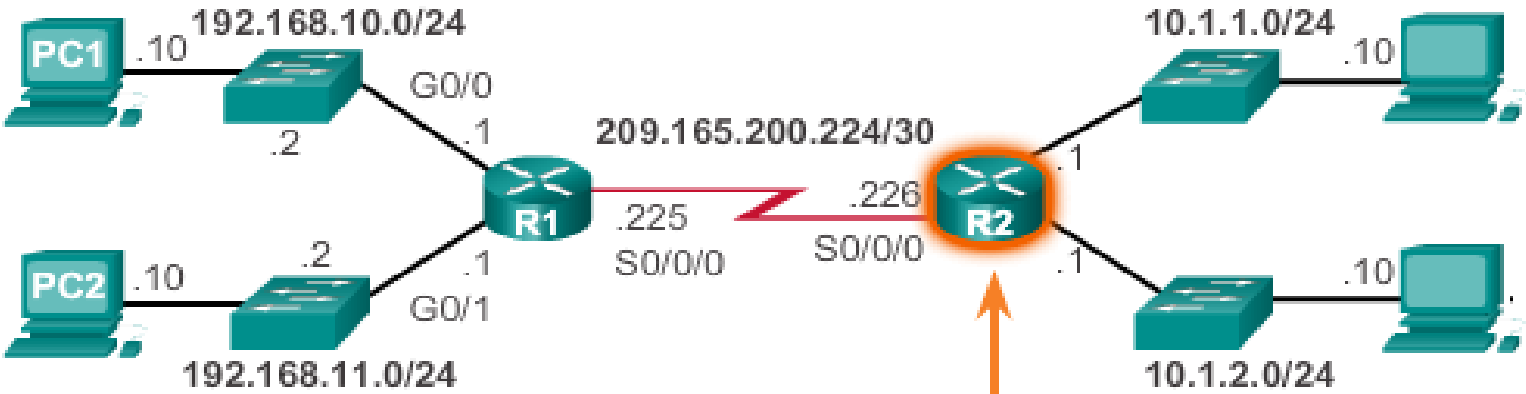


Static Default Route Example



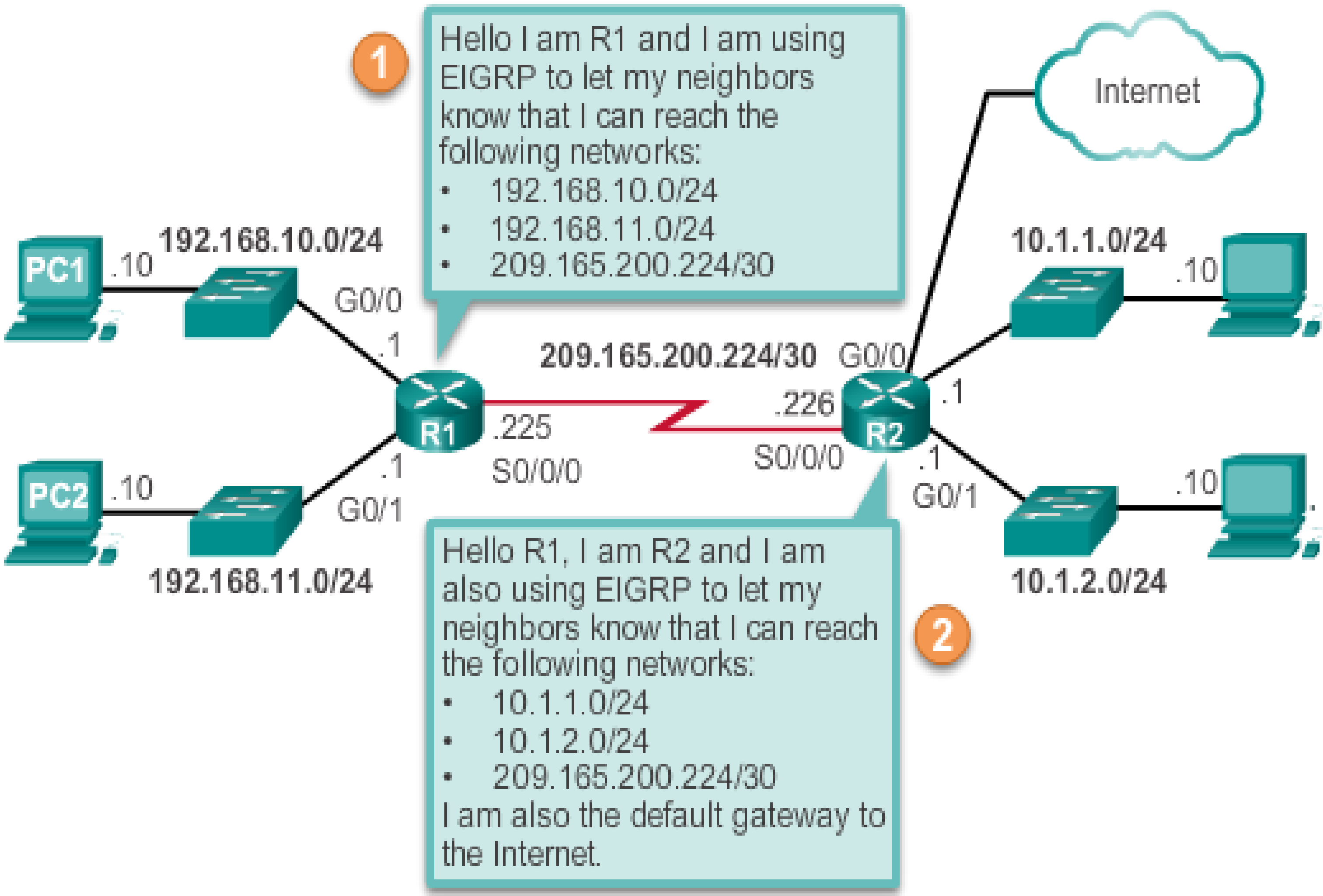

```
R1(config)# ip route 0.0.0.0 0.0.0.0 Serial0/0/0
R1(config)# exit
R1#
*Feb  1 10:19:34.483: %SYS-5-CONFIG_I: Configured from console
by console

R1# show ip route | begin Gateway
Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S* 0.0.0.0/0 is directly connected, Serial0/0/0
   192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.10.0/24 is directly connected, GigabitEthernet0/0
```

Static Route Example




```
R2(config)# ip route 192.168.10.0 255.255.255.0 s0/0/0
R2(config)# ip route 192.168.11.0 255.255.255.0 209.165.200.225
R2(config)# exit
R2#
R2# show ip route | begin Gateway
Gateway of last resort is not set

    10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C     10.1.1.0/24 is directly connected, GigabitEthernet0/0
L     10.1.1.1/32 is directly connected, GigabitEthernet0/0
C     10.1.2.0/24 is directly connected, GigabitEthernet0/1
L     10.1.2.1/32 is directly connected, GigabitEthernet0/1
S    192.168.10.0/24 is directly connected, Serial0/0/0
S    192.168.11.0/24 [1/0] via 209.165.200.225
```

Dynamic Routing



Dynamic Routing Protocols

- Dynamic routing is used by routers to share information about the reachability and status of remote networks.
- It performs network discovery and maintains routing tables.
- Cisco routers can support a variety of dynamic IPv4 routing protocols including:
  - **EIGRP –** Enhanced Interior Gateway Routing Protocol
  - **OSPF –** Open Shortest Path First
  - **IS-IS –** Intermediate System-to-Intermediate System
  - **RIP –** Routing Information Protocol

Directly Connected/Static/Dynamic Routes

Directly
Connected Routes
Static Routes
Dynamic Routing

Packet Tracer – Configuring and Verifying a Small Network

Configure Devices and Verify Connectivity
Gather Information with Show Commands

Packet Tracer – Configuring & Verifying a Small Network - 2

Configure Devices and
Verify Connectivity
Gather Information with
Show Commands

Testing the Network: Ping and ICMPv4

Testing the Network

Testing the Network

- IP is a best effort delivery system.
  - No mechanism to ensure that the data is delivered
- So how do we know if a packet encountered a problem along the way?
- **Internet Control Message Protocol (ICMP)**

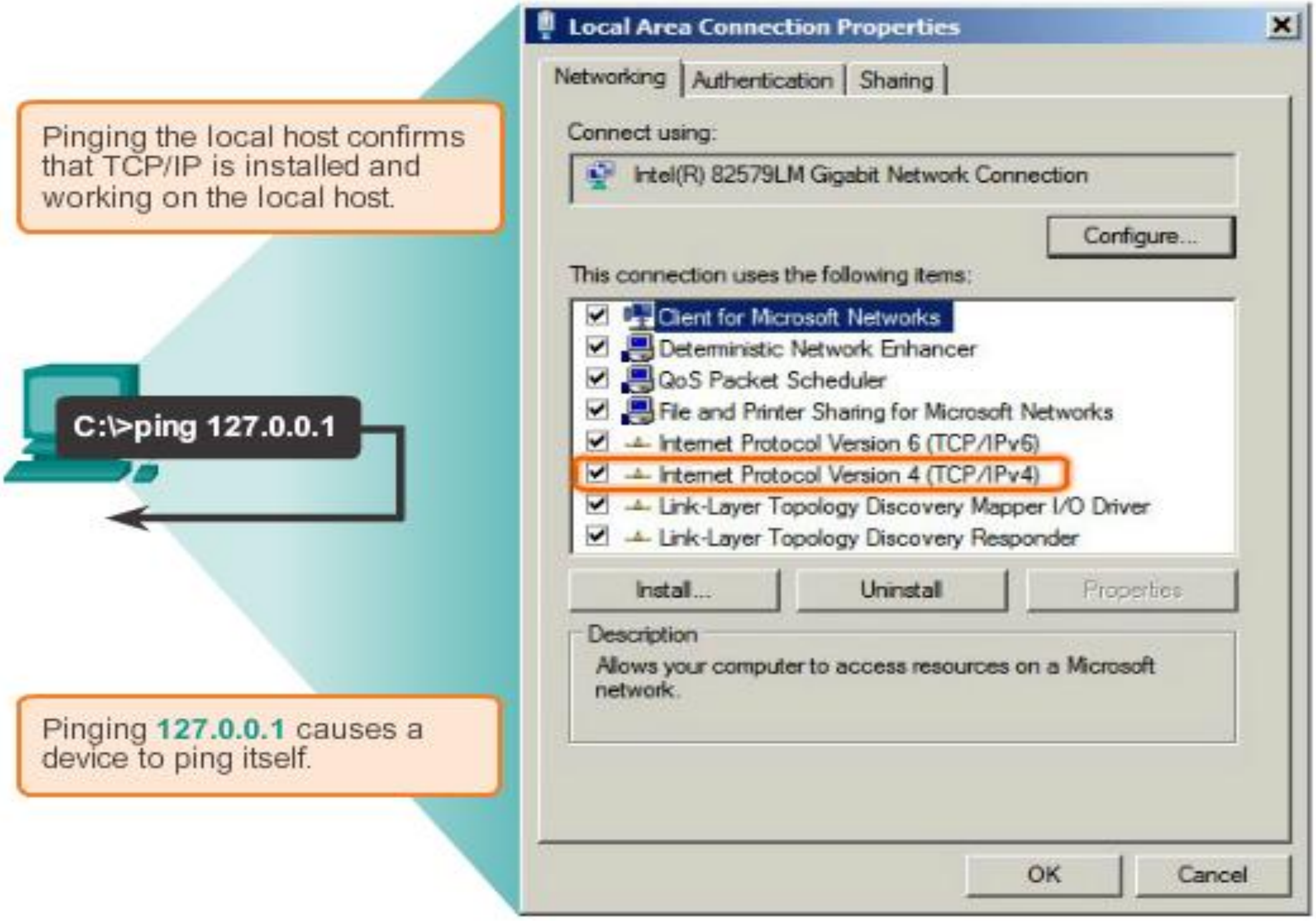
Internet Control Message Protocol (ICMP)

- ICMP is available for both IPv4 and IPv6.
- ICMP is used for::
  - Informational messages (ping, traceroute)
  - Error messages (network unreachable)
- ICMP is a layer 3 protocol directly encapsulated in another layer 3 protocol IP.
  - No transport header
- Knowledge of ICMP control messages is an essential part of network troubleshooting
- The ICMP packets are identified by **type** and **code** fields.

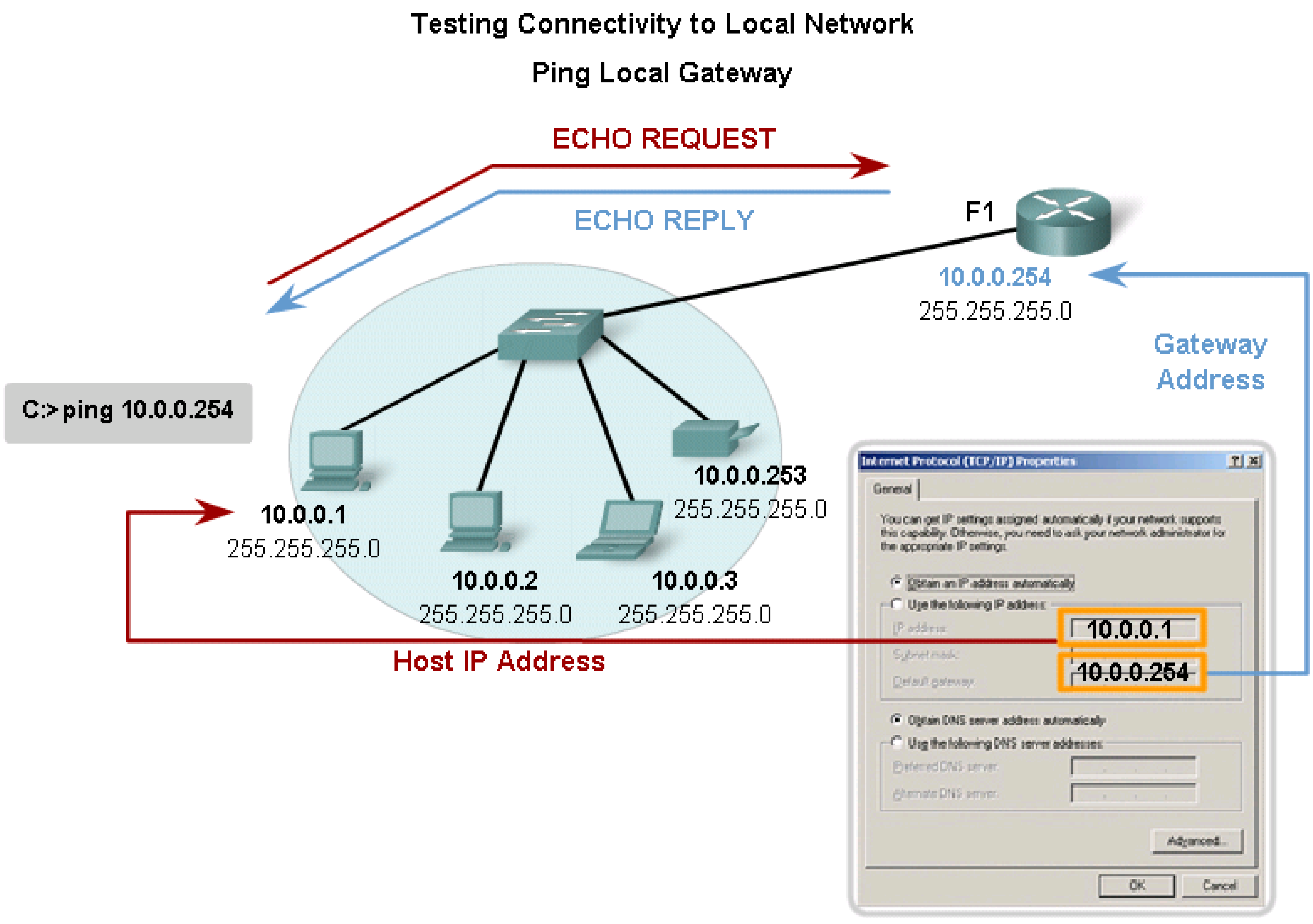
Host Confirmation - Ping

- Ping is a utility used to verify connectivity to an IP host.
  - It measures the round-trip time for messages sent from the originating host to a destination computer.
- Ping uses an ICMP Echo Message to determine if a host is reachable.
  - A host initiates a ping (ICMP Echo Request) and the destination replies (ICMP Echo Reply).
  - ICMP only reports on the status of the delivered packet to the source device.

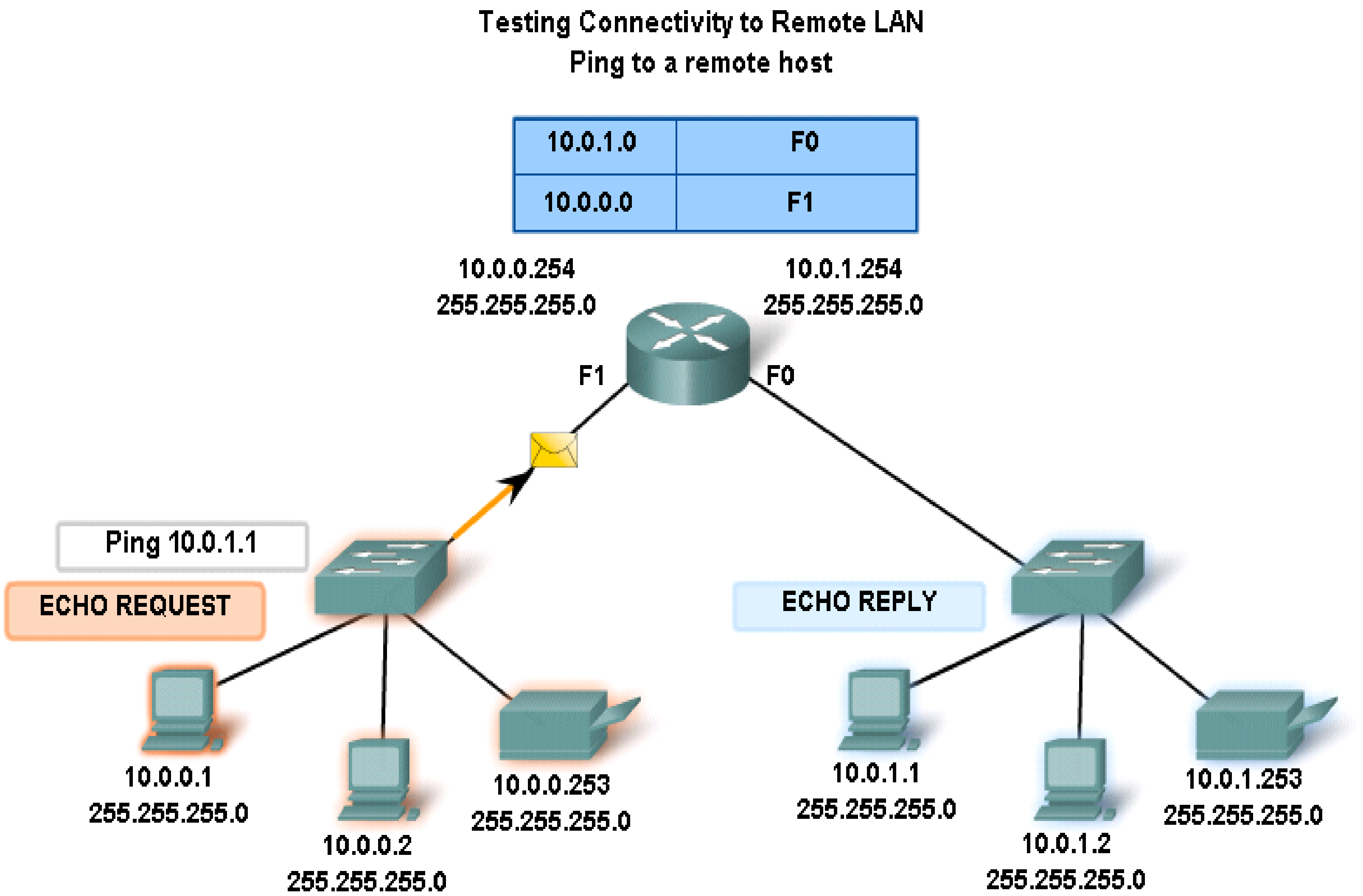
Ping – Testing the Local Stack



Ping – Testing Connectivity to the Local LAN



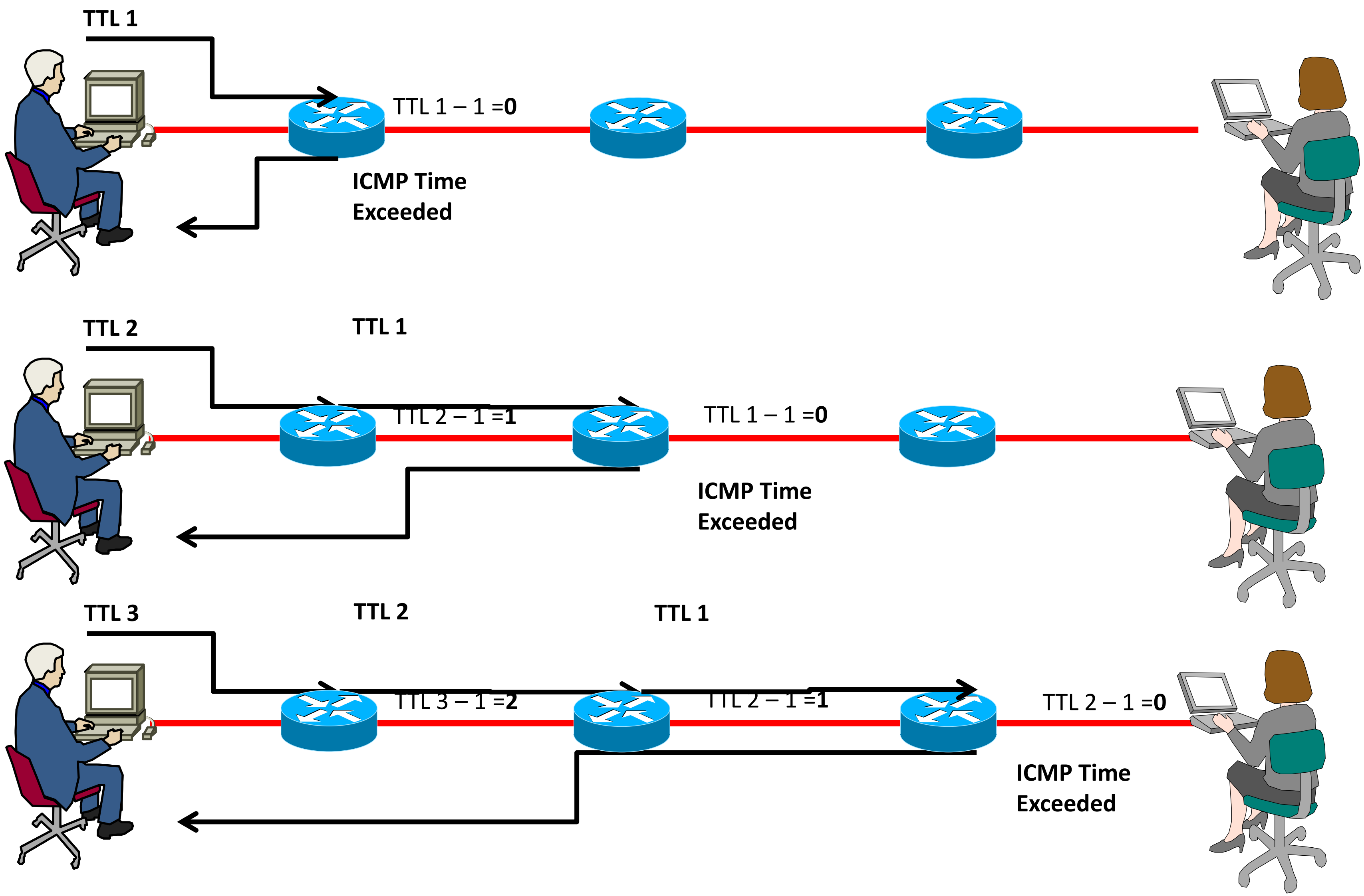
Ping – Testing Connectivity to Remote Host



Traceroute – Testing the Path

- **Ping** is used to indicate the connectivity between two hosts.
- **Traceroute** (**tracert**) is used to observe the path between these hosts.
    - The trace lists hops successfully reached along the way providing us with important verification and troubleshooting information.
    - If the data fails at some hop along the way, we have the address of the last router that responded to the trace indicating where the problem is.

Traceroute – Testing the Path



Testing the Network: Ping and ICMPv4

ICMPv4
Ping
Traceroute

Packet Tracer – Building a Switch and Router Network - 1

Setup Topology
Configure Devices
Verify Connectivity
Display Device Information

Packet Tracer – Building a Switch and Router Network - 2

Setup Topology
Configure Devices
Verify Connectivity
Display Device Information

Packet Tracer – Testing Network Connectivity with Ping & Traceroute

Build and Configure a Network

Ping Command

Tracert/Traceroute Command

Packet Tracer – Testing Network Connectivity with Ping & Traceroute - 2

Build and Configure a Network

Ping Command

Tracert/Traceroute Command