



# Chapter 1: Exploring the Network



## Introduction to Networks

Cisco | Networking Academy®  
Mind Wide Open™



# Chapter 1: Objectives

After completing this chapter, students will be able to:

- Explain how multiple networks are used in everyday life.
- Explain the topologies and devices used in a small- to medium-sized business network.
- Explain the basic characteristics of a network that supports communication in a small- to medium-sized business.
- Explain trends in networking that will affect the use of networks in small to medium-sized businesses.



# Chapter 1

- 1.1 Globally Connected
- 1.2 LANs, WANs, and the Internet
- 1.3 The Network as a Platform
- 1.4 The Changing Network Environment
- 1.5 Summary



## 1.1 Globally Connected



Cisco | Networking Academy®  
Mind Wide Open™



## Networking Today

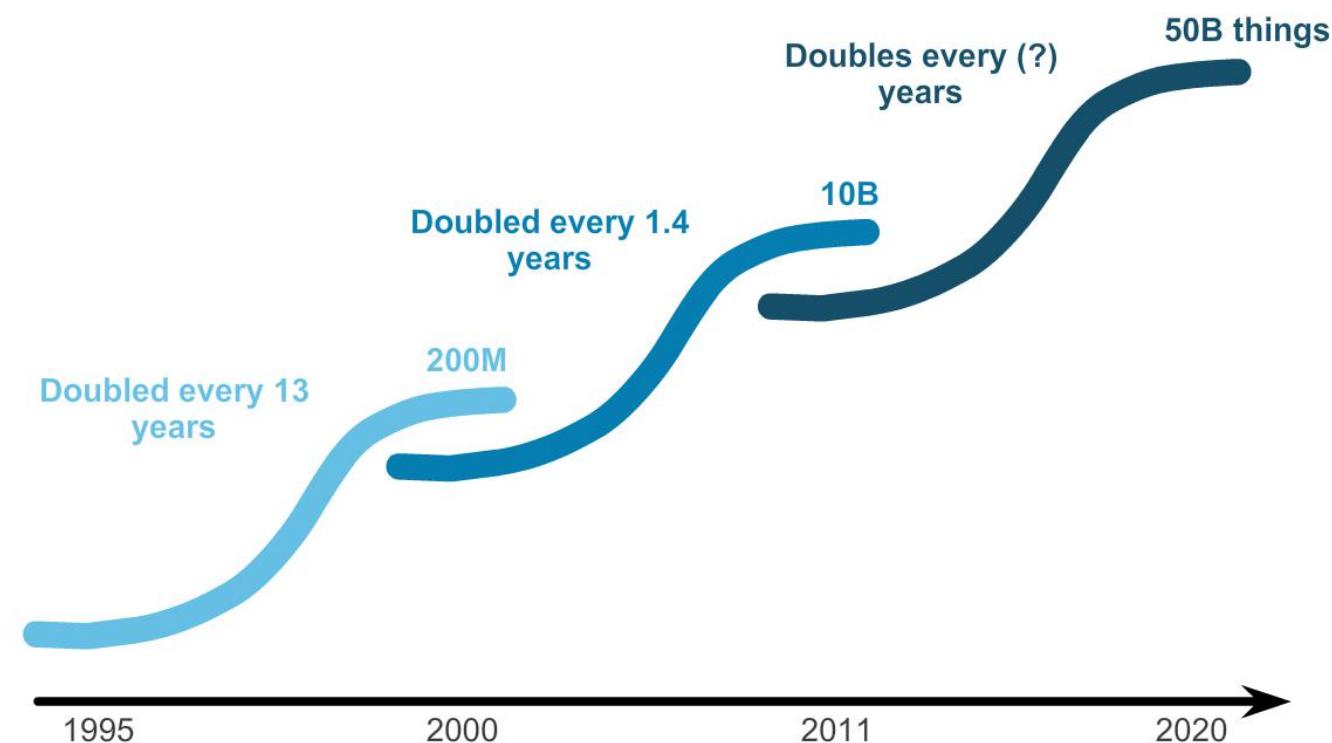
# Networks in Our Past and Daily Lives

**"Fixed"** Computing  
(You go to the device)

**Mobility/BYOD**  
(The device goes with you)

**Internet of Things**  
(Age of Devices)

**Internet of Everything**  
(People, Process, Data, Things)





# Networking Today

# The Global Community





Interconnecting Our Lives

# Networking Impacts in Our Daily Lives

- Networks support the way we learn.
- Networks support the way we communicate.
- Networks support the way we work.
- Networks support the way we play.



# Providing Resources in a Network

## Networks of Many Sizes



Small Home Networks



Small Office/Home Office Networks



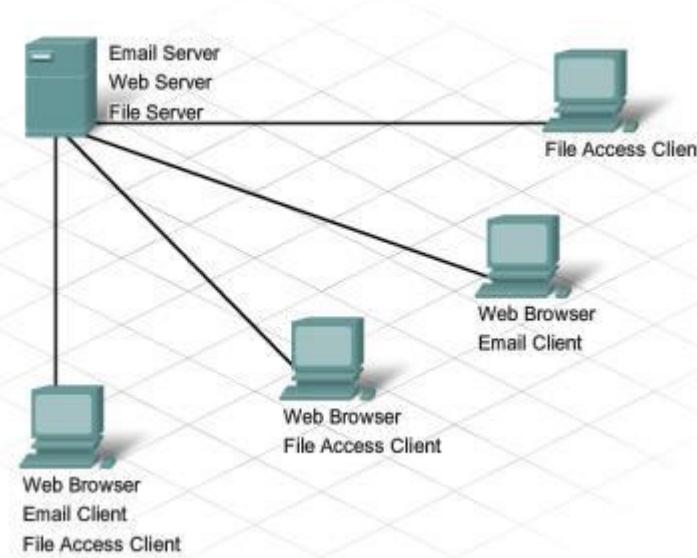
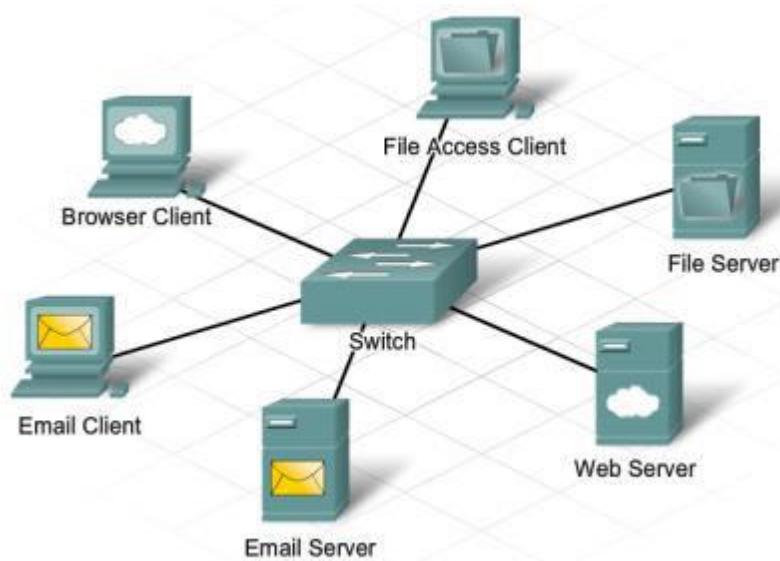
Medium to Large Networks



World Wide Networks



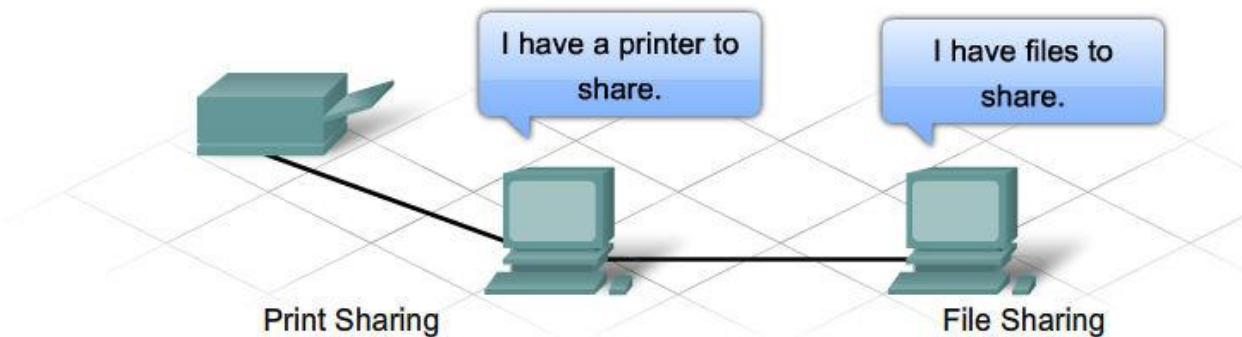
# Providing Resources in a Network Clients and Servers





# Providing Resources in a Network

## Peer-to-Peer



### The advantages of peer-to-peer networking:

- Easy to set up
- Less complexity
- Lower cost since network devices and dedicated servers may not be required
- Can be used for simple tasks such as transferring files and sharing printers

### The disadvantages of peer-to-peer networking:

- No centralized administration
- Not as secure
- Not scalable
- All devices may act as both clients and servers which can slow their performance

## 1.2 LANs, WANs, and the Internet



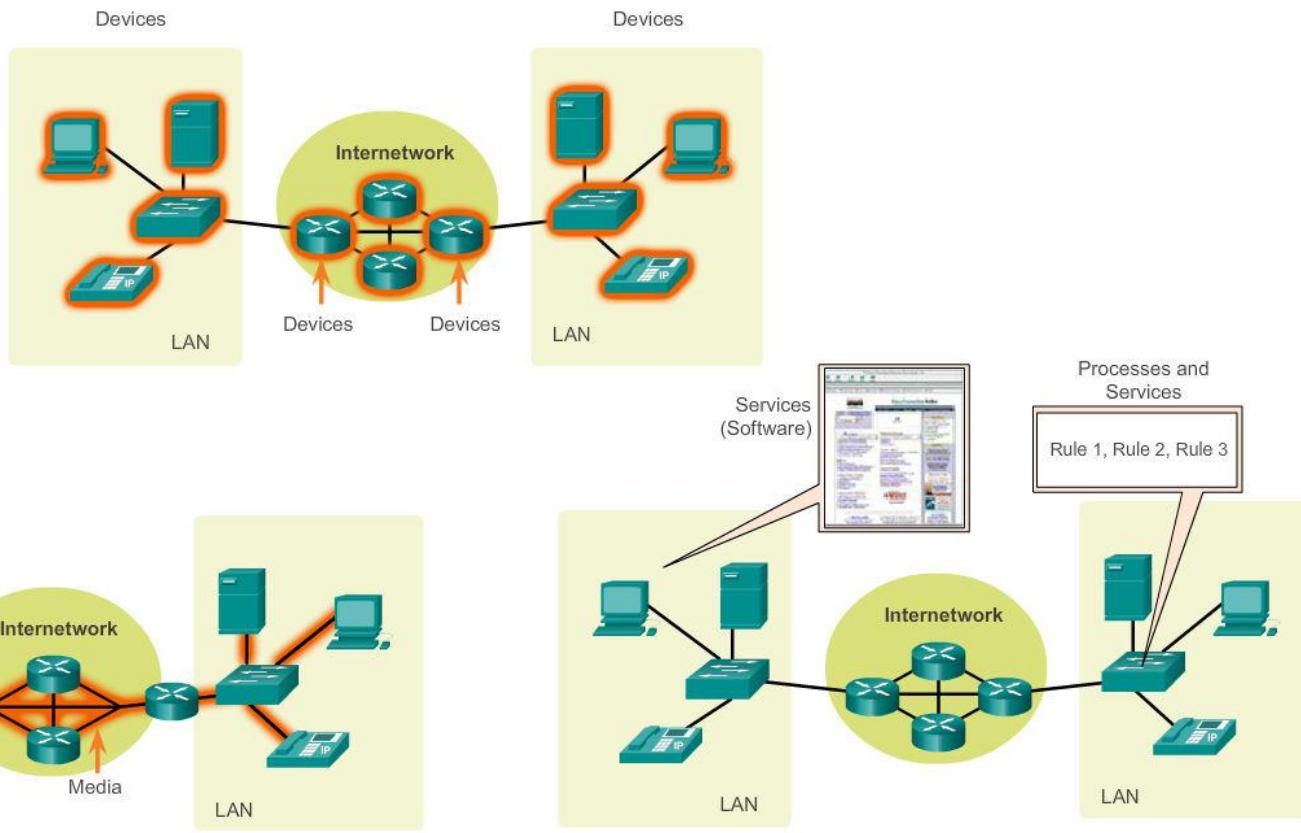


# LANs, WANs, and Internets

# Components of a Network

There are three categories of network components:

- Devices
- Media
- Services





# Components of a Network End Devices

Some examples of end devices are:

- Computers (work stations, laptops, file servers, web servers)
- Network printers
- VoIP phones
- TelePresence endpoint
- Security cameras
- Mobile handheld devices (such as smart phones, tablets, PDAs, and wireless debit / credit card readers and barcode scanners)



## Components of a Network

# Network Infrastructure Devices

Examples of intermediary network devices are:

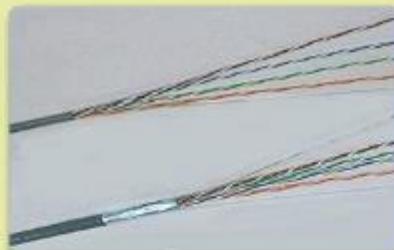
- Network Access Devices (switches, and wireless access points)
- Internetworking Devices (routers)
- Security Devices (firewalls)



# Components of a Network

## Network Media

Copper



Fiber Optic



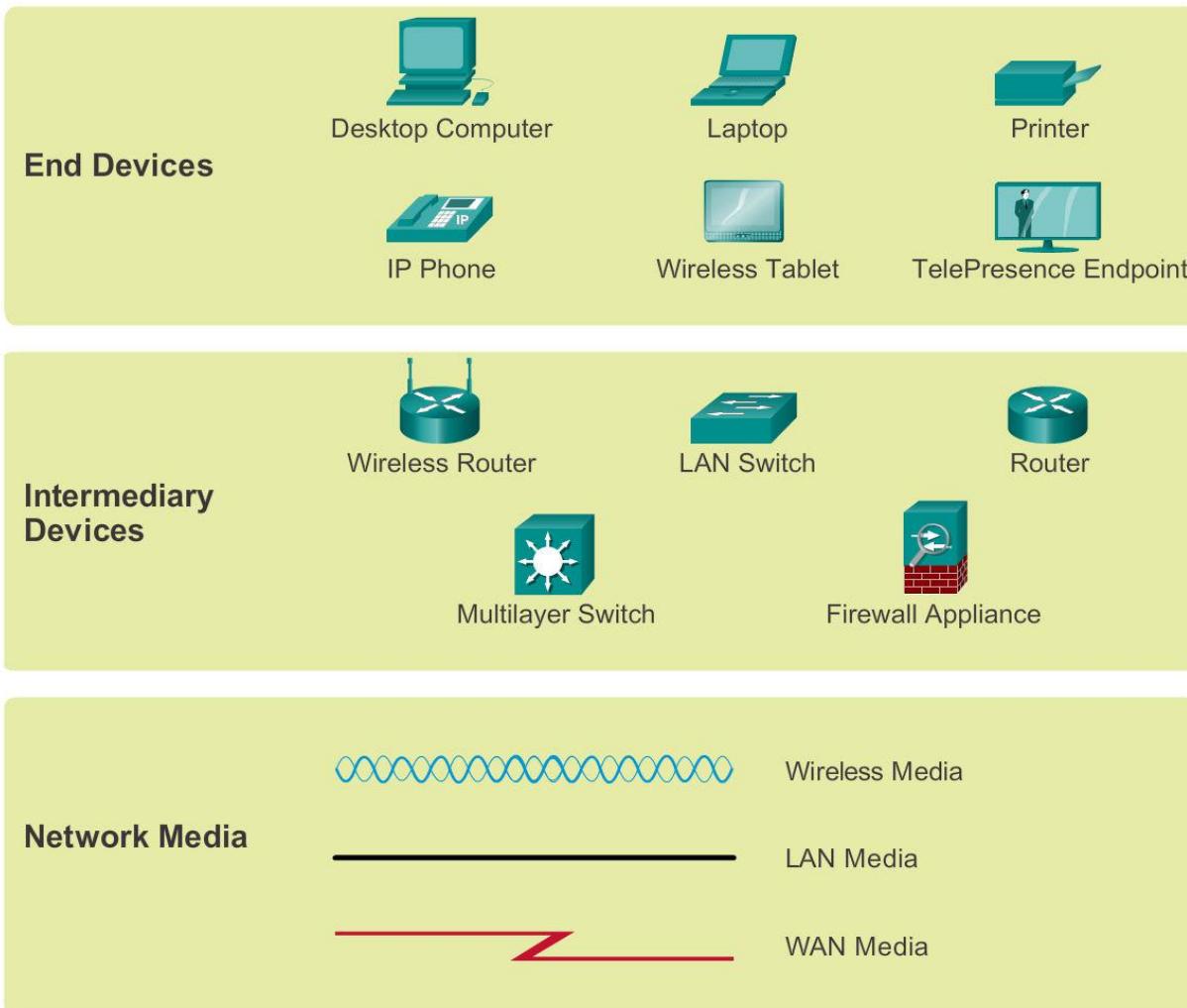
Wireless





# Components of a Network

# Network Representations





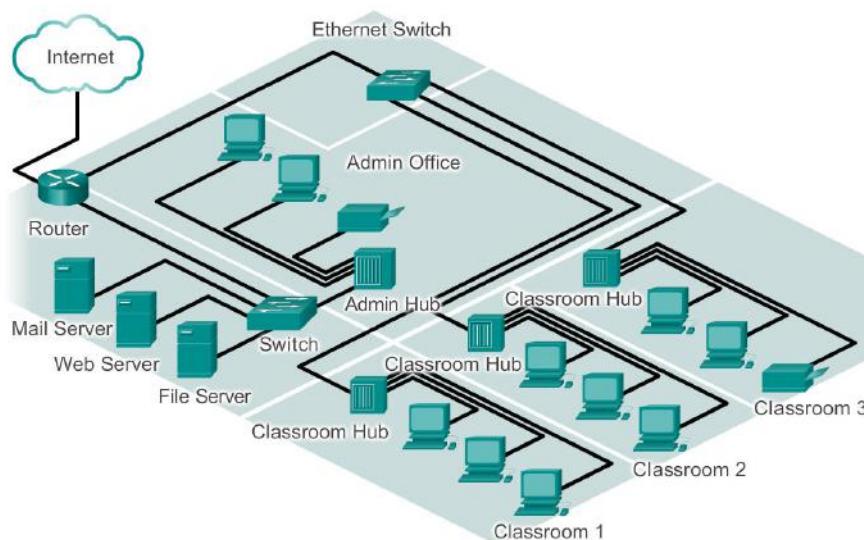
- how each of these devices and media connect to each other. Important terms to remember are:
- **Network Interface Card** - A NIC, or LAN adapter, provides the physical connection to the network at the PC or other end device. The media that are connecting the PC to the networking device, plug directly into the NIC (Figure Next Slide ).
- **Physical Port** - A connector or outlet on a networking device where the media is connected to an end device or another networking device.
- **Interface** - Specialized ports on a networking device that connect to individual networks. Because routers are used to interconnect networks, the ports on a router are referred to as network interfaces.
- **Note:** Often, the terms port and interface are used interchangeably.



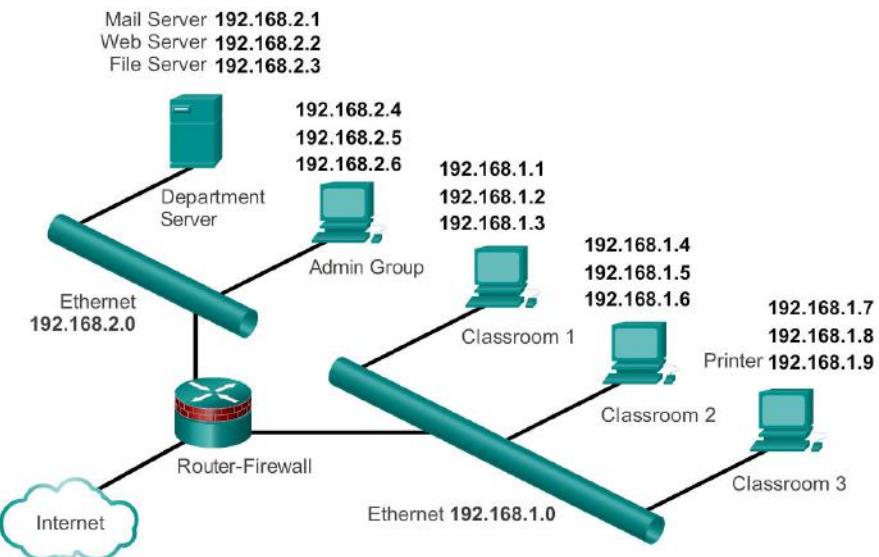


# Components of a Network Topology Diagrams

Physical Topology



Logical Topology





- Topology diagrams are mandatory [ضروري] for anyone working with a network. They provide a visual map of how the network is connected.
- There are two types of topology diagrams:
- **Physical topology diagrams** - Identify the physical location of intermediary devices and cable installation. (Figure 1)
- **Logical topology diagrams** - Identify devices, ports, and addressing scheme. (Figure 2)



## LANs and WANs

# Types of Networks

# Network infrastructures can vary greatly in terms of:

- \* Size of the area covered
- \* Number of users connected
- \* Number and types of services available
- \* Area of responsibility

The two most common types of network infrastructures are:

- Local Area Network (LAN)
- Wide Area Network (WAN).

Other types of networks include:

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



## LANs and WANs

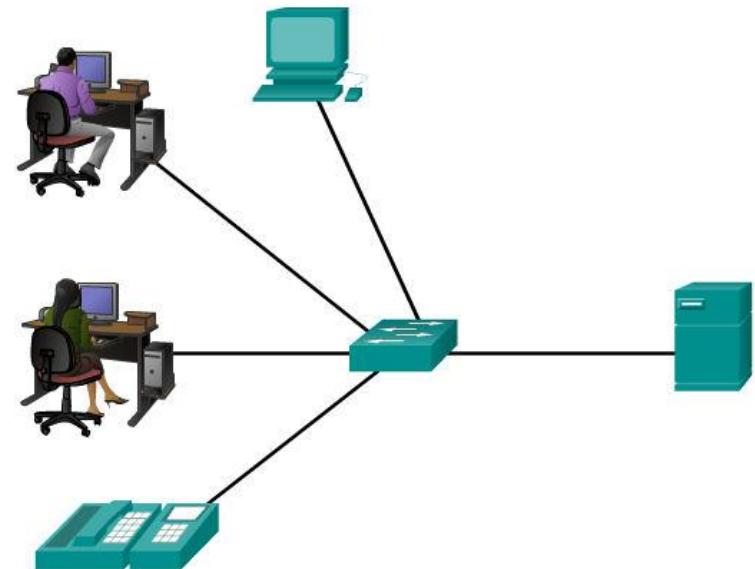
# Local Area Networks (LAN)

LANs are a network infrastructure that spans a small geographical area. Specific features of LANs include:

LANs interconnect end devices in a limited area such as a home, school, office building, or campus.

A LAN is usually administered by a single organization or individual. The administrative control that governs the security and access control policies are enforced on the network level.

LANs provide high speed bandwidth to internal end devices and intermediary devices.



A network serving a home, building, or campus is considered a LAN.

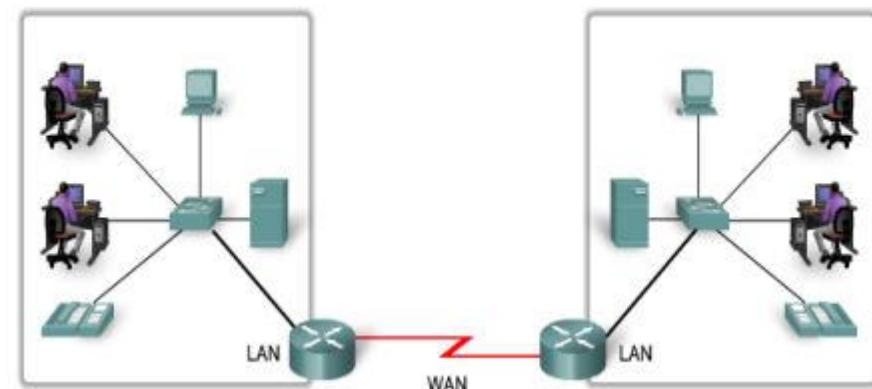


## LANs and WANs

# Wide Area Networks (WAN)

- WANs are a network infrastructure that spans a wide geographical area. WANs are typically managed by service providers (SP) or Internet Service Providers (ISP).
- Specific features of WANs include:
- WANs interconnect LANs over wide geographical areas such as between cities, states, provinces, countries, or continents.
- WANs are usually administered by multiple service providers.
- WANs typically provide slower speed links between LANs.

LANS separated by geographic distance are connected by a network known as a Wide Area Network (WAN).



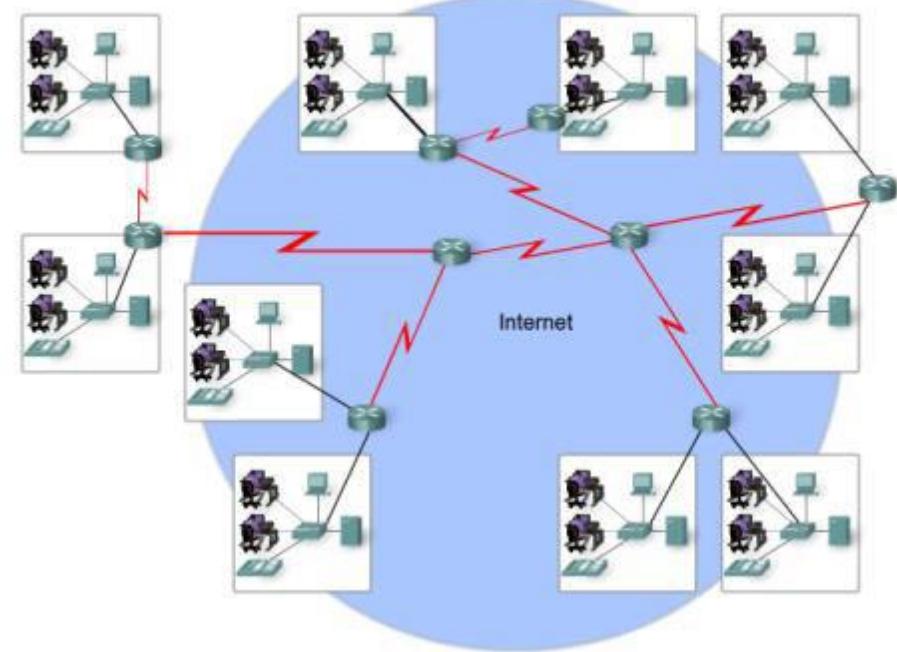


## LANs, WANs, and the Internet

# The Internet

The Internet is a worldwide collection of interconnected networks (internetworks or internet for short). The figure shows one way to view the Internet as a collection of interconnected LANs and WANs. Some of the LAN examples are connected to each other through a WAN connection. WANs are then connected to each other. The red WAN connection lines represent all the varieties of ways we connect networks. WANs can connect through copper wires, fiber optic cables, and wireless transmissions

LANs and WANs may be connected into internetworks.





## LANs, WANs, and the Internet

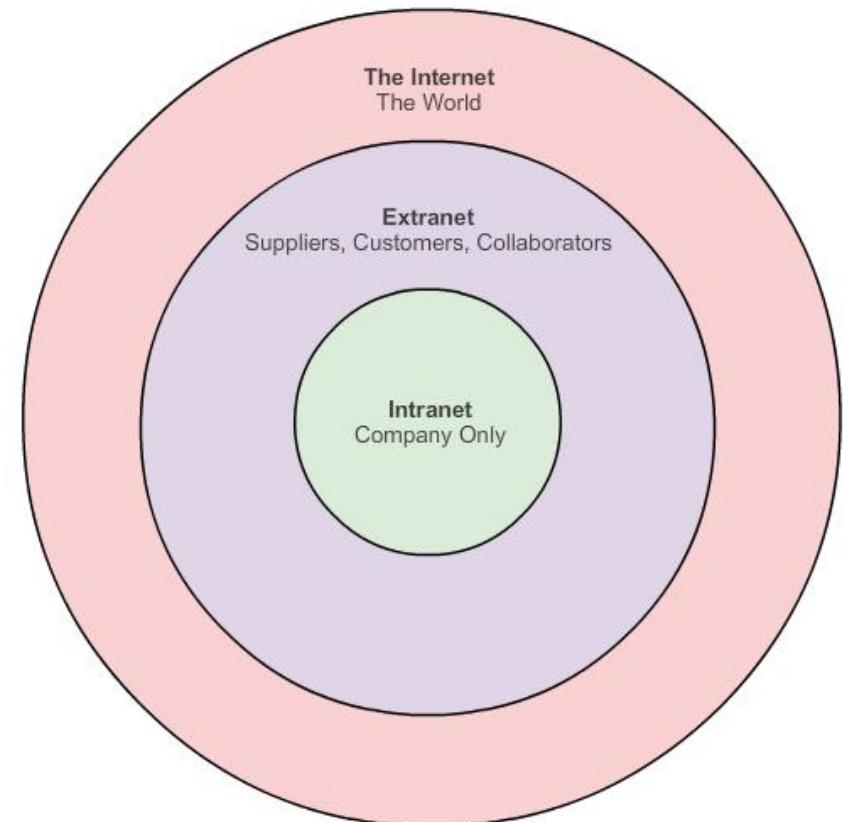
# Intranet and Extranet

There are two other terms which are similar to the term Internet: 1- Intranet 2- Extranet

Intranet is a term often used to refer to a private connection of LANs and WANs that belongs to an organization, and is designed to be accessible only by the organization's members, employees, or others with authorization.

An organization may use an extranet to provide secure and safe access to individuals who work for a different organization, but require access to the organization's data. Examples of extranets include:

- A company that is providing access to outside suppliers and contractors.
- A hospital that is providing a booking system to doctors so they can make appointments for their patients.
- A local office of education that is providing budget and personnel information to the schools in its district.





## Connecting to the Internet

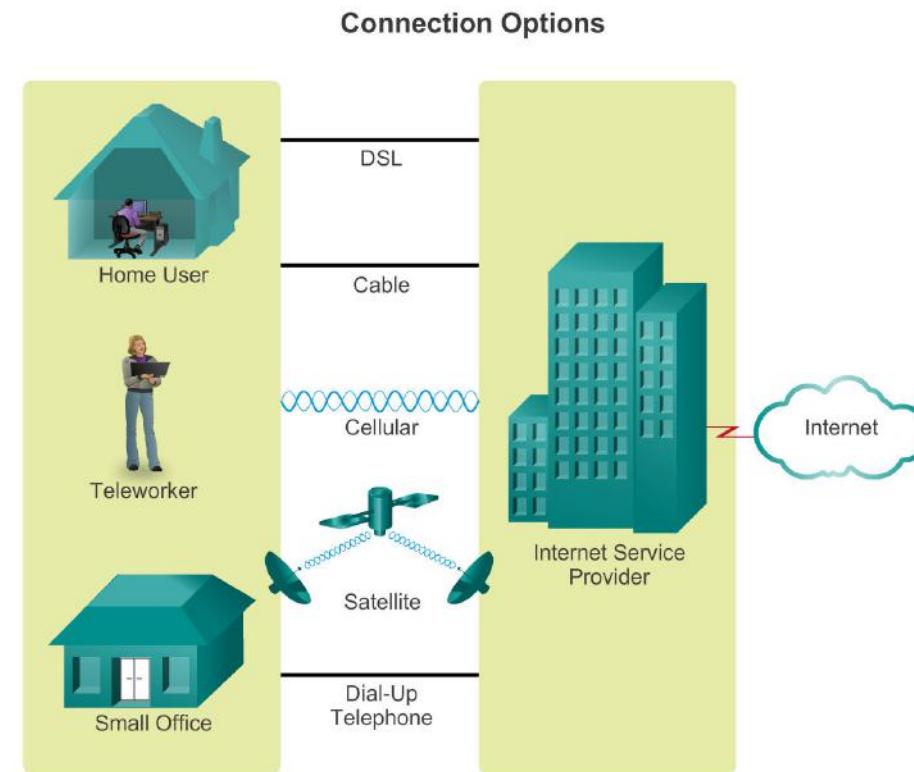
# Connecting Remote Users to the Internet

The figure illustrates common connection options for small office and home office users:

**Cable** - Typically offered by cable television service providers, the Internet data signal is carried on the same cable that delivers cable television. It provides a high bandwidth, always on, connection to the Internet.

**DSL** - Digital Subscriber Lines provide a high bandwidth, always on, connection to the Internet. DSL runs over a telephone line. In general, small office and home office users connect using Asymmetrical DSL (ADSL), which means that the download speed is faster than the upload speed.

**Cellular** - Cellular Internet access uses a cell phone network to connect. Wherever you can get a cellular signal, you can get cellular Internet access. Performance will be limited by the capabilities of the phone and the cell tower to which it is connected.





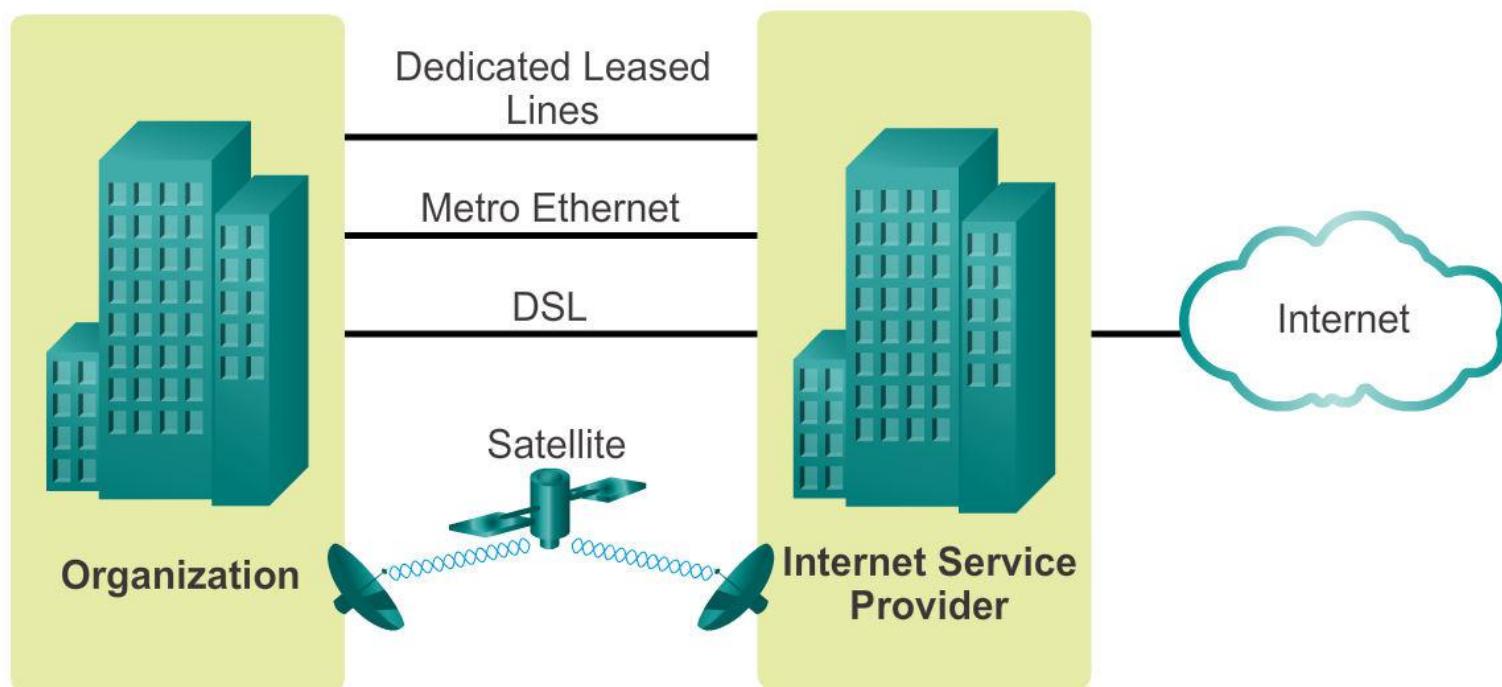
- **Satellite** - The availability of satellite Internet access is a real benefit in those areas that would otherwise have no Internet connectivity at all. Satellite dishes require a clear line of sight to the satellite.
- **Dial-up Telephone** - An inexpensive option that uses any phone line and a modem. The low bandwidth provided by a dial-up modem connection is usually not sufficient for large data transfer, although it is useful for mobile access while traveling.
- Many homes and small offices are more commonly being connected directly with fiber optic cables. This enables an ISP to provide higher bandwidth speeds and support more services such as Internet, phone, and TV.
- The choice of connection varies depending on geographical location and service provider availability.



Connecting to the Internet

# Connecting Businesses to the Internet

## Connection Options





- **common connection options for businesses:**
- **Dedicated Leased Line** - Leased lines are actually reserved circuits within the service provider's network that connect geographically separated offices for private voice and/or data networking. The circuits are typically rented at a monthly or yearly rate. They can be expensive.
- **Ethernet WAN** - Ethernet WANs extend LAN access technology into the WAN. Ethernet is a LAN technology you will learn about in a later chapter. The benefits of Ethernet are now being extended into the WAN.
- **DSL** - Business DSL is available in various formats. A popular choice is Symmetric Digital Subscriber Lines (SDSL) which is similar to the consumer version of DSL, but provides uploads and downloads at the same speeds.
- **Satellite** - Similar to small office and home office users, satellite service can provide a connection when a wired solution is not available.

## 1.3 The Network as a Platform

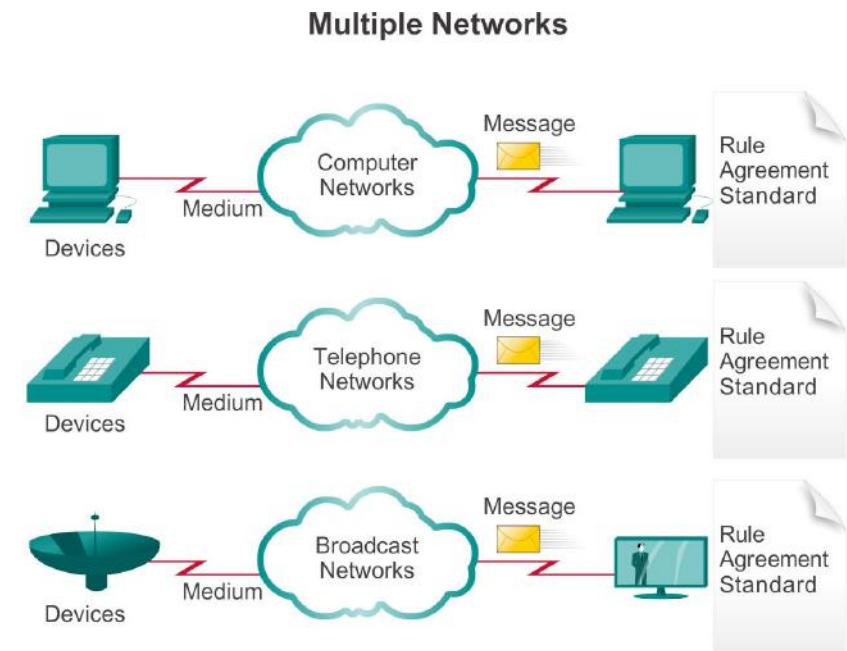




## Converged Networks

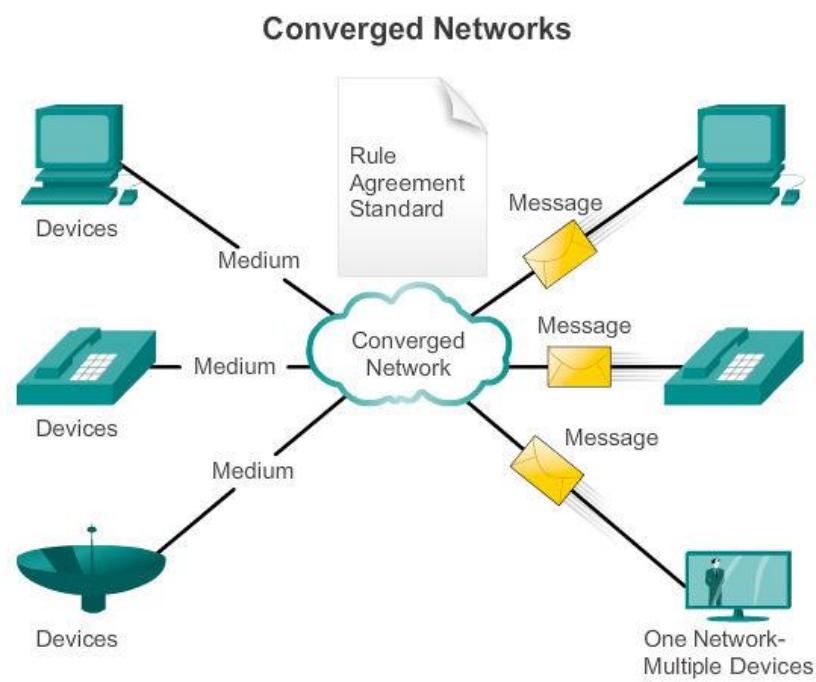
# The Converging (متقارب) Network

Consider a school built thirty years ago. Back then, some classrooms were cabled for the data network, telephone network, and video network for televisions. These separate networks could not communicate with each other, as shown in the figure. Each network used different technologies to carry the communication signal. Each network had its own set of rules and standards to ensure successful communication.





- Today, the separate data, telephone, and video networks are converging. Unlike dedicated networks, converged networks are capable of delivering data, voice, and video between many different types of devices over the same network infrastructure, as shown in the figure. This network infrastructure uses the same set of rules, agreements, and implementation standards.



Converged data networks carry multiple services on one network.



# Converged Networks

# Planning for the Future

## Intelligent Networks Are Bringing the World Together



Intelligent networks allow handheld devices to receive news and emails, and to send text.



Video conferencing around the globe is in the palm of your hand.



Phones connect globally to share voice, text, and images.



Online gaming connects thousands of people seamlessly.



## Reliable Network

# Supporting Network Architecture

As networks evolve, we are discovering that there are four basic characteristics that the underlying architectures need to address in order to meet user expectations:

- Fault Tolerance
- Scalability
- Quality of Service (QoS)
- Security



# Fault Tolerance

- A fault tolerant network is one that limits the impact of a failure, so that the fewest number of devices are affected. It is also built in a way that allows quick recovery when such a failure occurs.
- These networks depend on multiple paths between the source and destination of a message. If one path fails, the messages can be instantly sent over a different link. Having multiple paths to a destination is known as redundancy.
- One way reliable networks provide redundancy is by implementing a packet-switched network.
- Packet switching splits traffic into packets that are routed over a shared network. A single message, such as an email or a video stream, is broken into multiple message blocks, called packets.
- Each packet has the necessary addressing information of the source and destination of the message.
- The routers within the network switch the packets based on the condition of the network at that moment. This means that all the packets in a single message could take very different paths to the destination.



# Fault Tolerance

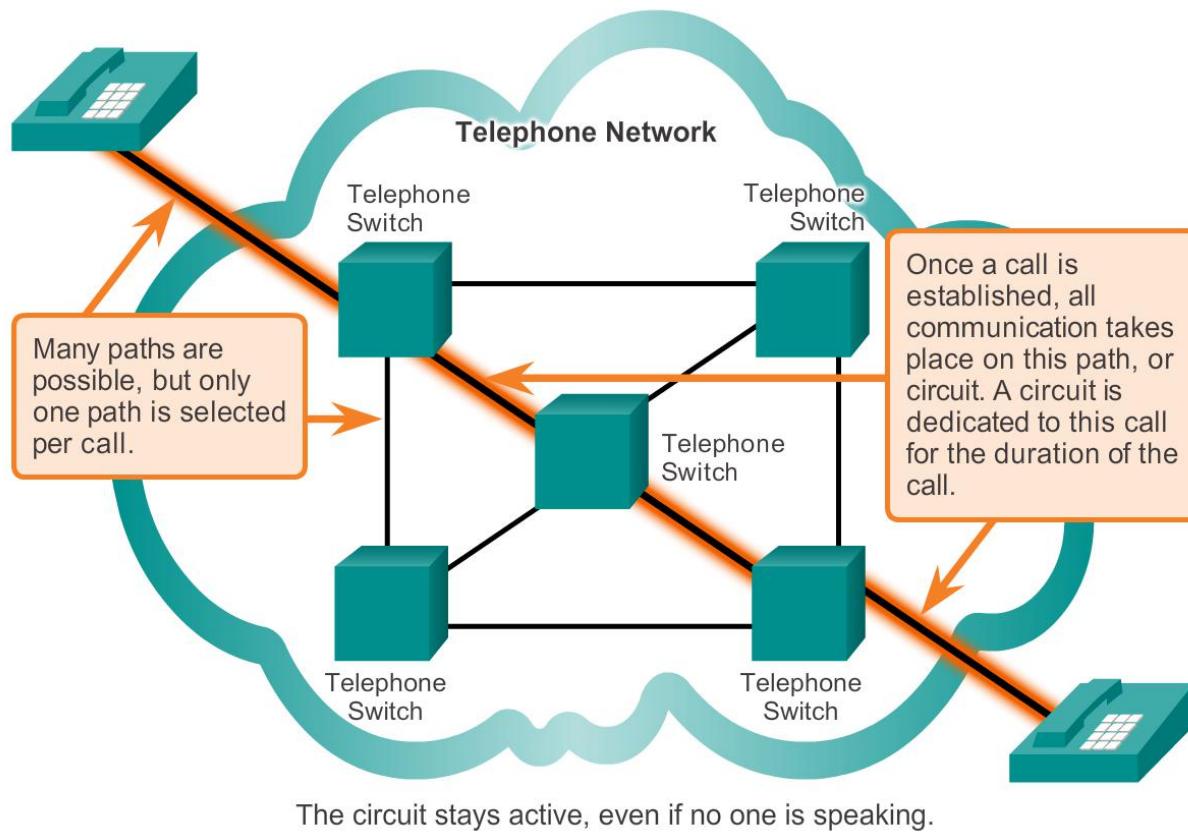
- This is not the case in circuit-switched networks traditionally used for voice communications.
- A circuit-switched network is one that establishes a dedicated circuit between the source and destination before the users may communicate. If the call is unexpectedly terminated, the users must initiate a new connection.



## Reliable Network

# Fault Tolerance in Circuit Switched Network

Circuit Switching in a Telephone Network



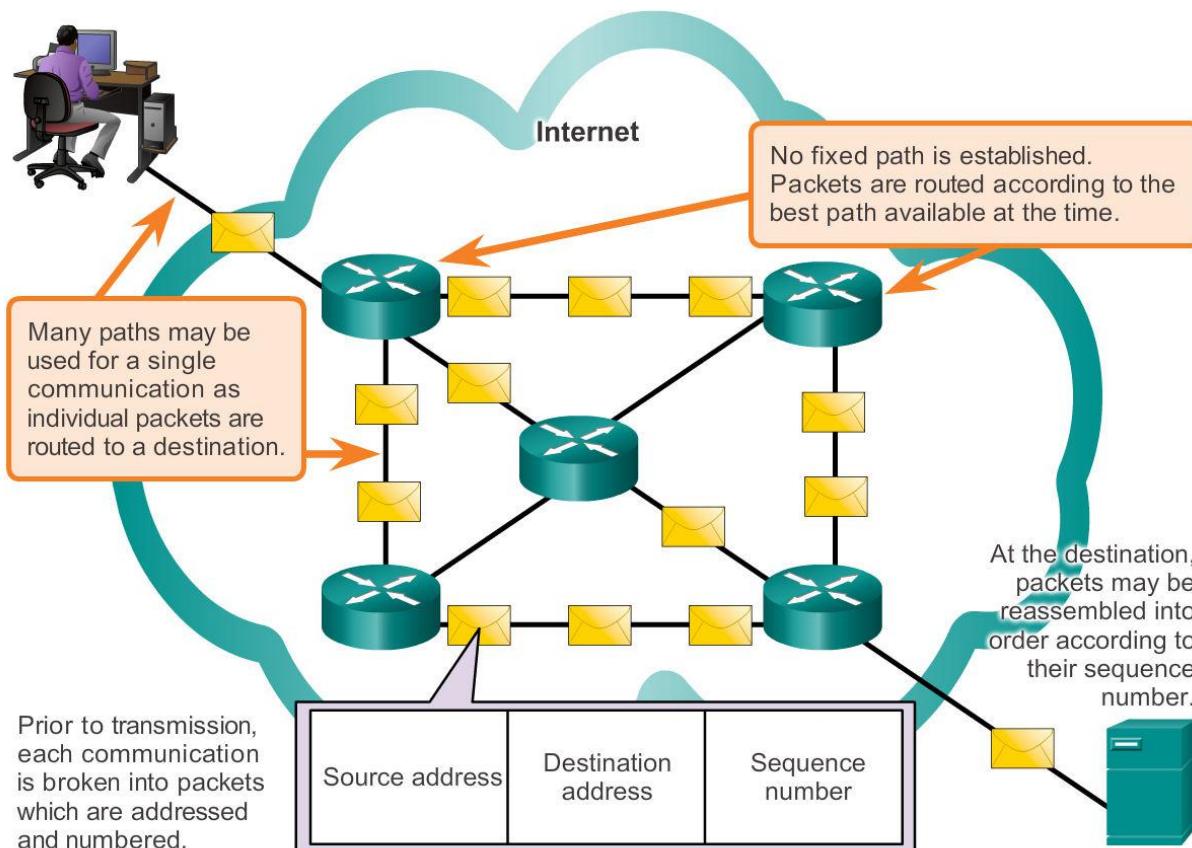
There are many, many circuits, but a finite number. During peak periods, some calls may be denied.



## Reliable Network

# Packet-Switched Networks

### Packet Switching in a Data Network



Prior to transmission, each communication is broken into packets which are addressed and numbered.

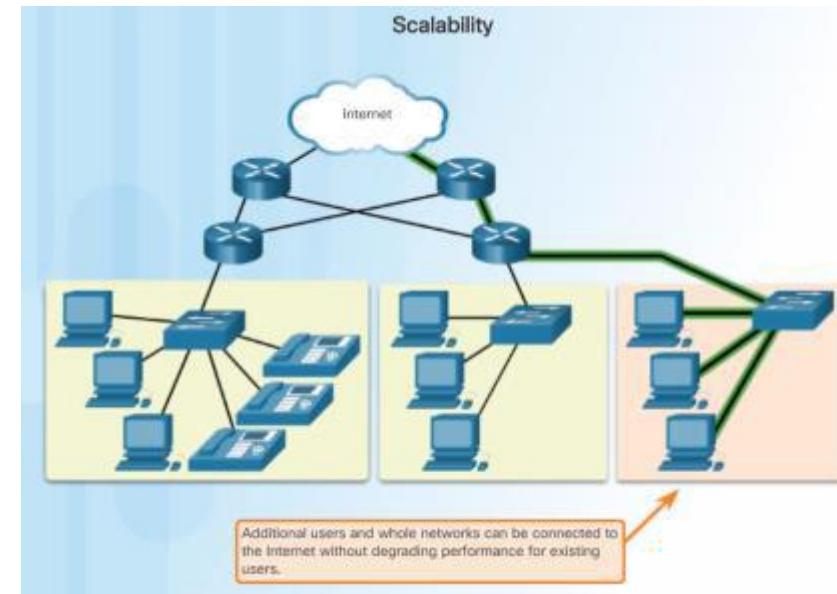
During peak periods, communication may be delayed, but not denied.



## Reliable Network

# Scalable Networks

- A scalable network can expand quickly to support new users and applications without impacting the performance of the service being delivered to existing users.
- The figure shows how a new network can be easily added to an existing network.
- In addition, networks are scalable because the designers follow accepted standards and protocols. This allows software and hardware vendors to focus on improving products and services without worrying about designing a new set of rules for operating within the network.





# Reliable Network Providing QoS

Examples of priority decisions for an organization might include:

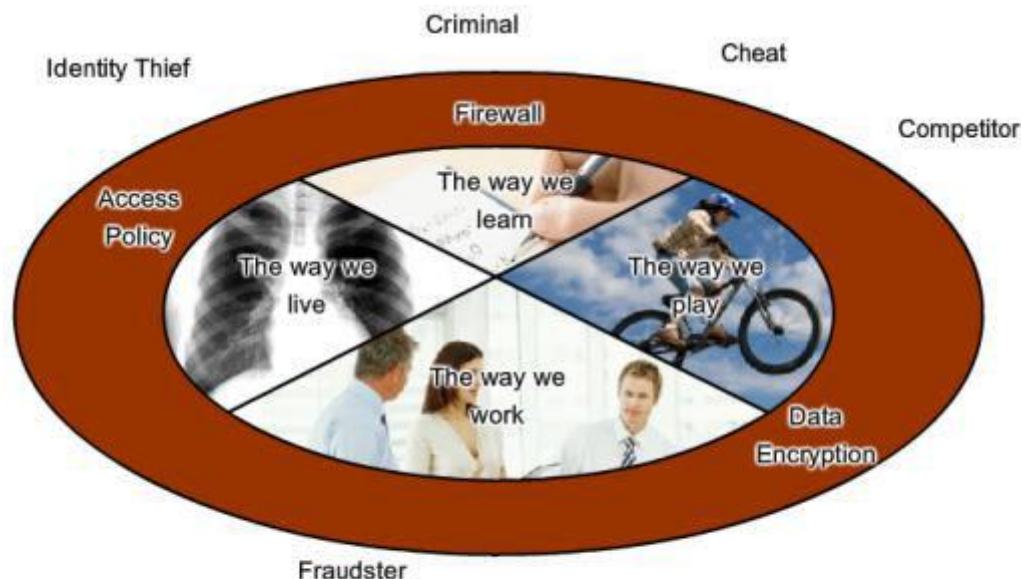
- Time-sensitive communication - increase priority for services like telephony or video distribution.
- Non time-sensitive communication - decrease priority for web page retrieval or email.
- High importance to organization - increase priority for production control or business transaction data.
- Undesirable communication - decrease priority or block unwanted activity, like peer-to-peer file sharing or live entertainment.



## Reliable Network

# Providing Network Security

- There are two types of network security concerns that must be addressed:
  1. network infrastructure security
  2. information security



The communication and information that we would like to be private is protected from those who would make unauthorized use of it.



- Securing a network infrastructure includes the physical securing of devices that provide network connectivity, and preventing unauthorized access to the management software that resides on them.
- Information security refers to protecting the information contained within the packets being transmitted over the network and the information stored on network attached devices.

## 1.4 The Changing Network Environment





# Network Trends

## New trends

Some of the top trends include:

- Bring Your Own Device (BYOD)
- Online collaboration
- Video
- Cloud computing



## Network Trends

# Bring Your Own Device (BYOD)



The concept of any device, to any content, in anyway is a major global trend that requires significant changes to the way devices are used. This trend is known as Bring Your Own Device (BYOD).



# Network Trends

# Online Collaboration

## Collaboration



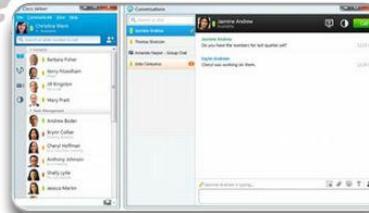
IP Communication



Mobile Applications



Telepresence



Messaging



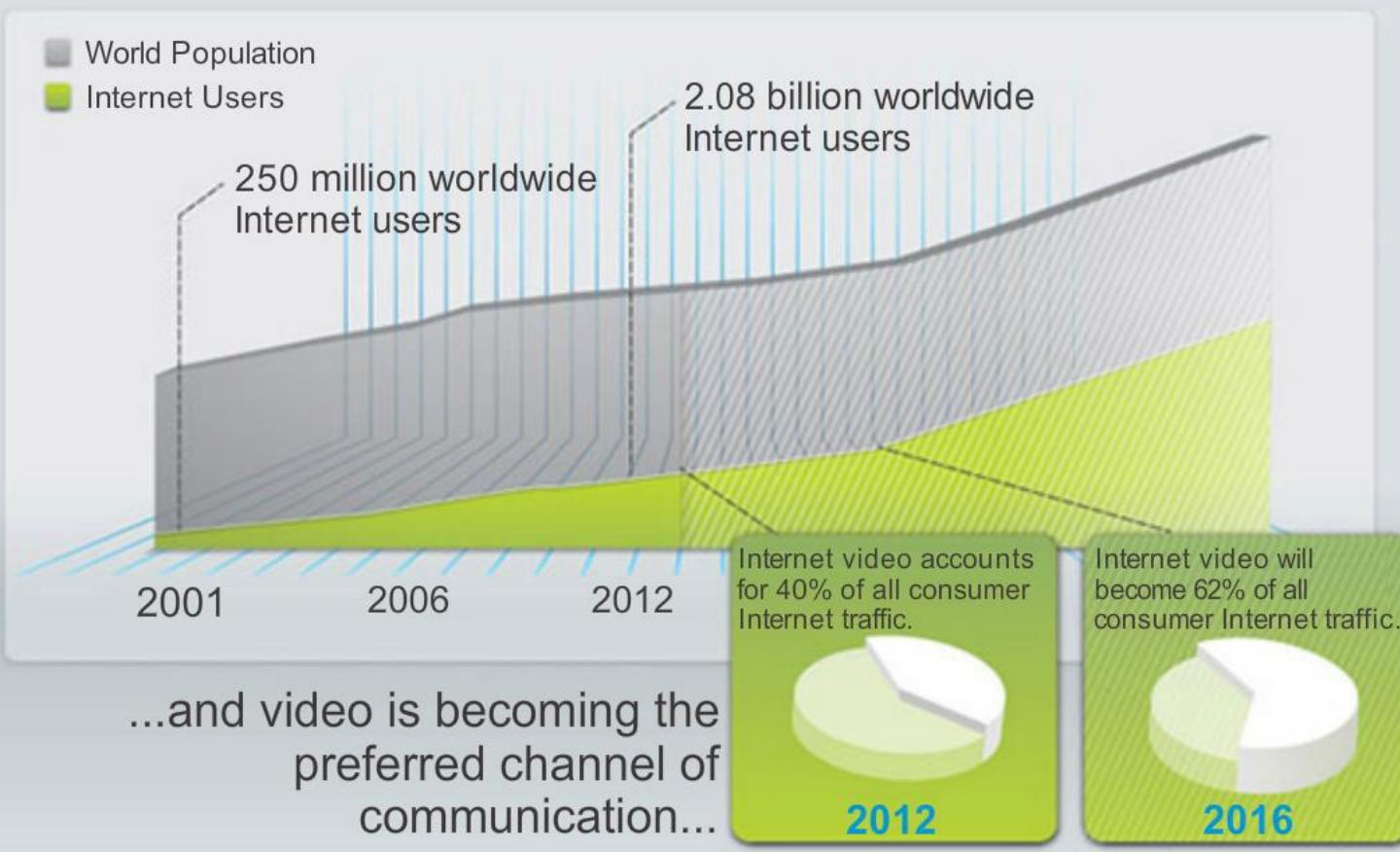
Online Conferencing



## Network Trends

# Video Communication

People are becoming more connected...





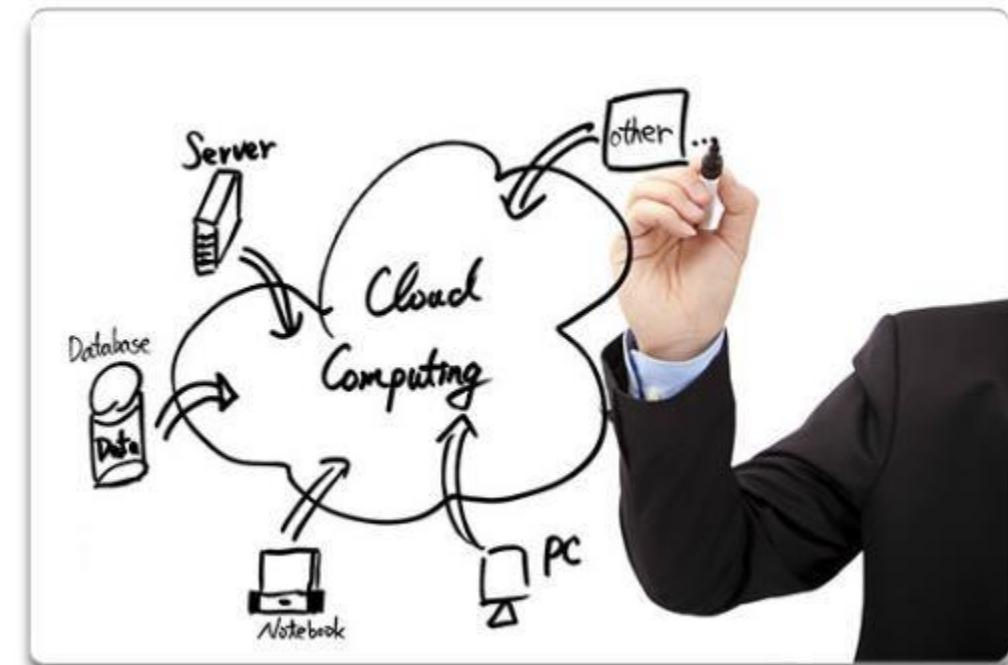
## Network Trends

# Cloud Computing

- Cloud computing is another global trend changing the way we access and store data. Cloud computing allows us to store personal files, even backup our entire hard disk drive on servers over the Internet. Applications such as word processing and photo editing can be accessed using the Cloud.

Cloud computing offers the following potential benefits:

- Organizational flexibility
- Agility and rapid deployment
- Reduced cost of infrastructure
- Refocus of IT resources
- Creation of new business models





## Network Trends

# Data Centers

A data center is a facility used to house computer systems and associated components including:

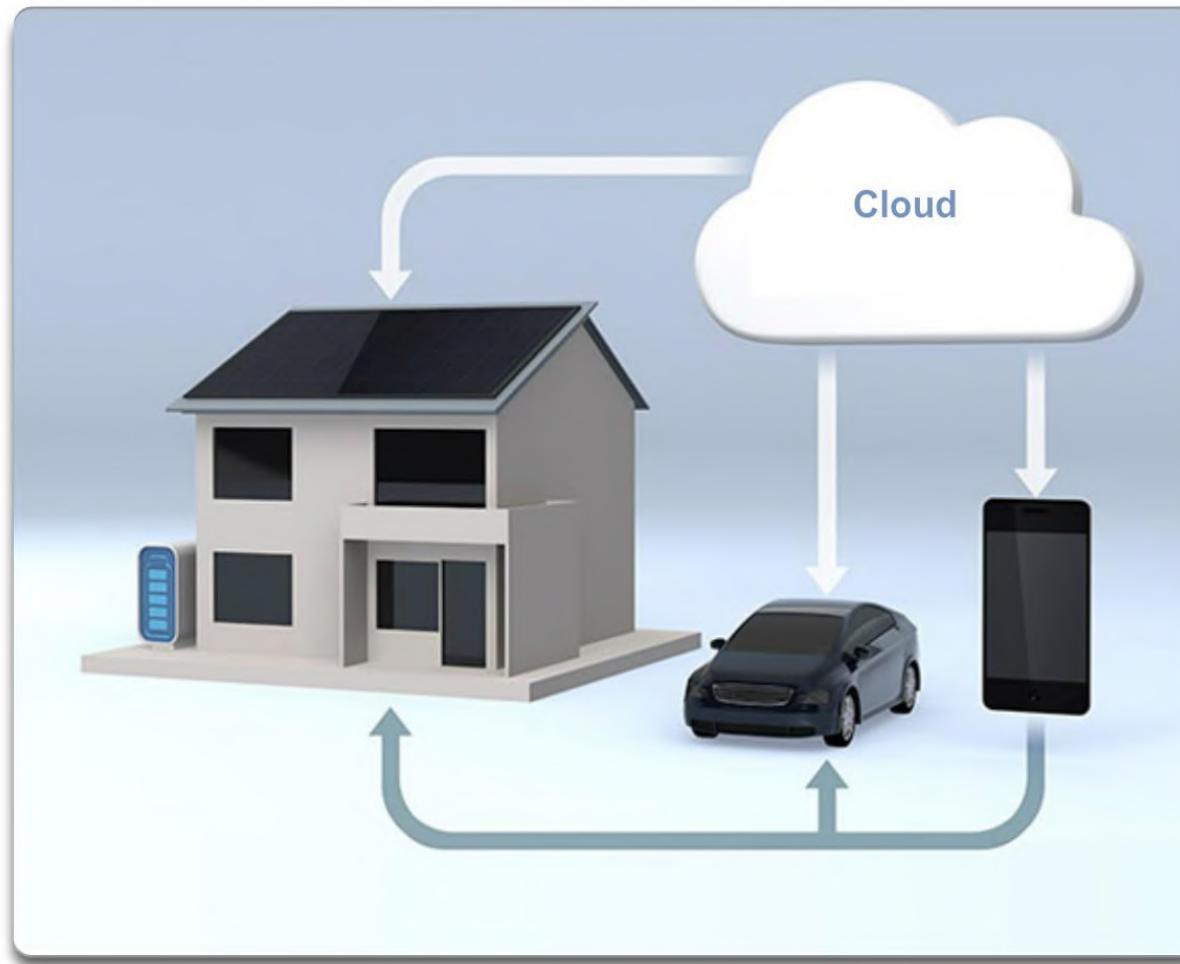
- Redundant data communications connections
- High-speed virtual servers (sometimes referred to as server farms or server clusters)
- Redundant storage systems (typically uses SAN technology)
- Redundant or backup power supplies
- Environmental controls (e.g., air conditioning, fire suppression)
- Security devices



# Networking Technologies for the Home

# Technology Trends in the Home

## Smart Home Technology



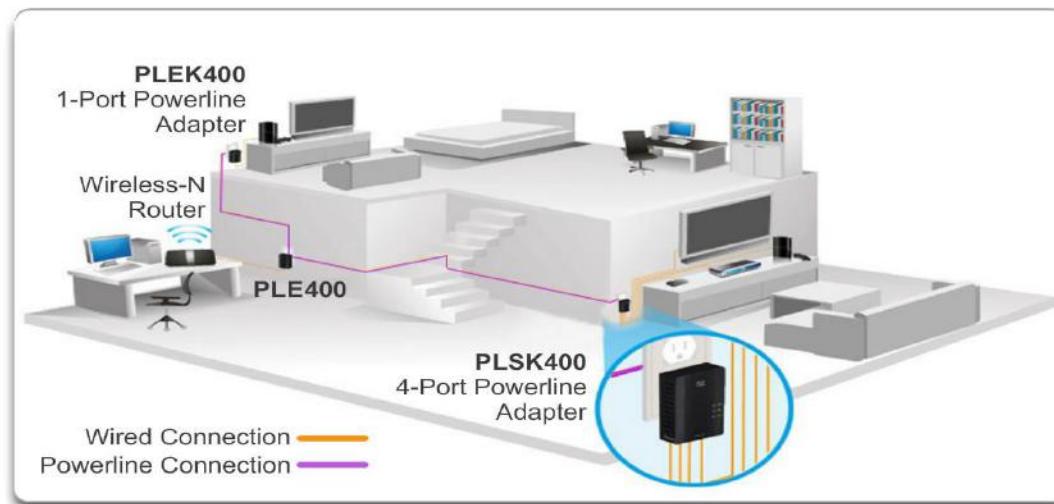


# Networking Technologies for the Home

## Powerline Networking

Powerline networking is an emerging trend for home networking that uses existing electrical wiring to connect devices, as shown in the figure. The concept of “no new wires” means the ability to connect a device to the network wherever there is an electrical outlet. This saves the cost of installing data cables and without any additional cost to the electrical bill. Using the same wiring that delivers electricity, powerline networking sends information by sending data on certain frequencies.

**Powerline Networking**

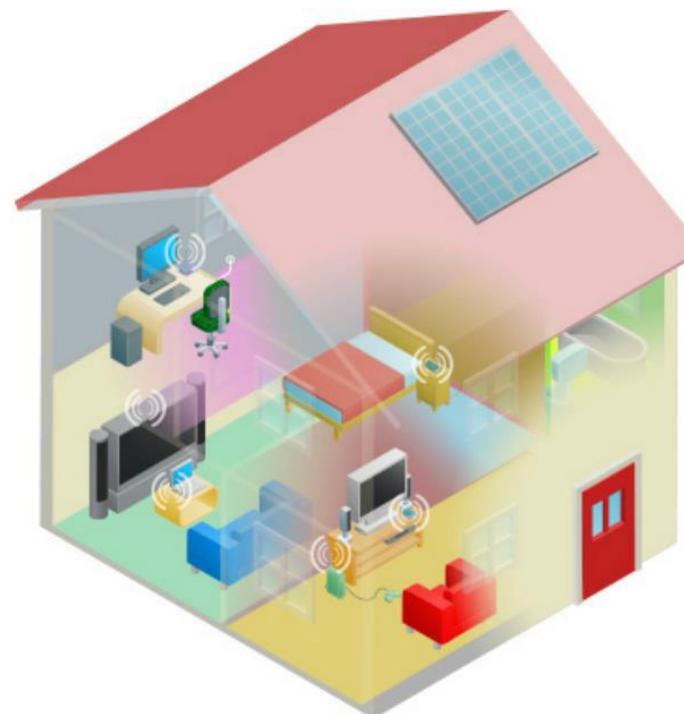




# Networking Technologies for the Home

## Wireless Broadband

### Wireless Broadband Service

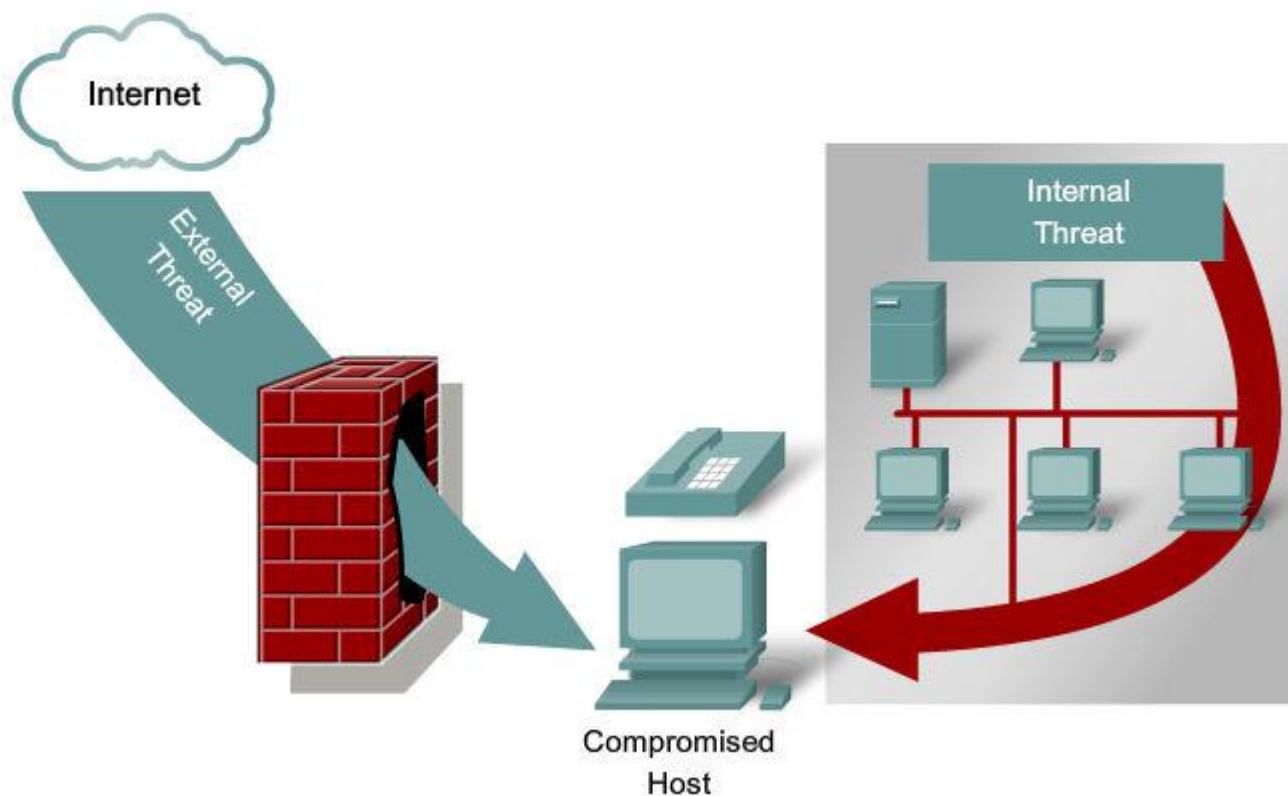




# Future of Networking

# Network Security

## Threats to Networks





# Network Security

# Security Threats

The most common external threats to networks include:

- Viruses, worms, and Trojan horses
- Spyware and adware
- Zero-day attacks, also called zero-hour attacks
- Hacker attacks
- Denial of service (DoS) attacks
- Data interception and theft
- Identity theft



# Network Security Security Solutions

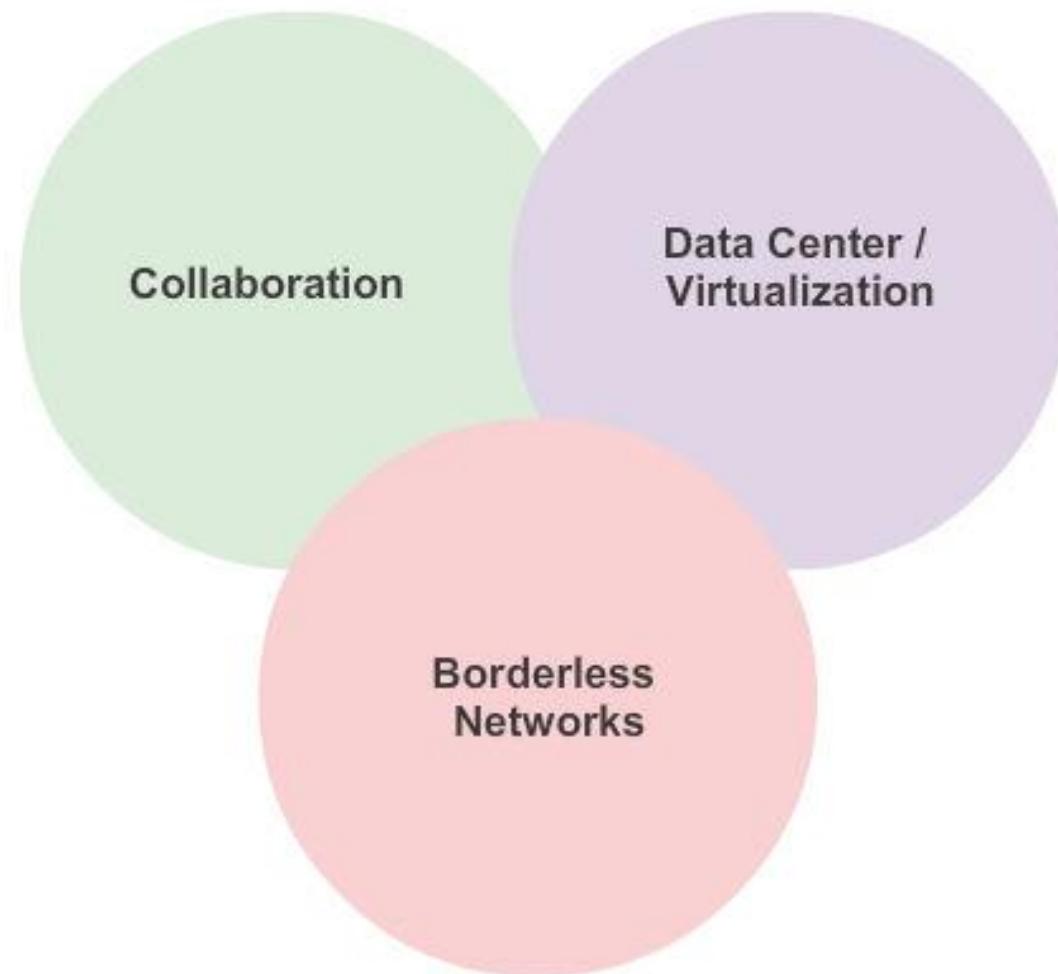
Network security components often include:

- Antivirus and antispyware
- Firewall filtering
- Dedicated firewall systems
- Access control lists (ACL)
- Intrusion prevention systems (IPS)
- Virtual Private Networks (VPNs)



Network Architectures

# Cisco Network Architectures





Network Architectures

# Cisco Certified Network Associate (CCNA)





# Exploring the Networking Summary

In this chapter, you learned:

- Networks and the Internet have changed the way we communicate, learn, work, and even play.
- Networks come in all sizes. They can range from simple networks consisting of two computers, to networks connecting millions of devices.
- The Internet is the largest network in existence. In fact, the term Internet means a ‘network of networks’. The Internet provides the services that enable us to connect and communicate with our families, friends, work, and interests.
- The network infrastructure is the platform that supports the network. It provides the stable and reliable channel over which communication can occur. It is made up of network components including end devices, intermediate devices, and network media.



# Exploring the Networking Summary (cont.)

In this chapter, you learned:

- Networks must be reliable.
- Network security is an integral part of computer networking, regardless of whether the network is limited to a home environment with a single connection to the Internet, or as large as a corporation with thousands of users.
- The network infrastructure can vary greatly in terms of size, number of users, and number and types of services that are supported on it. The network infrastructure must grow and adjust to support the way the network is used. The routing and switching platform is the foundation of any network infrastructure.

# Cisco | Networking Academy®

Mind Wide Open™



Servers are computers with software that enable them to provide information, like email or web pages, to other end devices on the network. For example, a server requires web server software in order to provide web services to the network.

Clients are computers with software installed that enable them to request and display the information obtained from the server. An example of client software is a web browser, like Chrome or FireFox

Peer-to-Peer:

Client and server software usually runs on separate computers, but it is also possible for one computer to carry out both roles at the same time.



Intermediary devices connect the individual end devices to the network and can connect multiple individual networks to form an internetwork. These intermediary devices provide connectivity and ensure that data flows across the network.



## Chapter 2: Configuring a Network Operating System



## Introduction to Networks

Cisco | Networking Academy®  
Mind Wide Open™



# Chapter 2 - Objectives

Upon completion of this chapter you will be able to:

- Explain the purpose of the Cisco IOS.
- Explain how to access and navigate Cisco IOS to configure network devices.
- Describe the command structure of the Cisco IOS software.
- Configure hostnames on a Cisco IOS device using the CLI.
- Use Cisco IOS commands to limit access to device configurations.
- Use Cisco IOS commands to save the running configuration.
- Explain how devices communicate across network media.
- Configure a host device with an IP address.
- Verify connectivity between two end devices.



# Chapter 2

- 2.0 Introduction
- 2.1 IOS Bootcamp
- 2.2 Getting Basic
- 2.3 Addressing Schemes
- 2.4 Summary



## 2.1 IOS Bootcamp

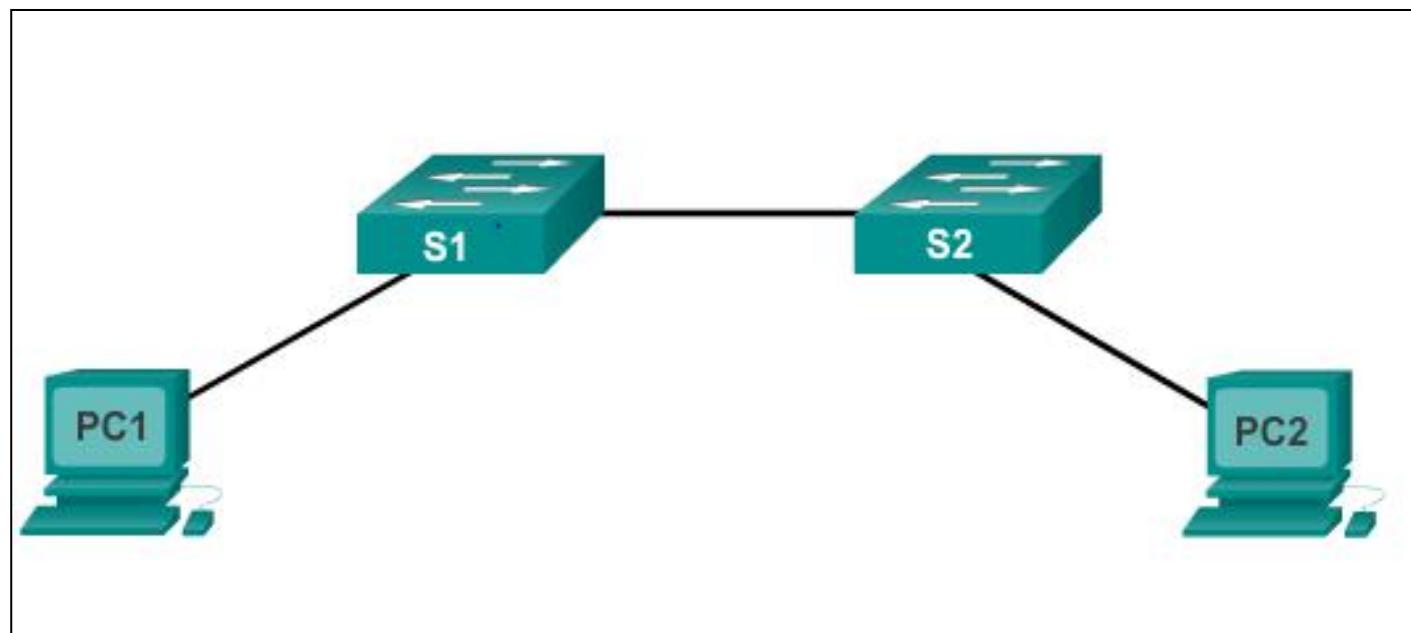


Cisco | Networking Academy®  
Mind Wide Open™



# Cisco IOS Operating Systems

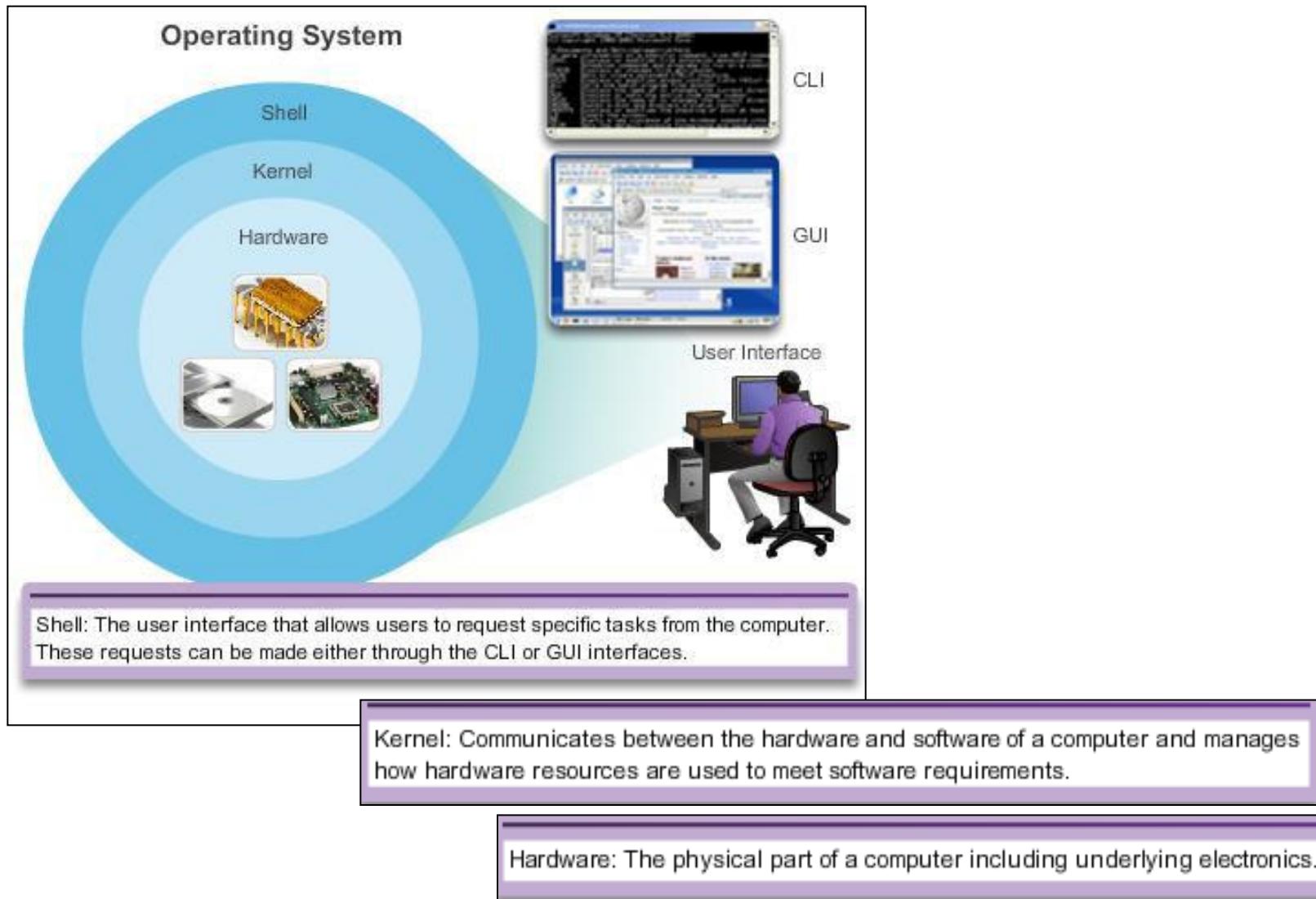
- All networking equipment dependent on operating systems
- The operating system on home routers is usually called firmware
- Cisco IOS – Collection of network operating systems used on Cisco devices





## Cisco IOS

# Operating Systems (cont.)





## Cisco IOS

# Purpose of OS

- PC operating systems (Windows 8 and OS X) perform technical functions that enable:
  - Use of a mouse
  - View output
  - Enter text
- Switch or router IOS provides options to:
  - Configure interfaces
  - Enable routing and switching functions
- All networking devices come with a default IOS
- Possible to upgrade the IOS version or feature set
- In this course, primary focus is Cisco IOS Release 15.x



## Cisco IOS

# Location of the Cisco IOS

### Cisco IOS stored in **Flash**

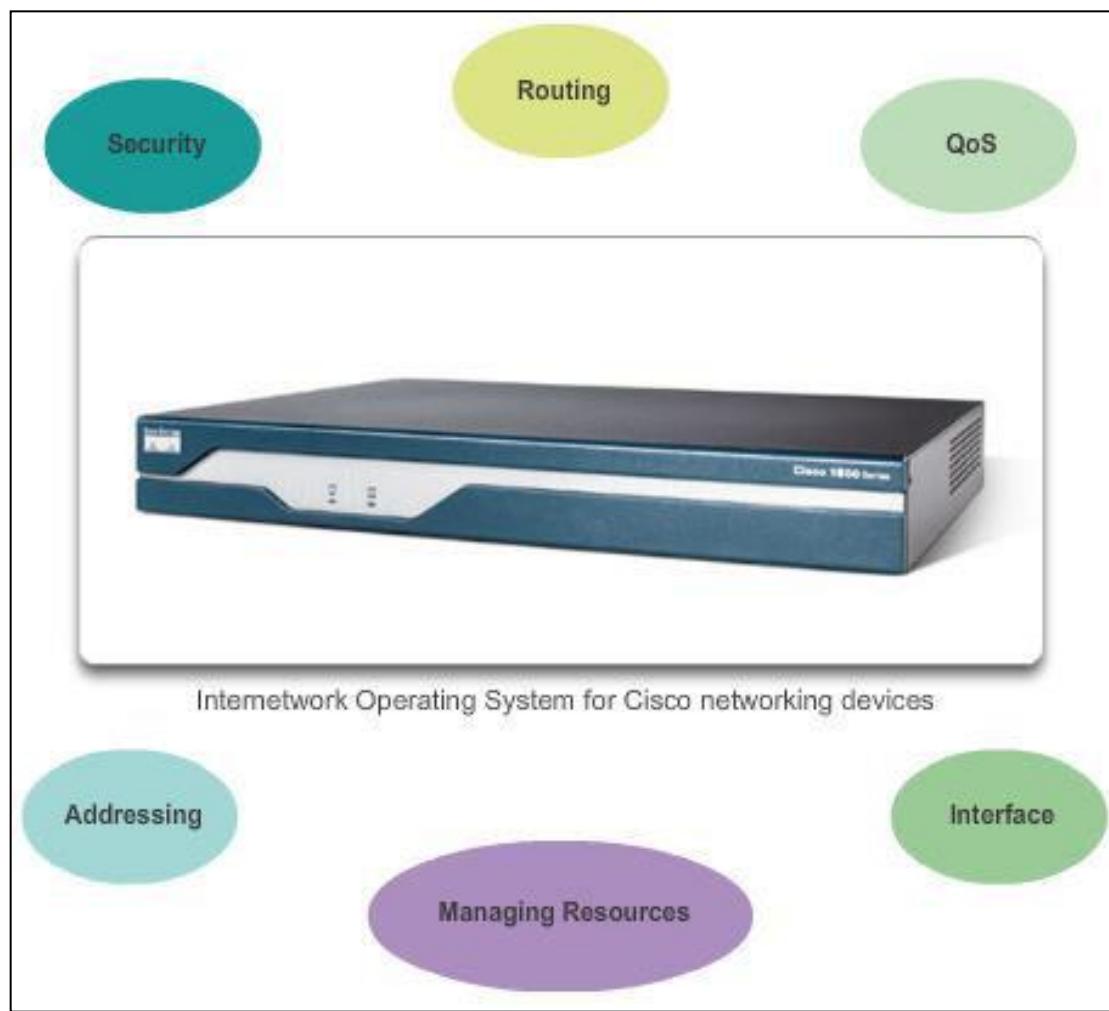
- Non-volatile storage, not lost when power is lost
- Can be changed or overwritten as needed
- Can be used to store multiple versions of IOS
- IOS copied from flash to volatile RAM
- Quantity of flash and RAM memory determines IOS that can be used





# Cisco IOS IOS Functions

These are the major functions performed or enabled by Cisco routers and switches.





# Accessing a Cisco IOS Device

## Console Access Method

Most common methods to access the CLI:

- Console
- Telnet or SSH
- AUX port



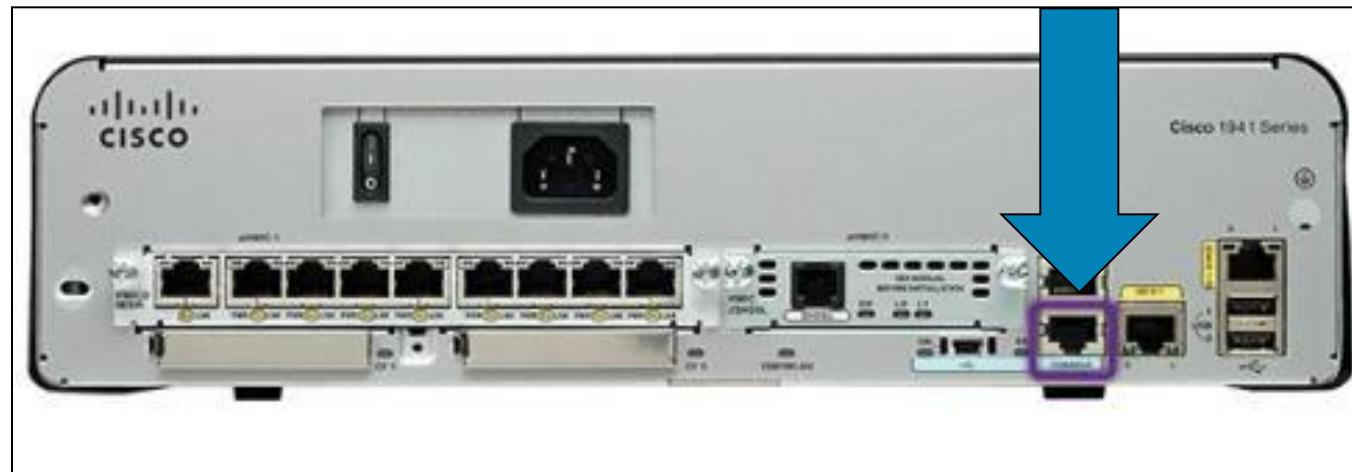


# Accessing a Cisco IOS Device

## Console Access Method

### Console Port

- Device is accessible even if no networking services have been configured (out-of-band)
- Need a special console 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 cannot be easily accessed





## Accessing a Cisco IOS Device

# Telnet, SSH, and AUX Access Methods

### Telnet

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

### Secure Shell (SSH)

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

### Aux Port

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

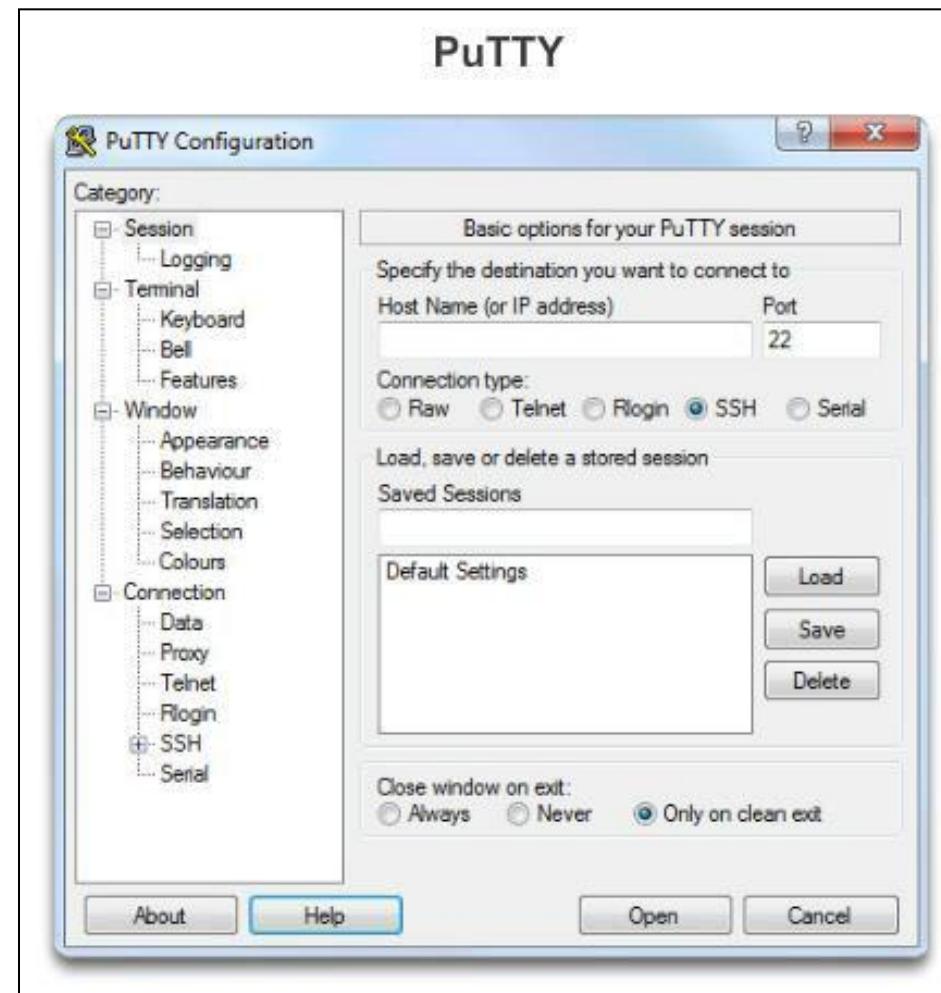




# Accessing a Cisco IOS Device Terminal Emulation Programs

Software available for connecting to a networking device:

- PuTTY
- Tera Term
- SecureCRT
- HyperTerminal
- OS X Terminal





# Navigating the IOS Cisco IOS Modes of Operation

## IOS Mode Hierarchical Structure

```
User EXEC Command-Router>
ping
show (limited)
enable
etc.
```

```
Privileged EXEC Commands-Router#
all User EXEC commands
debug commands
reload
configure
etc.
```

```
Global Configuration Commands-Router (config)#
hostname
enable secret
ip route
```

```
interface ethernet
    serial
    dsl
    etc.
```

```
Interface Commands-Router (config-if)#
    ip address
    ipv6 address
    encapsulation
    shutdown/no shutdown
    etc.
```

```
router      rip
            ospf
            eigrp
            etc.
```

```
Routing Engine Commands-Router (config-router)#
    network
    version
    auto summary
    etc.
```

```
line        vty
            console
            etc.
```

```
Line Commands-Router (config-line)#
    password
    login
    modem commands
    etc.
```



# Navigating the IOS 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.

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

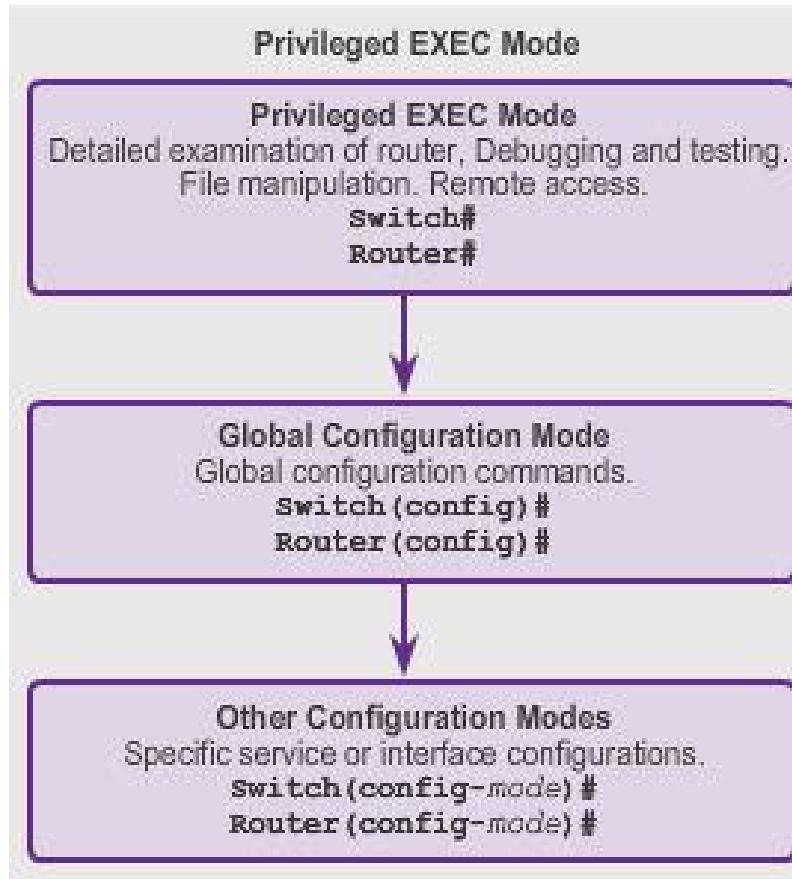
## Privileged EXEC Mode

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

```
switch#  
Router#
```



# Navigating the IOS 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 the IOS

# Navigating Between IOS Modes

```
Router con0 is now available.
```

```
Press RETURN to get started.
```

```
User Access Verification
```

```
Password:
```

```
Router>enable
```

```
Password:
```

```
Router#disable
```

```
Router>exit
```

User EXEC Mode Prompt

Privileged EXEC Mode Prompt

User EXEC Mode Prompt

Router



## Navigating the IOS

# Navigating Between IOS Modes (cont.)

```
Switch> enable
Switch# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.

Switch(config)# interface vlan 1
Switch(config-if)# exit
Switch(config)# exit
Switch#
```

```
Switch# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.

Switch(config)# vlan 1
Switch(config-vlan)# end
Switch#
```

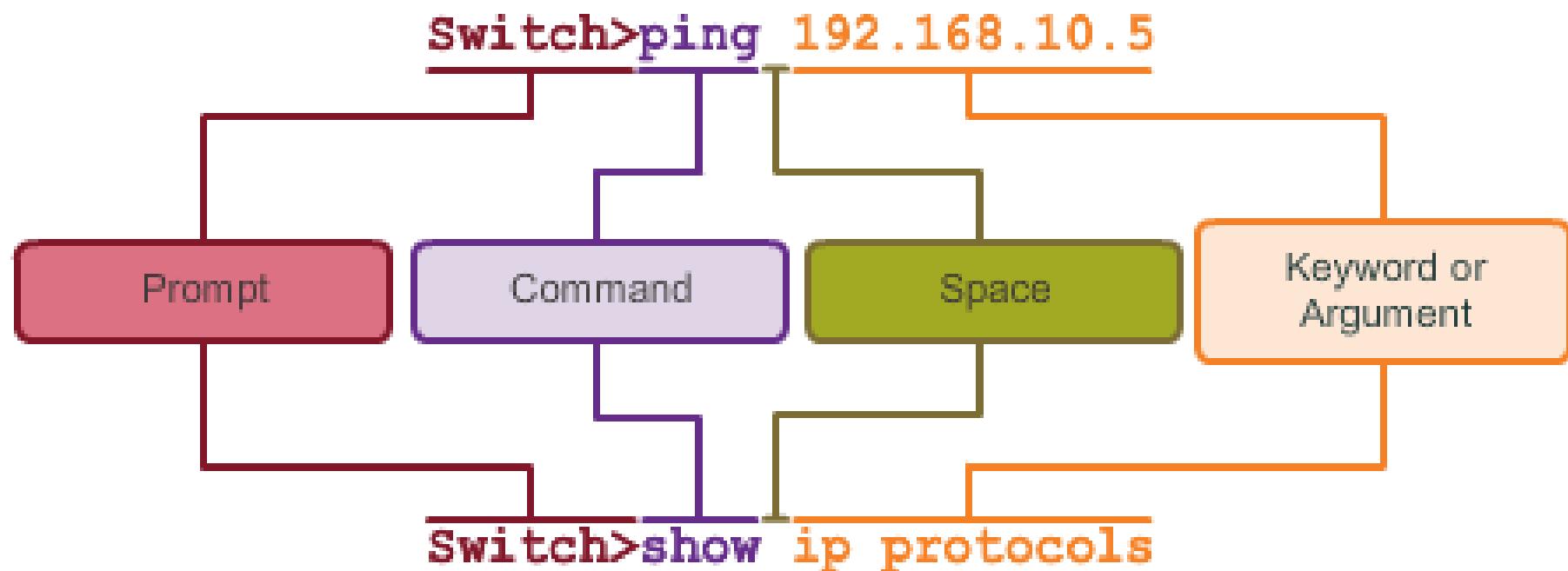
```
Switch# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.

Switch(config)# line vty 0 4
Switch(config-line)# interface fastethernet 0/1
Switch(config-if)# end
Switch#
```



## The Command Structure

# IOS Command Structure





## The Command Structure

# Cisco IOS Command Reference

To navigate to Cisco's *IOS Command Reference* to find a command:

1. Go to <http://www.cisco.com>.
2. Click **Support**.
3. Click **Networking Software (IOS & NX-OS)**.
4. Click **15.2M&T** (for example).
5. Click **Reference Guides**.
6. Click **Command References**.
7. Click the particular technology that encompasses the command you reference.
8. Click the link on the left that alphabetically matches the command you referencing.
9. Click the link for the command.



# The Command Structure

# Context-Sensitive Help

## Context Sensitive Help

```
Switch#cl?  
clear clock
```

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

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

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

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

Command explanation with more than one argument or variable option

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



## The Command Structure

# 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.



## The Command Structure

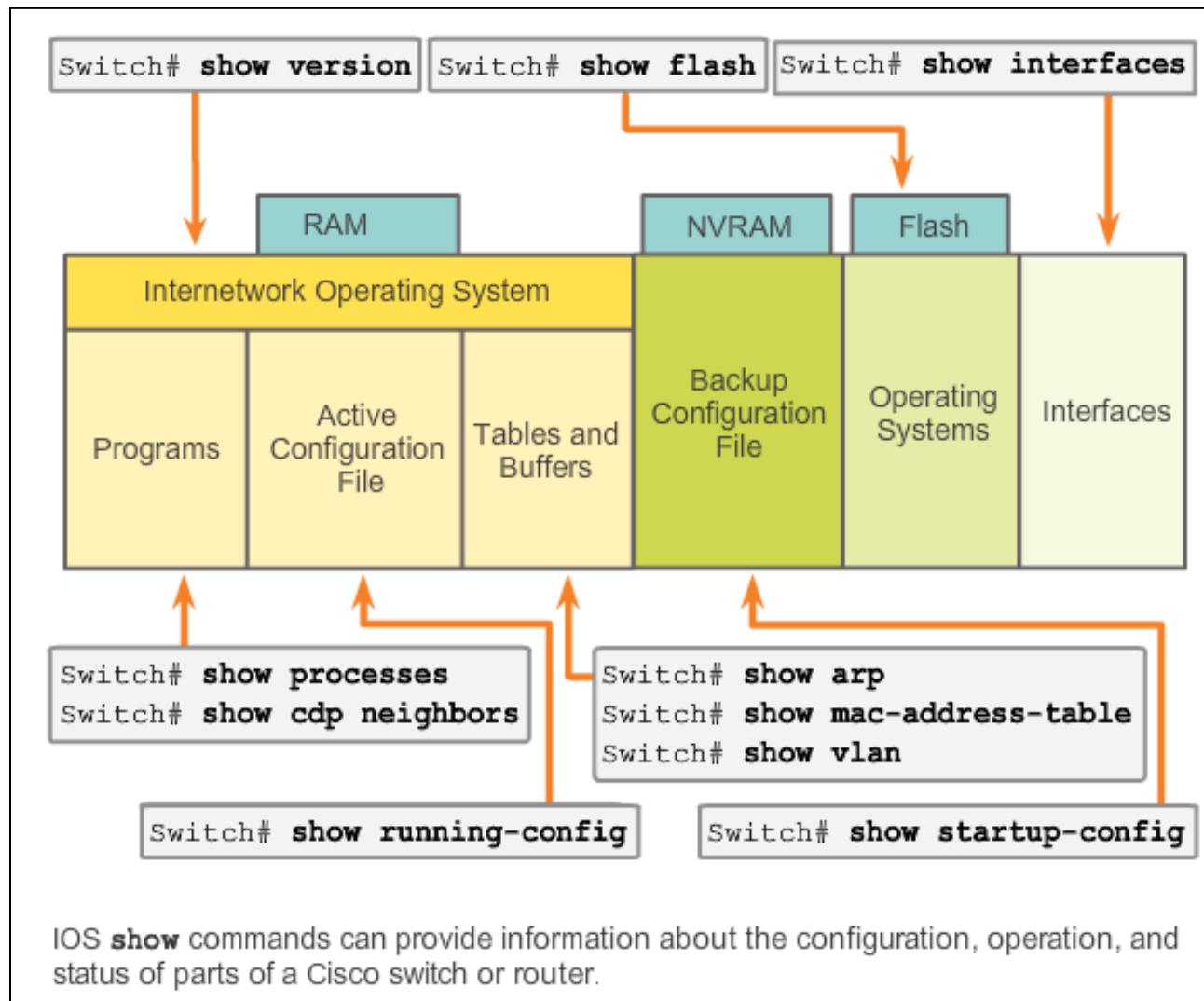
# Hot Keys and Shortcuts

- **Tab** – Completes the remainder of a partially typed command or keyword.
- **Ctrl-R** – Redisplays a line.
- **Ctrl-A** – Moves to the beginning of the line.
- **Ctrl-Z** – Exits the 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** – Exits the current configuration or aborts the current command.



# The Command Structure

## IOS Examination Commands





## The Command Structure

# 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
```

## 2.2 Getting Basic



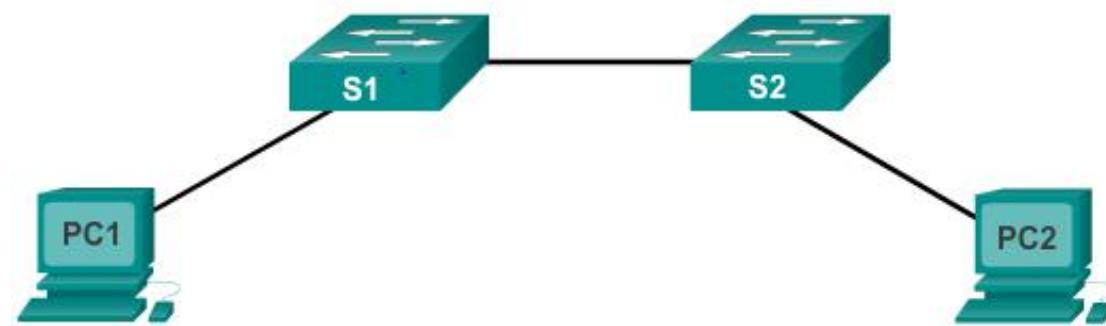


## Hostnames

# Why the Switch

Let's focus on:

- Creating a two PC network connected via a switch
- Setting a name for the switch
- Limiting access to the device configuration
- Configuring banner messages
- Saving the configuration



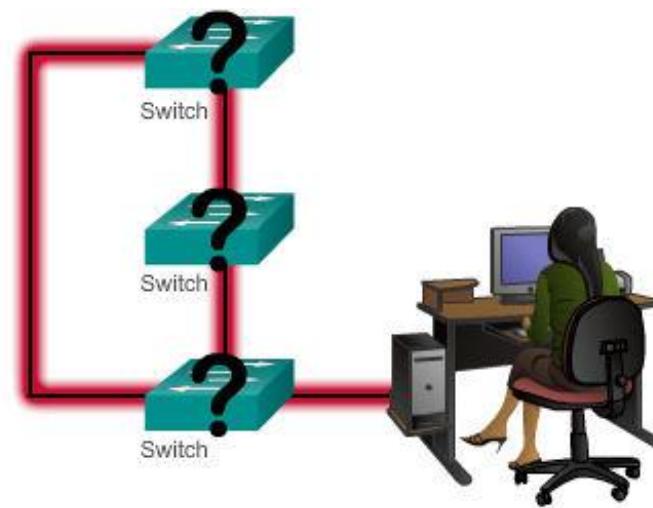


## Hostnames Device Names

Some guidelines for naming conventions:

- Start with a letter
- Contains no spaces
- Ends with a letter or digit
- Uses only letters, digits, and dashes
- Be less than 64 characters in length

Without names, network devices are difficult to identify for configuration purposes.

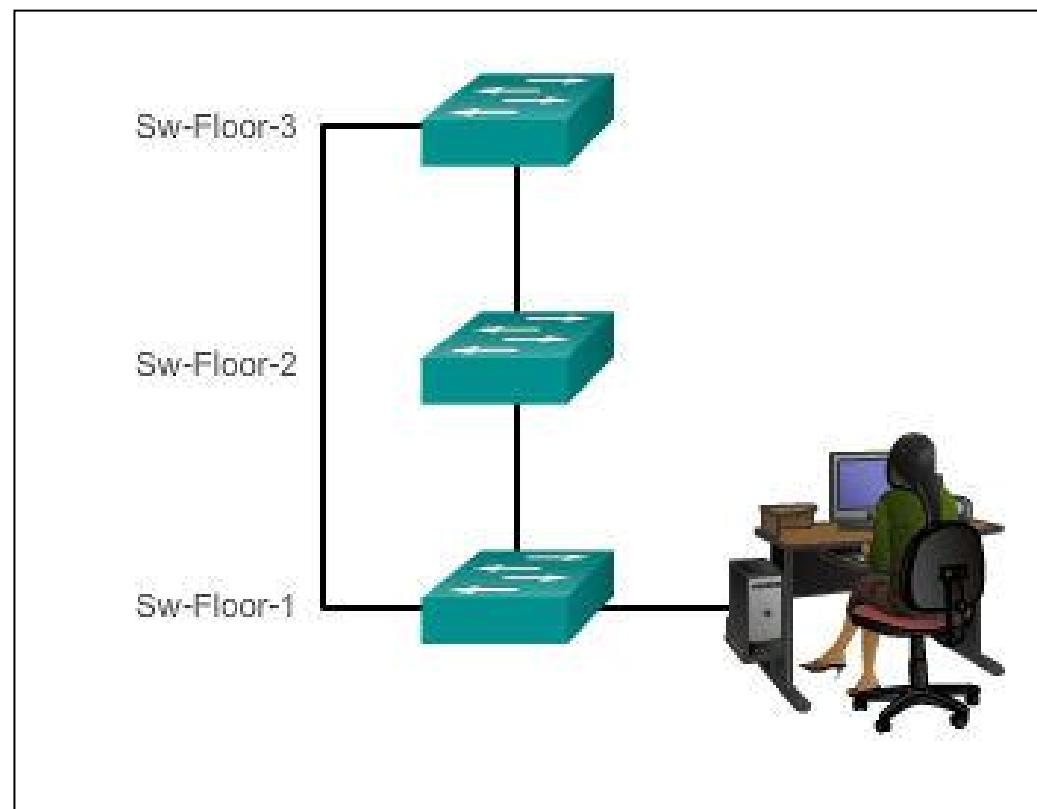




## Hostnames

# Configuring Device Names

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





## Hostnames

# Configuring Hostnames

### Configure a Hostname

**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

These are device access passwords:

- **enable password** – Limits access to the privileged EXEC mode
- **enable secret** – Encrypted, limits access to the privileged EXEC mode
- **console password** – Limits device access using the console connection
- **VTY password** – Limits device access over Telnet

**Note:** In most of the labs in this course, we will be using simple passwords such as **cisco** or **class**.



## Limiting Access to Device Configurations

# Securing Privileged EXEC Access Mode

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

```
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#
```



# Limiting Access to Device Configurations

## 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; it 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. The number of VTY lines supported varies with the type of device and the IOS version.



# Limiting Access to Device Configurations

## Encrypting Password Display

### Configuring Password Encryption

```
Enter the command to encrypt the plain text passwords.
```

```
Switch(config)# service password-encryption
```

```
Exit global configuration mode and view the running configuration.
```

```
Switch(config)# exit
```

```
Switch# show running-config
```

```
!
```

```
<output omitted>
```

```
!
```

```
line con 0
```

```
password 7 094F471A1A0A
```

```
login
```

```
!
```

```
line vty 0 4
```

```
password 7 03095A0F034F38435B49150A1819
```

```
login
```

```
!
```

```
!
```

```
end
```

### service password-encryption

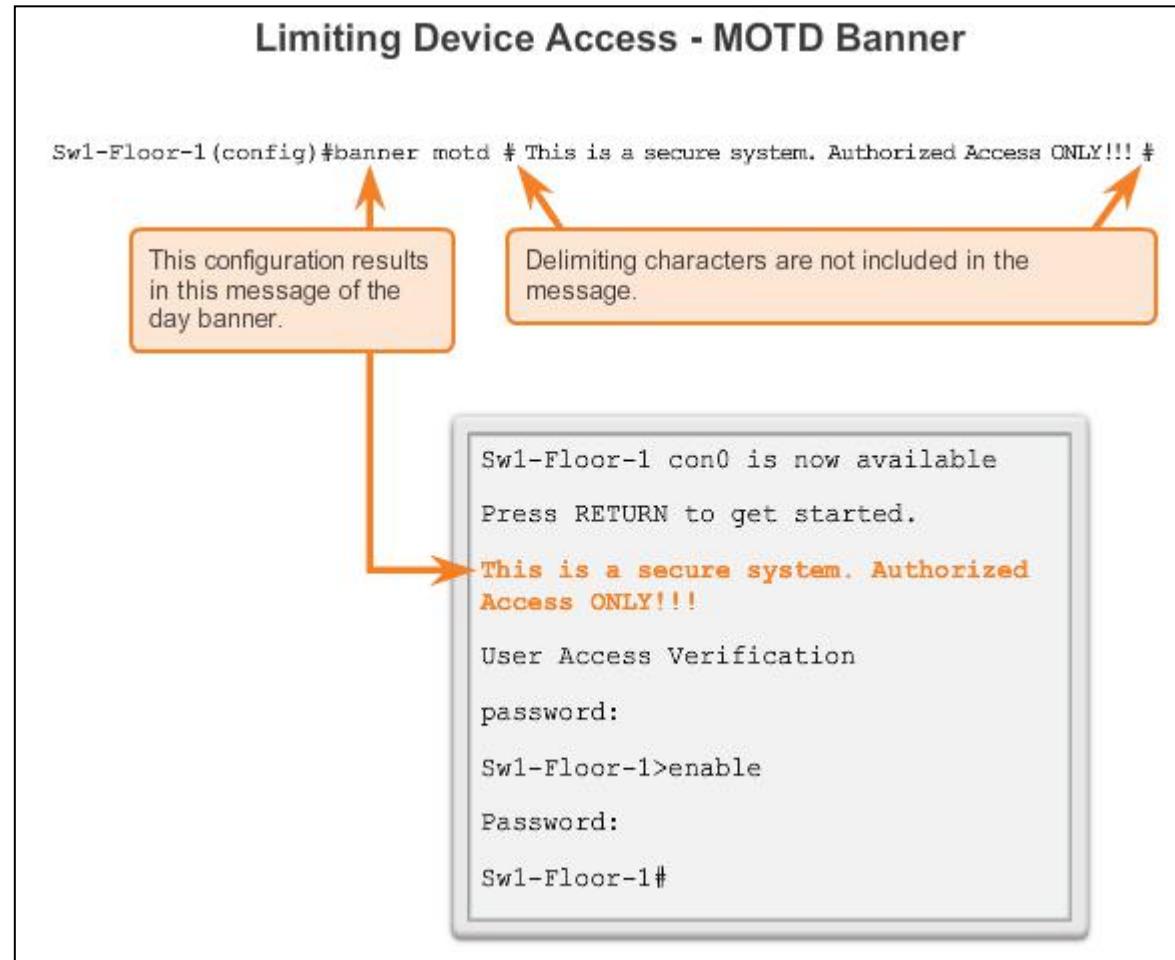
- Prevents passwords from showing up as plain text when viewing the configuration
- Keeps unauthorized individuals from viewing passwords in the configuration file
- Once applied, removing the encryption service does not reverse the encryption



# LIMITING ACCESS TO DEVICE CONFIGURATIONS

## BANNER MESSAGES

- Important part of the legal process in the event that someone is prosecuted for breaking into a device
- Wording that implies that a login is "welcome" or "invited" is not appropriate
- Often used for legal notification because it is displayed to all connected terminals





# Saving Configurations Configuration Files

## Saving and Erasing the Configuration

```
Switch#show running-config
```

Lists the complete configuration currently active in RAM.

```
Switch#show running-config
Building configuration...
Current configuration : 2904 bytes
!
! Last configuration change at 00:02:32
UTC Mon Mar 1 1993
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
<output omitted>
!
```

The active configuration can be copied to NVRAM.

```
Switch#copy running-config startup-config
```

- Switch# **reload**

System configuration has been modified. Save?

[yes/no]: **n**

Proceed with reload?  
[confirm]

- Startup configuration is removed by using the **erase startup-config**

```
Switch# erase startup-config
```

- On a switch, you must also issue the **delete vlan.dat**

```
Switch# delete
    vlan.dat
```

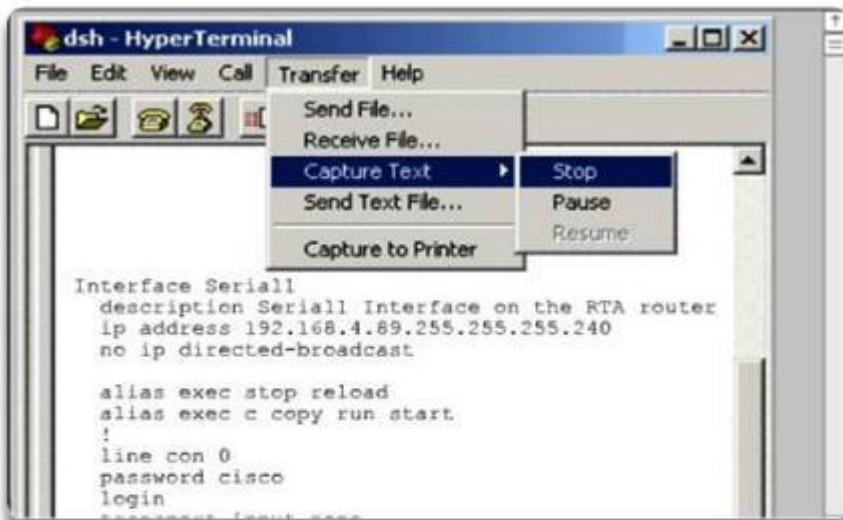
Delete filename  
[vlan.dat]?

Delete flash:vlan.dat?  
[confirm]



# Saving Configurations Capturing Text

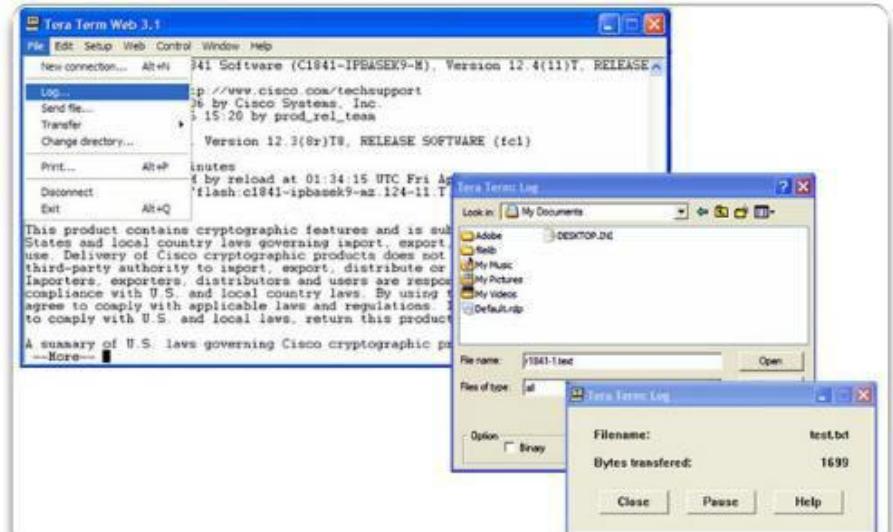
## Saving to a Text File in HyperTerminal



### In the terminal session:

1. Start the text capture process
2. Issue a **show running-config** command
3. Stop the capture process
4. Save the text file

## Saving to a Text File in Tera Term



### In the terminal session:

1. Start the log process
2. Issue a **show running-config** command
3. Close the log

## 2.3 Addressing Schemes

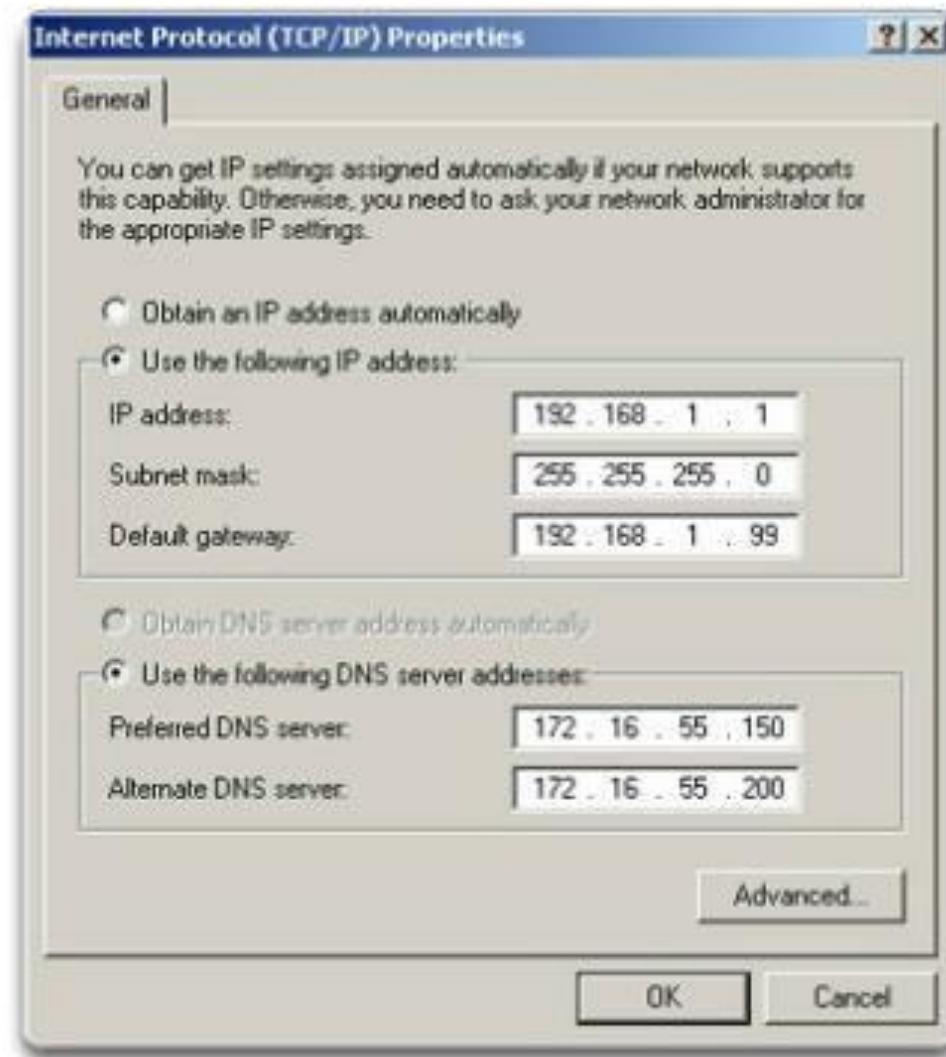




## Ports and Addresses

# IP Addressing of Devices

- Each end device on a network must be configured with an IP address.
- Structure of an IPv4 address is called *dotted decimal*.
- IP address displayed in decimal notation, with four decimal numbers between 0 and 255.
- With the IP address, a subnet mask is also necessary.
- IP addresses can be assigned to both physical ports and virtual interfaces.





## Ports and Addresses

# Interfaces and Ports

- Network communications depend on end user device interfaces, networking device interfaces, and the cables that connect them.
- Types of network media include twisted-pair copper cables, fiber-optic cables, coaxial cables, or wireless.
- Different types of network media have different features and benefits.
- Ethernet is the most common local area network (LAN) technology.
- Ethernet ports are found on end user devices, switch devices, and other networking devices.
- Cisco IOS switches have physical ports for devices to connect to, but also have one or more switch virtual interfaces (SVIs; no physical hardware on the device associated with it; created in software).
- SVI provides a means to remotely manage a switch over a network.





## Addressing Devices

# Configuring a Switch Virtual Interface

- **IP address** – Together with subnet mask, uniquely identifies end device on internetwork.
- **Subnet mask** – Determines which part of a larger network is used by an IP address.
- **interface VLAN 1** – Available in interface configuration mode,
- **ip address 192.168.10.2 255.255.255.0** – Configures the IP address and subnet mask for the switch.
- **no shutdown** – Administratively enables the interface.
- Switch still needs to have physical ports configured and VTY lines to enable remote management.



## Addressing Devices

# Configuring a Switch Virtual Interface

Enter interface configuration mode for VLAN 1.

```
Switch(config)# interface vlan 1
```

Configure the IP address as '192.168.10.2' and the subnet mask as '255.255.255.0'.

```
Switch(config-if)# ip address 192.168.10.2 255.255.255.0
```

Activate the interface.

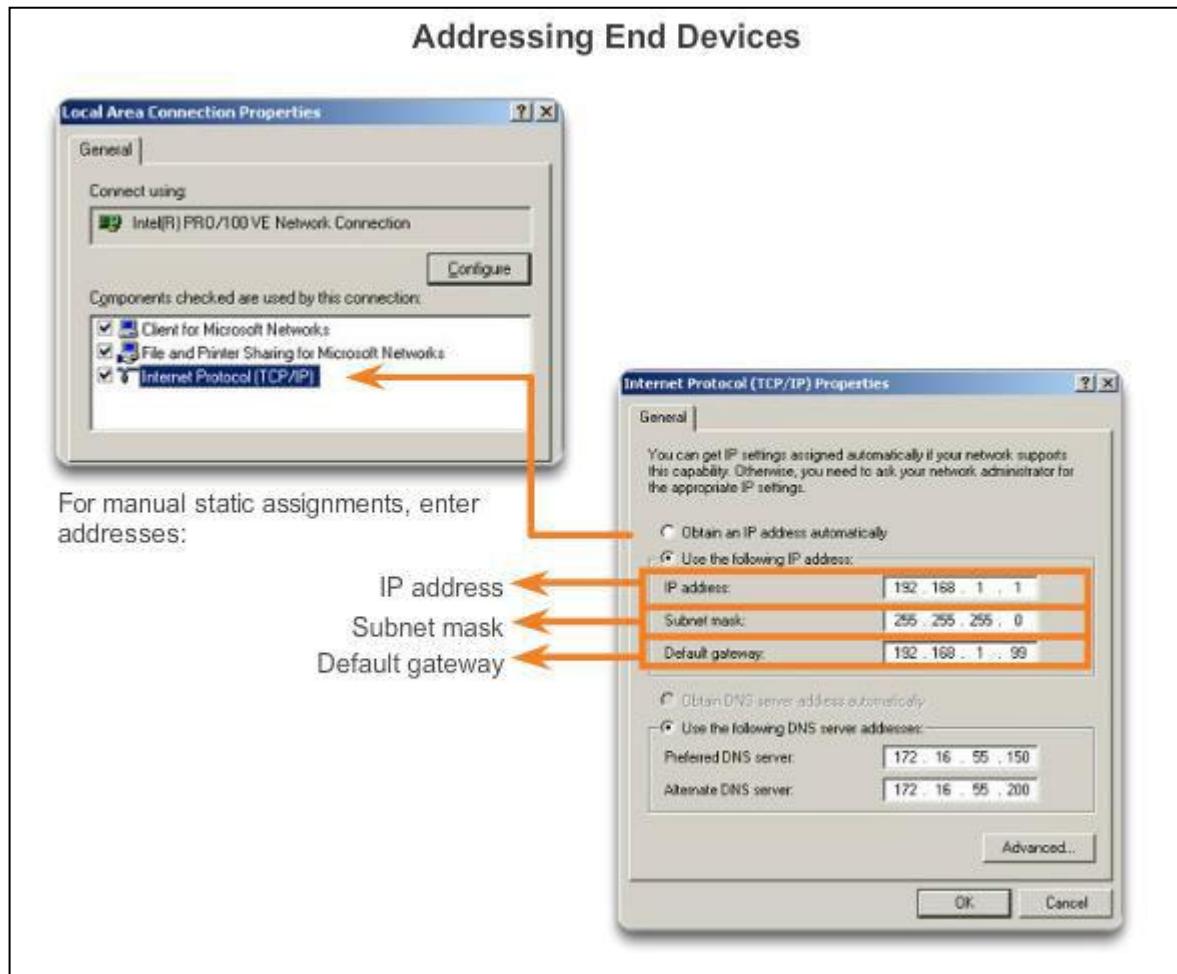
```
Switch(config-if)# no shutdown
```

```
%LINK-5-CHANGED: Interface Vlan1, changed state to up
```



# Addressing Devices

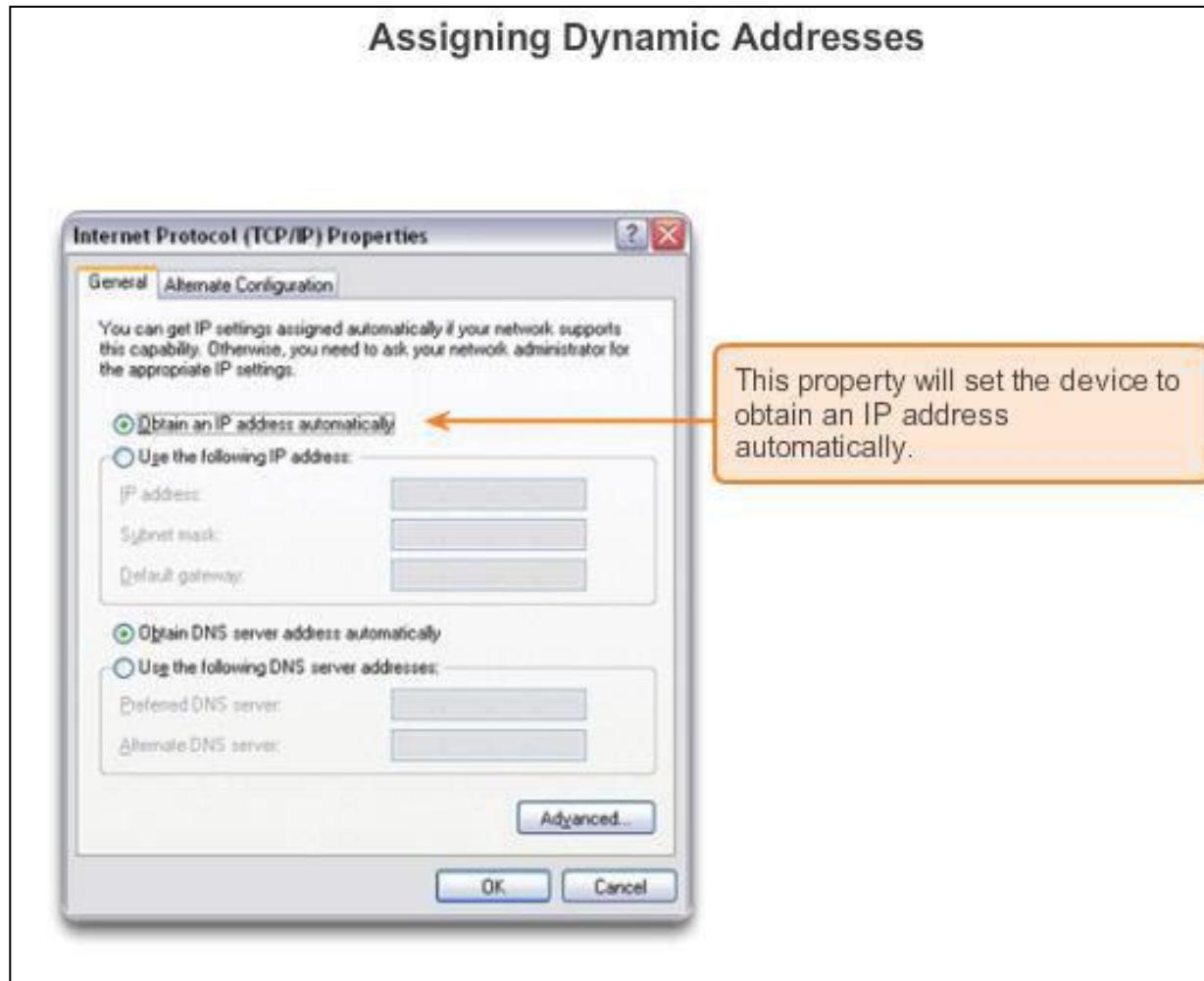
## Manual IP Address Configuration for End Devices





# Addressing Devices

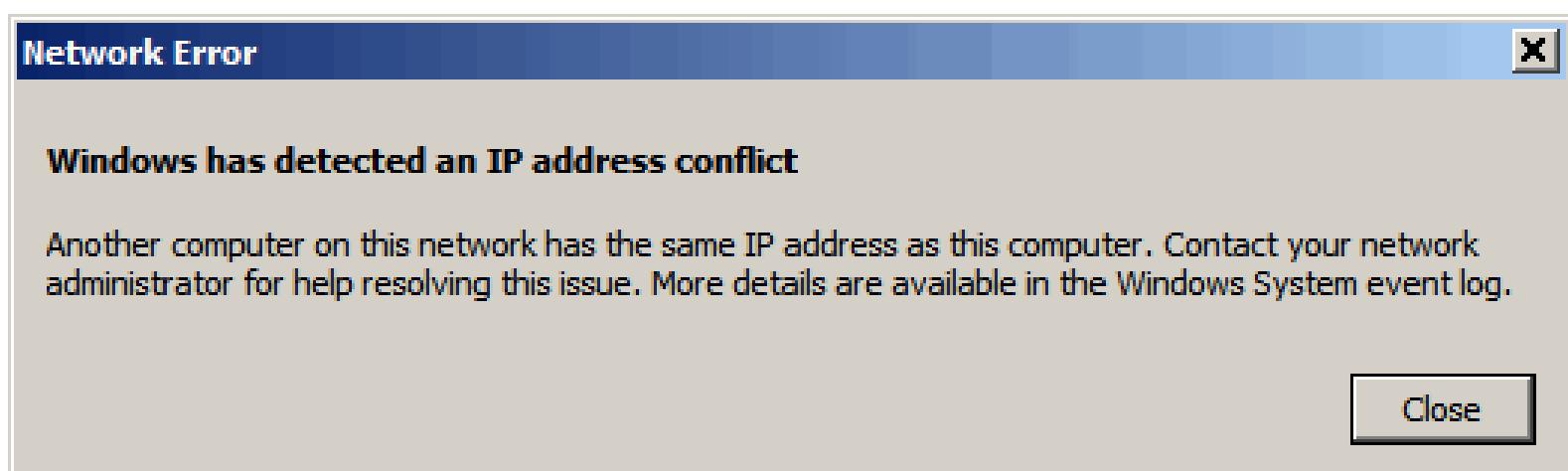
## Automatic IP Address Configuration for End Devices





# Addressing Devices

## IP Address Conflicts





## Verifying Connectivity

# Test the Loopback Address on an End Device

**Testing Local TCP/IP Stack**



Pinging the local host confirms that TCP/IP is installed and working on the local network adapter.



This connection uses the following items:

- QoS Packet Scheduler
- Network Monitor Driver
- Internet Protocol (TCP/IP)

Description: Allows your computer to access resources on a Microsoft network.

Show icon in notification area when connected  
Notify me when this connection has limited or no connectivity

OK Cancel

Pinging **127.0.0.1** causes a device to ping itself.



## Verifying Connectivity

# Testing the Interface Assignment

### Verifying the VLAN Interface Assignment

Enter the command to verify the interface configuration on S1.

```
S1# show ip interface brief
Interface          IP-Address      OK? Method Status   Protocol
FastEthernet0/1    unassigned      YES  manual  up       up
FastEthernet0/2    unassigned      YES  manual  up       up
<output omitted>
Vlan1             192.168.10.2   YES  manual  up       up
```

You are now on S2. Enter the command to verify the interface configuration on S2.

```
S2# show ip interface brief
Interface          IP-Address      OK? Method Status   Protocol
FastEthernet0/1    unassigned      YES  manual  up       up
FastEthernet0/2    unassigned      YES  manual  up       up
<output omitted>
Vlan1             192.168.10.3   YES  manual  up       up
```

You successfully verified the interface assignment on S1 and S2.



## Verifying Connectivity

# Testing End-to-End Connectivity

```
Enter the command to verify connectivity to PC2 at '192.168.10.11'.  
C:\> ping 192.168.10.11  
  
Pinging 192.168.10.11 with 32 bytes of data:  
Reply from 192.168.10.11: bytes=32 time=838ms TTL=35  
Reply from 192.168.10.11: bytes=32 time=820ms TTL=35  
Reply from 192.168.10.11: bytes=32 time=883ms TTL=36  
Reply from 192.168.10.11: bytes=32 time=828ms TTL=36  
  
Ping statistics for 192.168.10.11:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 820ms, Maximum = 883ms, Average = 842ms  
  
C:\>  
You successfully verified connectivity to S1 and PC2.
```



# Configuring a Network Operating System

## Chapter 2 Summary

Cisco IOS:

- The technician can enter commands to configure, or program, the device to perform various networking functions.
- Services are generally accessed using a command-line interface (CLI), which is accessed by either the console port, the AUX port, or through telnet or SSH.
- Once connected to the CLI, network technicians can make configuration changes to Cisco IOS devices.
- Cisco IOS is designed as a modal operating system, which means a network technician must navigate through various hierarchical modes of the IOS.
- Cisco IOS routers and switches support a similar modal operating system, support similar command structures, and support many of the same commands. In addition, both devices have identical initial configuration steps when implementing them in a network.



# Configuring a Network Operating System

## Chapter 2 Summary (cont.)

```
User EXEC Command-Router>
ping
show (limited)
enable
etc.
```



# Configuring a Network Operating System

## Chapter 2 Summary (cont.)

### Privileged EXEC Commands-Router#

all User EXEC commands  
debug commands  
reload  
configure  
etc.

### Global Configuration Commands-Router(config) #

hostname  
enable secret  
ip route

interface ethernet  
serial  
dsl  
etc.

### Interface Commands-Router(config-if) #

ip address  
ipv6 address  
encapsulation  
shutdown/ no shutdown  
etc.

router rip  
ospf  
eigrp  
etc.

### Routing Engine Commands-Router(config-router) #

network  
version  
auto summary  
etc.

line vty  
console  
etc.

### Line Commands-Router(config-line) #

password  
login  
modem commands  
etc.

# Cisco | Networking Academy®

Mind Wide Open™



## Chapter 3: Network Protocols and Communications



## Introduction to Networks

Cisco | Networking Academy®  
Mind Wide Open™



# Chapter 3: Objectives

After completing this chapter, you will be able to:

- Explain how rules are used to facilitate communication.
- Explain the role of protocols and standards organizations in facilitating interoperability in network communications.
- Explain how devices on a LAN access resources in a small to medium-sized business network.



# Chapter 3

- 3.1 Rules of Communication
- 3.2 Network Protocols and Standards
- 3.3 Moving Data in the Network
- 3.4 Summary

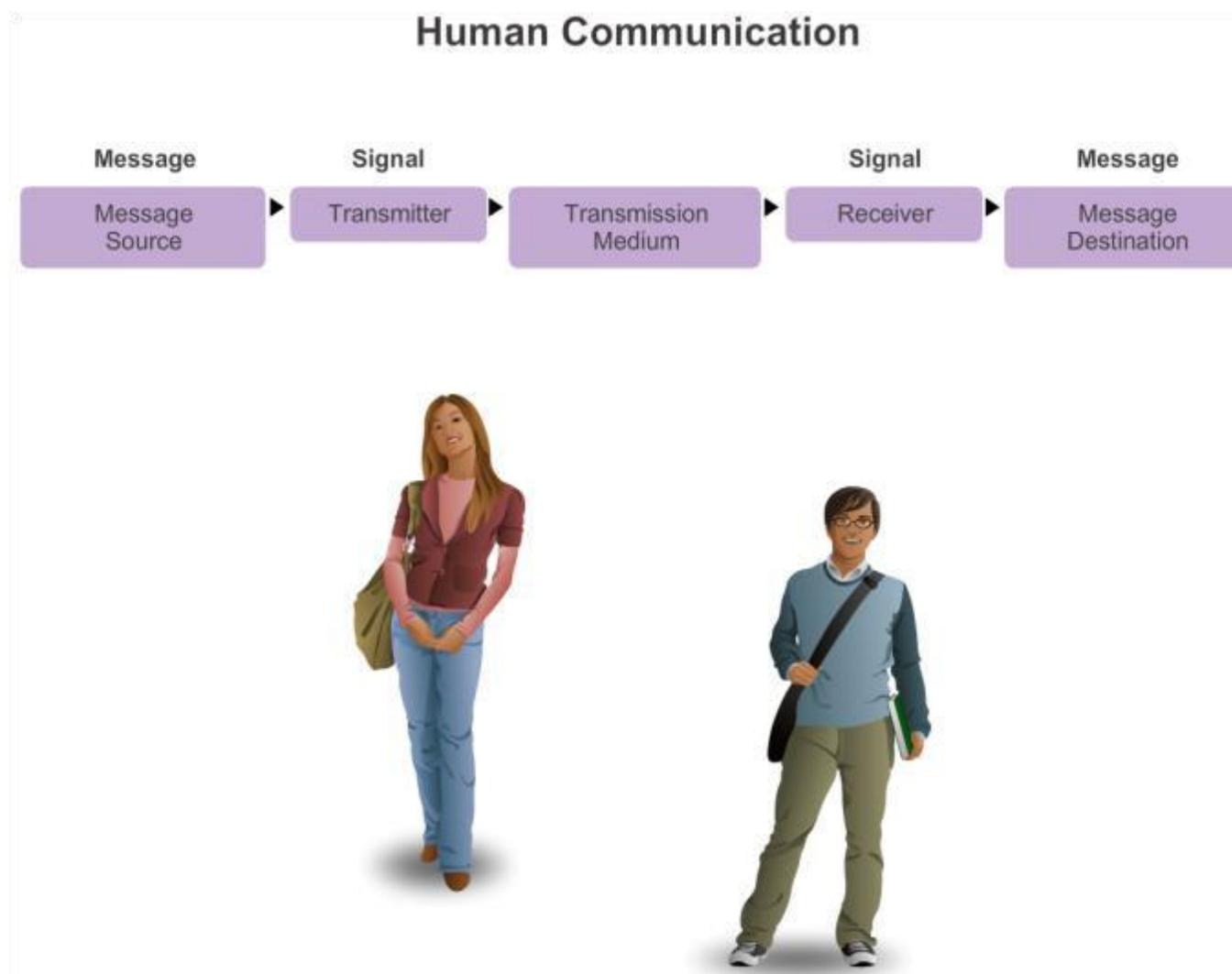
## 3.1 Rules of Communication





## The Rules

# What is Communication?





## The Rules

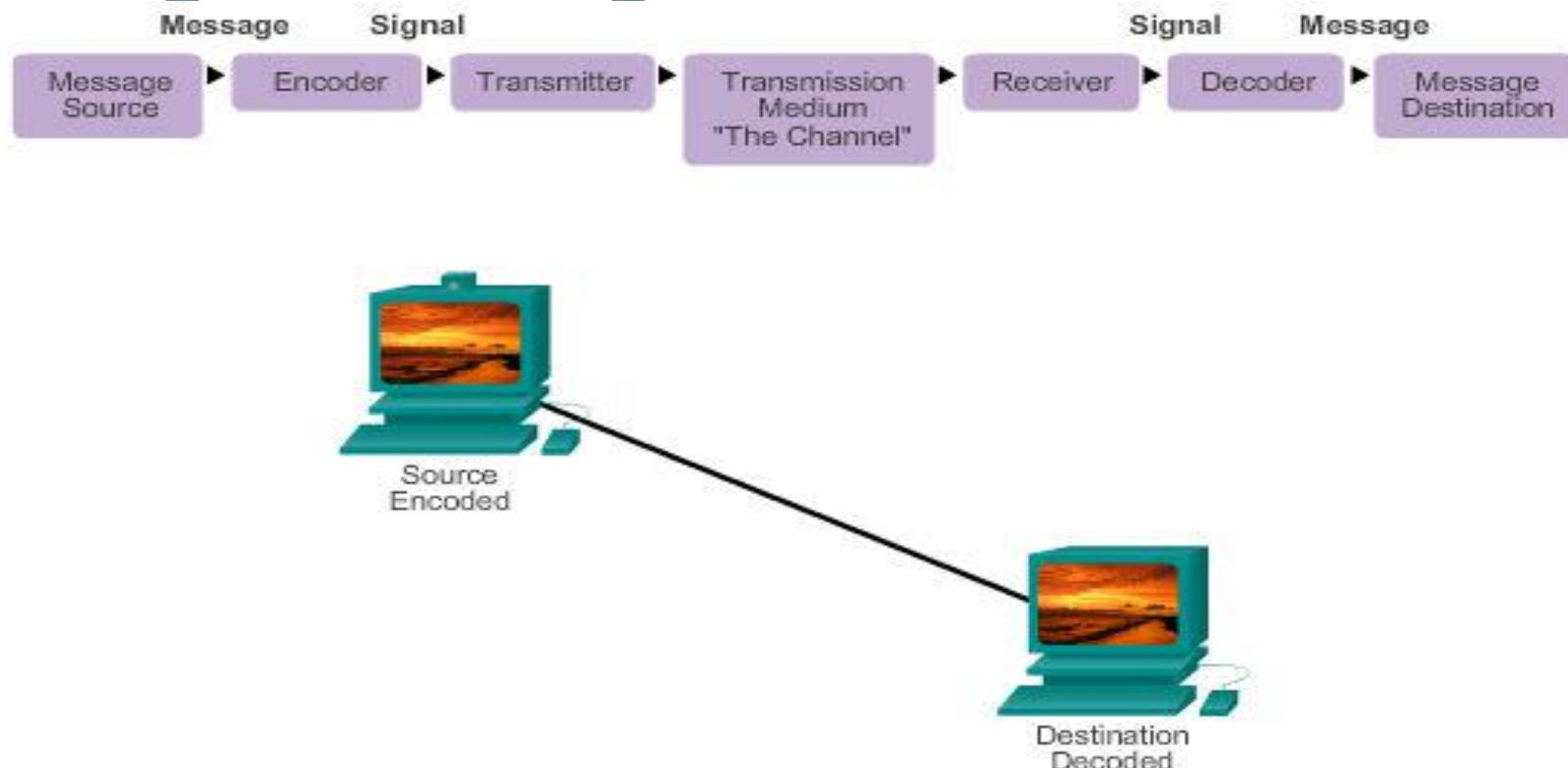
# Establishing the Rules

- An identified sender and receiver
- Agreed upon method of communicating (face-to-face, telephone, letter, photograph)
- Common language and grammar
- Speed and timing of delivery
- Confirmation or acknowledgment requirements



## The Rules

# Message Encoding



Encoding is the process of converting information into another acceptable form, for transmission.

Decoding reverses this process in order to interpret the information.



## The Rules

# Message Formatting and Encapsulation

Example: Personal letter contains the following elements:

- Identifier of the recipient's location
- Identifier of the sender's location
- Salutation or greeting
- Recipient identifier
- The message content
- Source identifier
- End of message indicator





- A message that is sent over a computer network follows specific format rules for it to be delivered and processed. Just as a letter is encapsulated in an envelope for delivery, so too are computer messages. Each computer message is encapsulated in a specific format, called a frame, before it is sent over the network. A frame acts like an envelope; it provides the address of the destination and the address of the source host,

Destination (physical / hardware address)	Source (physical / hardware address)	Start Flag (start of message indicator)	Recipient (destination identifier)	Sender (source identifier)	Encapsulated Data (bits)	End of Frame (end of message indicator)
Frame Addressing		Encapsulated Message				



## The Rules

# Message Size

An overview of the segmenting process:

- The size restrictions of frames require the source host to break a long message into individual pieces (or segments) that meet both the minimum and maximum size requirements.
- Each segment is encapsulated in a separate frame with the address information, and is sent over the network.
- At the receiving host, the messages are de-encapsulated and put back together to be processed and interpreted.



## The Rules

# Message Timing

- **Access Method:**

determines when someone is able to send a message.

If two people talk at the same time, a collision of information occurs and it is necessary for the two to back off and start again.

for computers to define an access method. Hosts on a network need an access method to know when to begin sending messages and how to respond when collisions occur.

- **Flow Control:**

how much information can be sent and the speed that it can be delivered. In network communication, source and destination hosts use flow control methods to negotiate correct timing for successful communication.

- **Response Timeout:**

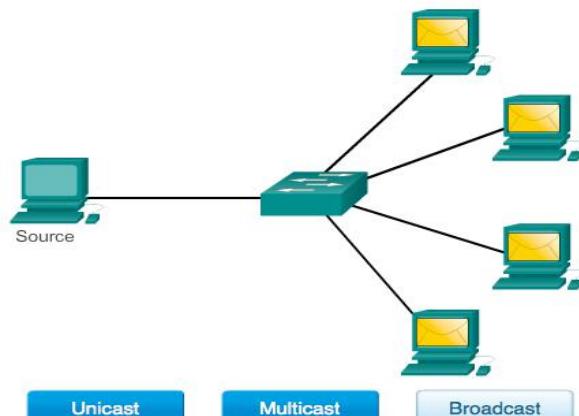
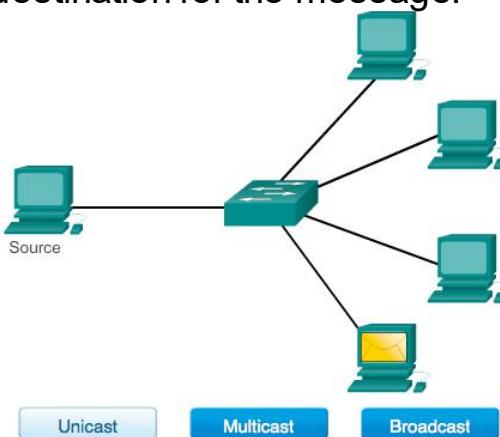
Hosts on the network also have rules that specify how long to wait for responses and what action to take if a response timeout occurs.



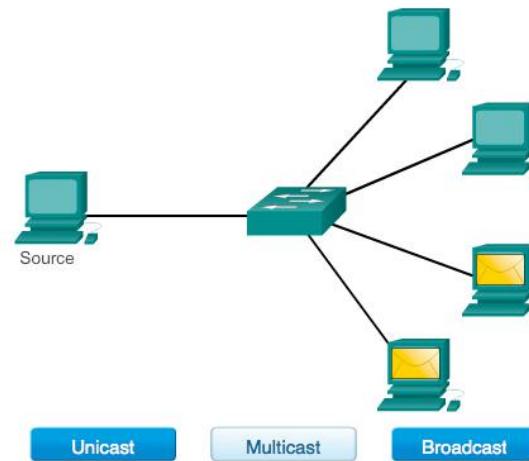
## The Rules

# Message Delivery Options

A one-to-one delivery option is referred to as a unicast, meaning there is only a single destination for the message.



When a host needs to send messages using a one-to-many delivery option, it is referred to as a multicast. Multicasting is the delivery of the same message to a group of host destinations simultaneously.



Broadcasting represents a one-to-all message delivery option. Some protocols use a special multicast message that is sent to all devices, making it essentially the same as a broadcast. Additionally, hosts may be required to acknowledge the receipt of some messages while not needing to acknowledge others.

## 3.2 Network Protocols and Standards





## Protocols

# Rules that Govern Communications

### Protocols: Rules that Govern Communications

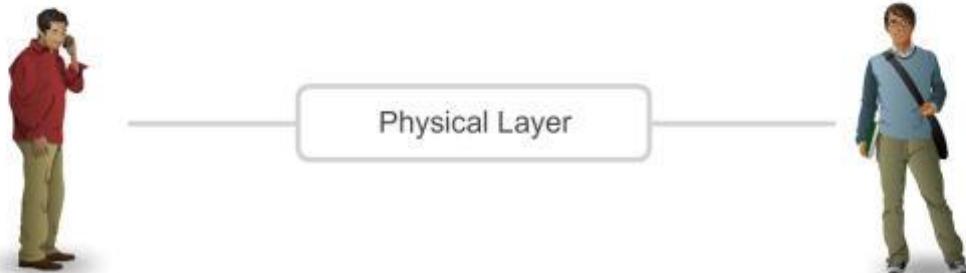
Content Layer

Where is the café?

#### Conversation protocol suite

1. Use a common language
2. Wait your turn
3. Signal when finished

Rules Layer



Protocol suites are sets of rules that work together to help solve a problem.



## Protocols

# Network Protocols

- **Networking protocols that describe the following processes:**
- How the message is formatted or structured
- The process by which networking devices share information about pathways with other networks
- How and when error and system messages are passed between devices
- The setup and termination of data transfer sessions

Networking protocols: define a common format and set of rules for exchanging messages between devices.

Some common networking protocols are:

Hypertext Transfer Protocol (HTTP),  
Transmission Control Protocol (TCP),  
and Internet Protocol (IP).



## Protocols

# Interaction of Protocols

- Application Protocol – Hypertext Transfer Protocol (HTTP)

**HTTP** - is an application protocol that governs the way a web server and a web client interact. HTTP defines the content and formatting of the requests and responses that are exchanged between the client and server.

- Transport Protocol – Transmission Control Protocol (TCP)

the transport protocol that manages the individual conversations. TCP divides the HTTP messages into smaller pieces, called segments. These segments are sent between the web server and client processes running at the destination host.

- Internet Protocol – Internet Protocol (IP)

**IP** - is responsible for taking the formatted segments from TCP, encapsulating them into packets, assigning them the appropriate addresses, and delivering them to the destination host.

- Network Access Protocols – Data link & physical layers

**Ethernet** - is a network access protocol that describes two primary functions: communication over a data link and the physical transmission of data on the network media. Network access protocols are responsible for taking the packets from IP and formatting them to be transmitted over the media.



## Protocol Suites

# Protocol Suites and Industry Standards

Protocol Suites and Industry Standards

TCP/IP	ISO	AppleTalk	Novell Netware
HTTP DNS DHCP FTP	ACSE ROSE TRSE SESE	AFP	NDS
TCP UDP	TP0 TP1 TP2 TP3 TP4	ATP AEP NBP RTMP	SPX
IPv4 IPv6 ICMPv4 ICMPv6	CONP/CMNS CLNP/CLNS	AARP	IPX
Ethernet	PPP	Frame Relay	ATM
			WLAN



## Protocol Suites

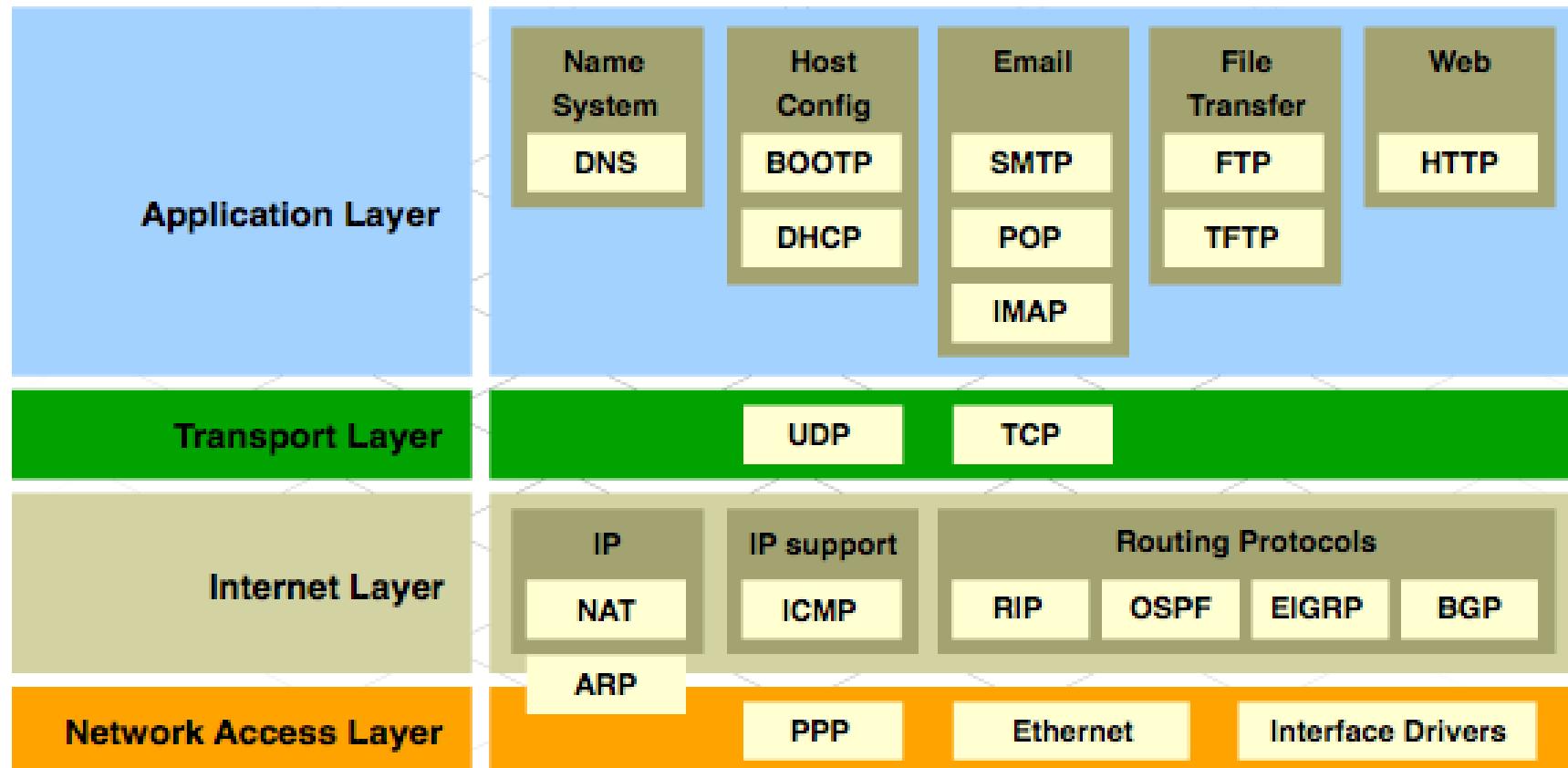
# Creation of Internet, Development of TCP/IP

- The first packet switching network and predecessor to today's Internet was the Advanced Research Projects Agency Network (ARPANET), which came to life in 1969 by connecting mainframe computers at four locations.
- ARPANET was funded by the U.S. Department of Defense for use by universities and research laboratories. Bolt, Beranek and Newman (BBN) was the contractor that did much of the initial development of the ARPANET, including creating the first router known as an Interface Message Processor (IMP).
- In 1973, Robert Kahn and Vinton Cerf began work on TCP to develop the next generation of the ARPANET. TCP was designed to replace ARPANET's current Network Control Program (NCP).
- In 1978, TCP was divided into two protocols: TCP and IP. Later, other protocols were added to the TCP/IP suite of protocols including Telnet, FTP, DNS, and many others.



## Protocol Suites

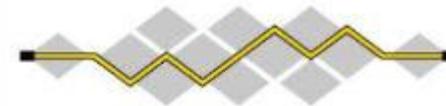
# TCP/IP Protocol Suite and Communication





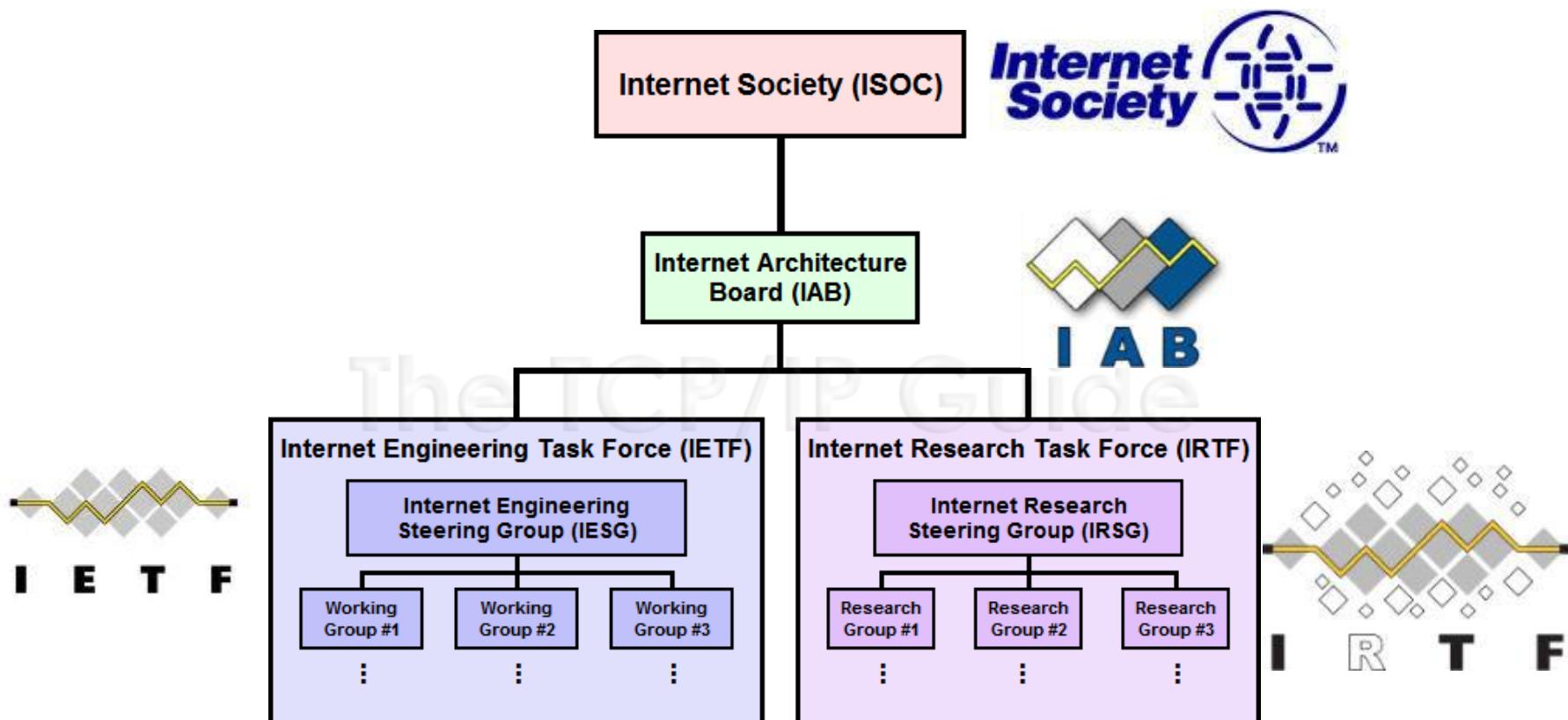
# Standards Organizations Open Standards

- The Internet Society (ISOC)
- The Internet Architecture Board (IAB)
- The Internet Engineering Task Force (IETF)
- Institute of Electrical and Electronics Engineers (IEEE)
- The International Organization for Standards (ISO)





# Standards Organizations ISOC, IAB, and IETF





## Standards Organizations

### IEEE

- 38 societies
- 130 journals
- 1,300 conferences each year
- 1,300 standards and projects
- 400,000 members
- 160 countries
- IEEE 802.3
- IEEE 802.11

#### 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



# Standards Organizations

## ISO



### OSI Model





## Standards Organizations

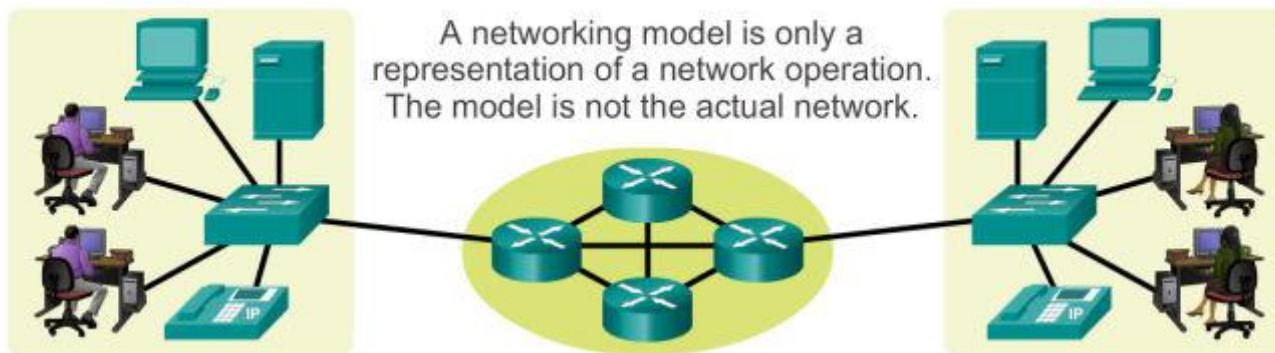
# Other Standards Organization

- The Electronic Industries Alliance (EIA)
- The Telecommunications Industry Association (TIA)
- The International Telecommunications Union – Telecommunications Standardization Sector (ITU-T)
- The Internet Corporation for Assigned Names and Numbers (ICANN)
- The Internet Assigned Numbers Authority (IANA)



## Reference Models

# Benefits of Using a Layered Model



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



## Reference Models

# The OSI Reference Model

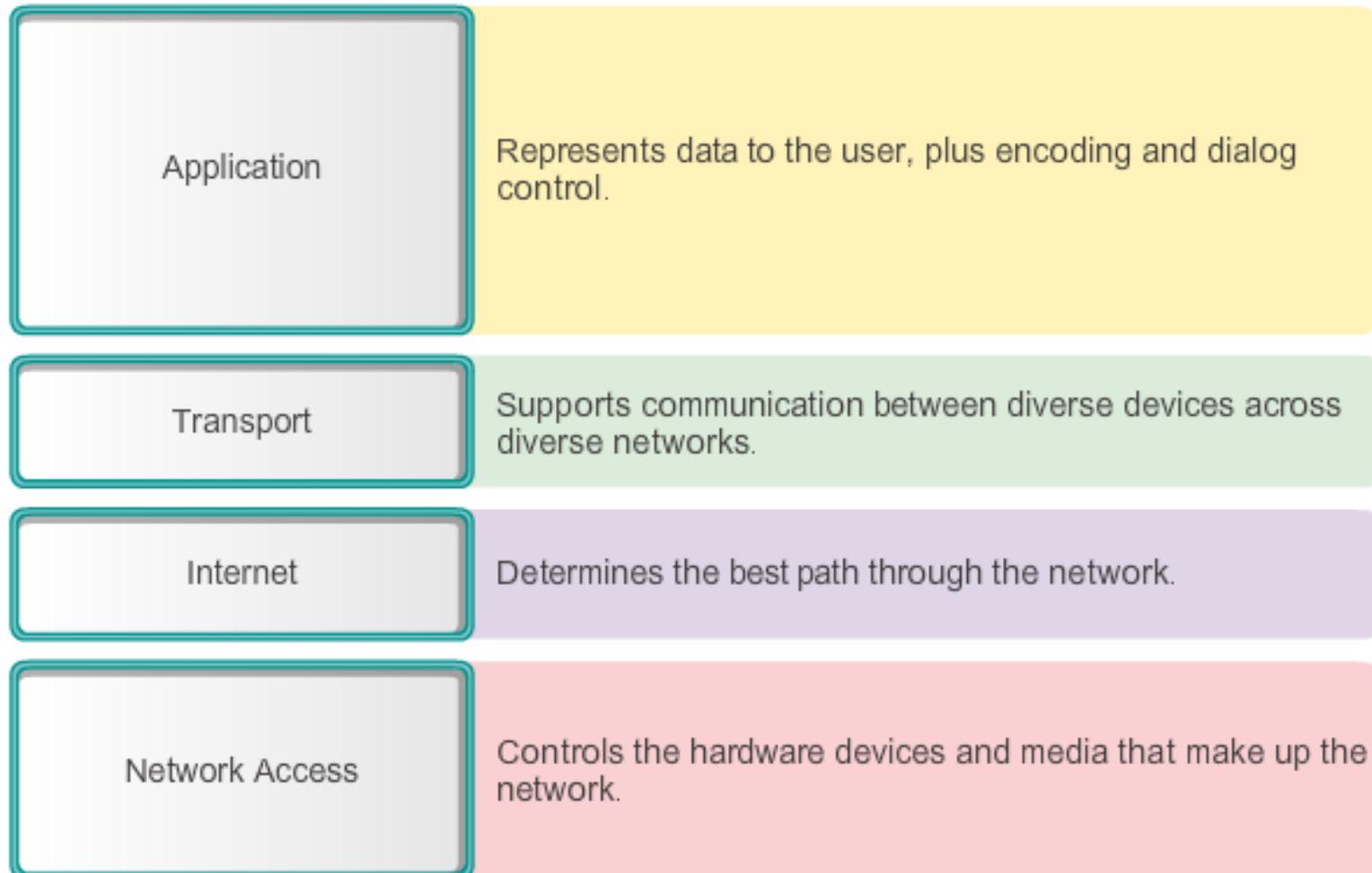




## Reference Models

# The TCP/IP Reference Model

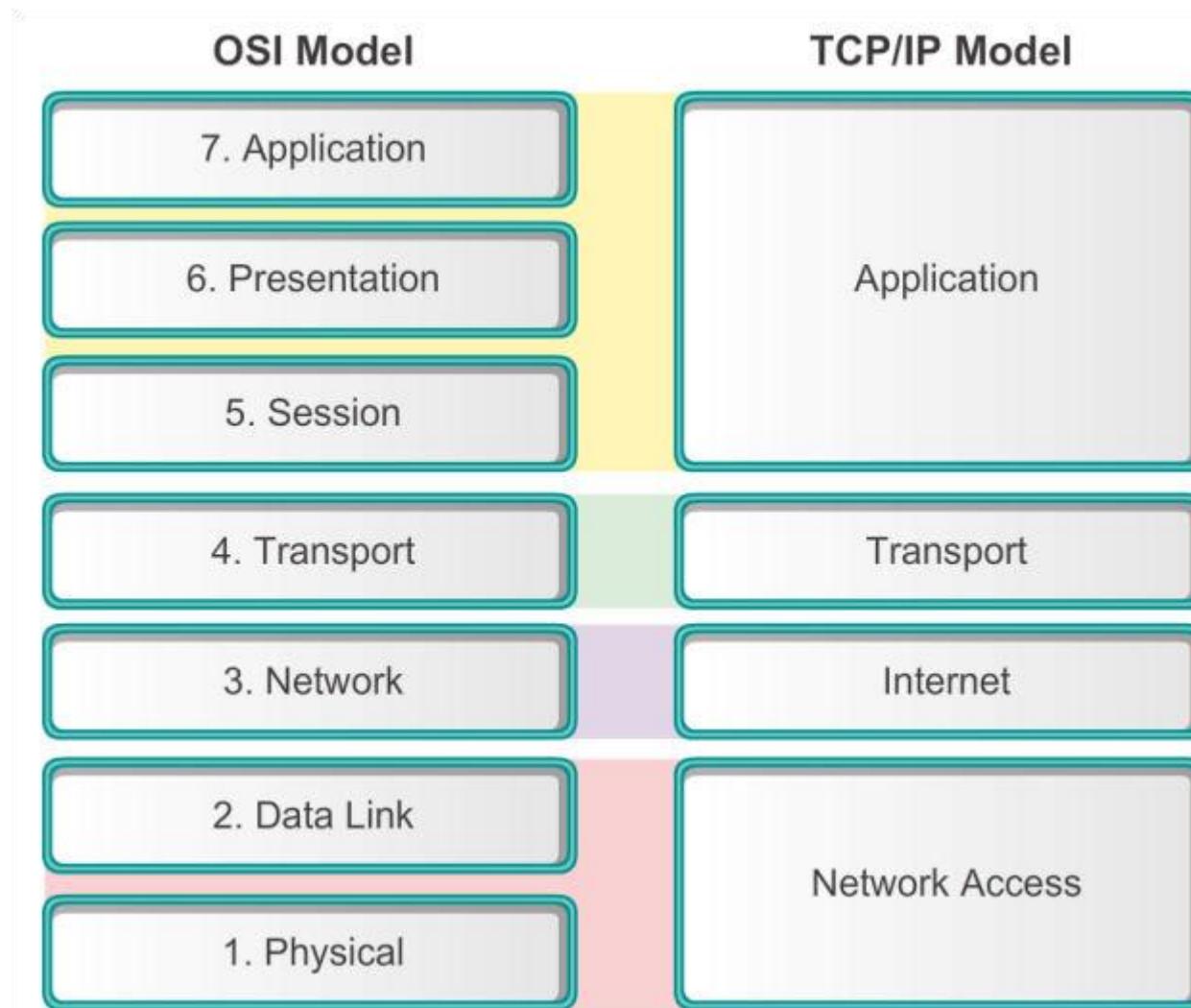
### TCP/IP Model





## Reference Models

# Comparing the OSI and TCP/IP Models



### 3.3 Moving Data in the Network





## Data Encapsulation

# Communicating the Messages

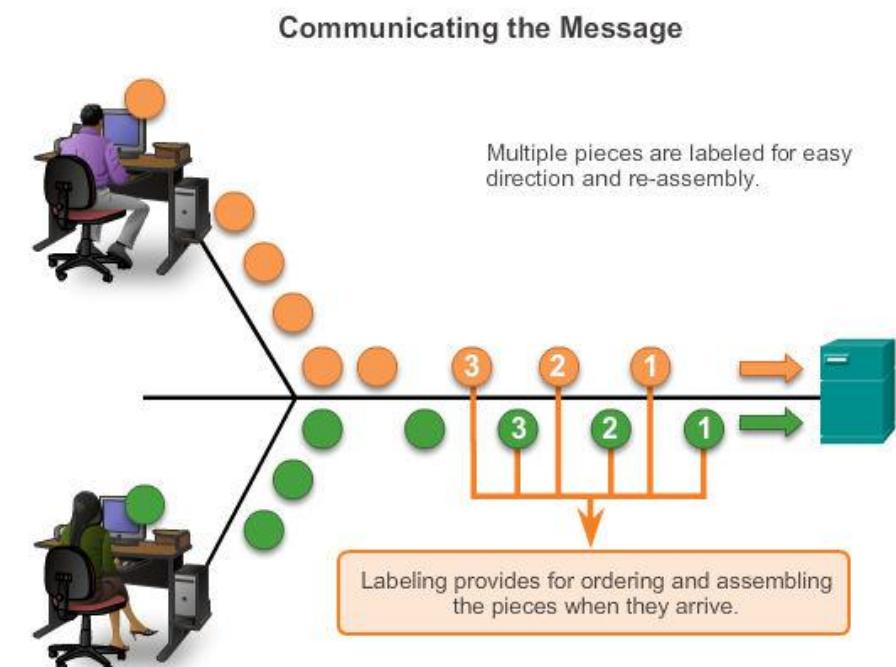
- Segmenting message benefits

  - Different conversations can be interleaved

  - Increased reliability of network communications

- Segmenting message disadvantage

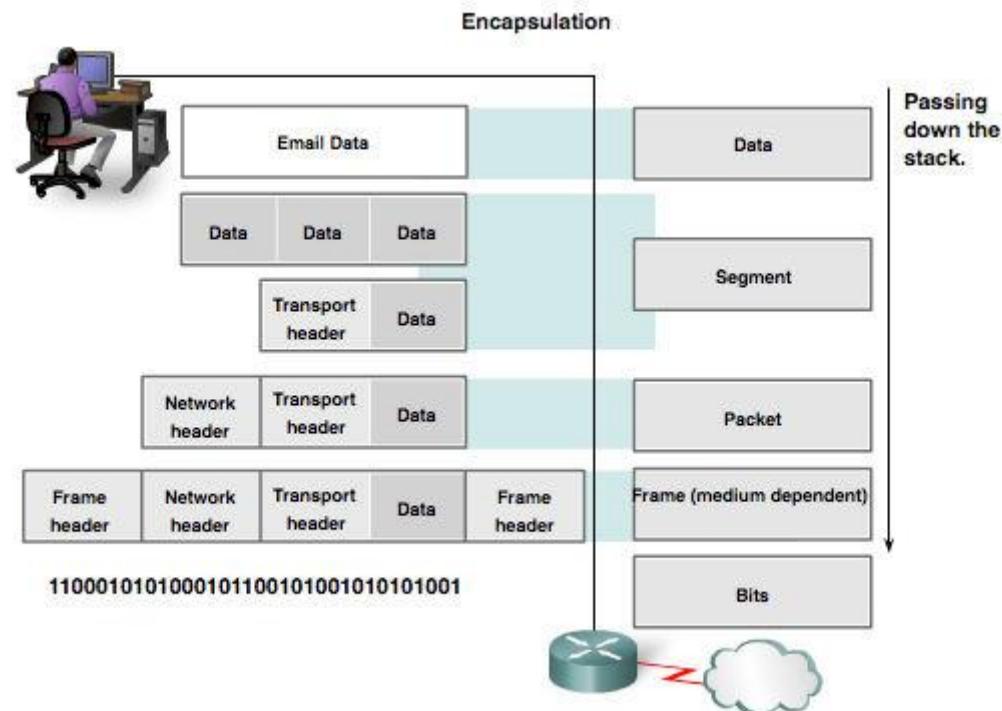
  - Increased level of complexity





# Data Encapsulation Protocol Data Units (PDUs)

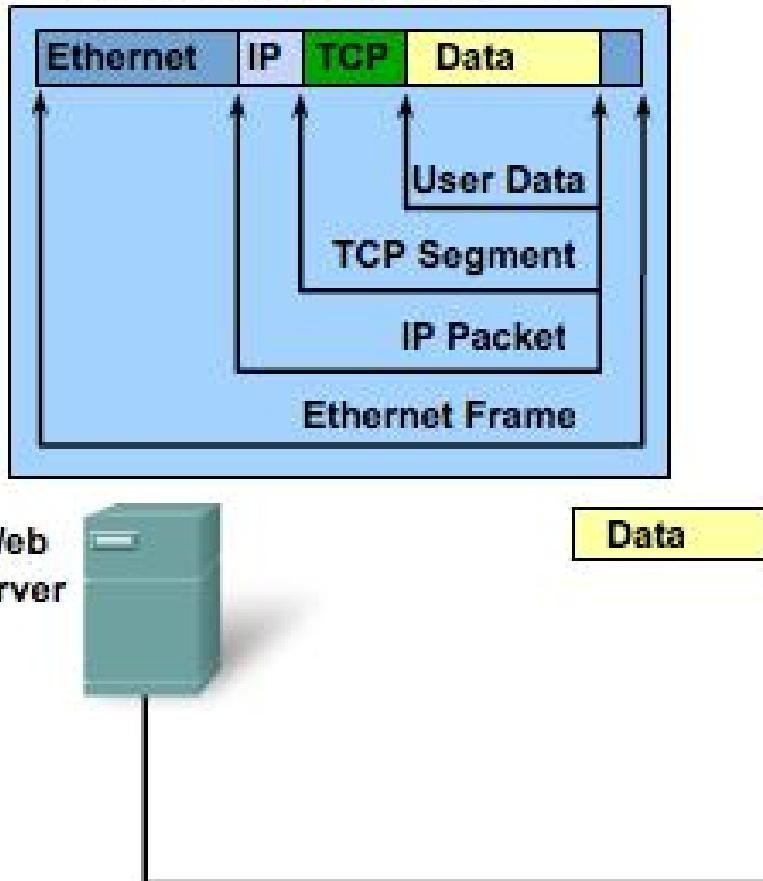
- Data – use at Application Layer
- Segment – use at Transport Layer
- Packet – use at Network Layer
- Frame – use at Data Link Layer
- Bits – use at Physical Layer



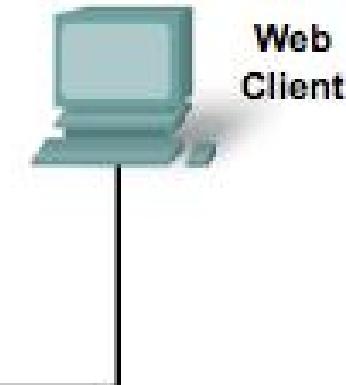


# Data Encapsulation Protocol Encapsulation

## Protocol Encapsulation Terms



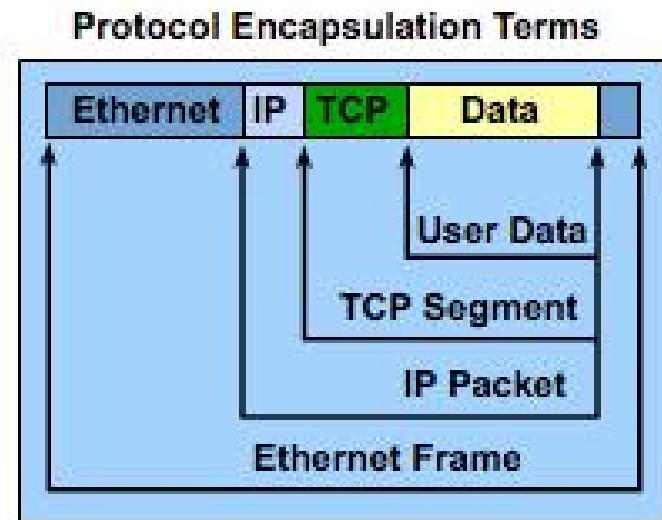
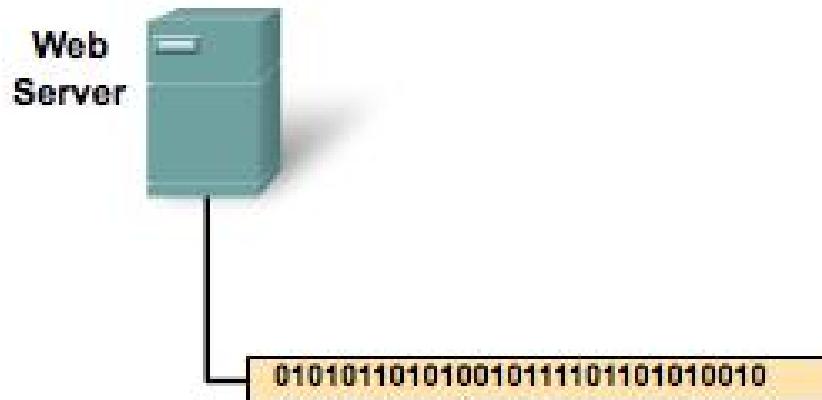
When sending messages on a network, the encapsulation process works from top to bottom. At each layer, the upper layer information is considered data within the encapsulated protocol. For example, the TCP segment is considered data within the IP packet.





# Data Encapsulation Protocol De-encapsulation

De-encapsulation is the process used by a receiving device to remove one or more of the protocol headers. The data is de-encapsulated as it moves up the stack toward the end-user application.





## Moving Data in the Network

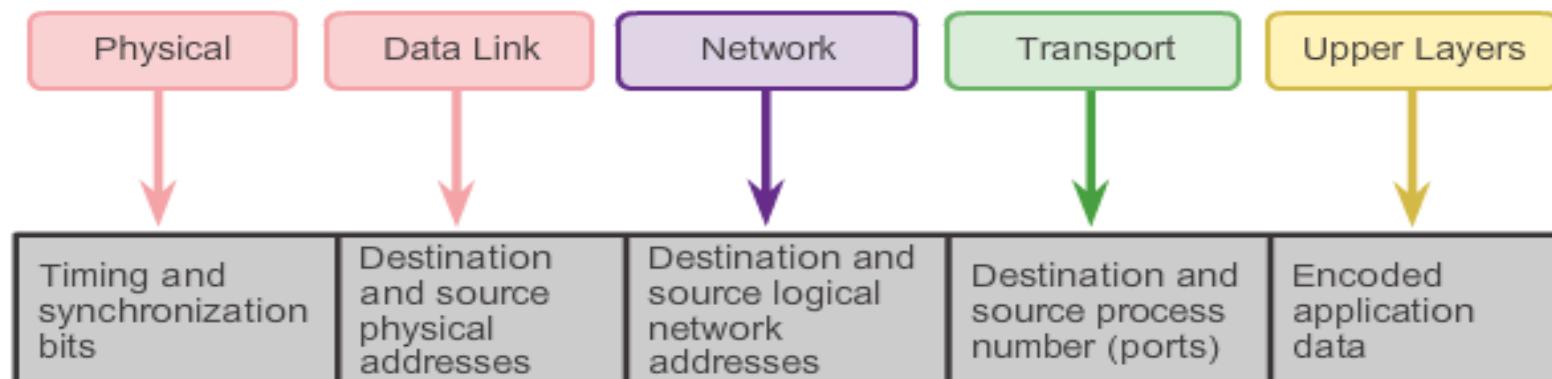
# Accessing Local Resources

The network and data link layers are responsible for delivering the data from the source device to the destination device.

**Network layer source and destination addresses** - Responsible for delivering the IP packet from the original source to the final destination, either on the same network or to a remote network.

**Data link layer source and destination addresses** – Responsible for delivering the data link frame from one network interface card (NIC) to another NIC on the same network.

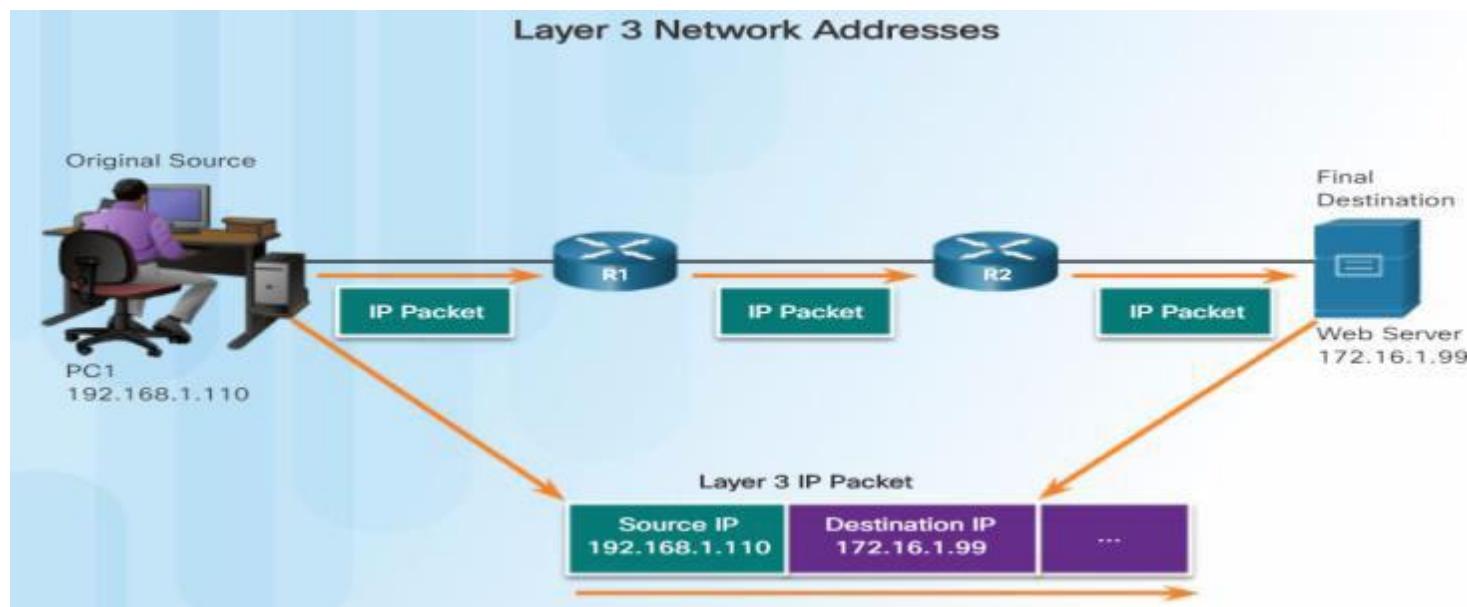
## Network Addresses and Data Link Addresses





# Data Link Addresses

- An IP address is the network layer, or Layer 3, logical address used to deliver the IP packet from the original source to the final destination.
- The IP packet contains two IP addresses:
  - Source IP address** - The IP address of the sending device, the original source of the packet.
  - Destination IP address** - The IP address of the receiving device, the final destination of the packet.





## Accessing Local Resources

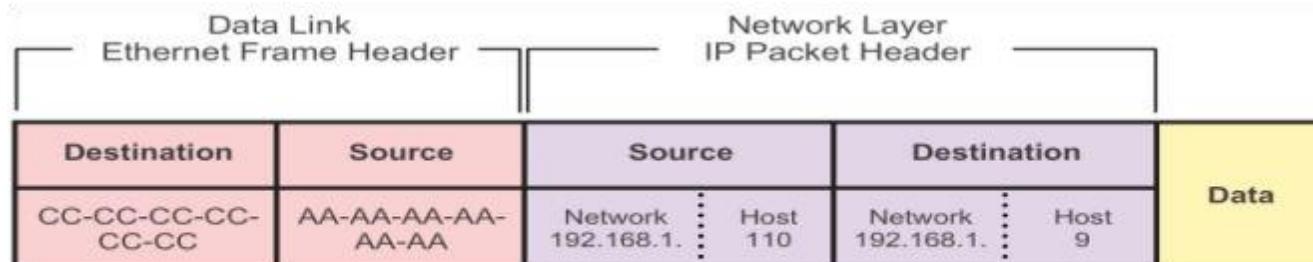
# Communicating with Device / Same Network

### Role of the Network Layer Addresses

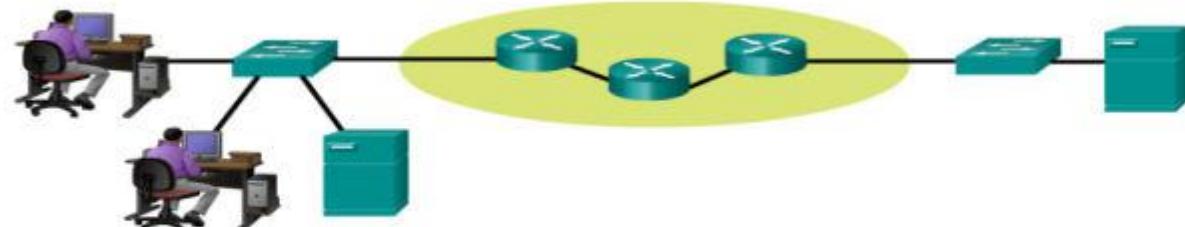
The network layer addresses, or IP addresses, indicate the original source and final destination. An IP address contains two parts:

**Network portion** – The left-most part of the address that indicates which network the IP address is a member. All devices on the same network will have the same network portion of the address.

**Host portion** – The remaining part of the address that identifies a specific device on the network. The host portion is unique for each device on the network.



**PC1**  
192.168.1.110  
AA-AA-AA-AA-AA-AA



**FTP Server**  
192.168.1.9  
CC-CC-CC-CC-CC-CC



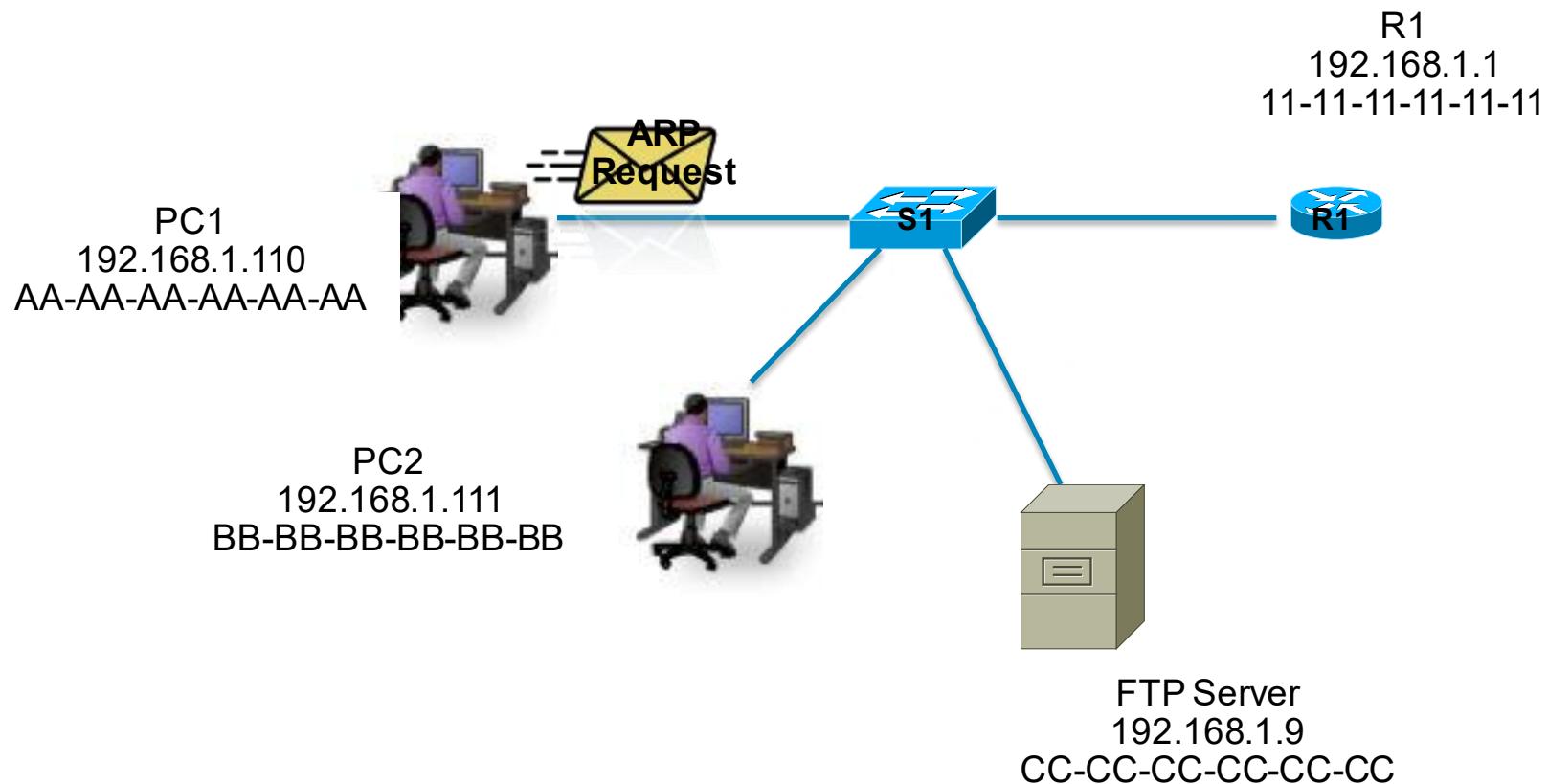
## Accessing Local Resources

# Communicating with Device / Same Network

- **Role of the Data Link Layer Addresses**
- When the sender and receiver of the IP packet are on the same network, the data link frame is sent directly to the receiving device. On an Ethernet network, the data link addresses are known as Ethernet (Media Access Control) addresses. MAC addresses are physically embedded on the Ethernet NIC.
- **Source MAC address** - This is the data link address, or the Ethernet MAC address, of the device that sends the data link frame with the encapsulated IP packet. The MAC address of the Ethernet NIC of PC1 is AA-AA-AA-AA-AA-AA, written in hexadecimal notation.
- **Destination MAC address** - When the receiving device is on the same network as the sending device, this is the data link address of the receiving device. In this example, the destination MAC address is the MAC address of the FTP server: CC-CC-CC-CC-CC-CC, written in hexadecimal notation.



# Accessing Local Resources MAC and IP Addresses

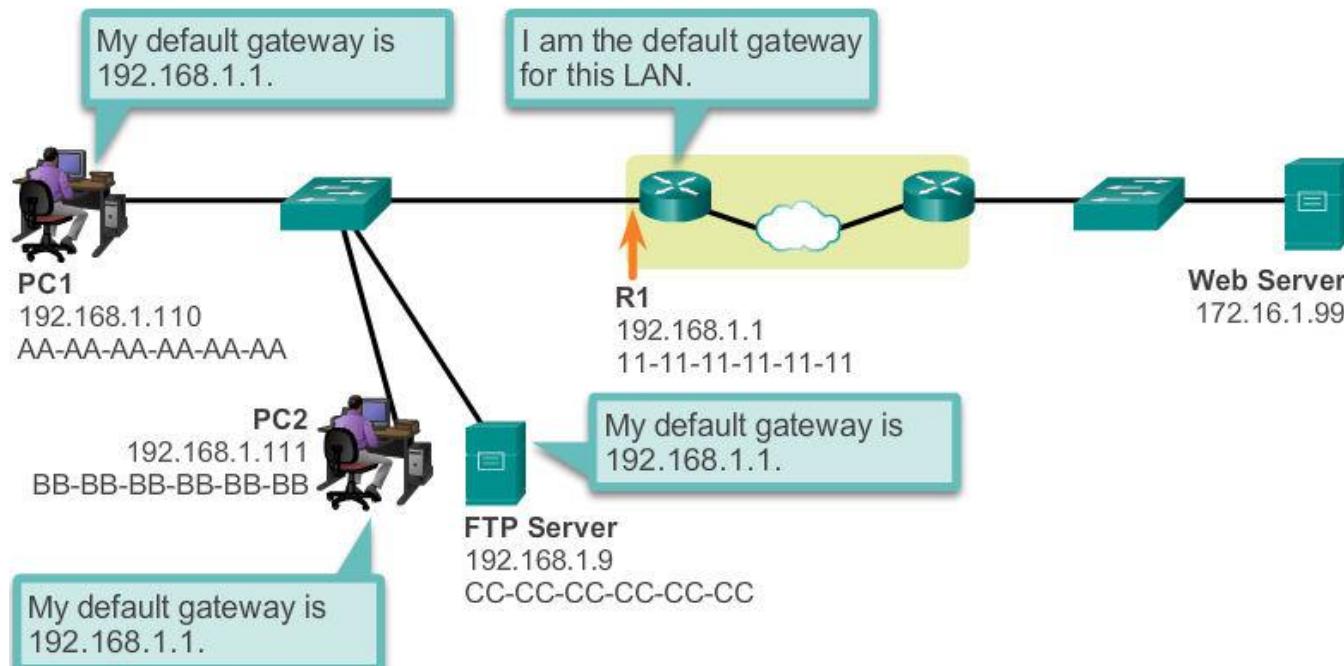




# Accessing Remote Resources Default Gateway

## Getting the Pieces to the Correct Network

Protocol Data Unit (PDU)				
Source		Destination		Data
Network 192.168.1	Device 110	Network 172.16.1	Device 99	





## Accessing Remote Resources

# Communicating Device / Remote Network

In this example we have a client computer, PC1, communicating with a server, named Web Server, on a different IP network.

### Role of the Network Layer Addresses

When the sender of the packet is on a different network from the receiver, the source and destination IP addresses will represent hosts on different networks. This will be indicated by the network portion of the IP address of the destination host.

**Source IP address** - The IP address of the sending device, the client computer PC1: 192.168.1.110.

**Destination IP address** - The IP address of the receiving device, the server, Web Server: 172.16.1.99.

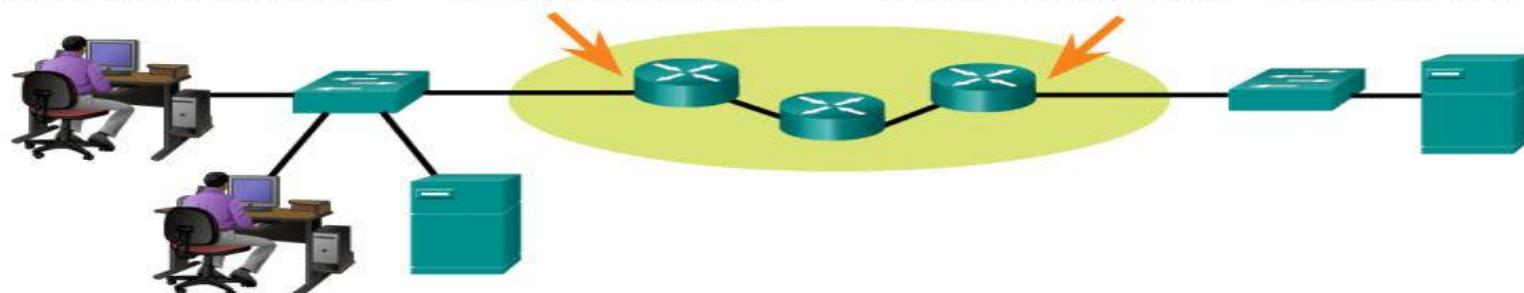
Data Link Ethernet Frame Header		Network Layer IP Packet Header			
Destination	Source	Source	Destination	Data	
11-11-11-11-11-11	AA-AA-AA-AA-AA-AA	Network 192.168.1.	Device 110	Network 172.16.1.	Device 99

**PC1**  
192.168.1.110  
AA-AA-AA-AA-AA-AA

**R1**  
192.168.1.1  
11-11-11-11-11-11

**R2**  
172.16.1.99  
22-22-22-22-22-22

**Web Server**  
172.16.1.99  
AB-CD-EF-12-34-56





## Accessing Remote Resources

# Communicating Device / Remote Network

- **Role of the Data Link Layer Addresses**
- When the sender and receiver of the IP packet are on different networks, the Ethernet data link frame cannot be sent directly to the destination host because the host is not directly reachable in the network of the sender. The Ethernet frame must be sent to another device known as the router or default gateway. In our example, the default gateway is R1. R1 has an Ethernet data link address that is on the same network as PC1. This allows PC1 to reach the router directly.
- **Source MAC address** - The Ethernet MAC address of the sending device, PC1. The MAC address of the Ethernet interface of PC1 is AA-AA-AA-AA-AA-AA.
- **Destination MAC address** - When the receiving device, the destination IP address, is on a different network from the sending device, the sending device uses the Ethernet MAC address of the default gateway or router. In this example, the destination MAC address is the MAC address of R1's Ethernet interface, 11-11-11-11-11-11. This is the interface that is attached to the same network as PC1.



# Network Protocols and Communications Summary

In this chapter, you learned:

- Data networks are systems of end devices, intermediary devices, and the media connecting the devices. For communication to occur, these devices must know how to communicate.
- These devices must comply with communication rules and protocols. TCP/IP is an example of a protocol suite.
- Most protocols are created by a standards organization such as the IETF or IEEE.
- The most widely-used networking models are the OSI and TCP/IP models.
- Data that passes down the stack of the OSI model is segmented into pieces and encapsulated with addresses and other labels. The process is reversed as the pieces are de-encapsulated and passed up the destination protocol stack.



# Network Protocols and Communications Summary (cont.)

In this chapter, you learned:

- The OSI model describes the processes of encoding, formatting, segmenting, and encapsulating data for transmission over the network.
- The TCP/IP protocol suite is an open standard protocol that has been endorsed by the networking industry and ratified, or approved, by a standards organization.
- The Internet Protocol Suite is a suite of protocols required for transmitting and receiving information using the Internet.
- Protocol Data Units (PDUs) are named according to the protocols of the TCP/IP suite: data, segment, packet, frame, and bits.
- Applying models allows individuals, companies, and trade associations to analyze current networks and plan the networks of the future.

# Cisco | Networking Academy®

Mind Wide Open™



## Chapter 4: Network Access



## Introduction to Networks

Cisco | Networking Academy®  
Mind Wide Open™



# Chapter 4: Objectives

Upon completion of this chapter, you will be able to:

- Identify device connectivity options.
- Describe the purpose and functions of the physical layer in the network.
- Describe basic principles of the physical layer standards.
- Identify the basic characteristics of copper cabling.
- Build a UTP cable used in Ethernet networks.
- Describe fiber-optic cabling and its main advantages over other media.
- Describe wireless media.
- Select the appropriate media for a given requirement and connect devices.



# Chapter 4: Objectives (cont.)

Upon completion of this chapter, you will be able to:

- Describe the purpose and function of the data link layer in preparing communication for transmission on specific media.
- Describe the Layer 2 frame structure and identify generic fields.
- Identify several sources for the protocols and standards used by the data link layer.
- Compare the functions of logical topologies and physical topologies.
- Describe the basic characteristics of media control methods on WAN topologies.
- Describe the basic characteristics of media control methods on LAN topologies.
- Describe the characteristics and functions of the data link frame.

## 4.4 Media Access Control





# Chapter 4

- 4.1 Physical Layer Protocols
- 4.2 Network Media
- 4.3 Data Link Layer Protocols
- 4.4 Media Access Control
- 4.5 Summary

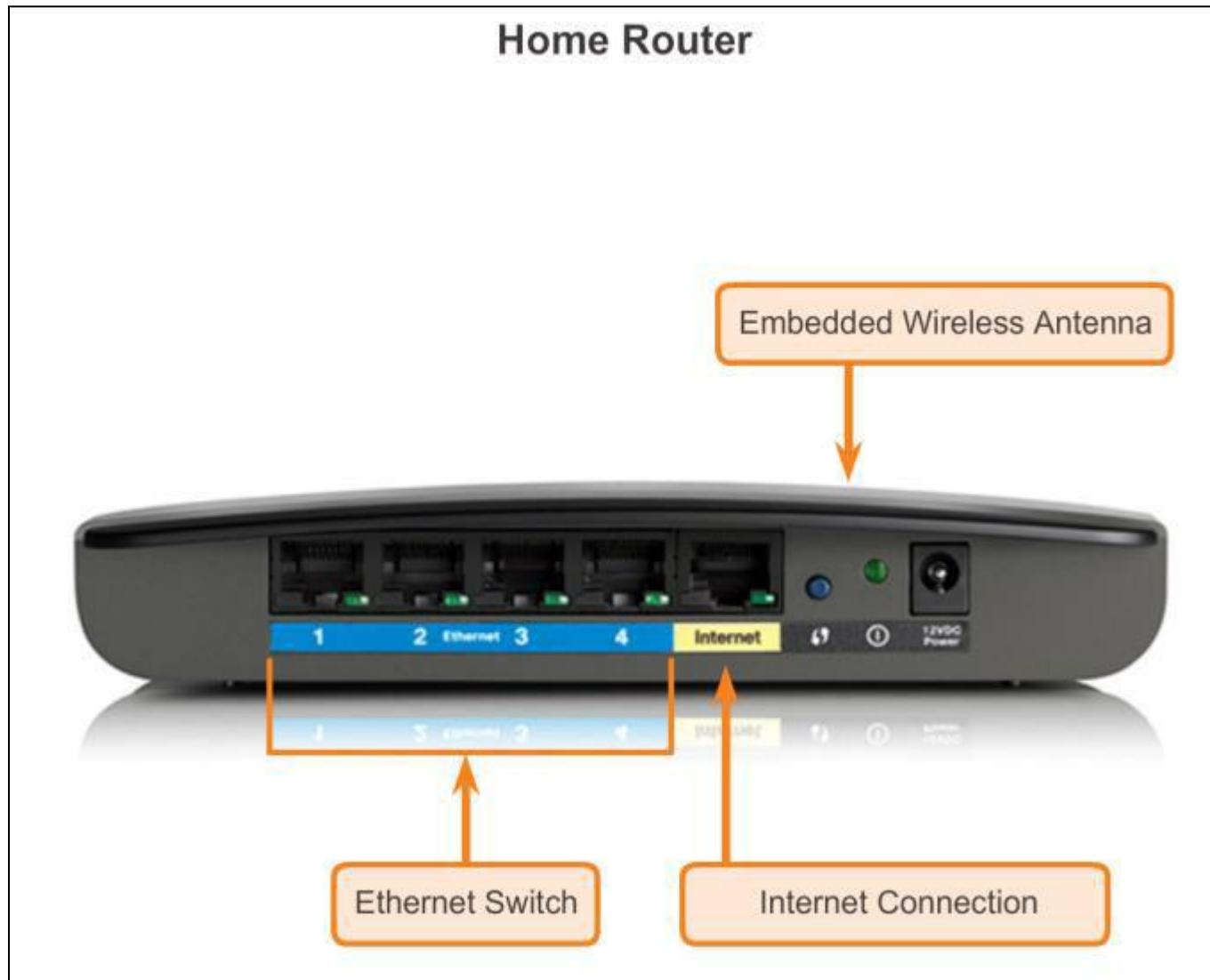
## 4.1 Physical Layer Protocols





Getting it Connected

# Connecting to the Network





## Getting it Connected

# Connecting to the Network (cont.)

### Connecting to the Wired LAN

Connect your computer to the Ethernet port (1, 2, 3, or 4).

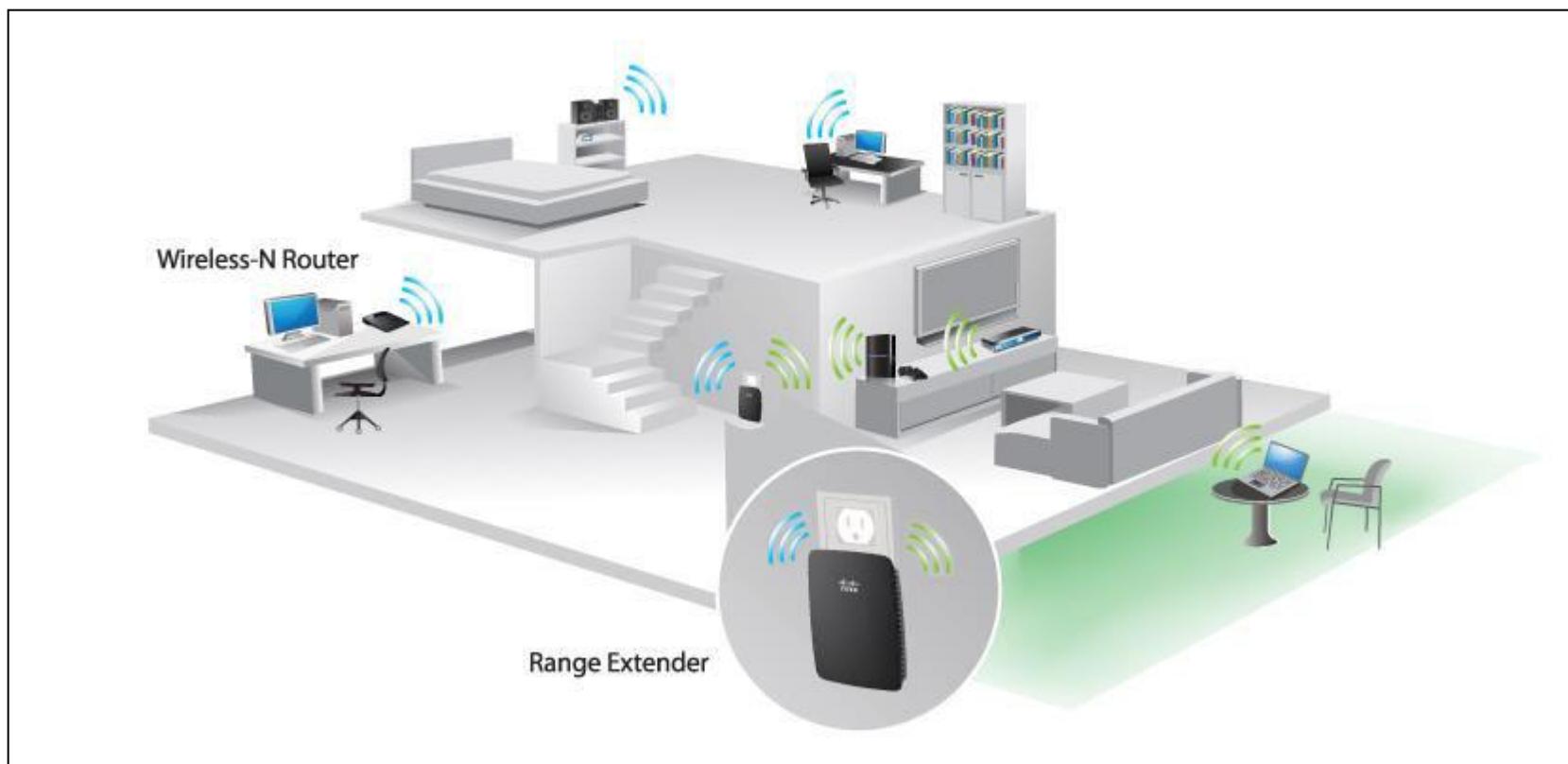




# Getting it Connected

# Network Interface Cards

## Connecting to the Wireless LAN with a Range Extender





- Network Interface Cards (NICs) connect a device to the network.
- Ethernet NICs are used for a wired connection, as shown in Figure, whereas WLAN (Wireless Local Area Network) NICs are used for wireless.
- An end-user device may include one or both types of NICs.
- A network printer, for example, may only have an Ethernet NIC, and therefore, must connect to the network using an Ethernet cable. Other devices, such as tablets and smartphones, might only contain a WLAN NIC and must use a wireless connection.
-

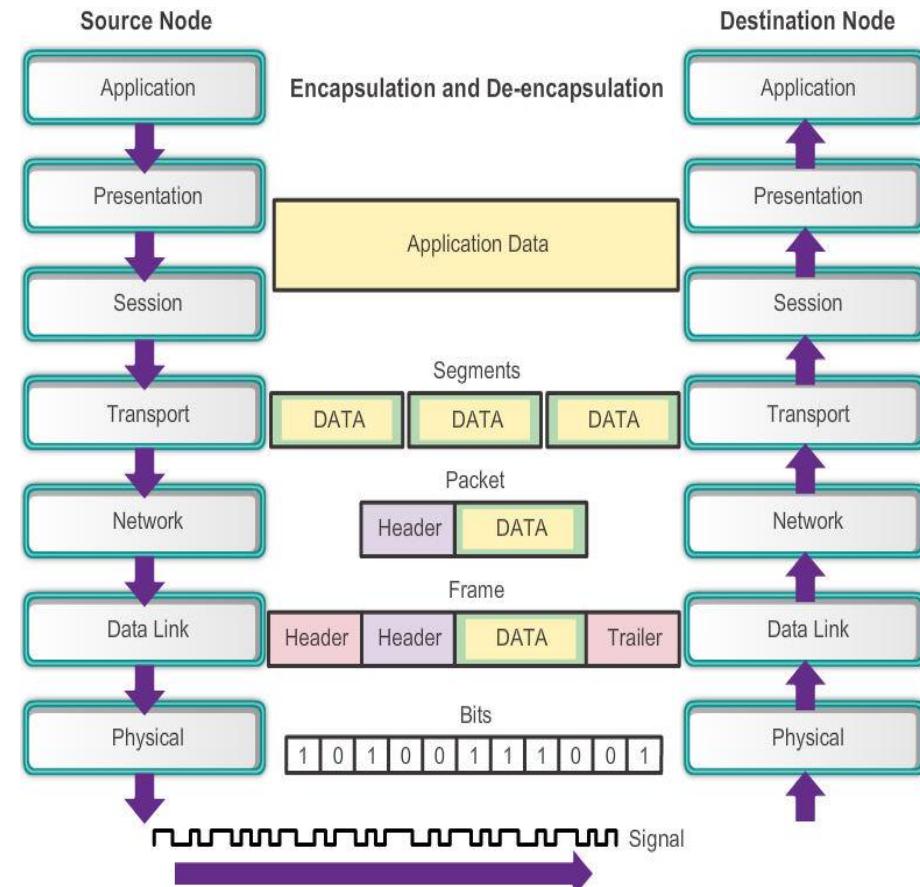


# Purpose of the Physical Layer

# The Physical Layer

The process that data undergoes from a source node to a destination node is:

- 1- The user data is segmented by the transport layer, placed into packets by the network layer, and further encapsulated into frames by the data link layer.
- 2- The physical layer encodes the frames and creates the electrical, optical, or radio wave signals that represent the bits in each frame.
- 3- These signals are then sent on the media, one at a time.
- 4- The destination node physical layer retrieves these individual signals from the media, restores them to their bit representations, and passes the bits up to the data link layer as a complete frame.





# Purpose of the Physical Layer

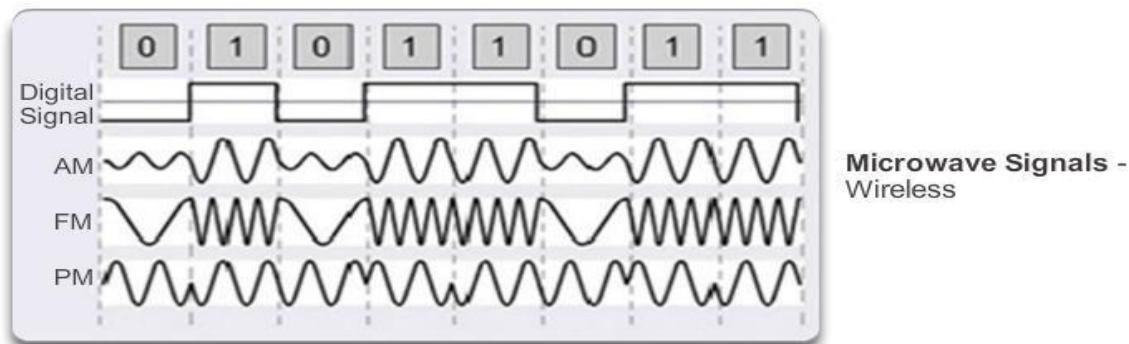
# Physical Layer Media

There are three basic forms of network 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.





# Purpose of the Physical Layer Physical Layer Standards

Standard Organization	Networking Standards
ISO	<ul style="list-style-type: none"><li>ISO 8877: Officially adopted the RJ connectors (e.g., RJ-11, RJ-45)</li><li>ISO 11801: Network cabling standard similar to EIA/TIA568.</li></ul>
EIA/TIA	<ul style="list-style-type: none"><li>TIA-568-C: Telecommunications cabling standards, used by nearly all voice, video and data networks.</li><li>TIA-569-B: Commercial Building Standards for Telecommunications Pathways and Spaces</li><li>TIA-598-C: Fiber optic color coding</li><li>TIA-942: Telecommunications Infrastructure Standard for Data Centers</li></ul>
ANSI	<ul style="list-style-type: none"><li>568-C: RJ-45 pinouts. Co-developed with EIA/TIA</li></ul>
ITU-T	<ul style="list-style-type: none"><li>G.992: ADSL</li></ul>
IEEE	<ul style="list-style-type: none"><li>802.3: Ethernet</li><li>802.11: Wireless LAN (WLAN) &amp; Mesh (Wi-Fi certification)</li><li>802.15: Bluetooth</li></ul>



# Fundamental Principles of Layer 1

# Physical Layer Fundamental Principles

Media	Physical Components	Frame Encoding Technique	Signalling Method
Copper Cable	<ul style="list-style-type: none"><li>• UTP</li><li>• Coaxial</li><li>• Connectors</li><li>• NICs</li><li>• Ports</li><li>• Interfaces</li></ul>	<ul style="list-style-type: none"><li>• Manchester Encoding</li><li>• Non-Return to Zero (NRZ) techniques</li><li>• 4B/5B codes are used with Multi-Level Transition Level 3 (MLT-3) signaling</li><li>• 8B/10B</li><li>• PAM5</li></ul>	<ul style="list-style-type: none"><li>• Changes in the electromagnetic field</li><li>• Intensity of the electromagnetic field</li><li>• Phase of the electromagnetic wave</li></ul>
Fiber Optic Cable	<ul style="list-style-type: none"><li>• Single-mode Fiber</li><li>• Multimode Fiber</li><li>• Connectors</li><li>• NICs</li><li>• Interfaces</li><li>• Lasers and LEDs</li><li>• Photoreceptors</li></ul>	<ul style="list-style-type: none"><li>• Pulses of light</li><li>• Wavelength multiplexing using different colors</li></ul>	<ul style="list-style-type: none"><li>• A pulse equals 1.</li><li>• No pulse is 0.</li></ul>
Wireless Media	<ul style="list-style-type: none"><li>• Access Points</li><li>• NICs</li><li>• Radio</li><li>• Antennae</li></ul>	<ul style="list-style-type: none"><li>• DSSS (direct-sequence spread-spectrum)</li><li>• OFDM (orthogonal frequency division multiplexing)</li></ul>	<ul style="list-style-type: none"><li>• Radio waves</li></ul>



# Fundamental Principles of Layer 1 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. Digital bandwidth measures the amount of data that can flow from one place to another in a given amount of time.

Bandwidth is sometimes thought of as the speed that bits travel

A combination of factors determines the practical bandwidth of a network:

- 1- The properties of the physical media
- 2- The technologies chosen for signaling and detecting network signals

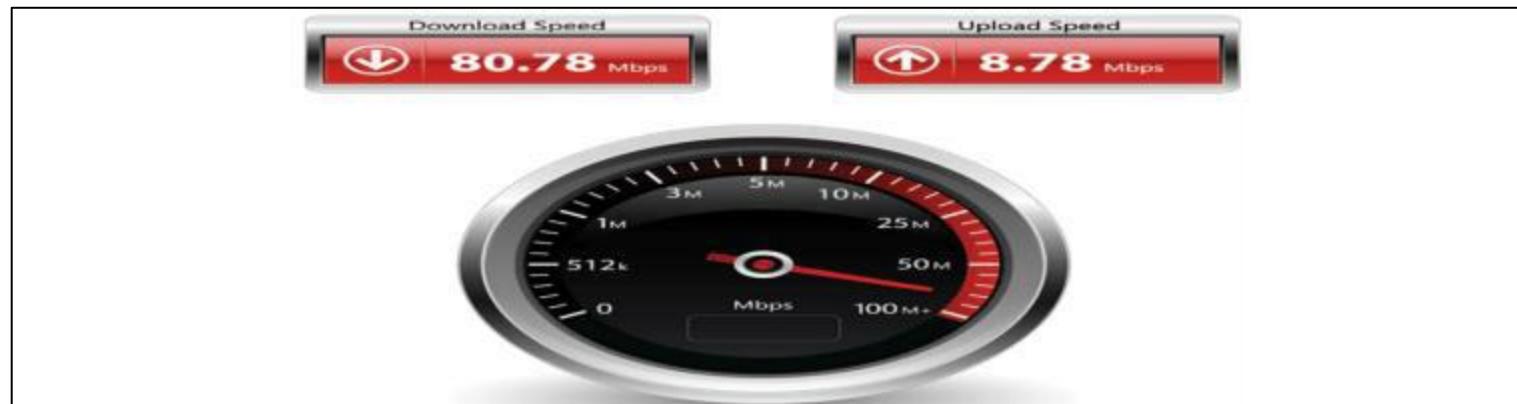


# Fundamental Principles of Layer 1 Throughput

Throughput is the measure of the transfer of bits across the media over a given period of time.

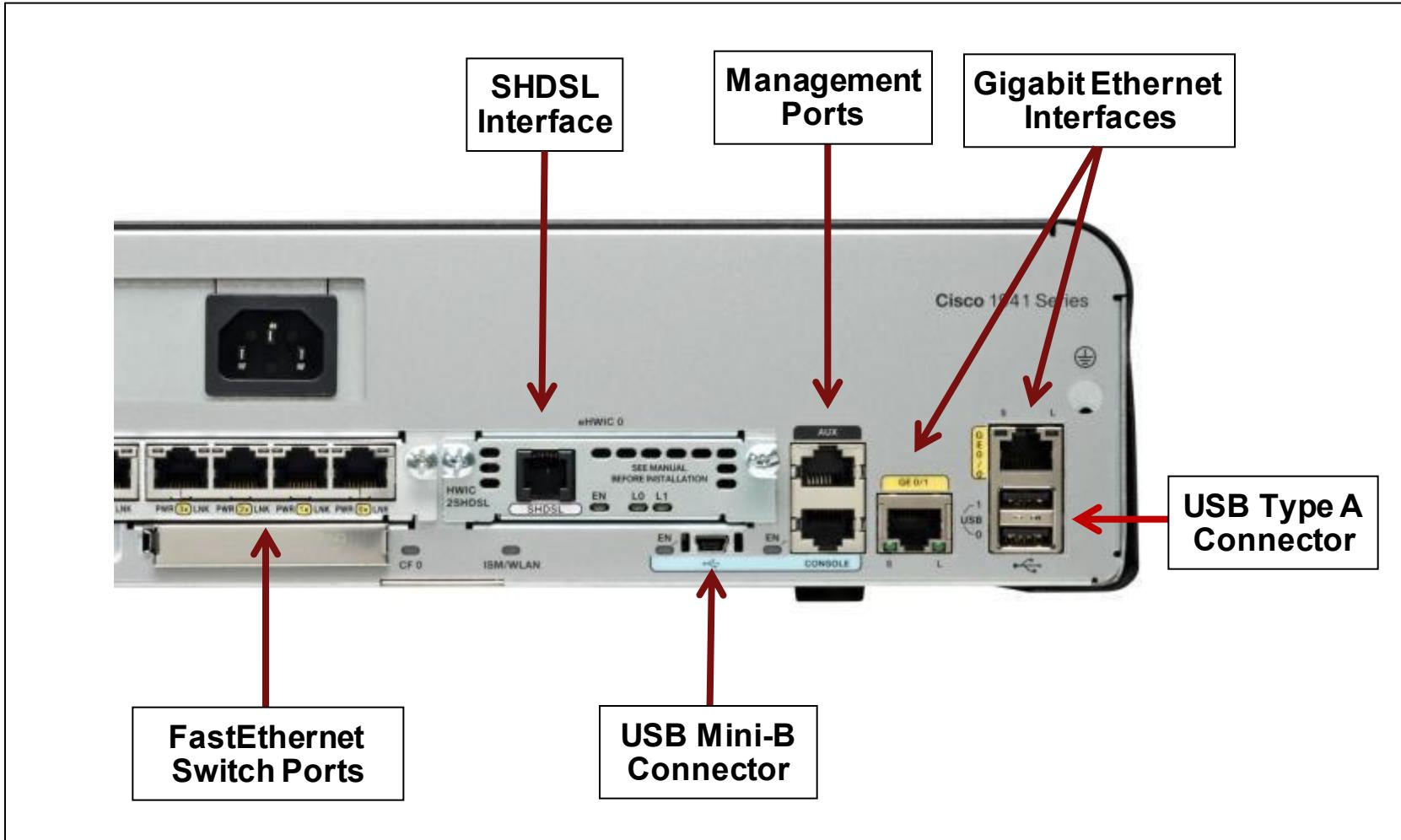
Many factors influence throughput, including:

- 1- The amount of traffic
- 2- The type of traffic
- 3- The latency created by the number of network devices encountered between source and destination





# Fundamental Principles of Layer 1 Types of Physical Media



The figure shows different types of interfaces and ports available on a 1941 router.

## 4.2 Network Media





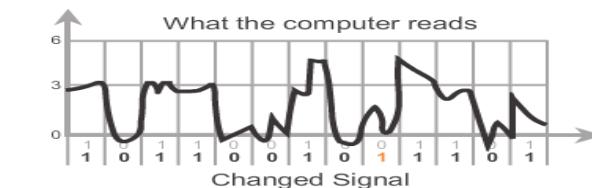
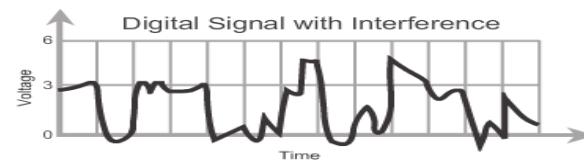
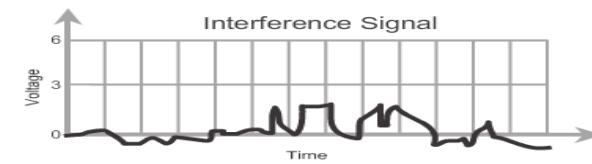
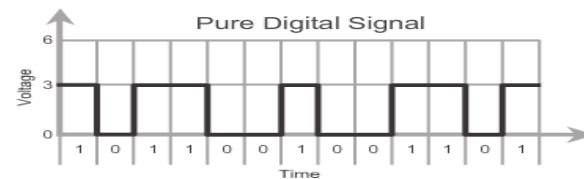
## Copper Cabling

# Characteristics of Copper Media

Networks use copper media because it is inexpensive, easy to install, and has low resistance to electrical current. However, copper media is limited by distance and signal interference.

Data is transmitted on copper cables as electrical pulses. A detector in the network interface of a destination device must receive a signal that can be successfully decoded to match the signal sent

the longer the signal travels, the more it deteriorates (فاسد). This is referred to as signal attenuation. For this reason, all copper media must follow strict distance limitations as specified by the guiding standards.





- The timing and voltage values of the electrical pulses are also susceptible to interference from two sources:
- **Electromagnetic interference (EMI) or radio frequency interference (RFI)** - EMI and RFI signals can distort and corrupt the data signals being carried by copper media. Potential sources of EMI and RFI include radio waves and electromagnetic devices, such as fluorescent lights or electric motors.
- **Crosstalk** - Crosstalk is a disturbance (اضطراب) caused by the electric or magnetic fields of a signal on one wire to the signal in an adjacent wire.
- In telephone circuits, crosstalk can result in hearing part of another voice conversation from an adjacent circuit. Specifically, when an electrical current flows through a wire, it creates a small, circular magnetic field around the wire, which can be picked up by an adjacent wire.
-



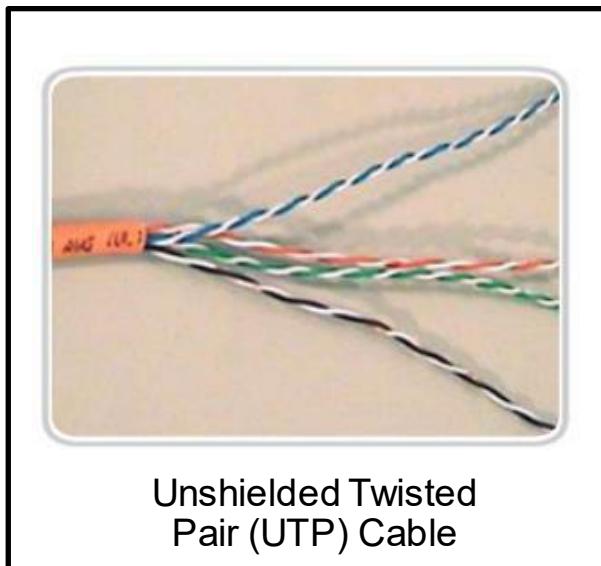
# Copper Media

- There are three main types of copper media used in networking:
- **Unshielded Twisted-Pair (UTP)**
- **Shielded Twisted-Pair (STP)**
- **Coaxial**

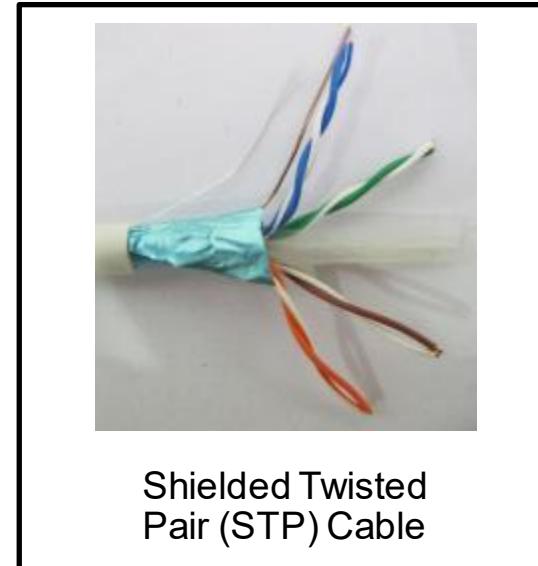


# Copper Cabling

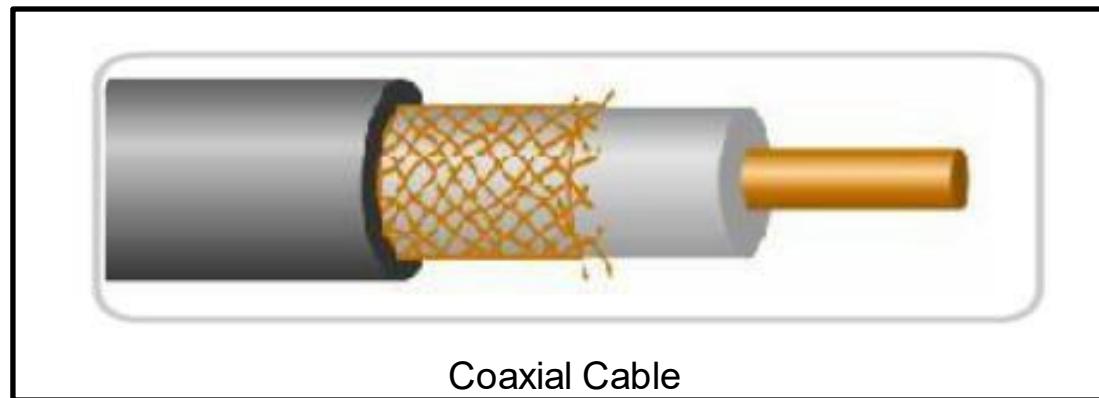
# Copper Media



Unshielded Twisted  
Pair (UTP) Cable



Shielded Twisted  
Pair (STP) Cable

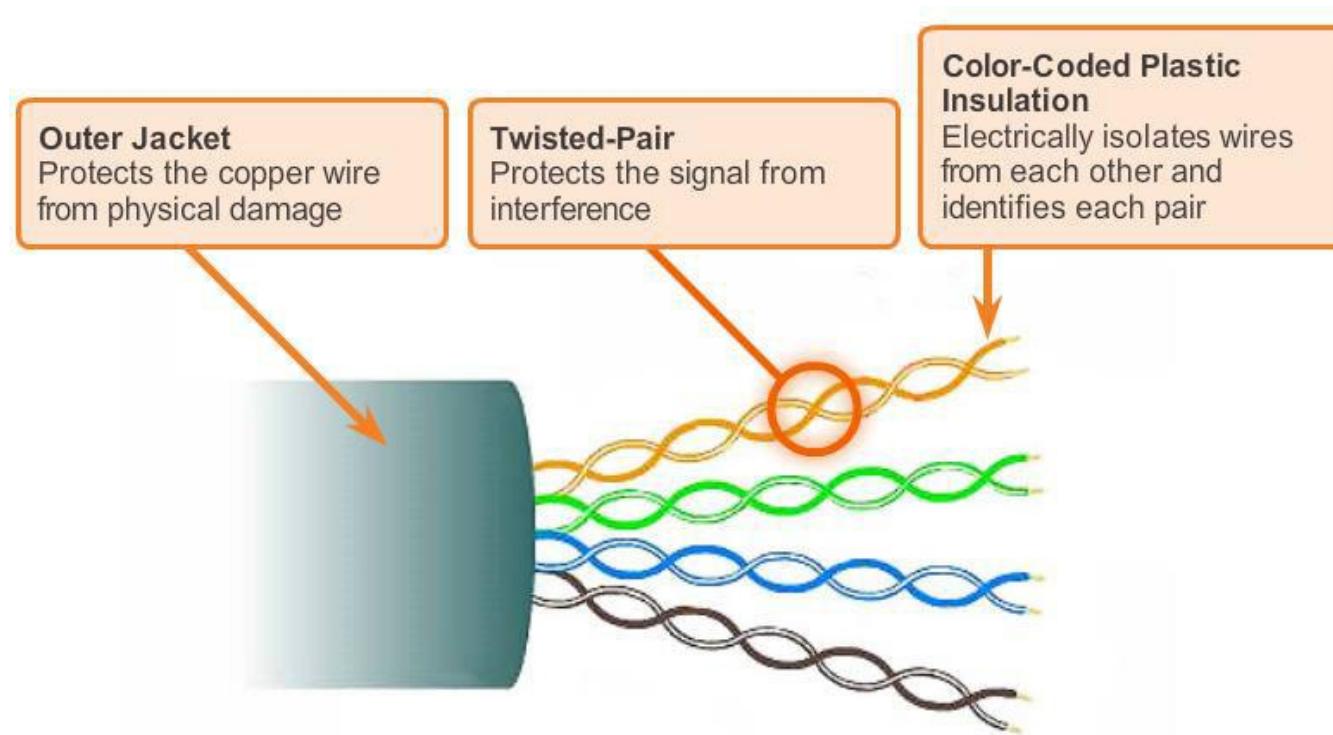


Coaxial Cable



# Copper Cabling UTP Cable

Unshielded twisted-pair (UTP) cabling is the most common networking media. UTP cabling, terminated with RJ-45 connectors, is used for interconnecting network hosts with intermediate networking devices, such as switches and routers.

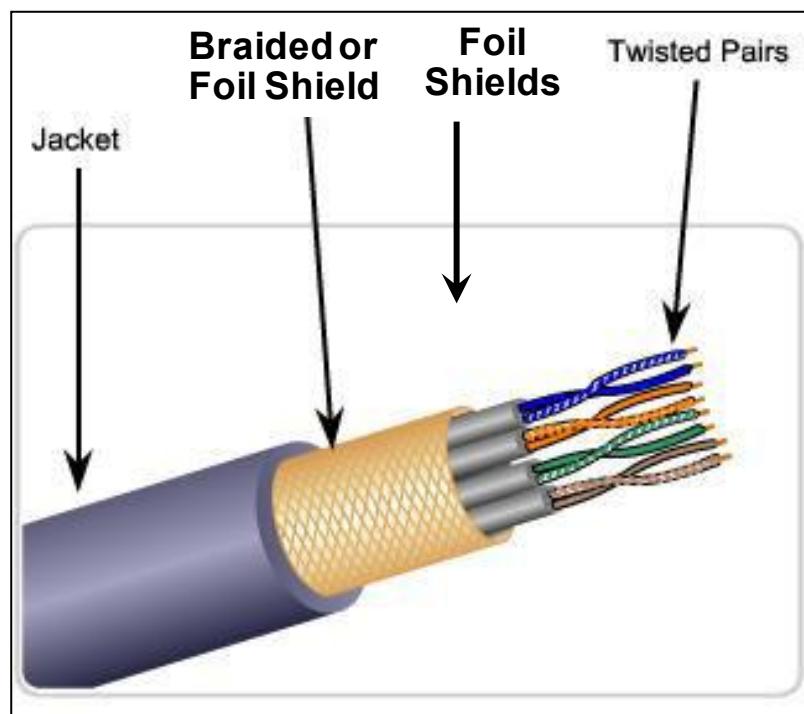




# Copper Cabling

## STP Cable

Shielded twisted-pair (STP) provides better noise protection than UTP cabling. However, compared to UTP cable, STP cable is significantly more expensive and difficult to install. Like UTP cable, STP uses an RJ-45 connector.

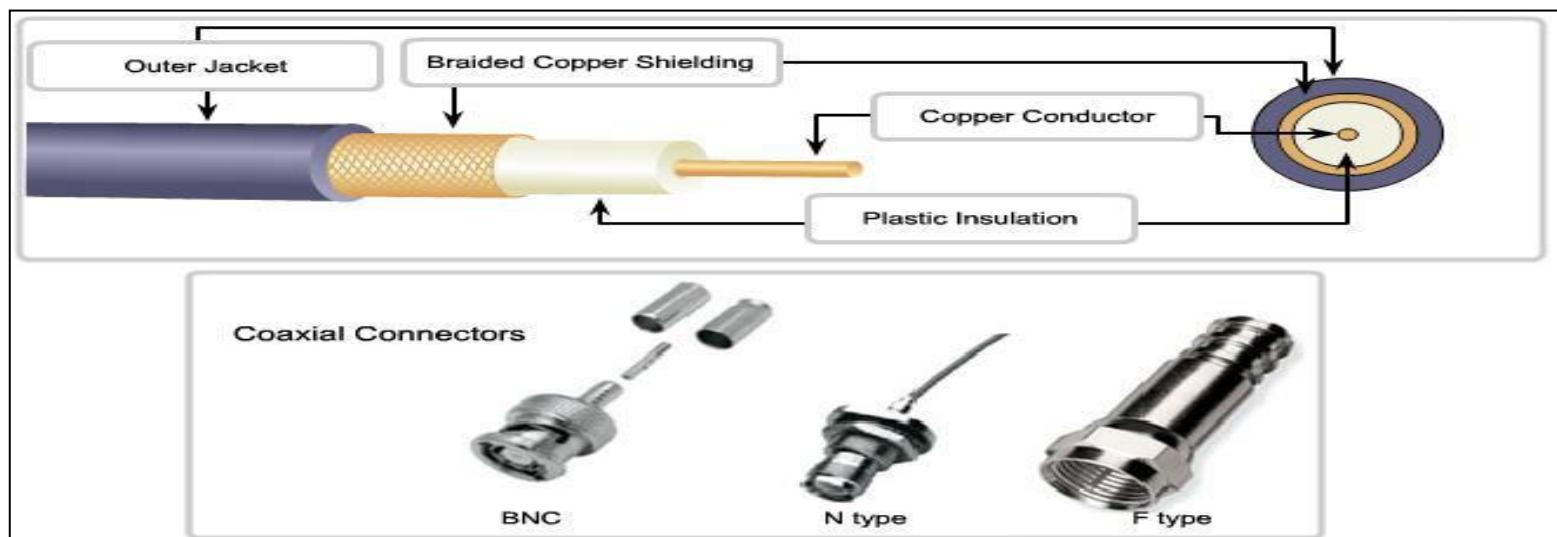




# Copper Cabling Coaxial Cable

Coaxial cable, or coax for short, gets its name from the fact that there are two conductors that share the same axis. As shown in the figure, coaxial cable consists of:

- \* A copper conductor used to transmit the electronic signals.
- \* A layer of flexible plastic insulation surrounding a copper conductor.
- \* The insulating material is surrounded in a woven copper braid, or metallic foil, that acts as the second wire in the circuit and as a shield for the inner conductor. This second layer, or shield, also reduces the amount of outside electromagnetic interference.
- \* The entire cable is covered with a cable jacket to prevent minor physical damage.





- Although UTP cable has essentially replaced coaxial cable in modern Ethernet installations, the coaxial cable design is used in:
- **Wireless installations:** Coaxial cables attach antennas to wireless devices. The coaxial cable carries radio frequency (RF) energy between the antennas and the radio equipment.
- **Cable Internet installations:** Cable service providers provide Internet connectivity to their customers by replacing portions of the coaxial cable and supporting amplification elements with fiber-optic cable. However, the wiring inside the customer's premises is still coax cable



# Copper Cabling Cooper 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.

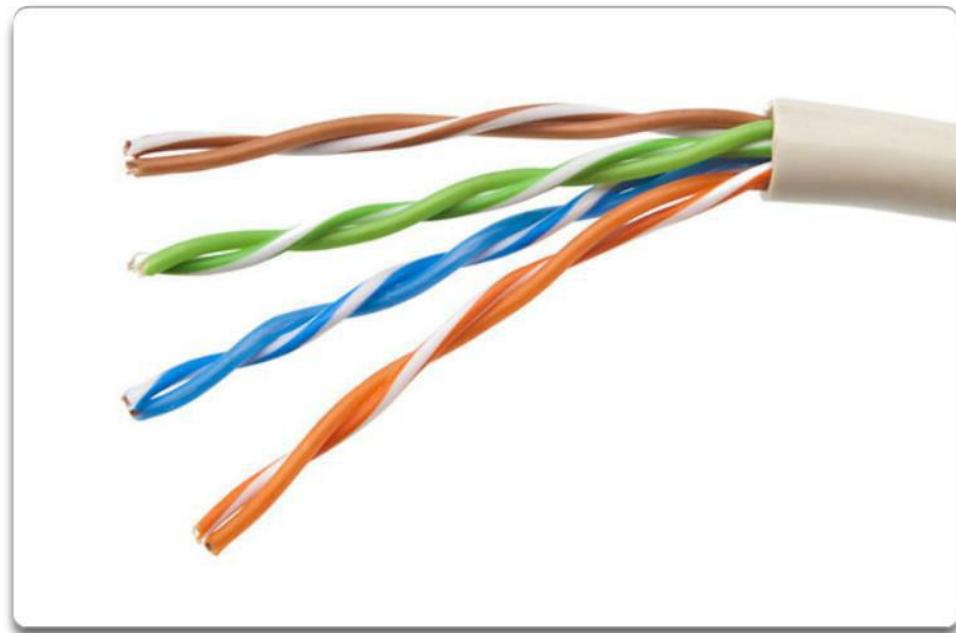


## UTP Cabling

# Properties of UTP Cabling

UTP cable does not use shielding to counter the effects of EMI and RFI. Instead, cable designers have discovered that they can limit the negative effect of crosstalk by:

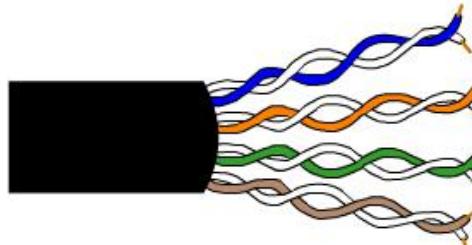
- Cancellation
- Varying the number of twists per wire pair



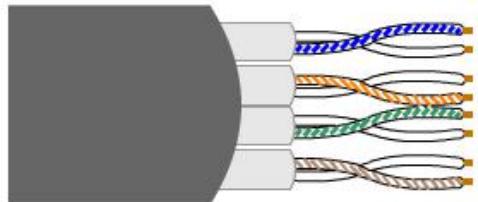


# UTP Cabling

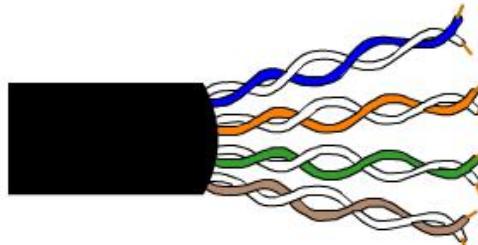
# UTP Cabling Standards



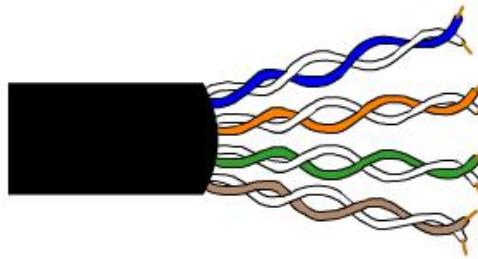
Category 3 Cable  
(UTP)



Category 7 Cable  
(ScTP)



Category 6 Cable  
(UTP)



Category 5 and 5e  
Cable (UTP)

Category 5 and 5e Cable  
(UTP)

- Used for Data transmission
- Cat 5 supports 100 Mbps and can support 1000 Mbps but it is not recommended
- Cat 5e supports 1000 Mbps



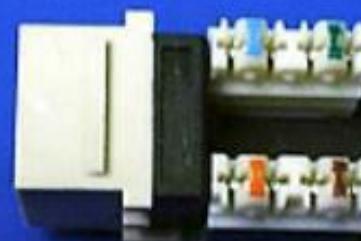
# UTP Cabling

## UTP Connectors

RJ-45 UTP Plugs



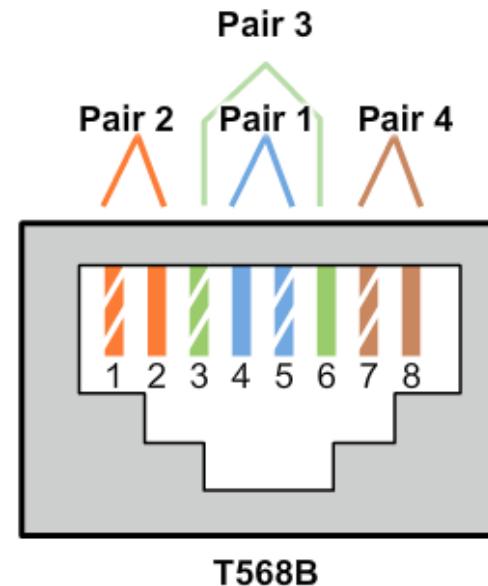
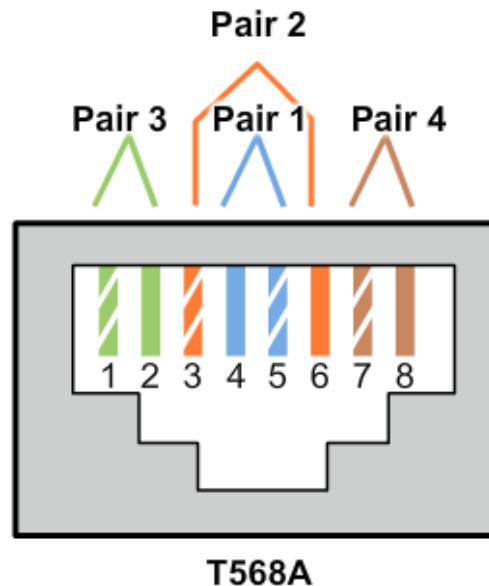
RJ-45 UTP Socket





# UTP Cabling

## Types of UTP Cable



Cable Type	Standard	Application
Ethernet Straight-through	Both ends T568A or both ends T568B	Connects a network host to a network device such as a switch or hub.
Ethernet Crossover	One end T568A, other end T568B	<ul style="list-style-type: none"><li>Connects two network hosts</li><li>Connects two network intermediary devices (switch to switch, or router to router)</li></ul>
Rollover	Cisco proprietary	Connects a workstation serial port to a router console port, using an adapter.



# UTP Cabling

## Testing UTP Cables

After installation, a UTP cable tester should be used to test for the following parameters:

- Wire map
- Cable length
- Signal loss due to attenuation
- Crosstalk





## Fiber Optic Cabling

# Properties of Fiber Optic Cabling

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

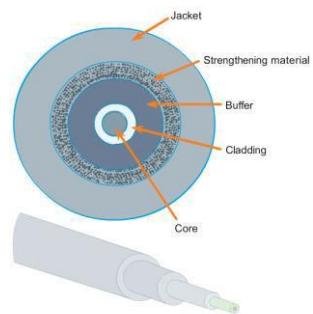
- **Enterprise Networks**  
Used for backbone cabling applications and interconnecting infrastructure devices.
- **Fiber-to-the-home (FTTH) and Access Networks**  
Used to provide always-on broadband services to homes and small businesses.
- **Long-Haul Networks**  
Used by service providers to connect countries and cities.
- **Submarine Networks**  
Used to provide reliable high-speed, high-capacity solutions capable of surviving in harsh environments up to transoceanic (عبر المحيط) (قاسية) undersea (تحت سطح البحر) distances.

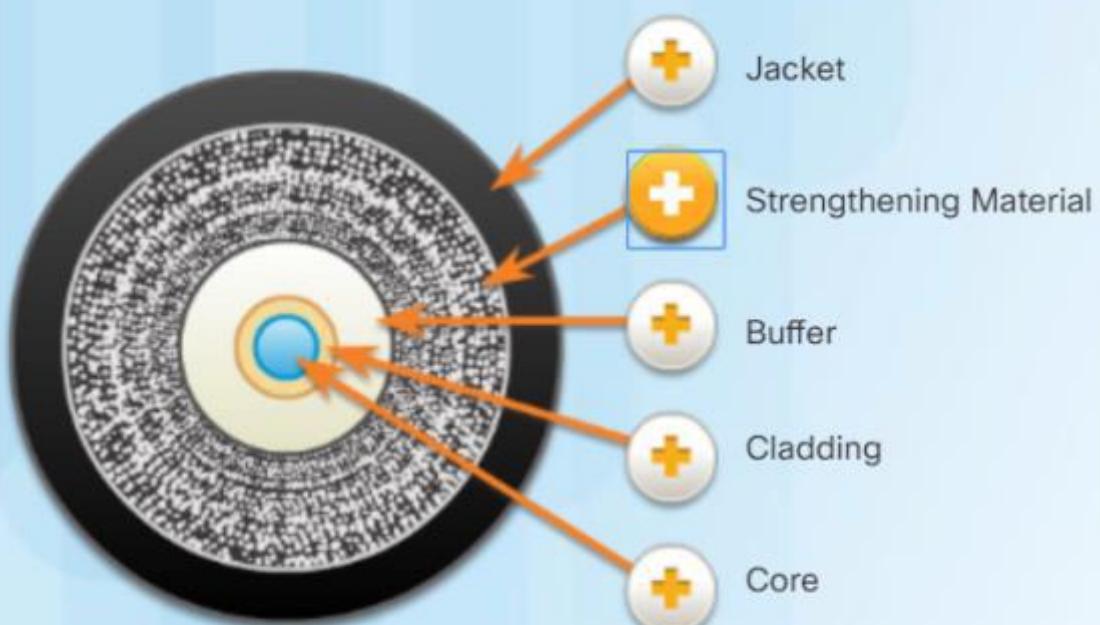




# Fiber Optic Cabling

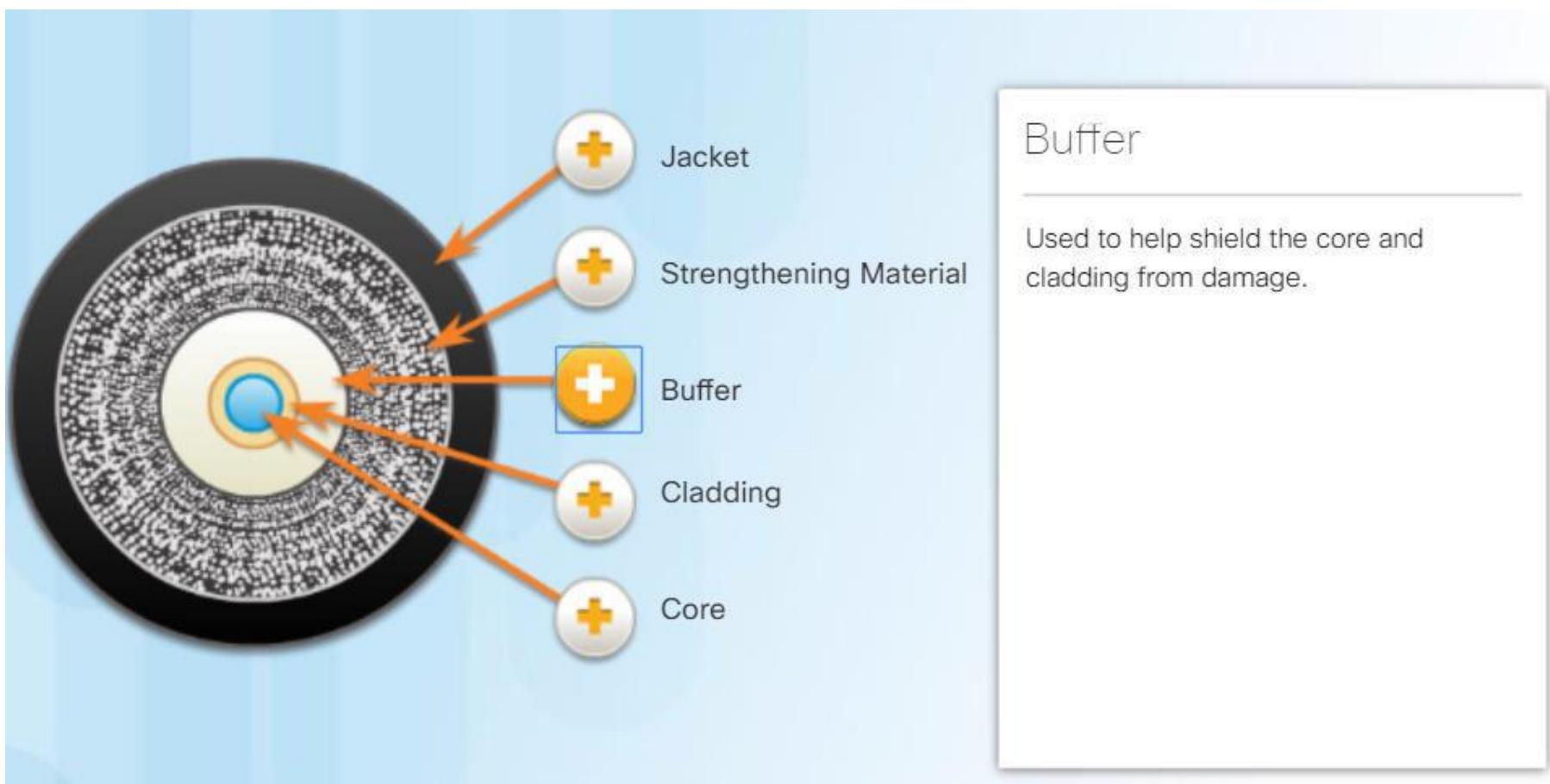
# Fiber Media Cable Design

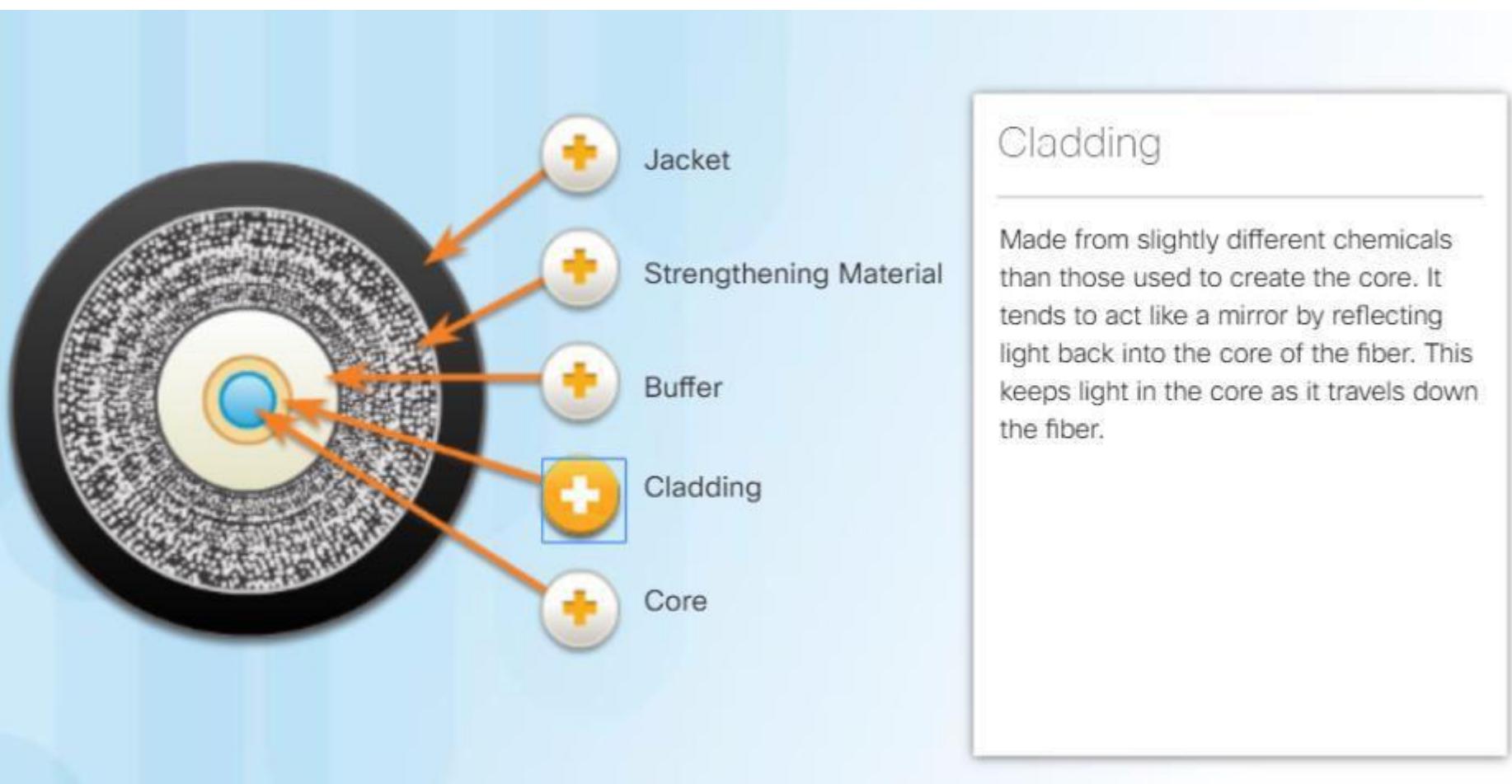




## Strengthening Material

Surrounds the buffer, prevents the fiber cable from being stretched when it is being pulled. The material used is often the same material used to produce bulletproof vests.







## Core

The core is actually the light transmission element at the center of the optical fiber. This core is typically silica or glass. Light pulses travel through the fiber core.



# Fiber Optic Cabling

## Types of Fiber Media

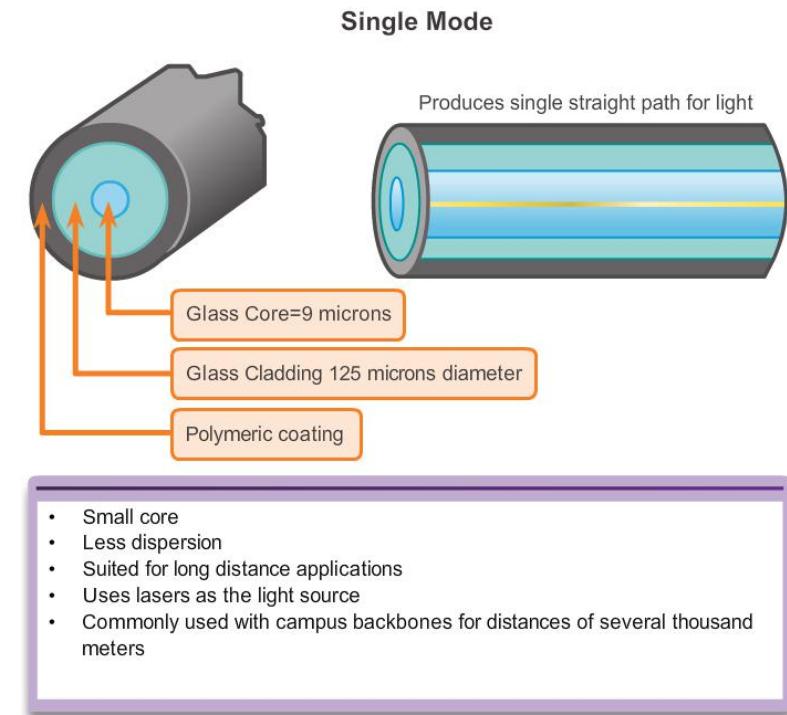
Light pulses representing the transmitted data as bits on the media are generated by either:

- 1- Lasers
- 2- Light emitting diodes (LEDs)

Fiber-optic cables are broadly classified into two types:

**1- Single-mode fiber (SMF):** Consists of a very small core and uses expensive laser technology to send a single ray of light, as shown in Figure.

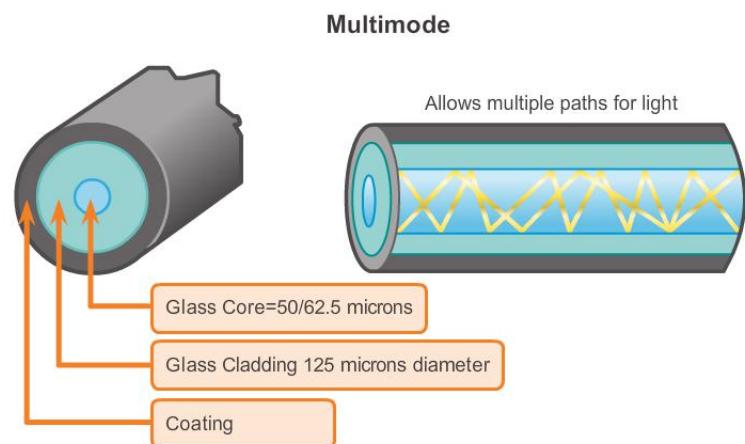
Popular in long-distance situations spanning hundreds of kilometers, such as those required in long haul telephony and cable TV applications.





## ■ 2- Multimode fiber (MMF):

Consists of a larger core and uses LED emitters to send light pulses. Specifically, light from an LED enters the multimode fiber at different angles, as shown in Figure 2. Popular in LANs because they can be powered by low-cost LEDs. It provides bandwidth up to 10 Gb/s over link lengths of up to 550 meters.



- Larger core than single mode cable
- Allows greater dispersion and therefore, loss of signal
- Suited for long distance applications, but shorter than single mode
- Uses LEDs as the light source
- Commonly used with LANs or distances of a couple hundred meters within a campus network



# Fiber Optic Cabling

# Network Fiber Connectors



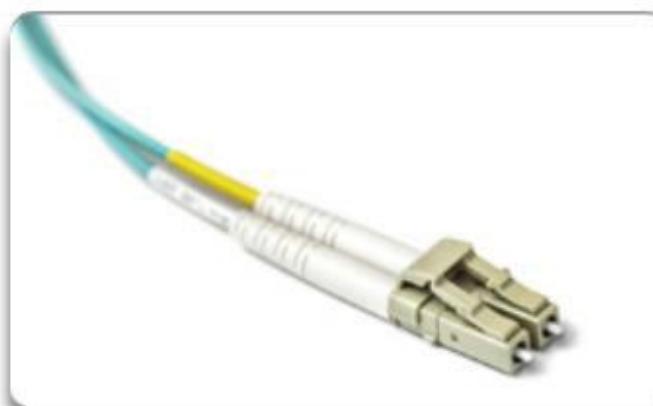
ST Connectors



SC Connectors



LC Connector



Duplex Multimode LC Connectors



# Fiber Optic Cabling

# Testing Fiber Cables

Three common types of fiber-optic termination and splicing errors are:

**Misalignment** (المحاذاة غير الصحيحة): The fiber-optic media are not precisely aligned to one another when joined.

**End gap**: The media does not completely touch at the splice or connection.

**End finish**: The media ends are not well polished (مصفول), or dirt is present at the termination.



Optical Time Domain Reflectometer (OTDR)



# Fiber Optic Cabling

## Fiber versus 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

# Properties of Wireless Media

Wireless does have some areas of concern including:

- Coverage area (تغطية)
- Interference (التشوش)
- Security





## Wireless Media

# Types of Wireless Media

	<ul style="list-style-type: none"><li>• IEEE 802.11 standards</li><li>• Commonly referred to as Wi-Fi.</li><li>• Uses CSMA/CA</li><li>• Variations include:<ul style="list-style-type: none"><li>• 802.11a: 54 Mbps, 5 GHz</li><li>• 802.11b: 11 Mbps, 2.4 GHz</li><li>• 802.11g: 54 Mbps, 2.4 GHz</li><li>• 802.11n: 600 Mbps, 2.4 and 5 GHz</li><li>• 802.11ac: 1 Gbps, 5 GHz</li><li>• 802.11ad: 7 Gbps, 2.4 GHz, 5 GHz, and 60 GHz</li></ul></li></ul>
	<ul style="list-style-type: none"><li>• IEEE 802.15 standard</li><li>• Supports speeds up to 3 Mb/s</li><li>• Provides device pairing over distances from 1 to 100 meters.</li></ul>
	<ul style="list-style-type: none"><li>• IEEE 802.16 standard</li><li>• Provides speeds up to 1 Gbps</li><li>• Uses a point-to-multipoint topology to provide wireless broadband access.</li></ul>



## Wireless Media

# Wireless LAN

- Wireless LAN requires the following network devices:
- **Wireless Access Point (AP)**: Concentrates the wireless signals from users and connects to the existing copper-based network infrastructure, such as Ethernet. Home and small business wireless routers integrate the functions of a router, switch, and access point into one device.
- **Wireless NIC adapters**: Provide wireless communication capability to each network host.



Cisco Linksys EA6500 802.11ac Wireless Router



# Wireless Media

# 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

## 4.3 Data Link Layer Protocols



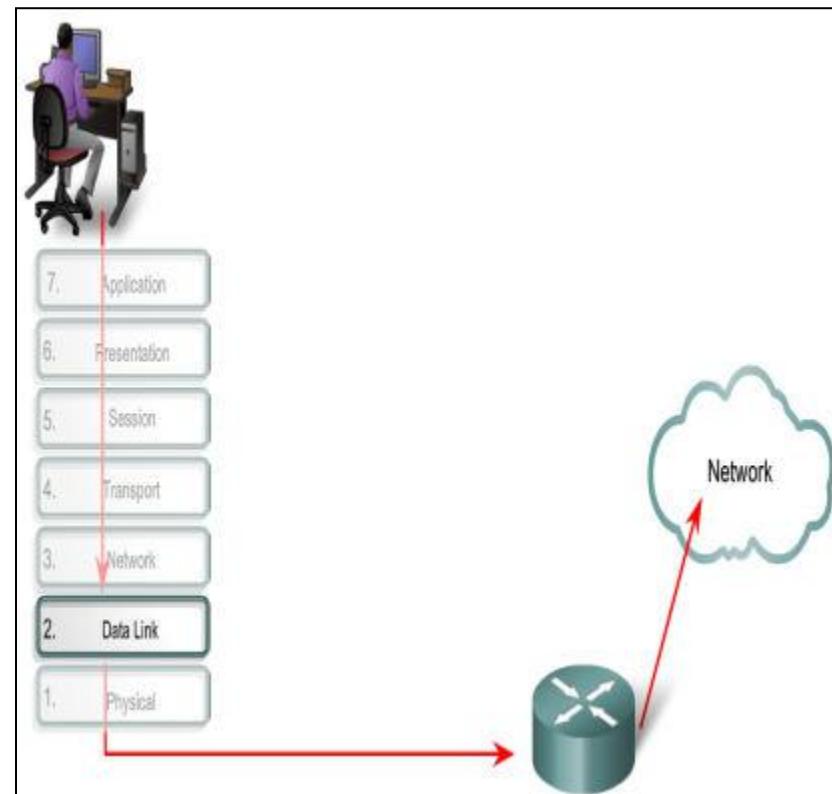


# Purpose of the Data Link Layer

# The Data Link Layer

The data link layer of the OSI model (Layer 2), as shown in Figure, is **responsible for**:

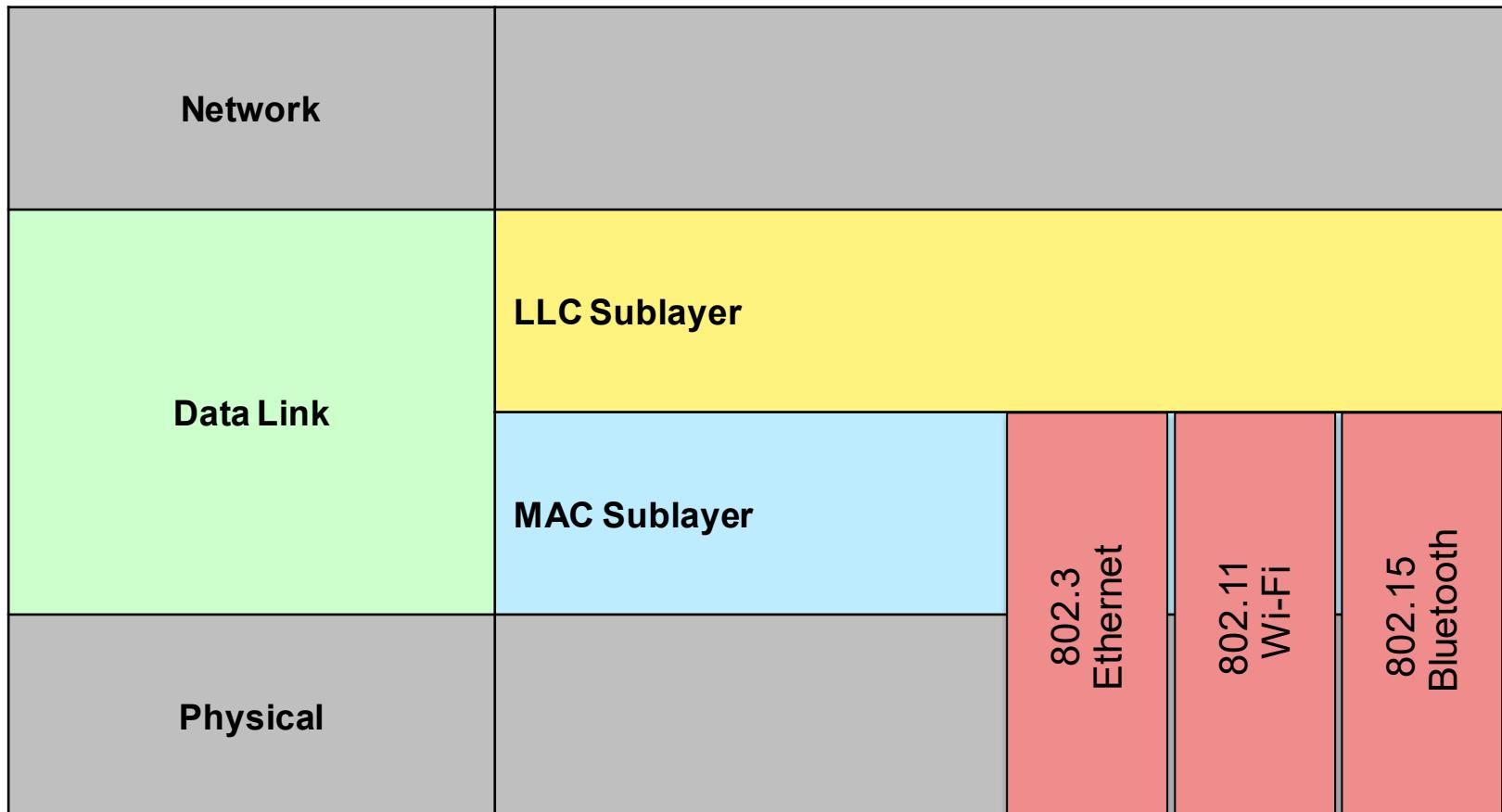
- Allowing the upper layers to access the media
- Accepting Layer 3 packets and packaging them into frames
- Preparing network data for the physical network
- Controlling how data is placed and received on the media
- Exchanging frames between nodes over a physical network media, such as UTP or fiber-optic
- Receiving and directing packets to an upper layer protocol
- Performing error detection





# Purpose of the Data Link Layer

# Data Link Sublayers





- The data link layer is divided into two sublayers:
- **Logical Link Control (LLC)** - This upper sublayer communicates with the network layer. It places information in the frame that identifies which network layer protocol is being used for the frame. This information allows multiple Layer 3 protocols, such as IPv4 and IPv6, to utilize the same network interface and media.
- **Media Access Control (MAC)** - This lower sublayer defines the media access processes performed by the hardware. It provides data link layer addressing and access to various network technologies.



# Purpose of the Data Link Layer Media Access Control

## The Data Link Layer

Data link layer protocols govern how to format a frame for use on different media.

Different protocols may be in use for different media.



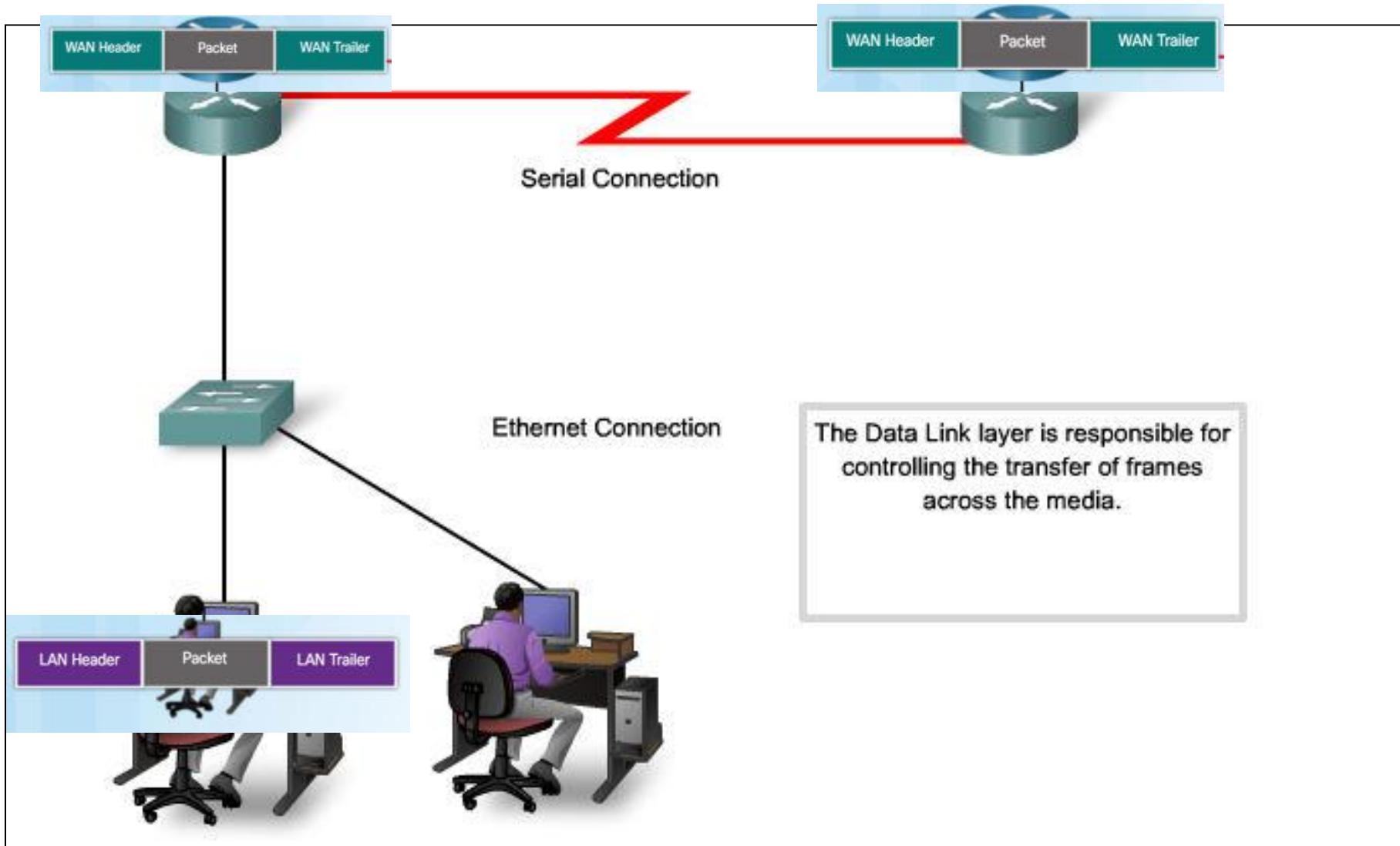
At each hop along the path, an intermediary device accepts frames from one medium, decapsulates the frame and then forwards the packets in a new frame. The headers of each frame are formatted for the specific medium that it will cross.





## Purpose of the Data Link Layer

# Providing Access to Media

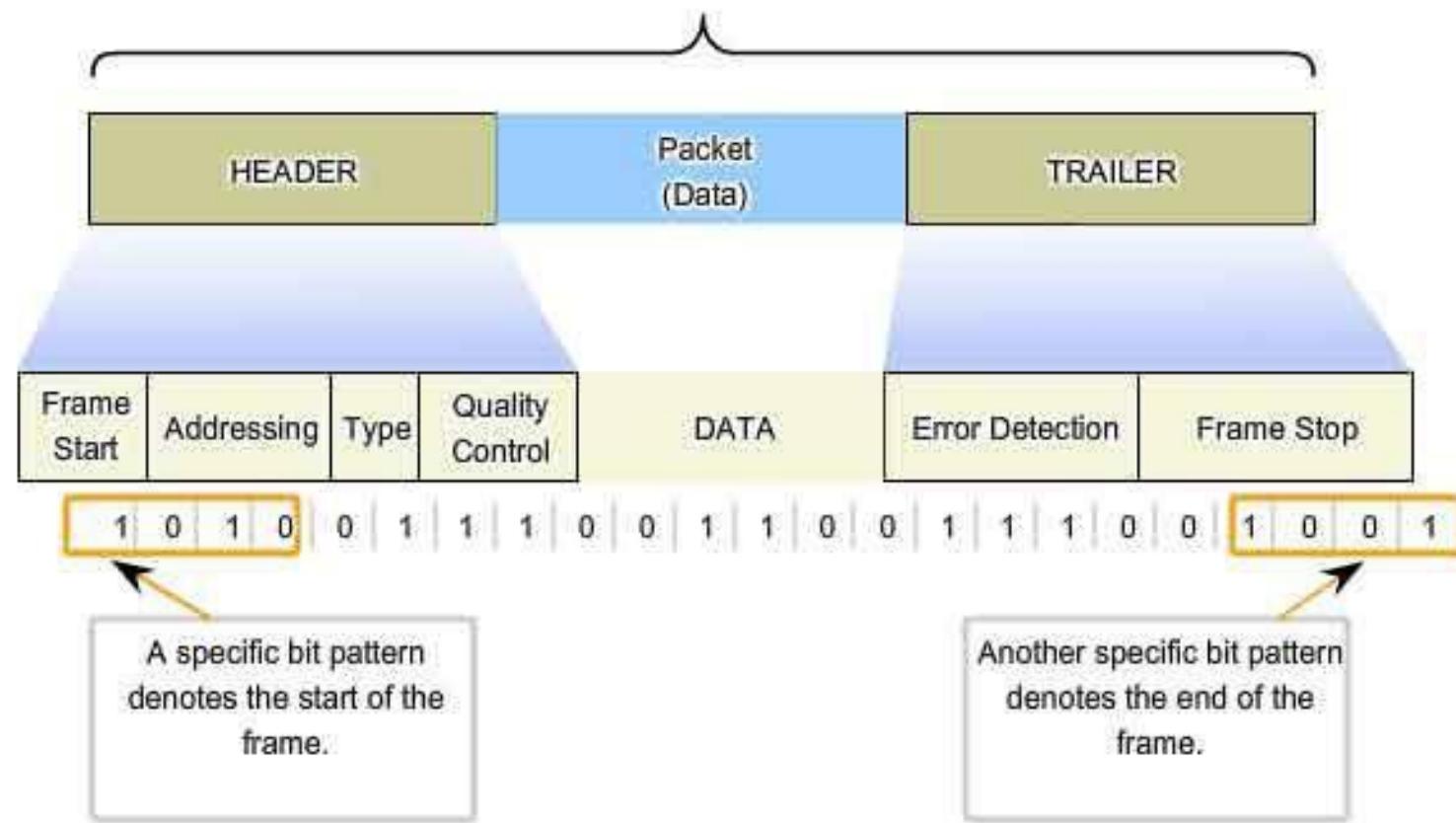




## Data Link Layer

# Formatting Data for Transmission

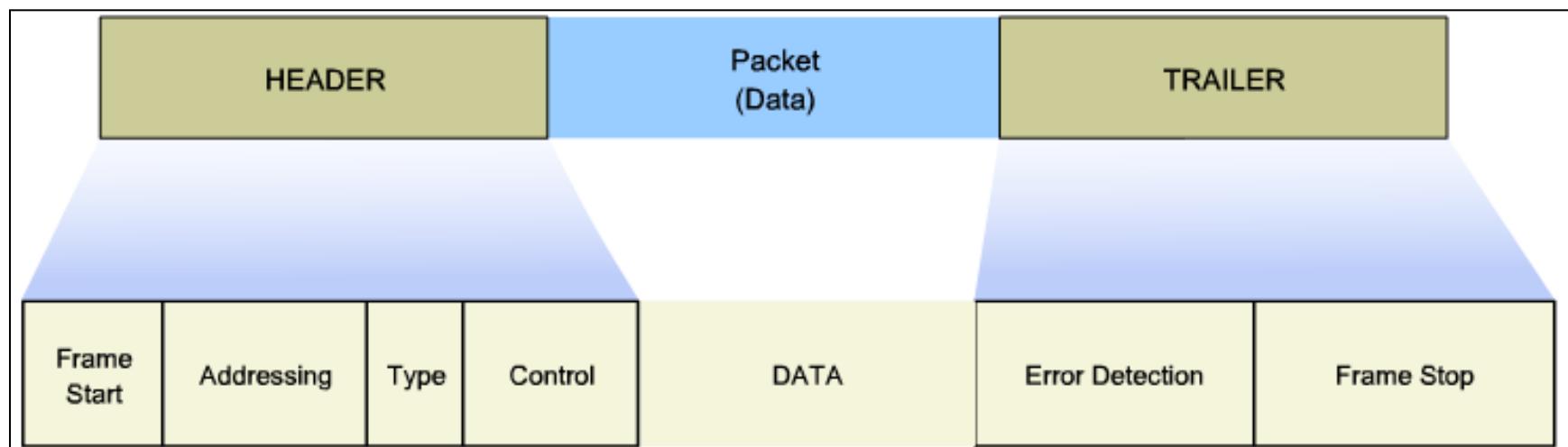
Formatting Data for Transmission





# Layer 2 Frame Structure

## Creating a Frame





## Layer 2 Standards

# Data Link Layer Standards

Standard organization	Networking Standards
IEEE	<ul style="list-style-type: none"><li>• 802.2: Logical Link Control (LLC)</li><li>• 802.3: Ethernet</li><li>• 802.4: Token bus</li><li>• 802.5: Token passing</li><li>• 802.11: Wireless LAN (WLAN) &amp; Mesh (Wi-Fi certification)</li><li>• 802.15: Bluetooth</li><li>• 802.16: WiMax</li></ul>
ITU-T	<ul style="list-style-type: none"><li>• G.992: ADSL</li><li>• G.8100 - G.8199: MPLS over Transport aspects</li><li>• Q.921: ISDN</li><li>• Q.922: Frame Relay</li></ul>
ISO	<ul style="list-style-type: none"><li>• HDLC (High Level Data Link Control)</li><li>• ISO 9314: FDDI Media Access Control (MAC)</li></ul>
ANSI	<ul style="list-style-type: none"><li>• X3T9.5 and X3T12: Fiber Distributed Data Interface (FDDI)</li></ul>



## Topologies

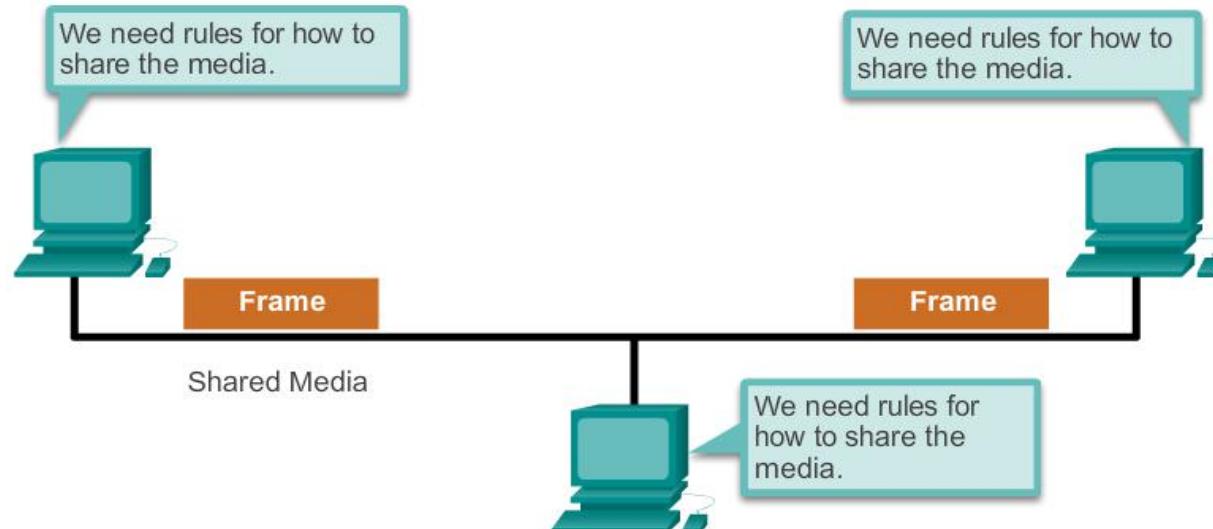
# Controlling Access to the Media

The actual media access control method used depends on:

**Topology** - How the connection between the nodes appears to the data link layer.

**Media sharing** - How the nodes share the media. The media sharing can be point-to-point, such as in WAN connections, or shared such as in LAN networks.

### Sharing the Media



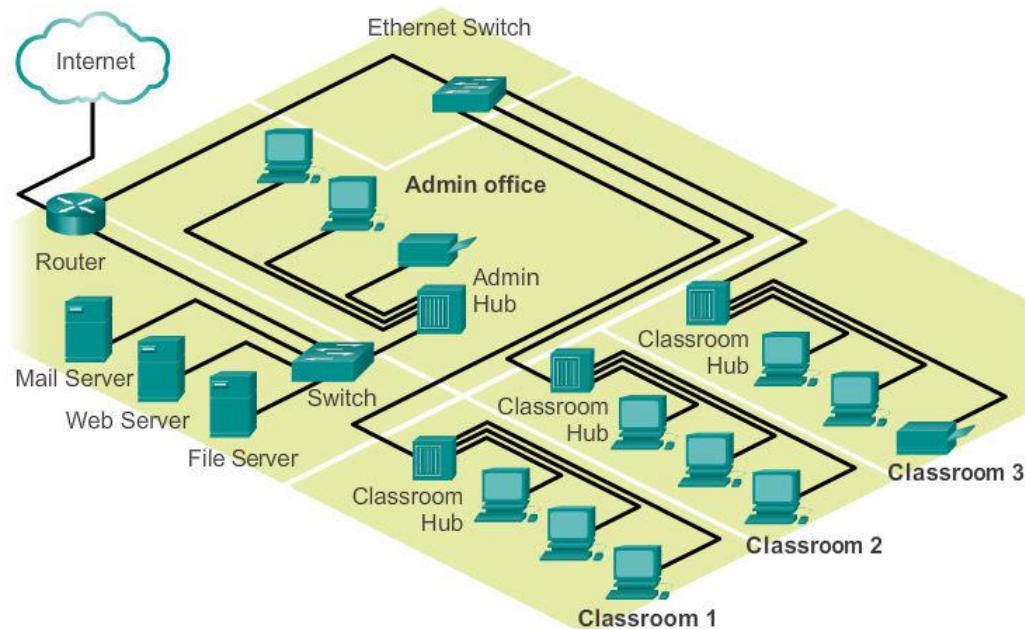


## Topologies

# Physical and Logical Topologies

**Physical topology** - Refers to the physical connections and identifies how end devices and infrastructure devices such as routers, switches, and wireless access points are interconnected. Physical topologies are usually point-to-point or star.

Physical Topology

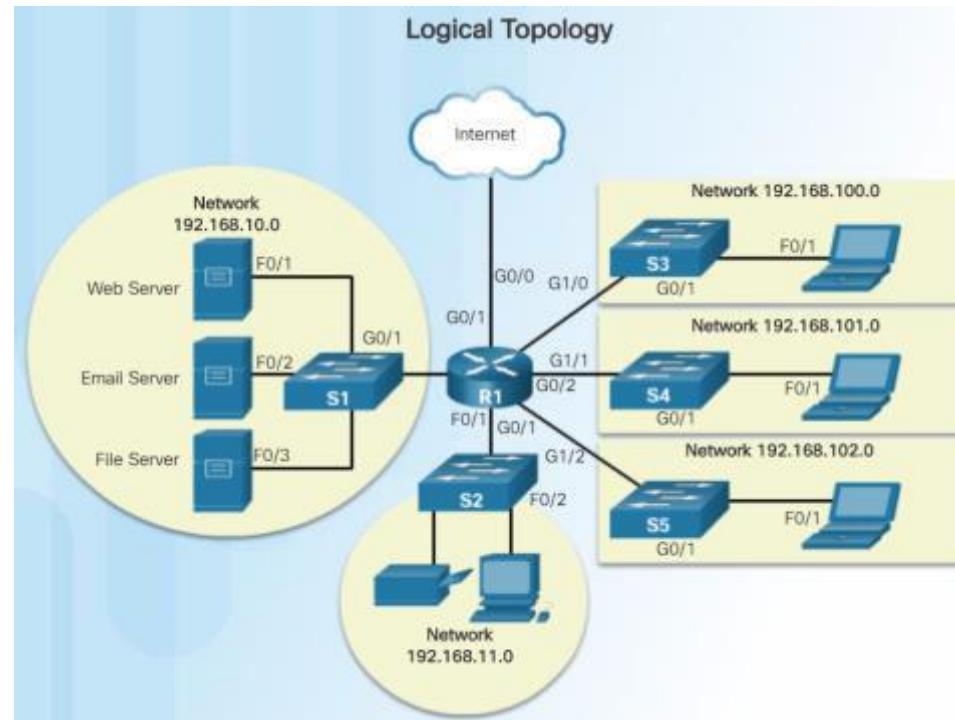




## Topologies

# Physical and Logical Topologies (cont.)

**Logical topology** - Refers to the way a network transfers frames from one node to the next. This arrangement consists of virtual connections between the nodes of a network. These logical signal paths are defined by data link layer protocols. The logical topology of point-to-point links is relatively simple while shared media offers different access control methods.



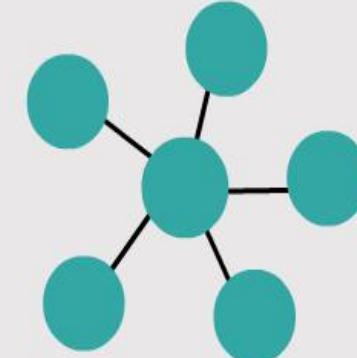


## WAN Topologies

# Common Physical WAN Topologies



Point-to-point topology

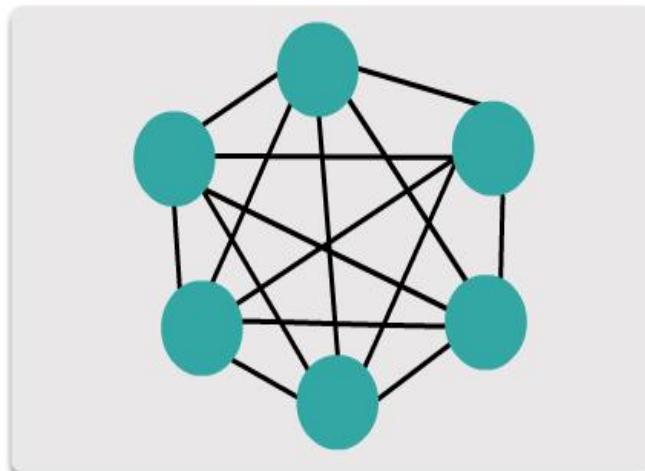


Hub and spoke topology

**Point-to-Point** - This is the simplest topology that consists of a permanent link between two endpoints. For this reason, this is a very popular WAN topology.

**Hub and Spoke** - A WAN version of the star topology in which a central site interconnects branch sites using point-to-point links.

**Mesh** - This topology provides high availability, but requires that every end system be interconnected to every other system. Therefore, the administrative and physical costs can be significant. Each link is essentially a point-to-point link to the other node.

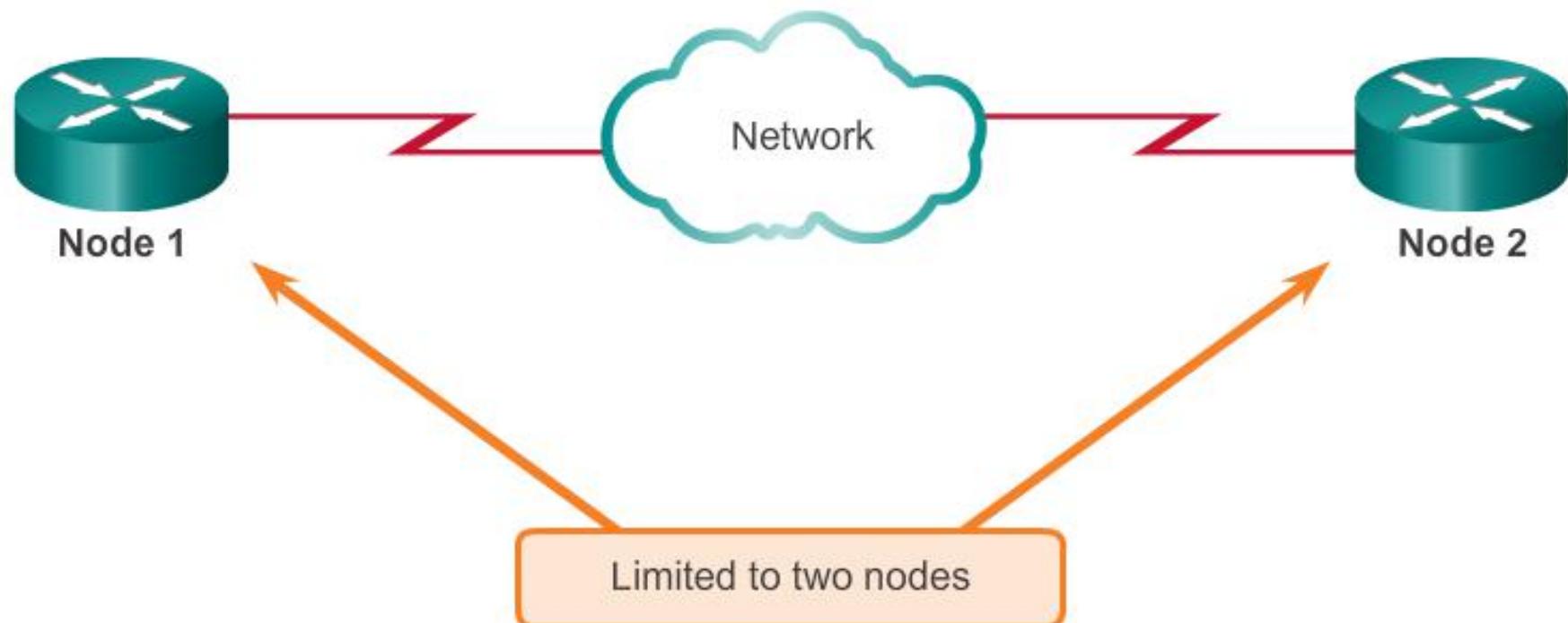


Full mesh topology



## WAN Topologies

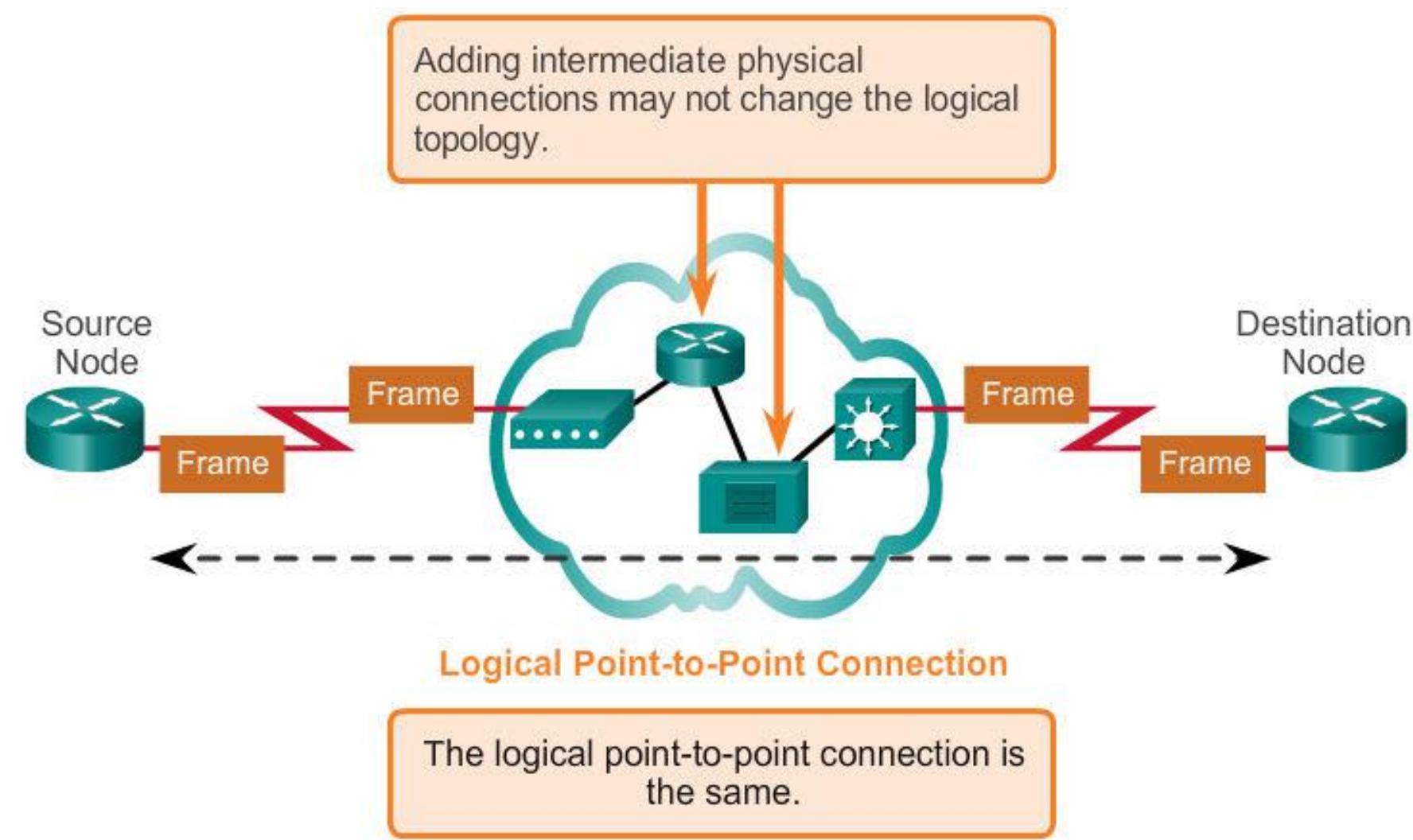
# Physical Point-to-Point Topology





## WAN Topologies

# Logical Point-to-Point Topology





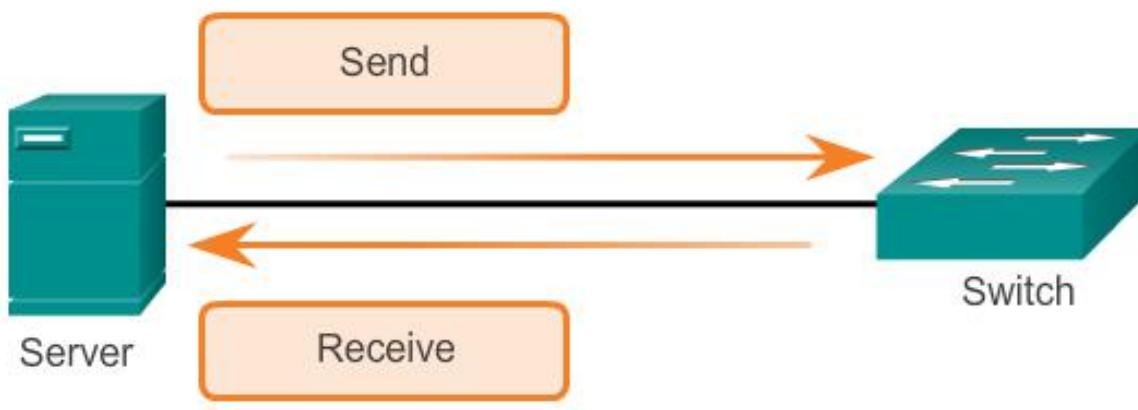
# WAN Topologies

## Half- and Full-Duplex

### Half-Duplex



### Full-Duplex





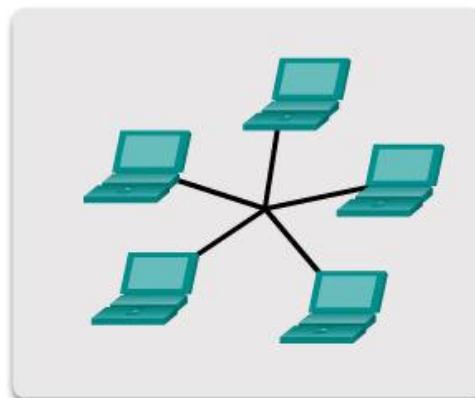
- **Half-duplex communication** - Both devices can transmit and receive on the media but cannot do so simultaneously. The half-duplex mode is used in legacy bus topologies and with Ethernet hubs. WLANs also operate in half-duplex. Half-duplex allows only one device to send or receive at a time on the shared medium and is used with contention-based access methods.
- **Full-duplex communication** - Both devices can transmit and receive on the media at the same time. The data link layer assumes that the media is available for transmission for both nodes at any time. Ethernet switches operate in full-duplex mode by default, but can operate in half-duplex if connecting to a device such as an Ethernet hub



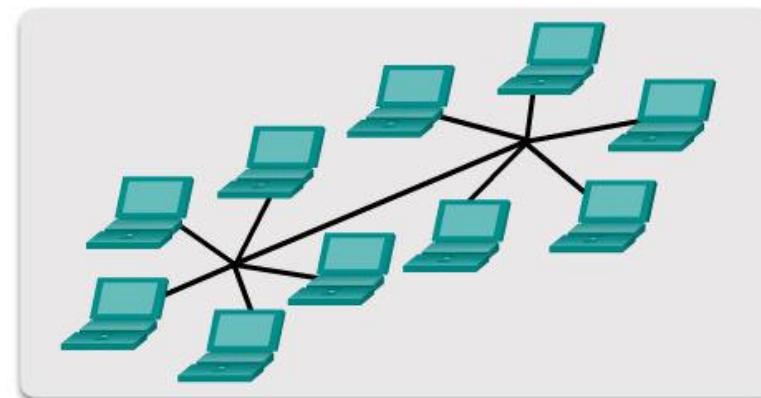
## LAN Topologies

# Physical LAN Topologies

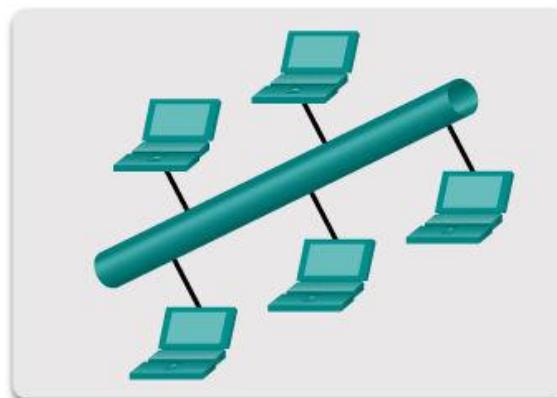
## Physical Topologies



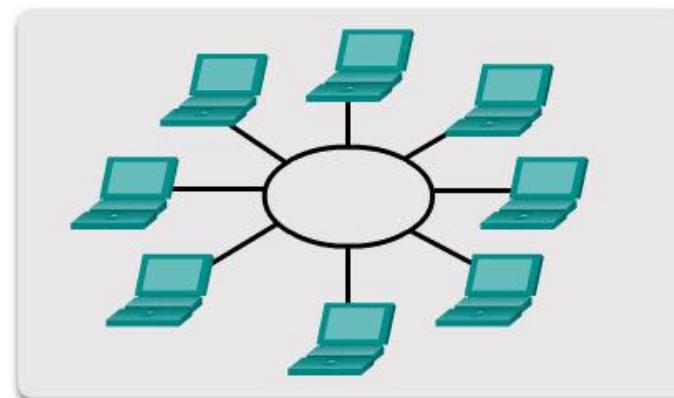
## Star topology



## Extended star topology



Bus topology



## Ring topology



## LAN Topologies

## Logical Topology for Shared Media

## Contention-Based Access

I try to send when I am ready.



FRAME

I try to send when I am ready.



Shared Media

I try to send when I am ready.



FRAME

## Controlled Access

I have a packet to send, but it is not my turn. I'll wait.



FRAME

I have nothing to send.



Shared Media

It is my turn to send. I will send now.



FRAME

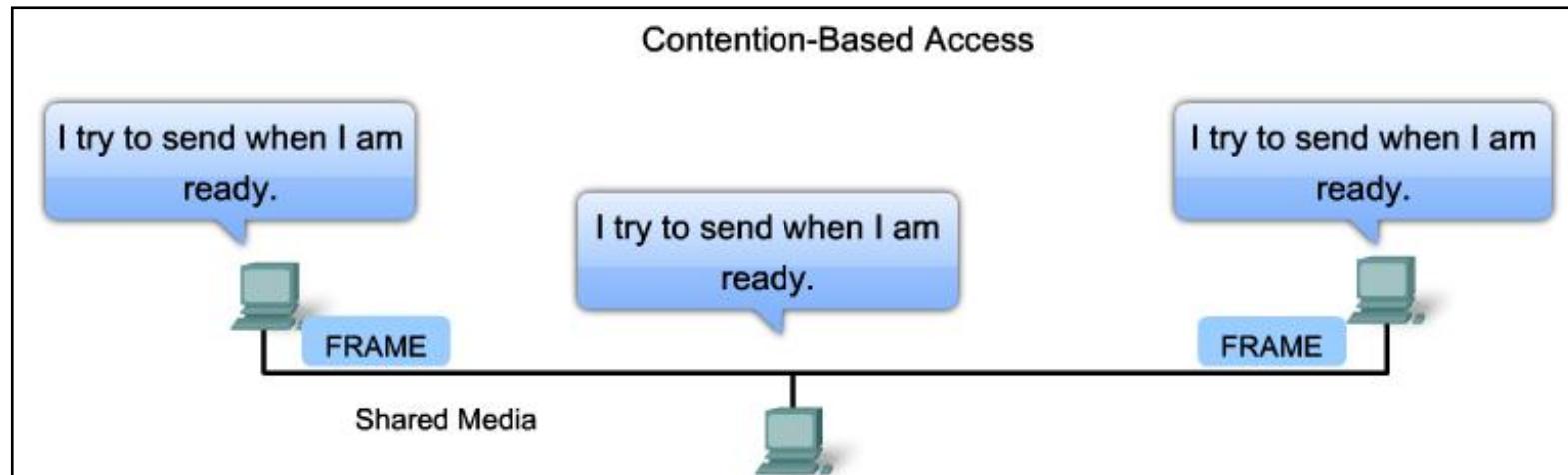


## LAN Topologies

# Contention-Based Access

There are two basic access control methods for shared media:

**1- Contention-based access** - All nodes operating in half-duplex compete for the use of the medium, but only one device can send at a time.



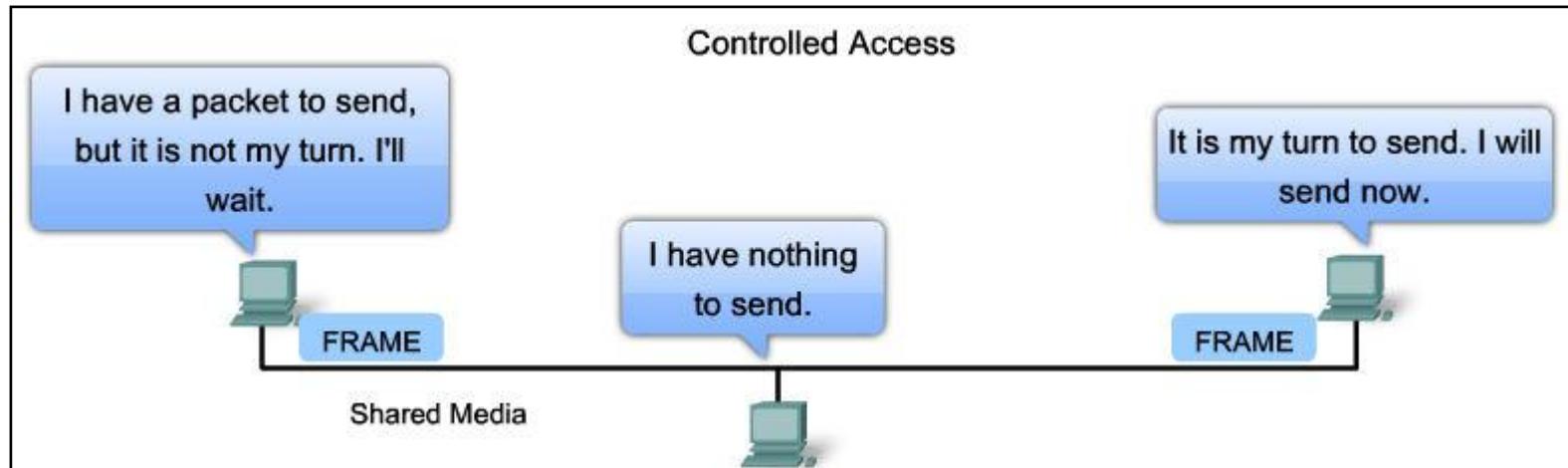
Characteristics	Contention-Based Technologies
<ul style="list-style-type: none"><li>• Stations can transmit at any time</li><li>• Collision exist</li><li>• There are mechanisms to resolve contention for the media</li></ul>	<ul style="list-style-type: none"><li>• CSMA/CD for 802.3 Ethernet networks</li><li>• CSMA/CA for 802.11 wireless networks</li></ul>



# LAN Topologies

## Controlled Access

**2- Controlled access** - Each node has its own time to use the medium. These deterministic types of networks are inefficient because a device must wait its turn to access the medium. Legacy Token Ring LANs are an example of this type of access control.



Characteristics	Controlled Access Technologies
<ul style="list-style-type: none"><li>• Only one station can transmit at a time</li><li>• Devices wanting to transmit must wait their turn</li><li>• No collisions</li><li>• May use a token passing method</li></ul>	<ul style="list-style-type: none"><li>• Token Ring (IEEE 802.5)</li><li>• FDDI</li></ul>



## LAN Topologies

## Multi-Access Topology

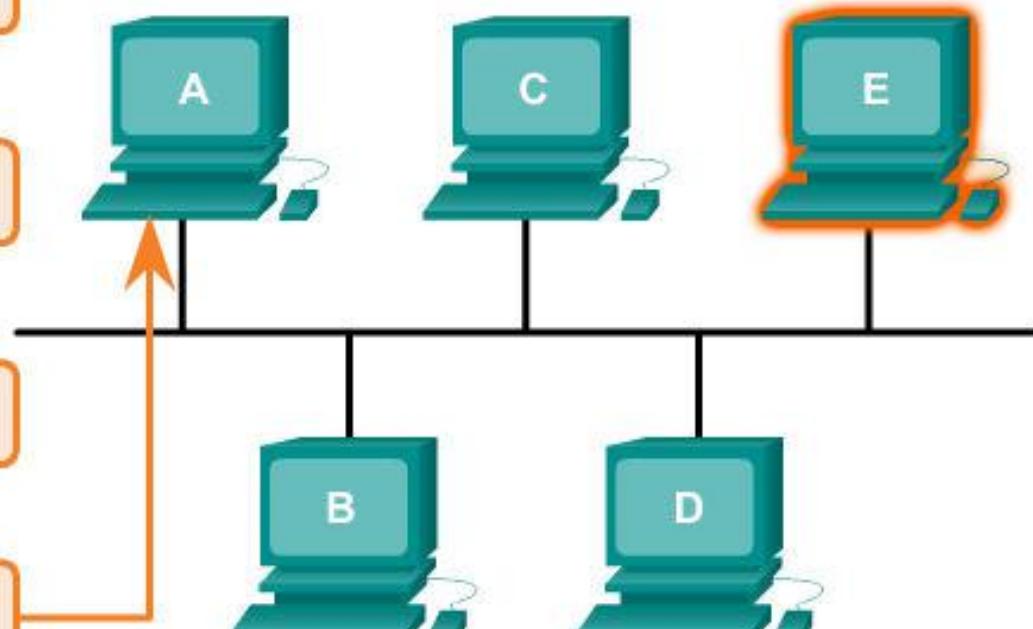
## Logical Multi-Access Topology

I need to transmit to E.

I check for other transmissions.

No other transmissions are detected.

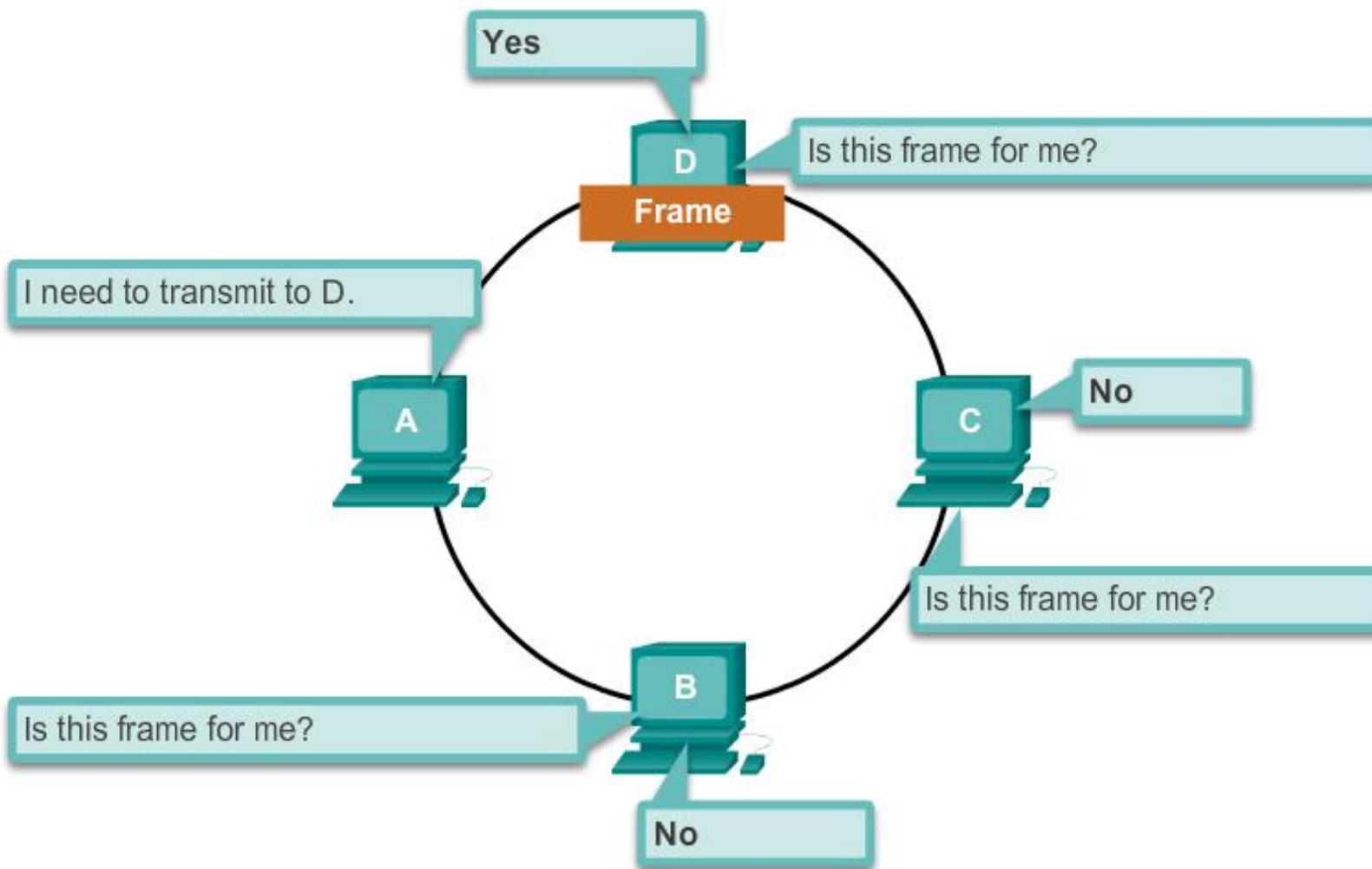
Transmitting...





# LAN Topologies

## Ring Topology





# Data Link Frame

## The Frame

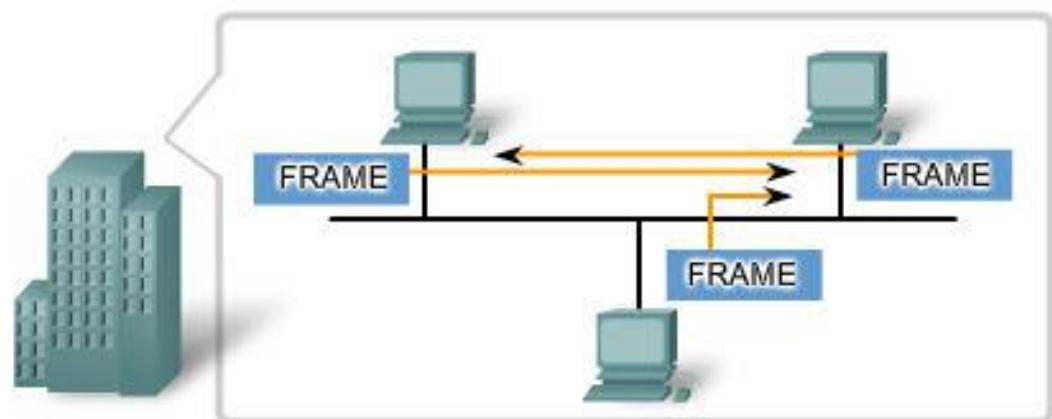
In a **fragile environment**, more controls are needed to ensure delivery. The header and trailer fields are larger as more control information is needed.

Greater effort needed to ensure delivery = higher overhead = slower transmission rates



In a **protected environment**, we can count on the frame arriving at its destination. Fewer controls are needed, resulting in smaller fields and smaller frames.

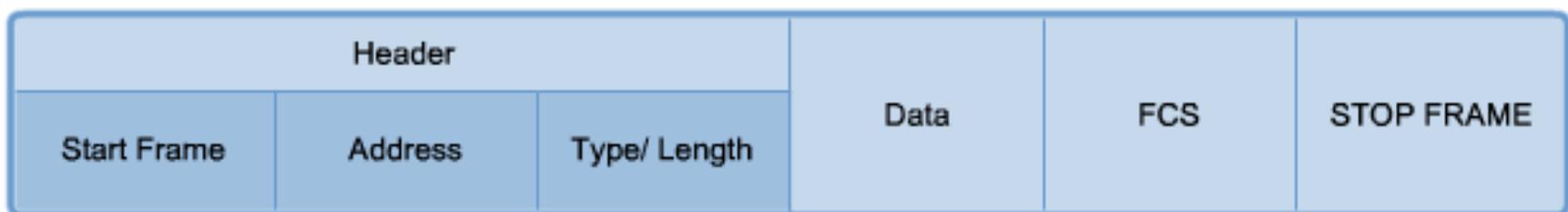
Less effort needed to ensure delivery = lower overhead = faster transmission rates





# Data Link Frame

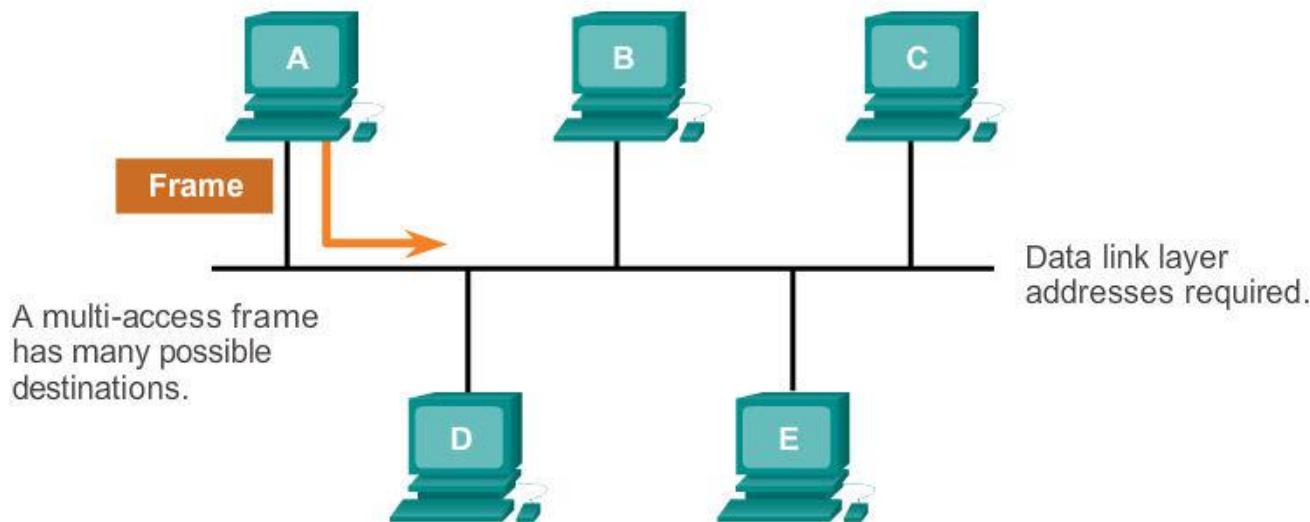
## The Header



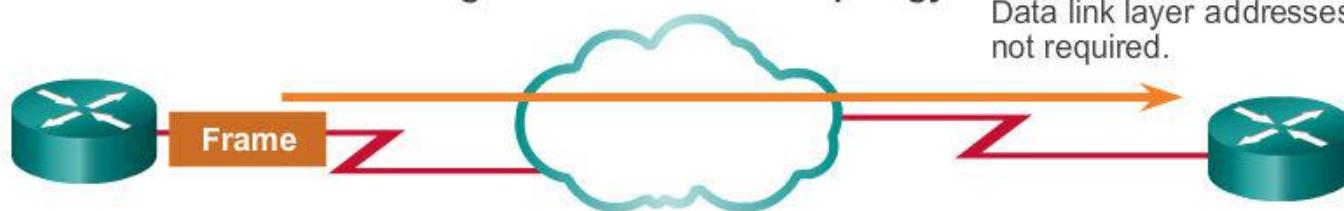


# Data Link Frame Layer 2 Address

Logical Multi-Access Topology



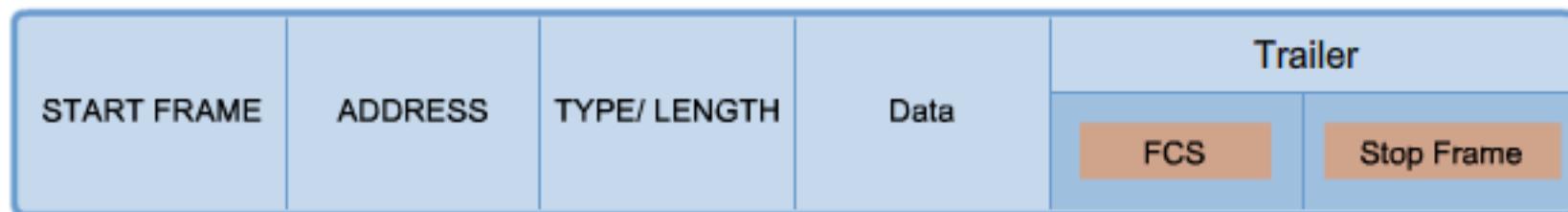
Logical Point-to-Point Topology



A point-to-point frame has only 1 possible destination.



# Data Link Frame The 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.

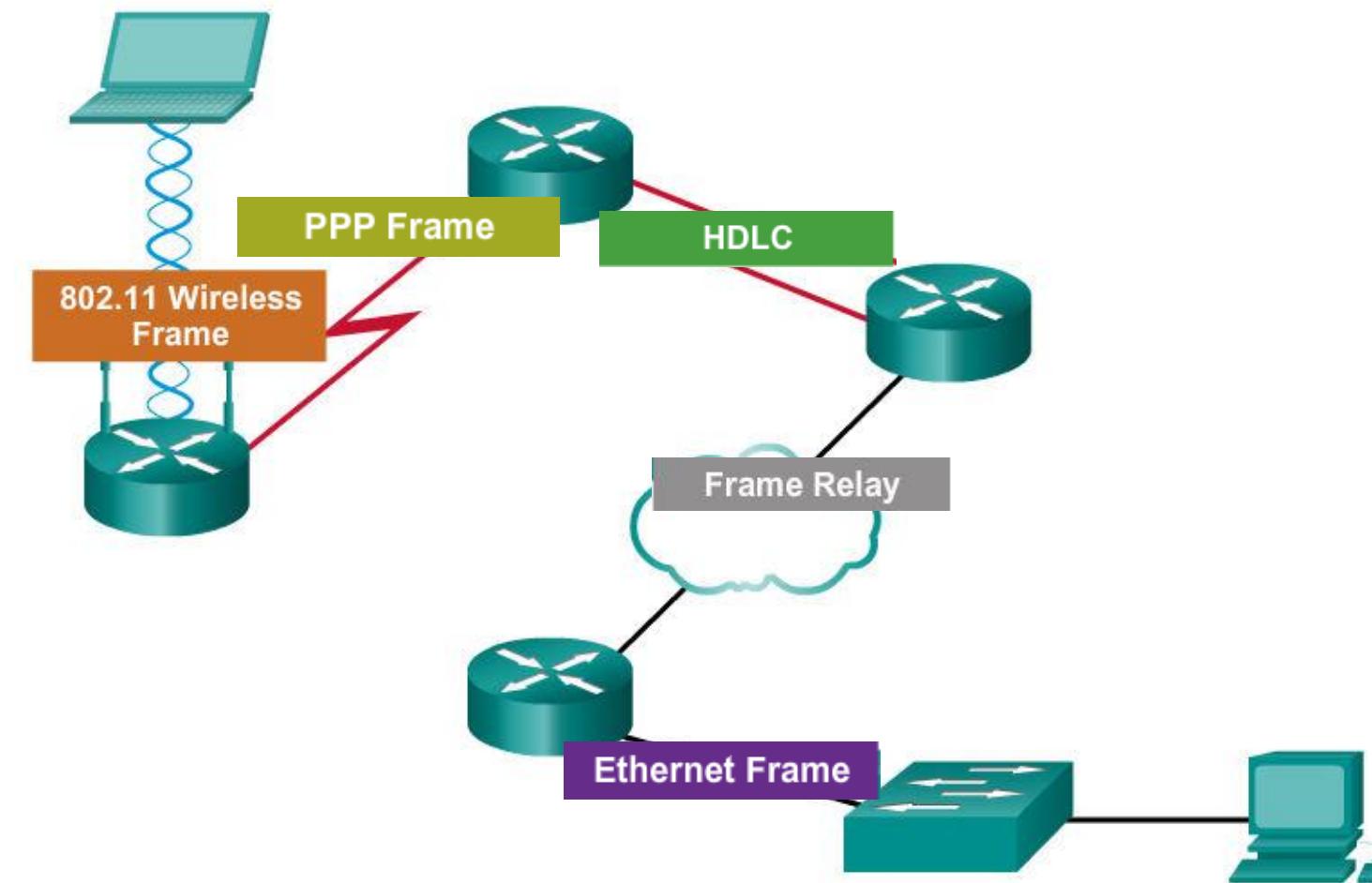
## Stop Frame

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.



# Data Link Frame LAN and WAN Frames

## Examples of Layer 2 Protocols





# Data Link Frame

# Ethernet Frame

## Ethernet Protocol

A Common Data Link Layer Protocol for LANs

Frame						
Field name	Preamble	Destination	Source	Type	Data	Frame Check Sequence
Size	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



## Data Link Frame

# Point-to-Point Protocol Frame

### Point-to-Point Protocol

A Common Data Link Protocol for WANs

Frame						
Field name	Flag	Address	Control	Protocol	Data	FCS
Size	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).

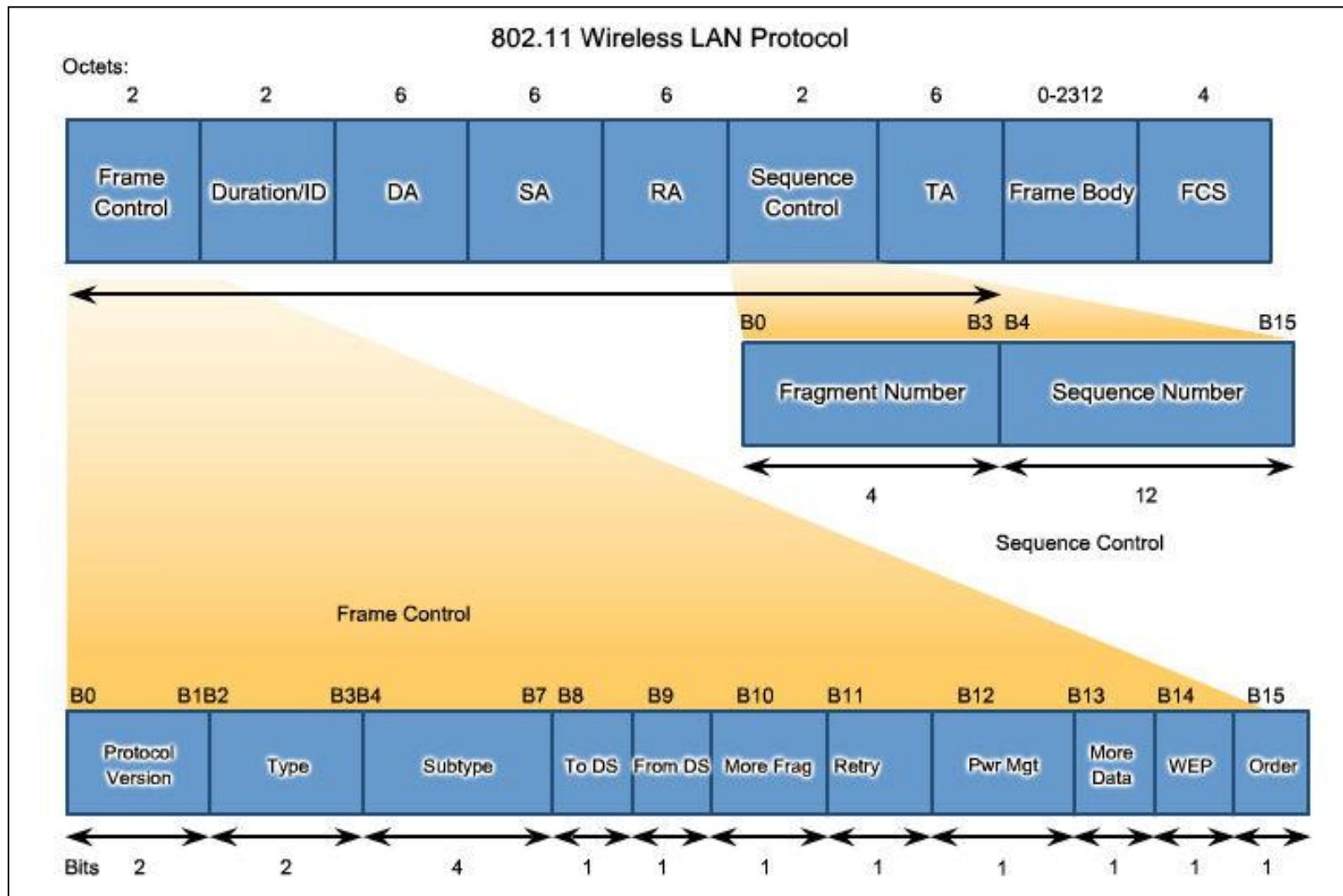
**Data** - Zero or more bytes that contain the datagram for the protocol specified in the protocol field.

**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.



## Data Link Frame

# 802.11 Wireless Frame





# Network Access Summary

- The TCP/IP network access layer is the equivalent of the OSI data link layer (Layer 2) and the physical layer (Layer 1).
- The OSI physical layer provides the means to transport the bits that make up a data link layer frame across the network media.
- The physical layer standards address three functional areas: physical components, frame encoding technique, and signaling method.
- Using the proper media is an important part of network communications. Without the proper physical connection, either wired or wireless, communications between any two devices will not occur.
- Wired communication consists of copper media and fiber cable.
- There are three main types of copper media used in networking: unshielded-twisted pair (UTP), shielded-twisted pair (STP), and coaxial cable. UTP cabling is the most common copper networking media.



## Network Access

# Summary (cont.)

- Optical fiber cable has become very popular for interconnecting infrastructure network devices. It permits the transmission of data over longer distances and at higher bandwidths (data rates) than any other networking media.
- Wireless media carry electromagnetic signals that represent the binary digits of data communications using radio or microwave frequencies.
- The data link layer is responsible for the exchange of frames between nodes over a physical network media. It allows the upper layers to access the media and controls how data is placed and received on the media.
- Among the different implementations of the data link layer protocols, there are different methods of controlling access to the media. These media access control techniques define if and how the nodes share the media.
- The actual media access control method used depends on the topology and media sharing. LAN and WAN topologies can be physical or logical.



## Network Access

# Summary (cont.)

- WANs are commonly interconnected using the point-to-point, hub and spoke, or mesh physical topologies.
- In shared media LANs, end devices can be interconnected using the star, bus, ring, or extended star (hybrid) physical topologies.
- All data link layer protocols encapsulate the Layer 3 PDU within the data field of the frame. However, the structure of the frame and the fields contained in the header and trailer vary according to the protocol.





## Chapter 5: Ethernet



## Introduction to Networks

Cisco | Networking Academy®  
Mind Wide Open™



# Chapter 5: Objectives

Upon completion of this chapter, you will be able to:

- Describe the operation of the Ethernet sublayers.
- Identify the major fields of the Ethernet frame.
- Describe the purpose and characteristics of the Ethernet MAC address.
- Describe the purpose of ARP.
- Explain how ARP requests impact network and host performance.
- Explain basic switching concepts.
- Compare fixed configuration and modular switches.
- Configure a Layer 3 switch.



# Chapter 5

5.0 Introduction

5.1 Ethernet Protocol

5.2 Address Resolution Protocol

5.3 LAN Switches

5.4 Summary

## 5.1 Ethernet Protocol





## Ethernet Operation

# LLC and MAC Sublayers

### Ethernet

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

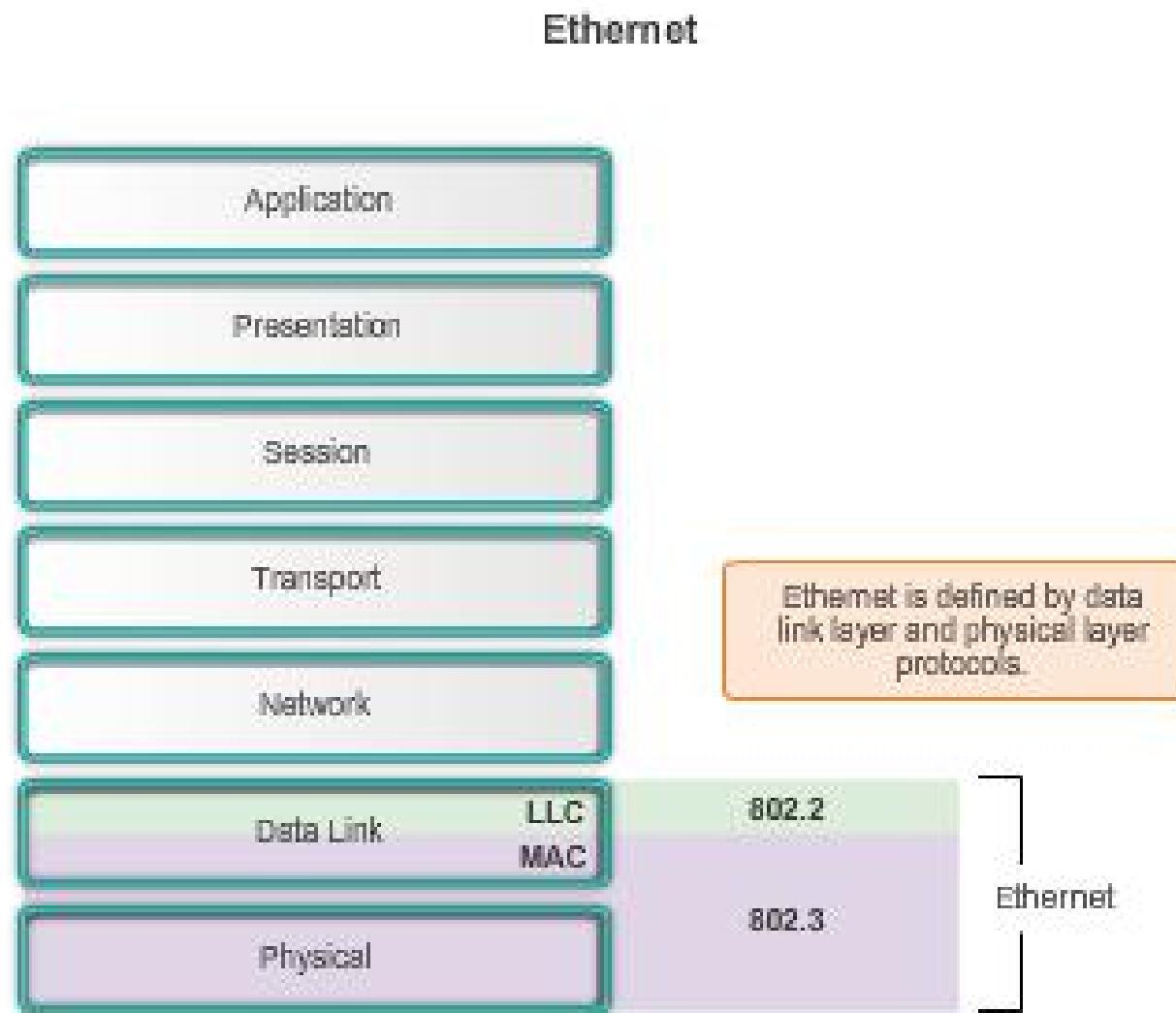
### Ethernet Standards

- Define Layer 2 protocols and Layer 1 technologies
- Two separate sub layers of the data link layer to operate – Logical link control (LLC) and the MAC sublayers



## Ethernet Operation

# LLC and MAC Sublayers (cont.)





## Ethernet Operation

# LLC and MAC Sublayers (cont.)

### LLC

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

### MAC

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



# Ethernet Operation

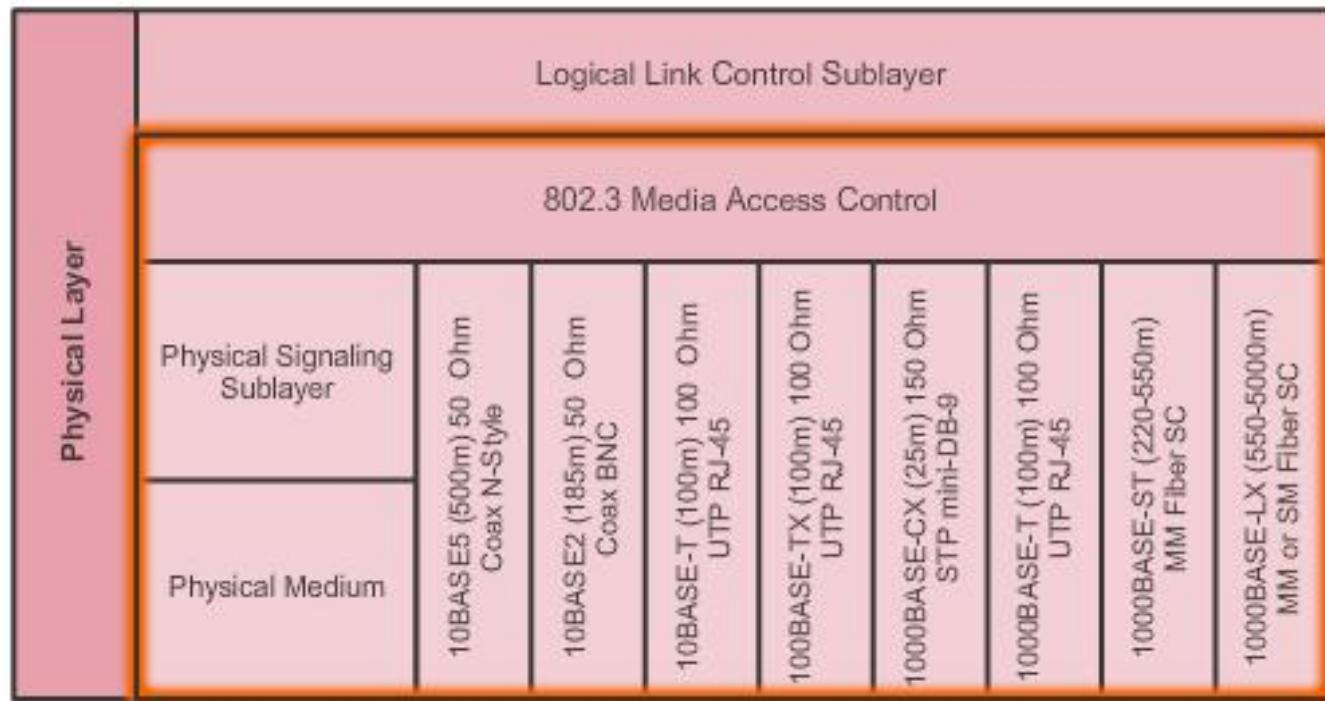
# MAC Sublayer

## Data Encapsulation

- Frame delimiting
- Addressing
- Error detection

## Media Access Control

- Control of frame placement on and off the media
- Media recovery





## Ethernet Operation

# MAC Sublayer (cont.)

### Data encapsulation

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

### Provides three primary functions:

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



## Ethernet Operation

# MAC Sublayer (cont.)

## MAC

- Responsible for the placement of frames on the media and the removal of frames from the media
- Communicates directly with the physical layer
- If multiple devices on a single medium attempt to forward data simultaneously, the data will collide resulting in corrupted, unusable data
- Ethernet provides a method for controlling how the nodes share access through the use a Carrier Sense Multiple Access (CSMA) technology



## Ethernet Operation

# Media Access Control

### Carrier Sense Multiple Access (CSMA) process

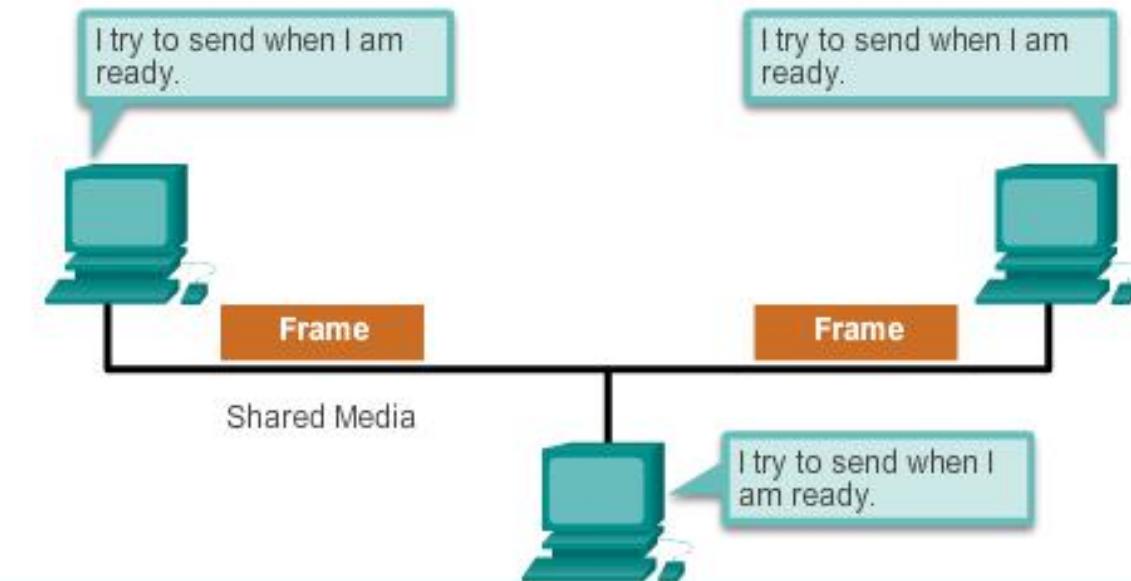
- Used to first detect if the media is carrying a signal
- If no carrier signal is detected, the device transmits its data
- If two devices transmit at the same time - data collision



## Ethernet Operation

# Media Access Control (cont.)

### Contention-Based Access



Method	Characteristics	Example
Contention-Based Access	<ul style="list-style-type: none"><li>Stations can transmit at any time</li><li>Collisions exist</li><li>Mechanisms exist to resolve contention problems<ul style="list-style-type: none"><li>CSMA/CD for Ethernet networks</li><li>CSMA/CA for 802.11 wireless networks</li></ul></li></ul>	<ul style="list-style-type: none"><li>Ethernet</li><li>Wireless</li></ul>



## Ethernet Operation

# Media Access Control (cont.)

CSMA is usually implemented in conjunction with a method for resolving media contention. The two commonly used methods are:

**CSMA/Collision Detection and CSMA/Collision Avoidance**

## CSMA/Collision Detection

- The device monitors the media for the presence of a data signal
- If a data signal is absent, indicating that the media is free, the device transmits the data
- If signals are then detected that show another device was transmitting at the same time, all devices stop sending & try again later
- While Ethernet networks are designed with CSMA/CD technology, with today's intermediate devices, collisions do not occur and the processes utilized by CSMA/CD are really unnecessary
- Wireless connections in a LAN environment still have to take collisions into account



## Ethernet Operation

# Media Access Control (cont.)

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

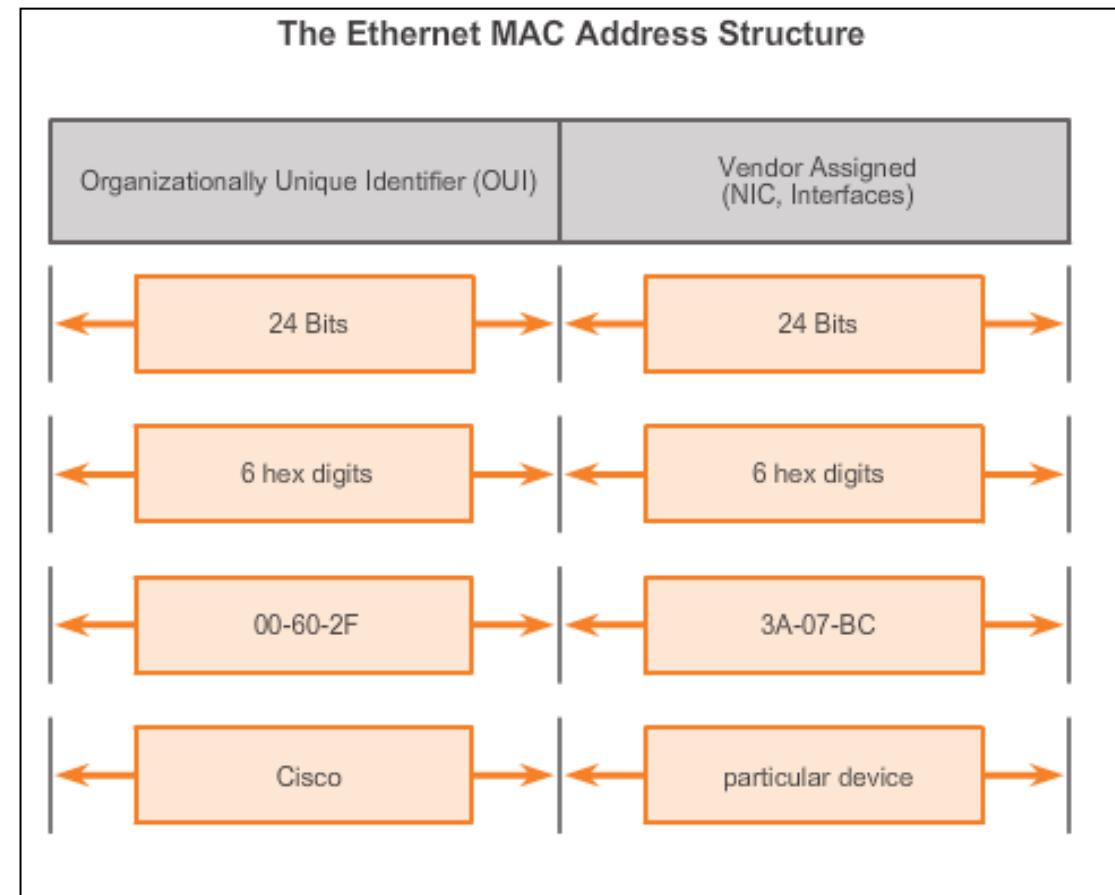
- Device examines the media for the presence of data signal - if the media is free, the device sends a notification across the media of its intent to use it
- The device then sends the data.
- Used by 802.11 wireless networking technologies



## Ethernet Operation

# MAC Address: Ethernet Identity

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





# Ethernet Operation Frame Processing

- MAC addresses assigned to workstations, servers, printers, switches, and routers.
- Example MACs:
  - 00-05-9A-3C-78-00
  - 00:05:9A:3C:78:00
  - 0005.9A3C.7800.
- When a device is forwarding a message to an Ethernet network, attaches header information to the packet, contains the source and destination MAC address.
- Each NIC views information to see if the destination MAC address in the frame matches the device's physical MAC address stored in RAM.
- No match, the device discards the frame.
- Matches the destination MAC of the frame, the NIC passes the frame up the OSI layers, where the de-encapsulation process takes place.



## Ethernet Frame Attributes

# Ethernet Encapsulation

- Early versions of Ethernet were slow at 10 Mb/s.
- Now operate at 10 Gb/s per second and faster.
- Ethernet frame structure adds headers and trailers around the Layer 3 PDU to encapsulate the message being sent.
- Ethernet II is the Ethernet frame format used in TCP/IP networks.

Comparison of 802.3 and Ethernet II Frame Structures and Field Size

IEEE 802.3

7	1	6	6	2	46 to 1500	4
Preamble	Start of Frame Delimiter	Destination Address	Source Address	Length	802.2 Header and Data	Frame Check Sequence

Field size in bytes

Ethernet II

8	6	6	2	46 to 1500	4
Preamble	Destination Address	Source Address	Type	Data	Frame Check Sequence



## Ethernet Frame Attributes

# Ethernet Frame Size

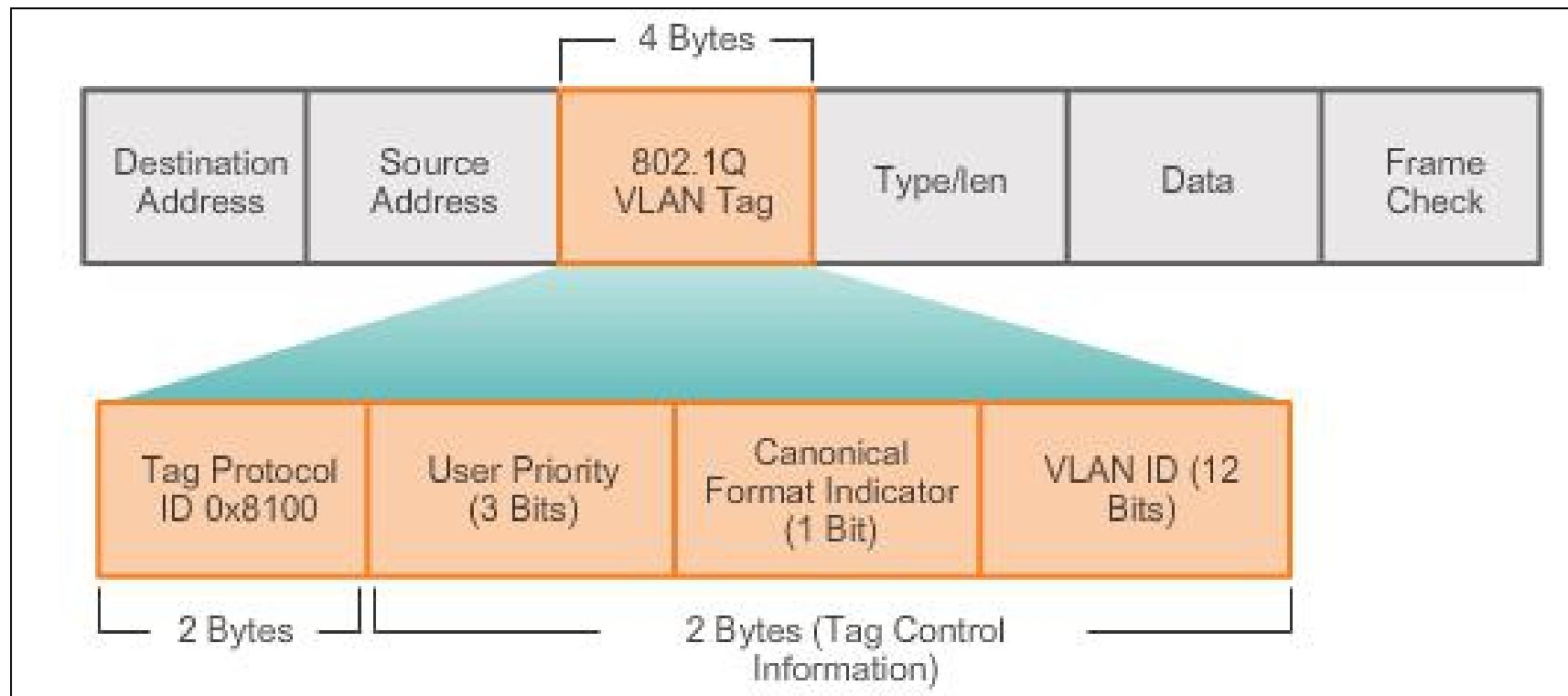
- Ethernet II and IEEE 802.3 standards define the minimum frame size as 64 bytes and the maximum as 1518 bytes
- Less than 64 bytes in length is considered a "collision fragment" or "runt frame"
- If size of a transmitted frame is less than the minimum or greater than the maximum, the receiving device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



## Ethernet Frame Attributes

# Ethernet Frame Size (cont.)

Extra 4 Bytes Allows for QoS and VLAN Technologies



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



## Ethernet Frame Attributes

# Introduction to the Ethernet Frame

IEEE 802.3

7 Preamble	1 Start of Frame Delimiter	6 Destinatio n Address	6 Source Address	2 Length	46 to 1500 802.2 Header and Data	4 Frame Check Sequence
---------------	-------------------------------------	------------------------------	------------------------	-------------	---	------------------------------

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

**Length/Type Field –**  
Defines the exact length of the frame's data field; describes which protocol is implemented.

**Data and Pad Fields –**  
Contains the encapsulated data from a higher layer, an IPv4 packet.



## Ethernet Frame Attributes

# Introduction to the Ethernet Frame (cont.)

IEEE 802.3

7 Preamble	1 Start of Frame Delimiter	6 Destination Address	6 Source Address	2 Length	46 to 1500 802.2 Header and Data	4 Frame Check Sequence
---------------	-------------------------------	--------------------------	---------------------	-------------	-------------------------------------	---------------------------

### Frame Check Sequence Field

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



## Ethernet MAC

# MAC Addresses and Hexadecimal

Decimal and Binary equivalents of 0 to F Hexadecimal

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

Selected Decimal, Binary and Hexadecimal equivalents

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



## Ethernet MAC

# MAC Address Representations

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

Ethernet adapter Local Area Connection:

```
Connection-specific DNS Suffix . : example.com
Description . . . . . : Intel(R) Gigabit Network Connection
Physical Address. . . . . : 00-18-DE-C7-E3-F8
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
IPv4 Address. . . . . : 192.168.1.67 (Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, November 26, 2012 12:14:48 PM
Lease Expires . . . . . : Saturday, December 01, 2012 12:15:02 AM
Default Gateway . . . . . : 192.168.1.254
DHCP Server. . . . . : 192.168.1.254
DNS Servers . . . . . : 192.168.1.254
```

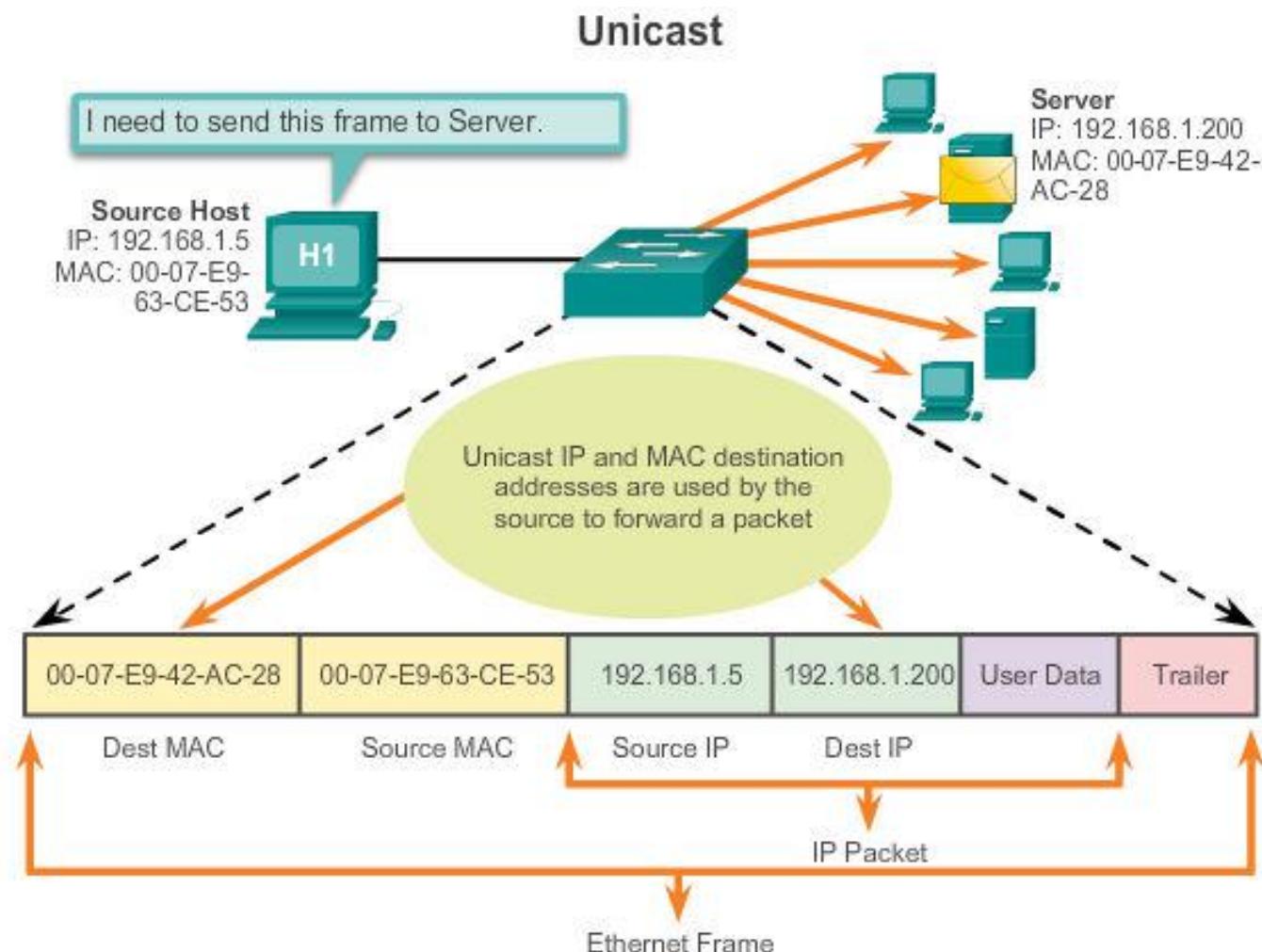
With Dashes 00-60-2F-3A-07-BC

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

With Periods 0060.2F3A.07BC

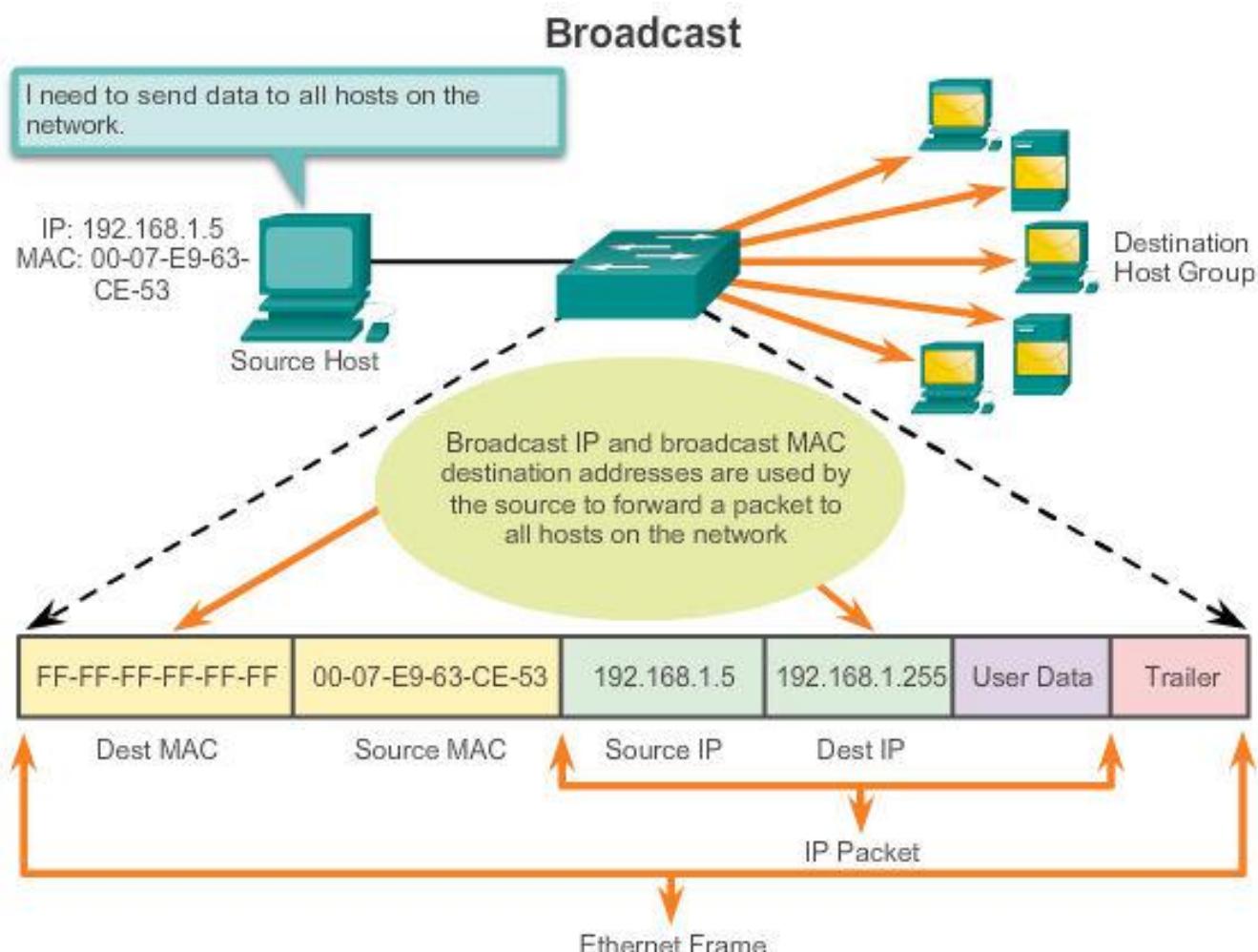


# Ethernet MAC Unicast MAC Address



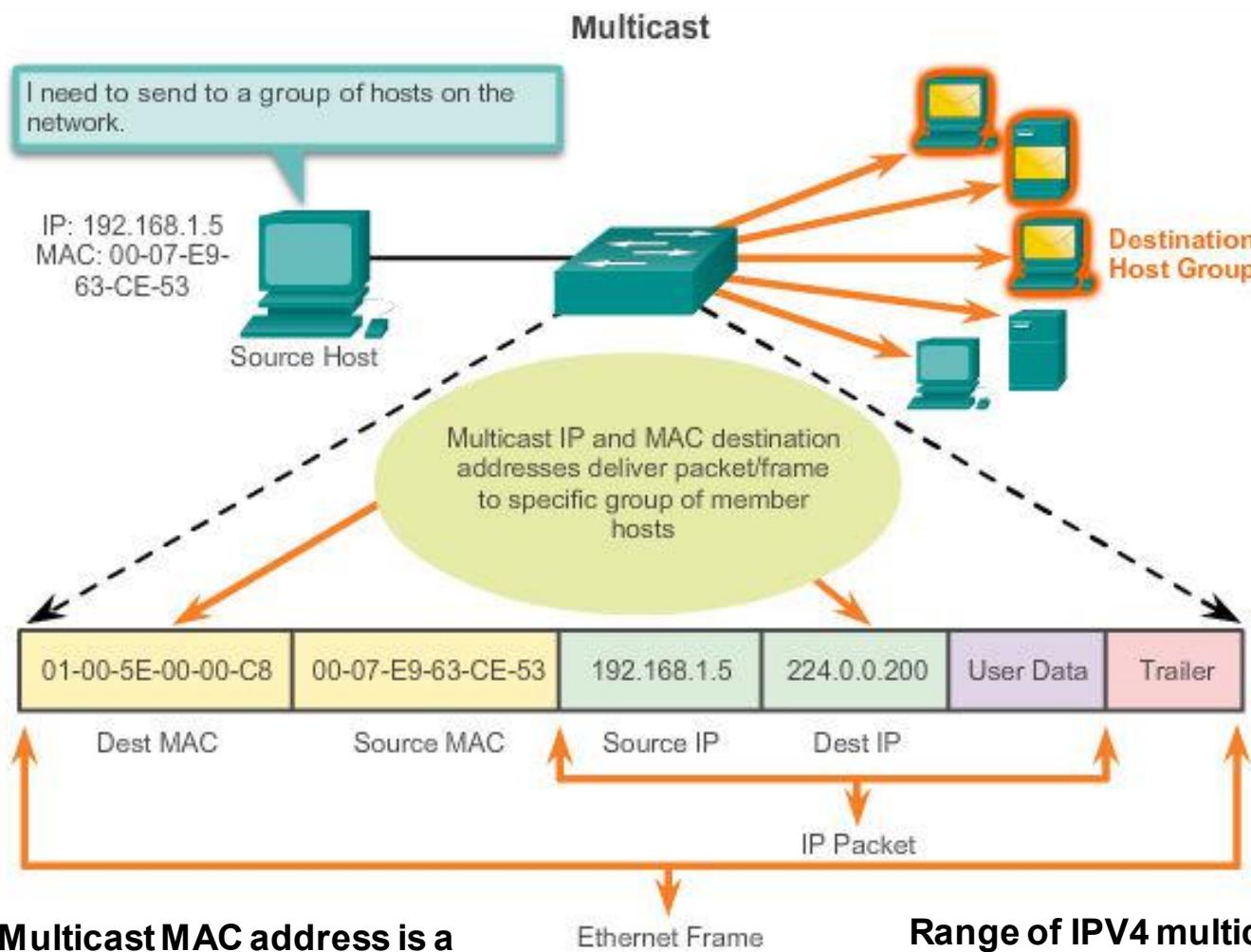


# Ethernet MAC Broadcast MAC Address





# Ethernet MAC Multicast MAC Address





## MAC and IP

# MAC and IP

### MAC Address

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

### IP Address

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

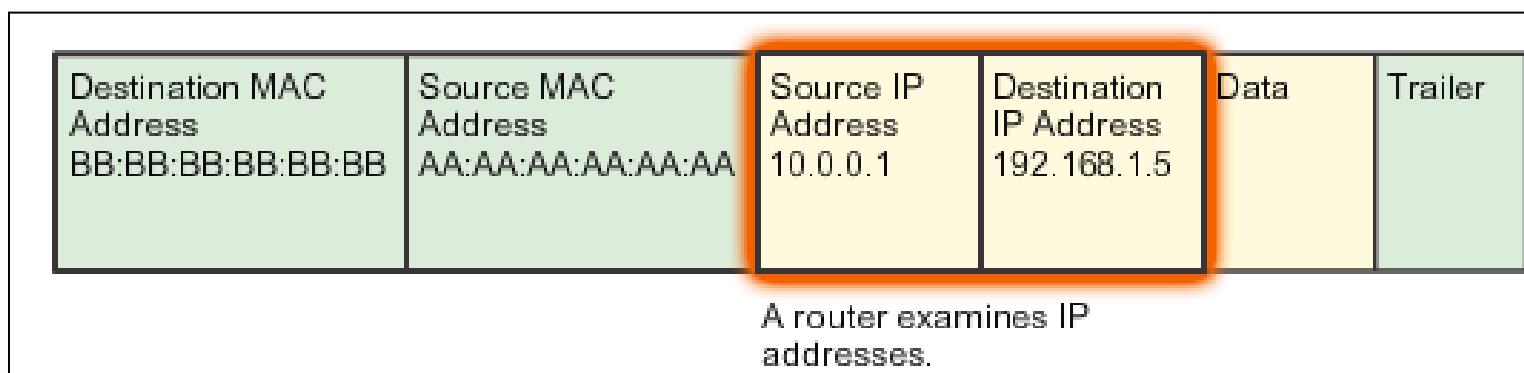
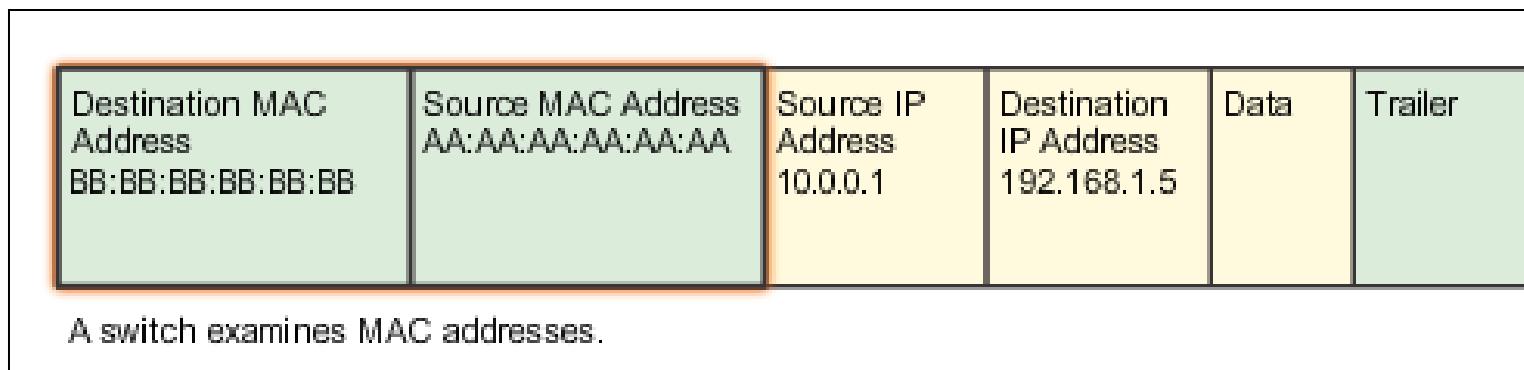
Both the physical MAC and logical IP addresses are required for a computer to communicate just like both the name and address of a person are required to send a letter.



## Ethernet MAC

# End-to-End Connectivity, MAC, and IP

## IP Packet Encapsulated in an Ethernet Frame





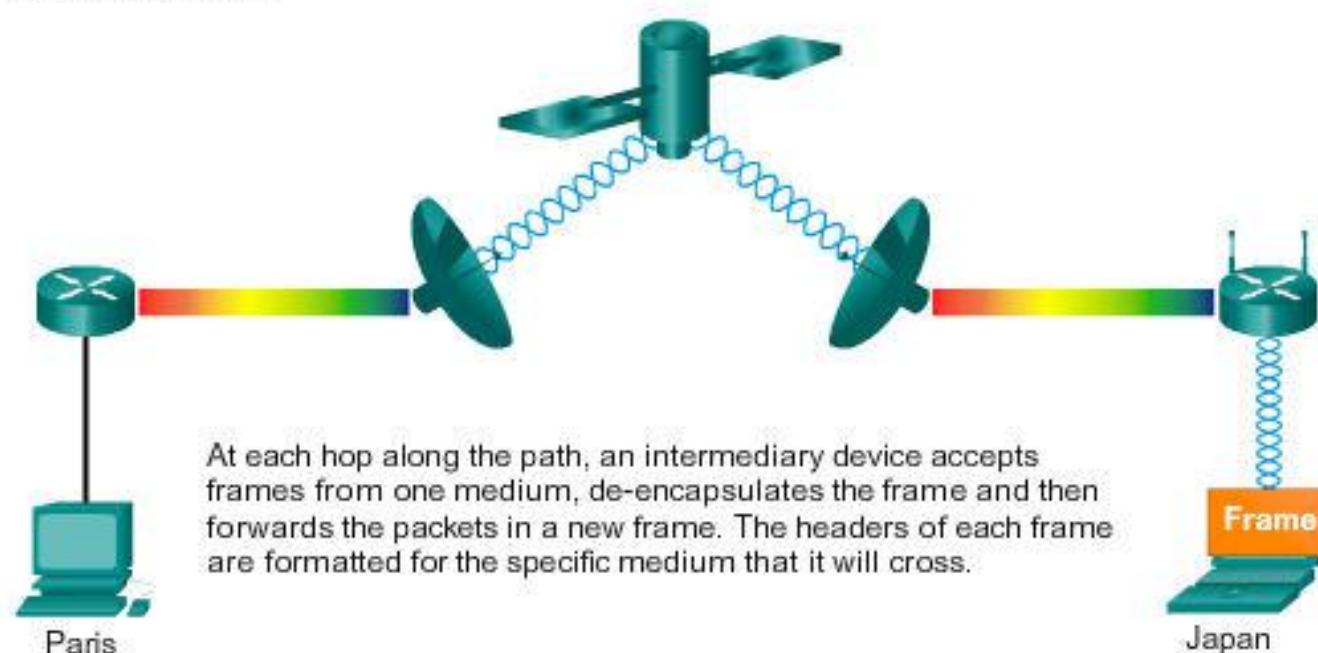
## Ethernet MAC

# End-to-End Connectivity, MAC, and IP (cont.)

### The Data Link Layer

Data link layer protocols govern how to format a frame for use on different media.

Different protocols may be in use for different media.



## 5.2 Address Resolution Protocol





## ARP

# Introduction to ARP

## ARP Purpose

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

The ARP protocol provides two basic functions:

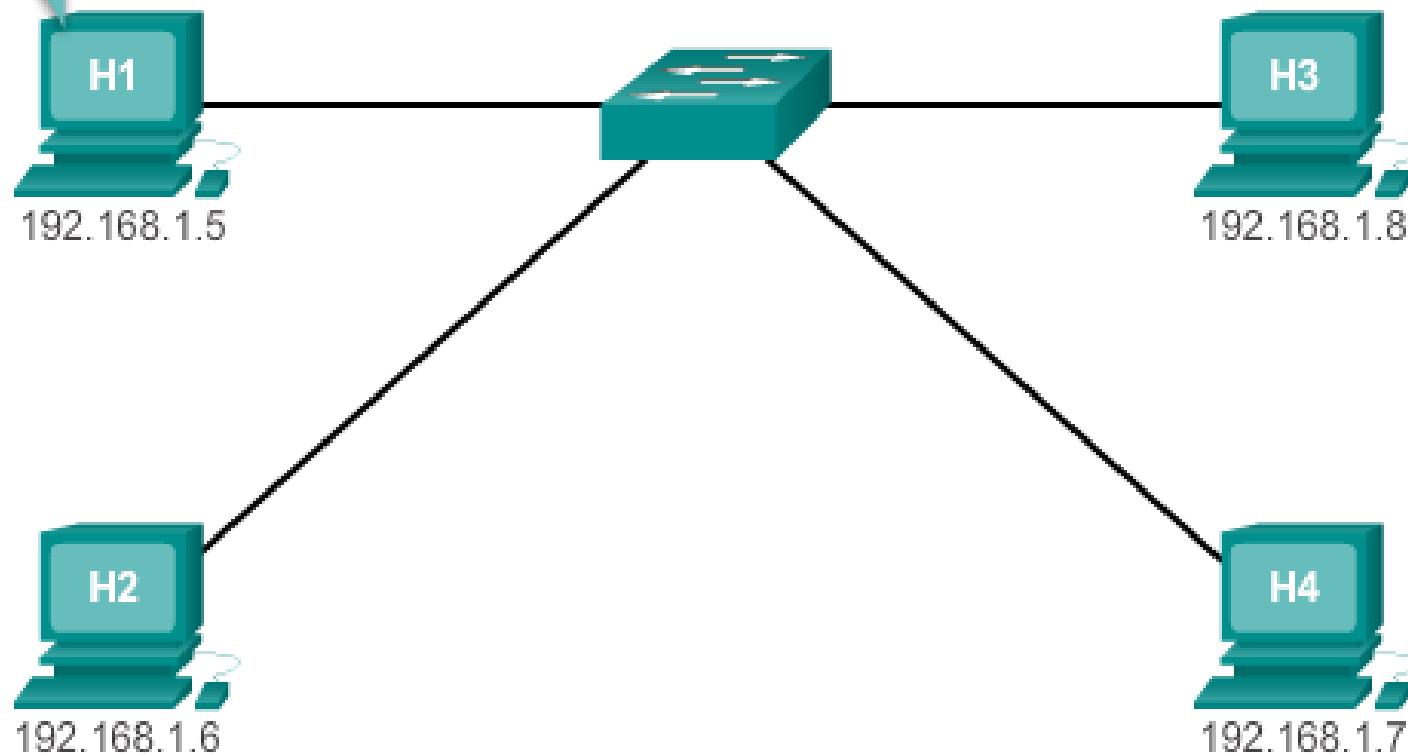
- Resolving IPv4 addresses to MAC addresses
- Maintaining a table of mappings



## ARP

# Introduction to ARP (cont.)

I need to send information to 192.168.1.7, but I only have the IP address. I don't know the MAC address of the device that has that IP.





## ARP

# ARP Functions/Operation

## ARP Table

- Used to find the data link layer address that is mapped to the destination IPv4 address.
- As a node receives frames from the media, it records the source IP and MAC address as a mapping in the ARP table.

## ARP Request

- Layer 2 broadcast to all devices on the Ethernet LAN.
- The node that matches the IP address in the broadcast will reply.
- If no device responds to the ARP request, the packet is dropped because a frame cannot be created.

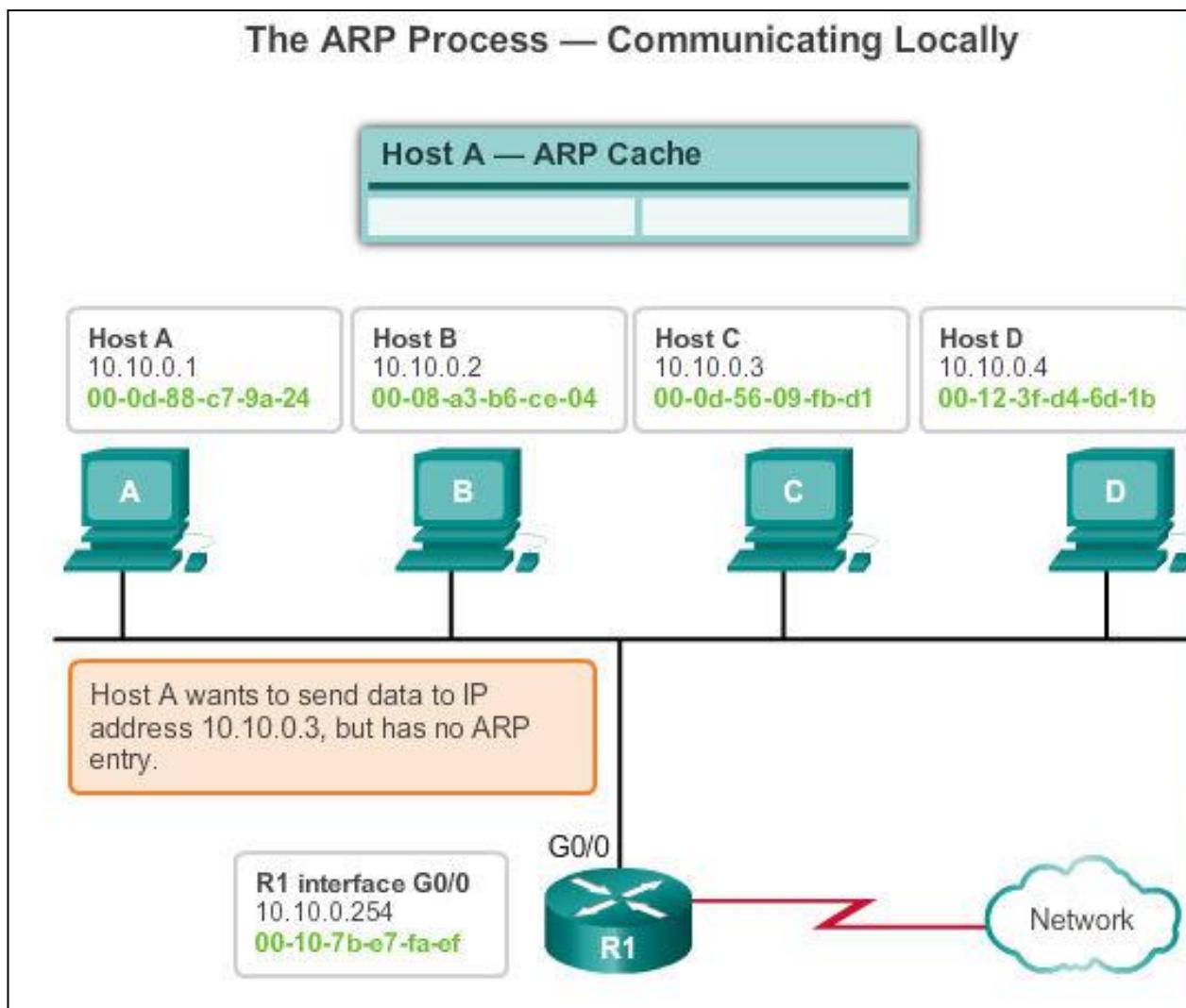
**Note:** Static map entries can be entered in an ARP table, but this is rarely done.



# ARP

# ARP Operation

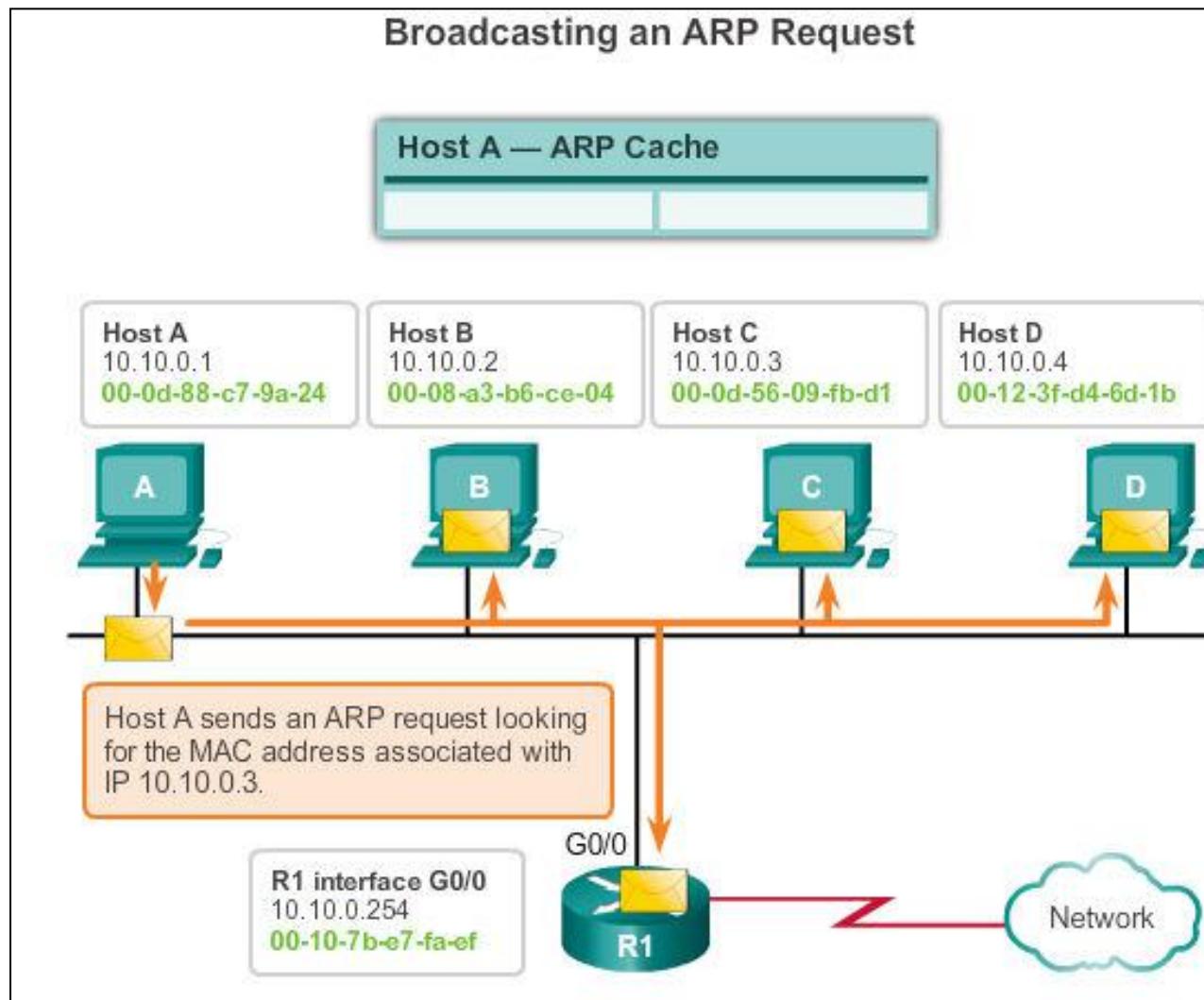
## The ARP Process — Communicating Locally





## ARP

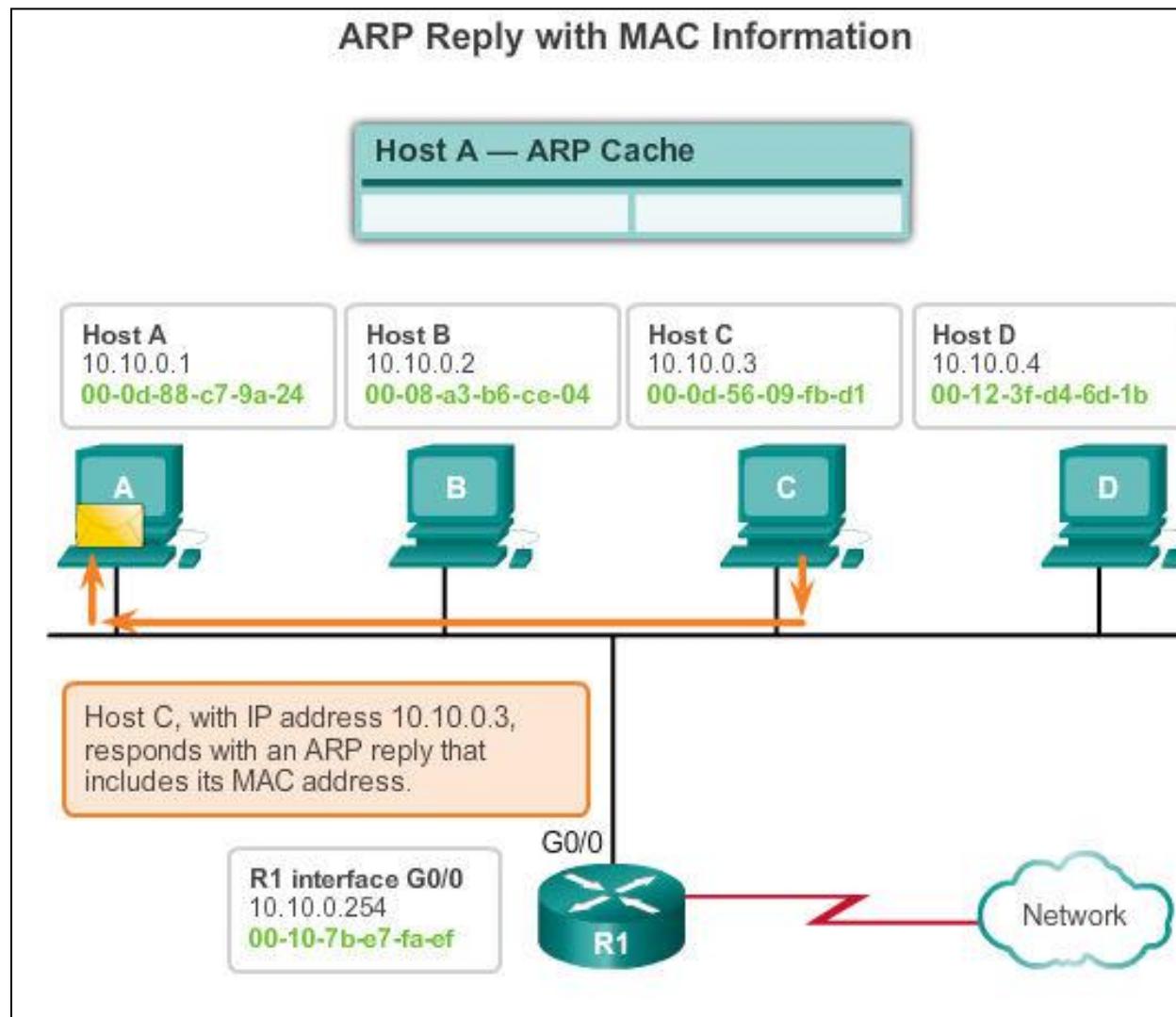
## ARP Operation (cont.)





## ARP

## ARP Operation (cont.)

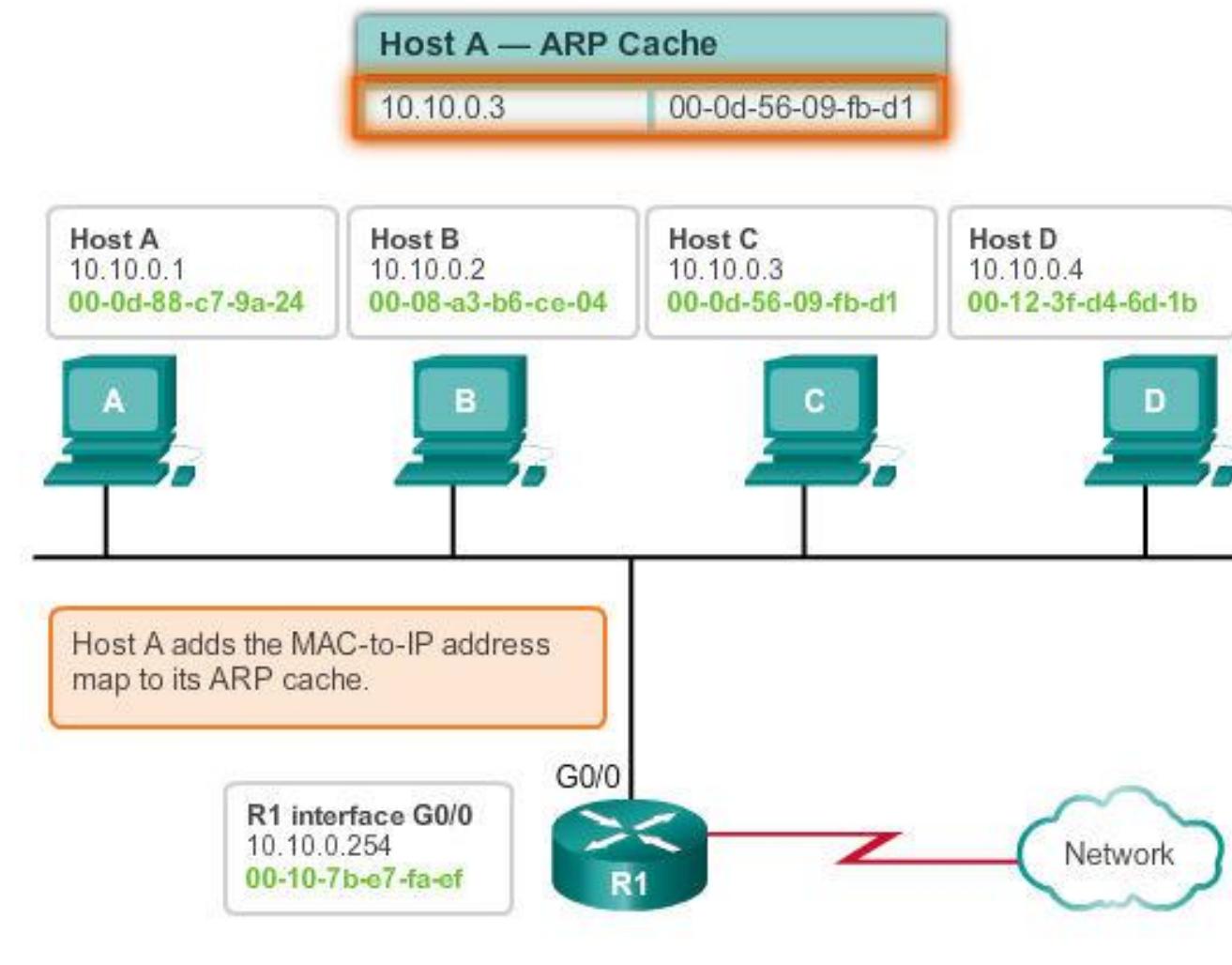




## ARP

## ARP Operation (cont.)

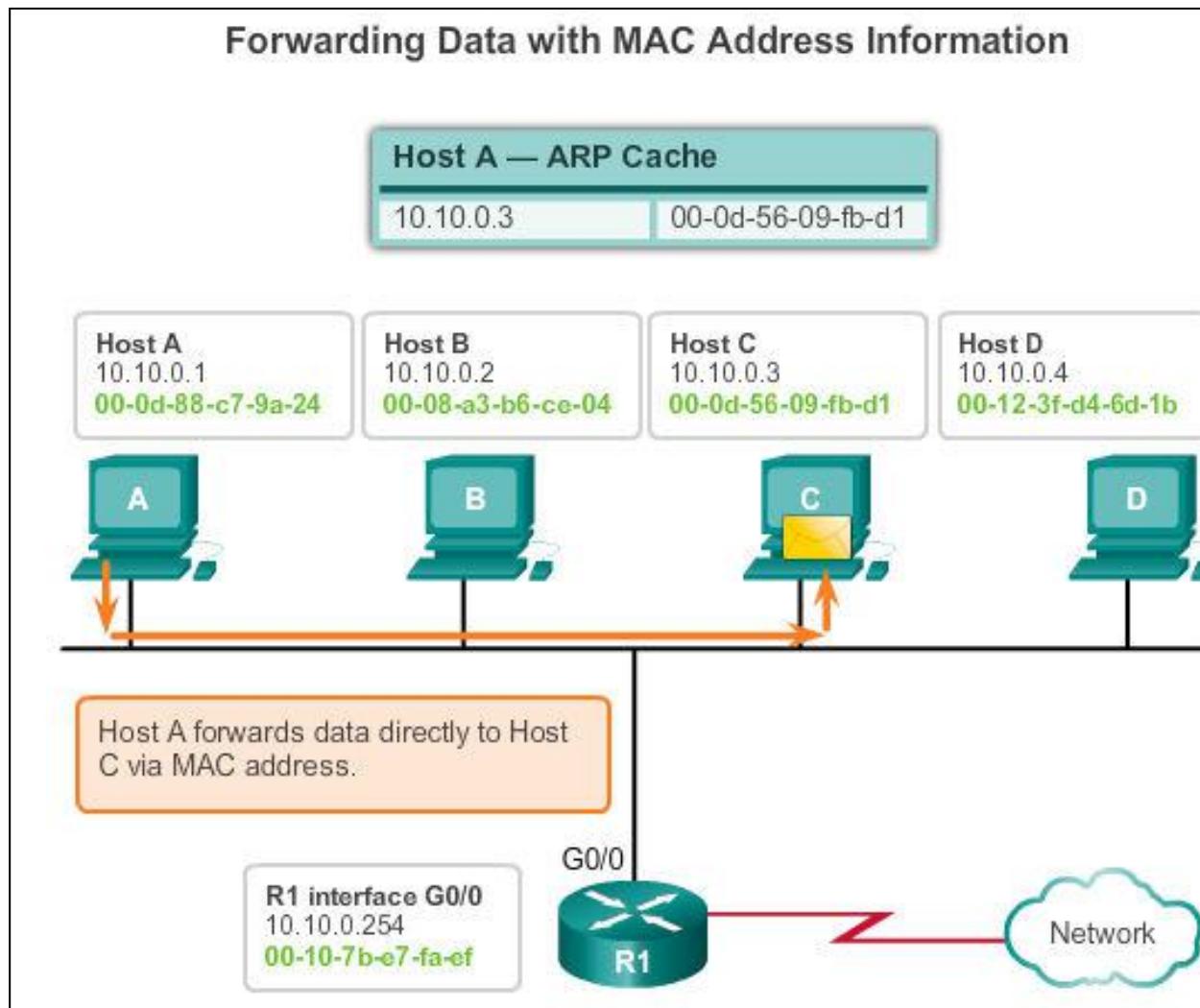
## Adding MAC-to-IP Map in ARP Cache





## ARP

## ARP Functions/Operation (cont.)





## ARP

# ARP Role in Remote Communication

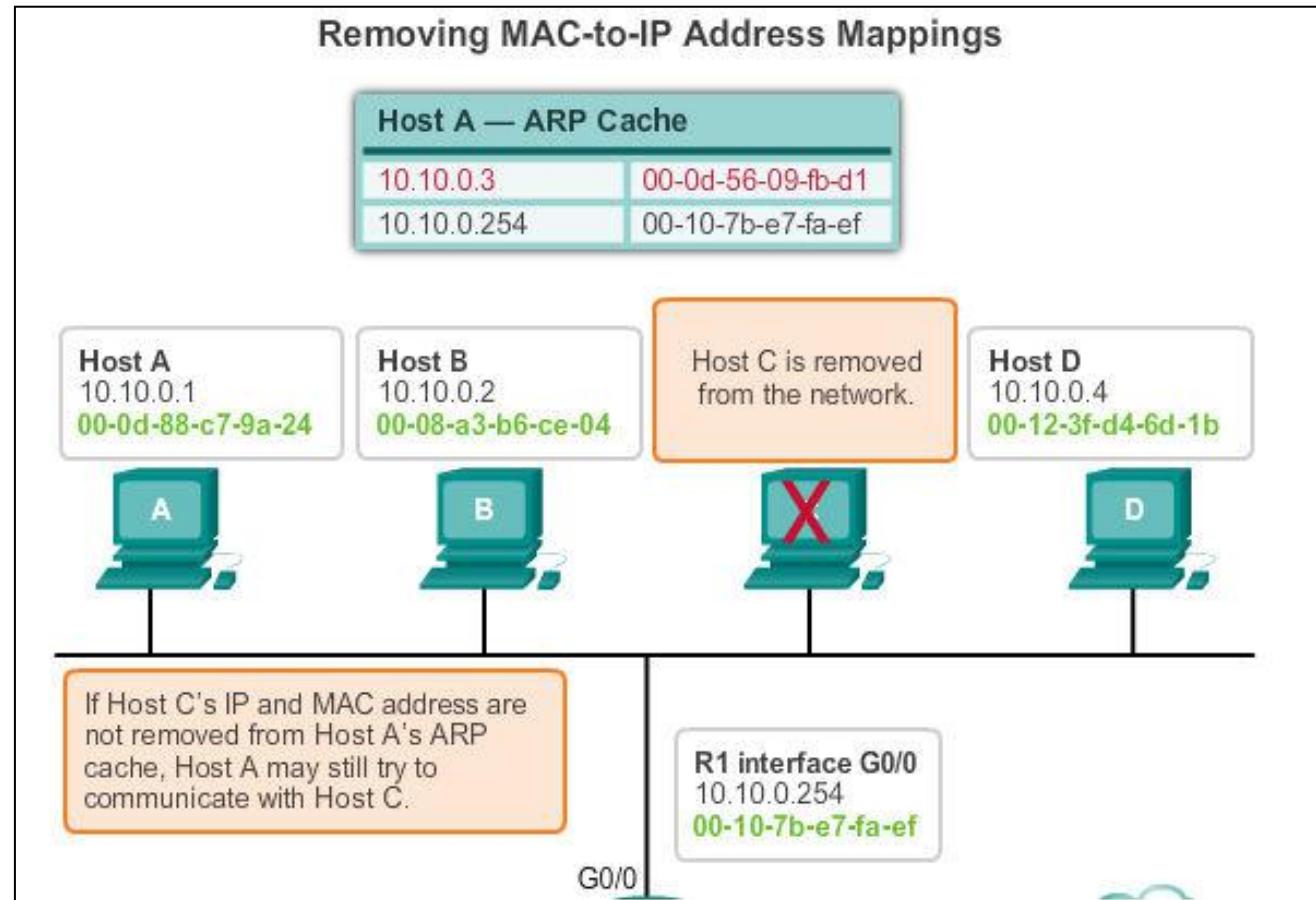
- If the destination IPv4 host is on the local network, the frame will use the MAC address of this device as the destination MAC address.
- If the destination IPv4 host is not on the local network, the source uses the ARP process to determine a MAC address for the router interface serving as the gateway.
- In the event that the gateway entry is not in the table, an ARP request is used to retrieve the MAC address associated with the IP address of the router interface.



## ARP

# Removing Entries from an ARP Table

- The ARP cache timer removes ARP entries that have not been used for a specified period of time.
- Commands may also be used to manually remove all or some of the entries in the ARP table.





## ARP

# ARP Tables on Networking Devices

```
Router#show ip arp
```

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	172.16.233.229	-	0000.0c59.f892	ARPA	Ethernet0/0
Internet	172.16.233.218	-	0000.0c07.ac00	ARPA	Ethernet0/0
Internet	172.16.168.11	-	0000.0c63.1300	ARPA	Ethernet0/0
Internet	172.16.168.254	9	0000.0c36.6965	ARPA	Ethernet0/0

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

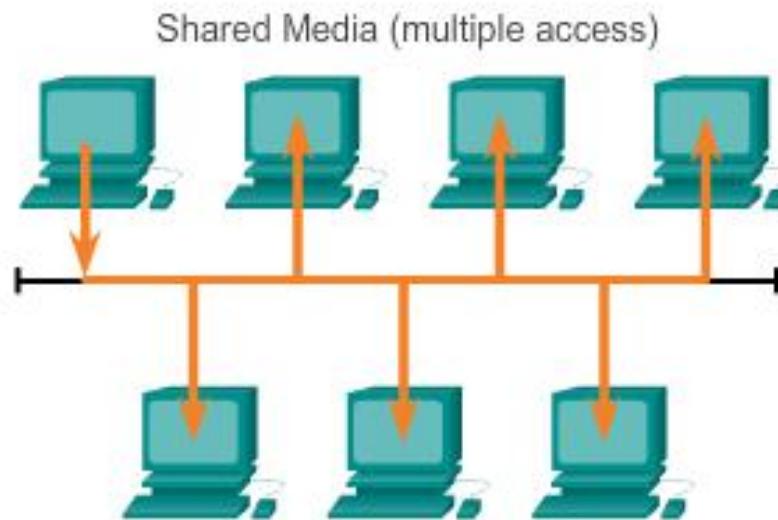
Internet Address	Physical Address	Type
192.168.1.254	64-0f-29-0d-36-91	dynamic
192.168.1.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static



## ARP Issues

# How ARP Can Create Problems

ARP broadcasts can flood the local media.



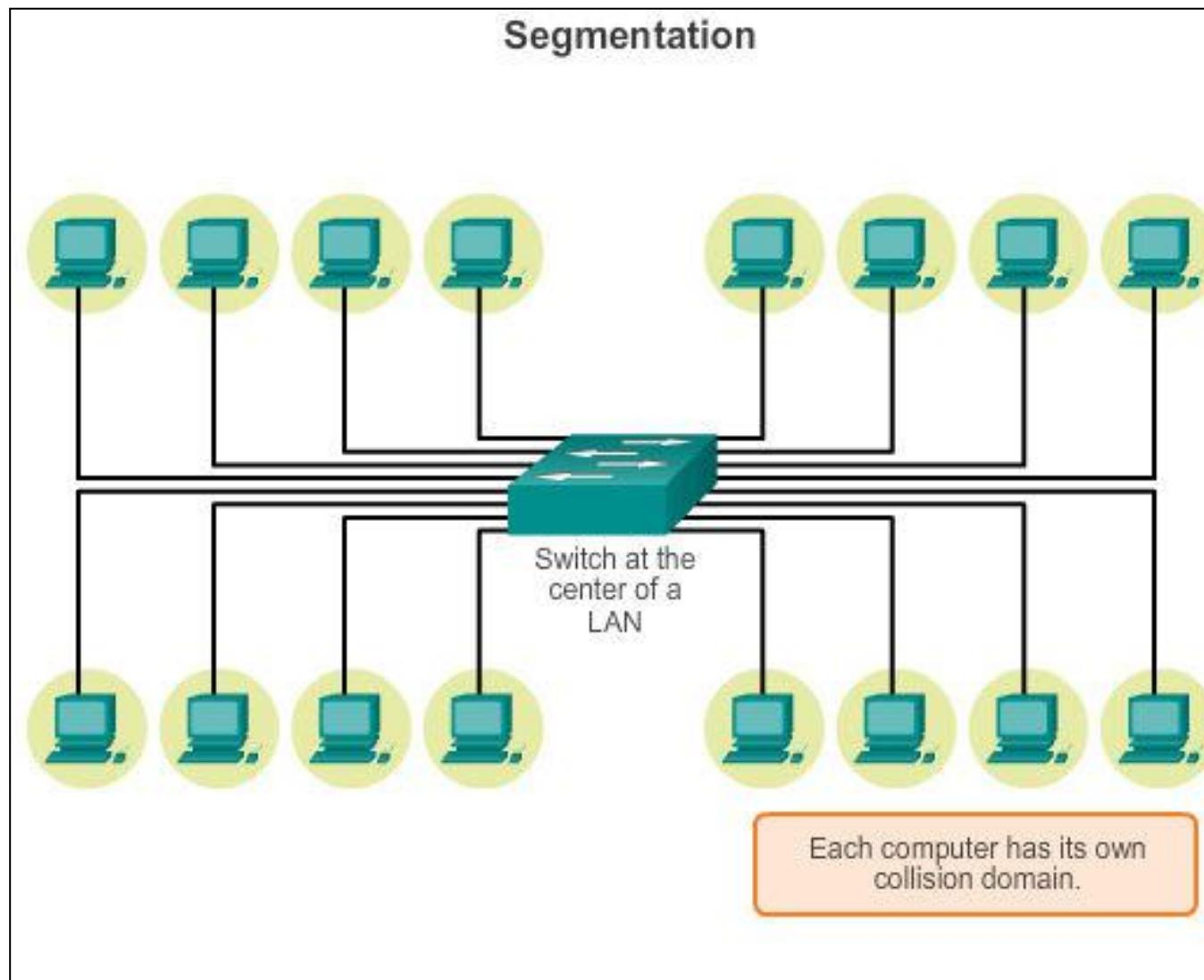
### ARP Issues:

- Broadcasts, overhead on the media
- Security



## ARP Issues

# Mitigating ARP Problems



## 5.3 LAN Switches





# Switching

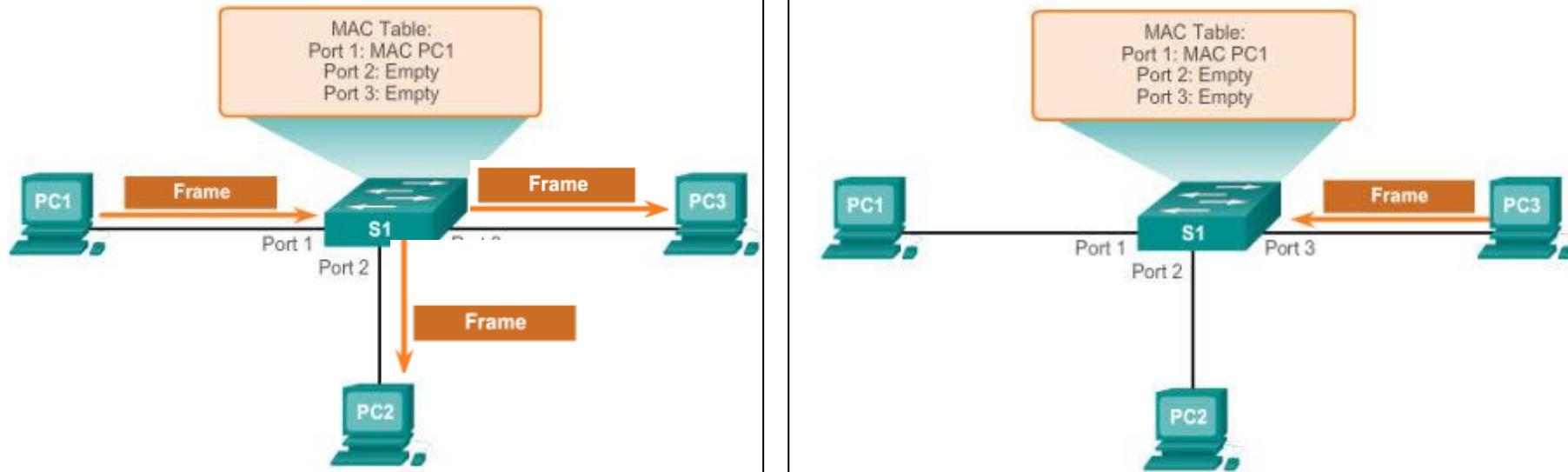
# Switch Port Fundamentals

## Layer 2 LAN Switch

- Connects end devices to a central intermediate device on most Ethernet networks
- Performs switching and filtering based only on the MAC address
- Builds a MAC address table that it uses to make forwarding decisions
- Depends on routers to pass data between IP subnetworks



# Switching Switch MAC Address Table

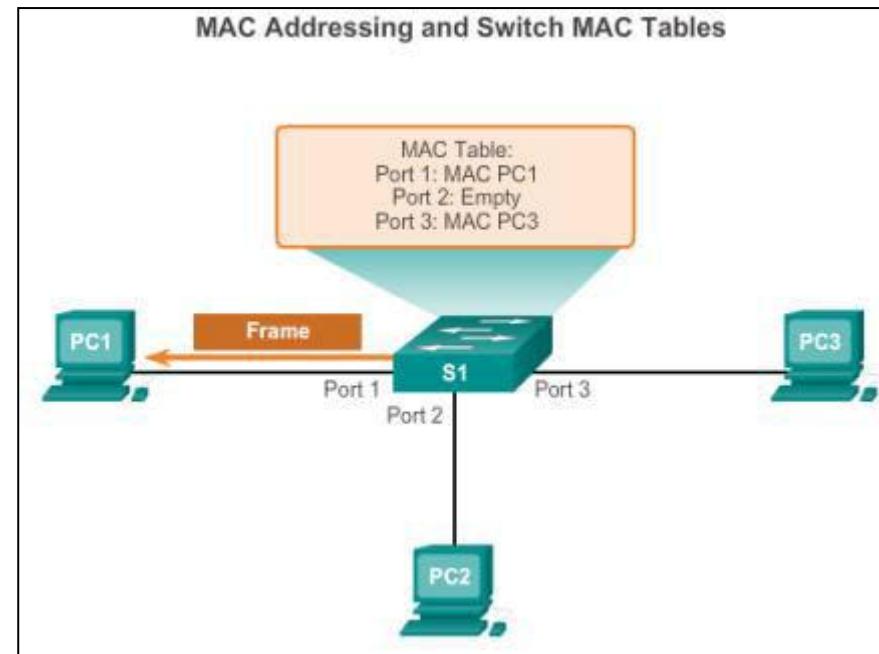
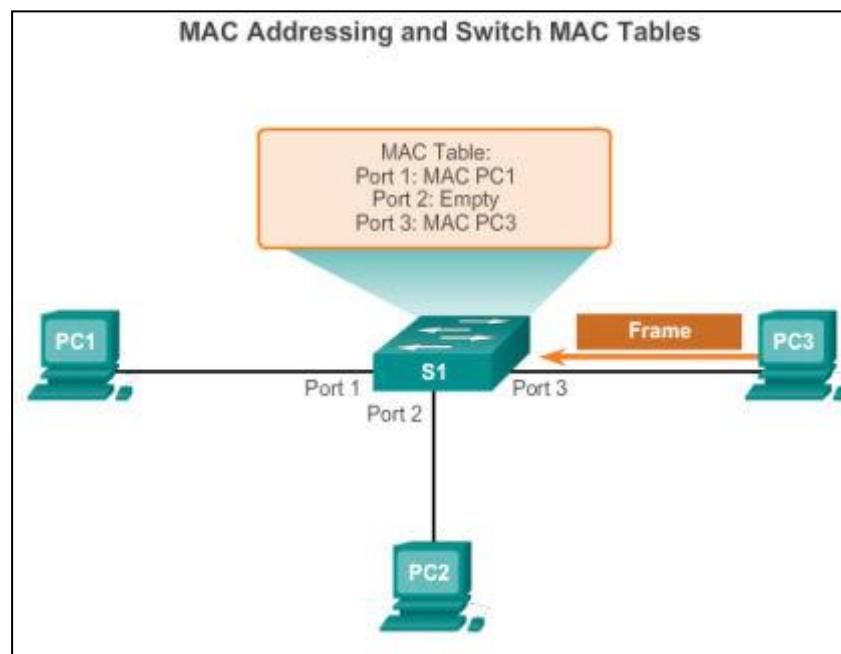


1. The switch receives a broadcast frame from PC 1 on Port 1.
2. The switch enters the source MAC address and the switch port that received the frame into the address table.
3. Because the destination address is a broadcast, the switch floods the frame to all ports, except the port on which it received the frame.
4. The destination device replies to the broadcast with a unicast frame addressed to PC 1.



# Switching

## Switch MAC Address Table (cont.)



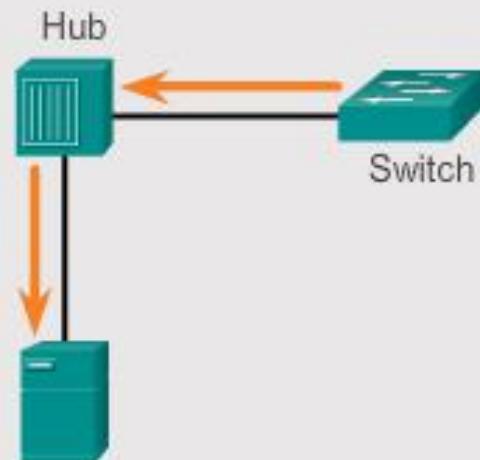
5. The switch enters the source MAC address of PC 2 and the port number of the switch port that received the frame into the address table. The destination address of the frame and its associated port is found in the MAC address table.
  6. The switch can now forward frames between source and destination devices without flooding, because it has entries in the address table that identify the associated ports.



# Switching Duplex Settings

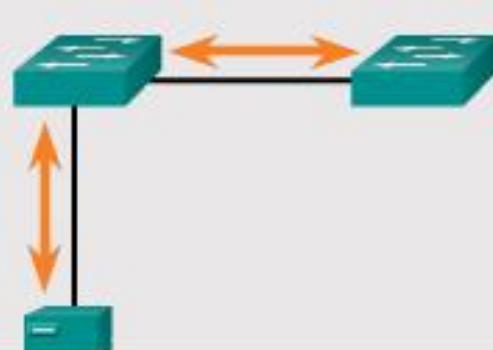
## Half Duplex (CSMA/CD)

- Unidirectional data flow
- Higher potential for collision
- Hub connectivity



## Full Duplex

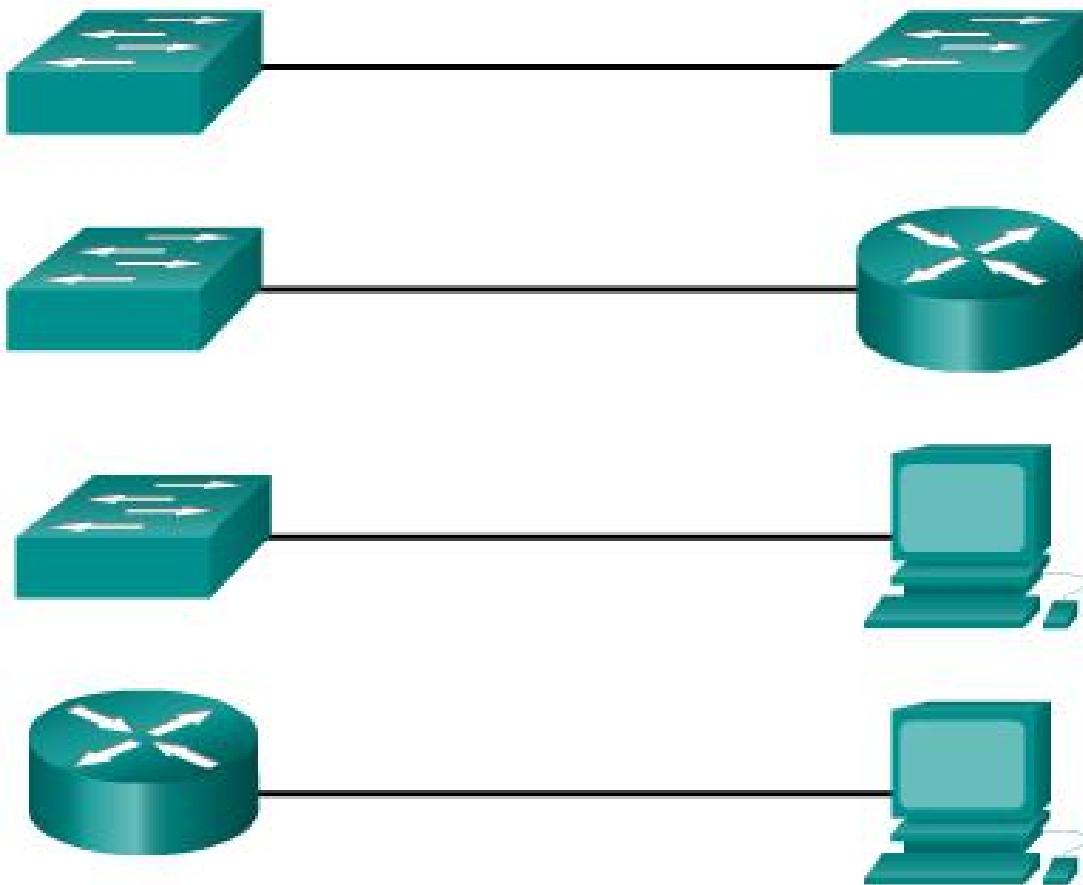
- Point-to-point only
- Attached to dedicated switched port
- Requires full-duplex support on both ends
- Collision-free
- Collision detect circuit disabled





# Switching Auto-MDIX

MDIX auto detects the type of connection required and configures the interface accordingly





# Switching Frame Forwarding Methods on Cisco Switches

Store-and-forward



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



# Switching Cut-through Switching

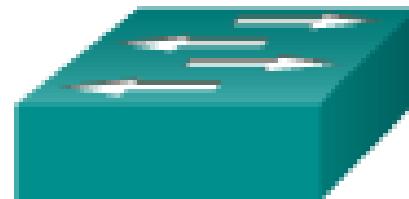
## Fast-forward switching:

- Lowest level of latency immediately forwards a packet after reading the destination address, typical cut-through method of switching

## Fragment-free switching:

- Switch stores the first 64 bytes of the frame before forwarding, most network errors and collisions occur during the first 64 bytes

Cut-through



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



# Switching Memory Buffering on Switches

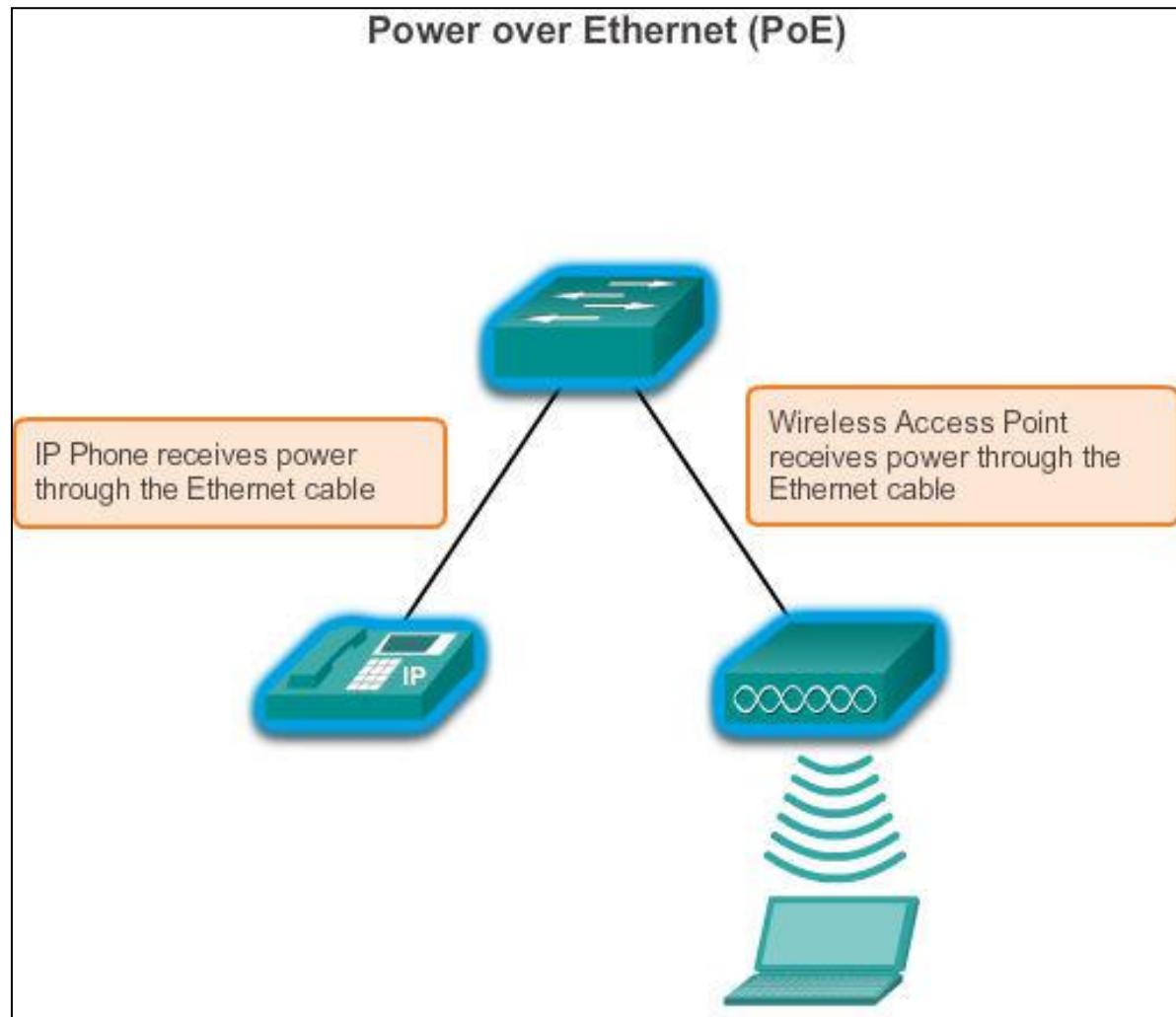
## Port-Based and Shared Memory Buffering

Port-based memory	In port-based memory buffering, frames are stored in queues that are linked to specific incoming and outgoing ports.
Shared memory	Shared memory buffering deposits all frames into a common memory buffer, which all the ports on the switch share.



Fixed or Modular

# Fixed versus Modular Configuration





Fixed or Modular

# Fixed versus Modular Configuration (cont.)

## Switch Form Factors

Fixed Configuration  
Switches



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

Modular Configuration  
Switches



Stackable Configuration Switches



The chassis accepts line cards that contain the ports.



# Fixed or Modular Module Options for Cisco Switch Slots

## SFP Modules



Cisco Optical Gigabit Ethernet SFP



Cisco 1000BASE-T Copper SFP



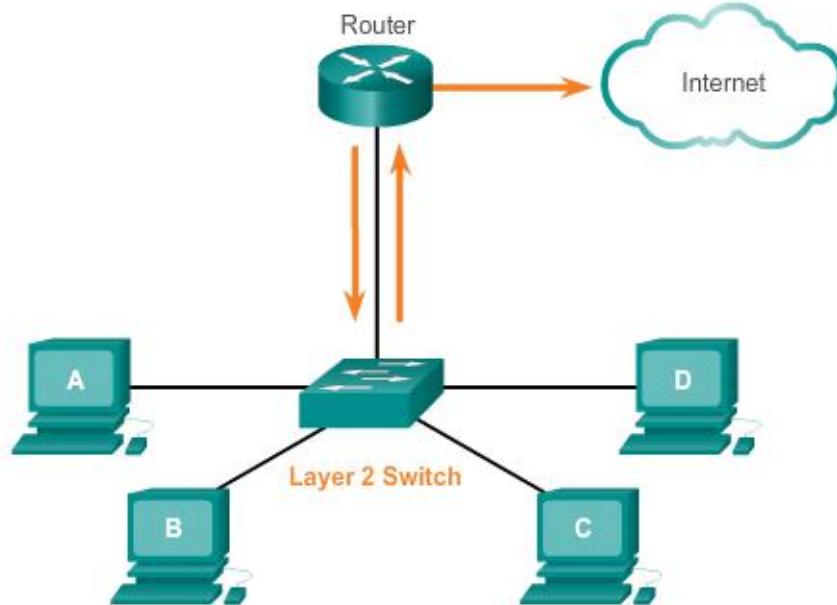
Cisco 2-channel 1000BASE-BX Optical SFP



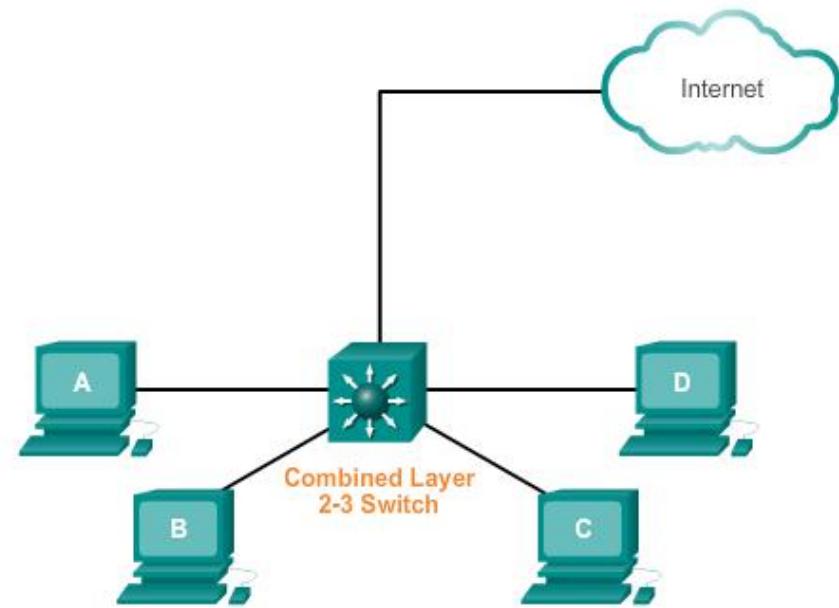
## Layer 3 Switching

# Layer 2 versus Layer 3 Switching

Layer 2 Switching



Layer 3 Switching





## Layer 3 Switching

# Cisco Express Forwarding

Cisco devices which support Layer 3 switching utilize Cisco Express Forwarding (CEF). Two main components of CEF operation are the:

- Forwarding Information Base (FIB)
  - Conceptually it is similar to a routing table.
  - A networking device uses this lookup table to make destination-based switching decisions during Cisco Express Forwarding operation.
  - Updated when changes occur in the network and contains all routes known at the time.
- Adjacency Tables
  - Maintain layer 2 next-hop addresses for all FIB entries.



## Layer 3 Switching

# Types of Layer 3 Interfaces

The major types of Layer 3 interfaces are:

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



## Layer 3 Switching

# Configuring a Routed Port on a Layer 3 Switch

### Routed Port Configuration

```
S1(config)#interface f0/6
S1(config-if)#no switchport
S1(config-if)#ip address 192.168.200.1 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#end
S1#
*Mar 1 00:15:40.115: %SYS-5-CONFIG_I: Configured from console by console
S1#show ip interface brief
Interface          IP-Address      OK? Method Status           Protocol
Vlan1              unassigned     YES unset administratively down down
FastEthernet0/1    unassigned     YES unset   down           down
FastEthernet0/2    unassigned     YES unset   down           down
FastEthernet0/3    unassigned     YES unset   down           down
FastEthernet0/4    unassigned     YES unset   down           down
FastEthernet0/5    unassigned     YES unset   down           down
FastEthernet0/6    192.168.200.1 YES manual up           up
FastEthernet0/7    unassigned     YES unset   up            up
FastEthernet0/8    unassigned     YES unset   up            up
<output omitted>
```



## Chapter 5 Summary

- Ethernet is the most widely used LAN technology used today.
- Ethernet standards define both the Layer 2 protocols and the Layer 1 technologies.
- The Ethernet frame structure adds headers and trailers around the Layer 3 PDU to encapsulate the message being sent.
- As an implementation of the IEEE 802.2/3 standards, the Ethernet frame provides MAC addressing and error checking.
- Replacing hubs with switches in the local network has reduced the probability of frame collisions in half-duplex links.
- The Layer 2 addressing provided by Ethernet supports unicast, multicast, and broadcast communications.
- Ethernet uses the Address Resolution Protocol to determine the MAC addresses of destinations and map them against known Network layer addresses.



## Chapter 5

# Summary (cont.)

- Each node on an IP network has both a MAC address and an IP address.
- The ARP protocol resolves IPv4 addresses to MAC addresses and maintains a table of mappings.
- A Layer 2 switch builds a MAC address table that it uses to make forwarding decisions.
- Layer 3 switches are also capable of performing Layer 3 routing functions, reducing the need for dedicated routers on a LAN.
- Layer 3 switches have specialized switching hardware so they can typically route data as quickly as they can switch.

# Cisco | Networking Academy®

Mind Wide Open™



## Chapter 6: Network Layer



## Introduction to Networks

Cisco | Networking Academy®  
Mind Wide Open™



# Chapter 6: Objectives

In this chapter, you will be able to:

- Explain how network layer protocols and services support communications across data networks.
- Explain how routers enable end-to-end connectivity in a small-to-medium-sized business network.
- Determine the appropriate device to route traffic in a small-to-medium-sized business network.
- Configure a router with basic configurations.



# Chapter 6

6.1 Network Layer Protocols

6.2 Routing

6.3 Routers

6.4 Configuring a Cisco Router

6.5 Summary

## 6.1 Network Layer Protocols





## Network Layer in Communication

# The Network Layer

The network layer, or OSI Layer 3, provides services to allow end devices to exchange data across the network. To accomplish this end-to-end transport, the network layer uses four basic processes:

- Addressing end devices
- Encapsulation
- Routing
- De-encapsulating



# Network Layer in Communication

# Network Layer Protocols

**Common network layer protocols include:**

- IP version 4 (IPv4)
- IP version 6 (IPv6)

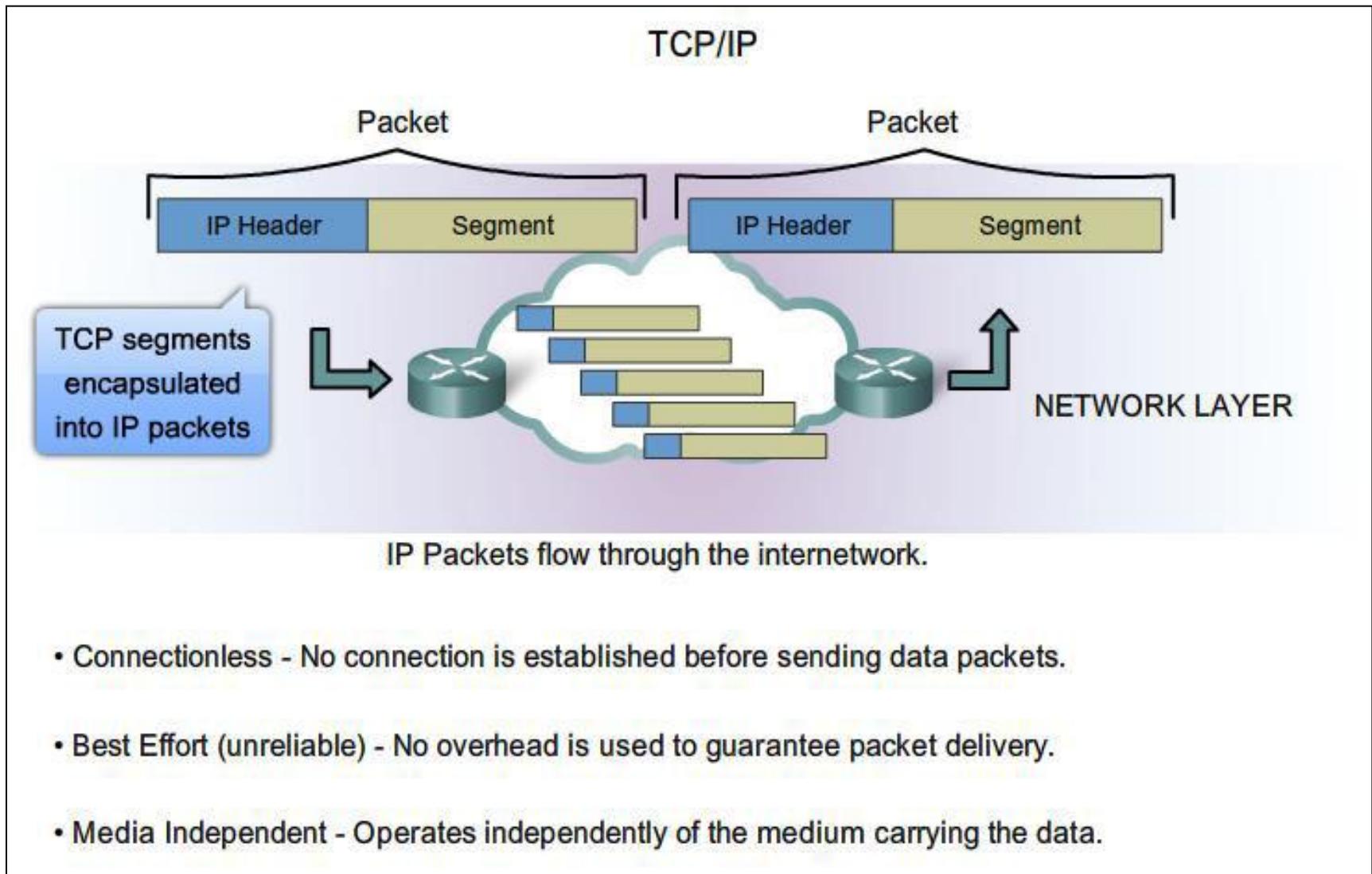
**Legacy network layer protocols include:**

- Novell Internetwork Packet Exchange (IPX)
- AppleTalk
- Connectionless Network Service (CLNS/DECNet)



# IP Characteristics

# IP Components

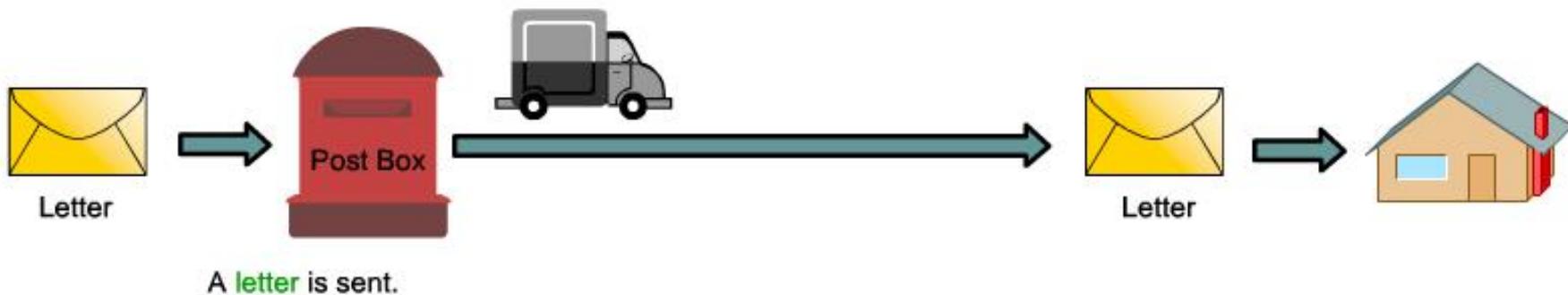




# Characteristics of the IP protocol

## IP - Connectionless

### Connectionless Communication



The sender doesn't know:

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

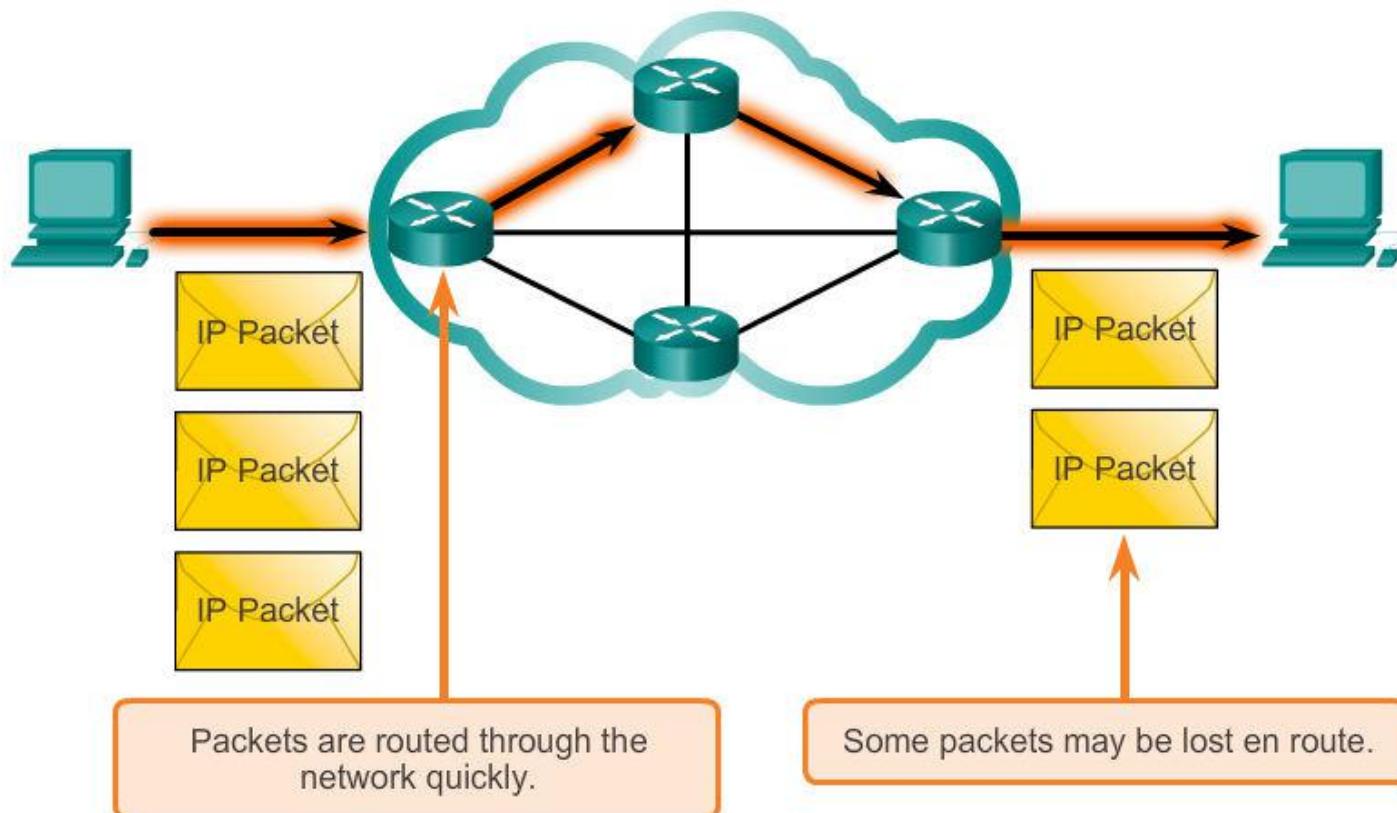
The receiver doesn't know:

- when it is coming



# Characteristics of the IP protocol

## Best Effort Delivery

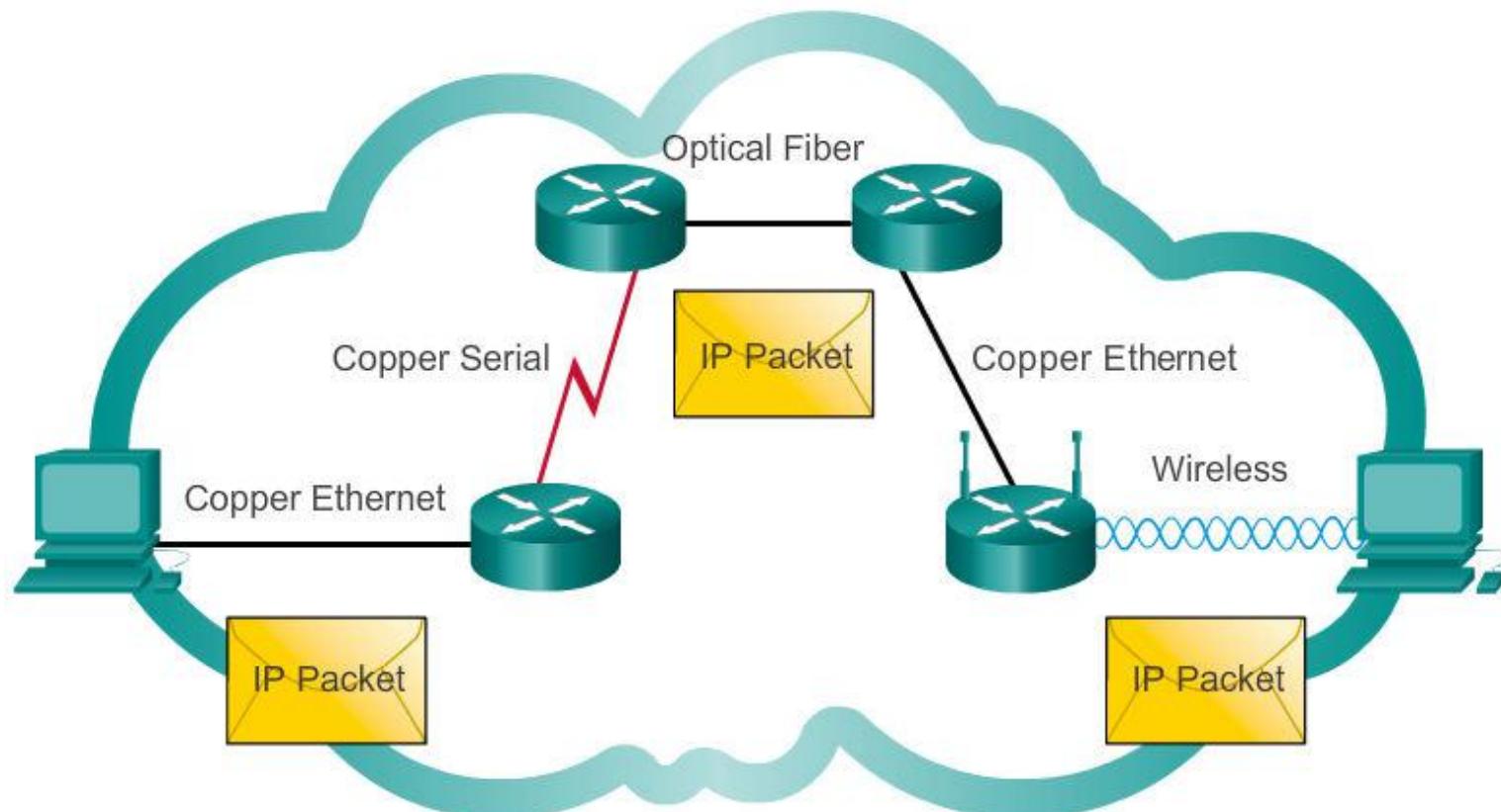


As an unreliable network layer protocol, IP does not guarantee that all sent packets will be received. Other protocols manage the process of tracking packets and ensuring their delivery.



# Characteristics of the IP protocol

## IP – Media Independent



IP packets can travel over different media.

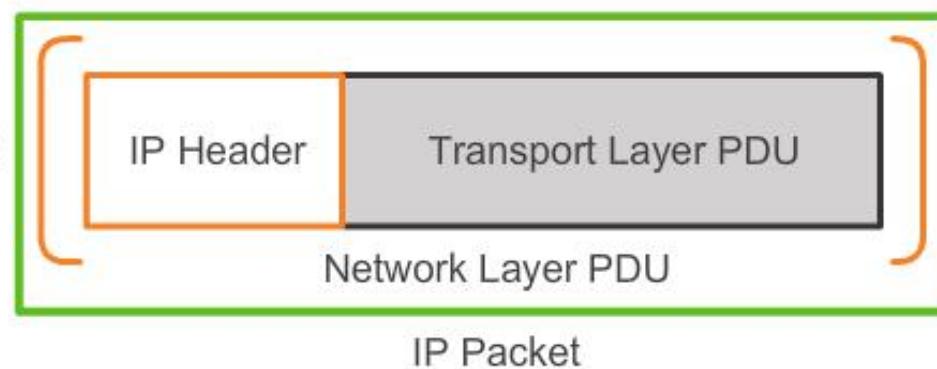


# IPv4 Packet Encapsulating IP

Transport Layer  
Encapsulation



Network Layer Encapsulation



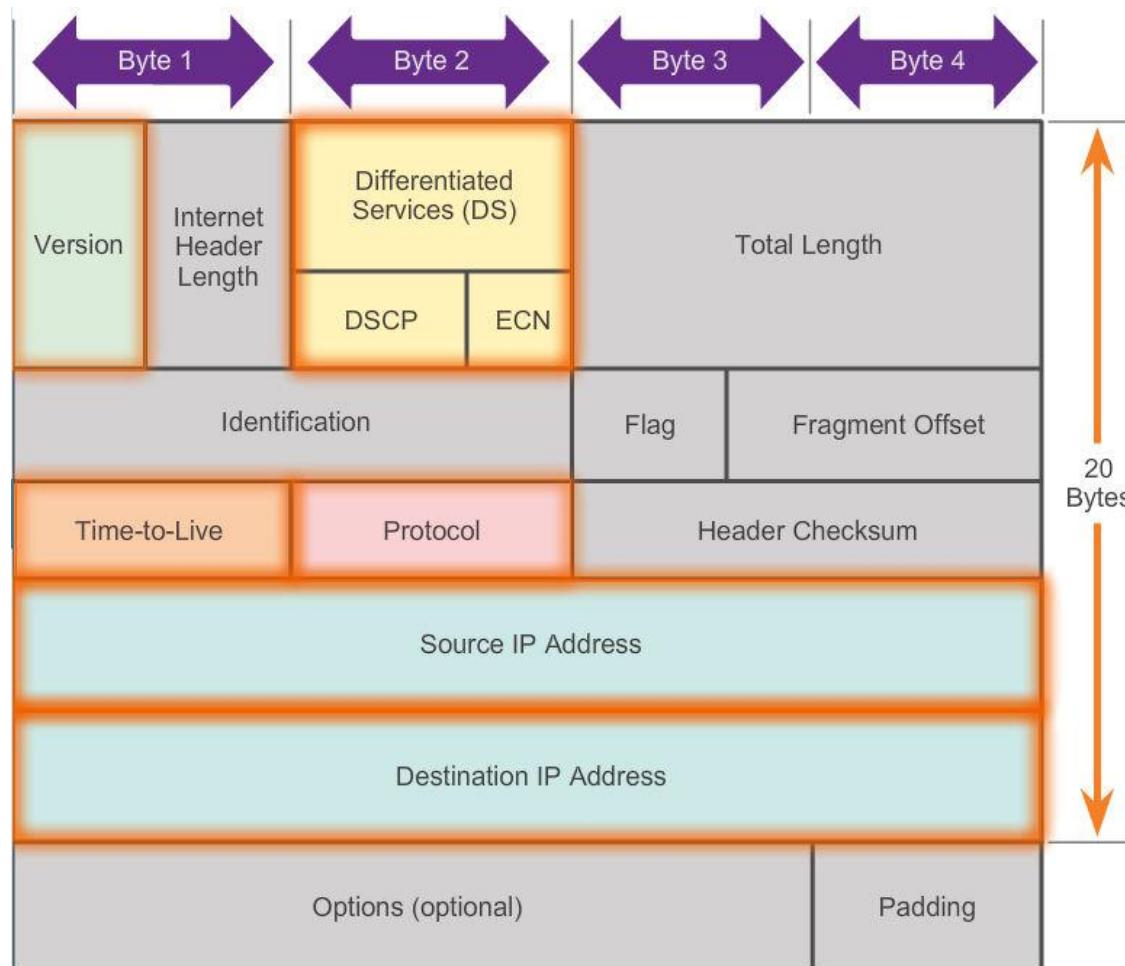
The network layer adds a header so packets can be routed through complex networks and reach their destination. In TCP/IP based networks, the network layer PDU is the IP packet.



## IPv4 Packet

# IPv4 Packet Header

Contents of the IPv4 packet header

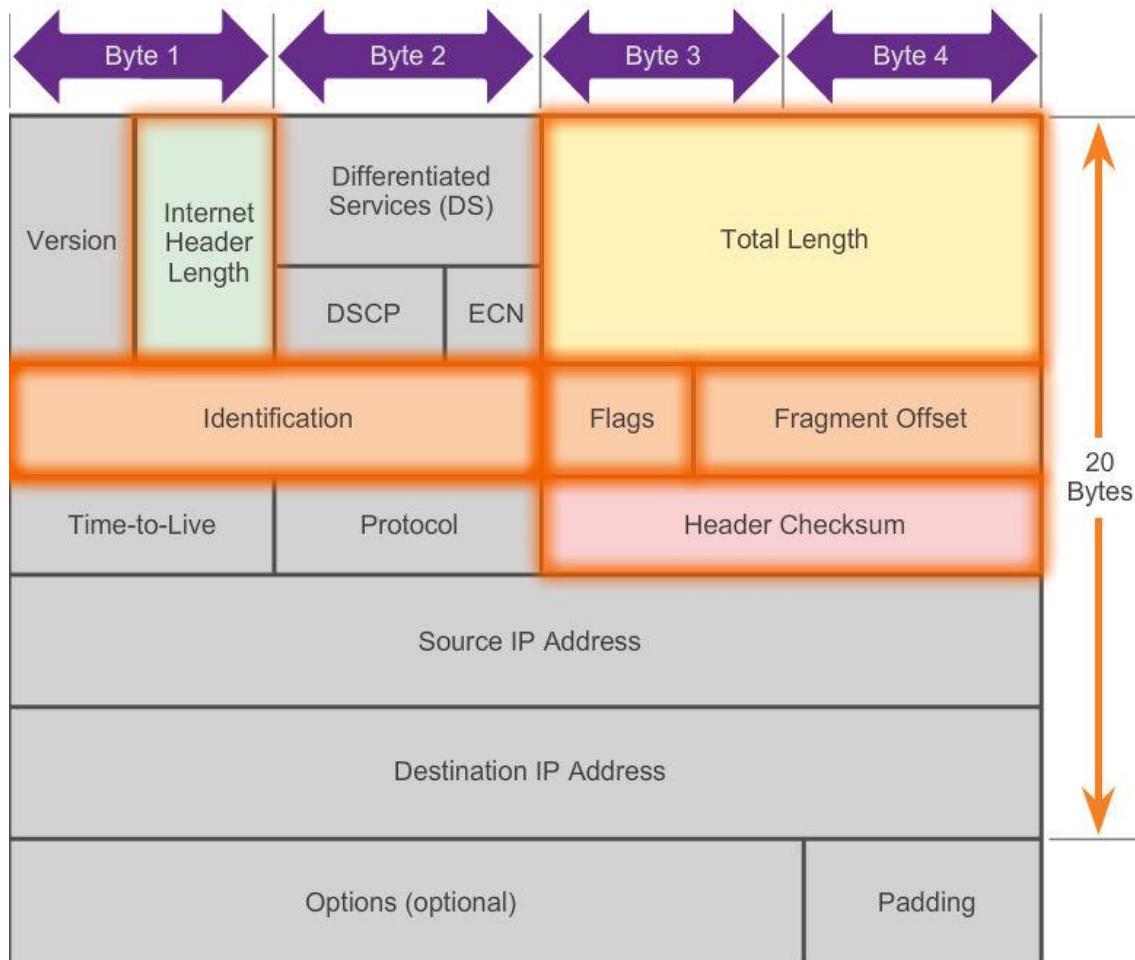




## IPv4 Packet

# IPv4 Header Fields

### Contents of the IPv4 header fields





# IPv4 Packet Sample IPv4 Headers

Microsoft: \Device\NPF\_{7BB3C130-30C5-4419-B79E-C0868085ABED} [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
16	3.64050300	192.168.1.109	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128
17	3.64506800	192.168.1.1	192.168.1.109	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=64
18	3.68215500	192.168.1.109	38.112.107.53	TCP	54	55502 > https [ACK] Seq=1 Ack=134 Win=16661 Len=0
19	4.19945400	fe80::15ff:98d8:d28ff02:c		SSDP	208	M-SEARCH * HTTP/1.1
20	4.60748800	fe80::15ff:98d8:d28fe80::b1ee:c4ae:a11		SSDP	453	HTTP/1.1 200 OK
21	4.64229900	192.168.1.109	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128
22	4.64509200	192.168.1.1	192.168.1.109	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=64
23	4.73605200	192.168.1.109	255.255.255.255	DB-LSP-	154	Dropbox LAN sync Discovery Protocol

+ Frame 16: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

+ Ethernet II, Src: Intelcor\_45:5d:c4 (24:77:03:45:5d:c4), Dst: Cisco-Li\_a0:d1:be (00:18:39:a0:d1:be)

- Internet Protocol Version 4, src: 192.168.1.109 (192.168.1.109), dst: 192.168.1.1 (192.168.1.1)

- Version: 4
- Header length: 20 bytes
- Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
- Total Length: 60
- Identification: 0x3704 (14084)
- Flags: 0x00
- Fragment offset: 0
- Time to live: 128
- Protocol: ICMP (1)
- Header checksum: 0x7ffe [correct]
- Source: 192.168.1.109 (192.168.1.109)
- Destination: 192.168.1.1 (192.168.1.1)
- [Source GeoIP: Unknown]
- [Destination GeoIP: Unknown]

+ Internet Control Message Protocol

Hex	Dec	Text
0000	00 18 39 a0 d1 be 24 77	03 45 5d c4 08 00 45 00 ..9...\$w .E]...E.
0010	00 3c 37 04 00 00 80 01	7f fe c0 a8 01 6d c0 a8 .<7..... ....m..
0020	01 01 08 00 4d 56 00 01	00 05 61 62 63 64 65 66 ...MV... ..abcdef
0030	67 68 69 6a 6b 6c 6d 6e	6f 70 71 72 73 74 75 76 ghiijklmn oprrstuv
0040	77 61 62 63 64 65 66 67	68 69 wabcdefg hi

Internet Protocol Version 4 (ip), 20 bytes

Packets: 35 Displayed: 35 Marked: 0 Dropped: 0

Profile: Default



# Network Layer in Communication

## Limitations of IPv4

- IP Address depletion
- Internet routing table expansion
- Lack of end-to-end connectivity





# Network Layer in Communication

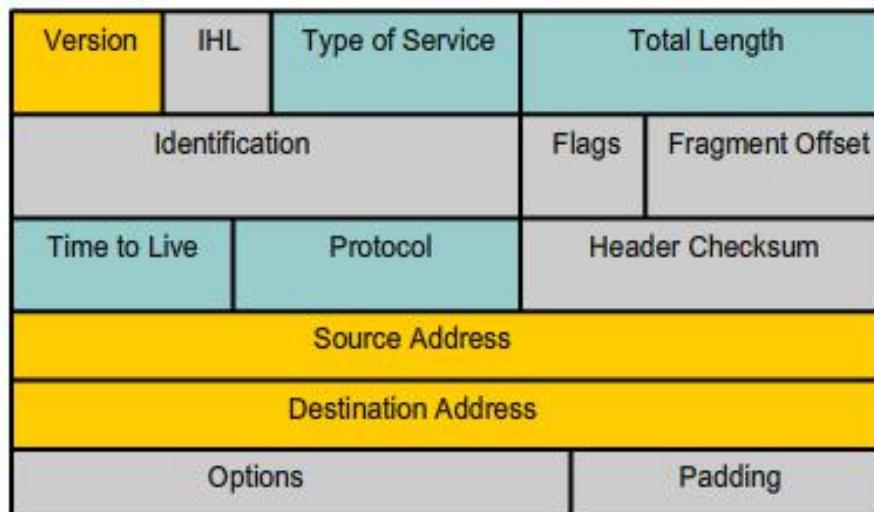
## Introducing IPv6



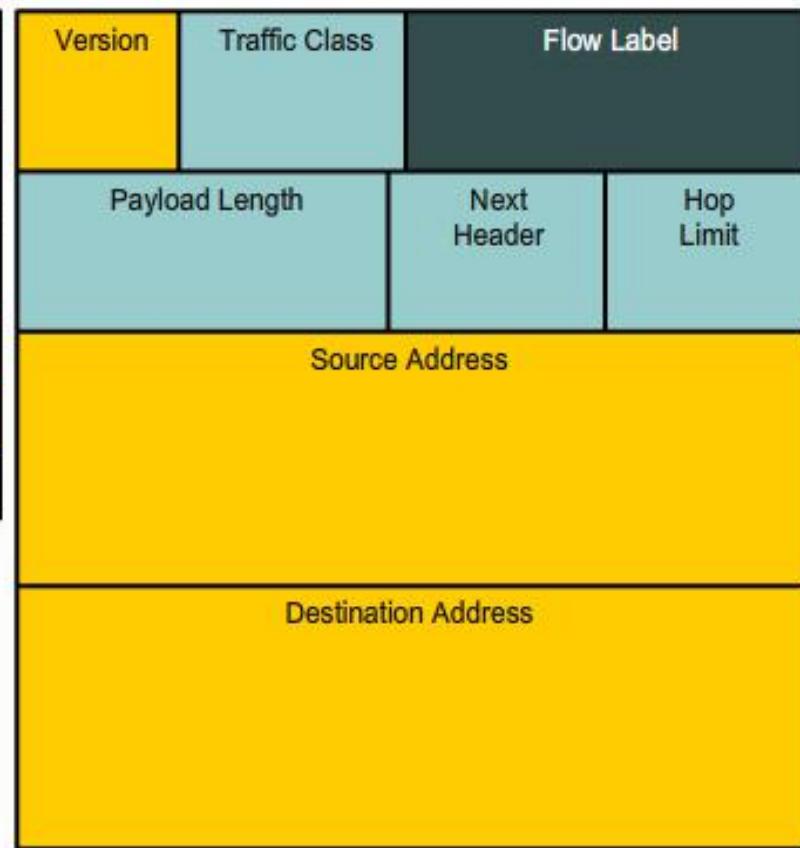
# IPv6 Packet Encapsulating IPv6

IPv4 and IPv6 Headers

IPv4 Header



IPv6 Header



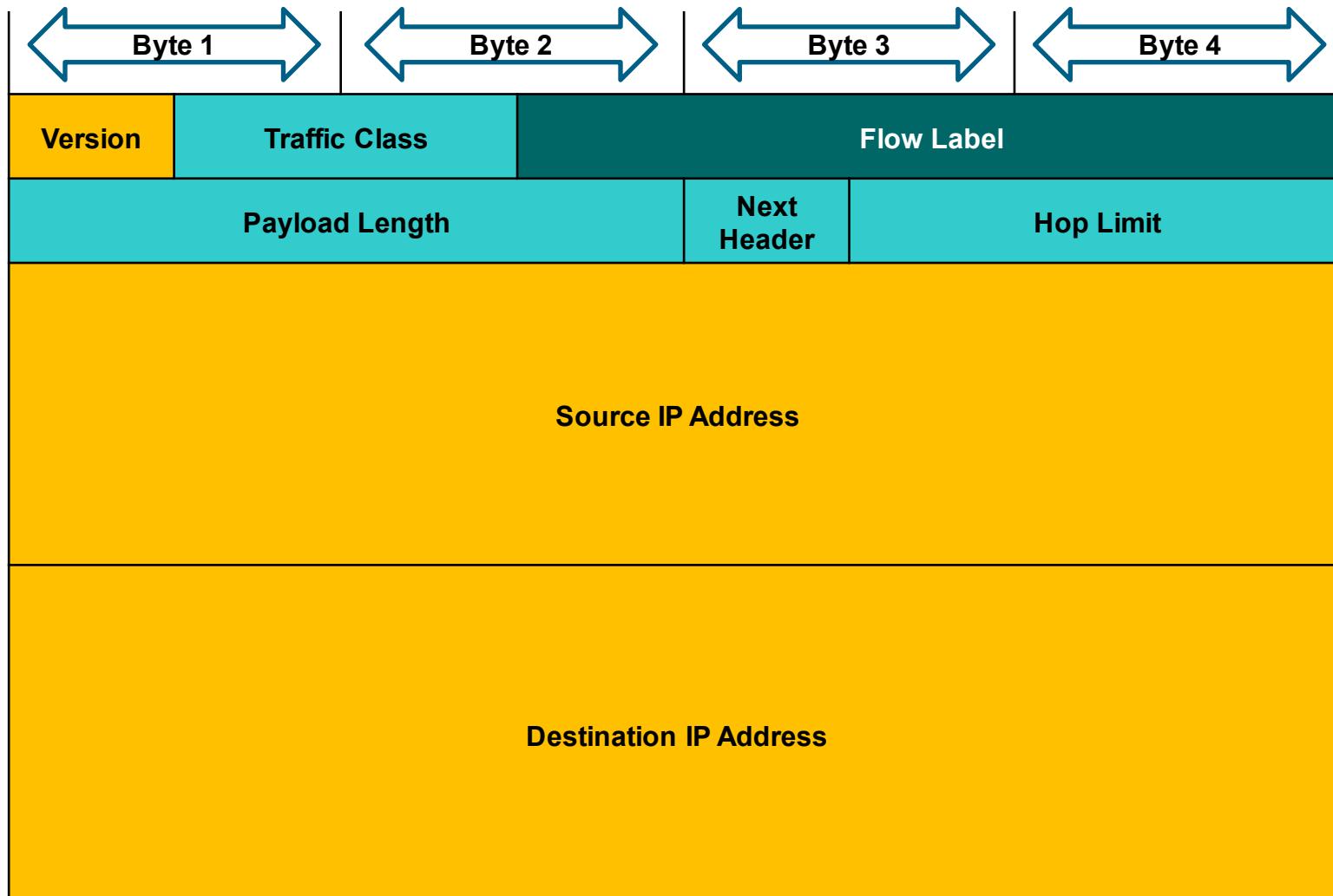
Legend

- Field names kept from IPv4 to IPv6
- Fields not kept in IPv6
- Name & position changed in IPv6
- New field in IPv6



## IPv6 Packet

# IPv6 Packet Header





# IPv6 Packet Sample IPv6 Header

**v6-http.cap [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)]**

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
47	325.030878	2001:6f8:900:7c0::2	2001:6f8:102d:0:2d0	TCP	82	http > 59201 [SYN, ACK] Seq=0 Ack=1 Win=64
48	325.031166	2001:6f8:102d:0:2d0:9ff:fee	2001:6f8:900:7c0::2	TCP	74	59201 > http [ACK] Seq=1 Ack=1 Win=5760 L
49	325.040411	2001:6f8:102d:0:2d0:9ff:fee	2001:6f8:900:7c0::2	HTTP	314	GET / HTTP/1.0
50	325.045496	2001:6f8:900:7c0::2	2001:6f8:102d:0:2d0	TCP	1506	[TCP segment of a reassembled PDU]
51	325.045525	2001:6f8:900:7c0::2	2001:6f8:102d:0:2d0	HTTP	901	HTTP/1.1 200 OK (text/html)
52	325.045627	2001:6f8:900:7c0::2	2001:6f8:102d:0:2d0	TCP	74	http > 59201 [FIN, ACK] Seq=2260 Ack=241

Frame 49: 314 bytes on wire (2512 bits), 314 bytes captured (2512 bits)  
**Ethernet II, Src: HsingTec\_e3:e8:de (00:d0:09:e3:e8:de), Dst: Ibm\_82:95:b5 (00:11:25:82:95:b5)**  
**Internet Protocol version 6, Src: 2001:6f8:102d:0:2d0:9ff:fee3:e8de (2001:6f8:102d:0:2d0:9ff:fee3:e8de), Dst: 2001:6f8**  
 0110 .... = Version: 6  
 .... 0000 0000 .... .... .... = Traffic class: 0x00000000  
 .... .... 0000 0000 0000 0000 = Flowlabel: 0x00000000  
 Payload length: 260  
 Next header: TCP (6)  
 Hop limit: 64  
 Source: 2001:6f8:102d:0:2d0:9ff:fee3:e8de (2001:6f8:102d:0:2d0:9ff:fee3:e8de)  
 [Source SA MAC: HsingTec\_e3:e8:de (00:d0:09:e3:e8:de)]  
 Destination: 2001:6f8:900:7c0::2 (2001:6f8:900:7c0::2)  
 [Source GeoIP: Unknown]  
 [Destination GeoIP: Unknown]  
**Transmission Control Protocol, Src Port: 59201 (59201), Dst Port: http (80), seq: 1, Ack: 1, Len: 240**  
**Hypertext Transfer Protocol**

0000	00 11 25 82 95 b5 00 d0 09 e3 e8 de 86 dd 60 00	..%....@.....
0010	00 00 01 04 06 40 20 01 06 f8 10 2d 00 00 02 d0	.....@.....
0020	09 ff fe e3 e8 de 20 01 06 f8 09 00 07 c0 00 00	.....A.P..a.J
0030	00 00 00 00 00 02 e7 41 00 50 ab dc d6 61 01 4a	s.P....H ..GET /
0040	73 9f 50 18 16 80 f4 48 00 00 47 45 54 20 2f 20	HTTP/1.0 ..Host:
0050	48 54 54 50 2f 31 2e 30 0d 0a 48 6f 73 74 3a 20	c1-1985. ham-01.d
0060	63 6c 2d 31 39 38 35 2e 68 61 6d 2d 30 31 2e 64	e.sixxs. net..Acc
0070	65 2e 73 69 78 78 73 2e 6e 65 74 0d 0a 41 63 63	

Internet Protocol Version 6 (ipv6), 40 bytes  
 Packets: 55 Displayed: 55 Marked: 0 Profile: Default

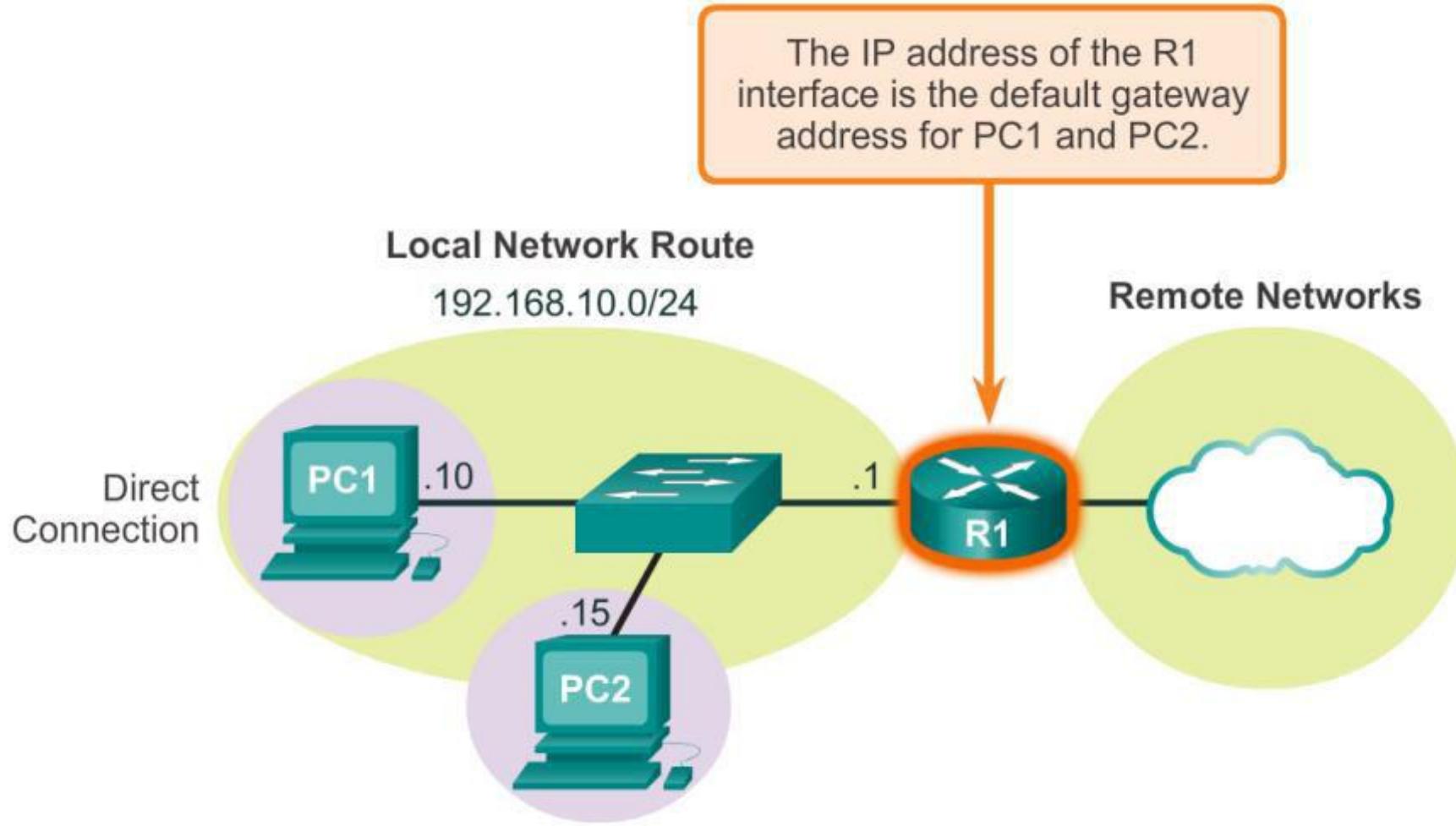
## 6.2 Routing





## Host Routing Tables

# Host Packet Forwarding Decision





## Host Routing Tables Default Gateway

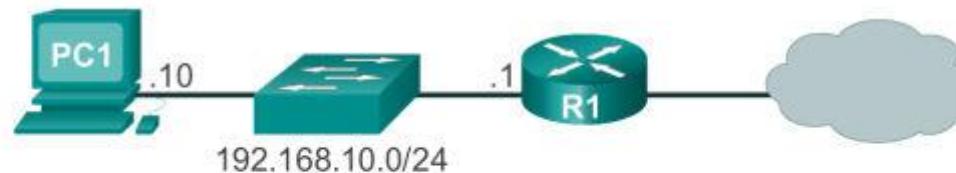
Hosts must maintain their own, local, routing table to ensure that network layer packets are directed to the correct destination network. The local table of the host typically contains:

- Direct connection
- Local network route
- Local default route



# Host Routing Tables

## IPv4 Host Routing Table



```
C:\Users\PC1>netstat -r
```

<Output omitted>

### IPv4 Route Table

#### Active Routes:

Network	Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.10.1	192.168.10.10	25	
127.0.0.0	255.0.0.0	On-link	127.0.0.1	306	
127.0.0.1	255.255.255.255	On-link	127.0.0.1	306	
127.255.255.255	255.255.255.255	On-link	127.0.0.1	306	
192.168.10.0	255.255.255.0	On-link	192.168.10.10	281	
192.168.10.10	255.255.255.255	On-link	192.168.10.10	281	
192.168.10.255	255.255.255.255	On-link	192.168.10.10	281	
224.0.0.0	240.0.0.0	On-link	127.0.0.1	306	
224.0.0.0	240.0.0.0	On-link	192.168.10.10	281	
255.255.255.255	255.255.255.255	On-link	127.0.0.1	306	
255.255.255.255	255.255.255.255	On-link	192.168.10.10	281	

<Output omitted>



## Host Routing Tables

# Sample IPv4 Host Routing Table

The network diagram illustrates a simple topology. On the left, a computer icon labeled "PC1" is connected to a teal-colored switch. The switch is connected to a router icon labeled "R1". Router R1 has a route to a destination represented by a cloud containing a computer icon with the IP address "10.10.10.10". Below the switch, the subnet mask "192.168.10.0/24" is displayed.

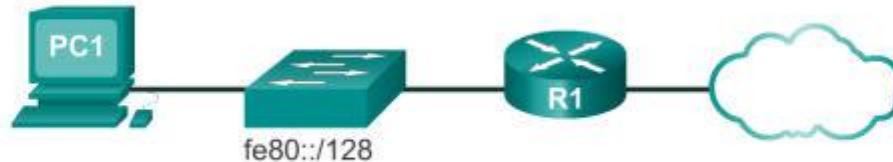
```
C:\Users\PC1> netstat -r
<Output omitted>
IPv4 Route Table
=====
Active Routes:
Network Destination      Netmask     Gateway       Interface Metric
          0.0.0.0      0.0.0.0  192.168.10.1  192.168.10.10    25
        127.0.0.0    255.0.0.0   On-link      127.0.0.1    306
        127.0.0.1  255.255.255.255   On-link      127.0.0.1    306
  127.255.255.255  255.255.255.255   On-link      127.0.0.1    306
        192.168.10.0  255.255.255.0   On-link    192.168.10.10   281
        192.168.10.10 255.255.255.255   On-link    192.168.10.10   281
        192.168.10.255 255.255.255.255   On-link    192.168.10.10   281
        224.0.0.0    240.0.0.0   On-link      127.0.0.1    306
        224.0.0.0    240.0.0.0   On-link    192.168.10.10   281
      255.255.255.255 255.255.255.255   On-link      127.0.0.1    306
      255.255.255.255 255.255.255.255   On-link    192.168.10.10   281
<Output omitted>
```



## Host Routing Tables

# Sample IPv6 Host Routing Table

fe80::2c30:3071:e718:a926/128  
2001:db8:9d38:953c:2c30:3071:e718:a926/128



```
C:\Users\PC1> netstat -r
```

<Output omitted>

### IPv6 Route Table

#### Active Routes:

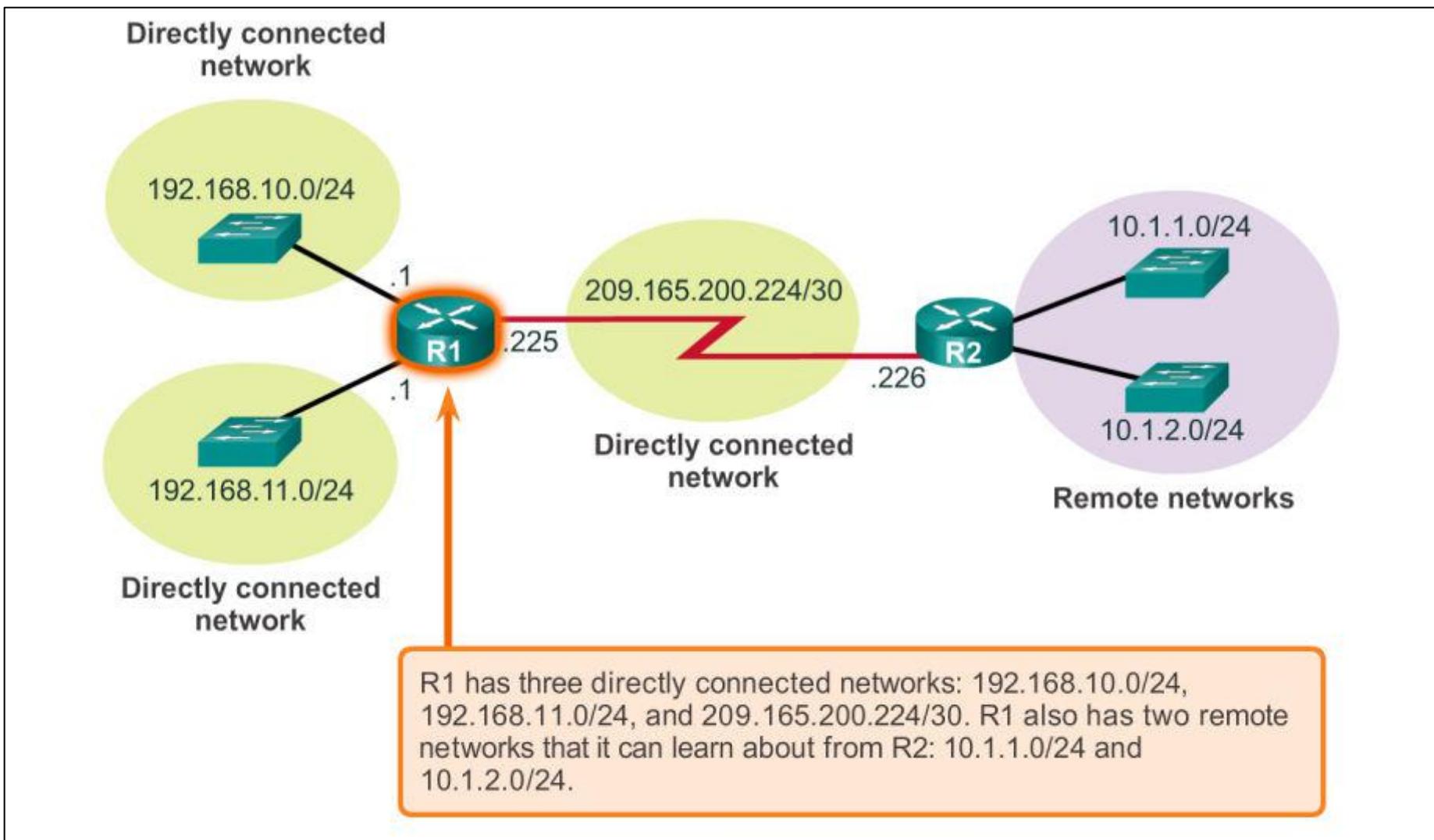
If	Metric	Network	Destination	Gateway
16	58	::/0		On-link
1	306	::1/128		On-link
16	58	2001::/32		On-link
16	306	2001:0:9d38:953c:2c30:3071:e718:a926/128		On-link
15	281	fe80::/64		On-link
16	306	fe80::/64		On-link
16	306	fe80::2c30:3071:e718:a926/128		On-link
15	281	fe80::blee:c4ae:a117:271f/128		On-link
1	306	ff00::/8		On-link
16	306	ff00::/8		On-link
15	281	ff00::/8		On-link

<Output omitted>



# Router Routing Tables

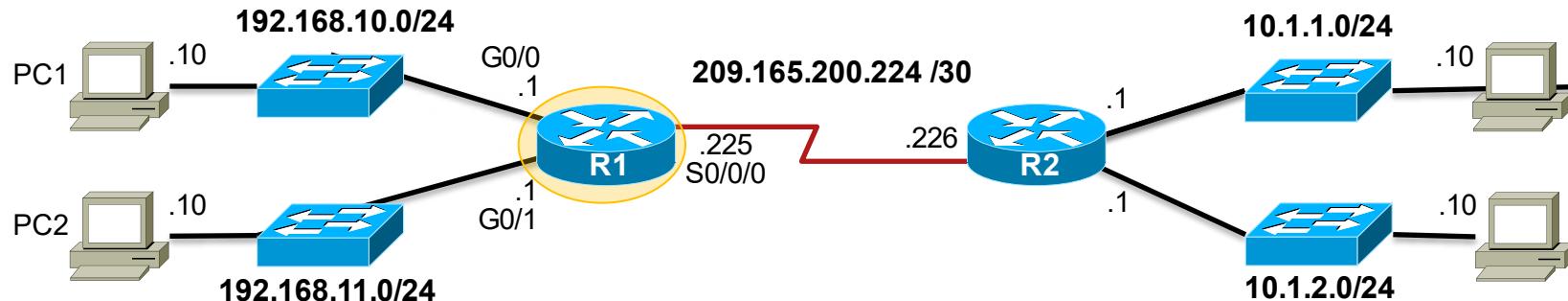
# Router Packet Forwarding Decision





# Router Routing Tables

## IPv4 Router Routing Table



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

```

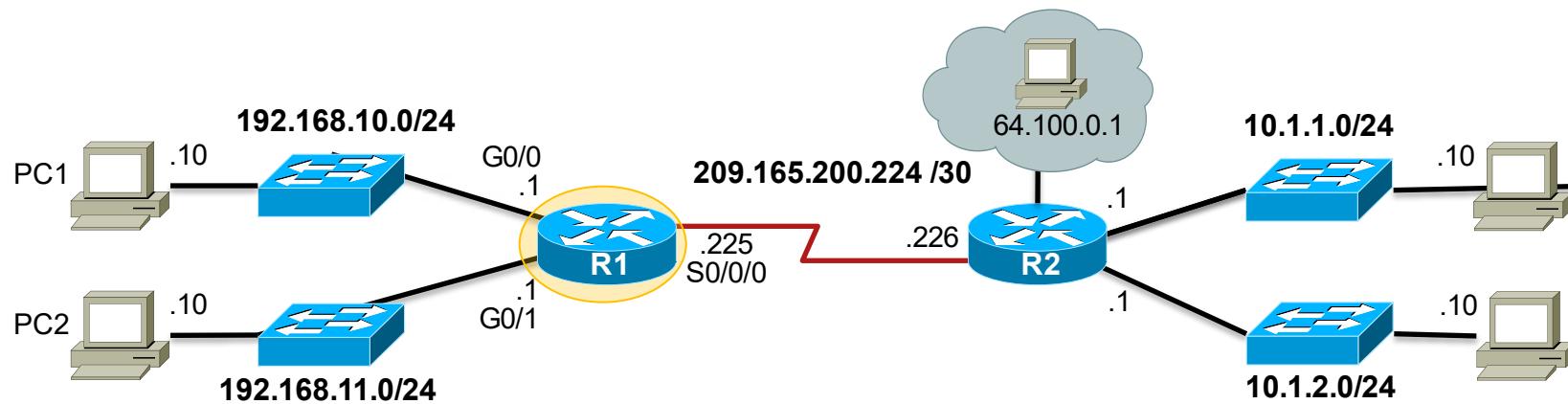
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D      10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05, Serial0/0/0
D      10.1.2.0/24 [90/2170112] via 209.165.200.226, 00:00:05, Serial0/0/0
192.168.10.0/24 is variably subnetted, 2 subnets, 3 masks
C      192.168.10.0/24 is directly connected, GigabitEthernet0/0
L      192.168.10.1/32 is directly connected, GigabitEthernet0/0
192.168.11.0/24 is variably subnetted, 2 subnets, 3 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, 3 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#

```



## Router Routing Tables

# Directly Connected Routing Table Entries

**A**C  
L

192.168.10.0/24 is directly connected, GigabitEthernet0/0  
192.168.10.1/32 is directly connected, GigabitEthernet0/0

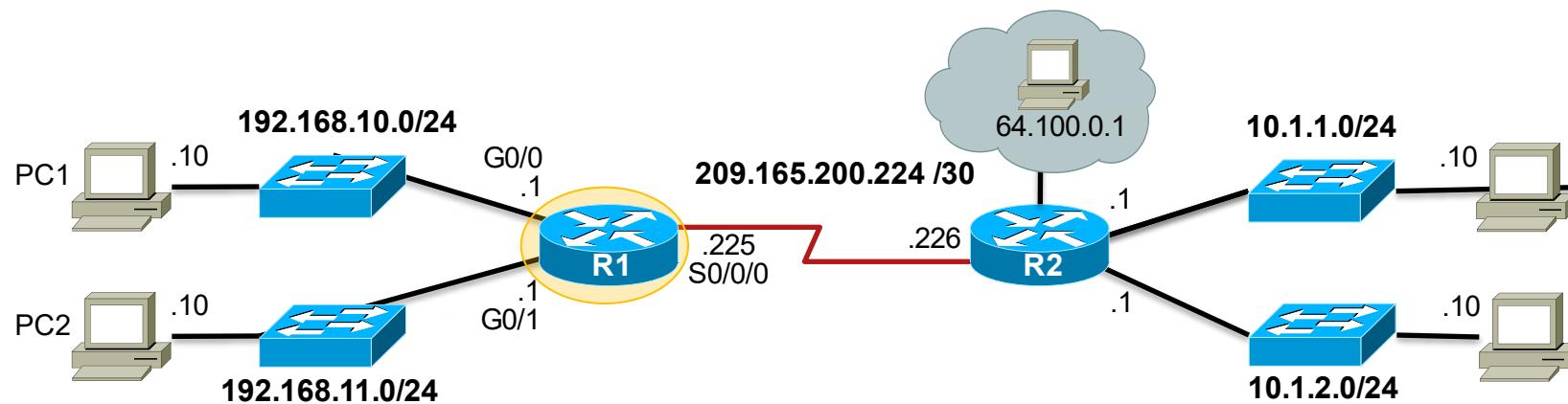
**C****B**

<b>A</b>	Identifies how the network was learned by the router.
<b>B</b>	Identifies the destination network and how it is connected.
<b>C</b>	Identifies the interface on the router connected to the destination network.



# Router Routing Tables

## Remote Network Routing Table Entries

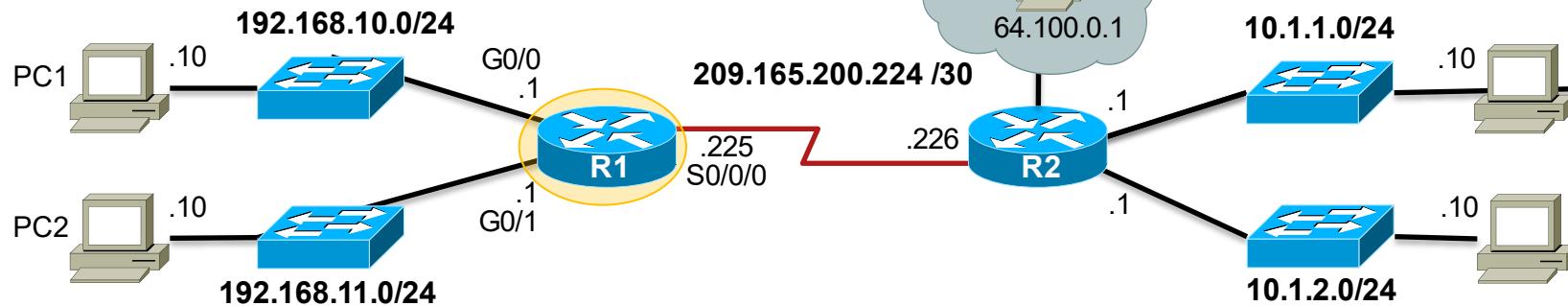


D	10.1.1.0/24	[90/2170112]	via	209.165.200.226, 00:00:05,	Serial0/0/0
---	-------------	--------------	-----	----------------------------	-------------

A	Identifies how the network was learned by the router.
B	Identifies the destination network.
C	Identifies the administrative distance (trustworthiness) of the route source.
D	Identifies the metric to reach the remote network.
E	Identifies the next hop IP address to reach the remote network.
F	Identifies the amount of elapsed time since the network was discovered.
G	Identifies the outgoing interface on the router to reach the destination network.



# Router Routing Tables Next-Hop Address



```
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, Serial0/0/0
D        10.1.2.0/24 [90/2170112] via 209.165.200.226, 00:00:05, Serial0/0/0
      192.168.10.0/24 is variably subnetted, 2 subnets, 3 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, 3 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, 3 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#
```

## 6.3 Routers



Cisco | Networking Academy®  
Mind Wide Open™



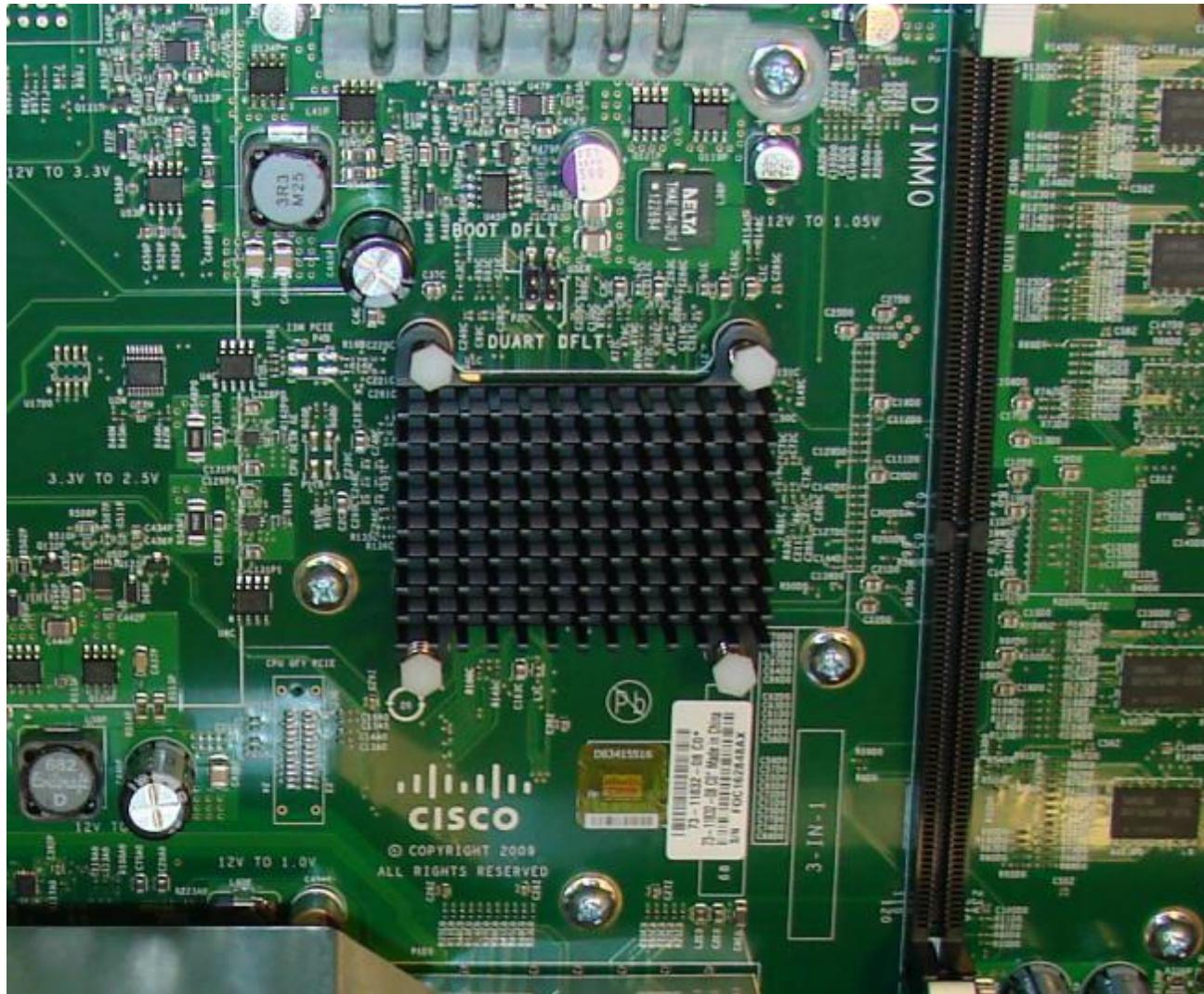
# Anatomy of a Router

# A Router is a Computer





# Anatomy of a Router Router CPU and OS





# Anatomy of a Router

## Router Memory

Memory	Volatile / Non-Volatile	Stores
RAM	Volatile	<ul style="list-style-type: none"><li>• Running IOS</li><li>• Running configuration file</li><li>• IP routing and ARP tables</li><li>• Packet buffer</li></ul>
ROM	Non-Volatile	<ul style="list-style-type: none"><li>• Bootup instructions</li><li>• Basic diagnostic software</li><li>• Limited IOS</li></ul>
NVRAM	Non-Volatile	<ul style="list-style-type: none"><li>• Startup configuration file</li></ul>
Flash	Non-Volatile	<ul style="list-style-type: none"><li>• IOS</li><li>• Other system files</li></ul>



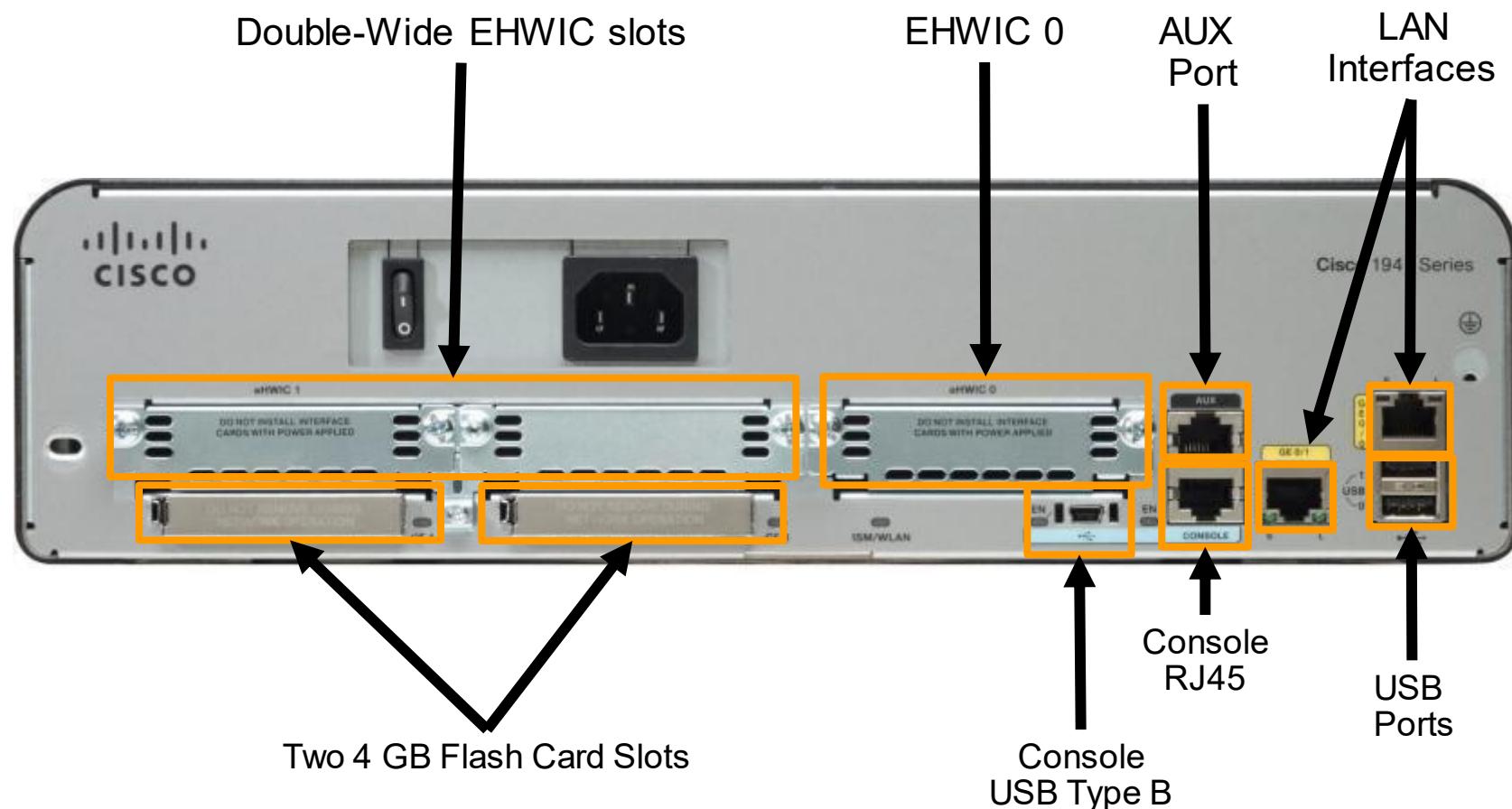
# Anatomy of a Router Inside a Router

1. Power Supply
2. Shield for WIC
3. Fan
4. SDRAM
5. NVRAM
6. CPU
7. Advanced Integration Module (AIM)



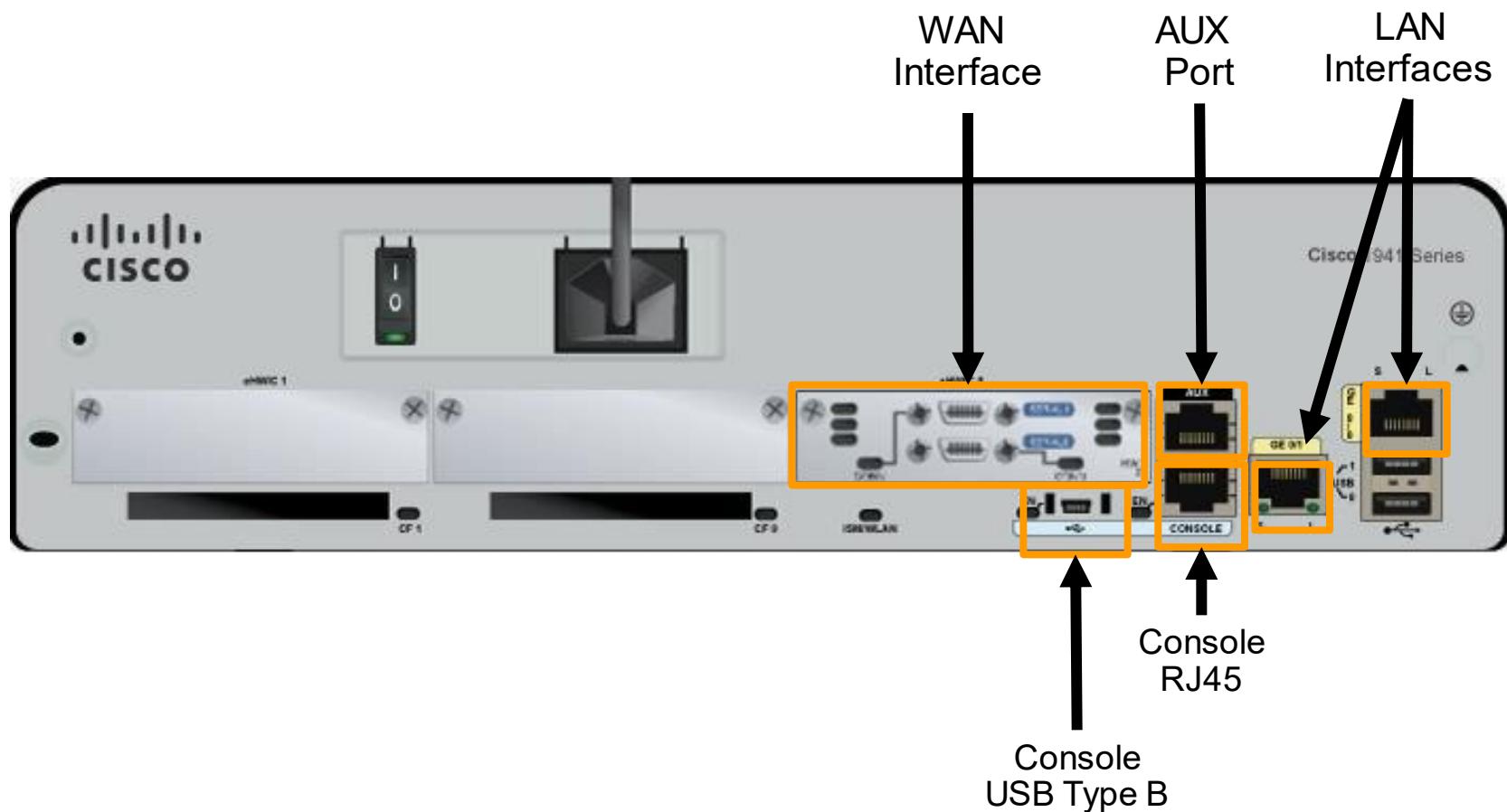


# Anatomy of a Router Router Backplane





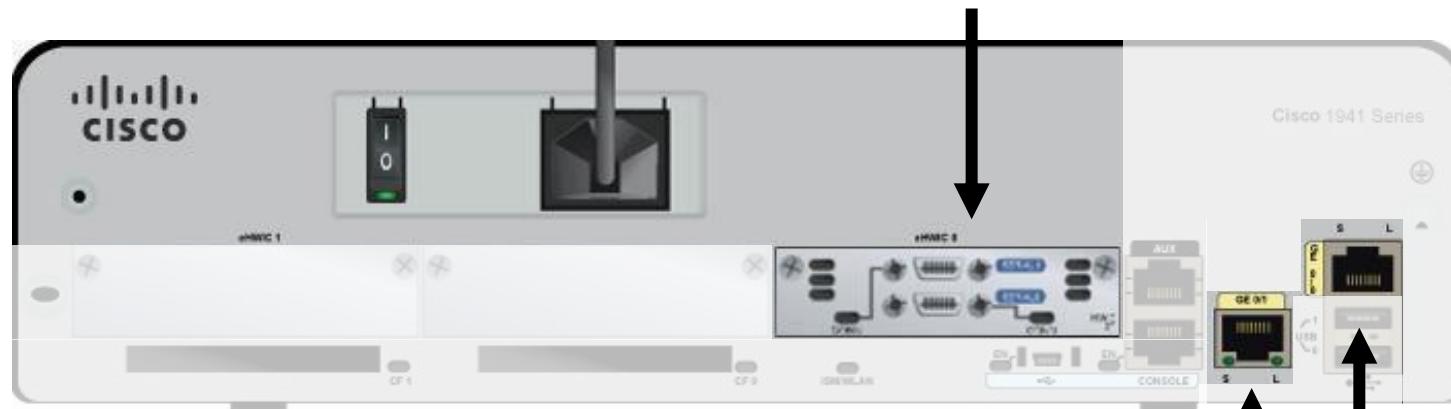
# Anatomy of a Router Connecting to a Router





# Anatomy of a Router LAN and WAN Interfaces

Serial Interfaces



LAN Interfaces



# Router Boot-up

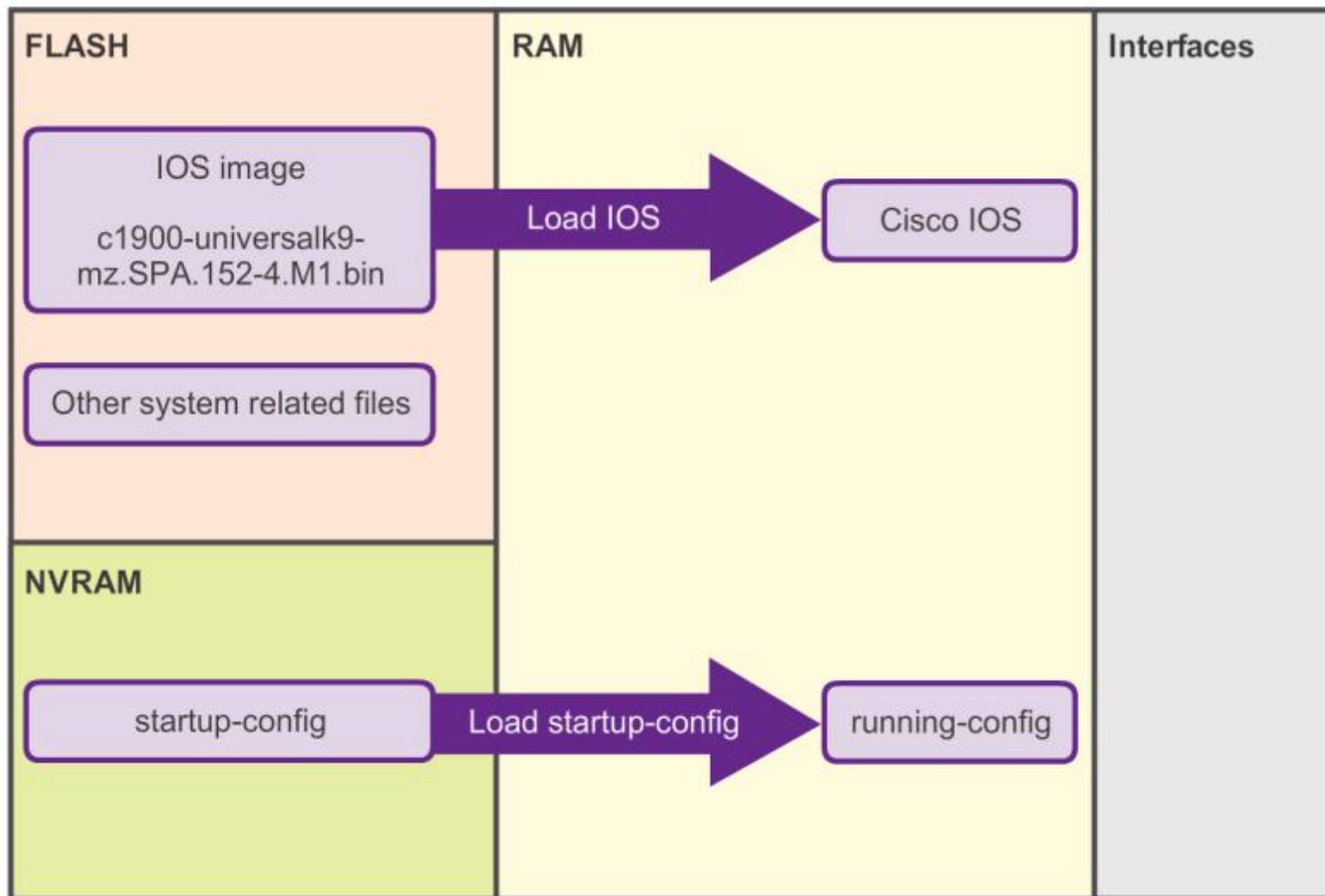
# Cisco IOS

The Cisco IOS operational details vary on different internetworking devices, depending on the device's purpose and feature set. However, Cisco IOS for routers provides the following:

- Addressing
- Interfaces
- Routing
- Security
- QoS
- Resources Management



# Router Boot-up Bootset Files

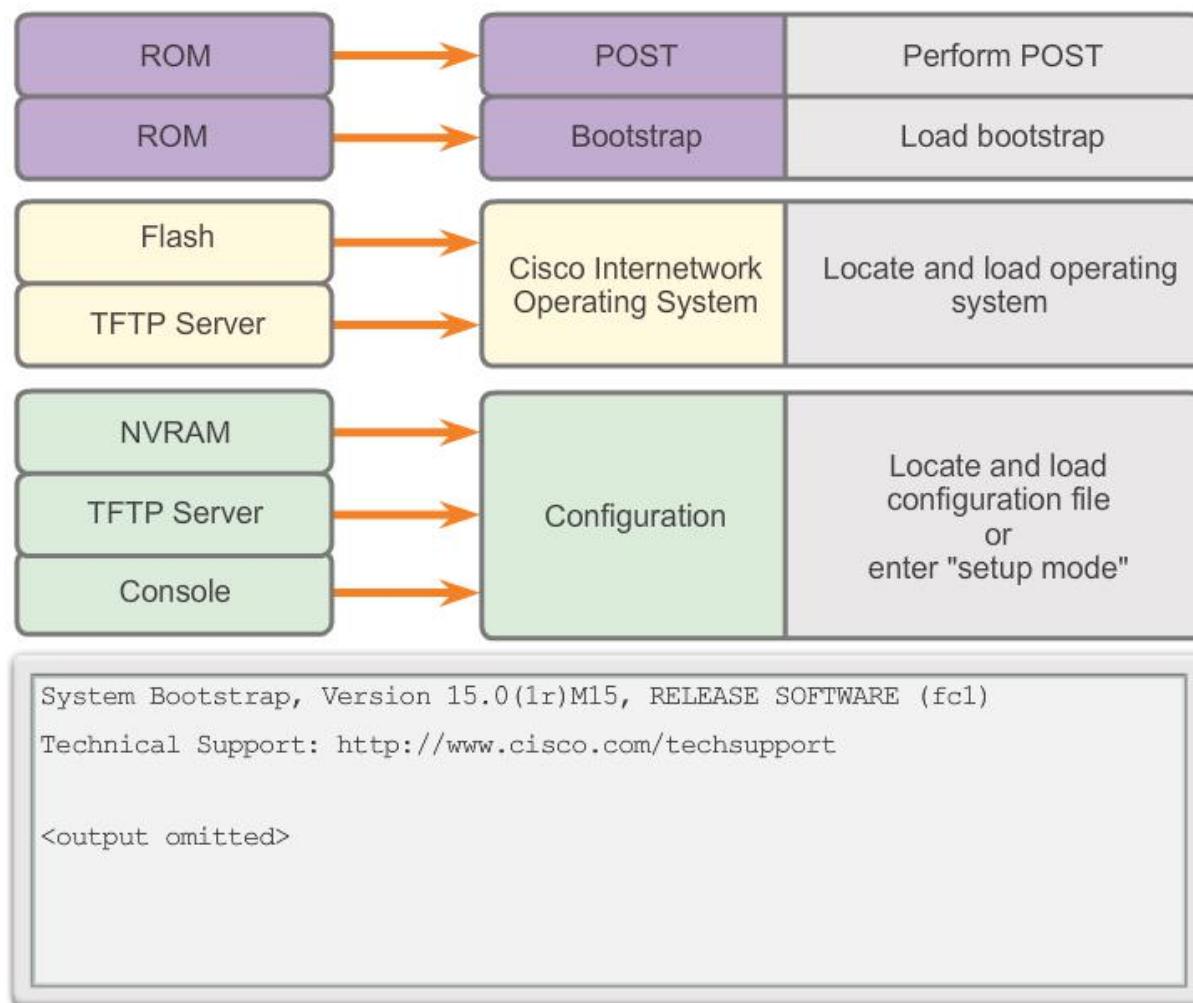




## Router Boot-up

# Router Bootup Process

### How a Router Boots Up





# Router Boot-up

# Show Versions Output

```
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)

Router uptime is 10 hours, 9 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

<Output omitted>

Cisco CISCO1941/K9 (revision 1.0) with 446464K/77824K bytes of memory.
Processor board ID FTX1636848Z
2 Gigabit Ethernet interfaces
2 Serial(sync/async) interfaces
1 terminal line
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
250880K bytes of ATA System CompactFlash 0 (Read/Write)

<Output omitted>

Technology Package License Information for Module:'c1900'

-----
Technology      Technology-package          Technology-package
                Current        Type            Next reboot
-----
ipbase         ipbasek9       Permanent     ipbasek9
security       None           None          None
data           None           None          None

Configuration register is 0x2142 (will be 0x2102 at next reload)

Router#
```



## 6.4 Configuring a Cisco Router

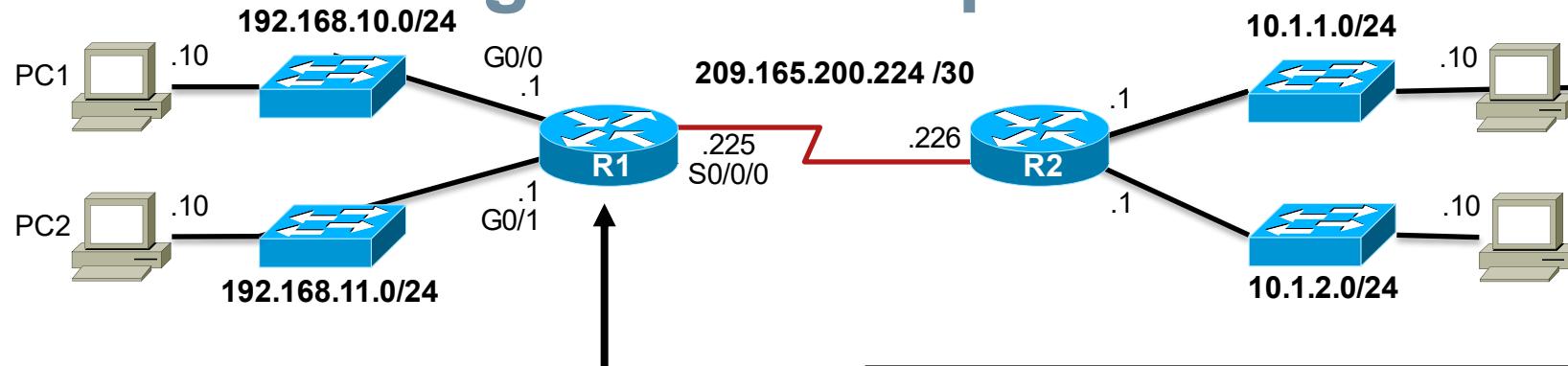


Cisco | Networking Academy®  
Mind Wide Open™



# Configure Initial Settings

# Router Configuration Steps



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

OR

```
Router> en
Router# conf t
Enter configuration commands, one per line.
End with CNTL/Z.
Router(config)# ho R1
R2(config) #
```

```
R1(config)# enable secret class
R1(config)#
R1(config)# line console 0
R1(config-line) # password cisco
R1(config-line) # login
R1(config-line) # exit
R1(config) #
R1(config)# line vty 0 4
R1(config-line) # password cisco
R1(config-line) # login
R1(config-line) # exit
R1(config) #
R1(config)# service password-encryption
R1(config) #
```

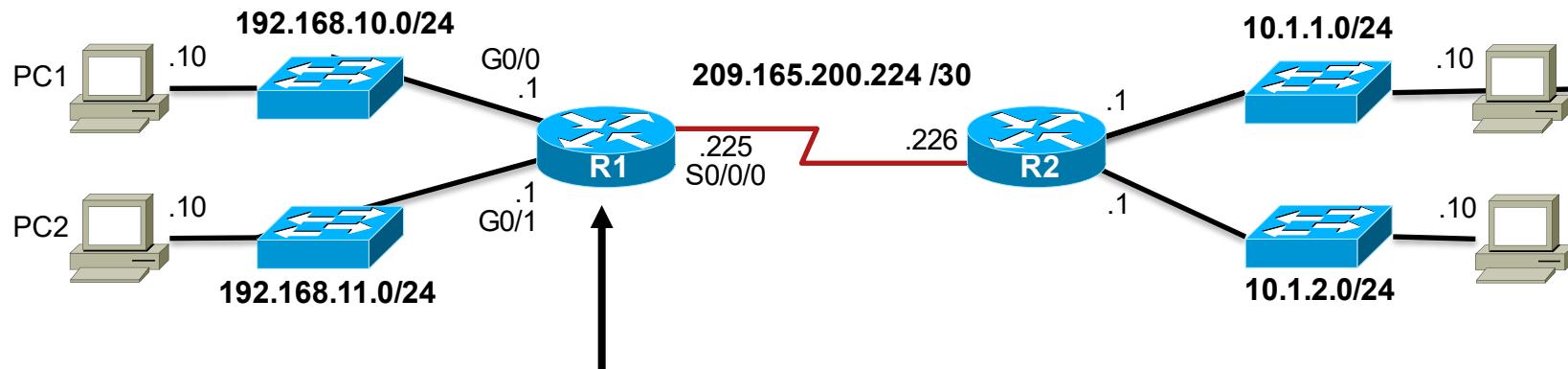
```
R1(config)# banner motd #
Enter TEXT message. End with the character '#'.
*****
WARNING: Unauthorized access is prohibited!
*****
#
R1(config) #
```

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```



# Configure Interfaces

# Configure LAN Interfaces



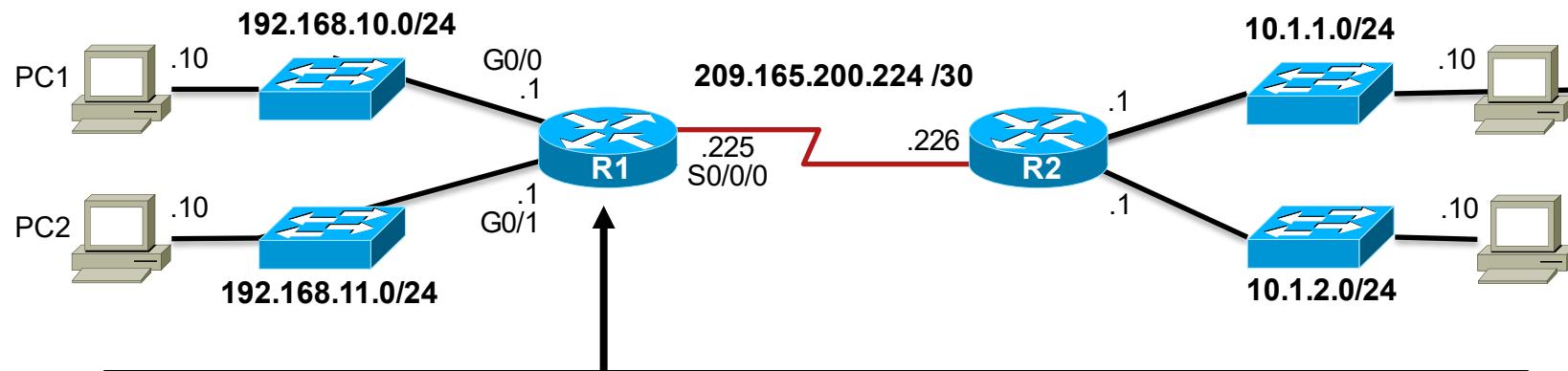
```
R1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#
R1(config)# interface gigabitethernet 0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# description Link to LAN-10
R1(config-if)# no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
R1(config-if)# exit
R1(config)#
R1(config)# int g0/1
R1(config-if)# ip add 192.168.11.1 255.255.255.0
R1(config-if)# des Link to LAN-11
R1(config-if)# no shut
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up
R1(config-if)# exit
R1(config)#

```



# Configure Interfaces

# Verify Interface Configuration



```
R1# show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0  192.168.10.1    YES manual up        up
GigabitEthernet0/1  192.168.11.1    YES manual up        up
Serial0/0/0         209.165.200.225 YES manual up        up
Serial0/0/1         unassigned      YES NVRAM administratively down down
Vlan1              unassigned      YES NVRAM administratively down down
R1#
R1# ping 209.165.200.226
```

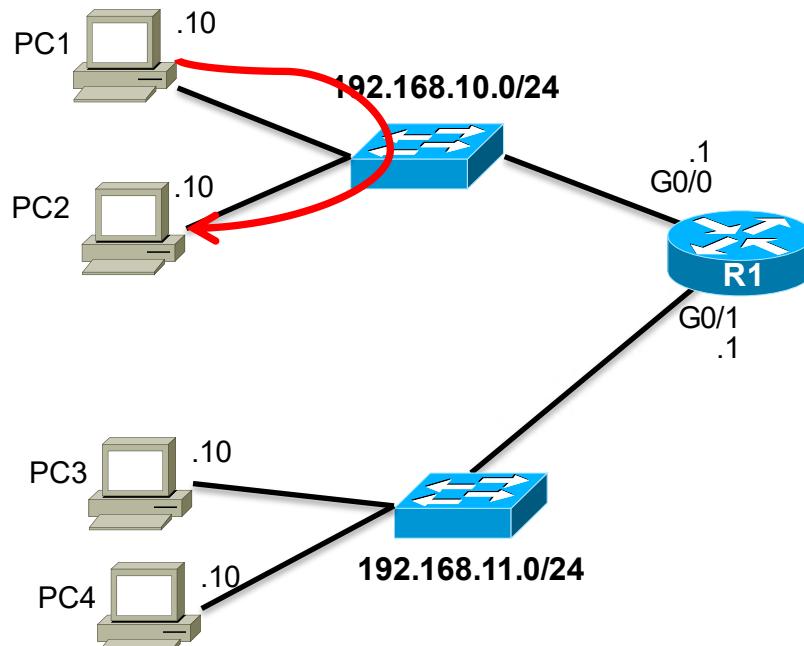
Type escape sequence to abort.  
 Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:  
 !!!!!  
 Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/9 ms

```
R1#
```

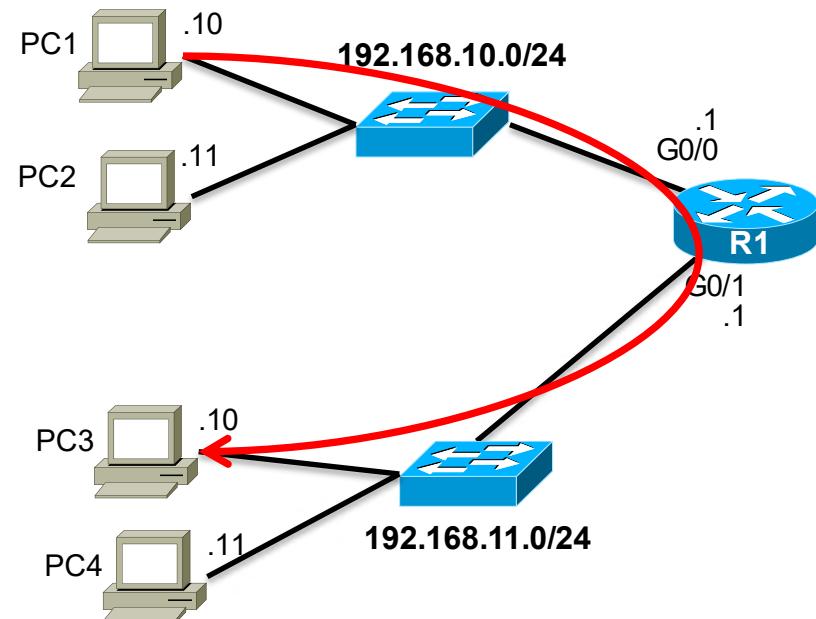


# Configuring the Default Gateway Default Gateway on a Host

Default Gateway  
not needed

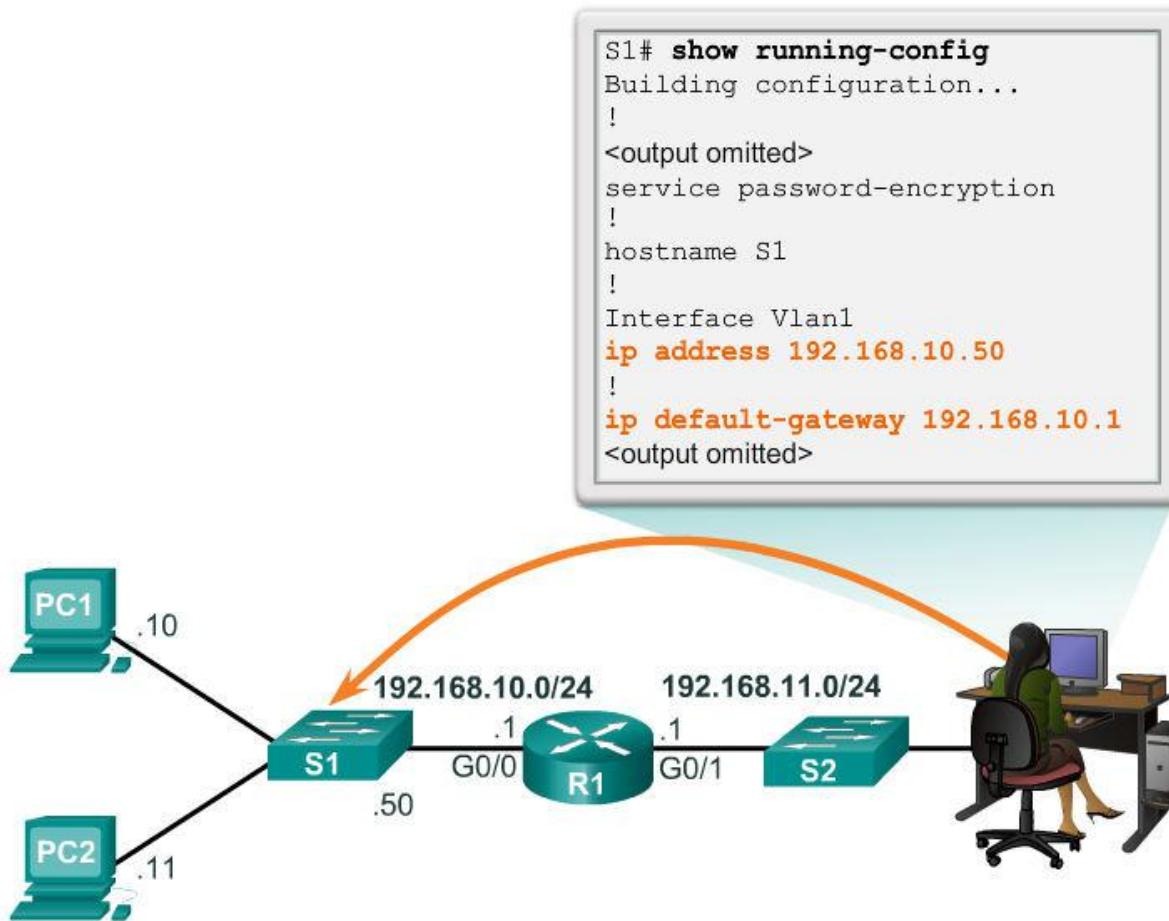


Default Gateway  
needed





# Configuring the Default Gateway Default Gateway on a Switch



If the default gateway was not configured on S1, response packets from S1 would not be able to reach the administrator at 192.168.11.10. The administrator would not be able to manage the device remotely.



# Network Layer Summary

In this chapter, you learned:

- The network layer, or OSI Layer 3, provides services to allow end devices to exchange data across the network.
- The network layer uses four basic processes: IP addressing for end devices, encapsulation, routing, and de-encapsulation.
- The Internet is largely based on IPv4, which is still the most widely-used network layer protocol.
- An IPv4 packet contains the IP header and the payload.
- The IPv6 simplified header offers several advantages over IPv4, including better routing efficiency, simplified extension headers, and capability for per-flow processing.



## Network Layer

# Summary (cont.)

- In addition to hierarchical addressing, the network layer is also responsible for routing.
- Hosts require a local routing table to ensure that packets are directed to the correct destination network.
- The local default route is the route to the default gateway.
- The default gateway is the IP address of a router interface connected to the local network.
- When a router, such as the default gateway, receives a packet, it examines the destination IP address to determine the destination network.



## Network Layer Summary (cont.)

- The routing table of a router stores information about directly-connected routes and remote routes to IP networks. If the router has an entry in its routing table for the destination network, the router forwards the packet. If no routing entry exists, the router may forward the packet to its own default route, if one is configured or it will drop the packet.
- Routing table entries can be configured manually on each router to provide static routing or the routers may communicate route information dynamically between each other using a routing protocol.
- For routers to be reachable, the router interface must be configured.

# Cisco | Networking Academy®

Mind Wide Open™

## Chapter 7: Transport Layer



## Introduction to Networking

Cisco | Networking Academy®  
Mind Wide Open™



# Chapter 7

7.0 Introduction

7.1 Transport Layer Protocols

7.2 TCP and UDP

7.3 Summary



# Chapter 7: Objectives

- Describe the purpose of the transport layer in managing the transportation of data in end-to-end communication.
- Describe characteristics of the TCP and UDP protocols, including port numbers and their uses.
- Explain how TCP session establishment and termination processes facilitate reliable communication.
- Explain how TCP protocol data units are transmitted and acknowledged to guarantee delivery.
- Explain the UDP client processes to establish communication with a server.
- Determine whether high-reliability TCP transmissions, or non-guaranteed UDP transmissions, are best suited for common applications.

## 7.1: Transport Layer Protocols





## Transportation of Data

# Role of the Transport Layer

The transport layer is responsible for establishing a temporary communication session between two applications and delivering data between them.

TCP/IP uses two protocols to achieve this:

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)

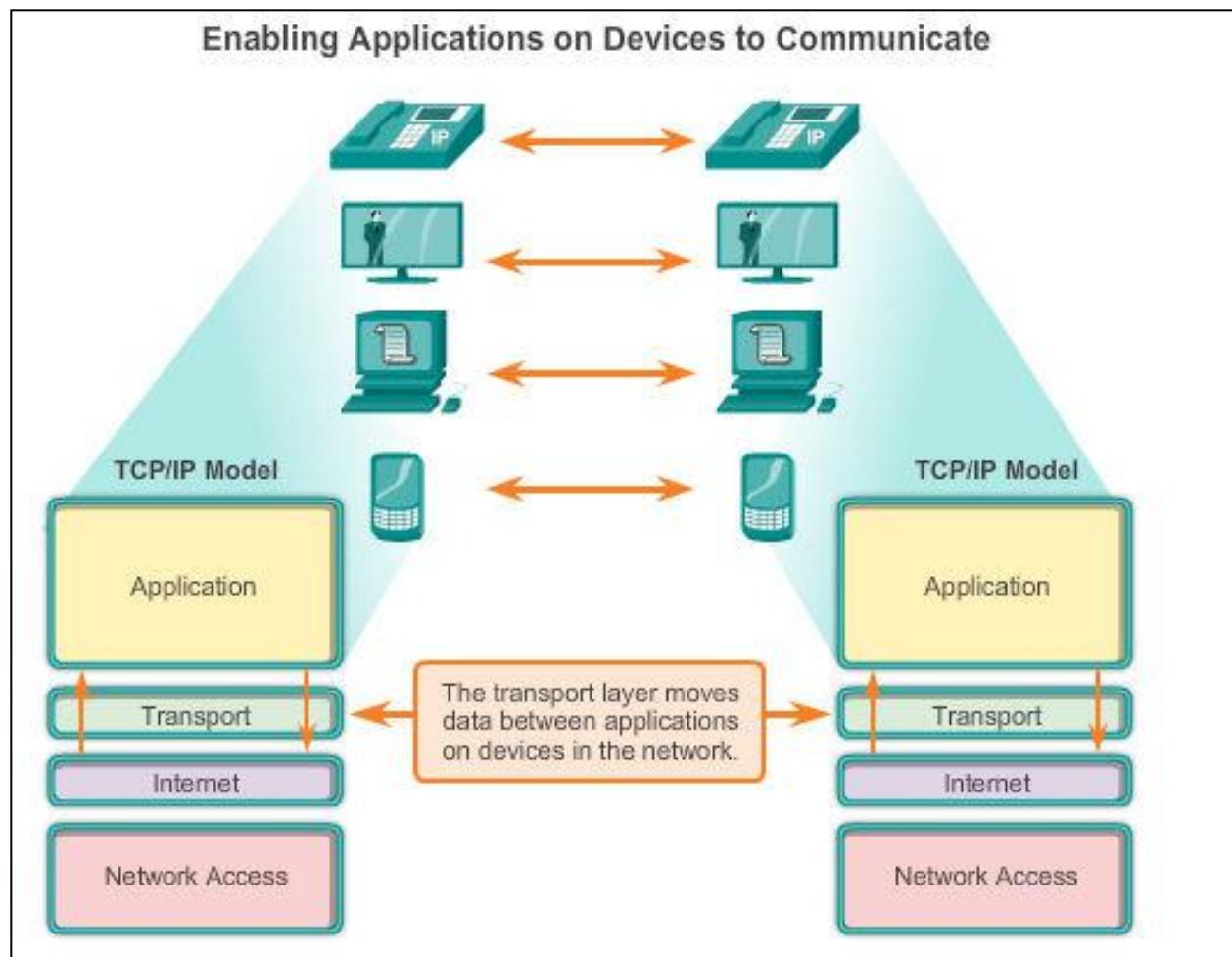
## Primary Responsibilities of Transport Layer Protocols

- Tracking the individual communication between applications on the source and destination hosts
- Segmenting data for manageability and reassembling segmented data into streams of application data at the destination
- Identifying the proper application for each communication stream



## Transportation of Data

# Role of the Transport Layer (Cont.)





## Transportation of Data

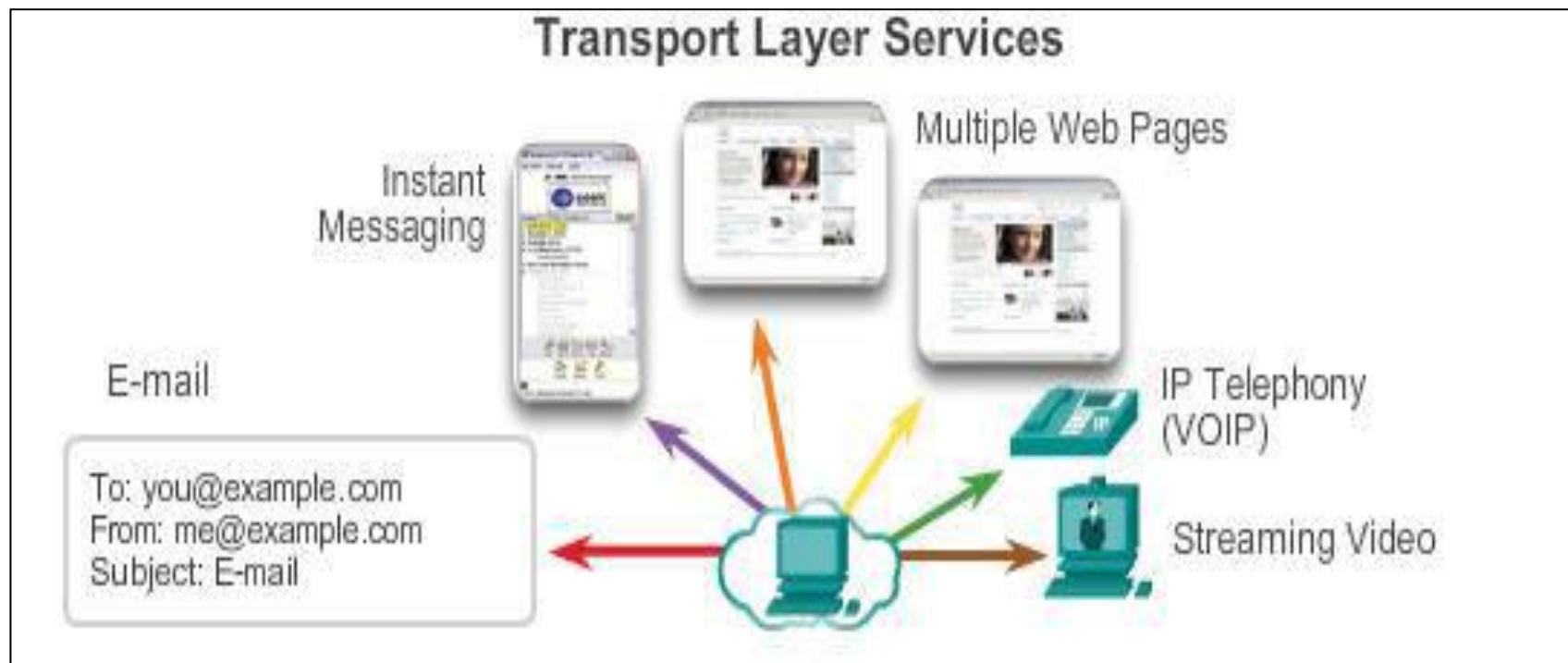
# Conversation Multiplexing

### Segmenting the Data

- Enables many different communications, from many different users, to be interleaved (multiplexed) on the same network, at the same time.
- Provides the means to both send and receive data when running multiple applications.
- Header added to each segment to identify it.



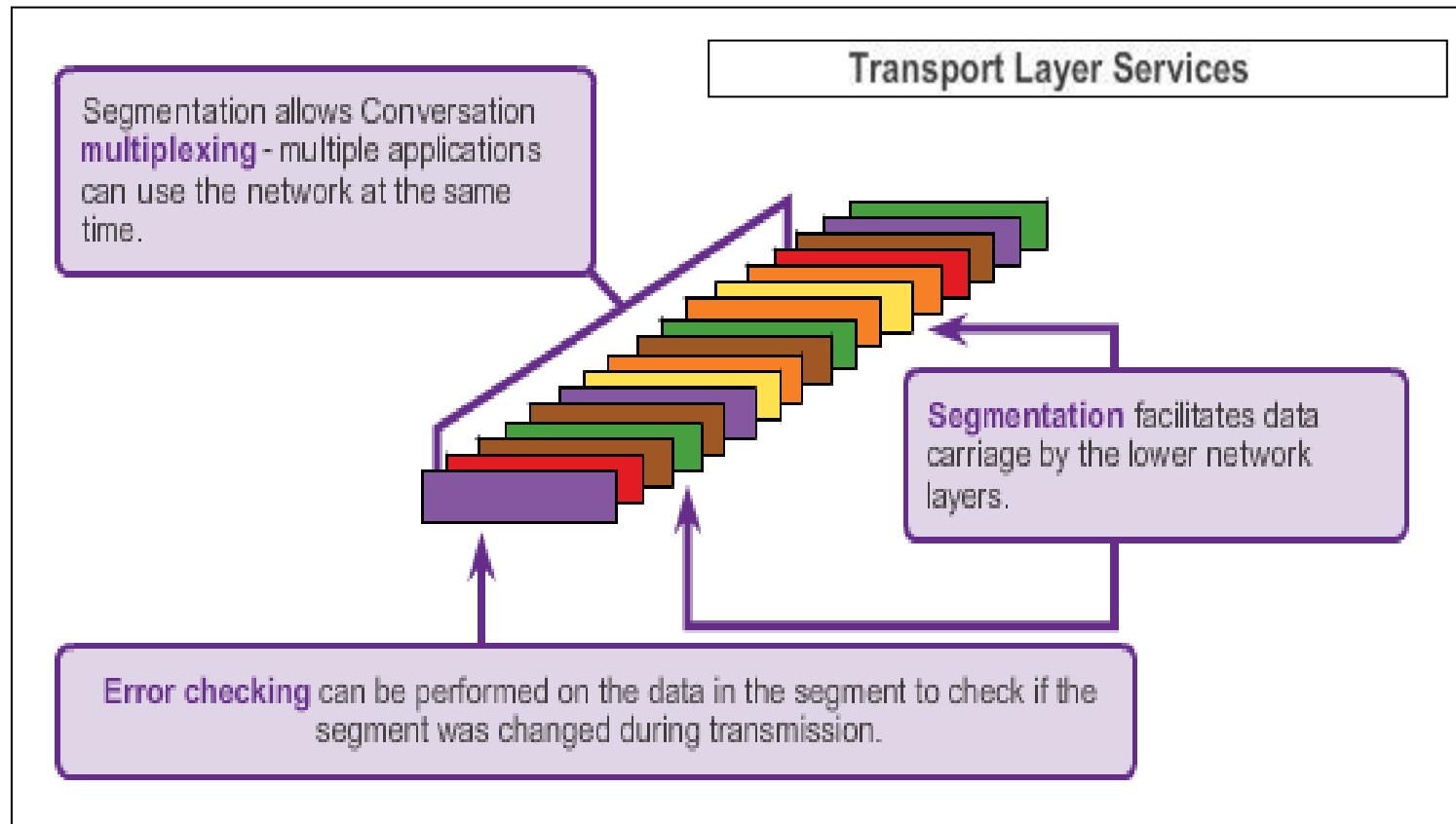
# Transportation of Data Conversation Multiplexing (Cont.)





# Transportation of Data

# Conversation Multiplexing (Cont.)





## Transportation of Data

# Transport Layer Reliability

Different applications have different transport reliability requirements.

TCP/IP provides two transport layer protocols, **TCP and UDP**.

## TCP

- Provides reliable delivery ensuring that all of the data arrives at the destination.
- Uses acknowledged delivery and other processes to ensure delivery
- Makes larger demands on the network – more overhead.

## UDP

- Provides just the basic functions for delivery – no reliability.
- Less overhead.

## TCP or UDP

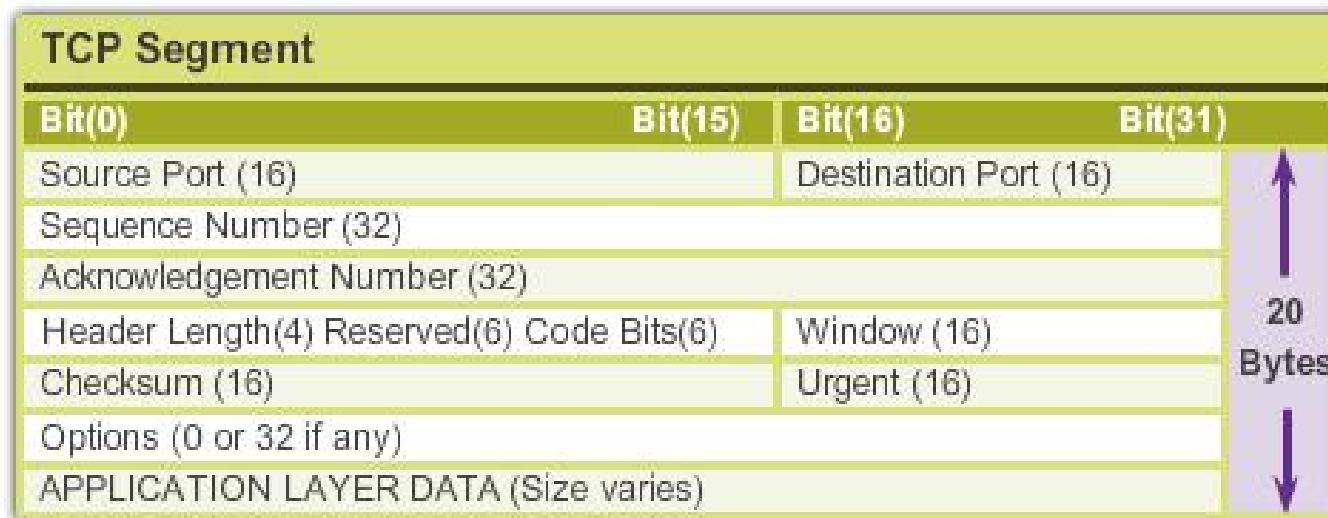
- There is a trade-off between the value of reliability and the burden it places on the network.
- Application developers choose the transport protocol based on the requirements of their applications.



## Introducing TCP and UDP

# Introducing TCP

- Defined in RFC 793
- Connection-oriented – Creates a session between the source and destination
- Reliable delivery – Retransmits lost or corrupt data
- Ordered data reconstruction – Reconstructs numbering and sequencing of segments
- Flow control – Regulates the amount of data transmitted
- Stateful protocol – Tracks the session





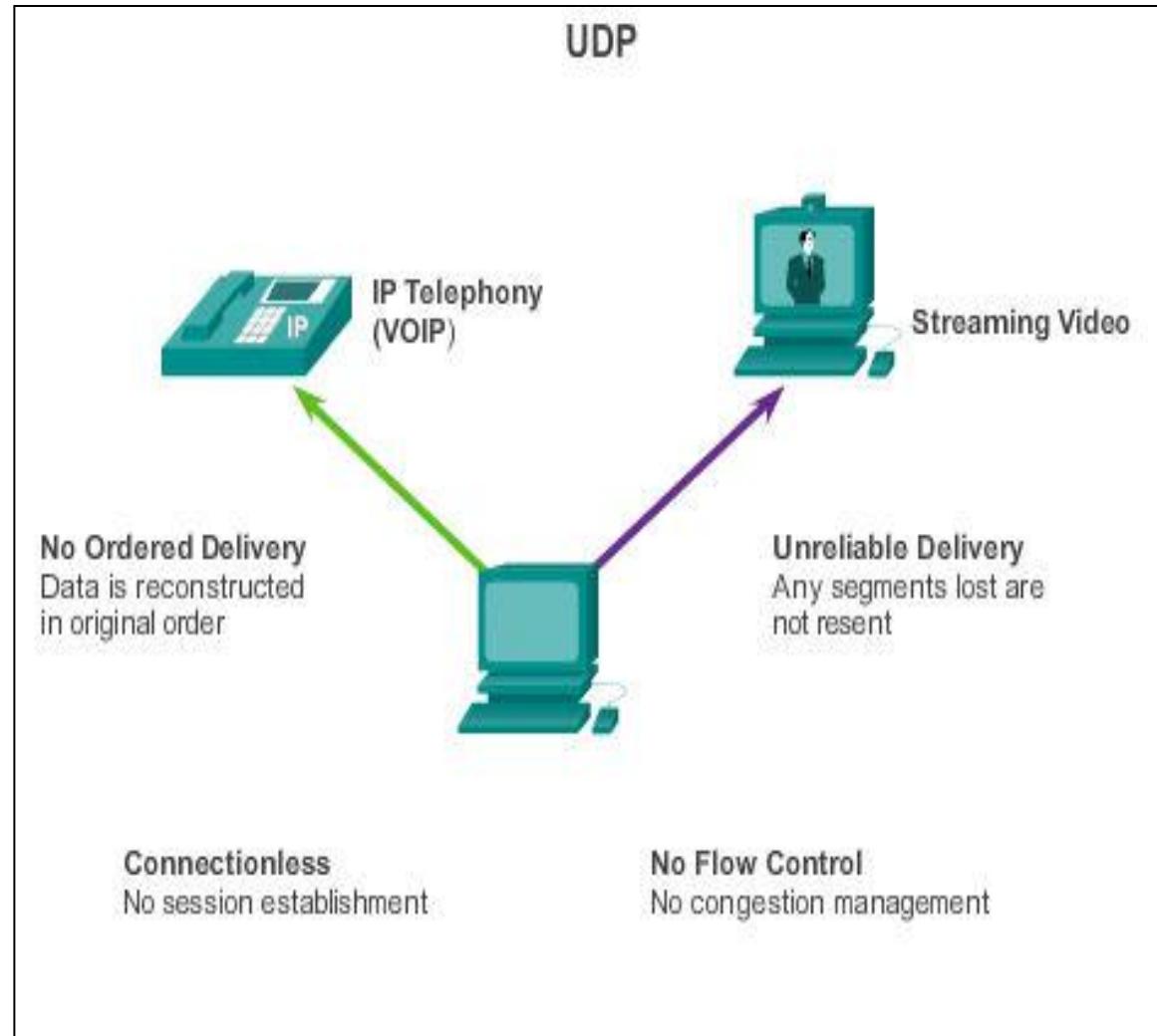
# Introducing TCP and UDP

## Introducing UDP

- RFC 768
- Connectionless
- Unreliable delivery
- No ordered data reconstruction
- No flow control
- Stateless protocol

### Applications that use UDP:

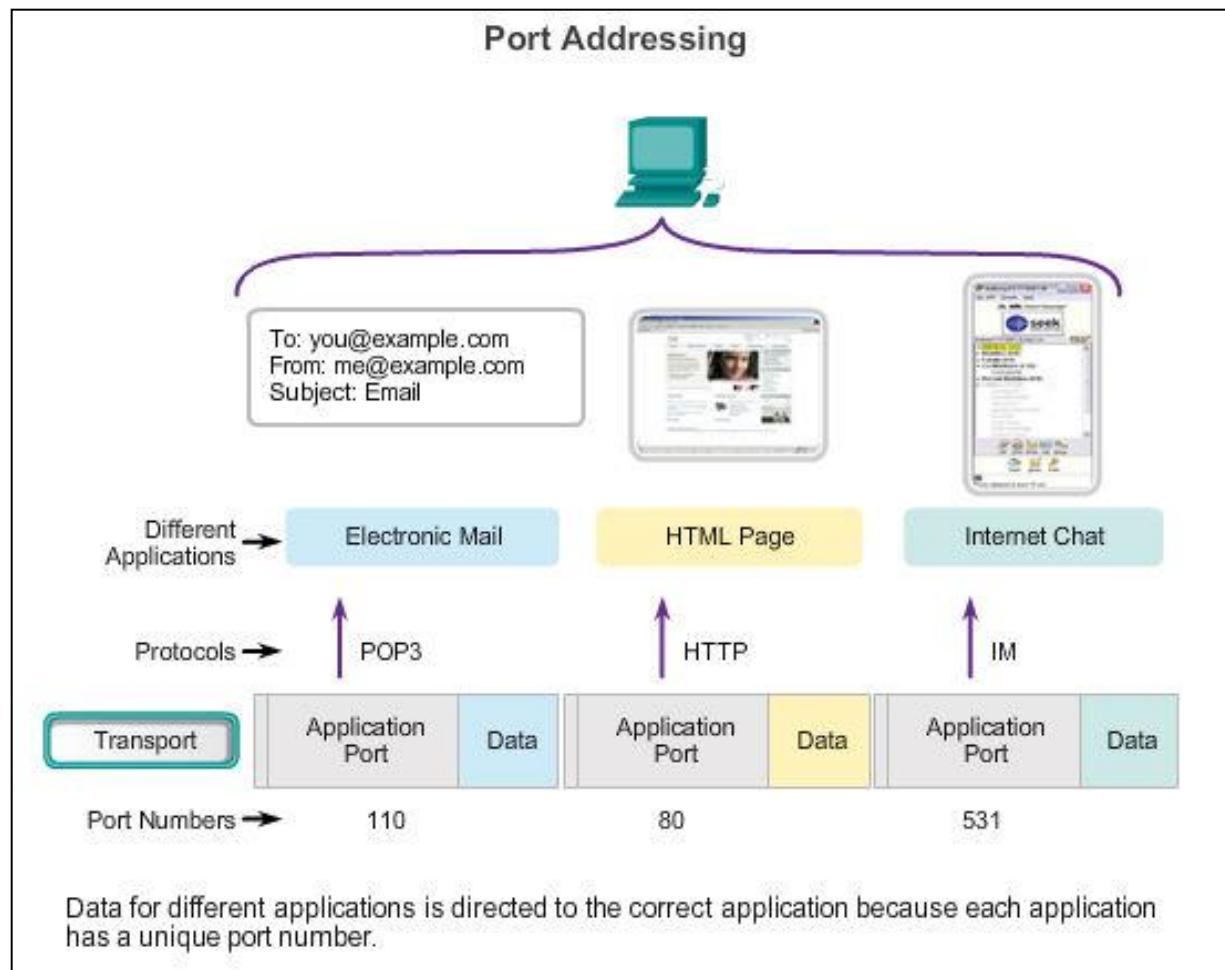
- Domain Name System (DNS)
- Video Streaming
- VoIP





# Introducing TCP and UDP Separating Multiple Communications

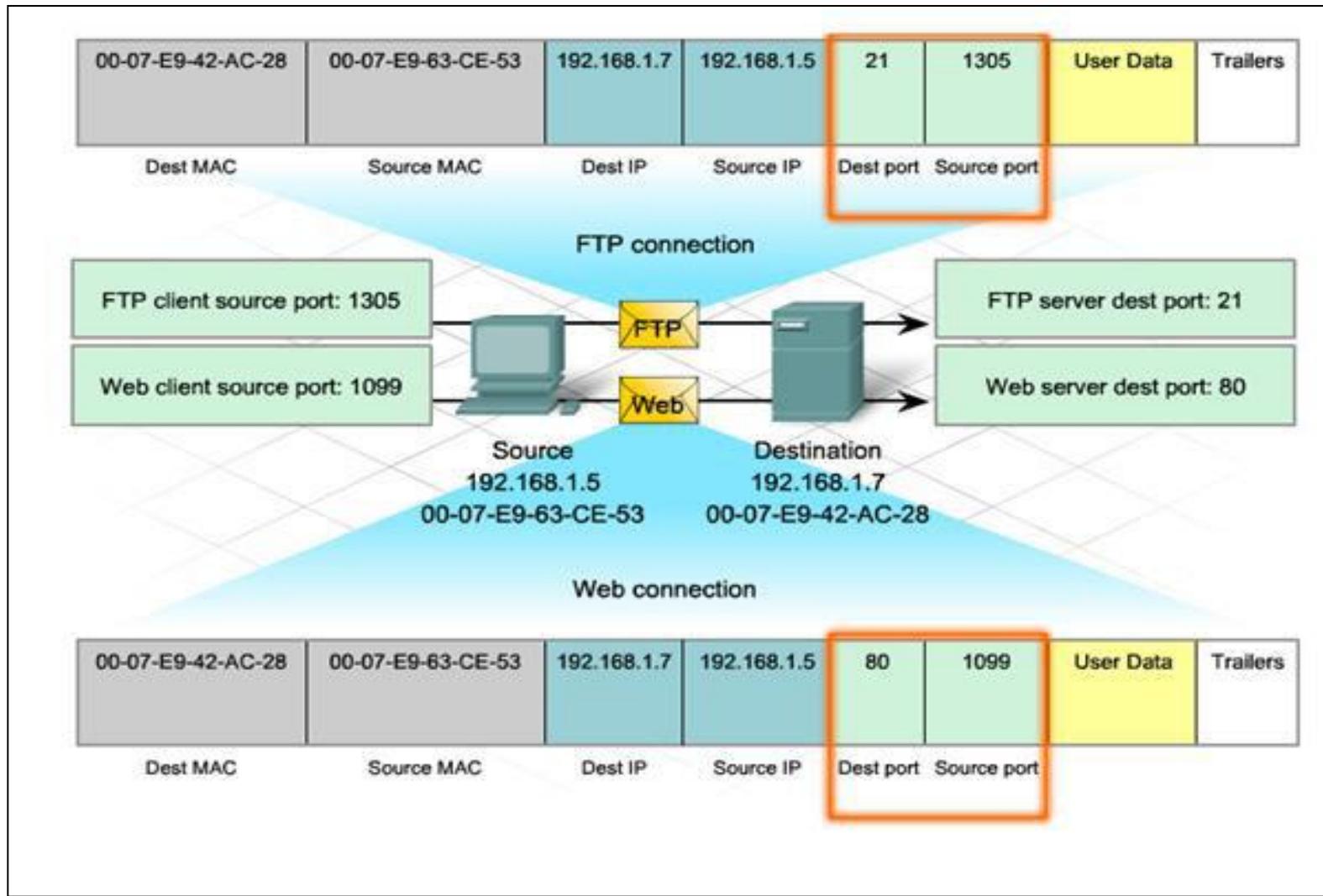
TCP and UDP use port numbers to differentiate between applications.





## Introducing TCP and UDP

# TCP and UDP Port Addressing





## Introducing TCP and UDP

# TCP and UDP Port Addressing (Cont.)

## Port Numbers

Port Number Range	Port Group
0 to 1023	Well Known (Contact) Ports
1024 to 49151	Registered Ports
49152 to 65533	Private and/or Dynamic Ports

### Registered TCP Ports:

- 1863 MSN Messenger
- 2000 Cisco SCCP (VoIP)
- 8008 Alternate HTTP
- 8080 Alternate HTTP

### Well Known TCP Ports:

- 21 FTP
- 23 Telnet
- 25 SMTP
- 80 HTTP
- 110 POP3
- 194 Internet Relay Chat (IRC)
- 443 Secure HTTP (HTTPS)



## Introducing TCP and UDP

# TCP and UDP Port Addressing (Cont.)

### Registered UDP Ports:

- 1812 RADIUS Authentication Protocol
- 5004 RTP (Voice and Video Transport Protocol)
- 5040 SIP (VoIP)

### Well Known UDP Ports:

- 69 TFTP
- 520 RIP

### Registered TCP/UDP Common Ports:

- 1433 MS SQL
- 2948 WAP (MMS)

### Well Known TCP/UDP Common Ports:

- 53 DNS
- 161 SNMP
- 531 AOL Instant Messenger, IRC



## Introducing TCP and UDP

# TCP and UDP Port Addressing (Cont.)

Netstat is used to examine TCP connections that are open and running on a networked host.

```
C:\>netstat
```

### Active Connections

Proto	Local Address	Foreign Address	State
<b>TCP</b>	kenpc:3126	192.168.0.2:netbios-ssn	ESTABLISHED
TCP	kenpc:3158	207.138.126.152:http	ESTABLISHED
TCP	kenpc:3159	207.138.126.169:http	ESTABLISHED
TCP	kenpc:3160	207.138.126.169:http	ESTABLISHED
TCP	kenpc:3161	sc.msn.com:http	ESTABLISHED
TCP	kenpc:3166	www.cisco.com:http	ESTABLISHED

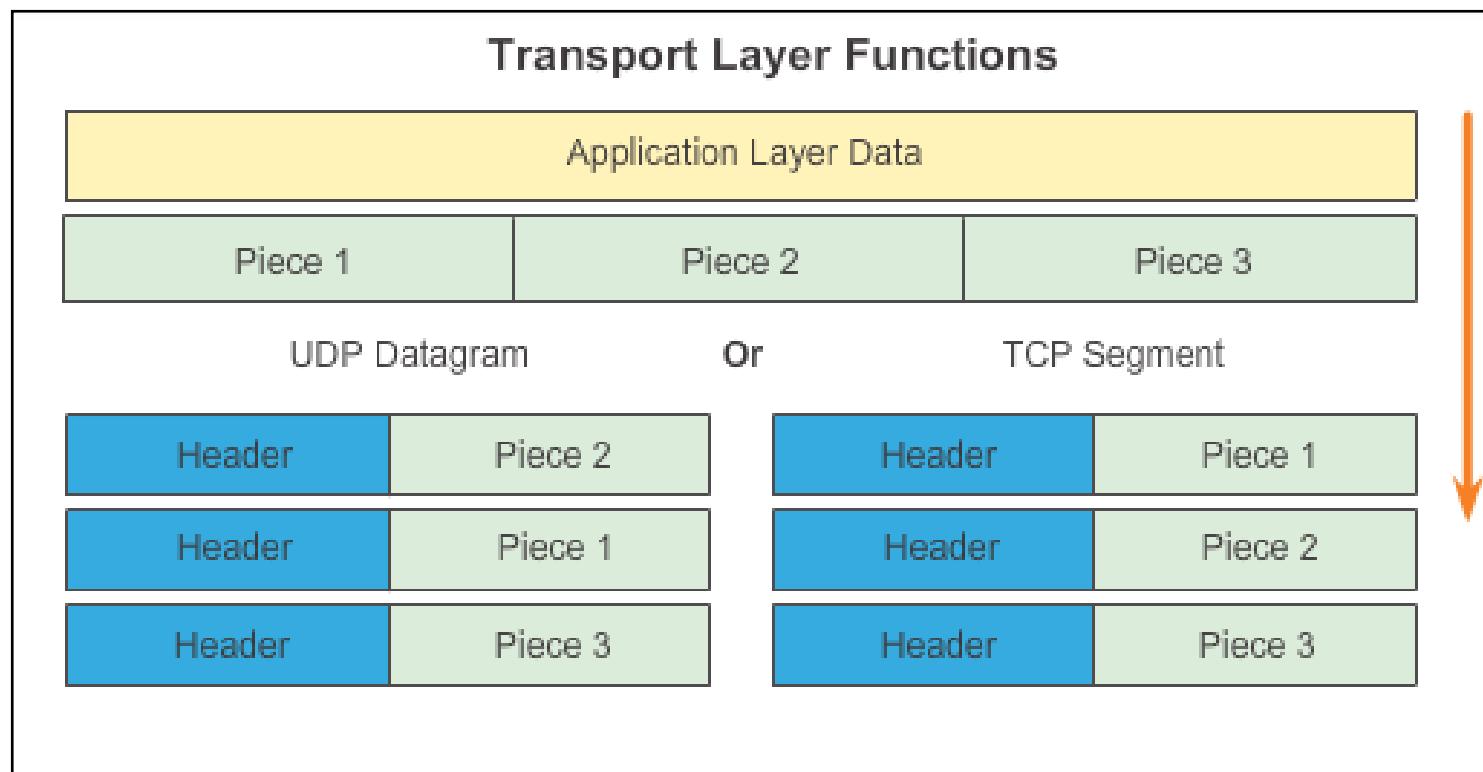
```
C:\>
```



## Introducing TCP and UDP

# TCP and UDP Segmentation

The transport layer divides the data into pieces and adds a header for delivery over the network



## 7.2 TCP and UDP

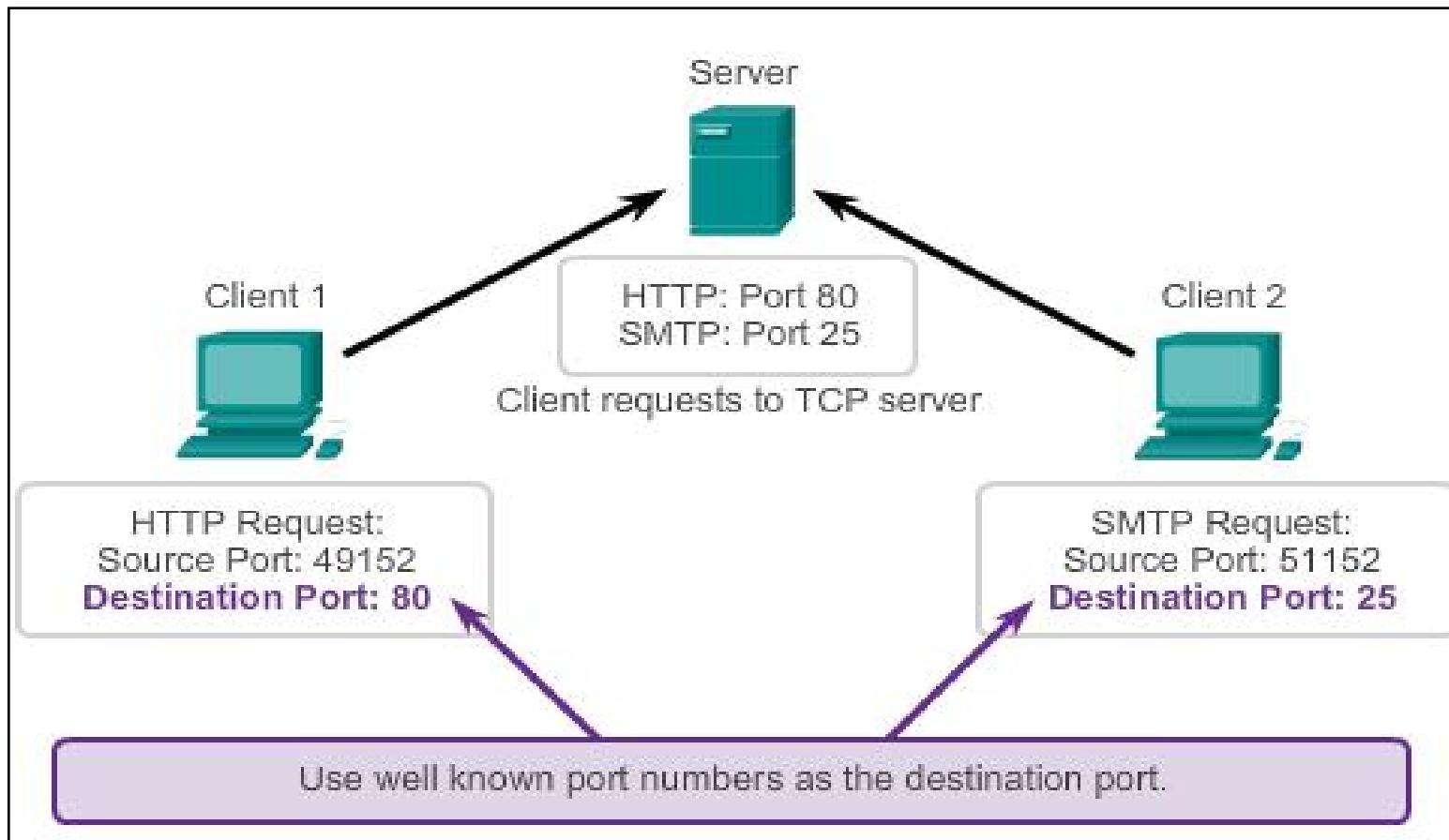




# TCP Communication

# TCP Server Processes

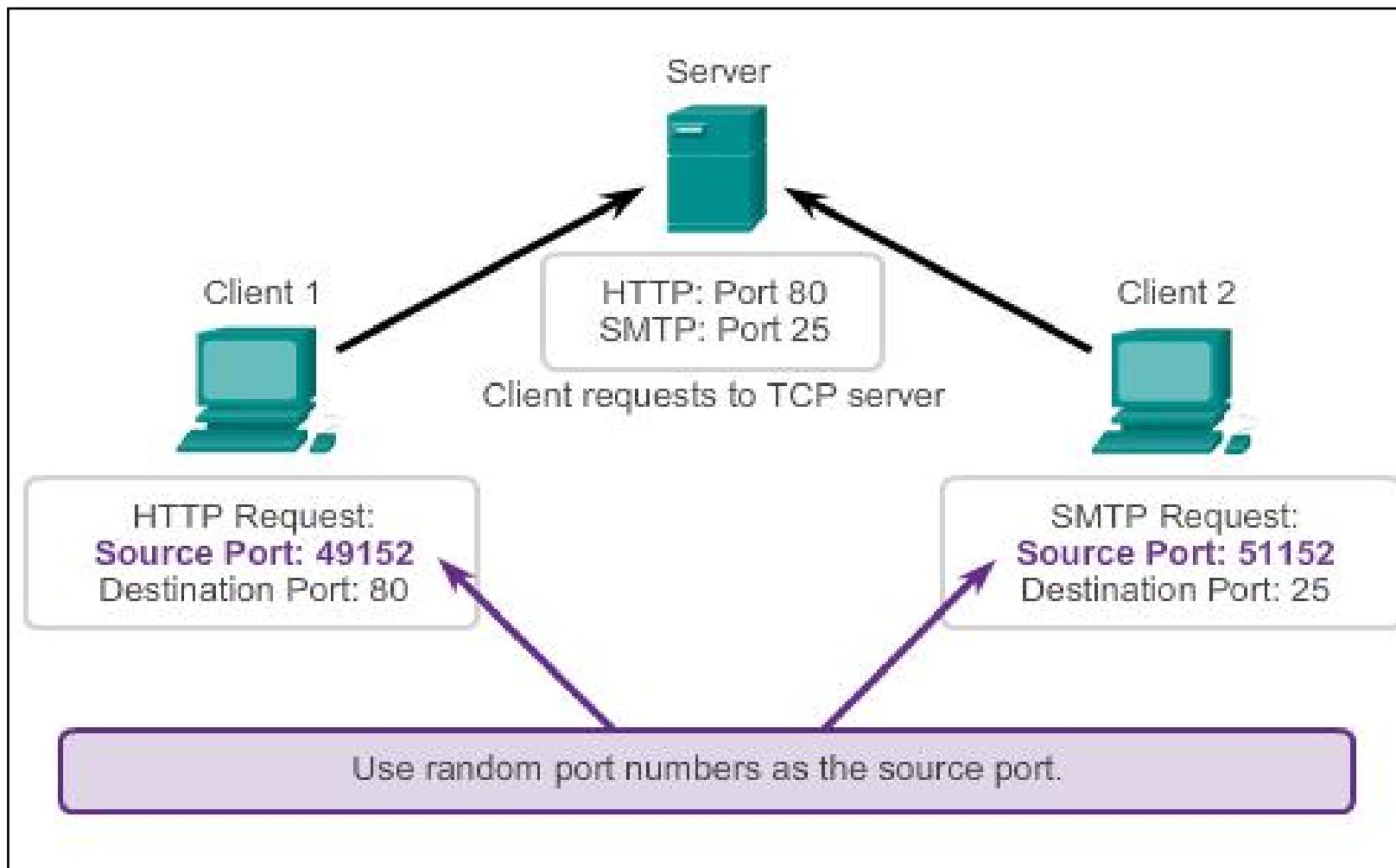
## Request Destination Ports





# TCP Communication

## TCP Server Processes (Cont.)





## TCP Communication

# TCP Connection, Establishment and Termination

### Three-Way Handshake

- Establishes that the destination device is present on the network
- Verifies that the destination device has an active service and is accepting requests on the destination port number that the initiating client intends to use for the session
- Informs the destination device that the source client intends to establish a communication session on that port number



## TCP Communication

# TCP Three-Way Handshake – Step 1

**Step 1:** The initiating client requests a client-to-server communication session with the server

TCP 3-Way Handshake (SYN)

The screenshot shows a protocol analyzer interface with the following details for Frame 10:

- Frame 10: 62 bytes on wire (496 bits), 62 bytes captured.
- Ethernet II, Src: VMware\_be:62:88 (00:50:56:be:62:88).
- Internet Protocol Version 4, Src: 10.1.1.1 (10.1.1.1).
- Transmission Control Protocol, Src Port: kiosk (1061), Dest Port: http (80).
  - Source port: kiosk (1061)
  - Destination port: http (80)
  - [Stream index: 0]
  - Sequence number: 0 (relative sequence number)
  - Header length: 28 bytes
  - Flags: 0x02 (SYN)
    - 000. .... .... = Reserved: Not set
    - 0 = Nonce - Not set

A protocol analyzer shows initial client request for session in frame 10

TCP segment in this frame shows:

- SYN flag set to validate an Initial Sequence Number
- Randomized sequence number valid (relative value is 0)
- Random source port 1061
- Well-known destination port is 80 (HTTP port) indicates web server (httpd)



## TCP Communication

# TCP Three-Way Handshake – Step 2

**Step 2:** The server acknowledges the client-to-server communication session and requests a server-to-client communication session.

TCP 3-Way Handshake (SYN, ACK)			
10	16.303490	10.1.1.1	192.168.254.254
11	16.304896	192.168.254.254	10.1.1.1
12	16.304925	10.1.1.1	192.168.254.254
13	16.305153	10.1.1.1	192.168.254.254
14	16.307875	192.168.254.254	10.1.1.1

Frame 11: 62 bytes on wire (496 bits), 62 bytes captured  
Ethernet II, Src: Cisco\_63:74:a0 (00:0f:24:63:74:a0), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)  
Internet Protocol Version 4, Src: 192.168.254.254 (192.168.254.254), Dst: 10.1.1.1 (10.1.1.1)  
Transmission Control Protocol, src port: http (80), dst port: http (80)  
Source port: http (80)

A protocol analyzer shows server response in frame 11

- ACK flag set to indicate a valid Acknowledgement number
- Acknowledgement number response to initial sequence number as relative value of 1
- SYN flag set to indicate the Initial Sequence Number for the server to client session
- Destination port number of 1061 to corresponding to the clients source port
- Source port number of 80 (HTTP) indicating the web server service (httpd)



## TCP Communication

# TCP Three-Way Handshake – Step 3

**Step 3:** The initiating client acknowledges the server-to-client communication session.

TCP 3-Way Handshake (ACK)				
No.	Time	Source	Destination	
10	15.303490	10.1.1.1	192.168.254.254	
11	16.304896	192.168.254.254	10.1.1.1	
12	16.304925	10.1.1.1	192.168.254.254	
13	16.305153	10.1.1.1	192.168.254.254	
14	16.307875	192.168.254.254	10.1.1.1	

Frame 12: 54 bytes on wire (432 bits), 54 bytes captured  
Ethernet II, Src: VMware\_Ke:62:88 (00:50:56:be:62:88)  
Internet Protocol Version 4, Src: 10.1.1.1 (10.1.1.1)  
Transmission Control Protocol, Src Port: k'osk (1061)

A protocol analyzer shows client response to session in frame 12

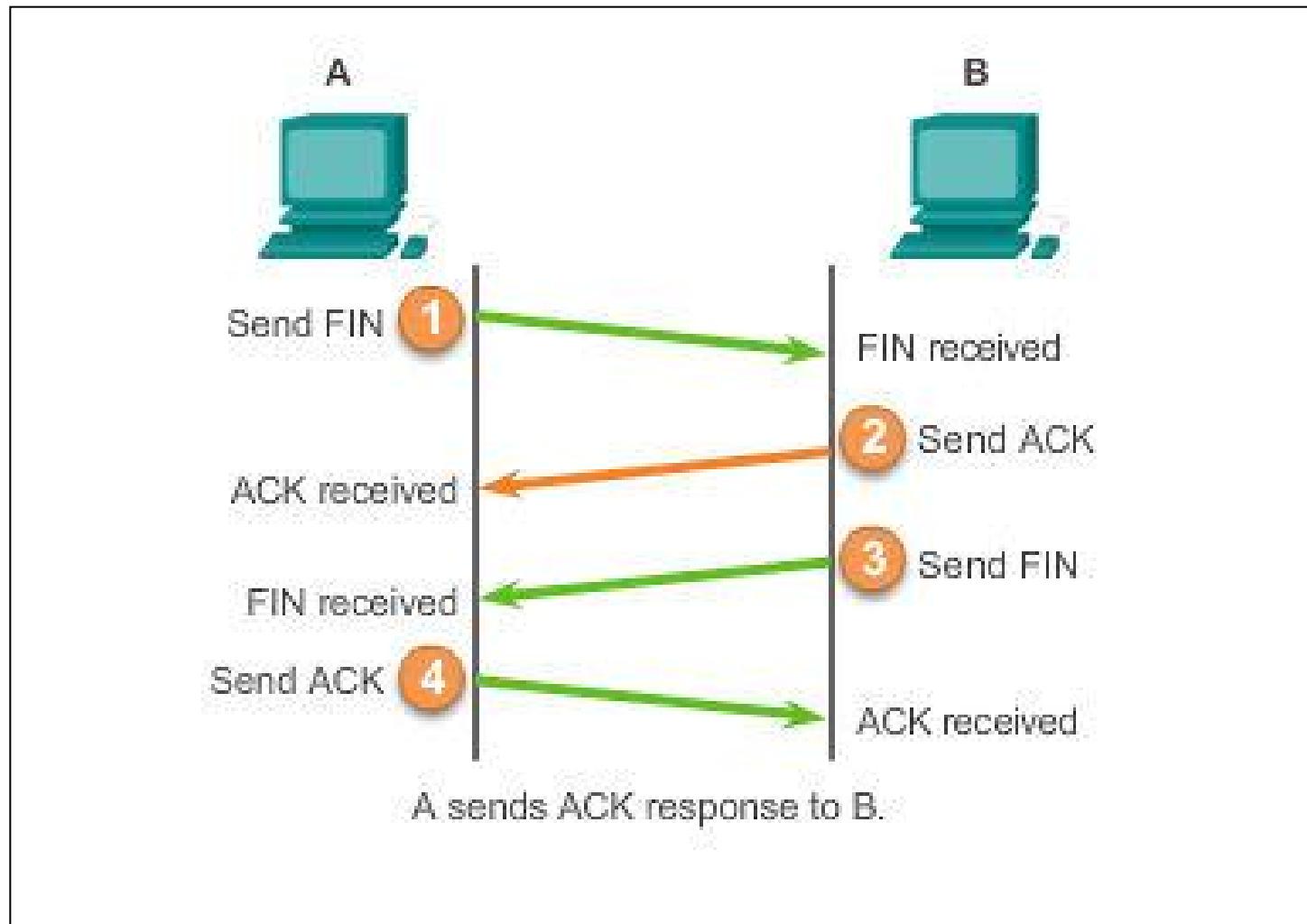
The TCP segment in this frame shows:

- ACK flag set to indicate a valid Acknowledgement number
- Acknowledgement number response to initial sequence number as relative value of 1
- Source port number of 1061 to corresponding
- Destination port number of 80 (HTTP) indicating the web server service (httpd)



## TCP Communication

## TCP Session Termination

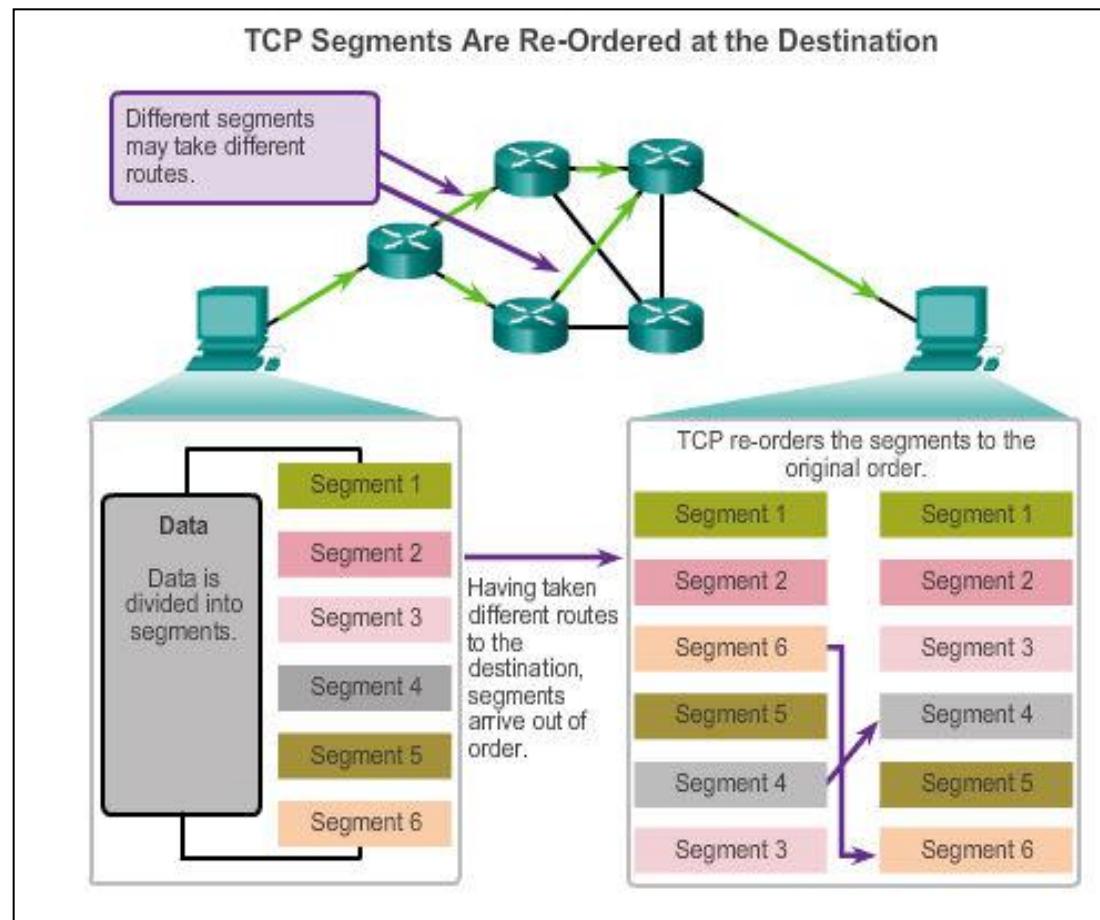




## Reliability and Flow Control

# TCP Reliability – Ordered Delivery

Sequence numbers are used to reassemble segments into their original order.

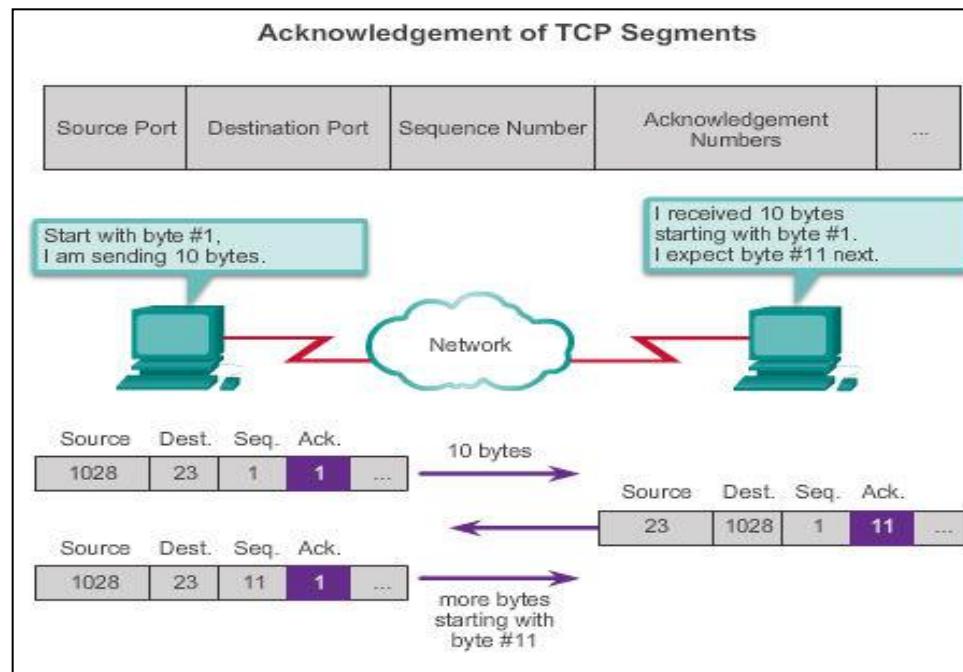




## Reliability and Flow Control

# Acknowledgement and Window Size

The sequence number and acknowledgement number are used together to confirm receipt.

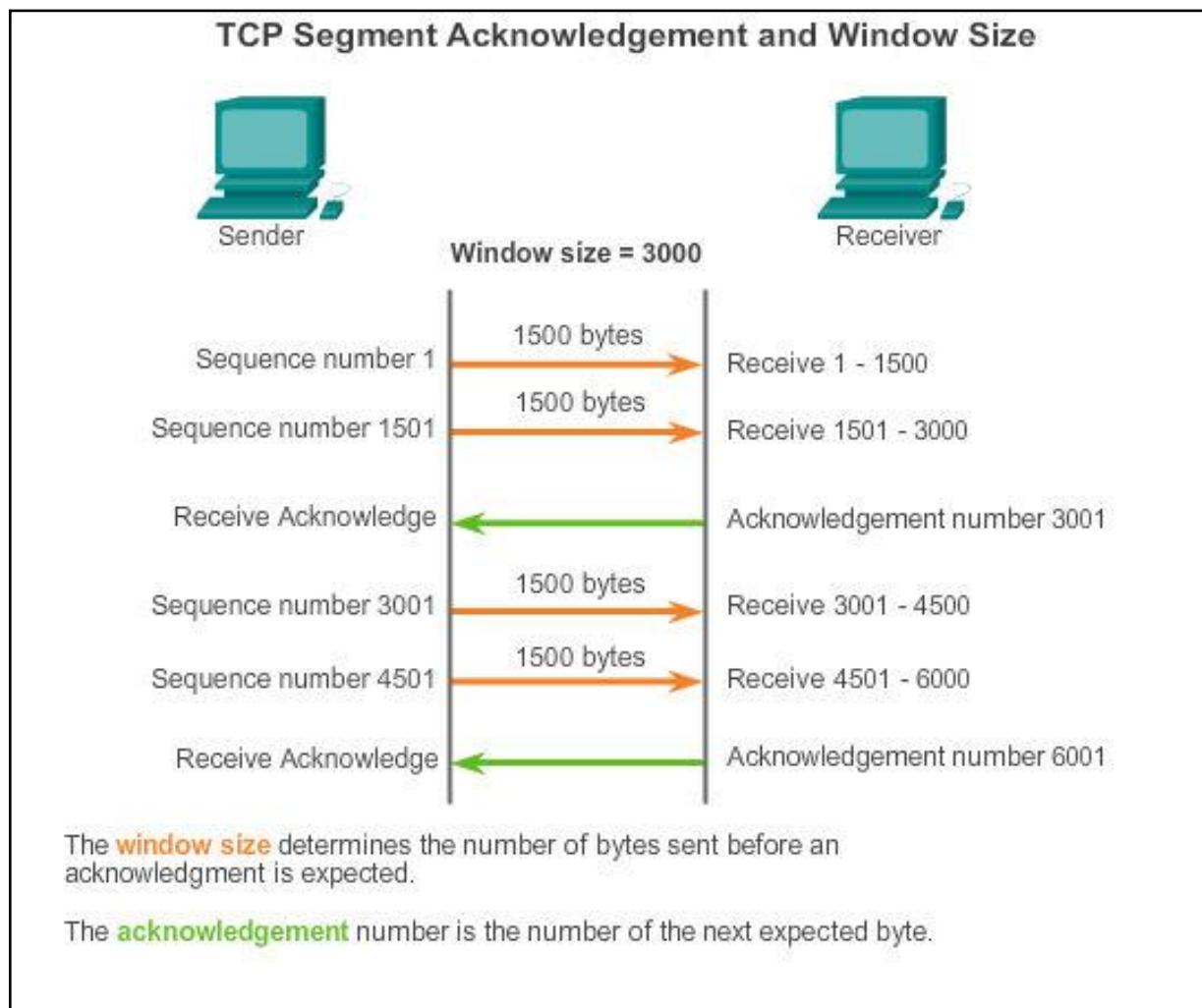


The window size is the amount of data that a source can transmit before an acknowledgement must be received.



# Reliability and Flow Control

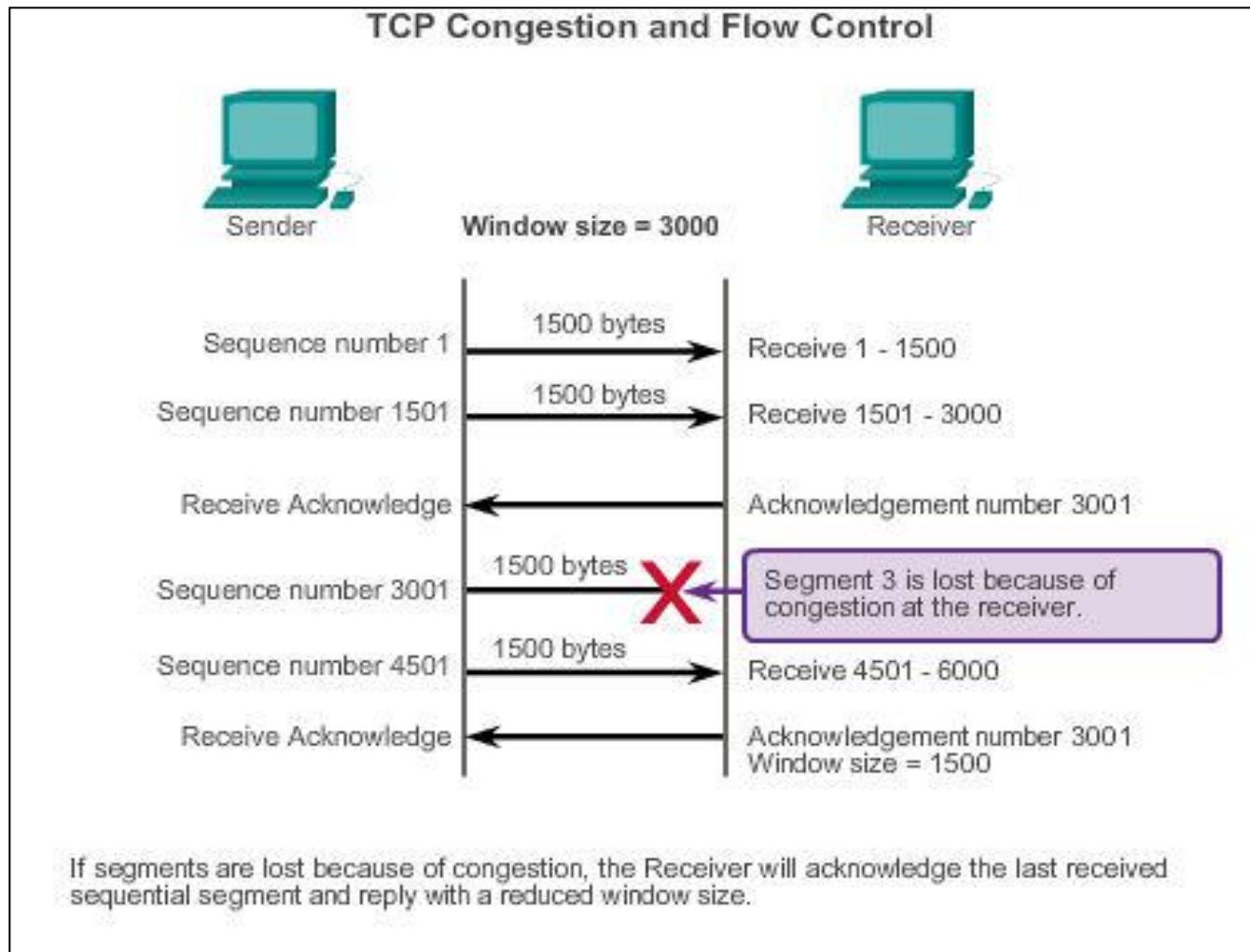
# Window Size and Acknowledgements





## Reliability and Flow Control

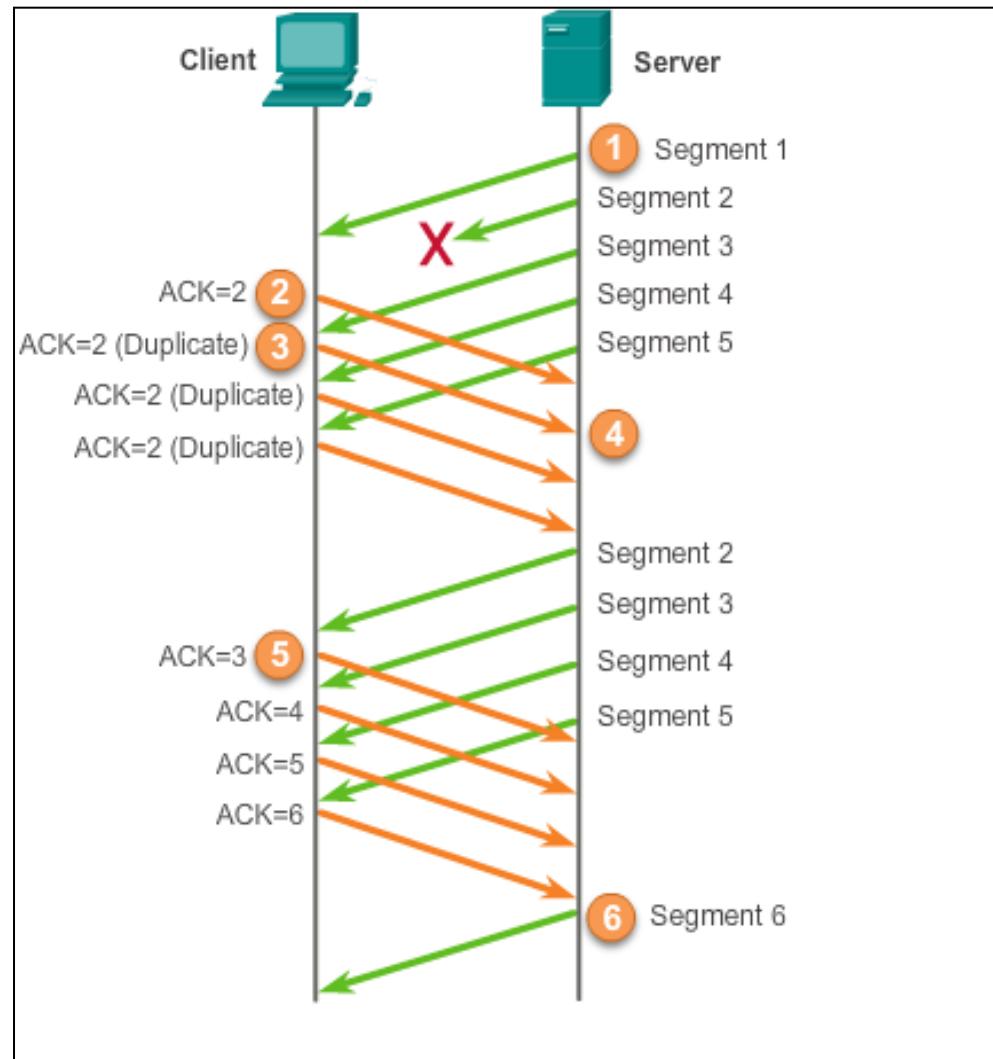
# TCP Flow Control – Congestion Avoidance





## Reliability and Flow Control

# TCP Reliability - Acknowledgements





## UDP Communication

# UDP Low Overhead vs. Reliability

### UDP

- Simple protocol that provides the basic transport layer function
- Used by applications that can tolerate small loss of data
- Used by applications that cannot tolerate delay

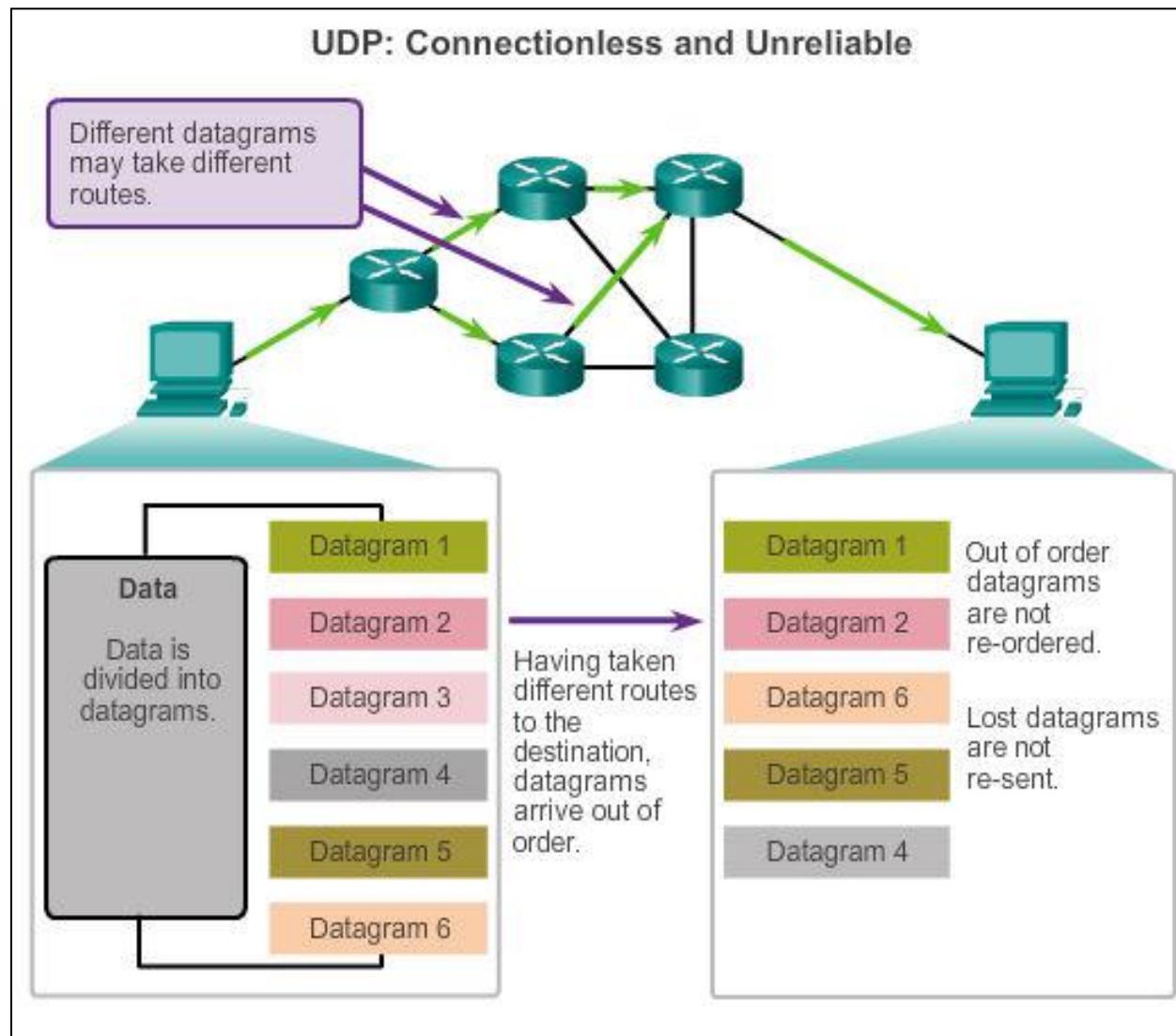
### Used by

- DNS
- Simple Network Management Protocol (SNMP)
- Dynamic Host Configuration Protocol (DHCP)
- Trivial File Transfer Protocol (TFTP)
- IP telephony or VoIP
- Online games



# UDP Communication

## Datagram Reassembly

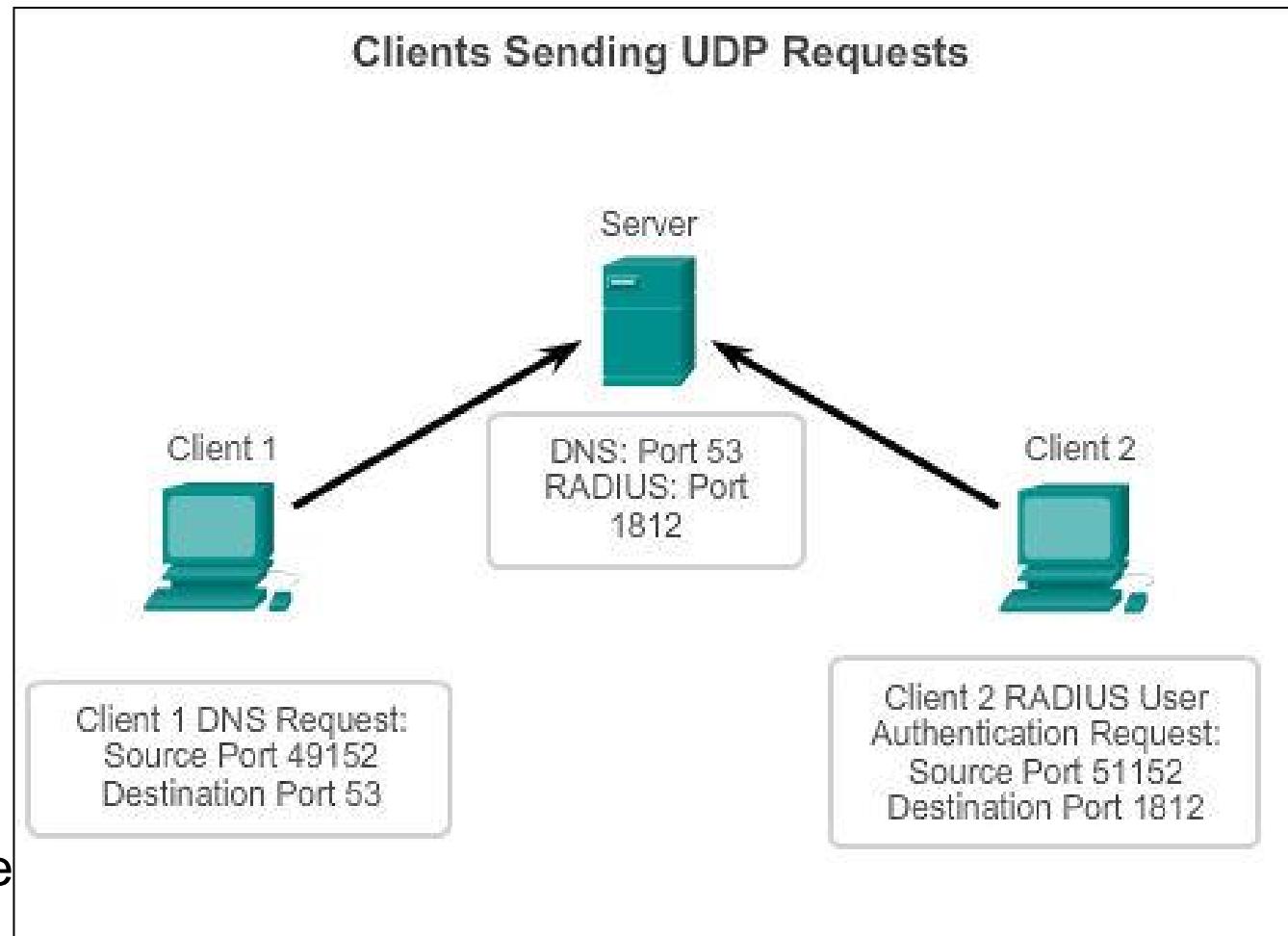




## UDP Communication

# UDP Server and Client Processes

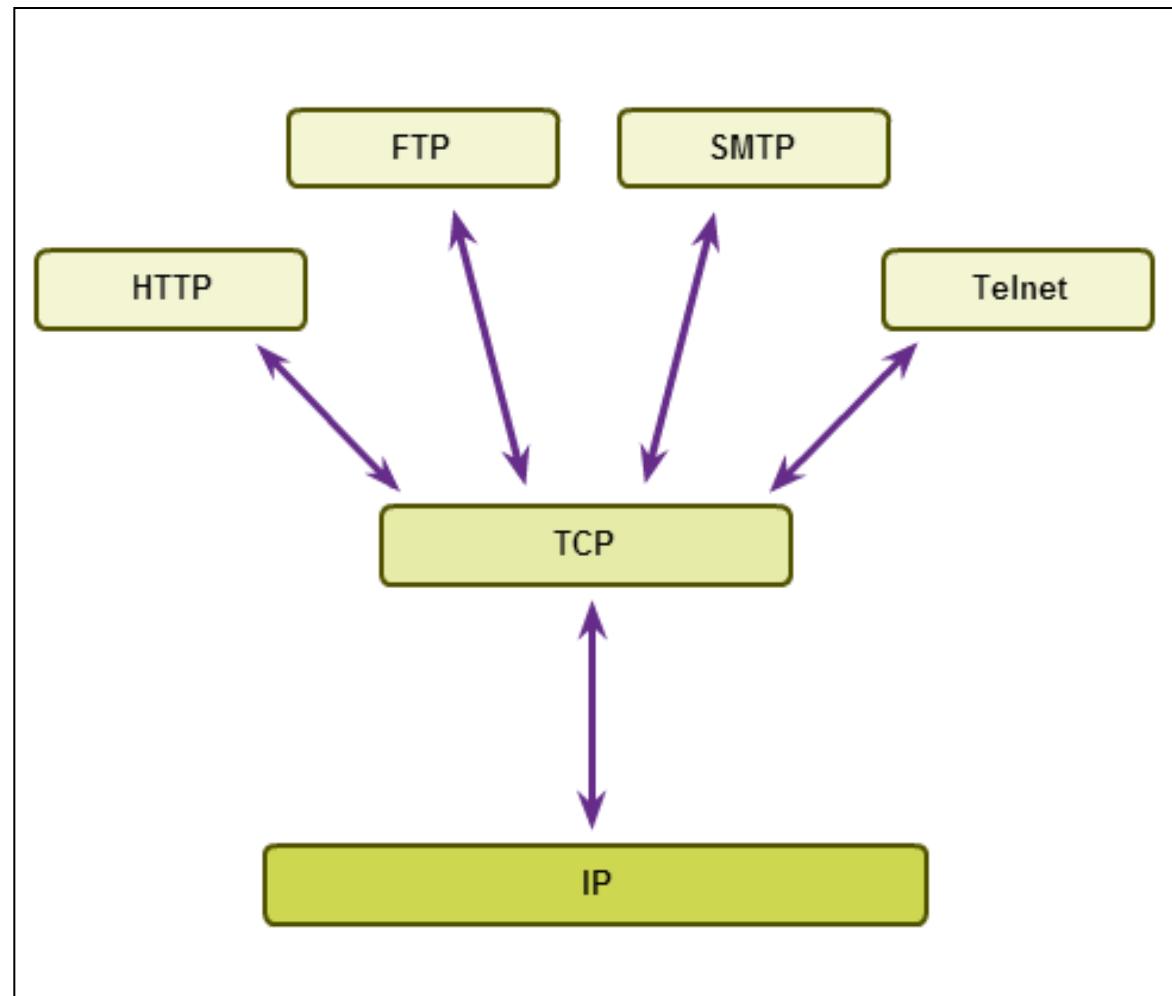
- UDP-based server applications are assigned well-known or registered port numbers.
- UDP client process randomly selects port number from range of dynamic port numbers as the source port.





TCP or UDP

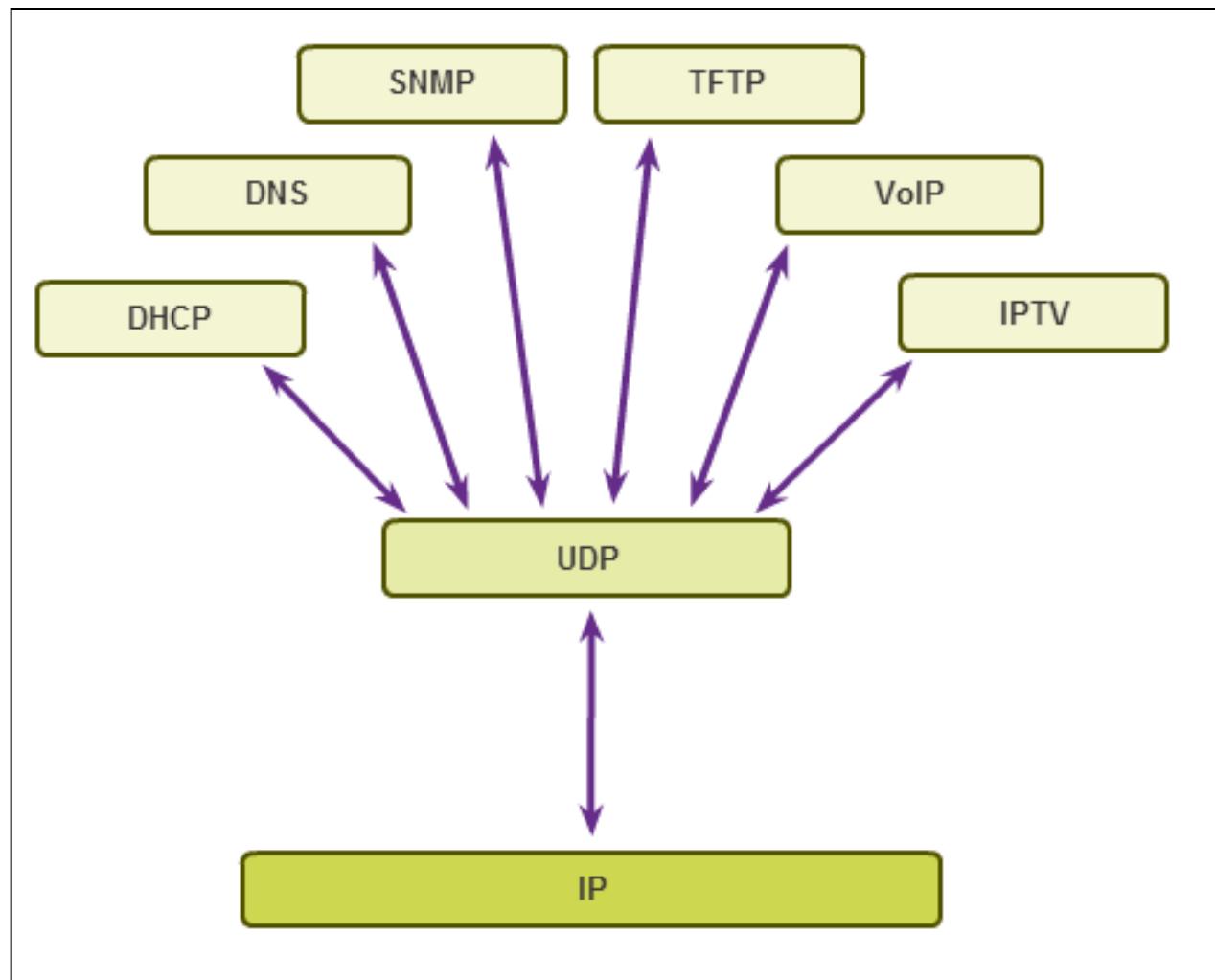
# Applications that use TCP





TCP or UDP

# Applications That Use UDP



## 7.3 Summary





# Chapter 7: Summary

In this chapter, you learned:

- The role of the transport layer is to provide three main services: multiplexing, segmentation and reassembly, and error checking. It does this by:
  - Dividing data received from an application into segments.
  - Adding a header to identify and manage each segment.
  - Using the header information to reassemble the segments back into application data.
  - Passing the assembled data to the correct application.
- How TCP and UDP operate and which popular applications use each protocol.
- Transport Layer functions are necessary to address issues in QoS and security in networks.
- Ports provide a “tunnel” for data to get from the transport layer to the appropriate application at the destination.

# Cisco | Networking Academy®

Mind Wide Open™



## Chapter 8: IP Addressing



## Introduction to Networks

Cisco | Networking Academy®  
Mind Wide Open™



# Chapter 8

- 8.0 Introduction
- 8.1 IPv4 Network Addresses
- 8.2 IPv6 Network Addresses
- 8.3 Connectivity Verification
- 8.4 Summary



# Chapter 8: Objectives

Upon completion of this chapter, you will be able to:

- Describe the structure of an IPv4 address.
- Describe the purpose of the subnet mask.
- Compare the characteristics and uses of the unicast, broadcast, and multicast IPv4 addresses.
- Compare the use of public address space and private address space.
- Explain the need for IPv6 addressing.
- Describe the representation of an IPv6 address.
- Describe types of IPv6 network addresses.
- Configure global unicast addresses.
- Describe multicast addresses.
- Describe the role of ICMP in an IP network. (Include IPv4 and IPv6.)
- Use ping and traceroute utilities to test network connectivity.



## 8.1 IPv4 Network Addresses



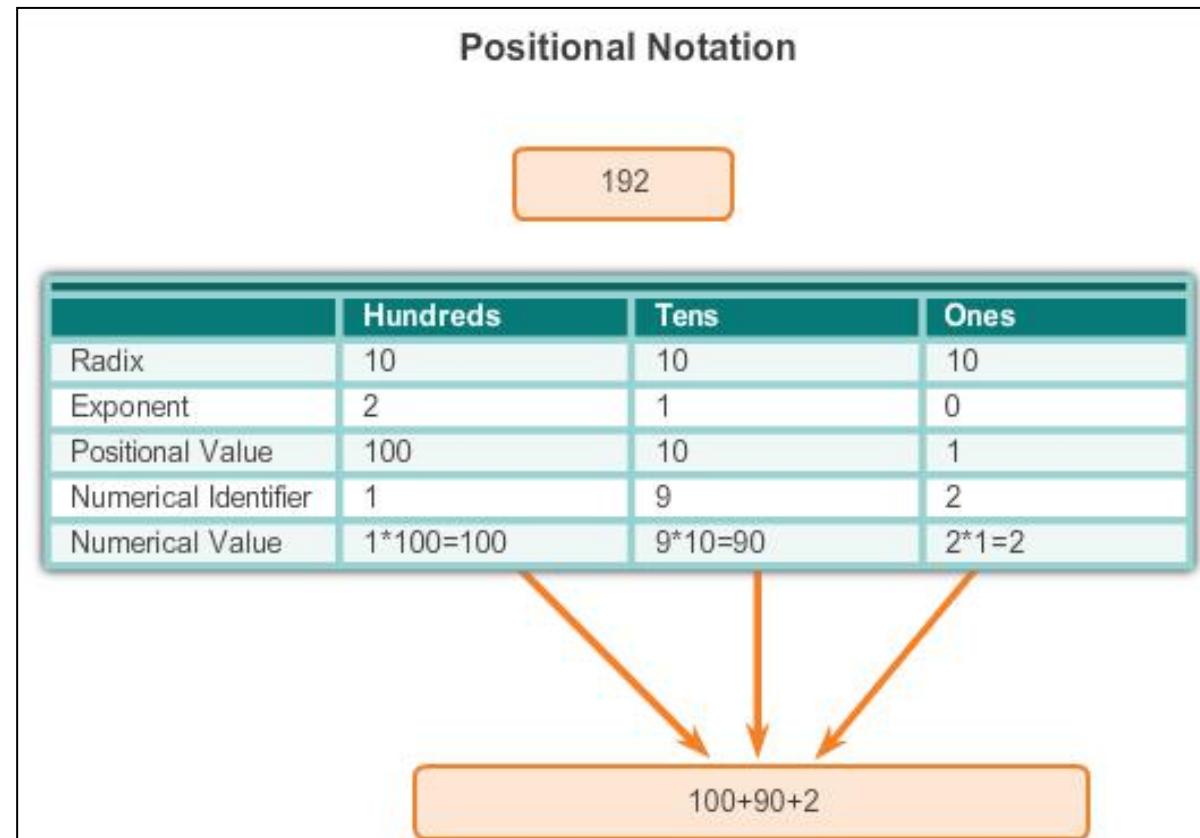
Cisco | Networking Academy®  
Mind Wide Open™



# IPv4 Address Structure

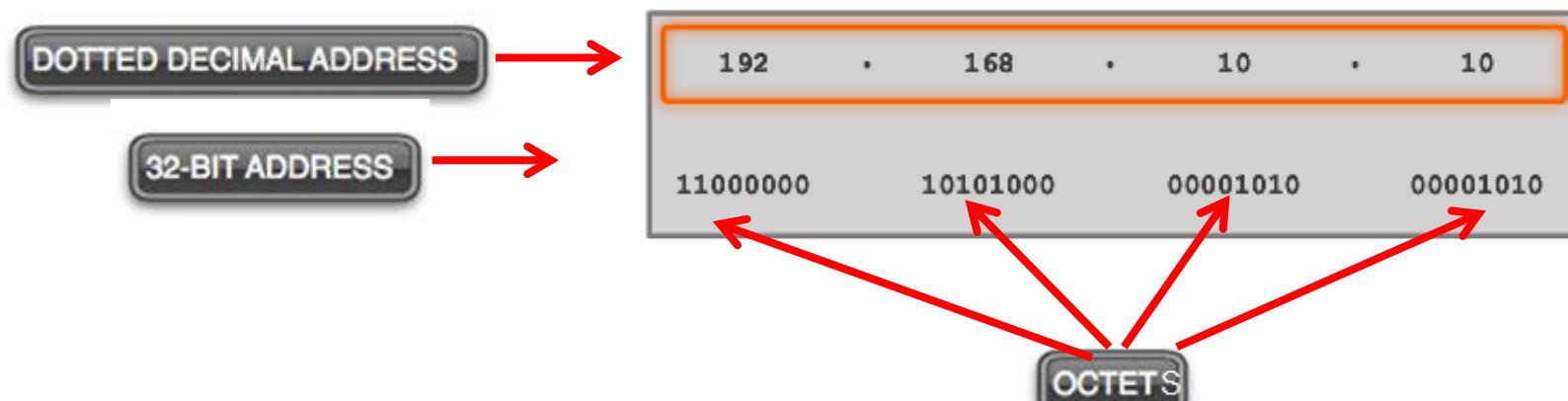
## Binary Notation

- Binary notation refers to the fact that computers communicate in 1s and 0s
- Positional notation - converting binary to decimal requires an understanding of the mathematical basis of a numbering system





# IPv4 Address Structure Binary Number System



Radix	2	2	2	2	2	2	2	2	2
Exponent	7	6	5	4	3	2	1	0	
Octet Bit Values	128	64	32	16	8	4	2	1	
Binary Address	1	1	0	0	0	0	0	0	
Binary Bit Values	128	64	0	0	0	0	0	0	

Add the binary bit values.  
 $128 + 64 = 192$



## IPv4 Address Structure

## Converting a Binary Address to Decimal

## Practice

$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$
128	64	32	16	8	4	2	1
1	0	1	1	0	0	0	0

$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$
128	64	32	16	8	4	2	1
1	1	1	1	1	1	1	1



## IPv4 Address Structure

## Converting a Binary Address to Decimal

## Practice

$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$
128	64	32	16	8	4	2	1
1	0	1	1	0	0	0	0

Answer = 176

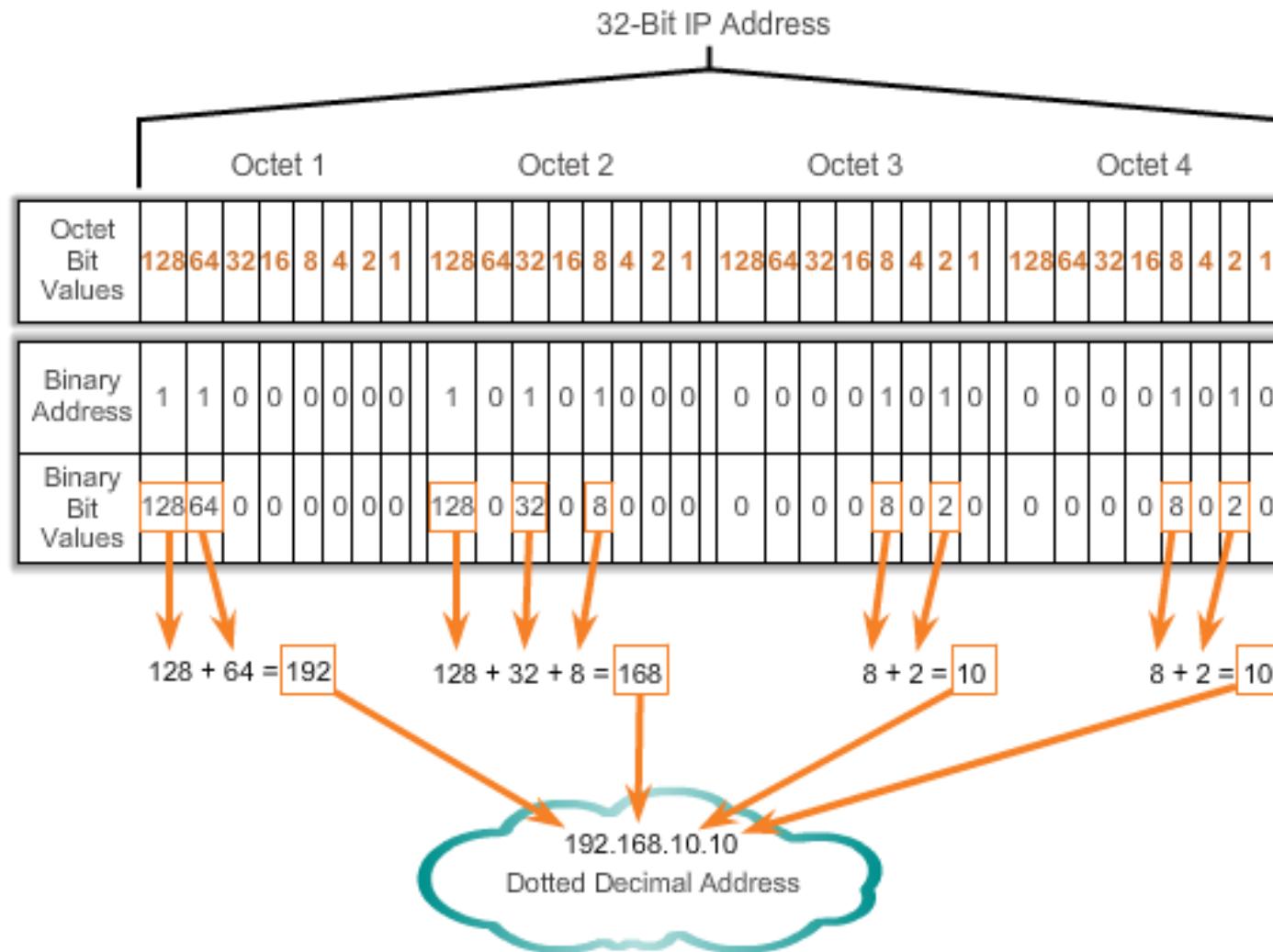
$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$
128	64	32	16	8	4	2	1
1	1	1	1	1	1	1	1

Answer = 255



## IPv4 Address Structure

## Converting a Binary Address to Decimal

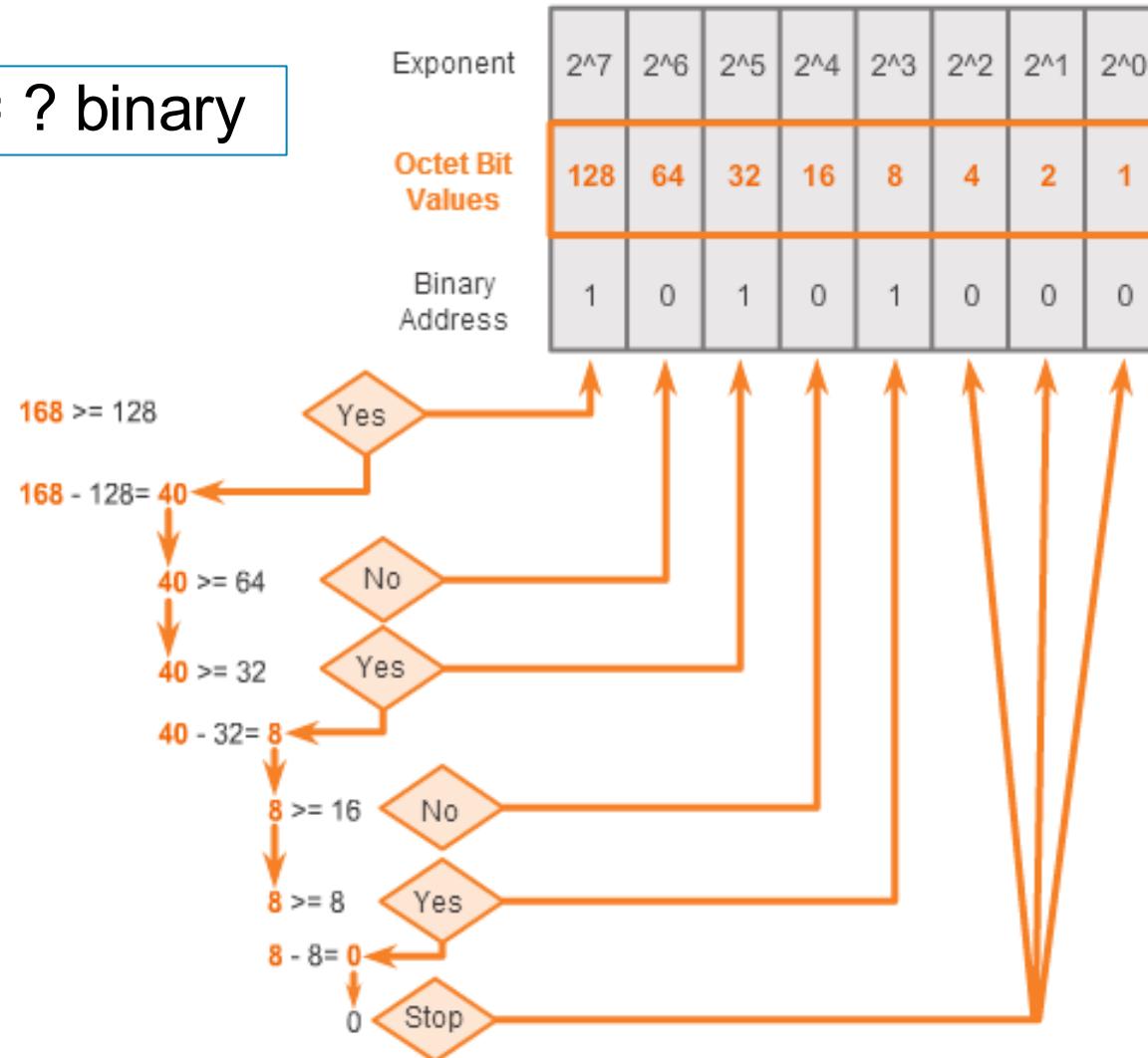




## IPv4 Address Structure

## Converting from Decimal to Binary

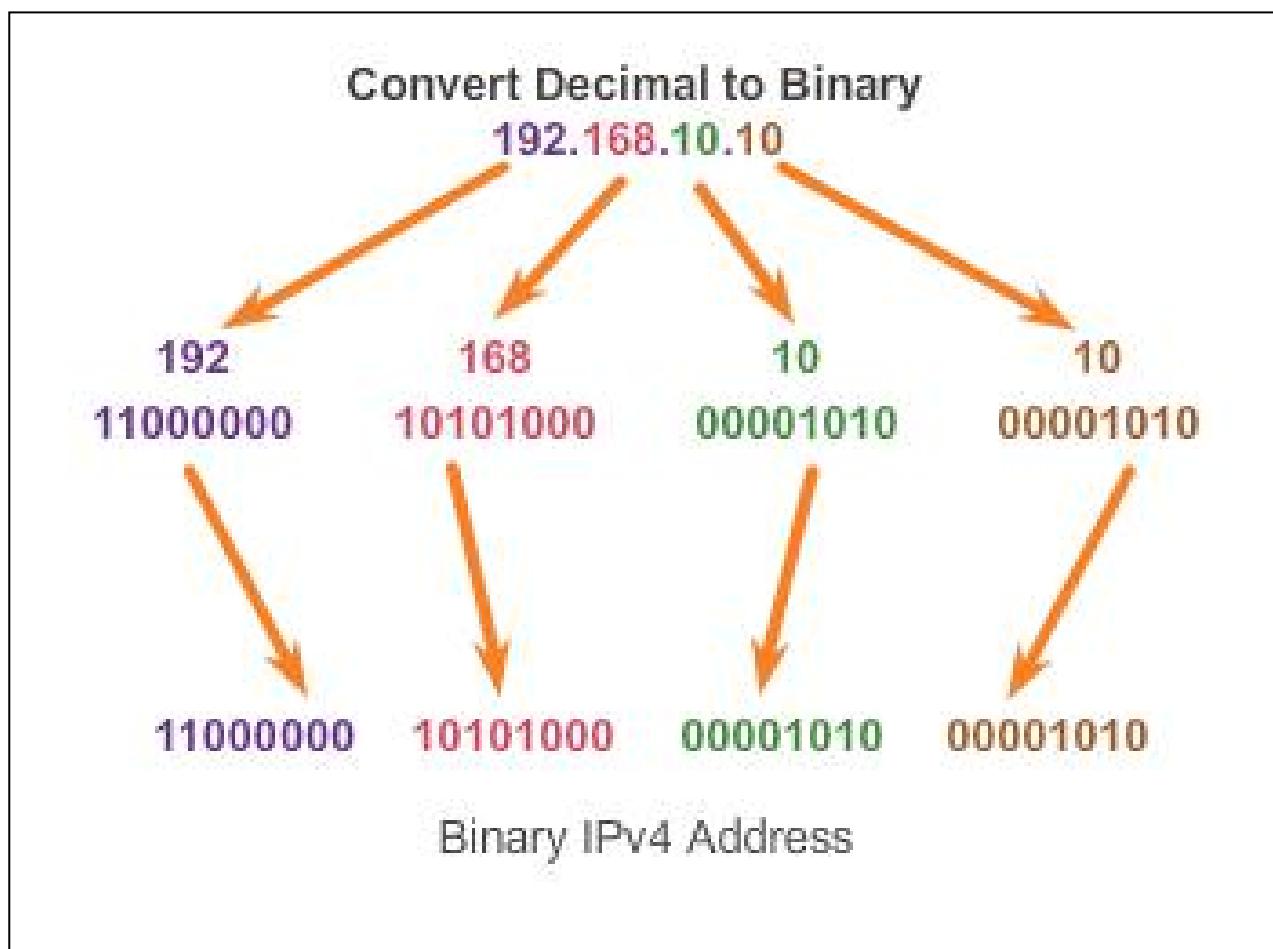
168 = ? binary





## IPv4 Address Structure

# Converting from Decimal to Binary (Cont.)

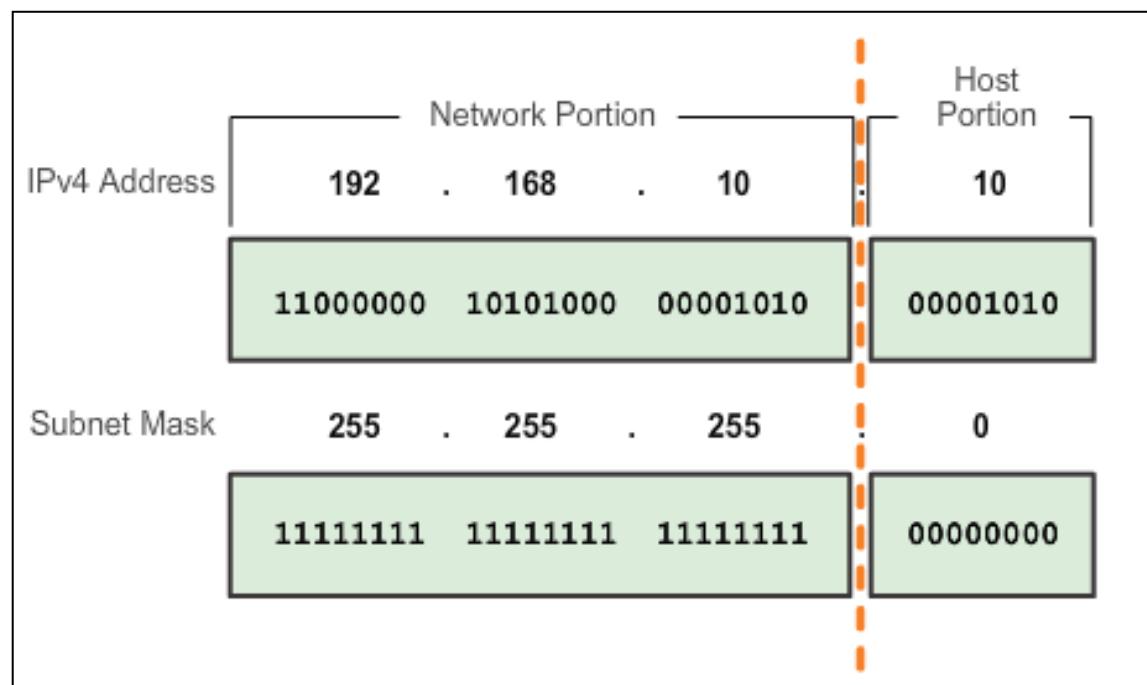




# IPv4 Subnet Mask

## Network Portion and Host Portion of an IPv4 Address

- To define the network and host portions of an address, a device uses a separate 32-bit pattern called a subnet mask
- The subnet mask does not actually contain the network or host portion of an IPv4 address, it just says where to look for these portions in a given IPv4 address





## IPv4 Subnet Mask

# Network Portion and Host Portion of an IPv4 Address (cont.)

### Valid Subnet Masks

Subnet Value
255
254
252
248
240
224
192
128
0

Bit Value								
128	64	32	16	8	4	2	1	
1	1	1	1	1	1	1	1	
1	1	1	1	1	1	1	0	
1	1	1	1	1	1	0	0	
1	1	1	1	1	0	0	0	
1	1	1	1	0	0	0	0	
1	1	1	0	0	0	0	0	
1	0	0	0	0	0	0	0	
0	0	0	0	0	0	0	0	



## IPv4 Subnet Mask

## Examining the Prefix Length

	Dotted Decimal	Significant bits shown in binary
<b>Network Address</b>	<b>10.1.1.0/24</b>	<b>10.1.1.00000000</b>
First Host Address	10.1.1.1	10.1.1.00000001
Last Host Address	10.1.1.254	10.1.1.11111110
Broadcast Address	10.1.1.255	10.1.1.11111111
Number of hosts:	$2^8 - 2 = 254$ hosts	

	Dotted Decimal	Significant bits shown in binary
<b>Network Address</b>	<b>10.1.1.0/25</b>	<b>10.1.1.00000000</b>
First Host Address	10.1.1.1	10.1.1.00000001
Last Host Address	10.1.1.126	10.1.1.01111110
Broadcast Address	10.1.1.127	10.1.1.01111111
Number of hosts:	$2^7 - 2 = 126$ hosts	

	Dotted Decimal	Significant bits shown in binary
<b>Network Address</b>	<b>10.1.1.0/26</b>	<b>10.1.1.00000000</b>
First Host Address	10.1.1.1	10.1.1.00000001
Last Host Address	10.1.1.62	10.1.1.00111110
Broadcast Address	10.1.1.63	10.1.1.00111111
Number of hosts:	$2^6 - 2 = 62$ hosts	



## IPv4 Subnet Mask

## Examining the Prefix Length (cont.)

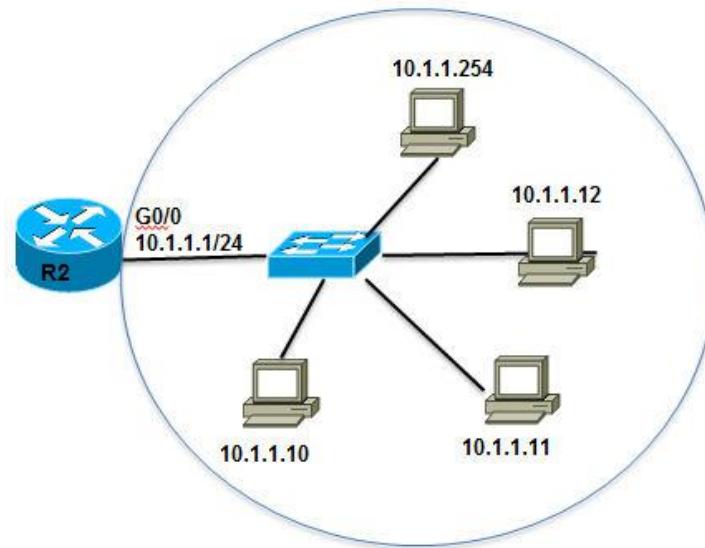
	Dotted Decimal	Significant bits shown in binary
Network Address	10.1.1.0/27	10.1.1.00000000
First Host Address	10.1.1.1	10.1.1.00000001
Last Host Address	10.1.1.30	10.1.1.00011110
Broadcast Address	10.1.1.31	10.1.1.00011111
Number of hosts: $2^5 - 2 = 30$ hosts		

Network Address	10.1.1.0/28	10.1.1.00000000
First Host Address	10.1.1.1	10.1.1.00000001
Last Host Address	10.1.1.14	10.1.1.00001110
Broadcast Address	10.1.1.15	10.1.1.00001111
Number of hosts: $2^4 - 2 = 14$ hosts		



## IPv4 Subnet Mask

## IPv4 Network, Host, and Broadcast Address

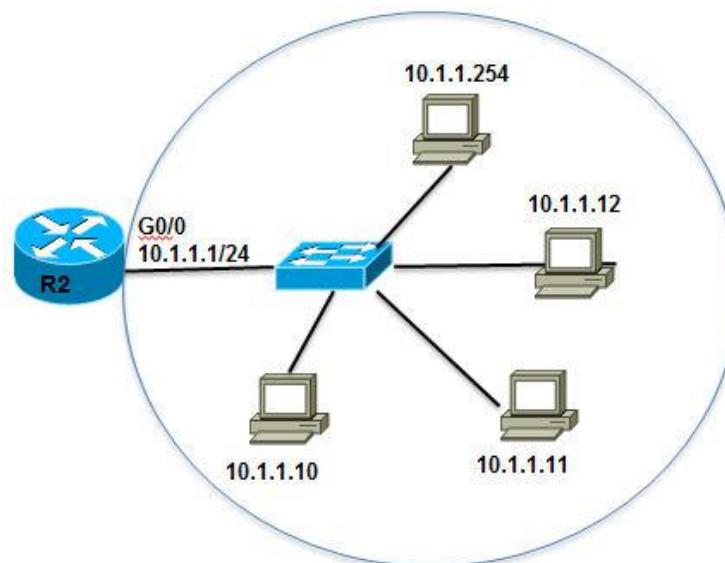


10.1.1.0/24

Network Portion			Host Portion	
10	1	1	0	
00001010	00000001	00000001	00000000	All 0s – NETWORK ADDRESS
10	1	1	10	
00001010	00000001	00000001	00001010	0s and 1s in host portion
10	1	1	255	
00001010	00000001	00000001	11111111	All 1s – BROADCAST ADDRESS



# IPv4 Subnet Mask First Host and Last Host Addresses



10.1.1.0/24

Network Portion			Host Portion	
10	1	1	1	FIRST HOST
00001010	00000001	00000001	00000001	All 0s and a 1 in the host portion
10	1	1	254	LAST HOST
00001010	00000001	00000001	11111110	All 1s and a 0 in the host portion



# IPv4 Subnet Mask Bitwise AND Operation

1 AND 1 = 1    1 AND 0 = 0    0 AND 1 = 0    0 AND 0 = 0

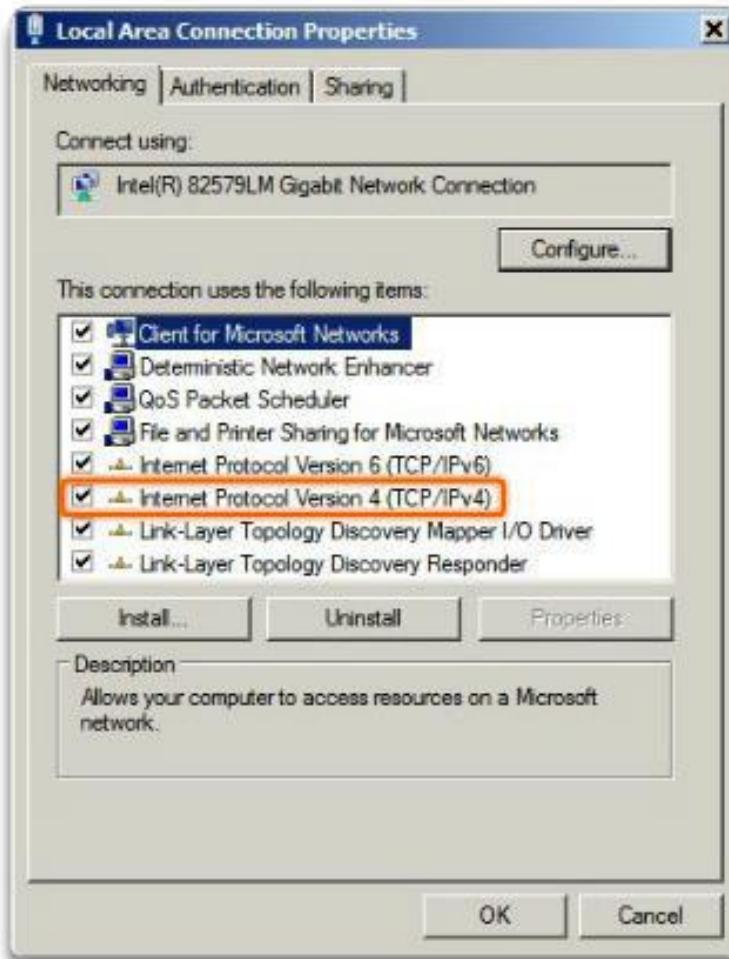
IPv4 Address	192	.	168	.	10	.	10
	11000000		10101000		00001010		00001010
Subnet Mask	255	.	255	.	255	.	0
	11111111		11111111		11111111		00000000
Network Address	192	.	168	.	10	.	0
	11000000		10101000		00001010		00000000



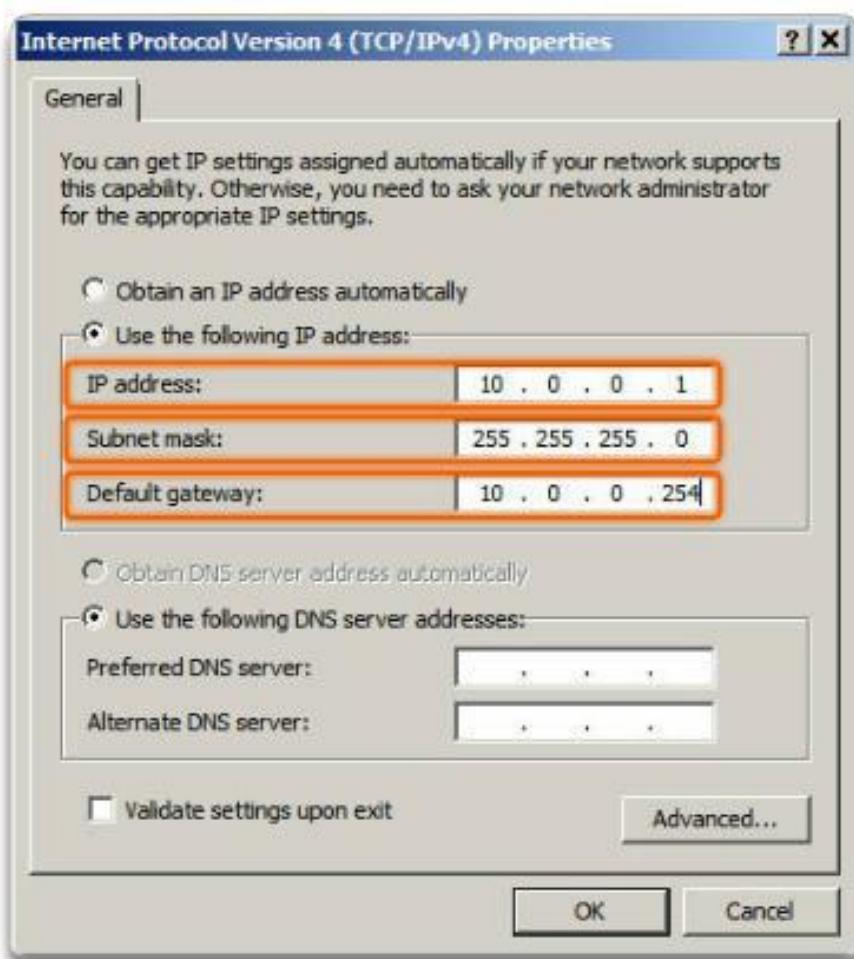
## IPv4 Unicast, Broadcast, and Multicast

# Assigning a Static IPv4 Address to a Host

### LAN Interface Properties



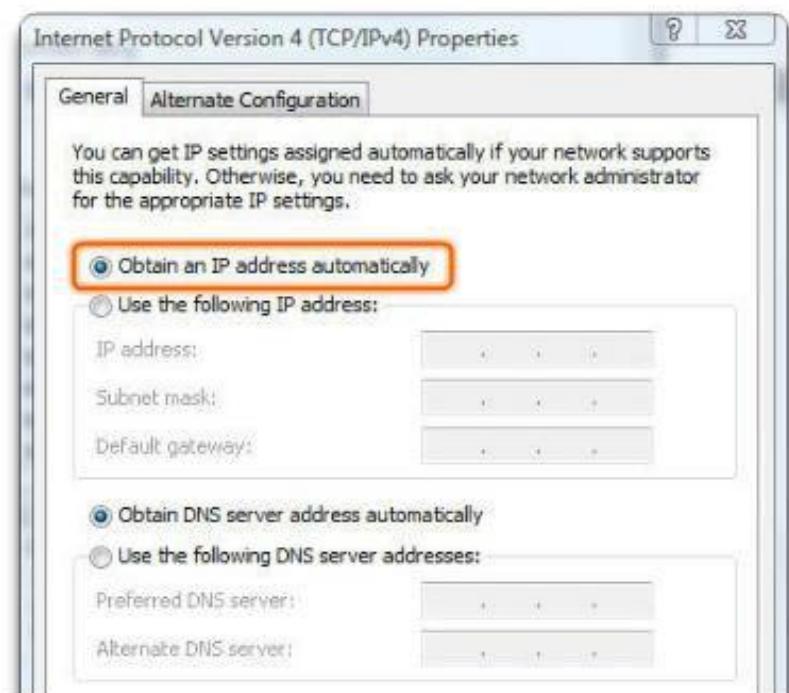
### Configuring a Static IPv4 Address





# IPv4 Unicast, Broadcast, and Multicast

## Assigning a Dynamic IPv4 Address to a Host



```
C:\> ipconfig

Ethernet adapter Local Area Connection:

  IP Address . . . . . 10.1.1.101
  Subnet Mask . . . . . 255.255.255.0
  Default Gateway . . . . . 10.1.1.1
  DNS Servers . . . . . 172.16.99.150
                                         172.16.99.151

C:\>
```

**Verification**

A screenshot of a Windows Command Prompt window titled "cmd". It displays the output of the "ipconfig" command. The output shows the following network configuration for the "Ethernet adapter Local Area Connection": IP Address: 10.1.1.101, Subnet Mask: 255.255.255.0, Default Gateway: 10.1.1.1, and DNS Servers: 172.16.99.150 and 172.16.99.151. Below the command prompt, a large rectangular box contains the word "Verification" in white text.

DHCP – The preferred method of assigning IPv4 addresses to hosts on large networks because it reduces the burden on network support staff and virtually eliminates entry errors.

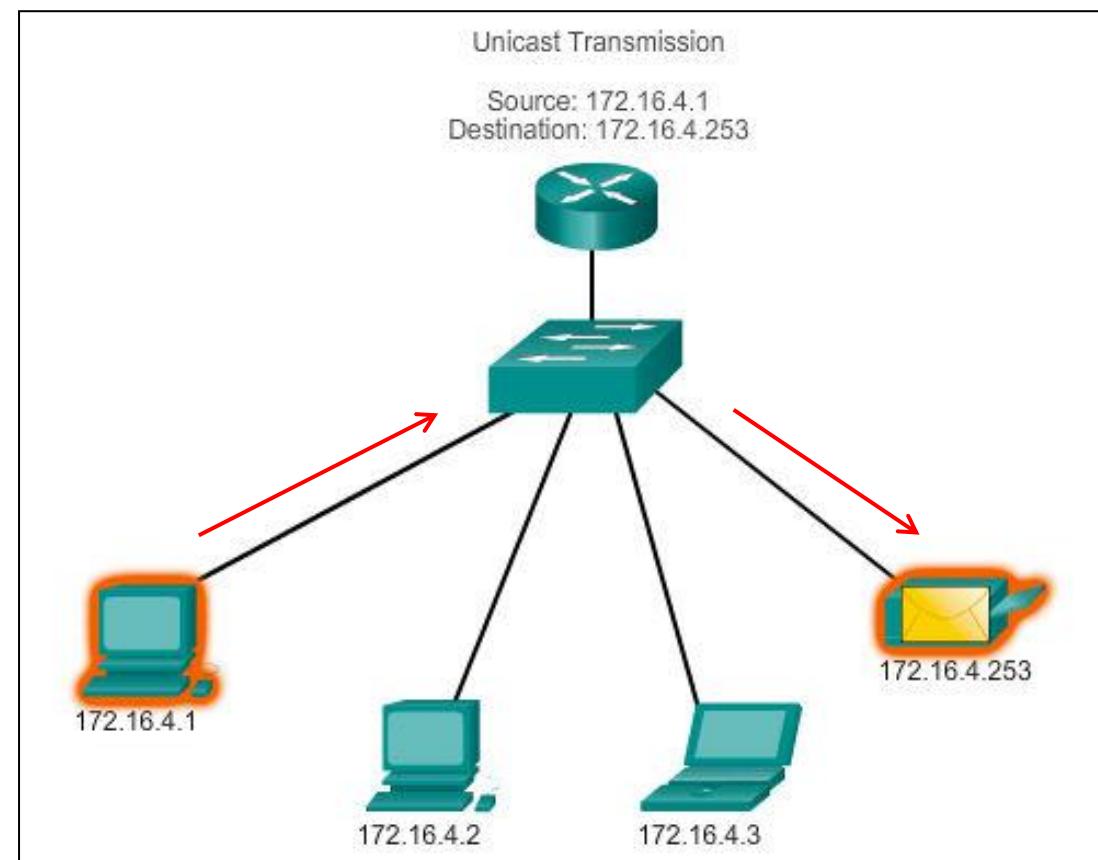


# IPv4 Unicast, Broadcast, and Multicast

## Unicast Transmission

In an IPv4 network, the hosts can communicate one of three different ways:  
**Unicast**, Broadcast, and Multicast

**#1 Unicast** – the process of sending a packet from one host to an individual host.





# IPv4 Unicast, Broadcast, and Multicast

## Broadcast Transmission

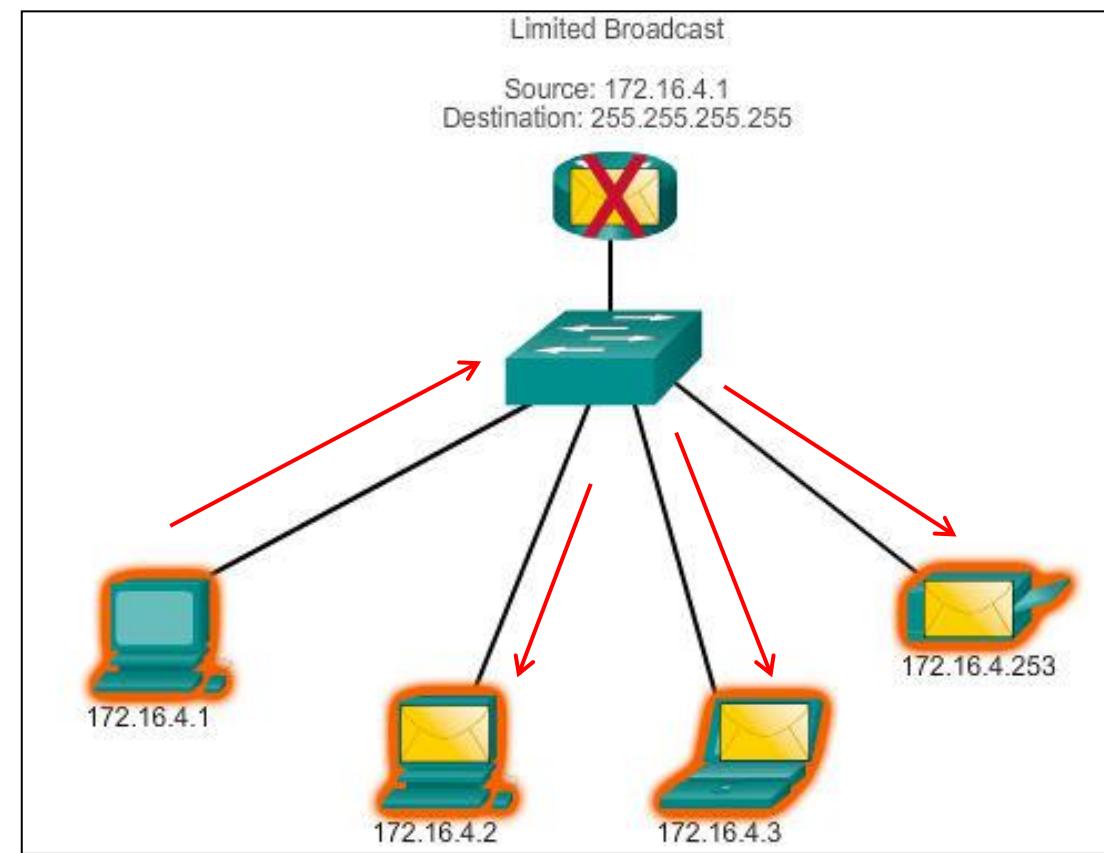
In an IPv4 network, the hosts can communicate one of three different ways: Unicast, **Broadcast**, and Multicast.

**#2 Broadcast** – the process of sending a packet from one host to all hosts in the network.

**NOTE:** Routers do not forward a limited broadcast!

### Directed broadcast

- Destination 172.16.4.255
- Hosts within the 172.16.4.0/24 network





## IPv4 Unicast, Broadcast, and Multicast

# Multicast Transmission

In an IPv4 network, the hosts can communicate one of three different ways: Unicast, Broadcast, and **Multicast**.

**#3 Multicast** – The process of sending a packet from one host to a selected group of hosts, possibly in different networks.

- Reduces traffic
- Reserved for addressing multicast groups – 224.0.0.0 to 239.255.255.255.
- Link local – 224.0.0.0 to 224.0.0.255 (Example: routing information exchanged by routing protocols)
- Globally scoped addresses – 224.0.1.0 to 238.255.255.255 (Example: 224.0.1.1 has been reserved for Network Time Protocol)



## Types of IPv4 Address

# Public and Private IPv4 Addresses

### Private address blocks are:

- Hosts that do not require access to the Internet can use private addresses
  - 10.0.0.0 to 10.255.255.255 (10.0.0.0/8)
  - 172.16.0.0 to 172.31.255.255 (172.16.0.0/12)
  - 192.168.0.0 to 192.168.255.255 (192.168.0.0/16)

### Shared address space addresses:

- Not globally routable
- Intended only for use in service provider networks
- Address block is 100.64.0.0/10



## Types of IPv4 Address

# Special Use IPv4 Addresses

- **Network and Broadcast addresses** – within each network the first and last addresses cannot be assigned to hosts
- **Loopback address** – 127.0.0.1 a special address that hosts use to direct traffic to themselves (addresses 127.0.0.0 to 127.255.255.255 are reserved)
- **Link-Local address** – 169.254.0.0 to 169.254.255.255 (169.254.0.0/16) addresses can be automatically assigned to the local host
- **TEST-NET addresses** – 192.0.2.0 to 192.0.2.255 (192.0.2.0/24) set aside for teaching and learning purposes, used in documentation and network examples
- **Experimental addresses** – 240.0.0.0 to 255.255.255.254 are listed as reserved



## Types of IPv4 Address

# Legacy Classful Addressing

IP Address Classes

Address Class	1st octet range (decimal)	1st octet bits (green bits do not change)	Network(N) and Host(H) parts of address	Default subnet mask (decimal and binary)	Number of possible networks and hosts per network
A	1-127**	00000000-01111111	N.H.H.H	255.0.0.0	128 nets ( $2^7$ ) 16,777,214 hosts per net ( $2^{24-2}$ )
B	128-191	10000000-10111111	N.N.H.H	255.255.0.0	16,384 nets ( $2^{14}$ ) 65,534 hosts per net ( $2^{16-2}$ )
C	192-223	11000000-11011111	N.N.N.H	255.255.255.0	2,097,150 nets ( $2^{21}$ ) 254 hosts per net ( $2^{8-2}$ )
D	224-239	11100000-11101111	NA (multicast)		
E	240-255	11110000-11111111	NA (experimental)		



## Types of IPv4 Address

# Legacy Classful Addressing (cont.)

## Classless Addressing

- Formal name is Classless Inter-Domain Routing (CIDR, pronounced “cider”)
- Created a new set of standards that allowed service providers to allocate IPv4 addresses on any address bit boundary (prefix length) instead of only by a class A, B, or C address



Types of IPv4 Address

# Assignment of IP Addresses

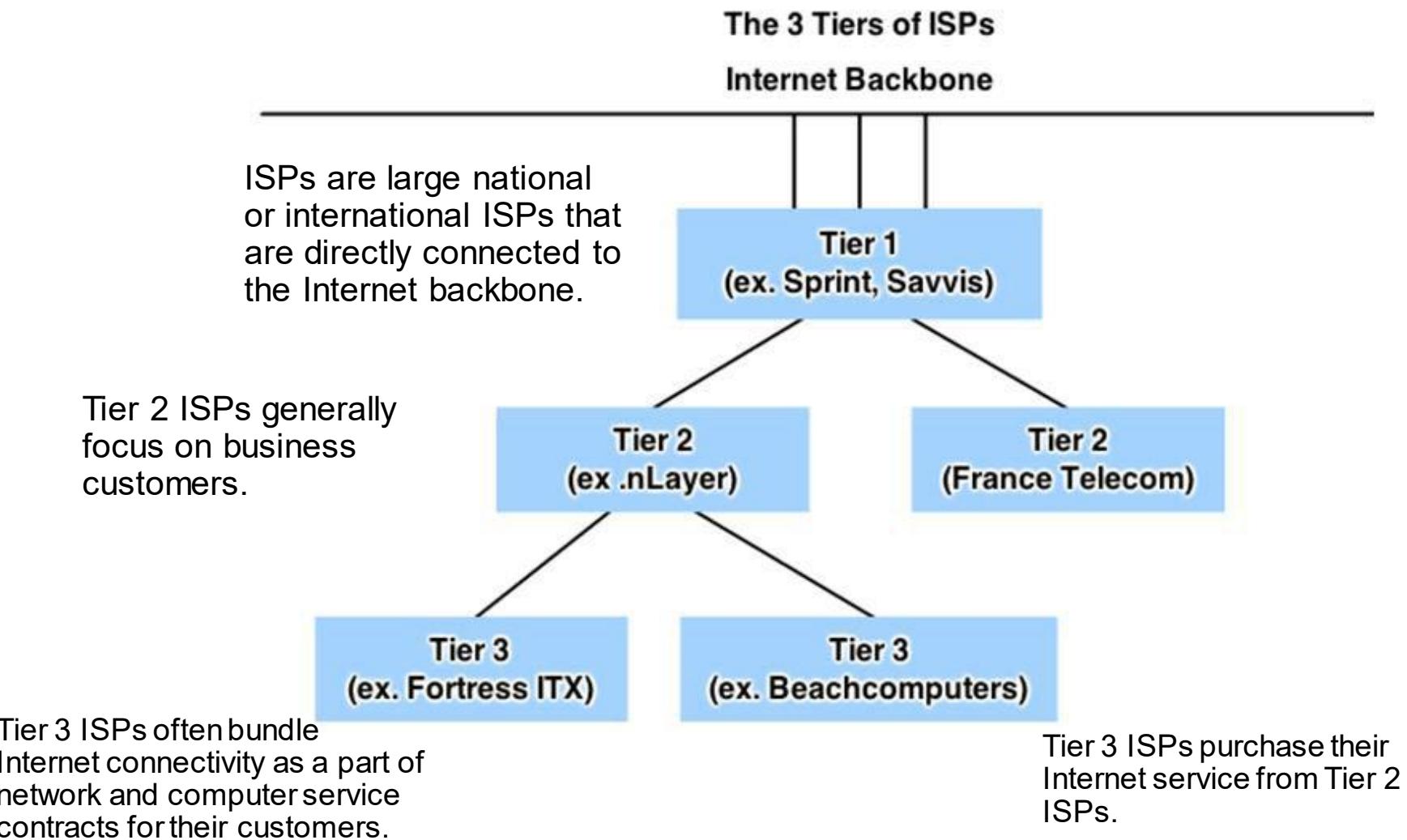
## Regional Internet Registries (RIRs)





## Types of IPv4 Address

# Assignment of IP Addresses (Cont.)



## 8.2 IPv6 Network Addresses





## IPv4 Issues

# The Need for IPv6

- IPv6 is designed to be the successor to IPv4.
- Depletion of IPv4 address space has been the motivating factor for moving to IPv6.
- Projections show that all five RIRs will run out of IPv4 addresses between 2015 and 2020.
- With an increasing Internet population, a limited IPv4 address space, issues with NAT and an Internet of things, the time has come to begin the transition to IPv6!
- IPv4 has a theoretical maximum of 4.3 billion addresses, plus private addresses in combination with NAT.
- IPv6 larger 128-bit address space provides for 340 undecillion addresses.
- IPv6 fixes the limitations of IPv4 and includes additional enhancements, such as ICMPv6.

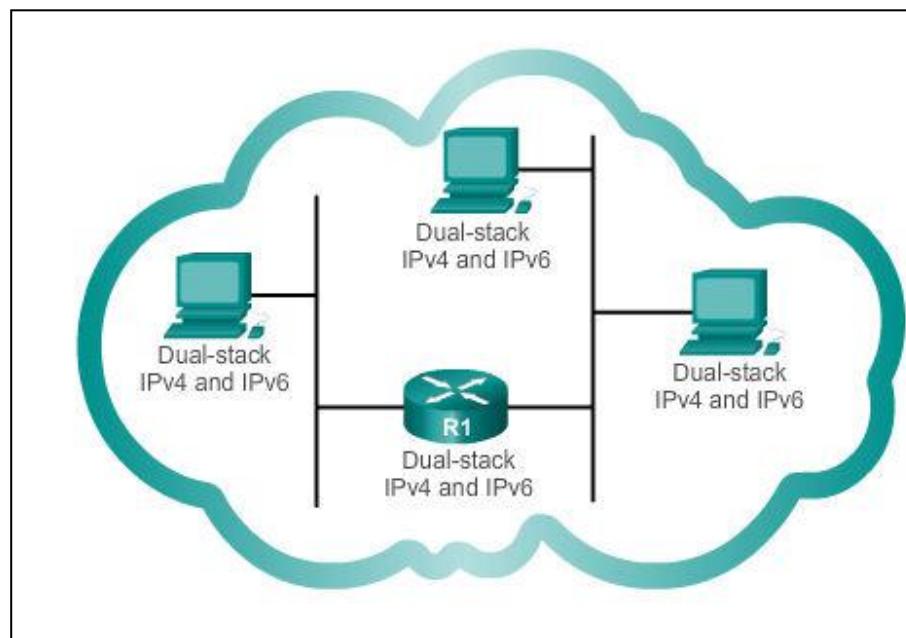


## IPv4 Issues

# IPv4 and IPv6 Coexistence

The migration techniques can be divided into three categories:  
Dual-stack, Tunnelling, and Translation.

### Dual-stack



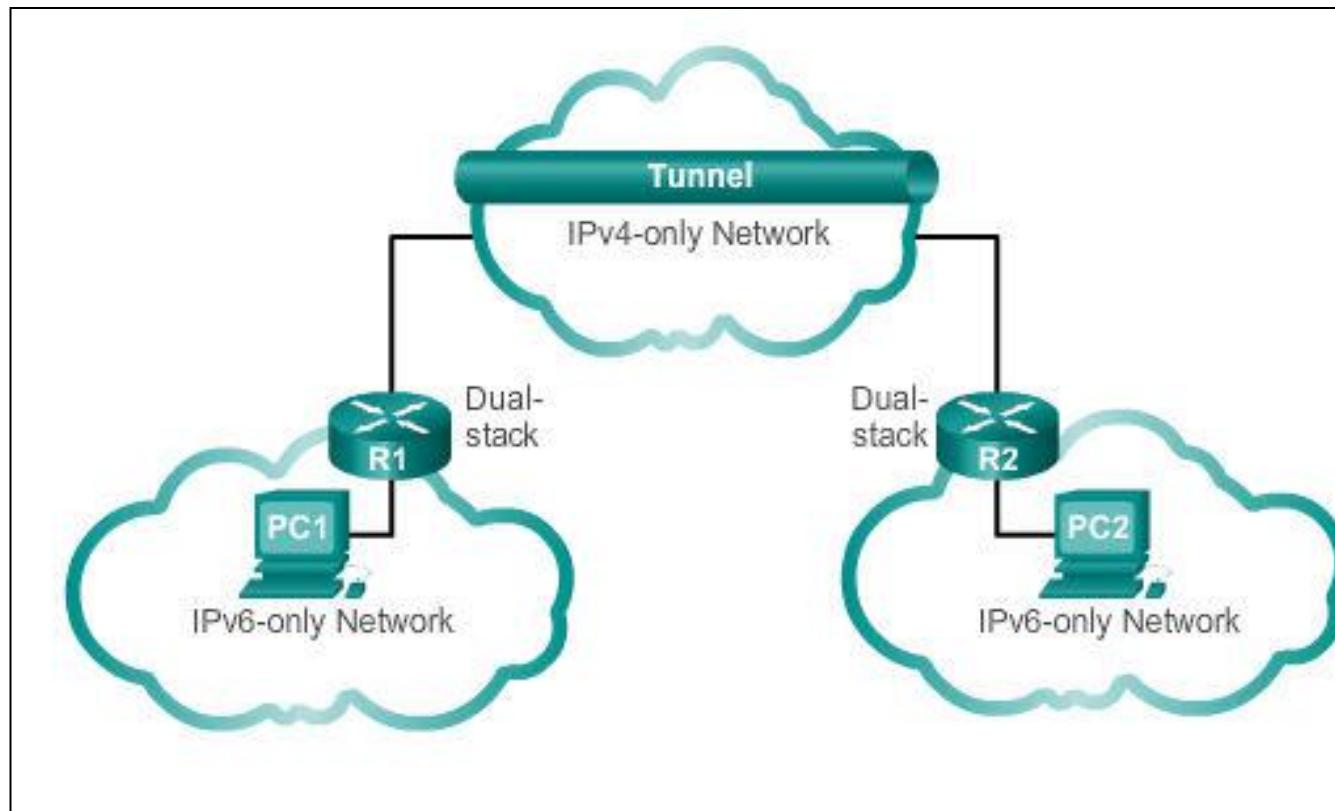
**Dual-stack:** Allows IPv4 and IPv6 to coexist on the same network.  
Devices run both IPv4 and IPv6 protocol stacks simultaneously.



## IPv4 Issues

## IPv4 and IPv6 Coexistence (cont.)

## Tunnelling



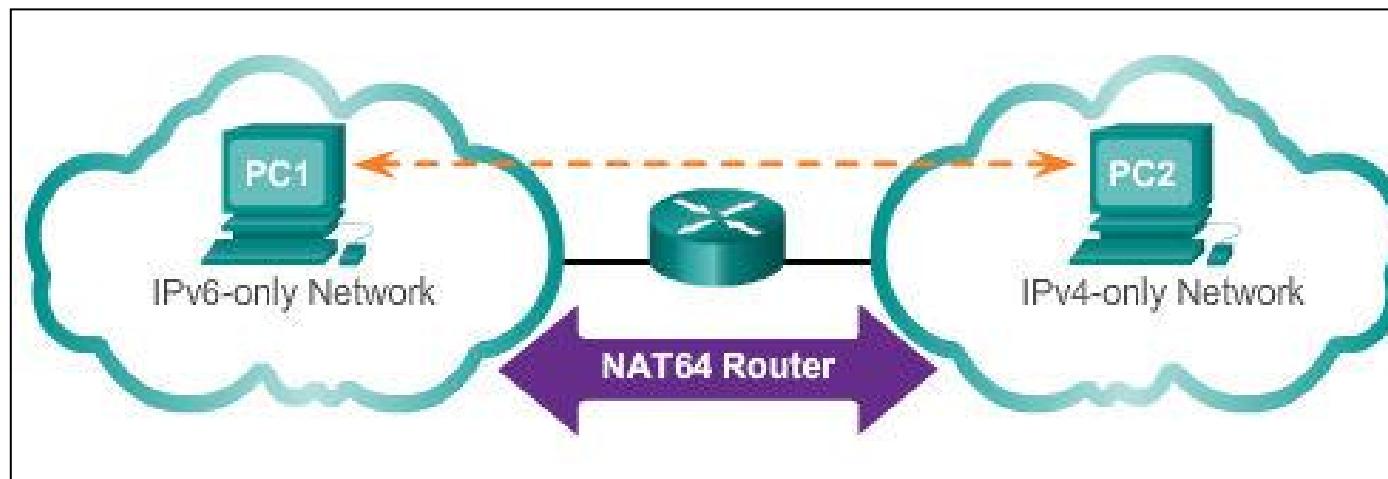
**Tunnelling:** A method of transporting an IPv6 packet over an IPv4 network. The IPv6 packet is encapsulated inside an IPv4 packet.



## IPv4 Issues

## IPv4 and IPv6 Coexistence (cont.)

## Translation



**Translation:** The Network Address Translation 64 (NAT64) allows IPv6-enabled devices to communicate with IPv4-enabled devices using a translation technique similar to NAT for IPv4. An IPv6 packet is translated to an IPv4 packet, and vice versa.



## IPv6 Addressing

## Hexadecimal Number System

- Hexadecimal is a base sixteen system.
- Base 16 numbering system uses the numbers 0 to 9 and the letters A to F.
- Four bits (half of a byte) can be represented with a single hexadecimal value.

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



# IPv6 Addressing

## Hexadecimal Number System (cont.)

Look at the binary bit patterns that match the decimal and hexadecimal values

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



## IPv6 Addressing

# IPv6 Address Representation

- 128 bits in length and written as a string of hexadecimal values
- In IPv6, 4 bits represents a single hexadecimal digit, 32 hexadecimal value = IPv6 address

**2001:0DB8:0000:1111:0000:0000:0000:0200**

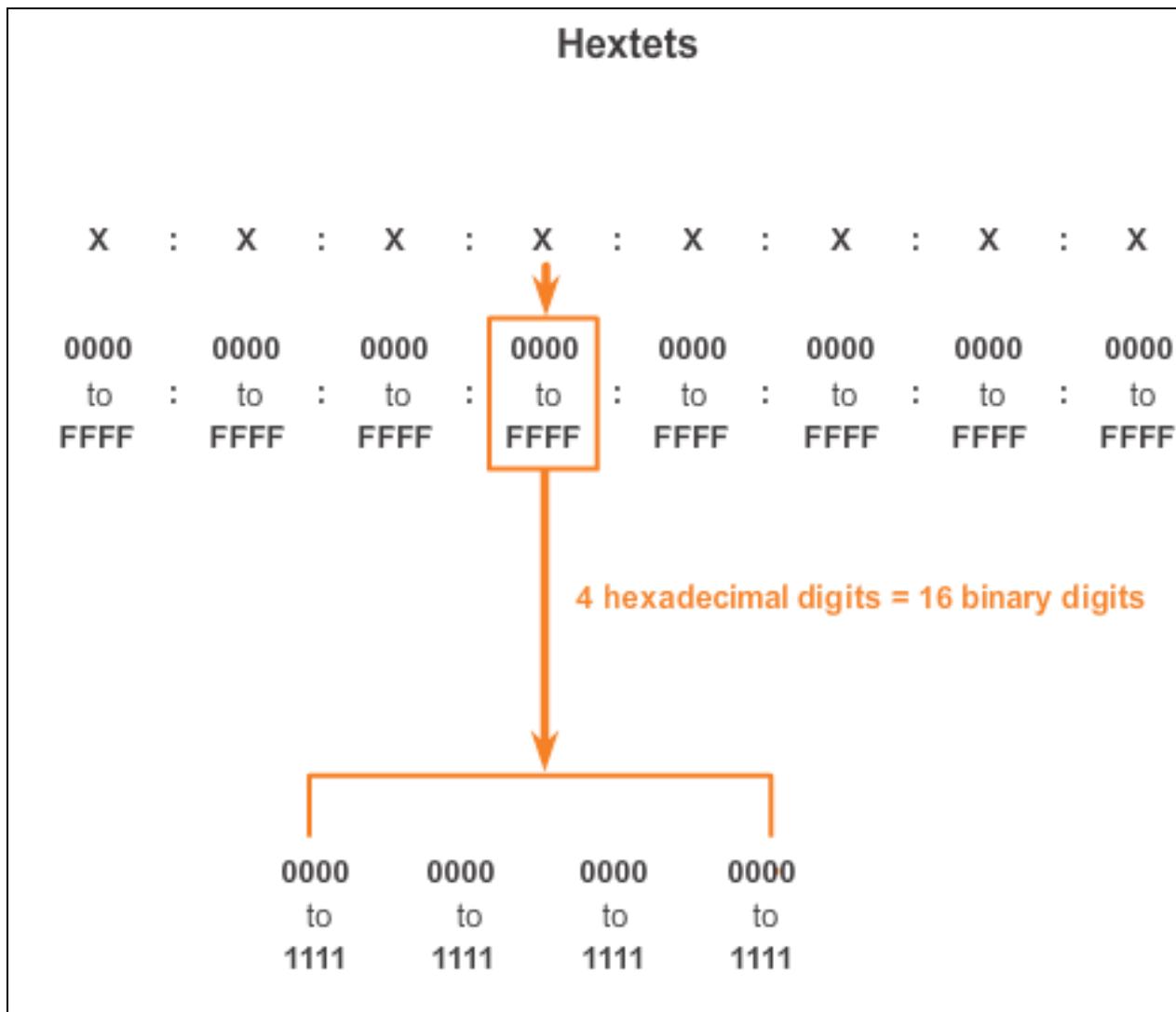
**FE80:0000:0000:0000:0123:4567:89AB:CDEF**

- Hextet used to refer to a segment of 16 bits or four hexadecimals
- Can be written in either lowercase or uppercase



## IPv6 Addressing

## IPv6 Address Representation (cont.)





## IPv6 Addressing

# Rule 1- Omitting Leading 0s

- The first rule to help reduce the notation of IPv6 addresses is any leading 0s (zeros) in any 16-bit section or hextet can be omitted.
- 01AB can be represented as 1AB.
- 09F0 can be represented as 9F0.
- 0A00 can be represented as A00.
- 00AB can be represented as AB.

Preferred	2001: <b>0</b> DB8: <b>000</b> A: <b>1000</b> : <b>000</b> 0: <b>000</b> 0: <b>000</b> 0: <b>0100</b>
No leading <u>0s</u>	2001: DB8: A:1000: 0: 0: 0: 100
Compressed	2001:DB8:A:1000:0:0:0:100



## IPv6 Addressing

# Rule 2 - Omitting All 0 Segments

- A double colon (::) can replace any single, contiguous string of one or more 16-bit segments (hextets) consisting of all 0's.
- Double colon (::) can only be used once within an address otherwise the address will be ambiguous.
- Known as the *compressed format*.
- Incorrect address - 2001:0DB8::ABCD::1234.

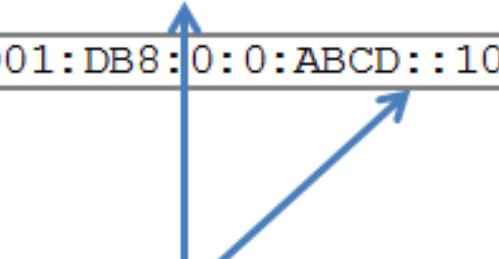


## IPv6 Addressing

## Rule 2 - Omitting All 0 Segments (cont.)

## Example #1

Preferred	2001: <b>0</b> DB8: <b>0000</b> : <b>0000</b> :ABCD: <b>0000</b> : <b>0000</b> : <b>0100</b>
Omit leading 0s	2001: DB8: <b>0</b> : <b>0</b> :ABCD: <b>0</b> : <b>0</b> : 100
Compressed	2001:DB8::ABCD:0:0:100
OR	
Compressed	2001:DB8: <b>0</b> : <b>0</b> :ABCD::100



Only one :: may be used.

## Example #2

Preferred	FE80: <b>0000</b> : <b>0000</b> : <b>0000</b> : <b>0123</b> :4567:89AB:CDEF
Omit leading 0s	FE80: <b>0</b> : <b>0</b> : <b>0</b> : <b>123</b> :4567:89AB:CDEF
Compressed	FE80: <b>0</b> : <b>0</b> : <b>0</b> : <b>123</b> :4567:89AB:CDEF

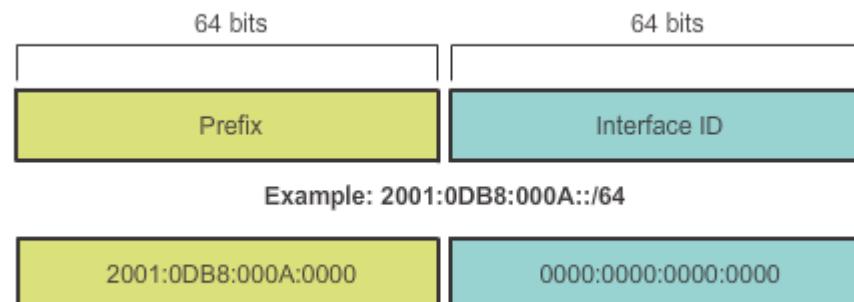


## Types of IPv6 Addresses

# IPv6 Prefix Length

- IPv6 does not use the dotted-decimal subnet mask notation
- Prefix length indicates the network portion of an IPv6 address using the following format:
  - IPv6 address/prefix length
  - Prefix length can range from 0 to 128
  - Typical prefix length is /64

## /64 Prefix





## Types of IPv6 Addresses

# IPv6 Address Types

There are three types of IPv6 addresses:

- Unicast
- Multicast
- Anycast.

**Note:** IPv6 does not have broadcast addresses.

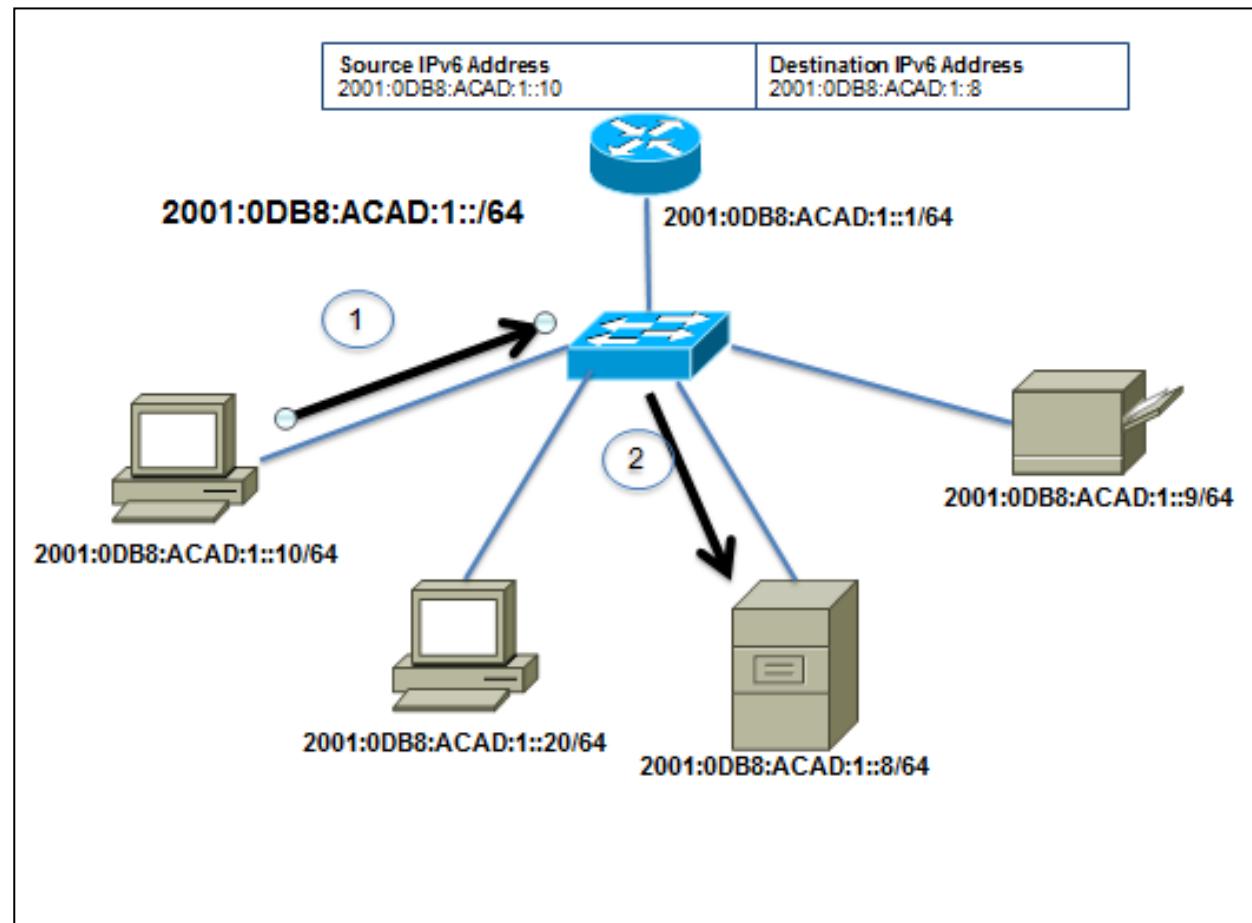


## Types of IPv6 Addresses

# IPv6 Unicast Addresses

## Unicast

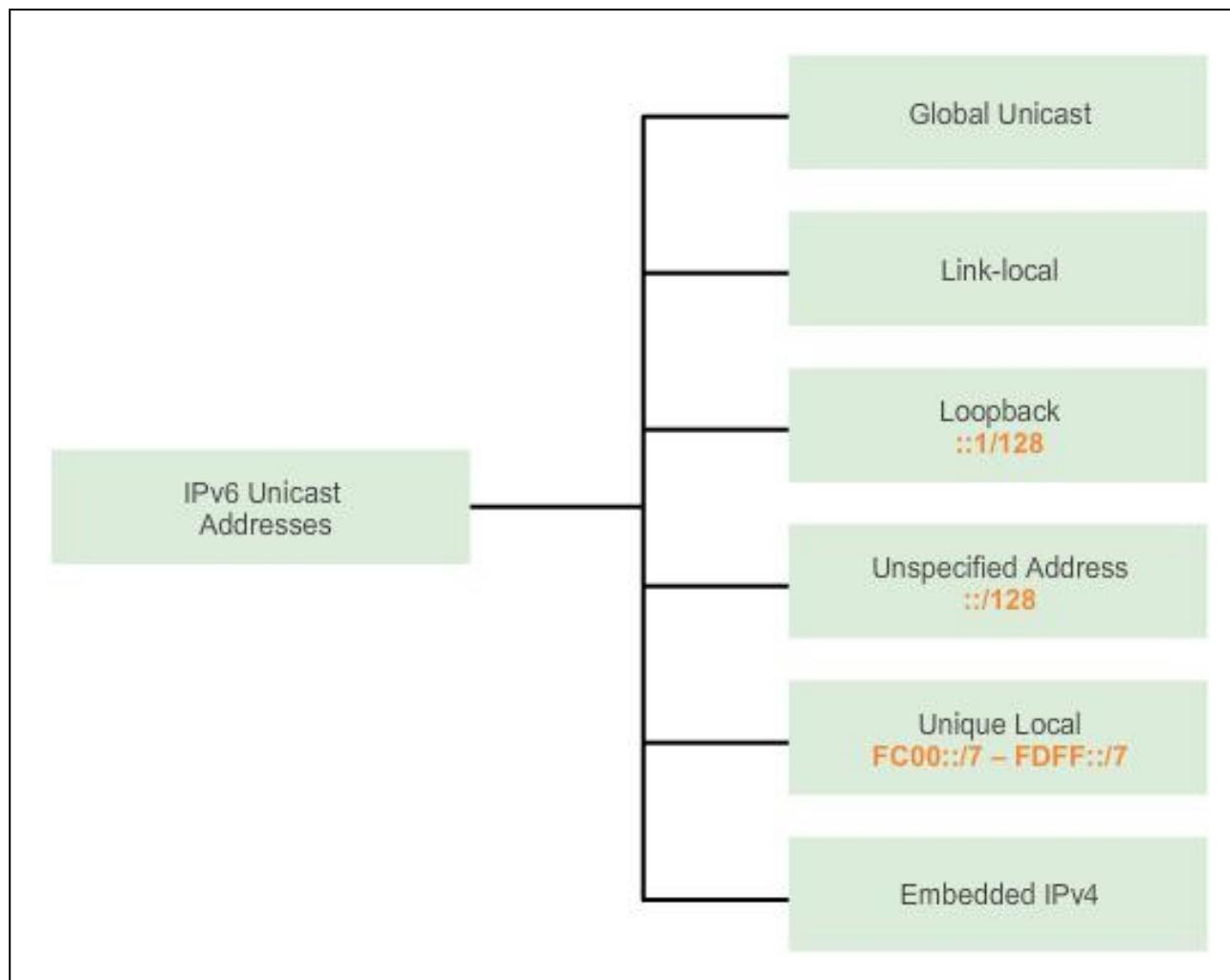
- Uniquely identifies an interface on an IPv6-enabled device.
- A packet sent to a unicast address is received by the interface that is assigned that address.





## Types of IPv6 Addresses

# IPv6 Unicast Addresses (cont.)





## Types of IPv6 Addresses

# IPv6 Unicast Addresses (cont.)

### Global Unicast

- Similar to a public IPv4 address
- Globally unique
- Internet routable addresses
- Can be configured statically or assigned dynamically

### Link-local

- Used to communicate with other devices on the same local link
- Confined to a single link; not routable beyond the link



## Types of IPv6 Addresses

# IPv6 Unicast Addresses (cont.)

### Loopback

- Used by a host to send a packet to itself and cannot be assigned to a physical interface.
- Ping an IPv6 loopback address to test the configuration of TCP/IP on the local host.
- All-0s except for the last bit, represented as ::1/128 or just ::1.

### Unspecified Address

- All-0's address represented as ::/128 or just ::
- Cannot be assigned to an interface and is only used as a source address.
- An unspecified address is used as a source address when the device does not yet have a permanent IPv6 address or when the source of the packet is irrelevant to the destination.



## Types of IPv6 Addresses

# IPv6 Unicast Addresses (cont.)

### Unique Local

- Similar to private addresses for IPv4.
- Used for local addressing within a site or between a limited number of sites.
- In the range of FC00::/7 to FDFF::/7.

### IPv4 Embedded (not covered in this course)

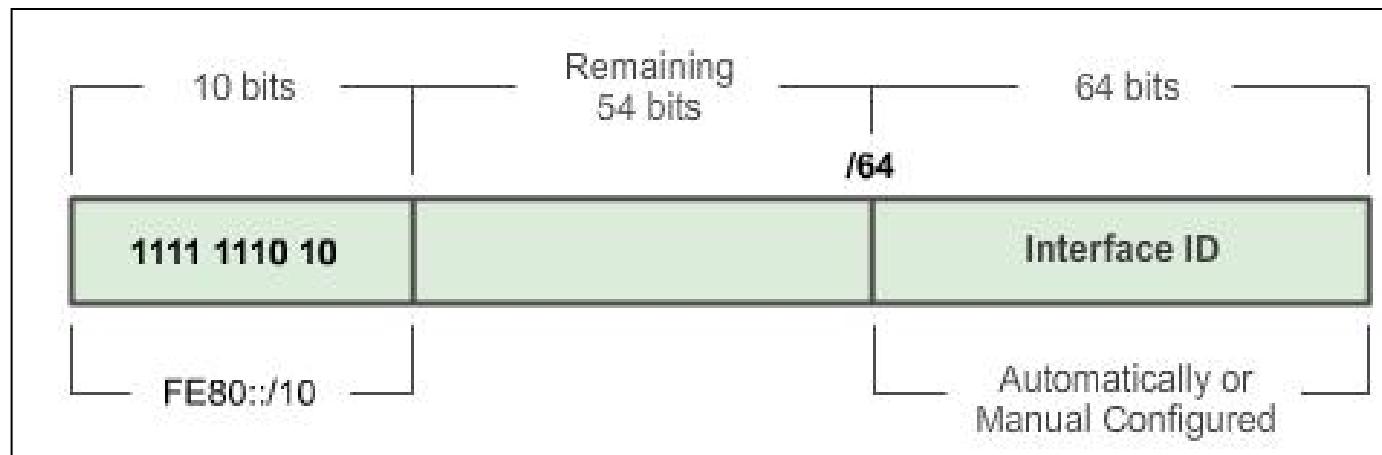
- Used to help transition from IPv4 to IPv6.



## Types of IPv6 Addresses

# IPv6 Link-Local Unicast Addresses

- Every IPv6-enabled network interface is REQUIRED to have a link-local address
- Enables a device to communicate with other IPv6-enabled devices on the same link and only on that link (subnet)
- FE80::/10 range, first 10 bits are 1111 1110 10xx xxxx
- 1111 1110 10**00 0000** (FE80) - 1111 1110 10**11 1111** (FEBF)

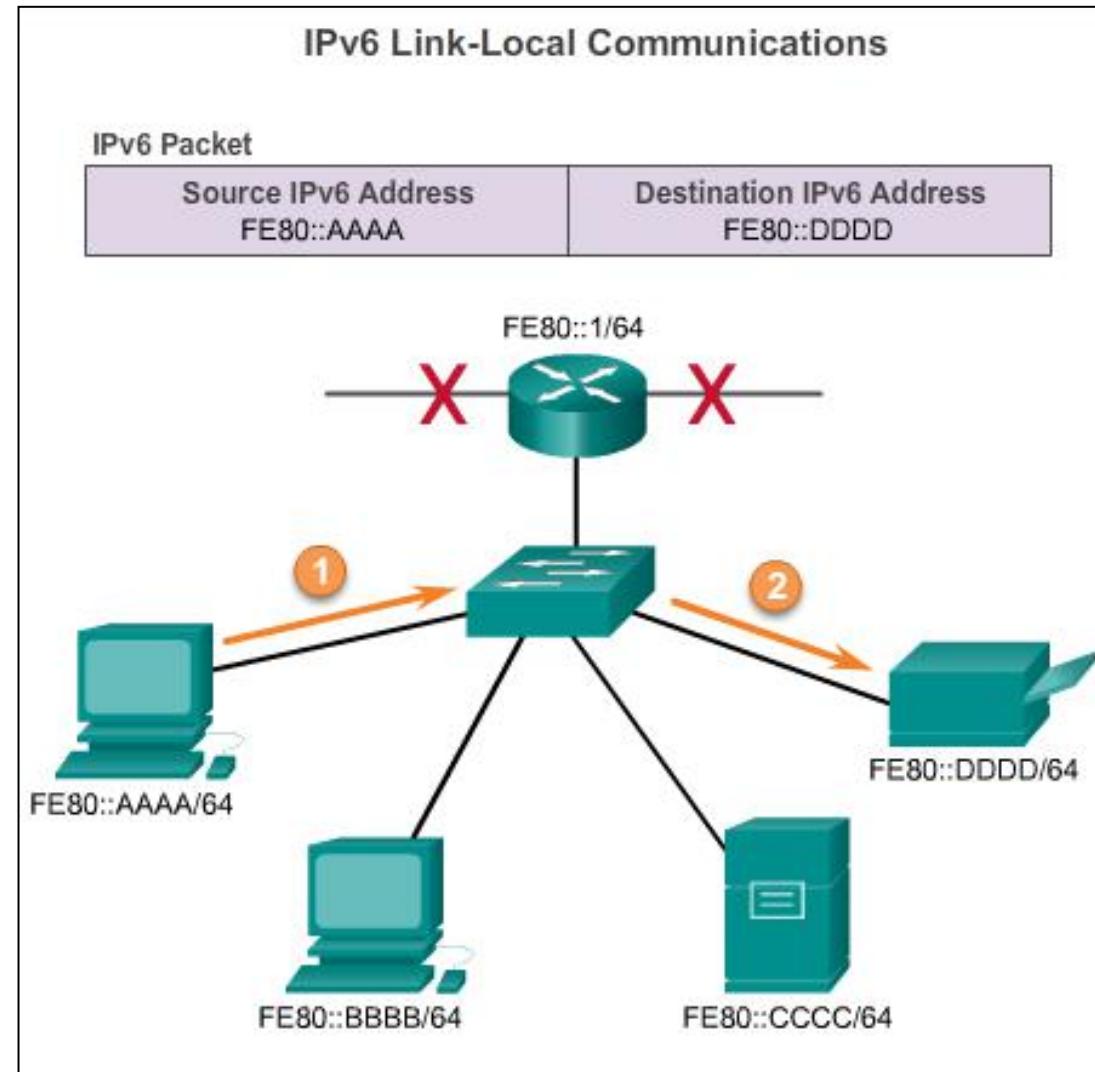




## Types of IPv6 Addresses

# IPv6 Link-Local Unicast Addresses (cont.)

Packets with a source or destination link-local address cannot be routed beyond the link from where the packet originated.





## IPv6 Unicast Addresses

# Structure of an IPv6 Global Unicast Address

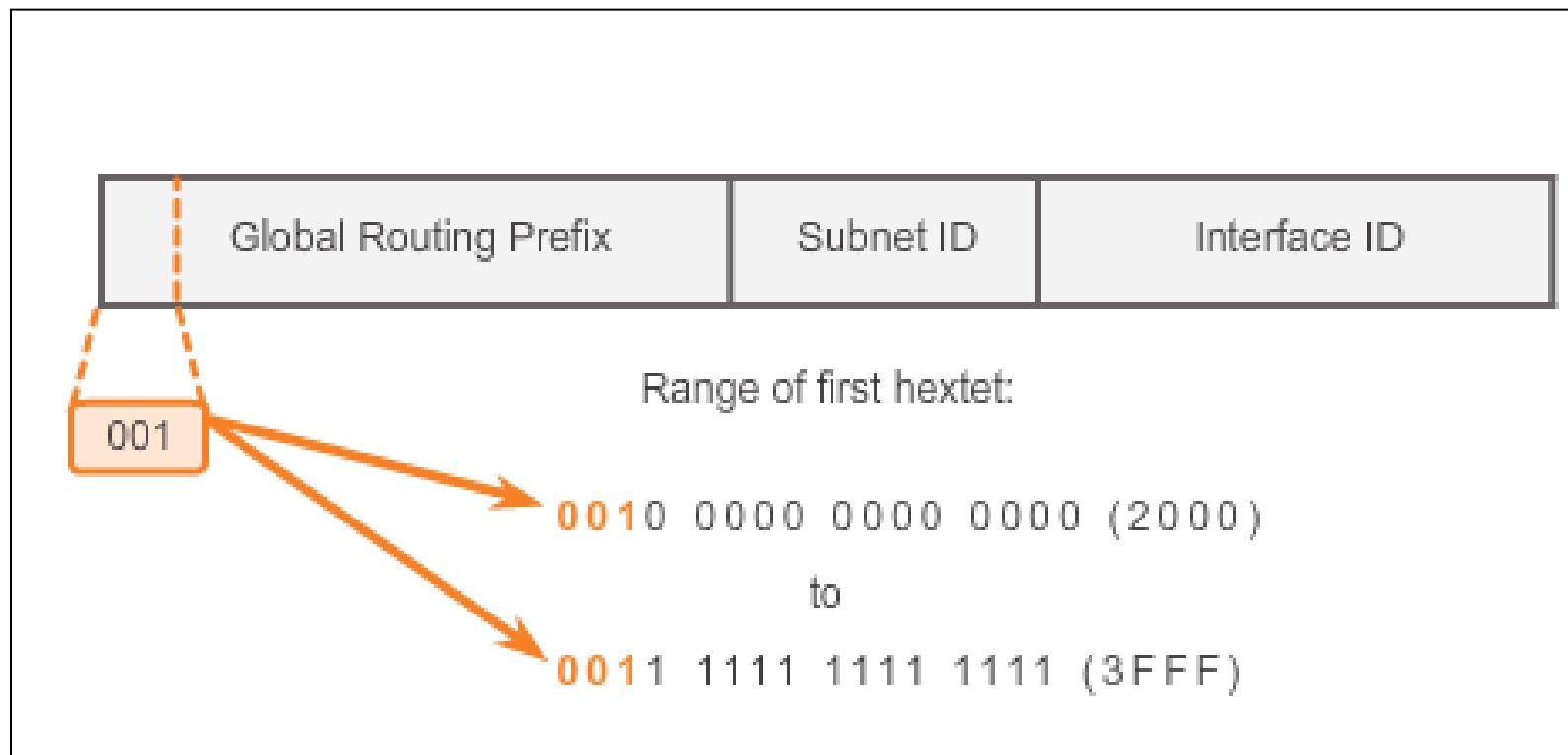
- IPv6 global unicast addresses are globally unique and routable on the IPv6 Internet
- Equivalent to public IPv4 addresses
- ICANN allocates IPv6 address blocks to the five RIRs



## IPv6 Unicast Addresses

### Structure of an IPv6 Global Unicast Address (cont.)

Currently, only global unicast addresses with the first three bits of 001 or 2000::/3 are being assigned



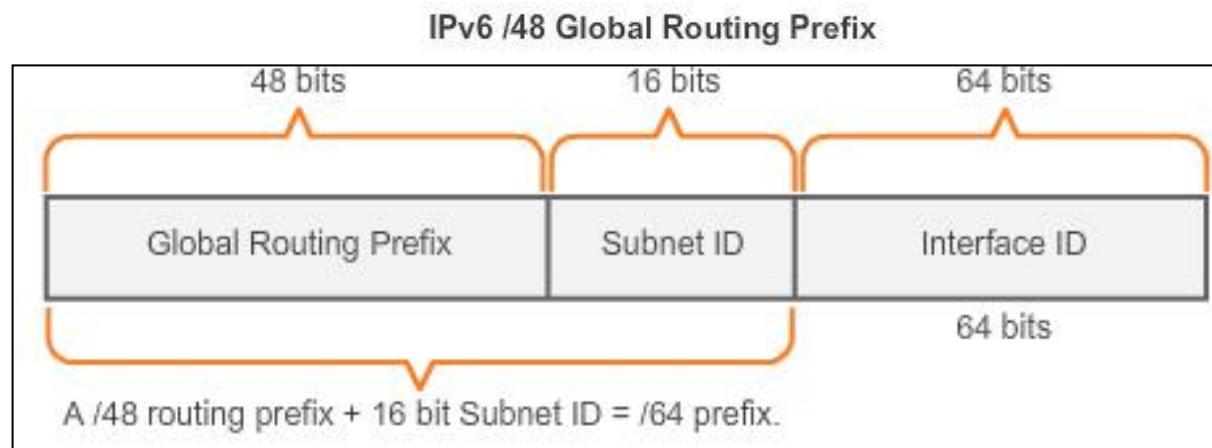


## IPv6 Unicast Addresses

### Structure of an IPv6 Global Unicast Address (cont.)

A global unicast address has three parts: Global Routing Prefix, Subnet ID, and Interface ID.

- **Global Routing Prefix** is the prefix or network portion of the address assigned by the provider, such as an ISP, to a customer or site, currently, RIR's assign a /48 global routing prefix to customers.
- 2001:0DB8:ACAD::/48 has a prefix that indicates that the first 48 bits (2001:0DB8:ACAD) is the prefix or network portion.



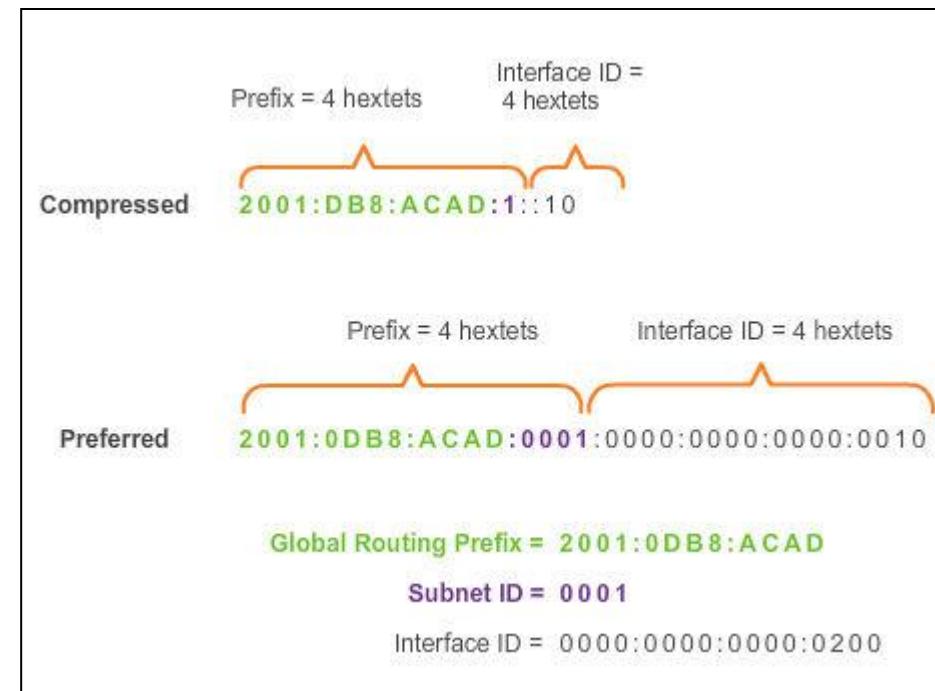


## IPv6 Unicast Addresses

# Structure of an IPv6 Global Unicast Address (cont.)

- **Subnet ID** is used by an organization to identify subnets within its site
- **Interface ID**
  - Equivalent to the host portion of an IPv4 address.
  - Used because a single host may have multiple interfaces, each having one or more IPv6 addresses.

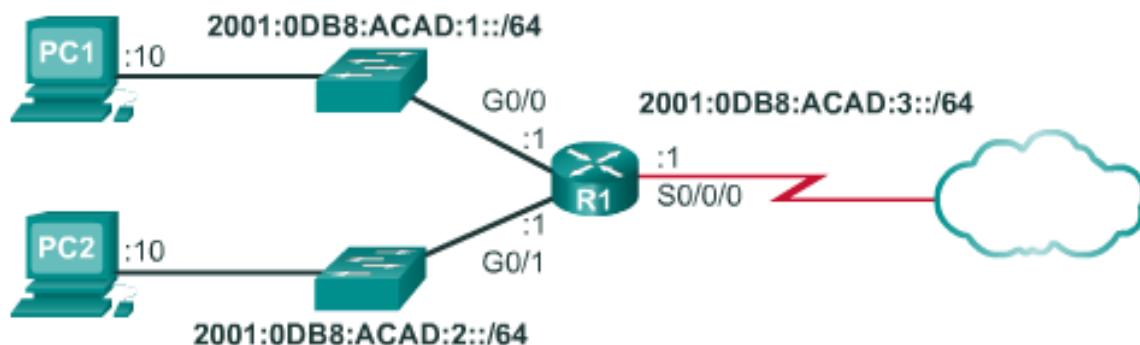
### Reading a Global Unicast Address





# IPv6 Unicast Addresses

## Static Configuration of a Global Unicast Address



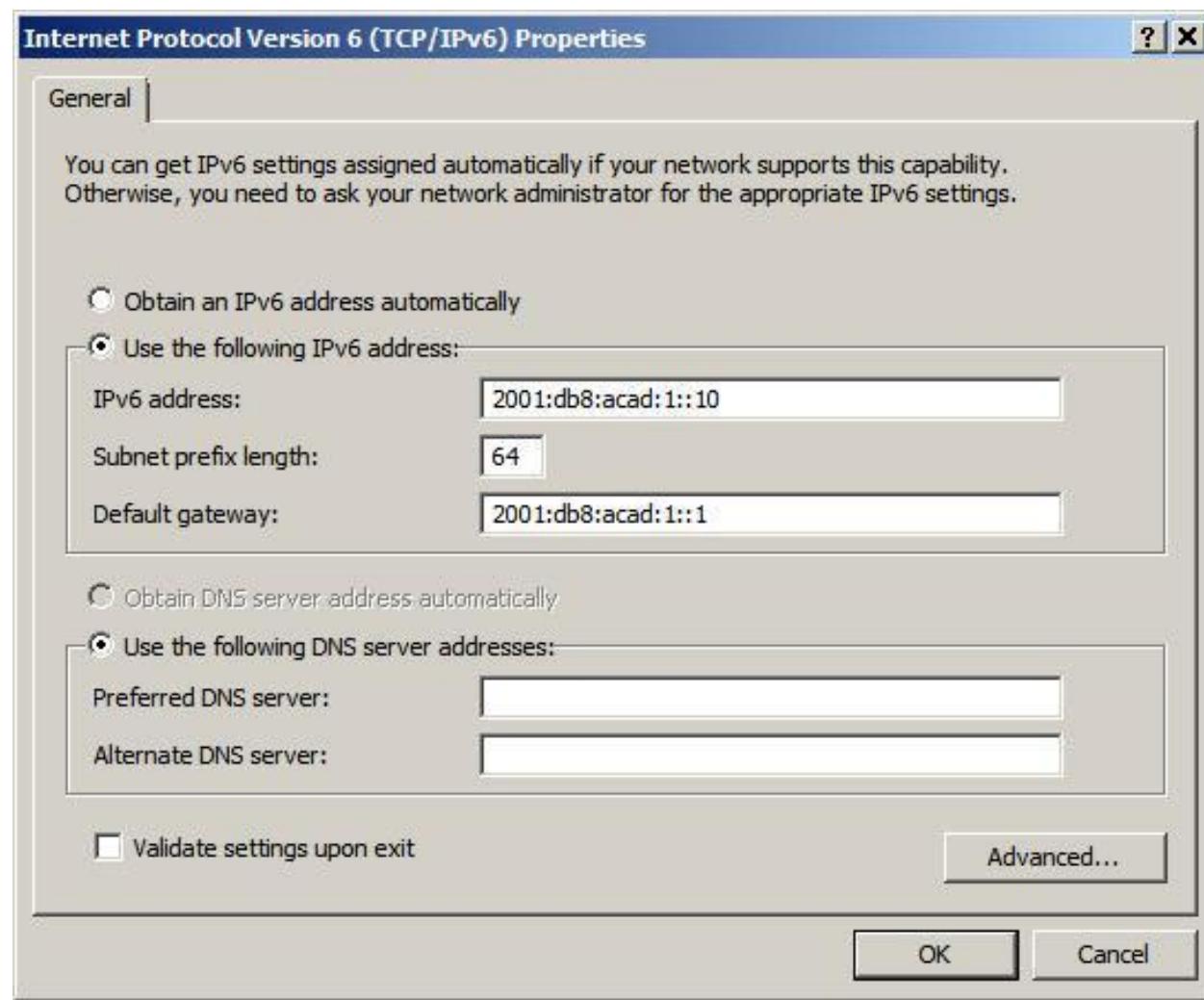
```
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface gigabitethernet 0/1
R1(config-if)#ipv6 address 2001:db8:acad:2::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface serial 0/0/0
R1(config-if)#ipv6 address 2001:db8:acad:3::1/64
R1(config-if)#clock rate 56000
R1(config-if)#no shutdown
```



# IPv6 Unicast Addresses

## Static Configuration of an IPv6 Global Unicast Address (cont.)

### Windows IPv6 Setup





## IPv6 Unicast Addresses

# Dynamic Configuration of a Global Unicast Address using SLAAC

### Stateless Address Autoconfiguration (SLAAC)

- A method that allows a device to obtain its prefix, prefix length and default gateway from an IPv6 router
- No DHCPv6 server needed
- Rely on ICMPv6 Router Advertisement (RA) messages

### IPv6 routers

- Forwards IPv6 packets between networks
- Can be configured with static routes or a dynamic IPv6 routing protocol
- Sends ICMPv6 RA messages



## IPv6 Unicast Addresses

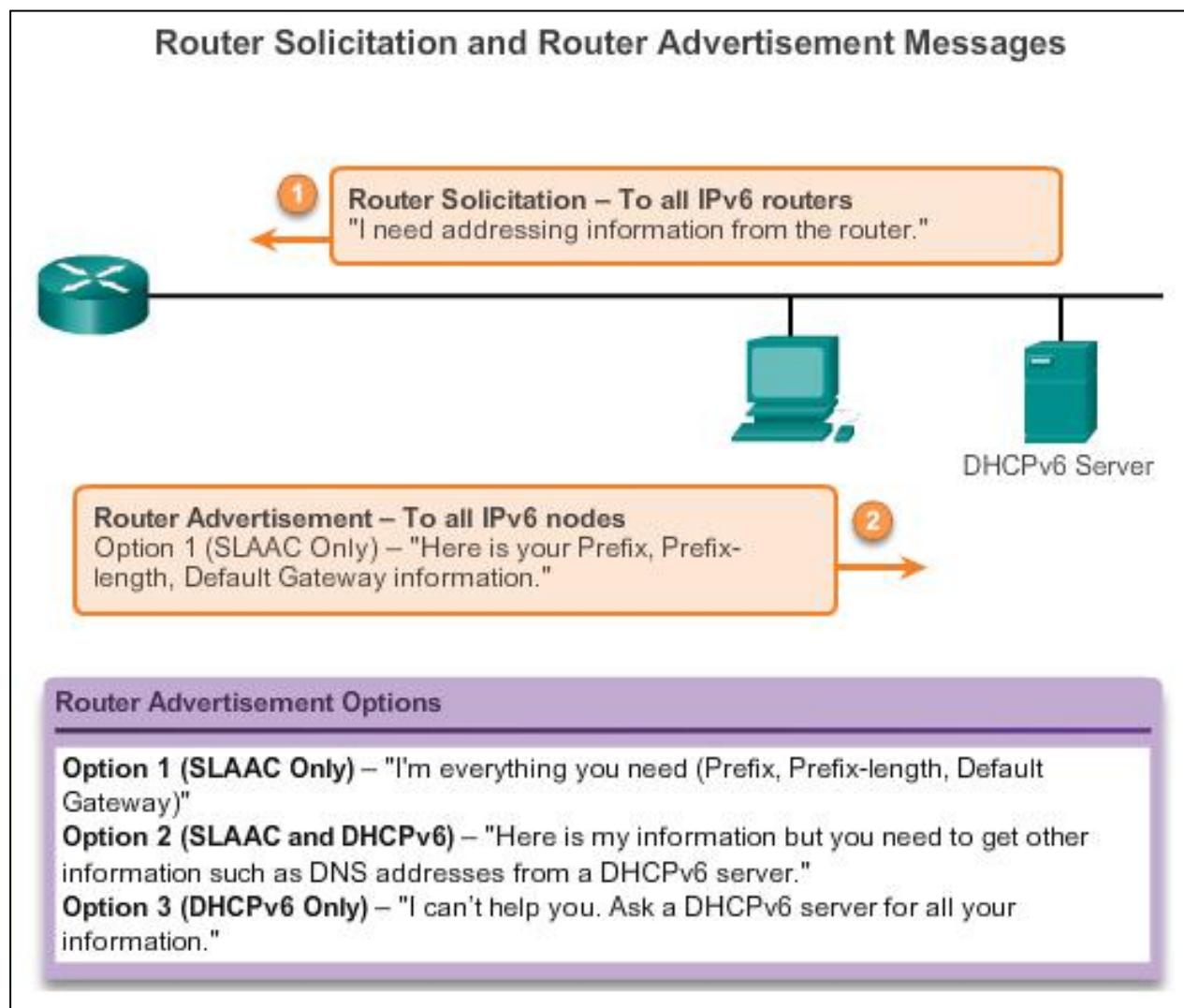
# Dynamic Configuration of a Global Unicast Address using SLAAC (cont.)

- The **IPv6 unicast-routing** command enables IPv6 routing.
- RA message can contain one of the following three options:
  - SLAAC Only – Uses the information contained in the RA message.
  - SLAAC and DHCPv6 – Uses the information contained in the RA message and get other information from the DHCPv6 server, stateless DHCPv6 (for example, DNS).
  - DHCPv6 only – The device should not use the information in the RA, stateful DHCPv6.
- Routers send ICMPv6 RA messages using the link-local address as the source IPv6 address



## IPv6 Unicast Addresses

# Dynamic Configuration of a Global Unicast Address using SLAAC (cont.)





## IPv6 Unicast Addresses

# Dynamic Configuration of a Global Unicast Address using DHCPv6 (cont.)

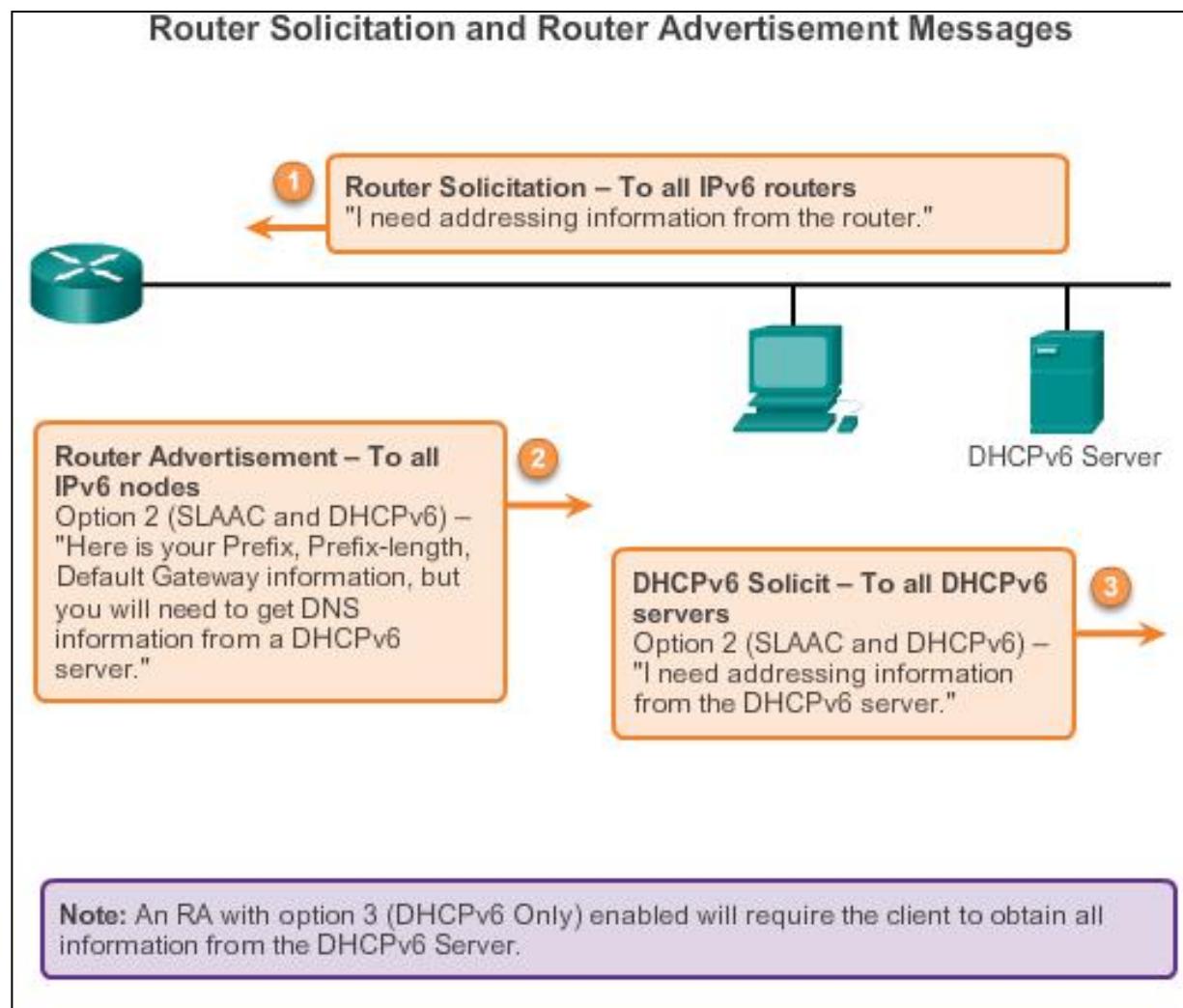
## Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

- Similar to IPv4
- Automatically receives addressing information, including a global unicast address, prefix length, default gateway address and the addresses of DNS servers using the services of a DHCPv6 server.
- Device may receive all or some of its IPv6 addressing information from a DHCPv6 server depending upon whether option 2 (SLAAC and DHCPv6) or option 3 (DHCPv6 only) is specified in the ICMPv6 RA message.
- Host may choose to ignore whatever is in the router's RA message and obtain its IPv6 address and other information directly from a DHCPv6 server.



## IPv6 Unicast Addresses

# Dynamic Configuration of a Global Unicast Address using DHCPv6 (cont.)





## IPv6 Unicast Addresses

# EUI-64 Process or Randomly Generated

### EUI-64 Process

- Uses a client's 48-bit Ethernet MAC address and inserts another 16 bits in the middle of the 46-bit MAC address to create a 64-bit Interface ID.
- Advantage is that the Ethernet MAC address can be used to determine the interface; is easily tracked.

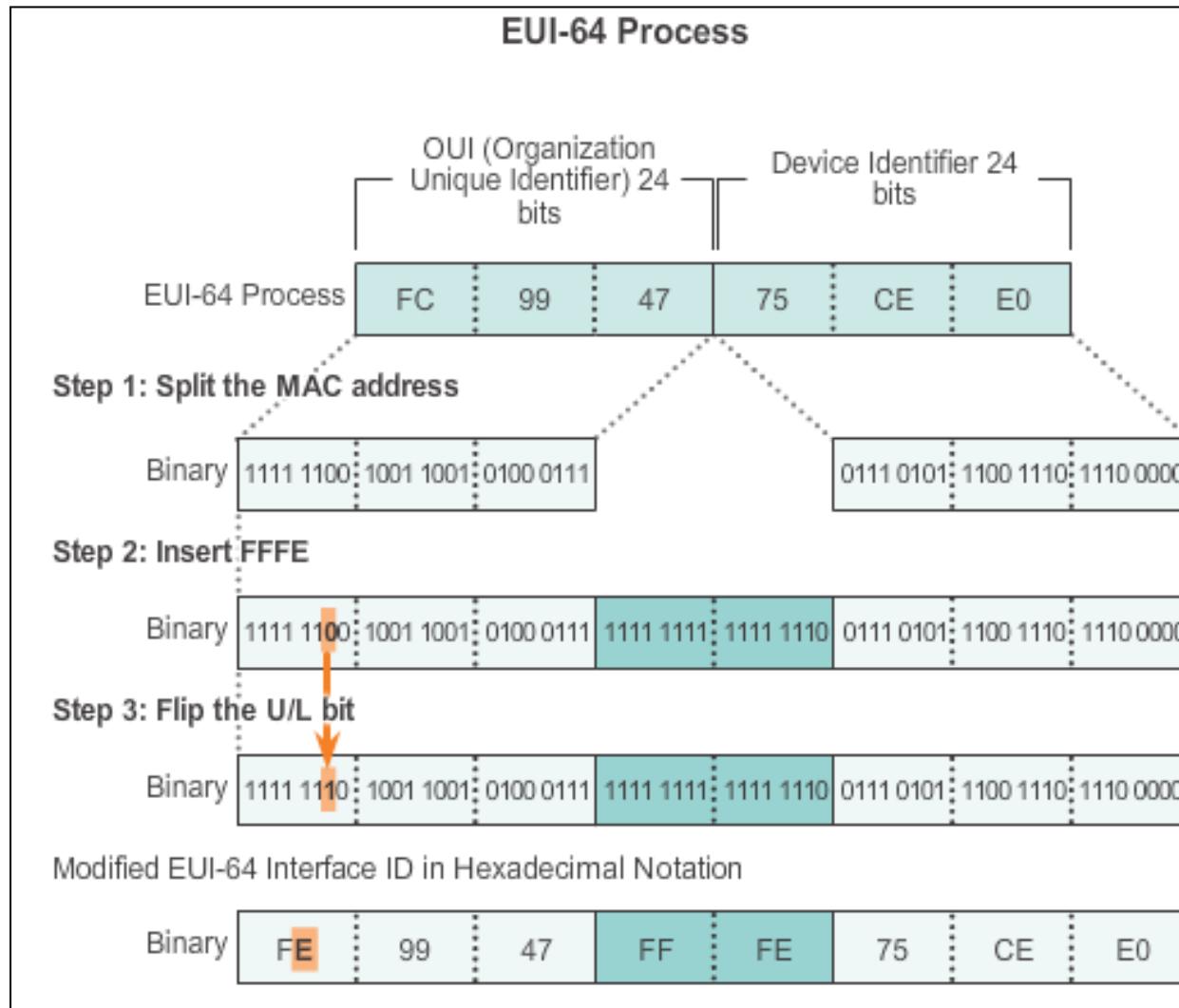
**EUI-64 Interface ID** is represented in binary and comprises three parts:

- 24-bit OUI from the client MAC address, but the 7<sup>th</sup> bit (the Universally/Locally bit) is reversed (0 becomes a 1).
- Inserted as a 16-bit value FFFE.
- 24-bit device identifier from the client MAC address.



## IPv6 Unicast Addresses

## EUI-64 Process or Randomly Generated (cont.)





## IPv6 Unicast Addresses

## EUI-64 Process or Randomly Generated (cont.)

```
R1#show interface gigabitethernet 0/0
GigabitEthernet0/0 is up, line protocol is up
    Hardware is CN Gigabit Ethernet, address is fc99.4775.c3e0
(bia fc99.4775.c3e0)
<Output Omitted>
```

```
R1#show ipv6 interface brief
GigabitEthernet0/0      [up/up]
  FE80::FE99:47FF:FE75:C3E0
  2001:DB8:ACAD:1::1
GigabitEthernet0/1      [up/up]
  FE80::FE99:47FF:FE75:C3E1
  2001:DB8:ACAD:2::1
Serial0/0/0             [up/up]
  FE80::FE99:47FF:FE75:C3E0
  2001:DB8:ACAD:3::1
Serial0/0/1             [administratively down/down]
  unassigned
R1#
```

Link-local addresses using  
EUI-64



## IPv6 Unicast Addresses

# EUI-64 Process or Randomly Generated (cont.)

### **Randomly Generated Interface IDs**

- Depending upon the operating system, a device can use a randomly generated Interface ID instead of using the MAC address and the EUI-64 process.
- Beginning with Windows Vista, Windows uses a randomly generated Interface ID instead of one created with EUI-64.
- Windows XP (and previous Windows operating systems) used EUI-64.



## IPv6 Unicast Addresses

# Dynamic Link-local Addresses

### Link-Local Address

- After a global unicast address is assigned to an interface, an IPv6-enabled device automatically generates its link-local address.
- Must have a link-local address that enables a device to communicate with other IPv6-enabled devices on the same subnet.
- Uses the link-local address of the local router for its default gateway IPv6 address.
- Routers exchange dynamic routing protocol messages using link-local addresses.
- Routers' routing tables use the link-local address to identify the next-hop router when forwarding IPv6 packets.

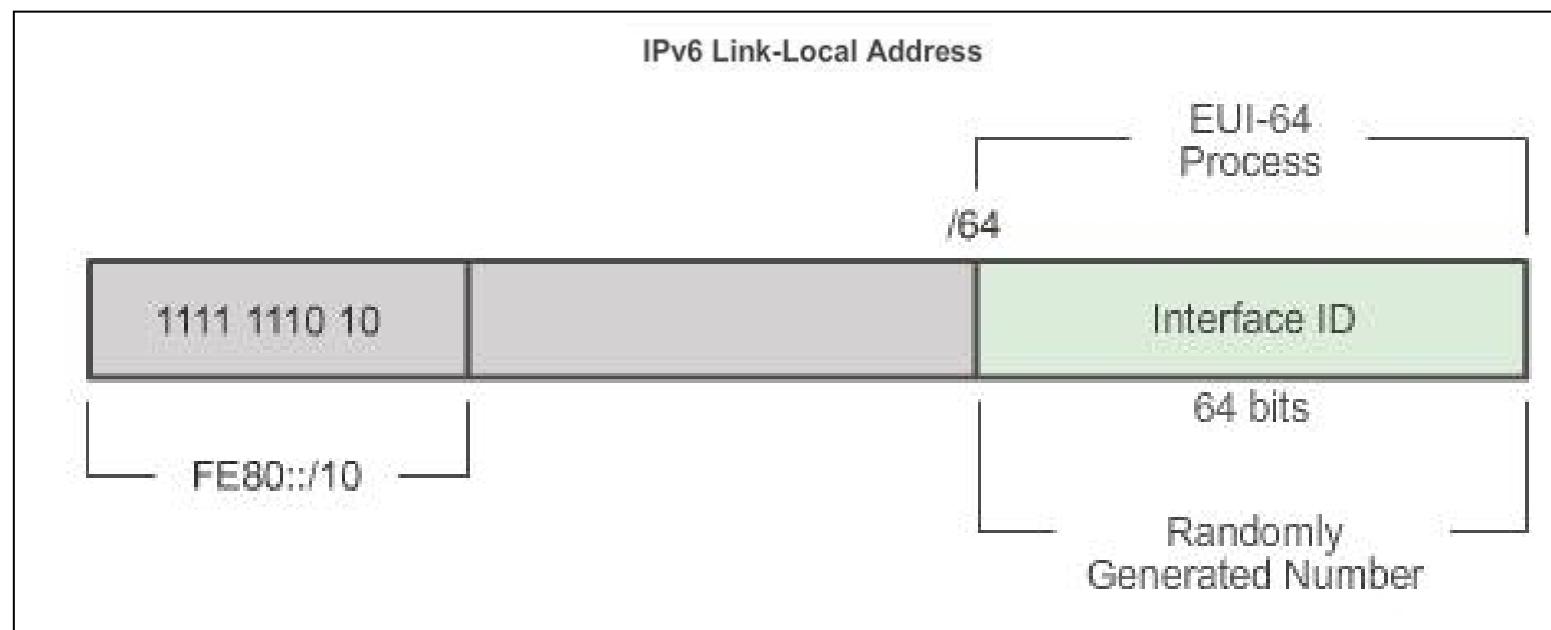


## IPv6 Unicast Addresses

# Dynamic Link-local Addresses (cont.)

### Dynamically Assigned

The link-local address is dynamically created using the FE80::/10 prefix and the Interface ID.





## IPv6 Unicast Addresses

## Static Link-local Addresses

## Configuring Link-local

```
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ipv6 address fe80::1 ?
    link-local  Use link-local address

R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#exit
R1(config)#interface gigabitethernet 0/1
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#exit
R1(config)#interface serial 0/0/0
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#

```



## IPv6 Unicast Addresses

## Static Link-local Addresses (cont.)

## Configuring Link-local

```
R1#show ipv6 interface brief
GigabitEthernet0/0      [up/up]
  FE80::1
  2001:DB8:ACAD:1::1
GigabitEthernet0/1      [up/up]
  FE80::1
  2001:DB8:ACAD:2::1
Serial0/0/0             [up/up]
  FE80::1
  2001:DB8:ACAD:3::1
Serial0/0/1             [administratively down/down]
  unassigned
R1#
```

Statically configured link-local addresses

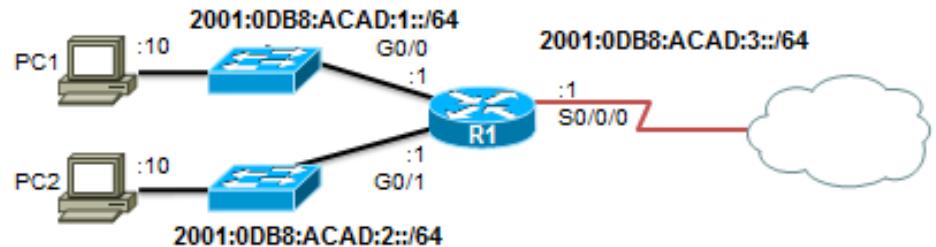


## IPv6 Global Unicast Addresses

# Verifying IPv6 Address Configuration

Each interface has two IPv6 addresses -

1. global unicast address that was configured
2. one that begins with FE80 is automatically added as a link-local unicast address



```
R1#show ipv6 interface brief
GigabitEthernet0/0      [up/up]
  FE80::FE99:47FF:FE75:C3E0
  2001:DB8:ACAD:1::1
GigabitEthernet0/1      [up/up]
  FE80::FE99:47FF:FE75:C3E1
  2001:DB8:ACAD:2::1
Serial0/0/0             [up/up]
  FE80::FE99:47FF:FE75:C3E0
  2001:DB8:ACAD:3::1
Serial0/0/1             [administratively down/down]
  unassigned
R1#
```



## IPv6 Global Unicast Addresses

## Verifying IPv6 Address Configuration (cont.)

```
R1#show ipv6 route
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user
Static

<output omitted>

C 2001:DB8:ACAD:1::/64 [0/0]
    via GigabitEthernet0/0, directly connected
L 2001:DB8:ACAD:1::1/128 [0/0]
    via GigabitEthernet0/0, receive
C 2001:DB8:ACAD:2::/64 [0/0]
    via GigabitEthernet0/1, directly connected
L 2001:DB8:ACAD:2::1/128 [0/0]
    via GigabitEthernet0/1, receive
C 2001:DB8:ACAD:3::/64 [0/0]
    via Serial0/0/0, directly connected
L 2001:DB8:ACAD:3::1/128 [0/0]
    via Serial0/0/0, receive
L FF00::/8 [0/0]
    via Null0, receive
R1#
```



## IPv6 Multicast Addresses

# Assigned IPv6 Multicast Addresses

- IPv6 multicast addresses have the prefix FF00::/8
- There are two types of IPv6 multicast addresses:
  - Assigned multicast
  - Solicited node multicast



## IPv6 Multicast Addresses

# Assigned IPv6 Multicast Addresses (cont.)

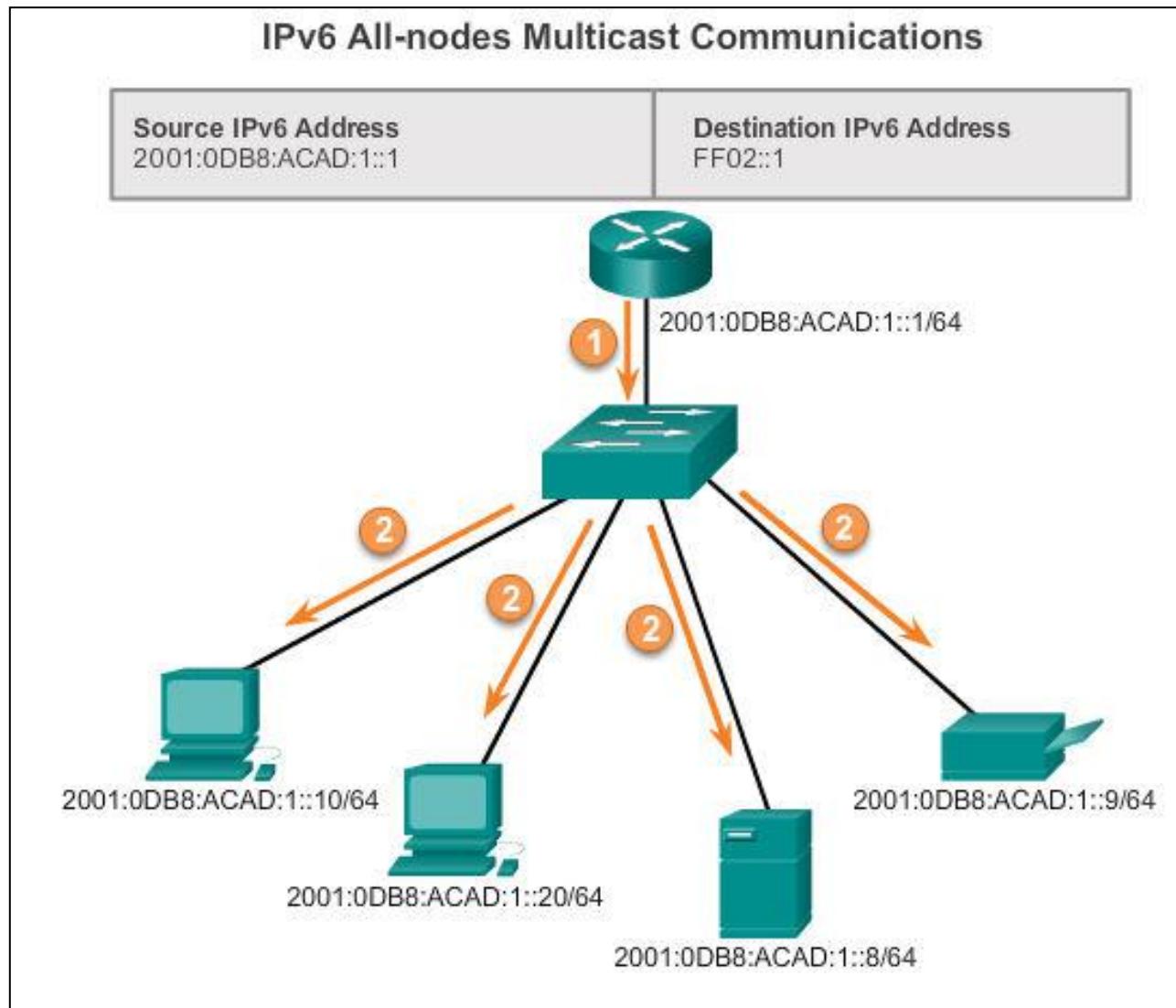
Two common IPv6 assigned multicast groups include:

- **FF02::1 All-nodes multicast group –**
  - All IPv6-enabled devices join
  - Same effect as an IPv4 broadcast address
- **FF02::2 All-routers multicast group**
  - All IPv6 routers join
  - A router becomes a member of this group when it is enabled as an IPv6 router with the `ipv6 unicast-routing` global configuration mode command.
  - A packet sent to this group is received and processed by all IPv6 routers on the link or network.



## IPv6 Multicast Addresses

## Assigned IPv6 Multicast Addresses (cont.)

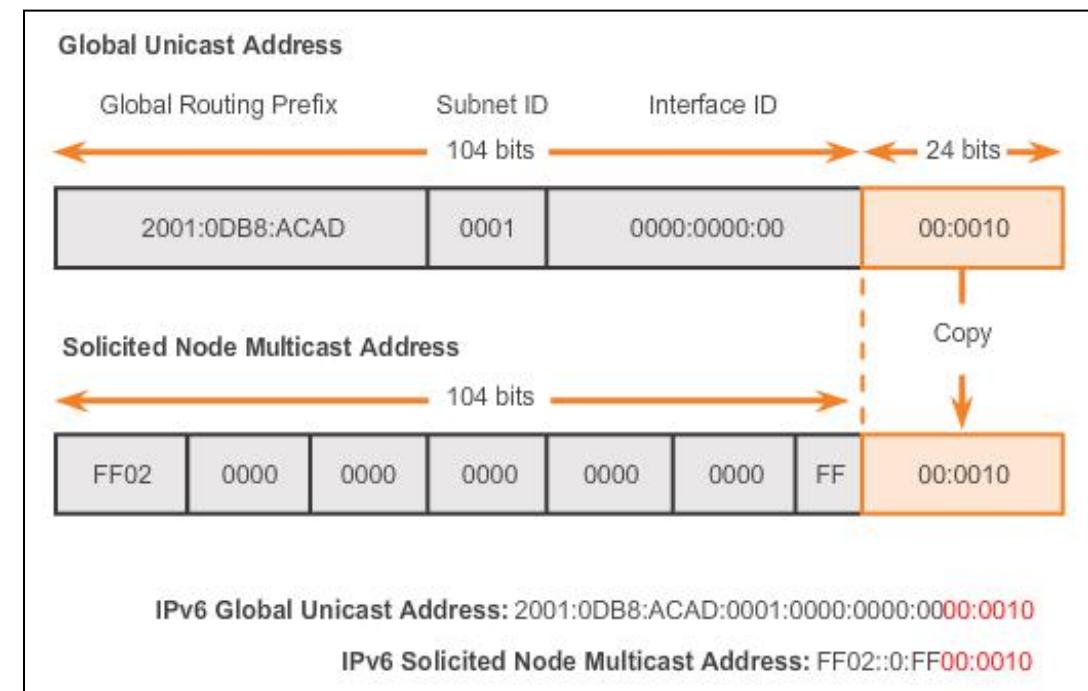




## IPv6 Multicast Addresses

# Solicited Node IPv6 Multicast Addresses

- Similar to the all-nodes multicast address, matches only the last 24 bits of the IPv6 global unicast address of a device
- Automatically created when the global unicast or link-local unicast addresses are assigned
- Created by combining a special FF02:0:0:0:0:FF00::/104 prefix with the right-most 24 bits of its unicast address



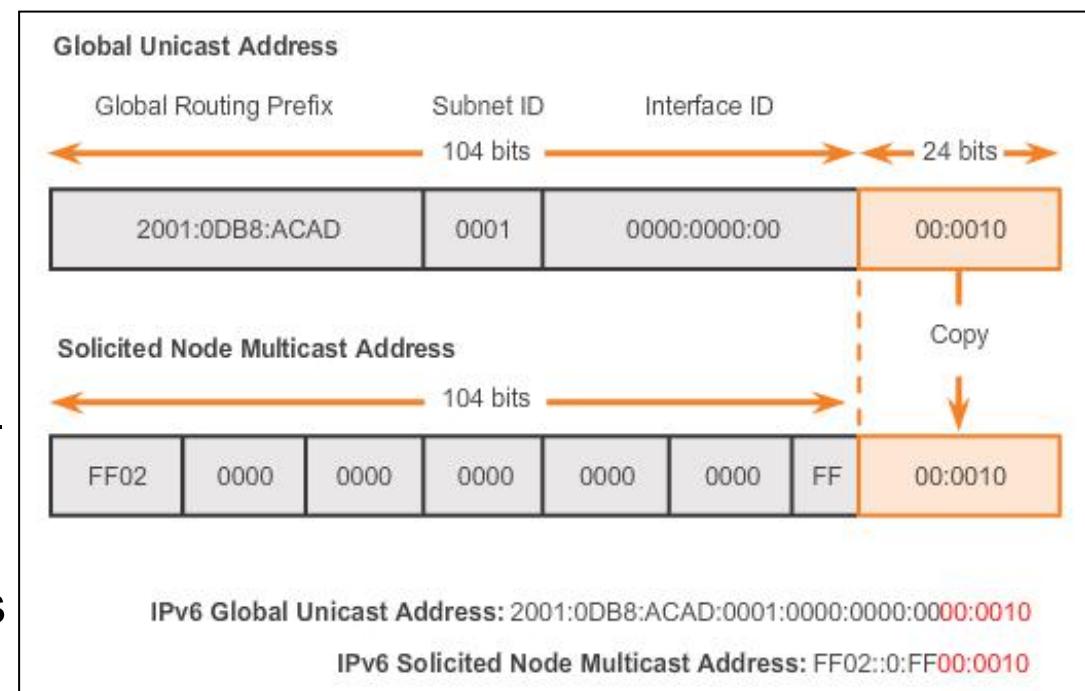


## IPv6 Multicast Addresses

# Solicited Node IPv6 Multicast Addresses (cont.)

The solicited node multicast address consists of two parts:

- **FF02:0:0:0:0:FF00::/104 multicast prefix** – First 104 bits of the all solicited node multicast address
- **Least significant 24-bits** – Copied from the right-most 24 bits of the global unicast or link-local unicast address of the device



## 8.3 Connectivity Verification





## ICMP

# ICMPv4 and ICMPv6 Messages

- ICMP messages common to both ICMPv4 and ICMPv6 include:
  - Host confirmation
  - Destination or Service Unreachable
  - Time exceeded
  - Route redirection
- Although IP is not a reliable protocol, the TCP/IP suite does provide for messages to be sent in the event of certain errors, sent using the services of ICMP.



## ICMP

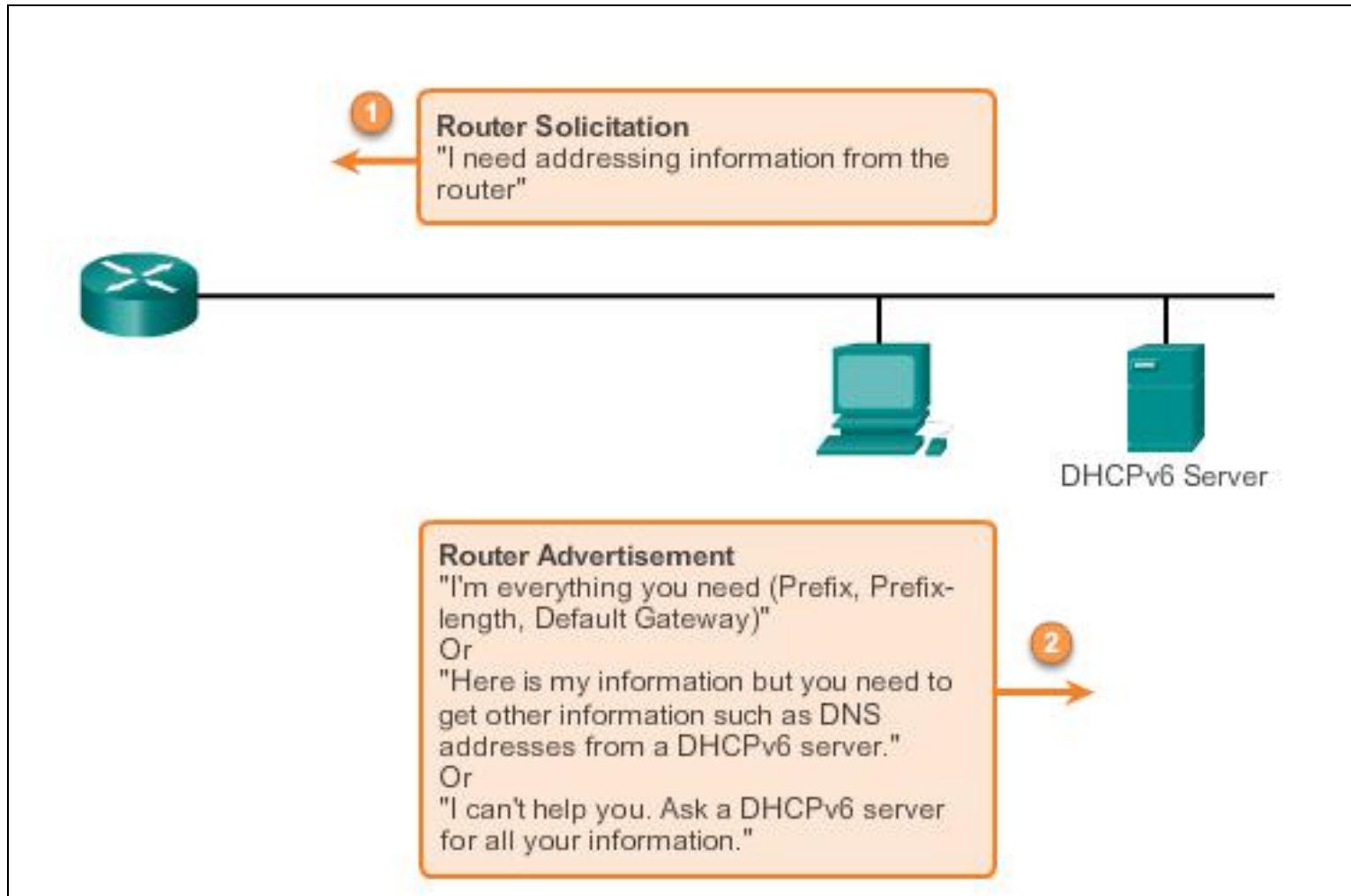
# ICMPv6 Router Solicitation and Router Advertisement Messages

- ICMPv6 includes four new protocols as part of the Neighbor Discovery Protocol (ND or NDP):
  - Router Solicitation message
  - Router Advertisement message
  - Neighbor Solicitation message
  - Neighbor Advertisement message
- **Router Solicitation and Router Advertisement Message** – Sent between hosts and routers.
- **Router Solicitation (RS) message** – RS messages are sent as an IPv6 all-routers multicast message.
- **Router Advertisement (RA) message** – RA messages are sent by routers to provide addressing information.



## ICMP

# ICMPv6 Router Solicitation and Router Advertisement Messages (cont.)





## ICMP

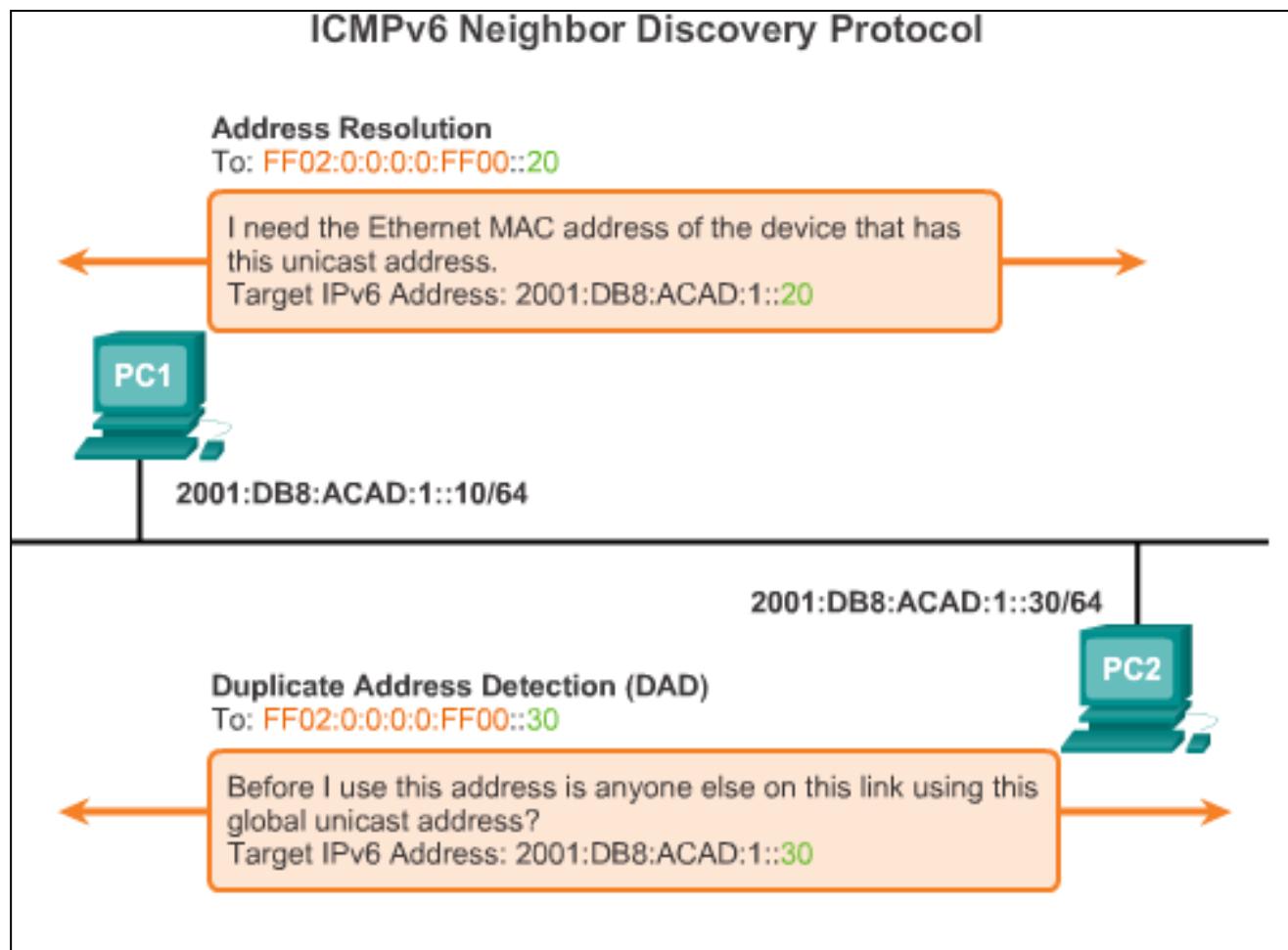
# ICMPv6 Neighbor Solicitation and Neighbor Advertisement Messages

- Two additional message types:
  - Neighbor Solicitation (NS)
  - Neighbor Advertisement (NA) messages
- **Used for address resolution** is used when a device on the LAN knows the IPv6 unicast address of a destination, but does not know its Ethernet MAC address.
- **Also used for Duplicate Address Detection (DAD)**
  - Performed on the address to ensure that it is unique.
  - The device sends an NS message with its own IPv6 address as the targeted IPv6 address.



## ICMP

# ICMPv6 Neighbor Solicitation and Neighbor Advertisement Messages (cont.)





## Testing and Verification

# Ping – Testing the Local Stack

**Testing Local TCP/IP Stack**

Pinging the local host confirms that TCP/IP is installed and working on the local host.

C:\>ping 127.0.0.1

Pinging 127.0.0.1 causes a device to ping itself.

**Local Area Connection Properties**

Networking | Authentication | Sharing |

Connect using:  
Intel(R) 82579LM Gigabit Network Connection

Configure...

This connection uses the following items:

- Client for Microsoft Networks
- Deterministic Network Enhancer
- QoS Packet Scheduler
- File and Printer Sharing for Microsoft Networks
- Internet Protocol Version 6 (TCP/IPv6)
- Internet Protocol Version 4 (TCP/IPv4)
- Link-Layer Topology Discovery Mapper I/O Driver
- Link-Layer Topology Discovery Responder

Install... Uninstall Properties

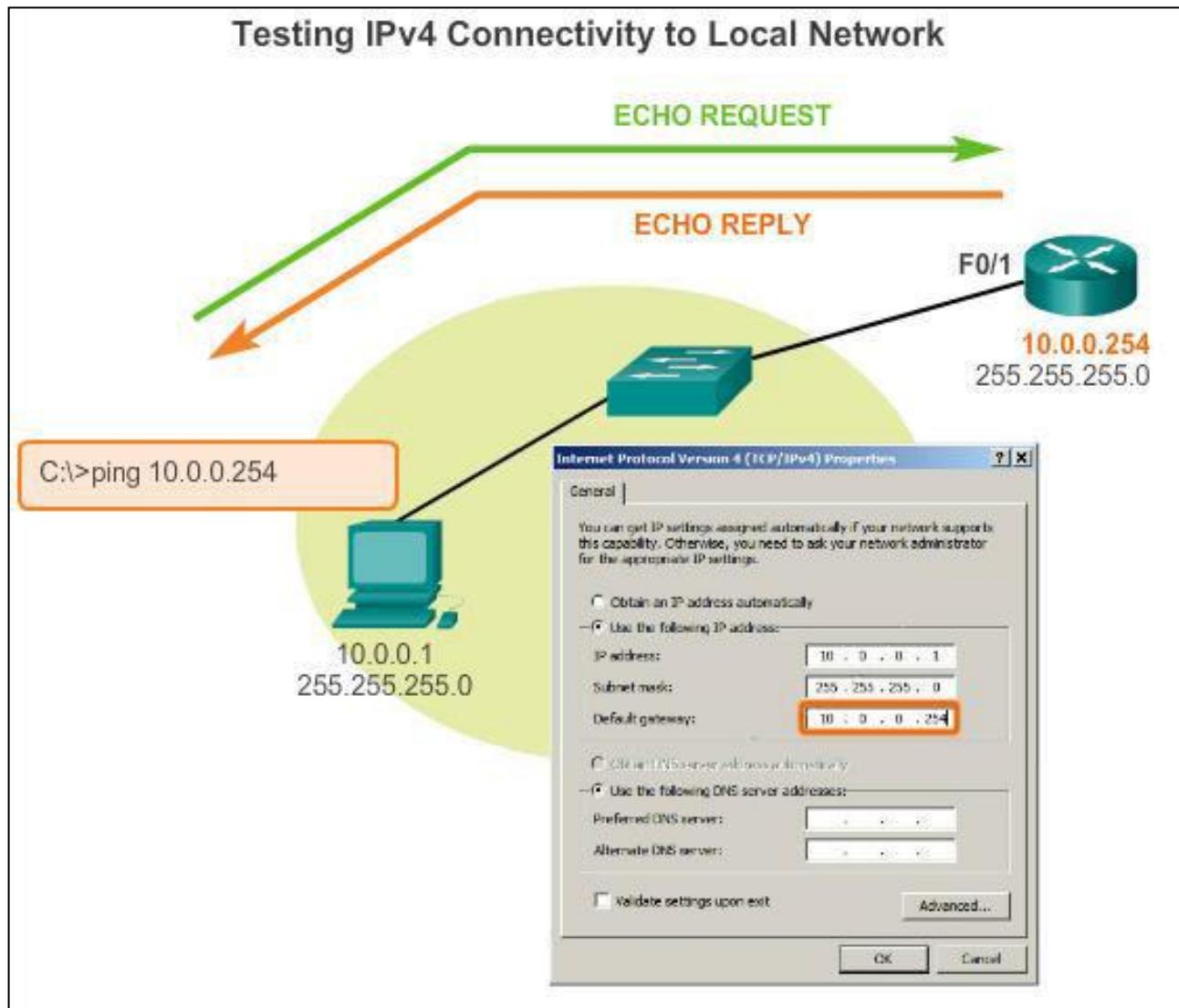
Description  
Allows your computer to access resources on a Microsoft network.

OK Cancel



## Testing and Verification

# Ping – Testing Connectivity to the Local LAN

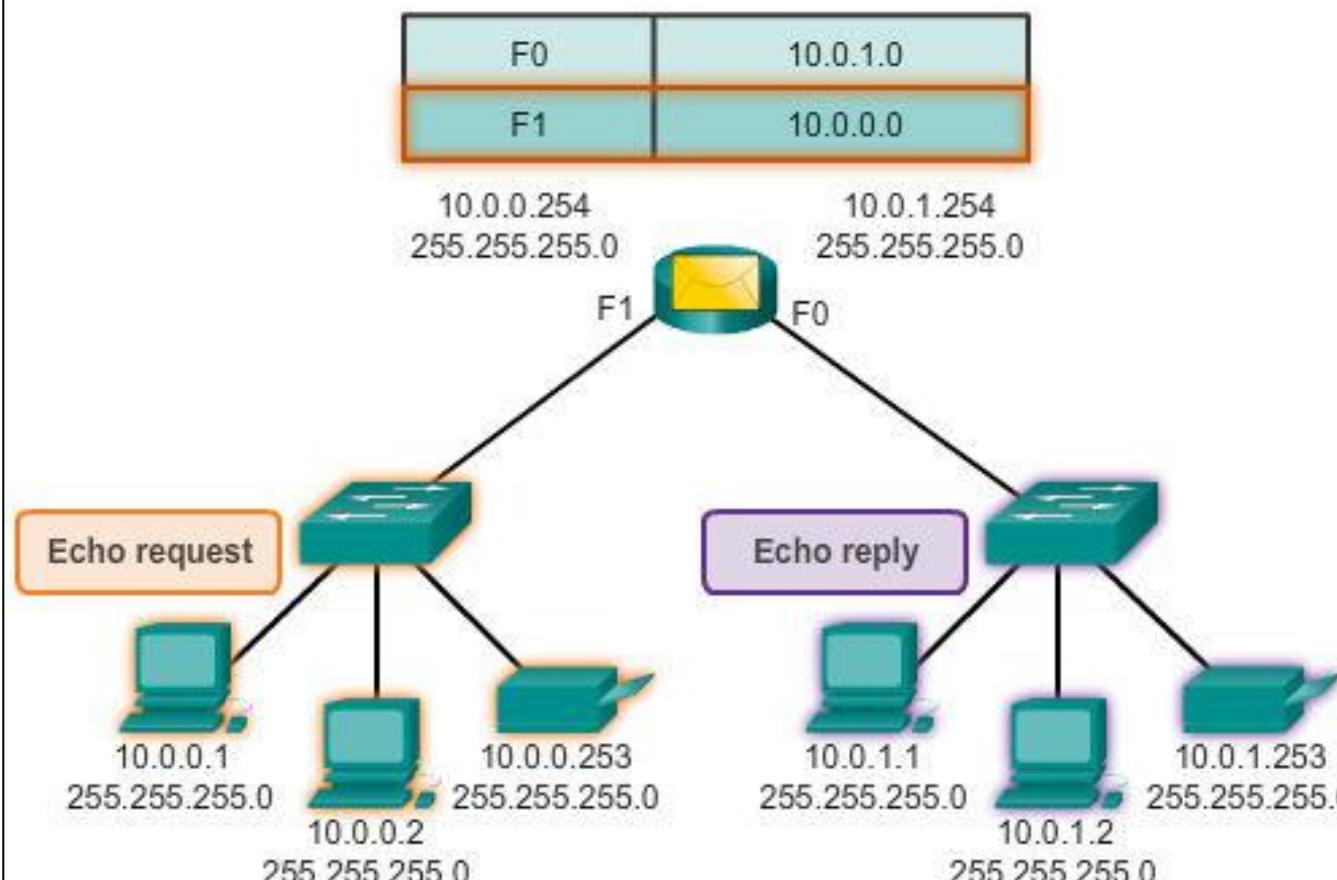




## Testing and Verification

# Ping – Testing Connectivity to Remote

Testing Connectivity to Remote LAN  
Ping to a Remote Host





## Testing and Verification

# Traceroute – Testing the Path

### Traceroute

- Generates a list of hops that were successfully reached along the path.
- Provides important verification and troubleshooting information.
- If the data reaches the destination, then the trace lists the interface of every router in the path between the hosts.
- If the data fails at some hop along the way, the address of the last router that responded to the trace can provide an indication of where the problem or security restrictions are found.
- Provides round-trip time for each hop along the path and indicates if a hop fails to respond.



# IP Addressing Summary

- IP addresses are hierarchical with network, subnetwork, and host portions.
- An IP address can represent a complete network, a specific host, or the broadcast address of the network.
- The subnet mask or prefix is used to determine the network portion of an IP address. Once implemented, an IP network needs to be tested to verify its connectivity and operational performance.
- DHCP enables the automatic assignment of addressing information such as IP address, subnet mask, default gateway, and other configuration information.



# IP Addressing Summary (cont.)

- IPv4 hosts can communicate one of three different ways: unicast, broadcast, and multicast.
- The private IPv4 address blocks are: 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16.
- The depletion of IPv4 address space is the motivating factor for moving to IPv6.
- Each IPv6 address has 128 bits versus the 32 bits in an IPv4 address.
- The prefix length is used to indicate the network portion of an IPv6 address using the following format: IPv6 address/prefix length.



# IP Addressing Summary (cont.)

- There are three types of IPv6 addresses: unicast, multicast, and anycast.
- An IPv6 link-local address enables a device to communicate with other IPv6-enabled devices on the same link and only on that link (subnet).
- Packets with a source or destination link-local address cannot be routed beyond the link from where the packet originated.
- IPv6 link-local addresses are in the FE80::/10 range.
- ICMP is available for both IPv4 and IPv6.

# Cisco | Networking Academy®

Mind Wide Open™



## Chapter 9: Subnetting IP Networks



## Introduction to Networks

Cisco | Networking Academy®  
Mind Wide Open™



# Chapter 9

- 9.0 Introduction
- 9.1 Subnetting an IPv4 Network
- 9.2 Addressing Schemes
- 9.3 Design Considerations for IPv6
- 9.4 Summary



# Chapter 9: Objectives

Upon completion of this chapter, you will be able to:

- Explain why routing is necessary for hosts on different networks to communicate.
- Describe IP as a communication protocol used to identify a single device on a network.
- Given a network and a subnet mask, calculate the number of host addresses available.
- Calculate the necessary subnet mask in order to accommodate the requirements of a network.
- Describe the benefits of variable length subnet masking (VLSM).
- Explain how IPv6 address assignments are implemented in a business network.



## 9.1 Subnetting an IPv4 Network



Cisco | Networking Academy®  
Mind Wide Open™



# Network Segmentation

## Reasons for Subnetting

**Subnetting** is the process of segmenting a network into multiple smaller network spaces called subnetworks or subnets.

- Large networks must be segmented into smaller subnetworks, creating smaller groups of devices and services to:
  - Control traffic by containing broadcast traffic within each subnetwork.
  - Reduce overall network traffic and improve network performance.

### Communication Between Subnets

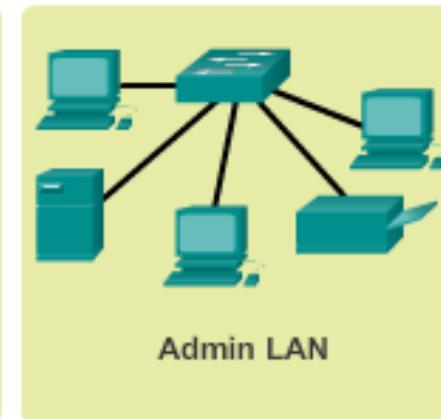
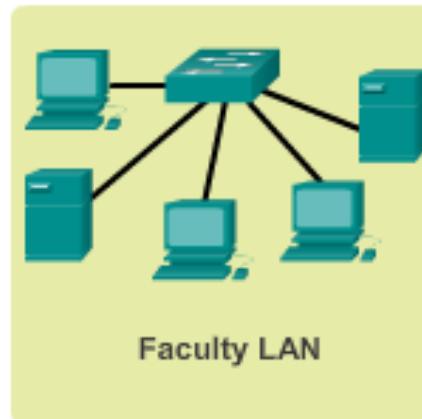
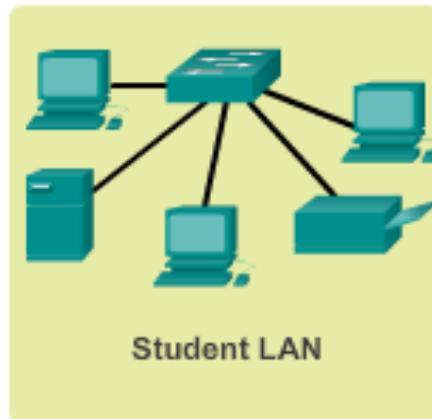
- A router is necessary for devices on different networks and subnets to communicate.
- Each router interface must have an IPv4 host address that belongs to the network or subnet that the router interface is connected.
- Devices on a network and subnet use the router interface attached to their LAN as their default gateway.



# IP Subnetting is FUNdamental

## The Plan

### Planning the Network



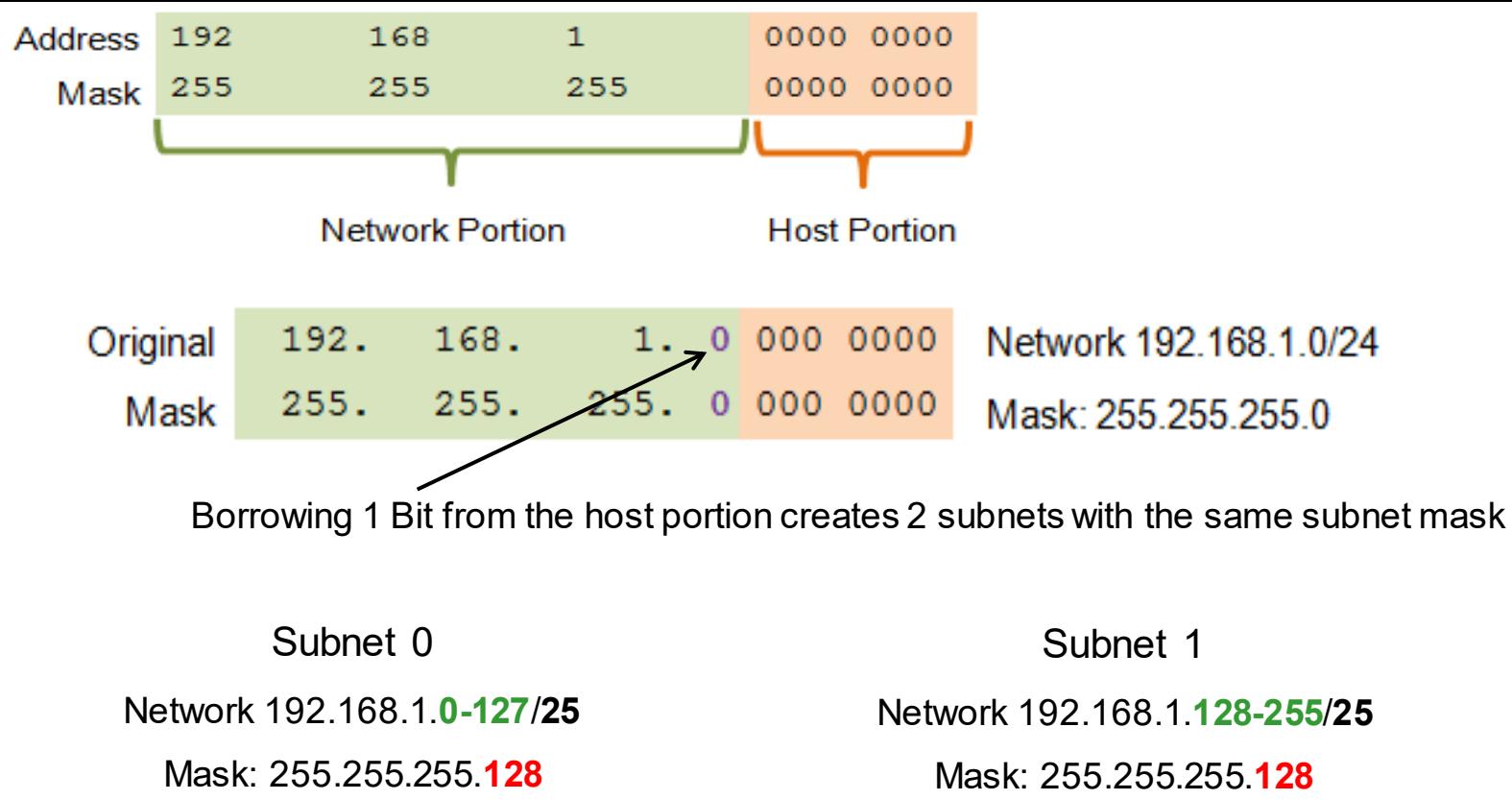
Planning requires decisions on each subnet in terms of size, the number of hosts per subnet, and how host addresses will be assigned.



# Subnetting an IPv4 Network

## Basic Subnetting

- Borrowing Bits to Create Subnets
- Borrowing 1 bit  $2^1 = 2$  subnets





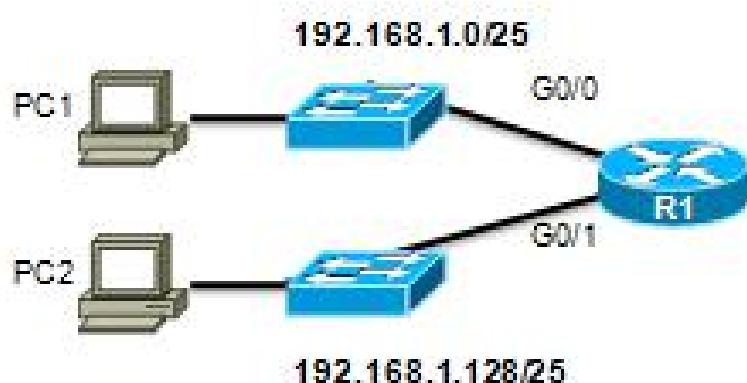
# Subnetting an IPv4 Network

## Subnets in Use

### Subnets in Use

Subnet 0

Network 192.168.1.0-127/25



Subnet 1

Network 192.168.1.128-255/25

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

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



# Subnetting an IPv4 Network

## Subnetting Formulas

Subnets =  $2^n$   
(where n = bits borrowed)

### Calculate number of subnets

192. 168. 1. 0 000 0000

1 bit was borrowed

$2^1 = 2$  subnets

Hosts =  $2^n$   
(where n = host bits remaining)

### Calculate number of hosts

192. 168. 1. 0 000 0000

7 bits remain in host field

$2^7 = 128$  hosts per subnet  
 $2^7 - 2 = 126$  valid hosts per subnet

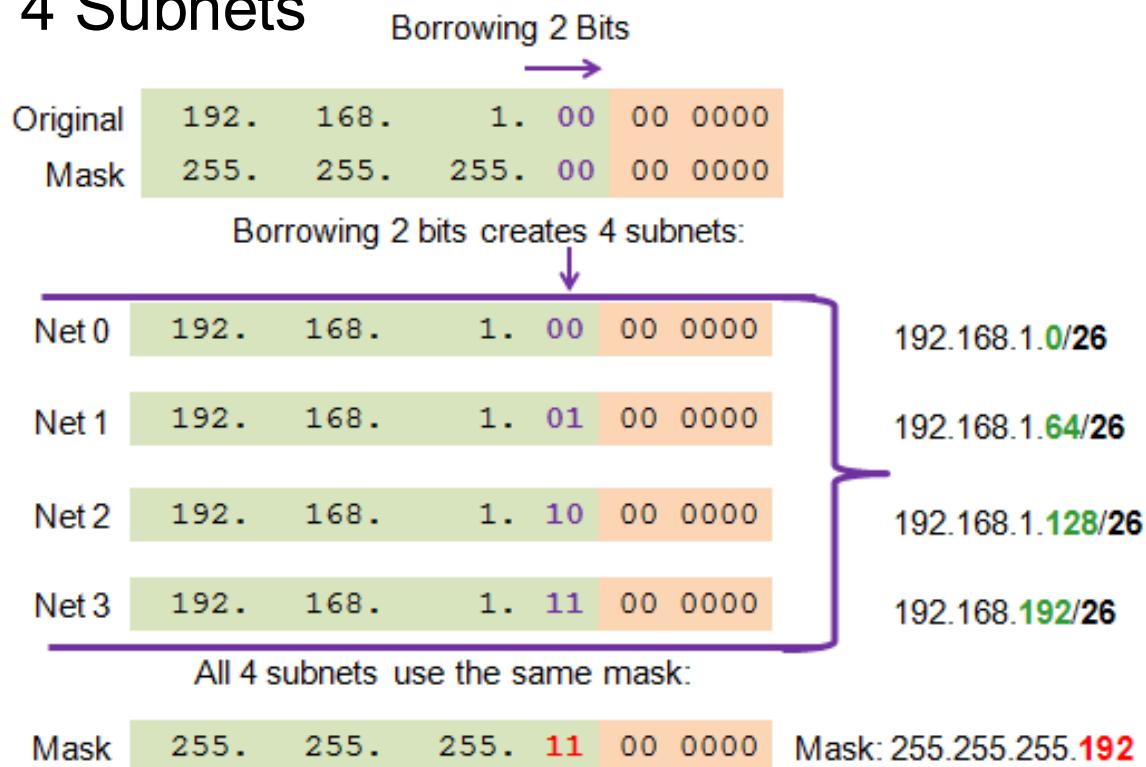


# Subnetting an IPv4 Network

## Creating 4 Subnets

Borrowing 2 bits to create 4 subnets.  $2^2 = 4$  subnets

### Creating 4 Subnets





# Subnetting an IPv4 Network

## Creating Eight Subnets

Borrowing 3 bits to Create 8 Subnets.  $2^3 = 8$  subnets

		Network	192.	168.	1.	000	0 0000	192.168.1.1
Net 0	Fist	192.	168.	1.	000	0 0001	192.168.1.1	
	Last	192.	168.	1.	000	1 1110	192.168.1.30	
	Broadcast	192.	168.	1.	000	1 1111	192.168.1.31	
	Network	192.	168.	1.	001	0 0000	192.168.1.32	
Net 1	Fist	192.	168.	1.	001	0 0001	192.168.1.33	
	Last	192.	168.	1.	001	1 1110	192.168.1.62	
	Broadcast	192.	168.	1.	001	1 1111	192.168.1.63	
	Network	192.	168.	1.	010	0 0000	192.168.1.64	
Net 2	Fist	192.	168.	1.	010	0 0001	192.168.1.65	
	Last	192.	168.	1.	010	1 1110	192.168.1.94	
	Broadcast	192.	168.	1.	010	1 1111	192.168.1.95	
	Network	192.	168.	1.	010	0 0000	192.168.1.96	
Net 3	Fist	192.	168.	1.	010	0 0001	192.168.1.97	
	Last	192.	168.	1.	010	1 1110	192.168.1.126	
	Broadcast	192.	168.	1.	010	1 1111	192.168.1.127	



# Subnetting an IPv4 Network

## Creating Eight Subnets (Cont.)

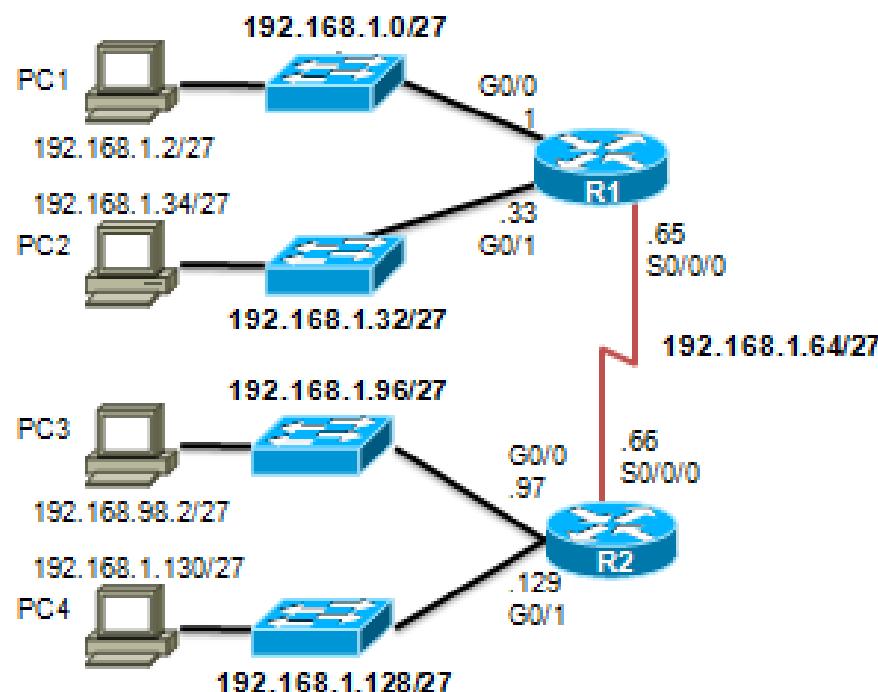
	Network	192.	168.	1.	100	0 0000	192.168.1.128
Net 4	Fist	192.	168.	1.	100	0 0001	192.168.1.129
	Last	192.	168.	1.	100	1 1110	192.168.1.158
	Broadcast	192.	168.	1.	100	1 1111	192.168.1.159
	Network	192.	168.	1.	101	0 0000	192.168.1.160
Net 5	Fist	192.	168.	1.	101	0 0001	192.168.1.161
	Last	192.	168.	1.	101	1 1110	192.168.1.190
	Broadcast	192.	168.	1.	101	1 1111	192.168.1.191
	Network	192.	168.	1.	110	0 0000	192.168.1.192
Net 6	Fist	192.	168.	1.	110	0 0001	192.168.1.193
	Last	192.	168.	1.	110	1 1110	192.168.1.222
	Broadcast	192.	168.	1.	110	1 1111	192.168.1.223
	Network	192.	168.	1.	111	0 0000	192.168.1.224
Net 7	Fist	192.	168.	1.	111	0 0001	192.168.1.225
	Last	192.	168.	1.	111	1 1110	192.168.1.254
	Broadcast	192.	168.	1.	111	1 1111	192.168.1.255



# Subnetting an IPv4 Network

## Creating Eight Subnets (Cont.)

### Subnet Allocation





## Determining the Subnet Mask

# Subnetting Based on Host Requirements

**Two considerations when planning subnets:**

- Number of subnets required
- Number of host addresses required

**Formula to determine number of usable hosts:  $2^n - 2$**

- $2^n$  (where  $n$  is the number of remaining host bits) is used to calculate the number of hosts.
- $-2$  (The subnetwork ID and broadcast address cannot be used on each subnet.)

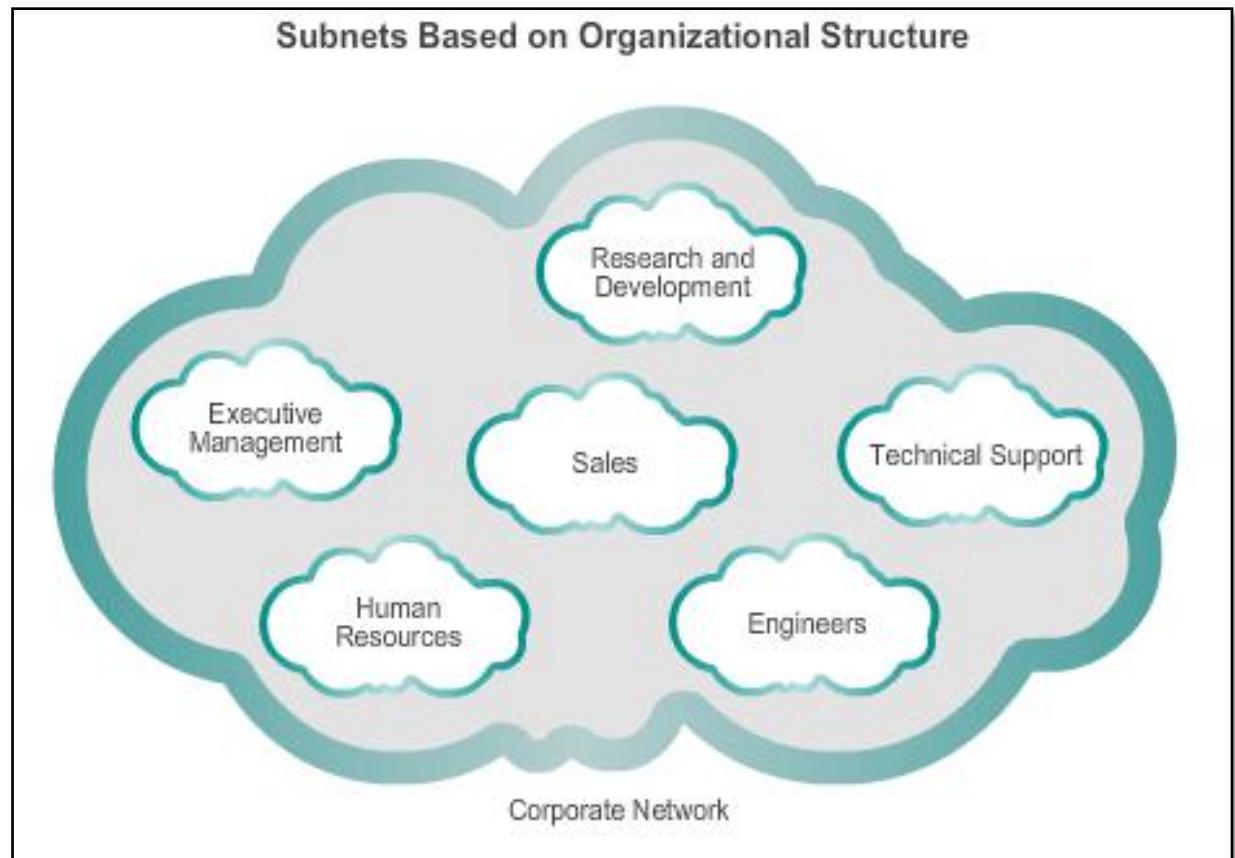


# Determining the Subnet Mask

## Subnetting Network-Based Requirements

### Calculate the number of subnets:

- $2^n$  (where n is the number of bits borrowed)
- Subnet needed for each department.

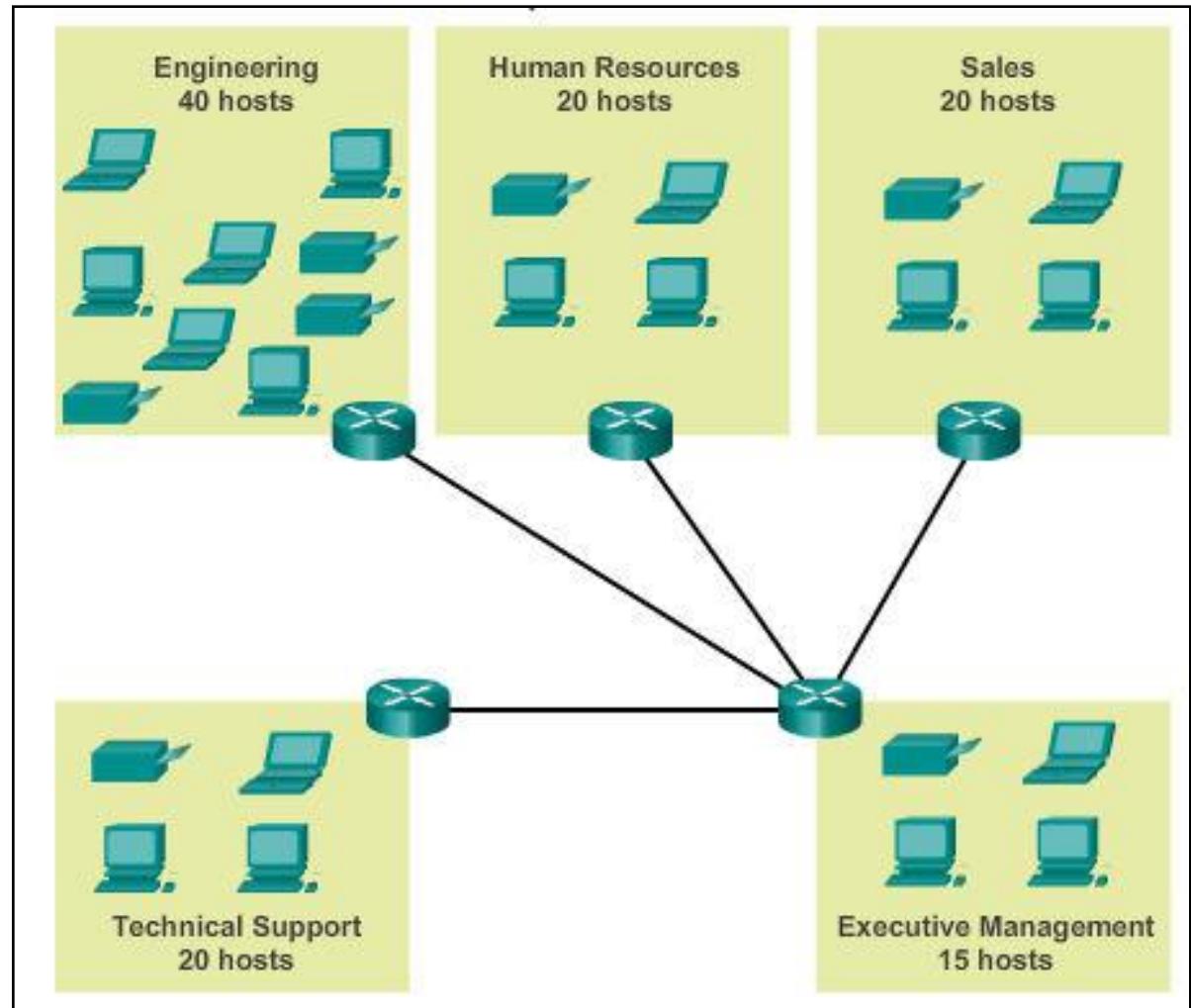




## Determining the Subnet Mask

# Subnetting To Meet Network Requirements

- Balance the required number of subnets and hosts for the largest subnet.
- Design the addressing scheme to accommodate the maximum number of hosts for each subnet.
- Allow for growth in each subnet.





## Determining the Subnet Mask

# Subnetting To Meet Network Requirements

### Subnets and Addresses

	10101100.00010000.00000000.00.00000000	172.16.0.0/22
0	10101100.00010000.00000000.00.01000000	172.16.0.0/26
1	10101100.00010000.00000000.00.01000000	172.16.0.64/26
2	10101100.00010000.00000000.00.10000000	172.16.0.128/26
3	10101100.00010000.00000000.00.11000000	172.16.0.192/26
4	10101100.00010000.00000000.01.00000000	172.16.1.0/26
5	10101100.00010000.00000000.01.01000000	172.16.1.64/26
6	10101100.00010000.00000000.01.10000000	172.16.1.128/26

Nets 7 – 14 not shown

15	10101100.00010000.00000000.11.10000000	172.16.3.128/26
16	10101100.00010000.00000000.11.11000000	172.16.3.192/26



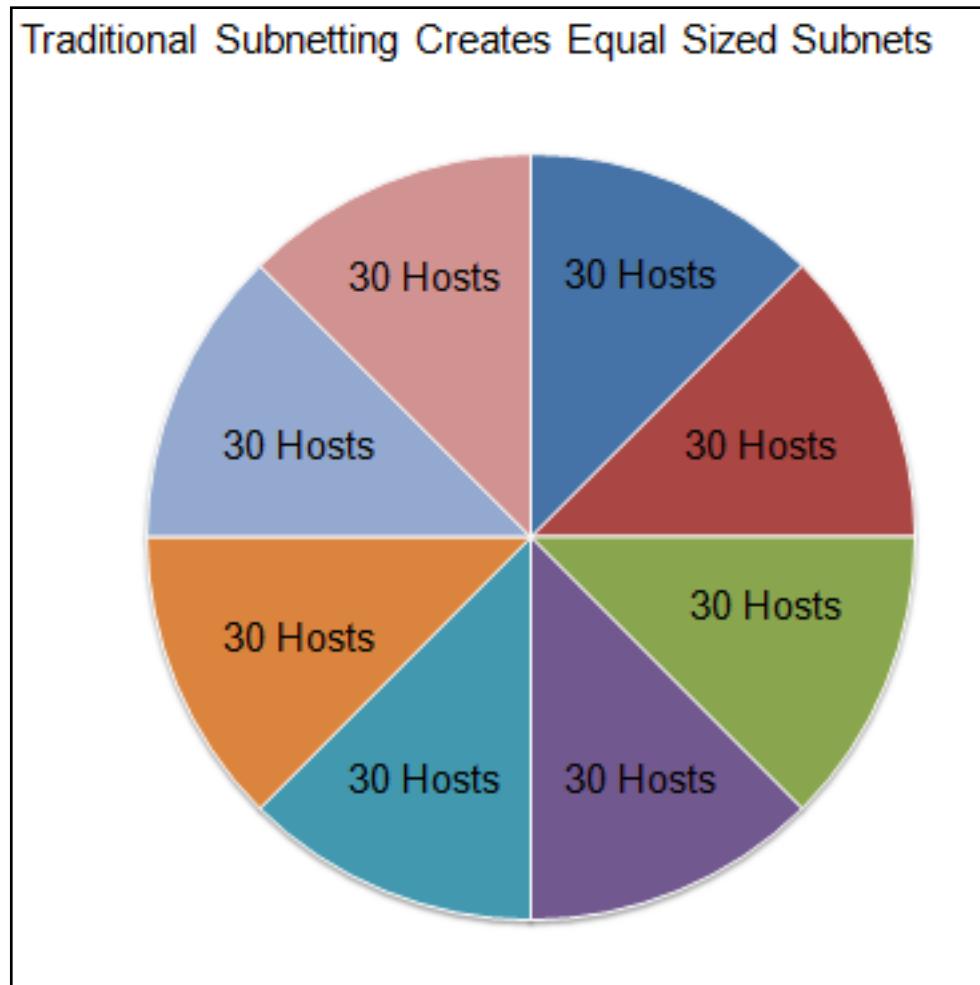
$$\begin{array}{ll} 2^4 = 16 & 2^6 - 2 = 62 \\ \text{subnets} & \text{Hosts per} \\ & \text{subnet} \end{array}$$



## Benefits of Variable Length Subnet Masking

# Traditional Subnetting Wastes Addresses

- Traditional subnetting – Uses the same number of addresses is allocated for each subnet.
- Subnets that require fewer addresses have unused (wasted) addresses; for example, WAN links only need two addresses.

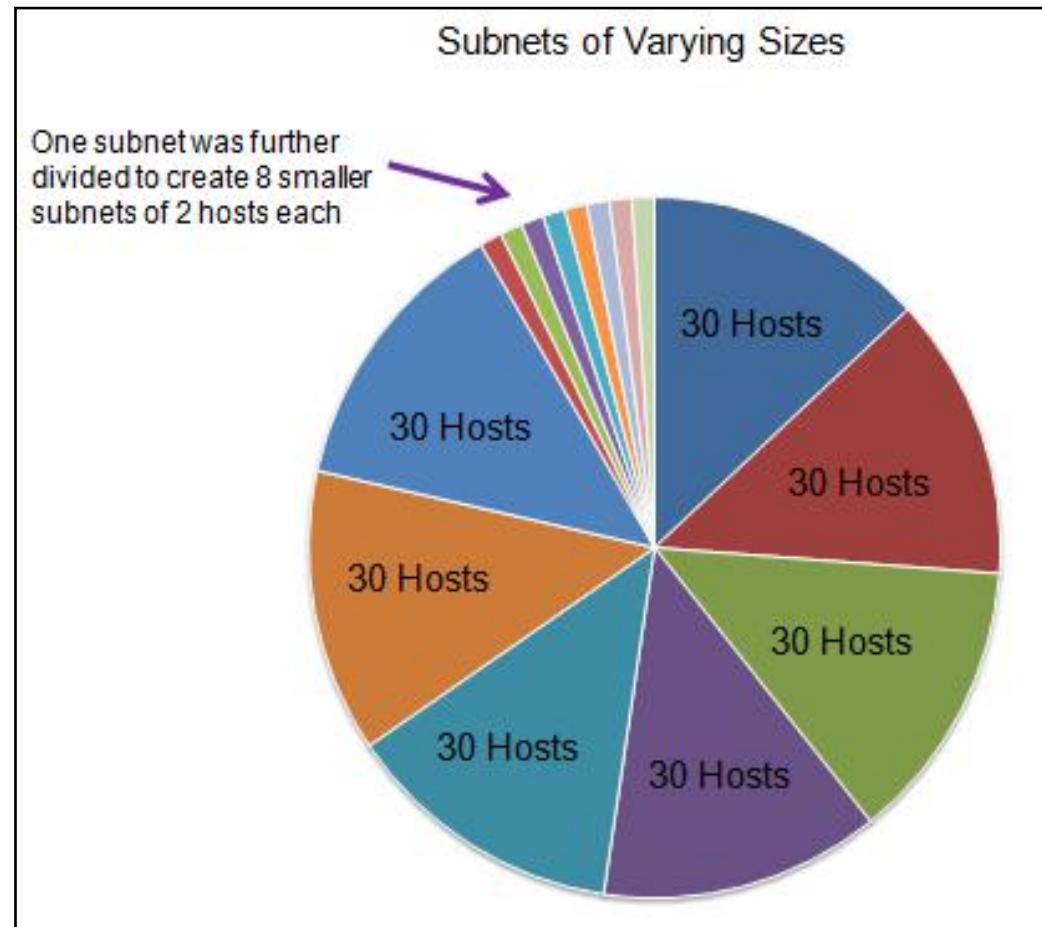




## Benefits of Variable Length Subnet Masking

# Variable Length Subnet Masks (VLSM)

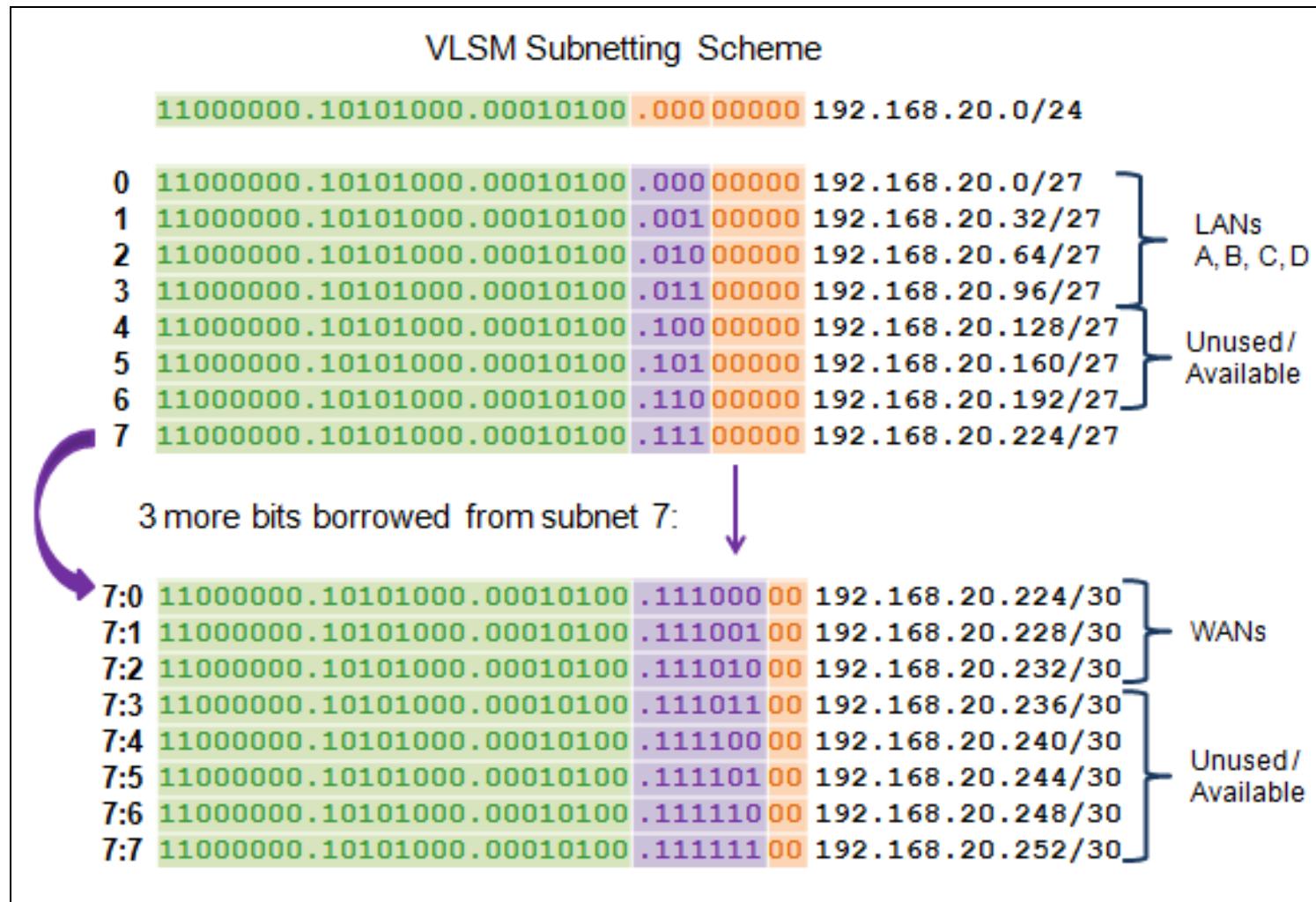
- The variable-length subnet mask (VLSM) or subnetting a subnet provides more efficient use of addresses.
- VLSM allows a network space to be divided in unequal parts.
- Subnet mask varies, depending on how many bits have been borrowed for a particular subnet.
- Network is first subnetted, and then the subnets are resubnetted.





# Benefits of Variable Length Subnet Masking

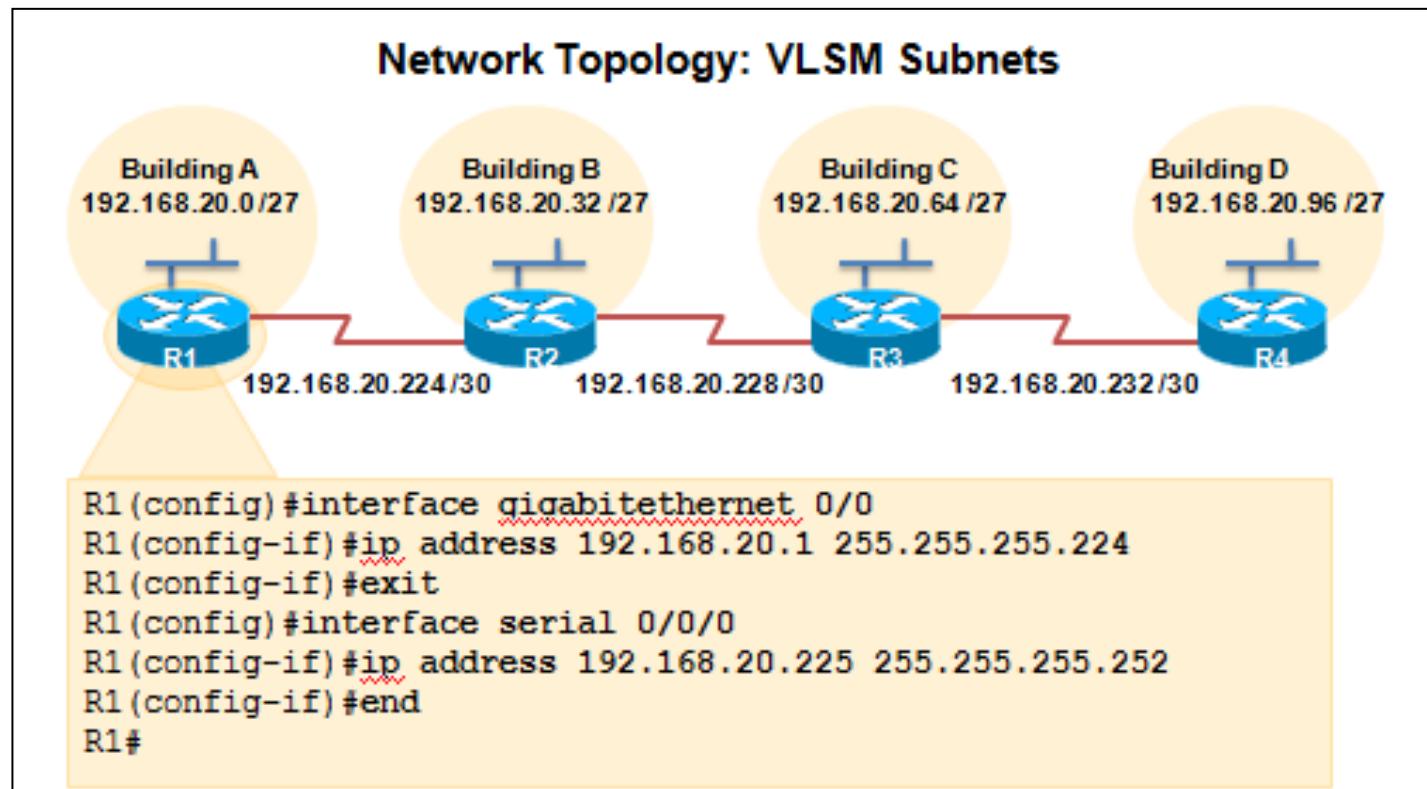
## Basic VLSM





# Benefits of Variable Length Subnet Masking VLSM in Practice

- Using VLSM subnets, the LAN and WAN segments in example below can be addressed with minimum waste.
- Each LANs will be assigned a subnet with /27 mask.
- Each WAN link will be assigned a subnet with /30 mask.





# Benefits of Variable Length Subnet Masking

## VLSM Chart

VLSM Subnetting of 192.168.20.0 /24

	/27 Network	Hosts
Bldg A	.0	.1 - .30
Bldg B	.32	.33 - .62
Bldg C	.64	.65 - .94
Bldg D	.96	.97 - .126
Unused	.128	.129 - .158
Unused	.160	.161 - .190
Unused	.192	.193 - .222
	.224	.225 - .254

	/30 Network	Hosts
WAN R1-R2	.224	.225 - .226
WAN R2-R3	.228	.229 - .230
WAN R3-R4	.232	.233 - .234
Unused	.236	.237 - .238
Unused	.240	.241 - .242
Unused	.244	.245 - .246
Unused	.248	.249 - .250
Unused	.252	.253 - .254

## 9.2 Addressing Schemes





# Structured Design

## Planning to Address the Network

Allocation of network addresses should be planned and documented for the purposes of:

- Preventing duplication of addresses
- Providing and controlling access
- Monitoring security and performance

Client addresses – Usually dynamically assigned using the Dynamic Host Configuration Protocol (DHCP).

Sample  
Network  
Addressing  
Plan

Network: 192.168.1.0/24		
Use	First	Last
Host Devices	.1	.229
Servers	.230	.239
Printers	.240	.249
Intermediary Devices	.250	.253
Gateway (router LAN interface)	.254	

## 9.3 Design Considerations for IPv6

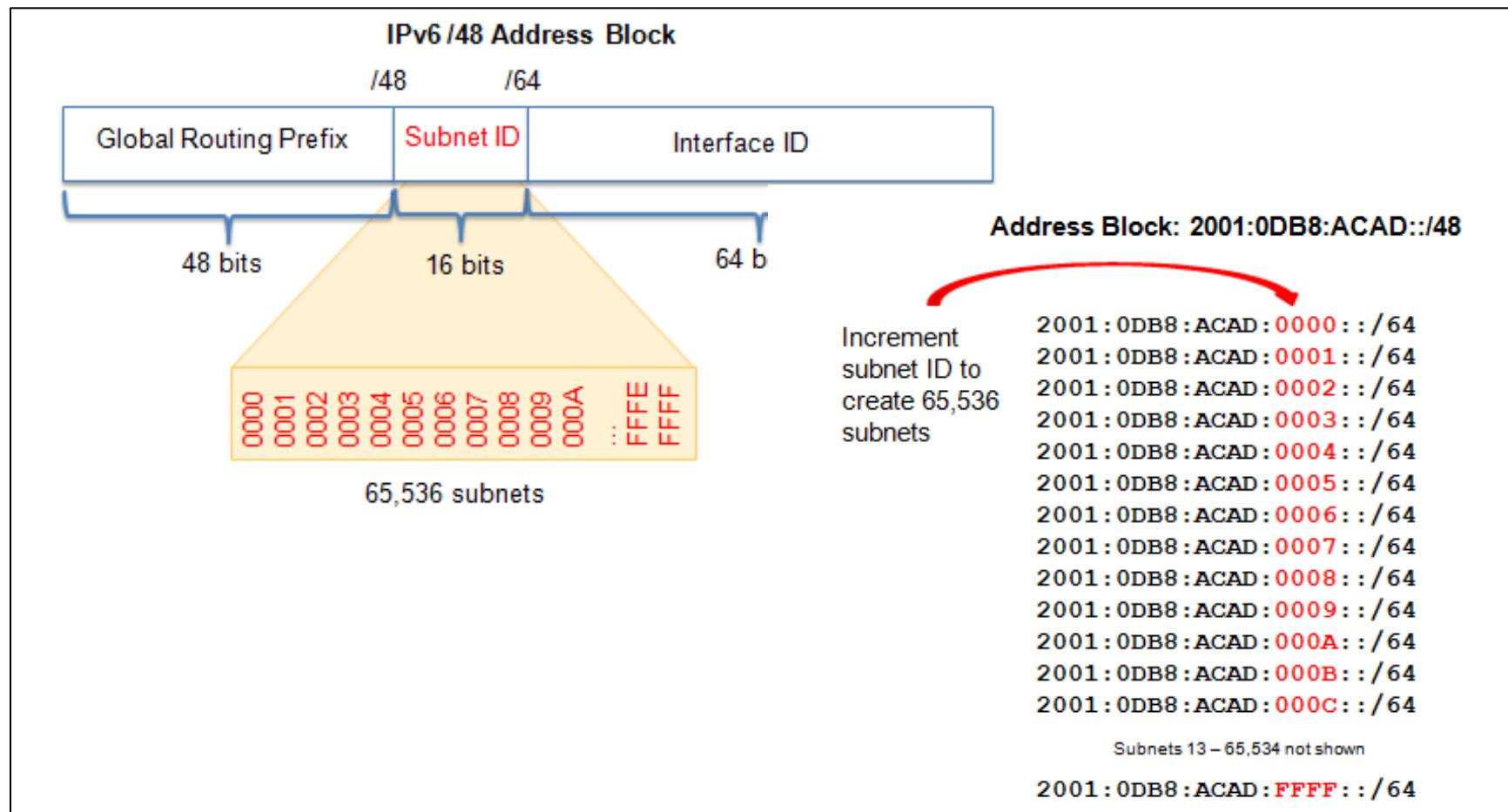




# Subnetting an IPv6 Network

## Subnetting Using the Subnet ID

An IPv6 Network Space is subnetted to support hierarchical, logical design of the network





# Subnetting an IPv6 Network

## IPv6 Subnet Allocation

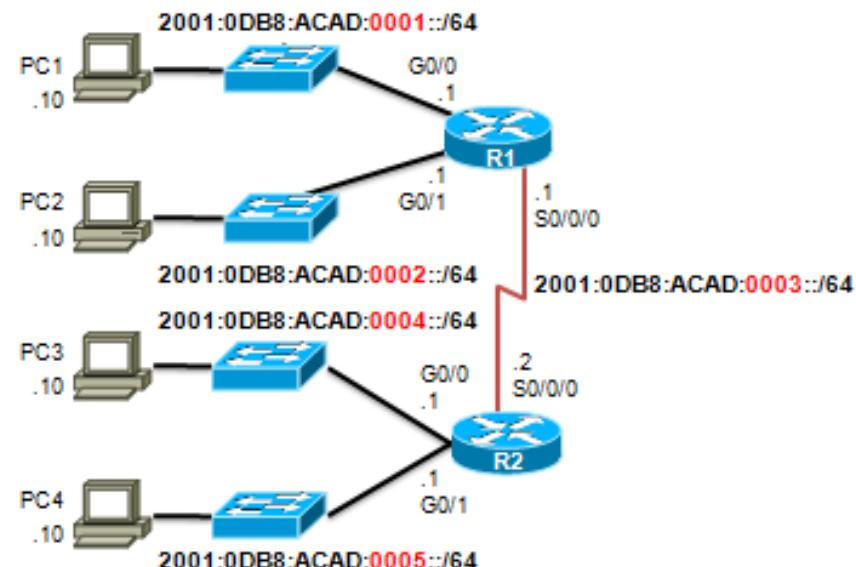
### IPv6 Subnetting

Address Block: 2001:0DB8:ACAD::/48

5 subnets  
allocated from  
65,536 available  
subnets

2001:0DB8:ACAD:0000::/64  
2001:0DB8:ACAD:0001::/64  
2001:0DB8:ACAD:0002::/64  
2001:0DB8:ACAD:0003::/64  
2001:0DB8:ACAD:0004::/64  
2001:0DB8:ACAD:0005::/64  
2001:0DB8:ACAD:0006::/64  
2001:0DB8:ACAD:0007::/64  
2001:0DB8:ACAD:0008::/64  
⋮  
2001:0DB8:ACAD:FFFF::/64

### IPv6 Subnet Allocation

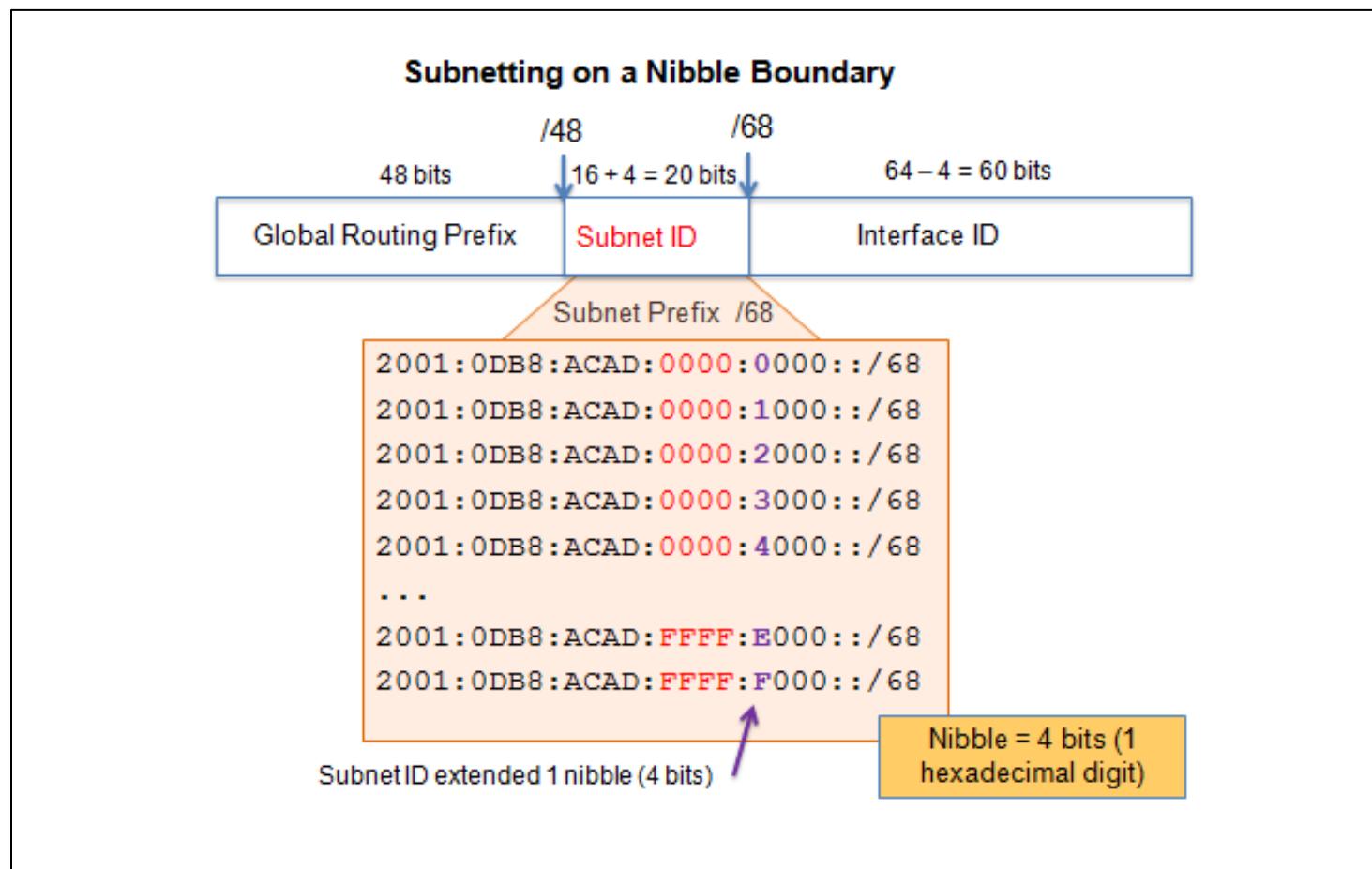




# Subnetting an IPv6 Network

## Subnetting into the Interface ID

IPv6 bits can be borrowed from the interface ID to create additional IPv6 subnets.



## 9.3 Summary





# Chapter 9: Summary

In this chapter, you learned that:

- Subnetting is the process of segmenting a network, by dividing it into multiple smaller network spaces.
- Subnetting a subnet, or using VLSM, was designed to avoid wasting addresses.
- IPv6 address space is subnetted to support the hierarchical, logical design of the network.
- Size, location, use, and access requirements are all considerations in the address planning process.
- IP networks must be tested to verify connectivity and operational performance.

**Cisco** | **Networking Academy**<sup>®</sup>  
| Mind Wide Open<sup>™</sup>

# Chapter 10:

## Application Layer



## Introduction to Networks



# Chapter 10: Objectives

By the end of this chapter, you will be able to:

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



# Chapter 10

10.0 Introduction

10.1 Application Layer Protocols

10.2 Well-Known Application Layer Protocols and Service

10.3 The Message Heard Around the World

10.4 Summary



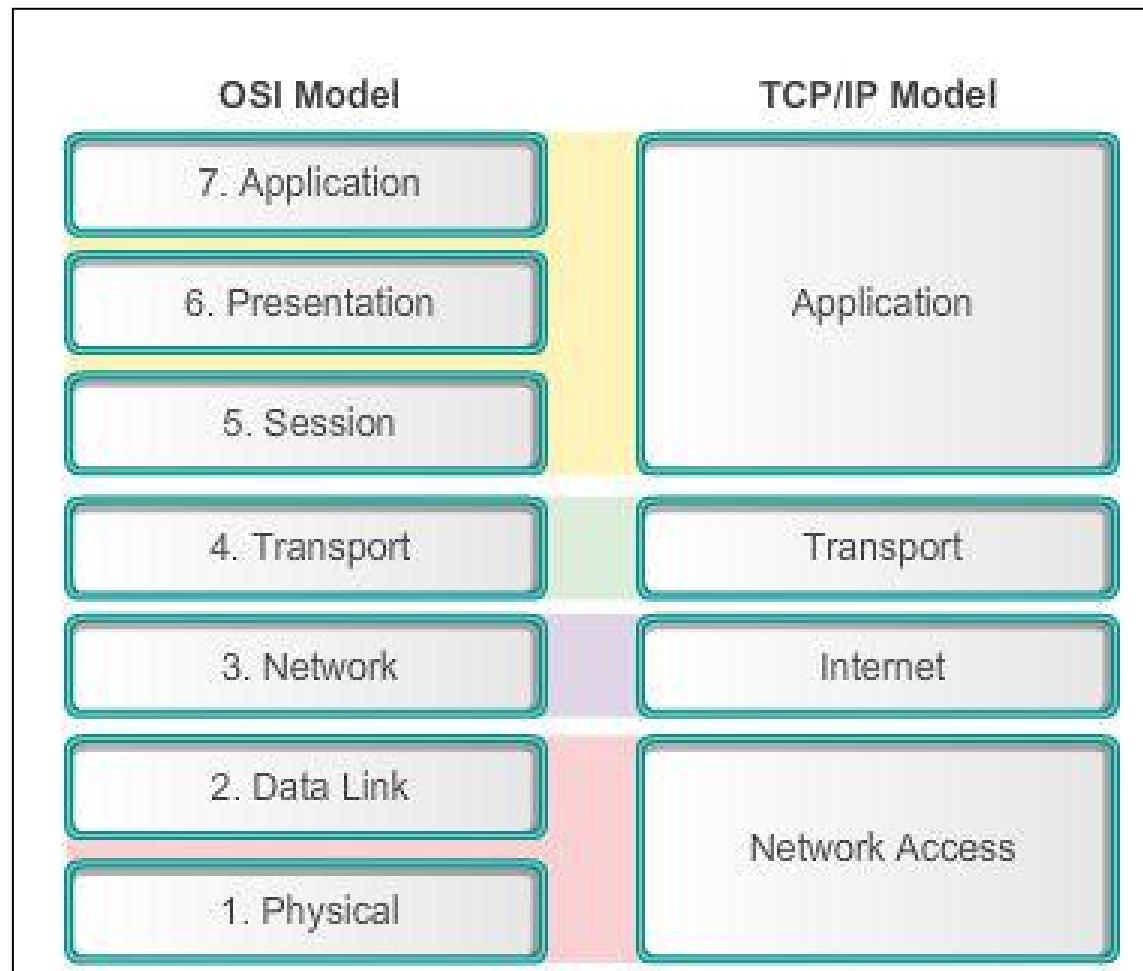
## 10.1 Application Layer Protocols



Cisco | Networking Academy®  
Mind Wide Open™



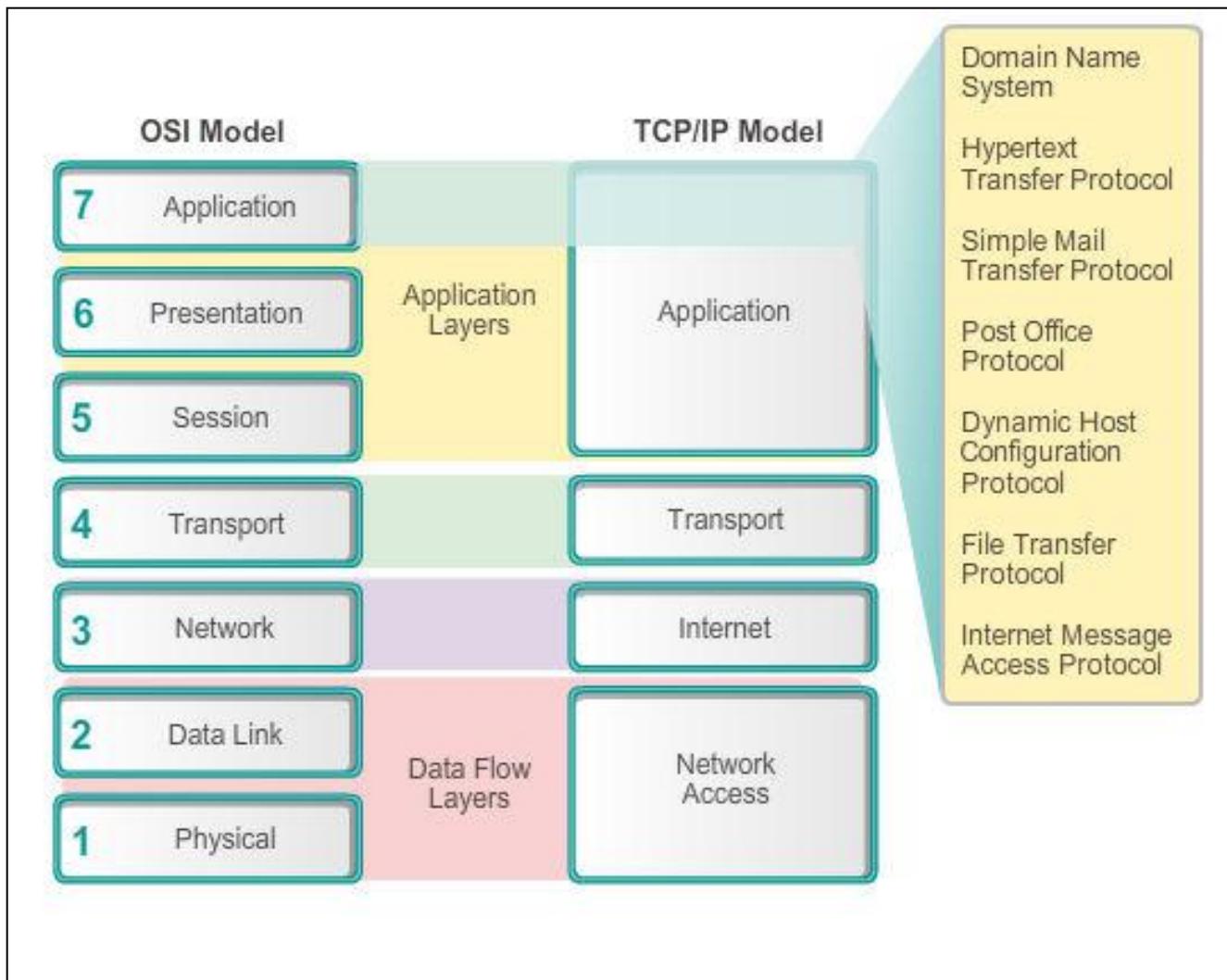
# Application, Session and Presentation OSI and TCP/IP Models Revisited



The key parallels are in the transport and network layer.



# Application Session and Presentation Application Layer





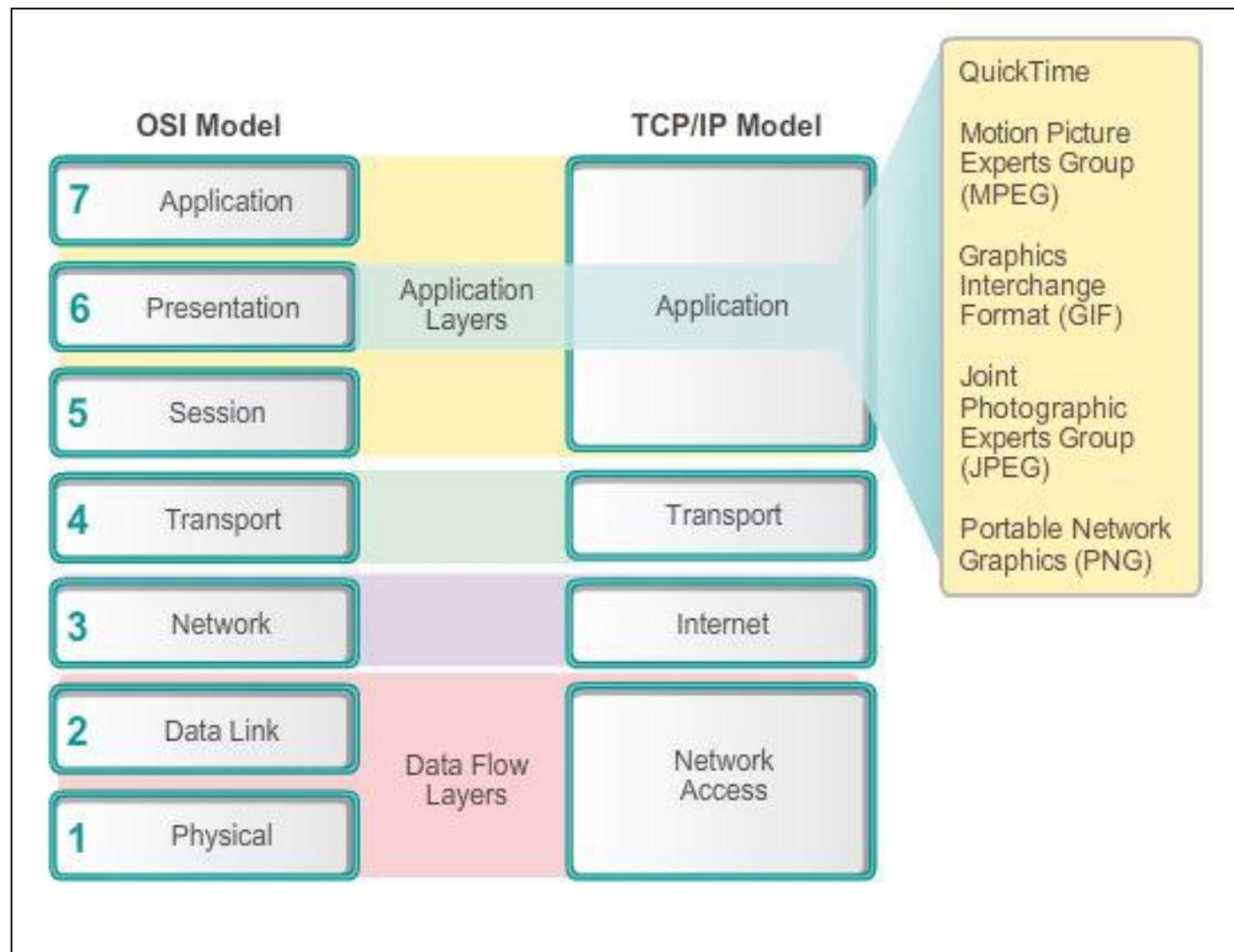
# Application, Session and Presentation Presentation and Session Layers

- **Presentation layer**
  - Coding and conversion of application layer data
  - Data compression
  - Data encryption for the transmission and decryption of data upon receipt by the destination
- **Session layer**
  - Functions, creates, and maintains dialogs between source and destination applications
  - Handles the exchange of information to initiate dialogs, keep them active, and to restart sessions



## Application, Session and Presentation

# Presentation and Session Layers (cont.)





# Application, Session and Presentation TCP/IP Application Layer Protocols

- **Domain Name Service Protocol (DNS)** – used to resolve Internet names to IP addresses
- **Telnet** – a terminal emulation protocol used to provide remote access to servers and networking devices
- **Bootstrap Protocol (BOOTP)** – a precursor to the DHCP protocol, a network protocol used to obtain IP address information during bootup
- **Dynamic Host Control Protocol (DHCP)** – used to assign an IP address, subnet mask, default gateway and DNS server to a host
- **Hypertext Transfer Protocol (HTTP)** – used to transfer files that make up the Web pages of the World Wide Web



## Application, Session and Presentation

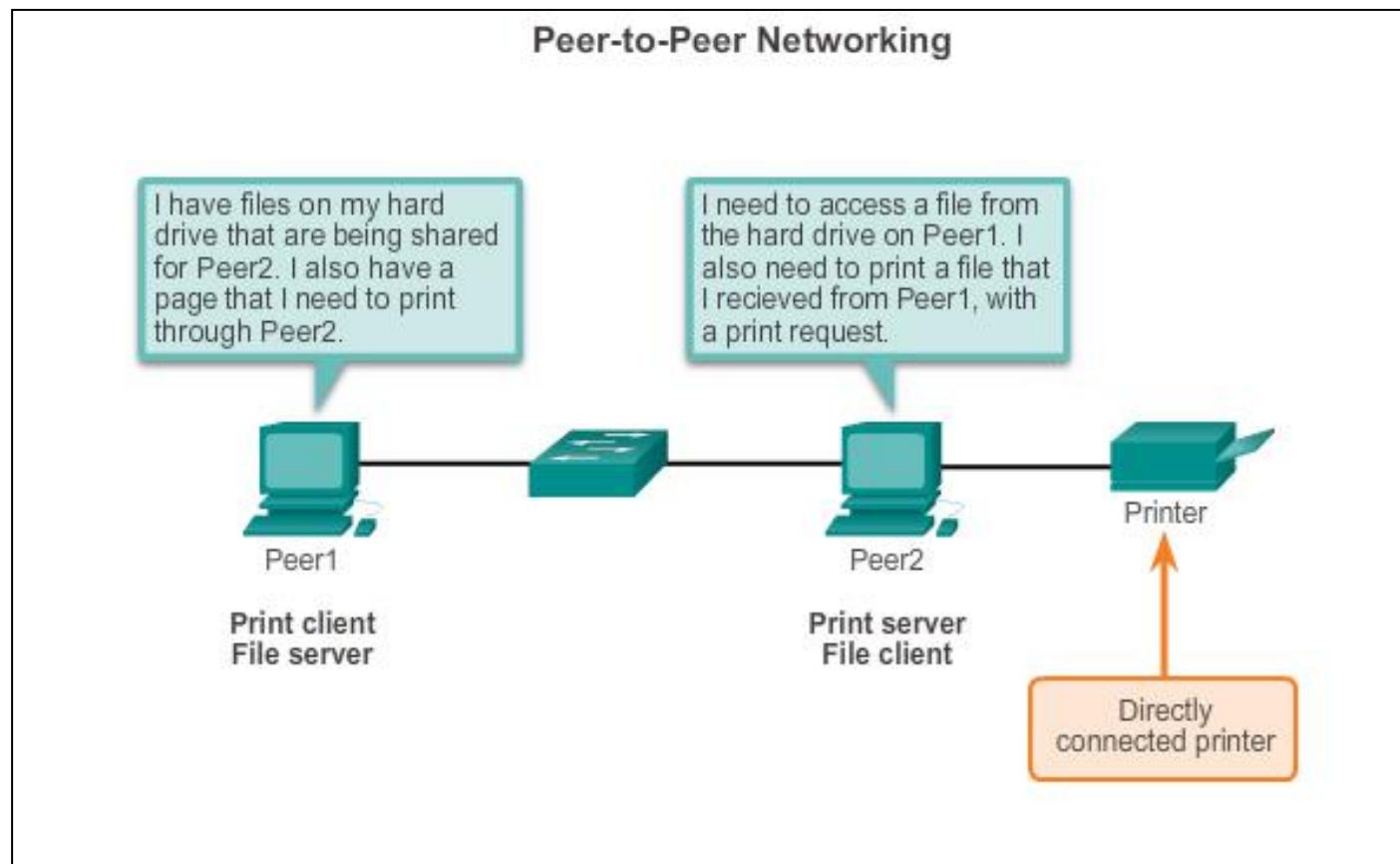
# TCP/IP Application Layer Protocols (cont.)

- **File Transfer Protocol (FTP)** - used for interactive file transfer between systems
- **Trivial File Transfer Protocol (TFTP)** - used for connectionless active file transfer
- **Simple Mail Transfer Protocol (SMTP)** - used for the transfer of mail messages and attachments
- **Post Office Protocol (POP)** - used by email clients to retrieve email from a remote server
- **Internet Message Access Protocol (IMAP)** – another protocol for email retrieval



# How Application Protocols Interact with End-User Applications

## Peer-to-Peer Networks



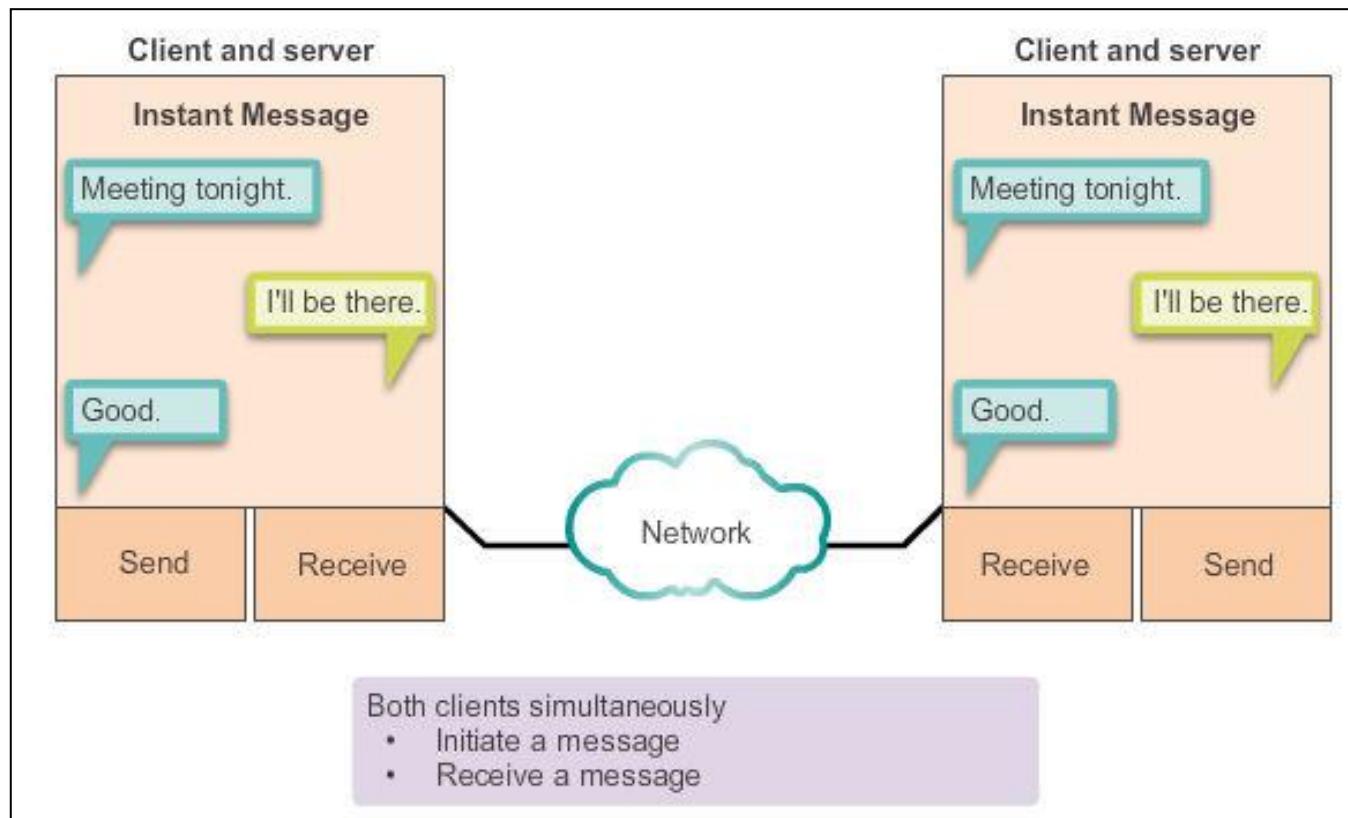
Both devices are considered equal in the communication.  
The roles of client and server are set on a per request basis.



# How Application Protocols Interact with End-User Applications

## Peer-to-Peer Applications

Client and server in the same communication.



Both can initiate a communication and are considered equal in the communication process.



## How Application Protocols Interact with End-User Applications

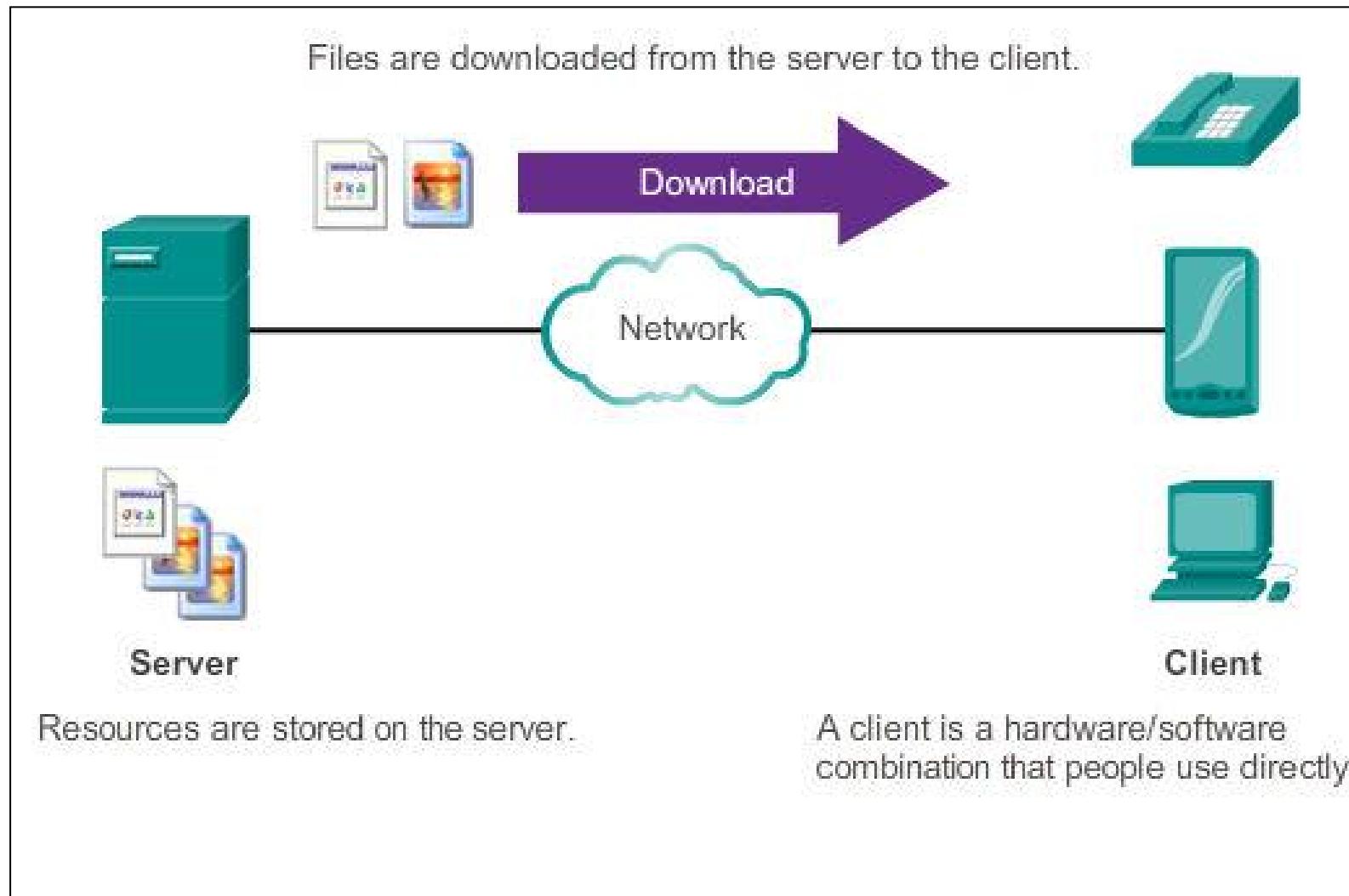
# Common P2P Applications

- With P2P applications, each computer in the network running the application can act as a client or a server for the other computers in the network running the application.
- Common P2P applications include:
  - eDonkey
  - eMule
  - Shareaza
  - BitTorrent
  - Bitcoin
  - LionShare
- Some P2P applications are based on the Gnutella protocol which enables people to share files on their hard disks with others



# How Application Protocols Interact with End-User Applications

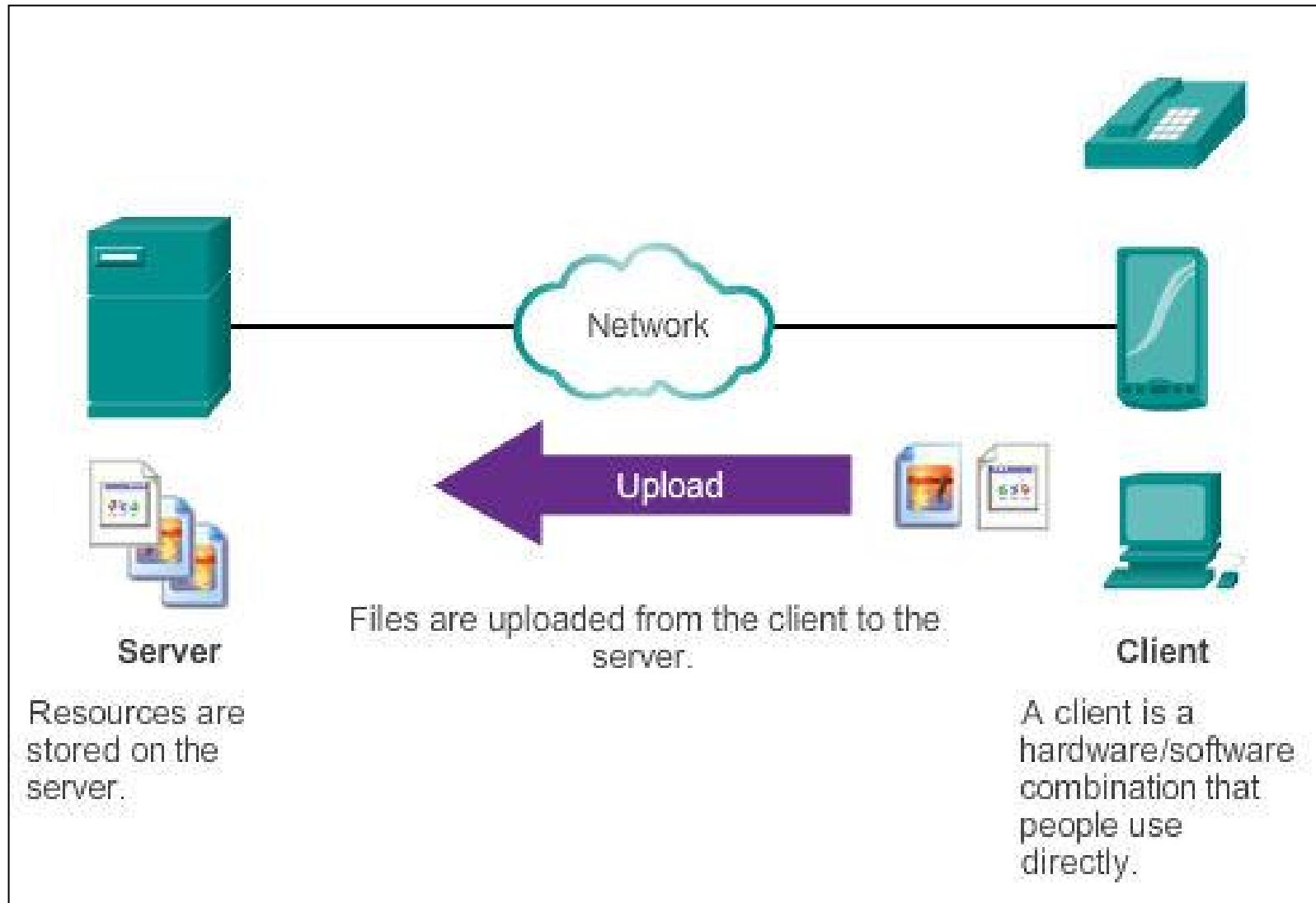
## Client-Server Model





# How Application Protocols Interact with End-User Applications

## Client-Server Model



## 10.2 Well-Known Application Layer Protocols and Services





## Common Application Layer Protocols

# Application Layer Protocols Revisited

Three application layer protocols involved in everyday work or play include:

- **HTTP** to browse the web.
- **Simple Mail Transfer Protocol (SMTP)** to enable users to send email.
- **Post Office Protocol (POP)** to enable users to receive email.



## Common Application Layer Protocols

# Hypertext Transfer Protocol and Hypertext Markup Language

Example URL: <http://www.cisco.com/index.html>

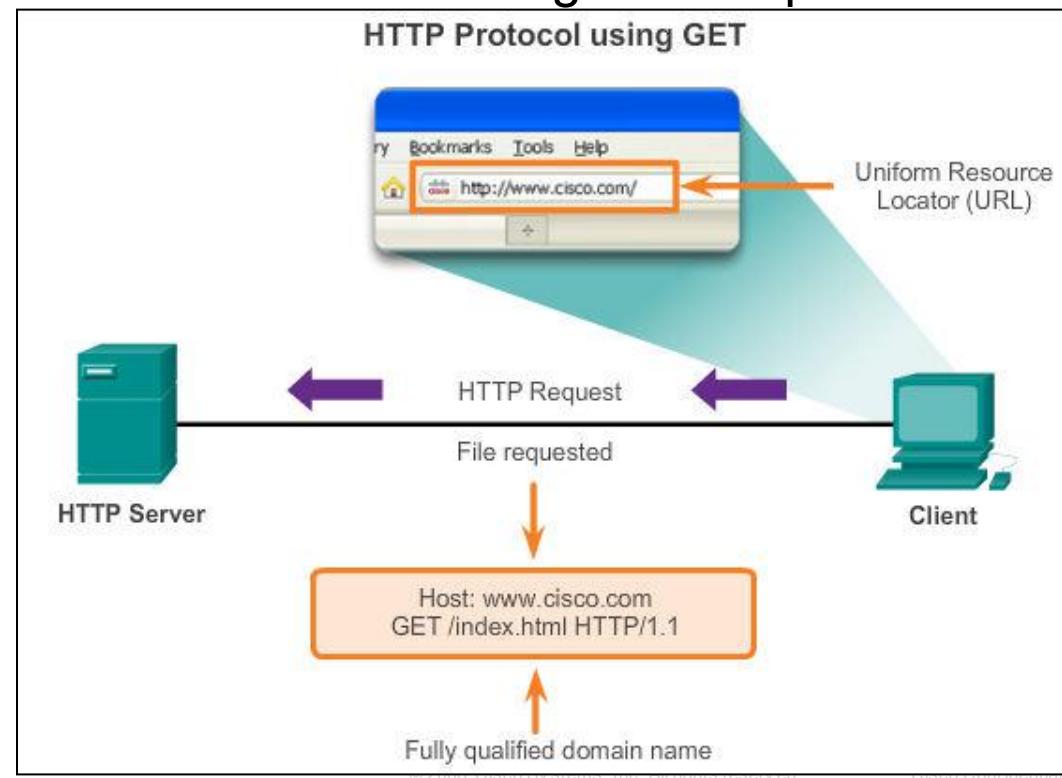
1. First, the browser interprets the three parts of the URL:
  - **http** (the protocol or scheme)
  - **www.cisco.com** (the server name)
  - **index.html** (the specific file name requested)
2. Browser checks with a name server to convert **www.cisco.com** into a numeric address
3. Using the HTTP protocol requirements sends a GET request to the server and asks for the file **index.html**
4. Server sends the HTML code for this web page
5. Browser deciphers the HTML code and formats the page



# Common Application Layer Protocols

## HTTP and HTTPS

- Developed to publish and retrieve HTML pages
- Used for data transfer
- Specifies a request/response protocol
- Three common message types are GET, POST, and PUT
- GET is a client request for data
- POST and PUT are used to send messages that upload data to the web server

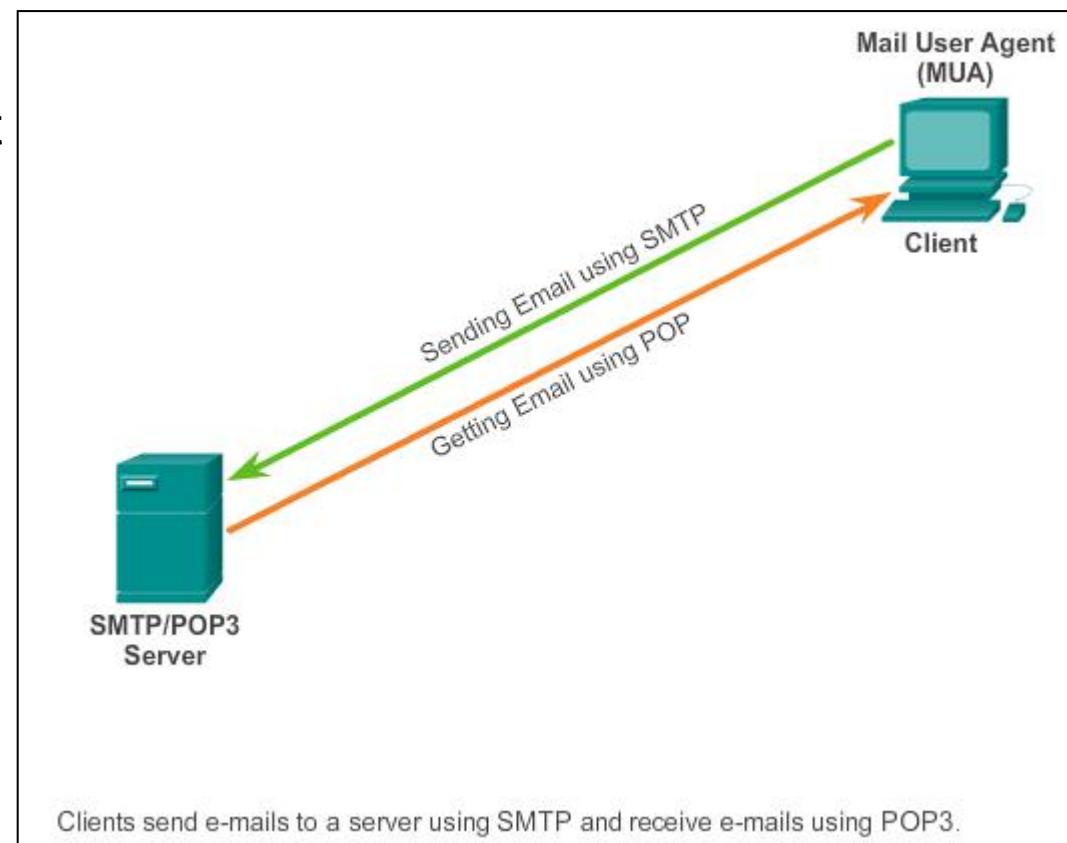




# Common Application Layer Protocols

## SMTP, POP, and IMAP

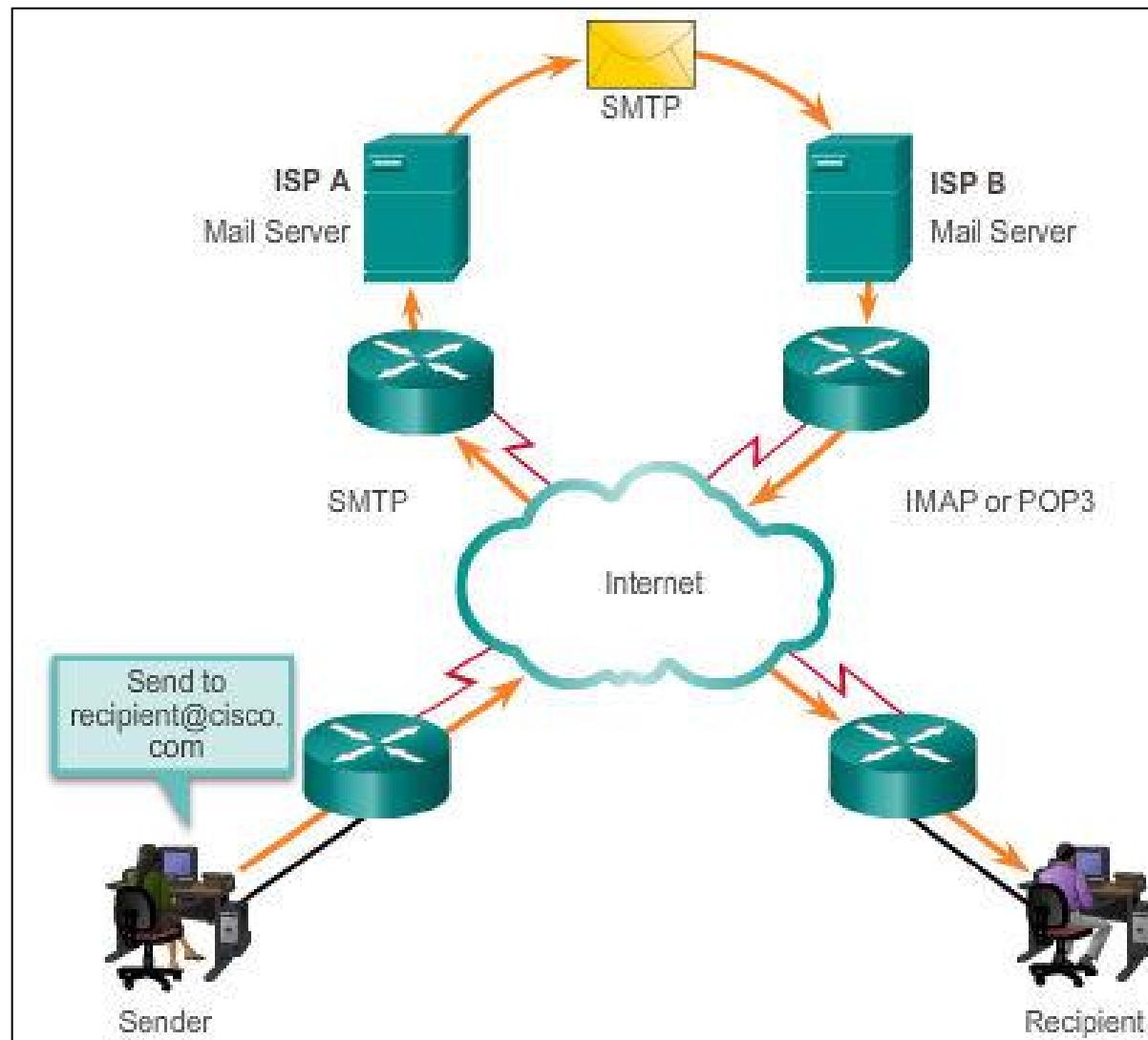
- Typically use an application called a Mail User Agent (email client)
- Allows messages to be sent
- Places received messages into the client's mailbox
- SMTP - Send email from either a client or a server
- POP - Receive email messages from an email server
- IMAP - Internet Message Access Protocol
- Email client provides the functionality of both protocols within one application





# Common Application Layer Protocols

## SMTP, POP, and IMAP (cont.)





# Common Application Layer Protocols

## SMTP, POP, and IMAP (cont.)

### Simple Mail Transfer Protocol (SMTP)

- transfers mail
- message must be formatted properly
- SMTP processes must be running on both the client and server
- message header must have a properly formatted recipient email address and a sender
- uses port 25

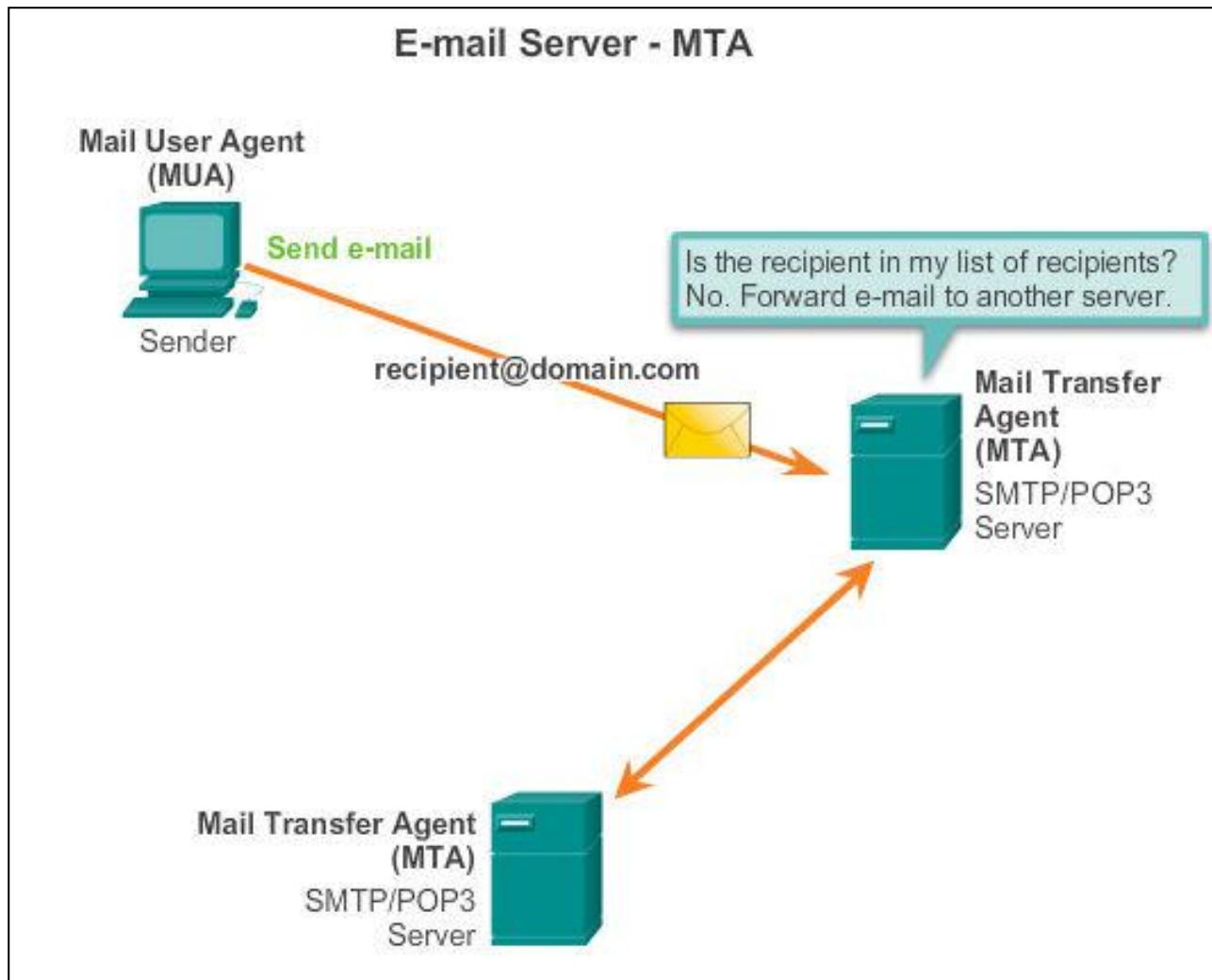
### Post Office Protocol (POP)

- enables a workstation to retrieve mail from a mail server
- mail is downloaded from the server to the client and then deleted on the server
- uses port 110
- POP does not store messages
- POP3 is desirable for an ISP, because it alleviates their responsibility for managing large amounts of storage for their email servers



# Common Application Layer Protocols

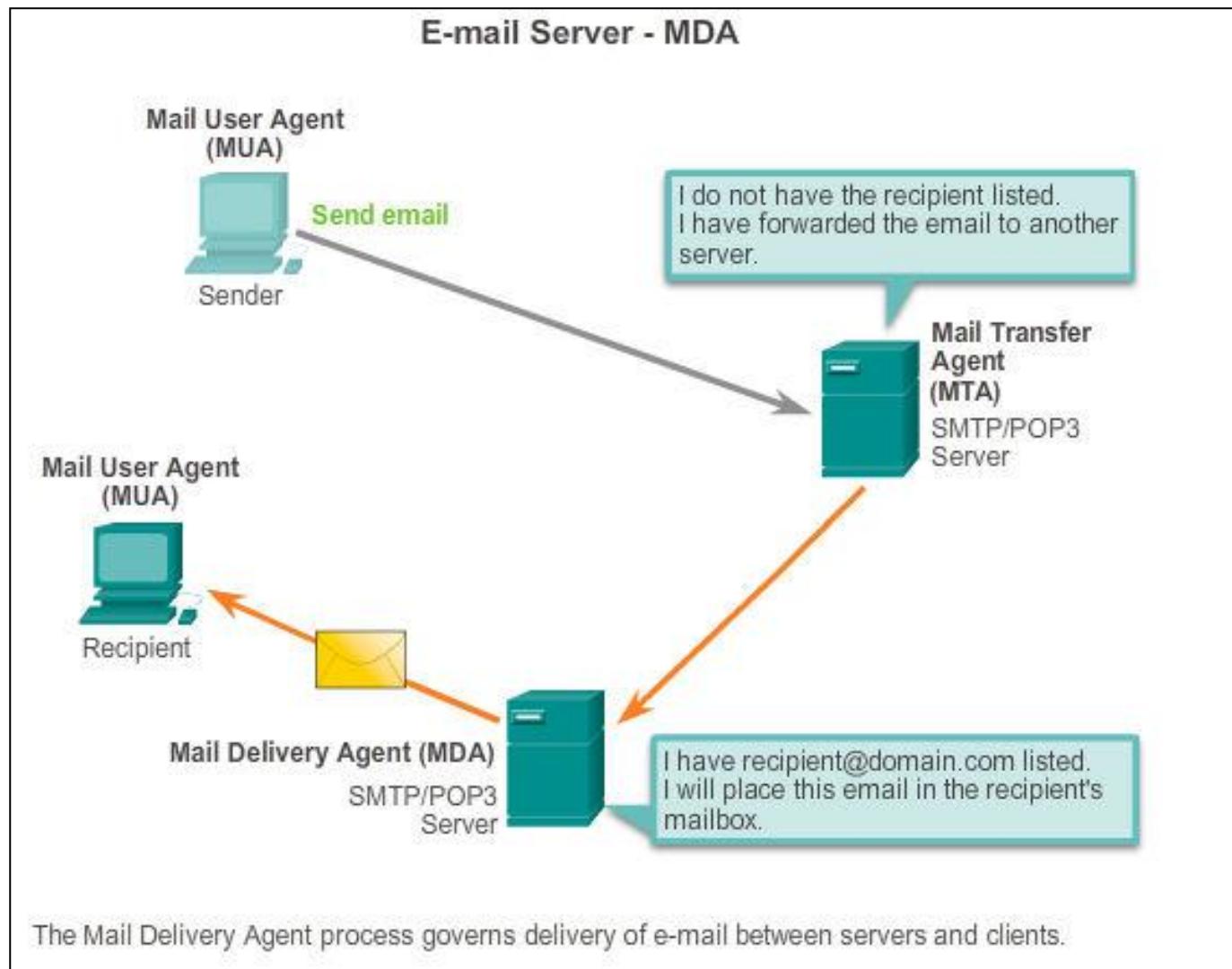
## SMTP, POP, and IMAP (cont.)



The Mail Transfer Agent process governs e-mail handling between servers and clients.



# Common Application Layer Protocols SMTP, POP, and IMAP (cont.)





## Everyday Application Layer Protocols SMTP, POP, and IMAP (cont.)

- MDA accepts a piece of email from MTA and performs the actual delivery.
- MDA receives all the inbound mail from the MTA and places it into mailboxes.
- MDA can also resolve final delivery issues, such as virus scanning, spam filtering, and return-receipt handling.



# Common Application Layer Protocols

## SMTP, POP, and IMAP (cont.)

### **Simple Mail Transfer Protocol (SMTP)**

- Transfers mail reliably and efficiently

### **Post Office Protocol (POP)**

- Enables a workstation to retrieve mail from a mail server
- With POP, mail is downloaded from the server to the client and then deleted on the server

### **Internet Message Access Protocol (IMAP)**

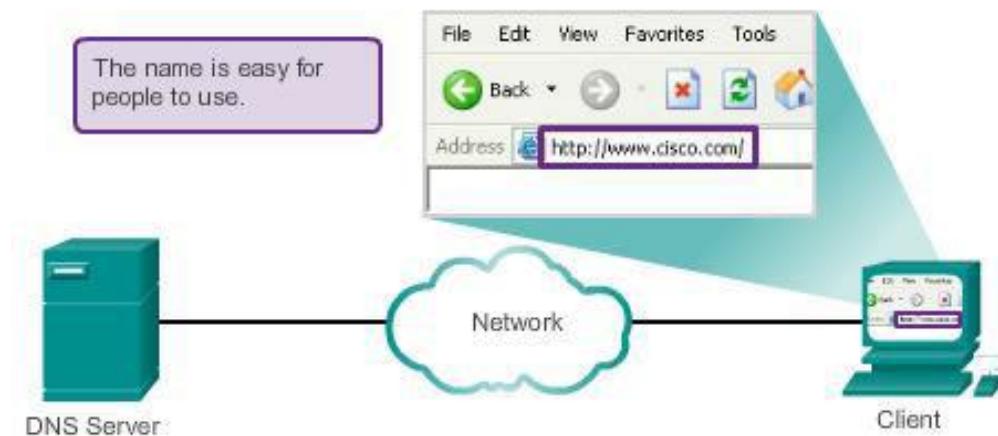
- Another protocol that retrieves email messages
- Unlike POP, when the user connects to an IMAP-capable server, copies of the messages are downloaded to the client application
- Original messages are kept on the server until manually deleted



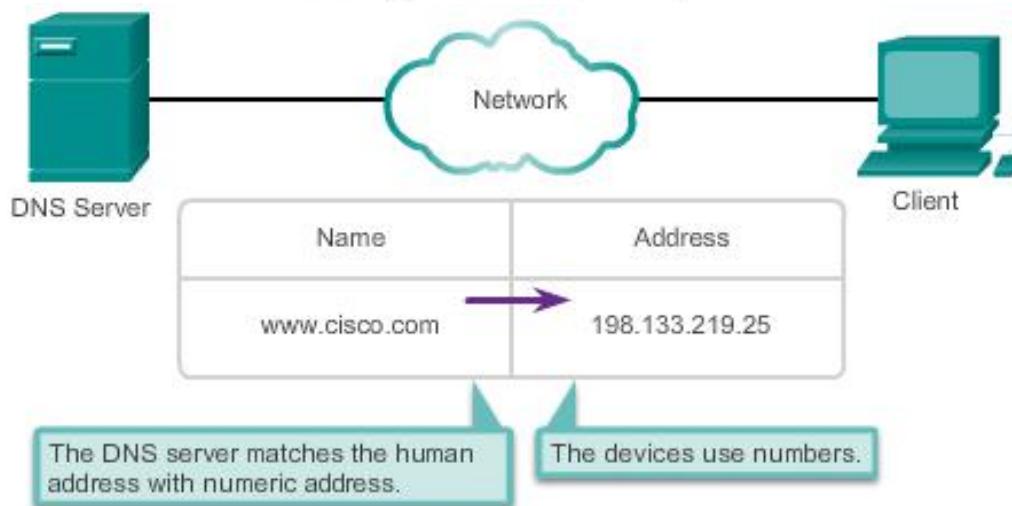
# Providing IP Addressing Services Domain Name Service

A human legible name is resolved to its numeric network device address by the DNS protocol.

Resolving DNS Addresses Step1



Resolving DNS Addresses Step2



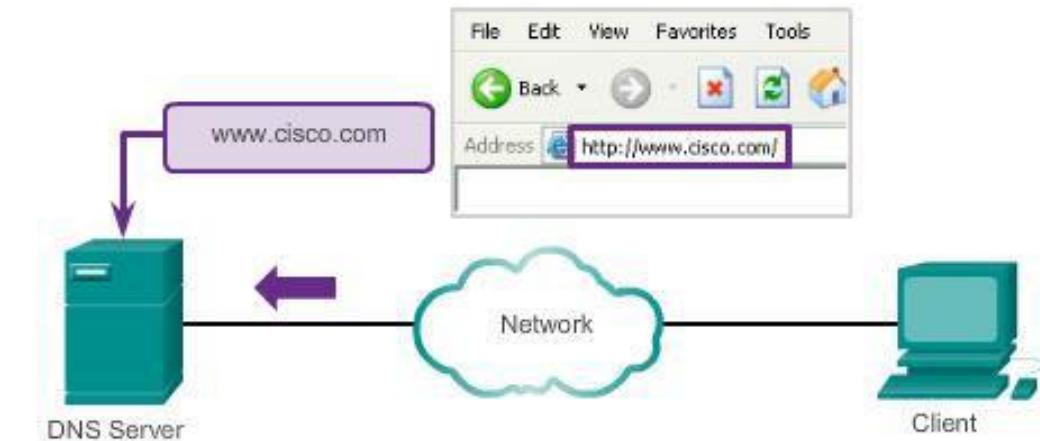


# Providing IP Addressing Services

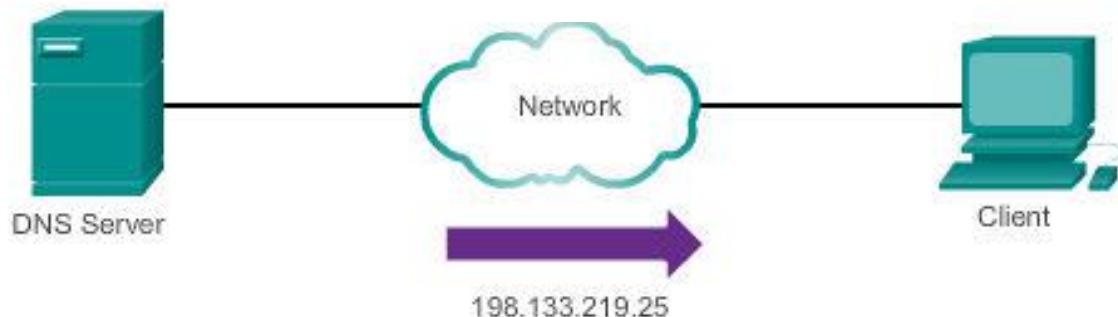
## Domain Name Service (cont.)

Resolving DNS Addresses Step3

A human legible name is resolved to its numeric network device address by the DNS protocol.



Resolving DNS Addresses Step4



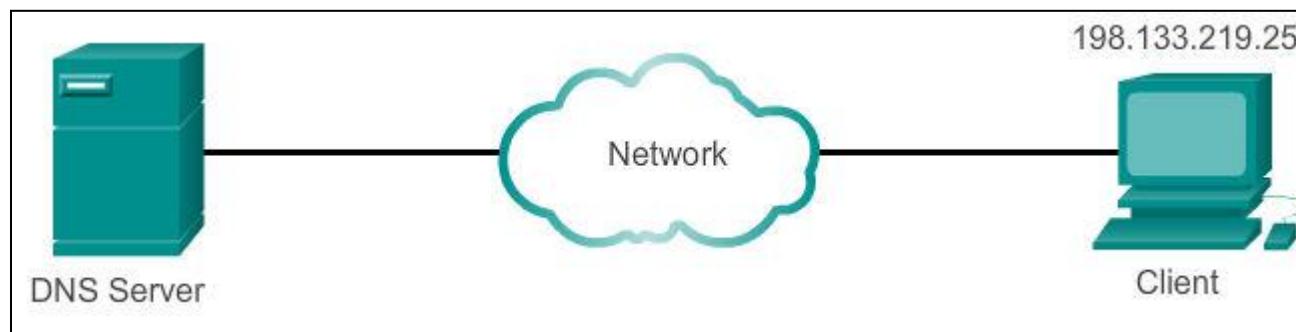
The number is returned back to the client for use in making requests of the server.



# Providing IP Addressing Services

## Domain Name Service (cont.)

Resolving DNS Addresses Step 5



A domain name is resolved to its numeric network device address by the DNS protocol.



# Providing IP Addressing Services

## DNS Message Format

- DNS server stores different types of resource records used to resolve names
- Contains the name, address, and type of record.
- Record types are:
  - **A** – An end device address
  - **NS** – An authoritative name server
  - **CNAME** – The canonical name for an alias; used when multiple services have the single network address, but each service has its own entry in DNS
  - **MX** – Mail exchange record; maps a domain name to a list of mail exchange servers
- Unable to resolve the name using its stored records, contacts other servers.
- Server temporarily stores the numbered address that matches the name in cache memory.
- Windows **ipconfig /displaydns** displays all cached DNS.



# Providing IP Addressing Services

## DNS Hierarchy

Examples top-level domains:

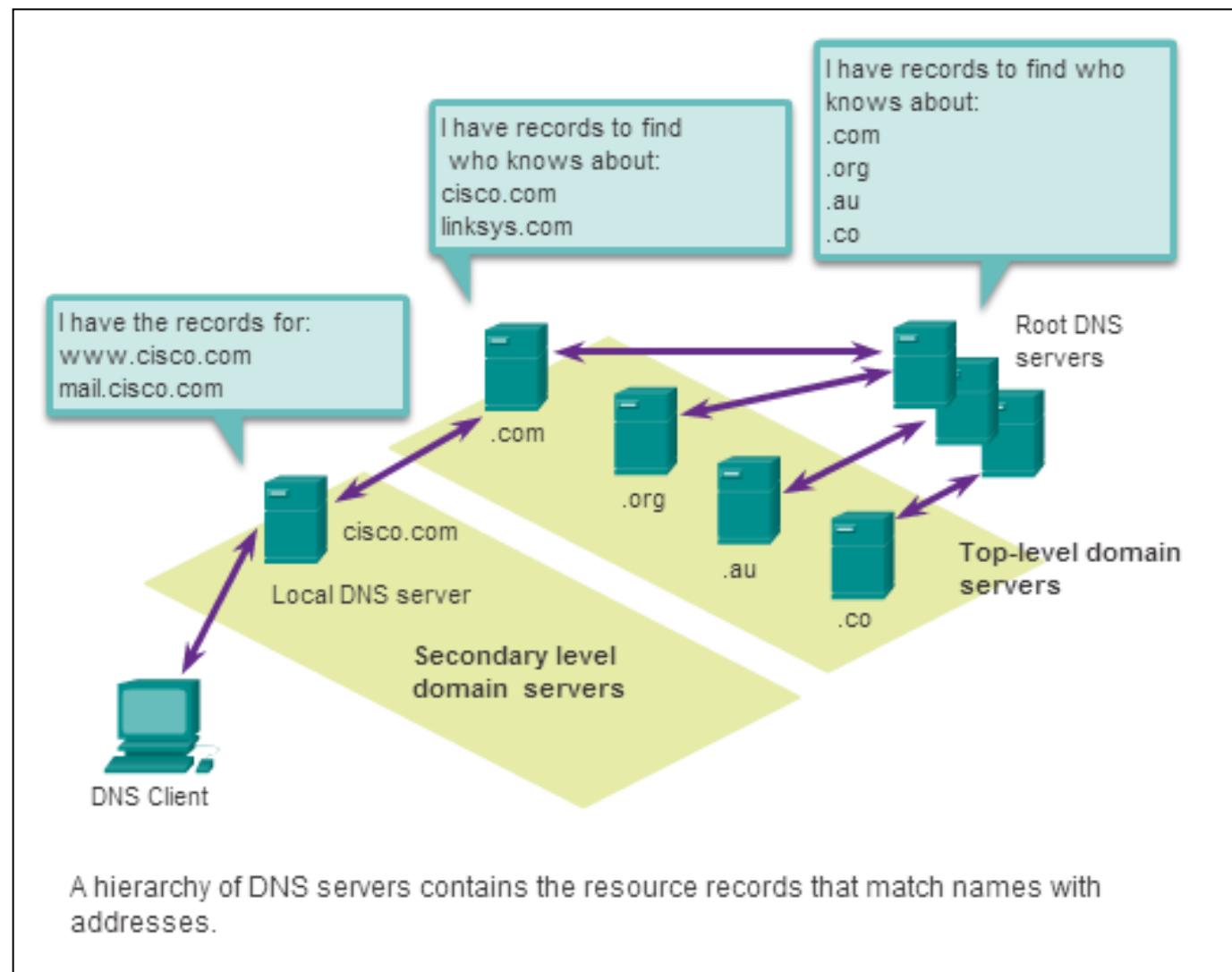
**.au** - Australia

**.co** - Colombia

**.com** - business or industry

**.jp** - Japan

**.org** - non-profit organization





## Providing IP Addressing Services nslookup

- Operating system utility called nslookup allows the user to manually query the name servers to resolve a given host name
- Utility can be used to troubleshoot name resolution issues and to verify the current status of the name servers

```
C:\Documents and Settings>nslookup
Default Server: dns-sj.cisco.com
Address: 171.78.168.183

> www.cisco.com
Server: dns-sj.cisco.com
Address: 171.78.168.183

Name: www.cisco.com
Address: 198.133.219.25

> cisco.netacad.net
Server: dns-sj.cisco.com
Address: 171.78.168.183

Non-authoritative answer:
Name: cisco.netacad.net
Address: 128.187.229.50

>
```



## Providing IP Addressing Services

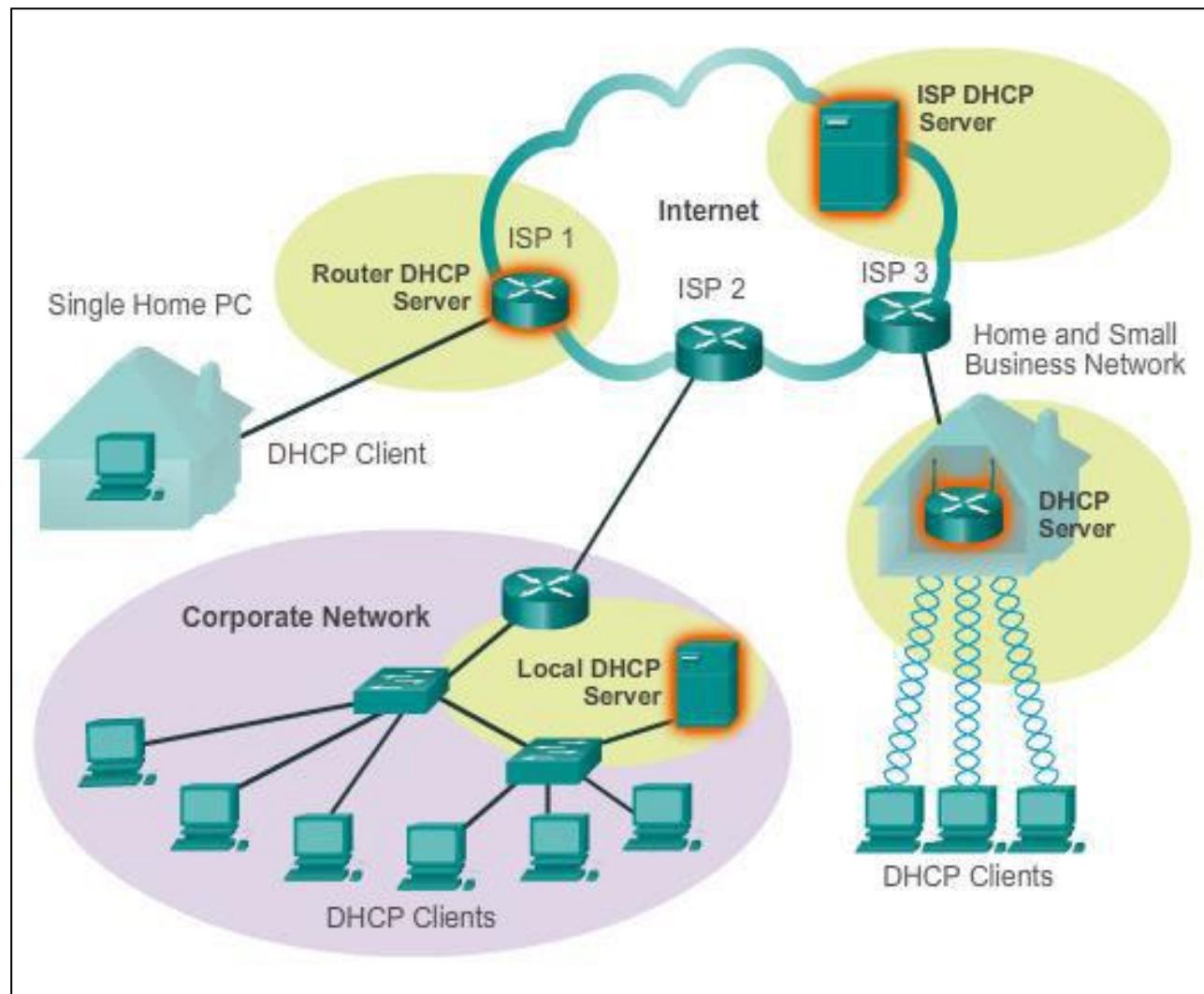
# Dynamic Host Configuration Protocol

- DHCP allows a host to obtain an IP address dynamically.
- DHCP server is contacted and address requested - chooses address from a configured range of addresses called a pool and “leases” it to the host for a set period.
- DHCP used for general purpose hosts such as end user devices, and static addressing is used for network devices such as gateways, switches, servers and printers.



# Providing IP Addressing Services

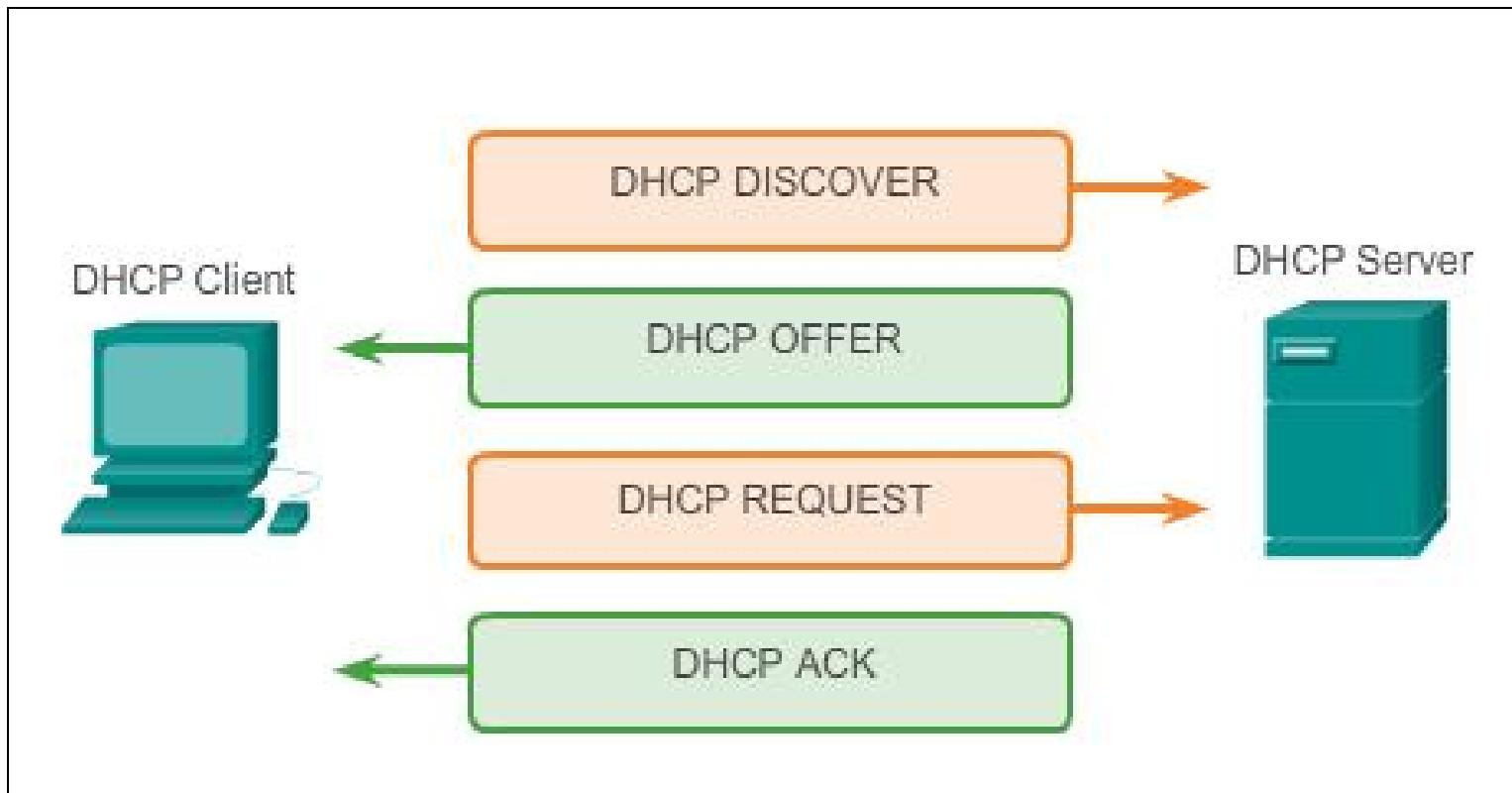
## Dynamic Host Configuration Protocol (cont.)





# Providing IP Addressing Services

## DHCP Operation





## Providing File Sharing Services

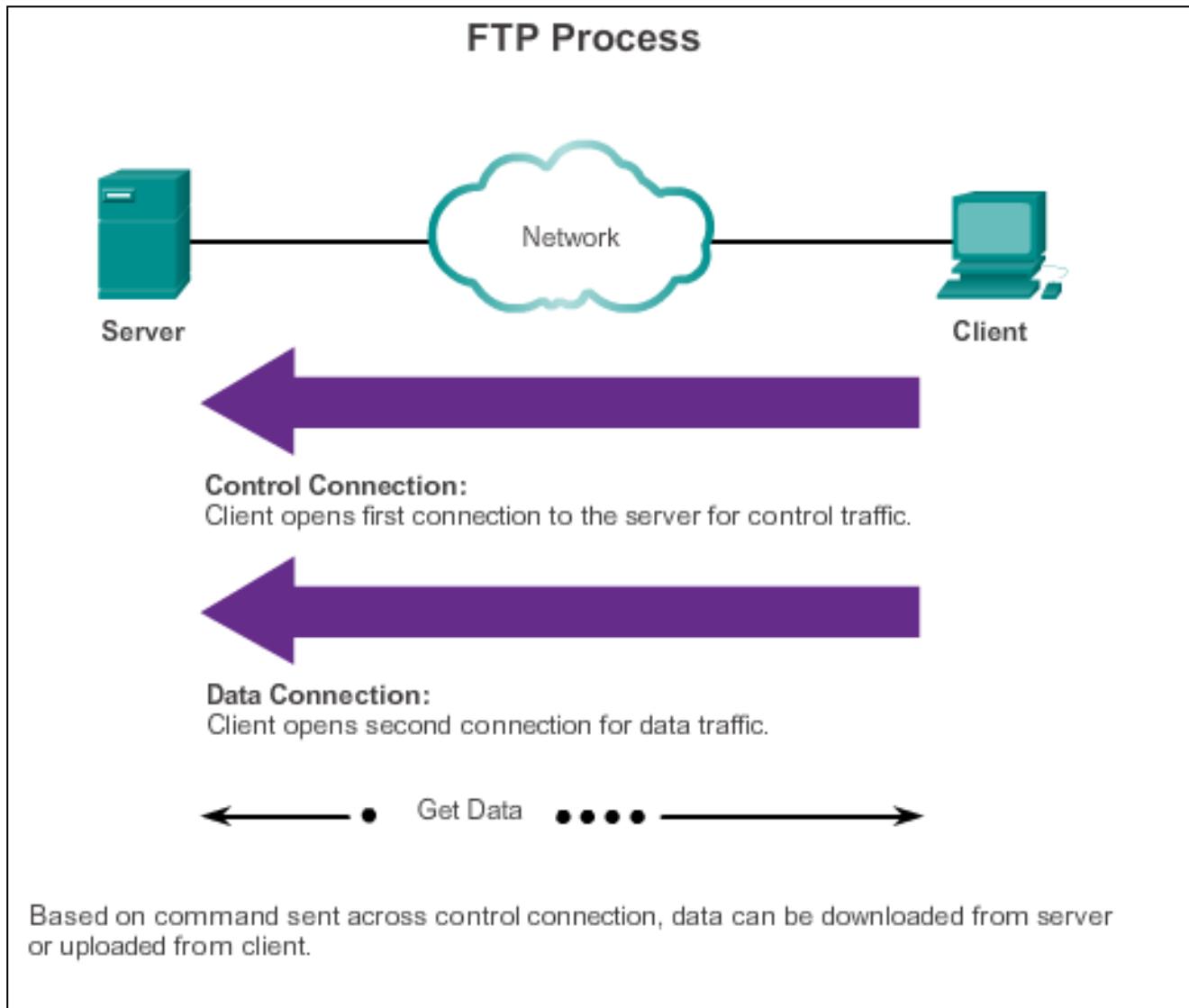
# File Transfer Protocol

- FTP allow data transfers between a client and a server.
- FTP client is an application that runs on a computer that is used to push and pull data from a server running an FTP daemon.
- To successfully transfer data, FTP requires two connections between the client and the server, one for commands and replies, the other for the actual file transfer.



# Providing File Sharing Services

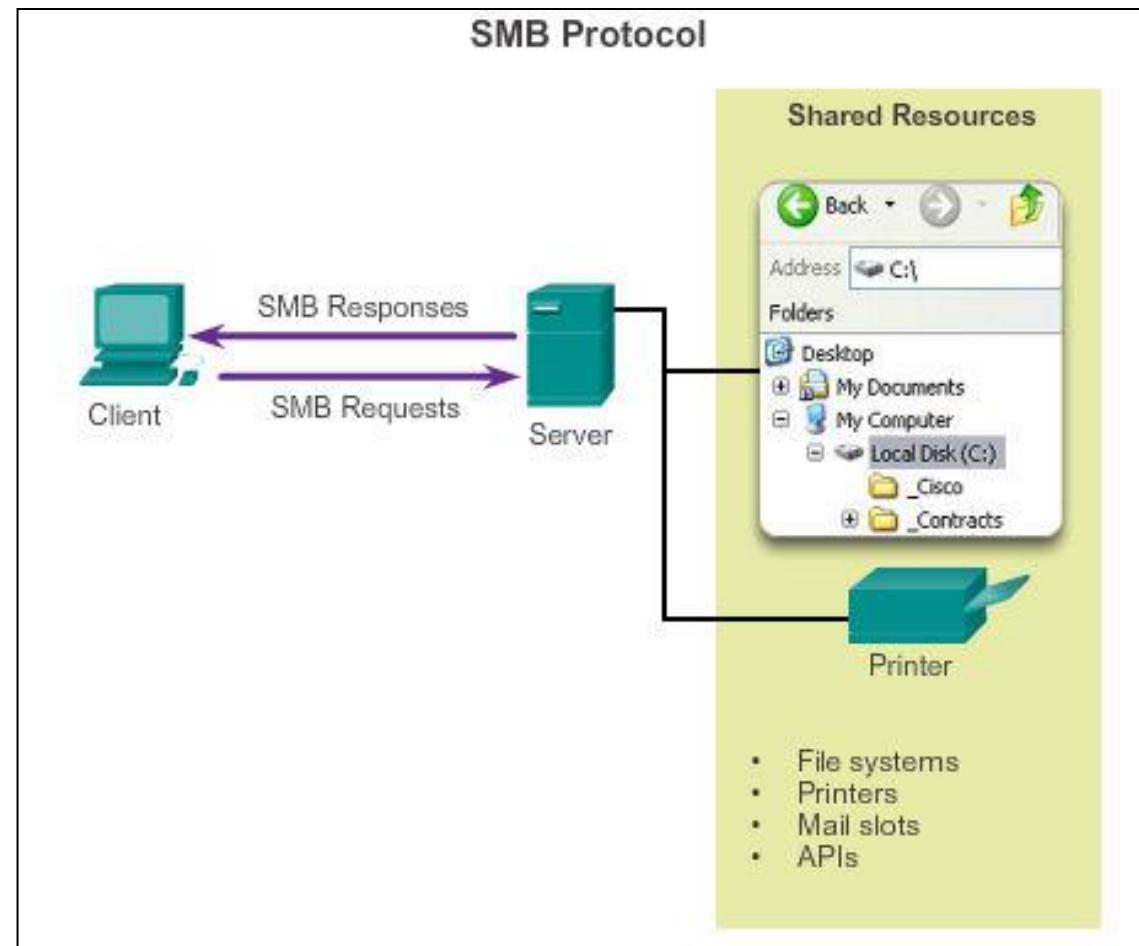
## File Transfer Protocol (cont.)





# Providing File Sharing Services Server Message Block

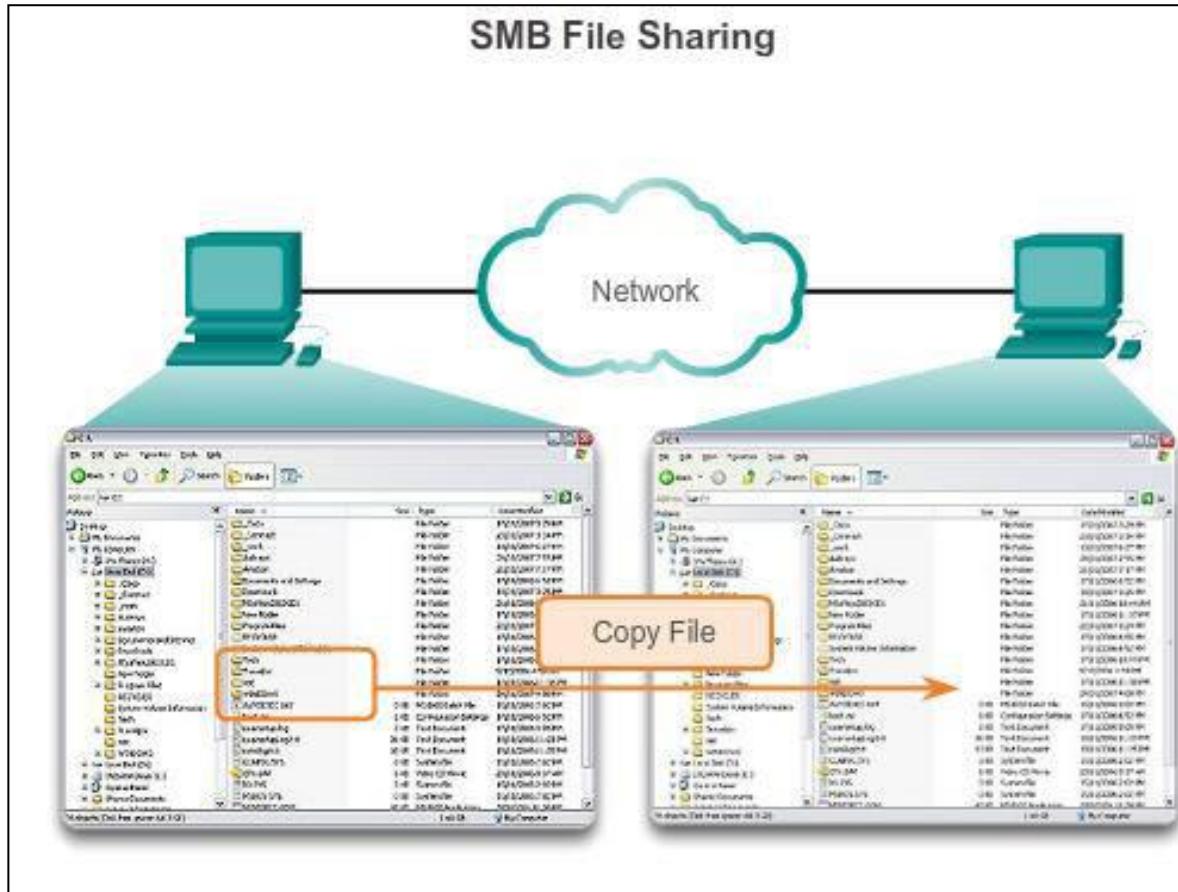
- Clients establish a long term connection to servers.
- After the connection is established, the user can access the resources on the server as if the resource is local to the client host.



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



# Providing File Sharing Services Server Message Block (cont.)



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

## 10.3 The Message Heard Around the World





Move It!

# The Internet of Things

**THE INTERNET OF EVERYTHING IS HERE.**

As the Internet evolves, so will we.

**37 billion new things will be connected by 2020.**



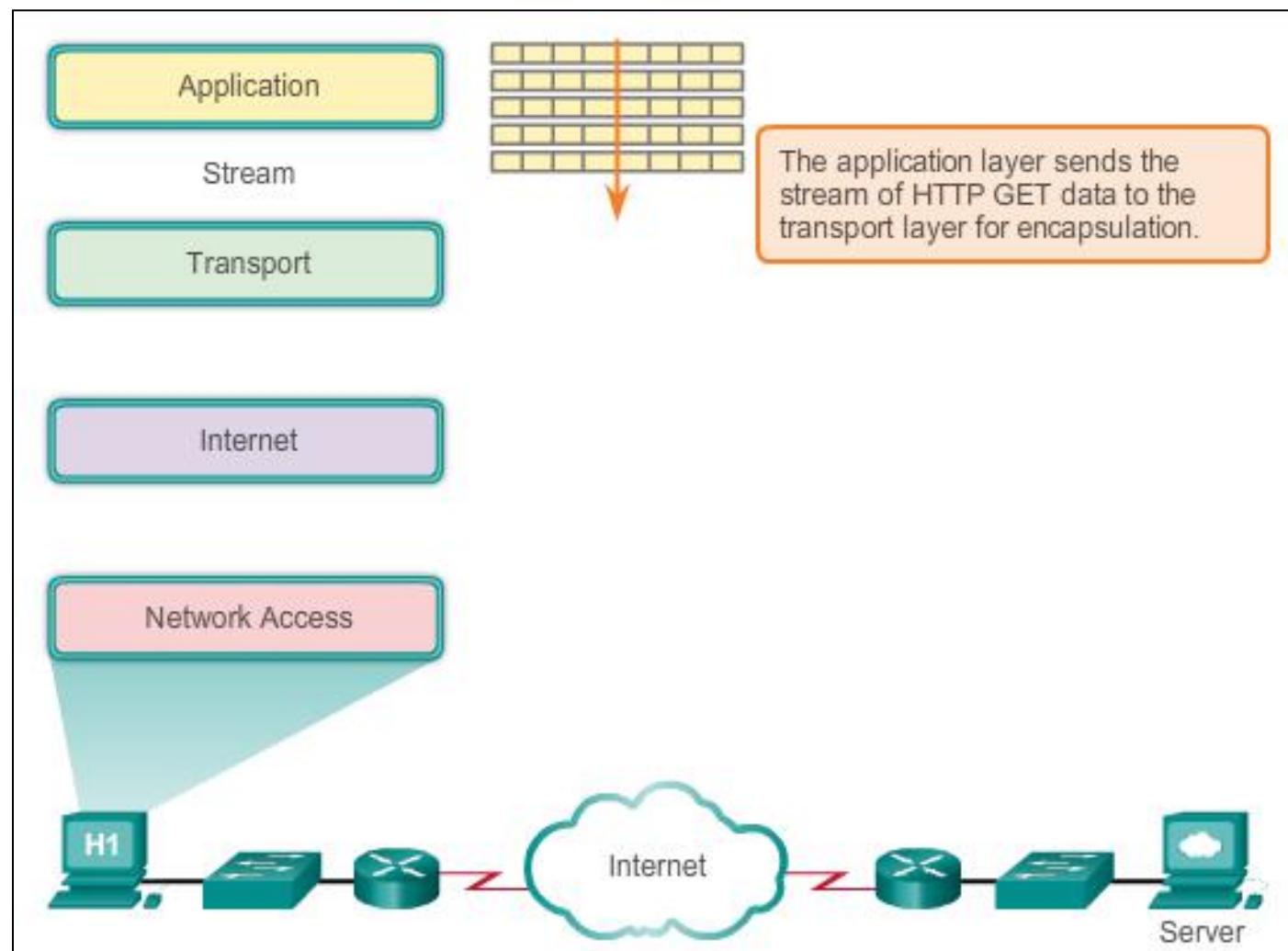
#IoE #TomorrowStartsHere

CISCO



Move It!

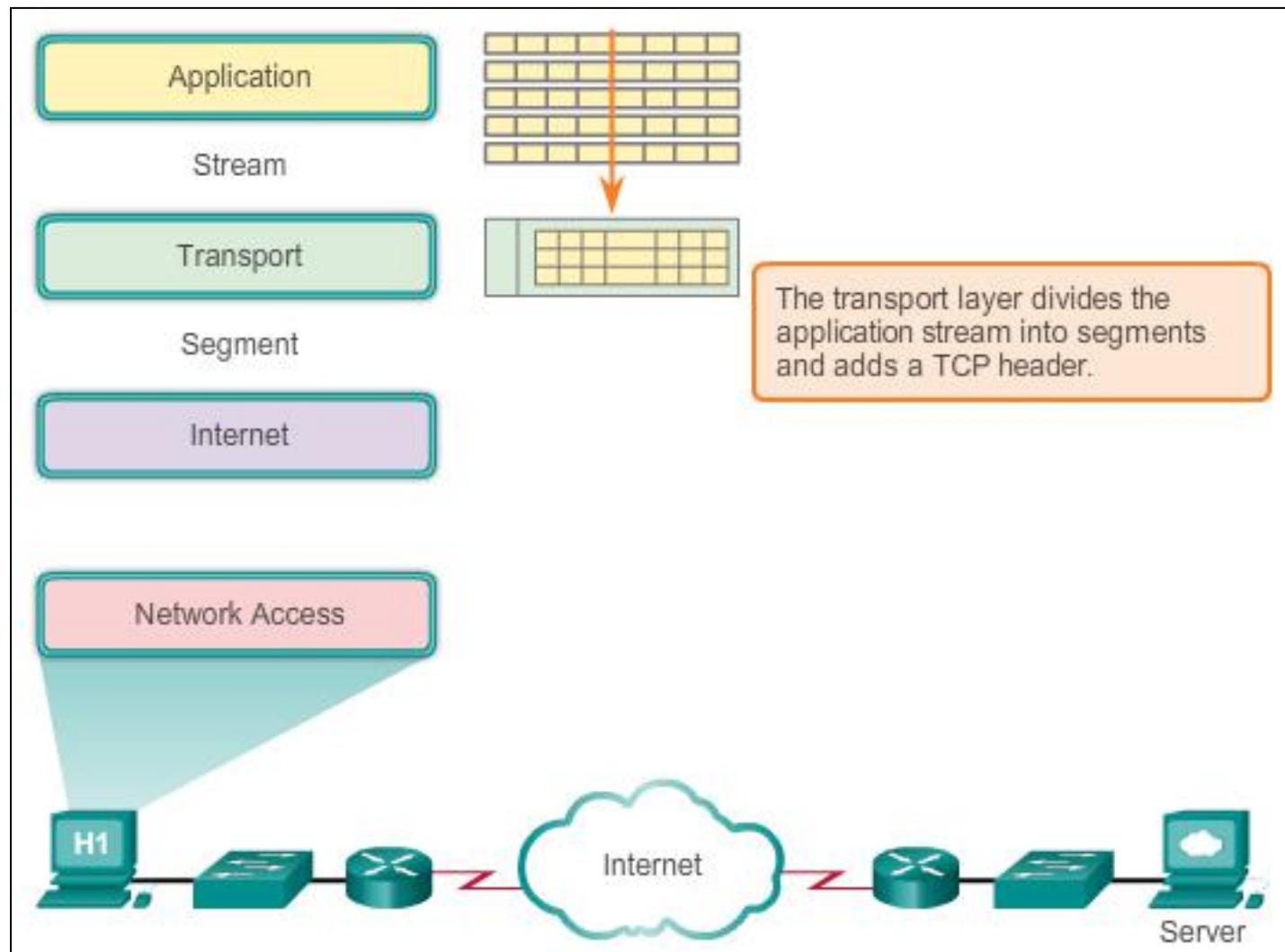
# Message Travels Through a Network





Move It!

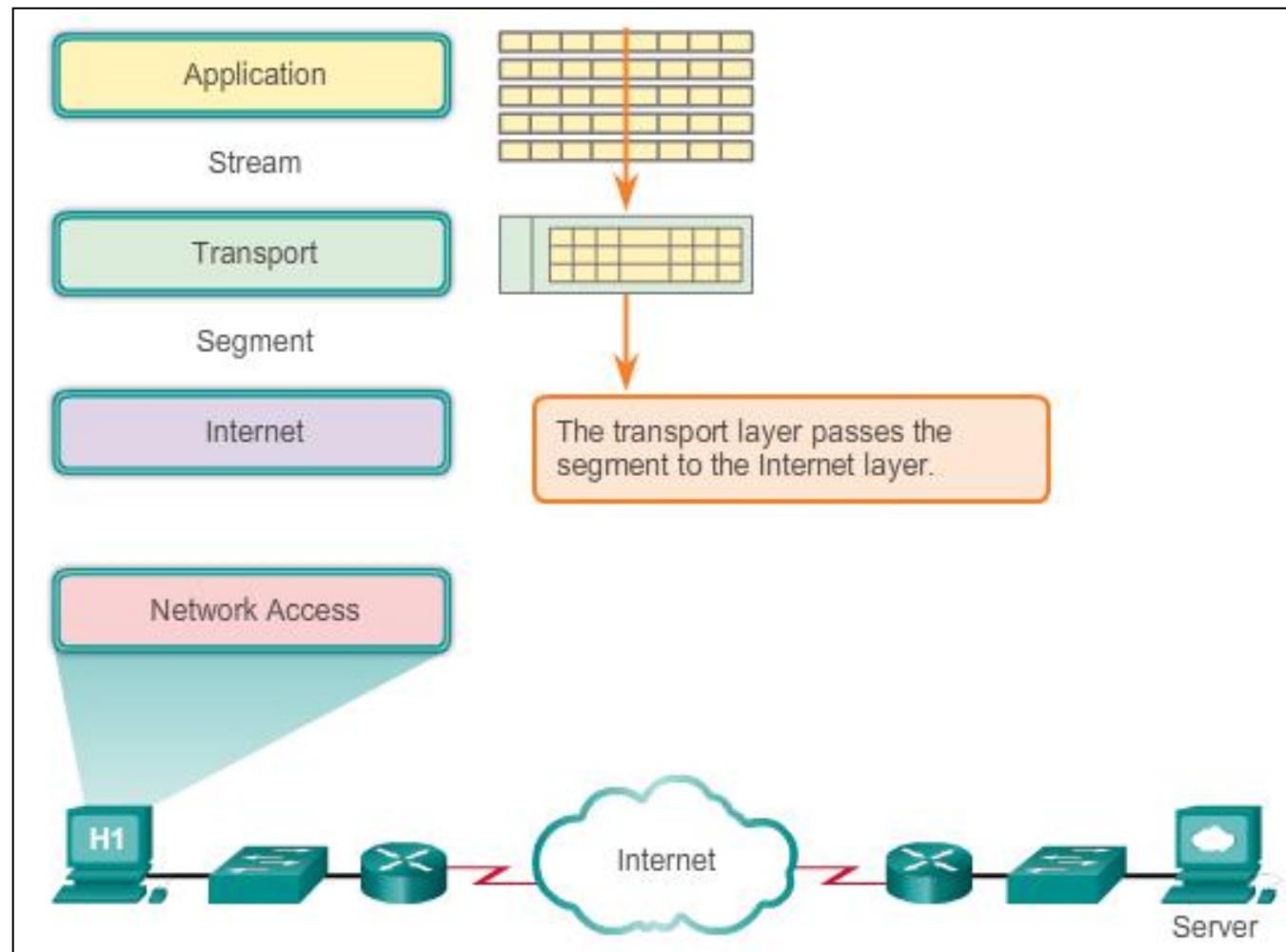
# Message Travels Through a Network (cont.)





Move It!

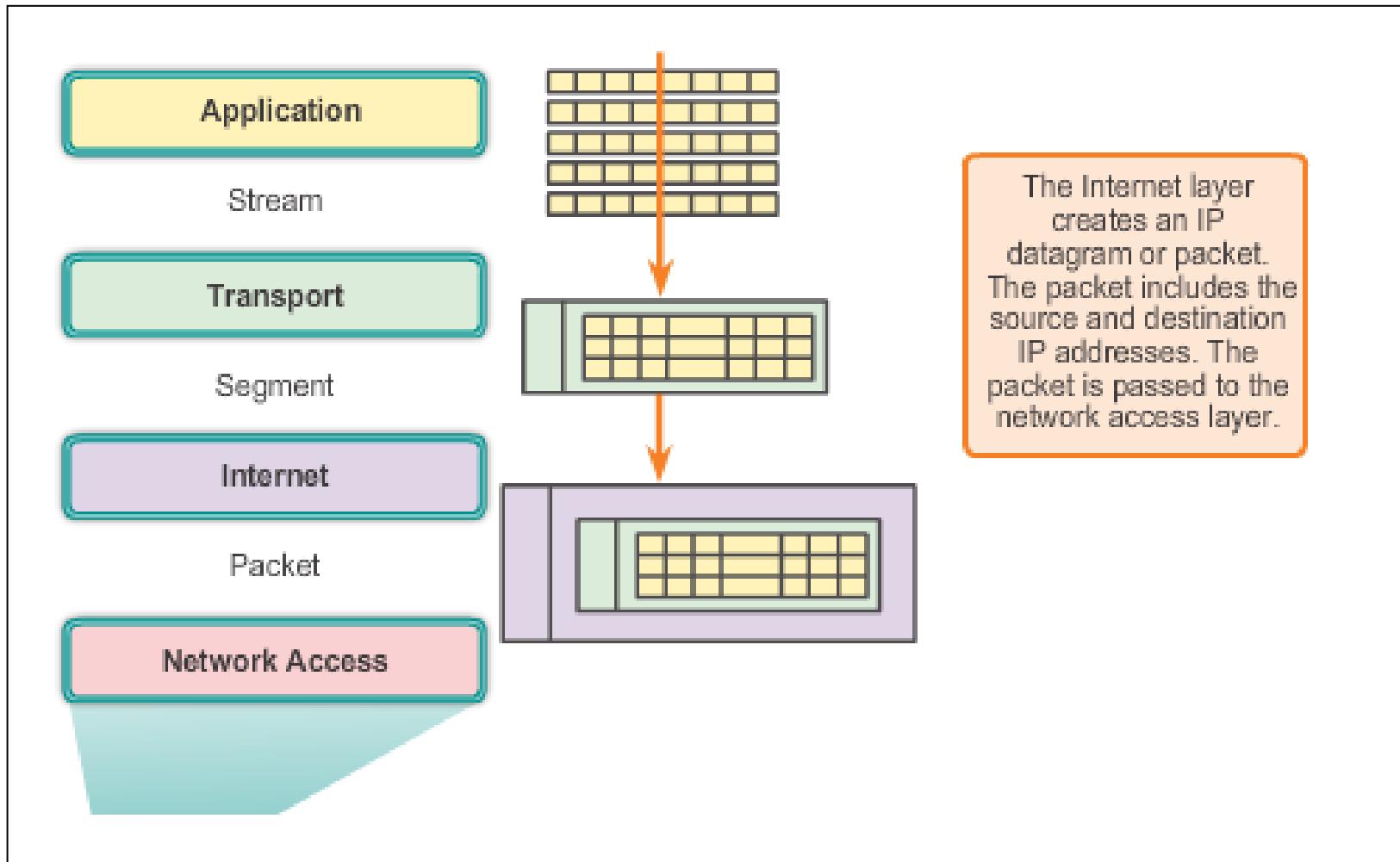
# Message Travels Through a Network (cont.)





Move It!

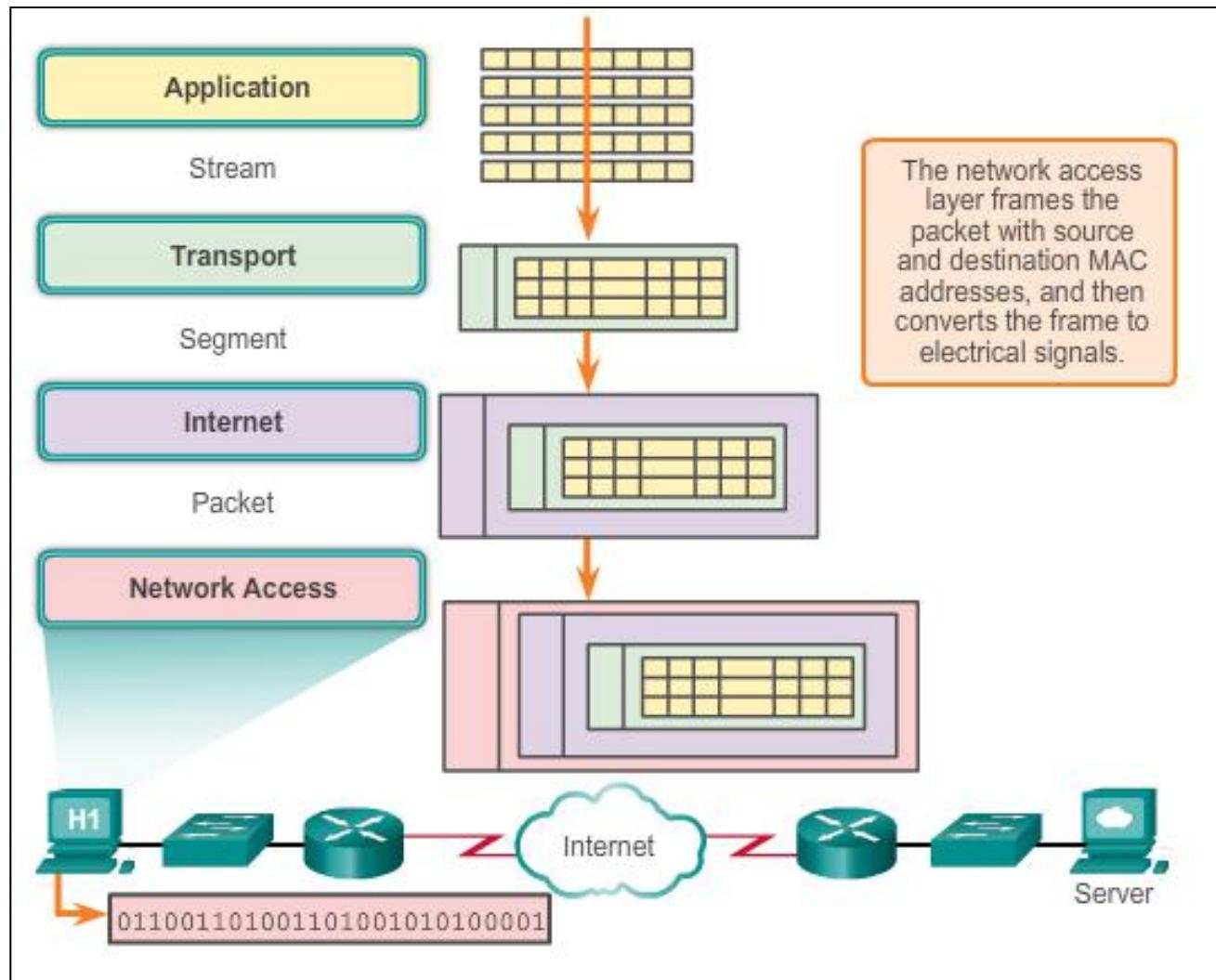
# Getting the Data to the End Device





Move It!

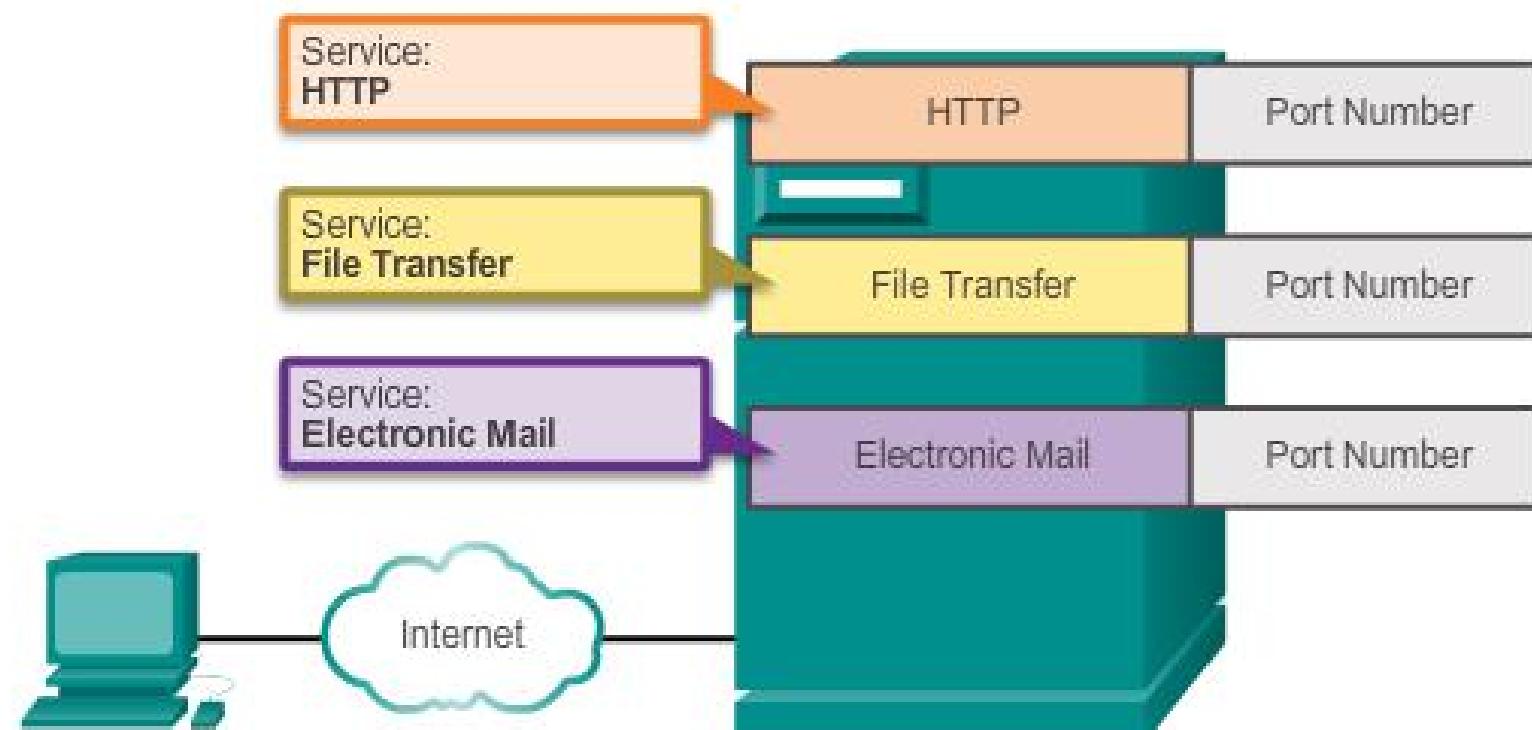
# Getting the Data through the Internet





Move It!

# Getting the Data to the Right Application



At the end device, the service port number directs the data to the correct conversation.



# Application Layer Summary

- Applications are computer programs with which the user interacts and which initiate the data transfer process at the user's request.
- Services are background programs that provide the connection between the application layer and the lower layers of the networking model.
- Protocols provide a structure of agreed-upon rules and processes that ensure services running on one particular device can send and receive data from a range of different network devices.
- HTTP supports the delivery of web pages to end devices.
- SMTP, POP, and IMAP support sending and receiving email.



# Application Layer Summary

- SMB and FTP enable users to share files.
- P2P applications make it easier for consumers to seamlessly share media.
- DNS resolves the human legible names used to refer to network resources into numeric addresses usable by the network
- All of these elements work together, at the application layer.
- The application layer enables users to work and play over the Internet.

# Cisco | Networking Academy®

Mind Wide Open™



## Chapter 11: It's a Network



## Introduction to Networking

Cisco | Networking Academy®  
Mind Wide Open™



# Chapter 11

11.0 Introduction

11.1 Create and Grow

11.2 Keeping the Network Safe

11.3 Basic Network Performance

11.4 Managing IOS Configuration Files

11.5 Integrated Routing Services

11.6 Summary



# Chapter 11: Objectives

Upon completion of this chapter, you will be able to:

- Identify the devices and protocols used in a small network.
- Explain how a small network serves as the basis of larger networks.
- Describe the need for basic security measures on network devices.
- Identify security vulnerabilities and general mitigation techniques.
- Configure network devices with device hardening features to mitigate security threats.
- Use the output of **ping** and **tracert** commands to establish relative network performance.
- Use basic **show** commands to verify the configuration and status of a device interface.



# Chapter 11: Objectives (Cont.)

- Use the basic host and IOS commands to acquire information about the devices in a network.
- Explain the file systems on Routers and Switches.
- Apply the commands to back up and restore an IOS configuration file.



## 11.1 Create and Grow



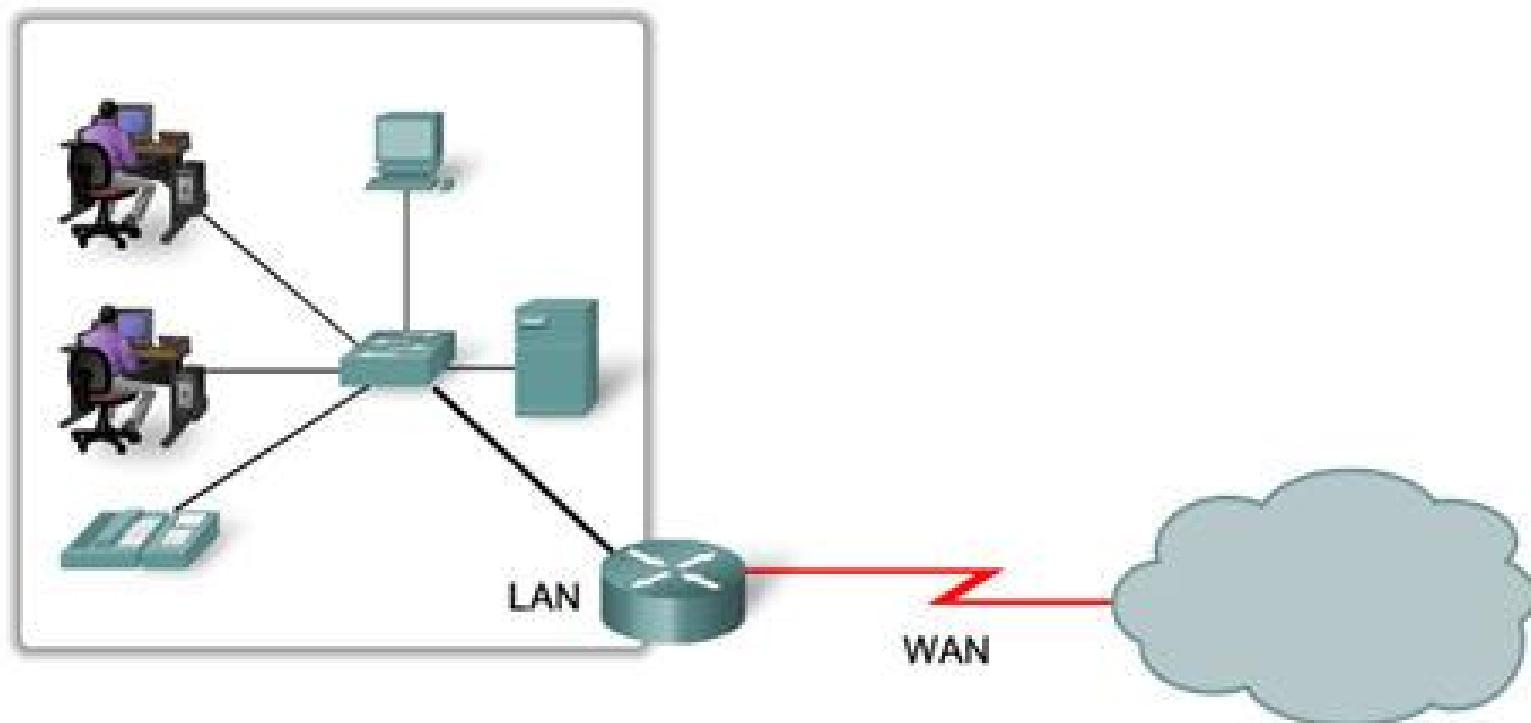
Cisco | Networking Academy®  
Mind Wide Open™



Devices in a Small Network

# Small Network Topologies

## Typical Small Network Topology





Devices in a Small Network

# Device Selection for a Small Network

Factors to be considered when selecting intermediate devices.



COST



PORTS



SPEED



EXPANDABLE/ MODULAR



MANAGEABLE



## Devices in a Small Network

# IP Addressing for a Small Network

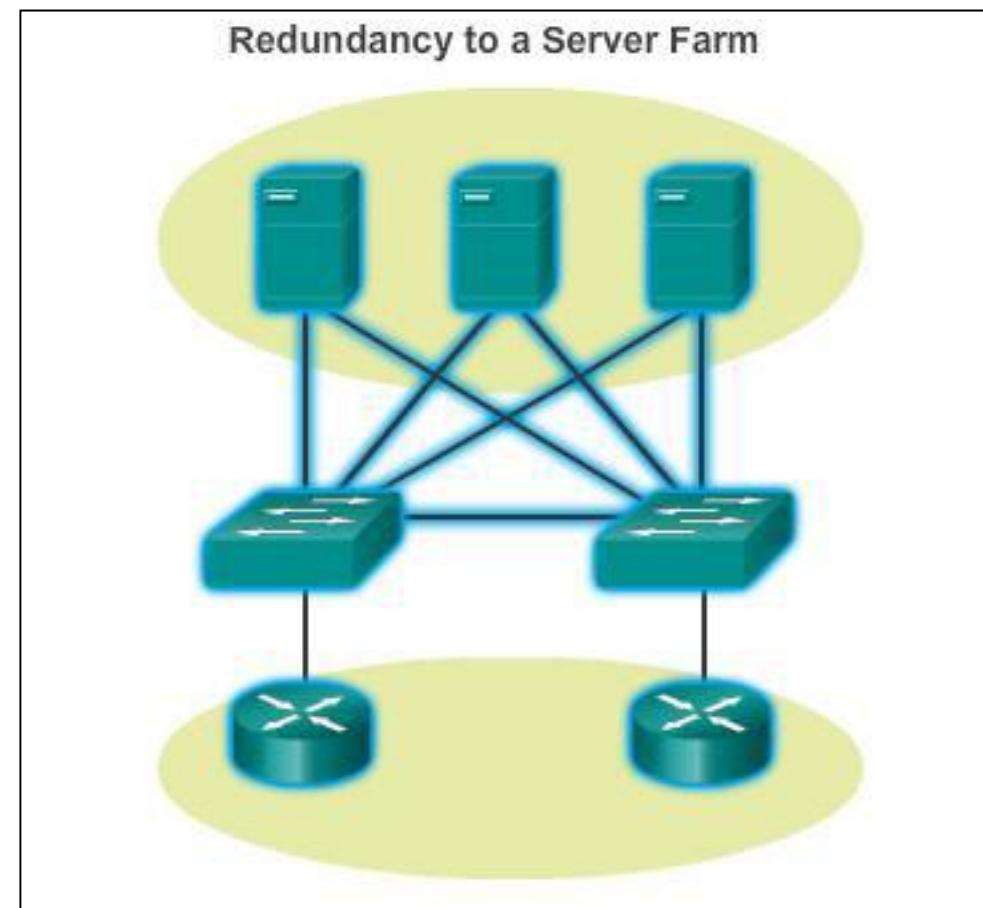
- IP addressing scheme should be planned, documented and maintained based on the type of devices receiving the address.
- Examples of devices that will be part of the IP design:
  - End devices for users
  - Servers and peripherals
  - Hosts that are accessible from the Internet
  - Intermediary devices
- Planned IP schemes help the administrator:
  - Track devices and troubleshoot
  - Control access to resources



## Devices in a Small Network

# Redundancy in a Small Network

- Redundancy helps to eliminate single points of failure.
- Improves the reliability of the network.

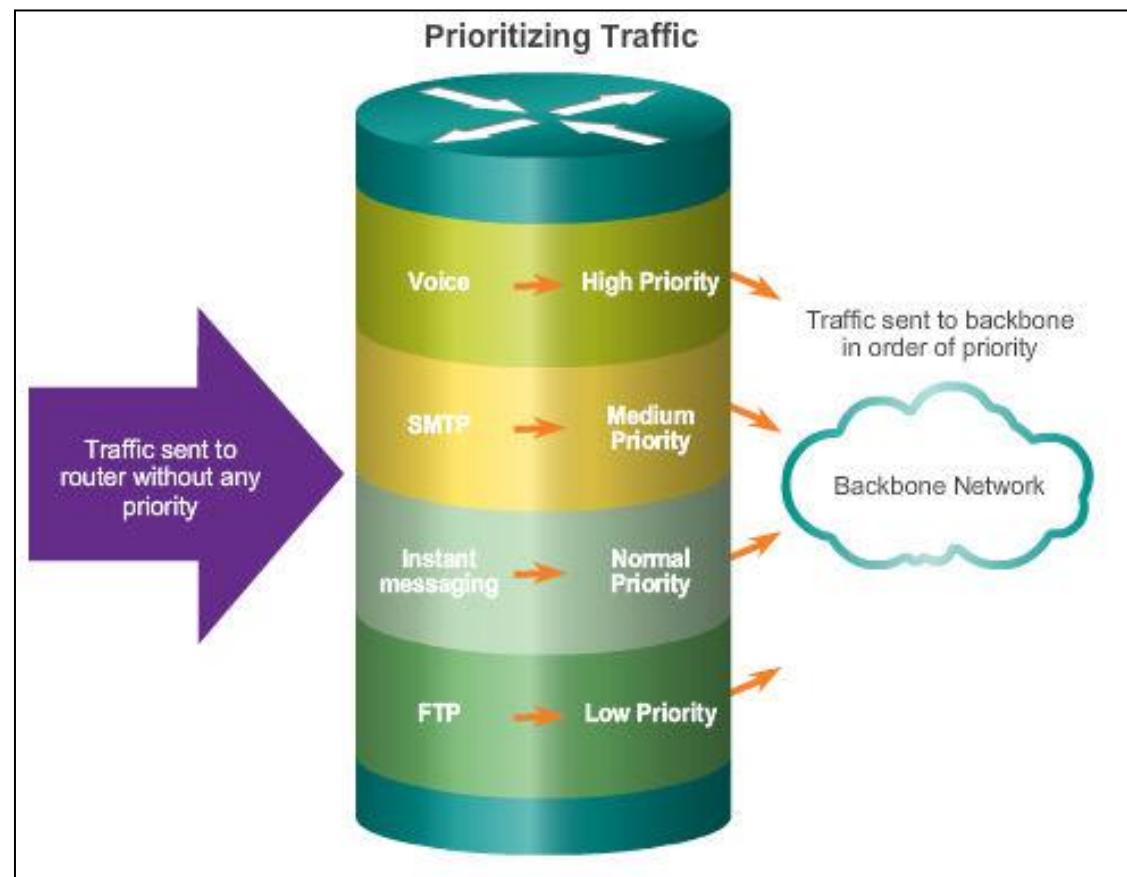




## Devices in a Small Network

# Design Considerations for a Small Network

- The following should be included in the network design:
  - Secure file and mail servers in a centralized location.
  - Protect the location by physical and logical security measures.
  - Create redundancy in the server farm.
  - Configure redundant paths to the servers.





## Protocols in a Small Network

# Common Applications in a Small Network

**Network-Aware Applications** – Software programs that are used to communicate over the network.

**Application Layer Services** – Programs that interface with the network and prepare the data for transfer.



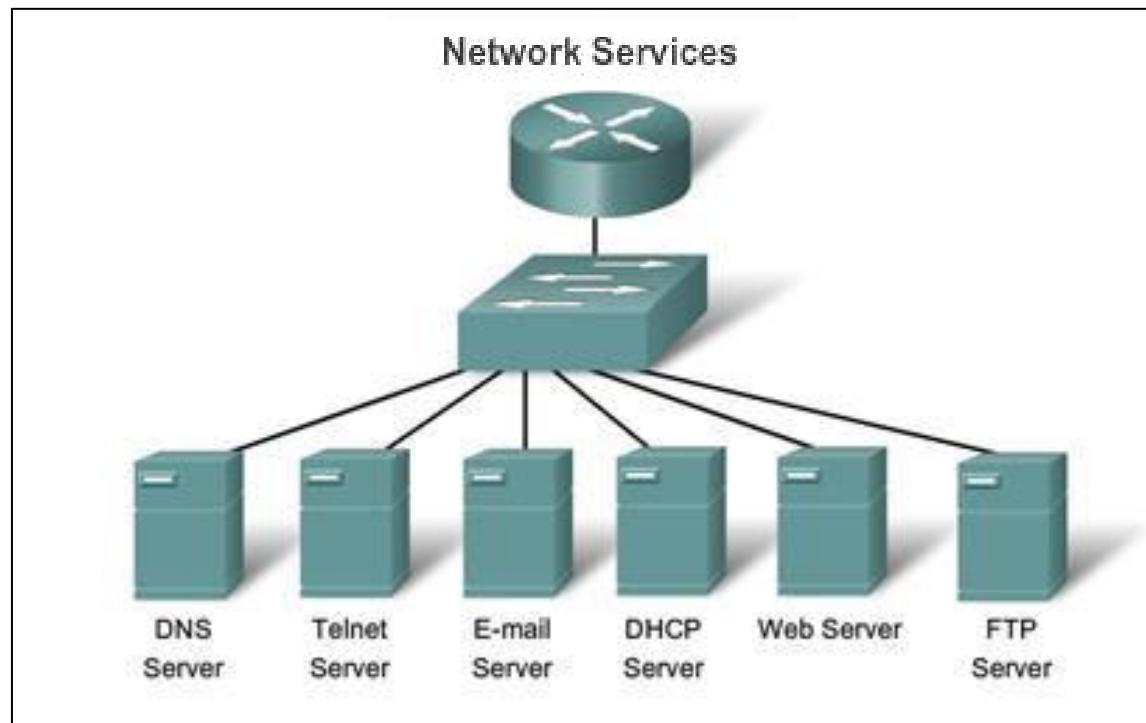
## Protocols in a Small Network

# Common Protocols in a Small Network

### Network Protocols

#### Define:

- Processes on either end of a communication session.
- Types of messages.
- Syntax of the messages.
- Meaning of informational fields.
- How messages are sent and the expected response.
- Interaction with the next lower layer.





## Protocols in a Small Network

# Real-Time Applications for a Small Network

Real-time applications require planning and dedicated services to ensure priority delivery of voice and video traffic.

- **Infrastructure** – Needs to be evaluated to ensure it will support proposed real time applications.
- **VoIP** – Is implemented in organizations that still use traditional telephones.
- **IP telephony** – The IP phone itself performs voice-to-IP conversion.
- **Real-time Video Protocols** – Use Time Transport Protocol (RTP) and Real-Time Transport Control Protocol (RTCP).



## Growing to Larger Networks

# Scaling a Small Network

**Important considerations when growing to a larger network:**

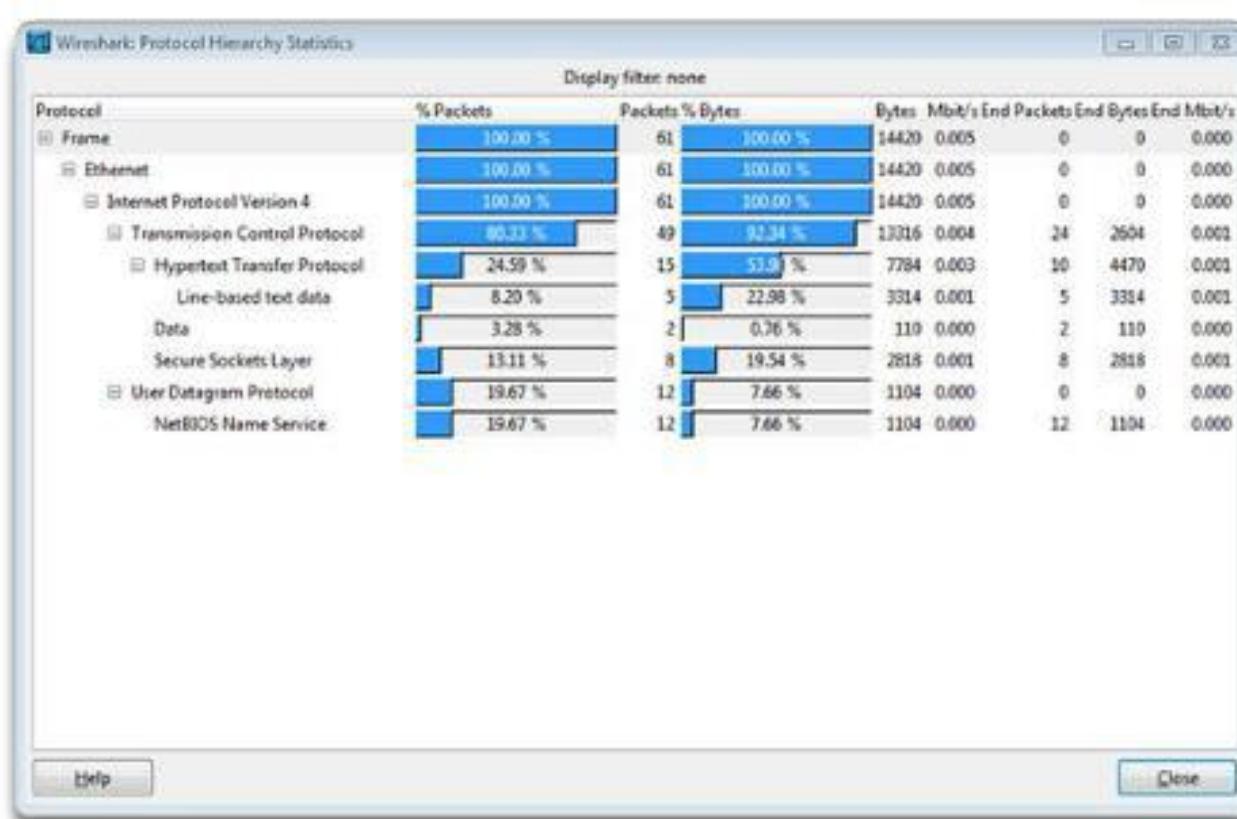
- **Documentation** –Physical and logical topology.
- **Device inventory** – List of devices that use or comprise the network.
- **Budget** – Itemized IT expense items, including the amount of money allocated to equipment purchase for that fiscal year.
- **Traffic Analysis** – Protocols, applications, and services and their respective traffic requirements should be documented.



## Growing to Larger Networks

# Protocol Analysis of a Small Network

Information gathered by protocol analysis can be used to make decisions on how to manage traffic more efficiently.





# Growing to Larger Networks

# Evolving Protocol Requirements

- Network administrator can obtain IT “snapshots” of employee application utilization.
- Snapshots track network utilization and traffic flow requirements.
- Snapshots help inform network modifications needed.

**Software Processes**

**Windows Task Manager**

File Options View Help

Applications Processes Performance Networking

Image Name	User Name	CPU	Mem Usage
Apoint.exe	frances	00	5,288 K
method.exe	frances	00	1,920 K
<b>EXCEL.EXE</b>	frances	00	2,011 K
WindowsCAL.exe	frances	00	4,244 K
DSentry.exe	frances	00	1,940 K
Directx.exe	frances	00	5,540 K
wfmgr.exe	LOCAL SERVICE	00	1,716 K
svchost.exe	LOCAL SERVICE	00	4,384 K
alg.exe	LOCAL SERVICE	00	3,512 K
scardvr.exe	LOCAL SERVICE	00	2,564 K
svchost.exe	NETWORK SERVICE	00	3,744 K
svchost.exe	NETWORK SERVICE	00	4,440 K
medit.exe	NETWORK SERVICE	00	4,852 K
System Idle Process	SYSTEM	96	16 K
System	SYSTEM	00	224 K
svchost.exe	SYSTEM	00	5,152 K
ViewpointService....	SYSTEM	00	2,208 K
WLTRYSVIC.EXE	SYSTEM	00	1,368 K
W7CRV.S.exe	SYSTEM	00	1,002 K

Show processes from all users

End Process

Processes: 64 CPU Usage: 4% Commit Charge: 507M / 2461M

Processes are individual software programs running concurrently.

Processes can be:

- 1 Applications
- 2 Services
- 3 System operations
- 4 One program may be running several times, each in its own process.

## 11.2 Keeping the Network Safe





# Network Device Security Measures

# Threats to Network Security

## Categories of Threats to Network Security



Information Theft



Data Loss and Manipulation



Identity Theft



Disruption of Service



## Network Device Security Measures

# Physical Security

**Four classes of physical threats are:**

- **Hardware threats** – Physical damage to servers, routers, switches, cabling plant, and workstations
- **Environmental threats** – Temperature extremes (too hot or too cold) or humidity extremes (too wet or too dry)
- **Electrical threats** – Voltage spikes, insufficient supply voltage (brownouts), unconditioned power (noise), and total power loss
- **Maintenance threats** – Poor handling of key electrical components (electrostatic discharge), lack of critical spare parts, poor cabling, and poor labeling



## Network Device Security Measures

# Types of Security Vulnerabilities

### Vulnerabilities - Technology

#### Types of Security Weaknesses:

- Technological
- Configuration
- Security policy

#### Network security weaknesses:

##### TCP/IP protocol weakness

- Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP) and Internet Control Message Protocol (ICMP) are inherently insecure.
- Simple Network Management Protocol (SNMP) and Simple Mail Transfer Protocol (SMTP) are related to the inherently insecure structure upon which TCP was designed.

##### Operating system weakness

- Each operating system has security problems that must be addressed.
- UNIX, Linux, Mac OS, Mac OS X, Windows Server 2012, Windows 7, Windows 8
- They are documented in the Computer Emergency Response Team (CERT) archives at <http://www.cert.org>.

##### Network equipment weakness

Various types of network equipment, such as routers, firewalls, and switches have security weaknesses that must be recognized and protected against. Their weaknesses include password protection, lack of authentication, routing protocols, and firewall holes.



## Vulnerabilities and Network Attacks

# Viruses, Worms and Trojan Horses

- **Virus** – Malicious software that is attached to another program to execute a particular unwanted function on a workstation.
- **Trojan horse** – An entire application written to look like something else, when in fact it is an attack tool.
- **Worms** – Worms are self-contained programs that attack a system and try to exploit a specific vulnerability in the target. The worm copies its program from the attacking host to the newly exploited system to begin the cycle again.



# Vulnerabilities and Network Attacks

## Reconnaissance Attacks

### Reconnaissance Attacks



Internet queries



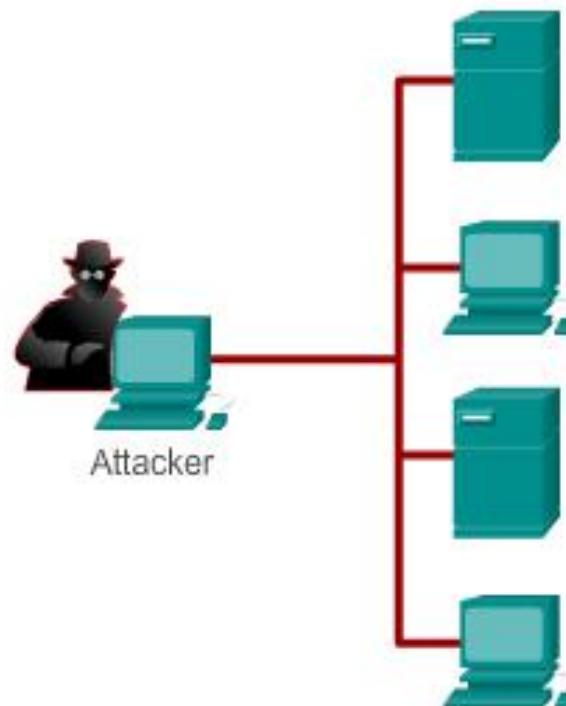
Ping sweeps



Port scans



Packet sniffers





# Vulnerabilities and Network Attacks

## Access Attacks

### Password Attack

Attackers can implement password attacks using several different methods:

- Brute-force attacks
- Trojan horse programs
- Packet sniffers



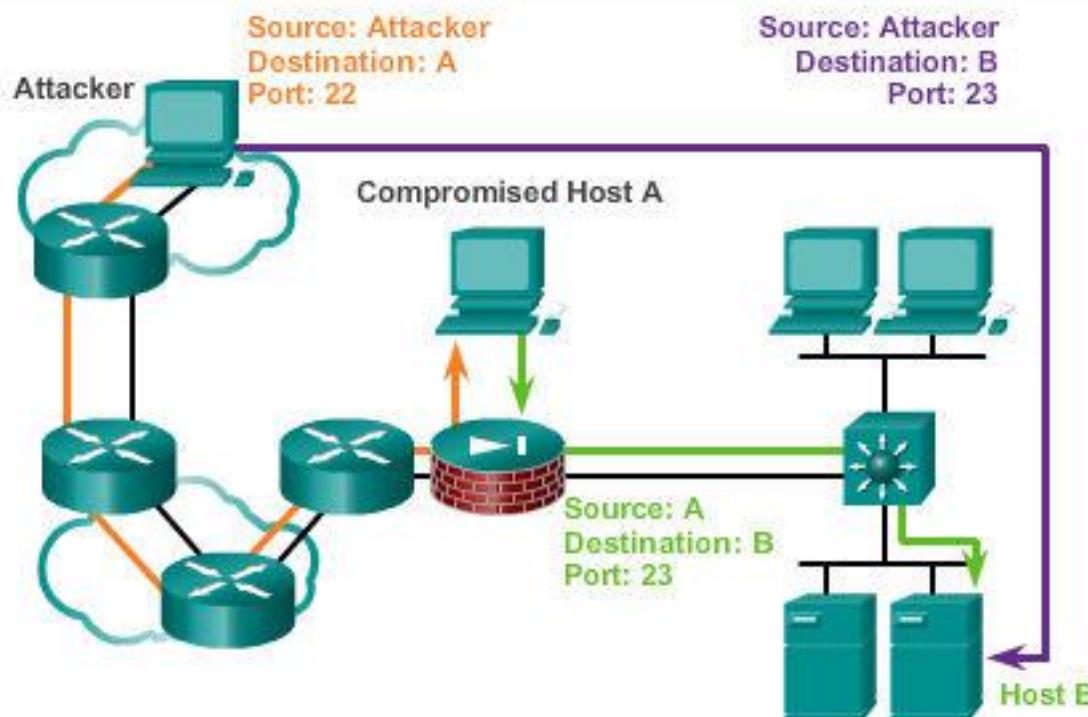


# Vulnerabilities and Network Attacks

## Access Attacks (Cont.)

### Port Redirection

Port redirection is a type of trust-exploitation attack that uses a compromised host to pass traffic through a firewall that would otherwise be dropped. It is mitigated primarily through the use of proper trust models. Antivirus software and host-based IDS can help detect and prevent an attacker installing port redirecting utilities on the host.



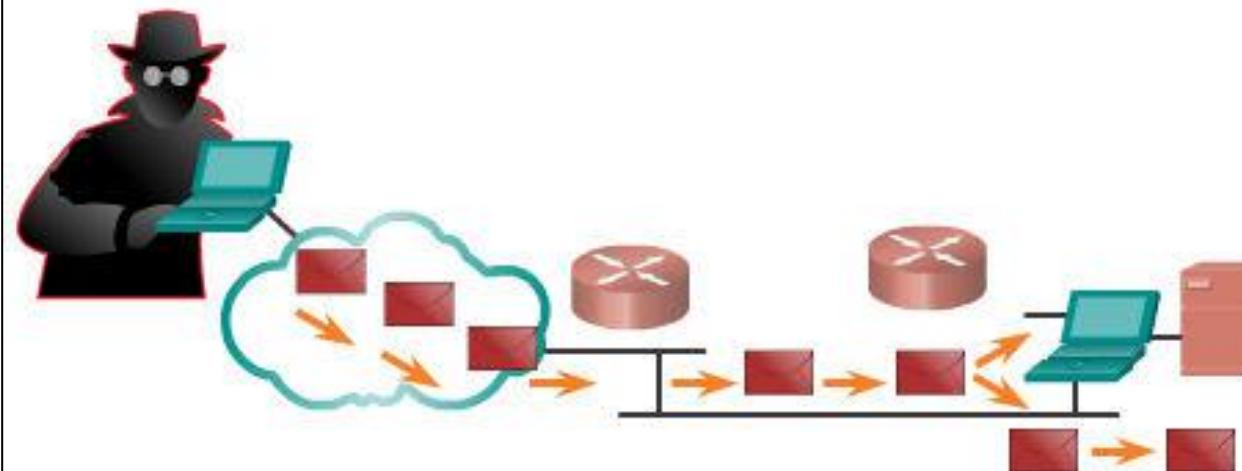


## Vulnerabilities and Network Attacks

# Denial of Service Attacks (DoS)

### DoS Attack

Resource overloads	Malformed data
Disk space, bandwidth, buffers	Oversized packets such as ping of death
Ping floods such as smurf	Overlapping packet such as winuke
Packet storms such as UDP bombs and fraggle	Unhandled data such as teardrop



DoS attacks prevent authorized people from using a service by using up system resources.



## Mitigating Network Attacks

# Backup, Upgrade, Update, and Patch

Antivirus software can detect most viruses and many Trojan horse applications and prevent them from spreading in the network.

- Keep current with the latest versions of antivirus software.
- Install updated security patches.





## Mitigating Network Attacks

# Authentication, Authorization, and Accounting

### Authentication, Authorization, and Accounting (AAA, or “triple A”)

- **Authentication** – Users and administrators must prove their identity. Authentication can be established using username and password combinations, challenge and response questions, token cards, and other methods.
- **Authorization** – Determines which resources the user can access and the operations that the user is allowed to perform.
- **Accounting** – Records what the user accessed, the amount of time the resource is accessed, and any changes made.



# Mitigating Network Attacks

## Firewalls

A Firewall resides between two or more networks. It controls traffic and helps prevent unauthorized access.

Methods used are:

- Packet Filtering
- Application Filtering
- URL Filtering
- Stateful Packet Inspection (SPI) – Incoming packets must be legitimate responses to requests from internal hosts.

### Firewalls



Cisco Security Appliances



Server-Based Firewall



Linksys Wireless Router with Integrated Firewall



Personal Firewall



# Mitigating Network Attacks

## Endpoint Security

- Common endpoints are laptops, desktops, servers, smart phones, and tablets.
- Employees must follow the companies documented security policies to secure their devices.
- Policies often include the use of anti-virus software and host intrusion prevention.

**Common Endpoint Devices**





## Securing Devices

# Introduction to Securing Devices

- Part of network security is securing devices, including end devices and intermediate devices.
- Default usernames and passwords should be changed immediately.
- Access to system resources should be restricted to only the individuals that are authorized to use those resources.
- Any unnecessary services and applications should be turned off and uninstalled, when possible.
- Update with security patches as they become available.



# Securing Devices Passwords

## Weak and Strong Passwords

Weak Password	Why it is weak
secret	Simple dictionary password
smith	Mother's maiden name
toyota	Make of car
bob1967	Name and birthday of user
Blueleaf23	Simple words and numbers

Strong Password	Why it is strong
b67n42d39c	Combines alphanumeric characters
12^h u4@1p7	Combines alphanumeric characters, symbols and also includes a space



# Securing Devices

## Basic Security Practices

- Encrypt passwords.
- Require minimum length passwords.
- Block brute force attacks.
- Use Banner Message.
- Set EXEC timeout.

### Securing Devices

```
Router(config)#service password-encryption
Router(config)#security password min-length 8
Router(config)#login block-for 120 attempts 3 within 60
Router(config)#line vty 0 4
Router(config-vty)#exec-timeout 10
Router(config-vty)#end
Router#show running-config
-more-
!
line vty 0 4
password 7 03095A0F034F38435B49150A1819
exec-timeout 10
login
```



# Securing Devices Enable SSH

The diagram shows two routers, R1 and R2, connected via their S0/0/0 ports. Router R1 has its Fa0/0 port connected to an unlabeled interface. Router R2 has its Fa0/1 port connected to an unlabeled interface. The connection between the S0/0/0 ports is labeled "DCE".

```
R1# conf t
R1(config)# ip domain-name span.com
R1(config)# crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.span.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R1(config)#
*Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)# username Bob secret cisco
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exit
```

Step 1: Configure the IP domain name.  
Step 2: Generate one-way secret keys.  
Step 3: Verify or create a local database entry.  
Step 4: Enable VTY inbound SSH sessions.

## 11.3 Basic Network Performance

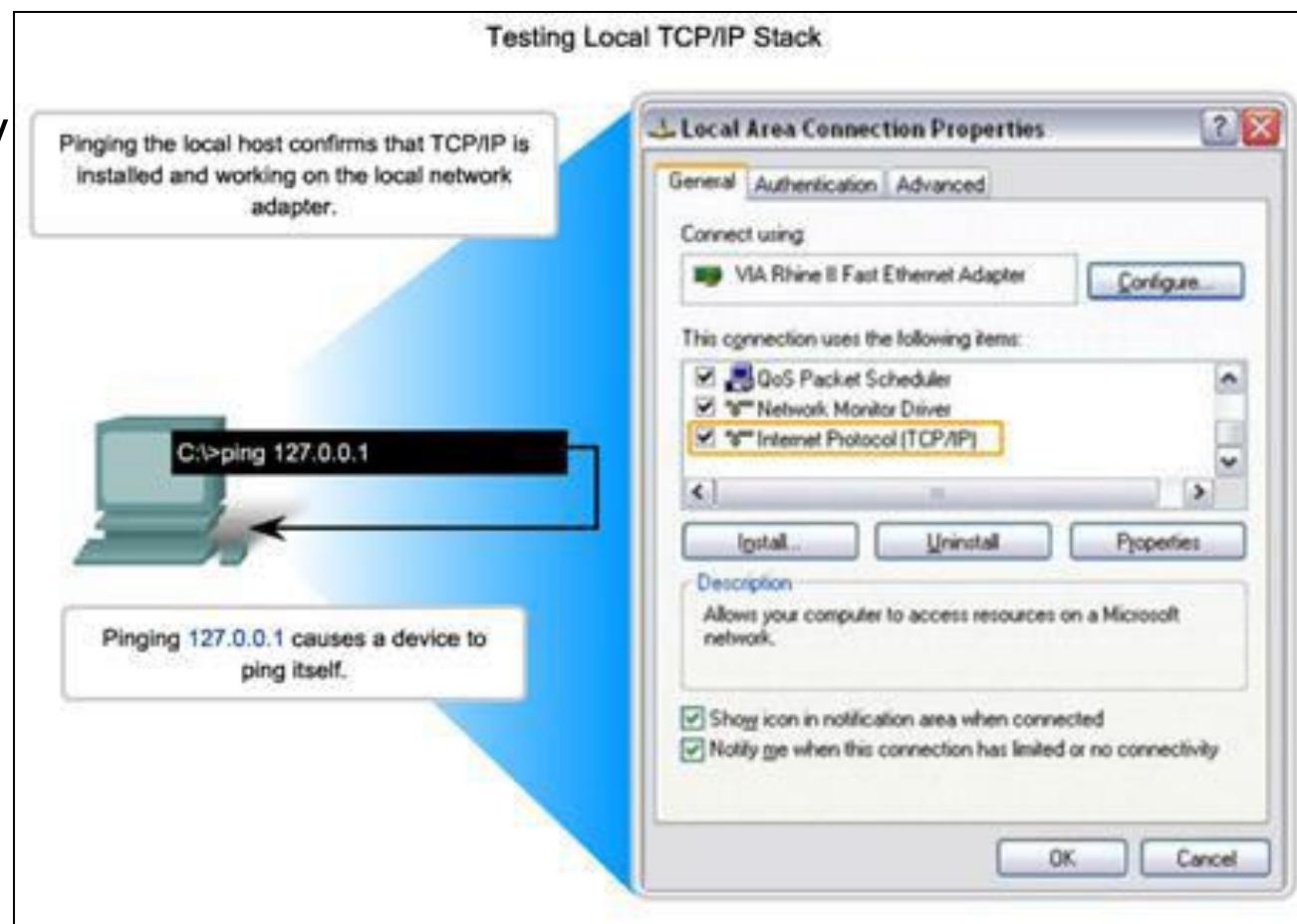




## Ping

## Interpreting ICMP Messages

- ! – indicates receipt of an ICMP echo reply message
- . – indicates a time expired while waiting for an ICMP echo reply message
- U – an ICMP unreachable message was received





## Ping

# Leveraging Extended Ping

The Cisco IOS offers an "extended" mode of the `ping` command:

- R2# `ping`
- Protocol [ip]:
- Target IP address: **192.168.10.1**
- Repeat count [5]:
- Datagram size [100]:
- Timeout in seconds [2]:
- Extended commands [n]: **y**
- Source address or interface: **10.1.1.1**
- Type of service [0]:



# Ping Network Baseline

## Baseline with ping

```
C:\>ping 10.66.254.159
```

```
Pinging 10.66.254.159 with 32 bytes of data:
```

```
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128
```

```
Ping statistics for 10.66.254.159:
```

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

MAR 17, 2013 14:41:06

```
C:\>ping 10.66.254.159
```

```
Pinging 10.66.254.159 with 32 bytes of data:
```

```
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128
```

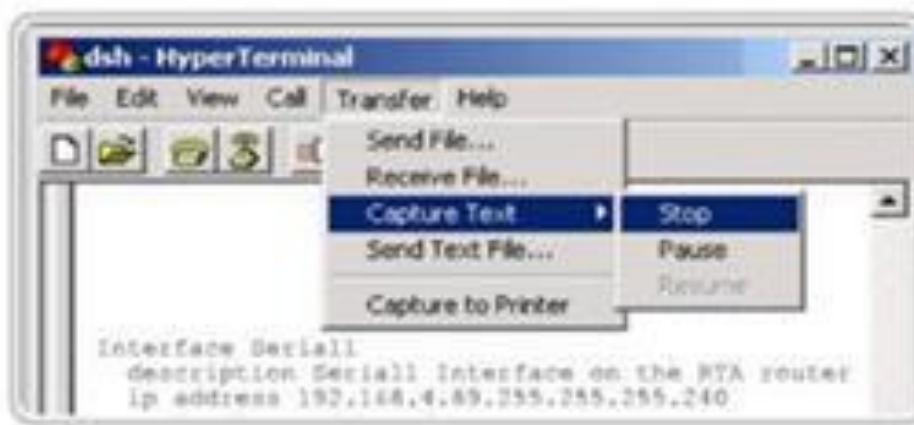
```
Ping statistics for 10.66.254.159:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 6ms, Maximum = 6ms, Average = 6ms
```



# Ping Network Baseline (Cont.)

Router Ping Capture - Saving to a text file



In the terminal session:

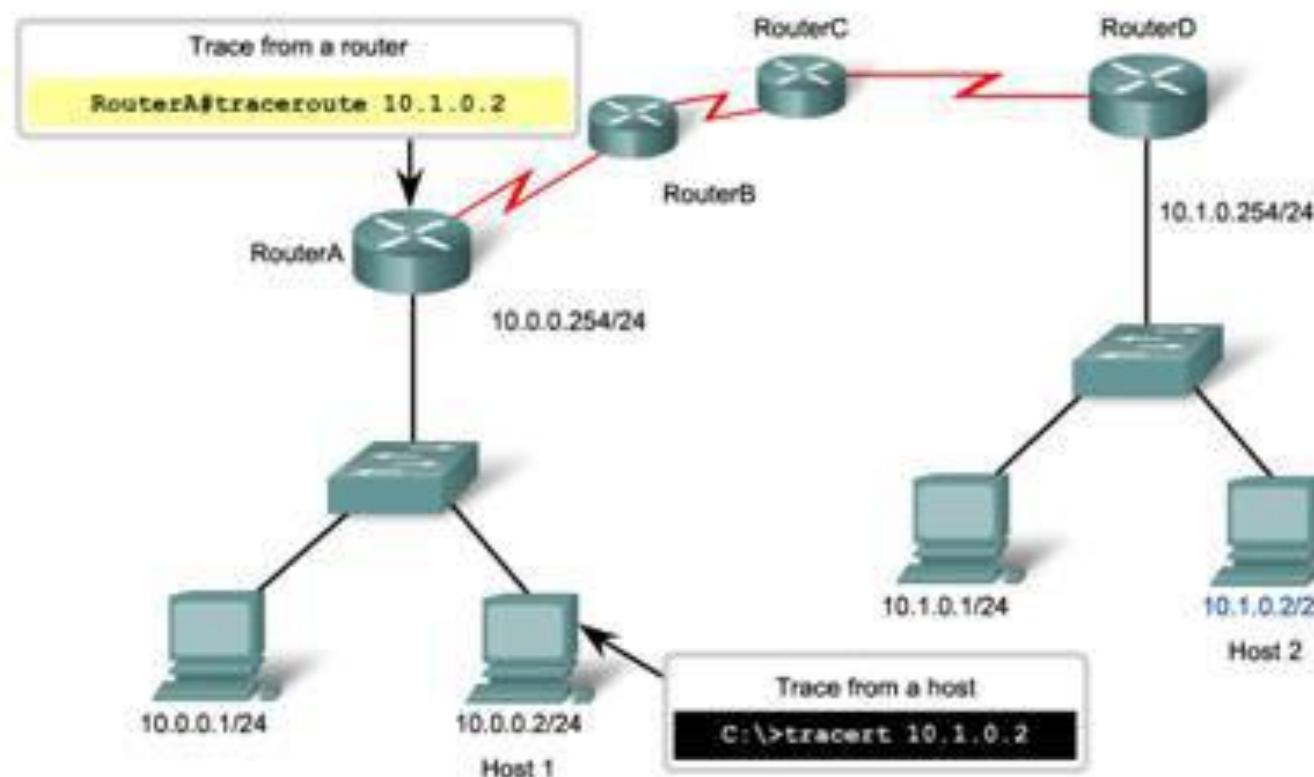
1. Start the text capture process.
2. Issue a ping <ip address> command.
3. Stop the capture process.
4. Save the text file.



## Tracert

## Interpreting Tracert Messages

Testing the Path to a Remote Host





## Show Commands

# Common Show Commands Revisited

The status of nearly every process or function of the router can be displayed using a **show** command.

Frequently used show commands:

- **show running-config**
- **show interfaces**
- **show arp**
- **show ip route**
- **show protocols**
- **show version**



## Show Commands

# Viewing Router Settings With Show Version

**Cisco IOS Version**

**System Bootstrap**

**Cisco IOS Image**

**CPU and RAM**

**Number and Type of Physical Interfaces**

**Amount of NVRAM**

**Amount of Flash**

**Configuration Register**

```
Router#show version
Cisco Internetwork Operating System Software
IOS(tm)2500 Software (C2500-I-1-L), Version 12.0(17a), RELEASE
SOFTWARE (fc1)
Copyright (c)1986-2002 by cisco Systems, Inc.
Compiled Mon 11-Feb-02 05:55 by kellythw
image text-base:0x00001000
ROM:system Bootstrap,Version 11.0(10c),SOFTWARE
BOOTFLASH :3000 Bootstrap Software (IGS-BOOT-R),Version
11.0(10c),RELEASE SOFTWARE(fc1)
System image file is "flash:c2500-i-1.120-17a.bin"
cisco 2500 (68030 processor(revision N) With 2048K/2048K
bytes of memory.
processor bord ID 08860060,with hardware revision 00000000
Bridging software.
X.25 software,version 3.0.0.
1 Ethernet/IEEE 802.3 interface(s)
2 Serial network interface(s)

32K bytes of non-volatile Configuration memory.

8192K bytes of processor board system flash (Read ONLY)

Configuration register is 0x2102
Router#
```



## Show Commands

# Viewing Switch Settings With Show Version

### show version Command

```
Switch#show version
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)SEE2,
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 28-Jul-06 04:33 by yenanh
Image text-base: 0x00003000, data-base: 0x00AA2F34

ROM: Bootstrap program is C2960 boot loader
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)SEE1, RELEASE
SOFTWARE (fc1)

Switch uptime is 2 minutes
System returned to ROM by power-on
System image file is "flash:c2960-lanbase-mz.122-25.SEE2/c2960-lanbase-
mz.122-25.SEE2.bin"

cisco WS-C2960-24TT-L (PowerPC405) processor (revision B0) with 61440K/4088K
bytes of memory.
Processor board ID FOC1107Z92N
Last reset from power-on
1 Virtual Ethernet interface
```



## Host and IOS Commands

# ipconfig Command Options

- **ipconfig** – Displays ip address, subnet mask, default gateway.
- **ipconfig /all** – Also displays MAC address.
- **ipconfig /displaydns** – Displays all cached dns entries in a Windows system.

**ipconfig**

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

  Connection-specific DNS Suffix . . . . . : 192.168.1.2
  IP Address . . . . . : 192.168.1.254
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.1.254
```

**Legend**

- IP address for this host computer
- Local network subnet mask
- Default gateway address for this host computer



# Host and IOS Commands

## arp Command Options

### arp Command Options

Diagram illustrating a network topology with five hosts connected to a central switch. The hosts are assigned IP addresses from the range 10.0.0.1/24 to 10.0.0.5/24. The switch is connected to a router with the IP address 10.0.0.254/24.

Internet Address	Physical Address	Type
10.0.0.2	00-08-a3-b6-ce-04	dynamic
10.0.0.3	00-0d-56-09-fb-d1	dynamic
10.0.0.4	00-12-3f-d4-6d-1b	dynamic
10.0.0.254	00-10-7b-e7-fa-ef	dynamic

An arrow points from the highlighted row in the table to a callout box labeled "IP-MAC Address Pair".



## Host and IOS Commands

# show cdp neighbors Command Options

**show cdp neighbors** command provides information about each directly connected CDP neighbor device.

```
R3#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID      Local Intrfce     Holdtme   Capability   Platform  Port ID
S3            Fas 0/0          151        S I          WS-C2950  Fas 0/6
R2            Ser 0/0/1        125        R           1841      Ser 0/0/1

R3#show cdp neighbors detail
Device ID: R2
Entry address(es):
  IP address : 192.168.1.2
Platform: Cisco 1841,  Capabilities: Router Switch IGMP
Interface: Serial0/0/1,  Port ID (outgoing port): Serial0/0/1
Holdtime : 161 sec

Version :
```



## Host and IOS Commands

# Using show ip interface brief Command

**show ip interface brief** command—used to verify the status of all network interfaces on a router or a switch.

```
Router1#show ip interface brief
Interface          IP-Address      OK?   Method    Status           Protocol
FastEthernet0/0    192.168.254.254  YES   NVRAM    up              up
FastEthernet0/1/0  unassigned       YES   unset    down            down
Serial0/0/0        172.16.0.254   YES   NVRAM    up              up
Serial0/0/1        unassigned       YES   unset    administratively down  down
```

```
Router1#ping 192.168.254.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.254.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
Router1#traceroute 192.168.0.1
Type escape sequence to abort.
Tracing the route to 192.168.0.1
 1 172.16.0.253 8 msec 4 msec 8 msec
 2 10.0.0.254 16 msec 16 msec 8 msec
 3 192.168.0.1 16 msec * 20 msec
```

## 11.4 Managing IOS Configuration Files





# Router and Switch File Systems

## Router File Systems

**show file systems** command – Lists all of the available file systems on a Cisco 1941 route.

The asterisk (\*) indicates this is the current default file system.

Router# show file systems					
File Systems:					
	Size (b)	Free (b)	Type	Flags	Prefixes
*	256487424	183234560	disk	rw	flash0: flash:#
	-	-	disk	rw	flash1:
	262136	254779	nvram	rw	nvram:
	-	-	opaque	ro	syslog:
	-	-	opaque	rw	xmodem:
	-	-	opaque	rw	ymodem:
	-	-	network	rw	rcp:
	-	-	network	rw	http:
	-	-	network	rw	ftp:
	-	-	network	rw	sco:
	-	-	opaque	ro	tac:
	-	-	network	rw	https:
	-	-	opaque	ro	CRL:



# Router and Switch File Systems

## Switch File Systems

**show file systems** command – Lists all of the available file systems on a Catalyst 2960 switch.

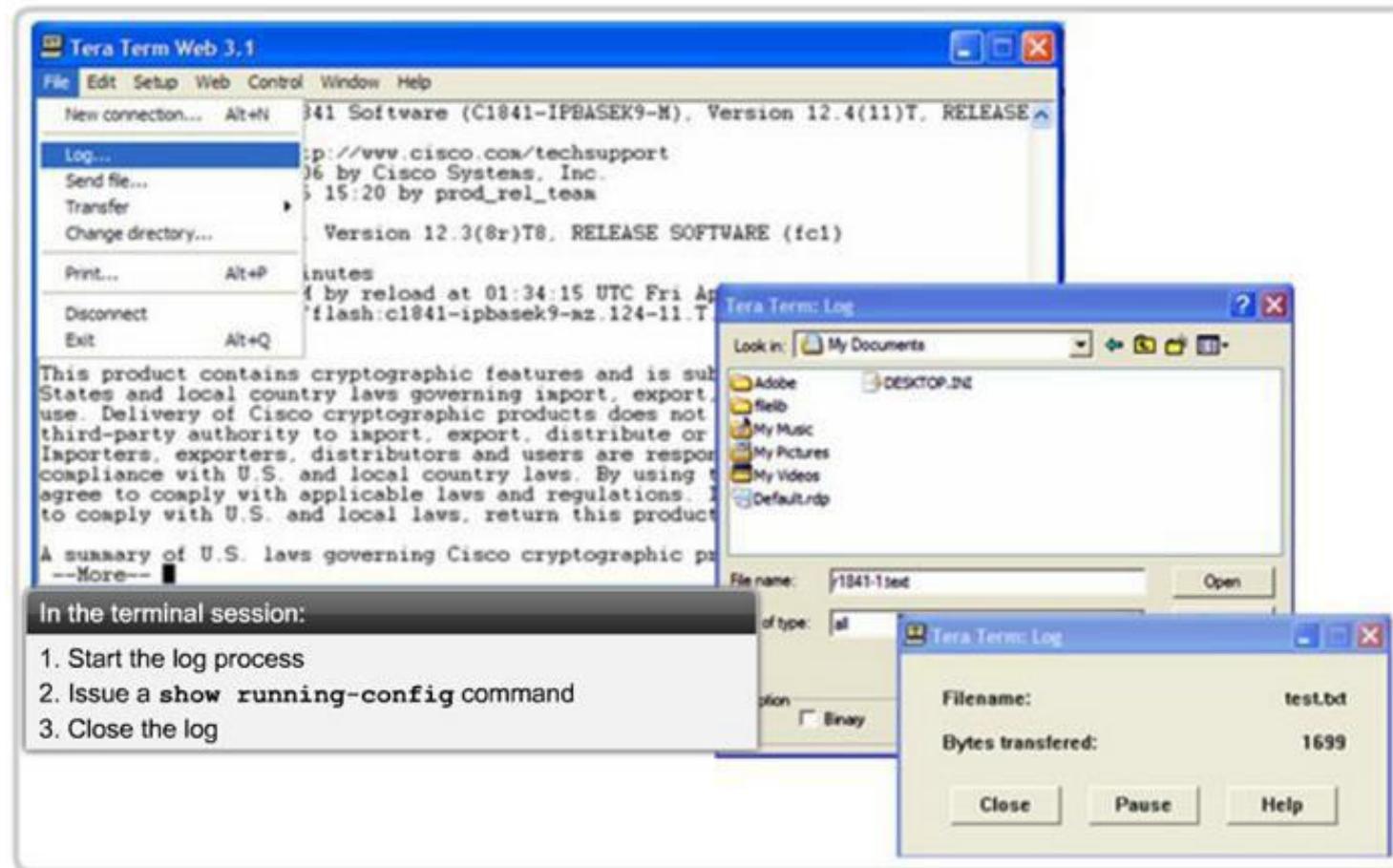
Switch#show file systems						
File Systems:						
	Size(b)	Free (b)	Type	Flags	Prefixes	
*	32514048	20887552	flash	rw	flash:	
	-	-	opaque	rw	vb:	
	-	-	opaque	ro	bs:	
	-	-	opaque	rw	system:	
	-	-	opaque	rw	tmpsys:	
	65536	48897	nvram	rw	nvram:	
	-	-	opaque	ro	xmodem:	
	-	-	opaque	ro	ymodem:	
	-	-	opaque	rw	null:	
	-	-	opaque	ro	tar:	
	-	-	network	rw	tftp:	
	-	-	network	rw	rpc:	
	-	-	network	rw	http:	
	-	-	network	rw	ftp:	
	-	-	network	rw	scp:	
	-	-	network	rw	https:	
	-	-	opaque	ro	cns:	



## Backup and Restore Configuration Files

# Backup and Restore Using Text Files

### Saving to a Text File in Tera Term





## Backup and Restore Configuration Files

# Backup and Restore Using TFTP

- Configuration files can be stored on a Trivial File Transfer Protocol (TFTP) server.
- **copy running-config tftp** – Save running configuration to a tftp server.
- **copy startup-config tftp** – Save startup configuration to a tftp server.

```
Router#copy running-config tftp
Remote host []? 131.108.2.155
Name of configuration file to write[tokyo-config]?tokyo.2
Write file tokyo.2 to 131.108.2.155? [confirm]
Writing tokyo.2 !!!!!! [OK]
```



# Backup and Restore Configuration Files Using USB Interfaces on a Cisco Router

- USB flash drive must be formatted in a FAT16 format.
- Can hold multiple copies of the Cisco IOS and multiple router configurations.
- Allows administrator to easily move configurations from router to router.





## Backup and Restore Configuration Files

# Backup and Restore Using USB

### Backup to USB Drive

```
R1#copy running-config usbflash0:/ ()  
Destination filename [running-config]? R1-Config  
5024 bytes copied in 0.736 secs (6826 bytes/sec)
```

Copying to USB flash drive, and no file pre-exists

```
R1#copy running-config usbflash0:/  
Destination filename [running-config]? R1-Config  
%Warning:There is a file already existing with this name  
Do you want to over write? [confirm]  
5024 bytes copied in 1.796 secs (2797 bytes/sec)
```

Copying to USB flash drive, and the same configuration file already exists on the drive.

## 11.5 Integrated Routing Services





# Integrated Router Multi-function Device

## Multi-function Device

- Incorporates a switch, router, and wireless access point.
- Provides routing, switching and wireless connectivity.
- Linksys wireless routers, are simple in design and used in home networks

**Cisco Integrated Services Router (ISR)** product family offers a wide range of products, designed for small office to larger networks.





## Integrated Router

# Wireless Capability

- **Wireless Mode** – Most integrated wireless routers support 802.11b, 802.11g and 802.11n.
- **Service Set Identifier (SSID)** – Case-sensitive, alpha-numeric name for your home wireless network.
- **Wireless Channel** – RF spectrum can be divided up into channels.

### Linksys Wireless Settings

The screenshot shows the 'Basic Wireless Settings' page of a Linksys WRT300N router. The 'Network Mode' dropdown is highlighted and set to 'Mixed'. The 'Network Name (SSID)' field contains 'linksys'. The 'Radio Band' dropdown is set to 'Auto'. The 'Wide Channel' and 'Standard Channel' dropdowns are both set to 'Auto'. The 'SSID Broadcast' radio button is selected ('Enabled'). At the bottom are 'Save Settings' and 'Cancel Changes' buttons.

#### Network Mode

Determines the type of technology that must be supported. For example, **802.11b**, **802.11g**, **802.11n** or **Mixed Mode**.



## Integrated Router

# Basic Security of Wireless

- Change default values
- Disable SSID broadcasting
- Configure Encryption using WEP or WPA
- **Wired Equivalency Protocol (WEP)** - Uses pre-configured keys to encrypt and decrypt data. Every wireless device allowed to access the network must have the same WEP key entered.
- **Wi-Fi Protected Access (WPA)** – Also uses encryption keys from 64 bits up to 256 bits. New keys are generated each time a connection is established with the AP; therefore, more secure.



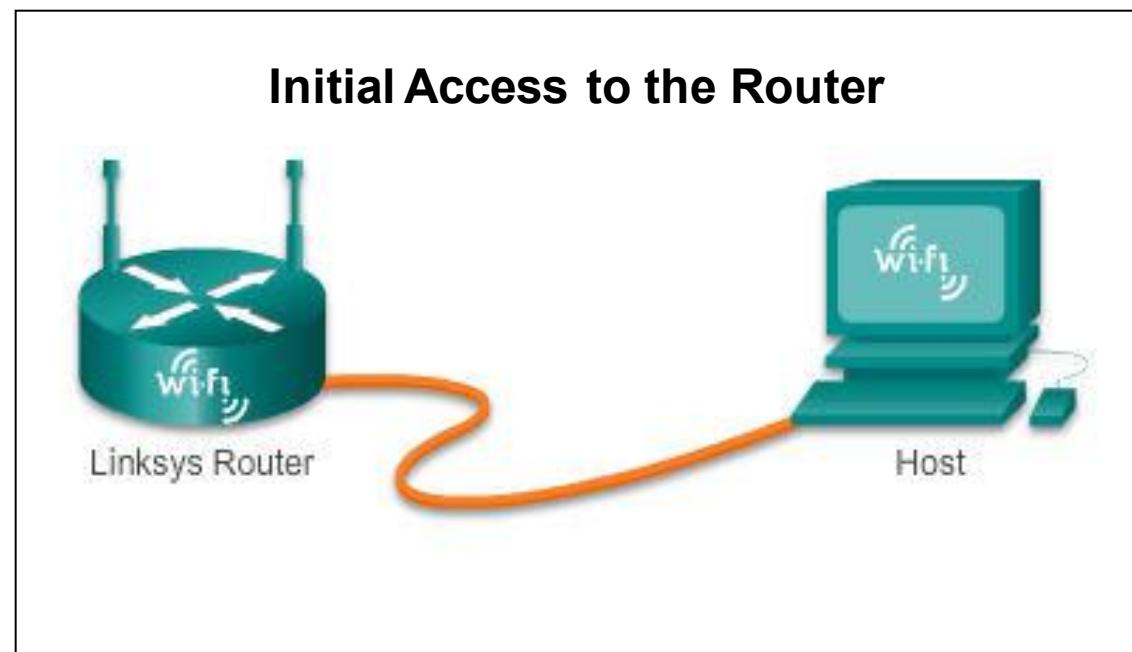
## Integrated Router

# Configuring the Integrated Router

**Step 1** - Access the router by cabling a computer to one of the router's LAN Ethernet ports.

**Step 2** - The connecting device will automatically obtain IP addressing information from Integrated Router.

**Step 3** - Change default username and password and the default Linksys IP address for security purposes.





# Integrated Router Enabling Wireless

**Step 1 - Configure the wireless mode**

**Step 2 - Configure the SSID**

**Step 3 - Configure RF channel**

**Step 4 - Configure any desired security encryption**

The screenshot shows the 'Basic Wireless Settings' page of the Linksys WRT300N router's web-based configuration interface. The 'Network Mode' dropdown is currently set to 'Mixed' and is open, displaying other options like 'BG-Mixed', 'Wireless-G Only', 'Wireless-B Only', 'Wireless-N Only', and 'Disabled'. Other settings visible include 'Radio Band' (2.4GHz), 'Channel' (1-11), and 'SSID Broadcast' (Enabled). The top navigation bar includes tabs for 'Setup', 'Wireless', 'Security', 'Access Restrictions', 'Applications & Gaming', 'Administration', and 'Status'. The top right corner indicates the firmware version is v9.03.0 and the model is WRT300N. The bottom of the screen features 'Save Settings' and 'Cancel Changes' buttons.



## Integrated Router

# Configure a Wireless Client

- The wireless client configuration settings must match that of the wireless router.
  - SSID
  - Security Settings
  - Channel
- Wireless client software can be integrated into the device operating system or stand alone, downloadable, wireless utility software.



## 11.6 Summary





# Chapter 11: Summary

In this chapter, you learned:

- Good network design incorporates reliability, scalability, and availability.
- Networks must be secured from viruses, Trojan horses, worms and network attacks.
- The importance of documenting Basic Network Performance.
- How to test network connectivity using **ping** and **traceroute**.
- How to use IOS commands to monitor and view information about the network and network devices.
- How to backup configuration files using TFTP or USB.
- Home networks and small business often use integrated routers, which provide the functions of a switch, router and wireless access point.

# Cisco | Networking Academy®

Mind Wide Open™