



Living in a Network Centric World



Network Fundamentals – Chapter 1

Cisco | Networking Academy®
Mind Wide Open™



Objectives

- Describe how networks impact our daily lives.
- Describe the role of data networking in the human network.
- Identify the key components of any data network.
- Identify the opportunities and challenges posed by converged networks.
- Describe the characteristics of network architectures: fault tolerance, scalability, quality of service and security.
- Labs: Install and use IRC clients and a Wiki server.

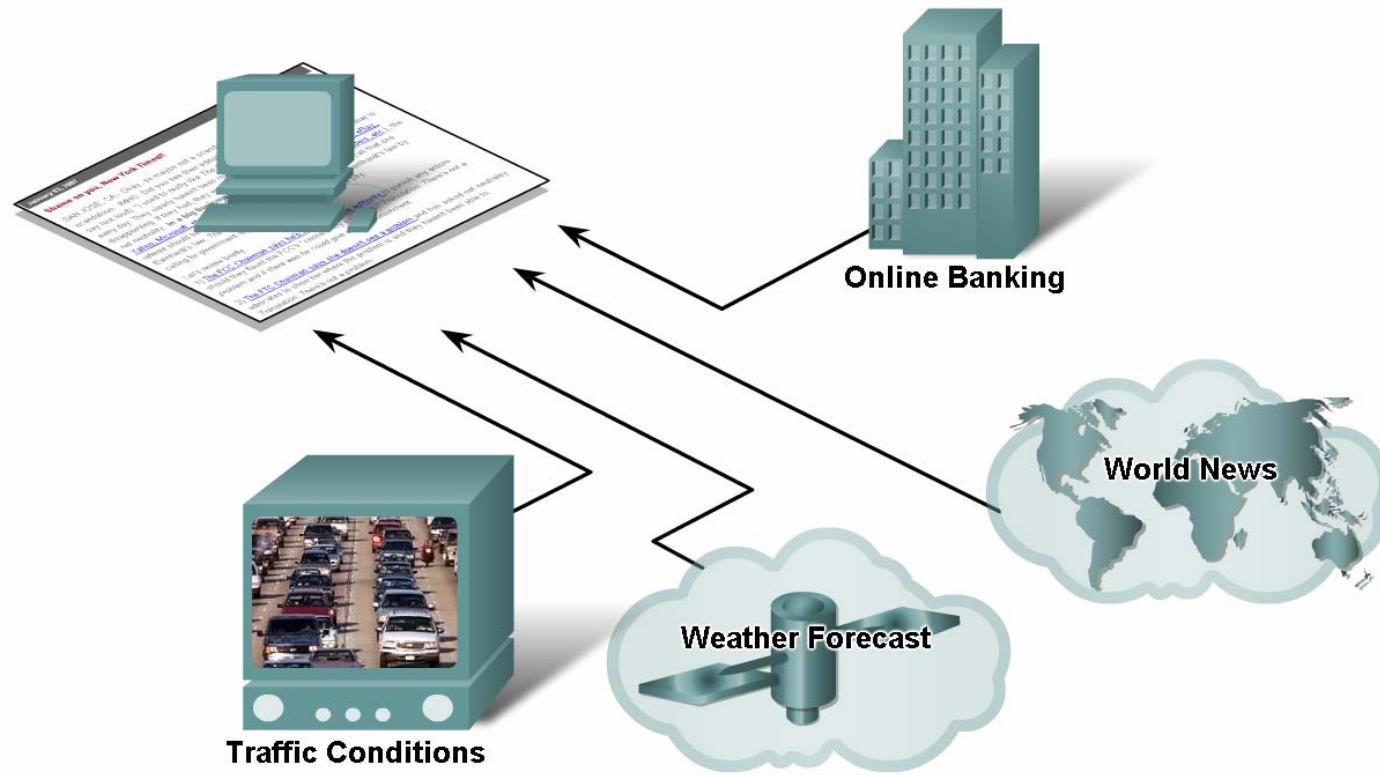


Role of the Communication

- **Communication** is almost as important to us as our reliance on air, water, food, and shelter.
- The methods that we use to share ideas and information are **constantly changing and evolving**.
- The human network was once limited to face-to-face conversations
- From the printing press to television, each new development has improved and enhanced our communication.
- Current networks have evolved to carry voice, video streams, text, and graphics between many different types of devices.
- Previously separate and distinct communication forms have **converged** onto a common platform.

How Networks Impact Daily Life

- The benefits of instantaneous communication and how it supports and improves our lives.





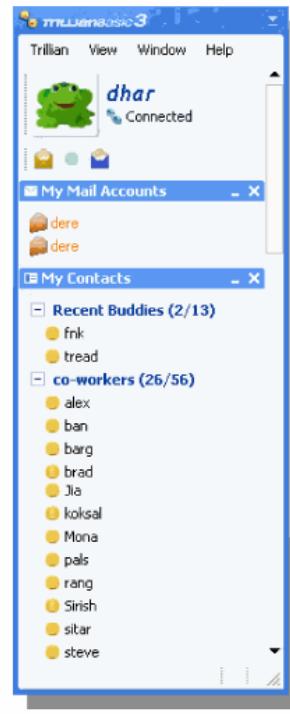
How Networks Impact Daily Life

- Popular communication tools: IM, Wikis , Blogs, Podcasting, and Collaboration Tools

—Instant messaging

- Real time communication between 2 or more people based on typed text

Instant Messaging



—Weblogs (Blogs)

- Web pages created by an individual

Weblog

January 03, 2007

Shame on you, New York Times!!

SAN JOSE, CA - Okay, so maybe not a scandal at New York Times, but nearly scandalous...IMHO. Did you see their editorial on net neutrality today? Made me say (out loud): "I used to really like *The New York Times*." Okay, so I do read it every day. They clearly haven't been reading this blog, however...which is disappointing. If they had, they would have not fallen into the hype machine that is net neutrality. In a big business versus big business debate ([Google, eBay, Yahoo, Microsoft, etc. versus Telcos, cable companies, service providers, etc.](#)), the referee should be the marketplace, not the government. You can call that one Eamhardt's law. *The New York Times* editorial today broke Eamhardt's law by calling for government regulation on the Internet. That's a pity.

Let's review briefly:

- 1) [The FCC Chairman says he's already got the authority](#) to punish any actors should they flaunt the FCC's "connectivity principles." Translation: There's not a problem and if there was he could give out any punishment.
- 2) [The FTC Chairman says she doesn't see a problem](#) and has asked net neutrality advocates to show her where the problem is and they haven't been able to. Translation: There's not a problem.

—Podcasting

- Website that contains audio files available for downloading

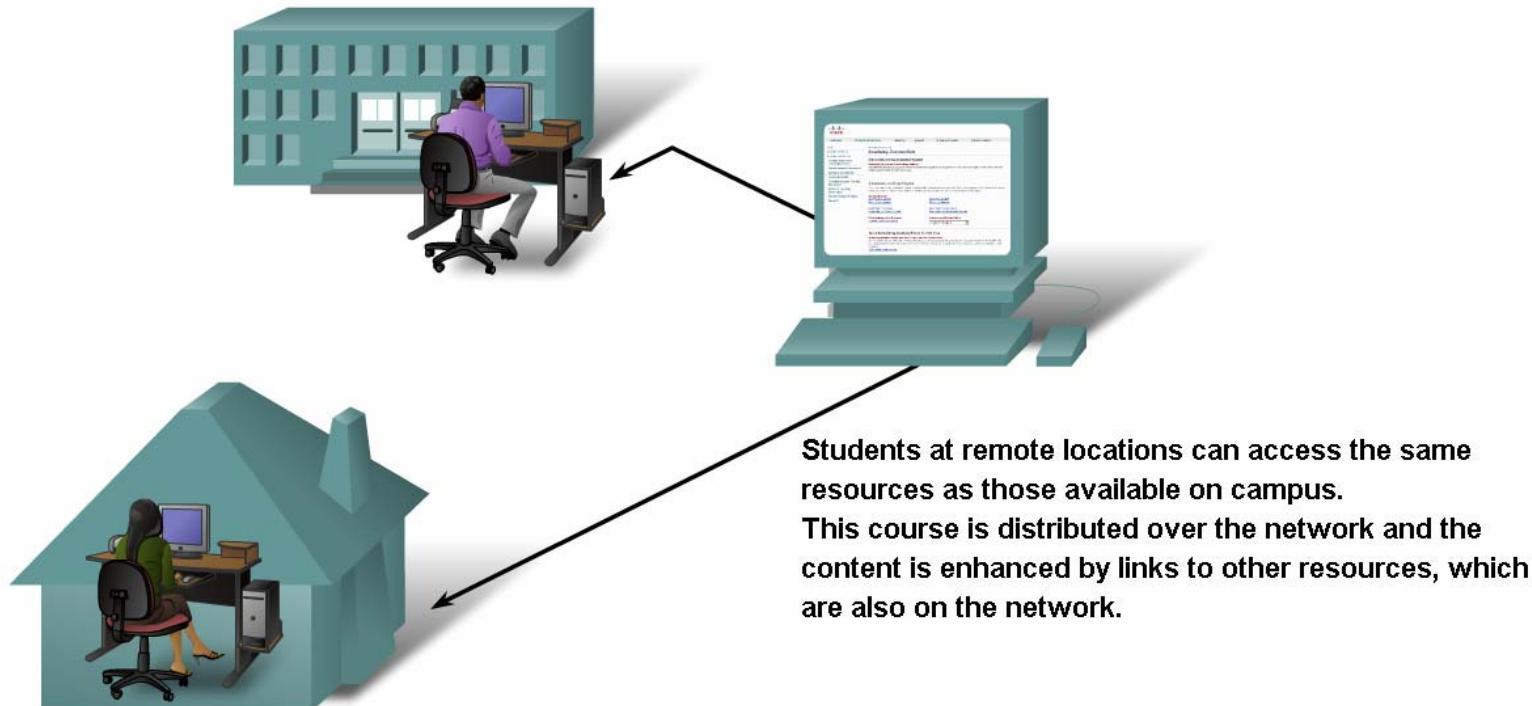
Podcasting





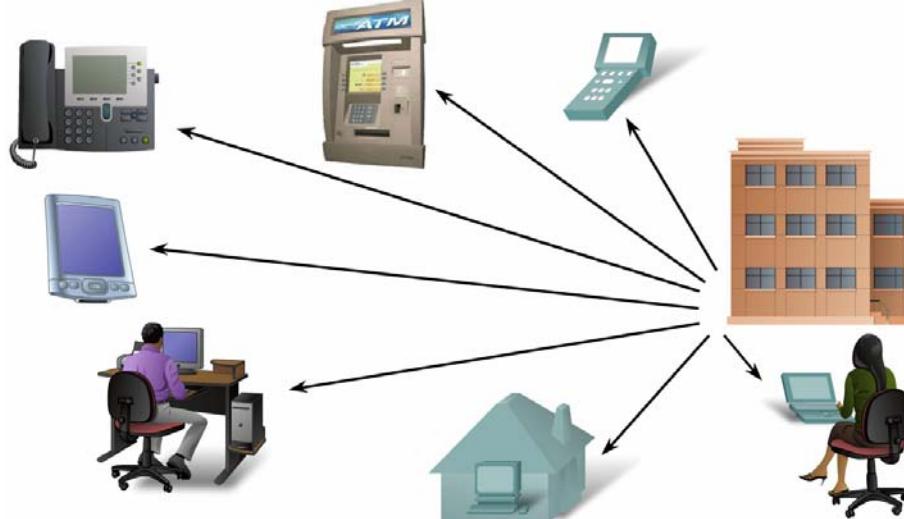
How Networks Impact Daily Life

- Collaboration tools: **e-learning** improves teaching and learning e.g. Cisco Networking Academy Program
- Benefits: current and accurate training materials, availability of training to a wide audience, consistent quality of instruction, cost reduction



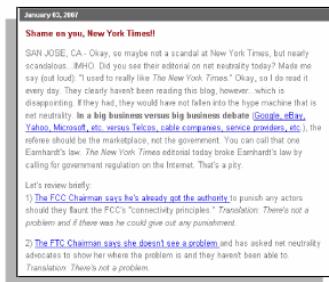
How Networks Impact Daily Life

- The ways of communication over a network changes the way we work
- **Intranets** (in use by just one company) enable businesses to communicate and perform transactions among global employee and branch locations.
- Now companies develop **extranets** to provide suppliers, vendors, and customers limited access to corporate data to check order status, inventory, and parts lists.



How Networks Impact Daily Life

- The ways of communication over a network supports the way we play



Online Interest Groups



Instant Messaging



The onboard data network provides a range of services to airline personal seatback video systems.

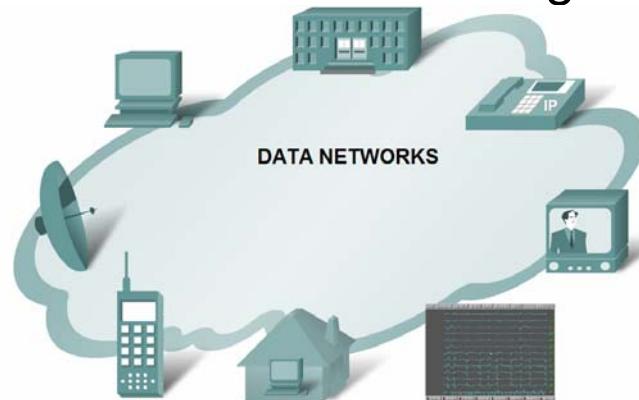


Data Networking Role, Components, and Challenges

- Basic characteristics of communication:
 - Rules or agreements** are 1st established (methods, languages, protocols...)
 - Important information** may need to be repeated
 - Various modes** of communication may impact the effectiveness of getting the message across.
- Quality of communication:
 - External factors** - e.g. quality of the pathway between the sender and the recipient, number of times the message has to change form or to be redirected or readressed or the number of other messages being transmitted simultaneously on the communication network
 - Internal factors** - e.g. size, complexity and importance of the message.

Data Networking Role, Components, and Challenges

- Data or information networks vary in size and capabilities, but all networks have four basic elements in common:
 - Rules or agreements** to govern how the messages are sent, directed, received and interpreted.
 - The **messages or units** of information that travel from one device to another
 - A **means of interconnecting** these **devices** - a medium that can transport the messages from one device to another
 - Devices** on the network that exchange messages with each other



Data Networking Role, Components, and Challenges

- There are various elements that make up a network:

- Devices**

- These are used to communicate with one another

- Medium**

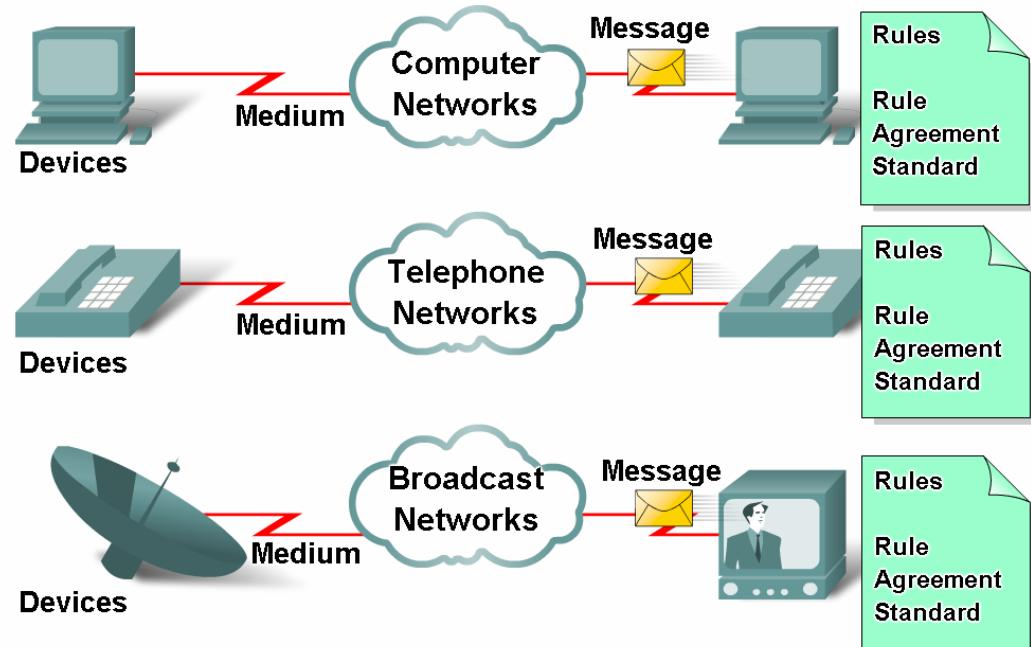
- This is how the devices are connected together

- Messages**

- Information that travels over the medium

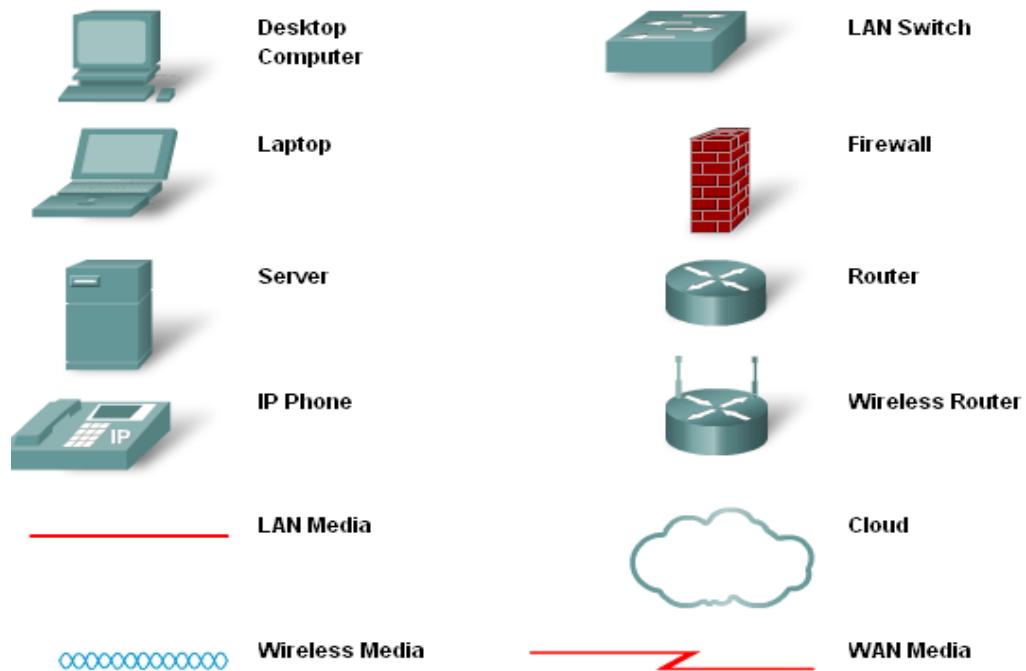
- Rules**

- Governs how messages flow across network



Data Networking Role, Components, and Challenges

Common Data Network Symbols



Devices, medium and rules

Fig. 1.3.2.5

Service	Protocol ("Rule")
World Wide Web (WWW)	HTTP (Hypertext Transport Protocol)
E-mail	SMTP (Simple Mail Transport Protocol) POP (Post Office Protocol)
Instant Message (Jabber; AIM)	XMPPTCP (Extensible Messaging and Presence Protocol) OSCAR (Open System for Communication in Realtime)
IP Telephony	SIP (Session Initiation Protocol)

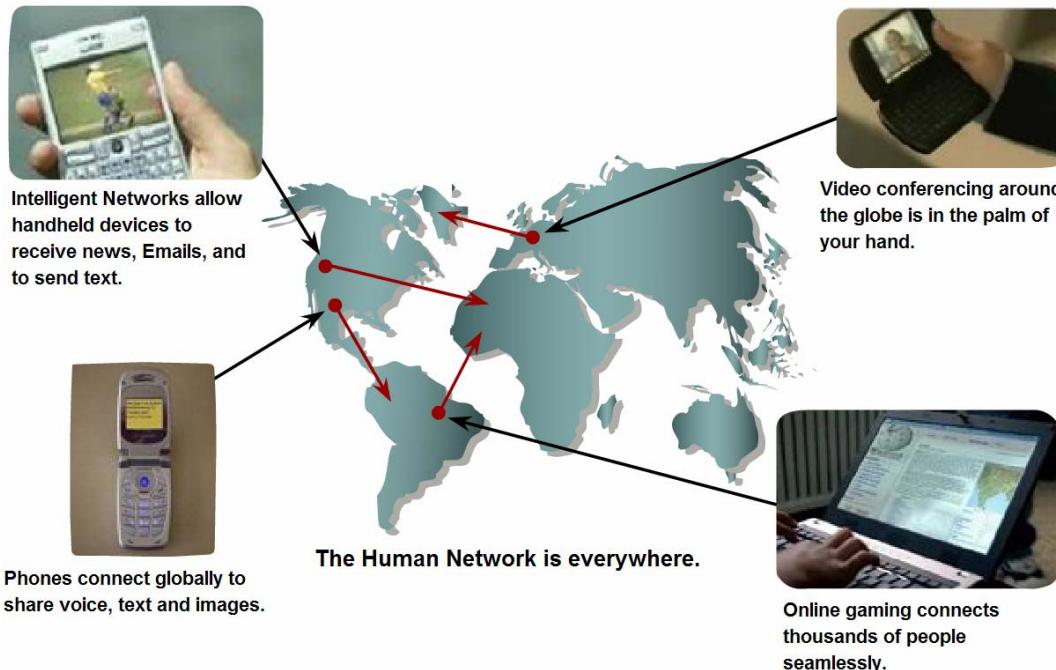


Data Networking Role, Components, and Challenges

■ The role of converged networks in communications

—Converged network

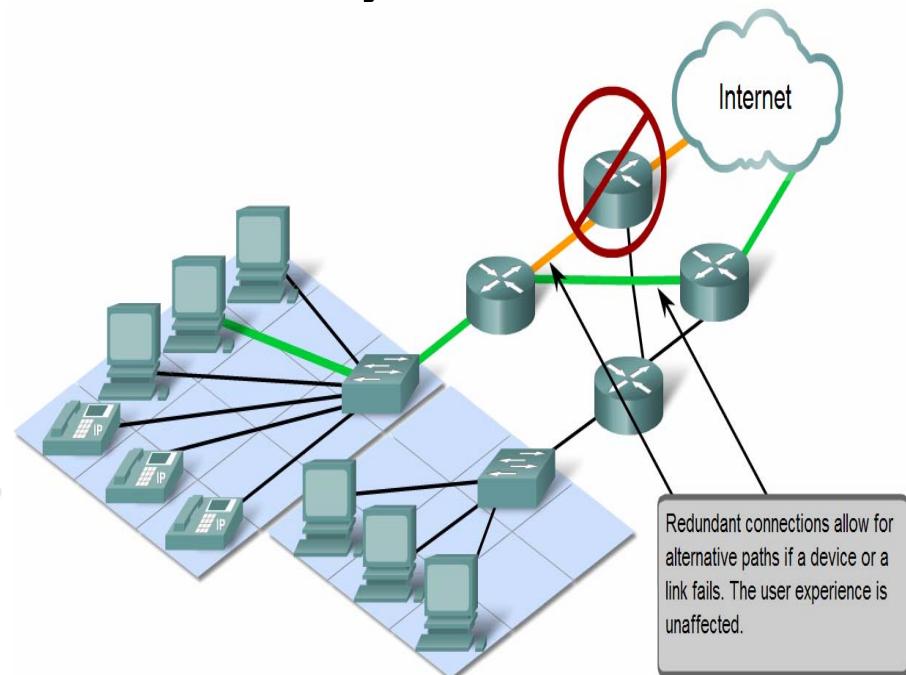
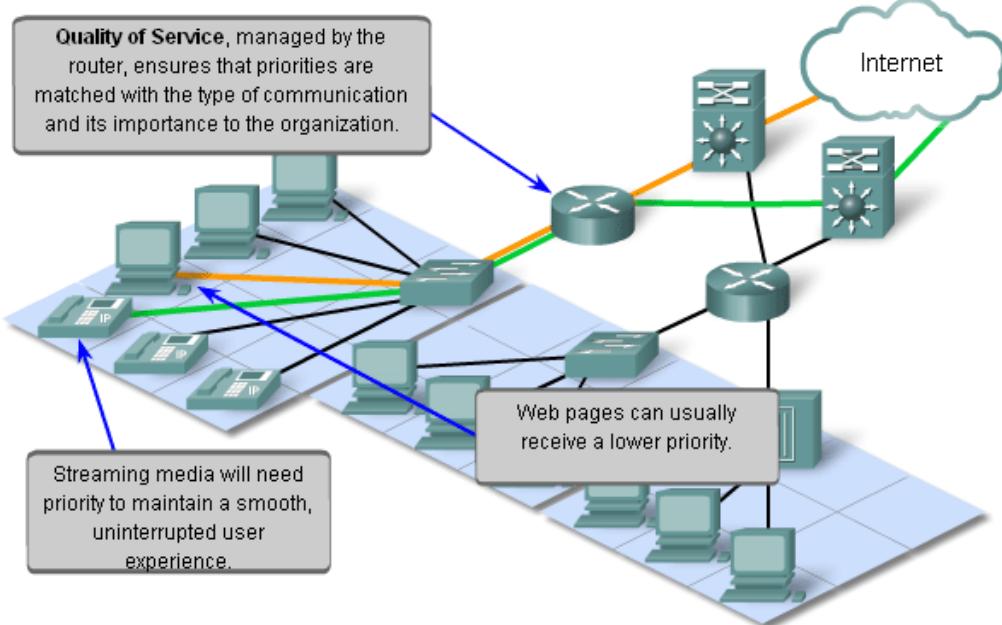
- A type of network that can carry voice, video & data over the same network



Network Architecture Characteristics

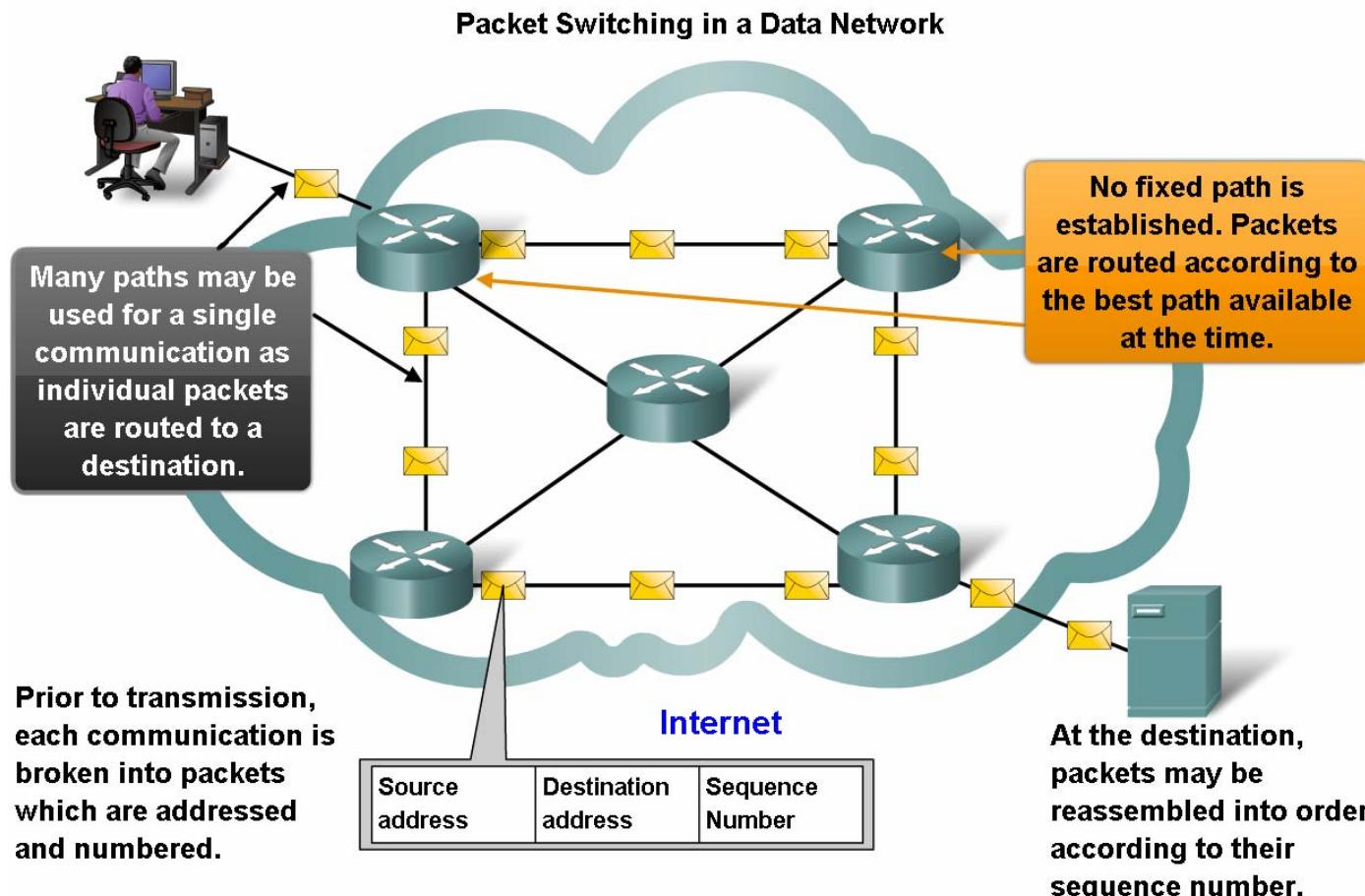
- Four characteristics that are addressed by network architecture design:

- Fault tolerance**
- Scalability**
- Quality of service**
- Security**



Network Architecture Characteristics

- How packet switching helps improve the resiliency and fault tolerance of the Internet architecture

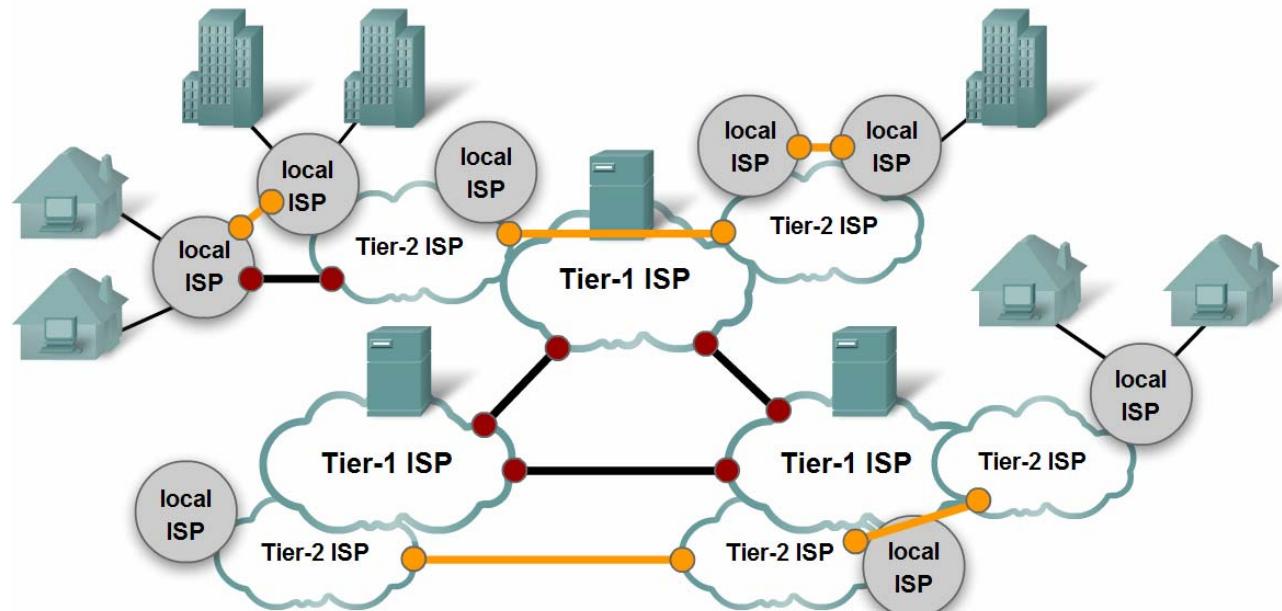


Network Architecture Characteristics

- Characteristics of the Internet that help it scale to meet user demand
 - Hierarchical
 - Common standards
 - Common protocols

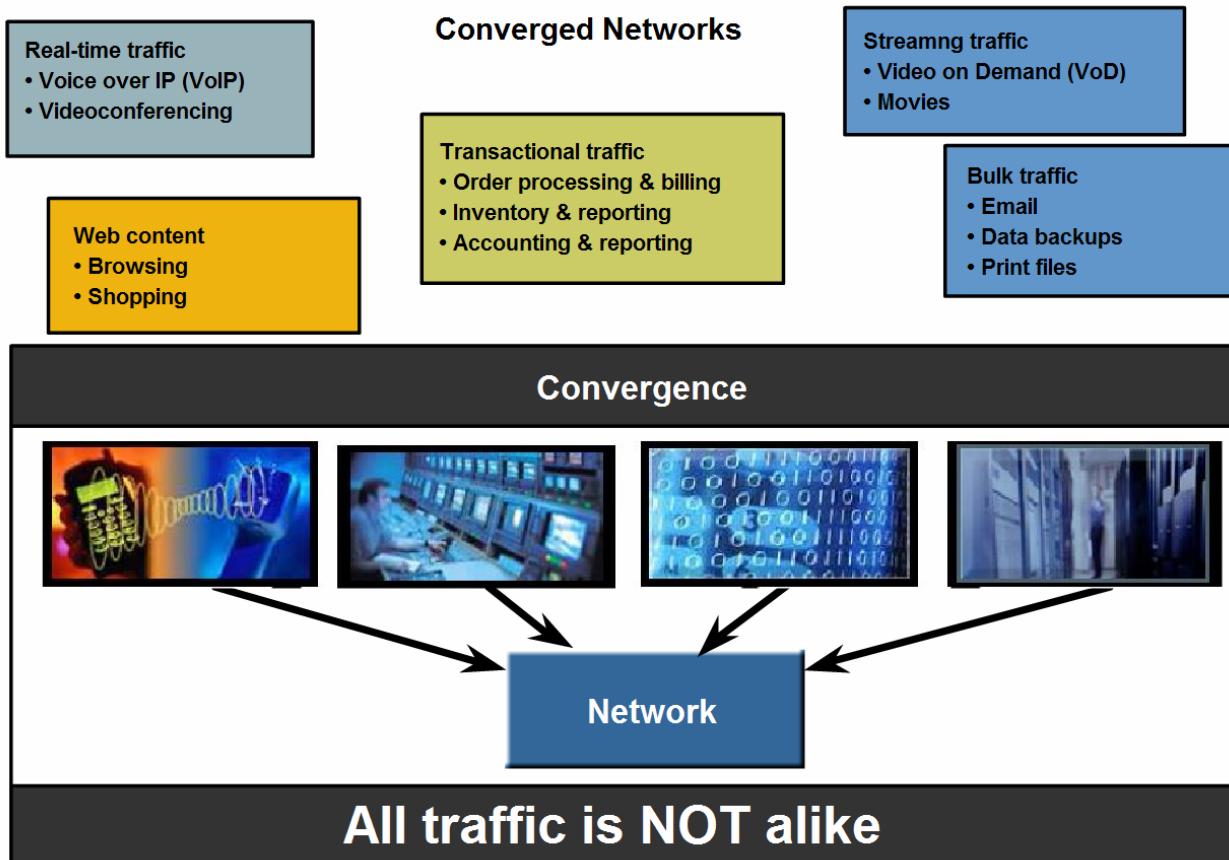
Fig. 1.4.3.1

Internet Structure - A Network of Networks



Network Architecture Characteristics

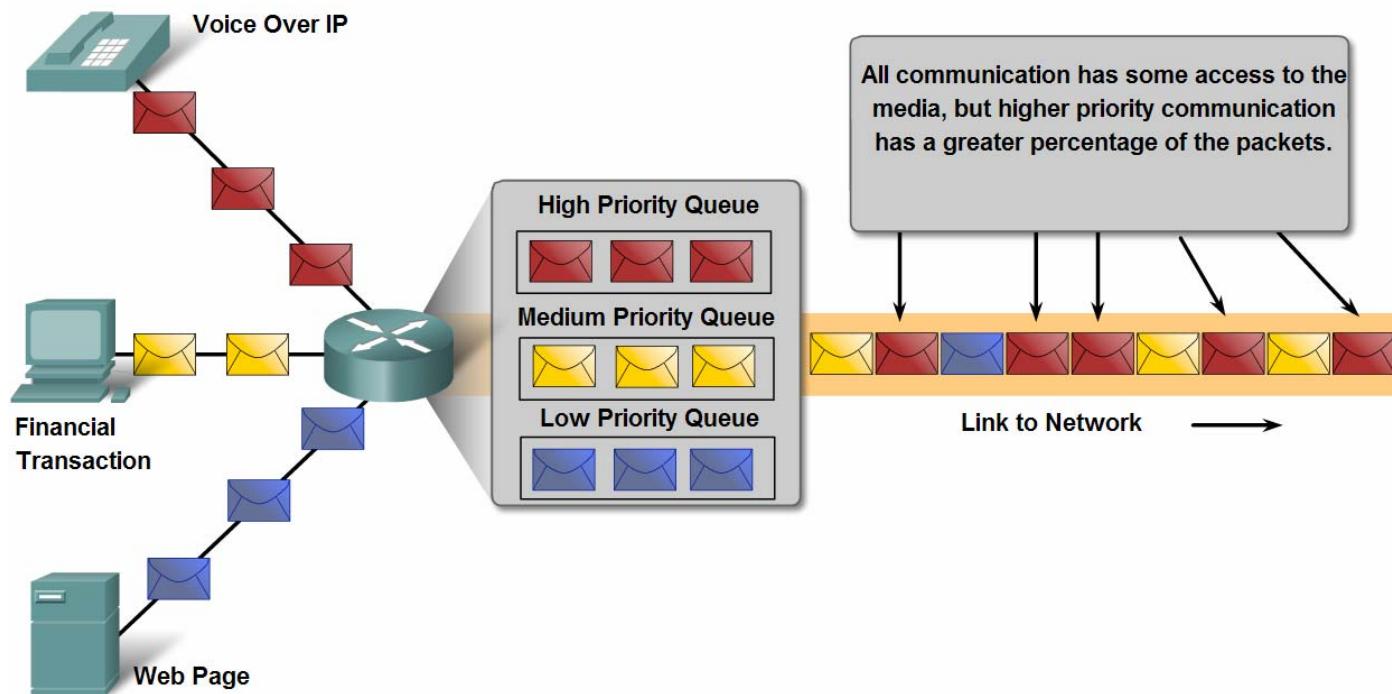
- How QoS mechanisms work to ensure quality of service for applications that require it.



Network Architecture Characteristics

- The factors that necessitate Quality of Service and the mechanisms necessary to ensure it

Using Queues to Prioritize Communication



Queuing according to data type enables voice data to have priority over transaction data, which has priority over web data.



Network Architecture Characteristics

- How to select the appropriate QoS strategy for a given type of traffic

Quality of Service Matters

Communication Type	Without QoS	With QoS
Streaming video or audio	A blurry, low-quality video frame showing two people, indicating poor service.	A clear, high-quality video frame showing the same two people, indicating good service.
Vital Transactions	Time : Price 02:14:05 \$1.54 Just one second earlier...	Time : Price 02:14:04 \$1.52 The price may be better.
Downloading web pages (often lower priority)	A blurry screenshot of a web browser displaying a news article, indicating slow download speed.	A clear screenshot of the same web browser showing the same news article, indicating fast download speed.



Network Architecture Characteristics

- Networks must be secure

Unauthorized Transactions

CREDIT CARD STATEMENT			
ACCOUNT NUMBER		NAME	STATEMENT DATE
4125-239-412		John Doe	2/13/01
CREDIT LINE	CREDIT AVAILABLE	NEW BALANCE	MINIMUM PAYMENT DUE
\$1200.00	\$1074.76	\$125.24	\$20.00
<hr/>			
REFERENCE	SOLD	POSTED	ACTIVITY SINCE LAST STATEMENT
403GB7382		1/25	PAYMENT THANK YOU -168.80
32F349ER3	1/12	1/15	RECORD RECYCLER ANYTOWN USA 14.83
89102DIS2	1/13	1/15	BEEFORAMA REST ANYTOWN USA 30.55
NX34FJD32	1/18	1/18	GREAT EXPECTORATIONS BIG CITY USA 27.50
84RT3293A	1/20	1/21	DINO-GEL PETROLEUM ANYTOWN USA 12.26
873DWS321	2/09	2/09	SHIRTS 'N SUCH TINYVILLEUSA 40.10
<hr/>			
Previous Balance	(+)	168.80	Current Amount Due 125.24
Purchases	(+)	125.24	Amount Past Due
Cash Advances	(+)		Amount Over Credit Line
Payments	(-)	168.80	Minimum Payment Due 20.00
Credits	(-)		
FINANCE CHARGES	(+)		
Late Charges	(+)		
NEW BALANCE	(+)	125.24	
<hr/>			
FINANCE CHARGE SUMMARY	PURCHASES	ADVANCES	For Customer Service Call:
Periodic Rate	1.55%	0.054%	1-800-XXX-XXXX
Annual Percentage Rate	19.80%	19.80%	For Lost or Stolen Card, Call:
			1-800-XXX-XXXX
			24-Hour Telephone Numbers
<hr/> <p>Please make check or money order payable to Your First Bank. Include account number on front.</p>			





Network Architecture Characteristics

- Basic measures to secure data networks:

- Ensure confidentiality through use of

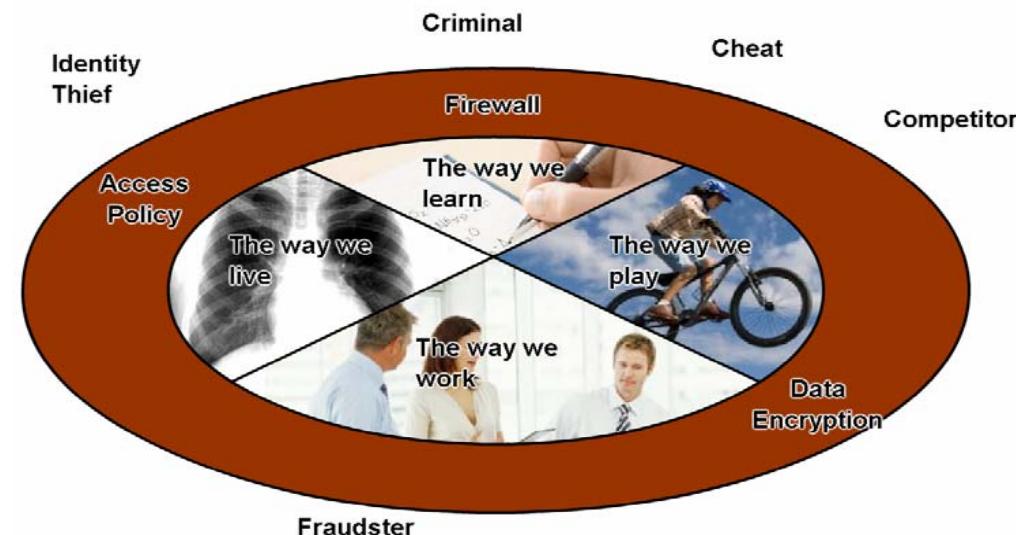
- User authentication
 - Data encryption

- Maintain communication integrity through use of

- Digital signatures

- Ensure availability through use of

- Firewalls
 - Redundant network architecture
 - Hardware without a single point of failure





Summary

In this chapter, you learned to:

- Describe how networks impact our daily lives.
- Describe the role of data networking in the human network.
- Identify the key components of any data network.
- Identify the opportunities and challenges posed by converged networks.
- Describe the characteristics of network architectures: fault tolerance, scalability, quality of service and security.
- Install and use IRC clients and a Wiki server.



IRC Clients and Wiki Server

- Install and use IRC clients and a Wiki server







Communicating over the Network



Network Fundamentals – Chapter 2

Cisco | Networking Academy®
Mind Wide Open™



Objectives

- Describe the structure of a network, including the devices and media that are necessary for successful communications.
- Explain the function of protocols in network communications.
- Explain the advantages of using a layered model to describe network functionality.
- Describe the role of each layer in two recognized network models: The TCP/IP model and the OSI model.
- Describe the importance of addressing and naming schemes in network communications.

Network Structure

- Define the elements of communication
 - 3 common elements of communication
 - message source
 - the channel
 - message destination



- Define a network

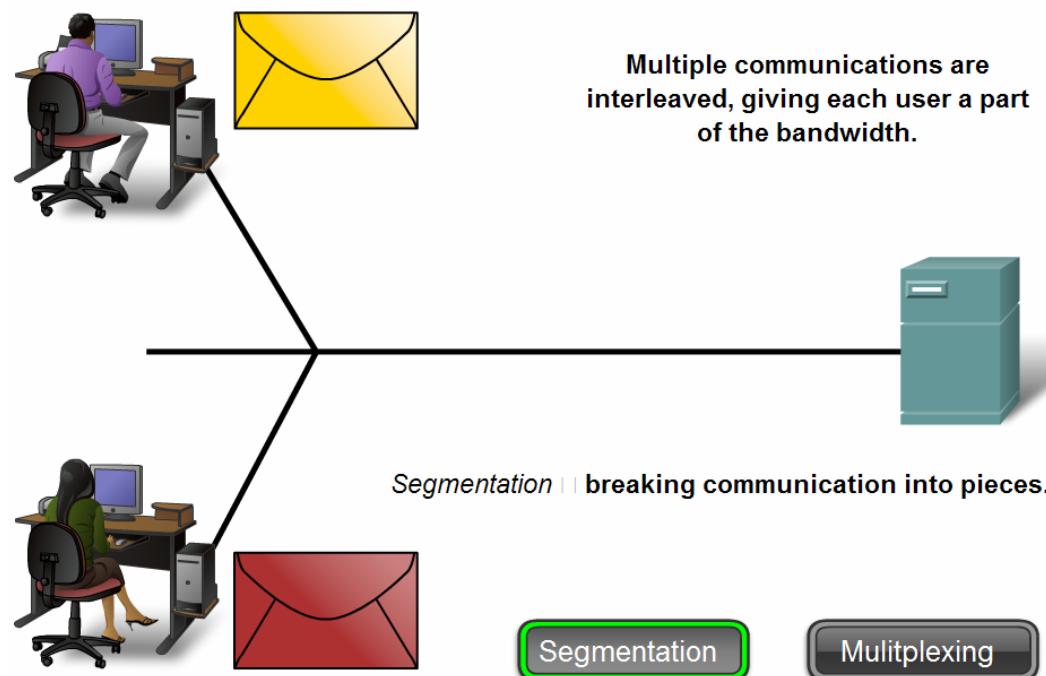
data or information networks capable of carrying many different types of communications

Network Structure

- Describe how messages are communicated

Data is sent across a network in small “chunks” called **segments**

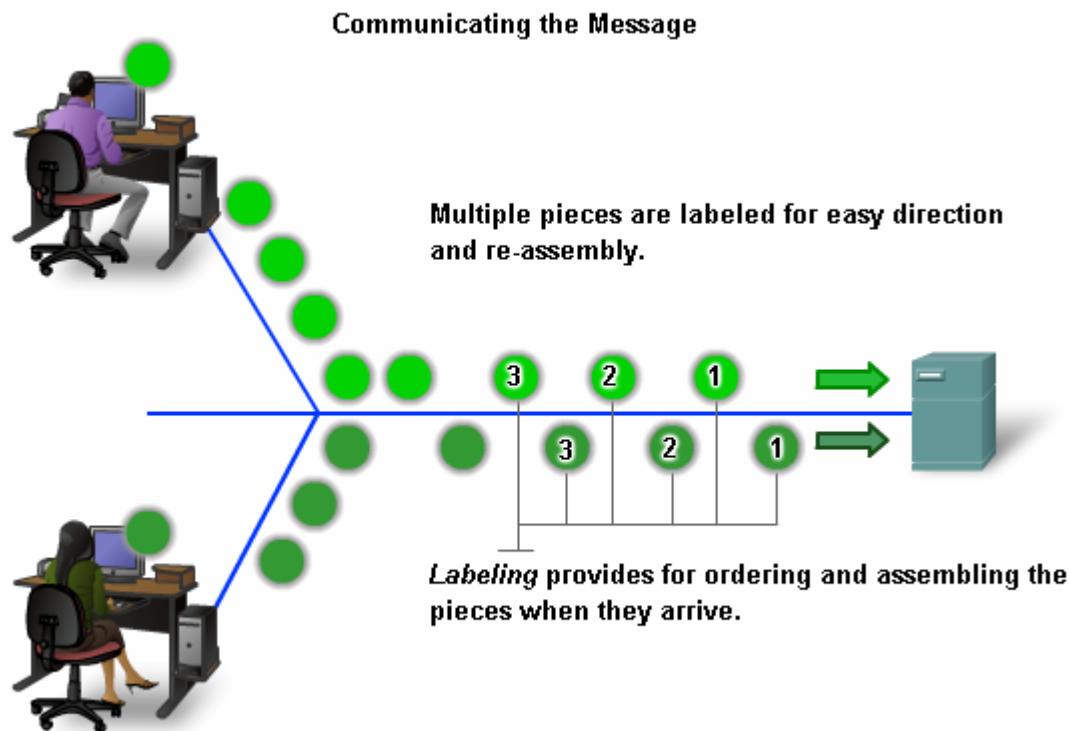
Multiplexing allows for interleaving the pieces as they traverse the media



Network Structure

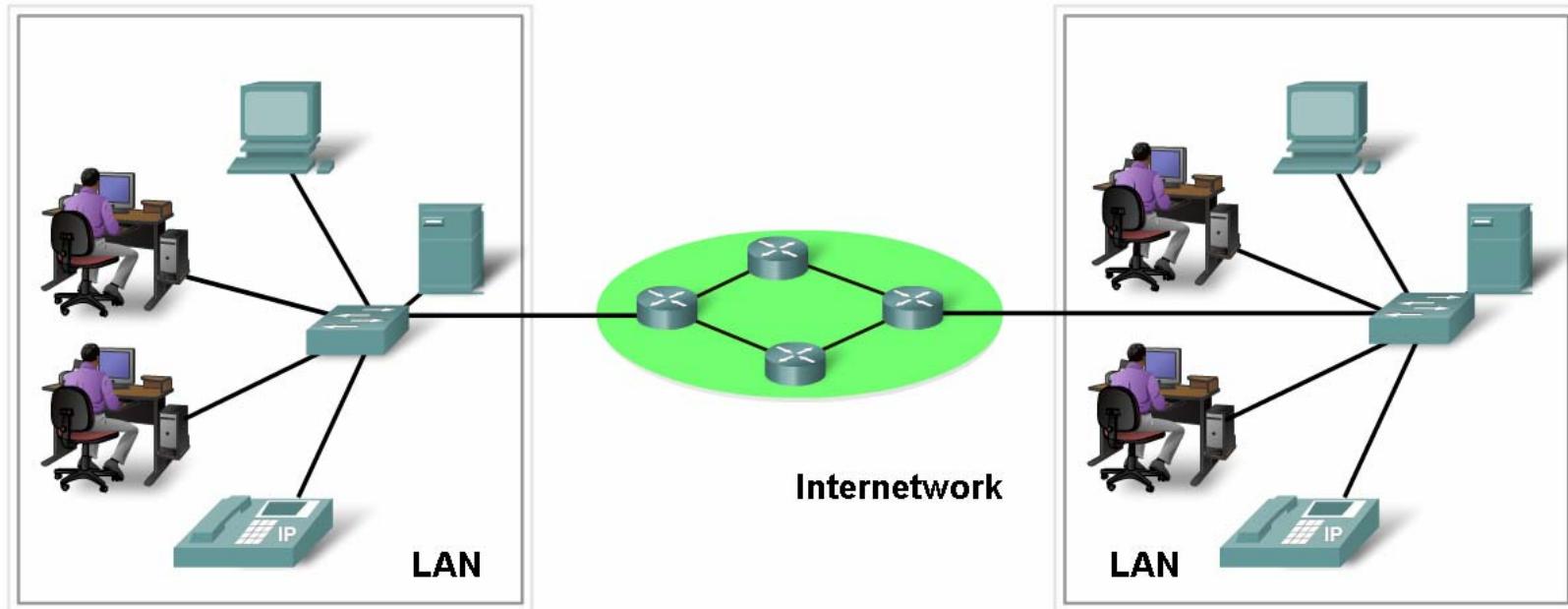
- Describe how messages are communicated

The downside to using segmentation and multiplexing to transmit messages across a network is the level of complexity that is added to the process.



Network Structure

- Define the components of a network
 - Network components
 - hardware (devices, media)
 - software (services)



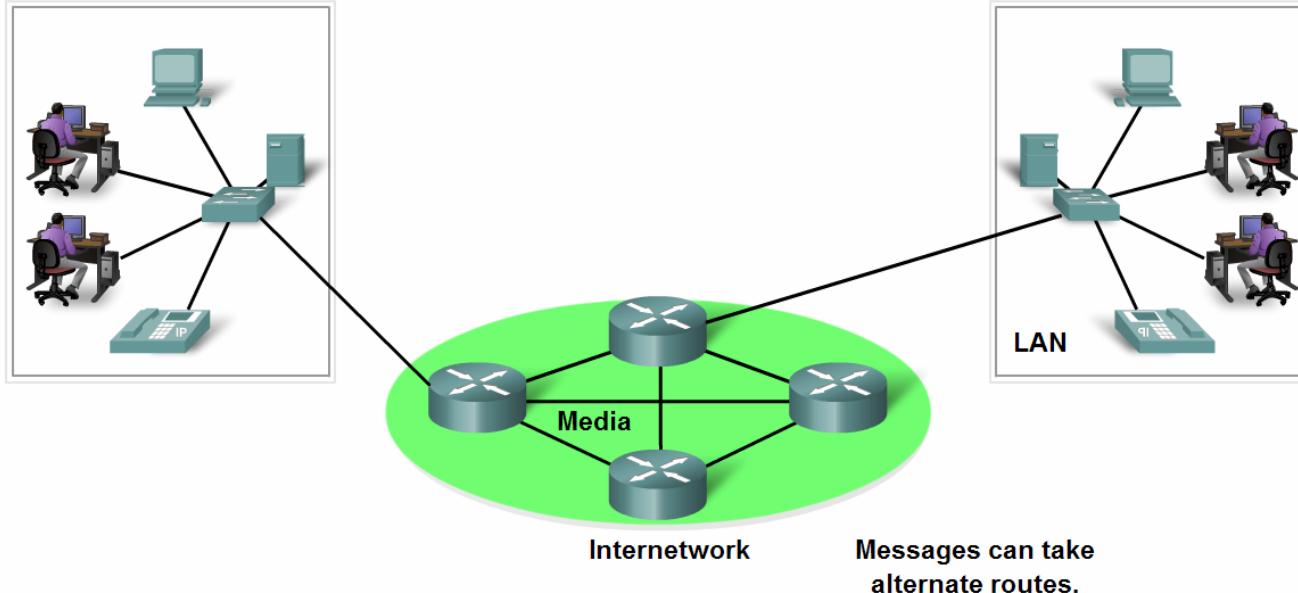
Network Structure

■ End Devices and their Role in the Network

- End devices form interface with human network & communications network
- Role of end devices:

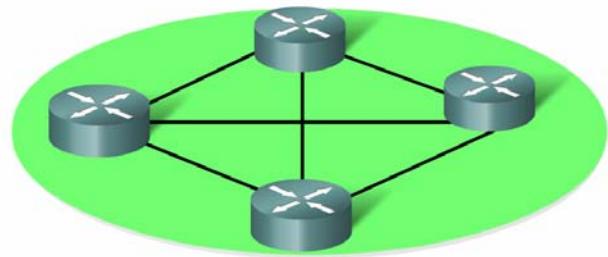
- client
- server
- both client and server

Data originates with an end device, flows through the network and arrives at an end device.



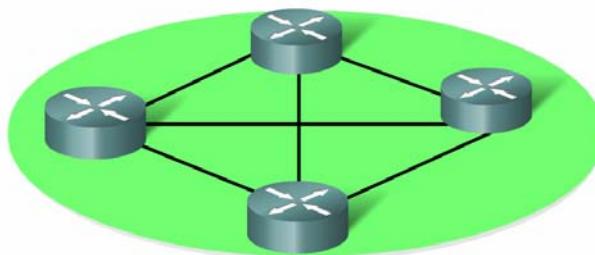
Network Structure

- Identify the role of an intermediary device in a data network and be able to contrast that role with the role of an end device
 - Role of an intermediary device
 - provides connectivity and ensures data flows across network
- Examples of intermediary network devices are:
 - Network Access Devices (Hubs, switches, and wireless access points)
 - Internetworking Devices (routers)
 - Communication Servers and Modems
 - Security Devices (firewalls)



Network Structure

- Processes running on the intermediary network devices perform these functions:
 - Regenerate and retransmit data signals
 - Maintain information about what pathways exist through the network and internetwork
 - Notify other devices of errors and communication failures
 - Direct data along alternate pathways when there is a link failure
 - Classify and direct messages according to QoS priorities
 - Permit or deny the flow of data, based on security settings



Network Structure

- Define network media and criteria for making a network media choice

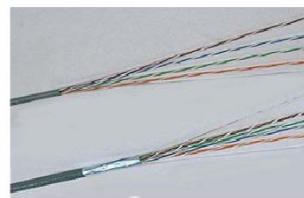
Network media

this is the channel over which a message travels

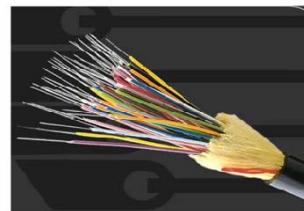
Network Media



Copper



Fiber Optics



Wireless





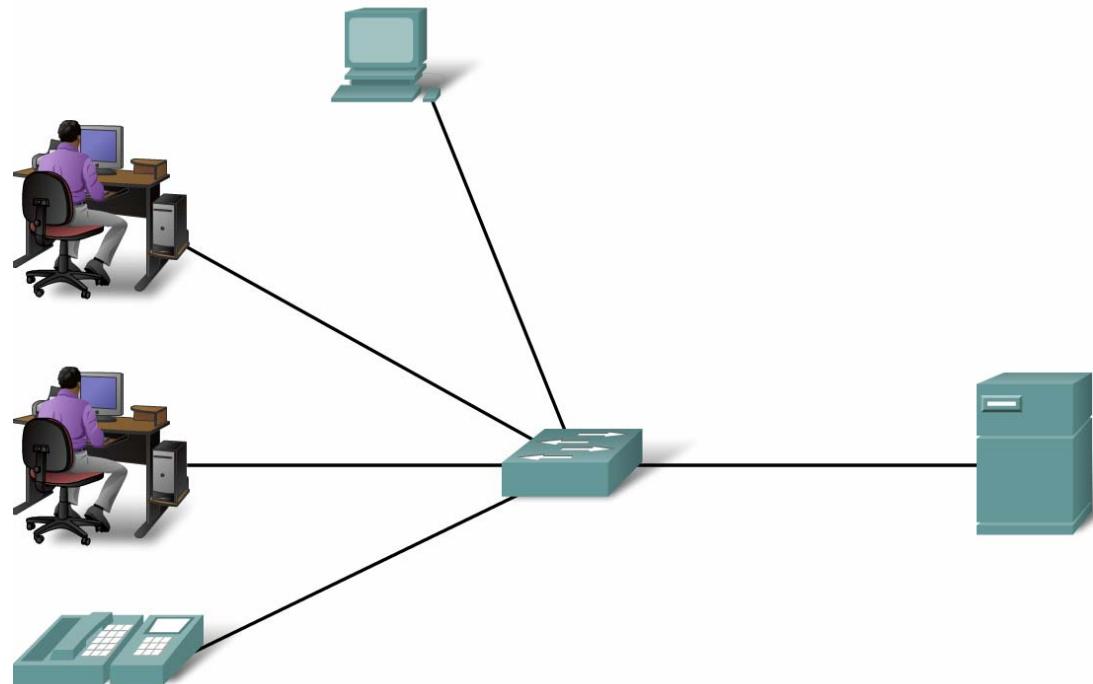
Network Structure

- Define network media and criteria for making a network media choice
 - Criteria for choosing a network media are:
 - The distance the media can successfully carry a signal.
 - The environment in which the media is to be installed.
 - The amount of data and the speed at which it must be transmitted.
 - The cost of the media and installation

Network Types

- Define Local Area Networks (LANs)

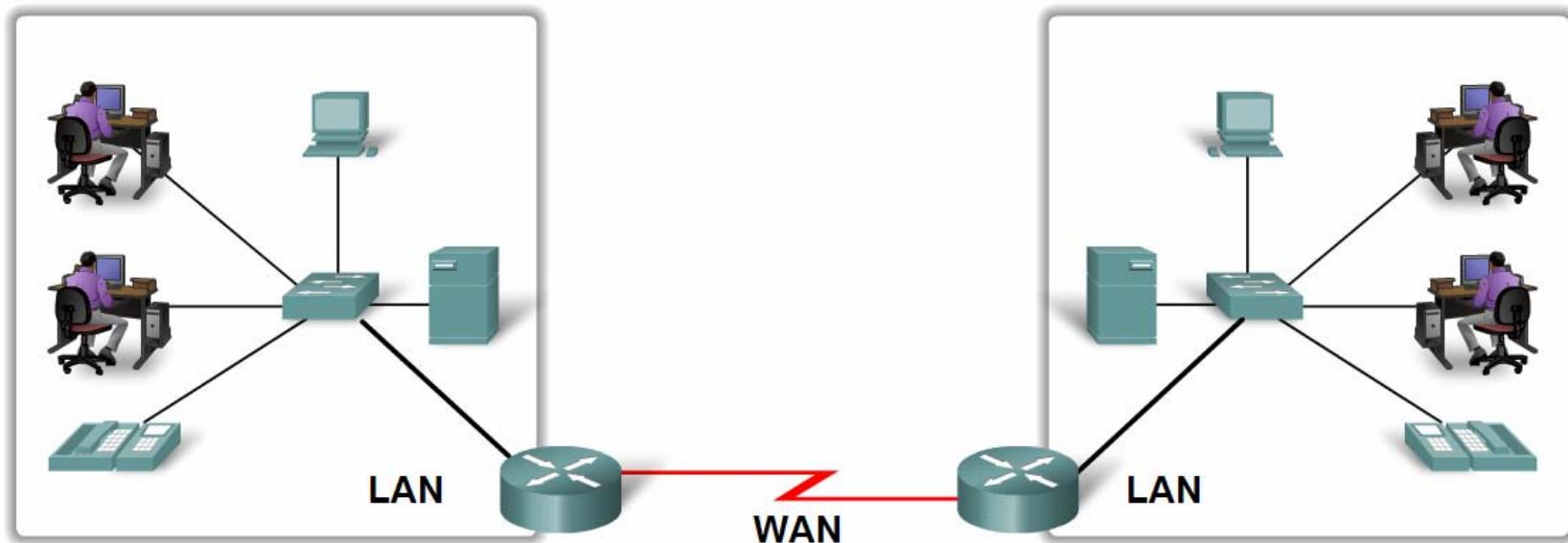
- A network serving a home, building or campus is considered a Local Area Network (LAN)



Network Types

- Define Wide Area Networks (WANs)

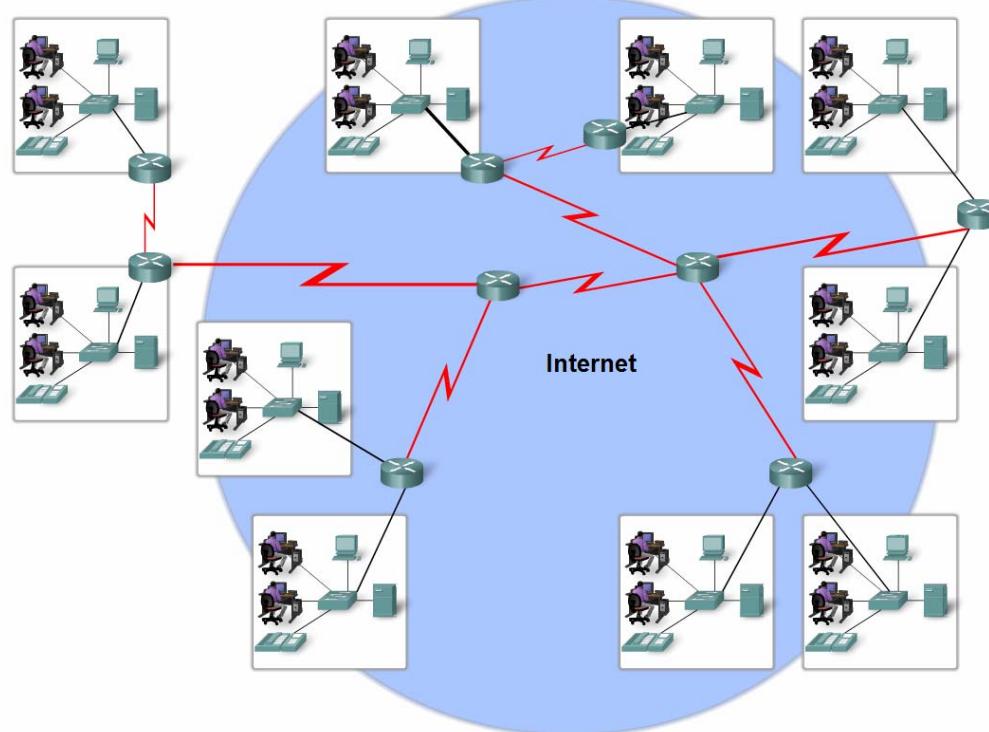
- LANs separated by geographic distance are connected by a network known as a Wide Area Network (WAN)



Network Types

- Define the Internet

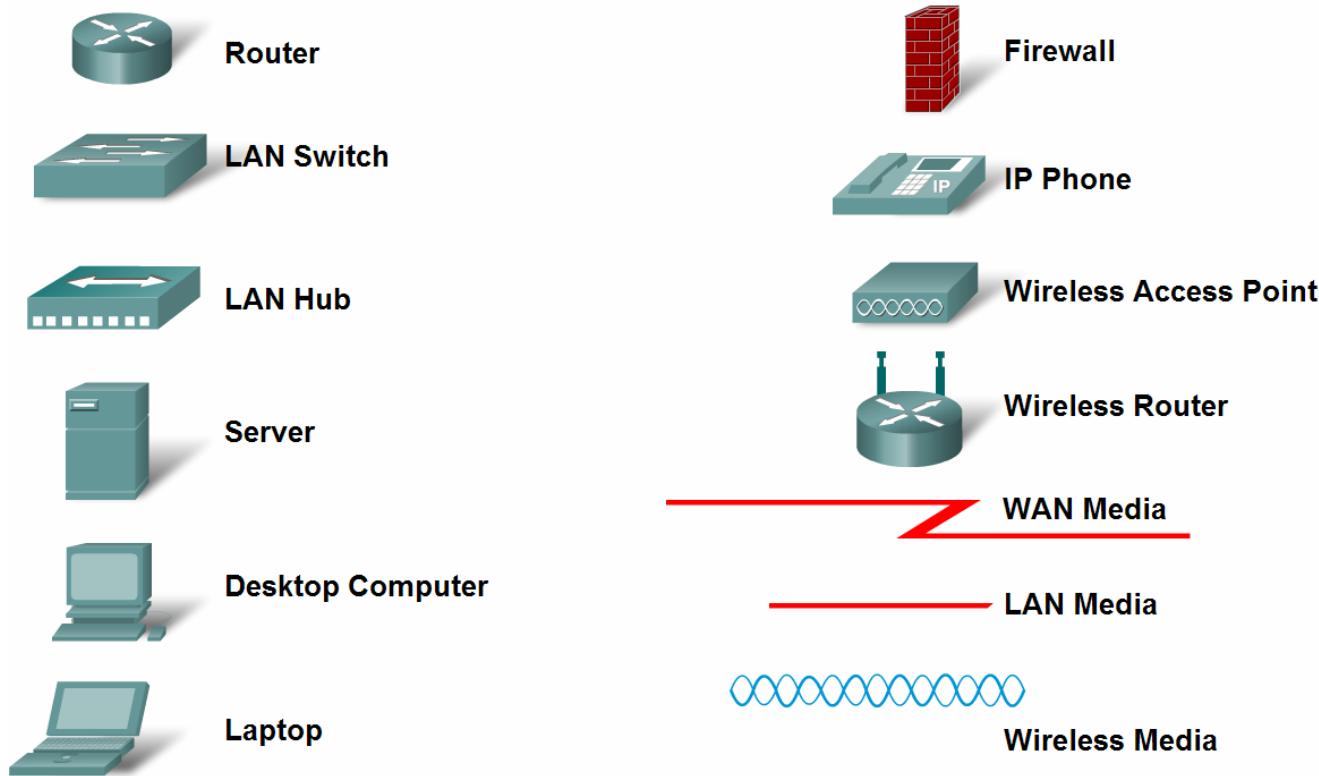
The internet is defined as a
global mesh of interconnected networks



Network Types

- Describe network representations

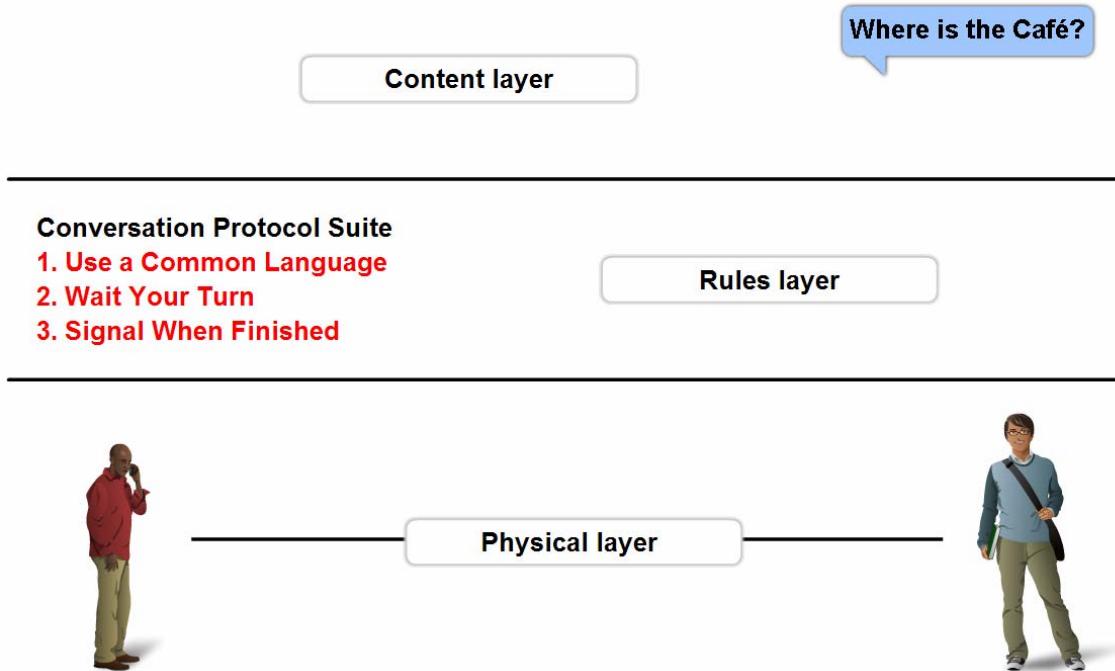
Common Data Network Symbols



Function of Protocol in Network Communication

- The importance of protocols and how they are used to facilitate communication over data networks

A protocol is a set of predetermined rules





Function of Protocol in Network Communication

- Explain network protocols

Network protocols are used to allow devices to communicate successfully

Proprietary VS Open

Protocols provide:

The format or structure of the message

The process by which networking devices share information about pathways to other networks

How and when error and system messages are passed between devices

The setting up and termination of data transfer sessions



Function of Protocol in Network Communication

- Describe Protocol suites and industry standards

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

Where is the Café?

Content layer

Conversation Protocol Suite

- 1. Use a Common Language
 - 2. Wait Your Turn
 - 3. Signal When Finished
-

Rules layer



Physical layer

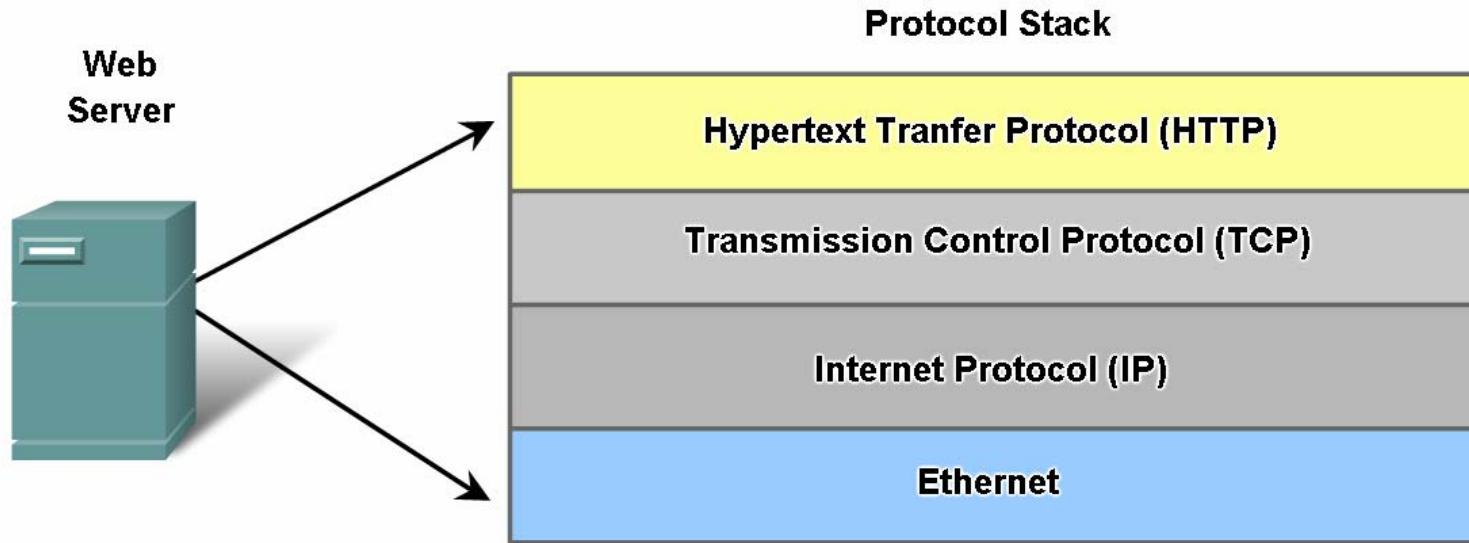


A standard is

a process or protocol that has been endorsed by the networking industry and ratified by a standards organization

Function of Protocol in Network Communication

- Define different protocols and how they interact



HTTP - governs web server and a web client interaction

TCP - manages the individual conversations between web servers and web clients

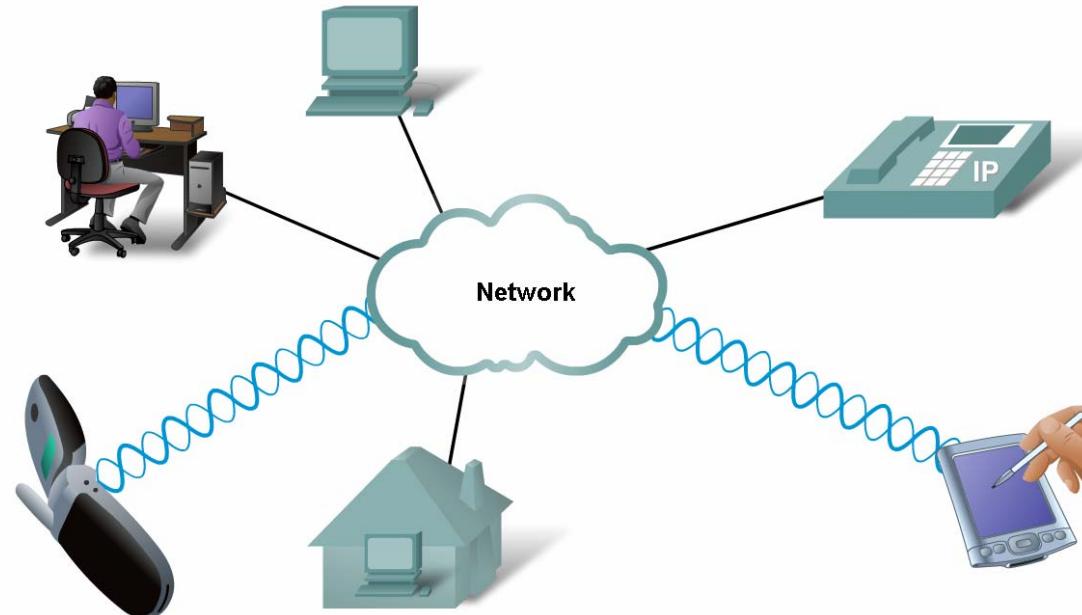
IP - selecting the best path to the destination host.

Media access - governs how the signals are sent over the media and how they are interpreted by the receiving clients.

Function of Protocol in Network Communication

- Technology independent Protocols

- Many diverse types of devices can communicate using the same sets of protocols. This is because protocols specify network functionality, not the underlying technology to support this functionality.



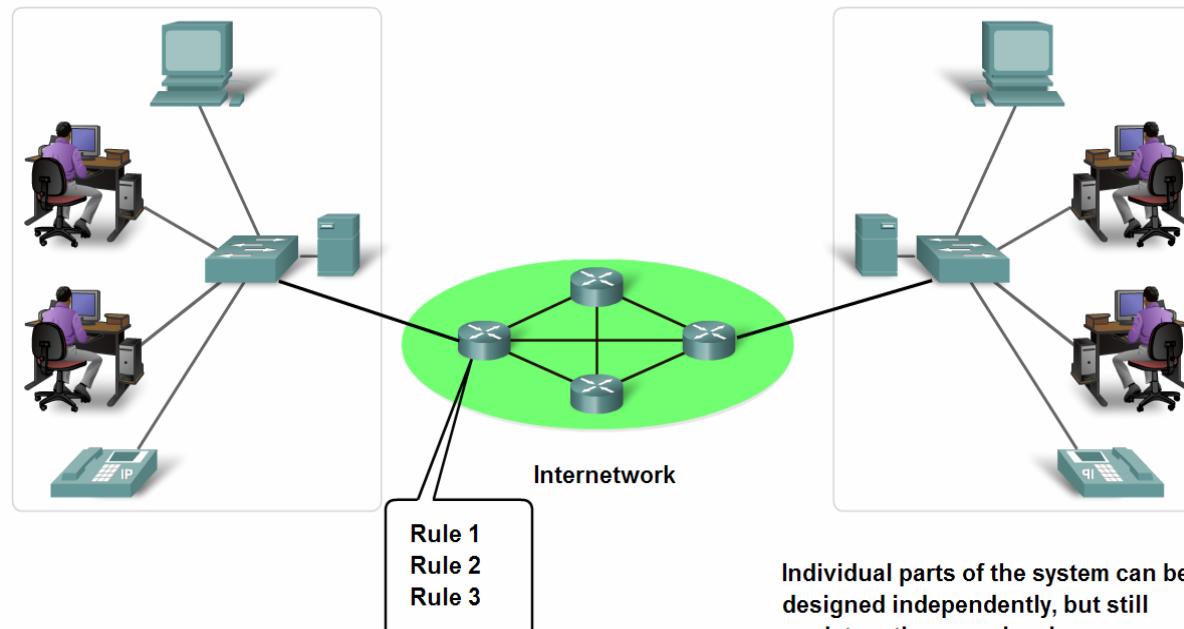
Layers with TCP/IP and OSI Model

- Explain the benefits of using a layered model

- Benefits include

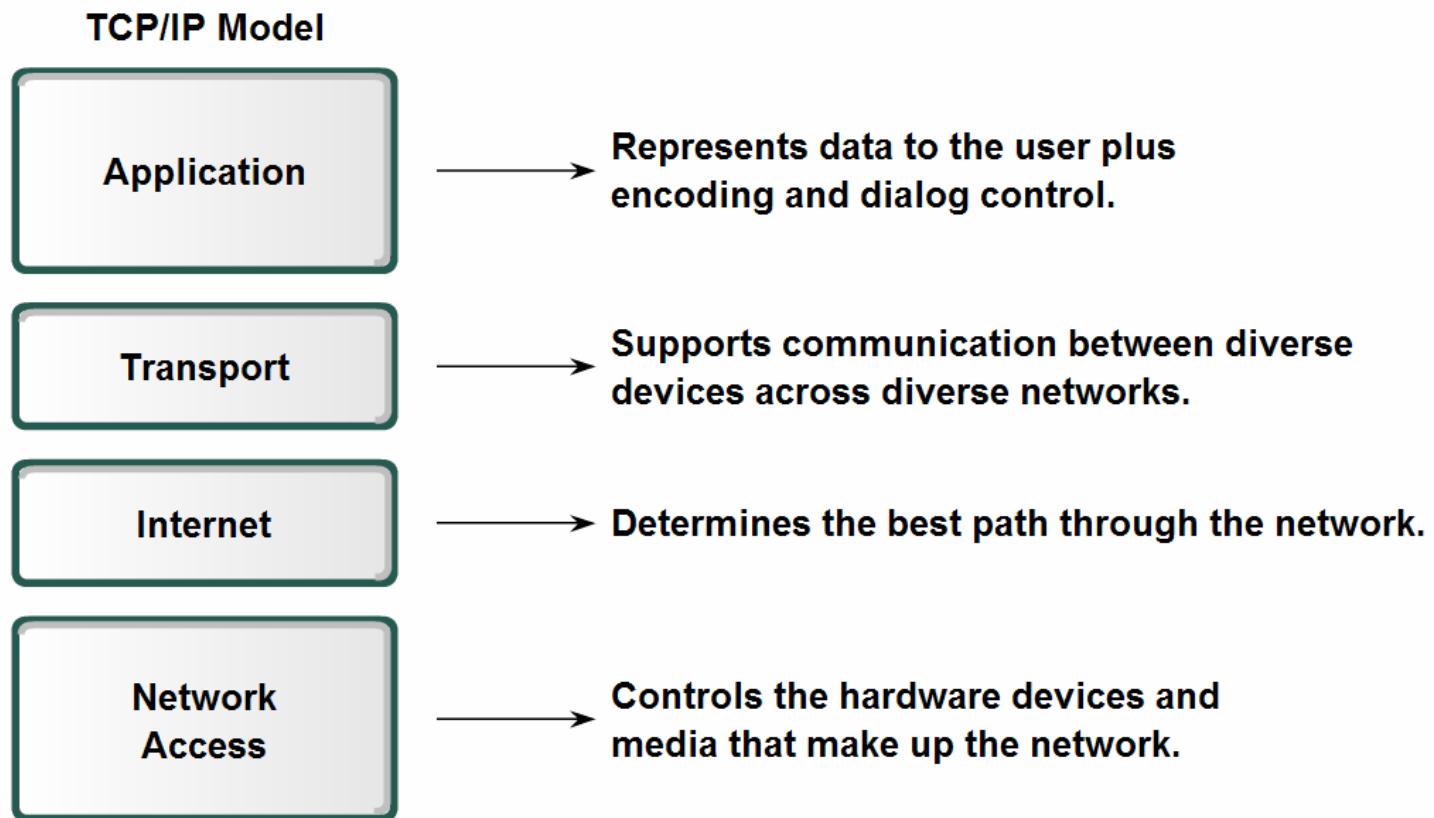
- assists in protocol design
 - fosters competition
 - changes in one layer do not affect other layers
 - provides a common language

Using a layered model helps in the design of complex, multi-use, multi-vendor networks.



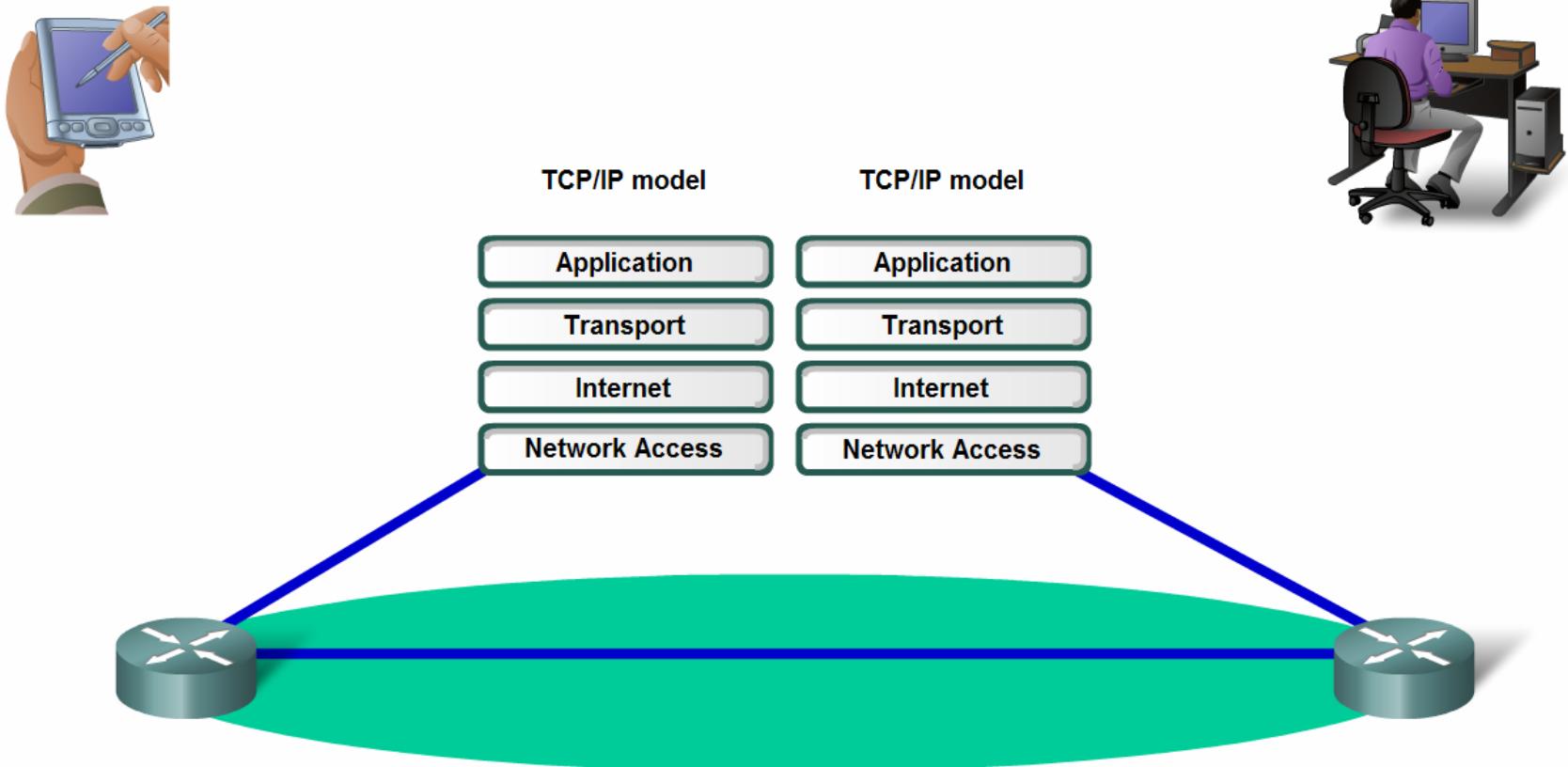
Layers with TCP/IP and OSI Model

- Describe TCP/IP Model



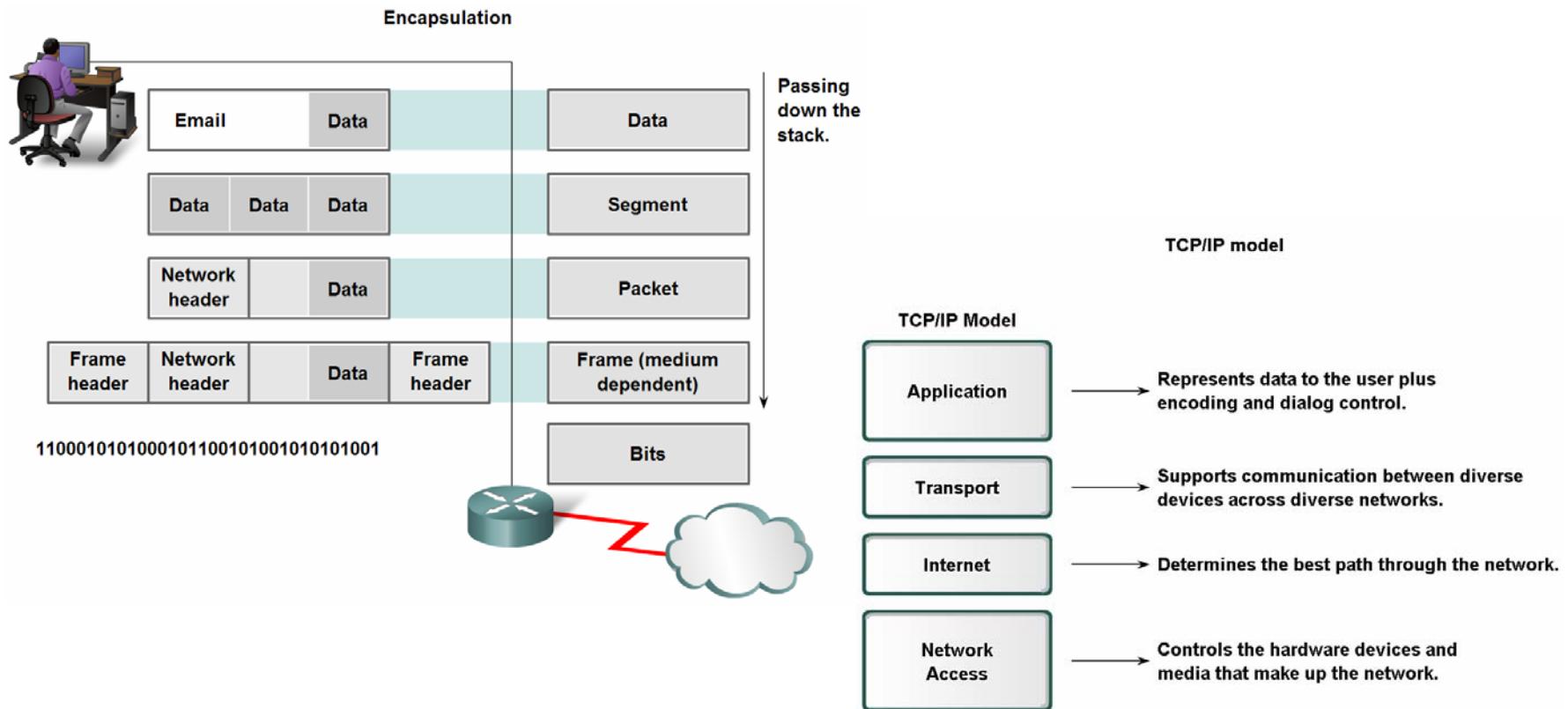
Layers with TCP/IP and OSI Model

- Describe the Communication Process



Layers with TCP/IP and OSI Model

- Explain protocol data units (PDU) and encapsulation

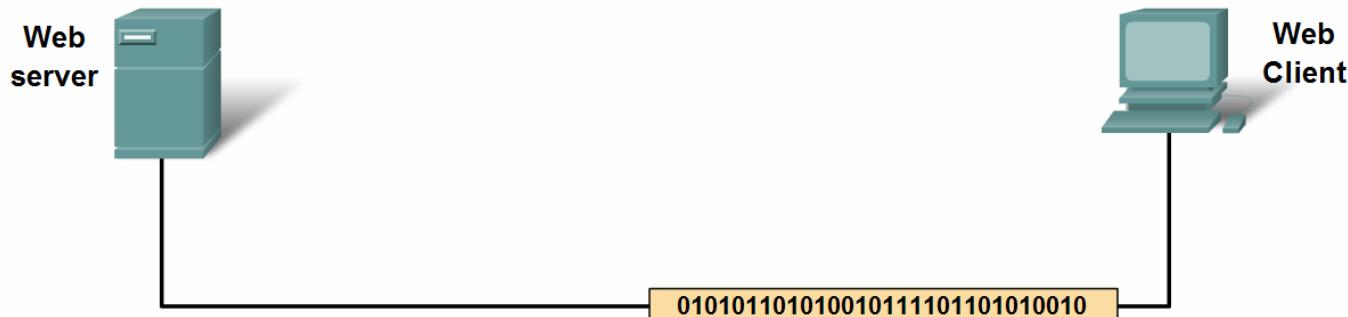
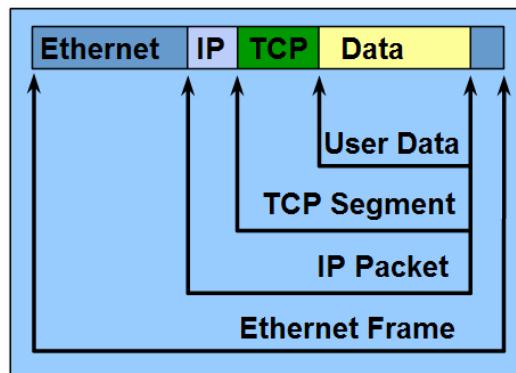


Layers with TCP/IP and OSI Model

- Describe the process of sending and receiving messages

Protocol Operation of Sending and Receiving a Message

Protocol Encapsulation Terms



Layers with TCP/IP and OSI Model

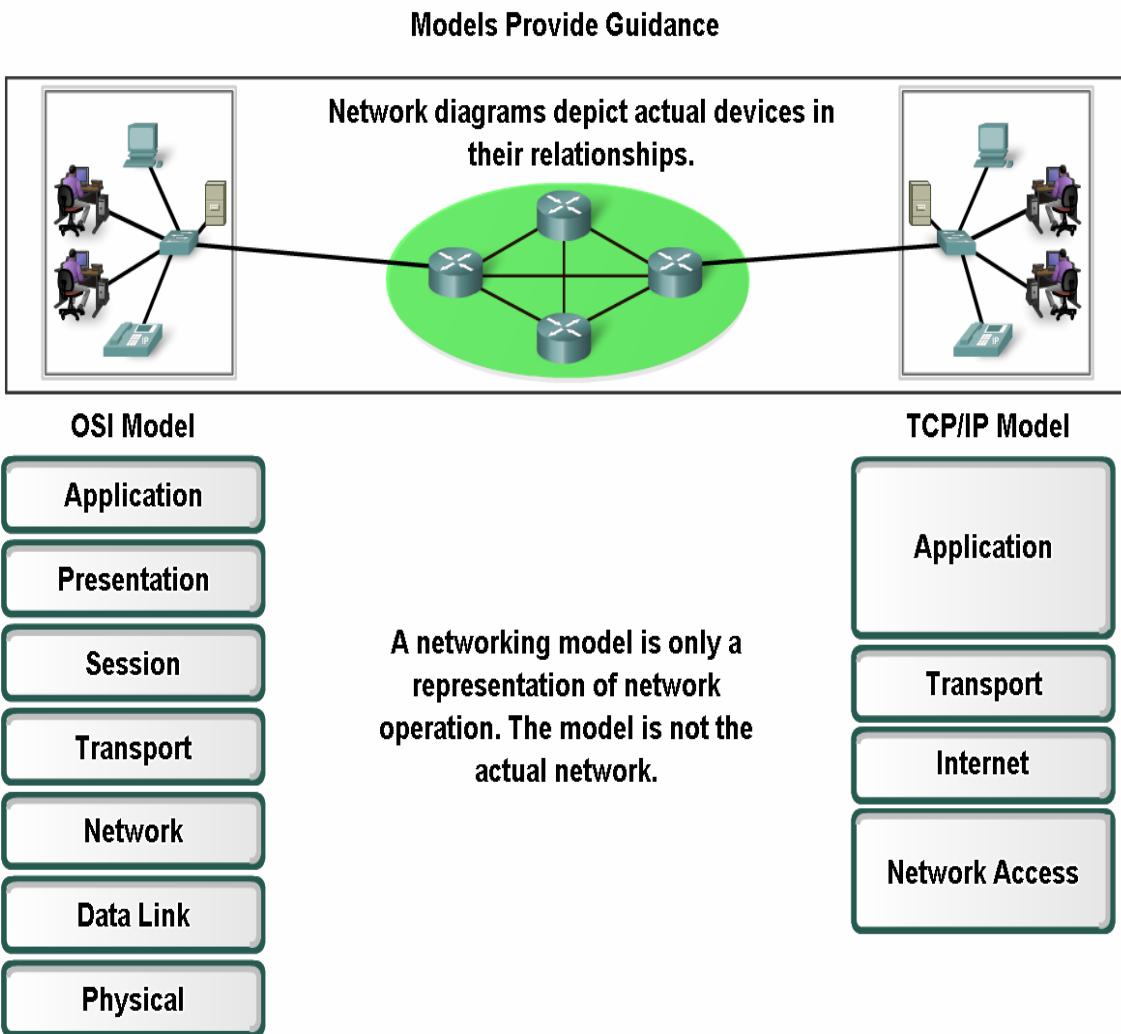
- Explain protocol and reference models

A protocol model

provides a model that closely matches the structure of a particular protocol suite.

A reference model

provides a common reference for maintaining consistency within all types of network protocols and services.



Layers with TCP/IP and OSI Model

- Define OSI

7. Application

6. Presentation

5. Session

4. Transport

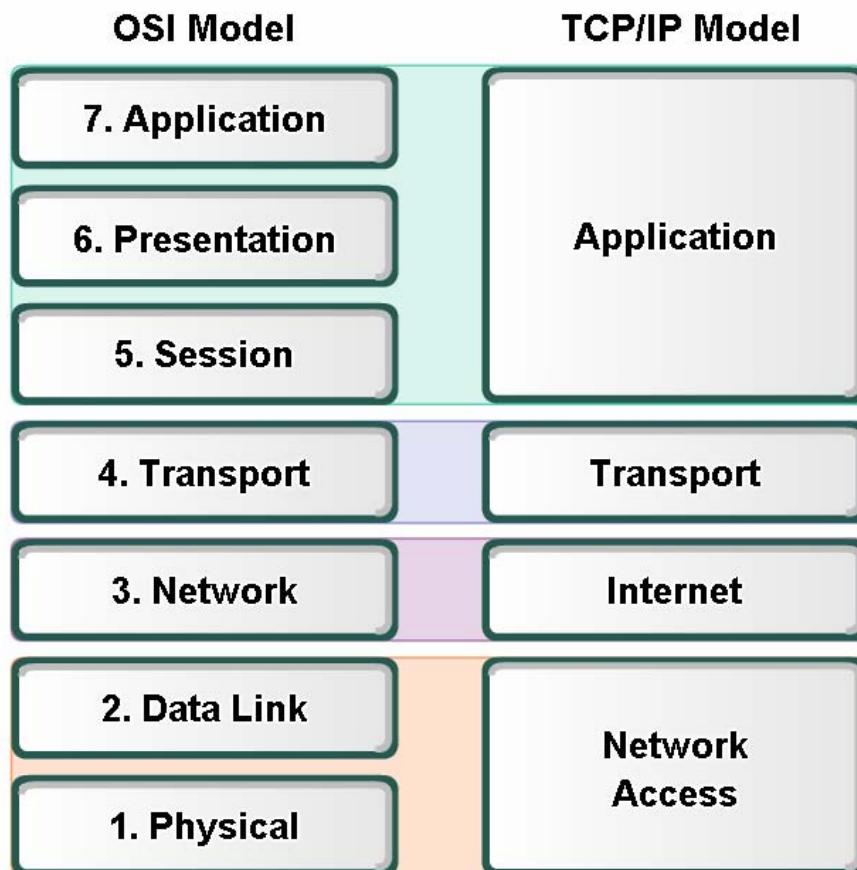
3. Network

2. Data Link

1. Physical

Layers with TCP/IP and OSI Model

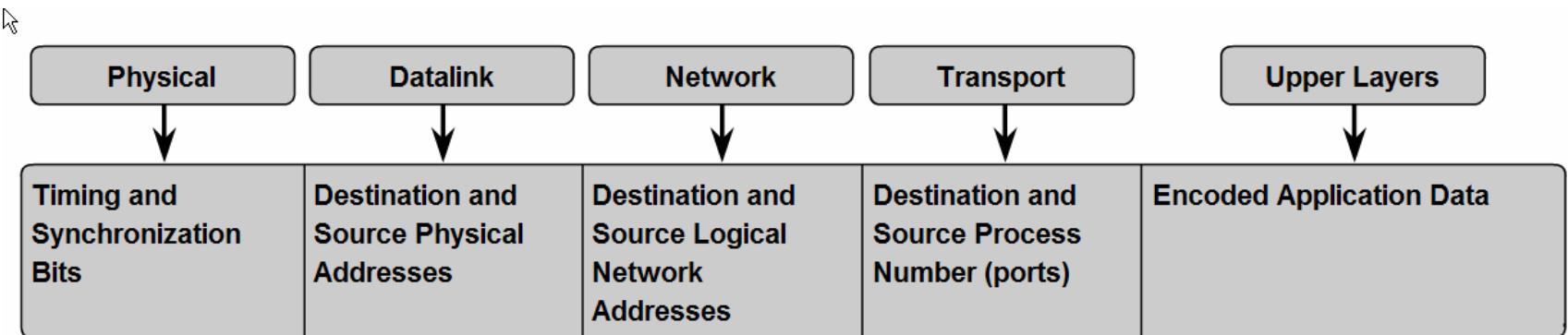
- Compare OSI and TCP/IP model



The key parallels are in the Transport and Network layers.

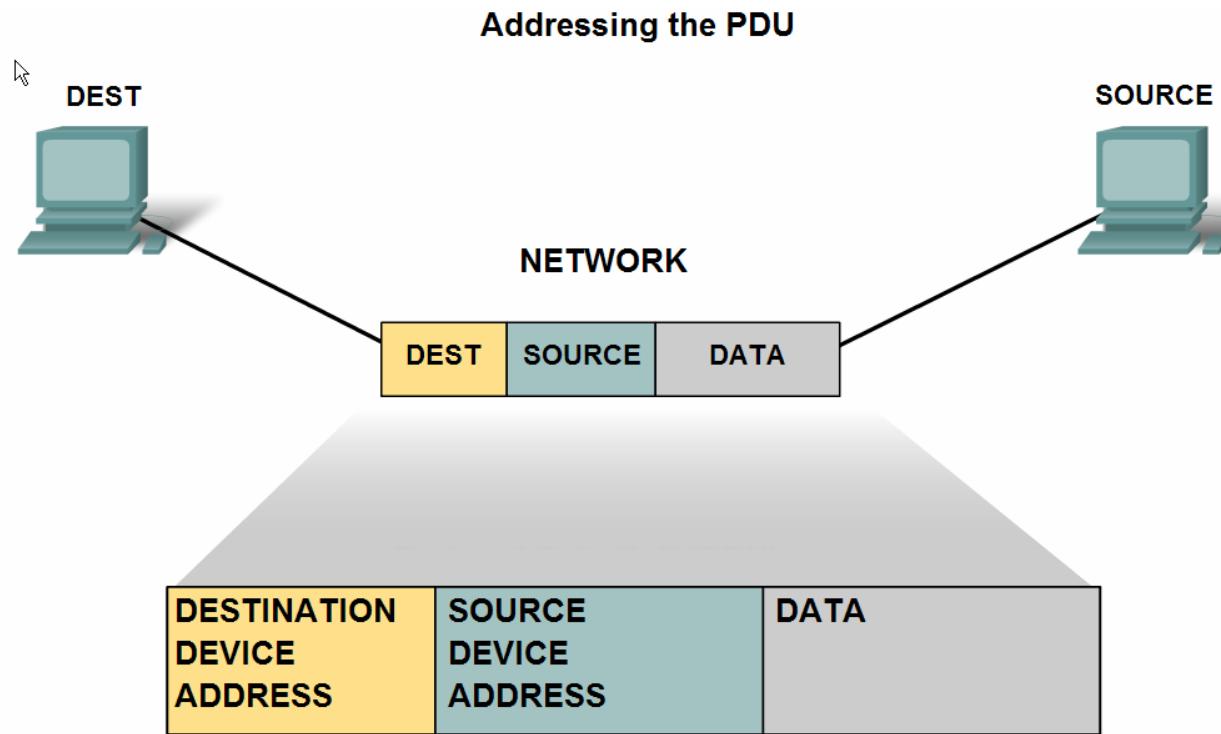
Addressing and Naming Schemes

- Explain how labels in encapsulation headers are used to manage communication in data networks



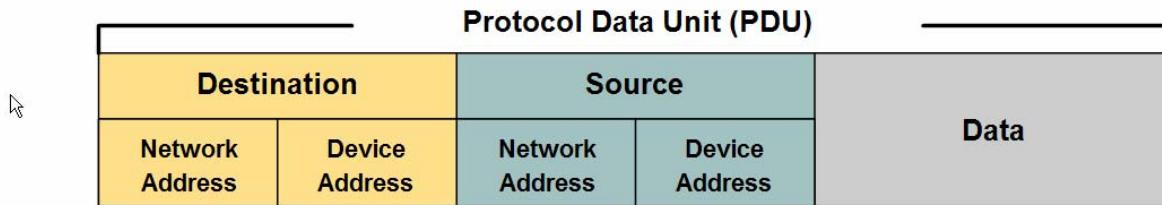
Addressing and Naming Schemes

- Describe examples of Ethernet MAC Addresses, IP Addresses, and TCP/UDP Port numbers

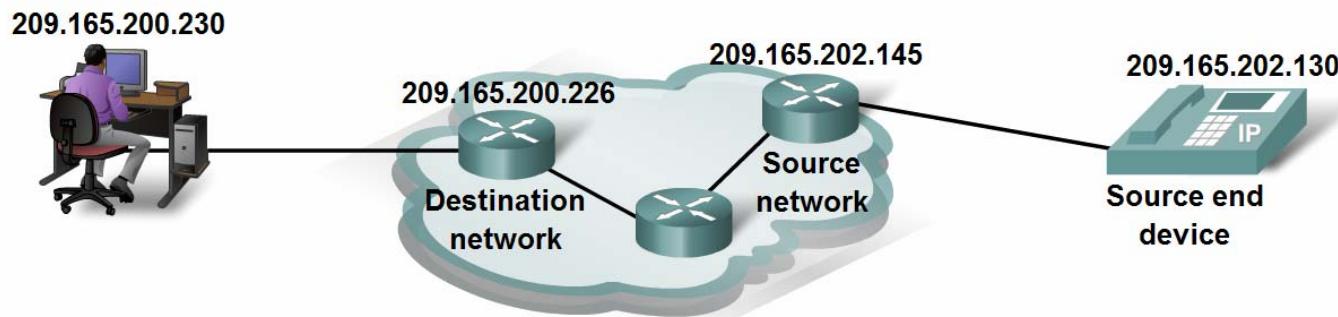


Addressing and Naming Schemes

- Explain how labels in encapsulation headers are used to manage communication in data networks



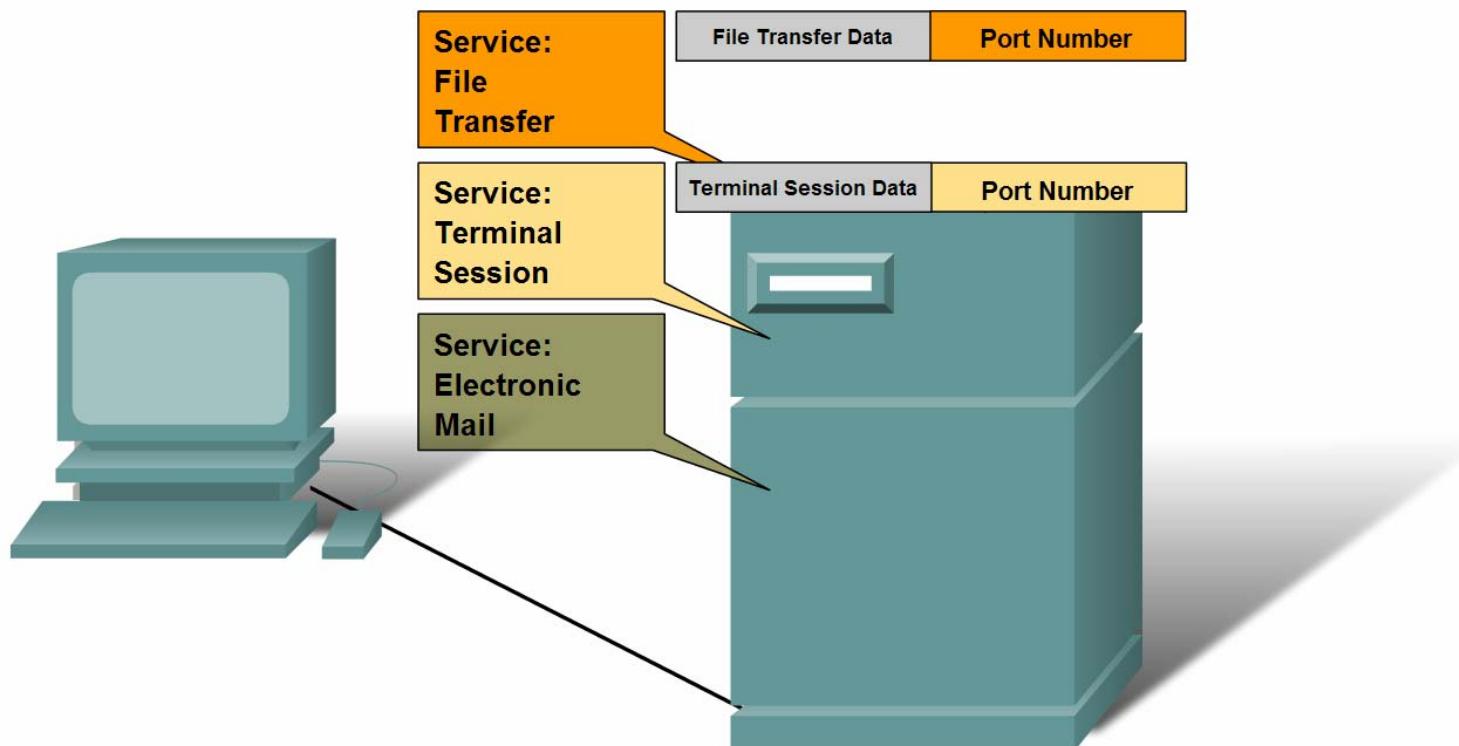
The Protocol Data Unit header also contains the network address.



Addressing and Naming Schemes

- Describe how information in the encapsulation header is used to identify the source and destination processes for data communication

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





Summary

In this chapter, you learned to:

- Describe the structure of a network, including the devices and media that are necessary for successful communications.
- Explain the function of protocols in network communications.
- Explain the advantages of using a layered model to describe network functionality.
- Describe the role of each layer in two recognized network models: The TCP/IP model and the OSI model.
- Describe the importance of addressing and naming schemes in network communications.





Application Layer Functionality and Protocols



Network Fundamentals – Chapter 3

Cisco | Networking Academy®
Mind Wide Open™

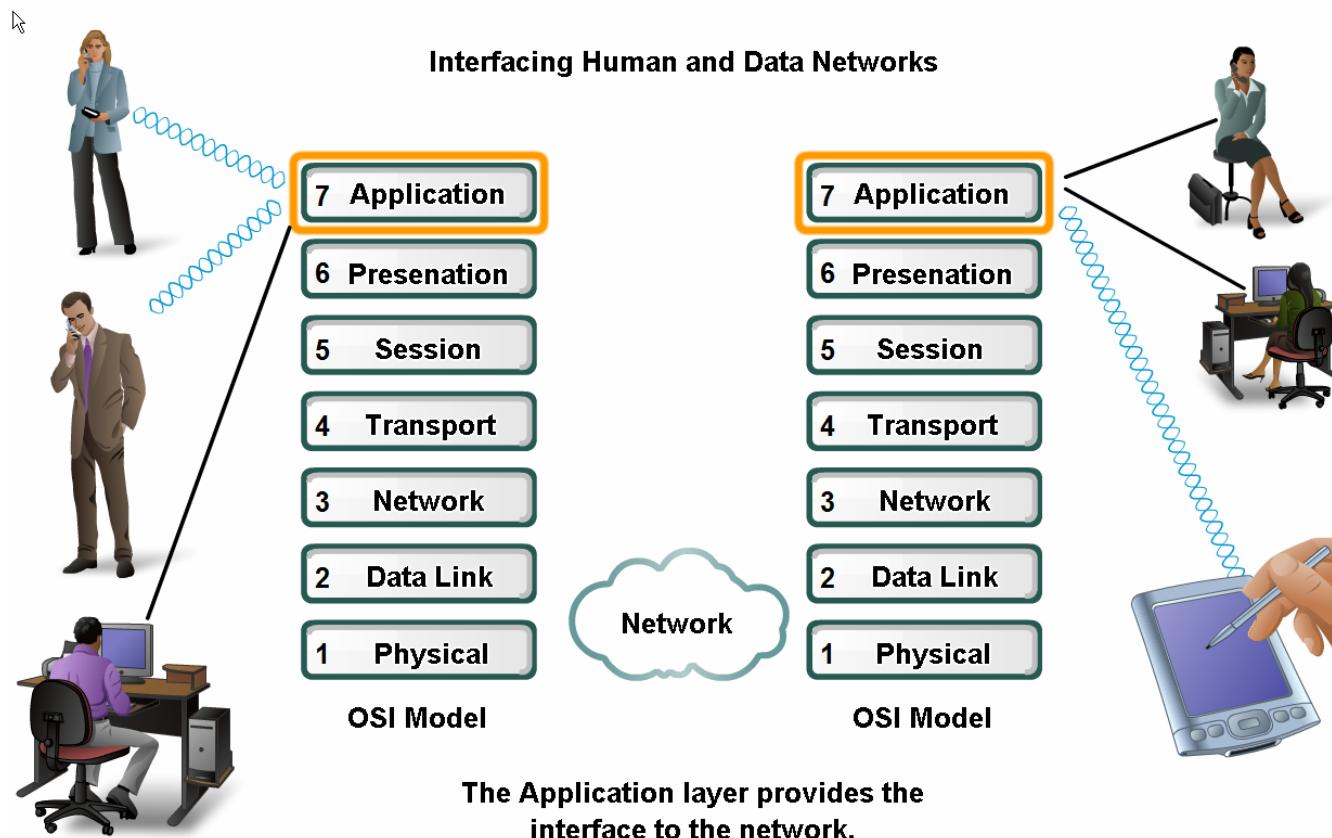


Objectives

- Define the application layer as the source and destination of data for communication across networks.
- Explain the role of protocols in supporting communication between server and client processes.
- Describe the features, operation, and use of well-known TCP/IP application layer services (HTTP, DNS, SMTP).

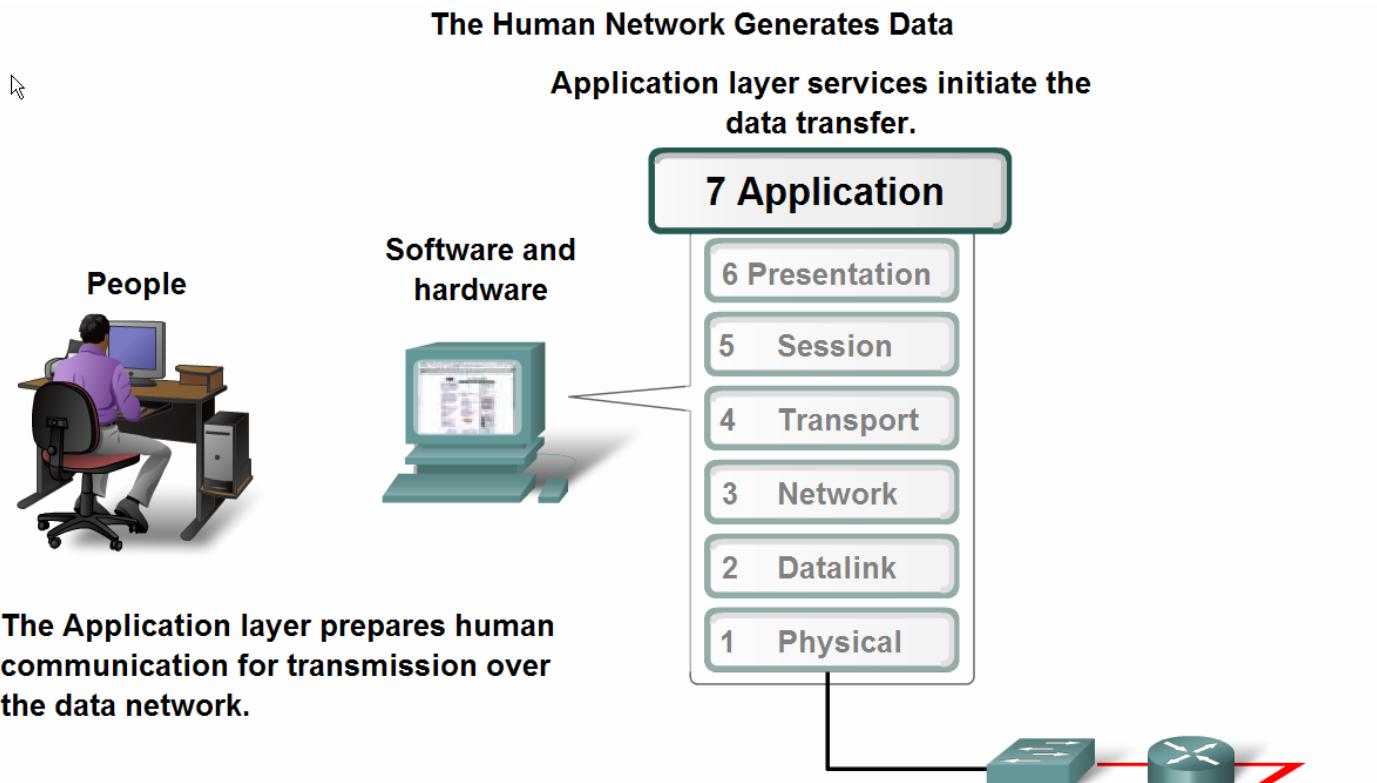
Applications – The Interface Between Human and Data Networks

- Applications provide the means for generating and receiving data that can be transported on the network



Applications – The Interface Between Human and Data Networks

- The role of applications, services and protocols in converting communication to data that can be transferred across the data network
- Fig 3.1.1.1



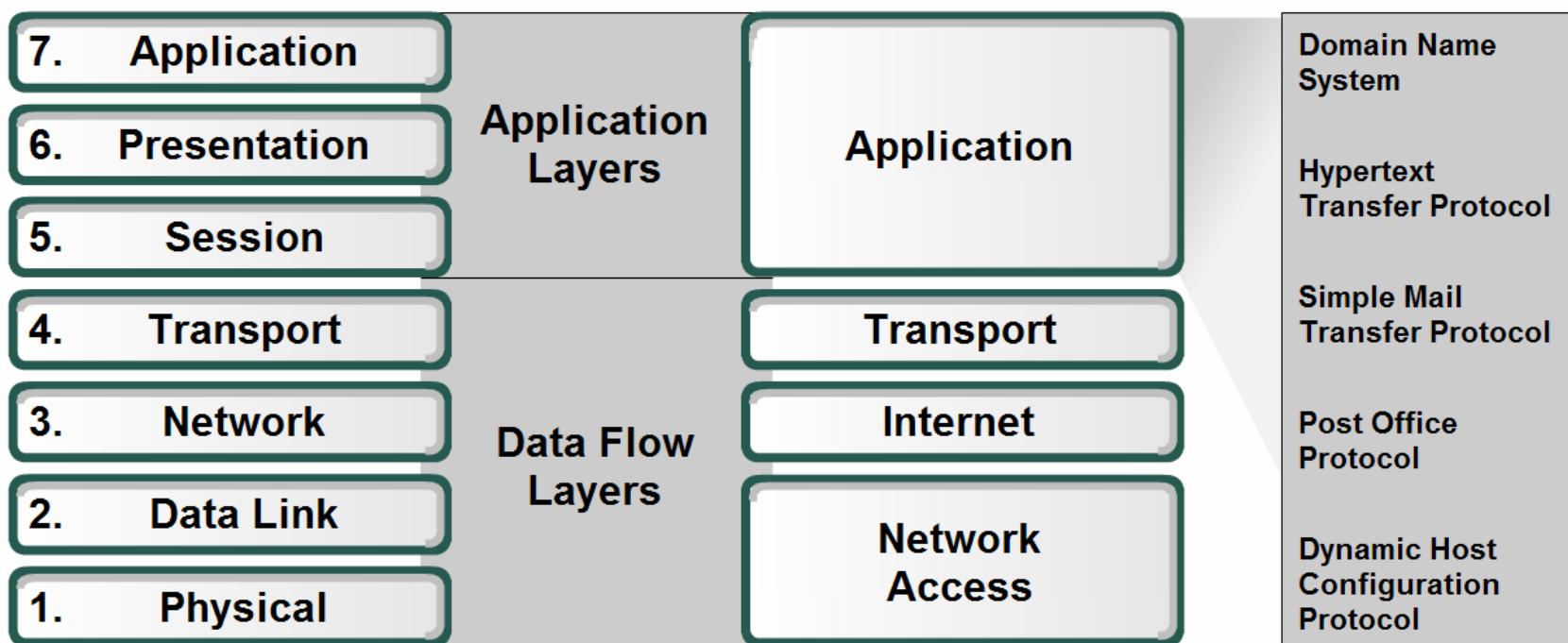
Applications – The Interface Between Human and Data Networks

- Define the separate roles applications, services and protocols play in transporting data through networks



OSI Model

TCP/IP Model



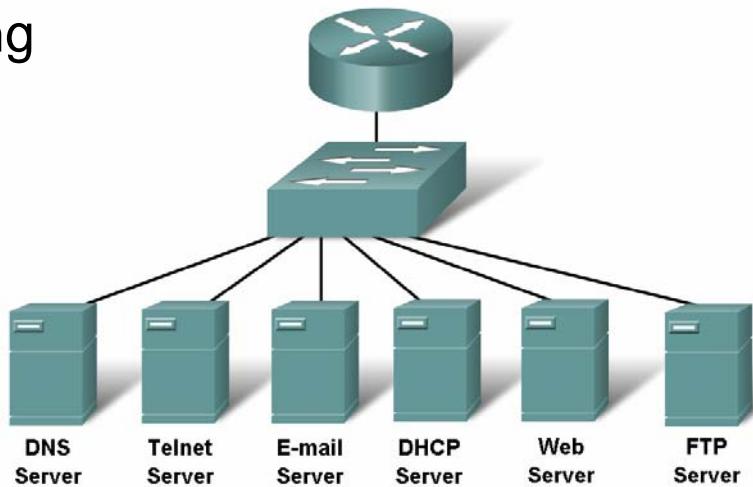


Applications – The Interface Between Human and Data Networks

- **Presentation layer** has three primary functions:
 - Coding and conversion** of Application layer data to ensure that data from the source device can be interpreted by the appropriate application on the destination device (e.g MPEG)
 - Compression** of the data in a manner that can be decompressed by the destination device (e.g. GIF, JPEG)
 - Encryption** of the data for transmission and the decryption of data upon receipt by the destination.
- **Session layer** - create and maintain dialogs between source and destination applications. It also handles the exchange of information to initiate dialogs, keep them active, and to restart sessions that are disrupted or idle for a long period of time.

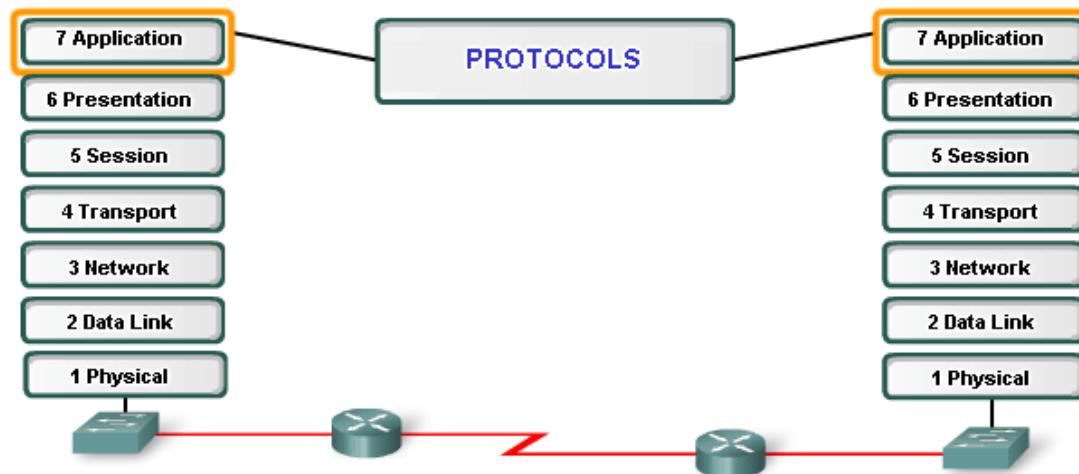
Applications – The Interface Between Human and Data Networks

- Within the Application layer, there are two forms of software programs or processes that provide access to the network: **applications** and **services**.
- Network-Aware Applications** - implement the application layer protocols and are able to communicate directly with the lower layers of the protocol stack (e.g. E-mail clients, web browsers)
- Application layer Services** - other programs may need the assistance of Application layer services to use network resources, like file transfer or network print spooling
- Fig. 3.1.2.1, Fig. 3.1.3.1



The Role of Protocols in Supporting Communication

- Application layer protocols are used by both the source and destination devices during a communication session.
- Application layer protocols implemented on the source and destination host must match.



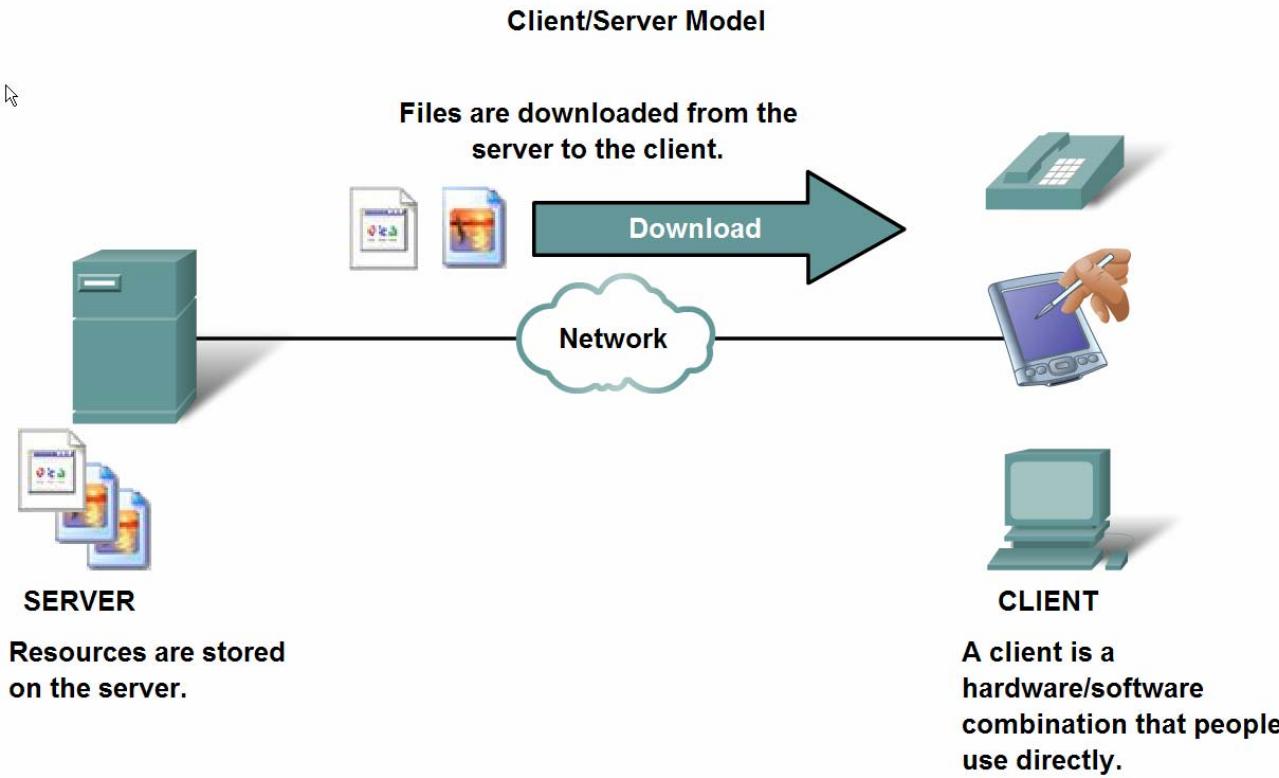
Application layer protocols provide the rules for communication between applications.

Protocols:

- Define processes on either end of the communication
- Define the types of messages
- Define the syntax of messages
- Define the meaning of any informational fields
- Define how messages are sent and the expected response
- Define interaction with the next lower layer

The Role of Protocols in Supporting Communication

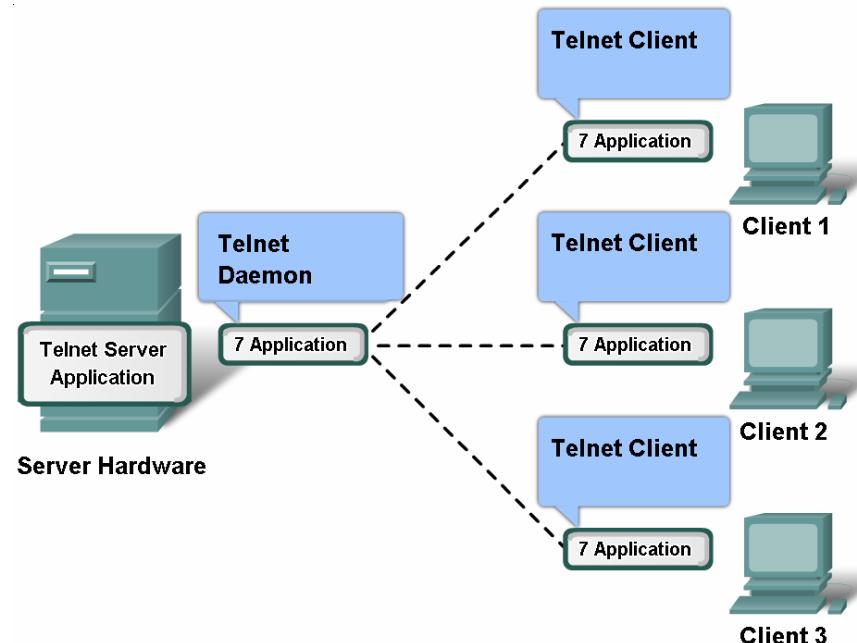
- **Client/server** model in data networks.
- Any device that responds to requests from client applications is functioning as a **server**. A server is usually a computer that contains information to be shared with many client systems.



The Role of Protocols in Supporting Communication

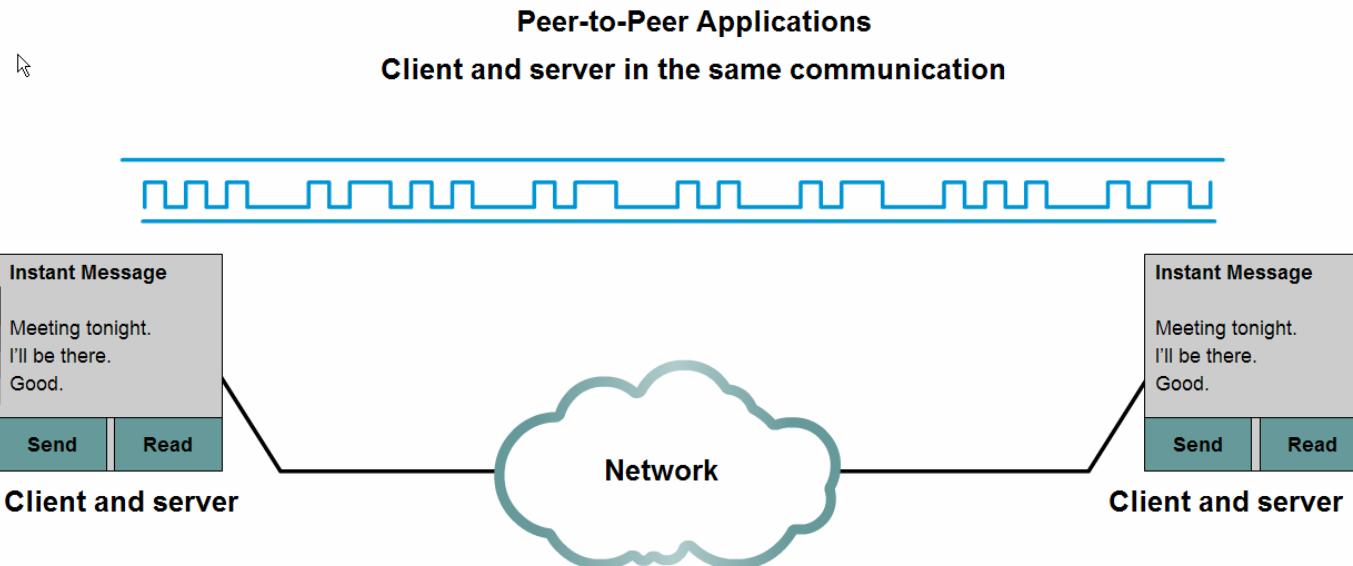
- In a client/server network, the server runs a service, or process, sometimes called a server **daemon**.
- Daemons** typically run in the background and are not under an end user's direct control. They „listen” for a request from a client, because they are programmed to respond whenever the server receives a request for the service provided by the daemon

Server processes may support multiple clients.



The Role of Protocols in Supporting Communication

- Client/server model vs. peer-to-peer model (P2P)
- Peer-to-peer applications (allows a device to act as both a client and a server within the same communication)



Both clients:

- Initiate a message
- Receive a message

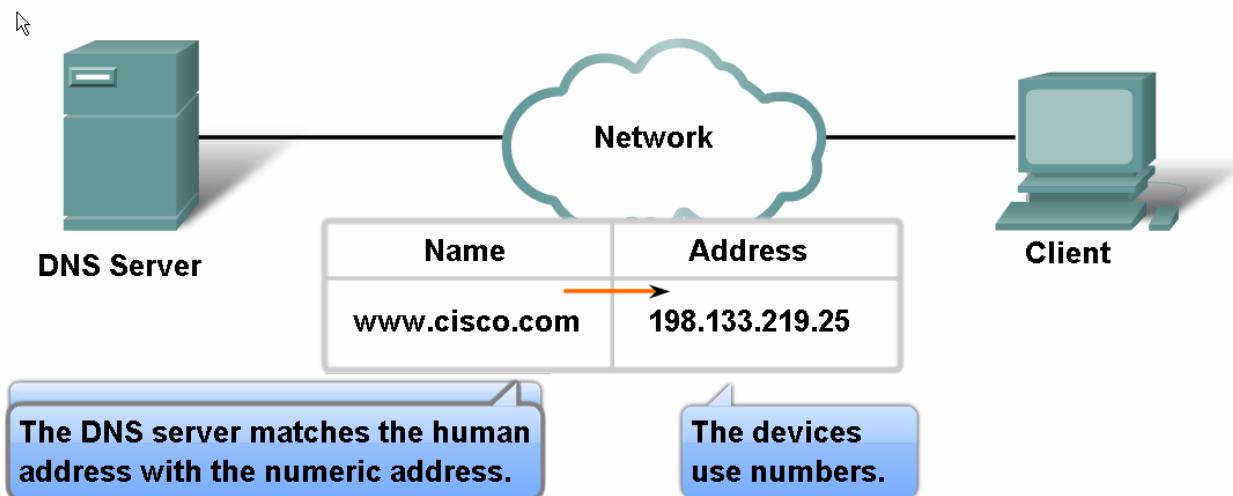
Both clients simultaneously:

- Send
- Receive

Features, Operation, and Use of TCP/IP Application Layer Services

- The features of the **DNS** (Domain Name System) protocol and how this protocol supports DNS services
- TCP/UDP port 53 – Fig. 3.3.1.1
- nslookup**

Resolving DNS Addresses





Features, Operation, and Use of TCP/IP Application Layer Services

- The **ipconfig /displaydns** command displays all of the cached DNS entries on a Windows XP or 2000 computer system

DNS Message Format

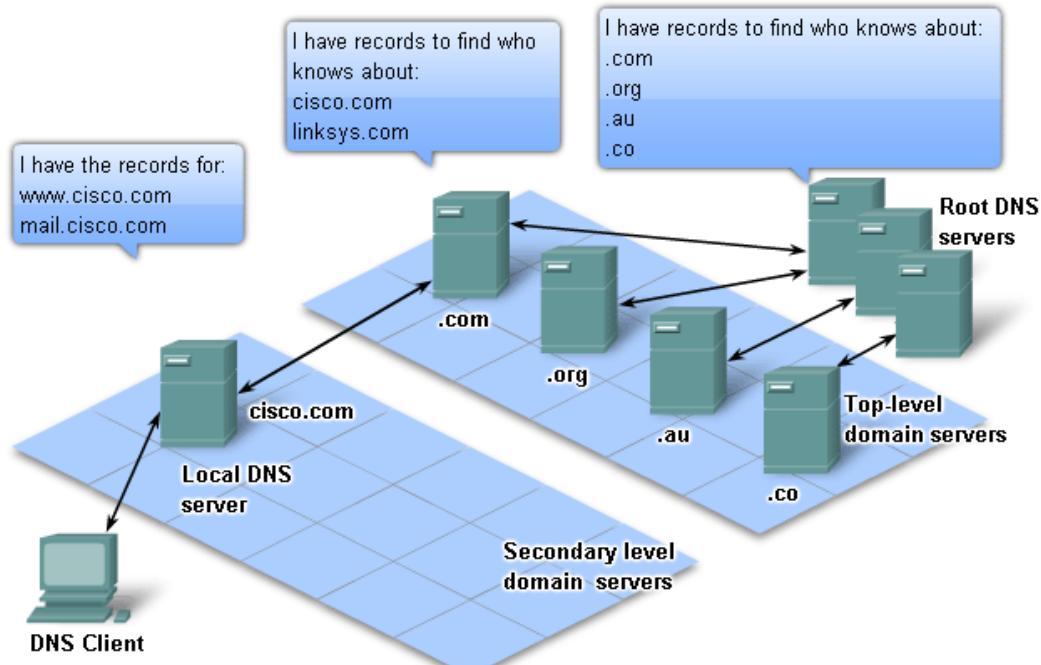
DNS uses the same message format for:

- all types of client queries and server responses
- error messages
- the transfer of resource record information between servers

Header	
Question	The question for the name server
Answer	Resource Records answering the question
Authority	Resource Records pointing toward an authority
Additional	Resource Records holding additional information

Features, Operation, and Use of TCP/IP Application Layer Services

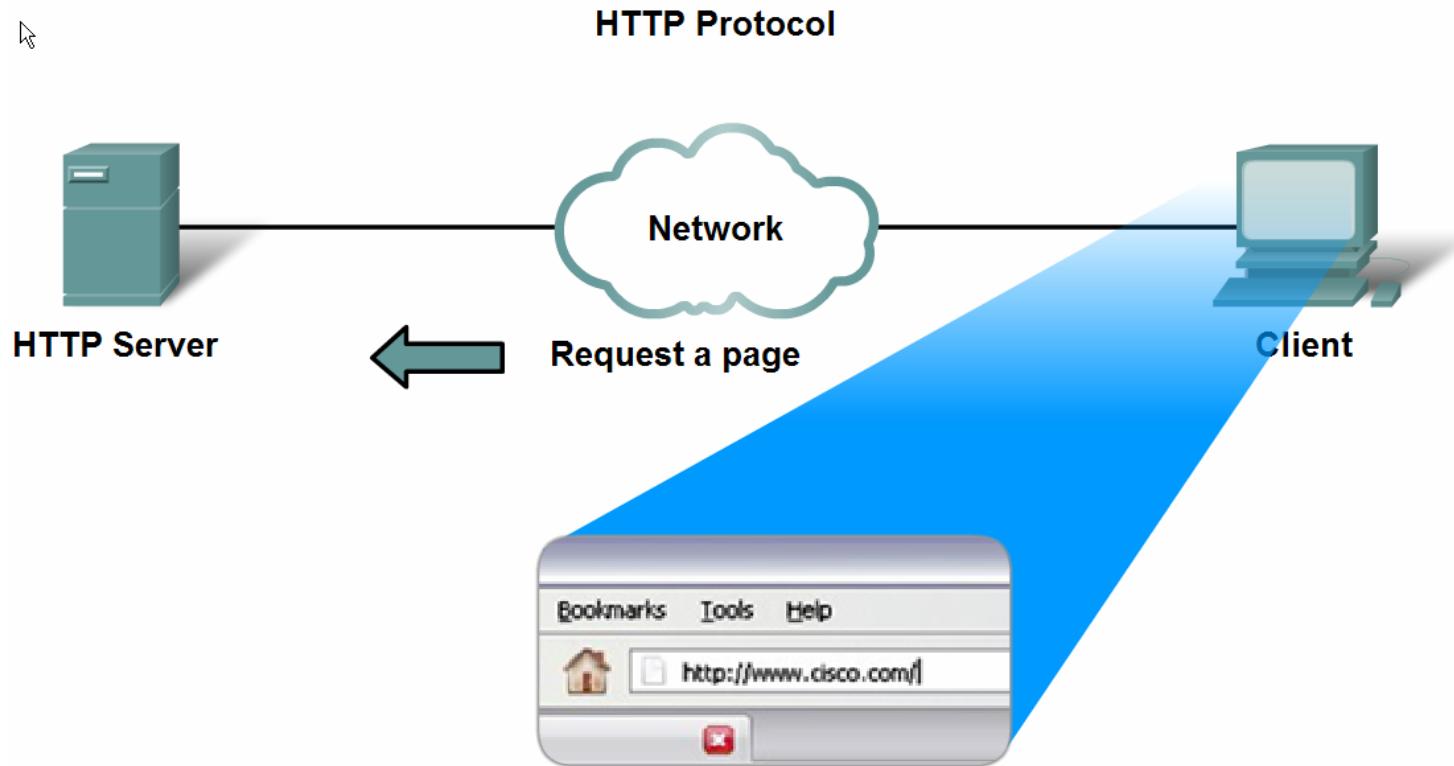
- DNS uses a hierarchical system to create a name database to provide name resolution.
- If a given server has resource records that correspond to its level in the domain hierarchy, it is said to be **authoritative** for those records.



A hierarchy of DNS servers contains the resource records that match names with addresses.

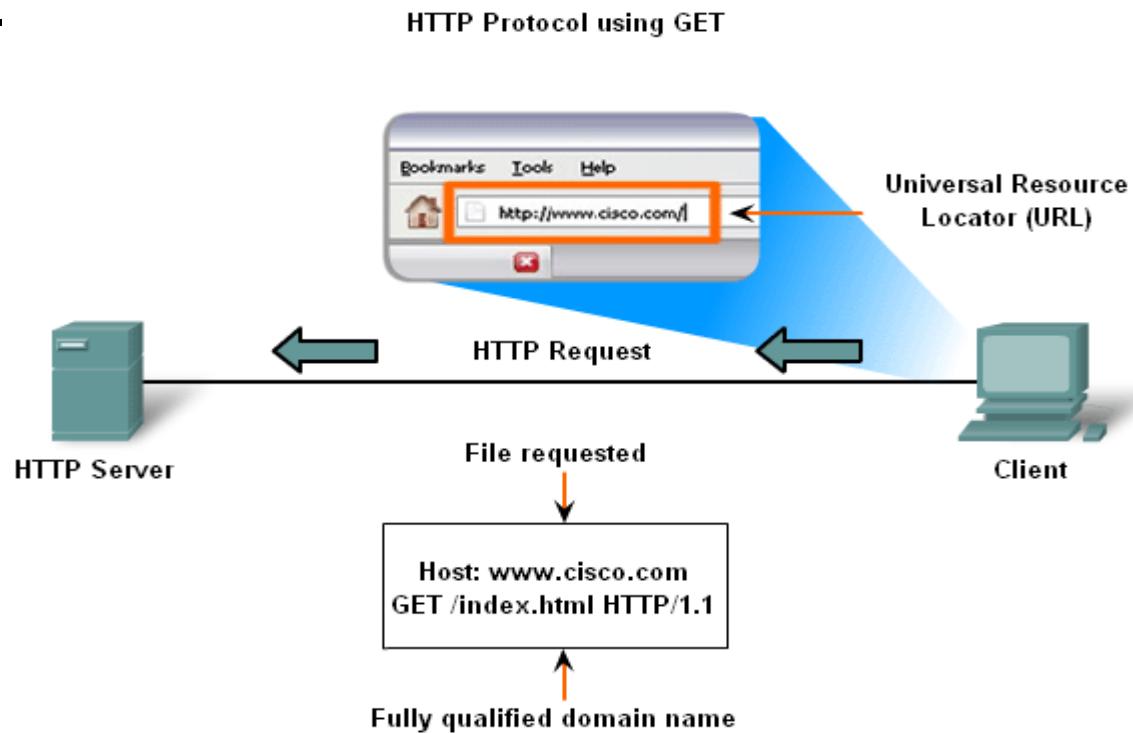
Features, Operation, and Use of TCP/IP Application Layer Services

- The features of the **HTTP** (Hypertext Transfer Protocol) protocol and how this protocol supports the delivery of web pages to the client
- TCP Port 80



Features, Operation, and Use of TCP/IP Application Layer Services

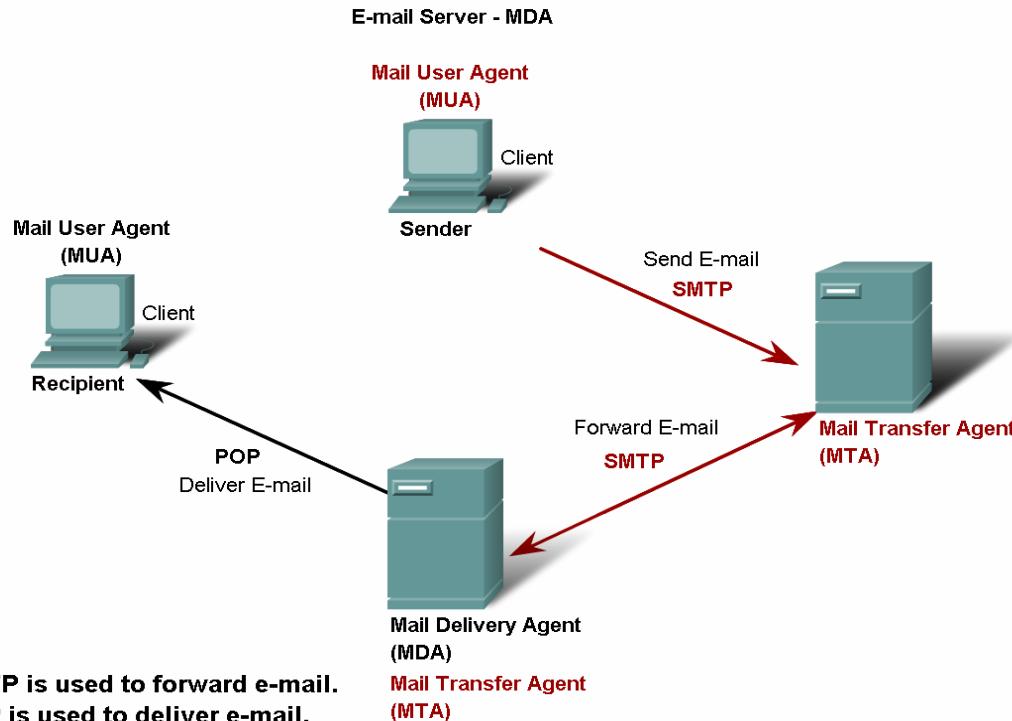
- HTTP is used across the WWW for data transfer and is one of the most used application protocols.
- The three common message types are GET, POST, and PUT.



Entering 'http://www.cisco.com' in the address bar of a web browser generates the HTTP 'GET' Message.

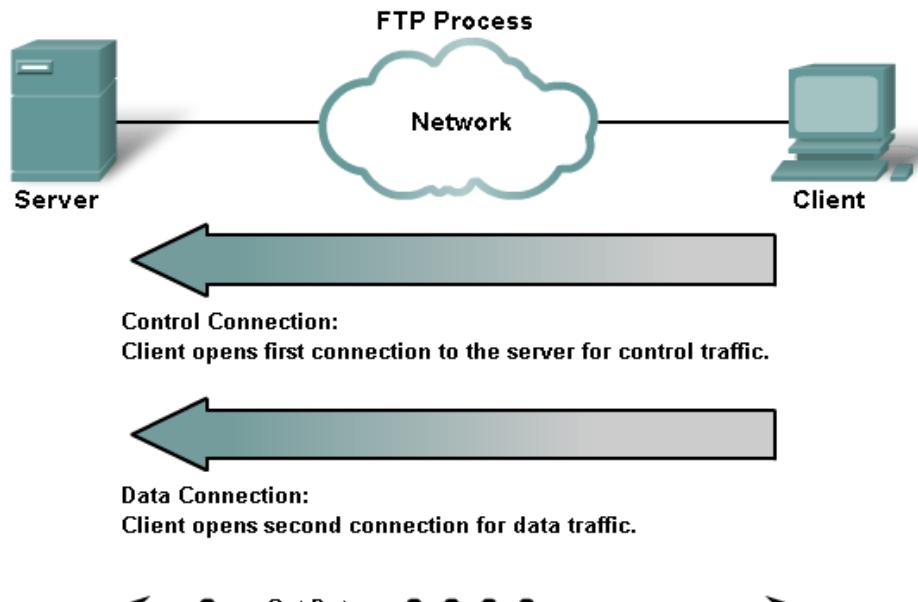
Features, Operation, and Use of TCP/IP Application Layer Services

- Features of the **POP** (Post Office Protocol) and **SMTP** (Simple Mail Transfer Protocol)
- The e-mail server operates two separate processes:
 - Mail Transfer Agent (MTA)** – servers-servers
 - Mail Delivery Agent (MDA)** – servers-clients



Features, Operation, and Use of TCP/IP Application Layer Services

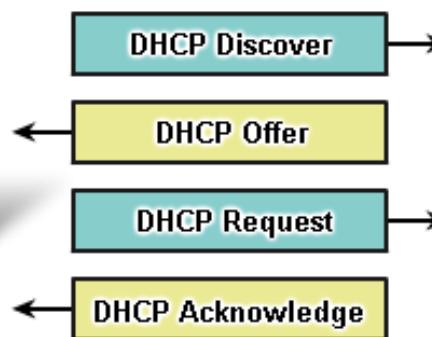
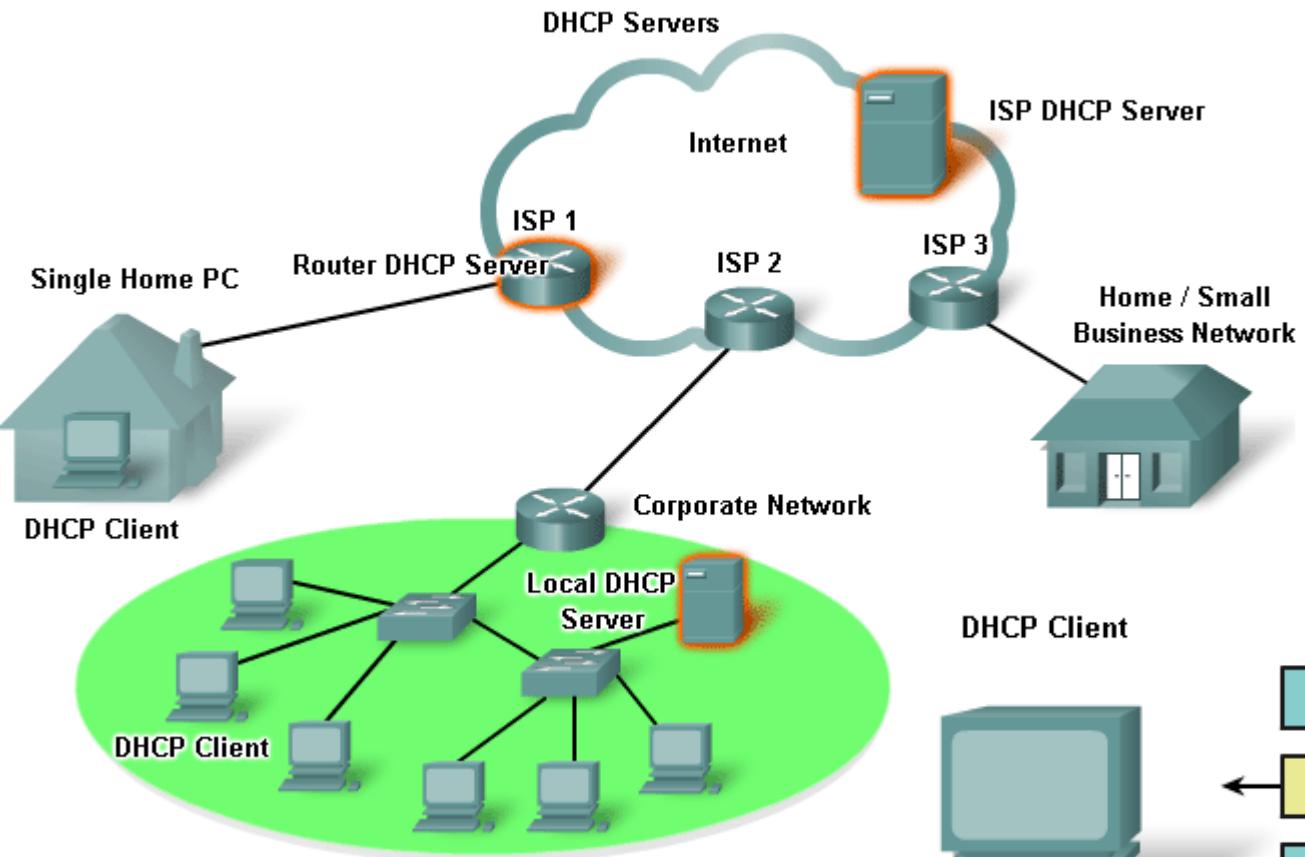
- **FTP (File Transfer Protocol)**
- Client establishes the 1st connection to the server on TCP port **21**. It is used for control traffic.
- Client establishes the 2nd connection to the server over TCP port **20**. It is used for the actual file transfer.



Based on command sent across control connection, data can be downloaded from server or uploaded from client.

Features, Operation, and Use of TCP/IP Application Layer Services

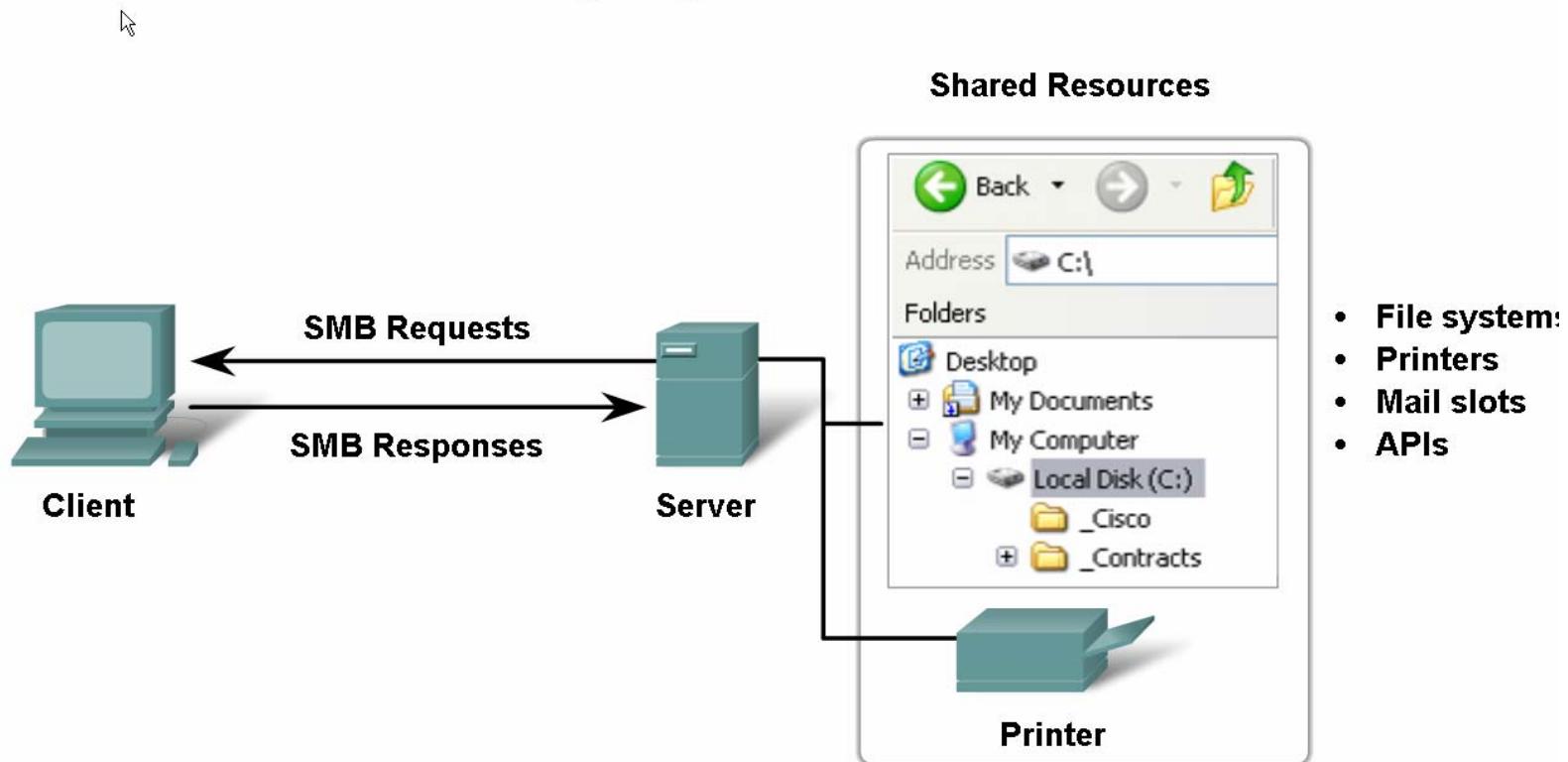
- DHCP (Dynamic Host Configuration Protocol)



Features, Operation, and Use of TCP/IP Application Layer Services

- **SMB** (Server Message Block) protocol it supports file sharing in Microsoft-based networks (by IBM) – SAMBA in UNIX/LINUX

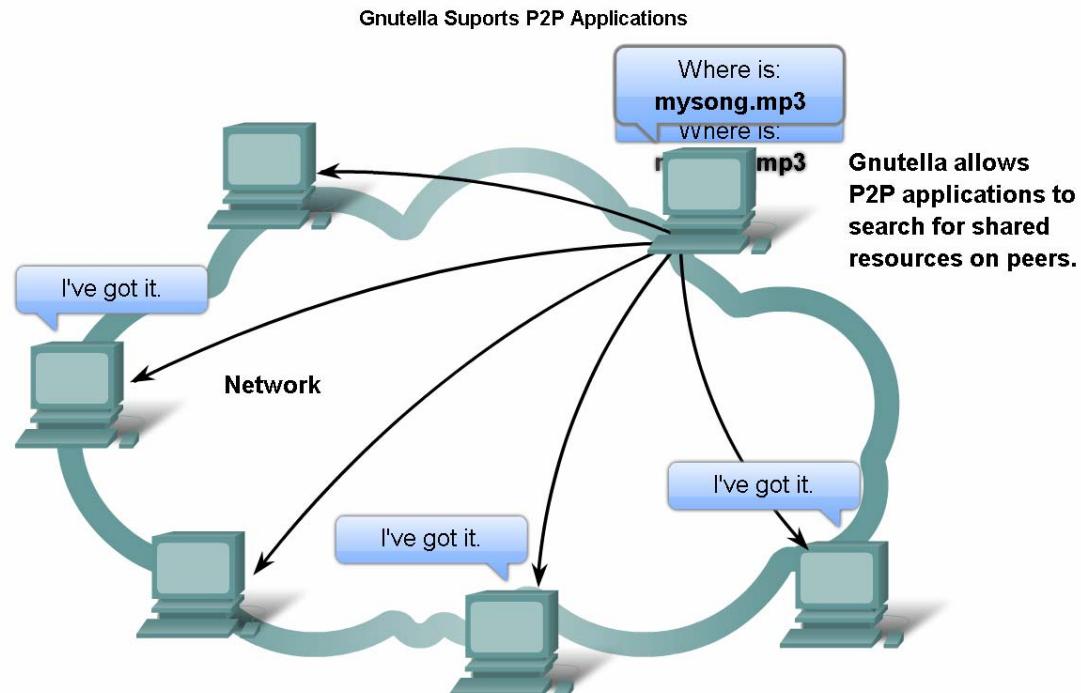
File Sharing Using the SMB Protocol



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

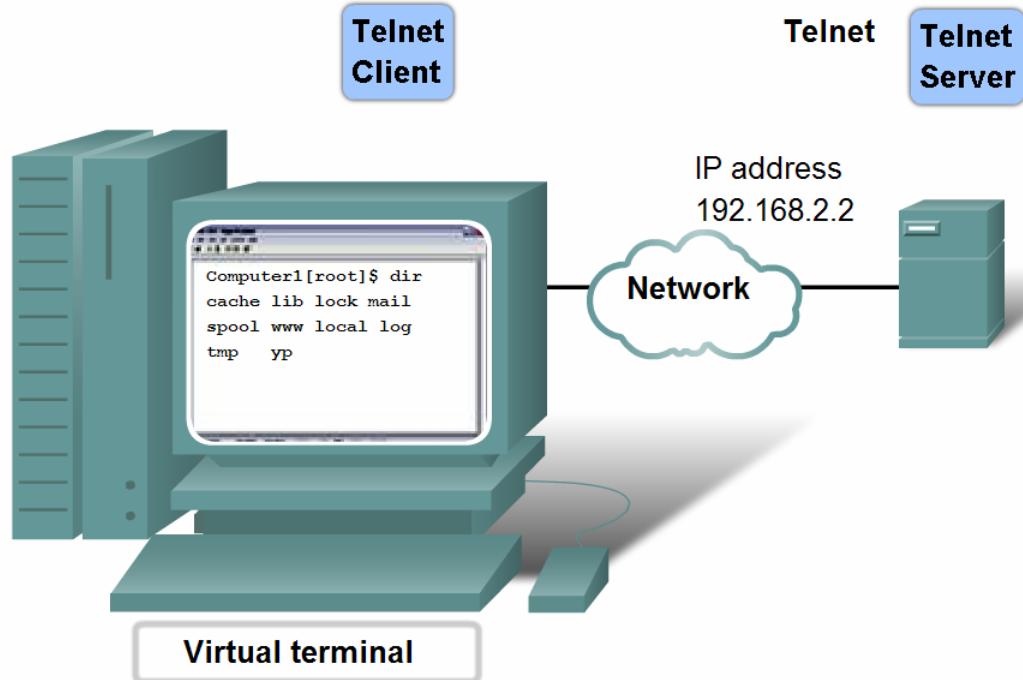
Features, Operation, and Use of TCP/IP Application Layer Services

- **Gnutella** protocol - supports P2P services
- It defines five different packet types:
 - query hit** - as a reply to a query
 - push** - as a download request
 - ping** - for device discovery
 - pong** - as a reply to a ping
 - query** - for file location



Features, Operation, and Use of TCP/IP Application Layer Services

- **Telnet** protocol (early 1970s) - examines and manages networks
- Connection using Telnet is called a **Virtual Terminal (VTY)** session, or connection



Telnet provides a way to use a computer, connected via the network, to access a network device as if the keyboard and monitor were directly connected to the device.



Summary

In this chapter, you learned to:

- Describe how the functions of the three upper OSI model layers provide network services to end user applications.
- Describe how the TCP/IP Application layer protocols provide the services specified by the upper layers of the OSI model.
- Define how people use the Application layer to communicate across the information network.
- Describe the function of well-known TCP/IP applications, such as the World Wide Web and email, and their related services (HTTP, DNS, SMB, DHCP, STMP/POP, and Telnet).
- Describe file-sharing processes that use peer-to-peer applications and the Gnutella protocol.
- Explain how protocols ensure services running on one kind of device can send to and receive data from many different network devices.
- Use network analysis tools to examine and explain how common user applications work.





OSI Transport Layer



Network Fundamentals – Chapter 4

Cisco | Networking Academy®
Mind Wide Open™



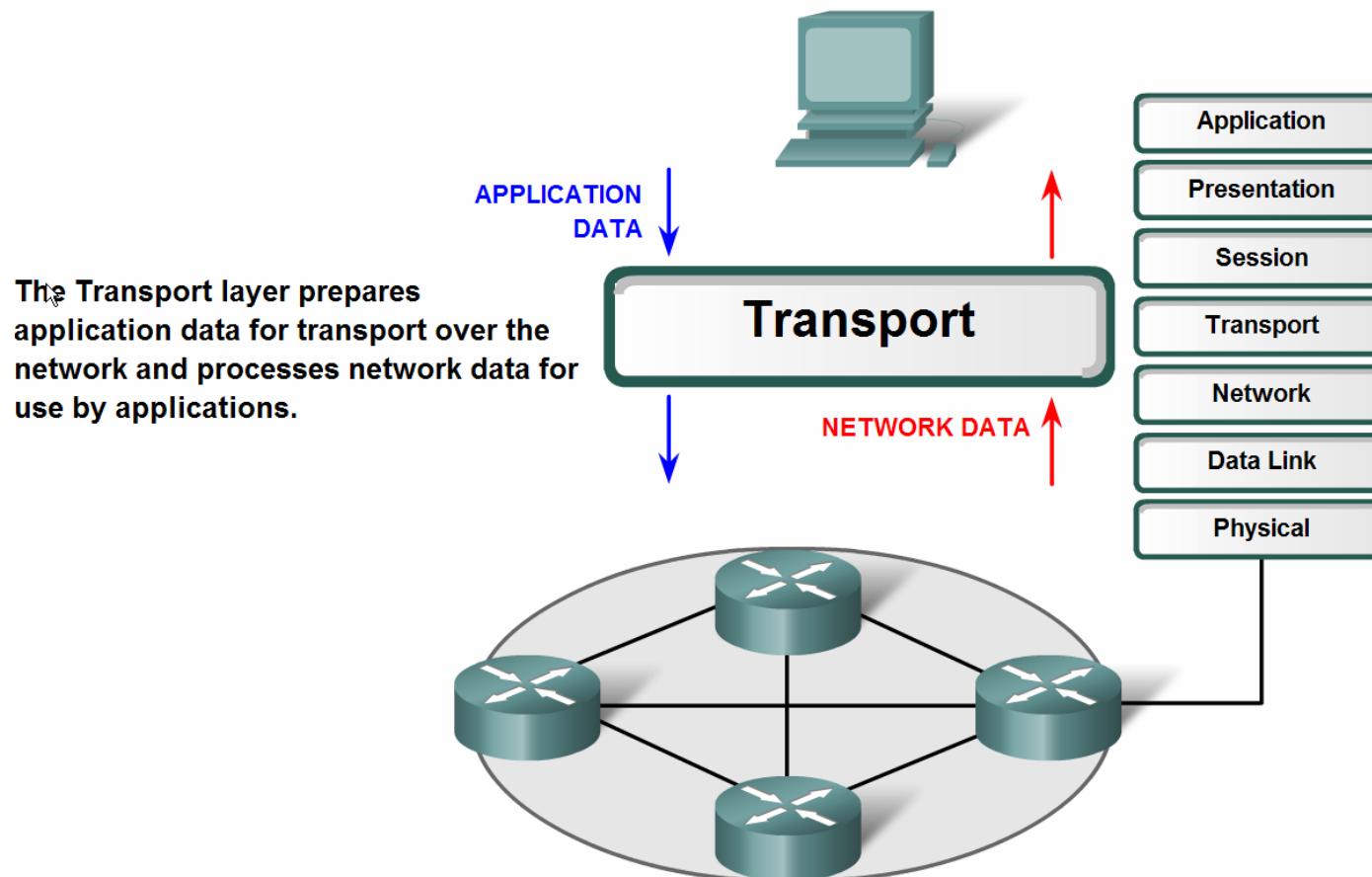
Objectives

- Explain the role of Transport Layer protocols and services in supporting communications across data networks
- Analyze the application and operation of TCP mechanisms that support reliability
- Analyze the application and operation of TCP mechanisms that support reassembly and manage data loss.
- Analyze the operation of UDP to support communicate between two processes on end devices

Transport Layer Role and Services

- Explain the purpose of the Transport layer

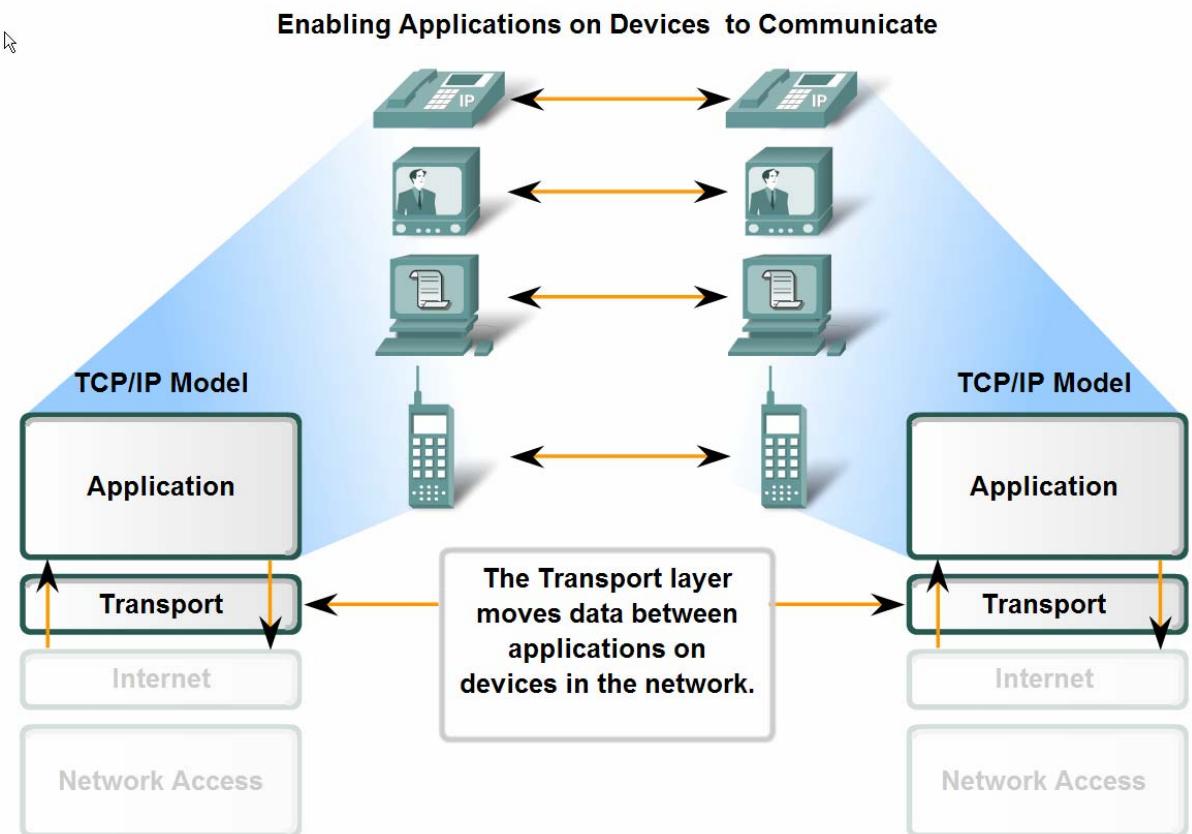
The OSI Transport Layer



Transport Layer Role and Services

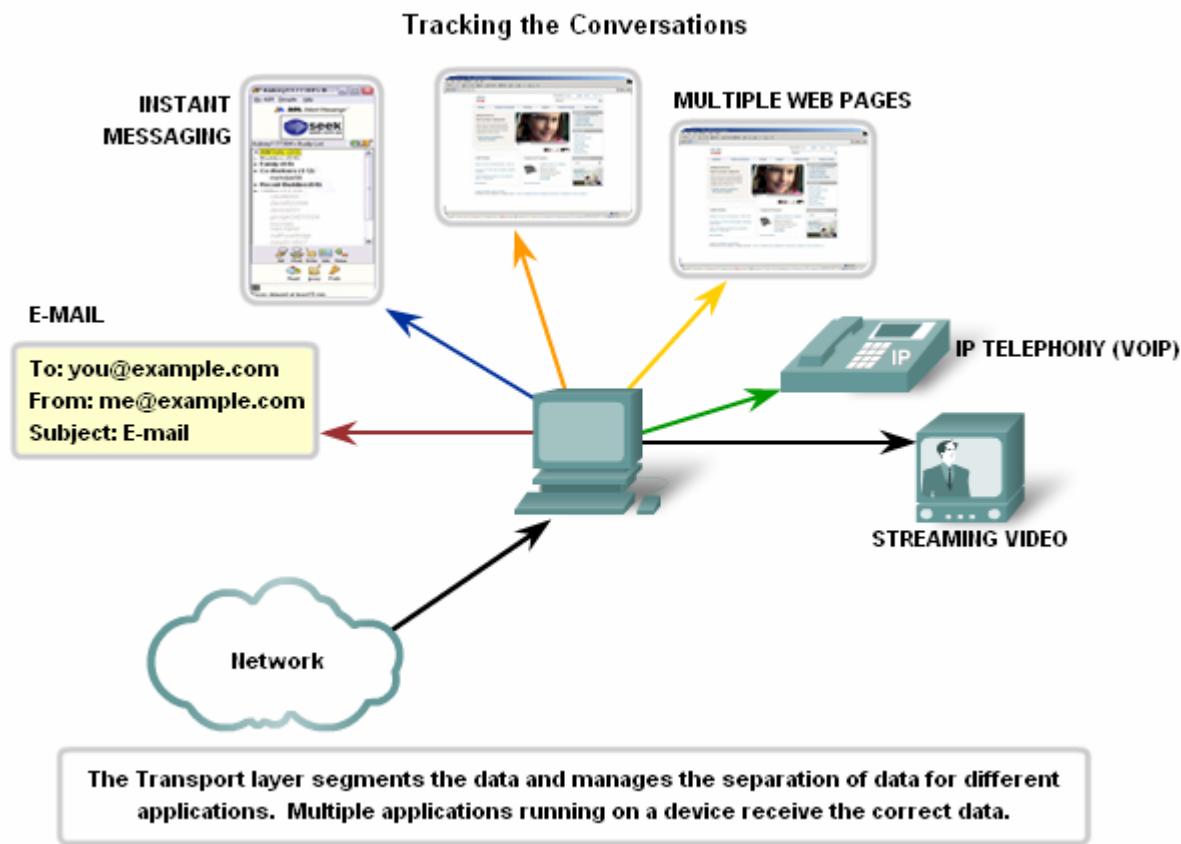
- Major functions of the transport layer and the role it plays in data networks

- Tracking the individual communication between applications on the source and destination hosts
- Segmenting data and managing each piece
- Reassembling the segments into streams of application data
- Identifying the different applications



Transport Layer Role and Services

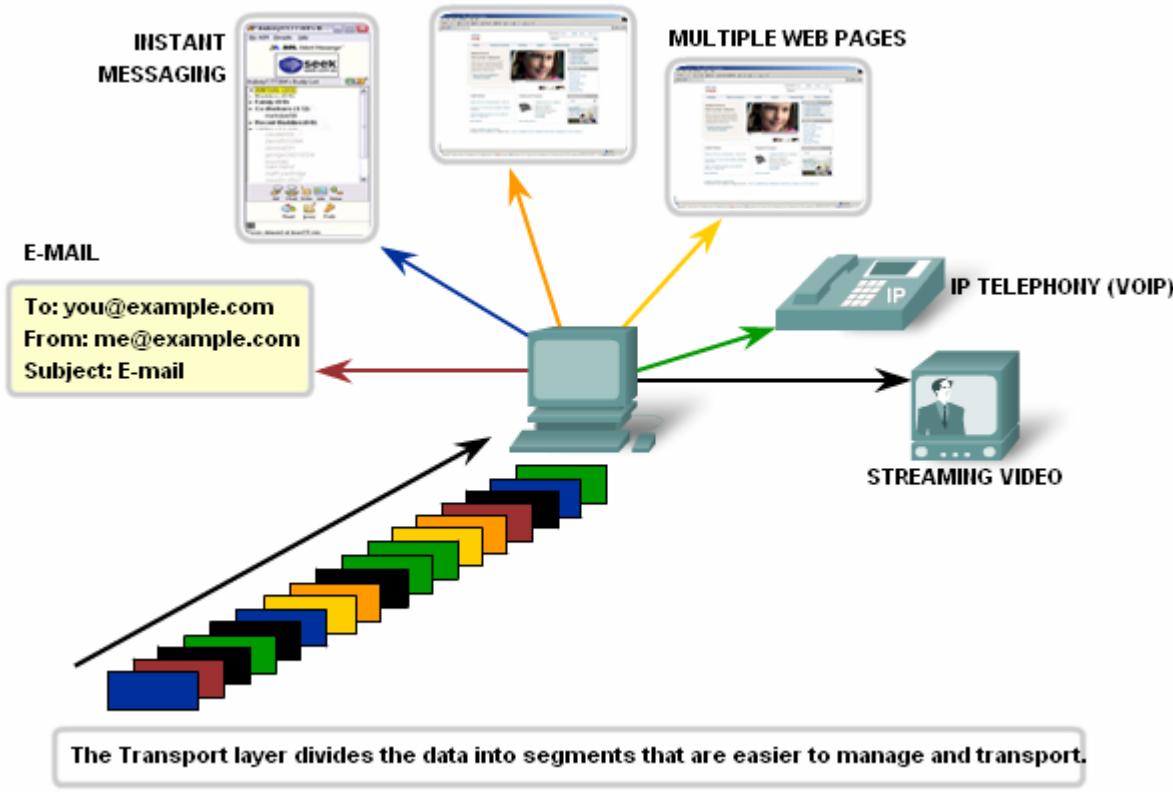
- Tracking the conversations
 - Allows multiple applications to use the network concurrently



Transport Layer Role and Services

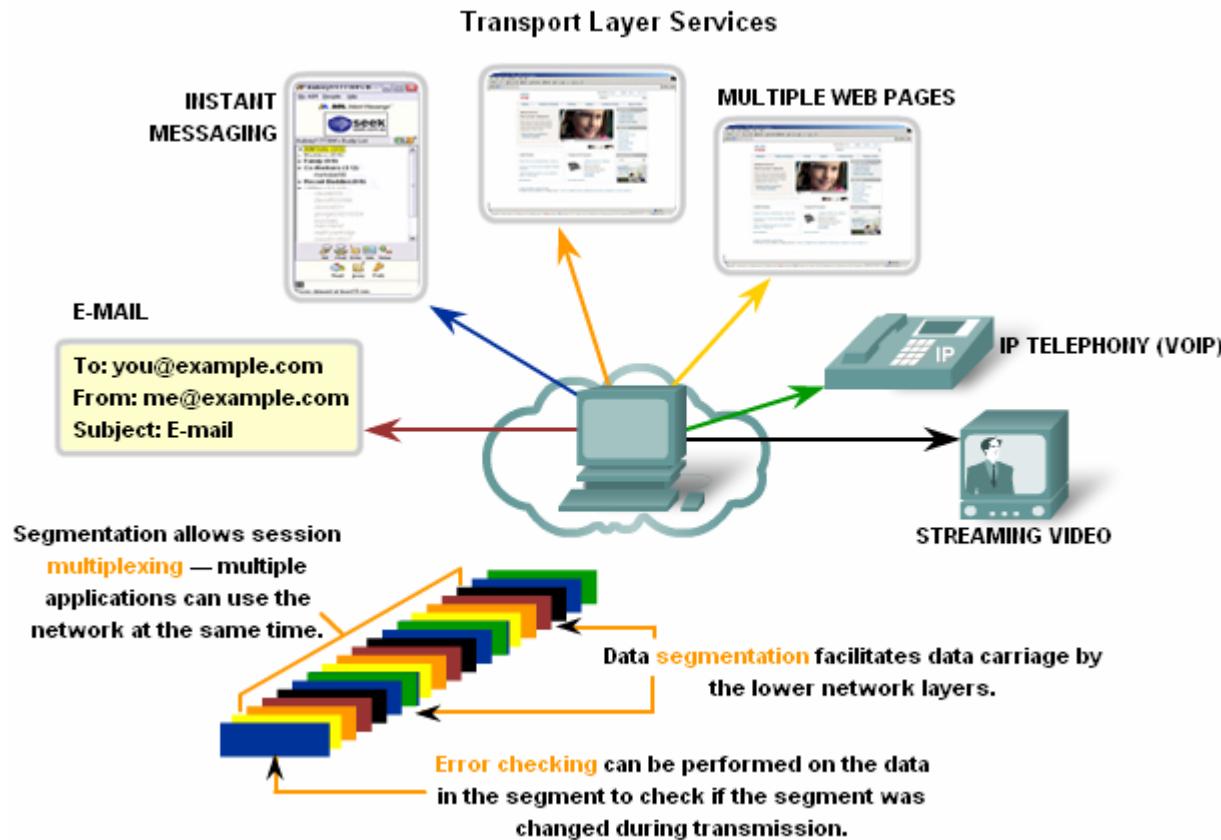
■ Segmentation

- Provides the means to both send and receive data when running multiple applications



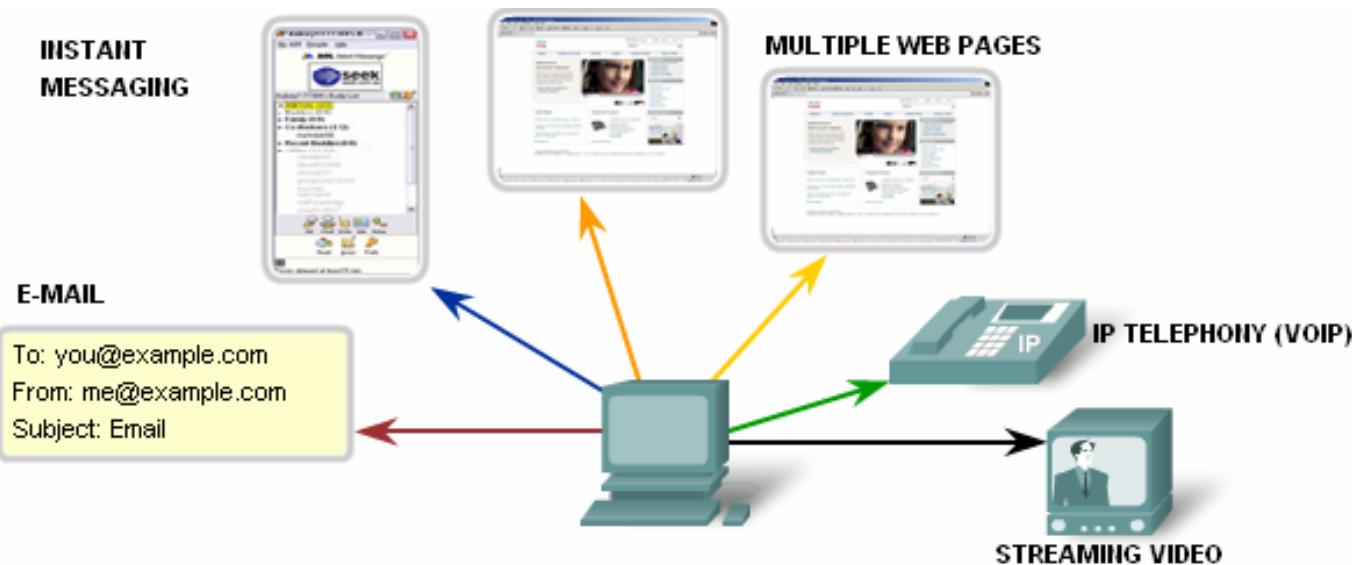
Transport Layer Role and Services

- Conversation Multiplexing & Error Checking



Transport Layer Role and Services

- Controlling the Conversations



Establishing a Session
ensures the application is ready to receive the data.

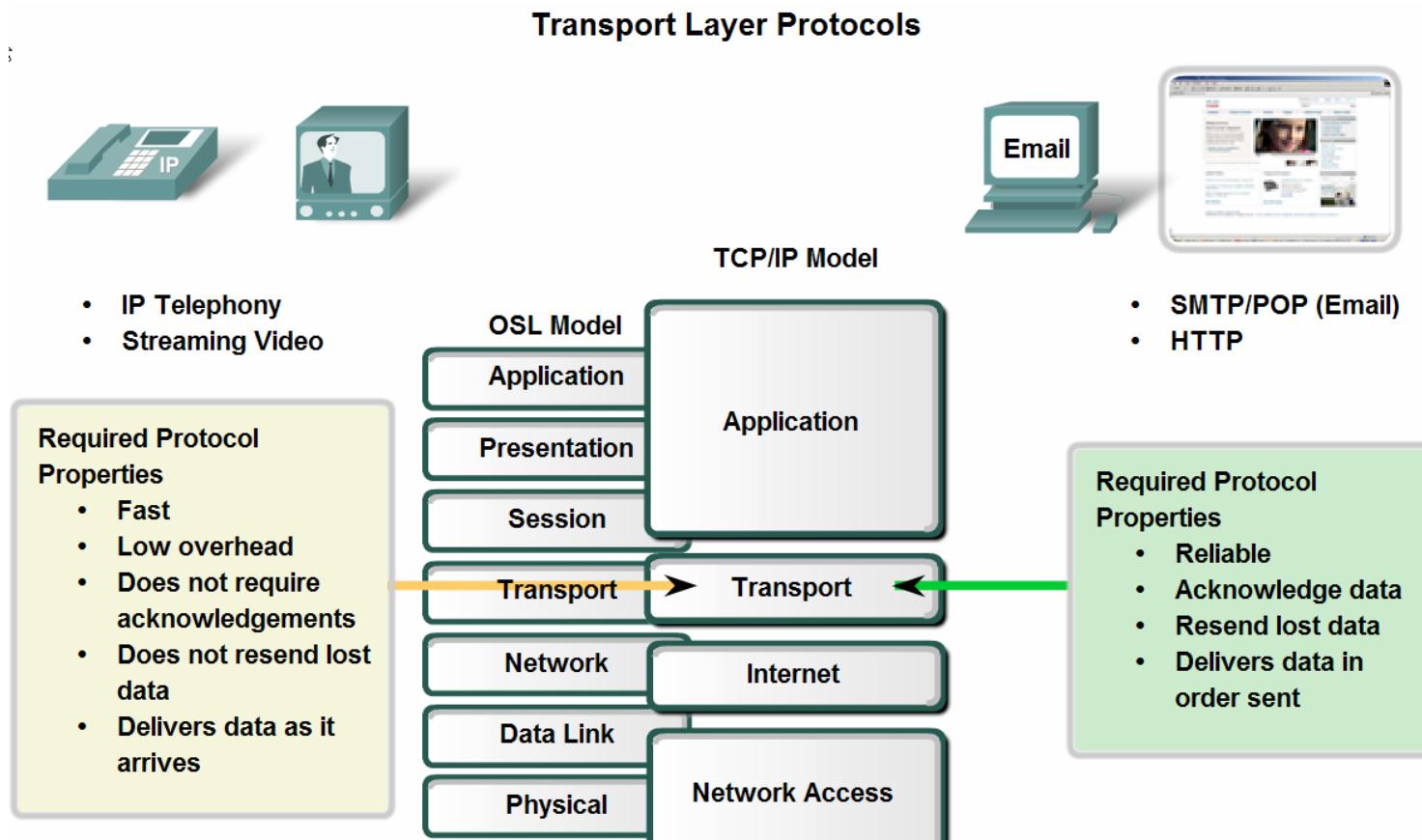
Reliable delivery means lost segments are resent so the data is received complete.

Same order delivery
ensures data is delivered sequentially as it was sent.

Flow Control manages data delivery if there is congestion on the host.

Transport Layer Role and Services

■ Supporting Reliable Communication

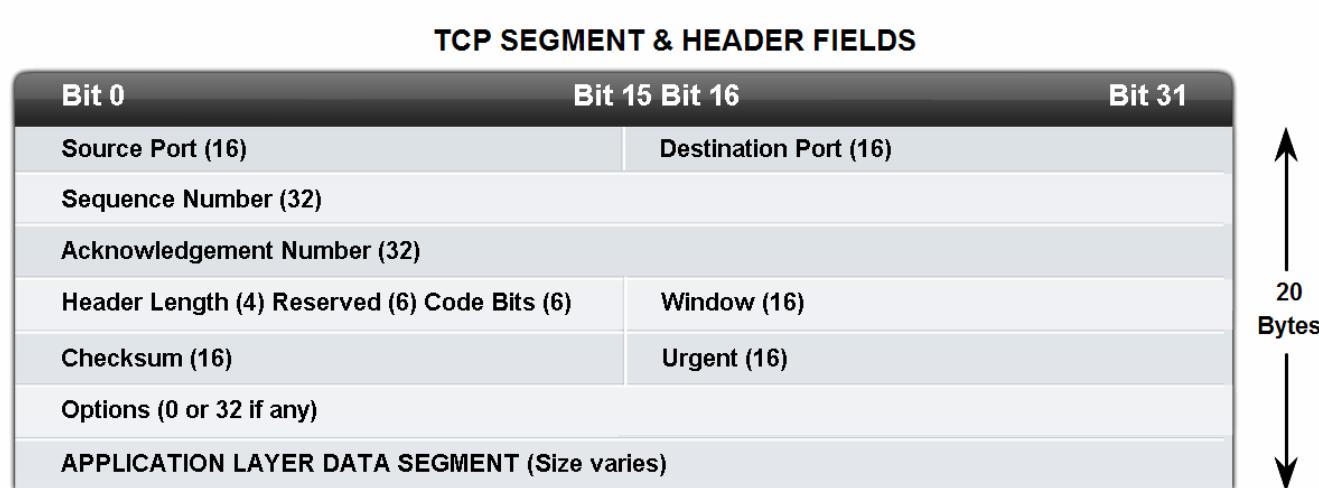


Application developers choose the appropriate Transport Layer protocol based on the nature of the application.

Transport Layer Role and Services

- Identify the basic characteristics of the UDP and TCP protocols

TCP and UDP Headers

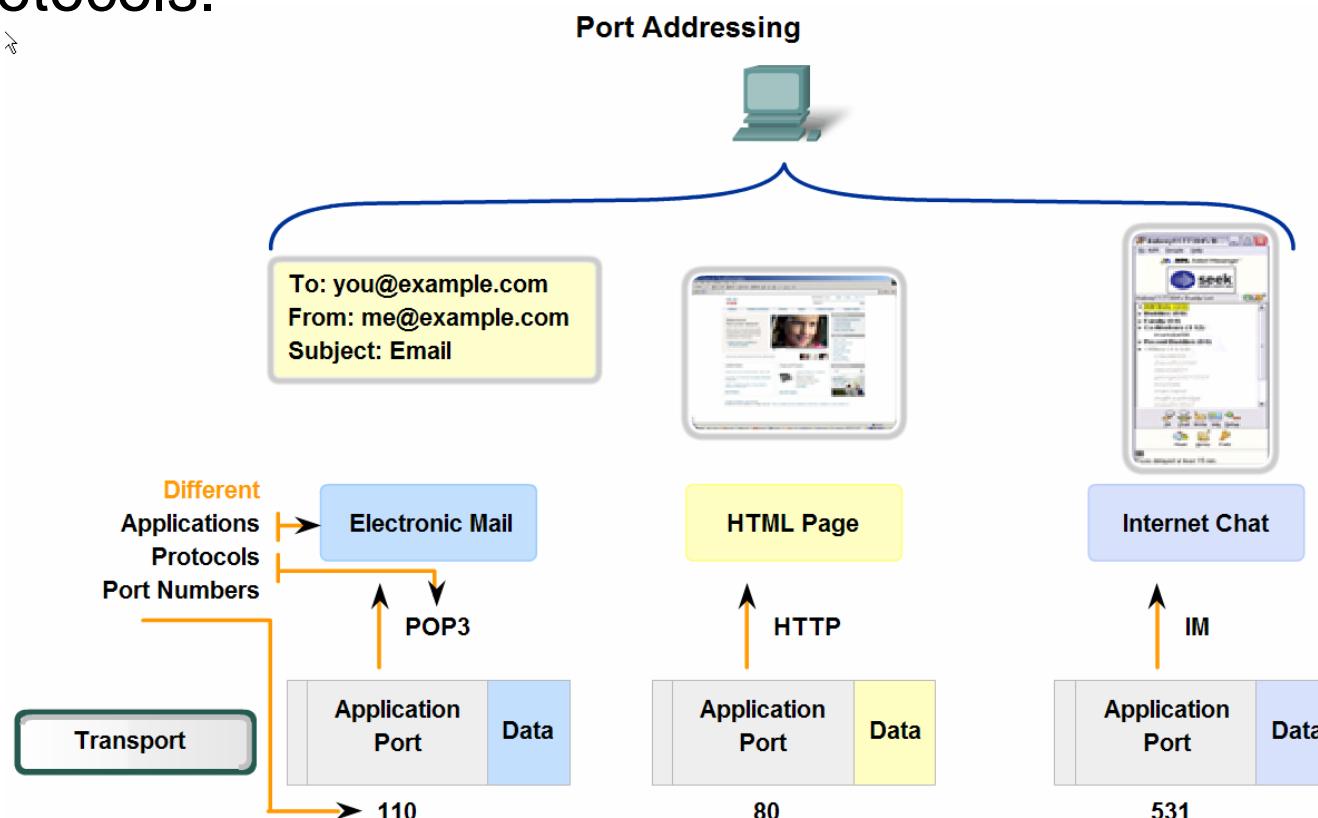


UDP SEGMENT & HEADER FIELDS



Transport Layer Role and Services

- Identify how a port number is represented and describe the role port numbers play in the TCP and UDP protocols.



Data for different applications is directed to the correct application because each application has a unique port number.

Transport Layer Role and Services

Port Number Range	Port Group
0 to 1023	Well Known (Contact) Ports
1024 to 49151	Registered Ports
49152 to 65535	Private and/or Dynamic Ports

TCP ports

Registered TCP Ports:
1863 MSN Messenger
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)

Port Number Range	Port Group
0 to 1023	Well Known (Contact) Ports
1024 to 49151	Registered Ports
49152 to 65535	Private and/or Dynamic Ports

UDP ports

Registered UDP Ports:
1812 RADIUS Authentication Protocol
2000 Cisco SCCP (VoIP)
5004 RTP (Voice and Video Transport Protocol)
5060 SIP (VoIP)

Well Known UDP Ports:
69 TFTP
520 RIP

Transport Layer Role and Services

■ Port Addressing

Netstat Output

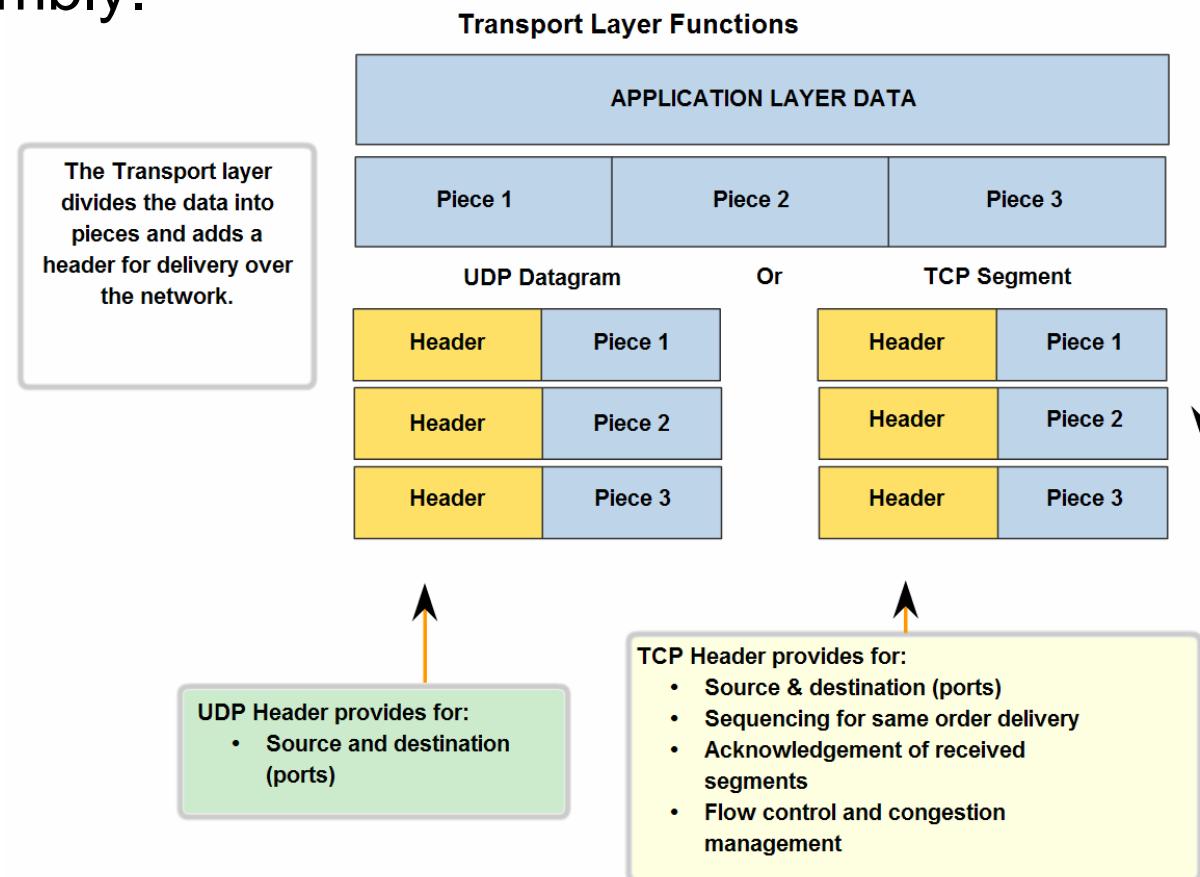
```
C:\>netstat  
  
Active Connections  
  
Proto Local Address Foreign Address State  
TCP kenpc:3126 192.168.0.2:netbios-ssn ESTABLISHED  
TCP kenpc:3158 207.138.126.152:http ESTABLISHED  
TCP kenpc:3159 207.138.126.169:http ESTABLISHED  
TCP kenpc:3160 207.138.126.169:http ESTABLISHED  
TCP kenpc:3161 sc.msn.com:http ESTABLISHED  
TCP kenpc:3166 www.cisco.com:http ESTABLISHED
```

```
C:\>
```

Protocol used

Transport Layer Role and Services

- Describe the role of segments in the transport layer and the two principle ways segments can be marked for reassembly.

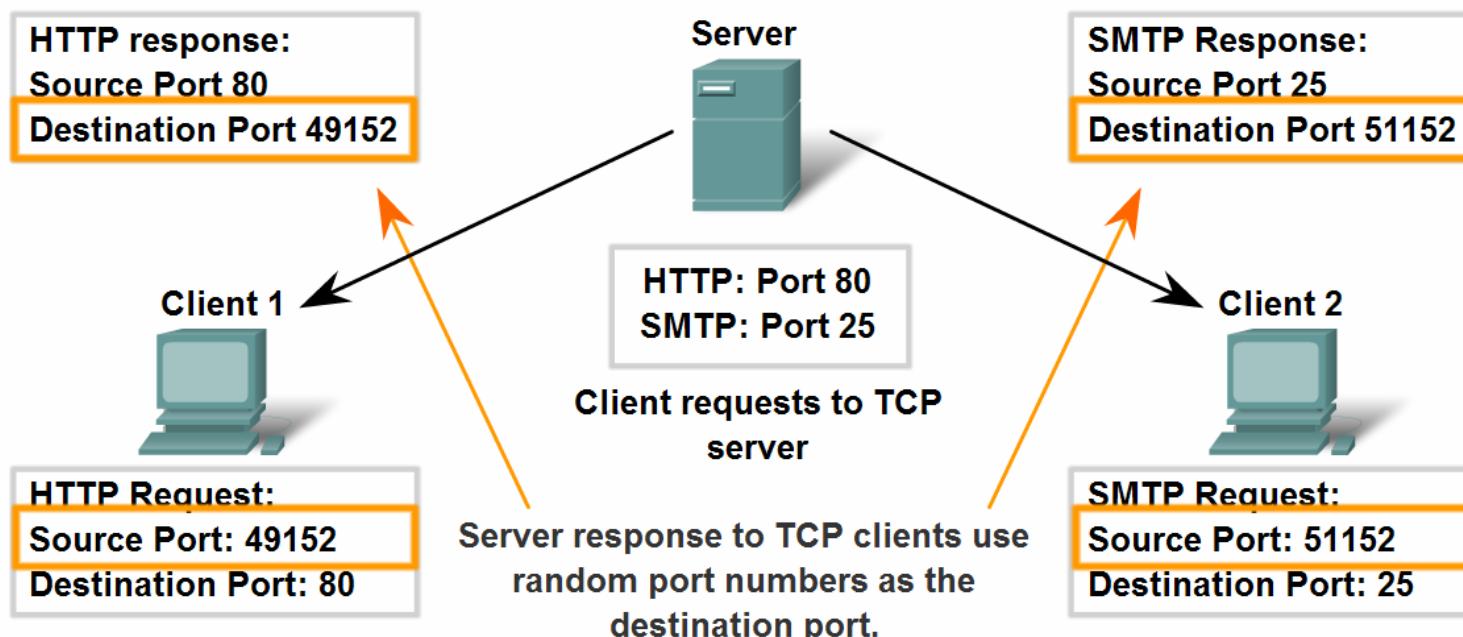


Application and Operation of TCP Mechanisms

- Describe the role of port numbers in establishing TCP sessions and directing segments to server process

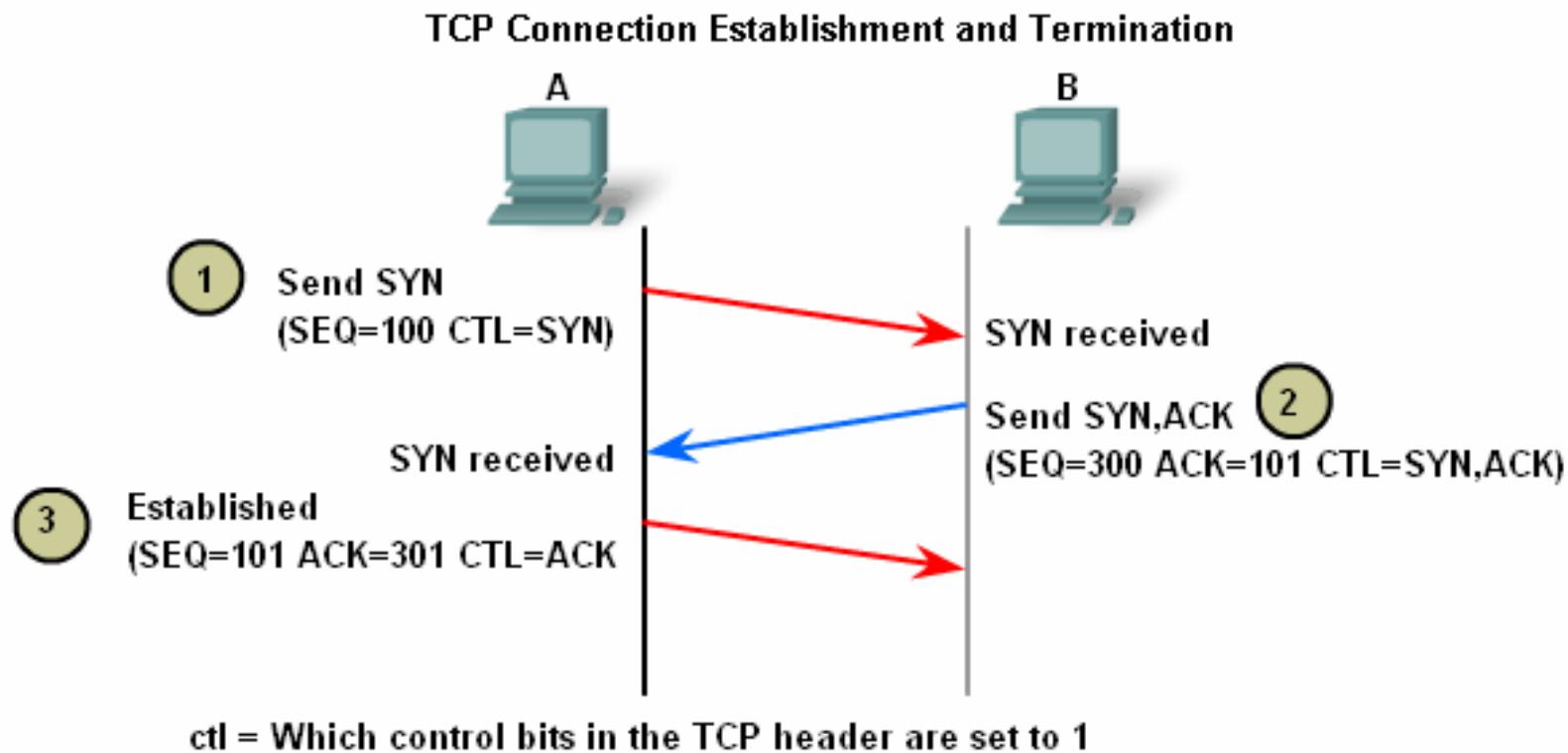


Clients Sending TCP Requests



Application and Operation of TCP Mechanisms

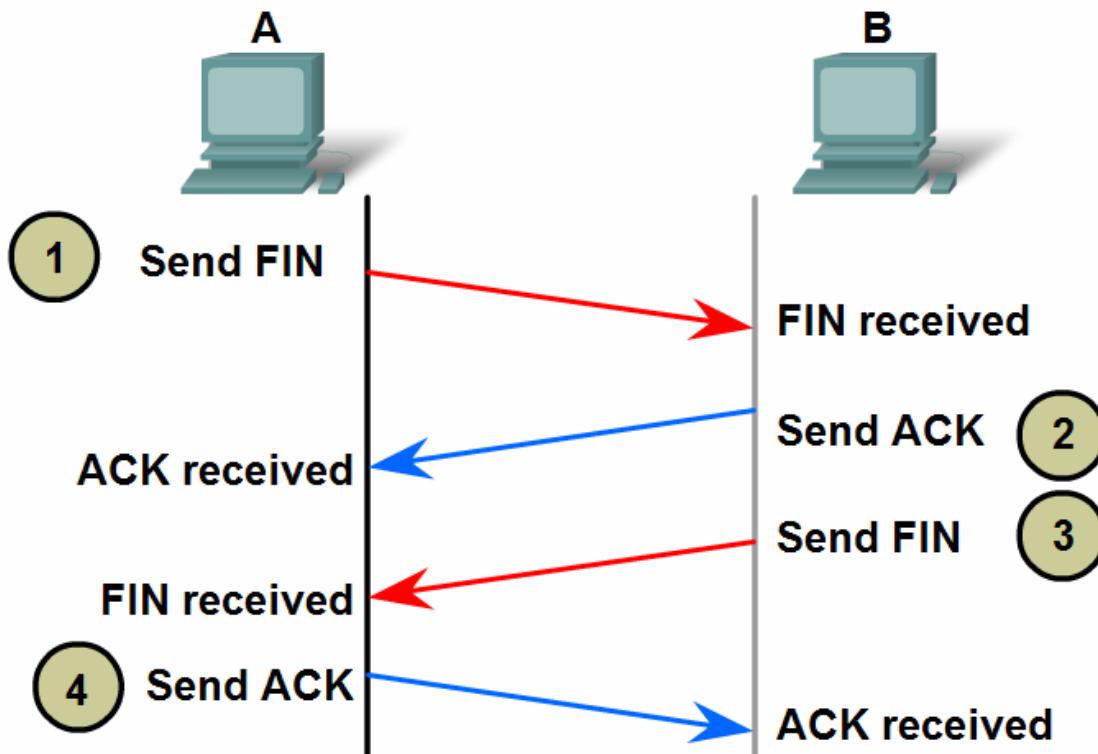
- Trace the steps in the handshake in the establishment of TCP sessions



Application and Operation of TCP Mechanisms

- Trace the steps in the handshake in the termination of TCP sessions

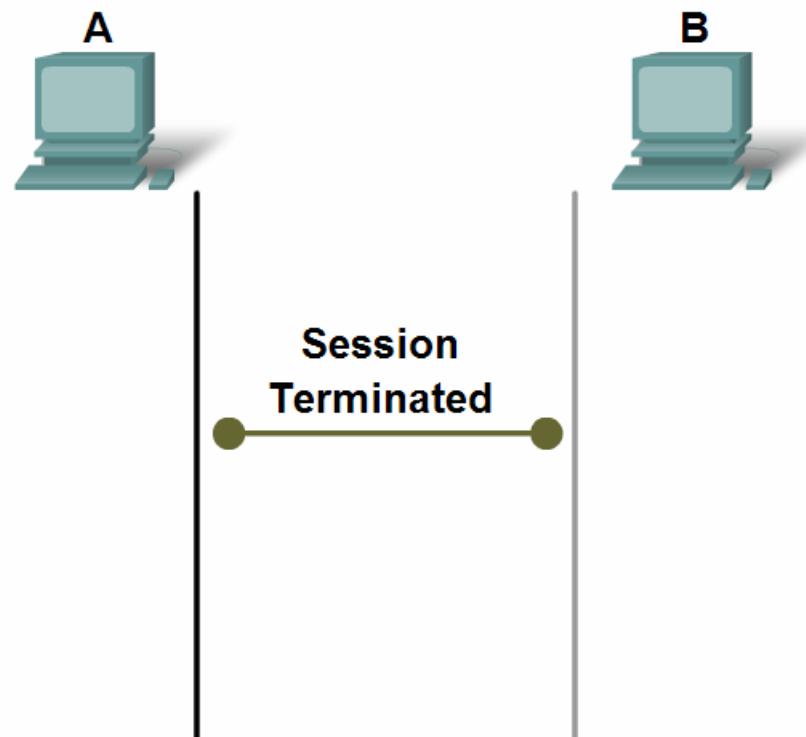
→ TCP Connection Establishment and Termination



Application and Operation of TCP Mechanisms

- Trace the steps in the handshake in the termination of TCP sessions

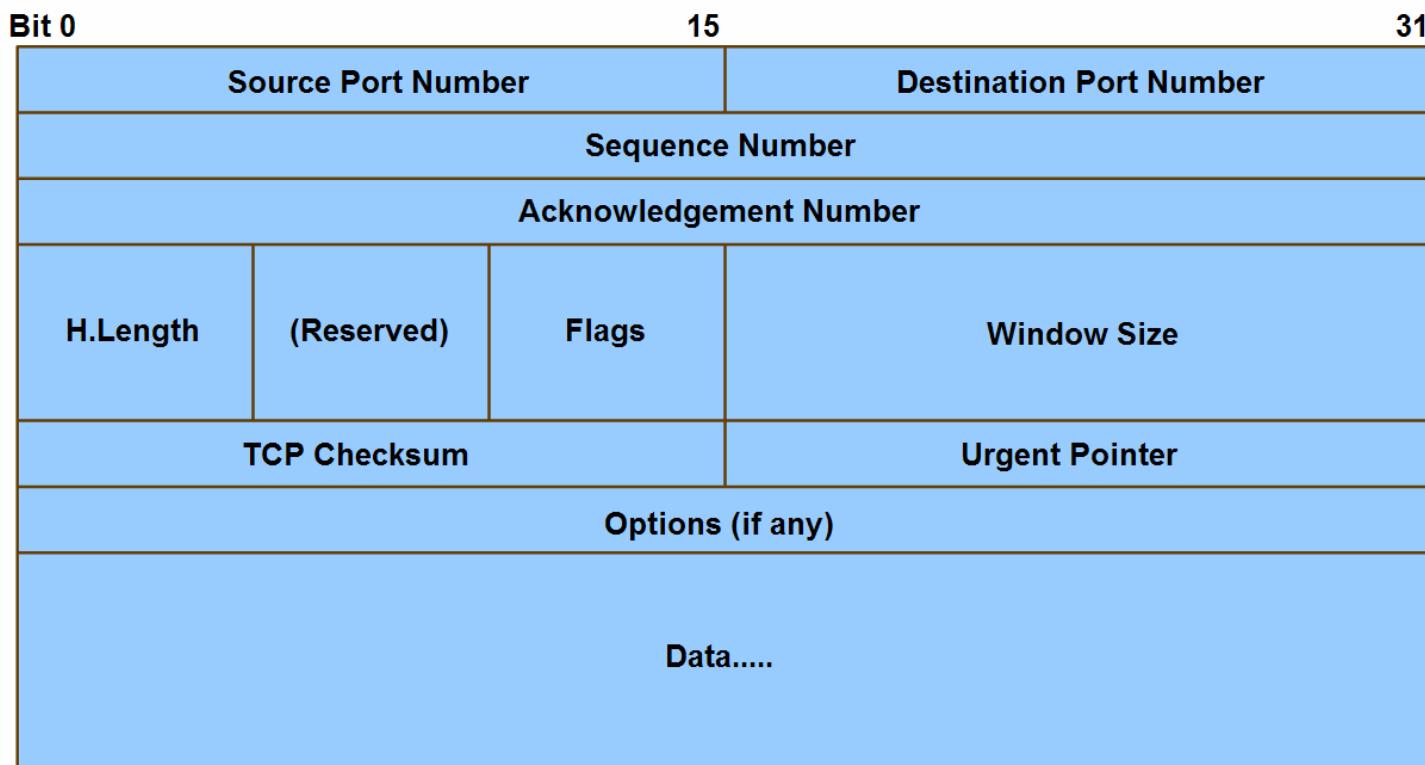
TCP Connection Establishment and Termination



Application and Operation of TCP Mechanisms

- Trace the steps that show how the TCP reliability mechanism works as part of a session

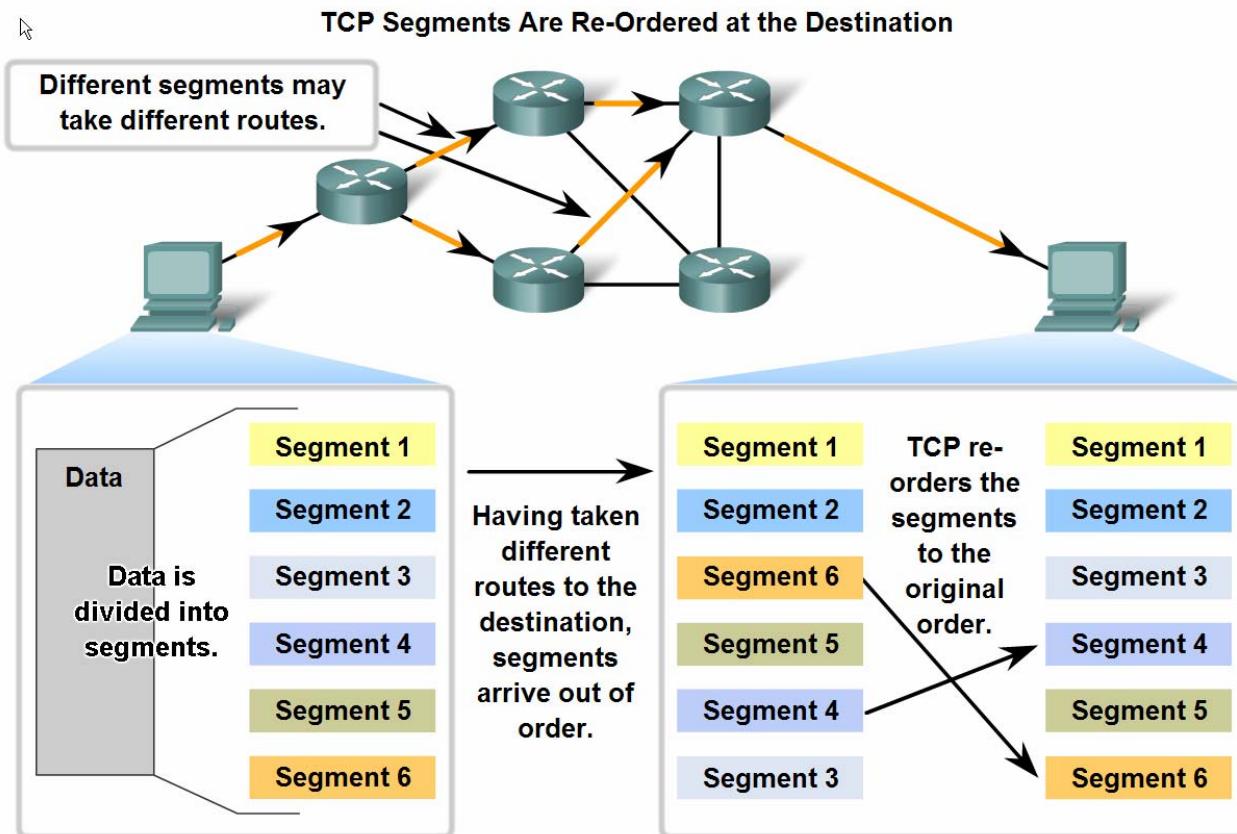
TCP Segment Header Fields



The fields of the TCP header enable TCP to provide connection-oriented, reliable data communications.

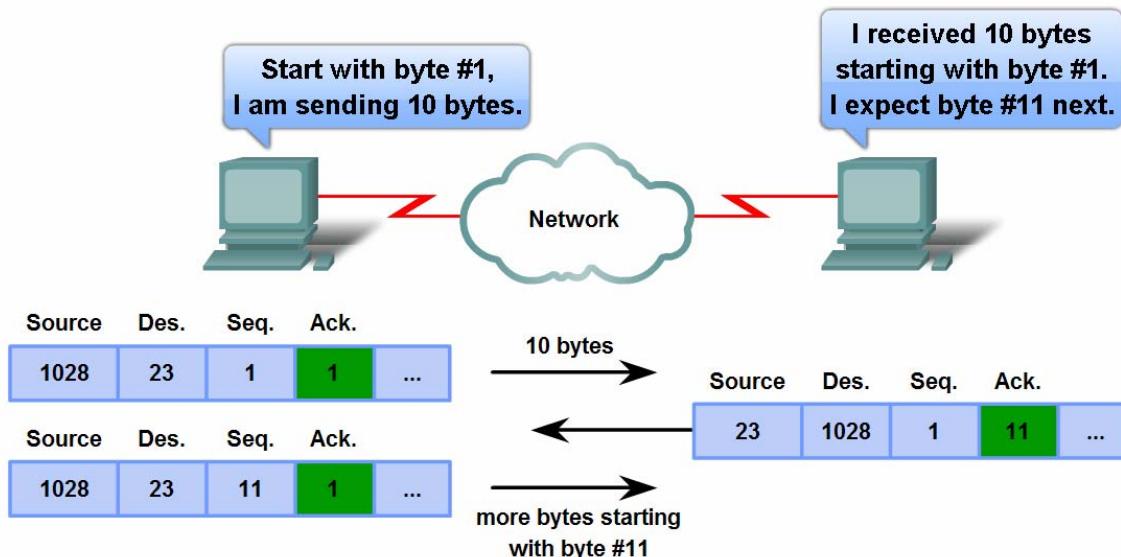
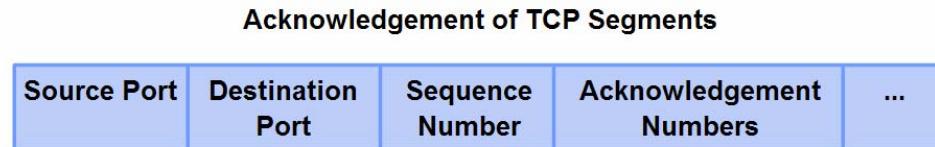
Managing TCP Sessions

- Describe how TCP sequence numbers are used to reconstruct the data stream with segments placed in the correct order



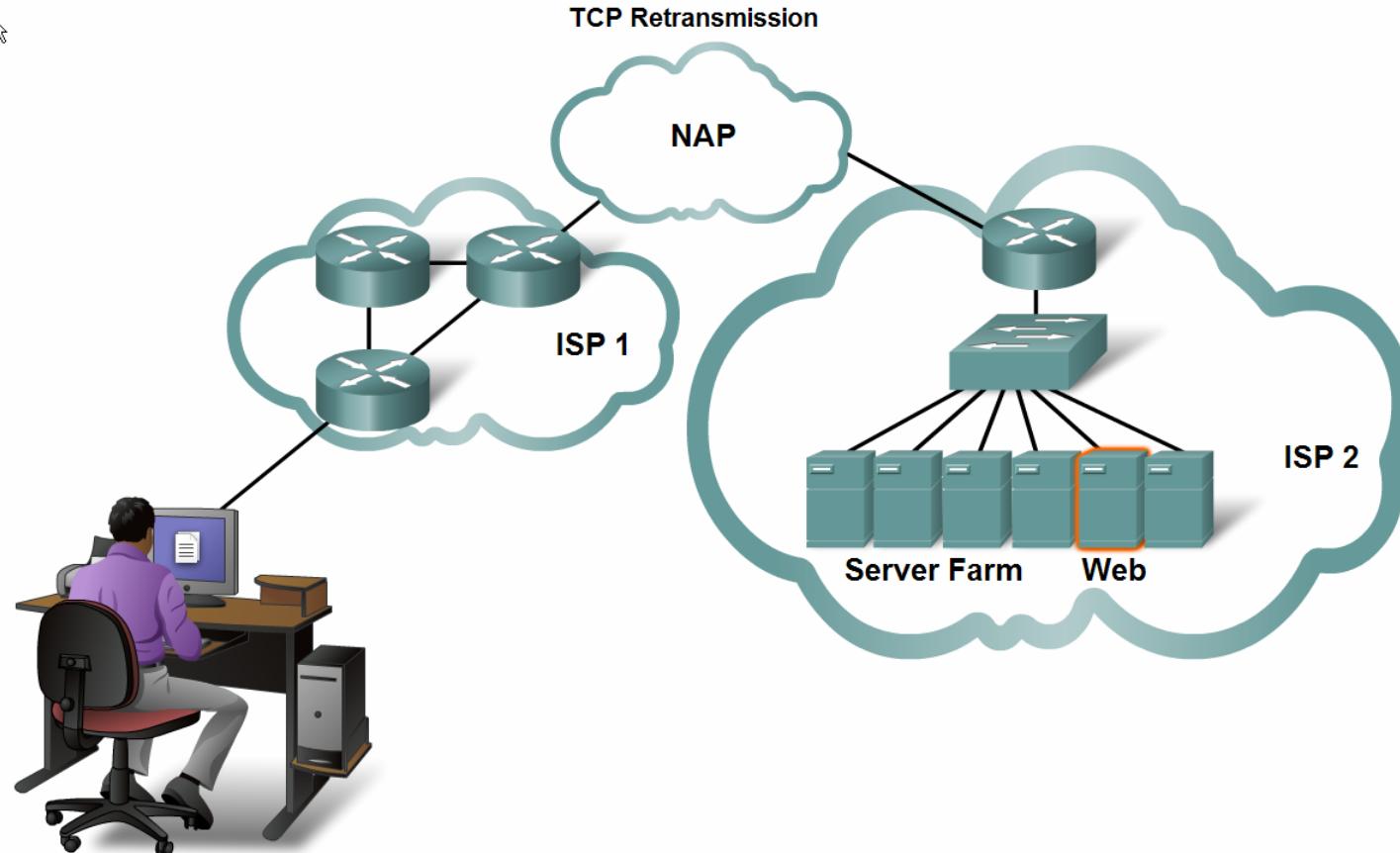
Managing TCP Sessions

- Trace the steps used by the TCP protocol in which sequence numbers and acknowledgement numbers are used to manage exchanges in a conversation



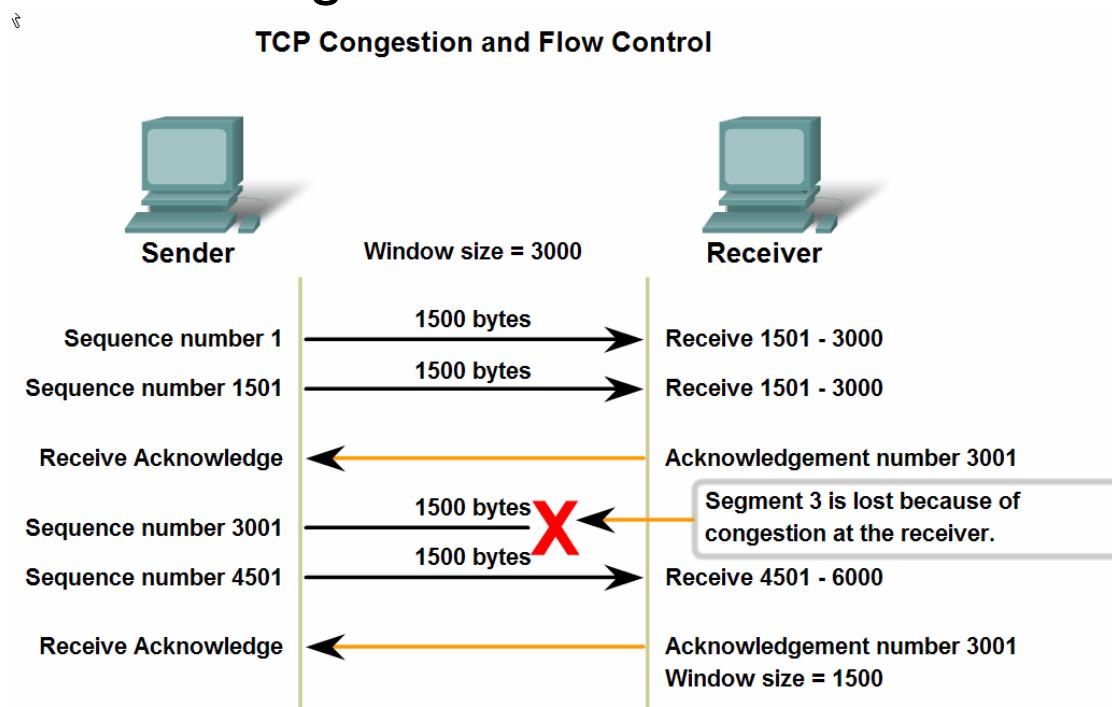
Managing TCP Sessions

- Describe the retransmission remedy for lost data employed by TCP



Managing TCP Sessions

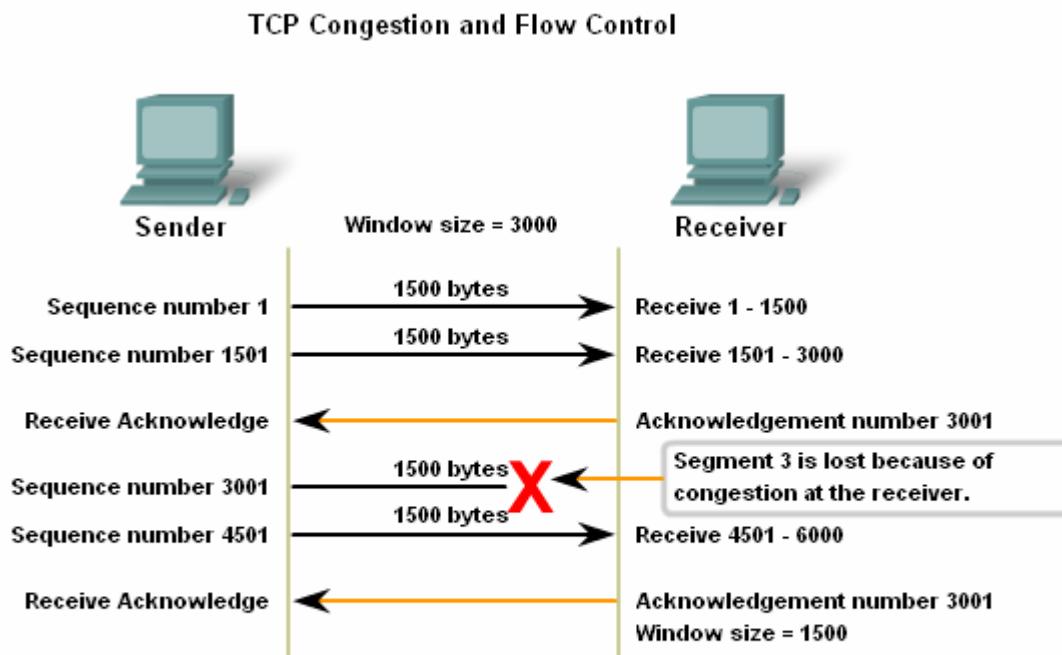
- Describe the mechanisms in TCP that manage the interrelationship between window size, data loss and congestion during a session



If segments are lost because of congestion, the Receiver will acknowledge the last received sequential segment and reply with a reduced window size.

Managing TCP Sessions

- Describe the mechanisms in TCP that manage the interrelationship between window size, data loss and congestion during a session

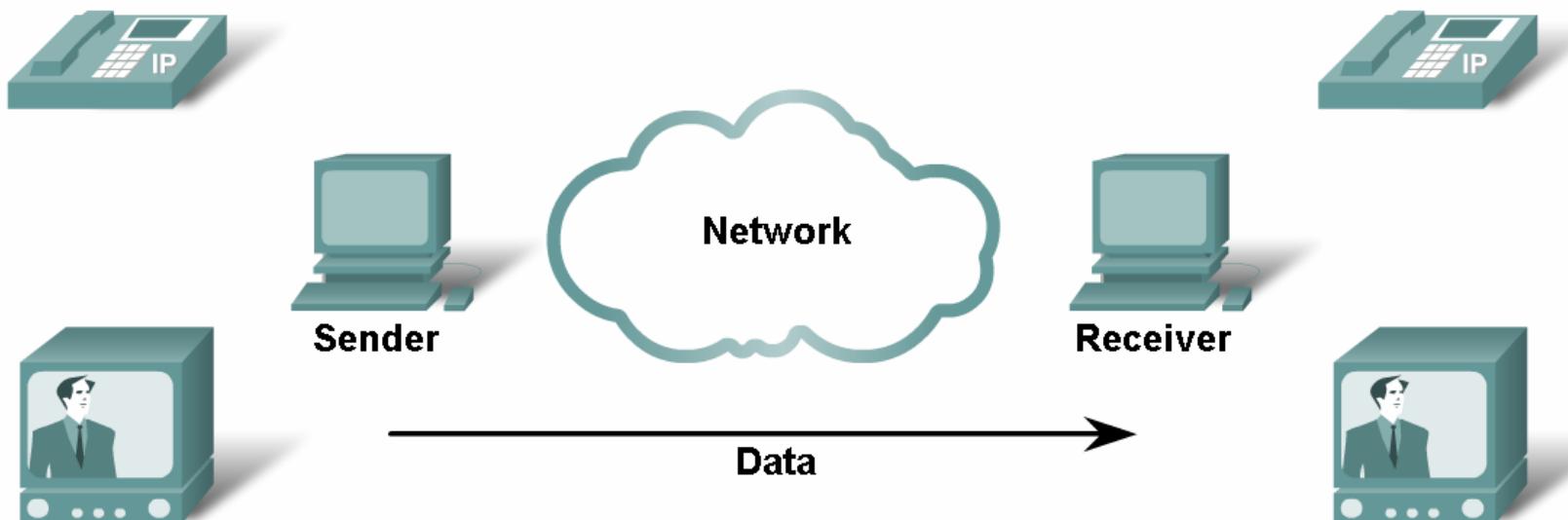


If segments are lost because of congestion, the Receiver will acknowledge the last received sequential segment and reply with a reduced window size.

UDP Protocol

- Describe the characteristics of the UDP protocol and the types of communication for which it is best suited

UDP Low Overhead Data Transport



UDP does not establish a connection before sending data.

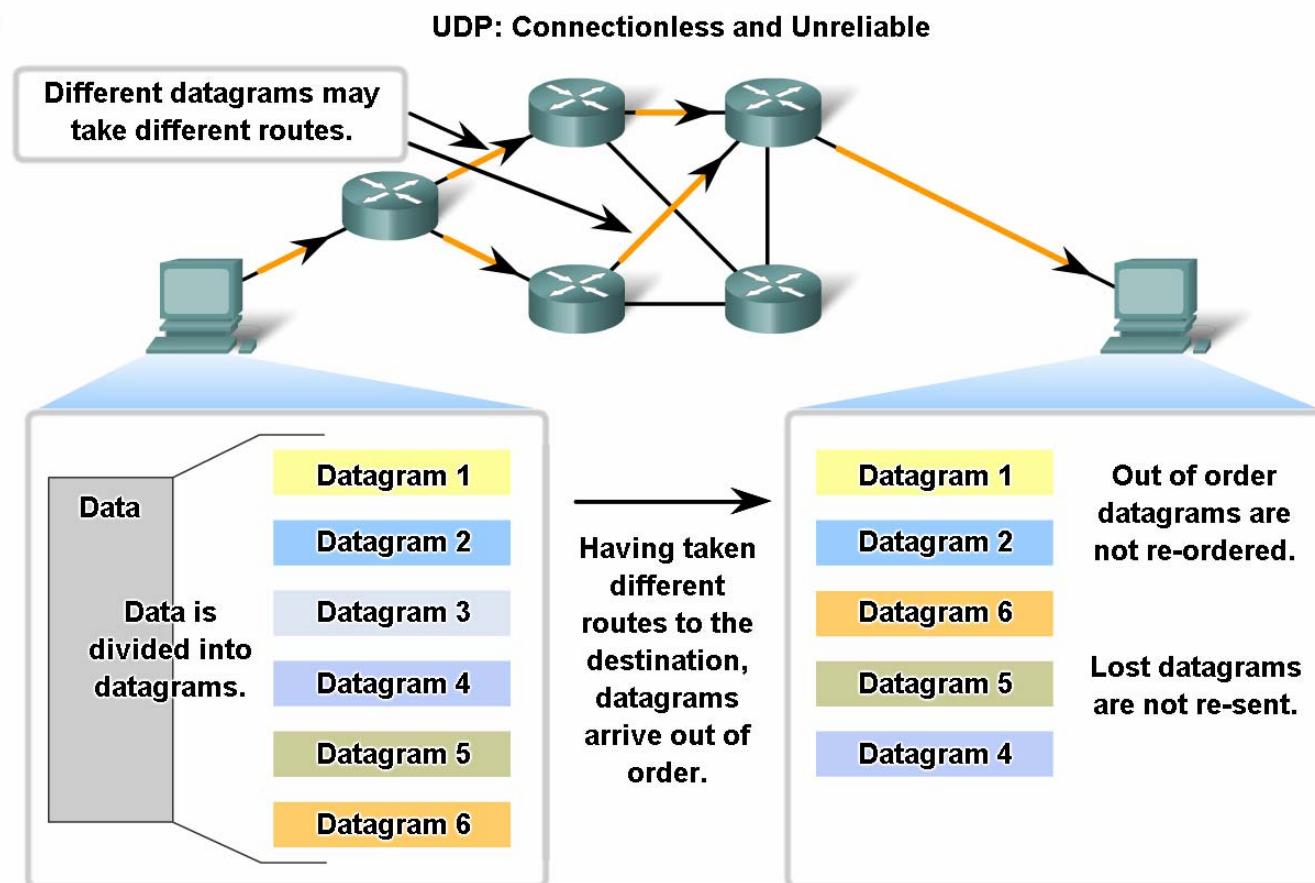


UDP Protocol

- Key Application layer protocols that use UDP include:
 - Domain Name System (DNS)
 - Simple Network Management Protocol (SNMP)
 - Dynamic Host Configuration Protocol (DHCP)
 - Routing Information Protocol (RIP)
 - Trivial File Transfer Protocol (TFTP)
 - VoIP
 - Online games

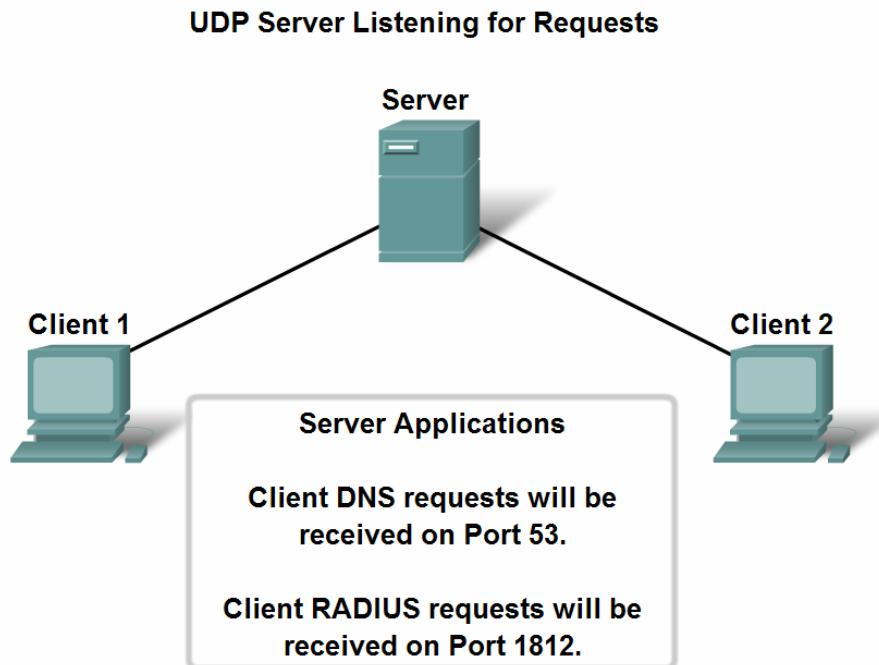
UDP Protocol

- Describe in detail the process specified by the UDP protocol to reassemble PDUs at the destination device



UDP Protocol

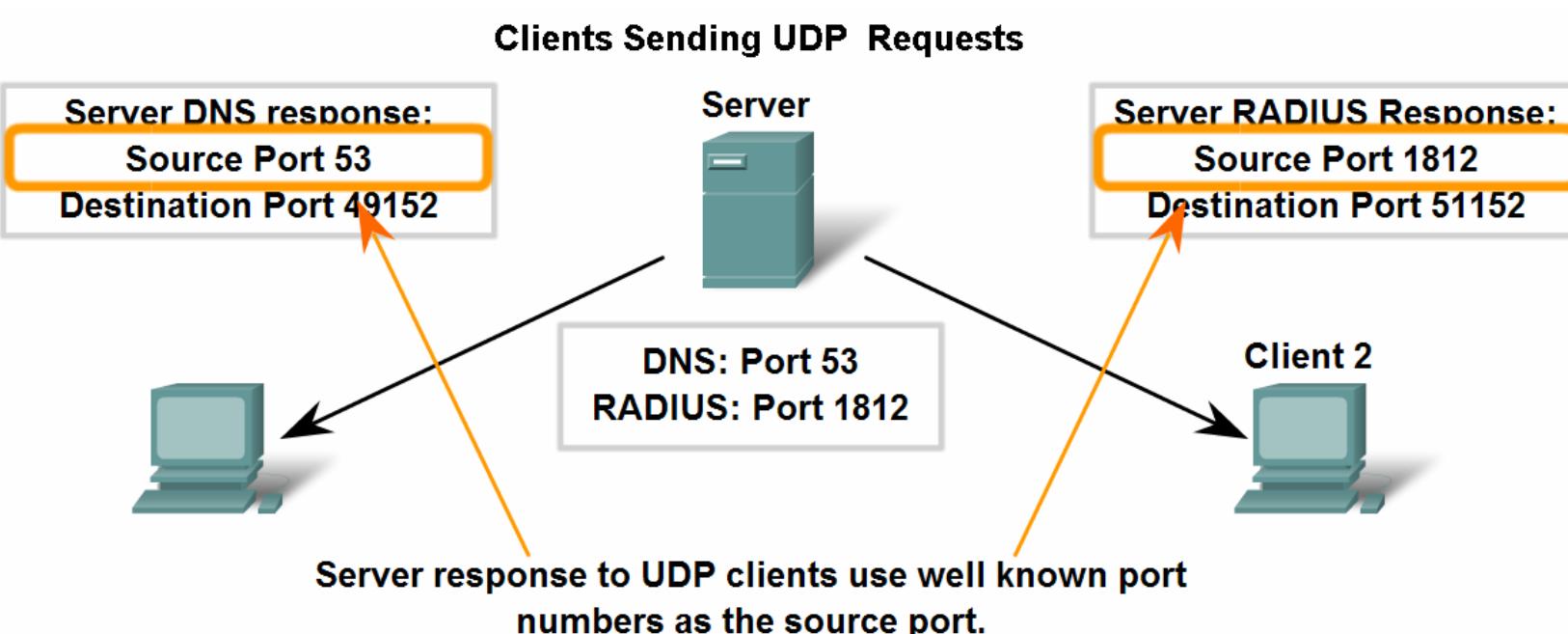
- Describe how servers use port numbers to identify a specified application layer process and direct segments to the proper service or application



Client requests to servers have well known ports numbers as the destination port.

UDP Protocol

- Trace the steps as the UDP protocol and port numbers are utilized in client-server communication.



Client 1 waiting for server DNS response on Port 49152

Client 2 waiting for server RADIUS response on Port 51152



Summary

In this chapter, you learned to:

- Explain the need for the Transport layer
- Identify the role of the Transport layer as it provides the end-to-end transfer of data between applications
- Describe the role of two TCP/IP Transport layer protocols, TCP and UDP
- Explain the key functions of the Transport layer including reliability, port addressing, and segmentation
- Explain how TCP and UDP each handle these key functions
- Identify when it is appropriate to use TCP or UDP and provide examples of applications that use each protocol





OSI Network Layer



Network Fundamentals – Chapter 5

Cisco | Networking Academy®
Mind Wide Open™

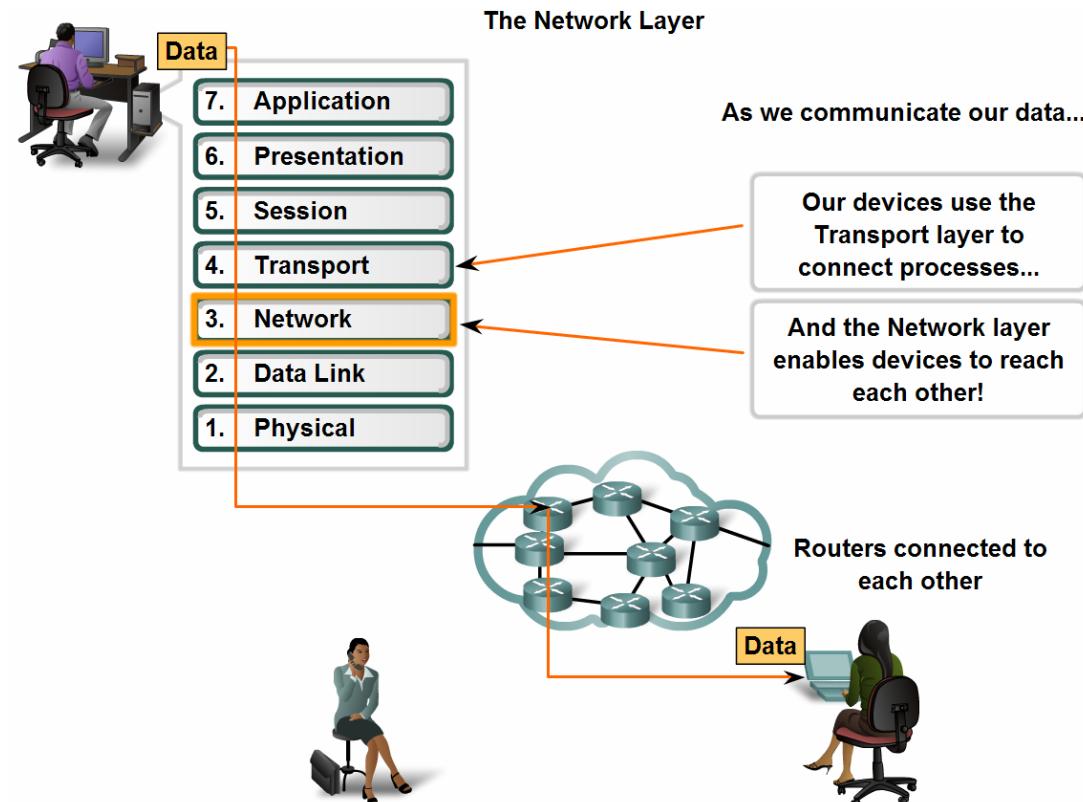


Objectives

- Identify the role of the Network Layer, as it describes communication from one end device to another end device
- Examine the most common Network Layer protocol, Internet Protocol (IP), and its features for providing connectionless and best-effort service
- Understand the principles used to guide the division or grouping of devices into networks
- Understand the hierarchical addressing of devices and how this allows communication between networks
- Understand the fundamentals of routes, next hop addresses and packet forwarding to a destination network

Network Layer Protocols and Internet Protocol (IP)

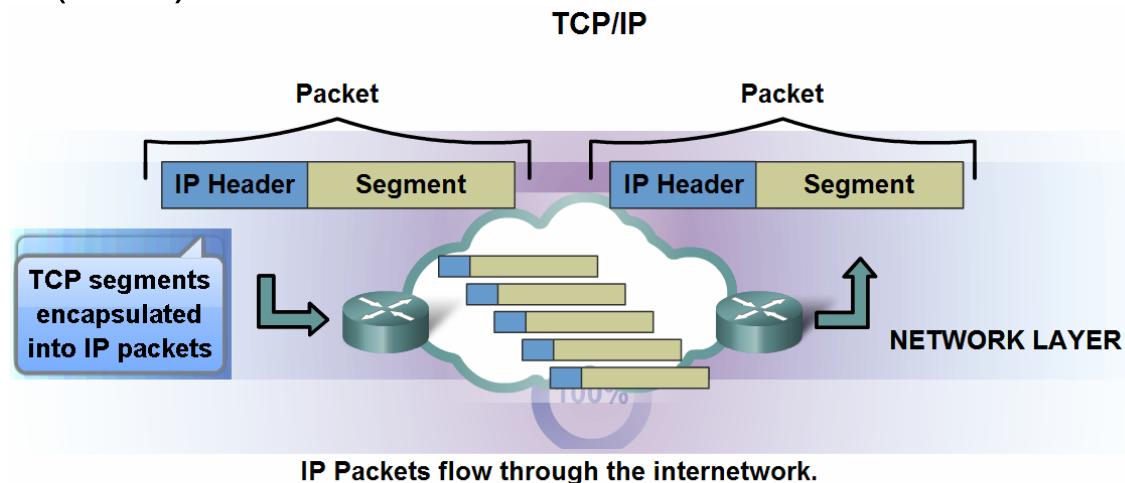
- The **Network layer**, or **OSI Layer 3**, provides services to exchange the individual pieces of data over the network between identified end devices.
- Four basic processes:
 - Addressing
 - Encapsulation
 - Routing
 - Decapsulation
- Fig. 5.1.1.1



Network Layer Protocols and Internet Protocol (IP)

- Protocols implemented at the Network layer that carry user data include:

- Novell Internetwork Packet Exchange (IPX)
- Internet Protocol v. 4 (IPv4)
- Internet Protocol v. 6 (IPv6)
- AppleTalk
- CLNS/DECNet

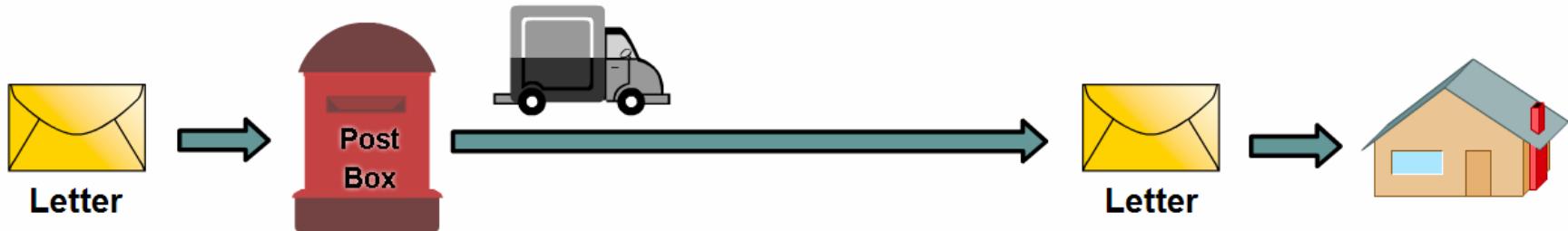


- Connectionless - No connection is established before sending data packets.
- Best Effort (unreliable) - No overhead is used to guarantee packet delivery.
- Media Independent - Operates independently of the medium carrying the data.

Network Layer Protocols and Internet Protocol (IP)

- The implications for the use of the IP protocol as it is **connectionless**

Connectionless Communication



A **letter** is sent.

The sender doesn't know:

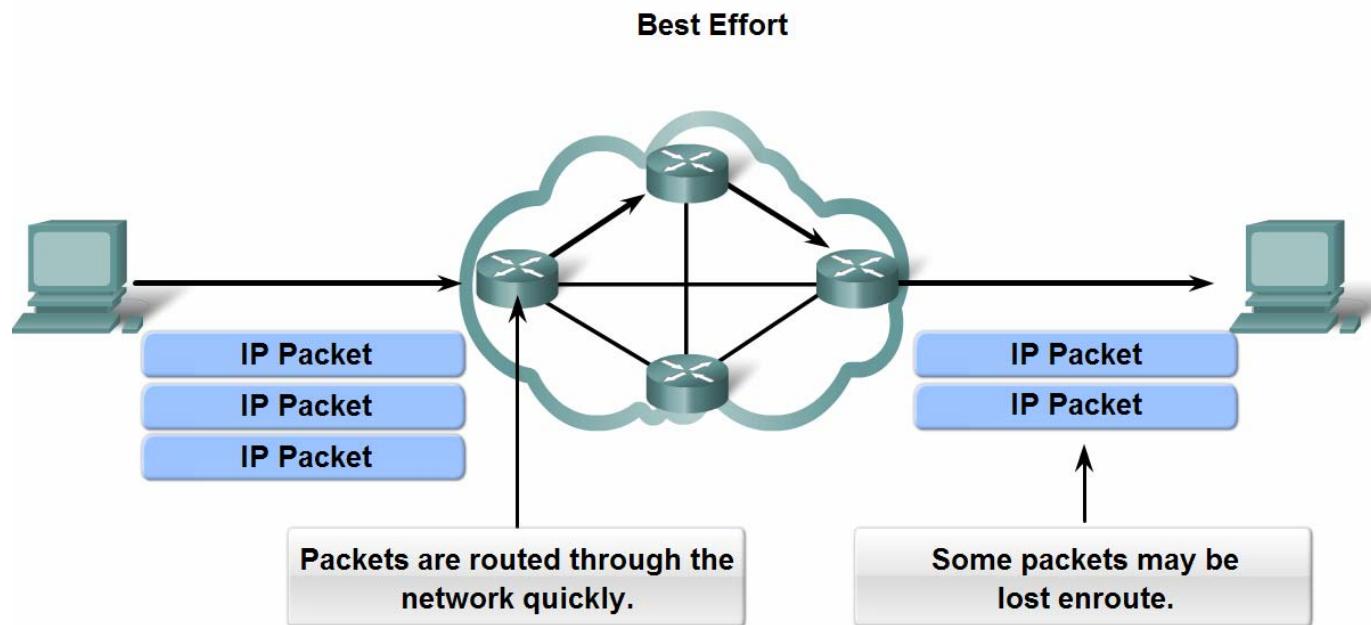
- if the receiver is present
- if the letter arrived
- if the receiver can read the letter

The receiver doesn't know:

- when it is coming

Network Layer Protocols and Internet Protocol (IP)

- The implications for the use of the IP protocol as it is considered an **unreliable protocol**

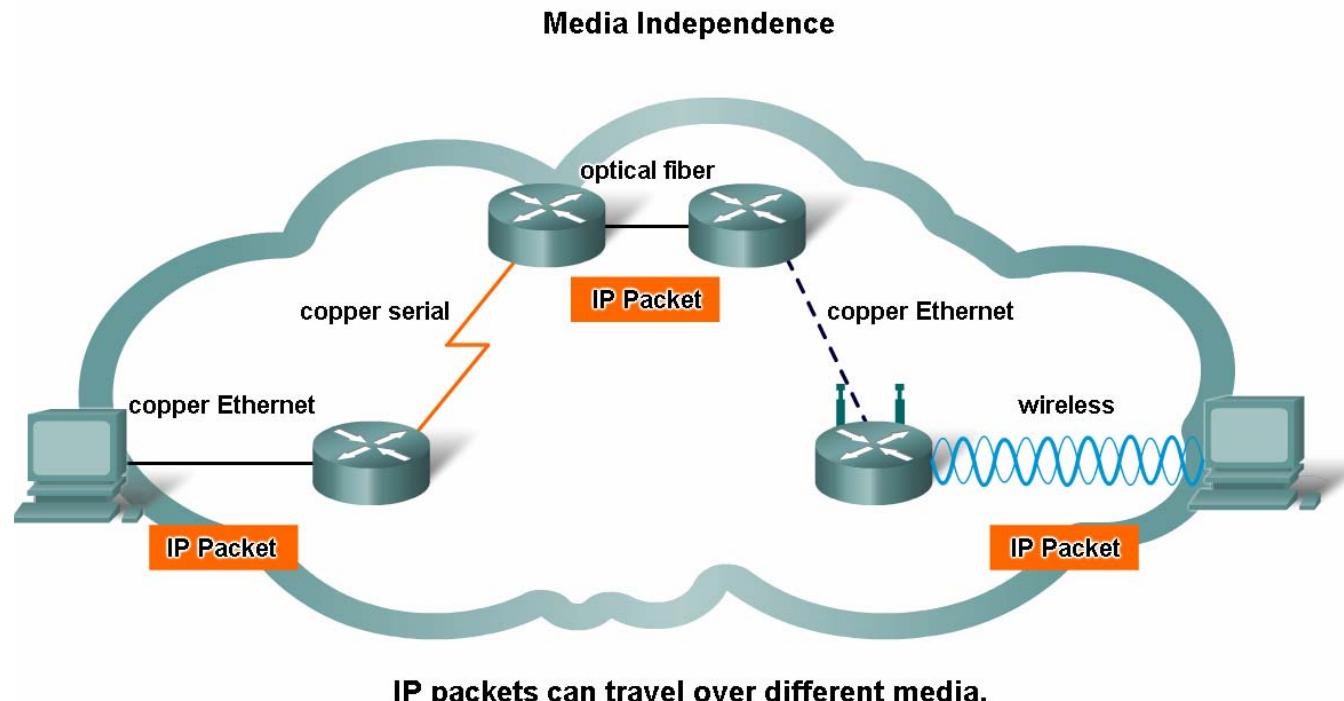


As an unreliable Network layer protocol, IP does not guarantee that all sent packets will be received.

Other protocols manage the process of tracking packets and ensuring their delivery.

Network Layer Protocols and Internet Protocol (IP)

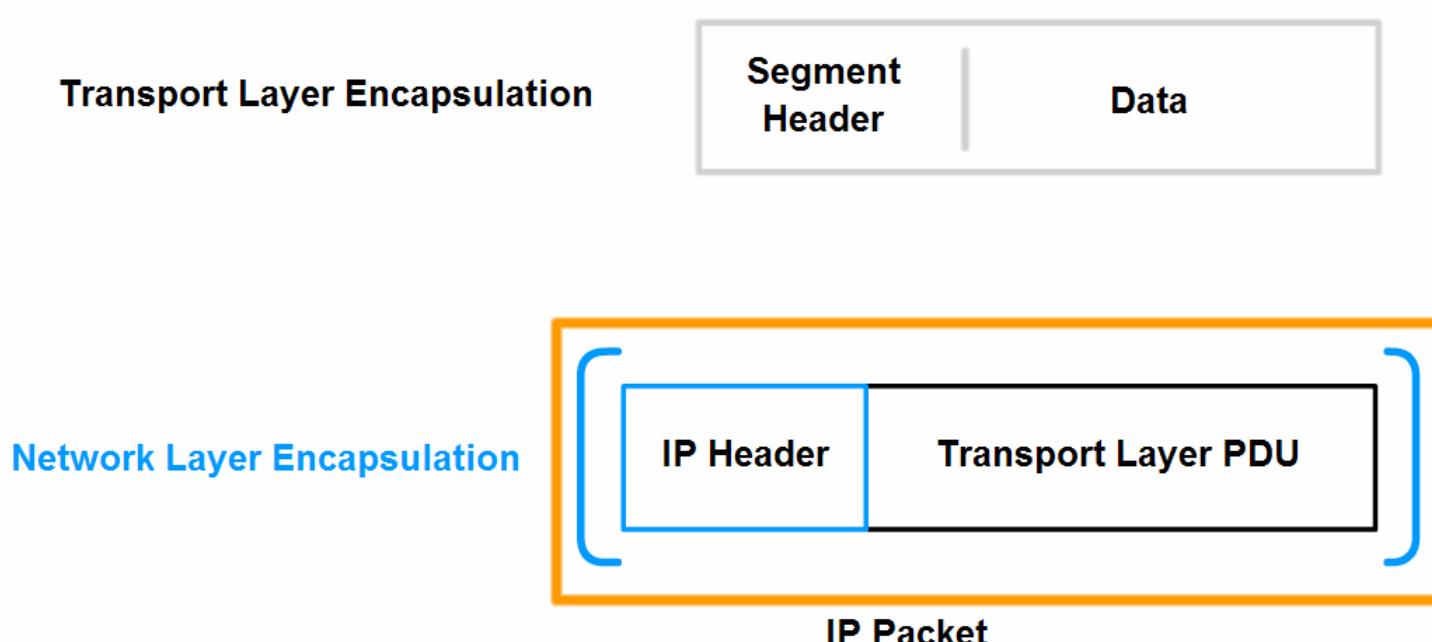
- The implications for the use of the IP as it is **media independent**
- One major characteristic of the media that the Network layer considers: the maximum size of PDU - **Maximum Transmission Unit (MTU)**



Network Layer Protocols and Internet Protocol (IP)

- The role of framing in the Transport Layer and
- Segments are encapsulated as packets

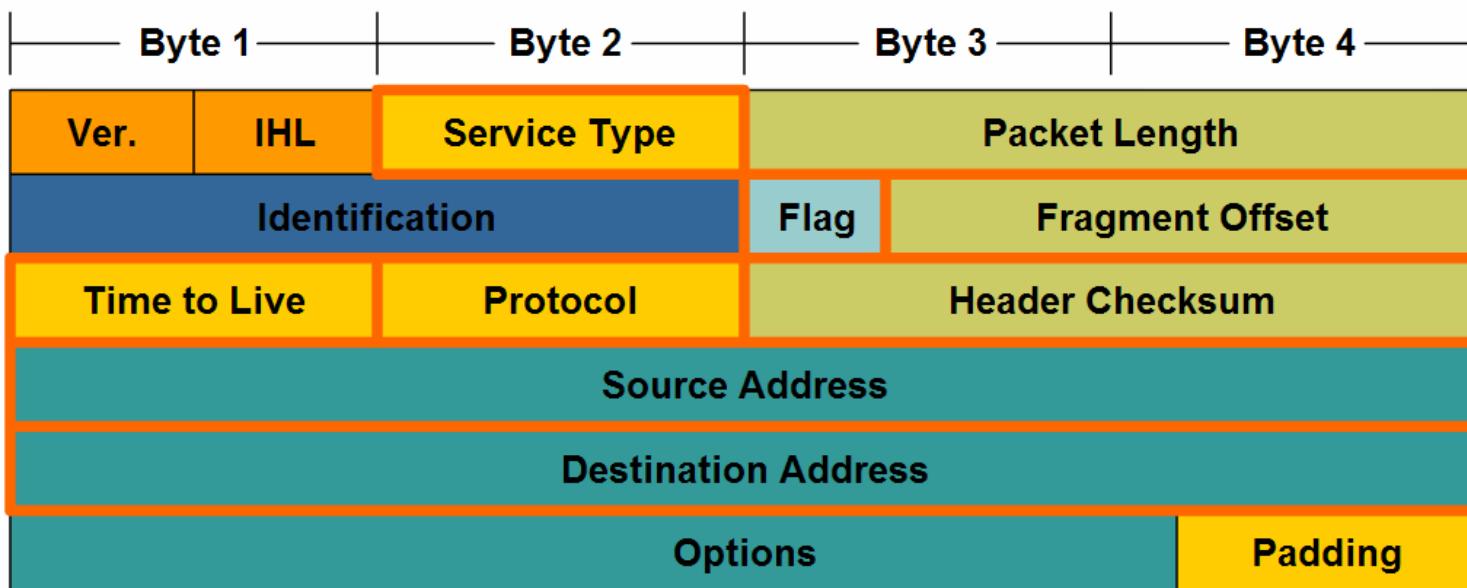
Generating IP Packets



In **TCP/IP based networks**, the Network layer PDU is the **IP packet**.

Network Layer Protocols and Internet Protocol (IP)

IPv4 Packet Header Fields



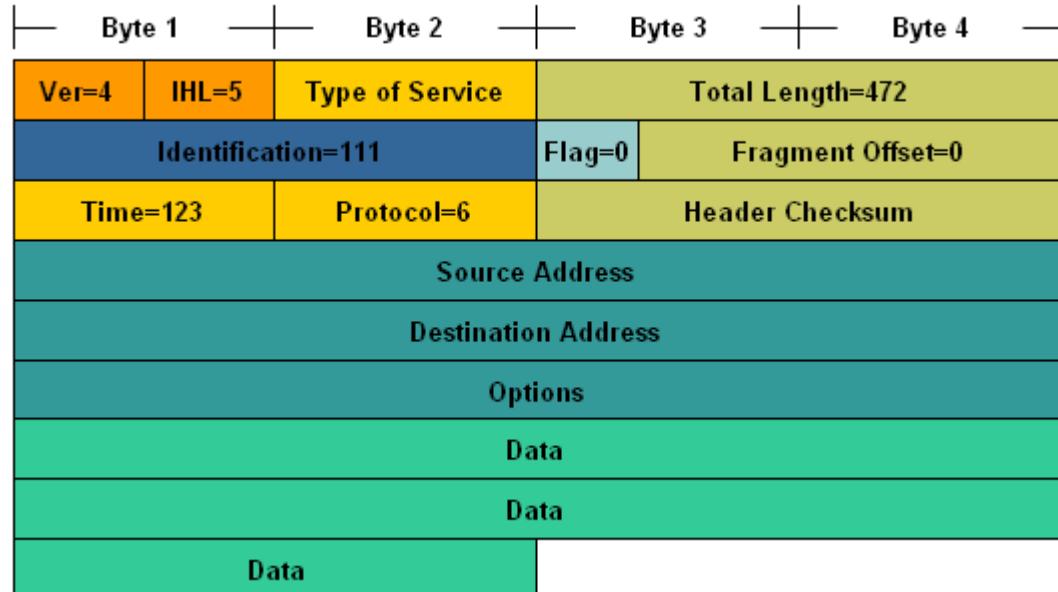


Network Layer Protocols and Internet Protocol (IP) – Fragment offset and MF flag

- When fragmentation occurs, the IPv4 packet uses the **Fragment Offset** field and the **MF** flag in the IP header to reconstruct the packet at the destination.
- The **fragment offset** field identifies the order in which to place the packet fragment in the reconstruction.
- When **MF (More fragments) = 1**, Fragment Offset must be examined to see where fragment is to be placed in the packet.
- When **MF = 0** and a non-zero value in the Fragment offset, it places that fragment as the last part of the reconstructed packet.
- An **unfragmented** packet has all zero fragmentation information (MF = 0, fragment offset =0).
- **Don't Fragment (DF)** flag is a single bit in the Flag field that indicates that fragmentation of the packet is not allowed.

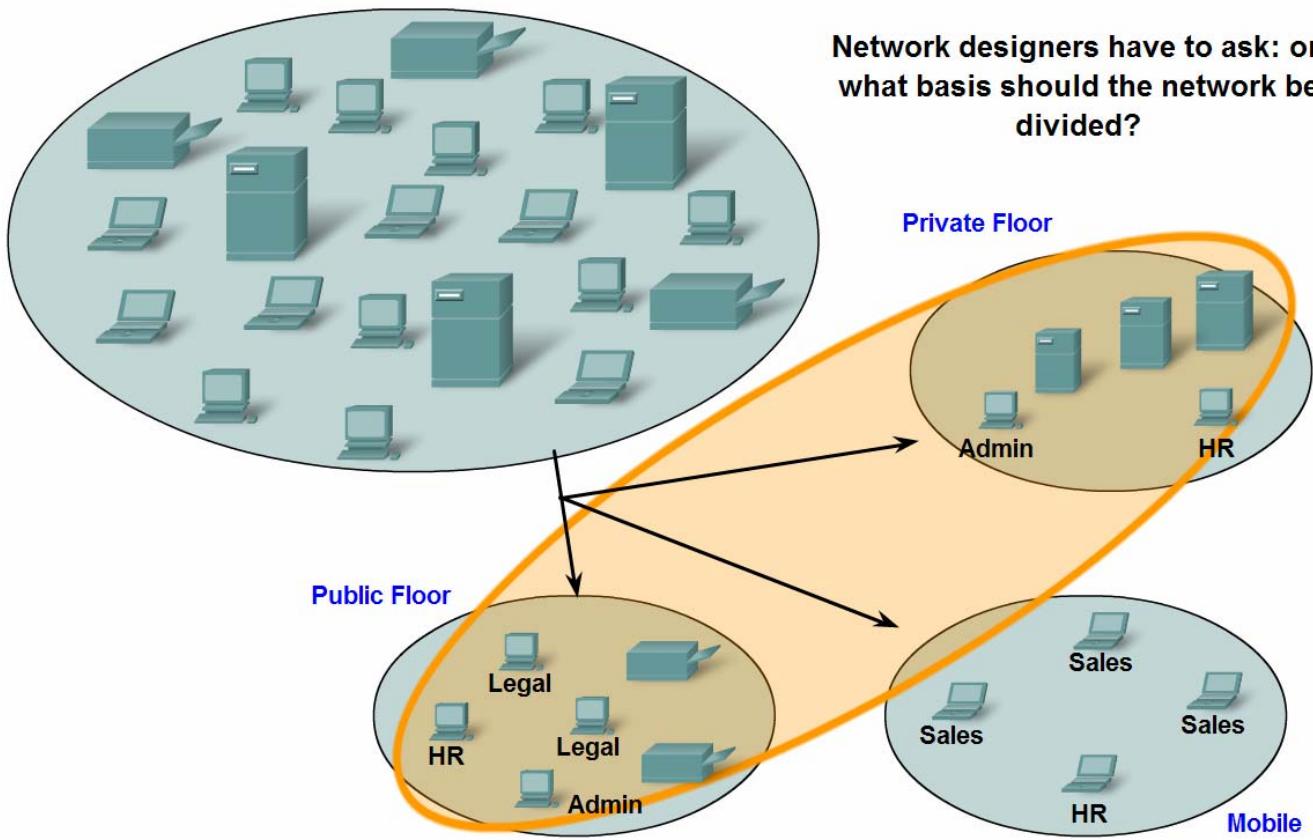
Network Layer Protocols and Internet Protocol (IP)

- **IHL = 5**; size of header in 32 bit words (4 bytes). This header is $5*4 = 20$ bytes, the minimum valid size.
- **Total Length = 472**; size of packet (header and data) is 472 bytes.
- **Identification = 111**; original packet identifier (required if it is later fragmented).
- **Time to Live = 123**; denotes the Layer 3 processing time in seconds before the packet is dropped (decremented by at least 1 every time a device processes the packet header).
- **Flag = 0**; denotes packet can be fragmented if required.
- **Fragment Offset = 0**; denotes that this packet is not currently fragmented (there is no offset).
- **Protocol = 6**; denotes that the data carried by this packet is a TCP segment .



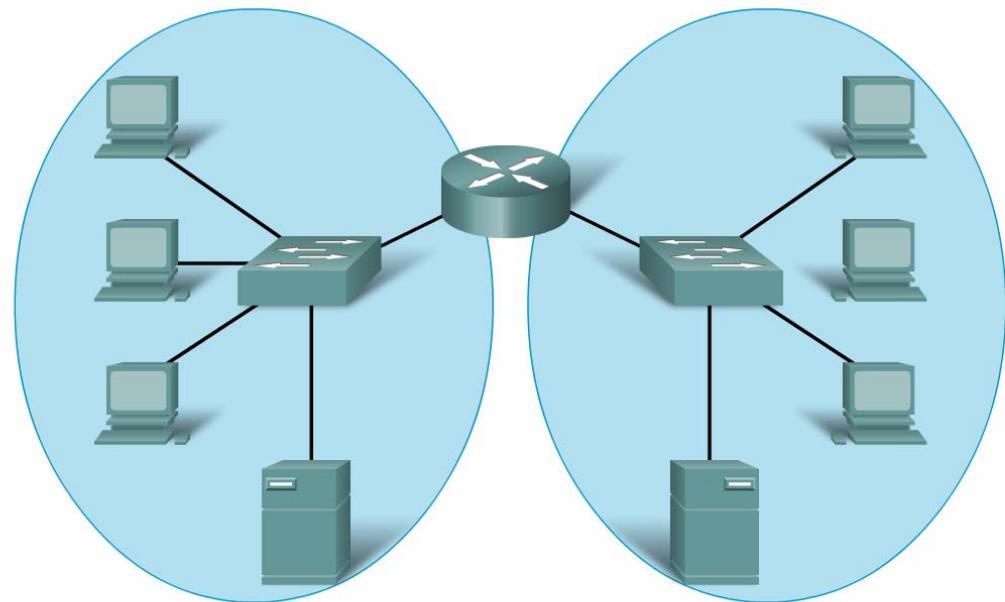
Grouping Devices into Networks and Hierarchical Addressing

- Reasons for grouping devices into sub-networks :
 - Geographic location
 - Purpose
 - Ownership



Grouping Devices into Networks and Hierarchical Addressing

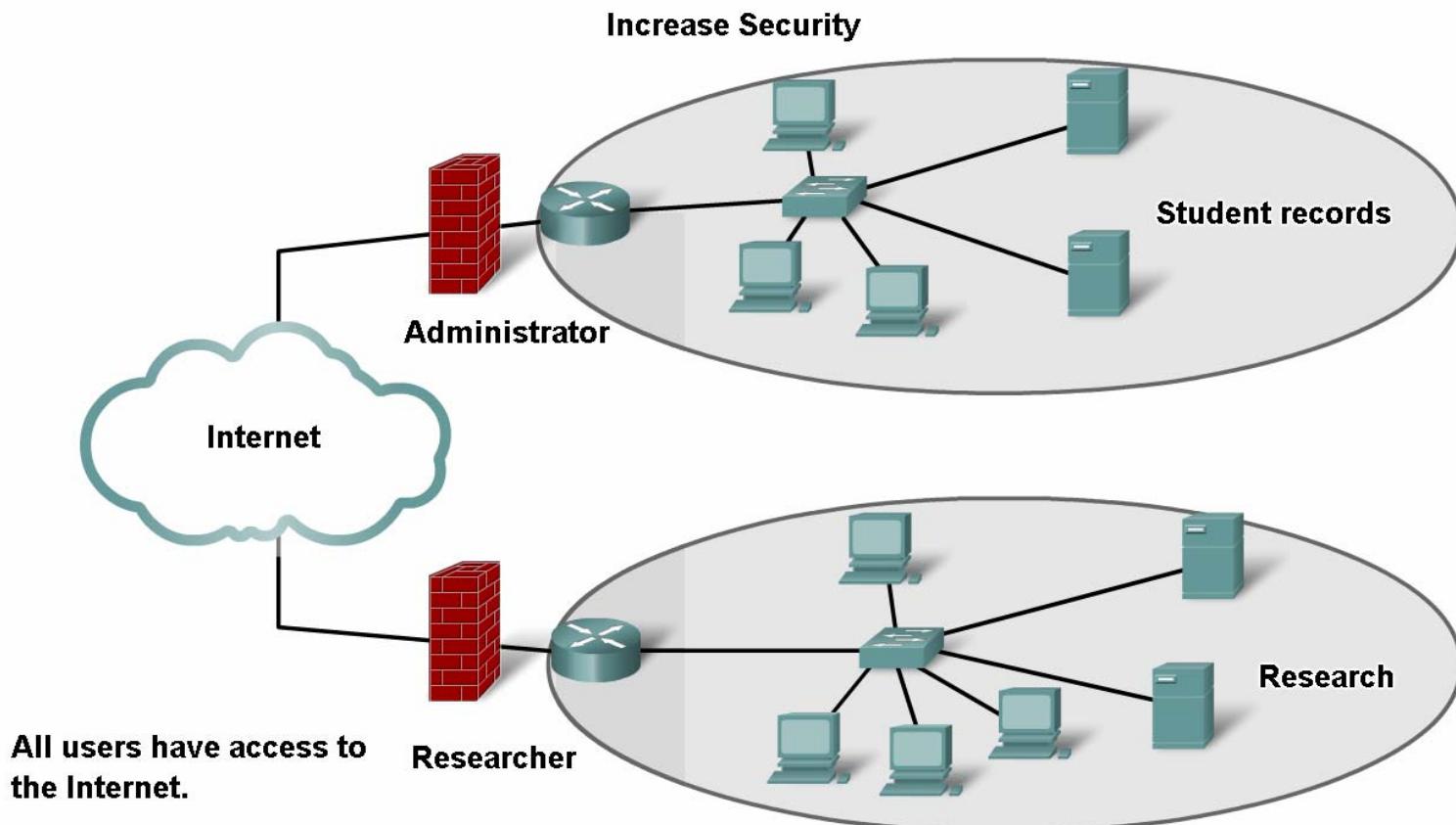
- Common issues with large networks are:
 - Performance degradation
 - Security issues
 - Address Management
- Dividing a large network can increase network **performance**



Replacing the middle switch with a router creates 2 IP subnets, hence, 2 distinct broadcast domains. All devices are connected but local broadcasts are contained.

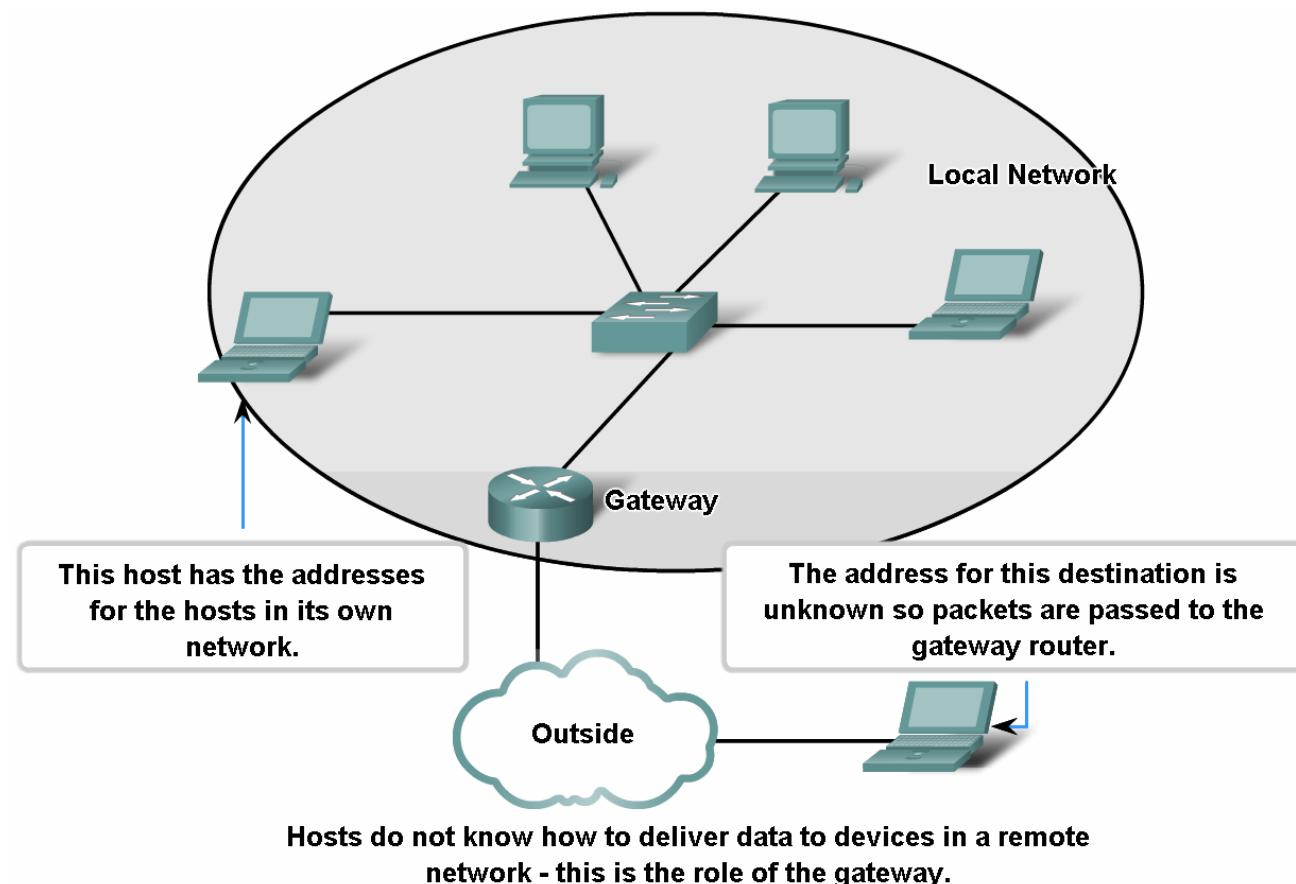
Grouping Devices into Networks and Hierarchical Addressing

- Dividing a large network can increase **network security**



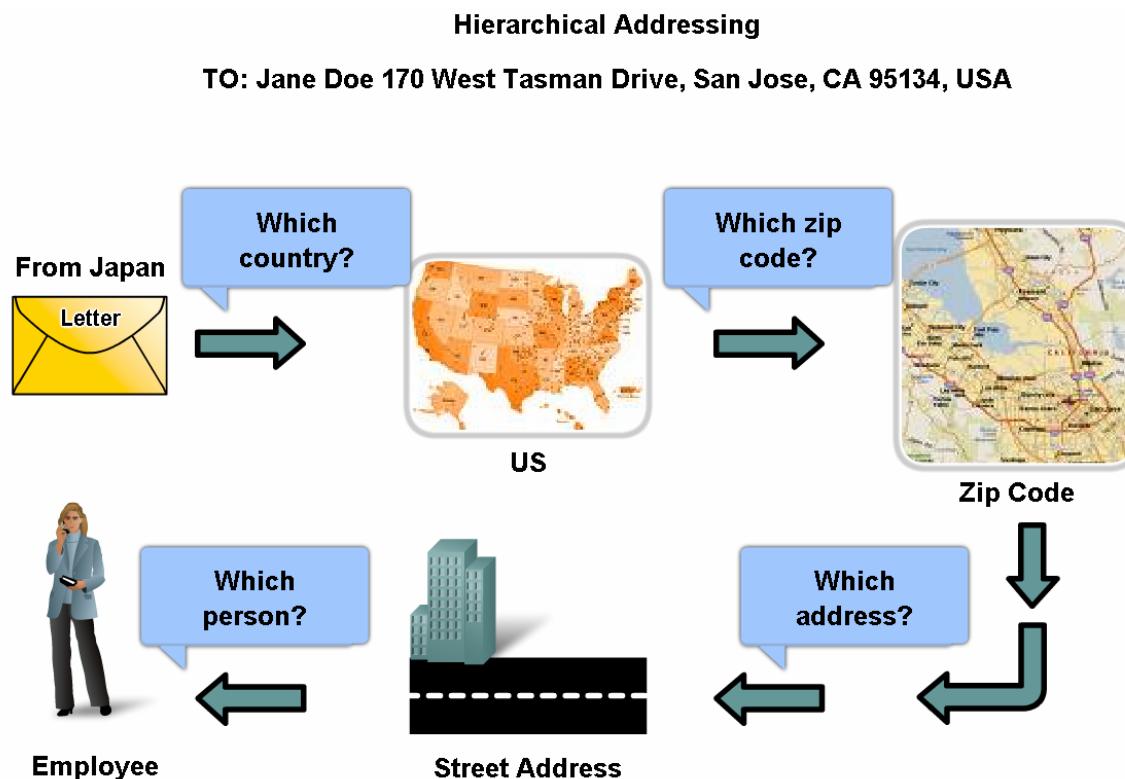
Grouping Devices into Networks and Hierarchical Addressing

- Communication problems that emerge when very large numbers of devices are included in one large network



Grouping Devices into Networks and Hierarchical Addressing

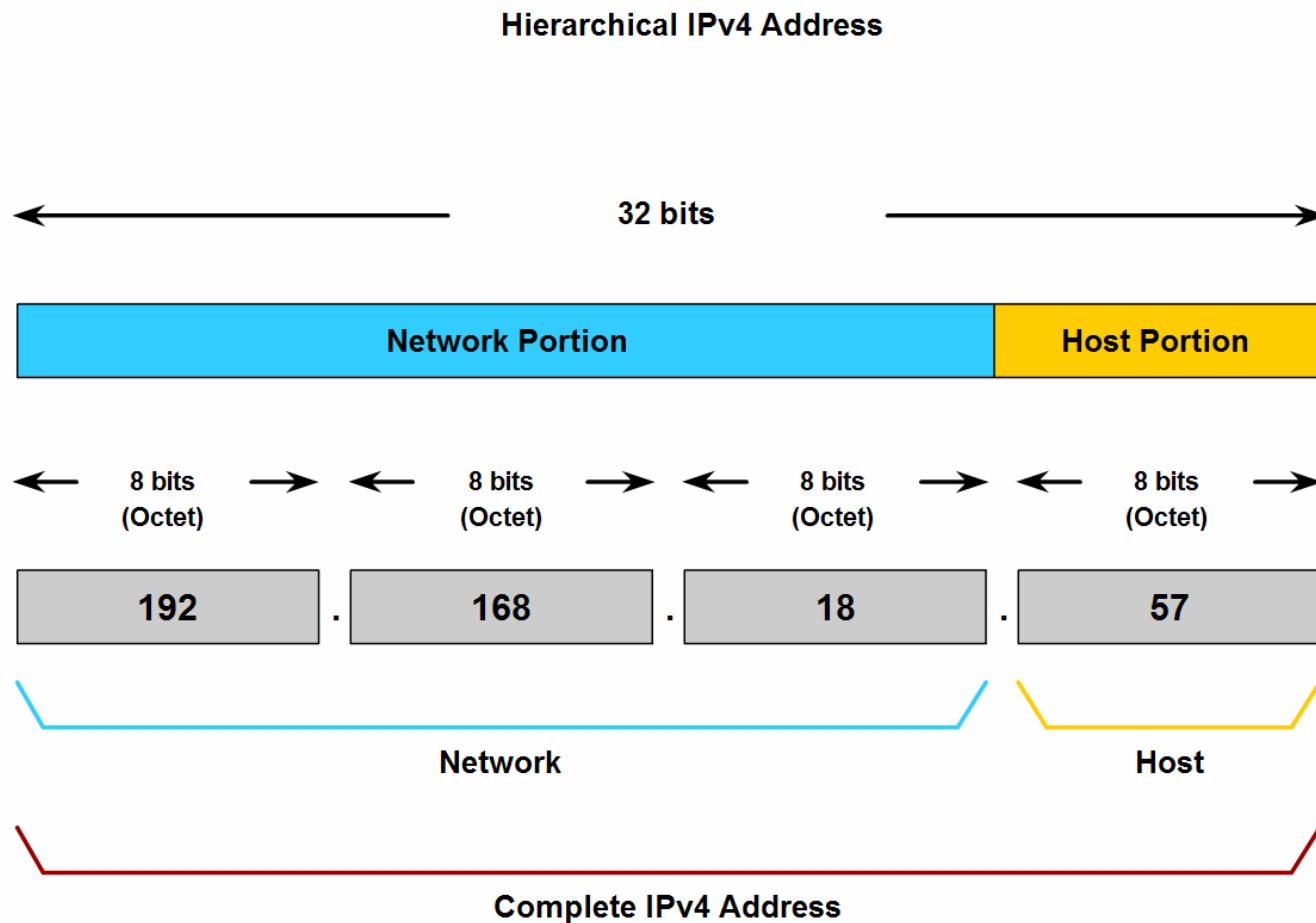
- How **hierarchical addressing** solves the problem of devices communicating across networks of networks



At each step of delivery, the post office need only examine the next hierarchical level.

Grouping Devices into Networks and Hierarchical Addressing

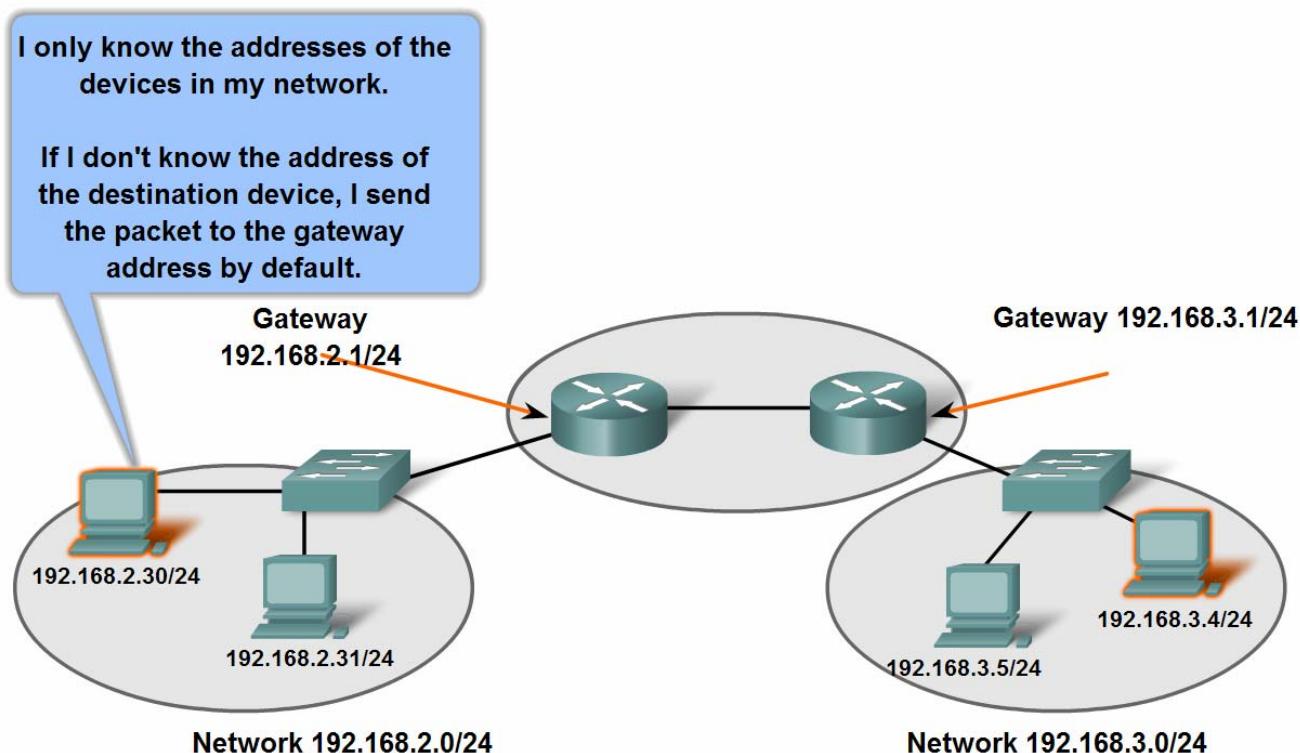
- The purpose of further subdividing networks into smaller networks



Fundamentals of Routes, Next Hop Addresses and Packet Forwarding

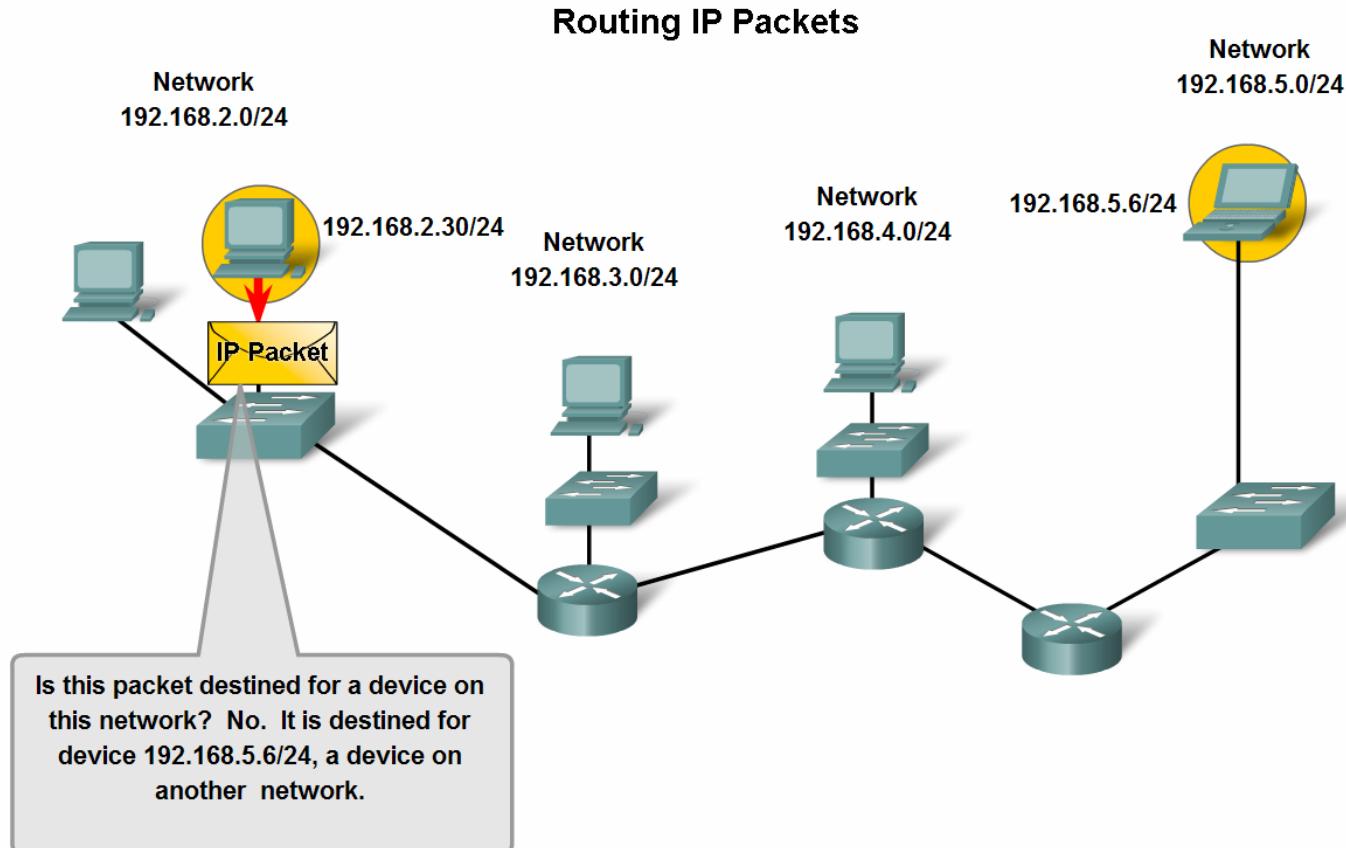
- The role of an intermediary gateway device in allowing devices to communicate across sub-divided networks

Gateways Enable Communications between Networks



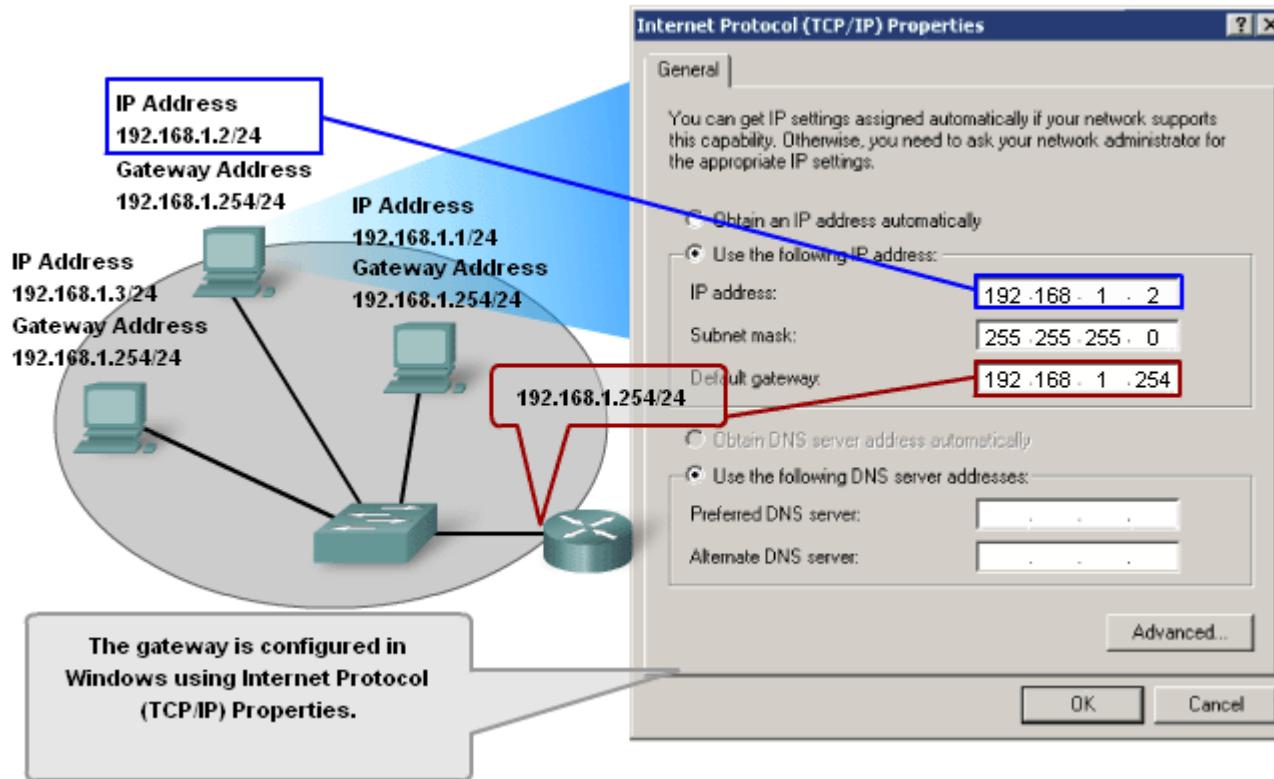
Fundamentals of Routes, Next Hop Addresses and Packet Forwarding

- Trace the steps of an IP packet as it traverses unchanged via routers from sub network to sub-network
- Fig. 5.3.2.1



Fundamentals of Routes, Next Hop Addresses and Packet Forwarding

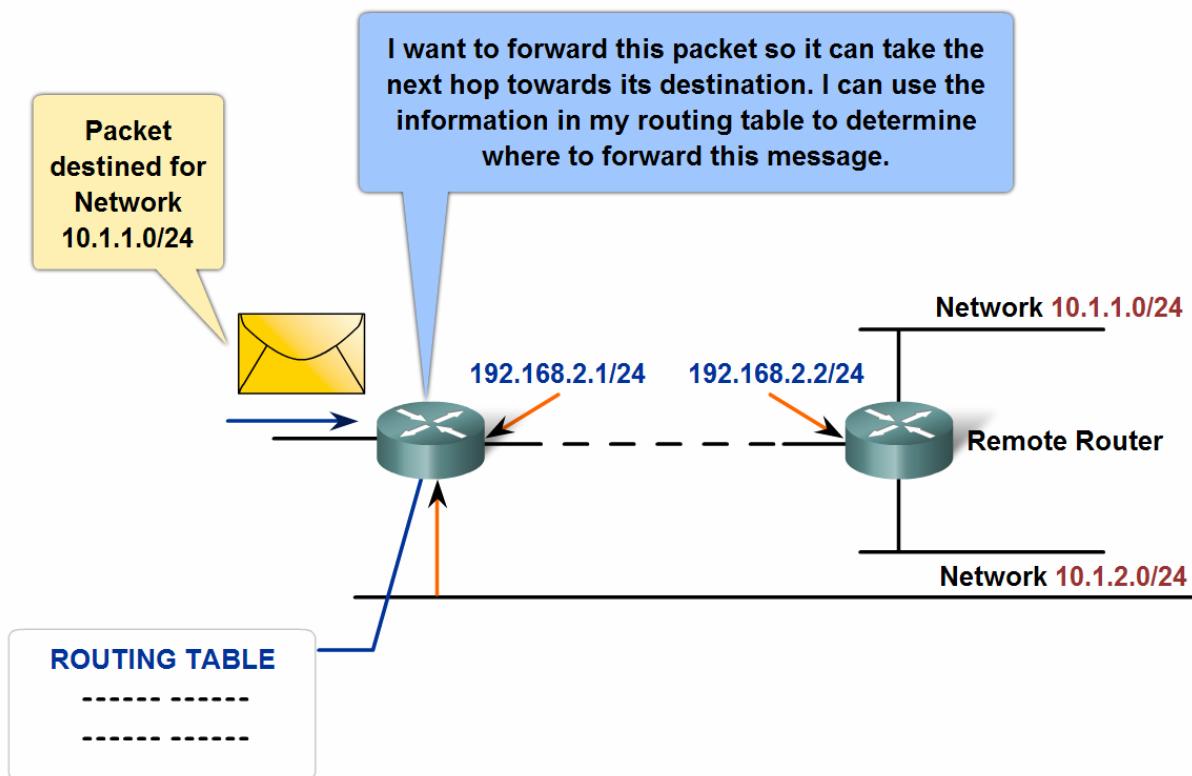
- The **gateway**, also known as the **default gateway**, is needed to send a packet out of the local network.



Fundamentals of Routes, Next Hop Addresses and Packet Forwarding

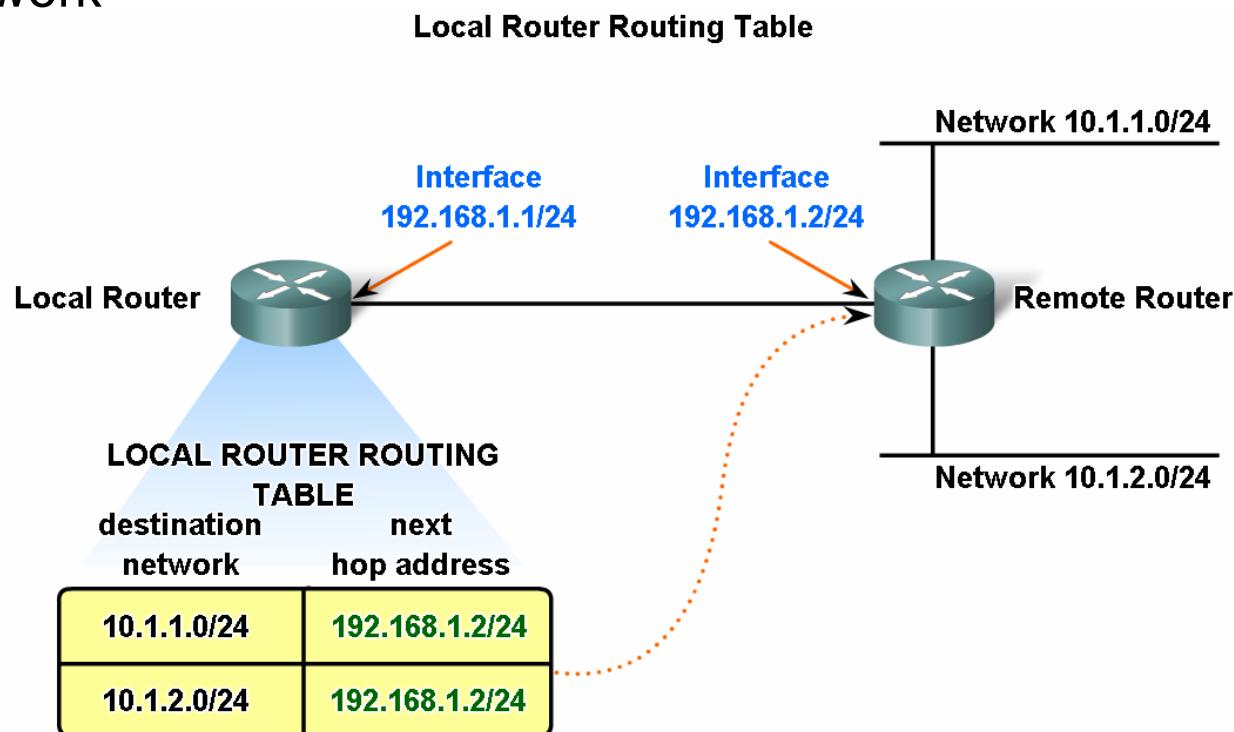
- No packet can be forwarded without a **route**.
- A host must either forward a packet to the **host** on the local network or to the **gateway**

Routing Tables



Fundamentals of Routes, Next Hop Addresses and Packet Forwarding

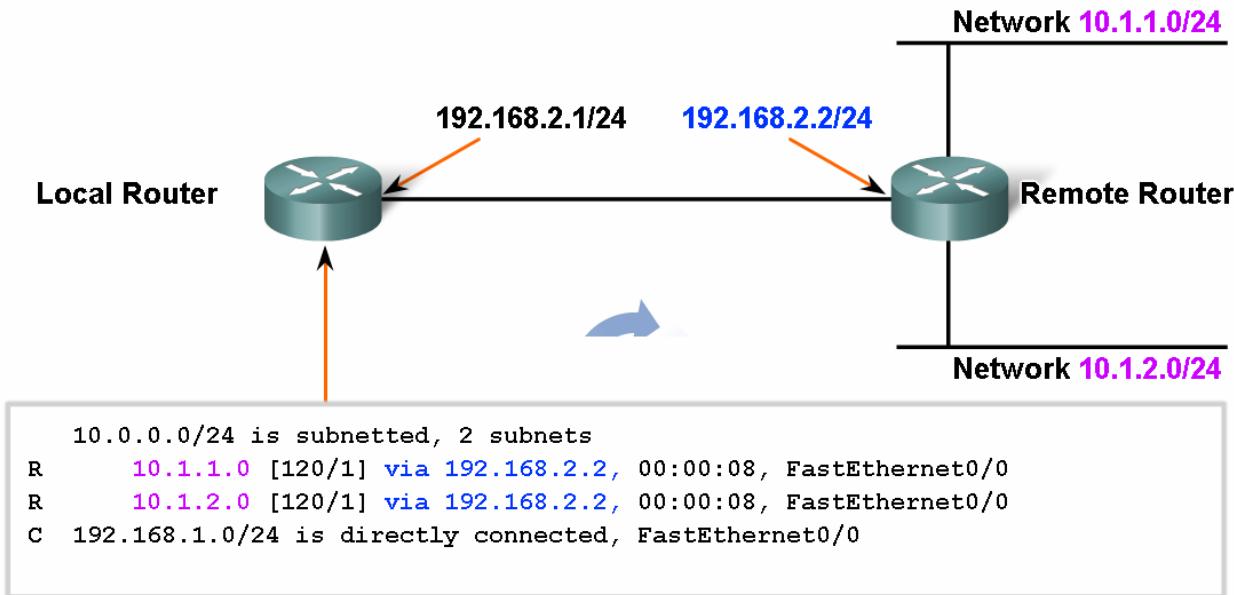
- To forward a packet the router must know where to send it. This information is available as **routes in a routing table**.
- Routes in a routing table have three main features:
 - Destination network
 - Next-hop
 - Metric



Fundamentals of Routes, Next Hop Addresses and Packet Forwarding

- The purpose and use of the destination network in a route

Confirming the Gateway and Route



This is the routing table output of Local Router when the "show ip route" is issued.

The next hop for networks 10.1.1.0/24 and 10.1.2.0/24 from Local Router is 192.168.2.2.

Fundamentals of Routes, Next Hop Addresses and Packet Forwarding

- The purpose and use of the next hop in a route
- **netstat -r, route, or route PRINT**

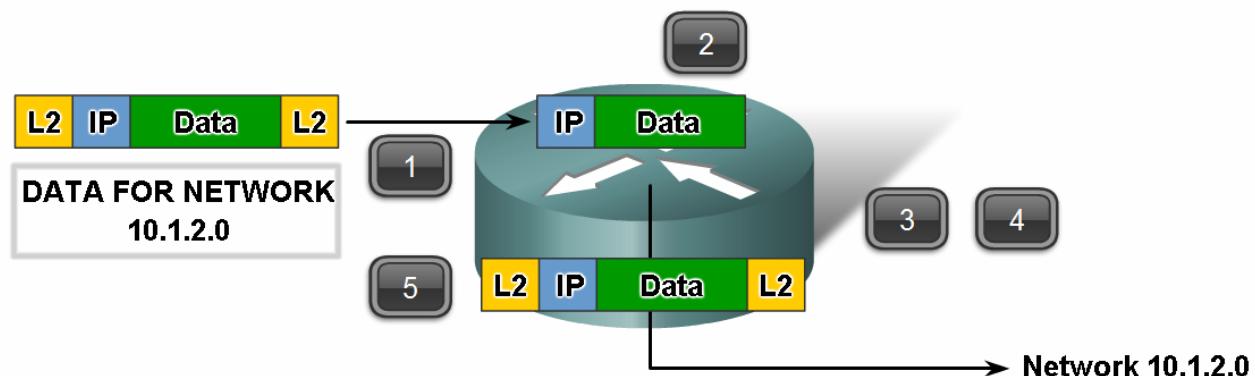
Routing Table Output with Next Hops

```
10.0.0.0/24 is subnetted, 2 subnets
R  10.1.1.0 [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
R  10.1.2.0 [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
C 192.168.1.0/24 is directly connected, FastEthernet0/0
```

Fundamentals of Routes, Next Hop Addresses and Packet Forwarding

- The router will do one of three things with the packet:
 - Forward it to the next-hop router
 - Forward it to the destination host
 - Drop it

Route Entry Exists

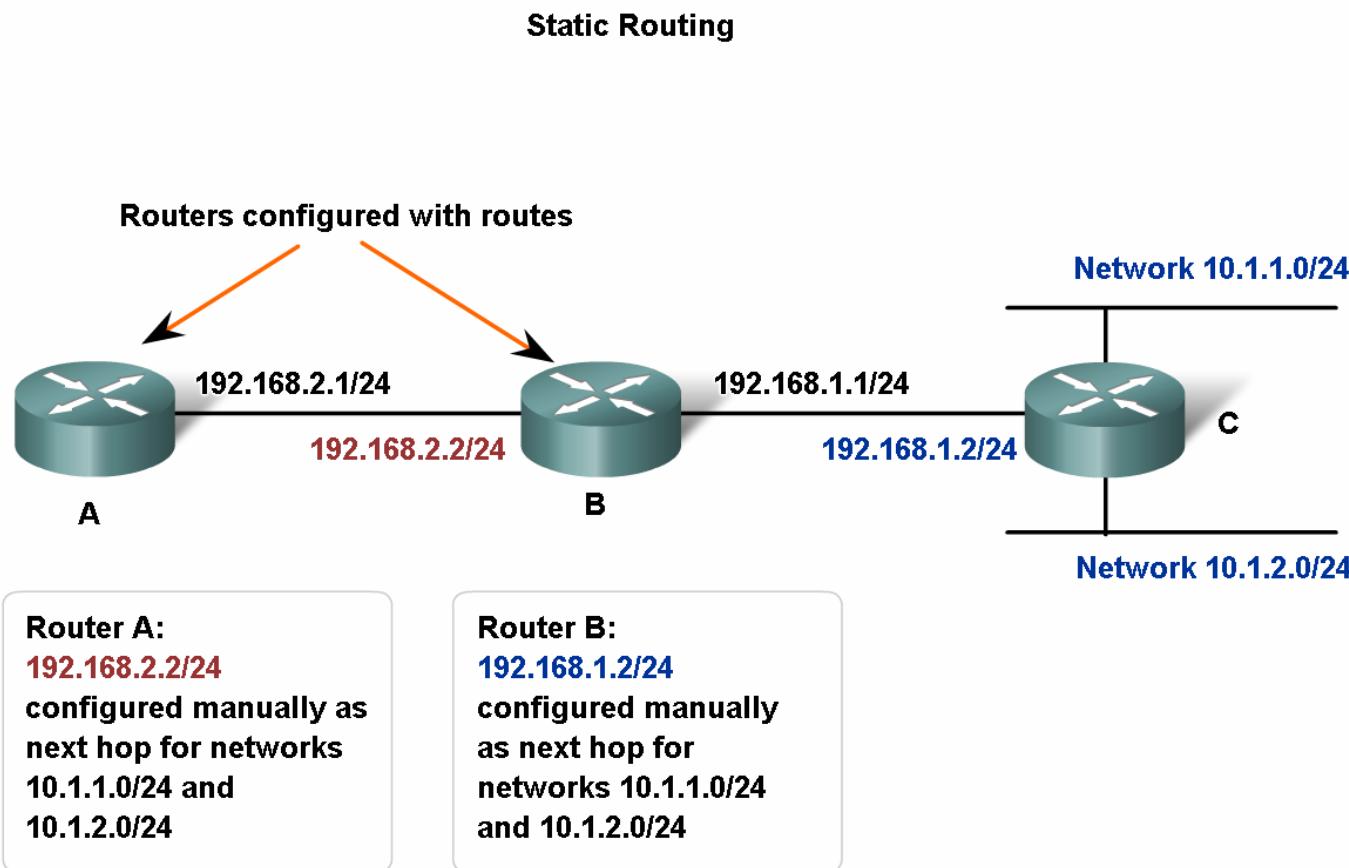


1. The router removes the Layer 2 encapsulation
2. Router extracts the destination IP address
3. Router checks the routing table for a match
4. Network 10.1.2.0 is found in the routing table
5. Router re-encapsulates the packet
6. Packet is sent to Network 10.1.2.0



Fundamentals of Routes, Next Hop Addresses and Packet Forwarding

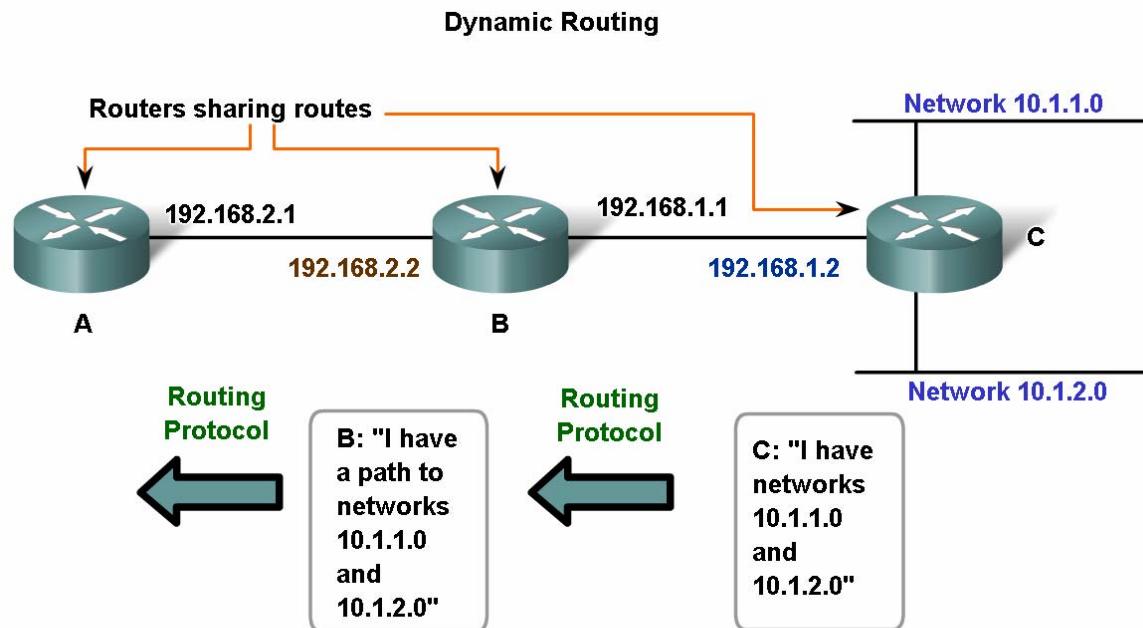
- The purpose of routing protocols and the need for both static and dynamic routes



Fundamentals of Routes, Next Hop Addresses and Packet Forwarding

- Common routing protocols are:

- Routing Information Protocol (RIP)
- Enhanced Interior Gateway Protocol (EIGRP)
- Open Shortest Path First (OSPF)



Router B learns about Router C's networks dynamically.

Router B's next hop to 10.1.1.0 and 10.1.2.0 is 192.168.1.2 (Router C).

Router A learns about Router C's networks dynamically from Router B.

Router A's next hop to 10.1.1.0 and 10.1.2.0 is 192.168.2.2 (Router B).



Summary

In this chapter, you learned to:

- Identify the role of the Network layer as it describes communication from one end device to another end device.
- Examine the most common Network layer protocol, Internet Protocol (IP), and its features for providing connectionless and best-effort service.
- Describe the principles used to guide the division, or grouping, of devices into networks.
- Explain the purpose of the hierarchical addressing of devices and how this allows communication between networks.
- Describe the fundamentals of routes, next-hop addresses, and packet forwarding to a destination network.





Addressing the Network – IPv4



Network Fundamentals – Chapter 6

Cisco | Networking Academy®
Mind Wide Open™

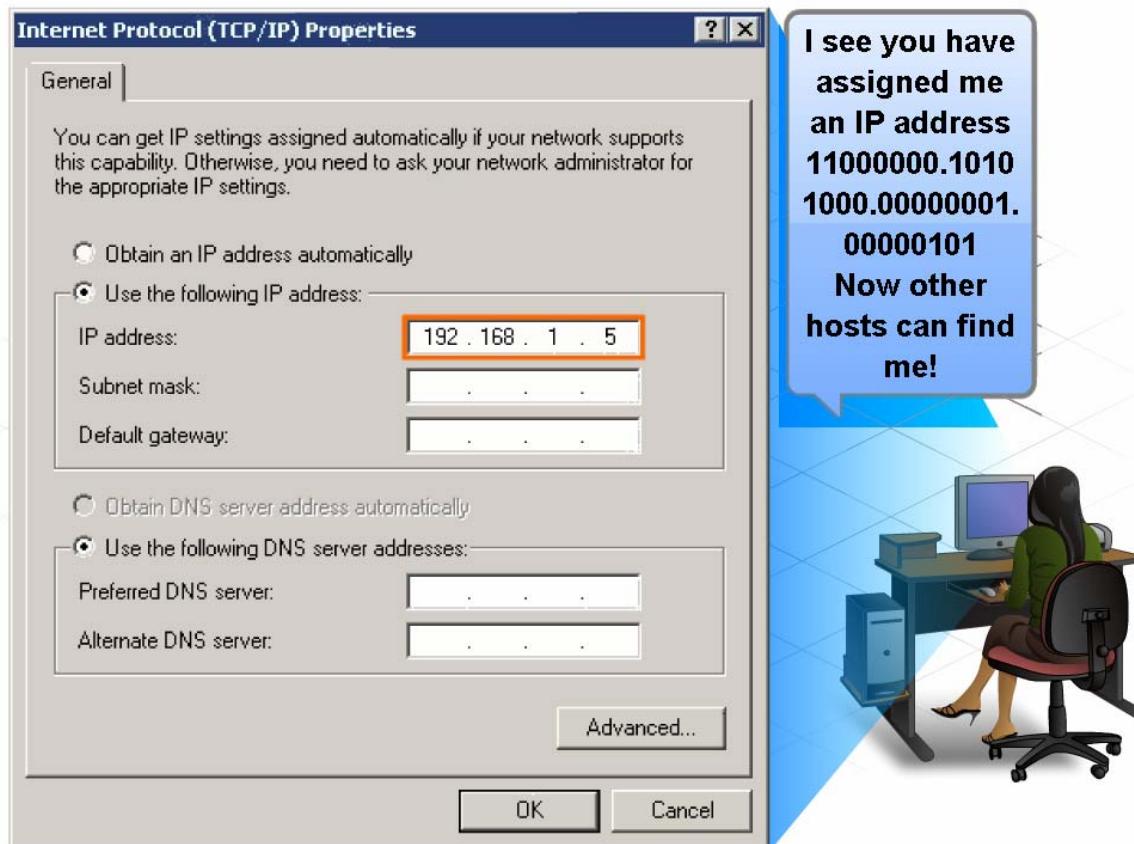


Objectives

- Explain the structure IP addressing and demonstrate the ability to convert between 8-bit binary and decimal numbers.
- Given an IPv4 address, classify by type and describe how it is used in the network
- Explain how addresses are assigned to networks by ISPs and within networks by administrators
- Determine the network portion of the host address and explain the role of the subnet mask in dividing networks.
- Given IPv4 addressing information and design criteria, calculate the appropriate addressing components.
- Use common testing utilities to verify and test network connectivity and operational status of the IP protocol stack on a host.

IP Addressing Structure

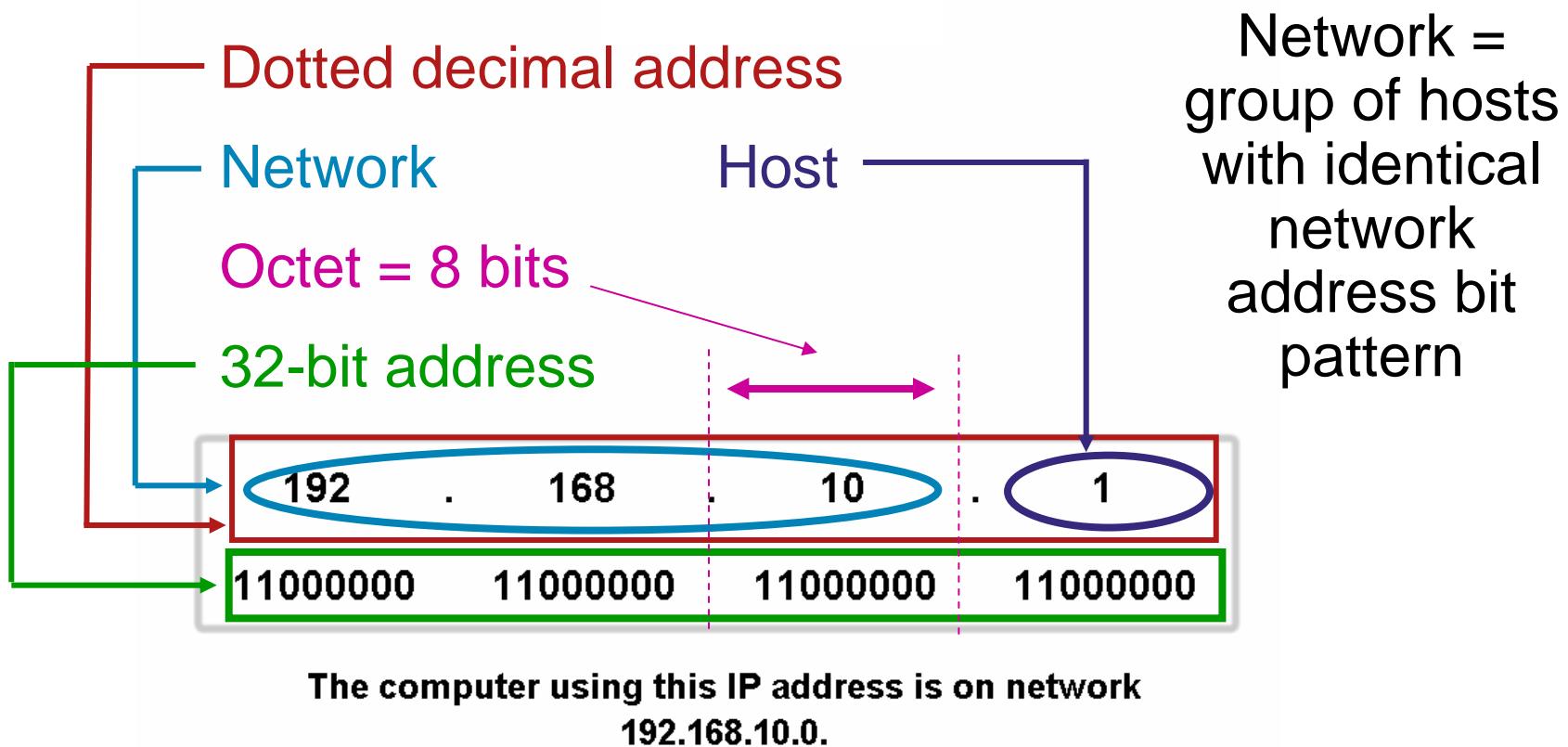
- Describe the dotted decimal structure of a binary IP address and label its parts



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

IP Addressing Structure

- Describe the general role of 8-bit binary in network addressing and convert 8-bit binary to decimal



IP Addressing Structure

- What is a network MASK?
 - Identifies the network portion of the IP address

IP:	10010011 10101100	00101001 00011001
Mask:	11111111 11111111	00000000 00000000
AND		
Network:	10010011 10101100	00000000 00000000

- $255.255.0.0 = /16$ (prefix notation)

IP Addressing Structure

- Practice converting 8-bit binary to decimal

Binary To Decimal Conversion

$$1*2^7+1*2^6+1*2^5+1*2^4+0*2^3+1*2^2+0*2^1+1*2^0 =$$

$$128+64+32+16+0+4+0+1 = 245$$

Exponent	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Position	128	64	32	16	8	4	2	1
Bits	1	1	1	1	0	1	0	1
Add these numbers together								1 BYTE / 1 Octet
Decimal	128 + 64 + 32 + 16 + 0 + 4 + 0 + 1							245

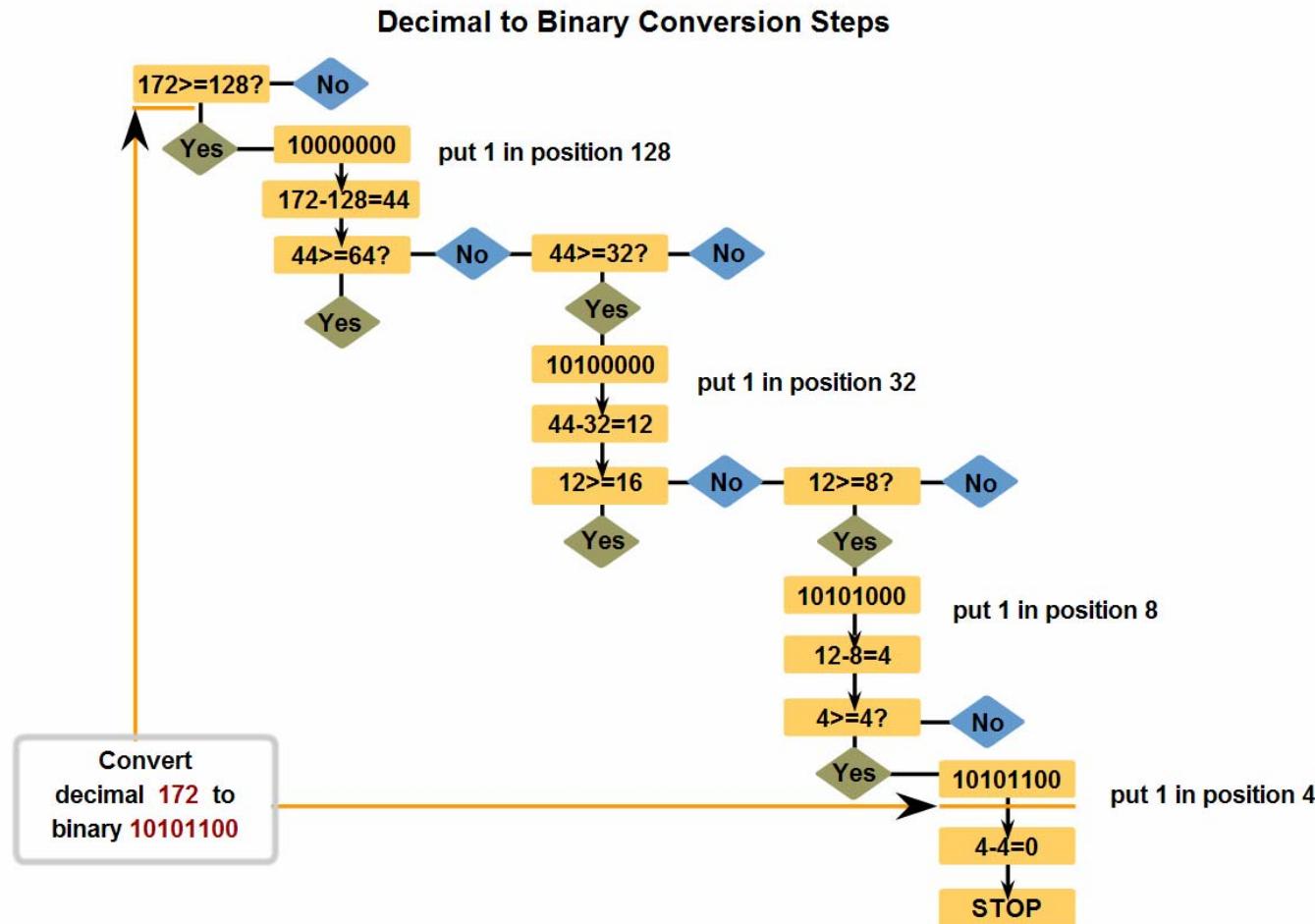
A 1 in this position means 64 is added to the total.

A 0 in any position means that 0 added to the total.

11110101 in Binary = Decimal Number 245

IP Addressing Structure

- Convert decimal to 8-bit binary





IP Addressing Structure

- Practice converting decimal to 8-bit binary (6.1.3, 6.1.5)
- Write down Your answers!
- Practise @home ! ☺

Decimal to Binary Conversion Activity

Given a decimal value, enter the correct binary values for each position.

Decimal Value	209							
Exponent	2^7 th	2^6 th	2^5 th	2^4 th	2^3 rd	2^2 nd	2^1 st	2^0
Position	128	64	32	16	8	4	2	1
Bit	<input type="text"/>							

Enter numbers for these 8 positions.



IP Addressing Structure

- Practice converting decimal to 8-bit binary

Decimal to Binary Conversion Activity

Given a decimal value, enter the correct binary values for each position.

Decimal Value	209							
Exponent	2^7 th	2^6 th	2^5 th	2^4 th	2^3 rd	2^2 nd	2^1 st	2^0
Position	128	64	32	16	8	4	2	1
Bit	1	1	0	1	0	0	0	1

Enter numbers for these 8 positions.

IP Addressing Structure

- Convert an IPv4 Dotted Decimal Notation to Binary

Convert Decimal to Binary

Decimal IPv4 address 172.16.4.20

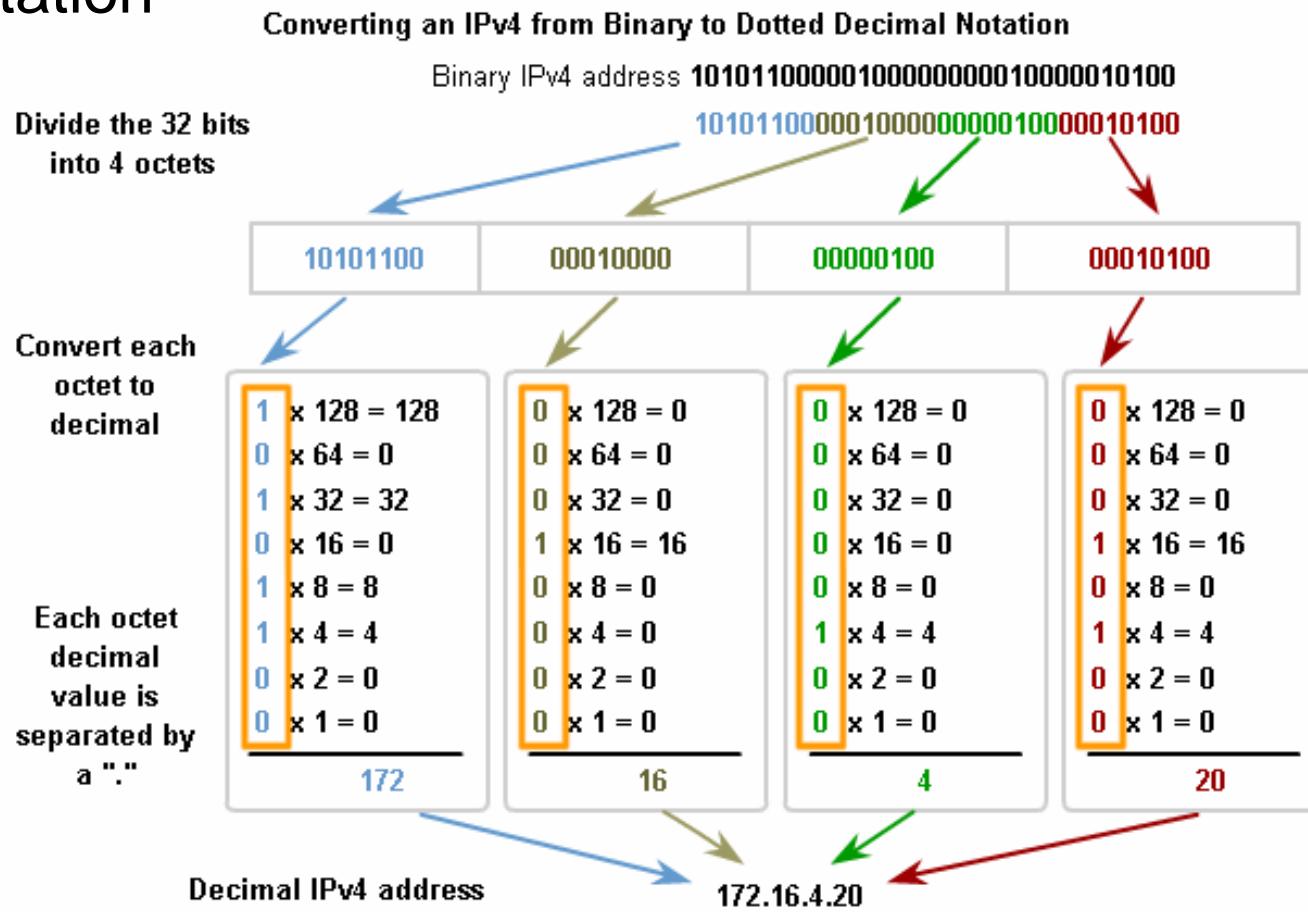
Separate and convert each decimal number separately

Convert 172	Convert 16	Convert 4	Convert 20
$172 - 128 = 44 \rightarrow 1 \times 128$	$16 < 128 \rightarrow 0 \times 128$	$4 < 128 \rightarrow 0 \times 128$	$20 < 128 \rightarrow 0 \times 128$
$44 - 64 = 0 \rightarrow 0 \times 64$	$16 < 64 \rightarrow 0 \times 64$	$4 < 64 \rightarrow 0 \times 64$	$20 < 64 \rightarrow 0 \times 64$
$44 - 32 = 12 \rightarrow 1 \times 32$	$16 < 32 \rightarrow 0 \times 32$	$4 < 32 \rightarrow 0 \times 32$	$20 < 32 \rightarrow 0 \times 32$
$12 - 16 = 0 \rightarrow 0 \times 16$	$16 - 16 = 0 \rightarrow 1 \times 16$	$4 < 16 \rightarrow 0 \times 16$	$20 - 16 = 4 \rightarrow 1 \times 16$
$12 - 8 = 4 \rightarrow 1 \times 8$	$0 < 8 \rightarrow 0 \times 8$	$4 < 8 \rightarrow 0 \times 8$	$4 < 8 \rightarrow 0 \times 8$
$4 - 4 = 0 \rightarrow 1 \times 4$	$0 < 4 \rightarrow 0 \times 4$	$4 - 4 = 0 \rightarrow 1 \times 4$	$4 - 4 = 0 \rightarrow 1 \times 4$
$0 < 2 = 0 \rightarrow 0 \times 2$	$0 < 2 \rightarrow 0 \times 2$	$0 < 2 \rightarrow 0 \times 2$	$0 < 2 \rightarrow 0 \times 2$
$0 < 1 = 0 \rightarrow 0 \times 1$	$0 < 1 \rightarrow 0 \times 1$	$0 < 1 \rightarrow 0 \times 1$	$0 < 1 \rightarrow 0 \times 1$

Binary IPv4 address 10101100 000100000000010000010100

IP Addressing Structure

- Convert an IPv4 from Binary to Dotted Decimal Notation



Classify and Define IPv4 Addresses

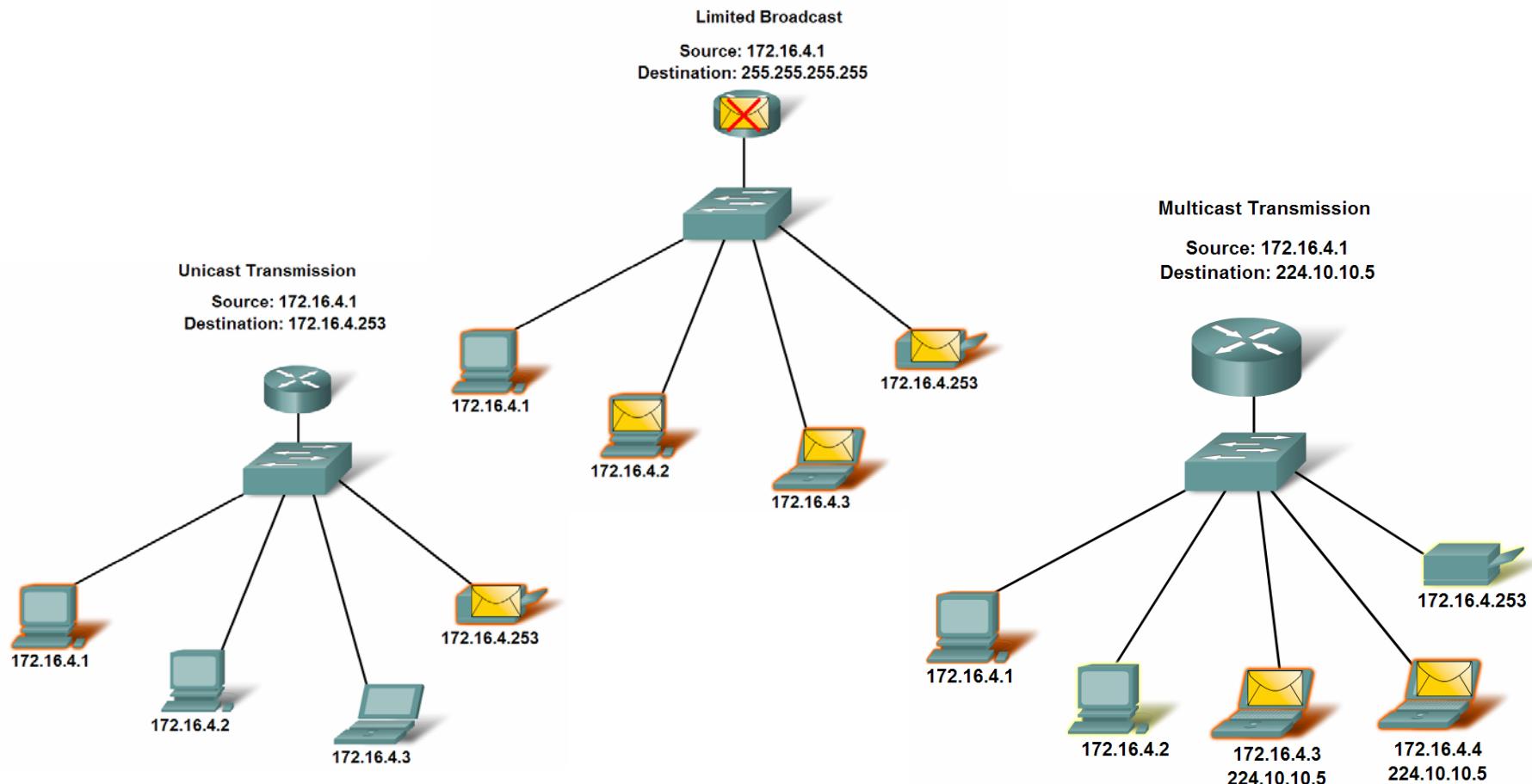
- Name the three types of addresses in the network and describe the purpose of each type

Address Types

	Network			Host
Network Address	10	0	0	0
	00001010	0000000	0000000	0000000
Broadcast Address	10	0	0	255
	11111111	0000000	0000000	11111111
Host Address	10	0	0	0
	00001010	0000000	0000000	0000001

Classify and Define IPv4 Addresses

- Name the three types of communication in the Network Layer and describe the characteristics of each type



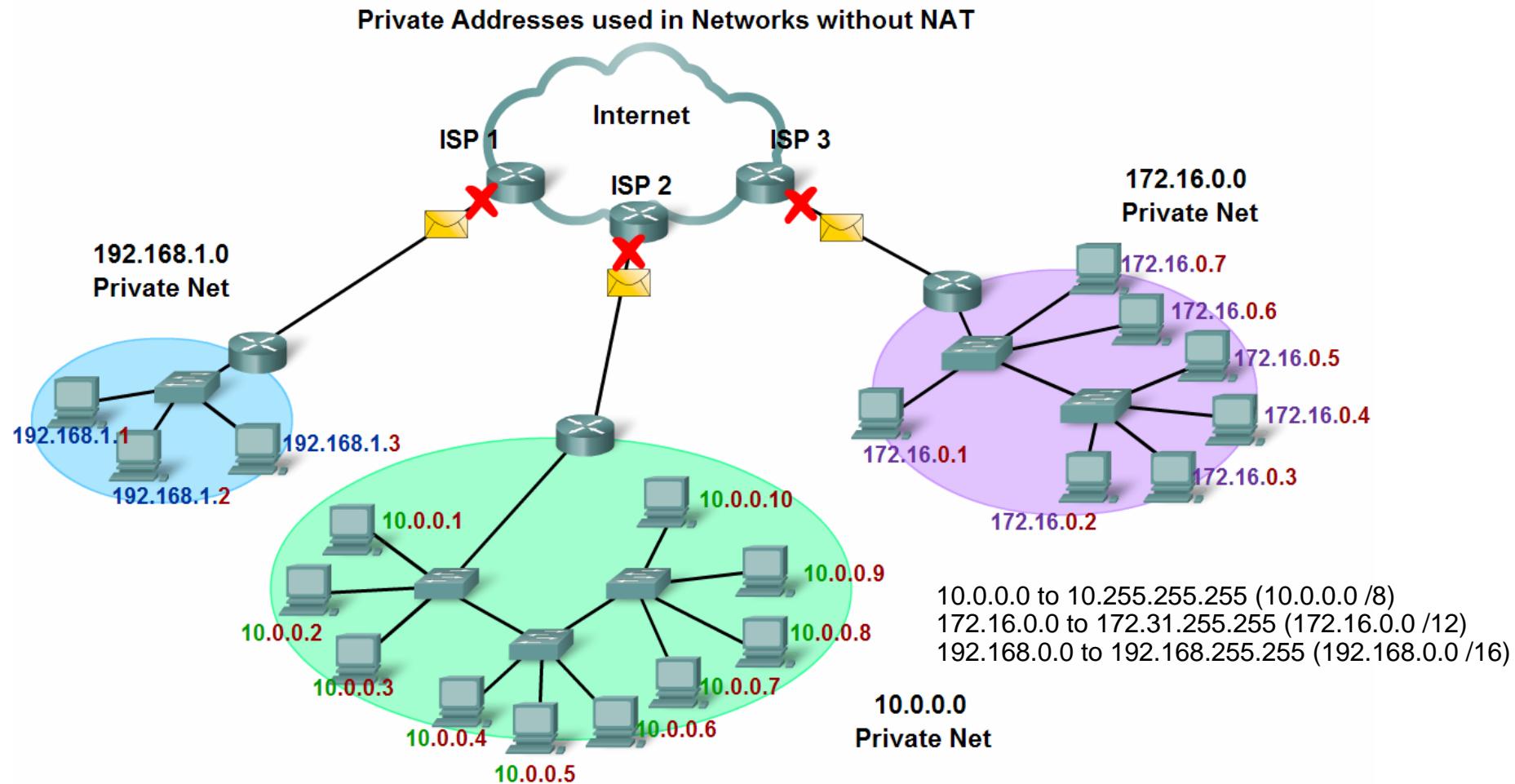
Classify and Define IPv4 Addresses

- Identify the address ranges reserved for these special purposes in the IPv4 protocol

Type of Address	Usage	Reserved IPv4 Address Range	RFC
Host Address	used for IPv4 hosts	0.0.0.0 to 223.255.255.255	790
Multicast Addresses	used for multicast groups on a local network	224.0.0.0 to 239.255.255.255	1700
Experimental Addresses	<ul style="list-style-type: none">used for research or experimentationcannot currently be used for hosts in IPv4 networks	240.0.0.0 to 255.255.255.254	1700 3330

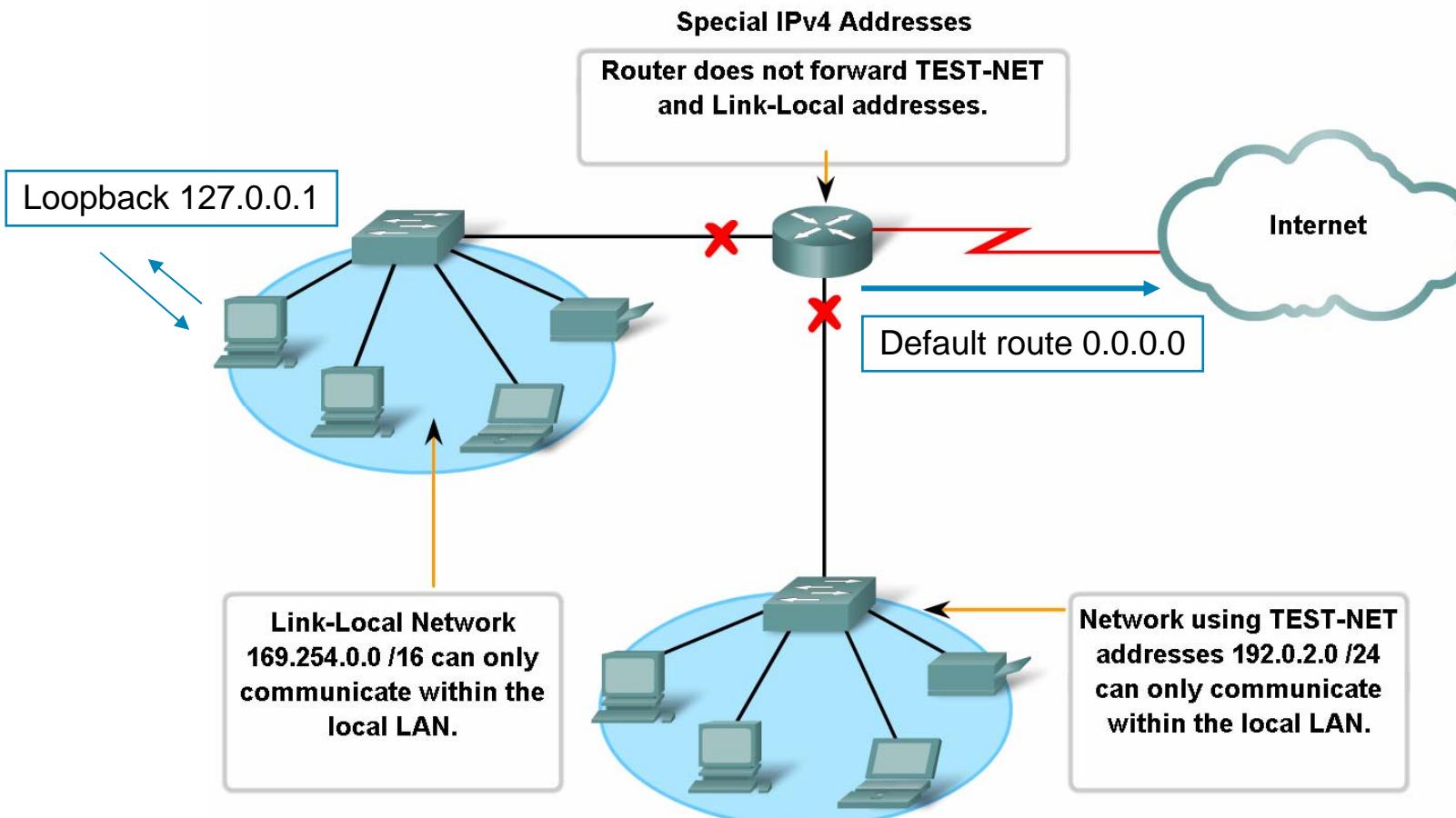
Classify and Define IPv4 Addresses

- Define public address and private address (RFC 1918)



Classify and Define IPv4 Addresses

- Describe the purpose of several special addresses (RFC 3927, RFC 3330)



Classify and Define IPv4 Addresses

- Identify the historic method for assigning addresses and the issues associated with the method

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)		

** All zeros (0) and all ones (1) are invalid hosts addresses.

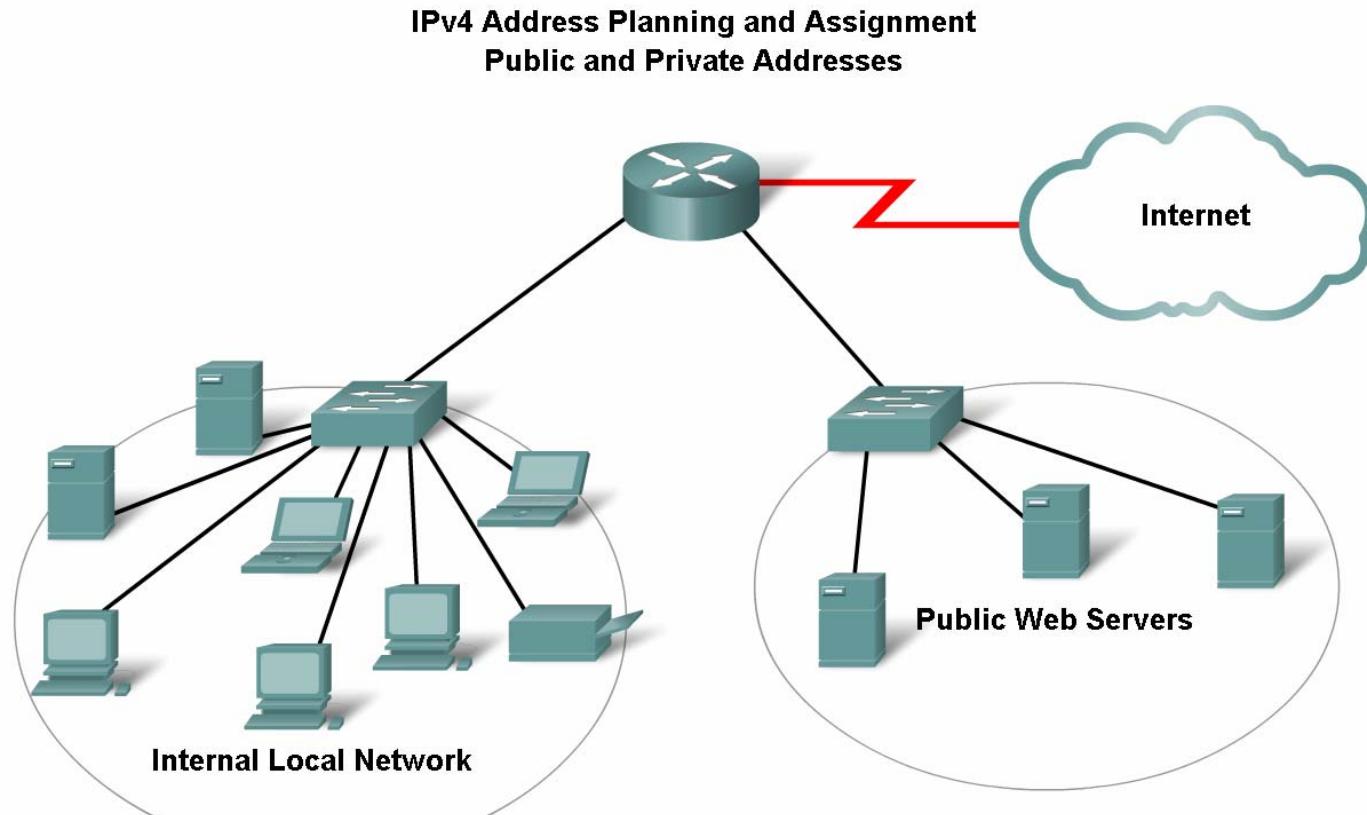
Classify and Define IPv4 Addresses

- Identify the historic method for assigning addresses and the issues associated with the method

Class A	0	Net ID	Host ID
Class B	1 0	Net ID	Host ID
Class C	1 1 0	Net ID	Host ID
Class D	1 1 1 0	Multicast group ID	
Class E	1 1 1 1	Experimental Usage	

Assigning Addresses

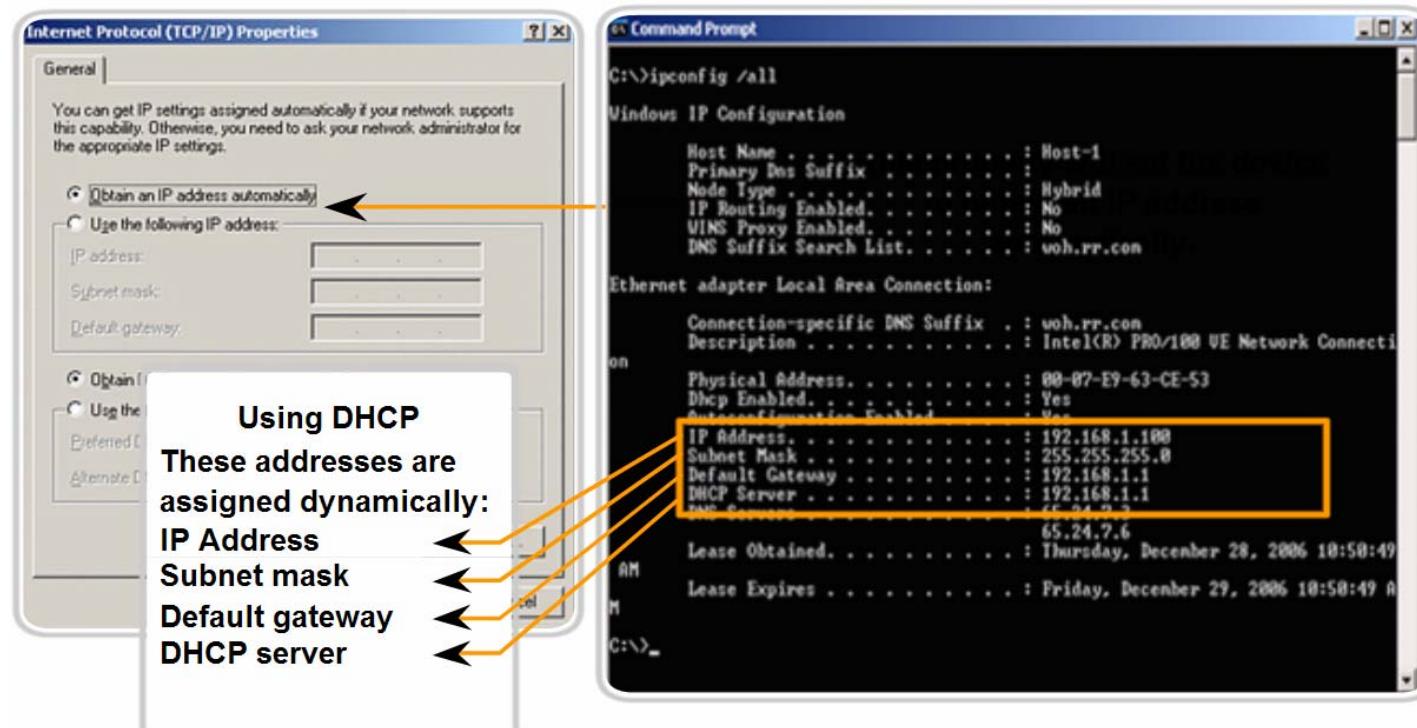
- Explain the importance of using a structured process to assign IP addresses to hosts and the implications for choosing private vs. public addresses



Assigning Addresses

- Explain how end user devices can obtain addresses either statically through an administrator or dynamically through DHCP

Assigning Dynamic Addresses

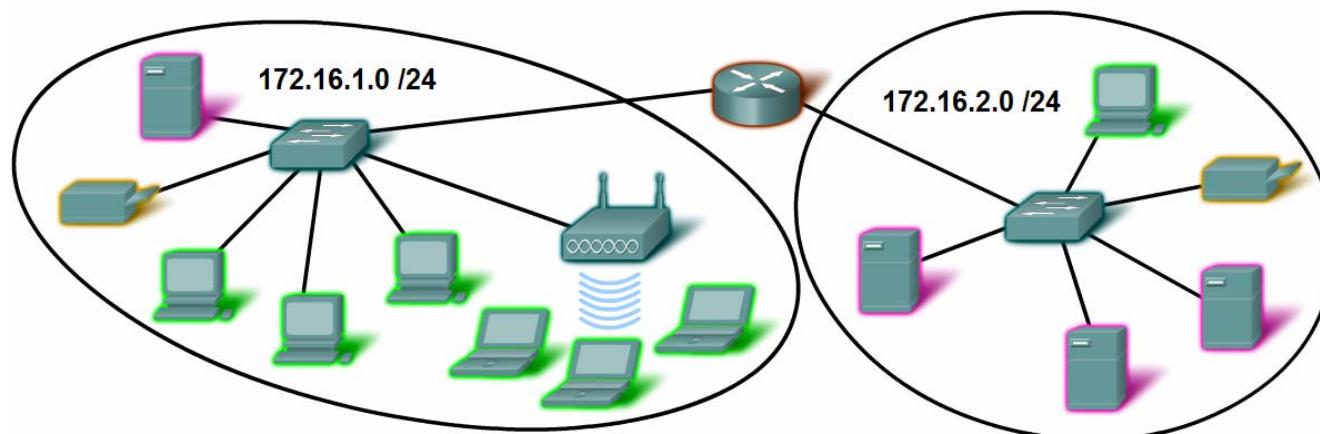


Assigning Addresses

- Explain which types of addresses should be assigned to devices other than end user devices

Devices IP Address Ranges

Use	First Address	Last Address	Summary Address
Network Address	172.16.x.0	
User hosts (DHCP pool)	172.16.x.1	172.16.x.127	172.16.x.0 /25
Servers	172.16.x.128	172.16.x.191	172.16.x.128 /26
Peripherals	172.16.x.192	172.16.x.223	172.16.x.192 /27
Networking devices	172.16.x.224	172.16.x.253	
Router (gateway)	172.16.x.254	172.16.x.224 /27
Broadcast	172.16.x.255	



Assigning Addresses

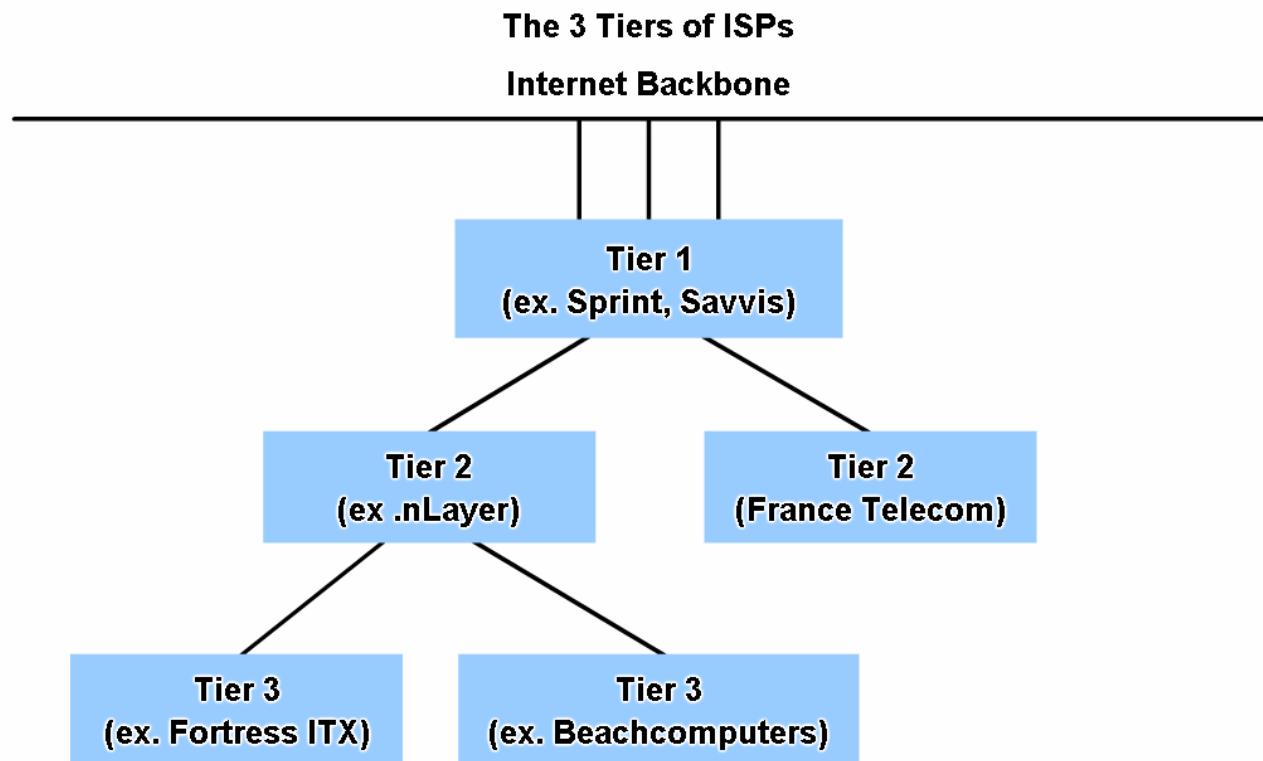
- Describe the process for requesting IPv4 public addresses, the role ISPs play in the process, and the role of the regional agencies that manage IP address registries

Entities that Oversee IP Address Allocation

Global	IANA				
Regional Internet Registries	AfriNIC	APNIC	LACNIC	ARIN	RIPE NCC
	Africa Region	Asia/Pacific Region	Latin America And Caribbean Region	North America Region	Europe, Middle East, Central Asia Region

Assigning Addresses

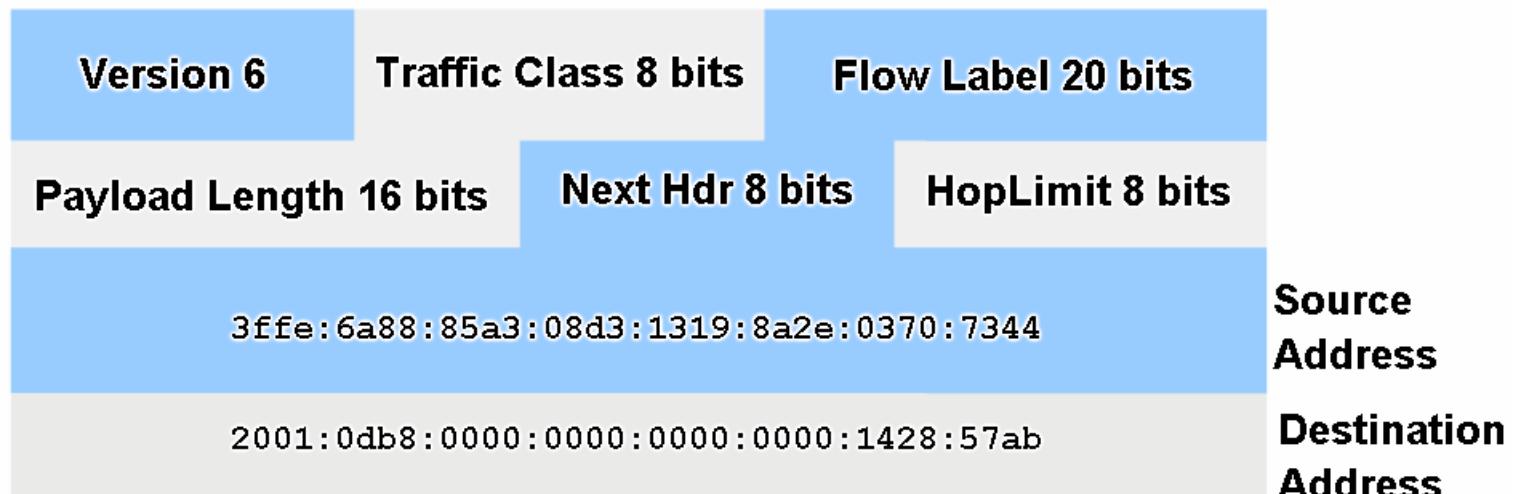
- Identify different types of ISPs and their roles in providing Internet connectivity



Assigning Addresses

- Identify several changes made to the IP protocol in IPv6 and describe the motivation for migrating from IPv4 to IPv6.

IPv6 Header



Determine the network portion of the host address and the role of the subnet mask

- Describe how the subnet mask is used to create and specify the network and host portions of an IP address

Network and Host Portions of an IP Address

IP address	172	.	16	.	4	.	1
	10101100		00010000		00010100		00100011
Subnet Mask	255	.	255	.	255	.	0
	11111111		1111111111		11111111		00000000

Prefix /24 (24 high order bits)

Determine the network portion of the host address and the role of the subnet mask

- Use the subnet mask and ANDing process to extract the network address from the IP address.

Applying the Subnet Mask

A device with address 192.0.0.1 belongs to network 192.0.0.0

		High order bits Prefix /16				Low order bits		
		192	.	0	.	0	.	1
Host		11000000		00000000		00000000		00000001
Subnet mask		255		255		0		0
AND		11111111		11111111		00000000		00000000
Network		11000000		00000000		00000000		00000000
Network		192	.	0	.	0	.	0

Determine the network portion of the host address and the role of the subnet mask

- Observe the steps in the ANDing of an IPv4 host address and subnet mask

Use the subnet mask to determine the network address for the host 173.16.132.70/20.

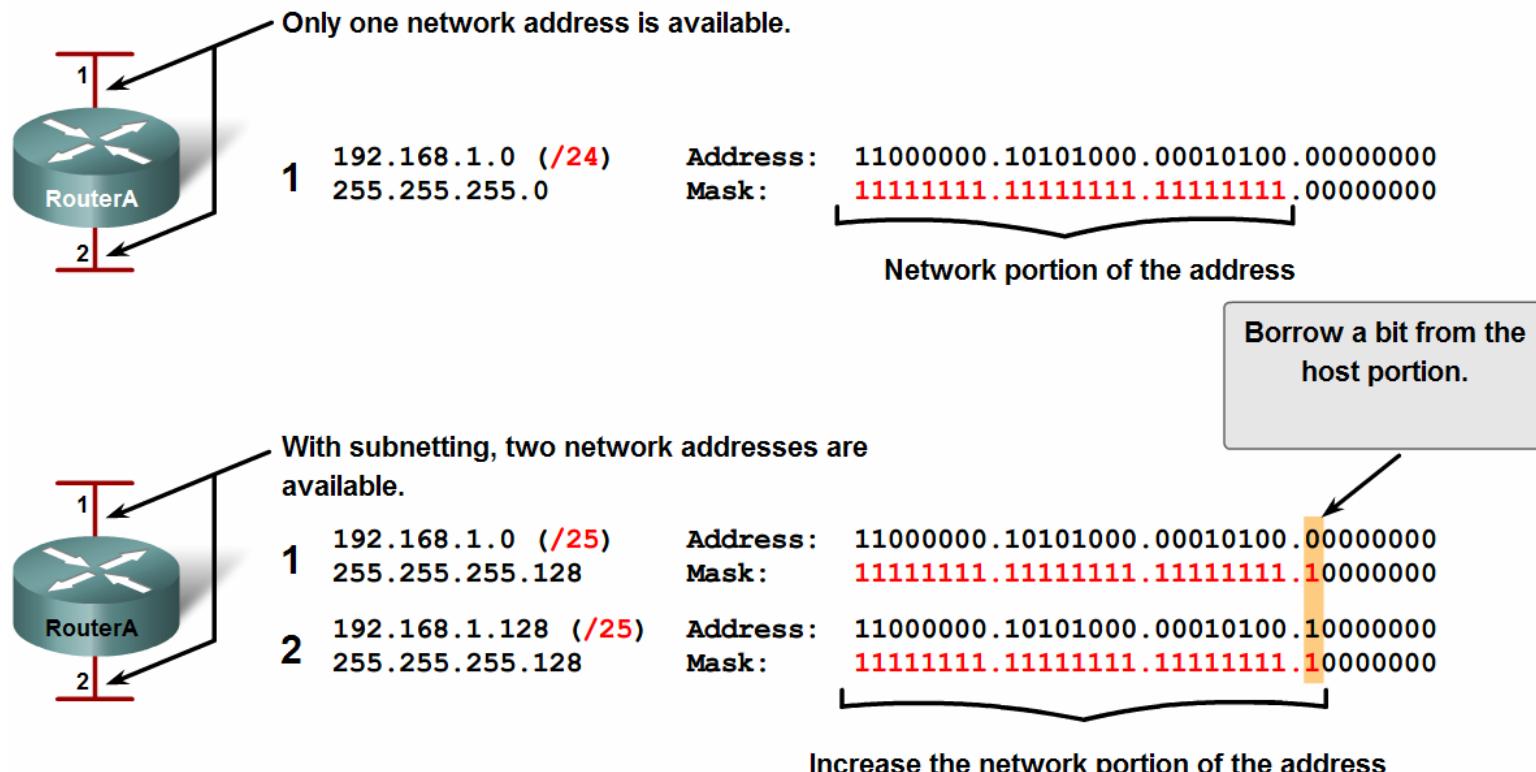
Convert binary network address to decimal

Host Address	172	.	16	.	132	.	70
Binary Host Address	10101100		00010000		10000100		01000110
Binary Subnet Mask	11111111		11111111		11110000		00000000
Binary Network Address	10101100		00010000		10000000		00000000
Network Address	172	.	16	.	128	.	0

Calculating Addresses

- Use the subnet mask to divide a network into smaller networks and describe the implications of dividing networks for network planners (see 6.5.1)

Borrowing Bits for Subnets



Calculating Addresses

- Class C subnet calculation example

11000010.11111100.10111110.01011100	194.252.190.92/29	IP Address / Mask
11111111.11111111.11111111. <u>11111000</u>	255.255.255.248	Subnet Mask

11000010.11111100.10111110.0101 <u>1000</u>	194.252.190.88	Subnet Address
11000010.11111100.10111110.0101 <u>1111</u>	194.252.190.95	Broadcast Address

Subnet Address can be calculated by means of logical AND operation performed on the given IP address and a given subnet mask. (all host bits are set to 0)

Subnet Broadcast Address can be obtained in the same way by performing an AND operation on the given IP address and a given subnet mask, but all host bits should be set to 1.

5 extra bits used for subnet => available subnets: 30 (2^5-2)

Each subnet has 6 (2^3-2) addresses for hosts
which gives 180 addresses (instead of 254)

Calculating Addresses (example 2)

- Class B subnet calculation example

10001100.10110011.11011100.11001000
11111111.11111111.11100000.00000000

140.179.220.200/19 IP Address / Mask
255.255.224.000 Subnet Mask

10001100.10110011.11000000.00000000
10001100.10110011.1101111.11111111

140.179.192.0 Subnet Address
140.179.223.255 Broadcast Address

Subnet Address can be calculated by means of logical AND operation performed on the given IP address and a given subnet mask. (all host bits are set to 0)

Subnet Broadcast Address can be obtained in the same way by performing an AND operation on the given IP address and a given subnet mask, but all host bits should be set to 1.

3 extra bits used for subnet => available subnets: 6 (2^3-2)
each subnet has 8190 ($2^{13}-2$) addresses for hosts
which gives 49,140 addresses (instead of 65,536)

Calculating Addresses

- Extract network addresses from host addresses using the subnet mask

$500 \rightarrow 512 = 2^9$
 $n = 9$ bits needed to address 510 devices

$$(2^{n-2})$$

$$32 - 9 = 23$$

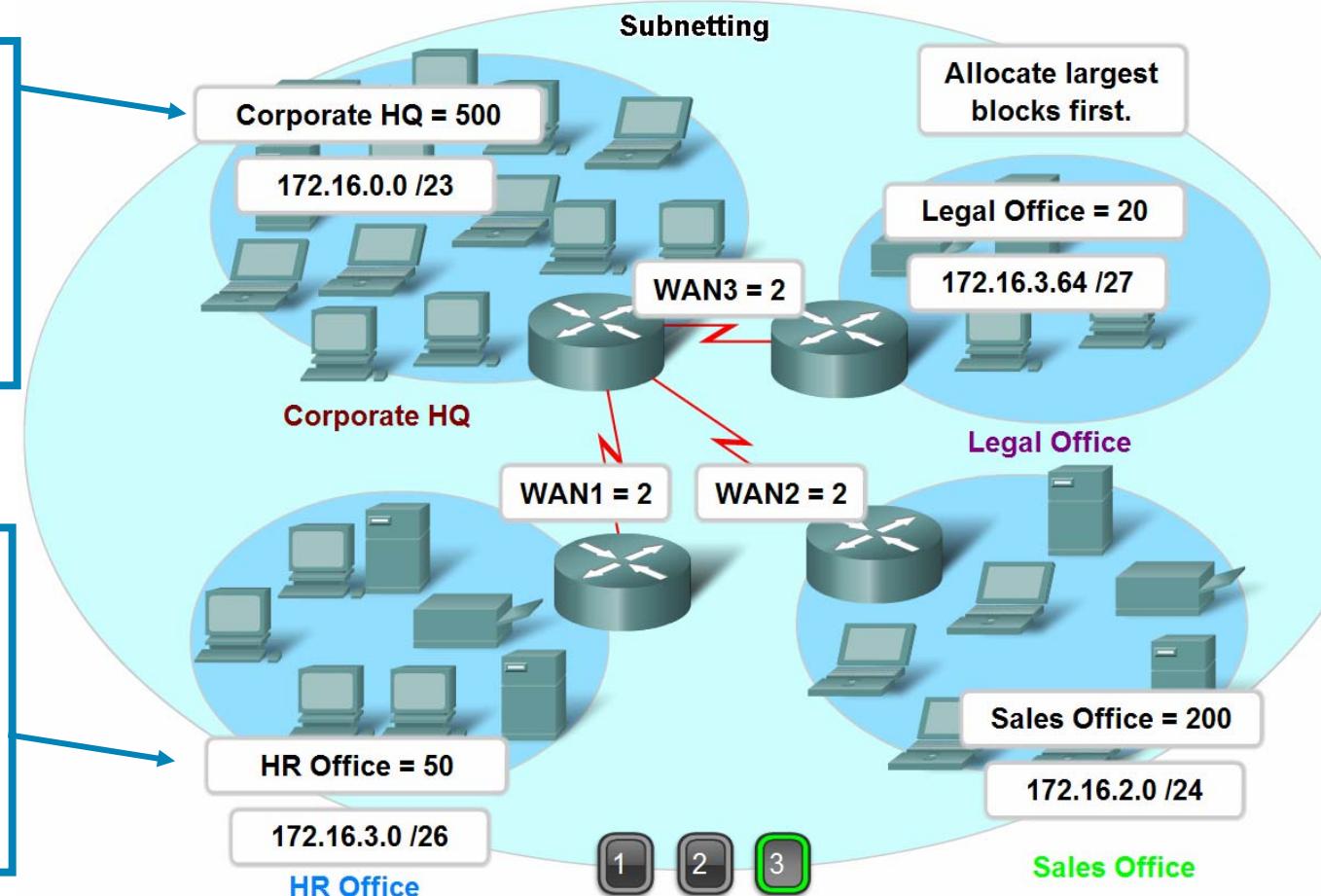
Subnet mask: /23

$50 \rightarrow 64 = 2^6$
 $n = 6$ bits needed to address 62 devices

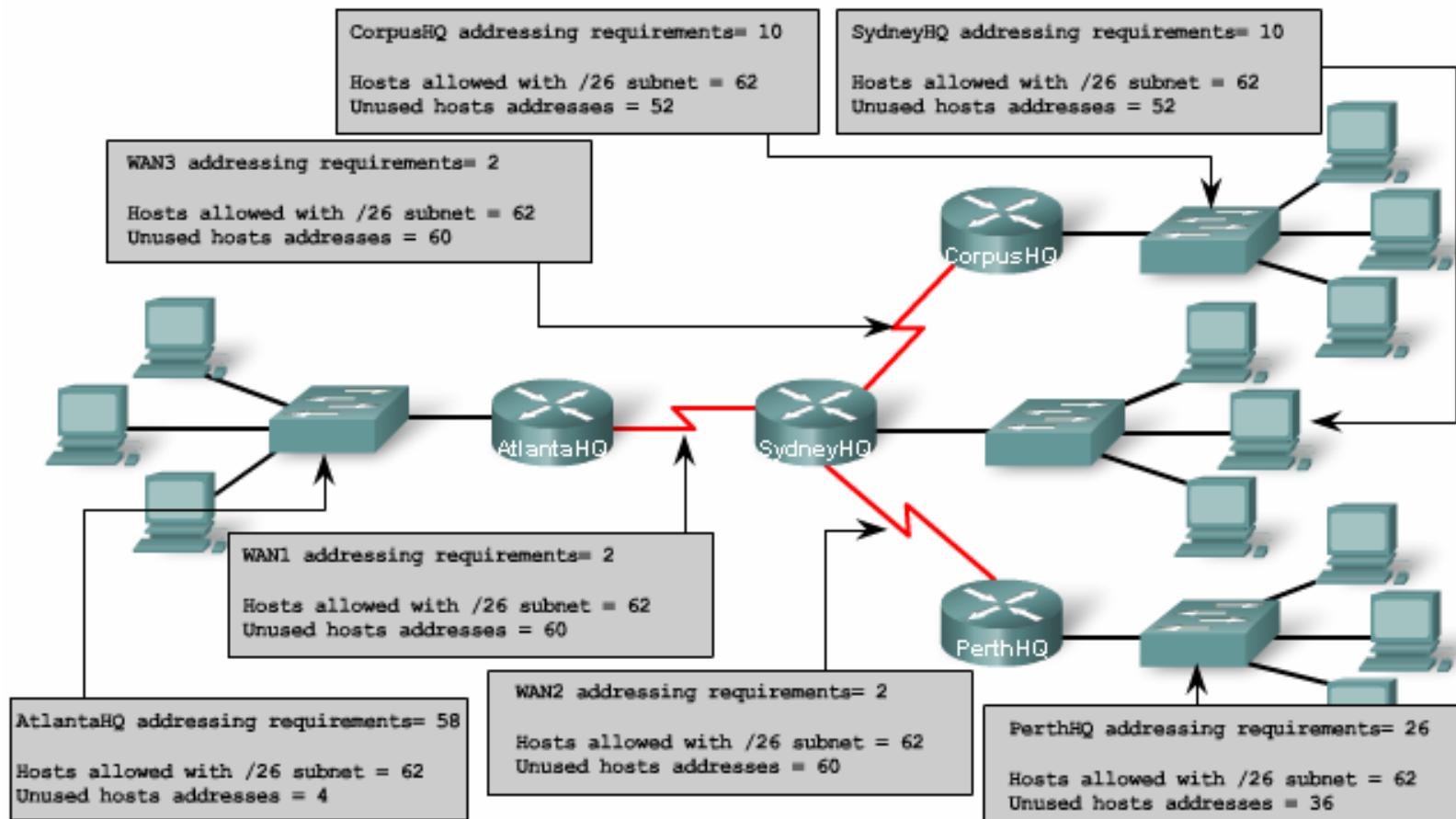
$$(2^{n-2})$$

$$32 - 6 = 26$$

Subnet mask: /26



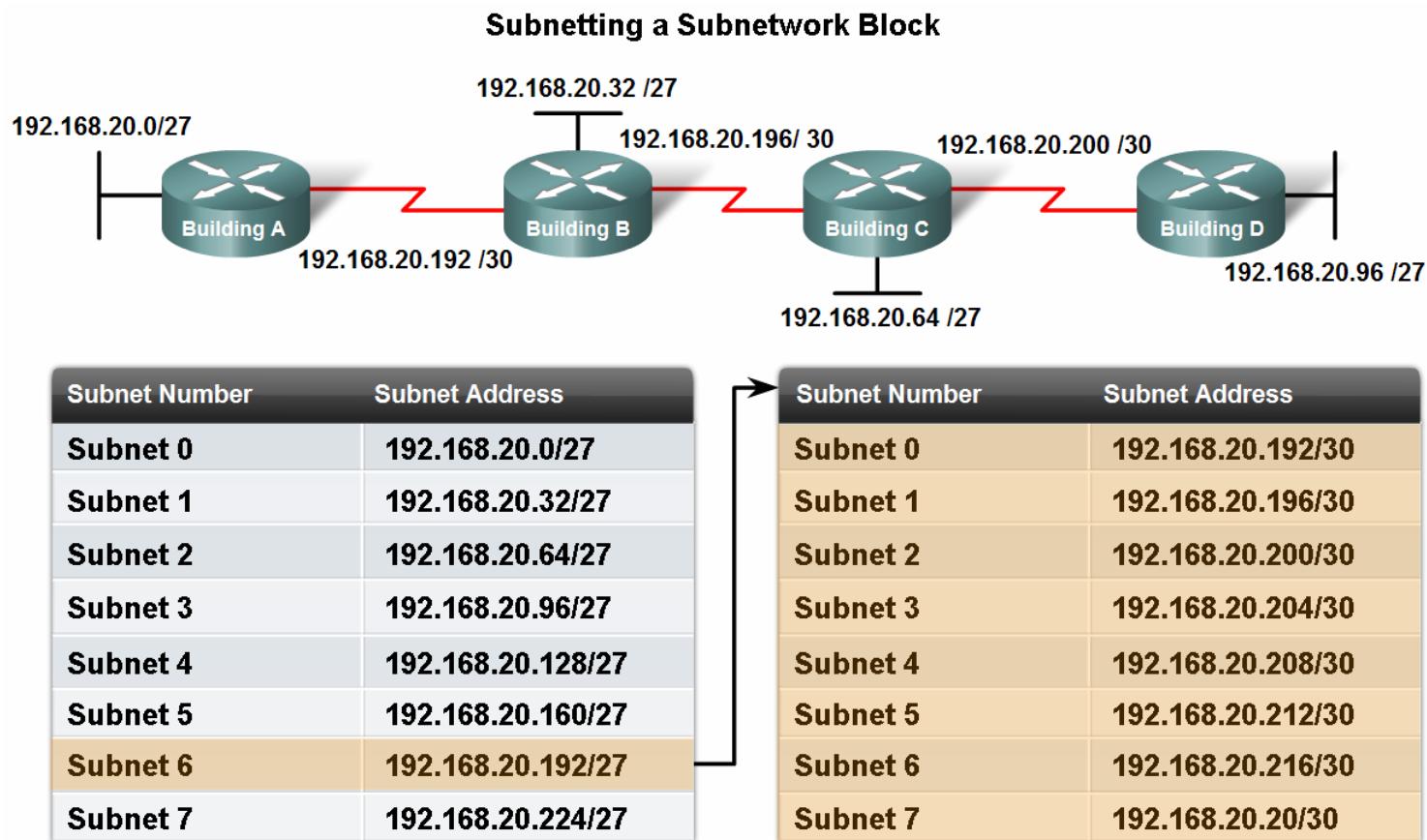
Network Requirements: Using standard subnetting would be inefficient.



	Actual Requirements	Total Wasted Addresses
AtlantaHQ	58 host addresses	4 addresses
PerthHQ	26 host addresses	36 addresses
SydneyHQ	10 host addresses	52 addresses
CorpusHQ	10 host addresses	52 addresses
WAN links	2 host addresses (each)	60 addresses

Calculating Addresses

- Calculate the number of hosts in a network range given an address and subnet mask



Calculating Addresses (Hands-On)

- Given a subnet address and subnet mask, calculate the network address, host addresses and broadcast address (6.5.4)

Activity

Given the host IP address and the subnet mask, enter the network address in binary and decimal.

Host Address	10	148	100	54
Subnet Mask	255	255	255	240
Host Address in binary	00001010	10010100	01100100	00110110
Subnet Mask in binary	11111111	11111111	11111111	11110000
Network Address in binary				
Network Address in decimal				

Calculating Addresses (Hands-On)

- Given a pool of addresses and masks, assign a host parameter with address, mask and gateway (6.5.5)

Given the network address and the subnet mask, enter the number of possible hosts. Click next to Number of Hosts to enter your response.

Network Address	10	0	0	0
Subnet Mask	255	255	255	192
Network address in binary	00001010	00000000	00000000	00000000
Subnet Mask in binary	11111111	11111111	11111111	11000000
Number of hosts				

Calculating Addresses (Hands-On)

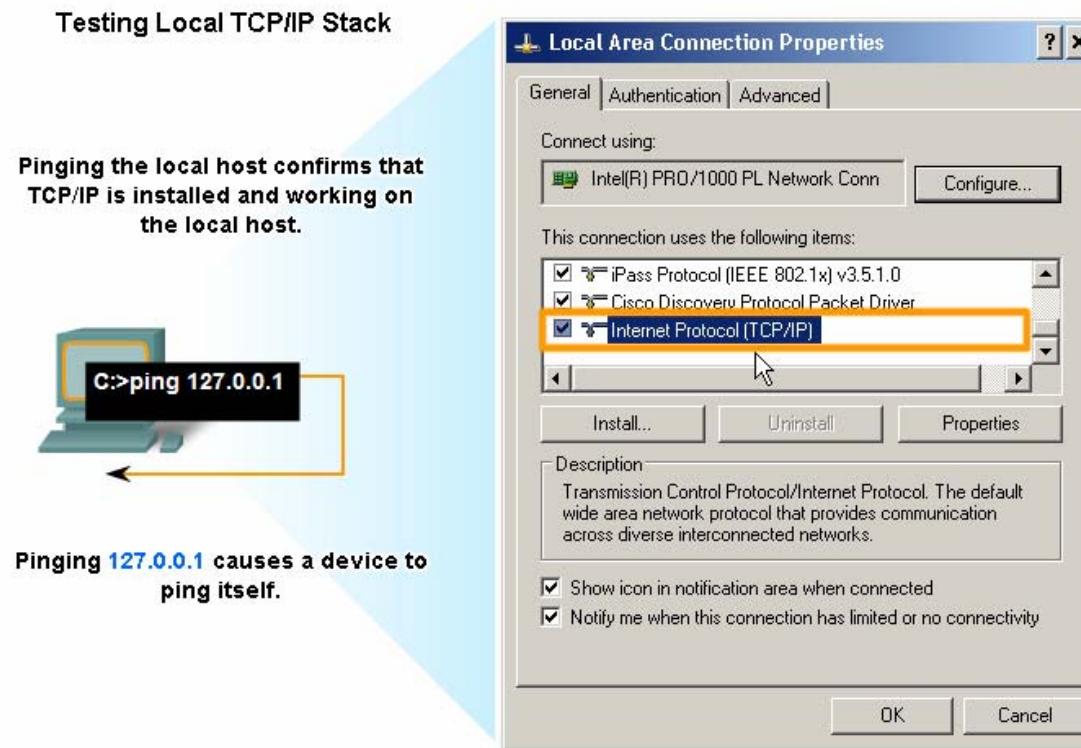
- Given a diagram of a multi-layered network, address range, number of hosts in each network and the ranges for each network, create a network scheme that assigns addressing ranges to each network (6.5.6)

Given the network address and the subnet mask, define the range of hosts, the broadcast address, and the next network address.

Network Address in decimal	10	187	0	0
Subnet Mask in decimal	255	255	224	0
Network address in binary	00001010	10111011	00000000	00000000
Subnet Mask in binary	11111111	11111111	11100000	00000000
First Usable Host IP Address in decimal	1st octet	2nd octet	3rd octet	4th octet
Last Usable Host IP Address in decimal	1st octet	2nd octet	3rd octet	4th octet
Broadcast Address in decimal	1st octet	2nd octet	3rd octet	4th octet
Next Network Address in decimal	1st octet	2nd octet	3rd octet	4th octet

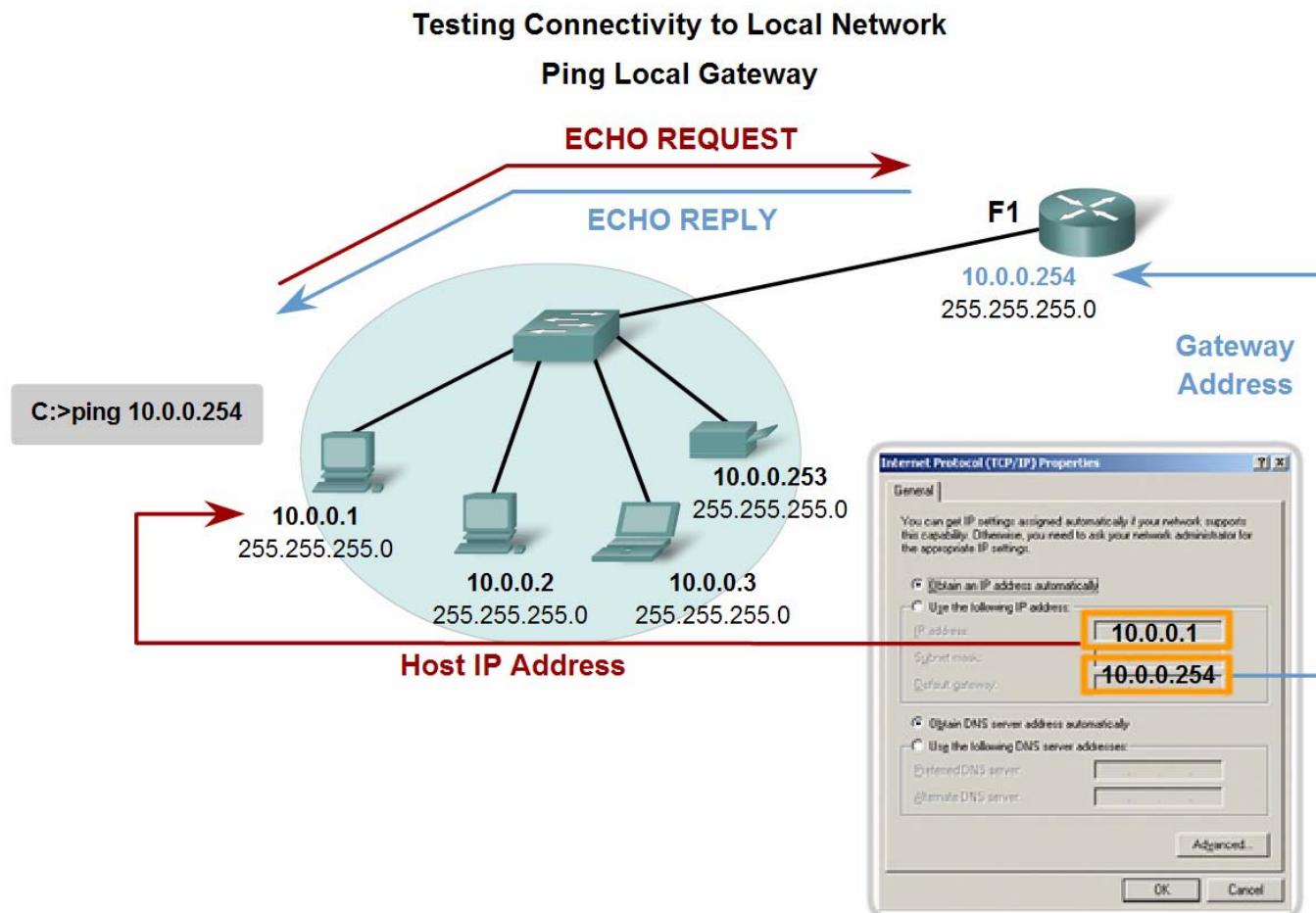
Testing the Network Layer

- Describe the general purpose of the ping command, trace the steps of its operation in a network, and use the ping command to determine if the IP protocol is operational on a local host



Testing the Network Layer

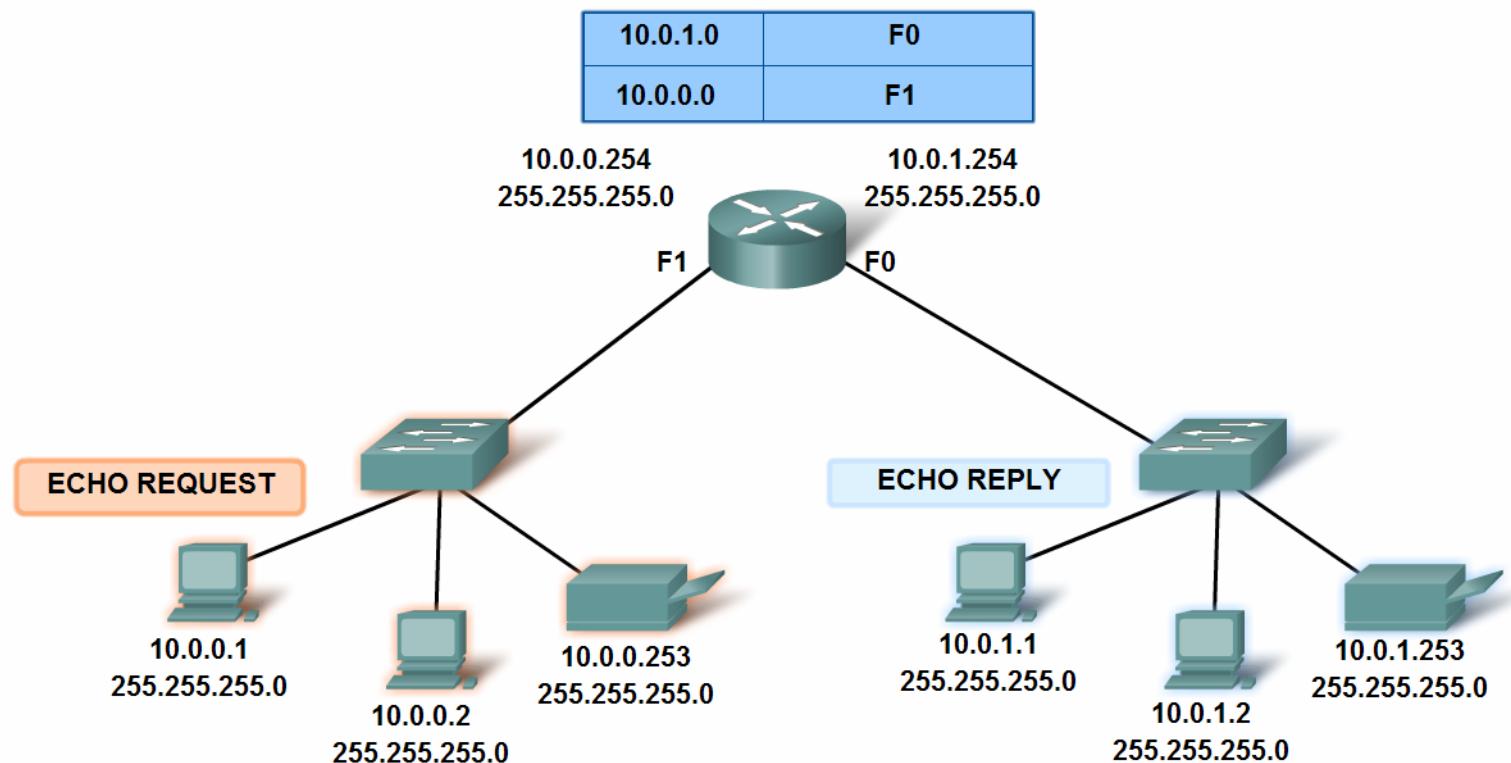
- Use ping to verify that a local host can communicate with a gateway across a local area network



Testing the Network Layer

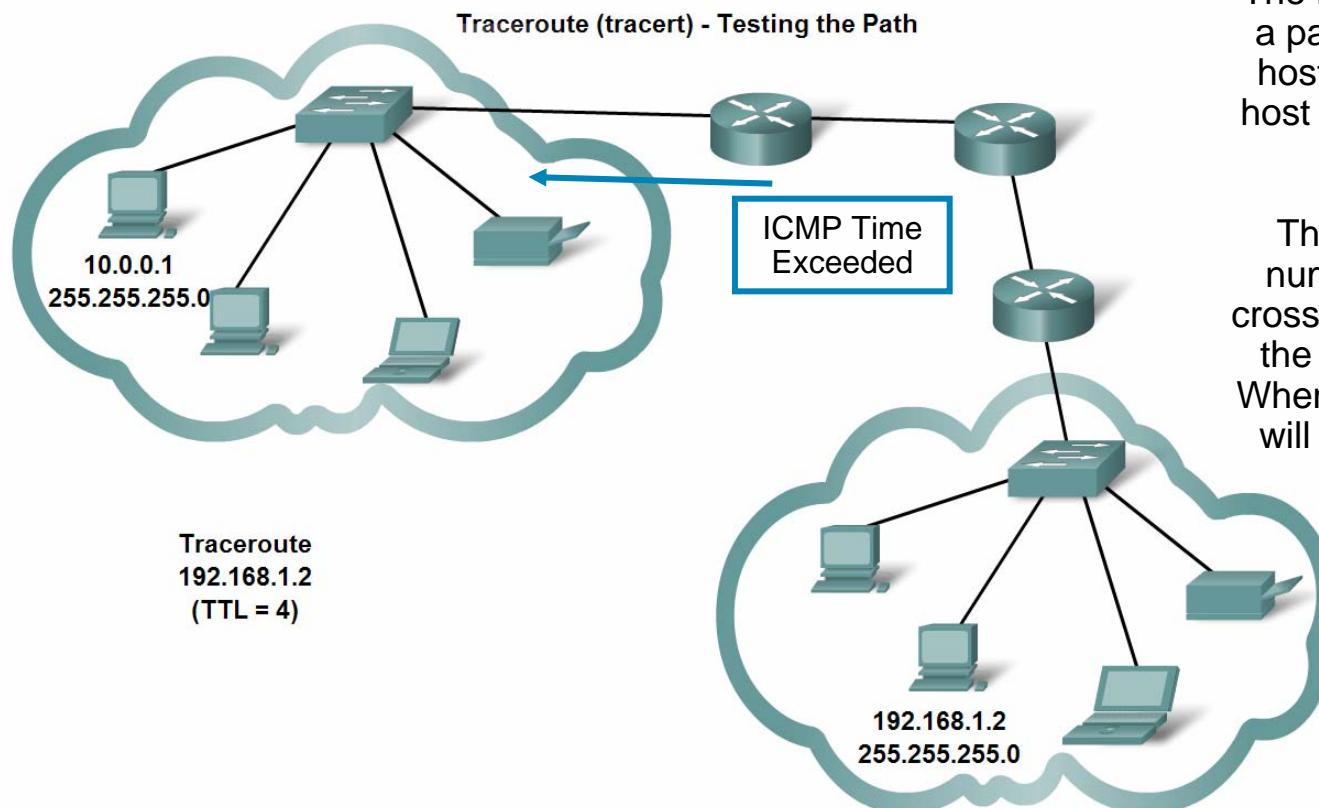
- Use ping to verify that a local host can communicate via a gateway to a device in remote network

Testing Connectivity to Remote LAN
Ping to a remote host



Testing the Network Layer

- Use tracert/traceroute to observe the path between two devices as they communicate and trace the steps of tracert/traceroute's operation (6.6.4)

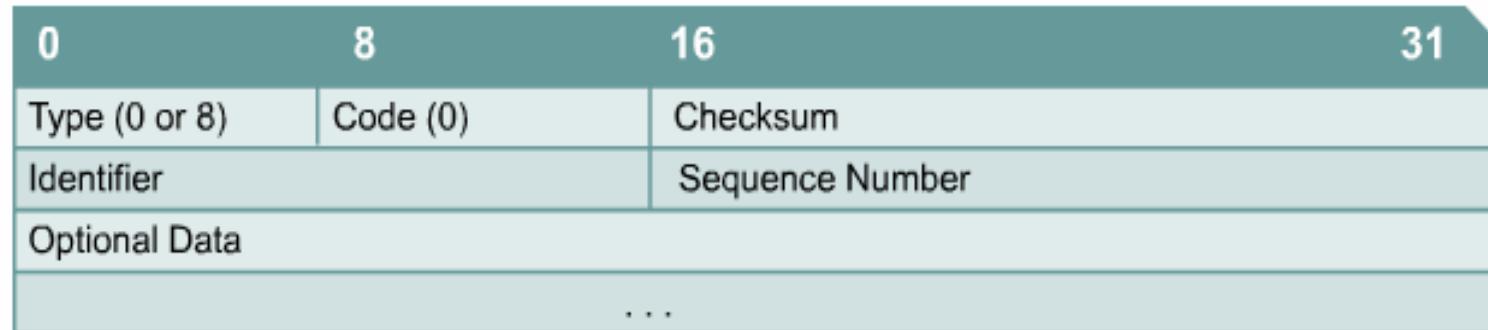


The round trip time (**RTT**) is the time a packet takes to reach the remote host and for the response from the host to return. An asterisk (*) is used to indicate a lost packet.

The **TTL** field is used to limit the number of hops that a packet can cross. When a packet enters a router, the TTL field is decremented by 1. When the TTL reaches zero, a router will not forward the packet and the packet is dropped.

Testing the Network Layer ICMPv4

- Although IPv4 is not a reliable protocol, it does provide for messages to be sent in the event of certain errors
- ICMP provides control and error messages and is used by the ping and traceroute utilities
- Message format



Testing the Network Layer ICMPv4

- Message types

ICMP Message Types	
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect/ Change Request
8	Echo Request
9	Router Advertisement
10	Router Selection
11	Time Exceeded
12	Parameter Problem
13	Timestamp Request
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply

Testing the Network Layer ICMPv4

- ICMP destination unreachable codes

0 = net unreachable
1 = host unreachable
2 = protocol unreachable
3 = port unreachable
4 = fragmentation needed and DF set
5 = source route failed
6 = destination network unknown
7 = destination host unknown
8 = source host isolated
9 = communication with destination network administratively prohibited
10 = communication with destination host administratively prohibited
11 = network unreachable for type device
12 = host unreachable for type of service



Summary

In this chapter, you learned to:

- Explain the structure IP addressing and demonstrate the ability to convert between 8-bit binary and decimal numbers.
- Given an IPv4 address, classify by type and describe how it is used in the network.
- Explain how addresses are assigned to networks by ISPs and within networks by administrators.
- Determine the network portion of the host address and explain the role of the subnet mask in dividing networks.
- Given IPv4 addressing information and design criteria, calculate the appropriate addressing components.
- Use common testing utilities to verify and test network connectivity and operational status of the IP protocol stack on a host.





OSI Data Link Layer



Network Fundamentals – Chapter 7

Cisco | Networking Academy®
Mind Wide Open™

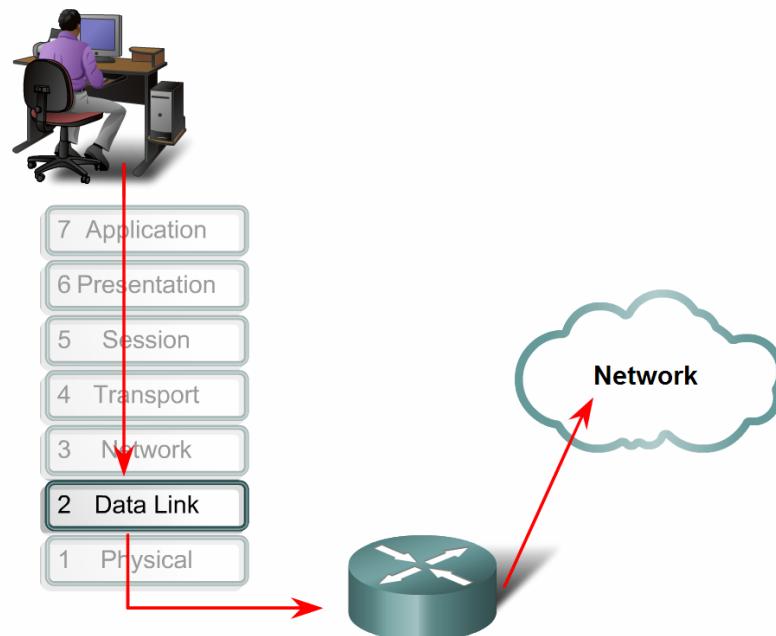


Objectives

- Explain the role of Data Link layer protocols in data transmission.
- Describe how the Data Link layer prepares data for transmission on network media.
- Describe the different types of media access control methods.
- Identify several common logical network topologies and describe how the logical topology determines the media access control method for that network.
- Explain the purpose of encapsulating packets into frames to facilitate media access.
- Describe the Layer 2 frame structure and identify generic fields.
- Explain the role of key frame header and trailer fields including addressing, QoS, type of protocol and Frame Check Sequence.

Data Link Layer – Accessing the Media

- The **Data Link** layer performs two basic services:
 - Allows the upper layers to **access the media** using techniques such as **framing**
 - Controls how data is placed onto the media and is received from the media using techniques such as **media access control** and **error detection**



The Data Link layer prepares network data for the physical network.

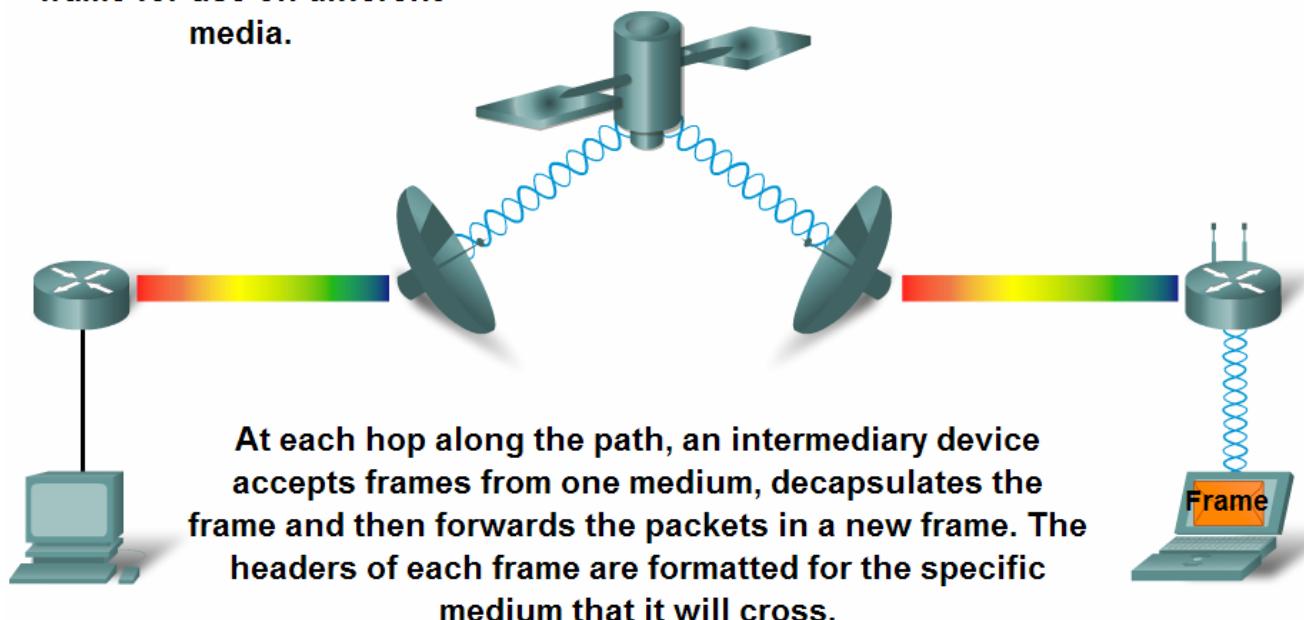
Data Link Layer – Accessing the Media

- Data Link layer protocols are required to **control media access**
- Fig. 7.1.1.2

The Data Link Layer

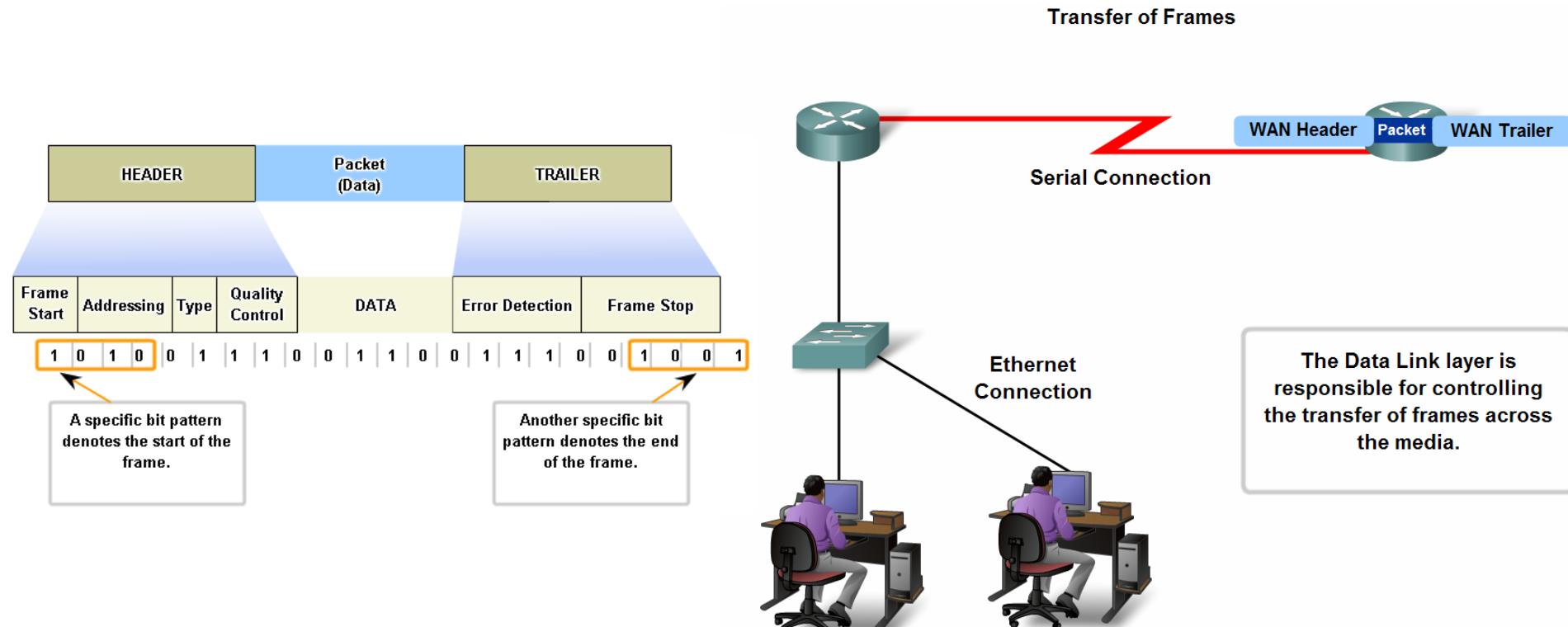
Data link layer protocols govern how to format a frame for use on different media.

Different protocols may be in use for different media.



Data Link Layer – Accessing the Media

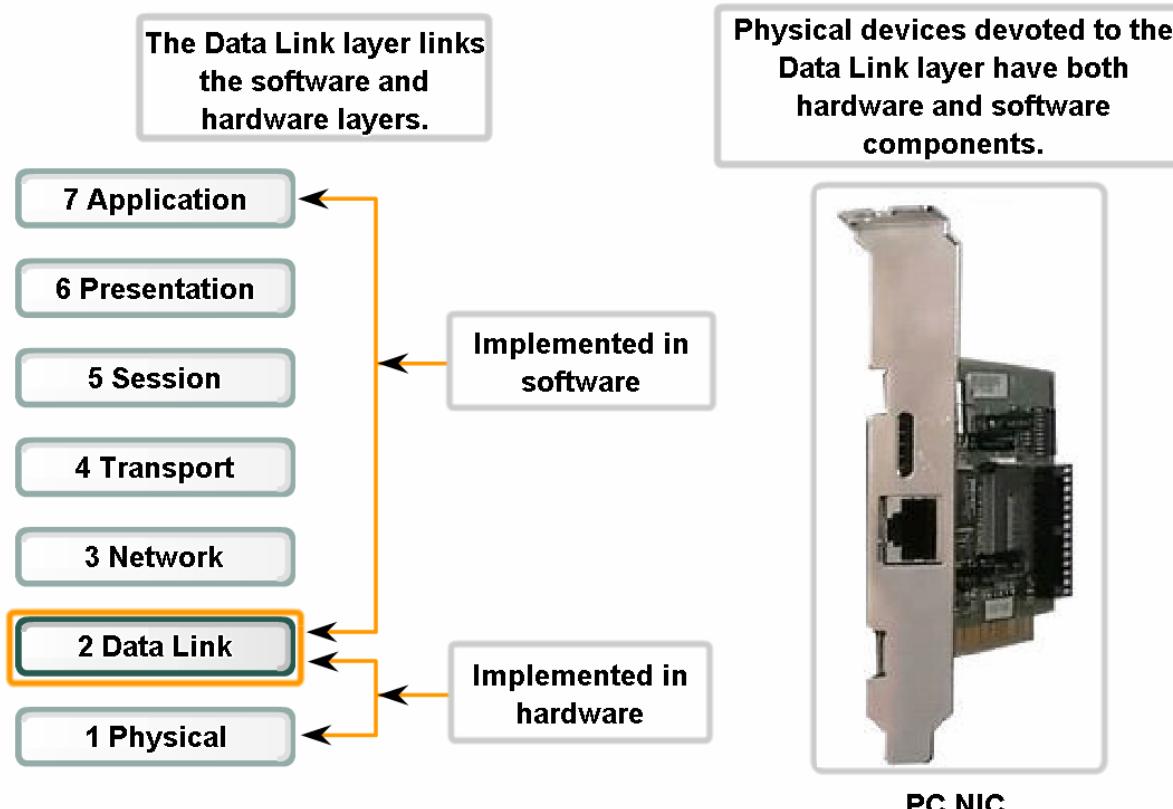
- The role of **framing** in preparing a packet for transmission on a given media
- The technique used for getting the frame on and off media is called the **media access control** method.



Data Link Layer – Accessing the Media

- The role the Data Link layer plays in linking the software and hardware layers

Connecting Upper Layer Services to the Media

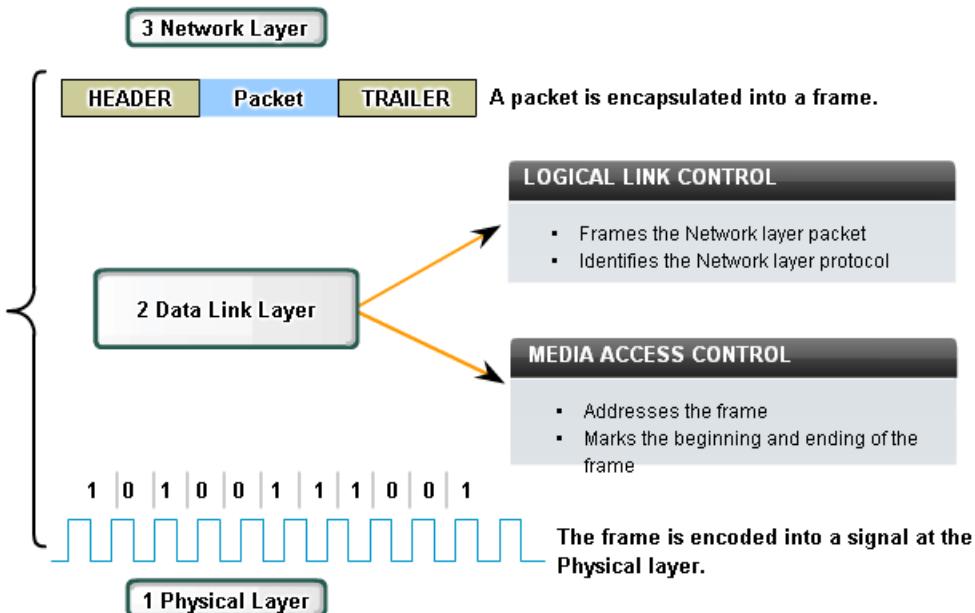


Data Link Layer – Accessing the Media

- **Logical Link Control (LLC)** 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 IP and IPX, to utilize the same network interface and media.
- **Media Access Control (MAC)** provides Data Link layer addressing and delimiting of data according to the physical signaling requirements of the medium and the type of Data Link layer protocol in use.

Data Link Sublayers

Separating the Data Link layer into sublayers allows for one type of frame defined by the upper layer **to access different types of media** defined by the lower layer. Such is the case in many LAN technologies, including **Ethernet**.



Data Link Layer – Accessing the Media

- Identify several sources for the protocols and standards used by the Data Link layer

Standards for the Data Link Layer

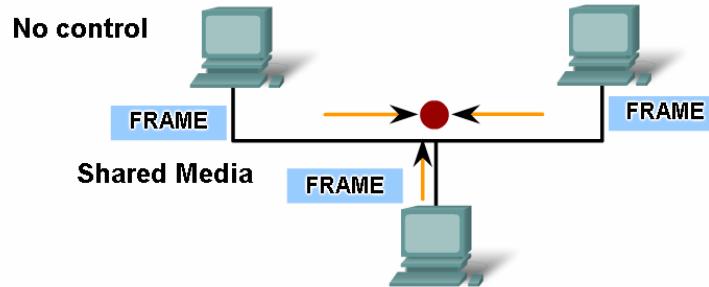
ISO:	HDLC (High Level Data Link Control)
IEEE:	802.2 (LLC), 802.3 (Ethernet) 802.5 (Token Ring) 802.11(Wireless LAN)
ITU:	Q.922 (Frame Relay Standard) Q.921 (ISDN Data Link Standard) HDLC (High Level Data Link Control)
ANSI:	3T9.5 ADCCP (Advanced Data Communications Control Protocol)

Media Access Control Techniques

- Regulating the placement of data frames onto the media is known as **media access control**.
- Media access control techniques define if and how the **nodes share the media**.

Media Access Control Methods

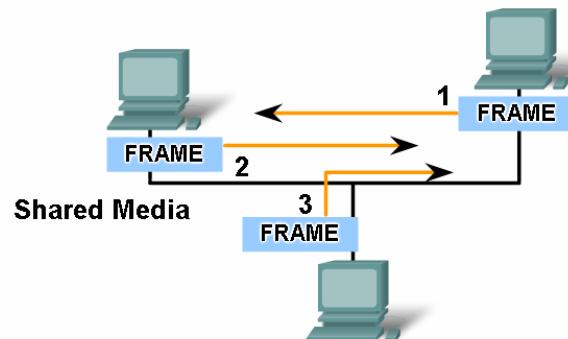
No control at all would result in many collisions.
Collisions cause corrupted frames that must be resent.



Methods that enforce a high degree of control prevent collisions, but the process has high overhead.

Methods that enforce a low degree of control have low overhead, but there are more frequent collisions.

Take turns

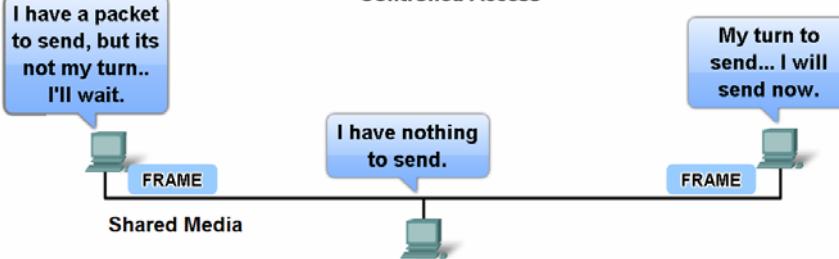


Media Access Control Techniques

- There are two basic media access control methods for shared media:
 - Controlled** - Each node has its **own time** to use the medium
 - Contention-based** - All nodes **compete** for the use of the medium

Media Access Control for Shared Media

Controlled Access



Media Access Control for Shared Media

Contention-Based Access



Method	Characteristics	Example
Controlled Access	<ul style="list-style-type: none"> Only one station transmits at a time Devices wishing to transmit must wait their turn No collisions Some deterministic networks use token passing 	<ul style="list-style-type: none"> Token Ring FDDI

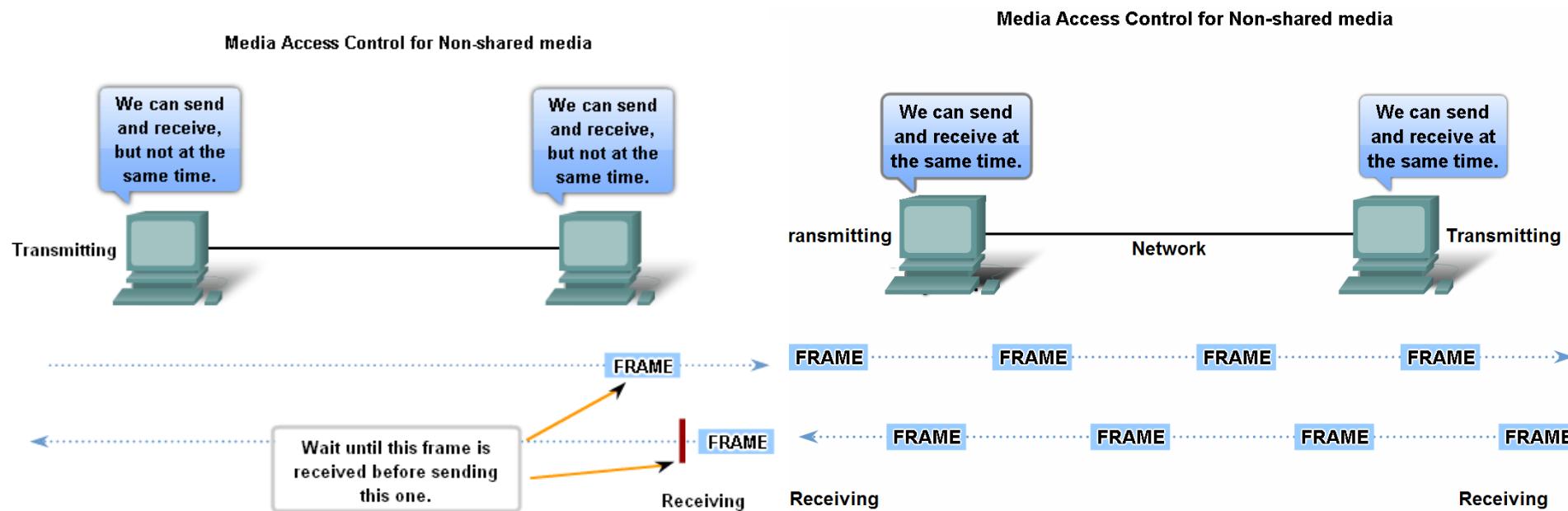
Method	Characteristics	Example
Contention Based Access	<ul style="list-style-type: none"> Stations can transmit at any time Collisions exist Mechanisms exist to resolve contention: <ul style="list-style-type: none"> CSMA/CD for Ethernet networks CSMA/CA for 802.11 wireless networks 	<ul style="list-style-type: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

Media Access Control Techniques

- **CSMA** is usually implemented in conjunction with a method for resolving the media contention. The two commonly used methods are:
 - In **CSMA/Collision Detection (CSMA/CD)**, 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 and try again later (Ethernet).
 - In **CSMA/Collision Avoidance (CSMA/CA)**, the device examines the media for the presence of a 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. This method is used by 802.11 wireless networking technologies.

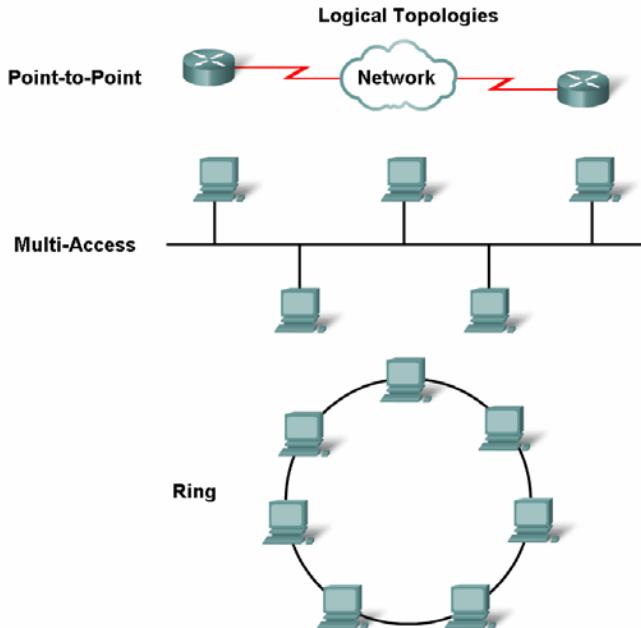
Media Access Control Techniques

- Define **Full Duplex** and **Half Duplex** as it relates to Media Access Control for non-shared media



Media Access Control Techniques

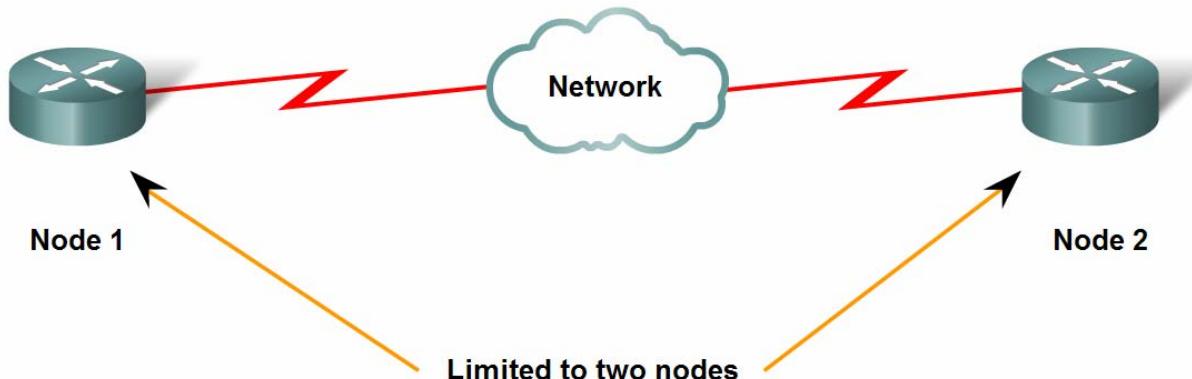
- The **physical topology** is an arrangement of the nodes and the physical connections between them.
- A **logical topology** is the way a network transfers frames from one node to the next.
- The **physical or cabled topology** of a network will most likely **not be the same** as the logical topology.



Media Access Control Techniques

- In data networks with **point-to-point** topologies, the media access control protocol can be very simple.
- In some cases, the logical connection between nodes forms a **virtual circuit**. It is a logical connection created within a network between two network devices.

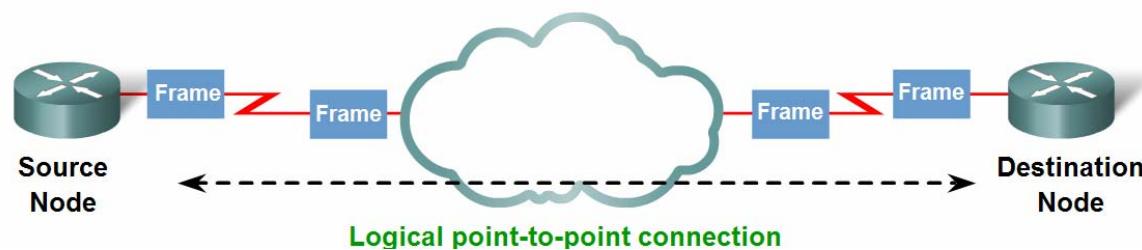
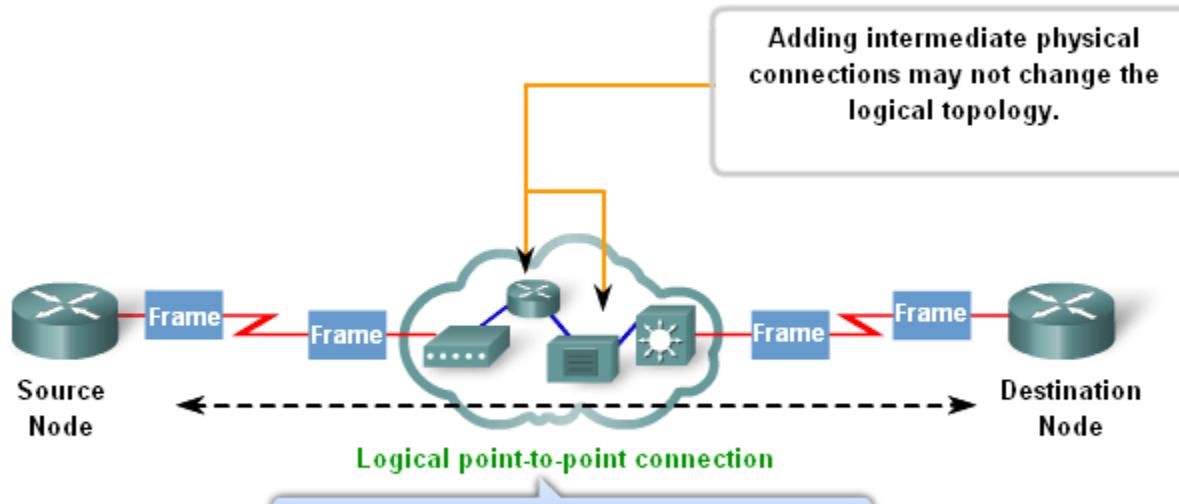
Point-to-Point Topology



Media Access Control Techniques

- Contrast logical and physical topologies

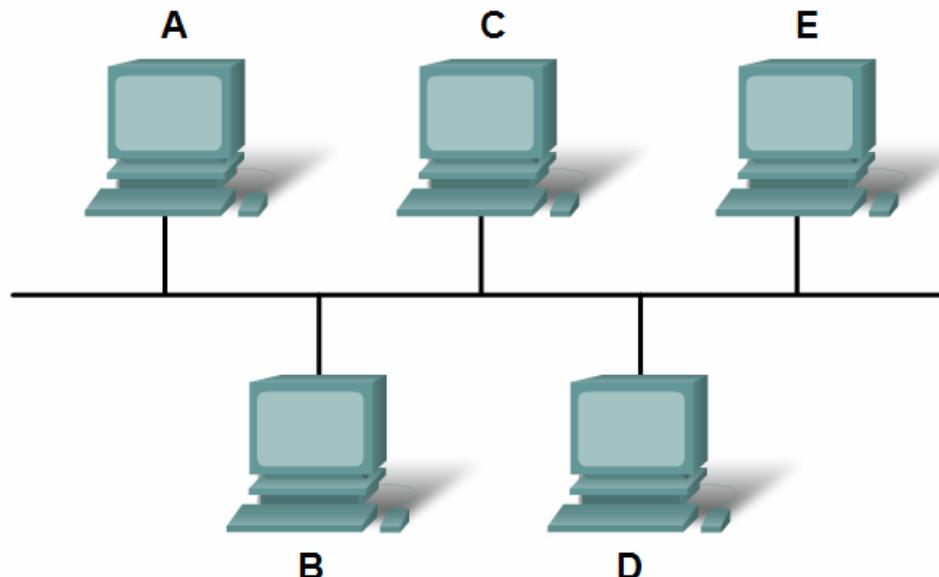
Logical Point-to-Point Topology



Media Access Control Techniques

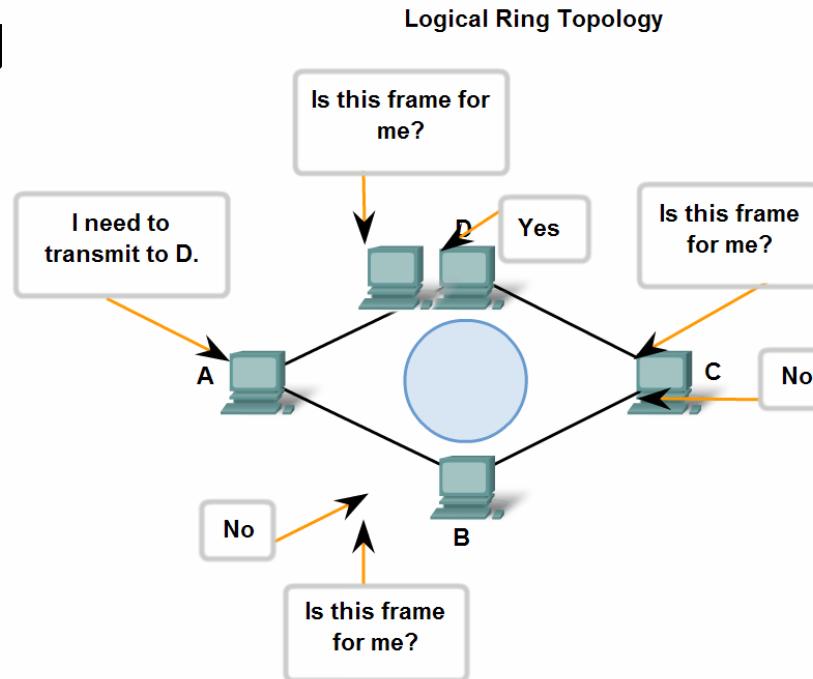
- A logical multi-access topology enables a number of nodes to communicate by using the **same shared media**.
- Fig. 7.2.6.1

Logical Multi-Access Topology



Media Access Control Techniques

- In a **logical ring topology**, each node in turn receives a frame.
- If the frame is not addressed to the node, the node passes the frame to the next node.
- It is a controlled media access control technique called **token passing**



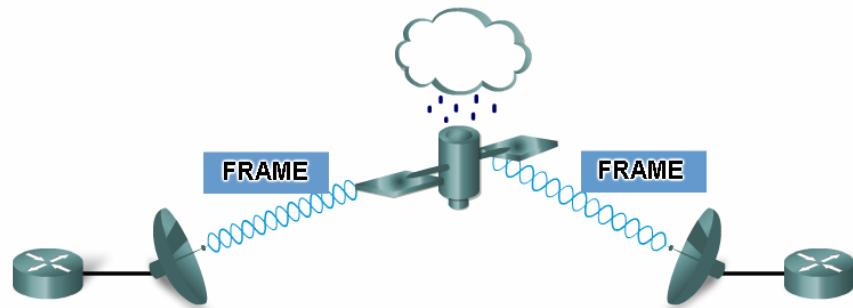
Media Access Control Addressing and Framing Data

- There is **no one frame structure** that meets the needs of all data transportation across all types of media.

Data Link Layer Protocols - The Frame

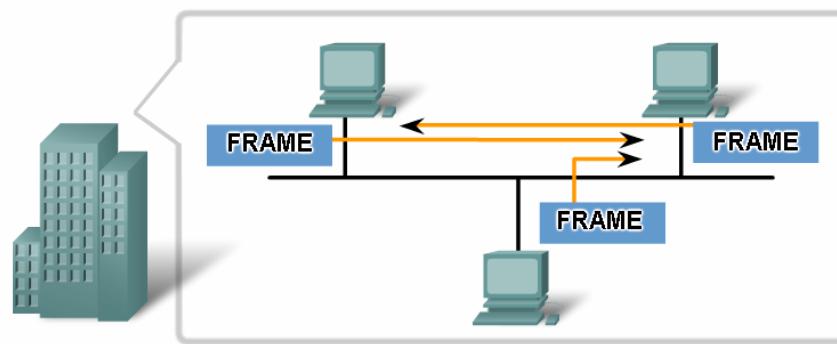
In a **fragile environment**, more controls are needed to ensure delivery. The header and trailer fields are larger as more control information is needed.

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.

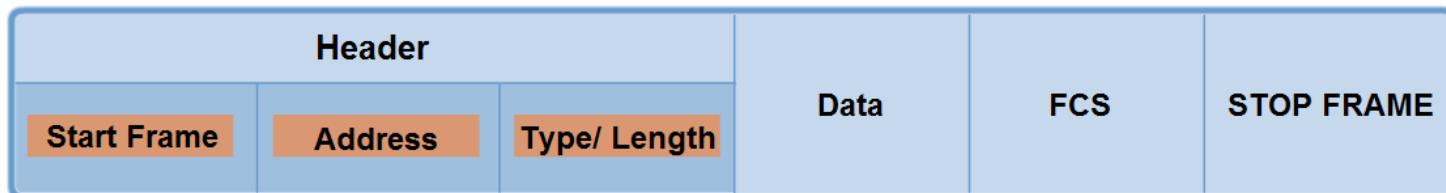
Less effort needed to ensure delivery = lower overhead = faster transmission rates





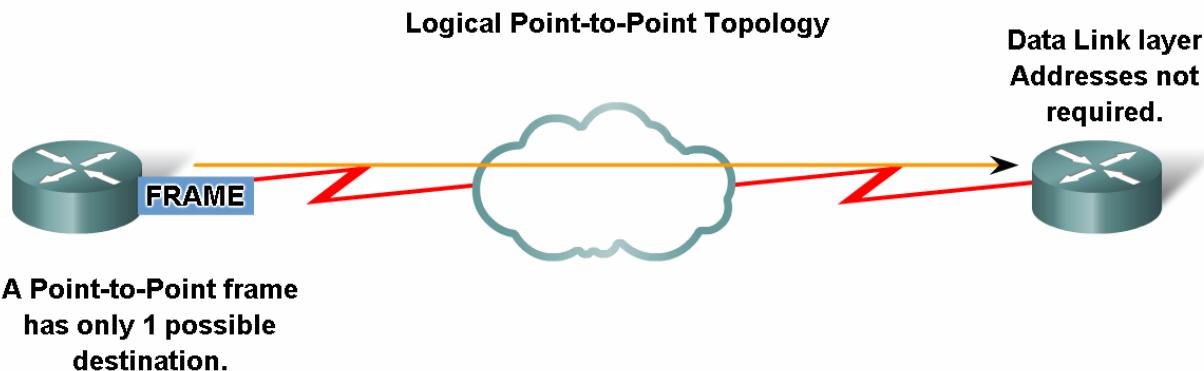
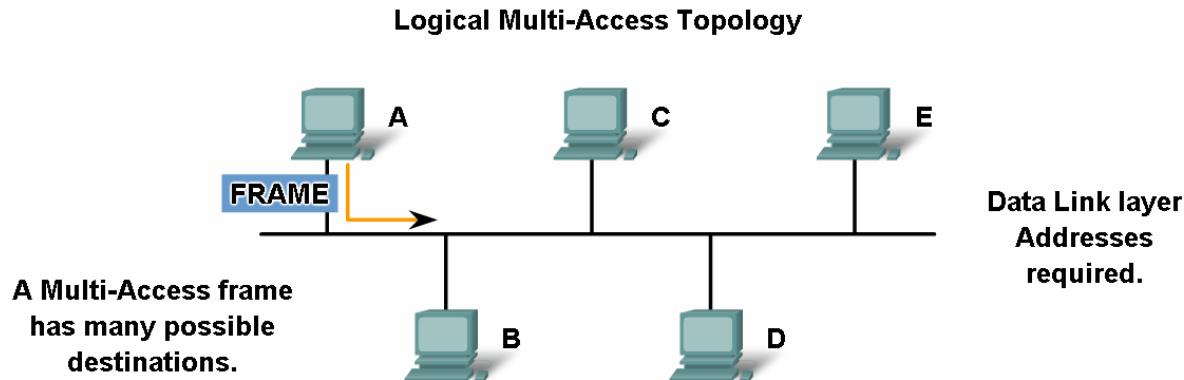
Media access control addressing and framing data

- Typical frame header fields include:
 - Start Frame** field - Indicates the beginning of the frame
 - Source and Destination address** fields - Indicates the source and destination nodes on the media
 - Priority/Quality of Service** field - Indicates a particular type of communication service for processing
 - Type field** - Indicates the upper layer service contained in the frame
 - Logical connection control** field - Used to establish a logical connection between nodes
 - Physical link control** field - Used to establish the media link
 - Flow control** field - Used to start and stop traffic over the media
 - Congestion control** field - Indicates congestion in the media



Media access control addressing and framing data

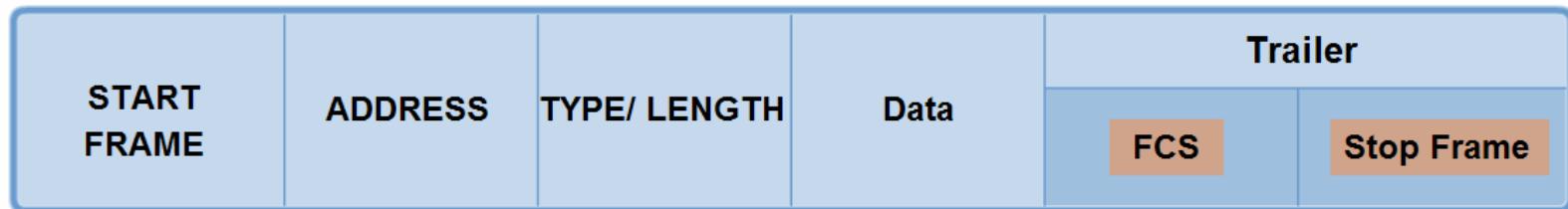
- The role of addressing in the Data Link layer. Cases where addresses are needed and cases where addresses are not needed





Media access control addressing and framing data

- Data Link layer protocols add a **trailer** to the end of each frame.
- The trailer is used to determine if the frame arrived without error. This process is called **error detection**.
- The **Frame Check Sequence** (FCS) field is used to determine if errors occurred in the transmission and reception of the frame.





Media access control addressing and framing data

- Protocols that will be covered in CCNA courses include:
 - Ethernet
 - Point-to-Point Protocol (**PPP**)
 - High-Level Data Link Control (**HDLC**)
 - Frame Relay
 - Asynchronous Transfer Mode (**ATM**)



Ethernet standard

- Ethernet is a family of networking technologies that are defined in the **IEEE 802.2** and **802.3** standards.
- Ethernet standards define both the Layer 2 protocols and the Layer 1 technologies.
- Ethernet is the most widely used LAN technology and supports data bandwidths of **10, 100, 1000, or 10,000 Mbps**.
- The basic frame format and the IEEE sublayers of OSI Layers 1 and 2 **remain consistent** across all forms of Ethernet.
- Ethernet provides unacknowledged connectionless service over a shared media using **CSMA/CD** as the media access methods.
- An Ethernet **MAC address** is **48 bits** and is generally represented in hexadecimal format.
- **Ethernet II** is the Ethernet frame format used in **TCP/IP** networks.



Ethernet frame

Ethernet Protocol

A Common Data Link Layer Protocol for LANs

Frame						Frame Check Sequence
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.

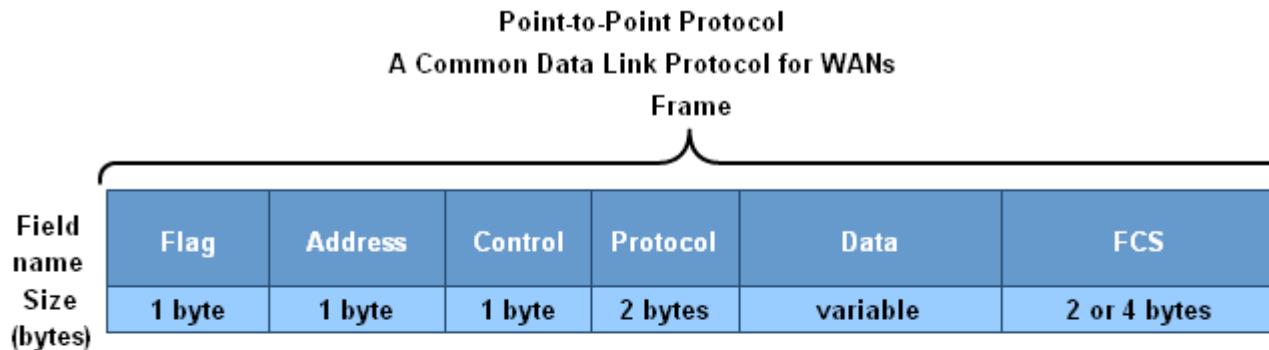
Data or payload - this is the PDU, typically an IPv4 packet, that is to be transported over the media.

Frame Check Sequence (FCS) - A value used to check for damaged frames.



PPP standard

- **Point-to-Point Protocol (PPP)** is a protocol used to deliver frames between two nodes.
- PPP can be used on various physical media



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.



Wireless Protocol for LANs

- **802.11 (Wi-Fi)** is an extension of the IEEE 802 standards.
- It uses the same 802.2 LLC and 48-bit addressing scheme as other 802 LANs.
- There are many differences at the MAC sublayer and Physical layer.
- Standard IEEE 802.11 is a contention-based system using a **Carrier Sense Multiple Access/Collision Avoidance** (CSMA/CA) media access process.
- **CSMA/CA** specifies a random backoff procedure for all nodes that are waiting to transmit. Making the nodes back off for a random period greatly reduces the likelihood of a collision.

Wireless Protocol for LANs

Destination Address (DA) - MAC address of the final destination node in the network

Source Address (SA) - MAC address of the node that initiated the frame

Receiver Address (RA) - MAC address that identifies the wireless device that is the immediate recipient of the frame

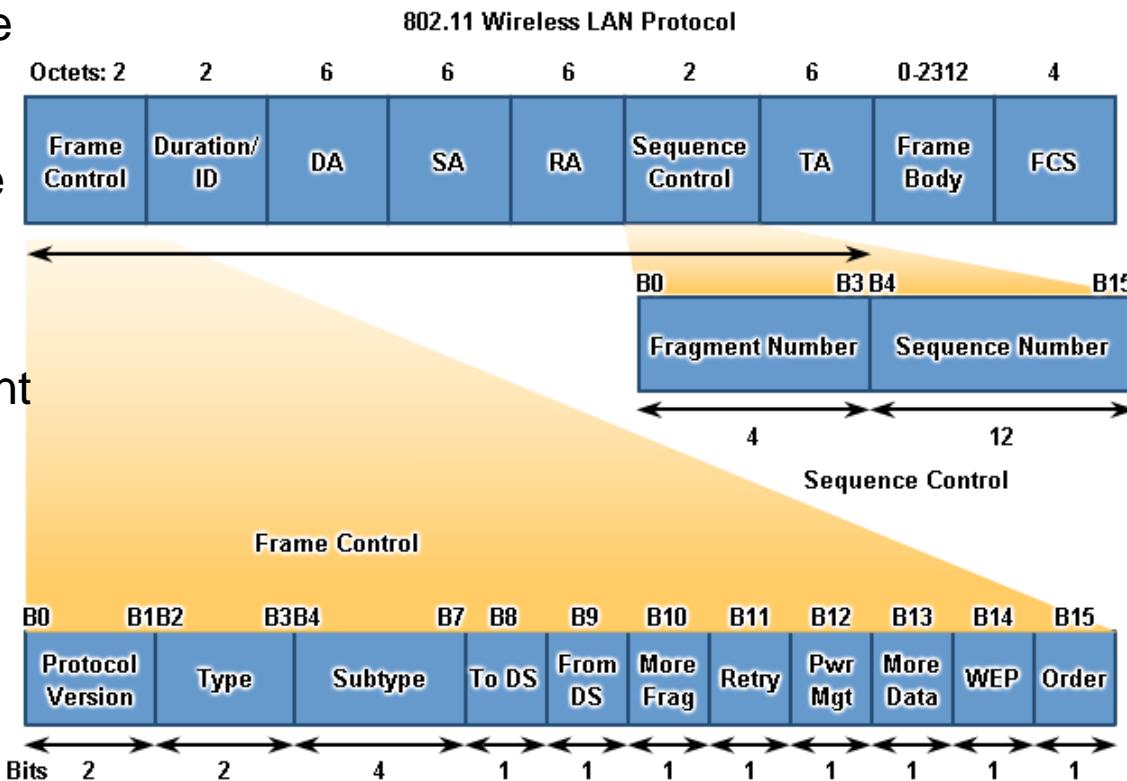
Transmitter Address (TA) - MAC address that identifies the wireless device that transmitted the frame

Sequence Number - number assigned to the frame

Fragment Number - Indicates the number for each fragment of a frame

Frame Body - Contains the information being transported; for data frames, typically an IP packet

FCS - Contains a 32-bit CRC of the frame



Summary

In this chapter, you learned to:

- Explain the role of Data Link layer protocols in data transmission.
- Describe how the Data Link layer prepares data for transmission on network media.
- Describe the different types of media access control methods.
- Identify several common logical network topologies and describe how the logical topology determines the media access control method for that network.
- Explain the purpose of encapsulating packets into frames to facilitate media access.
- Describe the Layer 2 frame structure and identify generic fields.
- Explain the role of key frame header and trailer fields, including addressing, QoS, type of protocol, and Frame Check Sequence.

Proces transmisji danych Fig. 7.4.1.2





OSI Physical Layer



Network Fundamentals – Chapter 8

Cisco | Networking Academy®
Mind Wide Open™

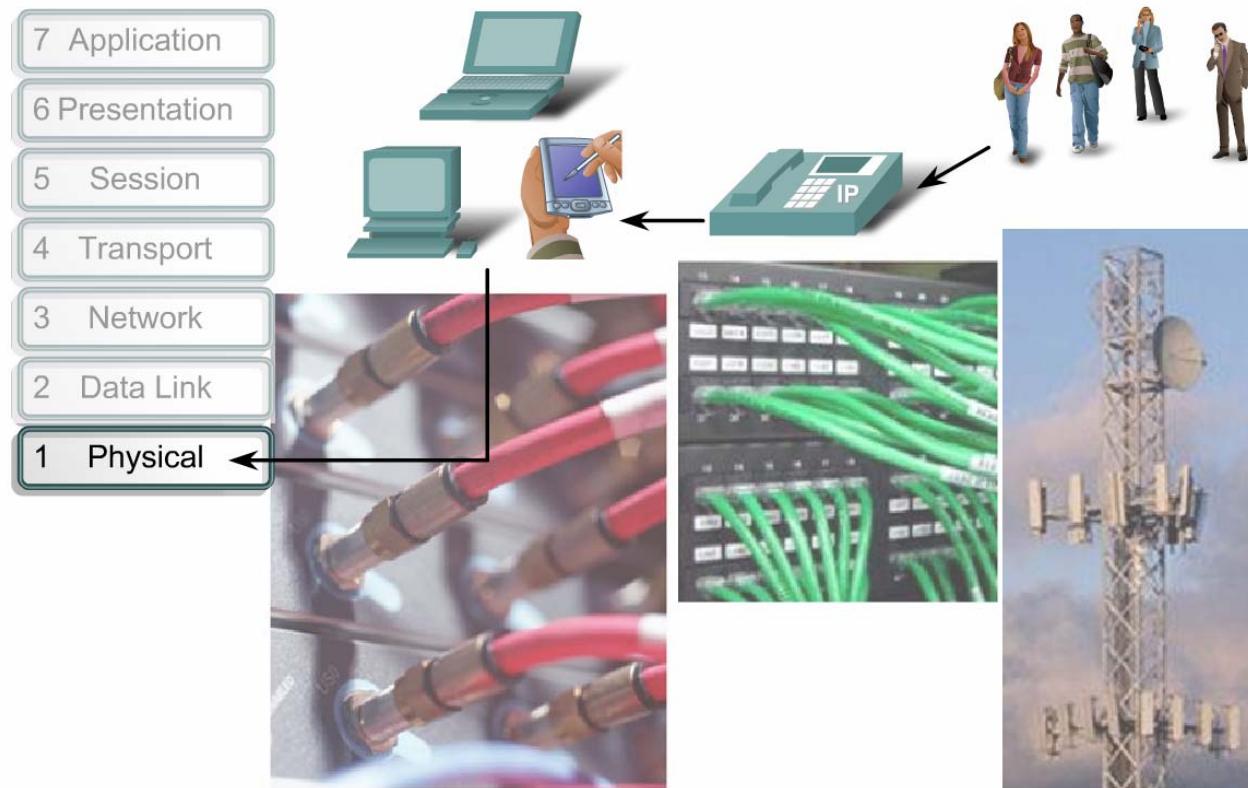


Objectives

- Explain the role of Physical layer protocols and services in supporting communication across data networks.
 - Describe the role of signals used to represent bits as a frame as the frame is transported across the local media
- Describe the purpose of Physical layer signaling and encoding as they are used in networks
- Identify the basic characteristics of copper, fiber and wireless network media
- Describe common uses of copper, fiber and wireless network media

Physical Layer Protocols & Services

- The OSI Physical layer provides the means to transport across the network media the bits that make up a Data Link layer frame.



The Physical layer interconnects our data networks.

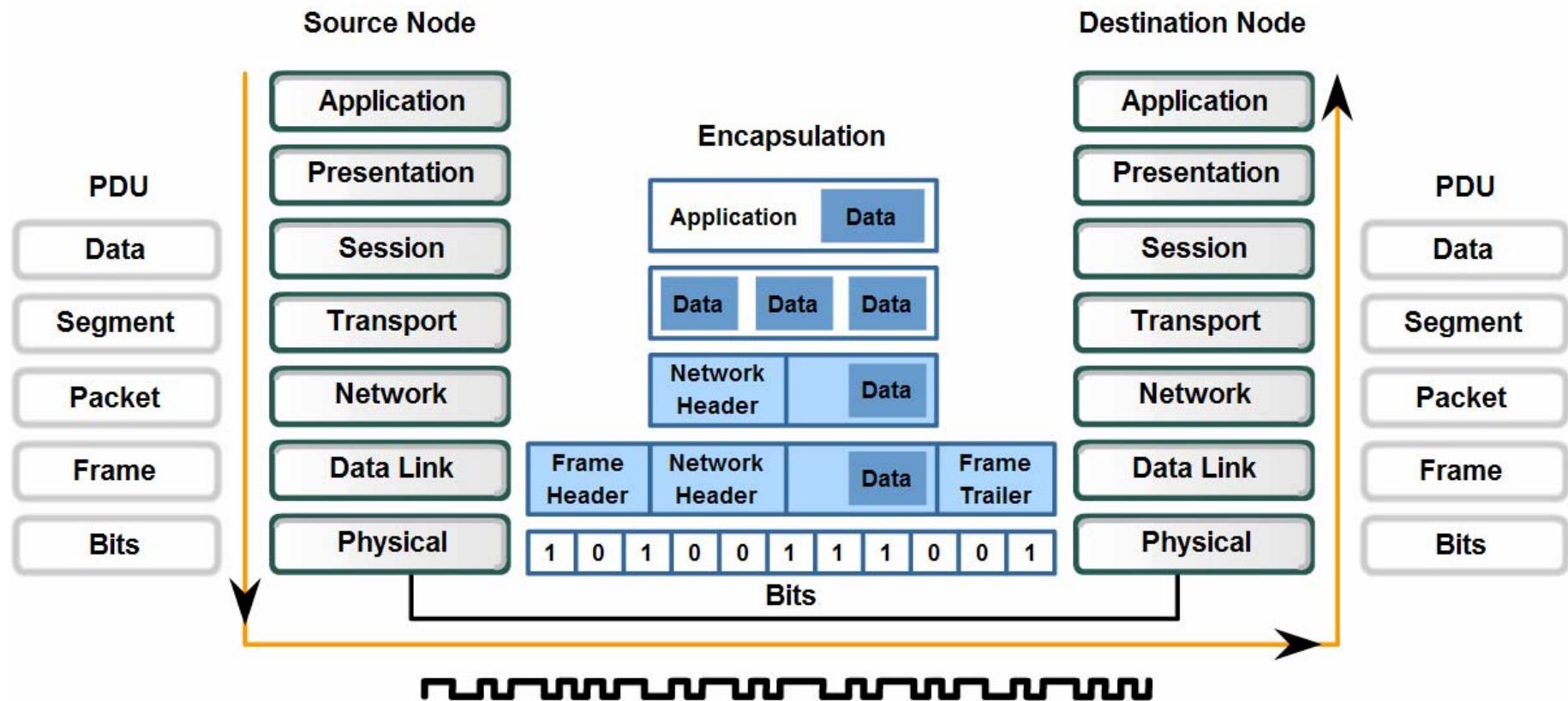


Physical Layer Protocols & Services

- The delivery of frames across the local media requires the following Physical layer elements:
 - The physical media and associated connectors
 - A representation of bits on the media
 - Encoding of data and control information
 - Transmitter and receiver circuitry on the network devices
- The purpose of the Physical layer is to create the electrical, optical, or microwave signal that represents the bits in each frame. These signals are then sent on the media one at a time.

Physical Layer Protocols & Services

Transforming Human Network Communications to Bits

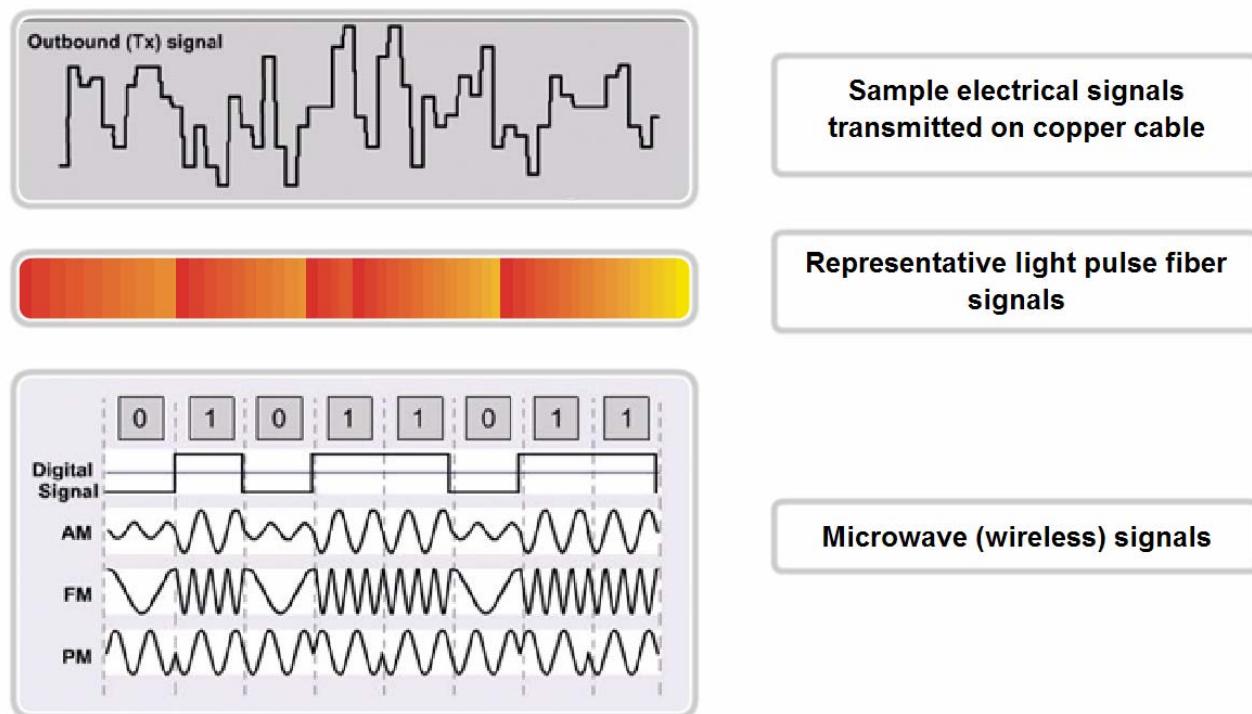




Physical Layer Protocols & Services

- Three basic forms of network media on which data is represented: Copper cable, Fiber, Wireless

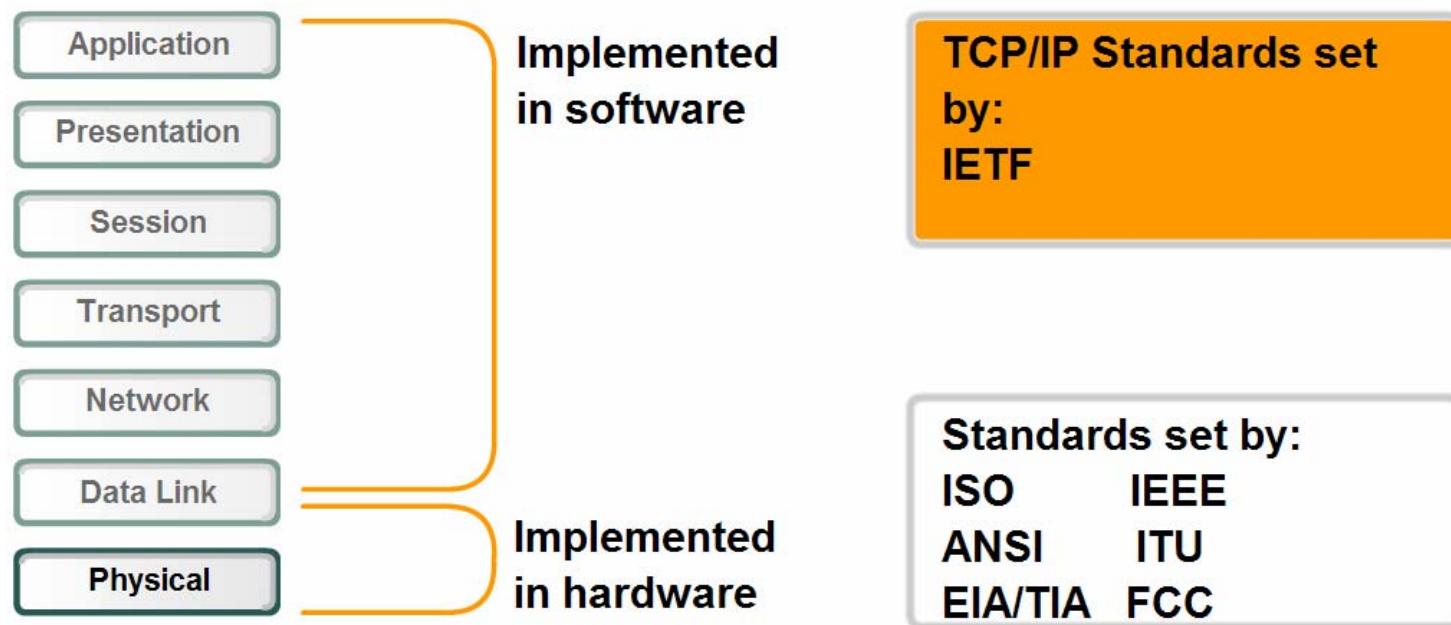
Representations of Signals on the Physical Media



Physical Layer Protocols & Services

- Distinguish who establishes and maintains standards for the Physical layers compared to those for the other layers of the network

Comparison of Physical layer standards and upper layer standards





Physical Layer Technologies and Hardware

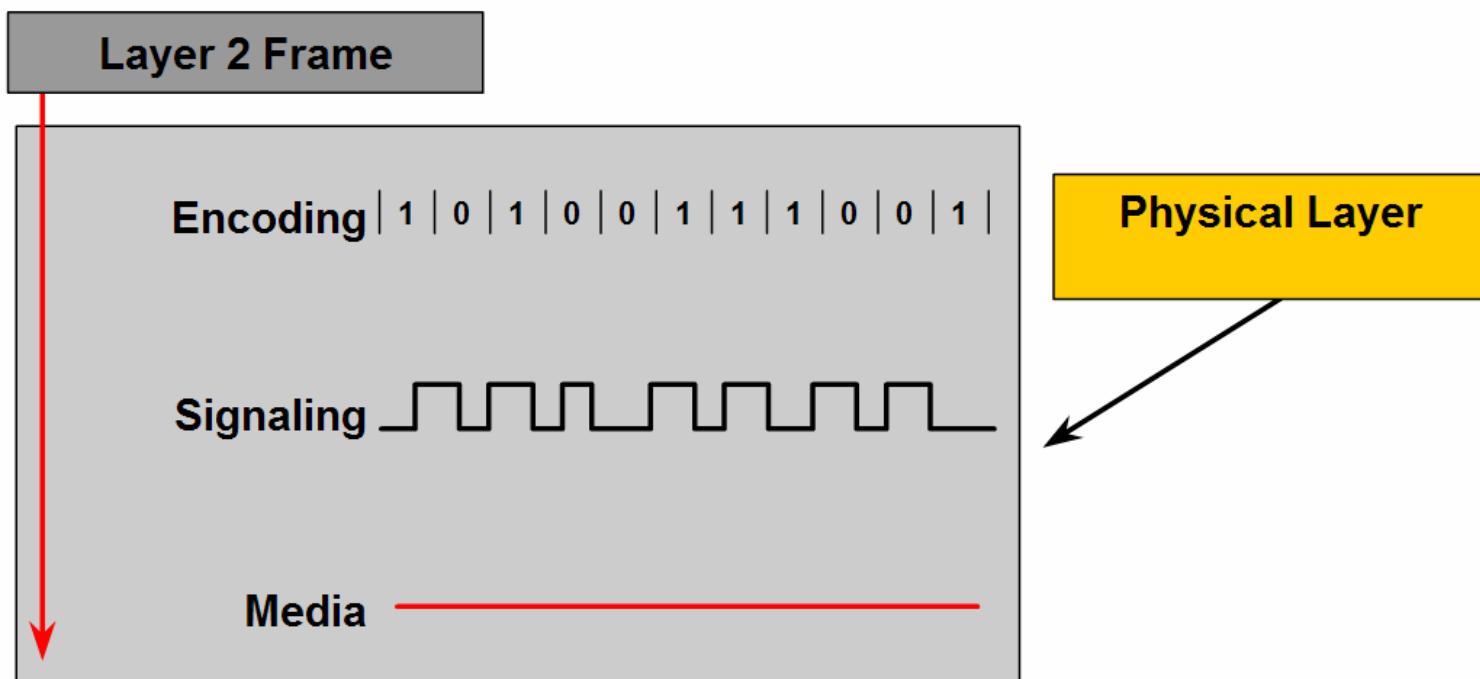
The technologies defined by these organizations include four areas of the Physical layer standards:

- Physical and electrical properties of the media
- Mechanical properties (materials, dimensions, pinouts) of the connectors
- Bit representation by the signals (encoding)
- Definition of control information signals

Physical Layer Protocols & Services

The three fundamental functions of the Physical layer are:

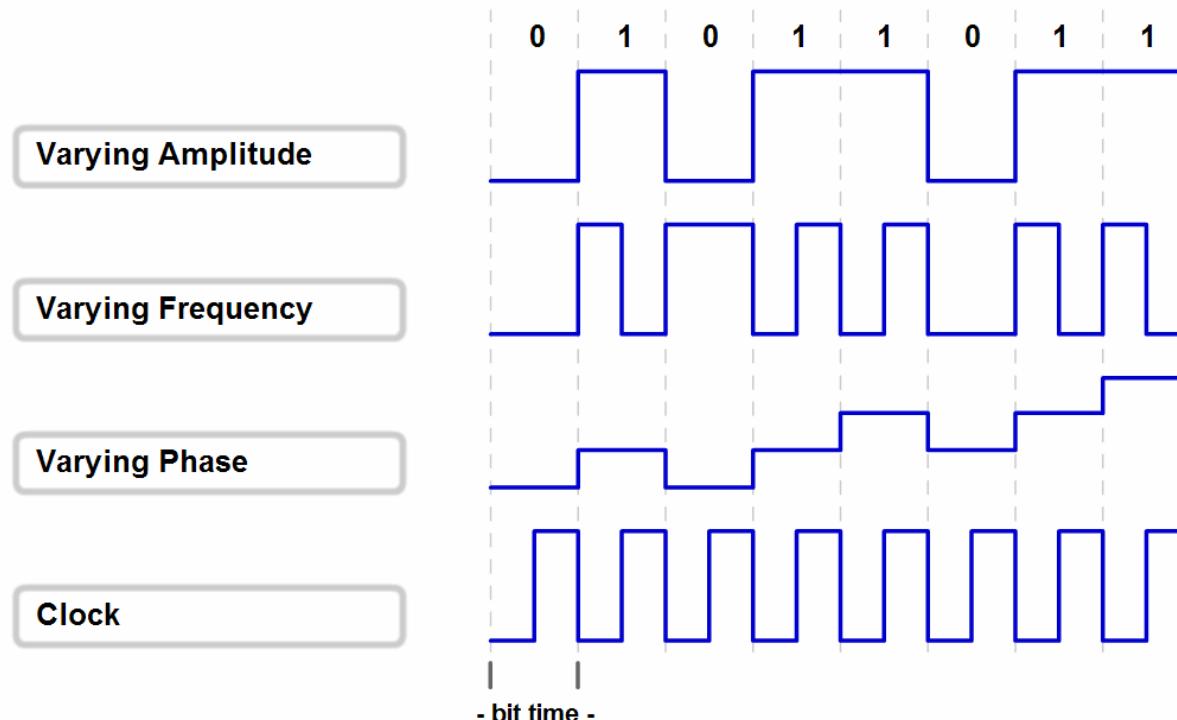
- The physical components
- Data encoding
- Signaling



Physical Layer Signaling and Encoding

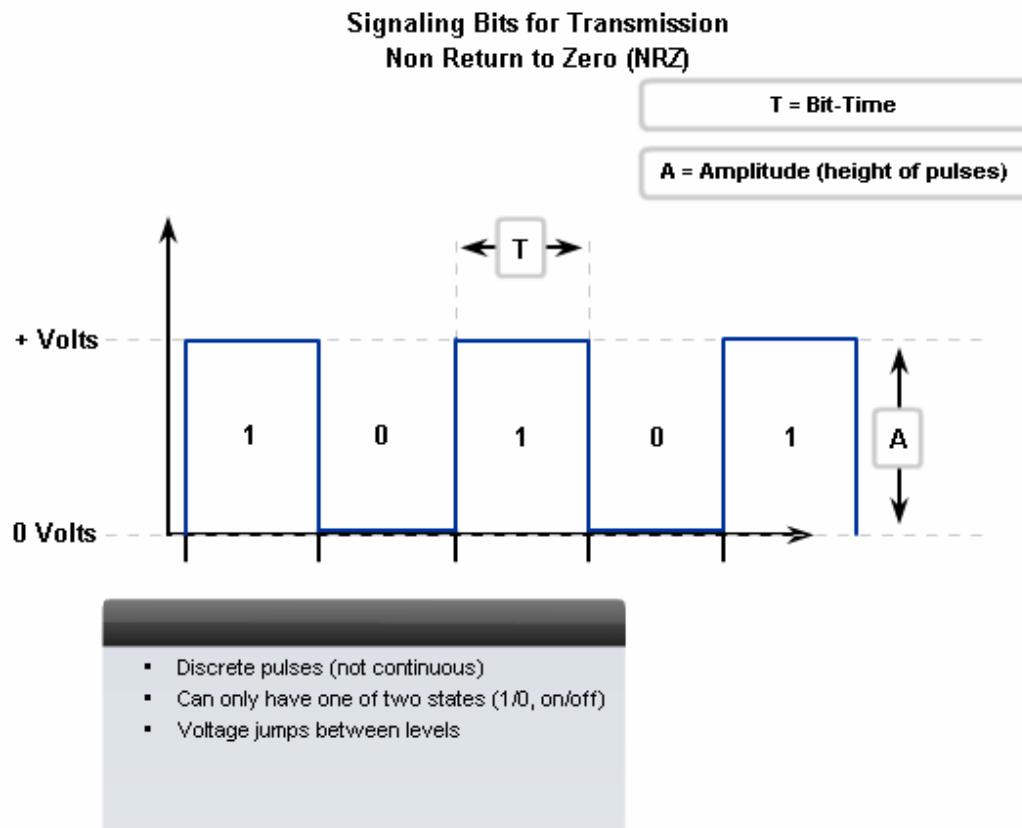
- Eventually, all communication from the human network becomes binary digits, which are transported individually across the physical media.

Ways to Represent a Signal on the Medium



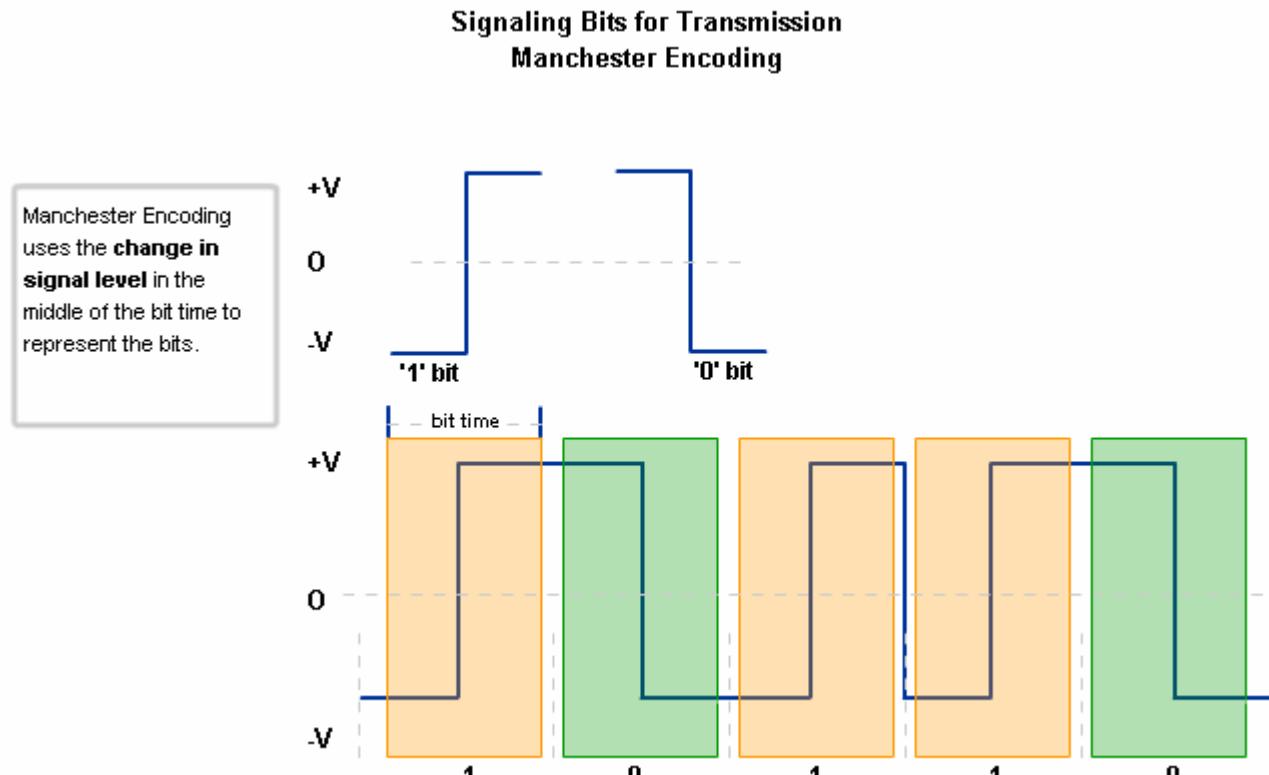
Non Return to Zero (NRZ)

- A low voltage value represents a logical 0 and a high voltage value represents a logical 1. The voltage range depends on the particular Physical layer standard in use.



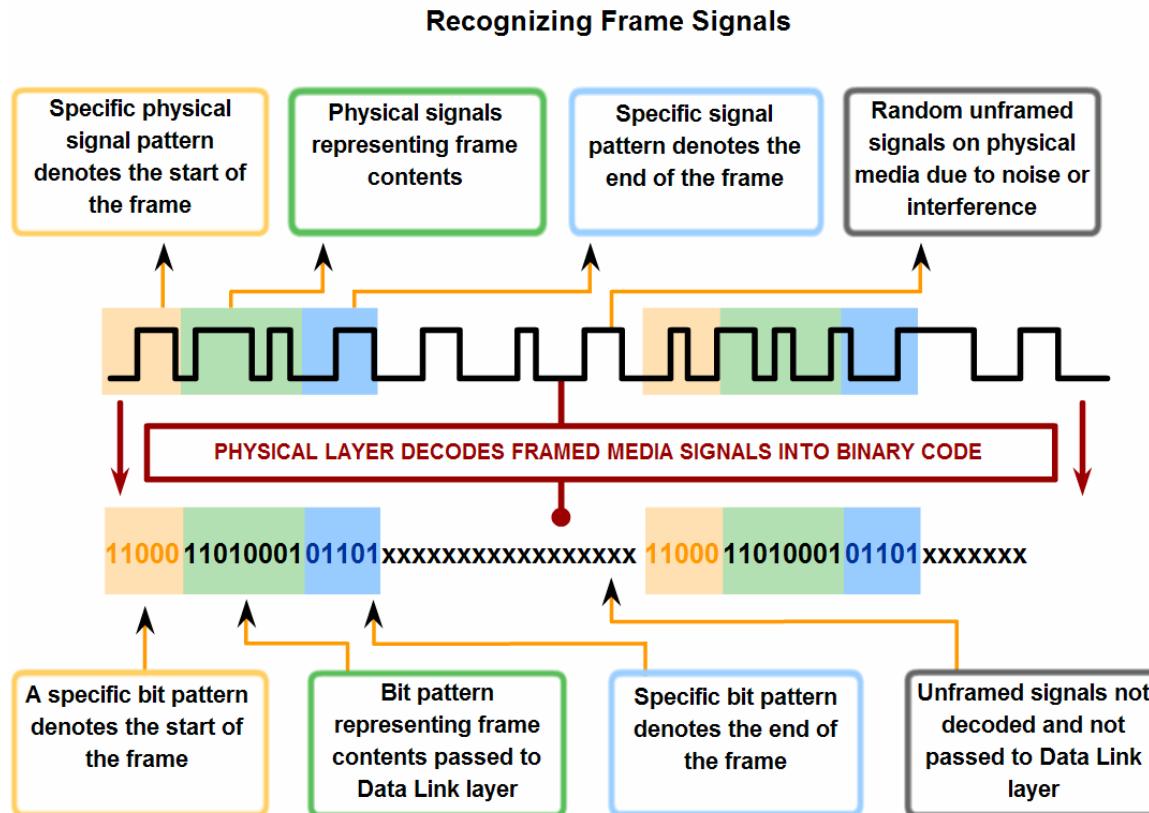
Manchester Encoding

- Although Manchester Encoding is not efficient enough to be used at higher signaling speeds, it is the signaling method employed by 10BaseT Ethernet (Ethernet running at 10 Megabits per second).



Physical Layer Signaling and Encoding

- By using an encoding step before the signals are placed on the media, we improve the efficiency at higher speed data transmission.





Physical Layer Signaling and Encoding

- A code group is a consecutive sequence of code bits that are interpreted and mapped as data bit patterns. For example, code bits 10101 could represent the data bits 0011.
- Although using code groups introduces overhead in the form of extra bits to transmit, they improve the robustness of a communications link. This is particularly true for higher speed data transmission.
- Advantages using code groups include:
 - Reducing bit level error (enhance synchronization)
 - Limiting the effective energy transmitted into the media
 - Helping to distinguish data bits from control bits
 - Better media error detection

Physical Layer Signaling and Encoding

- 4B/5B ensures that there is at least one level change per code to provide synchronization. Most of the codes used in 4B/5B balance the number of 1s and 0s used in each symbol.

4B/5B Code Symbols	
Data Codes	
4B Code	5B Symbol
0000	11110
0001	01001
0010	10100
0011	10101
0100	01010
0101	01011
0110	01110
0111	01111
1000	10010
1001	10011
1010	10110
1011	10111
1100	11010
1101	11011
1110	11100
1111	11101

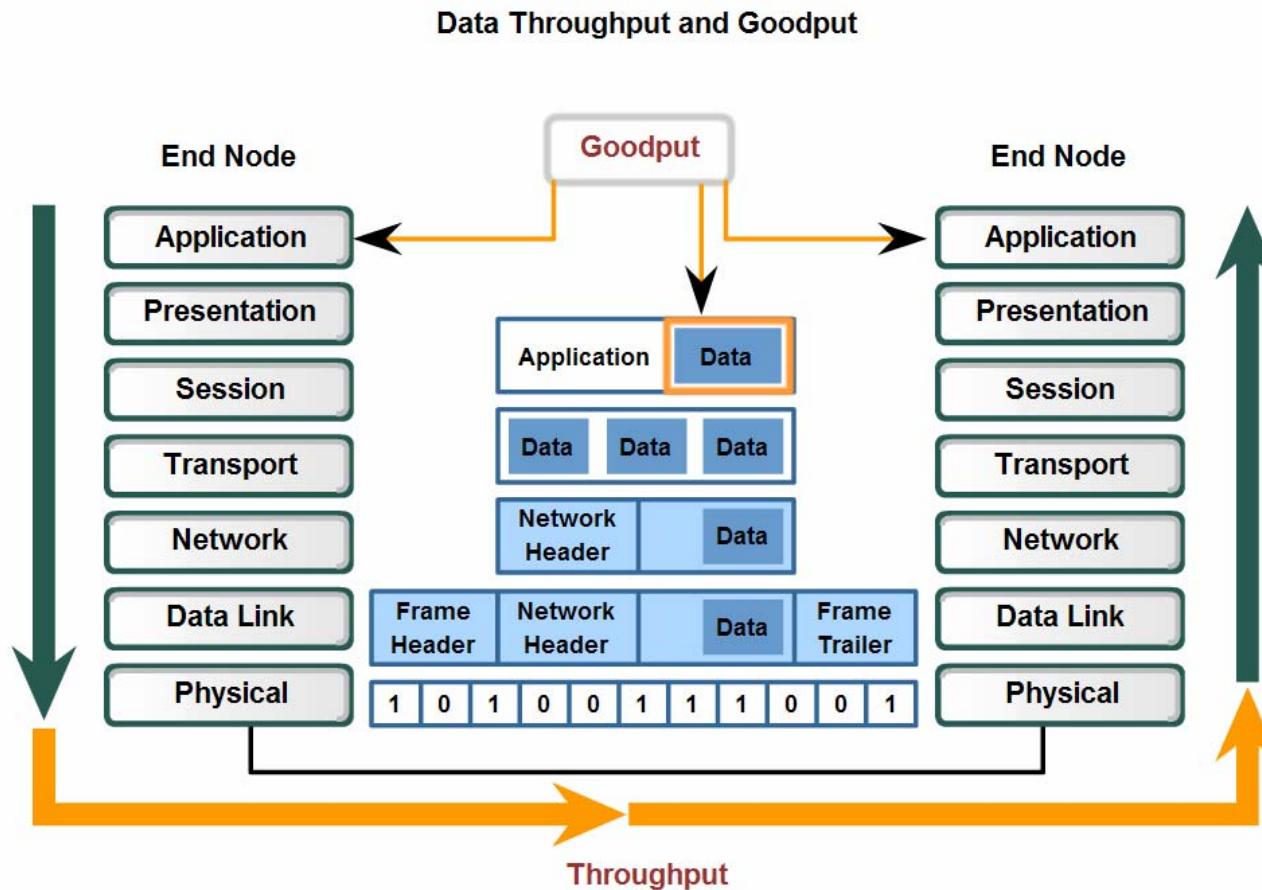
Control and Invalid Codes	
4B Code	5B Symbol
idle	11111
start of stream	11000
start of stream	10001
end of stream	01101
end of stream	00111
transmit error	00111
invalid	00000
invalid	00001
invalid	00010
invalid	00011
invalid	00100
invalid	00101
invalid	00110
invalid	01000
invalid	10000
invalid	11001

Physical Layer Signaling and Encoding

- The capacity of a medium to carry data is described as the raw data bandwidth of the media. Digital bandwidth measures the amount of information that can flow from one place to another in a given amount of time.

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

Physical Layer Signaling and Encoding



Data **throughput** is actual network performance. **Goodput** is a measure of the transfer of usable data after protocol overhead traffic has been removed.

Characteristics & Uses of Network Media

- Physical layer standards.

Physical Media - Characteristics

Ethernet Media

	10BASE-T	100BASE-TX	100BASE-FX	1000BASE-CX	1000BASE-T	1000BASE-SX	1000BASE-LX	1000BASE-ZX	10GBASE-ZR
Media	EIA/TIA Category 3, 4, 5 UTP, two pair	EIA/TIA Category 3, 4, 5 UTP, two pair	50/62.5 µm multi mode fiber	STP	EIA/TIA Category 3, 4, 5 UTP, four pair	62.5/50 micron multimode fiber	50/62.5 micron multimode fiber or 9 micron single mode fiber	9µm single mode fiber	9µm single mode fiber
Maximum Segment Length	100m (328 feet)	100m (328 feet)	2 km (6562 ft)	25 m (82 feet)	100 m (328 feet)	Up to 550 m (1,804 ft) depending on fiber used	550 m (MMF) 10 km (SMF)	Approx. 70 km	Up to 80 km
Topology	Star	Star	Star	Star	Star	Star	Star	Star	Star
Connector	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)		ISO 8877 (RJ-45)	ISO 8877 (RJ-45)				

Characteristics & Uses of Network Media

- Cable types with shielding or twisting of the pairs of wires are designed to minimize signal degradation due to electronic noise.

External Interference with Copper Media



Sources of interference to data signals on copper media



Fluorescent lighting



Electric motors

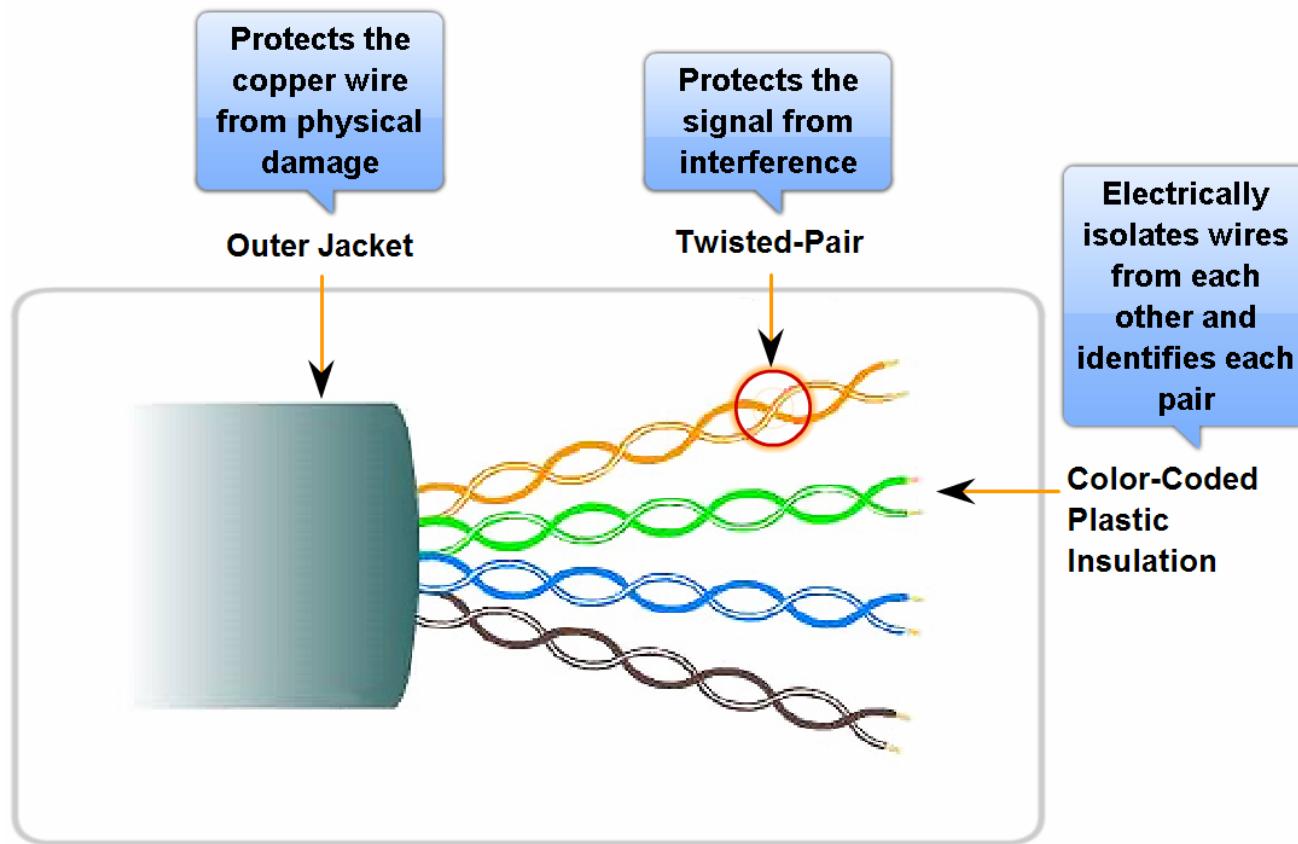


Radio waves

Characteristics & Uses of Network Media

- Basic characteristics of UTP cable, crosstalk, cancellation effect

Unshielded Twisted-Pair (UTP) Cable

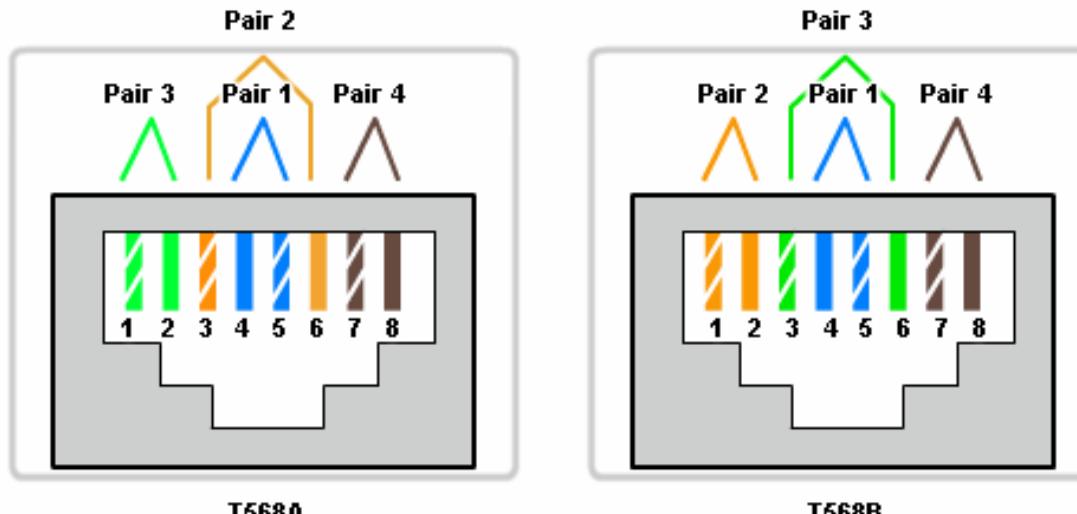


Characteristics & Uses of Network Media

■ UTP cable types:

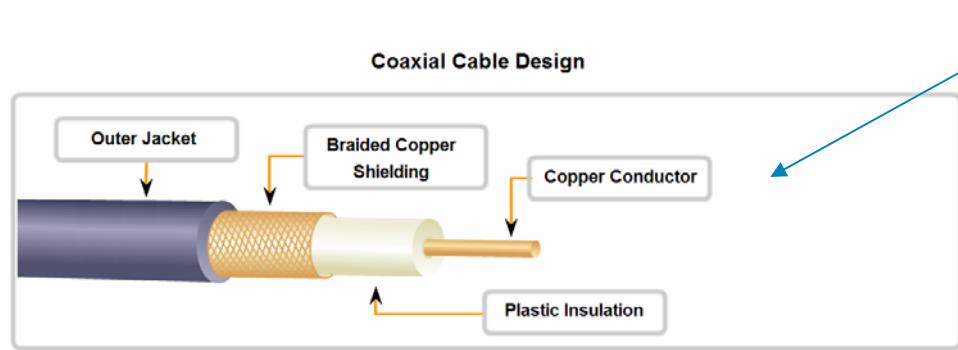
Straight-through, Crossover, and Rollover Cable Types

Cable Type	Standard	Application
Ethernet Straight-through	Both end T568A or both end T568B	Connecting a network host to a network device such as a switch or hub.
Ethernet Crossover	One end T568A, other end T568B	Connecting two network hosts. Connecting two network intermediary devices (switch to switch, or router to router).
Rollover	Cisco proprietary	Connect a workstation serial port to a router console port, using an adapter.



Characteristics & Uses of Network Media

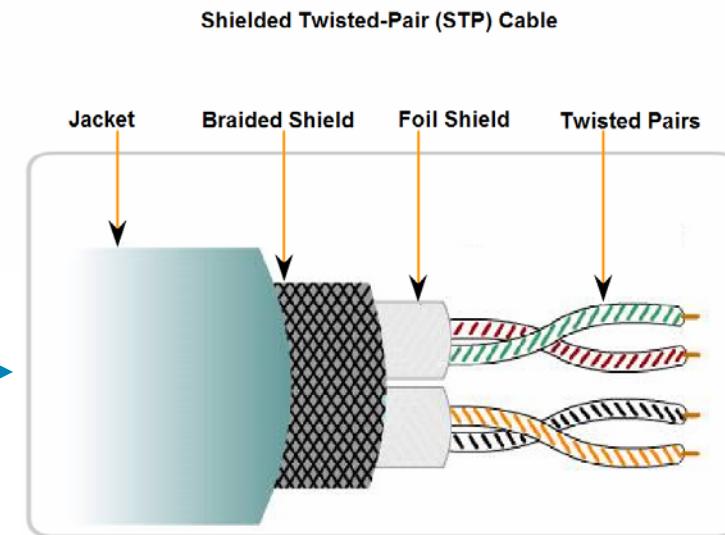
- Identify the basic characteristics of STP and Coaxial cable



Examples:
Thinnet 10Base2
Thicknet 10Base5



Examples:
Token Ring
10Gb Ethernet



Characteristics & Uses of Network Media

■ Electrical Hazards, Fire Hazards

Copper Media Safety



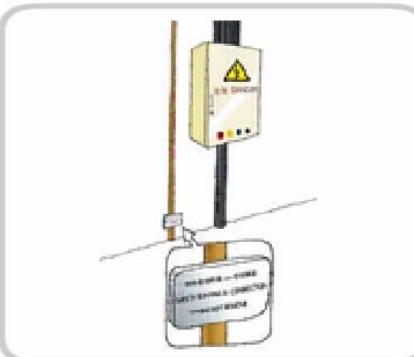
The separation of data and electrical power cabling must comply with safety codes.



Cables must be connected correctly.



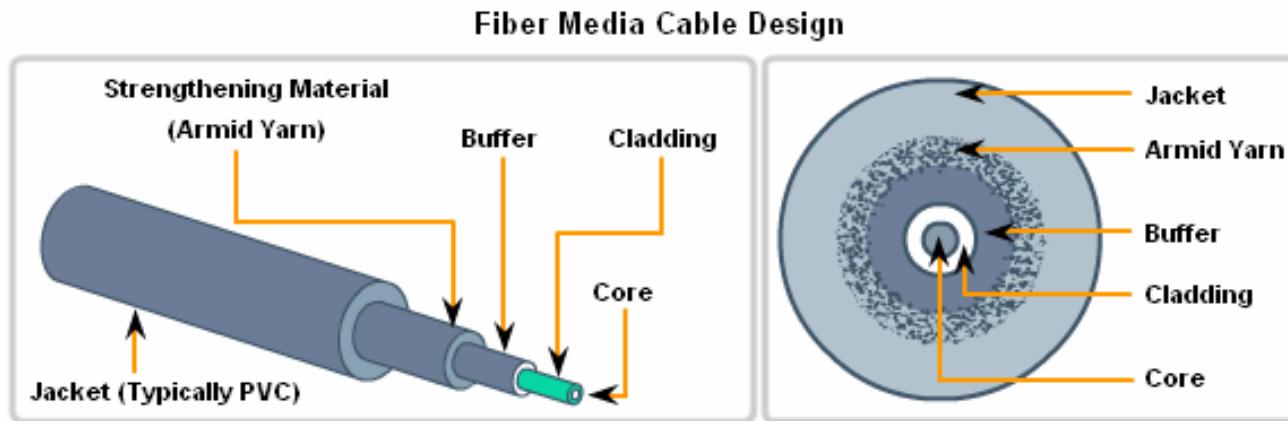
Installations must be inspected for damage.



Equipment must be grounded correctly.

Characteristics & Uses of Network Media

■ Fiber media structure

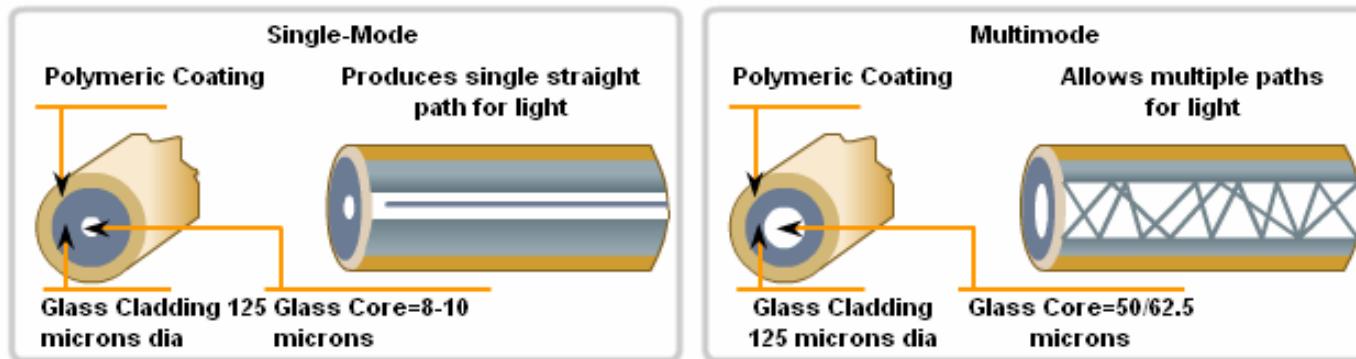


Fiber Connectors

Characteristics & Uses of Network Media

- Identify several primary characteristics of fiber cabling and its main advantages over other media

Fiber Media Modes



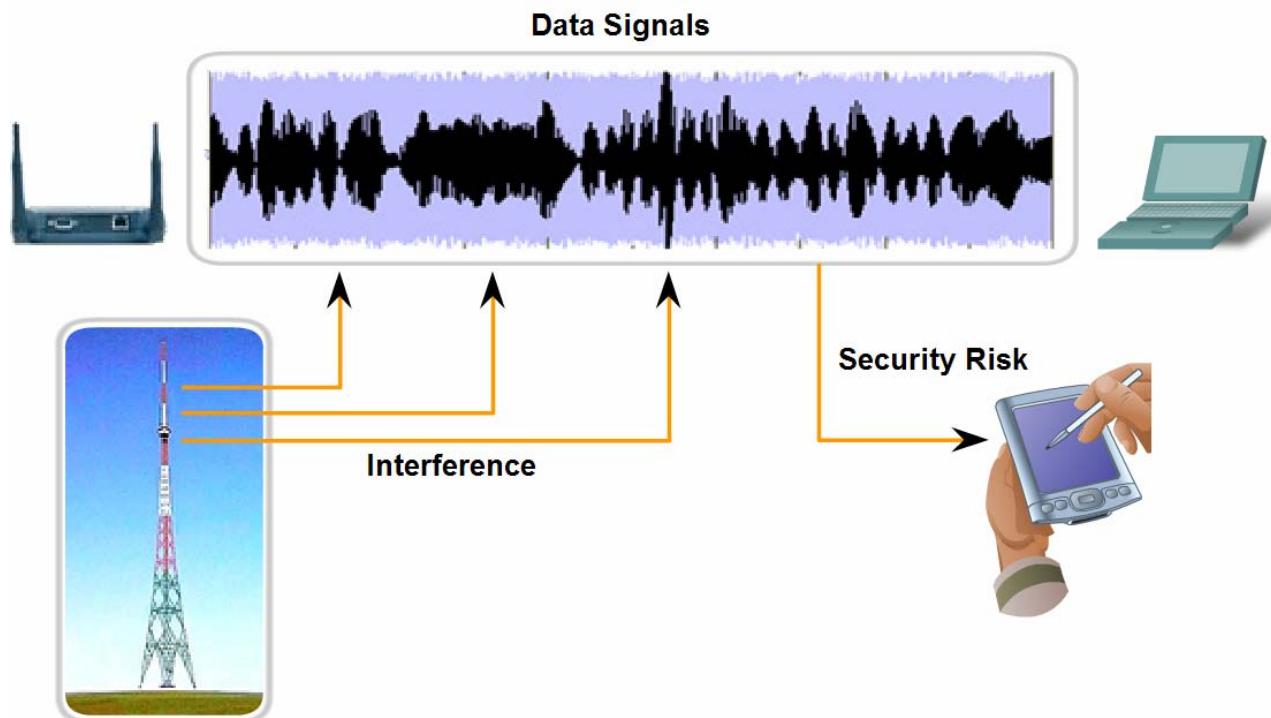
- Small Core
- Less Dispersion
- Suited for long distance applications (up to 100 km, 62,14 mi.)
- Uses lasers as the light source often within campus backbones for distance of several thousand meters

- Larger core than single-mode cable (50 microns or greater)
- Allows greater dispersion and therefore, loss of signal
- Used for long distance application, but shorter than single-mode (up to ~2km, 6560 ft)
- Uses LEDs as the light source often within LANs or distances of couple hundred meters within a campus network

Characteristics & Uses of Network Media

- Wireless media carry electromagnetic signals at radio and microwave frequencies that represent the binary digits of data communications. As a networking medium, wireless is not restricted to conductors or pathways, as are copper and fiber media.

Wireless Media Signals and Security





Characteristics & Uses of Network Media

Types of Wireless Networks:

- Standard IEEE 802.11 - Commonly referred to as Wi-Fi, is a Wireless LAN (WLAN) technology that uses a contention or non-deterministic system with a Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) media access process.
- Standard IEEE 802.15 - Wireless Personal Area Network (WPAN) standard, commonly known as "Bluetooth", uses a device pairing process to communicate over distances from 1 to 100 meters.
- Standard IEEE 802.16 - Commonly known as WiMAX (Worldwide Interoperability for Microwave Access), uses a point-to-multipoint topology to provide wireless broadband access.
- Global System for Mobile Communications (GSM) - Includes Physical layer specifications that enable the implementation of the Layer 2 General Packet Radio Service (GPRS) protocol to provide data transfer over mobile cellular telephony networks.

Characteristics & Uses of Network Media

WIFI Standards:

- **IEEE 802.11a** - Operates in the 5 GHz frequency band and offers speeds of up to 54 Mbps. Because this standard operates at higher frequencies, it has a smaller coverage area and is less effective at penetrating building structures. Devices operating under this standard are not interoperable with the 802.11b and 802.11g standards described below.
- **IEEE 802.11b** - Operates in the 2.4 GHz frequency band and offers speeds of up to 11 Mbps. Devices implementing this standard have a longer range and are better able to penetrate building structures than devices based on 802.11a.
- **IEEE 802.11g** - Operates in the 2.4 GHz frequency band and offers speeds of up to 54 Mbps. Devices implementing this standard therefore operate at the same radio frequency and range as 802.11b but with the bandwidth of 802.11a.
- The **IEEE 802.11n** standard is currently in draft form. The proposed standard defines frequency of 2.4 Ghz or 5 GHz. The typical expected data rates are 100 Mbps to 210 Mbps with a distance range of up to 70 meters.

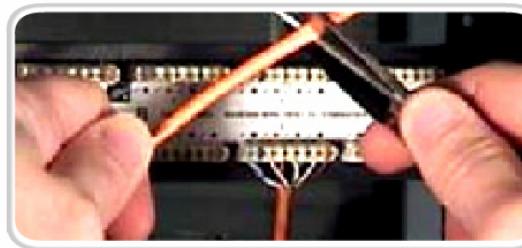
Characteristics & Uses of Network Media

- Different Physical layer standards specify the use of different connectors.

Copper Media Connectors



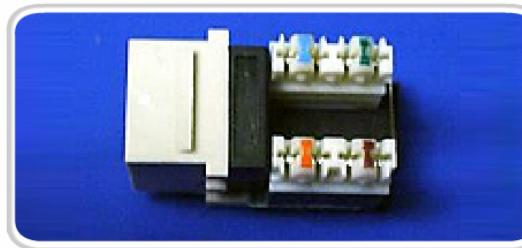
110 punch block



RJ45 UTP Plugs



RJ45 UTP Socket

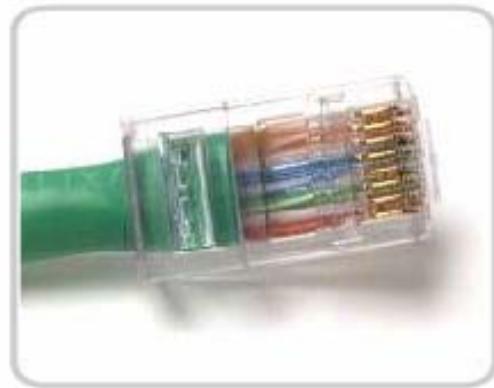


Characteristics & Uses of Network Media

- Copper Media Connectors RJ45 Termination



Bad connector - Wires are untwisted for too great a length.



Good connector - Wires are untwisted to the extent necessary to attach the connector.

- Improper cable termination can impact transmission performance.

Characteristics & Uses of Network Media

Fiber Media Connectors

ST Connector



Straight Tip (ST) connector is used with single-mode fiber

SC Connector



Subscriber Connector (SC) is used with multimode fiber

Single-Mode (LC)



Single-Mode Lucent Connector (LC)

Multimode (LC)



Multimode LC Connector

Duplex Multimode (LC)



Duplex Multimode LC Connector



Characteristics & Uses of Network Media

- Three common types of fiber-optic termination and splicing errors are:
 - Misalignment - the fiber-optic media are not precisely aligned to one another when joined.
 - End gap - the media do not completely touch at the splice or connection.
 - End finish - the media ends are not well polished or dirt is present at the termination.
- It is recommended that an Optical Time Domain Reflectometer (OTDR) be used to test each fiber-optic cable segment.



Summary

In this chapter, you learned to:

- Explain the role of Physical layer protocols and services in supporting communication across data networks.
- Describe the purpose of Physical layer signaling and encoding as they are used in networks.
- Describe the role of signals used to represent bits as a frame is transported across the local media.
- Identify the basic characteristics of copper, fiber, and wireless network media.
- Describe common uses of copper, fiber, and wireless network media.





Ethernet



Network Fundamentals – Chapter 9

Cisco | Networking Academy®
Mind Wide Open™

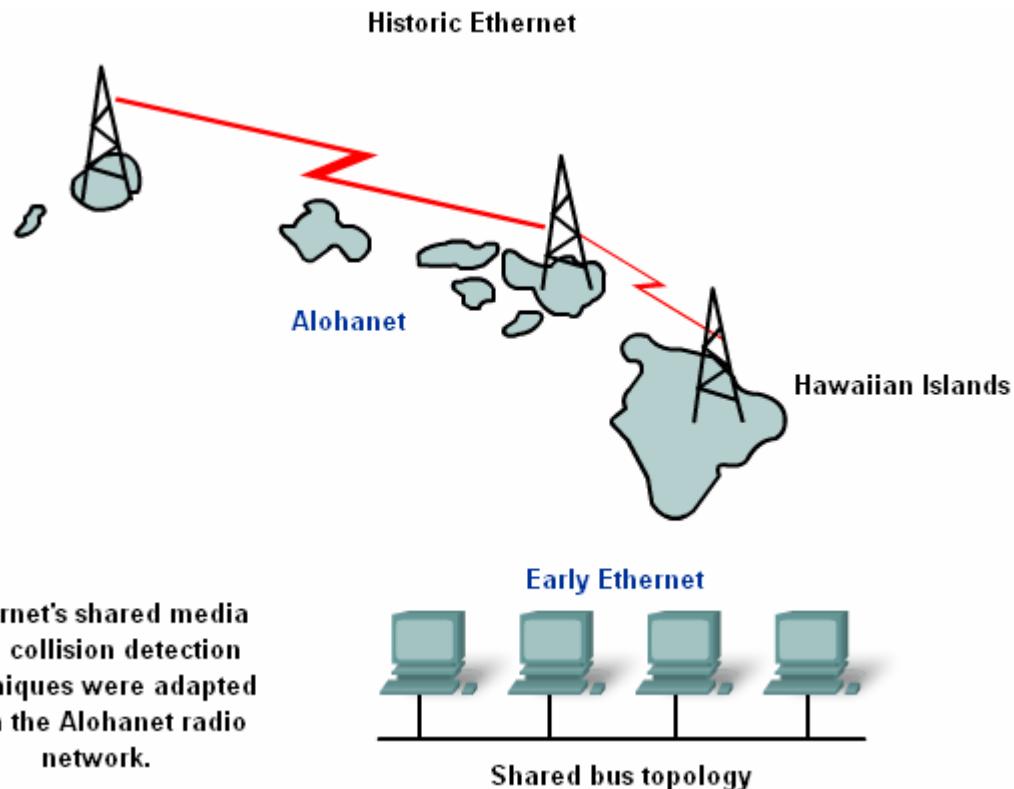


Objectives

- Identify the basic characteristics of network media used in Ethernet.
- Describe the physical and data link features of Ethernet.
- Describe the function and characteristics of the media access control method used by Ethernet protocol.
- Explain the importance of Layer 2 addressing used for data transmission and determine how the different types of addressing impacts network operation and performance.
- Compare and contrast the application and benefits of using Ethernet switches in a LAN as apposed to using hubs.
- Explain the ARP process.

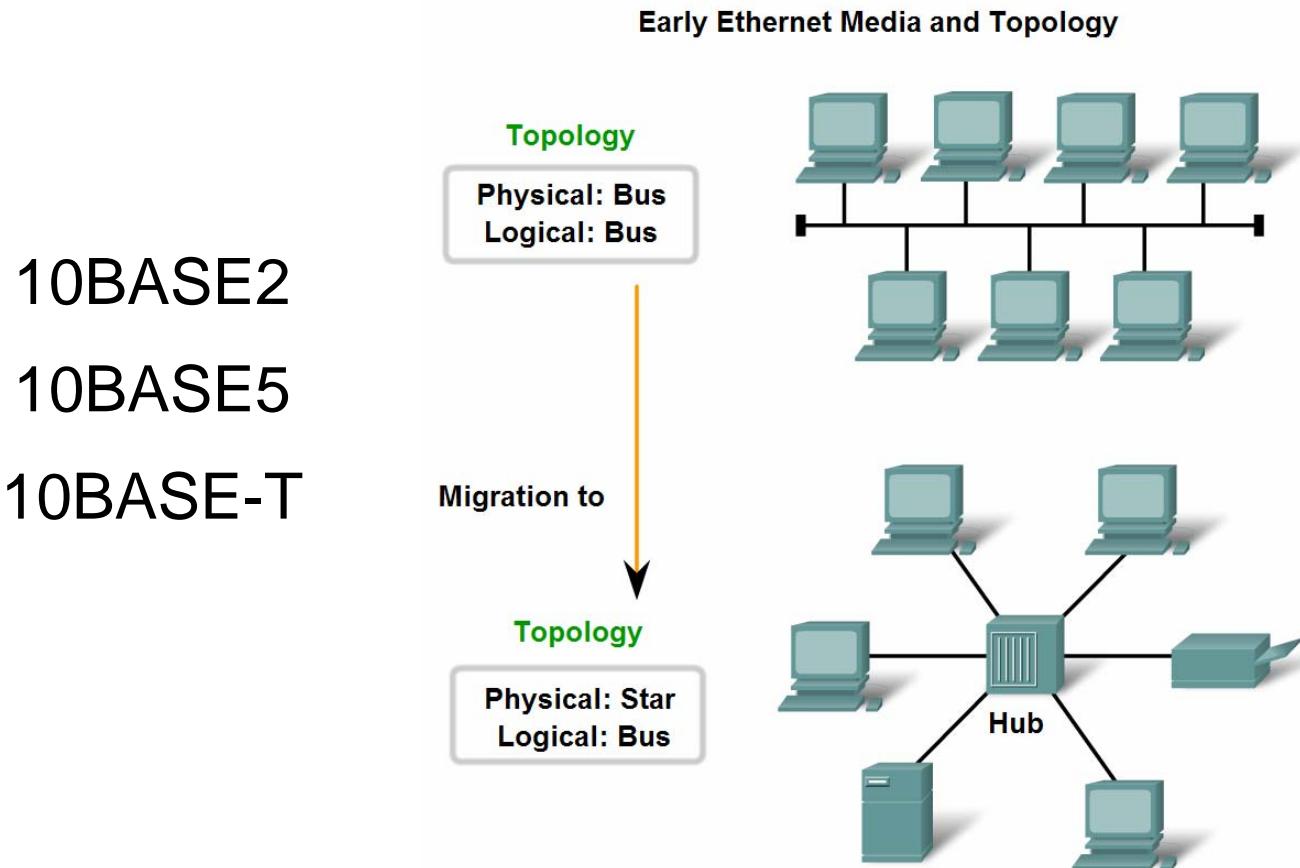
Historic Ethernet

- Alohanet
- First version of Ethernet – CSMA/CD



Characteristics of Network Media used in Ethernet

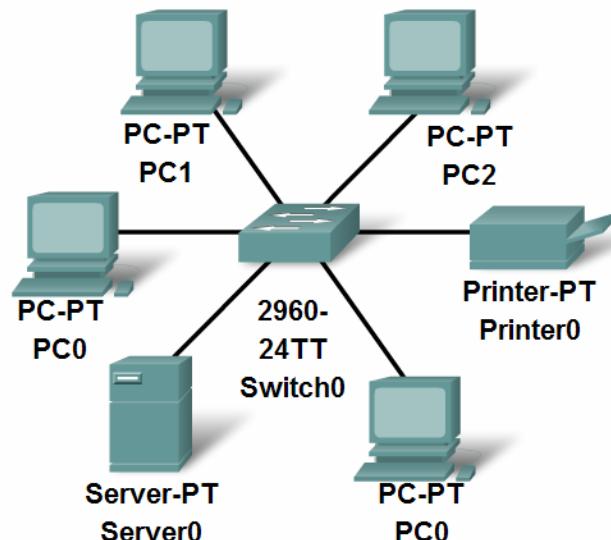
- Characteristics of Ethernet in its early years.



Characteristics of Network Media used in Ethernet

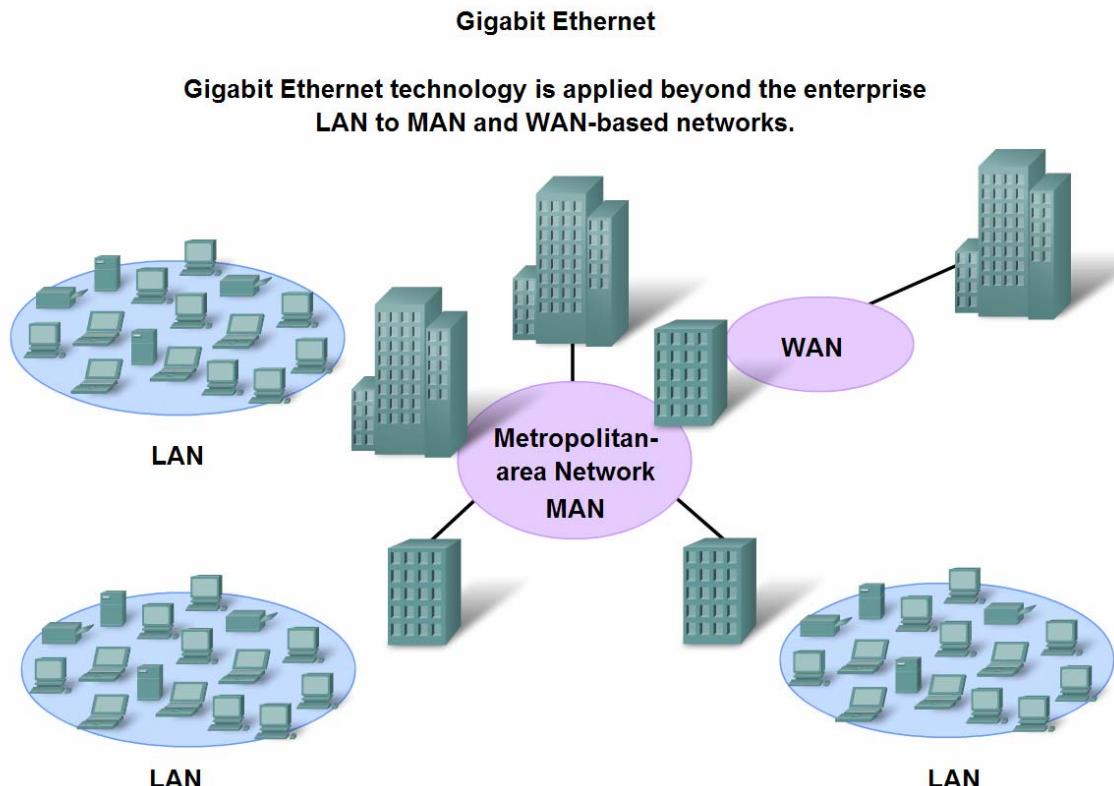
- Emergence of the LAN switch as a key innovation for managing collisions on Ethernet-based networks

Migration to Ethernet Switches



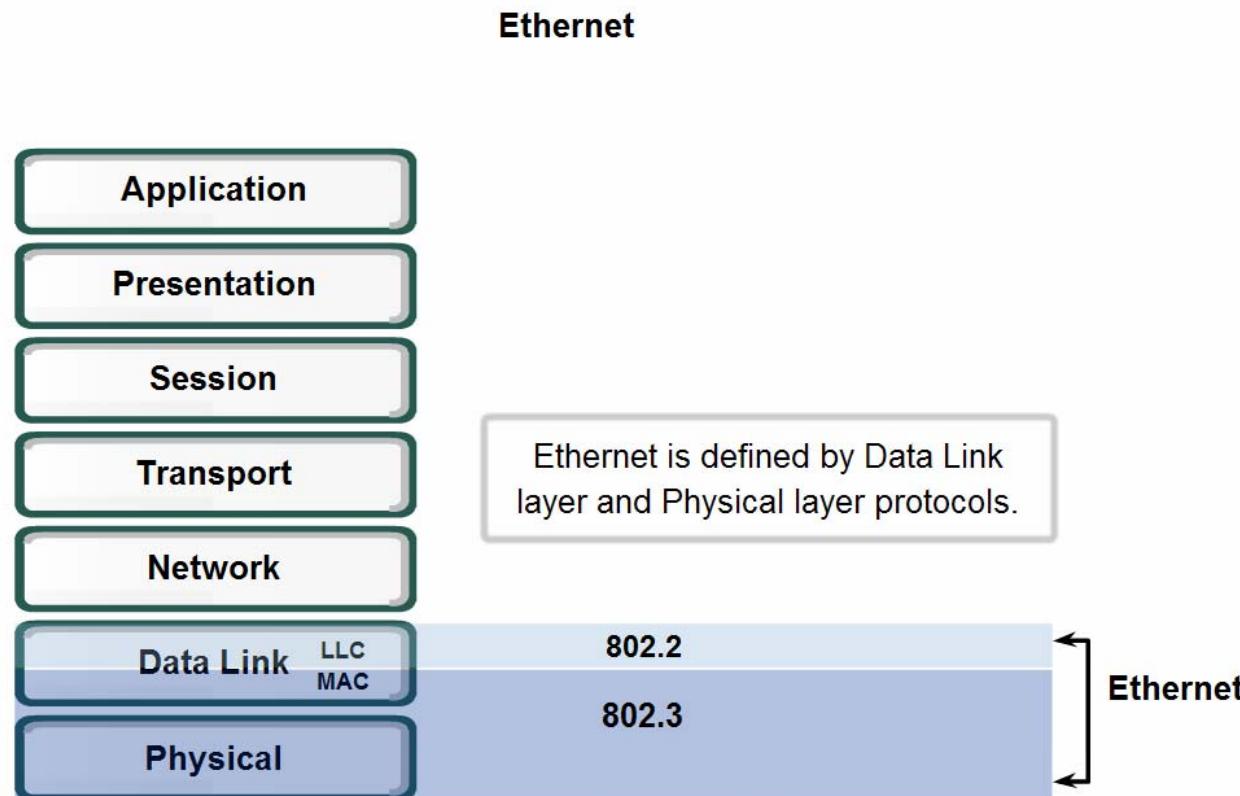
Characteristics of Network Media used in Ethernet

- Identify the characteristics of state-of-the-art Ethernet and describe its utilization of cabling and point-to-point topography



Physical and Data Link Features of Ethernet

- Standards and Implementation



Physical and Data Link Features of Ethernet

- Describe how the Ethernet operates across two layers of the OSI model

Layer 2 Addresses Layer 1 Limitations

Layer 1 Limitations	Layer 2 Functions
Cannot communicate with upper layers	Connects to upper layers via Logical Link Control (LLC)
Cannot identify devices	Uses addressing schemes to identify devices
Only recognizes streams of bits	Uses frames to organize bits into groups
Cannot determine the source of a transmission when multiple devices are transmitting	Uses Media Access Control (MAC) to identify transmission sources

Physical and Data Link Features of Ethernet

■ Logic Link Control – Connecting the Upper Layers

Logical Link Control (LLC)

- Makes the connection with the upper layers
- Frames the Network layer packet
- Identifies the Network layer protocol
- Remains relatively independent of the physical equipment

Logical Link Control Sublayer

802.3 Media Access Control

Physical Signaling Sublayer	10BASE5 (500m) 50 Ohm Coax N-Style	10BASE2 (185m) 50 Ohm Coax BNC	10BASE-T (100m) 100 Ohm UTP RJ-45	100BASE-TX (100m) 100 Ohm UTP RJ-45	1000BASE-CX (25m) 150 Ohm STP mini-DB-9	1000BASE-T (100m) 100 Ohm UTP RJ-45	1000BASE-SX (220-550m) MM Fiber SC	1000BASE-LX (550-5000m) MM or SM Fiber SC
Physical Medium								



Physical and Data Link Features of Ethernet

■ Media Access Control (MAC)

MAC—Getting Data to the Media

MEDIA ACCESS CONTROL

- Data Encapsulation
 - Frame delimiting
 - Addressing
 - Error detection
- Media Access Control
 - Control of frame placement on and off the media
 - media recovery

Physical and Data Link Features of Ethernet

- Physical Implementations of the Ethernet

Physical Devices Implementing Ethernet



UTP patch panels in a rack



Ethernet switches



Ethernet fiber connectors



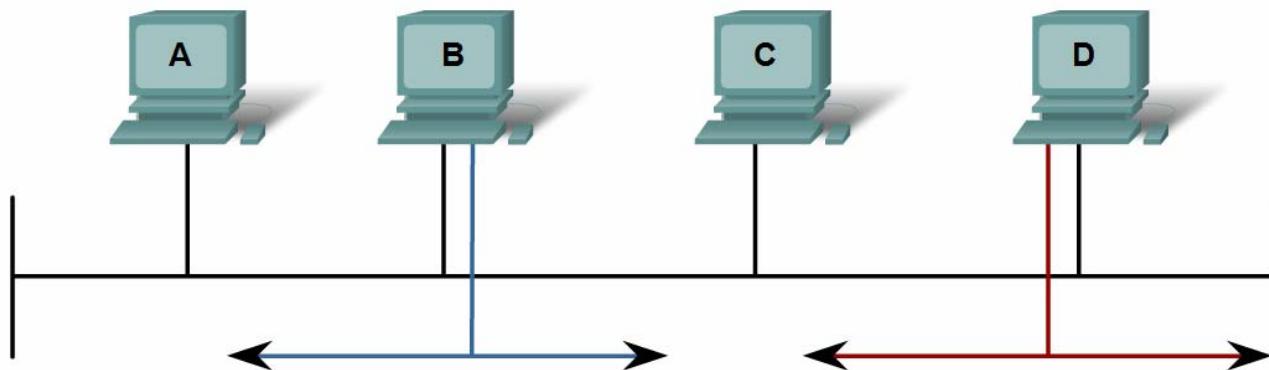
Ethernet switch

Function and Characteristics of the Media Access Control Method

- MAC in Ethernet

Media Access Control in Ethernet

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



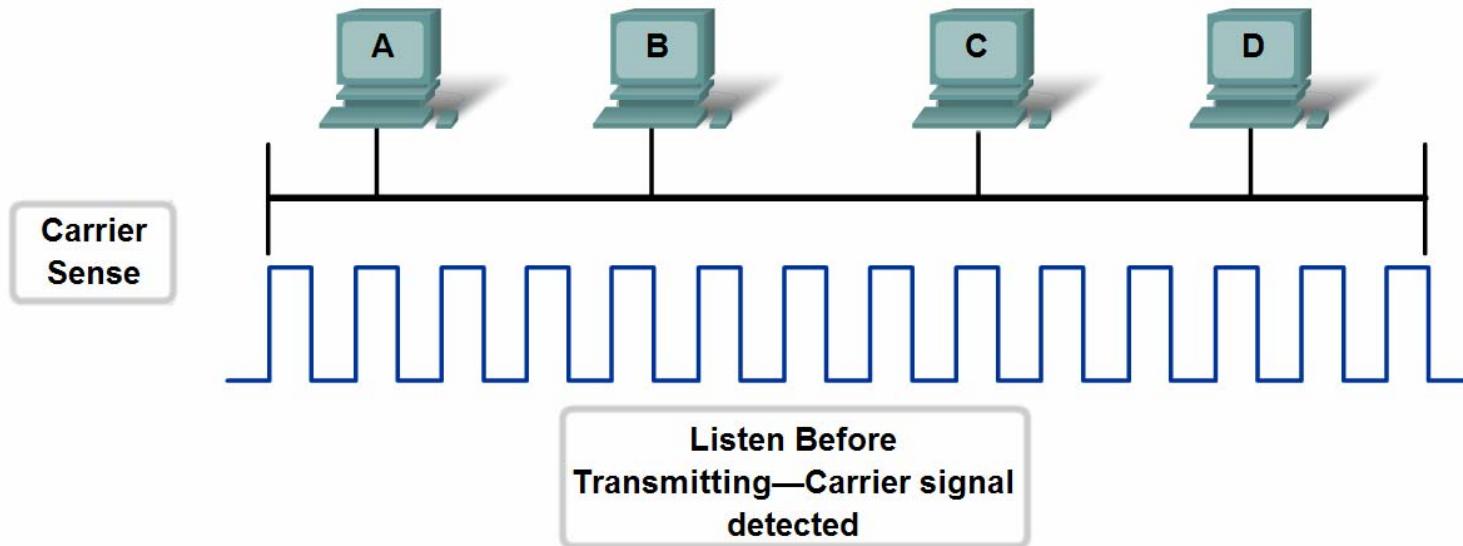
CSMA/CD controls access to the shared media. If there is a collision, it is detected and frames are retransmitted.

Function and Characteristics of the Media Access Control Method

- Carrier Sense Multiple Access with Collision Detection

Media Access Control in Ethernet

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

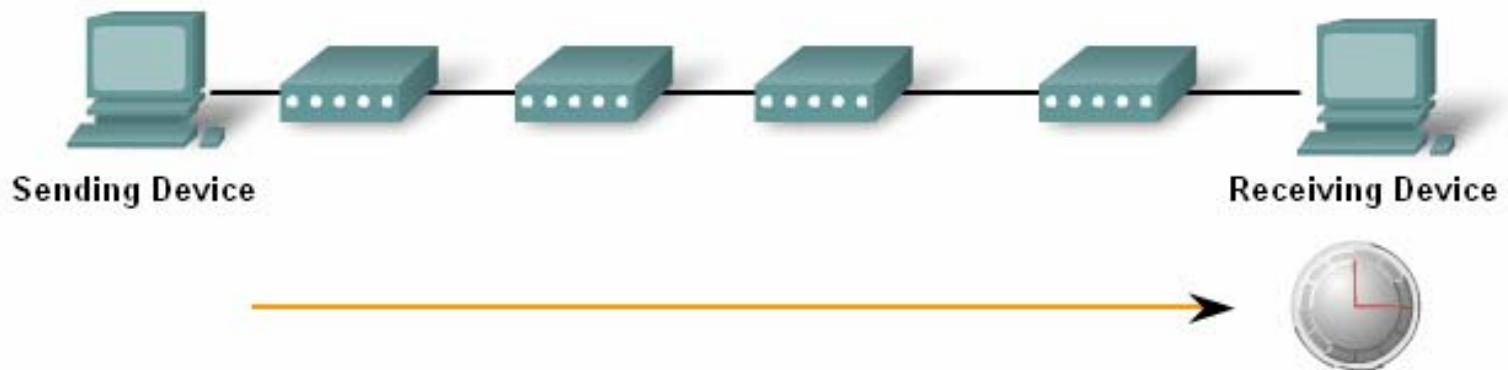


Ethernet concepts

- Delay (Latency)

- CSMA/CD
 - Signal travel time
 - Intermediary devices

Due to delay, collisions may occur



An Ethernet frame takes a measurable time to travel from the sending device to the receiver. Each intermediary device contributes to the overall latency.

Ethernet frame structure

- The Frame – Encapsulating the Packet

Comparison of 802.3 and Ethernet Frame Structures and Field Size

IEEE 802.3							Field size in bytes
7	1	6	6	2	46 to 1500	4	
Preamble	Start of Frame delimiter	Destination Address	Source Address	Length/ Type	802.2 Header and Data	Frame Check Sequence	
Ethernet							
8	6	6	2	46 to 1500	4		
Preamble	Destination Address	Source Address	Type	Data	Frame Check Sequence		



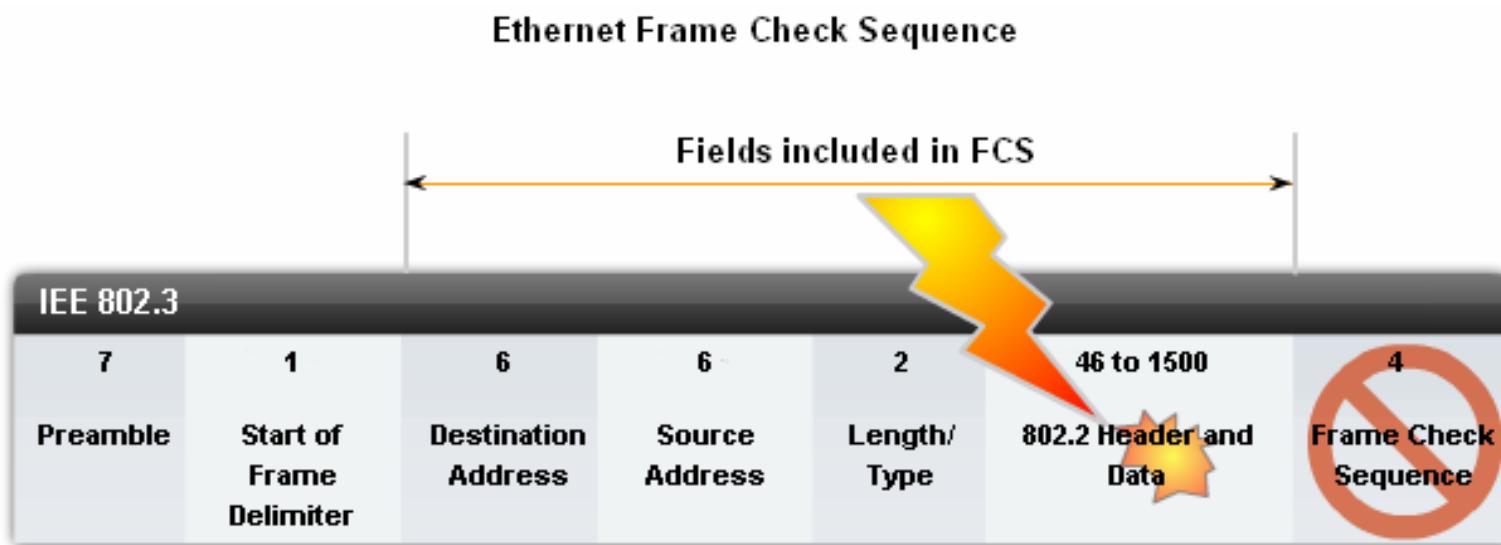
Ethernet frame structure

- The original Ethernet standard defined the minimum frame size as 64 bytes and the maximum as 1518 bytes. The Preamble and Start Frame Delimiter fields are not included when describing the size of a frame.
- The IEEE 802.3ac standard, released in 1998, extended the maximum allowable frame size to 1522 bytes to support VLAN technology
- If the size of a transmitted frame is less than the minimum or greater than the maximum, the receiving device drops the frame.



Layer 2 frame and its Impact on Network Operation and Performance

- Error detection



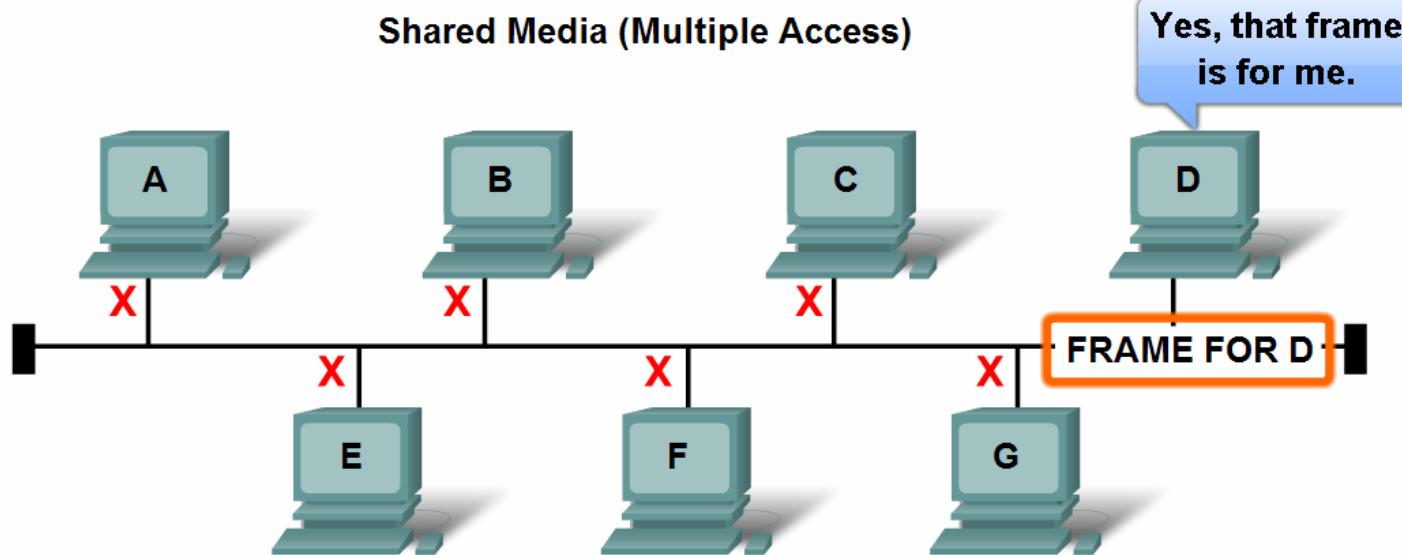
If the FCS calculated by the receiver (based on the contents of the received frame), does not equal the FCS calculated by the source (which is included in the frame), the frame is considered invalid and is dropped.

Layer 2 addressing and its Impact on Network Operation and Performance

- The Ethernet MAC Address

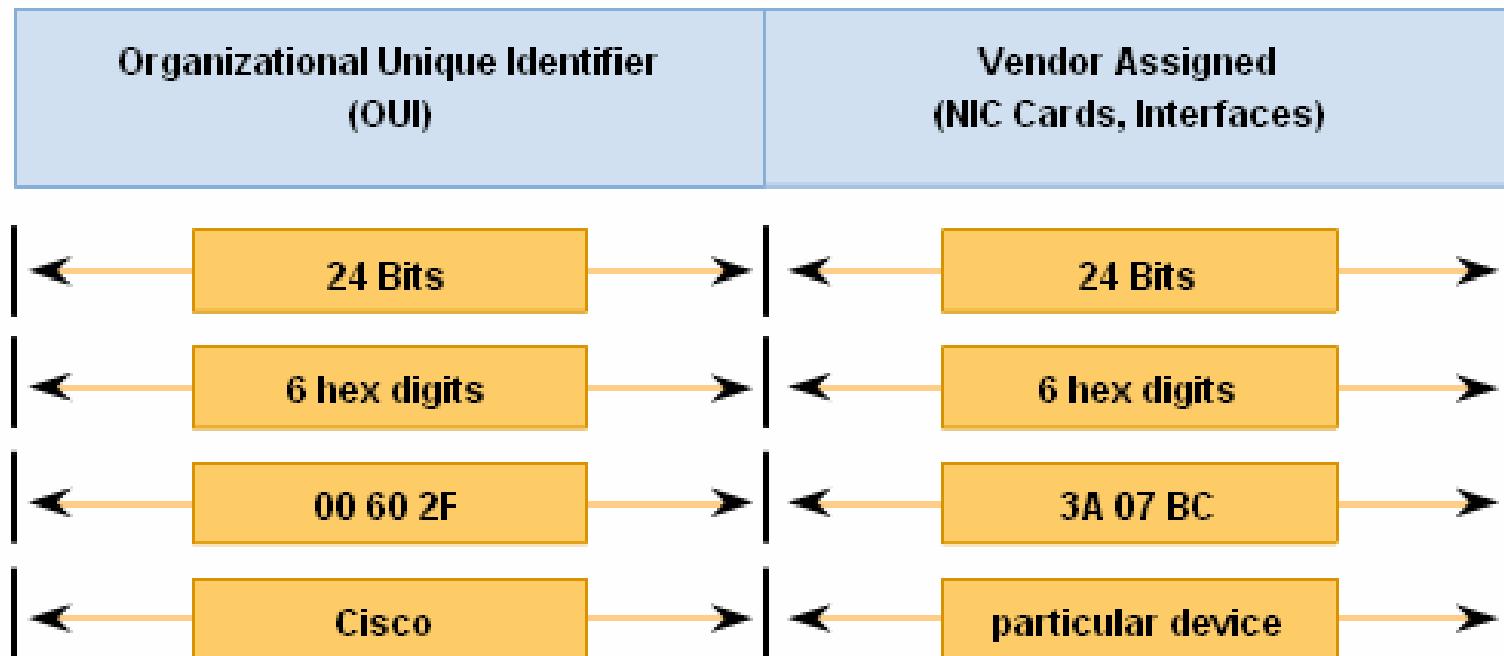
The MAC Address—Addressing in Ethernet

All Ethernet nodes share the media.
To receive the data sent to it, each node needs a unique address.



Layer 2 addressing and its Impact on Network Operation and Performance

- The Ethernet MAC Address Structure



Different representations of MAC Addresses

00-60-2F-3A-07-BC
00:60:2F:3A:07:BC
0060.2F3A.07BC

Layer 2 addressing and its Impact on Network Operation and Performance

■ Hexadecimal Numbering and Addressing

Hexadecimal Numbering

Decimal and Binary equivalents of 0 to F Hexadecimal			Selected Decimal, Binary and Hexadecimal equivalents		
Decimal	Binary	Hexadecimal	Decimal	Binary	Hexadecimal
0	0000	0	0	0000 0000	00
1	0001	1	1	0000 0001	01
2	0010	2	2	0000 0010	02
3	0011	3	3	0000 0011	03
4	0100	4	4	0000 0100	04
5	0101	5	5	0000 0101	05
6	0110	6	6	0000 0110	06
7	0111	7	7	0000 0111	07
8	1000	8	8	0000 1000	08
9	1001	9	10	0000 1010	0A
10	1010	A	15	0000 1111	0F
11	1011	B	16	0001 0000	10
12	1100	C	32	0010 0000	20
13	1101	D	64	0100 0000	40
14	1110	E	128	1000 0000	80
15	1111	F	192	1100 0000	C0
			202	1100 1010	CA
			240	1111 0000	F0
			255	1111 1111	FF

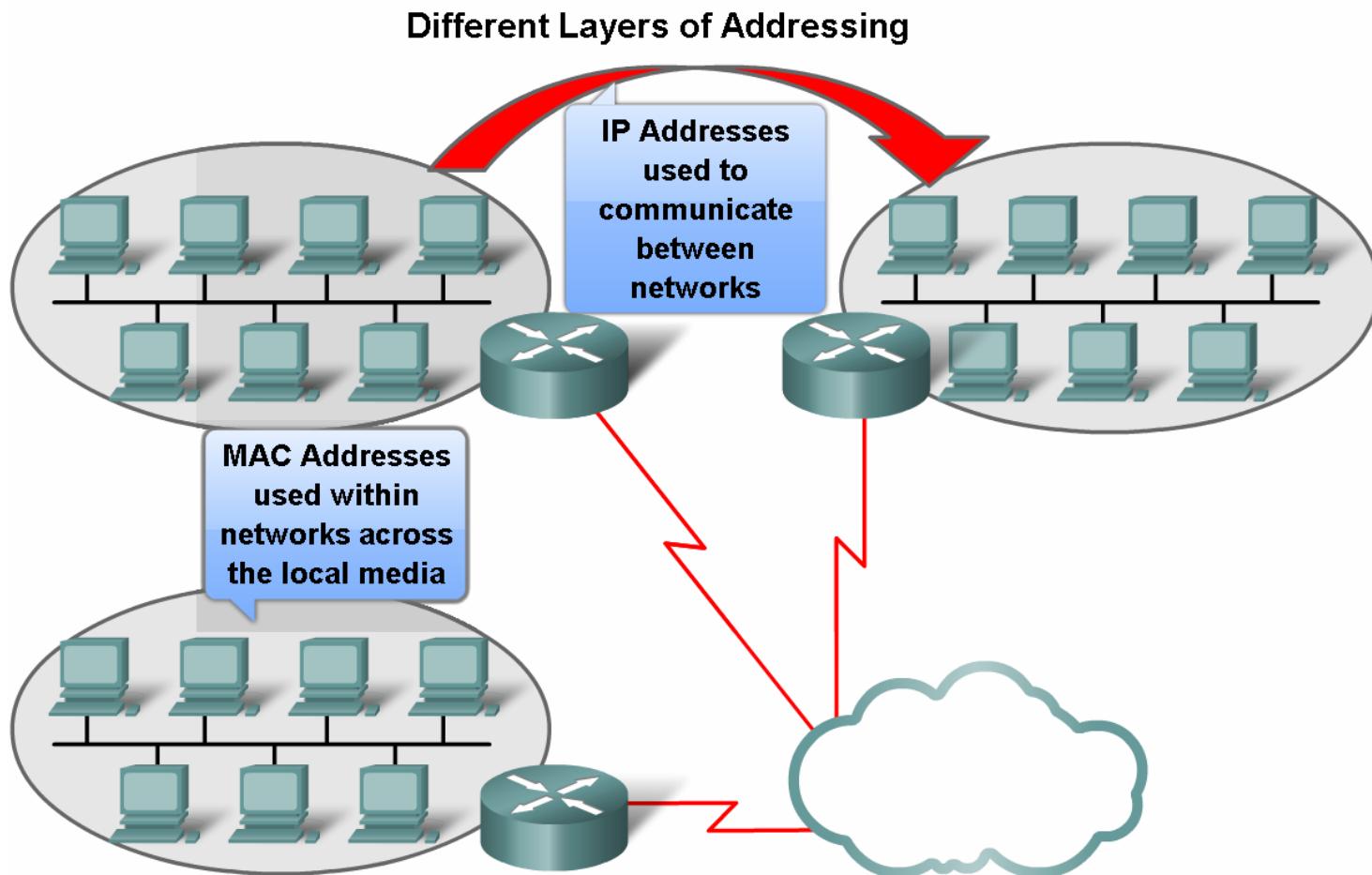
Layer 2 addressing and its Impact on Network Operation and Performance

Viewing the MAC Address

```
C:\>ipconfig /all
Ethernet adapter Network Connection:
  Connection-specific DNS Suffix: example.com
  Description . . . . . : Intel(R) PRO/Wireless 3945ABG Network
Connection
  Physical Address. . . . . : 00-18-DE-C7-F3-FB
  Dhcp Enabled. . . . . : Yes
  Autoconfiguration Enabled . . . . : Yes
  IP Address. . . . . : 10.2.3.4
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 10.2.3.254
  DHCP Server . . . . . : 10.2.3.69
  DNS Servers . . . . . : 192.168.226.120
  Lease Obtained. . . . . : Thursday, May 03, 2007 3:47:51 PM
  Lease Expires . . . . . : Friday, May 04, 2007 6:57:11 AM
C:\>
```

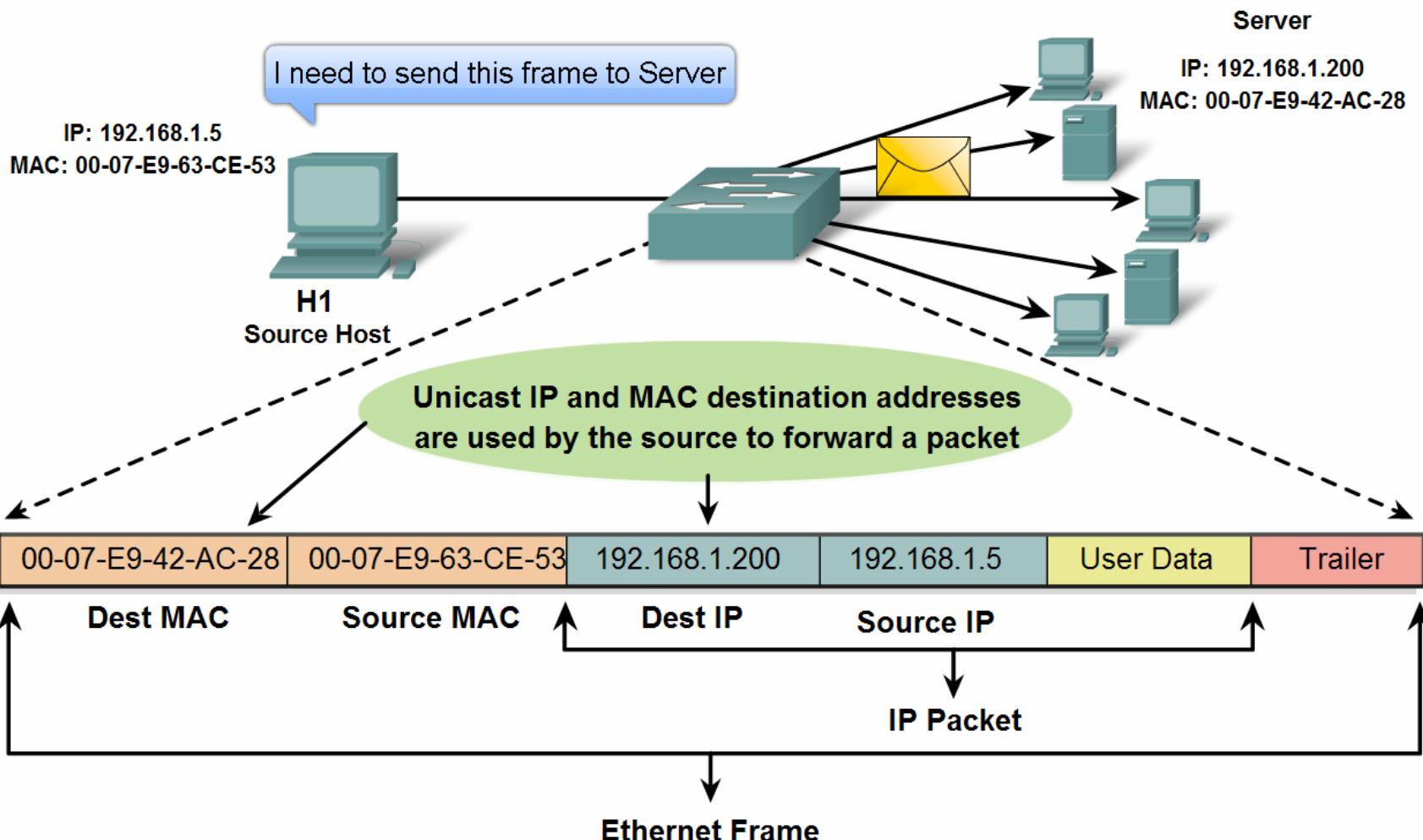
Layer 2 addressing and its Impact on Network Operation and Performance

- Another Layer of Addressing



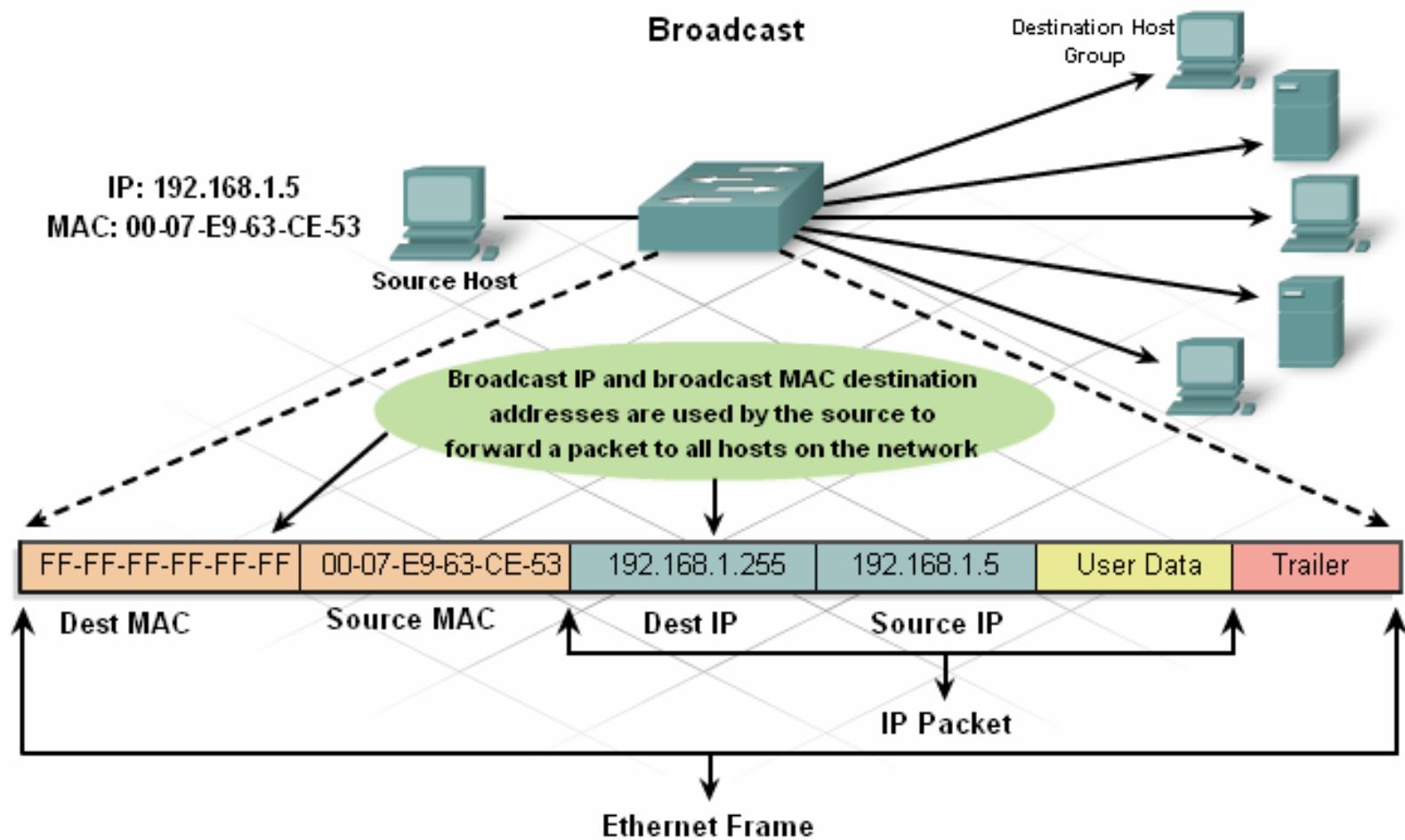
Layer 2 addressing and its Impact on Network Operation and Performance

Ethernet Unicast



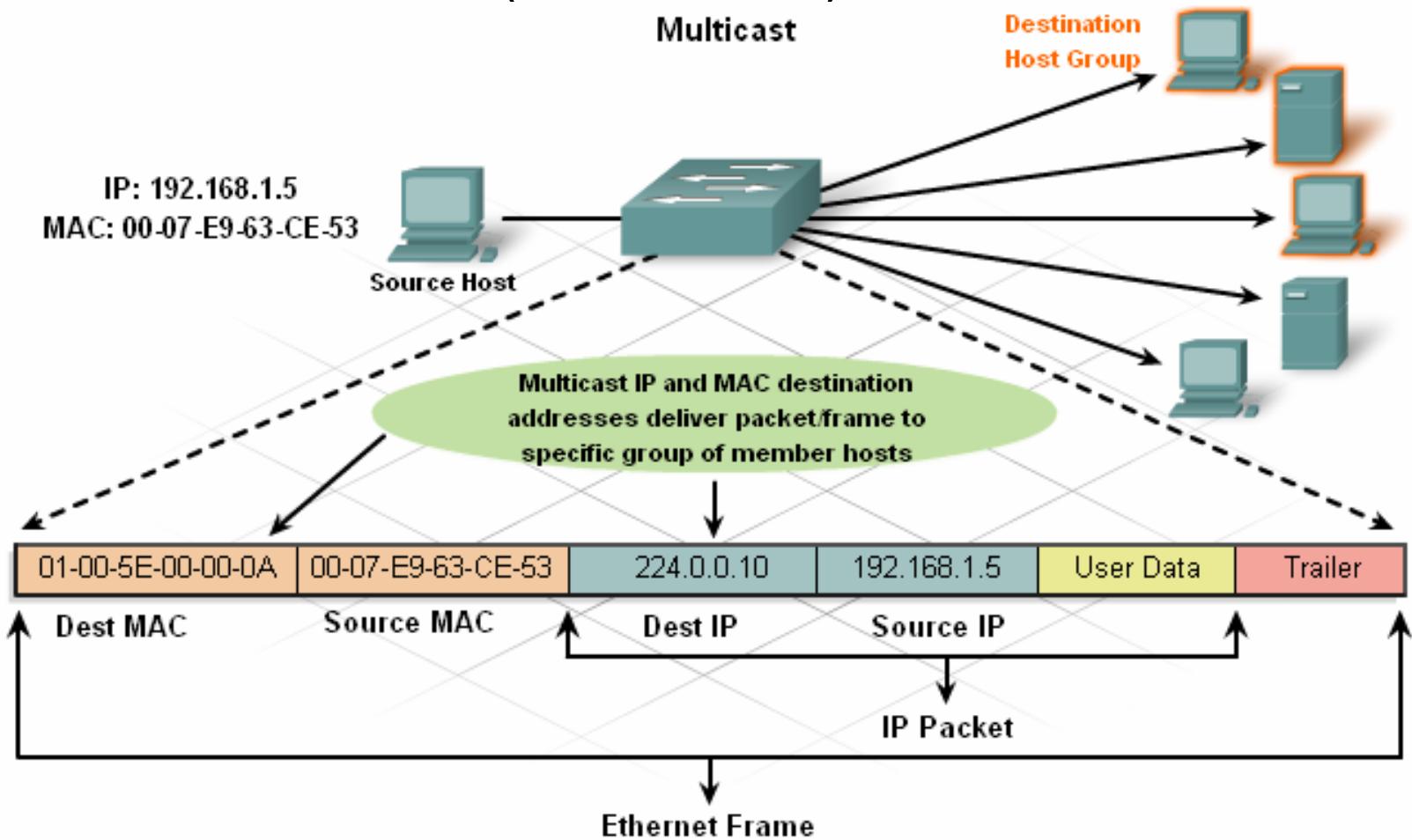
Layer 2 addressing and its Impact on Network Operation and Performance

Ethernet Broadcast



Layer 2 addressing and its Impact on Network Operation and Performance

- Ethernet Multicast (01-00-5E....)



Ethernet concepts

■ Frame synchronization

- Needed for asynchronous communication (10 Mbps and slower)
- Preamble and SFD kept for compatibility in faster, synchronous communication (>100Mbps)

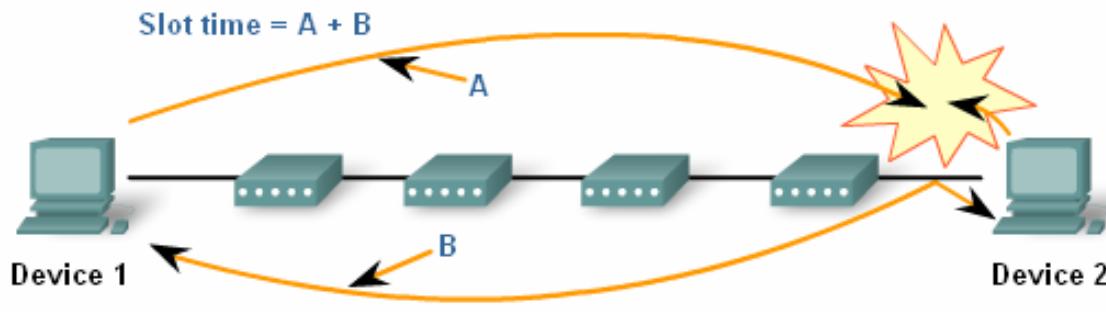
Field Names				
A	B	C	D	E
Start Frame Field	Address Field	Type/Length Field	Data Field	FCS Field



10 Mbps and slower Ethernet use the first 64 bits of the frame Preamble to synchronize the receiver.

Ethernet concepts

- Slot and Bit Times



Speed	Slot Time	Time Interval
10 Mbps	512 bit time	51.2 μ s
100 Mbps	512 bit time	5.12 μ s
1 Gbps	4096 bit time	4.096 μ s
10 Gbps	not applicable	not applicable

Ethernet Speed	Bit time
10 Mbps	100 ns
100 Mbps	10 ns
1000 Mbps = 1 Gbps	1 ns
10,000 Mbps = 10 Gbps	.1 ns

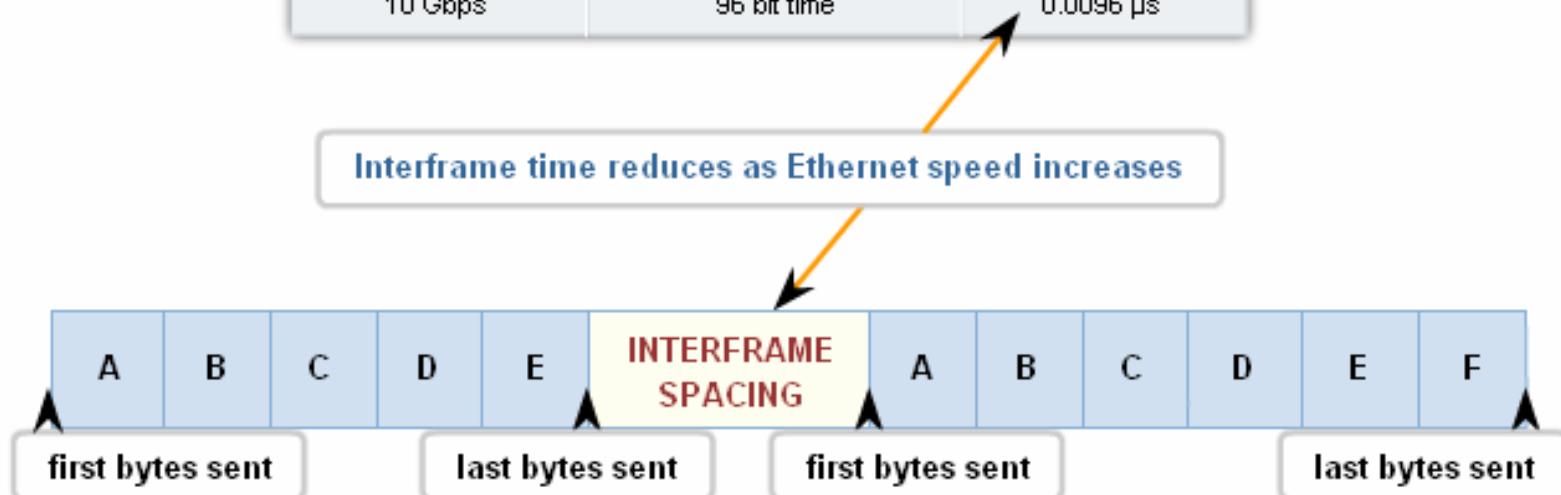
Ethernet concepts

■ Interframe Spacing

- a minimum spacing between two non-colliding frames

Speed	Interframe Spacing	Time Required
10 Mbps	96 bit time	9.6 μ s
100 Mbps	96 bit time	0.96 μ s
1 Gbps	96 bit time	0.096 μ s
10 Gbps	96 bit time	0.0096 μ s

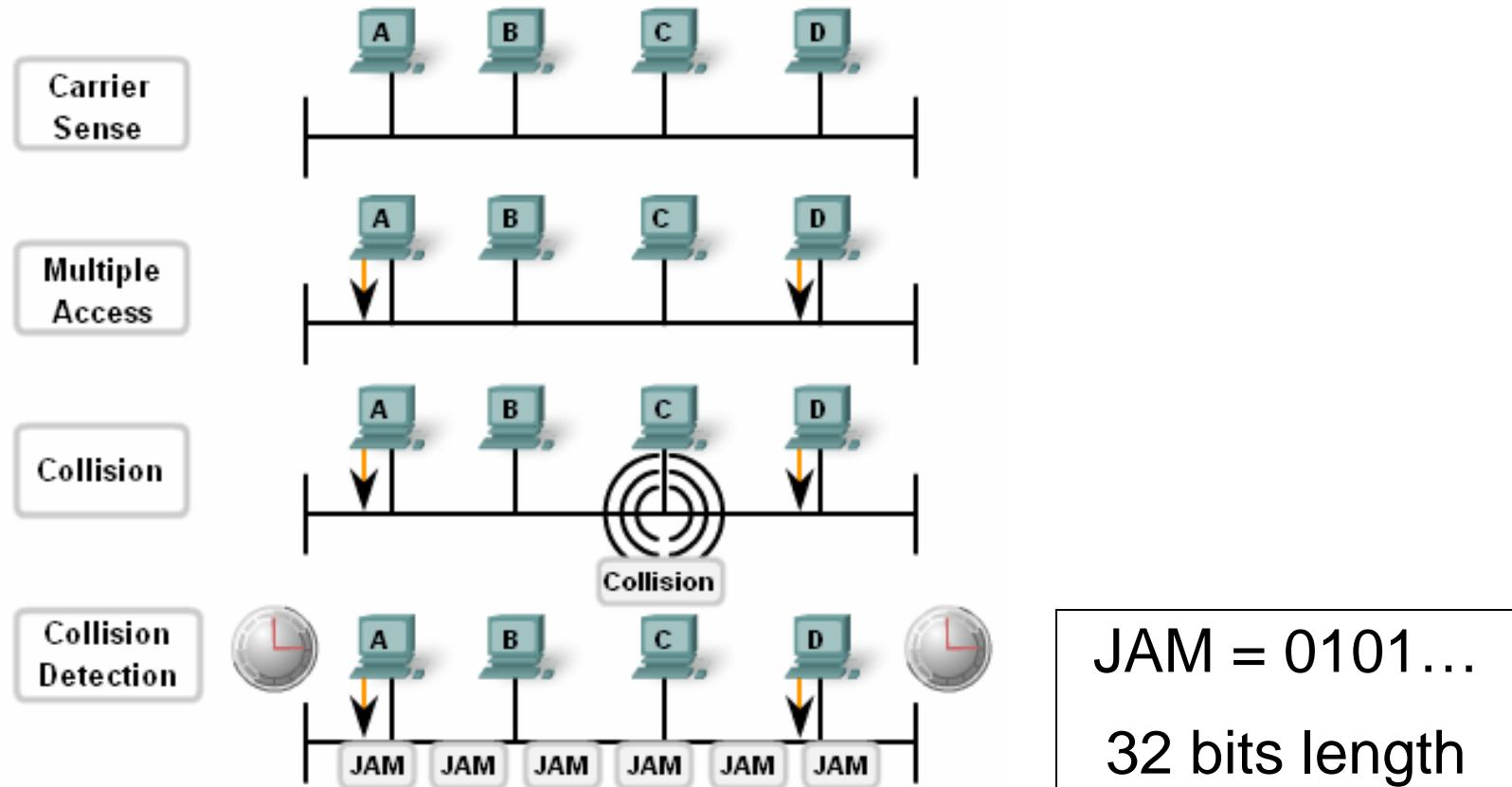
Interframe time reduces as Ethernet speed increases



Ethernet concepts

- Collision detection and handling

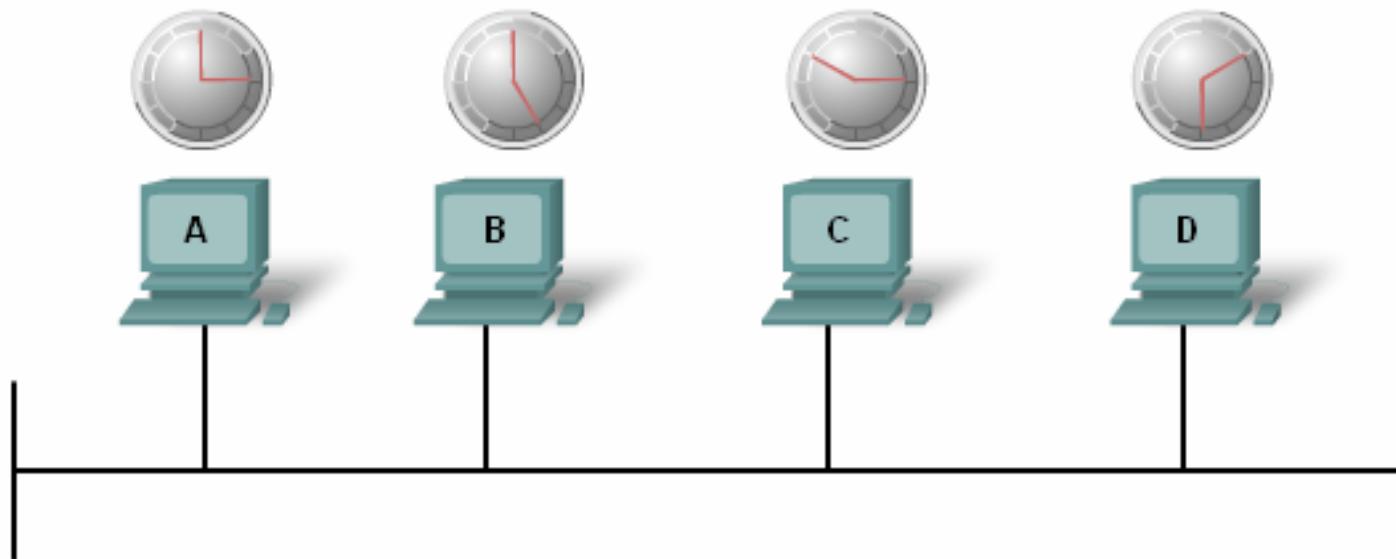
Stations detecting a collision send a jam signal.



Ethernet concepts

- Collision detection and handling

Backoff Timing



After a Jam signal is received, all stations cease transmission and each waits a random time period—set by the back off timer—before trying to send another frame.

Ethernet standards

Types of Ethernet

Ethernet Type	Bandwidth	Cable Type	Duplex	Maximum Distance
10Base-5	10 Mbps	Thicknet Coaxial	Half	500 m
10Base-2	10 Mbps	Thinnet Coaxial	Half	185 m
10Base-T	10 Mbps	Cat3/Cat5 UTP	Half	100 m
100Base-TX	100 Mbps	Cat5 UTP	Half	100 m
100Base-TX	200 Mbps	Cat5 UTP	Full	100 m
100Base-FX	100 Mbps	Multimode Fiber	Half	400 m
100Base-FX	200 Mbps	Multimode Fiber	Full	2 km
1000Base-T	1 Gbps	Cat5e UTP	Full	100 m
1000Base-TX	1 Gbps	Cat6 UTP	Full	100 m
1000Base-SX	1 Gbps	Multimode Fiber	Full	550 m
1000Base-LX	1 Gbps	Single-Mode Fiber	Full	2 km
10GBase-CX4	10 Gbps	Twin-axial	Full	100 m
10GBase-T	10 Gbps	Cat6a/Cat7 UTP	Full	100 m
10GBase-LX4	10 Gbps	Multimode Fiber	Full	300 m
10GBase-LX4	10 Gbps	Single-Mode Fiber	Full	10 km

Ethernet RJ45 connector

10Base-T Ethernet RJ45 Pinouts

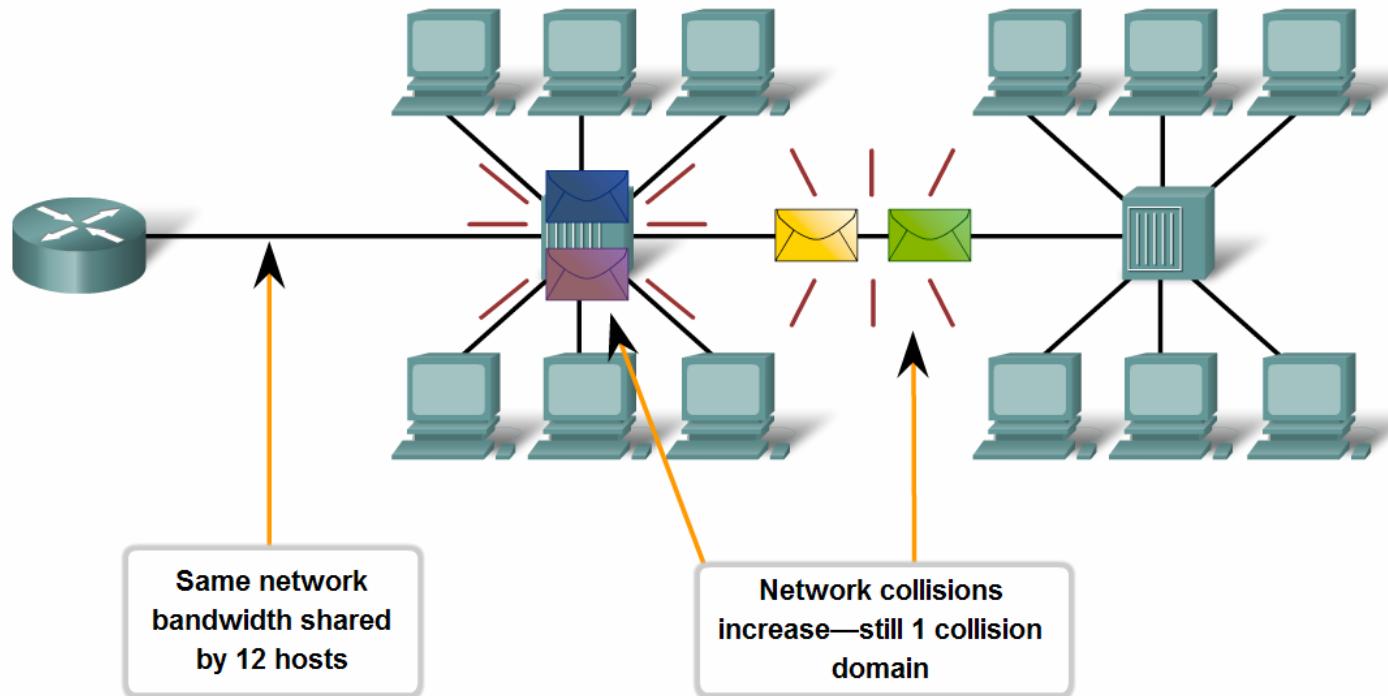


Pin Number	Signal
1	TD+ (Transmit Data, positive-going differential signal)
2	TD- (Transmit Data, negative-going differential signal)
3	RD+ (Receive Data, positive-going differential signal)
4	Unused
5	Unused
6	RD- (Receive Data, negative-going differential signal)
7	Unused
8	Unused

Compare and Contrast the Use of Ethernet Switches versus Hubs in a LAN.

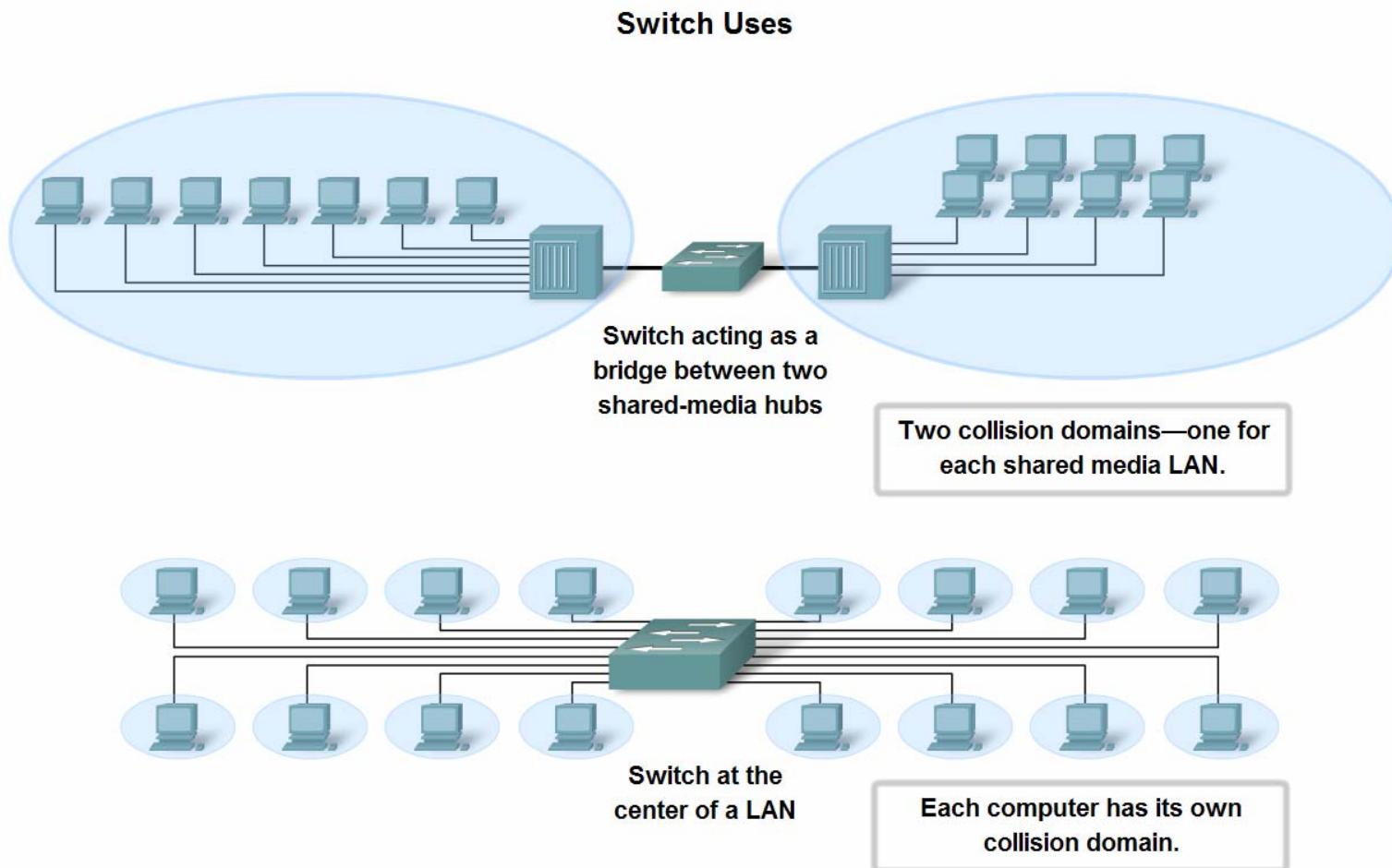
- Legacy Ethernet – Using Hubs

Poor Performance of Hub-based LANs



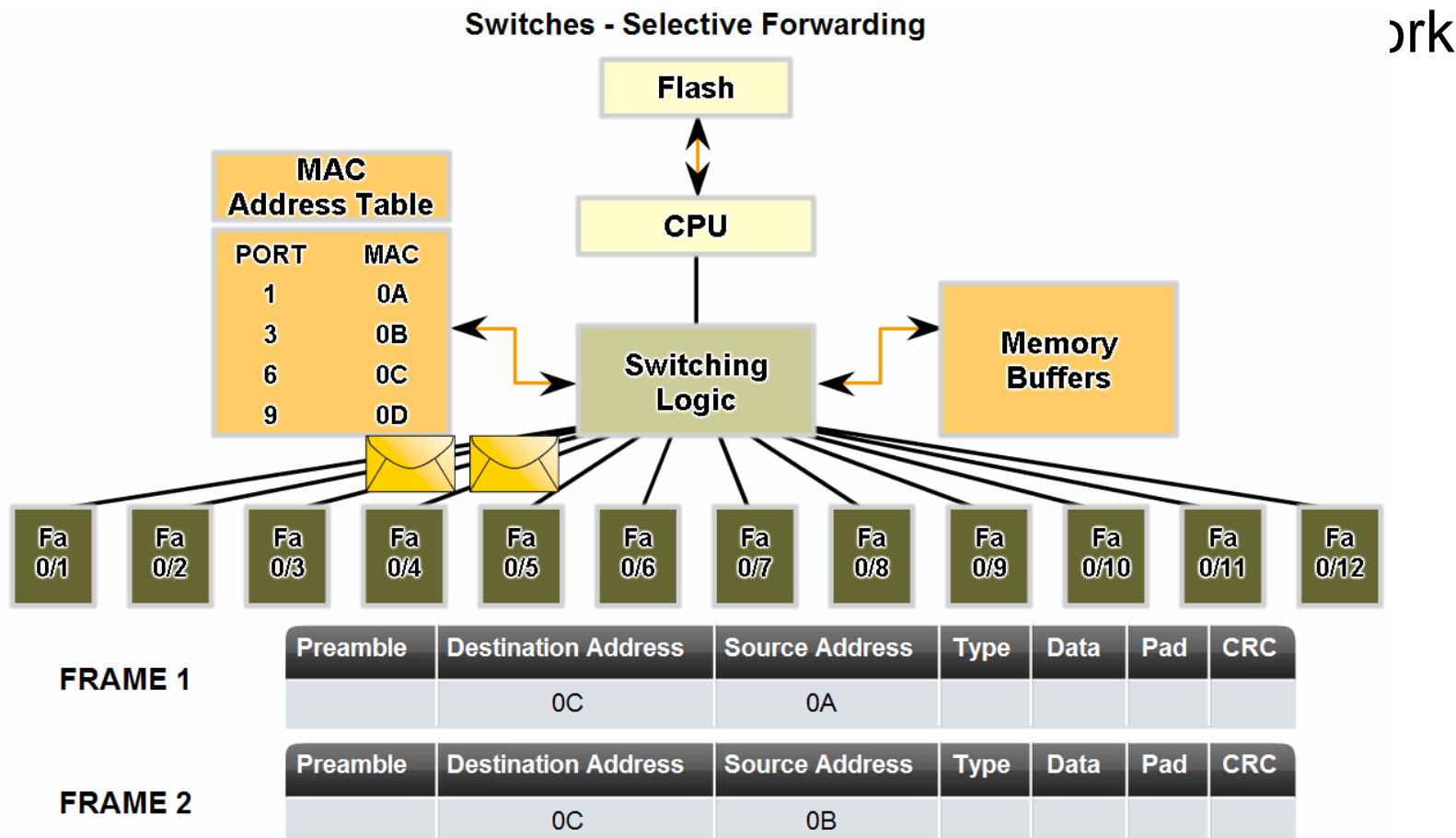
Compare and Contrast the Use of Ethernet Switches versus Hubs in a LAN.

- Ethernet – Using Switches



Compare and Contrast the Use of Ethernet Switches versus Hubs in a LAN.

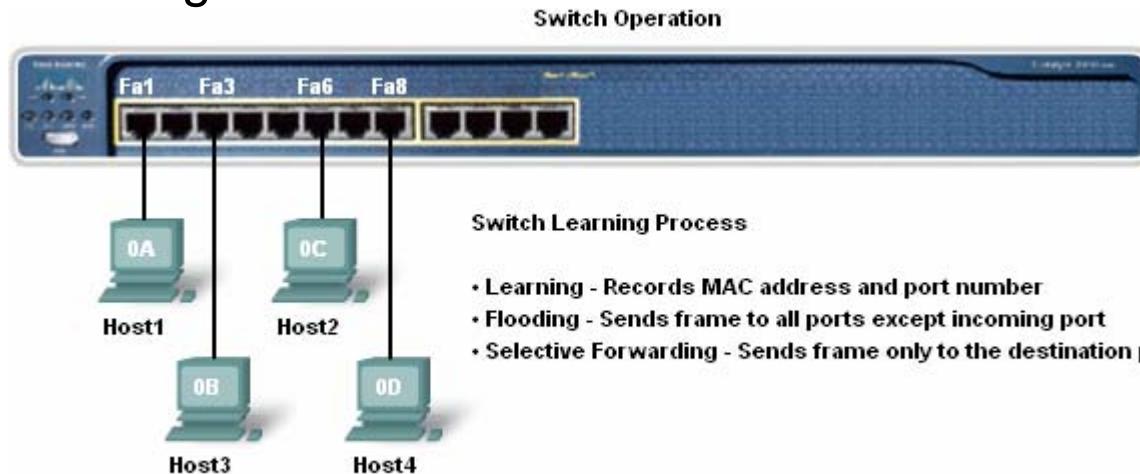
- Describe how a switch can eliminate collisions, backoffs and re-transmissions, the leading factors in



Switch Operation

- To accomplish their purpose, Ethernet LAN switches use five basic operations:

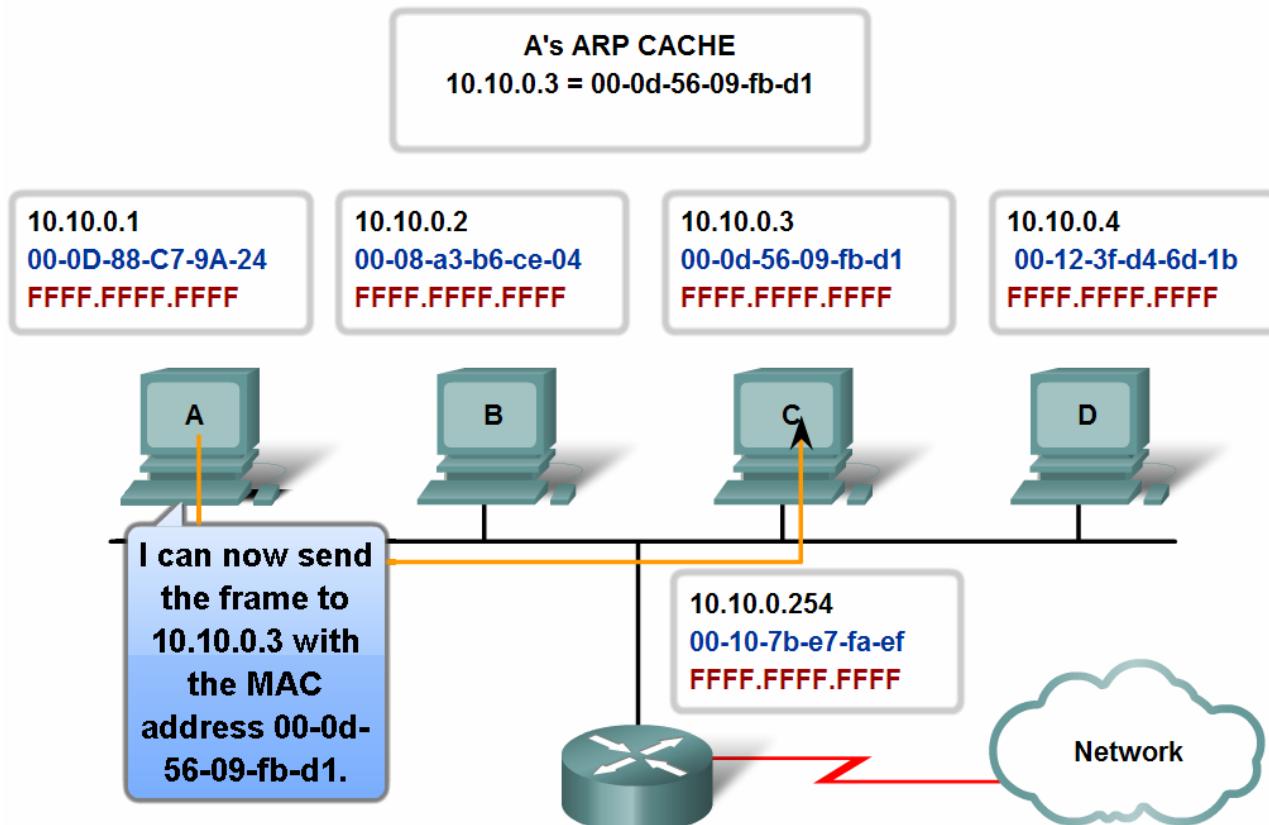
- Learning
- Aging
- Flooding
- Selective Forwarding
- Filtering



Explain the Address Resolution Protocol (ARP) process.

- Mapping IP to MAC Addresses

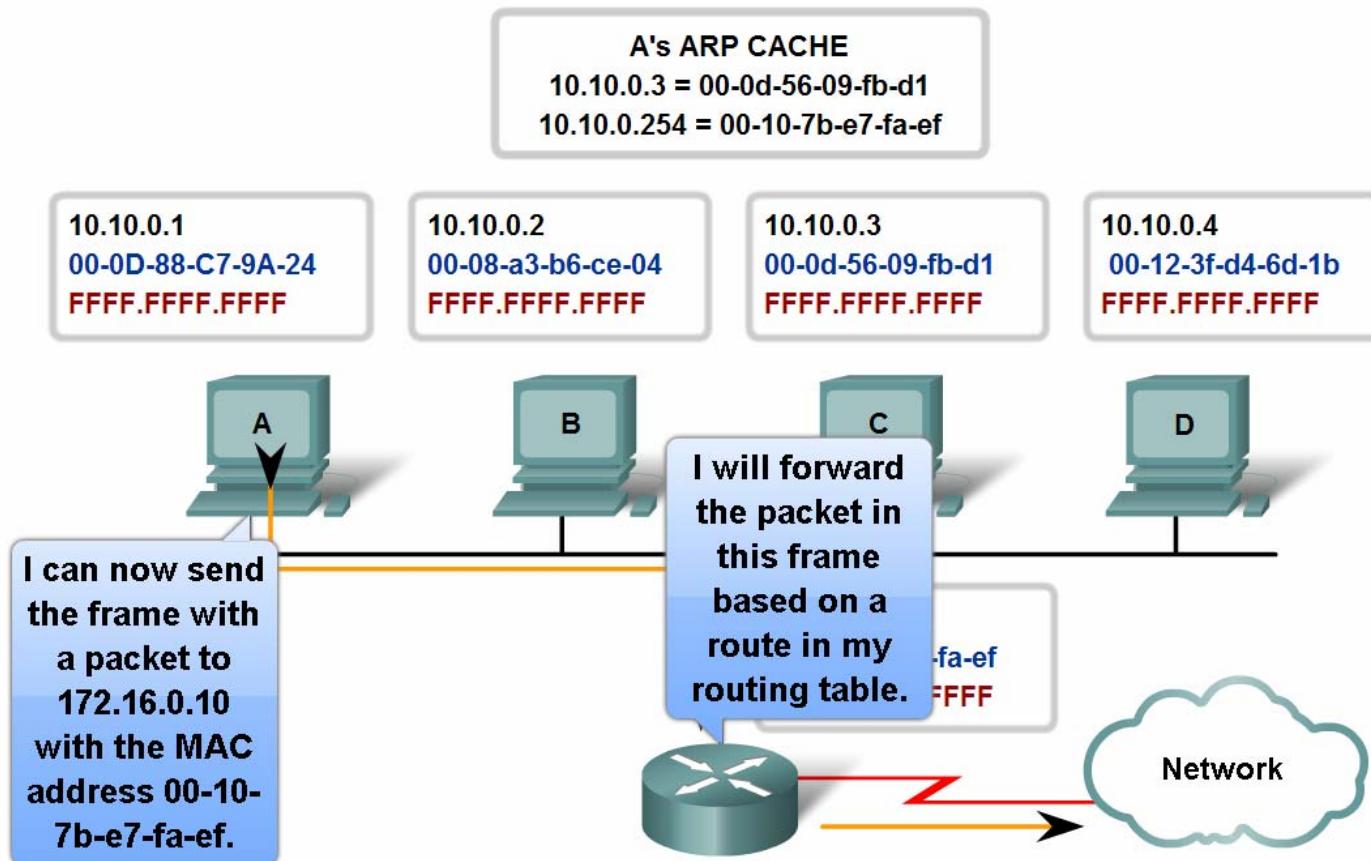
The ARP Process—ARP Entry Enables Frame to be Sent



Explain the Address Resolution Protocol (ARP) process.

- ARP – Destinations Outside the Local Network

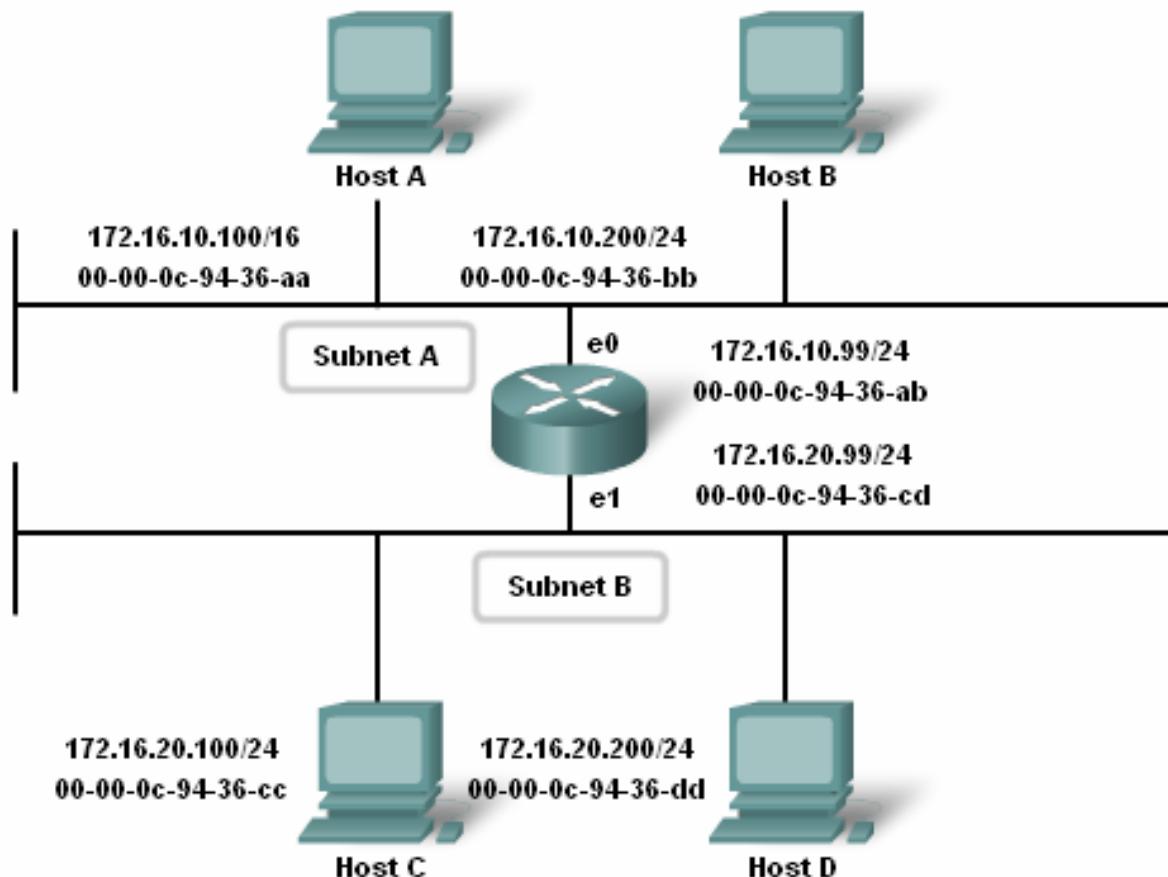
The ARP Process—ARP Entry Enables Frame to be Sent



Explain the Address Resolution Protocol (ARP) process.

- Proxy ARP

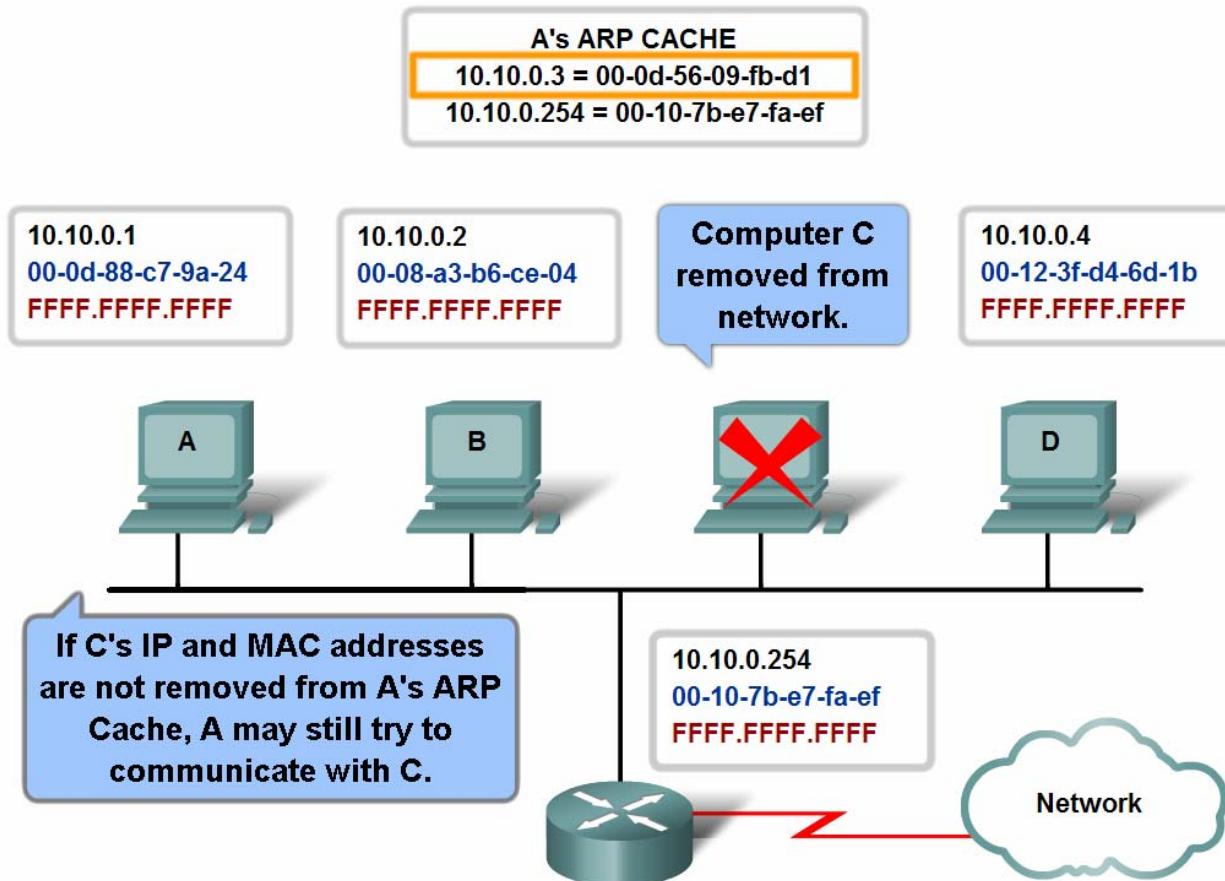
Proxy ARP Allows Router to Respond for Remote Host



Explain the Address Resolution Protocol (ARP) process.

- ARP – Removing Address Mappings

The ARP Process - Removing Address Mappings

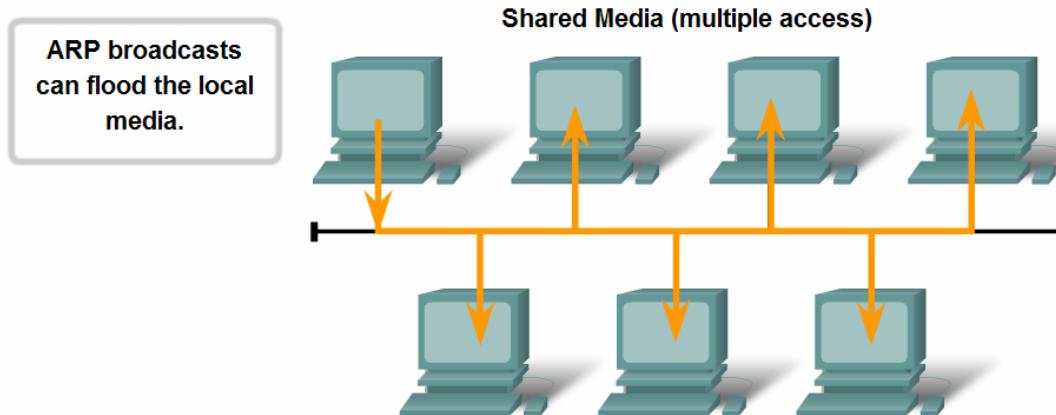


Explain the Address Resolution Protocol (ARP) process.

■ ARP Broadcasts - Issues

ARP Issues:

- Broadcasts, overhead on the Media
- Security



A false ARP message can provide an incorrect MAC address that will then hijack frames using that address (called a spoof).

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

Summary

In this chapter, you learned to:

- Identify the basic characteristics of network media used in Ethernet.
- Describe the Physical and Data Link layer features of Ethernet.
- Describe the function and characteristics of the media access control method used by Ethernet protocol.
- Explain the importance of Layer 2 addressing used for data transmission and determine how the different types of addressing impacts network operation and performance.
- Compare and contrast the application and benefits of using Ethernet switches in a LAN as opposed to using hubs.
- Explain the ARP process.





Planning and Cabling Networks



Network Fundamentals – Chapter 10

Cisco | Networking Academy®
Mind Wide Open™

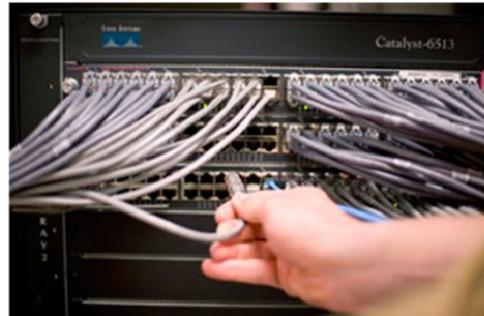
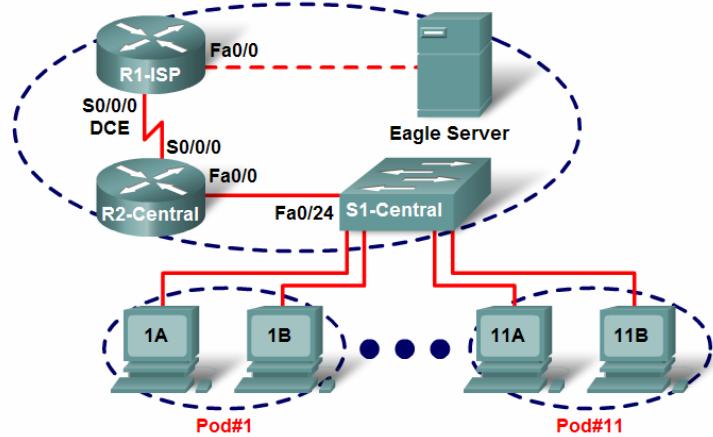


Objectives

- Identify the basic network media required to make a LAN connection.
- Identify the types of connections for intermediate and end device connections in a LAN.
 - Identify the pin out configurations for straight-through and crossover cables.
 - Identify the different cabling types, standards and ports used for WAN connections.
 - Define the role of device management connections when using Cisco equipment.
- Design an addressing scheme for an inter-network and assign ranges for hosts, network devices and the router interface.
- Compare and contrast the importance of network designs

Basic Network Media Required to Make a LAN Connection.

- Select the appropriate hardware, including the cabling, to install several computers together in a LAN



Planning & Cabling a Network

Basic Network Media Required to Make a LAN Connection.

- To identify some key aspects of the devices they will be employing in a LAN

Factors to Consider in Choosing a Device



COST



POTS



SPEED



EXPANDABLE/ MODULAR

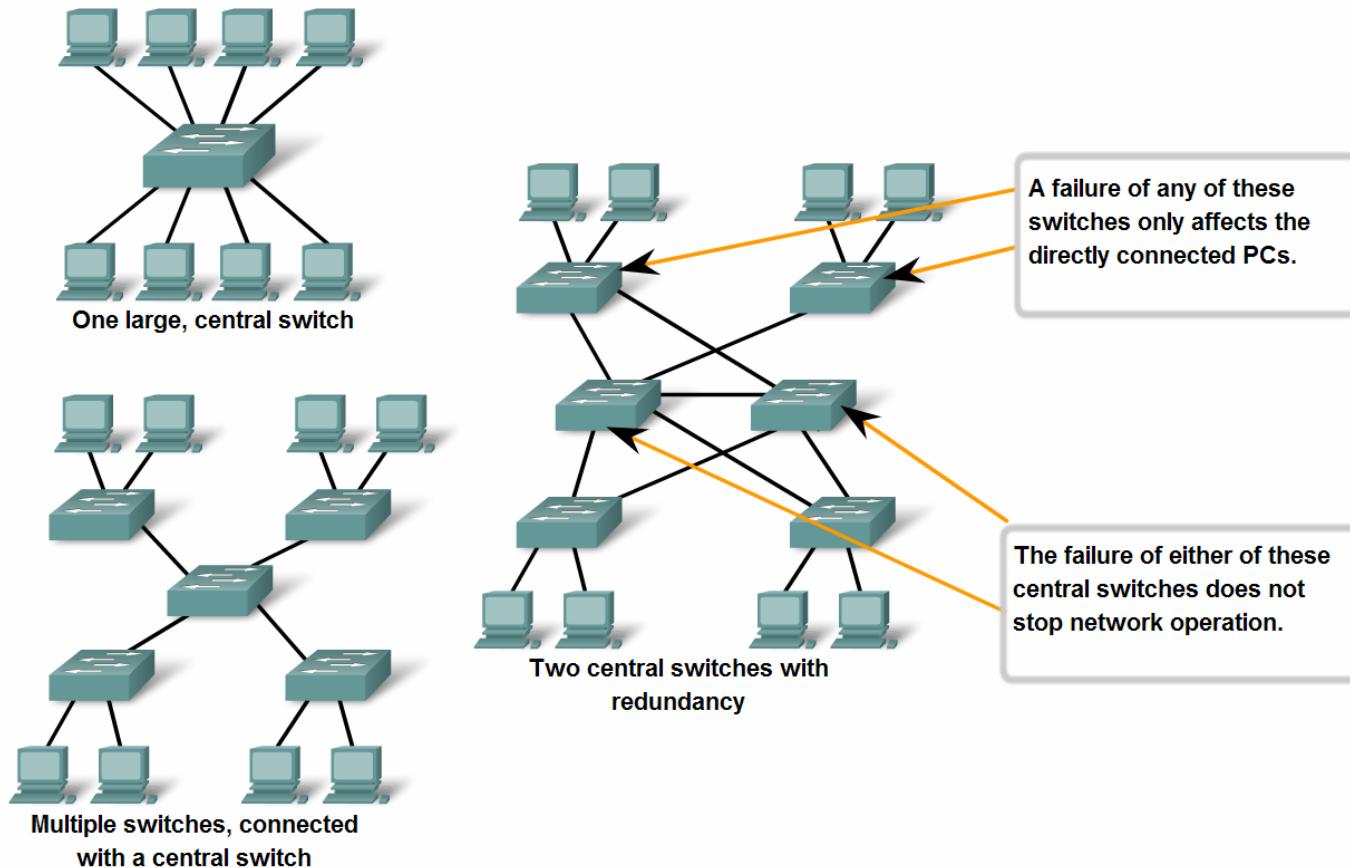


MANAGEABLE

Basic Network Media Required to Make a LAN Connection.

- Connect two computers with a switch

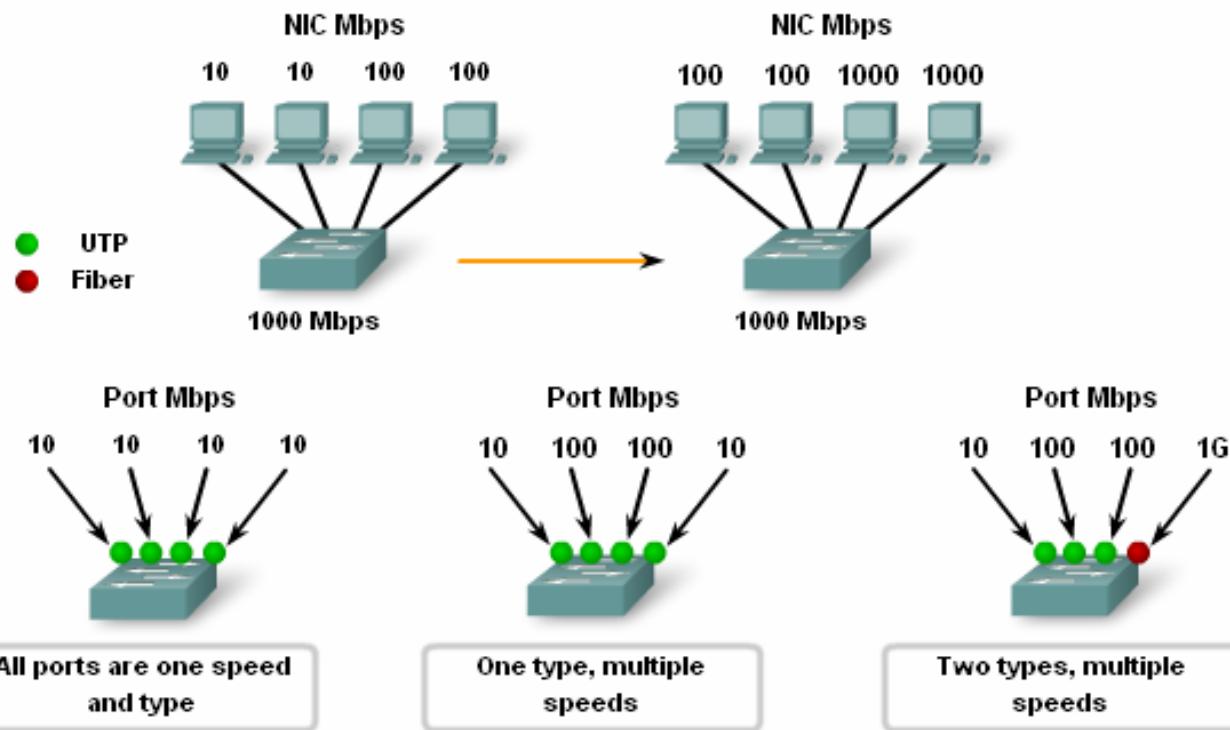
Factors Determining LAN Switch Selection



Types of Connections in a LAN

■ Factors Determining LAN Switch Selection

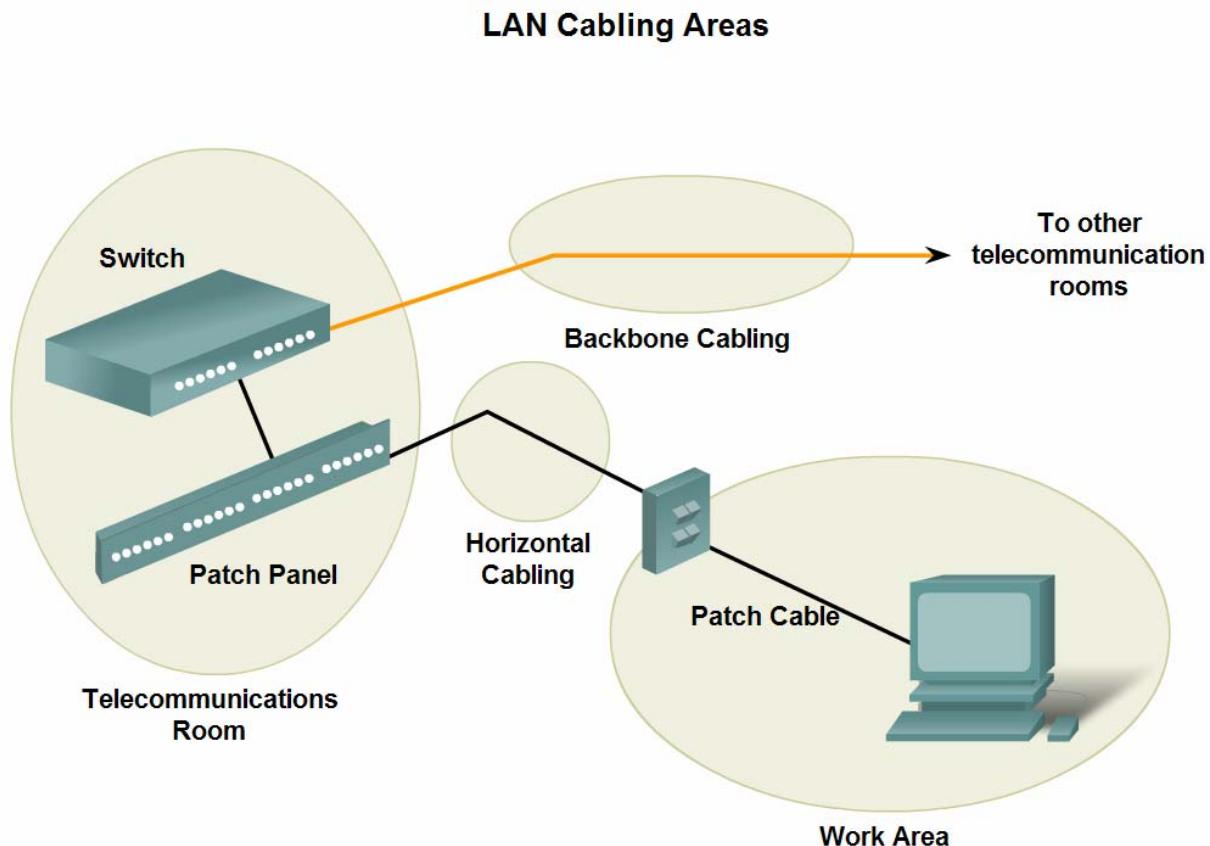
Port Speeds, Types and Expandability



Some switches can be expanded to meet new requirements with additional modules.

Types of Connections in a LAN

- Given a specific network connection, identify the type of cable required to make the connection

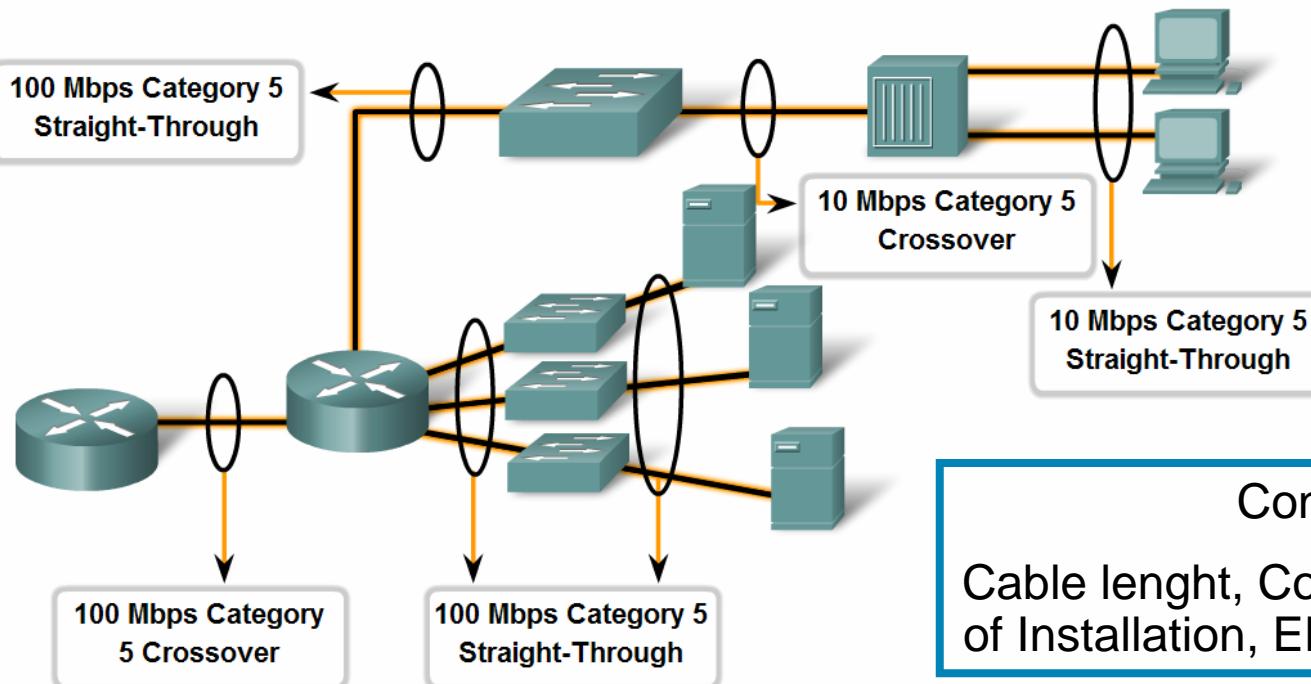


Types of Connections in a LAN

- Identify the correct cable to use in connecting intermediate and end devices in a LAN.

Making LAN Connections

Identify the correct UTP cable type and likely category to connect different intermediate and end devices in a LAN.



Consider:
Cable length, Cost, Bandwidth, Ease
of Installation, EMI/RFI interference

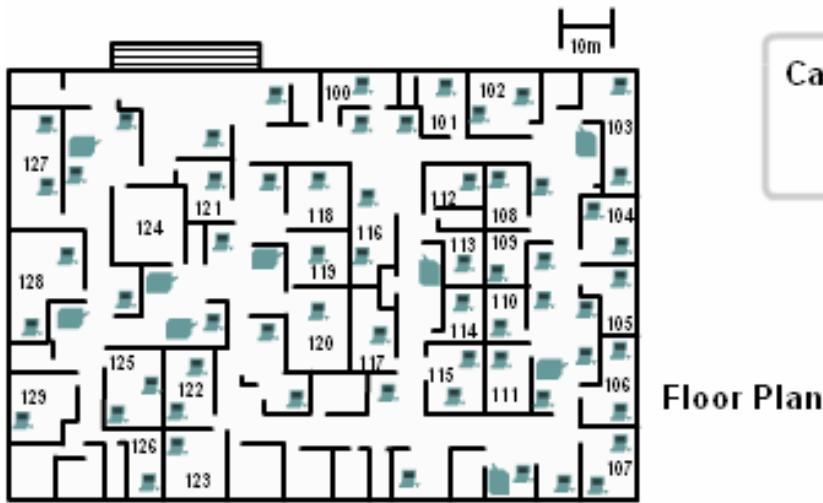


Types of Connections in a LAN

- Use straight-through cables for connecting:
 - Switch to router
 - Computer to switch
 - Computer to hub
- Use crossover cables for connecting:
 - Switch to switch
 - Switch to hub
 - Hub to hub
 - Router to router
 - Computer to computer
 - Computer to router
- MDIX (media-dependent interface, crossover)

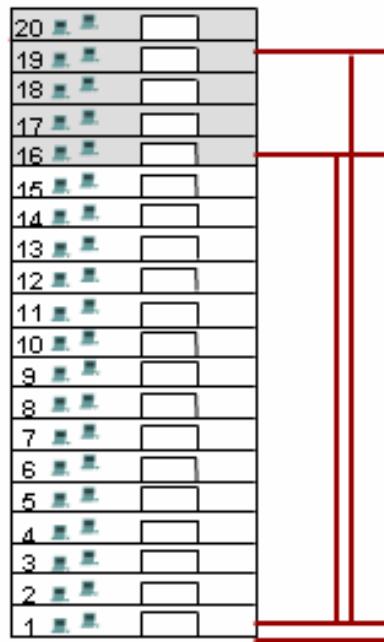
LAN design

- Calculate cable length and cost



Cable lengths need to be determined and matched with the technology used.

Multi-Floor Building



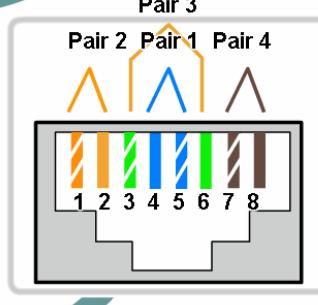
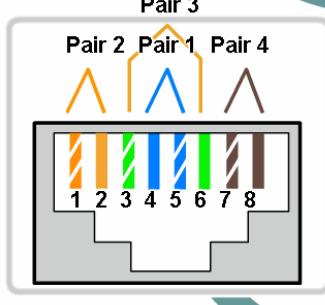
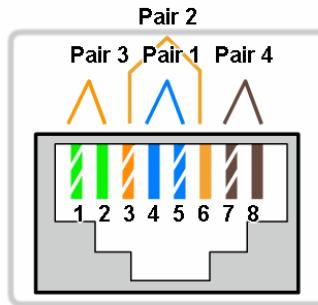
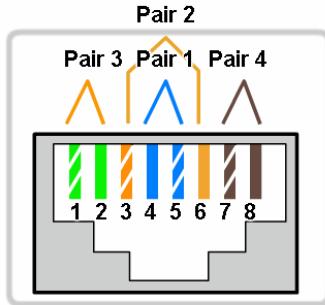
Ethernet Type	Bandwidth	Cable Type	Maximum Distance
10Base-T	10Mbps	Cat3/Cat5 UTP	100m
100Base-TX	100Mbps	Cat5 UTP	100m
100Base-TX	200Mbps	Cat5 UTP	100m
100Base-FX	100Mbps	Multi-Mode Fiber	400m
100Base-FX	200Mbps	Multi-Mode Fiber	2Km
1000Base-T	1Gbps	Cat5e UTP	100m
1000Base-TX	1Gbps	Cat6 UTP	100m

Types of Connections in a LAN

- Identify the pinout of the straight-through and cross-over cables

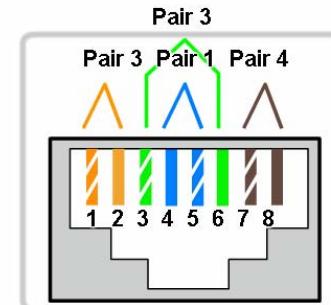
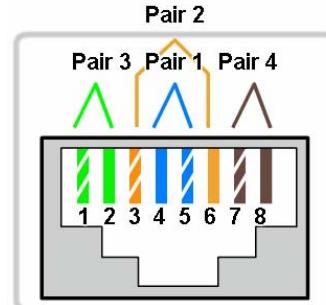
Straight-Through Cable

Straight-through cables have the same termination at each end - T568A or T568B.



Crossover Cable

Crossover cables have a T568A termination at one end and a T568B termination at the other end.



Pin Label	Pin Label
1 TD+	1 TD+
2 RD-	2 RD-
3 RD+	3 RD+
4 NC	4 NC
5 NC	5 NC
6 TD+	6 TD-
7 NC	7 NC
8 NC	8 NC

1 TP0+	1 TP0+
2 TP0-	2 TP0-
3 TP1+	3 TP1+
6 TP1-	6 TP1-
4 TP2+	4 TP2+
5 TP2-	5 TP2-
7 TP3+	7 TP3+
8 TP3-	8 TP3-

Transmit pins at each end connect to the receive pins at the other end.

Types of Connections in a WAN

- Different class of cables is used to connect WANs, and that the cables, standards and ports are different than those in use by LANs.

Types of WAN Connections

Cisco HDLC	PPP	Frame Relay	DSL Modem	Cable Modem
EIA/TIA-232 EIA/TIA-449 X.21V.24 V.35 High Speed Serial Interface (HSSI)	RJ-11 Note: Works over telephone line	F Note: Works over Cable TV line		



Router: Male Smart Serial



Network: Male Winchester Block Type

Types of Connections in a WAN

- **Data Communications Equipment (DCE)** - A device that supplies the clocking services to another device. Typically, this device is at the WAN access provider end of the link.
- **Data Circuit-Terminal Equipment (DTE)** - A device that receives clocking services from another device and adjusts accordingly. Typically, this device is at the WAN customer or user end of the link.



Data Terminal Equipment:

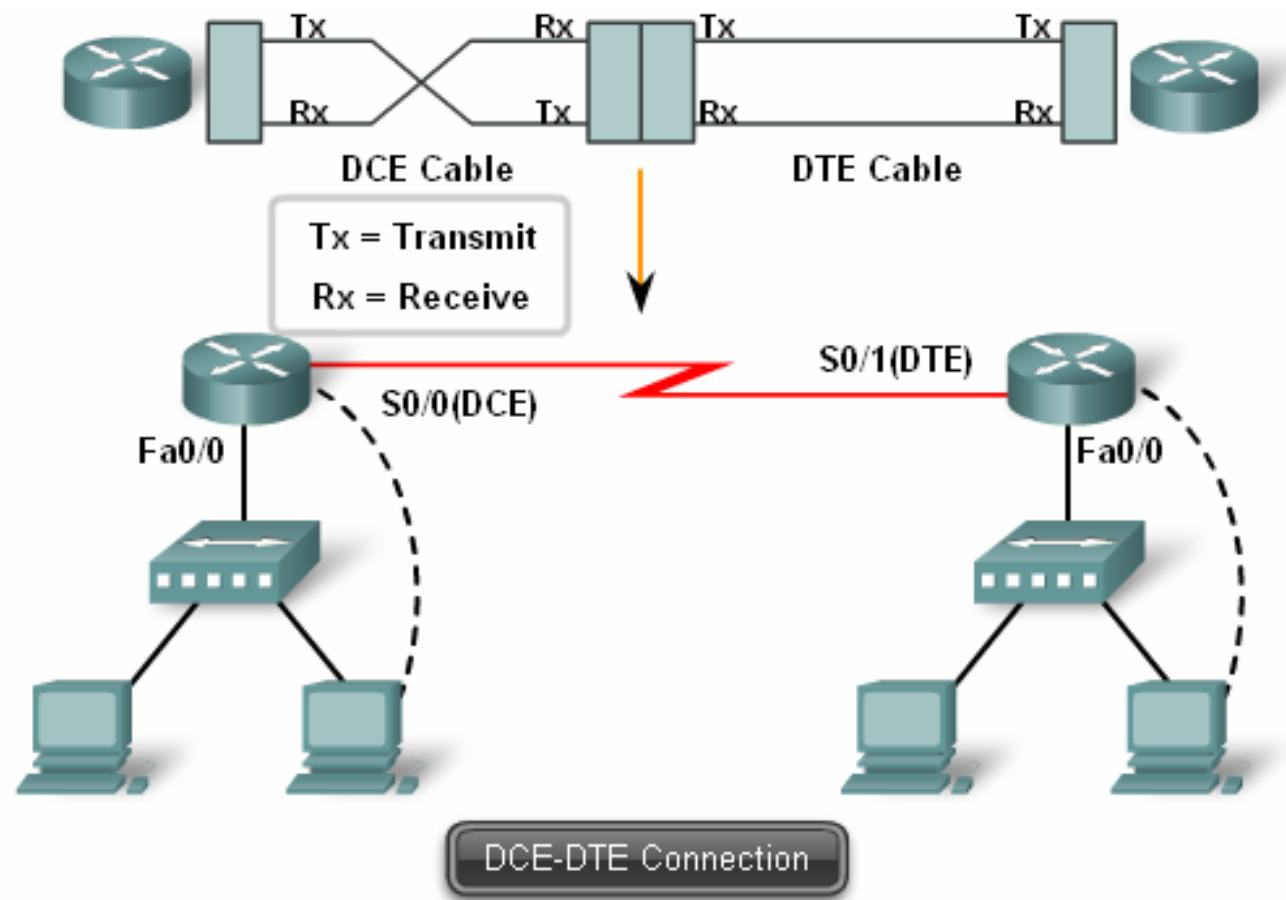
- End of the user's device on the WAN Link

Data Communications Equipment:

- End of the WAN provider's side of the communication facility
- Responsible for providing clocking signal.

Types of Connections in a WAN

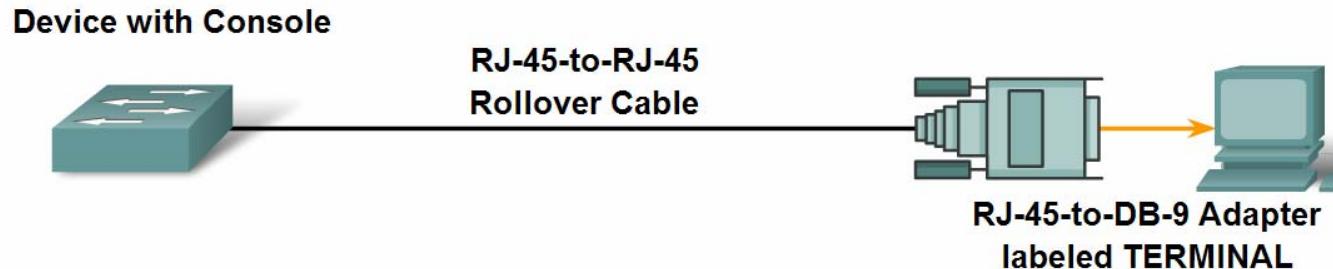
- Simulating WAN in LAB topology



Types of Connections - Device Management

- Define the role of device management connections when using Cisco equipment.

The Device Management Connection



- PCs require an RJ-45 to DB-9 or RJ-45 to DB-25 adapter.
- COM port settings are 9600 bps, 8 data bits, no parity, 1 stop bit, no flow control.
- This provides out-of-band console access.
- AUX switch port may be used for a modem-connected console.

Design an Addressing Scheme for an Internetwork.

- Design an address scheme for an internetwork and assign ranges for hosts, network devices and the router interface

Determining the Number of Hosts in the Network

Include these devices in the count:



Router Interfaces

Count the number of interfaces, and not the number of routers



Printers



IP Phones

Count other specialty IP devices as well



Switch Management Addresses



Administration Users



General Users



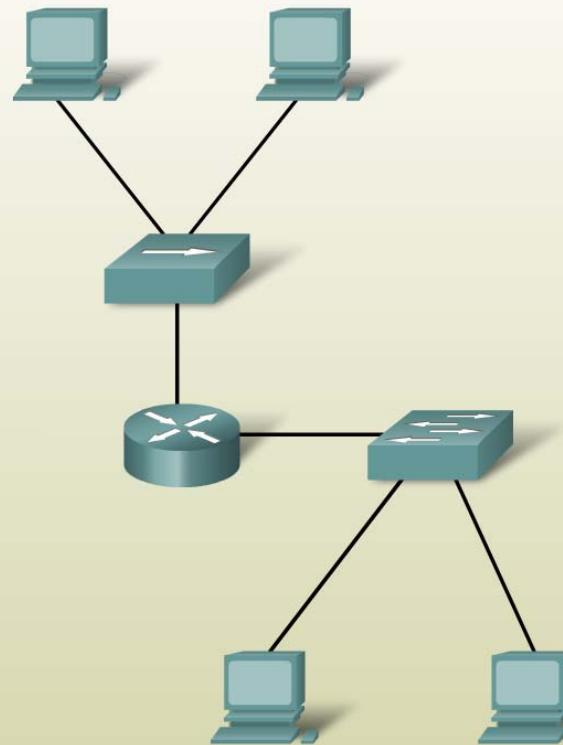
Servers

Importance of Network Designs

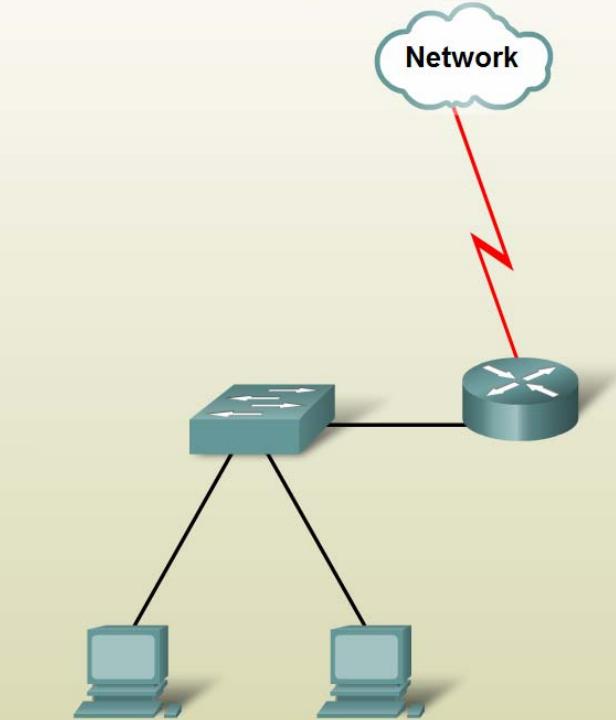
- Given a network requirement, determine the optimum number of sub networks in the larger internetwork.

Internetwork Connections with a Router

Router interconnecting two LANs



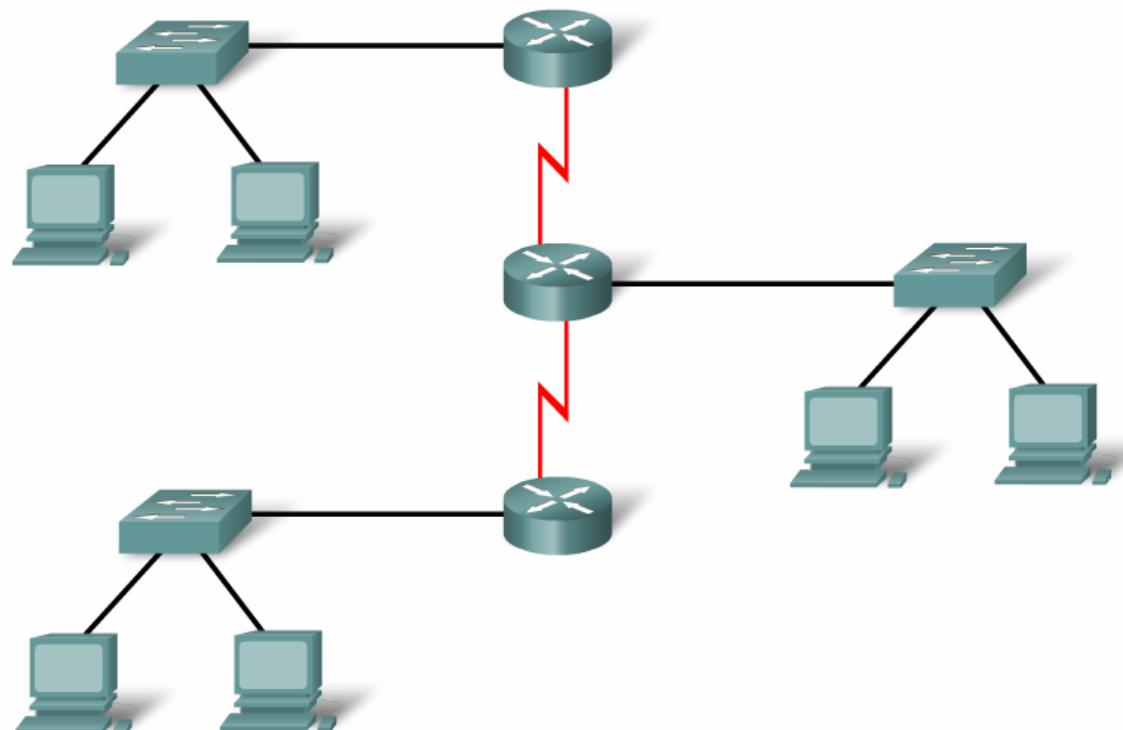
Router interconnecting a LAN and a WAN



Importance of Network Designs

- Describe how to count the segments between router interfaces.

Counting Subnets

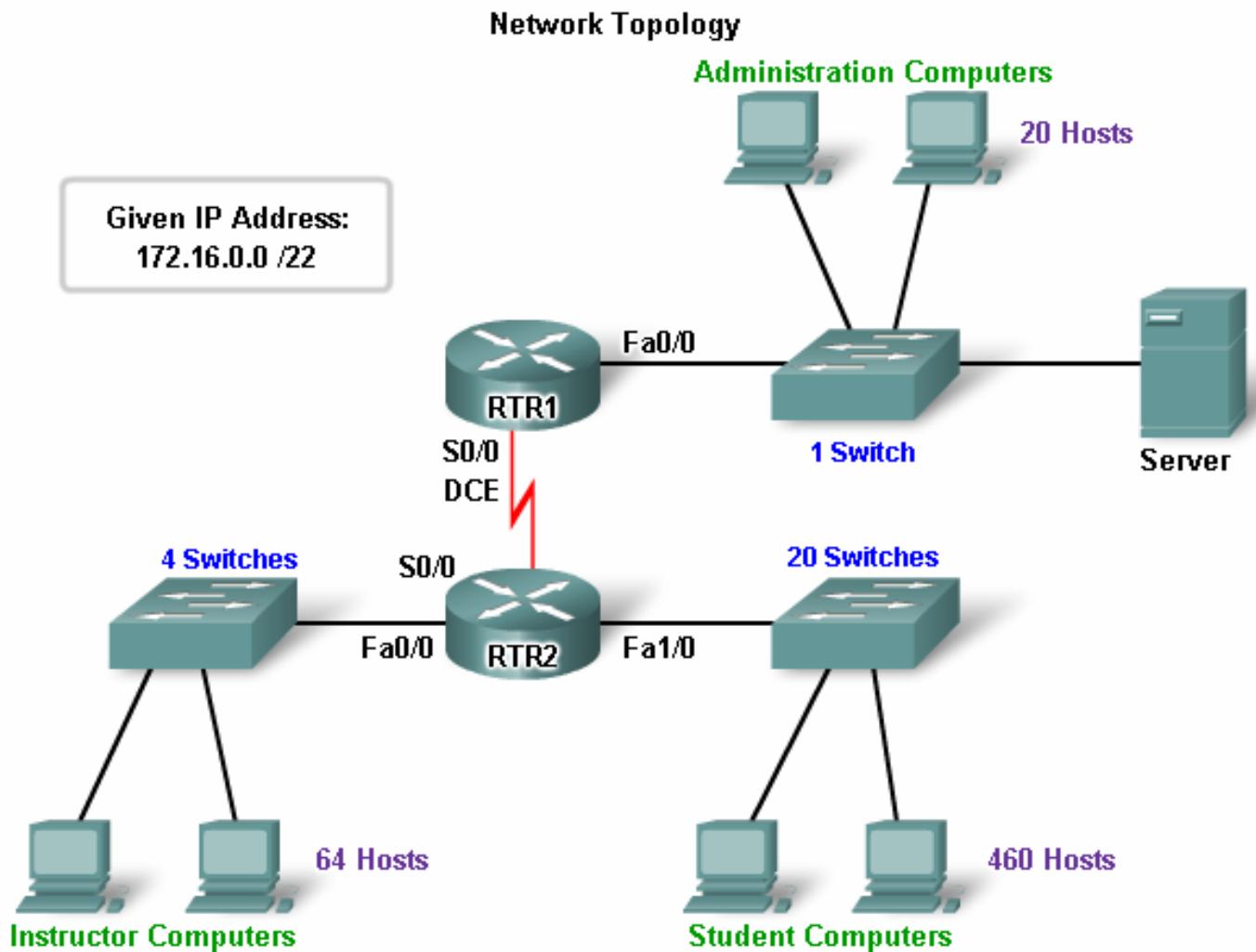


Importance of Network Designs

- Given a network scenario, develop an appropriate networking scheme – Exam Practise 10.3.2

Hands-on Lab:
How Many Networks

Network Design – Case 1



Network Design – Case 1

- Student LAN
 - Student Computers: 460
 - Router (LAN Gateway): 1
 - Switches (management): 20
 - Total for student subnetwork: 481
- Instructor LAN
 - Instructor Computers: 64
 - Router (LAN Gateway): 1
 - Switches (management): 4
 - Total for instructor subnetwork: 69
- Administrator LAN
 - Administrator Computers: 20
 - Server: 1
 - Router (LAN Gateway): 1
 - Switch (management): 1\Total for administration subnetwork: 23
- WAN
 - Router - Router WAN: 2
 - Total for WAN: 2



Network Design – Case 1

Calculating Addresses **without** VLSM Address Ranges for Subnets

Case 1

Network	Subnet Address	Host Address Range	Broadcast Address	
Student	172.16.0.0/23	172.16.0.1	172.16.1.254	172.16.1.255
Instructor	172.16.2.0/23	172.16.2.1	172.16.3.254	172.16.3.255
Administration	172.16.4.0/23	172.16.4.1	172.16.5.254	172.16.5.255
WAN	172.16.6.0/23	172.16.6.1	172.16.7.254	172.16.7.255

172.16.0.0 - 172.16.1.255

510 host addresses available in each subnet

481 Addresses used



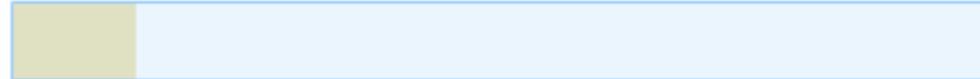
172.16.2.0 - 172.16.3.255

69 Addresses used



172.16.4.0 - 172.16.5.255

23 Addresses used



172.16.6.0 - 172.16.7.255

2 Addresses used

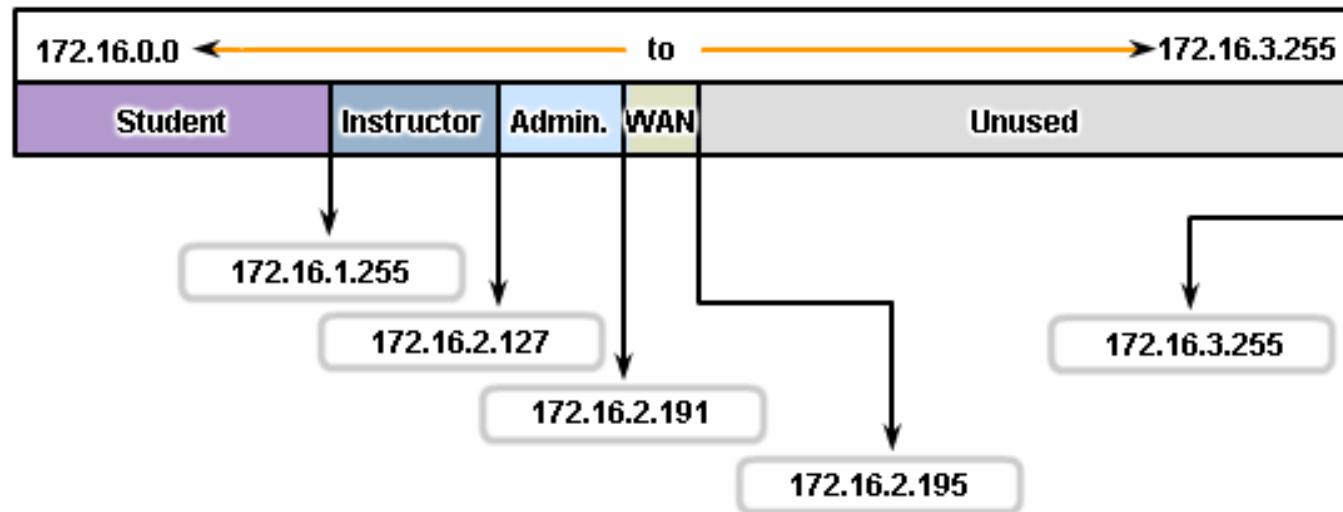


Network Design – Case 1

Calculating Addresses **with** VLSM Address Ranges for Subnets

Case 1

Network	Subnet Address	Host Address Range	Broadcast Address	
Student	172.16.0.0/23	172.16.0.1	172.16.1.254	172.16.1.255
Instructor	172.16.2.0/25	172.16.2.1	172.16.2.126	172.16.2.127
Administration	172.16.2.128/26	172.16.2.129	172.16.2.190	172.16.2.191
WAN	172.16.2.192/30	172.16.2.193	172.16.2.194	172.16.2.195
Unused	na	172.16.2.197	172.16.3.254	na





Summary

In this chapter, you learned to:

- Identify the basic network media required to make a LAN connection.
- Identify the types of connections for intermediate and end device connections in a LAN.
- Identify the pinout configurations for straight-through and crossover cables.
- Identify the different cabling types, standards, and ports used for WAN connections.
- Define the role of device management connections when using Cisco equipment.
- Design an addressing scheme for an internetwork and assign ranges for hosts, network devices, and the router interface.
- Compare and contrast the importance of network designs.





Configuring and Testing Your Network



Network Fundamentals – Chapter 11

Cisco | Networking Academy®
Mind Wide Open™



Objectives

- Define the role of the Internetwork Operating System (IOS)
- Use Cisco CLI commands to perform basic router and switch configuration and verification
- Given a network addressing scheme, select, apply, and verify appropriate addressing parameters to a host
- Use common utilities to verify network connectivity between hosts
- Use common utilities to establish a relative performance baseline for the network

Role of Internetwork Operating System (IOS)

- **Cisco Internetwork Operating System (IOS)** is the system software in Cisco devices.
- IOS provides devices with the following services:
 - Basic routing and switching functions
 - Reliable and secure access to networked resources
 - Network scalability

Cisco IOS



Internetwork Operating System for Cisco networking devices



Role of Internetwork Operating System (IOS)

- The **IOS** operational details **vary** on different internetworking devices, depending on the device's purpose and feature set.
- The services provided by the Cisco IOS are generally accessed using a **command line interface (CLI)**.
- The **IOS file** itself is **several megabytes** in size and is stored in a semi-permanent memory area called flash.

Cisco IOS



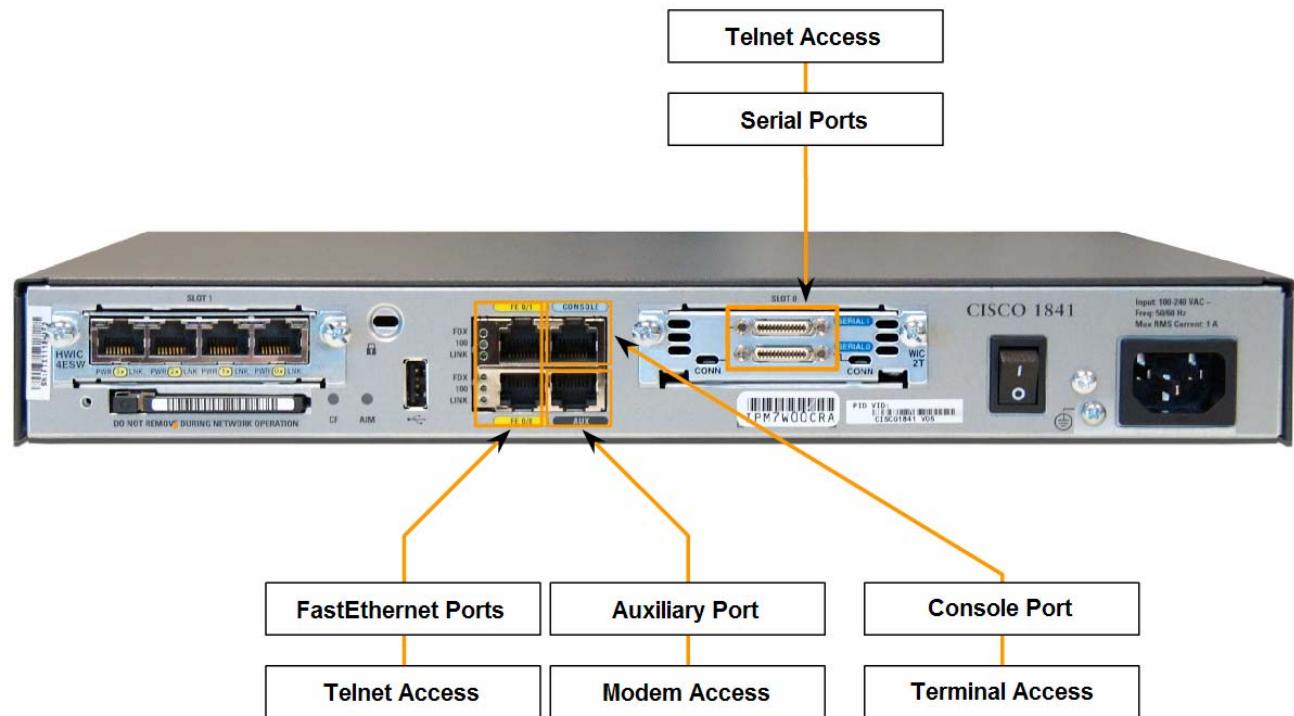
Internetwork Operating System for Cisco networking devices



Role of Internetwork Operating System (IOS)

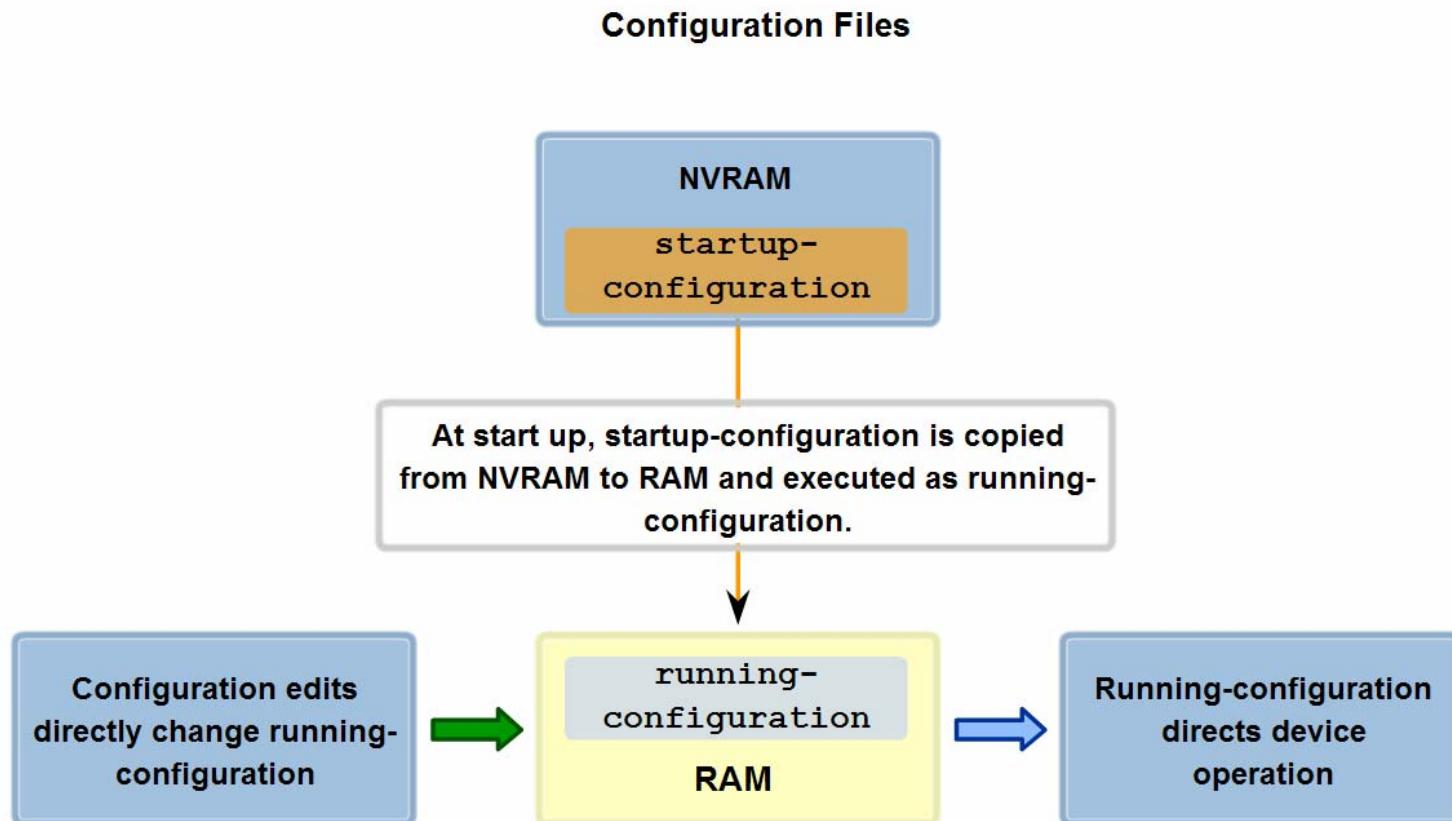
- There are several ways to access the CLI environment.
The most usual methods are:
 - Console
 - Telnet or SSH
 - AUX port

Accessing the Cisco IOS on a Device



Role of Internetwork Operating System (IOS)

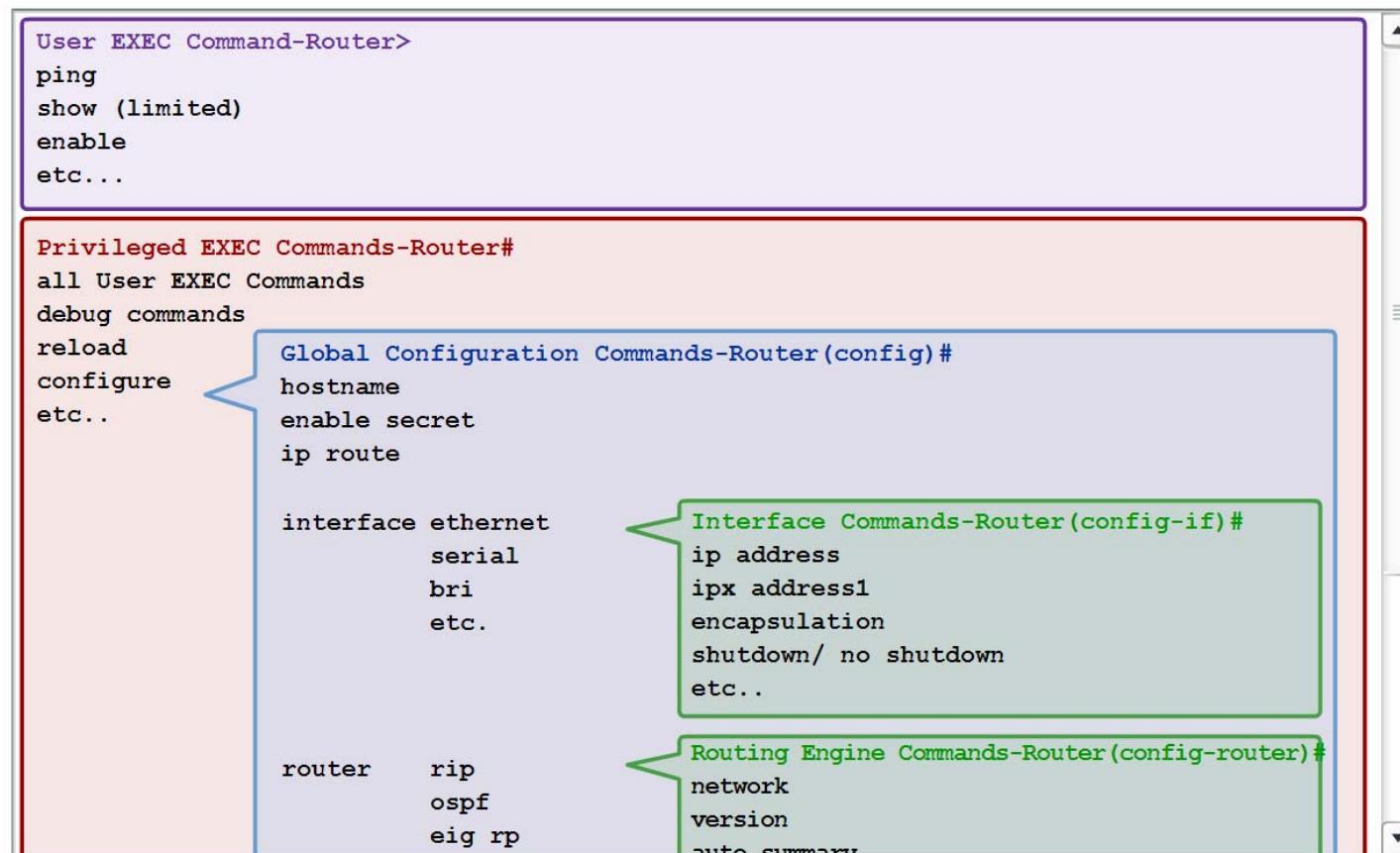
- Startup-configuration vs. Running-configuration



Role of Internetwork Operating System (IOS)

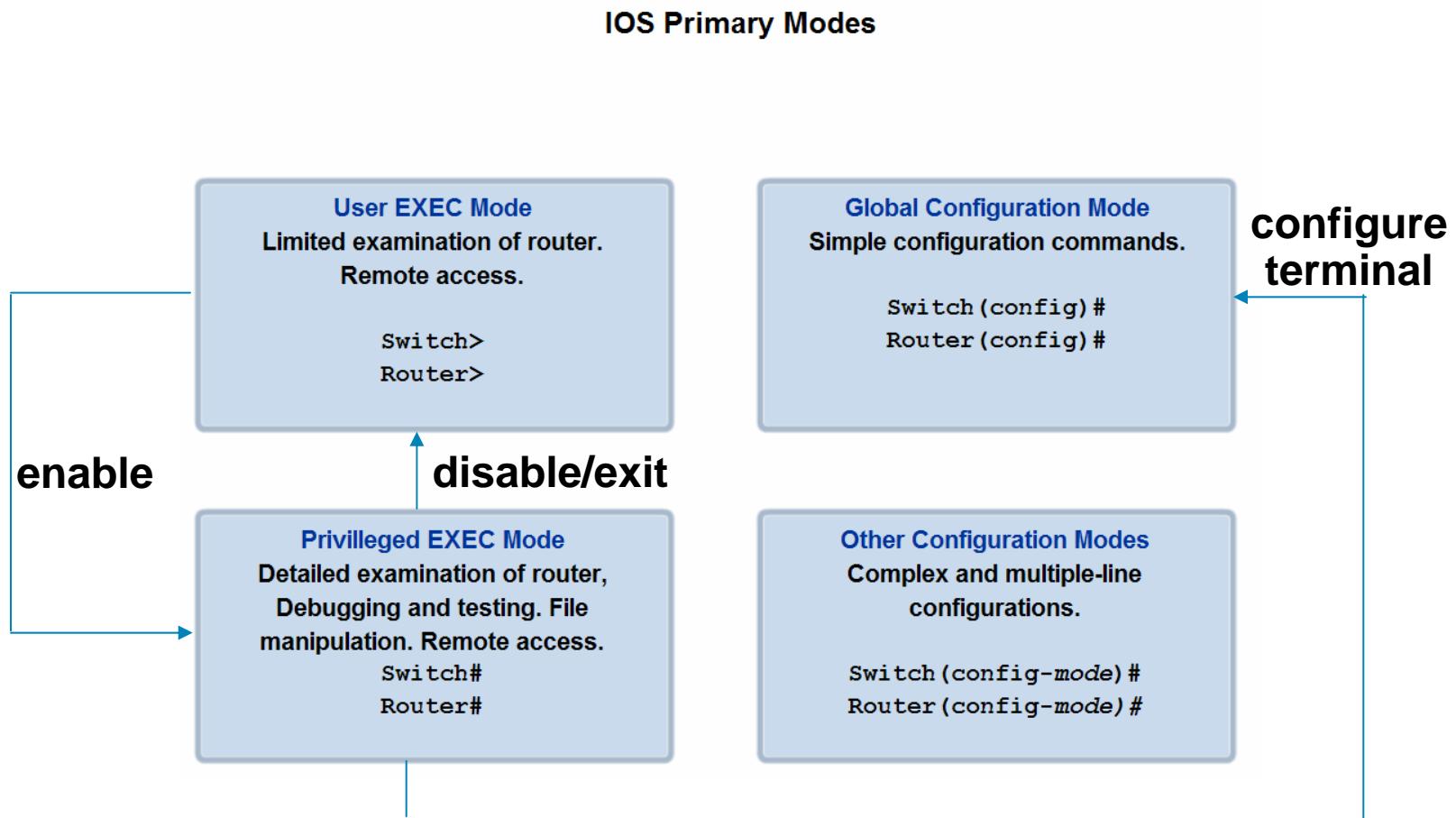
- Recognize that Cisco IOS is modal and describe the implications of modes.

IOS Mode Hierarchical Structure



Role of Internetwork Operating System (IOS)

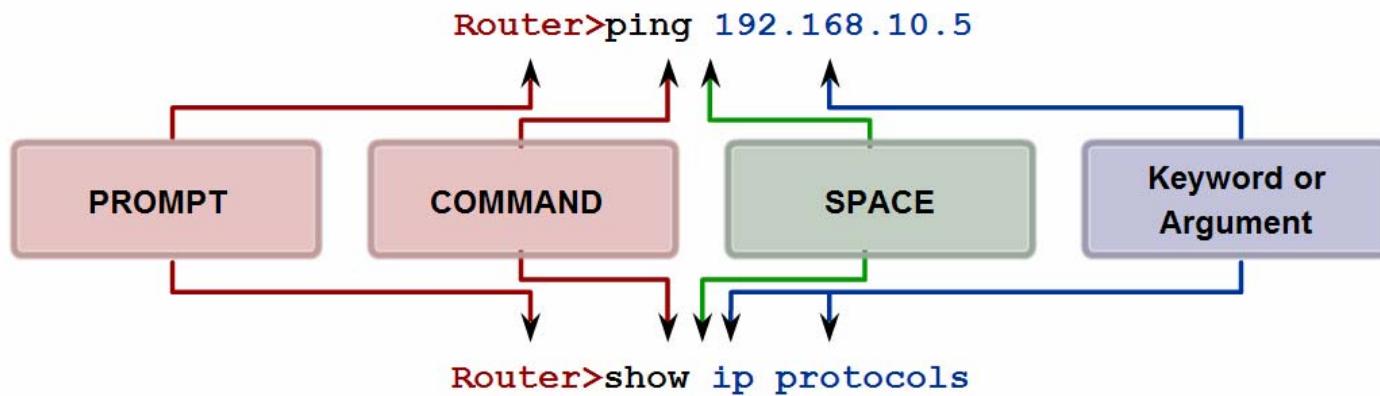
- Define the different modes and identify the mode prompts in the CLI



Role of Internetwork Operating System (IOS)

- Identify the basic command structure for IOS commands

Basic IOS Command Structure



Prompt commands are followed by a space and then the keyword or arguments.



Role of Internetwork Operating System (IOS)

- Identify the types of help and feedback available while using IOS and use these features to get help, take

Context Sensitive Help

Example of a sequence of commands using the CLI context sensitive help

```
Cisco#cl?  
clear clock  
Cisco#clock ?  
    set Set the time and date  
Cisco#clock set  
% Incomplete command.  
Cisco#clock set ?  
    hh:mm:ss Current Time  
Cisco#clock set 19:50:00  
% Incomplete command.
```

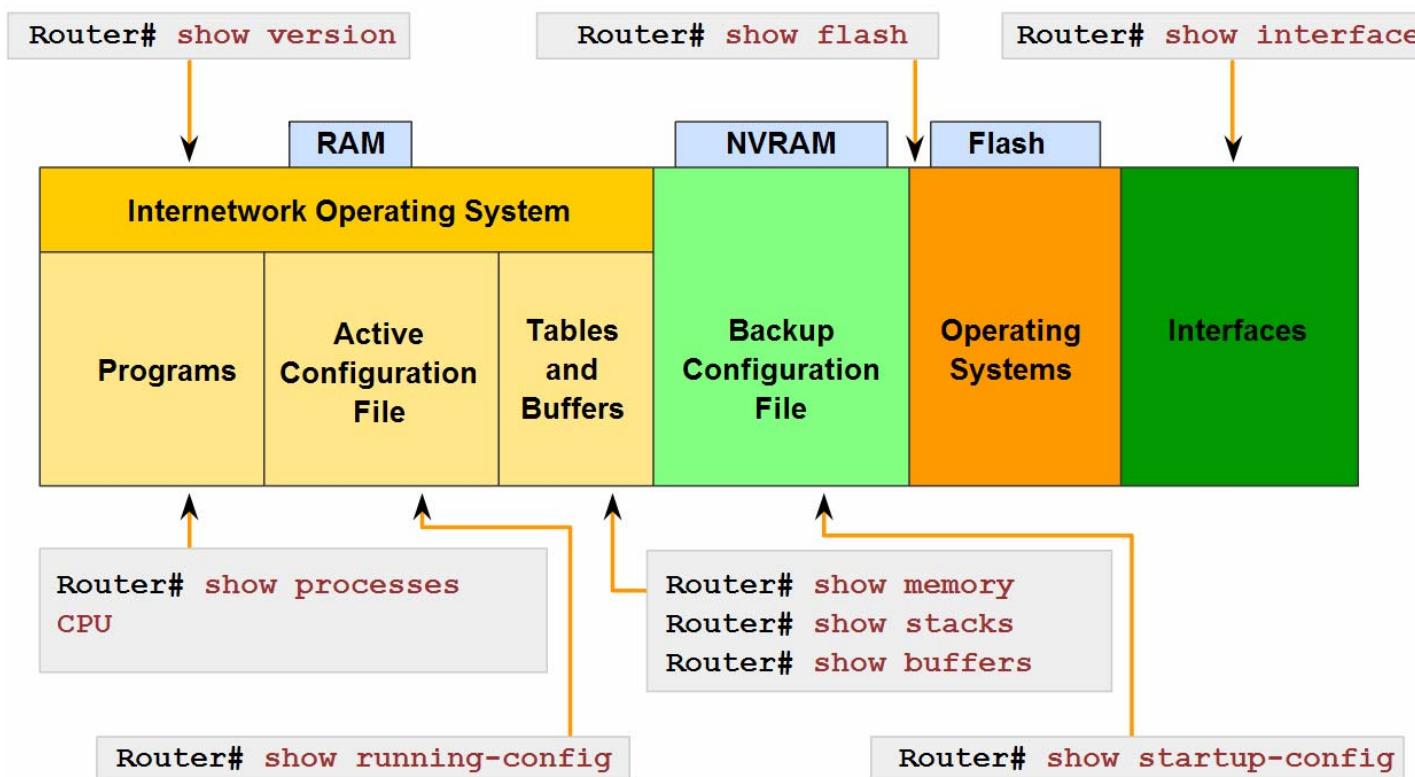
Command explanations
Incomplete Command messages
Invalid input messages
Variable formats

```
Cisco#clock set 19:50:00 ?  
    <1-31> Day of the month  
    MONTH Month of the year  
Cisco#clock set 19:50:00 25 6  
                                ^  
                                Invalid input detected at '^' marker.  
Cisco#clock set 19:50:00 25 June  
% Incomplete command.  
Cisco#clock set 19:50:00 25 June ?  
    <1993-2035> Year  
Cisco#clock set 19:50:00 25 June 2007  
Cisco#
```

Role of Internetwork Operating System (IOS)

- The purpose of the **show** command and several of its variations

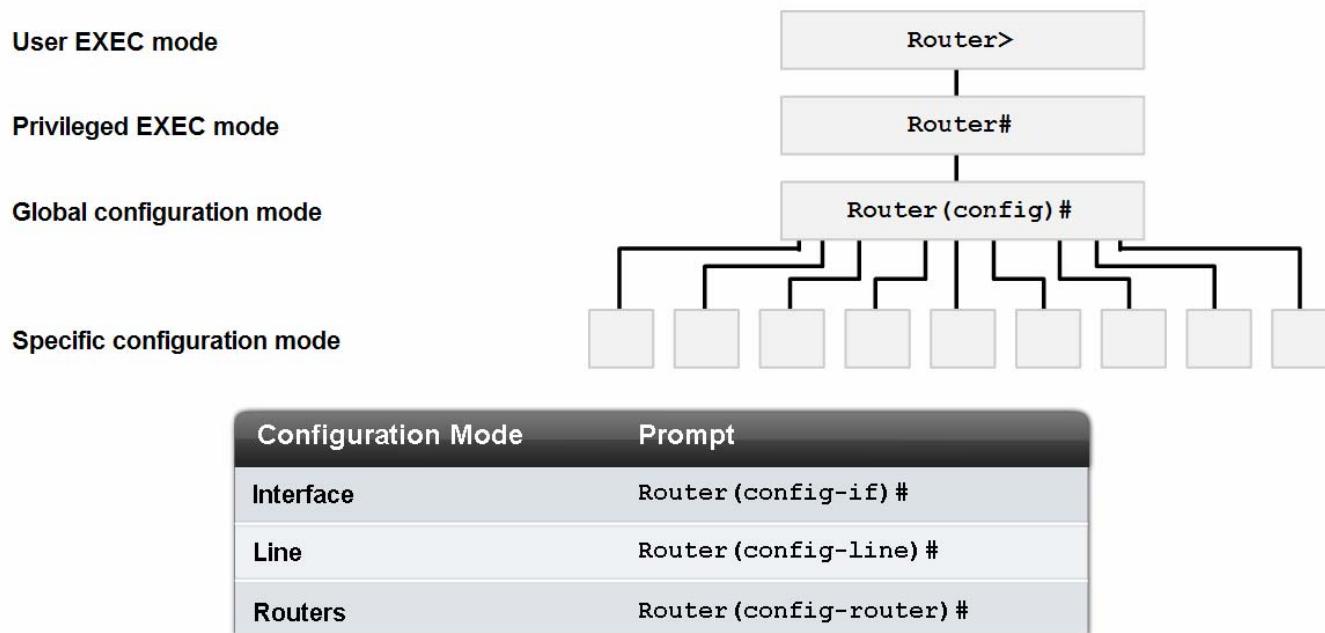
IOS **show** commands can provide information about the configuration, operation and status of parts of a Cisco router.



Role of Internetwork Operating System (IOS)

- Identify several of the configuration modes, their purpose and their associated prompt

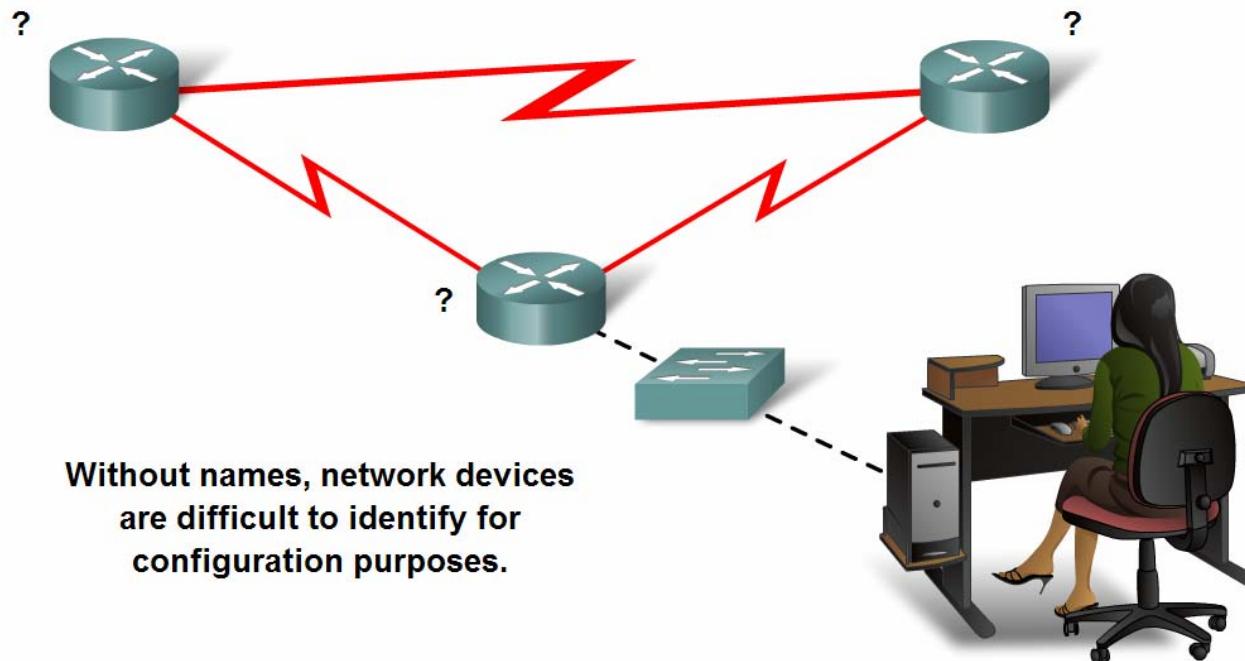
IOS Configuration Modes



Use Cisco CLI Commands to Perform Basic Router & Switch Configuration and Verification

- Explain the reasons for naming devices.

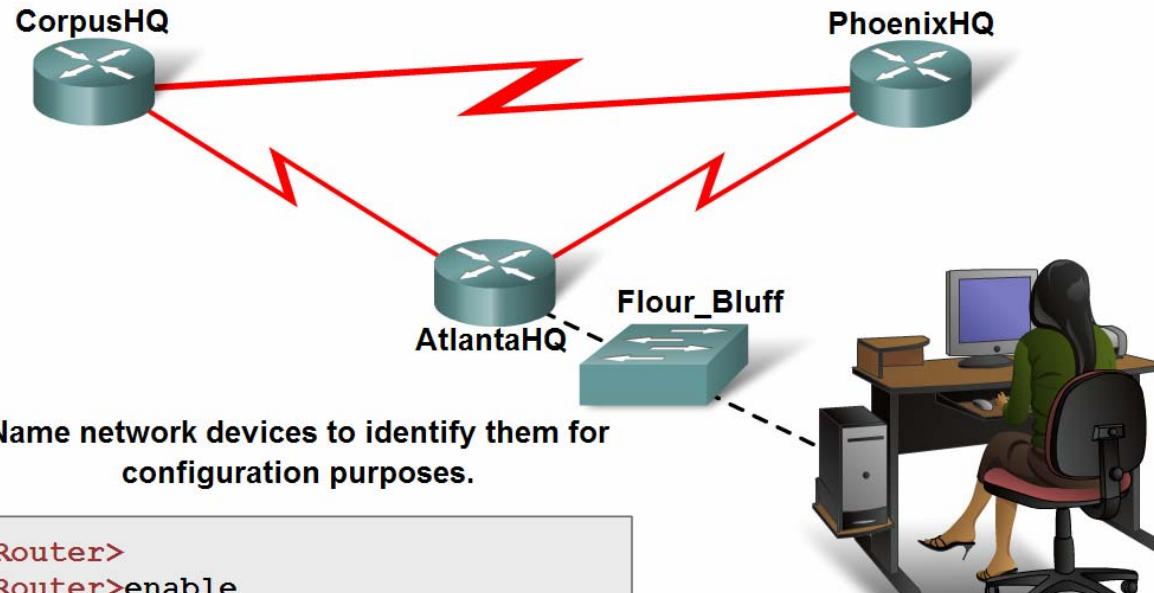
Basic Configuration Using Cisco IOS



Use Cisco CLI Commands to Perform Basic Router & Switch Configuration and Verification

- Describe two common approaches to establishing naming conventions: **location** and the **purpose** of the devices

Configuring Device Names



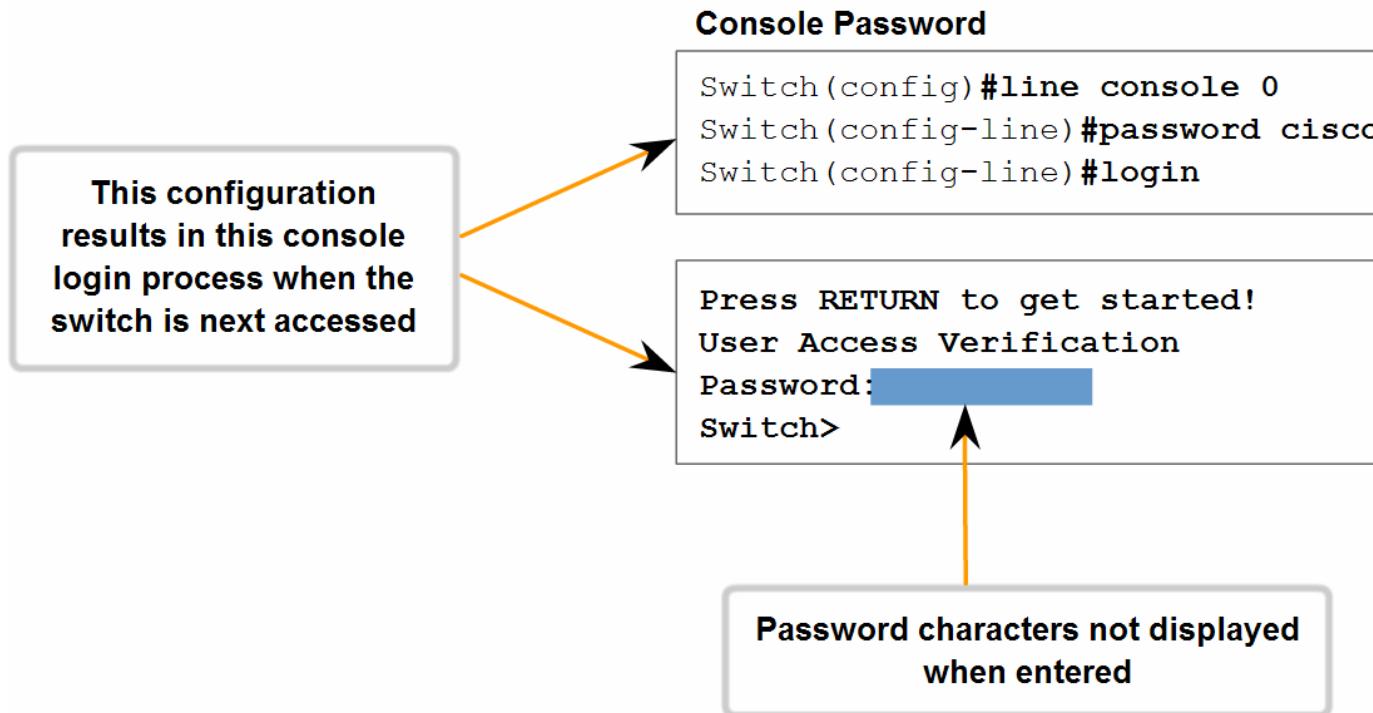
```
Router>
Router>enable
Router#
Router#configure terminal
Router(config)#hostname AtlantaHQ
AtlantaHQ(config)#

```

Use Cisco CLI Commands to Perform Basic Router & Switch Configuration and Verification

- The role of passwords in limiting access to device configurations

LIMITING DEVICE ACCESS - CONFIGURING CONSOLE PASSWORDS



Use Cisco CLI Commands to Perform Basic Router & Switch Configuration and Verification

- Several ways in which access to a device configuration can be limited

Limiting Device Access Configuring Telnet and Password Encryption

Virtual Terminal Password

```
Router(config)#line vty 0 4
Router(config-line)#password cisco
Router(config-line)#login
```

Enable Password

```
Router(config)#enable password san fran
```

Enable Secret Password

```
Router(config)#enable secret cisco
```

Strongly encrypted password

Use Cisco CLI Commands to Perform Basic Router & Switch Configuration and Verification

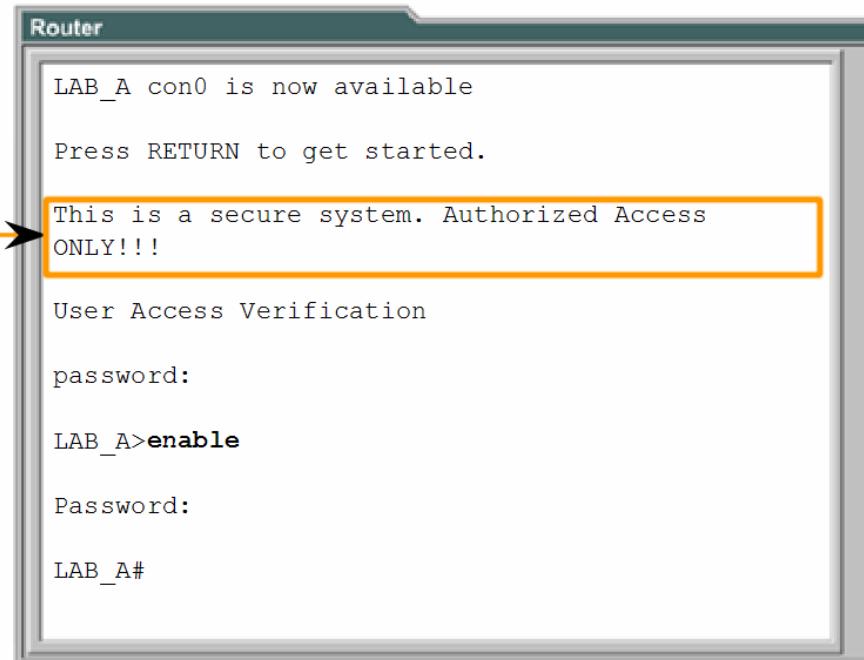
- Use the CLI to set passwords and add banners to a device

Limiting Device Access – Login Banner

```
LAB_A(config)#banner motd # This is a secure system. Authorized Access ONLY!!! #
```

This configuration results in this message of the day banner

Delimiting characters not included in message



```
Router
LAB_A con0 is now available
Press RETURN to get started.

This is a secure system. Authorized Access
ONLY!!!

User Access Verification

password:

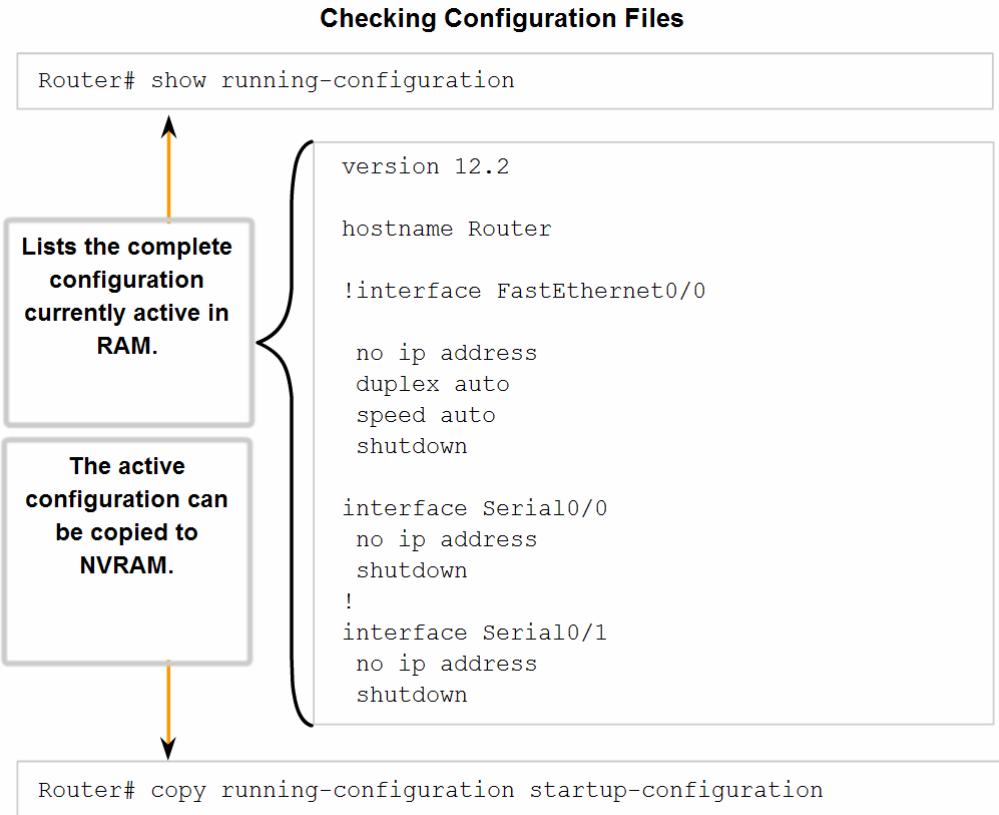
LAB_A>enable

Password:

LAB_A#
```

Use Cisco CLI Commands to Perform Basic Router & Switch Configuration and Verification

- Trace the steps used to examine the startup config, make changes to config, and replace the startup config with the running config





Use Cisco CLI Commands to Perform Basic Router & Switch Configuration and Verification

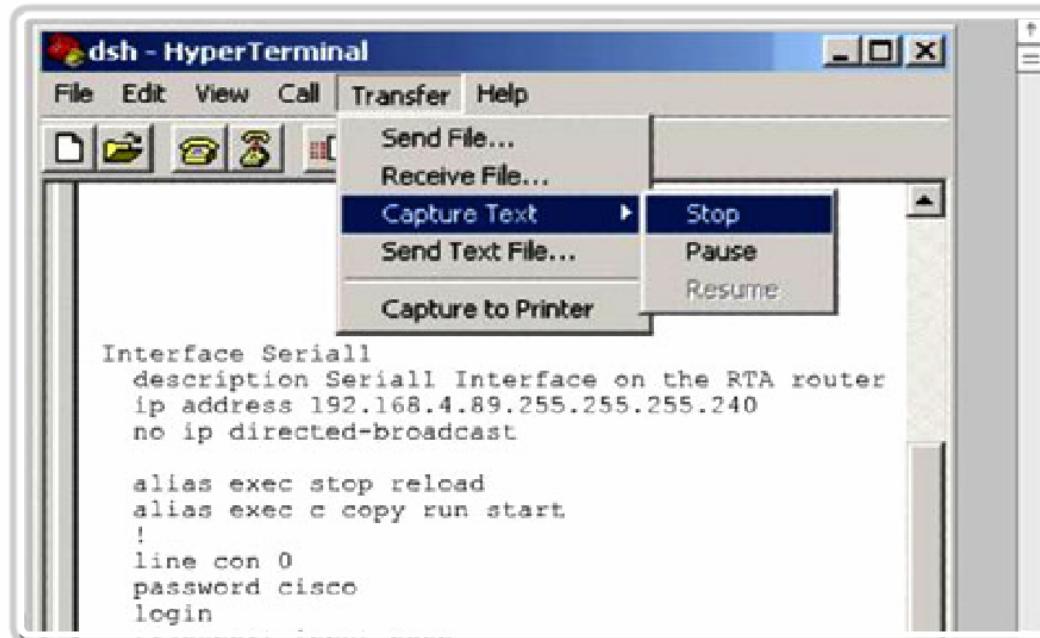
- Use basic IOS config commands to manage a device.

```
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] y
Writing tokyo.2 !!!!!!! [OK]
```

Use Cisco CLI Commands to Perform Basic Router & Switch Configuration and Verification

- Use a text file to backup and restore config settings

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



Use Cisco CLI Commands to Perform Basic Router & Switch Configuration and Verification

- Purpose of a router is to interconnect different networks, each interface on a router has its own unique IPv4 address.

Configuring Router Interfaces

All interfaces are accessed by issuing the `interface` command at the global configuration prompt.

In the following commands, the `type` argument includes serial, ethernet, fastethernet, and others:

```
Router(config) #interface type port  
Router(config) #interface type slot/port  
Router(config) #interface type slot/subslot/port
```

The following command is used to administratively turn off the interface:

```
Router(config-if) #shutdown
```

The following command is used to turn on an interface that has been shutdown:

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

The following command is used to quit the current interface configuration mode:

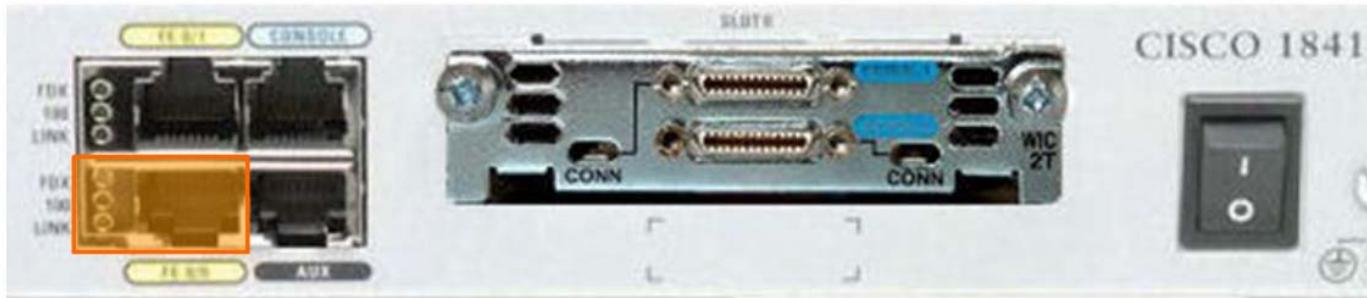
```
Router(config-if) #exit
```

When the configuration is complete, the interface is enabled and interface configuration mode is exited.

Use Cisco CLI Commands to Perform Basic Router & Switch Configuration and Verification

- Describe the purpose of having multiple interfaces in one router

Configuring Router Ethernet Interfaces



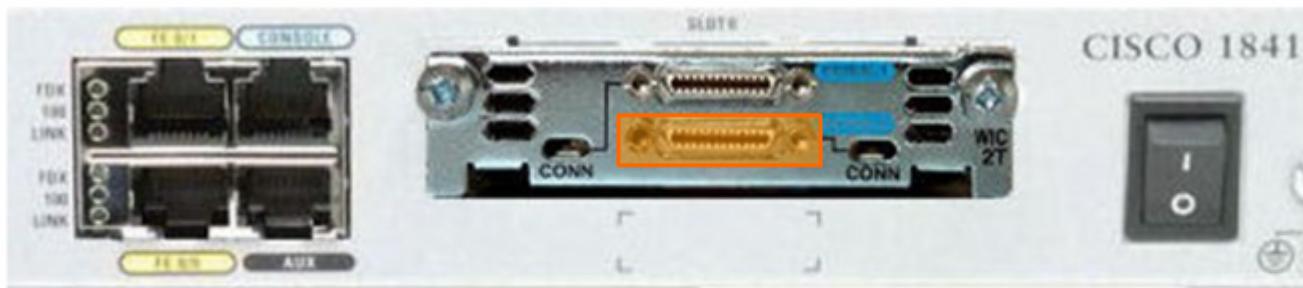
```
Router(config)#interface FastEthernet 0/0
Router(config-if)#ip address 192.168.10.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config) #
```

Configure Router Ethernet Interfaces

Use Cisco CLI Commands to Perform Basic Router & Switch Configuration and Verification

- Describe the purpose of having multiple interfaces in one router

Configure Router Serial Interfaces



```
Router(config)#interface Serial 0/0/0
Router(config-if)#ip address 192.168.11.1 255.255.255.252
Router(config-if)#clock rate 56000
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#

```

Configure Router Serial Interfaces

Use Cisco CLI Commands to Perform Basic Router & Switch Configuration and Verification

- Explain the purpose of assigning interface descriptions to a router

Router Interfaces Descriptions



The image shows a Cisco 1841 router chassis. It has several ports labeled F1-F6 and AUX at the top left. In the center, there is a WIC (Wide Area Interface Card) slot with two blue connectors labeled 'CONN'. On the right side, there is a black I/O module. The model number 'CISCO 1841' is printed on the right edge of the chassis.

```
Router(config)#interface fa0/0
Router(config-if)#description Building B Sales LAN
Router(config-if)#exit
```

```
Router(config)#interface s0/0/0
Router(config-if)#description To Perth CKT-PT27834365-01
Router(config-if)#exit
```

Description is all text after this space **Interface description used for internal network documentation**

Arrows point from the text boxes to the corresponding parts of the configuration commands:

- A green arrow points from the "Description is all text after this space" box to the word "Building" in the first configuration command.
- A blue arrow points from the "Interface description used for internal network documentation" box to the word "Perth" in the second configuration command.



Use Cisco CLI Commands to Perform Basic Router & Switch Configuration and Verification

- Configuration of the switch

Switch Configuration

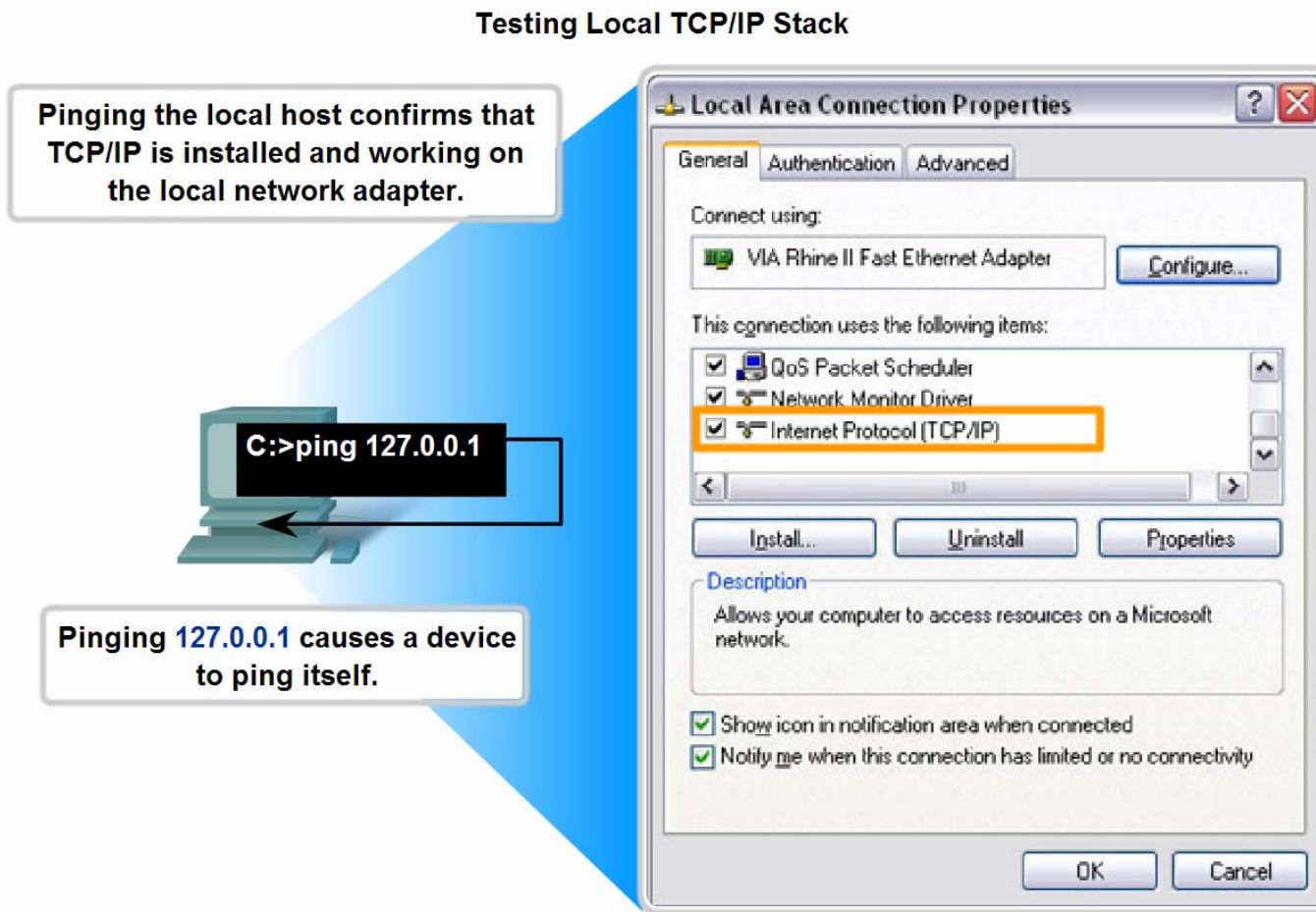
```
Switch#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Switch(config)#interface vlan 1  
Switch(config-if)#ip address 192.168.1.2 255.255.255.0  
Switch(config-if)#no shutdown  
Switch(config-if)#exit  
Switch(config)#ip default-gateway 192.168.1.1  
Switch(config)#exit  
Switch#
```

```
Switch#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Switch(config)#interface vlan 1  
Switch(config-if)#ip address 192.168.1.2 255.255.255.0  
Switch(config-if)#no shutdown  
Switch(config-if)#exit  
Switch(config)#ip default-gateway 192.168.1.1  
Switch(config)#exit  
Switch#
```

Note the prompt changes denoting the current IOS mode.

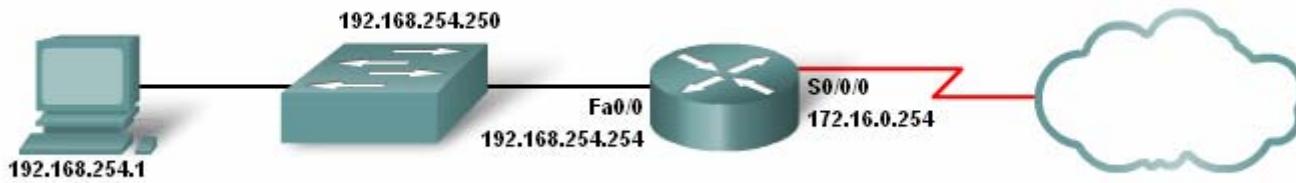
Select, Apply, and Verify Appropriate Addressing Parameters to a Host

- Given a type of host and a master addressing scheme, trace the steps for assigning host parameters to a host



Select, Apply, and Verify Appropriate Addressing Parameters to a Host

- Trace the steps for using ipconfig/ifconfig to verify host parameter assignments and for using ping to test assignments



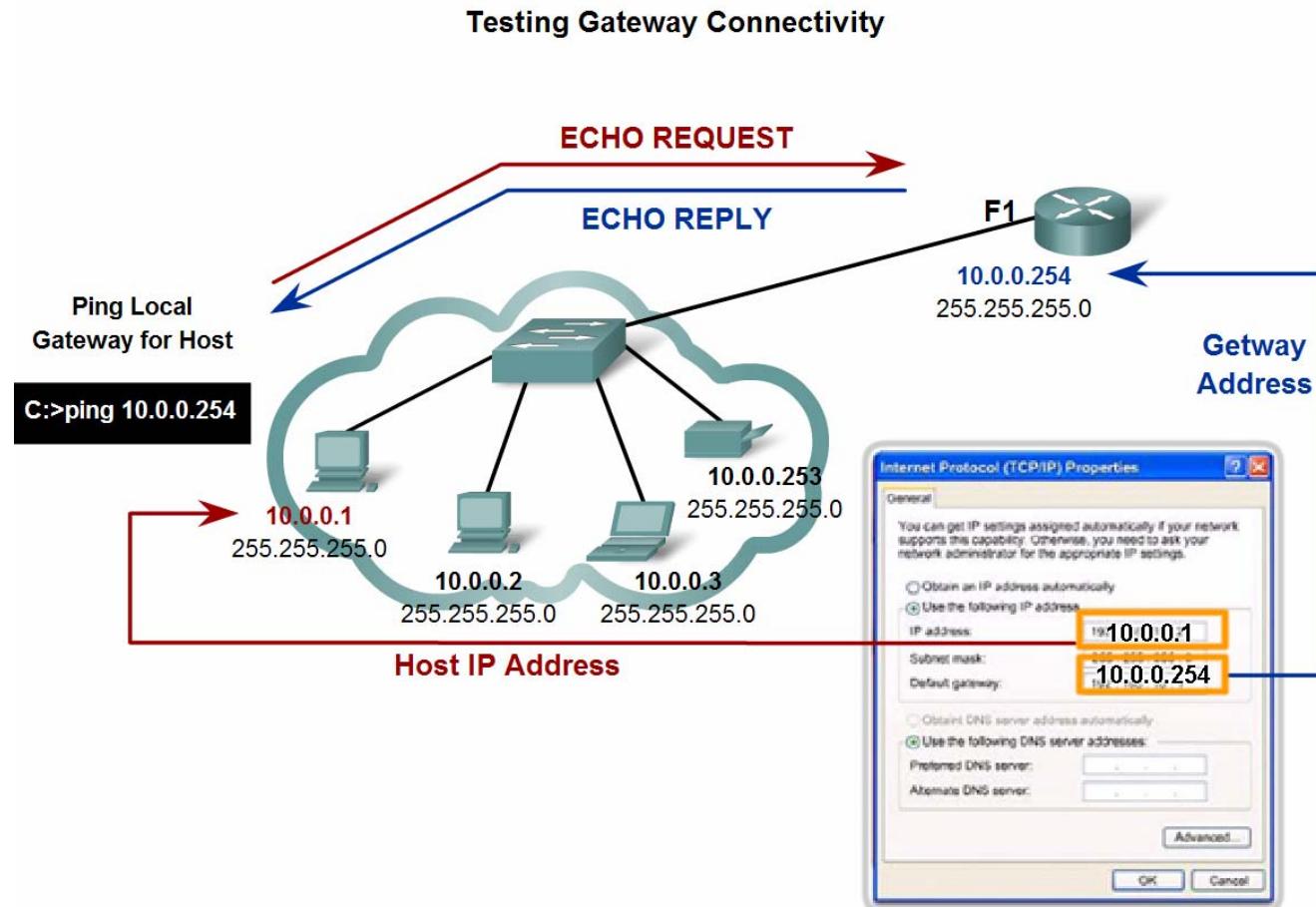
```
Router1#show ip interface brief
Interface          IP-Address      OK? Method Status          Protocol
FastEthernet0/0    192.168.254.254 YES  NVRAM   up       up
FastEthernet0/1/0  unassigned      YES  unset    down     down
Serial0/0/0        172.16.0.254  YES  NVRAM   up       up
Serial0/0/1 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

Use Common Utilities to Verify Network Connectivity Between Hosts

- Use the ping command in the CLI to determine if the IP protocol is operational on a local host

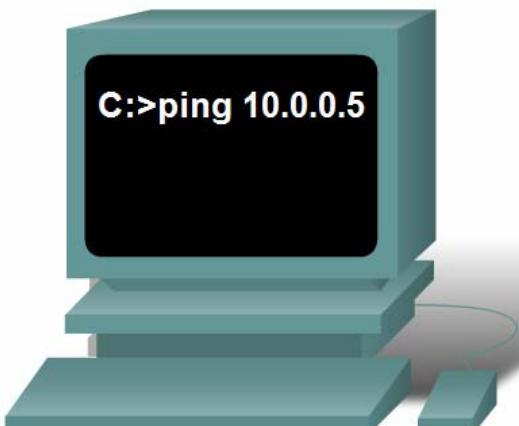


Use Common Utilities to Verify Network Connectivity Between Hosts

- Use the ping command to determine if the IP protocol is properly bound to an NIC

Testing the Local NIC Assignment

```
IP Address . . . . . : 10.0.0.5  
Subnet Mask . . . . . :  
255.255.255.0
```



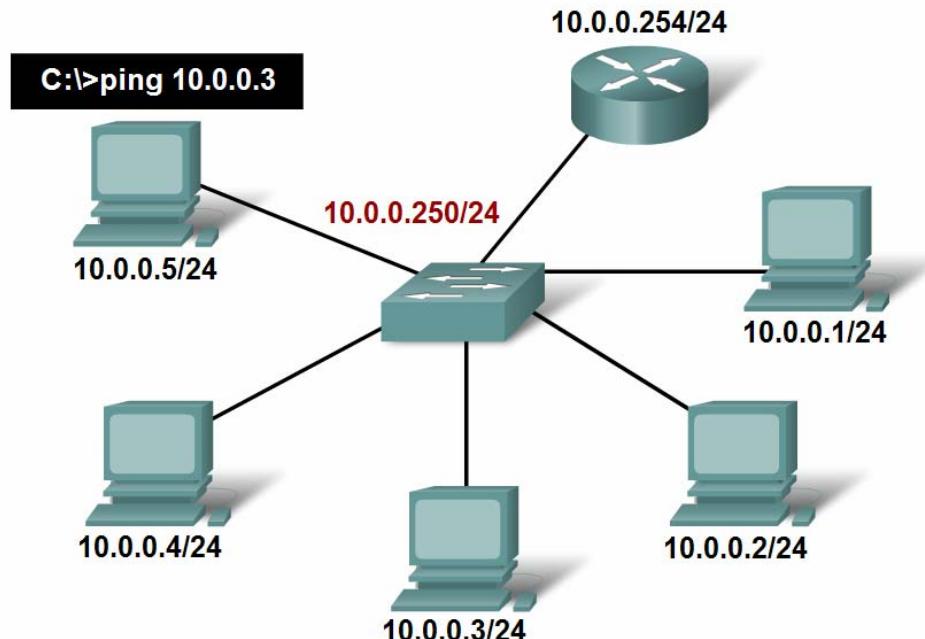
Verify the host NIC address is bound and ready for transmitting signals across the media by pinging its own IP address

Use Common Utilities to Verify Network Connectivity Between Hosts

- Use the ping command to determine if a host can actively communicate across the local network

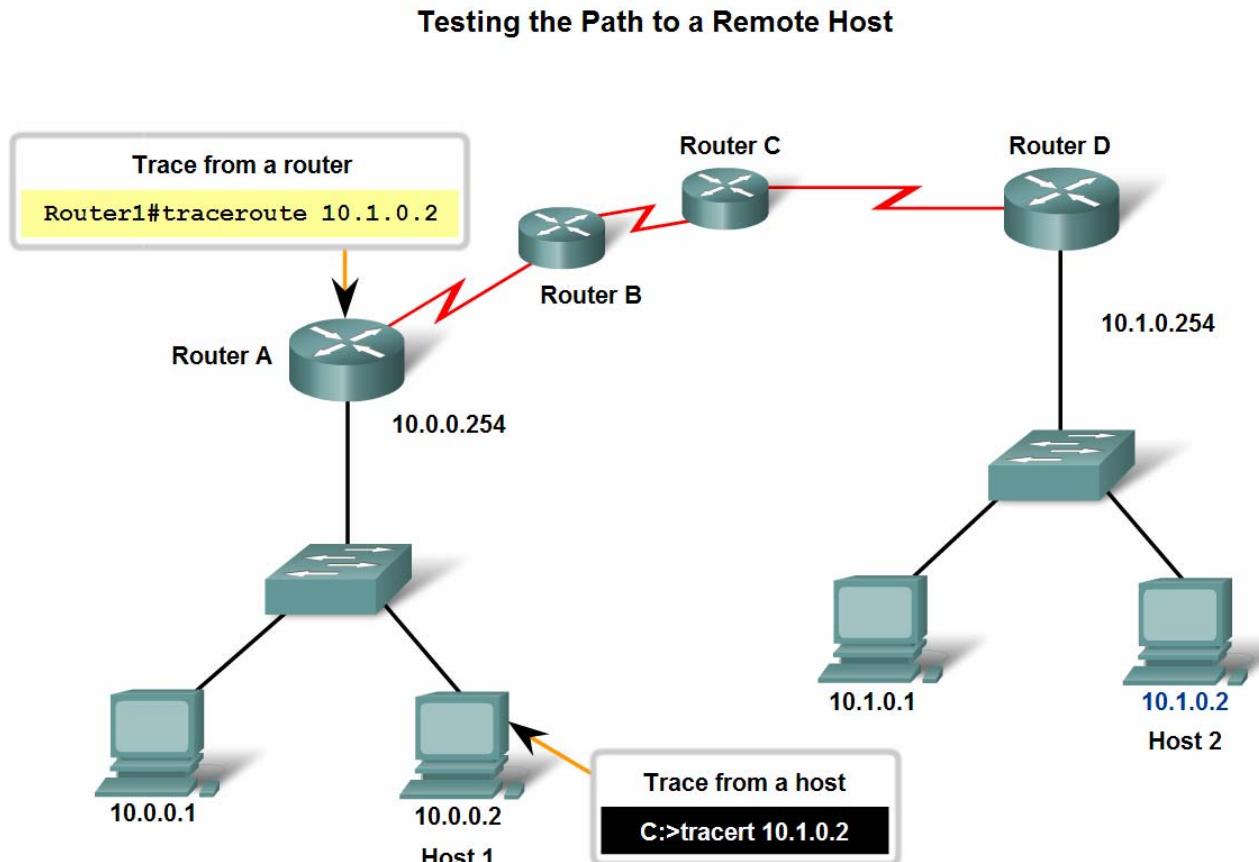
Testing Local Network

Successfully pinging the other host's IPv4 addresses will verify that not only the local host is configured properly but the other hosts are configured correctly as well.



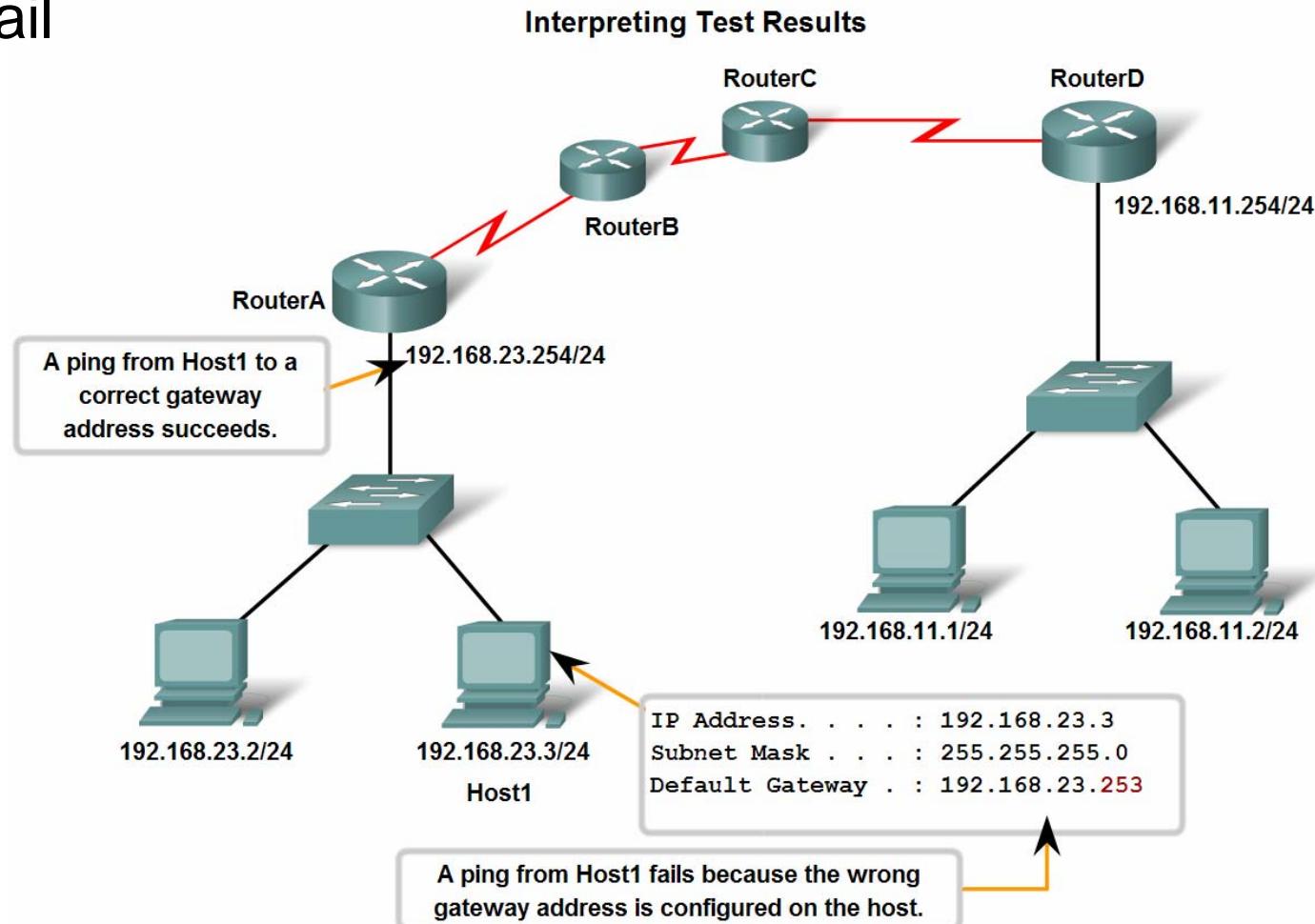
Use Common Utilities to Verify Network Connectivity Between Hosts

- Use the ping command to verify that the local host can communicate across the internetwork to a given remote host.



Use Common Utilities to Verify Network Connectivity Between Hosts

- Identify several conditions that might cause the test to fail





Use Common Utilities to Establish a Relative Performance Baseline for the Network

- Use the output of the ping command, saved into logs, and repeated over time, to establish relative network performance

Baseline with ping

FEB 2, 2007 08:14:43

```
C:\host1>ping 10.66.254.159
Pinging 10.66.254.159 with 32 bytes of data:
Reply from 10.66.254.159: bytes=32 time<1ms TTL=128
```

MAR 17, 2007 14:41:06

```
C:\host1>ping 10.66.254.159
Pinging 10.66.254.159 with 32 bytes of data:
Reply from 10.66.254.159: bytes=32 time<6ms TTL=128
```



Use Common Utilities to Establish a Relative Performance Baseline for the Network

- Use the output of the traceroute command, saved into logs, and repeated over time, to establish relative network performance

Capturing Trace Route

```
C:\>tracert www.cisco.com

Tracing route to www.cisco.com [198.133.219.25]
over a maximum of 30 hops:

 1      1 ms     <1 ms     <1 ms  192.168.0.1
 2     20 ms     20 ms     20 ms  nexthop.wa.ii.net [203.59.14.16]
 3     20 ms     19 ms     20 ms  gi2-4.per-qvl-bdr1.ii.net [203.215.4.32]
 4     79 ms     78 ms     78 ms  gi0-14-0-0.syd-ult-core1.ii.net [203.215.20.2]
 5     79 ms     81 ms     79 ms  202.139.19.33
 6    227 ms    228 ms    227 ms  203.208.148.17
 7    227 ms    227 ms    227 ms  203.208.149.34
 8    225 ms    225 ms    226 ms  208.30.205.145
 9    236 ms    249 ms    233 ms  sl-bb23-ana-8-0-0.sprintlink.net [144.232.9.23]

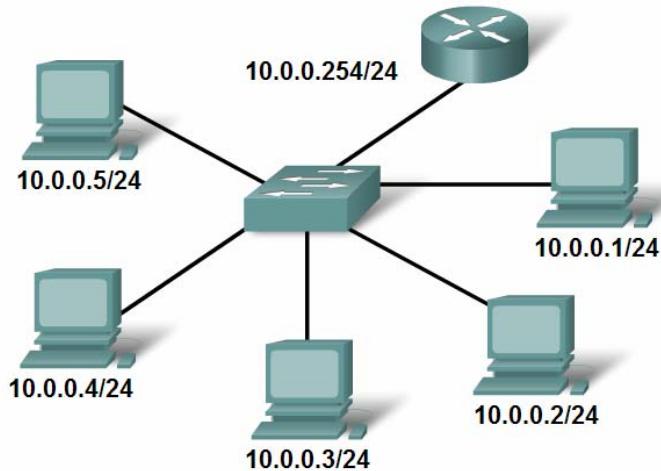
10   241 ms    244 ms    240 ms  sl-bb25-sj-9-0.sprintlink.net [144.232.20.159]
11   238 ms    238 ms    239 ms  sl-gw8-sj-10-0.sprintlink.net [144.232.3.114]
12   238 ms    239 ms    240 ms  144.228.44.14
13   240 ms    242 ms    248 ms  sjce-dmzbb-gwl.cisco.com [128.107.239.89]
```

Sample trace output

Use Common Utilities to Establish a Relative Performance Baseline for the Network

- Trace the steps for verifying the physical addresses of the hosts

Learning About the Nodes on the Network



C:\ >arp -a		
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

IP- MAC Address Pair

Use Common Utilities to Establish a Relative Performance Baseline for the Network

- Switch MAC address table

Switch Connections			
Mac Address Table			
Vlan	Mac Address	Type	Ports
All	0014.a8a8.8780	STATIC	CPU
All	0100.0ccc.cccc	STATIC	CPU
All	0100.0ccccccc	STATIC	CPU
All	0100.0cdd.dddd	STATIC	CPU
1	0001.e640.3b4b	DYNAMIC	Fa0/23
1	0002.fde1.6acb	DYNAMIC	Fa0/14
1	0006.5b88.dfc4	DYNAMIC	Gi0/2
1	0006.5bdd.6fee	DYNAMIC	Fa0/23
1	0006.5bdd.7035	DYNAMIC	Fa0/23
1	0006.5bdd.72fd	DYNAMIC	Fa0/23
1	0006.5bdd.73b0	DYNAMIC	Fa0/23
1	000e.0cb6.2b51	DYNAMIC	Fa0/2
1	000f.8f28.b7b5	DYNAMIC	Fa0/18
1	0011.1165.8acf	DYNAMIC	Fa0/1
1	0013.720b.40c3	DYNAMIC	Fa0/19
1	0080.9120.1766	DYNAMIC	Fa0/8
1	00a0.c949.702a	DYNAMIC	Fa0/15
1	00c0.b770.6c10	DYNAMIC	Fa0/22

Table showing MAC addresses connected to switch interfaces

Multiple devices
connected to Fa0/23

Summary

In this chapter, you learned to:

- Define the role of the Internetwork Operating System (IOS).
- Define the purpose of a configuration file.
- Identify several classes of devices that have the IOS embedded.
- Identify the factors contributing to the set of IOS commands available to a device.
- Identify the IOS modes of operation.
- Identify the basic IOS commands.
- Compare and contrast the basic show commands.

