Cisco Certified Network Associate
CCNA 640-802

Assist.Prof.It-arun Pitimon
Itarun.p@cpe.rmutt.ac.th

Cisco | Networking Academy®
Mind Wide Open™

DAY 1

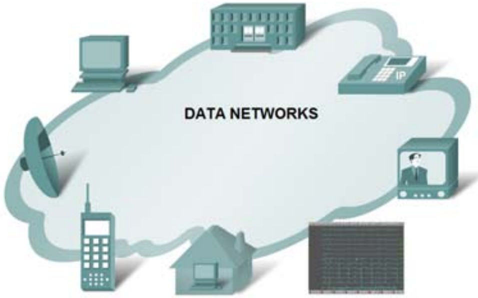
Agenda

- Network Fundamentals
- Transport Layer
- Network Layer
- Data Link Layer
- Physical Layer
- Ethernet and ARP
- Configuring and Testing your Network

NETWORK FUNDAMENTALS

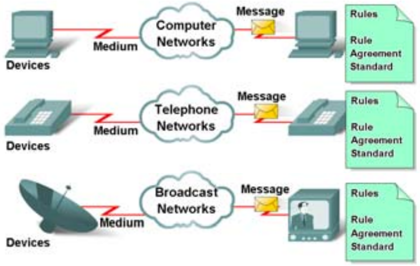
Data Networking Role, Components, and Challenges

- Describe the role of data networking in communications



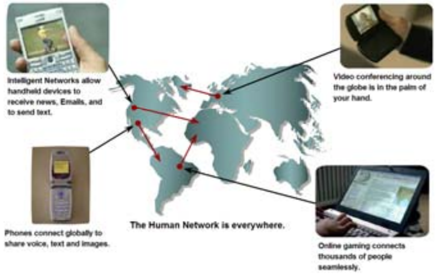
Data Networking Role, Components, and Challenges

- Describe the 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

- Describe the role of converged networks in communications
  - –Converged network
    - • A type of network that can carry voice, video & data over the same network



Intelligent Networks allow handheld devices to receive news, Emails, and to send text.

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

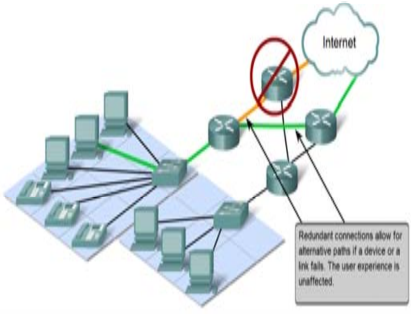
Phones connect globally to share voice, text and images.

The Human Network is everywhere.

Online gaming connects thousands of people seamlessly.

Network Architecture Characteristics

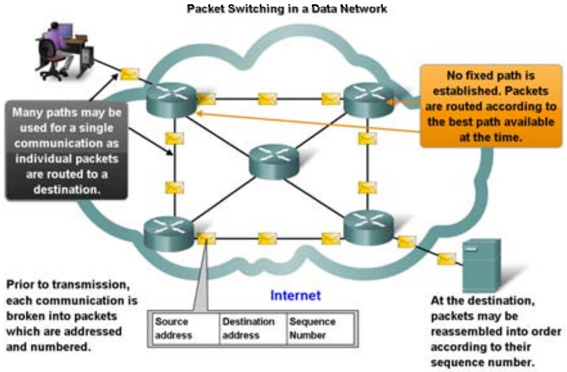
- Explain four characteristics that are addressed by network architecture design
  - –Fault tolerance
  - –Scalability
  - –Quality of service
  - –Security



Redundant connections allow for alternative paths if a device or a link fails. The user experience is unaffected.

Network Architecture Characteristics

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



Many paths may be used for a single communication as individual packets are routed to a destination.

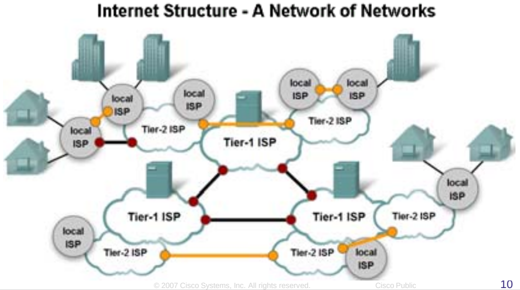
No fixed path is established. Packets are routed according to the best path available at the time.

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

At the destination, packets may be reassembled into order according to their sequence number.

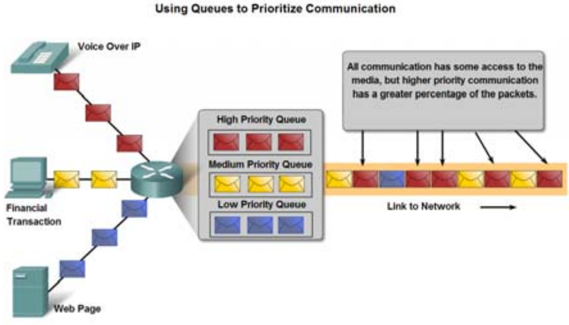
Network Architecture Characteristics

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



Network Architecture Characteristics

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

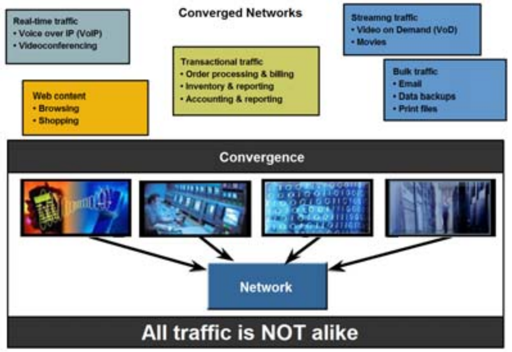


All communication has some access to the media, but higher priority communication has a greater percentage of the packets.

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

Network Architecture Characteristics

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



Real-time traffic
- Voice over IP (VoIP)
- Videoconferencing

Web content
- Browsing
- Shopping

Transactional traffic
- Order processing & billing
- Inventory & reporting
- Accounting & reporting

Streamng traffic
- Video on Demand (VoD)
- Movies

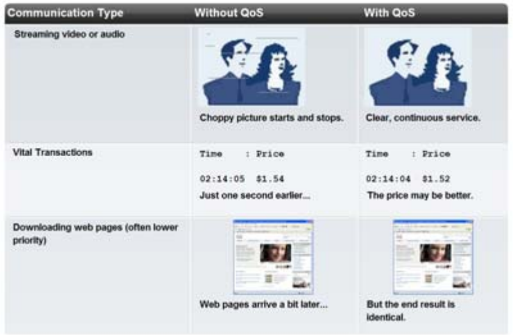
Bulk traffic
- Email
- Data backups
- Print files

All traffic is NOT alike

Network Architecture Characteristics

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

Quality of Service Matters

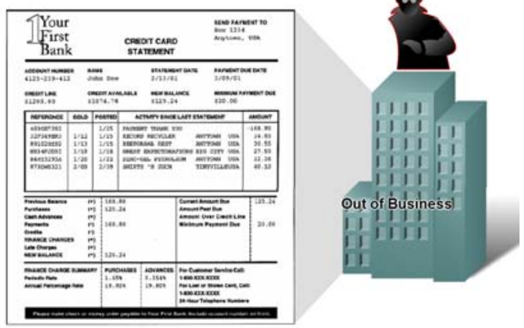


Communication Type	Without QoS	With QoS
Streaming video or audio	Choppy picture starts and stops.	Clear, continuous service.
Vital Transactions	Time : Price 02:14:05 $1.54 Just one second earlier...	Time : Price 02:14:04 $1.52 The price may be better.
Downloading web pages (often lower priority)	Web pages arrive a bit later...	But the end result is identical.

Network Architecture Characteristics

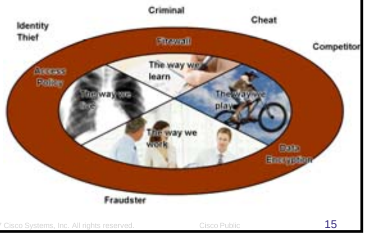
- Describe why networks must be secure

Unauthorized Transactions



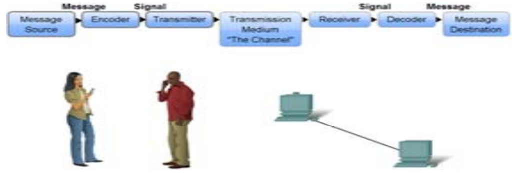
Network Architecture Characteristics

- Describe 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



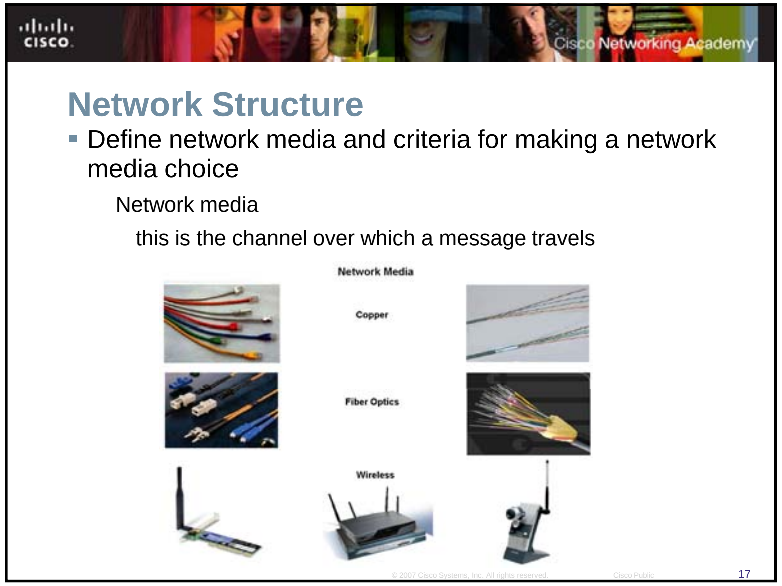
Network Structure

- 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

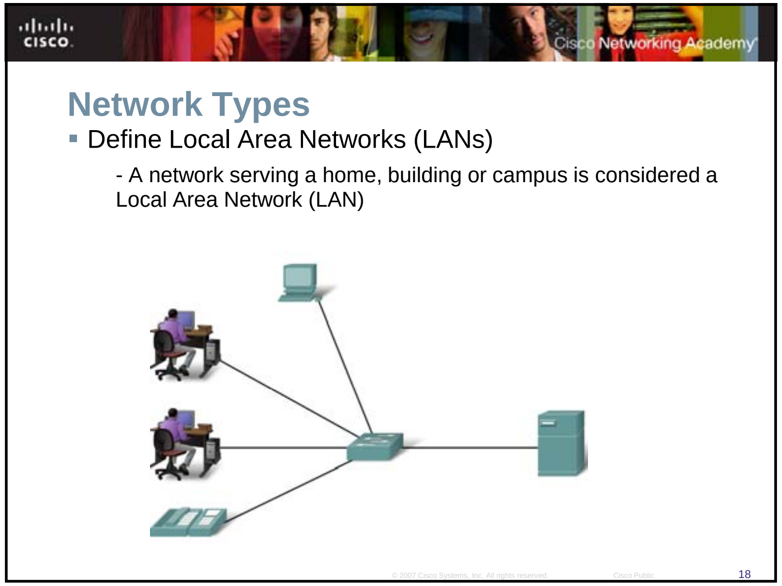


Network Structure

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

  Network media

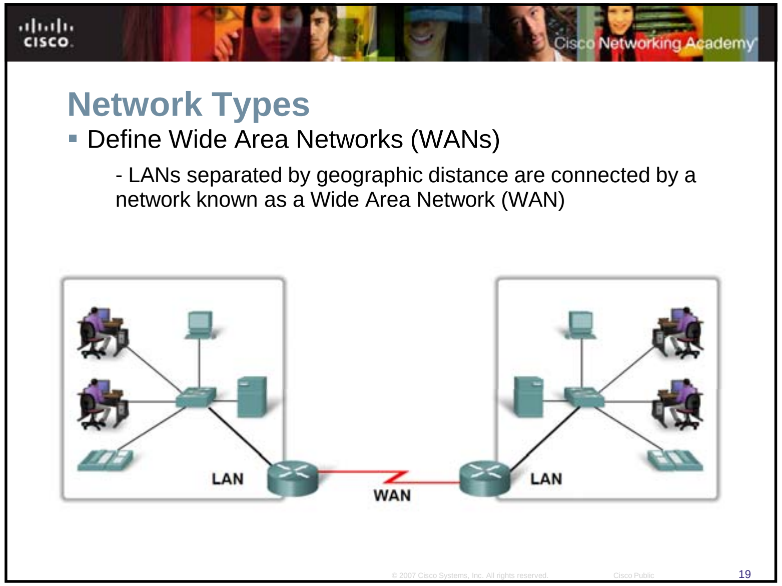
  this is the channel over which a message travels



Network Types

- Define Local Area Networks (LANs)

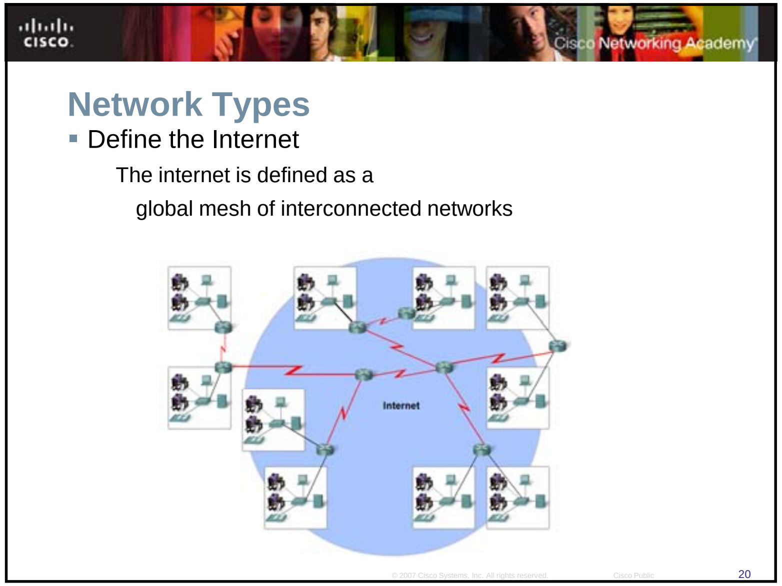
  - A network serving a home, building or campus is considered a Local Area Network (LAN)



Network Types

- Define Wide Area Networks (WANs)

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

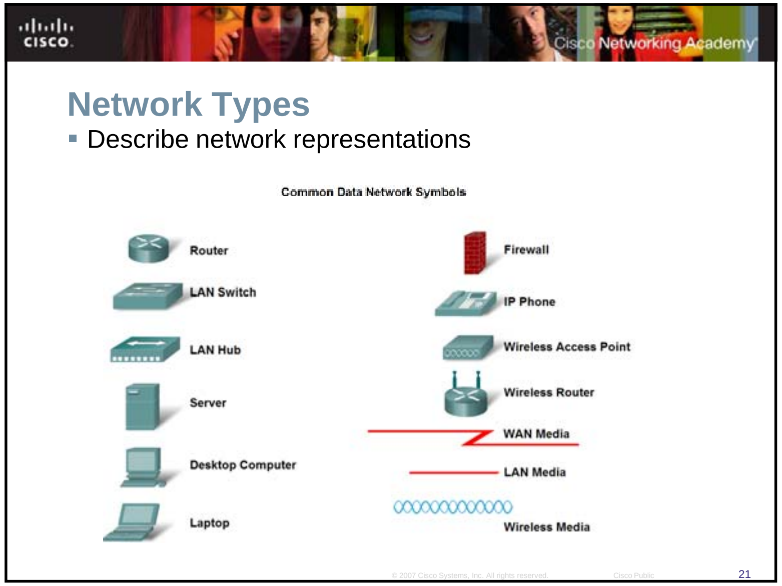


Network Types

- Define the Internet

  The internet is defined as a

  global mesh of interconnected networks



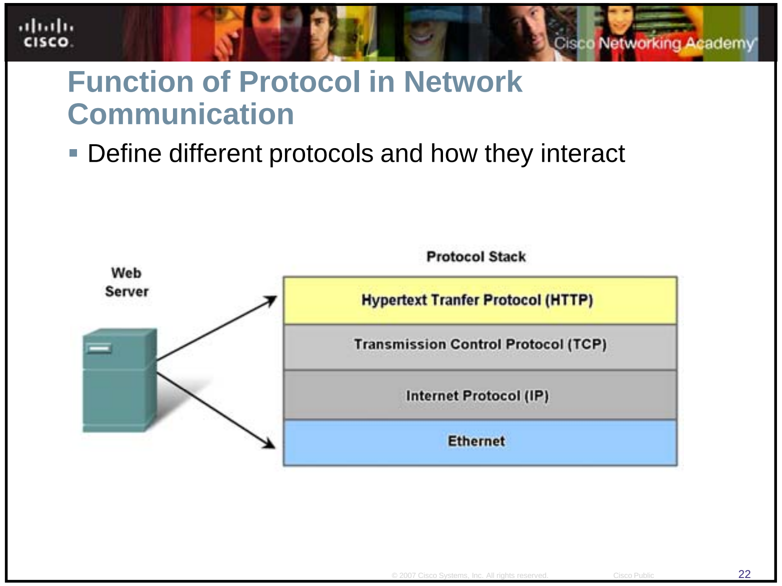
Cisco Networking Academy

Network Types

- Describe network representations

Common Data Network Symbols

Router
LAN Switch
LAN Hub
Server
Desktop Computer
Laptop
Firewall
IP Phone
Wireless Access Point
Wireless Router
WAN Media
LAN Media
Wireless Media



Cisco Networking Academy

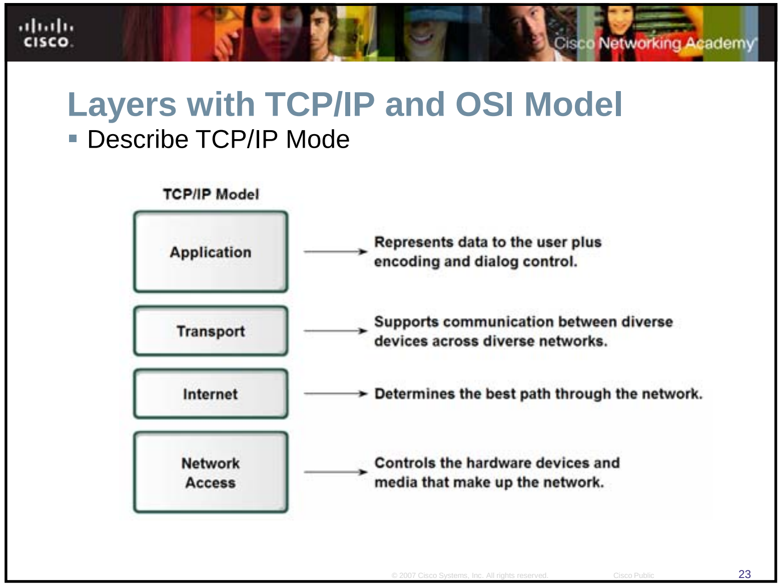
Function of Protocol in Network Communication

- Define different protocols and how they interact

Web Server

Protocol Stack

Protocol Stack
Hypertext Tranfer Protocol (HTTP)
Transmission Control Protocol (TCP)
Internet Protocol (IP)
Ethernet



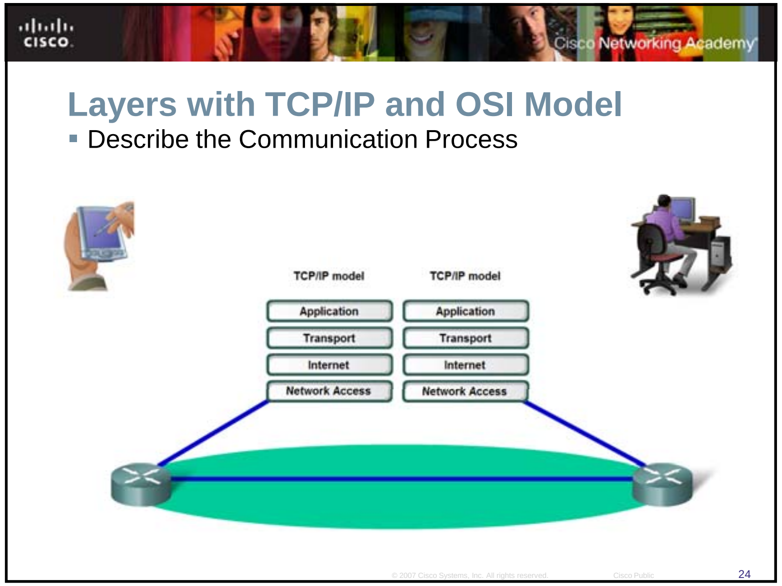
Cisco Networking Academy

Layers with TCP/IP and OSI Model

- Describe TCP/IP Mode

TCP/IP Model

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



Cisco Networking Academy

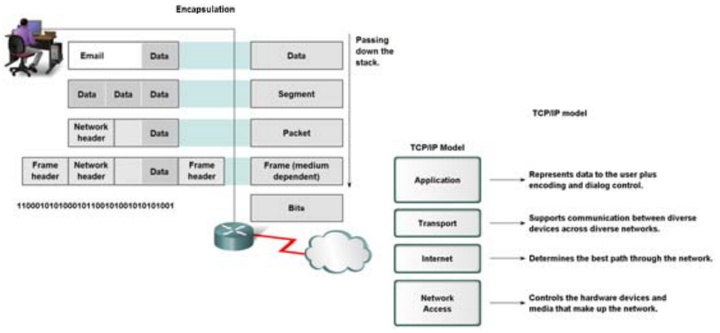
Layers with TCP/IP and OSI Model

- Describe the Communication Process

TCP/IP model	TCP/IP model
Application	Application
Transport	Transport
Internet	Internet
Network Access	Network Access

Layers with TCP/IP and OSI Model

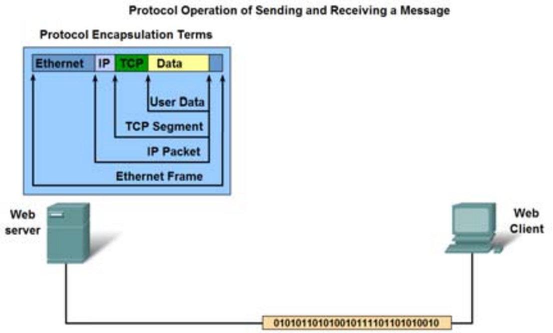
- Explain protocol data units (PDU) and encapsulation



Cisco Public

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
Ethernet
IP
TCP
Data
User Data
TCP Segment
IP Packet
Ethernet Frame
Web server
Web Client
01010110101001011110110101001O

Cisco Public

Layers with TCP/IP and OSI Model

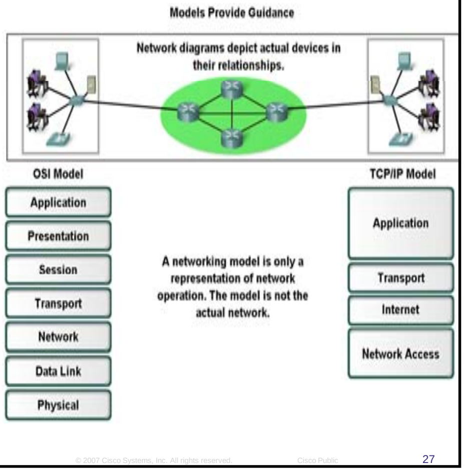
- Explain protocol and reference models

  A protocol model

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

  A reference model

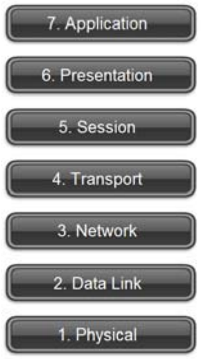
  provides a common reference for maintaining consistency within all types of network protocols and services.


Models Provide Guidance
Network diagrams depict actual devices in their relationships.
OSI Model
Application
Presentation
Session
Transport
Network
Data Link
Physical
A networking model is only a representation of network operation. The model is not the actual network.
TCP/IP Model
Application
Transport
Internet
Network Access

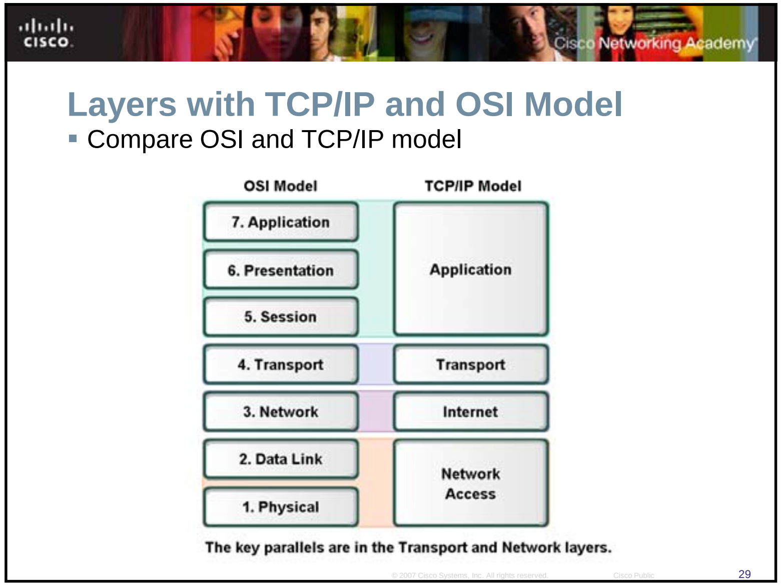
Cisco Public

Layers with TCP/IP and OSI Model

- Define OSI



Cisco Public

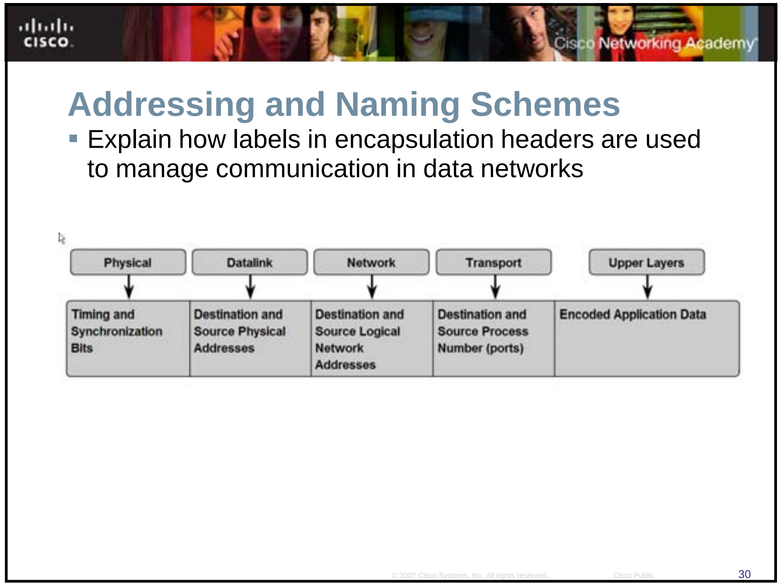


Layers with TCP/IP and OSI Model

- Compare OSI and TCP/IP model

OSI Model	TCP/IP Model
7. Application	Application
6. Presentation	
5. Session	
4. Transport	Transport
3. Network	Internet
2. Data Link	Network Access
1. Physical	

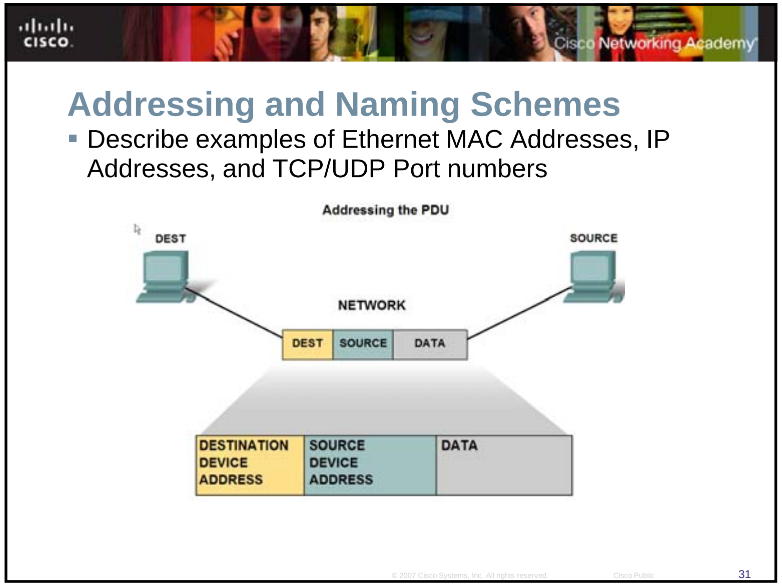
The key parallels are in the Transport and Network layers.



Addressing and Naming Schemes

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

Physical	Datalink	Network	Transport	Upper Layers
Timing and Synchronization Bits	Destination and Source Physical Addresses	Destination and Source Logical Network Addresses	Destination and Source Process Number (ports)	Encoded Application Data

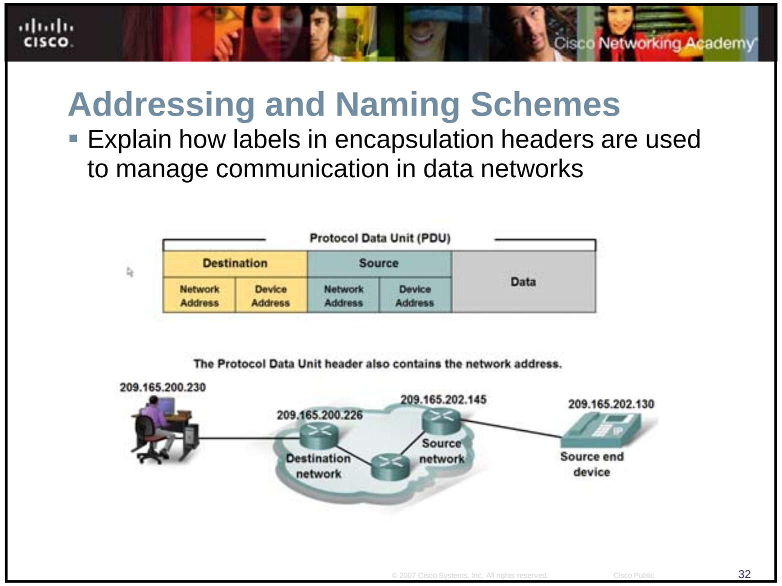


Addressing and Naming Schemes

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

Addressing the PDU

DESTINATION DEVICE ADDRESS	SOURCE DEVICE ADDRESS	DATA



Addressing and Naming Schemes

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

Protocol Data Unit (PDU)

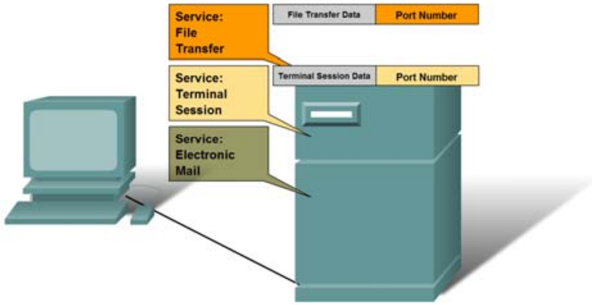
Destination		Source		Data
Network Address	Device Address	Network Address	Device Address	

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.

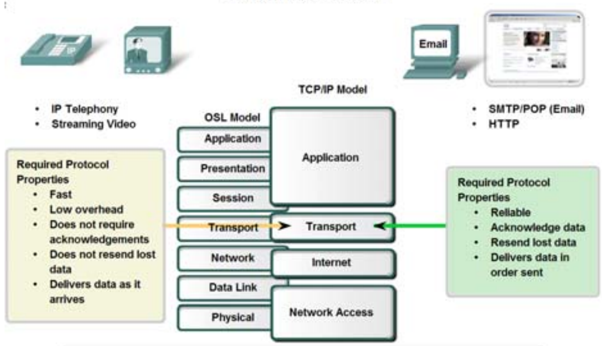


TRANSPORT LAYER

Transport Layer Role and Services

- Supporting Reliable Communication

Transport Layer Protocols

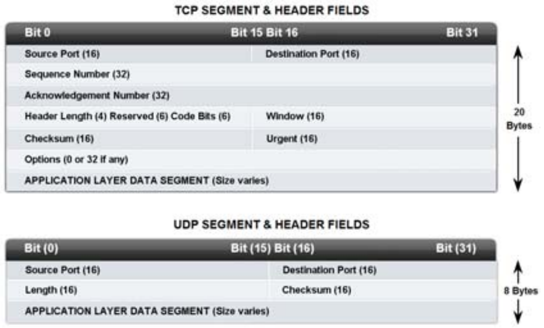


Application developers choose the appropriate Transport Layer protocol based on the nature of the application.

Transport Layer Role and Services

- Identify the basic characteristics of the UDP and TCP protocols

TCP and UDP Headers

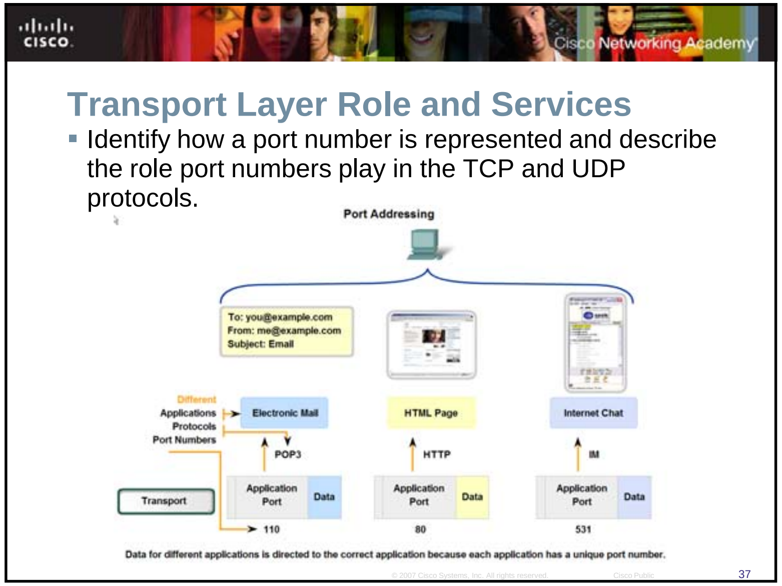


TCP SEGMENT & HEADER FIELDS

Bit 0	Bit 15 Bit 16	Bit 31
Source Port (16)	Destination Port (16)	20 Bytes
Sequence Number (32)		
Acknowledgement Number (32)		
Header Length (4) Reserved (6) Code Bits (6)	Window (16)	
Checksum (16)	Urgent (16)	
Options (0 or 32 if any)		
APPLICATION LAYER DATA SEGMENT (Size varies)		

UDP SEGMENT & HEADER FIELDS

Bit (0)	Bit (15) Bit (16)	Bit (31)
Source Port (16)	Destination Port (16)	8 Bytes
Length (16)	Checksum (16)	
APPLICATION LAYER DATA SEGMENT (Size varies)		



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.

Port Addressing

To: you@example.com
From: me@example.com
Subject: Email

Different
Applications
Protocols
Port Numbers

Electronic Mail

HTML Page

Internet Chat

POP3

HTTP

IM

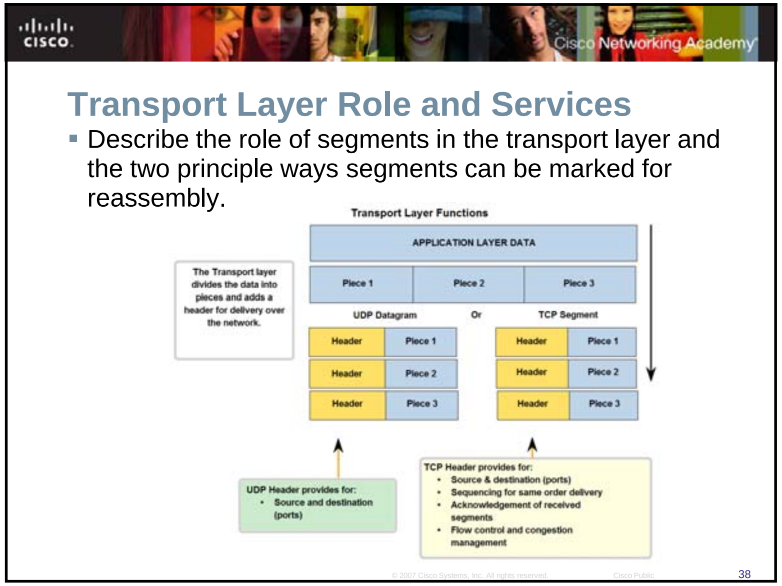
Transport

Application Port | Data
110

Application Port | Data
80

Application Port | Data
531

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



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.

Transport Layer Functions

APPLICATION LAYER DATA

Piece 1 | Piece 2 | Piece 3

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

UDP Datagram

Header | Piece 1
Header | Piece 2
Header | Piece 3

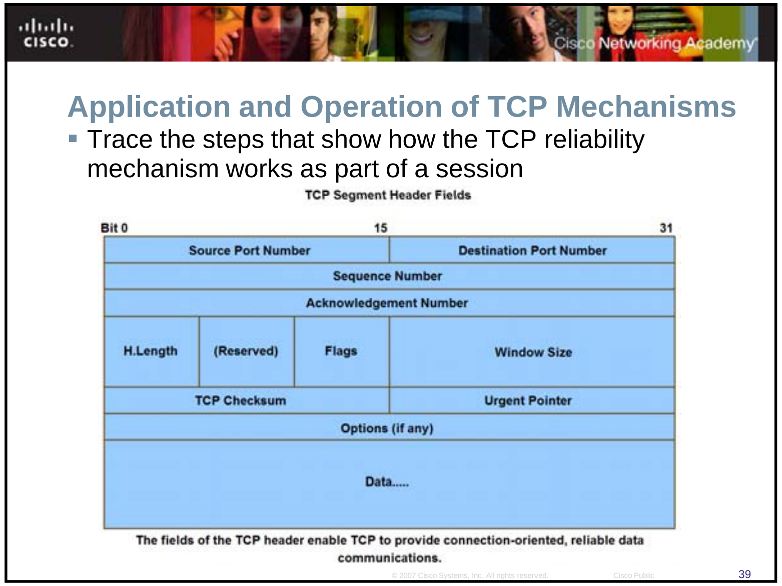
Or

TCP Segment

Header | Piece 1
Header | Piece 2
Header | Piece 3

UDP Header provides for:
- Source and destination (ports)

TCP Header provides for:
- Source & destination (ports)
- Sequencing for same order delivery
- Acknowledgement of received segments
- Flow control and congestion management



Application and Operation of TCP Mechanisms

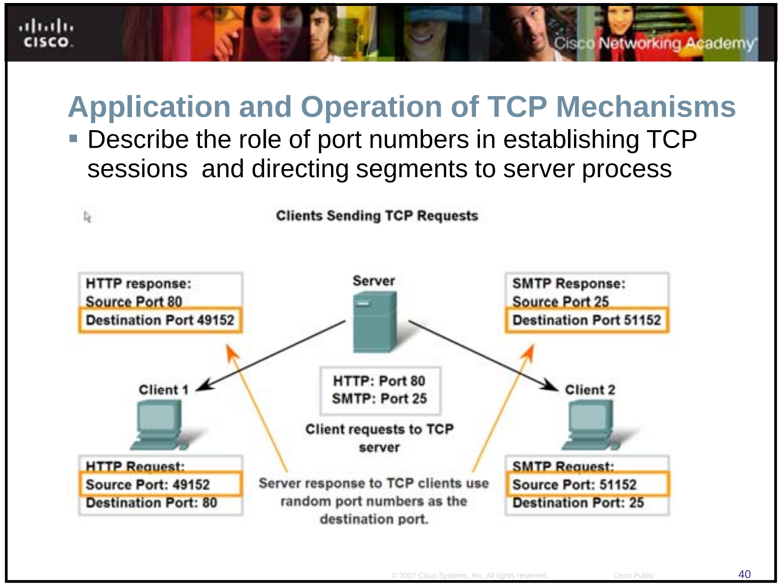
- Trace the steps that show how the TCP reliability mechanism works as part of a session

TCP Segment Header Fields

Bit 0 15 31

Source Port Number | Destination Port Number
Sequence Number
Acknowledgement Number
H.Length | (Reserved) | Flags | Window Size
TCP Checksum | Urgent Pointer
Options (if any)
Data.....

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



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

HTTP response:
Source Port 80
Destination Port 49152

Server

SMTP Response:
Source Port 25
Destination Port 51152

HTTP: Port 80
SMTP: Port 25

Client 1

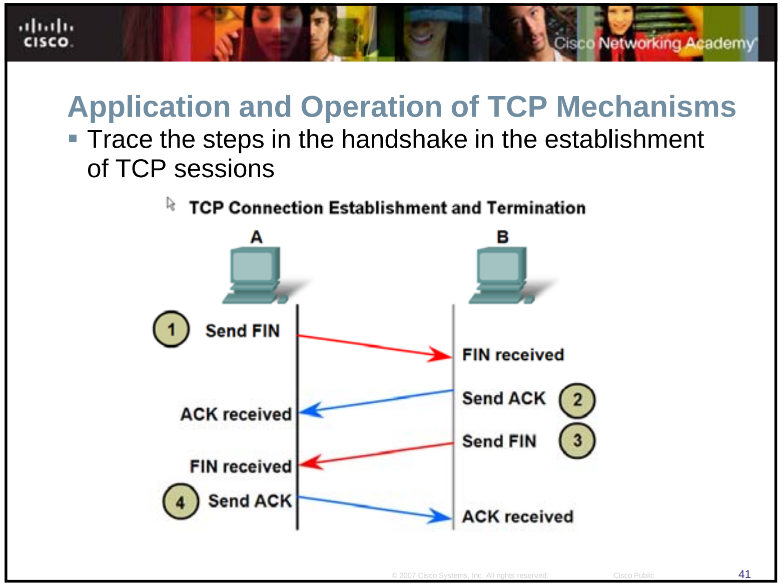
Client requests to TCP server

Client 2

HTTP Request:
Source Port: 49152
Destination Port: 80

Server response to TCP clients use random port numbers as the destination port.

SMTP Request:
Source Port: 51152
Destination Port: 25



Application and Operation of TCP Mechanisms

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

TCP Connection Establishment and Termination

A

B

1 Send FIN

FIN received

Send ACK 2

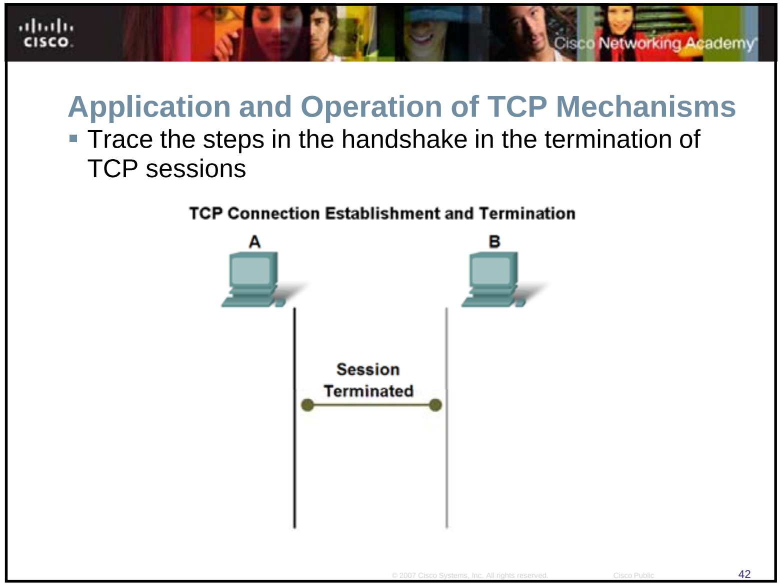
ACK received

Send FIN 3

FIN received

4 Send ACK

ACK received



Application and Operation of TCP Mechanisms

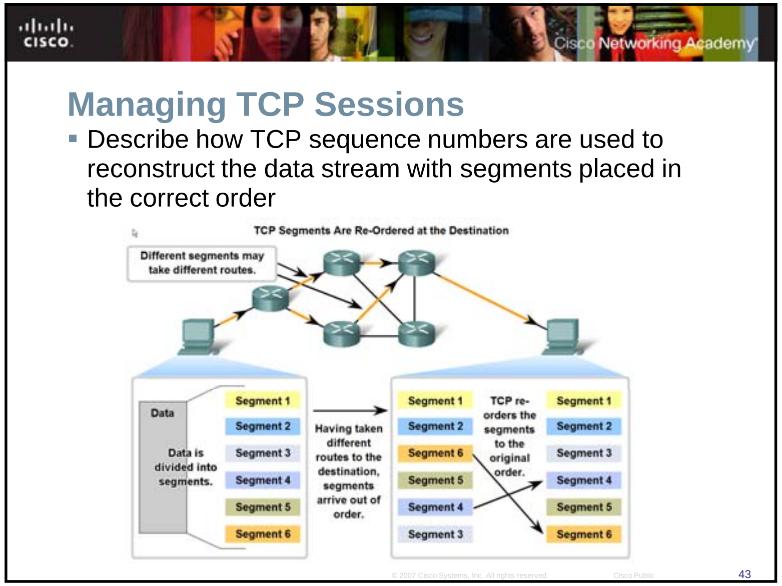
- Trace the steps in the handshake in the termination of TCP sessions

TCP Connection Establishment and Termination

A

B

Session Terminated



Managing TCP Sessions

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

TCP Segments Are Re-Ordered at the Destination

Different segments may take different routes.

Data

Data is divided into segments.

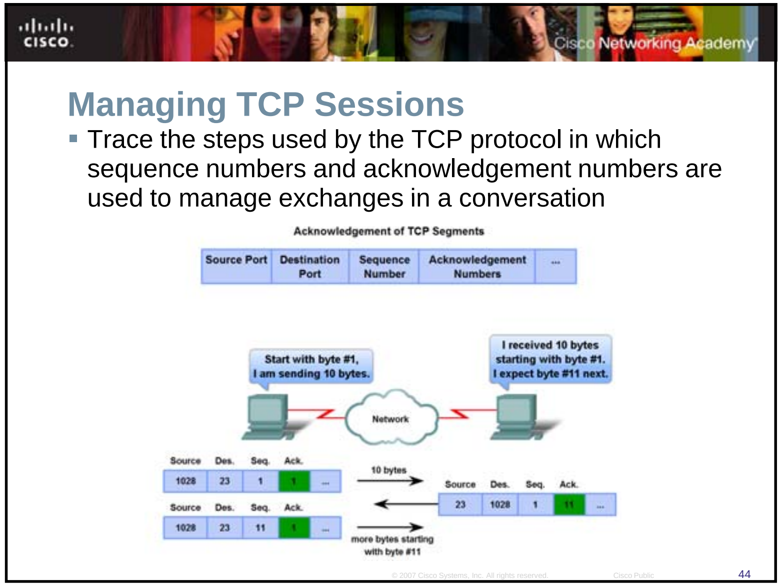
Segment 1
Segment 2
Segment 3
Segment 4
Segment 5
Segment 6

Having taken different routes to the destination, segments arrive out of order.

Segment 1
Segment 2
Segment 6
Segment 5
Segment 4
Segment 3

TCP re-orders the segments to the original order.

Segment 1
Segment 2
Segment 3
Segment 4
Segment 5
Segment 6



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

Acknowledgement of TCP Segments

Source Port	Destination Port	Sequence Number	Acknowledgement Numbers	...

Start with byte #1, I am sending 10 bytes.

I received 10 bytes starting with byte #1. I expect byte #11 next.

Network

Source	Des.	Seq.	Ack.	
1028	23	1	1	...

10 bytes →

Source	Des.	Seq.	Ack.	
23	1028	1	11	...

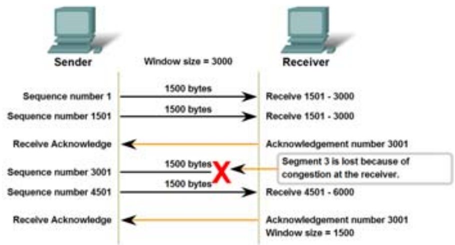
Source	Des.	Seq.	Ack.	
1028	23	11	1	...

more bytes starting with byte #11

Managing TCP Sessions

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

TCP Congestion and Flow Control

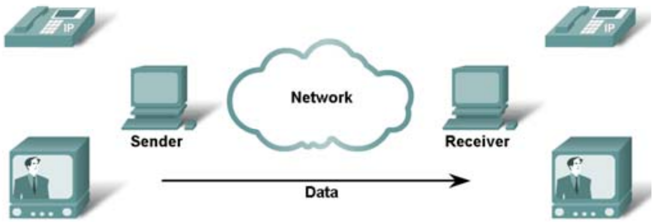


If segments are lost because of congestion, the Receiver will acknowledge the last received sequential segment and reply with a reduced window size.

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

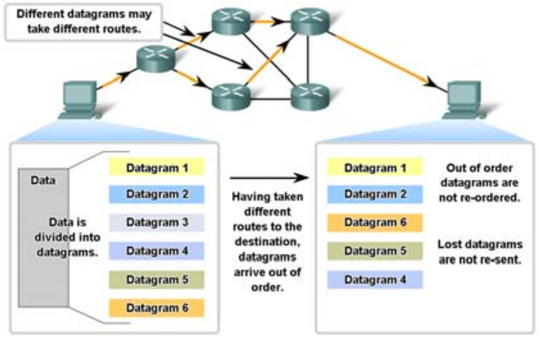


UDP does not establish a connection before sending data.

UDP Protocol

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

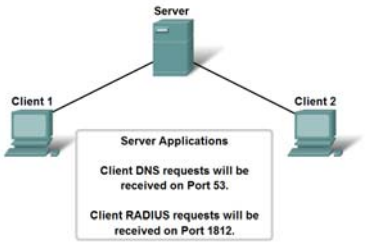
UDP: Connectionless and Unreliable


Different datagrams may take different routes.
Data
Data is divided into datagrams.
Datagram 1
Datagram 2
Datagram 3
Datagram 4
Datagram 5
Datagram 6
Having taken different routes to the destination, datagrams arrive out of order.
Datagram 1
Datagram 2
Datagram 6
Datagram 5
Datagram 4
Out of order datagrams are not re-ordered.
Lost datagrams are not re-sent.

UDP Protocol

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

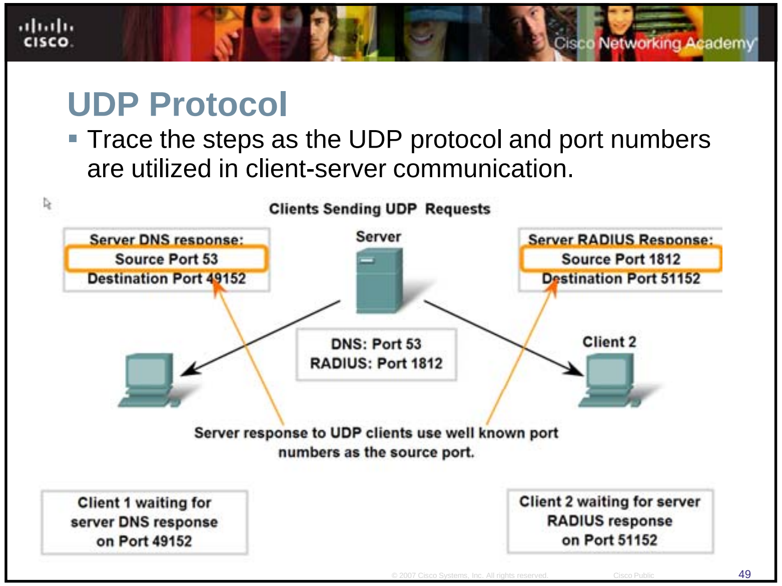
UDP Server Listening for Requests



Client DNS requests will be received on Port 53.

Client RADIUS requests will be received on Port 1812.

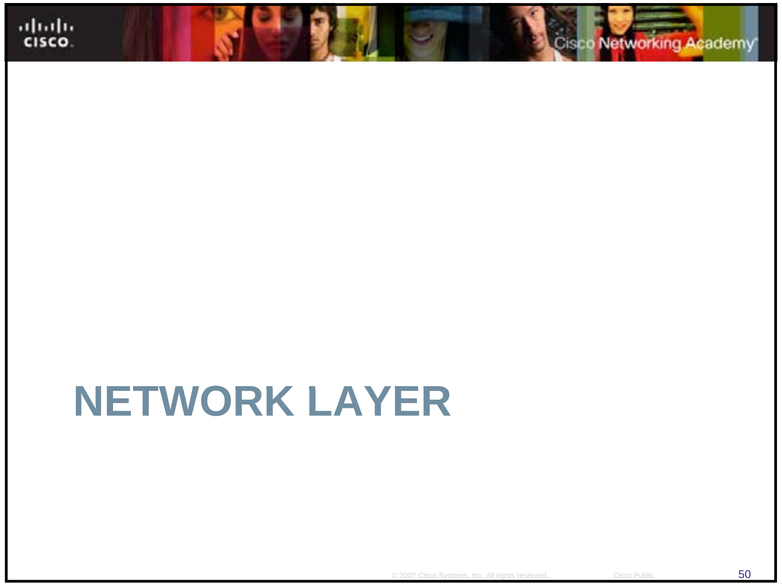
Client requests to servers have well known ports numbers as the destination port.



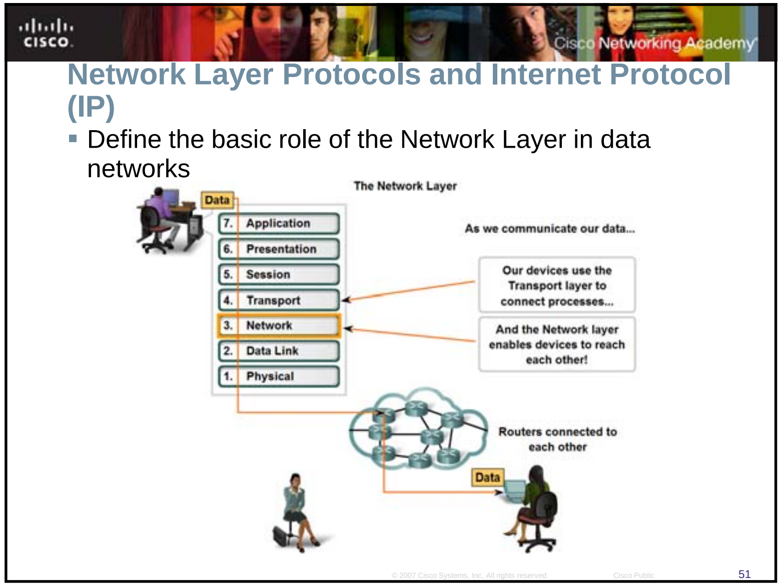
UDP Protocol

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

Clients Sending UDP Requests
Server DNS response:
Source Port 53
Destination Port 49152
Server
Server RADIUS Response:
Source Port 1812
Destination Port 51152
DNS: Port 53
RADIUS: Port 1812
Client 2
Server response to UDP clients use well known port numbers as the source port.
Client 1 waiting for server DNS response on Port 49152
Client 2 waiting for server RADIUS response on Port 51152



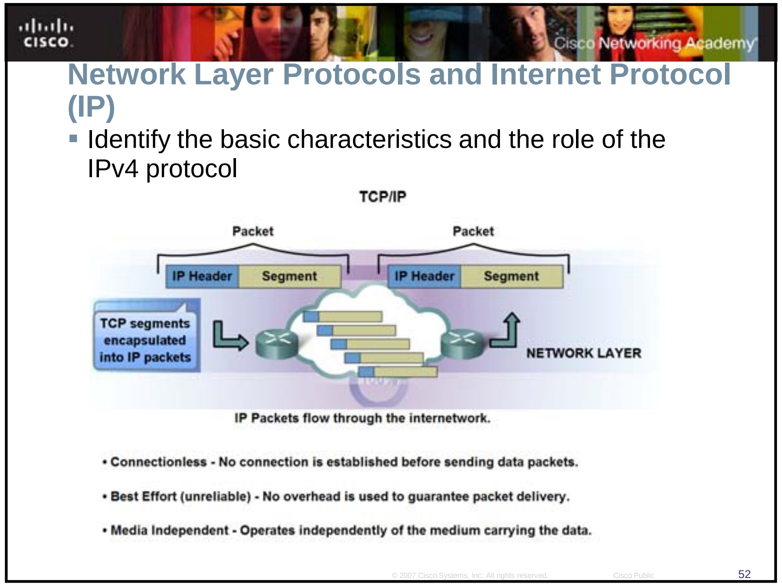
NETWORK LAYER



Network Layer Protocols and Internet Protocol (IP)

- Define the basic role of the Network Layer in data networks

The Network Layer
Data
7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Data Link
1. Physical
As we communicate our data...
Our devices use the Transport layer to connect processes...
And the Network layer enables devices to reach each other!
Routers connected to each other
Data

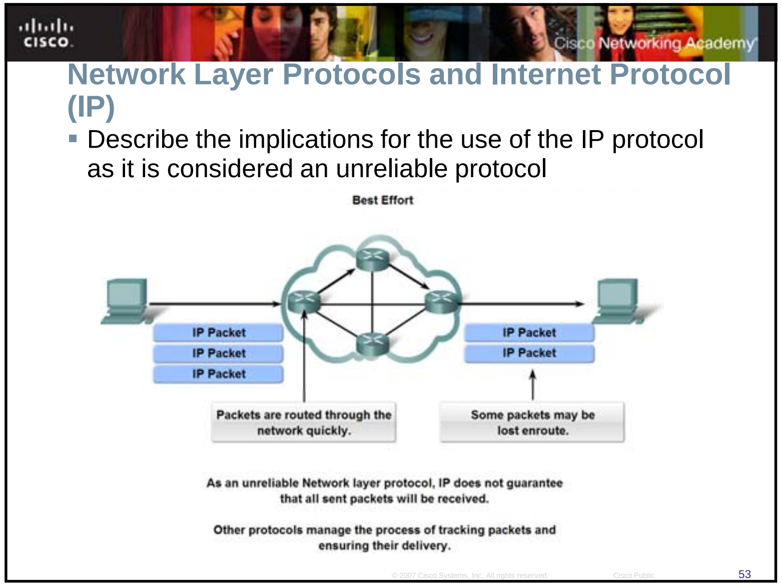


Network Layer Protocols and Internet Protocol (IP)

- Identify the basic characteristics and the role of the IPv4 protocol

IP Packets flow through the internetwork.

- 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)

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

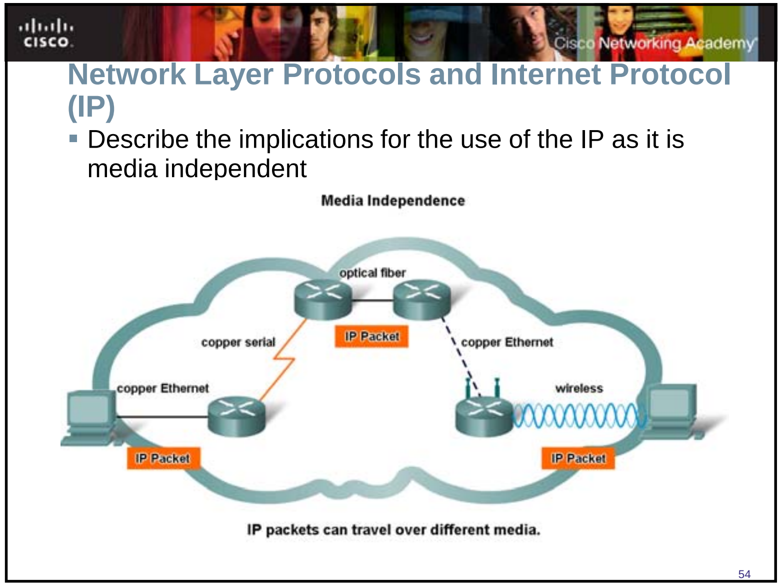
Best Effort

Packets are routed through the network quickly.

Some packets may be lost enroute.

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.

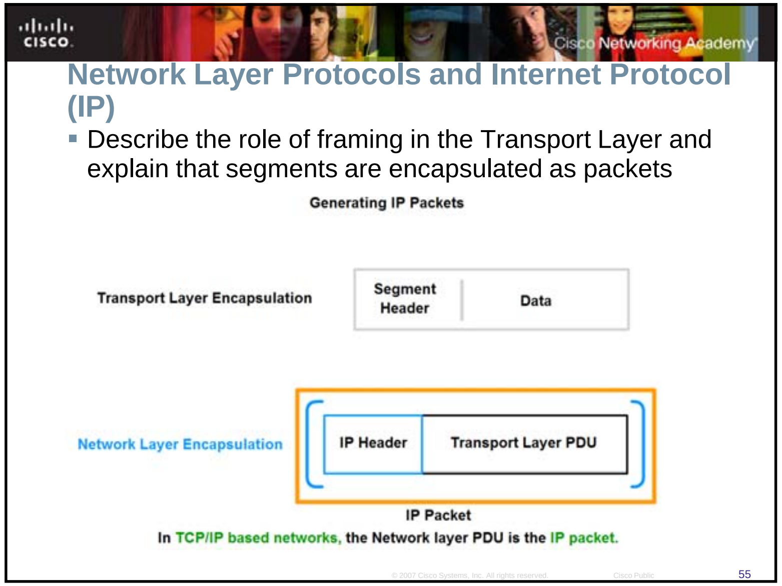


Network Layer Protocols and Internet Protocol (IP)

- Describe the implications for the use of the IP as it is media independent

Media Independence

IP packets can travel over different media.



Network Layer Protocols and Internet Protocol (IP)

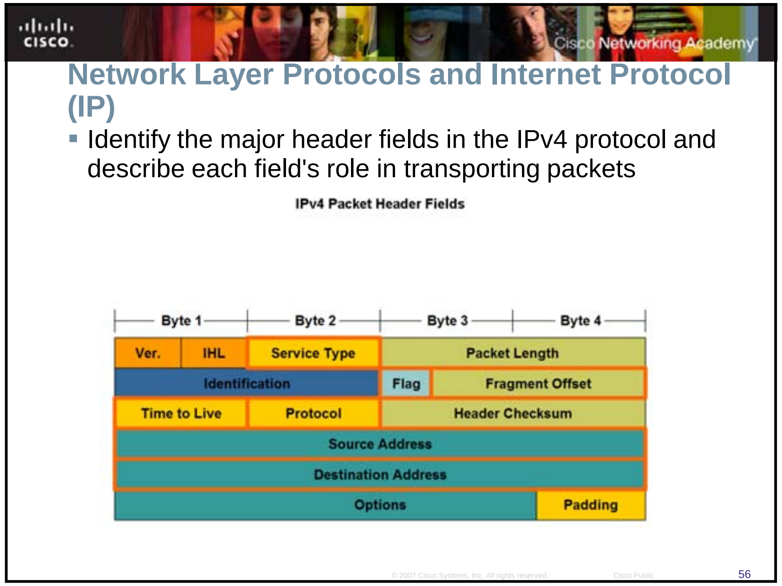
- Describe the role of framing in the Transport Layer and explain that segments are encapsulated as packets

Generating IP Packets

Transport Layer Encapsulation

Network Layer Encapsulation

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



Network Layer Protocols and Internet Protocol (IP)

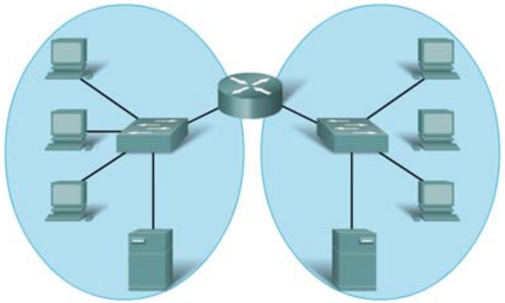
- Identify the major header fields in the IPv4 protocol and describe each field's role in transporting packets

IPv4 Packet Header Fields

<table>
<tr><th colspan="2">Byte 1</th><th colspan="2">Byte 2</th><th colspan="2">Byte 3</th><th colspan="2">Byte 4</th></tr>
<tr><td>Ver.</td><td>IHL</td><td colspan="2">Service Type</td><td colspan="4">Packet Length</td></tr>
<tr><td colspan="4">Identification</td><td>Flag</td><td colspan="3">Fragment Offset</td></tr>
<tr><td colspan="2">Time to Live</td><td colspan="2">Protocol</td><td colspan="4">Header Checksum</td></tr>
<tr><td colspan="8">Source Address</td></tr>
<tr><td colspan="8">Destination Address</td></tr>
<tr><td colspan="6">Options</td><td colspan="2">Padding</td></tr>
</table>

Grouping Devices into Networks and Hierarchical Addressing

- List several ways in which dividing a large network can increase network performance

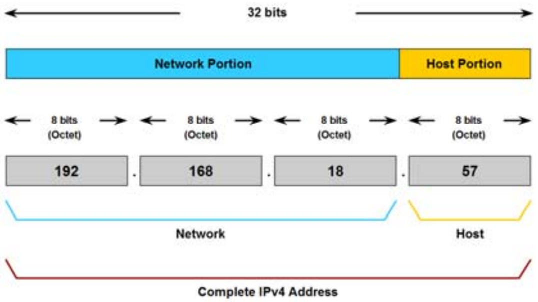


Replacing the middle switch with a router creates 2 IP subnets, hence, 2 distinct broadcast domains. All devices are connected but local broadcasts are contained.

Grouping Devices into Networks and Hierarchical Addressing

- Describe the purpose of further subdividing networks into smaller networks

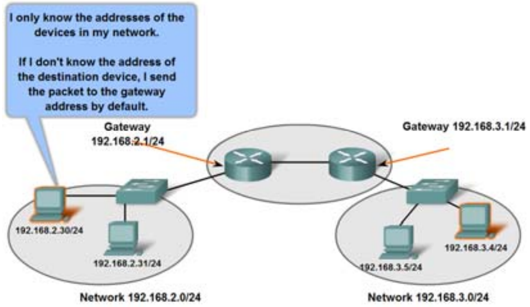
Hierarchical IPv4 Address



Fundamentals of Routes, Next Hop Addresses and Packet Forwarding

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

Gateways Enable Communications between Networks

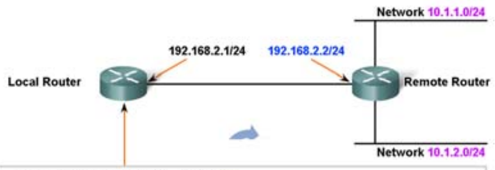

I only know the addresses of the devices in my network.

If I don't know the address of the destination device, I send the packet to the gateway address by default.
Gateway 192.168.2.1/24
Gateway 192.168.3.1/24
192.168.2.30/24
192.168.2.31/24
192.168.3.4/24
192.168.3.5/24
Network 192.168.2.0/24
Network 192.168.3.0/24

Fundamentals of Routes, Next Hop Addresses and Packet Forwarding

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

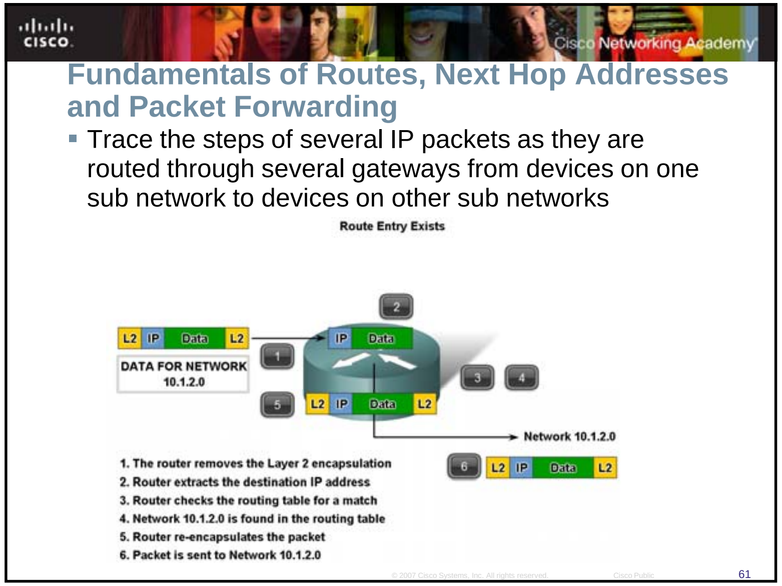
Confirming the Gateway and Route



```
   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
```

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.

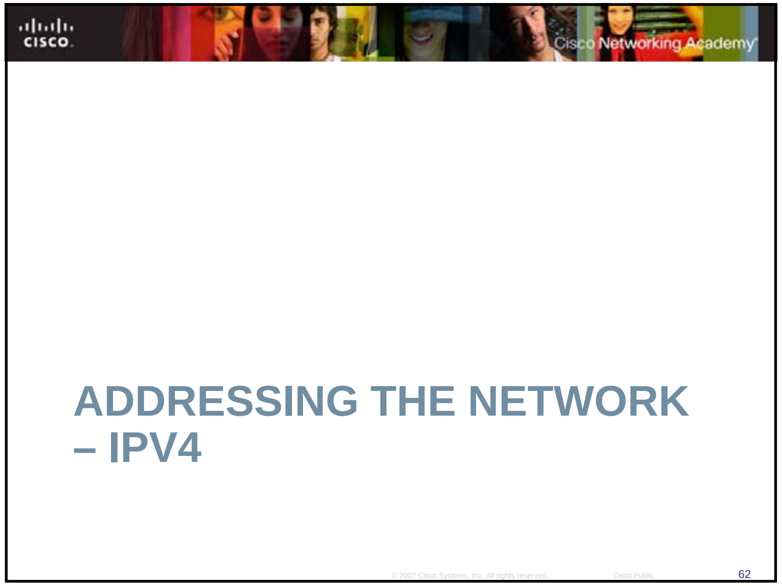


Fundamentals of Routes, Next Hop Addresses and Packet Forwarding

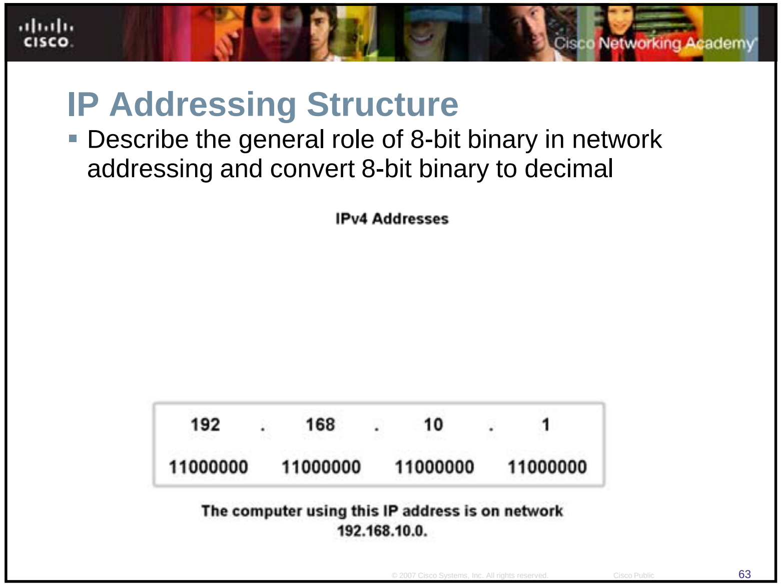
- Trace the steps of several IP packets as they are routed through several gateways from devices on one sub network to devices on other sub networks

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



ADDRESSING THE NETWORK – IPV4



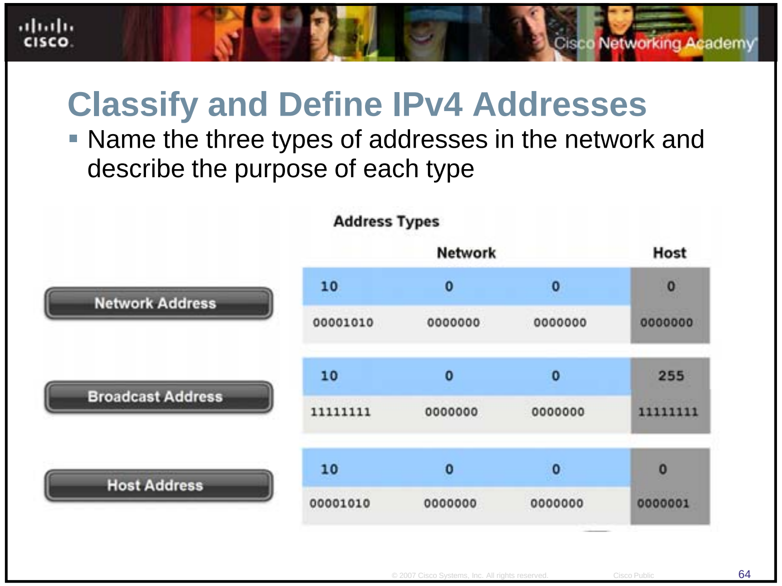
IP Addressing Structure

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

IPv4 Addresses

192	.	168	.	10	.	1
11000000		11000000		11000000		11000000

The computer using this IP address is on network 192.168.10.0.



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

- Determine the network, broadcast and host addresses for a given address and prefix combination

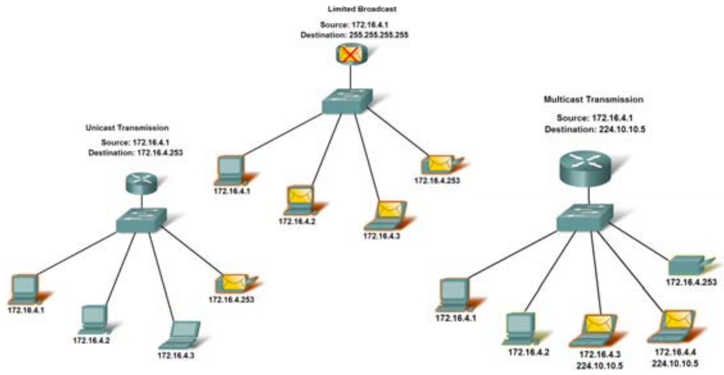
Given address/prefix of **183.26.103.215 /30**

For each row, enter the values ...

Type of Address	Enter LAST octet in binary	Enter LAST octet in decimal	Enter full address in decimal
Network			
Broadcast			
First Usable Host Address			
Last Usable Host Address			

Classify and Define IPv4 Addresses

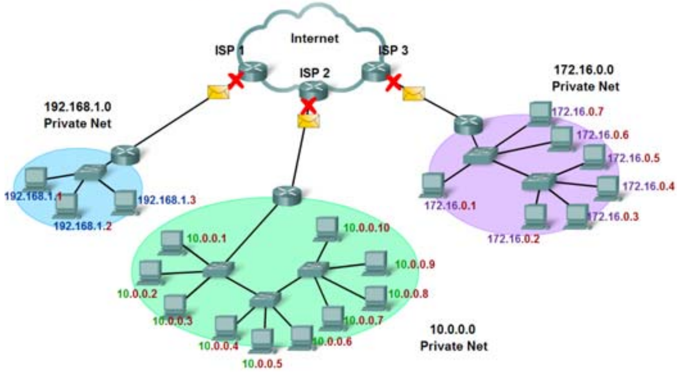
- Name the three types of communication in the Network Layer and describe the characteristics of each type



Classify and Define IPv4 Addresses

- Define public address and private address

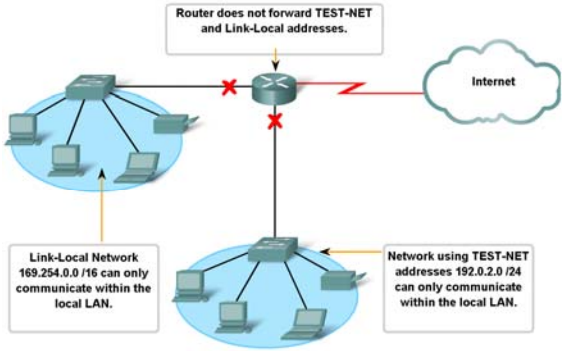
Private Addresses used in Networks without NAT



Classify and Define IPv4 Addresses

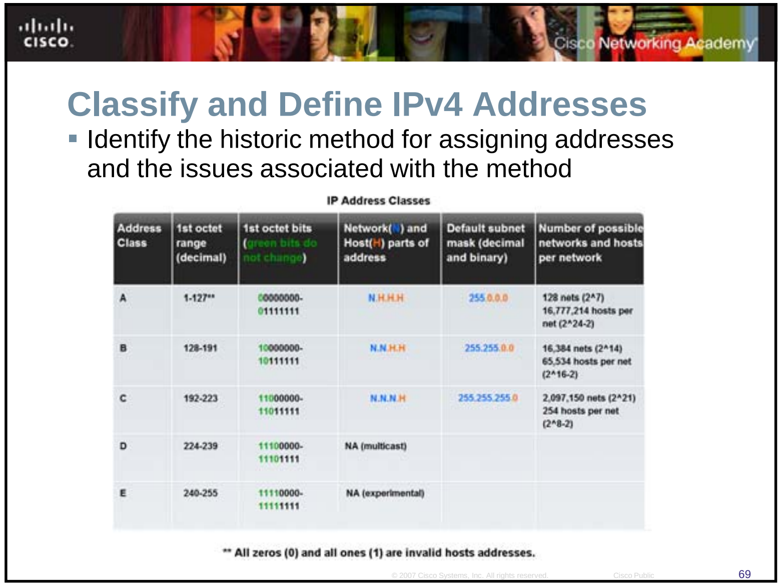
- Describe the purpose of several special addresses

Special IPv4 Addresses


Router does not forward TEST-NET and Link-Local addresses.

Link-Local Network 169.254.0.0 /16 can only communicate within the local LAN.

Network using TEST-NET addresses 192.0.2.0 /24 can only communicate within the local LAN.



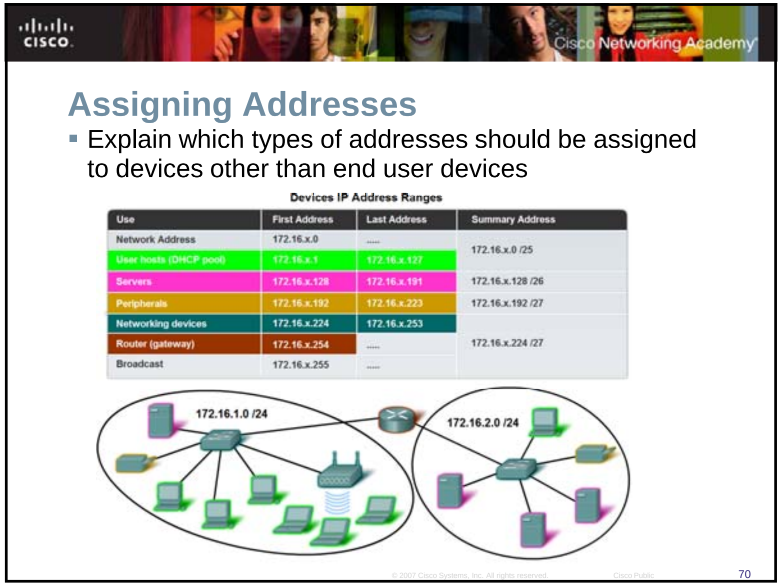
Classify and Define IPv4 Addresses

- 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.

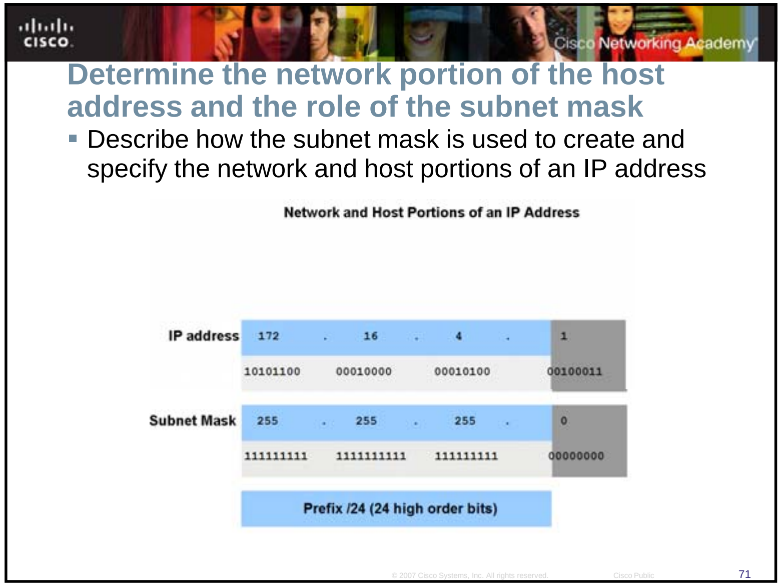


Assigning Addresses

- 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	......	172.16.x.0 /25
User hosts (DHCP pool)	172.16.x.1	172.16.x.127	
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	172.16.x.224 /27
Router (gateway)	172.16.x.254	......	
Broadcast	172.16.x.255	......	



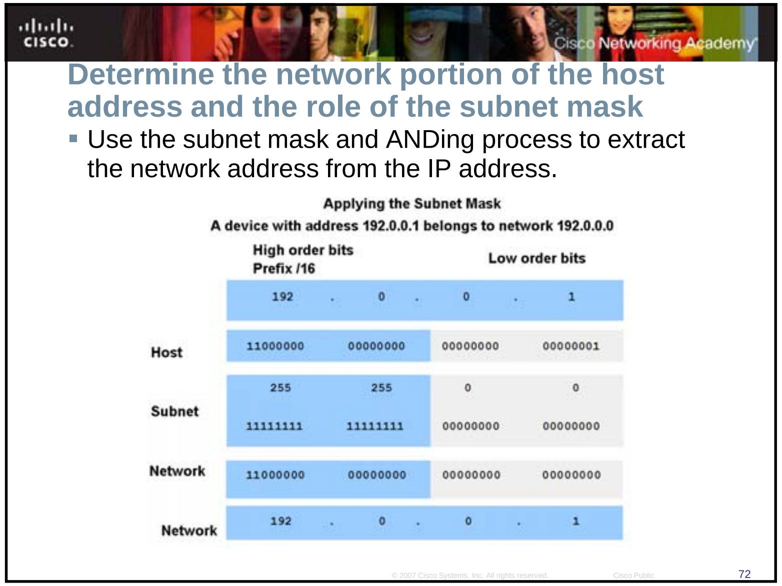
Determine the network portion of the host address and the role of the subnet mask

- 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
	111111111	1111111111	111111111	00000000

Prefix /24 (24 high order bits)



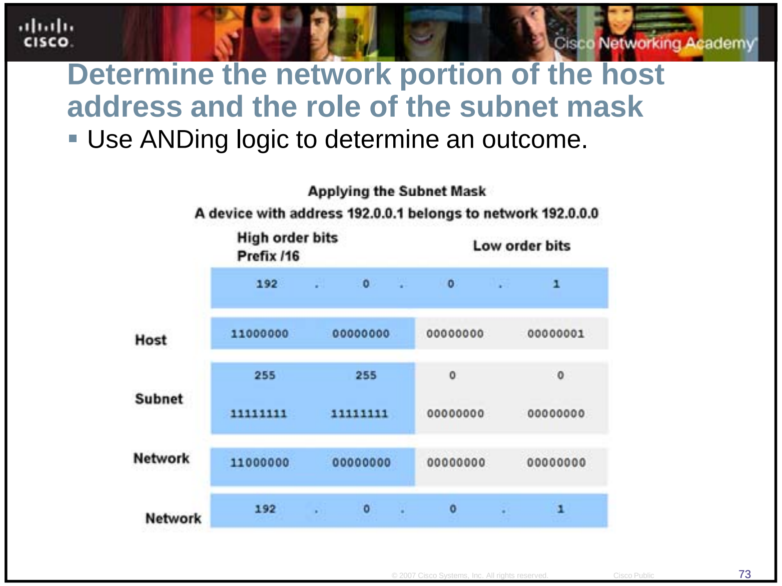
Determine the network portion of the host address and the role of the subnet mask

- 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	255	255	0	0
	11111111	11111111	00000000	00000000
Network	11000000	00000000	00000000	00000000
Network	192 .	0 .	0 .	1



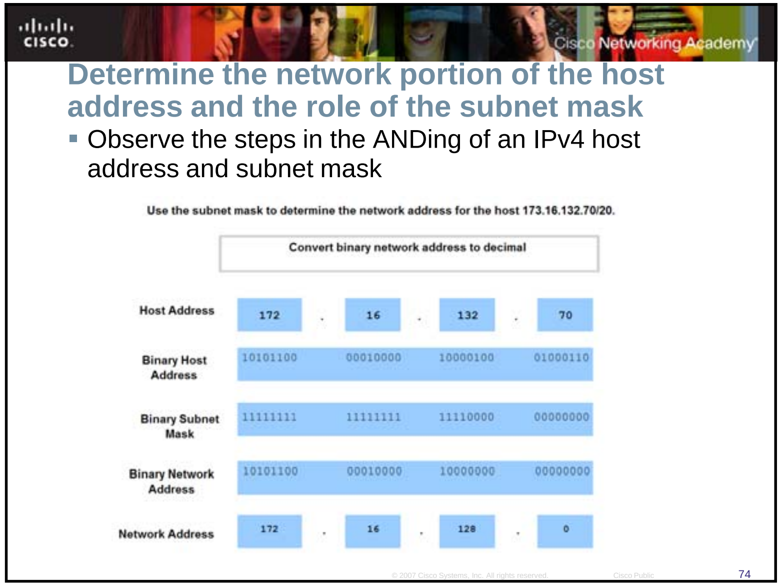
Determine the network portion of the host address and the role of the subnet mask

- Use ANDing logic to determine an outcome.

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	255	255	0	0
	11111111	11111111	00000000	00000000
Network	11000000	00000000	00000000	00000000
Network	192 .	0 .	0 .	1



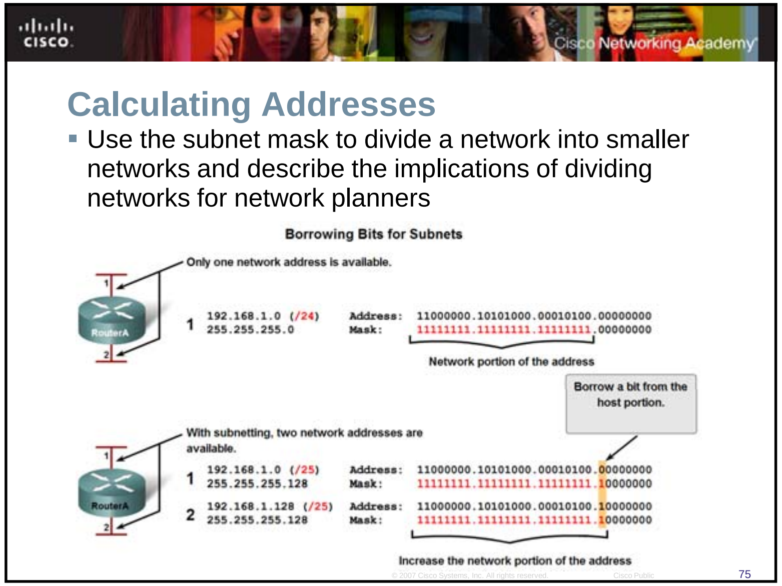
Determine the network portion of the host address and the role of the subnet mask

- 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

Borrowing Bits for Subnets

Only one network address is available.

```
1  192.168.1.0 (/24)      Address:  11000000.10101000.00010100.00000000
   255.255.255.0          Mask:     11111111.11111111.11111111.00000000
```

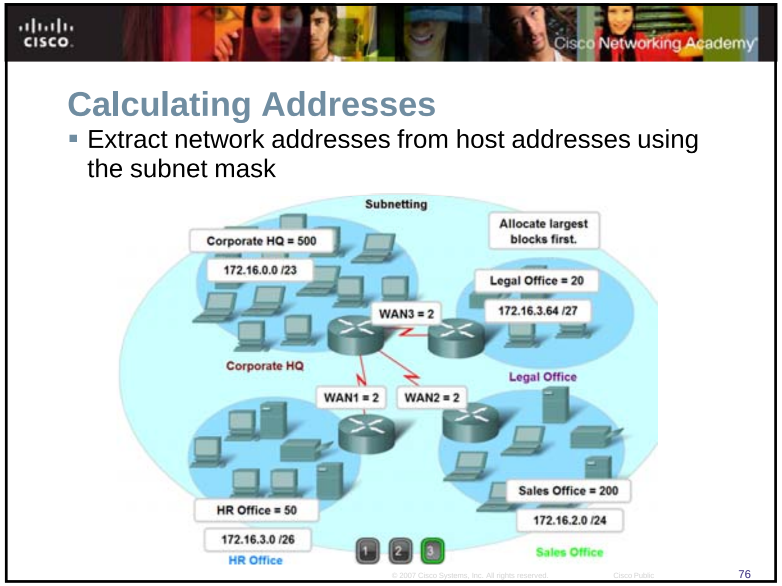
Network portion of the address

Borrow a bit from the host portion.

With subnetting, two network addresses are available.

```
1  192.168.1.0 (/25)      Address:  11000000.10101000.00010100.00000000
   255.255.255.128        Mask:     11111111.11111111.11111111.10000000
2  192.168.1.128 (/25)    Address:  11000000.10101000.00010100.10000000
   255.255.255.128        Mask:     11111111.11111111.11111111.10000000
```

Increase the network portion of the address



Calculating Addresses

- Extract network addresses from host addresses using the subnet mask

Subnetting

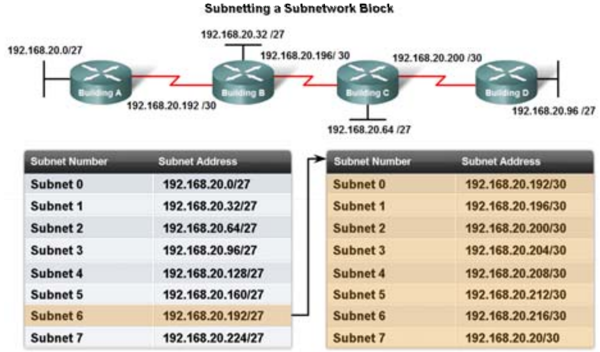
Allocate largest blocks first.

Cisco Networking Academy

Calculating Addresses

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

Subnetting a Subnetwork Block



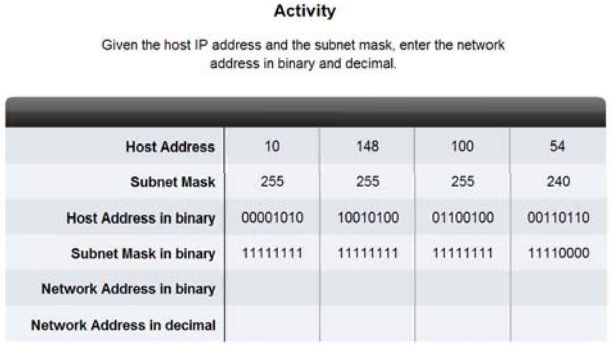
Subnet Number	Subnet Address
Subnet 0	192.168.20.0/27
Subnet 1	192.168.20.32/27
Subnet 2	192.168.20.64/27
Subnet 3	192.168.20.96/27
Subnet 4	192.168.20.128/27
Subnet 5	192.168.20.160/27
Subnet 6	192.168.20.192/27
Subnet 7	192.168.20.224/27

Subnet Number	Subnet Address
Subnet 0	192.168.20.192/30
Subnet 1	192.168.20.196/30
Subnet 2	192.168.20.200/30
Subnet 3	192.168.20.204/30
Subnet 4	192.168.20.208/30
Subnet 5	192.168.20.212/30
Subnet 6	192.168.20.216/30
Subnet 7	192.168.20.20/30

Cisco Networking Academy

Calculating Addresses

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



Activity

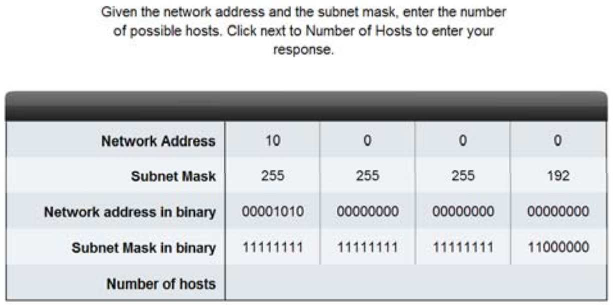
Given the host IP address and the subnet mask, enter the network address in binary and decimal.

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				

Cisco Networking Academy

Calculating Addresses

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



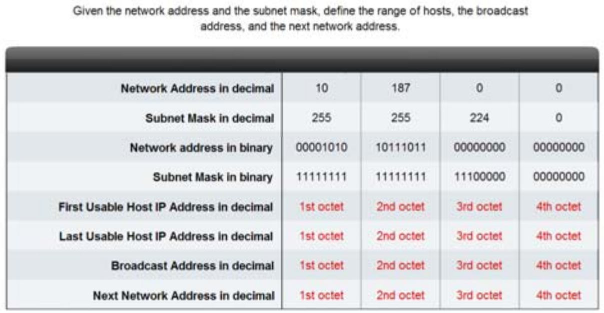
Given the network address and the subnet mask, enter the number of possible hosts. Click next to Number of Hosts to enter your response.

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				

Cisco Networking Academy

Calculating Addresses

- 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

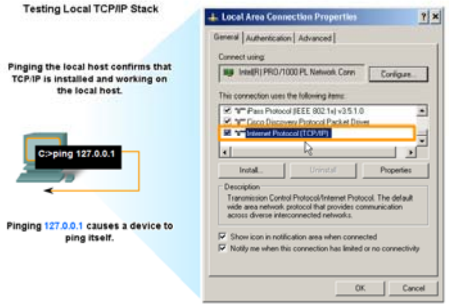


Given the network address and the subnet mask, define the range of hosts, the broadcast address, and the next network address.

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

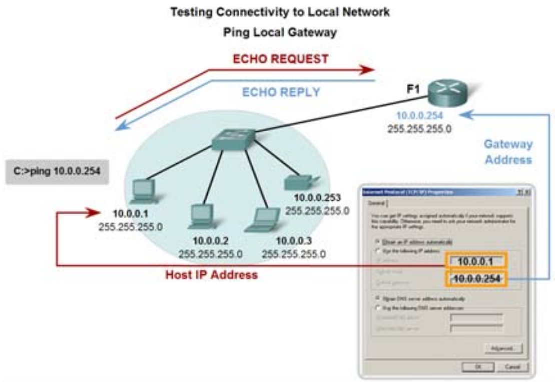
Testing the Network Layer

- 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 Local TCP/IP Stack
Pinging the local host confirms that TCP/IP is installed and working on the local host.
C:>ping 127.0.0.1
Pinging 127.0.0.1 causes a device to ping itself.
Local Area Connection Properties
General
Authentication
Advanced
Connect using:
Intel(R) PRO/1000 PL Network Conn
Configure...
This connection uses the following items:
iPass Protocol (IEEE 802.1x) v3.5.1.0
Cisco Discovery Protocol Packet Driver
Internet Protocol (TCP/IP)
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Show icon in notification area when connected
Notify me when this connection has limited or no connectivity
OK
Cancel

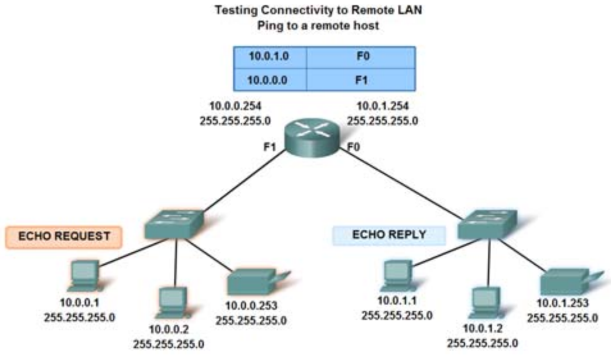
Testing the Network Layer

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



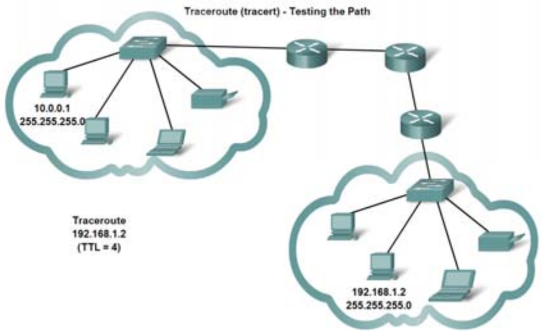
Testing the Network Layer

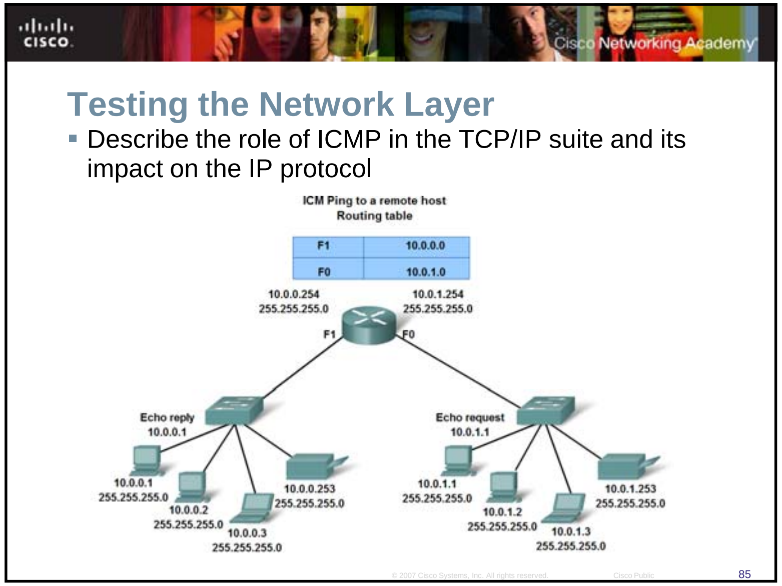
- Use ping to verify that a local host can communicate via a gateway to a device in remote network



Testing 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





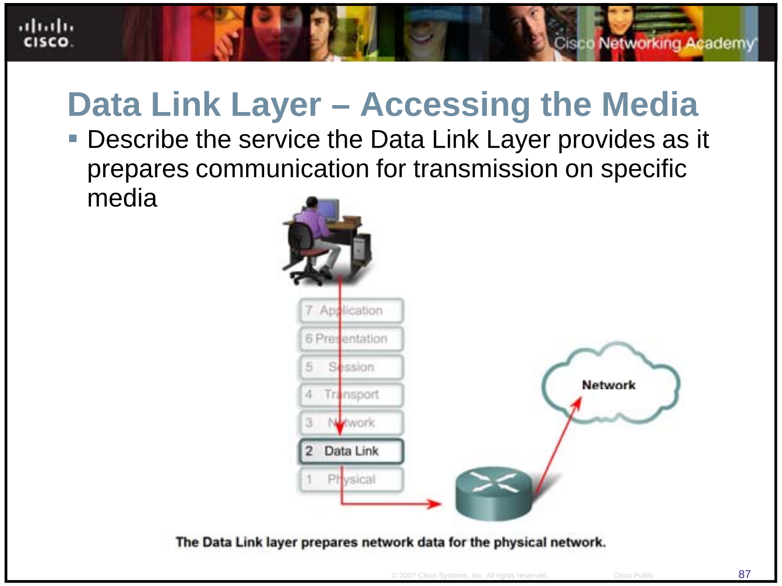
Testing the Network Layer

- Describe the role of ICMP in the TCP/IP suite and its impact on the IP protocol

ICM Ping to a remote host
Routing table

F1	10.0.0.0
F0	10.0.1.0

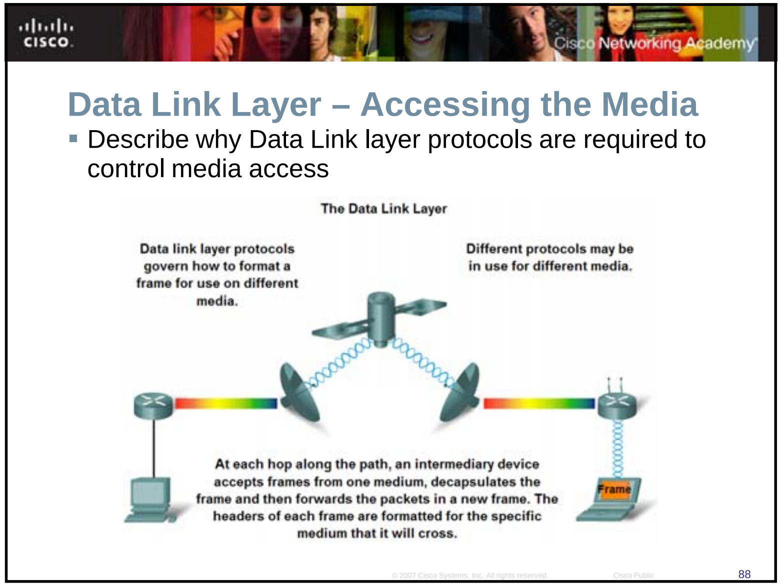
DATA LINK LAYER



Data Link Layer – Accessing the Media

- Describe the service the Data Link Layer provides as it prepares communication for transmission on specific media

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



Data Link Layer – Accessing the Media

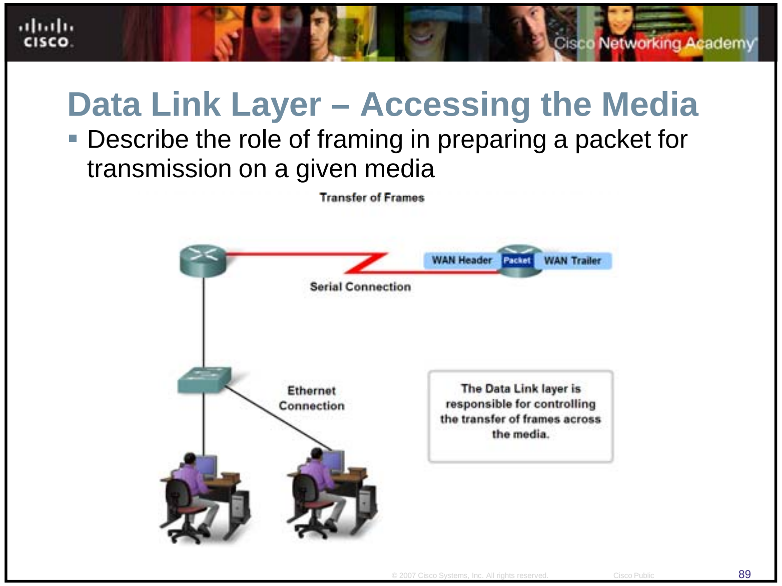
- Describe why Data Link layer protocols are required to control media access

The Data Link Layer

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

Different protocols may be in use for different media.

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



Data Link Layer – Accessing the Media

- Describe the role of framing in preparing a packet for transmission on a given media

Transfer of Frames

WAN Header

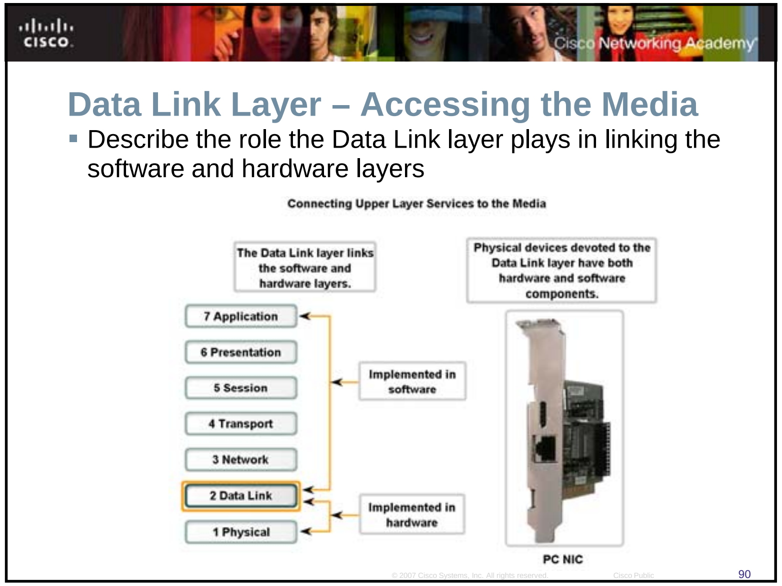
Packet

WAN Trailer

Serial Connection

Ethernet Connection

The Data Link layer is responsible for controlling the transfer of frames across the media.



Data Link Layer – Accessing the Media

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

Connecting Upper Layer Services to the Media

The Data Link layer links the software and hardware layers.

Physical devices devoted to the Data Link layer have both hardware and software components.

7 Application

6 Presentation

5 Session

4 Transport

3 Network

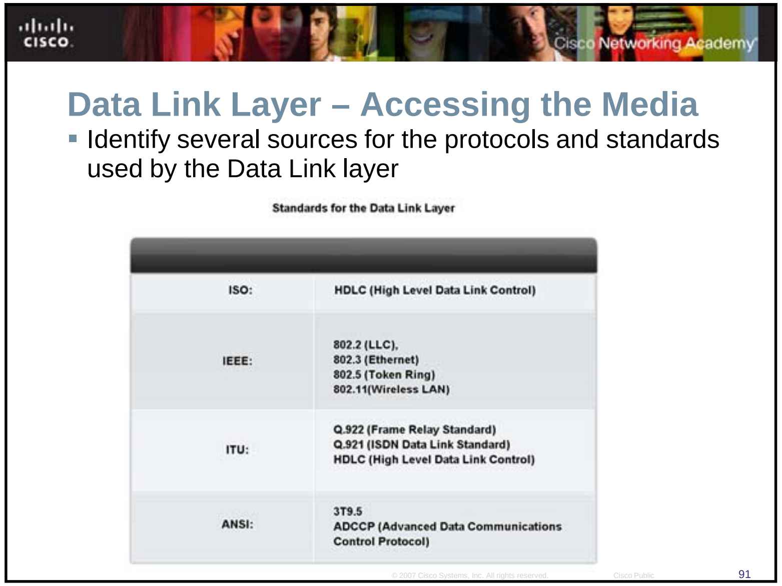
2 Data Link

1 Physical

Implemented in software

Implemented in hardware

PC NIC

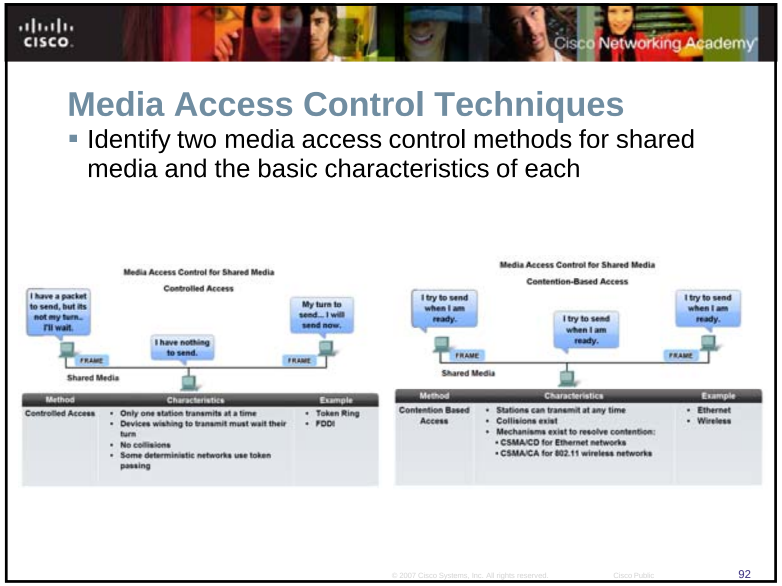


Data Link Layer – Accessing the Media

- 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

- Identify two media access control methods for shared media and the basic characteristics of each

Media Access Control for Shared Media

Controlled Access

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

I have nothing to send.

My turn to send... I will send now.

FRAME

FRAME

Shared Media

Method	Characteristics	Example
Controlled Access	• Only one station transmits at a time • Devices wishing to transmit must wait their turn • No collisions • Some deterministic networks use token passing	• Token Ring • FDDI

Media Access Control for Shared Media

Contention-Based Access

I try to send when I am ready.

I try to send when I am ready.

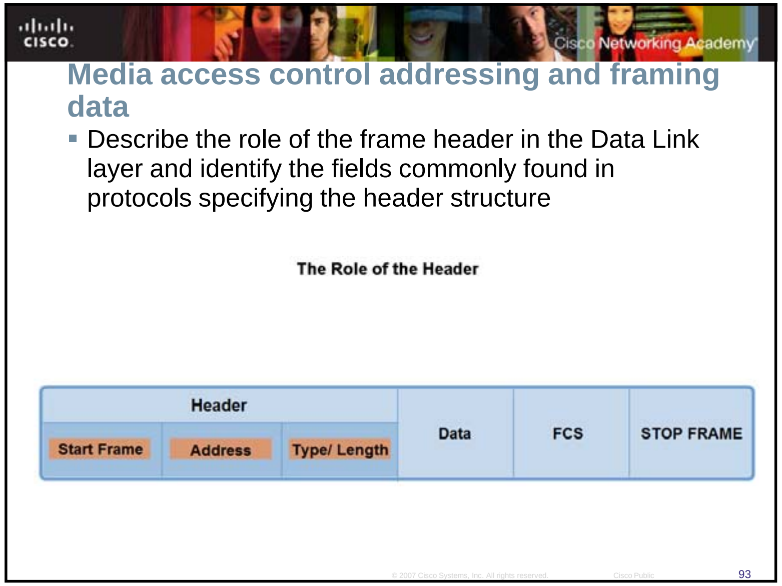
I try to send when I am ready.

FRAME

FRAME

Shared Media

Method	Characteristics	Example
Contention Based Access	• Stations can transmit at any time • Collisions exist • Mechanisms exist to resolve contention: • CSMA/CD for Ethernet networks • CSMA/CA for 802.11 wireless networks	• Ethernet • Wireless

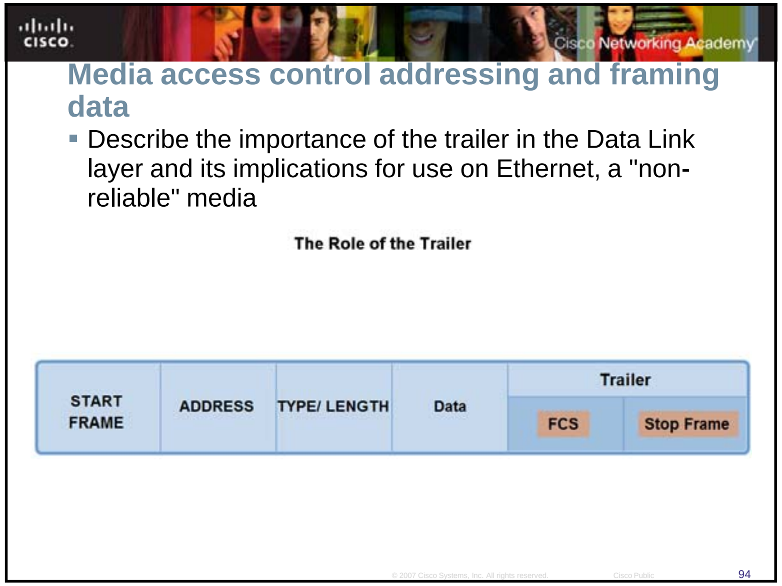


Media access control addressing and framing data

- Describe the role of the frame header in the Data Link layer and identify the fields commonly found in protocols specifying the header structure

The Role of the Header

Header			Data	FCS	STOP FRAME
Start Frame	Address	Type/ Length			

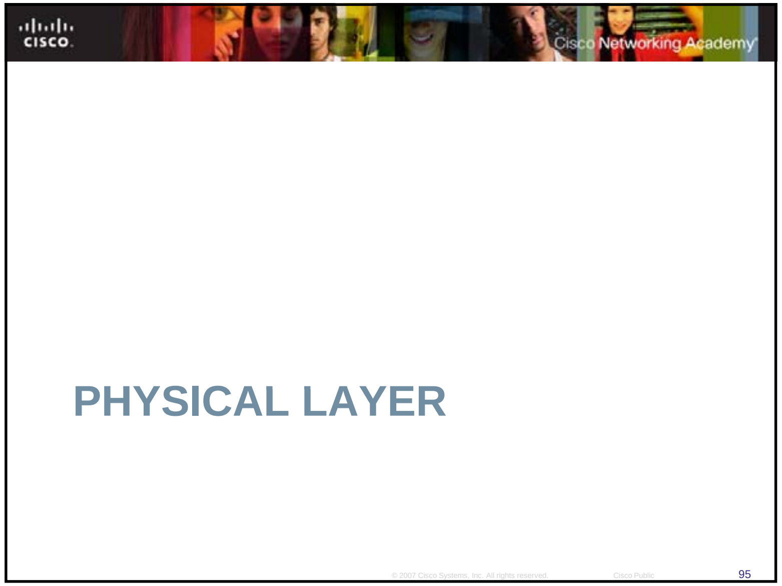


Media access control addressing and framing data

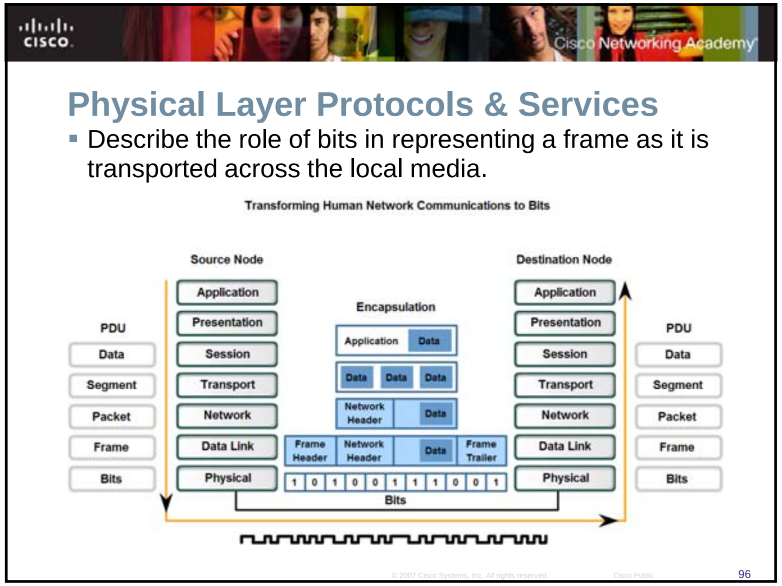
- Describe the importance of the trailer in the Data Link layer and its implications for use on Ethernet, a "non-reliable" media

The Role of the Trailer

START FRAME	ADDRESS	TYPE/ LENGTH	Data	Trailer	
				FCS	Stop Frame



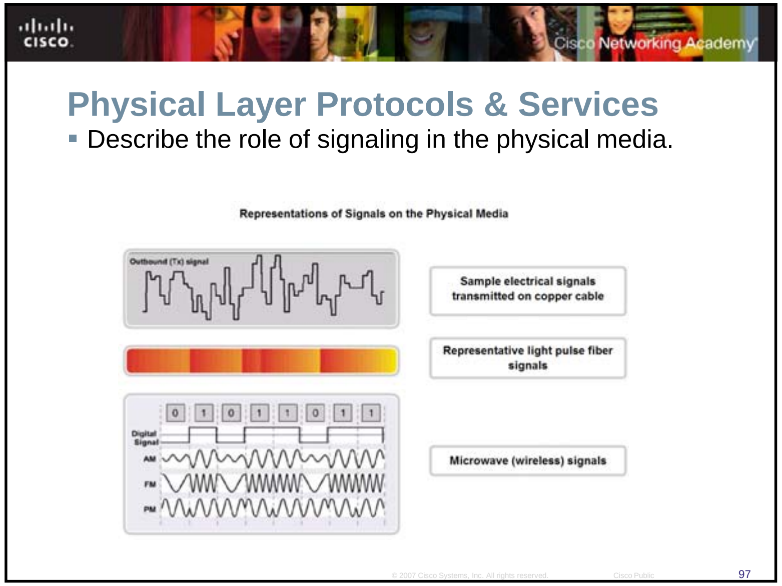
PHYSICAL LAYER



Physical Layer Protocols & Services

- Describe the role of bits in representing a frame as it is transported across the local media.

Transforming Human Network Communications to Bits



Physical Layer Protocols & Services

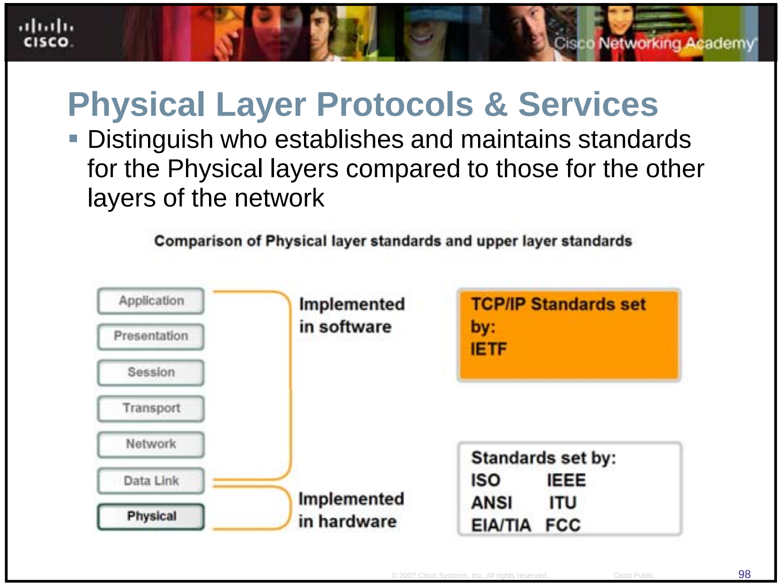
- Describe the role of signaling in the physical media.

Representations of Signals on the Physical Media

Sample electrical signals transmitted on copper cable

Representative light pulse fiber signals

Microwave (wireless) signals



Physical Layer Protocols & Services

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

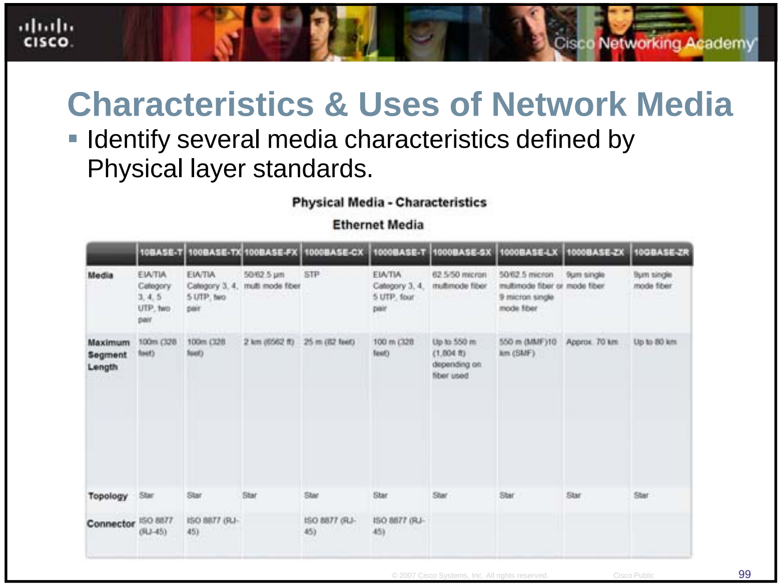
Comparison of Physical layer standards and upper layer standards

Implemented in software

TCP/IP Standards set by:
IETF

Implemented in hardware

Standards set by:
ISO IEEE
ANSI ITU
EIA/TIA FCC



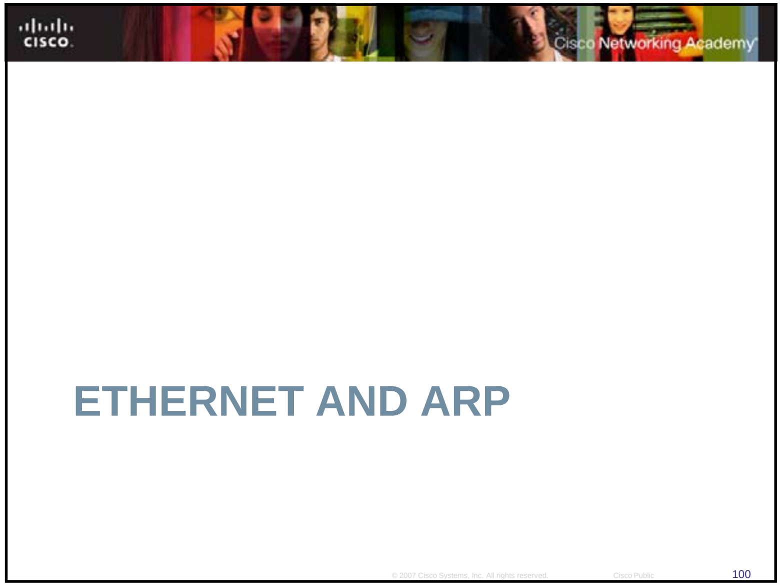
Characteristics & Uses of Network Media

- Identify several media characteristics defined by Physical layer standards.

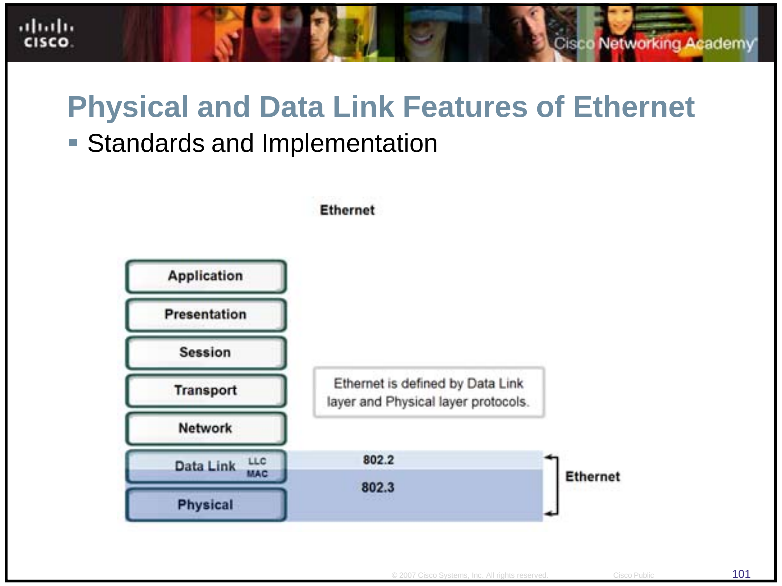
Physical Media - Characteristics

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)				



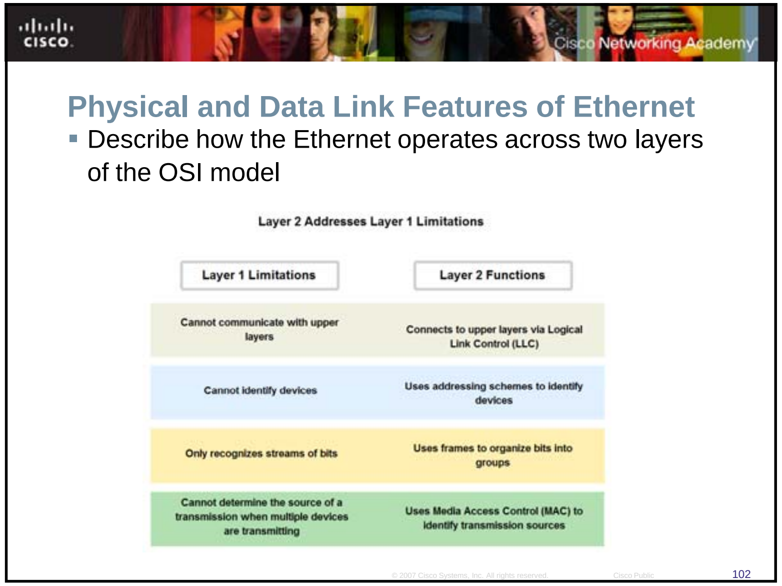
ETHERNET AND ARP



Physical and Data Link Features of Ethernet

- Standards and Implementation

Ethernet is defined by Data Link layer and Physical layer protocols.

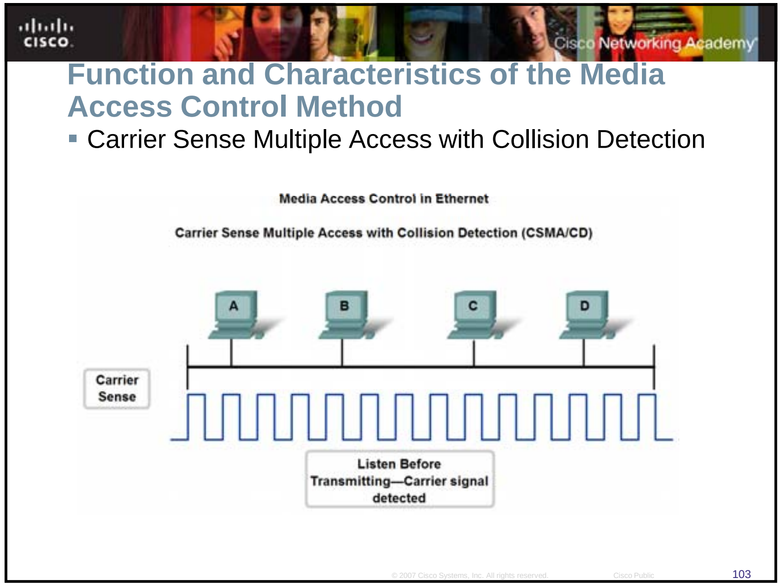


Physical and Data Link Features of Ethernet

- 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



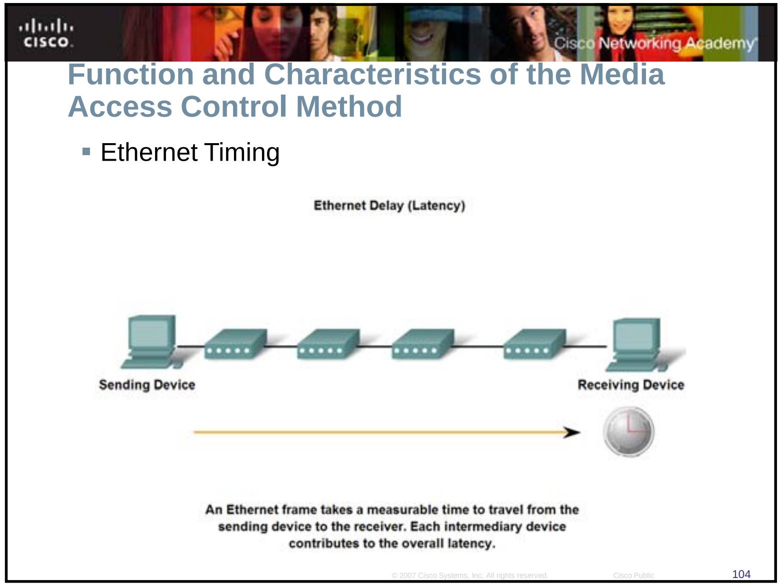
Function and Characteristics of the Media Access Control Method

- Carrier Sense Multiple Access with Collision Detection

Media Access Control in Ethernet

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

Listen Before Transmitting—Carrier signal detected

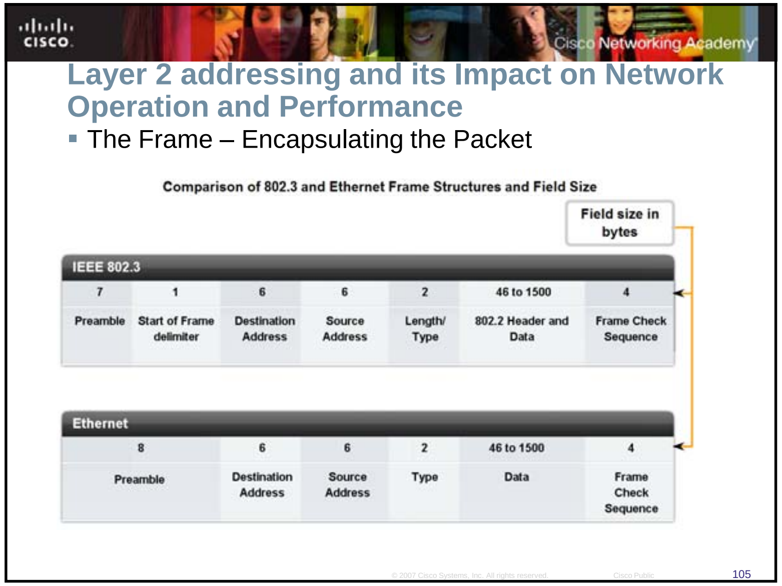


Function and Characteristics of the Media Access Control Method

- Ethernet Timing

Ethernet Delay (Latency)

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



Layer 2 addressing and its Impact on Network Operation and Performance

- The Frame – Encapsulating the Packet

Comparison of 802.3 and Ethernet Frame Structures and Field Size

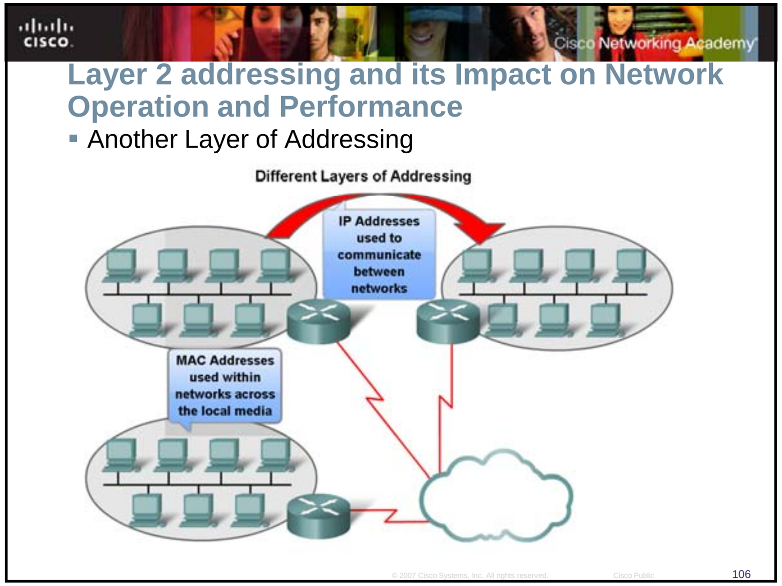
Field size in bytes

IEEE 802.3

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



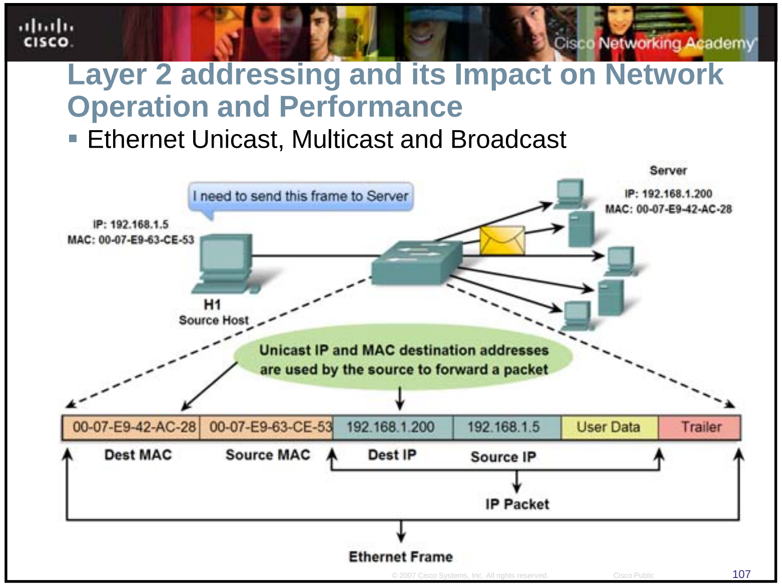
Layer 2 addressing and its Impact on Network Operation and Performance

- Another Layer of Addressing

Different Layers of Addressing

IP Addresses used to communicate between networks

MAC Addresses used within networks across the local media



Layer 2 addressing and its Impact on Network Operation and Performance

- Ethernet Unicast, Multicast and Broadcast

I need to send this frame to Server

IP: 192.168.1.5
MAC: 00-07-E9-63-CE-53

H1
Source Host

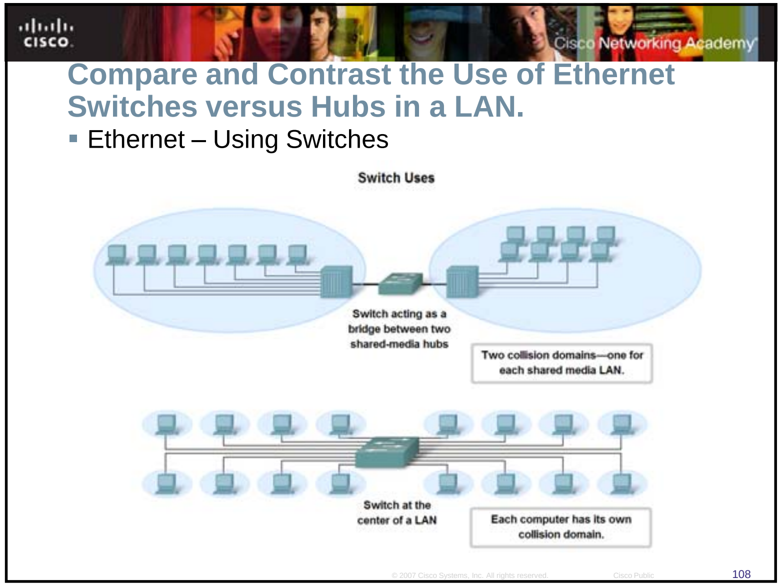
Server
IP: 192.168.1.200
MAC: 00-07-E9-42-AC-28

Unicast IP and MAC destination addresses are used by the source to forward a packet

00-07-E9-42-AC-28	00-07-E9-63-CE-53	192.168.1.200	192.168.1.5	User Data	Trailer
Dest MAC	Source MAC	Dest IP	Source IP		

IP Packet

Ethernet Frame



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

- Ethernet – Using Switches

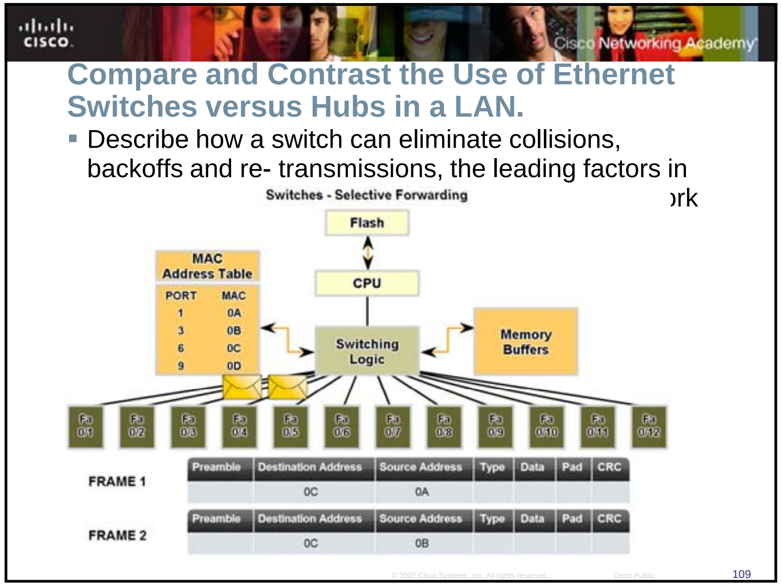
Switch Uses

Switch acting as a bridge between two shared-media hubs

Two collision domains—one for each shared media LAN.

Switch at the center of a LAN

Each computer has its own collision domain.



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

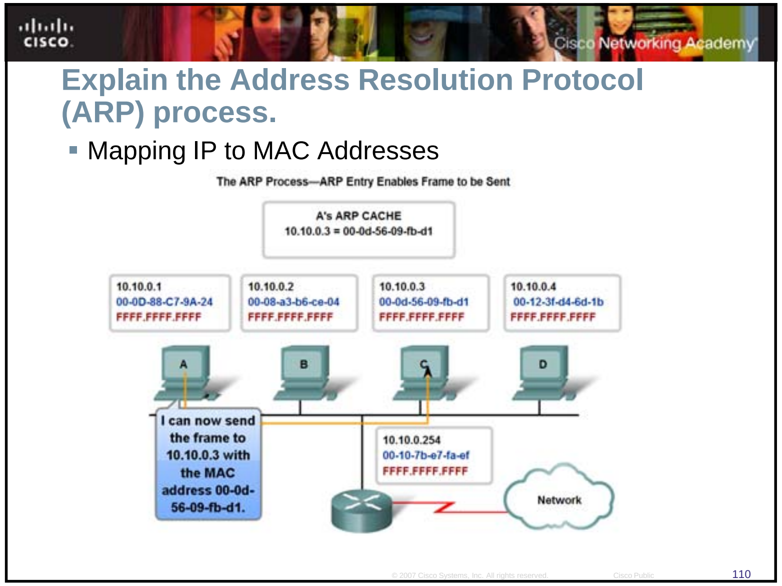
- Describe how a switch can eliminate collisions, backoffs and re- transmissions, the leading factors in ork

Switches - Selective Forwarding

MAC Address Table

PORT	MAC
1	0A
3	0B
6	0C
9	0D

	Preamble	Destination Address	Source Address	Type	Data	Pad	CRC
FRAME 1		0C	0A				
FRAME 2		0C	0B				



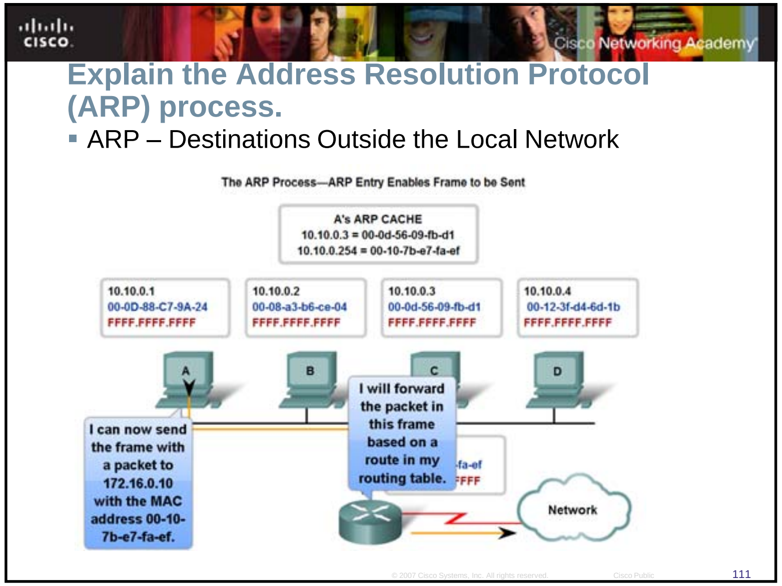
Explain the Address Resolution Protocol (ARP) process.

- Mapping IP to MAC Addresses

The ARP Process—ARP Entry Enables Frame to be Sent

A's ARP CACHE
10.10.0.3 = 00-0d-56-09-fb-d1

I can now send the frame to 10.10.0.3 with the MAC address 00-0d-56-09-fb-d1.



Explain the Address Resolution Protocol (ARP) process.

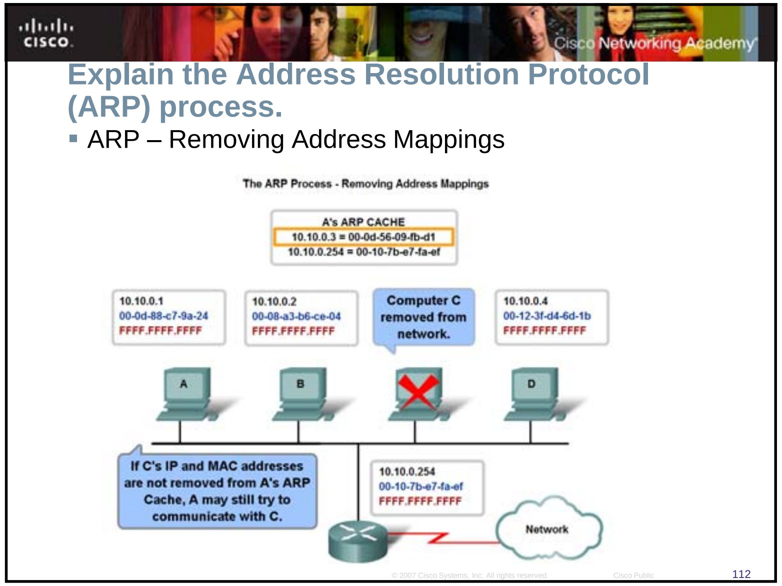
- ARP – Destinations Outside the Local Network

The ARP Process—ARP Entry Enables Frame to be Sent

A's ARP CACHE
10.10.0.3 = 00-0d-56-09-fb-d1
10.10.0.254 = 00-10-7b-e7-fa-ef

I can now send the frame with a packet to 172.16.0.10 with the MAC address 00-10-7b-e7-fa-ef.

I will forward the packet in this frame based on a route in my routing table.



Explain the Address Resolution Protocol (ARP) process.

- ARP – Removing Address Mappings

The ARP Process - Removing Address Mappings

A's ARP CACHE
10.10.0.3 = 00-0d-56-09-fb-d1
10.10.0.254 = 00-10-7b-e7-fa-ef

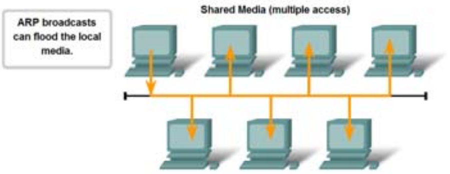
Computer C removed from network.

If C's IP and MAC addresses are not removed from A's ARP Cache, A may still try to communicate with C.

Explain the Address Resolution Protocol (ARP) process.

- ARP Broadcasts - Issues

ARP Issues:
- Broadcasts, overhead on the Media
- Security


Shared Media (multiple access)
ARP broadcasts can flood the local media.

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

CONFIGURING AND TESTING YOUR NETWORK (PACKET TRACER)

cisco