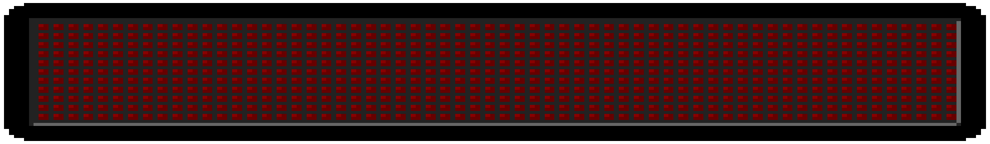
TOPIC 04 Network Devices

Objectives



- Describe the basic operation of network repeaters and hubs
- Explain the purpose of network switches
- Summarize the operation of wireless access points
- Describe the basic operation of network interface cards
- Explain the function of routers

© Cengage Learning 2017

Network Repeaters and Hubs

- Early networks didn't use interconnecting devices

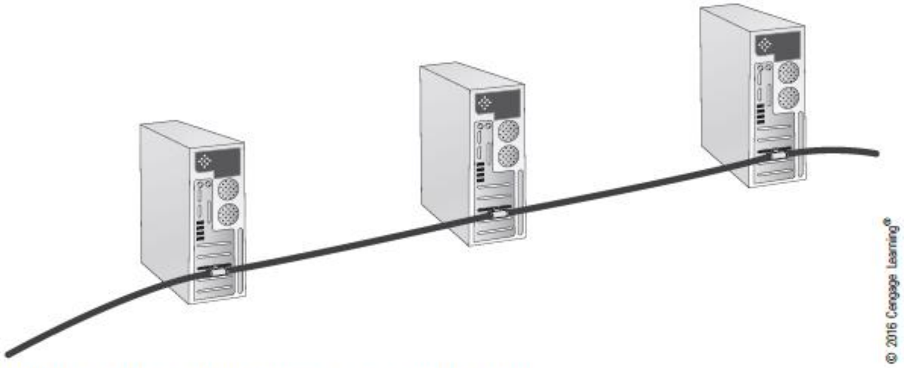
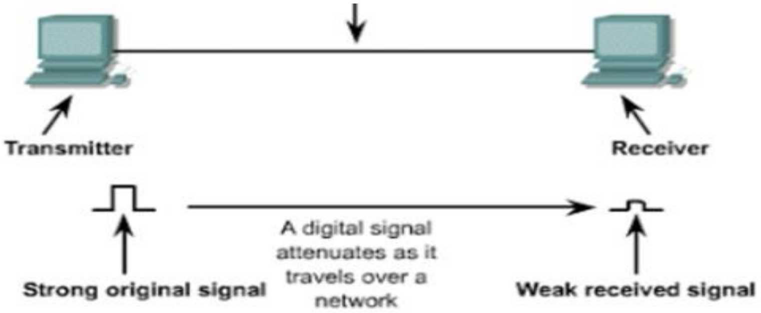
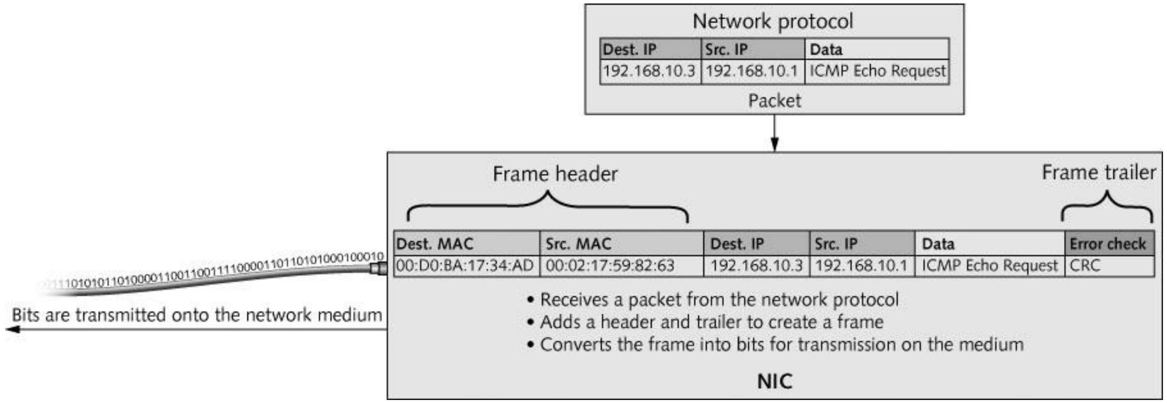


Figure 2-1 Older networks didn't use interconnecting devices

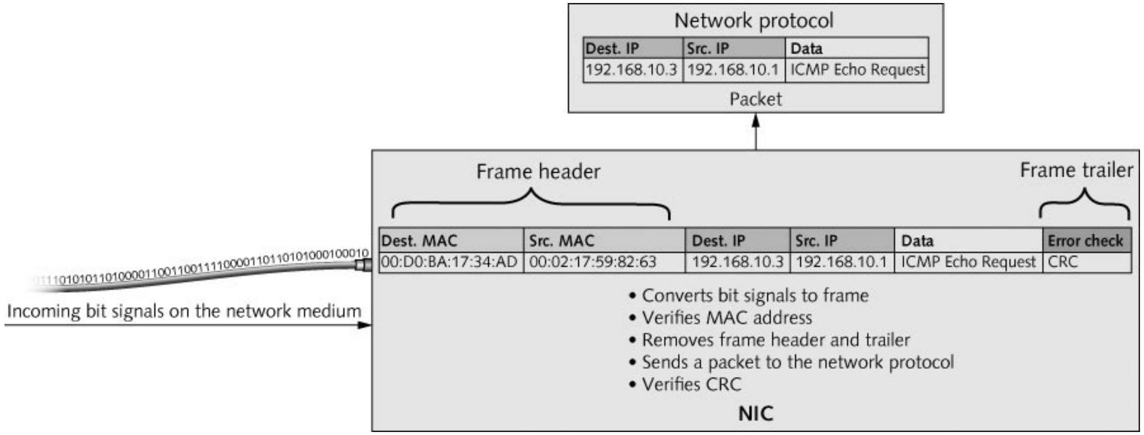
- Severely limited the total cable length (due to signal attenuation) and number of computers



© Cengage Learning 2017



A NIC handles outgoing data to the network medium



A NIC handles incoming data from the network medium

Copyright © 2012 Cengage Learning. All rights reserved.

© Cengage Learning 2017

Network Repeaters and Hubs

- Some problems were resolved with a device called a **repeater**
  - A repeater receives bit signals generated by NICs and other devices, strengthens them, and then “repeats” them to other parts of the network
- A repeater enables you to connect computers whose distance from one another would make communication impossible
- A traditional repeater has two ports or connections that you can use to extend your network

© Cengage Learning 2017

Network Repeaters and Hubs

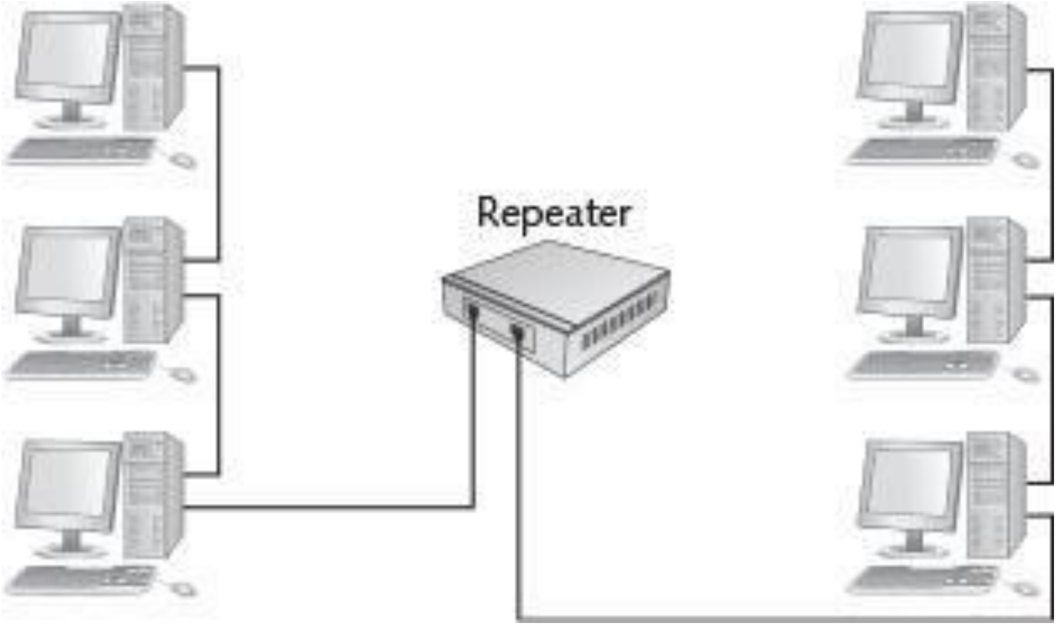


Figure 2-2 A repeater extends the distance a network can cover

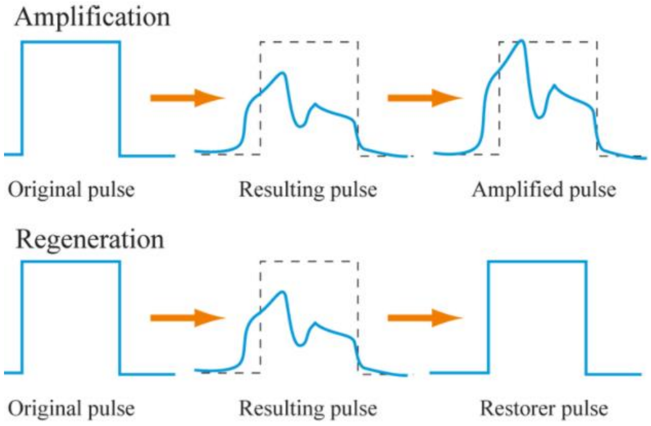
© Cengage Learning 2017

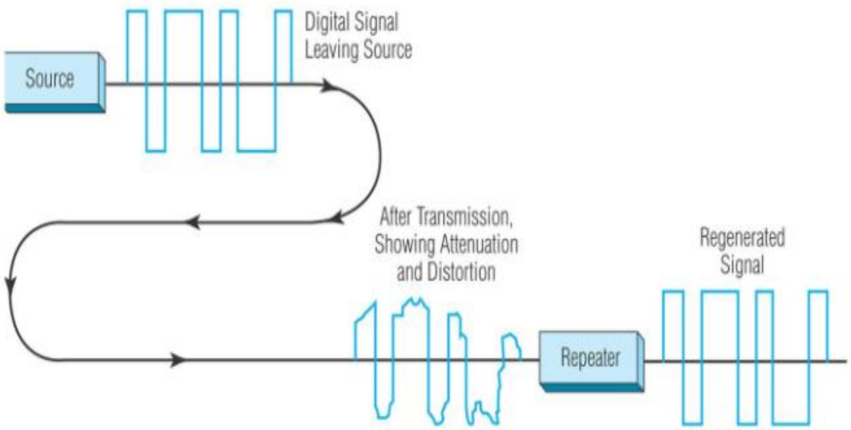
Multiport Repeaters and Hubs

- A multiport repeater is just a repeater with several ports to which you can connect cabling
  - Also referred to as a **hub**
- Receives bit signals generated from a connected computer's NIC on one of its ports
- Cleans the signal by filtering out electrical noise
- **Regenerates** the signal to full strength
- Transmits the regenerated signal to all other ports where a computer (or other network device) is connected to

© Cengage Learning 2017

- A repeater regenerates a signal not amplify





© Cengage Learning 2017

Multiport Repeaters and Hubs

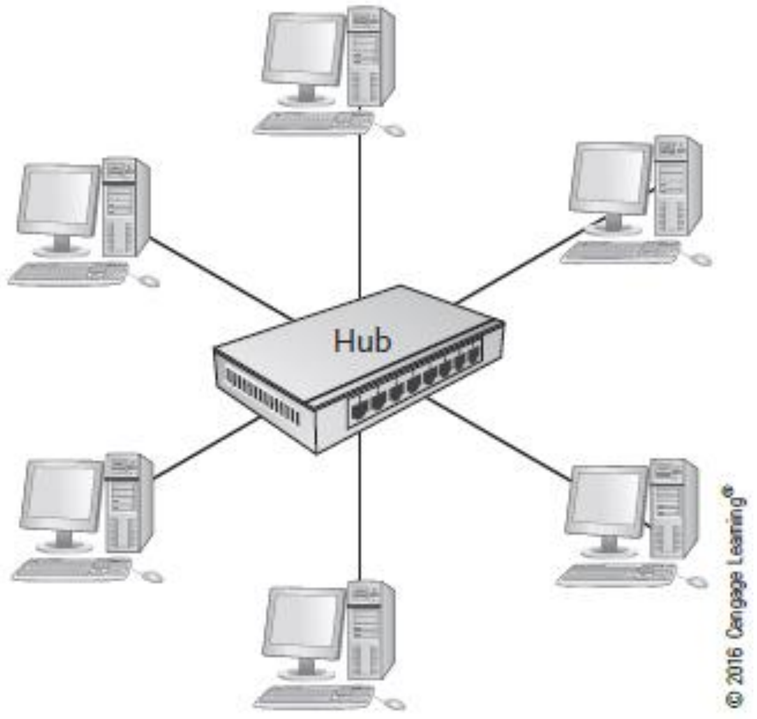
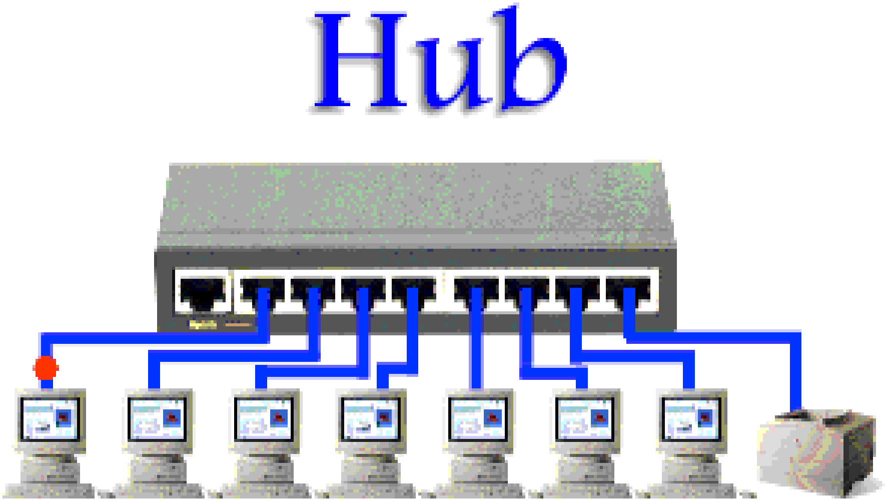


Figure 2-3 A multiport repeater or hub

© Cengage Learning 2017



In a hub, a frame is passed along or "broadcast" to every one of its ports. It doesn't matter that the frame is only destined for one port. The hub has no way of distinguishing which port a frame should be sent to. Passing it along to every port ensures that it will reach its intended destination. This places a lot of traffic on the network and can lead to poor network response times.

© Cengage Learning 2017

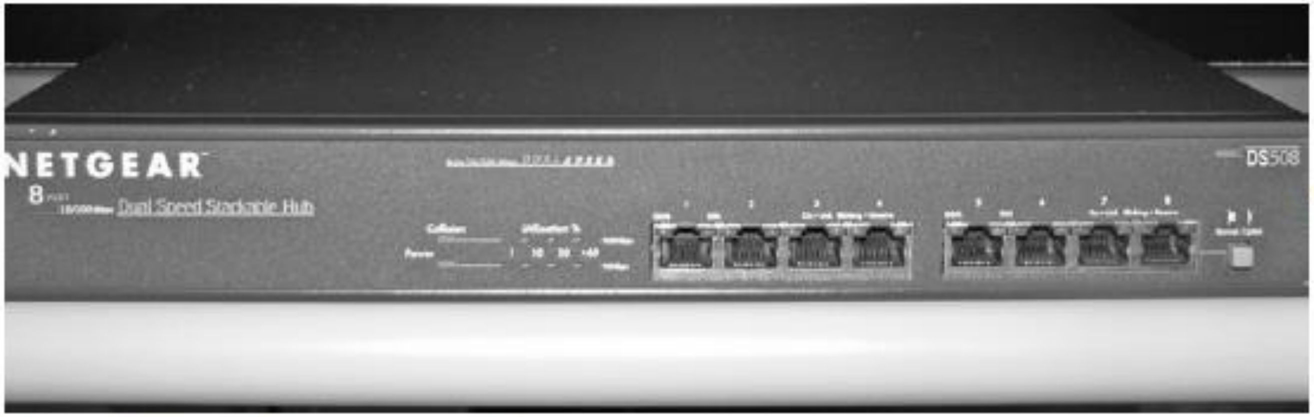
Hubs and Network Bandwidth

- Amount of data that can be transferred in an interval is **network bandwidth**
  - Usually measured in bits per second (bps) and networks operate at speeds from 10 million bps up to 10 gigabit per second (Gbps)
- Hubs share bandwidth with all other connected computers
  - Only one computer can successfully transmit data at a time
- **Bandwidth sharing** – when all computers connected to the hub must share the amount of bandwidth the hub provides

© Cengage Learning 2017

Hub Indicator Lights

- Power, link status, network activity, collisions
- Uplink port – port used to connect two hubs together or hub to a switch

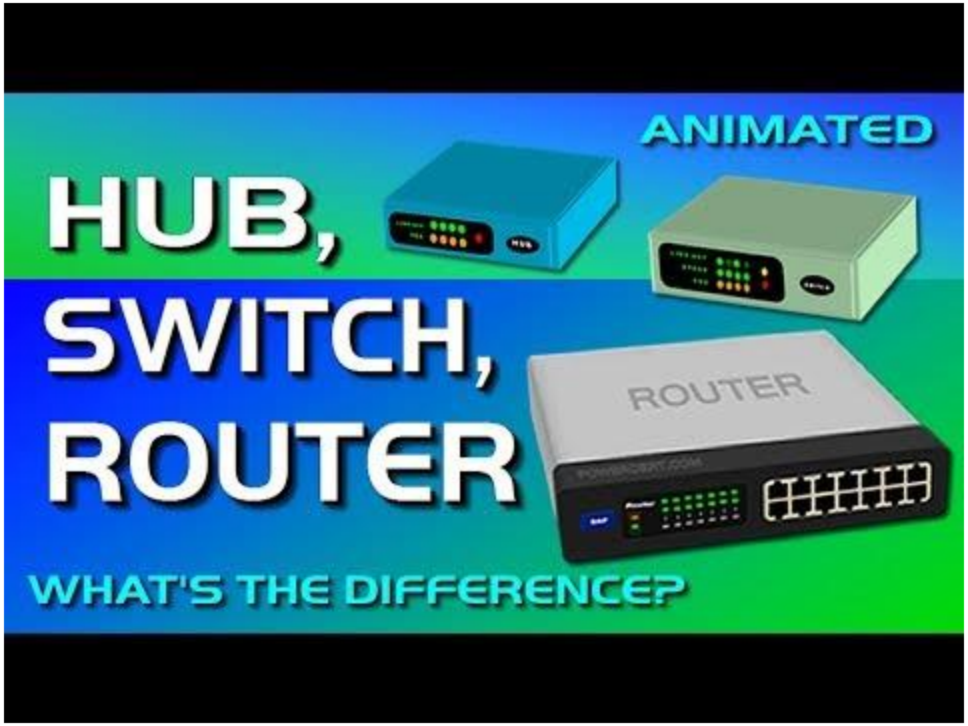


© 2016 Cengage Learning®

Figure 2-4 A typical hub with indicator lights

© Cengage Learning 2017

Difference between Hub And Switch



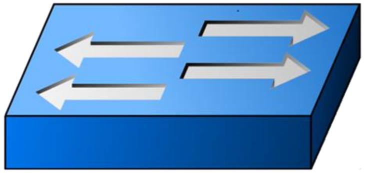
https://www.youtube.com/watch?v=1z0ULvg_pW8

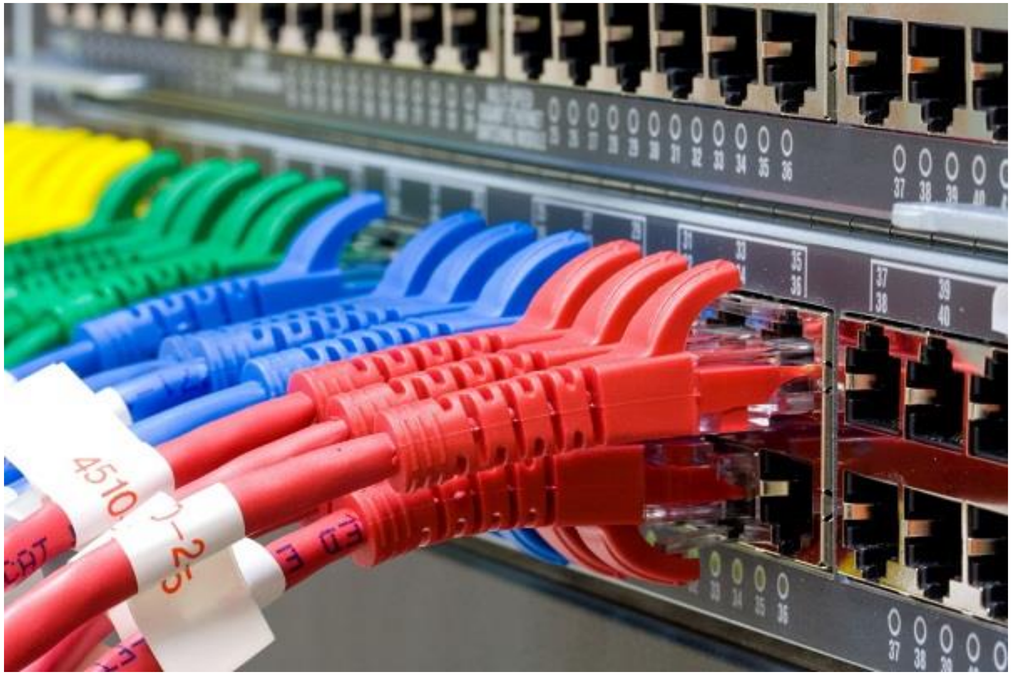
© Cengage Learning 2017

Dst MAC: MAC C	Src MAC: MAC A	Dst IP: 164.78.252.4	Src IP: 192.1.2.4	Protocol: TCP	Dst Port: 80	Src Port: 1234	HTTP Request	Frame Trailer

Network Switches

- Looks just like a hub
  - But a switch actually reads data in the message, determines which port the destination device is connected to, and forward the message to only that port





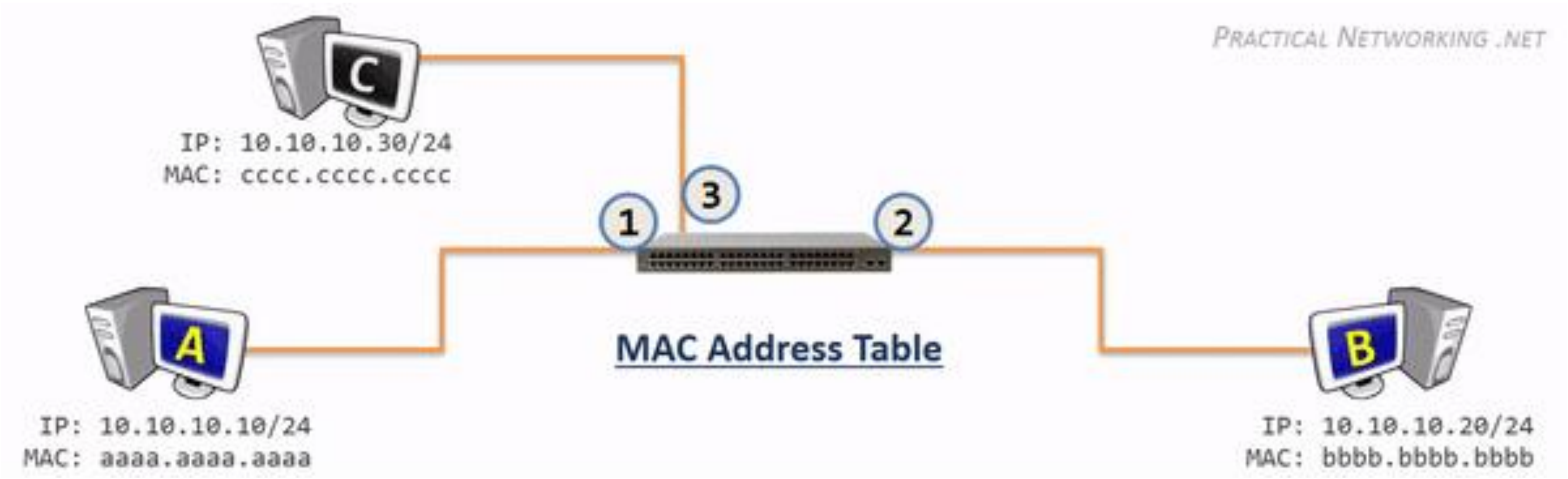
© Cengage Learning 2017

Dst MAC: MAC C	Src MAC: MAC A	Dst IP: 164.78.252.4	Src IP: 192.1.2.4	Protocol: TCP	Dst Port: 80	Src Port: 1234	HTTP Request	Frame Trailer

Network Switches

- Basic Switch Operation
  - Data is sent onto the medium one frame at a time
  - Each frame has the destination and source MAC addresses
  - Switch reads the addresses:
    - Use the source MAC address of frame to keep a record of which computer is on which port (**switching table**)
    - Forwards the frame to the port where the destination MAC can be found

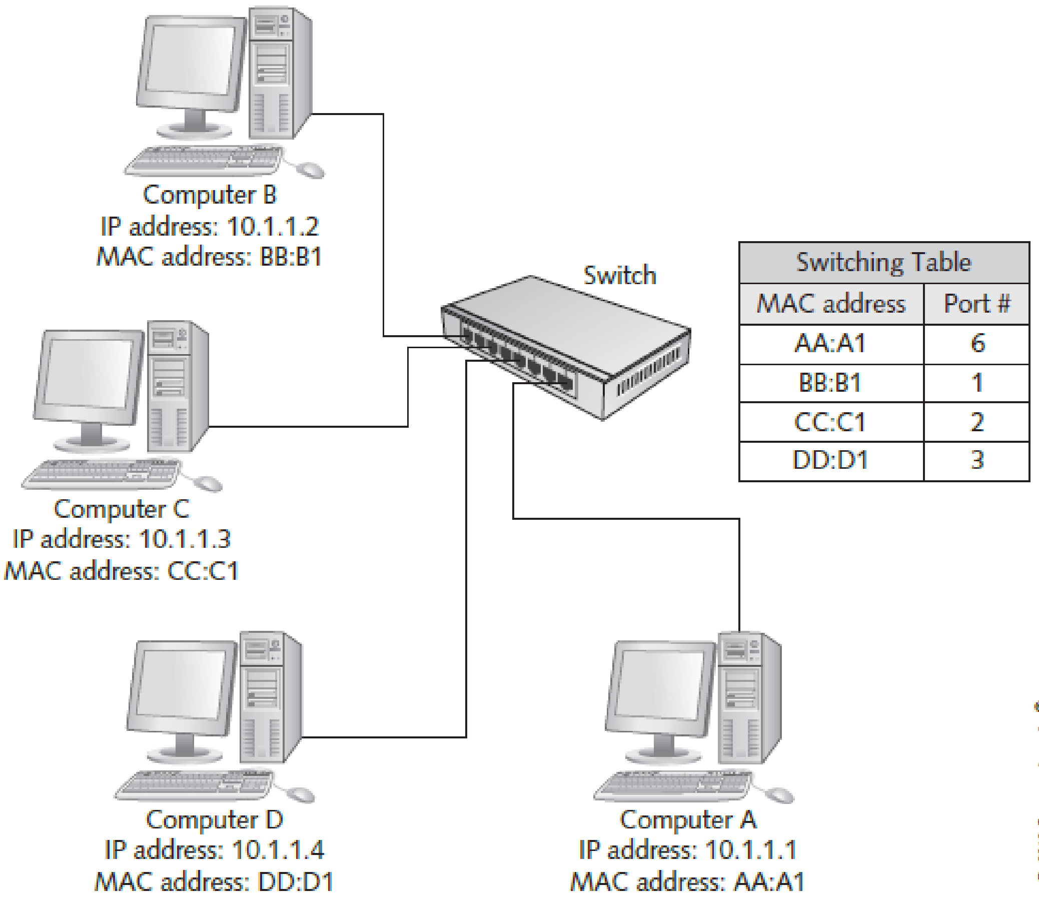
© Cengage Learning 2017



© Cengage Learning 2017

Dst MAC: MAC C	Src MAC: MAC A	Dst IP: 164.78.252.4	Src IP: 192.1.2.4	Protocol: TCP	Dst Port: 80	Src Port: 1234	HTTP Request	Frame Trailer

Network Switches



Switching Table	
MAC address	Port #
AA:A1	6
BB:B1	1
CC:C1	2
DD:D1	3

© 2016 Cengage Learning®

Figure 2-5 Switches maintain a switching table

© Cengage Learning 2017

Network Switches

- Steps of switch operation
  1. The switch receives a frame.
  2. The switch reads the source and destination MAC addresses.
  3. The switch looks up the destination MAC address in its switching table.
  4. The switch forwards the frame to the port where the computer owning the MAC address is found.
  5. The switching table is updated with the source MAC address and port information.

© Cengage Learning 2017

Switches and Network Bandwidth

- Each port gets **dedicated bandwidth**
  - Instead of having to share bandwidth with all ports
- Multiple conversations can occur simultaneously
- Can operate in **full-duplex mode**
  - Can send an receive data simultaneously
- Hubs can only operate in **half-duplex mode**
  - Can send or receive (but not both) at one time
- Switches are the preferred device because of these advantages

© Cengage Learning 2017

a switch, keeps a record of the MAC (Media Access Control) addresses of all the devices connected to it. With this information, a switch can identify which system is sitting on which port. So when a frame is received, it knows exactly which port to send it to, without significantly increasing network response times. In addition, unlike a hub, a 10/100Mbps switch will allocate a full 10/100Mbps to each of its ports. So regardless of the number of PCs transmitting, users will always have access to the maximum amount of bandwidth. It's for these reasons a switch is considered to be a much better choice than a hub.

© Cengage Learning 2017

Switch Indicator Lights

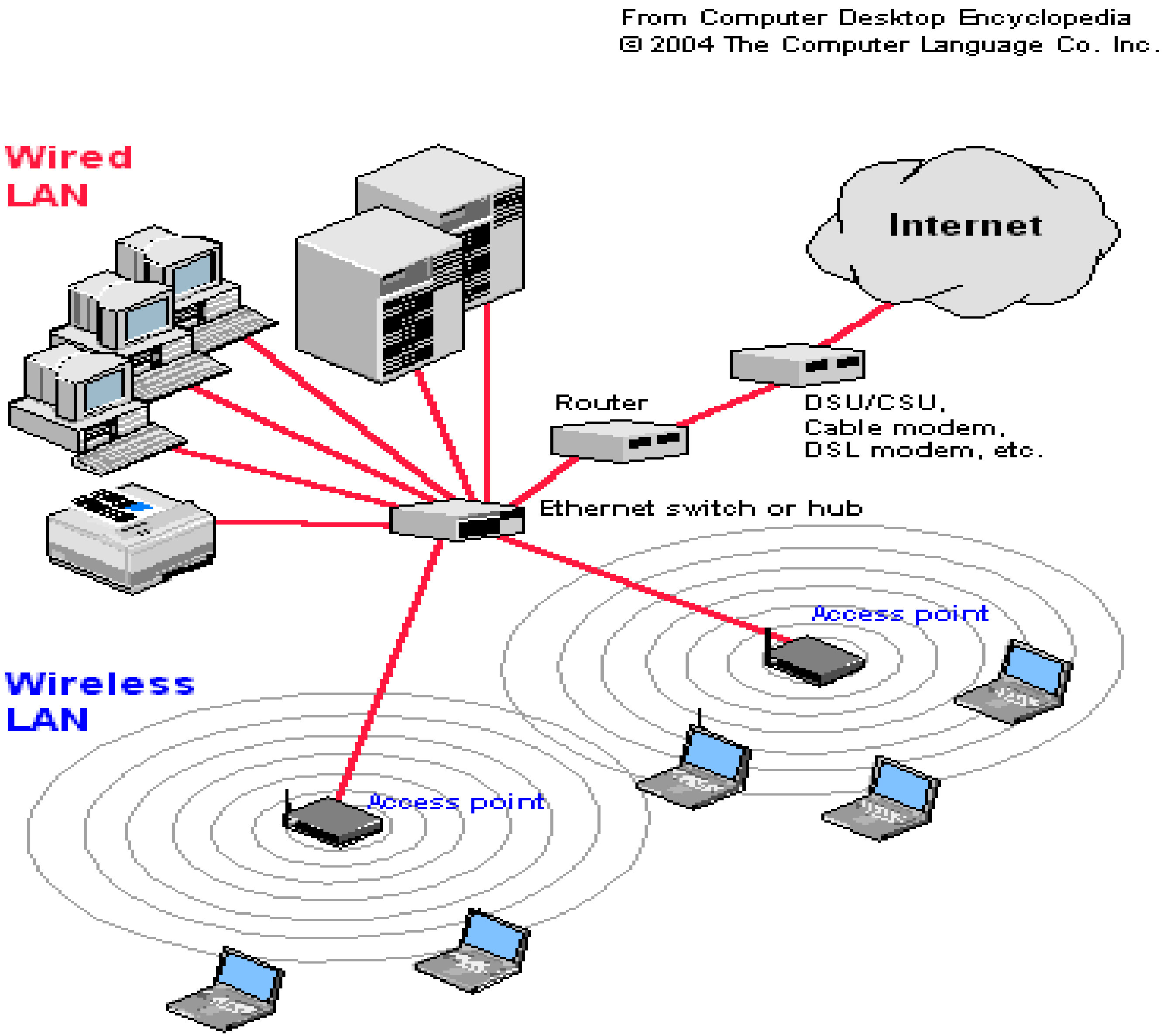
- Like hubs, switches have indicator lights
- Switches have link status indicators and activity indicators
  - May also have indicators for whether the switch is operating in full-duplex or half-duplex mode
- Switches can be connected to one another so that your LAN can grow beyond the limitations of ports on a single switch
  - Some switches have a dedicated port for **uplinking** to another switch

© Cengage Learning 2017

Wireless Access Points

- The heart of a wireless network is the wireless **access point (AP)**
- APs operate similarly to a hub without wires
- All communication passes through the AP
- Most small business and home networks use a device typically called a wireless router that combines the functions of an AP, a switch, and a router
- Wireless LANs are usually attached to wired networks

© Cengage Learning 2017



© Cengage Learning 2017

Wireless Access Points

Figure 2-9 A wireless router combines an access point, a switch, and a router

Source: *TK*

© Cengage Learning 2017

Network Interface Cards

- Most NICs are built into a computer’s motherboard
  - Occasionally fail or additional NICs are needed for an application
  - It is important to know how to install a new NIC

© Cengage Learning 2017

NIC Basics

- Attaching a computer to a network requires a **network interface card (NIC)** to create and mediate the connection between a computer and the networking medium
  - Networking medium might be copper wire, fiber-optic cable, or airwaves

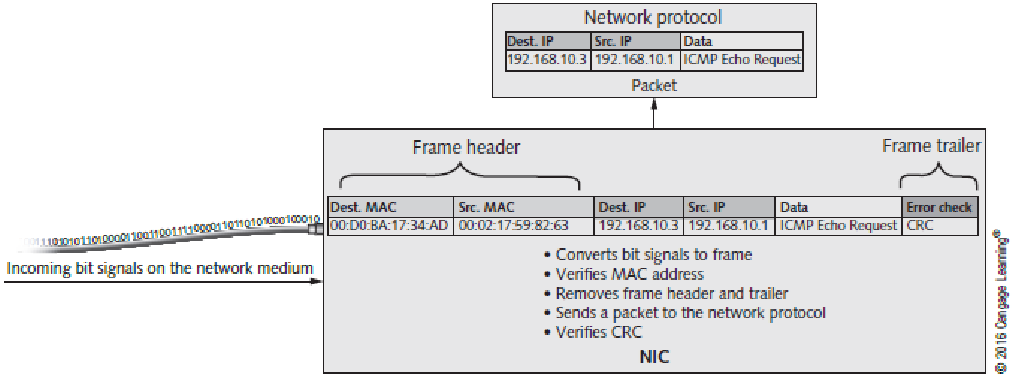
© Cengage Learning 2017

NIC Basics

- The tasks a NIC and its driver perform:
  - Provide a connection from computer to medium
  - Incoming messages: Receives bit signals and assembles them into frames
    - Verifies the destination address
    - Removes frame header and sends the resulting packet to the network protocol
  - Outgoing messages: receive packets from network protocol
    - Creates frames by adding MAC addresses/error check
  - Converts frame into bit signals suitable for the medium and transmits them

© Cengage Learning 2017

NIC Basics

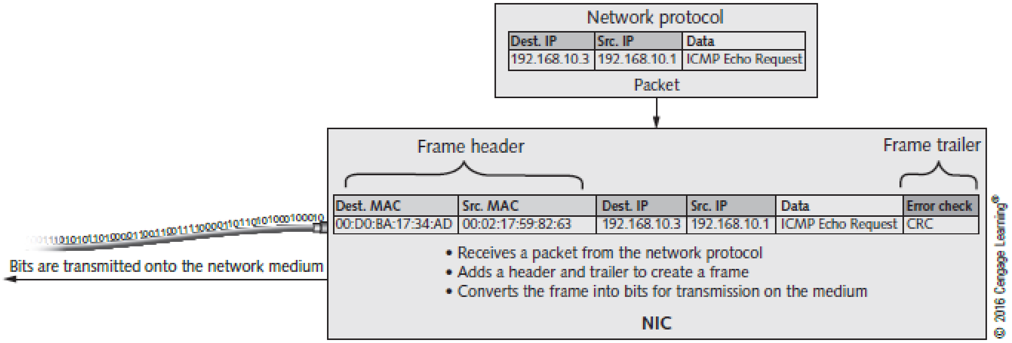


Dest. IP	Src. IP	Data
192.168.10.3	192.168.10.1	ICMP Echo Request

Dest. MAC	Src. MAC	Dest. IP	Src. IP	Data	Error check
00:D0:BA:17:34:AD	00:02:17:59:82:63	192.168.10.3	192.168.10.1	ICMP Echo Request	CRC

- Converts bit signals to frame
- Verifies MAC address
- Removes frame header and trailer
- Sends a packet to the network protocol
- Verifies CRC

Figure 2-10 A NIC handles incoming data from the network medium



Dest. IP	Src. IP	Data
192.168.10.3	192.168.10.1	ICMP Echo Request

Dest. MAC	Src. MAC	Dest. IP	Src. IP	Data	Error check
00:D0:BA:17:34:AD	00:02:17:59:82:63	192.168.10.3	192.168.10.1	ICMP Echo Request	CRC

- Receives a packet from the network protocol
- Adds a header and trailer to create a frame
- Converts the frame into bits for transmission on the medium

Figure 2-11 A NIC handles outgoing data to be sent to the network medium

© Cengage Learning 2017

NICs and MAC Addresses

- NIC manufacturers ensure that every NIC produced has a unique address
    - Networks won’t function correctly if duplicate MAC addresses exist
- MAC address is stored in read-only memory (ROM) on the NIC
- Two 24-bit hexadecimal numbers
    - 24-bit manufacturer ID called OUI
    - 24-bit serial number assigned by the manufacturer
- 48-bit address expressed in 12 hexadecimal digits: 04-40-31-5B-1A-C4

© Cengage Learning 2017

The NIC as Gatekeeper

- When a frame arrives at a NIC, the NIC check’s the frame’s destination MAC address to see whether it matches it’s built-in MAC address
- NIC only permits inbound communications if the destination MAC:
  - Matches the NICs burned-in address
  - Is a **broadcast address** (ff-ff-ff-ff-ff-ff)
  - NIC is in a special mode called promiscuous
- When the destination MAC address matches the MAC *burned-in address* (BIA), or the *physical address* of a NIC, it’s a **unicast frame**
  - Intended for a single computer

© Cengage Learning 2017

The NIC as Gatekeeper

- When the destination is the broadcast address, it’s a **broadcast frame**
  - Broadcast frames are intended to be processed by all computers on the network
- **Promiscuous mode** – turns off the gatekeeper functions and enables the NIC to process all frames it sees
  - Used by software called a protocol analyzer or packet sniffer

© Cengage Learning 2017

NIC Indicator Lights

- NICs have indicator lights to show status information
  - Usually a link status indicator and an activity indicator
- The link light is usually green when the NIC has a valid connection to the network medium
- Some NICs support multiple speeds
  - There is usually a separate light for each speed so that you can determine at what speed the NIC is connected to the hub or switch
  - In other cases the light is a different color for each speed, such as amber for 100 Mbps and green for 1000 Mbps

© Cengage Learning 2017

Selecting a NIC

- NICs are often built into motherboard
  - However, an additional NIC or a faster NIC may need to be installed
- When selecting a NIC you need to select correct bus interface
  - The connection the NIC makes to the motherboard is the bus connection
- The NIC driver (software) must be available for your OS
- Desktop NICs versus server NICs
  - For desktops a standard NIC is good enough
  - For servers, consider a NIC with onboard memory, multiple ports and performs faster

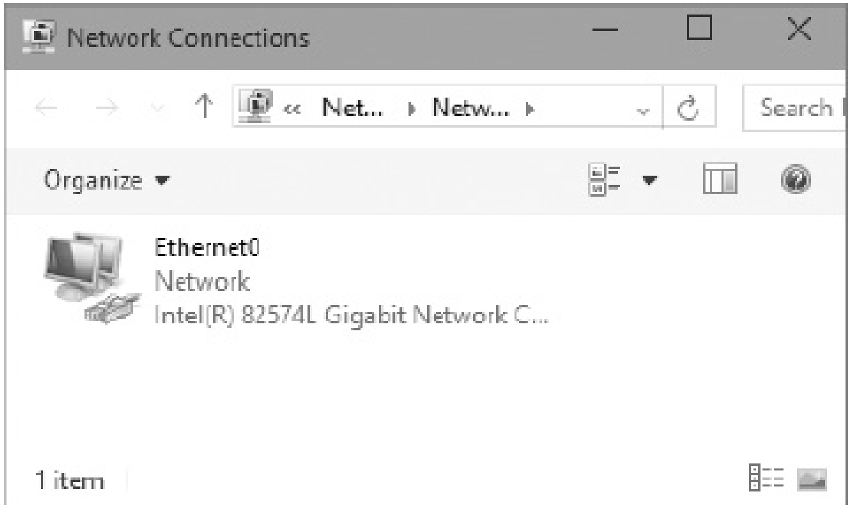
© Cengage Learning 2017

NIC Drivers

- Most OSs ship with drivers for wide range of NICs
- Most NICs include drivers for the most common OSs
  - In most cases you only need to install the NIC and restart your computer
    - If the OS has a suitable driver available it is installed automatically
- After installation, Windows 8.1 and later shows your installed NIC as a Network Connection
- In Windows, each connection is assigned a name
  - Which you can rename

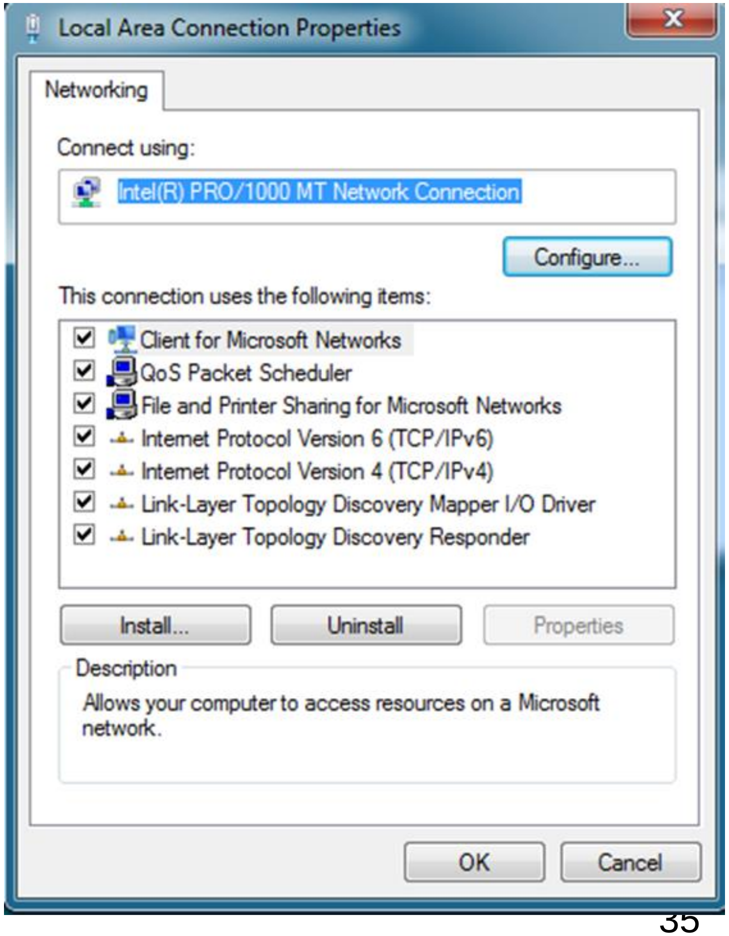
© Cengage Learning 2017

NIC Drivers



Ethernet0
Network
Intel(R) 82574L Gigabit Network C...

Figure 2-12 The Network Connections window in Windows 10



Connect using:

Intel(R) PRO/1000 MT Network Connection

This connection uses the following items:

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

Description

Allows your computer to access resources on a Microsoft network.

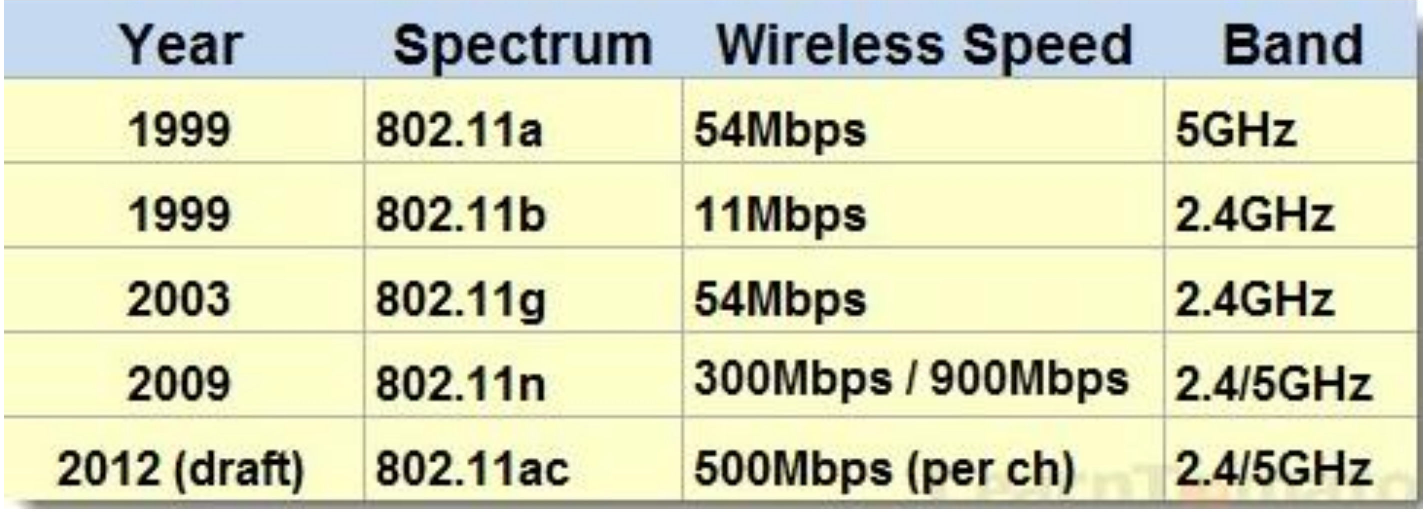
© Cengage Learning 2017

Wireless NICs

- Wireless NICs must be chosen according to type of wireless AP being used
- Typical are Wireless-n, 802.11ac or 802.11 a/b/g/n
  - The letter a,b,g, n, and ac refer to the wireless networking standard the device supports
- Wireless NICs connect to network using **service set identifier (SSID)**
  - SSID is the name assigned to the wireless network
- You may also need to enter a security key or a username and password, depending on the network’s security configuration

© Cengage Learning 2017

Wireless LAN Standards



Year	Spectrum	Wireless Speed	Band
1999	802.11a	54Mbps	5GHz
1999	802.11b	11Mbps	2.4GHz
2003	802.11g	54Mbps	2.4GHz
2009	802.11n	300Mbps / 900Mbps	2.4/5GHz
2012 (draft)	802.11ac	500Mbps (per ch)	2.4/5GHz

- Beside the speed and frequency band, other different are:
  - – Number of channels
  - – Cell size (coverage area)

© Cengage Learning 2017

Routers

- Most complex device
- Connect LANs together to create an internetwork (Network of Networks)

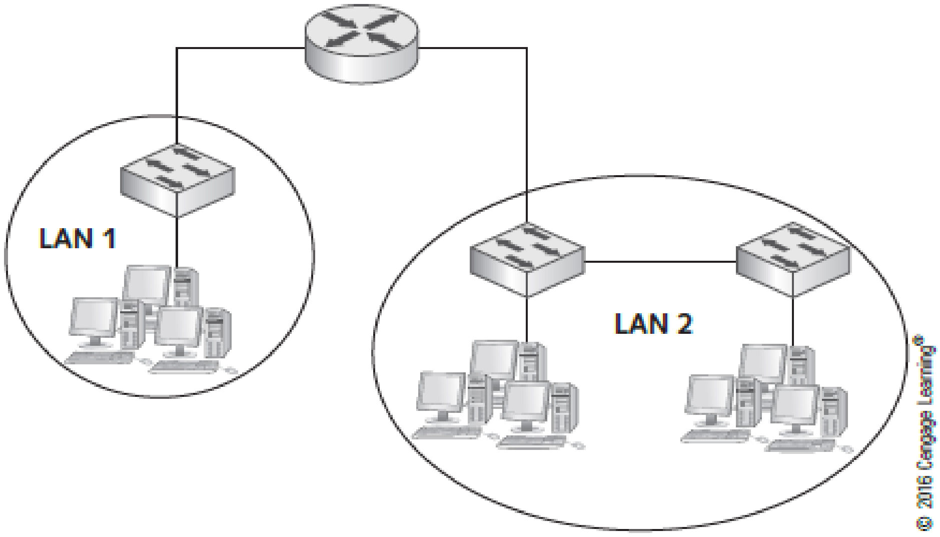


Figure 2-15 Two LANs connected by a router to make an internetwork

© Cengage Learning 2017

Routers

- **Routers** are devices that enable multiple LANs to communicate with one another by forwarding packets from one LAN to another

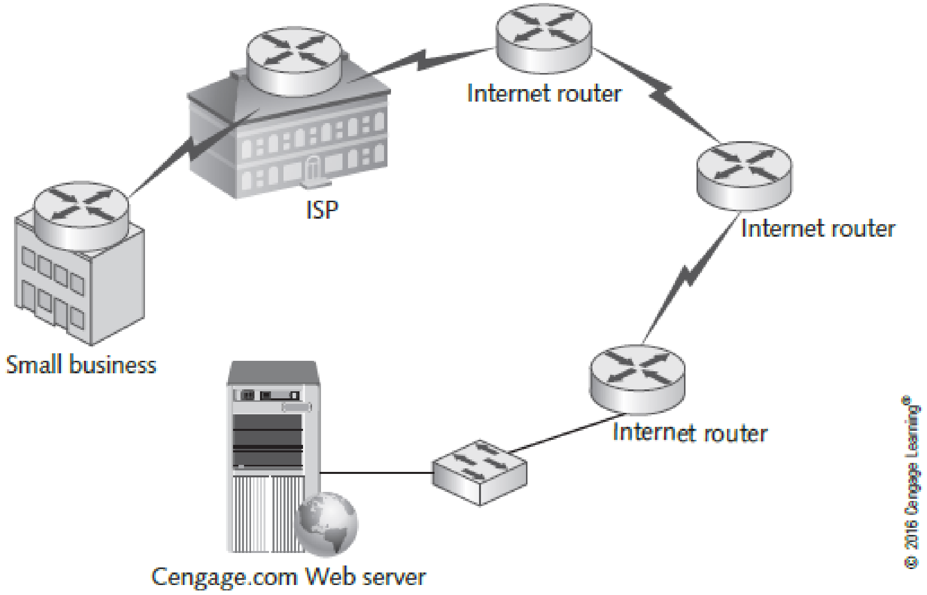


Figure 2-16 Routers interconnect LANs to form the Internet

© Cengage Learning 2017

Routers

- The following are the differences between routers and switches
  - Routers connect LANs, switches connect computers to form LANs
  - Routers work with logical (IP) addresses, switches work with physical (MAC) addresses
  - Routers work with packets, switches with frames
  - Routers don’t forward broadcasts, switches do
  - Routers use routing tables, switches use switching tables

© Cengage Learning 2017

Routers Connect LANs

- As computers are added to a LAN, effective communication can suffer
  - Broadcast traffic is forwarded to all members of a LAN and can cause a network to become congested
- The picture on the next slide shows 3 different groups of users and 3 different servers all connected by switches
  - Since they are connected by switches, they are all part of the same LAN and all broadcast traffic will be heard by all devices

© Cengage Learning 2017

Routers Connect LANs

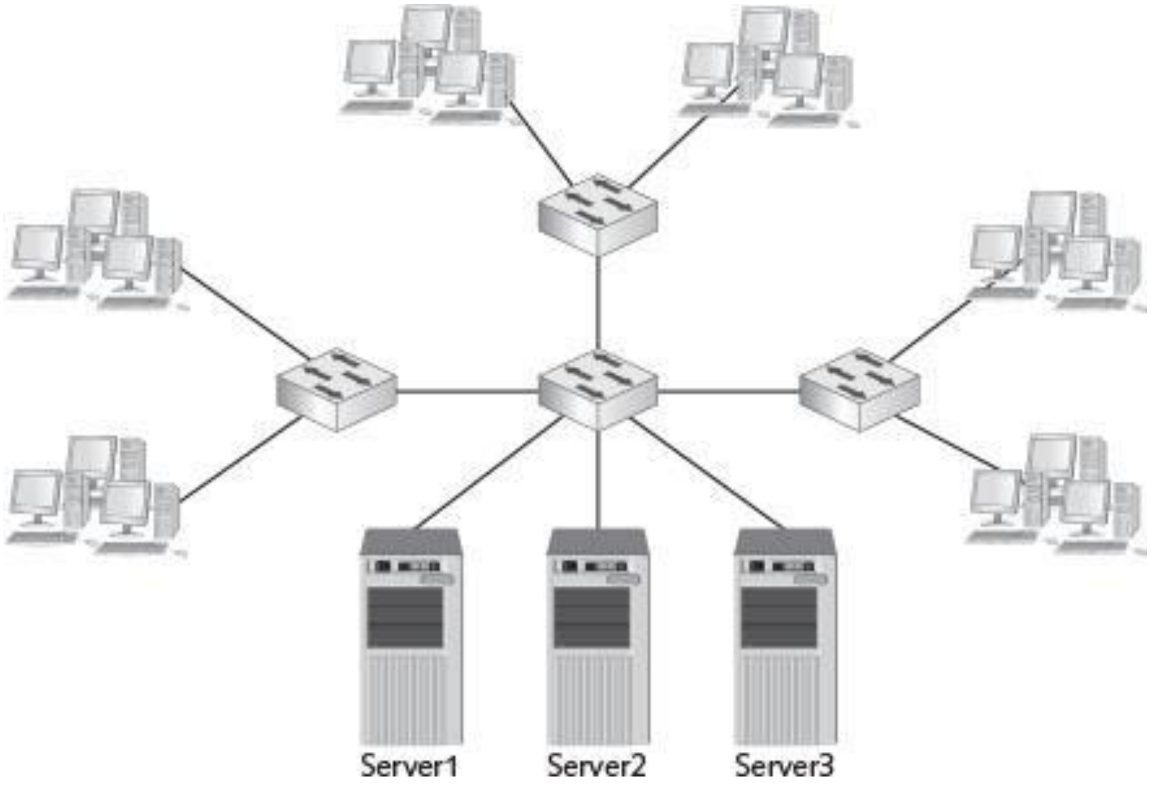
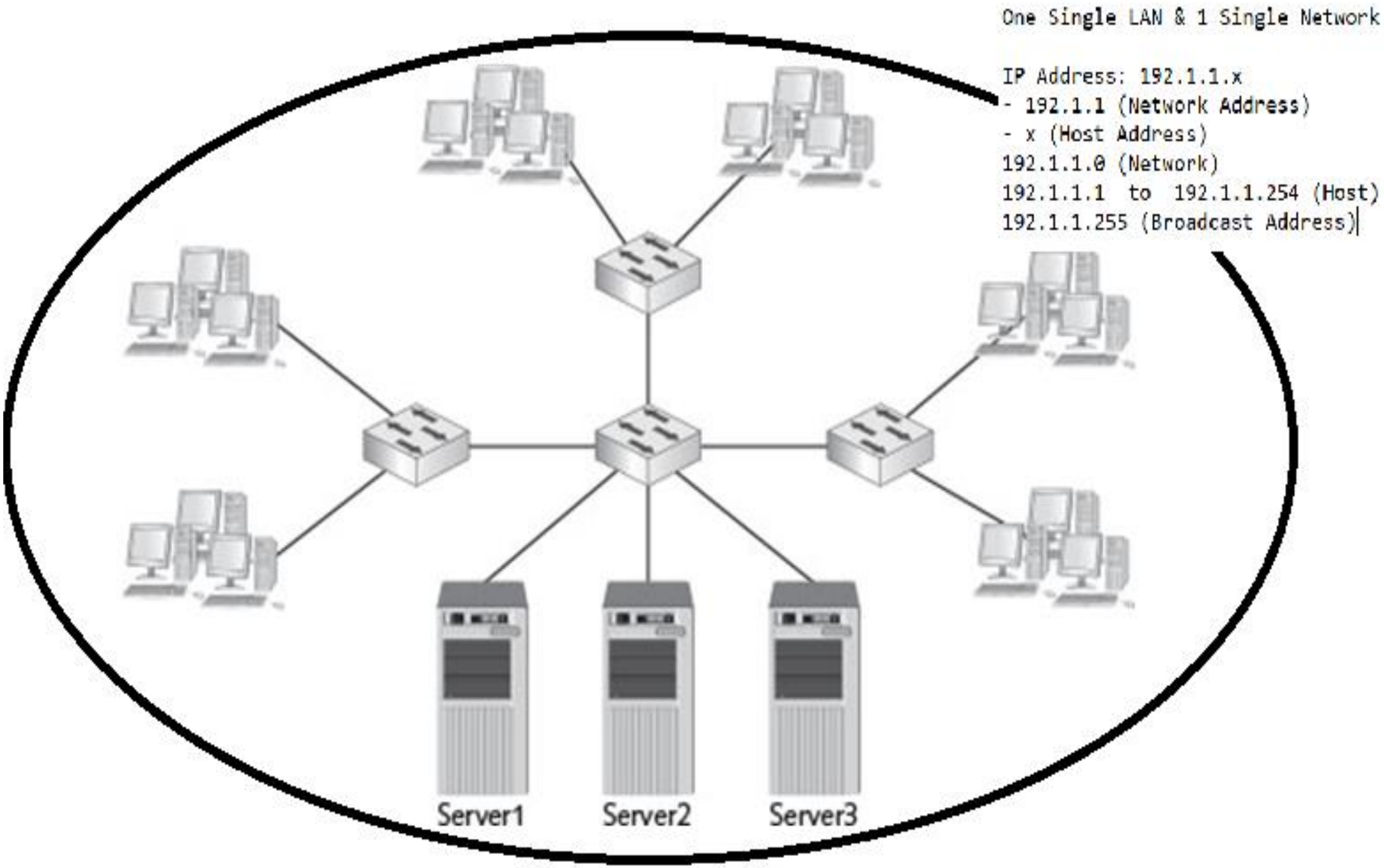


Figure 2-17 A large LAN connected by switches

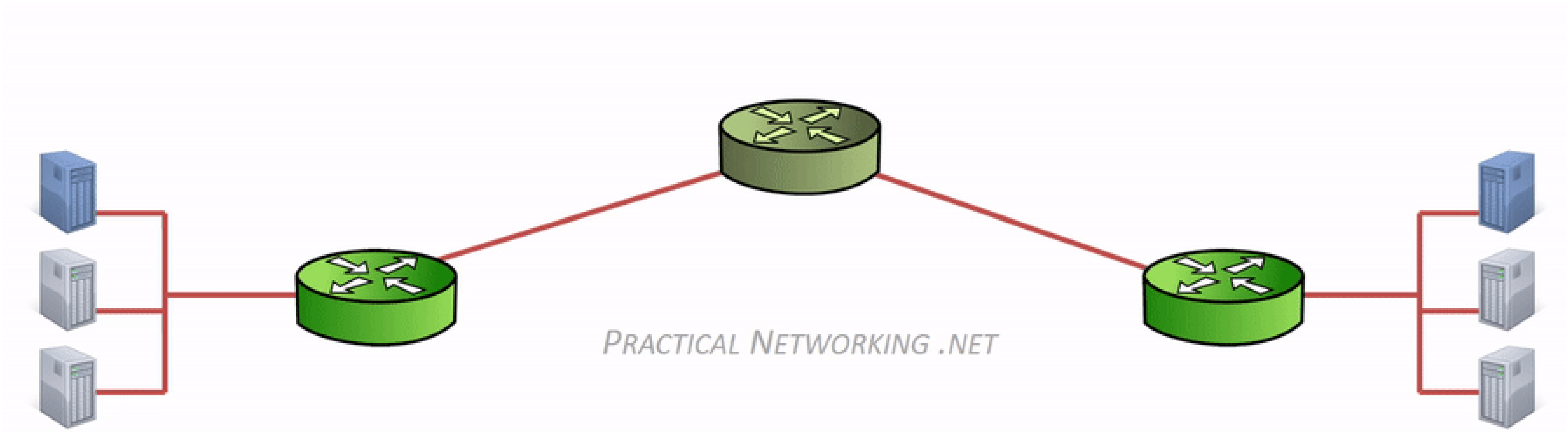
© Cengage Learning 2017



One Single LAN & 1 Single Network

IP Address: 192.1.1.x
- 192.1.1 (Network Address)
- x (Host Address)
192.1.1.0 (Network)
192.1.1.1 to 192.1.1.254 (Host)
192.1.1.255 (Broadcast Address)

© Cengage Learning 2017



Notice between each Router, the MAC address header is stripped and regenerated to get it to the next hop. The IP header generated by the first computer is only stripped off by the final computer, hence the IP header handled the “end to end” delivery, and each of the four *different* MAC headers involved in this animation handled the “hop to hop” delivery.

https://www.practicalnetworking.net/series/packet-traveling/osi-model/

© Cengage Learning 2017

Difference between Hub, Switch and Router

https://www.youtube.com/watch?v=1z0ULvg_pW8

© Cengage Learning 2017

Routers Connect LANs

- The picture on the next slide shows a better solution for the previous network
- The administrator groups users and servers together based on their department or function
  - The router is used to **connect** 3 separate LANs in order to contain broadcast traffic and facilitate more effective communication in each department LAN

© Cengage Learning 2017

Routers Connect LANs

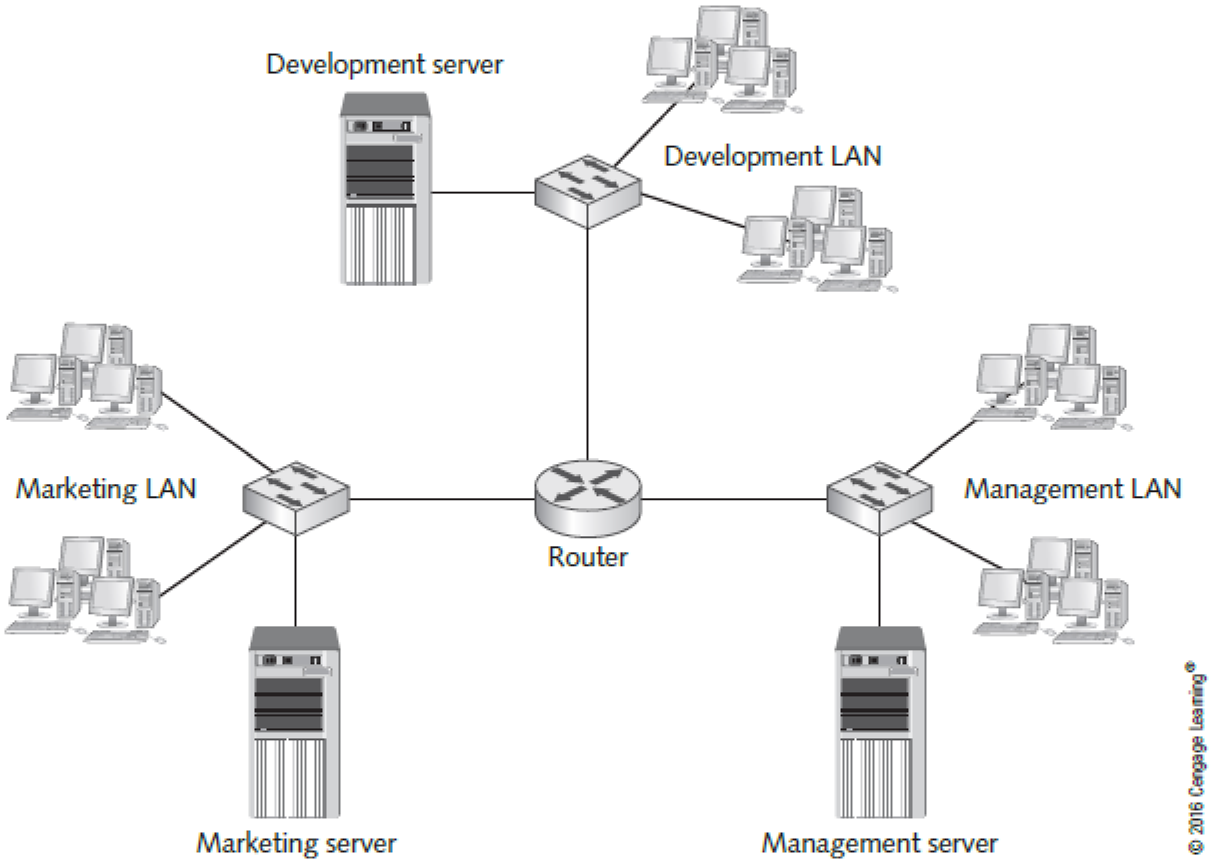
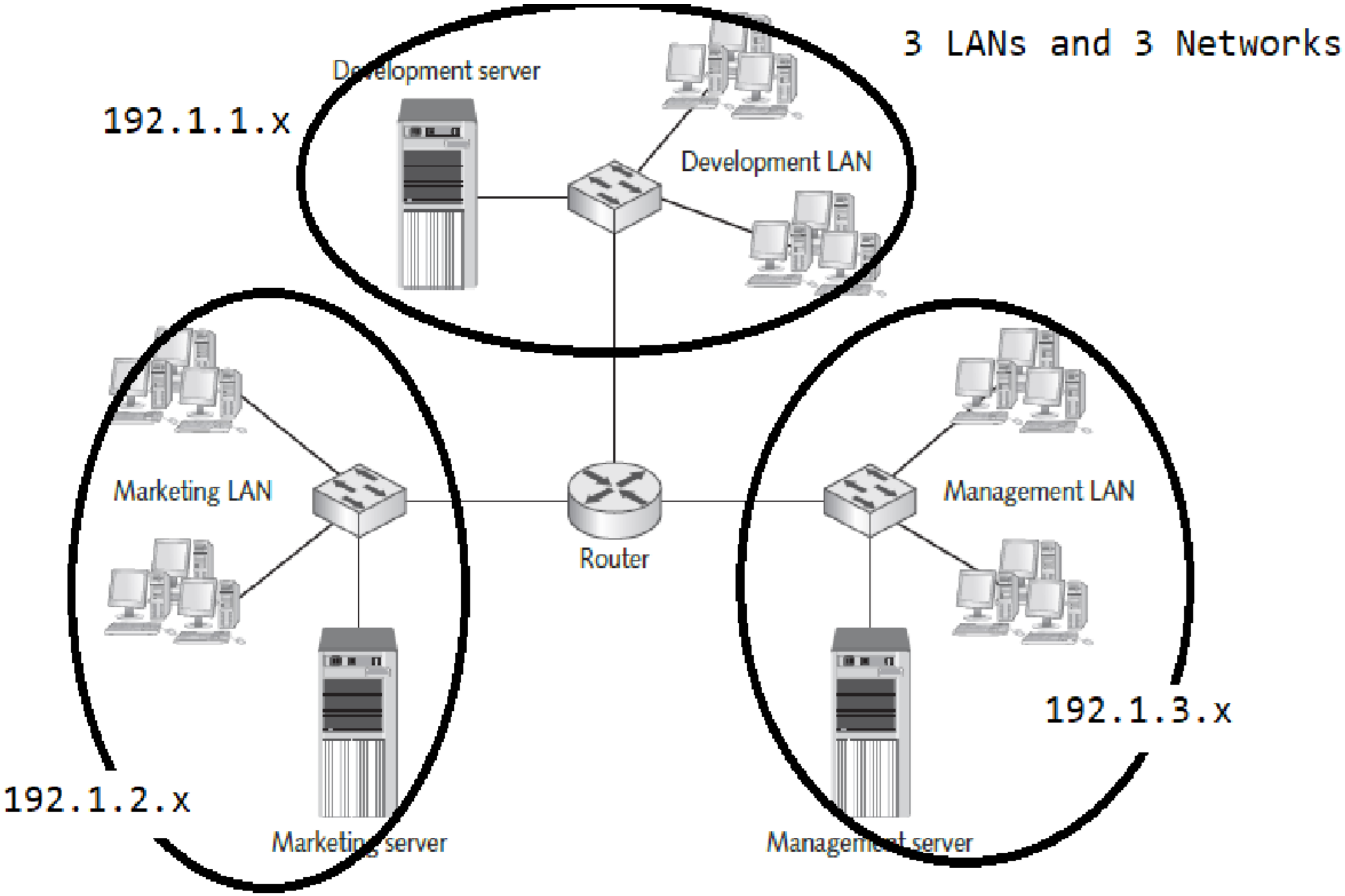


Figure 2-18 Three smaller LANs connected by a router

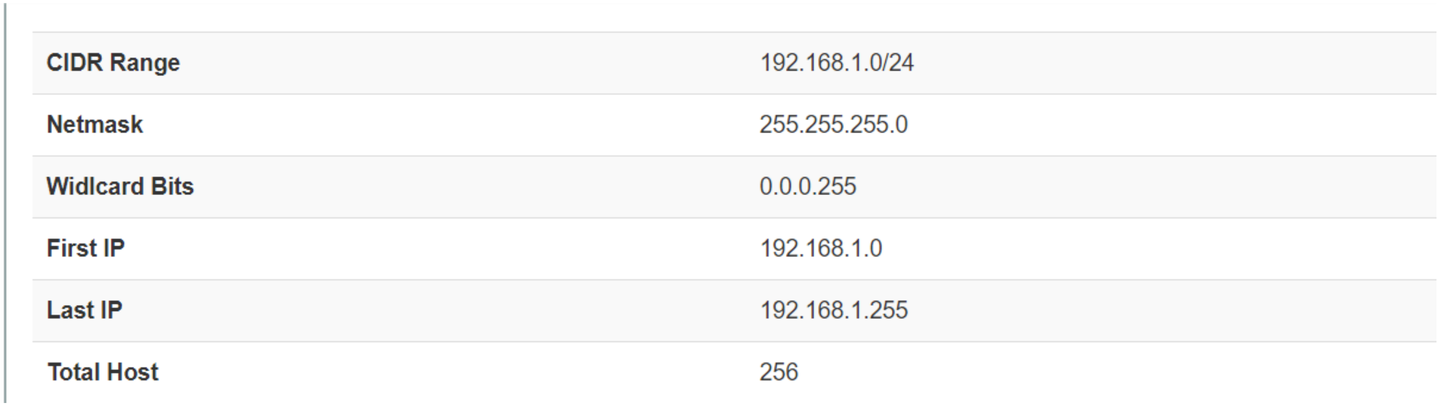
© Cengage Learning 2017



© Cengage Learning 2017

CIDR IP address (revision)

Online tools



CIDR Range	192.168.1.0/24
Netmask	255.255.255.0
Widlcard Bits	0.0.0.255
First IP	192.168.1.0
Last IP	192.168.1.255
Total Host	256

subnetmask: 11111111 11111111 11111111 00000000

RESERVED IP ADDRESS	
192.168.1.0	subnet
192.168.1.255	broadcast
256-2=254	Total usable hosts

© Cengage Learning 2016

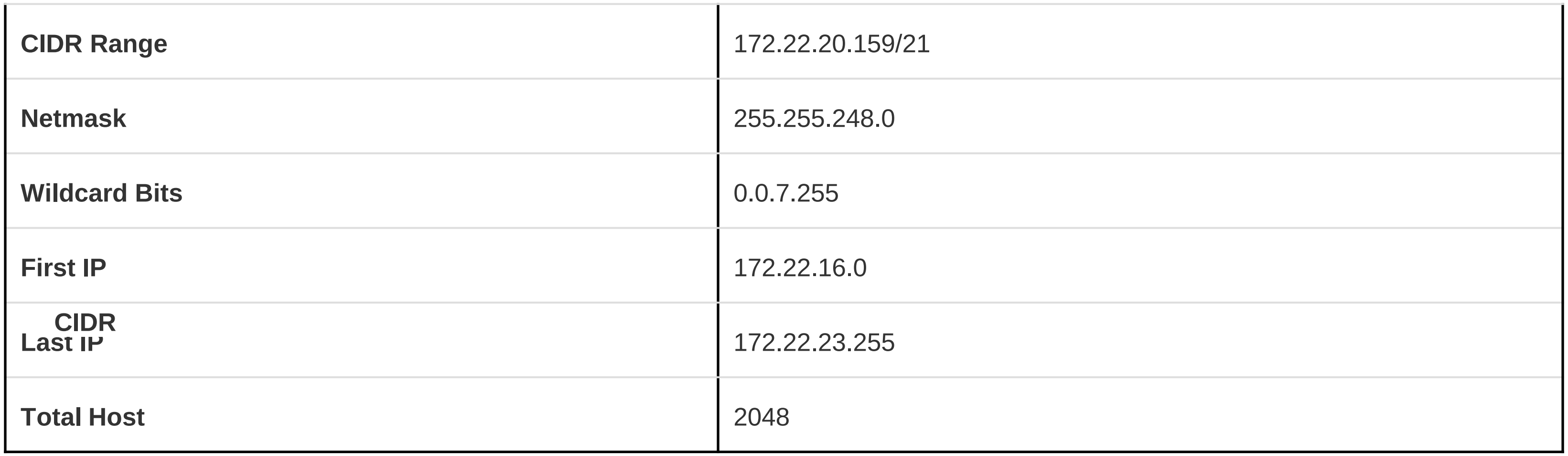
Result

CIDR Range	192.168.1.0/23
Netmask	255.255.254.0
Wildcard Bits	0.0.1.255
First IP	192.168.0.0
Last IP	192.168.1.255
Total Host	512

usable hosts: 512-2=510
Subnet mask: 11111111 11111111 11111110 00000000

© Cengage Learning 2016

SPStudent network

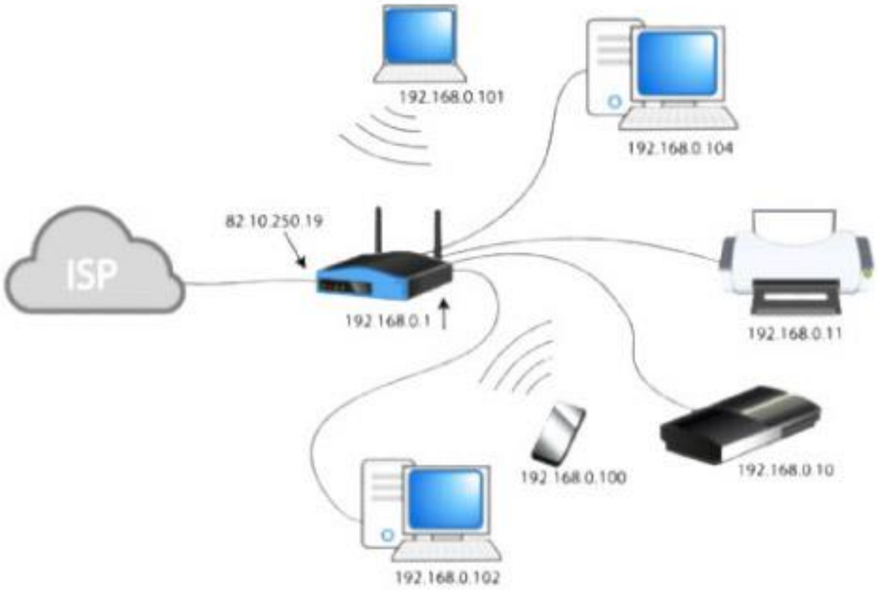


CIDR Range	172.22.20.159/21
Netmask	255.255.248.0
Wildcard Bits	0.0.7.255
First IP	172.22.16.0
CIDR **Last IP**	172.22.23.255
Total Host	2048

subnetmask: 11111111 11111111 11111000 00000000
usable hosts: 2048 -2=2046

© Cengage Learning 2016

LAN
Privated IP address

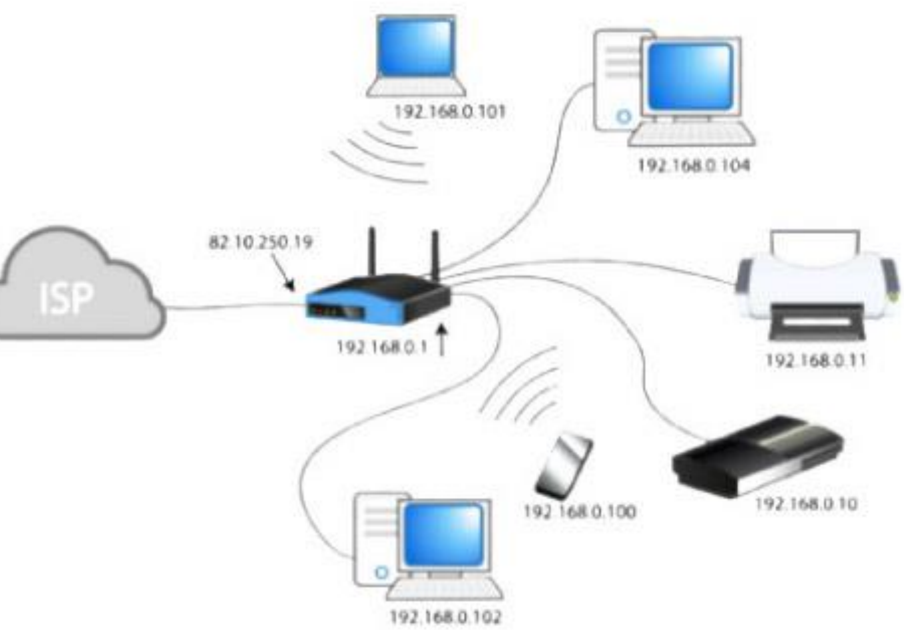


Reserved for private networks.
The organizations that distribute IP addresses to the world reserves a range of IP addresses for *private networks*.

- **192.168.0.0 - 192.168.255.255** (65,536 IP addresses)
- **172.16.0.0 - 172.31.255.255** (1,048,576 IP addresses)
- **10.0.0.0 - 10.255.255.255** (16,777,216 IP addresses)

© Cengage Learning 2017

Private IP address for LAN
Public IP Address for router



The power of two.

The two work together as a team. Both IPs are needed to so that when you go to Amazon.com, the Internet knows to send the information you request back to your computer and not someone else's (including not someone else in your home, using the same network).

The go-between for the public and non-public IP address is your *router*:

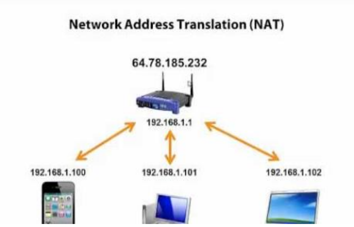
Your router has assigned to your computer an internal IP address, to which you're connected wirelessly or directly. (It also assigns a different, but similar internal IP address to any other computer connected on your network.)

Your router "asks" and receives an external IP address from your Internet Service Provider (Comcast, Verizon, etc.). This external IP address identifies your computer to the Internet.

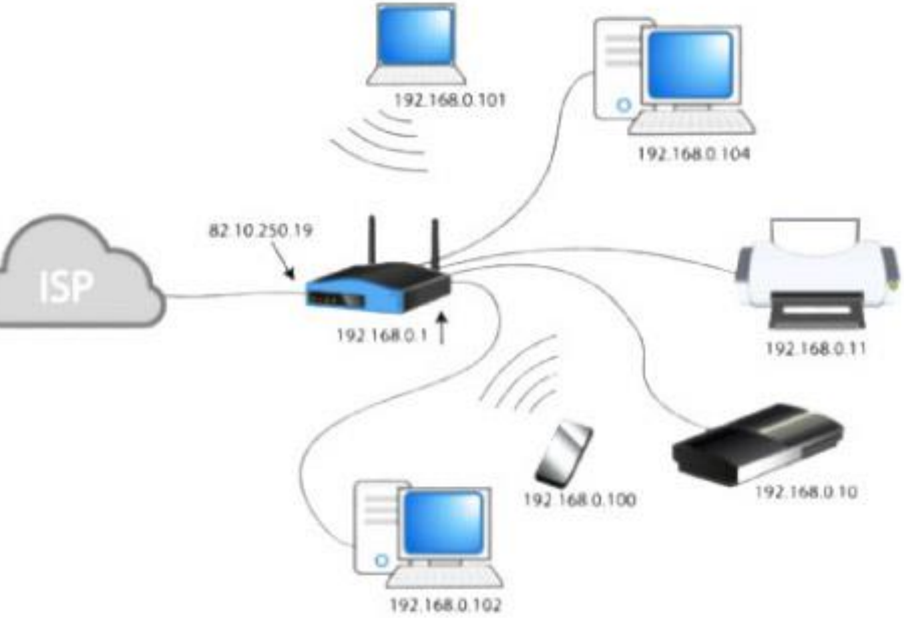
If there are two computers connected to your home router, each computer will show the same public IP address, but each has its own internal IP address. That's why you get your own email and not anyone else's—your router knows who made the request and who gets the reply.

© Cengage Learning 2017

[redacted]



Network Address Translation NAT

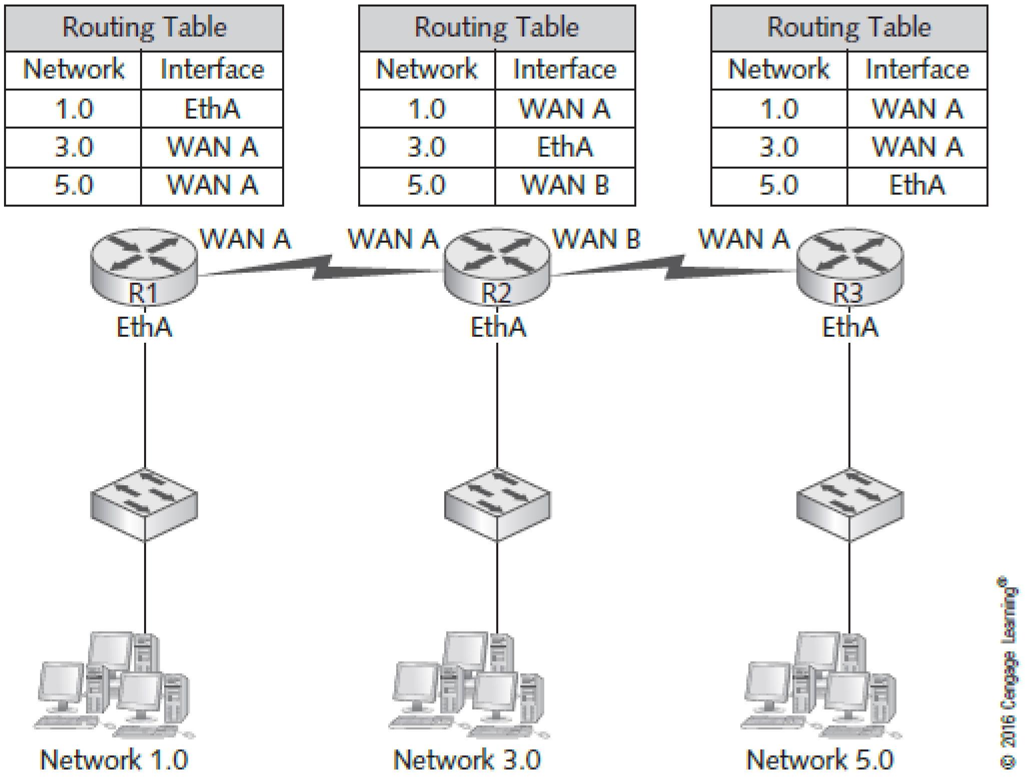


Network address translation (**NAT**) is a method of remapping one IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device

In a typical configuration, a local network uses one of the designated *private* IP address subnets (RFC 1918). A router on that network has a private address in that address space. The router is also connected to the Internet with a *public* address assigned by an Internet service provider. As traffic passes from the local network to the Internet, the source address in each packet is translated on the fly from a private address to the public address. The router tracks basic data about each active connection (particularly the destination address and port). When a reply returns to the router, it uses the connection tracking data it stored during the outbound phase to determine the private address on the internal network to which to forward the reply.

© Cengage Learning 2017

Routers Work with IP Addresses and Routing Tables



Routing Table

Network	Interface
1.0	EthA
3.0	WAN A
5.0	WAN A

Routing Table

Network	Interface
1.0	WAN A
3.0	EthA
5.0	WAN B

Routing Table

Network	Interface
1.0	WAN A
3.0	WAN A
5.0	EthA

© 2016 Cengage Learning®

Figure 2-21 Packets are forwarded through multiple routers

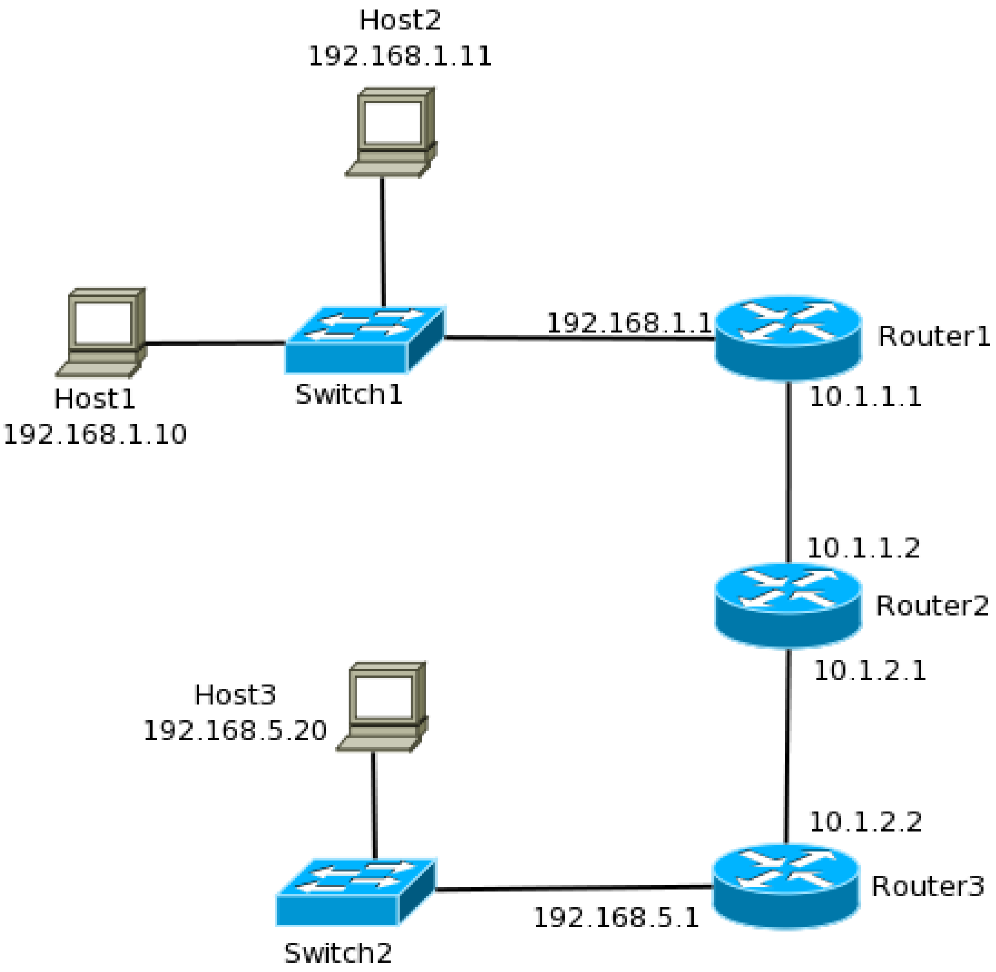
© Cengage Learning 2017

Routers Work with IP Addresses and Routing Tables

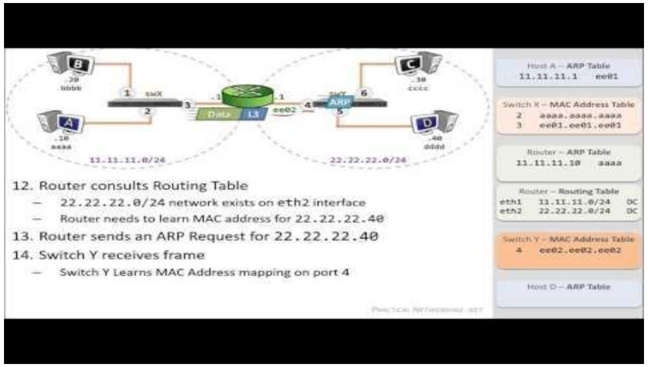
- **Default route** — where to send a packet when the router doesn’t have an entry in its routing table
- Network unreachable — Message sent when the network can’t be found and no default route
- **Default gateway** — In a computer’s IP address configuration – the IP address of the computer’s router

© Cengage Learning 2017

Case Study



© Cengage Learning 2017



12. Router consults Routing Table
    - 22.22.22.0/24 network exists on eth2 interface
    - Router needs to learn MAC address for 22.22.22.40
13. Router sends an ARP Request for 22.22.22.40
14. Switch Y receives frame
    - Switch Y Learns MAC Address mapping on port 4

Host A – ARP Table

11.11.11.1 ee01

Switch X – MAC Address Table

2 aaaa.aaaa.aaaa

3 ee01.ee01.ee01

Router – ARP Table

11.11.11.10 aaaa

Router – Routing Table

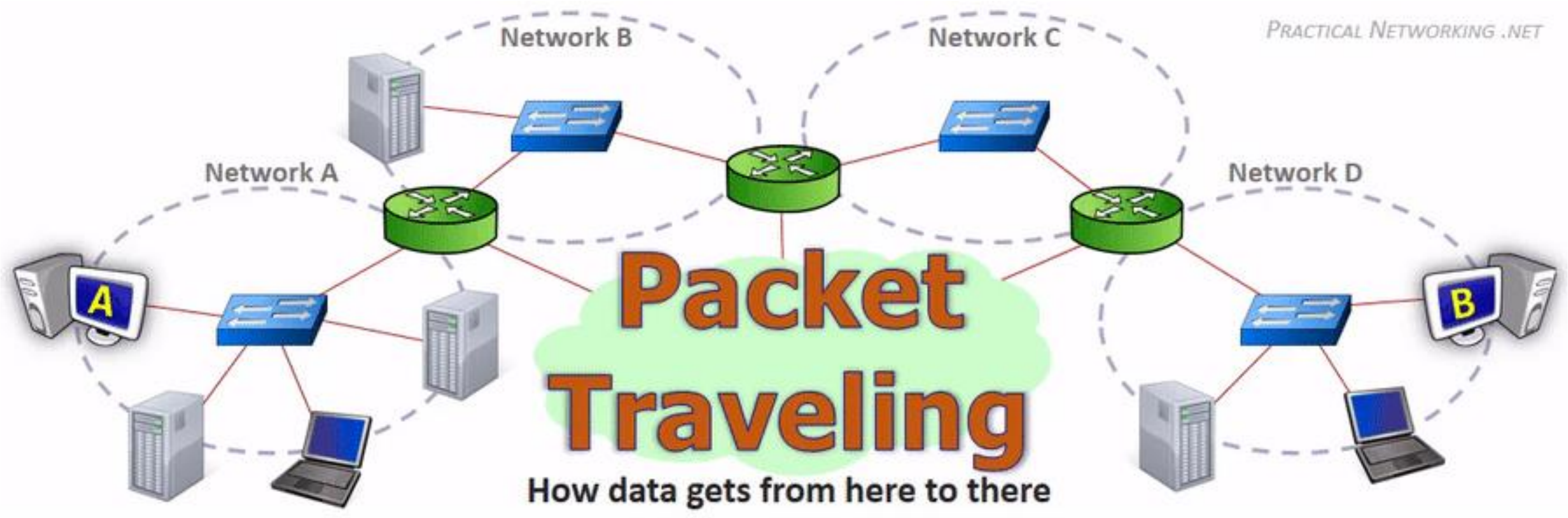
eth1 11.11.11.0/24 DC

eth2 22.22.22.0/24 DC

Switch Y – MAC Address Table

4 ee02.ee02.ee02

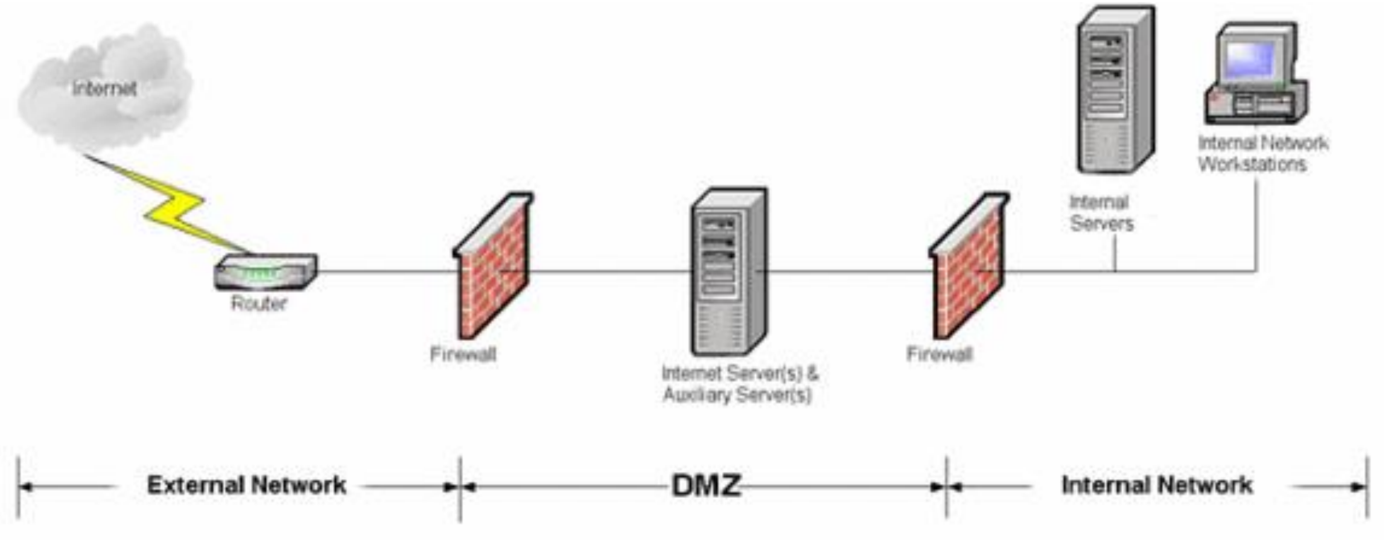
Host D – ARP Table



© Cengage Learning 2017

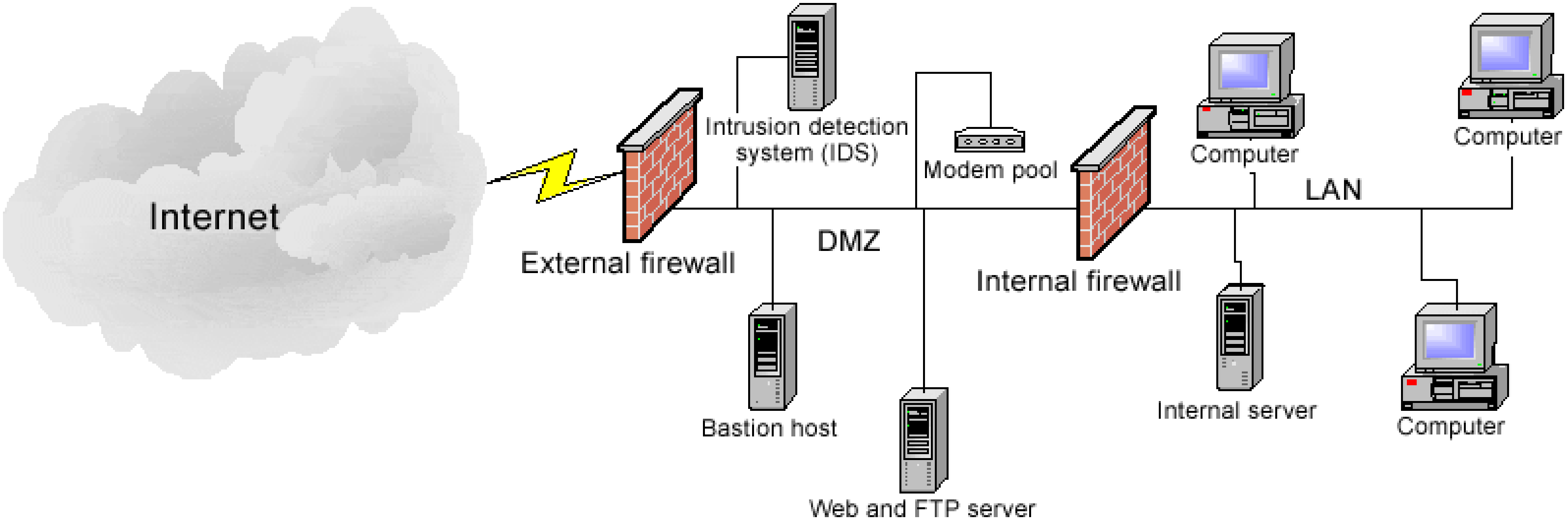
Firewall

an external firewall to protect the web server itself from attacks and an internal firewall to protect the internal corporate systems in case the web server is breached.



© Cengage Learning 2017

What servers in DMZ zone?



© Cengage Learning 2017

Summary

- Network repeaters and hubs take incoming bit signals and repeat those signals at their original strength out all connected ports
- Network switches interconnect multiple computers just as hubs do
- Switches use switching tables to determine which MAC address can be found on which port
- Access points are a central device in a wireless network and perform a similar function to hubs

© Cengage Learning 2017

Summary

- Network interface cards create and mediate the connection between the computer and network medium
- Wireless NICs perform the same function as wired NICs
- Routers connect LANs to one another and forward packets from one LAN to another according to the destination network specified by the destination IP address in the packet
- Unlike hubs and switches, routers do not forward broadcast frames

© Cengage Learning 2017