

# Chapter 4

Networks Protocols and Routing

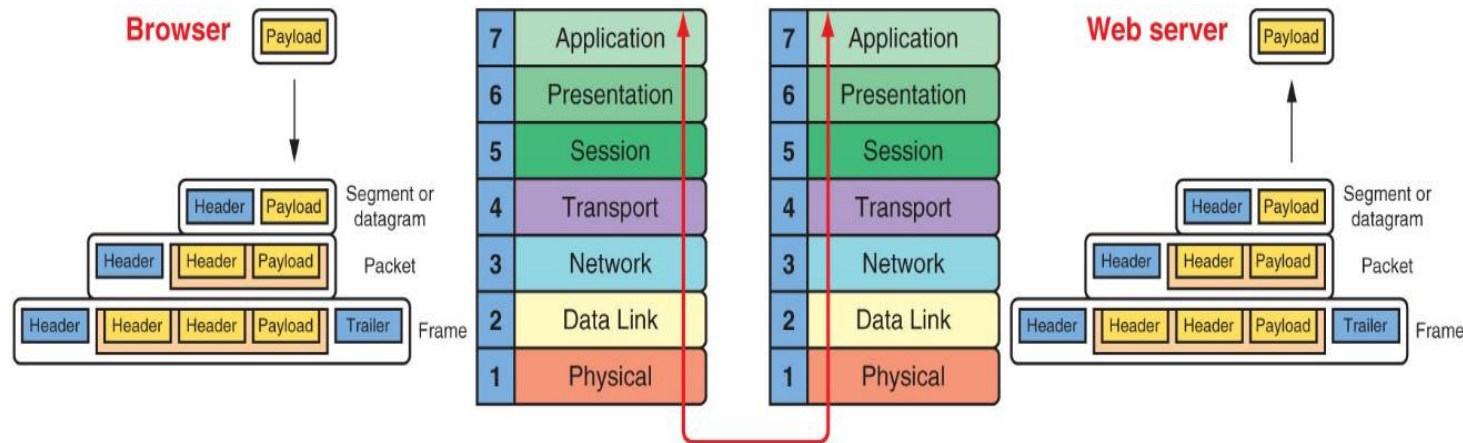
**Abdoul Rassaki**  
**arassaki@iie.ac.za**

# Objectives

- Describe the functions of core TCP/IP protocols
- Identify how each protocol's information is formatted in a TCP/IP message
- Explain how routers manage internetwork communications
- Employ various TCP/IP utilities for network discovery and troubleshooting

# TCP/IP Core Protocols (1 of 3)

- TCP/IP—A suite of protocols including:
  - TCP, IP, UDP, ARP, and many others
- TCP/IP protocols add a header to data inherited from the layer above it



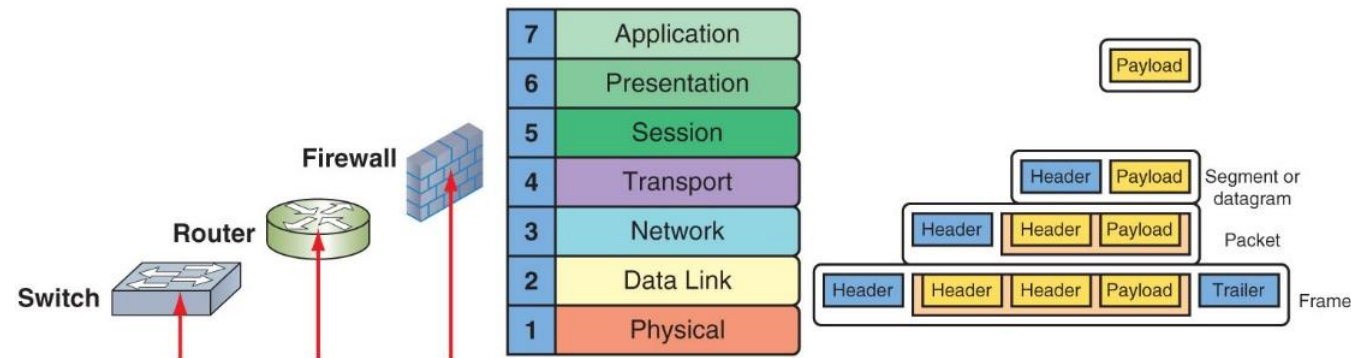
**Figure 4-1** Each layer adds its own data and addresses its transmission to the corresponding layer in the destination device

# TCP/IP Core Protocols (2 of 3)

- Layers 7, 6, and 5—Data and instructions, known as payload, are generated by applications running on source host
- Layer 4—A Transport layer protocol, usually TCP or UDP, adds a header to the payload
  - This header includes a port number to identify the receiving app
- Layer 3—Network layer adds its own header and becomes a packet
- Layer 2—Packet is passed to Data Link layer on NIC, which encapsulates data with its own header and trailer, creating a frame
- Layer 1—Physical layer on the NIC receives the frame and places the transmission on the network

# TCP/IP Core Protocols (3 of 3)

- Receiving host de-encapsulates the message at each layer in reverse order and presents payload to the receiving applications
  - In transit, transmissions might pass through a number of connectivity devices
- Connectivity devices are specialized devices that allow two or more networks or multiple parts of one network to connect and exchange data
  - Known by the highest OSI layer they read and process



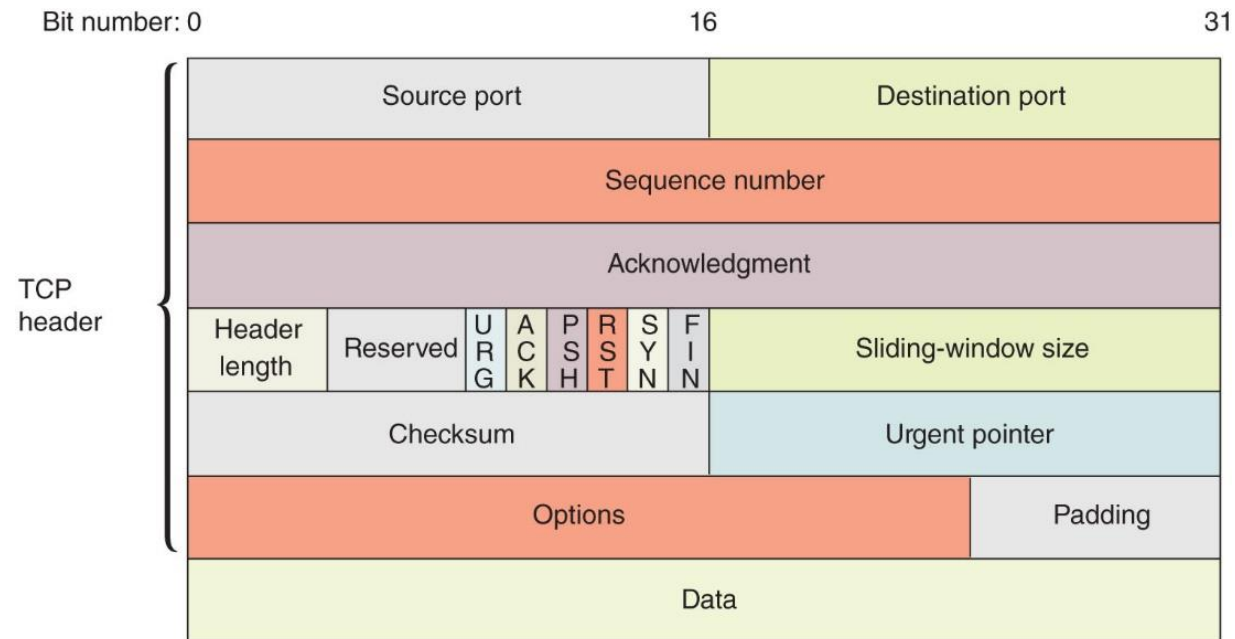
**Figure 4-2** Connectivity devices are known by the highest OSI layer they read and process

# TCP (Transmission Control Protocol) (1 of 4)

- TCP operates in the Transport layer of OSI model
- Three characteristics of TCP:
  - **Connection-oriented**—TCP ensures that a connection or session is established by using a three-step process called a **three-way handshake**
  - **Sequencing and checksums**—TCP sends a character string called a **checksum** that is checked by the destination host along with a sequence number for each segment
  - **Flow control**—Gauges rate of transmission based on how quickly recipient can accept data

# TCP (2 of 4)

- Fields in a TCP Segment



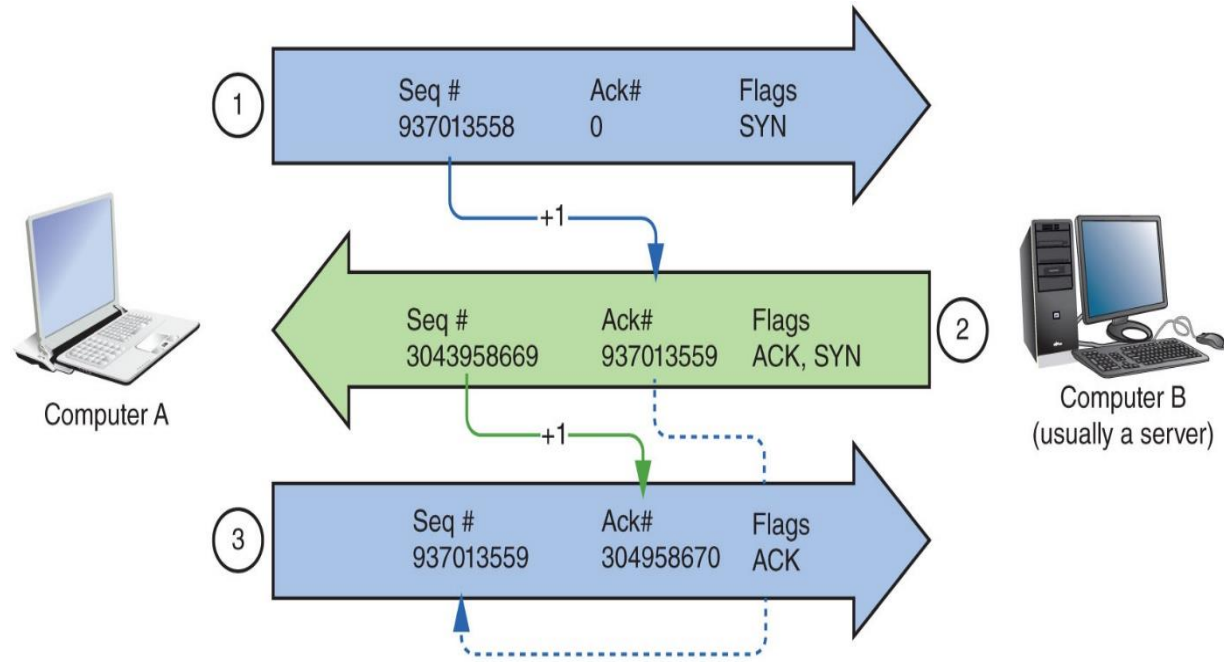
**Figure 4-3** A TCP segment

# TCP (3 of 4)

- TCP uses a three-way handshake to establish a connection
  - Three transmission sent before data transmission:
    - Step 1—Request for a connection (SYN)
    - Step 2—Response to the request (SYN/ACK)
    - Step 3—Connection established (ACK)
  - After the three initial messages, the payload or data is sent
  - Sequence numbers will be increased by the number of bits included in each received segment
    - Confirms the correct length of message was received



# TCP (4 of 4)



**Figure 4-4** The three-way handshake process establishes a TCP session

# UDP (User Datagram Protocol) (1 of 2)

- UDP is an unreliable, connectionless protocol:
  - No three-way handshake is performed
  - Does not guarantee delivery of data
- UDP provides no error checking, sequencing, or flow control
  - Makes UDP more efficient than TCP
- Useful for live audio or video transmissions over the Internet
- Also more efficient for carrying messages that fit within one data packet
- A UDP header contains only four fields: Source port, Destination port, Length, and Checksum
  - Use of Checksum field in UDP is optional in IPv4, but required in IPv6

# UDP (2 of 2)

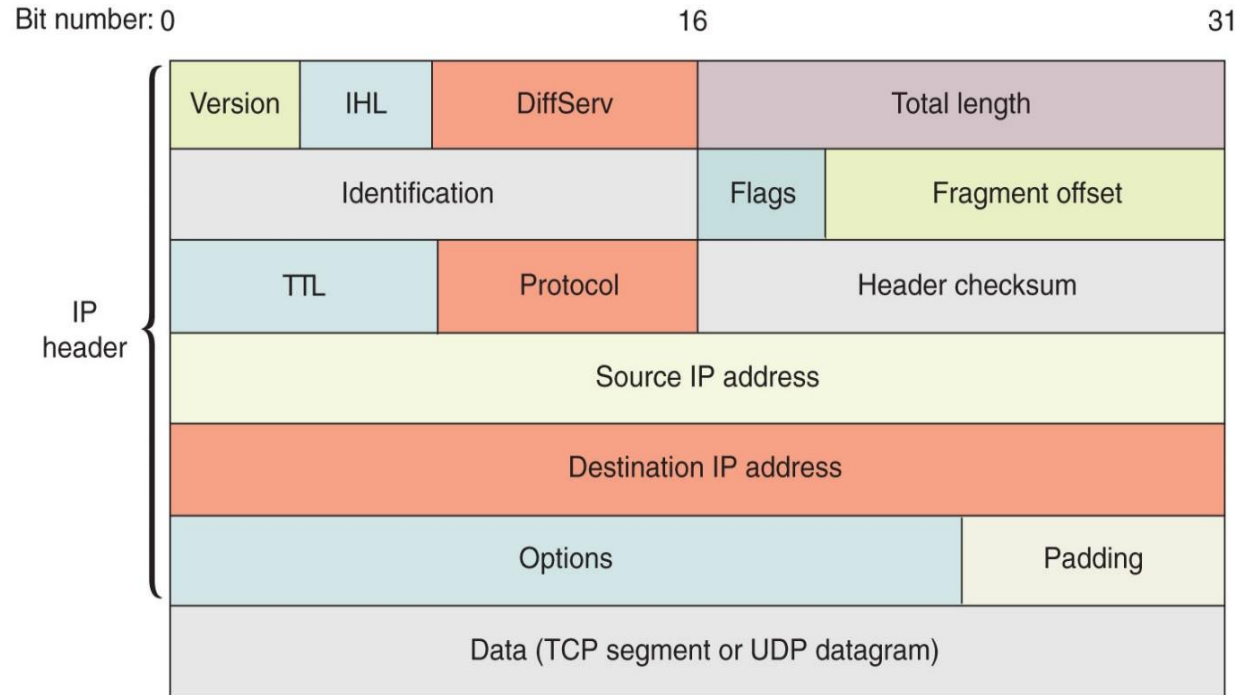


**Figure 4-6** A UDP datagram

# IP (Internet Protocol) (1 of 4)

- IP operates at the Network layer of the OSI model:
  - Specifies where data should be delivered
  - Identifies the data's source and destination IP addresses
- IP enables TCP/IP to internetwork
  - Traverse more than one LAN segment and more than one type of network through a router
- IP is an unreliable, connectionless protocol
  - Means that IP does not guarantee delivery of data and no session is established before data is transmitted
  - IP depends on TCP to ensure messages are put back together in the right order and to ensure each message reaches the correct application on the receiving host

# IP (2 of 4)

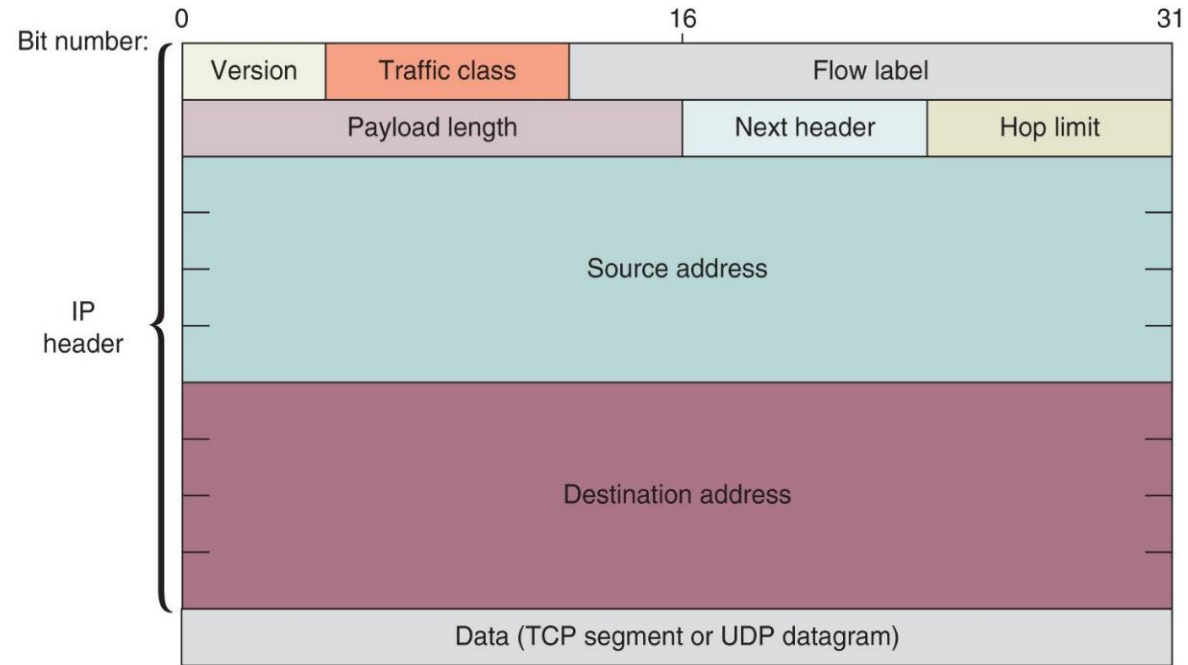


**Figure 4-7** An IPv4 packet

# IP (3 of 4)

- IPv6 packets:
  - IPv6 uses a different packet format than IPv4
  - Accommodate the much longer IPv6 addresses
  - There is no Fragment offset field
    - IPv6 hosts adjust their packet sizes to fit the requirements of the network before sending IPv6 messages

# IP (4 of 4)



**Figure 4-9** An IPv6 packet

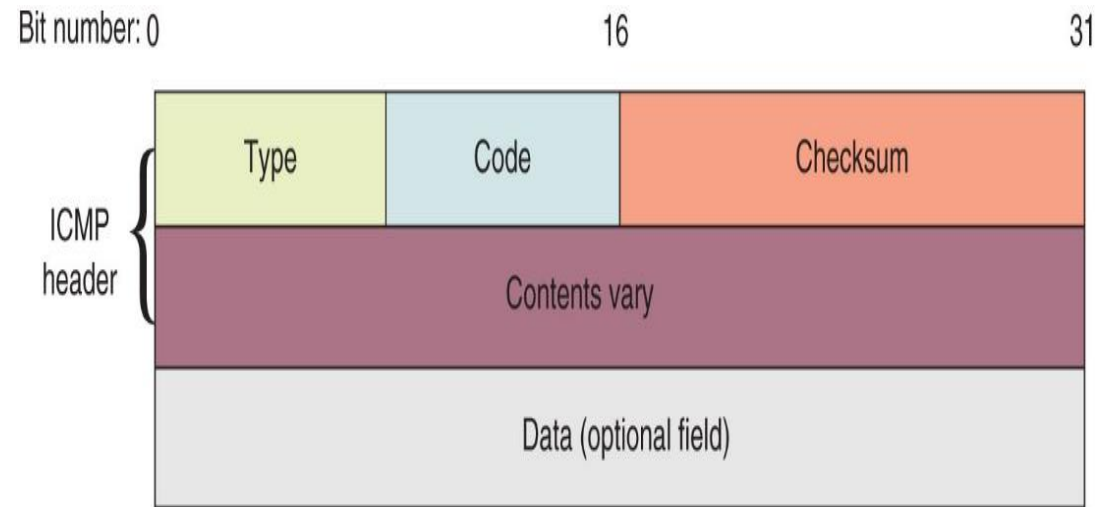
# ICMP (Internet Control Message Protocol)

## (1 of 3)

- ICMP is a Network layer, core protocol that reports on the success or failure of data delivery
- ICMP can indicate:
  - When part of a network is congested
  - When data fails to reach its destination
  - When data has been discarded because the allotted TTL has expired
- ICMP announces transmission failures to the sender
  - But does not correct errors it detects
- Provides critical information for troubleshooting network problems
- ICMPv6 on IPV6 networks performs the functions of ICMP and ARP on IPv4 networks



# ICMP (2 of 3)



**Figure 4-11** An ICMP packet

# ICMP (3 of 3)

- Table 4-7 An ICMP packet

Field	Length	Function
Type	8 bits	Indicates the type of ICMP message, such as Destination Unreachable
Code	8 bits	Indicates the subtype of the message, such as Destination host unknown
Checksum	16 bits	Allows the receiving node to determine whether the ICMP packet became corrupted during transmission
Rest of Header	32 bits	Varies depending on message type and subtype
Data	Variable	Usually contains the IP header and first 8 bytes of the data portion of the IP packet that triggered the ICMP message

# ARP (Address Resolution Protocol) on IPv4 Networks (1 of 4)

- ARP works in conjunction with IPv4 to discover the MAC address of a host or node on the local network
  - And to maintain a database that maps IP addresses to MAC addresses on the local network
- ARP is a Layer 2 protocol that uses IP in Layer 3
  - Operates only within its local network
- ARP relies on broadcasting
- ARP table—The database of IP-to-MAC address mappings

# ARP on IPv4 Networks (2 of 4)

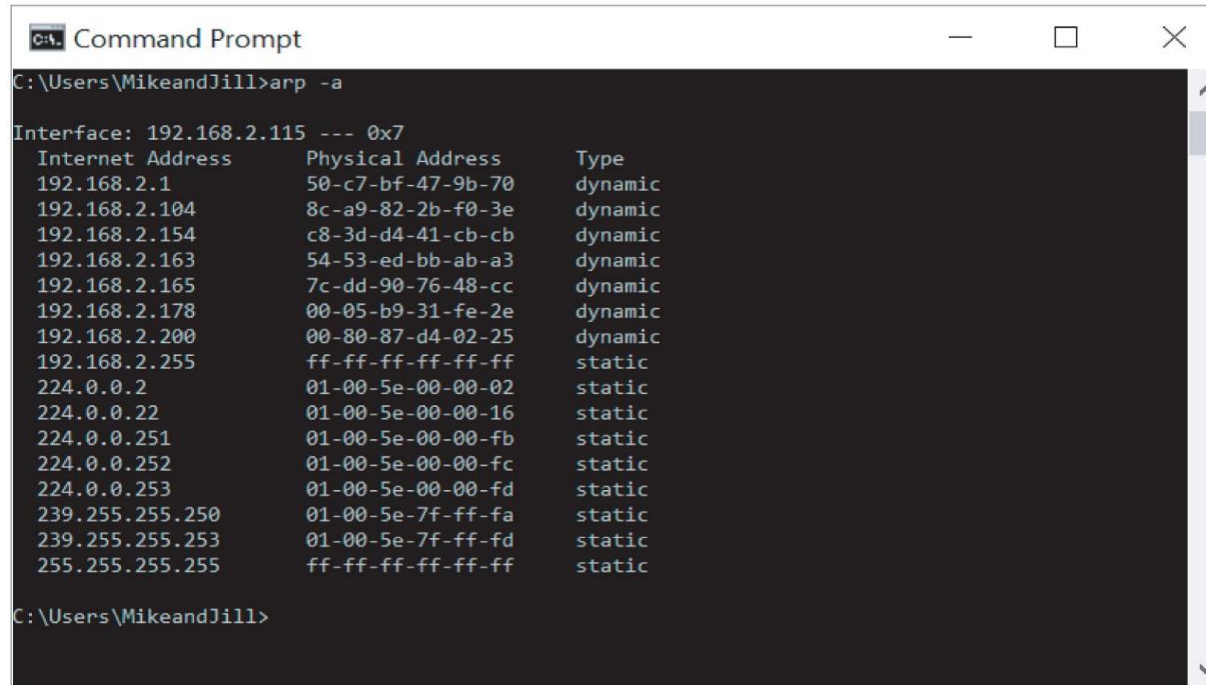
IP Address	Hardware Address	Type
123.45.67.80	60:23:A6:F1:C4:D2	Static
123.45.67.89	20:00:3D:21:E0:11	Dynamic
123.45.67.73	A0:BB:77:C2:25:FA	Dynamic

**Figure 4-12** Sample ARP table

# ARP on IPv4 Networks (3 of 4)

- An ARP table can contain two types of entries:
  - **Dynamic**—Created when a client makes an ARP request that could not be satisfied by data already in the ARP table
  - **Static**—Those someone entered manually using the ARP utility (**arp** command)
- To view a Window's workstation's ARP table, enter the command:
  - **arp -a**

# ARP on IPv4 Networks (4 of 4)



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

Interface: 192.168.2.115 --- 0x7
Internet Address      Physical Address      Type
192.168.2.1           50-c7-bf-47-9b-70     dynamic
192.168.2.104         8c-a9-82-2b-f0-3e     dynamic
192.168.2.154         c8-3d-d4-41-cb-cb     dynamic
192.168.2.163         54-53-ed-bb-ab-a3     dynamic
192.168.2.165         7c-dd-90-76-48-cc     dynamic
192.168.2.178         00-05-b9-31-fe-2e     dynamic
192.168.2.200         00-80-87-d4-02-25     dynamic
192.168.2.255         ff-ff-ff-ff-ff-ff     static
224.0.0.2             01-00-5e-00-00-02     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251           01-00-5e-00-00-fb     static
224.0.0.252           01-00-5e-00-00-fc     static
224.0.0.253           01-00-5e-00-00-fd     static
239.255.255.250       01-00-5e-7f-ff-fa     static
239.255.255.253       01-00-5e-7f-ff-fd     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static

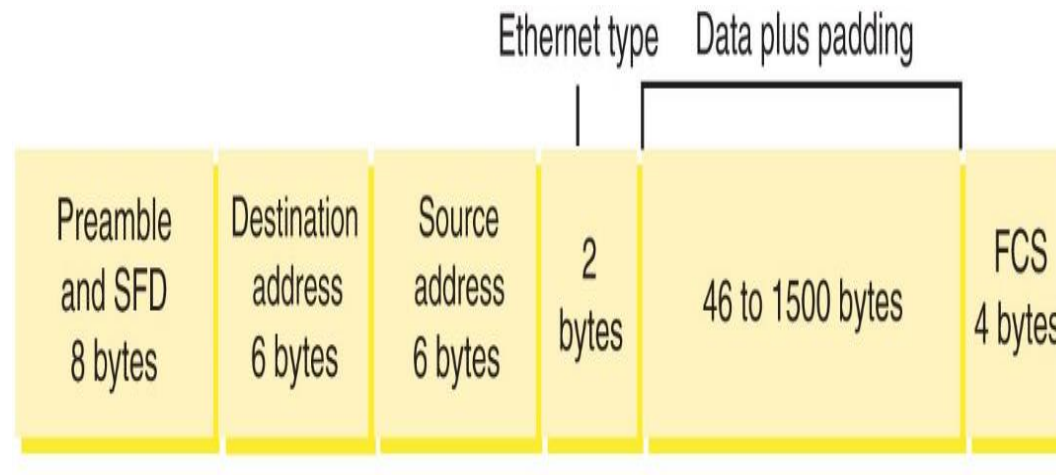
C:\Users\MikeandJill>
```

**Figure 4-13** The `arp -a` command lists devices on the network

# Ethernet (1 of 3)

- Ethernet:
  - Most important Data Link layer standard
  - Capable of running on a variety of network media
  - Offers excellent throughput at a reasonable cost
  - Most popular network technology used on modern LANs
- **Ethernet II** is the current standard
- Adds both a header and a trailer to the payload
  - Creates a frame around the payload

# Ethernet (2 of 3)



**Figure 4-14** Ethernet II frame



# Ethernet (3 of 3)

- The header and FCS make up the 18-byte “frame” around the data
- Data portion of an Ethernet frame may contain from 46 to 1500 bytes
- **MTU (maximum transmission unit)**
  - The largest size that routers in a message’s path will allow at the Network Layer
- Exceptions to Ethernet frame size limitations:
  - Ethernet frames on a VLAN can have an extra 4-byte field between the Source address field and the Type field
  - Some special-purpose networks use a proprietary version of Ethernet that allows for a jumbo frame
    - The MTU can be as high as 9198 bytes, depending on the type of Ethernet architecture used

# Routers and How They Work (1 of 4)

- A router joins two or more networks and passes packets from one network to another
- Routers can do the following:
  - Connect dissimilar networks (LANs and WANs)
  - Interpret Layer 3 and often Layer 4 addressing
  - Determine the best path for data to follow from point A to point B
  - Reroute traffic if the path of first choice is down but another path is available

# Routers and How They Work (2 of 4)



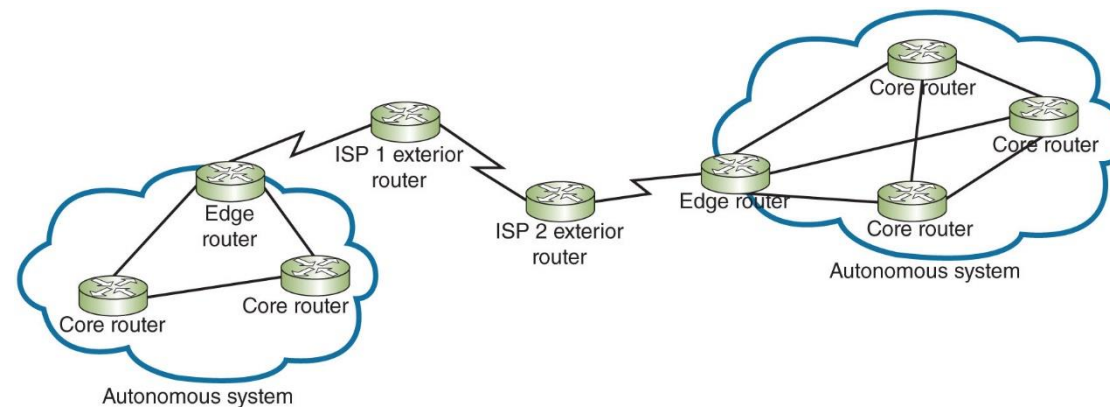
Figure 4-16 ISP, business, and consumer routers

# Routers and How They Work (3 of 4)

- Routers may perform any of the following optional functions:
  - Filter broadcast transmissions to alleviate network congestion
  - Prevent certain types of traffic from getting to a network
  - Support simultaneous local and remote connectivity
  - Provide high network fault tolerance through redundant components such as power supplies
  - Monitor network traffic and report statistics
  - Diagnose internal or other connectivity problems and trigger alarms

# Routers and How They Work (4 of 4)

- Router categories:
  - **Core routers**, also called **interior routers**—Direct data between networks within the same **autonomous system (AS)**
  - **Edge routers**, or **border routers**—Connect an autonomous system with an outside network, also called untrusted network
  - **Exterior routers**—Refers to any router outside the organization's AS
    - Direct data between autonomous systems



**Figure 4-17** Core, edge, and exterior routers

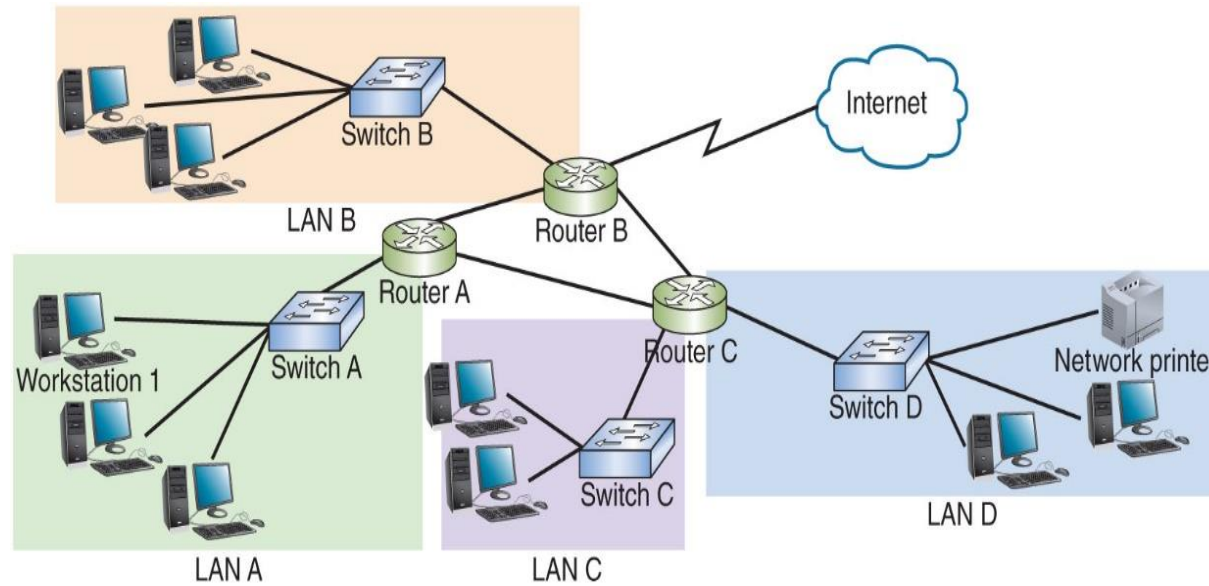
# Multilayer Switches

- **Layer 3 switch**—Capable of interpreting Layer 3 data and works much like a router:
  - Usually faster and less expensive
  - Primary difference is the way the hardware is built
- **Layer 4 switch**—Capable of interpreting Layer 4 data:
  - Also known as **content or application switches**
  - Enables switch to perform advanced filtering, keep statistics, and provide security functions
  - Typically used as part of a network's backbone

# Routing Tables (1 of 2)

- **Routing table**—A database that maintains information about where hosts are located and the most efficient way to reach them
  - Routers rely on them to identify which router is the next hop to reach a particular destination host
- Routing tables contain IP addresses and network masks that identify a network that a host or another router belongs to

# Routing Tables (2 of 2)



**Figure 4-18** Routers rely on routing tables to locate destination hosts



# Routing Path Types

- **Static routing**—Network administrators configures a routing table to direct messages along specific paths
  - Example—A static route between a small business and its ISP
- **Dynamic routing**—Automatically calculates the best path between two networks and maintains this information in a routing table
  - Router can detect problems with failed or congested routes and reroute messages through a different path

# The route Command

- The **route command** allows you to view a host's routing table:
  - On a Linux or UNIX system, use the command **route**
  - On a Windows-based system, use the command **route print**
  - On a Cisco IOS, use the command **show ip route**

# Routing Metrics

- **Routing metrics**—Properties of a route used by routers to determine the best path to a destination:
  - Hop count – number of network segments crossed
  - Theoretical bandwidth and actual throughput
  - **Delay**, or **latency**, on a potential path
  - Load, or the traffic or processing burden
  - MTU (maximum transmission unit) or the largest IP packet size in bytes allowable without fragmentation
  - **Routing cost**, or a value assigned to a particular route
  - Reliability of a potential path
  - Topology of a network

# Routing Protocols to Determine Best Paths (1 of 2)

- **Routing protocols**—Used by routers to communicate with each other to determine the best path
- Routers rate the reliability and priority of a routing protocol's data based on these criteria:
  - **Administrative distance (AD)**—A number indicating the protocol's reliability
  - **Convergence time**—Time it takes to recognize a best path in the event of a change or network outage
  - **Overhead**—The burden placed on the underlying network to support the protocol

# Routing Protocols to Determine Best Paths (2 of 2)

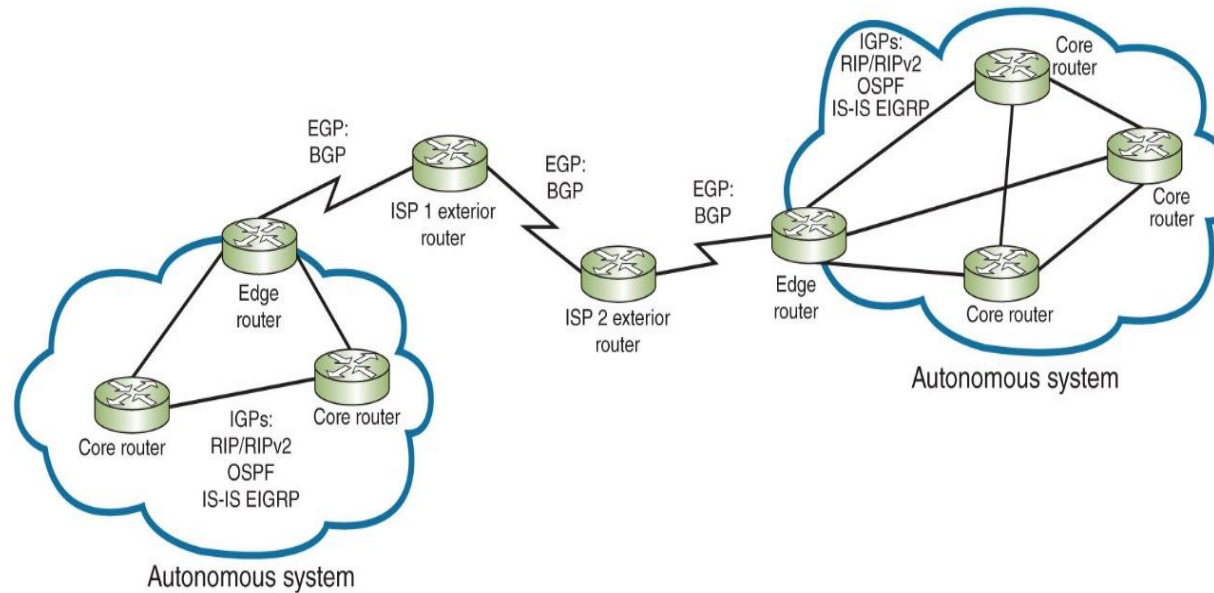
- Table 4-10 Summary of common routing protocols

Routing Protocol	Type	Algorithm Used
Routing Information Protocol (RIP)	IGP	Distance-vector
RIPv2	IGP	Distance-vector
Open Shortest Path First (OSPF)	IGP	Link-state
Intermediate System to Intermediate System (IS-IS)	IGP	Link-state
Enhanced Interior Gateway Routing Protocol (EIGRP)	IGP	Advanced distance-vector
Border Gateway Protocol (BGP)	IGP	Advanced distance-vector or path vector

# Interior and Exterior Gateway Protocols (1 of 6)

- **IGP (interior gateway protocols)**—Used by core routers and edge routers within autonomous systems and are often grouped according to the algorithms they use to calculate best paths:
  - **Distance-vector routing protocols**—Calculate path on the basis of the distance to that destination. Ex: RIP, EIGRP
  - **Link-state routing protocols**—Enables routers to communicate beyond neighboring routers in order to independently map the network and determine the best path. Ex: OSPF, IS-IS
- **EGP (exterior gateway protocols)**—Used by edge routers and exterior routers to distribute data outside of autonomous systems
  - The only EGP currently in use is BGP

# Interior and Exterior Gateway Protocols (2 of 6)



**Figure 4-19** BGP is the only routing protocol that communicates across the Internet

# Interior and Exterior Gateway Protocols

## (3 of 6)

- **OSPF (Open Shortest Path First)**—An IGP and a link-state protocol used on interior or border routers
  - Introduced as an improvement to RIP
  - Characteristics:
    - Supports large networks—Imposes no hop limits (unlike RIP)
    - Uses a more complex algorithm for determining best paths
    - Shared data—Maintains a database of other routers' links
    - Low overhead, fast convergence—Demands more memory and CPU power for calculations, but keeps network bandwidth to a minimum and provides a very fast convergence time
    - Stability—Uses algorithms that prevent routing loops
    - Multi-vendor routers—Supported by all modern routers



# Interior and Exterior Gateway Protocols

## (4 of 6)

- **IS-IS (Intermediate System to Intermediate System)**—An IGP and link-state routing protocol:
  - Uses a best-path algorithm similar to OSPF
  - Is designed for use on core routers only (unlike OSPF)
  - Not handcuffed to IPv4 (like OSPF) so it's easy to adapt to IPv6
  - Service providers generally prefer IS-IS because it's more scalable than OSPF

# Interior and Exterior Gateway Protocols

## (5 of 6)

- **EIGRP (Enhanced Interior Gateway Routing Protocol)**—An advanced distance-vector protocol that combines some of the features of a link-state protocol
  - Often referred to as a hybrid protocol
  - Fast convergence time and low network overhead
  - Easier to configure and less CPU-intensive than OSPF
  - Supports multiple protocols and limits unnecessary network traffic between routers
  - Originally proprietary to Cisco routers

# Interior and Exterior Gateway Protocols

## (6 of 6)

- **BGP (Border Gateway Protocol)**—The only current EGP and is known as the “protocol of the Internet”
  - Can span multiple autonomous systems
  - A path-vector routing protocol that communicates via BGP-specific messages that travel between routers
  - Determines the best paths based on many different factors
  - Can be configured to follow policies that might avoid a certain router or instruct a group of routers to prefer a particular route
  - The most complex of the routing protocols

# Troubleshooting Route Issues

- TCP/IP comes with a set of utilities that can help track down most TCP/IP related problems
- You should be familiar with the tools and their parameters

# Troubleshooting Tools (1 of 8)

- **netstat**—Displays TCP/IP statistics and details about TCP/IP components/connections on a host
  - Information that can be obtained from the **netstat** command includes:
    - The port on which a TCP/IP service is running
    - Which network connections are currently established for a client
    - How many messages have been handled by a network interface since it was activated
    - How many data errors have occurred on a particular network interface

# Troubleshooting Tools (2 of 8)

- Table 4-11 **netstat** command options

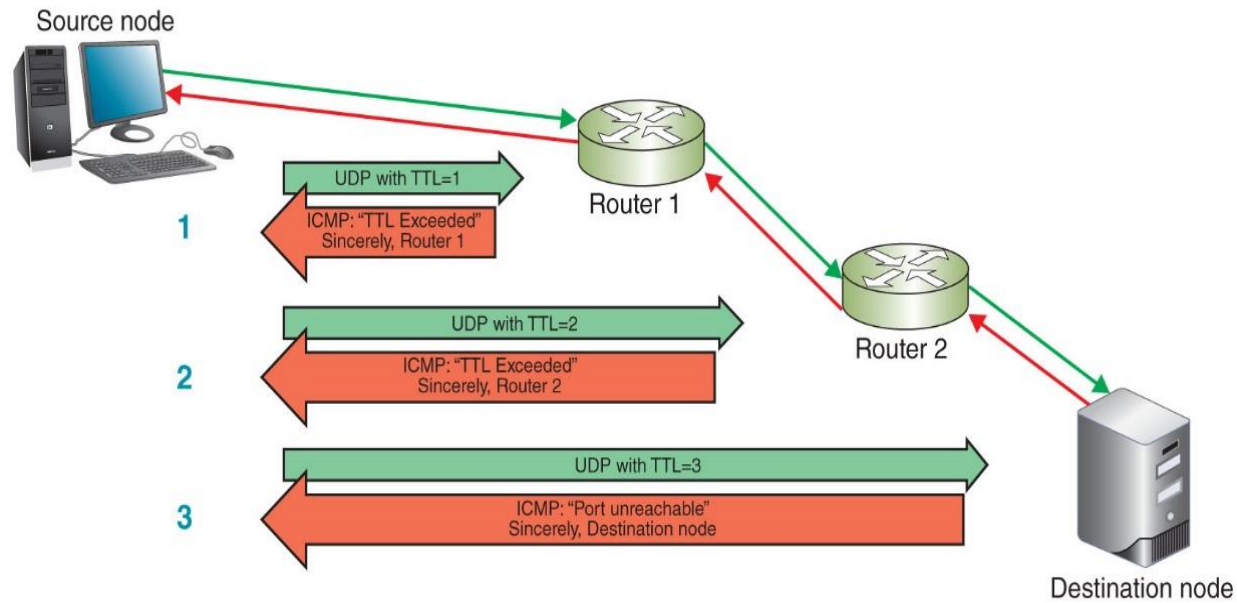
Netstat command	Description
netstat	Lists all active TCP/IP connections on the local machine, including the Transport layer protocol used, messages sent, and received, IP address, and state of those connections
netstat -n	Lists current connections, including IP addresses and ports
netstat -f	Lists current connections, including IP addresses, ports, and FQDNs
netstat -a	Lists all current TCP connections and all listening TCP and UDP ports
netstat -e	Displays statistics about messages sent over a network interface, including errors and discards

# Troubleshooting Tools (3 of 8)

- **tracert** or **tracert**

- Windows **tracert** utility uses ICMP echo requests to trace the path from one networked node to another, identifying all intermediate hops between the nodes
- Linux, UNIX, and OS X systems use the **tracert** utility to send UDP messages to a random port on the destination node (concept is the same as tracert)
- Both utilities employ a trial-and-error approach to discover the nodes at each hop from source to destination

# Troubleshooting Tools (4 of 8)



**Figure 4-20** The traceroute utility uses error messages from routers to map nodes on a route



# Troubleshooting Tools (5 of 8)

- **tracert** or **tracert** (continued)
  - A trace test might stop before reaching the destination for one of three reasons:
    - The device the trace is attempting to reach is down
    - It's too busy to process lower-priority messages such as UDP or ICMP
    - It does not accept the UDP or ICMP transmissions being sent because a firewall blocks these types of messages
  - A trace cannot detect router configuration problems or predict variations of routes over a period of time

# Troubleshooting Tools (6 of 8)

- **Pathping**—A Windows utility that combines elements of both ping and tracert to provide deeper information about network issues along a route
  - Sends multiple pings to each hope along a route, then compiles information into a single report
- Table 4-13 pathping command options

Pathping command	Description
pathping -n google.com	Instructs the command to not resolve IP addresses to host names
pathping -h 12 google.com	Specifies the maximum number of hops these messages should take when attempting to reach a host
pathping -p 2000 google.com	Identifies the wait time between pings

# Troubleshooting Tools (7 of 8)

- **tcpdump**—A free, command-line packet sniffer that runs on Linux and other Unix OSs
  - Captures traffic that crosses a computer's network interface
  - Output can be saved to a file that you can filter or play back
  - You must either use the **sudo** command or log in as root to access **tcpdump**

# Troubleshooting Tools (8 of 8)

- Table 4-14 **tcpdump** command options

tcpdump command	Description
tcpdump not port 22 or tcpdump not port 23	Filters out SSH or Telnet packets, which is helpful when running tcpdump on a remotely access network device
tcpdump -n	Instructs the command to not resolve IP addresses to host names
tcpdump -c 50	Limits the number of captured packets to 50
tcpdump -i any	Listens to all network interfaces on a device

# Solving Common Routing Problems (1 of 4)

- Table 4-15 Command-line utilities

Command	Common uses
arp	Provides a way of obtaining information from and manipulating a device's ARP table
dig	Queries DNS servers with more advanced options than nslookup
ipconfig or ifconfig	Provides information about TCP/IP network connections and the ability to manage some of those settings
netstat	Displays TCP/IP statistics and details about TCP/IP components and connections on a host
nmap	Detects, identifies, and monitors devices on a network

# Solving Common Routing Problems (2 of 4)

- **Duplicate MAC Addresses:**

- Two devices on the same network with the same MAC address is a problem
- MAC addresses can be impersonated
  - A security risk called **spoofing**
- Happens most often when managing multiple virtual devices on a large network
- Most switches will detect the problem and produce helpful error messages
  - Then it's a matter of tracking down which virtual devices have the same MAC address and update each device's configuration

# Solving Common Routing Problems (3 of 4)

- **Hardware failure**—When a router, switch, NIC, or other hardware goes down
  - Use **tracert** or **tracert** to track down malfunctioning routers and other devices on larger networks
  - Get more accurate trace feedback on a questionable router by targeting a node on the other side of that router, rather than aiming for that router itself
  - Use **ping** to test for network connectivity

# Solving Common Routing Problems (4 of 4)

- **Discovering neighbor devices**—A process used by routers to learn about all of the devices on their networks:
  - On IPv4 networks, **neighbor discovery** is managed by ARP with help from ICMP
  - IPv6 devices use **Neighbor Discovery Protocol (NDP)** to automatically detect neighboring devices and automatically adjust when neighboring nodes fail or are removed
    - Eliminates the need for ARP and ICMP functions in IPv6 networks



# Summary

- TCP/IP is a suite of protocols that includes TCP, IP (IPv4 and IPv6), UDP, ARP, and many others
- TCP operates at the Transport layer and provides reliable data delivery
- UDP is an unreliable, connectionless protocol that provides no delivery guarantees
- IP operates at the Network layer of the OSI model and specifies where data should be delivered
- ICMP is a Network layer core protocol that reports on the success or failure of data delivery
- ARP works in conjunction with IPv4 to obtain the MAC address of a host

# Summary

- A router joins two or more networks and passes packets from one network to another
- A Layer 3 switch is a switch that is capable of interpreting Layer 3 data and works much like a router
- A router relies on its routing table to identify which network a host belongs to and which of the router's interfaces points toward the best next hop to reach the network
- Routing paths are determined by:
  - Static routing, which are routes configured by a network administrator
  - Dynamic routing, which are routes automatically calculated by the router
- The **route** command allows you to view a host's routing table

# Summary

- Routers use routing metrics to determine the best route for messages to take across networks
- To communicate with each other, routers use routing protocols that are similar to scouting parties, exploring unknown territories, and collecting data about current network status
- Interior gateway protocols are used by core routers and edge routers within an autonomous system
- Exterior gateway protocols communicate between autonomous systems
- Helpful TCP/IP utilities include ping, ipconfig, ifconfig, nslookup, dig, arping, route, netstat, traceroute, pathping, and tcpdump