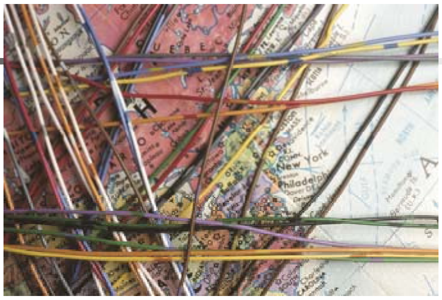
Network Fundamentals



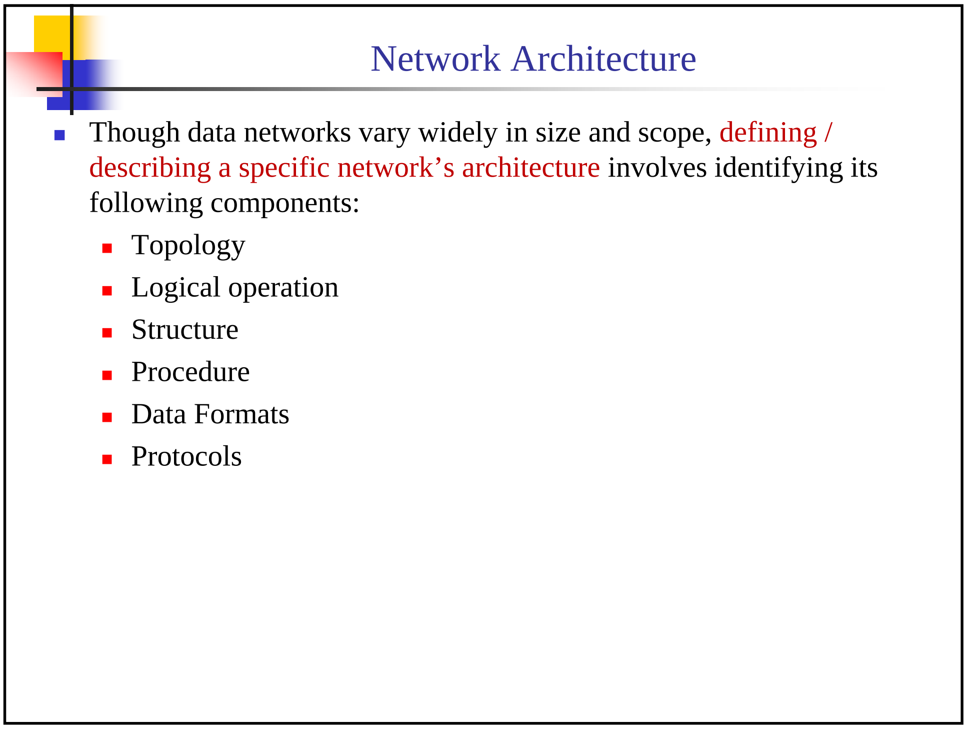
Chapter 9

Background

- Network
  - Different meanings depending on the context and usage
  - A mean to connect two or more computers together for the purpose of sharing information

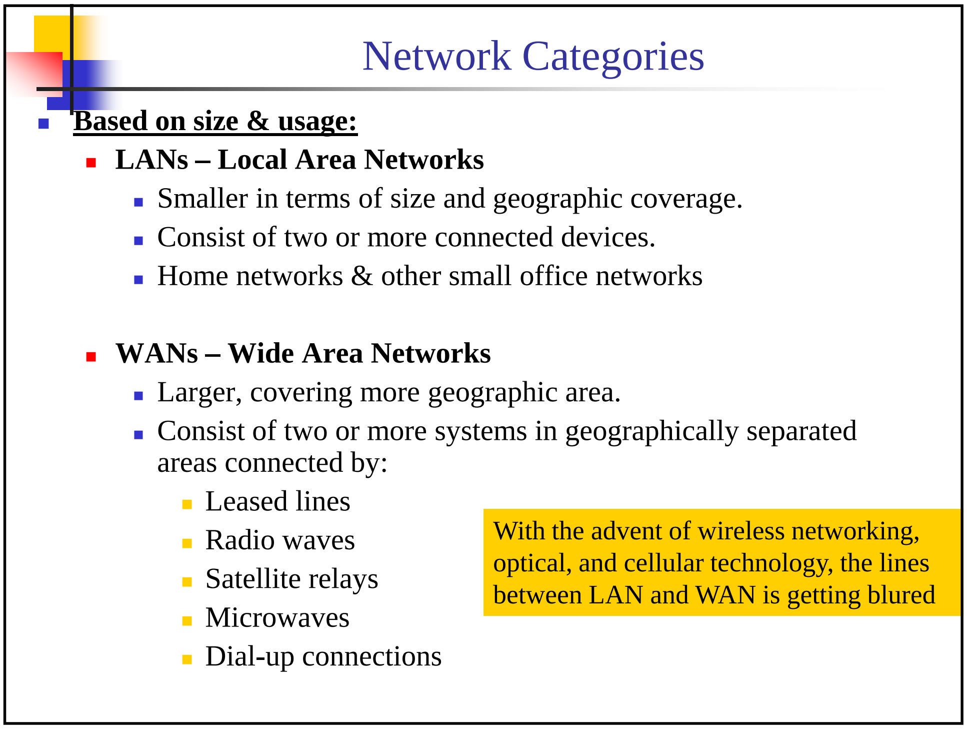
  - Enable computers to interact – exchanging information on everything, from credit card transactions to the latest news and weather.

  - Internet
    - A giant network consisting of interconnected PCs, servers, routers, and switches.



Network Architecture

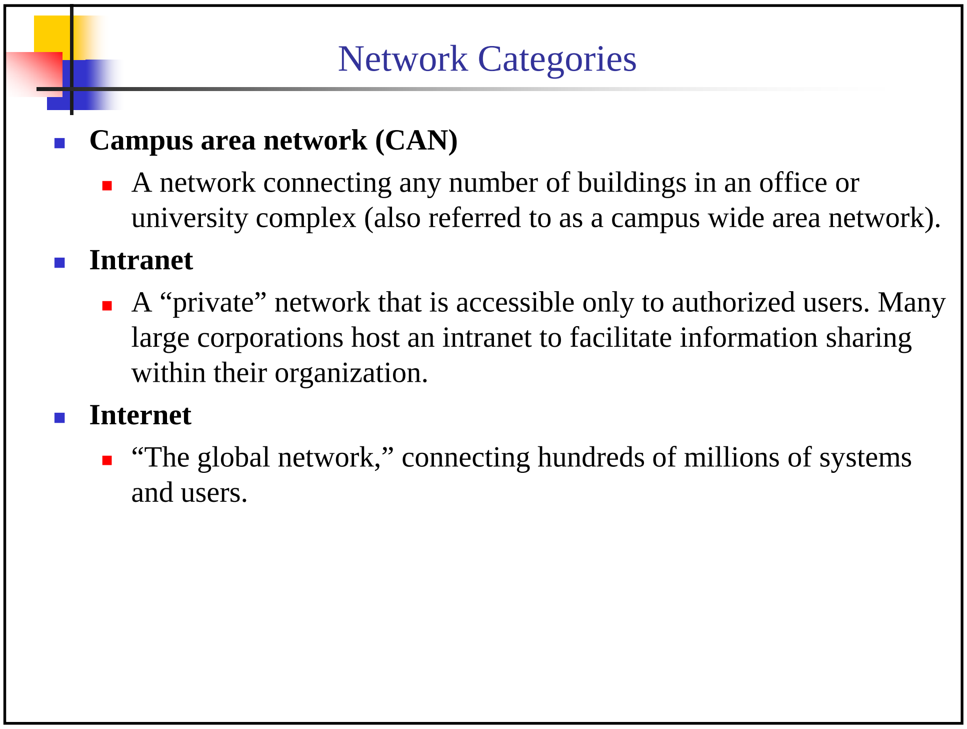
- Though data networks vary widely in size and scope, defining / describing a specific network’s architecture involves identifying its following components:
  - Topology
  - Logical operation
  - Structure
  - Procedure
  - Data Formats
  - Protocols



Network Categories

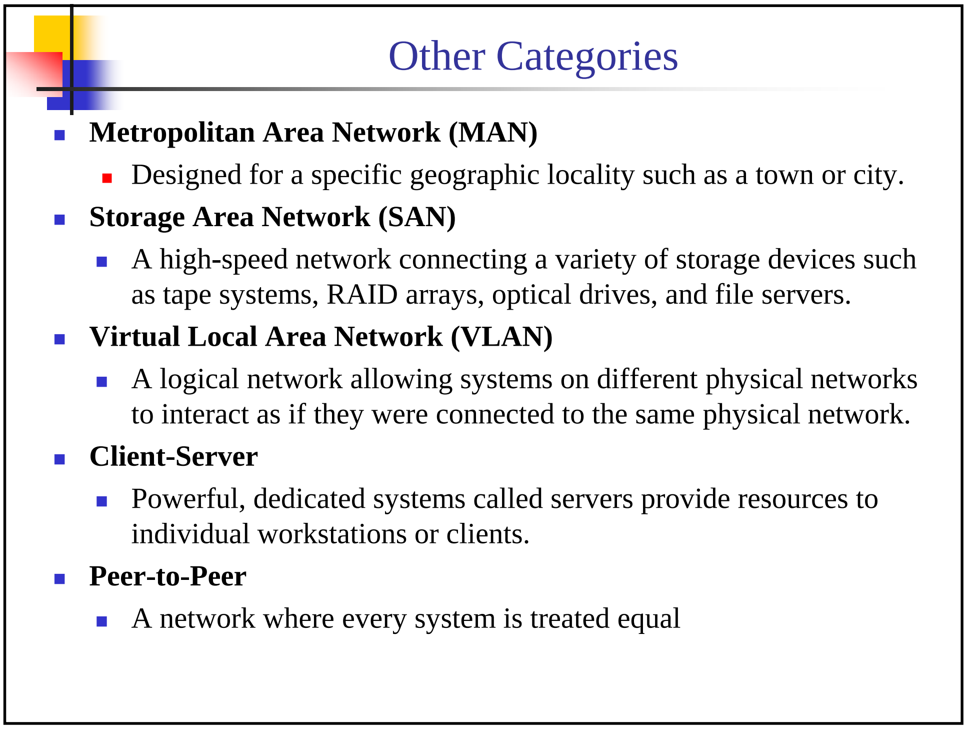
- **Based on size & usage:**
  - **LANs – Local Area Networks**
    - Smaller in terms of size and geographic coverage.
    - Consist of two or more connected devices.
    - Home networks & other small office networks
  - **WANs – Wide Area Networks**
    - Larger, covering more geographic area.
    - Consist of two or more systems in geographically separated areas connected by:
      - Leased lines
      - Radio waves
      - Satellite relays
      - Microwaves
      - Dial-up connections

With the advent of wireless networking, optical, and cellular technology, the lines between LAN and WAN is getting blured



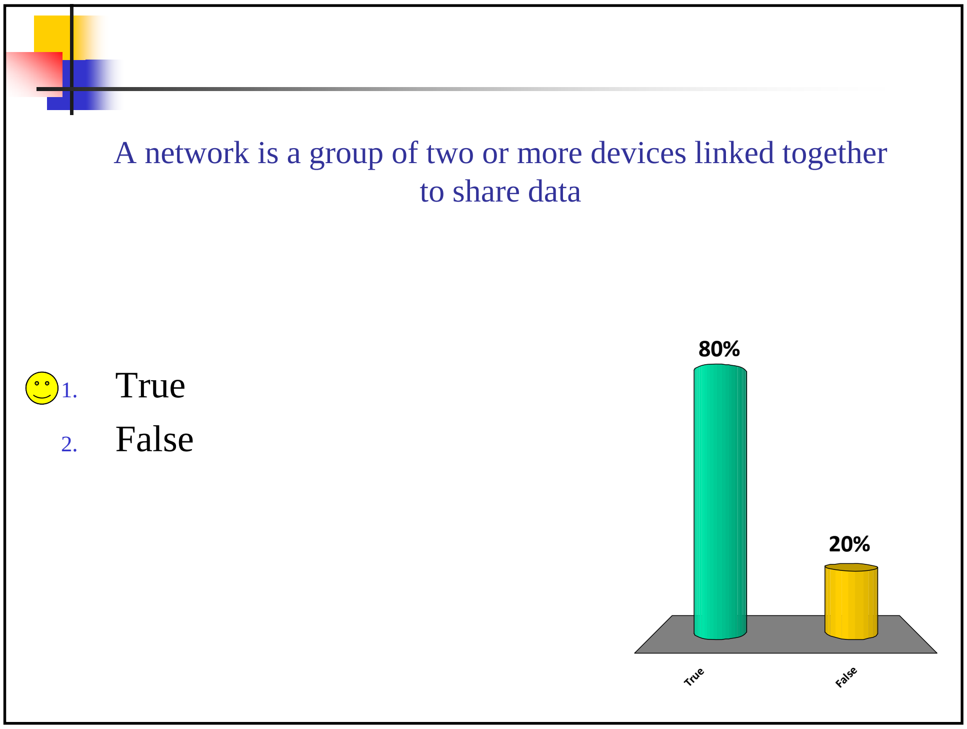
Network Categories

- **Campus area network (CAN)**
  - A network connecting any number of buildings in an office or university complex (also referred to as a campus wide area network).
- **Intranet**
  - A “private” network that is accessible only to authorized users. Many large corporations host an intranet to facilitate information sharing within their organization.
- **Internet**
  - “The global network,” connecting hundreds of millions of systems and users.



Other Categories

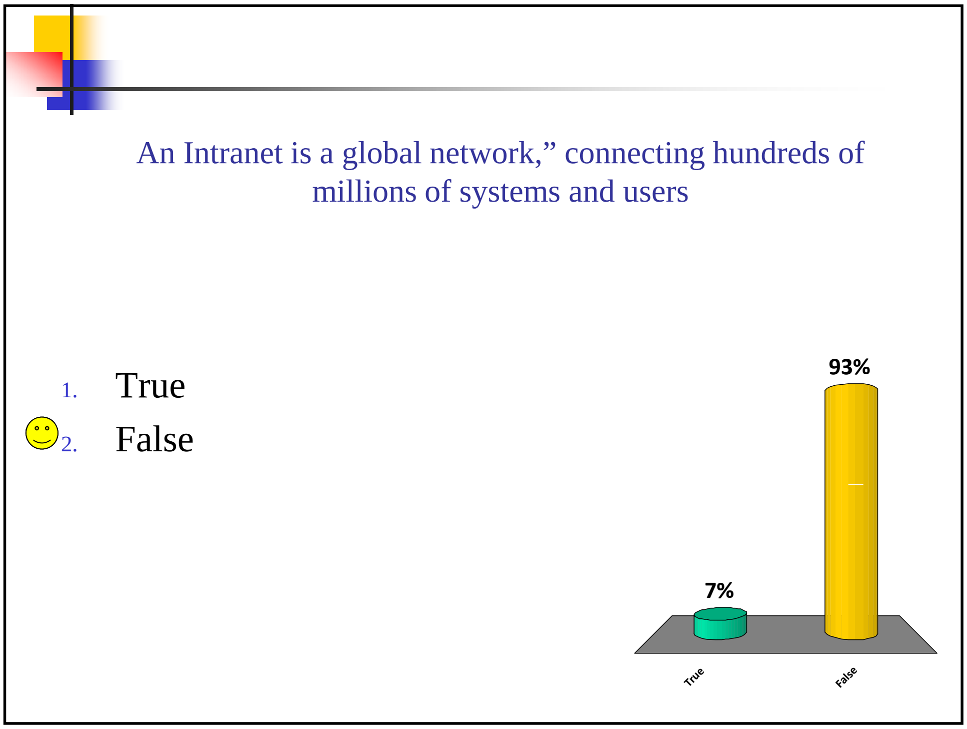
- **Metropolitan Area Network (MAN)**
  - Designed for a specific geographic locality such as a town or city.
- **Storage Area Network (SAN)**
  - A high-speed network connecting a variety of storage devices such as tape systems, RAID arrays, optical drives, and file servers.
- **Virtual Local Area Network (VLAN)**
  - A logical network allowing systems on different physical networks to interact as if they were connected to the same physical network.
- **Client-Server**
  - Powerful, dedicated systems called servers provide resources to individual workstations or clients.
- **Peer-to-Peer**
  - A network where every system is treated equal



A network is a group of two or more devices linked together to share data

☺ 1. True

2. False



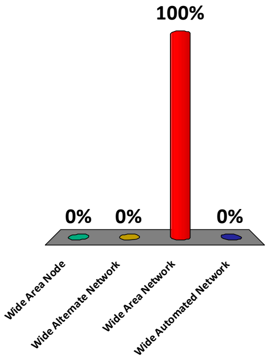
An Intranet is a global network," connecting hundreds of millions of systems and users

1. True

☺ 2. False

As it relates to networking, what does WAN stands for

1. Wide Area Node
2. Wide Alternate Network
3. ☺ Wide Area Network
4. Wide Automated Network

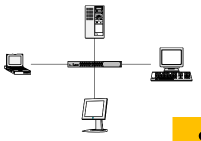


Network Topology

- Topology
  - How the network is physically or logically arranged
  - One of the major components of every network architecture.

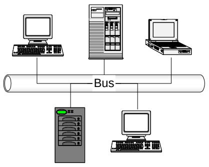
- The various network topologies are:
  - Star
  - Ring
  - Bus
  - Mixed

- **Star –**
  - Network components are connected to a central point.



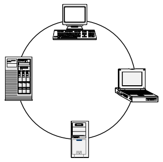
Star

- **Bus –**
  - Network components are connected to the same cable, often called “the bus” or “the backbone.”



Bus

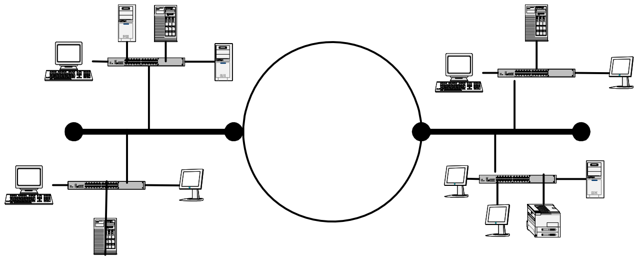
- **Ring –**
  - Network components are connected to each other in a closed loop with each device directly connected to two other devices.



Ring

Mixed Topology

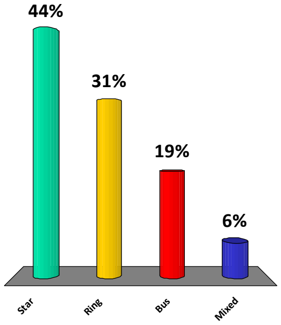
- Larger networks, such as those inside an office complex, may use more than one topology at the same time.



Mixed topology

Which of the following topologies connect all the network devices to a central point

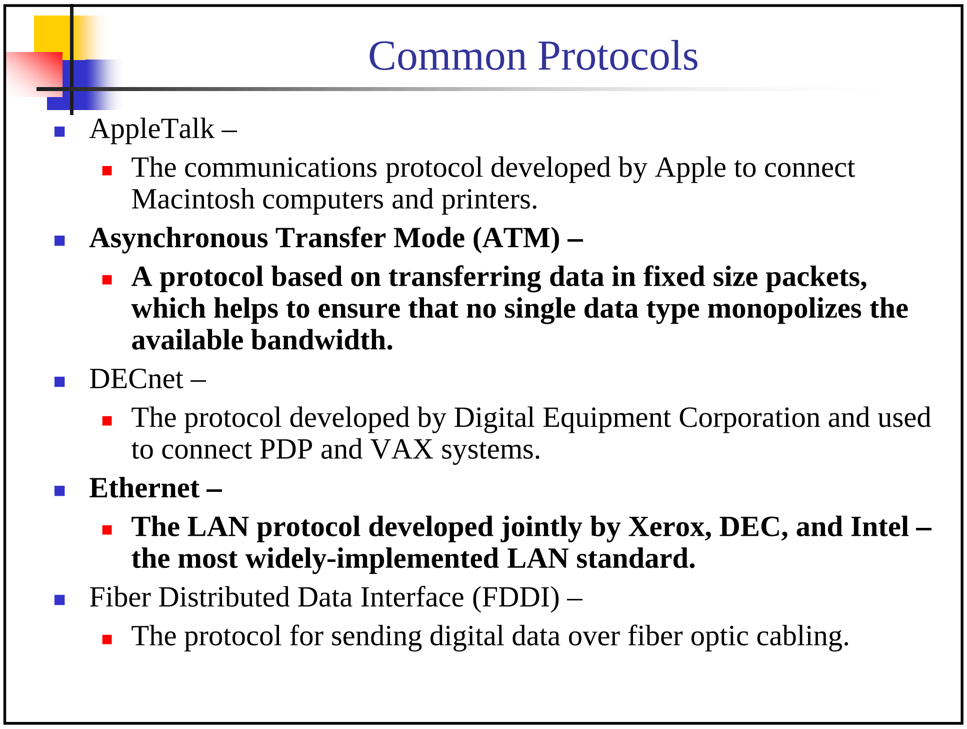
☺ 1. Star
2. Ring
3. Bus
4. Mixed



Network Protocol

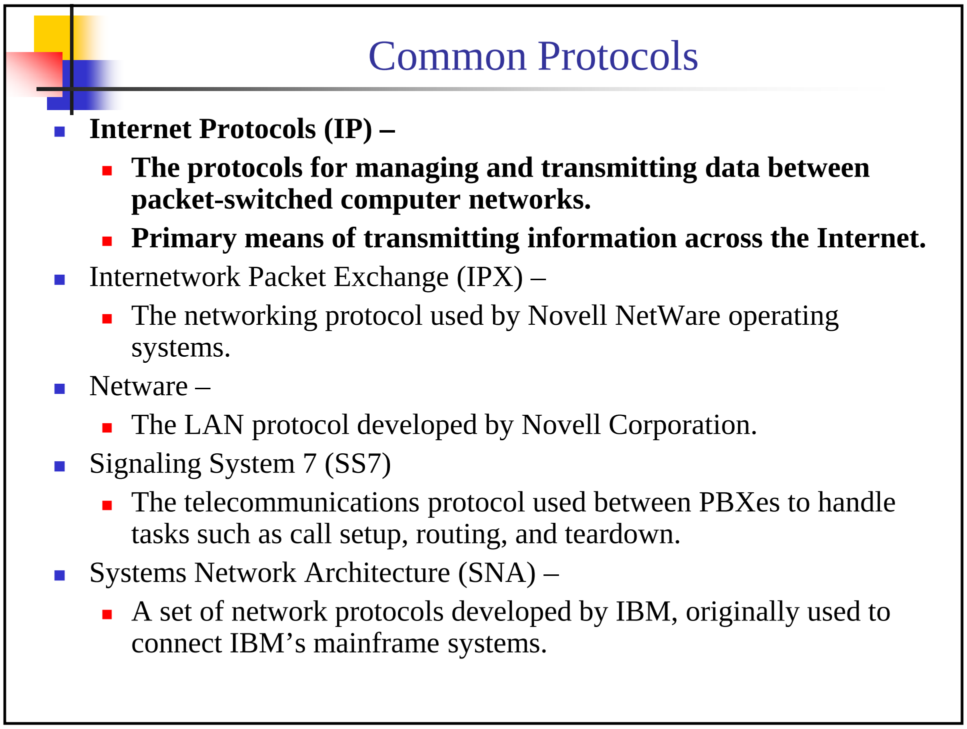
These devices are connected. But how do they communicate?

- **Protocol**
  - Agreed upon format for exchanging or transmitting data between systems.
  - Defines a number of agreed upon parameters such as:
    - Data compression method
    - Error checking
    - Mechanisms for systems to signal when they have finished receiving or transmitting data



Common Protocols

- AppleTalk –
  - The communications protocol developed by Apple to connect Macintosh computers and printers.
- **Asynchronous Transfer Mode (ATM) –**
  - **A protocol based on transferring data in fixed size packets, which helps to ensure that no single data type monopolizes the available bandwidth.**
- DECnet –
  - The protocol developed by Digital Equipment Corporation and used to connect PDP and VAX systems.
- **Ethernet –**
  - **The LAN protocol developed jointly by Xerox, DEC, and Intel – the most widely-implemented LAN standard.**
- Fiber Distributed Data Interface (FDDI) –
  - The protocol for sending digital data over fiber optic cabling.

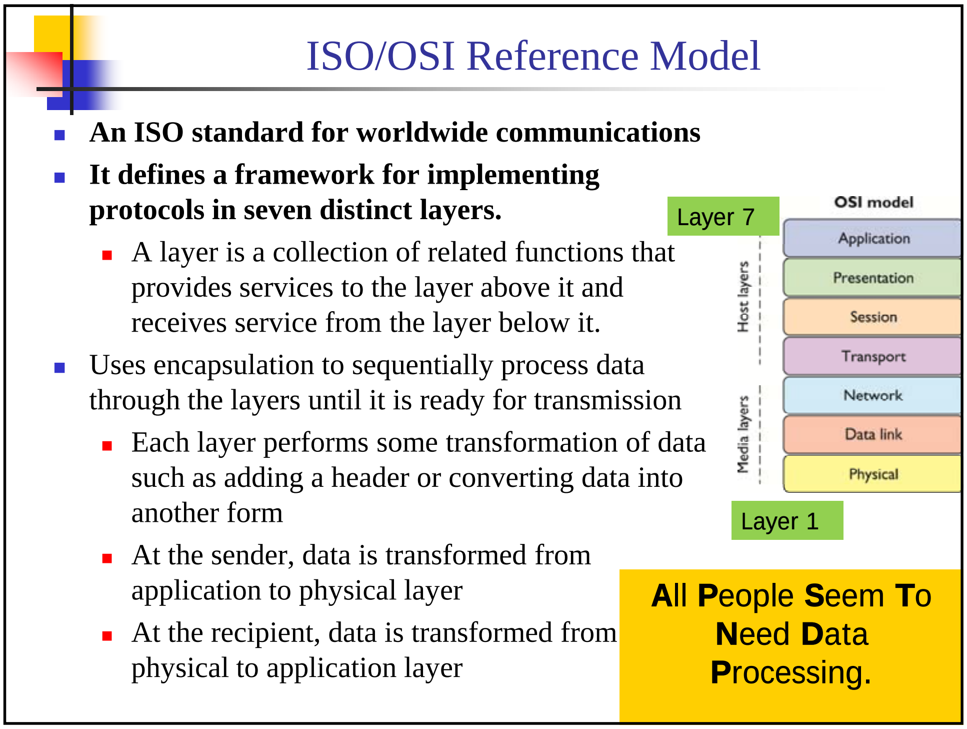


Common Protocols

- **Internet Protocols (IP) –**
  - **The protocols for managing and transmitting data between packet-switched computer networks.**
  - **Primary means of transmitting information across the Internet.**
- Internetwork Packet Exchange (IPX) –
  - The networking protocol used by Novell NetWare operating systems.
- Netware –
  - The LAN protocol developed by Novell Corporation.
- Signaling System 7 (SS7)
  - The telecommunications protocol used between PBXes to handle tasks such as call setup, routing, and teardown.
- Systems Network Architecture (SNA) –
  - A set of network protocols developed by IBM, originally used to connect IBM’s mainframe systems.

Common Protocols

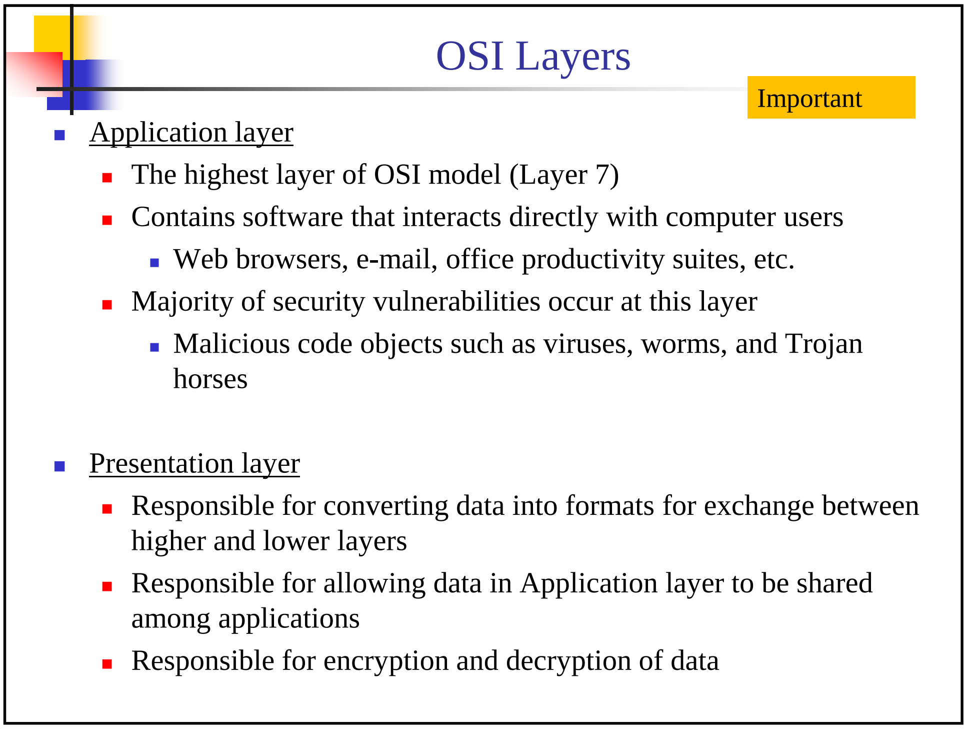
- Token Ring –
  - The LAN protocol developed by IBM where systems must possess the network "token" before transmitting data.
- **Transmission Control Protocol/Internet Protocol (TCP/IP)**
  - **The collection of communications protocols used to connect hosts on the Internet.**
- X.25 –
  - A protocol developed by the Comité Consultatif International Téléphonique et Télégraphique (CCITT) for use in packet-switched networks.



ISO/OSI Reference Model

- **An ISO standard for worldwide communications**
- **It defines a framework for implementing protocols in seven distinct layers.**
  - A layer is a collection of related functions that provides services to the layer above it and receives service from the layer below it.
- Uses encapsulation to sequentially process data through the layers until it is ready for transmission
  - Each layer performs some transformation of data such as adding a header or converting data into another form
  - At the sender, data is transformed from application to physical layer
  - At the recipient, data is transformed from physical to application layer

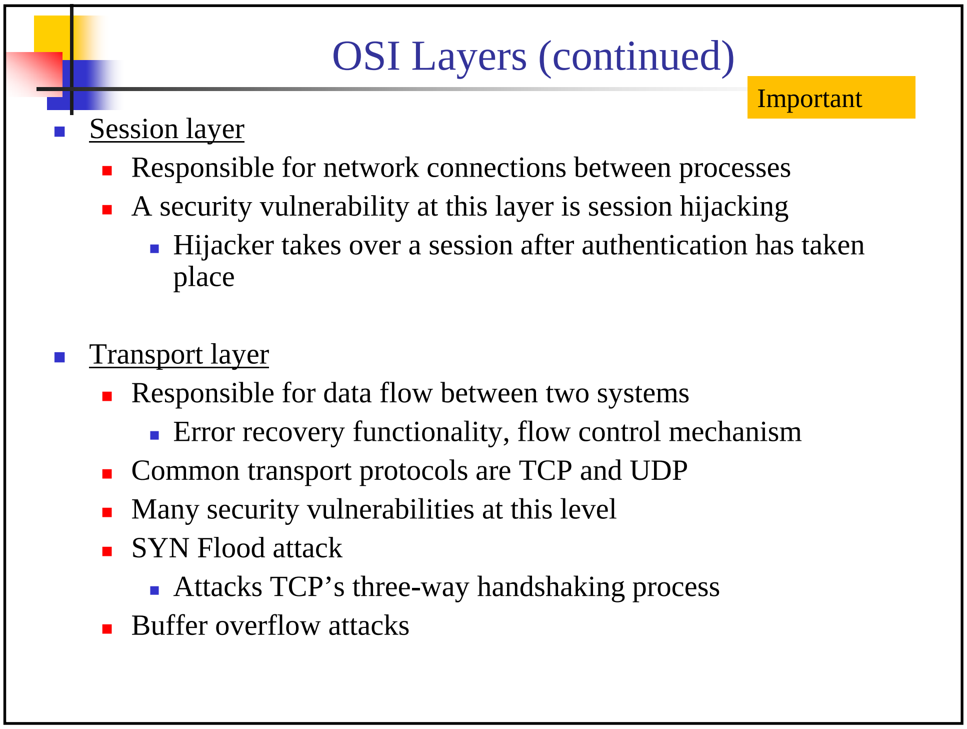
All **P**eople **S**eem **T**o **N**eed **D**ata **P**rocessing.



OSI Layers

Important

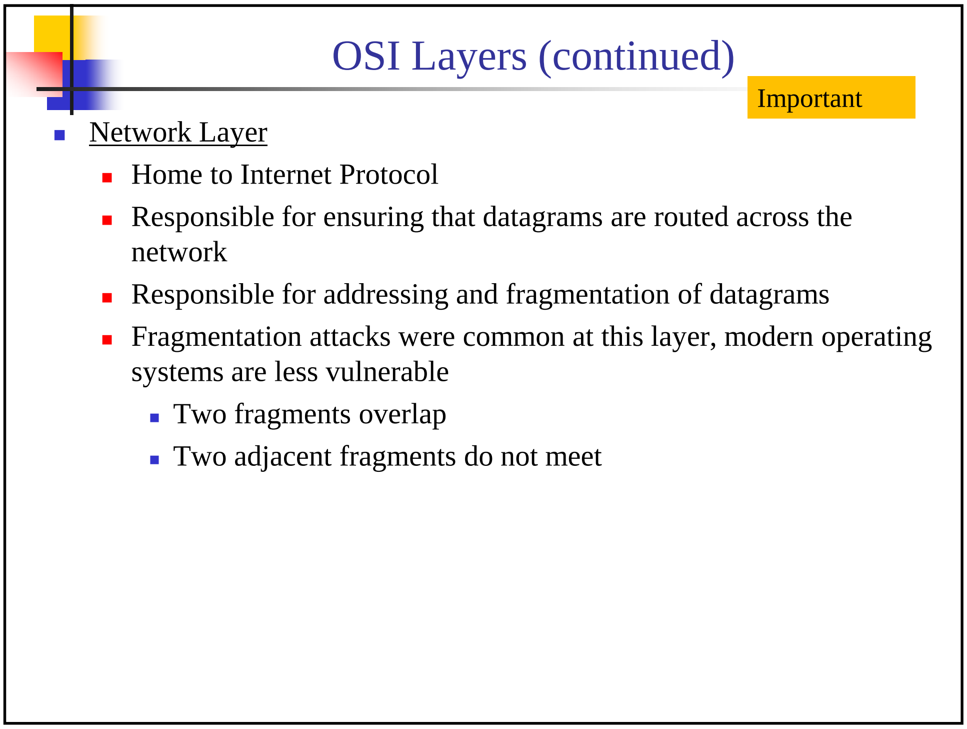
- Application layer
  - The highest layer of OSI model (Layer 7)
  - Contains software that interacts directly with computer users
    - Web browsers, e-mail, office productivity suites, etc.
  - Majority of security vulnerabilities occur at this layer
    - Malicious code objects such as viruses, worms, and Trojan horses
- Presentation layer
  - Responsible for converting data into formats for exchange between higher and lower layers
  - Responsible for allowing data in Application layer to be shared among applications
  - Responsible for encryption and decryption of data



OSI Layers (continued)

Important

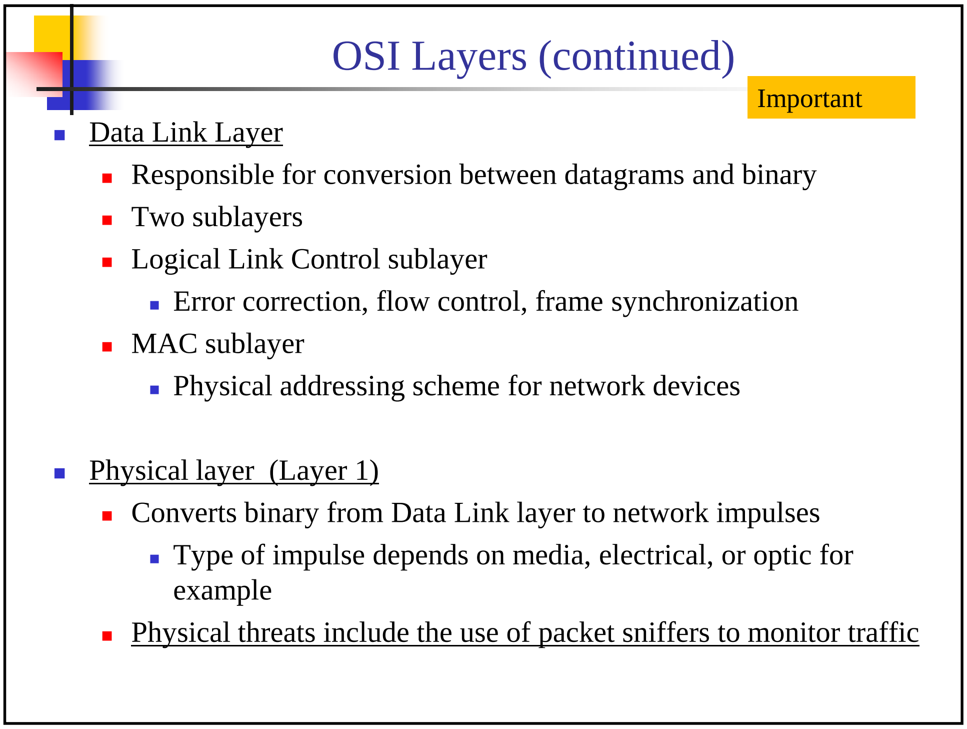
- Session layer
  - Responsible for network connections between processes
  - A security vulnerability at this layer is session hijacking
    - Hijacker takes over a session after authentication has taken place
- Transport layer
  - Responsible for data flow between two systems
    - Error recovery functionality, flow control mechanism
  - Common transport protocols are TCP and UDP
  - Many security vulnerabilities at this level
  - SYN Flood attack
    - Attacks TCP’s three-way handshaking process
  - Buffer overflow attacks



OSI Layers (continued)

Important

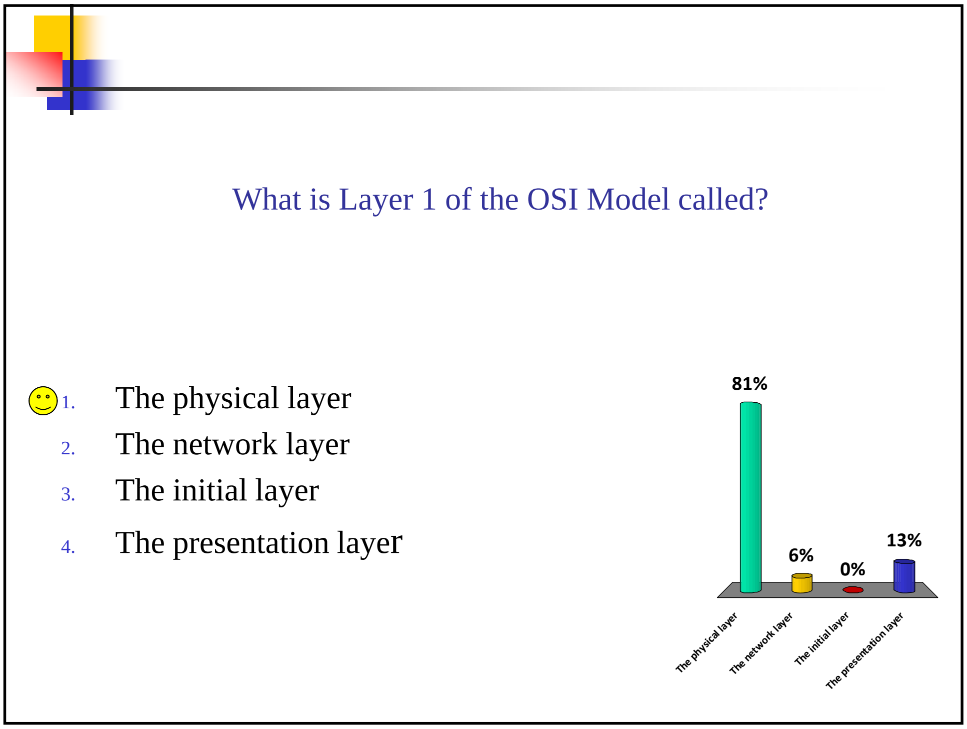
- Network Layer
  - Home to Internet Protocol
  - Responsible for ensuring that datagrams are routed across the network
  - Responsible for addressing and fragmentation of datagrams
  - Fragmentation attacks were common at this layer, modern operating systems are less vulnerable
    - Two fragments overlap
    - Two adjacent fragments do not meet



OSI Layers (continued)

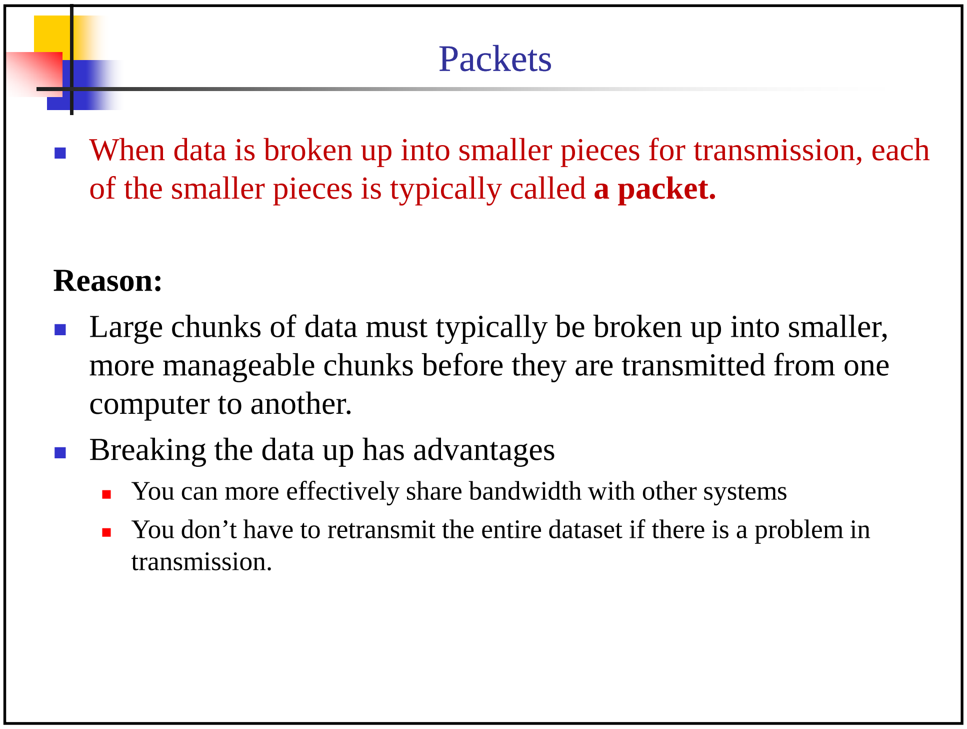
Important

- Data Link Layer
  - Responsible for conversion between datagrams and binary
  - Two sublayers
  - Logical Link Control sublayer
    - Error correction, flow control, frame synchronization
  - MAC sublayer
    - Physical addressing scheme for network devices
- Physical layer (Layer 1)
  - Converts binary from Data Link layer to network impulses
    - Type of impulse depends on media, electrical, or optic for example
  - Physical threats include the use of packet sniffers to monitor traffic



What is Layer 1 of the OSI Model called?

☺ 1. The physical layer
2. The network layer
3. The initial layer
4. The presentation layer

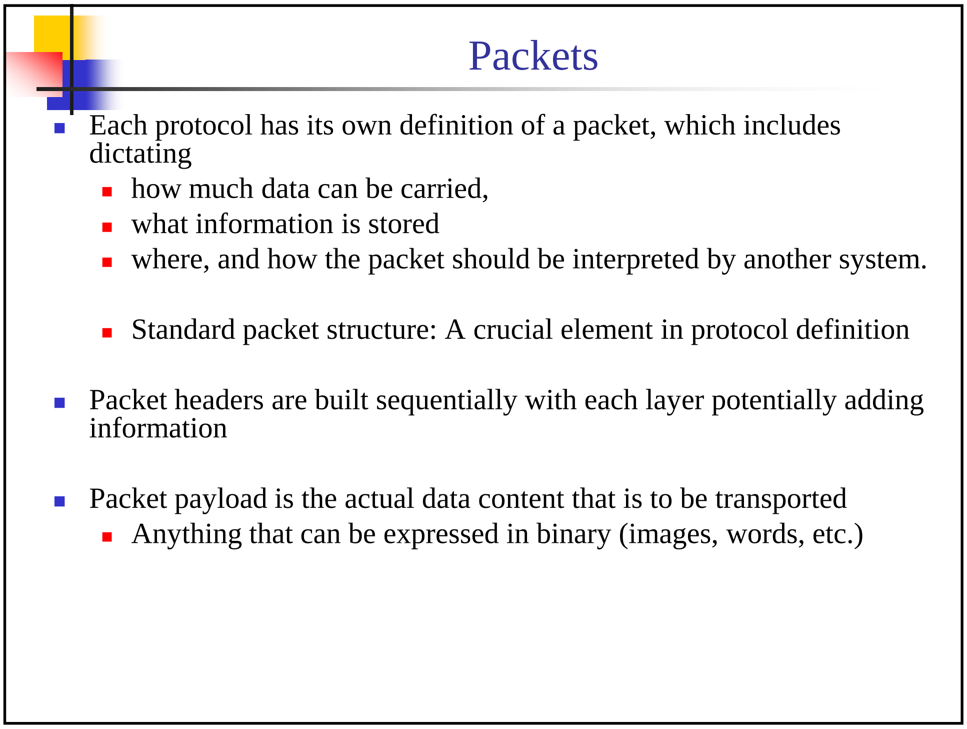


Packets

- When data is broken up into smaller pieces for transmission, each of the smaller pieces is typically called **a packet.**

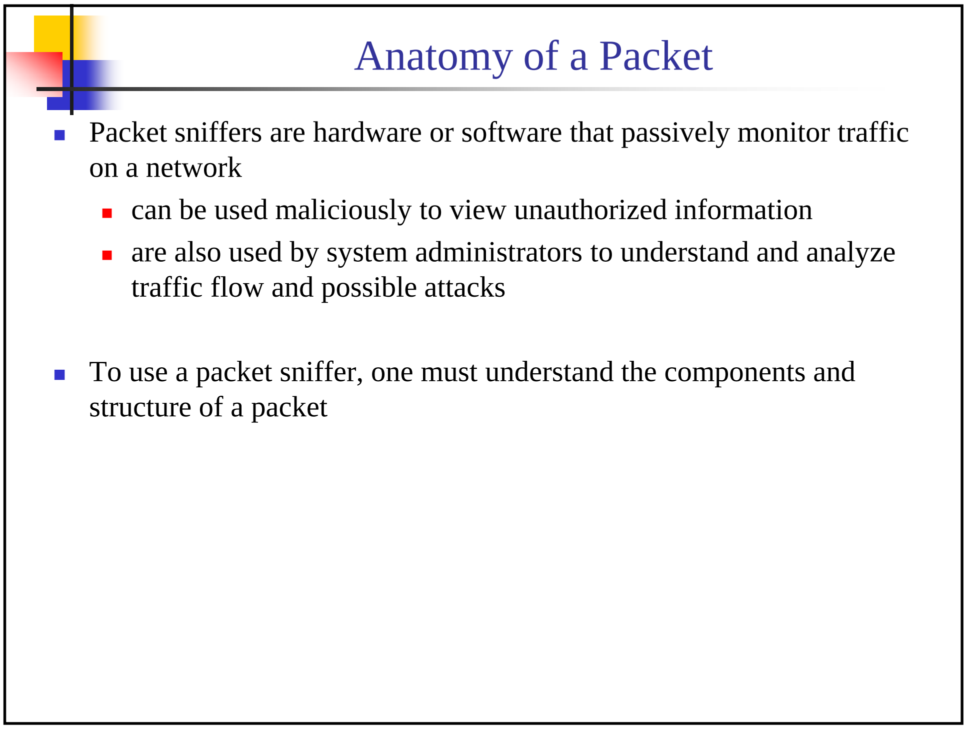
Reason:

- Large chunks of data must typically be broken up into smaller, more manageable chunks before they are transmitted from one computer to another.
- Breaking the data up has advantages
  - You can more effectively share bandwidth with other systems
  - You don't have to retransmit the entire dataset if there is a problem in transmission.



Packets

- Each protocol has its own definition of a packet, which includes dictating
  - how much data can be carried,
  - what information is stored
  - where, and how the packet should be interpreted by another system.
  - Standard packet structure: A crucial element in protocol definition
- Packet headers are built sequentially with each layer potentially adding information
- Packet payload is the actual data content that is to be transported
  - Anything that can be expressed in binary (images, words, etc.)



Anatomy of a Packet

- Packet sniffers are hardware or software that passively monitor traffic on a network
  - can be used maliciously to view unauthorized information
  - are also used by system administrators to understand and analyze traffic flow and possible attacks
- To use a packet sniffer, one must understand the components and structure of a packet

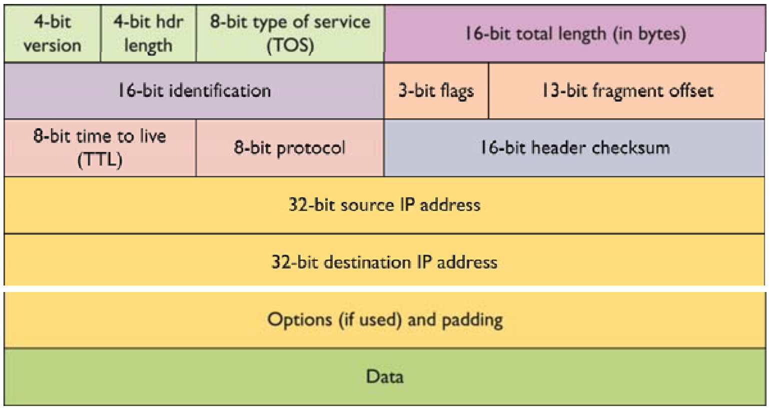
IP Packet

- **An IP packet, often called a datagram**, has two main sections:
  - The header
  - The data section (sometimes called the payload).
- **The Header - Contains all of the information needed to describe the packet.**
  - Kind of packet (Protocol version number)
  - Packet header length : How large the header of the packet is
  - How to process this packet (Whether or not to use options (minimize delay, maximize throughput, maximize reliability, and minimize cost)
  - How large the entire packet is.
  - A unique identifier so that the packet can be distinguished

The Header (contd.)

- Whether or not the packet is part of a longer data stream and should be handled relative to other packets.
- A description of where the packet fits into the data stream as compared to other packets.
- A checksum of the packet header:
  - To minimize data corruption during transmission.
- Where the packet is from.
  - Source IP address such as 10.10.10.5
- Where the packet is going.
  - Destination IP address such as 10.10.10.10
- Option flags that govern security and handling restrictions:
  - Record the route this packet has taken.
  - Record timestamps.

Packet Illustrated

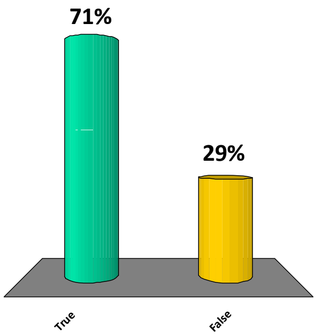


<table>
<tr><td>4-bit version</td><td>4-bit hdr length</td><td>8-bit type of service (TOS)</td><td colspan="2">16-bit total length (in bytes)</td></tr>
<tr><td colspan="3">16-bit identification</td><td>3-bit flags</td><td>13-bit fragment offset</td></tr>
<tr><td colspan="2">8-bit time to live (TTL)</td><td>8-bit protocol</td><td colspan="2">16-bit header checksum</td></tr>
<tr><td colspan="5">32-bit source IP address</td></tr>
<tr><td colspan="5">32-bit destination IP address</td></tr>
<tr><td colspan="5">Options (if used) and padding</td></tr>
<tr><td colspan="5">Data</td></tr>
</table>

Logical layout of an IP packet

A packet in an IP network is sometimes called a datagram

☺ 1. True
2. False

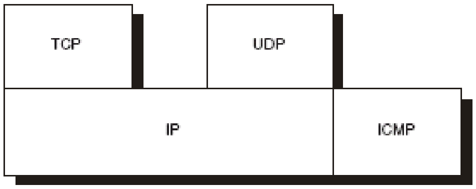


Internet Protocol (IP)

- The Internet Protocol provides routing functions for datagrams (IP packets) traversing the network
- Each datagram has source and destination addresses
- IP determines if the datagram has reached its destination or if it must be forwarded
  - If it must be forwarded, IP determines the next hop
- IP does not provide a reliability guarantee
  - No assurance that a packet will reach its specified destination
- IP is also responsible for fragmentation of datagrams
  - A datagram cannot exceed the maximum size for the network it is traveling on
    - This is not known at creation time
  - Datagrams that are too large must be broken into fragments
- Each fragment must contain the information required to reassemble the original datagram
  - Labeled with a length and an offset

TCP vs. UDP

- The two protocols, the **Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)**, are protocols that run **on top of the IP network protocol.**
- These two protocols that have grown so much in popularity and use that without them, the Internet as we know it would cease to exist.
- The most important difference between TCP and UDP is the concept of “guaranteed” reliability and delivery.



Relationships among protocols in the TCP/IP suite

Transmission Control Protocol (TCP)

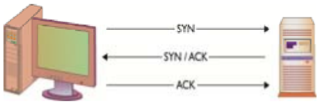
- Important features
  - TCP is a reliable protocol (guarantees delivery of packets from source to destination)
  - TCP provides error-checking (using a checksum)
  - TCP is connection-oriented (provides session establishment and teardown handshaking protocols to create dedicated process-to-process communication)
  - Ensure that packets are processed in the order they were sent.
- After a TCP packet is constructed, it is transformed into an IP datagram by adding information to the headers (encapsulation)

Transmission Control Protocol (TCP) – Connection-Oriented

- Each packet has a sequence number to show where the packet fits into the conversation.
  - Using sequence numbers, packets can arrive in any order and at different times.
  - The receiving system will still know the correct order for processing the packets.
- The sequence numbers let the receiving system know if packets are missing.
  - The receiving system can then request re-transmission of packets from the sender to fill any gaps.

TCP Three-Way Handshake

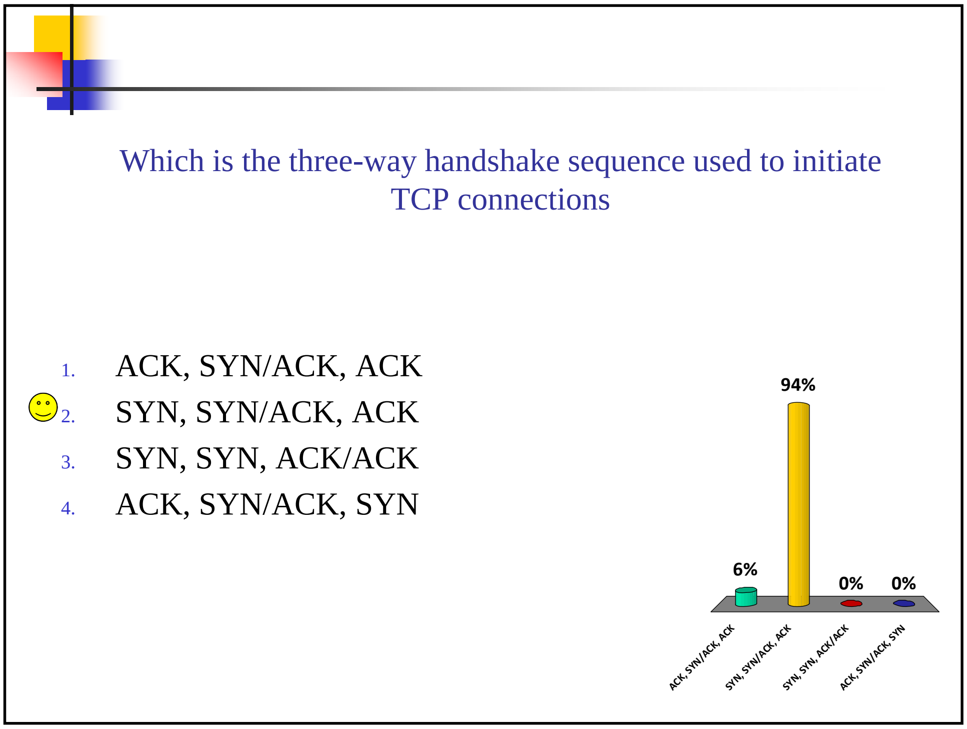
- **Step One**
  - The originating host (client) sends a SYN (synchronize) packet to the destination host (server).
  - This tells the server:
    - What port the client wants to connect.
    - The initial packet sequence number of the client



- **Step Two**
  - The server sends a SYN/ACK (synchronize/acknowledge) packet to the client which tells the client "I received your request."
  - It contains the server's initial packet sequence number.
- **Step Three**
  - The client responds to the server with an ACK packet.
  - This completes the connection establishment process.

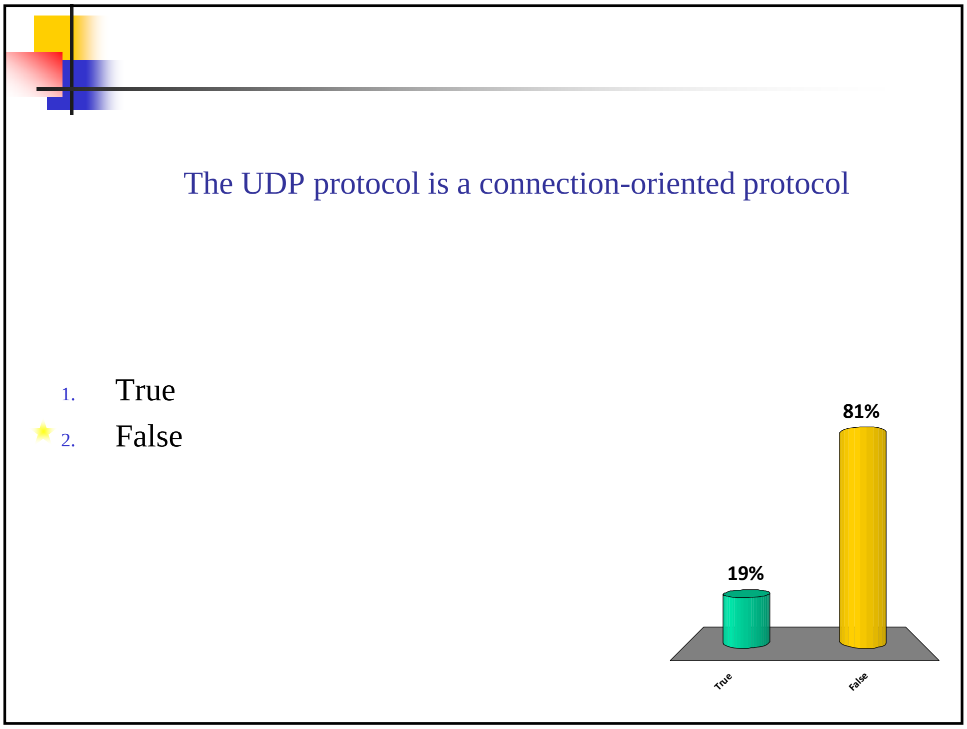
User Datagram Protocol (UDP)

- Like TCP, UDP is a transport protocol
- UDP a "connectionless" protocol.
  - No guarantee of packet delivery
  - Very few error recovery services.
- Used to deliver a packet from one process to another with very low overhead
  - With UDP, packets are created and sent on their way.
  - Does not use handshaking to establish connections
  - Does not keep track of sequencing and acknowledge information
- UDP is an unreliable protocol.
  - Used for network services not affected by the occasional lost or dropped packet.
- But Efficient
  - More time and space of a UDP session is dedicated to content or data delivery.
- Often used for application like streaming media that do not depend on guaranteed delivery of every packet



Which is the three-way handshake sequence used to initiate TCP connections

1. ACK, SYN/ACK, ACK
2. ☺ SYN, SYN/ACK, ACK
3. SYN, SYN, ACK/ACK
4. ACK, SYN/ACK, SYN



The UDP protocol is a connection-oriented protocol

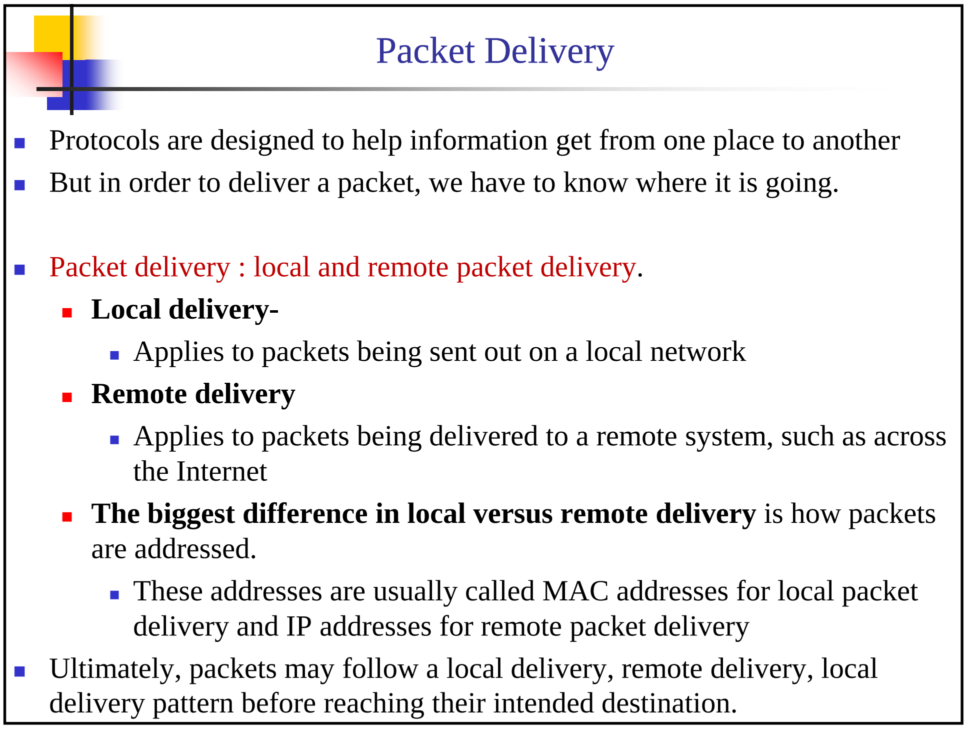
1. True
2. ★ False

Internet Control Message Protocol (ICMP)

- ICMP
  - The third most commonly used protocol
  - A control and information protocol, used to determine:
    - Remote network's availability.
    - Length of time to reach a remote network.
    - The best route for packets for that remote network.
  - Can handle the flow of traffic, telling other network devices to "slow down" transmission speeds if packets are coming in too fast.
  - ICMP, like UDP, is a connectionless protocol.
    - Designed to carry small messages quickly.
    - Has minimal overhead.
    - Has minimum impact to bandwidth.
  - Abused to execute Denial of Service attacks

Denial-of-Service (DoS) Attacks

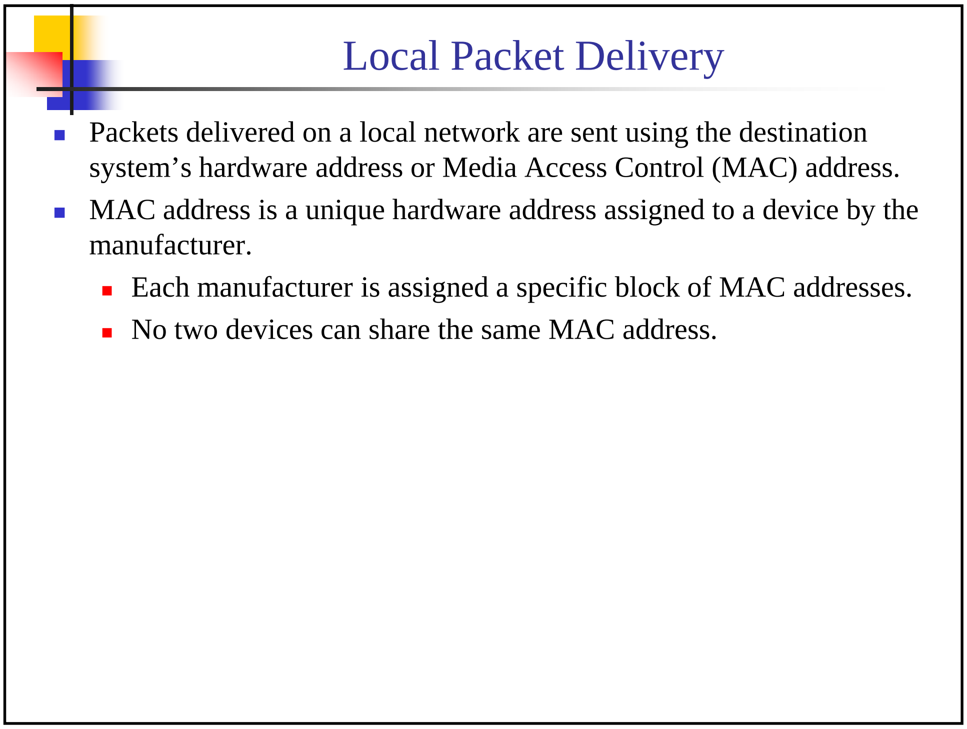
- ICMP protocol has been greatly abused by attackers to execute denial-of-service (DoS) attacks.
  - Because ICMP packets are very small and connectionless, thousands and thousands of ICMP packets can be generated by a single system in a very short period of time.
  - Attackers have developed methods to trick many systems into generating thousands of ICMP packets with a common destination—the attacker's target.



Packet Delivery

- Protocols are designed to help information get from one place to another
- But in order to deliver a packet, we have to know where it is going.

- Packet delivery : local and remote packet delivery.
  - **Local delivery-**
    - Applies to packets being sent out on a local network
  - **Remote delivery**
    - Applies to packets being delivered to a remote system, such as across the Internet
  - **The biggest difference in local versus remote delivery** is how packets are addressed.
    - These addresses are usually called MAC addresses for local packet delivery and IP addresses for remote packet delivery
- Ultimately, packets may follow a local delivery, remote delivery, local delivery pattern before reaching their intended destination.



Local Packet Delivery

- Packets delivered on a local network are sent using the destination system’s hardware address or Media Access Control (MAC) address.
- MAC address is a unique hardware address assigned to a device by the manufacturer.
  - Each manufacturer is assigned a specific block of MAC addresses.
  - No two devices can share the same MAC address.

MAC Address and ARP

- For one system to send data to another on the local network, it must first find out the destination system’s MAC address.
- To find a MAC address, the Address Resolution Protocol (ARP) is used.
  - It is the computer’s way of finding out “who owns the blue convertible with license number 123JAK.”
- Systems know the IP address of the computer to which they want to send data, but not the MAC address.
- Using an ARP request, the sending system will send out a query – “who is 10.1.1.140”?

Resolving the ARP Request

- This broadcast query is examined by every system on the local network, but only the system whose IP address is 10.1.1.140 will respond.
- That system will send back a response that says “I’m 10.1.1.140 and my MAC address is 00:07:e9:7c:c8:aa.”
- The sending system will then format the packet for delivery and drop it on the network media, with the MAC address of the destination workstation.

Remote Packet Delivery

- Local packet delivery is accomplished with MAC addresses.
- Remote packet delivery is usually accomplished using Internet Protocol (IP) addresses.
  - IP addresses are 32-bit numbers that we usually see expressed as a group of four numbers (such as 10.1.1.132).
- The Domain Name Service (DNS) protocol translates names into IP addresses.
  - The DNS server handles DNS queries by examining its local records to see if it knows the answer.
  - If it does not, the DNS server queries higher level domain servers. They check records or query the server above them and so on until a match is found.
- The name for the matching IP address is passed to the computer.
  - The user’s computer can create the Web request, stamp it with the right destination IP address, and send it.

Local or Remote?

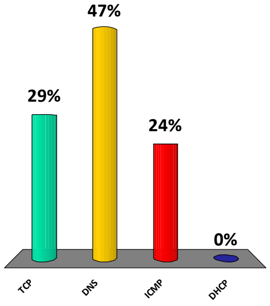
- Before sending the packet, the system will first determine if the destination IP address is on a local or remote network.
  - This is done by sending the packet to a network gateway.
- Network Gateways (Routers):
  - Interconnect networks.
  - Move packets from one network to another.
- The process of moving packets from one network to another is called routing and is critical to the flow of information across the Internet.
  - To accomplish this task, routers use forwarding tables to determine where a packet should go.

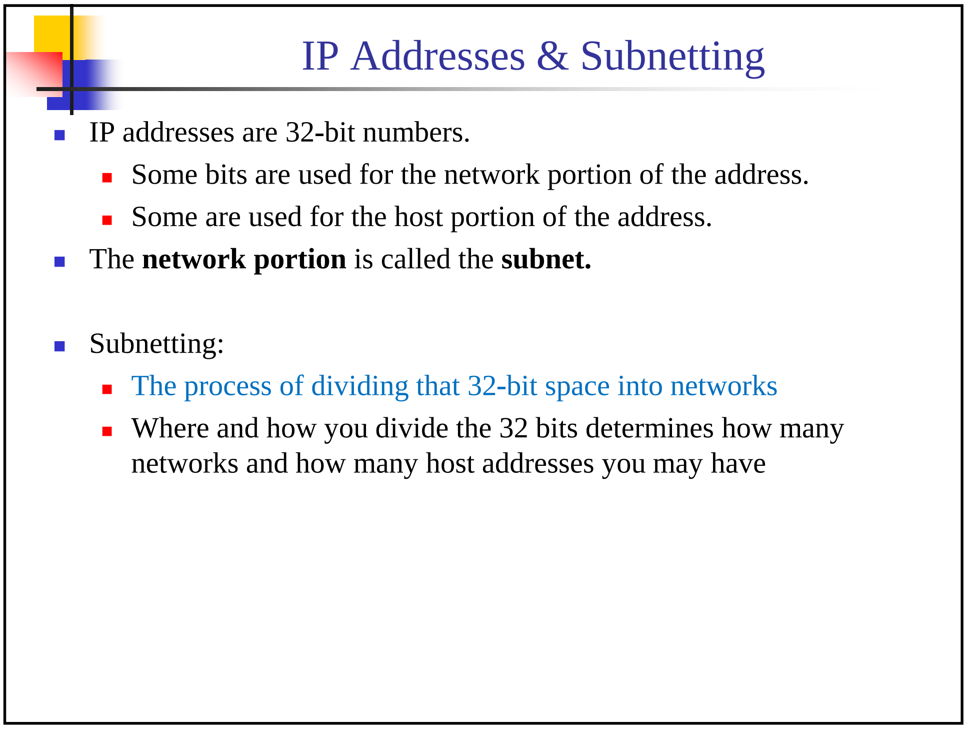
Packet Reaches Router

- When a packet reaches a router:
  - It examines the destination address to determine where to send the packet.
  - If the router’s forwarding tables know where the packet should go, the router sends the packet out along the appropriate route.
- If the router does not know where the destination network is:
  - It will forward the packet to its defined gateway which will repeat the same process.
  - After traversing various networks and routers, the packet will come to the router serving the network with the Web site.
- The destination router determines the MAC address of the destination system and forwards the packet accordingly.

What is the name of the protocol that translated names into IP addresses

1. TCP
2. ☺ DNS
3. ICMP
4. DHCP

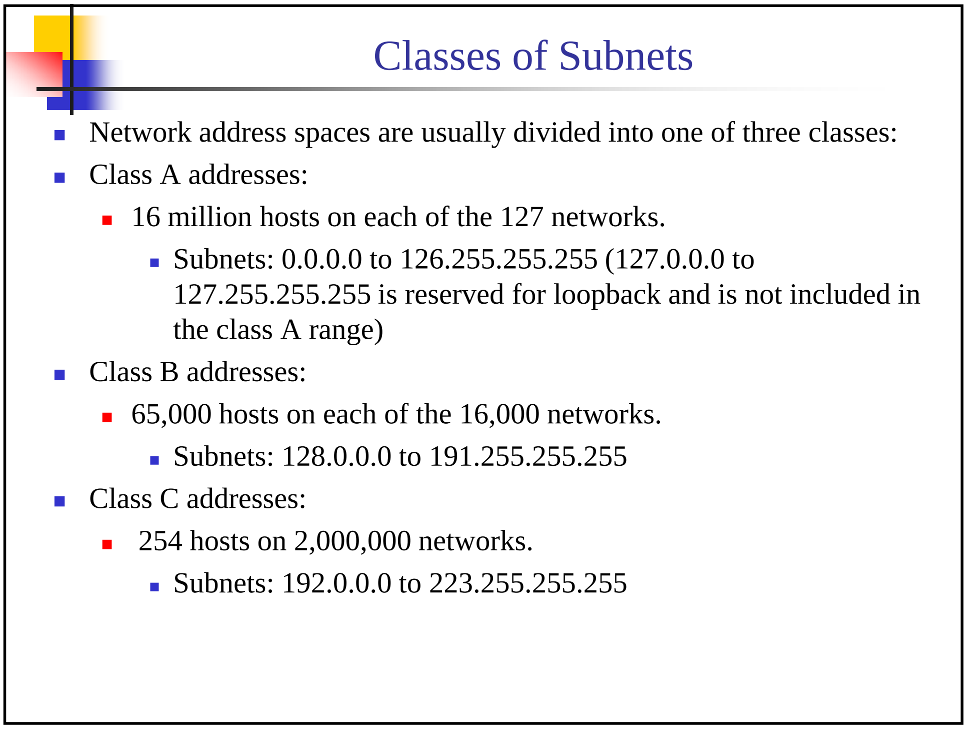




IP Addresses & Subnetting

- IP addresses are 32-bit numbers.
  - Some bits are used for the network portion of the address.
  - Some are used for the host portion of the address.
- The **network portion** is called the **subnet.**

- Subnetting:
  - The process of dividing that 32-bit space into networks
  - Where and how you divide the 32 bits determines how many networks and how many host addresses you may have



Classes of Subnets

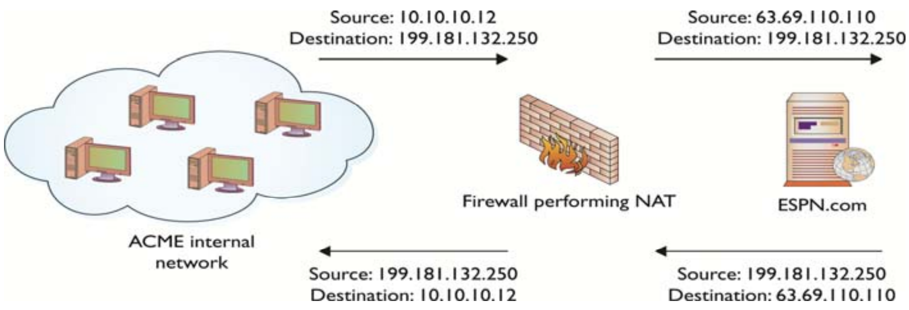
- Network address spaces are usually divided into one of three classes:
- Class A addresses:
  - 16 million hosts on each of the 127 networks.
    - Subnets: 0.0.0.0 to 126.255.255.255 (127.0.0.0 to 127.255.255.255 is reserved for loopback and is not included in the class A range)
- Class B addresses:
  - 65,000 hosts on each of the 16,000 networks.
    - Subnets: 128.0.0.0 to 191.255.255.255
- Class C addresses:
  - 254 hosts on 2,000,000 networks.
    - Subnets: 192.0.0.0 to 223.255.255.255

Network Address Translation

- **Network Address Translation** (NAT) compensates for the lack of available IP address space.
- NAT translates private (non-routable) IP addresses into public (routable) IP addresses.
  - Helps in hiding internal IP addresses

Example of NAT

- In the figure, we see an example of NAT being performed.
  - An internal workstation (10.10.10.12) wants to visit the ESPN.com



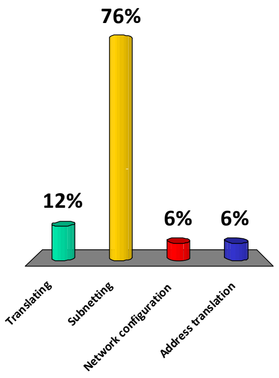
Logical depiction of NAT

Decoding for NAT

- A packet NAT device
  - The device translates the 10.10.10.12 source address to the globally routable 63.69.110.110 address.
  - This is the IP address of the device’s externally visible interface.
- When the ESPN Web site responds, it responds to the device’s address.
  - Just as if the NAT device had originally requested the information.
- The NAT device must then remember which internal workstation requested the information and route the packet to the appropriate destination.

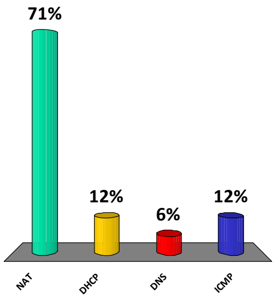
Dividing a network address space into smaller separate networks is called

1. Translating
2. ☺ Subnetting
3. Network configuration
4. Address translation



Which protocol translates private (nonroutable) IP addresses into public (routable) addresses

☺ 1. NAT
2. DHCP
3. DNS
4. ICMP



IP Address Assignment

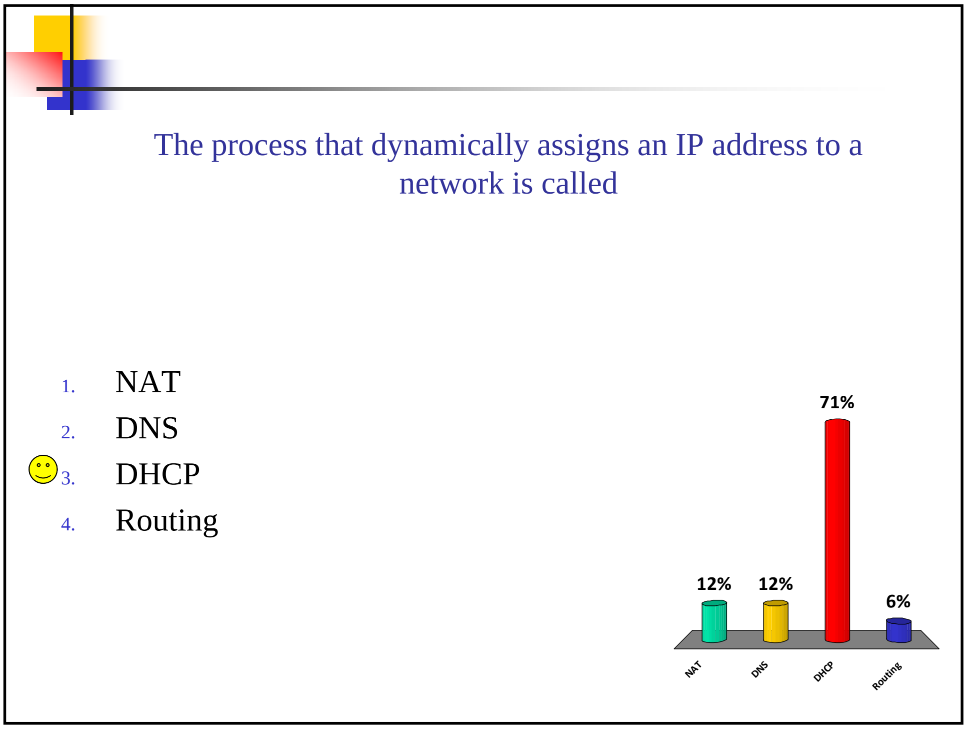
- When administrators set up a network, they usually assign IP addresses to systems in one of the two ways:
  - Statically
  - Via a DHCP
- Static IP address assignment is simple.
  - The administrator decides what IP address to assign to a server or PC and that IP address stays assigned to that system until the administrator decides to change it.

DHCP

- When a system boots or is connected to the network, it sends out a query for a DHCP server.
  - If a DHCP server is available on the network, it will answer the new system and assign the new system an IP address from a pool of dedicated, available addresses.
- DHCP is an “as available” protocol.
  - If the server has allocated the available IP addresses in the pool, new systems will not receive an IP address and will not be able to connect to the network.

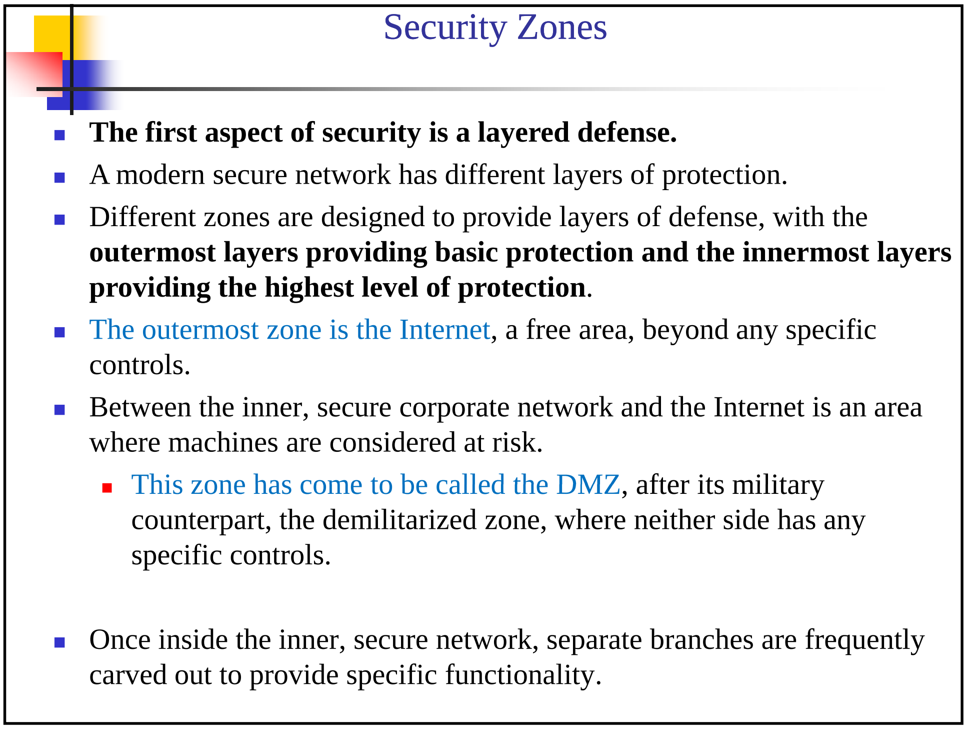
DHCP

- A key feature of DHCP is the ability to limit how long a system may keep its DHCP-assigned IP address.
  - These DHCP addresses have a limited lifespan.
    - Once the ‘lease’ expires, the system using that IP address must either renew that address or request another address from the DCHP server.
  - The requesting system may have the same IP address, or it may be assigned a completely new address depending on how the DHCP server is configured and the current demand for available addresses.
- DHCP is very popular in large user environments where the cost of assigning and tracking IP addresses is large.



The process that dynamically assigns an IP address to a network is called

1. NAT
2. DNS
3. ☺ DHCP
4. Routing



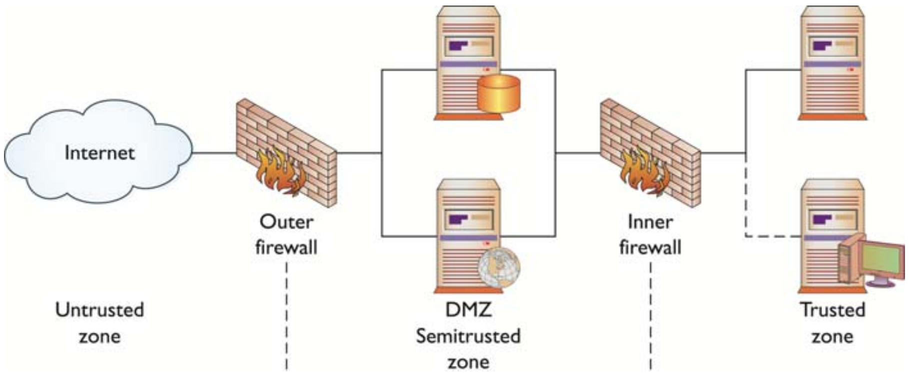
Security Zones

- **The first aspect of security is a layered defense.**
- A modern secure network has different layers of protection.
- Different zones are designed to provide layers of defense, with the **outermost layers providing basic protection and the innermost layers providing the highest level of protection**.
- The outermost zone is the Internet, a free area, beyond any specific controls.
- Between the inner, secure corporate network and the Internet is an area where machines are considered at risk.
  - This zone has come to be called the DMZ, after its military counterpart, the demilitarized zone, where neither side has any specific controls.
- Once inside the inner, secure network, separate branches are frequently carved out to provide specific functionality.

Internet

- The Internet is a worldwide connection of networks and is used to transport e-mail, files, financial records, remote access—you name it—from one network to another.
- It is a series of interconnected networks that allows protocols to operate to enable data to flow across it.
- This large web allows users almost infinite ability to communicate between systems.
- Because everything and everyone can access this interconnected web and it is outside of your control and ability to enforce security policies, the **Internet should be considered an untrusted network.**
- A firewall should exist at any connection between your trusted network and the Internet.

The DMZ and Zones of Trust



Intranet

- Intranet
  - Network that has the same functionality as the Internet for users but lies completely inside the trusted area of a network and is under the security control of the system and network administrators.

- Content on intranet web servers is not available over the Internet to untrusted users.

- This layer of security offers a significant amount of control and regulation, allowing users to fulfill business functionality while ensuring security.

Extranet

- Extranet
  - An extension of a selected portion of a company's intranet to external partners.
  - Allows a business to share information with customers, suppliers, partners, and other trusted groups while using a common set of Internet protocols to facilitate operations.
    - Can be accessed by more than one company, because they share information between organizations

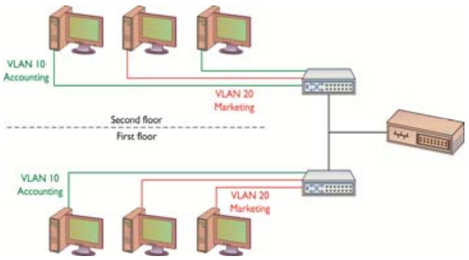
  - Business can use public networks to extend their reach beyond a company's own internal network, and some form of security, typically VPN, is used to secure this channel.

VLANs

- **LAN**
  - A set of devices with similar functionality and similar communication needs, typically co-located and operated off a single switch.
  - This is the lowest level of a network hierarchy and defines the domain for certain protocols at the data link layer for communication.
- **Virtual LAN (VLAN)**
  - A logical implementation of a LAN and allows computers connected to different physical networks to act and communicate as if they were on the same physical network.
  - Has many of the same characteristic attributes of a LAN and behaves much like a physical LAN but is implemented using switches and software.
  - A very powerful technique allows significant network flexibility, scalability, and performance
  - Allows administrators to perform network reconfigurations without having to physically relocate or recable systems.

Trunking

- Trunking is the process of spanning a single VLAN across multiple switches.
- A trunk-based connection between switches allows packets from a single VLAN to travel between switches.
- Trunks enable network administrators to set up VLANs across multiple switches with minimal effort.
  - With a combination of trunks and VLANs, network administrators can subnet a network by user functionality without regard to host location on the network or the need to recable machines.



Security Implications

- A security strength of VLANs is that systems on separate VLANs cannot directly communicate with each other.
- VLANs are used to divide a single network into multiple subnets based on functionality.
  - This permits accounting and marketing, for example, to share a switch because of proximity yet still have separate traffic domains.
- The physical placement of equipment and cables is logically and programmatically separated so that adjacent ports on a switch can reference separate subnets.
  - This prevents unauthorized use of physically close devices through separate subnets that are on the same equipment.

Security Implications

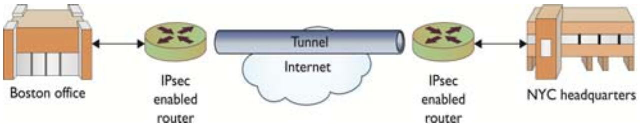
- VLANs also allow a network administrator to define a VLAN that has no users and map all of the unused ports to this VLAN
  - Some managed switches allow administrators to simply disable unused ports as well
  - If an unauthorized user should gain access to the equipment, that user will be unable to use unused ports, as those ports will be securely defined to nothing.
- Security strength of VLANs
  - Systems on separate VLANs cannot directly communicate with each other.

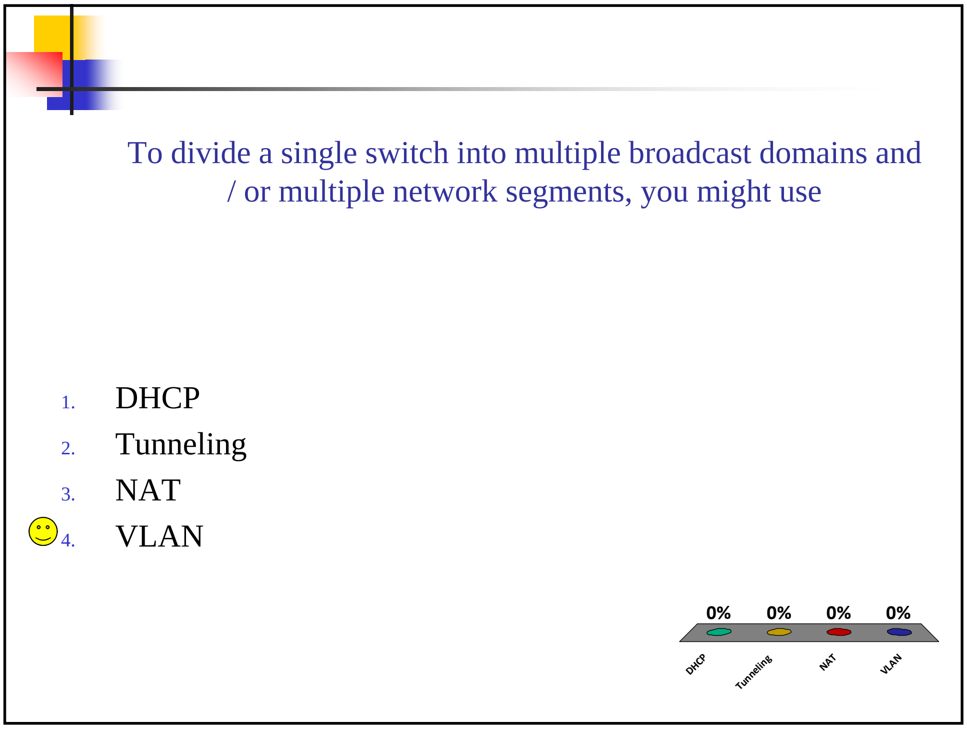
Tunneling

- Tunneling
  - A method of packaging packets so that they can traverse a network in a secure, confidential manner.
  - Involves encapsulating packets within packets, enabling dissimilar protocols to coexist in a single communication stream
  - Can provide significant measures of security and confidentiality through encryption and encapsulation methods.
  - Because of ease of use, low-cost hardware, and strong security, tunnels and the Internet are a combination likely to be used more in the future.
  - IPsec, VPN, and tunnels will become a major set of tools for users requiring secure network connections across public segments of networks.

Tunneling- Example

- A company has multiple locations and decides to use the public Internet to connect the networks at these locations.
- To make these connections secure from outside unauthorized use, the company employ a VPN connection between the different networks.
- On each network, an edge device, usually a router, connects to another edge device on the other network.
- Then, using IPsec protocols, these routers establish a secure, encrypted path between them.
- This securely encrypted set of packets cannot be read by outside routers; only the addresses of the edge routers are visible.
- **This arrangement acts as a tunnel across the public Internet and establishes a private connection, secure from outside snooping or use**.





To divide a single switch into multiple broadcast domains and / or multiple network segments, you might use

1. DHCP
2. Tunneling
3. NAT
4. ☺ VLAN

0%
0%
0%
0%
DHCP
Tunneling
NAT
VLAN