Telecommunications and Network Security

Domain 2

Objectives

- OSI Model and the TCP/IP Suite
- Cabling and data transmission types
- LAN and WAN technologies
- Network devices and service
- Telecommunication protocols and devices
- Remote access methods and technologies
- VPNs
- Wireless Technology
- Attacks

Agenda

- OSI Model, the TCP/IP suite, and other Protocols
- Signaling and Cabling
- Network Types and LAN Access Technologies
- Firewalls, Bastion Hosts, and Firewall Architecture
- Dial-up, Remote Access, Tunneling, and VPN Protocols
- MAN and WAN Technologies, VoIP, and PBX
- Wireless Networking and Network Attacks

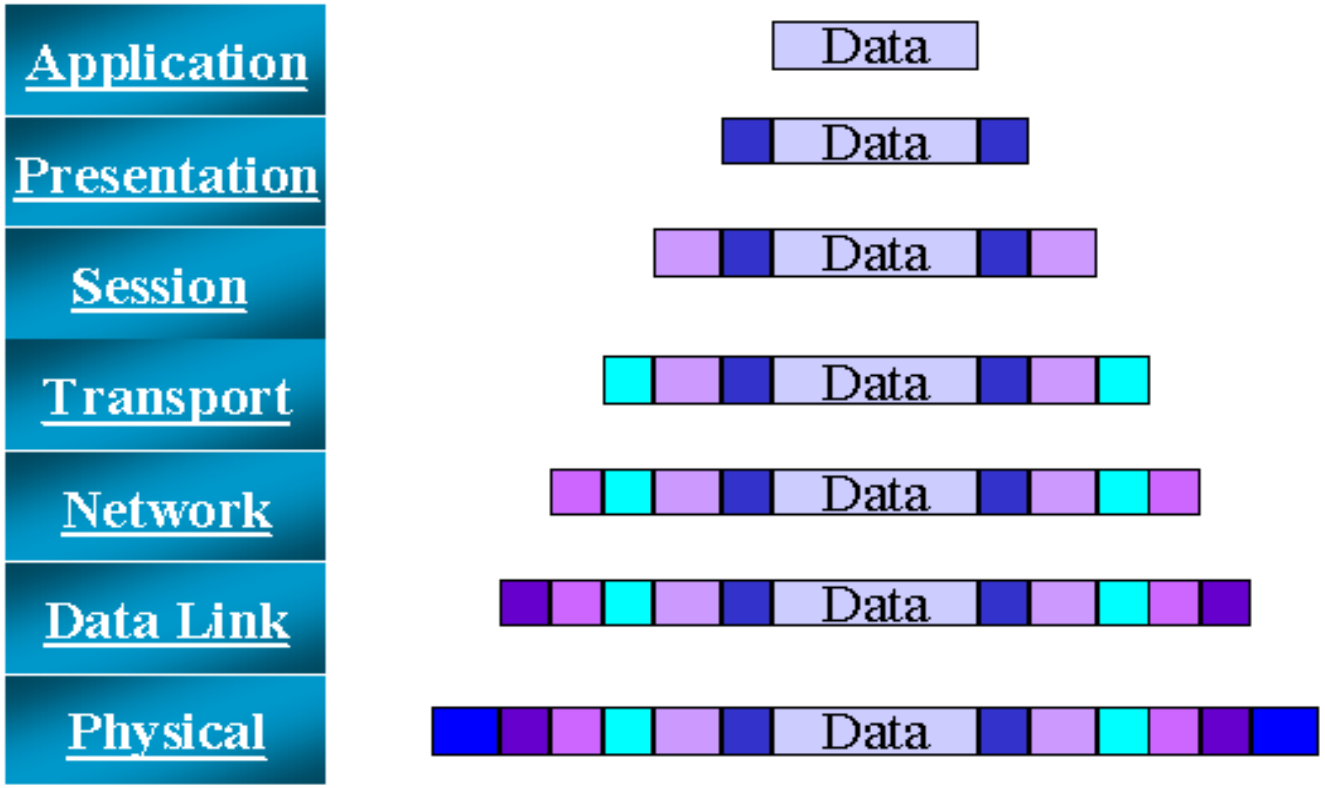
OSI Model

Purpose of the OSI Model

- Increase interoperability between vendor products
  - Using industry standard interfaces
- Clarify network services functionality and communication processes
  - Without looking at granular specifics
- Modular approach so that component can be modified without affecting others

Data Encapsulation**

- Each layer adds its own information to the data as it travels down the OSI layers



Physical Layer

- **Specifies how signals are transmitted on network**
  - Electrical Signaling
  - Bits converted to electrical signals
- **Interface to media**
  - Provides electrical and mechanical interfaces for a network
  - Data is sent across physical media
  - Applies to cables and cards
- **Responsible for encoding scheme**
  - Manchester encoding

Data Link Layer

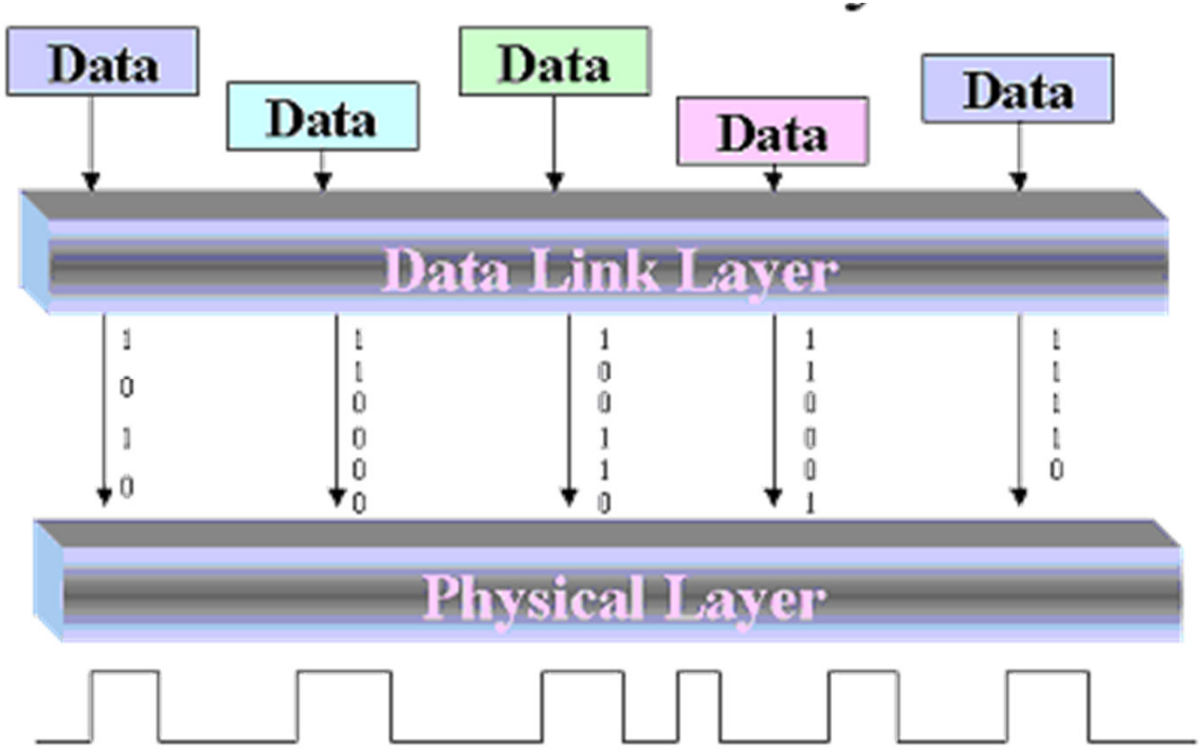
- **Sender breaks data into frames**
- **Formats frame for proper technology**
  - Token Ring
  - Ethernet
  - ATM
- **Media access**

Data Link Layer (cont.)

- **Media Access Methods**
  - CSMA/CD (Carrier Sense Multiple Access with Collision Detection) 802.3 Ethernet
  - Collision/Contention based
  - Token Passing 802.5 Token Ring, FDDI
  - 802.11 Wireless CSMA/CA
  - 802.12 Polling

- **Synchronization and error control**

Data Link and Physical Layers



Data Link

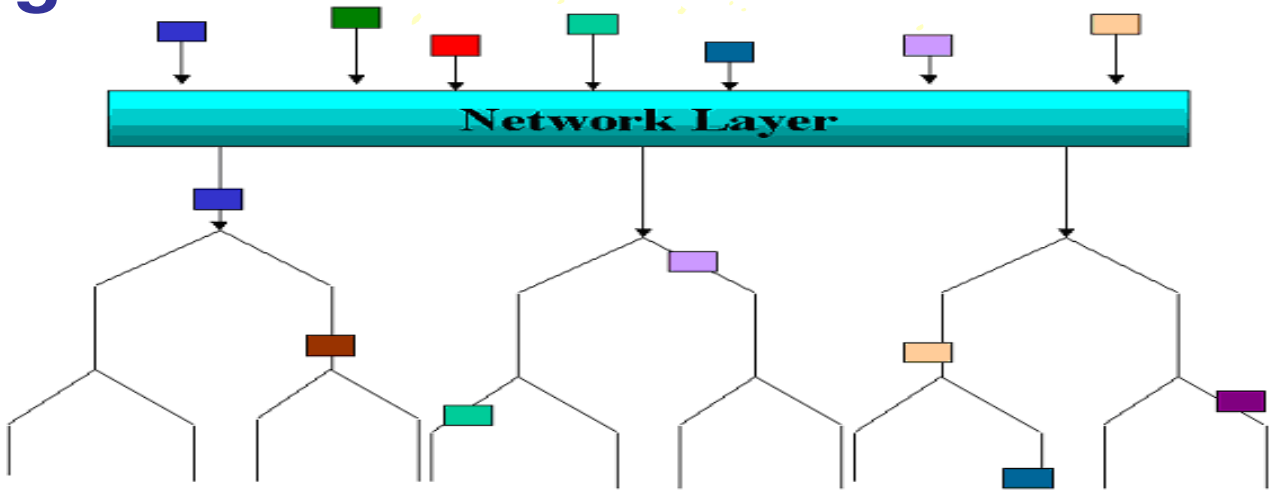
- **Rules of accessing the media**
- **Ethernet, Token Ring, Wireless**

Physical

- **Bits into voltage**
- **Coaxial, Twisted Pair, Fiber**

Network Layer

- Routes data between systems or different networks
- Confidentiality, authentication, and integrity can be provided at this layer
- Selects route for packets to take
- Fragmentation for dissimilar frame sizes



Transport Layer

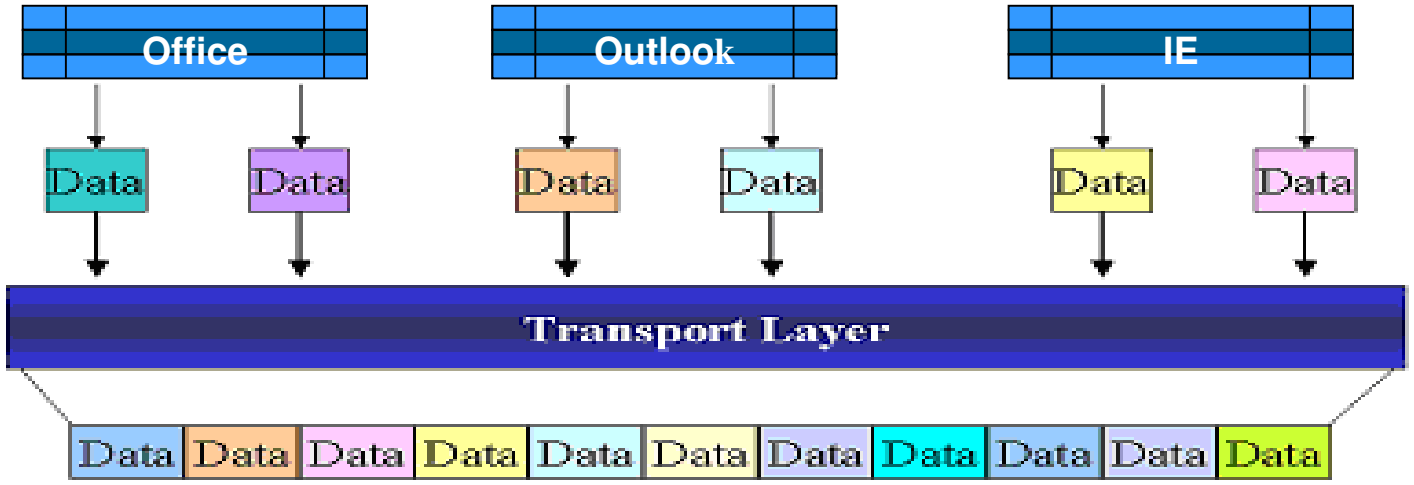
- End-to-end packet transfer using connection-oriented or connectionless services
- Buffering of data until all is sent or receiving system can process
- Error control and recovery if necessary

Transport Layer (cont.)

- Use of ports to communicate with higher level protocols
- Segmenting packets for processing by the network layer
- Packet sequencing

Transport Layer

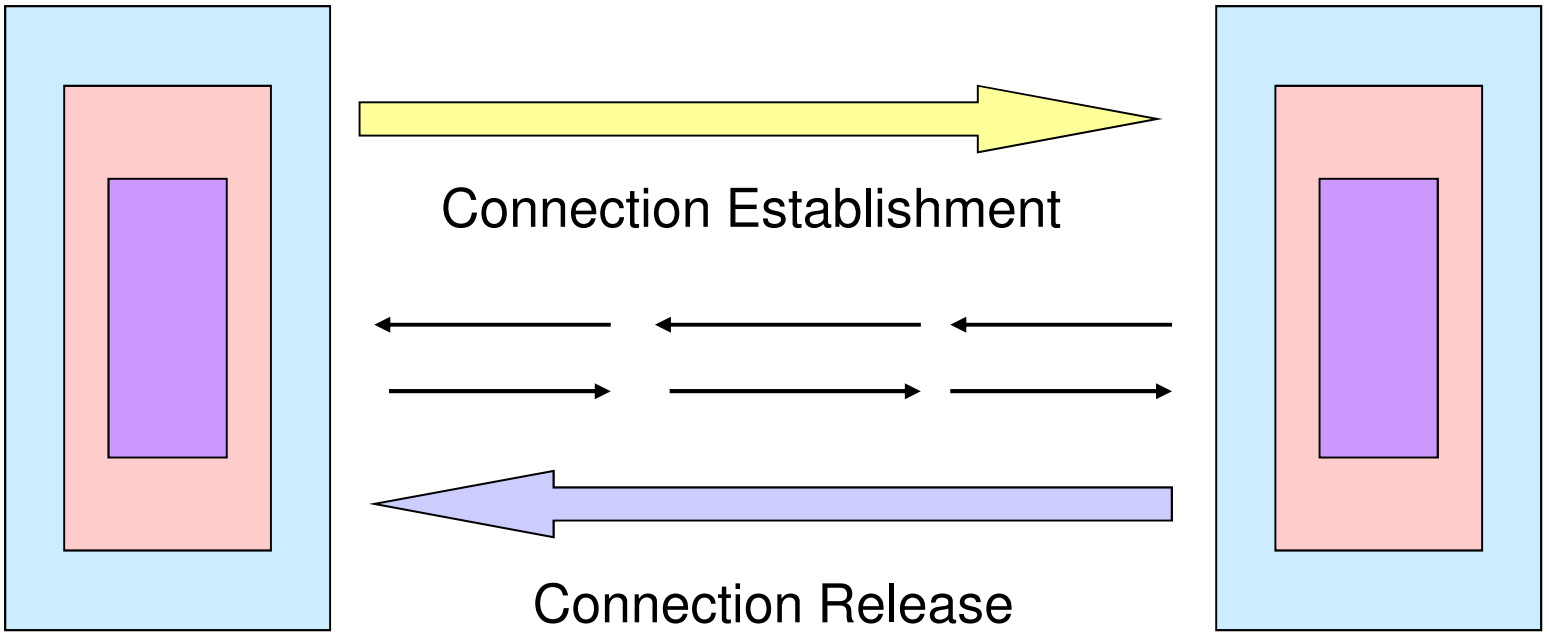
- Segment and reassemble data to form a data stream
- Sequence numbers, error control, ports, and flags
- Protocols that will “carry” the data to the destination



Assemble Data into a Stream

Session Layer

- Sets up communication with destination
- Maintenance of connection
- SQL, NFS, and RPC



Session Layer

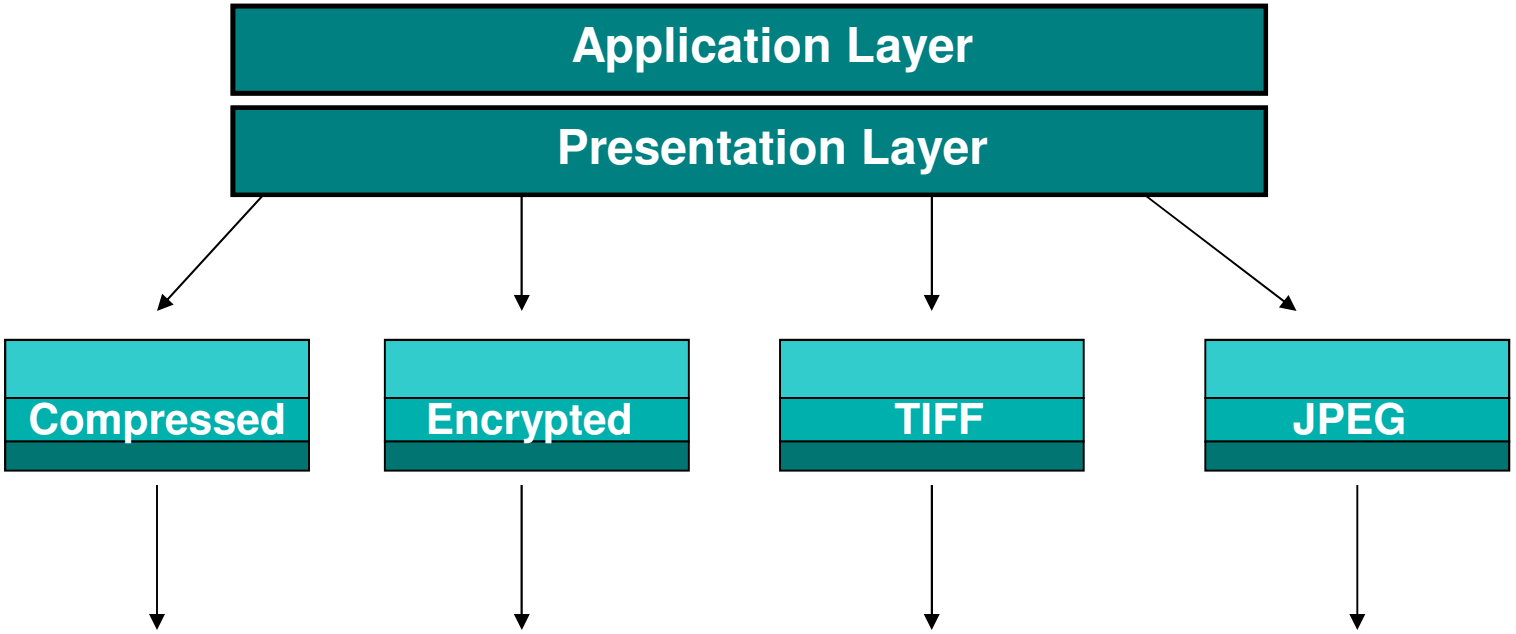
- **Allows applications to organize and synchronize how they will transfer data**
- **Exception reporting**
- **Session setup, maintenance, session tear down**
  - Dialog management between programs

Session Layer (cont.)

- Provides recovery services if required
- Full-duplex: two-way conversation at the same time
- Half-duplex: only one node can communicate at a time

Presentation Layer

- Translates message into standard presentations
- Formatting and encoding
- File level encryption
- File level compression



Presentation Layer

- **Specifies or negotiates how data is represented in binary when exchanged by applications**

- **Encoding**
  - ASCII: American National Standard Code for Information Interchange
  - EBCDIC: Extended Binary Coded Decimal Interchange Code

- **Formatting**
  - GIF, TIFF, and JPEG

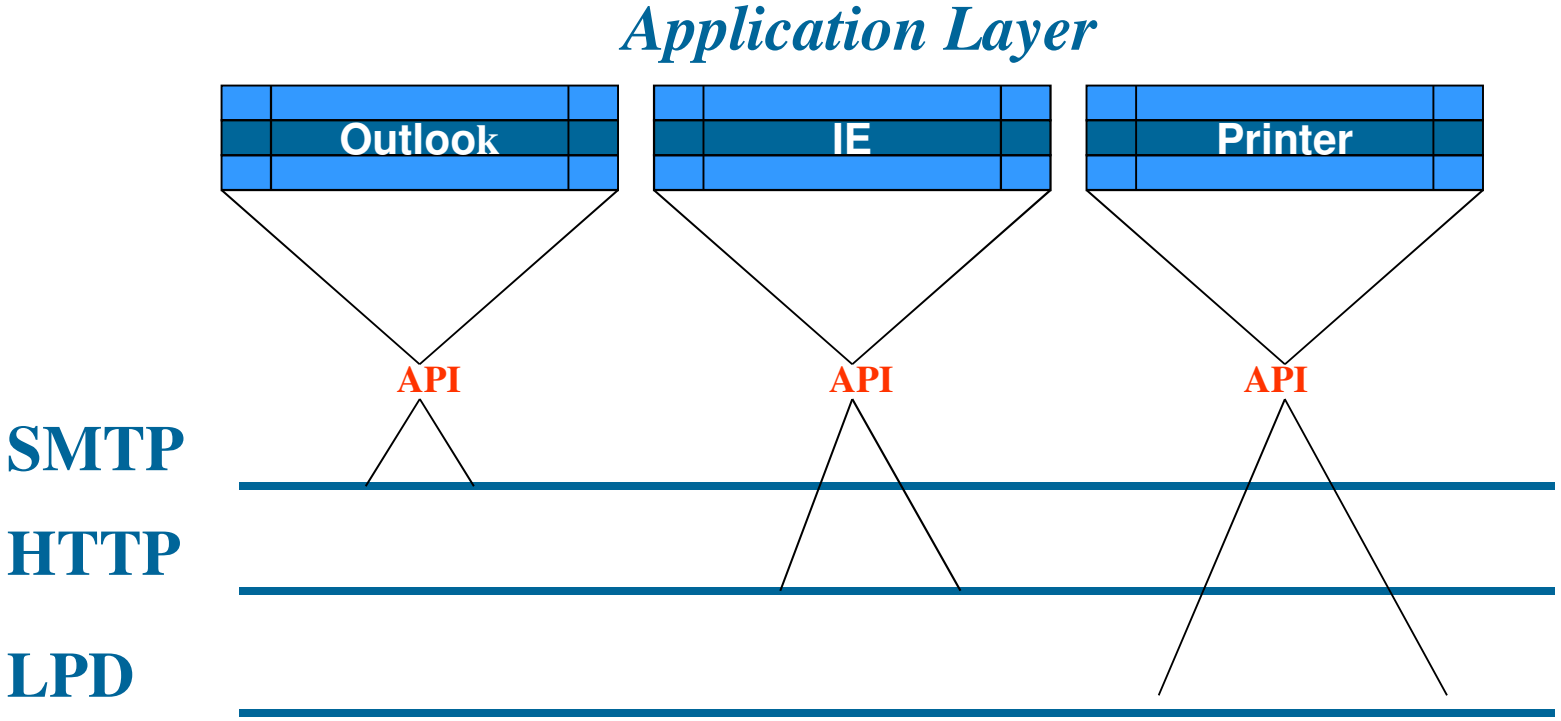
Application Layer

- **Functionality**

- **Allows for services and protocols required by application processes:**
  - File Transferring
  - E-mail
  - Access Control Services
  - Gateways
  - File Management
  - Web Browser
  - Non-repudiation

Application Layer

- Provide network communication to applications
- SMTP, HTTP, FTP, Telnet, and TFTP



OSI Review

OSI (Open Systems Interconnect) Model

7. Application: Protocols that drive the applications that users interface with. HTTP, FTP, SMTP, POP, IMAP, Telnet, NTP, NNTP, SNMP, TFTP –DATA

6. Presentation: Formatting (ASCII) Compression (jpeg vs. gif)

5. Session: End to end connection between applications-- Setup and Teardown

OSI Review (cont.)

4. Transport: Error Correction, Connection-oriented (TCP)—Acknowledgements—Window Size (flow control) or Connectionless (UDP)--Segment

3. Network: Logical Addressing, Routing, IP Address, IPX--Packets

2. Data Link: Error Detection, NIC, Hardware Addressing, Switches, Ethernet vs. Token Ring--Frames

   a. MAC (Media Access Control)

   b. LLC: Error Detection

OSI Review (cont.)

1. Physical: Moving bits on the wire. “Dumb devices” Hub, Cable, Connectors, NIC, repeaters--Bits

- **All People Seem To Need Delicious Pizza.**

Protocols and Devices at Each Layer

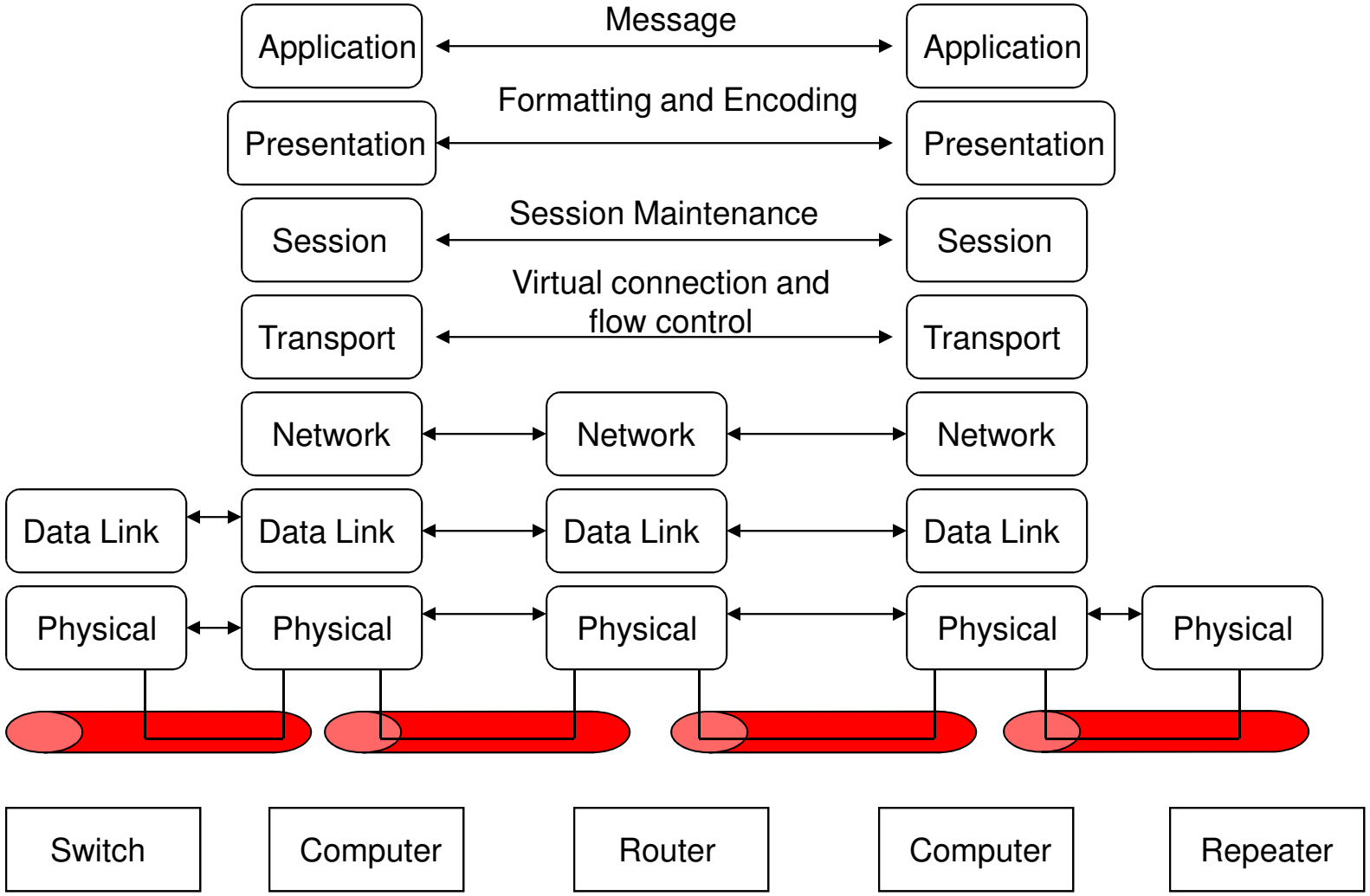
OSI Layer	Protocols and Devices
Application	FTP, TFTP, BOOTP, SNMP, RLOGIN, SMTP, MIME, FINGER, TELNET, NCP, APPC, AFP, SMB, HTTP *Gateways
Presentation	ASCII, TIFF, GIF, JPEG, MPEG, MIDI
Session	**DNS**, NetBIOS, NFS, SQL, RPC
Transport	TCP, UDP, SPX, SSL, TLS
Network	IP, ICMP, RIP, IGMP, IPX *Routers
Data Link	SLIP, PPP, ARP, RARP, L2F, L2TP, Ethernet, Token Ring, X.25, Frame Relay, ATM *Bridges, Switches
Physical	High-speed Serial Interface (HSSI), X.21, EIA/TIA-232, EIA/TIA-449, SONET *Amplifiers, Repeaters, Hubs

Protocols

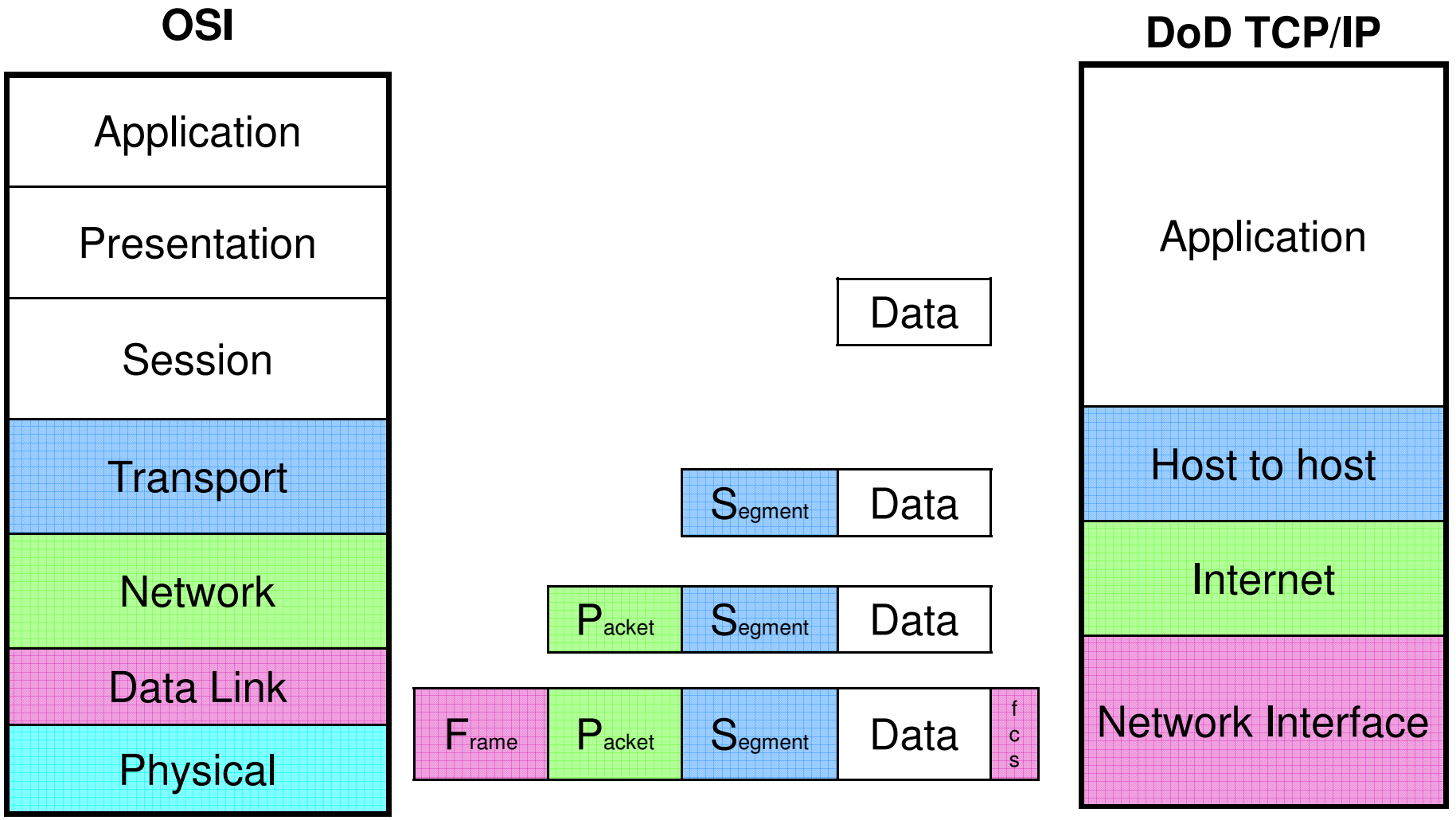
What Are Protocols?

- Protocols are the rules used to allow two or more computers to send and receive data
- Allow different operating systems and applications to communicate
- Different protocols have different functionalities and goals
- Different network models specify services carried out by protocols
- Protocol stack means modules of functionality at different layers

Activity at Different Layers



OSI and the TCP/IP Suite of Protocols



TCP/IP

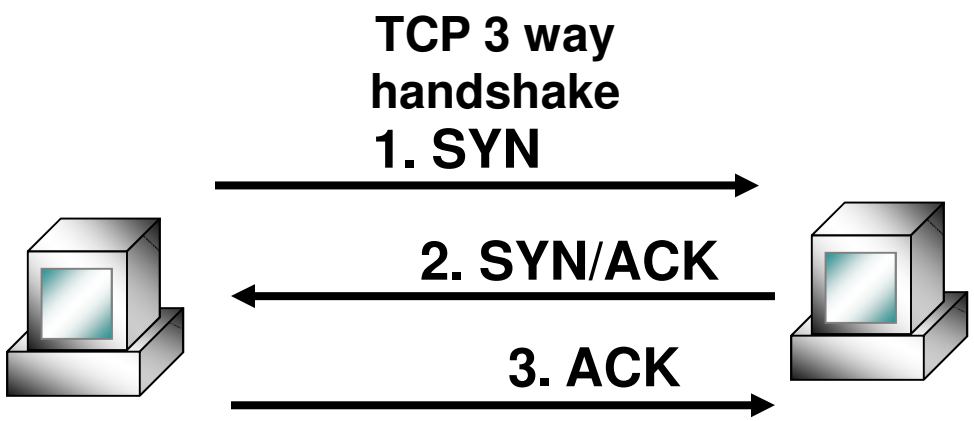
Protocol of the Internet

- Transmission Control Protocol/Internet Protocol
- Suite of protocols that govern how data transmission
- Port numbers track different conversations
  - FTP ports 20 and 21
  - SMTP port 25
  - SNMP port 161
  - HTTP port 80
  - Telnet port 23
- Source port numbers are dynamic
- Destination port values are usually under 1024

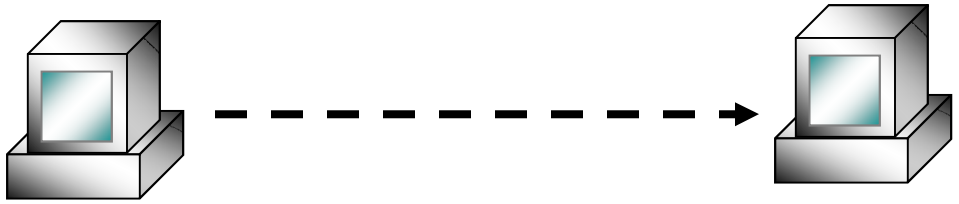
TCP vs. UDP

TCP

- Connection-oriented
- Reliable
- Provides flow control



UDP



- Connectionless
- Non-reliable
- No handshake is performed
- “Best effort” protocol

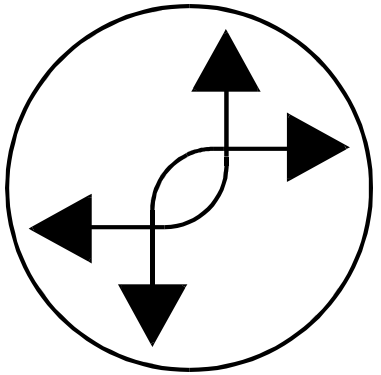
TCP and UDP Characteristics

Service	TCP	UDP
Reliability	Ensures that packets reach their destinations; Returns ACKs when packet is received; Considered reliable	Does not return ACKs; Does not guarantee delivery; Considered unreliable
Connection	Connection-oriented (performs handshaking and develops a virtual connection with destination computer)	Connectionless-oriented (does not handshake, does not use virtual connection)
Packet Sequencing	Uses sequence numbers within packets to make sure that each packet within a message is received	Does not use sequence numbers
Congestion Controls	Destination computer can tell the source, if it is overwhelmed, to slow the transmission rate	Destination computer does not communicate back to the source computer about flow control
Usage	Used when reliable delivery is required, as in e-mail, DNS, and HTTP requests	Used when reliable delivery is not required, as in streaming video and status broadcasts
Speed and Overhead	Uses a considerable amount of resources and is slower than UDP	Uses fewer resources and is faster than TCP

IP

Internet Protocol

- A connectionless protocol that routes data
- IP is unreliable and does not ensure that packets arrive in order or undamaged
- An IP datagram includes all necessary information to forward it to its destination



IP Addressing Basics

- IP Addressing
- Subnets
- CIDR (Classless Inter-Domain Routing)

IPv4 Addressing

IPv4 Addresses:

- Are 32-bits (4-bytes) long
- Uniquely identify a particular network interface
- Contain two parts:
  - Network ID or prefix
  - Locally administered bits

IP Classful Address Range

Specified by original IP document (RFC 721) is still used, but classless addressing is the norm

Address Class	Range and Class	Description
A	0.0.0.0 to 126.0.0.0 Mask 255.0.0.0 (/8)	First byte defines network
B	128.0.0.0 to 192.255.0.0 Mask 255.255.0.0 (/16)	First two bytes define network
C	192.0.0.0 to 223.255.255.0 Mask 255.255.255.0 (/24)	First three bytes define network
D	224.0.0.0 to 239.255.255.255	Used for multicast traffic
E	240.0.0.0 to 255.255.255	Reserved for future use

Addressing Basics

- **IPv4 Addressing basics**
  - Class A: About 16 million addresses
  - Class B: About 65 thousand addresses
  - Class C: Only 254 useable addresses
- **Without subnets, only one single broadcast domain exists**

Introducing IPv6

- 2113:0dc2:2f29:0000:0000:0000:003d:9c5a
- 128 bit address
- Eight blocks for four hexadecimal digits
- Cloned hexadecimal
- Can be shortened by eliminating leading 0s:
  - 2113:dc2:2f29:0:0:0:3d:9c5a
- Adjacent blocks of 0's can be replaced with ::, but only once:
  - 2113:dc2:2f29::3d:9c5a

Structure of IPv6

- **Unicast IPv6 are divided into 2 parts**
  - a 64 bit network and 64 bit host.
- **Network identifies each subnet as unique**
- **Host component is typically based on MAC, or can be randomly generated**
- **1st 64 bits of unicast address are always to id network, so no subnet mask is needed.**

Global Addresses

- Global Addresses are the equivalent of public addresses and are globally reachable
- 1st 48 bits of the address are the global routing prefix
- Next 16 bits are the subnet ID. Allows up to 65,536 internal subnets

Link-local Addresses

- Similar to APIPA addresses
- Self-configured, non-routable
- Used only for communication on the local subnet
- Always begins with “fe80::”, but understood as fe80:0000:0000:0000
- Second half address is the interface ID
- Zone ID follows address to differentiate different network segments

Unique Local Addresses

- Equivalent of IPv4 Private addresses (10.x.x.x, 172.16.x.x,192.168.x.x)
- Routable between subnets on a private network, but not across the internet
- Begin with “fd”
- The next 40 bits represent the global id and is randomly generated value that identifies a specific site within the organization
- Next 16 bits represent subnet ID
- Last 64 bits are the interface ID

States of an IPv6

- IPv6 hosts typically configure by interacting with an IPv6 enabled router and performing autoconfiguration
- Tentative State is the initial state of autoconfiguration, before the address is verified as unique
- Preferred State is the address once uniqueness has been verified

Agenda

- OSI Model, the TCP/IP suite, and other Protocols
- Signaling and Cabling
- Network Types and LAN Access Technologies
- Firewalls, Bastion Hosts, and Firewall Architecture
- Dial-up, Remote Access, Tunneling, and VPN Protocols
- MAN and WAN Technologies, VoIP, and PBX
- Wireless Networking and Network Attacks

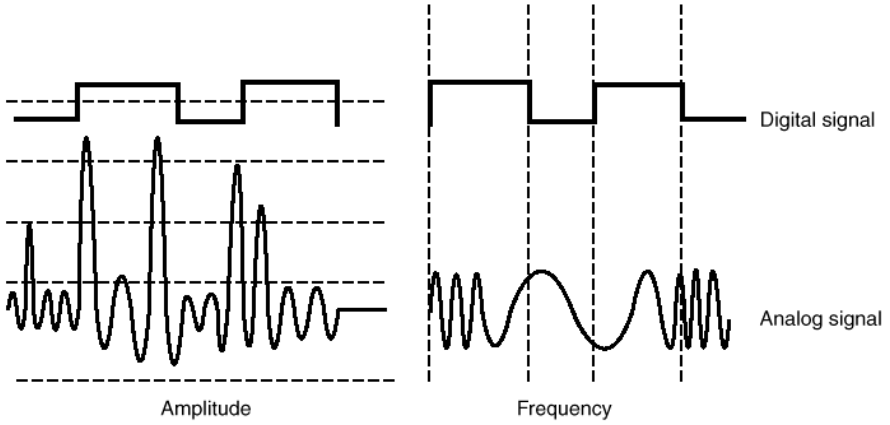
Signals

Analog Transmission

- Varying electromagnetic waves – continuous signal
- Varied by amplification

Digital Transmission

- Electrical pulses representing binary digits
- On-off only



Signaling Techniques

Synchronous Transmission

- Stream of data – no start and stop bits
- Two systems synchronize before data is sent – clocking mechanism
- Used to transfer Large amounts of data

Asynchronous Transmission

- Bits are sent sequentially
- Used to transfer small amounts of data
- Start and stop bits used
- Modems and dial-up communication

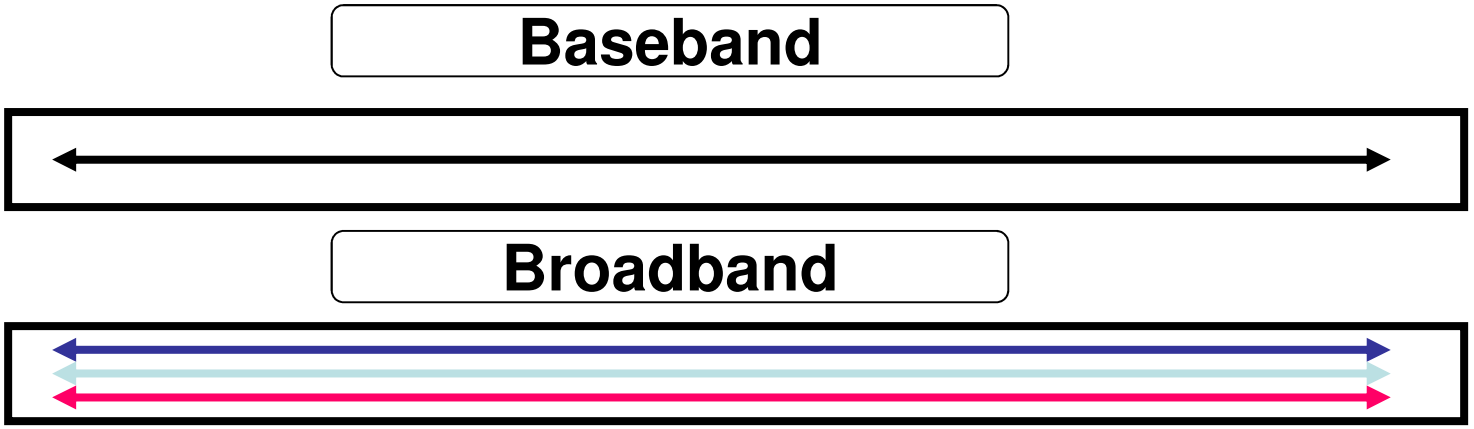
Baseband and Broadband

Baseband Signals

- Cable only uses one channel
- Uses dedicated frequencies

Broadband Signals

- Cable uses several channels at once
- Can transmit more data per unit of time



Network Topologies

Network Topology

- Physical arrangement of systems and devices
- Different than media access technologies

Topology Types

- Bus
- Ring
- Star
- Mesh

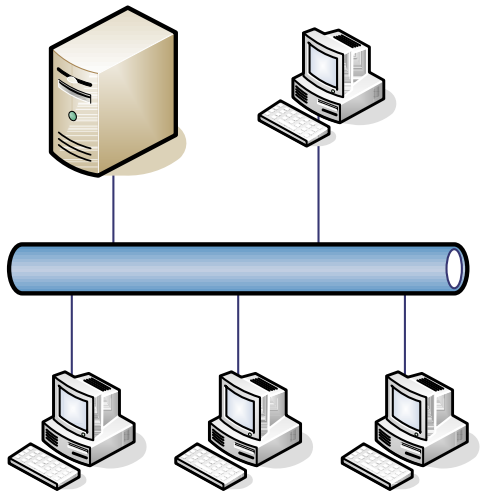
Bus

Bus Characteristics

- Single cable where computers are connected to drops
- Each computer “sees” each packet and accepts or denies it (depending on the address)
- Cable is the single point of failure

Linear Bus

- One cable with no cables branched off



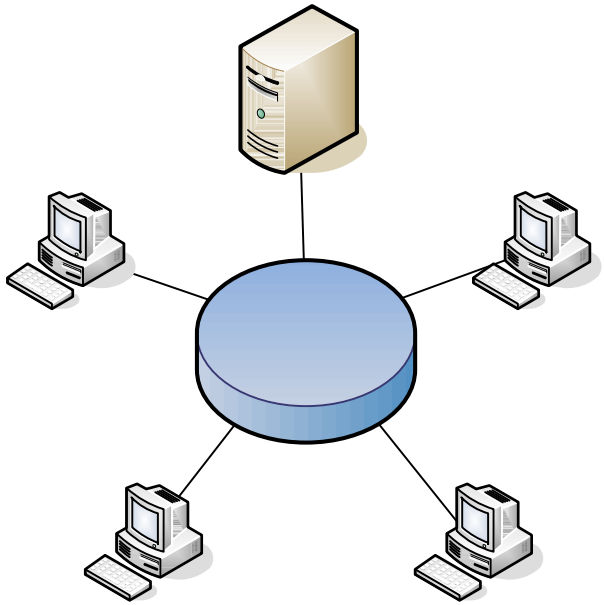
Tree Topology

- Network with branches of cables

Ring

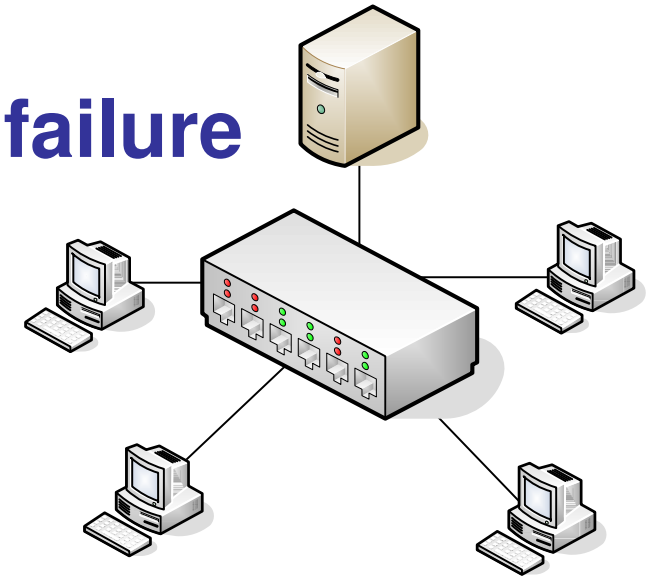
Ring Characteristics

- Series of computers and devices connected by unidirectional transmission links
- Each computer is dependent on the preceding computer
- If one system goes down, it can affect all other systems



Star

- All computers are connected to a central hub (or switch)
- The central hub needs to provide enough bandwidth not to affect the data throughput
- The hub is the single point of failure



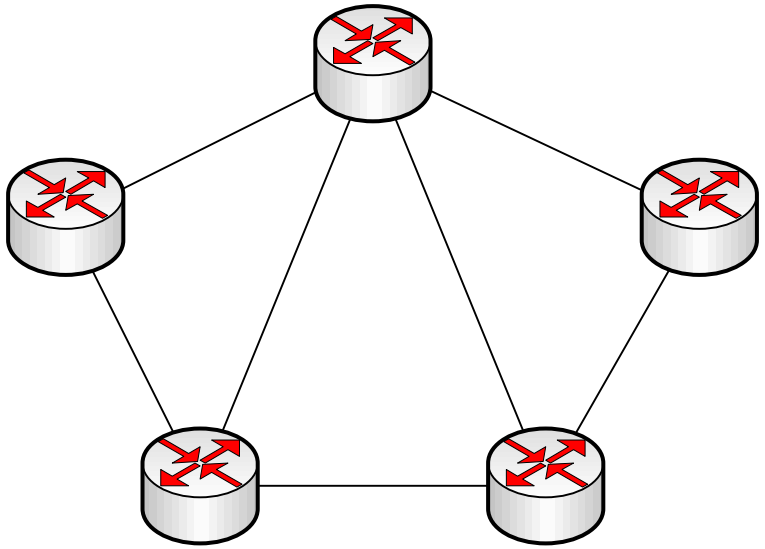
Mesh

Full Mesh

- Every device is connected to every other device
- Expensive
- Hard to maintain

Partial Mesh

- Enough interconnections to eliminate single points of failure



Summary of Topologies

Type	Characteristics	Problems
Bus	Linear, single cable for all computers attached; traffic travels the full cable and is received by all computers	If one station has a problem, it affects all other computers on the same cable
Ring	All computers are connected by a unidirectional transmission link, and the cable is in a closed loop	If one station experiences a problem, it can negatively affect all other computers on the same ring
Star	All computers are connected to a central device, which provides more resilience for the network	The central device is single point of failure
Tree	This is a bus topology that does not have one linear cable, but branches of cables	
Mesh	Computers are connected to each other, which provides redundancy	This requires more expense in cabling and effort to track down cable faults

Network Wiring

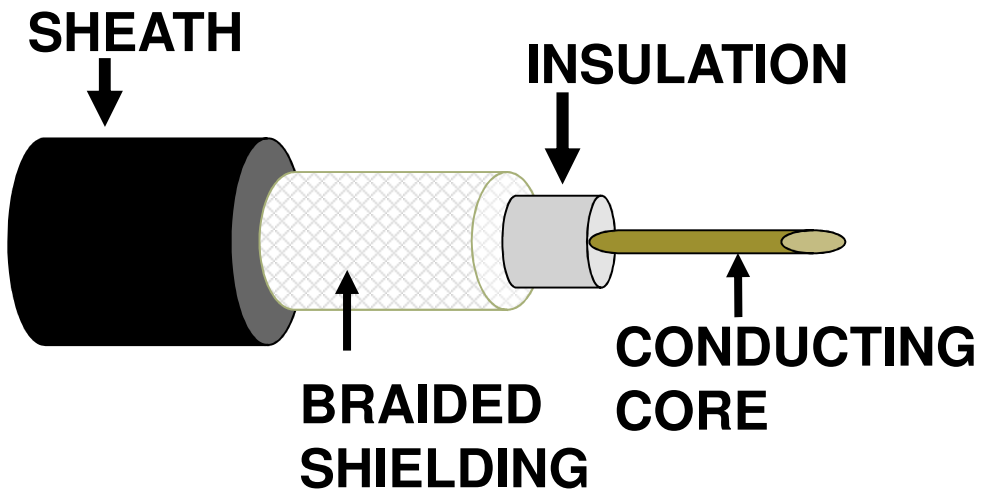
Cabling

- Different types for specific data link layer technologies
- Different for speeds and functionality
- Different levels of security and protection
- Cabling issues can cause different network issues
- Number one networking disruption is cabling problems

Coaxial Cable

Coaxial Characteristics

- Copper wire surrounded by shielding
- Hollow cylindrical conductor surrounded by inner wire conductor



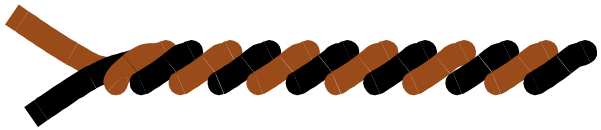
Coaxial Cable

Coaxial Characteristics

- More expensive than twisted pair
- More resistant to EMI
- Can transmit greater bandwidth and distance than twisted pair
- Now, usually only used in broadband communication
  - Thinnet segments are limited to 185 meters
    - Also called 10Base-2 or RG-58
  - Thicknet segments are limited to 500 meters
    - Also called 10Base-5, RG-8, or RG-11
  - Broadband Coax
    - RG6 should be used exclusively for satellite hookups and digital CATV. RG59 is fine for analog CATV signals but will not support the higher bandwidth used for satellite signals.

Twisted-Pair

- **Low-speed transmission medium using twisted copper wires**
  - Shielded Twisted-pair (STP)
    - Extra outer foil shielding
  - Unshielded Twisted-pair (UTP)
  - UTP is more vulnerable to interference, cross-talk, and eavesdropping



  - UTP least secure compared to STP and fiber

Coaxial and Twisted-Pair Usage

Coaxial Cabling

- Higher performance than twisted-pair and used in radio frequency type communications
- Used for cable television
- Used primarily in one-way networks

Twisted-Pair Cabling

- Most commonly used LAN media
- Cheap and easy to work with
- Used extensively in residential telephone systems

CAT Ratings

UTP Category	Characteristics	Usage
Cat 1	Voice-grade telephone cable	Not recommended for network use, ok for modems
Cat 2	Data transmission up to 4 Mbps	Used for mainframe and minicomputer terminals, not for fast networks
Cat 3	10 Mbps Ethernet or 4 Mbps Token Ring	Used in 10Base-T installations
Cat 4	16 Mbps	Used in Token Ring
Cat 5	100 MB for 100Base-TX and CDDI, high number of twists per foot for less crosstalk	Used in 100Base-TX, CDDI and ATM Widely used for new network installs
Cat 6	155 Mbps	Used in new network installations requiring hi-speed transmission
Cat 7	1 Gbps	Used in new network installs for hi-speeds

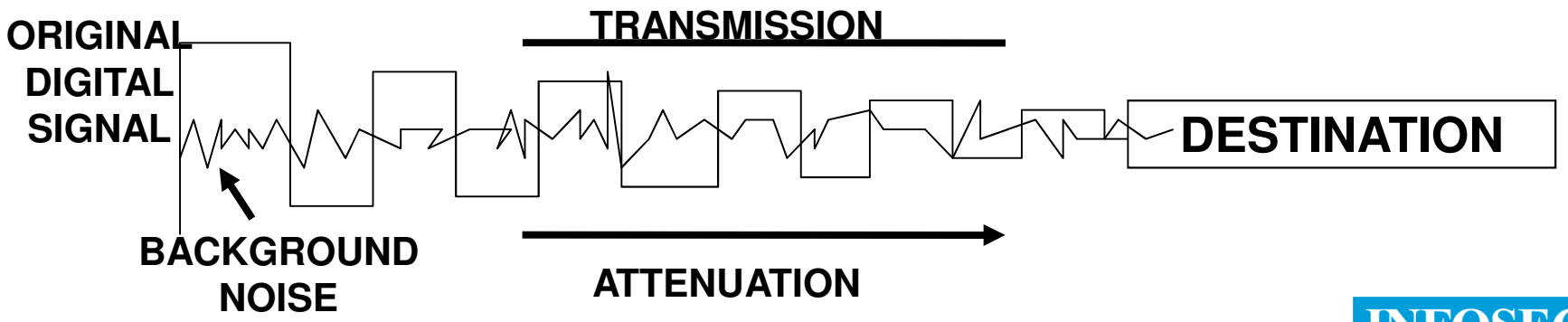
Fiber

Fiber Characteristics

- Data travels as light over a glass medium
- Higher speed and less attenuation
- Extremely resistant to eavesdropping
- Very expensive
- Hard to work when compared to other type of cabling
- Most secure cabling type

Cable Issues

- **Noise**
  - Dirty signals
- **Attenuation**
  - Loss of signal strength as the data travels
- **Cross Talk**
  - One signal spills over to a neighboring wire
  - UTP most susceptible



Fire Rating

Cable Fire Issues

- Certain chemicals give off toxic fumes when they burn
- In some areas, a fire may not be noticed right away
  - Need to use plenum cable types that do not release dangerous chemicals
  - Jacket covering of fluoropolymers instead of polyvinyl chloride (PVC)

Cable Review

Coaxial:

- Thicknet: RG-8 500 M vampire taps, AUI 50-ohm terminator
- Thinnet: RG-58 185 M BNC, T-connectors, Barrel Connectors 50-ohm terminator
- Broadband Cable RG-59 75 Ohm
- Broadband Cable RG-6 75 Ohm

Cable Review (cont.)

- **Twisted Pair**
  - UTP (Unshielded) 100 M RJ-45
  - STP (shielded) 100 M RJ-45

  Cat 3 10 Mbps 2 pair of wires

  Cat 5 100 4 pairs

  Cat 5e/6 1000

  Cat 7 10 Gbps
- **Fiber Optic: ST (twist), SC (clip)**
  - Single mode : 2000 M
  - Multi mode: 500 M

Transmission Methods

Unicast

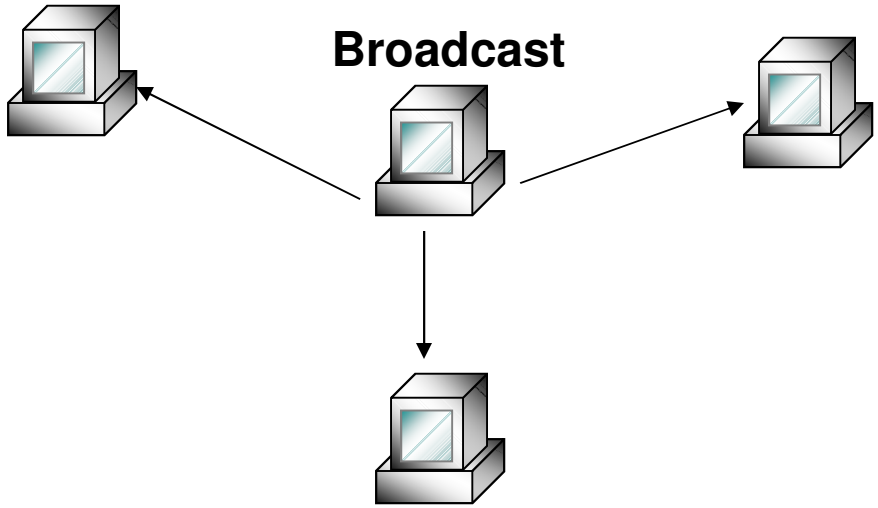
- One to one relationship

Multicast

- One to many relationship

Broadcast

- One to all relationship
- Ethernet broadcasts on its shared medium
- Usually just on a network segment



Agenda

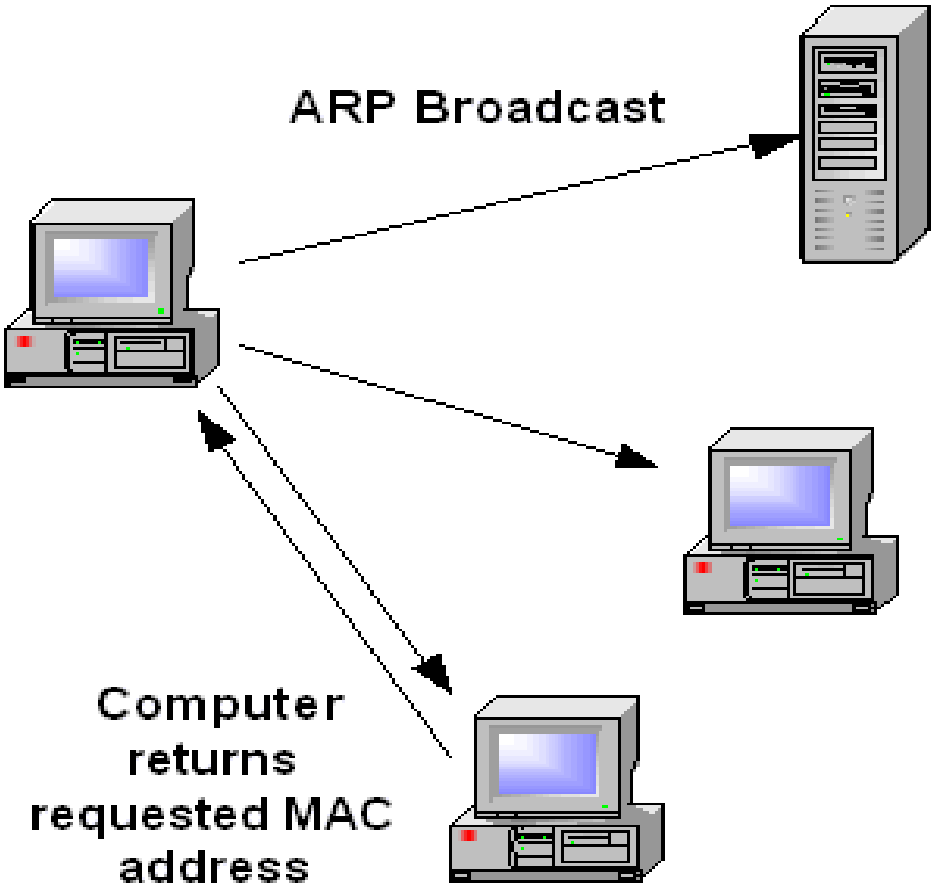
- OSI Model, the TCP/IP suite, and other Protocols
- Signaling and Cabling
- Network Types and LAN Access Technologies
- Firewalls, Bastion Hosts, and Firewall Architecture
- Dial-up, Remote Access, Tunneling, and VPN Protocols
- MAN and WAN Technologies, VoIP, and PBX
- Wireless Networking and Network Attacks

LAN Protocols

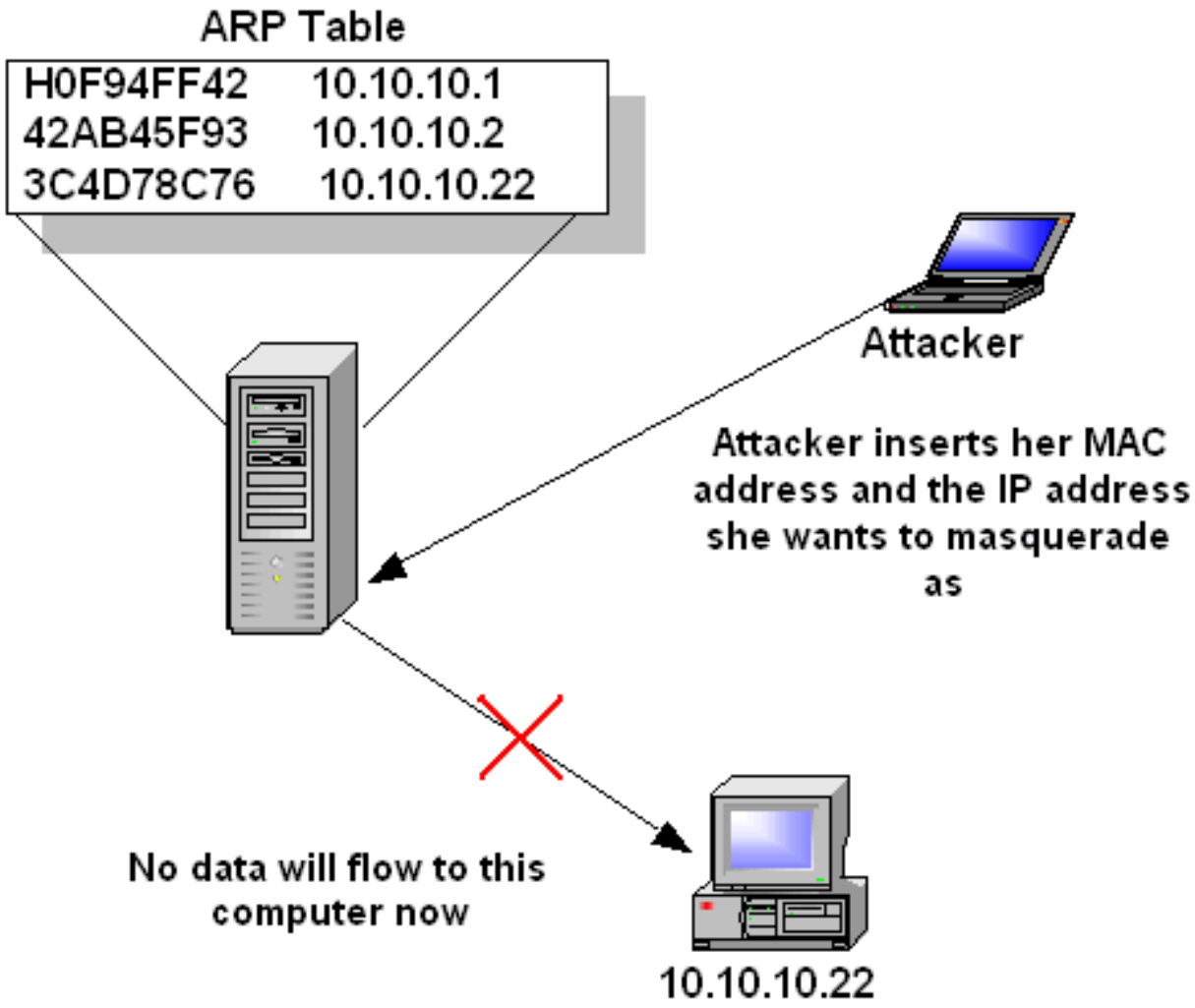
ARP

- Maps the IP address to the media access control (MAC) address
- MAC is only used to forward frames on same network segment, not for routing
- LAN media access technologies only understand MAC addresses, not IP addresses
  - IP address is a 32-bit software assigned value
  - MAC address is a 48-bit value hard-coded into an NIC

LAN Protocols ARP Broadcast



ARP Poisoning



Reverse Address Resolution Protocol

RARP

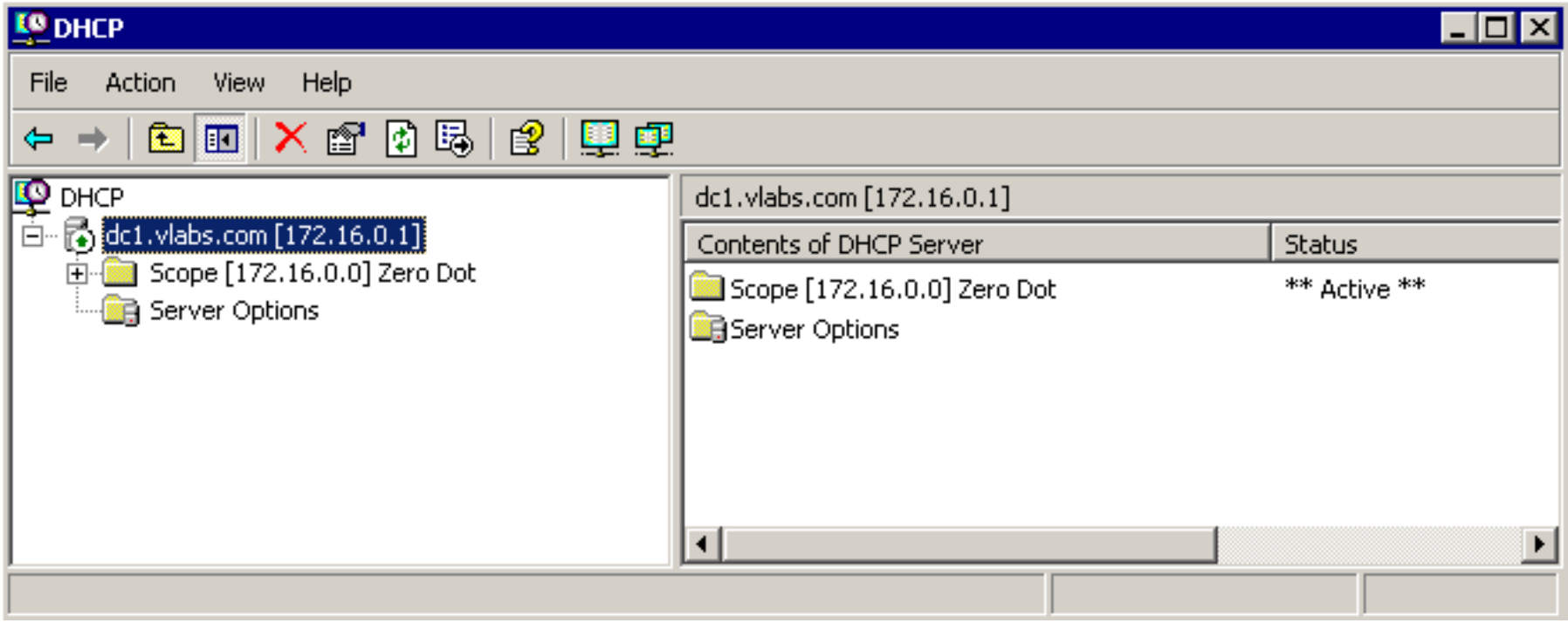
- RARP has the MAC address and broadcasts to find its IP address
  - ARP knows the IP address and broadcasts to find the MAC address
- RARP server responds to RARP broadcast
- Usually used in dumb terminal situations
- BOOTP was created after RARP and contains more functionality
  - Gives stations IP, gateway IP, and name server IP

DHCP Overview

- **Dynamic Host Configuration Protocol (DHCP)**
  - Automates IP configuration
  - Create scopes to manage
  - Options added to scope to set additional TCP/IP Parameters
  - Support for Superscopes and Multicast scopes
  - Integration with DNS

DHCP Overview (cont.)

- **Dynamic Host Configuration Protocol (DHCP)**

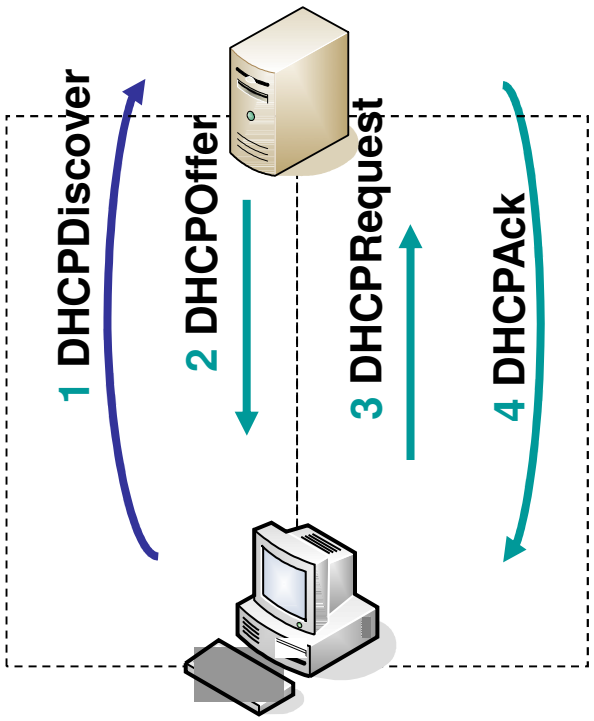


DHCP Leasing Process

DHCP Leasing Process

- Client Boots and broadcasts DHCPDiscover message
- Server(s) responds and returns a DHCPOffer message
- The client chooses the first DHCPOffer it receives and then sends a DHCPRequest accepting information from that server.
- Server sends a DHCPack
- The DHCP Renewal Process
- Client requests from original server at 50% lease time
- If no response, sends request to any server at 87.5% lease time

DHCP Leasing Process (cont.)



DHCPDiscover

DHCPOffer

DHCPRequest

DHCPAck

Internet Control Message Protocol

ICMP

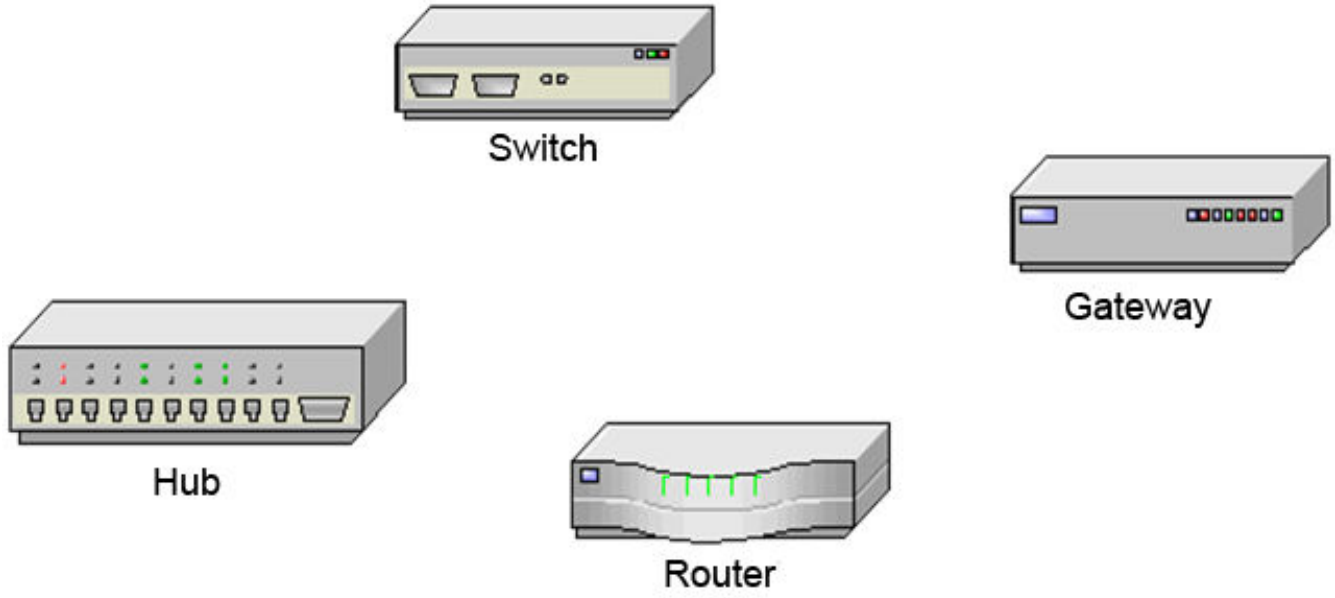
- Message protocol for IP
- IP sends ICMP messages, thus uses IP as its transport mechanism
- Status and error messages
  - Network congestion, downed link, sending failure
- Ping utility uses this protocol
  - ICMP ECHO Request and Reply
- Routers put ICMP messages into IP datagrams to indicate a message could not be delivered, or another problem occurred
- Can be used to trick routers into changing their tables, redirecting traffic

Other TCP/IP Protocols and Ports

- SNMP 161-162
- SMTP 25
- POP3 110
- SSH 22
- DNS 53
- TFTP 69
- FTP 20-21
- Telnet 23
- BootP 67-68
- HTTP 80
- HTTPS 443

Networking Devices **

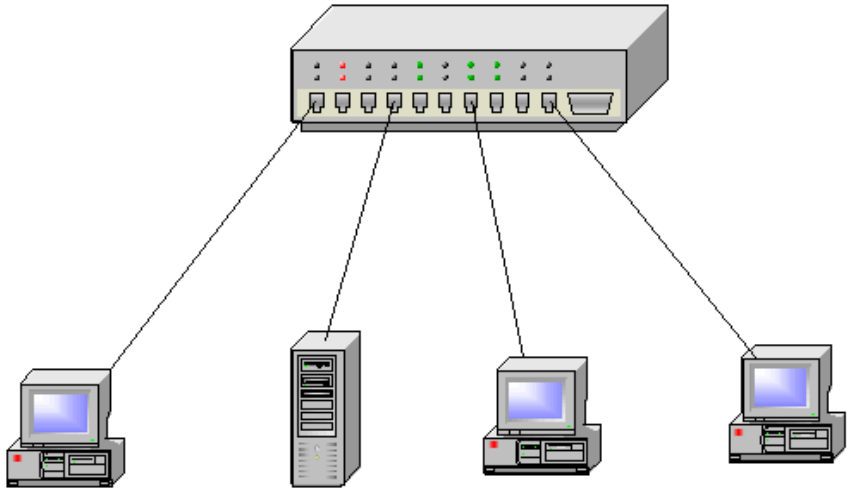
- There are several types of devices used in LANs, MANs, and WANs to allow for intercommunication between computers and networks
- The differences of these devices pertain to their functionality, capabilities, intelligence, and network placement:
  - Hub
  - Switch
  - Router
  - Gateway



Hub

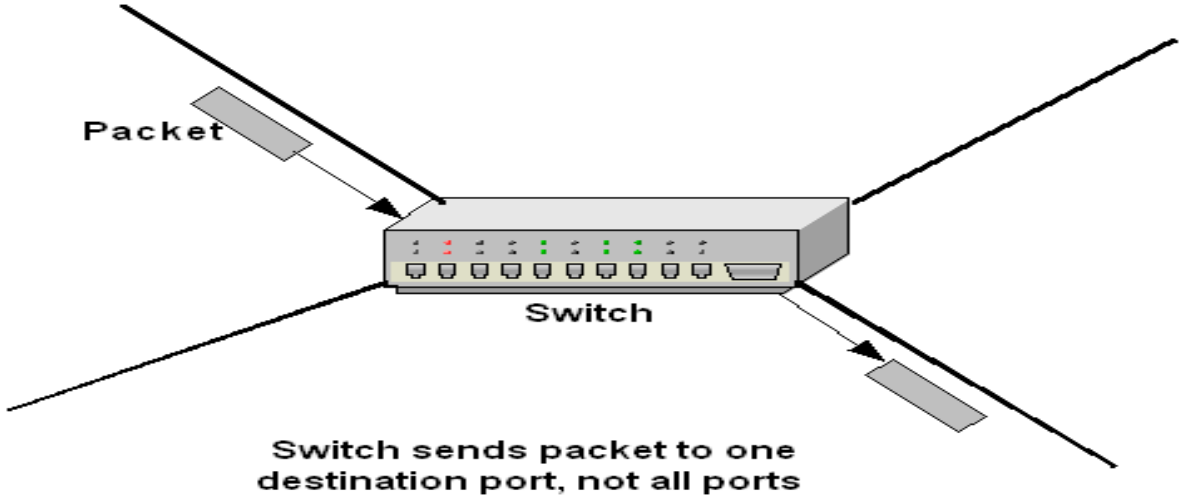
Hub Characteristics

- Used to connect multiple LAN devices



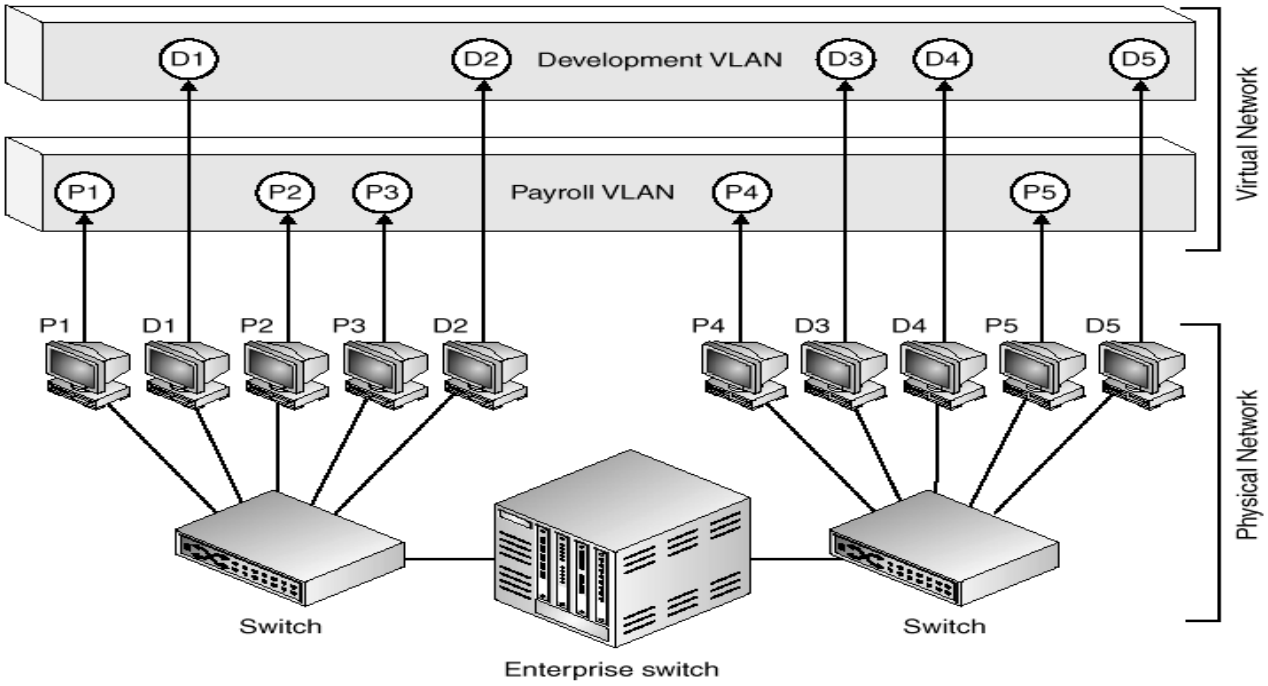
Switch

- Similar to a bridge, but when it receives a frame, it forwards it on to the correct network segment instead of all network segments
- Mainly a Data Link layer device, although some work at the Network layer and have more intelligence
- Subject to MAC Flooding



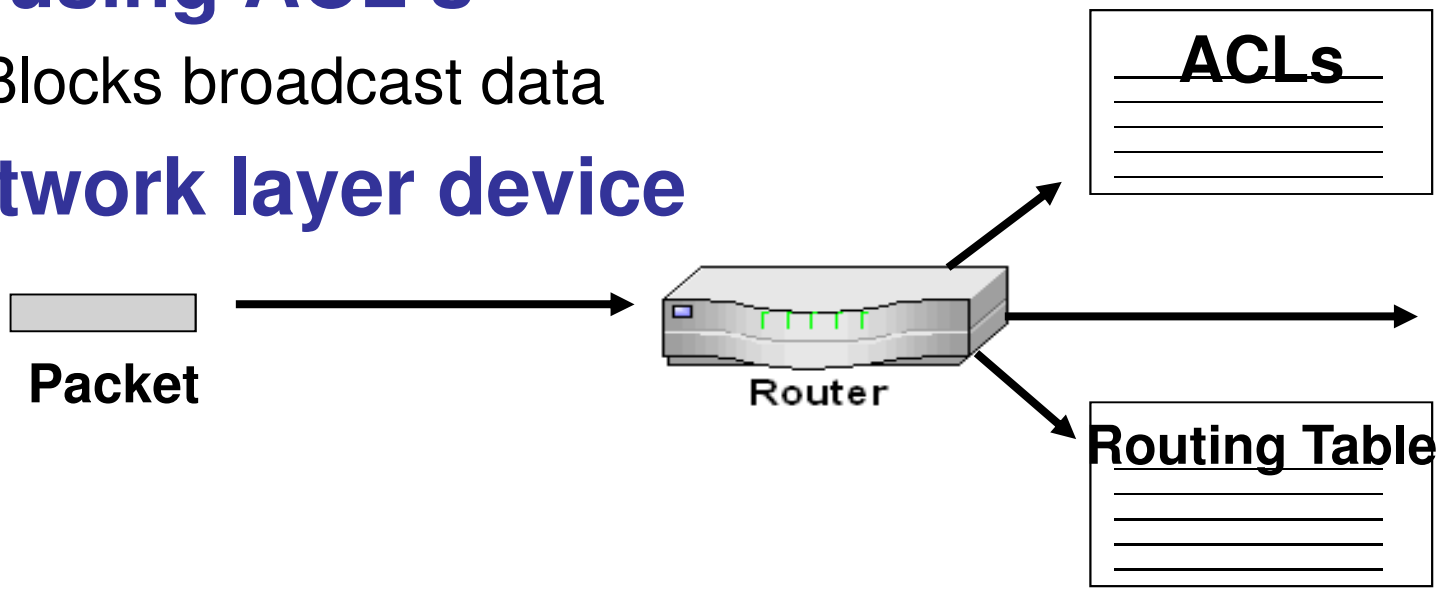
Virtual LAN

- Logically separating users, groups, and resources based on business and security requirements instead of physical location
- Deployed on switched networks



Router

- Routes packets based on IP addresses in headers
- Can connect similar or different networks
- Implements security through packet filtering by using ACL's
  - Blocks broadcast data
- Network layer device



Routing Protocols

- Types
- Protocol definitions
- Weaknesses

Routing Protocol Types

- **Routing protocols can be divided into two broad categories:**
  - Algorithms based on distance vector protocols
  - Algorithms based on link state protocols
  - Border Protocols
- **Routing protocols can be used for:**
  - Interior routing—RIP, OSPF
  - Exterior routing—BGP

Distance Vector Protocols (RIP/RIP v2)

- List of destination networks with direction and distance in hops
- Routing by Rumor
- Each Router periodically sends its entire routing table to its neighbors
- Should not update its table from unauthorized routers devices
- Noisy, not the most efficient
- Infinity = 16 to prevent routing loops (small network usage only)

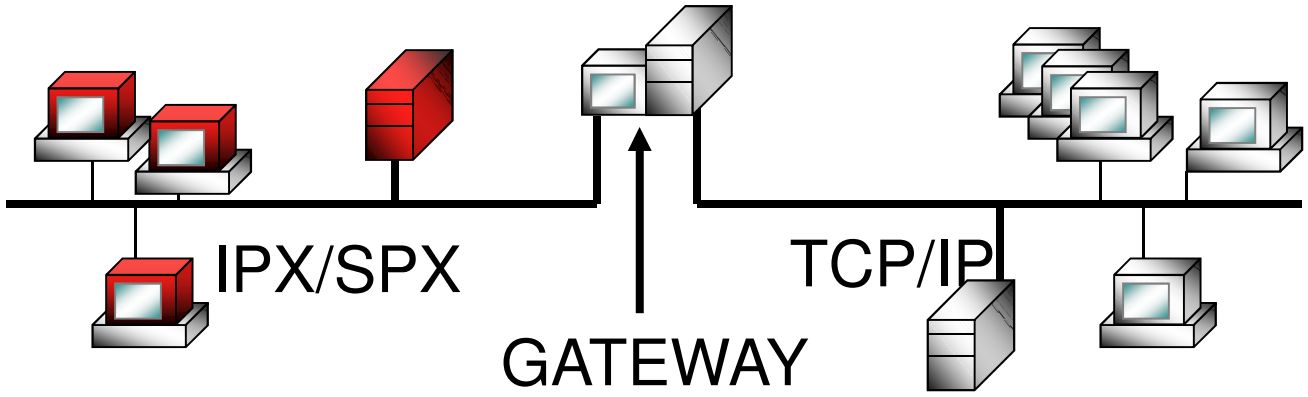
Link State Protocols OSPF

Link-state routing

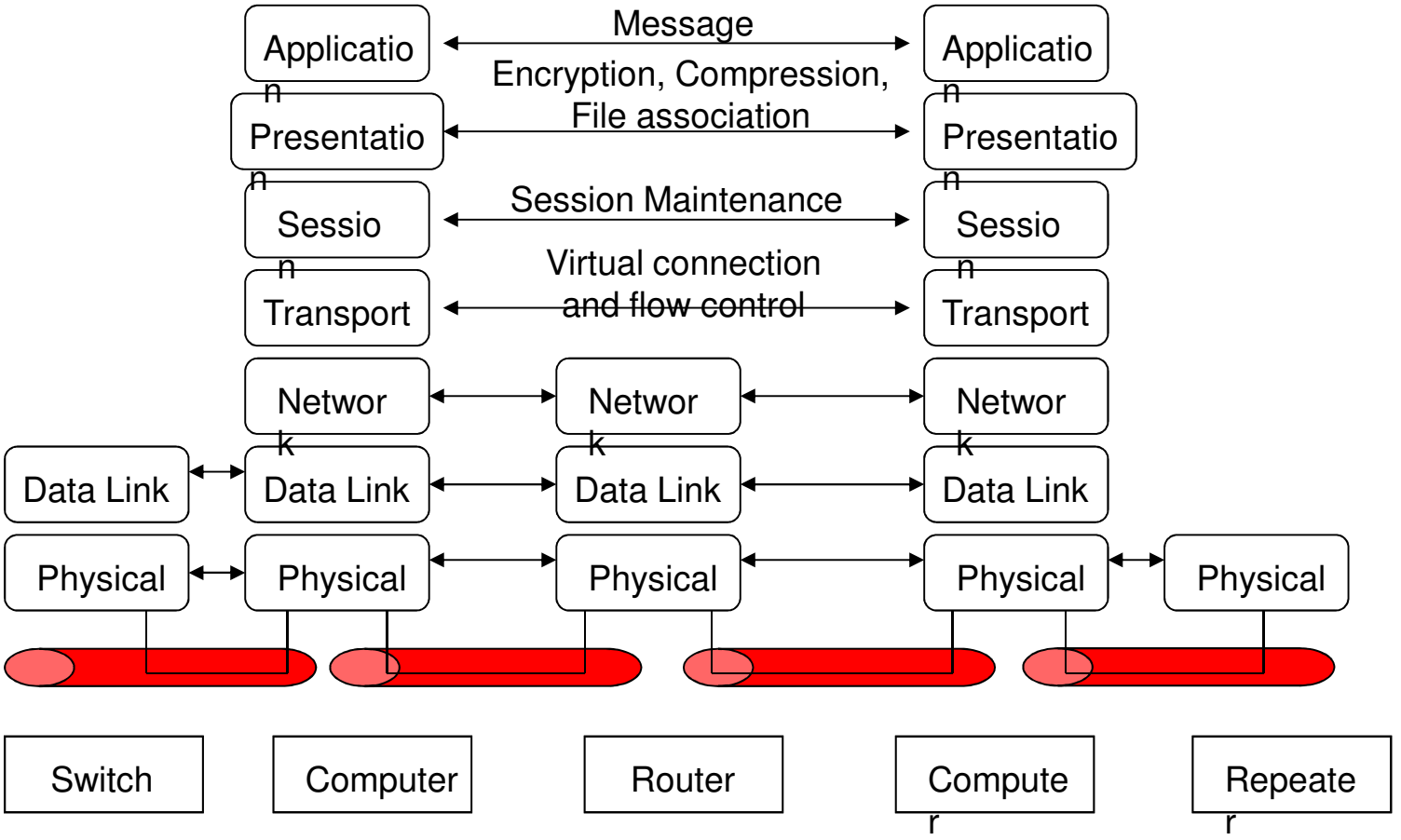
- Each router keeps a topology map of network and identifies all routers and sub-networks
- Route is determined from shortest path (speed) to destination
- Routers elect DR (designated router) within an “area”
- All routers establish their topology database using DR as gateway between areas
- LSA or Link State Advertisements are used to communicate between devices to ensure the topology has not changed
- These protocols can be very resource intensive

Gateway

- Usually software that links two different networks
- **Not to be confused with a “default gateway” which is most often used to describe a router.
- Gateway acts as a translator between different protocols and/or applications
  - It may be used to connect an IPX network to an IP network or connect two different mail servers



Review of Activity at Different Layers



Summary of Devices

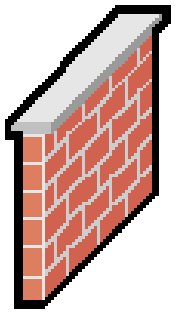
Device	OSI Layer	Functionality
Router	**Network Layer**	**Separates and connects LANs, creating internetworks; routers filter based on IP addresses**
Hub	**Physical Layer**	**Connects multiple to a single bus; performs repeater function**
Switch	**Data Link Layer – More intelligent switches work at the network layer**	**Provides a private virtual link between communicating devices, allows for VLANs, reduces traffic, and impedes network sniffing**
Gateway	**Application Layer (although different types of gateways can work at other layers)**	**Connects different types of networks, performs protocol and format translations**

Agenda

- OSI Model, the TCP/IP suite, and other Protocols
- Signaling and Cabling
- Network Types and LAN Access Technologies
- Firewalls, Bastion Hosts, and Firewall Architecture
- Dial-up, Remote Access, Tunneling, and VPN Protocols
- MAN and WAN Technologies, VoIP, and PBX
- Wireless Networking and Network Attacks

Firewalls **

- A firewall is a combination of software and hardware that supports and enforces the company's network security policy
- Firewalls are used to restrict access to network from another network
  - It is an access control mechanism

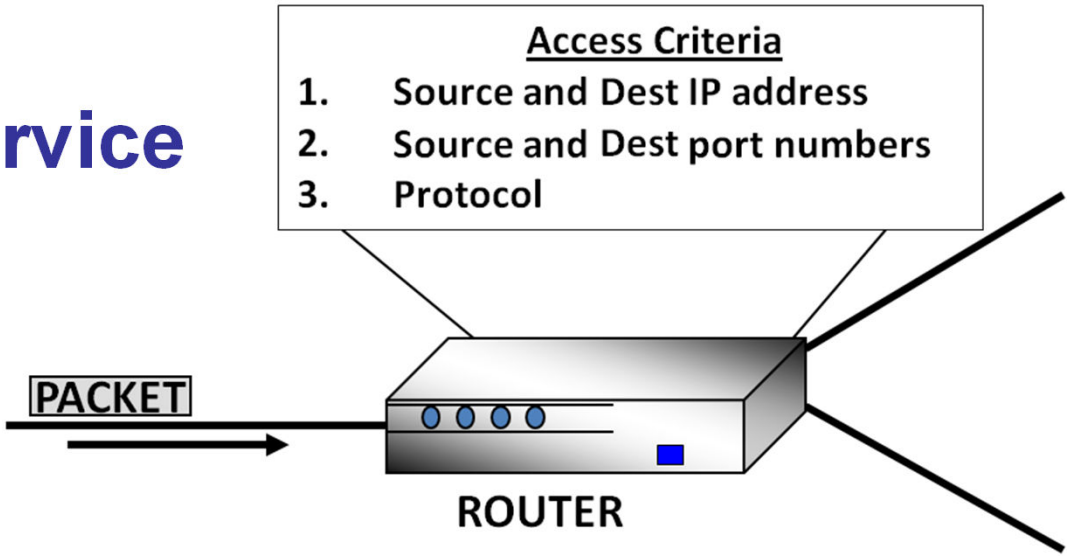


Firewall

- The five types are Static Packet Filtering, Stateful Packet Filtering, Circuit Proxy, Application Proxy, and Kernel Proxy

Packet Filtering

- Uses access control lists to make access decisions
- Access is based on source and destination IP addresses and port numbers
- Network layer service

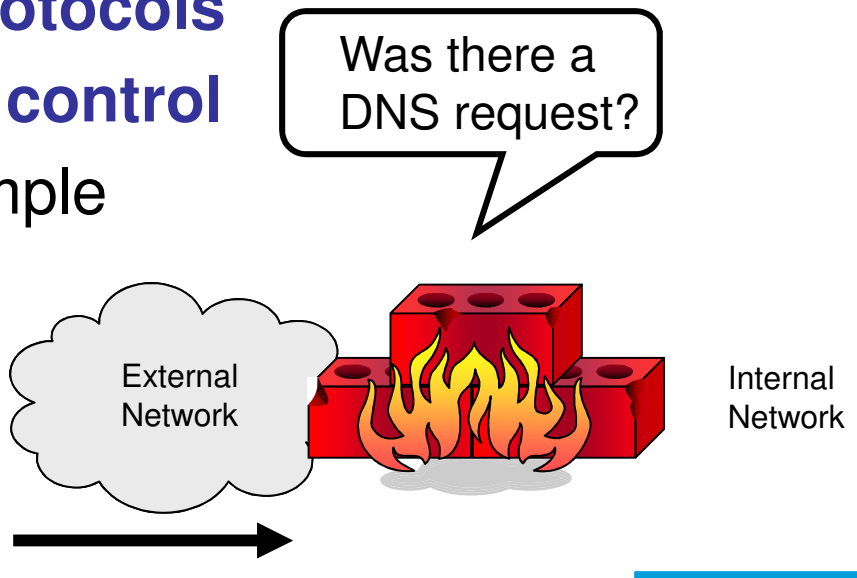


Static Packet Filter Firewall

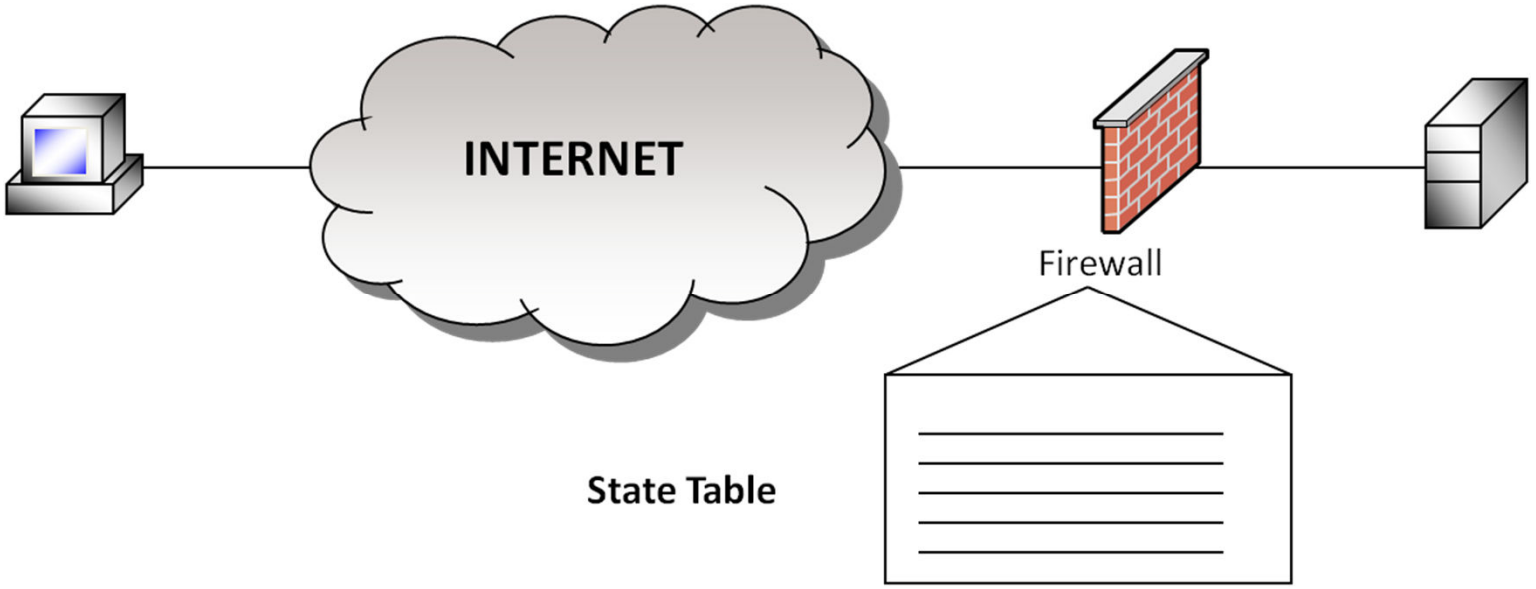
- Simplest and least expensive method to stop messages based on addresses, ports, and protocol type
- Minimum security for low-risk environments
- Screening routers with rules for rejecting or accepting data
- Cannot keep “state” information

Stateful Firewalls**

- Packets are captured by inspection engine and each OSI layer of the packet is inspected
- Keeps track of the "state" or dialog process of a communication stream
- Builds a state table to monitor each communication dialog
- Can track connectionless protocols
- Can enforce context access control
  - TCP Handshake is an example



Stateful Firewalls



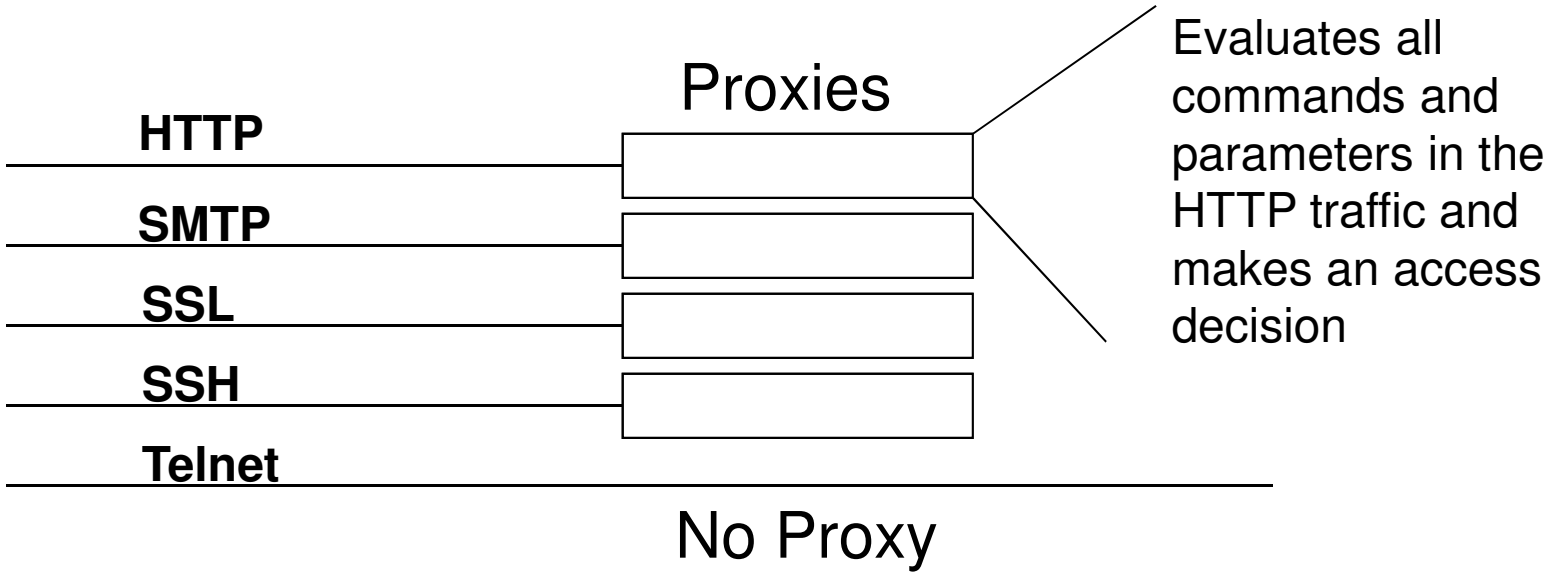
Proxy Firewalls

- **Circuit Level and Application Gateways**
- **Middle man between communicating computers**
  - Makes a copy of each packet and transfers it from one network to another
  - No direct connection between the inside and outside
- **Masks source computer because it copies the packet and inserts its own address**
- **High processing on each packet means lower performance**

Application-level Proxy Firewall

- **Looks deeper into packet for access decisions**
  - All the way to the application layer
- **Understands the command structure of a protocol**
- **Provides more granular control in access**
- **If no proxy for a specific protocol, must use a generic proxy or "punch a hole" in the firewall**

Application-level Proxy Firewall



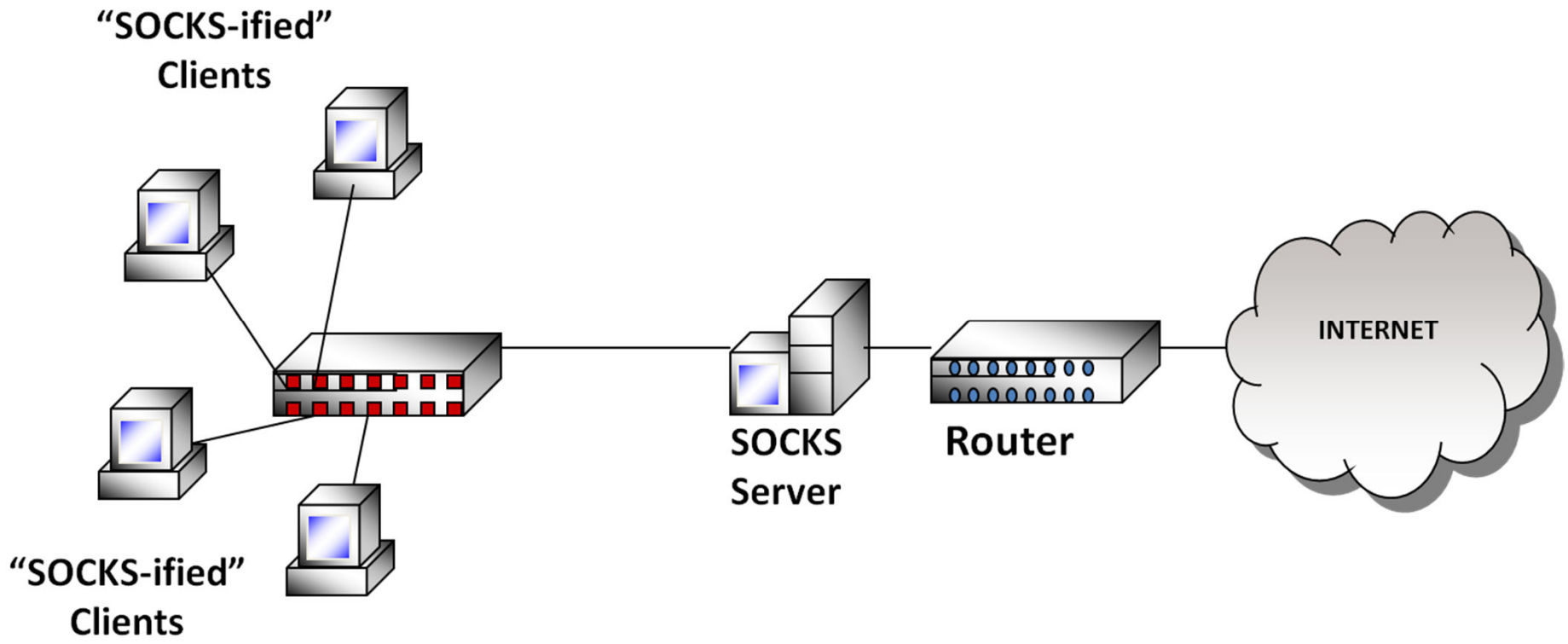
Circuit-level Firewall

- Does not look as deep into the packet as application-level proxy
- Provides protection for a wide variety of protocols and is easier to maintain than an application-based proxy firewall
- Makes access decision based on source and destination address, port, and protocol
- Similar functionality as a packet filter, but breaks connection
  - One example is SOCKS

SOCKS

- Circuit-level Proxy Server
- Requires clients to be SOCKS-ified with SOCKS client software
- Mainly used for outbound Internet access and VPN functionality
- Provides authentication and encryption features similar to other VPN protocols, but not considered a traditional VPN protocol

SOCKS


"SOCKS-ified"
Clients
"SOCKS-ified"
Clients
SOCKS
Server
Router
INTERNET

5. Kernel Proxy

- **Kernel proxies (Most advanced type of firewall):**
  - Build a virtual stack to examine each packet at each layer to ensure their integrity
  - Faster than regular application proxy, as the processing takes place in the kernel and does not have to be passed up to a higher software layer in the operating system
  - Also performs network address translation

Summary of Firewalls

Firewall Type	OSI Layer	Characteristics
Static Packet Filtering	Network Layer	• Routers using ACLs dictate acceptable access to a network • Looks at destination and source addresses, ports, and services requested
Stateful Packet Filtering	Can operate at all layers of OSI but is most commonly thought of as a layer 5 (session)	• Keeps track of each conversation using a state table • Looks at state and context of packets
Circuit-level Proxy	Session Layer	• Looks at header of packet only • Protects wider range of protocols and services than *app-level proxy*, but not as detailed a level of control
Application-level Proxy	Application layer	• Looks deep into packets and makes granular access control decisions • Requires one proxy per service
Kernel Firewall	Application Layer	•One network stack is created for each packet

Bastion Host

- Also known as a Hardened System or a Locked Down System
- Disable unnecessary services and subsystems, no file sharing, limited amount of open ports, and no unnecessary software or utilities
- Any computer that is in a non-trusted network segment, as in the DMZ, should be a bastion host
  - Firewall software should be installed on a bastion host

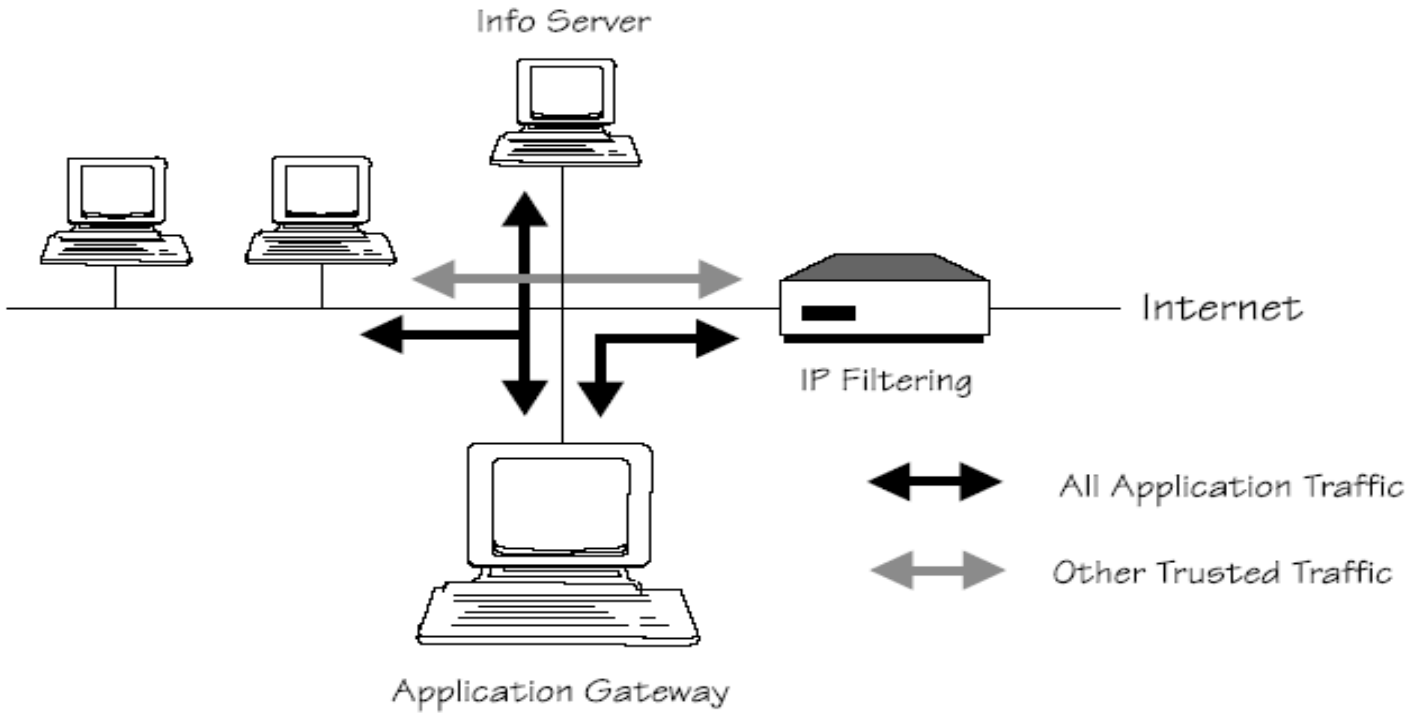
Firewall Placement

- **Protect an internal network from an external network and act as a "choke point" for all traffic**
- **Segment network sections and enforce access controls between different subnets**
- **Construct a DMZ to provide a buffer zone between the internal network and the external network**
- **Firewall architectures documented by NIST:**
  - Screened host
  - Dual-homed firewall
  - Screened subnet

Screened Host

Screened Host Definition

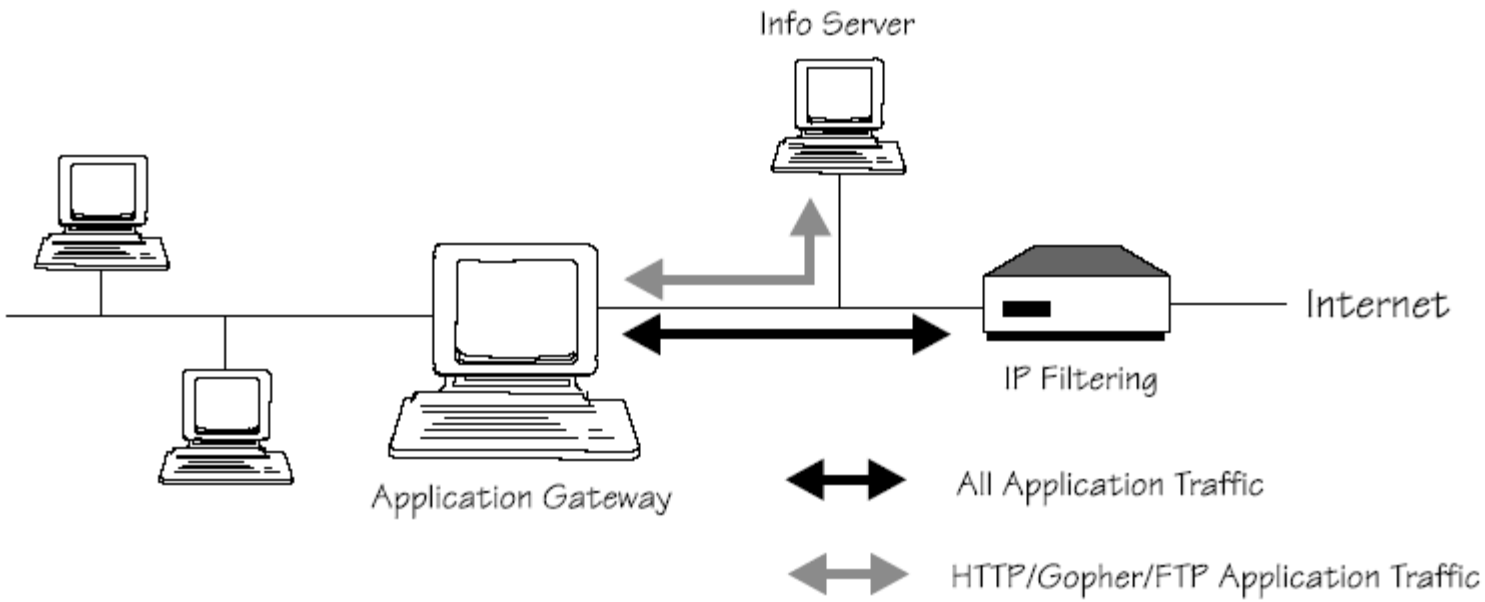
- Proxy directly behind a packet-filtering router
- Separates trusted and non-trusted networks



Dual-Homed Firewall

Dual-Homed Firewall Description

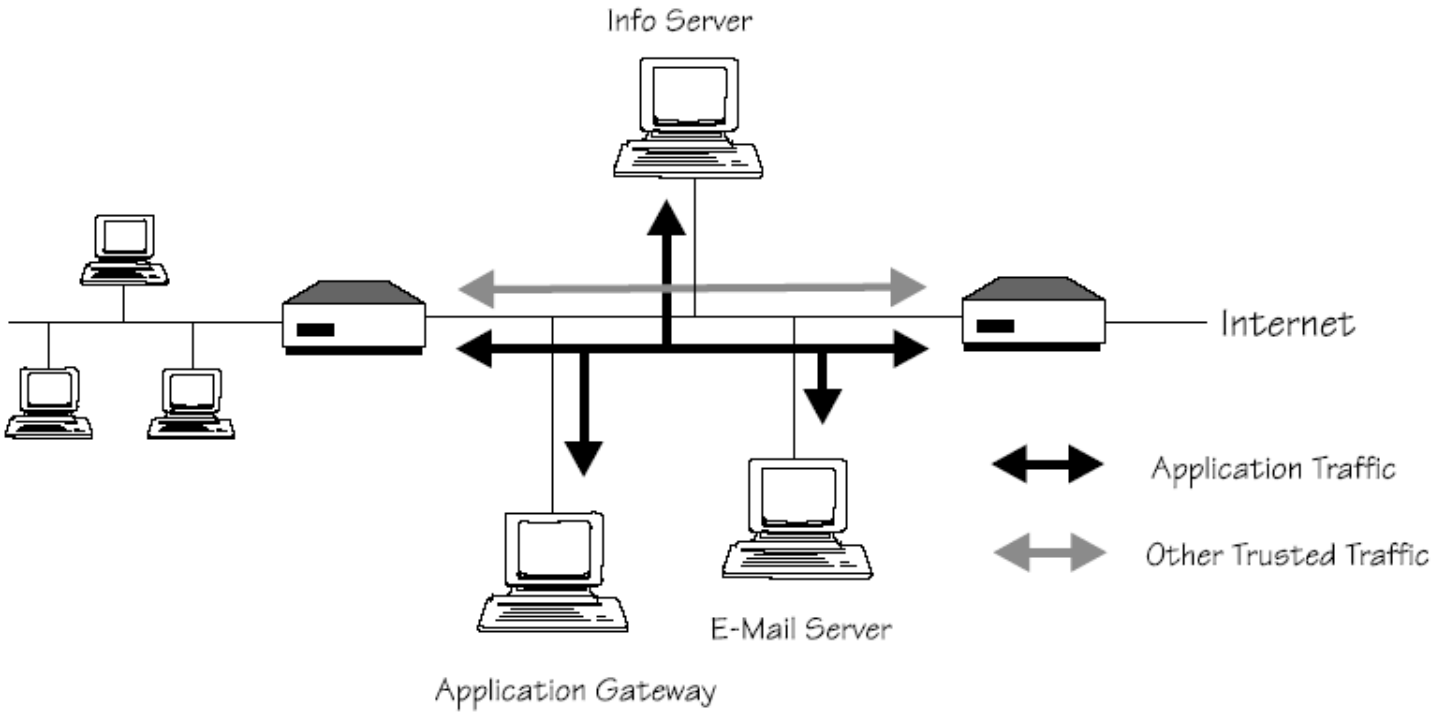
- Two interfaces, one for each network
- Forwarding and routing is turned off so the packets can be inspected



Screened Subnet

Screened Subnet Definition

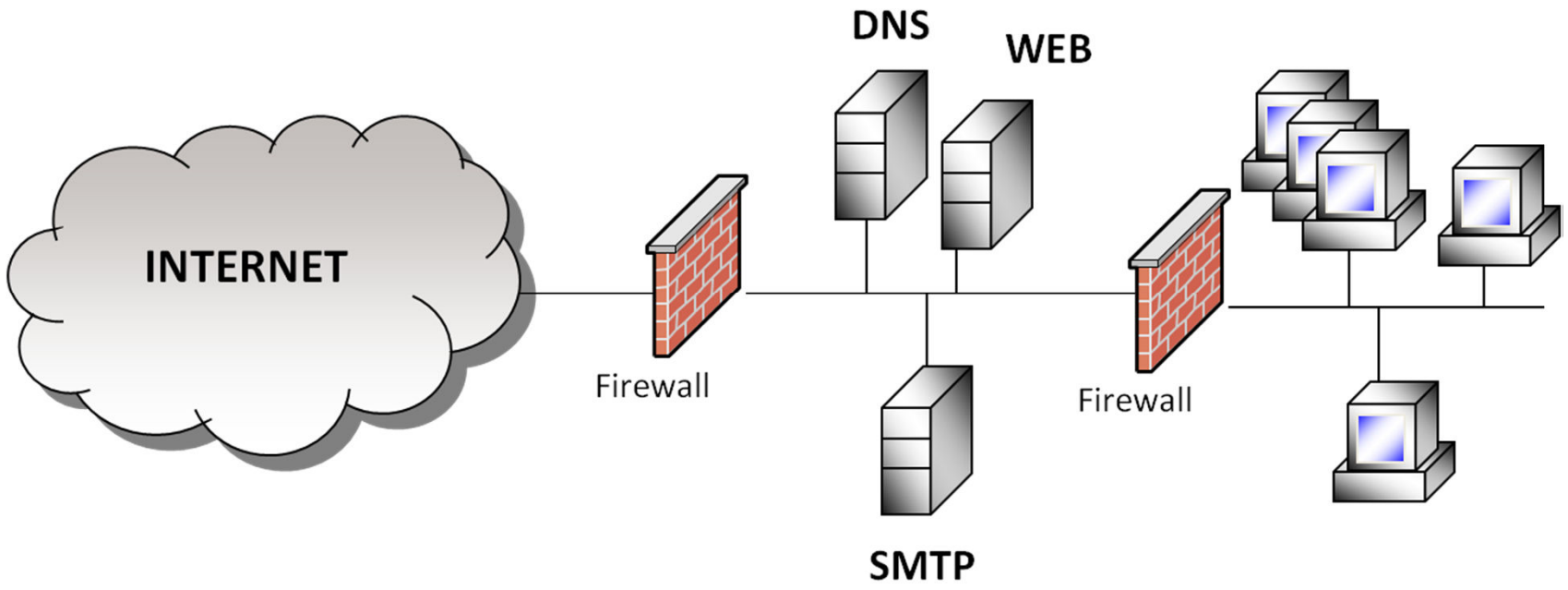
- A DMZ is created by implementing two screening routers
- Optionally can include a proxy



Demilitarized Zone

- Network segment that is between the protected internal network and the external non-trusted network
- Creates a buffer zone between the internal and external network
- Bastion hosts are put in the DMZ
- One router or firewall should connect the trusted network to the DMZ
- One entry path

Demilitarized Zone



Firewall Architecture Summary

ARCHITECTURE TYPE	CHARACTERISTICS
Dual-Homed	Single computer with 2 NICs, one connected to the trusted internal network and one connected to the untrusted external network
Screened Host	Router filters (screens) traffic before it is passed to the firewall
Screened Subnet	External router filters traffic before it enters the DMZ; traffic heads towards the internal network, then goes through a firewall and another router

Firewalls Should

- Should deny all traffic unless expressly permitted (white-listing)
- Should block directed broadcasts (defense against smurf and fraggle attacks)
- Block traffic leaving the network from a non-internal address (indicates the network is possibly being used as zombie systems in a possible DDoS attack

Firewalls Should (cont.)

- Block all traffic entering the network from an internal address (indicates a potential spoofing attack)
- If security is the top priority then packets should be reassembled before forwarding (Slow).

Downfalls of Firewalls

- **Security is concentrated in one spot**
  - A distributed approach that secures many different places within the network
- **Firewalls present a potential bottleneck to the flow of traffic**
- **Firewalls restrict desirable services that users may want to use**
  - This is a disadvantage to the users, but an advantage to the security professional

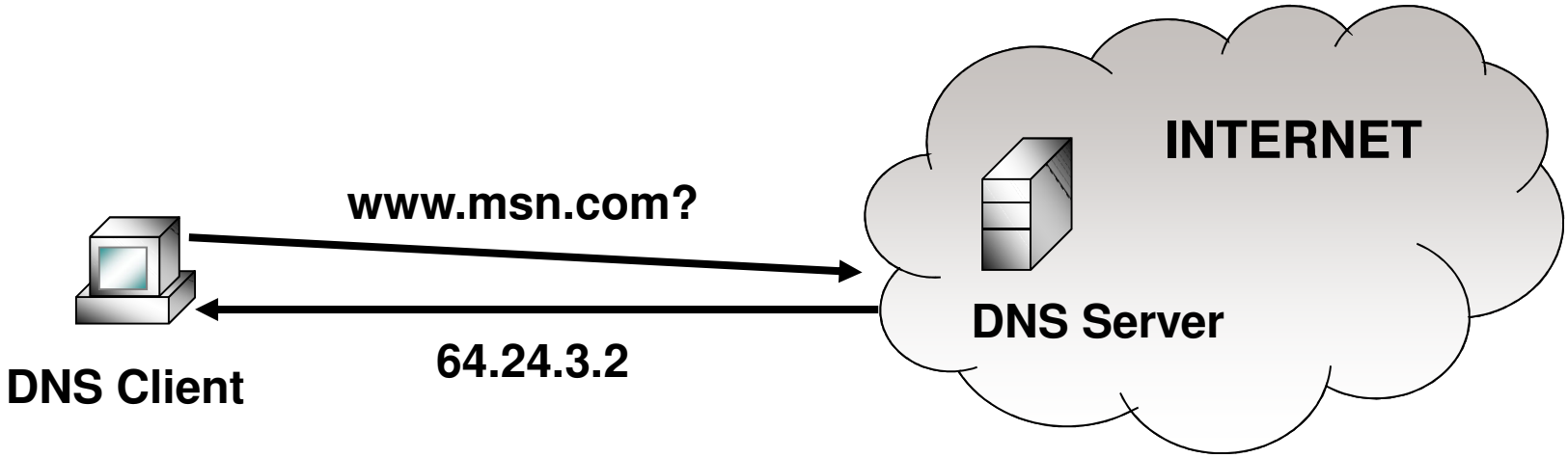
Downfalls of Firewalls (cont.)

- Most firewalls do not protect from viruses in e-mail
- Firewalls provide little protection against the inside attacker

Domain Name Service

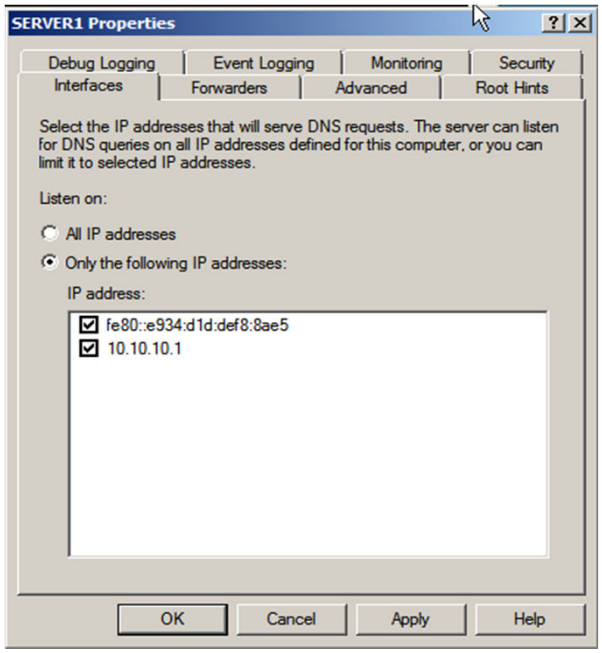
DNS

- Network service that translates host names to IP addresses
- Hosts names are divided into zones
- DNS server that holds resource records for a zone is the authoritative DNS server for that zone



Securing DNS

- **Enable DNSSec**
- **Place a DNS server on the external and internal networks**
  - Provides name resolution for the internal network separate from public network
- **Limit DNS Interface Access**
  - If DNS is multi-homed, indicate in properties of server the interface to listen for name requests



Securing DNS

Secure zone transfers

- Select to transfer to only name servers listed or specific IP addresses

Secure cache from pollution

- Protects from attackers adding entries to cache
- Use Secure Dynamic Updates
- Split DNS should be used to provide internal and external name resolution

Directory Services

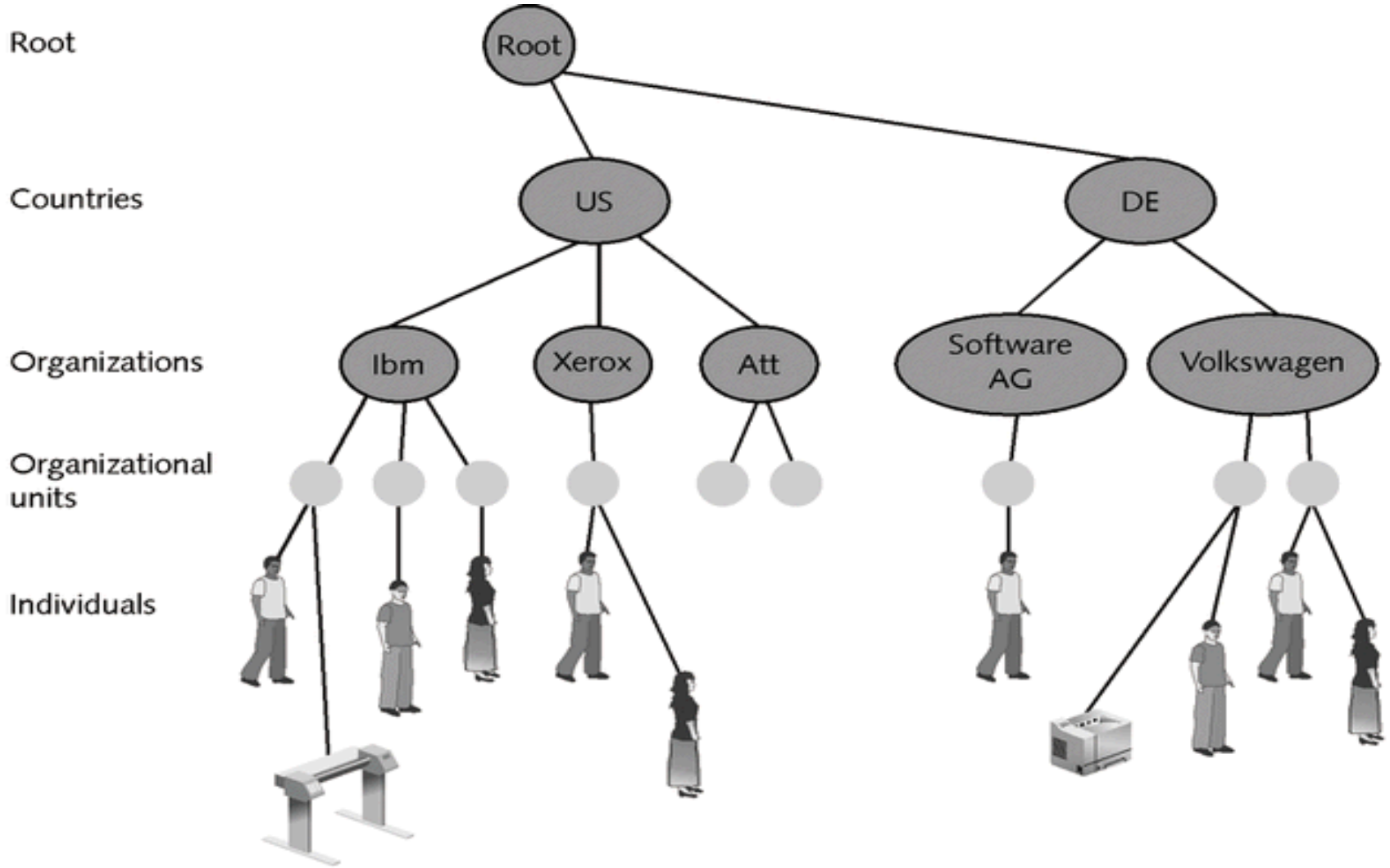
- ISO published X.500 – LDAP adapts the directory to work over TCP/IP
- Hierarchical database is an inverted tree structure
- Allows delegation of naming while maintaining (potentially) global uniqueness

Directory Service – LDAP

- **The full name of a "leaf" on the tree, the Distinguished Name (DN), must be unique, and specified the path from the root of the tree to the "leaf"**

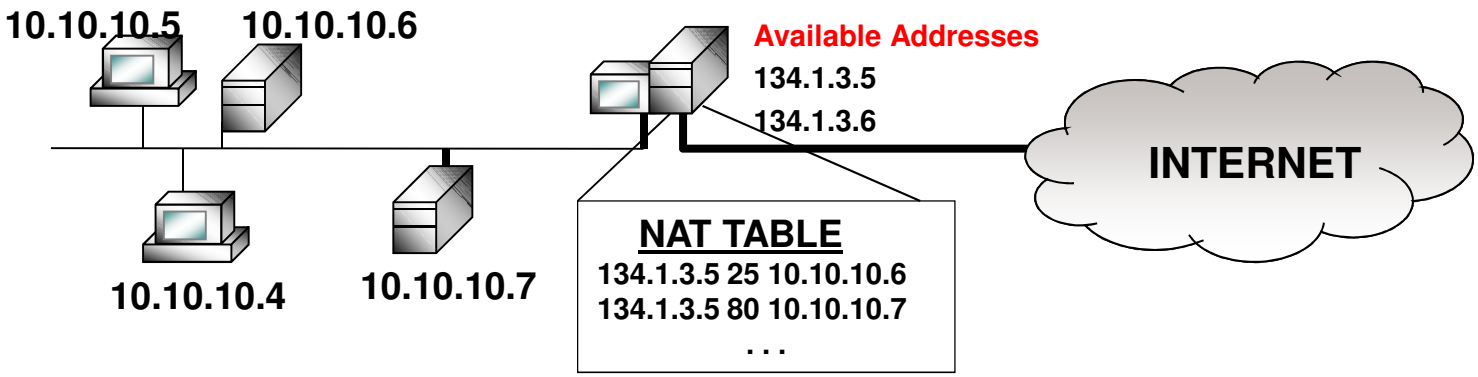
- **If the "leaf is a user, we can store all sorts of things about this user:**
  - Name
  - Location
  - Phone numbers
  - E-mail addresses
  - Digital certificates
  - Application or data access

Directory Tree



Network Address Translation

- Network Address Translation (NAT) allows the use of private IP addresses
- NAT device has a pool of public addresses that get mapped to internal computers
- Limits the understanding of the internal network to external entities



Network Address Translation **

- Converts addresses used internally and Internet IP addresses
- Developed because of the quick depletion of public addresses and ability to hide internal networks
- Static NAT – Each internal system has a corresponding external routable IP address
- Hiding NAT – All systems share same external routable IP address
- Dynamic or static mapping

Agenda

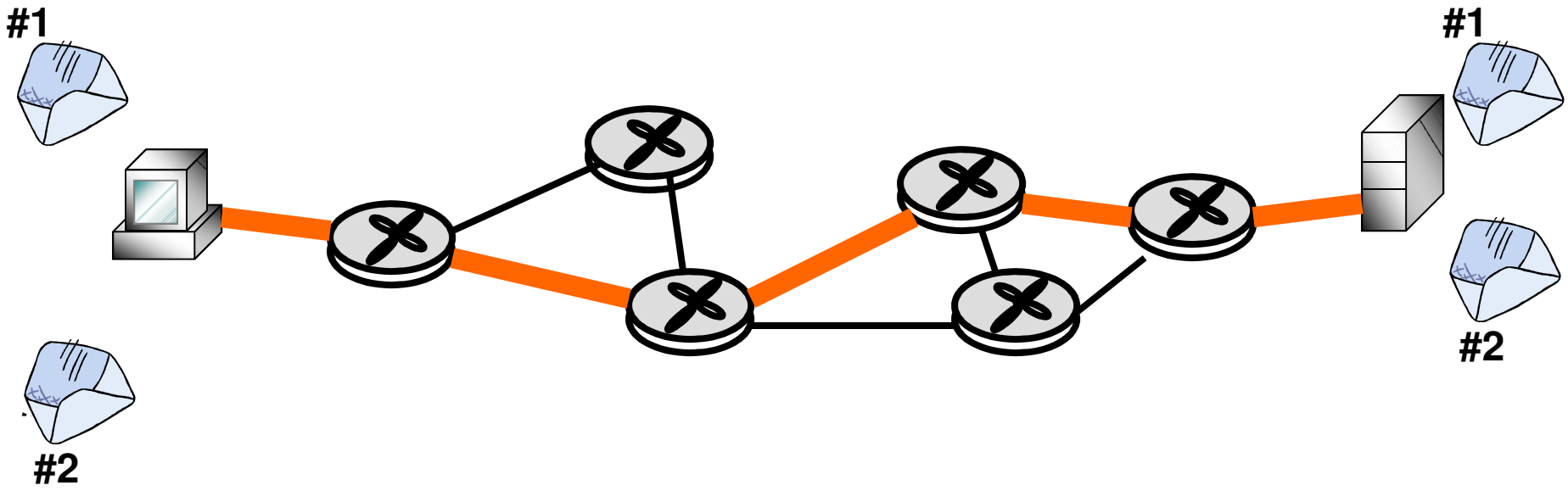
- OSI Model, the TCP/IP suite, and other Protocols
- Signaling and Cabling
- Network Types and LAN Access Technologies
- Firewalls, Bastion Hosts, and Firewall Architecture
- MAN and WAN Technologies, VoIP, and PBX
- Dial-up, Remote Access, Tunneling, and VPN Protocols
- Wireless Networking and Network Attacks

Circuit Switching and Packet Switching

Circuit Switching

- A virtual connection that acts like a dedicated link is built for two devices to communicate
- Connection-oriented virtual link
- Traffic travels in a predictable and constant manner
- Fixed delays
- Usually carries voice oriented data

Circuit Switching **

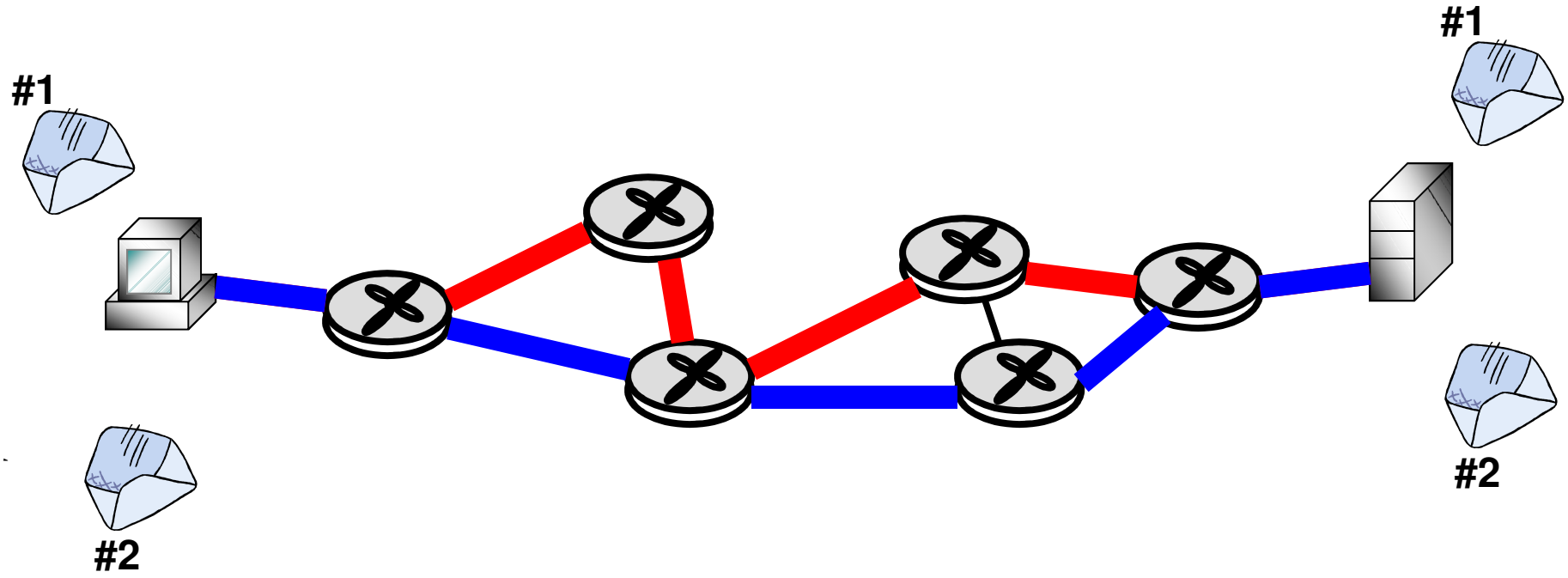


Circuit Switching and Packet Switching

Packet Switching

- Packets can use many different dynamic paths to get to the same destination
- Supports traffic that is bursty
- Variable delays
- Usually carries data oriented information

Packet Switching



Multiplexing **

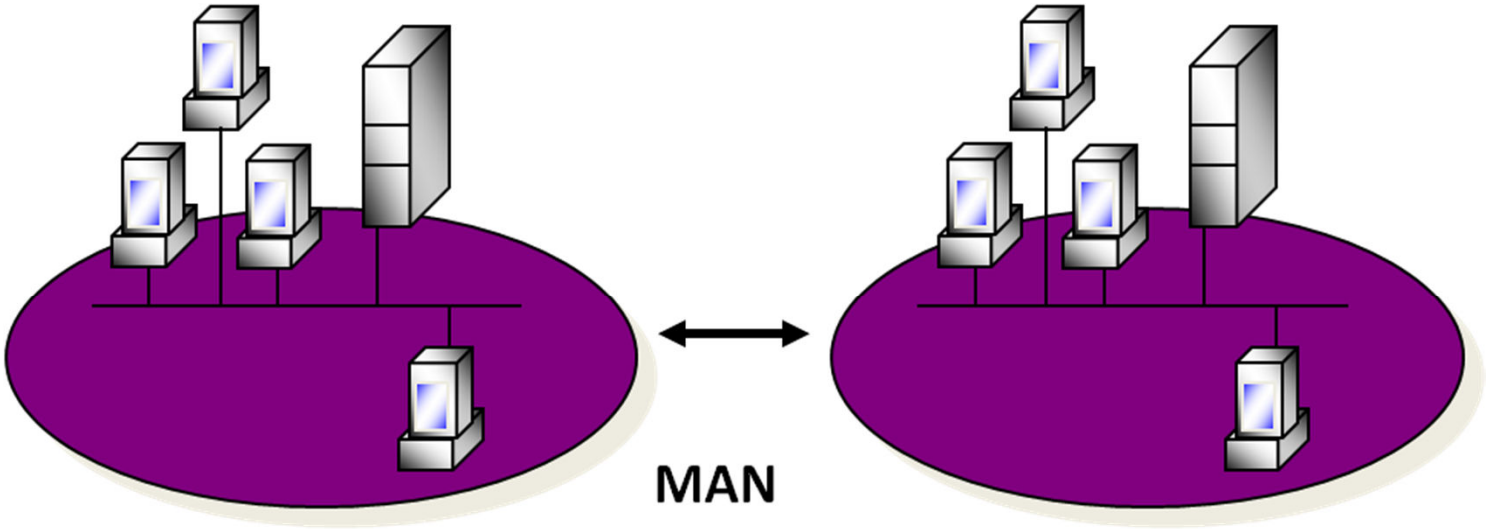
- Devices that combine two or more channels
- The channel is a single path that is physically separated (cables) or logically separated (frequency or time-division multiplexing)

Multiplexing ** (cont.)

- **Multiplexing is the process of combining two or more channels onto one common transmission medium**
  - Frequency-division multiplexing is assigning separate portions of an available spectrum
  - Time-division multiplexing is assigning discrete time intervals in sequence to individual channels

MAN Technologies

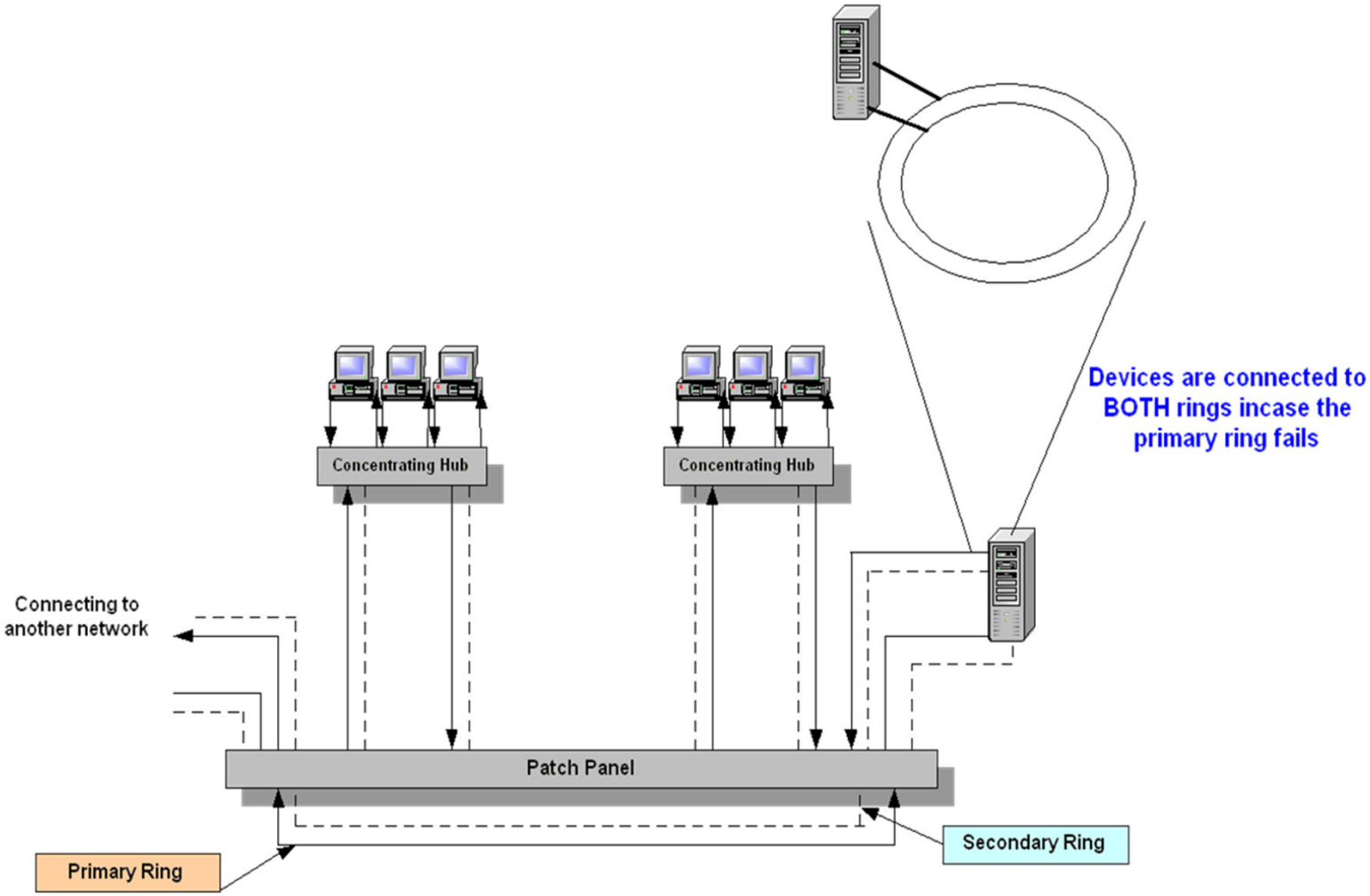
- Fiber Distributed Data Interface
- Synchronous Optical Network (SONET)



Fiber Distributed Data Interface **

- High-speed token-passing media access technology
- Dual rings going in opposite directions for fault tolerance
- Operates at 100 Mbps over fiber
- Can work over long distances at high speeds with minimal interference
- Copper Distributed Data Interface (CDDI) uses UTP instead of fiber
- Usually used for MANs

FDDI Implementation



Synchronous Optical Network

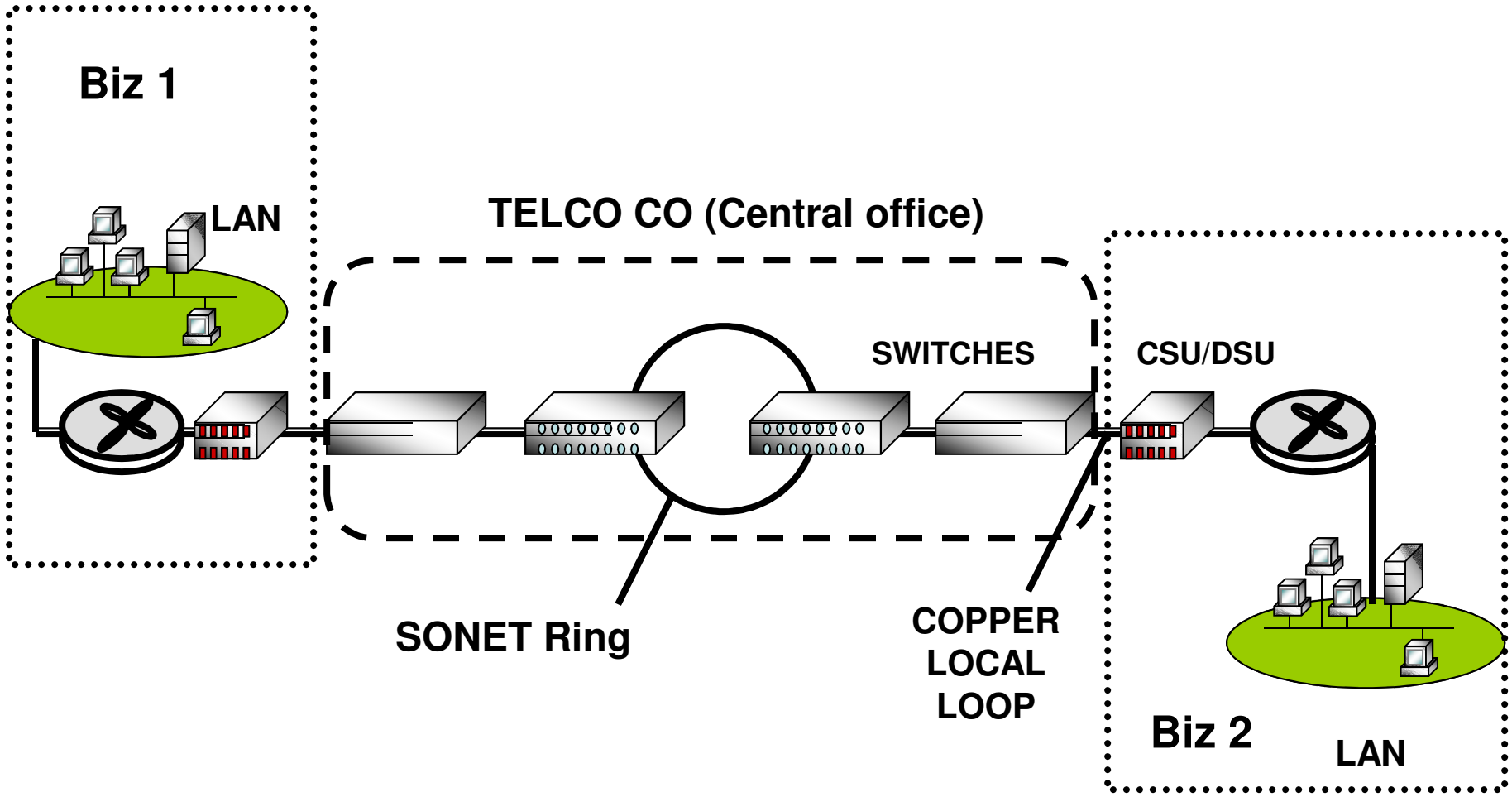
- **Standard for transferring data over fiber-optical lines**

- **Backbone carrier network**
  - Defines transmission rates, signal formats, and optical interfaces
  - Defines the way that telephone companies transmit digital voice and data over optical networks

Synchronous Optical Network (cont.)

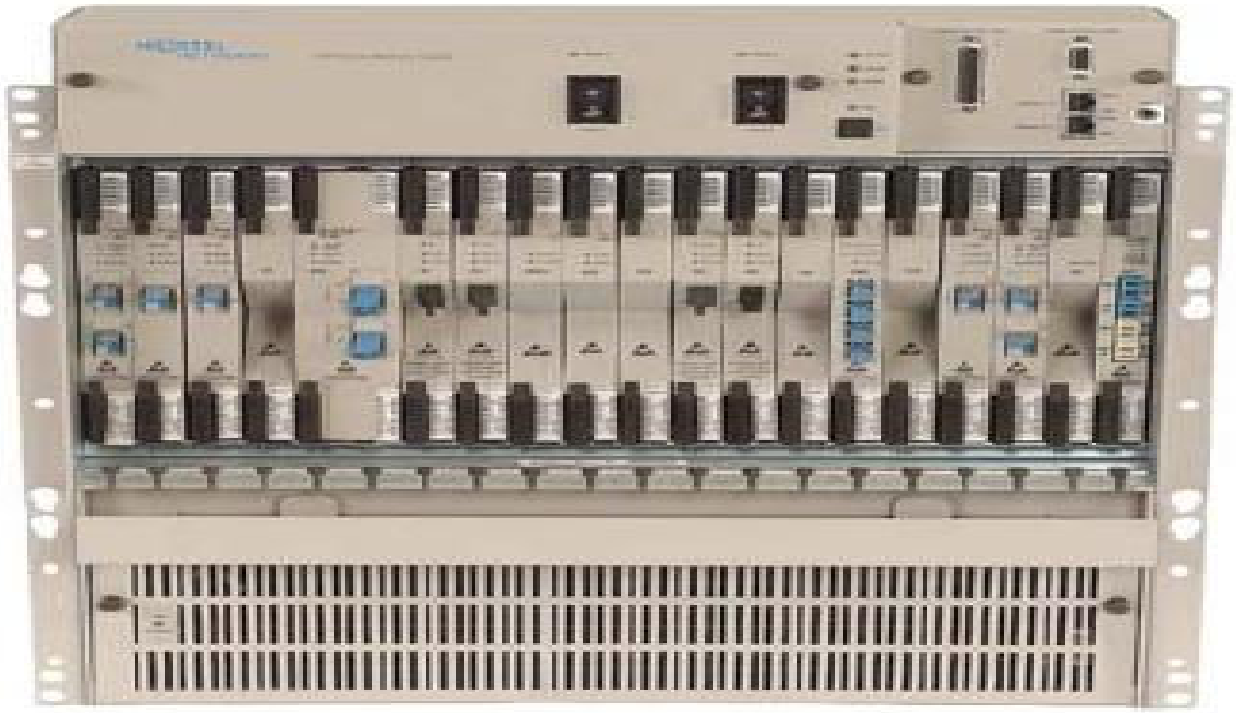
- **Layer 1 technology**
  - Frame relay, ATM, and SMDS can run over SONET
- **Many channels multiplexed together**
- **SONET is self-healing**
  - If there is a break in a line, it can use a backup redundant ring

SONET


Biz 1
LAN
TELCO CO (Central office)
SWITCHES
CSU/DSU
SONET Ring
COPPER
LOCAL
LOOP
Biz 2
LAN

Metro Ethernet

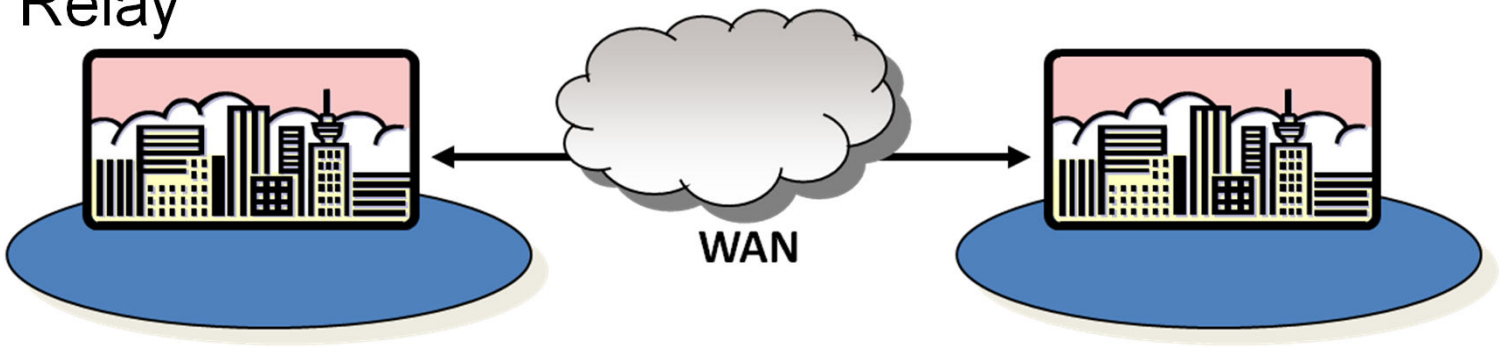
- Next generation LAN technology
- Not testable at this time, but a quickly emerging technology



Wide Area Network

WAN Technologies

- WAN – a network that interconnects systems located in a large geographic area
- PSTN
- ISDN
- DSL
- Frame Relay
- X.25
- ATM
- VoIP
- MPLS
- Metro Ethernet



PBX Protection **

Steps to Secure a PBX

- Change administrative password regularly
- Change default configurations
- Disable maintenance modems
- Block remote calling after business hour
- Block unassigned access codes
- Use call detail recording
- Review telephone bills

Issues with Telephone Security

Phreakers

- Attacks
  - Red Boxing
    - Simulating coins dropped in a pay phone
  - Blue Boxing
    - Tones used to trick phone company's system
  - Black Boxing
    - Manipulating line voltage

Slamming and Cramming

- Slamming: switching a customer's long distance provider without authorization
- Cramming: Adding additional unauthorized charges

Smart-phone/blue tooth attacks

Cell Phone attacks

- Spoofing based on phone serial number to make free long distance calls, often internationally

Bluetooth attacks

- bluejack send spam anonymously to victims
- bluebof exploit overflows in services remotely
- bluebug use AT commands on victims cell phone

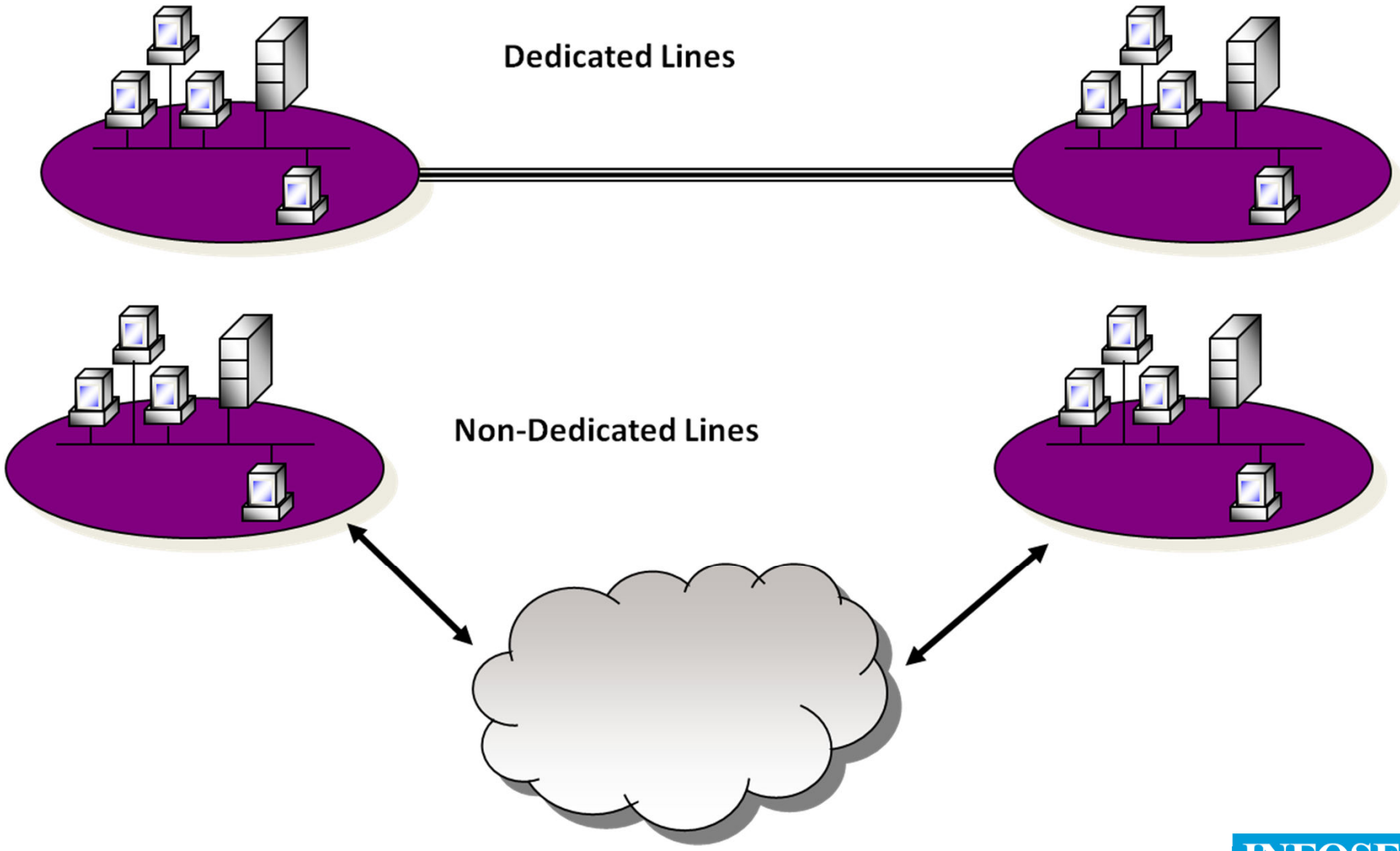
Smart-phone/blue tooth attacks (cont.)

- Bluesnarfing stealing info from a bluetooth device—up to a mile away with proper equipment

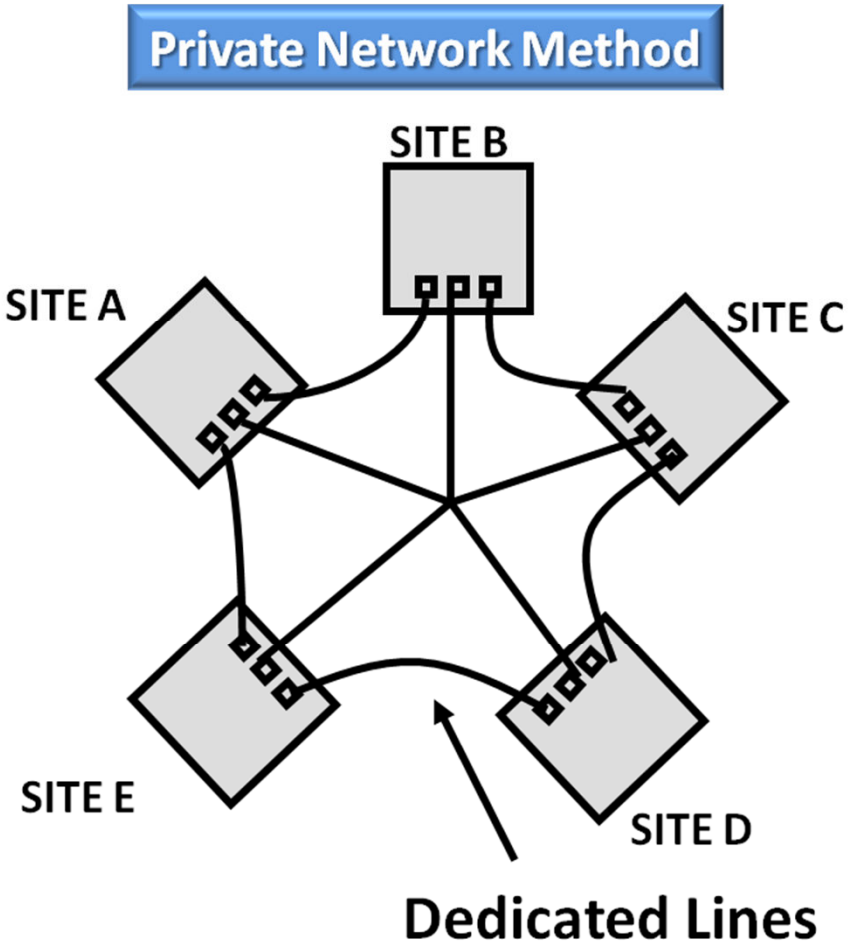
Dedicated Lines

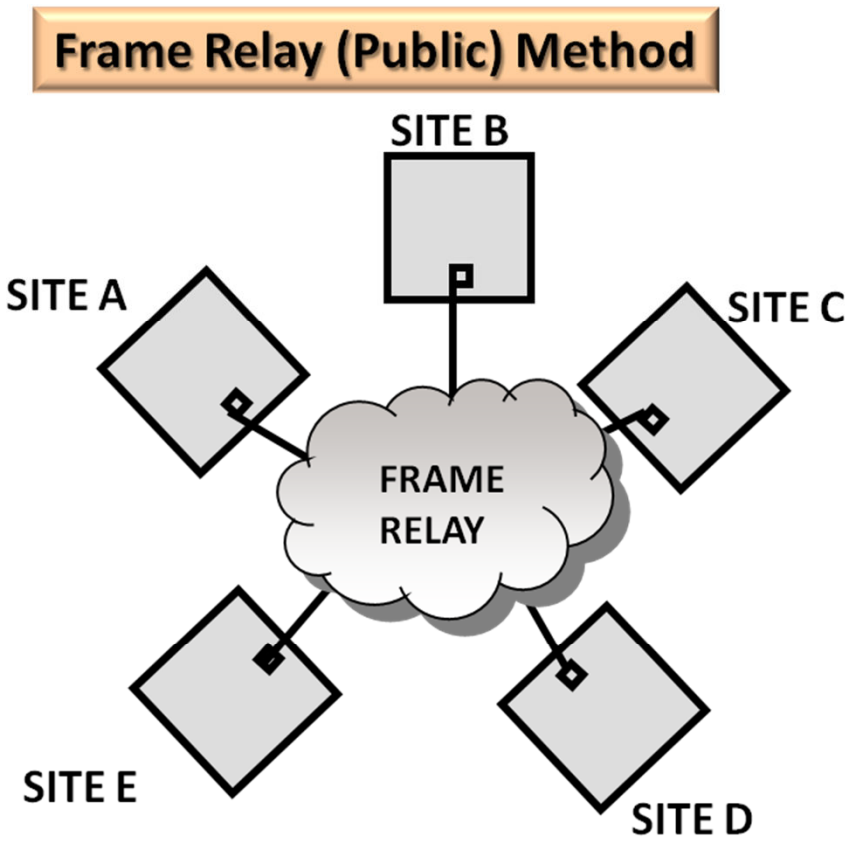
- **Dedicated, meaning communication can only happen between two entities, thus more secure than a shared medium. Only the endpoints can communicate with each other.**
- **Expensive and inflexible**
- **Dedicated lines are usually leased from large telephone carriers (T-Carriers)**
  - T1 = 1.544 Mbps
  - T3 = 44.736 Mbps

Dedicated Lines



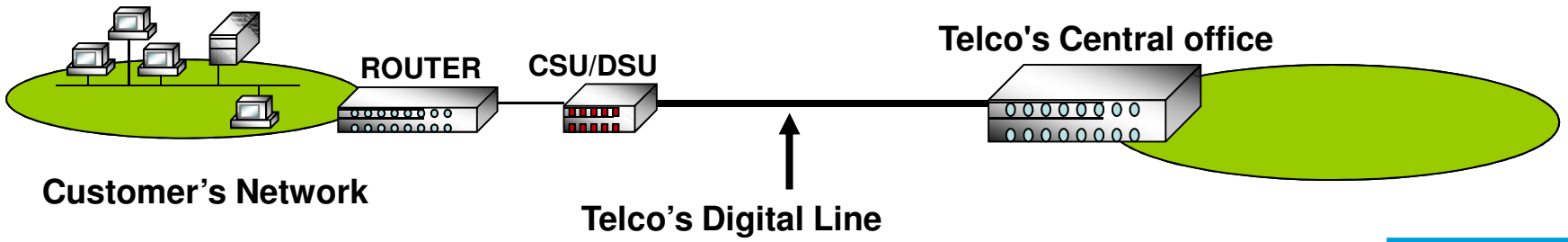
Dedicated Lines





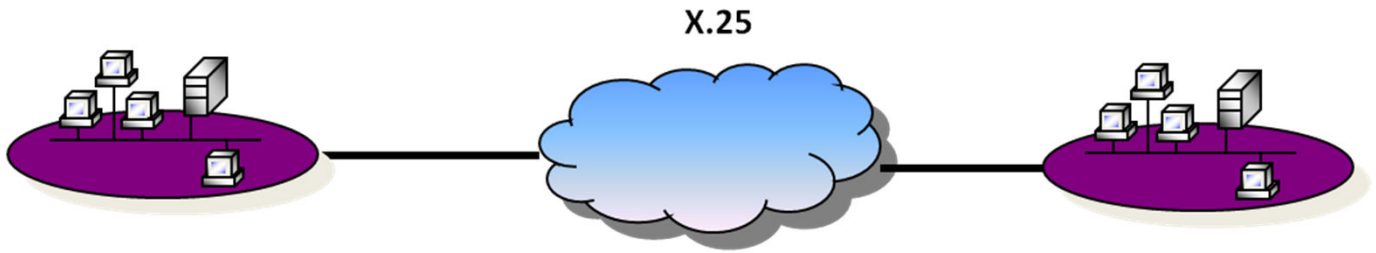
Channel Service Unit/Data Service Unit

- **Hardware required to allow network devices to communicate with a telephone network**
  - Interface between network device and telecommunication device
- **Converts digital signals from network devices to signals that can go over the SP's digital lines**
- **DSU connects to customer's device and CSU connects to telephone company's line**



X.25

- First packet-switching technology that also uses switched and permanent virtual circuits
- Slower than frame relay because of all the error detection and correction functionality
- Developed when the Internet was not as stable and redundant
- Uses Link Access Procedure-Balanced (LAPB) for error detection and correction procedures



Frame Relay

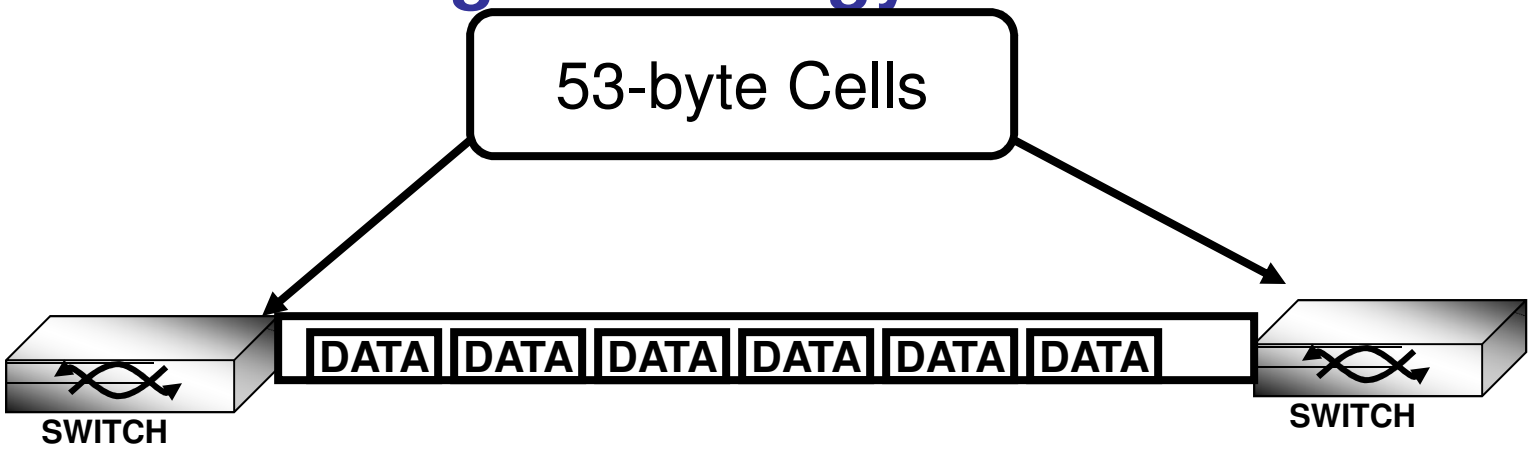
- **Faster WAN packet-switching protocol**
  - Simple framing and no error correction
- **Permanent Virtual Circuit (PVC)**
  - Construction to ensure a customer gets a certain bandwidth level
  - Configured into supporting switches

Frame Relay (cont.)

- **Switched Virtual Circuit (SVC)**
  - Dynamically built when required
- **Committed Information Rate (CIR)**
  - Customer pays a certain monthly payment to ensure a specific bandwidth availability

Asynchronous Transfer Mode (ATM)

- High bandwidth technology that uses switching and multiplexing
- 53-byte fixed cells instead of various frame lengths
- Cell switching technology



MPLS (Multiprotocol Layer Switching)

- MPLS is used to create cost effective, private Wide Area Networks (WANs) faster and more secure than regular routed “public” IP networks like the internet.
- More secure than the public internet, because a “virtual” private network can be built just for your organization
- Since it’s a private network, we don’t have to configure and maintain traditional encryption based Virtual Private Networking (VPN) equipment anymore, and can also avoid the latency and delay inherent in this technology.

MPLS (Multiprotocol Layer Switching)

- Fully meshed network topology meaning that all branches or locations on the network can reach or “talk” to any other (essential for VoIP or video conferencing)
- Relatively inexpensive when compared to other “private” IP facilities like private line or other point to point circuits.

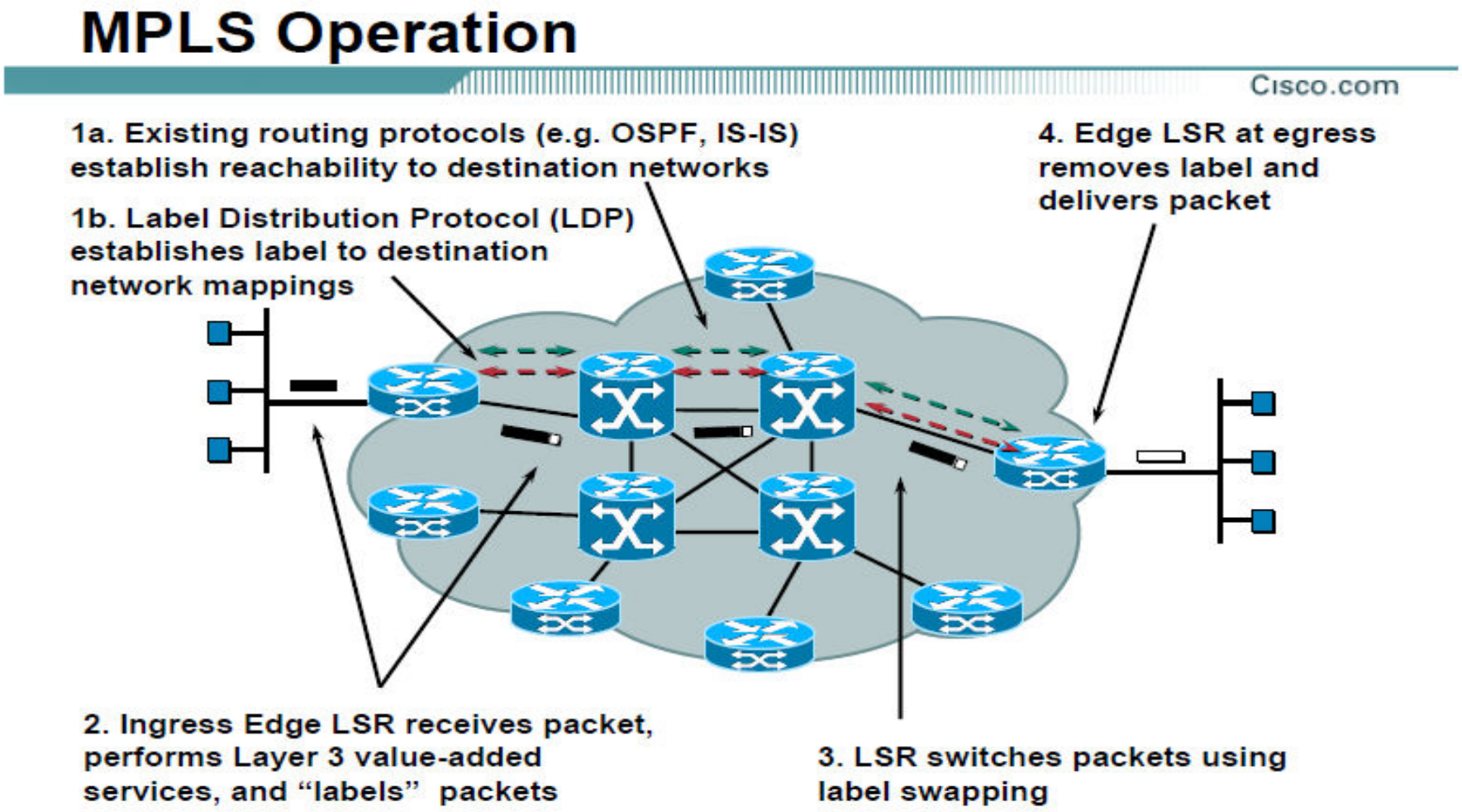
MPLS Acronyms

- MPLS Multiple Protocol Label Switching
- LER Label Edge Router
- LSR Label Switch Router
- LSP Label Switch Path
- FEC Functional Equivalent Class

MPLS (Multiprotocol Layer Switching)

- Encapsulates IP packets inside MPLS by adding labels
- Label Edge Routers determine routing of packets
- Uses labels to determine path
- Provides QoS
- Network routers running MPLS software

MPLS Operation



Voice Over IP

- Technology that can combine different types of data (data, voice, or video) into one packet
- Higher performance
- Reduced operational costs
- Greater flexibility
- Ease of administration

How VOIP Works

- Converts analog to digital through use of Telephony adapter or smartphone
- Data is channeled though gateways (often lacking in authentication mechanisms leading to TOLL FRAUD)
- At the end of a VOIP connection the smart-phone or TA converts the signal back to analog

Challenges with VOIP

- IP was designed for bursty data-based traffic, not voice. When voice and data are combined, jittering can result
- IP is connectionless, so packets can arrive out of sequence
- As IP is a store and forward technology, each hop introduces the potential for latency

Components Required for VOIP

- IP telephony device
- Call-processing manager
- Voicemail system
- Voice gateway

SIP (Session Initiation Protocol)

- Allows for the establishment of user location (i.e. translating from a user's name to their current network address).
- Provides for feature negotiation so that all of the participants in a session can agree on the features to be supported among them.
- A mechanism for call management - for example adding, dropping, or transferring participants.

SIP (Session Initiation Protocol) (cont.)

- Allows for changing features of a session while it is in progress.

- Provides signaling services like causing the phone to ring, dialing, generating busy signals. SIP is ONLY a signaling protocol. The voice stream is carried by other protocols like RTP (Real-time Transfer Protocol).

Security Threats with VOIP

- Toll Fraud (most significant)
- DDoS
- SPIT (SPam over Internet Telephony)
- Phishing

WAN Technology Summary – 1 of 2

Technology	Characteristics
Dedicated Lines	• Dedicated, leased line that connects two locations • Expensive compared to other WAN options • Secure because only two locations are using the same media
Frame Relay	• High-performance protocol that uses packet-switching, which works over public networks • Shared media between companies • Uses SVCs and PVCs • Fee based on used bandwidth
X.25	• First packet-switching network developed to work over public networks • Shared media between companies • Lower speed than frame relay from extra overhead • International standard and used more in countries other than the United States

ISDN **

- **Circuit switched technology to get digital services over standard voice lines for "last mile"**
- **Popular for dial backup on routers because control channel is out-of-band, which allows for quicker call setup and tear down**
  - Delta or D channel
- **Signal does not need to be converted from analog to digital**
- **Has a basic service (data transmission) and supplementary (call waiting, call transfer)**
  - Enriched features

Integrated Services Digital Network **

- **A technology that allows for digital signals to transmit over the existing telephone lines**
  - This replaces the analog dial-up technology
- **Basic Rate Interface (BRI) – This implementation uses 2 B channels and 1 D channel with a combined bandwidth of 144 Kbps**
  - This is used for home subscribers

Integrated Services Digital Network (cont.)

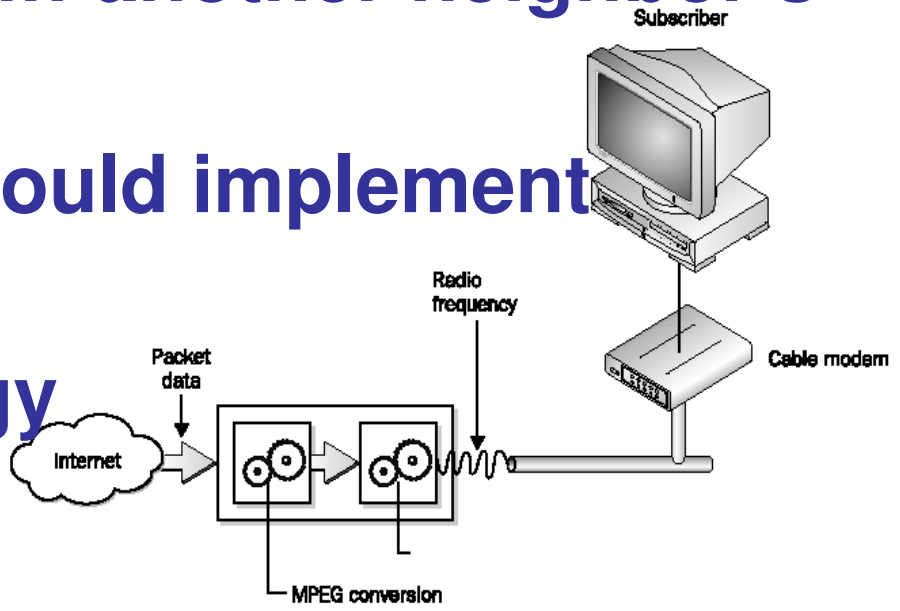
- **Primary Rate Interface (PRI) – This implementation has up to 23 B channels and 1 D channel, at 64-Kbit/sec**
  - The total bandwidth is equivalent to a T1 (1.544 Mb/s)
  - This would be more suitable for a company that requires a higher amount of bandwidth

Digital Subscriber Line (DSL)

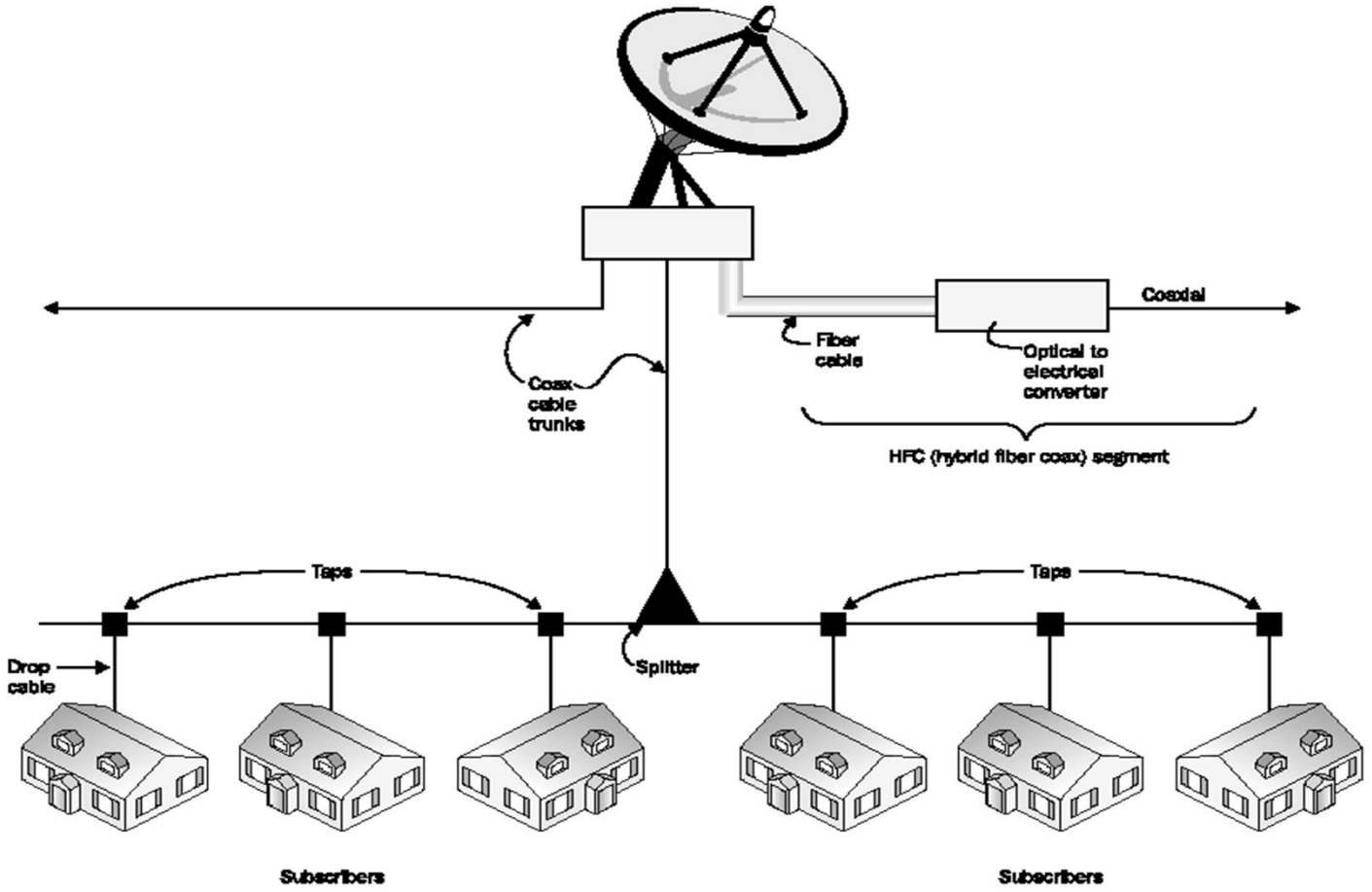
- Provides high digital data transmission over existing telephone lines
- Higher speeds than ISDN and analog dial-up technologies
- Security issue of being “always on”
- Users should use a personal firewall and shutdown system when not using it

Cable Modem

- High speed access to the Internet provided by a cable company
- All cable modems within an area eventually share the same coaxial trunks, thus one neighbor can easily sniff another neighbor's traffic
- Insecure, and users should implement personal firewalls
- "Always on" technology



Cable Modem Access

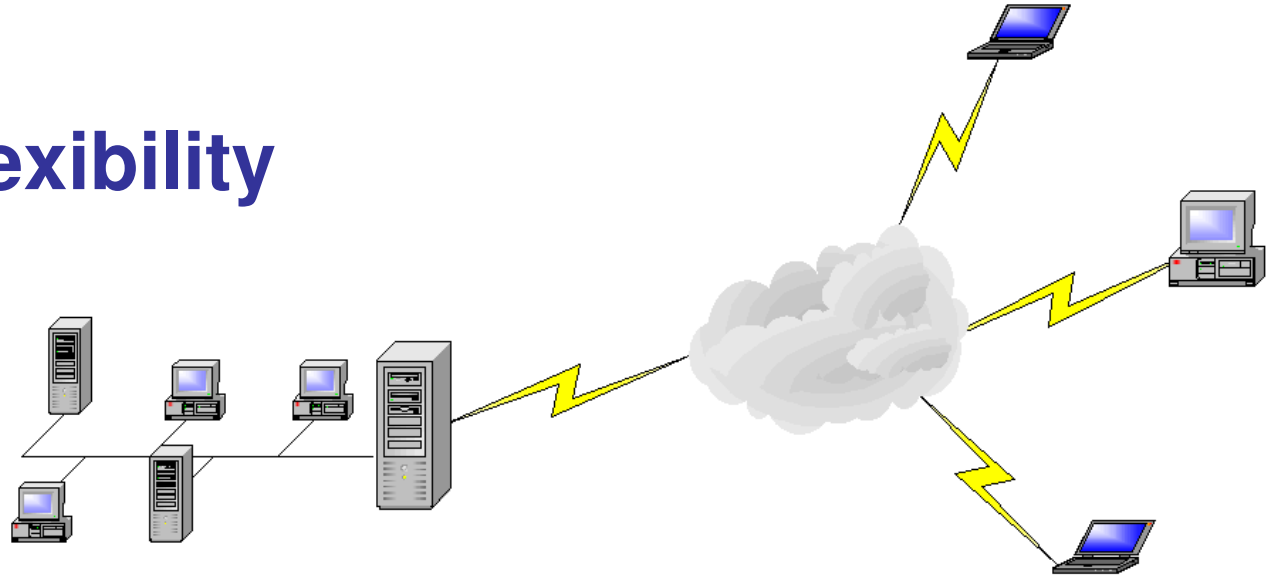


WAN Technology Summary – 2 of 2

WAN Technologies	Characteristics
ATM	• High-bandwidth switching and multiplexing technology that has a low delay; very fast • Uses 53-byte fixed-size cells transmitted over PVCs and SVCs
VoIP	• Combines voice and data over the same IP network media and protocol • Reduces costs of implementing and maintaining two different networks
MPLS	• High-speed switching technology to be used over public network

Remote Access

- Older technologies used to allow road warriors or home-based users to access network resources
- Reduces the cost of dedicated leased lines
- Provides flexibility



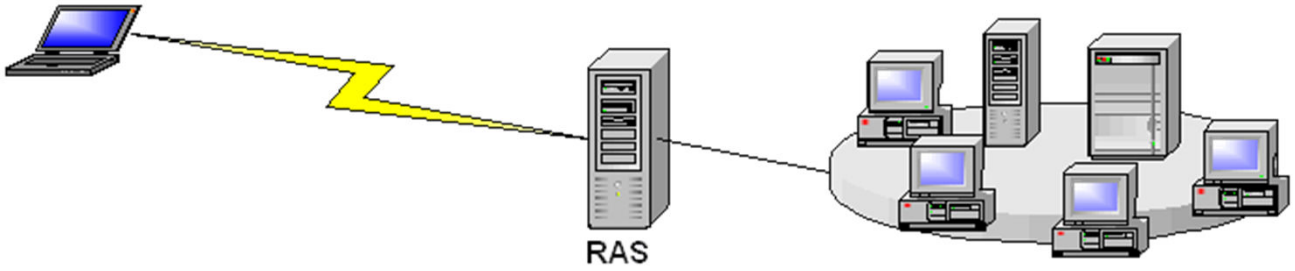
Dial-up Security Mechanisms

Call back

- User provides credentials, access server hangs up the connection and calls them back at a pre-configured number
- Less flexible and do not know who is really at that number

Caller ID

- Verifies number user is calling from and compares it against acceptable phone numbers before establishing the session
- More flexible

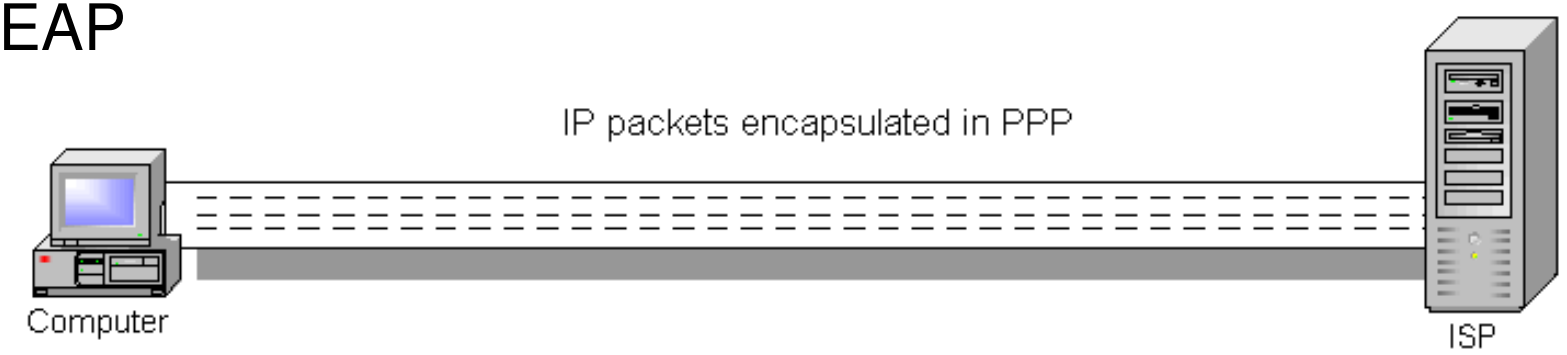


VPN and Tunneling Protocols

- **Remote Access**
- **Dial-up and RAS**
- **Dial-up Protocols**
  - PPP, Authentication Protocols (PAP, CHAP, EAP)
- **Tunneling Protocols**
  - PPTP, L2TP, SSTP, IPsec
- **Virtual Private Network**

Point-to-Point Protocol

- **Protocol used to encapsulate data over a serial line for dial-up connectivity**
  - Can encapsulate protocols that cannot route through the Internet
- **Authentication mechanisms:**
  - PAP
  - CHAP
  - EAP



Tunneling

- **Preserves original protocol headers**
- **Frame is wrapped, or encapsulated, within a second frame to allow that data to transmit through an intermediary network**
- **Second protocol insulates the frame and creates the illusion of a tunnel for the data to travel through**
- **The frame of one protocol is the data of another protocol**
  - First protocol may not be routable
  - First frame may need to be encrypted for confidentiality

Tunneling Protocols – PPTP **

- Point-to-Point Tunneling Protocol
- Encapsulation protocol based on PPP
- Data Link layer protocol that provides single point-to-point connections
- Data can be encrypted but negotiation information is in clear text
- Works only over IP traffic

Tunneling Protocols – L2TP

- Hybrid of L2F and PPTP
- Sets up a single point-to-point connection between two computers
- Works at the Data Link layer
- Transmits over multiple types of networks
  - not just IP
- Combined with IPsec for security

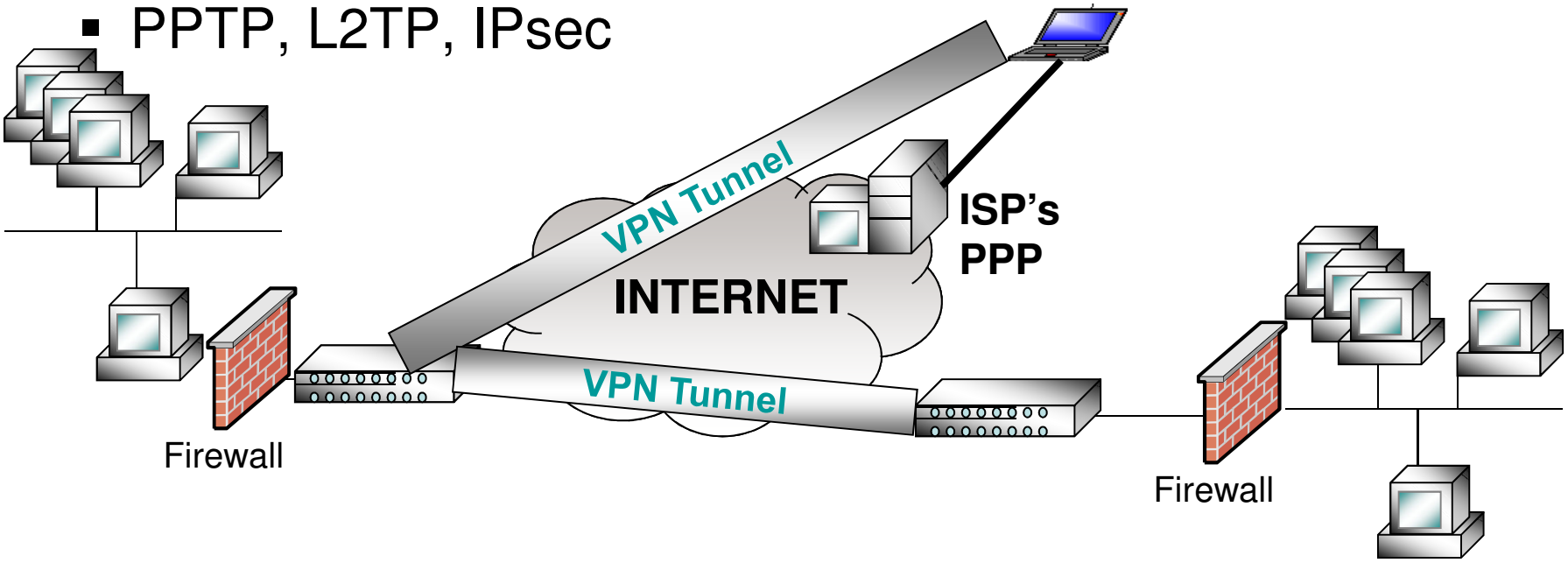
Virtual Private Networks

- Trusted communication channel through a network that is not trusted
- Cheaper and more flexible than dedicated links
- VPN is usually configured on the firewall – different link and trust levels

Virtual Private Network

- **Secure private connection through a public network**

- **Using tunneling protocols:**
  - PPTP, L2TP, IPsec



IPsec Review

- **Works at the Network layer, providing security on top of IP**
- **Can encrypt just the payload or the payload and the header**
  - Tunnel Mode
    - Payload and headers are protected
  - Transport Mode
    - Payload protected

IPsec Review (cont.)

- **Works at the Network layer, providing security on top of IP**
- **Can encrypt just the payload or the payload and the header**
  - Tunnel Mode
    - Payload and headers are protected
  - Transport Mode
    - Payload protected

Password Authentication Protocol (PAP)

- Authentication protocol used by remote users
- Authenticates after a PPP connection is set up
- Credentials are sent in clear text
- Vulnerable to sniffing, man-in-the-middle, and replay attacks

CHAP

- Challenge Handshake Authentication Protocol
- Authentication protocol that sends a challenge response
- User's password is used to encrypt challenge value
- Periodically sends a challenge to protect against man-in-the-middle attacks
- Password is not sent over the wire

Extensible Authentication Protocol **

- **EAP is a general protocol for authentication that also supports multiple authentication methods:**
  - Token cards
  - Kerberos
  - One-time passwords
  - public key authentication
- **IEEE 802.1x specifies how EAP is encapsulated in Ethernet**

Extensible Authentication Protocol **

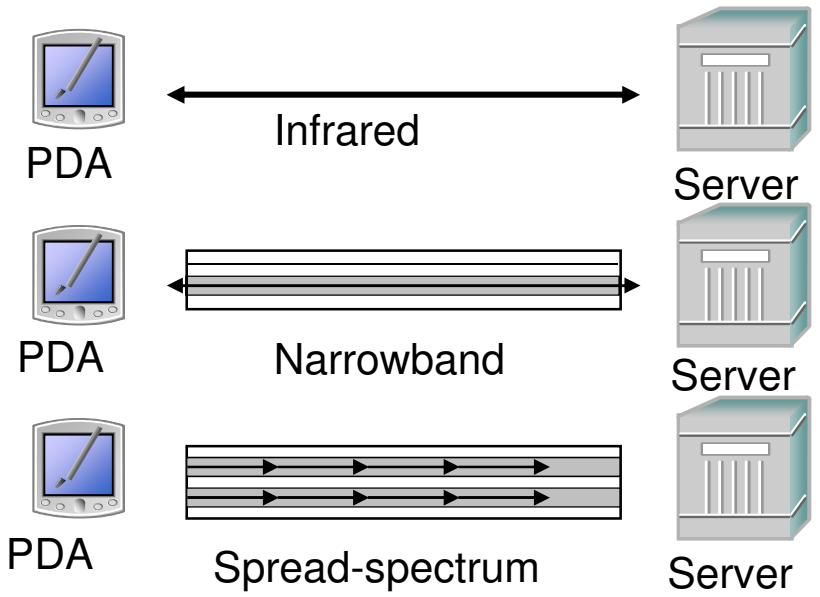
- **EAP services are available in various methodologies:**
  - EAP MD5
  - EAP-Tunneled TLS (EAP-TTLS)
  - Lightweight EAP (LEAP)
  - Protected EAP (PEAP)

Agenda

- OSI Model, the TCP/IP suite, and other Protocols
- Signaling and Cabling
- Network Types and LAN Access Technologies
- Firewalls, Bastion Hosts, and Firewall Architecture
- Dial-up, Remote Access, Tunneling, and VPN Protocols
- MAN and WAN Technologies, VoIP, and PBX
- Wireless Networking and Network Attacks

Wireless Transmission Methods

- **First wireless network standard: 802.11**
- **Defines three physical layers:**
  - Infrared
  - Narrowband
  - Spread-spectrum
- **Spread spectrum:**
  - Derived from military communication methods
- **Variations:**
  - DSSS (uses all of bandwidth)
  - FHSS (only uses part of available bandwidth)
  - ODM



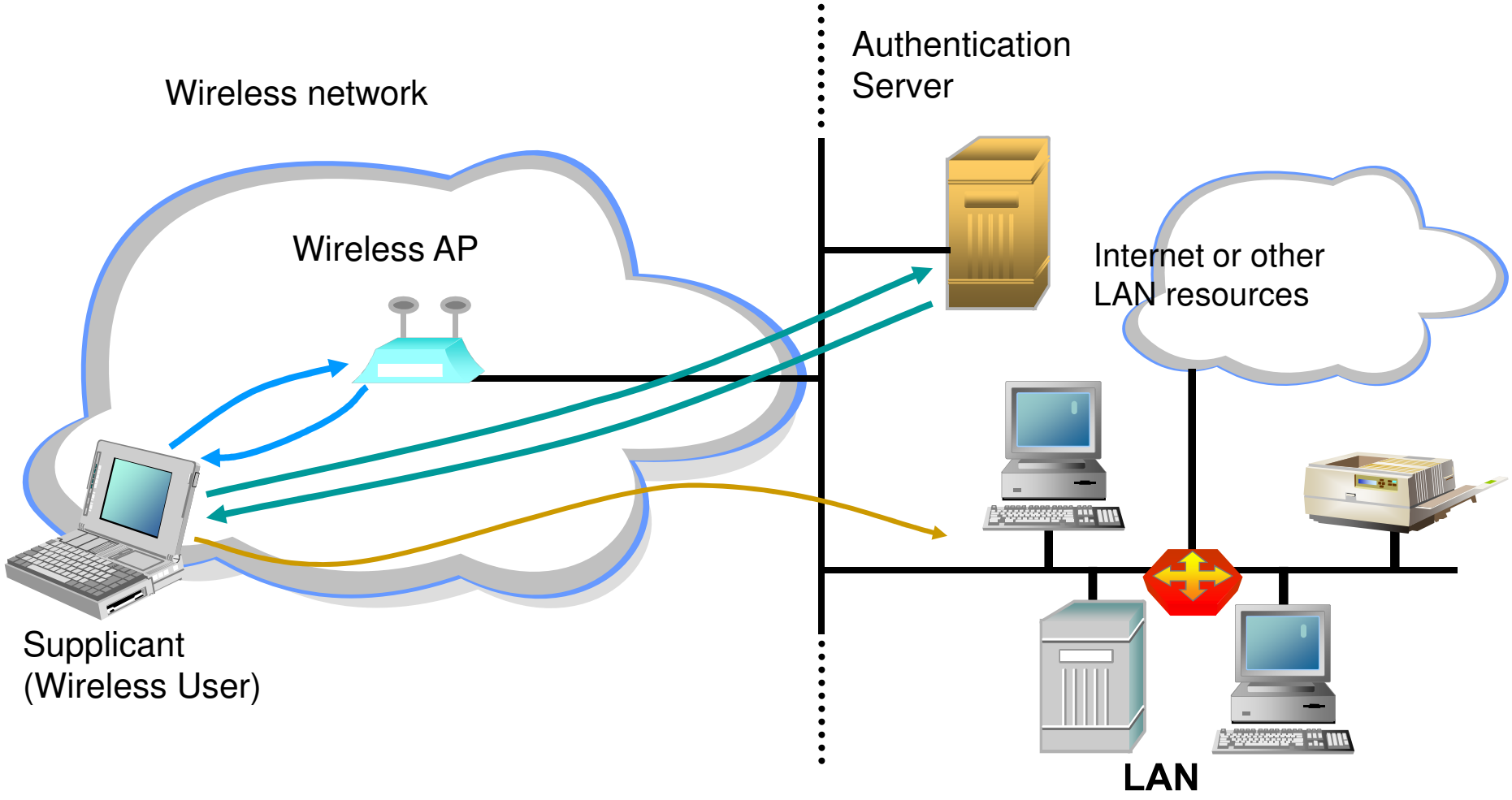
WLAN Frequencies and Signaling

- **Popular standards used for WLANs include:**
  - 802.11a: More channels, high speed, less interference
  - 802.11b: Protocol of Wi-Fi revolution, served as first true de facto standard
  - 802. 11g: Similar to 802.11b, only faster
  - 802.11i: Adds WPA II
  - 802.11n: 450 Mbps
  - 802.16: Long-distance wireless infrastructure

WLAN Components

- **APs (Access Points):**
  - Two modes:
    - Infrastructure mode
    - Peer-to-peer mode
- **SSID (Service Set ID):**
  - Same SSID required from all APs and devices
- **Encryption Mechanism: Most APs come without encryption enabled**

802.1x Example



Wireless LAN Security

- **Securing WLANs (Wireless LANs) is harder than securing a wired LAN**
- **Well-known wireless security methods include:**
  - WEP (Wired Equivalent Privacy)
  - WPA (Wi-Fi Protected Access)
  - WPA2 aka 802.11i

Wireless Standards: WEP

- **Wired Equivalent Privacy**
- **WEP is based on RC4**
- **Easy to recover the key:**
  - Single shared key
  - Cleartext IV transmission
  - Weak IVs
  - No checking for retransmissions of the same packet

WPA

- **WPA was the replacement for WEP**
- **WPA is more secure:**
  - Uses TKIP
  - Uses 48-bit IV
  - Uses a different session key for each packet
  - Uses MIC to detect invalid packets
- **WPA-Enterprise,**
- **WPA-Personal**

WPA2

- 802.11i IEEE Standard
- CCMP: (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) An AES-based encryption mechanism that is stronger than TKIP.
- AES uses 128, 192 or 256 bit encryption

Wireless Network Attacks

- **Wireless networking opens a network up to threats**
- **Attacks that can be launched against a WLAN include:**
  - Detection (wardriving)
  - Eavesdropping
  - Open authentication
  - Spoofing
  - Denial-of-service

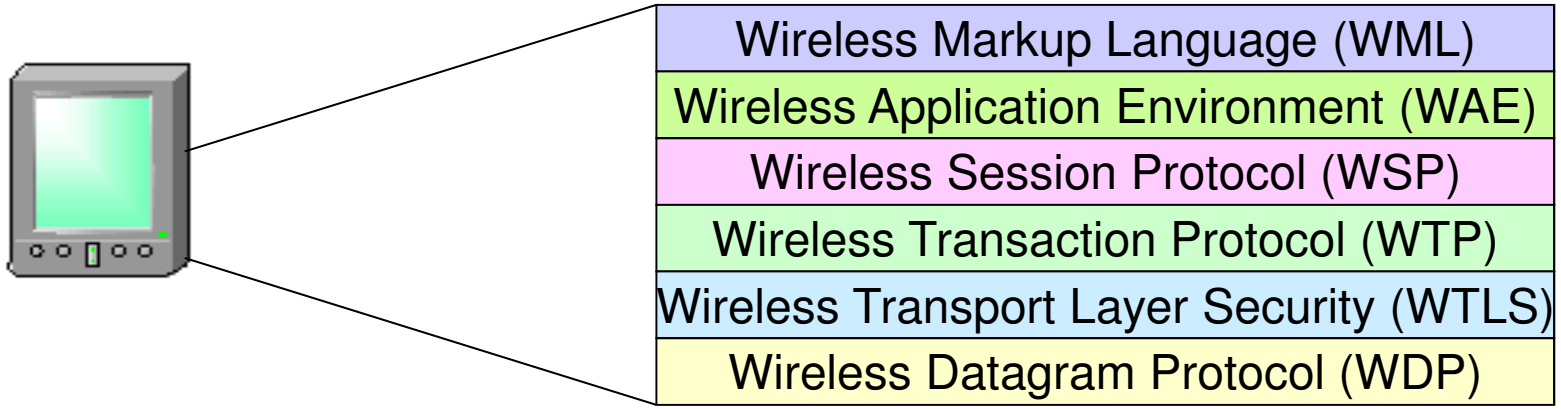
War Driving for WLANs

- **Warwalking: Walking around to look for open wireless networks**
- **Wardriving: Driving around to look for open wireless networks**
- **Warflying: Flying around to look for open wireless networks**
- **Warchalking: Using chalk to identify available open networks**
- **GPS (Global Positioning System)**
  - Used to help map the open networks that are found
- **Bluejacking: Sending unsolicited messages to a Bluetooth enabled device**

Wireless Application Protocol

WAP

- Set of protocols provides same type of functionality of TCP/IP and HTML
- Allows wireless device to access the Internet
- Lower overhead protocol than what is used in PCs
- Wireless devices have limited storage, memory and processing power



Attacks

Impersonation

- Impersonate a user with credentials, alter MAC address to impersonate another computer, e-mail spoof
- Countermeasures: strong authentication mechanisms (at least two factor), digital signatures, one-time passwords

Packet Modification

- Data altered during transmission
- Countermeasure: hashes, digital signatures

Attacks

Flooding

- Sending more data than a system can handle – pings, mail bombs, SYN packets
- Countermeasures: filter packets before reach destination, patch system

Web Spoofing

- Redirecting to a different site
- Changing a DNS resource record to point to a different site

DNS Poisoning

- Bogus resource records
- Countermeasure: DNSSEC

Attacks

Login Spoofing

- Counterfeit page inserted for login process
- Countermeasure: mutual authentication

Tunneling

- Use a mechanism in a way that it was not designed
  - Insert data behind ICMP header
  - Send malware through port 80
- Countermeasure: firewall device that looks deeper into packet
  - An application-level proxy

Bringing Things Together

- Protocols provide the rules of communication
- Topologies and media access technologies
- LAN and WAN devices
- Firewalls, DMZ, VPN
- WAN technologies
- Remote access and authentication protocols
- Redundancy and backups
- PBX security