



CompTIA N + N10-007

Course CompTIA N+ 2019

By Eng. Ahmad Hassan Al-Mashaikh

Email : Ahmad.private.mashaikh@Hotmail.com

LinkedIn : Ahmad H Al-Mashaikh

Facebook : Ahmad H Al-Mashaikh

Group : Ahmad H Al-Mashaikh - Information Technology

Page Facebook : Eng. Ahmad H Al-Mashaikh

Phone : 00972598053163 | This is WhatsApp

Phone : 009665508721



Certifications and Certified

Certified: Microsoft | Cisco | CompTIA | Citrix | ITIL | EC-Council | Oracle | Processing CCIE Lab R&S | CISSP | LTP.

- ✓ MCPS: Microsoft Certified Professional
- ✓ MCSE :Communication Lync Server
- ✓ MCSE : Private Cloud
- ✓ MCSE Exchange Server 2013
- ✓ MCITP: Enterprise Administrator on Windows Server 2008
- ✓ MCITP: Administrator on Windows Server 2008
- ✓ MCITP: Enterprise Messaging Administrator on Exchange 2010
- ✓ MCITP: Enterprise Desktop Support Technician on Windows 7
- ✓ MCITP: Enterprise Desktop Administrator on Windows 7
- ✓ MCITP: SharePoint Administrator 2010
- ✓ MCTS: Microsoft Exchange Server 2010
- ✓ MCTS: Windows Server 2008 Active Directory
- ✓ MCTS: Windows Server 2008 Network Infrastructure
- ✓ MCTS: Windows Server 2008 Applications Infrastructure
- ✓ MCTS: System Center 2012 Configuration Manager
- ✓ MCTS: Windows 7, Configuration
- ✓ MCTS: SharePoint 2010, Configuration
- ✓ MCSA: Windows Server 2016
- ✓ MCSA: Windows Server 2012
- ✓ MCSA: Windows Server 2008
- ✓ MCSA: Windows 8
- ✓ MCSA: Windows 7
- ✓ MS: Windows 7, Configuring
- ✓ MS: Windows 7, Enterprise Desktop Administrator
- ✓ MS: Windows 7, Enterprise Desktop Support Technician
- ✓ MS: Server Virtualization with Windows Server Hyper-V
- ✓ Windows 8 for IT Pros Jump Start
- ✓ Windows 8 Security lights
- ✓ Licensing Office 2013 and Office 365
- ✓ A+, Network +, Security +, Linux+, Server+ , Cloud+
- ✓ CCNA R&S,CCDA Design, CCNA Security, CCNA Wir , CCNA ISP
- ✓ CCNP R&S , CCNP Security , CCNP ISP , CCDP Design, CCIE Wr
- ✓ Citrix CCA, Oracle SQL, CEH, Personal Strategies Planning, ITIL

CompTIA Career Certifications

CompTIA®



How to be A+ certified ?

Exam Details

Exam Codes : **N10-007**

Exam Description

CompTIA Network+ N10-007 has been updated and reorganized to address the current networking technologies with expanded coverage of several domains by adding:

- Critical security concepts to helping networking professionals work with security practitioners
- Key cloud computing best practices and typical service models
- Coverage of newer hardware and virtualization techniques
- Concepts to give individuals the combination of skills to keep the network resilient

Number of Questions

Maximum of 90 questions

Type of Questions

Multiple choice questions (single and multiple response), drag and drops.

Length of Test

90 Minutes per exam

By : Eng. Ahmad Hassan Al-Mashaikh

Email : Ahmad.private.mashaikh@hotmail.com

Course Topics

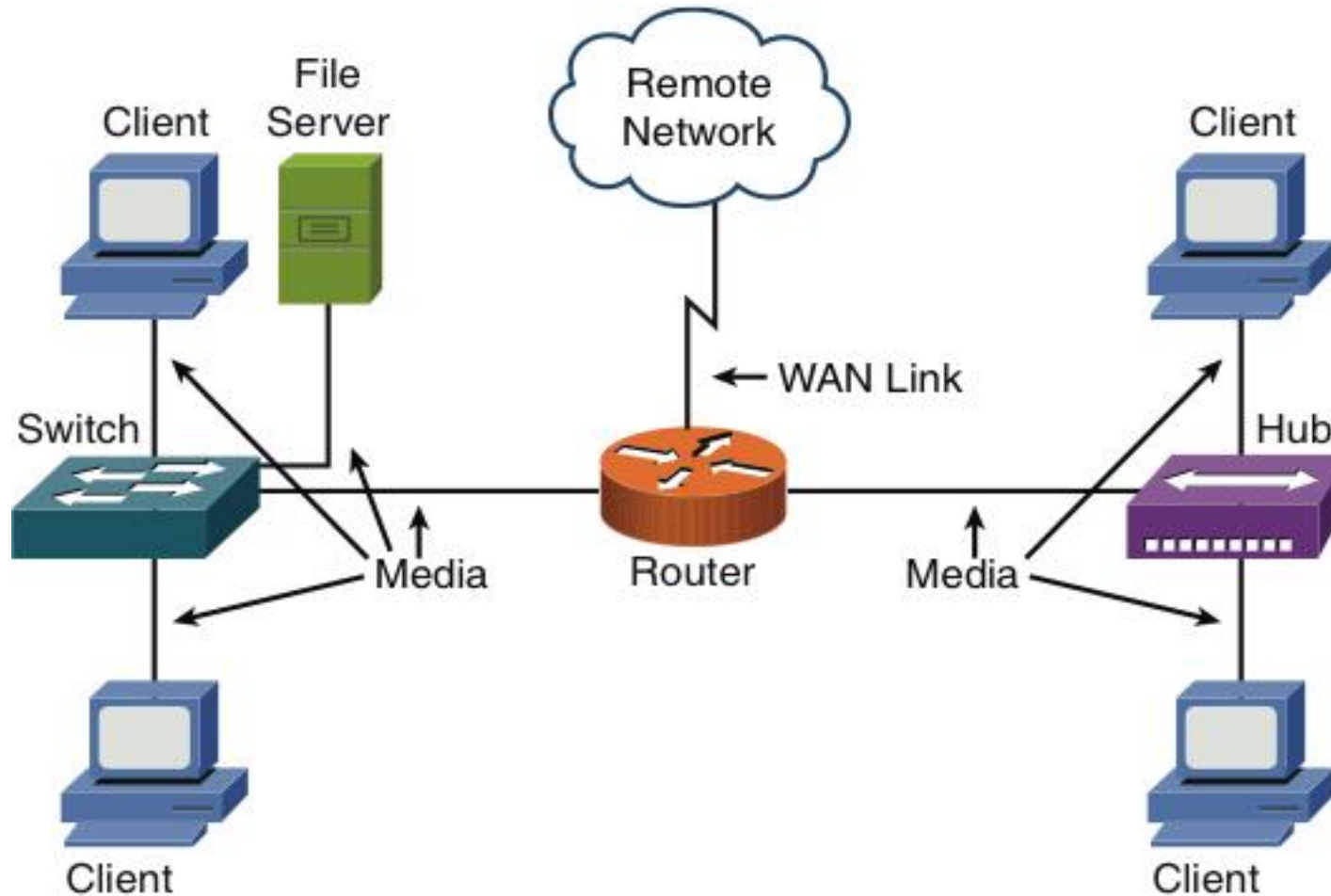
Objectives

- What is the purpose of a network?
- What are some examples of network components?
- How are networks defined by geography?
- How are networks defined by topology?
- How are networks defined by resource location?

Defining a Network

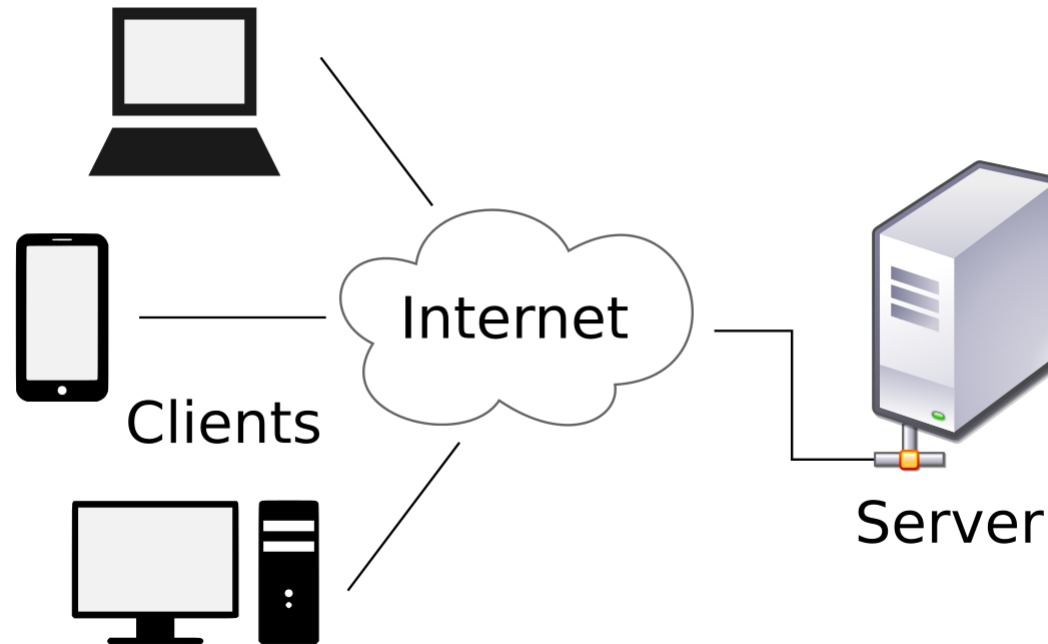
- A (computer) network is an interconnection of two or more computing devices.
- It can serve a variety of purposes including:
 - File sharing between two computers
 - Video chatting across different parts of the world
 - Surfing the Web
 - Instant messaging (IM) between computer with IM software installed.
 - E-mail
 - Voice over IP (VoIP)
- A converged network is one that transports multiple forms of traffic (video, voice, and data)

Overview of Network Components



Overview of Network Components

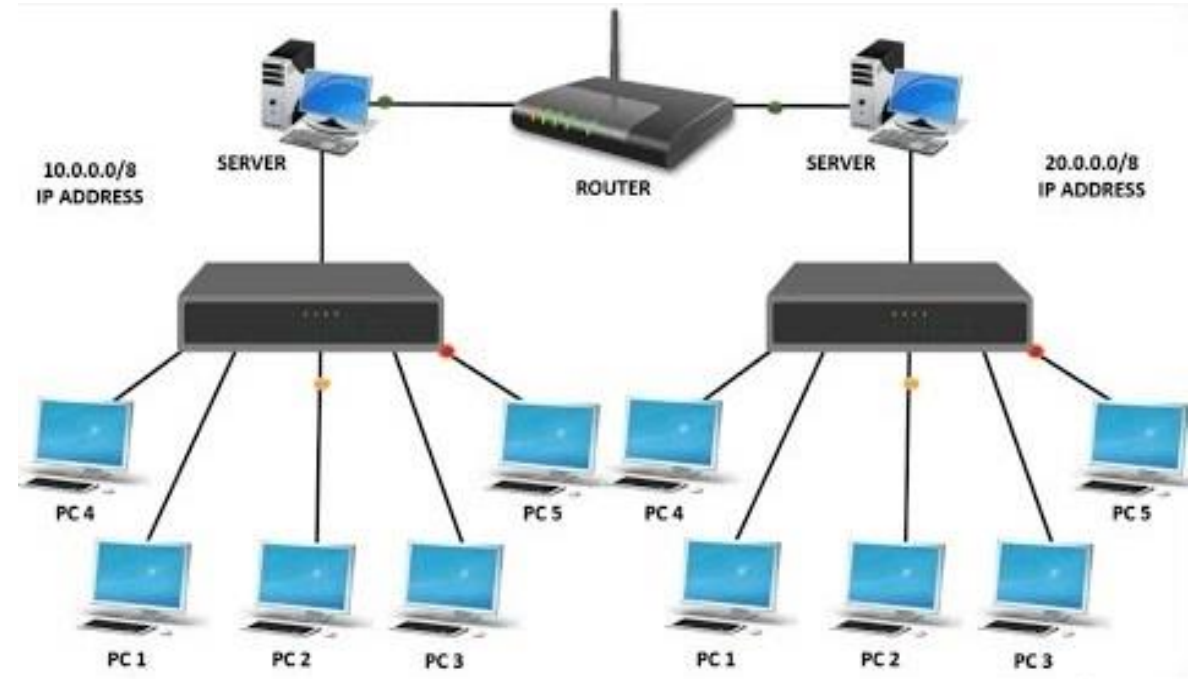
- **Client:** The term client defines the device an end user uses to access a network.
- **Server:** A server provides resources to a network. (Email, Web pages, or files)



Overview of Network Components

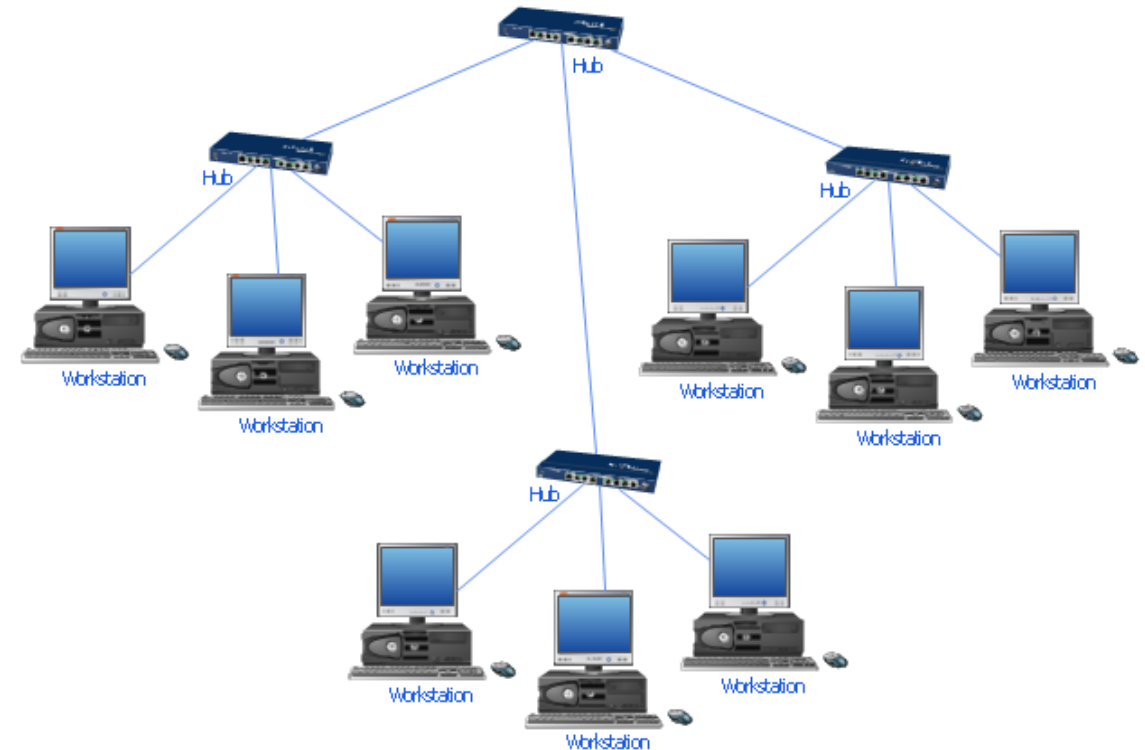
- **Switch:** A switch interconnects network components. Unlike a hub, a switch makes forwarding decisions based on physical addresses.
 - **Physical Address** is burned into the NIC, usually a **MAC Address**.
- **Router:** A router is connection device that makes forwarding decisions based on logical network addresses.
 - **Logical Address** is determined by physical location, usually an **IP Address**.
- **Media:** The media is the physical substance on which the information of the system travels, such as copper wire for carrying electronic signals.

Network Devices



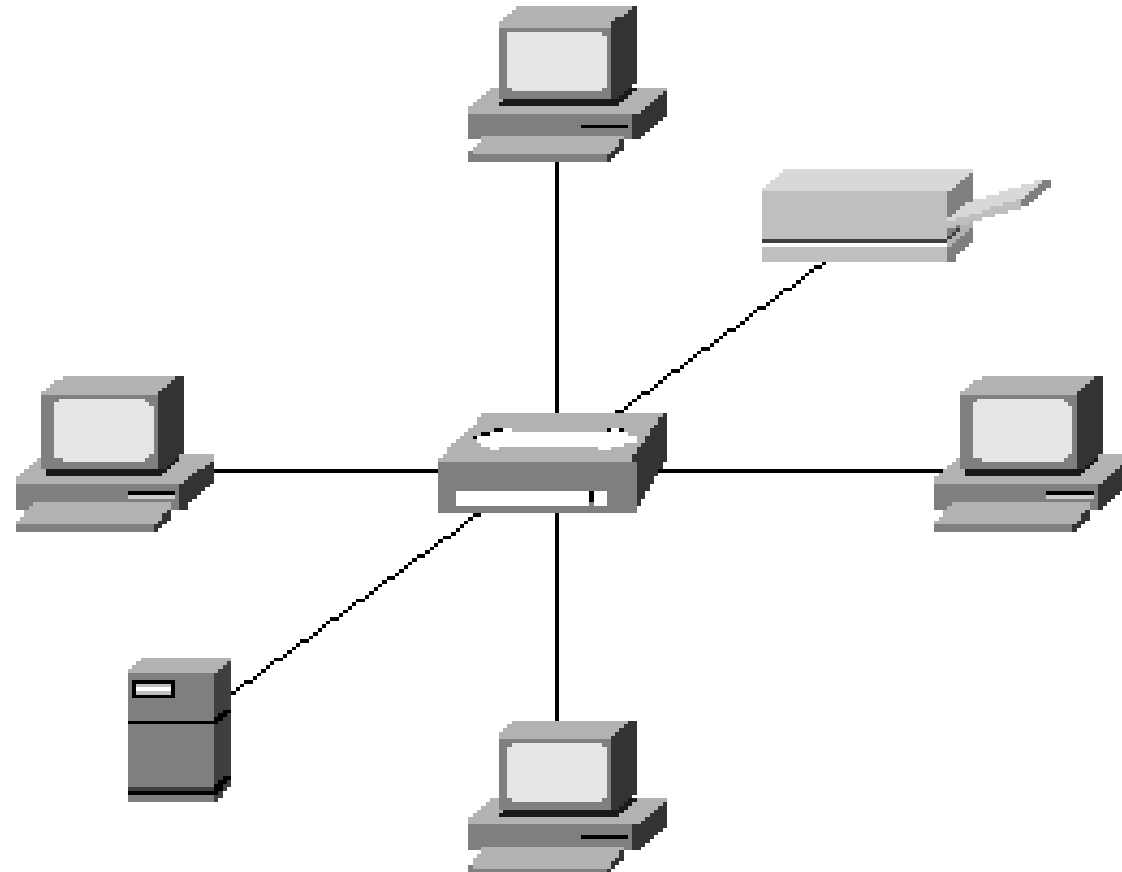
HUB Device

- A HUB is at layer 1 of the OSI model.
- A HUB does not make forwarding decisions.
- A HUB receives bits in on one port and then retransmits those bits out all other ports.
- HUB most often use UTP cabling to connect to other network devices.
- Three basic types of Ethernet HUBs exist.
 - Passive HUB
 - Active HUB
 - Smart HUB (with SNMP)



HUB Device

- Regenerate and repeat signals
- Used as network concentration points
- Multiport repeater



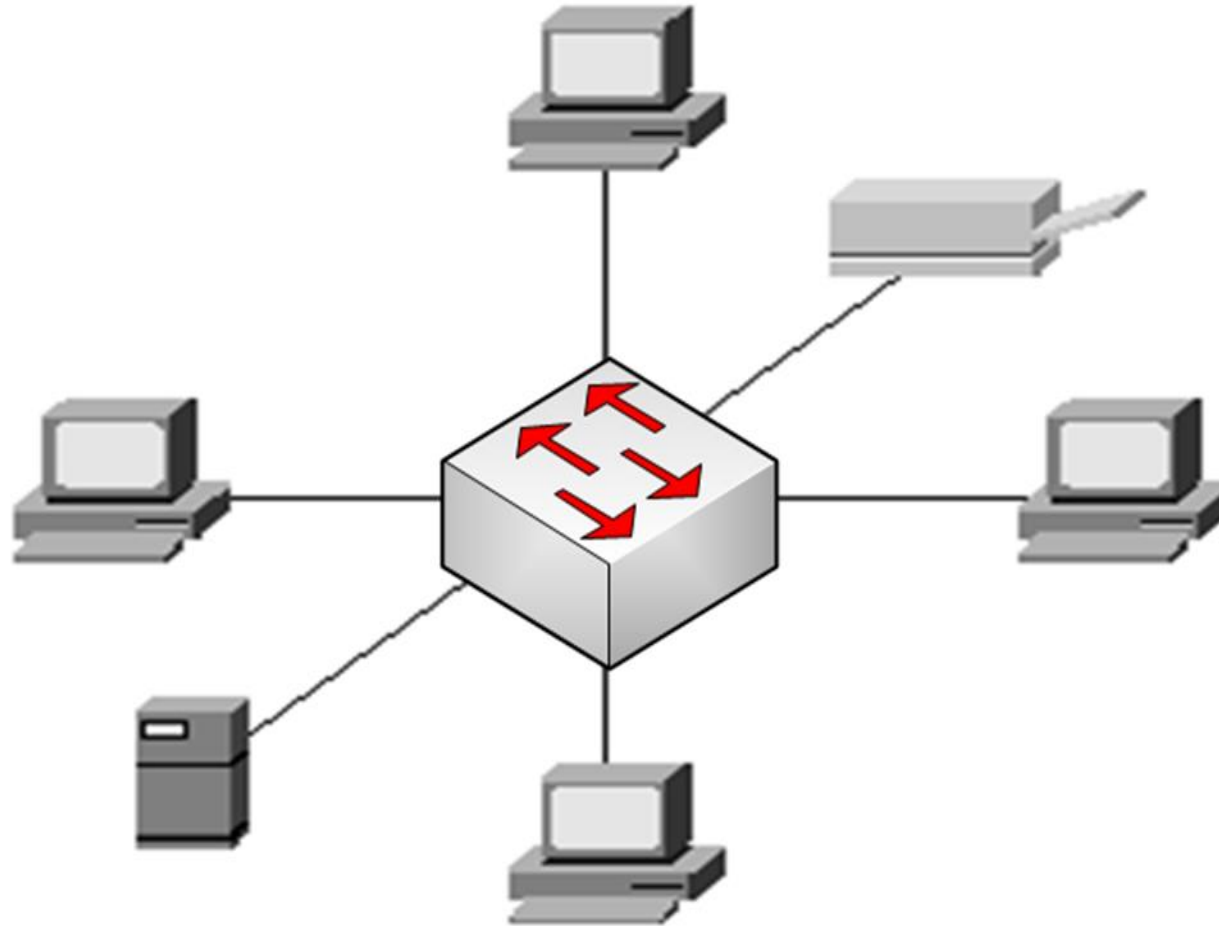
Switches Device

- Like a bridge, switch can dynamically learn the MAC address attached to various ports by looking at the source MAC address on frames coming into a port.
- Initially, however the switch is unaware of what MAC address reside off of which ports.
- When a switch receives a frame destined for a MAC address not yet present in the switch's MAC address table, the switch floods that frame out of all of the switch port, other than the port on which the frame arrived.



Switches Device

Designed to create two or more LAN segments, each of which is a separate collision domain



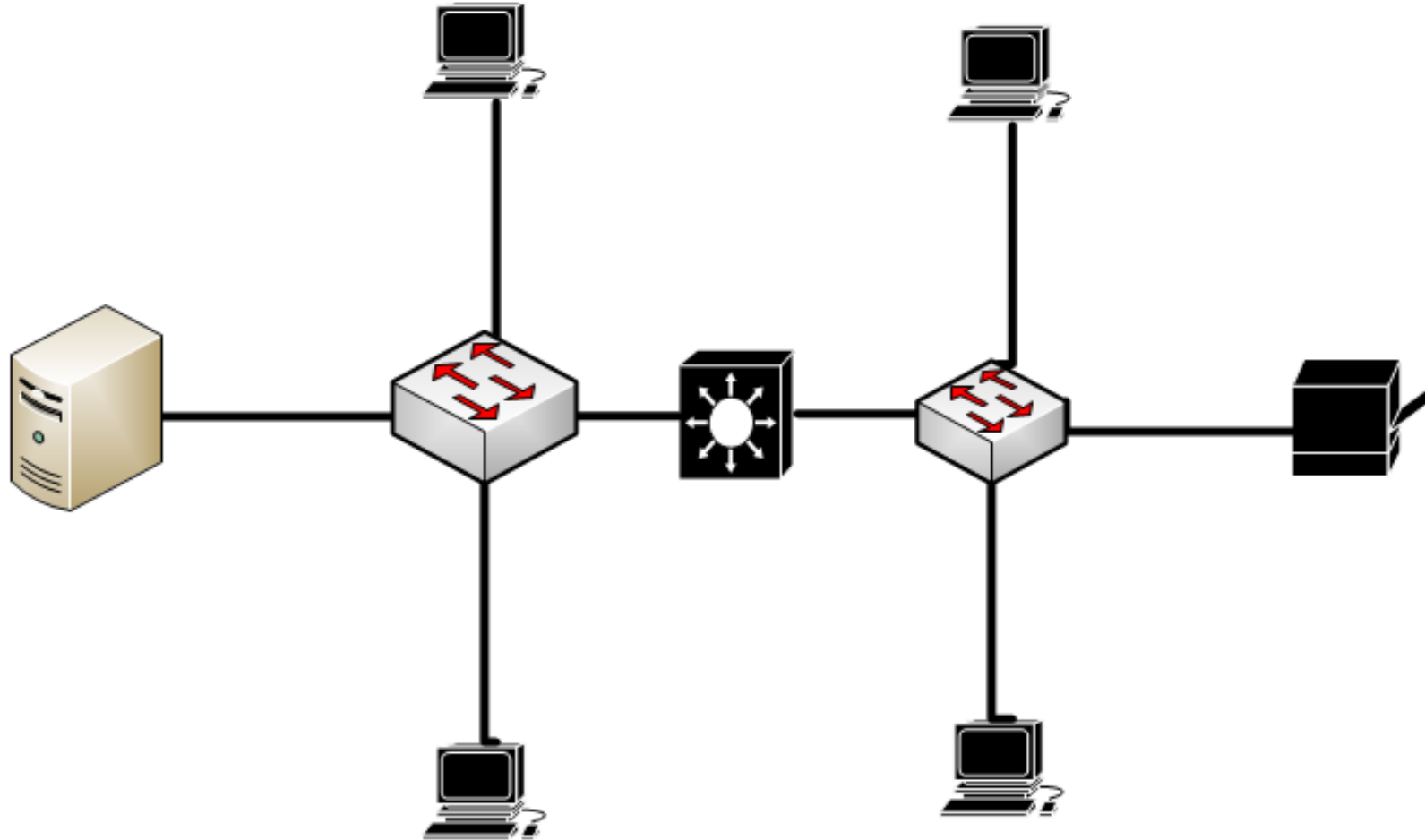
Multilayer Switches

- Although a Layer 2 switch, makes forwarding decisions based on MAC address information, a multilayer switch can make forwarding decisions based on upper-layer information.
- A multilayer switch could function as a router, and make forwarding decisions on IP address information.



Multilayer Switches

Eight collision Domains, Two Broadcast Domain



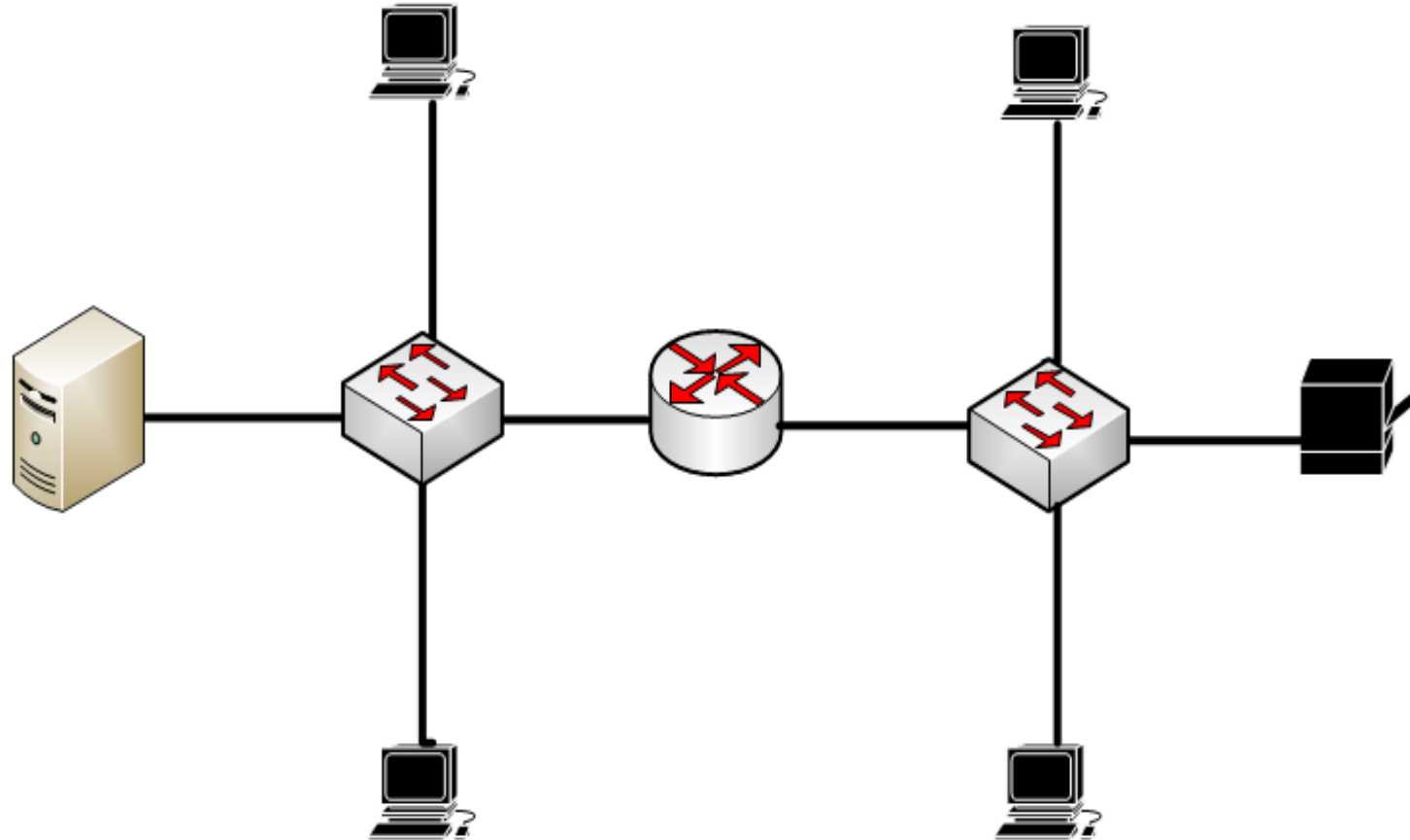
Routers Device

- A Router is a layer 3 device, meaning that it makes forwarding decisions based on logical network address information. Such as IP addresses.
- A router has the capability to consider high-layer traffic parameters in making its forwarding decisions.
- Each port on a Router is a separate collision domain and a separate broadcast domain.
- Routers are typically more feature-rich and support a broader range of interface types.



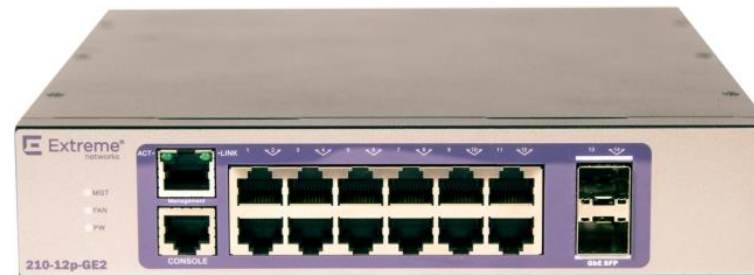
Routers Device

Eight collision Domains, Two Broadcast Domain



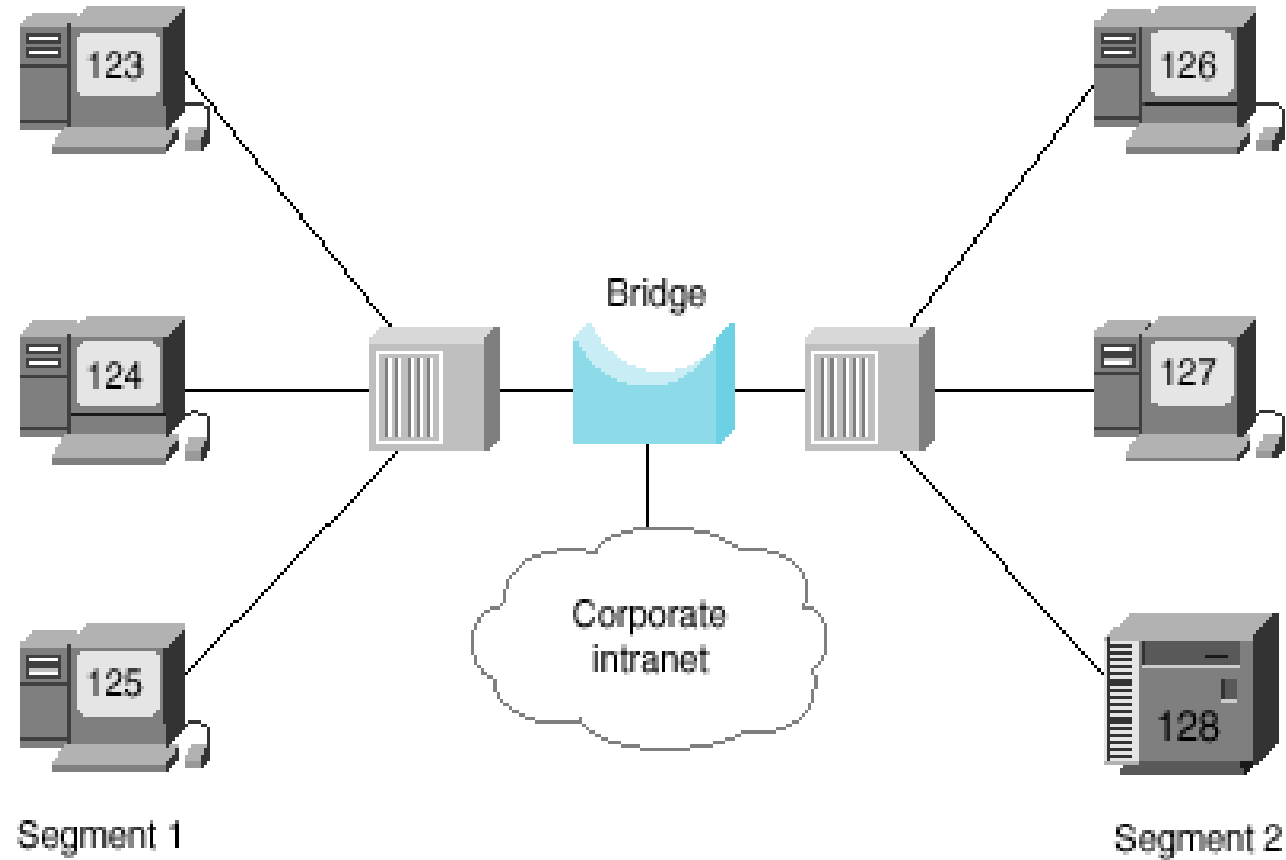
Bridges Device

- A bridge joins together two or more LAN segments, typically two Ethernet LAN segments.
- Each LAN segment is a separate collision domain.
- A bridge makes intelligent forwarding decisions based on the destination MAC address present in a frame.
- A bridge analyzes source MAC address information on frames entering the bridge and populates an internal MAC address table based on learned information.



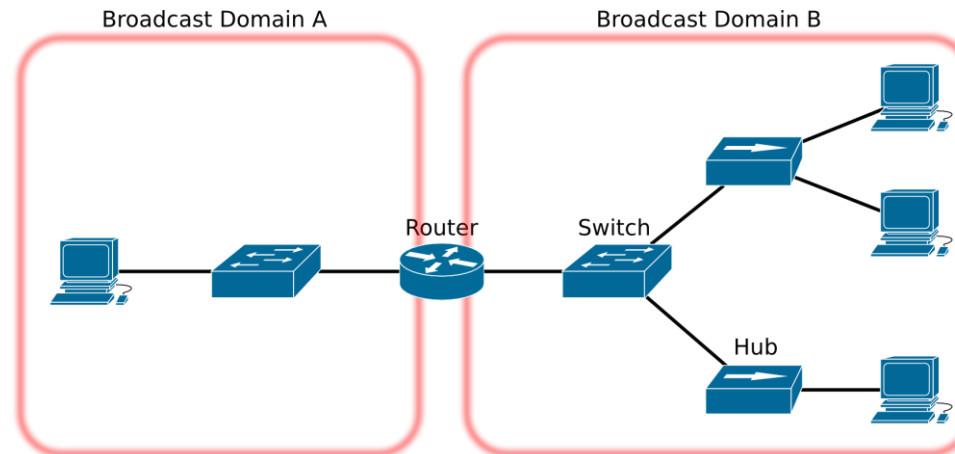
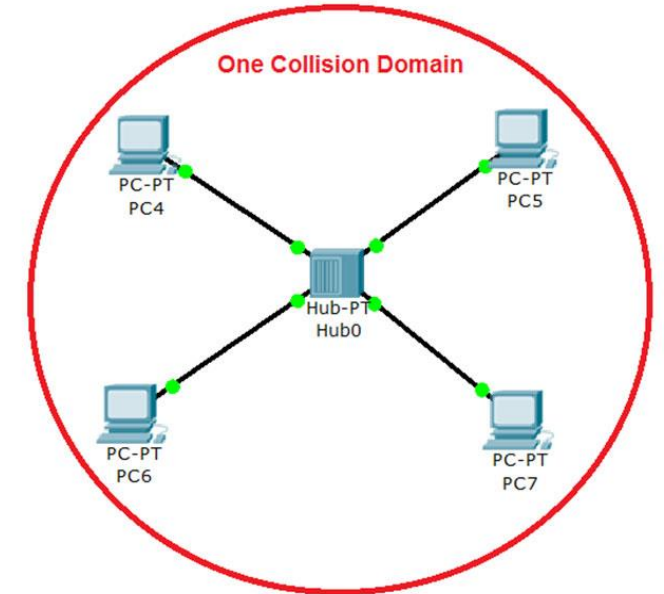
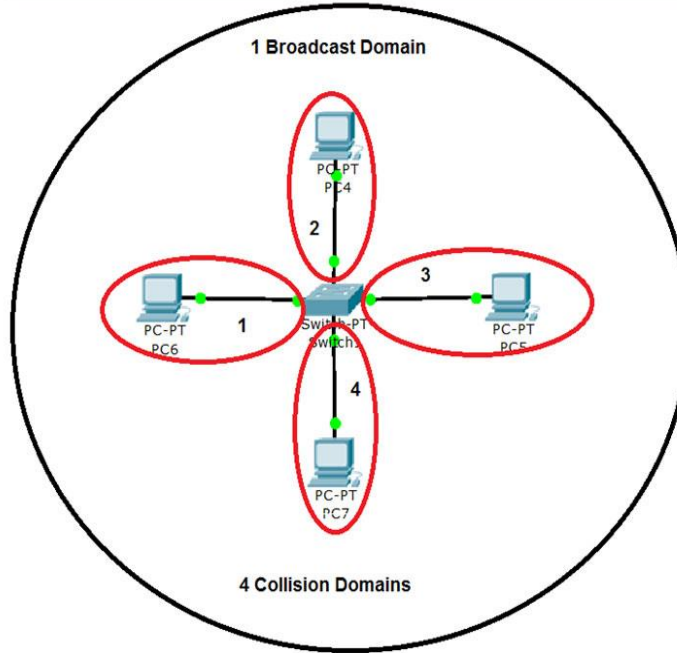
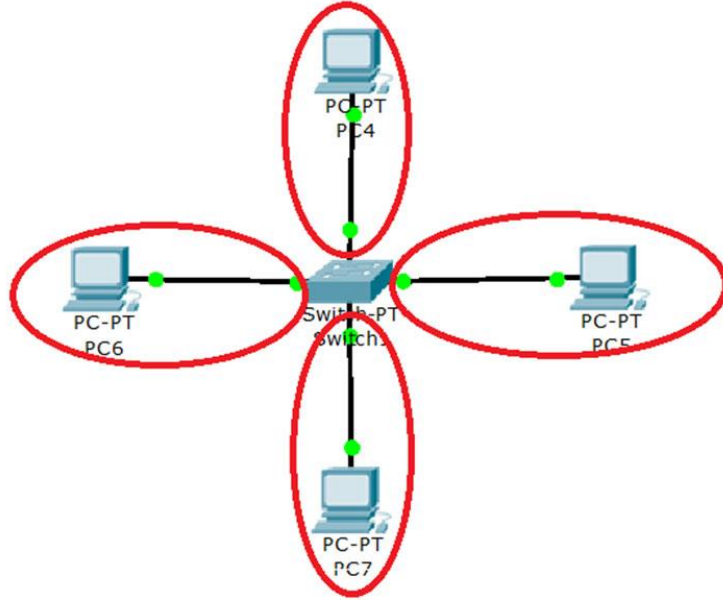
Bridges Device

Designed to create two or more LAN segments, each of which is a separate collision domain



Infrastructure Devices Collision Domain

Each switch port is a collision domain

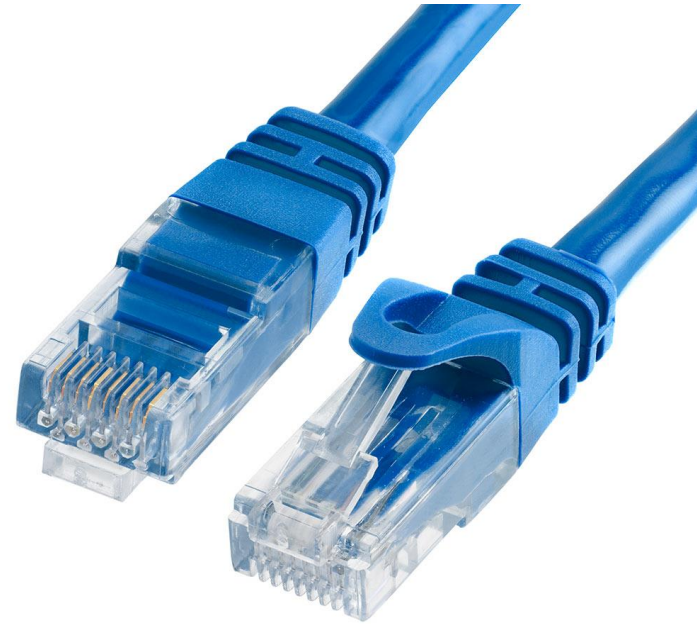


Infrastructure Devices Summary

Device	Number of Collision Domain Possible	Number of Broadcast Domains Possible	OSI Layer of Operation
HUB	1	1	1
Bridge	1 per port	1	2
Switch	1 per port	1	2
Multilayer switch	1 per port	1 per port	3+
Router	1 per port	1 per port	3+

Objectives Media

- What are the characteristics of various media types?
- What is the role of a given network infrastructure component?
- What features are provided by specified specialized network devices?
- How are virtualization technologies impacting traditional corporate data center designs?
- What are some of the primary protocols and hardware components found in a Voice over IP(VoIP) network?



Identify Network Components

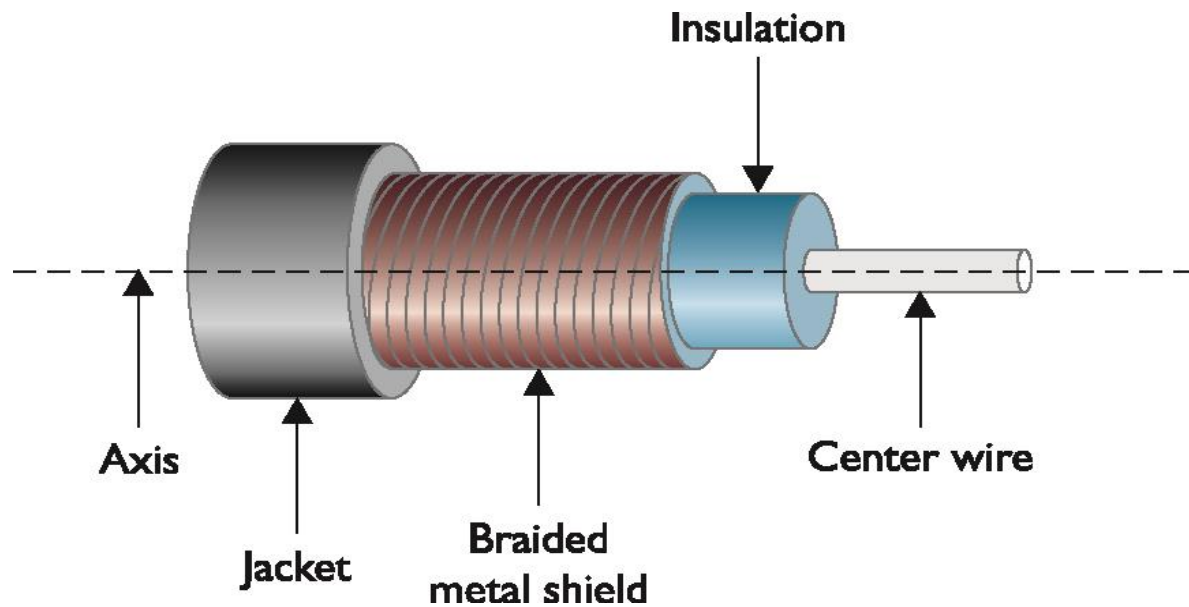
- Many modern networks contain a daunting number of devices.
- It is our job to understand the function of each device and how they work with each other.
- The interconnection of these devices uses one of a variety of media (cables) types.

The Media

- By definition, a network is an interconnection of devices. Those interconnections occur over some type of media.
- The media might be physical, such as a copper and fiber-optic cable or it might be the air, through which radio waves propagate.

Coaxial Cable

- Coaxial Cable is composed of two conductors.
- The inner, insulated conductor or center wire, passes the data.
- The outer, braided metal shield, which helps protect the data.



Coaxial Cable

- Three of the most common types of coaxial cables are;
 - RG-6: Commonly used by local cable companies to connect individual homes.
 - RG-58: This type of coaxial cable was popular with early 10BASE2 Ethernet networks.
 - RG-59: Typical used to carry composite video between two nearby devices. (i.e. cable box to TV)
- Although RG-58 was commonplace in early networks, coaxial cables role in modern computer networks is as the media used by cable modems.
- Common connectors used on coaxial cables:

BNC

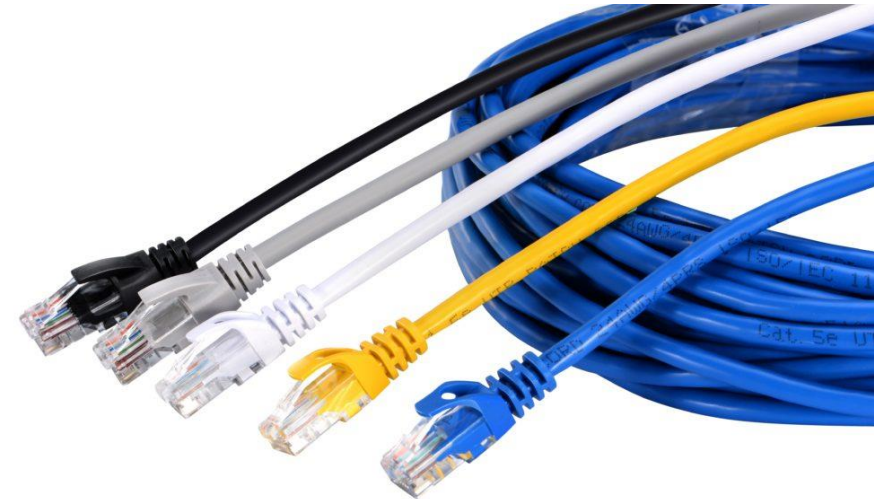


F-connector

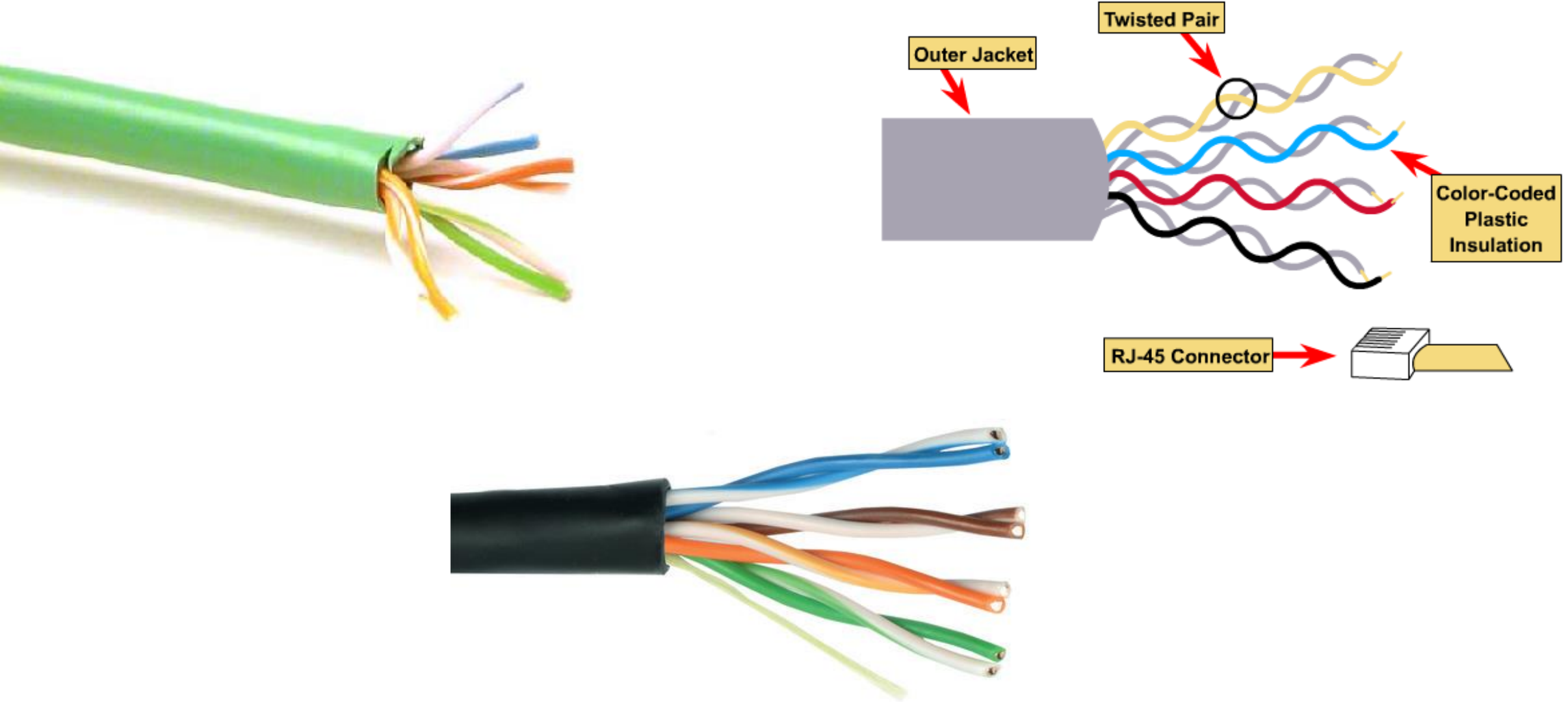


Twisted-Pair Cable

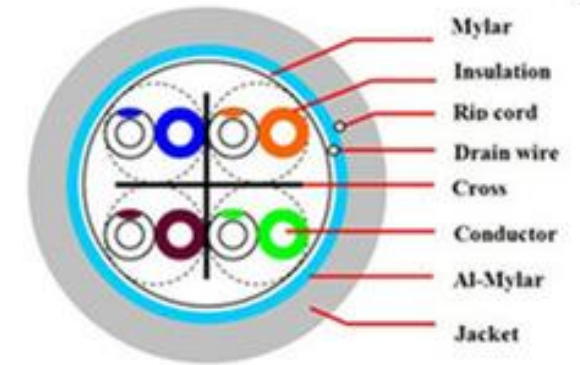
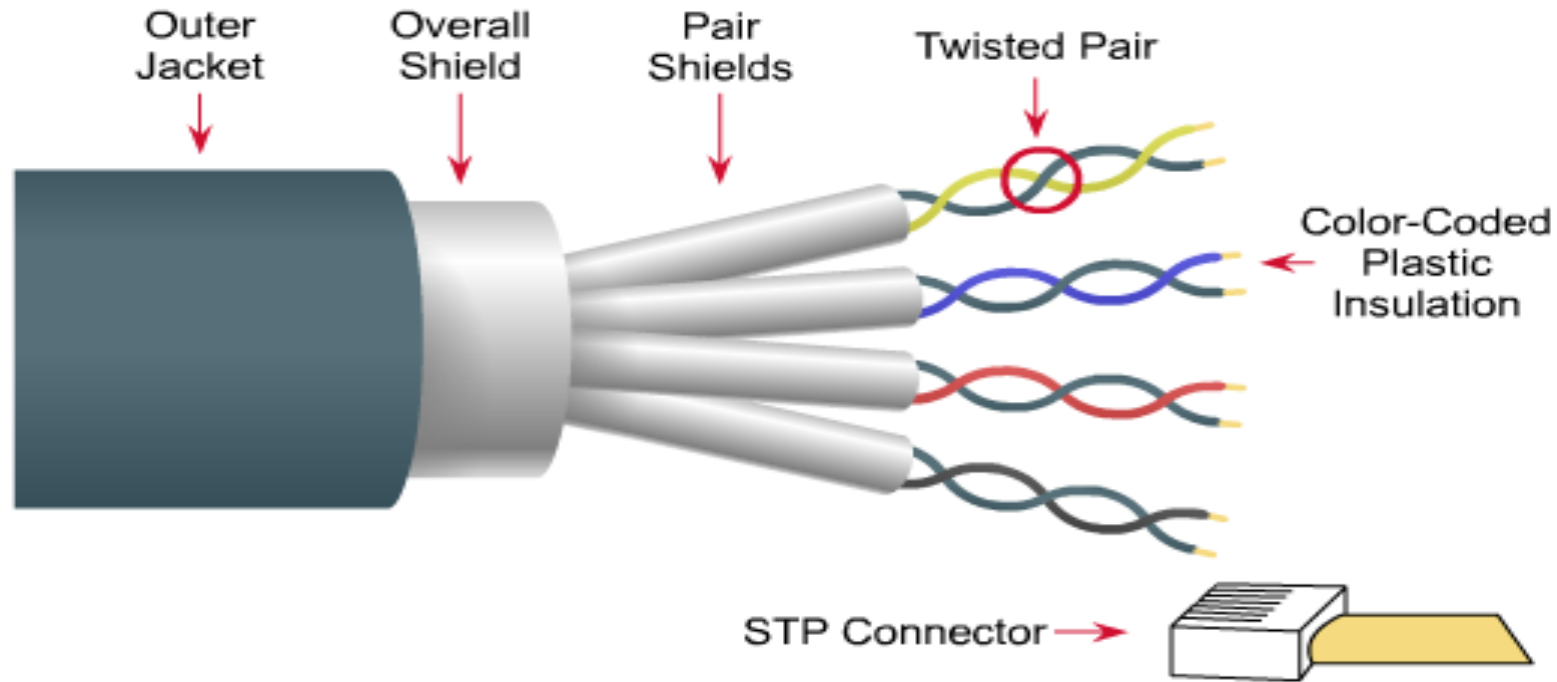
- The most popular LAN media type is twisted-pair cable, where individually insulated copper strands are intertwined into pairs.
- There are two categories of twisted pair:
 - UTP - Unshielded Twisted Pair
 - STP - Shielded Twisted Pair



Unshielded Twisted-Pair Cable



Shielded Twisted-Pair Cable



CAT Ratings

➤ Categories:

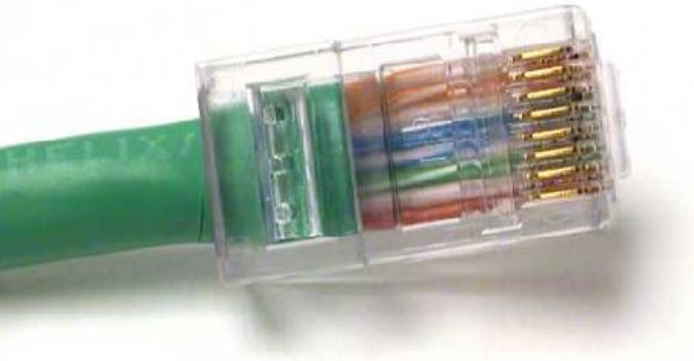
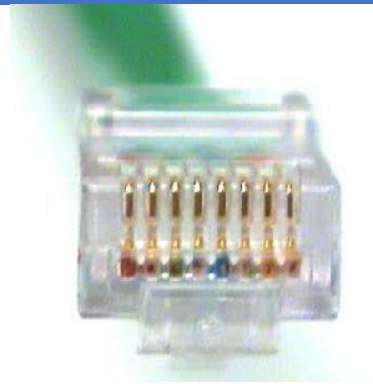
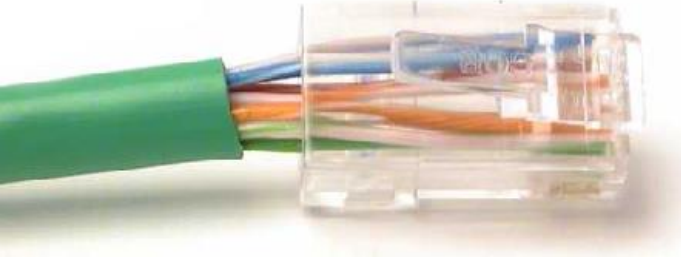
- CAT 3 (Category 3): up to 10 Mbps of data
- CAT 5 (Category 5): up to 100 Mbps throughput
- CAT 5e (Enhanced Category 5): higher twist ratio, up to 1000 Mbps throughput
- CAT 6 (Category 6): six times the throughput of CAT 5, used for 1000BASE-T
- CAT 6e (Enhanced Category 6): reduced attenuation and crosstalk, used for 10GBASE-T networks

Category	Standard	Data rate	Frequency	# of Conductors
Cat 5	100BASE-TX	100 Mbit	100 MHz	4 or 8
Cat 5e	1000BASE-TX	1 Gbit	100 MHz Duplex	8
Cat 6	EIA/TIA 568B2.1	1-10 Gbit*	250 MHz	8
Cat 6A	10GBASE-T	10 Gbit	500 MHz	8
Cat 7	10GBASE-T	10 Gbit	600 MHz	8
Cat 7A	10GBASE-T	10 Gbit	1000 MHz	8
Cat 8	40GBASE-T	40 Gbit	1600-2000 MHz	8
* Depends on length and cable type				

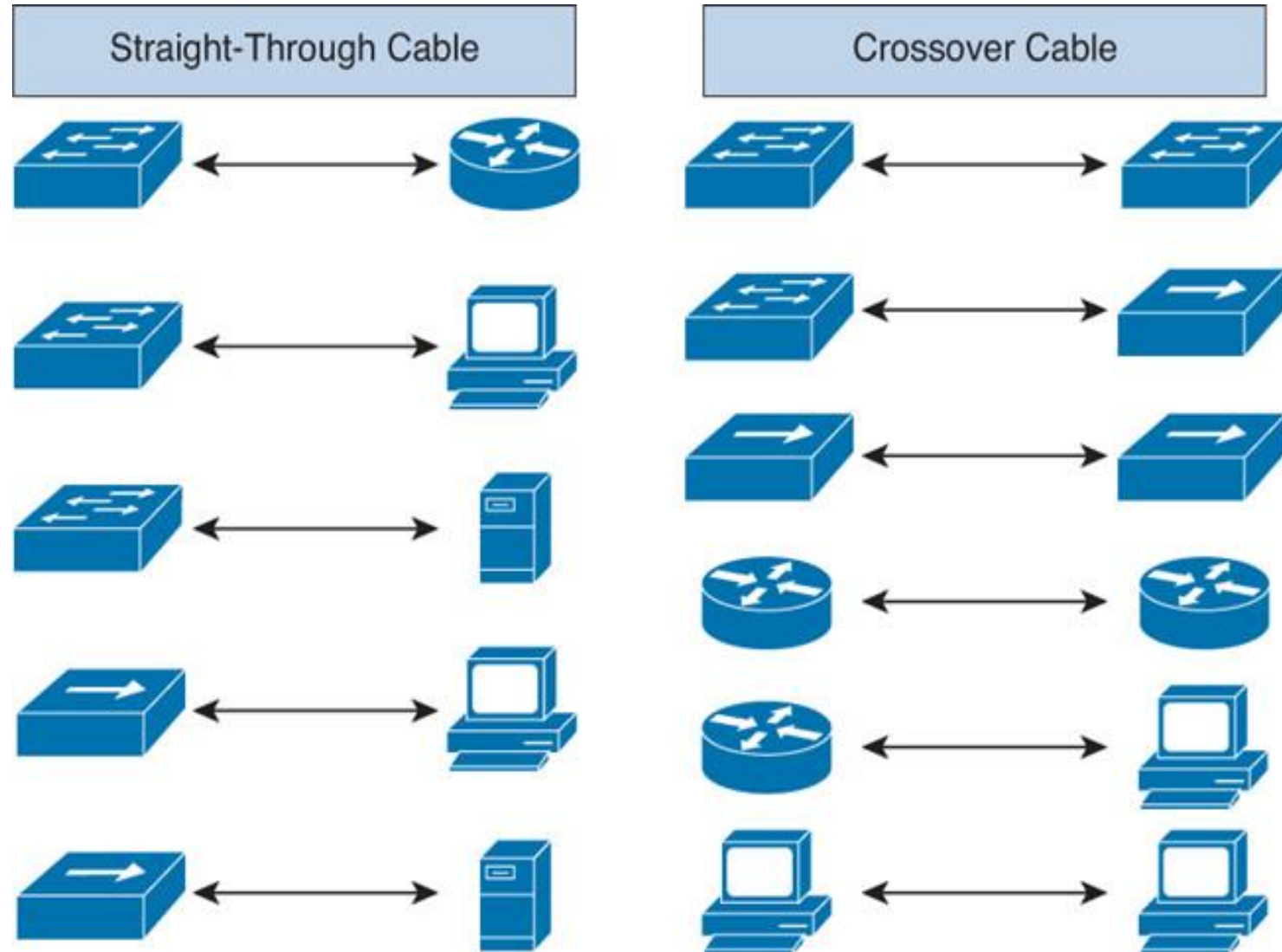
By : Eng. Ahmad Hassan Al-Mashaikh

Email : Ahmad.private.mashaikh@Hotmail.com

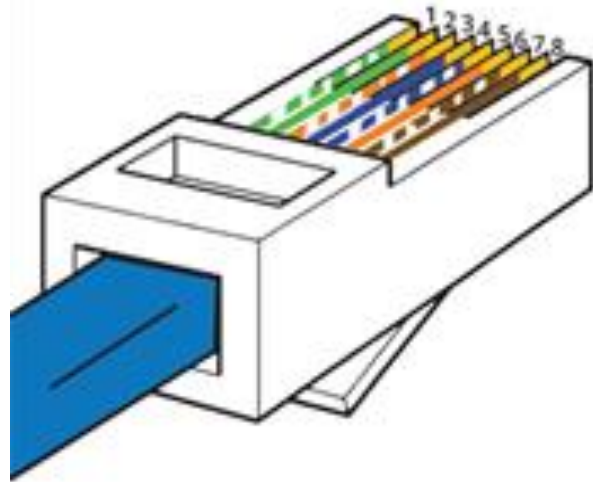
RJ-45



Twisted-Pair Cable

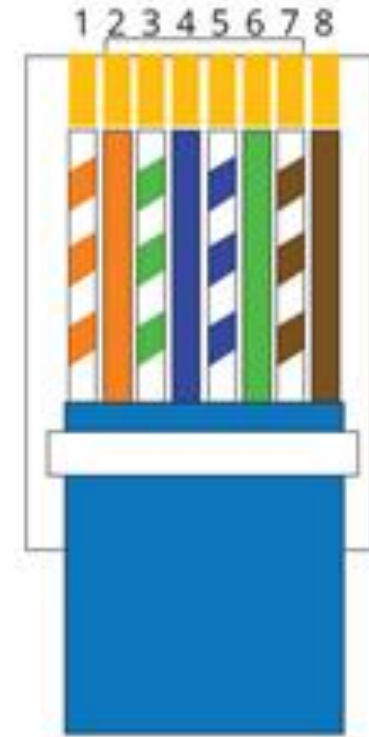
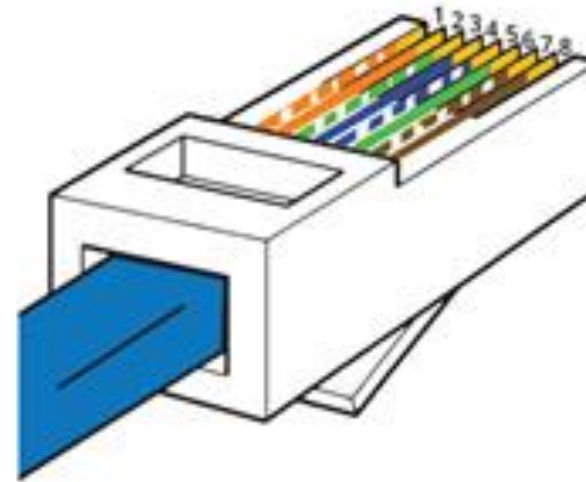


RJ45 Pinout T-568A



- | | |
|-----------------|----------------|
| 1. White Green | 5. White Blue |
| 2. Green | 6. Orange |
| 3. White Orange | 7. White Brown |
| 4. Blue | 8. Brown |

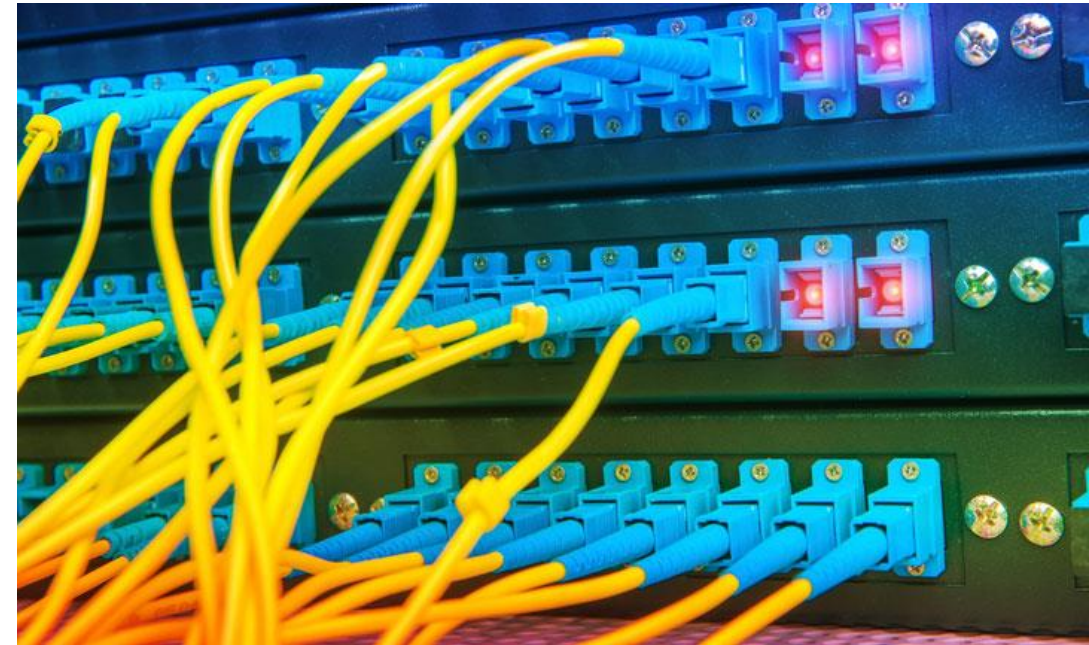
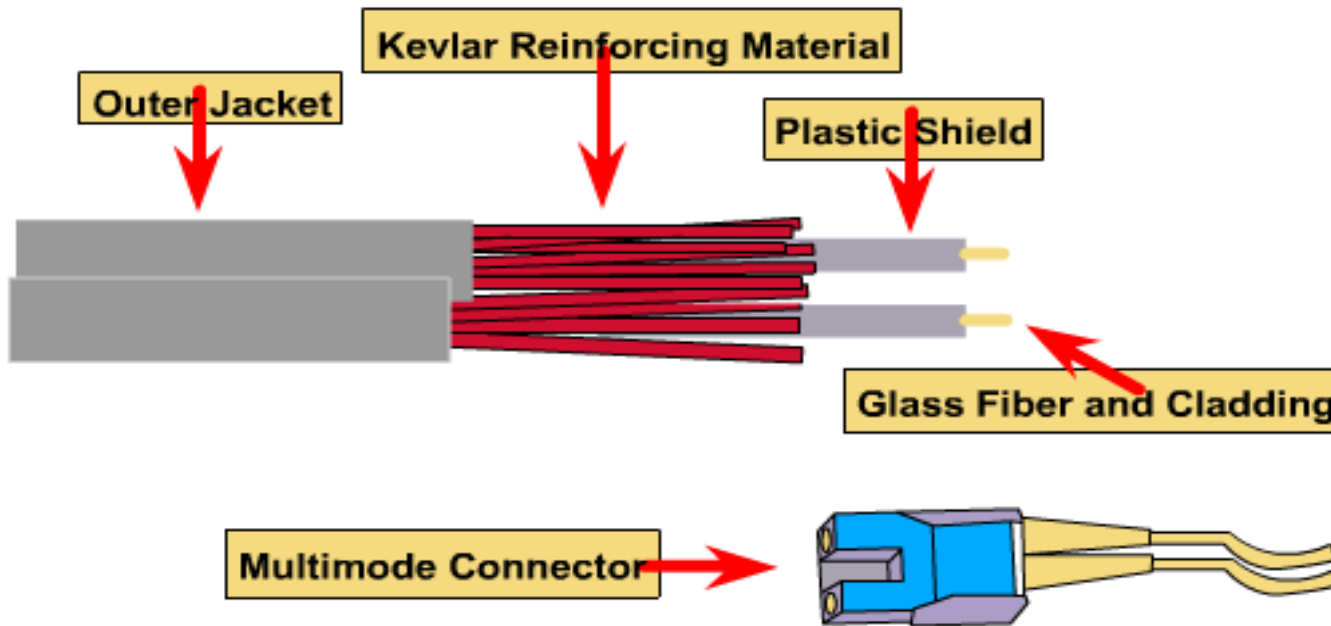
RJ45 Pinout T-568B



- | | |
|-----------------|----------------|
| 1. White Orange | 5. White Blue |
| 2. Orange | 6. Green |
| 3. White Green | 7. White Brown |
| 4. Blue | 8. Brown |

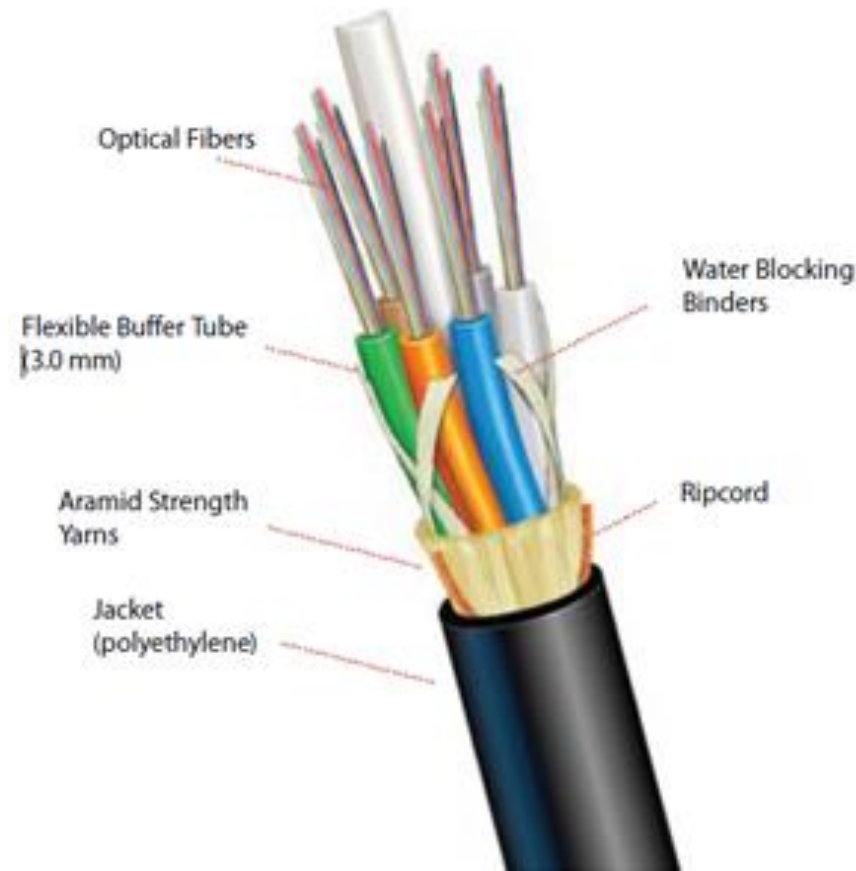
Fiber-Optic Cables

- Contains glass or plastic fibers at core surrounded by layer of glass or plastic cladding
- Reflects light back to core

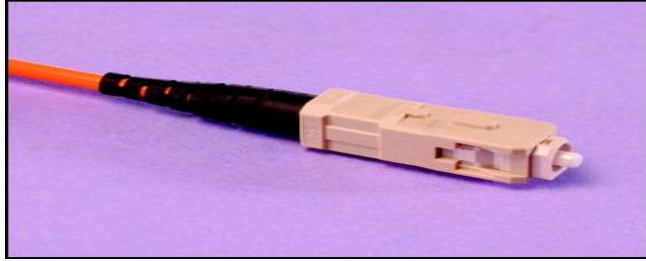


Fiber-Optic Cables

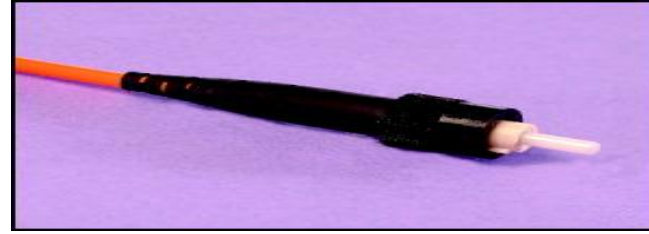
- Benefits over copper cabling:
- Nearly unlimited throughput
- Very high resistance to noise
- Excellent security
- Ability to carry signals for much longer distances before requiring repeaters than copper cable
- Industry standard for high-speed networking



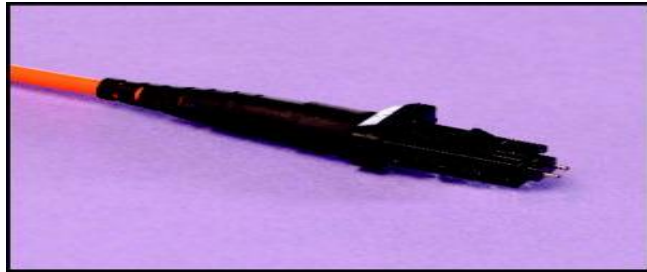
Common Connectors for Fiber



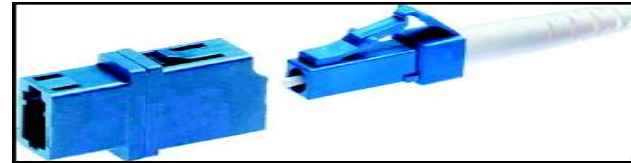
ST (straight tip) connector



SC (subscriber connector or
standard connector)



LC (local connector)



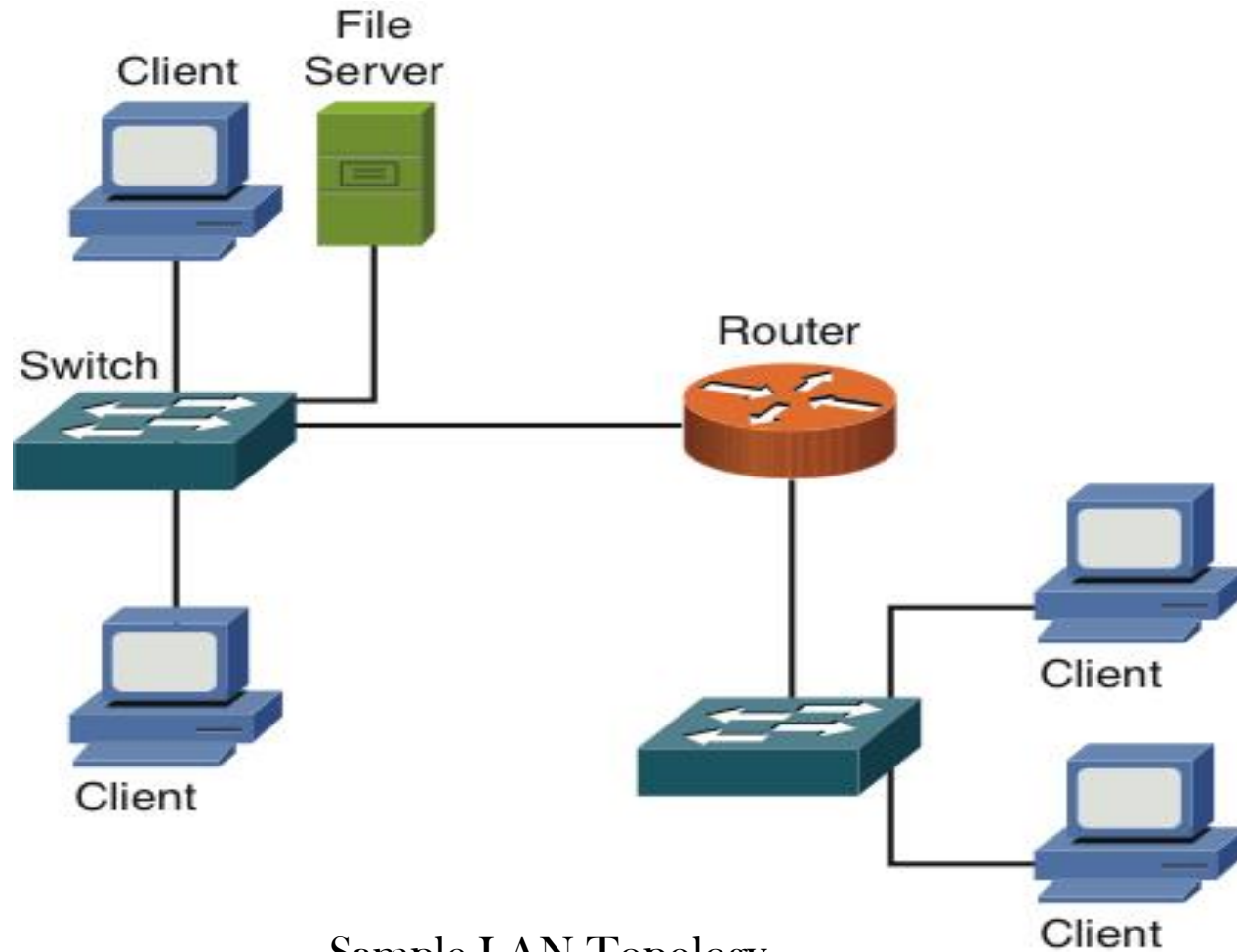
MT-RJ (mechanical transfer-
register jack) connector

Network Defined by Geography

- Local-area network (LAN)
- Wide-area network (WAN)
- Campus-area network (CAN)
- Metropolitan-area network (MAN)
- Personal-area network (PAN)

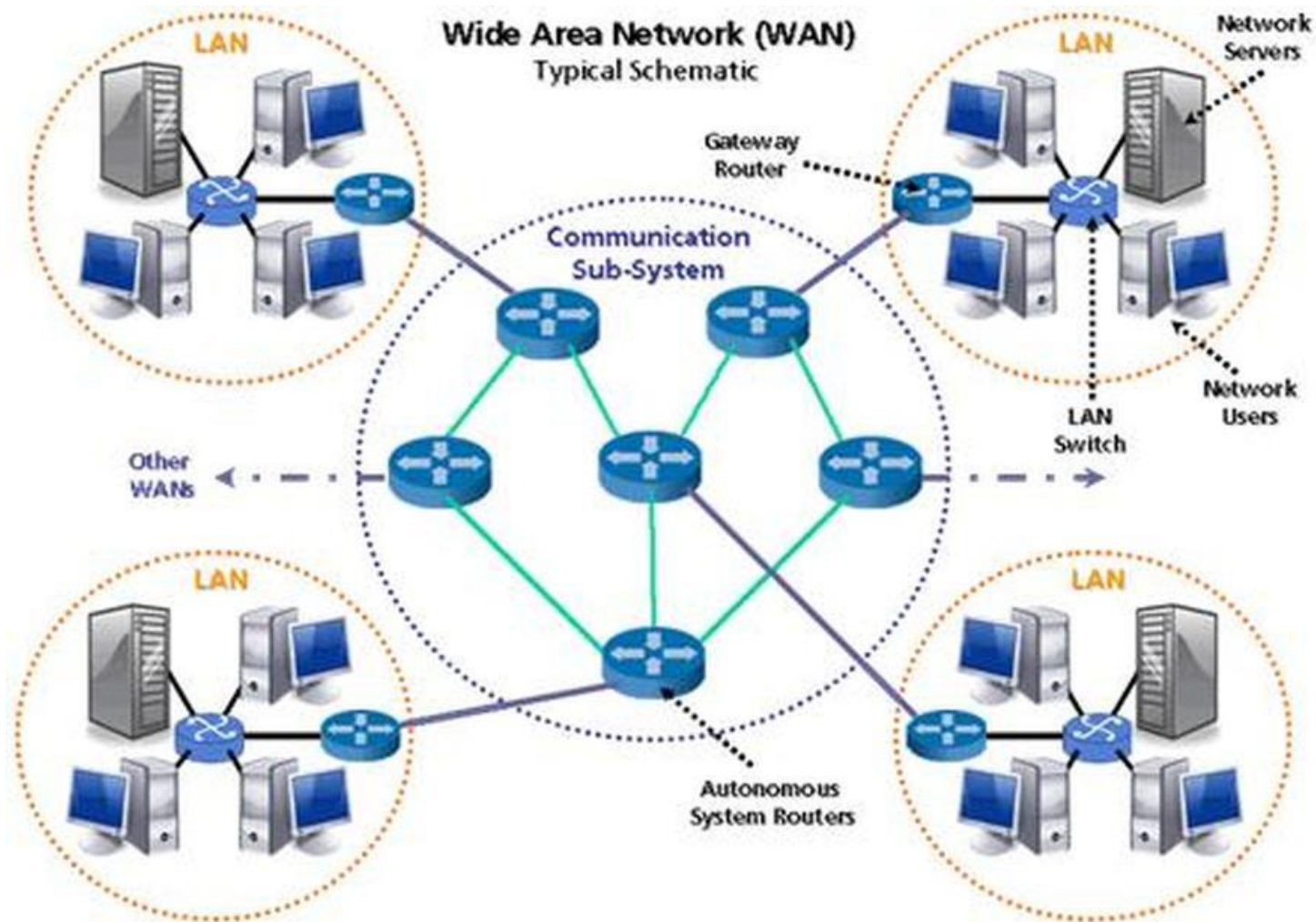


- Local-area network (LAN)



Sample LAN Topology

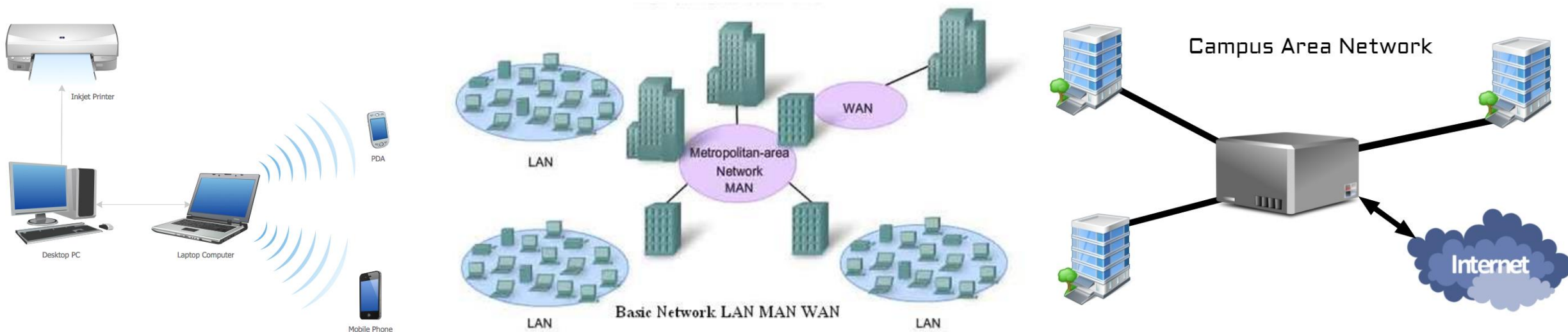
- Wide-area network (WAN)



Sample WAN Topology

Other Area Networks

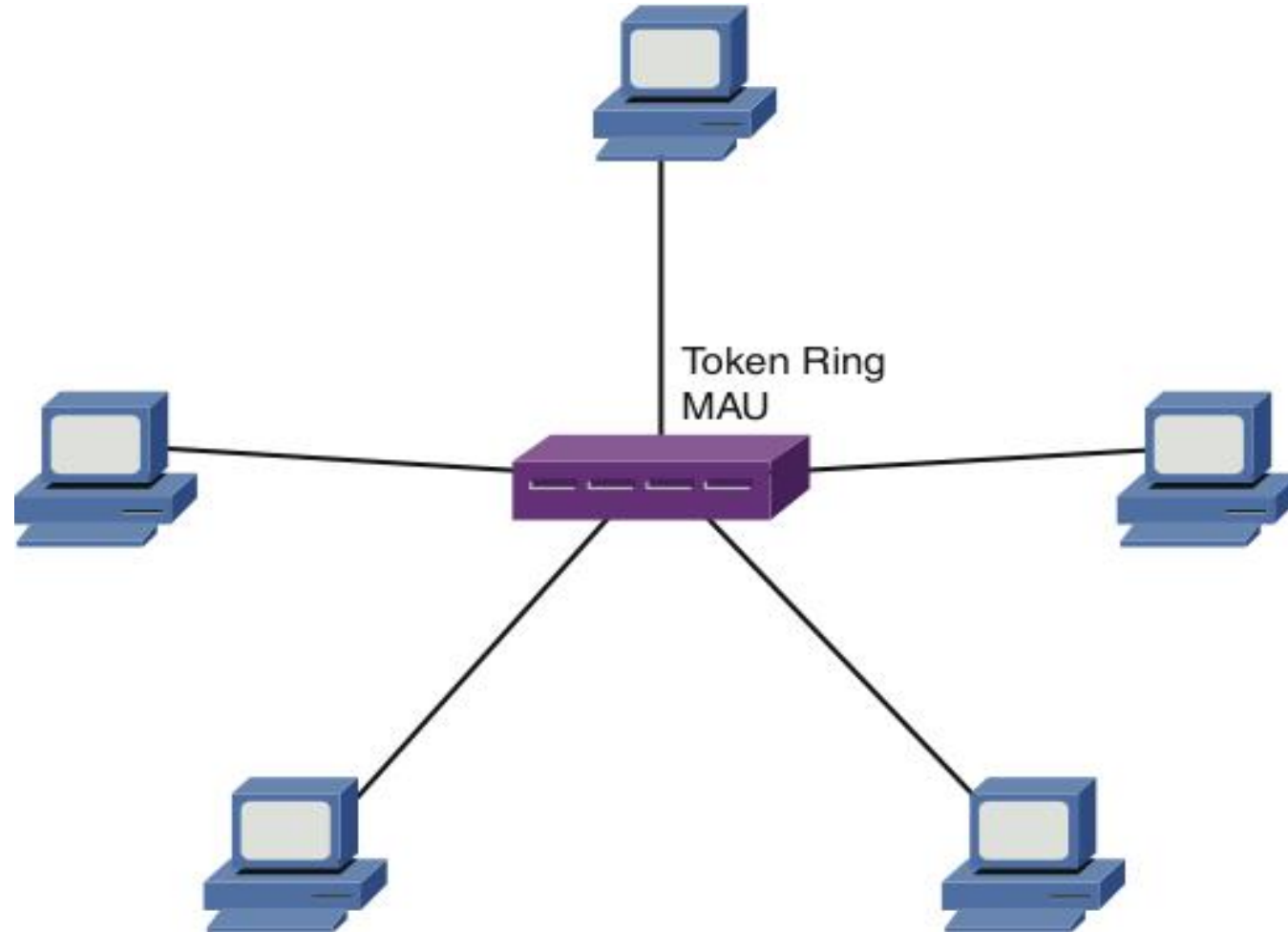
- **CAN:** A CAN is created from interconnecting multiple LANs
- **MAN:** A MAN is between a LAN and a WAN, typically covering a metropolitan area such as three office branches in the same city.
- **PAN:** A PAN is created from the interconnection of personal devices such as a phone, headset, and portable tablet.



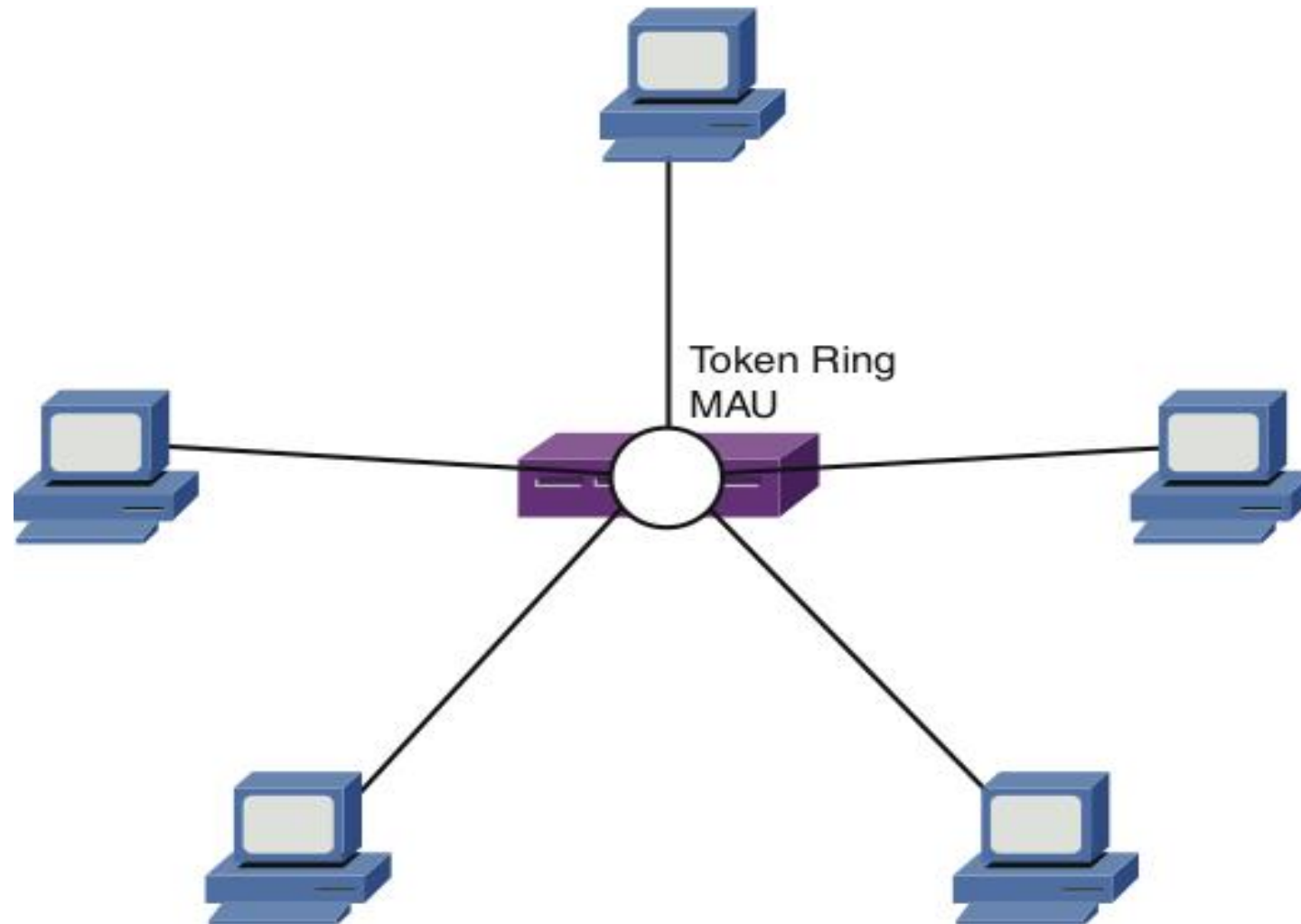
Network Defined by Topology

- In addition to classifying networks based on the geographical placement of their components, another approach to classifying a network is to use the networks **topology**.
- There are two major topology groupings
 - Physical Topology
 - Logical Topology
- Physical Versus Logical Topology
 - Physical Topology -- how components are physical interconnected determines the physical topology
 - Logical Topology -- the actual traffic flow determines the logical topology

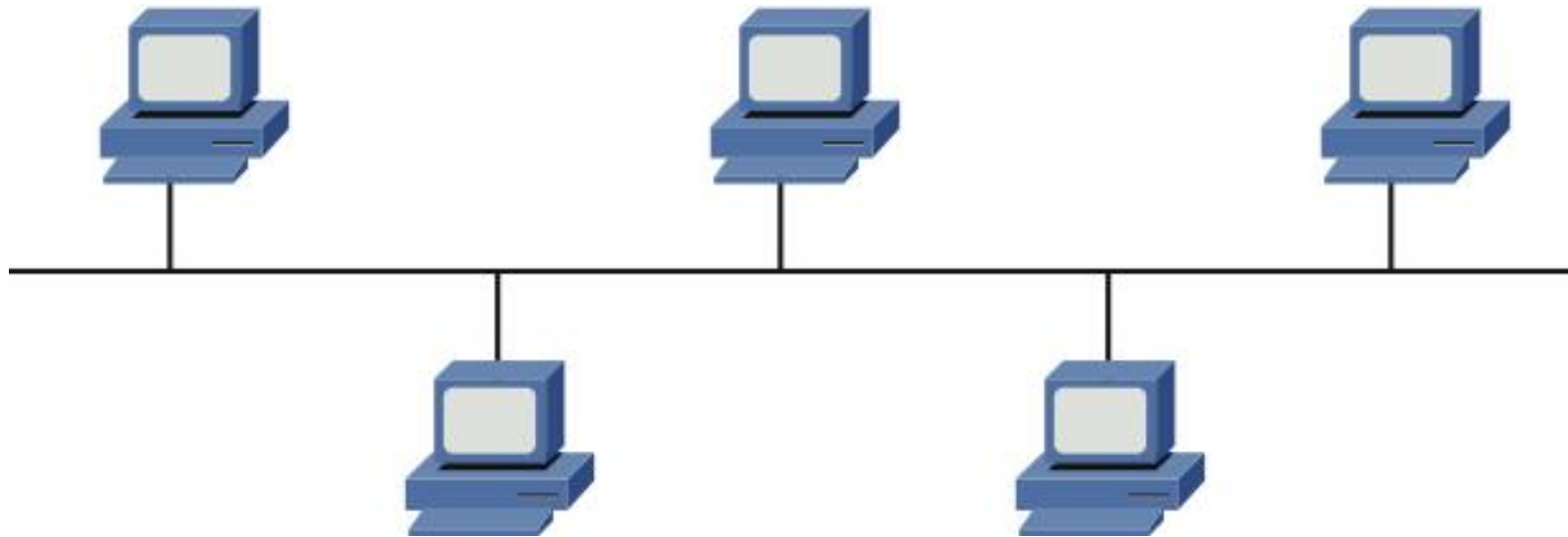
Physical Star Topology



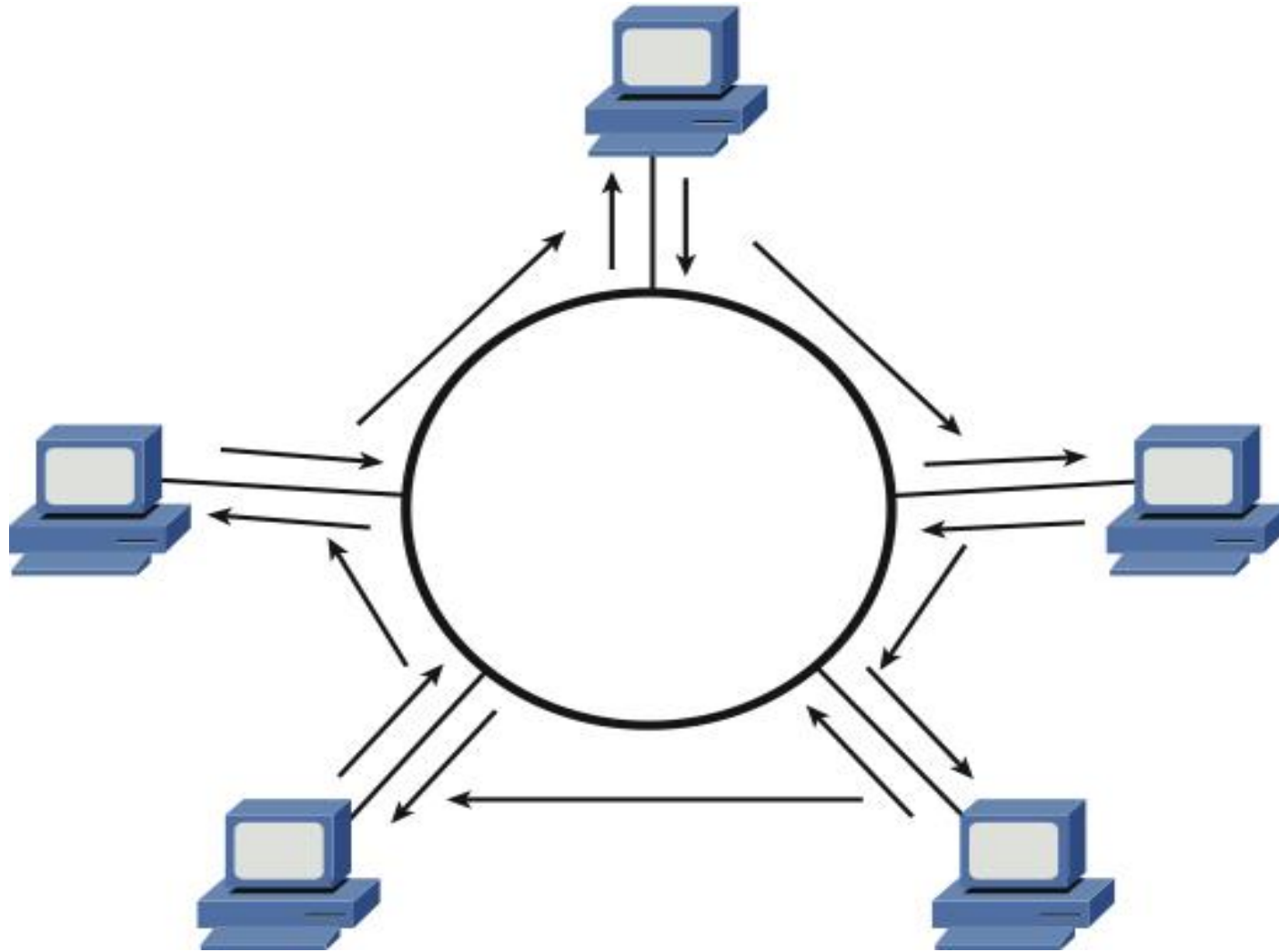
Logical Ring Topology



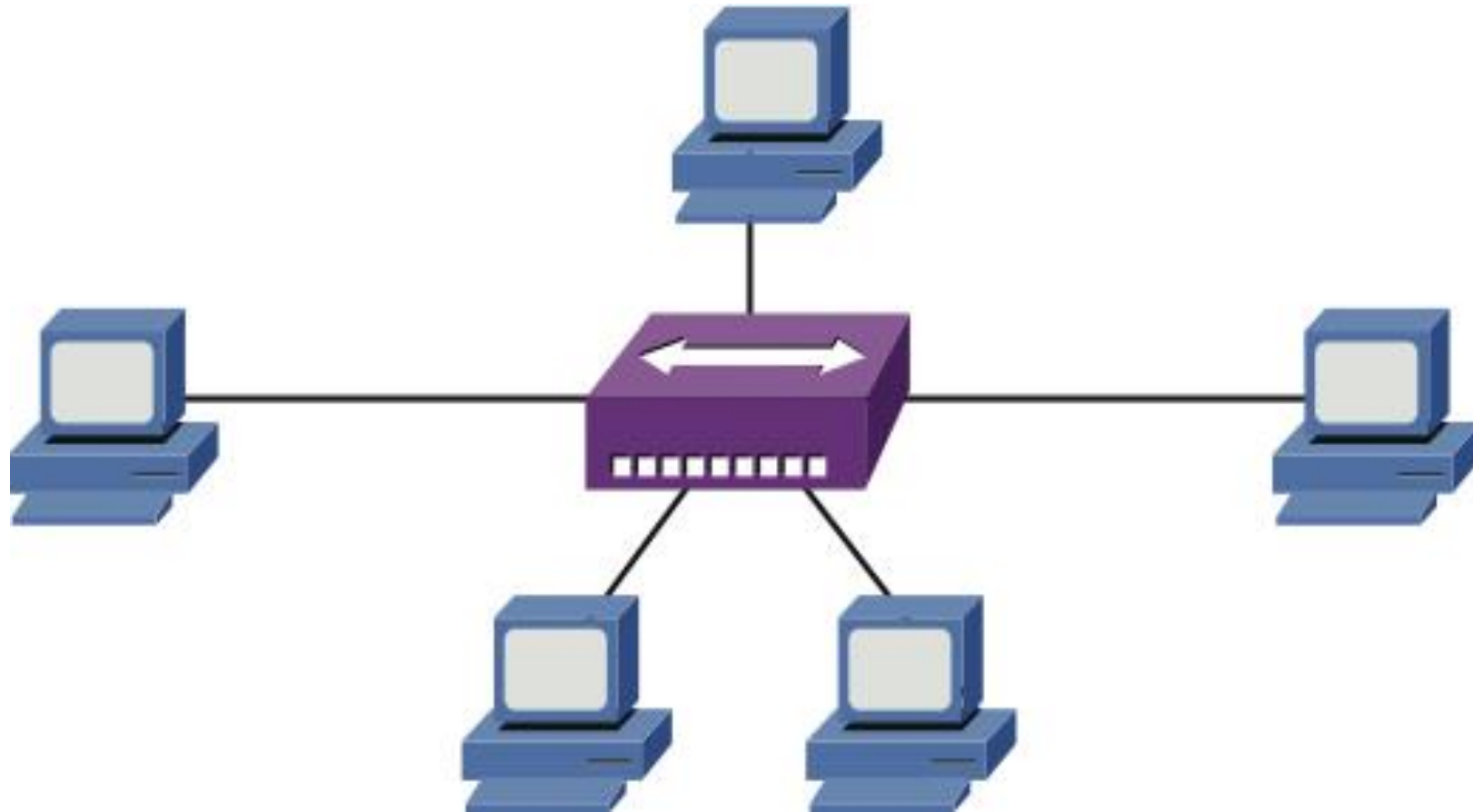
Bus Topology



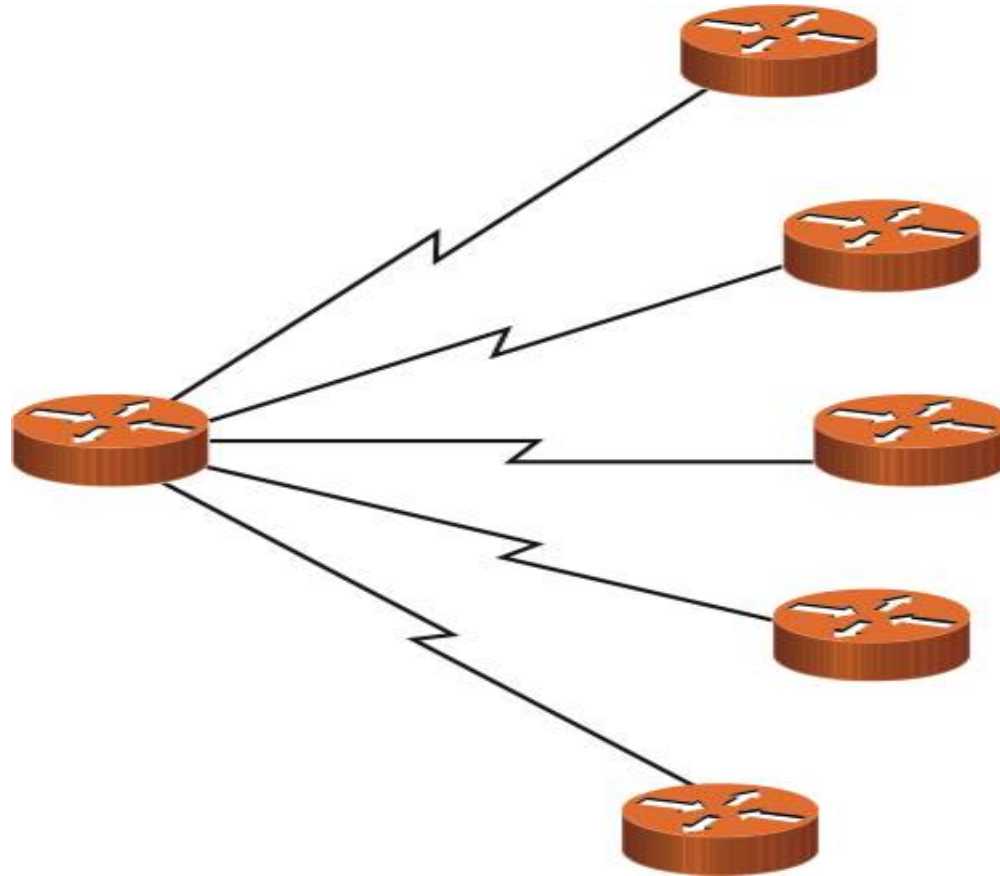
Ring Topology



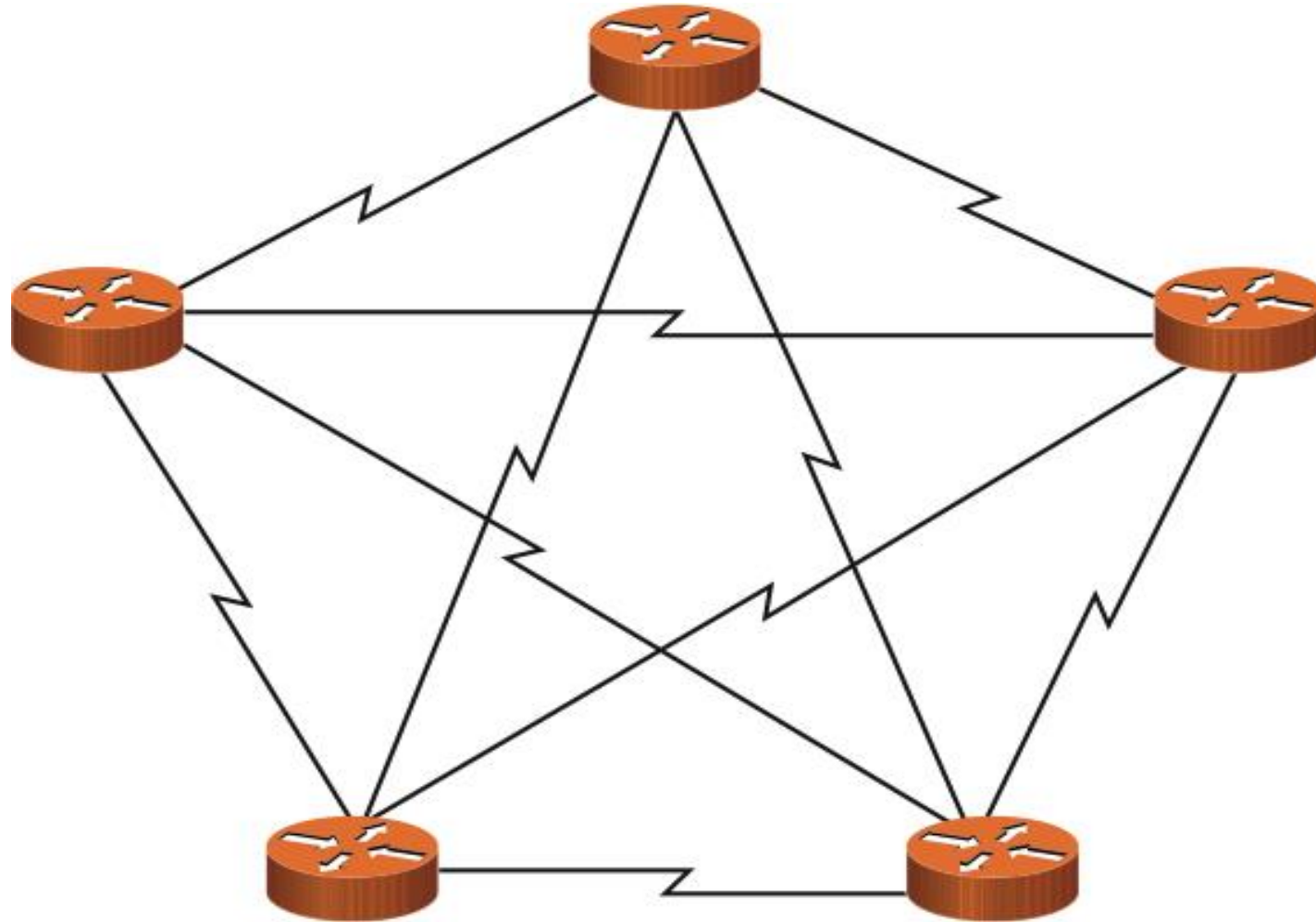
Star Topology



Hub-and-Spoke Topology

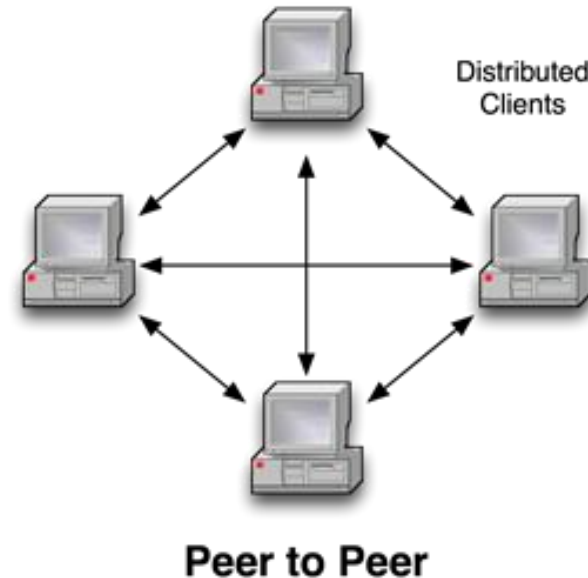
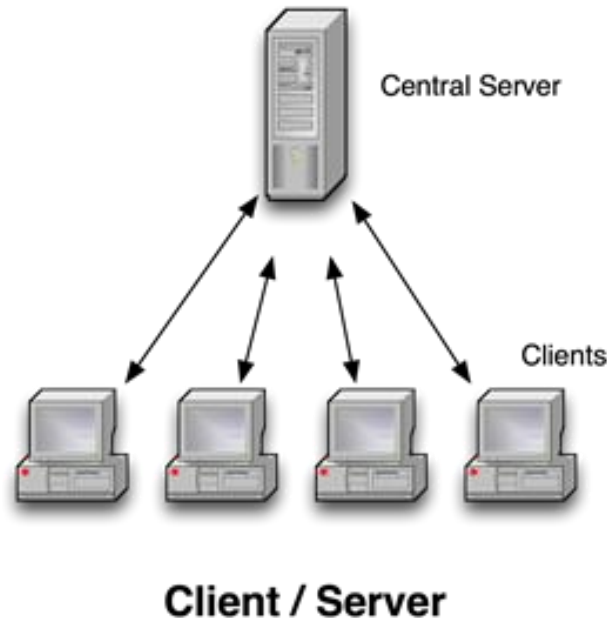


Full-Mesh Topology

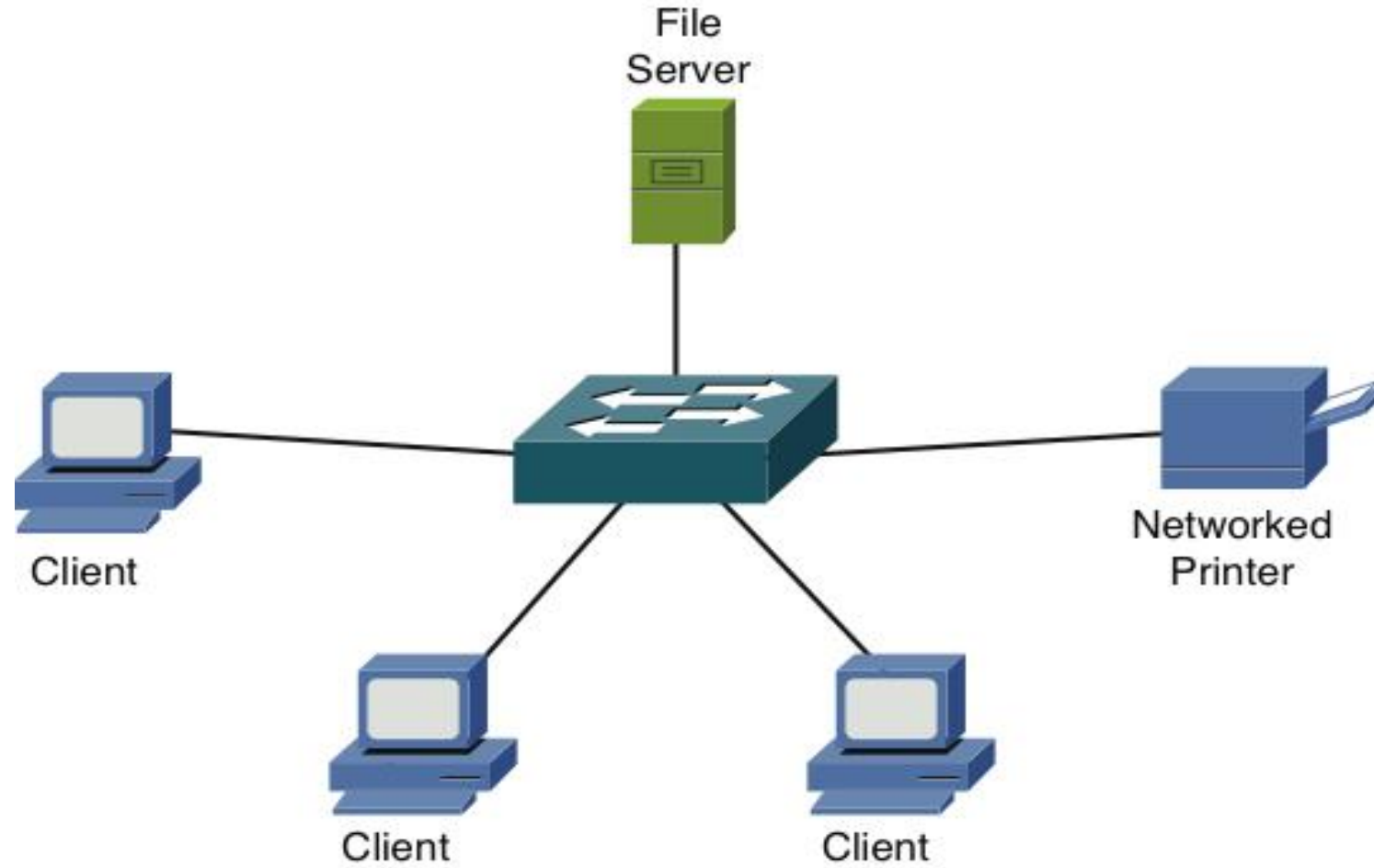


Network Defined by Resource Location

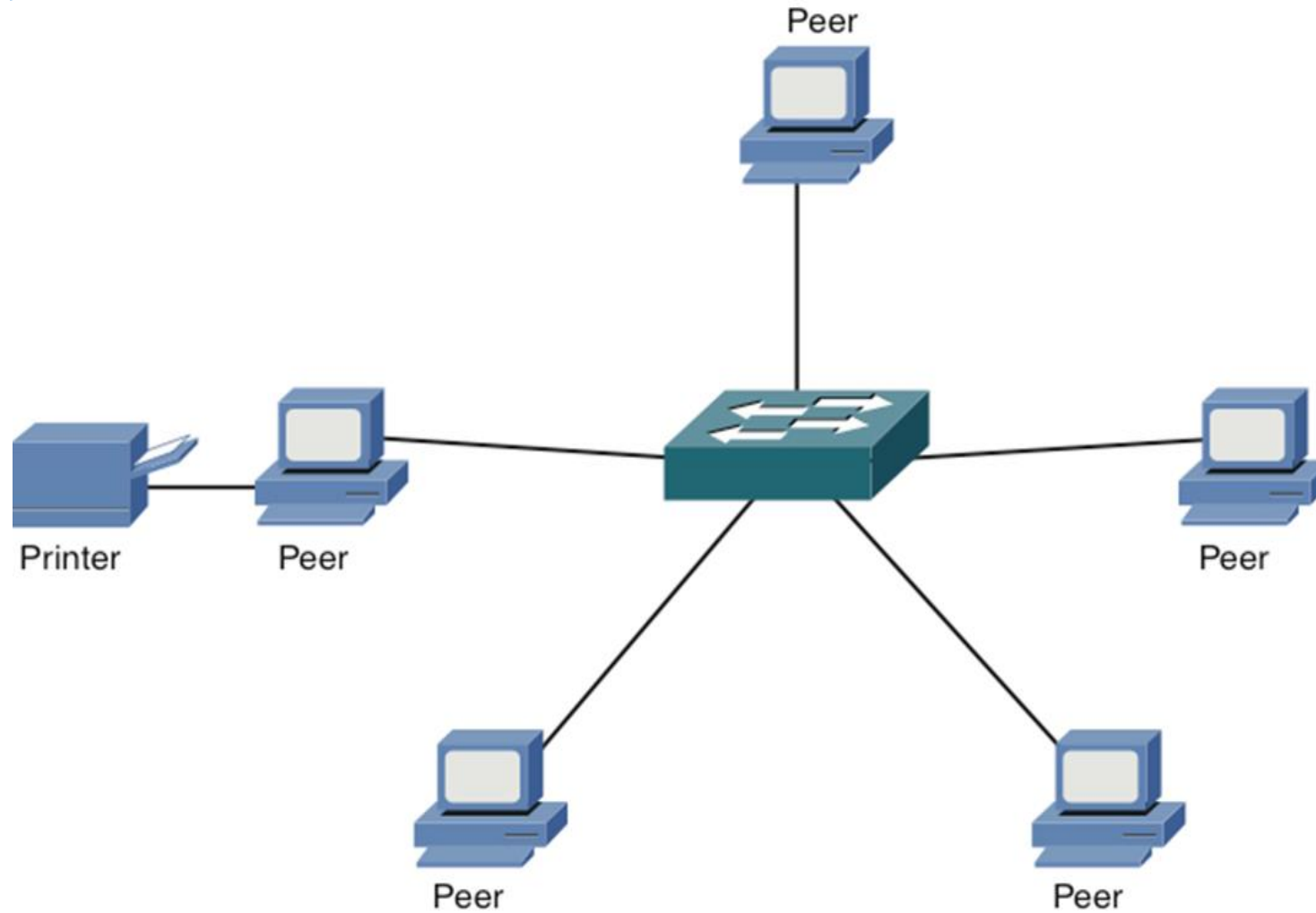
- Yet another way to categorize networks is based on where network resources reside.
- Network that have all the resources residing in a server are called **client -server networks**.
- Network that have their resources on several clients and no server is called a **peer-to-peer network**



Client-Server Network

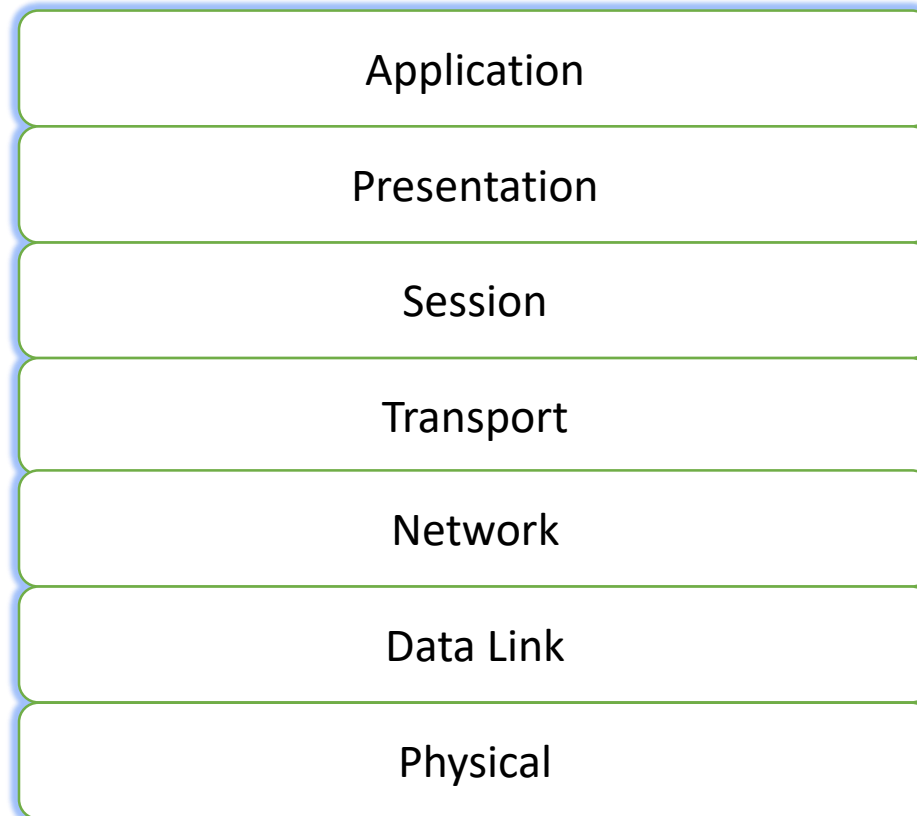


Peer-to-Peer Network



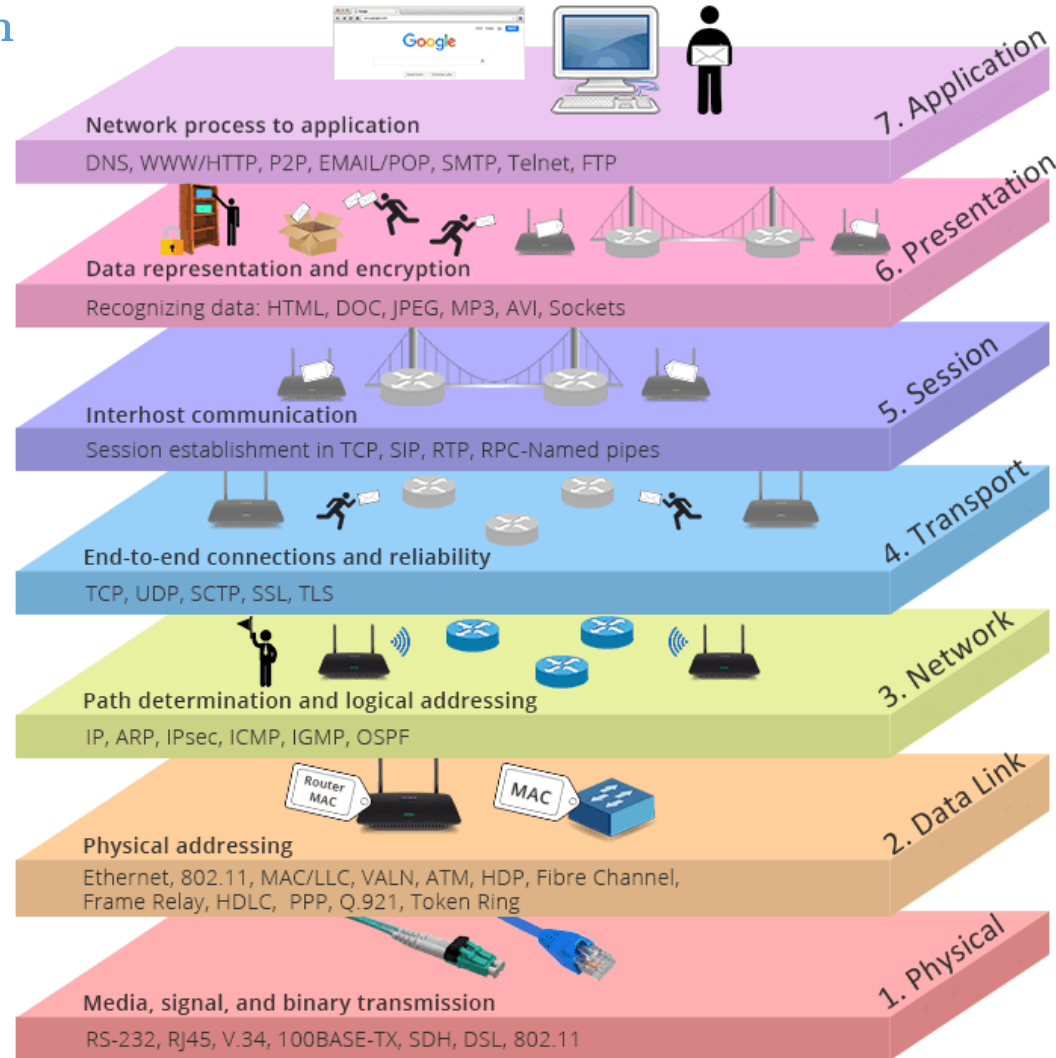
Objectives OSI model

- What is the purpose of a Network model?
- What are the layers of the OSI model?
- What are the characteristics of each layer of the OSI model?
- How does the TCP/IP stack compare to the OSI model?
- What are the well-known TCP and/or UDP port numbers for a given collection of common applications



The OSI seven-layer model

OSI - Open Systems Interconnection

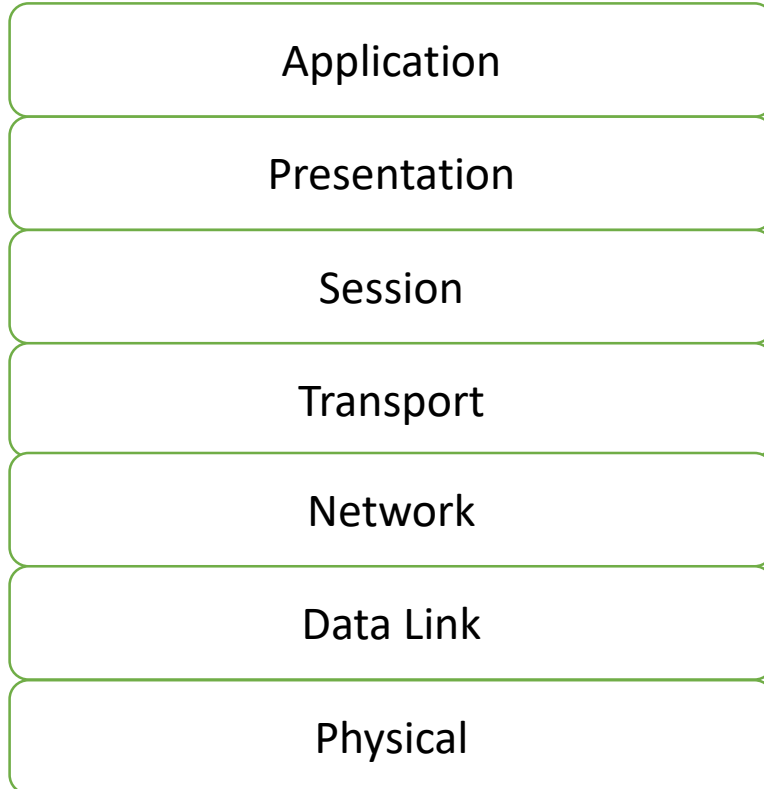


By : Eng. Ahmad Hassan Al-Mashaikh

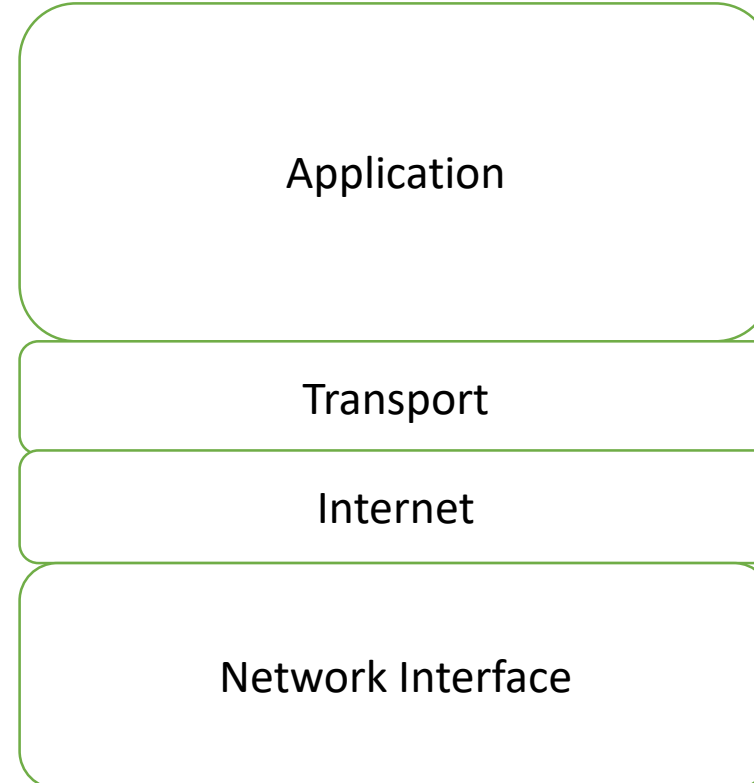
Email : Ahmad.private.mashaikh@Hotmail.com

The TCP/IP and OSI Models Compared

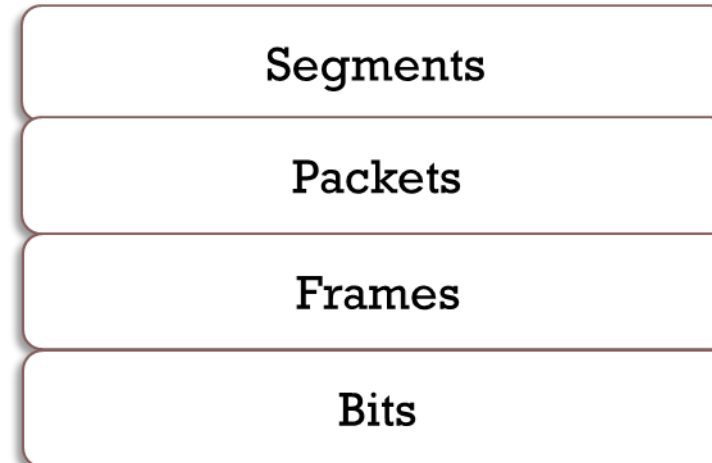
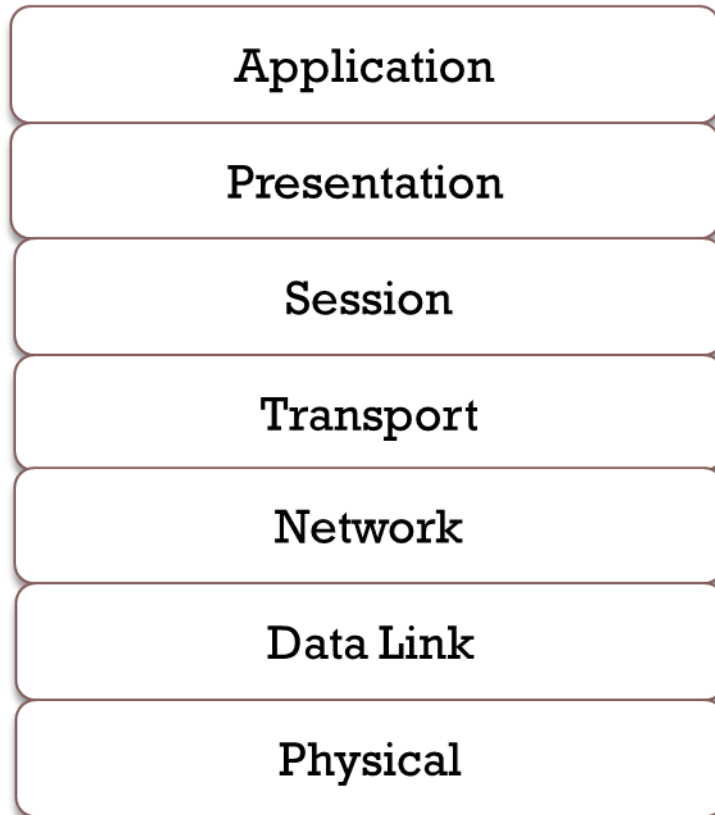
OSI Stack



TCP/IP Stack



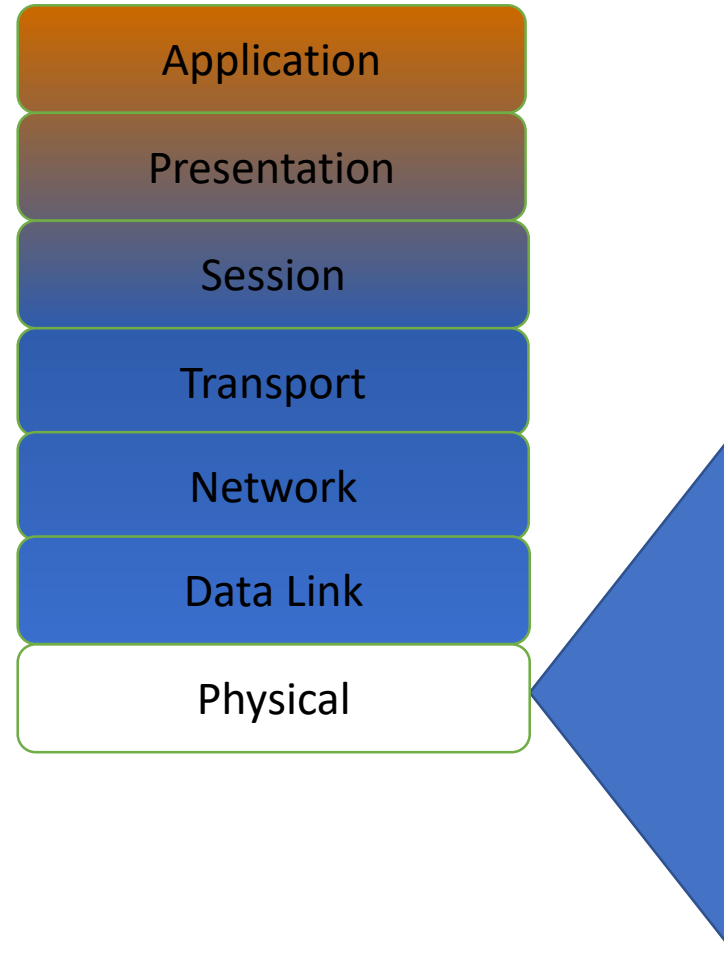
Protocol Data Unit (PDU)



Quick Summary of Layers 1-4

4	Transport	TCP & UDP Ports	Service
3	Network	Routers, IP Address	WAN
2	Data Link	Switches, MAC Address	LAN
1	Physical	Cables	

Physical Layer



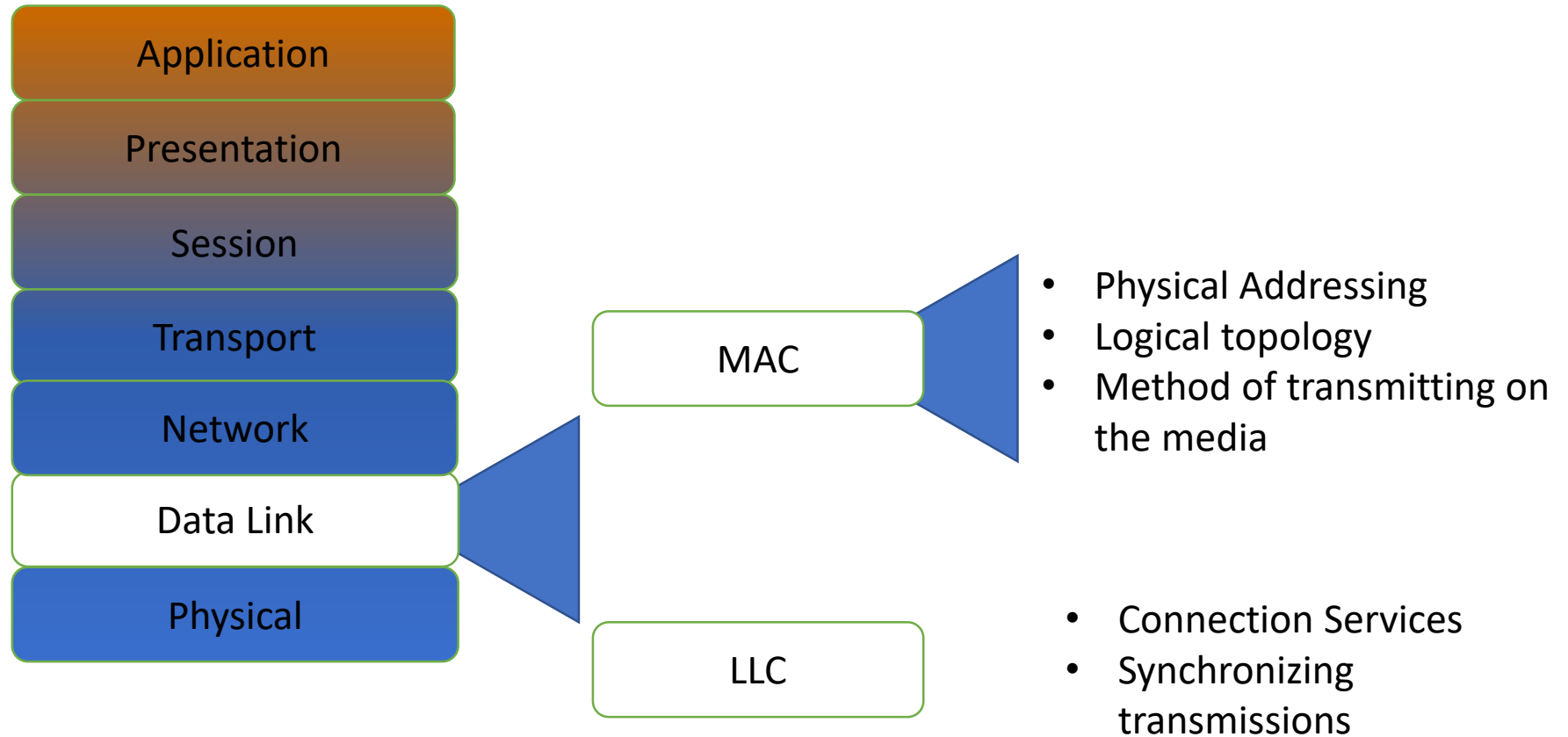
- How Bits are represented on the medium
- Wring standards for connectors and jacks
- Physical topology
- Synchronizing bits
- Bandwidth usage
- Multiplexing strategy

Layer 1 Devices

- Cables
- Wireless access points
- Hubs
- Because they don't pay any attention to addresses, they just deliver signals to every connected device like a crossover cable



Data Link Layer



MAC Addresses

- 48 bit address
- Hexadecimal Format
- Unique, Physical, and unchangeable
- IPCONFIG /ALL

00-0C-29-52-34-92

OUI

Vendor Assigned

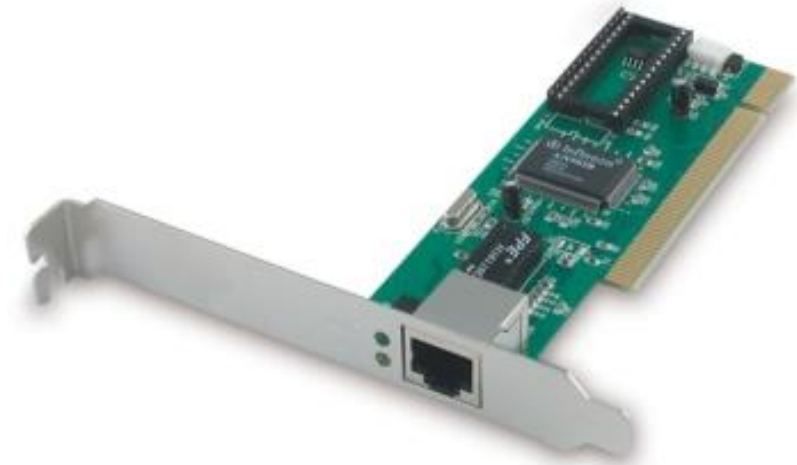
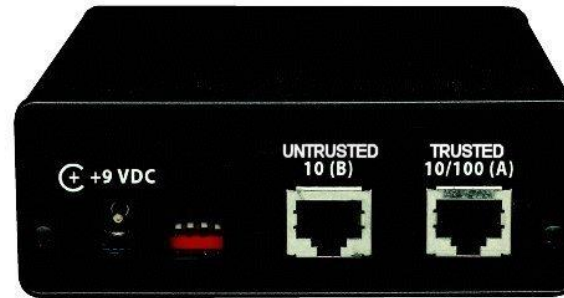
Ethernet adapter Local Area Connection:

```
Connection-specific DNS Suffix . : localdomain
Description . . . . . : Intel(R) PRO/1000 MT Network Connection
Physical Address. . . . . : 00-0C-29-52-34-92
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2::4(Preferred)
Link-local IPv6 Address . . . . . : fe80::5a7:33af:ed86:b39f%11(Preferred)
IPv4 Address. . . . . : 192.168.119.154(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Tuesday, August 20, 2013 12:37:23 PM
Lease Expires . . . . . : Tuesday, August 20, 2013 1:07:23 PM
Default Gateway . . . . . : 192.168.119.2
DHCP Server . . . . . : 192.168.119.254
DHCPv6 IAID . . . . . : 234884137
DHCPv6 Client DUID. . . . . : 00-01-00-01-15-0E-CB-08-00-0C-29-BB-32-CA

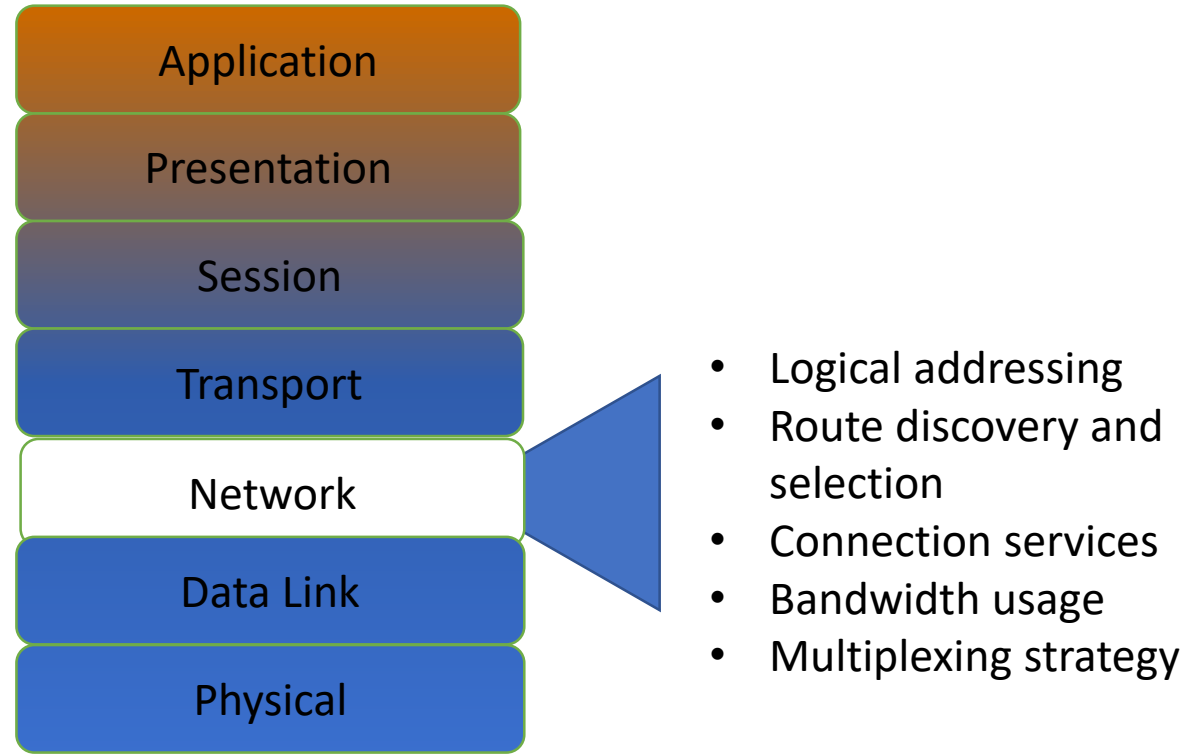
DNS Servers . . . . . : 192.168.119.2
Primary WINS Server . . . . . : 192.168.119.2
NetBIOS over Tcpip. . . . . : Enabled
```

Layer 2 Devices

- Switches
- Bridges
- Network Interface Cards (NICs)



Network Layer



IP Address

- Logical address
- Changes when the device is moved

```
Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : localdomain
Description . . . . . : Intel(R) PR0/1000 MT Network Connection
Physical Address. . . . . : 00-0C-29-52-34-92
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
IPv6 Address. . . . . : 2::4(Preferred)
Link-local IPv6 Address . . . . . : fe80::5a7:33af:ed86:b39f%11(Preferred)
IPv4 Address. . . . . : 192.168.119.154(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Tuesday, August 20, 2013 12:37:23 PM
Lease Expires . . . . . : Tuesday, August 20, 2013 1:07:23 PM
Default Gateway . . . . . : 192.168.119.2
DHCP Server . . . . . : 192.168.119.254
DHCPv6 IAID . . . . . : 234884137
DHCPv6 Client DUID. . . . . : 00-01-00-01-15-0E-CB-08-00-0C-29-BB-32-CA

DNS Servers . . . . . : 192.168.119.2
Primary WINS Server . . . . . : 192.168.119.2
NetBIOS over Tcpip. . . . . : Enabled
```


Switching

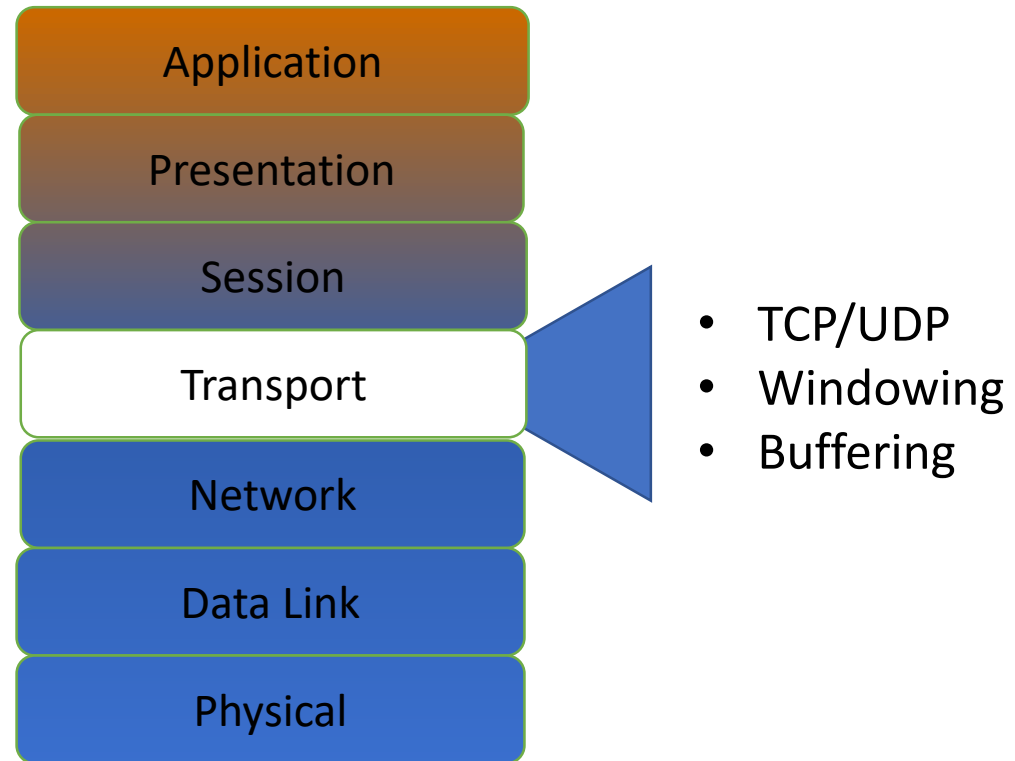
- Packet switching
 - Data is broken into packets
 - Many packets travel along network connections like cars on a freeway
- Circuit switching
 - A physical line is dedicated to each connection
 - Ex: old copper landline phone systems
- Message switching
 - Store-and-forward, like email

Layer 3 Devices

- Routers
- Multilayer Switches

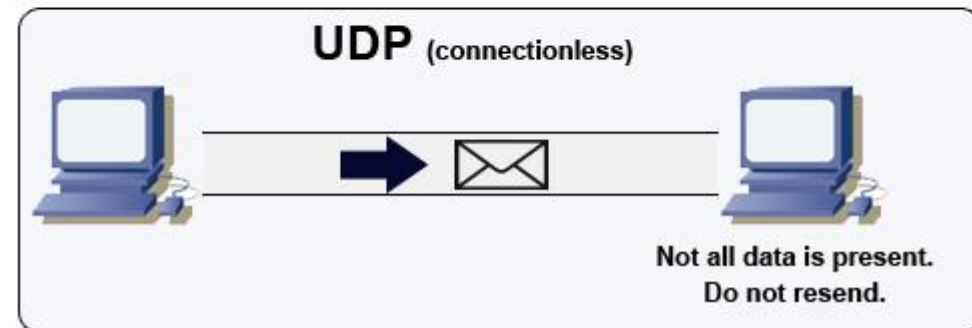
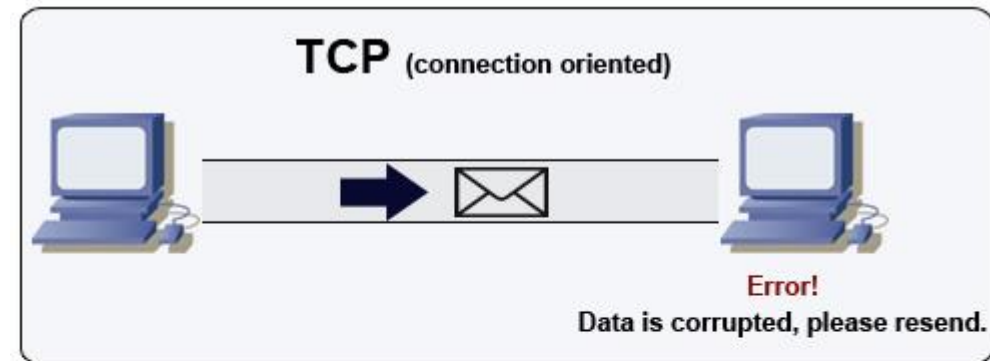


Transport Layer

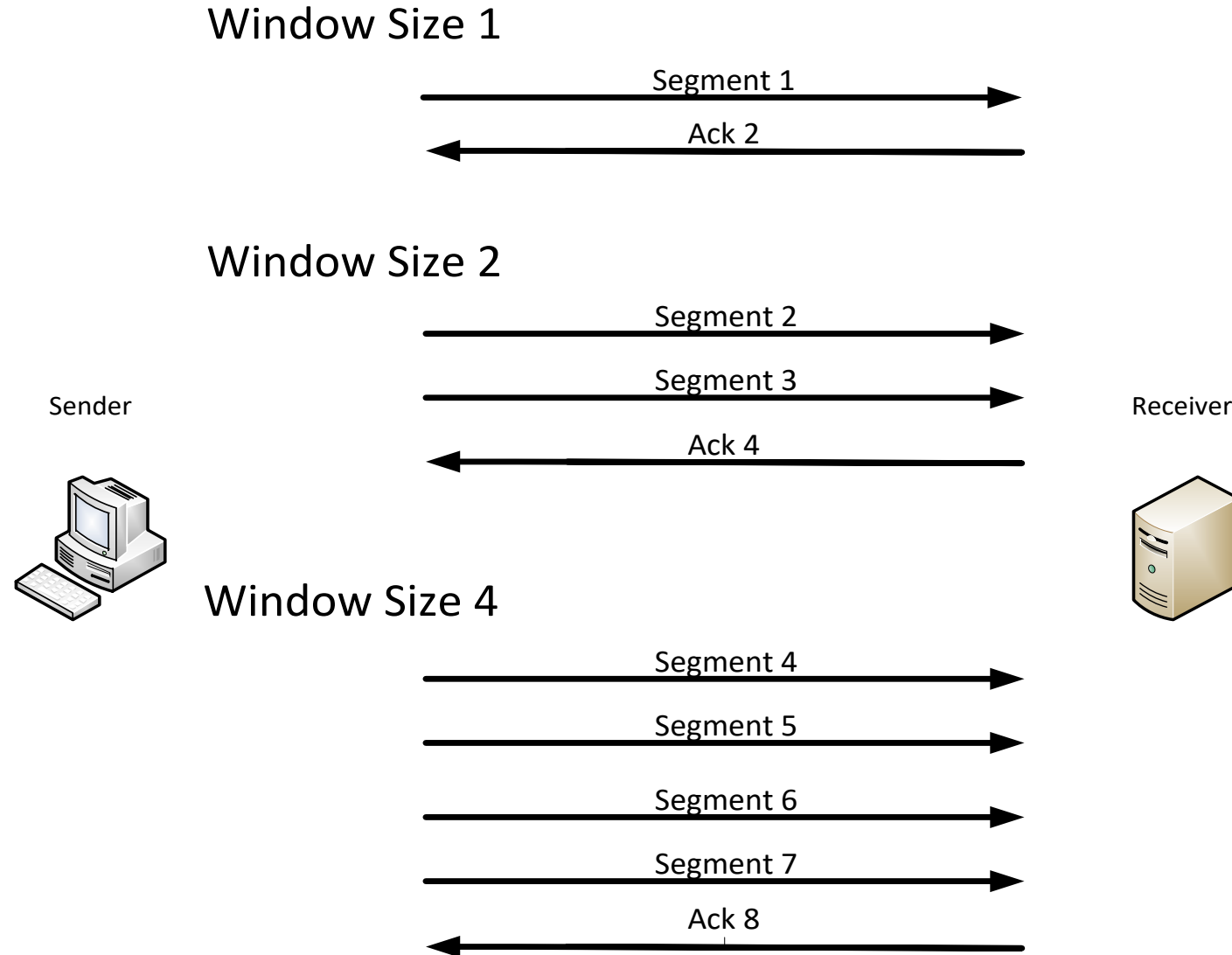


TCP and UDP

- Transmission Control Protocol (TCP)
 - Connection-oriented and reliable
 - Handshake makes sure both ends are ready
 - Segments are acknowledged and resent if necessary
- User Datagram Protocol (UDP)
 - Connectionless and unreliable
 - No handshake
 - Best-effort delivery, no acknowledgements

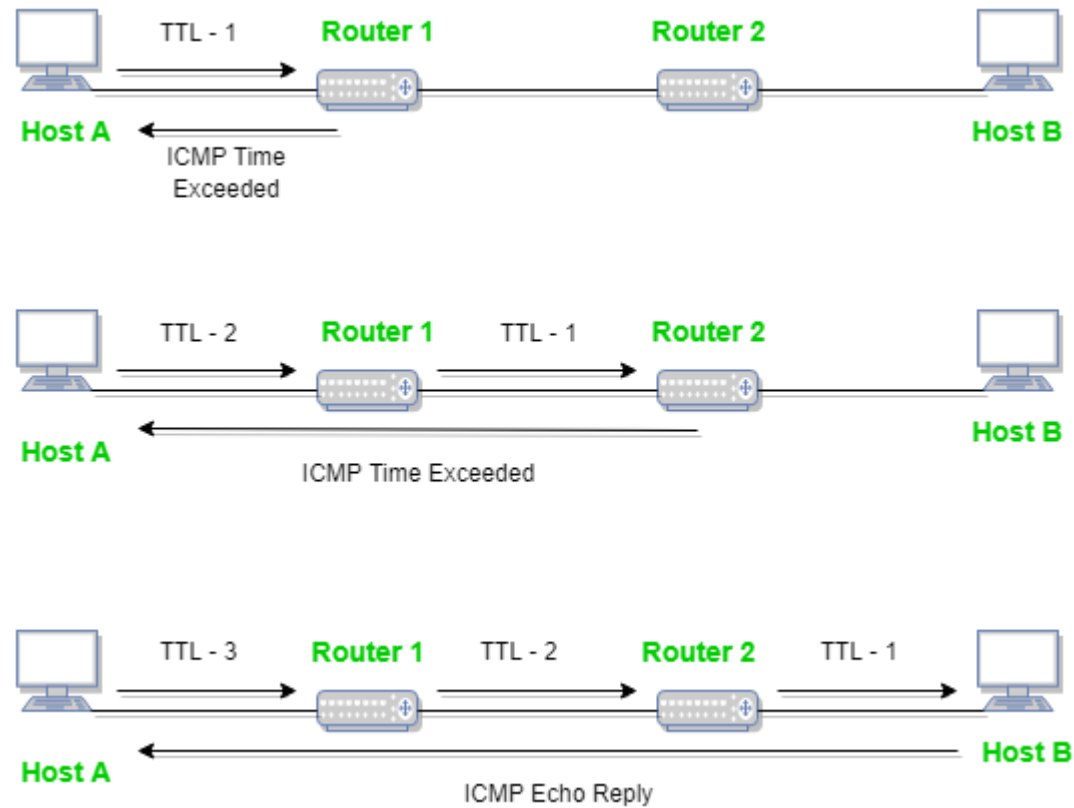


TCP Sliding Window

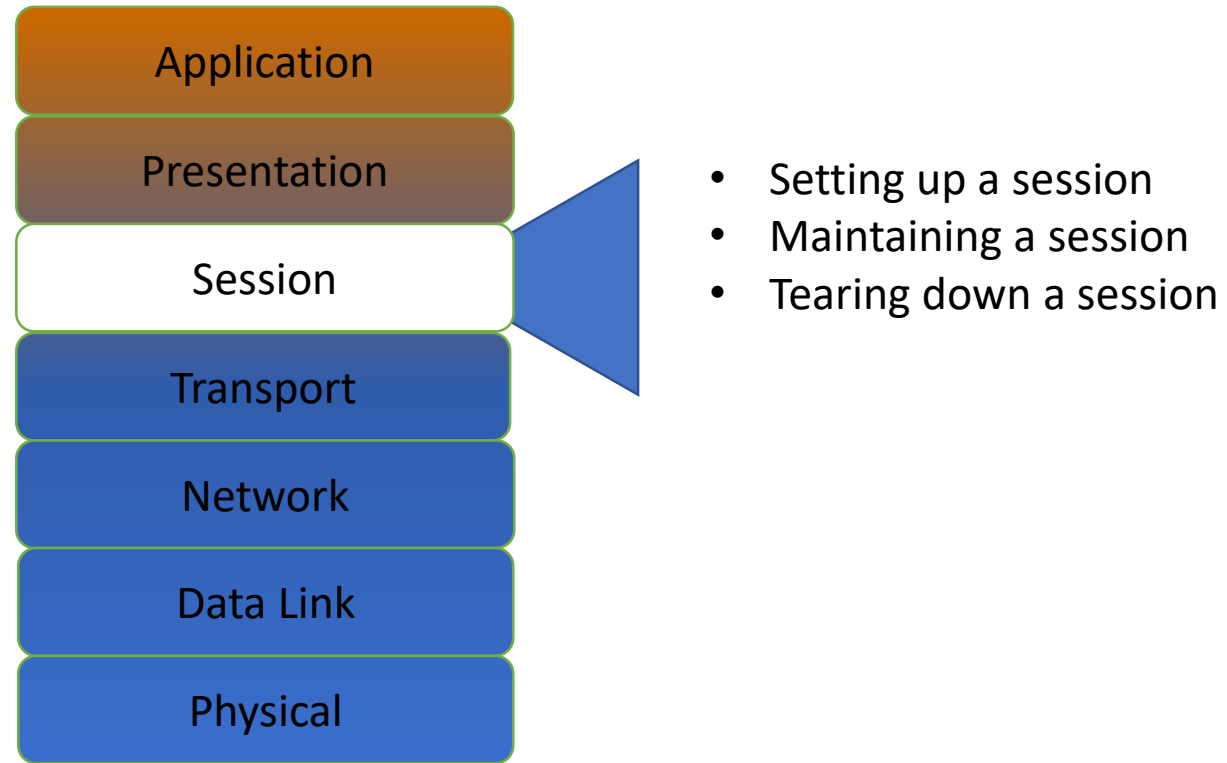


ICMP (Internet Control Message Protocol)

- At layer 4
- Used by ping and traceroute, and to indicate errors such as dropped packets

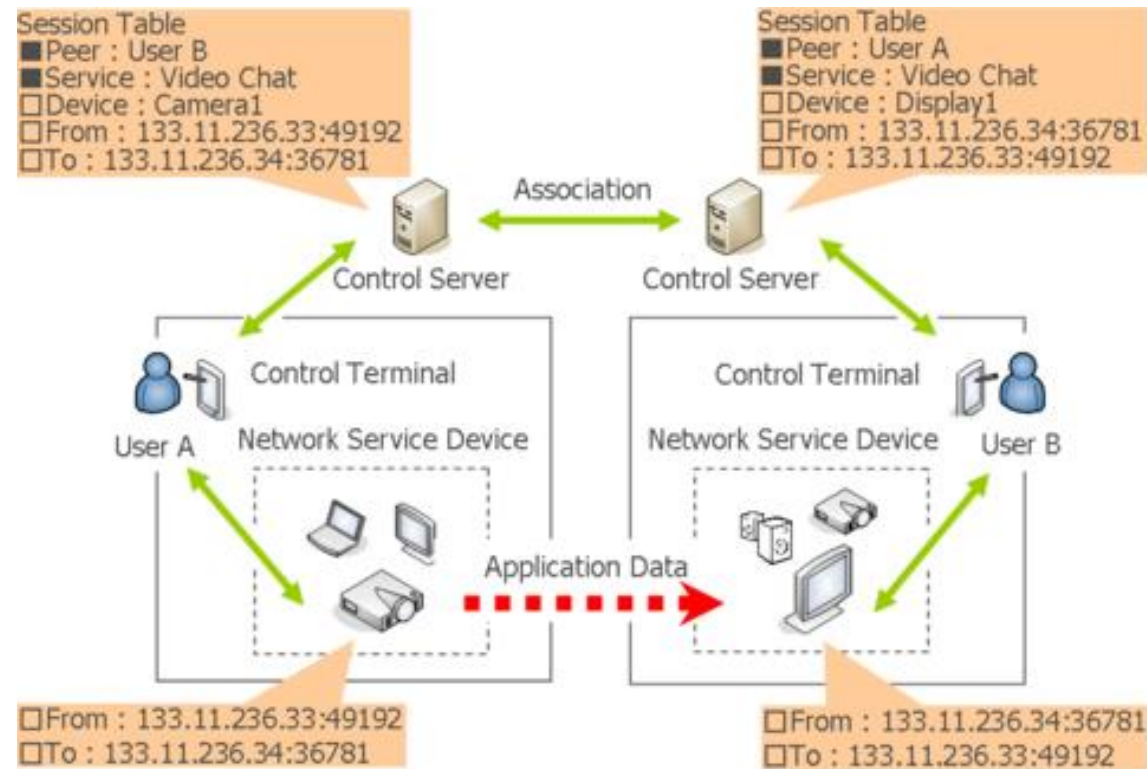


Session Layer

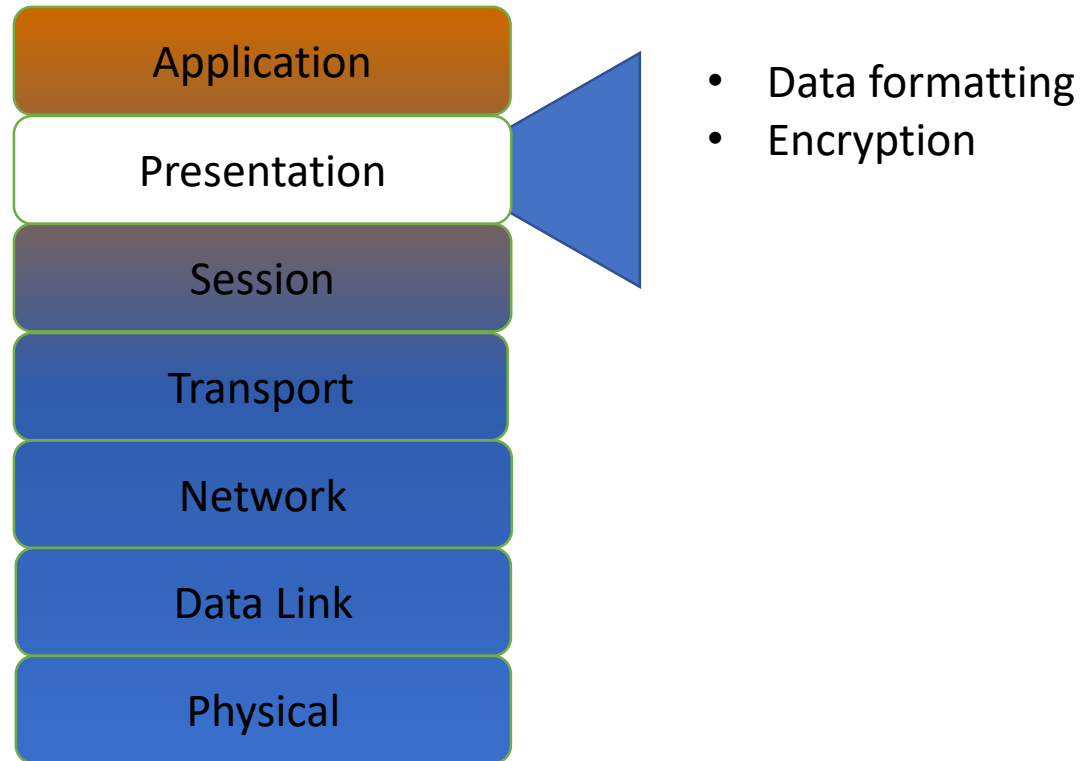


Example of a Session

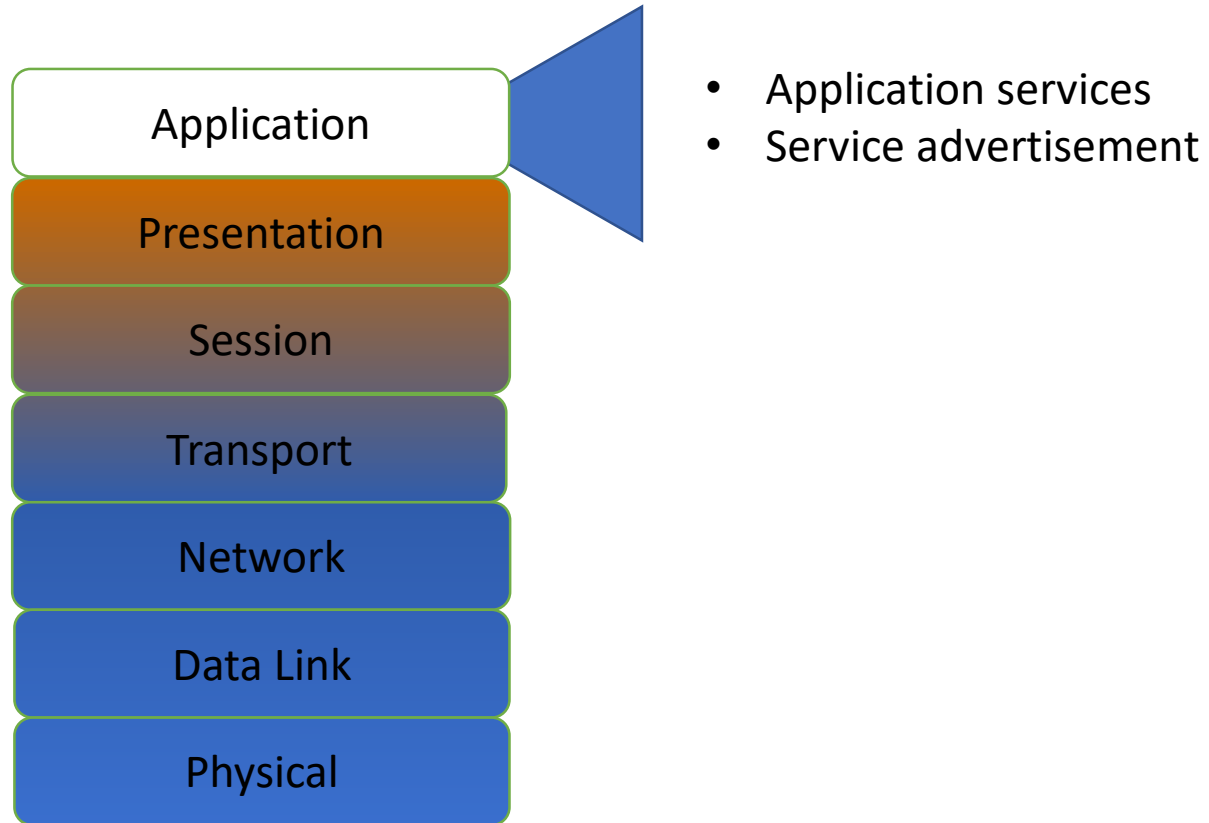
- User logs in with a username & password
- All data now has a special significance until that user logs off, or the session times out, or is terminated some other way
- Layer 6 Protocol
 - H.323 (voice or video)
 - NetBIOS (file sharing)



Presentation Layer

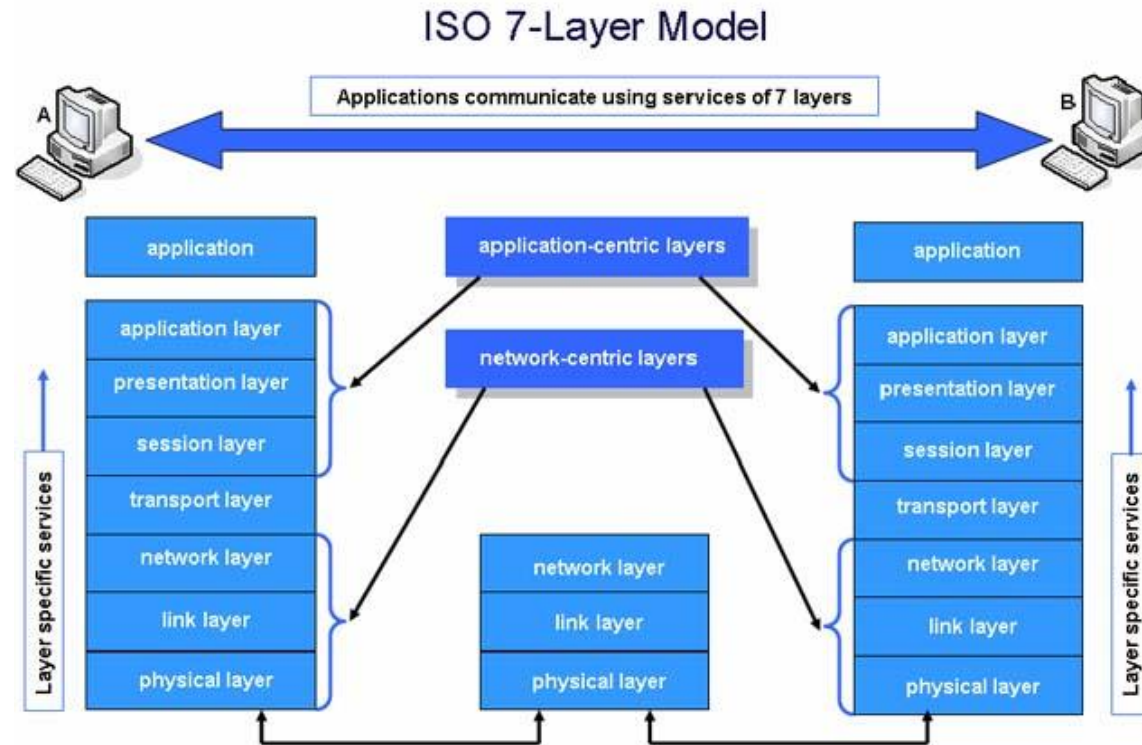


Application Layer



Application Layer

- Closest to the user
- Hands data to an application in the format it expects, with no addresses or other transmission artifacts
- Examples: a downloaded file, an email message



Common Ports

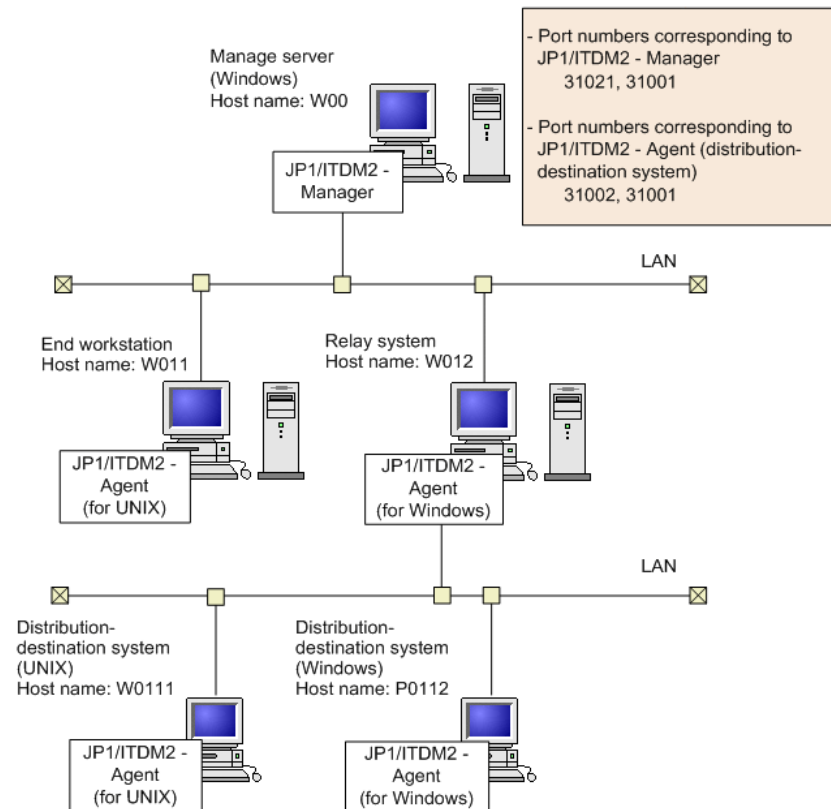
DNS (Domain Name System)	TCP/UDP 53
HTTP (Hypertext Transfer Protocol)	TCP 80
SMTP (Simple Mail Transfer Protocol)	TCP 25
POP (Post Office Protocol)	TCP 110
Telnet (DHCP)	TCP 23
DHCP (Dynamic Host Configuration Protocol)	UDP 67(IPv4 client) and 68(IPv4 server);
FTP (File Transfer Protocol)	TCP 20(data) and 21(control)
TFTP (Trivial File Transfer Protocol)	UDP 69
NBNS (NetBIOS Name Service)	UDP/TCP 137
IMAP4 (Internet Message Access Protocol)	TCP 143
SNMP (Simple Network Management Protocol)	TCP/UDP 161
HTTPS (Hypertext Transfer Protocol Secure)	TCP 443
NTP (Network Time Protocol)	UDP 123
SSL (Secure Sockets Layer)	TCP 443
SSH (Secure Shell)	TCP 22

By : Eng. Ahmad Hassan Al-Mashaikh

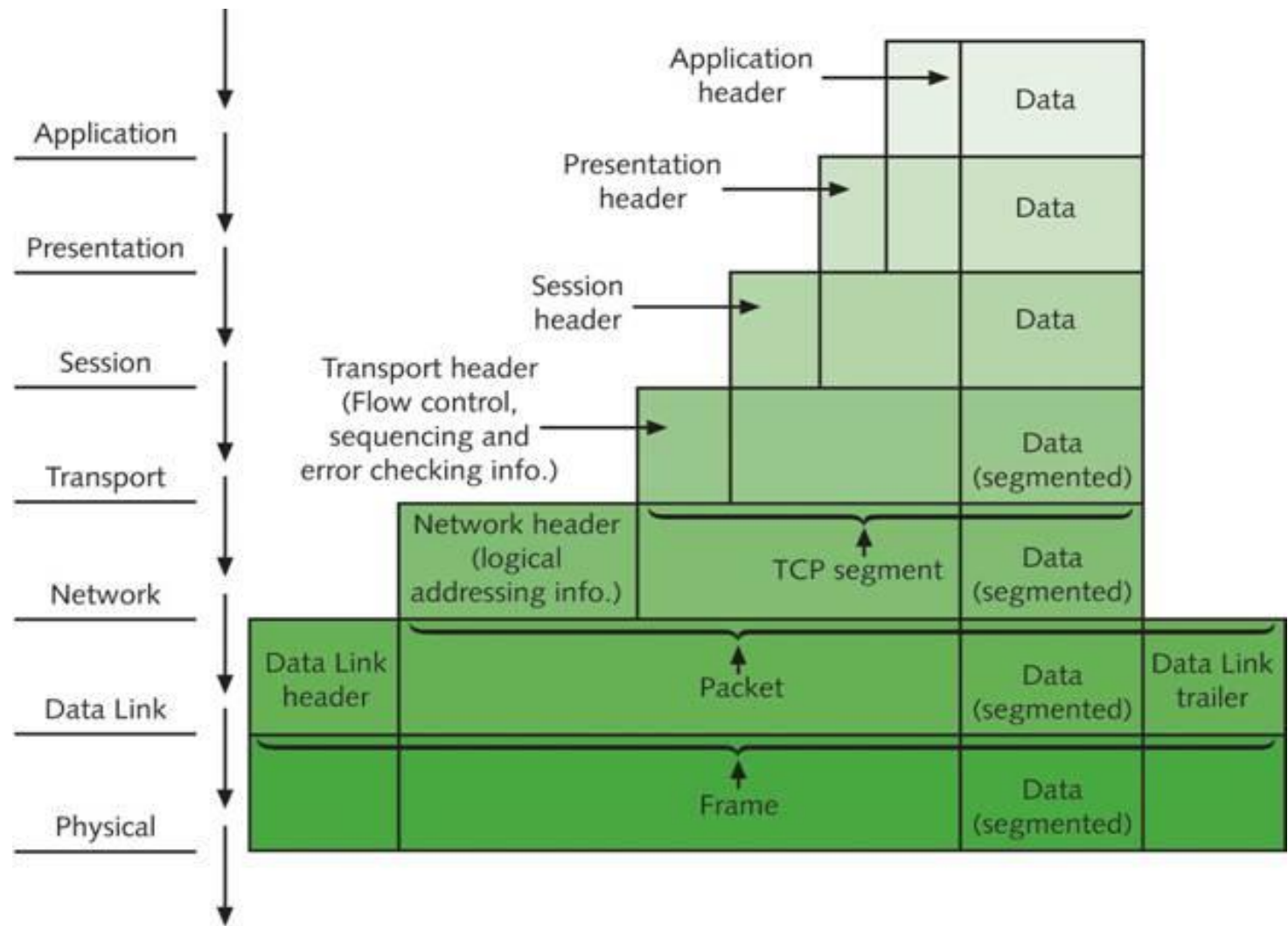
Email : Ahmad.private.mashaikh@Hotmail.com

Port Types

- Port numbers are assigned in various ways, based on three ranges:
- System Ports (0-1023), System Ports are assigned by IETF process for standards-track protocols, as per RFC6335. Also known as well-known-ports
- User Ports (1024-49151), User Ports are assigned by IANA using the "Expert Review" process, as per RFC6335
- Dynamic and/or Private Ports (49152-65535), Dynamic Ports are not assigned, they are dynamically created as your computer need them. Also known as ephemeral ports.



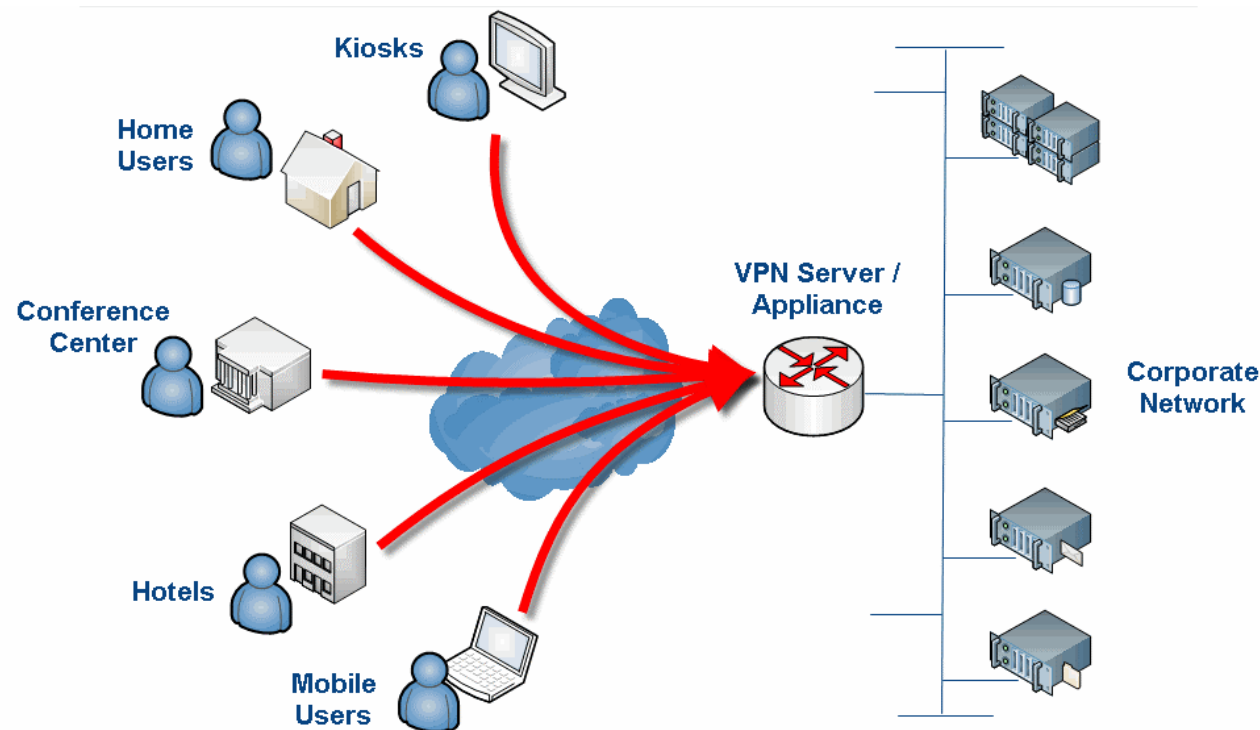
Communication Between Two Systems



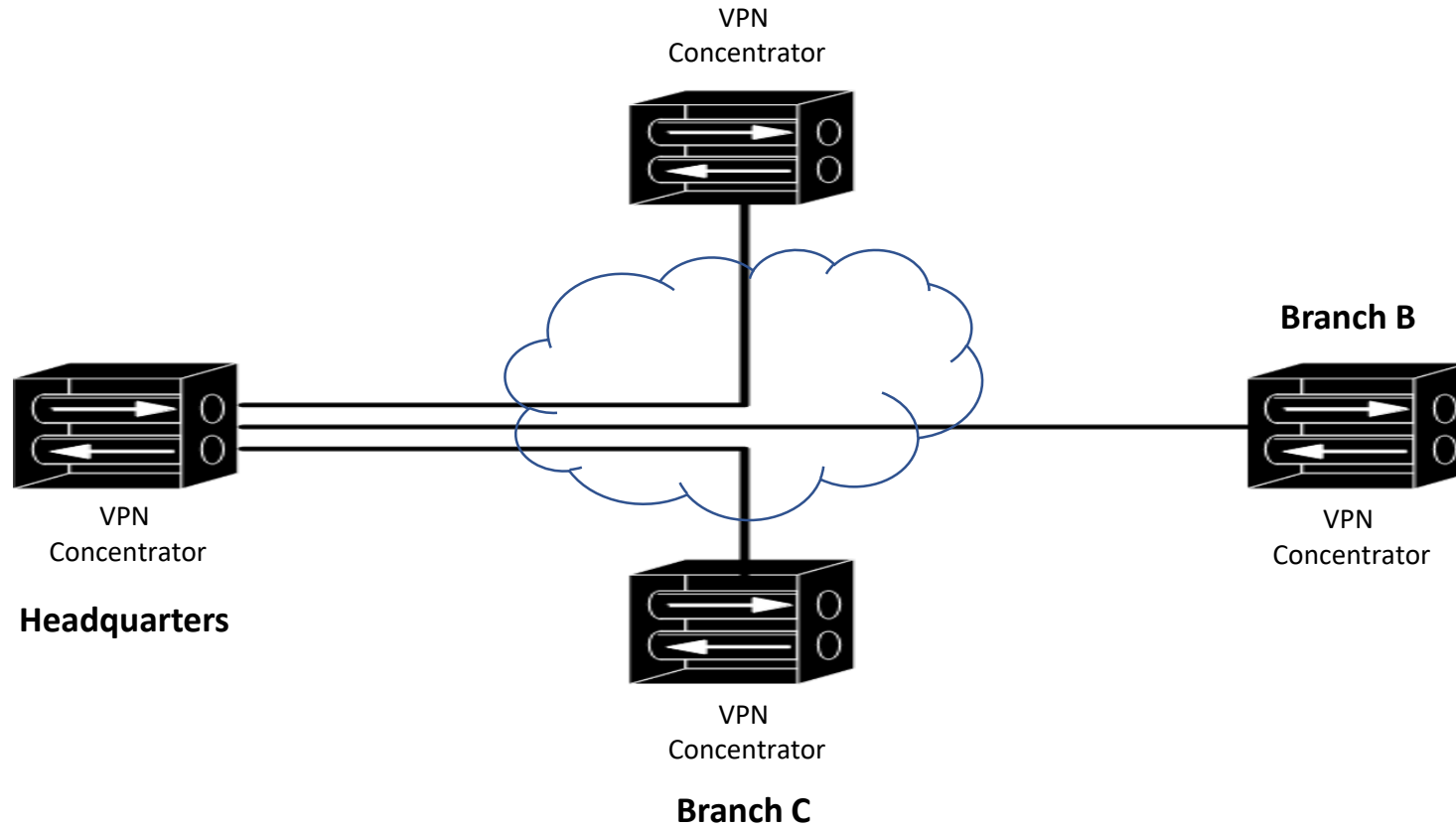
Identifying Network components

- VPN Concentrator

- Companies with locations spread across multiple sites require secure communications between those sites.
- One method is to create secure connections through an untrusted network, such as the Internet.
- Such a secure tunnel is called a virtual private network (VPN).
- The device that terminating these VPN tunnels, is a VPN Concentrator.
- A VPN concentrator performs the processor-intensive process required to terminate multiple VPN tunnels.

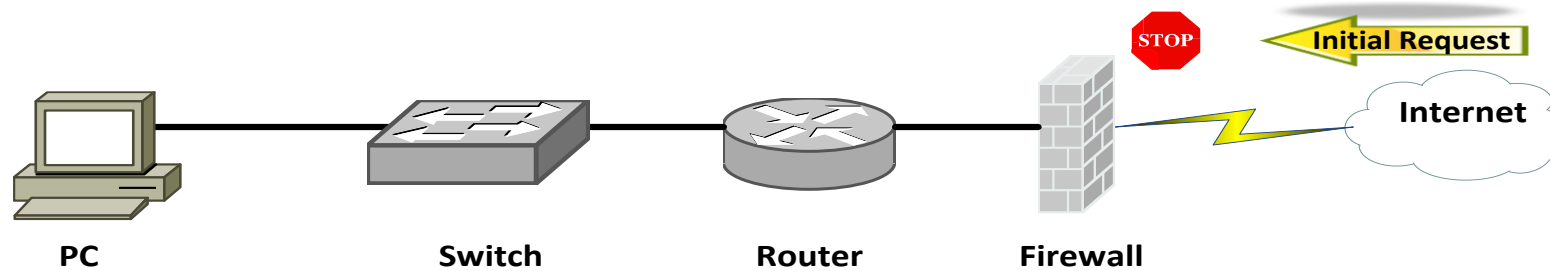
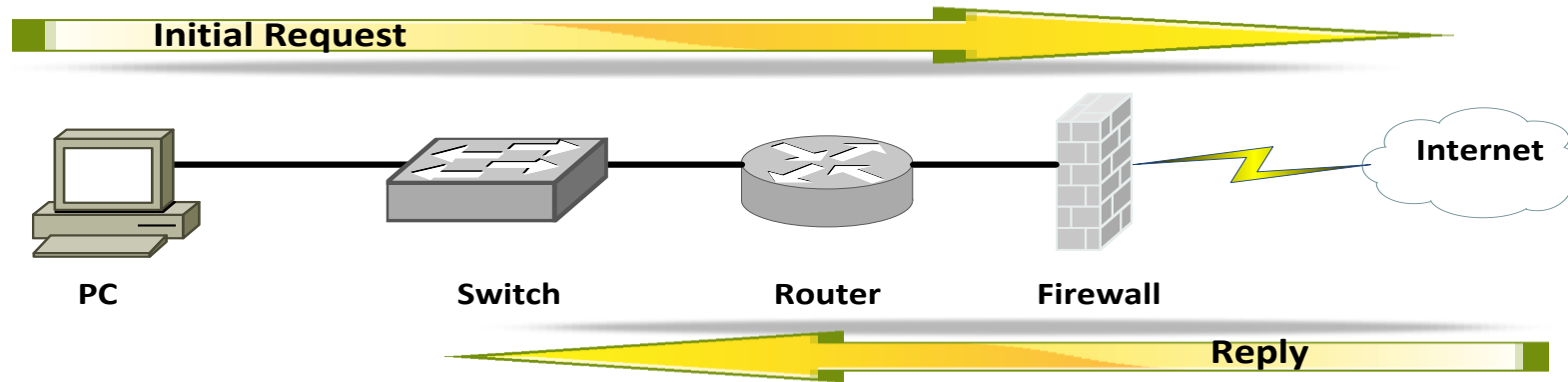


VPN Concentrator



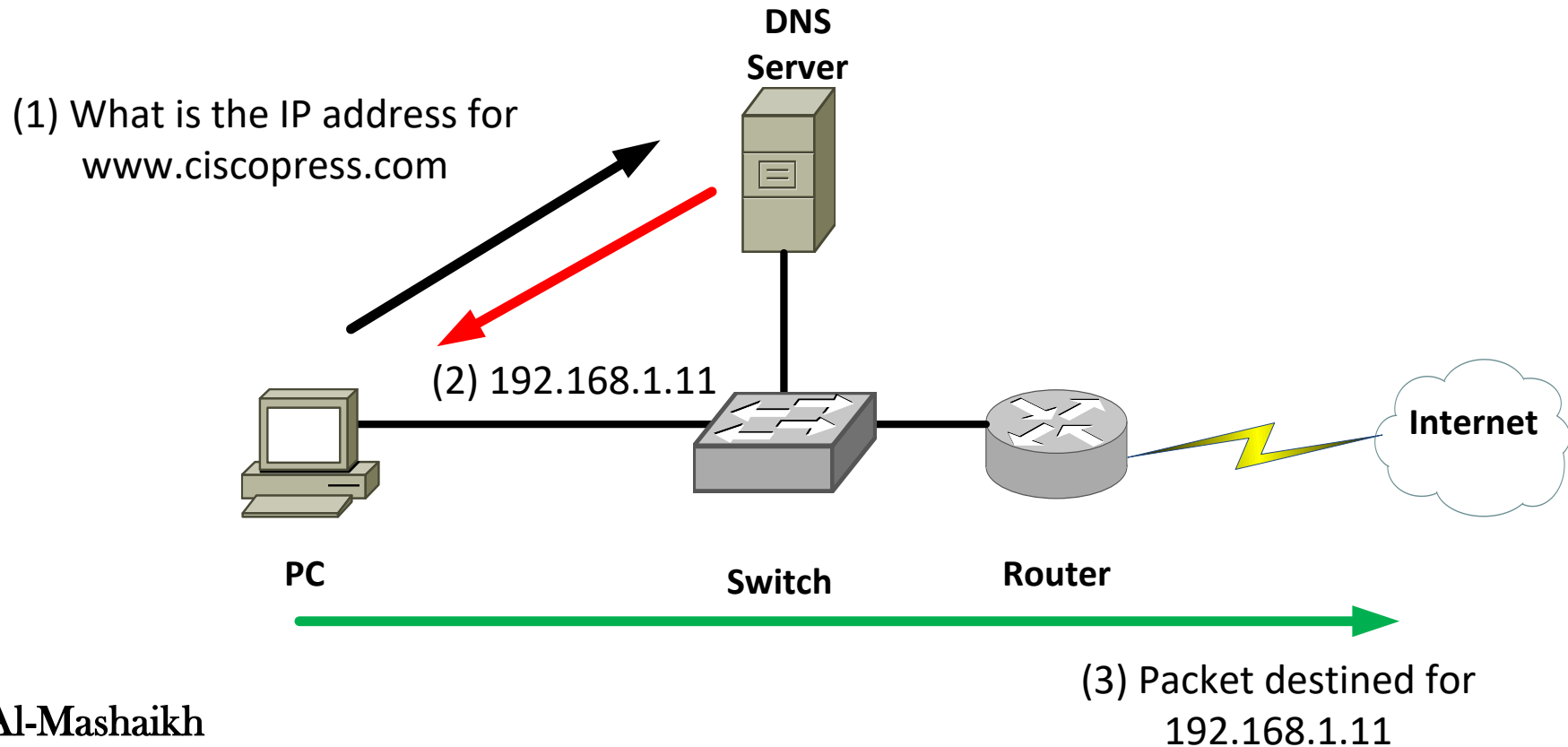
Firewalls

- A Firewall is primarily a network security appliance, it stands guard at the door of your network, protecting it from malicious Internet traffic.
- There are many types of firewalls, a stateful firewall is one example.

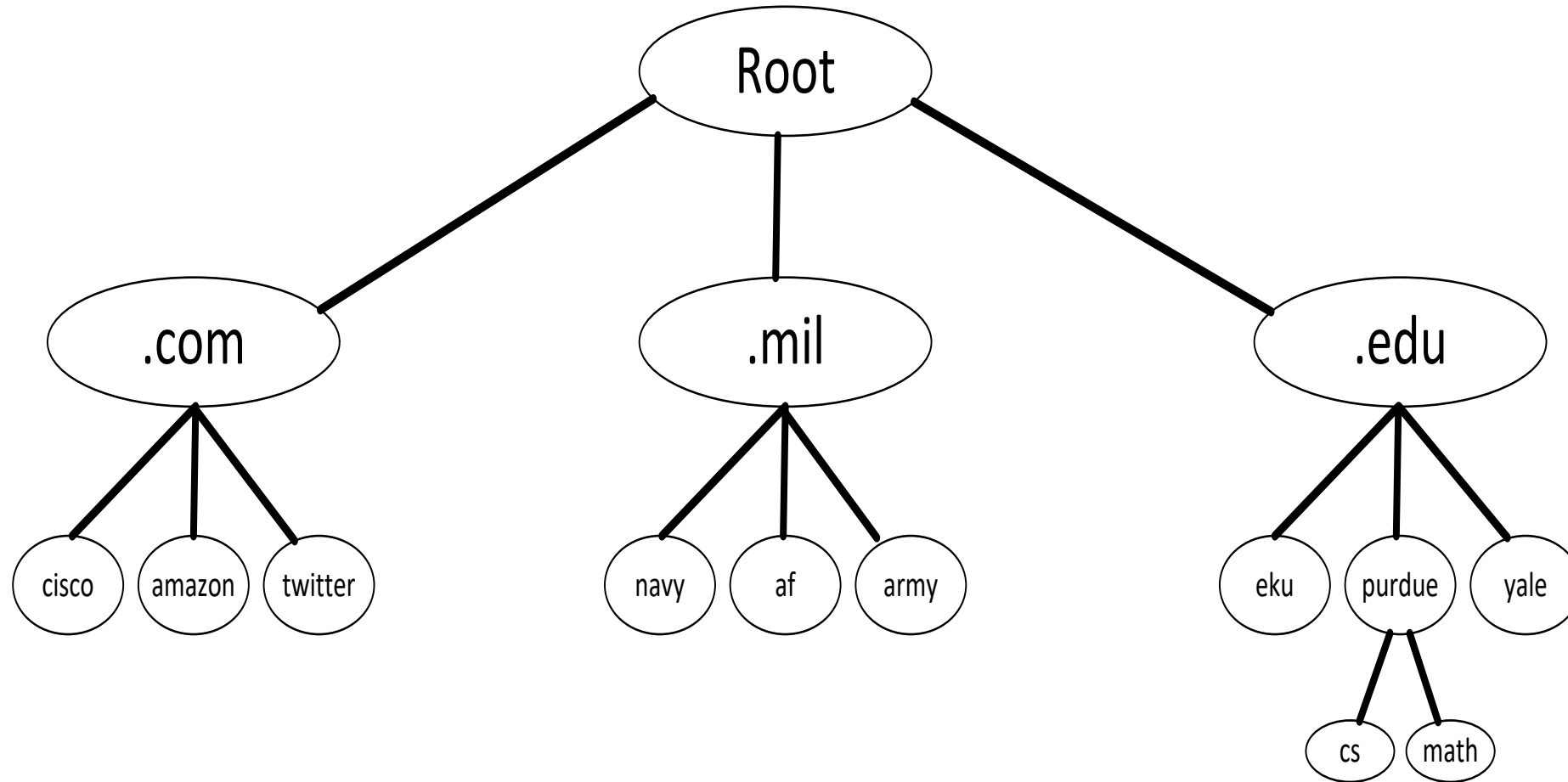


DNS Servers

- A Domain Name System (DNS) server performs the task of taking a domain name like, `www.ciscopress.com` and resolving that name into a corresponding IP address.
- Computers and the internet use numbers not names, but people recall names better than numbers.
- `www.ciscopress.com` is an example of a fully-qualified domain name (FQDN)
- An FQDN is a series of strings delimited by periods. The right-most string represents the root domain.

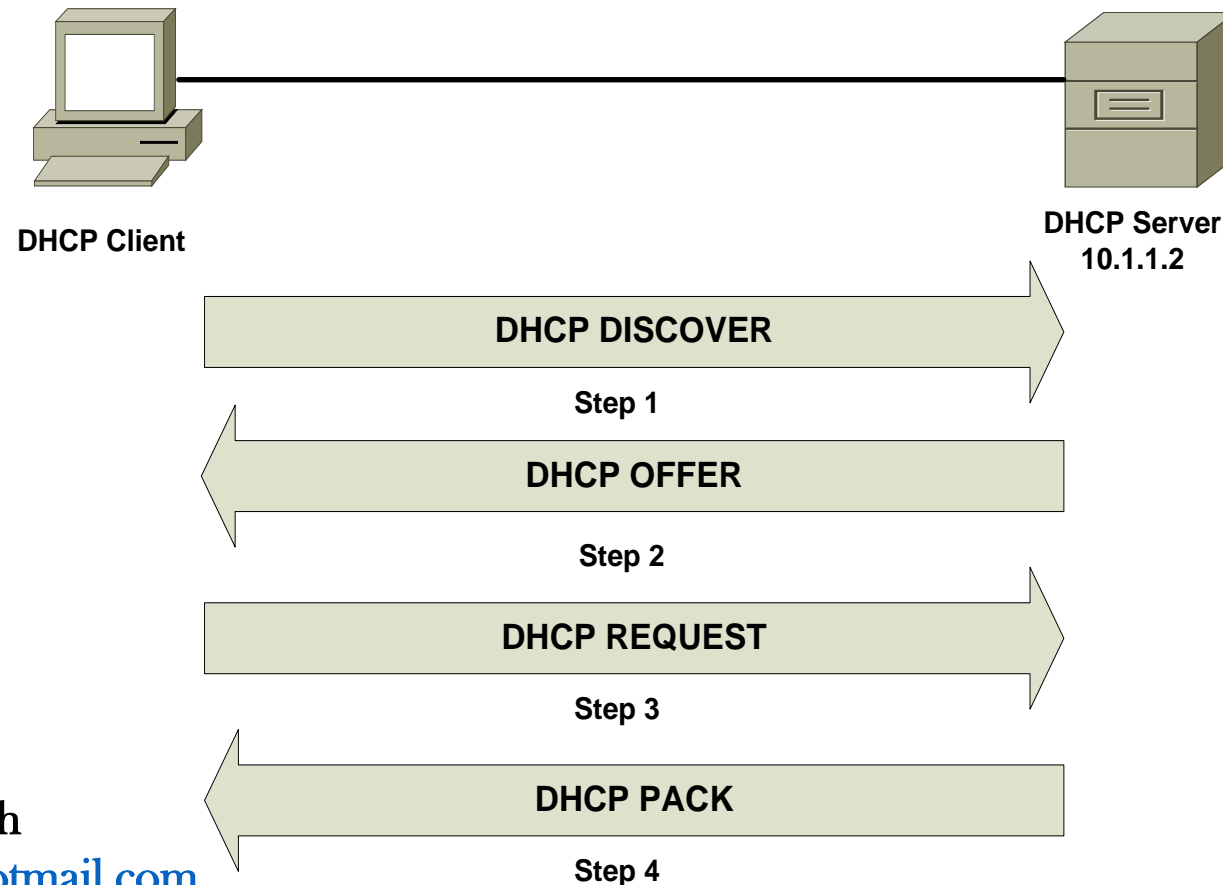


DNS Hierarchy



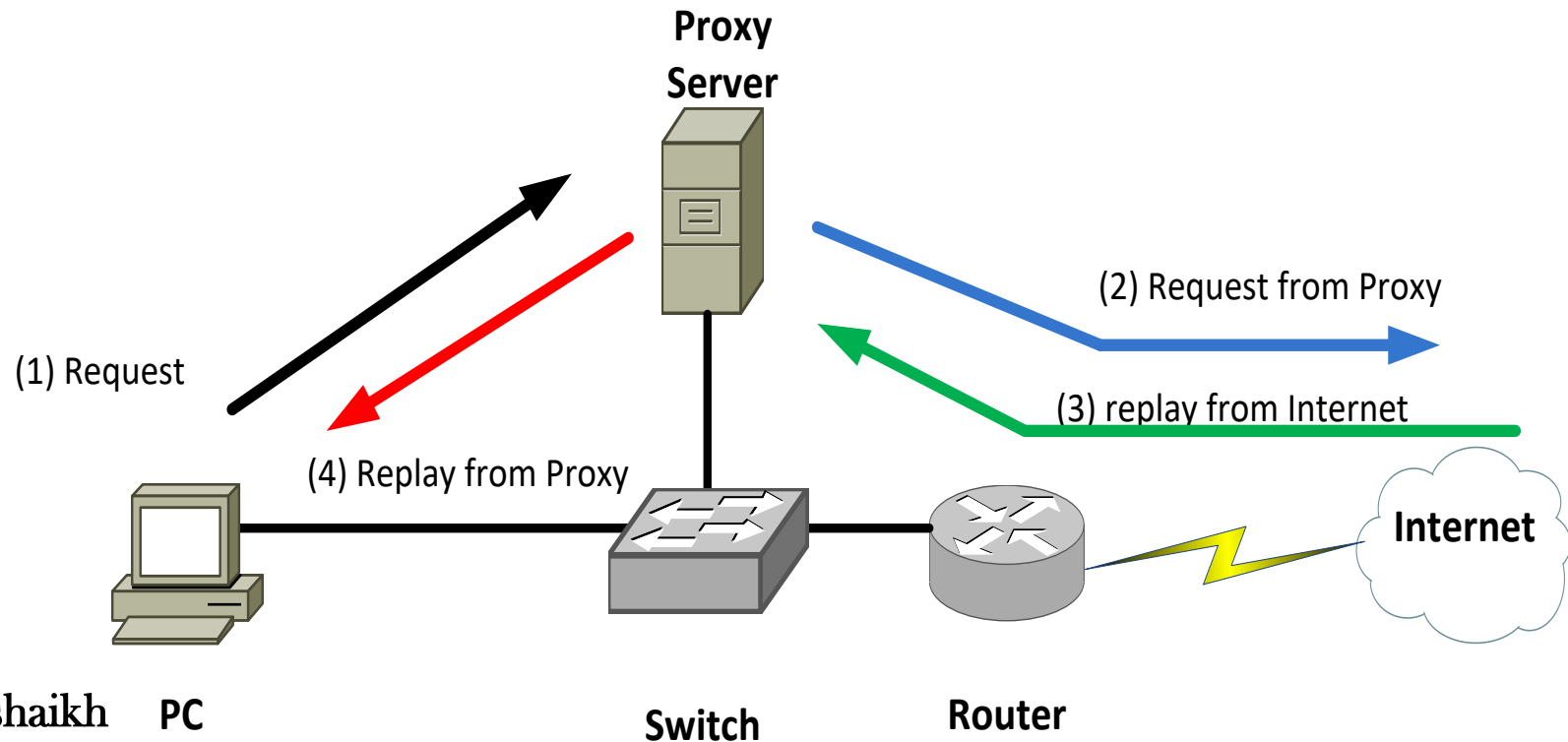
DHCP Servers

- Most modern networks have IP address assigned to networking devices, and those logical Layer 3 addresses are used to route traffic between networks.
- IP address can be statically configured on each host, however such process is time consuming and error prone (Manual).
- A far more efficient method of IP address assignment is to dynamically assign IP addresses to network devices (Automatic).
- This process assigns the; IP Address, Subnet Mask, Default Gateway, DNS Server to the host.

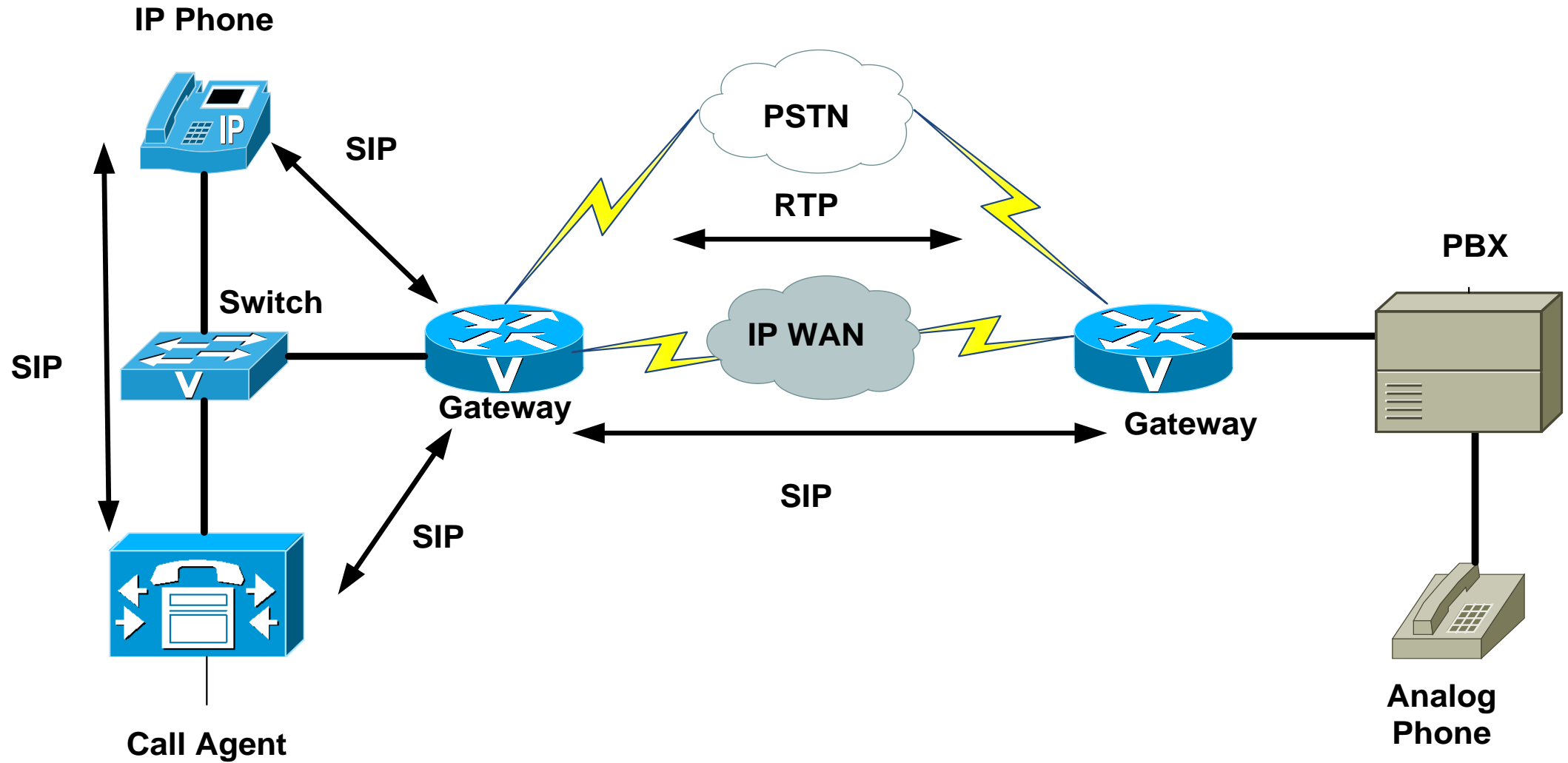


Proxy Servers

- A Proxy Server is a device that makes request on behalf of its client.
- Clients are configured to forward their packets, which are seemingly destined for the Internet, to a proxy server.
- The proxy server evaluates the request, if it has a copy of the information the client is looking for it replies with it.
- If the requested page is not in the server it forwards the request to the Internet.



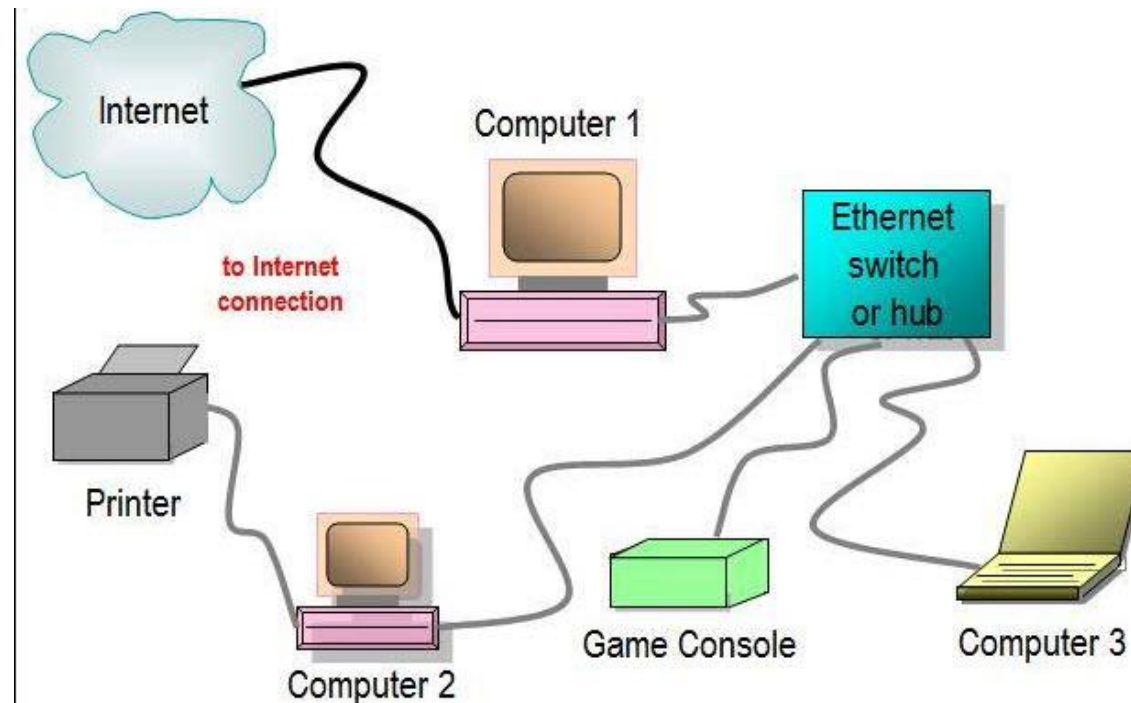
VoIP Protocols & Components



Understanding Ethernet

Objectives

- What are the characteristics of Ethernet networks, in terms of media access, collisions domains, broadcast domains, and distance/speed limitations of various Ethernet Standards?
- What functions are performed by Ethernet switch features, such as VLANs, trunks, Spanning Tree Protocol, link aggregation, Power over Ethernet, port monitoring, user authentication, and first-hop redundancy?



Understanding Ethernet

- Odds are, when you are working with local-area networks (LAN), you are working with Ethernet as the Layer 1 technology.
- Over the years, Ethernet has evolved. Several Ethernet standards exist in modern LANs, with a variety of distance and speed limitations.

Principles of Ethernet

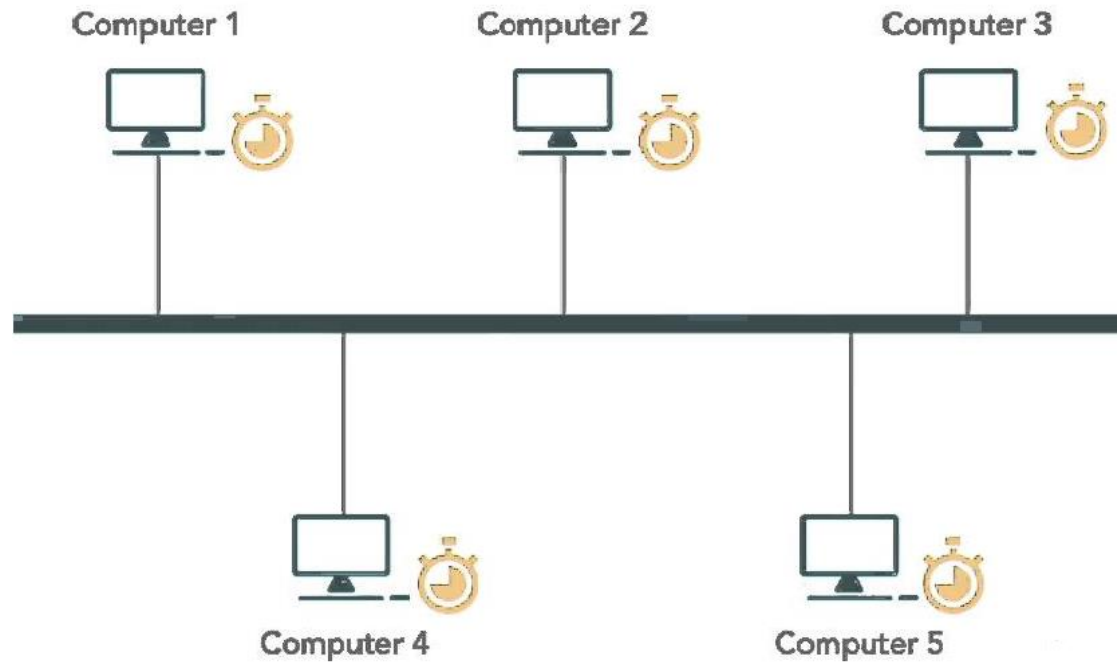
- Ethernet was first developed by Xerox Corporation. The original intent was to create a technology to allow computers to connect with laser printers.
- From this humble beginnings, Ethernet rose to be used to interconnect such devices as computers, printers, wireless access points, servers, switches, routers, video-game systems, and more.

Ethernet Origins

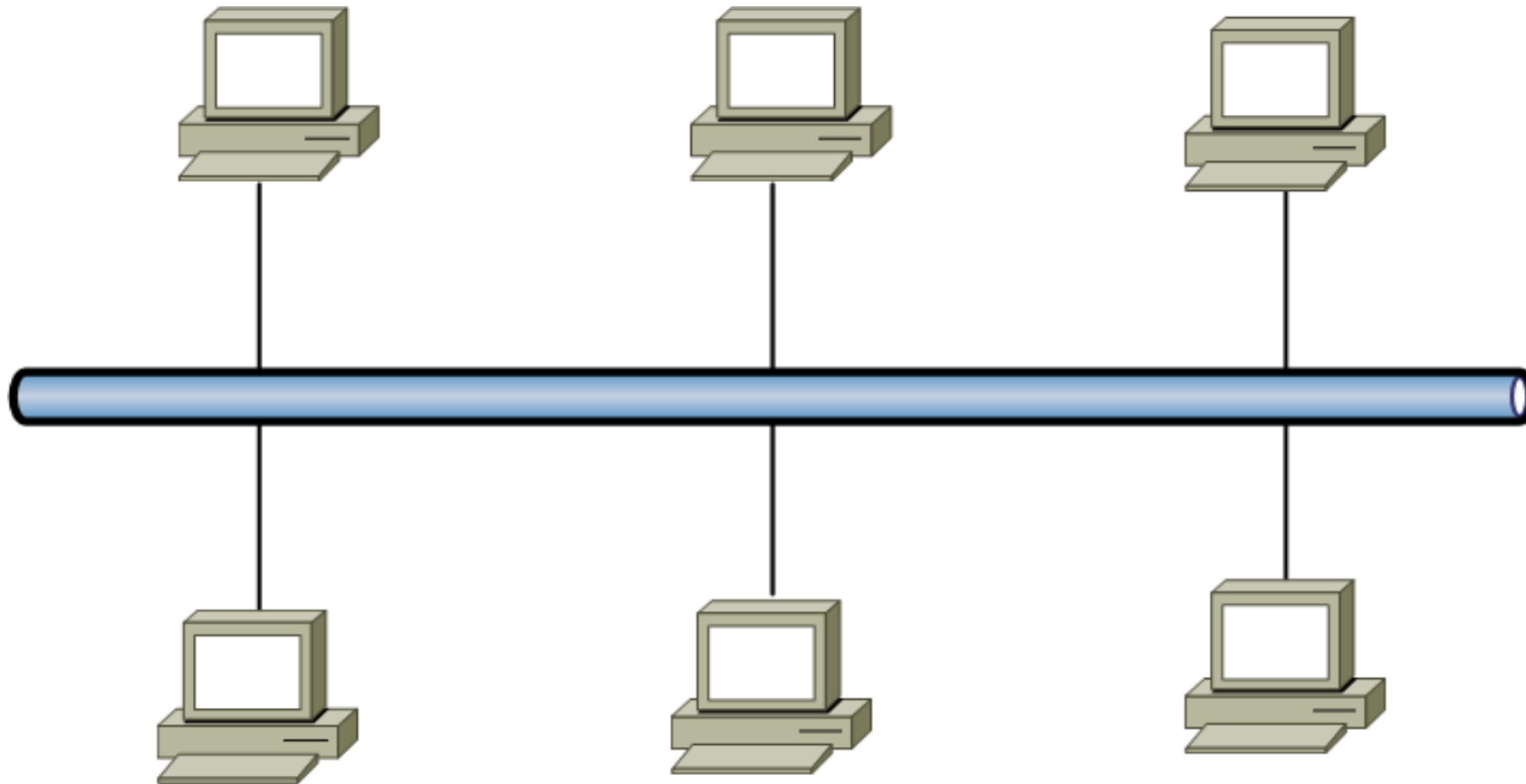
- IEEE 802.3, in general this is interchangeable with the term Ethernet.
 - In the early days, it was called 10BASE5.
 - 10 = 10 Mbps (10 million bits per second)
- BASE = Baseband, one signal on the line at a time.
 - 5 = 500 meters of cable max
 - The cable use was RG-6, became known as thicknet.
- Another early Ethernet implementation was 10BASE2.
 - 10 = 10 Mbps (10 million bits per second)
 - BASE = Baseband, one signal on the line at a time.
 - 2 = 185 meters of cable max
- The cable use was RG-58, became known as thinnet.
- 10BASE5 and 10BASE2 networks are rarely, if ever, seen today. Other than their 10-Mbps bandwidth limitation, the cables used by these network have been replaced with either UTP or STP cables.

Carrier Sense Multiple Access Collision Detect (CSMA/CD)

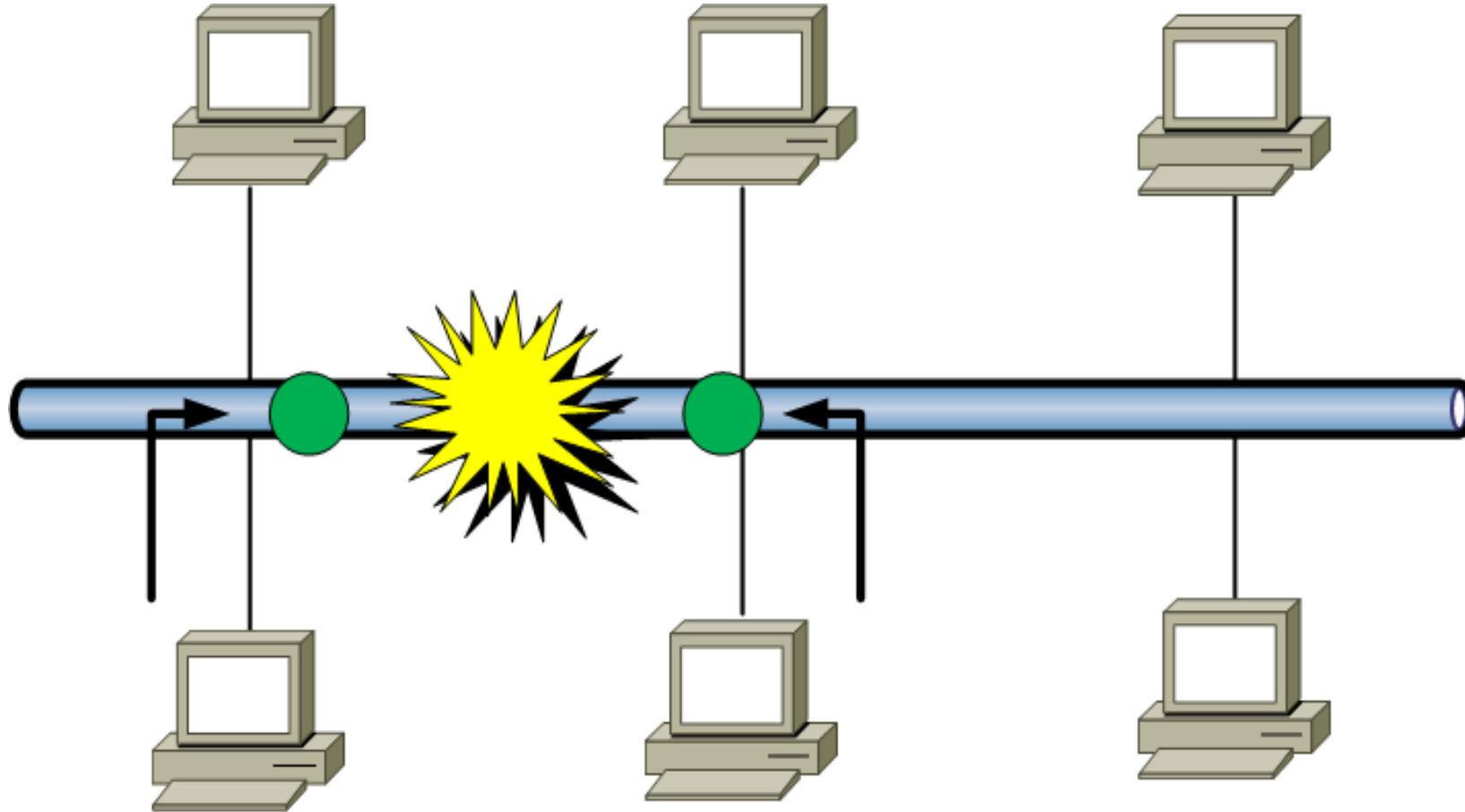
- Ethernet was based on the philosophy that all networked device should be eligible at any time, to transmit on a network
- At the core of this philosophy is the bus topology in which Ethernet was designed to operate.
- Ethernet permits only a single frame to be on a network segment at any one time.



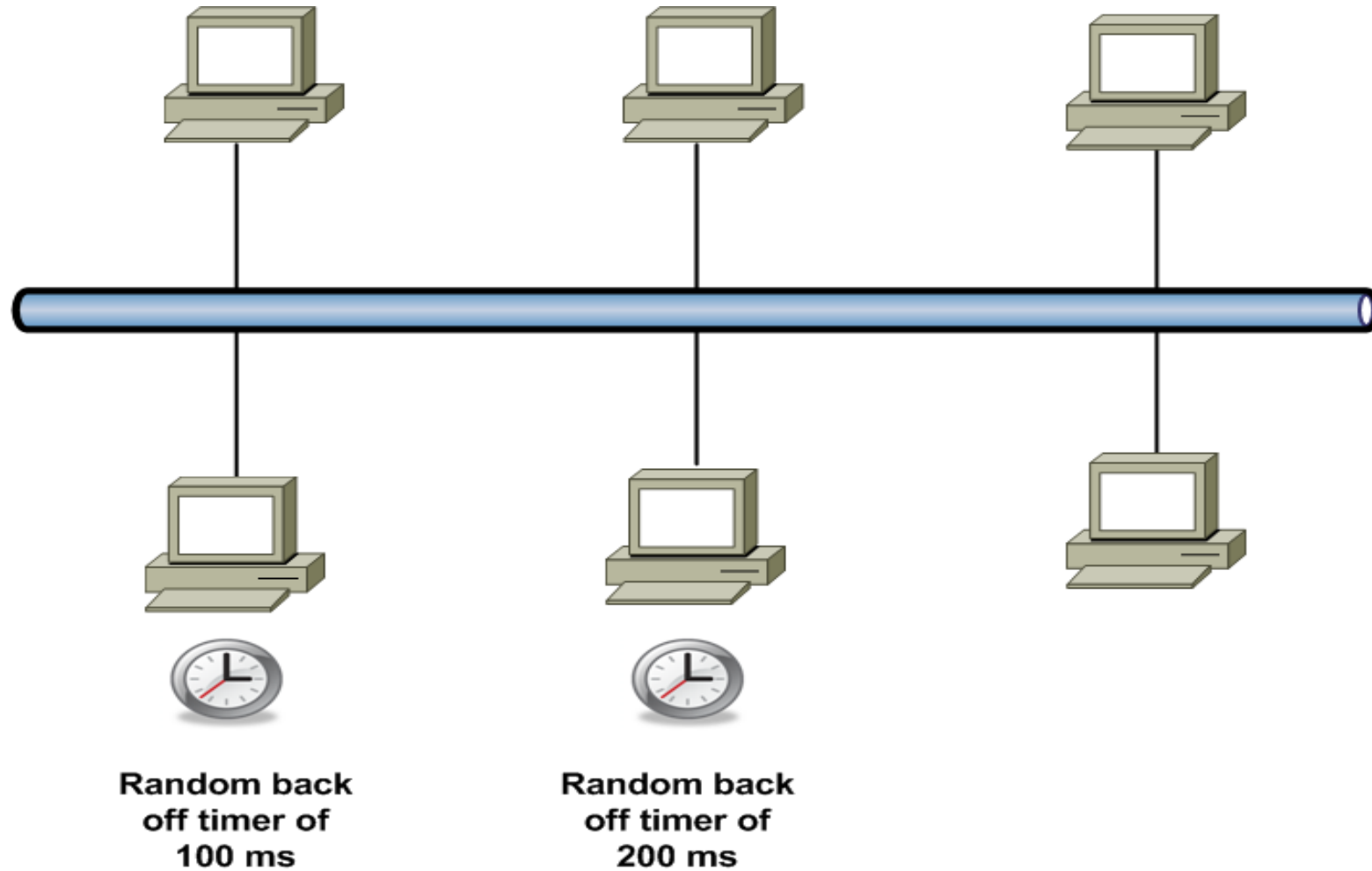
Ethernet Network Using a Shared Bus



Collision on an Ethernet Segment



Recovering from a Collision with Random Back Off Timers



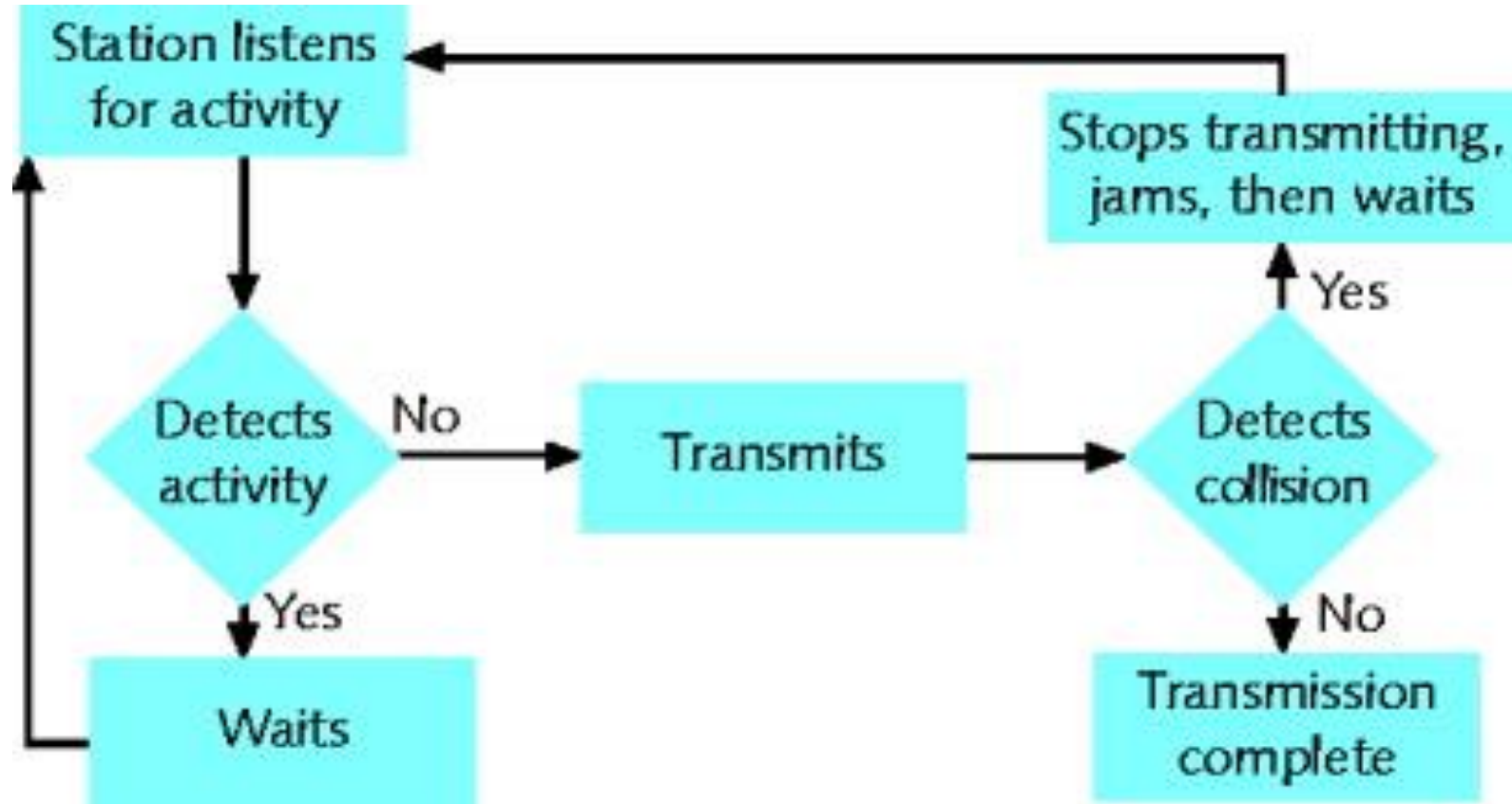
CSMA/CD (Carrier Sense Multiple Access with Collision Detection)

- Network access method
 - Controls how nodes access communications channel
 - Necessary to share finite bandwidth
- Carrier sense
 - Ethernet NICs listen, wait until free channel detected
- Multiple access
 - Ethernet nodes simultaneously monitor traffic, access media

CSMA/CD (cont'd.)

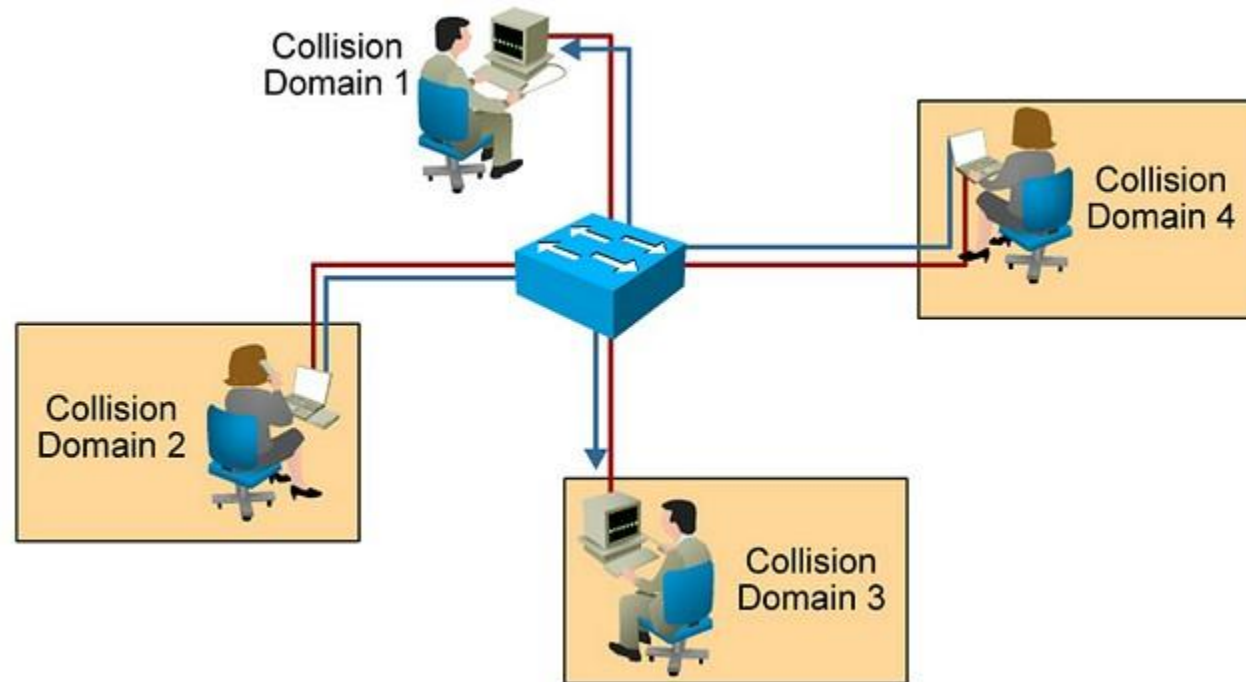
- Collision
 - Two nodes simultaneously:
 - Check channel, determine it is free, begin transmission
- Collision detection
 - Manner nodes respond to collision
 - Requires collision detection routine
 - Enacted if node detects collision
- Jamming
 - NIC issues 32-bit sequence
 - Indicates previous message faulty

CSMA/CD Process

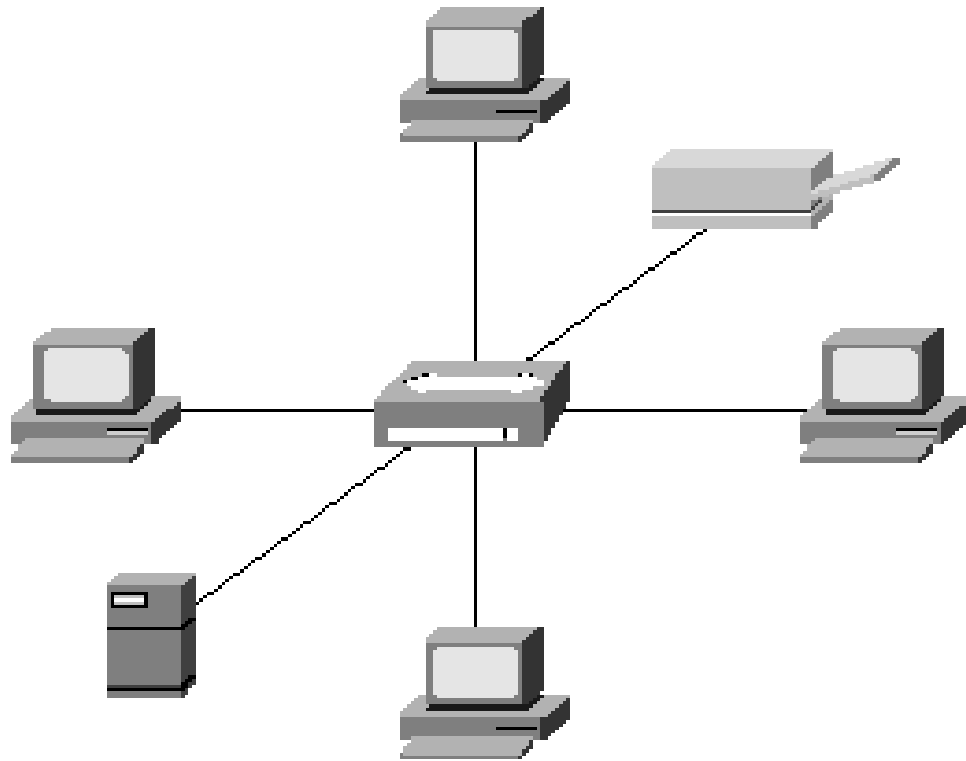


General Definition

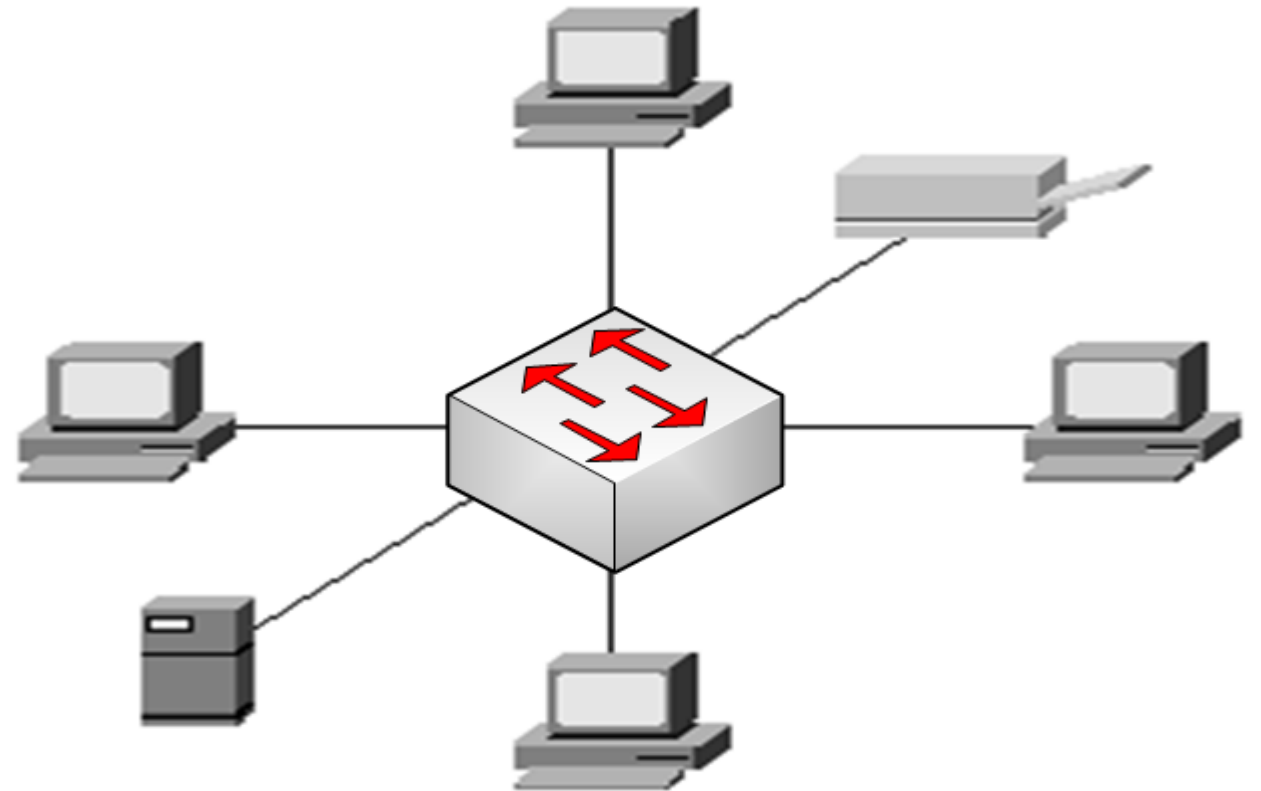
- A collision domain -- is a set of network interface cards (NICs) for which a frame sent by one NIC could result in a collision with a frame sent by any other NIC in the same network segment.
- A broadcast domain – is a set of NICs for which a broadcast frame sent by one NIC will be received by all other NICs in the same broadcast domain



HUB and Switch



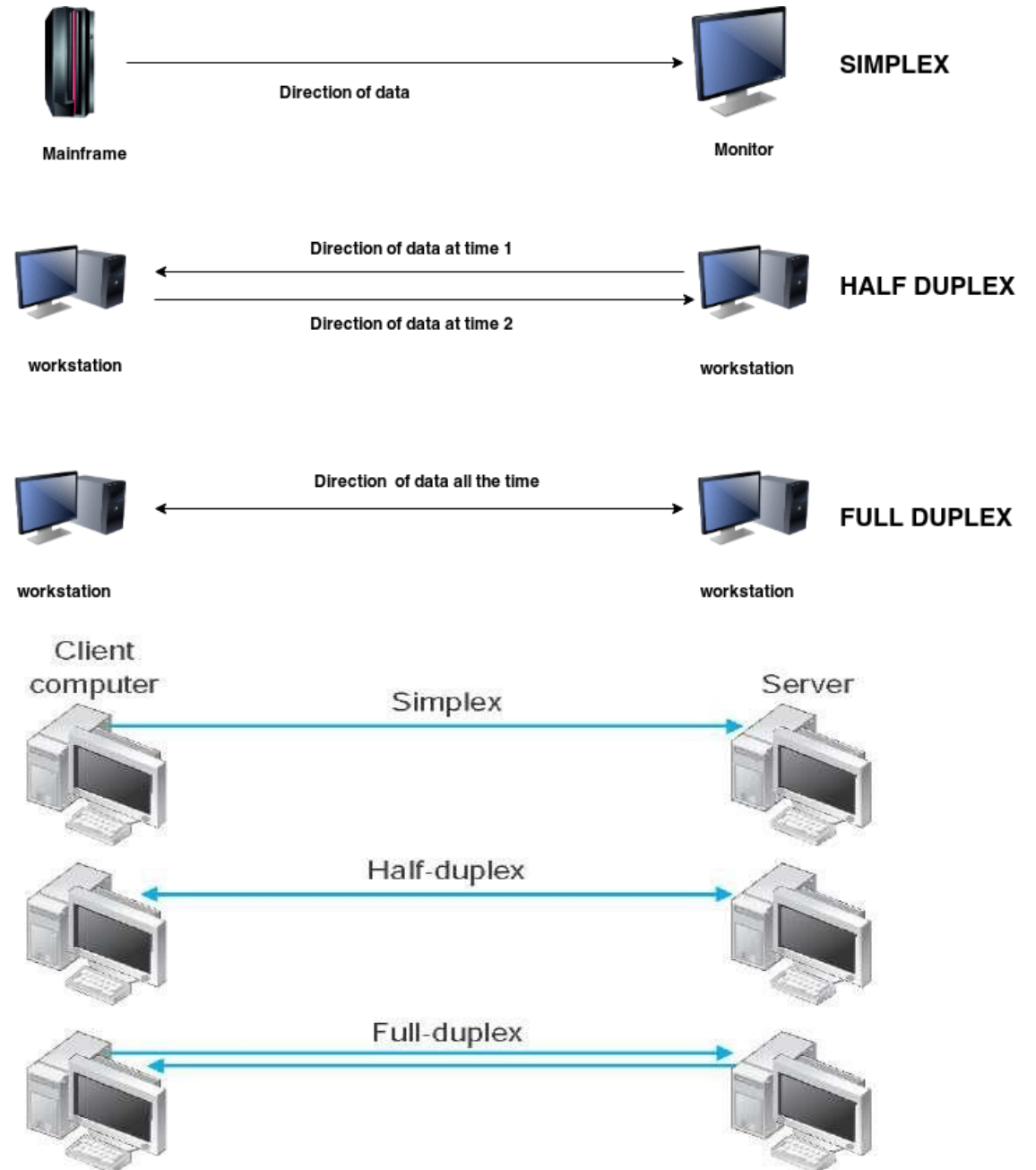
One collision Domain



Six Collision Domains

Simplex, Half-Duplex, and Duplex

- Simplex
 - Signal transmission: one direction
- Half-duplex transmission
 - Signal transmission: both directions
 - One at a time
- One communication channel
 - Shared for multiple nodes to exchange information
- Full-duplex
 - Signals transmission: both directions simultaneously
 - Used on data networks



Distance and Speed Limitations

Ethernet Types	Bandwidth Capacities
Standard Ethernet	10 Mbps: 10 million bits per second (that is 10 megabits per second)
FastEthernet	100 Mbps: 100 million bits per second (that is 100 megabits per second)
Gigabit Ethernet	1 Gbps: 1 billion bits per second (that is 1 gigabits per second)
10-Gigabit Ethernet	10 Gbps: 10 billion bits per second (that is 10 gigabits per second)
100-Gigabit Ethernet	100 Gbps: 100 billion bits per second (that is 100 gigabits per second)

The type of cabling used in your Ethernet work influences the bandwidth capacity and the distance limitation of your network.
See table 4-2, page 115

Ethernet Switch Features

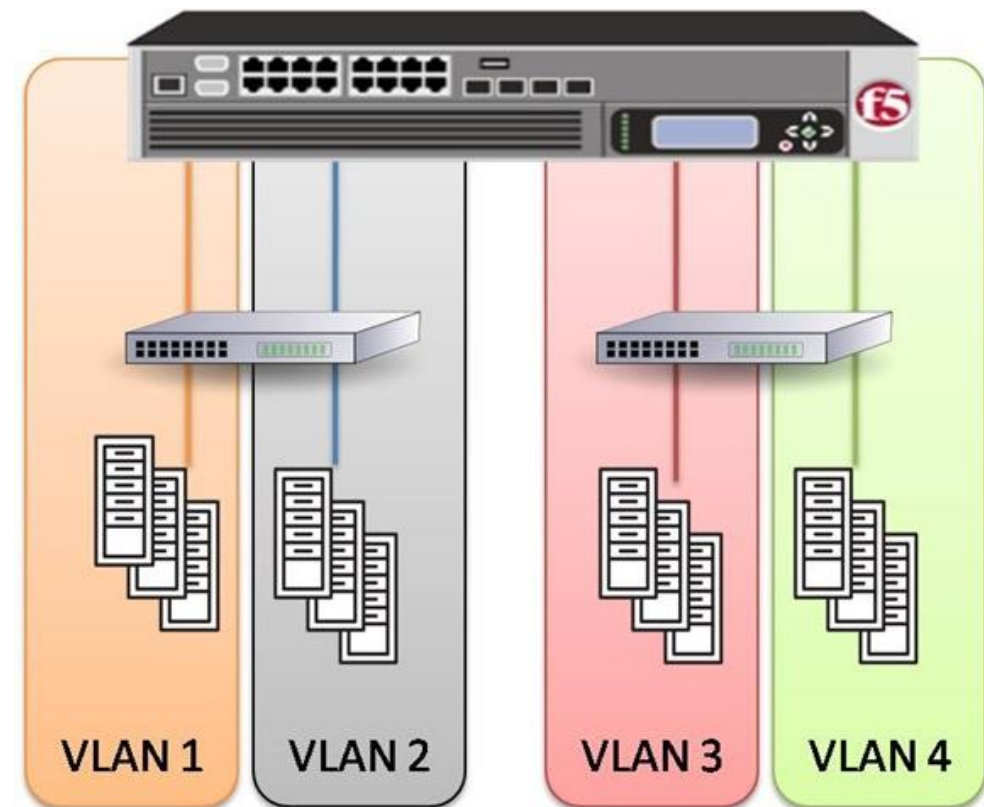
Virtual LANs (VLAN)

Most every Enterprise network today uses the concept of virtual LANs (VLAN).

Before understanding VLANs, you must have a very specific understanding of the definition of a LAN

What is a LAN?

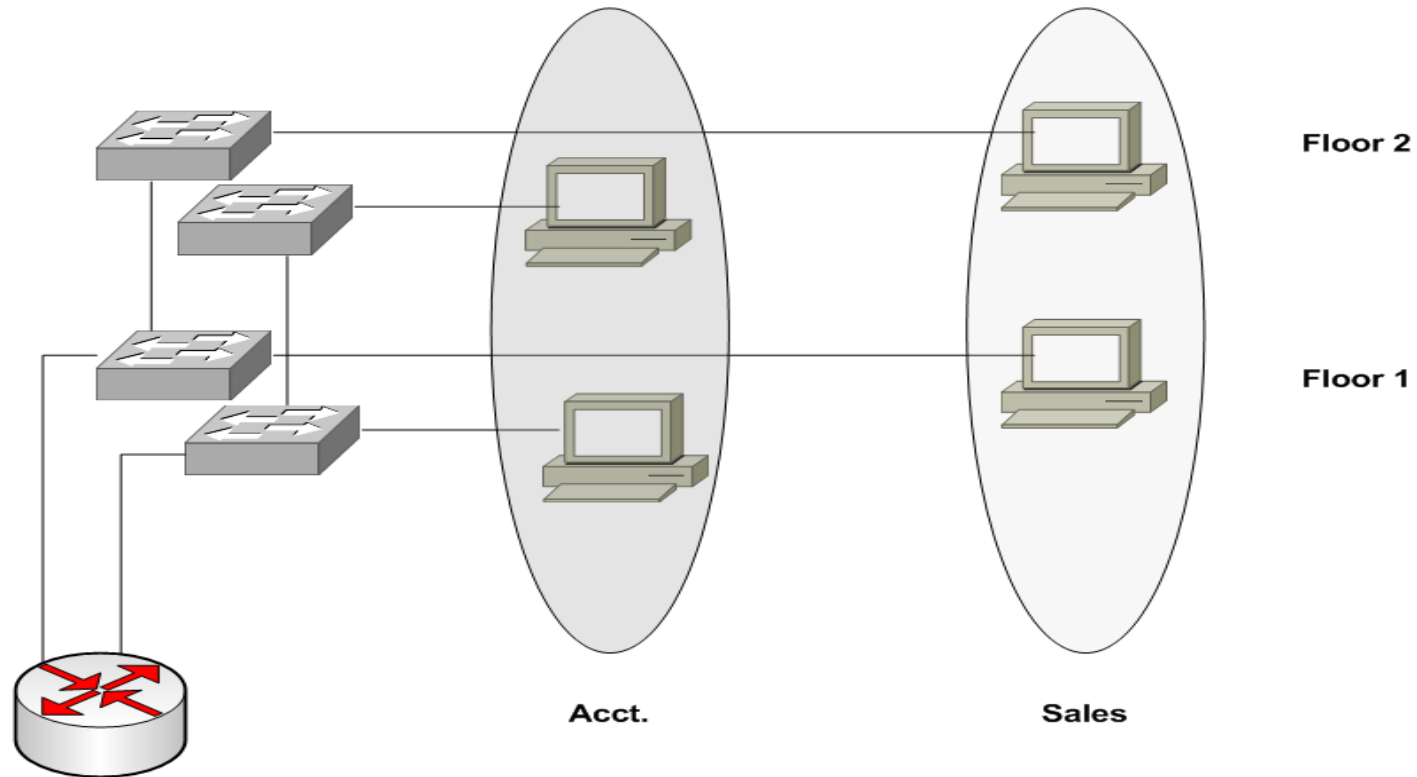
A LAN consists of all devices in the same broadcast domain.



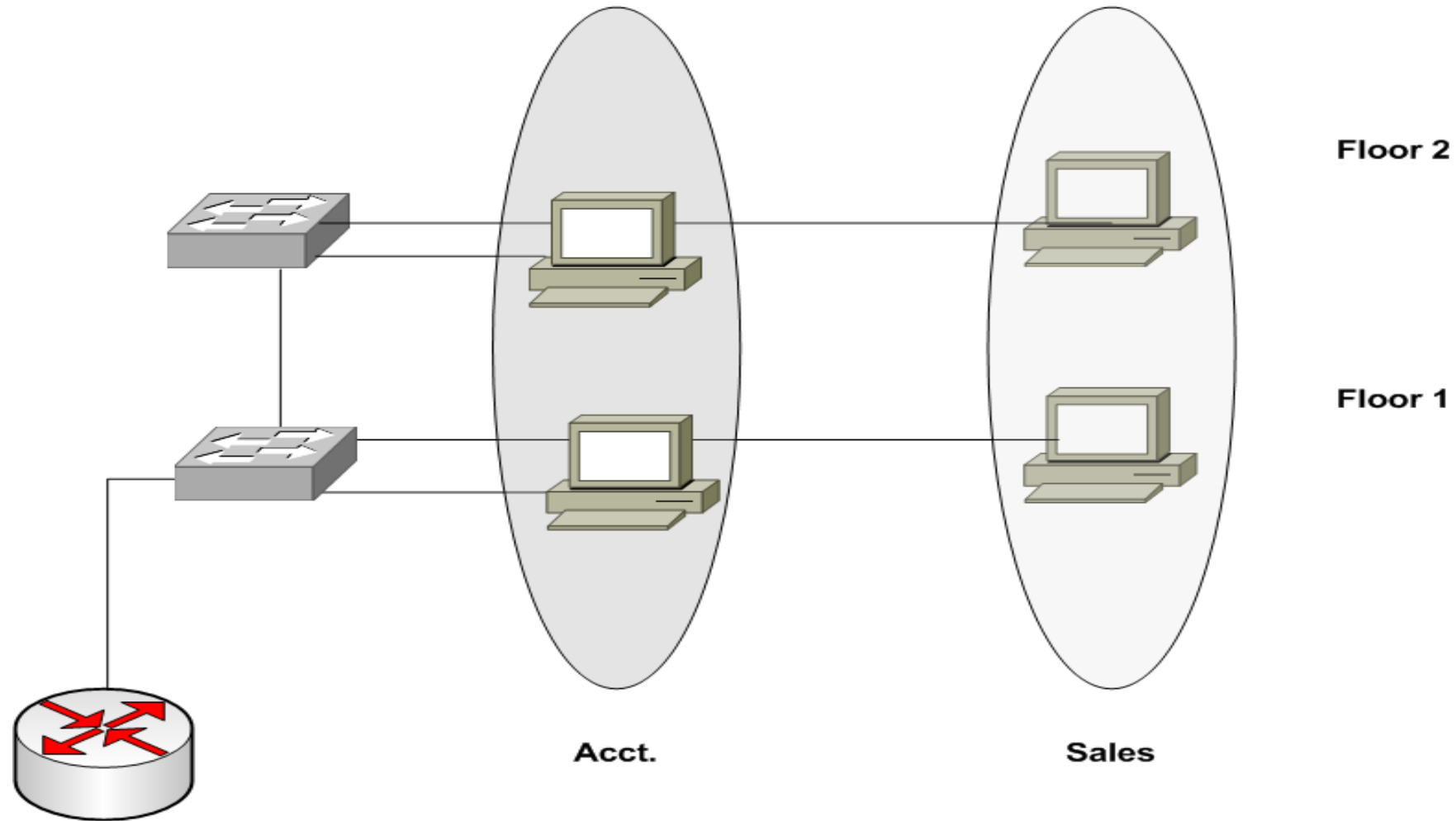
VLANs

- All ports on a switch form a single broadcast domain.
- To create VLANs the switch separates the ports into many broadcast domains based on configuration settings.

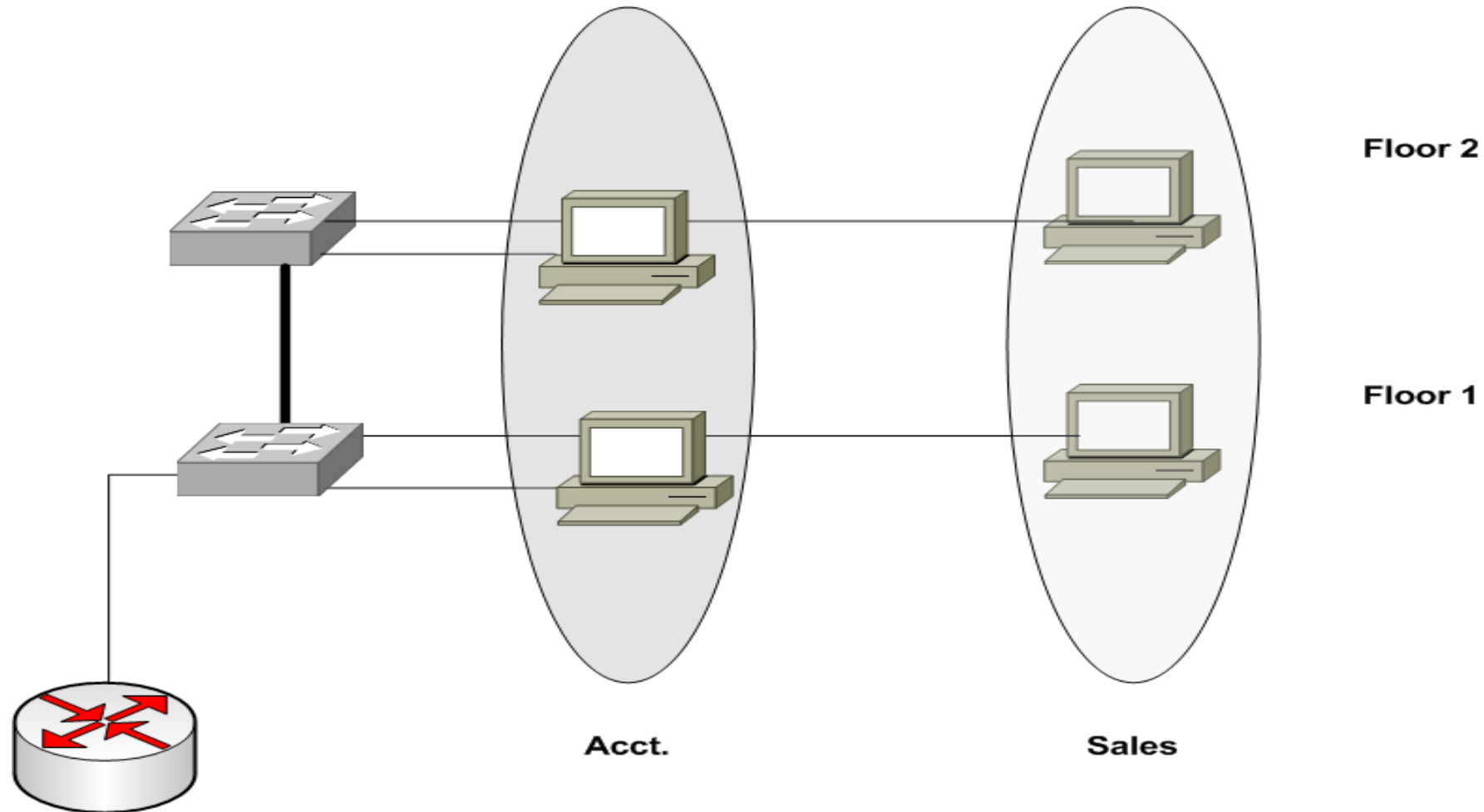
All Ports on a Switch belong to the same Subnet



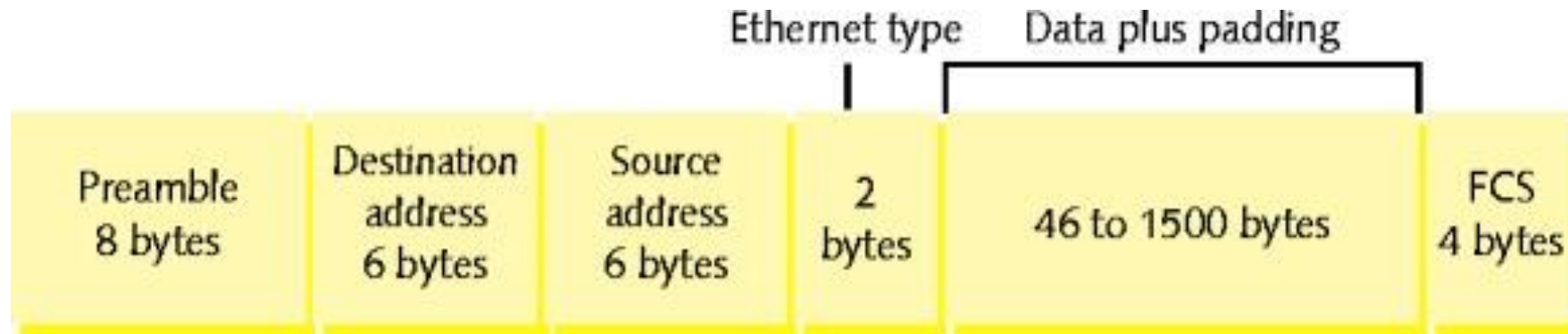
Ports on a Switch belong to the Different VLANs



Trunking Between Switches



Ethernet Frame

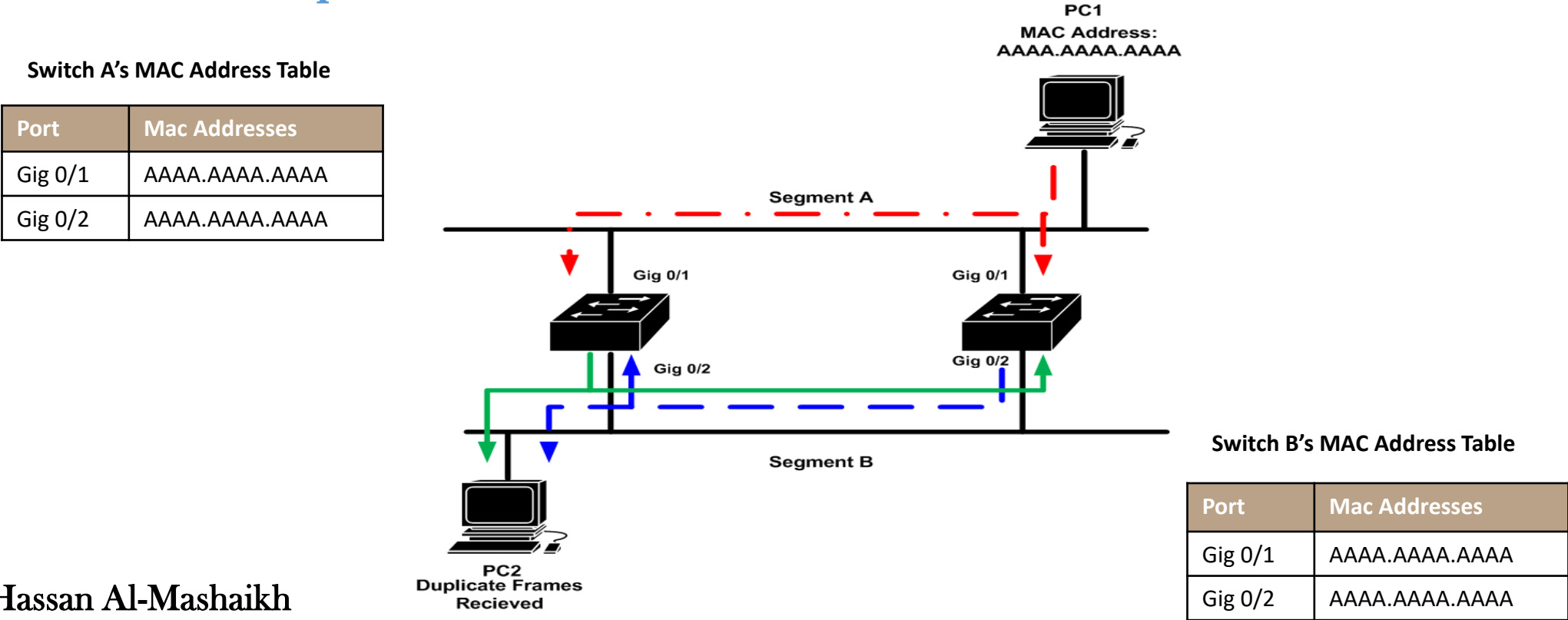


Ethernet_II (DIX) frame

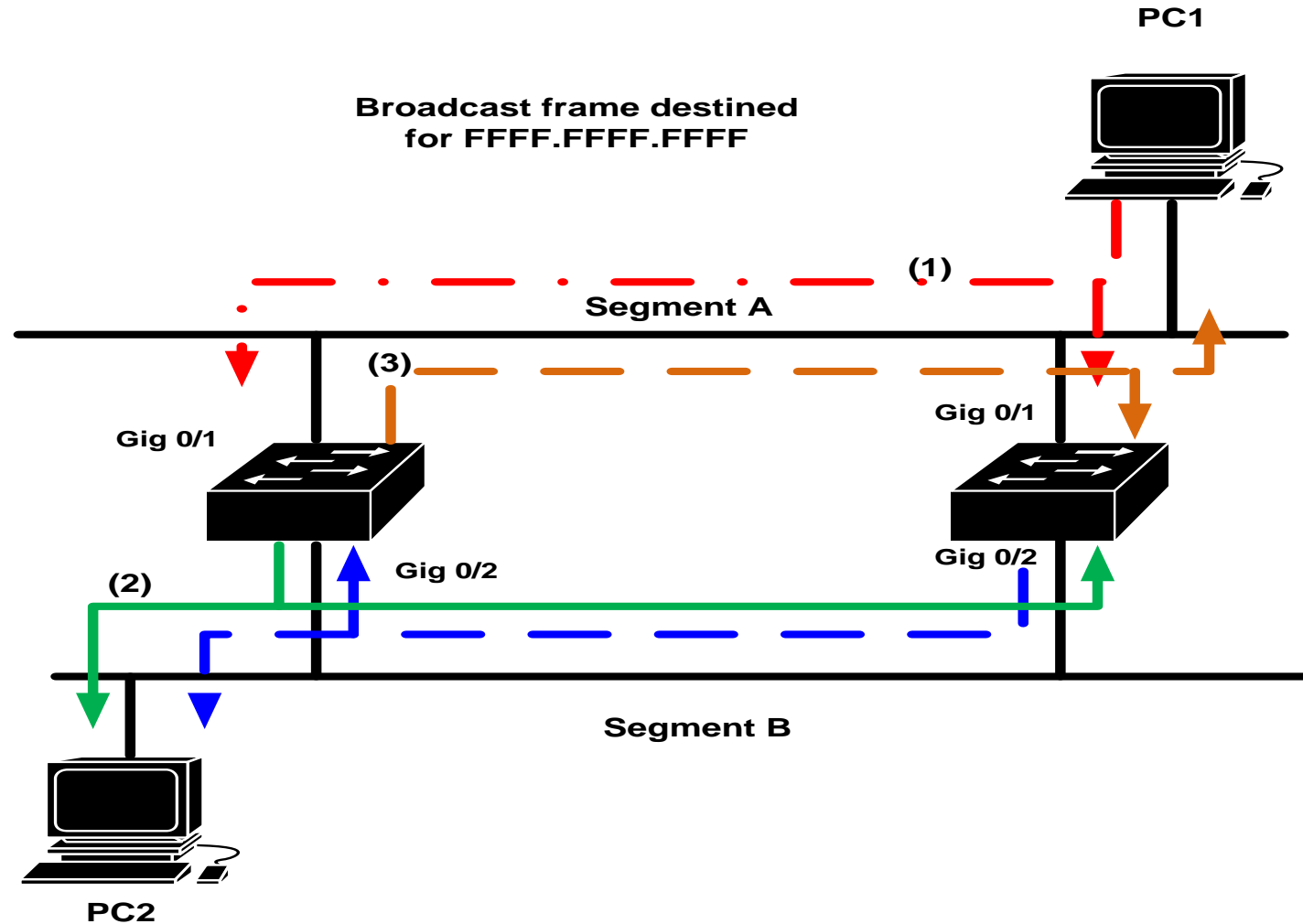
Spanning Tree Protocol

- Without the Spanning Tree Protocol (STP), frames would loop for an indefinite period of time in networks with physically redundant links.
- STP blocks some ports from forwarding frames so that only one active path exists between any pair of LAN segments.

MAC Address Table Corruption

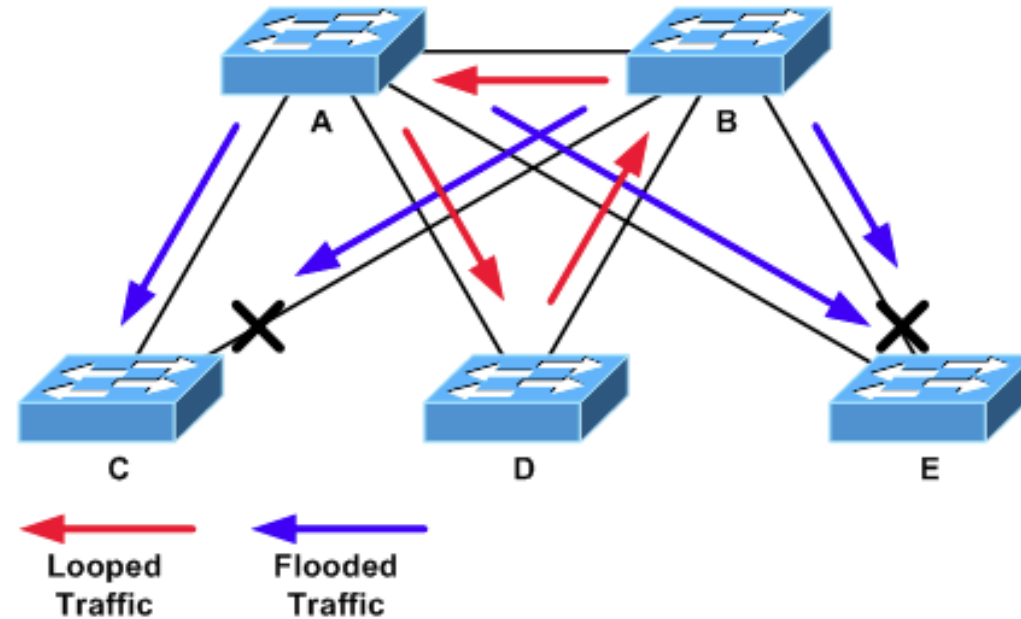


Broadcast Storm



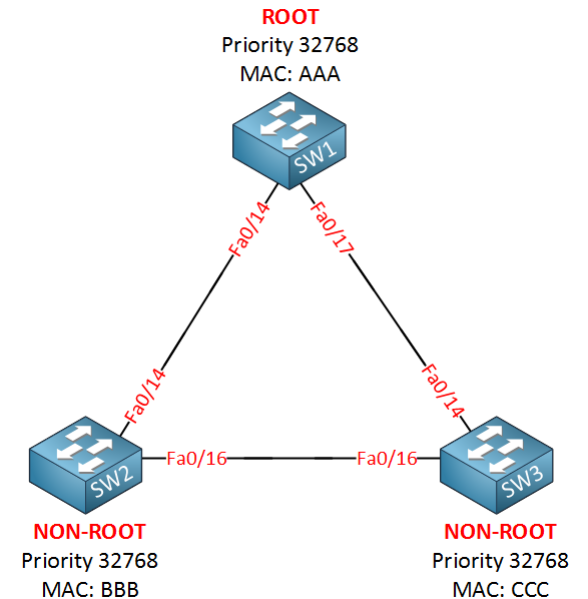
STP Terms

- Root Switch
- Non-root Switch
- Administrative Cost
- Root Port
- Designated Port
- Bridge ID
- Hello BPDU



How Spanning Tree Works

- First STP uses Hello messages, also called switch Protocol Data Units (BPDUs).
- Each switch and switch claims to be the root switch, and the one with the lowest bridge ID is elected root.
- The Bridge ID is a combination of a priority (2-byte) and a MAC address on the switch (6-byte).
- STP places all ports on the root switch into a forwarding state.
- The ROOT Switch continually sends Hello BPDUs.
- Each non-root switch receives and modifies the BPDUs and passes them on with a new cost inserted.
- Cost – port cost assigned to that interface plus the cost listed in a received Hello message..
- Each non-root switch uses the cost to find the lowest cost path back to the root.

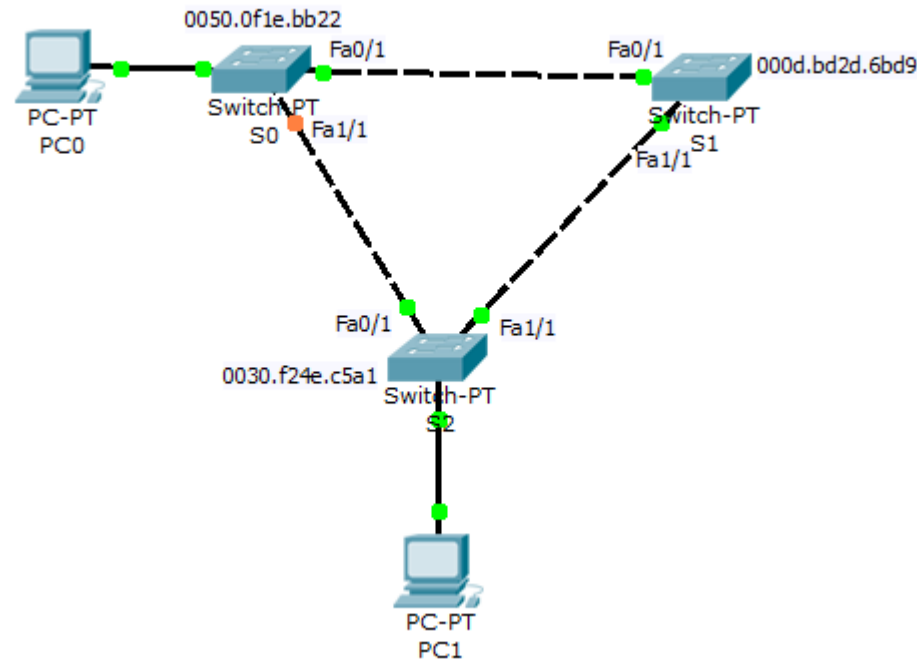


STP: Reasons for Forwarding State

Characterization of Port	STP STATE	Explanation
All the root switch's ports	Forwarding	The root switch is always the designated switch on all connected segments.
Each non-root switch's root port	Forwarding	The port through which the switch has the least cost to reach the root switch.
Each LAN's designated port	Forwarding	The switch forwarding the lowest-cost BDPU onto the segment is the designated switch for that segment.
All other ports	Blocking	The port is not used for forwarding frames, nor are any frames received on these interfaces considered for forwarding.

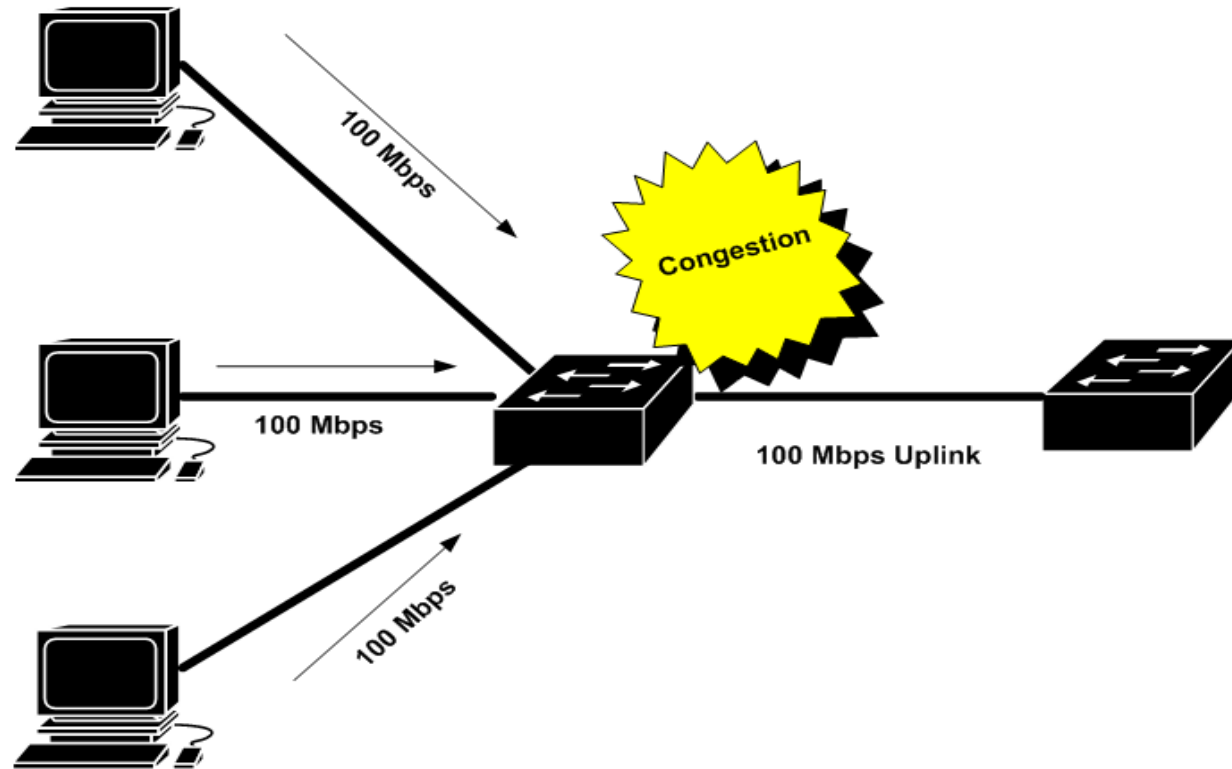
Other STP states

- Listening – Listens to incoming Hello messages to ensure that there are no loops, but does not forward traffic or learn MAC addresses on the interface. This is an interim state between blocking and forwarding.
- Learning – Still listens to BPDUs, plus learns MAC addresses from incoming frames. It does not forward traffic. This is an interim state between blocking and forwarding.
- Disabled – Administratively down.



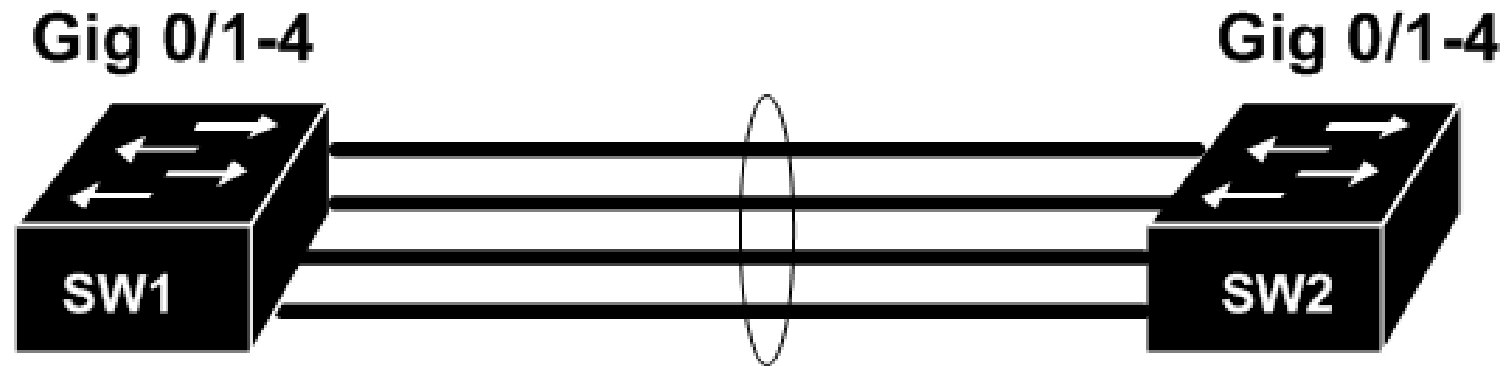
Link Aggregation

- If all port on a switch are operating at the same speed, the most likely ports to experience congestion is a port connecting to another switch or router up line from the device.



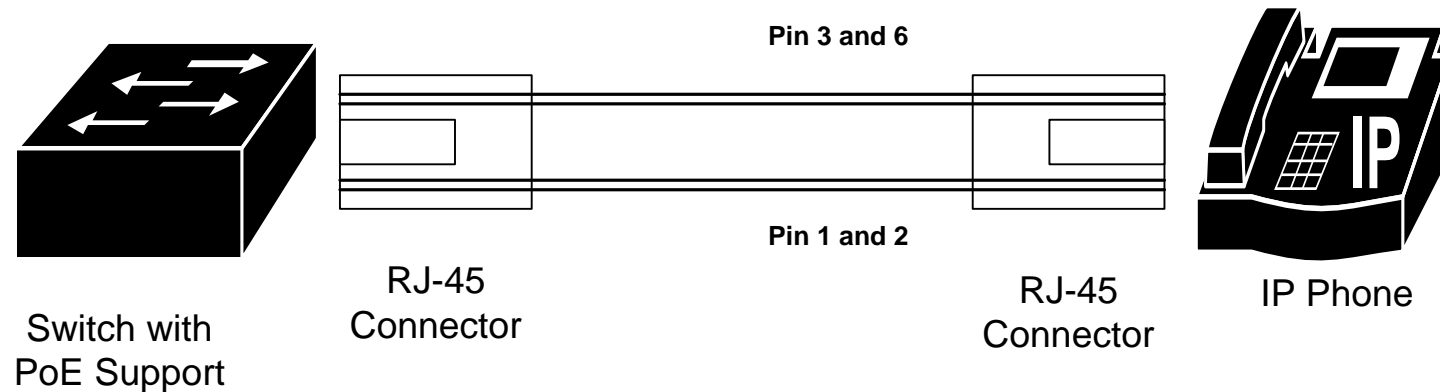
Link Aggregation

- To alleviate congested links between switches, you can logically combine multiple physical connection into a single logical connection.



Power over Ethernet (PoE)

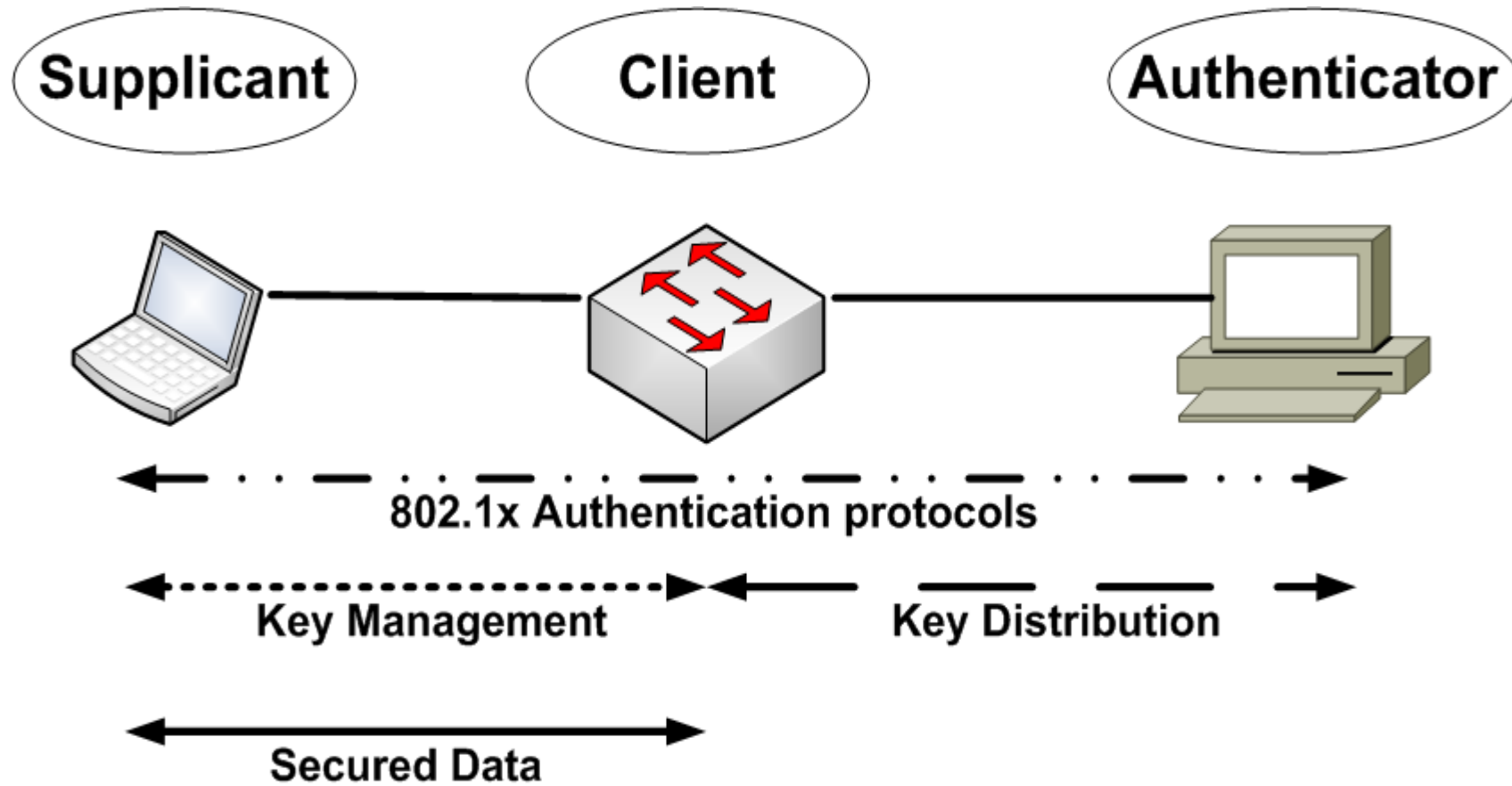
1. Switch applied 2.8 -10V DC to two pairs of leads to detect a 25k Ohm resistor in the attached device.
2. Next the switch must determine is how much power the attached device need. It does this by applying 15.5 – 20.5V DC, for a brief period.
3. Now the switch can apply the correct voltage, 44–57V DC



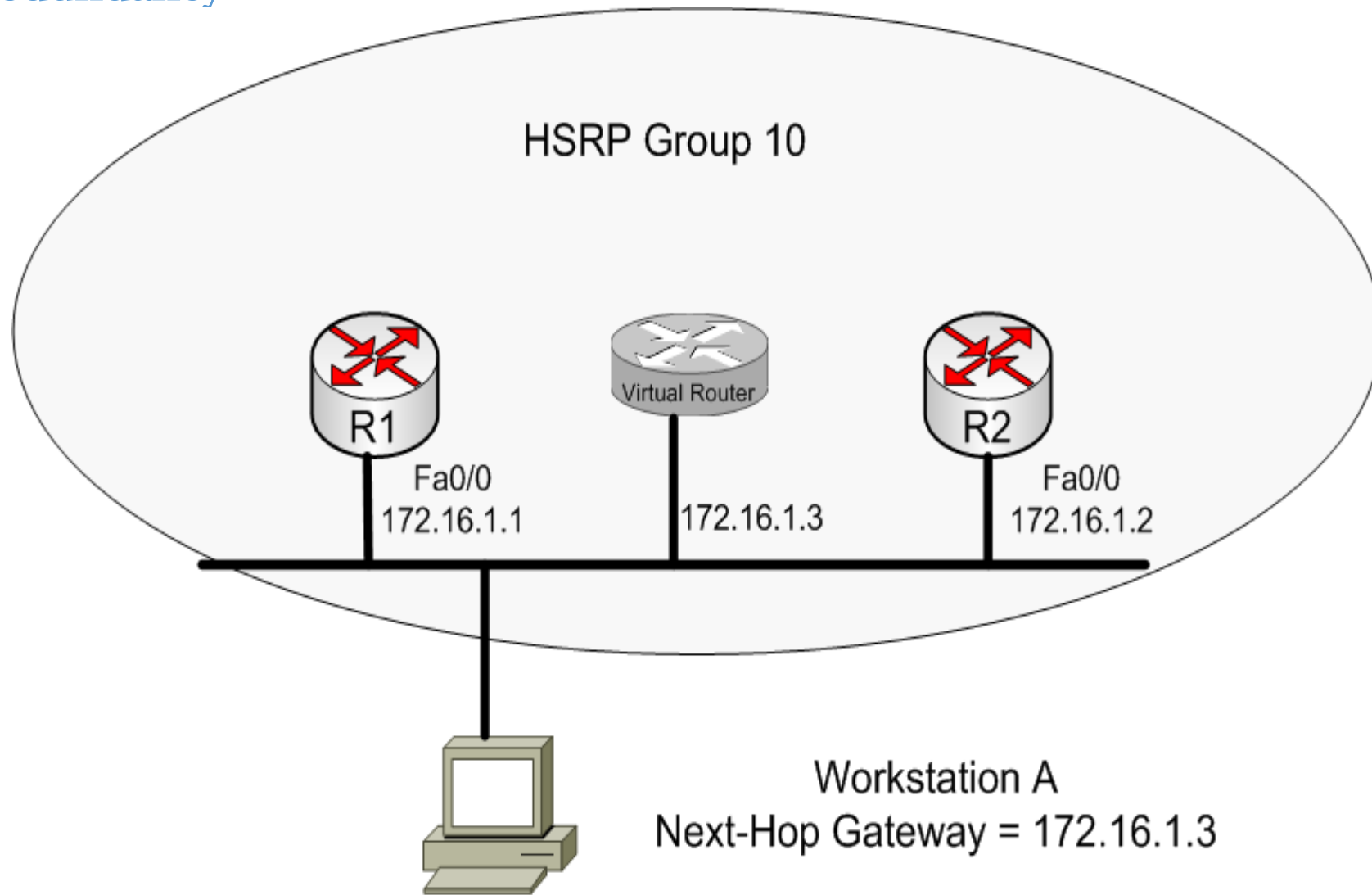
User Authentication

- For security purposes, some switches and AP's might require users to authenticate themselves before gaining access to the rest of the network.
- With 802.1X enabled, a switch or AP requires a client to authenticate before communicating on the network.
 - 802.1X terminology
 - Supplicant: the device that wants to gain access.
 - Client: the device that forwards the supplicant request to the server
 - Authenticator: the server that does the authentication.

User Authentication



First Hop Redundancy



Working with IP Addresses

Objectives

- What is the format of an IP version 4 (IPv4) address, and what are the distinctions between unicast, broadcast and multicast addresses?
- Which options are available for assigning IP addresses to network devices?
- Given a subnet design requirement (for example, a number of required subnets and a number of required hosts per subnet), how do you determine the appropriate subnet mask for a network?
- What are the primary characteristics of IPv6?



Working with IP Addresses

- When two devices on a network want to communicate, they need logical addresses.
- Most modern networks use Internet Protocol (IP) addressing, as opposed to other Layer 3 addressing.
- Two versions of IP addressed, first we will discuss how IP concepts are applied to IP version 4 (IPv4).
- Next, various options for assigning IP addresses to end stations are contrasted.

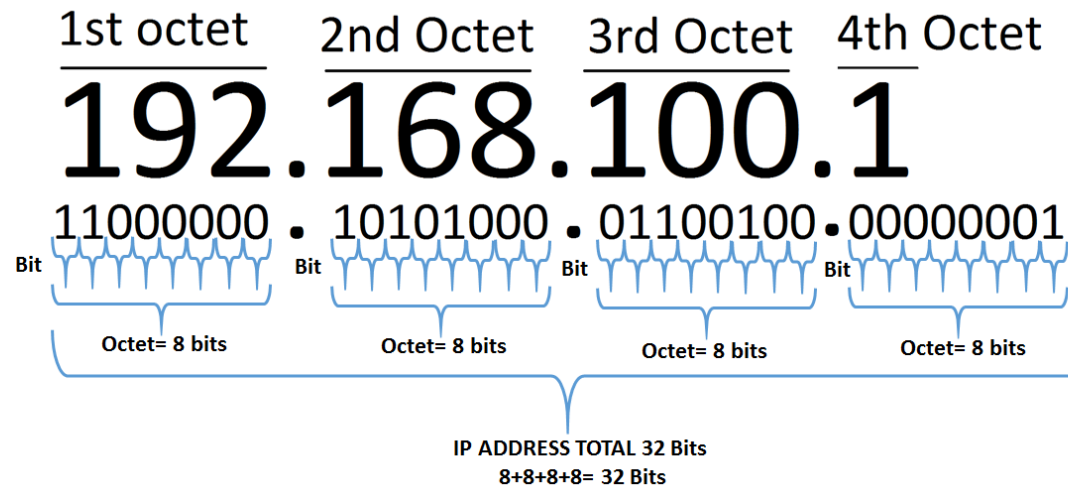
IPv4 Addressing

- Although IPv6 is increasingly being adopted in corporate networks, IPv4 is by far the most popular Layer 3 addressing scheme in today's networks.
- Devices on an Ipv4 network use unique IP addresses to communicate with one another.
- An IPv4 address is a 32-bit address. That is typically written in dotted-decimal notation. Such as 10.1.2.3
- Notice that the IP address is divided into four separate numbers, separated by periods.
- Each of these four divisions represents 8 bits, and are called octets.
- IP addressing
- Unique IP address per host
- Unique address per logical network
- Communicate between LANs without broadcasts



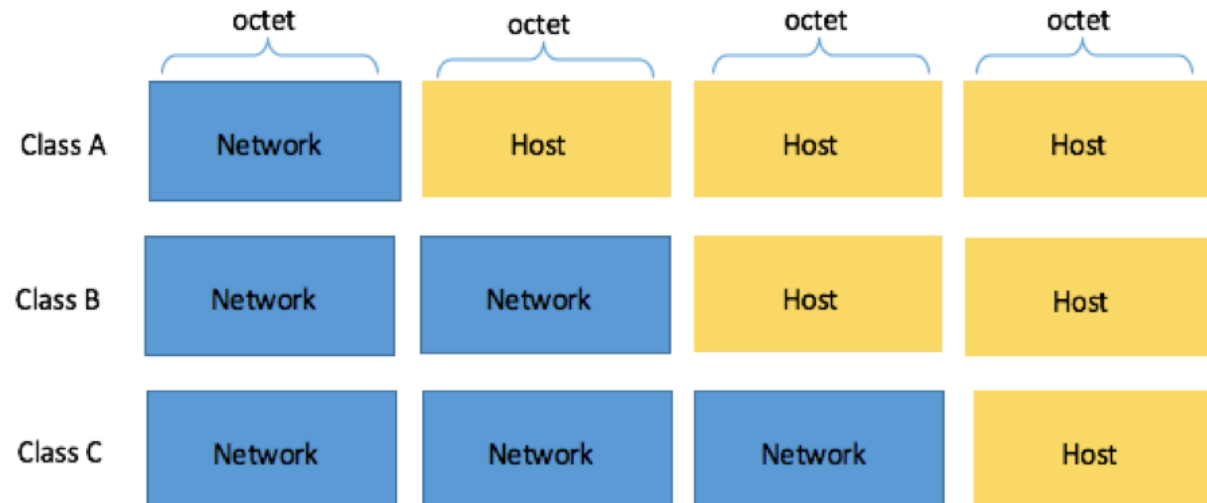
IPv4 Address Structure

- IP Addresses (IPv4 only)
- 32-bit value
- Example: 110000001010100000001000000010
- Broken into four groups of eight
11000000.10101000.00000100.00000010
- Each 8-bit value converted into a decimal number between 0 and 255, 192.168.4.2



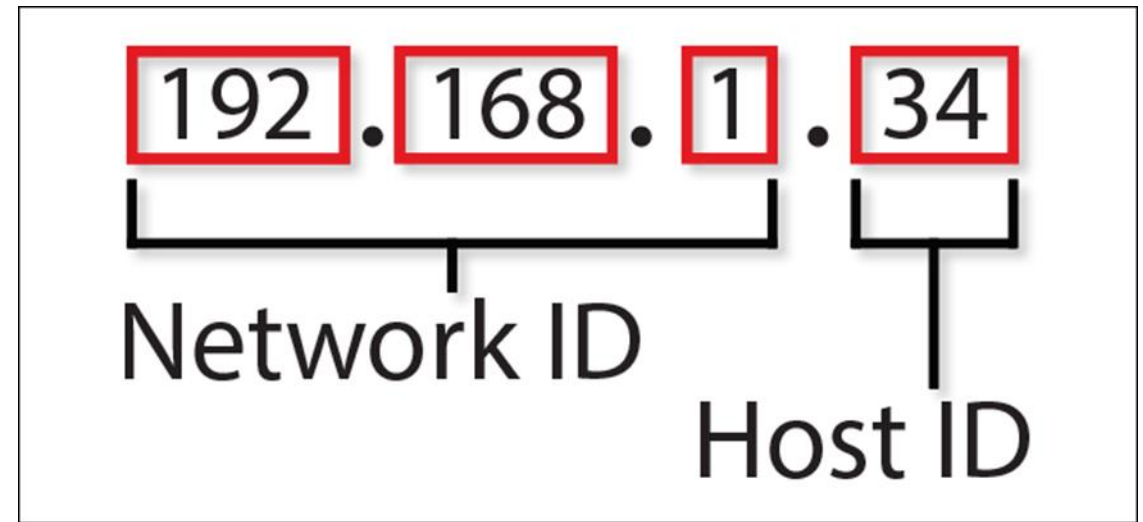
IPv4 Address Structure

- IP Addresses in Action
 1. IP must do three things
 2. Give each LAN its own identifier
 3. Allow routers connecting LANs to use network identifiers to send packets to the right network Give each computer a way to understand when a packet is intended for a computer on the local LAN or for a computer on the WAN
- 1. IP must give each LAN its own identifier
 - Network IDs
 - All computers on same LAN must have same **network ID**
 - Each computer on same LAN must have a **unique host ID**



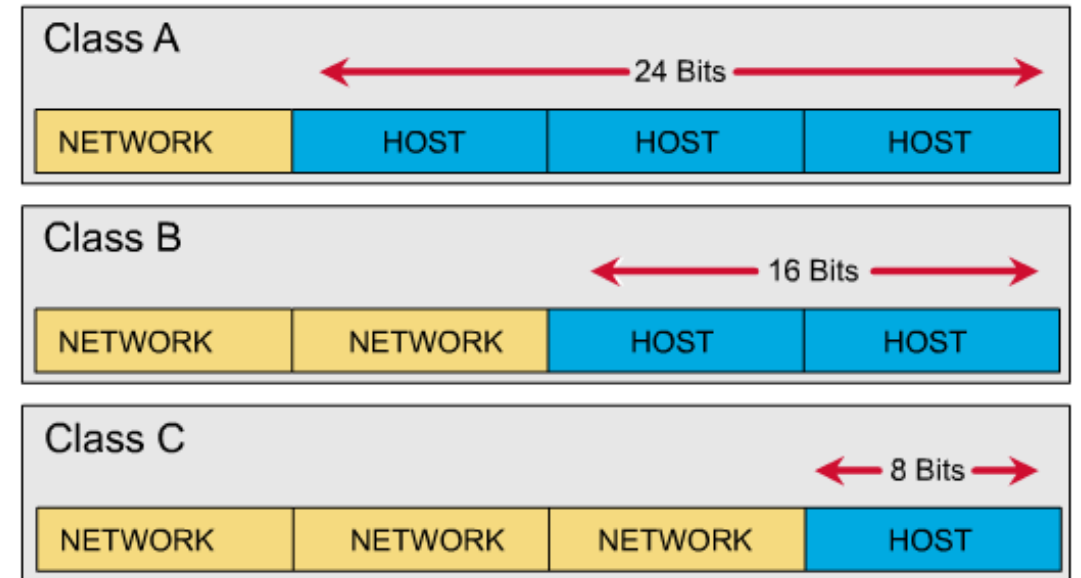
IPv4 Address Structure

- Network information (network ID)
 - First 8 bits in Class A address
 - First 16 bits in Class B address
 - First 24 bits in a Class C address
- Host information
 - Last 24 bits in Class A address
 - Last 16 bits in Class B address
 - Last 8 bits in Class C address



IPv4 Address Structure

- Example Class A network address: 114.56.20.33, 255.0.0.0
 - Network information = 114.
 - Host information = 56.20.33
- Example Class B network address: 147.12.38.81, 255.255.0.0
 - Network information = 147.12.
 - Host information = 38.81
- Example Class C network address: 214.51.42.7, 255.255.255.0
 - Network information = 214.51.42.
 - Host information = 7



IPv4 Address Classes

Address Class	Value in First Octet	Classful Mask (Dotted Decimal)	Classful Mask (Prefix Notation)
Class A	1 -126	255.0.0.0	/8
Class B	128 -191	255.255.0.0	/16
Class C	192 - 223	255.255.255.0	/24
Class D	224 – 239	N/A	N/A
Class E	240 – 255	N/A	N/A

IPv4 Special Address

Private Address

Address Class	Address Range	Default Subnet Mask
Class A	10.0.0.0 – 10.255.255.255	255.0.0.0
Class B	172.16.0.0 – 172.31.255.255	255.255.0.0
Class B	169.254.0.0 – 169.254.255.255	255.255.0.0
Class C	192.168.0.0 – 192.168.255.255	255.255.255.0

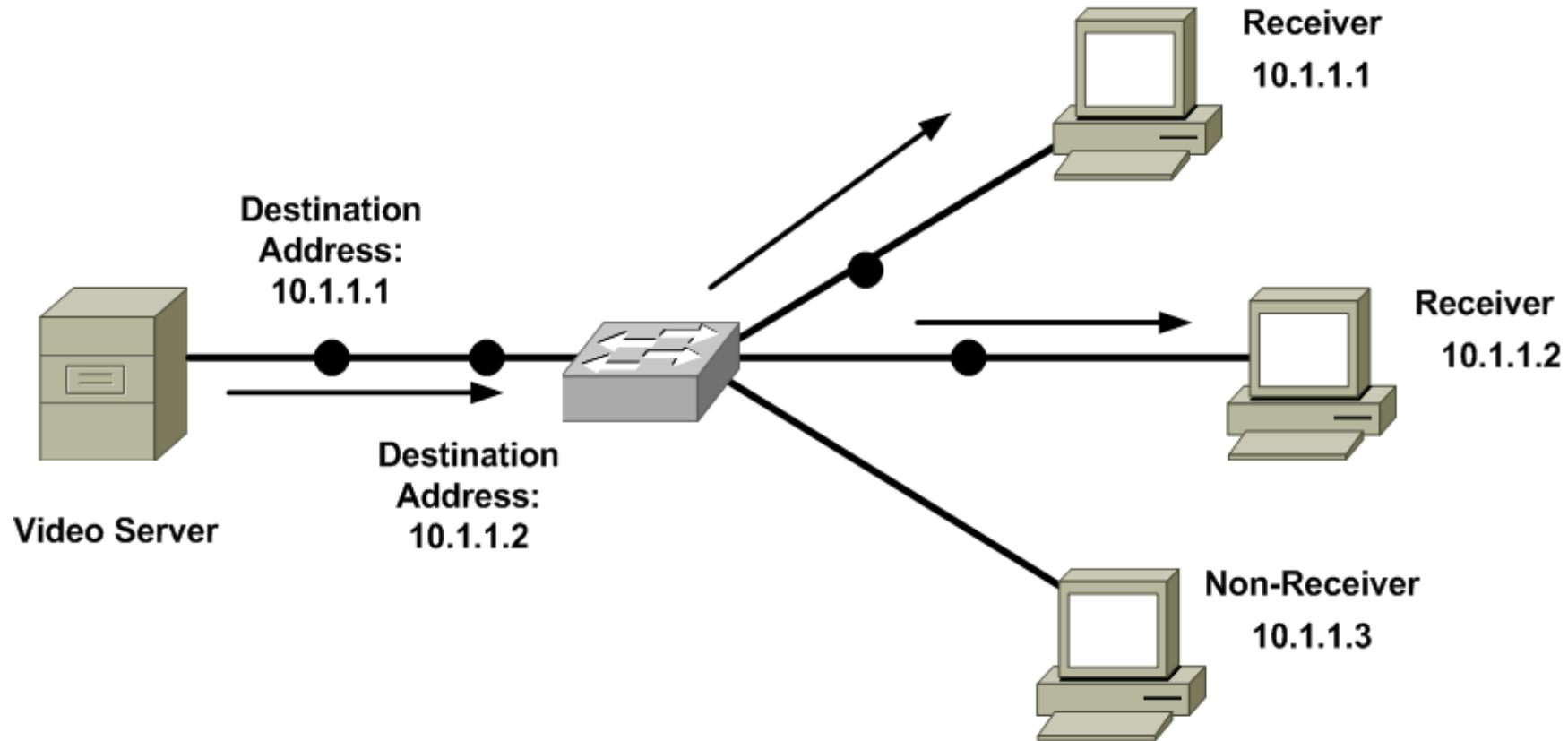
Loopback Address

Address Class	Address Range	Default Subnet Mask
Class A	127.0.0.1 – 127.255.255.255	255.0.0.0

Types of Addresses

■ Unicast

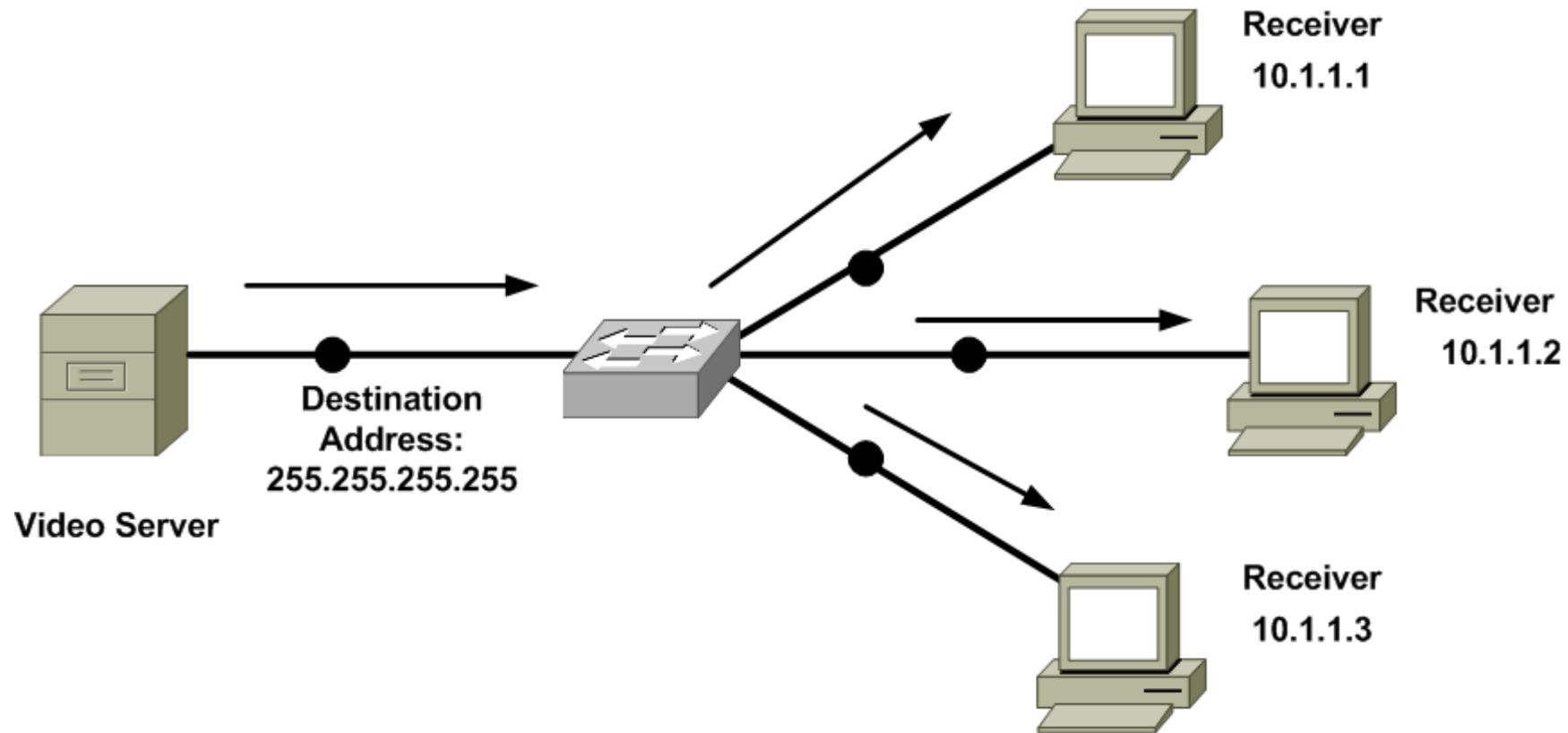
- meaning that traffic travels from a single source device, to a single destination device.



Types of Addresses

▪ Broadcast

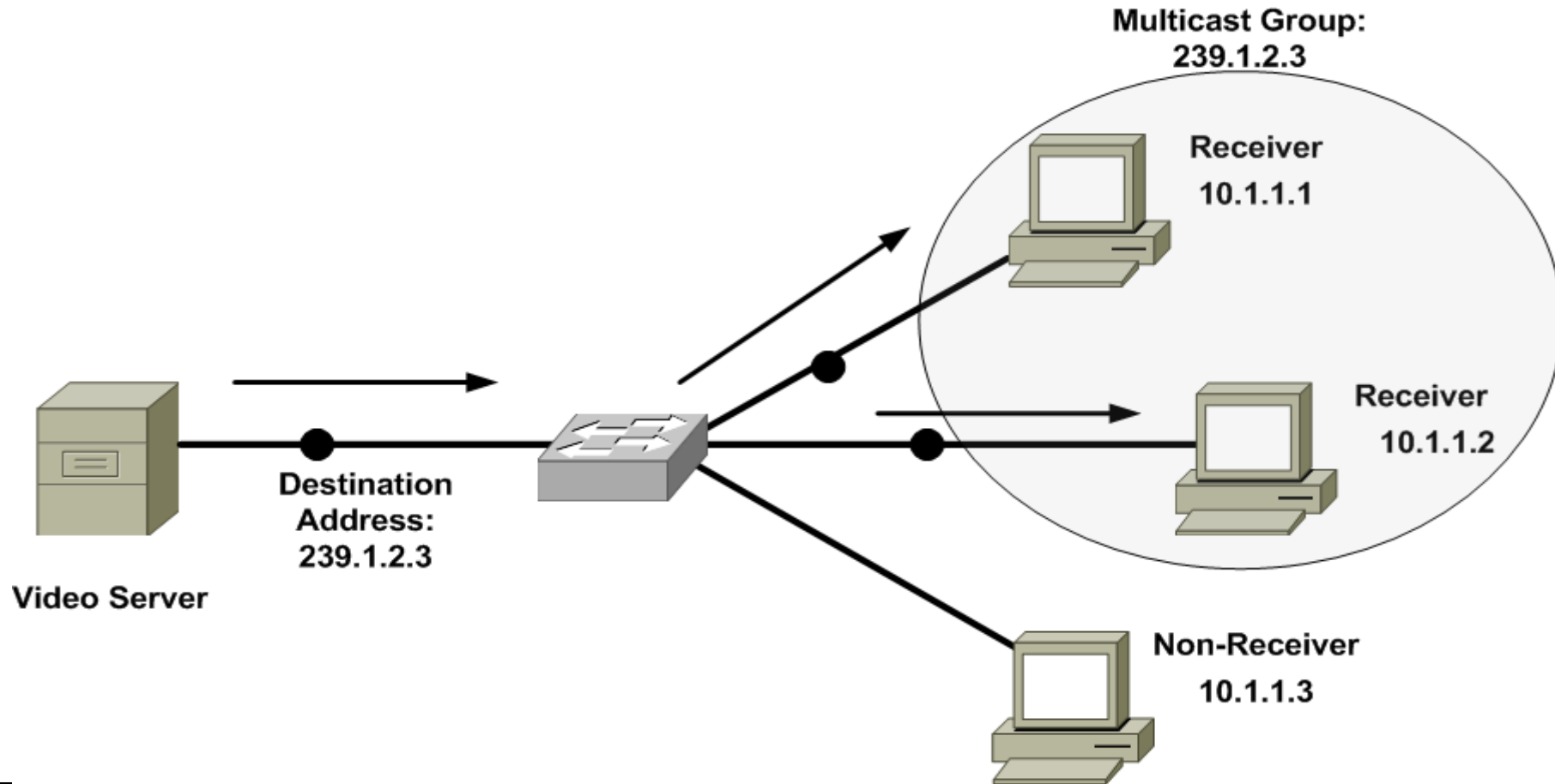
- meaning that traffic travels from a single source device, to all destination device.



Types of Addresses

■ Multicast

- meaning that traffic travels from a single source device, to multiple, yet specific, destination devices.



Assigning IPv4 Addresses

- At this point, you should understand that network each devices need an unique IP address.
- However, beyond just an IP address, what other IP address-related information does a host need to communicate?
- And how does it get them?
- IP address parameters required by each host to be able to communicate on the LAN and beyond.
- IP address
- Subnet mask
- Default gateway
- DNS server address
- A simple way of configuring a PC, with IP address parameters is to statically configure that information.
- This is time consuming, prone to human errors, and is not practical in large enterprise networks.
- Instead of static IP address assignments, many corporate networks dynamically assign IP address parameters to their devices.

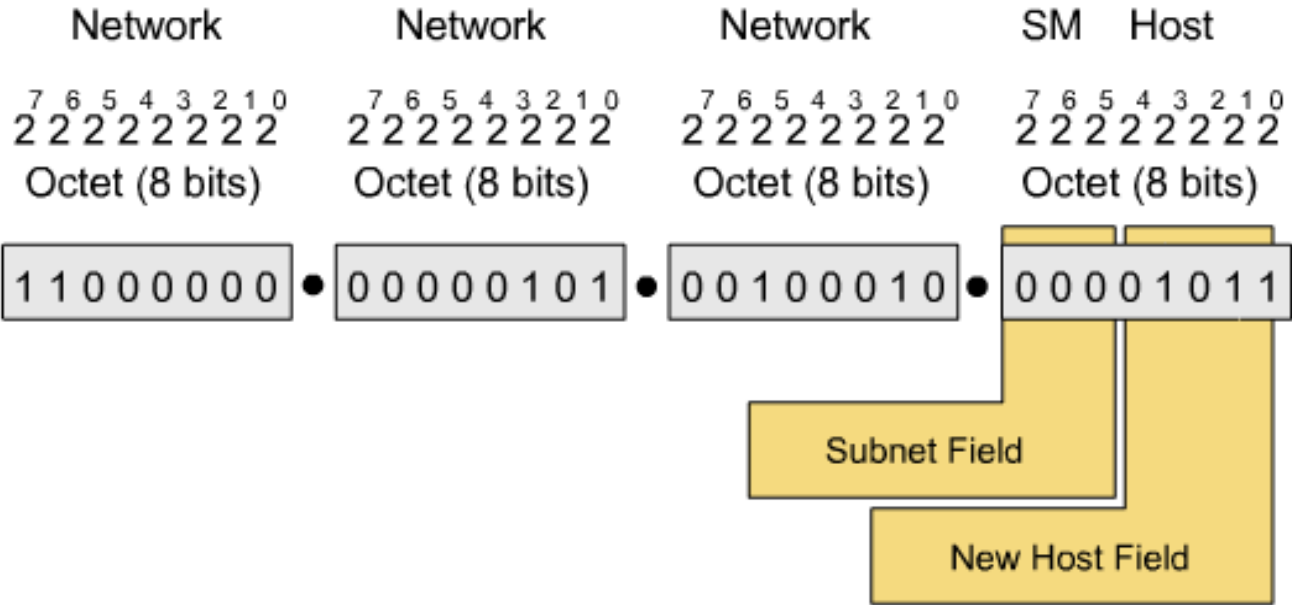
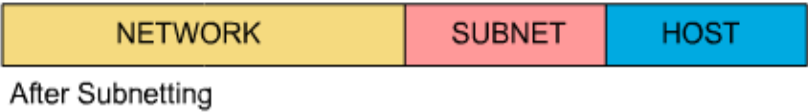
Assigning IPv4 Addresses

- There are two options when using automatic assigning of IP addresses.
- Bootstrap Protocol (BOOTP)
- A method of assigning IP address, subnet mask and default gateway information to diskless workstation.
- Dynamic Host Configuration Protocol (DHCP)
- A method of assigning IP address, subnet mask, default gateway, DNS server, and more.
- When a device does not have a static IP address configured and it can not contact a DHCP server, it still might be able to communicate on an IP network thanks to Automatic Private IP Addressing (APIPA).
- APIPA allows a network device to self-assign an IP address from the 169.254.0.0/16 network.

Subnetting

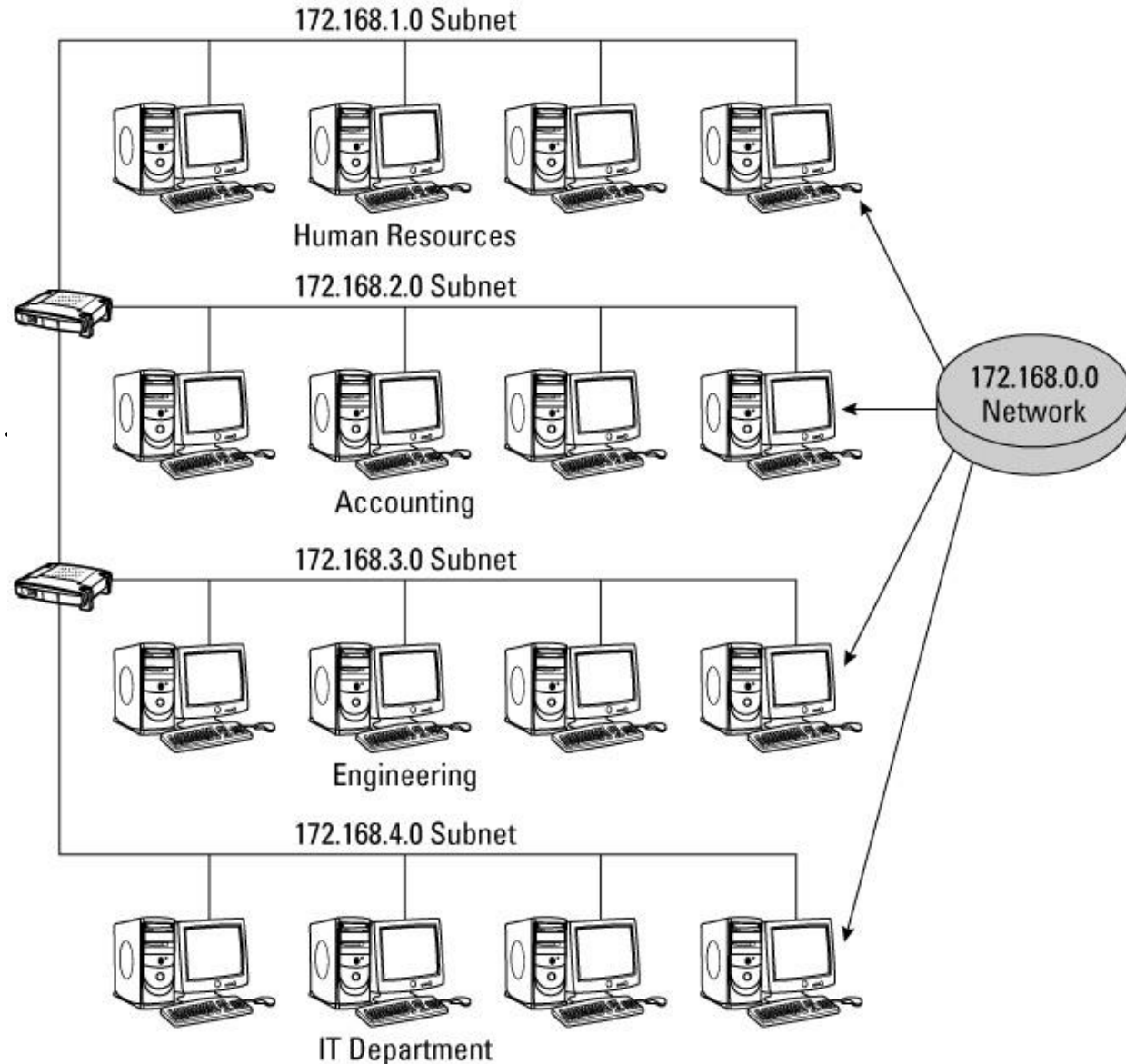
- Default subnet mask (that is, classful subnet mask) are not always the most efficient choice.
- Fortunately we can add additional bits to a subnet masks (thereby extending the subnet mask) to create subnets within a classful network.
- To create a subnet address, a network administrator borrows bits from the original host portion and designates them as the subnet field.

SOLUTION: Create another section in the IP address called the subnet.



Purpose of Subnetting

- More efficient use of IP addresses than classful default
- Enables separation of networks for security
- Enables bandwidth control
- Subnet mask is cornerstone of subnetting
 - Extend subnet masks of /8, /16, or /24 subnet by adding more ones (removing equal number of zeroes).



Subnetting (how-to)

- The process
- The class rules define the network part
- The mask binary 0s define the host part
- What's left over defines the size of the subnet part.
- Number of subnets = $2^{\text{number-of-subnet-bits}} - 2$
- Number of hosts per subnet = $2^{\text{number-of-host-bits}} - 2$
- IP addressing conventions define that two subnets per network should not be used and that two hosts per subnet should not be used.
- This equates to the formula $2^n - 2$

IP Subnetting Guide

1. To subnet an IP address we need to setup our work sheet as follows:
(this will aid you in completing the work.)
- First, at the top of your work sheet lay out the number line as shown.

7	6	5	4	3	2	1	0 Power of 2 line
128	64	32	16	8	4	2	1 Answer line

2[■] -2= 192.168.0.0

- Next, place the subnetting formula at the left of the number line.
- Third, write down the base IP address that you will be subnetting, as shown.
- Last, notice the box above the subnetting formula;
this is to place your power of two from the power line.

IP Subnetting Guide

2. It is time to start the process of subnetting an IP address.
 - a. The first thing that we must do is to decide how many subnets that you need. This is done by looking at how many ports are on your router. For example if your router has four ports on the back and three are going to be used for your network, we will need to subnet our base IP Address into three networks.
3. Turn to your work sheet; place the number 3 with a question mark next to the formula, as shown.

$$2^{\blacksquare} - 2 = 3?$$

IP Subnetting Guide

4. Next, look at the bottom line on the sheet and find the number that is closest to your answer after subtracting 2 from it.
 - a. Then, look at the number above it and place it in the box. (by looking at the answer line and subtracting 2 from it, we find the $8-2=6$ and the number above is 3, so 3 goes in the box) Then strike through your old answer
5. The next step is to calculate the new subnet mask number.
 - a. This is done by looking at the number that is in the box. (From this number we will be placing a one below the number line starting from the left, as shown).
 - b. Then take the numbers above the ones and add them up $128+64+32=224$. Then combine them with the default subnet mask for that class address as shown.
6. Now we have to figure out the network separation number. To do this look at the rightmost one; the number above it is your separation number.
 - a. This number is going to be used to set the beginning address for each of the three networks. In my example the number is 32. This is the number that we are going to use.
7. The next step is to create an IP Address for each of our router ports. This is generally the first usable IP Address after the network number.

By : Eng. Ahmad Hassan Al-Mashaikh

Email : Ahmad.private.mashaikh@Hotmail.com

IP Subnetting Guide

8. Now we need to find the broadcast address. This is always the last number in the range. To find it, subtract one from the next network number.
9. The last thing is to fill in between the router # and the broadcast #; this is called the **VALID HOST RANGE**.
10. Now you are done

Classless Inter-Domain Routing

- Although subnetting is the process of extending a classful subnet mask (that is, adding 1's to a classful mask), **Classless Inter-Domain Routing (CIDR)** does both.
- CIDR, is used by our ISP's in the world to control the addressing groups assigned to them by ARIN.



IPv6 Addressing

With the global proliferation of IP-based networks, available IPv4 address have run out.

Fortunately, IPv6 provides enough IP address for many generations to come.

IPv6 dramatically increases the number of available IP address. IPv6 offers approximately $5 * 10^{28}$ IP address for each person on the planet.



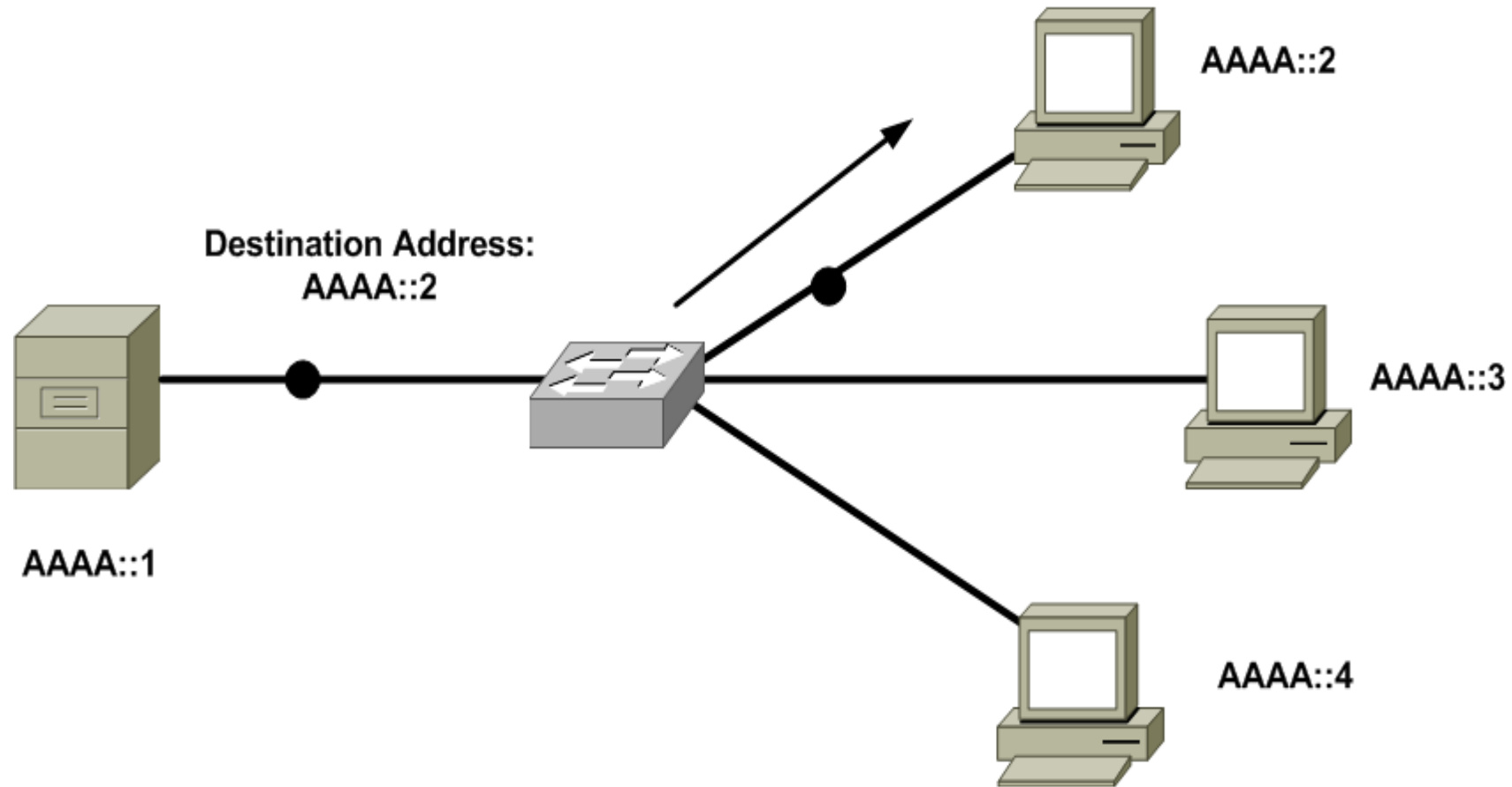
IPv6 Addressing

- IPv6 Features:
- Simplified header
- No broadcast
- No fragmentation
- Can coexist with IPv4

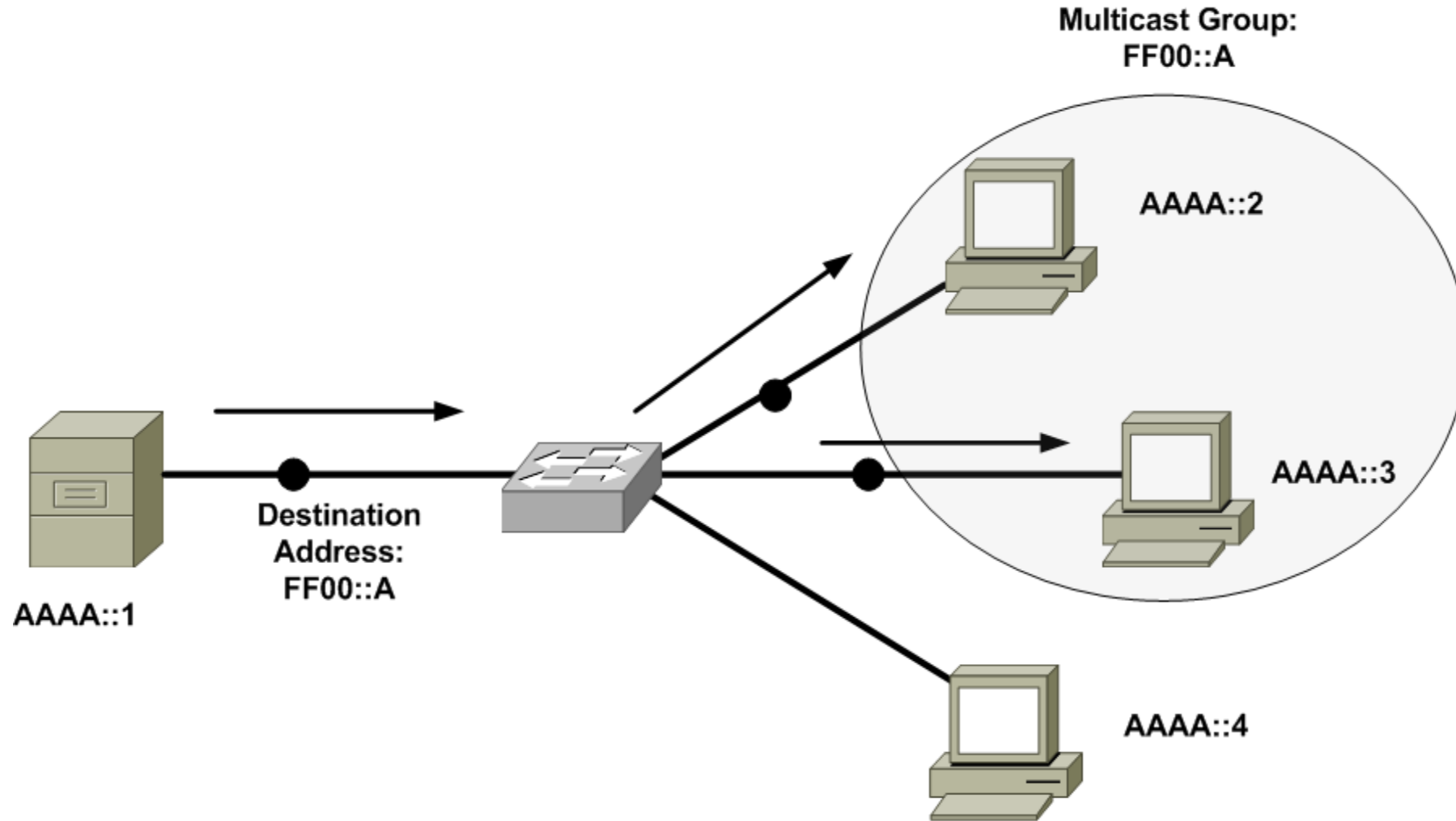
IPv6 Address Structure

Feature	IPv6
Size of address (bits or bytes per octets)	128 bits, 16 octets
Example address	0000:0000:0000:0000:0000:FFFF:FFFF:0A01:0101
Number of possible address, ignoring reserved values	2^{128} , or roughly $3.4 * 10^{38}$

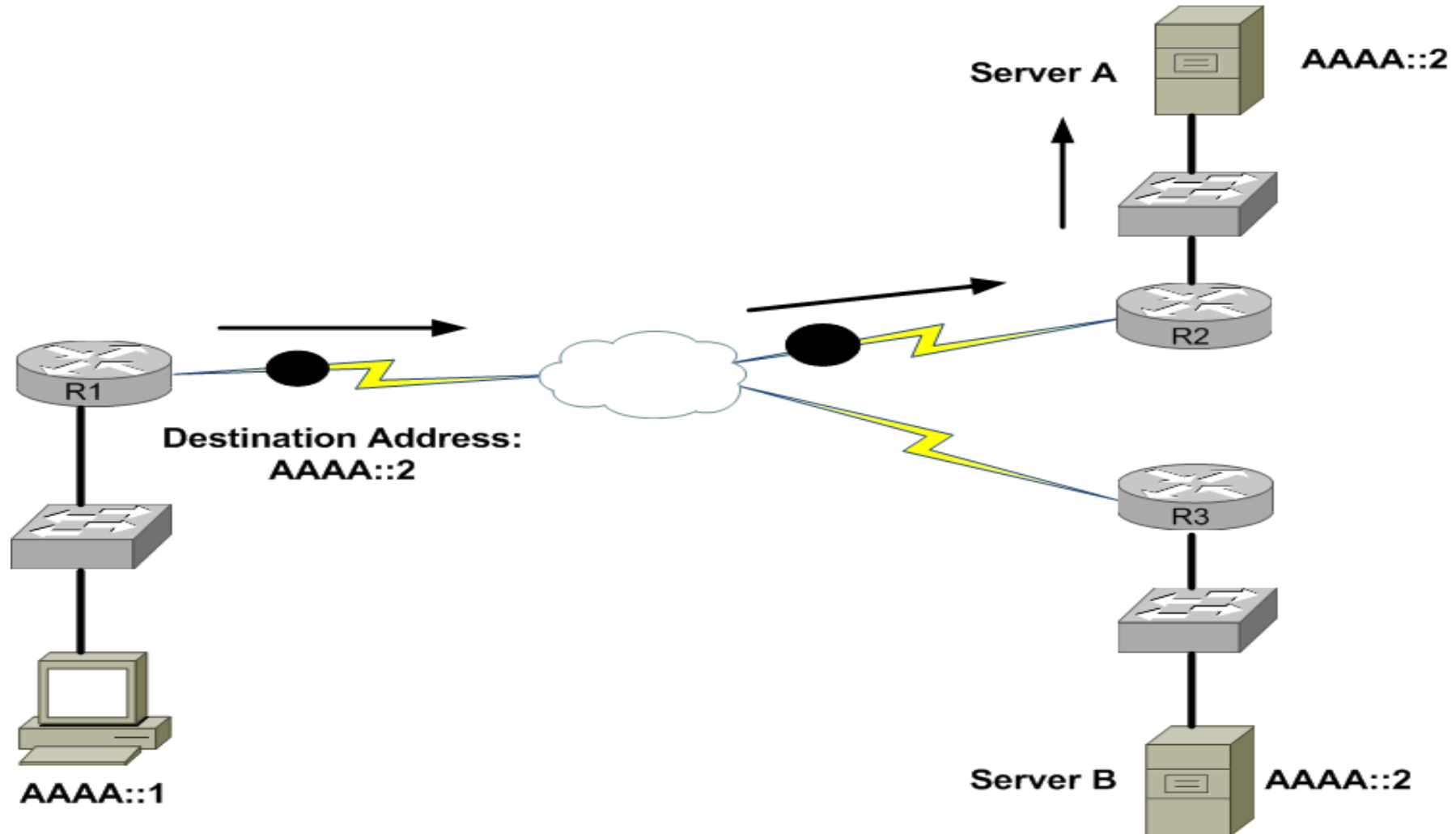
IPv6 Unicast



IPv6 Multicast



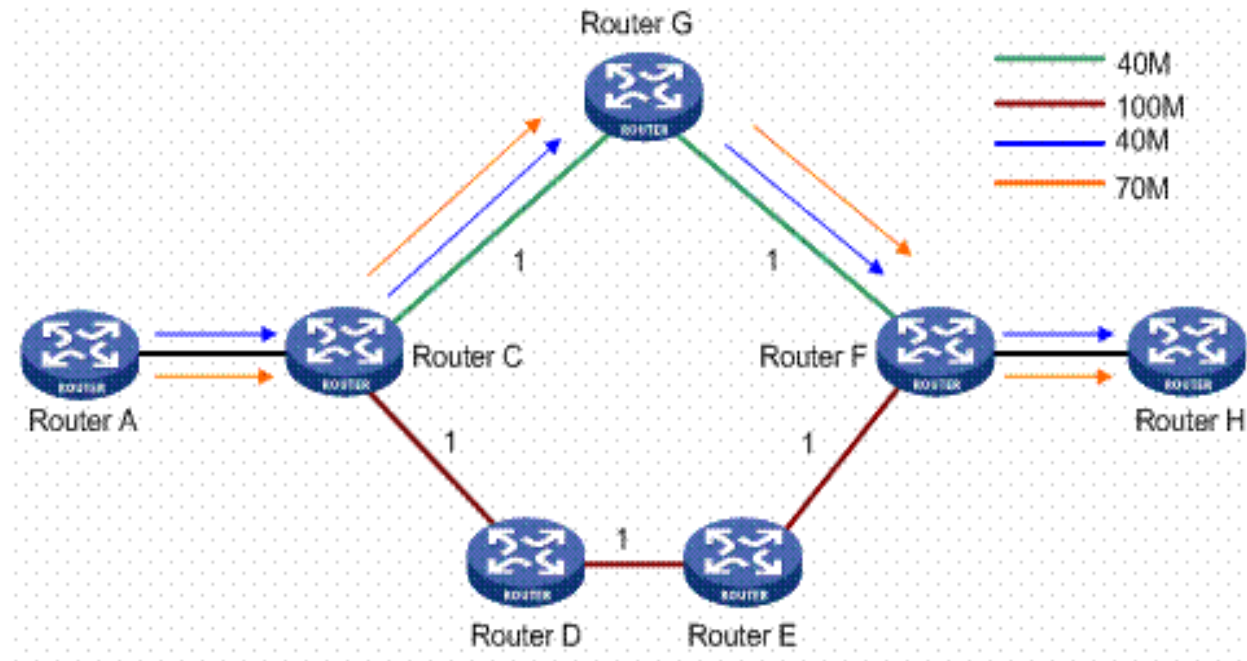
IPv6 Anycast



Routing Traffic

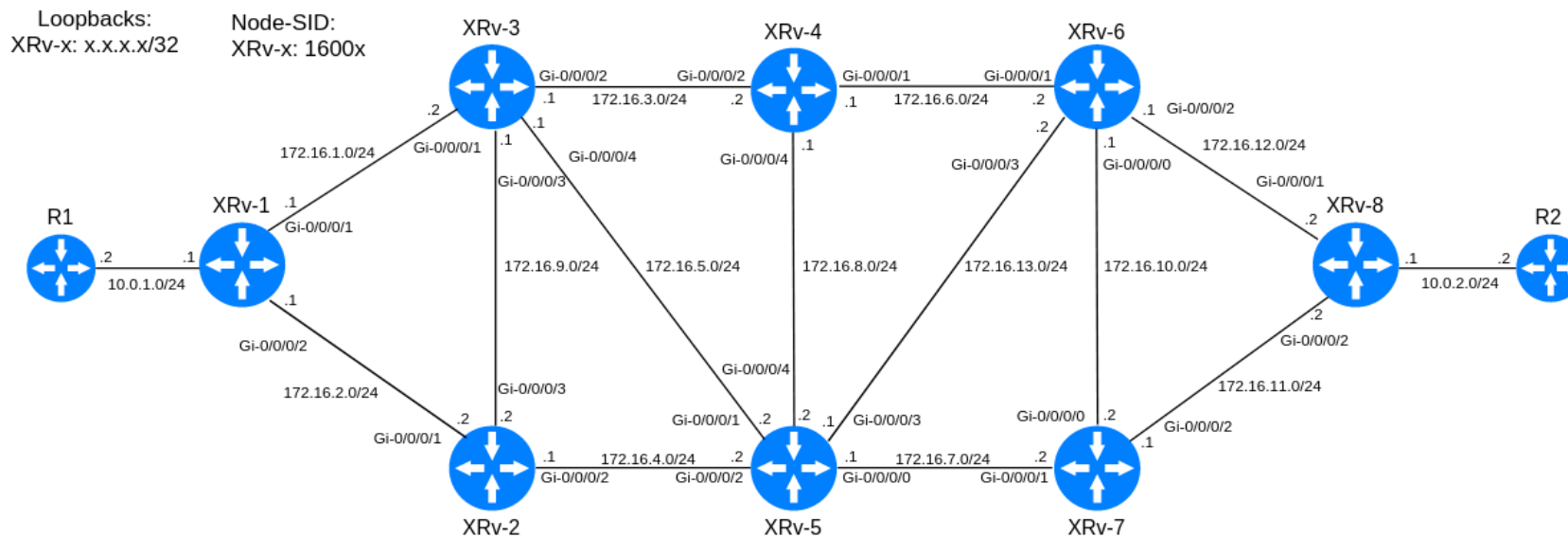
Objectives

- How are source and destination IP addresses used to route traffic through a network?
- What are sources for routing information used to populate a router's routing table?
- How do routed protocols differ from routing protocols?
- When multiple routing protocols know how to reach a destination network, which route is chosen?
- When a single routing protocols knows of multiple routes to reach a destination network, how is the preferred path (or paths) chosen?

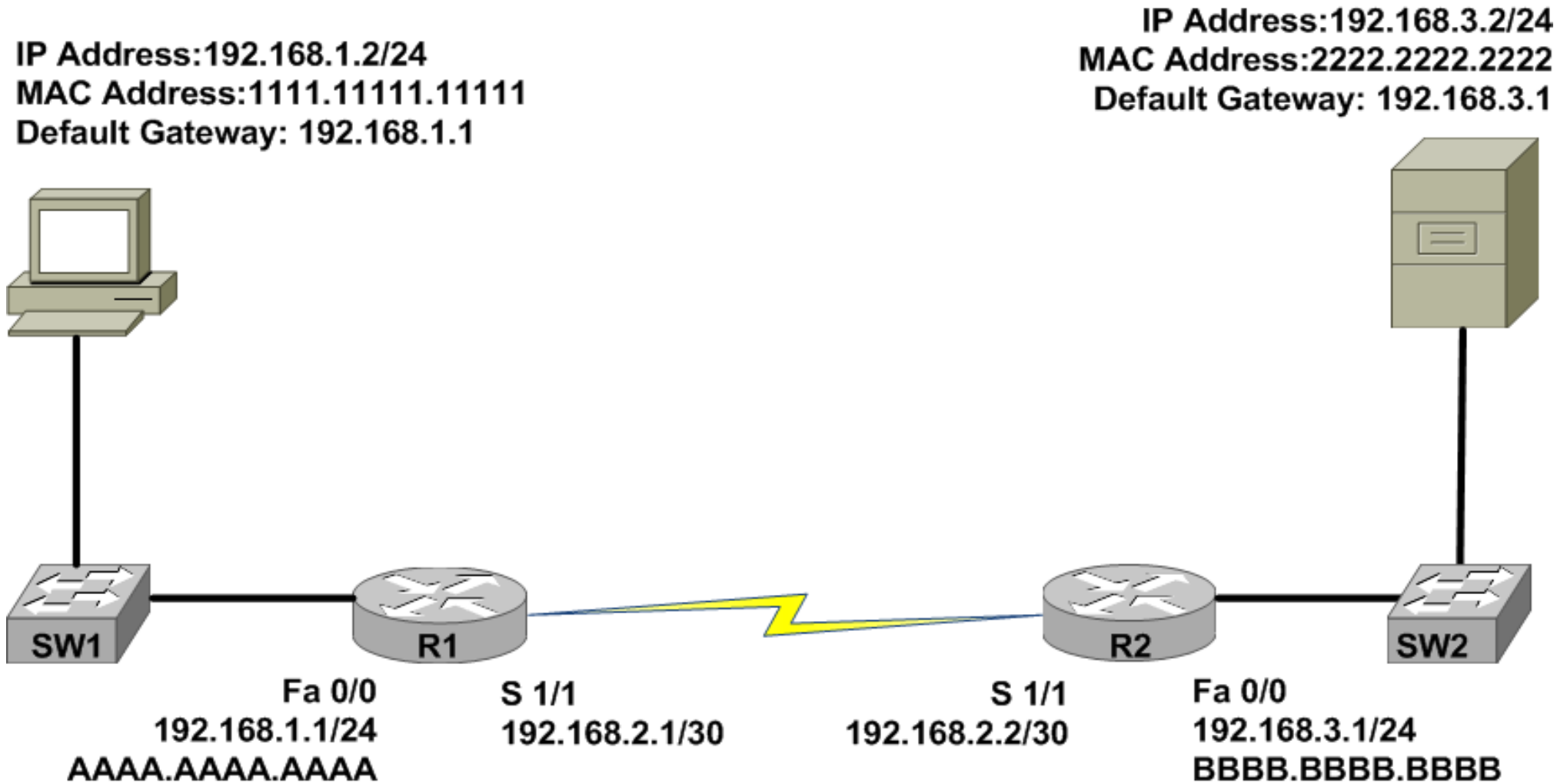


Objectives

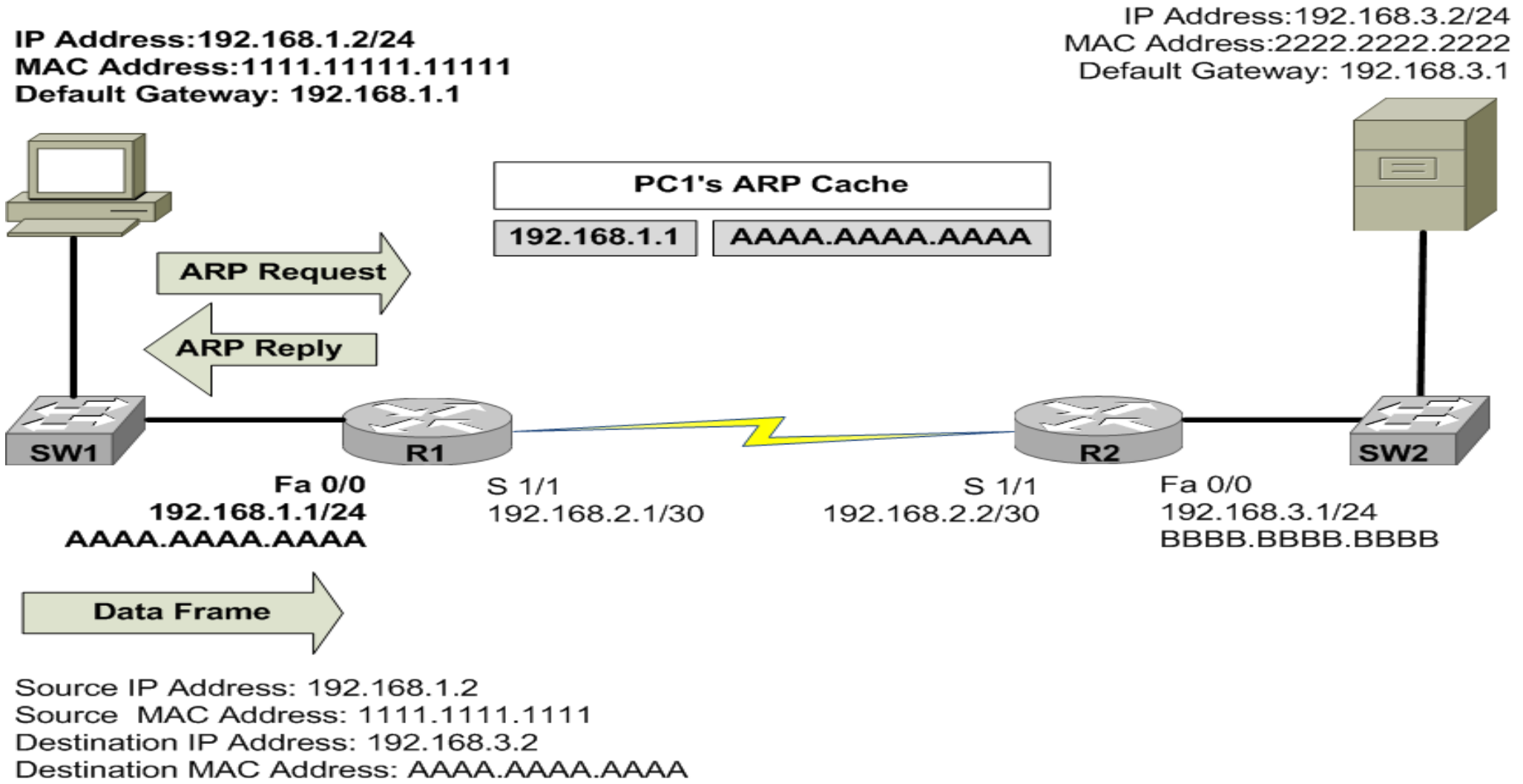
- What is the distinction between IGP and EGP?
- What are the primary differences between distance-vector and link-state routing protocols?
- What are the characteristics of the following routing protocols: RIP, OSPF, IS-IS, EIGRP, and BGP?
- How does NAT perform IP address translation, and how do the PAT, SNAT and DNAT approaches to NAT differ?
- What protocols are used to route multicast traffic?



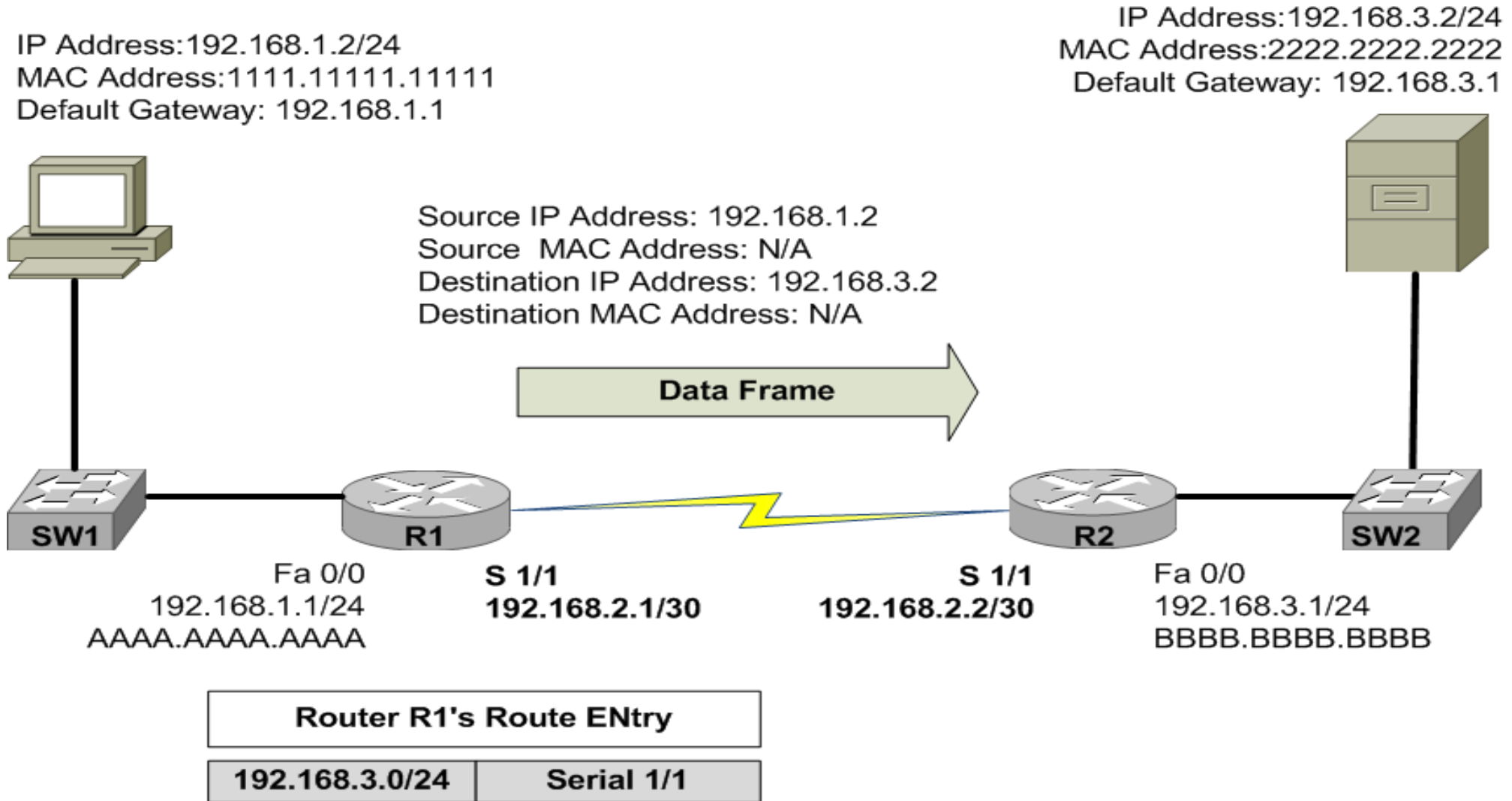
Basic Routing Processes



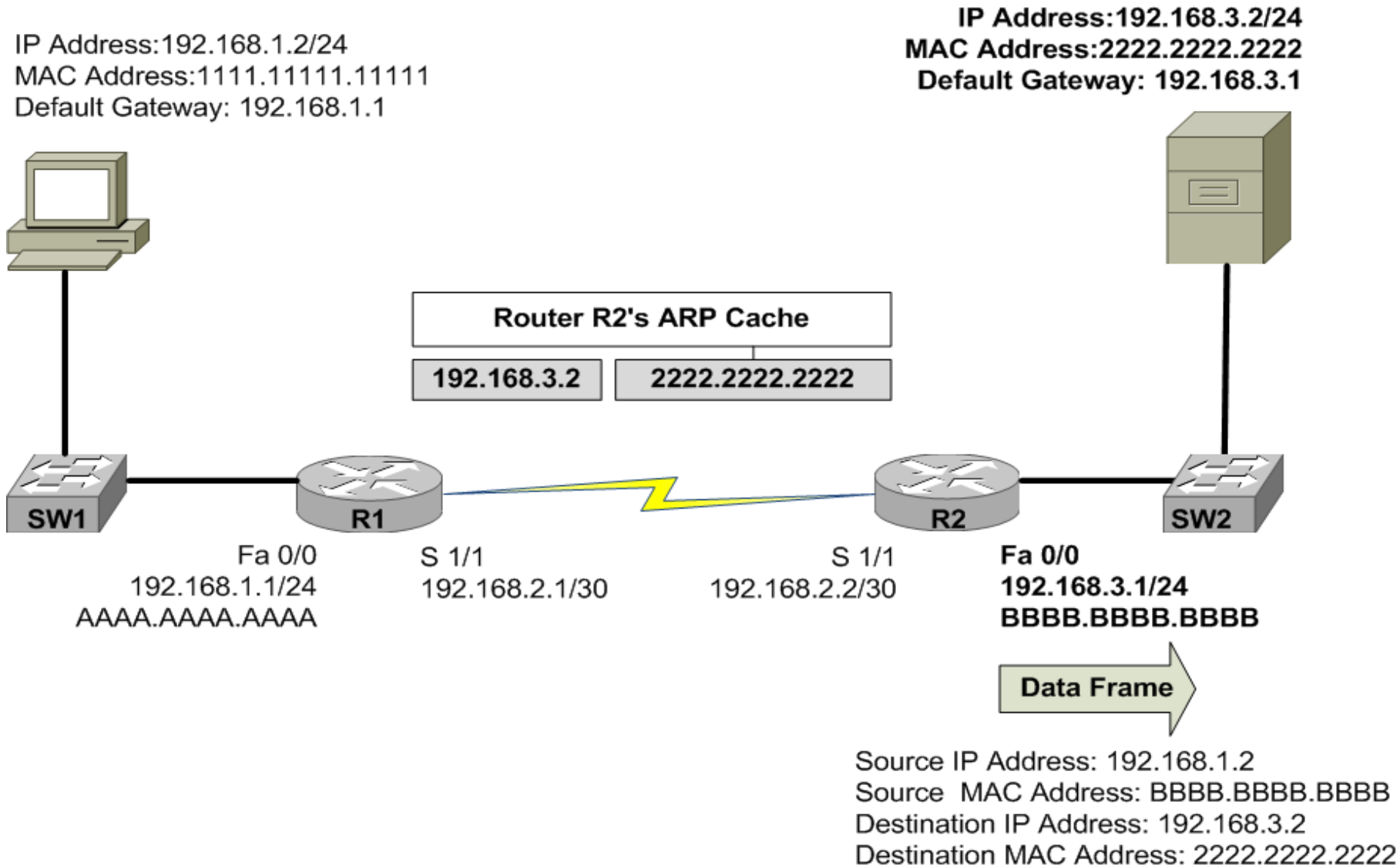
Basic Routing Processes



Basic Routing Processes

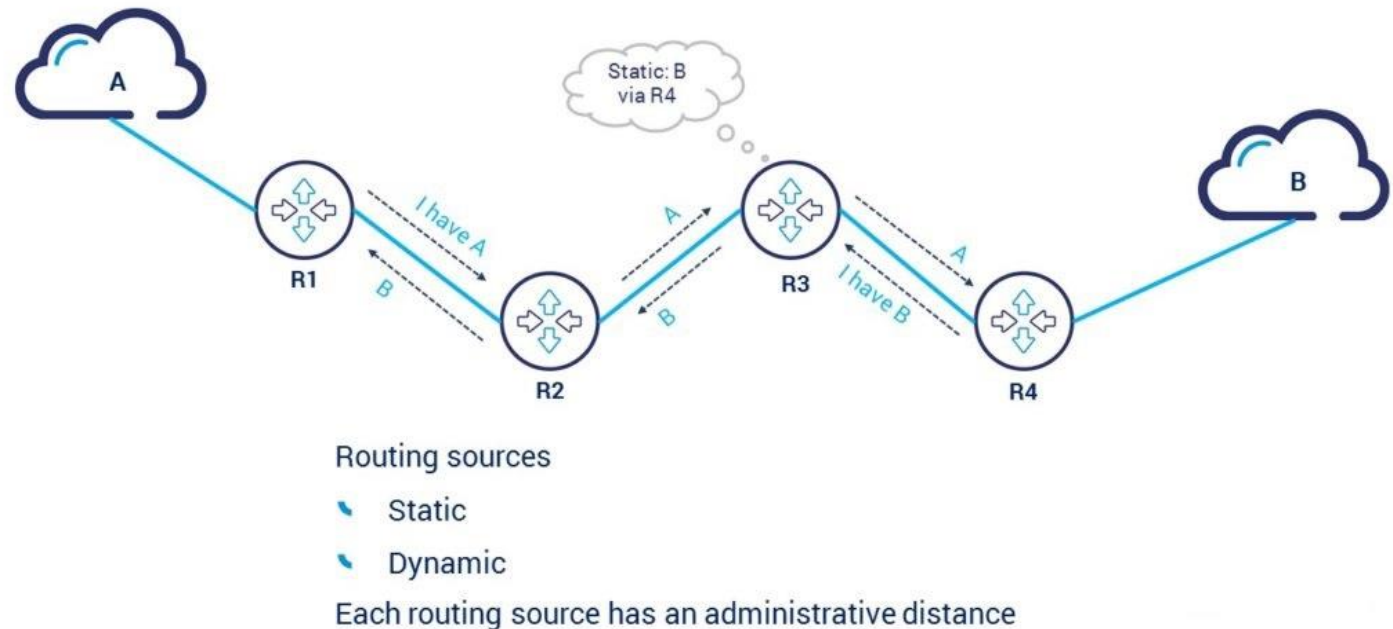


Basic Routing Processes

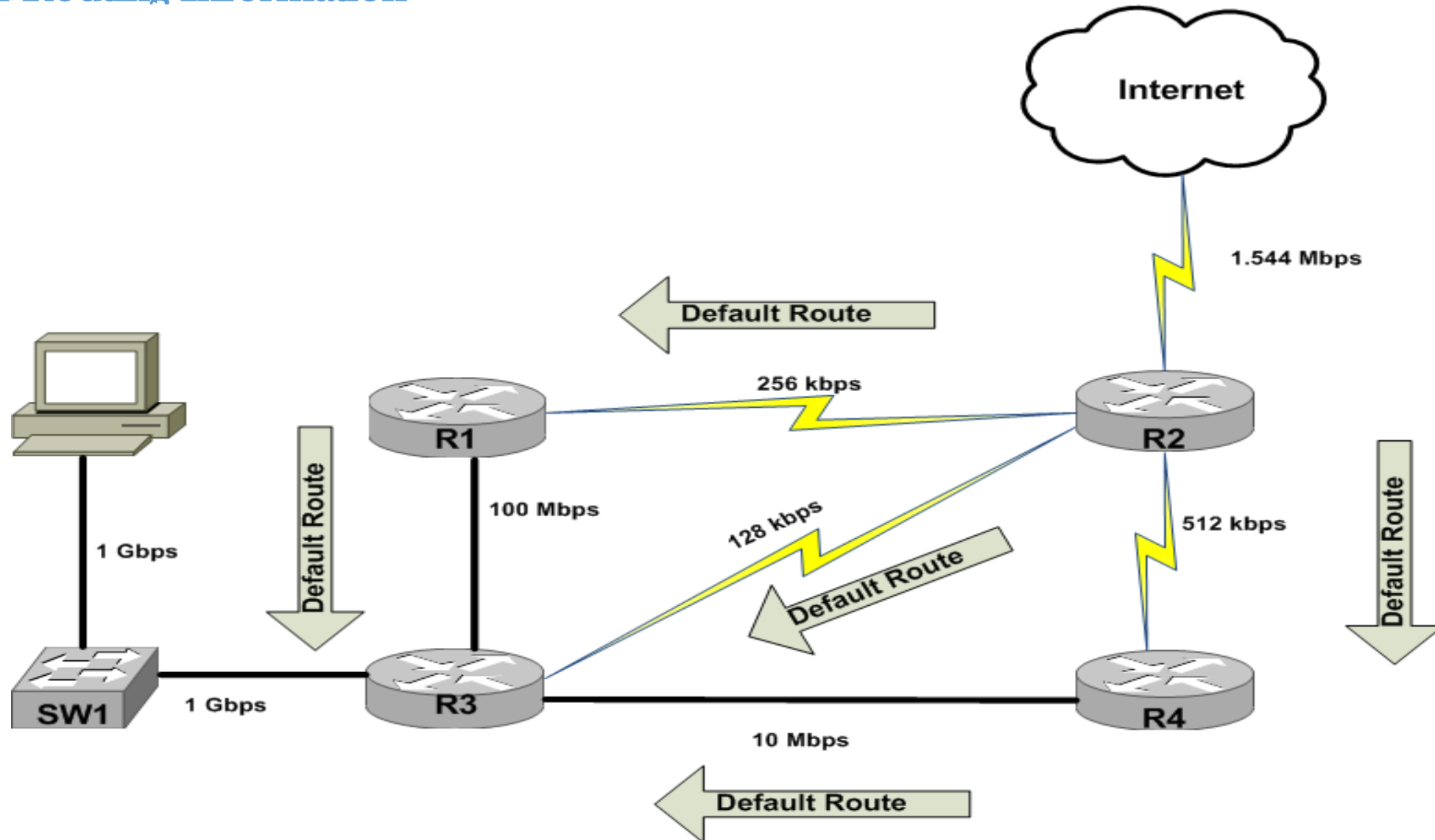


Source of Routing Information

- Before a router can route an IP packet, it needs to populate its routing table. A Router's routing table can be populated from the following sources.
 - From directly connected networks (configured interfaces)
 - Called a **directly connected route**
 - An administrator could statically configure a route table.
 - Called a **static route**, an/or **default static route**
 - A router could learn routes dynamically via routing protocols.
 - Called a **dynamic route** or **learned route**

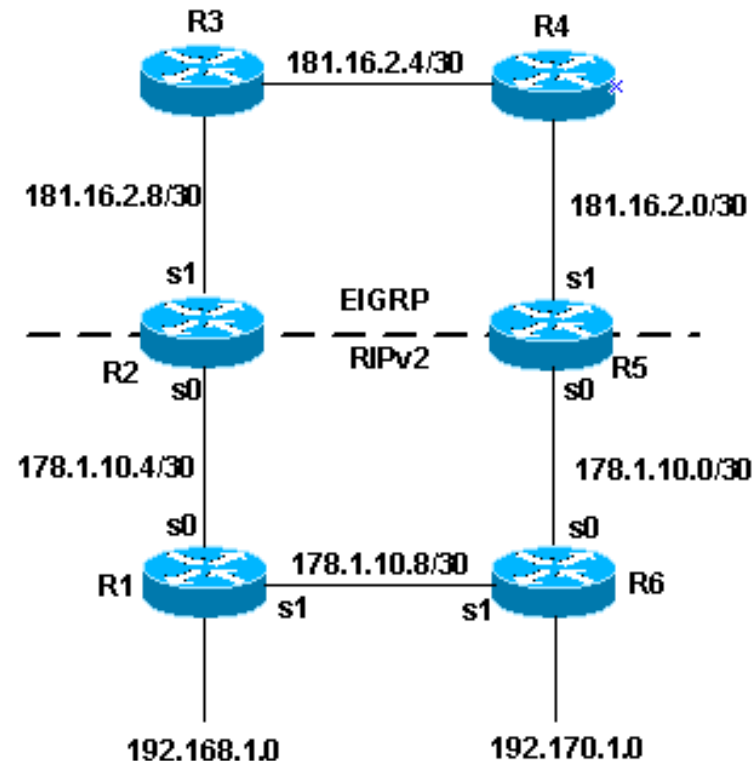


Sources of Routing Information



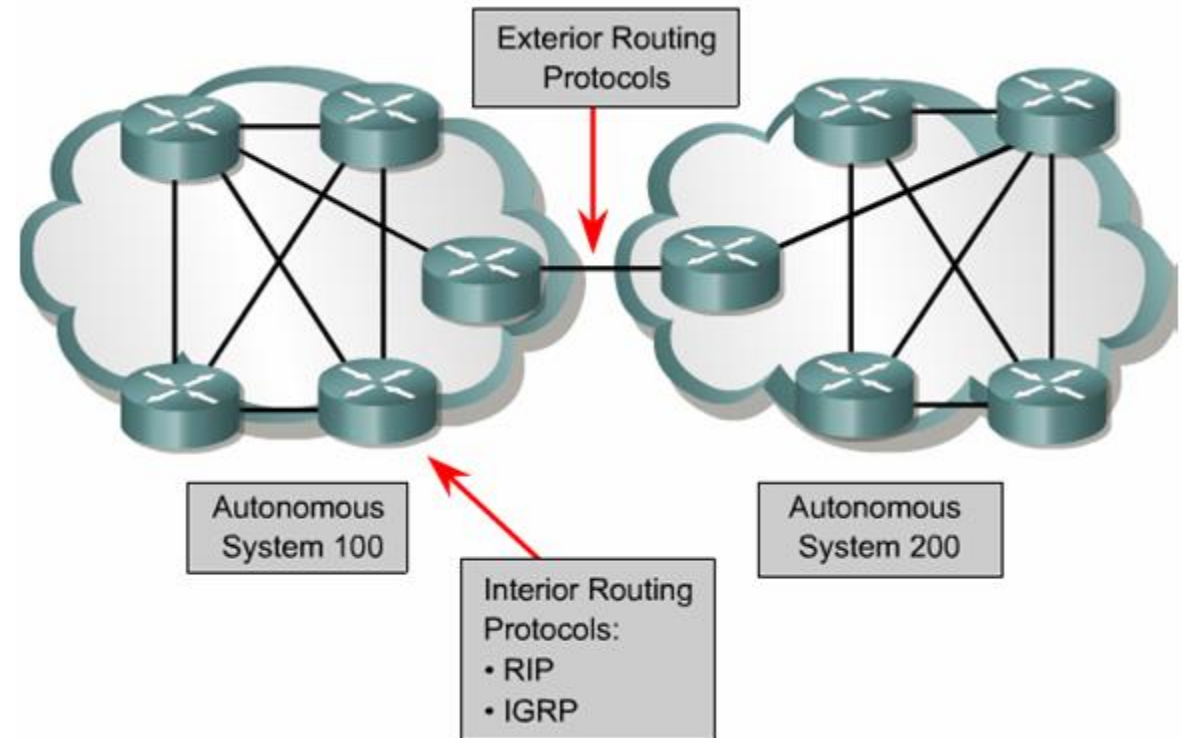
Routing Protocol Characteristics

- Before we can examine the characteristics of routing protocols, we must understand the following terms:
 - routed – is a protocol with an addressing scheme that defines different network
 - examples: IP, IPX, AppleTalk
 - routing – is a protocol that advertises route information between routers.
 - examples: RIP, OSPF, EIGRP, BGP



Routing Protocol Characteristics

- Routing Protocol hierarchy:
 - **Exterior Gateway Protocol (EGP's)**
 - Distance Vector
 - Border Gateway Protocol (BGP)
 - Link State
 - None
 - **Interior Gateway Protocol (IGP's)**
 - Distance Vector
 - RIPv1
 - RIPv2
 - Link State
 - OSPF
 - Hybrid
 - EIGRP



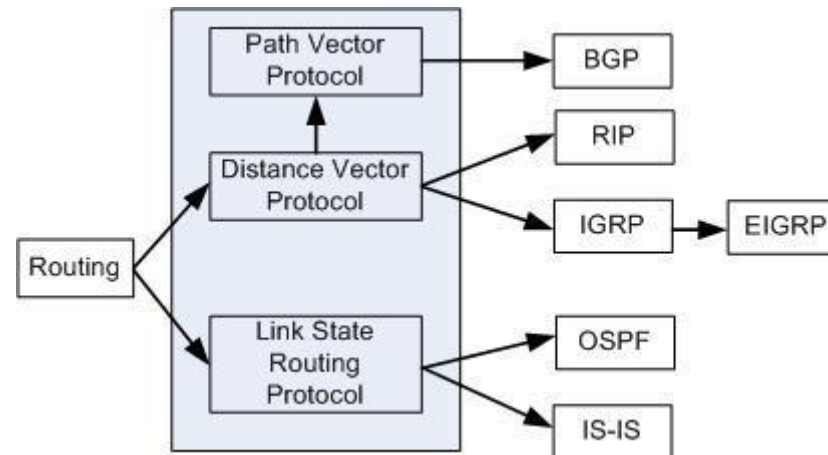
Believability of a Route

- If a network is running more than one routing protocol, which advertisement does the router believe?

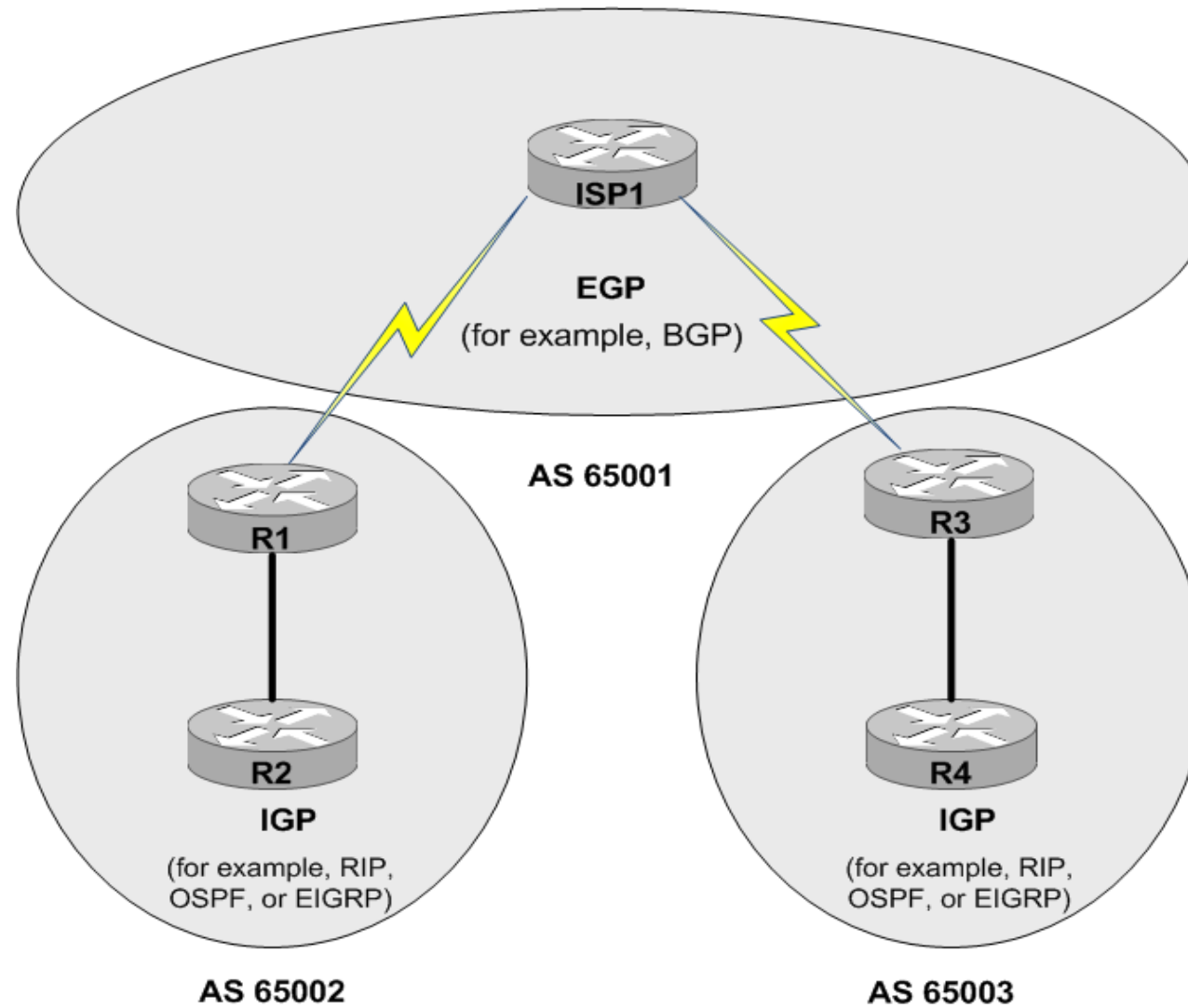
Route Source	Default Distance	Routing Table Entry
Connected interface	0	C
Static route out an interface	0	S
Static route to a next-hop address	1	S
EIGRP summary route	5	D
External BGP	20	B
Internal EIGRP	90	D
IGRP	100	I
OSPF	110	O
IS-IS	115	i
RIPv1, RIPv2	120	R
Exterior Gateway Protocol (EGP)	140	E
ODR	160	O
External EIGRP	170	D EX
Internal BGP	200	B
Unknown	255	

Believability of a Route

- The index of believability is called **administrative distance (AD)**. The lower the AD values the more the router trust the information source.
- If the routing protocol learns of more than one path to reach a remote network, it must choose one over the other, how?
- It varies on the routing protocol and what that routing protocol uses as a **metric**.
- A metric – is a value assigned to a route, and the **lower the value**, the better the route.

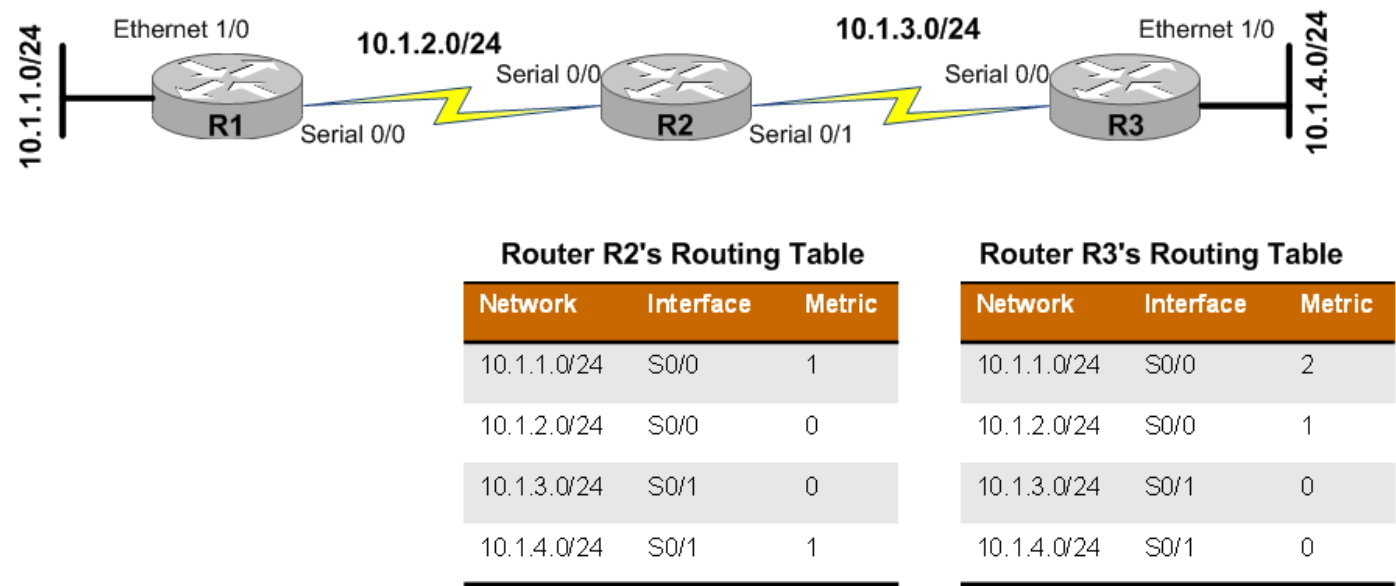


Interior versus Exterior Gateway Protocols



Route Advertisement Method

- Routing Protocol hierarchy:
 - Distance Victor
 - Sends a full copy of its routing table to its directly connected neighbors.
 - This is a periodic advertisement, meaning that, at regular intervals, re-advertise its full routing table.
 - Slow convergence time.
 - Metric, equals hop count.
 - Uses hold down timers, split horizon, poison reverse for loop avoidance.

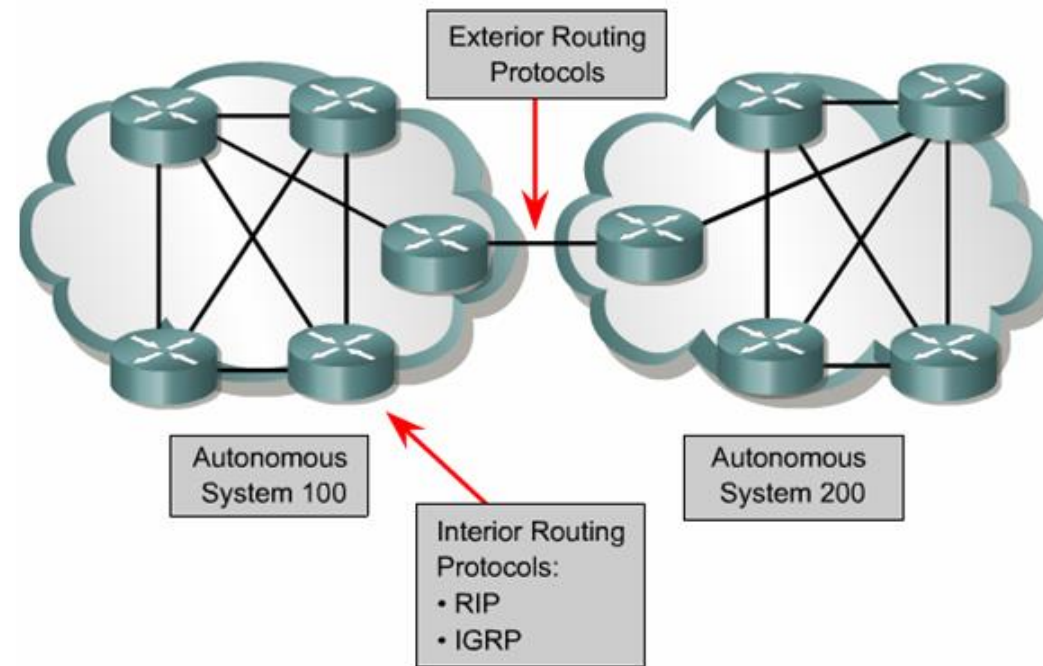


Route Advertisement Method

- Routing Protocol hierarchy:
 - Link State
 - Rather than having neighboring routers exchange their full routing tables with one another, a link state protocol allows routers to build a topology map of the network.
 - They send link-state advertisements (LSA) to advertise the networks they know how to reach.
 - Router than use these LSAs to build a topology map.
 - From this map, using the Dijkstra's Shortest Path First algorithm to build there route table.
 - New LSA's our only sent when the topology changes.

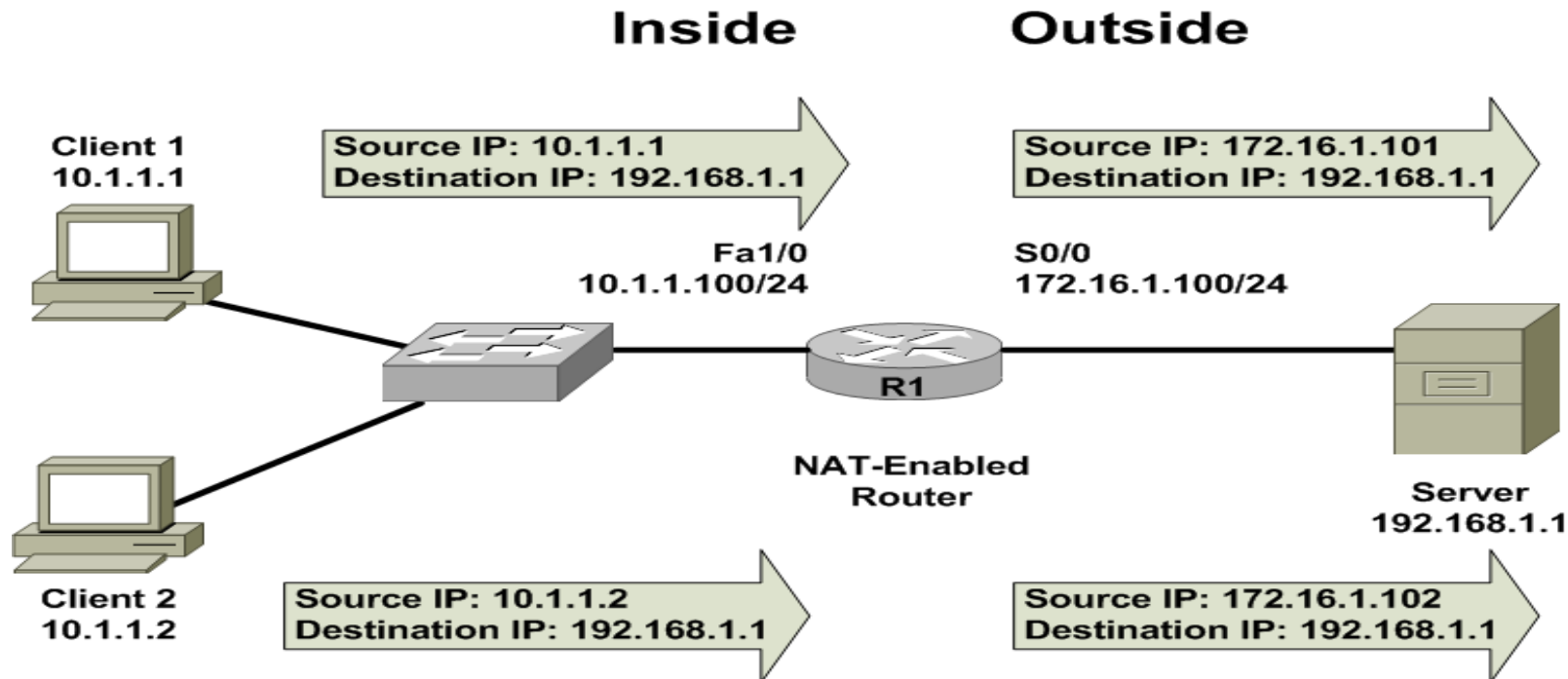
Routing Protocol Examples

- Interior Gateway Protocols
 - Router Information Protocol (RIP)
 - Open Shortest Path First (OSPF)
 - Enhanced Interior Gateway Routing Protocol (EIGRP)
- Exterior Gateway Protocols
 - Border Gateway Protocol (BGP)



Address Translation

- Network Address Translation (NAT)
- Dynamic NAT (DNAT) - assigns IP address from a pool of addresses, one to one translations.
- Static NAT (SNAT) - assigns IP address manually, one to one translations
- Port Address Translation (PAT) - assigns IP address using a many to one translation.

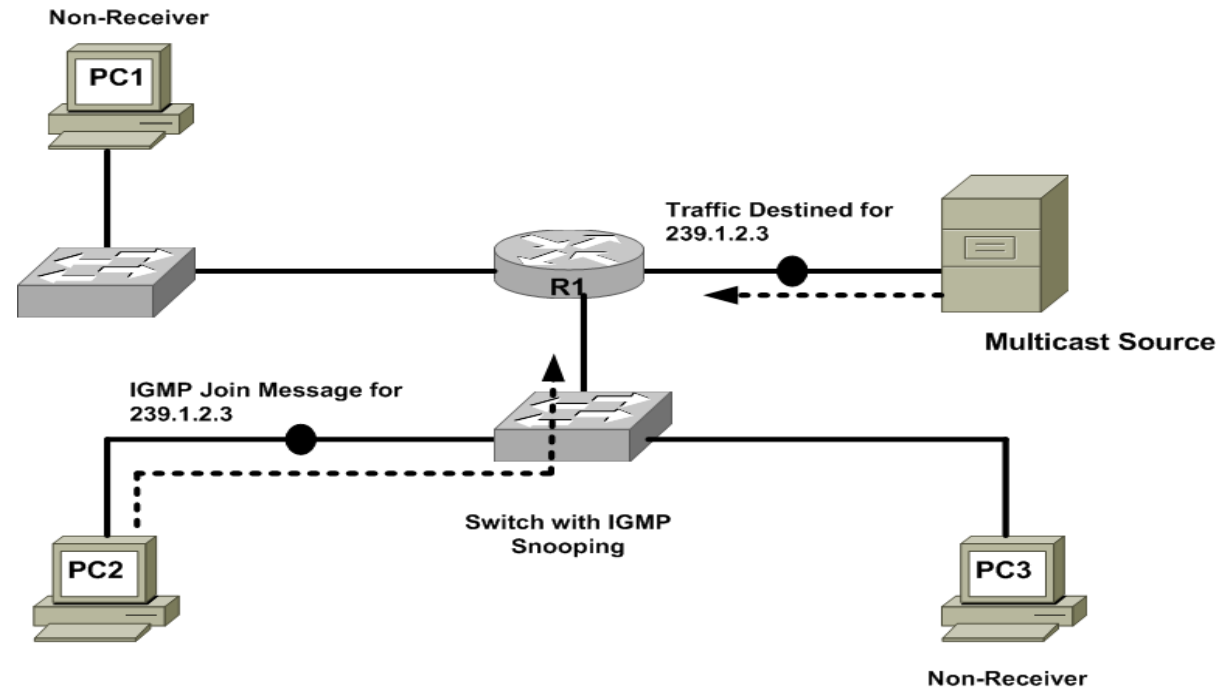


By : Eng. Ahmad Hassan Al-Mashaikh

Email : Ahmad.private.mashaikh@Hotmail.com

Multicast Routing

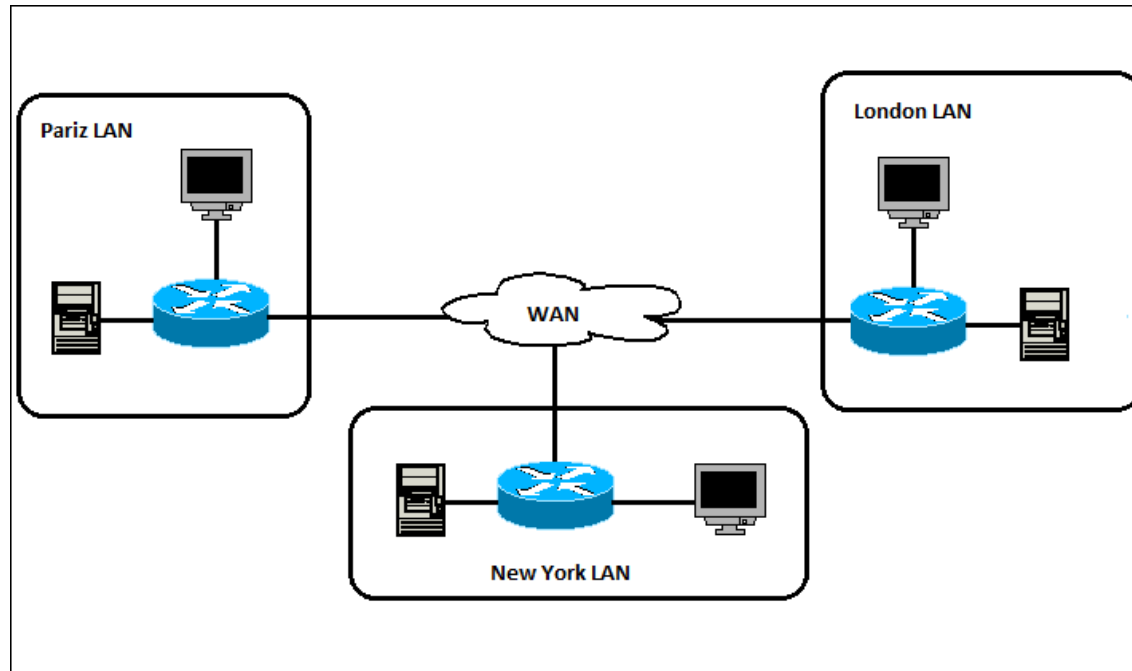
- Network Address Translation (NAT)
- Dynamic NAT (DNAT) - assigns IP address from a pool of addresses, one to one translations.
- Static NAT (SNAT) - assigns IP address manually, one to one translations
- Port Address Translation (PAT) - assigns IP address using a many to one translation.



Introducing Wide-Area Networks

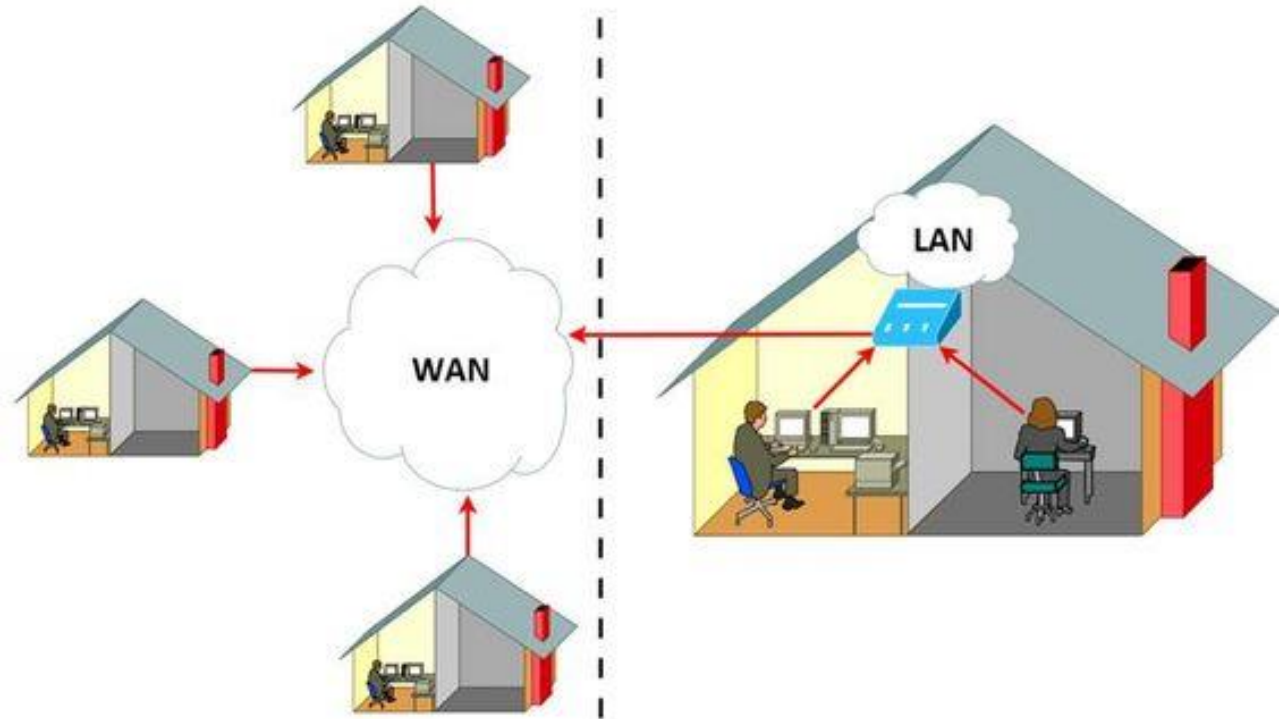
Objectives

- What are three categories of wide-area networks (WAN) connections?
- How are data rates measured a various WAN technologies?
- Which are the characteristics of the following WAN technologies: dedicated leased line, digital subscriber line (DSL), cable modem, Synchronous Optical Network (SONET), satellite, Plain Old Telephone Service (POTS), Integrated Services Digital Network (ISDN), Frame Relay, Asynchronous Transfer Mode (ATM), and Multiprotocol Label Switching (MPLS)?

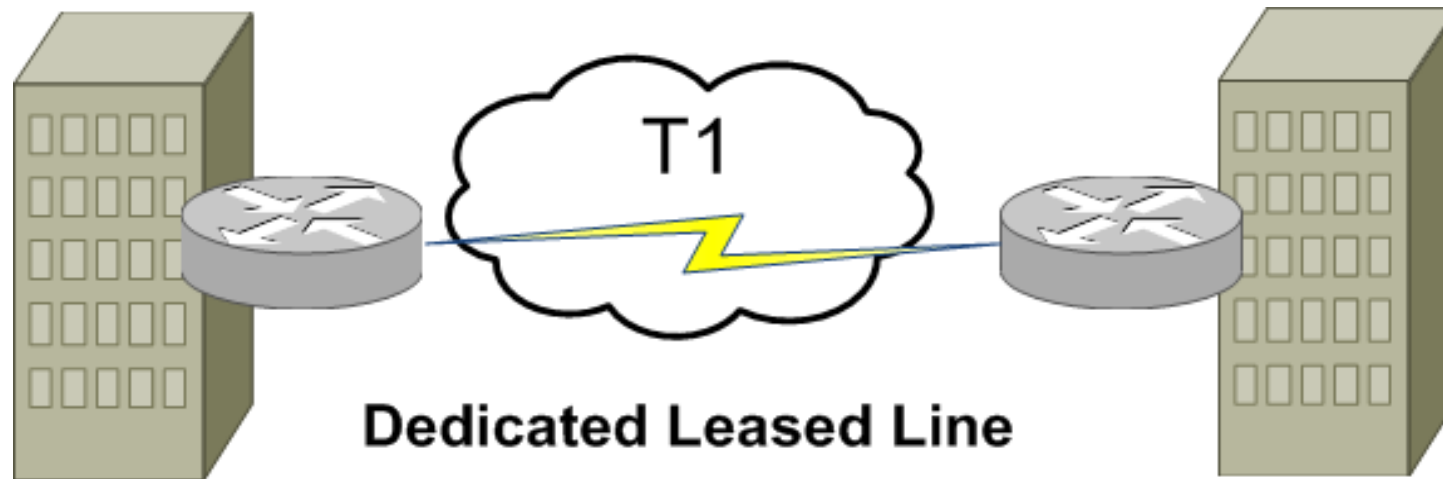


WAN Properties

- Some WAN connections are considered to be always-on, in that the connection is always available without having to first set up the connection.
- Conversely, some WAN technologies are on-demand, meaning that the connection is not established until needed.
- WAN connection can generally be classified into one of three categories:
- Dedicated leased Line
- Circuit-switched Connection
- Packet-switched Connection

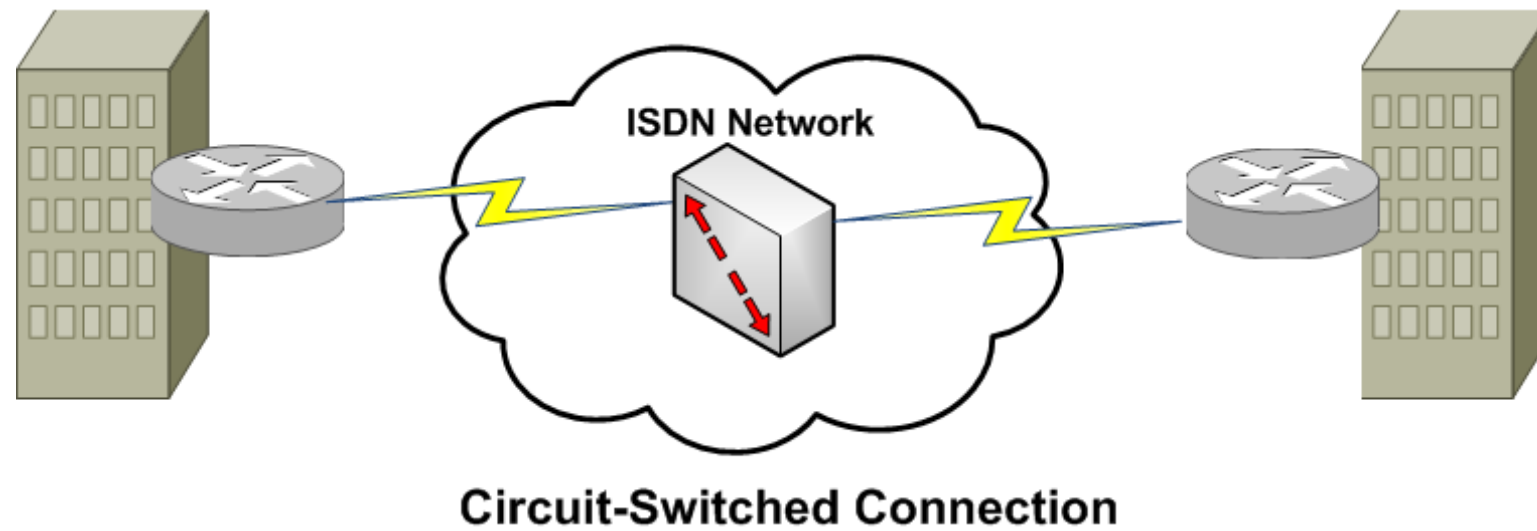


WAN Connection Types



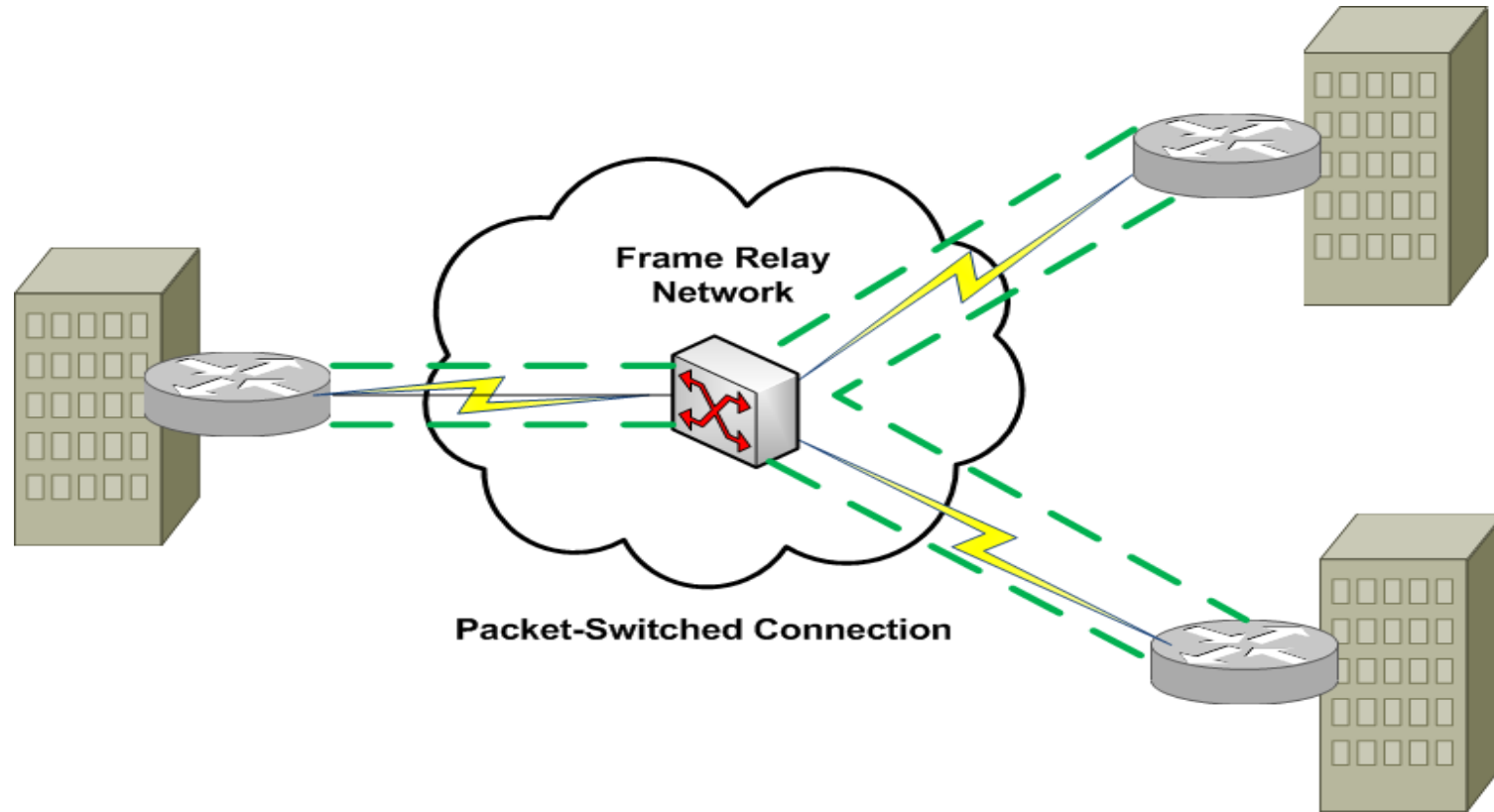
WAN Connection Types

- Connection brought up when needed, like a phone call (virtual circuit)



WAN Connection Types

- Always on
- Multiple customers share bandwidth



WAN Data Rates

- WAN links are typically slower than LAN links; however, some WAN technologies boast a bandwidth capacity in tens of Gbps.
- Aside from measuring bandwidth in kbps, Mbps or Gbps, high-speed optical networks often use optical carrier (OC) levels to indicate bandwidth.
- OC-1 link is 51.84 Mbps

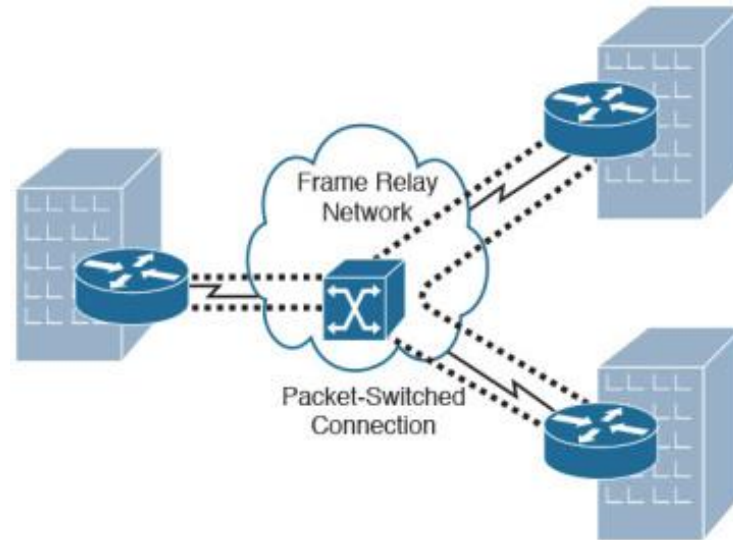
WAN Technology	Typical Available Bandwidth
Frame Relay	56 kbps – 1.544 Mbps
T1	1.544 Mbps
T3	44.736 Mbps
E1	2.048 Mbps
E3	34.4 Mbps
ATM	155 Mbps – 622 Mbps
SONET	51.84 Mbps (OC-1) – 159.25 Gbps (OC-3072)

WAN Media Types

- Physical Media
 - Unshielded twisted pair (UTP)
 - Coaxial Cable
 - Fiber-optic cable
 - Electric power lines
- Wireless Media
 - Cellular phone
 - LTE goes up to 100 Mbps
 - WIMAX is slower, and being replaced by LTE
 - Satellite
 - HSPA+
 - Wireless broadband up to 84 <bps

WAN Technologies

- Dedicated Leased Line
- A dedicated leased line is typically a point-to-point connection interconnecting two sites.
- All the bandwidth on that line is available to those sites.
- WAN technologies commonly used with dedicated leased lines include digital circuit, such as T1, T3 circuits.
- A single 64-kbps channel is called a Digital Signal 0 (DS0)

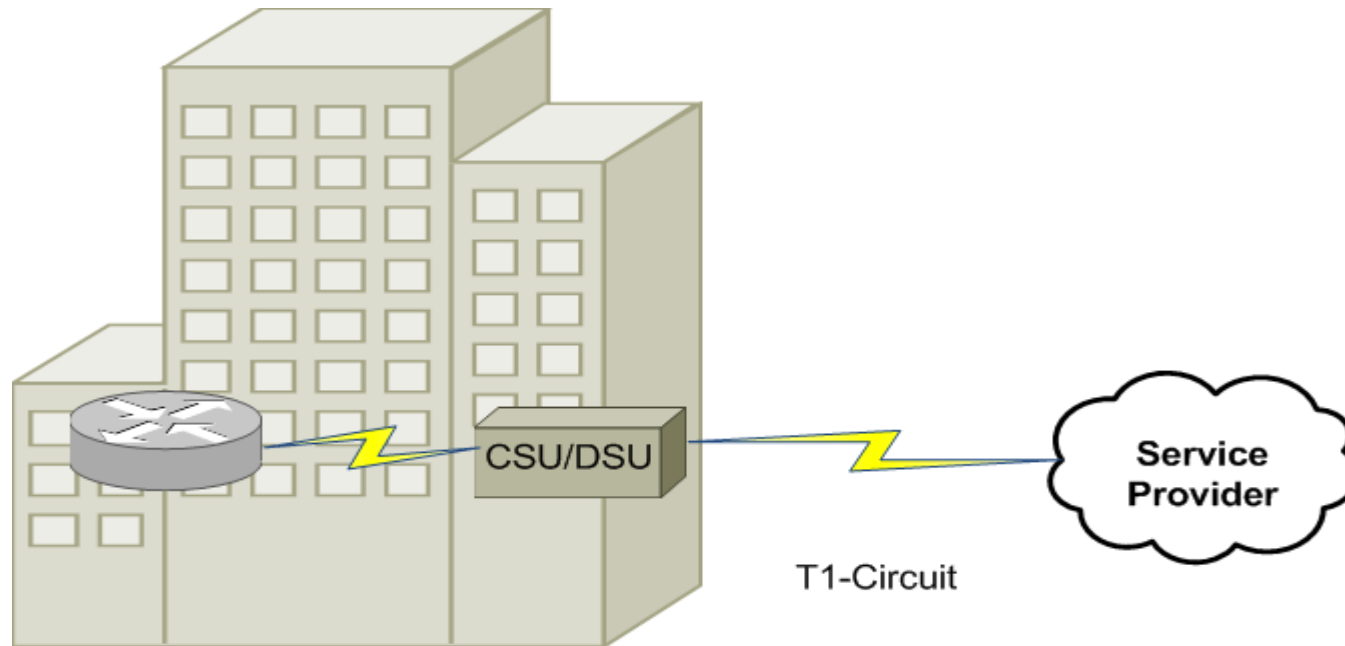


WAN Technologies

T-carriers Single Levels

Carrier	Signal Level	# of T1 signals	# of Voice Channels	Speed
T1	DS-1	1	24	1.544 Mbps
T1c	DS-1c	2	48	3.152 Mbps
T2	DS-2	4	96	6.312 Mbps
T3	DS-3	28	672	44.736 Mbps
T4	DS-4	168	4032	274.760 Mbps

Channel Service Unit / Data Service Unit (CSU/DSU)

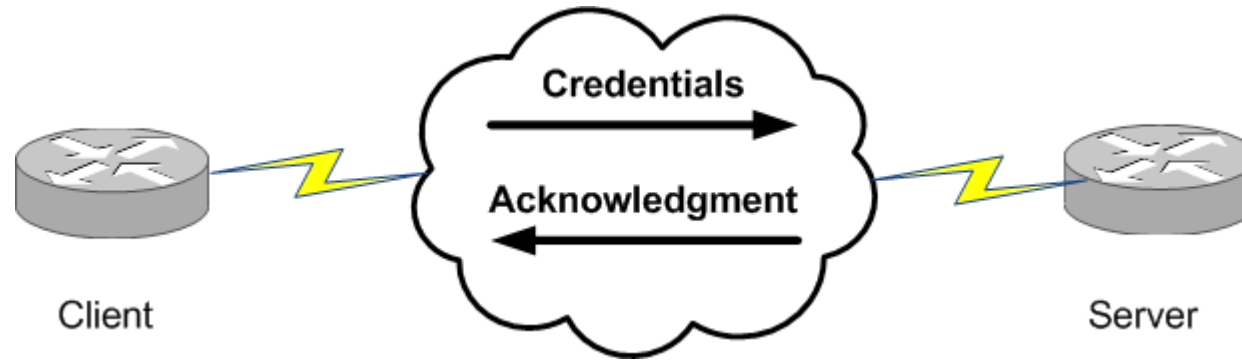


CSU/DSU Terminating a Synchronous Circuit

Point-to-Point Protocol

- One of the common Layer 2 protocols used on dedicated leased lines is **Point-to-Point Protocol (PPP)**.
 - Capability to simultaneously transmit multiple Layer 3 protocols.
 - PPP does this through the use of **Control Protocols (CP)**.
 - Each Layer 3 CP runs an instance of PPP's **Link Control Protocol (LCP)**.
 - Multilink interface
 - Bonds several physical connections to a single logical interface
 - For load balancing
 - Looped link detection
 - Error detection
 - Authentication
 - PAP
 - CHAP

PAP



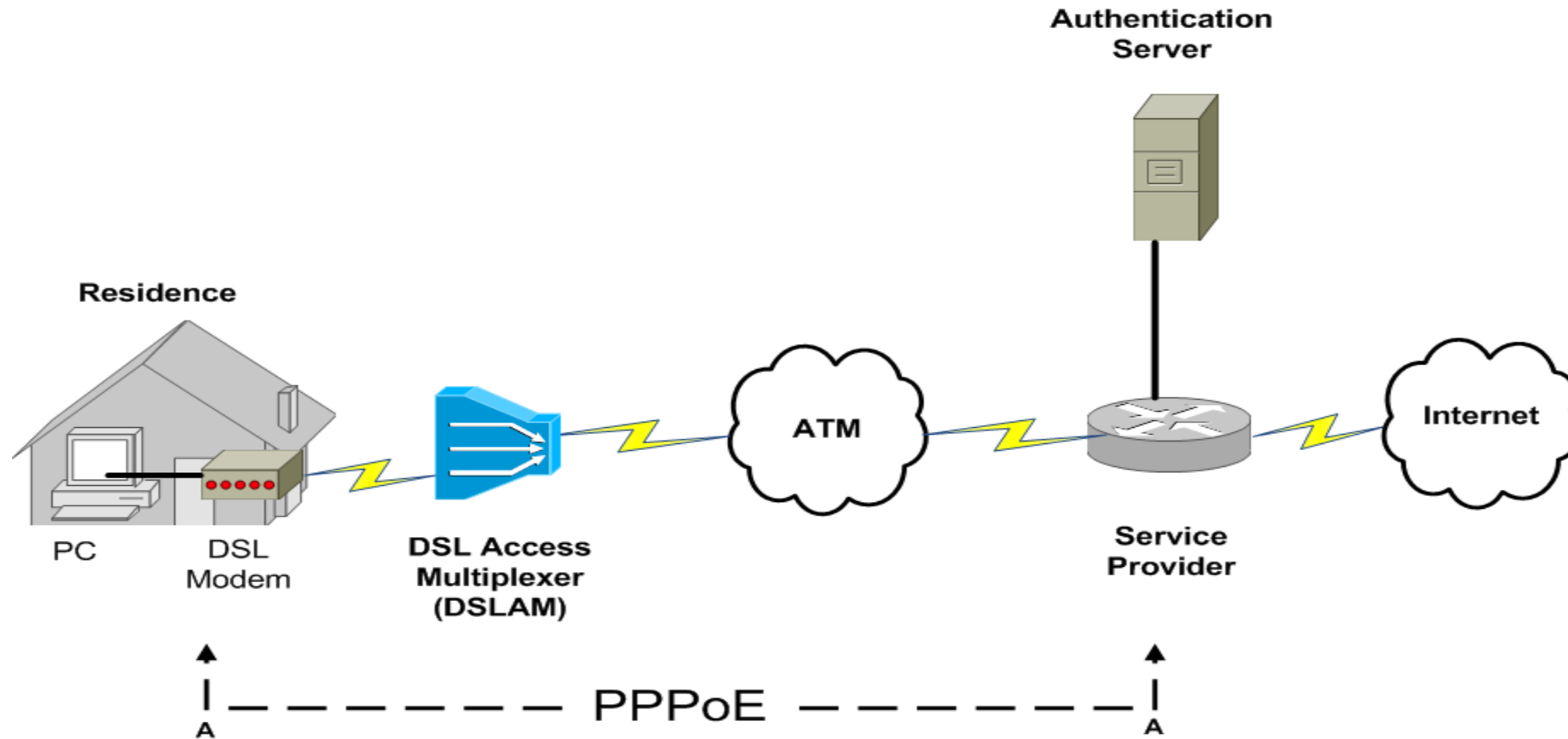
PAP Authentication

CHAP



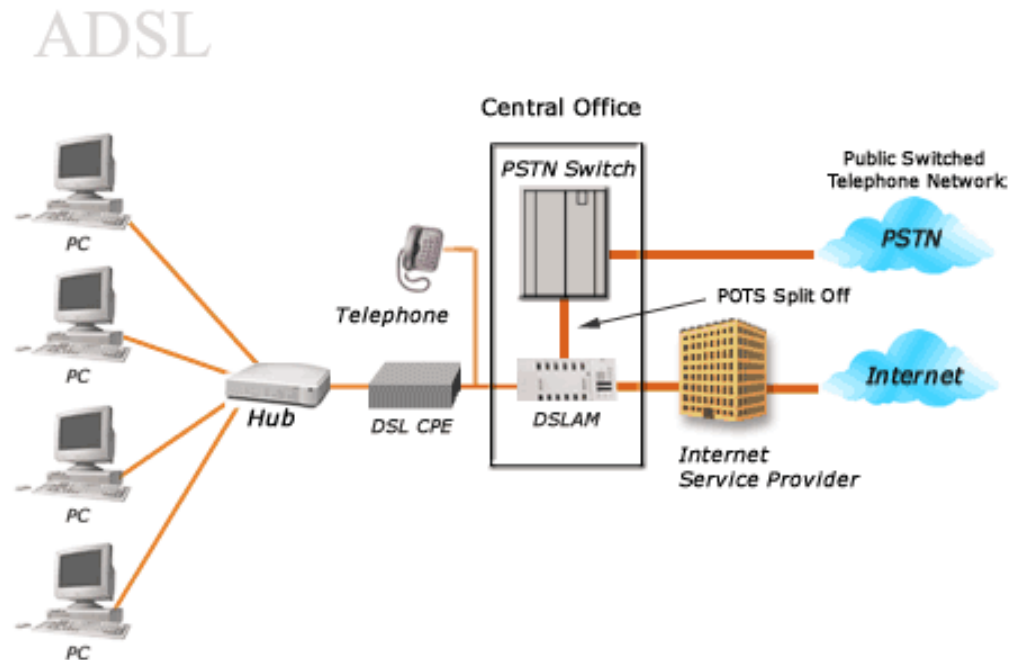
CHAP Authentication

PPPoE

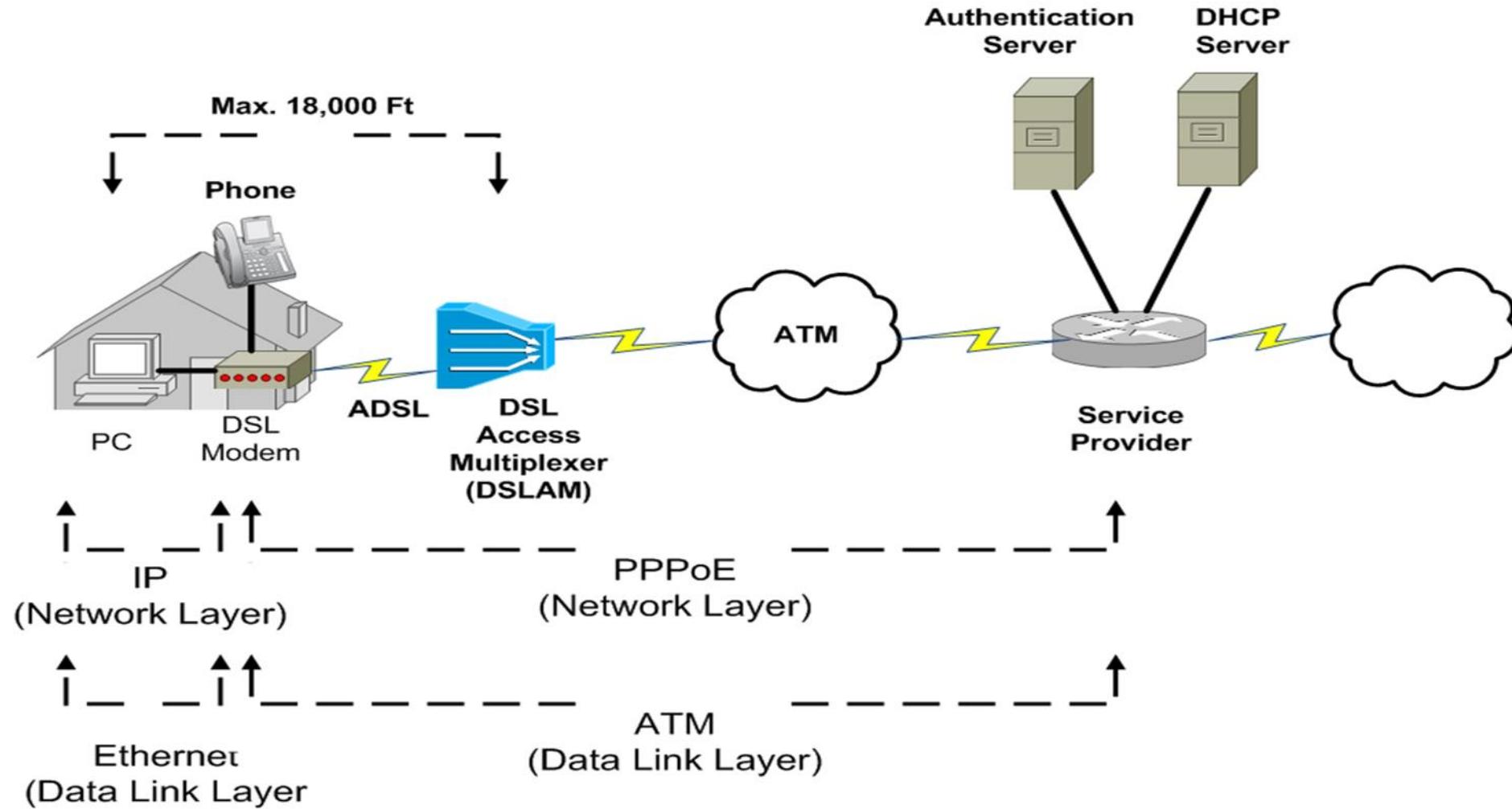


Digital Subscriber Line

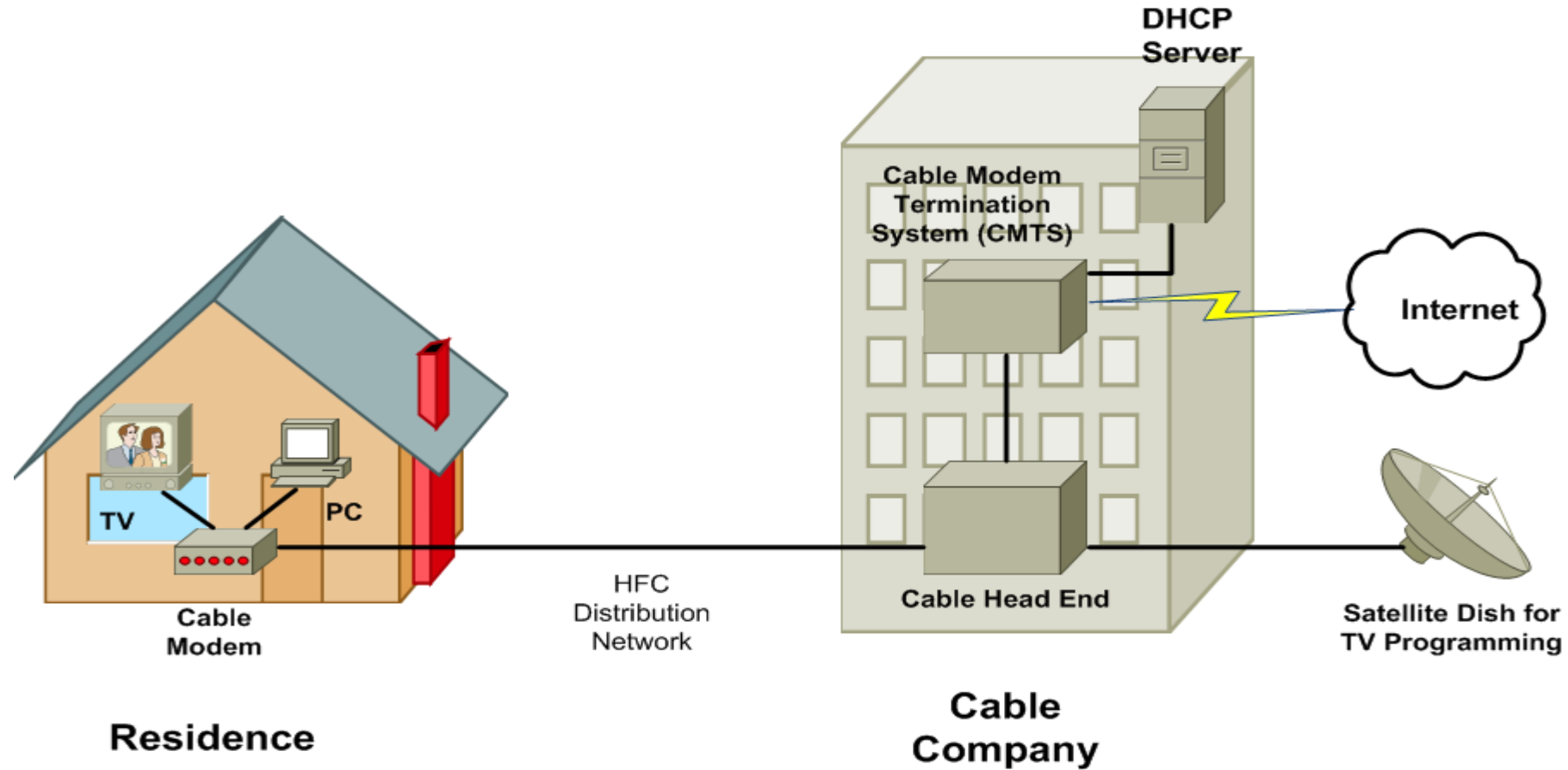
- Commonplace in many residential and small business locations (SOHO), digital subscriber line (DSL) is a group of technologies that provide high-speed data transmission over existing telephone wiring.
- DSL has several variants, which differ in data rate and distance limitations.
 - Asymmetric DSL (ADSL)
 - Symmetric DSL (SDSL)
 - Very High Bit-Rate DSL (VDSL)



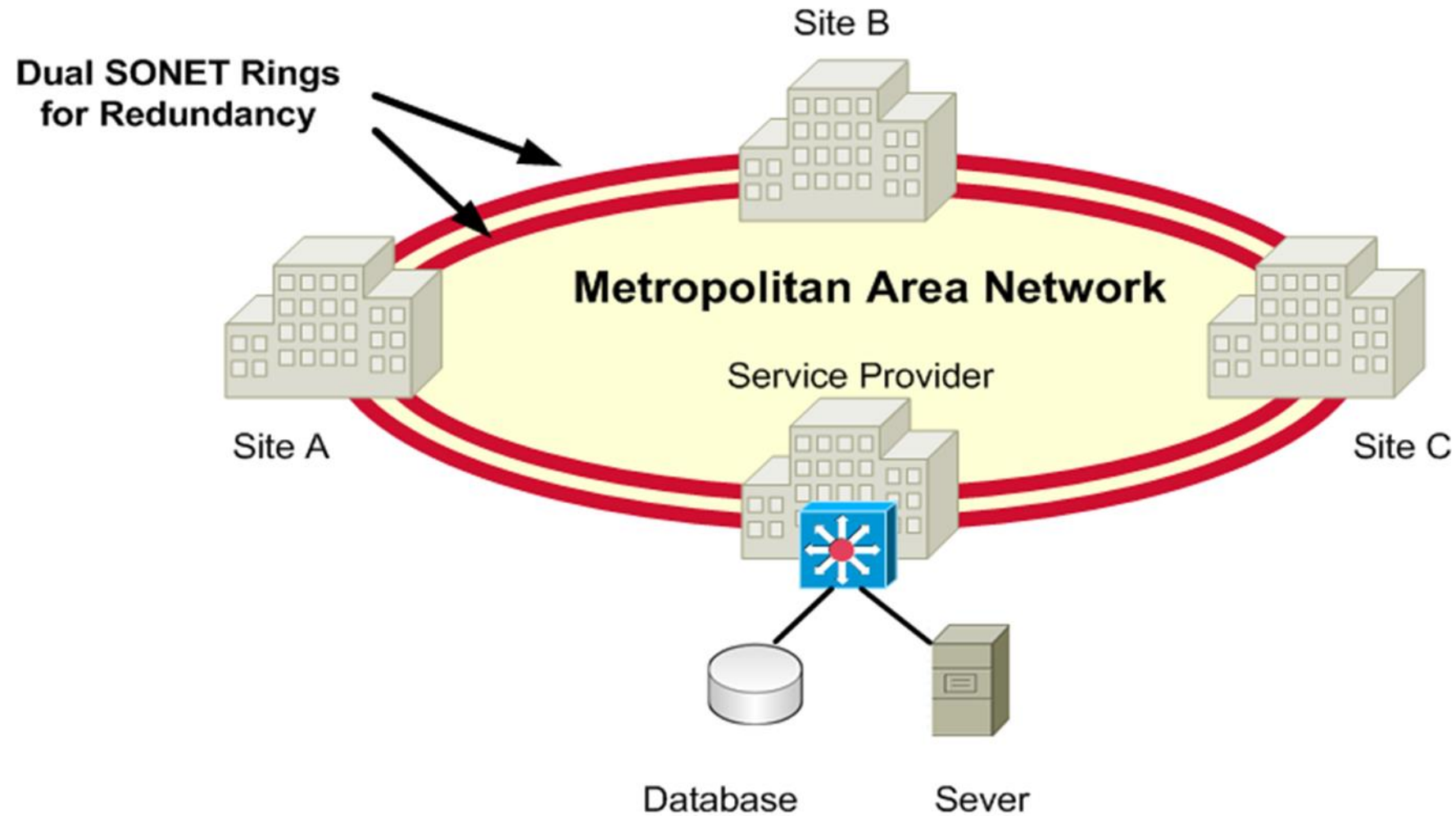
ADSL Sample Topology



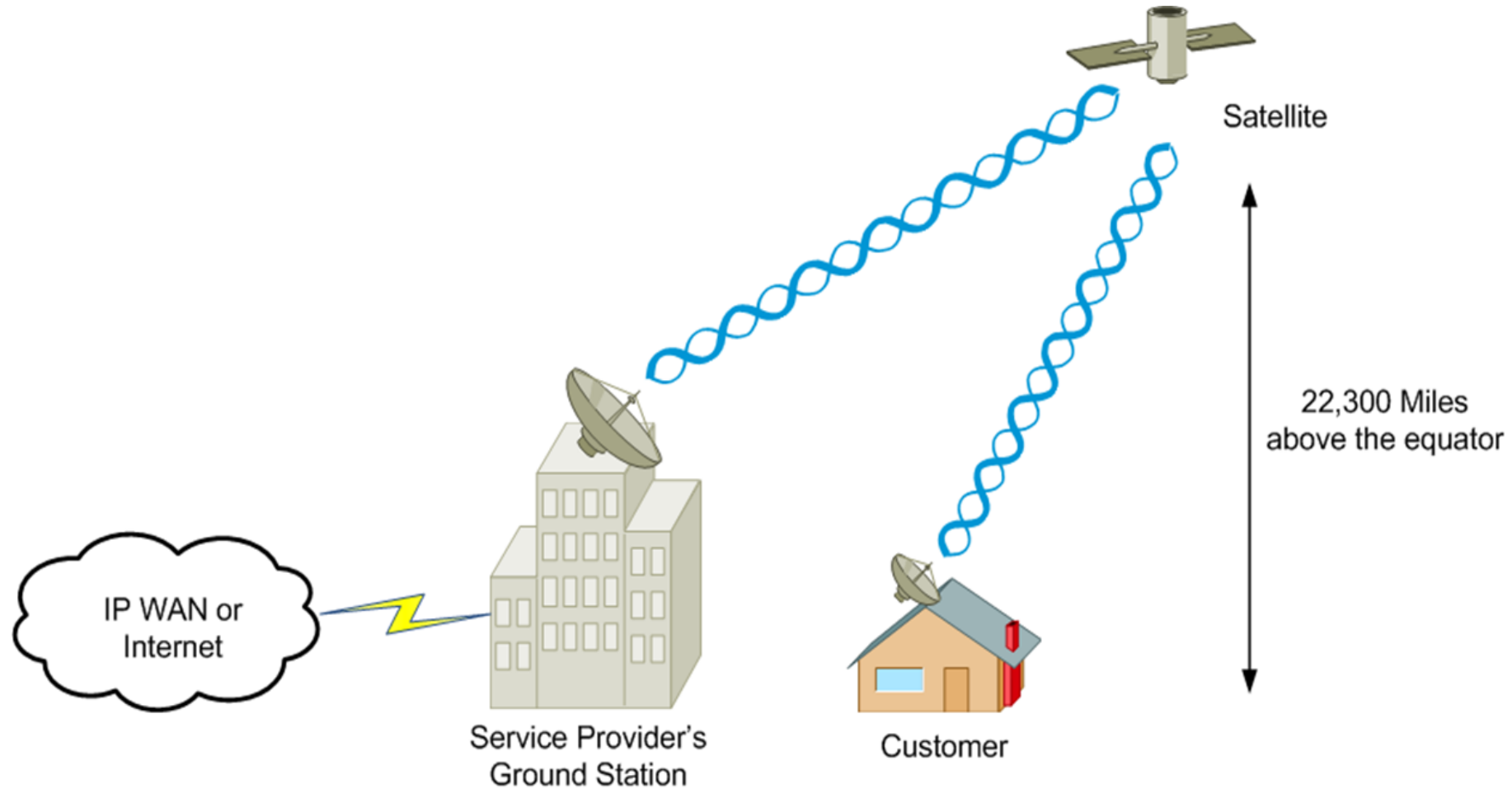
Cable Modem



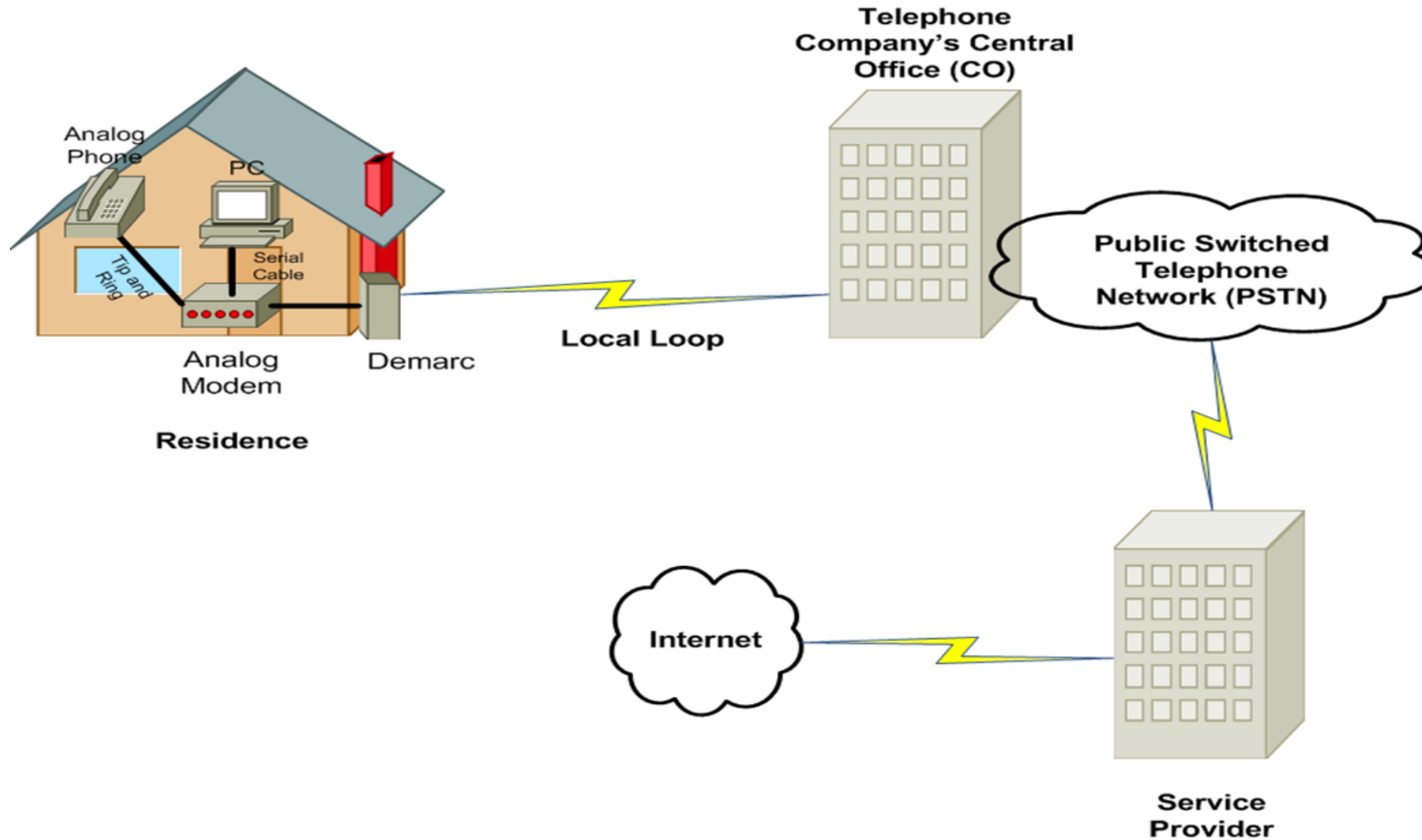
SONET



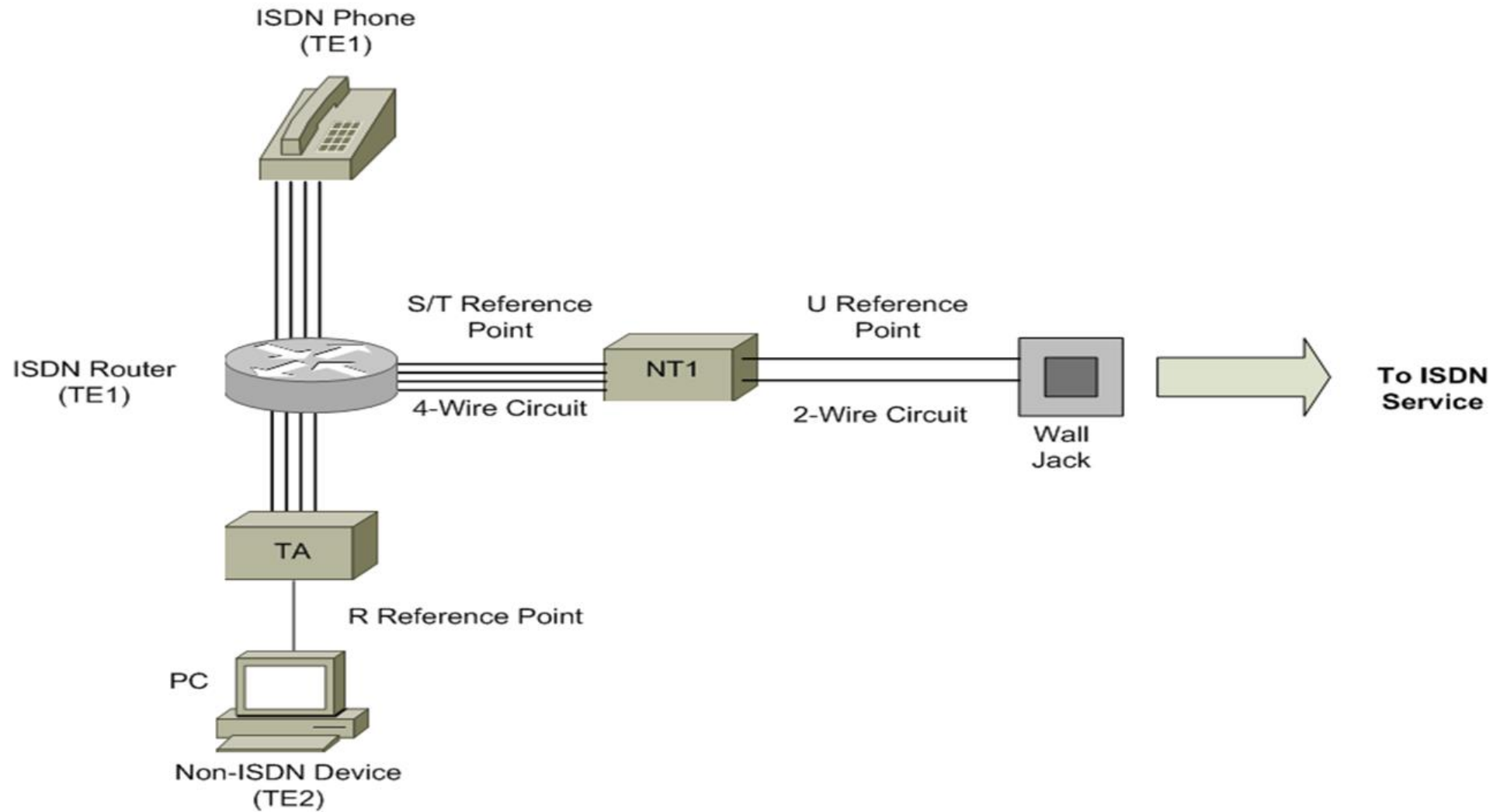
Satellite



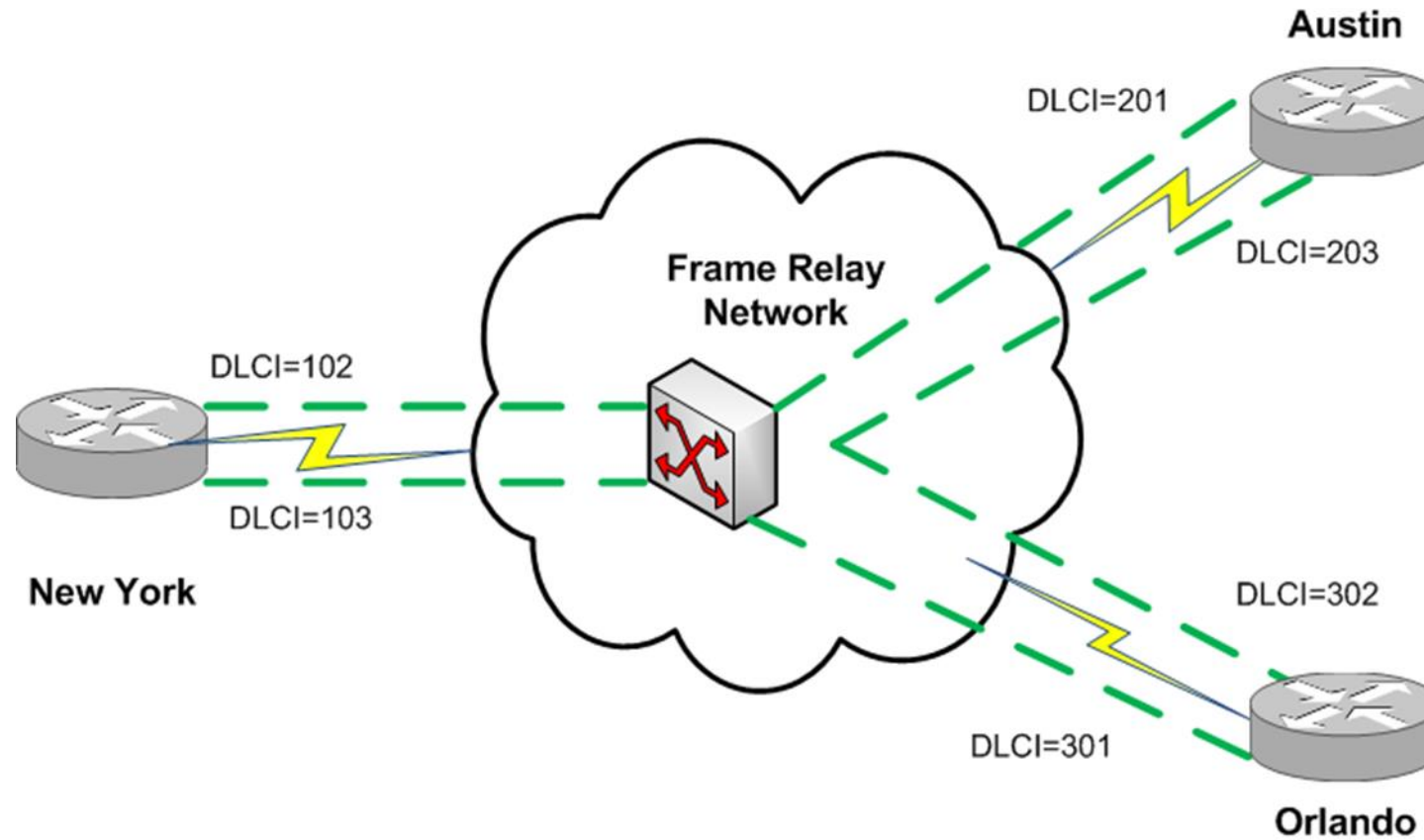
Plain Old Telephone Service



Integrated Services Digital Network

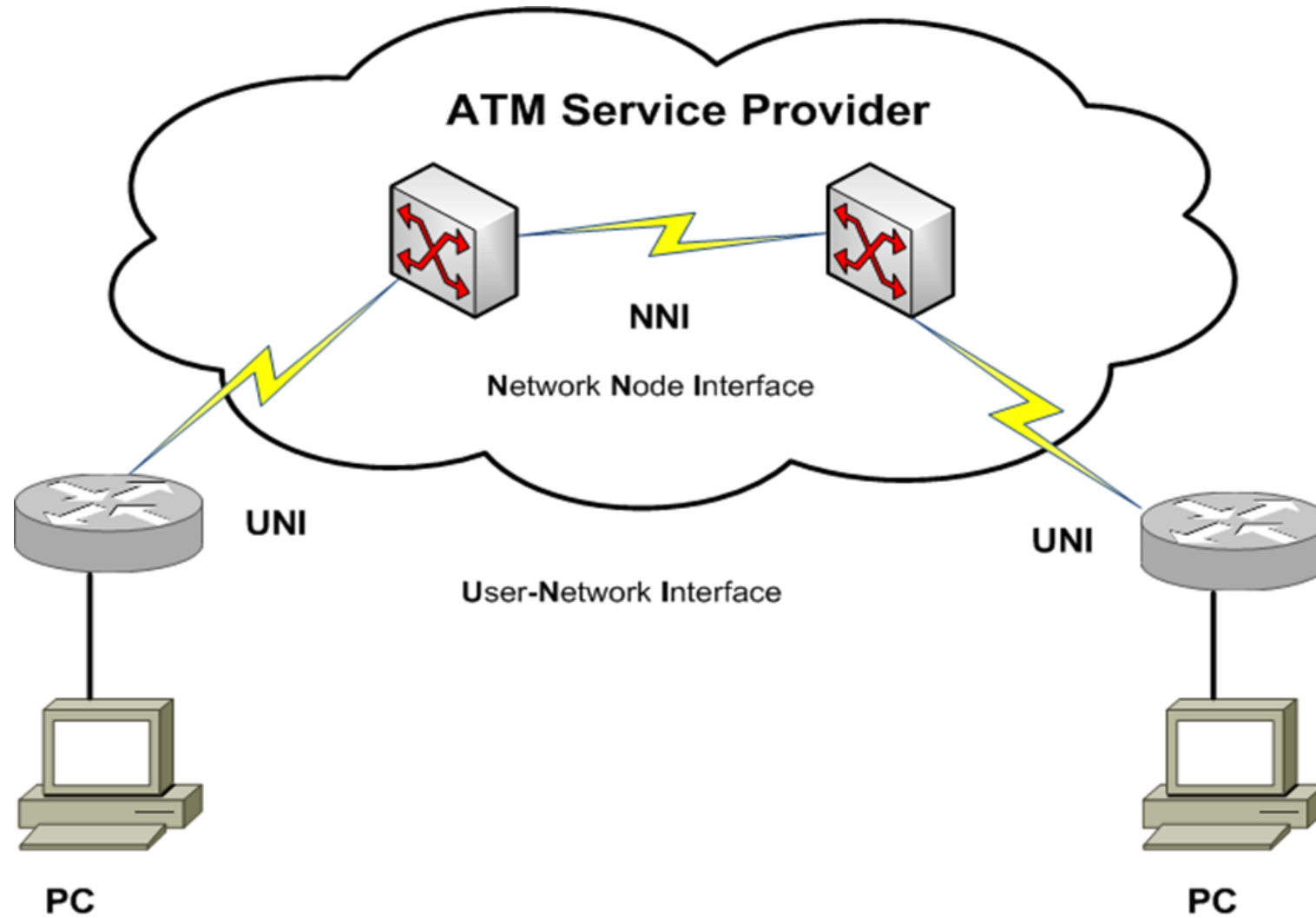


Frame Relay

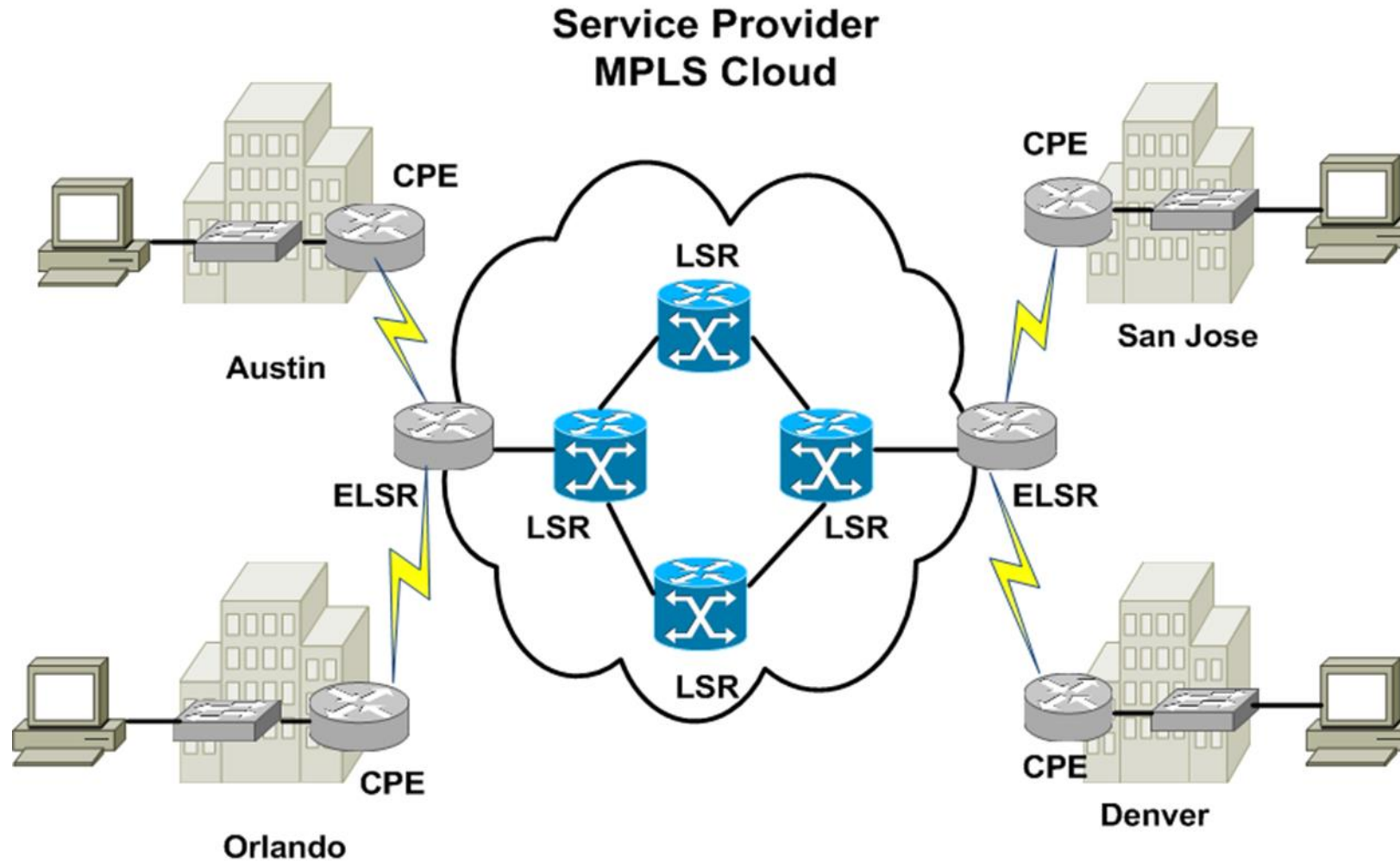


- Virtual circuits at layer 2
- PVCs (permanent virtual circuits)
- SVCs (switched virtual circuits)

ATM



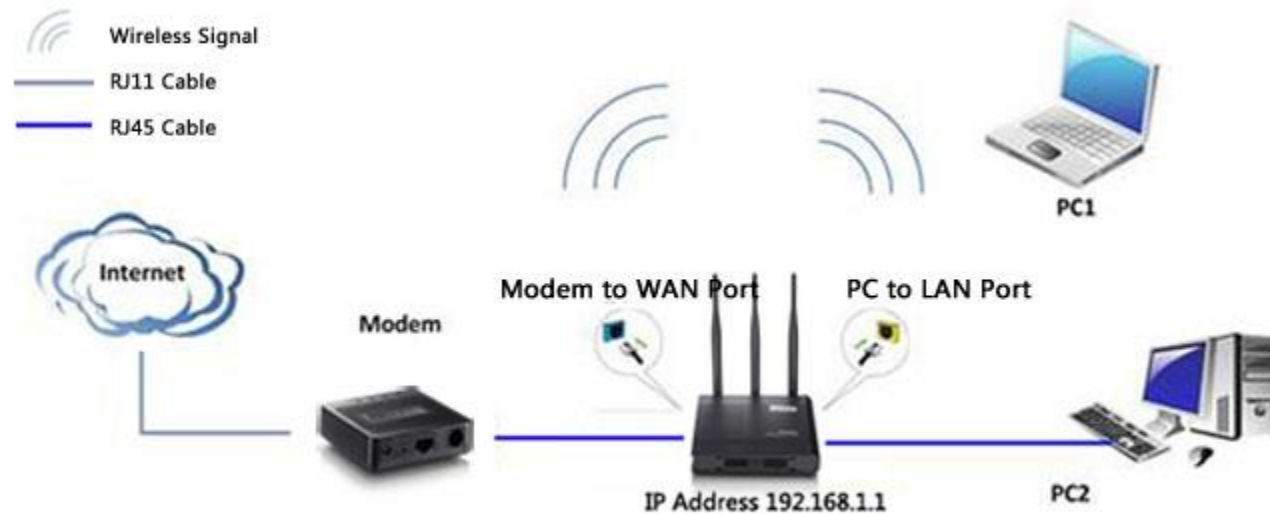
Multiprotocol Label Switching



Connecting Wirelessly

Objectives

- How do various *wireless* LAN (WLAN) technologies function, and what wireless standards are in common use?
- What are some of the most important WLAN design considerations?
- What WLAN security risks exist, and how can those risks be mitigated?



Introducing Wireless LANs

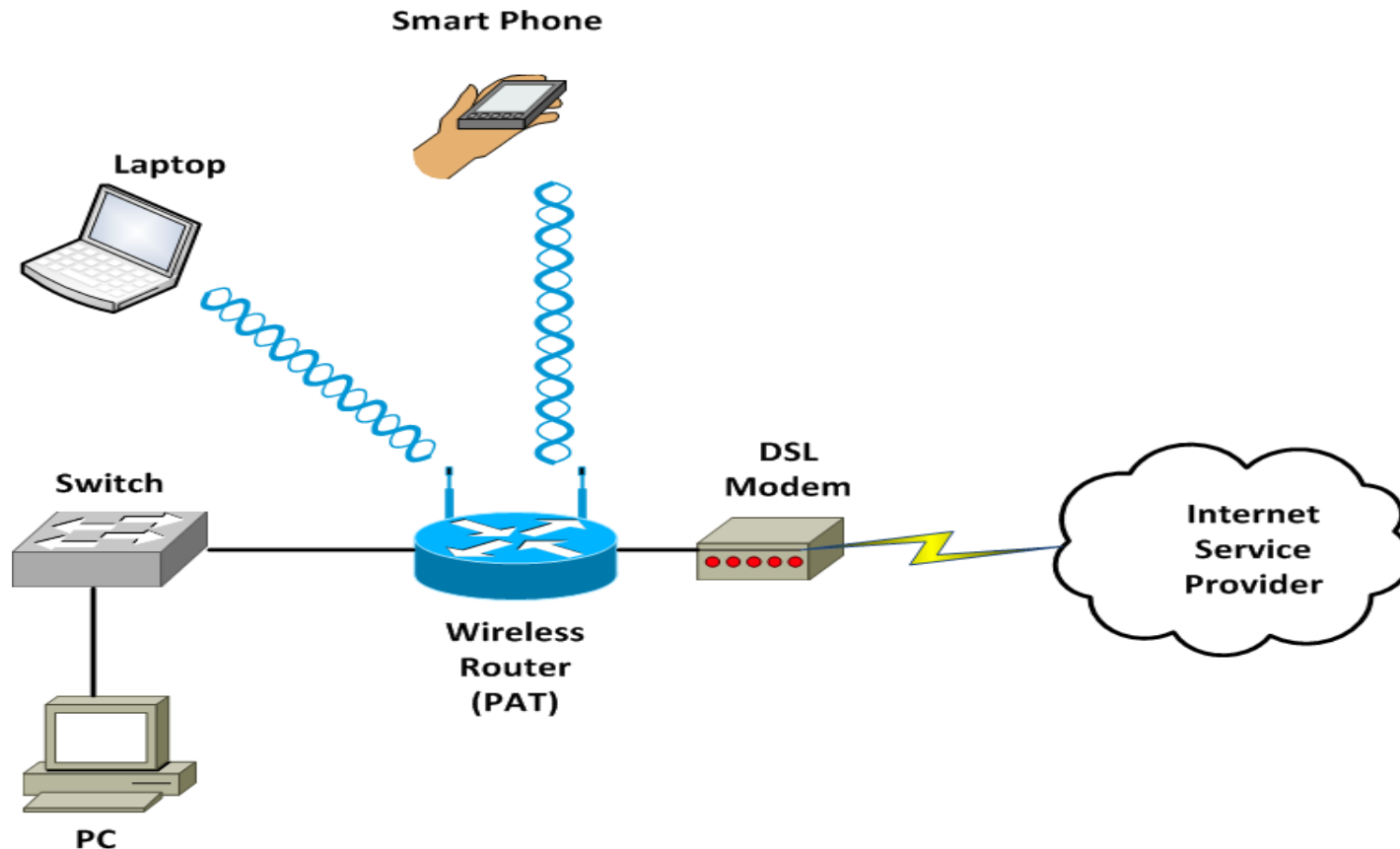
- The popularity of wireless LANs (WLAN) has exploded over the past decade, allowing users to roam within a WLAN coverage area, allowing users to take their laptops with them and maintain network connectivity as they move throughout a building or campus environment.
- Wireless device, such as laptops and smart phone, often have a built-in wireless card that allows those devices to communicate on a WLAN.

WLAN Concepts and Components

- Wireless Routers
- The wireless router obtains an IP address via DHCP from the Internet service provider(ISP).
- The router uses PAT, to provide IP addressing services to devices attaching to it wireless or through a wired connection.
- The process through which a wireless client attaches with a wireless router (or wireless AP) is called association.
- All wireless devices associating with a single wireless router or AP share a collision domain.

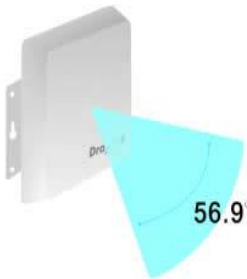
WLAN Concepts and Components

- Wireless Access Point
- A wireless access Point (AP) interconnects a wired LAN with a WLAN, it does not interconnect two networks
- The AP connects to the wired LAN, and the wireless devices that connect to the wired LAN via the AP are on the same subnet as the AP.

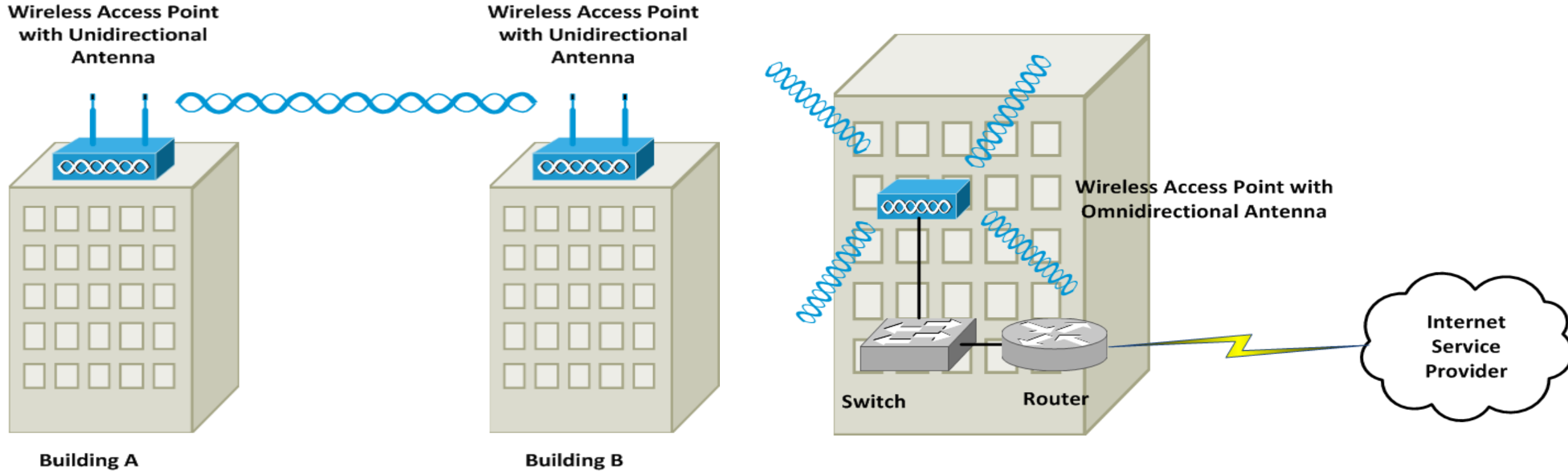


WLAN Concepts and Components

- Antennas
- The coverage area of a WLAN is largely determined by the type of antenna used on the wireless AP or wireless router.
- Design goals to keep in mind when selecting an antenna include the following
- Required distance between an AP and a wireless client.
- Pattern of coverage area (for example, the coverage area might radiate out in all directions, forming a spherical coverage area around an antenna, or an antenna might provide increased coverage in only one or two directions.
- Indoor or outdoor environment
- Avoiding interference with other Aps
- Omnidirectional: An omnidirectional antenna radiates power at relatively equal power levels in all directions.
- Unidirectional: Unidirectional antennas can focus their power in a specific direction, thus avoiding interference with other wireless devices and perhaps reaching greater distances.

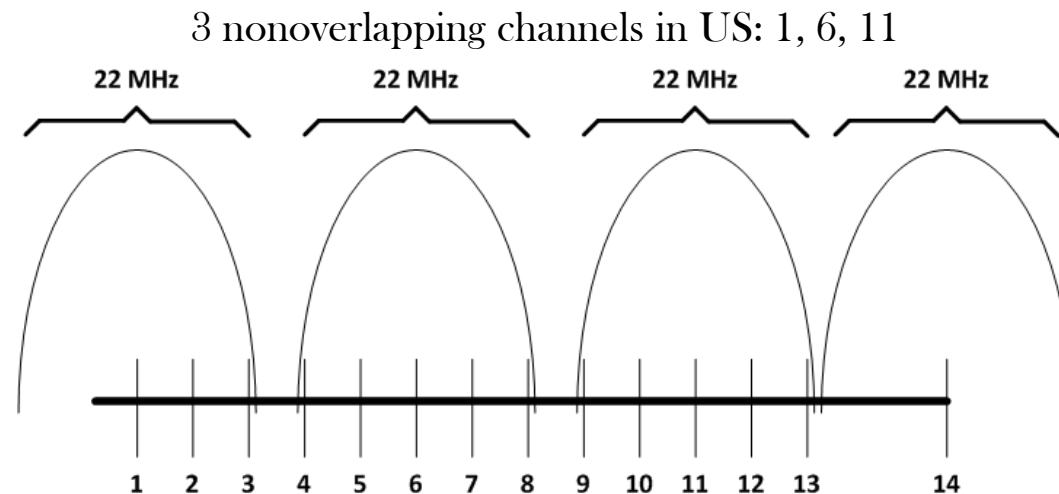


WLAN Concepts and Components



WLAN Concepts and Components

- Frequencies and Channels
- A characteristic to watch out for is the frequencies at which these standards operate.
- There are some country-specific variations, certain frequency ranges (or frequency bands) have been reserved internationally for industrial, scientific, and medical purposes.
- These frequency bands are called the ISM bands.
- Two of these bands are commonly used for WLANs.
- 2.4 GHz - 2.5 GHz range. Referred to as the 2.4 GHz band.
- 5.75 GHz - 5.875 GHz range. Referred to as the 5 GHz Band
- Within each band are specific frequencies (or channels) at which device operate.



WLAN Concepts and Components

- CSMA/CA
- We already learned that Ethernet's carrier sense multiple access / collision detection (CSMA/CD) technology is used to control traffic on a wired network.
- WLAN use a similar technology called carrier sense multiple access/collision avoidance (CSMA/CA).
- A WLAN device listens for a transmission on a wireless channel to determine if it is safe to transmit.
- Transmission Methods
- Earlier you saw the frequencies used for various wireless channels.
- Those frequencies are considered to be the center frequencies of a channel.
- In actual operation, a channel uses more than one frequency, which is a transmission method called spread spectrum.
- These frequency are, however, very close to one another, which is called narrowband transmission.
- Transmission Methods
- WLAN use one of the following types of spread-spectrum technology:
- Direct-sequence spread spectrum (DSSS)
- Modulates data over an entire range of frequencies.
- Frequency-hopping spread spectrum (FHSS)
- Allows the participants in a communication to hop between predetermined frequencies or channels.
- Orthogonal frequency division multiplexing (OFDM)
- Uses a relatively slow modulation rate, combined with the simultaneous transmission of data over 52 data streams.

By : Eng. Ahmad Hassan Al-Mashaikh

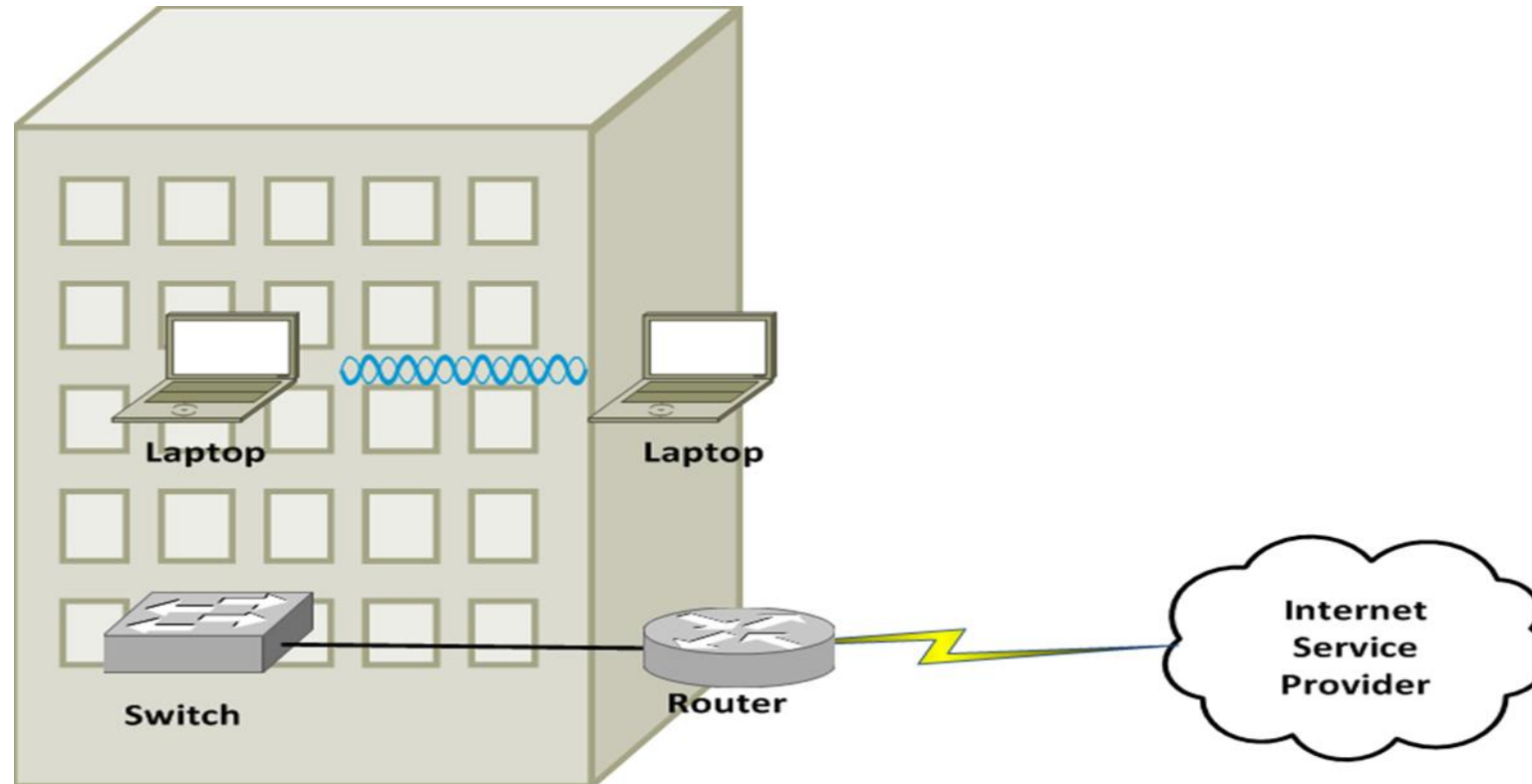
Email : Ahmad.private.mashaikh@Hotmail.com

WLAN Standard

Standard	Band	Max. Bandwidth	Transmission method	Max. Range
802.11	2.4GHz	1 Mbps or 2 Mbps	DSSS or FHSS	20m indoors/100 m outdoors
802.11a	5 GHz	54 Mbps	OFDM	35m indoors/120m outdoors
802.11b	2.4GHz	11 Mbps	DSSS	32m indoors/140m outdoors
802.11g	2.4GHz	54 Mbps	OFDM or DSSS	32m indoors / 140m outdoors
802.11n	2.4GHz or 5GHz (or both)	130-150Mbps > 300 Mbps (with channel bonding)	OFDM	70m indoors/250m outdoors

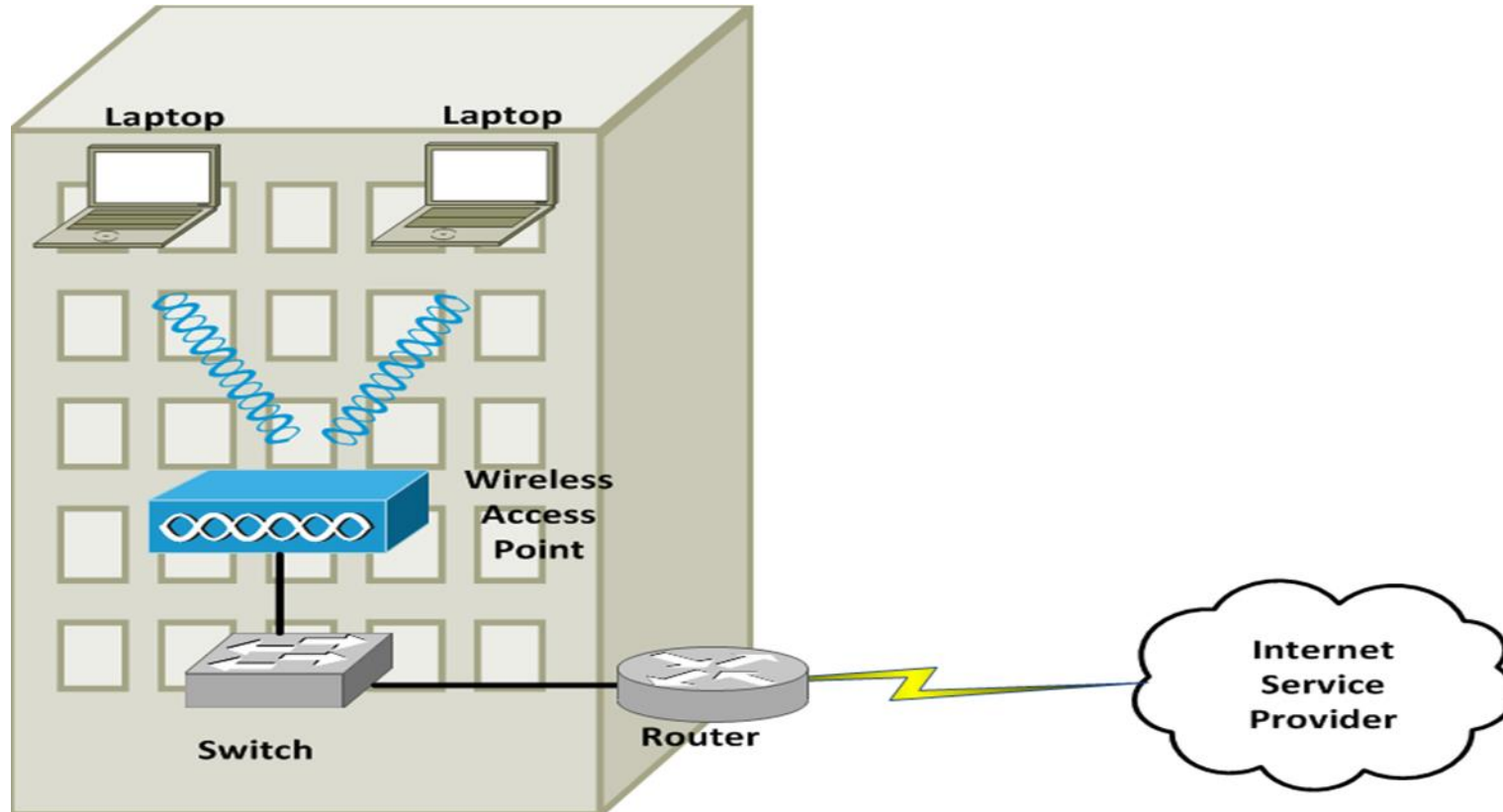
WLAN Standard

- Independent Basic Service Set (IBSS) WLAN (ad-hoc)



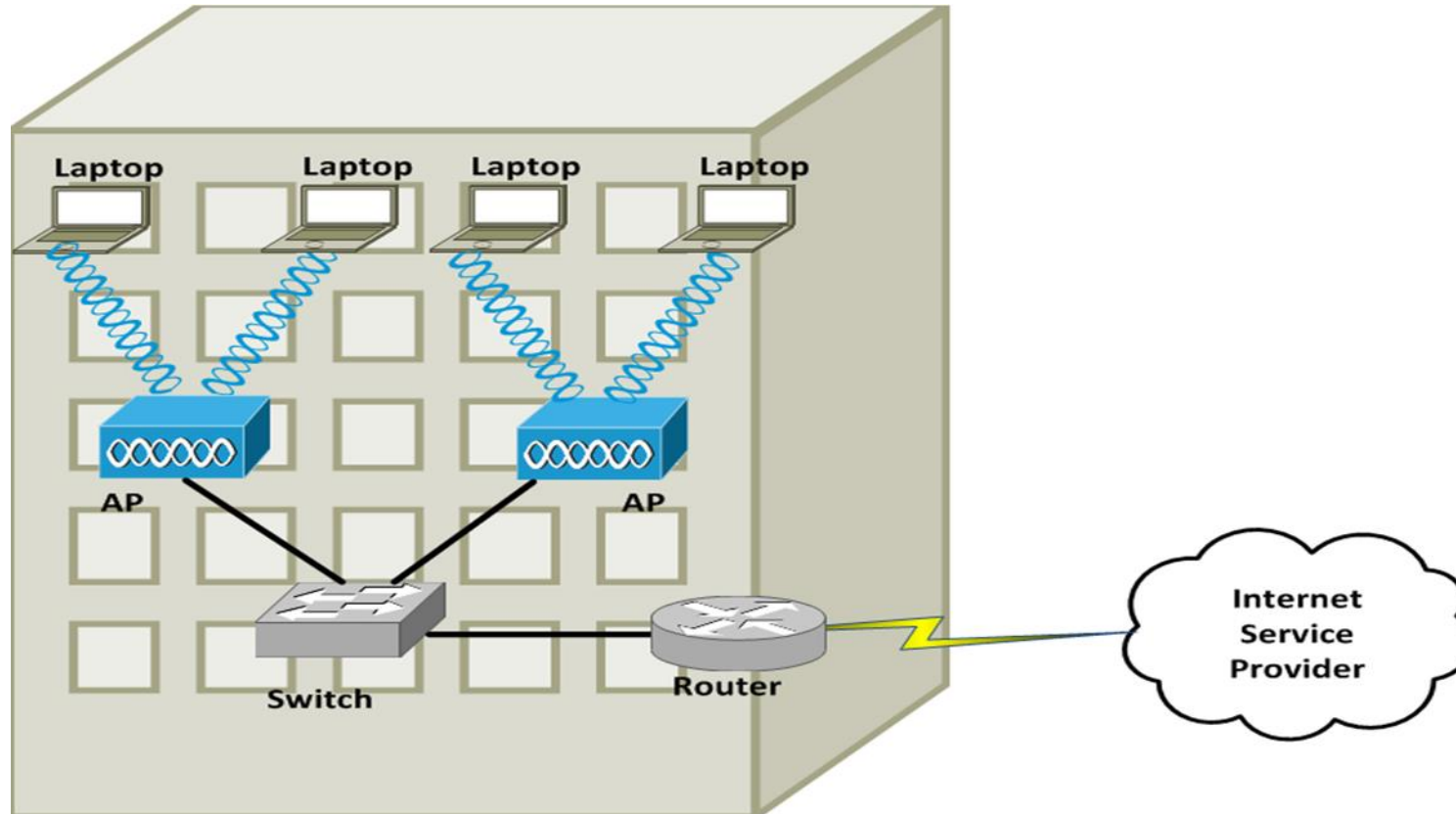
WLAN Standard

- Basic Service Set (BSS) WLAN



WLAN Standard

- Extended Service Set (ESS) WLAN



Sources of Interference

- A major issue for WLANs is radio frequency interference (RFI) caused by other devices using similar frequencies to the WLAN device.
- Other WLAN devices
- Cordless Phone/ Baby Monitors
- Microwave ovens
- Wireless security systems devices
- Physical obstacles
- Signal strength

Wireless AP Placement

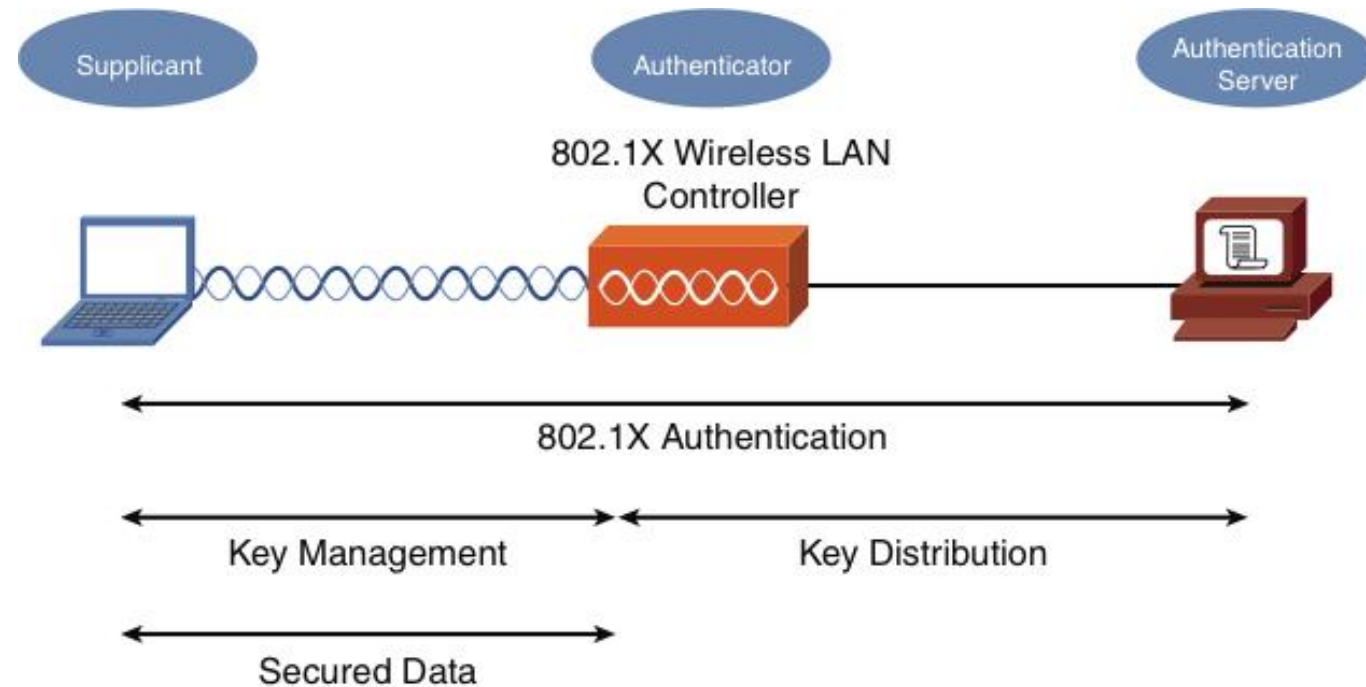
- WLAN using more than one AP (an ESS WLAN) require careful planning to prevent the Aps from interfering with one another, which still servicing a desired coverage area.
- An overlapping of coverage between APs should exist to allow uninterrupted roaming from one WLAN cell (which is the coverage area provided by the AP) to another.
- However, those overlapping coverage areas should not use overlapping frequencies.

Securing Wireless LANs

- Security Issues
- WLANs introduce some unique concerns to your network.
- Improperly installed wireless APs, and routers are roughly equivalent to putting an Ethernet Port in a building's parking lot, where anyone can drive up and have access to your network.
- Today hackers and those who want to use free internet access perform reconnaissance, known as war driving, looking for unsecured WLANs
- Other WLAN security threat include the following
 - WEP cracking – WEP is worthless, easily cracked
 - My students crack WEP as a CNIT 123 project
 - WPA and WPA-2 are both very secure
 - WPS ruins it (Wi-Fi Protected Setup)
 - Rouge access points – A malicious user could set up his own AP to which legitimate users would connect.

Securing Wireless LANs

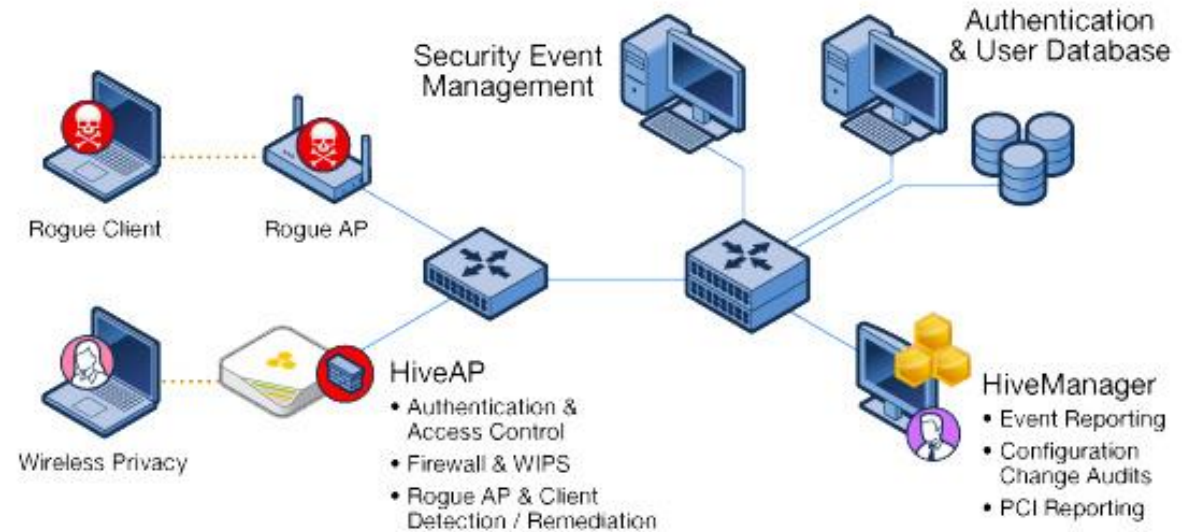
- Approaches to WLAN Security
- A WLAN that does not require any authentication or provide encryption for wireless devices is said to be using open authentication.
- To protect WLAN traffic from eavesdroppers, a variety of security standards and practices have been developed, including the following.
- MAC address Filtering
- Disabling SSID broadcast
- Preshared Key
- IEEE 802.1X



IEEE 802.1x Security for a WLAN

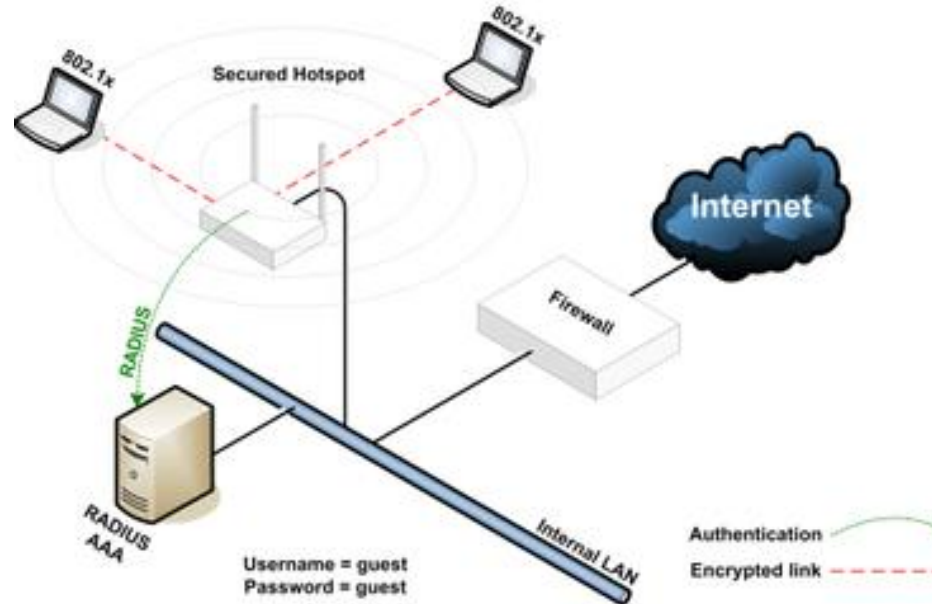
Securing Wireless LANs

- Security Standards
- When configuring a wireless client for security, the most common security standards form which you can select are as follows:
- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- Wi-Fi Protected Access version 2 (WPA2)
- WEP
- 40-bit WEP Key
- APs and client must use the same key.
- 24-bit initialization vector (IV)
- Sent in clear text.
- It could be compromised with a brute-force attack.



Securing Wireless LANs

- WAP
- Can require a user to authenticated before keys are exchanged.
- The keys used between a wireless client and an access point are temporary session keys.
- Temporal Key Integrity Protocol (TKIP)
- Message Integrity Check (MIC)
- WAP2
- Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)
- Advanced Encryption Standard (AES)



Optimizing Network Performance

Objectives

- Why is high availability a requirement in today's network designs, and what mechanisms can help provide that high availability?
- What various technologies optimize network performance?
- What QoS mechanisms can help optimize network performance?
- Using what you have learned in this and previous chapters, how do you design a SOHO (Small Office/Home Office) network based on a set of requirements?

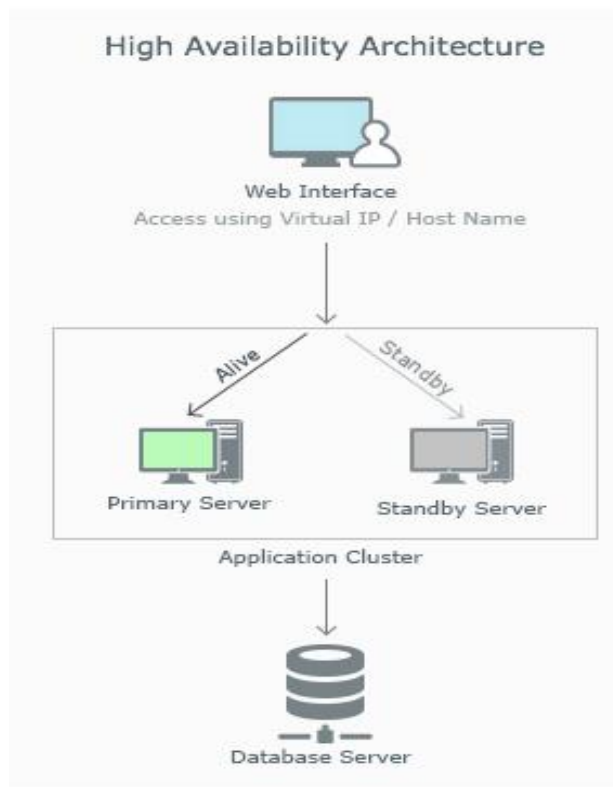
Optimizing Network Performance

- Networks were once relegated to the domain of data, can now carry voice and video.
- These additional media types, in addition to mission-critical data applications, need a network to be up and available for its users.
- Beyond basic availability, today's networks need optimization tools to make the most of their available bandwidth.
- QoS, as one example, can give priority treatment to latency-sensitive traffic, such as Voice over IP (VoIP).



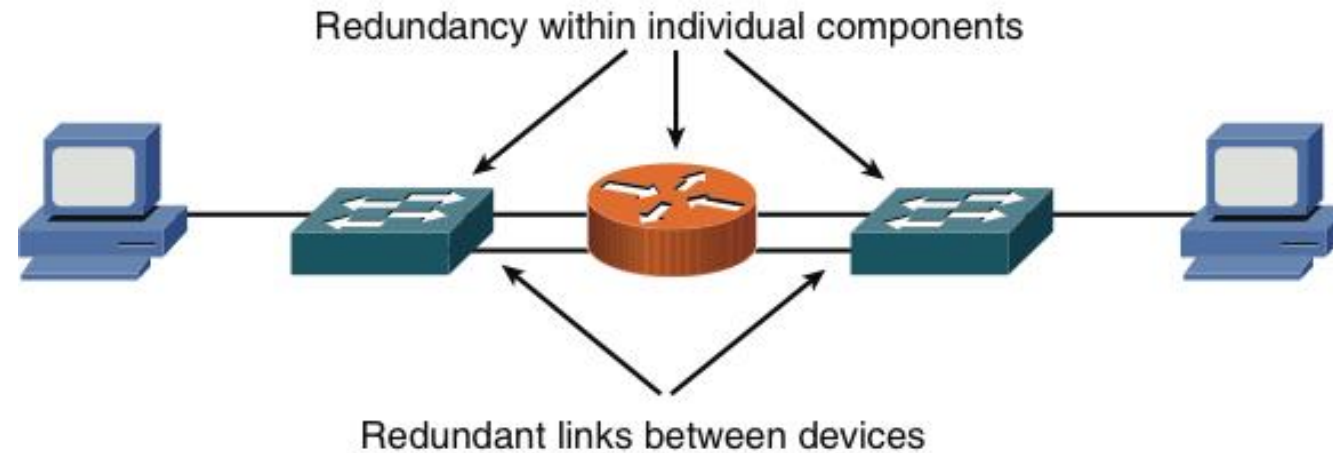
High Availability

- If a network router or switch stops operating correctly (meaning that a network fault occurs), communication through the network could be disrupted, resulting in a network becoming unavailable to its users (a failure).
- Therefore, network availability, called uptime, is a major design consideration.
- The availability of a network is measured by its uptime during a year. For example if a network is said to have five nines of availability, it is up 99.999% of the time, which translates to a maximum of 5 minute of downtime per year.



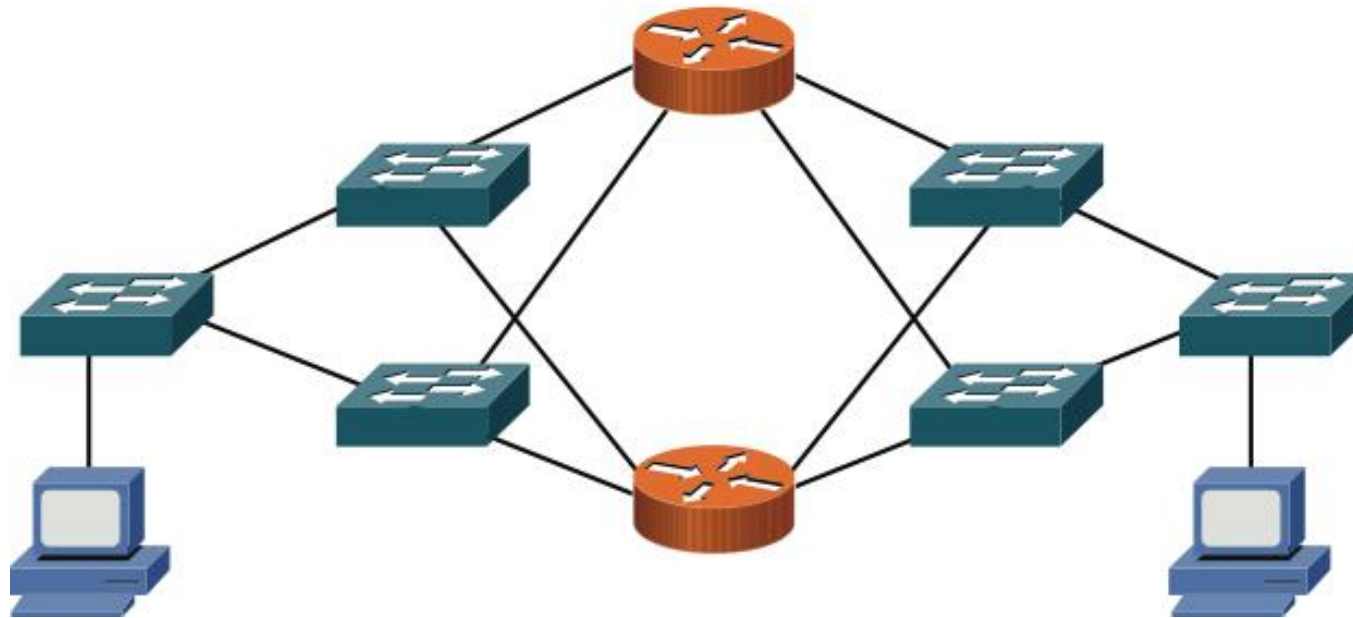
Fault-Tolerant Network Design

- Redundant Network with Single Points of Failure



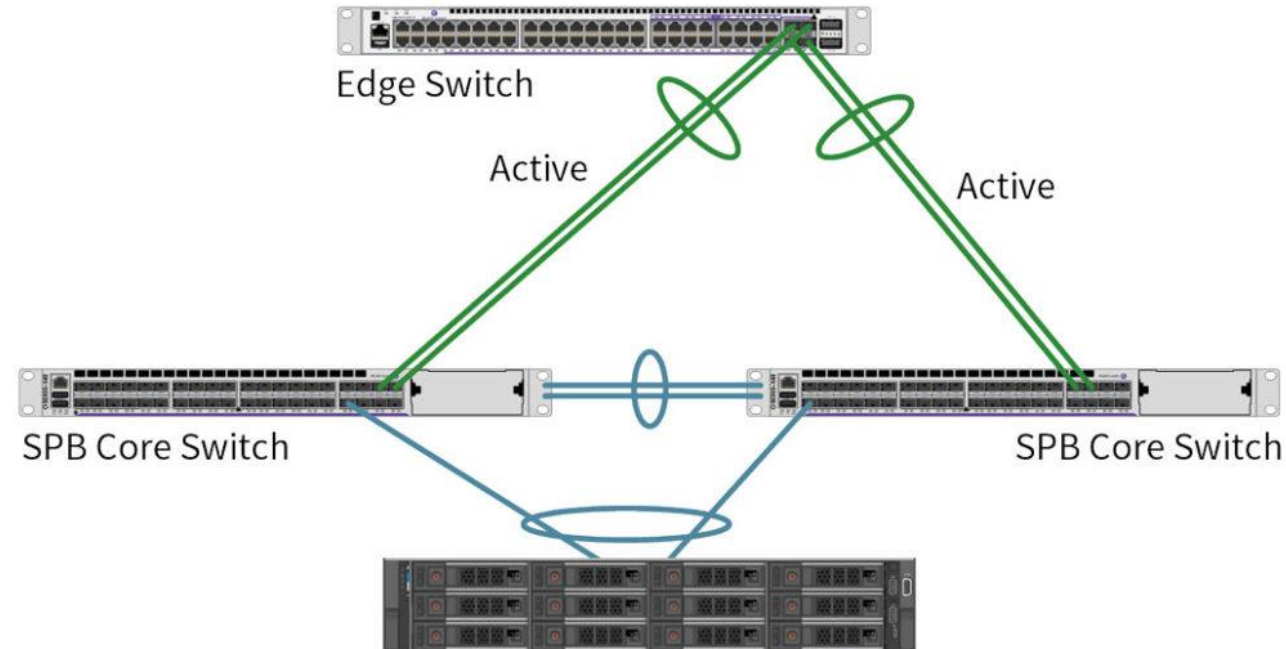
Fault-Tolerant Network Design

- Redundant Network with No Single Point of Failure



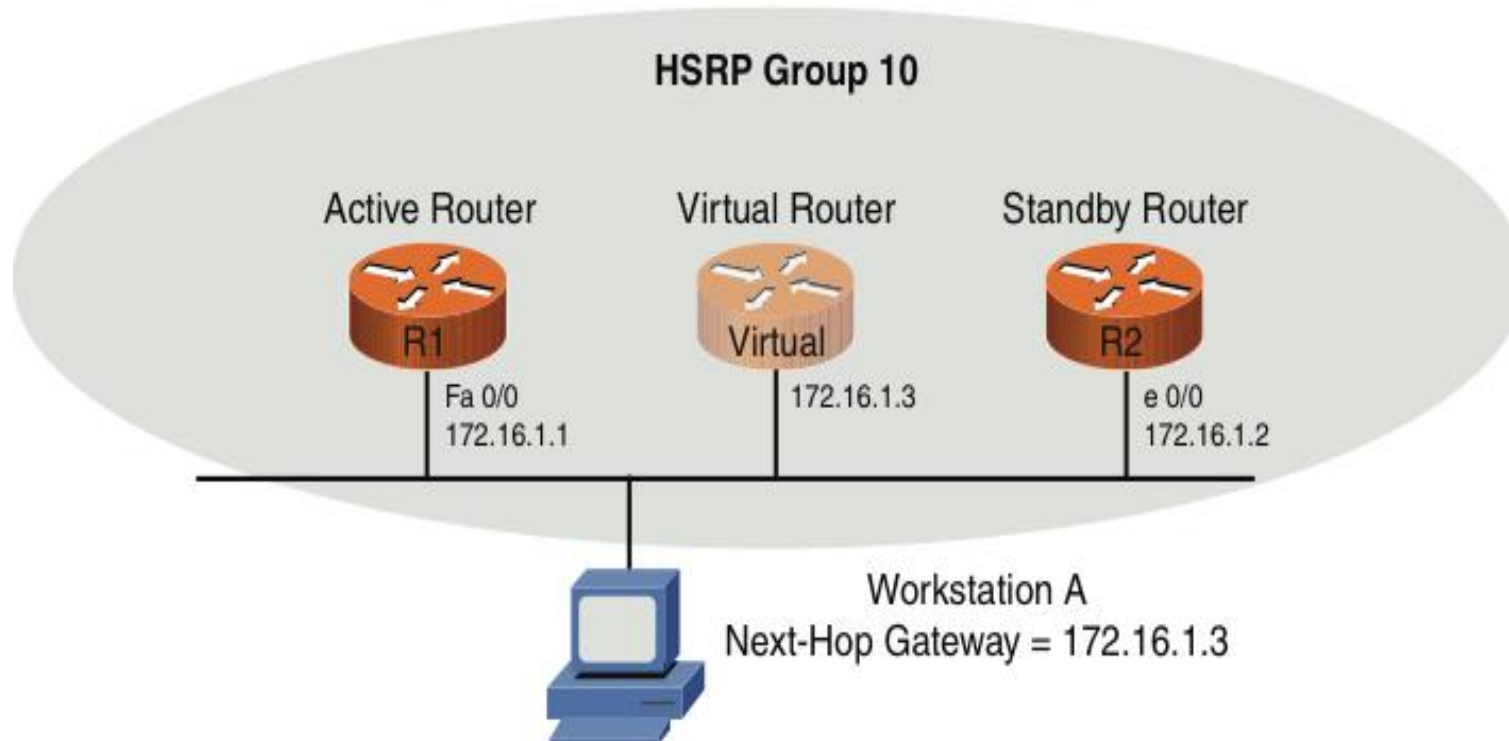
Hardware Redundancy

- Having redundant route processors in a switch or router chassis improves the chassis' reliability.
- An end system can have redundant NIC's. The two modes of NIC redundancy are;
- Active-active: both NIC are active at the same time.
- Active-standby: one NIC is active and the other is waiting to take over, in the event of a failure.
- Have redundant routers and switches improves the network's reliability.
- Hot standby Router Protocol (HSRP) (Cisco proprietary)
- Common Address Redundancy Protocol (CARP) (Open)



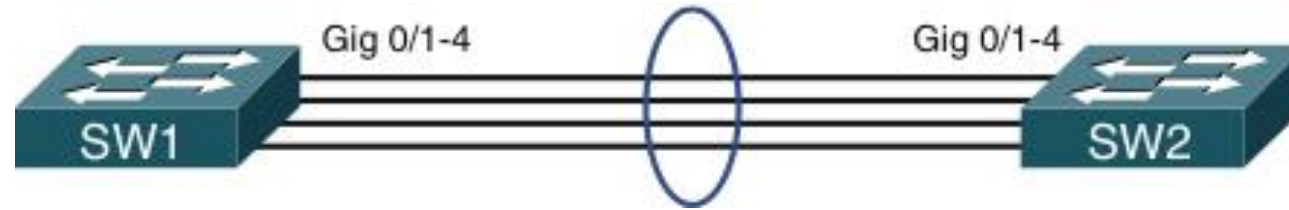
Hardware Redundancy

- HSRP Sample Topology



LACP (Link Aggregation Control Protocol)

- Combines multiple physical links into a single logical link



Design Considerations

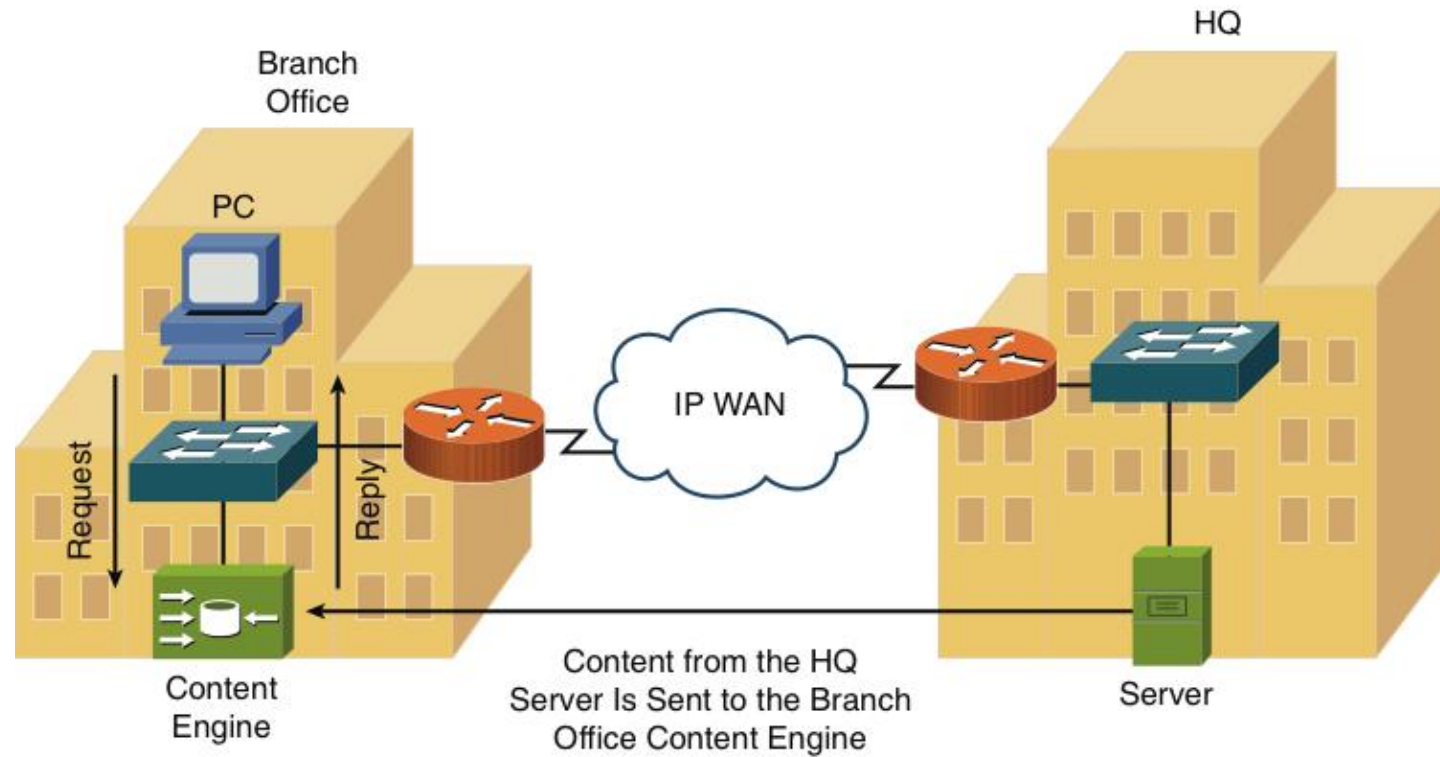
- When designing networks for high availability, answer the following questions:
- Where will module and chassis redundancy be used?
- What software redundancy features are appropriate?
- What protocols characteristics affect design requirements?
- What redundancy features should be used to provide power to an infrastructure device.
- What redundancy features should be used to maintain environmental conditions.

High-Availability Best Practices

- The following steps are five best practices for designing high-availability networks:
 1. Examine technical goals.
 2. Identify the budget to fund high-availability features.
 3. Categorize business applications into profiles, each of which requires a certain level of availability.
 4. Establish performance standards for high-availability solutions
 5. Define how manage and measure the high-availability solution

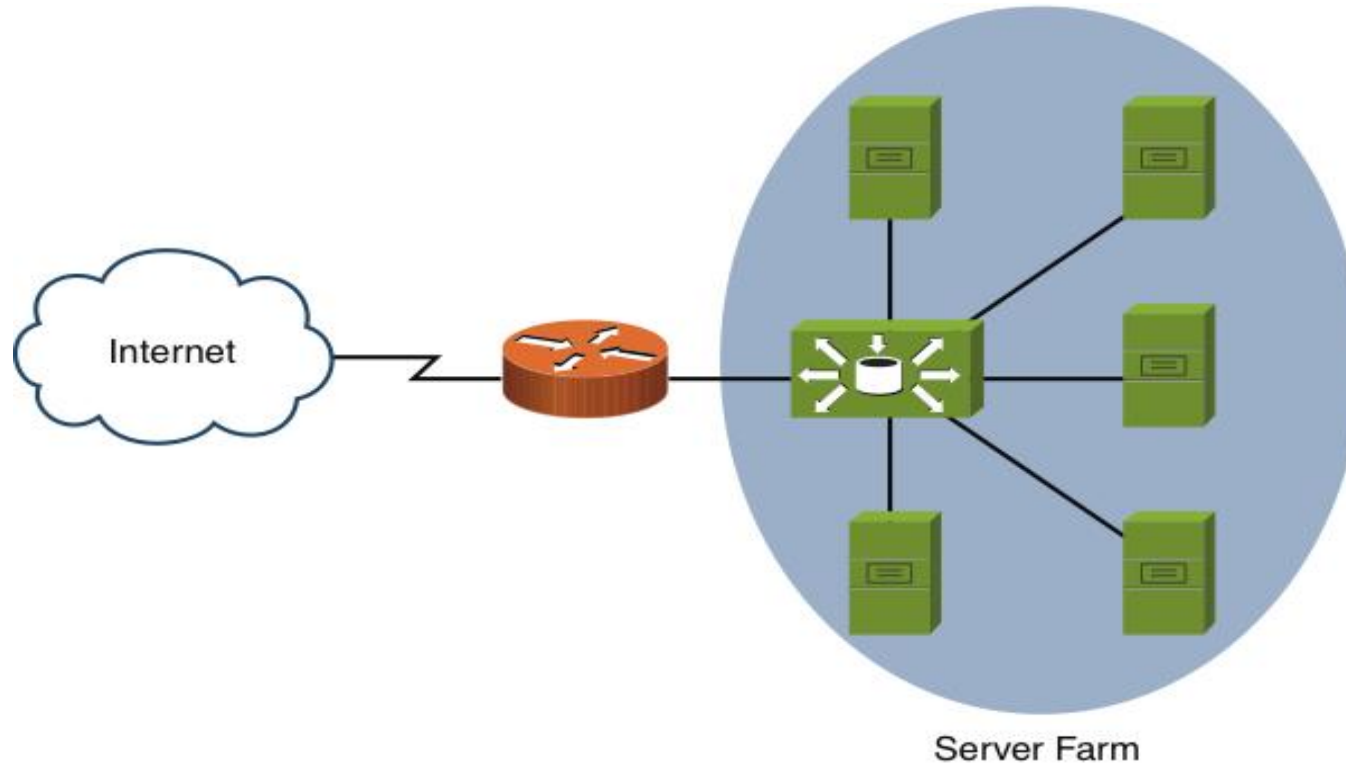
Content Caching

- Content Engine Sample Topology



Load Balancing

- Content Switching Sample Topology



QoS Technologies

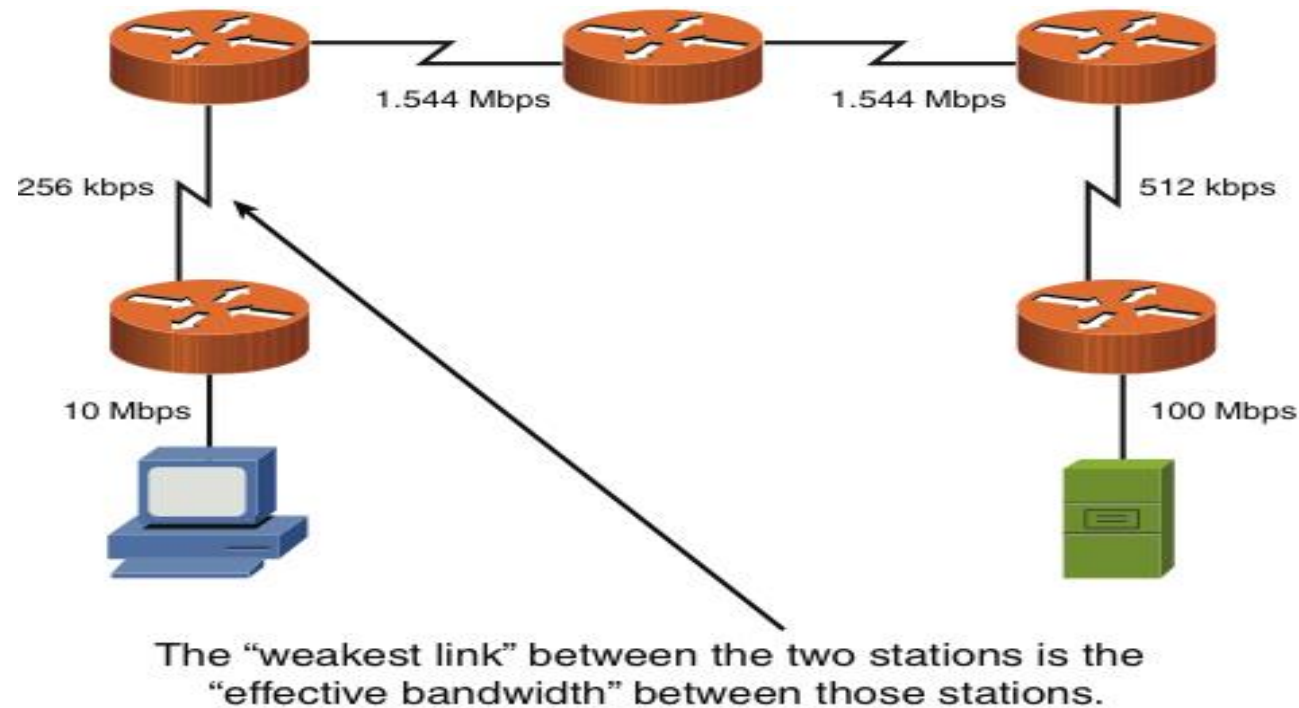
- Quality of Service (QoS) is a suite of technologies that allows you to strategically optimize network performance for select traffic types.
- Through the use of QoS, you can identify which traffic types need to be sent first, how much bandwidth to allocate to various traffic types, which traffic types should be dropped first in the event of congestion, and how to make the most efficient use of the relatively limited bandwidth of an IP WAN.

Issue	Description
Delay	Delay is the time required for a packet to travel from its source to its destination.
Jitter	Jitter is the uneven arrival of packets.
Drops	Packets drops occur when a link is congested and a router's interface queue overflows.

QoS Technologies

- Fortunately, QoS features available on many routers and switches can recognize important traffic and treat it in a special way.
- As a packet travels from its source to its destination, its effective bandwidth is the bandwidth of the slowest link along that path.

Effective Bandwidth of 256 kbps



QoS Configuration Steps

1. Determine network performance requirement for various traffic types.
 - Voice:
 - Video
 - Data
2. Categorize traffic into specific categories.
 - Low Delay
 - Low Priority
3. Document your QoS policy and make it available to your users.

QoS Components

Issue	Description
Best-effort	Best-effort treatment of traffic does not truly provide QoS to that traffic, because there is no reordering of packets. Best-effort uses FIFO queuing.
Integrated Services (IntServ)	IntServ is often referred to as hard QoS, because it can make strict bandwidth reservations. IntServ uses signaling among the network devices to provide bandwidth reservations.
Differentiated services	DiffServ, differentiates between multiple traffic flows. Specifically, packets are <i>marked</i> , and routers and switches can then make decisions based on those markings.

QoS Mechanisms

- The DiffServ approach to QoS marks traffic. However, for markings to impact the behavior of traffic, a QoS tool must reference those markings and alter the packets' treatment based on them.
- The following is a collection of commonly used QoS mechanisms:
 - Classification
 - Marking
 - Congestion management
 - Congestion avoidance
 - Policing and shaping
 - Link efficiency

Using Command-Line Utilities

Objectives

- What are some of the more useful Microsoft Windows command for configuring and troubleshooting network client and servers?
- What are some of the more useful UNIX/LINUX command for configuring and troubleshooting network client and servers?
- Your configuration and troubleshooting of networks will undoubtedly involve issuing command at an operating system (OS) prompt of an end-user computer (a client) or a server.
- Some commands, you will notice, exist on both Microsoft Windows and UNIX/LINUX platforms.

Windows Commands

- **arp** -- this command can be used to see what a Layer 2 MAC address corresponds to a known Layer3 IP address.
- **ipconfig** – this command can be used to display IP address configuration parameters on a Windows PC.
- **nbtstat** – this command display NetBIOS information for IP-based networks.
- **netstat** – command can be used to display various information about IP-based connection on a PC.
- You can view information about current sessions, including source and destination IP address and port numbers.
- **nslookup** – this command can be used to resolve an FQDN to an IP address.
- **ping** – this command is used to check IP connectivity between two network devices.
- **route** – command can display a PC's current IP routing table.
- **tracert** – this command pings every router hop from the source to the destination and reports the round-trip time for each router hop.

Unix Commands

- **man** – this command is used to find information how to use a UNIX command.
- **arp** -- this command can be used to see what a Layer 2 MAC address corresponds to a known Layer3 IP address.
- **dig** and **nslookup** – these commands can be used to resolve FQDNs to IP addresses.
- The **dig** command returns more information
- **host** – is another command that will resolve FQDNs to IP addresses.
- **ifconfig** – this command can be used to display IP address configuration parameters on a Windows PC.
- **traceroute** – this command pings every router hop from the source to the destination and reports the round-trip time for each router hop.
- **netstat** – command can be used to display various information about IP-based connection on a PC.
- You can view information about current sessions, including source and destination IP address and port numbers.
- **ping** – this command is used to check IP connectivity between two network devices.
- Unlike the windows version you must give a count or the number of pings to conduct.

Managing a Network

Objectives

- What are some of the more common tools used to physically maintain a network?
- What components are involved in configuration management?
- What sorts of networking monitoring tools are available to network administrators, and what type of information are included in various logs?
- Even with a network's increasing dependence on wireless technologies, physical cabling still comprises the critical backbone of a network.
- A network management, monitoring, and troubleshooting require a familiarity with variety of cable maintenance tools.
- Another key network-management element is documentation.

Maintenance Tools

- The number of troubleshooting issues occurring in a network can be reduced by proper installation and configuration of the media and devices.
- A network administrator, need to be familiar with a collection of maintenance tools to help diagnose, isolate, and resolve the wiring issue.

Bit-Error Rate Tester

- The bit-error rate tester is used to make sure that the cable can past data with out and errors.



Bit-Error Rate Tester (BERT)

Butt Set

- Used by telephone technicians
- Connects to punch-down block
- Lets the technician butt into a phone call in progress
- To check the phone lines when troubleshooting connections



Cable Certifier

- The cable certifier is used by the cable installation technician to verify that a newly installed network cable works correctly.
- The cable certifier insures that the cable operates at the correct speeds.



Cable Tester

- The cable tester is used by the cable installation technician to test the continuity of the cable.
- It verifies that the correct pairs are connected together.



Connectivity Software

- When you are physical separated from the network you are maintaining or troubleshooting, you might be able to access the network through remote connectivity software
- Examples, **RealVNC**, **GoToMyPC**, **Remote Desktop Protocol**, **TeamViewer**, **LogMeIn**



Microsoft's Remote Desktop Connection

Crimper

- The crimper is use to make the cables. It attaches the RJ-45 ends to the cable.



Crimper



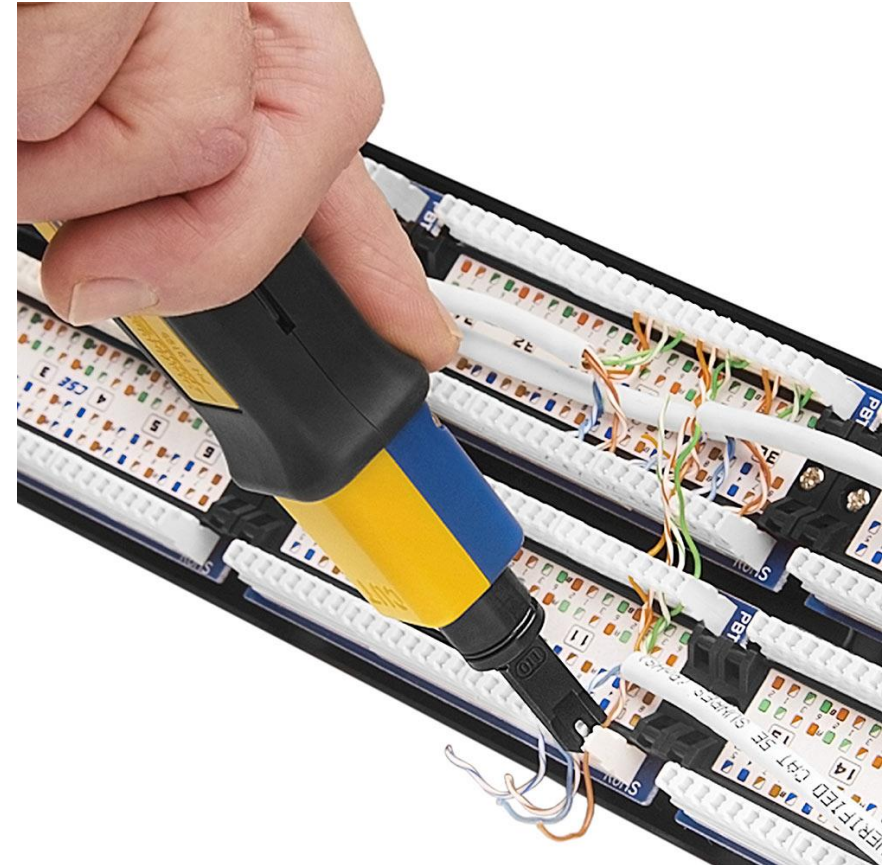
Jack Rapid



Crimper

Punch-Down Tool

- This tool terminating wires on a punch-down block, an insulated wire is inserted between two contact blades. These blades cut through the insulation and make electrical contact with the inner wire.
- As a result, you do not have to strip off the insulation.



Electrostatic Discharge Wrist Strap

- The ESD wrist strap is used to protect the equipment from ESD while you are working in it.

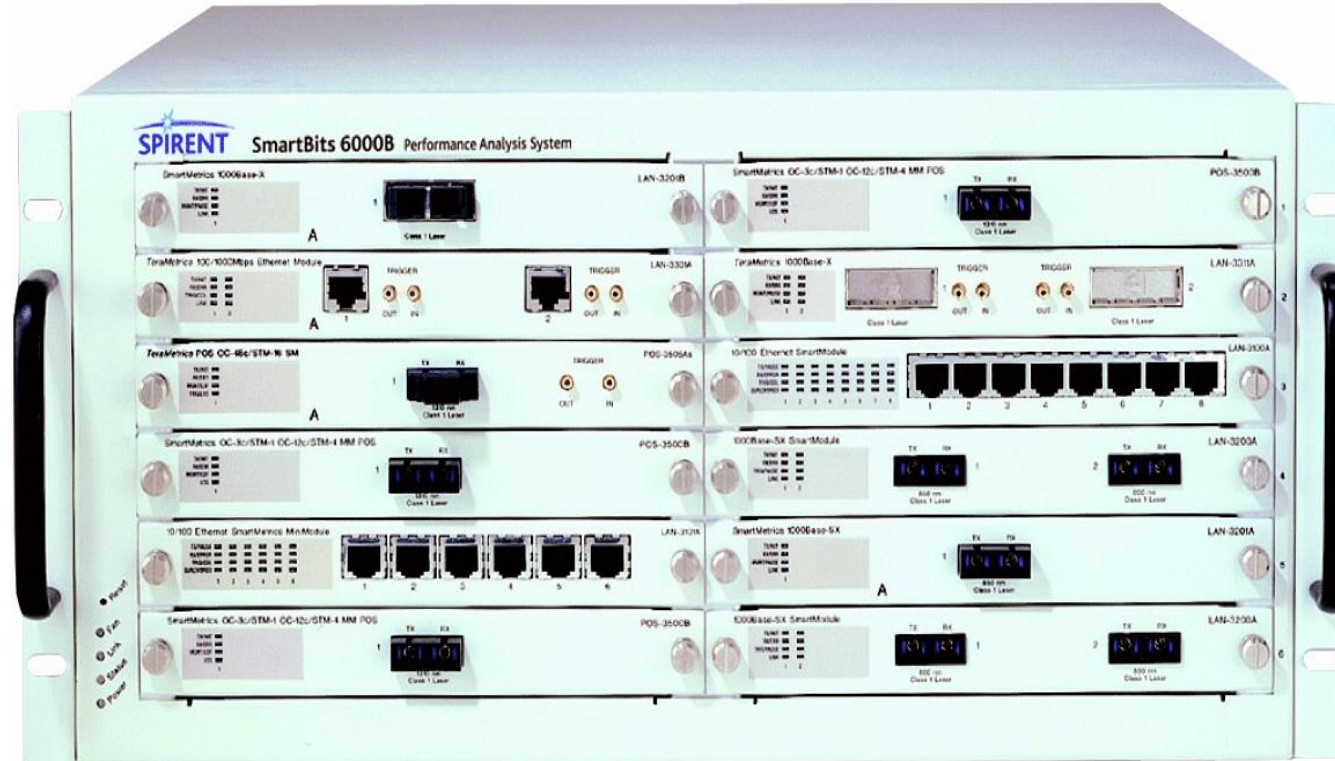


Multimeter

- When working with copper cabling, a multimeter can check a variety of a cable's electrical characteristics.
- These characteristics include;
 - Resistance (Ohms)
 - Current (Amps)
 - Voltage (Volts)



Throughput Tester



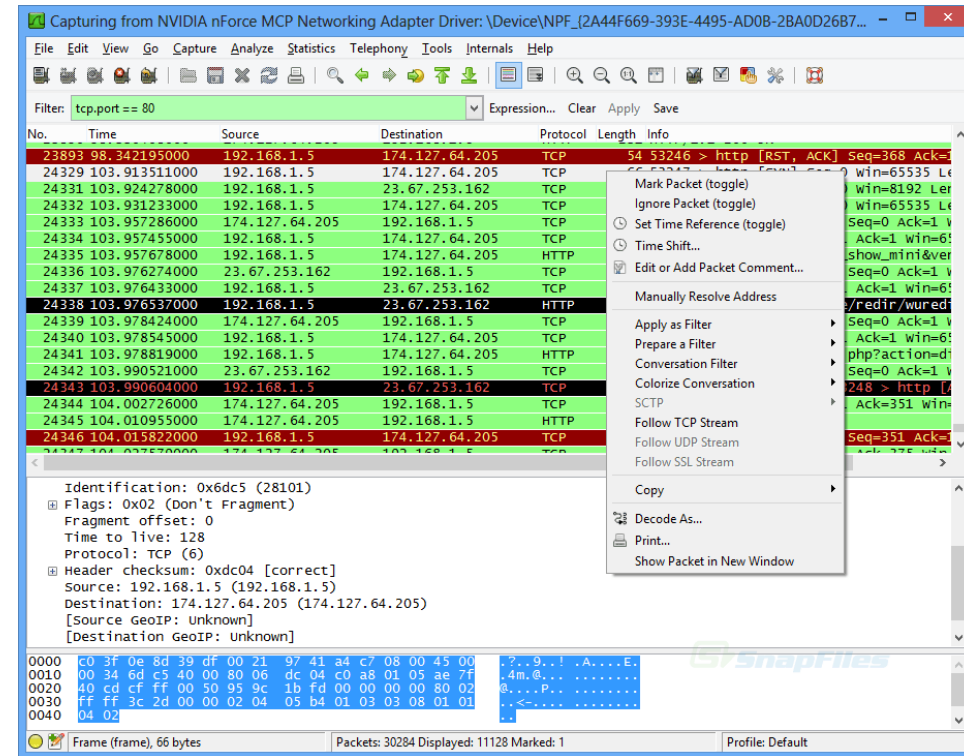
Throughput Tester (Photo Courtesy of NSS Labs)

Configuration Management

- Configuration Management (CM) focuses on maintaining up-to-date documentation of network's configuration.
- CM encompasses a variety of procedures, including the following:
- Asset Management
- Baselining
- Cable Management
- Change Management
- Network Documentation
- Contact information
- Policies
- Network Maps
- Wiring Schematics

Protocol Analyzer

- A protocol analyzer can be a standalone device or software running on a computer.
- You use a protocol analyzer to capture traffic flowing through a network.
- By examining the captured packets, you can discern the details of communication flows (session) as they are being setup, maintained, and torn down.
- Protocol Analyzer is also known as a network sniffer.



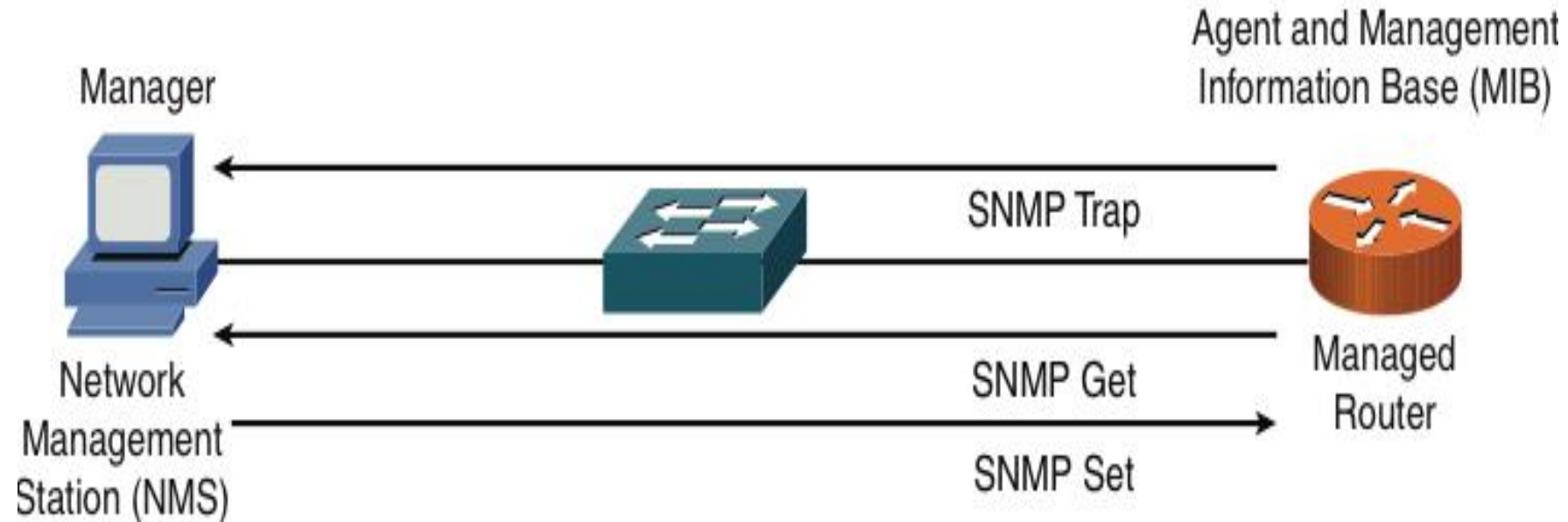
Wireshark Protocol Analyzer Software

Monitoring Resources and Reports

- Networks administrators routinely monitor network resources and review reports to be proactive in their administration.
- Monitoring resources and reports come from various sources, such as a syslog server, a Simple Network Management Protocol (SNMP) server, Event Viewer logs or packet captures from a network sniffer.
- SNMP – manage network nodes, such as network servers, routers, switches and hubs.

SNMP v1 & 2

- SNMPv1 and SNMPv2c Network-Management Components and Messages
- **Trap:** Unsolicited message about a significant event
 - Insecure cleartext transmission of community strings (passwords)



SNMP v3

- SNMPv3 Entities Much better security

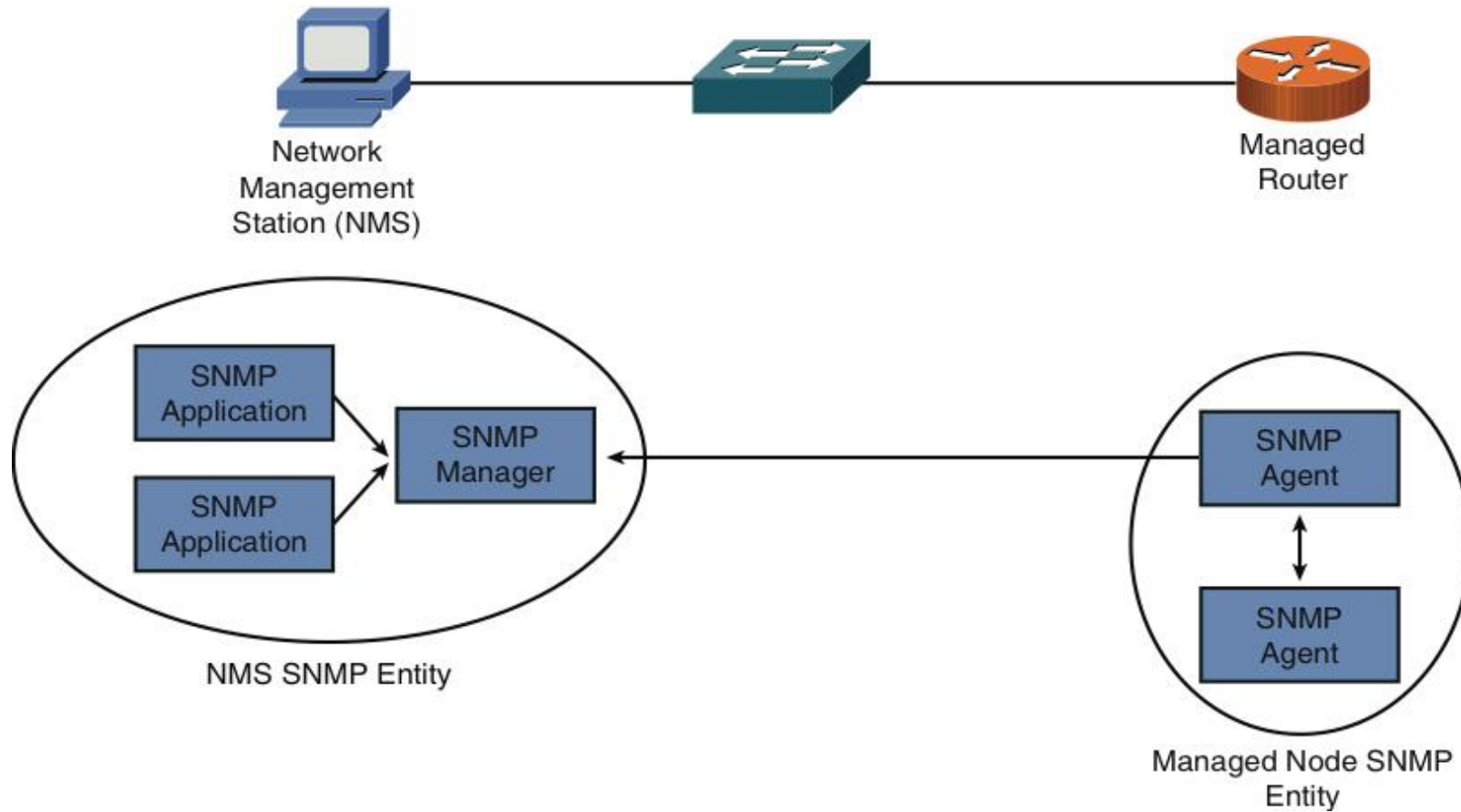
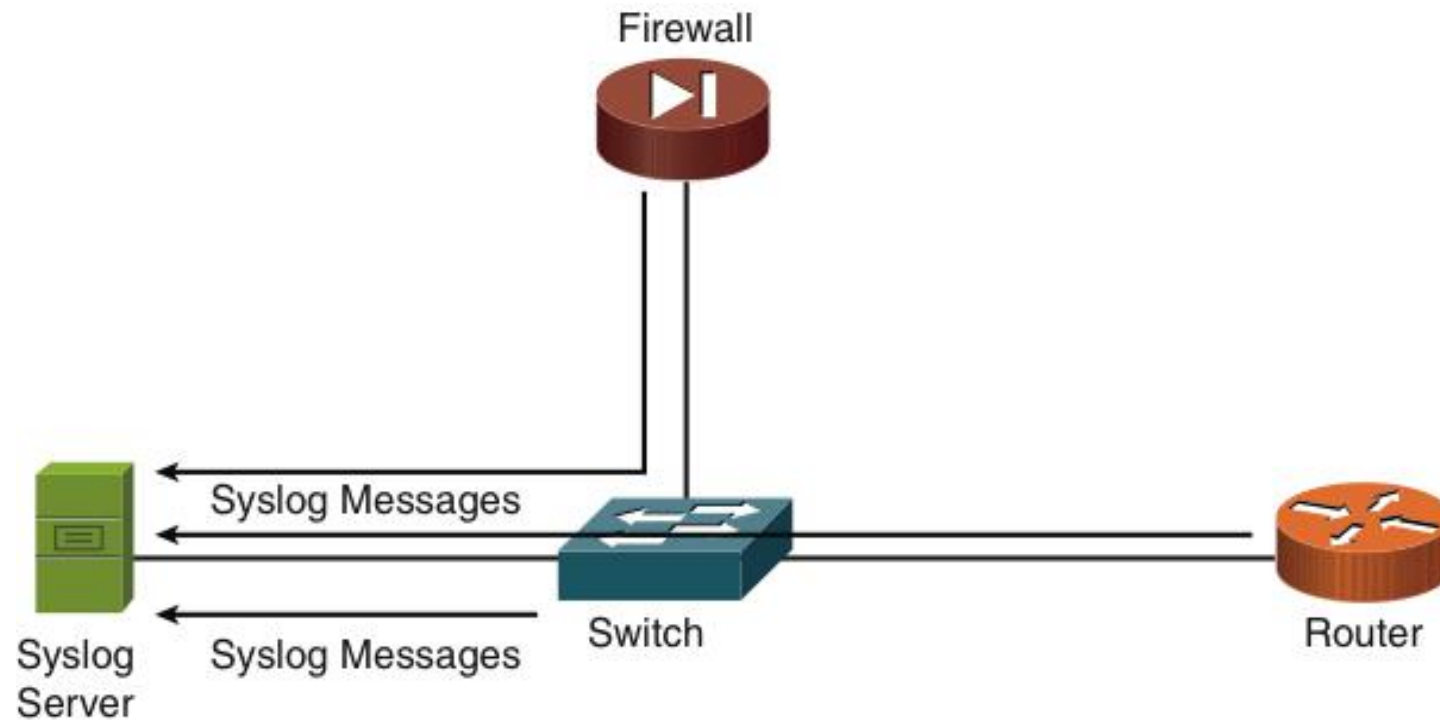


Table 11-2 Security Models and Security Levels Supported by Cisco IOS

Security Model	Security Level	Authentication Strategy	Encryption Type
SNMPv1	noAuthNoPriv	Community string	None
SNMPv2c	noAuthNoPriv	Community string	None
SNMPv3	noAuthNoPriv	Username	None
SNMPv3	authNoPriv	MD5 or SHA	None
SNMPv3	authPriv	MD5 or SHA	CBC-DES (DES-56)

Syslog

- A variety of network components can send their log information to a common syslog server.
- By having log information for multiple devices in a common log, network administrators can better correlate events.
- Syslog-logging solution consists of two primary components:
 - Syslog server
 - Syslog clients



Sample Syslog Clients

Level	Name	Description
0	Emergencies	The most severe error conditions, which render the system unusable
1	Alerts	Conditions requiring immediate attention
2	Critical	A less severe condition, as compared to alerts, which should be addressed to prevent and interruption of service
3	Errors	Notifications about error conditions within the system, which do not render the system unusable
4	Warnings	Notifications that specific operations failed to complete successfully
5	Notifications	Non-errors notifications that alert an administrator about state changes within a system
6	Informational	Detailed information about the normal operation of a system
7	Debugging	Highly detailed information (for example, information about individual packets), which is typically used for troubleshooting

Names of Log Message
and Severity Levels

Time Stamps

Text of Syslog Messages

Date	Time	Priority	Hostname	Message
06-15-2011	16:02:48	Local7:Notice	192.168.1.11	74: *Aug 13 07:38:47.126: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 192.168.0.22 (FastEthernet0/1) is down: interface down
06-15-2011	18:02:48	Local7:Notice	192.168.1.11	73: *Aug 13 07:38:47.108: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
06-15-2011	17:30:42	Local7:Notice	192.168.1.11	72: *Aug 13 07:06:41.776: %SYS-5-CONFIG_I: Configured from console by console
06-15-2011	17:30:42	Local7:Notice	192.168.1.11	71: *Aug 13 07:06:40.814: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 192.168.0.22 (FastEthernet0/1) is up: summary configured
06-15-2011	17:02:11	Local7:Notice	192.168.1.11	70: *Aug 13 06:38:09.293: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 192.168.0.22 (FastEthernet0/1) is up: new adjacency
06-15-2011	17:01:52	Local7:Notice	192.168.1.11	69: *Aug 13 06:37:51.159: %SYS-5-CONFIG_I: Configured from console by console
06-15-2011	17:01:49	Local7:Notice	192.168.1.11	68: *Aug 13 06:37:47.954: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.2 on FastEthernet0/1 from FULL to DOWN, Neighbor Down: Interface down or detached
06-15-2011	17:01:49	Local7:Notice	192.168.1.11	67: *Aug 13 06:37:47.914: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.2 on OSPF_VL1 from FULL to DOWN, Neighbor Down: Interface down or detached
06-15-2011	16:52:38	Local7:Notice	192.168.1.11	66: *Aug 13 06:28:36.770: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.2 on OSPF_VL1 from LOADING to FULL, Loading Done
06-15-2011	16:52:29	Local7:Notice	192.168.1.11	65: *Aug 13 06:28:28.096: %SYS-5-CONFIG_I: Configured from console by console
06-15-2011	15:44:42	Local7:Alert	192.168.1.72	5: Jun 15 2011 19:48:33.938 UTC : %C_CALLMANAGER-1-SDLinkD0S: %([Local Node ID=2])(Local Application ID=100)[Remote Application IP Address=192.168.1.71][Remote Node ID=1][Remote Application ID=100][Unique Link ID=2:100:1:100][App ID=Cisco CallManager][Cluster ID=StandAloneCluster][Node ID=SUB-8]: SDLink to remote application is out of service
06-15-2011	15:44:38	Local7:Warning	192.168.1.11	64: *Aug 13 05:20:36.570: %OSPF-4-ERRRCV: Received invalid packet: mismatch area ID, from backbone area must be virtual-link but not found from 192.168.1.77, FastEthernet0/0
06-15-2011	15:44:28	Local7:Warning	192.168.1.11	63: *Aug 13 05:20:26.757: %OSPF-4-ERRRCV: Received invalid packet: mismatch area ID, from backbone area must be virtual-link but not found from 192.168.1.77, FastEthernet0/0
06-15-2011	15:44:18	Local7:Warning	192.168.1.11	62: *Aug 13 05:20:16.805: %OSPF-4-ERRRCV: Received invalid packet: mismatch area ID, from backbone area must be virtual-link but not found from 192.168.1.77, FastEthernet0/0
06-15-2011	15:44:09	Local7:Warning	192.168.1.11	61: *Aug 13 05:20:07.642: %OSPF-4-ERRRCV: Received invalid packet: mismatch area ID, from backbone area must be virtual-link but not found from 192.168.1.77, FastEthernet0/0
06-15-2011	15:44:00	Local7:Warning	192.168.1.11	60: *Aug 13 05:19:58.219: %OSPF-4-ERRRCV: Received invalid packet: mismatch area ID, from backbone area must be virtual-link but not found from 192.168.1.77, FastEthernet0/0
06-15-2011	15:43:50	Local7:Warning	192.168.1.11	59: *Aug 13 05:19:48.278: %OSPF-4-ERRRCV: Received invalid packet: mismatch area ID, from backbone area must be virtual-link but not found from 192.168.1.77, FastEthernet0/0
06-15-2011	15:43:40	Local7:Warning	192.168.1.11	58: *Aug 13 05:19:38.362: %OSPF-4-ERRRCV: Received invalid packet: mismatch area ID, from backbone area must be virtual-link but not found from 192.168.1.77, FastEthernet0/0
06-15-2011	15:43:30	Local7:Warning	192.168.1.11	57: *Aug 13 05:19:28.482: %OSPF-4-ERRRCV: Received invalid packet: mismatch area ID, from backbone area must be virtual-link but not found from 192.168.1.77, FastEthernet0/0
06-15-2011	15:43:29	Local7:Notice	192.168.1.11	56: *Aug 13 05:19:28.005: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.2 on FastEthernet0/1 from LOADING to FULL, Loading Done
06-15-2011	15:43:20	Local7:Warning	192.168.1.11	55: *Aug 13 05:19:18.846: %OSPF-4-ERRRCV: Received invalid packet: mismatch area ID, from backbone area must be virtual-link but not found from 192.168.1.77, FastEthernet0/0
06-15-2011	15:43:11	Local7:Warning	192.168.1.11	54: *Aug 13 05:19:09.547: %OSPF-4-ERRRCV: Received invalid packet: mismatch area ID, from backbone area must be virtual-link but not found from 192.168.1.77, FastEthernet0/0

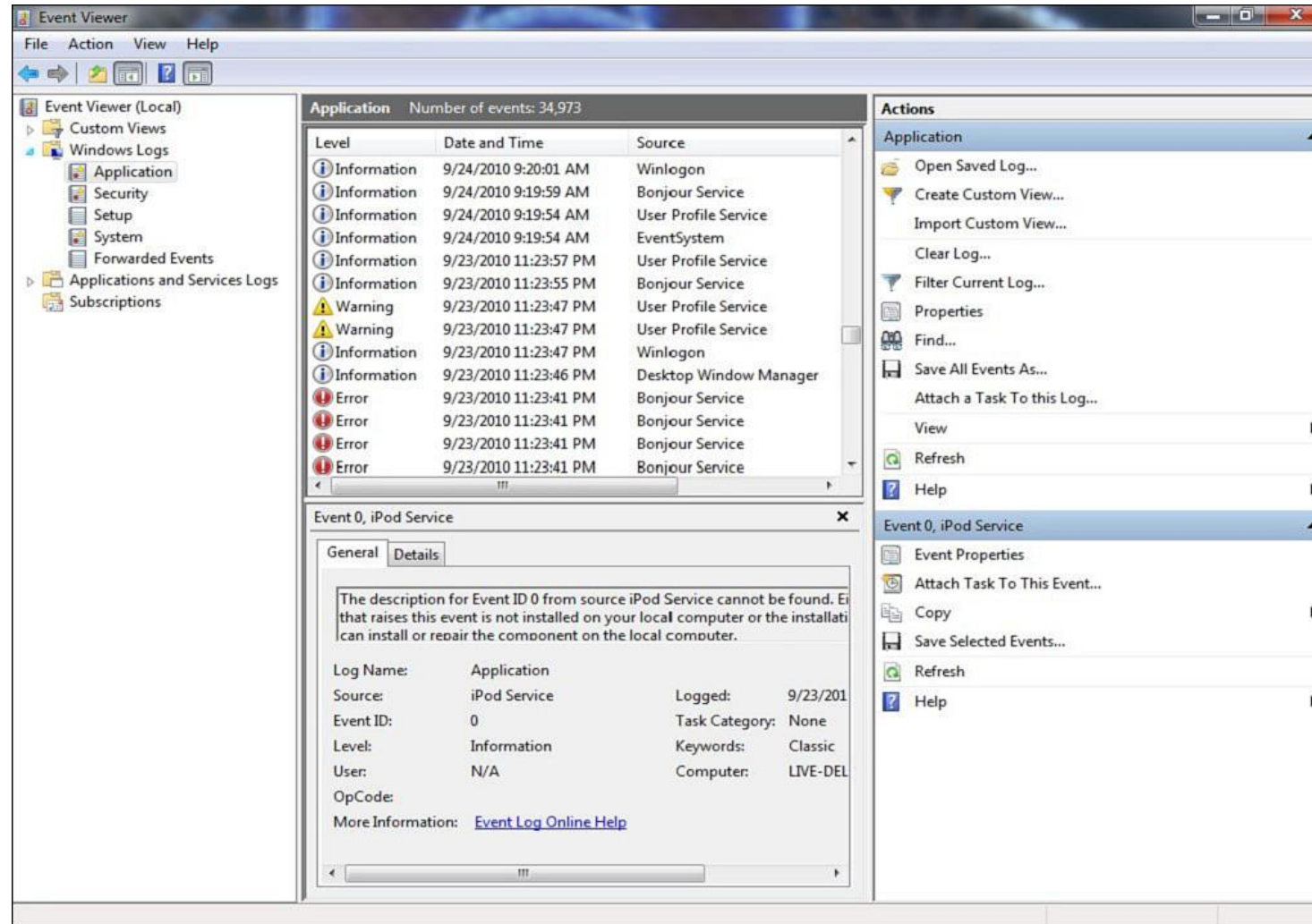
Structure of a Syslog Message

Logs

- In addition to logs generated by routers, switches, and other infrastructure gear, the operating systems powering network clients and servers generally have the capability to produce log outputs.
- Microsoft Windows incorporates an Event Viewer application that allows you to view the following logs;
 - Application
 - Security
 - System

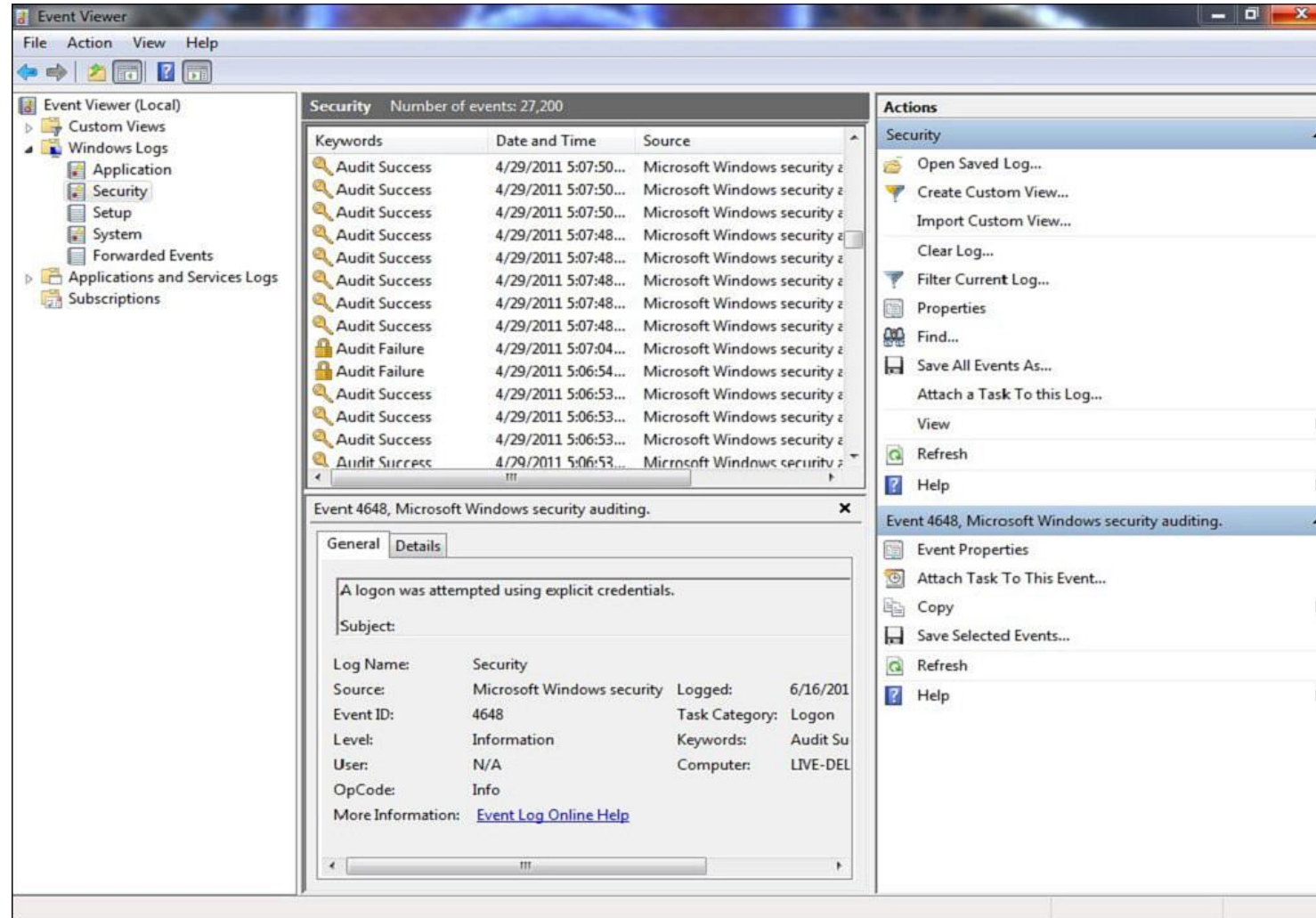


Application Log



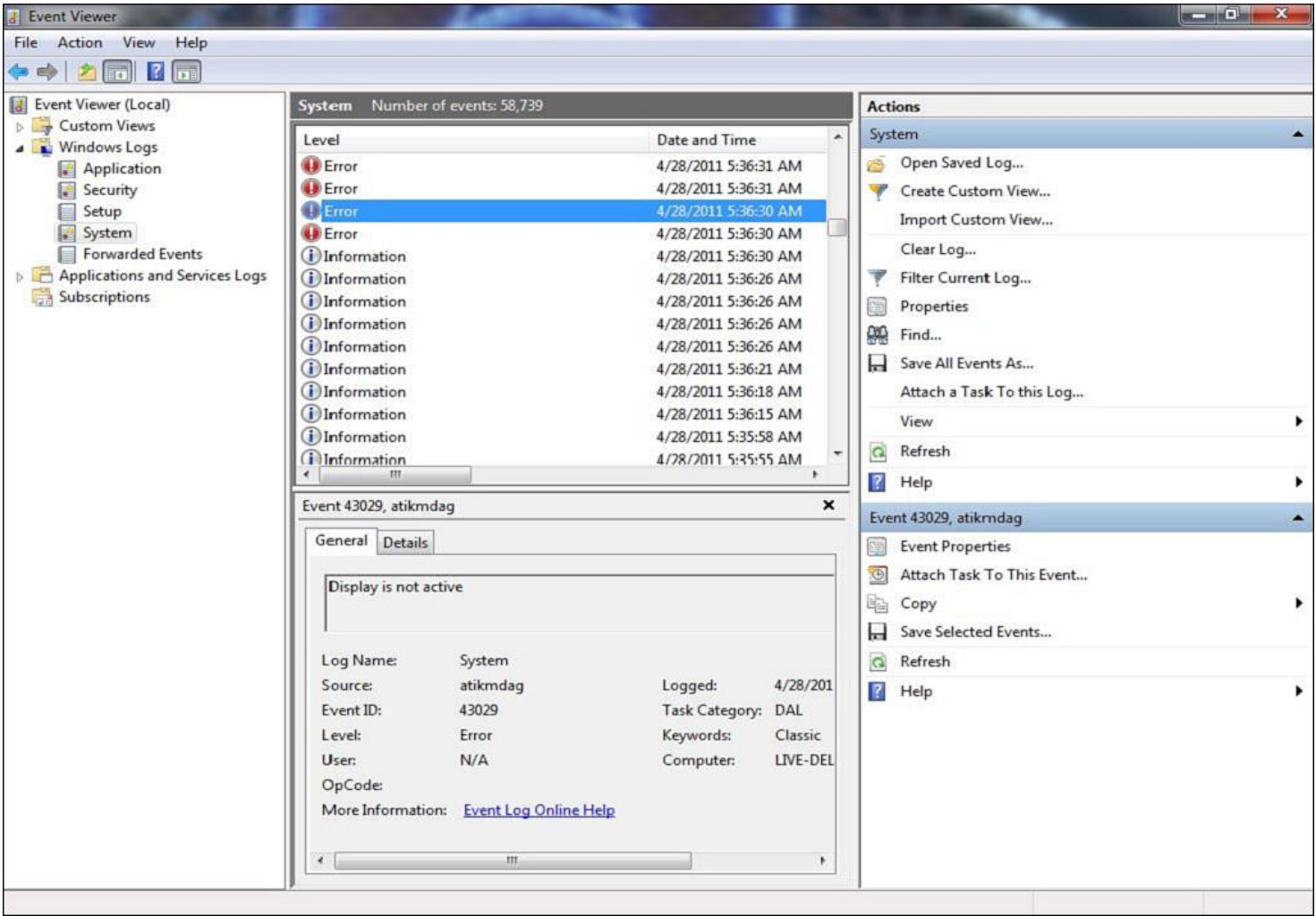
Application Log

Security Log



Security Log

System Log



System Log

Securing a Network

Objectives

- What are the goals of network security, and what sorts of attacks do you need to defend against?
- What best practices can be implemented to defend against security threats?
- What are the characteristics of various remote-access security technologies?
- How can firewalls be used to protect an organization's internal network, while allowing connectivity to an untrusted network, such as the Internet?
- How can virtual private networks (VPN) be used to secure traffic as that traffic flows over an untrusted network?
- What is the difference between intrusion prevention and intrusion detection systems, and how do they protect an organization from common security threats?

Securing a Network

- Today's networks are increasingly dependent on connectivity with other networks.
- However, connecting an organization's trusted network to untrusted network's such as the Internet, introduces security risks.
- To protect your organization's data from malicious users, you need to understand the types of threats against which you might have to defend.



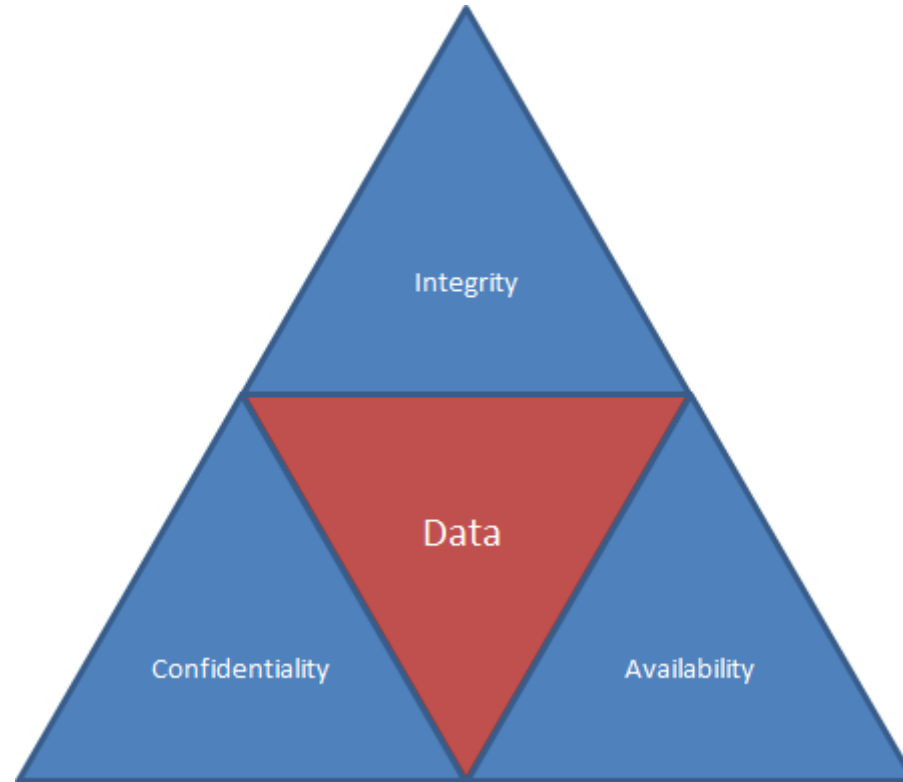
Security Fundamentals

- For most of today's corporate networks, the demands of e-commerce and customer contact require connectivity between internal corporate networks and the outside world.
- All networks require network security



Three Primary Goals of Network Security

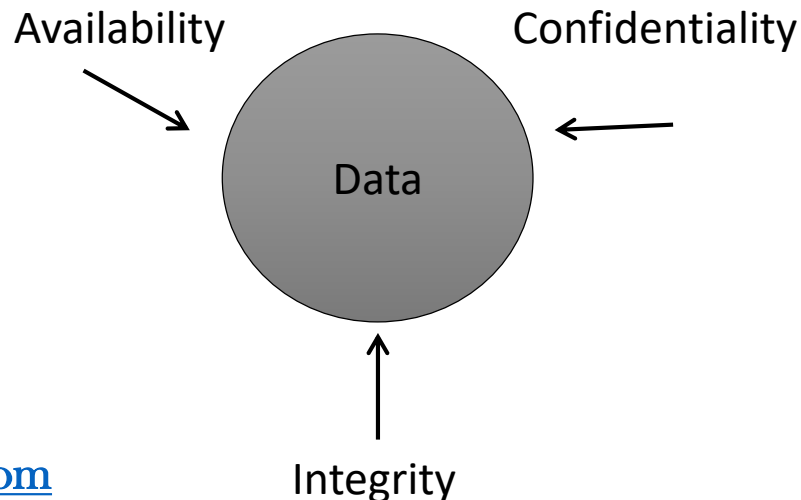
- Confidentiality – keeping the data private
- Integrity – ensures that data has not been modified
- Availability – the data is accessible when needed



Security Fundamentals

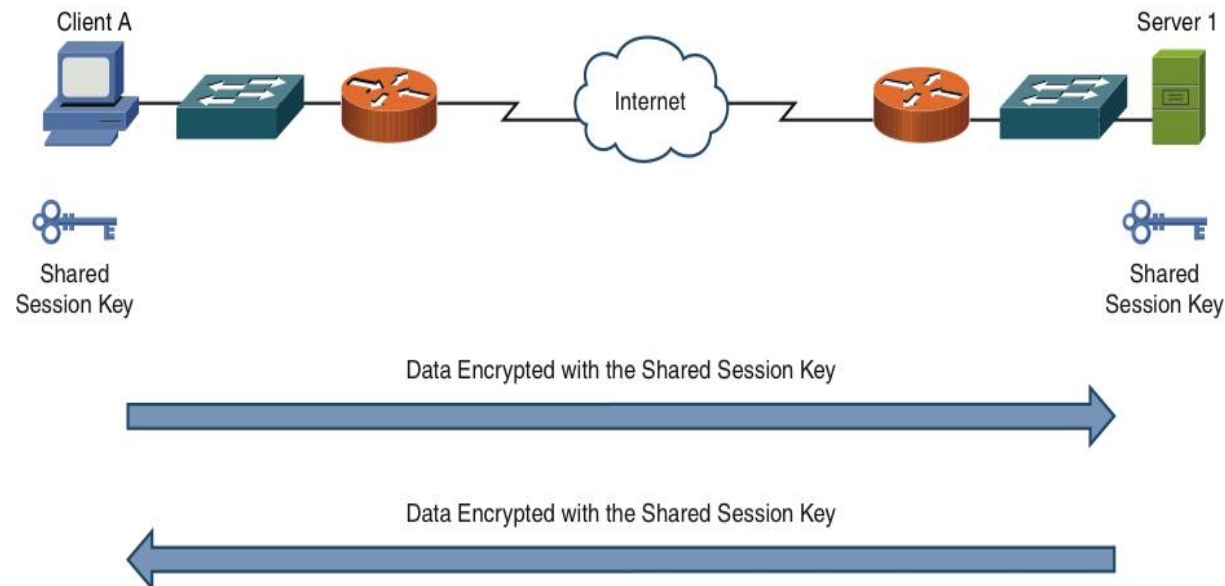
- Confidentiality can be provided by encryption.
- Encryption has two basic forms:
 - Symmetric encryption -- implies that the same key is used by both the sender and receiver to encrypt and decrypt a packet.
 - DES is an old, insecure protocol
 - 3DES and AES are much better
- Asymmetric encryption -- uses different keys for the sender and receiver of a packet
 - RSA is the most common system, used by HTTPS

C I A

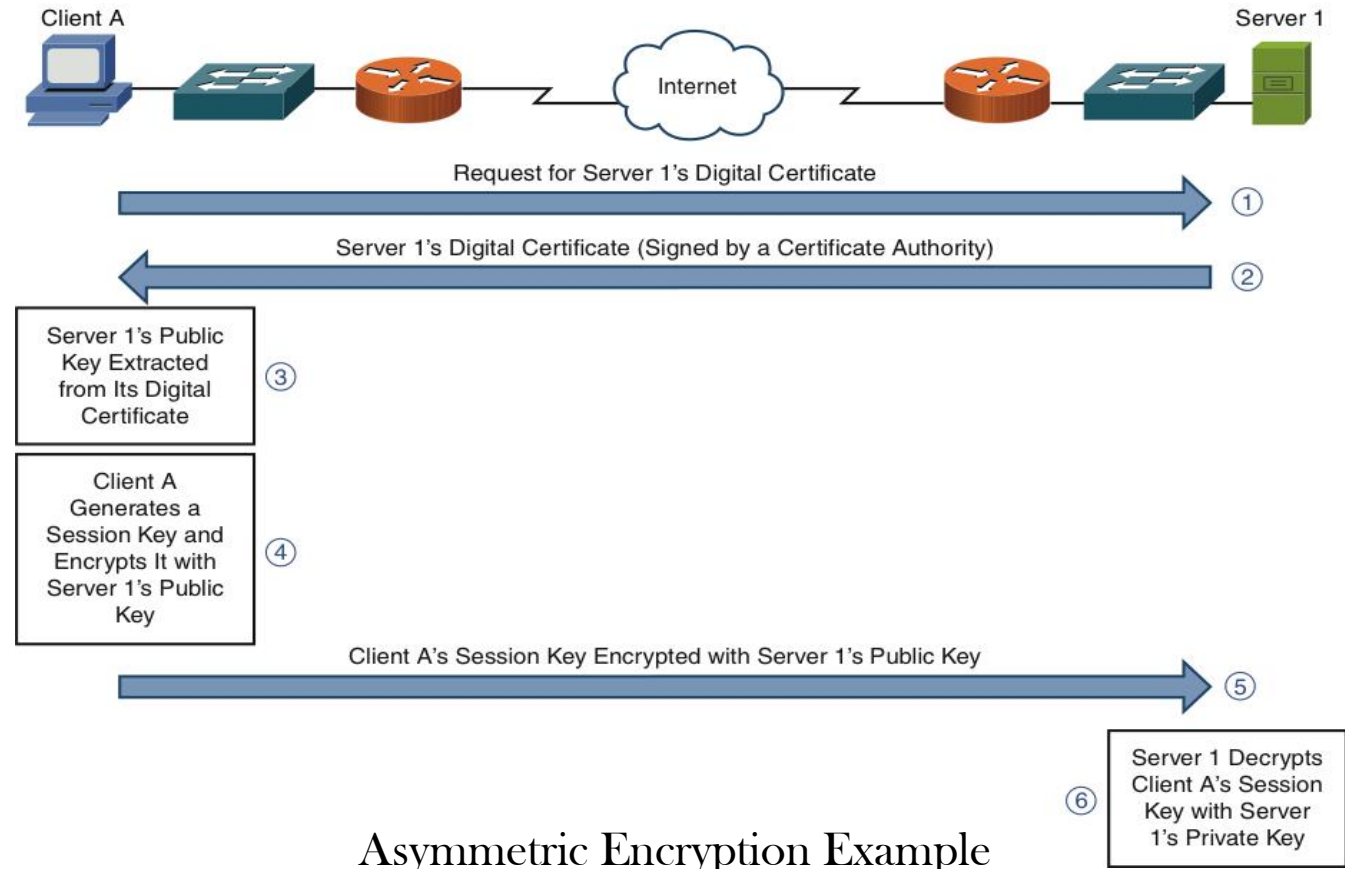


Security Fundamentals

- Integrity can be provided by hashing
- Hash value is like a fingerprint of the data
- Any alteration in data changes the hash
- Ethernet uses CRC32 to detect transmission errors
- MD5 is an old, insecure hash function
- SHA-1, SHA-2, and SHA-3 are newer and more secure
- Availability can be provided by fault tolerance
- Attacks on availability are called Denial of Service (DoS) attacks
- A DoS attack from many machines is called a Distributed Denial of Service (DDoS) attack



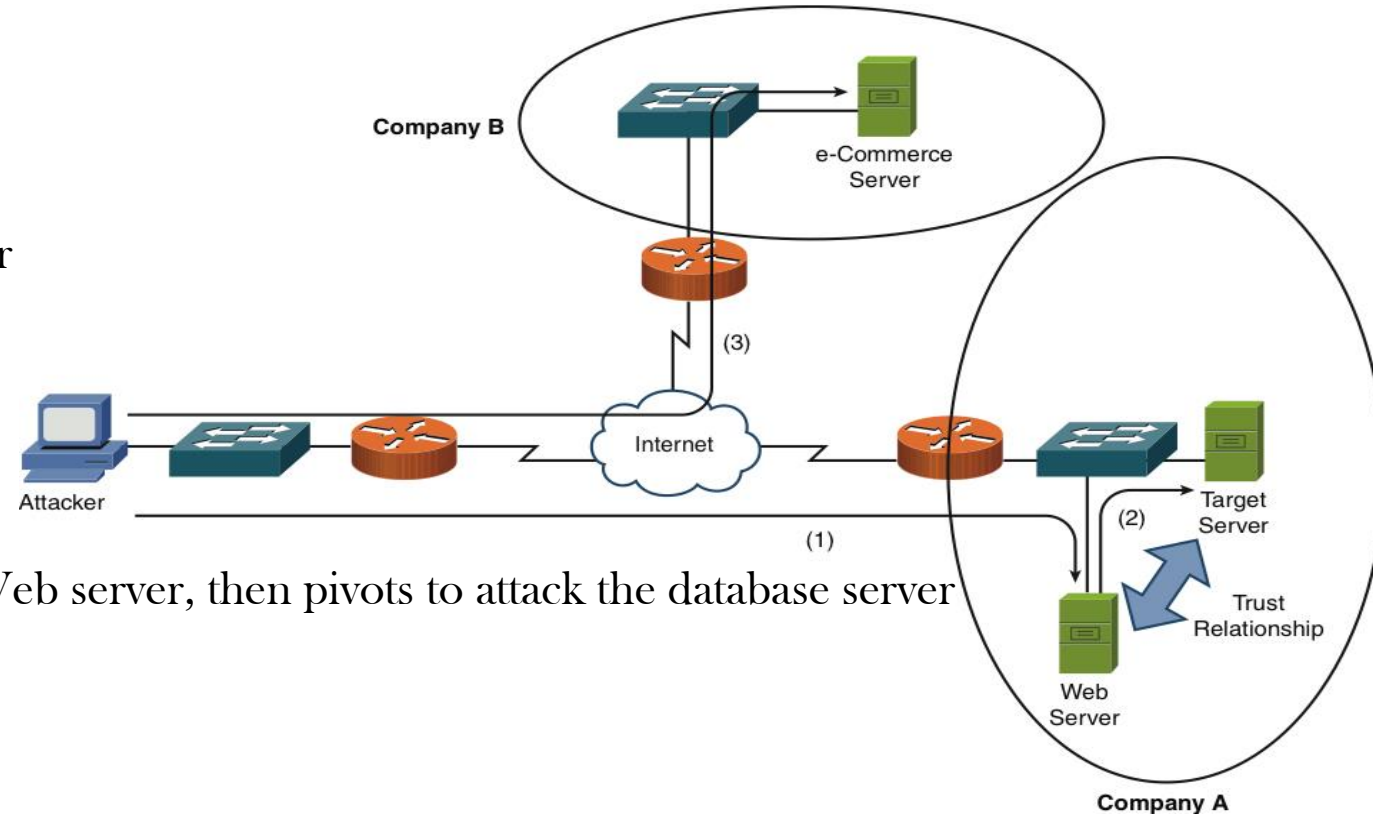
Security Fundamentals



Asymmetric Encryption Example

Security Fundamentals

- Categories of Network Attacks
 - Confidentiality Attacks
 - Makes confidential data visible to an attacker
 - Integrity Attacks
 - Alters data in transit or at rest
 - Availability Attacks
 - Makes system unavailable to authorized users

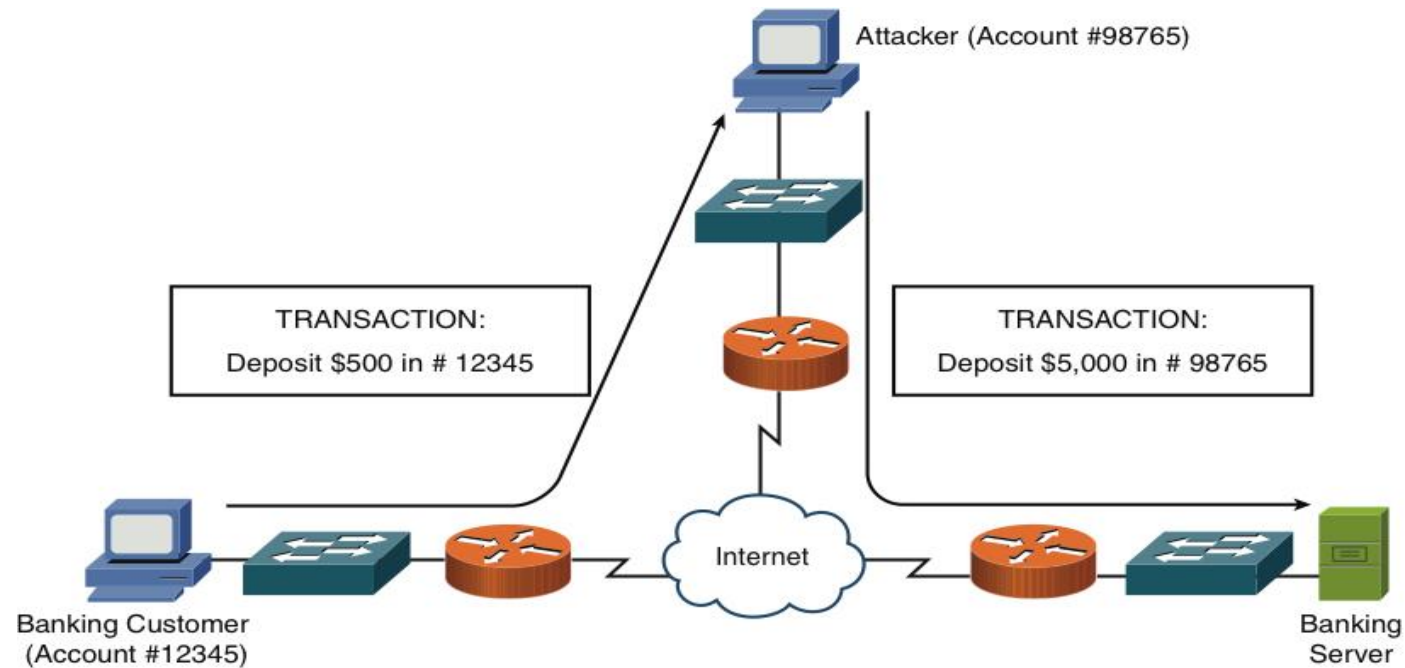


Confidentiality Attack Example Attacker compromises the Web server, then pivots to attack the database server

- Attack techniques
 - Packet capture
 - Ping sweep and port scan
 - Dumpster diving
 - Electromagnetic emanations
 - Wiretapping telephone lines
 - Social engineering
 - Steganography
 - Covert channels
 - Bouncing attack

Protocol Analyzer

- Integrity Attack

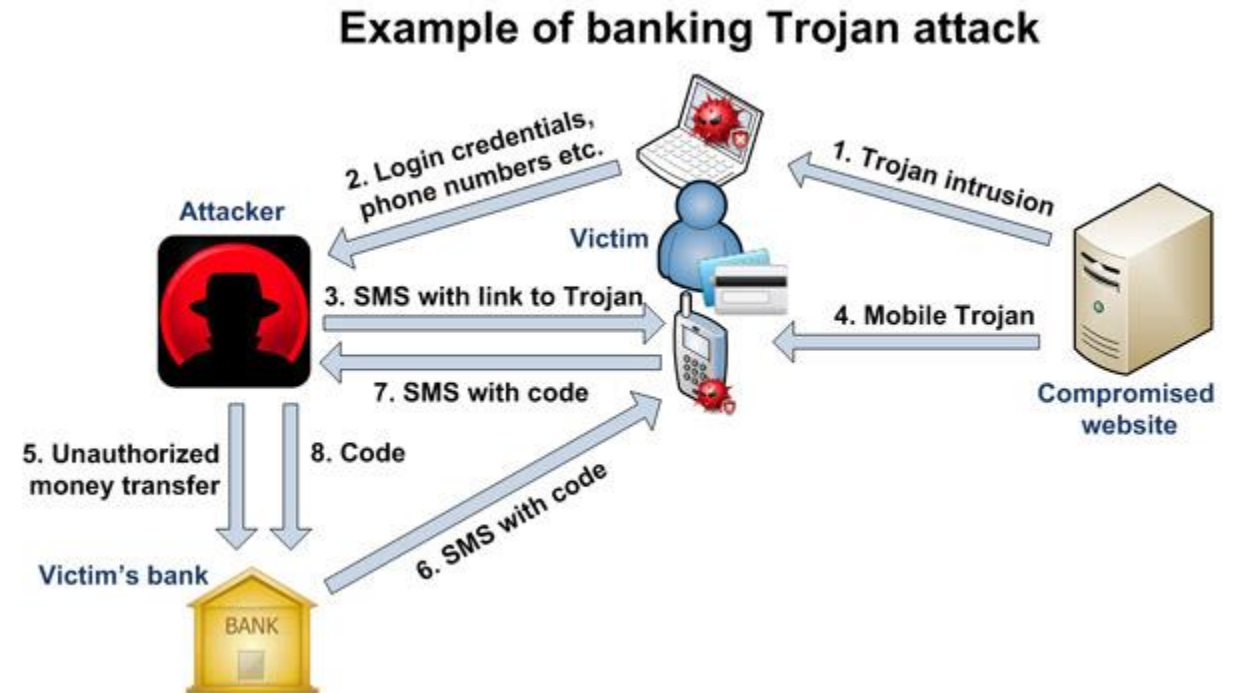


Traffic diverted to attacker due to a man-in-the-middle attack

Security Fundamentals

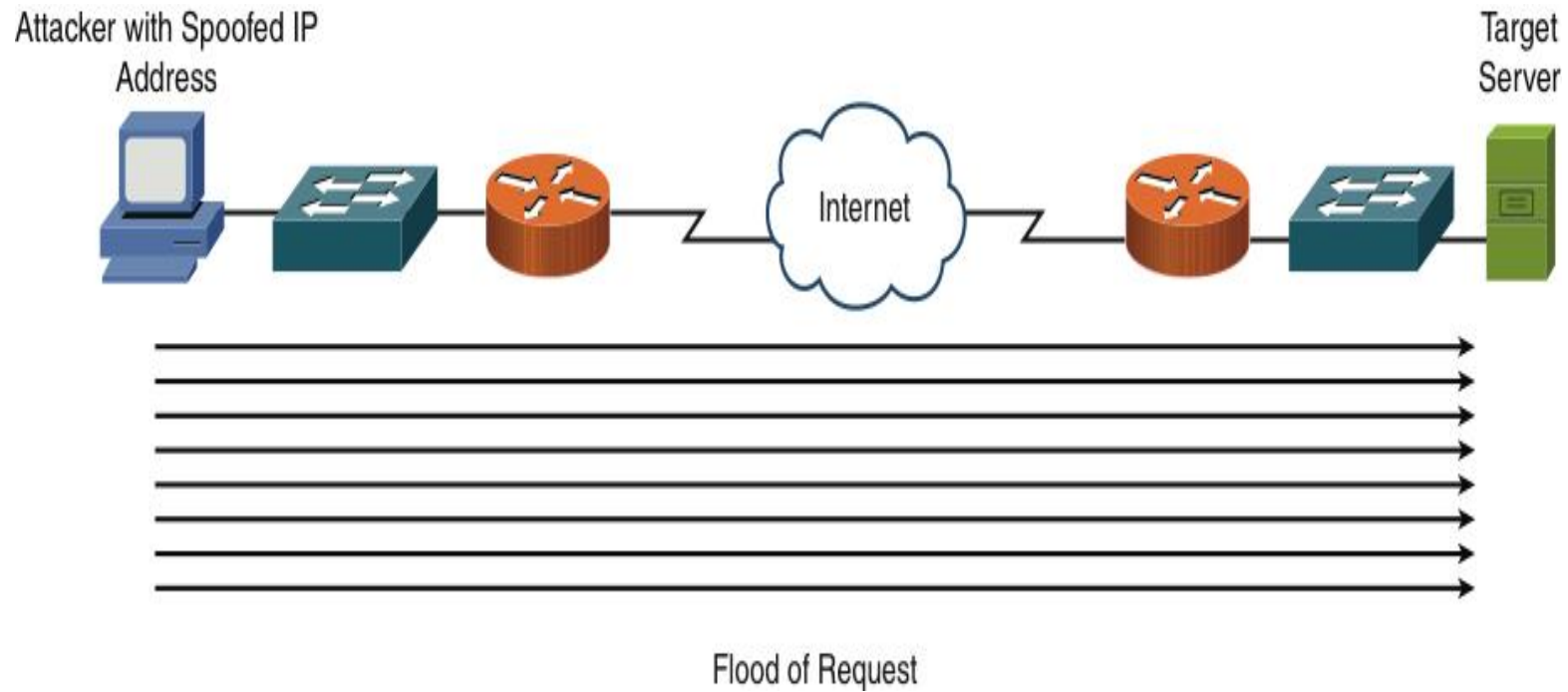
- Integrity Attack Methods

- Salami attack (many small alterations)
- Data diddling (changes data before it is stored)
- Virus (attached to an EXE file)
- Worm (travels through a network)
- Trojan (masquerades as innocent software)
- Trust relationship exploitation
- Botnet
- Session hijacking
- Password attacks
 - Keylogger (steal keypresses)
 - Packet capture
 - Brute force (guess all possible passwords)
 - Dictionary (try passwords from a dictionary)



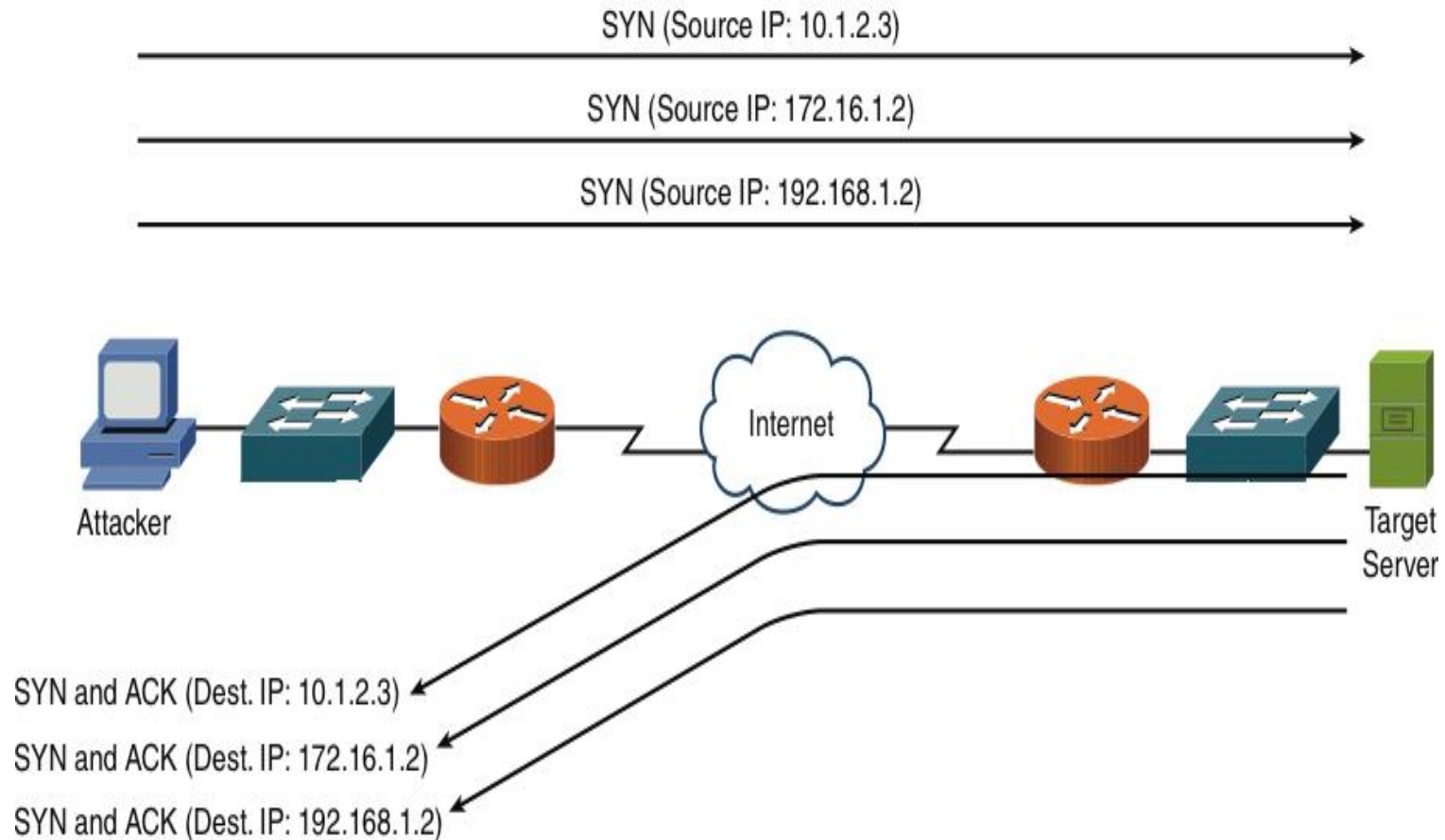
Security Fundamentals

- DoS Attack



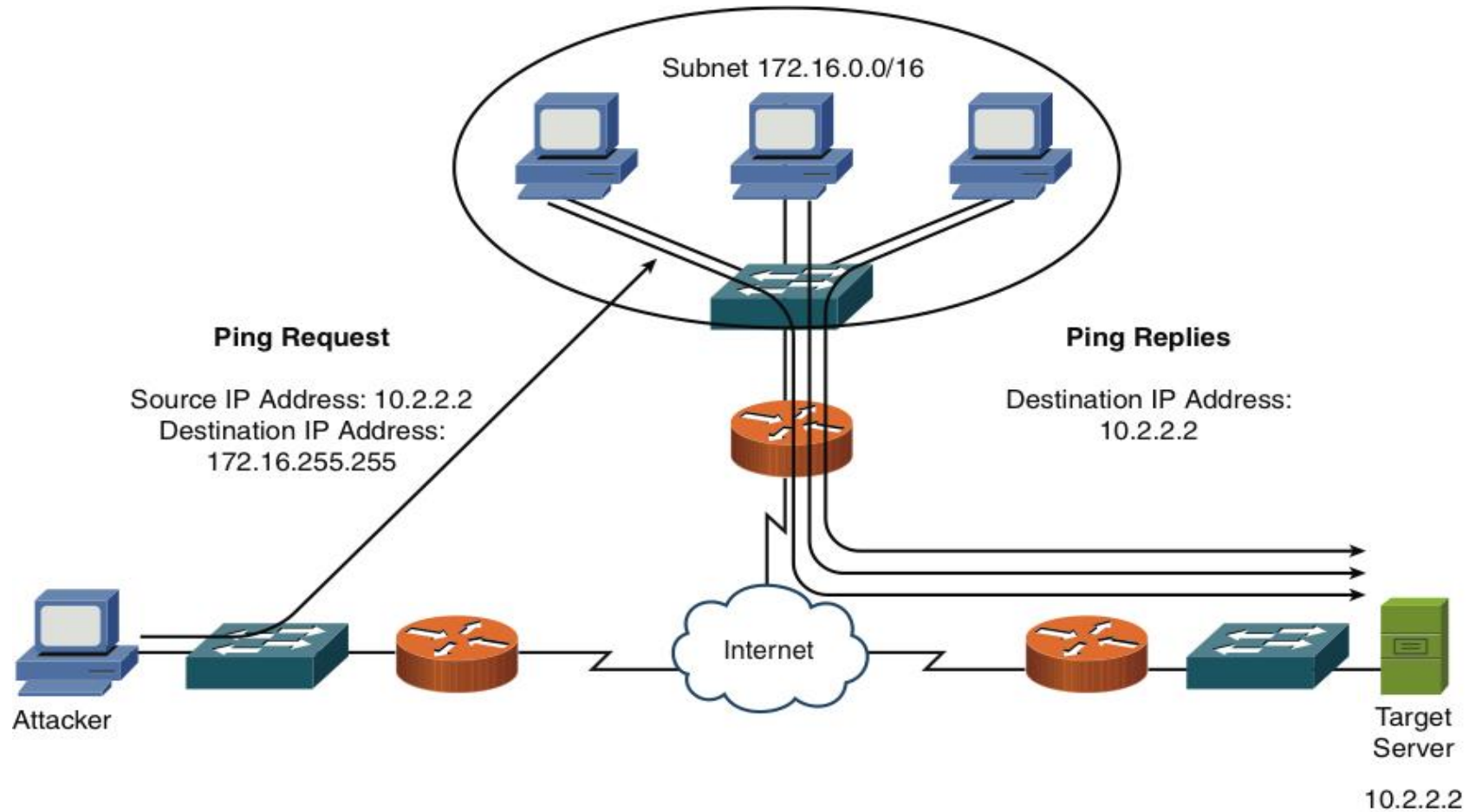
Security Fundamentals

- TCP SYN Flood Attack Example



Security Fundamentals

- Smurf Attack Example



Security Fundamentals

- **Availability Attacks**
 - DoS
 - DDoS
 - SYN flood
 - Buffer overflow
 - ICMP flood (Smurf attack)
- **Electrical Disturbances**
 - At a physical level, an attacker could launch an availability attack by interrupting or interfering with electrical service available to a system, such as the following:
 - Power Spikes
 - Electrical surges
 - Power faults
 - Blackouts
 - Power sag
 - Brownout
 - To combat these threats, you might want to install uninterruptable power supplies (UPS) and generator backup for strategic devices in your network.

Security Fundamentals

- Attacks on a System's Physical Environment
 - Attackers could also intentionally damage computing equipment by influencing the equipment's physical environment.
 - Temperature
 - Humidity
 - Gas
- Consider the following recommendations to mitigate such environmental threats:
 - Computing facilities should be locked.
 - Access should require access credentials
 - Access point should be visually monitored.
 - Climate control system should be monitored.
 - Fire detection and suppression systems should not do damage to computer equipment if possible.

Defending Against Attacks

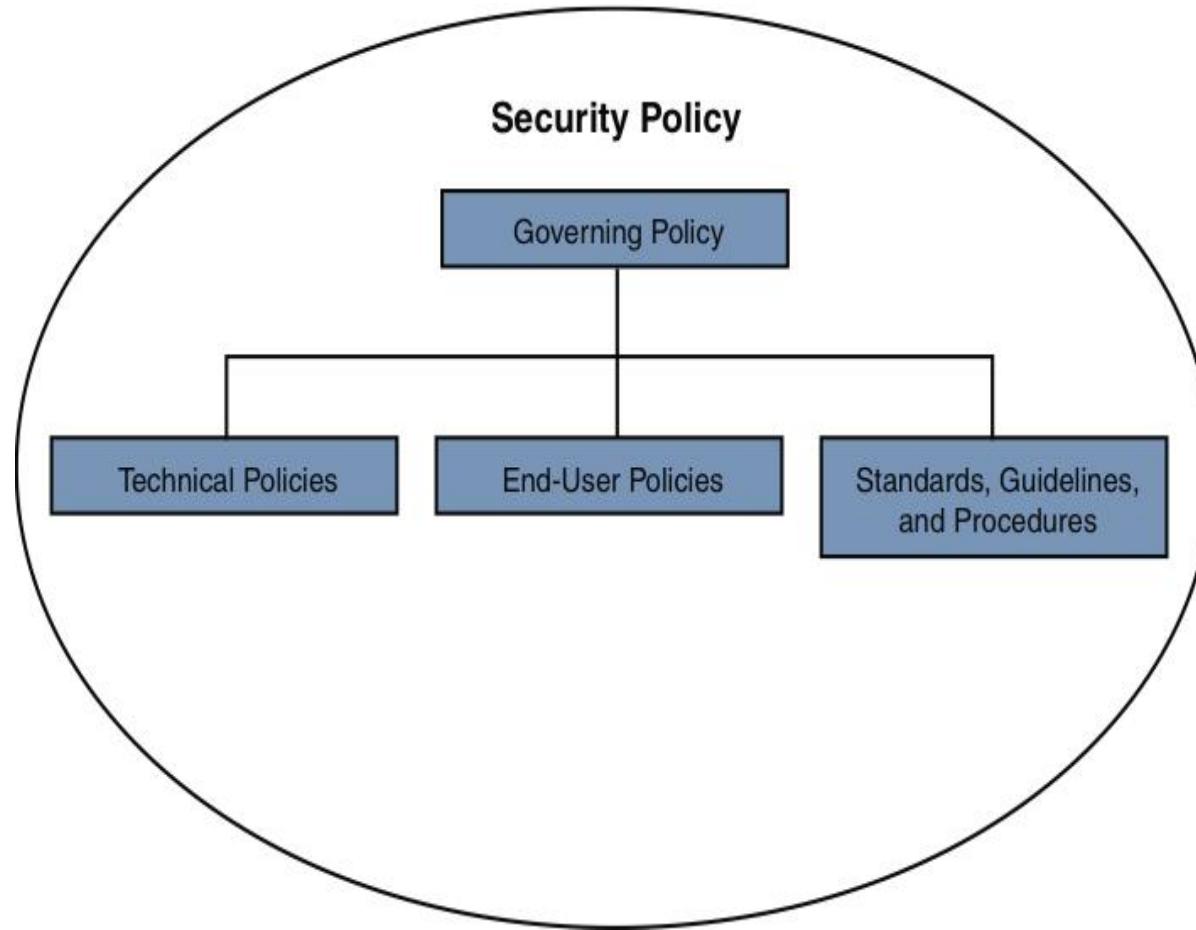
- Now that we have an understanding of security fundamentals, it is now time to talk about how to defend against security threats using network devices.
- **User Training**
 - Many attacks require user intervention in order to be carried out.
 - For example a user needs to execute an application containing a virus before the virus takes any actions.
 - Similarly, social engineering requires a user to give sensitive information to an attacker in order for the attacker to access the user's account.
- **User Training (cont.)**
 - As a result, several potential attacks can be thwarted through effective user training.
 - As a few examples, users could be trained on using policies such as the following:
 - Never give your password to anyone, even if they claim to be from IT.
 - Do not open e-mail attachments from unknown sources.
 - Select strong passwords, consisting of at least eight characters and containing a mixture of alphabetical (upper- and lowercase), numeric, and special characters.
 - Change your password monthly (or more often)

Defending Against Attacks

- **Patching**
 - Some attacks are directed at vulnerabilities known to exist in various OSs and applications.
- As these are discovered, the vendors of the OSs, or application often respond by releasing a **patch**.
 - A patch is designed to correct a known bug or fix a known vulnerability in a piece of software
- A network administrator should have a plan for implementing patches as they become available.
- **Security Policies**
 - One of the main reasons security breaches occur within an organization is the lack of a security policy or, if a security policy is in place, the lack of effectively communicating/enforcing that security policies to all concerned.
 - A security policy is a continually changing document that dictates a set of guidelines for network use.
 - The main purpose of a security policy is to protect the asset of an organization.
 - Asset – intellectual property, processes and procedures, sensitive customer data, and specific server functions.

Defending Against Attacks

- Components of a Security Policy



Security Fundamentals

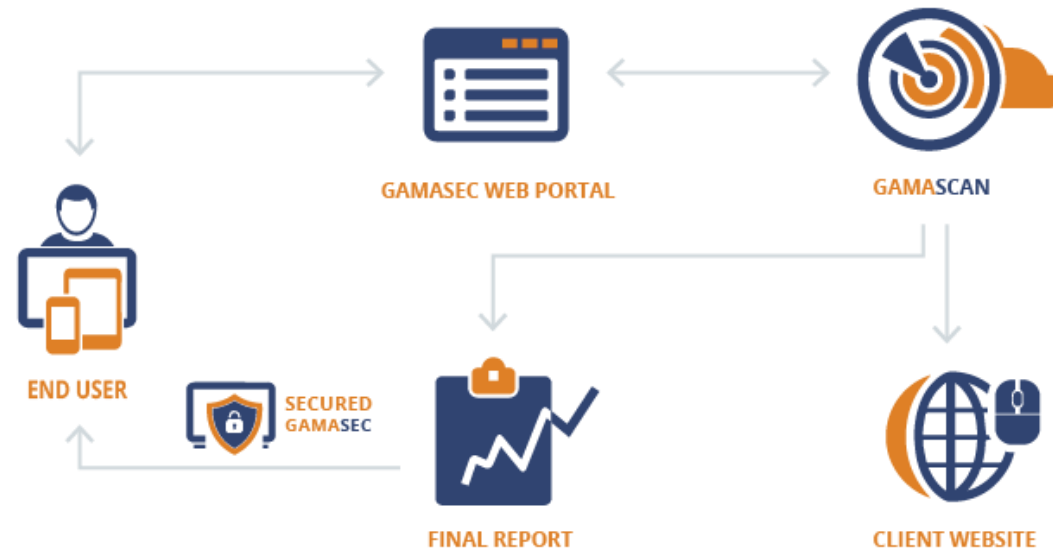
- **Incident Response**
 - Everyone will get hacked
 - Respond effectively
 - Contain damage
 - Reverse harm
 - Improve security to prevent repeated attack



Defending Against Attacks

- **Vulnerability Scanners**

- After you deploy your network-security solution, components of that solution might not behave as expected.
- Additionally, you might not be aware of some of the vulnerabilities in your network devices.
- You should periodically test your network for weakness.
- These test can be performed using application designed to check for a variety of known weakness.
- These application are known as vulnerability scanners.
 - Nessus is a full vulnerability scanner
 - Nmap (actually just a port scanner, not a full **vulnerability scanner**)



Defending Against Attacks

- Nessus

Nessus - Mozilla Firefox

File Edit View History Bookmarks Tools Help

localhost https://localhost:8834/

Tenable Nessus | Tenable Network ... Sample Reports | Tenable Network ... Nessus

kevin | Help | About | Log out

Reports Reports Scans Policies Users

Report Info

Hosts

- 192.168.1.1
- 192.168.1.3
- 192.168.1.50

Download Report

Show Filters

Reset Filters

Active Filters

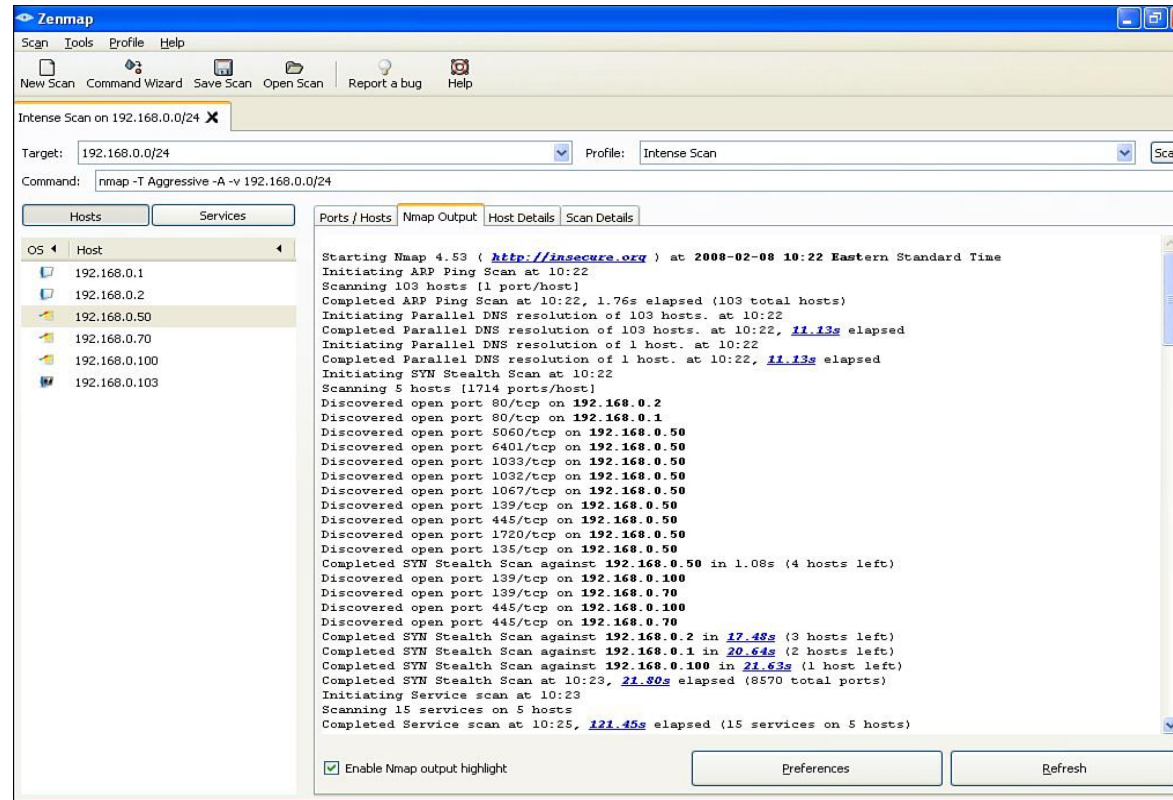
Demo 192.168.1.1 20 results

Port	Protocol	SVC Name	Total	High	Medium	Low	Open Port
53	tcp	domain?	1	0	0	0	1
67	udp	bootps?	1	0	0	0	1
68	udp	bootpc?	1	0	0	0	1
137	udp	netbios-ns	2	0	0	1	1
138	udp	netbios-dgm?	1	0	0	0	1
139	tcp	smb	2	0	0	1	1
161	udp	snmp	2	0	0	1	1
192	udp	osu-nms?	1	0	0	0	1
445	tcp	cifs	5	0	0	4	1
514	udp	syslog?	1	0	0	0	1
548	tcp	afpovertcp?	1	0	0	0	1
922	udp	unknown	1	0	0	0	1
923	udp	unknown	1	0	0	0	1
5009	tcp	ultima-online-ga	1	0	0	0	1
5351	udp	nat-pmp?	1	0	0	0	1
5353	udp	mdns?	1	0	0	0	1
10000	tcp	ndmp?	1	0	0	0	1
49624	udp	unknown	1	0	0	0	1
57006	udp	unknown	1	0	0	0	1

Transferring data from localhost...

Defending Against Attacks

- Nmap

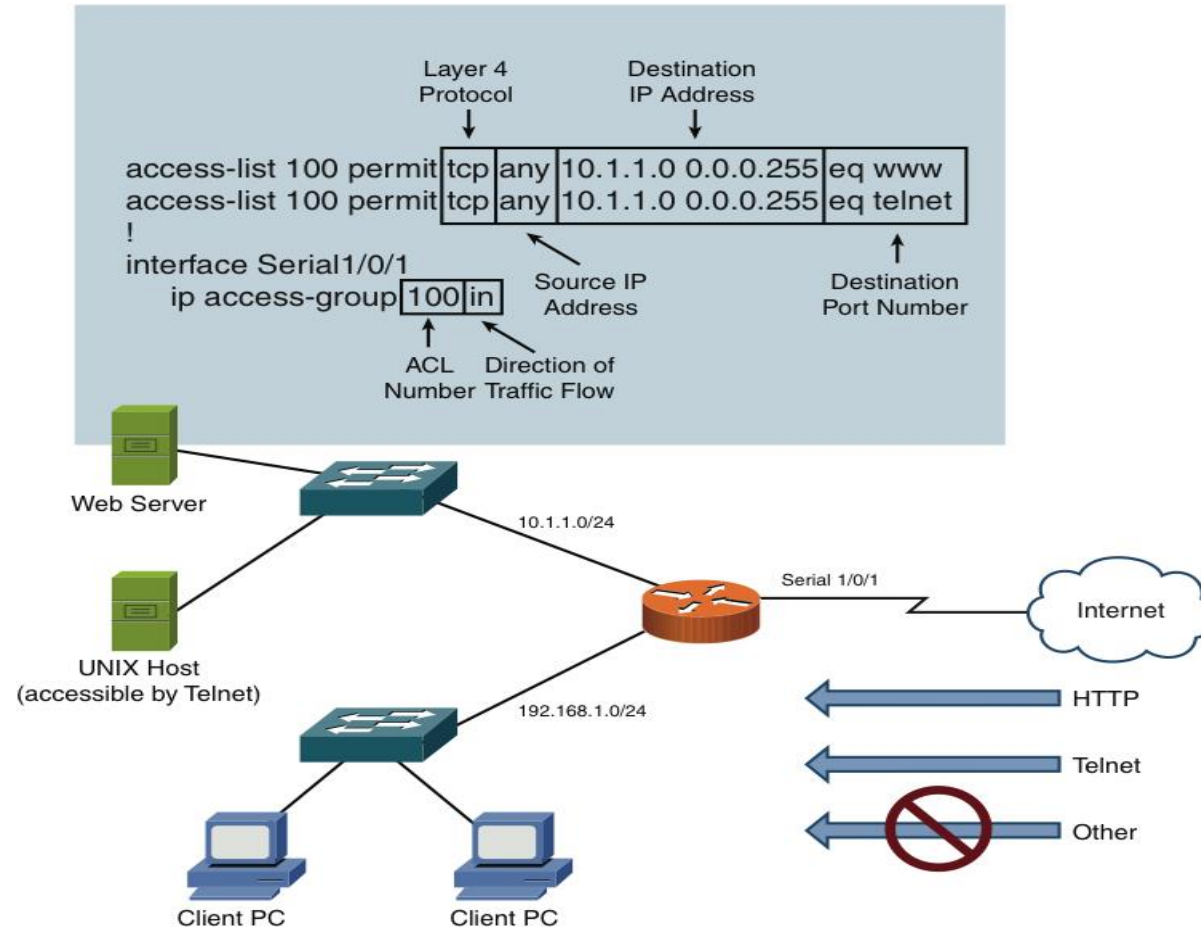


Defending Against Attacks

- Honey Pots and Honey Nets
 - A honey pot acts as a distracter. Specifically, a system designated as a honey pot appears to be an attractive target.
- The attacker then use their resources attacking the honey pot, the end result of which is the they leave the real servers alone.
 - honey pot -- signal machine that draws they attacker attention.
 - Honey net -- multiple machines that draw the attacker attention.
- A honey pot/net can also be used to study how attackers conduct their attacks.
- Access Control List (ACL)
 - ACLs are rules, typically applied to router interfaces, that specify permit or deny traffic.
- ACL's filtering criteria:
 - Source IP
 - Destination IP
 - Source Port
 - Destination Port
 - Source MAC
 - Destination MAC

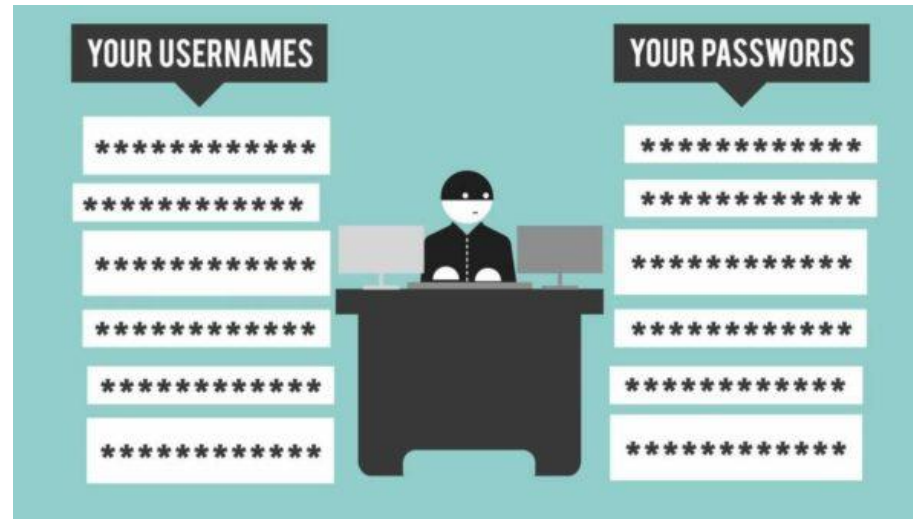
Defending Against Attacks

- ACL Example



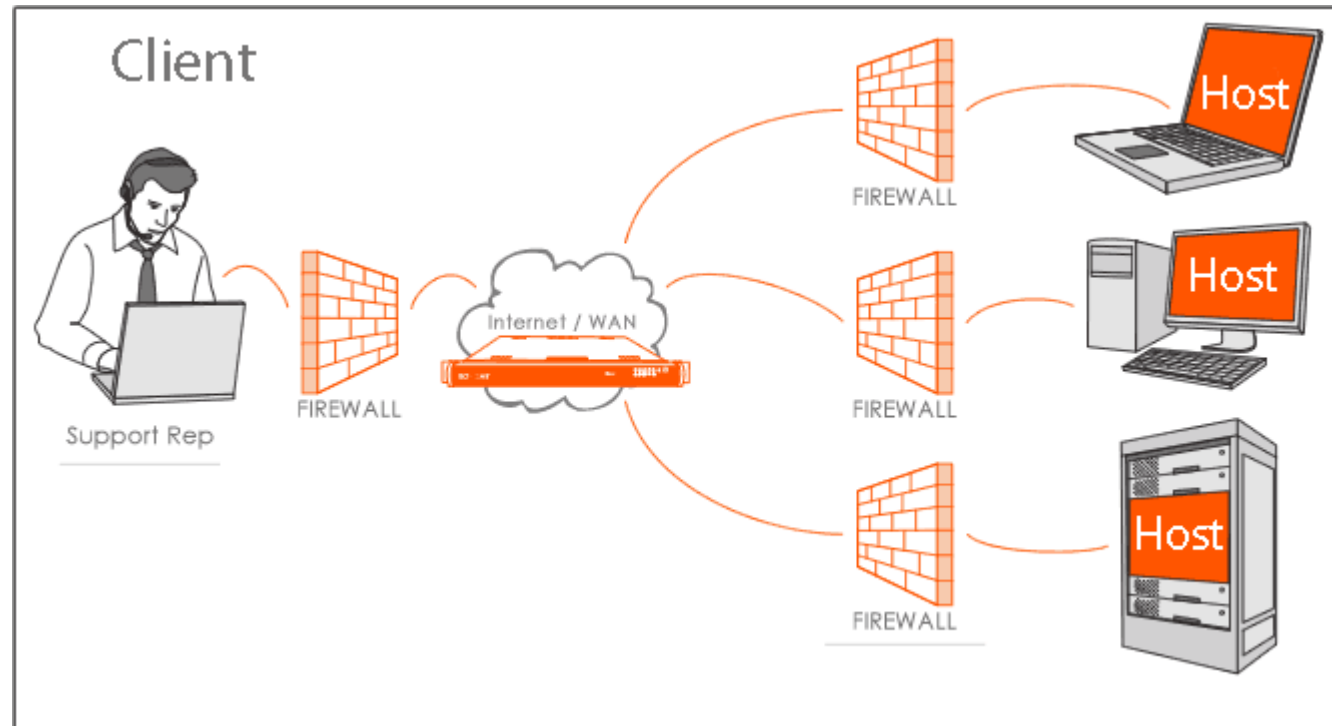
Defending Against Attacks

- Remote Access Security
- Although ACLs can be used to permit or deny specific connections flowing through a router, you also need to control connections to network devices.
- Many of these remote-access security methods have been introduced in preceding chapters



Remote Access Security Methods

- RAS
- RDP
- PPPoE
- PPP
- SSH
- Kerberos
- AAA
- RADIUS
- TACACS+
- NAC
- 802.1x
- CHAP
- MS-CHAP
- EAP
- Two-factor authentication
- Single sign-on

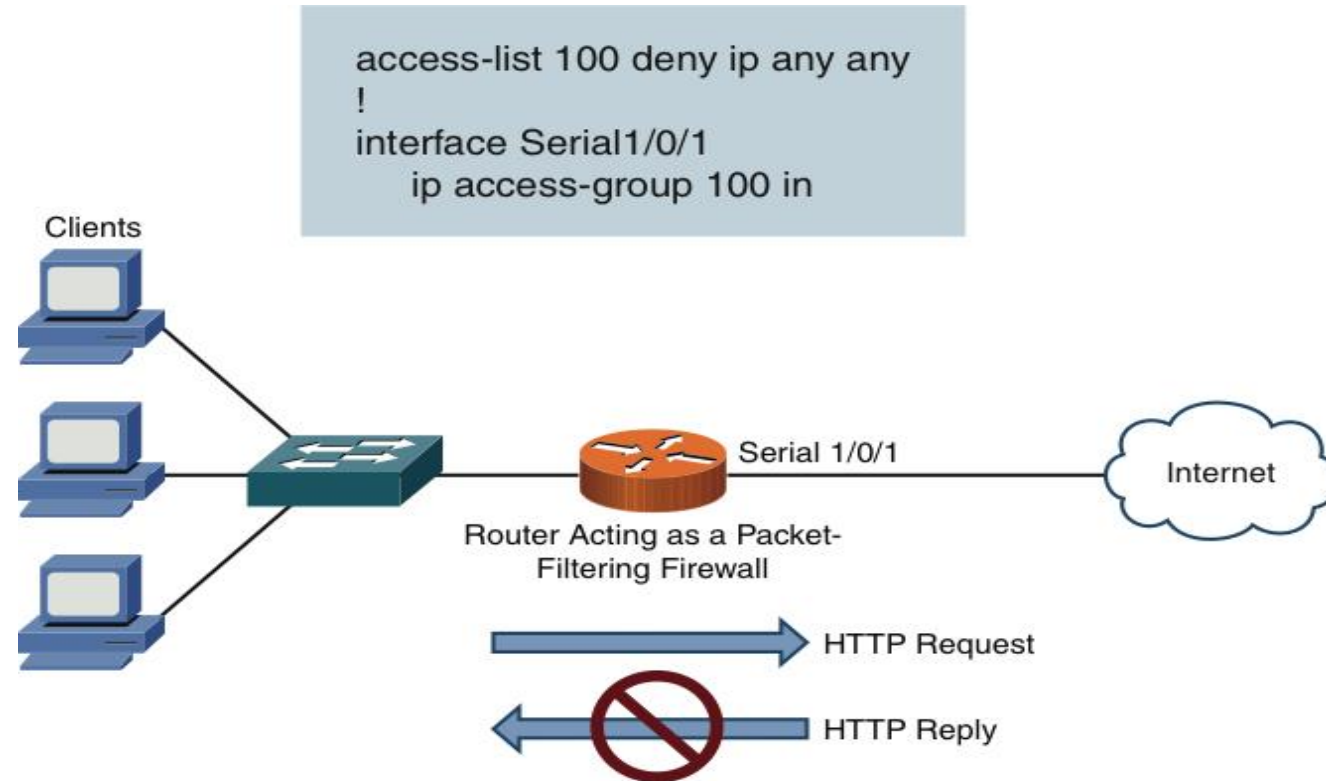


Defending Against Attacks

- Firewalls
 - At this point, we have introduced various security threats, along with best practices to protect your network from those threats.
 - Now we are going to cover three additional layers of security that can be applied to a network.
- The additional layers consist of **firewalls, virtual private networks**, and **intrusion detection and prevention systems**.
- Firewall Types
 - A firewall defines a set of rules to dictate which types of traffic are permitted or denied as that traffic enters or exits a firewall interface.
 - **Software firewall** -- can be used to protect a single system or can be software loaded in a computer with more than one NIC, controlling traffic between them.
 - **Hardware firewall** - is an appliance that acts as the firewall.
- Firewall Inspection Types
 - **Packet-filtering firewall** (stateless) -- inspect traffic solely on a packet's header. One at a time.
 - **Stateful firewall** - recognize that a packet is part of a session that might have originated inside the LAN or outside the LAN

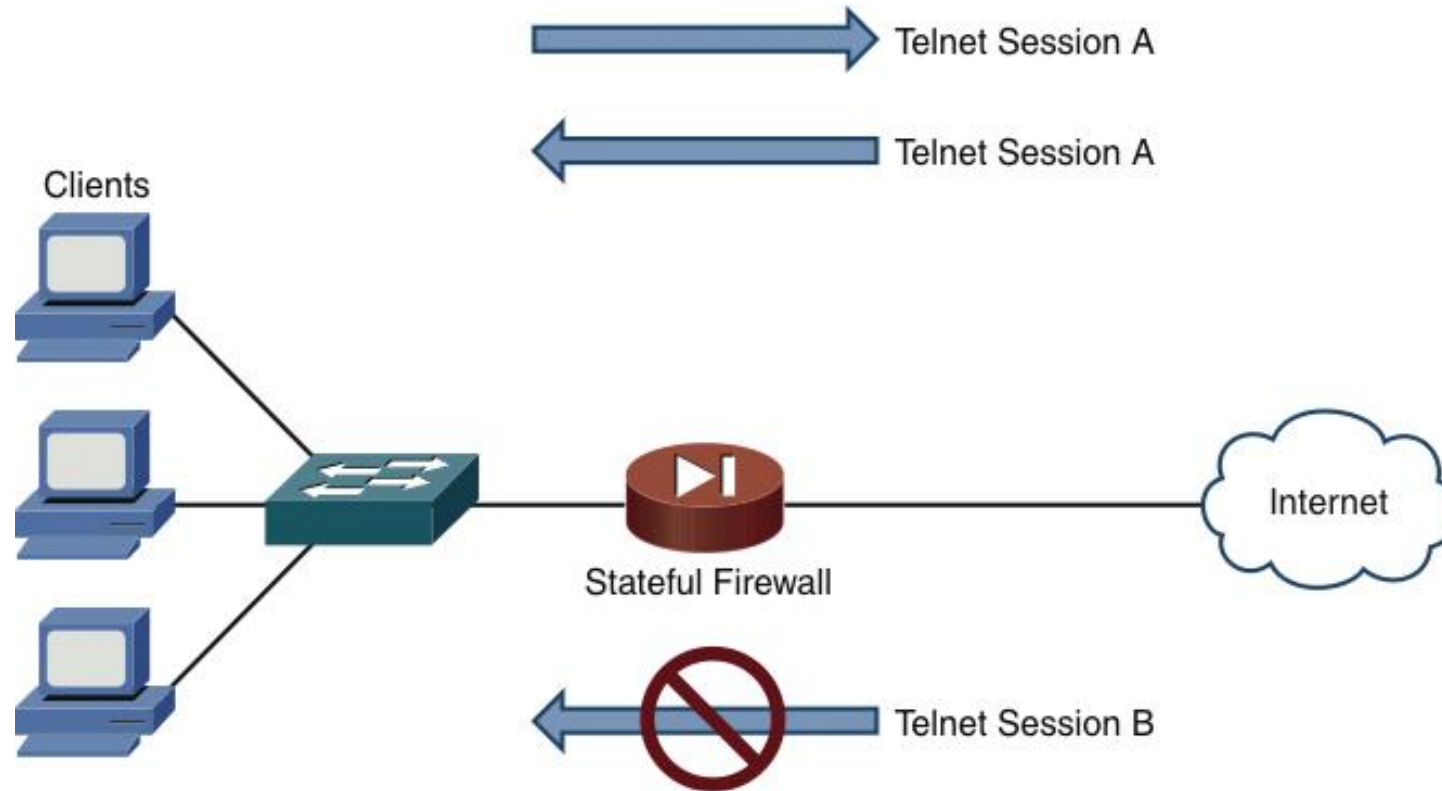
Defending Against Attacks

- Packet-Filtering Firewall



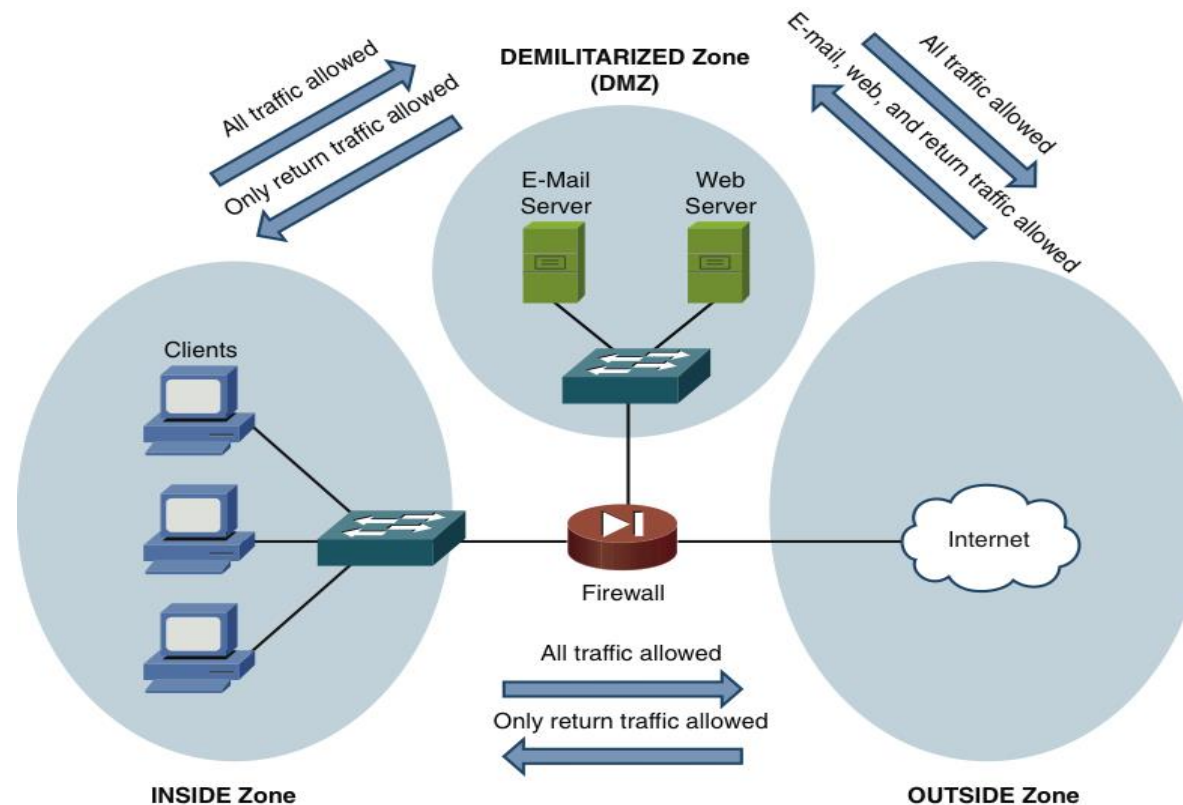
Defending Against Attacks

- Stateful Firewall



Defending Against Attacks

- Firewall Zones
 - A firewall's interface can be defined as belonging to different **firewall zones**.
 - After the zones are created, you then set up rules based on those zones.
- Typical zones names:
 - Inside
 - Outside
 - DMZ



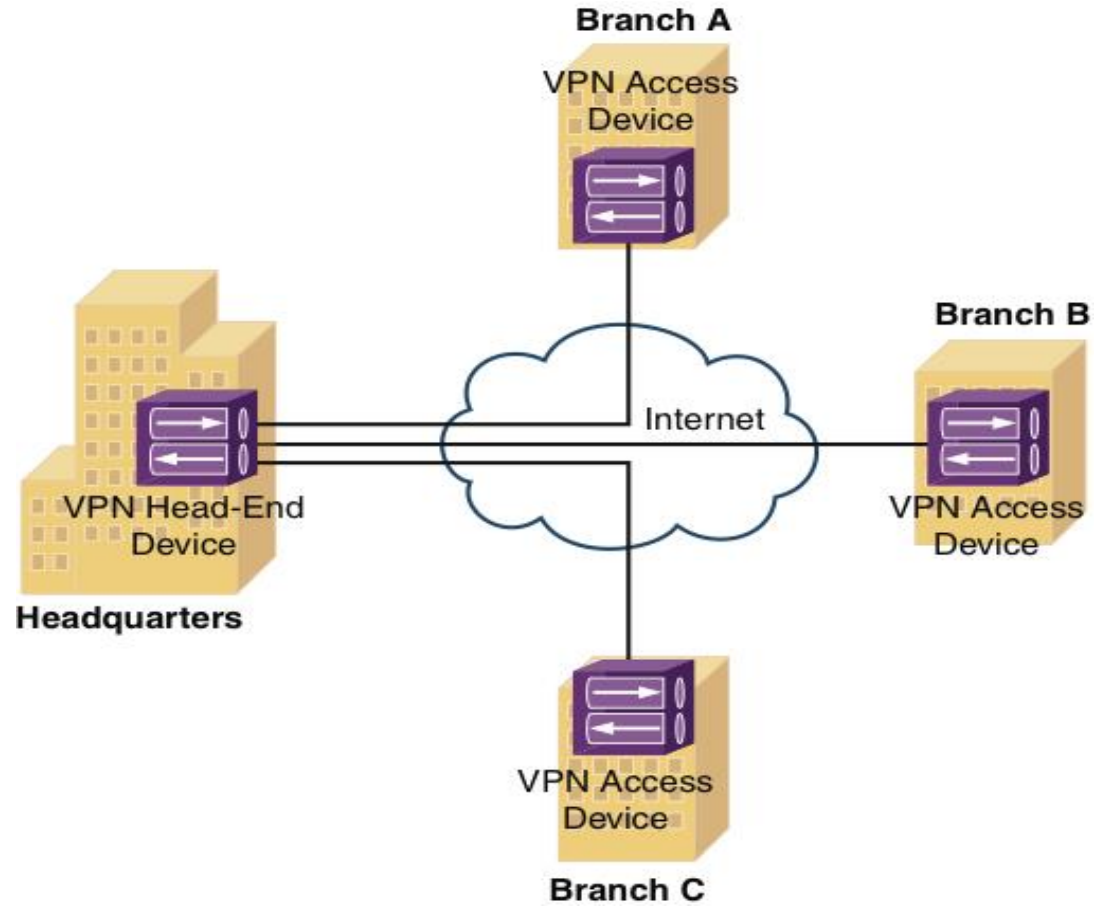
Firewall Zone Example

Defending Against Attacks

- **Virtual Private Networks (VPN).**
 - Much of today's workforce is located outside of a corporate headquarters location.
 - Some employees work in remote offices, while other telecommute, and other travel as part of their job.
 - These employees need a secure method to connect back to the headquarters (HQ).
 - WAN technologies could be used but would be expensive to implement.
 - A VPN supports secure communication between two sites over an untrusted network.
- **VPN (cont.)**
 - There are two primary categories of VPNs
 - **Site to Site** -- interconnects two sites, as an alternative to a leased line, at a reduced cost.
 - **Client to Site** – interconnects a remote user with a site, as an alternative to dial-up or ISDN connectivity, at a reduced cost.

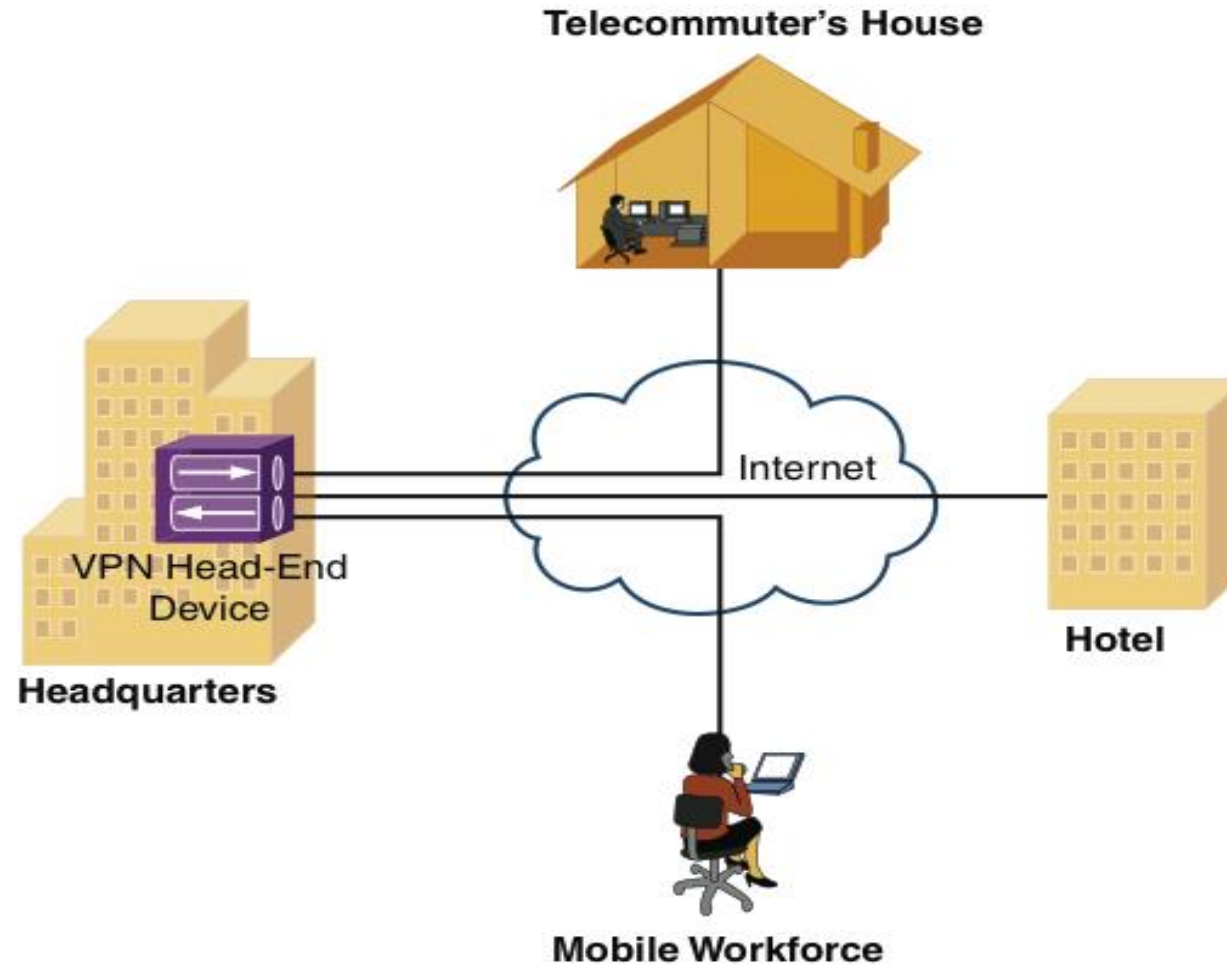
Defending Against Attacks

- Sample Site-to-Site VPN



Defending Against Attacks

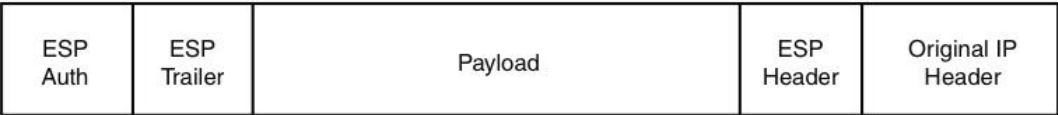
- Sample Client-to-Site VPN



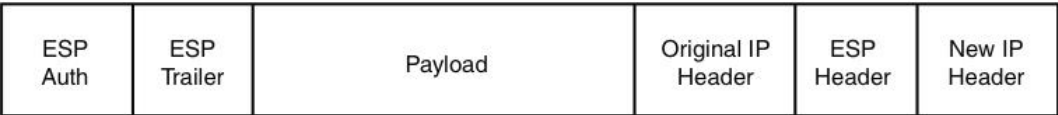
Defending Against Attacks

- Overview of IPsec
 - Broadband technologies, such as cable and DSL, in addition to other VPN transport mechanisms, often traverse and untrusted network, such as the Internet.
 - IPsec VPNs offer strong security features, such as the following:
 - Confidentiality
 - Integrity
 - Authentication
- IKE Modes and Phase
 - IPsec use a collection of protocols to provide features. One of the primary protocols the IPsec uses is the Internet Key Exchange

Transport Mode



Tunnel Mode

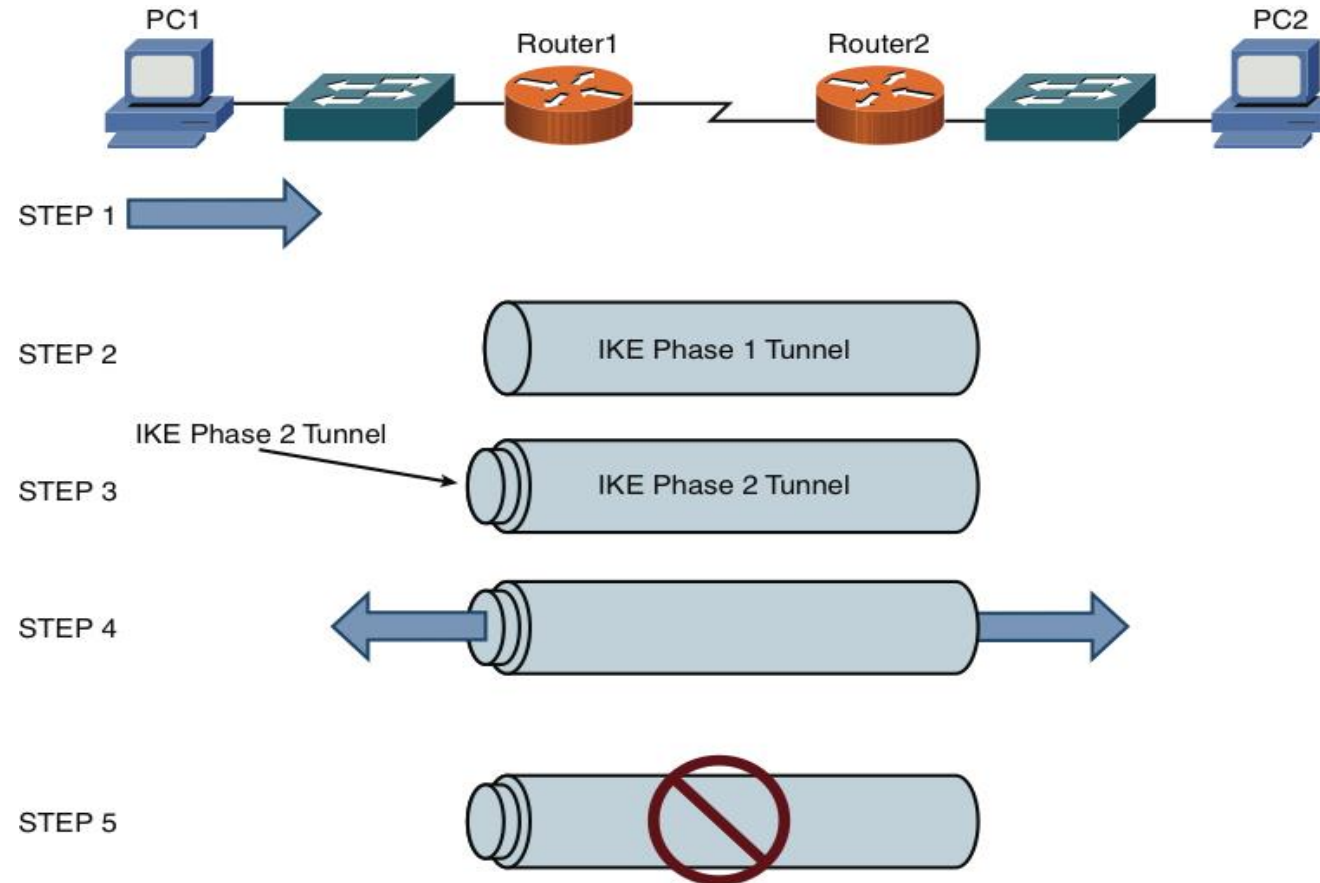


Transport mode encrypts only the payload

Tunnel mode encrypts the whole packet

Defending Against Attacks

- IPsec VPN Steps

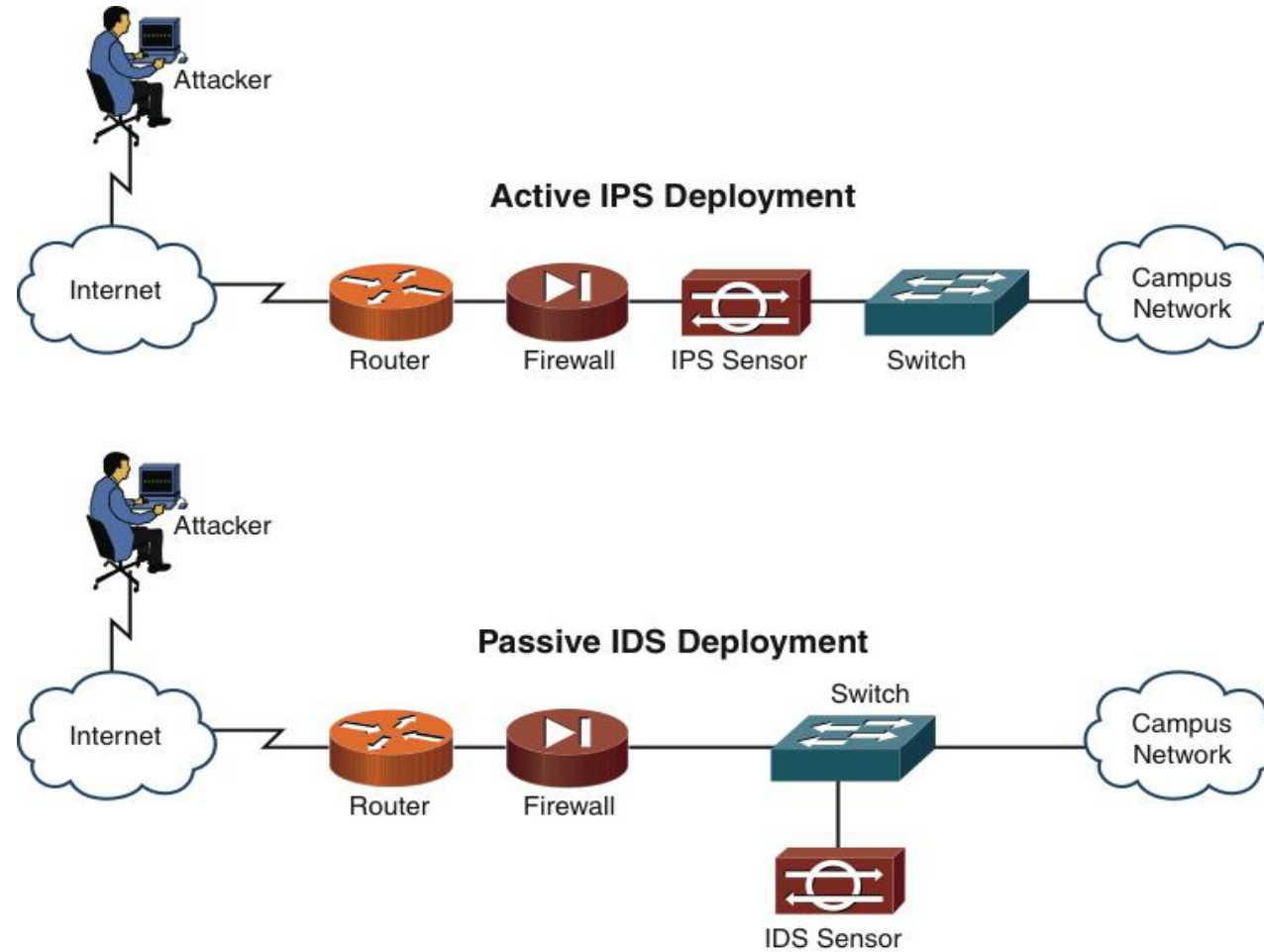


Defending Against Attacks

- VPN Protocols
 - SSL/TLS
 - Strong, used by HTTPS
- L2TP / IPSec
- L2F
 - Old tunneling protocol from Cisco, no encryption
- PPTP
 - Old Microsoft VPN protocol, weak encryption
- Intrusion Detection and Prevention
 - When an attacker launches an attack against a network, intrusion detection systems (IDS), and intrusion prevention systems (IPS) technologies are often able to recognize the attack and respond appropriately.
 - Attacks might be recognizable by comparing incoming data streams against a database of well-known attack signatures.
- **IDS Versus IPS**
 - IDS, sits parallel to the network, is a passive device, that monitors all traffic and sends alerts.
 - IPS, sits in-line to the network, is an active device, that monitors all traffic and sends alerts and deals with the offending traffic.

Defending Against Attacks

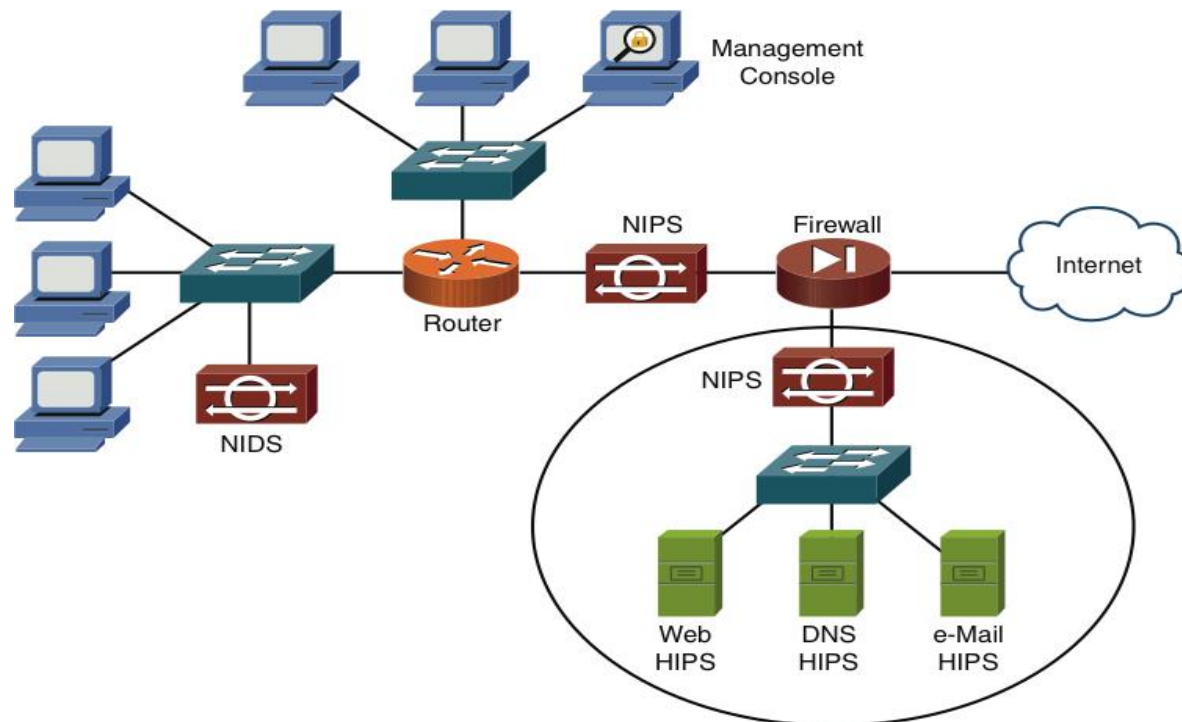
- IDS and IPS Network Placement



Defending Against Attacks

- **IDS and IPS Device Categories**
 - IDS and IPS device can be categorized based on how they detect malicious traffic.
- **Detection Methods**
 - Signature-based detection
 - Policy-based detection
 - Anomaly-based detection
- **Deploying Network-Based and Host-Based Solutions**
 - NIPS and HIPS solutions can work in tandem. This help further protect the system.

NIDS, NIPS, and HIPS Deployment Example



Troubleshooting Network Issues

Objectives

- What are the elements in a structured troubleshooting model?
- What common physical layer troubleshooting issues might you encounter?
- What potential Layer2 issues are you most likely to face when troubleshooting a network containing Ethernet switches?
- Aside from routing protocols troubleshooting, what Layer 3 troubleshooting issues are common in a routed network?
- How do characteristics unique to wireless network impact your troubleshooting of a network containing wireless access points?



Troubleshooting Network Issues

- As you perform your day-to-day tasks of administering a network, a significant percentage of your time will be dedicated to resolving network issues.
- Without a plan, your efforts might be inefficient, as you try one thing after another, possibly causing other issues in the process.
- Although your troubleshooting efforts can most definitely benefit from a structured approach, realize that troubleshooting is part art and part science.
- Specifically, your intuition and instincts play a huge role in isolating an issue.
- To help you start developing, or continue honing, your troubleshooting skills, this chapter begins by presenting you with a formalized troubleshooting methodology, which can act a guide for addressing most any network issue

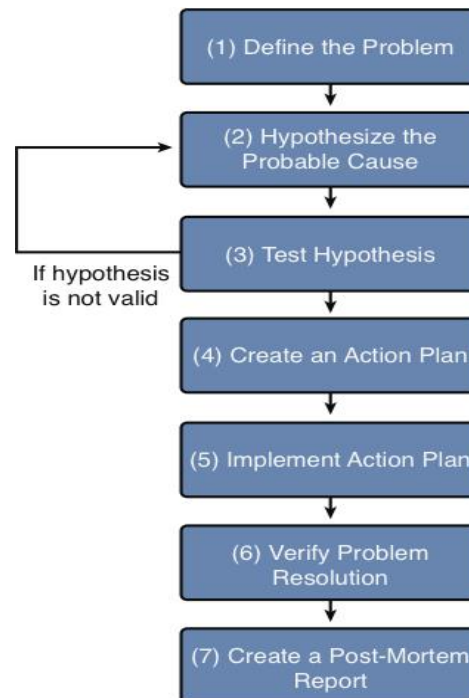
Troubleshooting Basics

- The process of troubleshooting, at its essence, is the process of responding to a problem report (sometimes in the form of a trouble ticket), diagnosing the underlying cause of the problem, and resolving the problem.
- Simplified Troubleshooting Flow



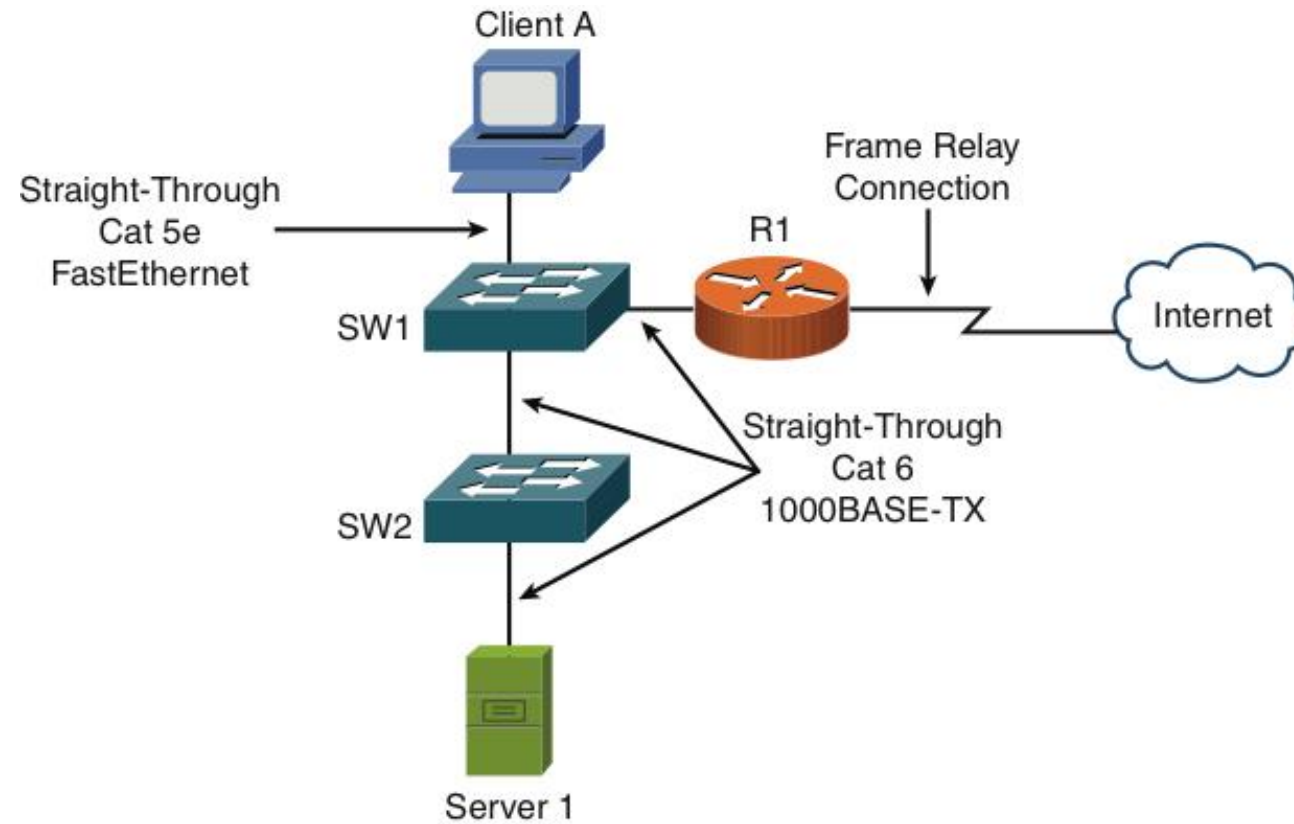
Structured Troubleshooting Methodology

- Structured Troubleshooting Approach



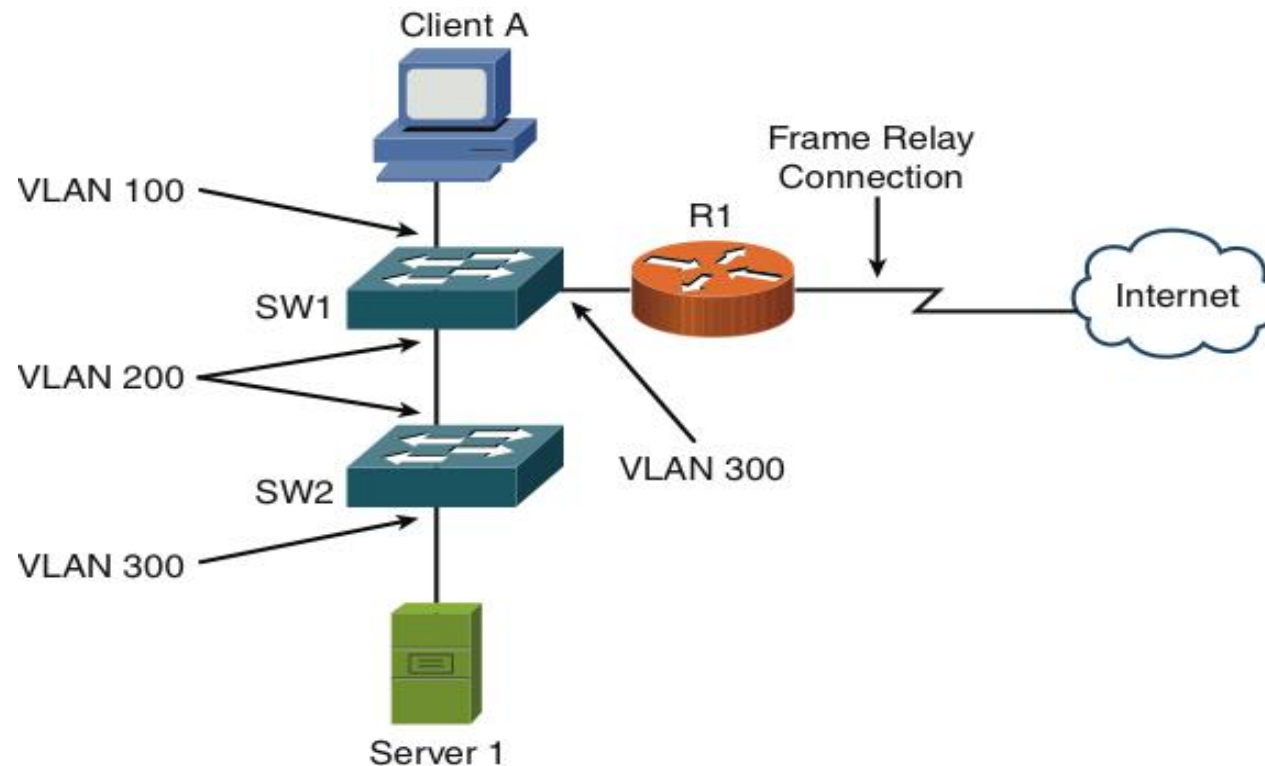
Physical Layer Troubleshooting

- Physical Layer Troubleshooting: Sample Topology



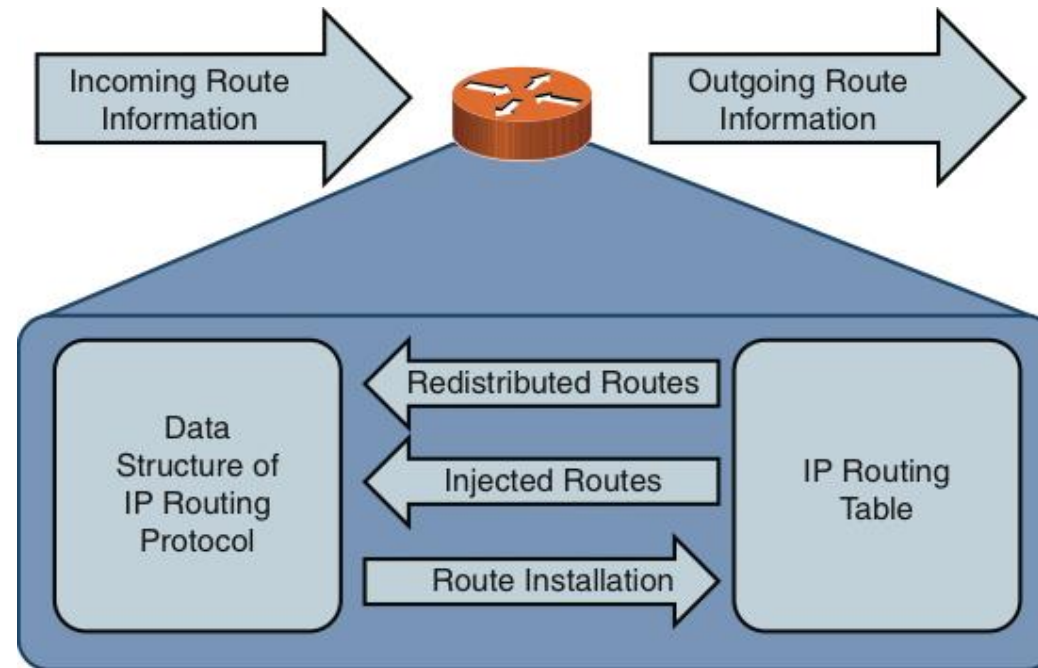
Data Link Layer Troubleshooting

- When troubleshooting Layer 2 and above, we must remember that, in these devices there is the flow of the user's data, we call the data plan.
- Then there is the controls that we place on this data, called the control plan.
- Data Link Layer Troubleshooting: Sample Topology



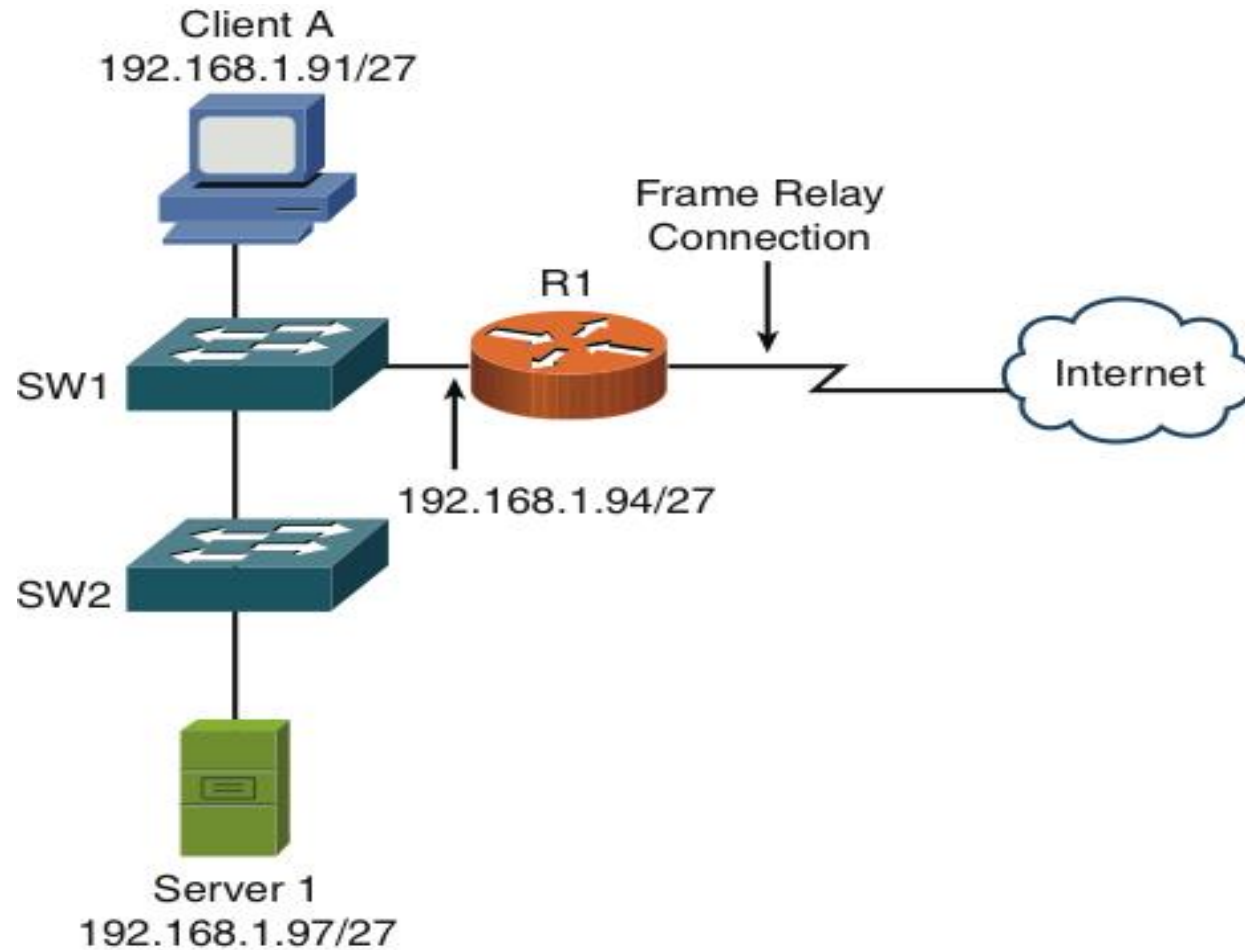
Network Layer Troubleshooting

- When troubleshooting connectivity issues for an IP-based network, the network layer (Layer 3) is often an appropriate place to begin your troubleshooting efforts.
- To better troubleshoot Layer 3 we must understand how our routing protocols affect how the router moves the IP packet.
- Interaction Between IP Routing Protocol Data Structures and IP Routing Tables



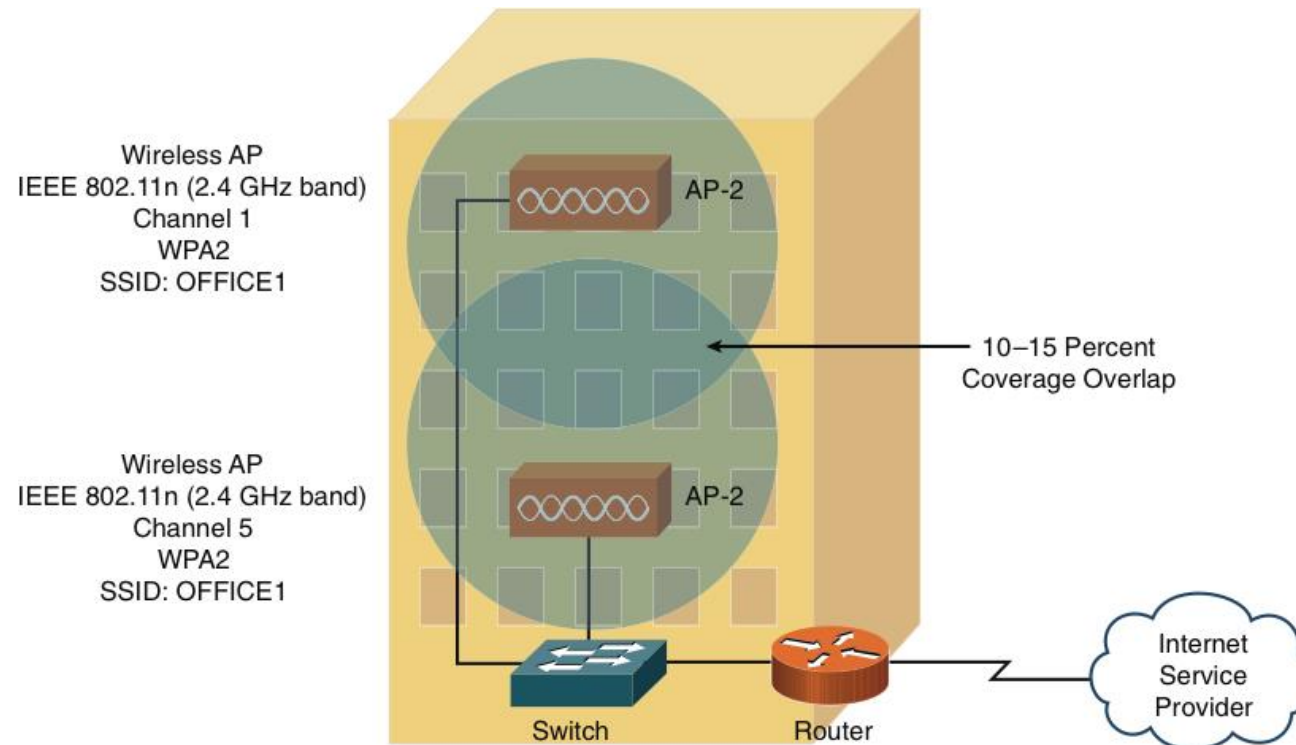
Network Layer Troubleshooting

- Network Layer Troubleshooting: Sample Topology



Wireless Troubleshooting

- Troubleshooting wireless networks can require a variety of skill sets. For example, some troubleshooting scenarios might require an understanding of antenna theory and the radio frequency spectrum.
- Again remember that we have a data plan and a control plan in this device also.
- Wireless Network Troubleshooting: Sample Topology



It has been completed Slides CompTIA Network +
Reference

CompTIA Network+ Study Guide

CompTIA Network+ Certification All-In-One Exam
Guide, Seventh Edition (Exam N10-007)

By : Eng. Ahmad Hassan Al-Mashaikh

LinkedIn : Ahmad H Al-Mashaikh

Facebook : Ahmad H Al-Mashaikh

Phone : 00972598053163 | This is WhatsApp

لكل من يحصل على هذا المرجع اتمنى منكم الدعاء بكل خير

وسلام عليكم ورحمة الله وبركاته

By : Eng. Ahmad Hassan Al-Mashaikh

Email : Ahmad.private.mashaikh@Hotmail.com

