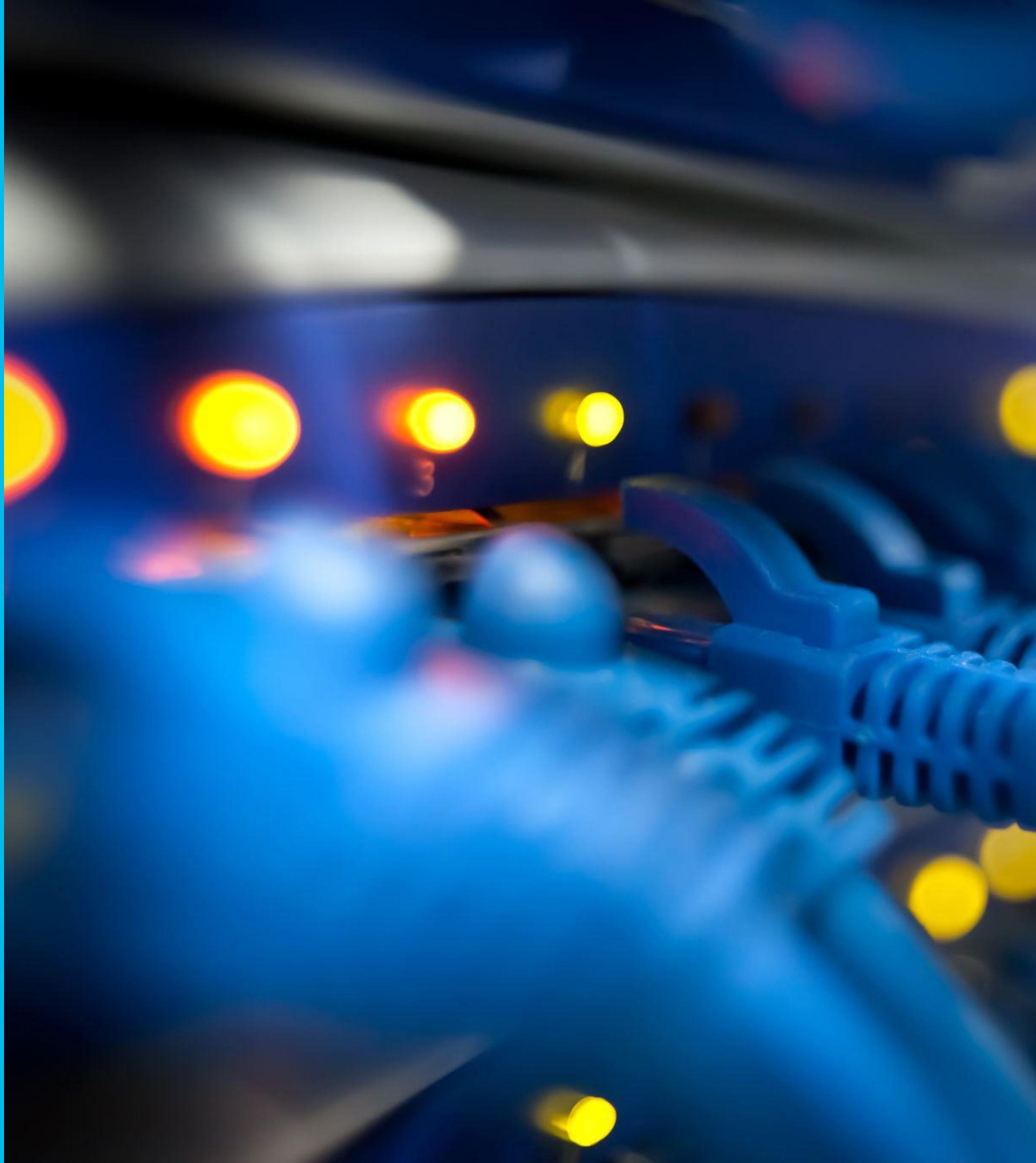
institute of continuing education

Networking Academy

Network Infrastructure Security

Md Manirul Islam
Director, Institute of Continuing Education
American International University-Bangladesh

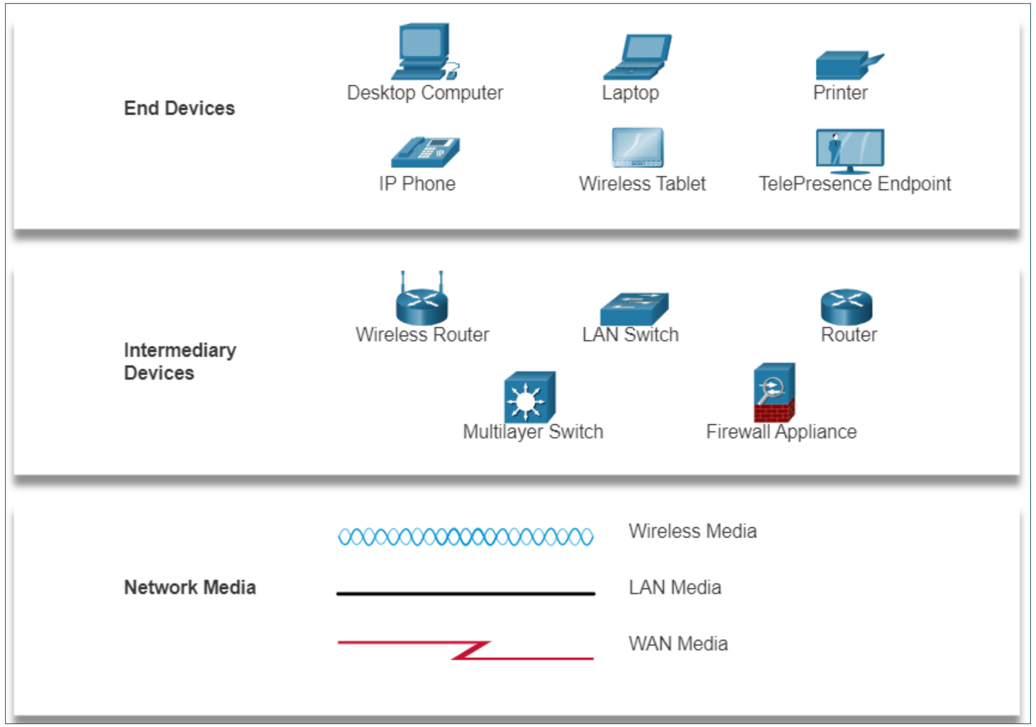
- Network Topologies
- Network Communication Devices
- Network Security Infrastructure



Network Topologies

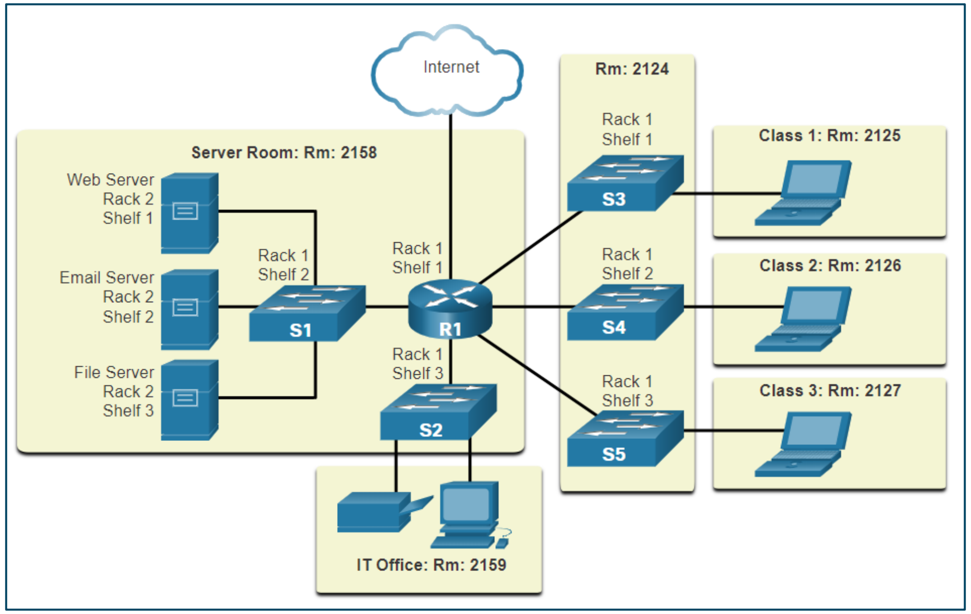
Overview of Network Components

- Network infrastructure contains three categories of network components:
  - Devices
  - Media
  - Services
- Network diagrams, often called topology diagrams, use symbols to represent different devices and connections within the network.

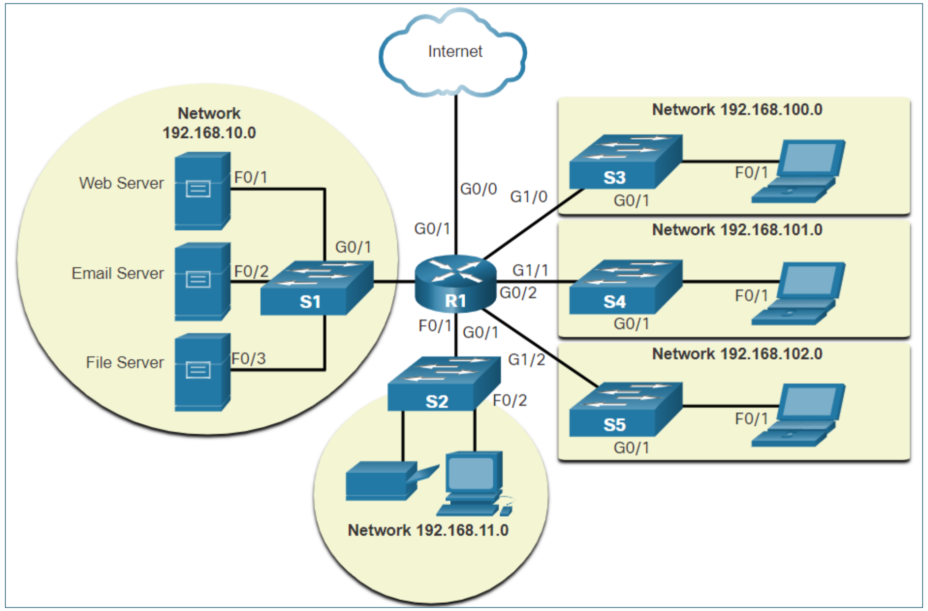


Topology Diagrams

Physical topology diagrams illustrate the physical location of intermediary devices and cable installation.



Logical topology diagrams illustrate devices, ports, and the addressing scheme of the network.



Networks of Many Sizes

- Small Home Networks – connect a few computers to each other and the Internet.
- Small Office and Home Office (SOHO) – enables computer within a home, office or remote office to connect to a corporate network, or access centralized, shared resources.
- Medium to Large Networks – can have many locations with hundreds or thousands of interconnected computers.
- World Wide Networks – connects hundreds of millions of computers world-wide – such as the internet.

Small Home

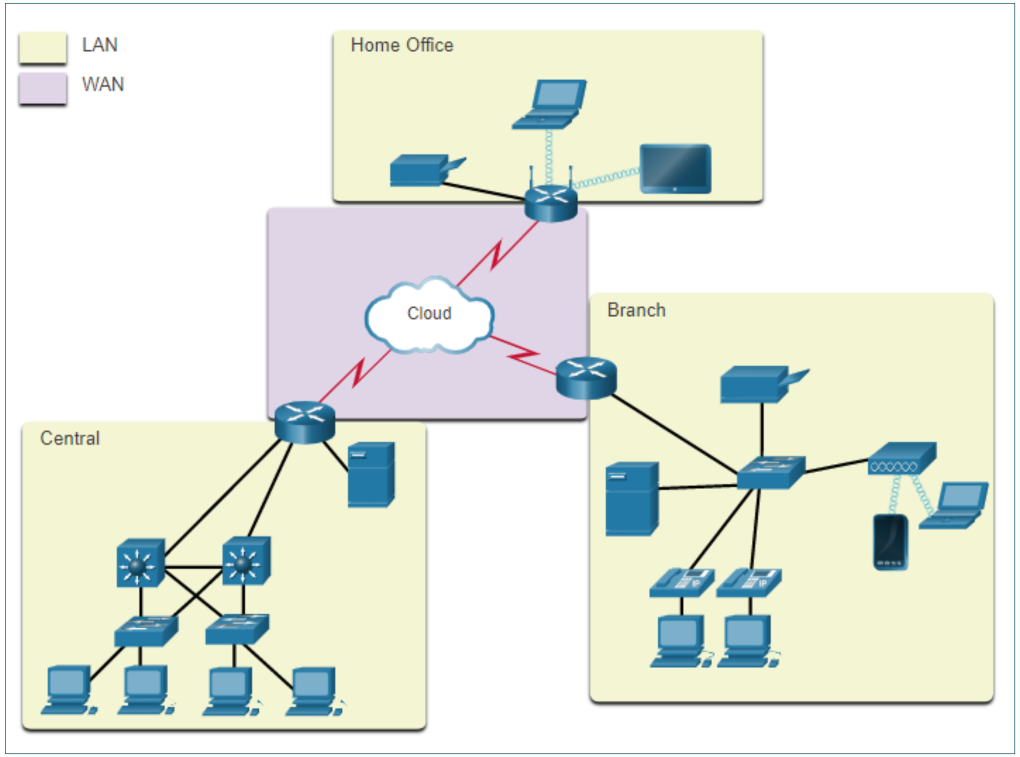
SOHO

Medium/Large

World Wide

LANs and WANs

- Network infrastructures vary greatly in terms of:
  - Size of the area covered
  - Number of users connected
  - Number and types of services available
  - Area of responsibility
- The two most common types of network infrastructures are
  - Local Area Networks (LANs)
  - Wide Area Networks (WANs)

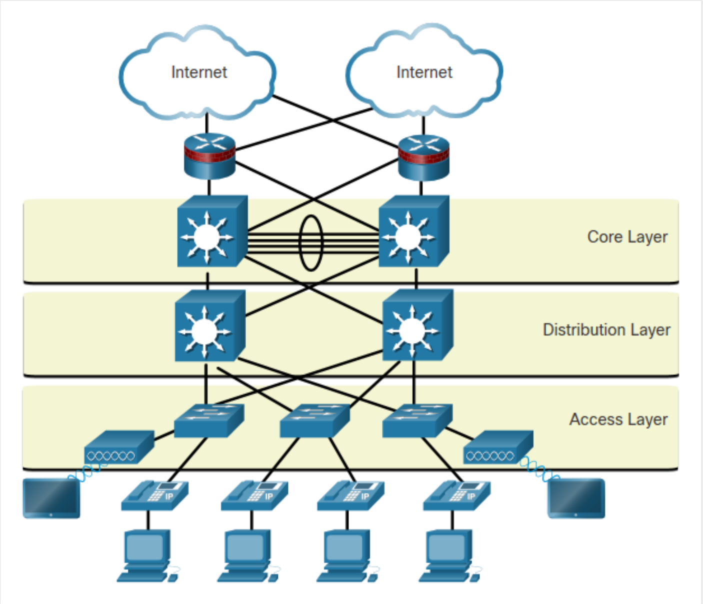


LANs connected to a WAN

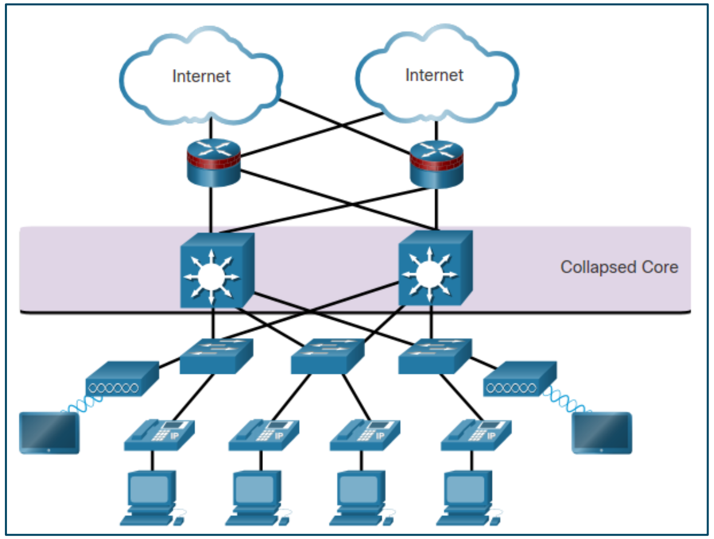
LAN	WAN
Interconnect end devices in a limited area.	Interconnect LANs over wide geographical areas.
Administered by a single organization or individual.	Typically administered by multiple service providers.
Provide high-speed bandwidth to internal end devices and intermediary devices.	Typically provide slower speed links between LANs.

The Three-Layer Network Design Model

- The campus wired LAN uses a hierarchical design model to separate the network topology into modular groups or layers.
- The hierarchical LAN design includes three layers:
  - **Access** - Provides endpoints and users direct access to the network.
  - **Distribution** - Aggregates access layers and provides connectivity to services.
  - **Core** - Provides connectivity between distribution layers for large LAN environments.
- Although the hierarchical model has three layers, some smaller enterprise networks may implement a two-tier hierarchical design.
- In this two-tier hierarchical design, the core and distribution layers are collapsed into one layer, thus reducing cost and complexity.



Hierarchical Design Model



Collapsed Core

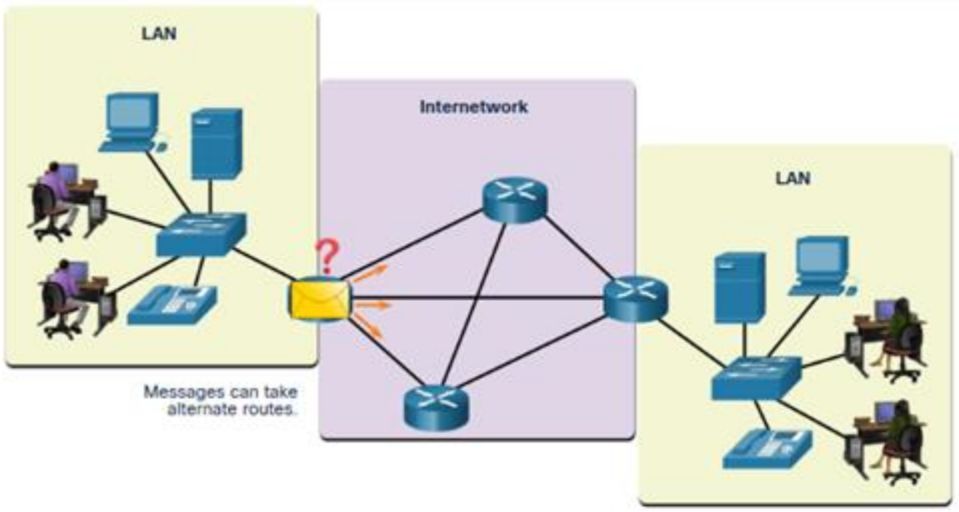
Network Devices

Network Communication Devices

Network Devices

End Devices

- The most familiar network devices are end devices. An end device is either the source or destination of a message transmitted over the network.
- To distinguish one end device from another, each end device on a network has an address.
- When an end device initiates communication, it uses the address of the destination end device to specify where to deliver the message.
- Data originates with an end device, flows through the network, and arrives at an end device.



Data originates with an end device, flows through the network, and arrives at an end device.

Routers

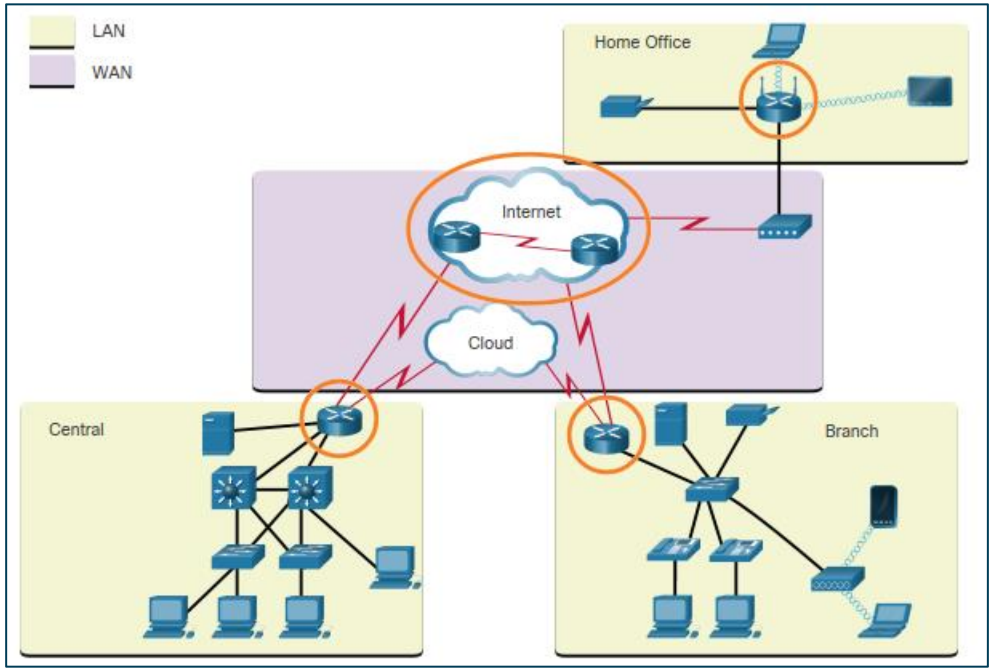
Function of a Router:

- Provides path determination and packet forwarding.
- Responsible for encapsulating and de-encapsulating packets.
- Uses a routing table to determine the best path to use to send packets to a specified network.

Routing Table:

- Contains directly connected routes and remote routes.
- Router searches its routing table for a network address that matches the destination IP address of a packet.
- Uses the gateway of last resort if learned or configured; otherwise, the packet is discarded.

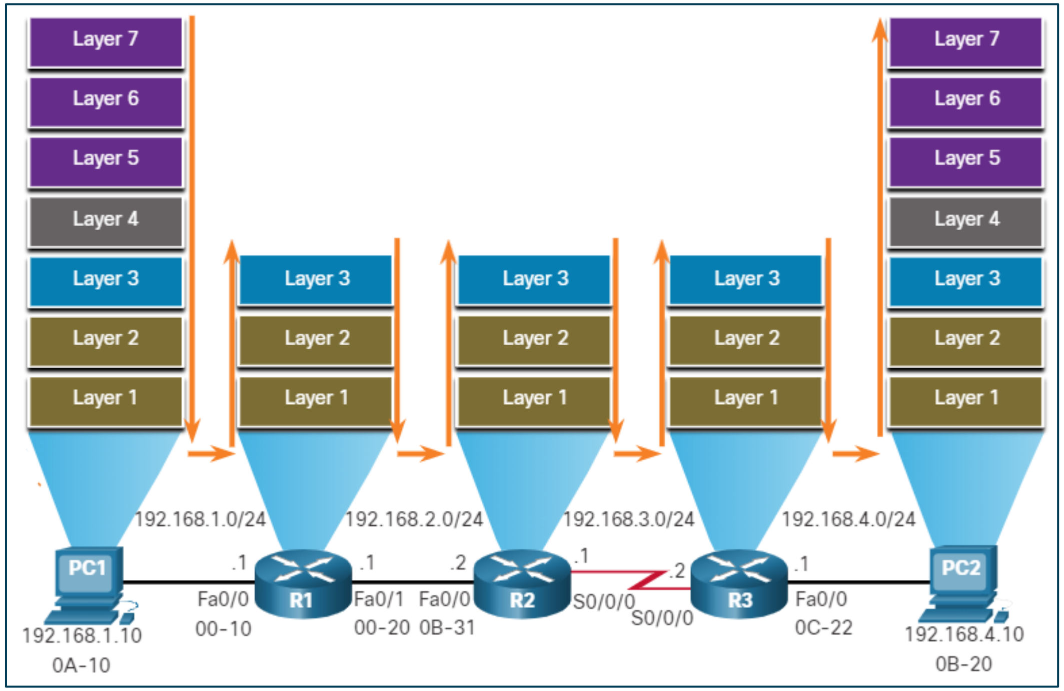
The Router Connection



Routers (Cont’d)

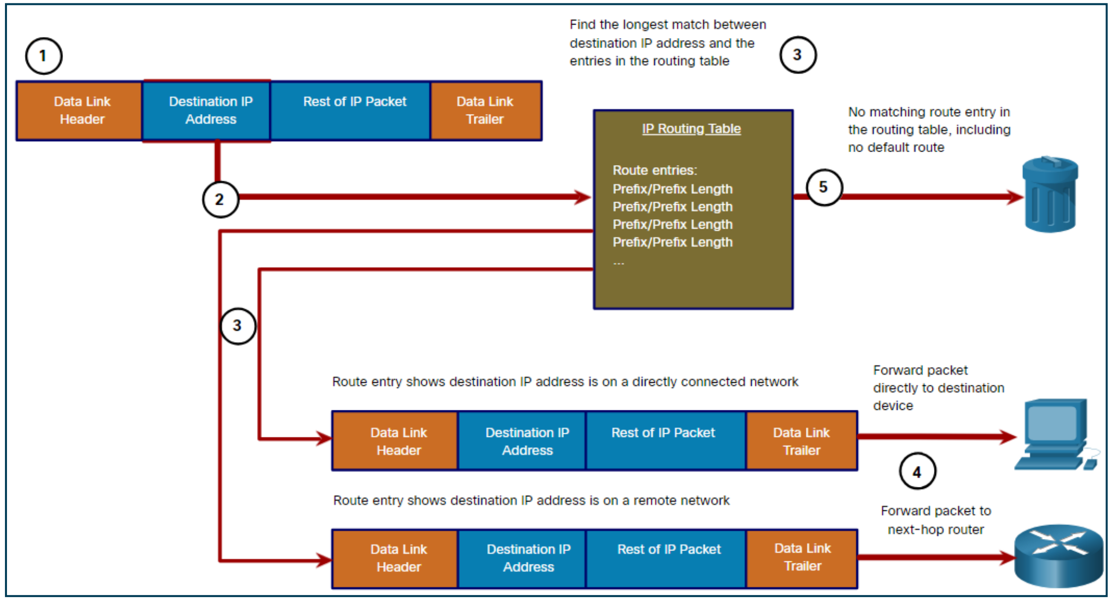
- The router performs the following three major steps:
  1. It de-encapsulates the Layer 2 frame header and trailer to expose the Layer 3 packet.
  2. It examines the destination IP address of the IP packet to find the best path in the routing table.
  3. If the router finds a path to the destination, it encapsulates the Layer 3 packet into a new Layer 2 frame and forwards that frame out the exit interface.
- Devices have Layer 3 IPv4 addresses, while Ethernet interfaces have Layer 2 data link addresses. The MAC addresses are shortened to simplify the illustration.

Encapsulating and De-Encapsulating Packets



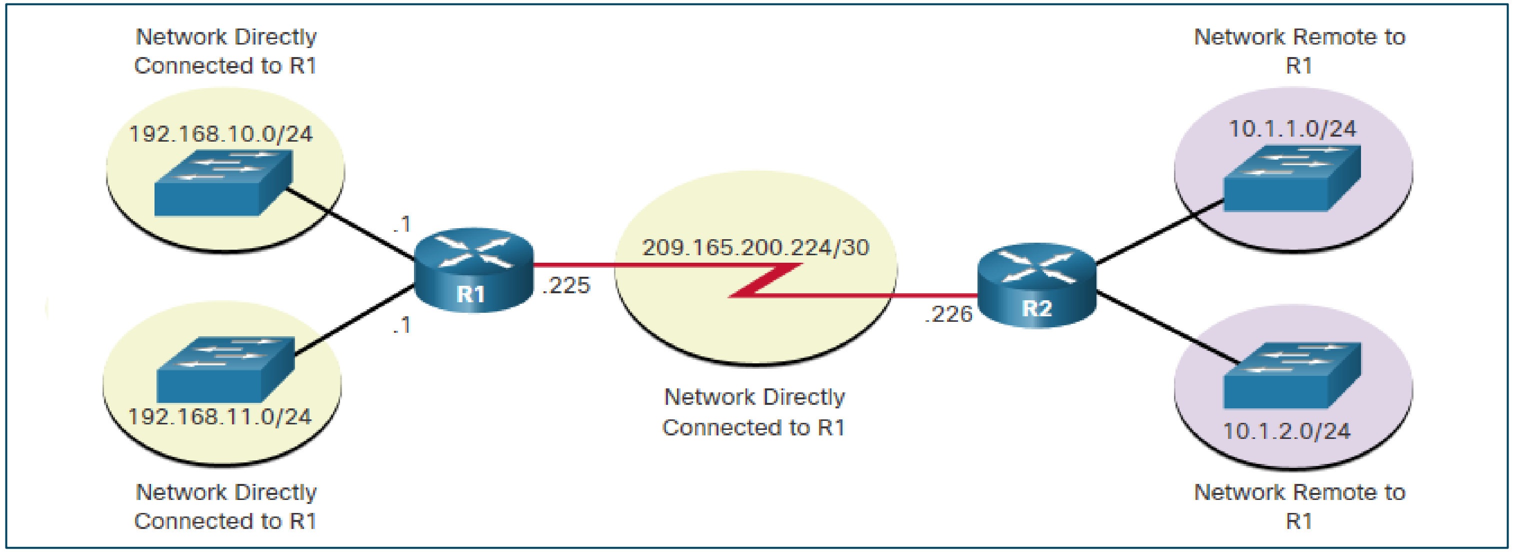
Packet Forwarding Decision Process

- Router must determine how to encapsulate the packet and forward it out the correct egress interface. The following steps describe the packet forwarding process shown in the figure:
- The data link frame with an encapsulated IP packet arrives on the ingress interface.
- The router examines the destination IP address in the packet header and consults its IP routing table.
- The router finds the longest matching prefix in the routing table.
- The router encapsulates the packet in a data link frame and forwards it out the egress interface.
- The destination could be a device connected to the network or a next-hop router.
- If there is no matching route entry the packet is dropped.


1
Data Link Header
Destination IP Address
Rest of IP Packet
Data Link Trailer
Find the longest match between destination IP address and the entries in the routing table
3
2
IP Routing Table
Route entries:
Prefix/Prefix Length
Prefix/Prefix Length
Prefix/Prefix Length
Prefix/Prefix Length
...
No matching route entry in the routing table, including no default route
5
3
Route entry shows destination IP address is on a directly connected network
Forward packet directly to destination device
Data Link Header
Destination IP Address
Rest of IP Packet
Data Link Trailer
4
Route entry shows destination IP address is on a remote network
Forward packet to next-hop router
Data Link Header
Destination IP Address
Rest of IP Packet
Data Link Trailer

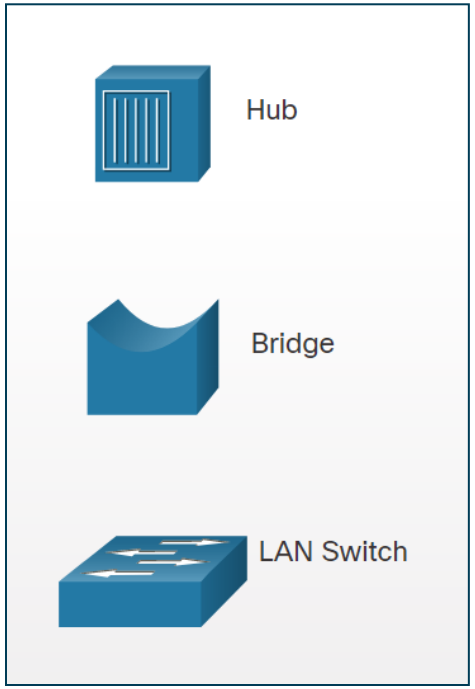
Routing Information

- The routing table stores the following information:
  - **Directly connected routes** - These routes come from the active router interfaces. Routers add a directly connected route when an interface is configured with an IP address and is activated.
  - **Remote routes** - These are remote networks connected to other routers.
- The destination network entries in the routing table can be added in several ways:
  - **Local Route interfaces** – These are added when an interface is configured and active.
  - **Directly connected interfaces** – These are added to the routing table when an interface is configured and active.
  - **Static routes** – These are added when a route is manually configured, and the exit interface is active.
  - **Dynamic routing protocol** – This is added when routing protocols that dynamically learn about the network, such as EIGRP or OSPF, are implemented and networks are identified.



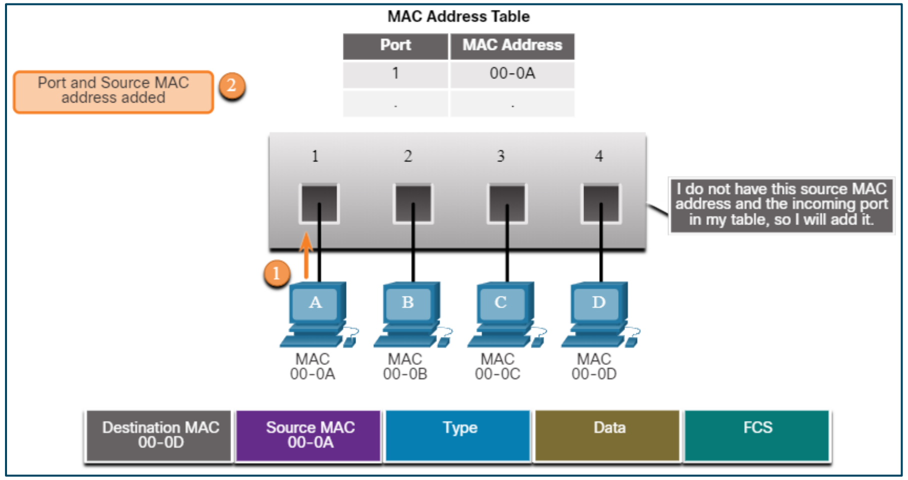
Hubs, Bridges, LAN Switches

- The topology icons for hubs, bridges, and LAN switches are shown in the figure.
- An Ethernet hub acts as a multiport repeater that receives an incoming electrical signal (data) on a port. It then immediately forwards a regenerated signal out all other ports. Hubs use physical layer processing to forward data.
- Bridges have two interfaces and are connected between hubs to divide the network into multiple collision domains. Each collision domain can have only one sender at a time.
- LAN switches are multiport bridges that connect devices into a star topology. Switches also segment a LAN into separate collision domains, one for each switch port. A switch makes forwarding decisions based on Ethernet MAC addresses.



Switching Operation

- Switches use MAC addresses to direct network communications through the switch, to the appropriate port, and toward the destination.
- A switch is made up of integrated circuits and the accompanying software that controls the data paths through the switch.
- For a switch to know the port to transmit a frame, it must first learn the devices existing on each port. As the switch learns the relationship of ports to devices, it builds a table called a MAC address table, or content addressable memory (CAM) table which is a special type of memory used in high-speed searching applications.
- LAN switches determine how to handle incoming data frames by maintaining the MAC address table.
- The switch uses the information in the MAC address table to send frames destined for a specific device out of the port to which the device is connected.



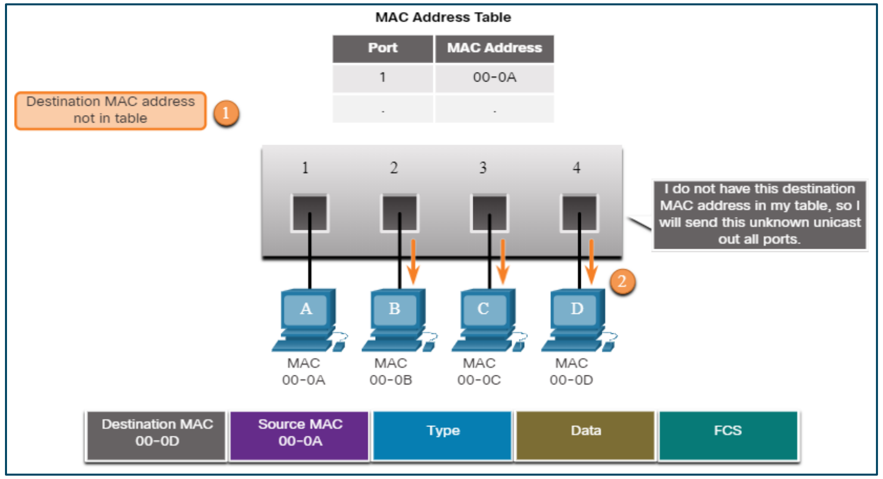
MAC Address Table

Port	MAC Address
1	00-0A
.	.

Port and Source MAC address added 2

I do not have this source MAC address and the incoming port in my table, so I will add it.

Learn: Examining the Source MAC Address



MAC Address Table

Port	MAC Address
1	00-0A
.	.

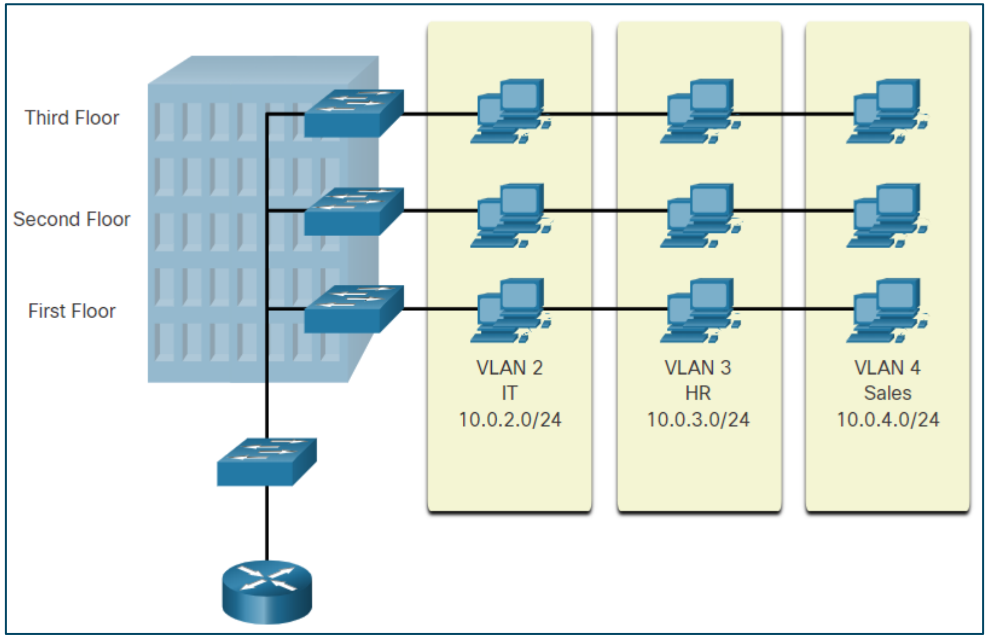
Destination MAC address not in table 1

I do not have this destination MAC address in my table, so I will send this unknown unicast out all ports.

Forward: Examining the Destination MAC Address

VLANs

- VLANs provide a way to group devices within a LAN.
- It provides segmentation and organizational flexibility within a switched internetwork.
- It allows an administrator to segment networks based on factors such as function, project team, or application, without regard for the physical location of the user or device.
- It creates a logical broadcast domain that can span multiple physical LAN segments.
- It prevent users on different VLANs from snooping on each other’s traffic.

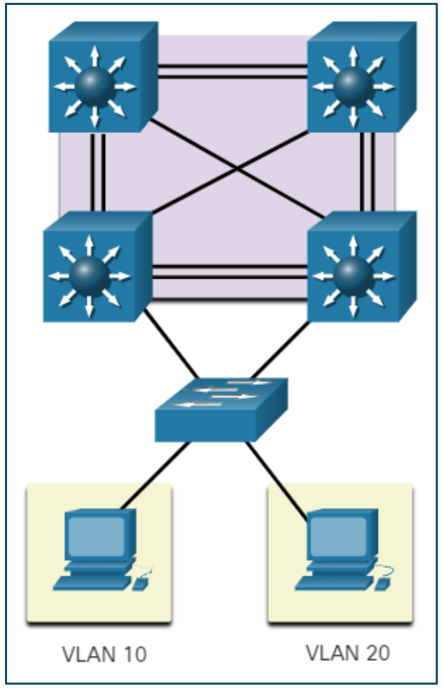


STP

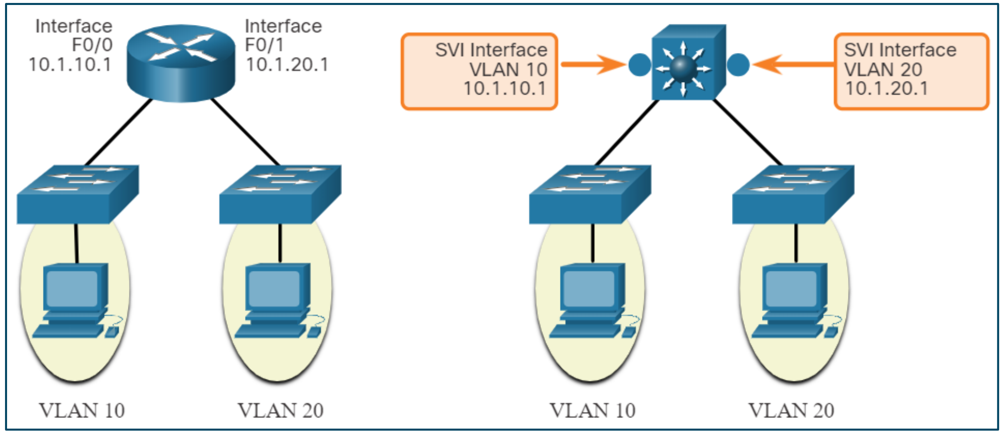
- The Spanning Tree Protocol is used to maintain one loop-free path in the Layer 2 network, at any time.
- Loops and duplicate frames have severe consequences for a switched network. STP was developed to address these issues.
- It ensures that there is one logical path between all destinations on the network by blocking redundant paths.
- A port is considered blocked when user data is prevented from entering or leaving that port. This does not include bridge protocol data unit (BPDU) frames that are used by STP to prevent loops.
- If the path is ever needed to compensate for a network cable or switch failure, STP recalculates the paths and unblocks the necessary ports to allow the redundant path to become active.

Multilayer Switching

- Multilayer switches (Layer 3 switches) perform Layer 2 switching and also forward frames based on Layer 3 and 4 information.
- All Cisco Catalyst multilayer switches support the following types of Layer 3 interfaces:
  - **Routed port** - A pure Layer 3 interface similar to a physical interface on a Cisco IOS router.
  - **Switch virtual interface (SVI)** - A virtual VLAN interface for inter-VLAN routing. In other words, SVIs are the virtual-routed VLAN interfaces.



Routed Ports



Switch Virtual Interface

Wireless Communications

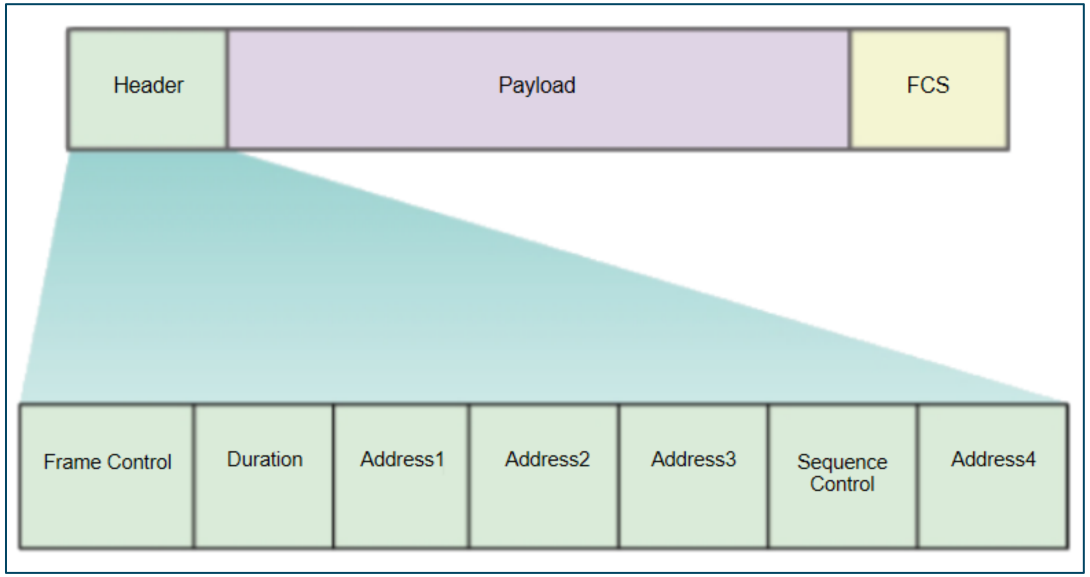
Wireless versus Wired LANs

- **Wireless LANs (WLANs)**:
  - Use Radio Frequencies (RF) instead of cables at the physical layer and MAC sublayer of the data link layer.
  - Connect clients to a network through a wireless access point (AP) or wireless router, instead of an Ethernet switch.

Characteristic	802.11 Wireless LAN	802.3 Wired Ethernet LANs
Physical Layer	Radio frequency (RF)	Physical cables
Media Access	Collision avoidance	Collision detection
Availability	Anyone with a wireless NIC in range of an access point	Physical cable connection required
Signal Interference	Yes	Minimal
Regulation	Different regulations by country	IEEE standard dictates

802.11 Frame Structure

All 802.11 wireless frames contain the following fields:



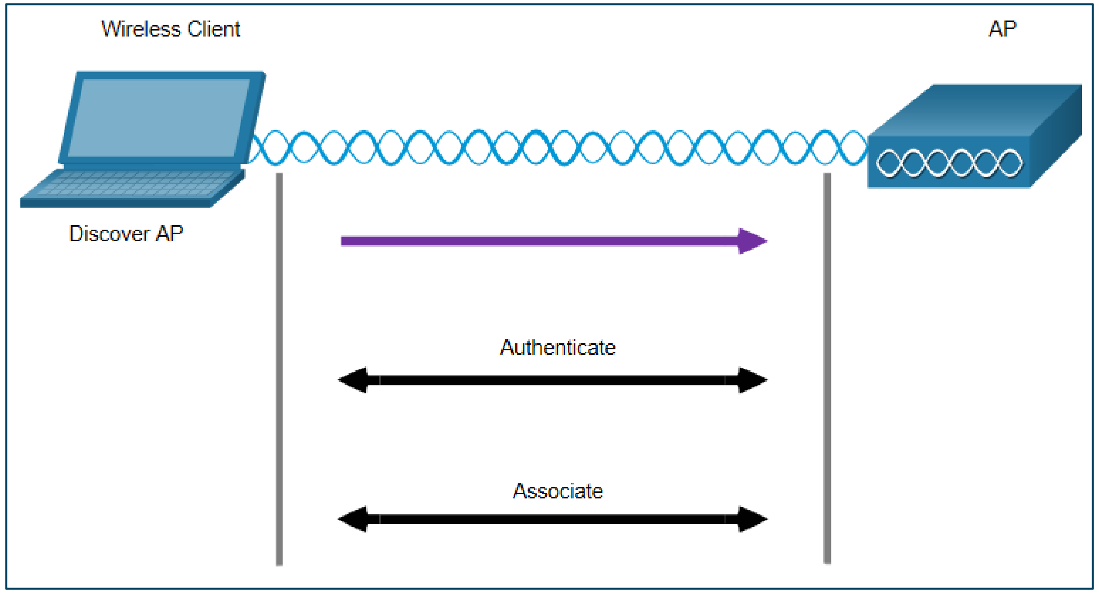
- **Frame Control** – This identifies the type of wireless frame and contains subfields for protocol version, frame type, address type, power management, and security settings.
- **Duration** – This is used to indicate the remaining duration needed to receive the next frame transmission.
- **Address1** – This contains the MAC address of the receiving wireless device or AP.
- **Address2** – This contains the MAC address of the transmitting wireless device or AP.
- **Address3** - This contains the MAC address of the destination, such as the router interface with AP attached.
- **Sequence Control** – This contains information to control sequencing and fragmented frames.
- **Address4** - This is usually missing as it is used only in ad hoc mode.
- **Payload** – This contains the data for transmission.
- **FCS** – This is used for Layer 2 error control.

CSMA/CA

- WLANs are half-duplex, shared media configurations.
- Half-duplex means that only one client can transmit or receive at any given moment.
- Shared media means that wireless clients can all transmit and receive on the same radio channel.
- This creates a problem because a wireless client cannot hear while it is sending, which makes it impossible to detect a collision.
- To resolve this problem, WLANs use Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) method to determine how and when to send data on the network.
- A wireless client does the following:
  - Listens to the channel to see if it is idle. The channel is also called the carrier.
  - Sends a Ready To Send (RTS) message to the AP to request dedicated access to the network.
  - Receives a Clear To Send (CTS) message from the AP granting access to send.
  - If the wireless client does not receive a CTS message, it waits a random amount of time before restarting the process.
  - After it receives the CTS, it transmits the data.
  - All transmissions are acknowledged.

Wireless Client and AP Association

- For wireless devices to communicate over a network, they must first associate with an AP or wireless router.
- An important part of the 802.11 process is discovering a WLAN and subsequently connecting to it.
- Wireless devices complete the following three stage process, as shown in the figure:
  - Discover a wireless AP
  - Authenticate with AP
  - Associate with AP



Wireless Client and AP Association

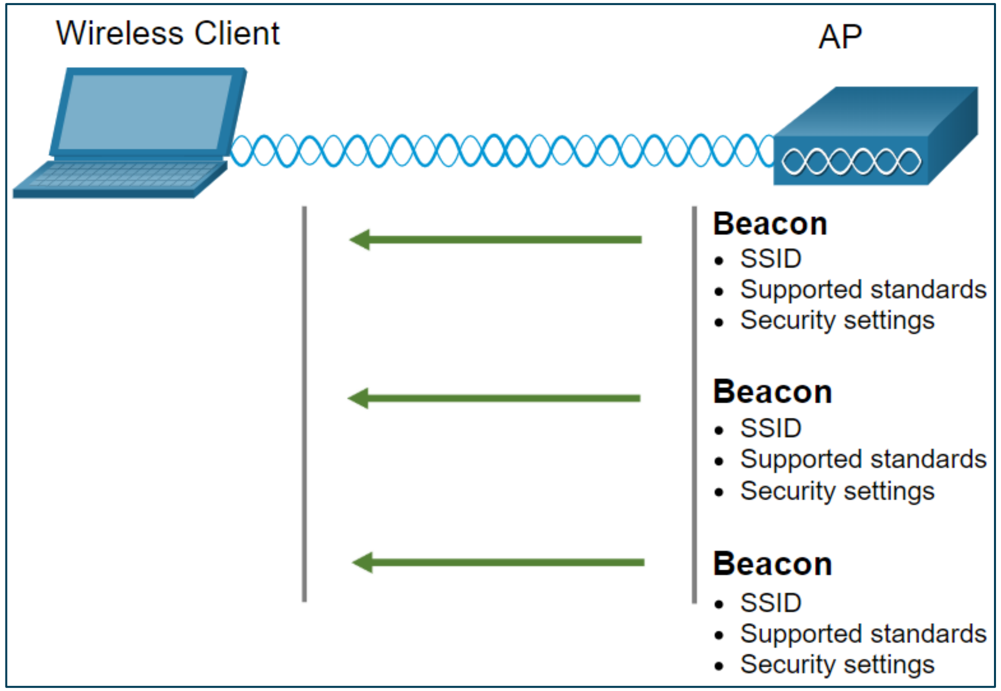
- In order to have a successful association, a wireless client and an AP must agree on specific parameters. Parameters must then be configured on the AP and subsequently on the client. The configurable wireless parameters include:
  - **SSID** -The SSID name appears in the list of available wireless networks on a client.
  - **Password** – This is required from the wireless client to authenticate to the AP.
  - **Network mode** - This refers to the 802.11a/b/g/n/ac/ad WLAN standards.
  - **Security mode** - This refers to the security parameter settings, such as WEP, WPA, or WPA2. Always enable the highest security level supported.
  - **Channel settings** - This refers to the frequency bands used to transmit wireless data.

Passive and Active Discover Mode

Wireless devices must discover and connect to an AP or wireless router. Wireless clients connect to the AP using a scanning (probing) process such as passive and active.

Passive Mode

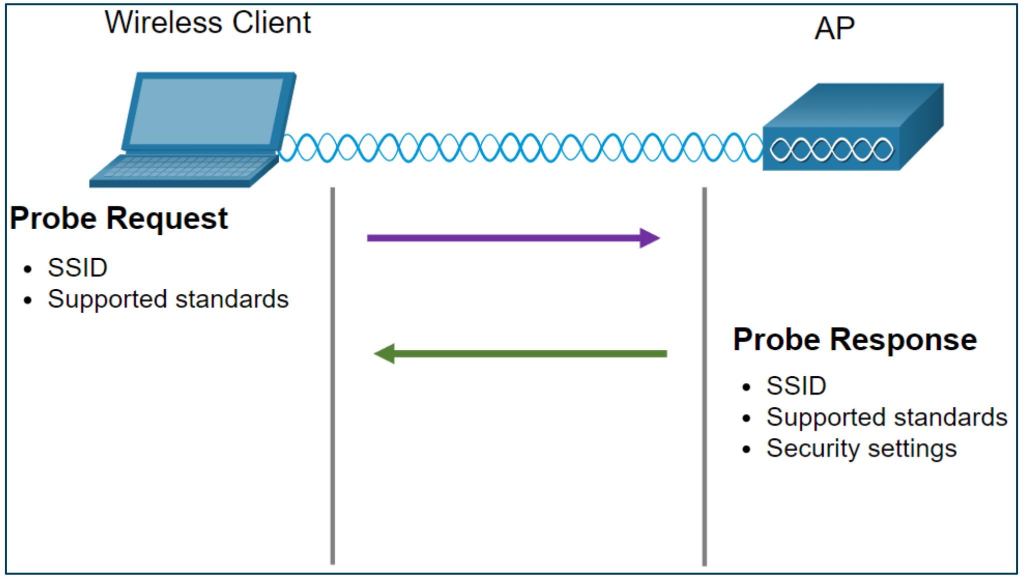
- In this mode, the AP openly advertises its service by periodically sending broadcast beacon frames containing the SSID, supported standards, and security settings.
- The primary purpose of the beacon is to allow wireless clients to learn which networks and APs are available in a given area.
- This allows the wireless clients to choose which network and AP to use.



Passive and Active Discover Mode (Cont’d)

Active Mode

- In this mode, wireless clients must know the name of the SSID.
- The wireless client initiates the process by broadcasting a probe request frame on multiple channels includes the SSID name and standards supported.
- APs configured with the SSID will send a probe response that includes the SSID, supported standards, and security settings.



- Active mode may be required if an AP is configured to not broadcast beacon frames.
- A wireless client could also send a probe request without a SSID name to discover nearby WLAN networks. APs configured to broadcast beacon frames would respond to the wireless client with a probe response and provide the SSID name.

Wireless Devices - AP, LWAP, and WLC

- A common wireless data implementation is enabling devices to connect wirelessly via a LAN.
- In general, a wireless LAN requires wireless access points and clients that have wireless NICs.
- Home and small business wireless routers integrate the functions of a router, switch, and access point into one device as shown in the figure.
- In small networks, the wireless router may be the only AP as only a small area requires wireless coverage.
- In larger networks, there can be many APs.

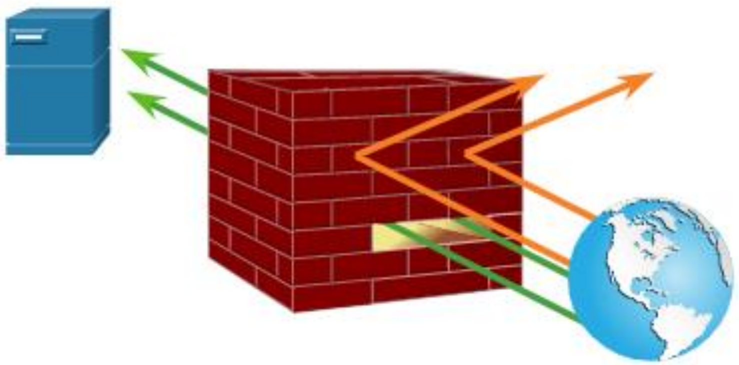
- All of the control and management functions of the APs on a network can be centralized into a Wireless LAN Controller (WLC).
- When using a WLC, the APs no longer act autonomously, but instead act as lightweight APs (LWAPs).
- LWAPs only forward data between the wireless LAN and the WLC.
- All management functions, such as defining SSIDs and authentication are conducted on the centralized WLC rather than on each individual AP.
- A major benefit of centralizing the AP management functions in the WLC is simplified configuration and monitoring of numerous access points, among many other benefits.

Network Security Infrastructure

Security Devices

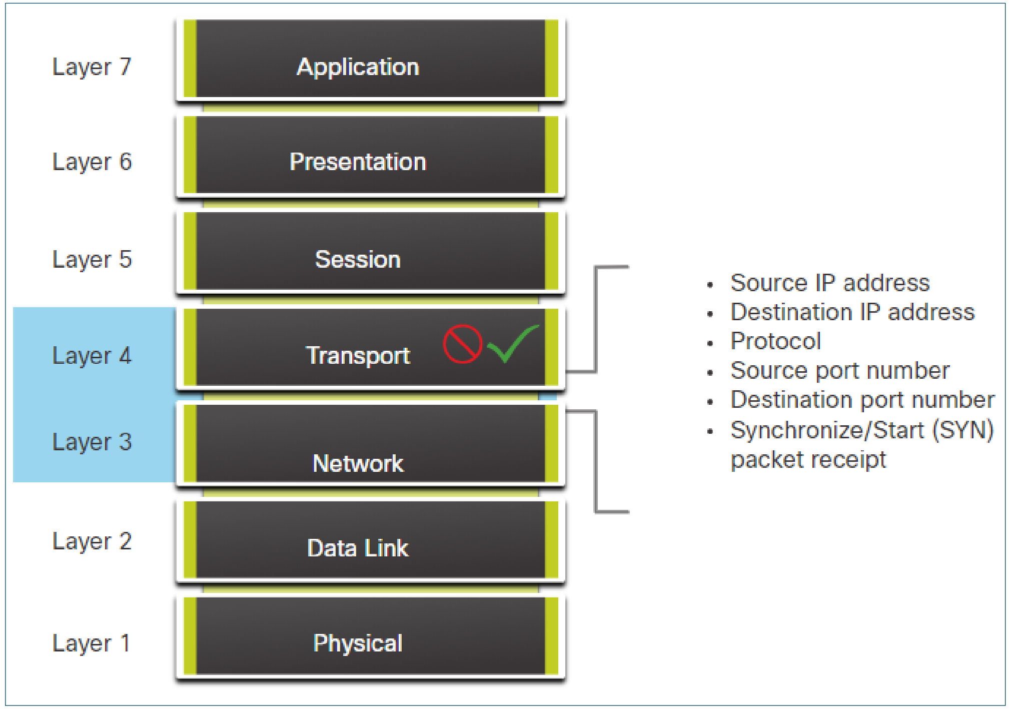
Firewalls

- Some common firewall properties:
  - Firewalls are resistant to network attacks.
  - All traffic flows through the firewall.
  - Firewalls enforce the access control policy.
- Several benefits of using a firewall in a network:
  - Prevents the exposure of sensitive hosts, resources, and applications to untrusted users.
  - Sanitizes protocol flow.
  - Blocks malicious data from servers and clients.
  - Reduces security management complexity.
- Firewalls also present some limitations:
  - A misconfigured firewall can have serious consequences for the network.
  - The data from many applications cannot be passed over firewalls securely.
  - Users search for ways around the firewall to receive blocked material.
  - Network performance can slow down.
  - Unauthorized traffic can be tunneled as legitimate traffic through the firewall.



Firewall Type Descriptions

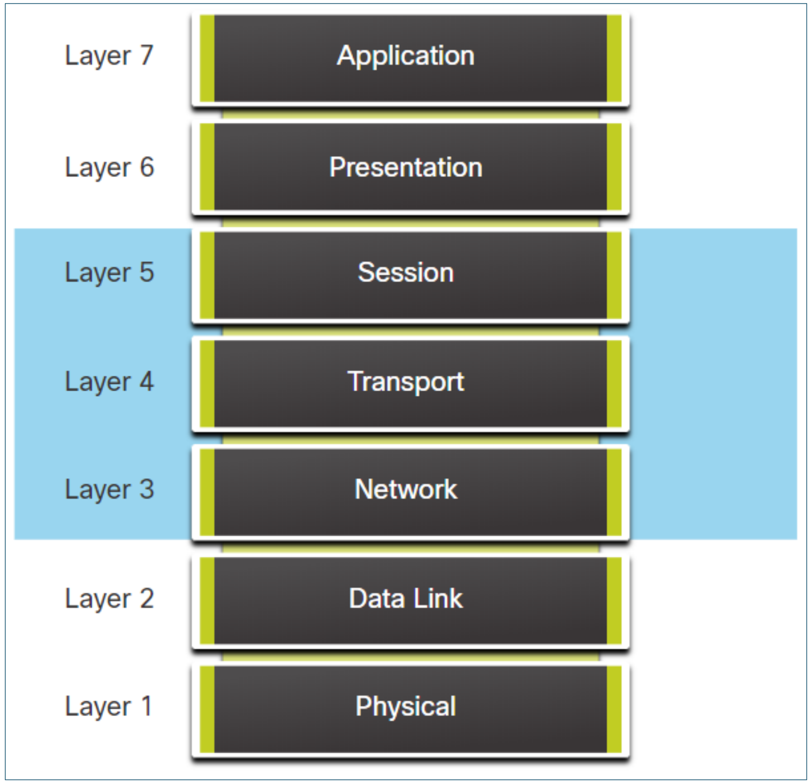
- **Packet Filtering (Stateless) Firewall**
  - Packet Filtering firewalls are part of a router firewall, which permits or denies traffic based on Layer 3 and Layer 4 information.
  - They are stateless firewalls that use a simple policy table look-up that filters traffic based on specific criteria.



- Source IP address
- Destination IP address
- Protocol
- Source port number
- Destination port number
- Synchronize/Start (SYN) packet receipt

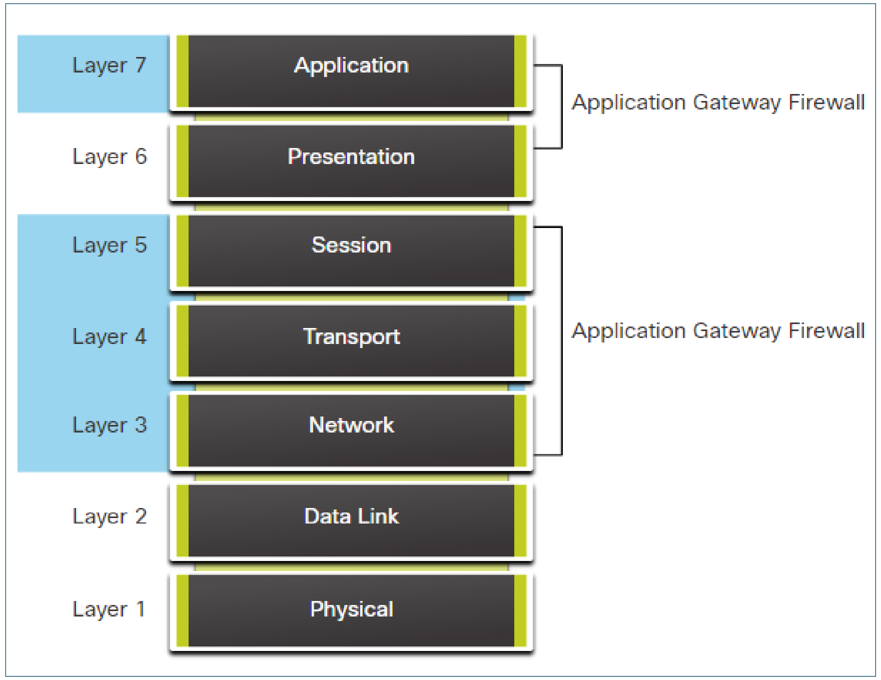
Firewall Type Descriptions (Cont'd)

- **Stateful Firewalls**
  - Stateful firewalls are the most versatile and the most common firewall technologies in use.
  - These firewalls provide stateful packet filtering by using connection information maintained in a state table.



Firewall Type Descriptions (Cont'd)

- **Application gateway firewall (proxy firewall)**
  - Application gateway firewall filters information at Layers 3, 4, 5, and 7 of the OSI reference model.
  - Most of the firewall control and filtering is done in the software.



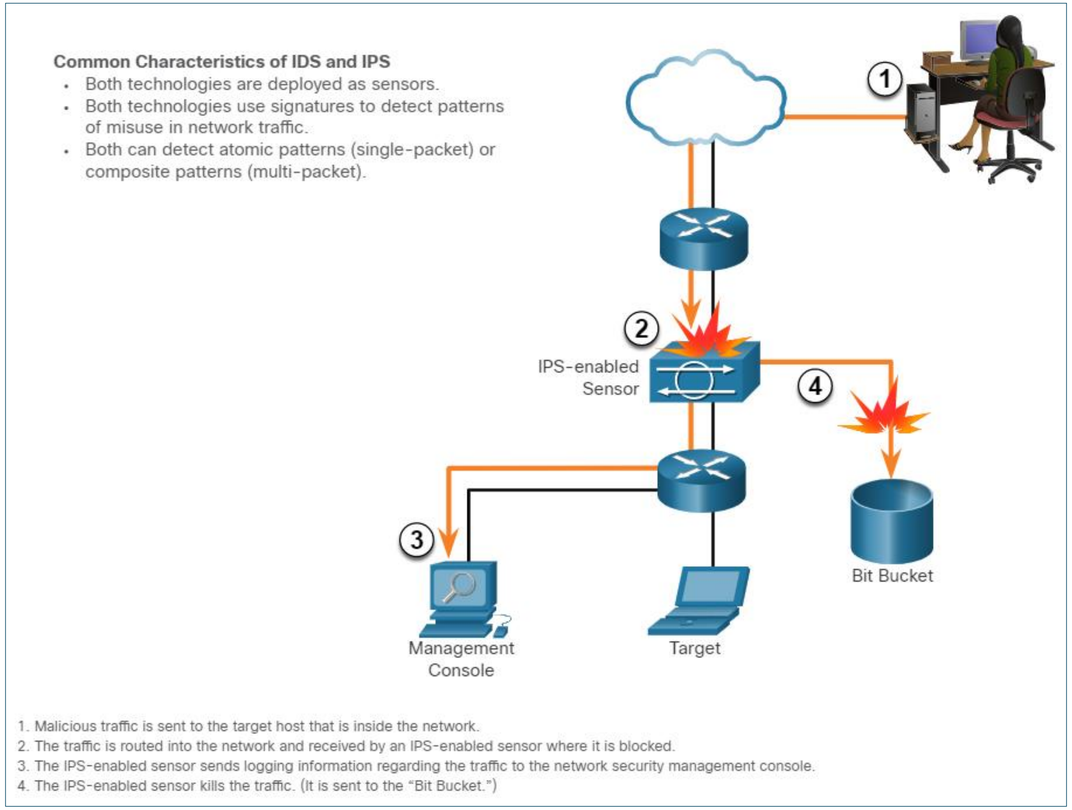
Firewall Type Descriptions (Cont'd)

- **Next-generation firewalls (NGFW)**
  - NGFW go beyond stateful firewalls by providing:
  - Integrated intrusion prevention
  - Application awareness and control to see and block risky apps
  - Upgrade paths to include future information feeds
  - Techniques to address evolving security threats

- Other methods of implementing firewalls include:
  - **Host-based (server and personal) firewall** - A PC or server with firewall software running on it.
  - **Transparent firewall** - Filters IP traffic between a pair of bridged interfaces.
  - **Hybrid firewall** - A combination of various firewall types.

Intrusion Prevention and Detection Devices

- A networking architecture paradigm shift is required to defend against fast-moving and evolving attacks. This must include cost effective and prevention systems such as:
  - **Intrusion Detection Systems (IDS)**
  - **Intrusion Prevention Systems (IPS)**
- The network architecture integrates these solutions into the entry and exit points of the network.
- The figure shows how an IPS device handles malicious traffic.



Common Characteristics of IDS and IPS

- Both technologies are deployed as sensors.
- Both technologies use signatures to detect patterns of misuse in network traffic.
- Both can detect atomic patterns (single-packet) or composite patterns (multi-packet).

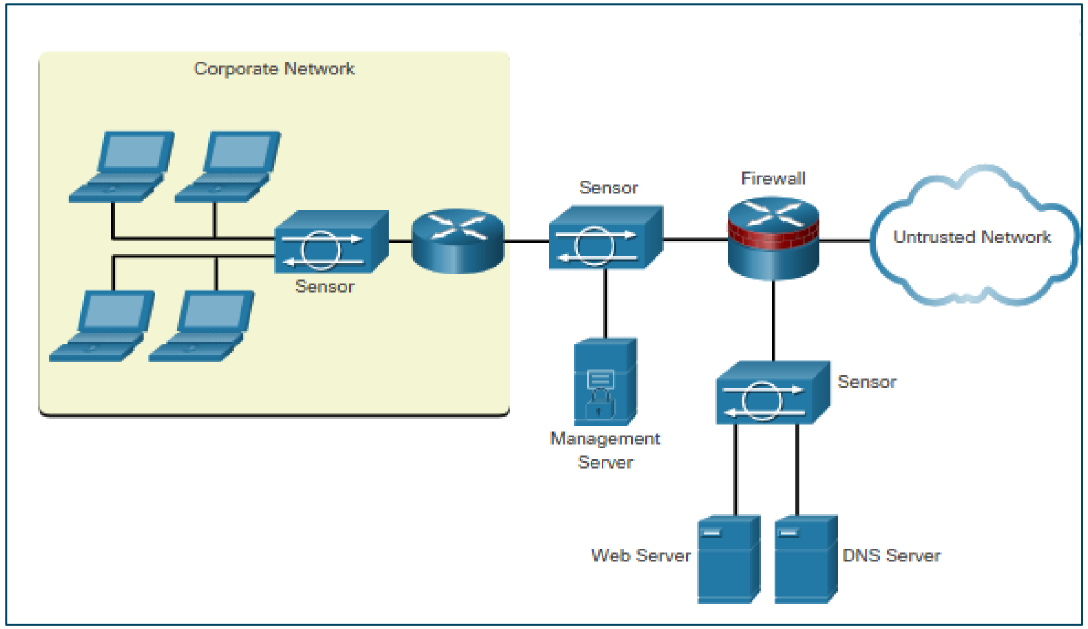
1. Malicious traffic is sent to the target host that is inside the network.
2. The traffic is routed into the network and received by an IPS-enabled sensor where it is blocked.
3. The IPS-enabled sensor sends logging information regarding the traffic to the network security management console.
4. The IPS-enabled sensor kills the traffic. (It is sent to the "Bit Bucket.")

Solution	Advantages	Disadvantages
IDS	• No Impact on network (latency, jitter) • No Network impact if there is a sensor failure • No network impact if there is sensor overload	• Response action cannot stop trigger packets • Correct tuning required for response actions • More vulnerable to network security evasion techniques
IPS	• Stops trigger packets • Can use stream normalization techniques	• Sensor issues might affect network traffic • Sensor overloading impacts the network • Some impact on network (latency, jitter)

Types of IPS

- **Host-based IPS (HIPS):**
  - Software installed on a single host to monitor and analyze suspicious activity.
  - Monitor and protect operating system and critical system processes that are specific to that host.
  - Combine antivirus software, antimalware software, and firewall.
- **Network-based IPS:**
  - Implemented using a dedicated or non-dedicated IPS device.
  - Are a critical component of intrusion prevention.
  - Sensors detect malicious and unauthorized activity in real time and can take action when required.

HIPS	
Advantages	**Disadvantages**
• Provides protection specific to a host operating system • Provides operating system and application level protection • Protects the host after the message is decrypted	• Operating system dependent • Must be installed on all hosts



Network-based IPS

Specialized Security Appliances

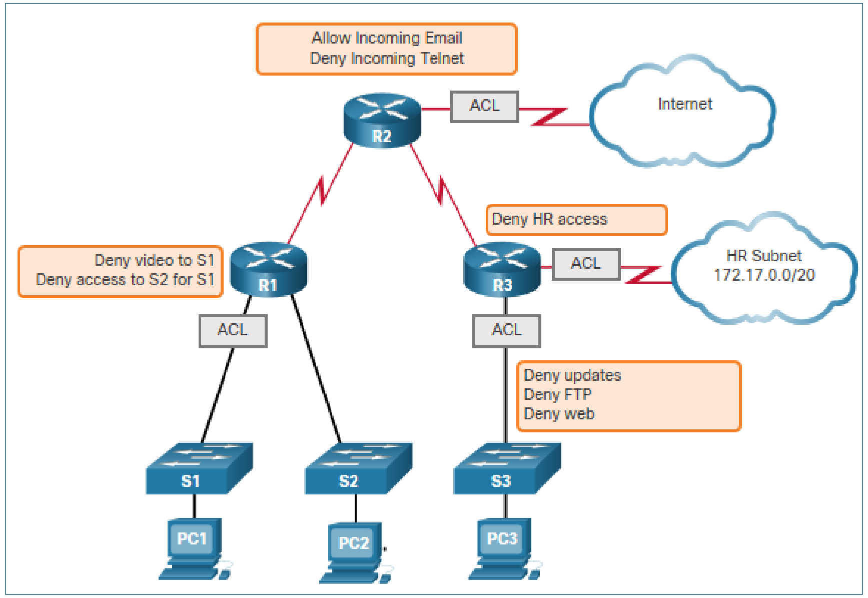
- Few examples of specialized security appliances:

Cisco Advanced Malware Protection (AMP)	Cisco Web Security Appliance (WSA)	Cisco Email Security Appliance (ESA)
An enterprise-class advanced malware analysis and protection solution	A secure web gateway that combines leading protections to help organizations address the growing challenges of securing and controlling web traffic	ESA/Cisco Cloud Email Security helps to mitigate email-based threats and the ESA defends mission-critical email systems **Features**: Global threat intelligence, Spam blocking, Advanced Malware Protection, Outbound Message Control
It provides comprehensive malware protection for organizations before, during, and after an attack	Protects the network by automatically blocking risky sites and testing unknown sites before allowing users to access them	Constantly updated by real-time feeds from Cisco Talos, which detects and correlates threats using a worldwide database monitoring system

Security Services

Traffic Control with ACLs

- An Access Control List (ACL) is a series of commands that control whether a device forwards or drops packets based on information found in the packet header.
- When configured, ACLs perform the following tasks:
  - Limit network traffic to increase network performance.
  - Provide traffic flow control.
  - Provide basic level of security for network access.
  - Filter traffic based on traffic type.
  - Screen hosts to permit or deny access to network services.
- The two types of Cisco IPv4 ACLs are:
  - **Standard ACL** - Used to permit or deny traffic only from source IPv4 addresses.
  - **Extended ACL** - Filters IPv4 packets based on several attributes that include Protocol type, Source IPv4 address, Destination IPv4 address, Source TCP or UDP ports, Destination TCP or UDP ports, Optional protocol type information for finer control
- Standard and extended ACLs can be created using either a number or a name to identify the ACL and its list of statements.

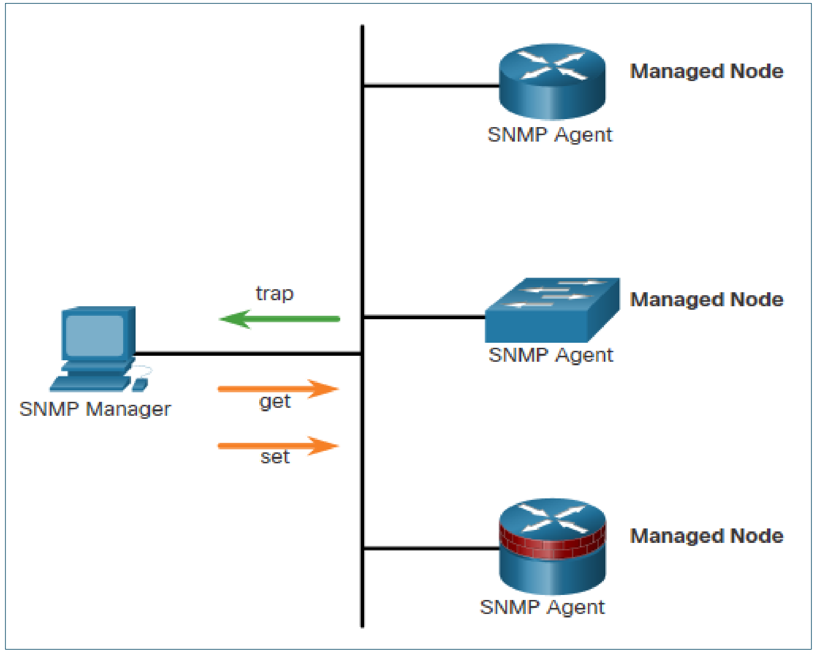


Sample Topology with ACLs applied to routers R1, R2, and R3.

SNMP

- Simple Network Management Protocol (SNMP) is an application layer protocol that provides a message format for communication between managers and agents.

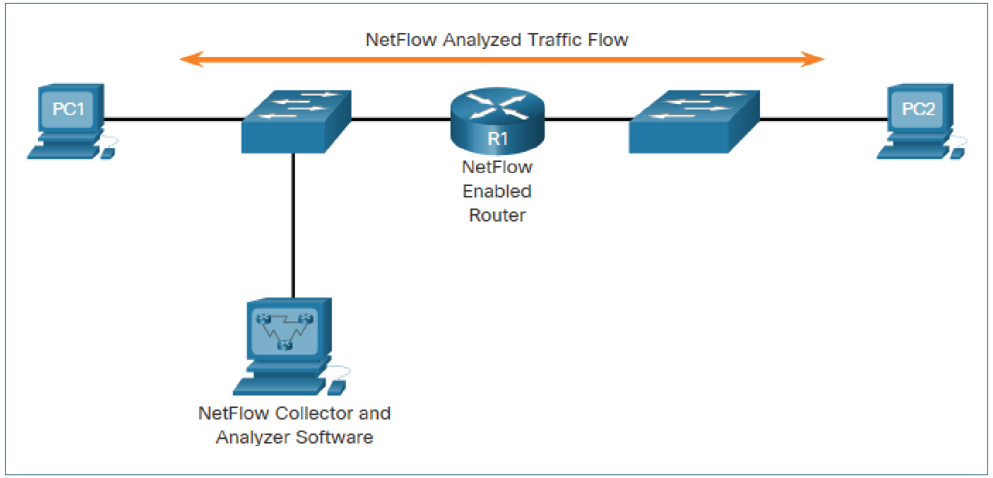
- It allows network administrators to perform the following:
  - Manage end devices such as servers, workstations, routers, switches, and security appliances, on an IP network.
  - Monitor and manage network performance.
  - Find and solve network problems.
  - Plan for network growth.
- The SNMP system consists of two elements:
  - **SNMP manager**: Runs SNMP management software.
  - **SNMP agents**: Nodes being monitored and managed.



NetFlow

- NetFlow is a Cisco IOS technology that provides statistics on packets flowing through a Cisco router or multilayer switch.

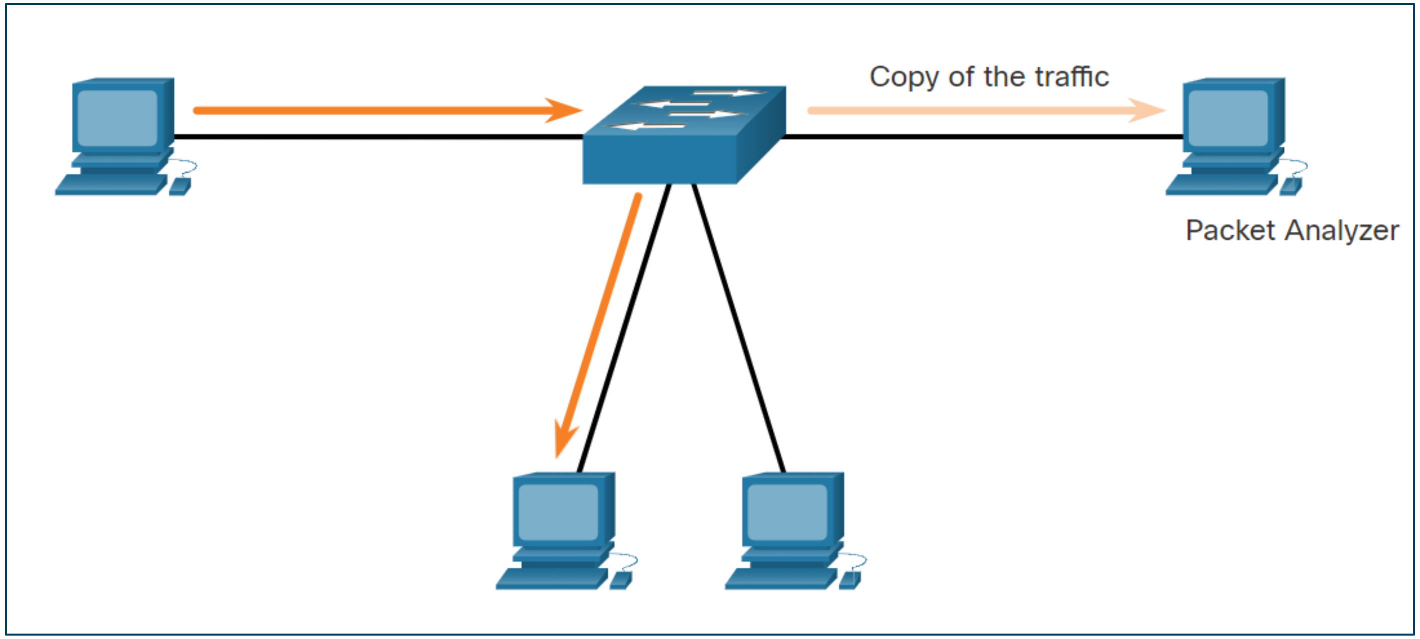
- NetFlow provides data to enable:
  - network and security monitoring,
  - network planning
  - traffic analysis to include identification of network bottlenecks
  - IP accounting for billing purposes.
- NetFlow can monitor application connection, tracking byte and packet counts for that individual application flow.
- It then pushes the statistics over to an external server called a NetFlow collector.


NetFlow Analyzed Traffic Flow
PC1
R1
NetFlow Enabled Router
PC2
NetFlow Collector and Analyzer Software

PC 1 connects to PC 2 using HTTPS

Port Mirroring

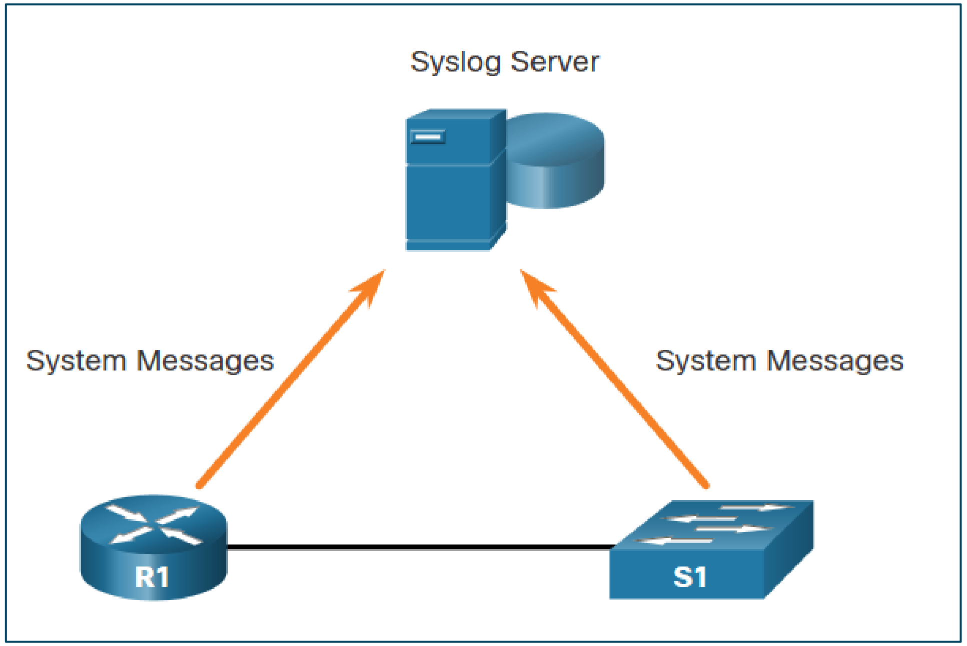
Port mirroring is a feature that allows a switch to make duplicate copies of traffic passing through a switch, and then sending it out a port with a network monitor attached.



Traffic Sniffing using a Switch

Syslog Servers

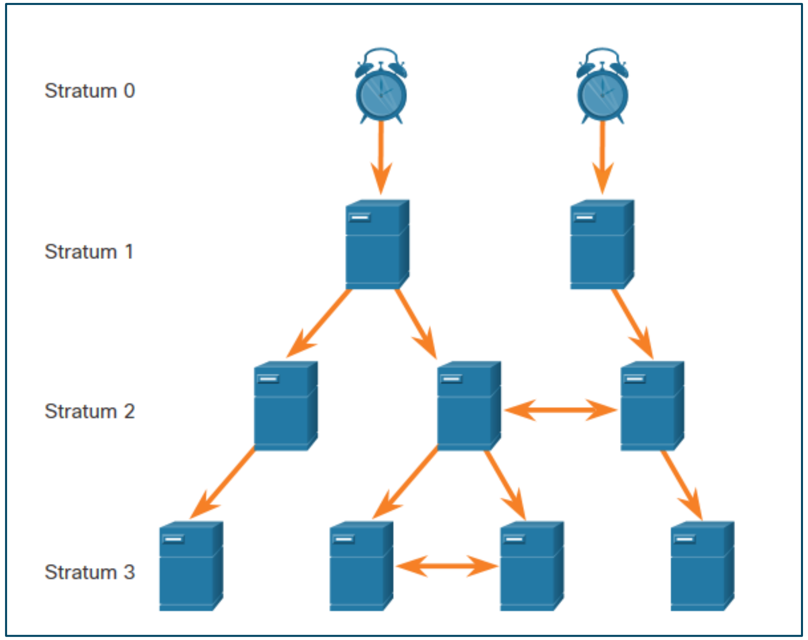
- The most common method of accessing system messages is to use a protocol called syslog.
- The Syslog protocol allows networking devices to send their system messages across the network to syslog servers.
- It provides three primary functions:
  - The ability to gather logging information for monitoring and troubleshooting
  - The ability to select the type of logging information that is captured
  - The ability to specify the destination of captured syslog messages



Syslog

NTP

- It is important to synchronize the time across all devices on the network. The date and time settings on a network device can be set using one of two methods:
  - Manual configuration of the date and time
  - Configuring the Network Time Protocol (NTP)
- NTP networks use a hierarchical system of time sources, where each level in this system is called a stratum. NTP servers are arranged in three levels known as strata:
  - **Stratum 0**: An NTP network gets the time from authoritative time sources.
  - **Stratum 1**: Devices are directly connected to the authoritative time sources.
  - **Stratum 2 and lower strata**: Stratum 2 devices, such as NTP clients, synchronize their time using the NTP packets from stratum 1 servers.



NTP Stratum Levels

AAA Servers

The below table lists the three independent security functions provided by the AAA architectural framework.

Functions	Description
Authentication	• Users and administrators must prove that they are who they say they are. • Authentication can be established using username and password combinations, challenge and response questions, token cards, and other methods. • AAA authentication provides a centralized way to control access to the network.
Authorization	• After the user is authenticated, authorization services determine which resources the user can access and which operations the user is allowed to perform. • An example is “User ‘student’ can access host serverXYZ using SSH only.”
Accounting	• Accounting records what the user does, including what is accessed, the amount of time the resource is accessed, and any changes that were made. • Accounting keeps track of how network resources are used. • An example is "User ‘student’ accessed host serverXYZ using SSH for 15 minutes."

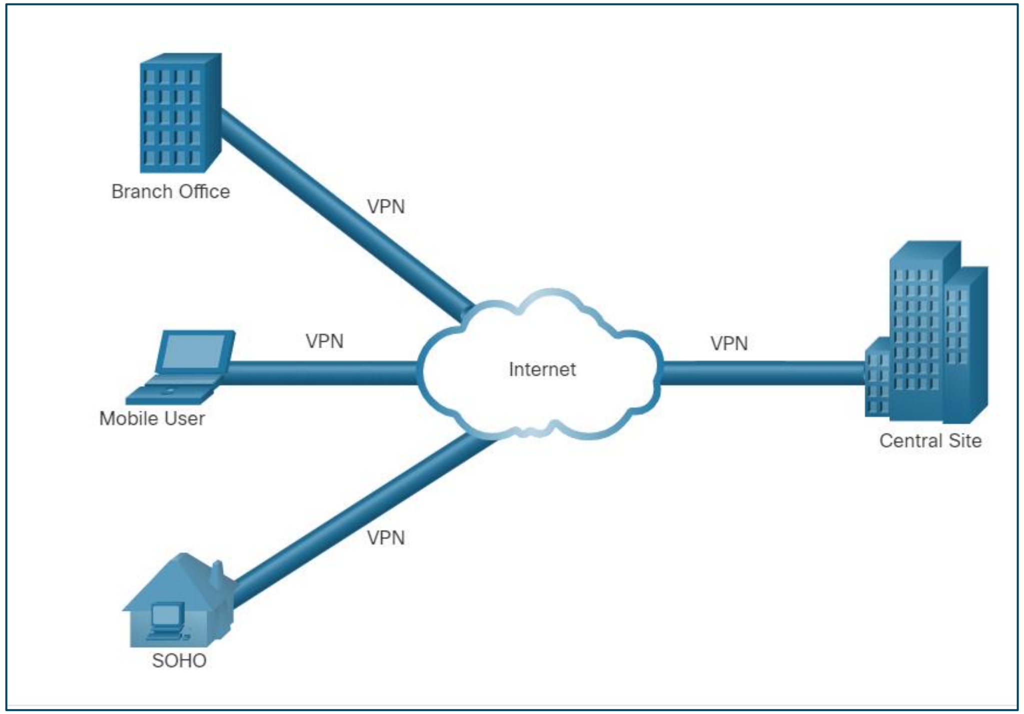
AAA Servers (Cont'd)

The below table lists the difference between Terminal Access Controller Access-Control System Plus (TACACS+) and Remote Authentication Dial-In User Service (RADIUS) protocols.

	TACACS+	RADIUS
Functionality	Separates AAA according to the AAA architecture,	Combines authentication and authorization but separates accounting,
Standard	Mostly Cisco supported	Open/RFC standard
Transport	TCP	UDP
Protocol CHAP	Bidirectional challenge and response as used in Challenge Handshake Authentication Protocol (CHAP)	Unidirectional challenge and response from the RADIUS security server to the RADIUS client
Confidentiality	Entire packet encrypted	Password encrypted
Customization	Provides authorization of router commands on per-user or per-group basis	No option to authorize router commands on a per-user or per-group basis
Accounting	Limited	Extensive

VPN

- A VPN is a private network that is created over a public network (usually the internet).
- A VPN uses virtual connections routed through the Internet from the organization to the remote site.
- A VPN is a communications environment in which access is strictly controlled to permit peer connections within a defined community of interest.
- Confidentiality is achieved by encrypting the traffic within the VPN.
- In short, VPN connects two endpoints over a public network, to form a logical connection which can be made at Layer 2 or Layer 3.

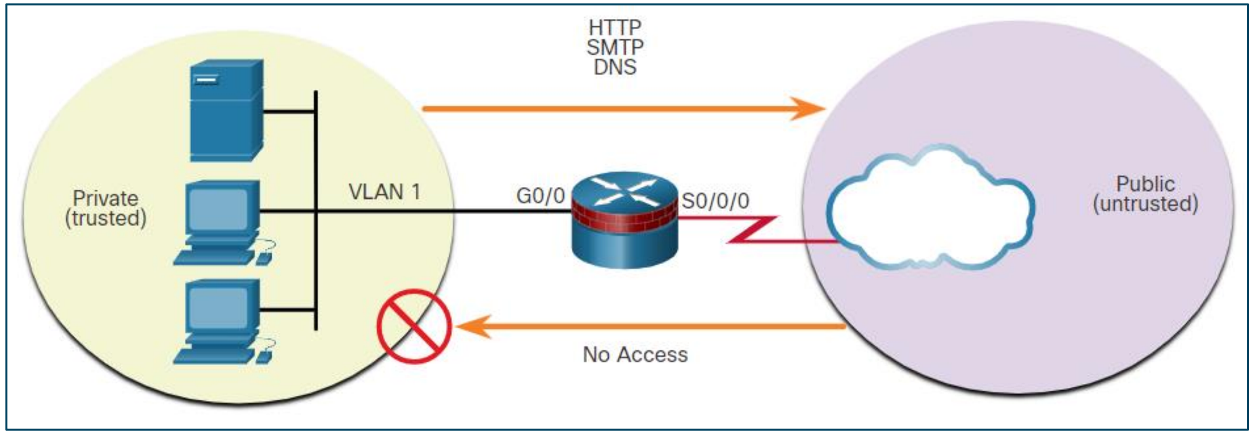


Virtual Private Network

Security Architectures

Common Security Architectures

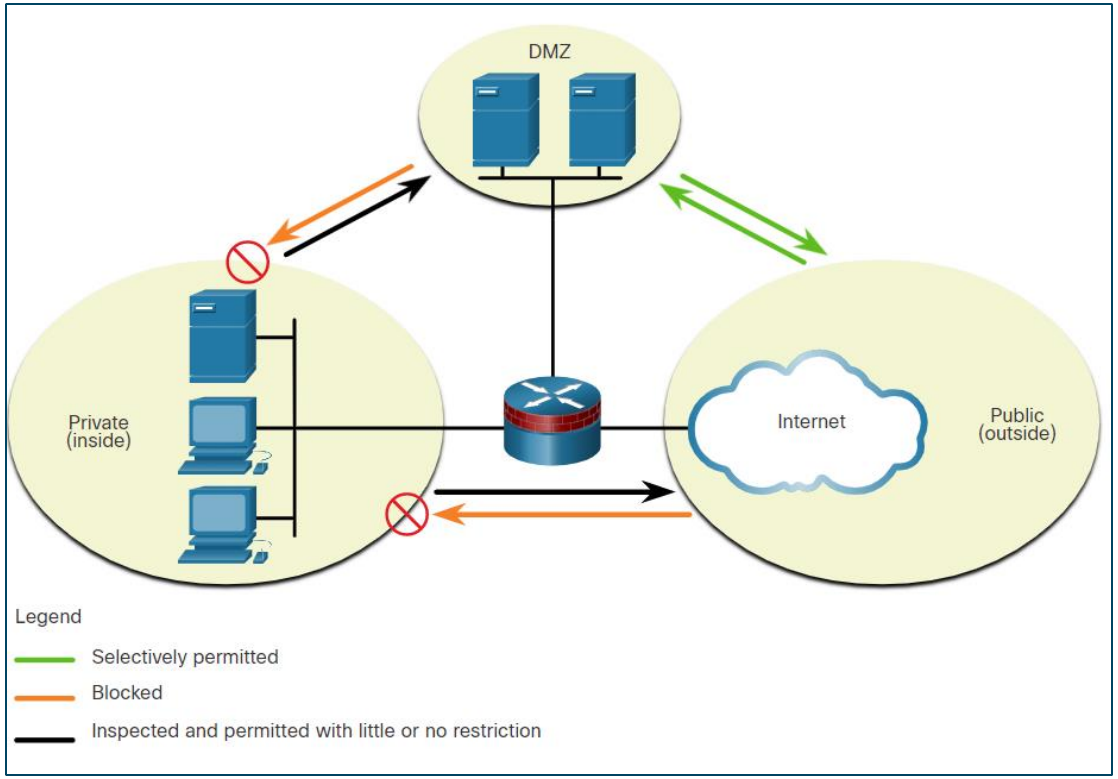
- Firewall design is primarily about device interfaces permitting or denying traffic based on the source, the destination, and the type of traffic. Some designs are as simple as designating an outside network and inside network. A firewall with two interfaces is configured as follows:
  - The **public** network (or outside network) is untrusted, and the **private** network (or inside network) is trusted.
  - Traffic originating from the private network is permitted and inspected as it travels toward the public network. Inspected traffic returning from the public network and associated with traffic that originated from the private network is permitted.
  - Traffic originating from the public network and traveling to the private network is generally blocked.



Public and Private

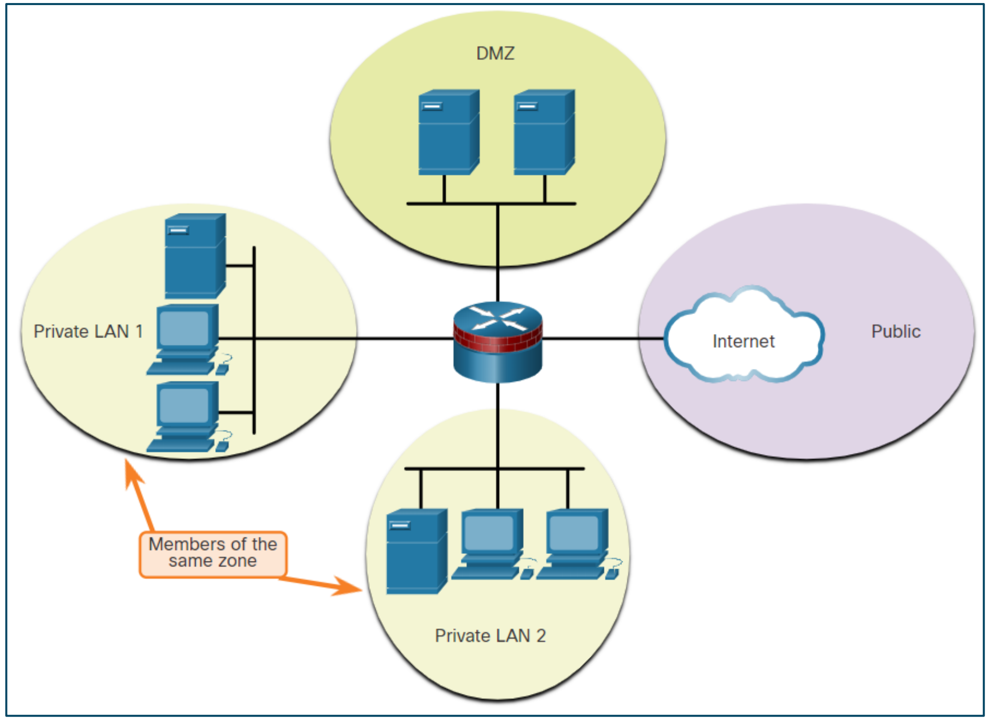
Common Security Architectures (Cont'd)

- A **demilitarized zone (DMZ)** is a firewall design where there is typically one inside interface connected to the private network, one outside interface connected to the public network, and one DMZ interface:
  - Traffic originating from the private network is inspected as it travels toward the public or DMZ network. This traffic is permitted with little or no restriction. Return traffic is usually permitted.
  - Traffic originating from the DMZ network and traveling to the private network is usually blocked.
  - Traffic originating from the DMZ network and traveling to the public network is selectively permitted based on service requirements.
  - Traffic originating from the public network and traveling toward the DMZ is selectively permitted and inspected. Return traffic is dynamically permitted.
  - Traffic originating from the public network and traveling to the private network is blocked.



Common Security Architectures (Cont'd)

- **Zone-based Policy Firewalls (ZPFs)**
  - ZPFs use the concept of zones to provide additional flexibility.
  - A zone is a group of one or more interfaces that have similar functions or features.
  - Zones help to specify where a Cisco IOS firewall rule or policy should be applied



AMERICAN INTERNATIONAL UNIVERSITY
PRAESIDIUM
DISCIPLINA CIVITATIS
1994
BANGLADESH

cisco Networking Academy

ice.aiub.edu

ice@aiub.edu

☎ 01630-665666