



# Chapter 5: Network Infrastructure

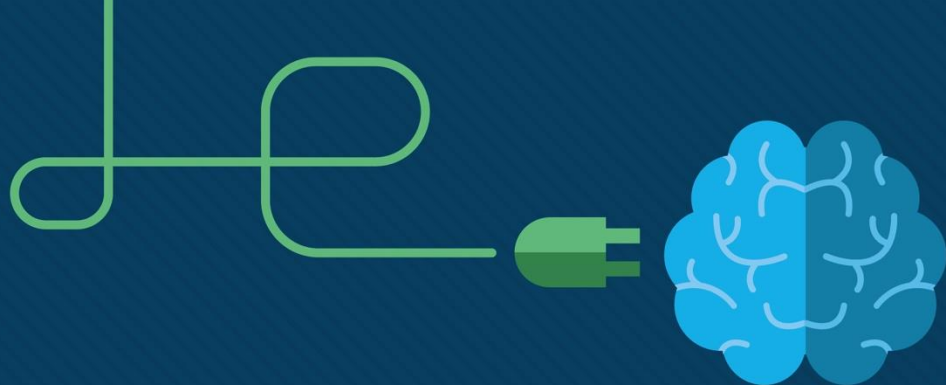
## Instructor Materials

CCNA Cybersecurity Operations v1.1



# Chapter 5: Network Infrastructure

**CCNA Cybersecurity Operation v1.1**  
**Planning Guide**



# Chapter 5: Network Infrastructure

CCNA Cybersecurity Operations v1.1



# Chapter 5 - Sections & Objectives

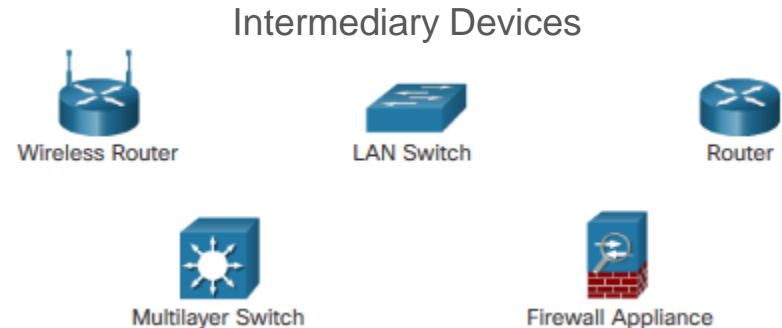
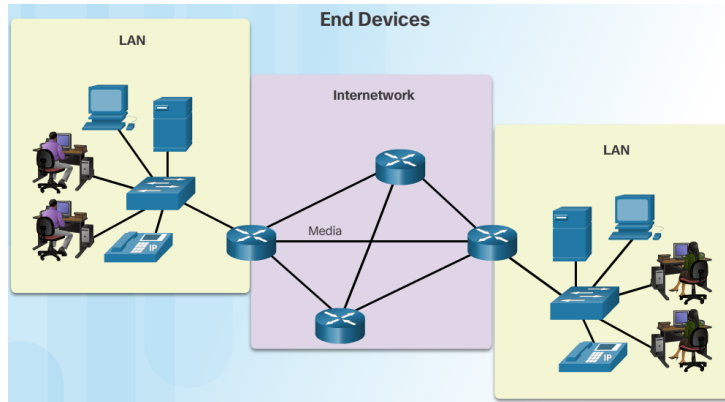
- 5.1 Network Communication Devices
  - Explain how network devices enable wired and wireless network communication.
    - Explain how network devices enable network communication.
    - Explain how wireless devices enable network communication.
- 5.2 Network Security Infrastructure
  - Explain how devices and services are used to enhance network security.
    - Explain how specialized devices are used to enhance network security.
    - Explain how network services enhance network security.
- 5.3 Network Representation
  - Explain how networks and network topologies are represented.
  - Explain how network designs are represented by interconnected symbols.

# 5.1 Network Communication Devices

# Network Devices

## End Devices

- End Devices:
  - Computers, laptops, servers, printers, smart devices, and mobile devices.
  - Individual end devices are connected to the network by intermediary devices.
- Intermediary Devices:
  - Connect the individual end devices to the network and also connect multiple individual networks to form an internetwork.
  - Provide connectivity and ensure that data flows across the network.



# Video Tutorial – End Devices

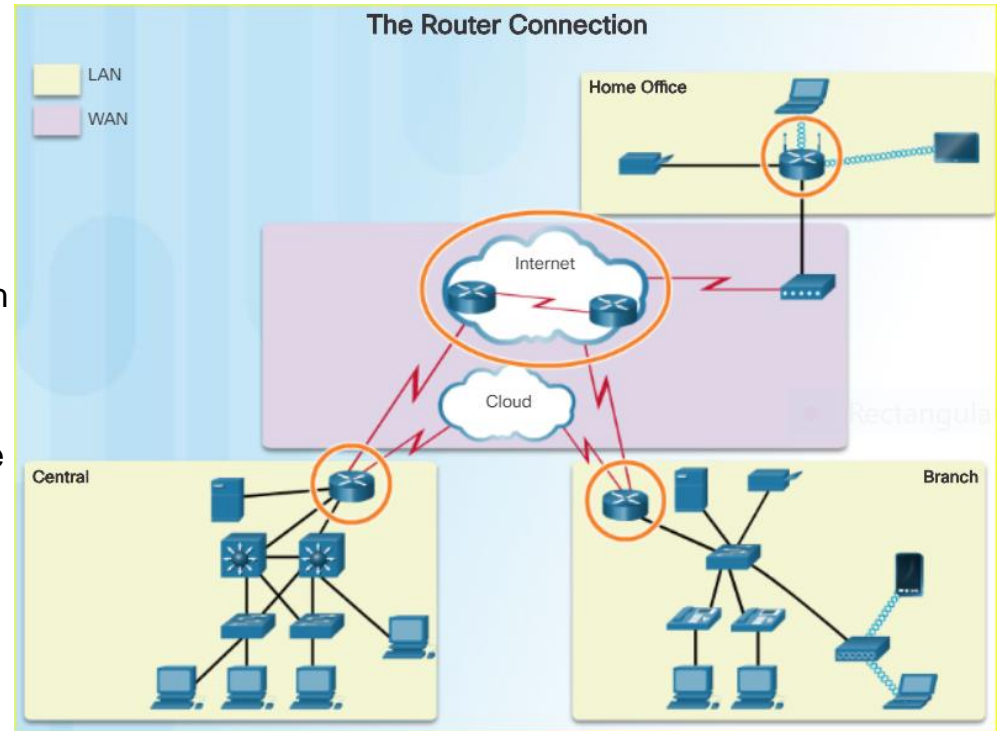
- End device is any device on the network that initiates communication, either source or destination.
- Intermediary devices connect the end devices to the network, provide connectivity, and ensure data flow.



# Network Devices

## Routers

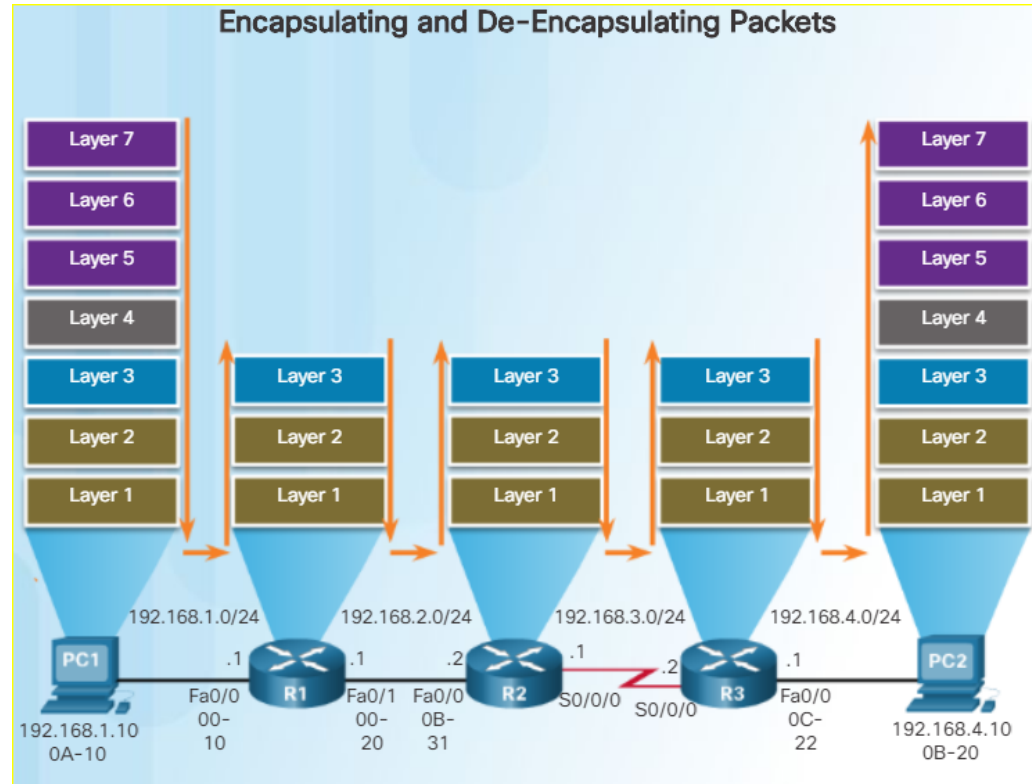
- **Function of a Router:**
  - Provides path determination and packet forwarding.
  - Responsible for encapsulating and de-encapsulating packets.
  - Uses a routing table to determine the best path to use to send packets to a specified network.
- **Routing Table:**
  - Contains directly connected routes 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.





## Routers (Cont.)

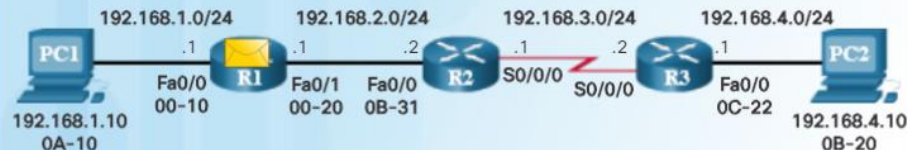
- The router performs the following three major steps:
  1. It de-encapsulates the Layer 2 frame header and trailer to expose the Layer 3 packet.
  2. It examines the destination IP address of the IP packet to find the best path in the routing table.
  3. If the router finds a path to the destination, 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.



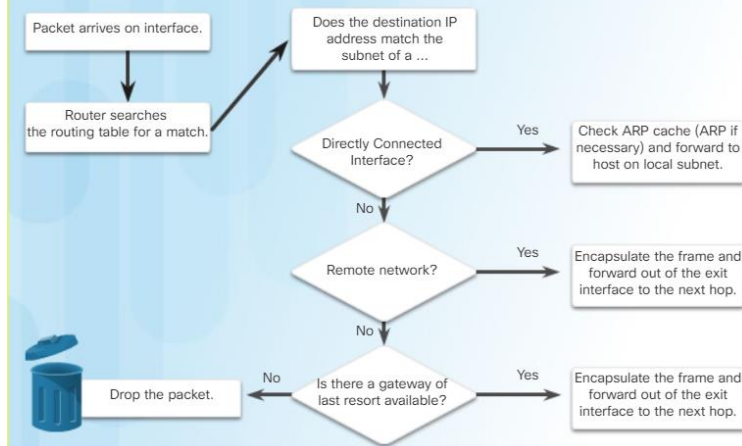
## Router Operation

- A primary function of a router is to determine the best path to use to send packets to each subnet. To determine the best path, the router searches its routing table for a network address that matches the destination IP address of the packet. The routing table search results in one of three path determinations:
  - **Directly connected network**
  - **Remote network**
  - **No route determined**

PC1 Builds a Packet to Send to PC2

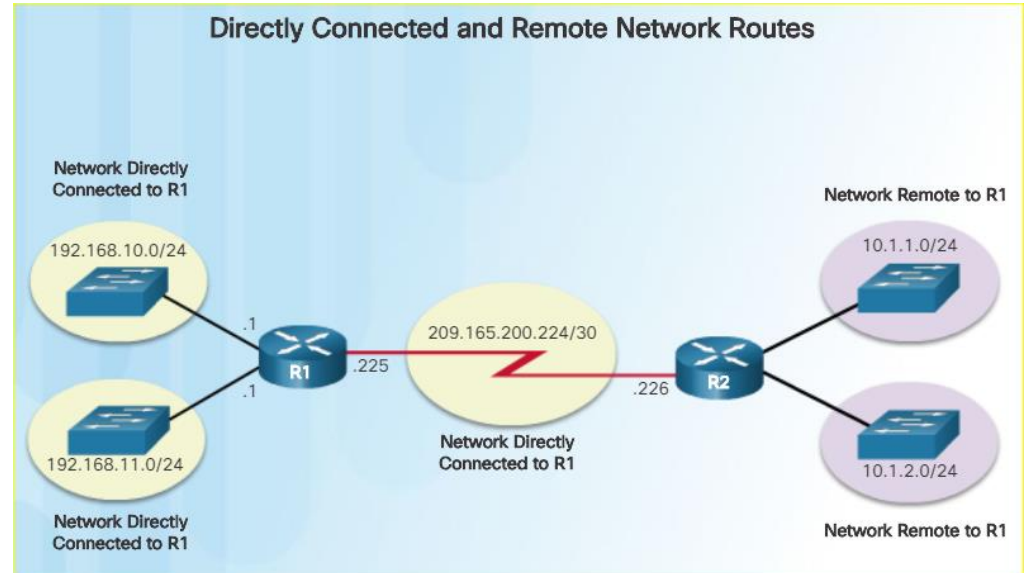


Packet Forwarding Decision Process



# Routing Information

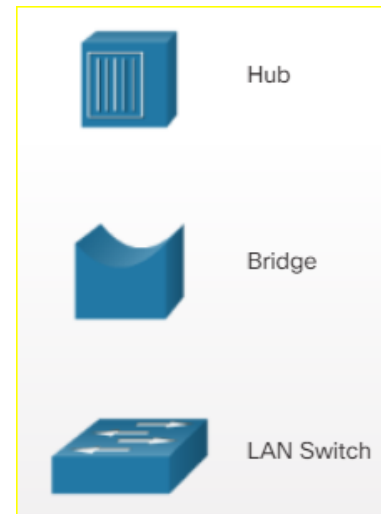
- The routing table of a router stores the following information:
  - **Directly connected routes**
  - **Remote routes**
- The destination network entries in the routing table can be added in several ways:
  - **Local Route interfaces** – These are added when an interface is configured and active.
  - **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

- 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 essentially multiport bridges that connect devices into a star topology. Like bridges, switches segment a LAN into separate collision domains, one for each switch port. A switch makes forwarding decisions based on Ethernet MAC addresses.



# Network Devices

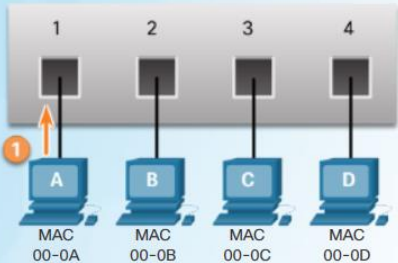
## Switching Operation

### Learn: Examine Source MAC Address

MAC Address Table	
Port	MAC Address
1	00-0A

Port and Source MAC address added

2



Destination MAC 00-0D	Source MAC 00-0A	Type	Data	FCS
--------------------------	---------------------	------	------	-----

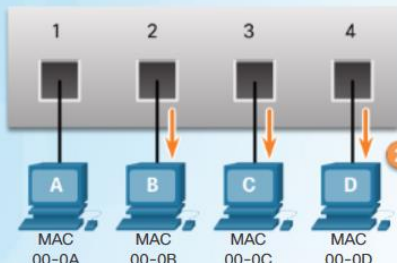
MAC addresses are shortened for demonstration purposes.

### Forward: Examining the Destination MAC Address

MAC Address Table	
Port	MAC Address
1	00-0A

Destination MAC address not in table

1



Destination MAC 00-0D	Source MAC 00-0A	Type	Data	FCS
--------------------------	---------------------	------	------	-----

MAC addresses are shortened for demonstration purposes.

# Video Tutorial – MAC Address Tables on Connected Switches

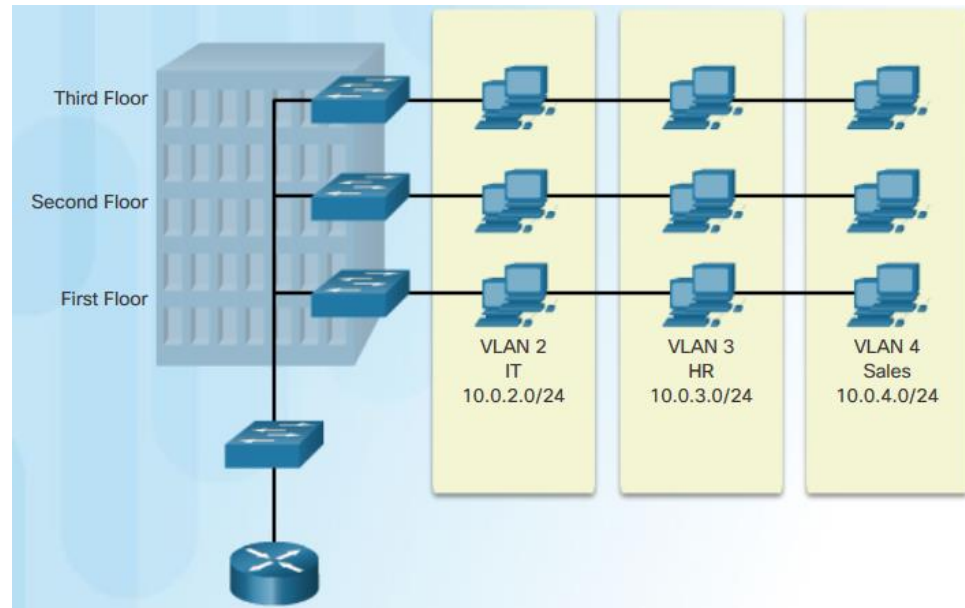
- A switch can have multiple MAC addresses associated with a single port.
- The switch will have a separate MAC address table entry for each frame received with a different source MAC address.





# VLANs

- Segments networks based on multiple factors (function, project team, or application) regardless of physical location.
- Creates logical broadcast domains that can span multiple physical LAN segments.
- Improves network performance by separating large broadcast domains into smaller ones.
- Prevents users on different VLANs from snooping on each other's traffic.

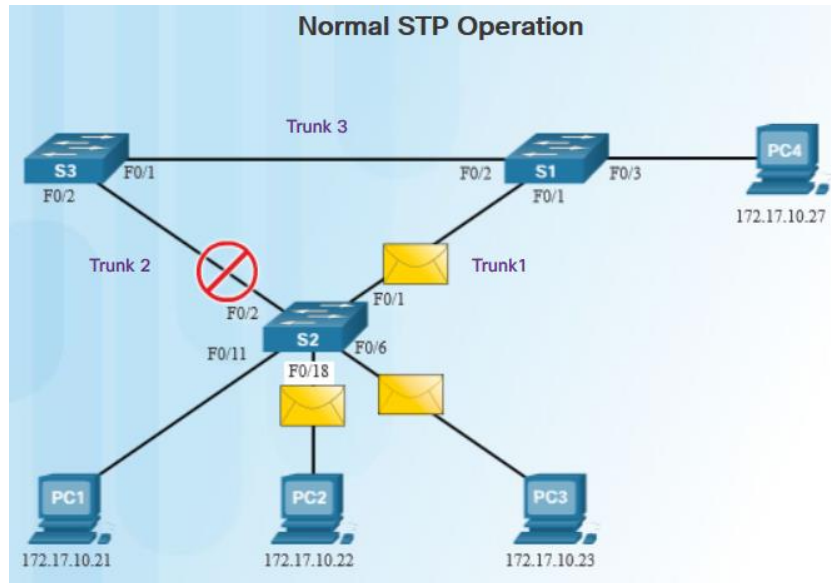




# Network Devices

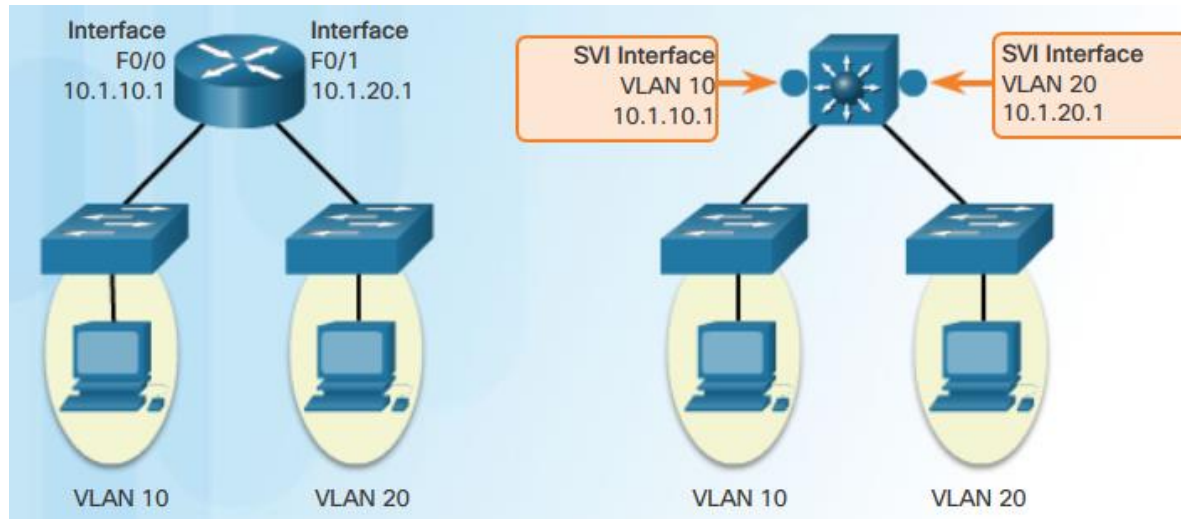
## STP

- Spanning Tree Protocol (STP)
  - Ensures a single logical pathway between all destinations on a network by blocking redundant paths.
  - Prevents loops using strategically placed "blocking-state" ports.
  - Uses bridge protocol data unit (BPDU) frames to prevent loops.



# Multilayer Switching

- Multilayer switches support routed ports and Switched Virtual Interfaces (SVIs) to forward frames based on Layer 3 information.
  - **Routed Ports** – physical port acts like an interface on a router, not associated with any VLANs.
  - **SVI** – virtual interface can be configured for any VLAN within a multilayer switch.



# Video Tutorial – Wireless Communications

- Wireless LAN controller:
  - Offers centralized management configuration deployment over the Lightweight Access Points.
  - Controls Lightweight Access Points using the Lightweight Access Point Protocol.



# Wireless Communications

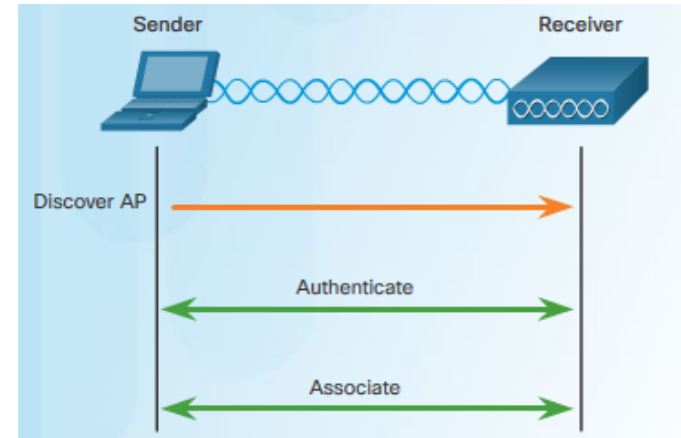
## Protocols and Features

- 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 Ethernet LANs
Physical Layer	Radio Frequency (RF)	Cable
Media Access	Collision Avoidance	Collision Detection
Availability	Anyone with a radio NIC in range of an access point	Cable connection required
Signal Interference	Yes	Inconsequential
Regulation	Additional regulation by country authorities	IEEE standard dictates

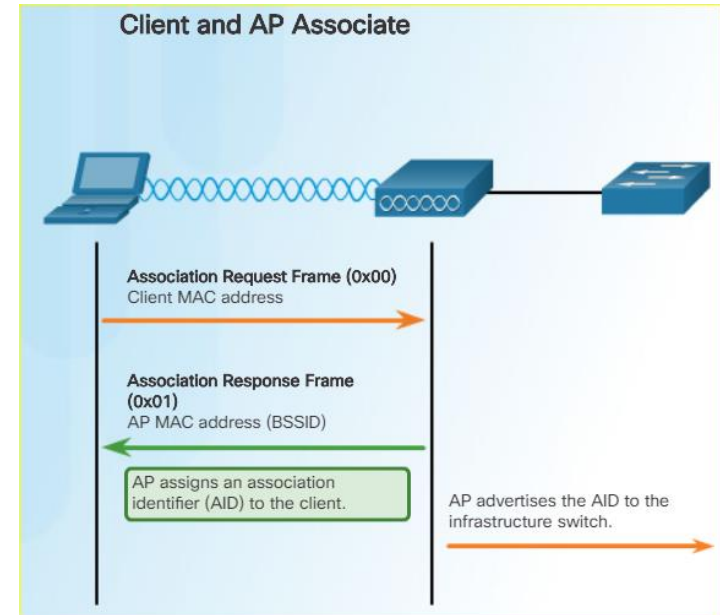
# Wireless Network Operations

- Wireless client association process with AP includes discovering a new wireless AP, authenticating with that AP, then associating with that AP.
- Common configurable wireless parameters include:
  - Network mode**
  - SSID**
  - Channel settings**
  - Security mode**
  - Encryption**
  - Password**
- Wireless devices must discover and connect to an AP or wireless router. This process can be passive or active.
- The 802.11 standard was originally developed with two authentication mechanisms: **open authentication** provides wireless connectivity to any wireless device, and the **shared key authentication** technique is based on a key that is pre-shared between the client and the AP.



# The Client to AP Association Process

- A wireless client goes through a three-stage process to associate with an AP.
- Discovery: A wireless client locates the AP to associate.
- Authentication:
  - The wireless client sends an authentication frame to the AP.
  - The AP responds with a challenge text.
  - The client encrypts the message using its shared key and returns the encrypted text back to the AP.
  - The AP then decrypts the encrypted text using its shared key.
  - If the decrypted text matches the challenge text, the AP authenticates the client.
- Association:
  - The wireless client forwards an Association Request frame that includes its MAC address.
  - The AP responds with an Associate Response that includes the AP MAC address.
  - The AP maps a logical port to the wireless client.



# Wireless Devices – AP, LWAP, WLC

- Access Point (AP):
  - **Small network** – usually a wireless router that integrates the functions of a router.
  - **Large network** – can be many APs.
- Wireless LAN Controller (WLC):
  - Controls and manages the functions of the APs on a network.
  - Simplifies configuration and monitoring of numerous APs.
- Lightweight AP (LWAP):
  - Centralized management by WLC.
  - No longer acts autonomously.



# 5.2 Network Security Infrastructure



# Video Tutorial – Security Devices

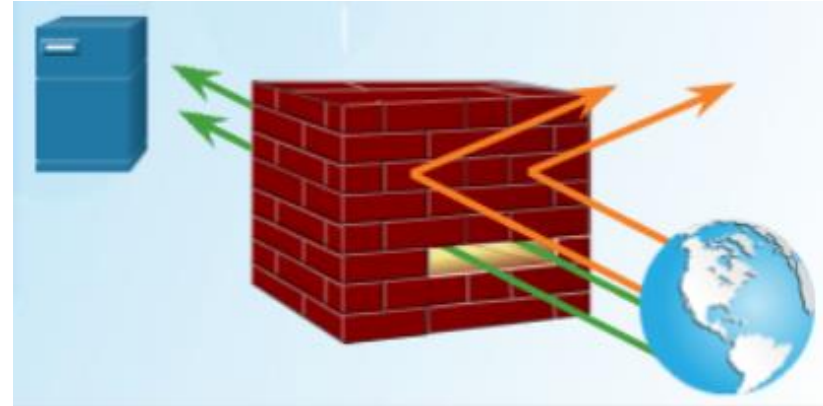
- Access Layer:
  - Port security, dynamic ARP inspection and DHCP snooping
- Distribution Layer
  - Access lists for a Layer 3 firewall
  - Layer 4 stateful firewall
  - Permitting and denying traffic based on IP addressing, and TCP and UDP ports.
- Core Layer
  - **Proxy Firewall** – inspect traffic
  - **Web proxy firewall** – inspect web traffic
  - **Email proxy firewall** – spam detection
  - **SSL security appliance** – decrypt HTTPS traffic
  - **IDS** – offline scanning against network attack signatures
- Wireless network
  - WPA2 encryption and authentication



# 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.

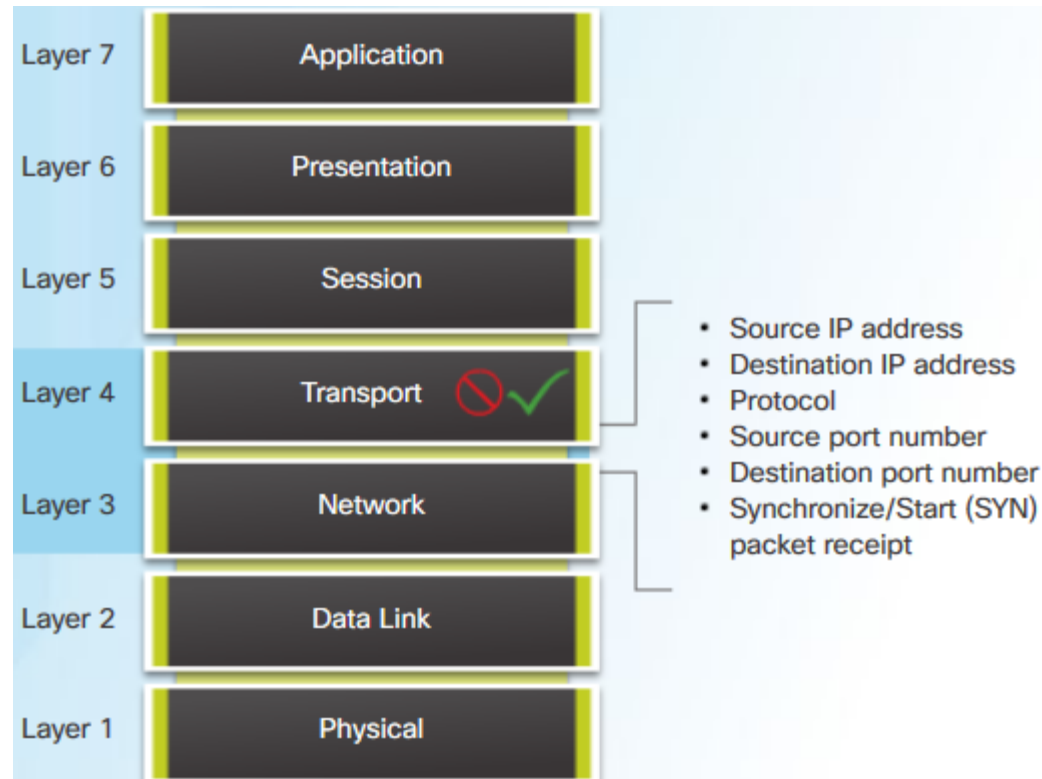


# Firewall Type Descriptions

- **Packet filtering (Stateless) firewalls** - usually part of a router firewall, which permits or denies traffic based on Layer 3 and Layer 4 information.
- **Stateful firewalls:**
  - Allows or blocks traffic based on state, port, and protocol.
  - Monitors all activity from the opening of a connection until it is closed.
- **Application gateway firewalls (Proxy firewall)** - filters information at Layers 3, 4, 5, and 7 of the OSI reference model.
- **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 the various firewall types.

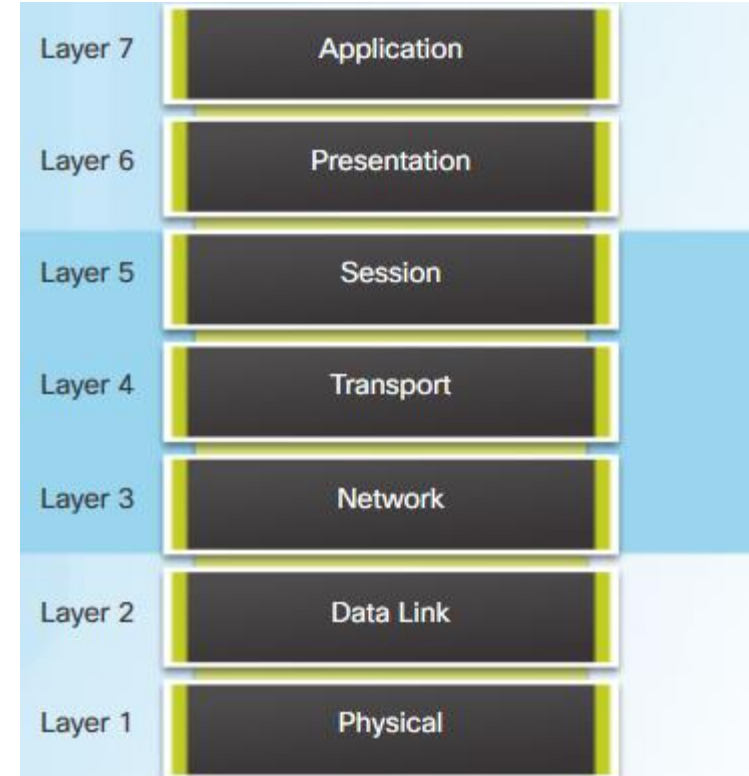
# Packet Filtering Firewalls

- Usually part of a router firewall, which permits or denies traffic based on Layer 3 and Layer 4 information.
- Are stateless firewalls that use a simple policy table look-up that filters traffic based on specific criteria.



# Stateful Firewalls

- The most versatile and common firewall technology in use.
- Provides stateful packet filtering by using connection information maintained in a state table.
- Classified at the network layer but also analyzes traffic at OSI Layer 4 and Layer 5.



# Next-Generation Firewalls

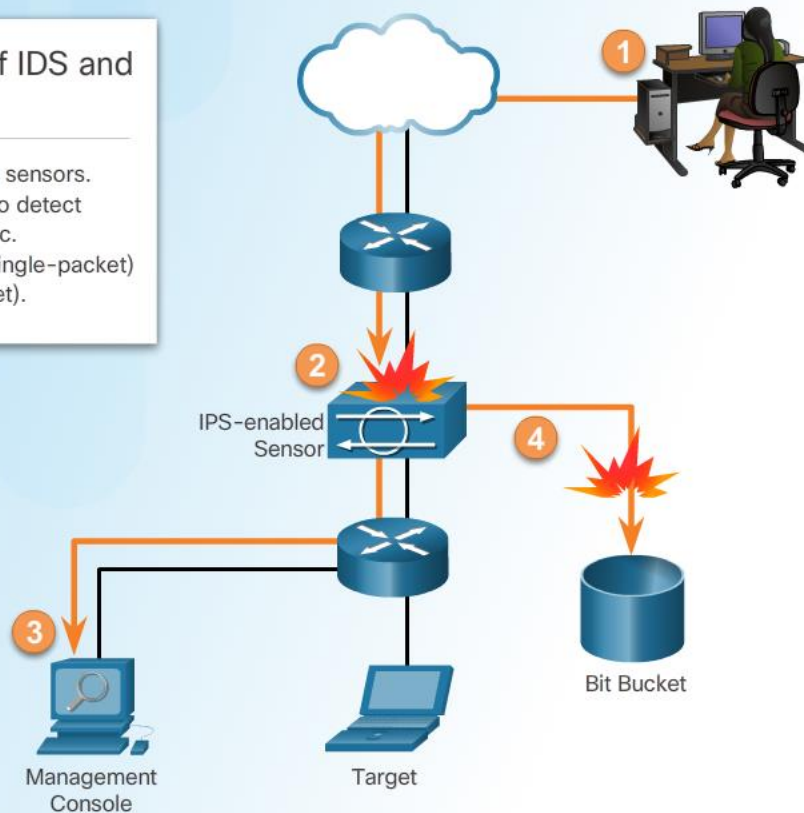
- Provide standard firewall capabilities like stateful inspection.
- Contain integrated intrusion prevention.
- Use application awareness and control to see and block risky apps.
- Upgrade paths to include future information feeds.
- Implement techniques to address evolving security threats.



# Intrusion Prevention and Detection Devices

### 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).



# Advantages and Disadvantages of IDS and IPS

	Advantages	Disadvantages
IDS	<ul style="list-style-type: none"><li>▪ No impact on network (latency, jitter)</li><li>▪ No network impact if there is a sensor failure</li><li>▪ No network impact if there is sensor overload</li></ul>	<ul style="list-style-type: none"><li>▪ Response action cannot stop trigger packets</li><li>▪ Correct tuning required for response actions</li><li>▪ More vulnerable to network security evasion techniques</li></ul>
IPS	<ul style="list-style-type: none"><li>▪ Stops trigger packets</li><li>▪ Can use stream normalization techniques</li></ul>	<ul style="list-style-type: none"><li>▪ Sensor issues might affect network traffic</li><li>▪ Sensor overloading impacts the network</li><li>▪ Some impact on network (latency, jitter)</li></ul>



# 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.

	Advantages	Disadvantages
Host-Based IPS	<ul style="list-style-type: none"><li>• Provides protection specific to a host operating system</li><li>• Provides operating system and application level protection</li><li>• Protects the host after the message is decrypted</li></ul>	<ul style="list-style-type: none"><li>• Operating system dependent</li><li>• Must be installed on all hosts</li></ul>

# Specialized Security Appliances

- Cisco Advanced Malware Protection (AMP):
  - Is enterprise-class advanced malware analysis and protection solution.
  - Provides comprehensive malware protection for organizations before, during, and after an attack.
- Cisco Web Security Appliance (WSA) with Cloud Web Security (CWS):
  - WSA protects the network by automatically blocking risky sites and testing unknown sites before allowing users to access them.
  - WSA provides malware protection, application visibility and control, acceptable use policy controls, insightful reporting and secure mobility.
  - CWS enforces secure communication to and from the Internet.
  - CWS provides remote workers the same level of security as onsite employees.
- Cisco Email Security Appliance (ESA):
  - Defends mission-critical email systems.
  - Detects and correlates threats using a worldwide database monitoring system.



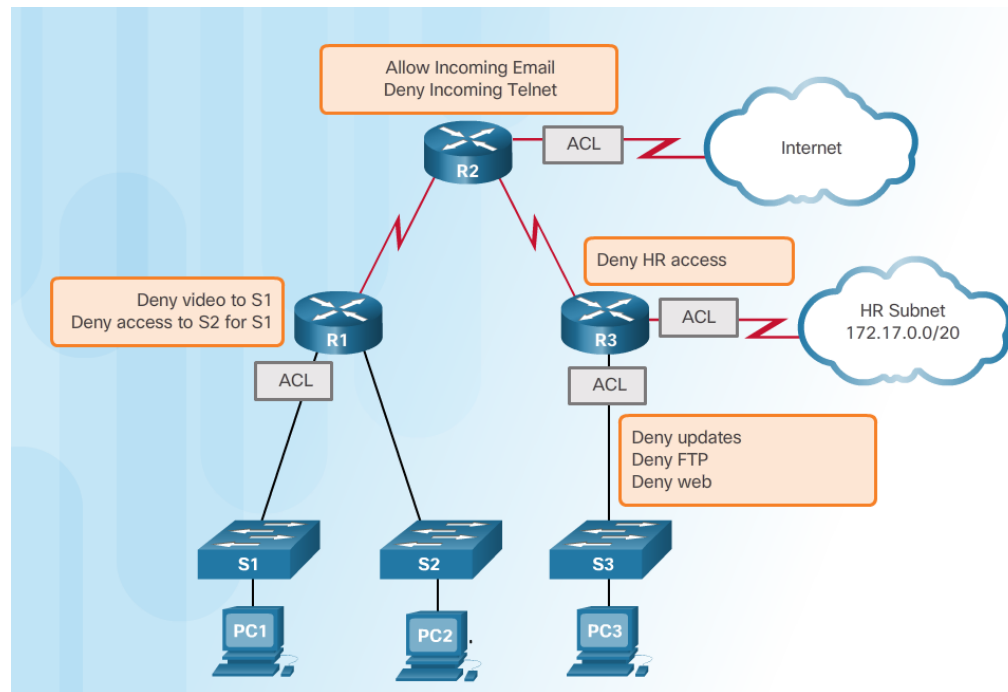
# Video Tutorial - Security Services

- Intrusion Detection System (IDS) scans packets against security signatures looking for network attacks.
- Authentication, Authorization, and Accounting (AAA) is a server that is configured to handle all user account authentication on the network.
- Netflow collects information in the packet headers, such as IP address, TCP UDP port numbers, type of service field, and protocol information on ingress and egress traffic.
- Simple Network Management Protocol (SNMP) can read information and monitor devices on the network which have been configured as SNMP agents.



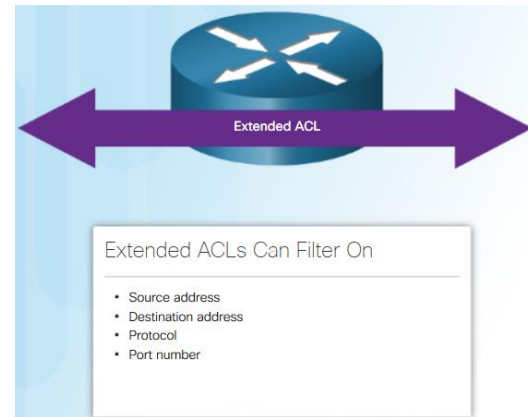
# Traffic Control with ACLs

- Access Control Lists (ACLs) - Is a series of commands that control whether a device forwards or drops packets based on information found in the packet header:
  - Limit network traffic to increase network performance.
  - Provide traffic flow control.
  - Provide a basic level of security for network access.
  - Filter traffic based on traffic type.
  - Screen hosts to permit or deny access to network services.



# ACLs: Important Features

- The two types of Cisco IPv4 ACLs are standard and extended.
- Standard ACLs can be used to permit or deny traffic only from source IPv4 addresses. Extended ACLs filter 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.
- An ACL message can be generated and logged when traffic meets the permit or deny criteria defined in the ACL.

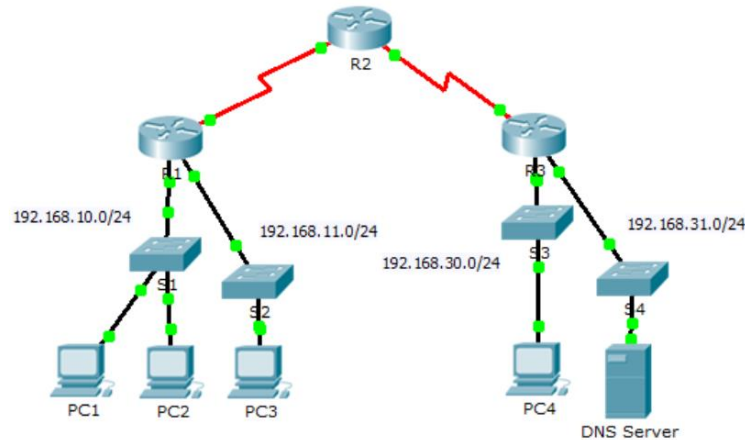


# Packet Tracer – ACL Demonstration



## Packet Tracer – Access Control List Demonstration

### Topology



### Objectives

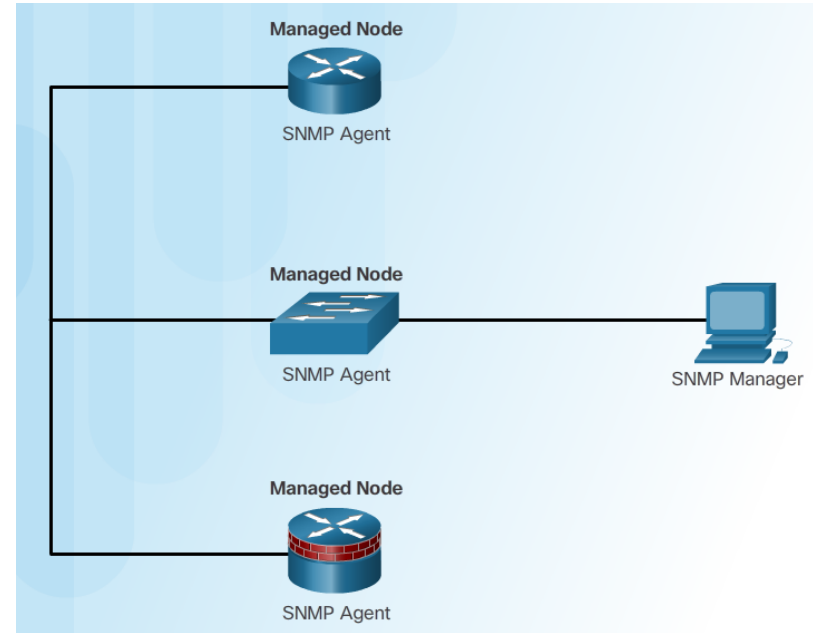
**Part 1: Verify Local Connectivity and Test Access Control List**

**Part 2: Remove Access Control List and Repeat Test**

## Security Services

# SNMP

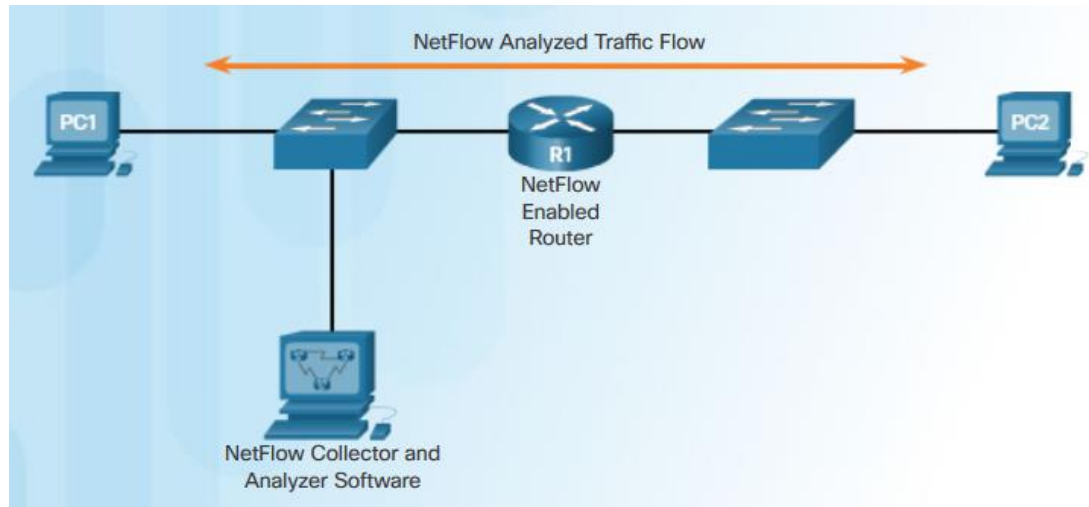
- SNMP allows administrators to manage end devices such as servers, workstations, routers, switches, and security appliances.
- The SNMP system consists of three elements:
  - Manager that runs SNMP management software.
  - Agents which are the nodes being monitored and managed.
  - Management Information Base (MIB) – this is a database on the agent that stores data and operational statistics about the device.



## Security Services

# NetFlow

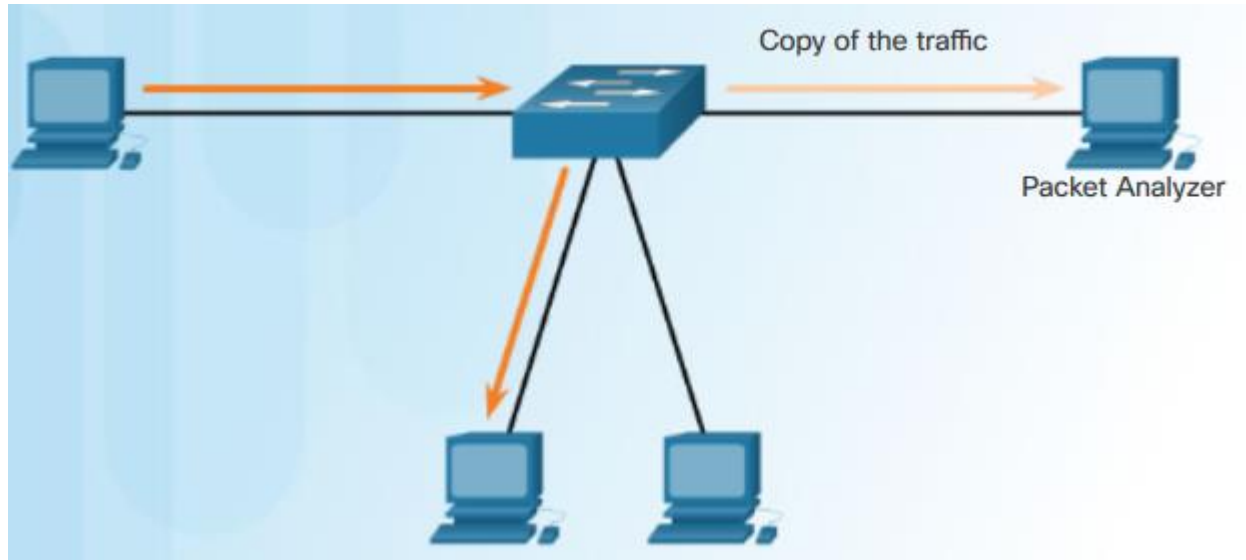
- A Cisco IOS technology that provides statistics on packets flowing through a Cisco router or multilayer switch.
- Provides data to enable network and security monitoring, network planning, traffic analysis, and IP accounting for billing purposes.





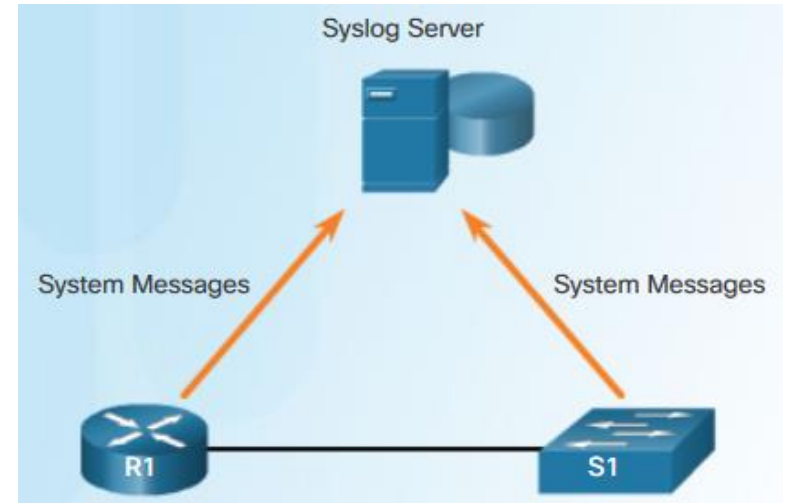
# Port Mirroring

- A feature that allows a switch to make duplicate copies of traffic passing through a switch, and then send data out a port with a network monitor attached.
- The original traffic is forwarded in the usual manner.



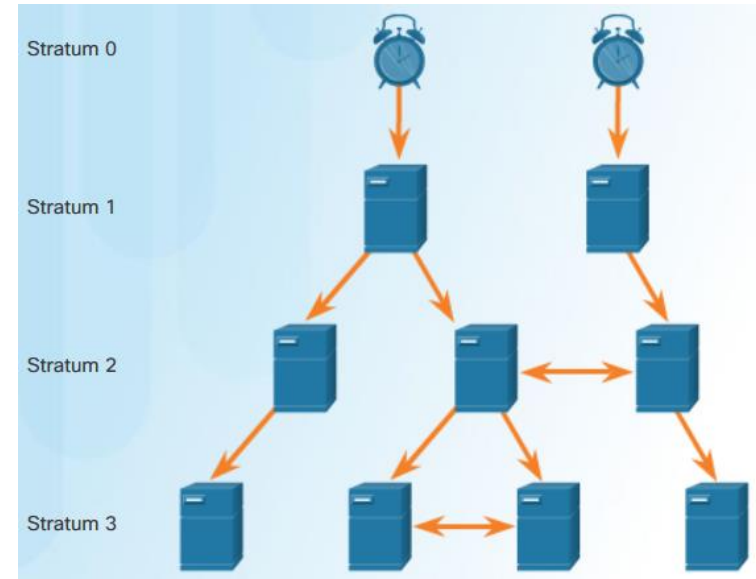
# Syslog Servers

- The most common method of accessing system messages.
- Allows networking devices to send their system messages across the network to syslog servers.
- The syslog logging service provides three primary functions:
  - Gather logging information for monitoring and troubleshooting.
  - Select the type of logging information that is captured.
  - Specify the destination of captured syslog messages.



# NTP

- Allows routers on the network to synchronize their time settings with an NTP server and use strata levels.
- NTP can be set up to synchronize to a private master clock or it can synchronize to a publicly available NTP server on the Internet.
- NTP servers are arranged in levels known as strata:
  - **Stratum 0** - high-precision timekeeping devices assumed to be accurate and with little or no delay.
  - **Stratum 1** - connected to the authoritative time sources. They act as the primary network time standard.
  - **Stratum 2 and Lower** - connected to stratum 1 devices through network connections. Stratum 2 devices synchronize their time using the NTP packets from stratum 1 servers. They could also act as servers for stratum 3 devices.



# Security Services

## AAA Servers

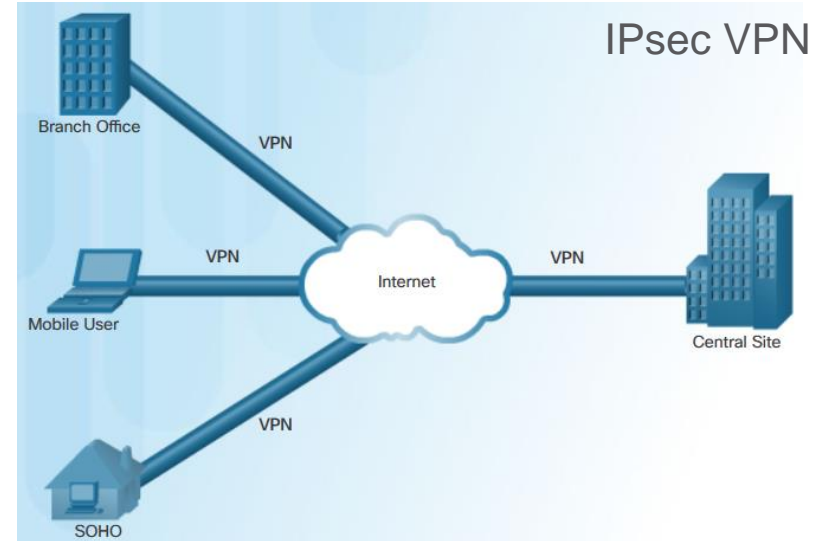
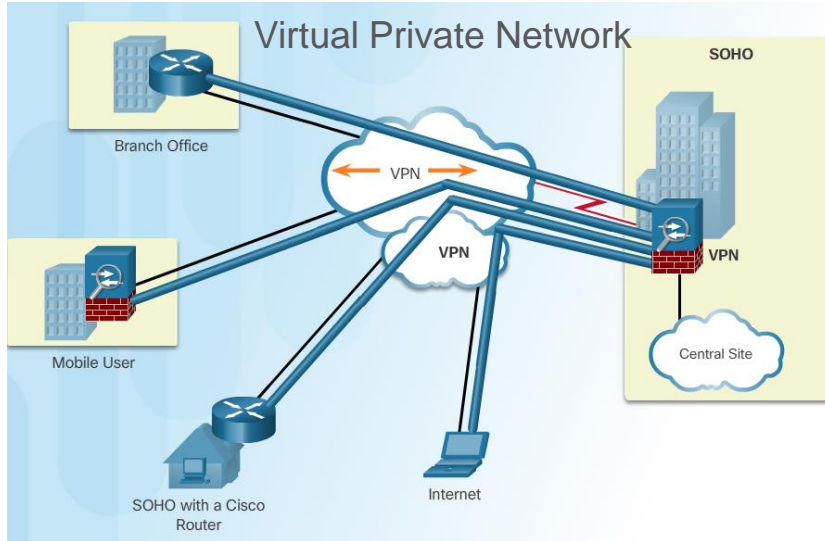
- AAA Services is a set of three independent security functions: Authentication, Authorization, and Accounting/auditing.

	TACACS+	RADIUS
Functionality	Separates AAA according to the AAA architecture, allowing modularity of the security server implementation	Combines authentication and authorization but separates accounting, allowing less flexibility in implementation than TACACS+
Standard	Mostly Cisco supported	Open/RFC standard
Transport Protocol	TCP	UDP
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 a per-user or per-group basis	Has no option to authorize router commands on a per-user or per-group basis
Accounting	Limited	Extensive

# Security Services

## VPN

- This is a private network that is created over a public network.
- A VPN is private in that the traffic is encrypted to keep the data confidential while it is transported across the public network.
- IPsec services allow for authentication, integrity, access control, and confidentiality.

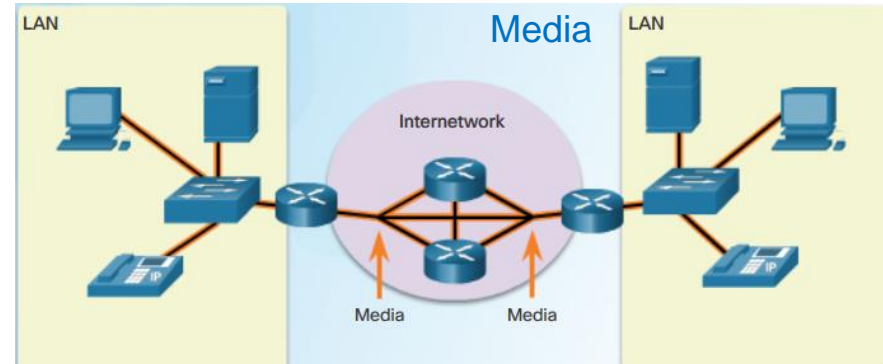
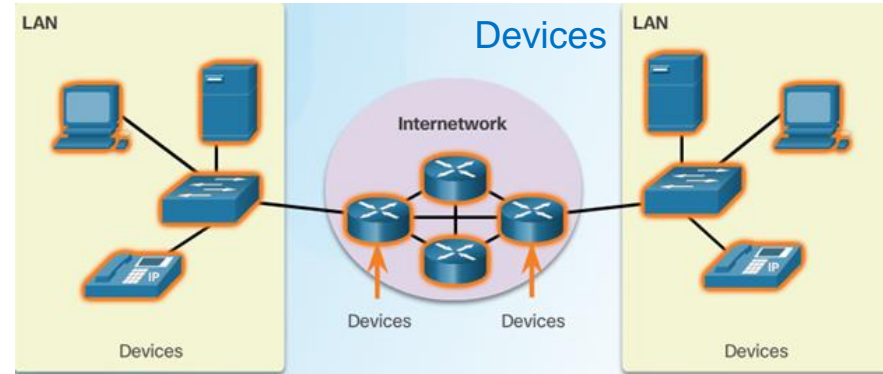
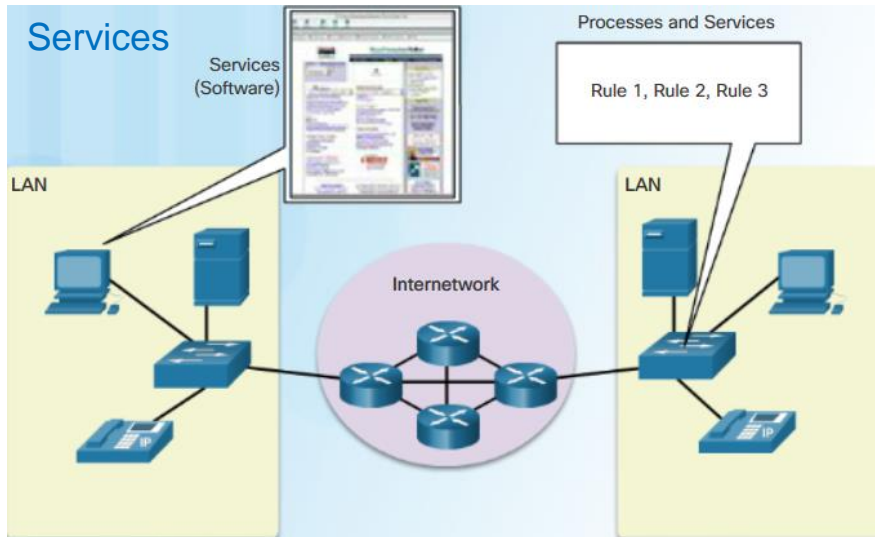


# 5.3 Network Representations

# Overview of Network Components

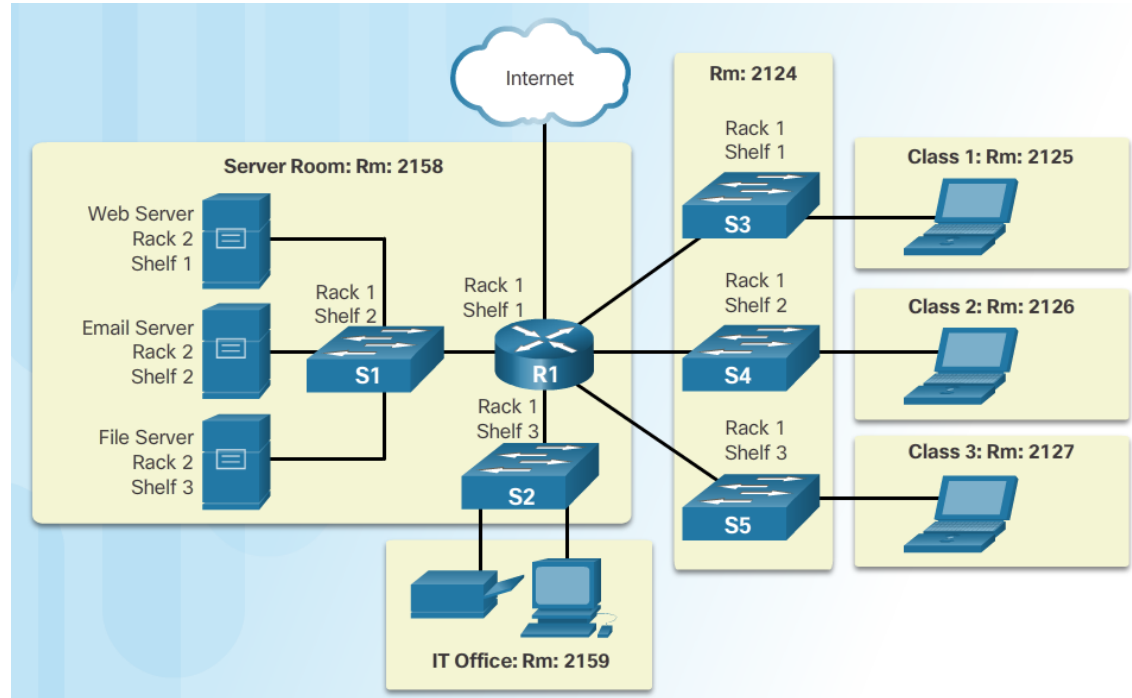
- Network infrastructure contains three categories of network components:

- Devices
- Media
- Services



# Physical and Logical Topologies

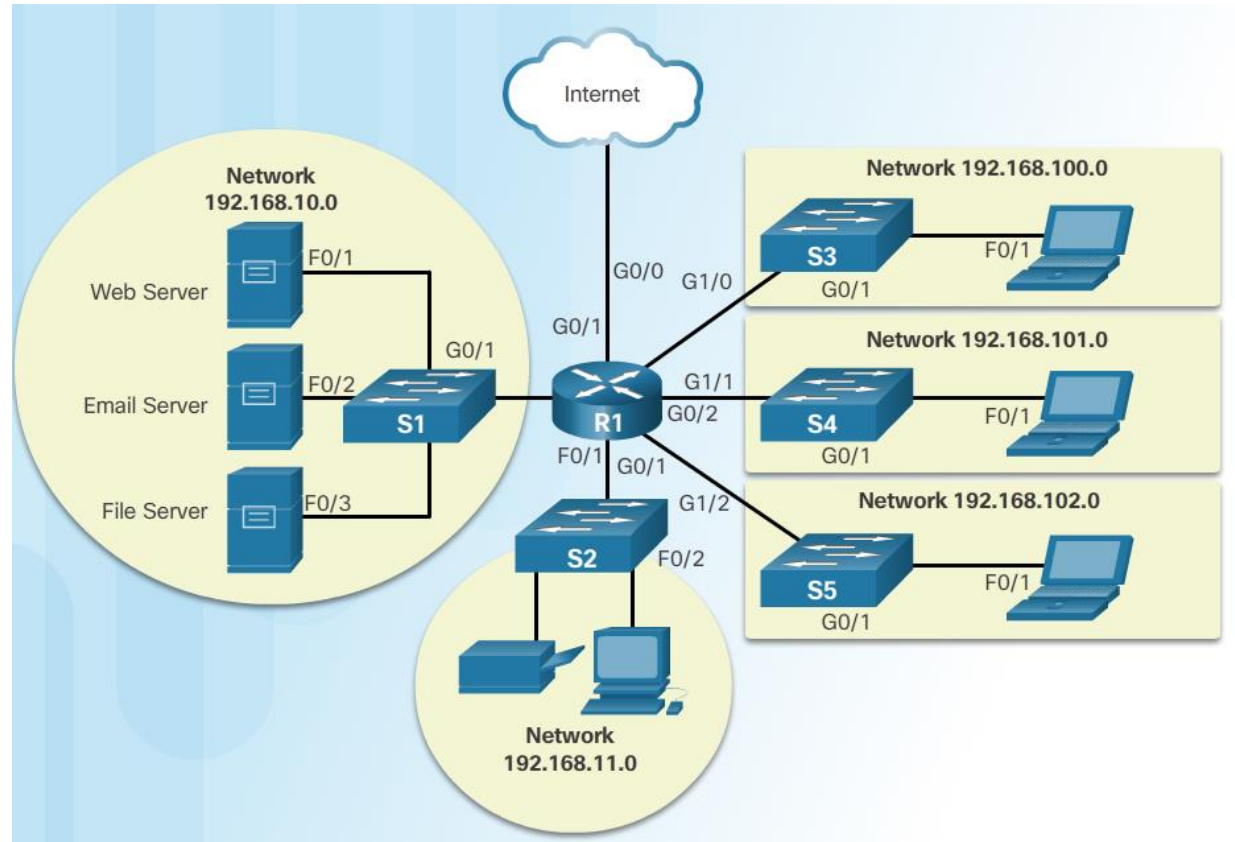
- Physical Topology refers to the physical connections and identifies how end devices and infrastructure devices are interconnected.





# Physical and Logical Topologies (Cont.)

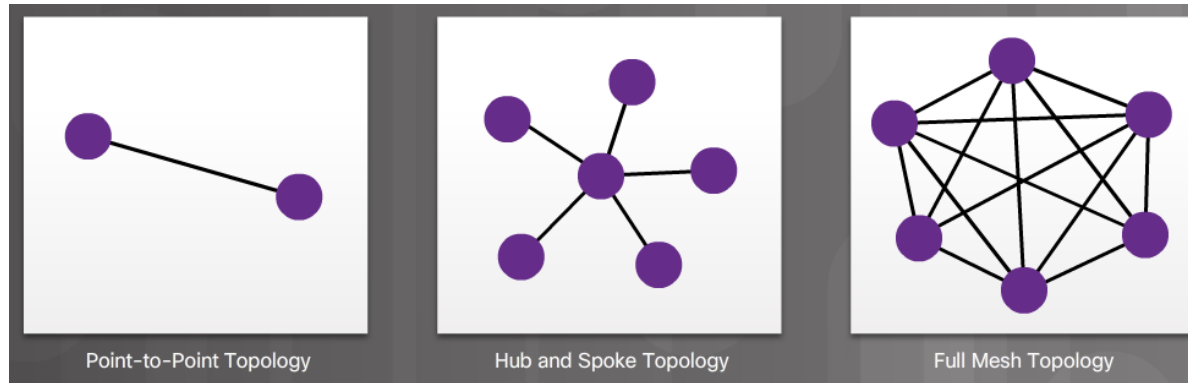
- Logical Topology refers to the way a network transfers frames from one node to the next.



## Network Topologies

# WAN Topologies

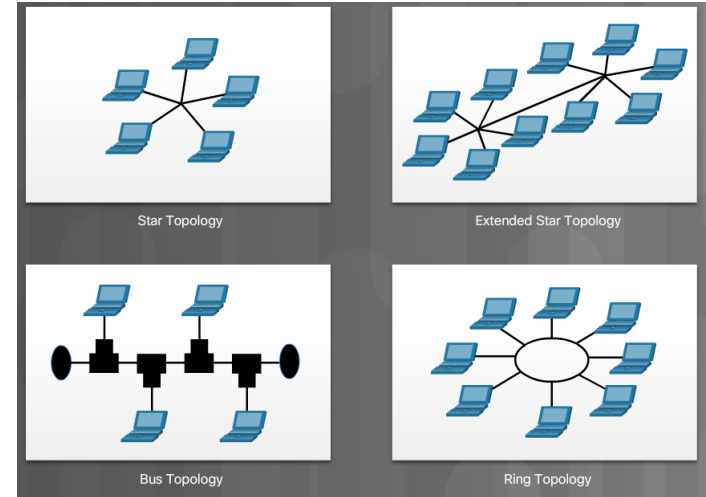
- **Point-to-Point** - Consists of a permanent link between two endpoints.
- **Hub and Spoke** - A WAN version of the star topology in which a central site interconnects branch sites using point-to-point links.
- **Mesh** - This topology provides high availability, but requires that every end system be interconnected to every other system.



## Network Topologies

# LAN Topologies

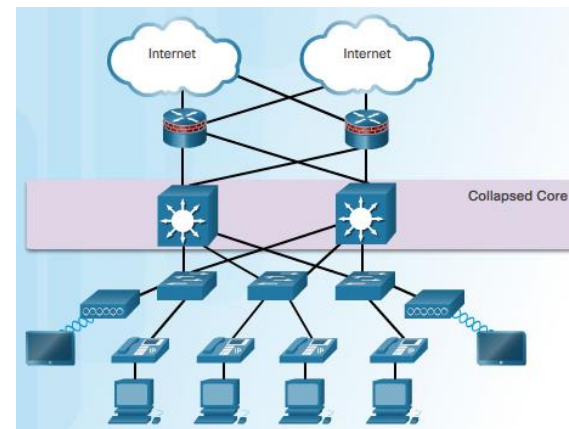
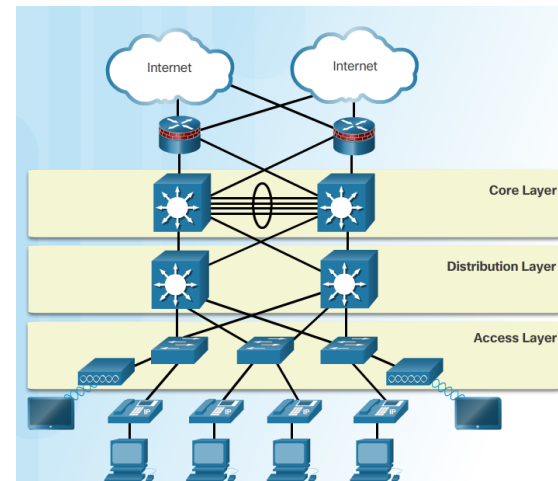
- **Star** - End devices are connected to a central intermediate device.
- **Extended Star** - In an extended star topology, additional Ethernet switches interconnect other star topologies. A
- **Bus** - All end systems are chained to each other and terminated in some form on each end.
- **Ring** - End systems are connected to their respective neighbors, forming a ring. Unlike the bus topology, the ring does not need to be terminated.



# The Three-Layer Network Design Model

## Three-Layer Hierarchical Model

- Access layer:
    - Provides endpoints and users direct access to the network.
    - User traffic is initiated at this layer.
  - Distribution layer
    - Aggregates access layers.
    - Provides connectivity to services.
  - Core layer
    - Provides connectivity between distribution layers.
- Collapsed Core
- Core and distribution layers are collapsed into one layer.
  - Reduces cost and complexity.



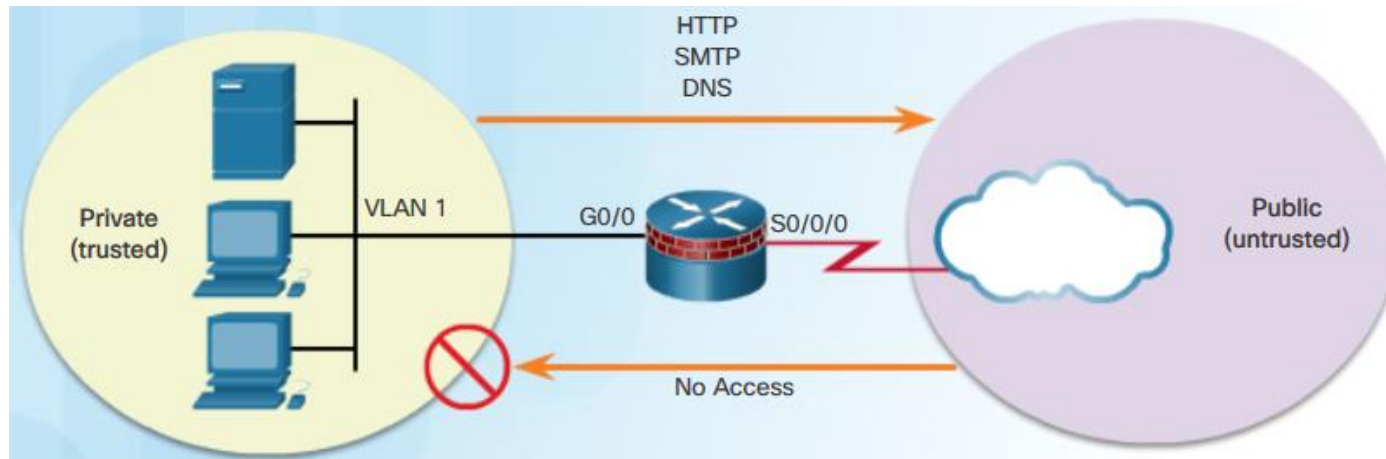
# Video Tutorial - Three-Layer Network Design Model

- Access Layer – At this layer, workgroup switches support VLAN, quality of service (QoS), and power over Ethernet.
- Distribution Layer:
  - Multilayer switches capable of switching and routing.
  - Apply network policy.
- Core Layer:
  - Forward packets as fast as possible.
  - Uses NAT.



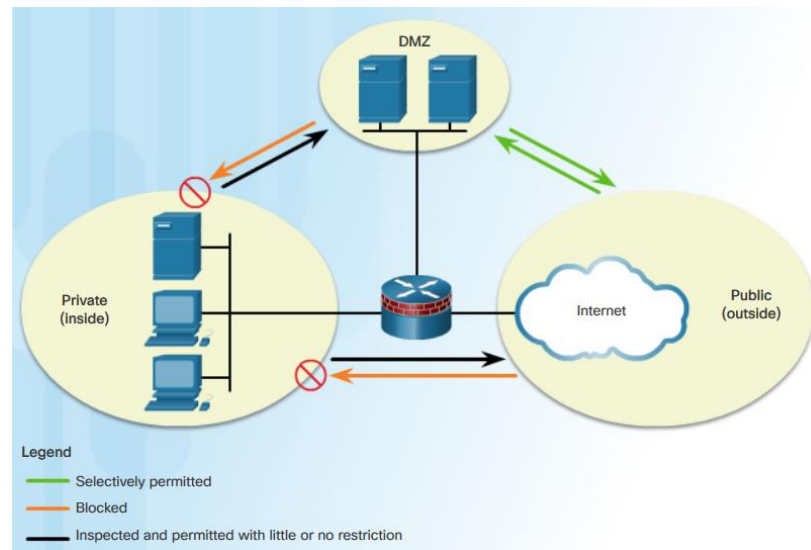
# Common Security Architectures

- 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:
  - 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.



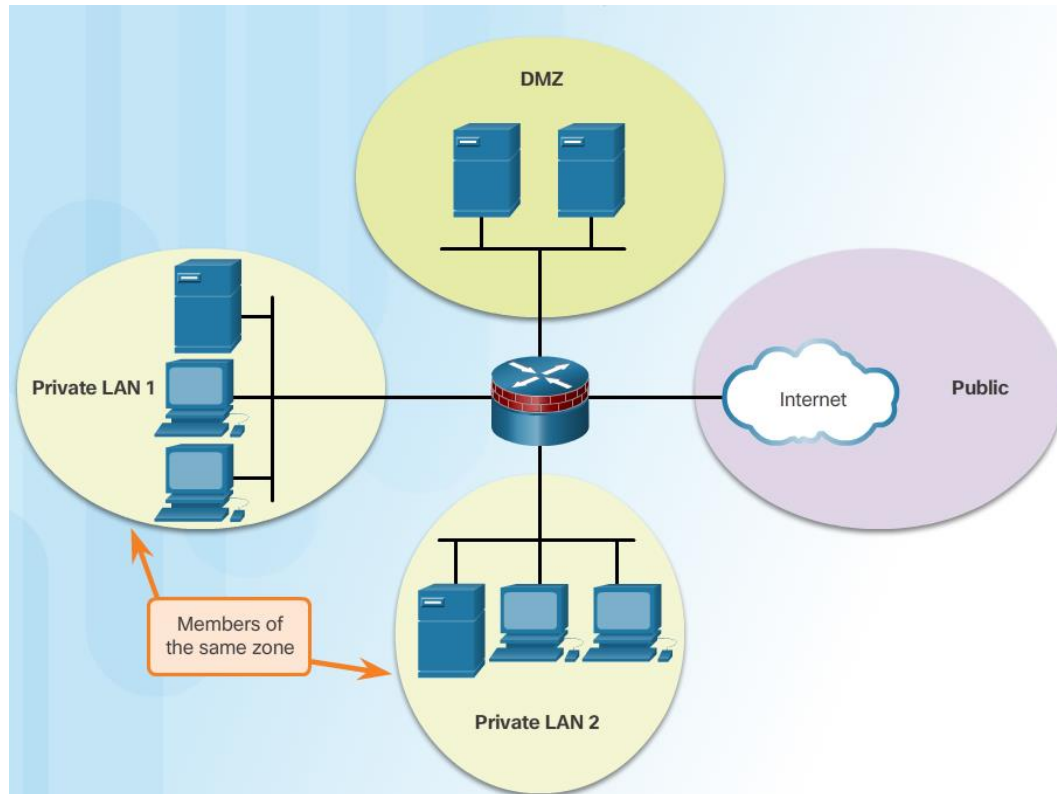
# Common Security Architectures (Cont.)

- 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.)

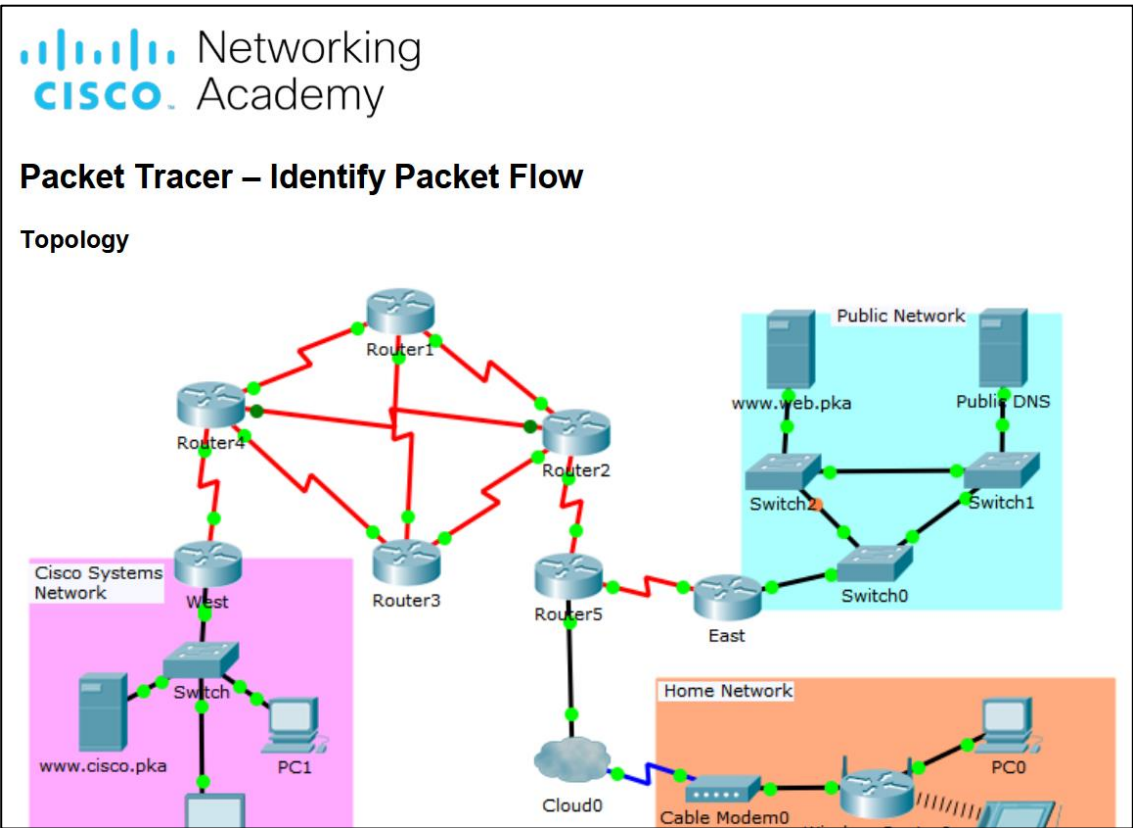
- Zone-based policy firewalls (ZPFs) use the concept of zones to provide additional flexibility.
- A zone is a group of one or more interfaces that have similar functions or features.





# Network Topologies

## Packet Tracer – Identify Packet Flow



# 5.4 Chapter Summary

## Chapter Summary

# Summary

- Intermediary Devices connect the individual end devices to the network and also connect multiple individual networks to form an internetwork.
- Routers provide path determination and packet forwarding.
- The routing table search results in a directly connected network, a remote network, or no route determined.
- The destination network entries in the routing table can be added by local route interfaces, directly connected interfaces, static routes, or through a dynamic routing protocol.
- An Ethernet hub acts as a multiport repeater, bridges have two interfaces and are connected between hubs, and LAN switches connect devices into a star topology.
- LAN switches determine how to handle incoming data frames by maintaining the MAC address table.
- Devices within a VLAN act as if they are in their own independent network, even if they share a common infrastructure with other VLANs.

# Summary (Cont.)

- STP ensures that there is only one logical path between all destinations on the network by intentionally blocking redundant paths that could cause a loop.
- Multilayer switches (also known as Layer 3 switches) not only perform Layer 2 switching, but also forward frames based on Layer 3 and 4 information.
- Wireless LANs (WLANs) use Radio Frequencies (RF) instead of cables at the physical layer and MAC sublayer of the data link layer.
- Management frames are used by wireless devices to complete the three-stage process of Access Point (AP) Discovery, Authentication, and Association.
- When using a Wireless LAN Controller (WLC), the APs no longer act autonomously, but instead act as lightweight APs (LWAPs).
- A firewall is a system, or group of systems, that enforces an access control policy between networks

# Summary (Cont.)

- There are many different types of firewalls: packet filtering (stateless) firewall, stateful firewall, application gateway firewall (proxy firewall), host-based (server and personal) firewall, transparent firewall, and hybrid firewall.
- Packet filtering firewalls are usually part of a router firewall, which permits or denies traffic based on Layer 3 and Layer 4 information.
- Stateful firewalls provide stateful packet filtering by using connection information maintained in a state table.
- Next-generation firewalls go beyond stateful firewalls by providing standard firewall capabilities, integrated intrusion prevention, application awareness, upgrade paths to include future information feeds, and techniques to address evolving security threats.
- When implementing IDS or IPS, it is important to be familiar with the types of systems available, host-based and network-based approaches, the placement of these systems, the role of signature categories, and possible actions that a Cisco IOS router can take when an attack is detected.

# Summary (Cont.)

- Deciding which implementation of IDS and IPS to use is based on the security goals of the organization as stated in their network security policy.
- There are two primary kinds of IPSs available: host-based and network-based.
- Specialized security appliances like web security appliance, email security appliance, and next-generation firewalls provides comprehensive protection against malware and help to mitigate email-based threats.
- 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.
- Standard ACLs can be used to permit or deny traffic only from source IPv4 addresses while extended ACLs filter IPv4 packets based on different attributes.
- Simple Network Management Protocol (SNMP) allows administrators to manage end devices on an IP network and it enables network administrators to monitor and manage network performance, find and solve network problems, and plan for network growth.

# Summary (Cont.)

- NetFlow provides data to enable network and security monitoring, network planning, traffic analysis to include identification of network bottlenecks, and IP accounting for billing purposes.
- Port mirroring is a feature that allows a switch to make duplicate copies of traffic passing through a switch, and then send it out a port with a network monitor attached.
- The syslog protocol allows networking devices to send their system messages across the network to syslog servers.
- The Network Time Protocol (NTP) allows routers on the network to synchronize their time settings with an NTP server.
- AAA is an architectural framework for configuring authentication, authorization, and accounting.
- A VPN connects two endpoints, such as a remote office to a central office, over a public network, to form a logical connection.

# Summary (Cont.)

- The network infrastructure contains three categories of network components: devices, media, and services.
- LAN and Wide Area Networks (WAN) topologies can be viewed in two ways: physical topology or logical topology.
- WANs are commonly interconnected using point-to-point, hub and spoke, or mesh physical topologies.
- End devices can be interconnected using star, extended star, bus, or ring physical topologies.
- A hierarchical LAN design includes access, distribution, and core layers.
- Firewall design is primarily about device interfaces permitting or denying traffic based on the source, the destination, and the type of traffic.



# New Terms and Commands

- |   |   |
|---|---|
| <ul style="list-style-type: none"><li>• Access Control List (ACL)</li><li>• access layer</li><li>• application gateway firewall (proxy firewall)</li><li>• content addressable memory (CAM)</li><li>• core layer</li><li>• CSMA/CA</li><li>• CSMA/CD</li><li>• demilitarized zone (DMZ)</li><li>• distribution layer</li><li>• dynamic routing protocol</li><li>• Generic Routing Encapsulation (GRE)</li><li>• Host-based IPS (HIPS)</li><li>• intermediary device</li></ul> | <ul style="list-style-type: none"><li>• intrusion prevention systems (IPS)</li><li>• lightweight APs (LWAPs)</li><li>• Logical topology</li><li>• Multilayer switch</li><li>• NetFlow</li><li>• Network Time Protocol (NTP)</li><li>• packet analyzer</li><li>• Packet filtering (stateless) firewall</li><li>• Packet forwarding</li></ul> |
|---|---|

# New Terms and Commands

- |  |  |
|--|--|
| <ul style="list-style-type: none"><li>• Path determination</li><li>• Physical topology</li><li>• Port mirroring</li><li>• Remote Authentication Dial-In User Service (RADIUS)</li><li>• Routed port</li><li>• Router</li><li>• Service set identifier (SSID)</li><li>• Simple Network Management Protocol (SNMP)</li><li>• Spanning Tree Protocol (STP)</li><li>• Stateful firewall</li><li>• Static routes</li><li>• Switch virtual interface (SVI)</li></ul> | <ul style="list-style-type: none"><li>• Syslog protocol</li><li>• Terminal Access Controller Access-Control System Plus (TACACS+)</li><li>• Virtual LAN (VLAN)</li><li>• Virtual private network (VPN)</li><li>• Wireless access point (AP)</li><li>• Wireless LAN Controller (WLC)</li><li>• Wireless LANs (WLANS)</li><li>• Zone-based policy firewall (ZPF)</li></ul> |
|--|--|

# Cybersecurity Operations Certification

This chapter covers the following areas in the Cybersecurity Operations Certification:

From 210-250 SECFND - Understanding Cisco Cybersecurity Fundamentals:

- **Domain 1: Network Concepts**

- 1.4 Describe the basic operation of the following network device types:
  - Router
  - Switch
  - Hub
  - Bridge
  - Wireless Access Point (WAP)
  - Wireless LAN Controller (WLC)

# Cybersecurity Operations Certification (Cont.)

This chapter covers the following areas in the Cybersecurity Operations Certification:

From 210-250 SECFND - Understanding Cisco Cybersecurity Fundamentals:

- **Domain 1: Network Concepts**

- 1.5 Describe the functions of the following network security systems as deployed on the host, network, or the cloud:
  - Firewall
  - Intrusion Prevention System (IPS)
  - Advance Malware Protection (AMP)
  - Web Security Appliance (WSA) / Cisco Cloud Web Security (CWS)
  - Email Security Appliance (ESA) / Cisco Cloud Email Security (CES)

# Cybersecurity Operations Certification (Cont.)

This chapter covers the following areas in the Cybersecurity Operations Certification:

From 210-250 SECFND - Understanding Cisco Cybersecurity Fundamentals:

- **Domain 1: Network Concepts**

- 1.7 Describe the relationship between VLANs and data visibility
- 1.8 Describe the operation of ACLs applied as packet filters on the interfaces of network devices
- 1.9 Compare and contrast deep packet inspection with packet filtering and stateful firewall operation
- 1.10 Compare and contrast inline traffic interrogation and taps or traffic mirroring
- 1.11 Compare and contrast the characteristics of data obtained from taps or traffic mirroring and Netflow in the analysis of network traffic

# Cybersecurity Operations Certification (Cont.)

This chapter covers the following areas in the Cybersecurity Operations Certification:

From 210-250 SECFND - Understanding Cisco Cybersecurity Fundamentals:

- **Domain 4: Host Based Analysis**

- 4.4 Interpret the following operating system log data to identify an event:
  - Unix based syslog

