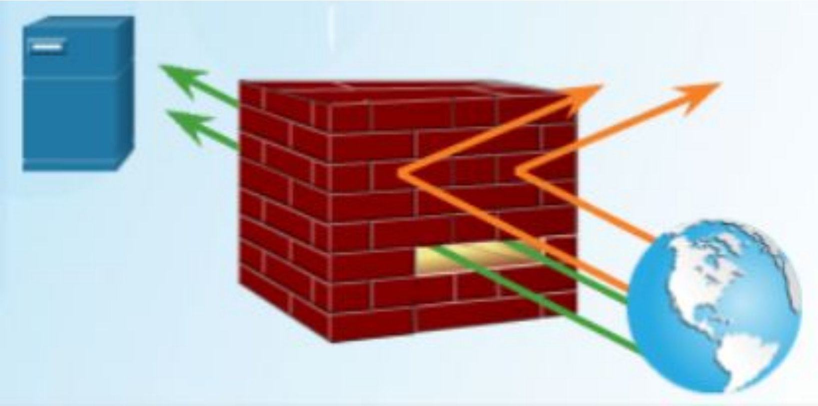
Network Security Infrastructure

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.



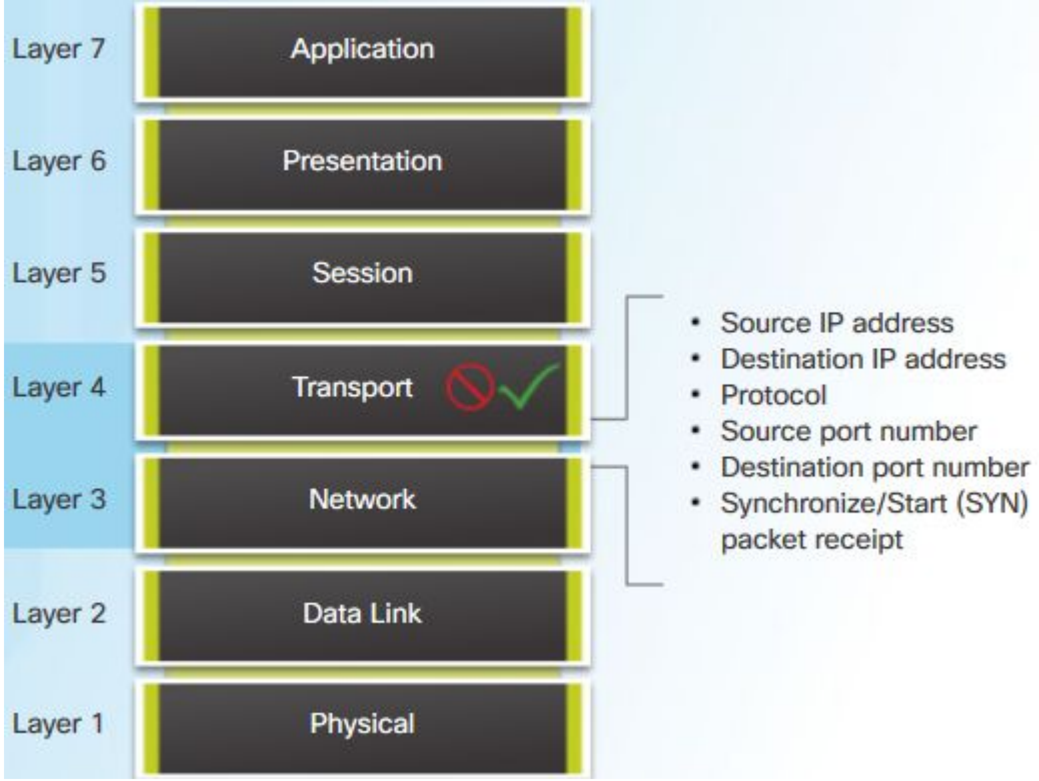
Firewall Type Descriptions

- **Packet filtering (Stateless) 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.

Security Devices

Packet Filtering Firewalls

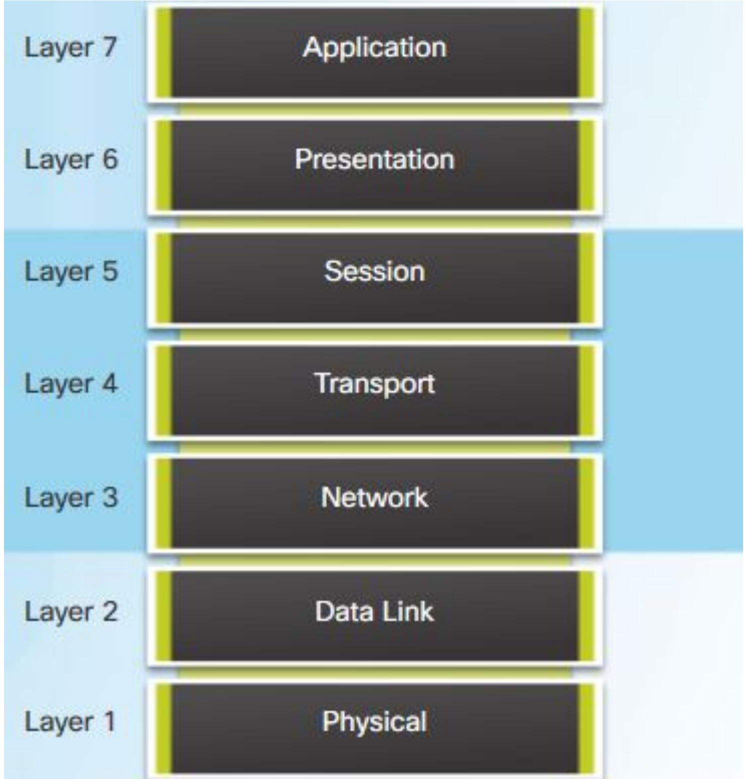
- Usually part of a router firewall, which permits or denies traffic based on Layer 3 and Layer 4 information.
- Are stateless firewalls that use a simple policy table look-up that filters traffic based on specific criteria.



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

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.



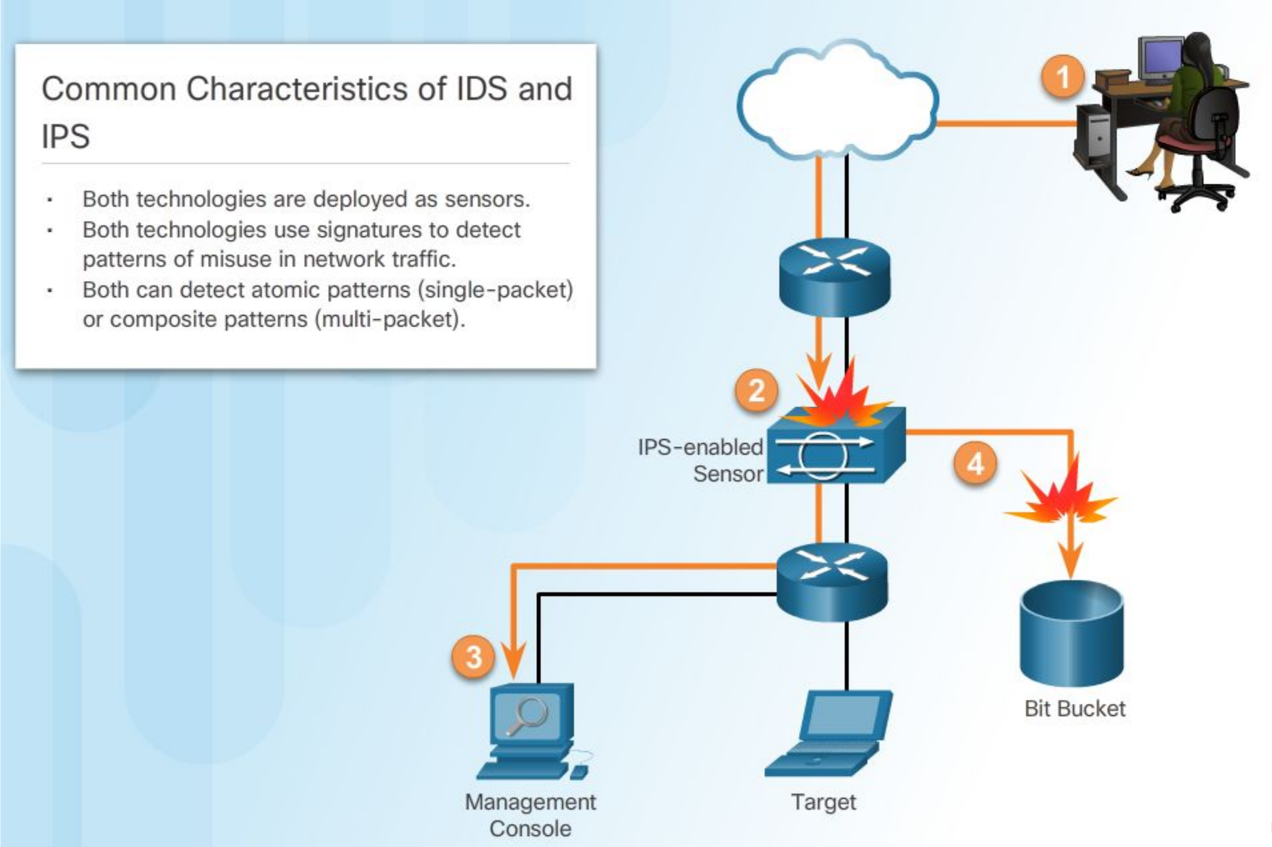
Security Devices

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.

Security Devices

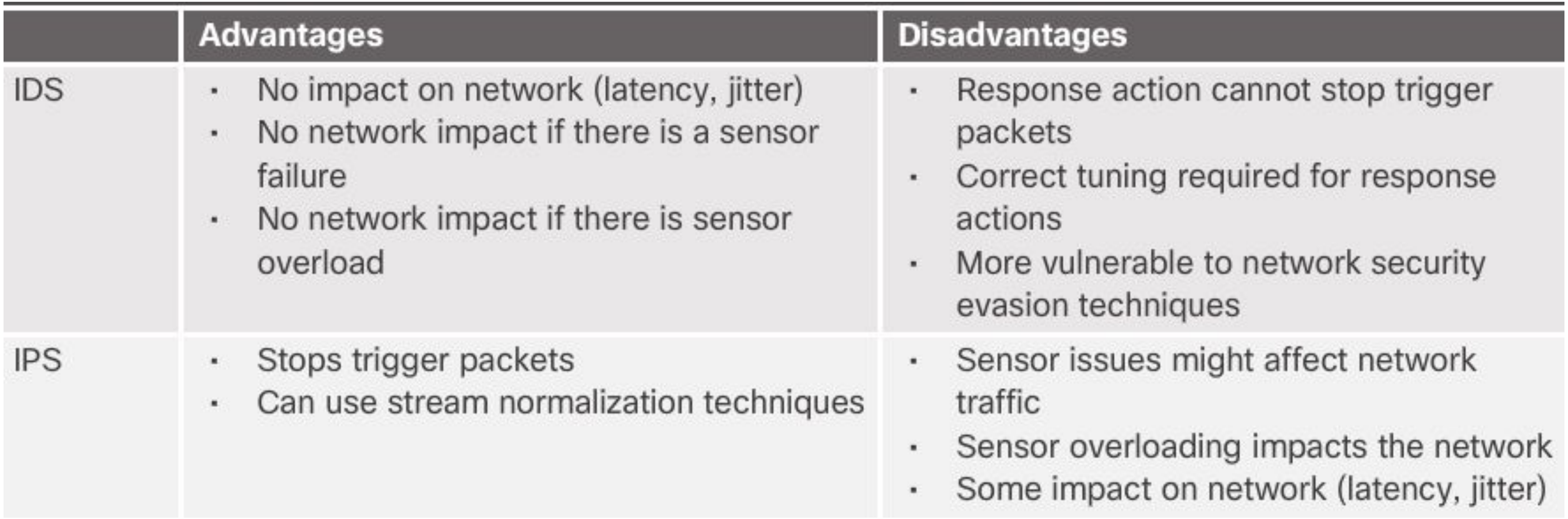
Intrusion Prevention and Detection Devices



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).

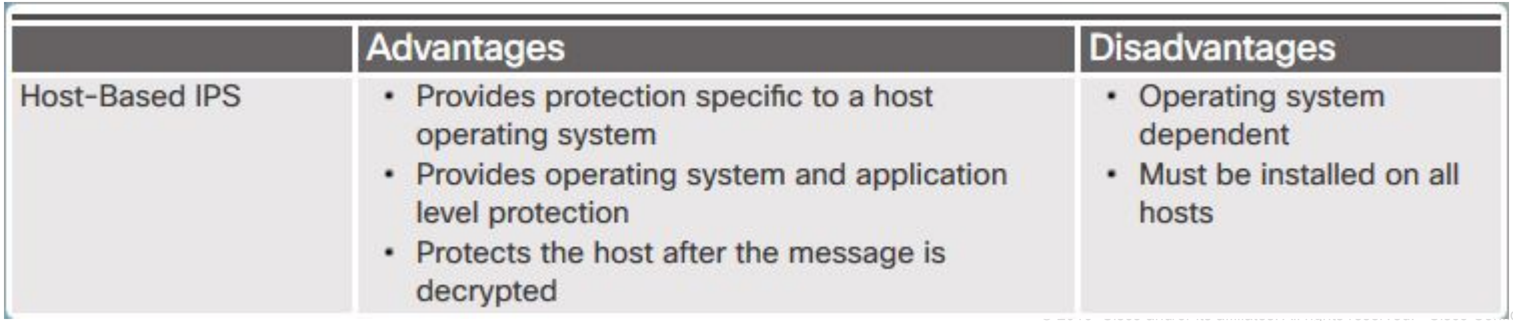
Advantages and Disadvantages of IDS and IPS



	Advantages	Disadvantages
IDS	▪ 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.



	Advantages	Disadvantages
Host-Based IPS	• 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

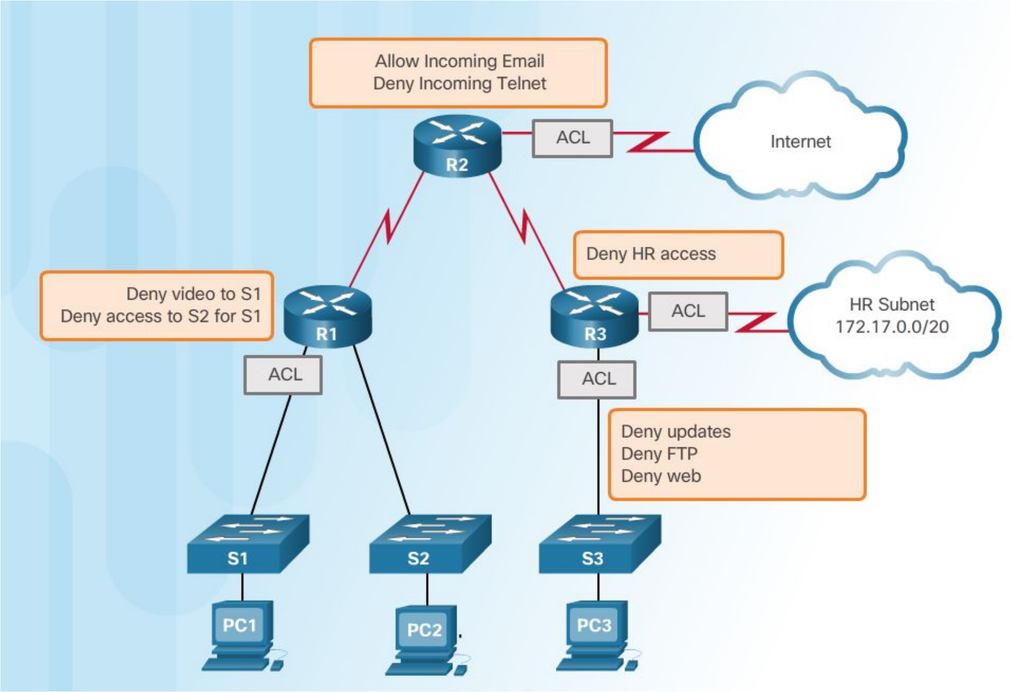
Specialized Security Appliances

- 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.

Security Services

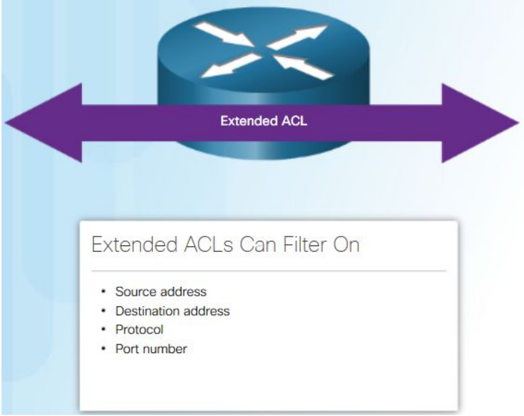
Traffic Control with ACLs

- 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



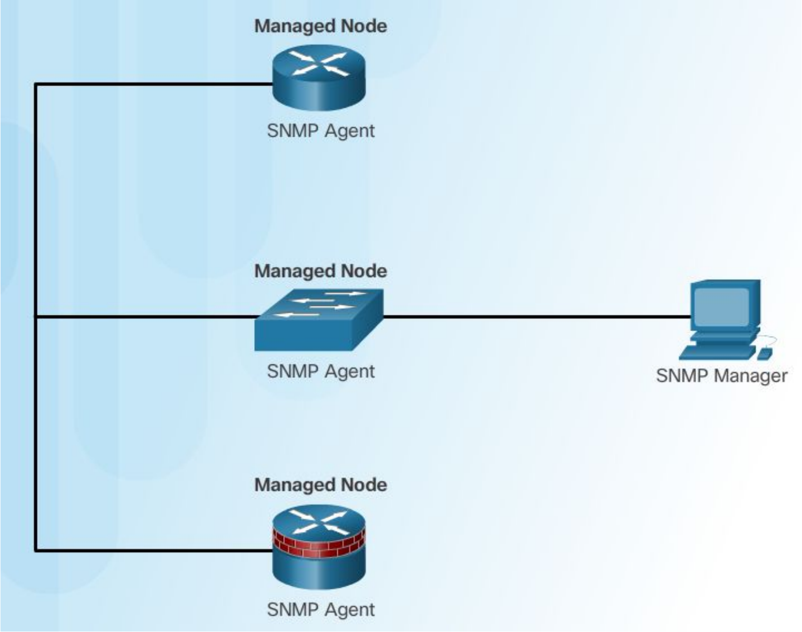
Extended ACLs Can Filter On

- Source address
- Destination address
- Protocol
- Port number

- 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.

SNMP

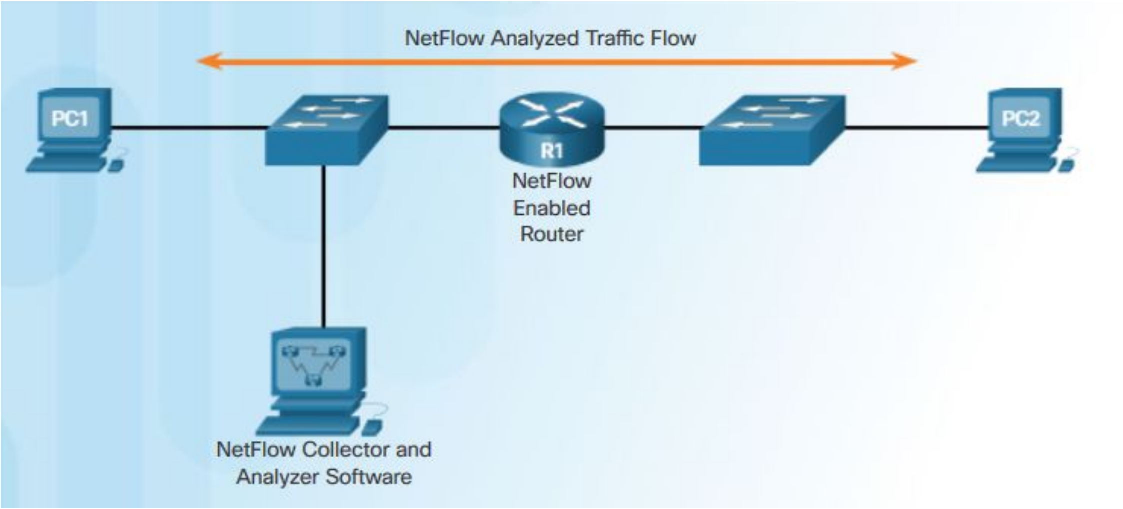
- SNMP allows administrators to manage end devices such as servers, workstations, routers, switches, and security appliances.
- The SNMP system consists of three elements:
  - Manager that runs SNMP management software.
  - Agents which are the nodes being monitored and managed.
  - Management Information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



Security Services

NetFlow

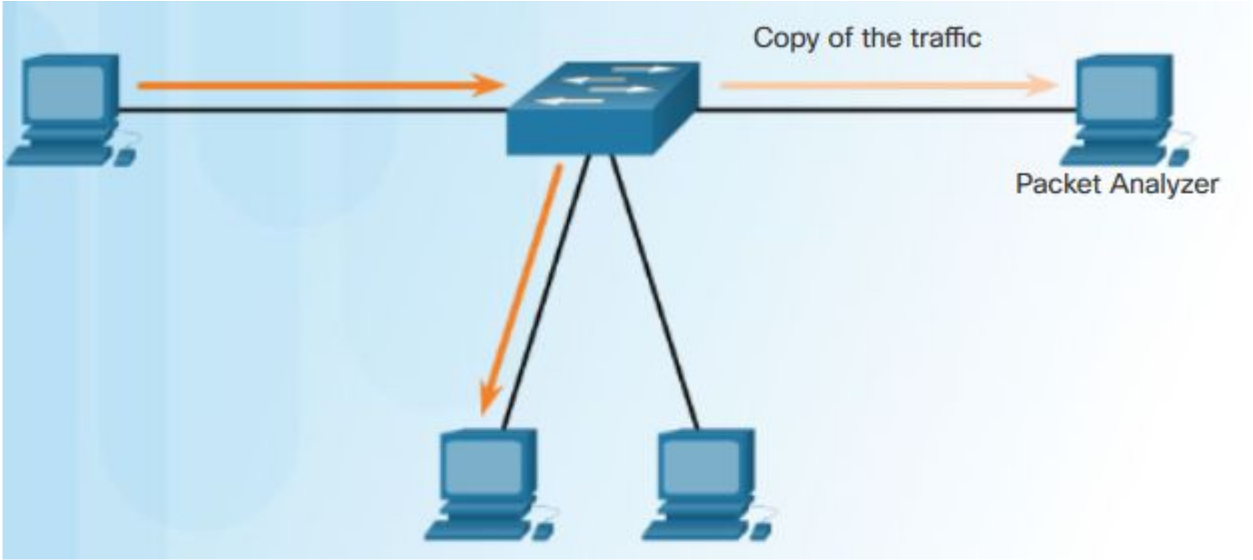
- A Cisco IOS technology that provides statistics on packets flowing through a Cisco router or multilayer switch.
- Provides data to enable network and security monitoring, network planning, traffic analysis, and IP accounting for billing purposes.


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

Security Services

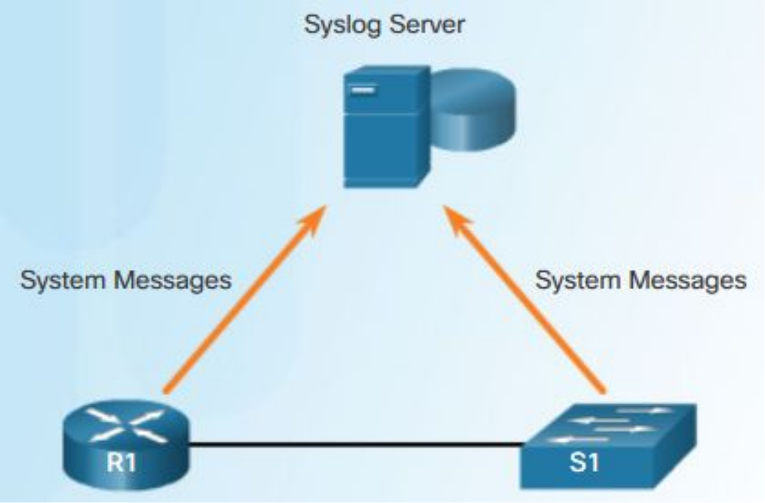
Port Mirroring

- 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.



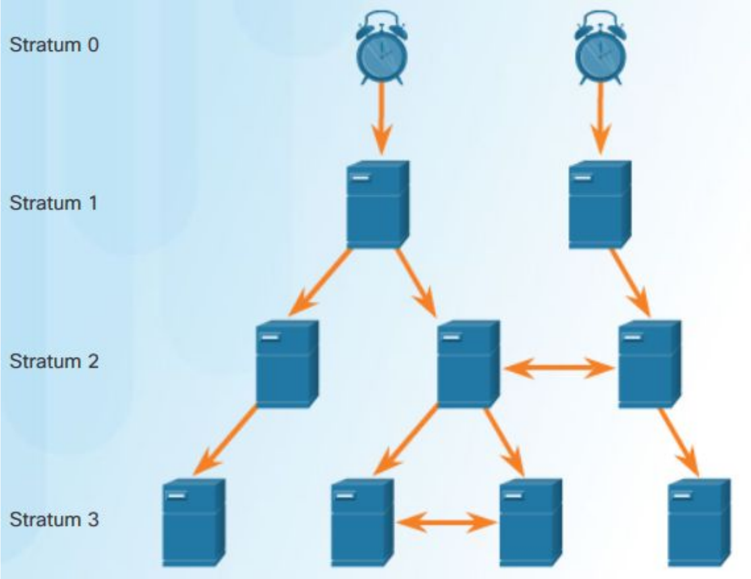
Security Services

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.

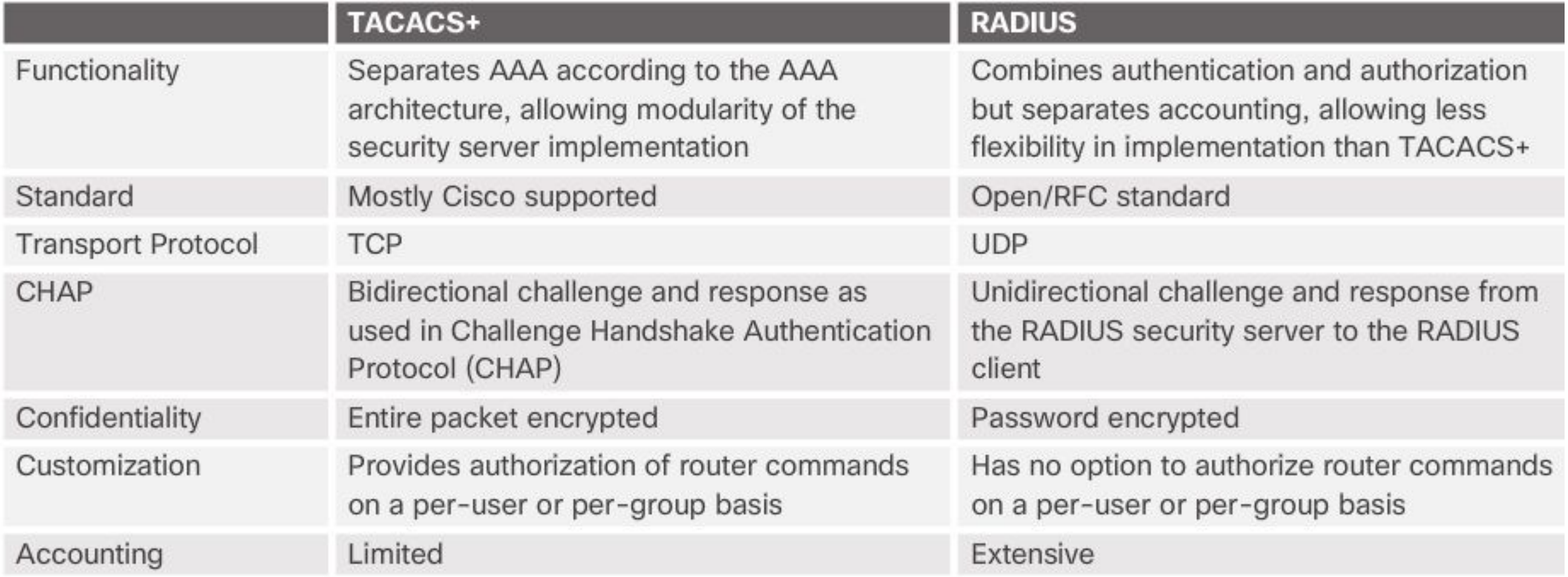
- NTP servers are arranged in levels known as strata:
  - **Stratum 0** - high-precision timekeeping devices assumed to be accurate and with little or no delay.
  - **Stratum 1** - connected to the authoritative time sources. They act as the primary network time standard.
  - **Stratum 2 and Lower** - 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.

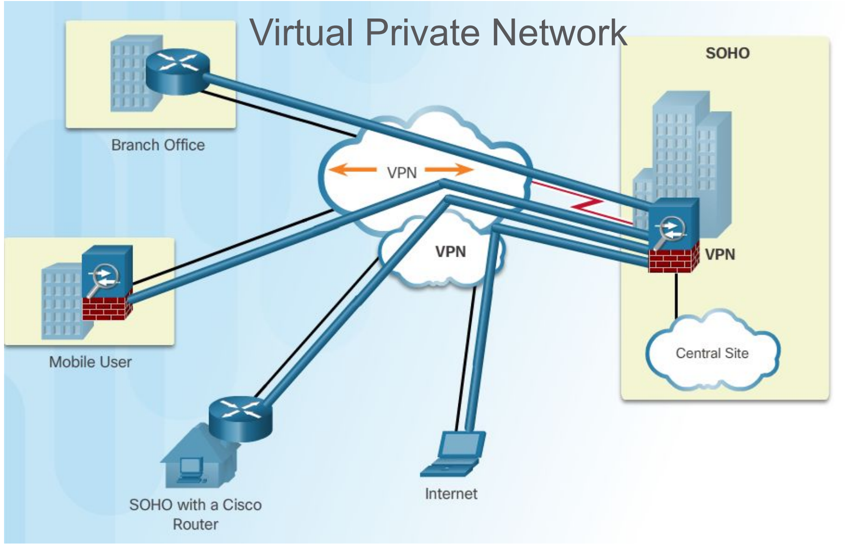


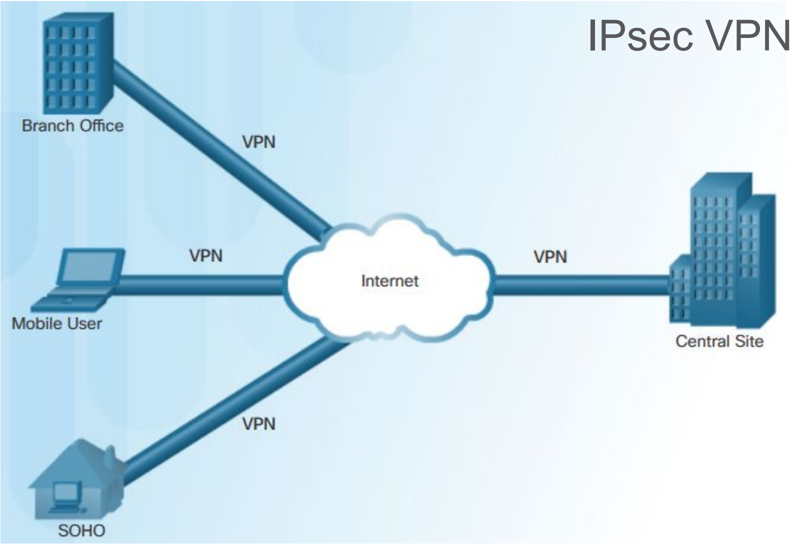
	TACACS+	RADIUS
Functionality	Separates AAA according to the AAA architecture, allowing modularity of the security server implementation	Combines authentication and authorization but separates accounting, allowing less flexibility in implementation than TACACS+
Standard	Mostly Cisco supported	Open/RFC 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.

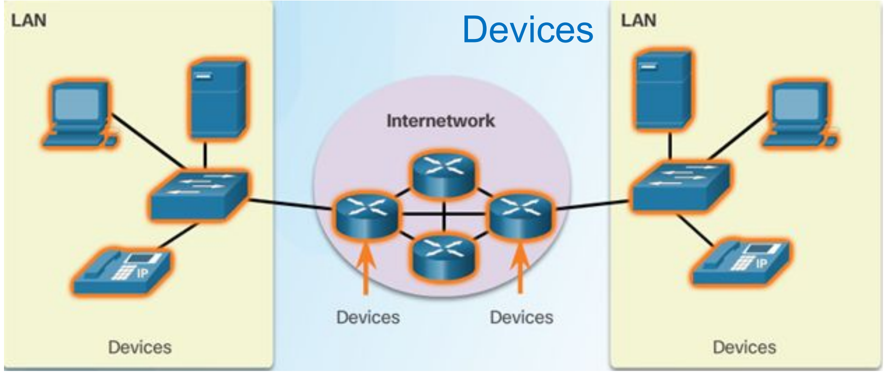


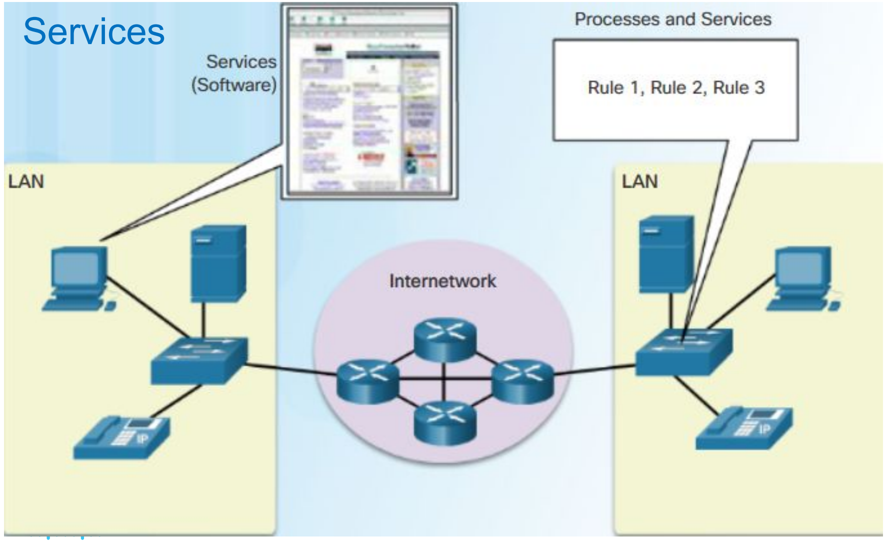


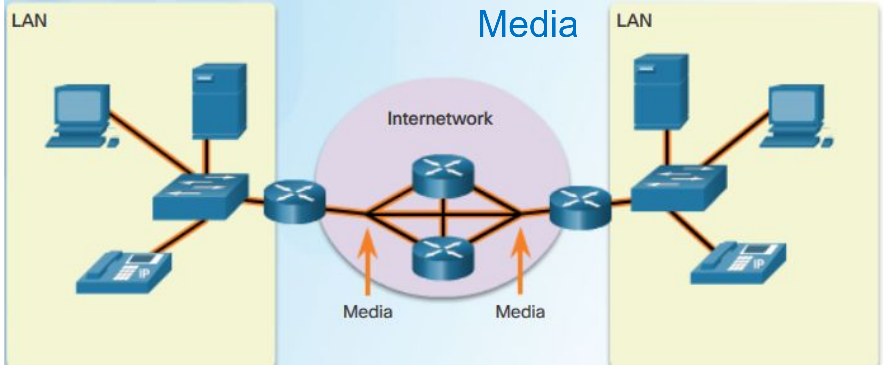
Network Representations

Overview of Network Components

- Network infrastructure contains three categories of network components:
  - Devices
  - Media
  - Services

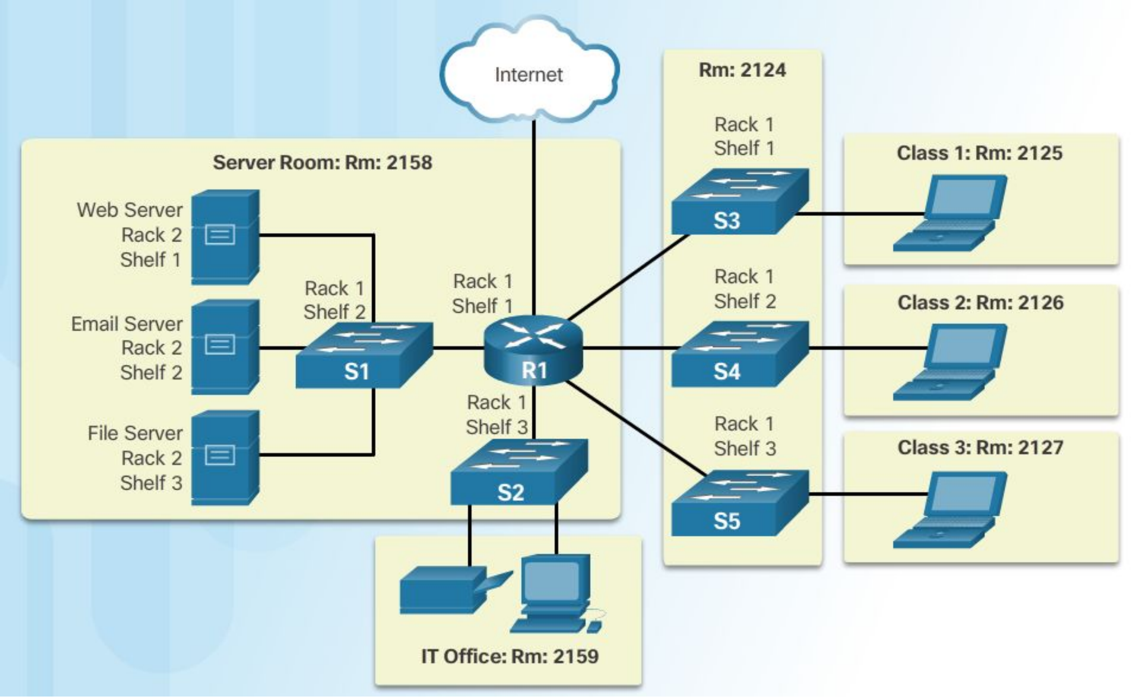






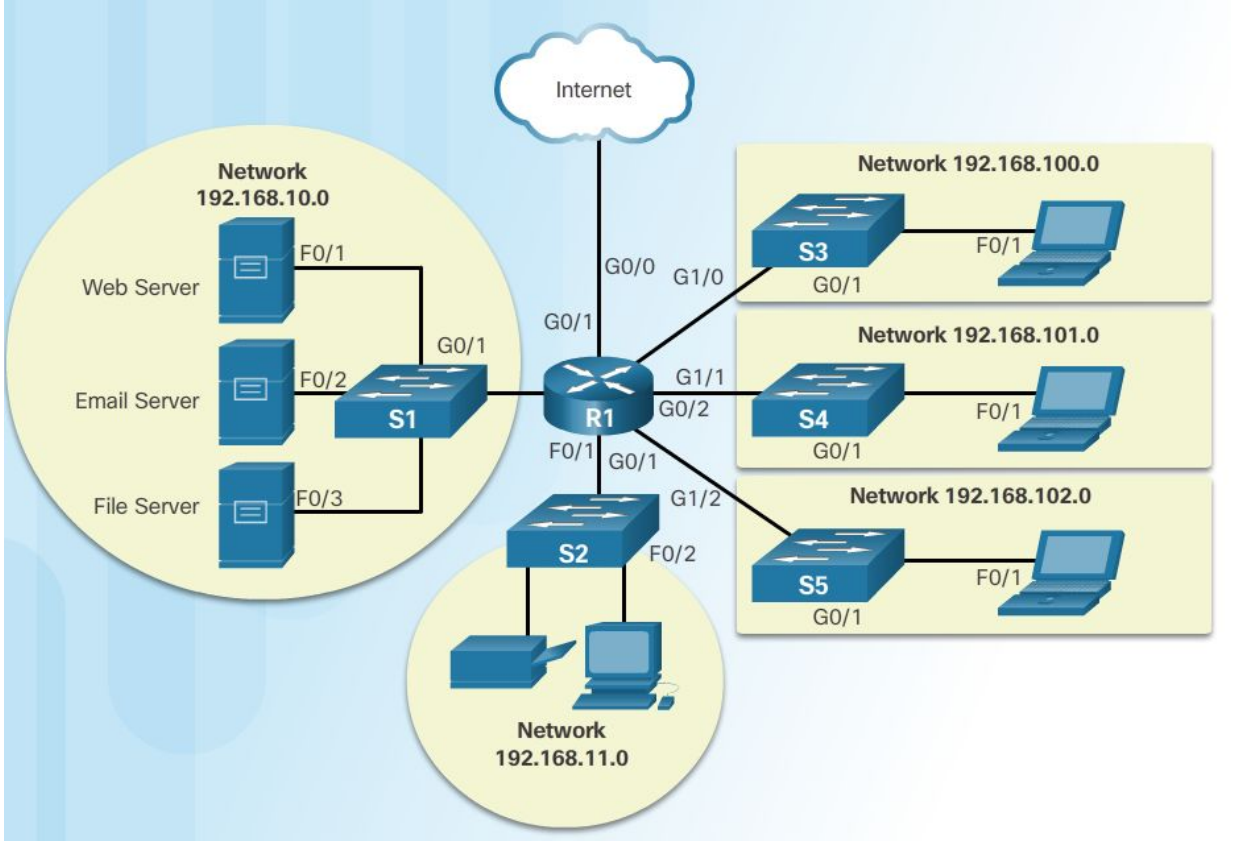
Physical and Logical Topologies

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



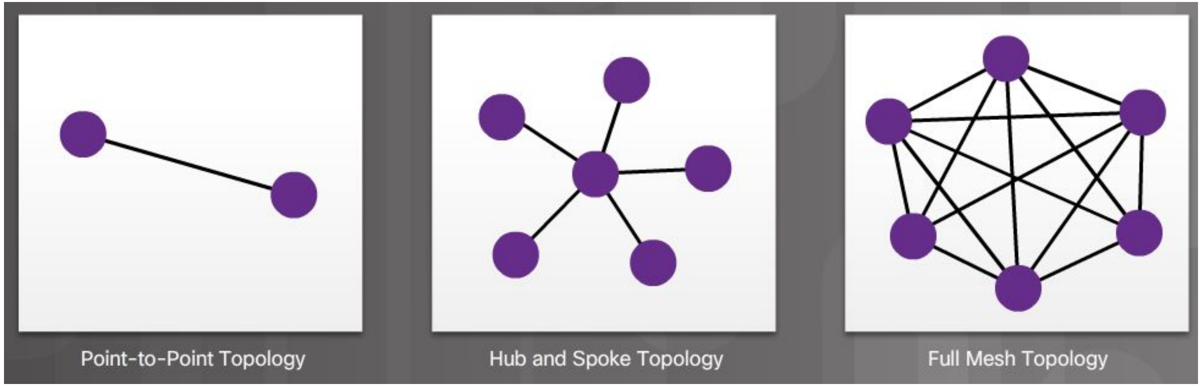
Physical and Logical Topologies (Cont.)

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



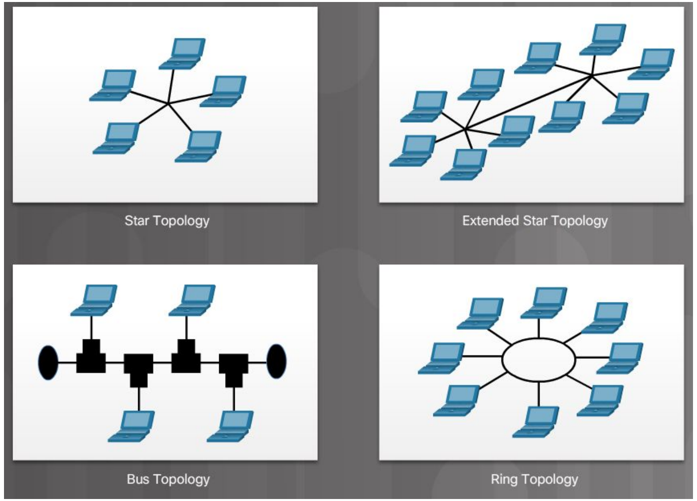
WAN Topologies

- **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.



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.



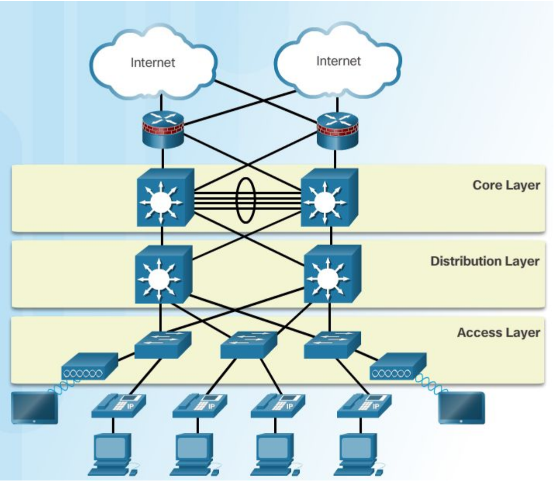
The Three-Layer Network Design Model

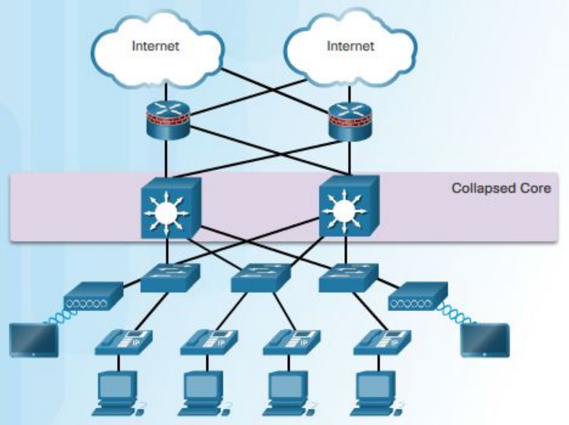
Three-Layer Hierarchical Model

- 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

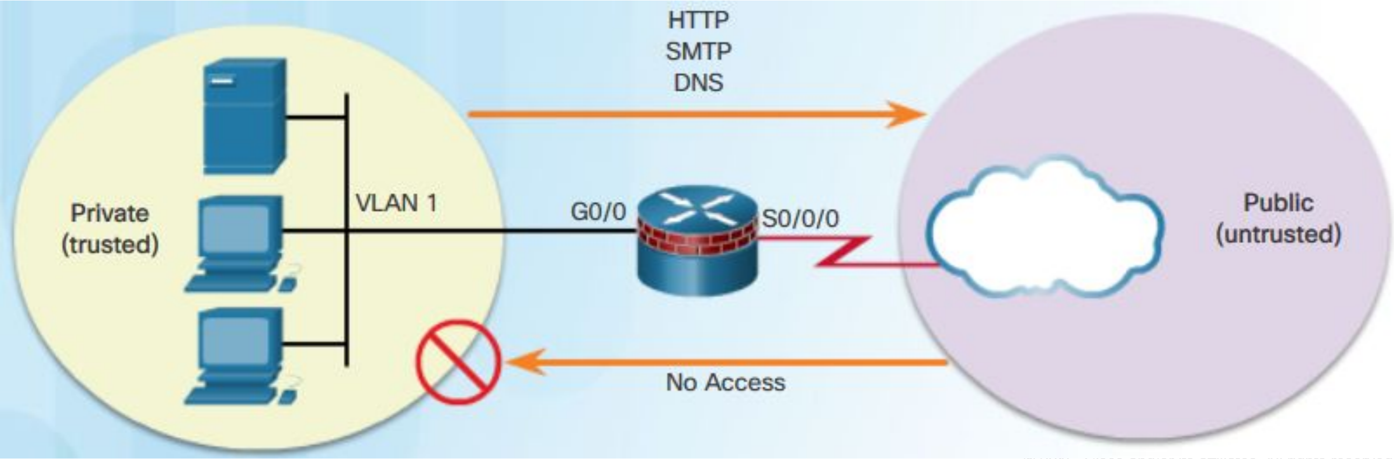
- Core and distribution layers are collapsed into one layer.
- Reduces cost and complexity.





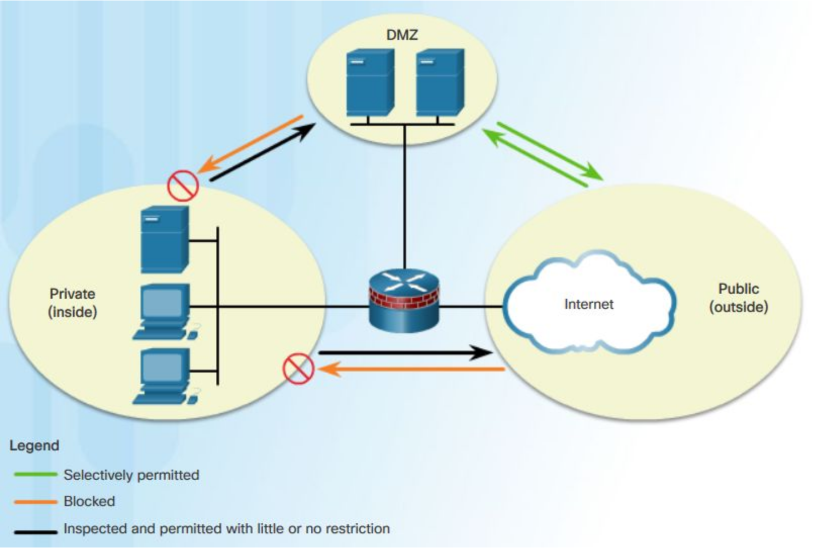
Common Security Architectures

- 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.



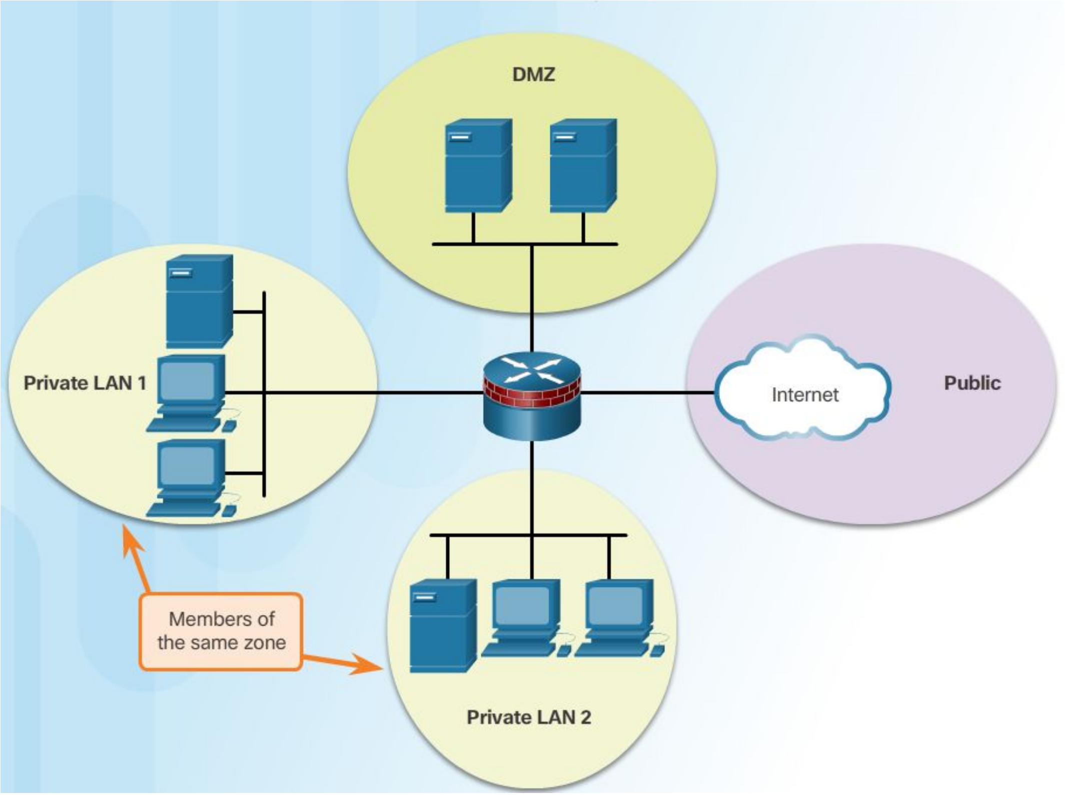
Common Security Architectures (Cont.)

- 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.



Summary

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 itt 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

- Access Control List (ACL)
- access layer
- application gateway firewall (proxy firewall)
- content addressable memory (CAM)
- core layer
- CSMA/CA
- CSMA/CD
- demilitarized zone (DMZ)
- distribution layer
- dynamic routing protocol
- Generic Routing Encapsulation (GRE)
- Host-based IPS (HIPS)
- intermediary device
- intrusion prevention systems (IPS)
- lightweight APs (LWAPs)
- Logical topology
- Multilayer switch
- NetFlow
- Network Time Protocol (NTP)
- packet analyzer
- Packet filtering (stateless) firewall
- Packet forwarding

Chapter 5

New Terms and Commands

- Path determination
- Physical topology
- Port mirroring
- Remote Authentication Dial-In User Service (RADIUS)
- Routed port
- Router
- Service set identifier (SSID)
- Simple Network Management Protocol (SNMP)
- Spanning Tree Protocol (STP)
- Stateful firewall
- Static routes
- Switch virtual interface (SVI)
- Syslog protocol
- Terminal Access Controller Access-Control System Plus (TACACS+)
- Virtual LAN (VLAN)
- Virtual private network (VPN)
- Wireless access point (AP)
- Wireless LAN Controller (WLC)
- Wireless LANs (WLANS)
- Zone-based policy firewall (ZPF)