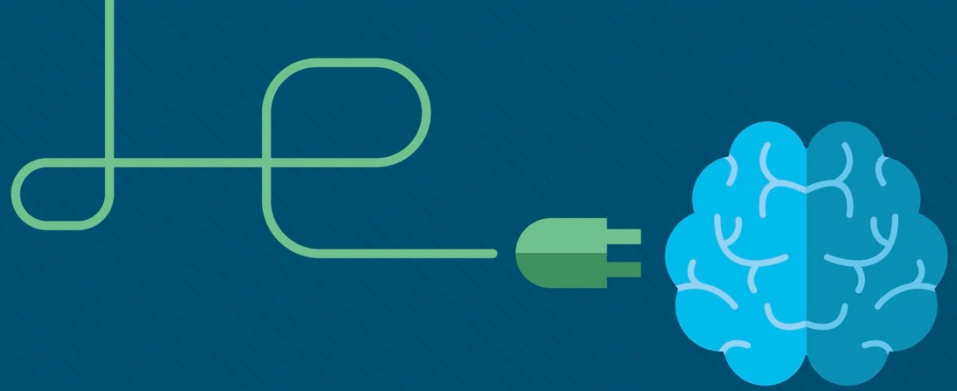


Chapter 4: Network Infrastructure

Information Security

Dr. Ayman Aljarbouh

4.1 Network Representation and Security Infrastructure

Module Objectives

Module Title: Network Representation and Security Infrastructure

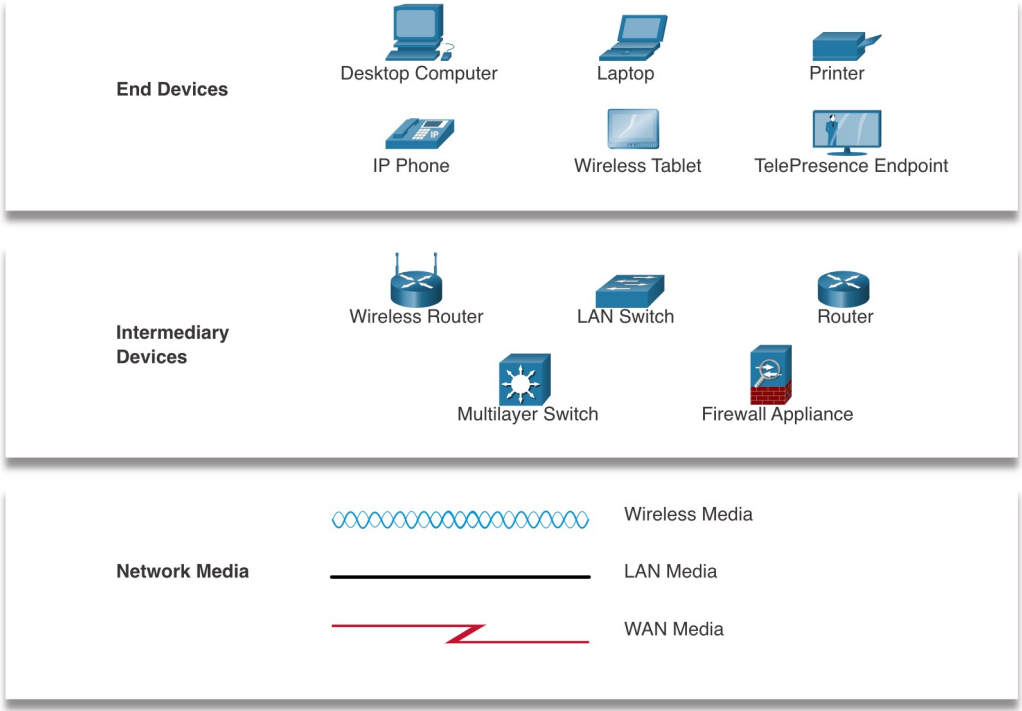
Module Objective:

- Explain how networks and network topologies are represented
- Explain how devices and services are used to enhance network security

Topic Title	Topic Objective
Network Topologies	Explain how network designs influence the flow of traffic through the network.
Security Devices	Explain how specialized devices are used to enhance network security.
Security Services	Explain how network services enhance network security.

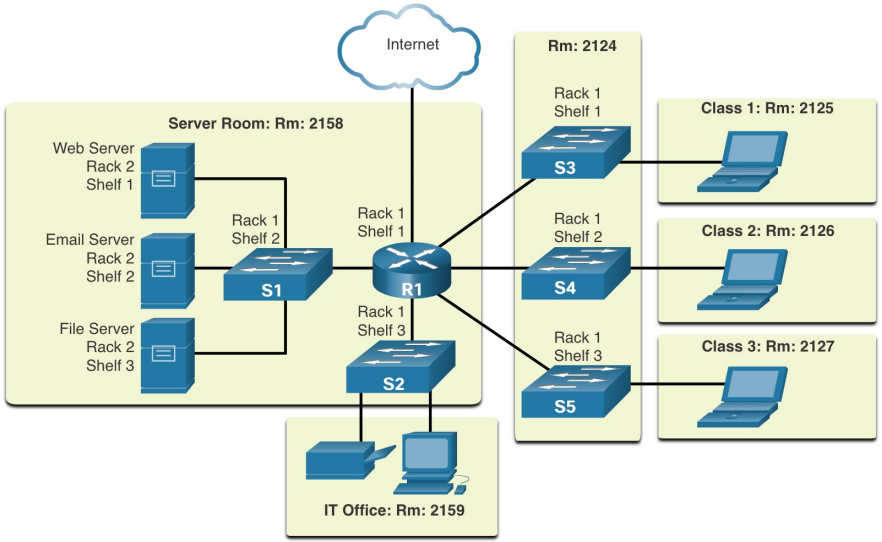
Network Representations

- Network diagrams, often called topology diagrams, use symbols to represent different devices and connections within the network.
- The important terminologies to be known include:
  - **Network Interface Card (NIC)**
  - **Physical Port**
  - **Interface**

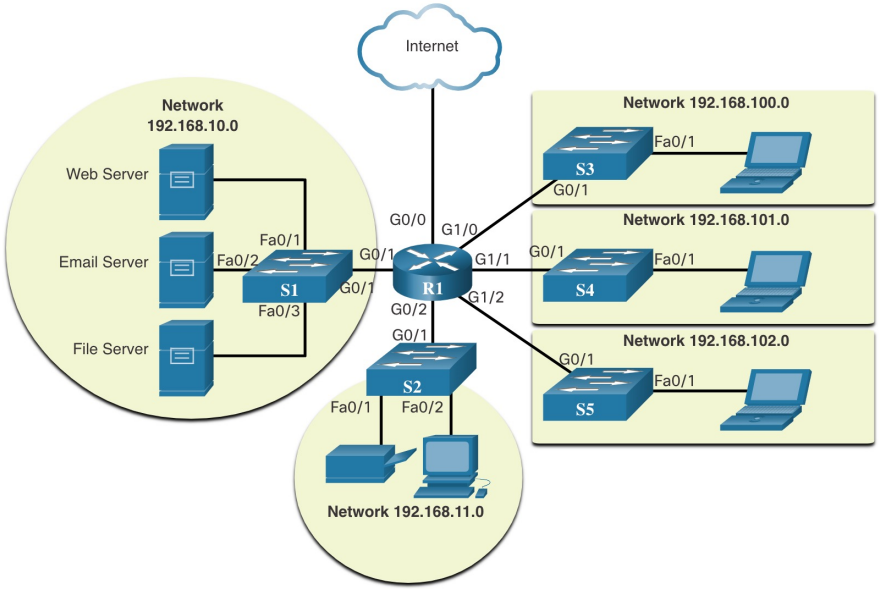


Topology Diagrams

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

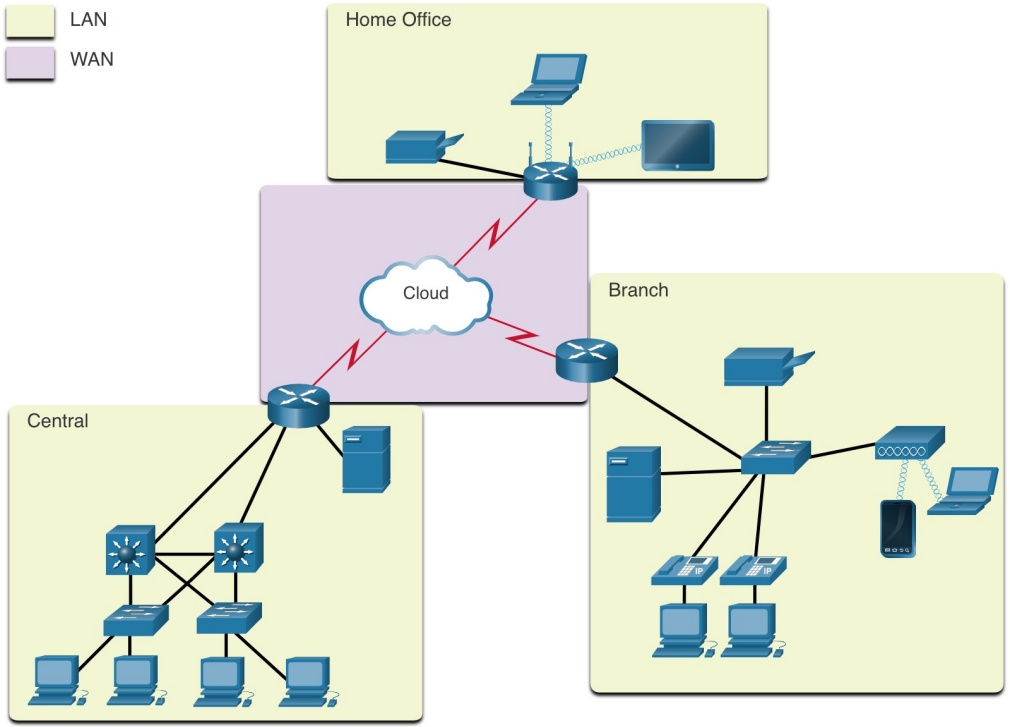


Logical topology diagrams illustrate devices, ports, and the addressing scheme of the network.



LANs and WANs

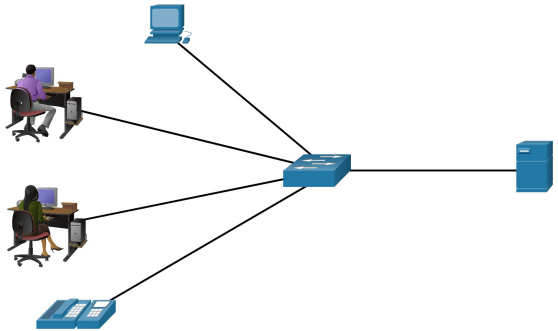
- Network infrastructures vary greatly in terms of:
  - Size of the area covered
  - Number of users connected
  - Number and types of services available
  - Area of responsibility
- The two most common types of network infrastructures are
  - Local Area Networks (LANs)
  - Wide Area Networks (WANs)



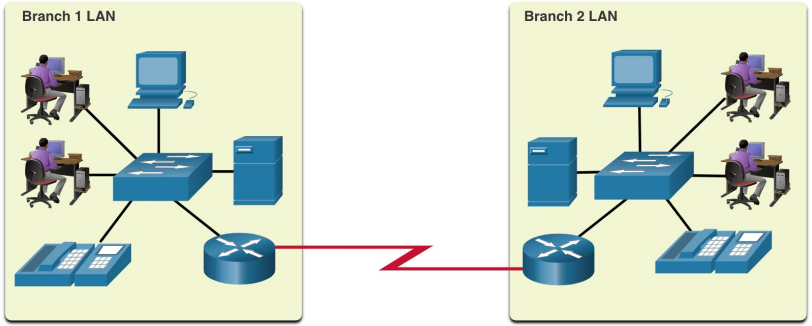
LANs connected to a WAN

LANs and WANs (Contd.)

A LAN is a network infrastructure that spans a small geographical area.



A WAN is a network infrastructure that spans a wide geographical area.



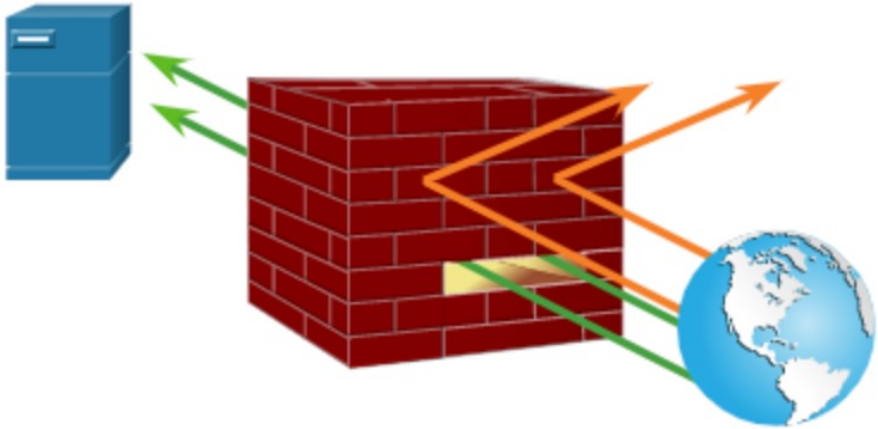
LAN	WAN
Interconnect end devices in a limited area.	Interconnect LANs over wide geographical areas.
Administered by a single organization or individual.	Typically administered by multiple service providers.
Provide high-speed bandwidth to internal end devices and intermediary devices.	Typically provide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

Firewalls

A firewall is a system, or group of systems, that enforces an access control policy between networks.

Common Firewall Properties:

- Resistant to network attacks
- The only transit point between internal corporate networks and external networks because all traffic flows through the firewall
- Enforce the access control policy

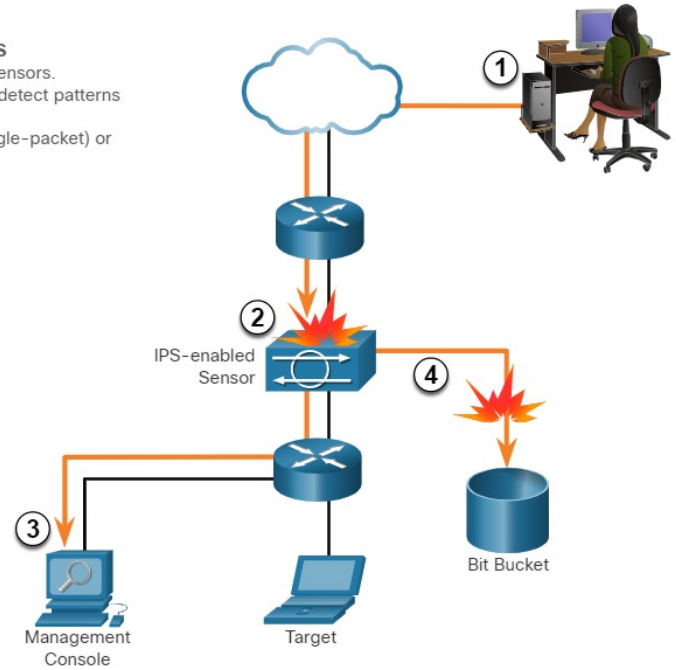


Intrusion Prevention and Detection Devices

- 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.")

Types of IPS

There are two primary kinds of IPS :

- Host-based IPS
- Network-based IPS

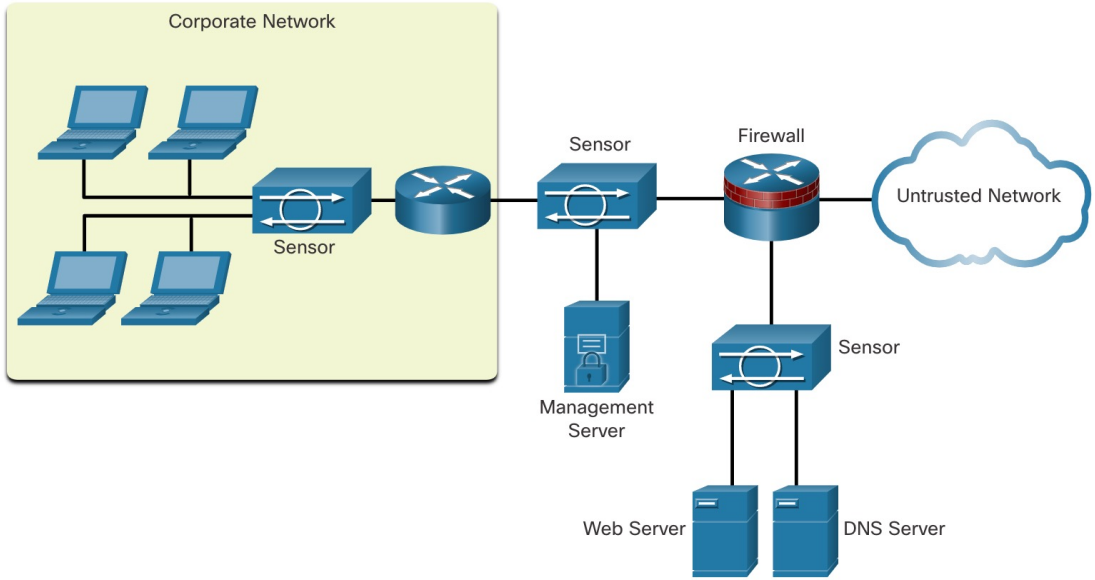
- **Host-based IPS (HIPS)**

  HIPS is a software installed on a host to monitor and analyze suspicious activity.

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

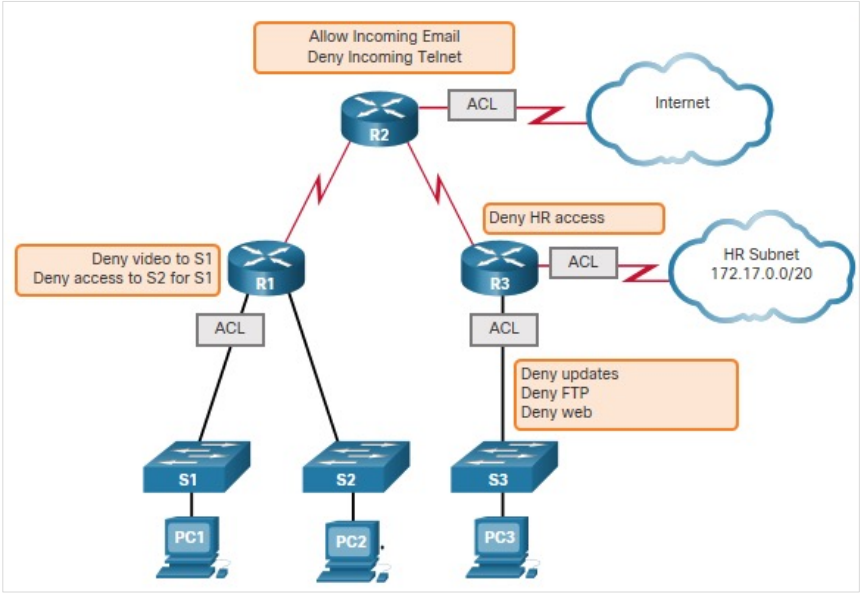
Types of IPS (Contd.)

- **Network-based IPS**
  - Network-based IPS are Implemented using a dedicated or non-dedicated IPS device.
  - Host-based IDS/IPS solutions are integrated with a network-based IPS implementation to ensure a robust security architecture.
  - Sensors detect malicious and unauthorized activity in real time and can take action when required.



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.



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

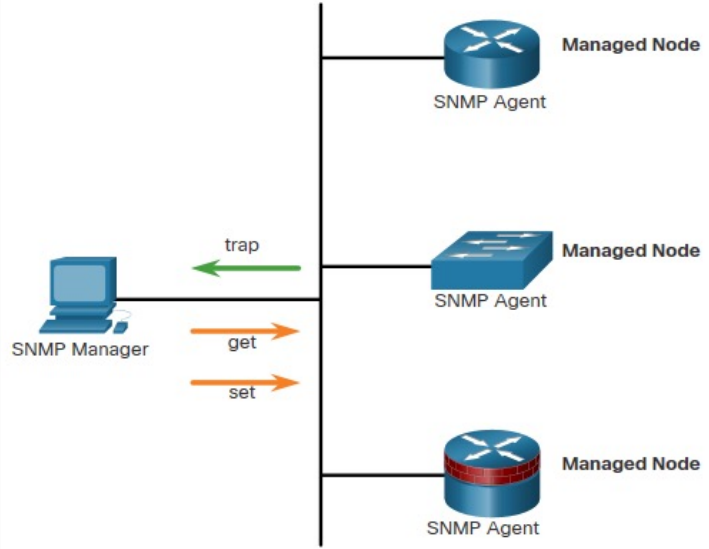
ACLs: Important Features

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.

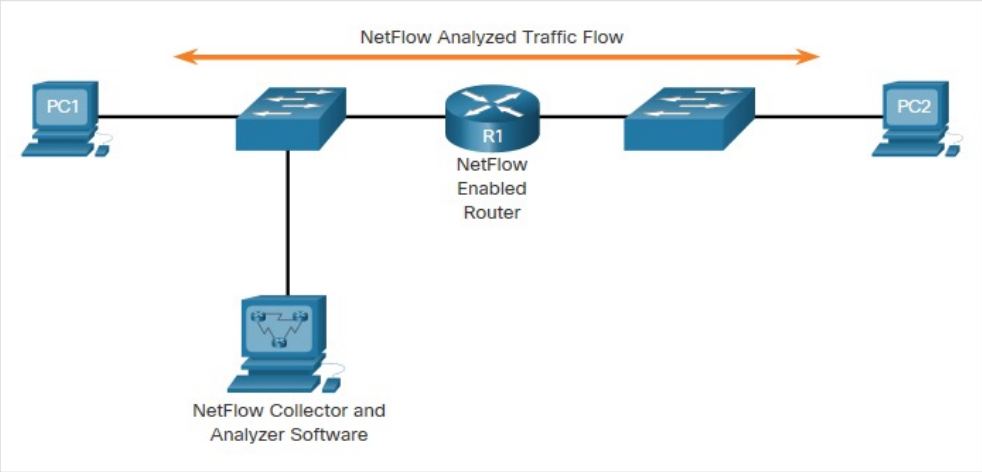
SNMP

- 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

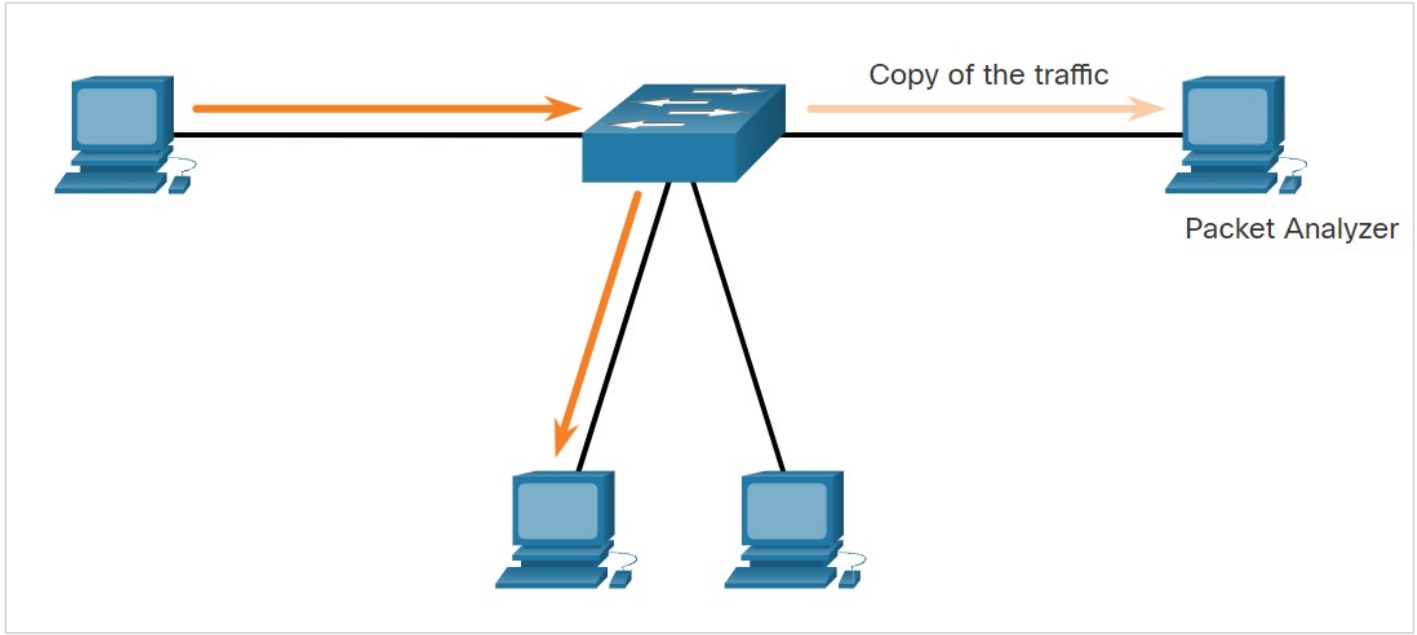
- NetFlow is a Cisco IOS technology that provides statistics on packets flowing through a Cisco router or multilayer switch.
- NetFlow provides data to enable:
  - network and security monitoring,
  - network planning
  - traffic analysis to include identification of network bottlenecks
  - IP accounting 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.



PC 1 connects to PC 2 using HTTPS

Port Mirroring

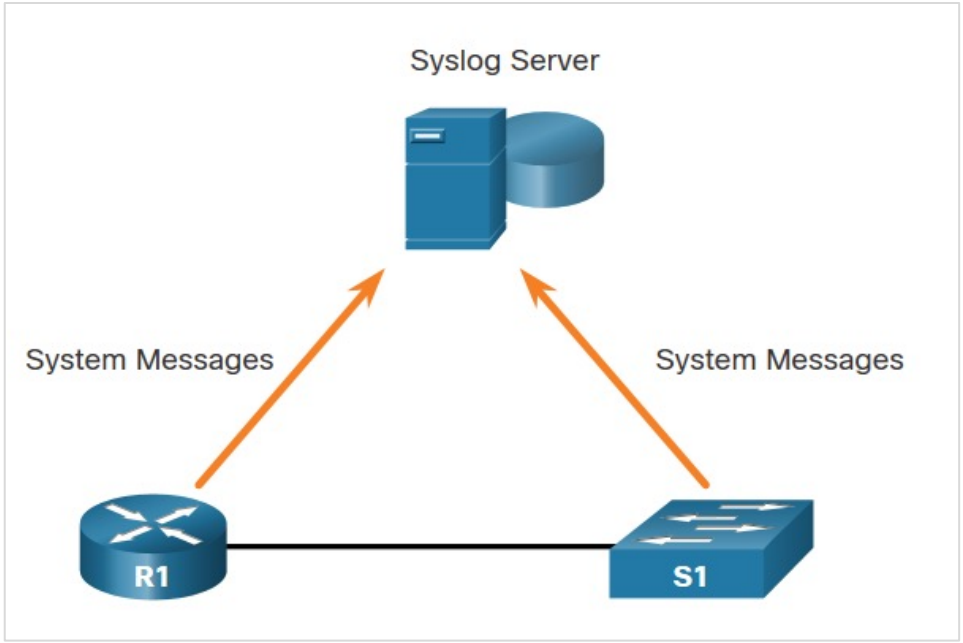
Port mirroring is a feature that allows a switch to make duplicate copies of traffic passing through a switch, and then sending it out a port with a network monitor attached.



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

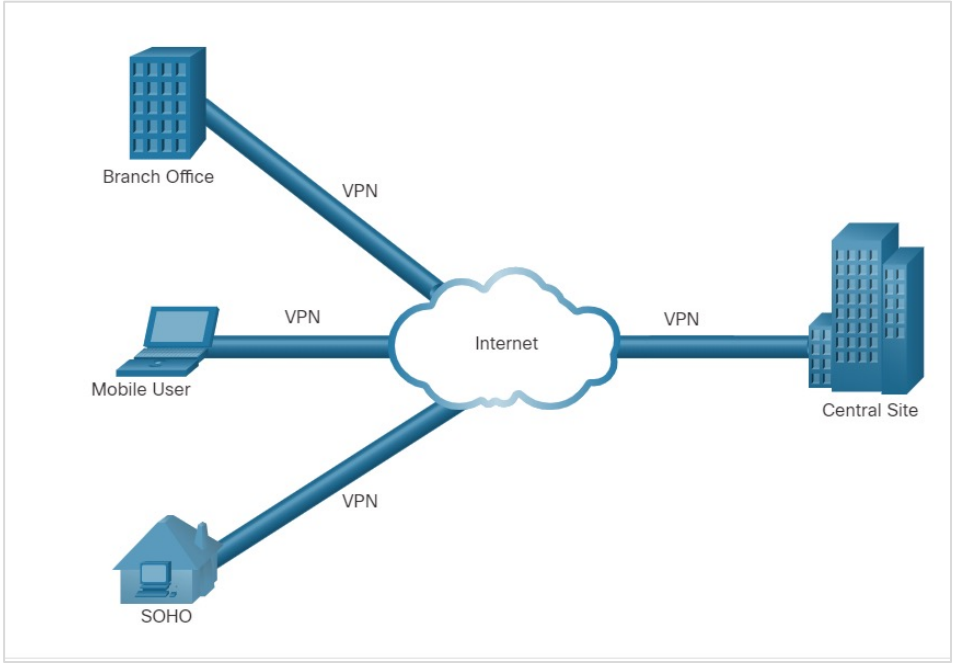
AAA Servers

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."

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

New Terms and Commands

• Local Area Networks (LANs) • Wide Area Networks (WANs) • Intrusion Detection Systems (IDS) • Intrusion Prevention Systems (IPS)	• Access Control List (ACL) • Simple Network Management Protocol (SNMP) • Network Time Protocol (NTP)

Lab 17 - Identify Packet Flow

- In this lab, you will complete the following objectives:
  - Observe packet flow in a LAN and WAN topology.
  - Observe how the packet flow path may change when there is a change in the network topology.