Networking

Networking Implementation

2.1.1 Networking Devices

What are different networking devices and what are their purposes?

Overview

The student will compare and contrast various devices, their features, and their appropriate placement on the network.

Grade Level(s)

10, 11, 12

Cyber Connections

- Threats & Vulnerabilities
- Networks & Internet
- Hardware & Software

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

CYBER.ORG

Teacher Notes:

CompTIA N10-008 Network+ Objectives

Objective 2.1

- Compare and contrast various devices, their features, and their appropriate placement on the network.
    - Networking devices
        - Layer 2 switch
        - Layer 3 capable switch
        - Router
        - Hub
        - Access point
        - Bridge
        - Wireless LAN controller
        - Load balancer
        - Proxy server
        - Cable modem
        - DSL modem
        - Repeater
        - Voice gateway
        - Media converter
        - Intrusion prevention system (IPS)/intrusion detection system (IDS) device
        - Firewall
        - VPN headend

Networking Devices

Numerous devices connect network entities, hence why they're known as connectivity devices. Many devices, users are already familiar with (at least by name). We will discuss those required for creating the network connection in this lesson and discuss devices that connect to the network in lesson 2.1.2.

Devices Galore!

A *hub* is the device that connects all the segments of a network together in a star topology Ethernet network. This works by connecting each device directly to the hub via a cable. Multiple devices can be connected without needing to segment the network. A hub is a layer 1 device. Hubs have ports sizes of 4 ports, 8 ports, 16 ports and so on with a single collision domain.

Teacher Notes:

Every device connected to a hub is at "half-duplex" meaning we can either send information to the hub or receive information from the hub, but not at the same time.

An ***access point*** (AP) is a hub that accepts wireless clients through an analog wireless signal. APs are layer 2 devices. Home wireless routers can function as access points (but not all access points can function as a wireless router).

A ***bridge*** is a network device that connects two similar network segments together. The purpose of a bridge is to keep traffic separated on each side of the bridge to break up collision domains. Bridges are considered layer 2 devices because they use MAC addresses to make forwarding decisions. One example of a bridge is a wireless access point because it bridges wired Ethernet to wireless connections.

A ***switch*** connects multiple segments of a network together, like a hub. However, a switch is a layer 2 device. Switches have port sizes of 8 ports, 12 ports, 16 ports, 24 ports, 28 ports, 48 ports and so on, with each port having its own collision domain. A switch can provide packet filtering, unlike a hub. It is possible for a switch to provide Power over Ethernet (we'll discuss PoE further in objective 2.3).

A ***router*** is a network device used to connect multiple network segments together, into what is sometimes referred to as an internetwork (internet + network), a layer 3 switch, or a multilayer switch. A well-configured router can decide how to get network data to its destination. Routers are a layer 3 device because they use IP addresses to make forwarding decisions. Many devices referred to as routers are both routers and switches, providing the functionality of both (hence the layer 3 switch and multilayer switch names).

A ***modem*** is a device that modulates an analog carrier signal to encode digital information and demodulates the signal to decode the transmitted information. In layman's terms, a modem connects your network to the Internet. There are four kinds of modems: cable, DSL, fiber, and dial-up, but we only need to focus on ***cable modems*** and ***DSL modems*** for the Network+ exam. Cable modems deliver high-speed Internet (ranging between 10-500 Mbps) to your devices by using coaxial cables connecting the modem to a cable box or specific outlet in a wall. The Data Over Cable Service Interface Specifications (DOCSIS) standard enables high-bandwidth data transfer via existing coaxial cable systems that were originally used in the transmission of cable television program signals. DSL (digital subscriber line) modems use a cable to connects to a phone line to deliver Internet (speeds of 5-35 Mbps). Previous, dial-up sacrificed landline telephone usage while connecting to the Internet but DSL keeps the landline phone available for use.

Teacher Notes:

A home network may have a single device serve as the modem, router, switch, and access point (and is just referred to as a modem).

A ***repeater*** is an electronic device that can be used to increase network connect beyond the standard range. It works by receiving a signal, regenerating that signal, then resending that signal. It makes no forwarding decisions, it just "boosts" the signal, but can convert from one network media to another, like fiber to copper. Repeaters are layer 1 devices.

A ***media converter*** can convert one type of cabling to another. Some repeaters include a media converter as well, for example Ethernet-to-fiber.

Advanced Network Devices

A ***wireless LAN controller***, WLAN controller, or WLC, manages wireless network access points that allow wireless devices to connect to the network. The purpose of a WLC is to handle many wireless access points. A complete network can be configured on a single WLC and send the configurations out to the wireless access points. From a WLC, we can monitor the performance and security of the wireless devices.

To lessen the burden on an individual server, a ***load balancer*** can be used. Load balancers efficiently distribute incoming network traffic across a group of backend servers. Load balancers allow for large-scale implementations because we can scale up or down as needed based on the load coming into the web services. Load balancers also provide a failsafe because if one of the servers fails, another server or servers can take over for the failed server. There are additional functions with load balancers such as TCP offloading, SSL offloading, and caching.

A ***proxy server*** is a gateway between a client requesting a resource and the server providing that resource, commonly a user browsing the Internet. There are two main types of proxy servers: web proxy servers and caching proxy servers. Typically, a web proxy server creates a web cache. We have seen this in action when we have googled a site that we have visited before. A caching proxy server speeds up the network's service requests by using information from a client's earlier requests.

A ***voice gateway*** (or VoIP gateway) is used to connect an enterprise VoIP network with a telecommunications provider. A voice gateway converts the voice traffic into the necessary form for receipt. A common use is to convert between VoIP protocols and traditional PSTN (public switched telephone network, our traditional phone lines) protocols.

Teacher Notes:

Intrusion detection systems (IDS) and *intrusion prevention systems* (IPS) are important for network security. These systems are responsible for monitoring networks and packets for malicious activity. An IDS detects the problem and is in monitor mode whereas an IPS *prevents* threats by stopping them in real time. IPS can drop malicious packets, offer malware protection, and can reset the connection of source hosts.

A ***VPN concentrator/headend*** is a device that accepts multiple VPN connections from remote locations. VPNs create encrypted tunnels between a device and the location the device is trying to connect to. VPN concentrators are often integrated into a ***firewall***. Like firewalls, VPN concentrators can be either hardware or software. Firewalls only purpose is to act as a network's line of defense. They monitor and control incoming and outgoing network traffic based on predetermined security rules.