Networking

Networking Implementation

2.3.1 - Ethernet Switching Features

What are some common ethernet switching features?

Overview
Given a scenario, the student will be able to configure and deploy common Ethernet switching features.

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).

Teacher Notes:

CompTIA N10-008 Network+ Objectives

Objective 2.3

- Given a scenario, configure and deploy common Ethernet switching features
    - Port configurations
        - Data Virtual local area network (VLAN)
        - Voice VLAN
        - Media Access Control (MAC) address tables
        - Power over Ethernet (PoE)/Power over Ethernet plus (PoE+)
        - Spanning Tree Protocol
        - Carrier-sense multiple access with collision detection (CSMA/CD)
        - Address Resolution Protocol (ARP)
        - Neighbor Discovery Protocol

Ethernet Switching Features

VLAN Basics

A VLAN (virtual local area network) is a logical grouping of network users and resources connected to administratively defined ports on a switch. A VLAN is a segment(s) of a LAN, typically separated by switches, that can only be accessed by the systems on it. Organizations will have VLANs to help limit collisions on the network, to increase security as well as increase performance by limiting the number of network resources that packets travel across.

A data VLAN is a VLAN that is configured to only carry user-generated traffic. A voice VLAN is configured to carry voice traffic from an IP phone. Traffic used to manage a switch could also be part of a VLAN but that would be a different type of VLAN. It is common practice to separate these three.

Two more important terms are trunk port and trunk link. Trunk ports can carry multiple VLANs at the same time. A trunk link is a 100 Mbps or 1 Gbps point-to-point link between two switches, a switch and a router, or a switch and a server. This carries the traffic of multiple VLANs (up to 4,094).

Teacher Notes:

MAC/ARP Tables

In the OSI model, the 2nd layer of networking is the data link layer that controls the data being transferred between two nodes. One of the most important parts of this system is the switch and the ***address resolution protocol (ARP)*** which is used by all devices to find the destination address. The destination address is the MAC address of that certain device, this ARP table is sometimes referred to as a ***MAC address table*** since it holds all the MAC addresses of the devices on the network. When a user is trying to access the internet, they request the MAC address of the router, from the ARP, so it knows where to find the router so it can access the internet. In our Cybersecurity course, we go into detail on issues like ARP poisoning and MAC cloning.

Power over Ethernet

Power over Ethernet (PoE and PoE+) technology refers to a system of transmitting electrical power along with data to remote devices over a standard twisted-pair cable in an Ethernet network. PoE technology can be used with IP telephones, network cameras, WLAN access points, embedded computers, and more! The IEEE has standards for PoE and PoE+ called 802.3af and 802.3at, respectively. They describe how a powered device is detected and how power is given to a device from PoE/PoE+ technologies.

Spanning Tree Protocol

Spanning Tree Protocol (STP) is a link management protocol that provides path redundancy while avoiding looping in a network. The most common reason a loop occurs in a network is from trying to provide multiple levels of redundancy. Ethernet network function properly when only one active path exists between two stations. If looping occurs, the forwarding algorithm could duplicate packets. STP uses the Spanning Tree Algorithm (STA) to create a topology database and search out and destroy redundant links. Switches transmit Bridge Protocol Data Units (BPDUs) out to all ports to find all links between switches.

Teacher Notes:

CSMA/CD

When a device sending a frame is transmitting over a wired network, the carrier sense multiple access with collision detection (CSMA/CD) contention method is used. Wired computers can detect collisions where wireless stations cannot, making this method more efficient. When a host's or router's interface tries to send a frame, the wire is checked and as long as no traffic is detected, it is sent without checking a back-off timer. Although there is no back-off timer, it continues to listen and if a collision is detected, a jam signal is set out requiring all stations to stop transmitting. The two machines involved in the collision will wait a random amount of time before attempting to resume communication.

Hello Neighbor

A new technology with IPv6 that was not available with IPv4 is called the ***Neighbor Discovery Protocol (NDP)***. NDP operates at the link layer of the OSI model and is responsible for gathering necessary information for Internet communication. This includes local connection configurations, domain name servers, and gateways. NDP helps make data transmission more efficient and consistent across multiple networks and processes.