Networking

Networking Implementation

2.1.2 - Networked Devices

What are different devices that connect to a network and how do they differ?

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 2.2

- Compare and contrast various devices, their features, and their appropriate placement on the network.
    - Networked devices
        - Voice over Internet Protocol (VoIP) phone
        - Printer
        - Physical Access Control devices
        - Cameras
        - Heating, ventilation, and air conditioning (HVAC) sensors
        - Internet of Things (IoT)
            - Refrigerator
            - Smart speakers
            - Smart thermostats
            - Smart doorbells
        - Industrial control systems/supervisory control and data acquisition (SCADA)

Networked Devices

What Next, Smart Bricks?

In 2.1.1, we discussed all the different devices covered on the Network+ exam that are used to help setup a secure network. Here we'll discuss the actual devices that can connect to said networks.

Most phones in modern offices are a ***Voice over IP (VoIP) phones***. These phones, by name, connect over Internet Protocol rather than analog phone line or the POTS (plain old telephone service). Each device is a computer, having a separate boot process, network connection, individual configurations, and different capabilities and functionalities.

Rather than every computer being physically connected to its own ***printer***, a printer can be shared on the network if the printer has a NIC card installed or by using a printer server that connects to the Ethernet network. These could be multi-function printers that are capable of copying, faxing, and scanning as well.

Teacher Notes:

Another common feature for most modern offices are ***physical access control devices***. One example is a key point such as a door or a gate requiring a smart card or badge for access. These devices are connect to an authorization server on the network. A user will scan their badge, the server performs a lookup and the response is sent back to the access control device to either permit or prohibit entry. Biometric authentication could also be incorporated like a fingerprint scanner, retina scanner, or voiceprint.

Cameras can be used to replace physical guards as a part of CCTV (closed circuit television). These cameras can include features such as motion recognition, object detection, or heat and metal sensing. Along with video surveillance, some cameras are also able to capture and record audio.

Another important device that isn't always thought about as a networked device is ***HVAC (heating, venting, and air conditioning)***. Modern HVAC systems use sensors to monitor and control heating and cooling. Users can manually adjust controls or they may be programmed to adjust automatically, saving money if the system isn't needed to run. HVACs need to be integrated into the fire system to mitigate any damage if a fire were to occur.

Smart Devices

In 1992, IBM produced the first smartphone and released it to the public in 1994. Arguably, in the early 2000s, smartphones "took off" and other devices started gaining the ability to connect to the Internet. Simply put, the ***Internet of Things (IoT)*** refers to physical devices that embedded with sensors, software, and other technologies for the purpose of communicating over the Internet. ***Refrigerators, smart speakers, smart thermostats***, and ***smart doorbells*** can be connected to the Internet to gain additional functionality. Unfortunately, since these devices are connected to the Internet, malicious actors are capable of compromising them and if the Internet connection were to go down, these devices may cease functioning entirely.

While not necessary for Network+, a real concern is what can happen long-term if the servers shut down for some IoT devices. If curious, google "GNARBOX," a portable backup & editing system for cameras as an example of a machine that has lost most of its functionality since the company has gone under.

Teacher Notes:

SCADA

SCADA stands for ***Supervisory Control and Data Acquisition*** System. SCADA is also sometimes referred to as ***Industrial Control Systems (ICS)***. SCADA systems are used in manufacturing or power distribution. You need a way to connect all your devices together so you can control them from one central location, that is why you would use a SCADA network.

SCADA is a distributed control system (DCS). The DCS is a system of sensors, controllers, and associated computers that are distributed throughout a plant with real-time access. SCADA systems allow for centralized control of very large industrial systems. When discussing a SCADA system that manages power infrastructure, there are security concerns which is why you will see most of them on their own private segmented network. Usually these are air gapped so there is no internet or access outside of the immediate network.