Networking

Networking Implementation

2.4.3 - Wireless Technologies

What are some different wireless technologies and how do they differ from each other?

Overview

Given a scenario, the student will be able to install and configure the appropriate wireless standards and technologies

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 2.4

- Given a scenario, install and configure the appropriate wireless standards and technologies
    - Antenna Types
        - Omni
        - Directional
    - Encryption standards
        - WiFi Protected Access (WPA)/WPA2 Personal [Advanced Encryption Standard (AES)/Temporal Key Integrity Protocol (TKIP)]
        - WPA/WPA2 Enterprise (AES/TKIP)
    - Cellular technologies
        - Code-division multiple access (CDMA)
        - Global System for Mobile Communications (GSM)
        - Long-Term Evolution (LTE)
        - 3G, 4G, 5G
    - Multiple input, multiple output (MIMO) and multi-user MIMO (MU-MIMO)

Wireless Technologies

Rabbit Ears

Wireless antennas are both transmitters and receivers. We classify them into two types, ***omnidirectional*** and ***directional***. Omnidirectional antennas (sometimes called point-to-multipoint) send and receive signals equally from all directions. Directional antennas pull in signals best from one direction. Directional antennas can provide a greater range because all their power is focused on a single direction.

Protecting WiFi

Even within an office, the convenience of portability is important. However, with that portability comes a need for WiFi and with that, a need for securing that WiFi. One way of encrypting WiFi communication is ***WiFi Protected Access (WPA)***. WPA replaced WEP (Wired Equivalent Privacy) because WEP had a serious cryptographic weakness.

Teacher Notes:

Because of this cryptographic weakness, we needed a "bridge" to run on existing hardware that would temporarily provide better security than WEP. We created WPA using an encryption cipher of RC4 with ***Temporal Key Integrity Protocol (TKIP)***. This improved on WEP by having a larger initialization vector and an encrypted hash. Every packet is assigned a unique 128-bit encryption key.

Although WPA is an improvement on WEP it still has its own weaknesses. Since all wireless computers are both transmitters and receivers, we need to encrypt the data. WPA2 and WPA3 helped solve this by ensuring that only people with the right key can transmit and listen. WPA2 uses CCMP block cipher mode. CCMP uses the AES encryption for data confidentiality and CBC-MAC for message integrity check.

In home networks, we use WPA2 or WPA3 with a pre-shared key. Everyone on the network uses the same 256-bit key. This is sometimes referred to as WPA/2/3-Personal or WPA/2/3-PSK. At the enterprise level, each individual user authenticates with an authentication server like RADIUS. This is sometimes referred to as WPA/2/3-Enterprise or WPA/2/3-802.1X.

Cellular Technologies

When implementing cellular and mobile wireless technologies and configurations, there are some options to consider

Code-division multiple access (CDMA): CDMA assigns a unique code to every call or transmission and spreads the data across the spectrum. This allows the call or transmission to be broadcast across all frequencies.

Global System for Mobile Communications (GSM): GSM is a type of cellular phone that contains a subscriber identity module (SIM) chip. These chips contain the subscriber's information and are required for the phone to function. A cybersecurity attack known as SIM cloning allows a malicious user to make a copy of the SIM chip and make calls as if they are the original user.

Long-Term Evolution (LTE): LTE and 4G LTE are commonly used interchangeably. When 4G was first released, phone couldn't actually reach the minimum speed the standard mandated.

Teacher Notes:

The regulating body decided that, even though the minimum speed could not be reached, devices could be labeled 4G as long as they provided an improvement over 3G.

3G, 4G, 5G: Starting with 3G (third generation), cellular communication was revolutionized. 3G provided 2 Mbps which, at the time, was a huge amount of bandwidth. 3G provided the start of smartphone applications. 4G (as mentioned above) improved upon 3G. 5G is capable of speeds up to 100 times faster than 4G. As reference, here's a table comparing the three.

Technology	3G	4G	5G
Bandwidth	2Mbps	200 to 1000 Mbps (1 Gbps)	1 to 10 Gbps
Standards	WCDMA, CDMA- 2000	CDMA, LTE, WiMAX	OFDM, MIMO, nm Waves

MIMO

As seen above, ***Multiple-Input, Multiple-Output (MIMO)*** is one of the standards for 5G. MIMO works by sending multiple frames via multiple antennas over multiple paths and then recombined by another set of antennas to optimize throughput and multipath resistance. This is known as spatial multiplexing. ***Multiuser Multiple-Input, Multiple-Output (MU-MIMO)*** improves upon MIMO by allowing multiple users/devices transmit at once.