

Module 5.3: Secure WLANs

Endpoint Security | Cisco Networking Academy
Prepared by: Kudzaishe Majeza

Agenda

- ▶ SSID Cloaking and MAC Address Filtering
- ▶ 802.11 Original Authentication Methods
- ▶ Shared Key Authentication
- ▶ Authenticating a Home User
- ▶ Encryption Methods
- ▶ Enterprise Authentication
- ▶ WPA3
- ▶ Summary & Key Takeaways

SSID Cloaking & MAC Address Filtering

- ▶ SSID cloaking hides the network name from broadcasts.
- ▶ MAC Address Filtering allows only approved devices.
- ▶ These methods provide basic security but are not foolproof.

802.11 Original Authentication Methods

- ▶ Open Authentication allows any device to connect.
- ▶ System authentication checks device identity.
- ▶ Early methods lacked strong security protections.

Shared Key Authentication

- ▶ Uses a shared secret key.
- ▶ Vulnerable to key capture attacks.
- ▶ Rarely used today due to weak security.

Authenticating a Home User

- ▶ Home users typically use WPA2 or WPA3 with a passphrase.
- ▶ Security depends on strong passwords.
- ▶ Default credentials should always be changed.

Encryption Methods

- ▶ WEP is outdated and insecure.
- ▶ WPA improved security but has weaknesses.
- ▶ WPA2 uses AES encryption.
- ▶ WPA3 provides the strongest protection.

Authentication in the Enterprise

- ▶ Uses centralized authentication servers.
- ▶ Supports user-based access control.
- ▶ More secure than shared passwords.

WPA3

- ▶ Latest Wi-Fi security standard.
- ▶ Protects against brute-force attacks.
- ▶ Provides forward secrecy.
- ▶ Recommended for modern networks.

Summary

- ▶ Wireless security requires strong authentication.
- ▶ Encryption protects data confidentiality.
- ▶ WPA3 offers the best WLAN security today.