Cambium Networks™

2019

Wireless Security

Azif

Agenda

1. Authentication and Encryption
2. Evolution of wireless security
3. Encryption and authentication standards
   - WEP, WPA, WPA2, WPA3…
   - Types of EAP, General EAP call flow, When to use EAP-PSK/802.1x?
4. Secure way to connect public wireless
5. Additional layers of securities like
   1. Management Frame Protection.
   2. Vlan for wired traffic separation.
   3. Mac authentication.
   4. Access Control Lists.
   5. Rouge AP detection.
6. Best practices for wireless security

Authentication and Encryption

- What is Authentication?
  - Dictionary definition: act of showing something is real, true or genuine.
  - Could be password, certificate or a token.
  - Needs an Authentication server to validate credentials.

- What is Encryption?
  - Process of scrambling of plain text data in such a way that can be only read by the legitimate user.
  - A malicious user in the network will not able to read the actual data, even though he get the scrambled data.

Evolution of wireless security

- On ethernet networks connectivity more important than layer 2 security. (Need physical access)
- With the development of 802.11 standard, layer 2 security become essential. (Data transmitted over air)
- So along with the development of 802.11 standard, layer 2 Security Standards also evolved,
  - In 1997 Wired Equivalent Privacy (WEP) was introduced as part of 802.11 standard.
    - This is mainly to provide wireless data confidentiality (WEP64 and WEP128)
    - WEP uses RC4 to encrypt 802.11 wireless data packet.
  - In 2003 Wi-Fi Protected Access (WPA) was announced by Wi-Fi Alliance.
    - WPA was a gap filling before actual 802.11i (WPA2) standard release.
    - WPA uses TKIP(Temporal Key Integration Protocol) for encryption, actually it was designed by 802.11i task group.
    - TKIP also uses RC4 to encrypt 802.11 wireless data packets, but is better than WEP.
  - In 2004 Wi-Fi Protected Access 2 (WPA2) was announced by Wi-Fi Alliance.
    - WPA2 certification mandates the elements of 802.11i protocol.
    - Encryption method CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) is used to encrypt wireless data packets. Based on AES.
    - WPA2 still secure: but use complex passphrases. Enterprise better than Pre-shared-keys.
  - In 2018 Wi-Fi Protected Access 3 (WPA3) was announced by Wi-Fi Alliance.
    - Evolving Standard.

Encryption and Authentication Standards

- **WEP64/WEP128 (Deprecated by IEEE. No longer secure)**
  - Usually the passphrase is configured using 10 or 26 Hexadecimal characters (shared key) / Configured using 5 or 13 ASCII characters.
  - Unfortunately still some of the old 802.11a and 802.11b clients only have the capability of WEP encryption.
  - We highly recommend not to use WEP due the weakness of protocol.
  - Configuration of WEP in cnPilot / cnMaestro via a service CLI just for these old clients.

Encryption and Authentication Standards

- **Wi-Fi Protected Access (WPA - TKIP) – (Deprecated)**
  - WPA -TKIP was an interim solution to replace WEP, but TKIP uses the same underlying mechanism like WEP.
  - TKIP uses the shared key and IV pass through a key mixing function before passing it to RC4.
  - Key mixing function exclude the WEP key recovery attacks, but still it was prone to other vulnerabilities.
  - We don’t recommend using WPA as an encryption method as it is insecure.
  - By Default WPA – TKIP mode is disabled in cnPilot / cnMaestro, but this can be enabled using CLI or user defined override for clients that can only do TKIP.

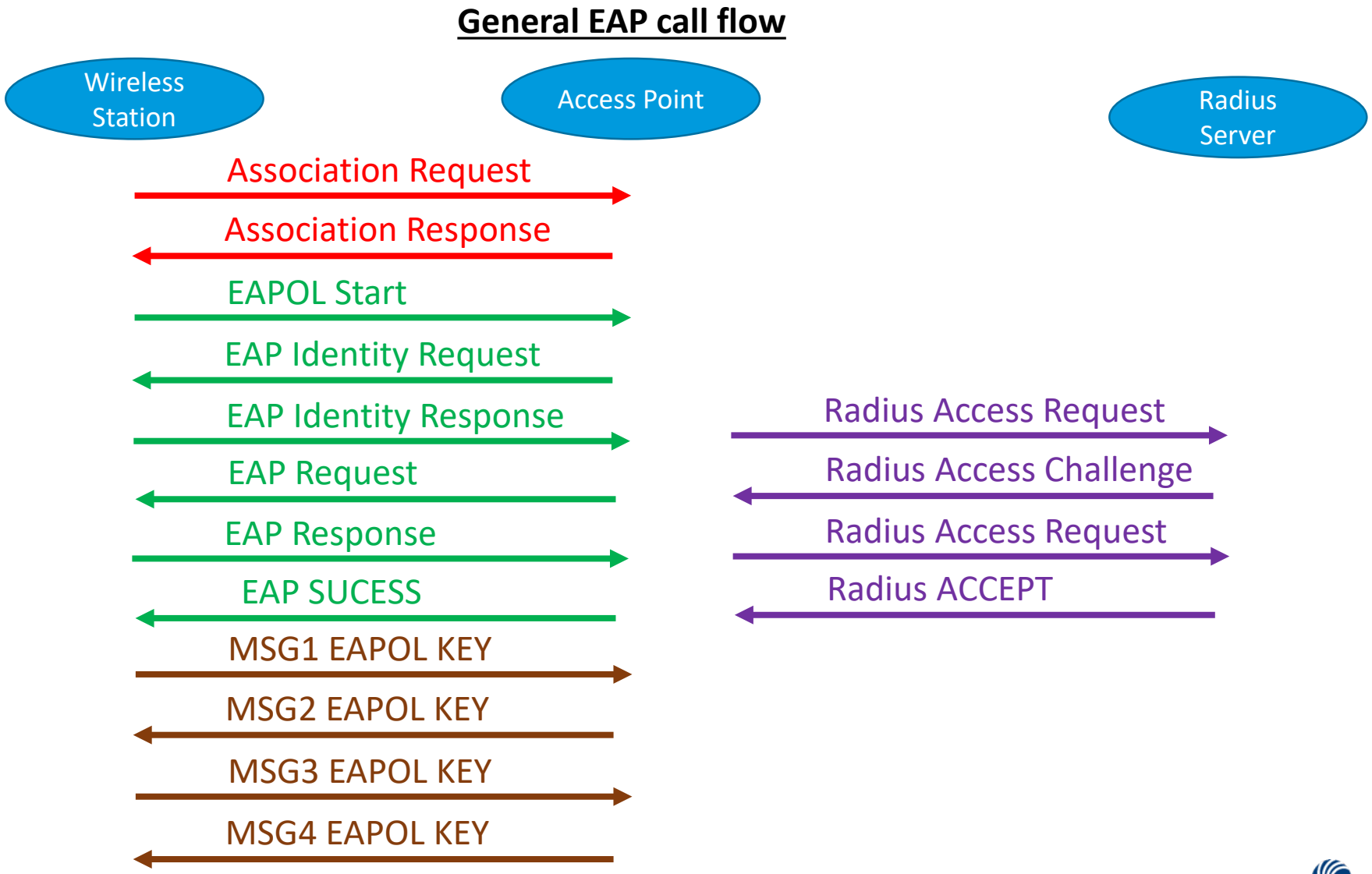
Encryption and Authentication Standards

- Wi-Fi Protected Access 2 (WPA2)
  - WPA2 uses AES as the encryption mechanism for good security..
  - Two authentication modes of Protected Access:
    - WPA2- Personal (PSK)
      - WPA2-PSK was commonly used method for securing the small wireless network.
      - User need to key in the pass phase, which will be used as the Pairwise Master Key.
      - In WPA2 Personal, wireless data is encrypted using a per-session 128 bit AES key derived from a 256 bit shared key.
    - WPA2- Enterprise (802.1x)
      - WPA2-802.1x authentication, which needs a radius server for authenticating the user.
      - End of Radius authentication, the AP receives the session master-key which is used for generating the per-session encryption key./
  - For encrypting the unicast , broadcast / multicast data, two different keys are generated via a 4-way handshake.
  -

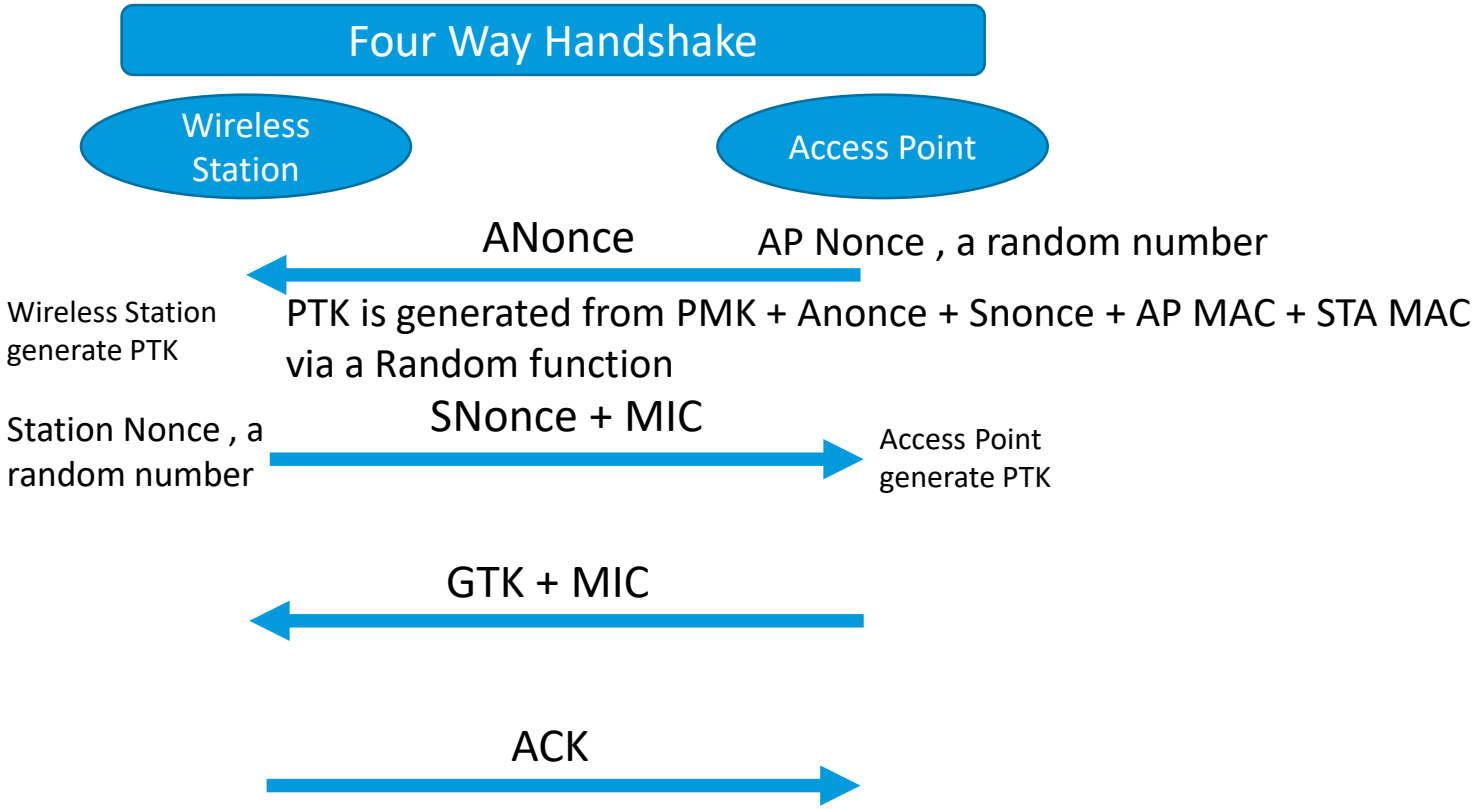
Flavors of EAP

- **Flavors of EAP**
  - ***EAP-TLS (Transport Layer Security):-*** Is the most secure method of authentication as it verify both client and server side certificates. Server uses TLS to demonstrate that it holds a digital certificate and request the same from client. And client as well request the same from the server and exchanges the identity and keying material.
  - ***EAP-TTLS (Tunnel TLS):-*** This method server authenticate using the certificate and client uses its identity using any authentication method like PAP,CHAP, or MS-CHAPv2 . The actual identity of client is send through the TLS Tunnel.
  - ***EAP-PEAP (Protected EAP):-*** This method is very similar to EAP-TTLS except the client authentication uses another authentication such as EAP-MSCHAPv2 or EAP-GTC.
  - ***EAP-SIM/AKA (Subscriber Identity Module):-*** This is most common authentication method in cellular network, which uses SIM card as the identity and getting verified with the GSM authentication server. Heavily used in Passpoint / Hotspot 2.0 networks.

General EAP Call flow



4Way EAPOL handshake



Four way handshake is used to generate PTK (Pairwise Transient Key) and GTK (GroupWise Transient Key).
PTK is used for encrypting unicast wireless data packets.
GTK is used for encrypting broadcast and multicast wireless packets. This is same for WPA/WPA2-PSK and WPA/WPA2-802.1x.

When to use WPA2-Personal, when to use WPA2-Enterprise

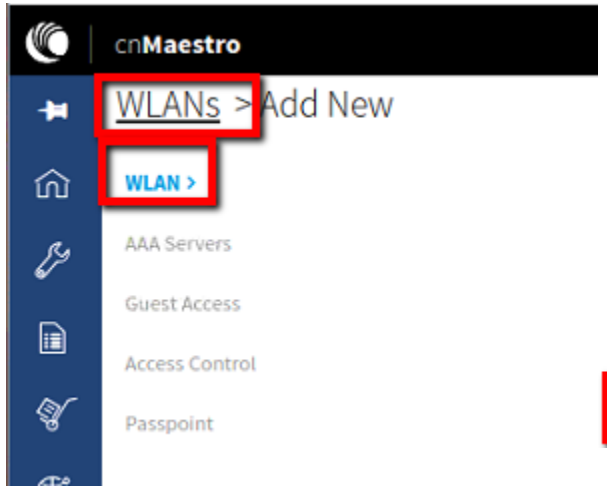
- WPA2-Enterprise is always preferred:
  - Provides stronger security than passphrases
  - Easy to revoke credentials for a particular user
  - Easier to apply per-user policies

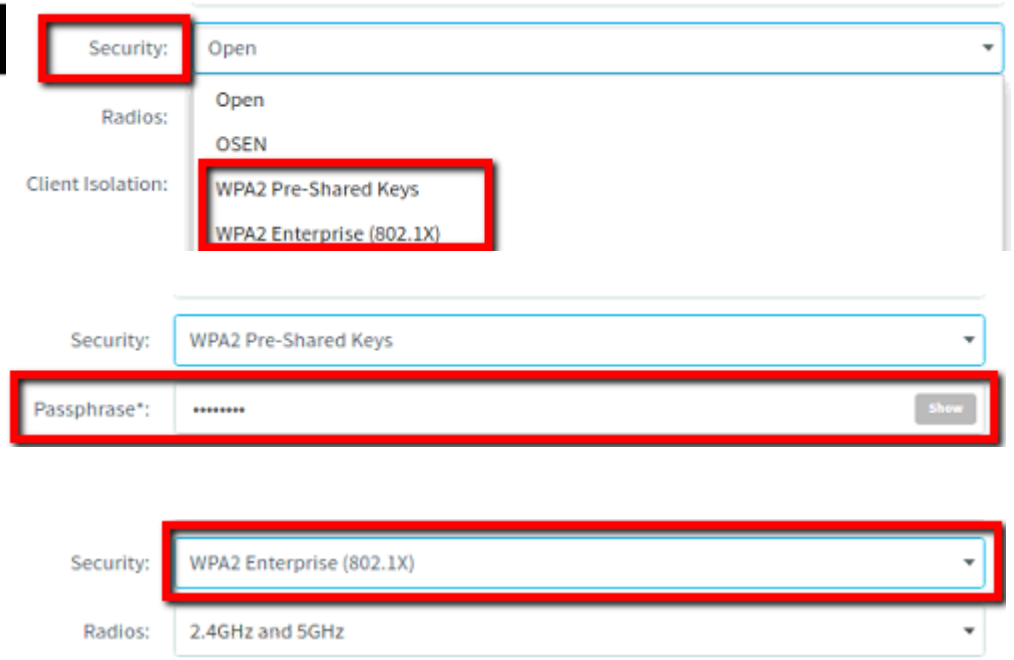
- WPA2-PSK might be needed because:
  - Easier to manage and set up (does not need a RADIUS server)
  - Supported by more clients than WPA2-Enterprise
  - Does not require certificate or token management (easier on IT)

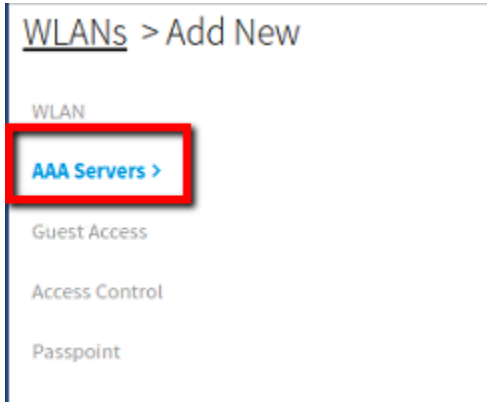
If using WPA2-PSK, recommend using strong (complex) passphrases.

WPA2 Configuration on cnMaestro

WPA2-PSK / WPA2-802.1x can be configuring from Wireless Lan context → Configuration → Security.
In case of WPA2-PSK , user needs to configure the pass phrase
And for WPA-802.1x, user needs a AAA server address for Authentication, Authorization and Accounting.







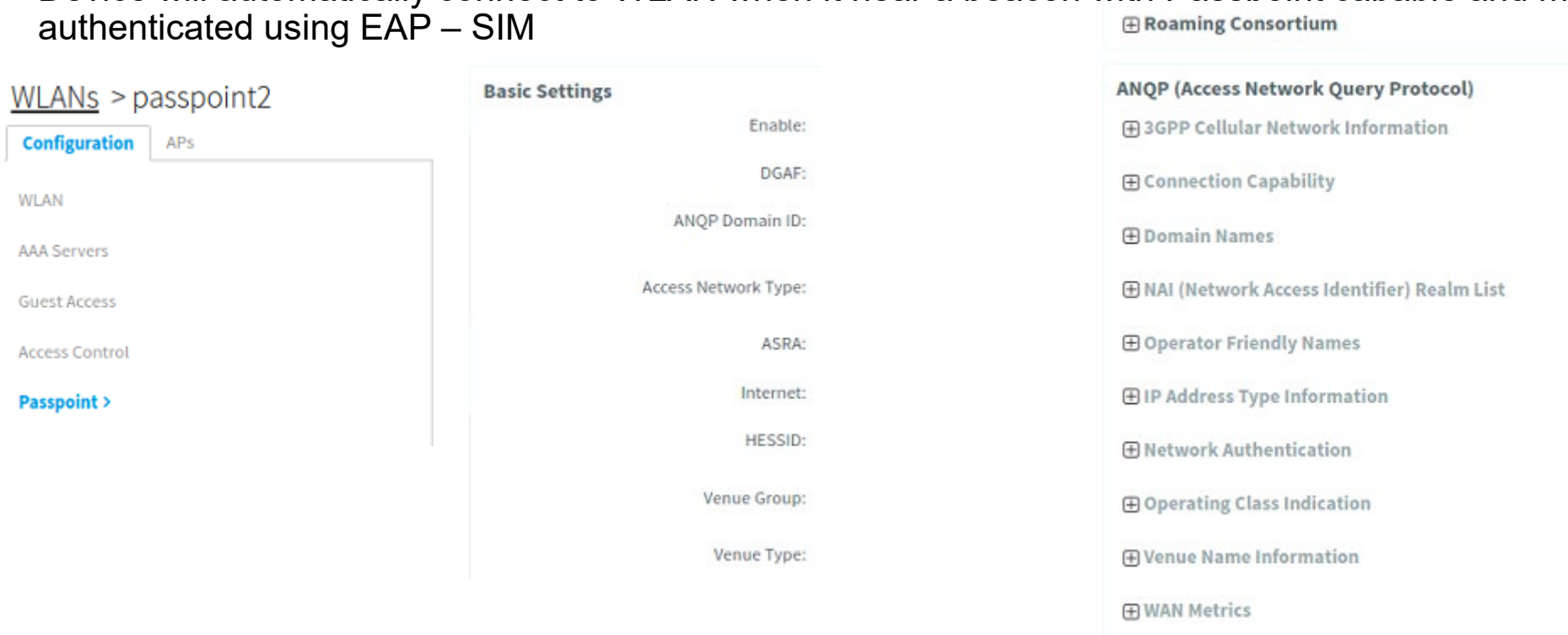
Cambium Networks™

WPA3

- Wi-Fi Alliance announced an improvement over WPA2, called WPA3 with two distinct mode of operation.
- WPA3-SAE (Personal) :- more resilient, password-based authentication uses Simultaneous Authentication for Equals (SAE), a secure key establishment protocol between wireless client and Access point.
  - Provide stronger protections for users against password guessing attempts by third parties
- WPA3-Enterprise :- Offers192-bit cryptographic strength (Compared to 128-bit)
- In April 2019, researchers discovered some WPA3 design flaws, vendors are updating implementations accordingly.

Secure way to connect public wireless

- Passpoint / Hotspot 2.0
  - Seamless, secure connection to Wi-Fi hotspot networks
  - This eliminates the need of user to find wifi and authenticate the network each time they connect.
  - Device will automatically connect to WLAN when it hear a beacon with Passpoint capable and mostly it will be authenticated using EAP – SIM



Cambium Networks™

Management Frame Security

- 802.11w PMF (Protected Management Frames)
  - 802.11w amendment added management protection functionality to the 802.11 standard.
  - Encrypts some of the management frames like de-authentication , dis-association and some action frames after successful authentication.
  - Protects from hackers/attackers injecting management frames onto a network, disruption legitimate user connection.

VLAN for WIRED traffic

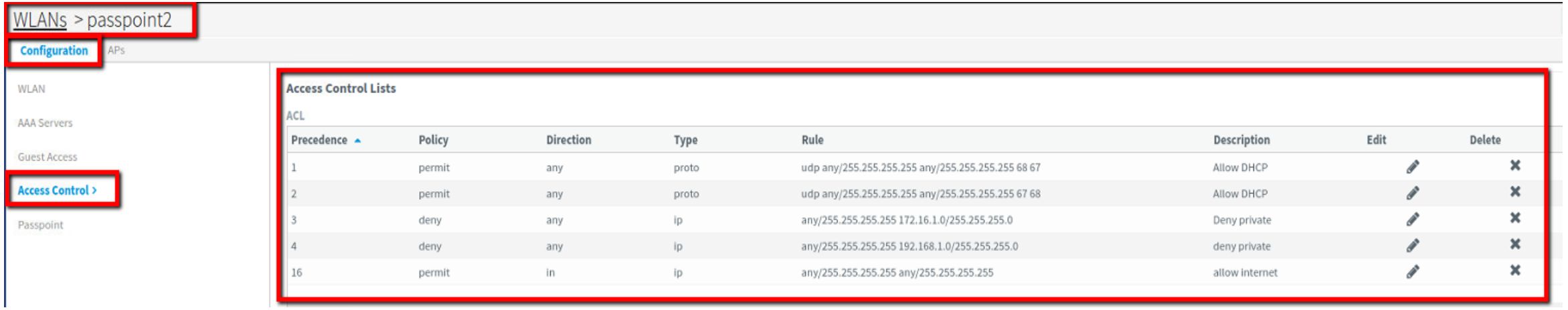
- Wired Traffic Separation
  - Vlans (Virtual LAN) allow network level separation and firewall the traffic based on the requirement.
  - Two ways of assigning the VLANs
    - Static VLAN:- Assignment of VLANS based on the wlan
    - Dynamic VLAN:- Assignment of VLANS based on the user / device

Additional layers of security

- MAC Authentication
  - In addition to WPA2, as a second layer of security.
  - MAC can be spoofed, so not recommend using by itself.
  - Some of the headless devices may not be friendly with WPA/WPA2 can be put to mac auth wlan and apply policies based on the network requirements.

Additional layers of security

- Access Control List
  - Additional security can be configured using ACL
  - It can be L2 , L3 or L4 access control list based on the your network requirement
  - Can be navigated from cnMaesto -> WLAN -> Configuration -> Access Control



Cambium Networks™

Rogue AP and Wireless Intrusion Detection

- Rogue APs are typically APs connected onto your wired network by some user trying to gain access to the network remotely. Could be a malicious user, or even someone plugging in an AP for convenience.
  - PROBLEM: Bypasses all your authentication controls and encryption standards.
  - SOLUTION: Enable rogue-detection on your wireless infrastructure and monitor for rogues.
- Wireless Intrusion Detection (WIDS) looks for malicious users carrying out attacks on the network denying service to legit users.

Best Practices for Security

- Avoid open wireless networks, always use authentication and encryption .
- Use certificate based authentication or very strong password enforced to the users.
- Enable PMF for protecting the wireless network from attacks like de-authentication.
- Keep all devices (APs, client-devices, servers) patched up to latest software releases from vendors.
- Use strong passwords for access points and controllers.

Thank You