Content

Chapter 1 Protected Management Frames

1.1 Standard Custom and Application

1.1.1 Introduction to 802.11w Protocol

IEEE 802.11w wireless encryption standard is based on the framework of IEEE 802.11i (agreement on the protection of data frame), which can resist the attack of the wireless LAN (WLAN) management frame, to protect the associated frame between the client and the AP. It can prevent wireless network attacks, and protect the security of the client network. IEEE Task Group is improving IEEE 802.11 medium protection layer, the purpose is to provide data integrity, the authenticity of the data source and replay protection.

IEEE 802.11w can provide protection in three main types of frames. The first one is used for "Unicast management packet", which is a packet between a AP and a STA.IEEE 802.11w extends the temporal Key Integrity Protocol of IEEE 802.11i and encryption algorithm of RC4, it will extend the existing data encryption calculations to a unicast management frames.In this way, you can prevent attackers from forging the management packets, so as to be blocked by the decryption engine, thereby increasing privacy. The second is a "broadcast management frames", and such information is usually used to adjust the radio frequency or start measure,does not need to be kept secret, like a single point of packet and broadcast packet encryption action is more complex than unicast packets. Therefore, 802.11w IEEE only for this kind of broadcast packets to provide forgery, the protection of the eavesdropping, it does not provide the protection of encryption, only rely on a set of information integrity code is attached to a non-encrypted management package.The last method is used for "deauthentication and disassociation frames", through a pair of one-time keys on the AP and STA, it can be determined using the end whether the lifting frame work.

1.1.2 Introduction to PMF Service

WIFI is a broadcast medium that can be involved in both legal and illegal devices. Management frame (such as authentication frame, deauthentication frame, association frame, disassociation frame, probe frame and beacon frame) are used to initiate or shut down the client service of network session.Data frames can be encrypted (TKIP or CCMP) to protect the security of data, but the management frame must be transparent transmission in order to be understood by all clients.Because it is transparent transmission, the associated frame must be protected from the wireless network attack.802.11w agreement through PMF (Protected Management Frames) service defines a set of powerful management framework to prevent wireless attacks, including the following management frames:

- Disassociation
- De-authentication
- Spectrum Management
- QoS
- DLS
- Block Ack
- Radio Measurement
- Fast BSS Transition
- SA Query
- Protected Dual of Public Action
- Vendor-specific Protected

1. The wireless frames which do not support PMF:
    1) Beacon and Probe Request/Response
    2) Announcement traffic indication message(AITM)
    3) Authentication
    4) Association request/response
    5) Spectrum Management Action
2. The wireless frames which support PMF:

    The management protection frame can use the protection key layer of 802.11 after the key is created. The RFC amendment of 802.11w says that only the frame of TKIP/AES is protected but the frame of WEP/OPEN is not protected.

    1) Disassociation and Deauthentication
    2) Radio Measurement Action for infrastructure BSS(802.11k frames)
    3) Qos Action Frame(802.11e frames)
    4) Future 11v management frames(802.11v frames)

1.1.3 Introduction to Robust Management Frame Protection

•CCMP

- Unicast robust protected management frames
- Start after the key agreement is completed (4-way handshaking)
- Provides the data confidentiality, data source authentication, integrity protection and replay protection for the unicast robust management frames.

- The provisional key is same with the one used in the CCMP protected unicast data frame.
- The compute of AAD is the same; the compute of Nonce is changed.

•BIP

- Broadcast/Multicast Integrity Protocol
- Multicast robust protected management frames
- AES-128 algorithm based on CMAC (Cipher-based Message Authentication Code, 128bits data block, 128bits integrity key)
- Uses the key of IGTK, enables BIP after the successful IGTK conference.
- Adds an MIME after the frame subject.
- When the STA sends a protected multicast robust management frame:

  A. Chooses IGTK, creates MMIE, configures the MIC as 0, and configures the eyedD as the one of IGTK, inputs a monotone increasing nonnegative integer in IPN.

  B. Calculates ADD.

  C. Calculates AES-128-CMAC and inserts the 64bits outputs into the MIC field of MMIE.

  D. Combination frames, including IEEE 802.11 head, management frame subject (including MMIE) and FCS. MMIE should be in the end of the frame subject.

  F. Sends frames.

•SA Query Procedure

- Security Association Query
- Verifies the effectiveness of the current security association.
- Prevents the Association Lockout problem.
- Runs through the Action frame of SA Query.
- AP and STA both can start the process of SA Query.
- Two kinds of frames: SA Query Request and SA Query Response

1.1.4 Introduction to Issued PMF

When a user needs to modify to open PMF function, AC issued a profile, set PMF enable switch. After the AP is on-line, turn on/off function PMF according to the received profile configuration. AP stores the PMF’s enable switch to the configuration file, use in the creation of vap.

User Profiles PMF function modes as required, there are two kinds of models to choose from, compatible mode or force mode.

Compatible mode includes two kinds of situations, one is not carrying digital signature algorithm sha256 to open the management of the protection, and one is to carry the digital signature algorithm sha256 to open the protected management frames. AP configuration compatible mode, regardless of the terminal support 802.11w protocol or not, it can interact with AP.If the terminal support 802.11 w, the AP to interact with terminal based on 802.11 w agreement, if the terminal does not support 802.11 w, the AP can interact with terminal, which is not based on a 802.11 w agreement.

Force mode requires that the terminal must support 802.11w protocol, in order to interact with the AP, or the terminal can not be successful.

1.2 PMF Configuration

1. Enable/disable the pmf without sha256 digital signature under the compatibility mode.

Command	Explanation
Network Configuration Mode	
pmf enable **no pmf**	Enable the protected management frames function of compatibility mode. The no command disables the pmf function.

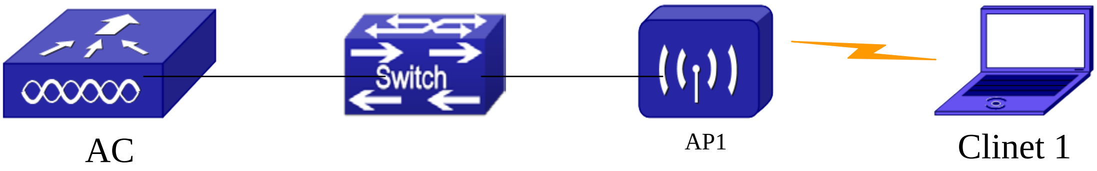
2. Enable/disable the pmf with sha256 digital signature under the compatibility mode.

Command	Explanation
Network Configuration Mode	
pmf enable-sha256 **no pmf**	Enable the protected management frames function of compatibility mode and enable to support SHA256. The no command disables pmf.

3. Enable/disable the pmf under the enforcement mode.

Command	Explanation
Network Configuration Mode	
pmf required **no pmf**	Enable the protected management frames function of enforcement mode. The no command disables pmf function.

1.3 PMF Configuration Examples



Set up the environment, AC is connected to AP through the switch or POE, AP is successfully managed, client1 is associated with AP1.

1.3.1 WPA2-PSK Configuration Examples

1. AC configuration: Configure the pmf, wireless authentication method, ssid, wireless encryption method, wap version, etc. under the network configuration mode.

   ```
   AC#config
   AC(config)#wireless
   AC(config-wireless)#network 1
   AC(config-network)# pmf enable
   AC(config-network)#security mode wpa-personal
   AC(config-network)#ssid vlan116
   AC(config-network)#wpa ciphers ccmp
   AC(config-network)#wpa versions wpa2
   ```

2. Configure the network and apply it.

   ```
   AC(config-wireless)#ap profile 1
   AC(config-ap-profile)#radio 1
   AC(config-ap-profile-radio)#vap 0
   AC(config-ap-profile-vap)#network 1
   AC#wirelessap profile apply 1
   ```

3. Make the terminal to associate with ssid vlan116, it can be successful.

1.3.2 WPA2-EAP Configuration Examples

1. AC configuration: Configure the pmf, authentication server name, accounting server name, wireless authentication method, ssid, wireless encryption method, wap version, etc. under the network configuration mode.

   ```
   AC#config
   AC(config)#wireless
   AC(config-wireless)#network 1
   AC(config-network)# pmf required
   AC(config-network)#radius server-name auth abcd1234
   ```

```
AC(config-network)# radius server-name acct abcd5678
AC(config-network)#security mode wpa-enterprise
AC(config-network)#ssid vlan116
AC(config-network)#wpa ciphers ccmp
AC(config-network)#wpa versions wpa2
```

2. Configure the network and apply it.

```
AC(config-wireless)#ap profile 1
AC(config-ap-profile)#radio 1
AC(config-ap-profile-radio)#vap 0
AC(config-ap-profile-vap)#network 1
AC(config-ap-profile-vap)#end
AC#wirelessap profile apply 1
```

3. Make the terminal to associate with ssid vlan116, it can be successful.

1.4 Configuration Notes

It is important to note that the WPA wpa2-psk and WPA - EAP require configuration CCMP encryption and configuration keys at the same time, so as to AP and STA wireless connection to support protected management frames. If only configure authentication and WPA version, not configuration WPA authentication key, the management of the wireless link frame will not be protected by PMF.

Unicast deauthentication frame, unicast disassociation frame, unicast frame action, AP send SA Query frame, AP sending SA Query response frame, the BIP protection radio frame, the message is within the scope of PMF protection.

When the deployment of the network within the scope of the STA part support 11 w, part does not support 802.11 w, in order to ensure compatibility, we can configure the PMF enable, PMF enable - sha256, of course, no PMF can also. When deployed on the network security requirements are relatively high, and network devices are supported by 802.11w, we can choose to configure the required PMF mode, but also to prevent unrelated terminal access. PC terminal can be used in the CMD window WLAN show netsh.exe driver to see whether the network card supports 802.11w protected management frames.

1.5 PMF Troubleshooting

If the PMF configuration is not effective or STA cannot be connected in using, please adopt the following steps to check out.

☞ Check if the hardware and version of the current AC and AP support the protected management frames function.

- Use **show wireless network 1 | include PMF** to check if the network corresponding to the ssid associated with the client is configured PMF and check what mode is configured.
- Check if the authentication method configured in network of AC is WPA2-PSK or WPA2-EAP.
- Check if the encryption method configured in network of AC is CCMP. TKIP or CCMP+TKIP do not support PMF.
- Check if the WPA version configured in network of AC is WPA2.
- Check if the terminal network card supports the 802.11w protocol. Currently, parts of Intel wireless network cards and win8.1 or the above systems are used cooperatively for supporting 802.11w.