CCNP Security - SISAS
Layer 2 Authentication - EAP

EAP – Extensible Authentication Protocol

- EAP is an authentication framework
  - Mainly used in Wi-Fi and wired
- 802.1x defines the encapsulation of EAP over IEEE 802, namely EAP over LAN (EAPOL)
- 802.1x is a flexible layer 2 authentication mechanism
  - Makes use of EAP methods, tunneled inside RADIUS packets
  - Currently there are about 40 different methods defined
- EAP method types
  - Tunneled (protects the supplicant's identity and credentials)
  - Non-tunneled (does not protect supplicant's credentials)

Common EAP Tunneled Methods

- PEAP - Protected EAP (developed by Microsoft, Cisco, RSA)
  - Two phase method
    - Phase 1, called outer method, used to authenticate server and form the TLS channel
    - Phase 2, called inner method, used to authenticate supplicant and protect its EAP identity
  - Theoretically, inner authentication method can be any EAP type
  - Mutual authentication
    - Server is always authenticated by certificate
    - Supplicant is authenticated by certificate (EAP-TLS), username/password (EAP-MSCHAPv2), or OTP (EAP-GTC)
    - Requires server certificates, on client is optional
  - Identity protection available only in PEAPv1 and PEAPv2

Common EAP Tunneled Methods

- EAP-FASTv1 (Flexible Authentication via Secure Tunneling)
  - Cisco proprietary, similar with PEAP in scope but very different in functionality
    - Developed to allow faster re-authentication and wireless roaming
  - Based on PAC files (Protected Access Credentials)
    - Can be seen as a cookie locally stored on the supplicant
    - Generated by the RADIUS server from a master key known by itself only
  - Three-phase method
    - Phase 0 is optional and used to provision the supplicant with a PAC file
    - Phase 1 is used to establish the TLS tunnel based on the PAC file
    - Phase 2 is used to authenticate the supplicant within the TLS tunnel
- EAP-FASTv2 (EAP Chaining)
  - Ties machine authentication to user authentication
    - Relies on machine PAC and user PAC
    - Performs double authentication within single EAP transaction
  - Will become standard, known as EAP-TEAP (RFC draft)

The image cannot be displayed. Your computer may not

Common EAP Tunneled Methods

» EAP-TTLS - Tunneled TLS (RFC5281)

- Very similar with PEAP
  - Two-phase method
  - Requires server side certificate
- Major difference as compared to PEAP is that inner method can use any authentication
  - Non-EAP methods such as PAP and CHAP supported
- Not widely implemented
  - Two versions EAP-TTLSv0 and EAP-TTLSv1

The image cannot be displayed. Your computer may not

Common EAP Non-Tunneled Methods

» EAP-TLS (RFC 5216)

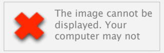
- Single phase protocol
- Mutual authentication based on certificates
- Requires client and server certificates
  - TLS tunneled created based on certificates
  - The RFC requires only server side certificates
- No supplicant identity protection
  - Passed in EAP-Identity and in certificate exchange

Common EAP Non-Tunneled Methods

- EAP-MD5 (RFC2284)
  - The only EAP method defined in original EAP RFC
  - Only supplicant authentication based on username/password
  - Challenge-response through MD5
- EAP-GTC (RFC3748)
  - Developed by Cisco as alternative to PEAP
  - Supports OTP through challenge-response based authentication of supplicant
- EAP-LEAP (Light EAP)
  - Cisco proprietary used only for wireless (WEP or TKIP keys)
  - Mutual authentication based on shared secret which is client’s password
  - Uses modified version of MS-CHAP, thus is challenge-response based
  - Supplicant authenticated based on username/password

802.1x Configuration Steps on Supplicant

- Configure the supplicant to use appropriate EAP method
  - It cannot be negotiated
- Two types of supplicants
  - Built-in operating system supplicant
  - Cisco AnyConnect NAM module
- Ideally do not let both supplicants configured



802.1x Configuration Steps on NAD

- Enable AAA
  - `aaa new-model`
- Configure dot1x default authentication list
  - `aaa authentication dot1x default group`
- Globally enable 802.1x
  - `dot1x system-auth-control`
- Enable 802.1x on switch port facing the supplicant
  - `dot1x pae authenticator`
- Enforce authentication on switch port facing the supplicant
  - `authentication port-control auto`
- Define RADIUS server settings
  - `radius-server host <IP> key <radius key>`
- Optionally configure other global/interface level settings

802.1x Configuration Steps on ISE

- Configure 802.1x authentication policy
  - Optionally use a default one
  - Enable same EAP method as on supplicant
- Configure authorization policy
  - Optionally use a default one
- Enroll ISE into PKI infrastructure
  - Only if tunneled EAP methods are used by supplicant
- Enroll ISE into Active Directory
  - Only if EAP-TLS or EAP-MSCHAPv2 is the authentication method of supplicant

802.1x Verification and Troubleshooting

» Verification

```
show dot1x all
show authentication session
show authentication interface <if_number>
show aaa servers
```

» Troubleshooting

```
show authentication session interface
<if_number>
debug dot1x all
debug radius authentication
```