Document Name: EAP

Extensible Authentication Protocol or EAP is an authentication framework for encapsulating authentication data.

Three main parts

1. Supplicant: Endpoint requesting access to the network (PC, Laptop, Mobile Device)
2. Authenticator: Network device controlling physical access to the network. (WLC, AP, Switch)
3. Authentication Server: Performs the actual authentication of the endpoint (ISE, NPS, ClearPass)

Most Common EAP types

Native EAP Types:

- EAP-TLS
  - One of most secure
  - X.509 Certs for mutual authentication (requires a CA)
  - Most desirable in BYOD deployments
- EAP-MD5
  - Hashes credentials
  - Common on IP Phones
- EAP-MSCHAPv2
  - Credentials encrypted inside a MSCHAPv2 session
  - Simple transmissions of credentials
  - Ability to integrate with AD
- EAP-GTC
  - Cisco alternative to MSCHAPv2
  - Enables more generic authentication

Tunneled EAP Types:

- PEAP (Protected EAP)
  - Proposed originally proposed by MS
  - Uses X.509 Certs
  - Uses an additional native EAP type for inner method
- EAP-FAST (Flexible Authentication via Secure Tunnel)
  - PEAP alternative created by Cisco
  - Faster re-auth
  - Faster roaming