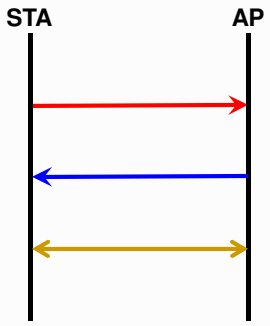
802.1X network authentication framework

IEEE 802.11i (WPA2)

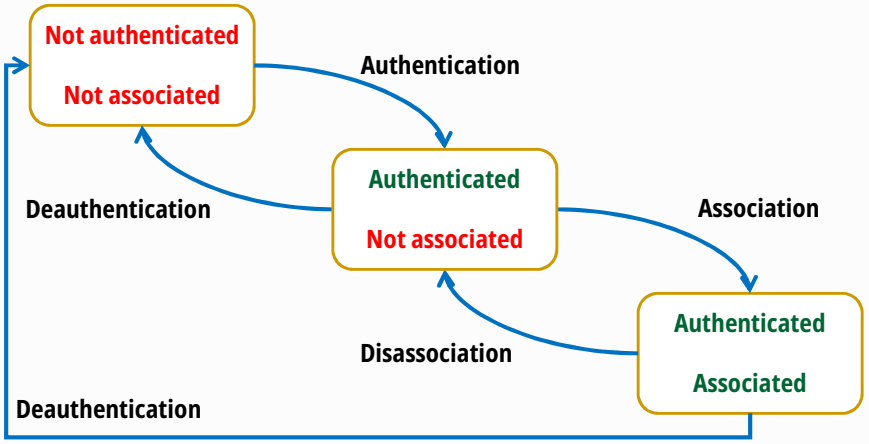
- Defines Robust Security Networks (RSN)
  - Those that support WPA and 802.11i
- Advanced security mechanisms for frame protection
  - AES for payload encryption and frame integrity control
- Uses 802.1X for network access authentication
  - Simplified Pre-Shared Key (PSK) mode for SOHO (Small Office, Home Office) environments
  - EAP-based protocol for enterprise environments

IEEE 802.11: Frame types

- Management frames
  - Beacon
  - Probe Request & Response
  - Authentication Request & Response
  - Deauthentication
  - Association Request & Response
  - Reassociation Request & Response
  - Disassociation
- Control frames
  - Request to Send (RTS)
  - Clear to Send (CTS)
  - Acknowledgment (ACK)
- Data frames



IEEE 802.11: Authentication & Association state machine



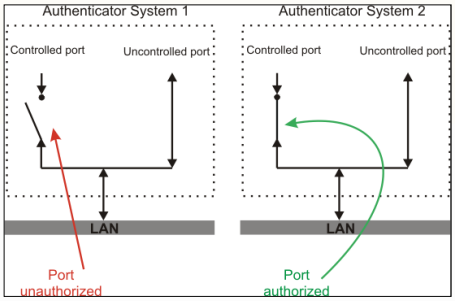
IEEE 802.11: Open System Authentication (OSA)

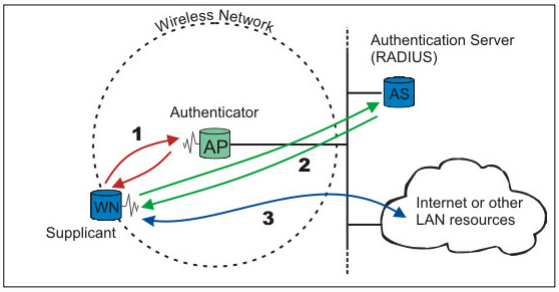
- No-authentication protocol
  - Designed for open networks
- Simple request/response message exchange that always succeeds
  - The goal is to pass the authentication step on the state machine

IEEE 802.1X: Port-Based Authentication

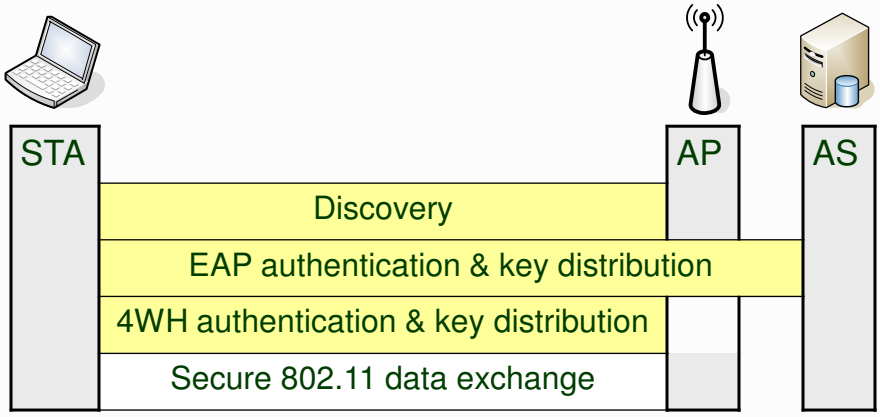
- Authentication model for all IEEE 802 networks
  - Layer 2 mutual authentication
- Originally conceived for large networks
  - University campus, etc.
  - Model was extended for wireless networks
- Performs key distribution

IEEE 802.1X: Architecture

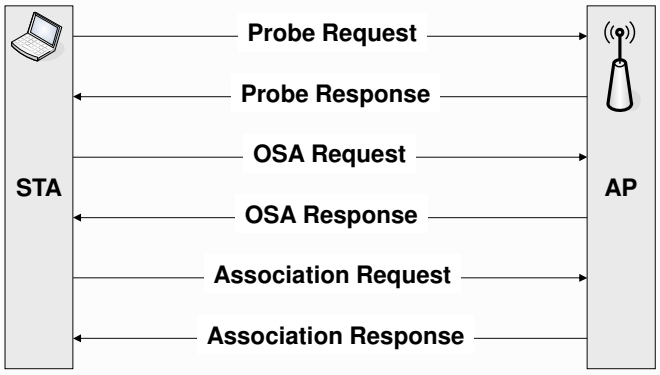




IEEE 802.1X: Operational phases

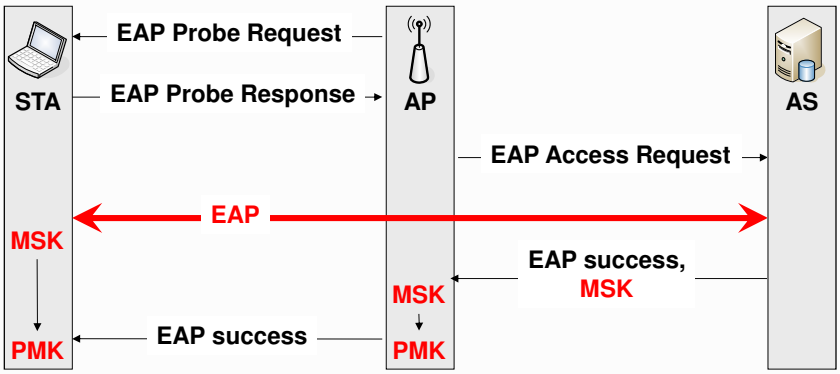


IEEE 802.1X Phase 1: Discovery (802.11 messages)



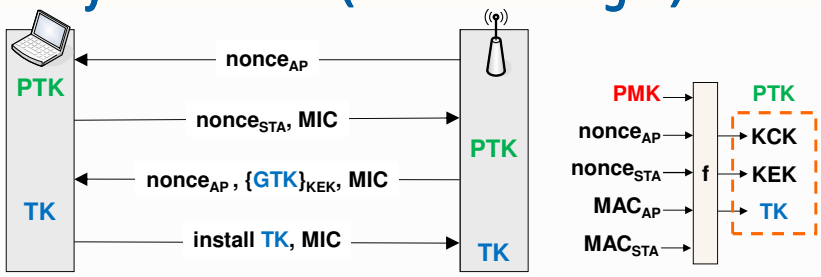
- STA only got access to the AP
  - 802.1X controlled port still closed

IEEE 802.1X Phase 2: Authentication (EAP messages)



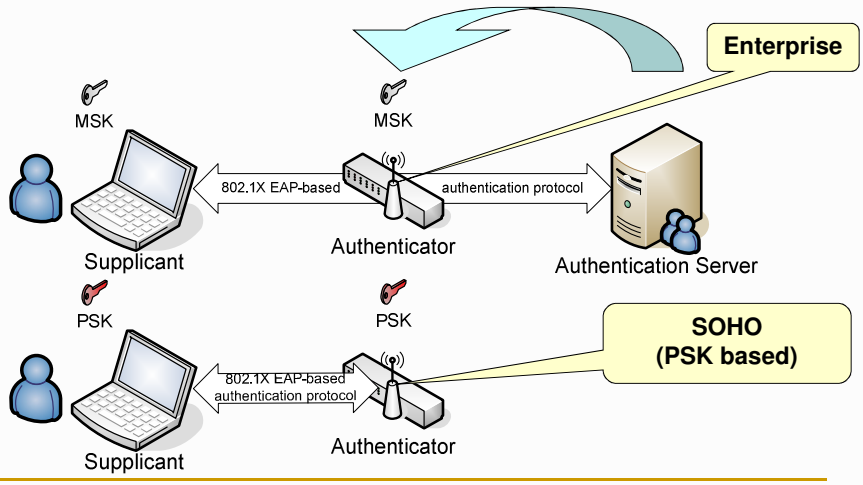
- At the end of this phase AP and STA share crypto data
  - MSK (Master Session Key) → PMK (Pairwise Master Key)
  - But 802.1X controlled port still closed

IEEE 802.1X Phase 3: 4-Way Handshake (EAPoL messages)

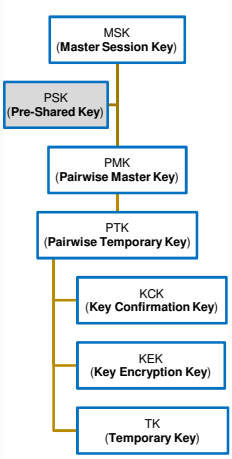


- At the end AP and STA share new, fresh crypto data
  - PTK (Pairwise Transient Key) → TK (Temporal Key)
  - GTK (Group Transient Key)
- Both are convinced that the peer knows PMK and PTK
  - Due to the use of MICs
- 802.1X controlled port is now open for unicast traffic
  - STA-AP unicast traffic will be protected with TK
  - STA-AP broadcast traffic with GTK

IEEE 802.1X: Architectural options



IEEE 802.1X: Complete key hierarchy



- MSK
  - Fresh outcome of an EAP protocol run
  - Enterprise architecture
- PSK
  - Long-term AP-STA pre-shared key
  - SOHO architecture
- PMK
  - Fresh key used for AP-STA mutual authentication and for key distribution in 4WH protocol runs
- PTK
  - Key used to protect AP-STA data exchanges
    - KCK / KEK: 4WH protocol
    - TK: 802.11 data frames

EAP (Extensible Authentication Protocol)

- Initially conceived for PPP
  - Adapted to 802.1X
- AP not involved
  - Relay EAP traffic
  - Support all EAP-based protocols
- Not conceived for wireless networks
  - EAP traffic not protected
  - Mutual authentication not mandatory
    - An STA can be fooled by a stronger, rogue AP

Some EAP protocols for 802.1X

	EAP-MD5	LEAP	EAP-TLS	EAP-TTLS	PEAP
AS authentication	N/A	digest(password)	Public key (certificate)		
Supplicant authentication	digest(password)	digest(password)	Public key (certificate)	PAP, CHAP, MS-CHAP, EAP	EAP, public key (certificate)
Key distribution	No	Yes			
Risks	Identity exposure Dictionary attacks Host-in-the-Middle attacks Connection stealing	Identity exposure Dictionary attacks Host-in-the-Middle attacks	Identity exposure		Possible identity exposure in phase 1

802.11w: Management Frame Protection

- Authentication of disassociation / deauthentication
  - No confidentiality, just integrity control
  - Uses TK
- Authentication of broadcast management frames
  - BIP (Broadcast Integrity Protocol)
  - Extra field: MMIE (Management MIC Information Element)
  - Uses IGTK (Integrity Group Temporal Key)
- Duas novas tramas
  - SA Query request / response