Network Access Control and Wireless

Lennart Franked

Avdelningen för informationssystem och -teknologi (IST)
Mittuniversitetet

December 4, 2014

Overview

1. Network Access Control (NAC) and IEEE 802.1X
   - Network Access Control
   - Extensible Authentication Protocol
   - IEEE 802.1x

2. Wireless Network Security
   - Wireless Security

3. 802.11 Wireless Overview
   - 802.11 - Wireless LAN
   - Wireless LAN Security

Literature

The lecture covers chapter 5.1 - 5.3 and chapter 7 “Wireless Network Security” in [1]. To check that you have fully understood these chapters, you should solve problems 7.1, and 7.2

Network Access Control

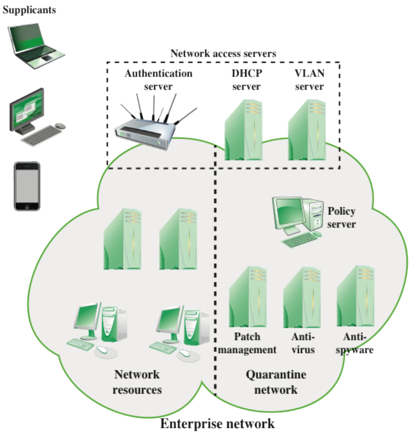


Figure 5.1 Network Access Control Context

Figure: [1]

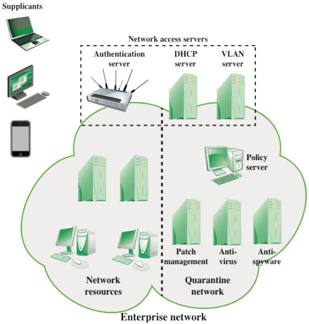


Figure 5.1 Network Access Control Context

Figure: [1].

Access Requestor

- Access Requestor, Client, Supplicants, peer
- Access the network.

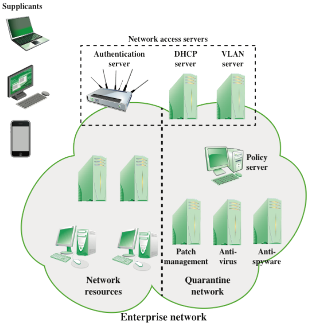


Figure 5.1 Network Access Control Context

Figure: [1].

Policy Server

- Enforce access restrictions.

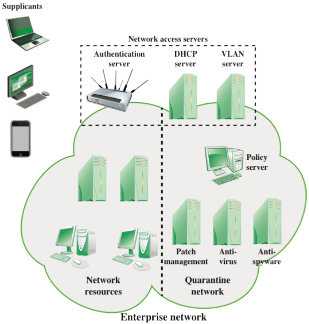


Figure 5.1 Network Access Control Context

Figure: [1].

Network Access Server

- Control access to Network.

- IEEE 802.1X - EAP over LAN.
- VLAN.
- Firewall.
- DHCP management.

- IEEE 802.1X - EAP over LAN.
- VLAN.
- Firewall.
- DHCP management.

- IEEE 802.1X - EAP over LAN.
- VLAN.
- Firewall.
- DHCP management.

Network Access Enforcement Methods

Network Access Control

- IEEE 802.1X - EAP over LAN.
- VLAN.
- Firewall.
- DHCP management.

Extensible Authentication Protocol

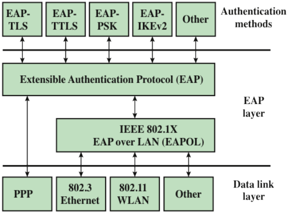


Figure 5.2 EAP Layered Context

Figure: [1].

- *Framework* for network access and authentication protocols.
- Mostly encountered in wireless networks and PPP-connections.
- Extension to PPP

Extensible Authentication Protocol

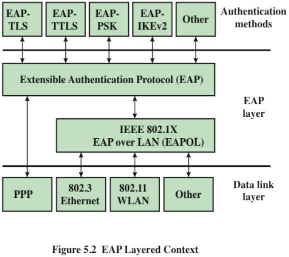


Figure: [1].

- *Framework* for network access and authentication protocols.
- Mostly encountered in wireless networks and PPP-connections.
- Extension to PPP

Extensible Authentication Protocol

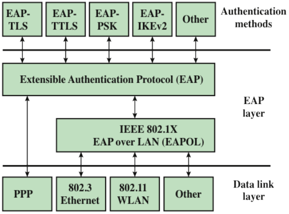


Figure 5.2 EAP Layered Context

Figure: [1].

- *Framework* for network access and authentication protocols.
- Mostly encountered in wireless networks and PPP-connections.
- Extension to PPP

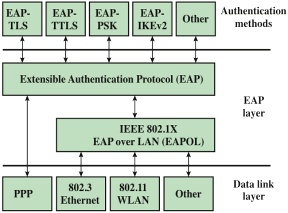


Figure 5.2 EAP Layered Context

Figure: [1].

EAP authentication methods.

- EAP-TLS.
- EAP-TTLS.
- EAP-GPSK.
- EAP-IKEv2.

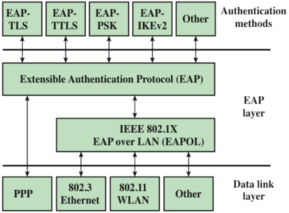


Figure 5.2 EAP Layered Context

Figure: [1].

EAP authentication methods.

- EAP-TLS.
- EAP-TTLS.
- EAP-GPSK.
- EAP-IKEv2.

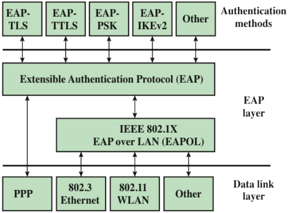


Figure 5.2 EAP Layered Context

Figure: [1].

EAP authentication methods.

- EAP-TLS.
- EAP-TTLS.
- EAP-GPSK.
- EAP-IKEv2.

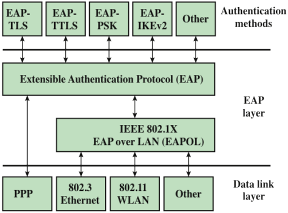


Figure 5.2 EAP Layered Context

Figure: [1].

EAP authentication methods.

- EAP-TLS.
- EAP-TTLS.
- EAP-GPSK.
- EAP-IKEv2.

EAP Exchanges

Extensible Authentication Protocol

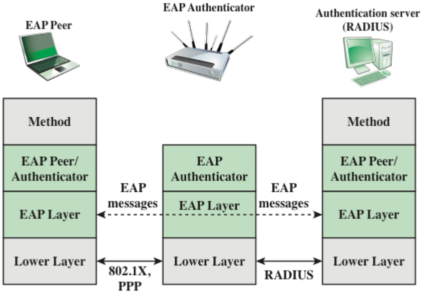


Figure: EAP Protocol Exchange [1]

EAP Messages
Extensible Authentication Protocol

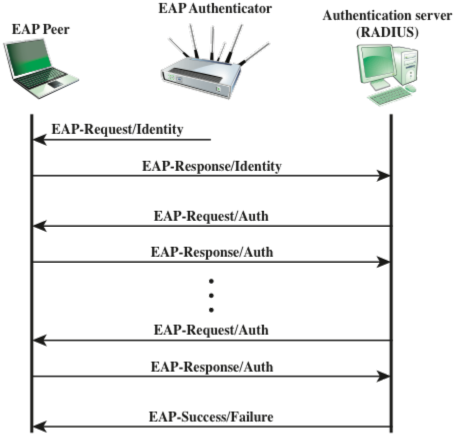


Figure: EAP Message Flow [1]

IEEE 802.1x

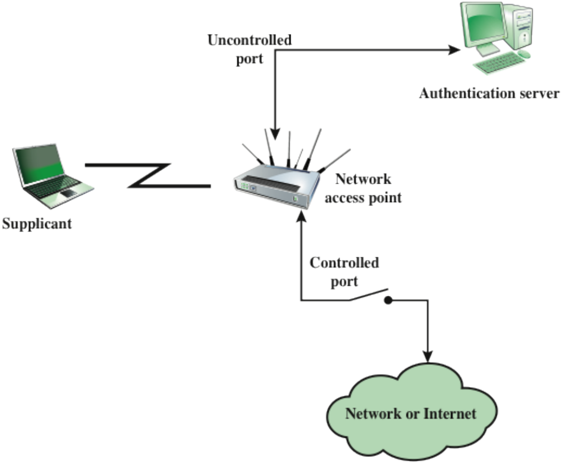


Figure: IEEE 802.1x operation [1]

IEEE 802.1x EAPOL Message types

- EAPOL-EAP – Encapsulated EAP packet.
- EAPOL-Start – Initiates the start of EAP authentication process.
- EAPOL-Logoff – Closes the EAP session.
- EAPOL-Key – Exchange key information.

IEEE 802.1x EAPOL Message types

- EAPOL-EAP – Encapsulated EAP packet.
- EAPOL-Start – Initiates the start of EAP authentication process.
- EAPOL-Logoff – Closes the EAP session.
- EAPOL-Key – Exchange key information.

- EAPOL-EAP – Encapsulated EAP packet.
- EAPOL-Start – Initiates the start of EAP authentication process.
- EAPOL-Logoff – Closes the EAP session.
- EAPOL-Key – Exchange key information.

IEEE 802.1x EAPOL Message types

- EAPOL-EAP – Encapsulated EAP packet.
- EAPOL-Start – Initiates the start of EAP authentication process.
- EAPOL-Logoff – Closes the EAP session.
- EAPOL-Key – Exchange key information.

Overview

1. Network Access Control (NAC) and IEEE 802.1X
   - Network Access Control
   - Extensible Authentication Protocol
   - IEEE 802.1x

2. Wireless Network Security
   - Wireless Security

3. 802.11 Wireless Overview
   - 802.11 - Wireless LAN
   - Wireless LAN Security

Wireless Network Security

Why wireless network are more susceptible to attacks.

- Broadcast communication allows eavesdropping.
- Jamming traffic
- Mobile devices
- Implemented on a variety of devices with limited memory and computational resources.
- Easy to access.

Why wireless network are more susceptible to attacks.

- Broadcast communication allows eavesdropping.
- Jamming traffic
- Mobile devices
- Implemented on a variety of devices with limited memory and computational resources.
- Easy to access.

Why wireless network are more susceptible to attacks.

- Broadcast communication allows eavesdropping.
- Jamming traffic
- Mobile devices
- Implemented on a variety of devices with limited memory and computational resources.
- Easy to access.

Why wireless network are more susceptible to attacks.

- Broadcast communication allows eavesdropping.
- Jamming traffic
- Mobile devices
- Implemented on a variety of devices with limited memory and computational resources.
- Easy to access.

Why wireless network are more susceptible to attacks.

- Broadcast communication allows eavesdropping.
- Jamming traffic
- Mobile devices
- Implemented on a variety of devices with limited memory and computational resources.
- Easy to access.

Threats

- Accidental Association
- Malicious Association
- Ad hoc Networks
- Nontraditional Networks
- MAC Spoofing
- Man-in-the-middle attacks
- DoS
- Network Injection

Threats

- Accidental Association
- Malicious Association
- Ad hoc Networks
- Nontraditional Networks
- MAC Spoofing
- Man-in-the-middle attacks
- DoS
- Network Injection

Threats

- Accidental Association
- Malicious Association
- Ad hoc Networks
- Nontraditional Networks
- MAC Spoofing
- Man-in-the-middle attacks
- DoS
- Network Injection

Threats

- Accidental Association
- Malicious Association
- Ad hoc Networks
- Nontraditional Networks
- MAC Spoofing
- Man-in-the-middle attacks
- DoS
- Network Injection

Threats

- Accidental Association
- Malicious Association
- Ad hoc Networks
- Nontraditional Networks
- MAC Spoofing
- Man-in-the-middle attacks
- DoS
- Network Injection

Threats

- Accidental Association
- Malicious Association
- Ad hoc Networks
- Nontraditional Networks
- MAC Spoofing
- Man-in-the-middle attacks
- DoS
- Network Injection

Threats

- Accidental Association
- Malicious Association
- Ad hoc Networks
- Nontraditional Networks
- MAC Spoofing
- Man-in-the-middle attacks
- DoS
- Network Injection

Threats

- Accidental Association
- Malicious Association
- Ad hoc Networks
- Nontraditional Networks
- MAC Spoofing
- Man-in-the-middle attacks
- DoS
- Network Injection

- Signal-hiding techniques
  - Hide SSID (Security by obscurity)
  - Reducing Signal Strength
- Encryption (Confidentiality)
- Authentication
- MAC (Integrity)
- IEEE 802.1x

- Signal-hiding techniques
  - Hide SSID (Security by obscurity)
  - Reducing Signal Strength
- Encryption (Confidentiality)
- Authentication
- MAC (Integrity)
- IEEE 802.1x

- Signal-hiding techniques
  - Hide SSID (Security by obscurity)
  - Reducing Signal Strength
- Encryption (Confidentiality)
- Authentication
- MAC (Integrity)
- IEEE 802.1x

- Signal-hiding techniques
  - Hide SSID (Security by obscurity)
  - Reducing Signal Strength
- Encryption (Confidentiality)
- Authentication
- MAC (Integrity)
- IEEE 802.1x

- Signal-hiding techniques
  - Hide SSID (Security by obscurity)
  - Reducing Signal Strength
- Encryption (Confidentiality)
- Authentication
- MAC (Integrity)
- IEEE 802.1x

- Signal-hiding techniques
  - Hide SSID (Security by obscurity)
  - Reducing Signal Strength
- Encryption (Confidentiality)
- Authentication
- MAC (Integrity)
- IEEE 802.1x

- Signal-hiding techniques
  - Hide SSID (Security by obscurity)
  - Reducing Signal Strength
- Encryption (Confidentiality)
- Authentication
- MAC (Integrity)
- IEEE 802.1x

- Lack of physical Control
- Use of untrusted mobile devices
- Use of untrusted network
- Use of applications created by unknown parties
- Interaction with other systems
- Use of untrusted content
- Use of location services

- Lack of physical Control
- Use of untrusted mobile devices
- Use of untrusted network
- Use of applications created by unknown parties
- Interaction with other systems
- Use of untrusted content
- Use of location services

- Lack of physical Control
- Use of untrusted mobile devices
- Use of untrusted network
- Use of applications created by unknown parties
- Interaction with other systems
- Use of untrusted content
- Use of location services

- Lack of physical Control
- Use of untrusted mobile devices
- Use of untrusted network
- Use of applications created by unknown parties
- Interaction with other systems
- Use of untrusted content
- Use of location services

- Lack of physical Control
- Use of untrusted mobile devices
- Use of untrusted network
- Use of applications created by unknown parties
- Interaction with other systems
- Use of untrusted content
- Use of location services

- Lack of physical Control
- Use of untrusted mobile devices
- Use of untrusted network
- Use of applications created by unknown parties
- Interaction with other systems
- Use of untrusted content
- Use of location services

- Lack of physical Control
- Use of untrusted mobile devices
- Use of untrusted network
- Use of applications created by unknown parties
- Interaction with other systems
- Use of untrusted content
- Use of location services

Overview

1. Network Access Control (NAC) and IEEE 802.1X
   - Network Access Control
   - Extensible Authentication Protocol
   - IEEE 802.1x

2. Wireless Network Security
   - Wireless Security

3. 802.11 Wireless Overview
   - 802.11 - Wireless LAN
   - Wireless LAN Security

802.11 - Wireless LAN

- IEEE 802 work group.
  - Develops standards for LAN.
  - 802.11 was formed 1990
- Wi-Fi Alliance
  - Wireless Ethernet Compatibility Alliance (WECA)
  - Certifies compatibility between Wi-Fi vendors.
  - 802.11a,b,g,n,ac,ad
  - Creates security standards as well.

802.11 - Wireless LAN

- IEEE 802 work group.
  - Develops standards for LAN.
  - 802.11 was formed 1990
- Wi-Fi Alliance
  - Wireless Ethernet Compatibility Alliance (WECA)
  - Certifies compatibility between Wi-Fi vendors.
  - 802.11a,b,g,n,ac,ad
  - Creates security standards as well.

- IEEE 802 work group.
  - Develops standards for LAN.
  - 802.11 was formed 1990
- Wi-Fi Alliance
  - Wireless Ethernet Compatibility Alliance (WECA)
  - Certifies compatibility between Wi-Fi vendors.
  - 802.11a,b,g,n,ac,ad
  - Creates security standards as well.

802.11 - Wireless LAN

- IEEE 802 work group.
  - Develops standards for LAN.
  - 802.11 was formed 1990
- Wi-Fi Alliance
  - Wireless Ethernet Compatibility Alliance (WECA)
  - Certifies compatibility between Wi-Fi vendors.
  - 802.11a,b,g,n,ac,ad
  - Creates security standards as well.

- IEEE 802 work group.
  - Develops standards for LAN.
  - 802.11 was formed 1990
- Wi-Fi Alliance
  - Wireless Ethernet Compatibility Alliance (WECA)
  - Certifies compatibility between Wi-Fi vendors.
  - 802.11a,b,g,n,ac,ad
  - Creates security standards as well.

- IEEE 802 work group.
  - Develops standards for LAN.
  - 802.11 was formed 1990
- Wi-Fi Alliance
  - Wireless Ethernet Compatibility Alliance (WECA)
  - Certifies compatibility between Wi-Fi vendors.
  - 802.11a,b,g,n,ac,ad
  - Creates security standards as well.

- IEEE 802 work group.
    - Develops standards for LAN.
    - 802.11 was formed 1990
- Wi-Fi Alliance
    - Wireless Ethernet Compatibility Alliance (WECA)
    - Certifies compatibility between Wi-Fi vendors.
    - 802.11a,b,g,n,ac,ad
    - Creates security standards as well.

- IEEE 802 work group.
  - Develops standards for LAN.
  - 802.11 was formed 1990
- Wi-Fi Alliance
  - Wireless Ethernet Compatibility Alliance (WECA)
  - Certifies compatibility between Wi-Fi vendors.
  - 802.11a,b,g,n,ac,ad
  - Creates security standards as well.

- Access point
- Basic Service Set
- Extended Service Set
- Distribution System
- Protocol Data Unit
- Service Data Unit

- Access point
- Basic Service Set
- Extended Service Set
- Distribution System
- Protocol Data Unit
- Service Data Unit

- Access point
- Basic Service Set
- Extended Service Set
- Distribution System
- Protocol Data Unit
- Service Data Unit

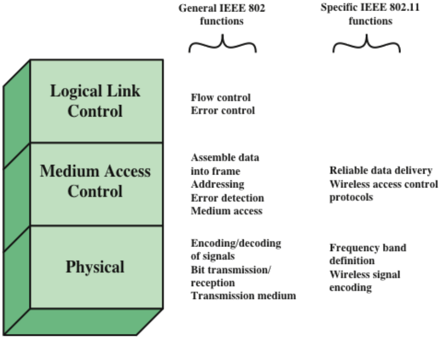
- Access point
- Basic Service Set
- Extended Service Set
- Distribution System
- Protocol Data Unit
- Service Data Unit

- Access point
- Basic Service Set
- Extended Service Set
- Distribution System
- Protocol Data Unit
- Service Data Unit

- Access point
- Basic Service Set
- Extended Service Set
- Distribution System
- Protocol Data Unit
- Service Data Unit

IEEE 802.11 protocol stack

802.11 - Wireless LAN



General IEEE 802 functions

Specific IEEE 802.11 functions

Logical Link Control

Flow control
Error control

Medium Access Control

Assemble data into frame
Addressing
Error detection
Medium access

Reliable data delivery
Wireless access control protocols

Physical

Encoding/decoding of signals
Bit transmission/ reception
Transmission medium

Frequency band definition
Wireless signal encoding

Figure: 802.11 protocol stack [1]

IEEE 802.11 Architectural Model

802.11 - Wireless LAN

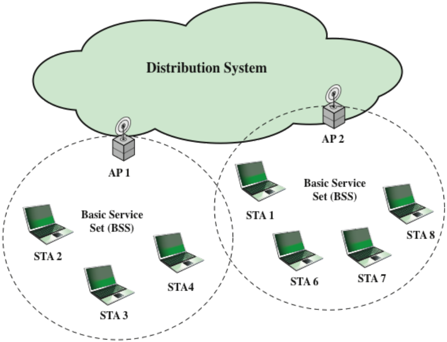


Figure: 802.11 Architectural Model [1]

Table: IEEE 802.11 Services [1]

Service	Provider	Used to support
Association	Distribution system	MSDU delivery
Reassociation	Distribution system	MSDU delivery
Authentication	Station	LAN access and Security
Deauthentication	Station	LAN access and Security
Privacy	Station	LAN access and Security
Disassociation	Distribution system	MSDU delivery
Distribution	Distribution system	MSDU delivery
Integration	Distribution system	MSDU delivery
MSDU delivery	Station	MSDU delivery

Table: IEEE 802.11 Services [1]

Service	Provider	Used to support
Association	Distribution system	MSDU delivery
Reassociation	Distribution system	MSDU delivery
Authentication	Station	LAN access and Security
Deauthentication	Station	LAN access and Security
Privacy	Station	LAN access and Security
Disassociation	Distribution system	MSDU delivery
Distribution	Distribution system	MSDU delivery
Integration	Distribution system	MSDU delivery
MSDU delivery	Station	MSDU delivery

Table: IEEE 802.11 Services [1]

Service	Provider	Used to support
Association	Distribution system	MSDU delivery
Reassociation	Distribution system	MSDU delivery
Authentication	Station	LAN access and Security
Deauthentication	Station	LAN access and Security
Privacy	Station	LAN access and Security
Disassociation	Distribution system	MSDU delivery
Distribution	Distribution system	MSDU delivery
Integration	Distribution system	MSDU delivery
MSDU delivery	Station	MSDU delivery

Table: IEEE 802.11 Services [1]

Service	Provider	Used to support
Association	Distribution system	MSDU delivery
Reassociation	Distribution system	MSDU delivery
Authentication	Station	LAN access and Security
Deauthentication	Station	LAN access and Security
Privacy	Station	LAN access and Security
Disassociation	Distribution system	MSDU delivery
Distribution	Distribution system	MSDU delivery
Integration	Distribution system	MSDU delivery
MSDU delivery	Station	MSDU delivery

Table: IEEE 802.11 Services [1]

Service	Provider	Used to support
Association	Distribution system	MSDU delivery
Reassociation	Distribution system	MSDU delivery
Authentication	Station	LAN access and Security
Deauthentication	Station	LAN access and Security
Privacy	Station	LAN access and Security
Disassociation	Distribution system	MSDU delivery
Distribution	Distribution system	MSDU delivery
Integration	Distribution system	MSDU delivery
MSDU delivery	Station	MSDU delivery

Table: IEEE 802.11 Services [1]

Service	Provider	Used to support
Association	Distribution system	MSDU delivery
Reassociation	Distribution system	MSDU delivery
Authentication	Station	LAN access and Security
Deauthentication	Station	LAN access and Security
Privacy	Station	LAN access and Security
Disassociation	Distribution system	MSDU delivery
Distribution	Distribution system	MSDU delivery
Integration	Distribution system	MSDU delivery
MSDU delivery	Station	MSDU delivery

Table: IEEE 802.11 Services [1]

Service	Provider	Used to support
Association	Distribution system	MSDU delivery
Reassociation	Distribution system	MSDU delivery
Authentication	Station	LAN access and Security
Deauthentication	Station	LAN access and Security
Privacy	Station	LAN access and Security
Disassociation	Distribution system	MSDU delivery
Distribution	Distribution system	MSDU delivery
Integration	Distribution system	MSDU delivery
MSDU delivery	Station	MSDU delivery

Table: IEEE 802.11 Services [1]

Service	Provider	Used to support
Association	Distribution system	MSDU delivery
Reassociation	Distribution system	MSDU delivery
Authentication	Station	LAN access and Security
Deauthentication	Station	LAN access and Security
Privacy	Station	LAN access and Security
Disassociation	Distribution system	MSDU delivery
Distribution	Distribution system	MSDU delivery
Integration	Distribution system	MSDU delivery
MSDU delivery	Station	MSDU delivery

Table: IEEE 802.11 Services [1]

Service	Provider	Used to support
Association	Distribution system	MSDU delivery
Reassociation	Distribution system	MSDU delivery
Authentication	Station	LAN access and Security
Deauthentication	Station	LAN access and Security
Privacy	Station	LAN access and Security
Disassociation	Distribution system	MSDU delivery
Distribution	Distribution system	MSDU delivery
Integration	Distribution system	MSDU delivery
MSDU delivery	Station	MSDU delivery

Table: IEEE 802.11 Services [1]

Service	Provider	Used to support
Association	Distribution system	MSDU delivery
Reassociation	Distribution system	MSDU delivery
Authentication	Station	LAN access and Security
Deauthentication	Station	LAN access and Security
Privacy	Station	LAN access and Security
Disassociation	Distribution system	MSDU delivery
Distribution	Distribution system	MSDU delivery
Integration	Distribution system	MSDU delivery
MSDU delivery	Station	MSDU delivery

Wireless LAN

Any station within then range of a wireless AP can transmit and receive data on the LAN.

Wired LAN

Only devices with a physical connection to the network can send and receive data on the LAN.

Wireless LAN

Any station within then range of a wireless AP can transmit and receive data on the LAN.

Wired LAN

Only devices with a physical connection to the network can send and receive data on the LAN.

- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)

- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)

- Use RC4 stream cipher.
- 128 bit random number used as a challange.
- 64 bit (40 bit user generated) or 128 bit (104 bit user generated) key sizes.
- 24 bit initialization vector

- Use RC4 stream cipher.
- 128 bit random number used as a challange.
- 64 bit (40 bit user generated) or 128 bit (104 bit user generated) key sizes.
- 24 bit initialization vector

- Use RC4 stream cipher.
- 128 bit random number used as a challange.
- 64 bit (40 bit user generated) or 128 bit (104 bit user generated) key sizes.
- 24 bit initialization vector

- Use RC4 stream cipher.
- 128 bit random number used as a challange.
- 64 bit (40 bit user generated) or 128 bit (104 bit user generated) key sizes.
- 24 bit initialization vector

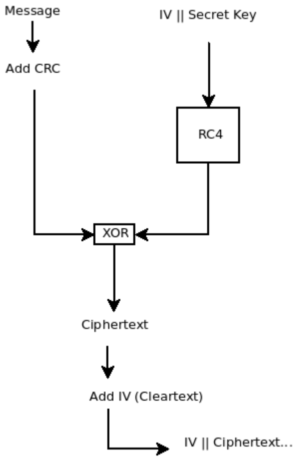


Figure: WEP encryption process

Wi-Fi Protected Access (WPA)

- Replace WEP
- 802.11i - Robust Security Network
- RSN services
    - Authentication
    - Access Control
    - Privacy with message integrity

- Replace WEP
- 802.11i - Robust Security Network
- RSN services
  - Authentication
  - Access Control
  - Privacy with message integrity

- Replace WEP
- 802.11i - Robust Security Network
- RSN services
  - Authentication
  - Access Control
  - Privacy with message integrity

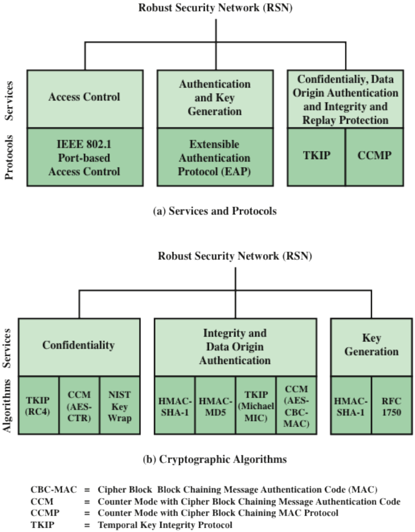
- Replace WEP
- 802.11i - Robust Security Network
- RSN services
  - Authentication
  - Access Control
  - Privacy with message integrity

- Replace WEP
- 802.11i - Robust Security Network
- RSN services
  - Authentication
  - Access Control
  - Privacy with message integrity

- Replace WEP
- 802.11i - Robust Security Network
- RSN services
  - Authentication
  - Access Control
  - Privacy with message integrity

WPA

Wireless LAN Security



Robust Security Network (RSN)

Services: Access Control; Authentication and Key Generation; Confidentialiy, Data Origin Authentication and Integrity and Replay Protection

Protocols: IEEE 802.1 Port-based Access Control; Extensible Authentication Protocol (EAP); TKIP; CCMP

(a) Services and Protocols

Robust Security Network (RSN)

Services: Confidentiality; Integrity and Data Origin Authentication; Key Generation

Algorithms: TKIP (RC4); CCM (AES-CTR); NIST Key Wrap; HMAC-SHA-1; HMAC-MD5; TKIP (Michael MIC); CCM (AES-CBC-MAC); HMAC-SHA-1; RFC 1750

(b) Cryptographic Algorithms

CBC-MAC = Cipher Block Block Chaining Message Authentication Code (MAC)
CCM = Counter Mode with Cipher Block Chaining Message Authentication Code
CCMP = Counter Mode with Cipher Block Chaining MAC Protocol
TKIP = Temporal Key Integrity Protocol

Figure: Elements of 802.11i [1]

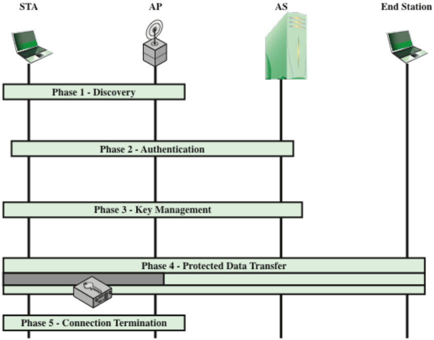


Figure: 802.11i Phases of operation [1]

802.11i - Discovery/Authentication phase
Wireless LAN Security

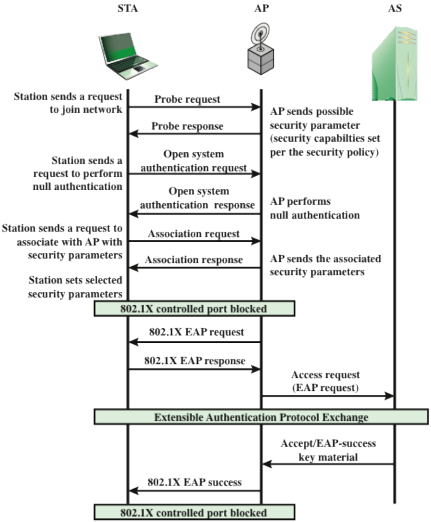
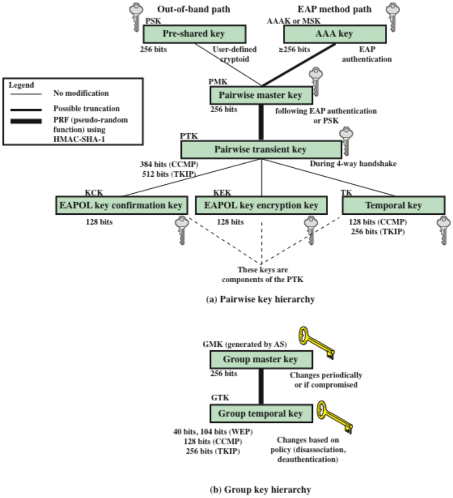

STA
AP
AS
Station sends a request to join network
Probe request
Probe response
AP sends possible security parameter (security capabilties set per the security policy)
Station sends a request to perform null authentication
Open system authentication request
Open system authentication response
AP performs null authentication
Station sends a request to associate with AP with security parameters
Association request
Association response
AP sends the associated security parameters
Station sets selected security parameters
802.1X controlled port blocked
802.1X EAP request
802.1X EAP response
Access request (EAP request)
Extensible Authentication Protocol Exchange
Accept/EAP-success key material
802.1X EAP success
802.1X controlled port blocked

Figure: Discovery, authentication and association [1]

802.11i - Key Hierarchies

Wireless LAN Security



(a) Pairwise key hierarchy

(b) Group key hierarchy

Figure: Key Hierarchies [1]

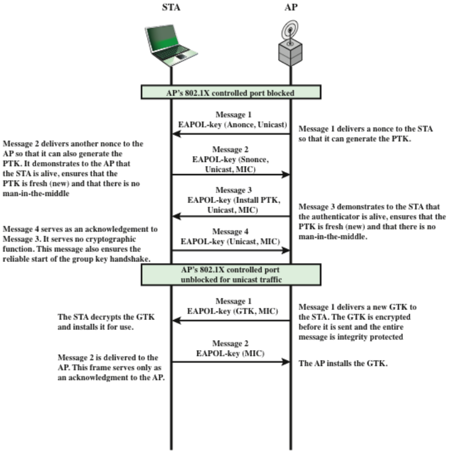
Keys used in Wi-Fi Protected Access

- Pairwise Keys
  - Used for communication between a pair of devices.
- Pre-Shared Key
  - A secret key installed outside the scope of 802.11i
- Master Session Key
  - Master key generated using IEEE 802.1x EAPOL
- Pairwise Master Key
  - Derived from MSK or PSK
- Pairwise Transient Key
  - Consists of three keys:
  - Key Confirmation Key (KCK)
  - Key Encryption Key (KEK)
  - Temporal Key (TK)

- Used for multicast communication
- Two keys are used
  - Group Master Key - Used to generate Group Temporal Key
  - Group Temporal Key - Used to encrypt the MPDUs
  - Changed every time a devices leaves the group.

IEEE 802.11i Four-way Handshake

Wireless LAN Security


STA
AP
AP's 802.1X controlled port blocked
Message 1
EAPOL-key (Anonce, Unicast)
Message 2
EAPOL-key (Snonce, Unicast, MIC)
Message 3
EAPOL-key (Install PTK, Unicast, MIC)
Message 4
EAPOL-key (Unicast, MIC)
AP's 802.1X controlled port unblocked for unicast traffic
Message 1
EAPOL-key (GTK, MIC)
Message 2
EAPOL-key (MIC)

Message 1 delivers a nonce to the STA so that it can generate the PTK.

Message 2 delivers another nonce to the AP so that it can also generate the PTK. It demonstrates to the AP that the STA is alive, ensures that the PTK is fresh (new) and that there is no man-in-the-middle

Message 3 demonstrates to the STA that the authenticator is alive, ensures that the PTK is fresh (new) and that there is no man-in-the-middle.

Message 4 serves as an acknowledgement to Message 3. It serves no cryptographic function. This message also ensures the reliable start of the group key handshake.

Message 1 delivers a new GTK to the STA. The GTK is encrypted before it is sent and the entire message is integrity protected

The STA decrypts the GTK and installs it for use.

Message 2 is delivered to the AP. This frame serves only as an acknowledgment to the AP.

The AP installs the GTK.

Figure: Four-way handshake and Group Key Handshake [1]

- TKIP (Temporal Key Integrity Protocol)
  - Software backward compatible with WEP devices
  - Message integrity using a MAC (Michael)
  - Encrypts data using RC4.
- CCMP (Counter Mode-CBC MAC Protocol)
  - Use CBC-MAC for message integrity
  - Encrypts data using AES-CTR.

IEEE 802.11i PRF

- Used for amongst other things generating nonces.
- Built on the HMAC-SHA1 hash algorithm.

IEEE 802.11i PRF

Wireless LAN Security

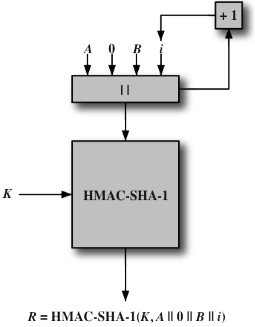


Figure 7.11 IEEE 802.11i Pseudorandom Function

Figure: IEEE 802.11i PRF [1]

Referenser

[1] William Stallings. *Network security essentials : applications and standards*. 5th ed. International Edition. Pearson Education, 2013. ISBN: 978-0-273-79336-6.