# Network Access Control and Wireless

Lennart Franked

Avdelningen för informations- och kommunikationssytem (IKS),
Mittuniversitetet, Sundsvall.

October 30, 2014

Mittuniversitetet
MID SWEDEN UNIVERSITY

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

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

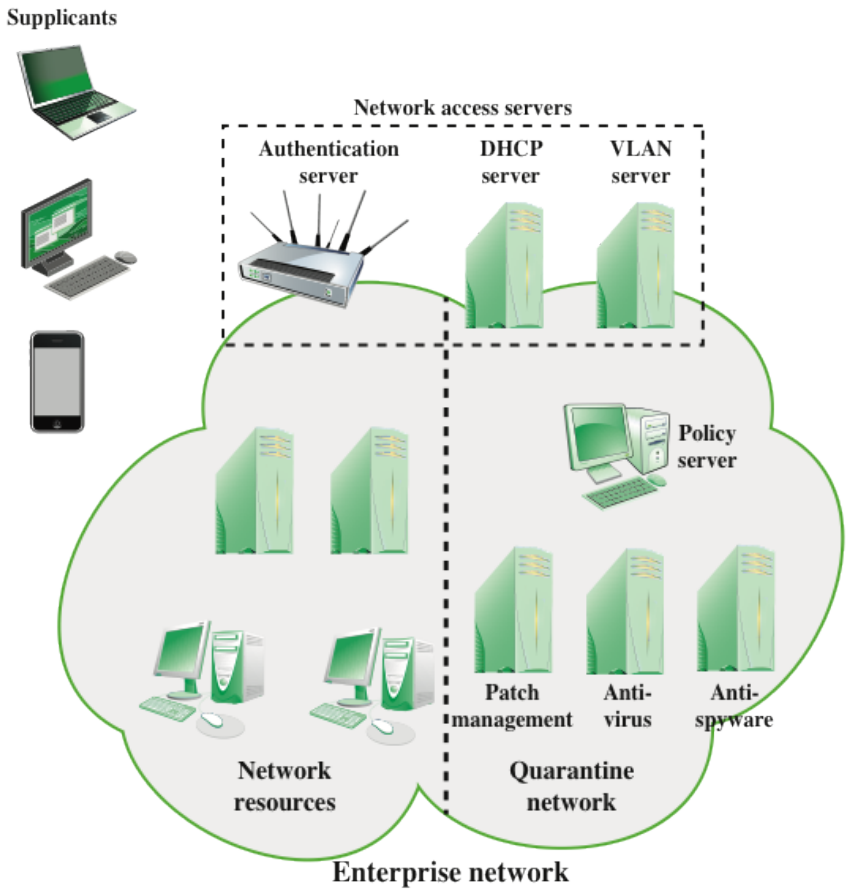


Figure 5.1 Network Access Control Context

Figure : [1]

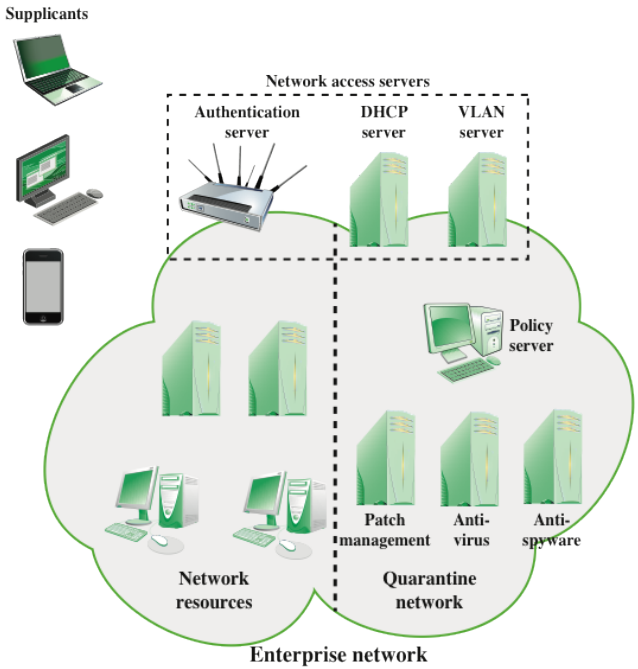


Figure 5.1 Network Access Control Context

## Access Requestor

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

Figure : [1].

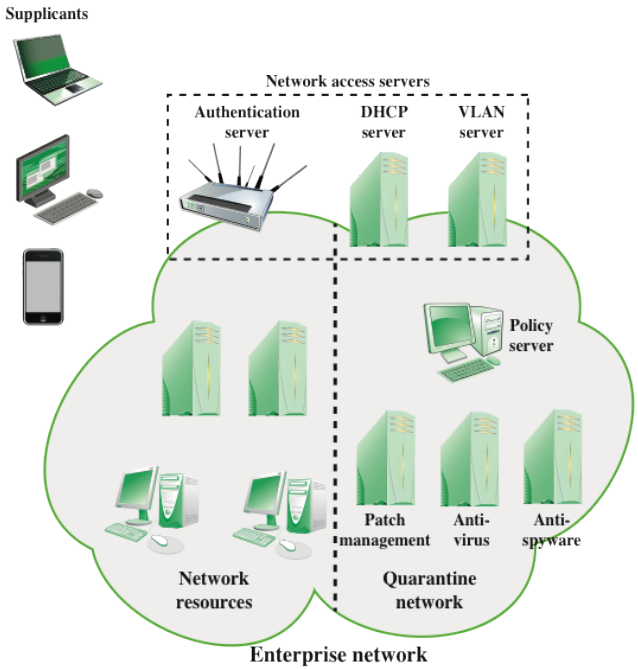


Figure 5.1 Network Access Control Context

## Policy Server

- Enforce access restrictions.

Figure : [1].

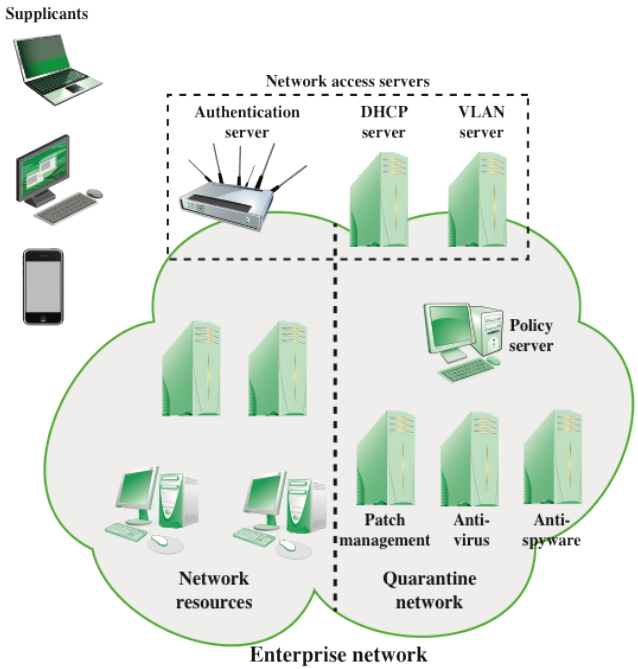


Figure 5.1 Network Access Control Context

## Network Access Server

- Control access to Network.

Figure : [1].

- 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.

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

# Extensible Authentication Protocol

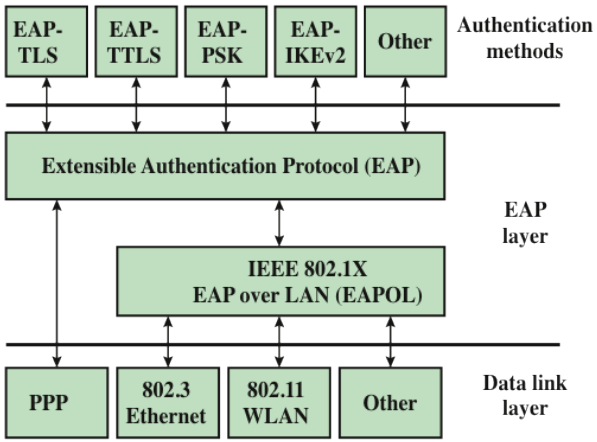


Figure 5.2 EAP Layered Context

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

Figure : [1].

Mittuniversitetet
MID SWEDEN UNIVERSITY

# Extensible Authentication Protocol

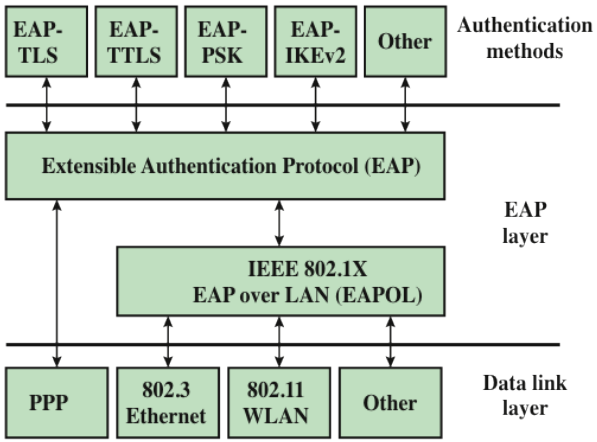


Figure 5.2 EAP Layered Context

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

Figure : [1].

Mittuniversitetet
MID SWEDEN UNIVERSITY

# Extensible Authentication Protocol

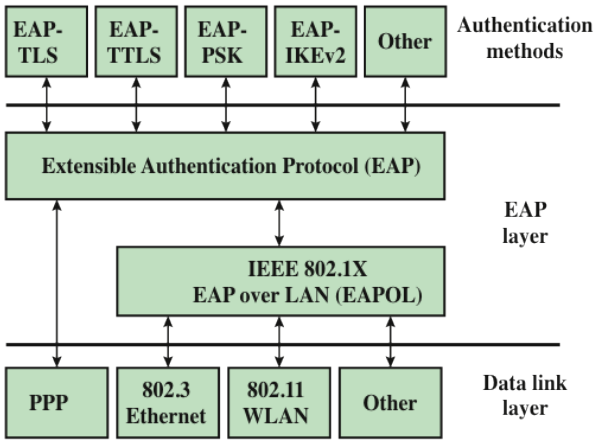


Figure 5.2 EAP Layered Context

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

Figure : [1].

Mittuniversitetet
MID SWEDEN UNIVERSITY

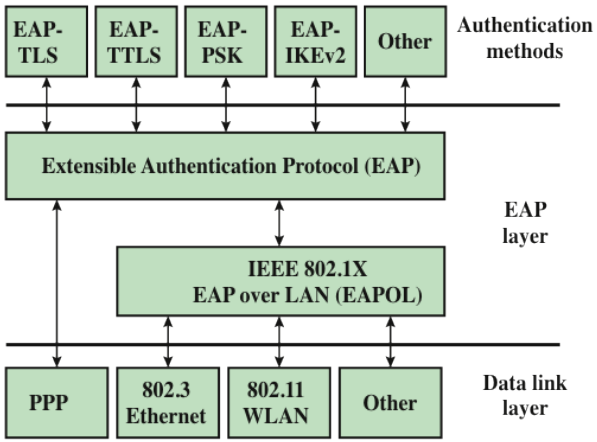


Figure 5.2 EAP Layered Context

## EAP authentication methods.

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

Figure : [1].

Mittuniversitetet
MID SWEDEN UNIVERSITY

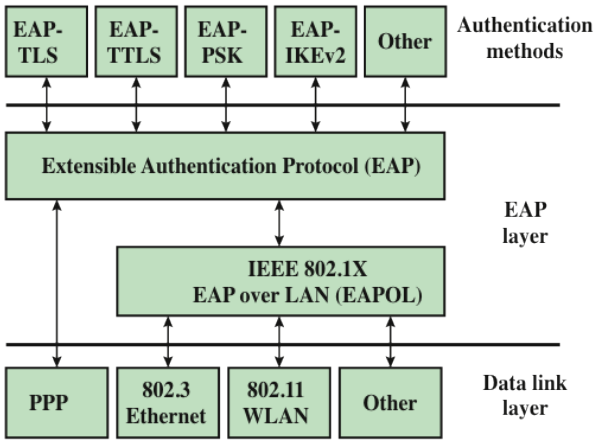


Figure 5.2 EAP Layered Context

## EAP authentication methods.

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

Figure : [1].

Mittuniversitetet
MID SWEDEN UNIVERSITY

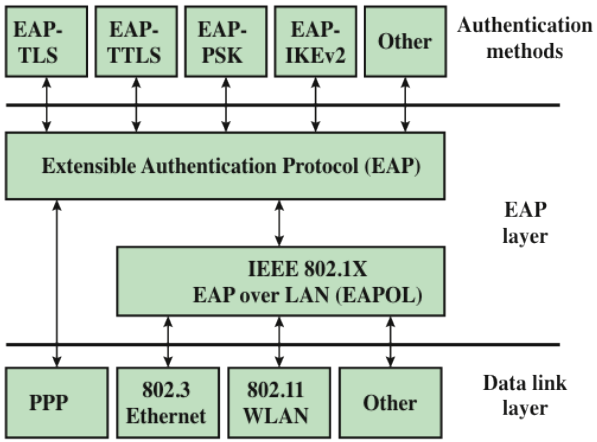


Figure 5.2 EAP Layered Context

## EAP authentication methods.

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

Figure : [1].

Mittuniversitetet
MID SWEDEN UNIVERSITY

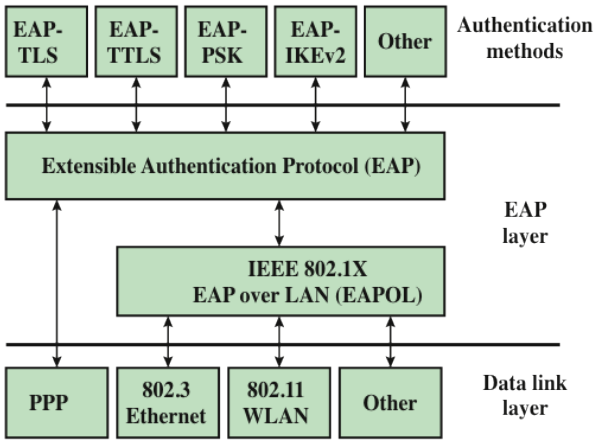


Figure 5.2 EAP Layered Context

## EAP authentication methods.

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

Figure : [1].

Mittuniversitetet
MID SWEDEN UNIVERSITY

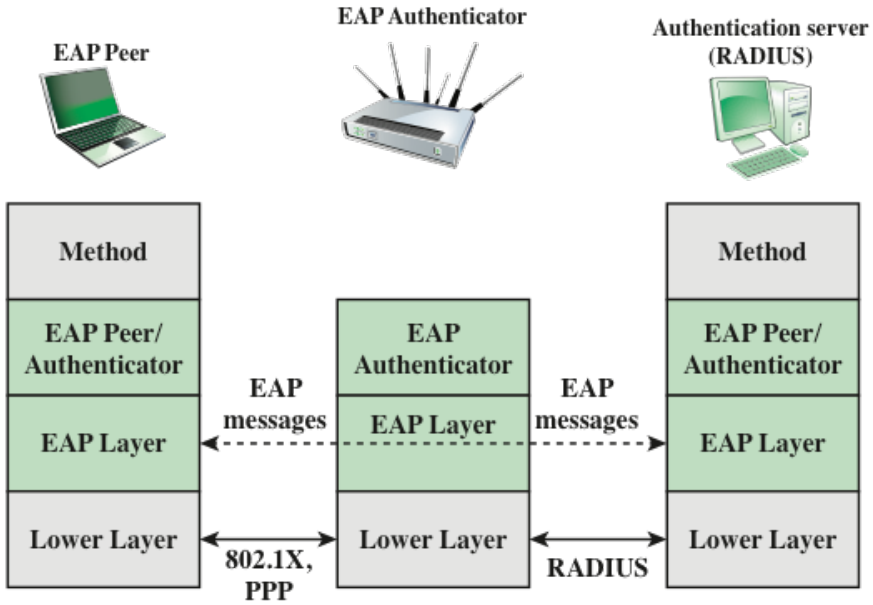


Figure : EAP Protocol Exchange [1]

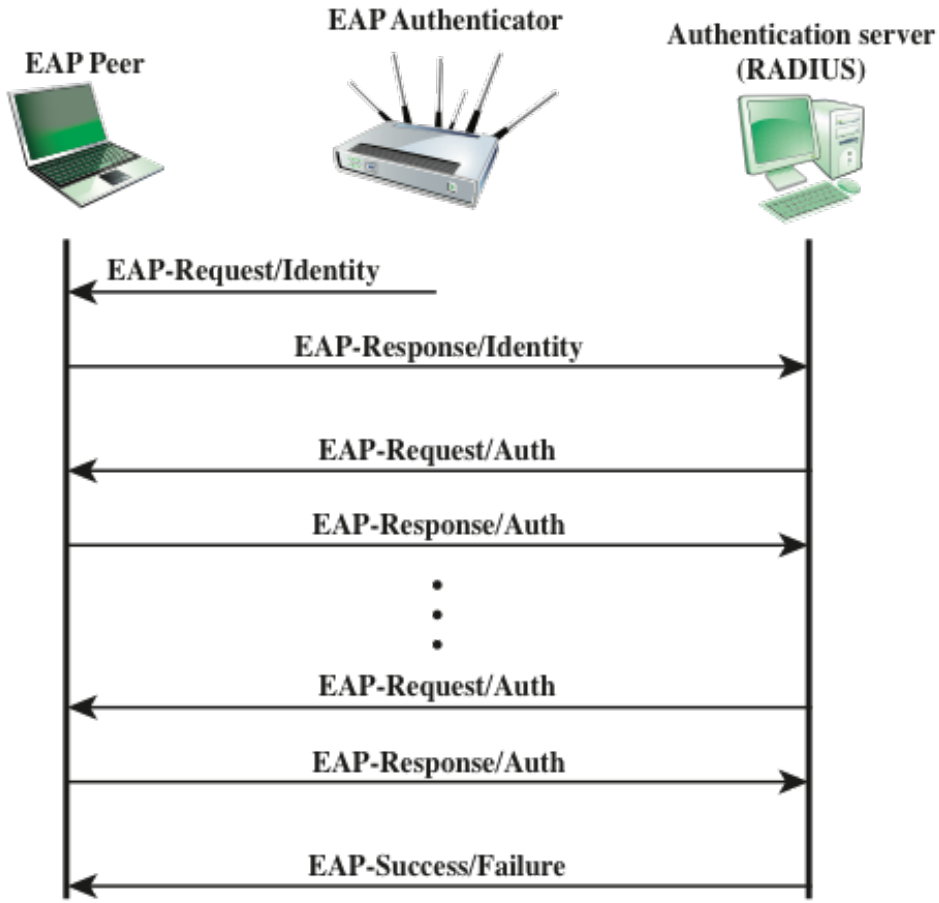


Figure : EAP Message Flow [1]

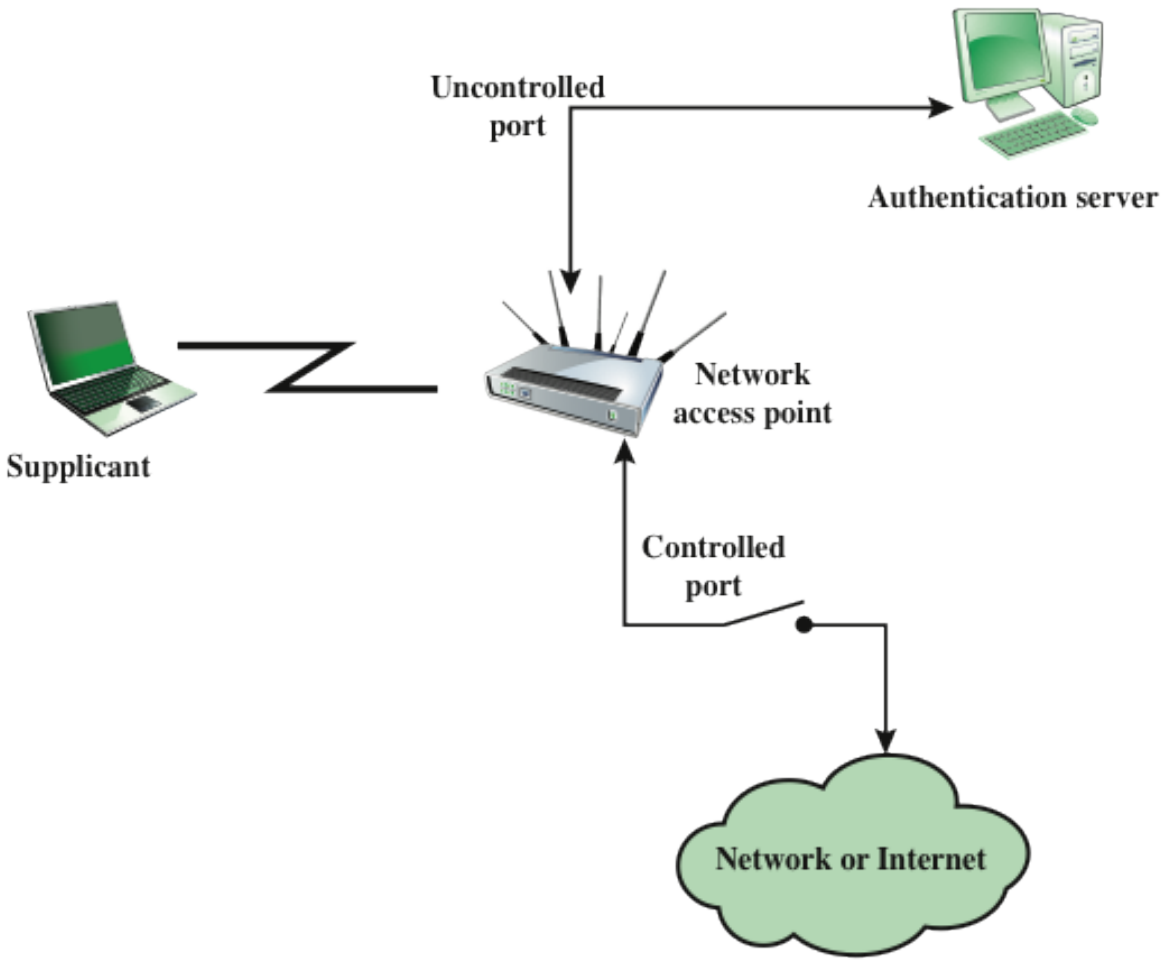


Figure : IEEE 802.1x operation [1]

- 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.

- 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.

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

Mittuniversitetet
MID SWEDEN UNIVERSITY

# 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

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

Mittuniversitetet
MID SWEDEN UNIVERSITY

- 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
  - Creates security standards as well.

Mittuniversitetet
MID SWEDEN UNIVERSITY

- 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
  - Creates security standards as well.

Mittuniversitetet
MID SWEDEN UNIVERSITY

- 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
  - Creates security standards as well.

Mittuniversitetet
MID SWEDEN UNIVERSITY

- 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
  - 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
  - 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
  - Creates security standards as well.

Mittuniversitetet
MID SWEDEN UNIVERSITY

- 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
  - 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
  - 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

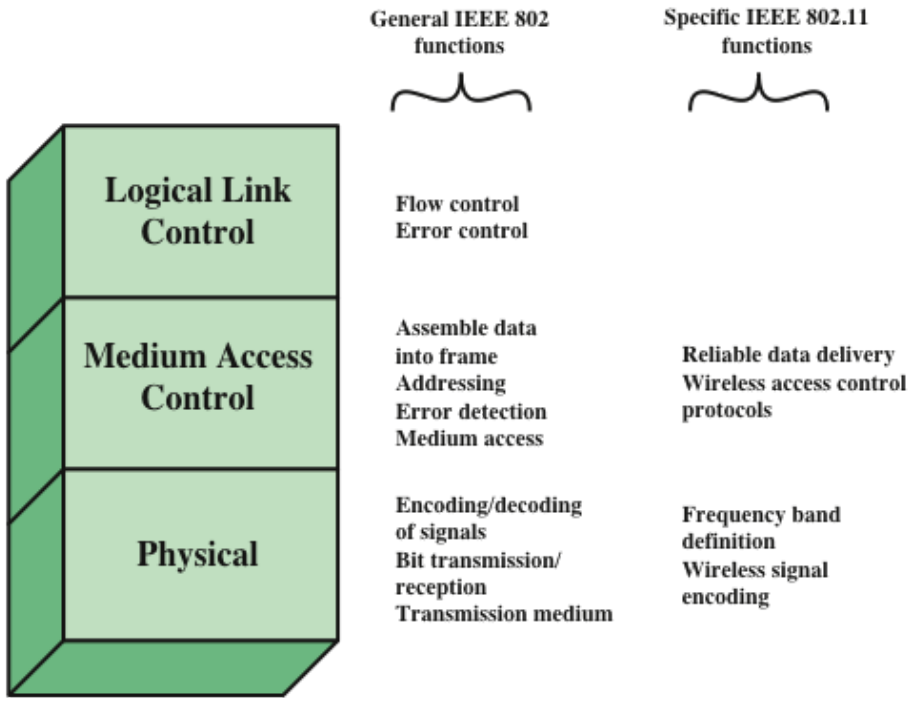


Figure : 802.11 protocol stack [1]

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 |

Mittuniversitetet
MID SWEDEN UNIVERSITY

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 |

Mittuniversitetet
MID SWEDEN UNIVERSITY

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 |

Mittuniversitetet
MID SWEDEN UNIVERSITY

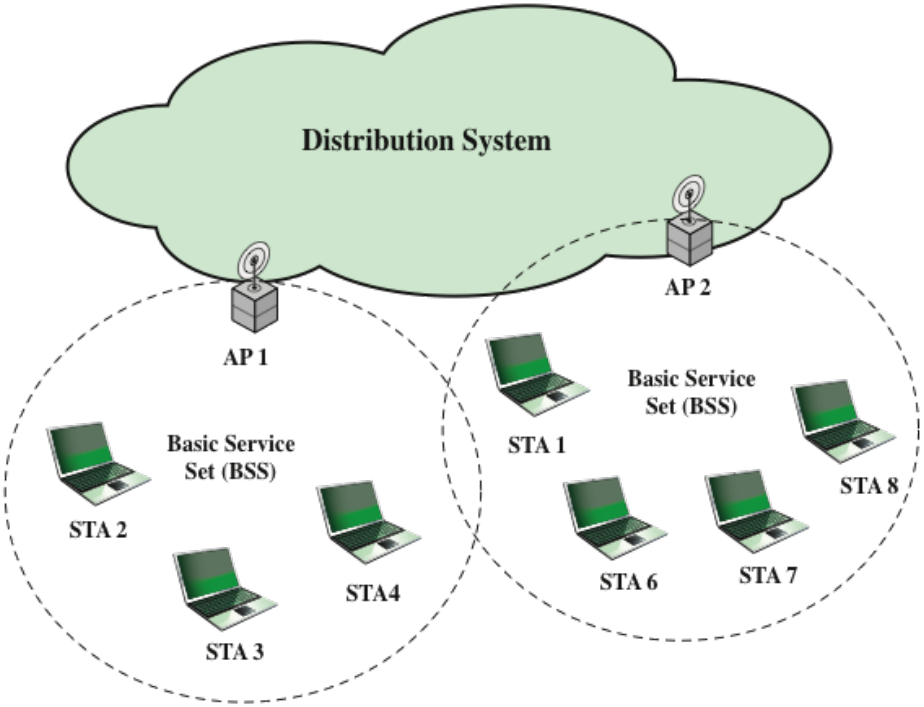


Figure : 802.11 Architectural Model [1]

## 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

# WEP Authentication Process

## Wireless LAN Security

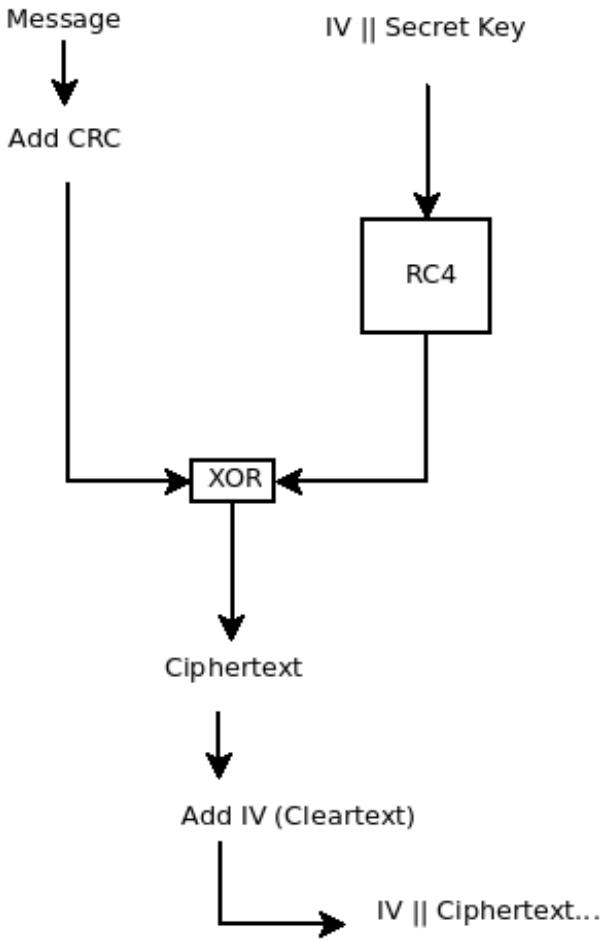


Figure : WEP encryption process

- 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

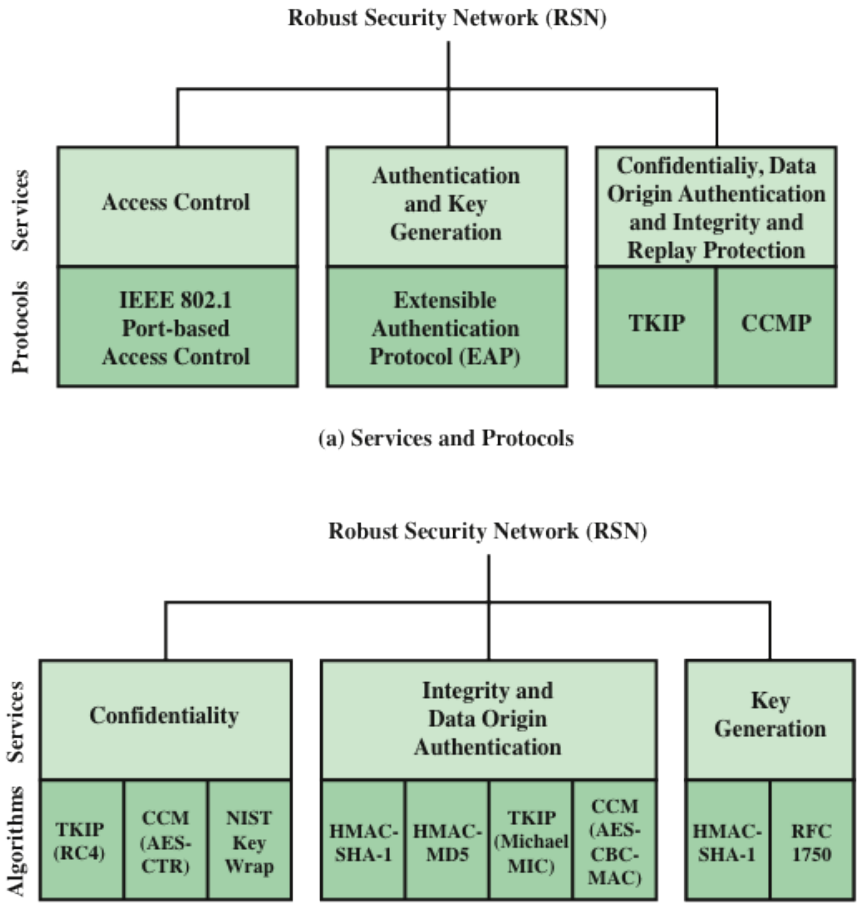


Figure : Elements of 802.11i [1]

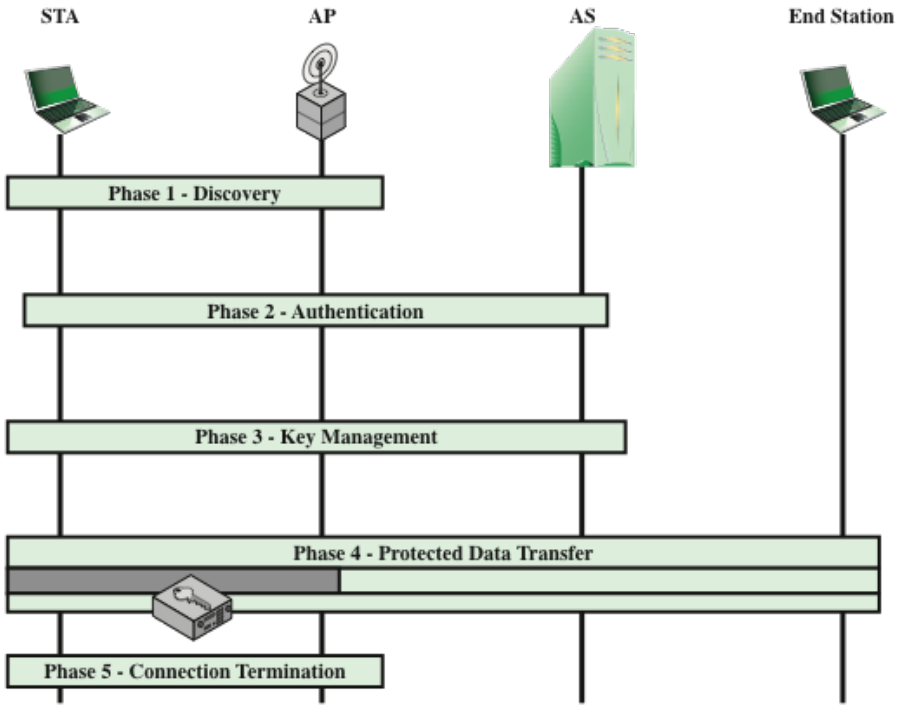


Figure : 802.11i Phases of operation [1]

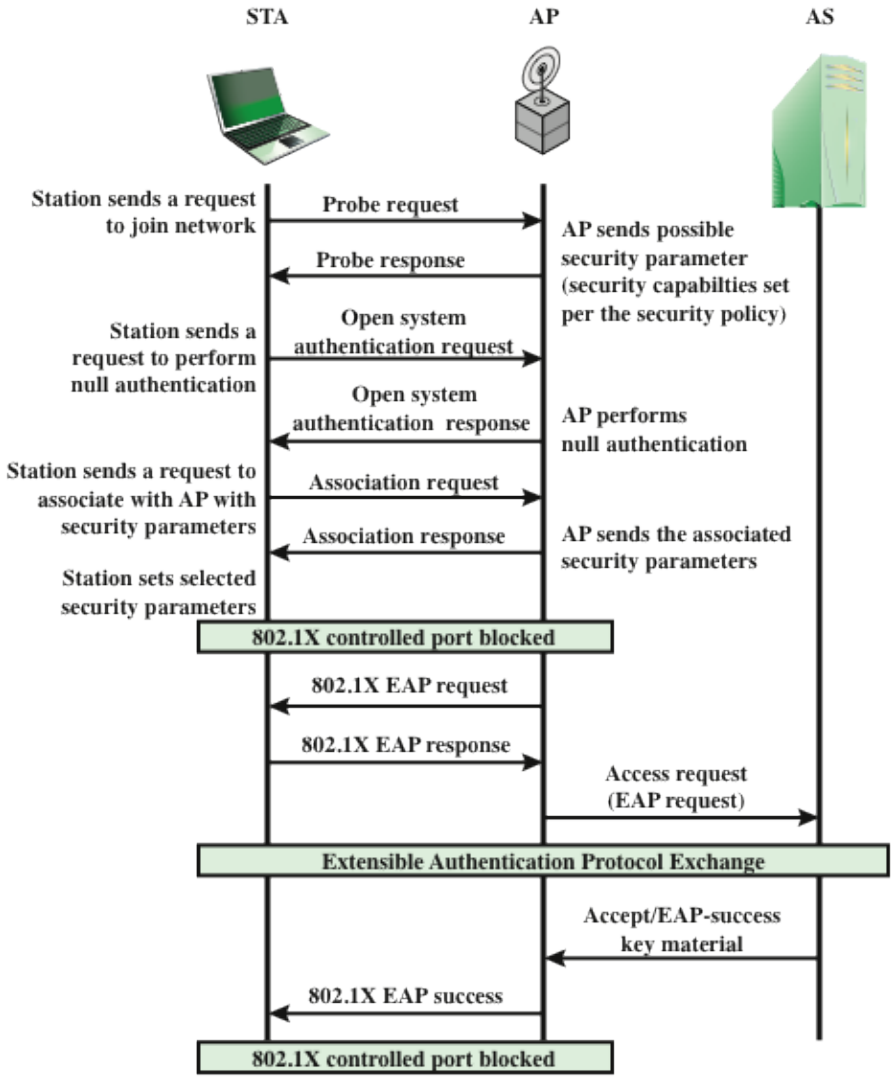


Figure : Discovery, authentication and association [1]

Mittuniversitetet
MID SWEDEN UNIVERSITY

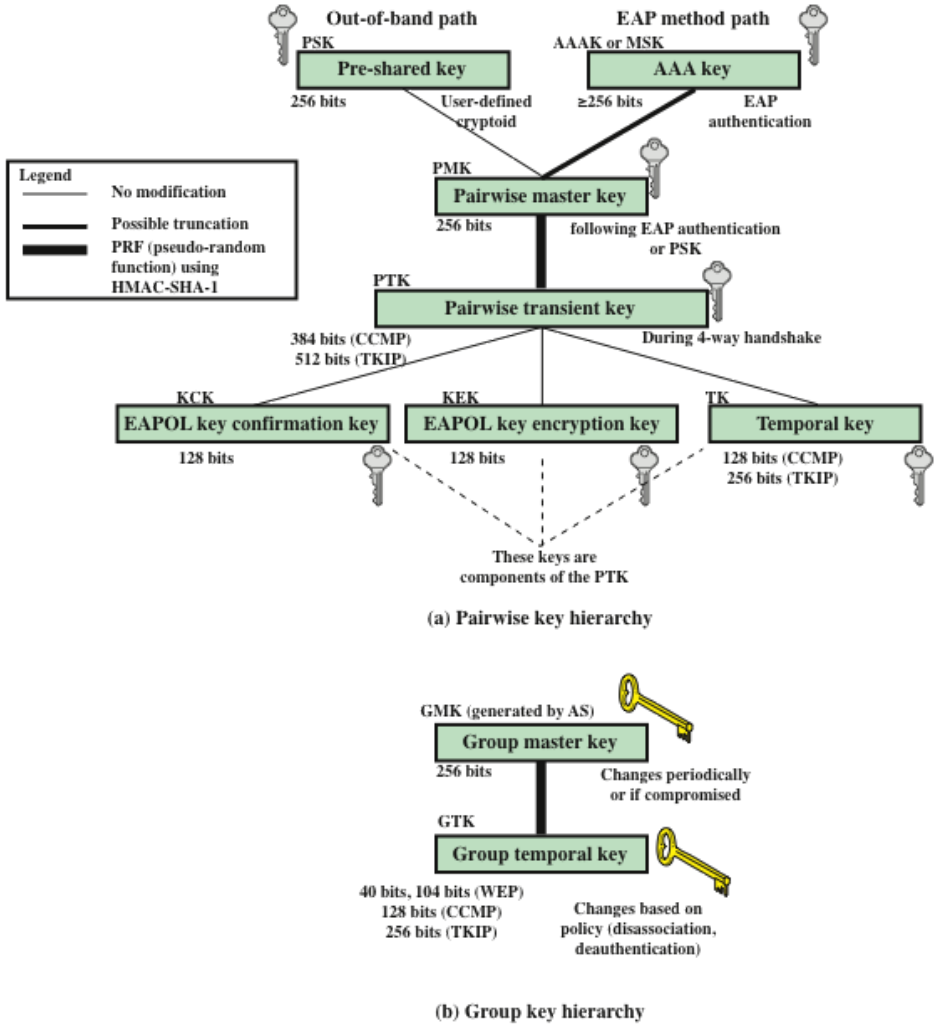


Figure : Key Hierarchies [1]

- 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.

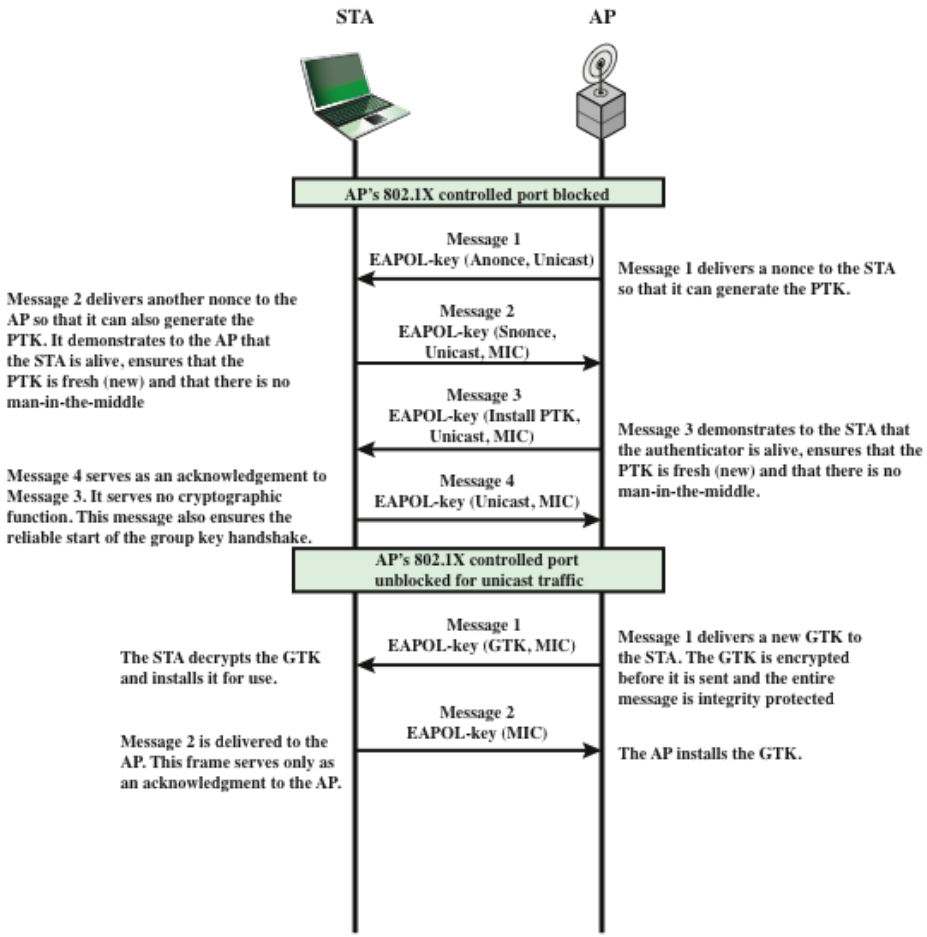


Figure : Four-way handshake and Group Key Handshake [1]

- 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.

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

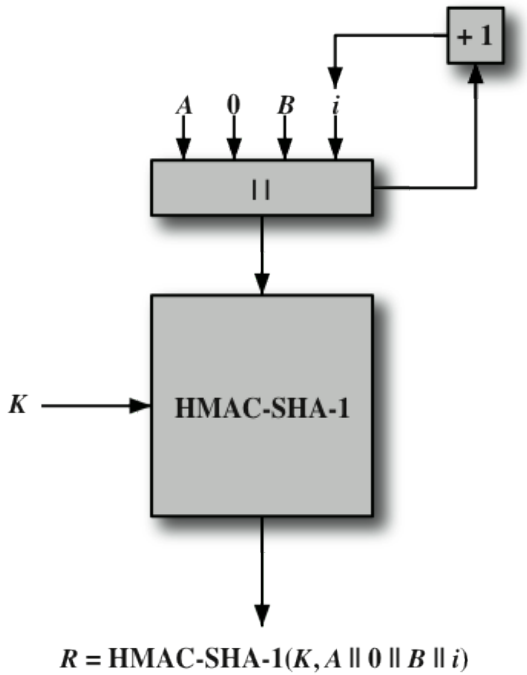


Figure 7.11 IEEE 802.11i Pseudorandom Function

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