b
UNIVERSITÄT
BERN

b
UNIVERSITÄT
BERN

Network Security

VII. Wireless Networks

Prof. Dr. Torsten Braun, Institut für Informatik

Bern, 04.04.2022 – 11.04.2022

Wireless Networks

Table of Contents

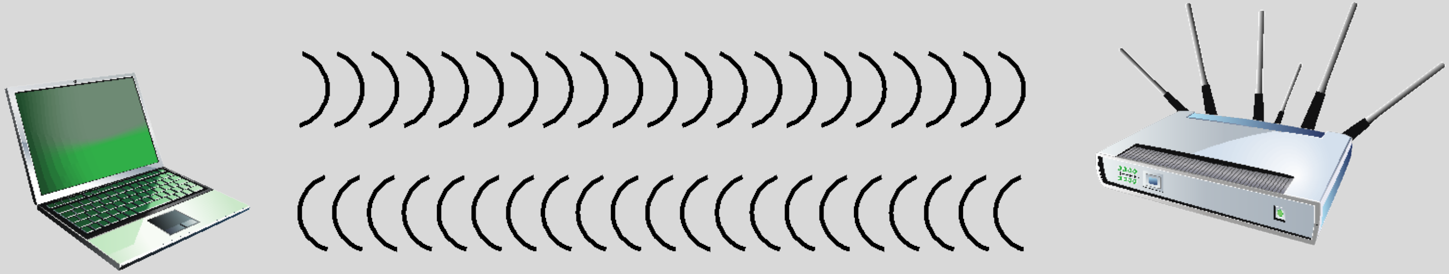
1. Wireless Security
2. Mobile Device Security
3. IEEE 802.11 Wireless LAN
4. IEEE 802.11 Wireless LAN Security

1. Wireless Security

1. Key Factors

- Channel
  - Broadcast Communications are more vulnerable to eavesdropping and jamming.
  - more vulnerable to active attacks
- Mobility
  - Portability creates risks.
- Resources
  - Limited memory and processing resources to counter threads including denial of service attacks
- Accessibility
  - Devices like sensors might be left unattended.
  - Vulnerability to physical attacks

1. Wireless Security
2. Wireless Networking components



Endpoint

Wireless medium

Access point (AP)

1. Wireless Security

3.1 Wireless Network Threats

- Accidental association
  - Company wireless LANs in proximity may create overlapping transmission ranges.
  - User intending to connect to one WLAN may unintentionally log in to a wireless AP from a neighboring network.
- Malicious association
  - A wireless device is configured to appear to be a legitimate access point, enabling the operator to steal passwords from legitimate users.
  - Then it penetrates a wired network through a legitimate wireless AP.
- Ad hoc networks
  - Peer-to-peer networks between wireless computers with no AP between them.
  - Such networks can pose a security threat due to a lack of a central point of control.
- Nontraditional networks
  - Personal network devices, e.g., Bluetooth devices, barcode readers, pose a security risk in terms of both eavesdropping and spoofing.

1. Wireless Security

3.2 Wireless Network Threats

- Identity theft (spoofing)
  - occurs when an attacker is able to eavesdrop network traffic and identify the (MAC) address of a computer with network privileges
- Man-in-the-middle attacks
  - persuading user and AP to believe that they are talking to each other, when in fact the communication is going through an intermediate attacking device
- Denial of Service
  - An attacker continually bombards a wireless AP or some other accessible wireless port with various protocol messages to consume system resources.
- Network injection
  - targets wireless APs that are exposed to non-filtered network traffic, such as routing protocol or network management messages
  - Example:
    bogus reconfiguration commands

1. Wireless Security

4.1 Measures: Securing Wireless Transmissions

Principal **threats** to wireless transmission:

- Eavesdropping
- Altering or inserting messages
- Disruption

Countermeasures

- Signal-hiding techniques
  - Turn off Service Set Identifier broadcasting by wireless APs
  - Cryptic names for SSIDs
  - Reduce signal strength to lowest level that still provides good coverage
  - Locate wireless APs inside the building, away from windows and exterior walls
- Encryption
  - effective against eavesdropping assuming encryption keys are secured

1. Wireless Security

4.2 Measures: Securing Wireless Access Points

Main threat involving wireless APs: unauthorized network access

Principal approach for preventing such access: IEEE 802.1X

- for port-based network access control
- to prevent rogue APs and other unauthorized devices from becoming insecure backdoors

1. Wireless Security

4.3 Measures: Securing Wireless Networks

- Use
  - (built-in) encryption at wireless routers
  - antivirus software
  - antispyware software
  - firewall
- Turn off
  - identifier broadcasting
- Change
  - identifier on router from default
  - router’s pre-set password for administration
- Allow
  - only specific computers to access a wireless network

2. Mobile Device Security

1. Organizational Requirements

- Mobile devices are essential for organizations as part of the overall network infrastructure.
- Prior to the widespread use of smartphones, network security was based upon clearly defined perimeters that separated trusted internal networks from the untrusted Internet.

- Due to massive changes, an organization’s networks must accommodate:
  - growing number of devices
  - cloud-based applications
  - de-perimeterization
  - external business requirements

2. Mobile Device Security

2. Security Threats

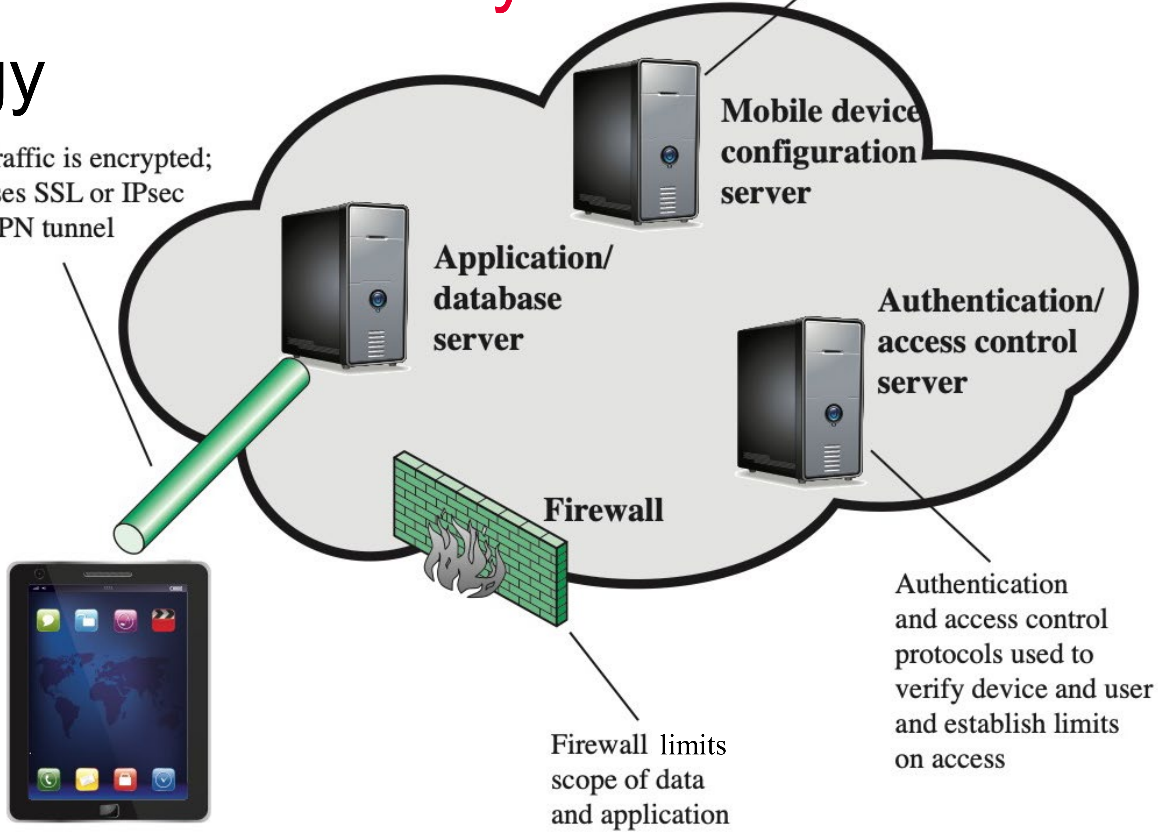
- Lack of physical security controls
  - Security policy must assume that mobile devices can become stolen.
- Use of untrusted devices
  - Assumption that not all devices are trustworthy
- Use of untrusted networks
  - Networks are not trustworthy
- Use of applications created by unknown parties
  - Risk of installing malicious software
- Interaction with other systems
  - Data synchronization with other devices and the cloud
- Use of untrusted content
  - e.g., using QR code
- Use of location services

2. Mobile Device Security

3. Strategy

Mobile device is configured with security mechanisms and parameters to conform to organization security policy

Traffic is encrypted; uses SSL or IPsec VPN tunnel


Mobile device configuration server
Application/ database server
Authentication/ access control server
Firewall

Authentication and access control protocols used to verify device and user and establish limits on access

Firewall limits scope of data and application access

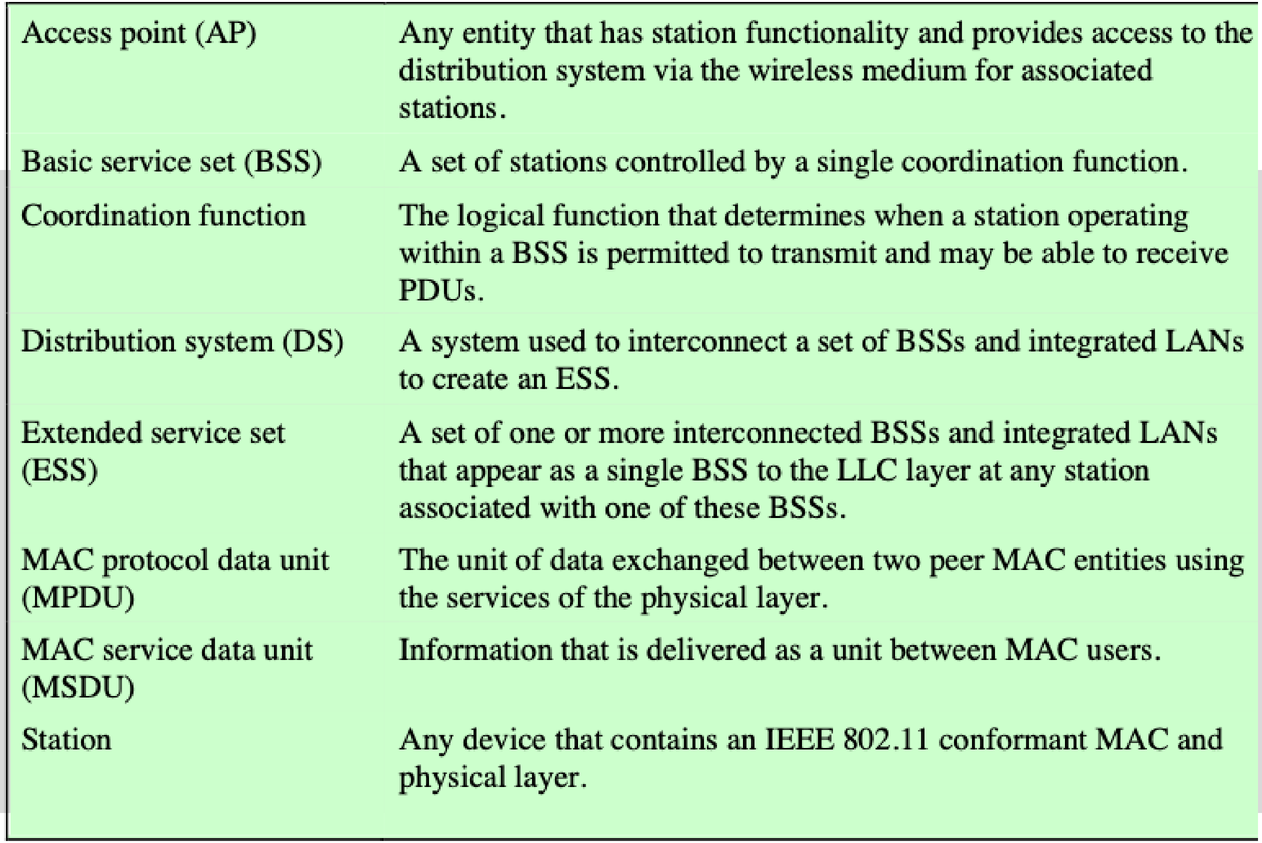
2. Mobile Device Security

4. Categories of Principal Mobile Device Security Elements

- Device security
  - Auto-lock
  - Password or PIN protection
  - Avoid auto-complete for passwords
  - Ensure use of SSL
  - Ensure software and system updates
  - Install antivirus software
  - Encrypted storage of sensitive data
  - Avoid installation of 3rd party software
  - Security training
  - Disable location services
- Client/server traffic security
  - Traffic encryption, e.g., using SSL or VPNs
  - Strong authentication, e.g., multi-factor authentication
- Barrier security
  - Firewalls
  - Intrusion detection and prevention systems

3. IEEE 802.11 Wireless LAN

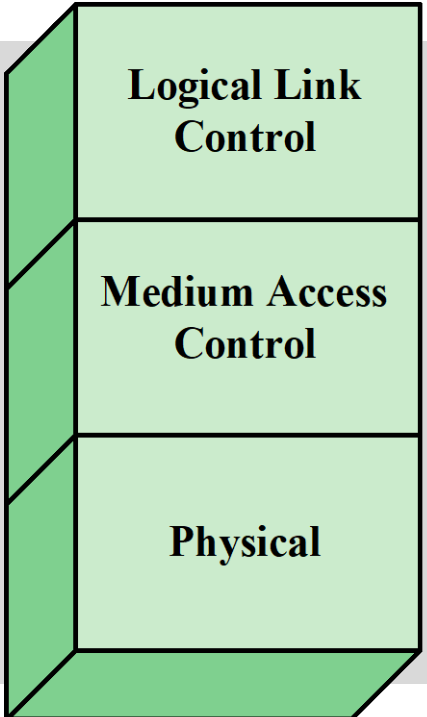
1. Terminology



Access point (AP)	Any entity that has station functionality and provides access to the distribution system via the wireless medium for associated stations.
Basic service set (BSS)	A set of stations controlled by a single coordination function.
Coordination function	The logical function that determines when a station operating within a BSS is permitted to transmit and may be able to receive PDUs.
Distribution system (DS)	A system used to interconnect a set of BSSs and integrated LANs to create an ESS.
Extended service set (ESS)	A set of one or more interconnected BSSs and integrated LANs that appear as a single BSS to the LLC layer at any station associated with one of these BSSs.
MAC protocol data unit (MPDU)	The unit of data exchanged between two peer MAC entities using the services of the physical layer.
MAC service data unit (MSDU)	Information that is delivered as a unit between MAC users.
Station	Any device that contains an IEEE 802.11 conformant MAC and physical layer.

3. IEEE 802.11 Wireless LAN

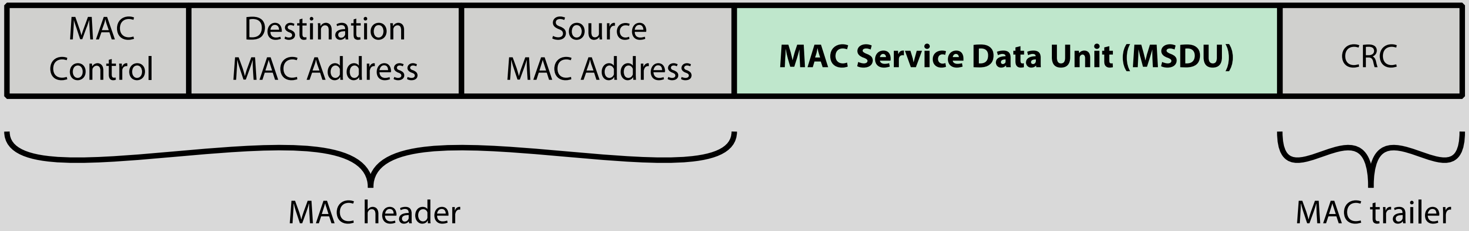
2. Protocol Stack



	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

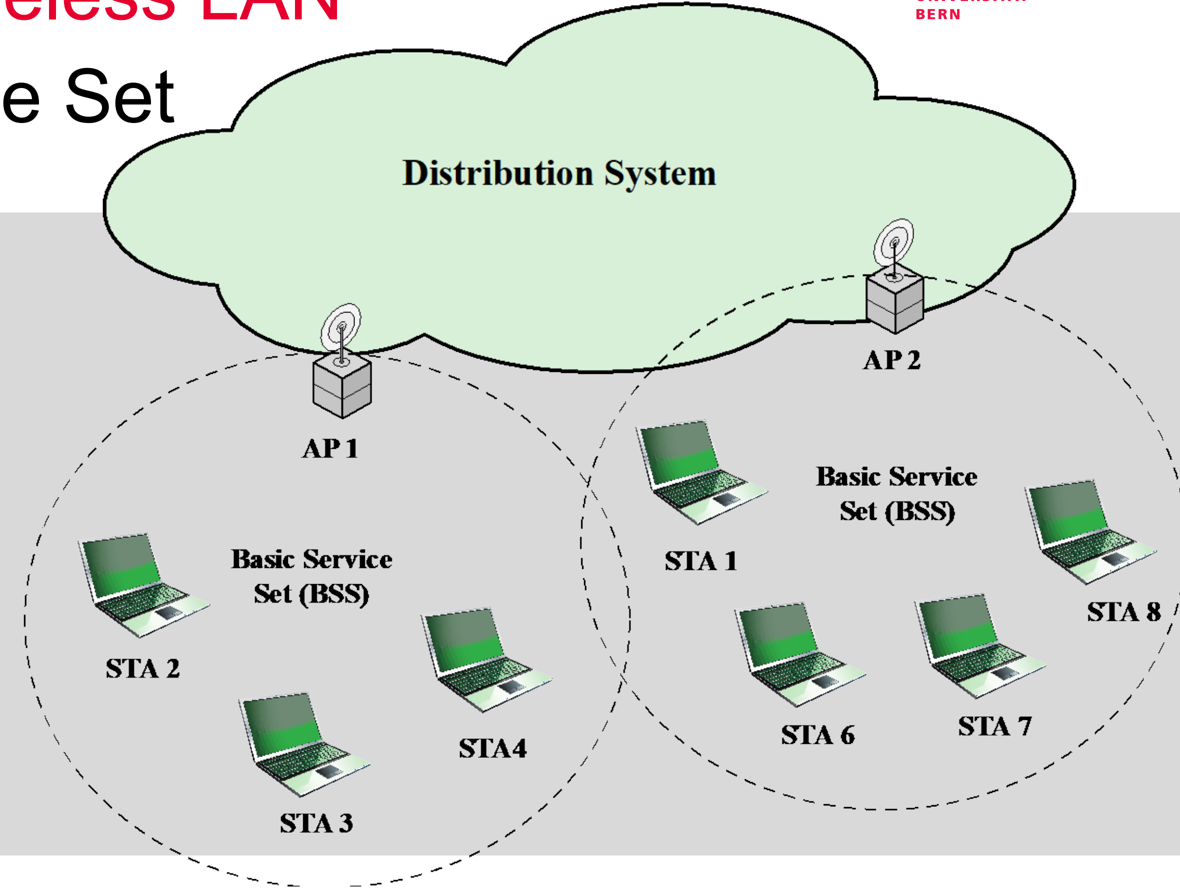
3. IEEE 802.11 Wireless LAN

3. General MPDU Format



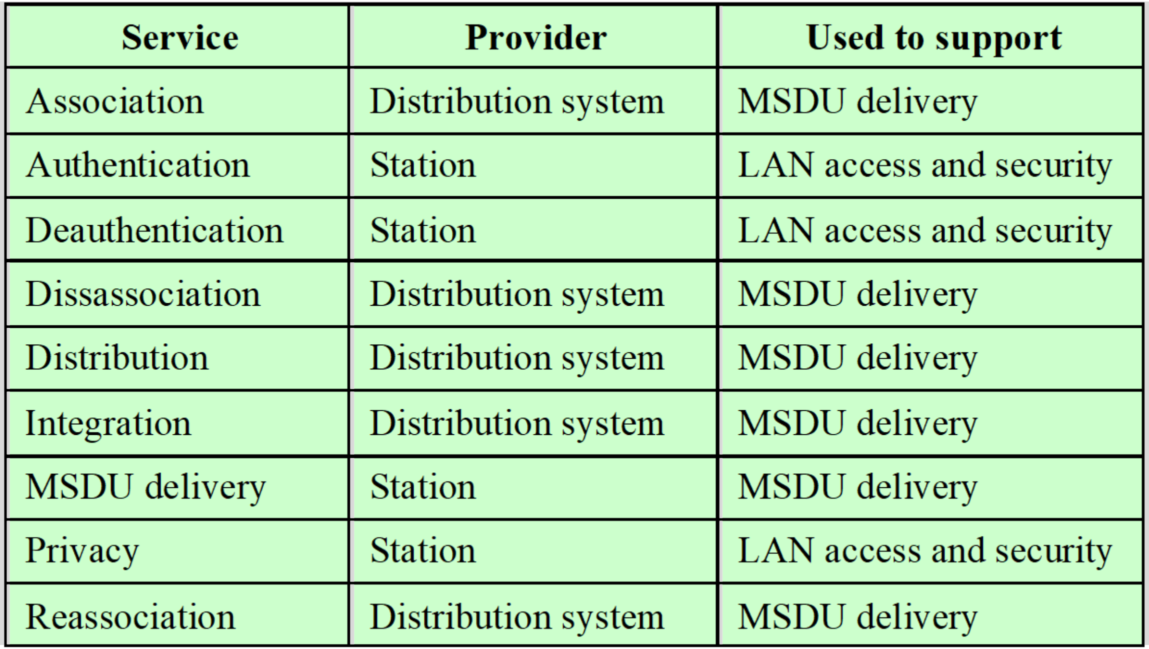
3. IEEE 802.11 Wireless LAN

4. Extended Service Set



3. IEEE 802.11 Wireless LAN

5. Services



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

3. IEEE 802.11 Wireless LAN

6. Association-Related Services: Transition Types

- No transition
  - A station is either stationary or moves only within the direct communication range of the communicating stations of a single BSS.
- BSS transition
  - A station moves from one BSS to another BSS within the same ESS.
  - Data delivery to station requires the addressing capability to recognize the new location of the station.
- ESS transition
  - A station moves from a BSS in an ESS to a BSS within another ESS.
  - Maintenance of upper-layer connections supported by IEEE 802.11 cannot be guaranteed.
  - Disruption of service is likely to occur.

3. IEEE 802.11 Wireless LAN

7. Association-Related Services

To deliver a message within a DS, the DS must know the identity of the AP to which the message should be delivered for that message to reach the destination station.

Services relating to a station maintaining an association with the AP within its current BSS:

- **Association** establishes an initial association between a station and an AP
- **Reassociation** enables an established association to be transferred from one AP to another, allowing a mobile station to move from one BSS to another
- **Disassociation**: A notification from either a station or an AP that an existing association is terminated

4. IEEE 802.11i Wireless LAN Security

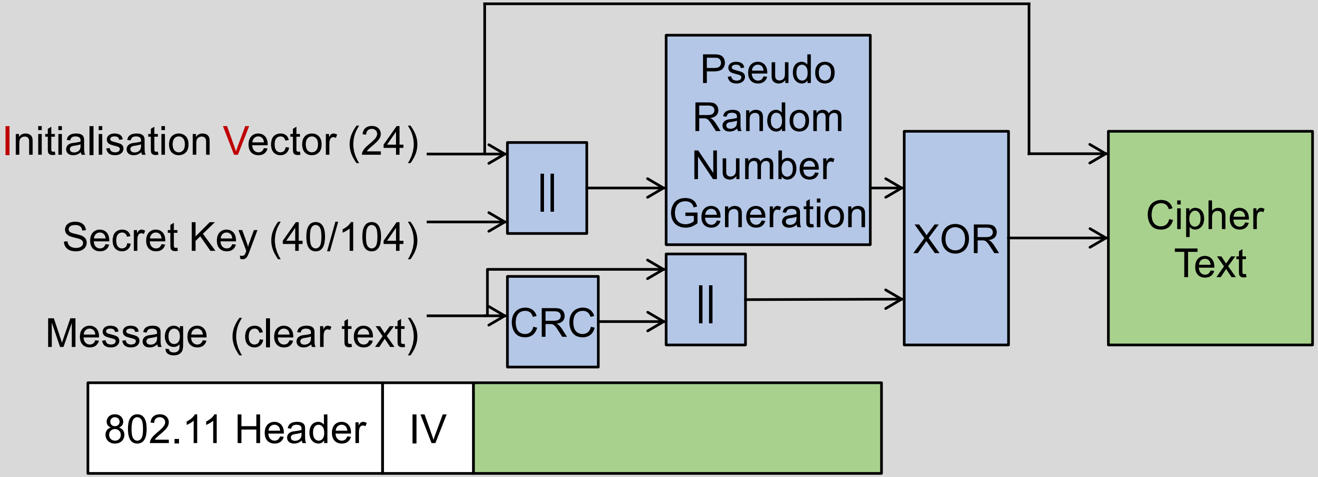
1. Standards

- Wired Equivalent Privacy
  - Privacy portion of IEEE 802.11 standard
  - Some major security flaws
- Wi-Fi Protected Access (WiFi Alliance)
  - A set of security mechanisms that eliminates most IEEE 802.11 security issues
  - WPA2 for 802.11i standard
- Robust Security Network
  - Final form of 802.11i standard

4. IEEE 802.11i Wireless LAN Security

2. Wired Equivalent Privacy

Authentication and encryption with shared keys



4. IEEE 802.11i Wireless LAN Security

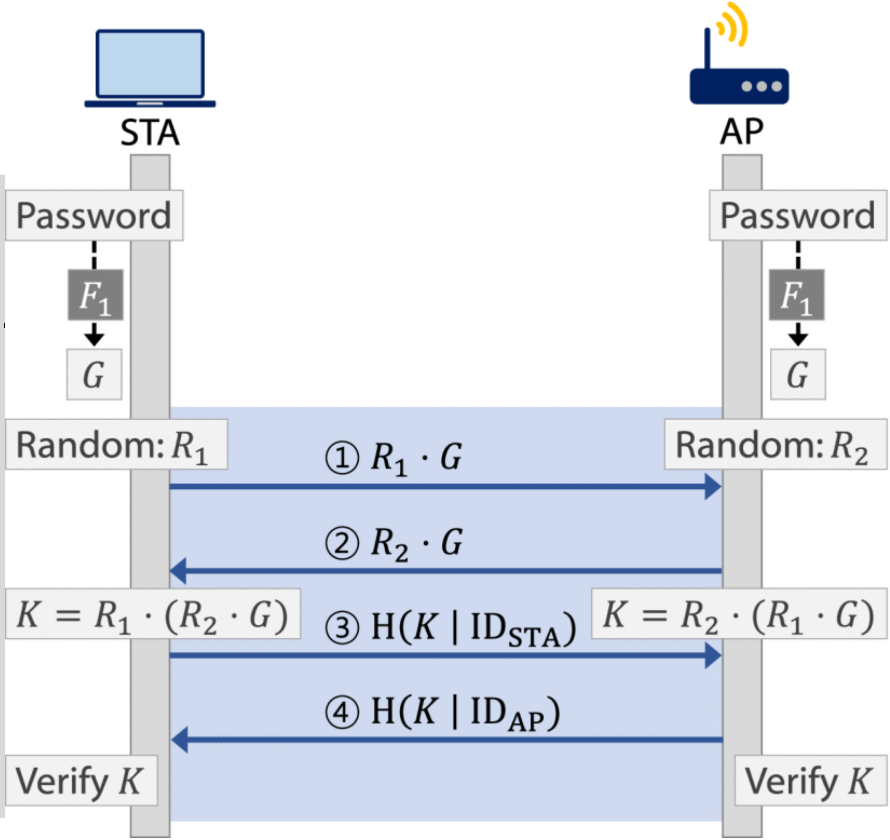
3.1 WiFi-Protected Access

- WPA
  - Temporary Key Integrity Protocol
  - Message Integrity Check replaces CRC.
- WPA2
  - IEEE 802.11i
  - Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCM mode Protocol) based on AES.
- WPA3
  - Enterprise mode: AES-256 with Galois Counter Mode with SHA-384 as HMAC
  - Personal mode: CCMP-128 as minimum encryption algorithm
  - replaces Pre-Shared Key exchange with Simultaneous Authentication of Equals exchange
    - a variant of the Dragonfly Key Exchange [RFC 7664] based on Diffie-Hellman key exchange using finite cyclic groups, e.g., elliptic curves.
    - resistant to dictionary attacks

4. IEEE 802.11i Wireless LAN Security

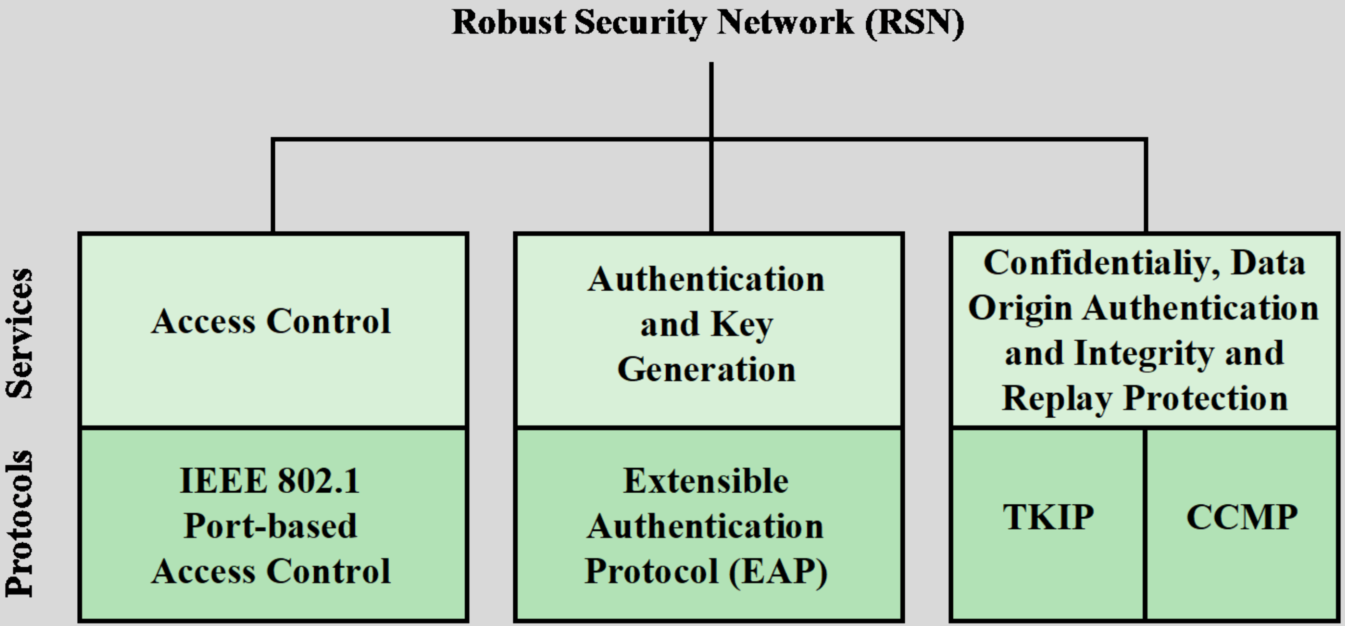
3.2 Dragonfly

Pre-shared password is transformed into generator *G* by the known function.


STA
AP
Password
Password
F_1
F_1
G
G
Random: R_1
Random: R_2
① $R_1 \cdot G$
② $R_2 \cdot G$
$K = R_1 \cdot (R_2 \cdot G)$
③ $\mathrm{H}(K \mid \mathrm{ID}_{\mathrm{STA}})$
$K = R_2 \cdot (R_1 \cdot G)$
④ $\mathrm{H}(K \mid \mathrm{ID}_{\mathrm{AP}})$
Verify K
Verify K

4. IEEE 802.11i Wireless LAN Security

4.1 Robust Security Network: Services and Protocols



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

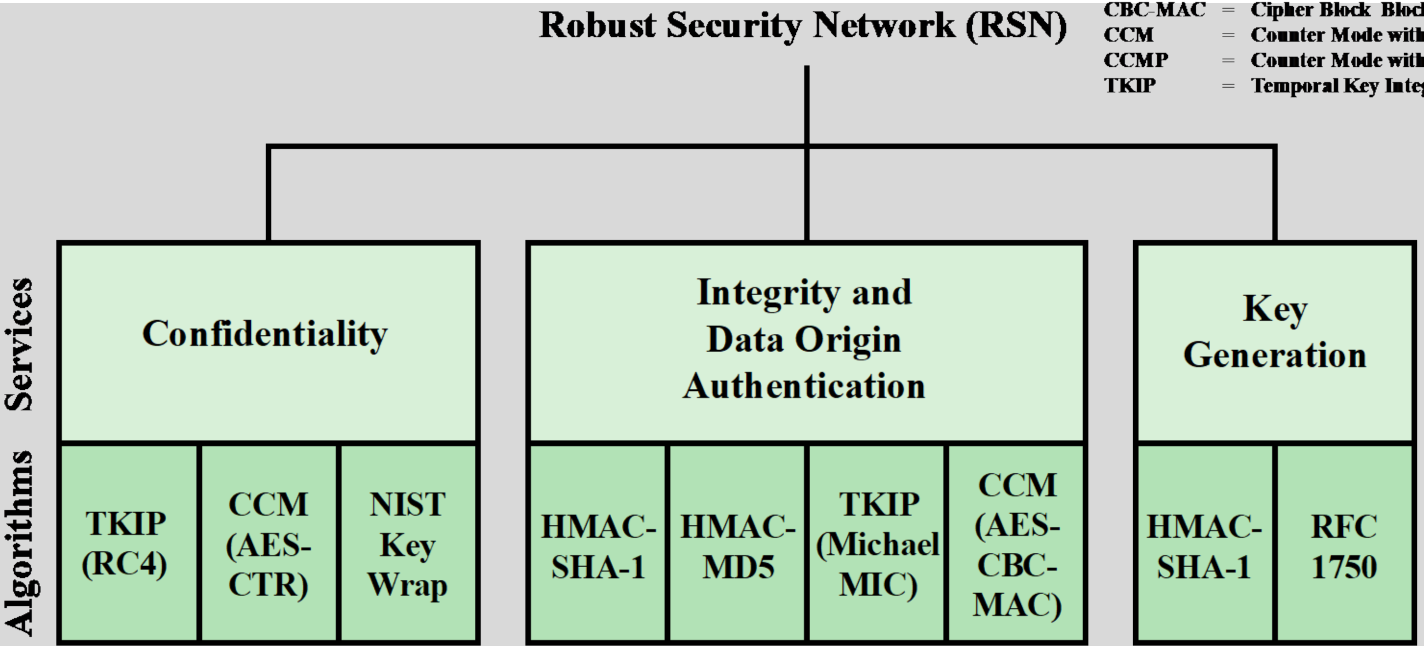
Extensible Authentication Protocol (EAP)

TKIP

CCMP

4. IEEE 802.11i Wireless LAN Security

4.2 RSN Services and Algorithms



Robust Security Network (RSN)

Services

Algorithms

Confidentiality: TKIP (RC4); CCM (AES-CTR); NIST Key Wrap

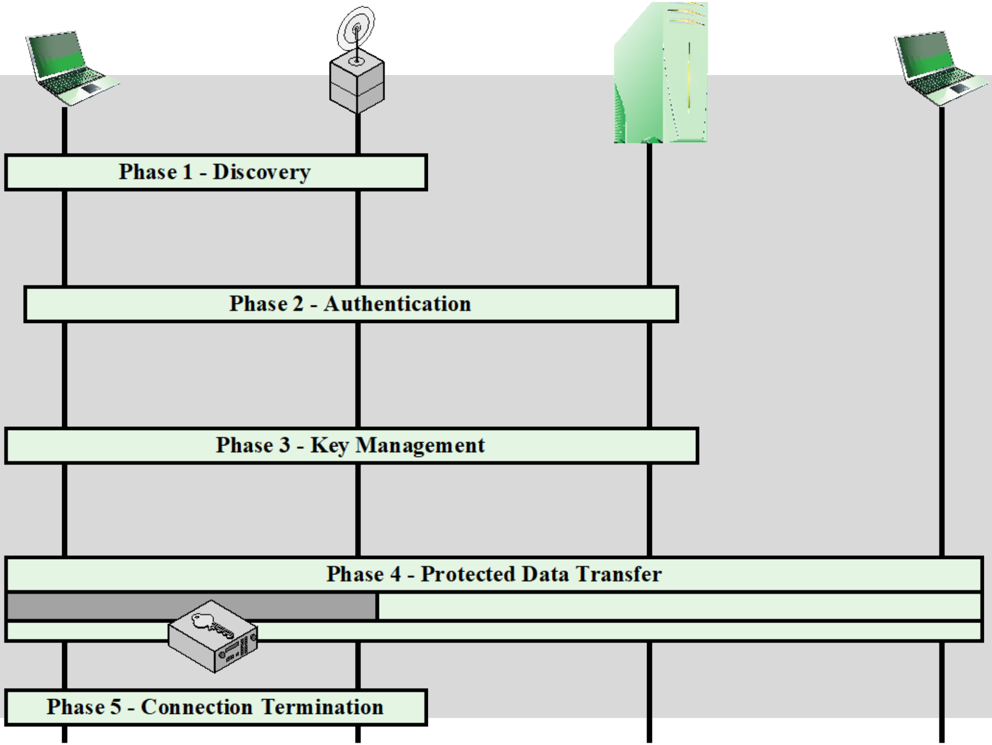
Integrity and Data Origin Authentication: HMAC-SHA-1; HMAC-MD5; TKIP (Michael MIC); CCM (AES-CBC-MAC)

Key Generation: HMAC-SHA-1; RFC 1750

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

4. IEEE 802.11i Wireless LAN Security

4.3 RSN: Phases of Operation



4. IEEE 802.11i Wireless LAN Security

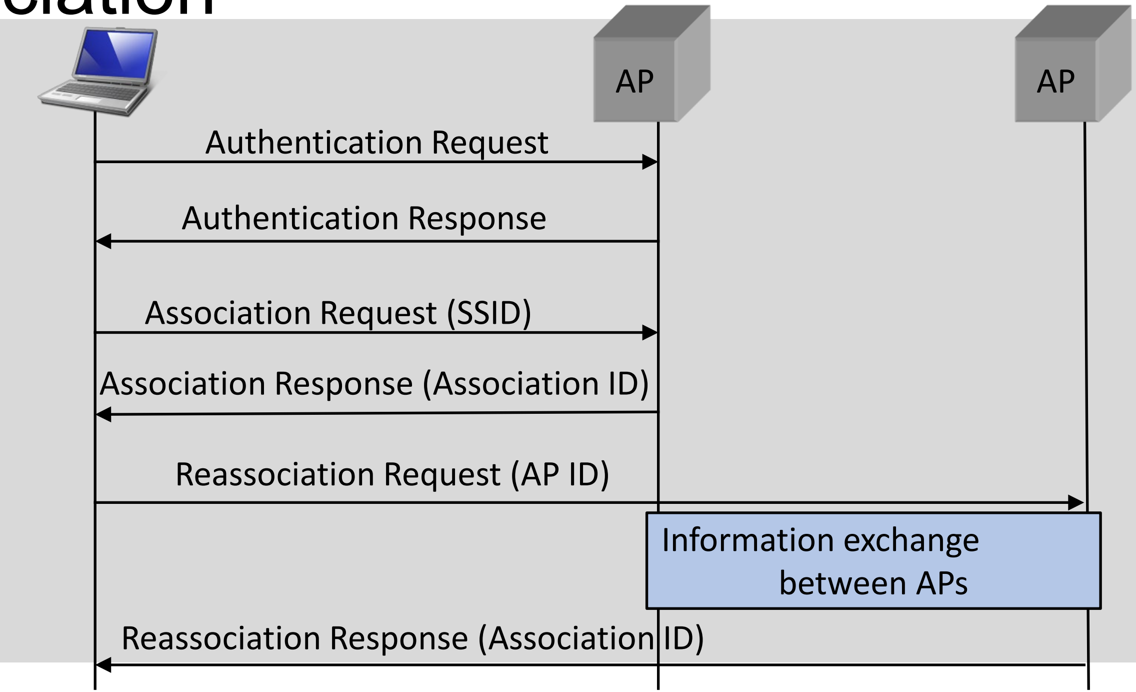
4.4 RSN: Discovery Phase

STA and AP decide on

- Confidentiality and MPDU integrity protocols
  - WEP, TKIP, CCMP
- Authentication method
  - Pre-shared key authentication
  - IEEE 802.1X
- Cryptography key management approach

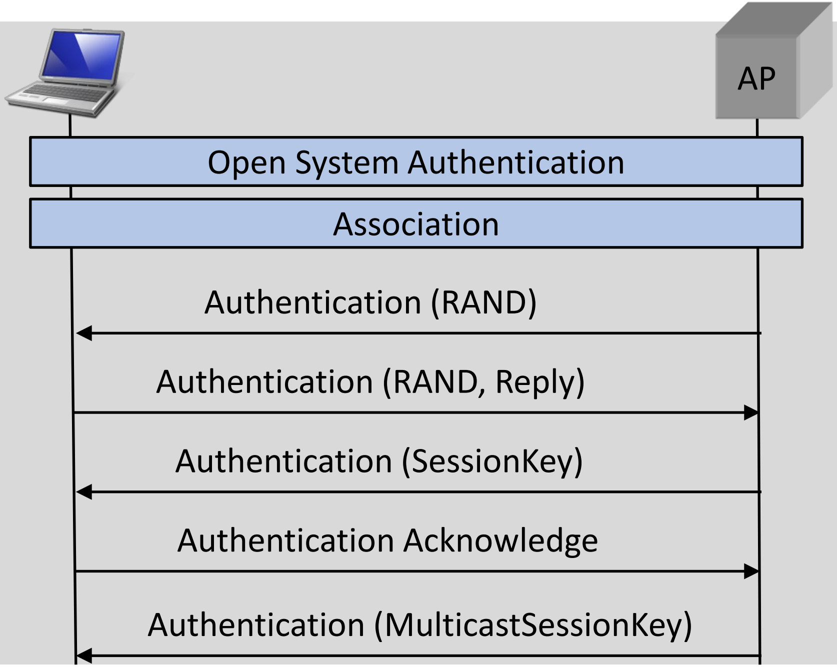
4. IEEE 802.11i Wireless LAN Security

5.1 Open System Authentication, Association and Reassociation


AP
AP
Authentication Request
Authentication Response
Association Request (SSID)
Association Response (Association ID)
Reassociation Request (AP ID)
Information exchange between APs
Reassociation Response (Association ID)

4. IEEE 802.11i Wireless LAN Security

5.2 Pre-Shared Key Authentication


AP
Open System Authentication
Association
Authentication (RAND)
Authentication (RAND, Reply)
Authentication (SessionKey)
Authentication Acknowledge
Authentication (MulticastSessionKey)

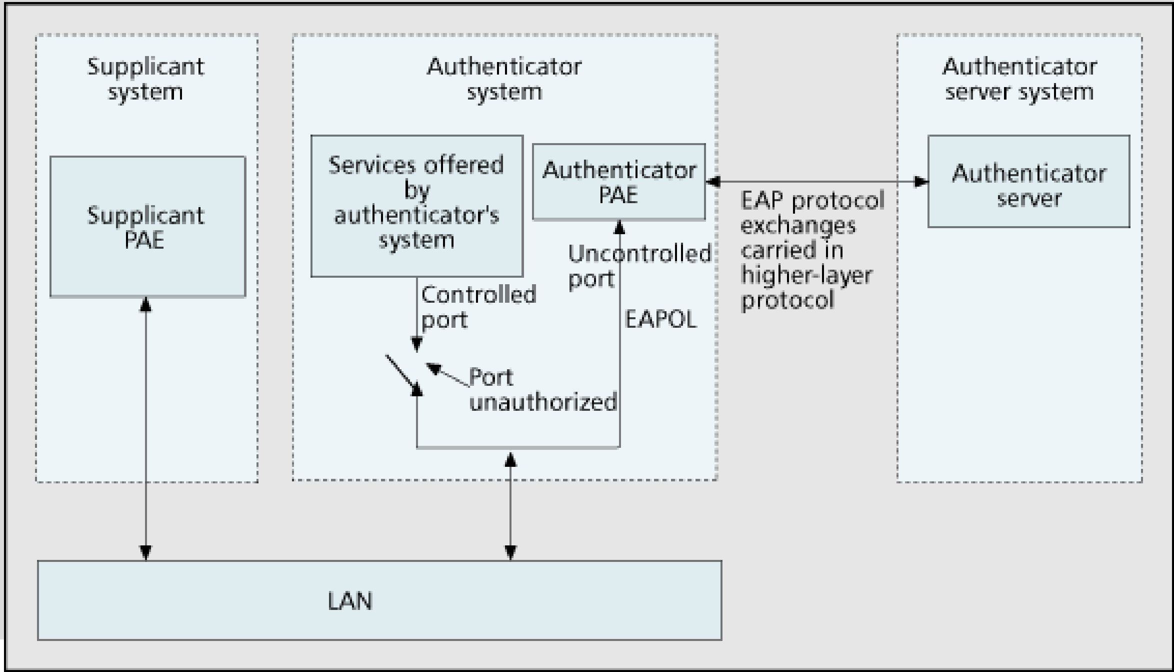
4. IEEE 802.11i Wireless LAN Security

5.3.1 IEEE 802.1X Access Control

- Port-Based Network Access Control
- Extensible Authentication Protocol defined in IEEE 802.1X standard

802.1X uses

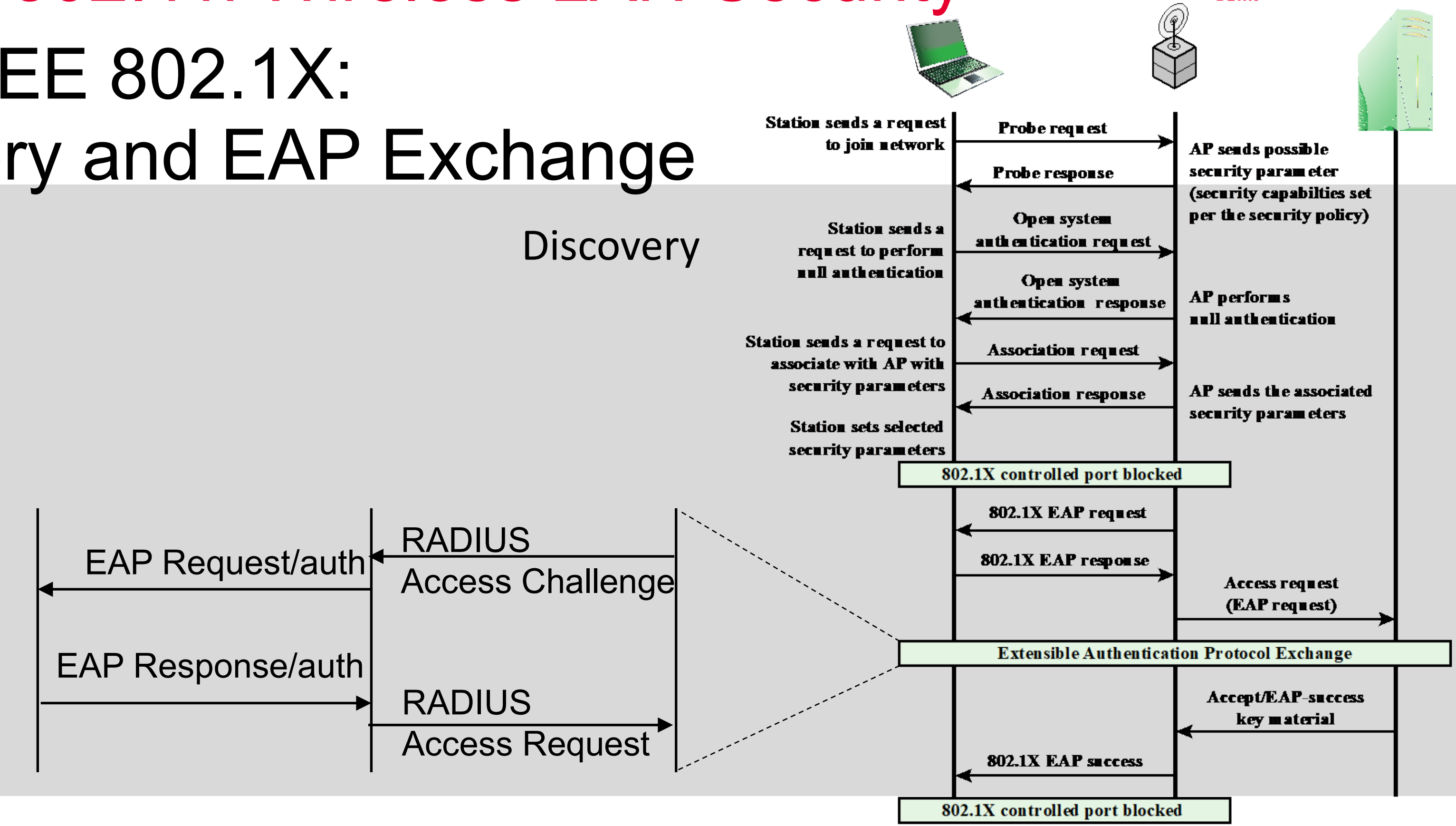
- controlled ports
  - to allow the exchange of PDUs between a supplicant and other systems on the LAN only if the current state of the supplicant authorizes such an exchange
- uncontrolled ports
  - to allow the exchange of PDUs between supplicant and AS, regardless of the authentication state of the supplicant



4. IEEE 802.11i Wireless LAN Security

5.3.2 IEEE 802.1X: Discovery and EAP Exchange

Discovery



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

EAP Request/auth

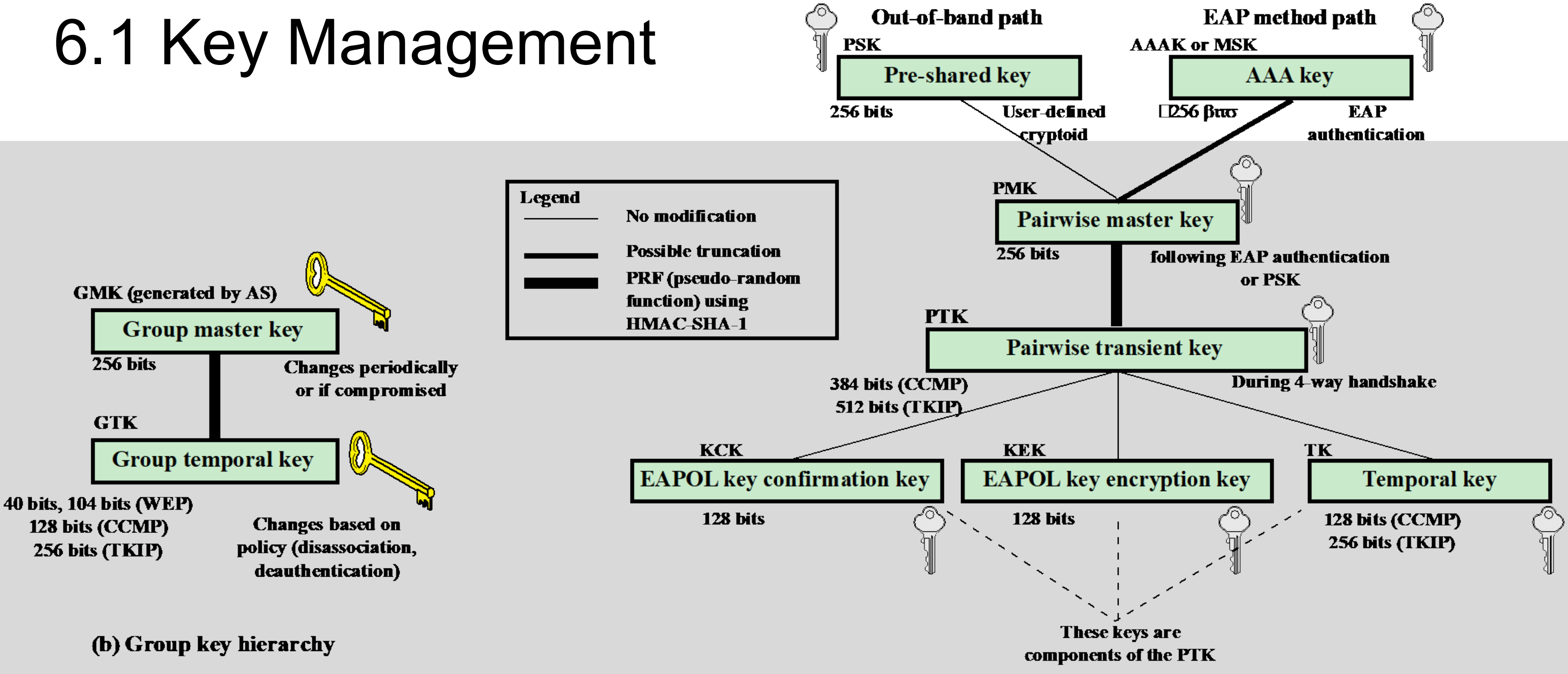
RADIUS Access Challenge

EAP Response/auth

RADIUS Access Request

4. IEEE 802.11i Wireless LAN Security

6.1 Key Management

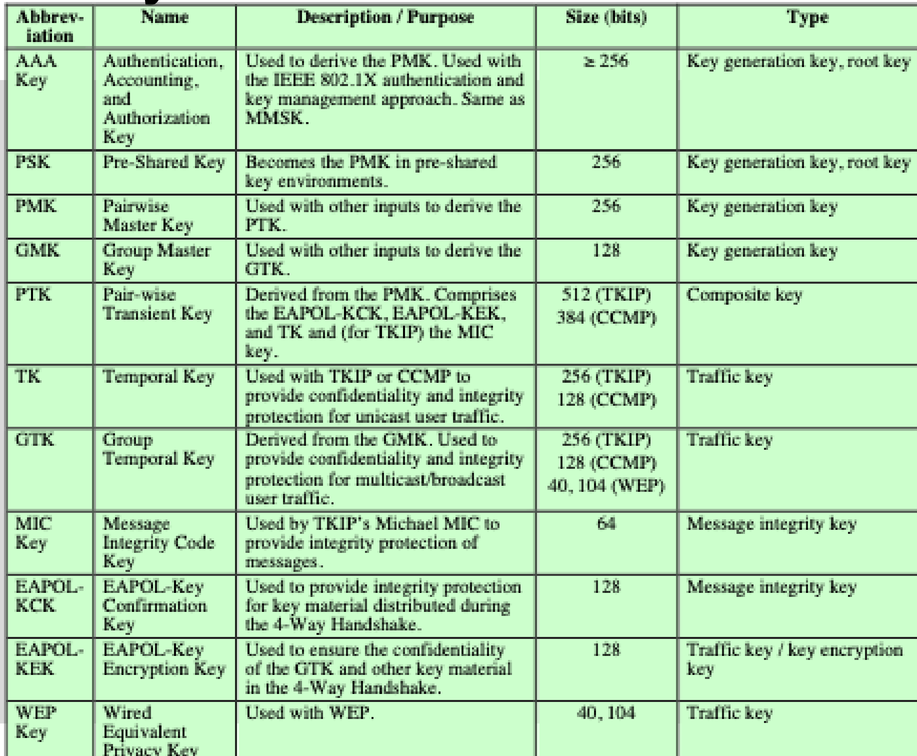


(b) Group key hierarchy

(a) Pairwise key hierarchy

4. IEEE 802.11i Wireless LAN Security

6.2 Keys for Data Confidentiality and Integrity Protocols



Abbrev-iation	Name	Description / Purpose	Size (bits)	Type
AAA Key	Authentication, Accounting, and Authorization Key	Used to derive the PMK. Used with the IEEE 802.1X authentication and key management approach. Same as MMSK.	≥ 256	Key generation key, root key
PSK	Pre-Shared Key	Becomes the PMK in pre-shared key environments.	256	Key generation key, root key
PMK	Pairwise Master Key	Used with other inputs to derive the PTK.	256	Key generation key
GMK	Group Master Key	Used with other inputs to derive the GTK.	128	Key generation key
PTK	Pair-wise Transient Key	Derived from the PMK. Comprises the EAPOL-KCK, EAPOL-KEK, and TK and (for TKIP) the MIC key.	512 (TKIP) 384 (CCMP)	Composite key
TK	Temporal Key	Used with TKIP or CCMP to provide confidentiality and integrity protection for unicast user traffic.	256 (TKIP) 128 (CCMP)	Traffic key
GTK	Group Temporal Key	Derived from the GMK. Used to provide confidentiality and integrity protection for multicast/broadcast user traffic.	256 (TKIP) 128 (CCMP) 40, 104 (WEP)	Traffic key
MIC Key	Message Integrity Code Key	Used by TKIP's Michael MIC to provide integrity protection of messages.	64	Message integrity key
EAPOL-KCK	EAPOL-Key Confirmation Key	Used to provide integrity protection for key material distributed during the 4-Way Handshake.	128	Message integrity key
EAPOL-KEK	EAPOL-Key Encryption Key	Used to ensure the confidentiality of the GTK and other key material in the 4-Way Handshake.	128	Traffic key / key encryption key
WEP Key	Wired Equivalent Privacy Key	Used with WEP.	40, 104	Traffic key

4. IEEE 802.11i Wireless LAN Security

6.3.1 Pairwise Keys

Used for communication between a pair of devices, typically between a STA and an AP

- These keys form a hierarchy beginning with a master key from which other keys are derived dynamically and used for a limited period of time

Pre-Shared Key

- secret key shared by AP and STA, which is installed outside the scope of IEEE 802.11i

Master Session Key

- (also known as the AAAK) is generated using the IEEE 802.1X protocol during the authentication phase

Pairwise Master Key

- derived from MSK
- If a PSK is used: PSK is used as PMK;
  if a MSK is used:
  PMK is derived from the MSK by truncation

Pairwise Transient Key

- consists of three keys to be used for communication between a STA and AP after they have been mutually authenticated.
- Using the STA and AP MAC addresses in the generation of the PTK provides protection against session hijacking and impersonation; using nonces provides additional random keying material

4. IEEE 802.11i Wireless LAN Security

6.3.2 PTK Parts

EAP Over LAN – Key Confirmation Key

– supports the integrity and data origin authenticity of STA-to-AP control frames during operational RSN setup

– performs access control function: proof-of-possession of the PMK

– An entity that possesses the PMK is authorized to use the link.

EAPOL – Key Encryption Key

– protects the confidentiality of keys and other data during some RSN association procedures.

Temporal Key

– provides the actual protection for user traffic.

4. IEEE 802.11i Wireless LAN Security

6.4 Group Keys

Group keys for multicast communication: 1 STA sends MPDUs to multiple STAs.

Group Master Key

- Key-generating key used with other inputs to derive the GTK

Group Temporal Key

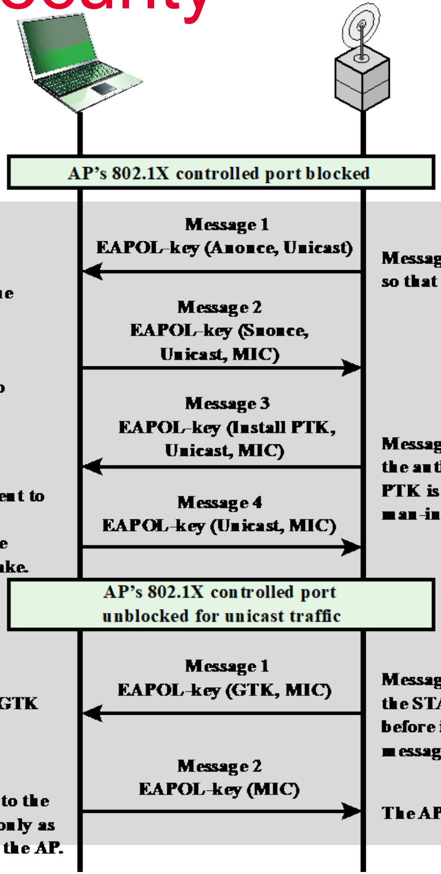
- is generated by the AP and transmitted to its associated STAs
- IEEE 802.11i requires that its value is computationally indistinguishable from random
- is distributed securely using the pairwise keys that are already established
- is changed every time a device leaves the network

4. IEEE 802.11i Wireless LAN Security

6.5 Pairwise Key Distribution

4-Way Handshake

Group Key Handshake



AP's 802.1X controlled port blocked

Message 1
EAPOL-key (Anonce, Unicast)

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

Message 2
EAPOL-key (Snonce, Unicast, MIC)

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
EAPOL-key (Install PTK, Unicast, MIC)

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
EAPOL-key (Unicast, MIC)

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.

AP's 802.1X controlled port unblocked for unicast traffic

Message 1
EAPOL-key (GTK, MIC)

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
EAPOL-key (MIC)

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

The AP installs the GTK.

4. IEEE 802.11i Wireless LAN Security

7.1 Protected Data Transfer Phase

Temporal Key Integrity Protocol

- designed to require only software changes to devices that are implemented with WEP
- Periodic rekeying, after not more than 10'000 frames
- Services
  - Message integrity
    - adds Message Integrity Code to MAC frame after data field
  - Data confidentiality
    - Encrypting MPDU/MIC by RC4

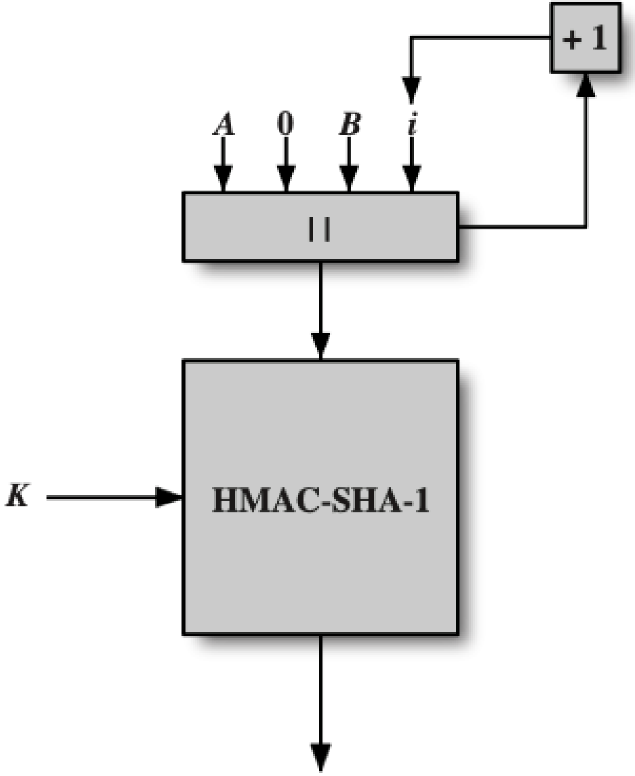
Counter Mode-CBC MAC Protocol

- intended for newer IEEE 802.11 devices that are equipped with the hardware to support this scheme
- Services
  - Message integrity
    - CBC-MAC
  - Data confidentiality
    - CTR block cipher mode with AES

4. IEEE 802.11i Wireless LAN Security

7.2 Pseudorandom Function

- used at a number of places in the IEEE 802.11i scheme to
  - generate nonces
  - expand pairwise keys
  - generate the GTK
- HMAC-SHA-1 to generate a pseudorandom bit stream



$R = \text{HMAC-SHA-1}(K, A \parallel 0 \parallel B \parallel i)$

Thanks

for your Attention

b
UNIVERSITÄT
BERN

Prof. Dr. Torsten Braun, Institut für Informatik

Bern, 04.04.2022 – 11.04.2022