4.4 IEEE 802.11 MAC Layer

4.4.1 Introduction
4.4.2 Medium Access Control
4.4.3 MAC Management
4.4.4 Extensions
4.4.3 802.11 - MAC management

• Synchronization
  – try to find a LAN, try to stay within a LAN
  – timer etc.

• Power management
  – Periodic sleep without missing a message by negotiated sleep periods and buffering frames during such periods
  – Implemented, but rarely used

• Association/Reassociation
  – integration into a LAN
  – roaming, i.e. change networks by changing access points
  – scanning, i.e. active search for a network

• MIB – Management Information Base
  – managing, read, write
Synchronisation

• Each station has an internal clock; 802.11 specifies Timing Synchronisation Function (TSF) to synchronise all these clocks

• Exact synchronised clocks are important for
  – Power saving, PCF coordination, synchronisation of frequency hopping of FHSS

• In a BSS (Basic Service Set) synchronisation is supported by a beacon periodically transmitted
  – Beacon contains time stamp + info on power saving and roaming (BSSID)
  – Beacon is used to adjust clocks
  – Exact periodic transmission of beacon is not possible as medium is shared by all stations

• In infrastructure networks beacon is transmitted by Access Point
Synchronization (infrastructure)

Beacon Interval: 20ms – 1s
No or bad connection? Then perform:

- **Scanning**
  - scan the environment, i.e., listen into the medium for beacon signals *(passive scanning)*, send probes into medium and wait for an answer *(active scanning)*

- **Reassociation Request**
  - station sends a request to one or several AP(s)

- **Reassociation Response**
  - success: AP has answered, station can now participate
  - failure: continue scanning

- **AP accepts Reassociation Request**
  - signal the new station to the distribution system
  - the distribution system updates its data base (i.e., location information)
  - typically, the distribution system now informs the old AP so it can release resources
802.11 – Roaming (2)

- Roaming implementation is often not compatible between different hardware manufacturers
- Therefore 802.11F (Inter Access Point Protocol, IAPP) had been standardised:
  - Also enables load balancing between Access Points
  - Generation of new keys for security algorithms based on 802.1x
  - Was however only published as recommended practice, meanwhile abandoned
  - Nowadays roaming solutions vendor specific
MAC Services

• **802.11 requires provisioning of 9 services:**
  – 5 Distribution Services, 4 Station Services

• **Distribution Services**
  – Association: register with exactly one AP
  – Disassociation: deregister from AP
  – Re-Association: reregister with new AP after roaming
  – Distribution: deliver packets across the distribution system
  – Integration: cooperation with LANs

• **Station Services**
  – Authentication: with AP
  – De-Authentication: from AP
  – Privacy: e.g., encryption
  – Data Delivery: deliver packets to another physically connected station

www.intelligraphics.com/introduction-ieee-80211
and Tanenbaum
4.4.4 IEEE802.11e: Motivation

- 802.11 almost only used as best-effort networks
- No priorisation between different traffic types
- Limited support of time-critical applications
  - No consideration of certain throughput and delay demands
  - Works if load is low (cf. 802.3 load curve)
- Precise control of the channel needed in any situation
IEEE802.11e: EDCA

- Enhanced Distributed Channel Access
- Extends DCF of legacy 802.11
- Up to 8 queues / traffic classes (TC) for different application types, each with individual backoff
- Transmission parameters configurable for each TC: CWmin, CWmax, arbitrary IFS (AIFS) with configurable duration, min. duration = DIFS duration
- Virtual collisions (inside the station's protocol stack)
  If two queues decide to send packet at same time
  - queue with higher priority sends first
  - queue with lower priority retransmits, but CW is not increased, because no physical collision
IEEE802.11e: HCCA

- Hybrid Coordination Function Controlled Channel Access
- Extends PCF of legacy 802.11
- Up to 8 queues / traffic classes (TC) for different application types
- Channel access determined by scheduler
  - Determines order of data packets (downlink) and polling packets (uplink)
  - Algorithm out of the scope of standard, vendor-specific
- Like in PCF, mixing of contention-free periods and contention periods possible
IEEE802.11n: Frame Aggregation

- On the MAC: frame aggregation / packet trains
  - Multiple packets are sent consecutively and acknowledged by one single Block ACK
### 802.11n Aggregated Frame Format

<table>
<thead>
<tr>
<th>Reserved</th>
<th>length</th>
<th>CRC</th>
<th>Delimiter</th>
<th>MAC Frame</th>
<th>Pad</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>12</td>
<td>8</td>
<td>8</td>
<td>variable</td>
<td>0-3</td>
</tr>
</tbody>
</table>

- **Delimiter**: signature to support recovery in case of transmission errors
In the infrastructure mode
• Access points in infrastructure networks are connected by wires
• Mobile stations can only communicate via the access point
802.11s Mesh Networks: Architecture

- MGs and APs can be connected by wireless backhaul
- Mobile stations can communicate directly or via intermediate hops
802.11s Mesh Networks: Usage

W. Conner et al.: IEEE 802.11s Tutorial, IEEE 802 Plenary, November 2006
4.5 WLAN Security

4.5.1 WEP
4.5.2 WPA, EAP, 802.1X
4.5.3 WAP2/802.11i
4.5.4 WPS
4.5.5 other security layers
Objectives of Security

- Authorisation
  - Only authorised terminals can access BSS
  - Terminal is accessing authorised AP and not “rogue” AP
  - Certificates or passwords for authorisation
- Privacy/Encryption
  - Generally anyone can listen to wireless channel with appropriate tools
- Authentication
  - Authenticate the originator or the message
- Integrity
  - Data manipulation, can be prevented by encryption and checksums
Security a problem?

Sender, Receiver and Intruder (Alice, Bob and Trudy)

- Packet sniffing
- IP spoofing
- Denial-of-service attack

Kurose/Ross
Security Overview in legacy 802.11

MAC layer (OSI Layer 2) access control and encryption mechanisms:

• ESSID (WLAN Service Area ID) is required knowledge for a station to associate with an AP
  – ESSIDs can be easily sniffed

• Access Control List: a table of MAC addresses restricting access to clients whose MAC addresses are on the list
  – Not feasible for large environments with changing users
  – MAC addresses can be easily forged

• Wired Equivalent Privacy (WEP)

http://www.pulsewan.com/data101/802_11_b_basics.htm
4.5.1 **WEP: encryption**

A. Arnold, Jenseits von WEP, Heise, c’t 21/2004, p. 214ff

Weaknesses: IV too short, static shared key
WEP: Shared Key Authentication

- Uses private key authentication scheme shown on previous slide

STA

identity assertion

identity assertion/challenge text

encrypted text

success/failure

Encrypted using shared WEP key

AP

128-bit one-time nonce

Decrypted using shared WEP key
WEP weaknesses

• All users share the same key
• Keys are not regularly changed, but stay constant until changed by the user
• IV is recommended to be changed with every packets, but many manufacturers do not do it
• IV too short
• Known attacks since several years
• AP does not have to authenticate against client
  – “wild” APs can attack client
4.5.2 WPA: Security Improvements

- Design Objectives:
  - no new chip design
  - backwards compatible to old hardware
- Therefore
  - No fixed WEP key, but dynamic assignment of keys
    - for each connection set-up and during ongoing connections
  - User-specific keys
- Introduced 1999; intermediate step towards 802.11i
- marketed as WPA
- For key exchange: 802.1X carries EAP (Extensible Authentication Protocol) messages – counterpart for RADIUS on the wired side
- For encrypted connection: Algorithms TKIP and Michael replacing WEP
EAP and 802.1X (1)

- EAP (Extensible Authentication Protocol)
  Primary objective: Authentication for secure access to (fixed) Network
- Client and Server have to authenticate – no “wild” AP
- Secure tunnel between client and server for Access
- At the end Server sends Master Secret to AP
- AP manages tunnel and sends encryption key to client via tunnel
  - regular update of key via tunnel (e.g. 5 min)
- Disadvantage: RADIUS server infrastructure difficult to install & maintain
- For SOHO usage: pre-shared key
  - Passphrase 8 to 64 characters is used with SSID to calculate Master Secret via Hash
EAP and 802.1X (2)

Only EAP traffic allowed before this point

Only EAP traffic allowed beyond this point
Signalling in WPA

• For Broadcast packets encryption needs to be supported by all clients of BSS
  – If mixed WEP/WPA clients are allowed, the weaker WEP encryption has to be used for broadcasts

• Info broadcasted via beacon
  – Encryption modes for pairwise keys: WEP is included/excluded
  – Authentication: EAP/802.1x or PSK
Temporal Key Integrity Protocol (TKIP)(1)

- Should be implementable on existing WEP/RC4 HW with minimum additional efforts, SW encryption too slow for 802.11g and up
- Initialisation Vector
- No direct connection to RC4 key, IV
- 48 instead of 24 bits long
  - to reduce processing time split IV into hi and lo part
    - recalculate phase 1 only all 65536 packets
    - MAC address is part of IV key, i.e. key is different for different devices and same IV
    - IV is increased by 1 for each packets; repeated IVs (replay) are discarded
Temporal Key Integrity Protocol (2)

- Michael – Message Integrity Check (64 bits, 40 effective)
  - added to each packet before encryption
  - prevents attacker to falsify packets
- If > 2 Michael errors per minute
  - Abort communication
  - renegotiate keys after 1 min.

A. Arnold, Jenseits von WEP, Heise, c’t 21/2004, p. 214ff
WPA Key Exchange

Handshake
• Modern WLAN chip sets allow for 4 group keys for broadcasts and one individual session key per user
• Phase I: Pairwise Key Handshake
  – Nonce (Random Seq.) for key negotiation
• Phase II: Group Key Handshake
  – Group Key needed for broadcasts
  – Group Key is distributed from AP to Client using secure connection
• During Transmission AP and Client can initiate key renegotiation

A. Arnold, Jenseits von WEP, Heise, c't 21/2004, p. 214ff
### 4.5.3 802.11i/WPA2: AES

**WPA2**
- 802.11i was finalised in 2004; mandatory for WiFi devices since 2006
- Marketed as WPA2
- Predecessor WPA meanwhile also broken

**AES Encryption**
- The Advanced Encryption Standard (AES) is published by NIST as the successor to Data Encryption Standard (DES)
- Operation
  - 128-byte blocks of data (cleartext)
  - 128-, 192-, or 256-bit symmetric keys
- NIST estimates that a machine that can break 56-bit DES key in 1 second would take about 149 trillion years to crack a 128-bit AES key (unless someone is very lucky)
- Replaces RC4 – new hardware needed
802.11i/WPA2: AES-CCM

- AES-CCM – Advanced Encryption Standard – Counter with CBC-MAC
- Replaces RC4/TKIP
- Mandatory for 802.11n
- AES only needs one 128 bit key for ciphering & protection against falsification, i.e. no extra scheme like Michael required
- CCM is symmetric – both stations have same key
- Initialisation Vector (IV) 48 bits, increased with each packet
- Supports fast roaming by PMK (Pairwise Master Key) Caching
  – if station roams within limited number of APs, keys are cached to decrease delay caused by authentication
4.5.4 WPS: Wi-Fi Protected Setup

- introduced to simplify the process of key configuration between AP and mobile station in case of home use
  - Simplify configuration for unexperienced users
  - PIN available on a label on AP's enclosure is entered into mobile device
  - WPA2 encryption key is generated from PIN
  - Implemented as a series of EAP messages
  - Broken since December 2011; PIN can be recovered within a few hours using brute-force attacks
4.5.5 Other encryption layers

- WLAN encryption only secures the wireless link
- Using a VPN (e.g., IPsec, OpenVPN) above the WLAN provides the security present in the environment of the VPN server
- End-to-end encryption provides encryption until the terminal nodes (e.g., https)