IEEE 802.11
Wireless LAN
(wLan)
IEEE 802.11

Specified by IEEE 802 Committee for LAN/ MAN
Standards for Infrastructure Layers (OSI 1 and 2)

Extends Ethernet for wireless physical layer

Data rates

802.11 (1997) specified 1 or 2 Mbps (legacy)
802.11a (1999) specifies 6 to 54 Mbps
802.11b (1999) 5.5 Mbps and 11 Mbps (WiFi)
802.11g (2003) 54 Mbps (WiFi)
802.11n (2009) specifies up to 300 Mbps
<table>
<thead>
<tr>
<th>OSI Layer</th>
<th>IEEE 802 Layer</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Link Layer</strong></td>
<td>Logical Link Control (LLC)</td>
<td>Transmission reliability</td>
</tr>
<tr>
<td></td>
<td>Bridging</td>
<td>LAN-to-LAN frame forwarding</td>
</tr>
<tr>
<td></td>
<td>MAC Sublayer</td>
<td>Medium access, frame structure, physical addresses</td>
</tr>
<tr>
<td><strong>Physical Layer</strong></td>
<td>Convergence Sublayer</td>
<td>PHY-specific header</td>
</tr>
<tr>
<td></td>
<td>PHY</td>
<td>Bits: Electricity, Optics, Radio</td>
</tr>
</tbody>
</table>
Ethernet in IEEE 802 Model

<table>
<thead>
<tr>
<th>LLC</th>
<th>802.2 LLC frame for SEQ/ACK/Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridging</td>
<td>Ethernet bridge protocols (spanning tree, promiscuous, etc.)</td>
</tr>
<tr>
<td>MAC</td>
<td>Ethernet header/trailer fields and CSMA/CD access</td>
</tr>
<tr>
<td>Convergence</td>
<td>64 bit preamble for transceiver training</td>
</tr>
<tr>
<td>PHY</td>
<td>10/100/1000/10,000 Mbps</td>
</tr>
<tr>
<td></td>
<td>Baseband, wire cable or optical fiber</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Preamble</th>
<th>802.3 Header</th>
<th>802.2 Header</th>
<th>Data</th>
<th>Trailer</th>
</tr>
</thead>
</table>

- LLC PDU = MAC SDU
- MAC PDU
- Ethernet Frame

- 64 bit preamble for transceiver training
- 10/100/1000/10,000 Mbps
- Baseband, wire cable or optical fiber

- Ethernet bridge protocols (spanning tree, promiscuous, etc.)

- Ethernet header/trailer fields and CSMA/CD access

- 802.2 LLC frame for SEQ/ACK/Control
Wireless Issues in LANs

Mobility

Addressable unit is a mobile station (STA)
Dynamic topologies
Medium boundaries are neither absolute nor visible
Lack full connectivity — STAs may be "hidden"

Reliability

Medium less reliable than wired PHY
Time-varying and asymmetric propagation

Power management
IEEE 802.11 wLAN Architectures

Ad Hoc Mode

Simple Peer-To-Peer Mode (STA-to-STA)
Limited to local communication
No WAN access or hand-off
Authentication and Registration
Permitted but not required

Infrastructure Mode

Basic topology
Permits forwarding to wired LANs and WANs
All communication via central Access Point (AP)
Permits Authentication
Requires Registration

Extended topology
Permits hand-off among WLAN segments
**Ad Hoc Mode (Peer-To-Peer Mode)**

**Independent Basic Service Set (IBSS)**
- Any set of 802.11 STAs (wireless stations)
- No connection to a wired network
- Simple unmediated communication
  - STAs communicate directly with one another
  - Useful for quick set up
  - Authentication or Registration not required

**Multiple IBSSs are independent**
- No bridging
- No hand-off
Infrastructure Mode

Basic Service Set (BSS)

A set of wireless end stations (STA)

An Access Point (AP)

Connected to the wired network infrastructure
Acts as base station for the wireless network
All traffic flows through AP by Contention or Polling (CFP)

Stations must Associate with AP

Authentication
Registration
Infrastructure Mode

Extended Service Set (ESS)

Two or more BSSs
- Form single subnetwork (broadcast domain)
- Looks like one large BSS to LLC layer
- One Access Point (AP) in each BSS

BSSs connected via Distribution System (DS)
- DS is backbone network
- DS performs MAC-level transport of MAC SDUs
- DS implementation not specified in 802.11

Portal

Software gateway function in AP
- Bridges BSS to any non-802.11 DS protocol

DS services permit handoff
- Station moving from one BSS to another
- Requires coordination between APs
Defined Services in IEEE 802.11

Station Services (SS)
- Privacy
- Authentication
- Deauthentication
- MAC Service Data Unit (MSDU) Delivery

Distribution System Services (DSS)
- Association
- Reassociation
- Disassociation
- Distribution
- Integration
**802.11 Protocol Layers**

**PHY Dependent Sublayer**
- Transmission type
- Modulation scheme
- Data transmission rates

**Physical Layer Convergence Sublayer**
- PHY medium dependent
- Specifies header for PHY Dependent Sublayer

**MAC layer**
- Medium access

<table>
<thead>
<tr>
<th>Data Link Layer</th>
<th>LLC</th>
<th>Bridging</th>
<th>MAC</th>
<th>PHY</th>
<th>802.11</th>
<th>802.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Layer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>LLC frame for SEQ/ACK/Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Exchange of 802.2 PDUs</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CSMA/CA, MACA, CFP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>PHY-Dependent Convergence Sublayer</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>FHSS, DSSS, IR, Data rates</td>
</tr>
</tbody>
</table>
Station Services (SS) — 1

Privacy in wired LAN

Design assumes physical closure
Illegal access requires physical connection

Privacy in wLAN

Any 802.11 receiver in range can receive all frames
Wired Equivalent Privacy (WEP) algorithm
  Shared key encryption
  Not secure
  No worse than wire
Station Services (SS) — 2

Authentication

Station provides proof of identity to AP or STA
Method not specified in 802.11
Required before Association

Deauthentication

Terminate authentication of another station
Deauthentication invokes Disassociation

MAC Service Data Unit (MSDU) Delivery

End-to-end delivery of LLC packets
LLC packets (PDUs) are the SDUs of the MAC
Distribution System Services (DSS) — 1

**Association**

Station associates with one AP

Association provides STA/AP mapping to the DS

DS forwards to STA via unique AP association

**Reassociation**

Station moves from BSS to New BSS

Station associates with New AP in New BSS

**Disassociation**

New AP informs Old AP of Reassociation

Old AP terminates old association

APs may also disassociate all STAs (for maintenance)
Distribution System Services (DSS) — 2

**Distribution**

Delivery of packets to stations through DS

STA sends to source AP

Logically invokes DSS Distribution Service

DS passes frame to Destination AP

Destination AP passes frame to Destination STA

**Integration**

Portal services provided by DS

Source AP sends frame to Portal

Portal forwards to foreign (not 802.11) network
Synchronization

All STAs in BSS are synchronized to common clock

Timing Synchronization Function (TSF)

Synchronizes timers for all STAs in same BSS
STAs maintain a local TSF timer

Infrastructure networks

AP initializes its TSF timer independently
AP periodically transmits beacon frames with its TSF
Receiving STA accepts TSF timing

Independent BSS (IBSS)

Distributed algorithm among BSS members
Each STA in BSS transmits a beacon
Each STA adopts latest (largest) TSF
802.11 Physical Medium

Three Bit-Serial Transmission Bands

Infra Red (IR) Optical Transmission
2 km line-of-sight
20 meter omnidirectional

Point-to-Point Microwave Radio

Omnidirectional Radio
Industrial/Scientific/Medical (ISM) band
2.4 — 2.483 GHz
10 to 100 mW
Data Coding Schemes for 802.11

**Spread Spectrum techniques**
- Use more capacity than required minimum
- Increases error control and security

**Direct Sequence Spread Spectrum (DSSS)**
- Transmit $m$ bits for each data bit
- Data rate of $n$ bps $\Rightarrow$ transmission rate of $m \times n$ bps
- Similar to CDMA, but only one code is used

**Frequency Hopping Spread Spectrum (FHSS)**
- Radio transmit frequency jumps around
- Use $m$ frequencies of bandwidth $B$ $\Rightarrow$ bandwidth $m \times B$
- Stations must know how and when to jump
## Convergence Layer Frames

### Direct Sequence Spread Spectrum (DSSS)

DSSS Physical Layer Convergence Protocol (PLCP)

<table>
<thead>
<tr>
<th>PLCP preamble</th>
<th>PLCP header</th>
</tr>
</thead>
<tbody>
<tr>
<td>synch</td>
<td>signal</td>
</tr>
<tr>
<td>start frame delimiter</td>
<td>service</td>
</tr>
<tr>
<td>128</td>
<td>length</td>
</tr>
<tr>
<td>16</td>
<td>CRC</td>
</tr>
<tr>
<td>variable</td>
<td>PSDU</td>
</tr>
</tbody>
</table>

- **Preamble**: Receiver synchronization bits (like Ethernet)
- **Signal**: Data transmission rate
- **PSDU**: Physical-layer Service Data Unit (SDU)
  - Protocol Data Unit (PDU) of MAC layer
- **Length**: Length of PSDU
## Convergence Layer Frames

### Frequency Hopping Spread Spectrum (FHSS)

FHSS Physical Layer Convergence Protocol (PLCP)

<table>
<thead>
<tr>
<th>PLCP preamble</th>
<th>PLCP header</th>
<th>whitened PSDU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synch</td>
<td>start frame delimiter</td>
<td>PLW</td>
</tr>
<tr>
<td>80</td>
<td>16</td>
<td>12</td>
</tr>
</tbody>
</table>

**PLW**
PSDU Length Word

**PSF**
PLCP Signaling Field

**HEC**
Header Error Check

**Whitened**
Encoding scheme to smooth statistics of data

Encoding scheme to smooth statistics of data

Whitened

Header Error Check

PLCP Signaling Field

PSDU Length Word

Start frame delimiter

Sync
IEEE 802.11a-1999

Specifies new PHY entity in 5 GHz band

Orthogonal Frequency Division Multiplexing (OFDM)
  Advanced data coding method
  Permits higher transmission rates

Radio frequencies
  5.15–5.25, 5.25–5.35 GHz
  5.725–5.825 GHz

Data rates: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps
IEEE 802.11b-1999

Extends existing PHY in 2.4 GHz band (ISM)

Enhances 802.11 DSSS system

Provides 5.5 Mbps and 11 Mbps data rates

No change to PLCP frame structure
   Both PHYs can operate simultaneously in same BSS

Basis for WiFi products
New Enhancements to PHY

IEEE 802.11g-2003

- Extends existing PHY in 2.4 GHz band (ISM)
- Enhances 802.11 DSSS system
- Provides 6, 9, 12, 18, 24, 36, 48, and 54 Mbps data rates
- Minor changes to PLCP frame structure
- Both PHYs can operate simultaneously in same BSS

IEEE 802.11h-2003

- Extends existing PHY in 5 GHz band
- Provides Spectrum and Transmit Power management
MAC Layer Issues

Channel Allocation Method
- Contention (distributed control)
- Round Robin (deterministic)
- Polling (centralized control)

Collision Detection and Error Detection

Fragmentation

Addressing

Control and Management Frames
Hidden Node Problem

A transmits to B
C cannot receive from A — out of range
C is may interfere with A’s transmission
Exposed Node Problem

B transmits to A
C receives B’s transmission and is not free to start
C delays its transmission to D unnecessarily
Older MAC Schemes for wLAN

**Pure ALOHA protocol**
- Stations transmit at random
- Collisions occur when transmissions overlap
- Avoid collisions
  - Limit access to 18% duty cycle
  - Reach 36% duty cycle with slotted ALOHA

**Carrier Sense Multiple Access (CSMA)**
- ALOHA with carrier sense
- Stations do not transmit if radio medium is active

**Polling**
- Access Point polls STAs
- STAs only transmit after being polled
Channel Allocation Methods in IEEE 802.11

Distributed Control Function (DCF)
- Contention-based multiple access methods
- DCF based on CSMA/CA is mandatory
  Carrier Sense Multiple Access with Collision Avoidance
- DCF based on CSMA/CA with MACA is optional
  Multiple Access with Collision Avoidance

Point Control Function (PCF)
- Centralized Access Control (polling)
- PCF polling is optional
CSMA with Collision Avoidance (CSMA/CA)

**Carrier Sense Multiple Access (CSMA)**

- Stations listen for transmissions
- Do not transmit if carrier is detected
- Collision detection not possible
  - Hidden node problem
  - Antenna cannot receive while transmitter active

**Collision Avoidance (CA)**

- Non-persistent access
- Random backoff
Multiple Access with Collision Avoidance (MACA)

Channel set-up before data transmission

- RTS — Request To Send
- CTS — Clear To Send
- ACK — Acknowledgment of error-free transmission

Net Allocation Vector (NAV)

- Transmitted in RTS
- Predicted data transmission time

Improves behavior of Hidden Nodes and Exposed Nodes
Multiple Access with Collision Avoidance (MACA)

B sends 30-byte RTS (request to send) packet to C

- Includes a NAV for the data to be sent
- All stations in B’s range hear RTS

C responds with CTS (clear to send) packet to B

- Echoes NAV
- All stations in C’s range hear CTS

B in range of A but not D

- A receives RTS but not CTS
- A can transmit without interfering with B’s destination

C in range of B but not A

- D receives CTS but not RTS
- D waits data transmit time before transmitting
Priority Control in (DCF)

Interframe Space (IFS)
Idle time between frames

Three defined IFS lengths
- Short IFS (SIFS)
- Point-coordination IFS (PIFS)
- DCF IFS (DIFS)

Each node has definite IFS
- Waiting time before attempt to transmit
- Node with short IFS transmits before node with long IFS
- Defines effective priority
Point Control Function (PCF) — Polling

**Mobile Station**

- Does not initiate communication
- Waits to be polled
  - Receives data from Access Point
  - Sends data for other stations to Access Point

**Access Point**

- Polls stations according to schedule
- Sets up connection oriented channel
- Sends stored data from other Mobile Stations
Point Control Function (PCF) in IEEE 802.11

Polling by Point Controller (PC) in AP
Determines access for all stations
Scheduling is implementation dependent

Mixed Contention and PCF
Most transmission is contention-based
Periodic Contention-Free period (CFP)
  AP begins Point Control (polling)
  No contention/collision allowed

Contention-Free Period (CFP)
  CFP repetition interval — frequency of CFP
  AP initiates CFP with a beacon signal
PCF Sequence

**Point Controller (PC)**
Polling function in AP

**CF-Aware Node**
Station which can respond to polling

**Beacon Frame**
Indicates beginning of Contention Free Period (CFP) for polling

**CF-Poll**
PC polls a node for data

**CF-ACK**
Node indicates no more data to send

Data can be sent with a Poll or an ACK

**CF-END**
Indicates end of Contention Free Period (CFP) for polling
PCF Sequences

PC side
- Senses idle medium, waits PIFS
- Transmits beacon frame
- Waits SIFS
- Sends: CF-Poll (no data), data, or CF-Poll with data

CF-aware node side
- Receives CF-Poll (no data)
- Sends CF-ACK (no data), or CF-ACK (with data)

PC side can respond
- Send CF-ACK (no data), or CF-ACK (with data), or
  CF-ACK (no data) + CF-Poll (ACK and poll new node)

PC may end CFP with CF-End frame
Fragmentation

LLC can create long MPDUs (packets)

Convergence Sublayer fragments long MPDU

- Maximum length parameter
- Fragments transmitted sequentially
- Each fragment independently ACKed
Power Management States and Modes

Awake state: STA is fully powered

Doze state

- STA not able to transmit or receive
- Consumes very low power

Active mode (AM)

- STA in the Awake state
- STA may receive frames at any time
- CFP-aware STA must be active for CFP

Power Save mode (PS)

- STA listens for selected beacons
- Sends PS-Poll frames to AP (requesting buffered data)
- AP transmits response to PS-Poll (sends waiting frames)
State Transitions — 1

Power Save mode (PS)

STA in Doze state

STA enters Awake state

To receive selected beacons
To transmit
To send PS-Poll frames and wait for responses
For contention-free transmissions
State Transitions — 2

**STAs changing Power Management mode**
- Inform AP using Power Management bits
- In Frame Control field of transmitted frames

**AP transmission to STAs in power-save (PS) mode**
- No arbitrarily transmissions
- AP buffers MSDUs
- AP transmits them at designated times

**STAs that have buffered MSDUs within AP**
- Identified in a Traffic Indication Map (TIM)
- Are included as an element within all AP beacons
- STAs in PS mode periodically listen for beacons
- STA receives a TIM and knows AP has buffered data
- STA sends PS-poll and waits for response

**TIM identifies STAs with buffered traffic in AP**
- Information is coded in a partial virtual bitmap
# MAC Sublayer Frame Structure

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frame Control</td>
<td>Control flags</td>
</tr>
<tr>
<td>Duration/ID</td>
<td>Timing control</td>
</tr>
<tr>
<td>Addresses</td>
<td>Various MAC entities</td>
</tr>
<tr>
<td>Sequence Control</td>
<td>Sequence/Fragment number for error/flow control</td>
</tr>
<tr>
<td>Frame Body</td>
<td>0 or more data bytes (SDU)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frame Control</td>
<td>2 bytes</td>
</tr>
<tr>
<td>Duration/ID</td>
<td>2 bytes</td>
</tr>
<tr>
<td>Address 1</td>
<td>6 bytes</td>
</tr>
<tr>
<td>Address 2</td>
<td>6 bytes</td>
</tr>
<tr>
<td>Address 3</td>
<td>6 bytes</td>
</tr>
<tr>
<td>Sequence Control</td>
<td>2 bytes</td>
</tr>
<tr>
<td>Address 4</td>
<td>6 bytes</td>
</tr>
<tr>
<td>Frame Body</td>
<td>0-2312 bytes</td>
</tr>
<tr>
<td>FCS</td>
<td>4 bytes</td>
</tr>
</tbody>
</table>
# Frame Control

<table>
<thead>
<tr>
<th>Type and Subtype</th>
<th>Data, Control, Management with subtypes</th>
</tr>
</thead>
<tbody>
<tr>
<td>To DS/From DS</td>
<td>Access Point (AP) is destination/source</td>
</tr>
<tr>
<td>More Fragments</td>
<td>Part of fragmented LLC packet</td>
</tr>
<tr>
<td>Retry</td>
<td>Indicates re-transmission of bad packet</td>
</tr>
<tr>
<td>Power Management</td>
<td>STA alerts AP of its mode</td>
</tr>
<tr>
<td>More Data</td>
<td>AP alerts STA (in power-save mode) of buffered frames</td>
</tr>
<tr>
<td>WEP</td>
<td>Indicates WEP encrypted data</td>
</tr>
<tr>
<td>Order</td>
<td>Indicates Strictly Ordered service class</td>
</tr>
</tbody>
</table>

**Protocol Version**:
- 2 bits

**Type**:
- 2 bits

**Subtype**:
- 4 bits

**To DS**:
- 1 bit

**From DS**:
- 1 bit

**More Fragments**:
- 1 bit

**Retry**:
- 1 bit

**Power Management**:
- 1 bit

**More data**:
- 1 bit

**WEP**:
- 1 bit

**Order**:
- 1 bit
MAC Layer Address Fields

4 Address Fields

5 possible MAC entities:

- **BSSID**
  - BSS Identification Number
- **Source Address (SA)**
  - Station which initiated the message
- **Destination Address (DA)**
  - Final destination for the message
- **Transmitting Station Address (TA)**
  - Station sending the message on this hop
- **Receiving Station Address (RA)**
  - Destination for the message on this hop
# Address Field Definitions

<table>
<thead>
<tr>
<th>To DS</th>
<th>From DS</th>
<th>Address 1</th>
<th>Address 2</th>
<th>Address 3</th>
<th>Address 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>DA</td>
<td>SA</td>
<td>BSSID D</td>
<td>—</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>DA</td>
<td>BSSID D</td>
<td>SA</td>
<td>—</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>BSSID D</td>
<td>SA</td>
<td>DA</td>
<td>—</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>RA</td>
<td>TA</td>
<td>DA</td>
<td>SA</td>
</tr>
</tbody>
</table>

**Address 1**
- Immediate destination address

**Address 2**
- Immediate source address

**Address 3**
- Final destination or source when DS performs distribution

**Address 4**
- Source address for DS to DS messages (802.11 is also DS)
Addressing in an IBSS

<table>
<thead>
<tr>
<th>To DS</th>
<th>From DS</th>
<th>Address 1</th>
<th>Address 2</th>
<th>Address 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>DA</td>
<td>SA</td>
<td>BSSID</td>
</tr>
</tbody>
</table>

Independent Basic Service Set (IBSS)

- No Access Point (AP) and no DS
- Fields To DS and From DS are 0

- **Address 1**: Immediate destination address (DA)
- **Address 2**: Immediate source address (SA)
- **Address 3**: BSSID
  - Identifies Ad Hoc network
  - Prevents message from reaching outside IBSS
Data Addressing in a BSS

<table>
<thead>
<tr>
<th>To DS</th>
<th>From DS</th>
<th>Address 1</th>
<th>Address 2</th>
<th>Address 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>DA</td>
<td>BSSID</td>
<td>SA</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>BSSID</td>
<td>SA</td>
<td>DA</td>
</tr>
</tbody>
</table>

Basic Service Set (BSS)

All transmissions are sent To/From Access Point
To/From DS actually means To/From AP

<table>
<thead>
<tr>
<th>Address 1</th>
<th>Immediate destination address (DA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address 2</td>
<td>Immediate source address (SA)</td>
</tr>
<tr>
<td>Address 3</td>
<td>Final Destination or Source</td>
</tr>
</tbody>
</table>
# BSS Addressing Example

<table>
<thead>
<tr>
<th>To DS</th>
<th>From DS</th>
<th>Address 1</th>
<th>Address 2</th>
<th>Address 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>DA</td>
<td>BSSID</td>
<td>SA</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>BSSID</td>
<td>SA</td>
<td>DA</td>
</tr>
</tbody>
</table>

**Station A sends message to Station B via AP (BSSID)**

- **To DS = 0**
- **From DS = 1**

Address 1 = Station B  
Address 2 = BSSID  
Address 3 = Station A

Address 1 = BSSID  
Address 2 = Station A  
Address 3 = Station B
Control and Management Addressing in a BSS

<table>
<thead>
<tr>
<th>To DS</th>
<th>From DS</th>
<th>Address 1</th>
<th>Address 2</th>
<th>Address 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>DA</td>
<td>SA</td>
<td>BSSID</td>
</tr>
</tbody>
</table>

Control and Management messages in a BSS:

Only involve stations in the BSS and the AP
Are sent with To DS = From DS = 0
Either the Source or the Destination will be the AP (BSSID)
Address 3 included as an error check
## Addressing in an ESS

<table>
<thead>
<tr>
<th>To DS</th>
<th>From DS</th>
<th>Address 1</th>
<th>Address 2</th>
<th>Address 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>DA</td>
<td>BSSID D</td>
<td>SA</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>BSSID D</td>
<td>SA</td>
<td>DA</td>
</tr>
</tbody>
</table>

### Extended Service Set (ESS)

All transmissions are sent via an AP

To the stations, entire ESS looks like one BSS

Stations do not know if message passes via DS or not

<table>
<thead>
<tr>
<th>Address 1</th>
<th>Immediate destination address (DA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address 2</td>
<td>Immediate source address (SA)</td>
</tr>
<tr>
<td>Address 3</td>
<td>Final Destination or Source</td>
</tr>
</tbody>
</table>
ESS Addressing Example

<table>
<thead>
<tr>
<th>To DS</th>
<th>From DS</th>
<th>Address 1</th>
<th>Address 2</th>
<th>Address 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>DA</td>
<td>BSSID D</td>
<td>SA</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>BSSID D</td>
<td>SA</td>
<td>DA</td>
</tr>
</tbody>
</table>

Station A sends message to Station B via

AP1 (BSSID1) → DS → AP2 (BSSID2)

DS must forward Data, Sequence, SA, and DA

By some legal means
# 802.11 as Distribution System

<table>
<thead>
<tr>
<th>To DS</th>
<th>From DS</th>
<th>Address 1</th>
<th>Address 2</th>
<th>Address 3</th>
<th>Address 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>DA</td>
<td>BSSID D</td>
<td>SA</td>
<td>—</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>BSSID D</td>
<td>SA</td>
<td>DA</td>
<td>—</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>RA</td>
<td>TA</td>
<td>DA</td>
<td>SA</td>
</tr>
</tbody>
</table>

![Diagram showing the distribution system in 802.11]
## Duration/ID

<table>
<thead>
<tr>
<th>Bit 15</th>
<th>Bit 14</th>
<th>Bits 13–0</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0–32,767</td>
<td>0</td>
<td>Duration — Set in NAV</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>Transmitted During CFP</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1–16,383</td>
<td>Reserved</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>Reserved</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1–2,007</td>
<td>Association ID (AID) in PC-Poll frames</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2,008–16,383</td>
<td>Reserved</td>
</tr>
</tbody>
</table>

### Definitions

- **Duration**: Estimated packet transmission time (as sent in RTS)
- **CFP**: Used in Contention-Free Period
- **AID**: ID assigned to STA by AP during Association
Data Frame Types

**Type Data Frame includes these subtypes:**

- Data
- Data + CF-ACK
- Data + CF-Poll
- Data + CF-ACK + CF-Poll
- Null function (no data)
- CF-ACK (no data)
- CF-Poll (no data)
- CF-ACK + CF-Poll (no data)
Control Frame Types

Type Control Frame includes these subtypes:

- Request To Send (RTS)
- Clear To Send (CTS)
- Acknowledgment (ACK)
- Power Save (PS)-Poll
- Contention-Free (CF)-End
- CF-End + CF-ACK
Control Frame Structure

<table>
<thead>
<tr>
<th>Frame Control</th>
<th>Duration</th>
<th>RA</th>
<th>TA</th>
<th>FCS</th>
</tr>
</thead>
</table>

Frame Control

<table>
<thead>
<tr>
<th>Protocol Version</th>
<th>Type</th>
<th>Subtype</th>
<th>Power Management</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Frame Structure:

- **RTS Frame**
  - Frame Control
  - Duration
  - RA
  - TA
  - FCS

- **CTS Frame**
  - Frame Control
  - Duration
  - RA
  - FCS

- **ACK Frame**
  - Frame Control
  - Duration
  - RA
  - FCS

**RA** — Receiving Address

**TA** — Transmitting Address

**FCS** — Frame Check Sequence
Management Frame Types

**Type Management Frame includes these subtypes:**

- Authentication
- Deauthentication Association request
- Association response
- Disassociation
- Reassociation request
- Reassociation response
- Probe request
- Probe response
- Beacon
Management Frame Fields

<table>
<thead>
<tr>
<th>Frame Control</th>
<th>Duration</th>
<th>DA</th>
<th>SA</th>
<th>BSSID</th>
<th>Sequence Control</th>
<th>Frame Body</th>
<th>FCS</th>
</tr>
</thead>
</table>

**SA** — Source Address

**DA** — Destination Address

**Frame Body contains Information Elements**

Depend on management function

Parameters, identifications, status codes
## Beacon Frame Body

### Information Elements

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timestamp</td>
<td>Time at transmission</td>
</tr>
<tr>
<td>Beacon Interval</td>
<td>Time between beacons</td>
</tr>
<tr>
<td>Capability</td>
<td>System features</td>
</tr>
<tr>
<td>Information</td>
<td>Service Set Identity (ESS or IBSS)</td>
</tr>
<tr>
<td>SSI D</td>
<td>Service Set Identity (ESS or IBSS)</td>
</tr>
<tr>
<td>Supported Rates</td>
<td>Supported data rates</td>
</tr>
<tr>
<td>FH Parameter</td>
<td>When FHSS is used</td>
</tr>
<tr>
<td>Parameter Set</td>
<td>When DSSS is used</td>
</tr>
<tr>
<td>DS Parameter</td>
<td>When DSSS is used</td>
</tr>
<tr>
<td>Parameter Set</td>
<td>When a PCF is used</td>
</tr>
<tr>
<td>CF Parameter</td>
<td>When a PCF is used</td>
</tr>
<tr>
<td>Parameter Set</td>
<td>When Beacon is generated by a STA in an IBSS</td>
</tr>
<tr>
<td>TIM</td>
<td>Traffic Information Map — If the AP has</td>
</tr>
<tr>
<td></td>
<td>buffered data for a group of STAs</td>
</tr>
</tbody>
</table>

If the AP has buffered data for a group of STAs.
## Association Request Frame Body

### Information Elements

<table>
<thead>
<tr>
<th>Capability Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Listen Interval</td>
<td>How often STA wakes up to hear beacon</td>
</tr>
<tr>
<td>SSID</td>
<td></td>
</tr>
<tr>
<td>Supported Rates</td>
<td></td>
</tr>
</tbody>
</table>
Association Response Frame Body

Information Elements

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Capability Information</td>
<td></td>
</tr>
<tr>
<td>Status Code</td>
<td></td>
</tr>
<tr>
<td>Association ID (AID)</td>
<td>Identifies Station to AP</td>
</tr>
<tr>
<td>Supported Rates</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Status Code</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Successful</td>
</tr>
<tr>
<td>1</td>
<td>Unspecified Failure</td>
</tr>
<tr>
<td>2–9</td>
<td>Reserved</td>
</tr>
<tr>
<td>10</td>
<td>Cannot support all requested capabilities in the Capability Information field</td>
</tr>
<tr>
<td>11</td>
<td>Reassociation denied due to inability to confirm that association exists</td>
</tr>
<tr>
<td>12</td>
<td>Association denied due to reason outside the scope of this standard</td>
</tr>
<tr>
<td>13</td>
<td>Responding station does not support the specified authentication algorithm</td>
</tr>
<tr>
<td>14</td>
<td>Received an Authentication frame with authentication transaction sequence number out of expected sequence</td>
</tr>
<tr>
<td>15</td>
<td>Authentication rejected because of challenge failure</td>
</tr>
<tr>
<td>16</td>
<td>Authentication rejected due to timeout waiting for next frame in sequence</td>
</tr>
<tr>
<td>17</td>
<td>Association denied because AP is unable to handle additional associated stations</td>
</tr>
<tr>
<td>18</td>
<td>Association denied due to requesting station not supporting all of the data rates in the BSSBasicRateSet parameter</td>
</tr>
</tbody>
</table>
# Authentication Frame Body

## Information Elements

| Authentication Algorithm Number | Authentication algorithm number = 0: Open System  
Authentication algorithm number = 1: Shared Key  
All other values of authentication number are reserved. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Transaction</td>
<td>Indicates the current state of progress through a multistep transaction</td>
</tr>
<tr>
<td>Sequence Number</td>
<td></td>
</tr>
<tr>
<td>Status Code</td>
<td>Authentication Status or Reserved</td>
</tr>
<tr>
<td>Challenge Text</td>
<td>Only present in certain Shared Key systems</td>
</tr>
</tbody>
</table>
# Association Response Frame Body

## Information Elements

<table>
<thead>
<tr>
<th>Information Elements</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capability Information</td>
<td></td>
</tr>
<tr>
<td>Status Code</td>
<td></td>
</tr>
<tr>
<td>Association ID (AID)</td>
<td>Identifies Station to AP</td>
</tr>
<tr>
<td>Supported Rates</td>
<td></td>
</tr>
</tbody>
</table>

## Status Code Meaning

<table>
<thead>
<tr>
<th>Status Code</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Successful</td>
</tr>
<tr>
<td>1</td>
<td>Unspecified Failure</td>
</tr>
<tr>
<td>2–9</td>
<td>Reserved</td>
</tr>
<tr>
<td>10</td>
<td>Cannot support all requested capabilities in the Capability Information field</td>
</tr>
<tr>
<td>11</td>
<td>Reassociation denied due to inability to confirm that association exists</td>
</tr>
<tr>
<td>12</td>
<td>Association denied due to reason outside the scope of this standard</td>
</tr>
<tr>
<td>13</td>
<td>Responding station does not support the specified authentication algorithm</td>
</tr>
<tr>
<td>14</td>
<td>Received an Authentication frame with authentication transaction sequence number out of expected sequence</td>
</tr>
<tr>
<td>15</td>
<td>Authentication rejected because of challenge failure</td>
</tr>
<tr>
<td>16</td>
<td>Authentication rejected due to timeout waiting for next frame in sequence</td>
</tr>
<tr>
<td>17</td>
<td>Association denied because AP is unable to handle additional associated stations</td>
</tr>
<tr>
<td>18</td>
<td>Association denied due to requesting station not supporting all of the data rates in the BSSBasicRateSet parameter</td>
</tr>
</tbody>
</table>
Intel® PRO/Wireless 2011 LAN PC Card
## Intel® PRO/Wireless 2011 LAN PC Card

<table>
<thead>
<tr>
<th>Specifications</th>
<th>Intel® PRO/Wireless LAN PC Card</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NOTEBOOK SLOT TYPE</strong></td>
<td>Type II 16-bit PC card</td>
</tr>
<tr>
<td><strong>SOFTWARE DRIVERS</strong></td>
<td>Windows* 2000, 98, 95, NT*, Pocket PC and DOS; Linux*; Palm OS*</td>
</tr>
<tr>
<td><strong>DEVICE DRIVERS</strong></td>
<td>NDIS2, NDIS3, NDIS4, NDIS5 and ODI</td>
</tr>
<tr>
<td><strong>SOFTWARE UTILITIES</strong></td>
<td>Location profiles “My WLAN places”; Real-time signal strength/quality “NIC Utilities”; Diagnostic and Configuration “NIC Info”; Firmware upgrade “NIC Update”; Site Survey Tool</td>
</tr>
<tr>
<td><strong>NETWORK ARCHITECTURE TYPES</strong></td>
<td>Supports peer-to-peer networking and communication to wired networks via Access Points</td>
</tr>
<tr>
<td><strong>RANGE AT 1MBPS (TYPICAL)</strong></td>
<td>1500ft (460m) open environment; 300ft (90m) office environment</td>
</tr>
<tr>
<td><strong>RANGE AT 11MBPS (TYPICAL)</strong></td>
<td>400ft (120m) open environment; 100ft (30m) office environment</td>
</tr>
<tr>
<td><strong>ANTENNA</strong></td>
<td>Integrated internal diversity antenna</td>
</tr>
<tr>
<td><strong>LED INDICATORS</strong></td>
<td>Link status and link activity</td>
</tr>
<tr>
<td><strong>RECEIVE SENSITIVITY</strong></td>
<td>-87dBm @ 1Mbps; -85dBm @ 2Mbps; -84dBm @ 5.5Mbps - 81dBm @ 11Mbps</td>
</tr>
<tr>
<td><strong>MAX OUTPUT POWER</strong></td>
<td>Typical 18dBm; Minimum 14dBm</td>
</tr>
<tr>
<td><strong>POWER CONSUMPTION</strong></td>
<td>Transmit: 300mA typical (500mA max.); Receive: 170mA typical (300mA max.); Sleep: 10mA typical (25mA max.)</td>
</tr>
<tr>
<td><strong>SAFETY COMPLIANCE</strong></td>
<td>USA/Canada: UL1950/CSA 22.2; Europe: CE Marked</td>
</tr>
<tr>
<td><strong>DIMENSIONS</strong></td>
<td>Length: 111mm/4.37in; Width: 54mm/2.23in; Thickness: 5mm/.20in; Weight: 1.6oz/45.36g</td>
</tr>
</tbody>
</table>
Intel® PRO/Wireless 2010 LAN Access Point
# Intel® PRO/Wireless 2010 LAN Access Point

<table>
<thead>
<tr>
<th>SPECIFICATIONS</th>
<th>Intel® PRO/Wireless LAN Access Point</th>
</tr>
</thead>
<tbody>
<tr>
<td>STANDARDS CONFORMANCE</td>
<td>IEEE 802.11b High Rate, IEEE 802.3 (10BASE-T), 802.1H, 802.1d Spanning Tree, SNMP v2</td>
</tr>
<tr>
<td>LOCAL CONFIGURATION</td>
<td>Direct console port (serial EIA-232 DB-9 male)</td>
</tr>
<tr>
<td>REMOTE CONFIGURATION</td>
<td>HTTP, Telnet, SNMP, PPP, tFTP, and Intel feature to perform bulk configuration to many APs</td>
</tr>
<tr>
<td>AUTOMATIC CONFIGURATION</td>
<td>BOOTP and DHCP</td>
</tr>
<tr>
<td>MAXIMUM CLIENTS</td>
<td>256</td>
</tr>
<tr>
<td>MANAGEMENT FEATURES</td>
<td>Client Access Control via MAC address; Embedded HTTP Server SNMP traps; Multilevel passwords</td>
</tr>
<tr>
<td>DIAGNOSTIC CAPABILITIES</td>
<td>Event logging, data packet tracing, SNMP alarm generation, operating statistics; Protocol and bandwidth filters; Site Survey utility with signal strength logging</td>
</tr>
<tr>
<td>ROAMING SUPPORT</td>
<td>IEEE 802.11b High Rate compliant with Intel enhanced roaming features; Mobile IP</td>
</tr>
<tr>
<td>PERFORMANCE ENHANCEMENTS</td>
<td>Proxy ARP; Short preamble support; QoS Voice and Data Prioritization</td>
</tr>
<tr>
<td>SECURITY</td>
<td>64- or 128-bit Encryption; Access Control List; MD5 Member Authentication (Mobile IP)</td>
</tr>
<tr>
<td>RANGE AT 1MBPS (TYPICAL)</td>
<td>1500ft (460m) open environment; 300ft (90m) office environment</td>
</tr>
<tr>
<td>RANGE AT 11MBPS (TYPICAL)</td>
<td>400ft (120m) open environment; 100ft (30m) office environment</td>
</tr>
<tr>
<td>ANTENNA</td>
<td>Two 2.2dBi dipole antennas with diversity support; also supports specialty antennas</td>
</tr>
<tr>
<td>LED INDICATORS</td>
<td>Status, network activity, and RF activity</td>
</tr>
<tr>
<td>RECEIVE SENSITIVITY</td>
<td>-87dBm @ 1Mbps; -85dBm @ 2Mbps; -84dBm @ 5.5Mbps; -81dBm @ 11Mbps</td>
</tr>
<tr>
<td>MAX OUTPUT POWER</td>
<td>Typical 18dBm; Minimum 14dBm</td>
</tr>
<tr>
<td>POWER SUPPLY</td>
<td>Input: 85 to 270V AC; Output: 12V DC</td>
</tr>
<tr>
<td>POWER ENHANCEMENTS</td>
<td>Power over Ethernet option2 (eliminates need for AC power at AP location)</td>
</tr>
<tr>
<td>SAFETY COMPLIANCE</td>
<td>USA/Canada: UL1950/CSA 22.2; Europe: CE Marked</td>
</tr>
<tr>
<td>DIMENSIONS</td>
<td>Length: 15.24cm/6in; Width: 21.59mm/0.85in; Height: 4.45cm/1.75in; Weight (w/ power supply): 1lbs./0.454kg</td>
</tr>
<tr>
<td>HARDWARE SHIPPING CONFIGURATION</td>
<td>Access Point, two dipole antennas, one power supply, one country-specific power supply cord (three in &quot;EU&quot; SKU), mounting brackets, clips and screws</td>
</tr>
</tbody>
</table>
Infrastructure Network Configurations — 1

1. Setup Using a Single, Wired Client
Infrastructure Network Configurations — 2

Figure 2. Setup Using Multiple, Wired Clients
Infrastructure Network Configurations — 3

Installation example with multiple gateways
(one Intel Gateway in gateway/AP mode and other Intel Gateways in AP only mode)
Infrastructure Network Configurations — 4

Installation example with multiple Intel Gateways and T1 or other Internet connection (all Gateway’s in AP only mode)

Third Floor

Second Floor

First Floor

Desktop Wired Computer

Intel Gateway (AP Only Mode)

Desktop Wired Computer

Intel Gateway (AP Only Mode)

Desktop Wired Computer

ISP and the Internet

Laptop Wireless Computer

Router with T1 Connection

Hub

Desktop Wired Computer

Desktop Wired Computer

Laptop Wireless Computer

Desktop Wired Computer

Laptop Wireless Computer

Desktop Wired Computer
Wired Equivalent Privacy (WEP)

Protects users from casual eavesdropping
Implementation and use is optional in IEEE 802.11
WEP may be used without authentication

Key encryption algorithm
Short secret key
Longer public key

"Reasonably" strong
Requires effort to discover the secret key
Frequently changes public key

External key management service
Distributes secret keys
Not defined as part of WEP

May be implemented in either hardware or software
Definitions

<table>
<thead>
<tr>
<th>Encryption (E)</th>
<th>Disguising data to hide information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plaintext (P)</td>
<td>Data that is not enciphered (encrypted)</td>
</tr>
<tr>
<td>Ciphertext (C)</td>
<td>Data that is enciphered</td>
</tr>
<tr>
<td>Decryption (D)</td>
<td>Returning ciphertext to plaintext</td>
</tr>
<tr>
<td>Key Sequence (k)</td>
<td>Used in encryption operation</td>
</tr>
</tbody>
</table>

Encryption function $E$ maps $P$ to $C$
\[ E_k(P) = C \]

Decryption function $D$ maps $C$ to $P$
\[ D_k(C) = P \]

Symmetry: Same key for encryption and decryption
\[ D_k(E_k(P)) = P \]
Encryption and Decryption

Key Distribution System

Key Sequence

Plaintext → Encryption → Ciphertext 

Decryption → Original Plaintext

Key Sequence
WEP Encryption/Decryption Technique

Bitwise XOR of plaintext and pseudorandom key

\[ C = E_k (P) = P \oplus k \]

\[ P = D_k (C) = C \oplus k \]

**example:**

\[
\begin{array}{cccccccccc}
P &=& 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\
k &=& 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
C &=& P \text{ XOR } k &=& 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1
\end{array}
\]

\[
\begin{array}{cccccccccc}
C &=& 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\
k &=& 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
P &=& C \text{ XOR } k &=& 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1
\end{array}
\]
WEP Encryption and Decryption are Symmetric

\[ (a \oplus b) \oplus c = (\overline{ab} + \overline{ab}) \oplus c \]
\[ = (\overline{ab} + \overline{ab}) c + (\overline{ab} + \overline{ab}) \overline{c} \]
\[ = (\overline{ab})(\overline{ab}) c + (\overline{ab} + \overline{ab}) \overline{c} \]
\[ = (a + b)(\overline{a} + \overline{b}) c + (\overline{ab} + \overline{ab}) \overline{c} \]
\[ = abc + abc + \overline{abc} + \overline{abc} \]
\[ = \overline{abc} + \overline{abc} + abc + \overline{abc} \]
\[ = \overline{abc} + \overline{abc} + abc + \overline{abc} \]
\[ = (\overline{abc} + \overline{abc}) + a(b + c)(\overline{b} + \overline{c}) \]
\[ = (\overline{abc} + \overline{abc}) + a(\overline{bc})(b\overline{c}) \]
\[ = a \oplus (\overline{bc} + \overline{bc}) a(\overline{bc} + \overline{bc}) \]
\[ = a \oplus (b \oplus c) \]

\[ a \oplus a = (a\overline{a} + \overline{a}a) \equiv 0 \]

\[ a \oplus 0 = (a\overline{0} + \overline{a}0) \equiv a \]

\[ C = E_k (P) = P \oplus k \]
\[ P = D_k (C) = C \oplus k \]
\[ = (P \oplus k) \oplus k \]
\[ = P \oplus (k \oplus k) \]
\[ = P \oplus 0 \]
\[ = P \]
WEP Encryption/Decryption Procedure

**Plaintext**

- MAC Layer PDU (MPDU)
- CRC-32 Frame Check Sequence (FCS) on MPDU

**Key Sequence**

- Generated from Secret Key and Initialization Vector (IV)
- Key length is MPDU length + 4

**Transmission**

- Encrypted Plaintext
- Unencrypted Initialization Vector (IV)

**Receiver**

- Generates Key Sequence from Secret Key and IV
- Deciphers Plaintext and checks FCS for errors
WEP Encryption Algorithm

Secret Key distributed by some background process
Initialization Vector (IV) 24-bit suffix generated by transmitter

- IV may be changed as frequently as every MPDU
- IV transmitted unencrypted with message to receiver
  - Receiver needs IV to decrypt
  - IV provides no information about secret key

Seed

- 64-bit concatenation: Secret Key ## IV
- Seed input to Pseudo-Random Number Generator (PRNG)

Key Sequence k

- Pseudo-Random Number generated by PRNG using seed

Integrity Check Value (ICV)

- 32-bit CRC on MPDU

Plaintext (MPDU ## ICV) encrypted with Key Sequence
WEP Encryption Algorithm

Initialization Vector (IV) → Seed → WEP PRNG → Key Sequence k → Encryption → Ciphertext

Secret Key

Plaintext → Integrity Algorithm (32-bit CRC) → Integrity Check Value (ICV) → # #
WEP Decryption Algorithm

Key Sequence generated from IV and Secret Key

Decryption

- Key Sequence applied to Ciphertext
- Plaintext includes MPDU and ICV

Integrity check performed on Plaintext

- On error in received MPDU
  - Error indication is sent to MAC management
  - Data not passed to LLC
Problems with WEP Algorithm

XOR encryption is not very strong

Secret Key is too easy to deduce
Part of MPDU may be easy to guess
Example: IP header fields
Can find k from P and C

Encryption strength
Depends on lifetime of Initialization Vector (IV)
Best privacy when IV is changed for every MPDU
More Problems with WEP

**AP beacons**
Announce service availability
Can be found by unauthorized listeners

**WEP not always implemented**

**Weak encryption**
40-bit secret key
Simple XOR of key with plaintext

**Weak authentication**
STA requests service
AP sends random number
STA returns number encrypted with key (password)

**Authentication password is used as encryption key**
Eavesdropper can learn key from plaintext and encrypted number
WEP Encryption/Decryption Can Be Cracked

Authentication

STA requests association
AP sends Random Number $R$ as challenge text
STA encrypts $R$ with Secret Key $k$ as Ciphertext $C$
Same key is used for Encryption of traffic

Eavesdropper

Hears Random Number $R$
Hears Ciphertext $C$
Computes Secret Key $k$

\[
C = E_k (R) = R \oplus k
\]
\[
R = D_k (C) = C \oplus k
\]
\[
R \oplus C = R \oplus (R \oplus k)
\]
\[
= (R \oplus R) \oplus k
\]
\[
= k
\]
802.11i-2004 Improved wLAN Security

Recognizes problems with WEP
- Key protection vulnerability
- Weak authentication
- Weak encryption

802.11i Robust Security Network (RSN)
- Authentication and Encryption
  - Algorithms negotiated dynamically by APs and STAs
- Authentication
  - 802.1X and Extensible Authentication Protocol (EAP)
- Encryption
  - Advanced Encryption Standard (AES)

Wi-Fi Protected Access (WPA)
- Subset of 802.11i adopted by Wi-Fi Alliance
- Key Management — Temporal Key Integrity Protocol (TKIP)
- Authentication — Extensible Authentication Protocol (EAP)
- Encryption — Keeps WEP for hardware compatibility
802.11i Authentication

Implements 802.1X

Supplicant

STA requesting access to network

Authenticator

802.1x capable AP

Authentication server

Enterprise — RADIUS server
Non-enterprise — privately distributed keys

Controlled/ Uncontrolled Ports

Uncontrolled ports used for authentication exchange
Controlled ports after authentication

Authentication Message Exchange

IEEE 802.11i allows choice of authentication
WPA recommends Extensible Authentication Protocol (EAP)
Security Operations

Station

Access Point

Authentication Server

Security capabilities discovery

802.1X authentication

802.1X key management

Data protection

RADIUS-based key distribution
Problems in Extended Service Set (ESS)

ESS is a single broadcast domain
To STAs, entire ESS looks like one BSS

All transmissions are sent via an AP
Each STA must associate with one AP
STA may roam from BSS to BSS

802.11 does not specify mechanisms for:
Coordinating between APs
Forwarding 802.11 packets over DS

Example
STA A sends to STA B via AP1
AP1 must learn that STA B belongs to AP2
AP1 must locate AP2 via DS
AP1 must send information to AP2 over DS protocol
Station A sends message to Station B via: STA_A → bridge → STA_B

Routers do not forward 802.3 MAC layer fields

Routers use routing protocols and ARP to locate destination
802.11f Recommendation for DS in an ESS

No specification of DS implementation
- 802.11 frame forwarding not affected
- Operates in parallel to DS
- APs forward 802.11 frames via user-specified protocol

Specifies Inter-AP Access Protocol (IAPP)
- AP-to-AP mobility management protocol
- Integrates with existing AP management software
- Provides Service API to AP
- APs exchange information on associated STAs
- Enables AP1 to locate AP2 as gateway for STA B

Specifies TCP/IP for AP-to-AP coordination
- IAPP operates over TCP/IP stack
- IAPP does not specify 802.11 DS behavior
  - DS implementation may not be TCP/IP
  - TCP/IP must be available in AP
Overview of IAPP Protocol Stack

### IAPP Protocol Stack for AP-to-AP Signaling

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APME</td>
<td>AP Management Entity</td>
</tr>
<tr>
<td>IAPP</td>
<td>Inter-AP Protocol</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial-in User Service</td>
</tr>
<tr>
<td>ESP</td>
<td>IP Encapsulating Security Payload</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IAPP</td>
<td>AP control program (manages the AP)</td>
</tr>
<tr>
<td></td>
<td>Exchanges IAPP messages with other APs</td>
</tr>
<tr>
<td>RADIUS</td>
<td>IETF Authentication Database protocol</td>
</tr>
<tr>
<td></td>
<td>Manages authentication and encryption for users</td>
</tr>
<tr>
<td>ESP</td>
<td>Provides security services (authentication/encryption) for IP data</td>
</tr>
</tbody>
</table>
802.11f Definitions

802.11f defines transaction protocol between APs
Service primitives allow APME to invoke IAPP service functions

- APP frame structure and transfer via TCP or UDP
- Access to RADIUS for IP routing in DS

![Diagram](image-url)
802.11f Address Mapping

AP Addresses

802.11 traffic in BSS
- AP uses BSSID as MAC address
- AP may have some network address in BSS (or not)

IAPP traffic between APs
- AP uses IAPP IP address
- AP have some MAC address on IAPP (or not)
  - IAPP may operate on Ethernet, PPP, or other data link protocol

RADIUS server
- Authentication of APs for IAPP traffic
- Encryption keys for IAPP traffic between APs
- Database of BSSID (MAC addresses) to IP address for IAPP traffic
  - Allows APs to find IAPP address for a given BSSID

Without RADIUS server
- BSSID to IP mapping performed by Inverse ARP server
802.11f Basic Operations

STA associates with AP (802.11 procedure)
AP issues IAPP-ADD.request (802.11f procedure)

STA reassociates with new AP (802.11 procedure)
AP issues IAPP-MOVE.request (802.11f procedure)
AP issues IAPP-CACHE.request (802.11f procedure)
STA requests association from AP
AP Management Entity (APME) sends IAPP-ADD.request to IAPP layer
IAPP layer sends association message to all APs
All APs on IAPP network receive IAPP-ADD.notify message

In each AP

IAPP layer sends IAPP-ADD.notify message to APME

Contains

- BSS MAC address of Associating STA
- SEQ of Association request on BSS

All APs remove STA from location tables

Associated AP sends broadcast message from Associating STA

All DS nodes learn that STA is associated with AP
In Associated AP, IAPP sends IAPP-ADD.confirm message to APME

APME adds STA to its association list

AP sends 802.11 Association Confirm message to STA
## IAPP ADD Move

<table>
<thead>
<tr>
<th>New APME</th>
<th>IAPP</th>
<th>Old IAPP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IAPP-MOVE.request</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IAPP-MOVE.announce</td>
<td>IAPP-MOVE.notify</td>
</tr>
<tr>
<td></td>
<td>→</td>
<td>→</td>
</tr>
<tr>
<td>IAPP-MOVE.confirm</td>
<td>Security information</td>
<td>Security information</td>
</tr>
<tr>
<td></td>
<td>←</td>
<td>←</td>
</tr>
</tbody>
</table>

Security information — keys for previous transfers between **STA** and **Old AP**
**IAPP-CACHE.request**

AP receives IAPP-cache.request

AP provides STA Context to all APs within one-hop

Used to speed up roaming and hand-off

Usually a STA will roam from a BSS to a neighbor BSS
802.11 Frame Forwarding Over DS

Station A sends message to Station B via:

\[
\text{STA}_A \rightarrow \text{AP1 (BSSID1)} \rightarrow \text{DS} \rightarrow \text{AP2 (BSSID2)} \rightarrow \text{STA}_B
\]

DS forwards Data, Sequence, SA, and DA fields

From AP1 to AP2

By some legal means (not specified in 802.11)
 Choices for Implementing DS

Proprietary protocol

Some communications protocol runs between AP1 and AP2
AP1 accepts 802.11 frame from STA A
DS function in AP1 provides AP2 with information from the 802.11 frame
AP2 builds a 802.11 frame for STA B

Tunneling protocol

APs running 802.11f

Connected by TCP/IP network
Know BSSID and IP address of Associated AP for each STA MAC
AP can tunnel (encapsulate) complete 802.11 frames to AP2 as IP SDU
**Possible STA-to-STA Forwarding Over DS**

<table>
<thead>
<tr>
<th>Application</th>
<th>Transport</th>
<th>Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11 Data Link</td>
<td>IP</td>
<td>TCP/ESP</td>
</tr>
<tr>
<td>802.11 PHY</td>
<td>DS Data Link</td>
<td>IP</td>
</tr>
<tr>
<td>STA</td>
<td>DS PHY</td>
<td>DS PHY</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application</th>
<th>Transport</th>
<th>Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11 Data Link</td>
<td>IP</td>
<td>TCP/ESP</td>
</tr>
<tr>
<td>802.11 PHY</td>
<td>DS Data Link</td>
<td>IP</td>
</tr>
<tr>
<td>AP</td>
<td>DS PHY</td>
<td>DS PHY</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application</th>
<th>Transport</th>
<th>Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11 Data Link</td>
<td>IP</td>
<td>TCP/ESP</td>
</tr>
<tr>
<td>802.11 PHY</td>
<td>DS Data Link</td>
<td>IP</td>
</tr>
<tr>
<td>DS</td>
<td>DS PHY</td>
<td>DS PHY</td>
</tr>
</tbody>
</table>

**IEEE 802.11f IAPP requires TCP/IP functionality in DS**

APs use TCP/IP or UDP/IP for IAPP signaling

TCP/IP protocols available in DS

Likely that APs will use TCP/IP to tunnel 802.11 STA frames

“Leverages” TCP/IP capability

Not the only possibility

Not discussed in 802.11f