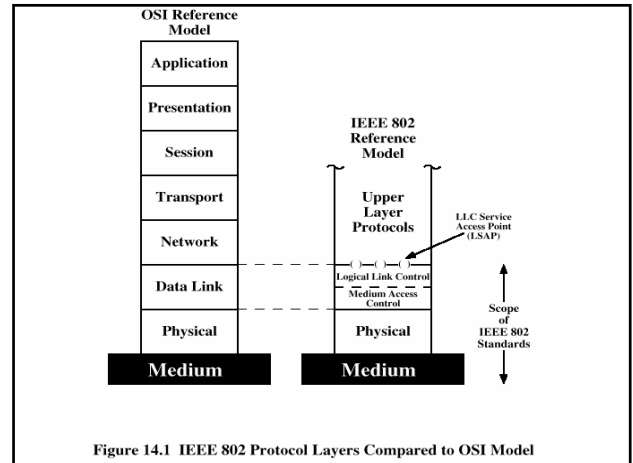


IEEE 802.11 Wireless LAN Standard

Chapter 14



Protocol Architecture

- Functions of physical layer:
 - Encoding/decoding of signals
 - Preamble generation/removal (for synchronization)
 - Bit transmission/reception
 - Includes specification of the transmission medium

Protocol Architecture

- Functions of medium access control (MAC) layer:
 - On transmission, assemble data into a frame with address and error detection fields
 - On reception, disassemble frame and perform address recognition and error detection
 - Govern access to the LAN transmission medium
- Functions of logical link control (LLC) Layer:
 - Provide an interface to higher layers and perform flow and error control

Separation of LLC and MAC

- The logic required to manage access to a shared-access medium not found in traditional layer 2 data link control
- For the same LLC, several MAC options may be provided

MAC Frame Format

- MAC control
 - Contains Mac protocol information
- Destination MAC address
 - Destination physical attachment point
- Source MAC address
 - Source physical attachment point
- CRC
 - Cyclic redundancy check

Logical Link Control

- Characteristics of LLC not shared by other control protocols:
 - Must support multiaccess, shared-medium nature of the link
 - Relieved of some details of link access by MAC layer

LLC Services

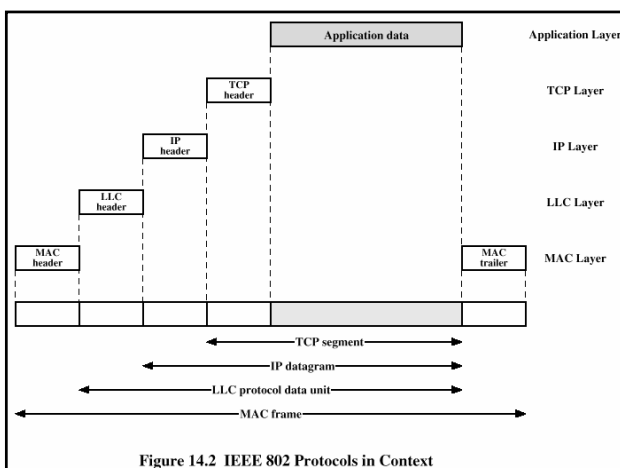
- Unacknowledged connectionless service
 - No flow- and error-control mechanisms
 - Data delivery not guaranteed
- Connection-mode service
 - Logical connection set up between two users
 - Flow- and error-control provided
- Acknowledged connectionless service
 - Cross between previous two
 - Datagrams acknowledged
 - No prior logical setup

Differences between LLC and HDLC

- LLC uses asynchronous balanced mode of operation of HDLC (type 2 operation)
- LLC supports unacknowledged connectionless service (type 1 operation)
- LLC supports acknowledged connectionless service (type 3 operation)
- LLC permits multiplexing by the use of LLC service access points (LSAPs)

IEEE 802.11 Architecture

- Distribution system (DS)
- Access point (AP)
- Basic service set (BSS)
 - Stations competing for access to shared wireless medium
 - Isolated or connected to backbone DS through AP
- Extended service set (ESS)
 - Two or more basic service sets interconnected by DS



Distribution of Messages Within a DS

- Distribution service
 - Used to exchange MAC frames from station in one BSS to station in another BSS
- Integration service
 - Transfer of data between station on IEEE 802.11 LAN and station on integrated IEEE 802.x LAN

Transition Types Based On Mobility

- No transition
 - Stationary or moves only within BSS
- BSS transition
 - Station moving from one BSS to another BSS in same ESS
- ESS transition
 - Station moving from BSS in one ESS to BSS within another ESS

Association-Related Services

- Association
 - Establishes initial association between station and AP
- Reassociation
 - Enables transfer of association from one AP to another, allowing station to move from one BSS to another
- Disassociation
 - Association termination notice from station or AP

Access and Privacy Services

- Authentication
 - Establishes identity of stations to each other
- Deauthentication
 - Invoked when existing authentication is terminated
- Privacy
 - Prevents message contents from being read by unintended recipient

IEEE 802.11 Medium Access Control

- MAC layer covers three functional areas:
 - Reliable data delivery
 - Access control
 - Security

Reliable Data Delivery

- More efficient to deal with errors at the MAC level than higher layer (such as TCP)
- Frame exchange protocol
 - Source station transmits data
 - Destination responds with acknowledgment (ACK)
 - If source doesn't receive ACK, it retransmits frame
- Four frame exchange
 - Source issues request to send (RTS)
 - Destination responds with clear to send (CTS)
 - Source transmits data
 - Destination responds with ACK

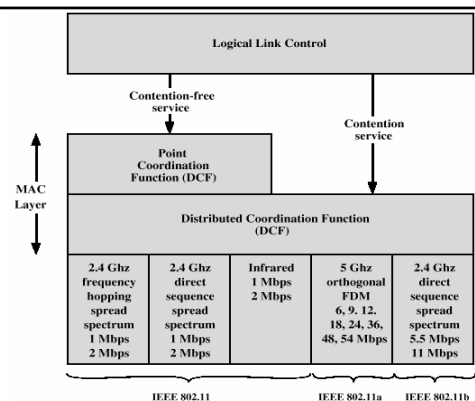


Figure 14.5 IEEE 802.11 Protocol Architecture

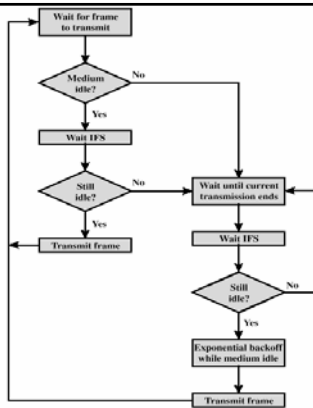


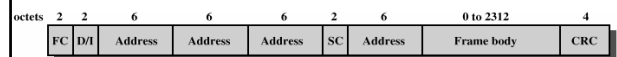
Figure 14.6 IEEE 802.11 Medium Access Control Logic

Interframe Space (IFS) Values

- Short IFS (SIFS)
 - Shortest IFS
 - Used for immediate response actions
- Point coordination function IFS (PIFS)
 - Midlength IFS
 - Used by centralized controller in PCF scheme when using polls
- Distributed coordination function IFS (DIFS)
 - Longest IFS
 - Used as minimum delay of asynchronous frames contending for access

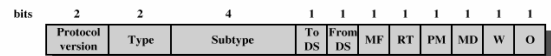
IFS Usage

- SIFS
 - Acknowledgment (ACK)
 - Clear to send (CTS)
 - Poll response
- PIFS
 - Used by centralized controller in issuing polls
 - Takes precedence over normal contention traffic
- DIFS
 - Used for all ordinary asynchronous traffic



FC = Frame control
D/I = Duration/Connection ID
SC = Sequence control

(a) MAC frame



DS = Distribution system
MF = More fragments
RT = Retry
PM = Power management
MD = More data
W = Wired equivalent privacy bit
O = Order

(b) Frame control field

Figure 14.8 IEEE 802.11 MAC Frame Format

MAC Frame Fields

- Frame Control – frame type, control information
- Duration/connection ID – channel allocation time
- Addresses – context dependant, types include source and destination
- Sequence control – numbering and reassembly
- Frame body – MSDU or fragment of MSDU
- Frame check sequence – 32-bit CRC

Frame Control Fields

- Protocol version – 802.11 version
- Type – control, management, or data
- Subtype – identifies function of frame
- To DS – 1 if destined for DS
- From DS – 1 if leaving DS
- More fragments – 1 if fragments follow
- Retry – 1 if retransmission of previous frame

Frame Control Fields

- Power management – 1 if transmitting station is in sleep mode
- More data – Indicates that station has more data to send
- WEP – 1 if wired equivalent protocol is implemented
- Order – 1 if any data frame is sent using the Strictly Ordered service

Control Frame Subtypes

- Power save – poll (PS-Poll)
- Request to send (RTS)
- Clear to send (CTS)
- Acknowledgment
- Contention-free (CF)-end
- CF-end + CF-ack

Data Frame Subtypes

- Data-carrying frames
 - Data
 - Data + CF-Ack
 - Data + CF-Poll
 - Data + CF-Ack + CF-Poll
- Other subtypes (don't carry user data)
 - Null Function
 - CF-Ack
 - CF-Poll
 - CF-Ack + CF-Poll

Management Frame Subtypes

- Association request
- Association response
- Reassociation request
- Reassociation response
- Probe request
- Probe response
- Beacon

Management Frame Subtypes

- Announcement traffic indication message
- Dissociation
- Authentication
- Deauthentication

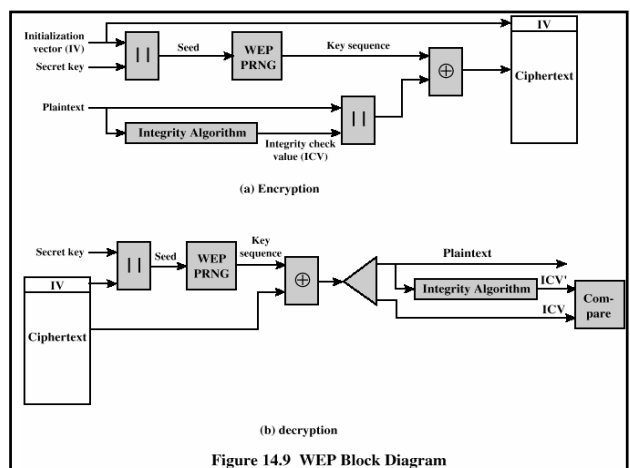


Figure 14.9 WEP Block Diagram



Authentication

- Open system authentication
 - Exchange of identities, no security benefits
- Shared Key authentication
 - Shared Key assures authentication



Physical Media Defined by Original 802.11 Standard

- Direct-sequence spread spectrum
 - Operating in 2.4 GHz ISM band
 - Data rates of 1 and 2 Mbps
- Frequency-hopping spread spectrum
 - Operating in 2.4 GHz ISM band
 - Data rates of 1 and 2 Mbps
- Infrared
 - 1 and 2 Mbps
 - Wavelength between 850 and 950 nm



IEEE 802.11a and IEEE 802.11b

- IEEE 802.11a
 - Makes use of 5-GHz band
 - Provides rates of 6, 9, 12, 18, 24, 36, 48, 54 Mbps
 - Uses orthogonal frequency division multiplexing (OFDM)
 - Subcarrier modulated using BPSK, QPSK, 16-QAM or 64-QAM
- IEEE 802.11b
 - Provides data rates of 5.5 and 11 Mbps
 - Complementary code keying (CCK) modulation scheme