Wireless LANs
2014

IEEE 802.11 Overview (1)

รศ. ดร. อนันต์ ผลเพิ่ม

Assoc. Prof. Anan Phonphoem, Ph.D.

anan.p@ku.ac.th

Intelligent Wireless Network Group (IWING Lab)

http://iwing.cpe.ku.ac.th

Computer Engineering Department

Kasetsart University, Bangkok, Thailand

Outline

- IEEE 802 Standards
- IEEE 802.11 Overview
- IEEE 802.11 Services
- History and present of IEEE 802.11

Why Wireless LAN not so popular in the past?

- Low data rate
- High price
- Lack of standard
  - Proprietary products

Types of Standards

- Official Standard
  - Controlled by an official standard organization
  - E.g. IEEE
- Public Standard
  - Controlled by a private organization
  - E.g. Wireless LAN Interoperability Forum
  - Called “De Facto Standard”

Why Std. is so important?

- Interoperability
  - Multiple-vendor products
- Fast product development
  - Well-tested blueprint
- Stable for migration
  - IEEE 802.3 → 10 → 100/1000 Mbps
  - IEEE 802.11b → 802.11g → 802.11n
- Price Reduction
  - Low research & development budget
  - Increase price competition
- Easy to manage

IEEE

- **I**nstitute for **E**lectrical and **E**lectronic **E**ngineers
- Nonprofit organization
- Publication, conferences, accreditation, standard developments
- Based in the US. → 150 countries

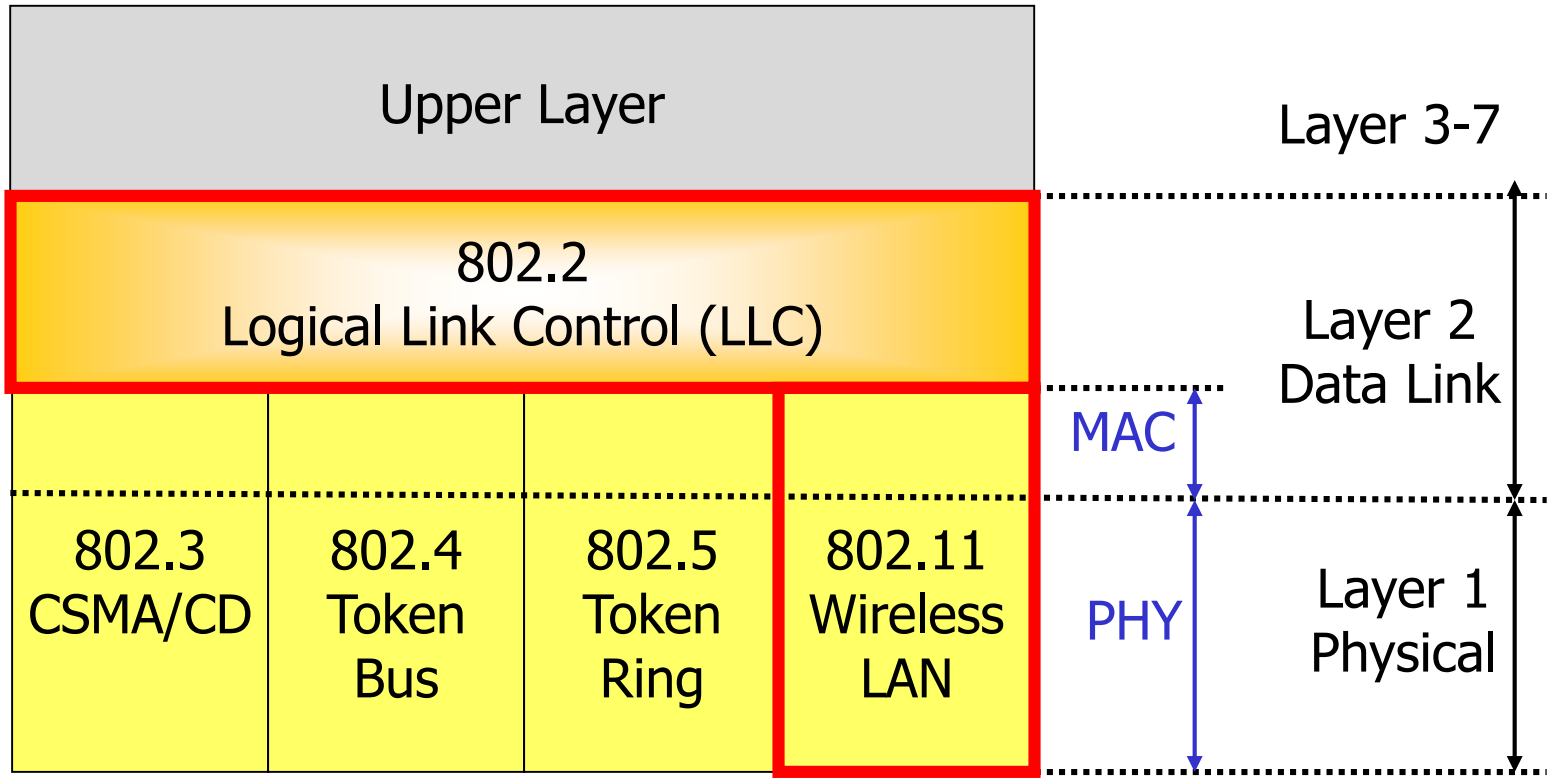
IEEE 802 LAN Std. Family

802	Overview and Architecture
802.1	Network Management
~~802.2~~	~~Logical Link Control (LLC)~~
802.3	CSMA/CD - Ethernet
1802.3	Conformance Test Methodology for IEEE 802.3
~~802.4~~	~~Token Passing Bus~~
~~802.5~~	~~Token Ring~~
~~802.6~~	~~Metropolitan Area~~ Network (MAN) : DQDB

~~802.7~~	~~Broadband LAN~~
~~802.8~~	~~Fiber Optic~~
~~802.9~~	~~Isochonous LAN~~
~~802.10~~	~~Integrated Service~~ Security
802.11	Wireless LAN
~~802.12~~	~~Demand Priority 100BaseVG~~
802.15	Wireless PAN
802.16	Broadband Wireless Access (Wireless MAN)
802.17	Resilient Packet Ring
802.21	Media Independent Handoff

~~Disbanded / Inactive~~

IEEE 802 LAN Std. Family

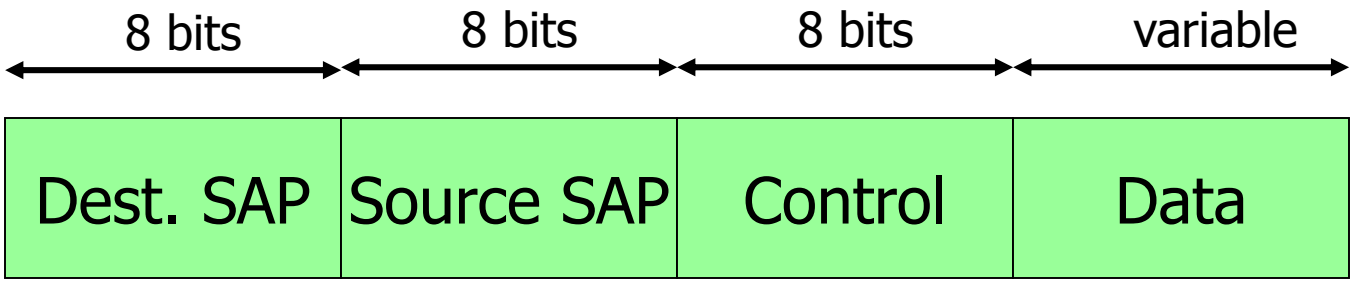


IEEE 802.2 LLC

- Data link control protocol
- Exchange data between end users across LAN using a 802-based MAC
- Independent
  - Network topology
  - Transmission medium
  - MAC

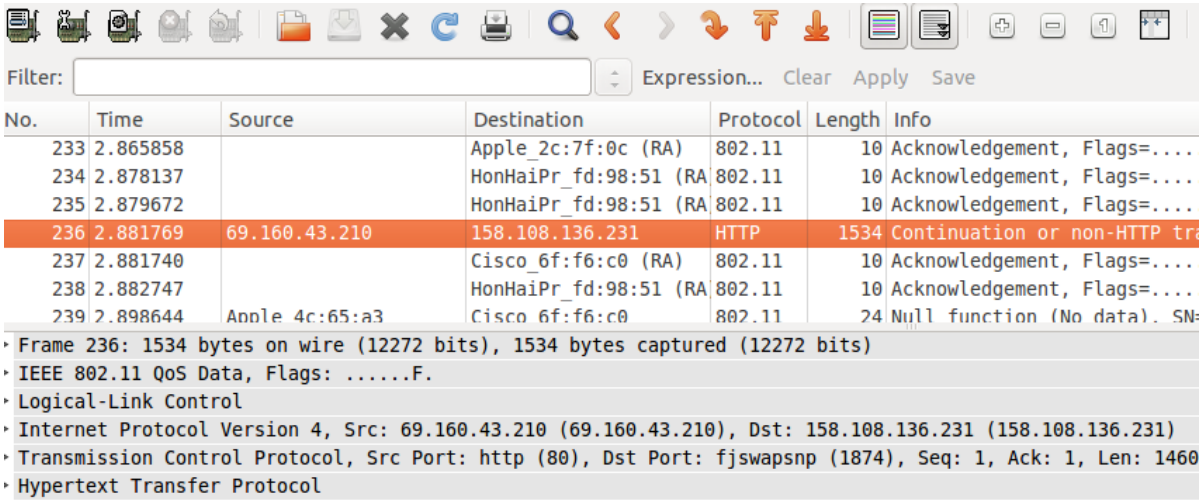
IEEE 802.2 LLC services

- Unacknowledged Connectionless
- Connection-oriented
- Acknowledged Connectionless



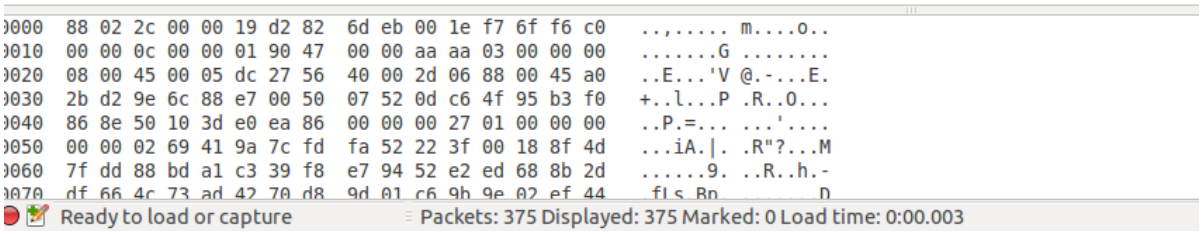
LLC Protocol Data Unit (PDU)

Example I

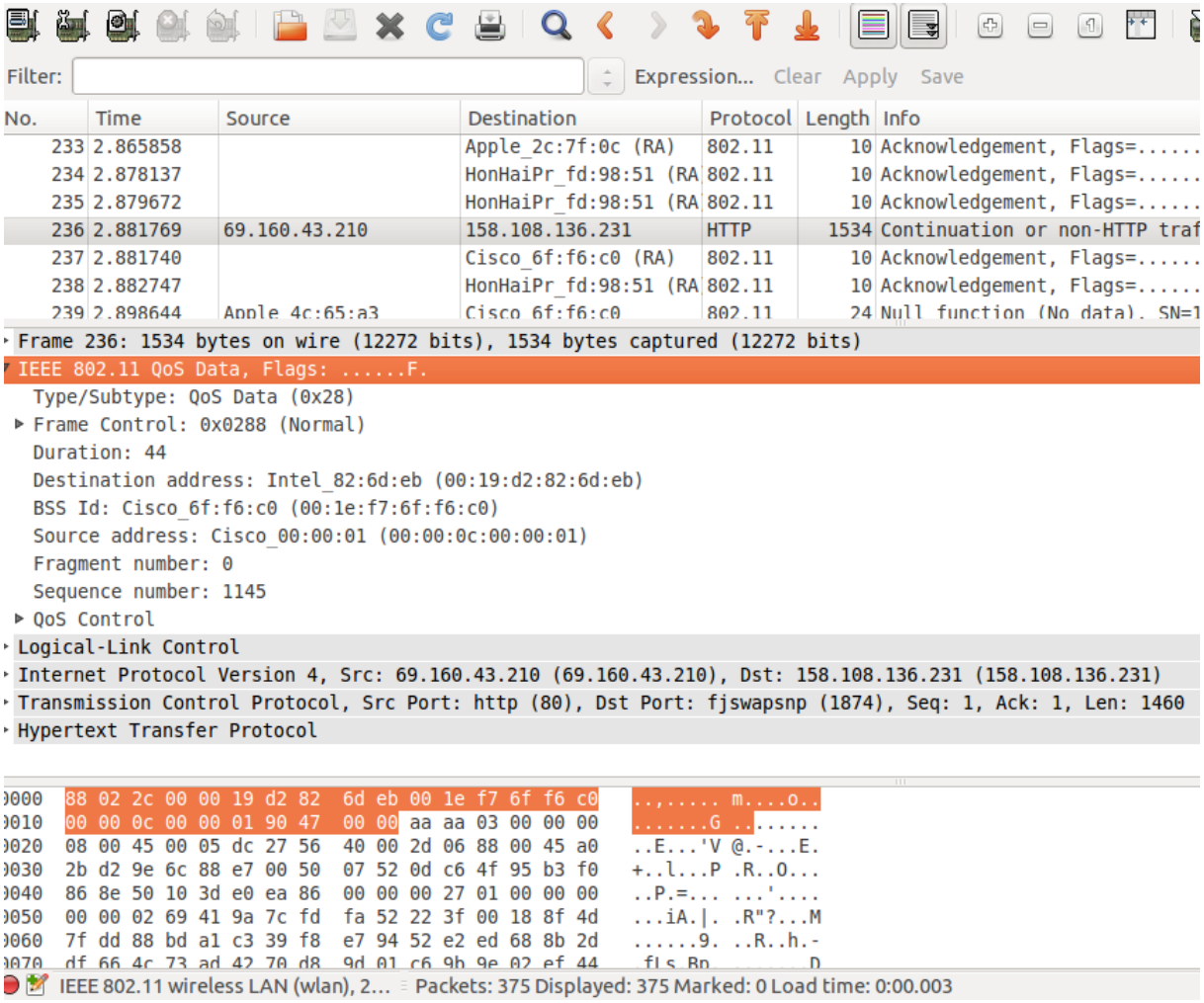


Note:

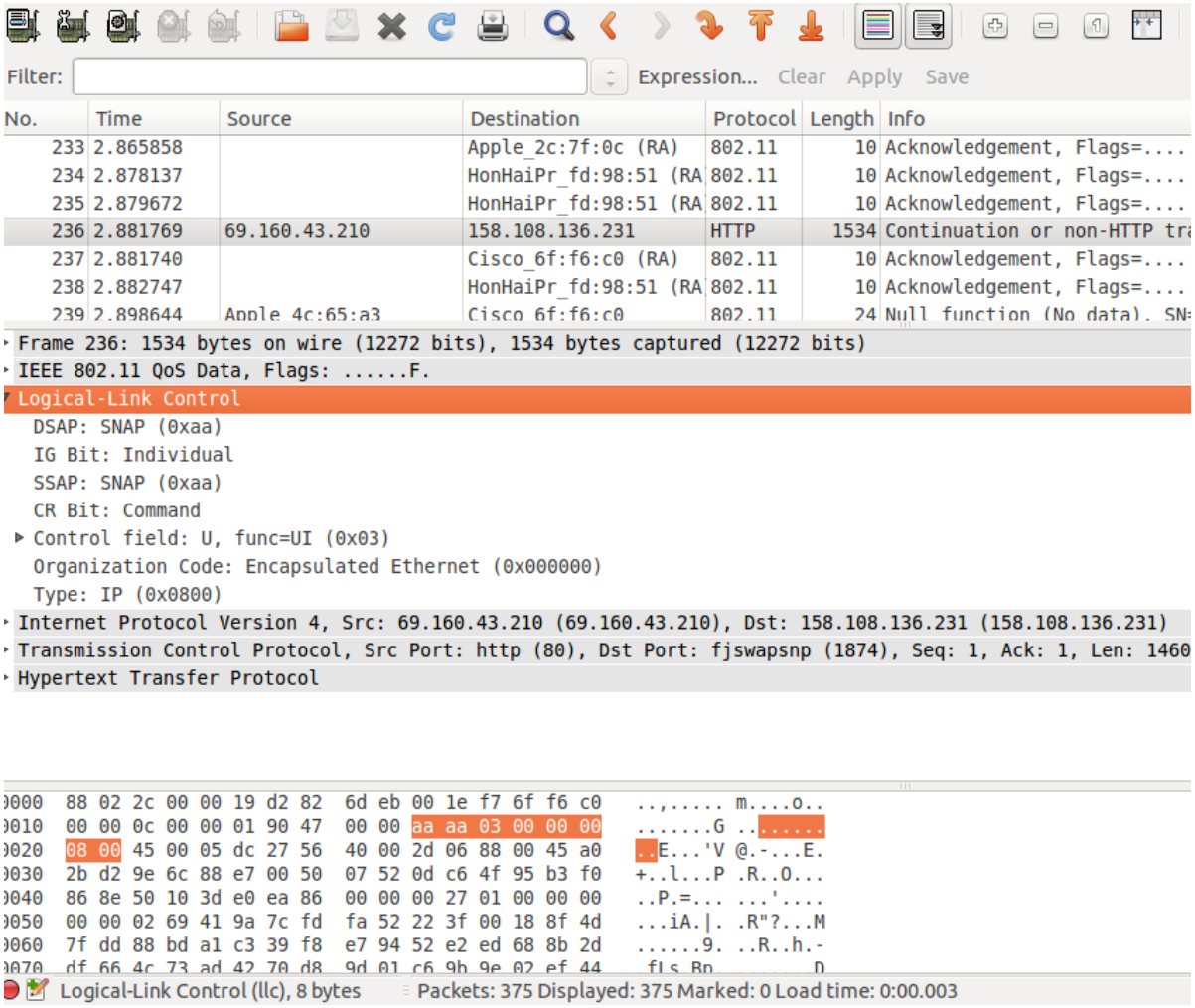
1. turn off Network manager (top right of the screen)
2. Use airmon-ng to change to promiscuous mode → create mon0
3. Use airrodump-ng to capture and write to file
4. Open file with Wireshark



Example II


Filter:
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
233 2.865858 Apple_2c:7f:0c (RA) 802.11 10 Acknowledgement, Flags=.....
234 2.878137 HonHaiPr_fd:98:51 (RA 802.11 10 Acknowledgement, Flags=.....
235 2.879672 HonHaiPr_fd:98:51 (RA 802.11 10 Acknowledgement, Flags=.....
236 2.881769 69.160.43.210 158.108.136.231 HTTP 1534 Continuation or non-HTTP traf
237 2.881740 Cisco_6f:f6:c0 (RA) 802.11 10 Acknowledgement, Flags=.....
238 2.882747 HonHaiPr_fd:98:51 (RA 802.11 10 Acknowledgement, Flags=.....
239 2.898644 Apple_4c:65:a3 Cisco_6f:f6:c0 802.11 24 Null function (No data), SN=1
Frame 236: 1534 bytes on wire (12272 bits), 1534 bytes captured (12272 bits)
IEEE 802.11 QoS Data, Flags: .....F.
Type/Subtype: QoS Data (0x28)
Frame Control: 0x0288 (Normal)
Duration: 44
Destination address: Intel_82:6d:eb (00:19:d2:82:6d:eb)
BSS Id: Cisco_6f:f6:c0 (00:1e:f7:6f:f6:c0)
Source address: Cisco_00:00:01 (00:00:0c:00:00:01)
Fragment number: 0
Sequence number: 1145
QoS Control
Logical-Link Control
Internet Protocol Version 4, Src: 69.160.43.210 (69.160.43.210), Dst: 158.108.136.231 (158.108.136.231)
Transmission Control Protocol, Src Port: http (80), Dst Port: fjswapsnp (1874), Seq: 1, Ack: 1, Len: 1460
Hypertext Transfer Protocol
0000 88 02 2c 00 00 19 d2 82 6d eb 00 1e f7 6f f6 c0 ..,..... m....o..
0010 00 00 0c 00 00 01 90 47 00 00 aa aa 03 00 00 00 ....G ....
0020 08 00 45 00 05 dc 27 56 40 00 2d 06 88 00 45 a0 ..E...'V @.-...E.
0030 2b d2 9e 6c 88 e7 00 50 07 52 0d c6 4f 95 b3 f0 +..l...P .R..O...
0040 86 8e 50 10 3d e0 ea 86 00 00 00 27 01 00 00 00 ..P.=... ...'....
0050 00 00 02 69 41 9a 7c fd fa 52 22 3f 00 18 8f 4d ...iA.|. .R"?...M
0060 7f dd 88 bd a1 c3 39 f8 e7 94 52 e2 ed 68 8b 2d ......9. ..R..h.-
IEEE 802.11 wireless LAN (wlan), 2... Packets: 375 Displayed: 375 Marked: 0 Load time: 0:00.003

Example III


Filter:
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
233 2.865858 Apple_2c:7f:0c (RA) 802.11 10 Acknowledgement, Flags=....
234 2.878137 HonHaiPr_fd:98:51 (RA 802.11 10 Acknowledgement, Flags=....
235 2.879672 HonHaiPr_fd:98:51 (RA 802.11 10 Acknowledgement, Flags=....
236 2.881769 69.160.43.210 158.108.136.231 HTTP 1534 Continuation or non-HTTP tra
237 2.881740 Cisco_6f:f6:c0 (RA) 802.11 10 Acknowledgement, Flags=....
238 2.882747 HonHaiPr_fd:98:51 (RA 802.11 10 Acknowledgement, Flags=....
239 2.898644 Apple_4c:65:a3 Cisco_6f:f6:c0 802.11 24 Null function (No data), SN=
Frame 236: 1534 bytes on wire (12272 bits), 1534 bytes captured (12272 bits)
IEEE 802.11 QoS Data, Flags: ......F.
Logical-Link Control
DSAP: SNAP (0xaa)
IG Bit: Individual
SSAP: SNAP (0xaa)
CR Bit: Command
Control field: U, func=UI (0x03)
Organization Code: Encapsulated Ethernet (0x000000)
Type: IP (0x0800)
Internet Protocol Version 4, Src: 69.160.43.210 (69.160.43.210), Dst: 158.108.136.231 (158.108.136.231)
Transmission Control Protocol, Src Port: http (80), Dst Port: fjswapsnp (1874), Seq: 1, Ack: 1, Len: 1460
Hypertext Transfer Protocol
0000 88 02 2c 00 00 19 d2 82 6d eb 00 1e f7 6f f6 c0 ..,..... m....o..
0010 00 00 0c 00 00 01 90 47 00 00 aa aa 03 00 00 00 ....G ....
0020 08 00 45 00 05 dc 27 56 40 00 2d 06 88 00 45 a0 ..E...'V @.-...E.
0030 2b d2 9e 6c 88 e7 00 50 07 52 0d c6 4f 95 b3 f0 +..l...P .R..O...
0040 86 8e 50 10 3d e0 ea 86 00 00 00 27 01 00 00 00 ..P.=... ...'....
0050 00 00 02 69 41 9a 7c fd fa 52 22 3f 00 18 8f 4d ...iA.|. .R"?...M
0060 7f dd 88 bd a1 c3 39 f8 e7 94 52 e2 ed 68 8b 2d ......9. ..R..h.-
Logical-Link Control (llc), 8 bytes
Packets: 375 Displayed: 375 Marked: 0 Load time: 0:00.003

Outline

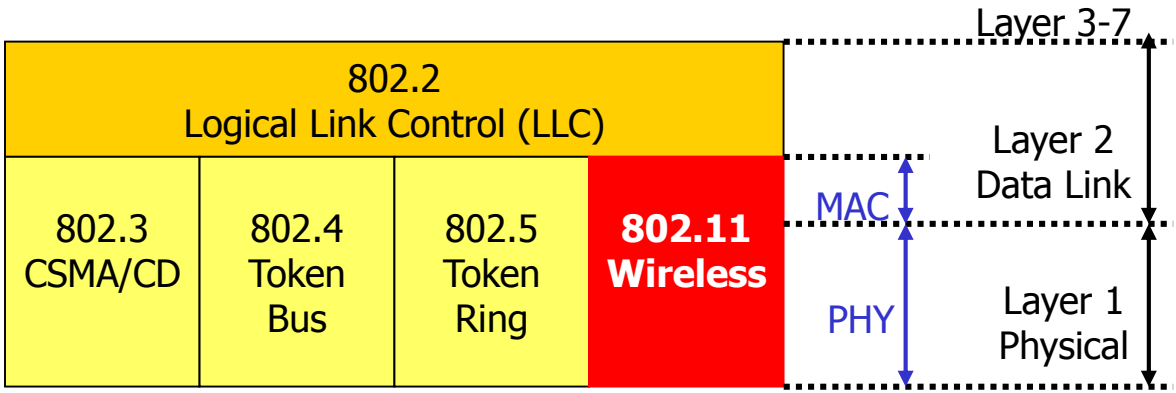
- IEEE 802 Standards
- IEEE 802.11 Overview
- IEEE 802.11 Services
- History and present of IEEE 802.11

IEEE 802.11 design concern

- Wireless / Wired LANs Differences
- Power management
  - Switch to low power mode (sleep)
- Bandwidth
  - Compress data, utilize of the available BW
- Security
  - Works with IEEE 802.10
- Addressing
  - Location / destination address → mobileIP

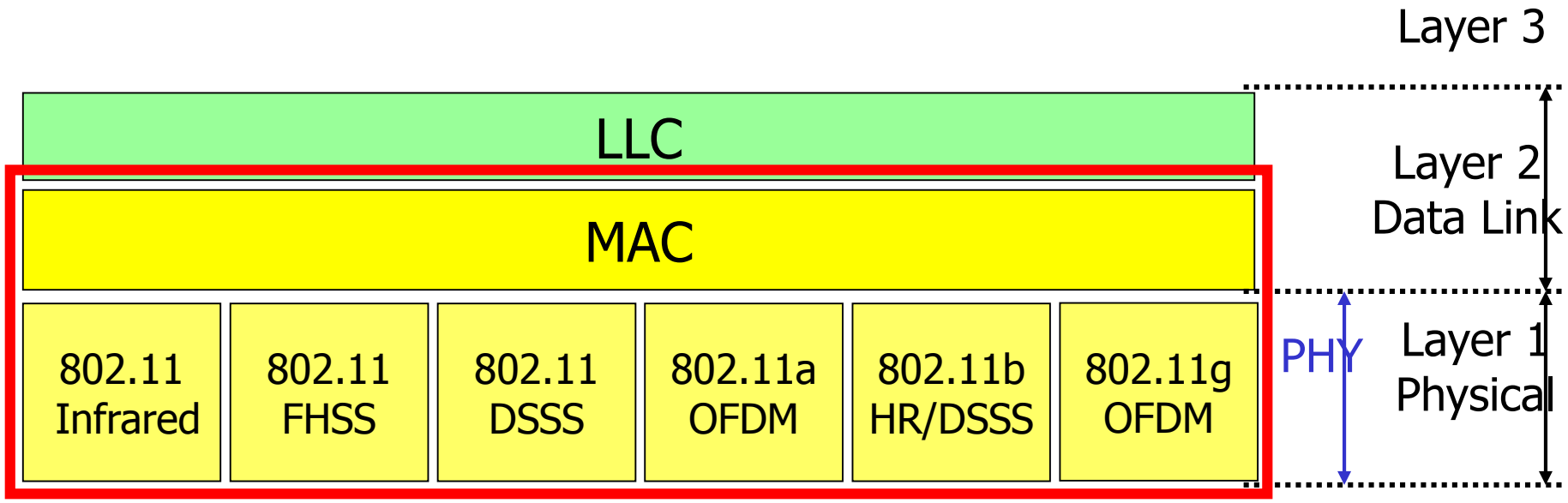
IEEE 802.11 Logical Architecture

- Deliver **M**AC **S**ervice **D**ata **U**nit (MSDU) between peer LLC
- Transparent to higher layer (LLC)
- Provide both MAC and PHY functionality
- Typically resides in NIC or Access Point



IEEE 802.11 Logical Architecture

- Define the network operation
  - Topology → necessary physical components



802.11 MAC Layer

- Provide access control functions
  - Addressing
  - Access coordination
  - Frame check generating / checking
  - LLC PDU delimiting
- CSMA/CA
  - Cannot Tx/Rx simultaneously

802.11 Physical Layers

Radio Frequency

- Frequency Hopping Spread Spectrum (FHSS)
- Direct Sequence Spread Spectrum (DSSS)
- Orthogonal Frequency Division Multiplexing (OFDM)

802.11 Physical Layers

Infrared

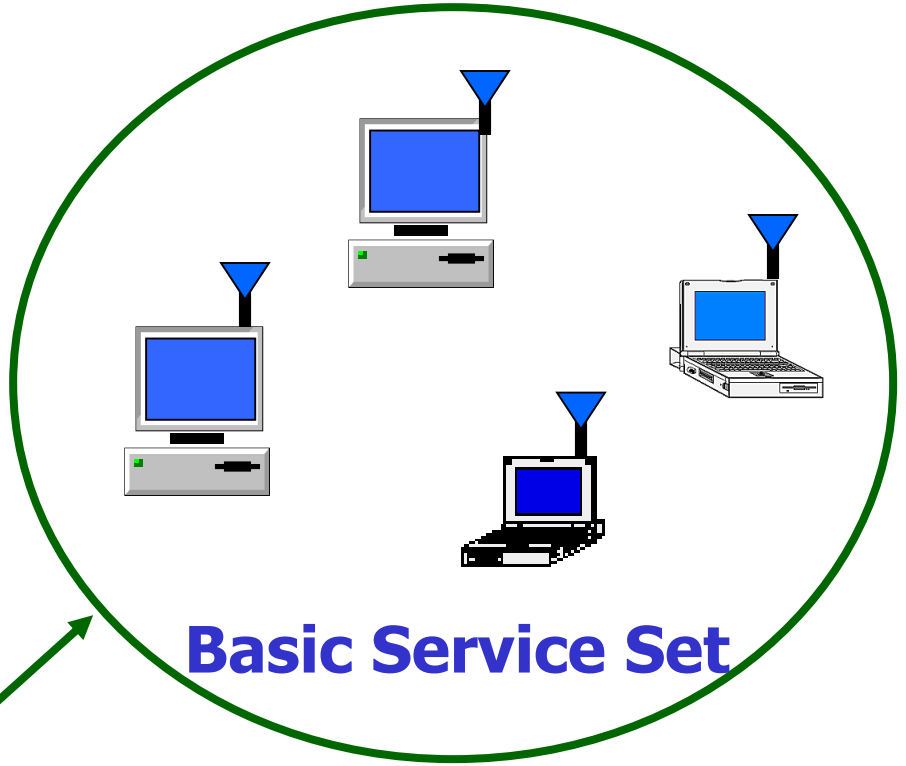
- 850-950 nM, Peak power = 2 Watts
- 16-Pulse position Mod, PPM (1 Mbps)
- 4-PPM (2 Mbps)

IEEE 802.11 Topology

- Independent Basic Service Set (IBSS)
- Extended Service Set (ESS)

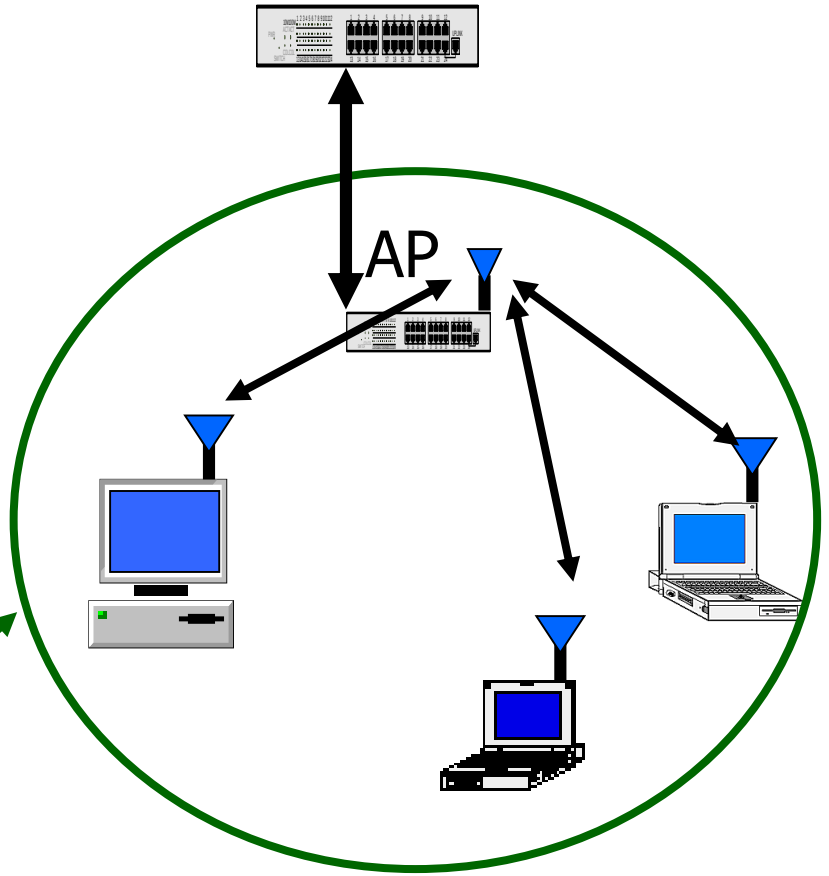
Independent Basic Service Set (IBSS)

- Stand-alone BSS
- No backbone infrastructure
- At least 2 stations
- **Ad hoc** Network
- Small area



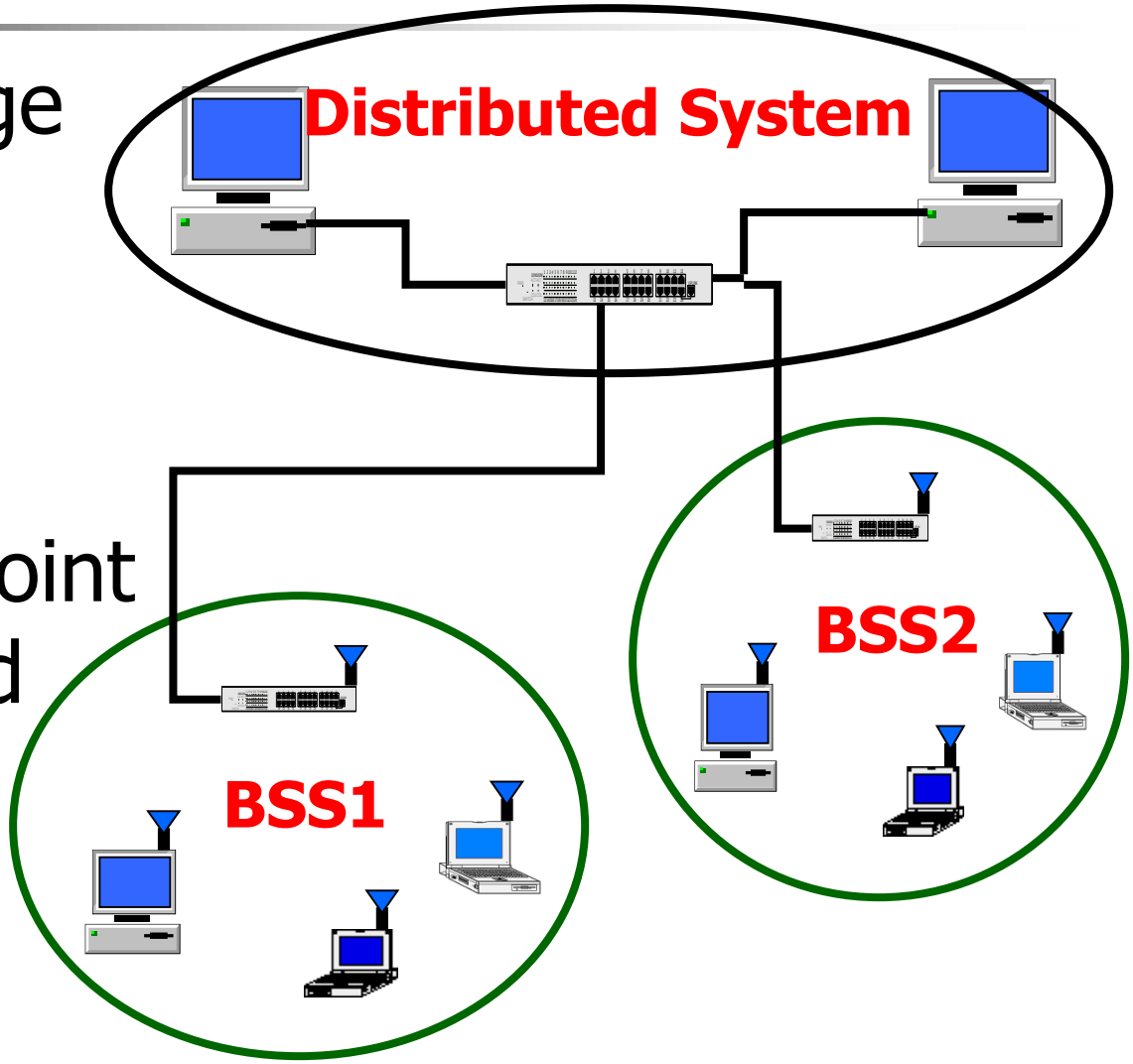
Infrastructure Basic Service Set

- Stand-alone BSS
- Connect to backbone infrastructure
- Access Point
- Small area



Extended Service Set (ESS)

- Extending range
- Arbitrary size
- Multiple cells interconnect
- Need Access Point and Distributed system

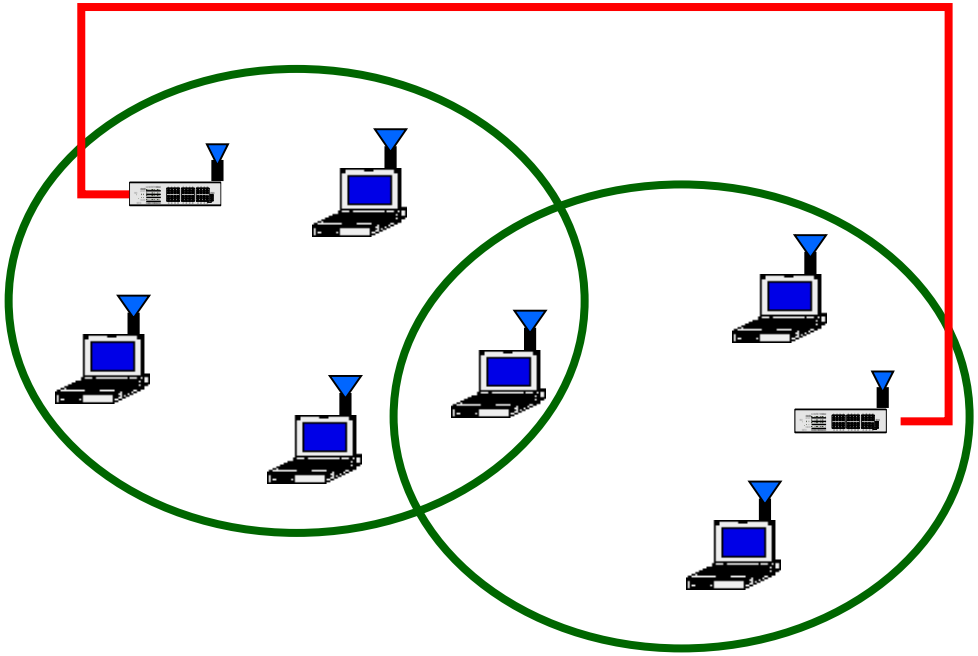


802.11 Mobility Types

- No-transition
  - Not move
  - Moving within a local BSS
- BSS-transition
  - Move from one BSS to another BSS, same ESS
- ESS-transition
  - Move from one BSS to another BSS, different ESS
- Guarantee for No-transition and BSS-transition
- IBSS & ESS are transparent to the LLC

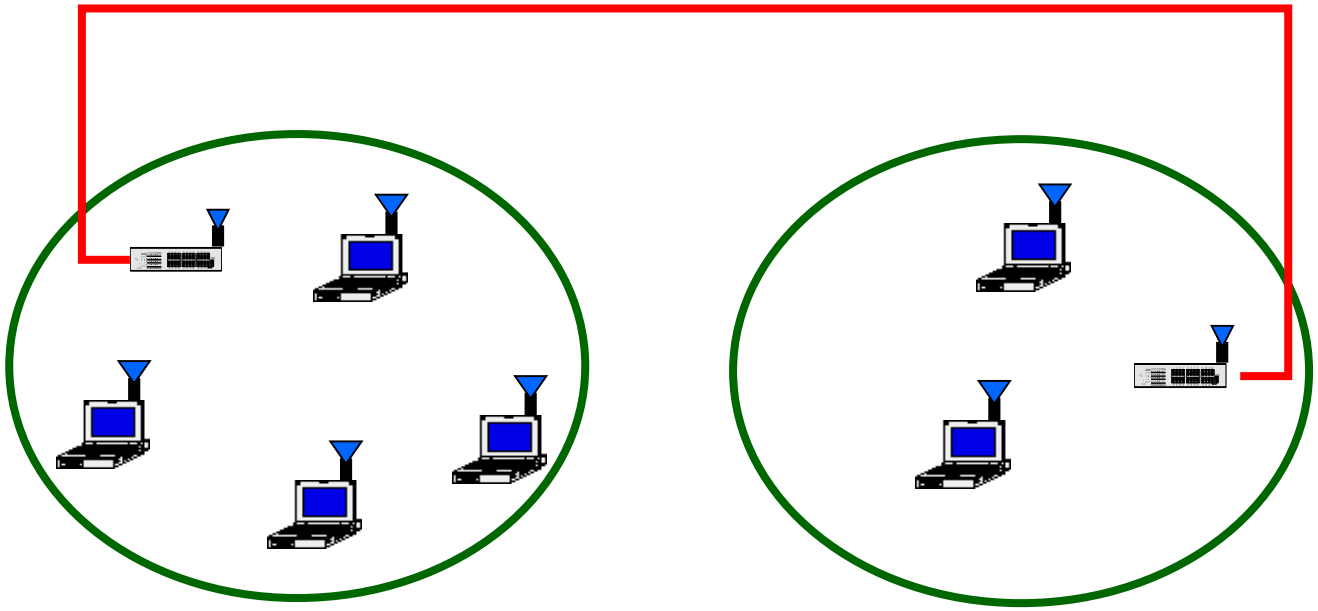
ESS Physical Configuration

- Partial overlap
  - Contiguous coverage in a defined area
  - No disruption



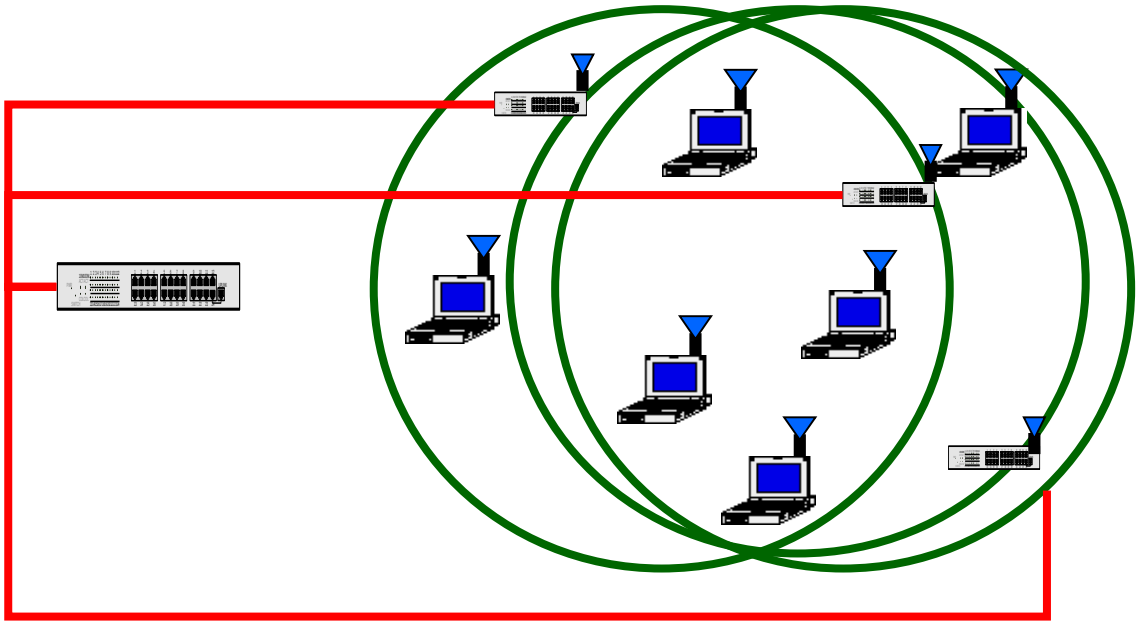
ESS Physical Configuration

- Physical disjoint
  - No contiguous coverage →no distance limit



ESS Physical Configuration

- Physical collocate
  - Redundant or high-performance network



Outline

- IEEE 802 Standards
- IEEE 802.11 Overview
- IEEE 802.11 Services
- History and present of IEEE 802.11

802.11 Services

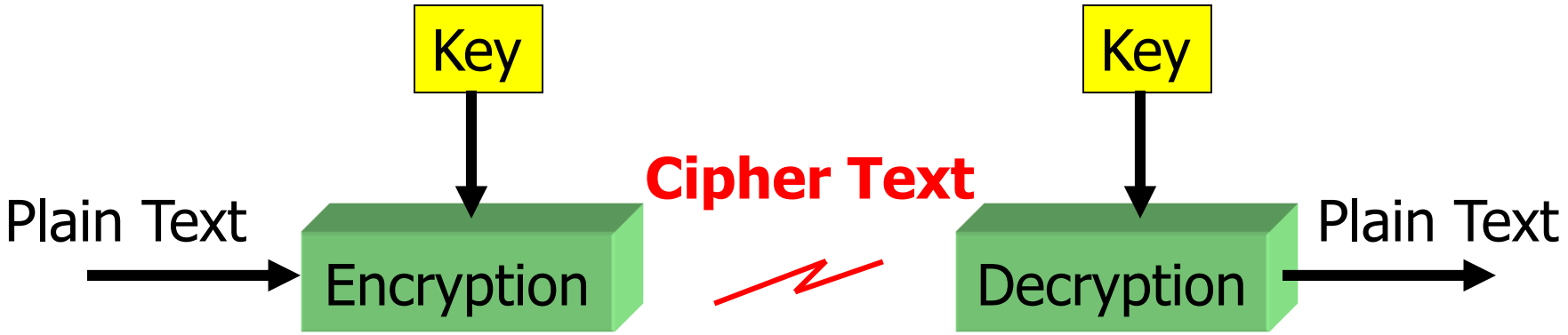
- Station Services (in wireless station)
  - Authentication / Deauthentication
  - Privacy
  - MSDU delivery
- Distribution System Services
  - Association / Disassociation / Reassociation
  - Distribution / Integration

Authentication

- Prevent unauthorized access
- Open system authentication
  - send authen. with ID → get back if recognize
- Shared key authentication
  - Secret shared key (through secure channel)
  - Authen. through shared key
  - Required Wireless Equivalent Privacy Algorithm (WEP) /or others

Privacy

- 802.11 offers a privacy service option
- Based on 802.11 Wired Equivalent Privacy (WEP) algorithm



Association

- Perform @ access point
- Map a station to the distribution system via access point
- Otherwise the transmission is not allowed

Reassociation

- Change the status of association
- Support BSS-transition mobility
- Change the association attribute

802.11 State Diagram