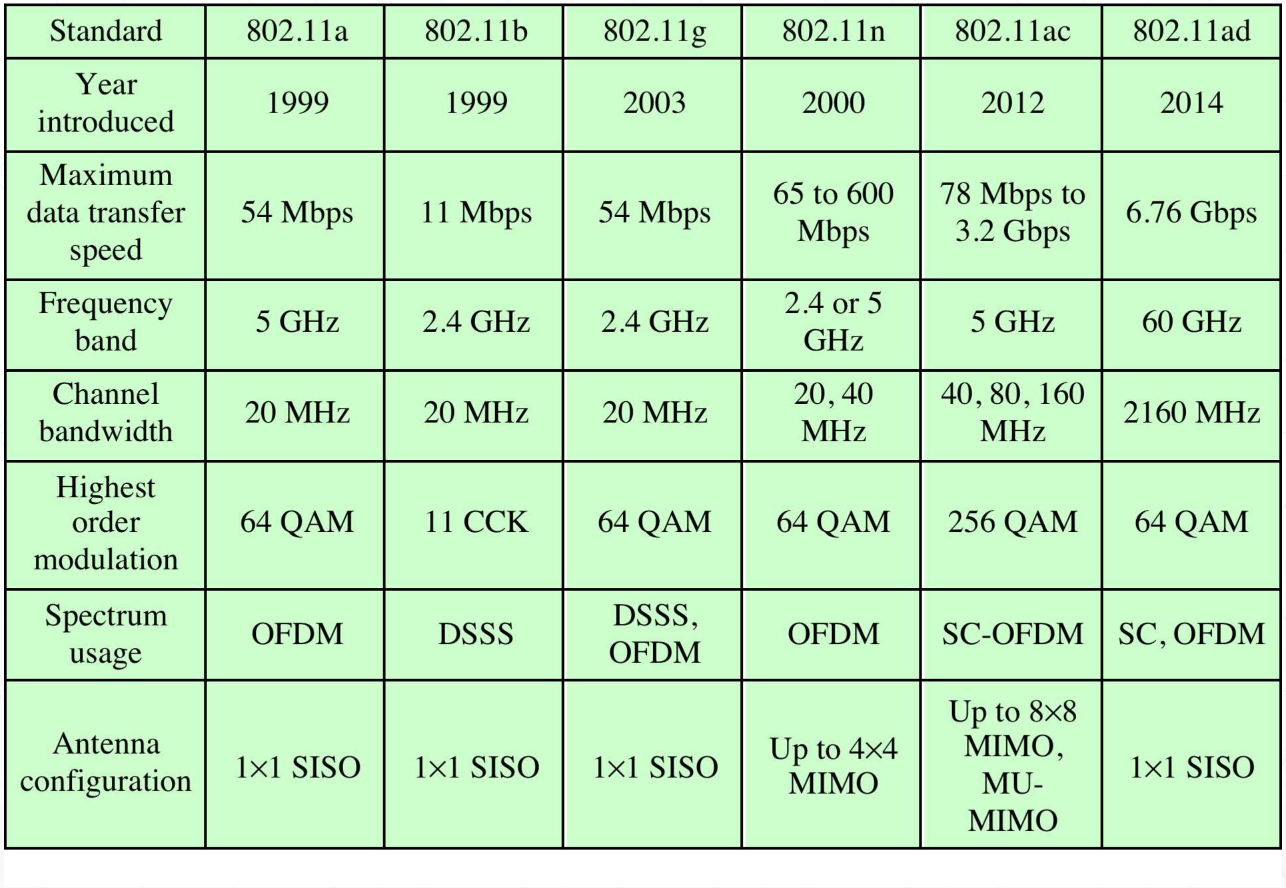
IEEE 802.11 Wireless LAN Standard : Physical Aspects and Security

CS-1699 Wireless Networks
Term : Spring 2018

Instructor : Xerandy

IEEE 802.11 : Physical Layer Standards



Standard	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ad
Year introduced	1999	1999	2003	2000	2012	2014
Maximum data transfer speed	54 Mbps	11 Mbps	54 Mbps	65 to 600 Mbps	78 Mbps to 3.2 Gbps	6.76 Gbps
Frequency band	5 GHz	2.4 GHz	2.4 GHz	2.4 or 5 GHz	5 GHz	60 GHz
Channel bandwidth	20 MHz	20 MHz	20 MHz	20, 40 MHz	40, 80, 160 MHz	2160 MHz
Highest order modulation	64 QAM	11 CCK	64 QAM	64 QAM	256 QAM	64 QAM
Spectrum usage	OFDM	DSSS	DSSS, OFDM	OFDM	SC-OFDM	SC, OFDM
Antenna configuration	1×1 SISO	1×1 SISO	1×1 SISO	Up to 4×4 MIMO	Up to 8×8 MIMO, MU-MIMO	1×1 SISO

IEEE 802.11a and IEEE802.11b

- IEEE 802.11b
  - DSSS
  - Provides data rates of 5.5 and 11 Mbps
  - Complementary code keying (CCK) and packet binary convolution coding (PBCC) modulation schemes
  - First standard to make Wi-Fi become popular
- 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
  - Never became popular, but its formats and channel schemes are used for later releases of 802.11

IEEE 802.11a and IEEE802.11b

- Make use of frequency band called Universal Networking Information Infrastructure(UNII)
  - Three parts :
    - UNII-1 (5.15 to 5.25 GHz) : Indoor use
    - UNII-2 (5.25 to 5.35 GHz) : either indoor and outdoor
    - UNII-3 (5.725 to 5.825 GHz) : outdoor use
- Advantage IEEE 802.11a over IEEE 802.11 b/g
  - More bandwidth
  - Higher data rate
  - Relatively uncluttered frequency spectrum

IEEE 802.11a Channel Structure

- Recommended UNII Channel use in US

Band	Allowed Power	Channel number	Center Frequency (GHz)
UNII – 1	40 mW	36 40 44 48	5.180 5.200 5.220 5.240
UNII-2	200 mW	52 56 60 64	5.260 5.280 ( ) ( )
UNII-3	800 mW	149 153 157 161	( ) ( ) ( ) ( )

IEEE 802.11g

- An extension of IEEE 802.11b
  - These two standards (IEEE 802.11 b and g) are compatible
  - Support date rate up to 54 Mbps
  - The same of modulation and framing schemes as of IEEE 802.11b for data rate 1, 2, 5.5 and 11 Mbps
  - Adopt IEEE 802.11a OFDM for data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbps at 2.4 GHz frequency
  - Using extended PBCC modulation that uses DSSS to support rates 22 and 33 Mbps

IEEE 802.11: Speed vs Distance

- IEEE 802.11 does not include a specification of speed vs distance objectives
- Estimated values for typical office environment (distance in m)

Data rate (Mbps)	Distance		
	802.11b	802.11a	802.11g
1	90+	-	90+
2	75	-	75
5.5(b)/6(a/g)	60	60+	65
9	-	50	55
11(b)/12(a/g)	50	45	50
18	-	40	50
24	-	30	45
36	-	25	35
48	-	15	25
54	-	10	20

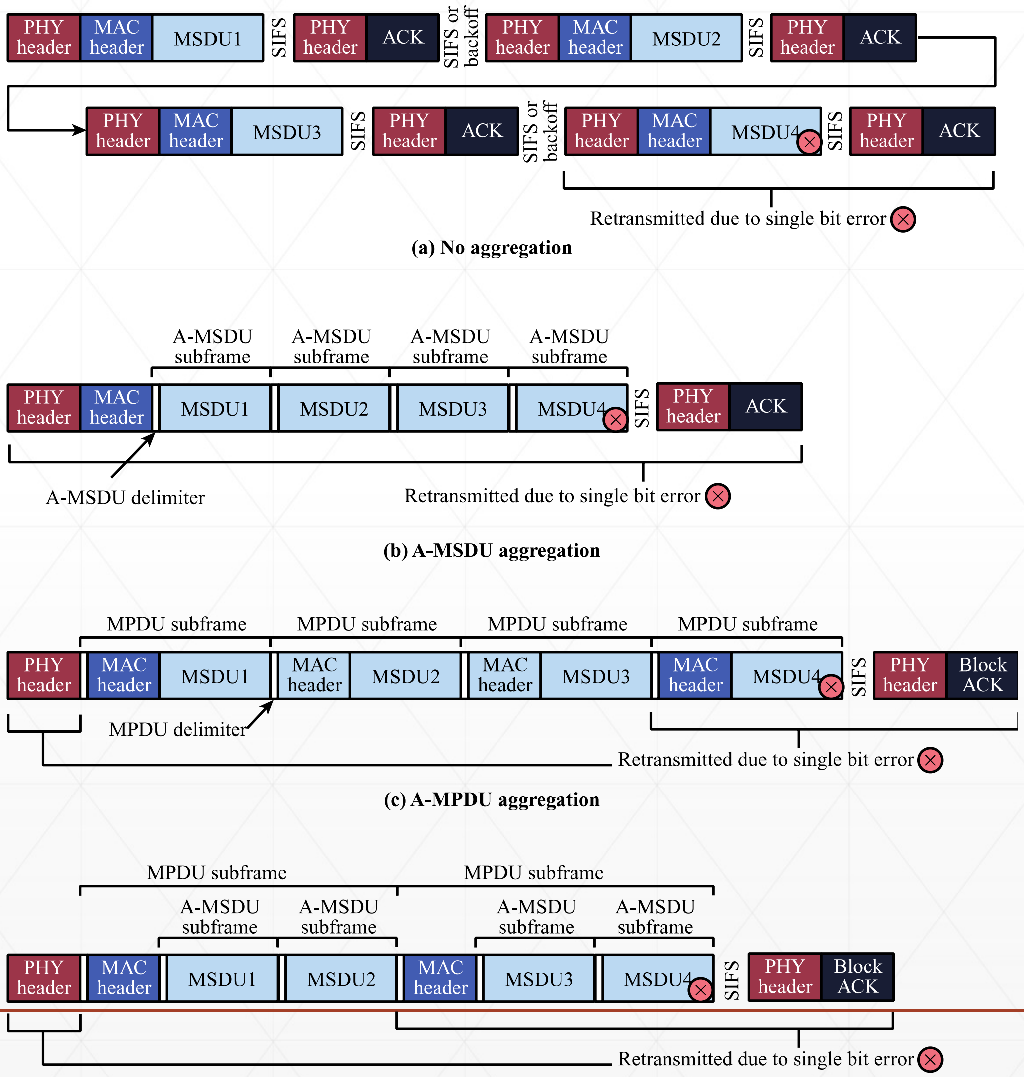
IEEE 802.11n

- Operates in both 2.4-GHz and 5-GHz bands
- MIMO
  - Multiple parallel streams (up to 4 × 4), beamforming, or diversity
- Radio transmission schemes
  - Channel bonding to combine two 20 MHz channels
    - From 48 subcarriers per 20 MHz to 108 carriers per 40 MHz (2.25 times increase in available bandwidth)
    - Can only use 20 MHz channels if other nodes are active
    - Modulation up to 64 QAM
  - Shorter 400 ns guard band (11% increase in data rate)
  - Higher coding rate of 5/6 (11% increase)
  - 150 Mbps per 40 MHz, 600 Mbps for 4 parallel streams

IEEE 802.11n

- MAC enhancements
  - Reduce header bits, backoffs, and IFS times
  - Block acknowledgements
    - One ACK to cover multiple packets
  - Frame aggregation
    - Three forms of aggregation
    - MSDUs come down from the LLC layer, MPDUs come from the MAC layer
      - A-MSDU aggregation – shared PHY and MAC headers and FCS
      - A-MPDU aggregation – shared PHY header
        - Still keep separate MAC headers, to less header reduction
        - But not as much to retransmit if there is an error
      - A-MPDU and A-MSDU aggregation – balances the two

IEEE 802.11n : MSDU Aggregation



(a) No aggregation

(b) A-MSDU aggregation

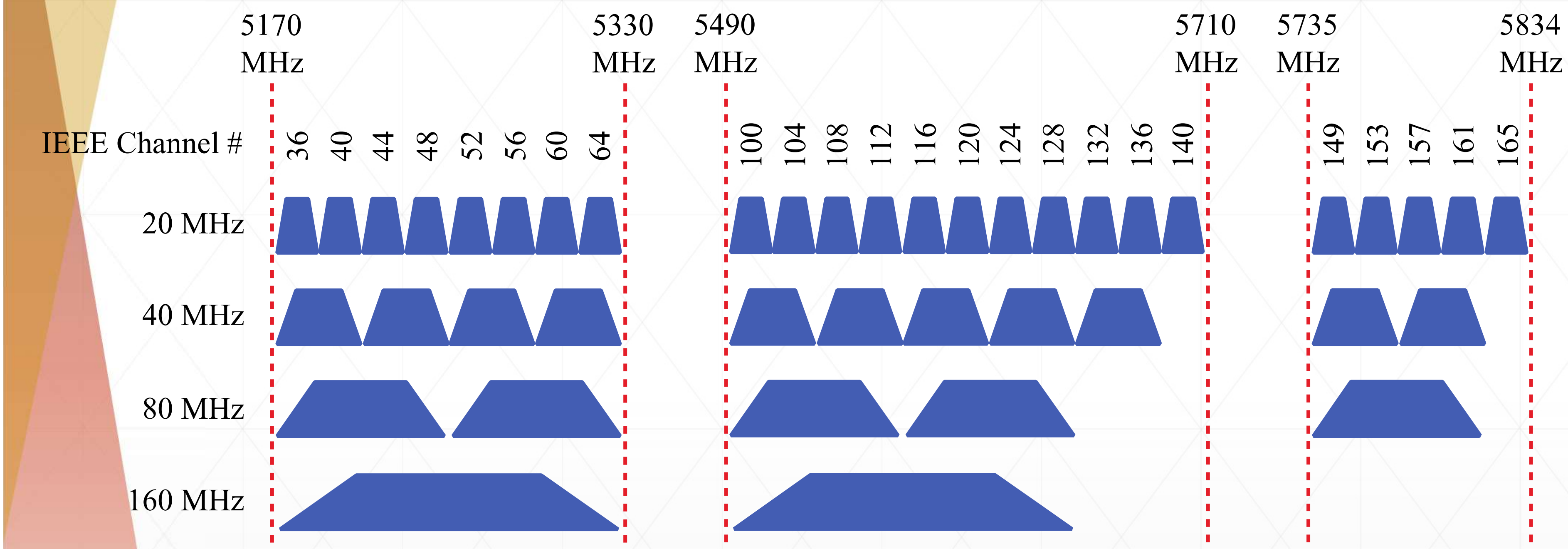
(c) A-MPDU aggregation

(d) A-MPDU of A-MSDU aggregation

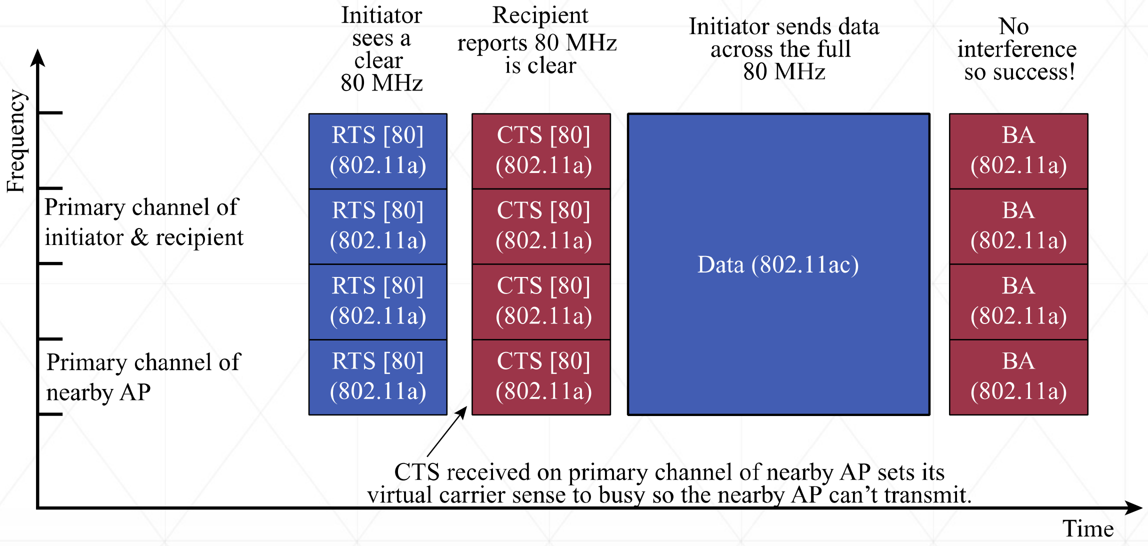
IEEE 802.11: Gigabit WiFi

- 802.11ac
  - Up to 6.937 Gbps
  - 5-GHz only operation
  - Up to 8 × 8 MIMO
  - Bandwidth expansion
    - Up to 160 MHz (8 × 20 MHz channels)
    - Special CSMA and RTS/CTS, to check for legacy devices
  - Modulation is up to 256 QAM
  - Multiuser MIMO
    - Simultaneous beams to multiple stations
    - Advanced channel measurements
  - Larger frame size
  - A-MPDU is required

IEEE 802.11ac Channel Allocation



IEEE 802.11ac RTS/CTS to Probe Bandwidth Availability



Initiator sees a clear 80 MHz

Recipient reports 80 MHz is clear

Initiator sends data across the full 80 MHz

No interference so success!

Frequency

Primary channel of initiator & recipient

Primary channel of nearby AP

RTS [80] (802.11a)

RTS [80] (802.11a)

RTS [80] (802.11a)

RTS [80] (802.11a)

CTS [80] (802.11a)

CTS [80] (802.11a)

CTS [80] (802.11a)

CTS [80] (802.11a)

Data (802.11ac)

BA (802.11a)

BA (802.11a)

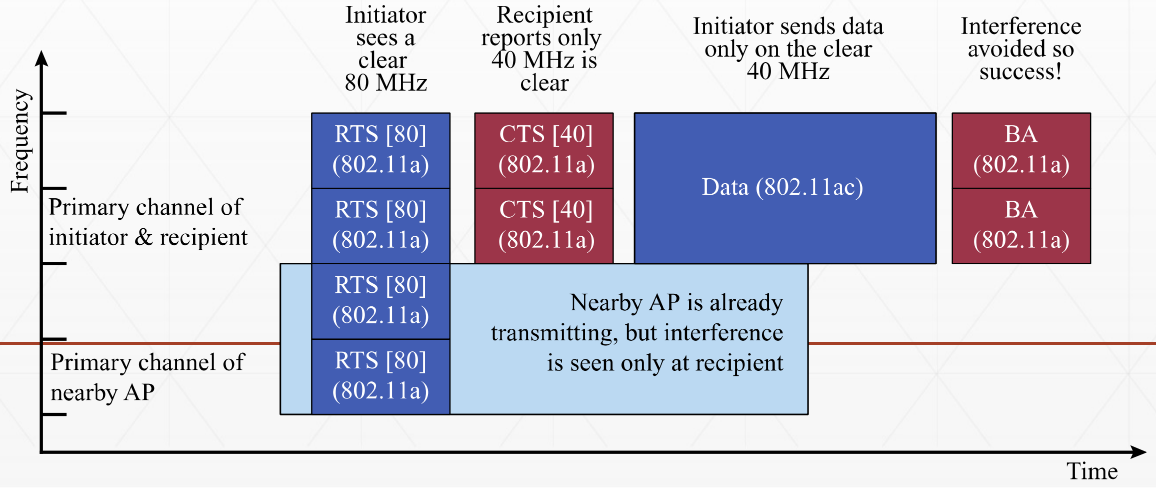
BA (802.11a)

BA (802.11a)

CTS received on primary channel of nearby AP sets its virtual carrier sense to busy so the nearby AP can't transmit.

Time

(a) No interference case



Initiator sees a clear 80 MHz

Recipient reports only 40 MHz is clear

Initiator sends data only on the clear 40 MHz

Interference avoided so success!

Frequency

Primary channel of initiator & recipient

Primary channel of nearby AP

RTS [80] (802.11a)

RTS [80] (802.11a)

RTS [80] (802.11a)

RTS [80] (802.11a)

CTS [40] (802.11a)

CTS [40] (802.11a)

Data (802.11ac)

BA (802.11a)

BA (802.11a)

Nearby AP is already transmitting, but interference is seen only at recipient

Time

IEEE 802.11: Gigabit WiFi

- 802.11ad
  - WiGig, Up to 7 Gbps
    - Replacement of wires for video to TVs and projectors
  - Uses 60-GHz bands
    - Called millimeter waves (mmWave)
    - Fewer devices operate in these bands
    - Higher free space loss, poor penetration of objects
    - Likely only useful in a single room
    - Bandwidth is 2,160 MHz
  - Adaptive beamforming and high gain directional antennas
    - Can even find reflections when direct path is obstructed
  - Personal BSS so devices can talk directly

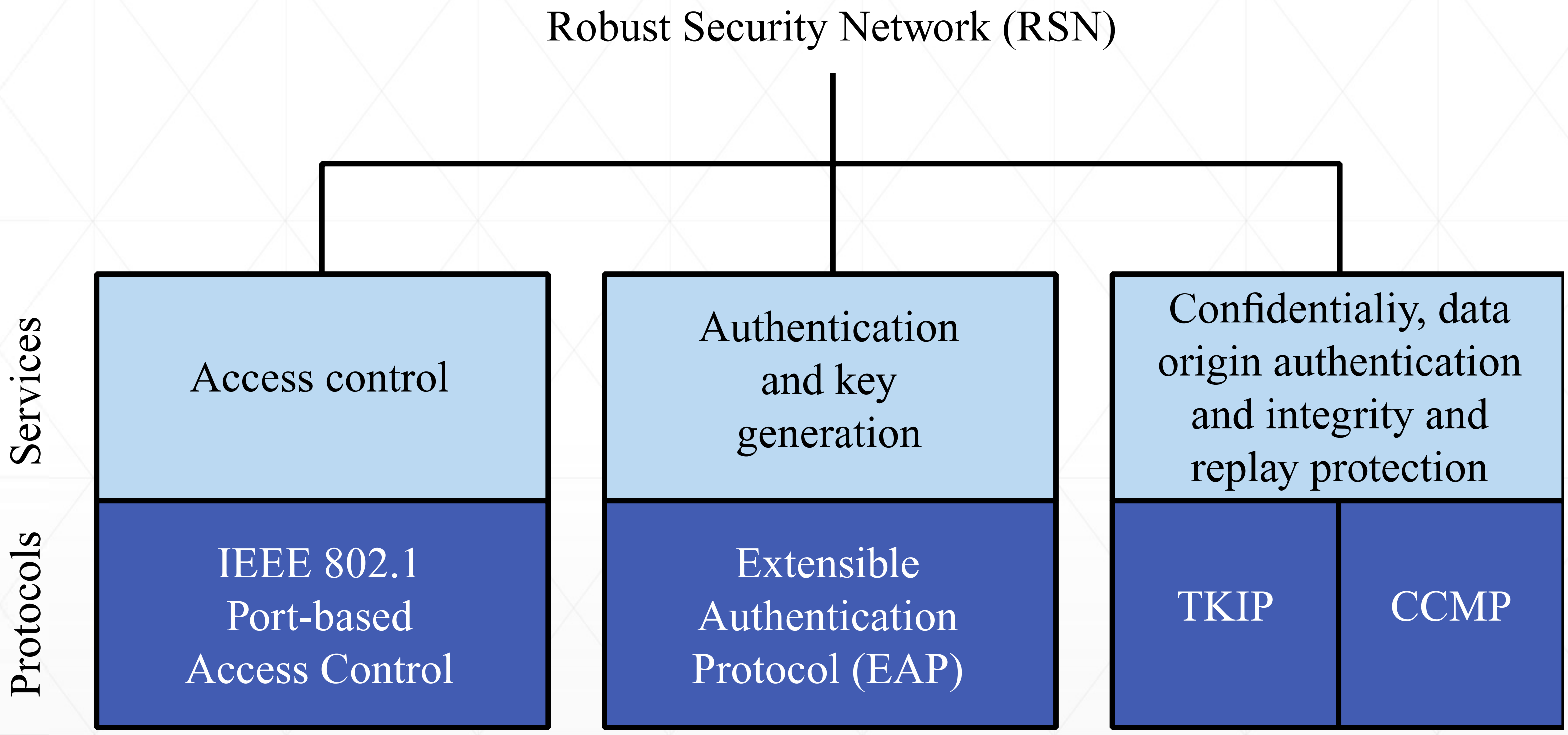
IEEE 802.11: WLAN Security

- Key contributing factors
  - Channel
    - Involves broadcast communications, which is far more susceptible to eavesdropping and jamming
  - Mobility
    - Wireless devices far more portable than wired devices
  - Resources
    - Mobile devices have limited memory and processing resources, especially to counter denial of service and malware attacks
  - Accessibility
    - Some wireless devices may be left unattended in remote or hostile locations.

IEEE 802.11: WLAN Security

- Three points of attack
  - Client
  - Access Point
  - Wireless medium
- Original Wired Equivalent Privacy (WEP) was much too weak
  - 802.11i provided stronger Wi-Fi Protected Access (WPA)
  - Robust Security Network (RSN) is the final 802.11i standard
- 802.11i services
  - Authentication through an authentication server
  - Access control : enforces the use of the authentication function, routes the messages, facilitates key exchanges
  - Encryption for privacy with message integrity: Encrypted data at LLC PDU

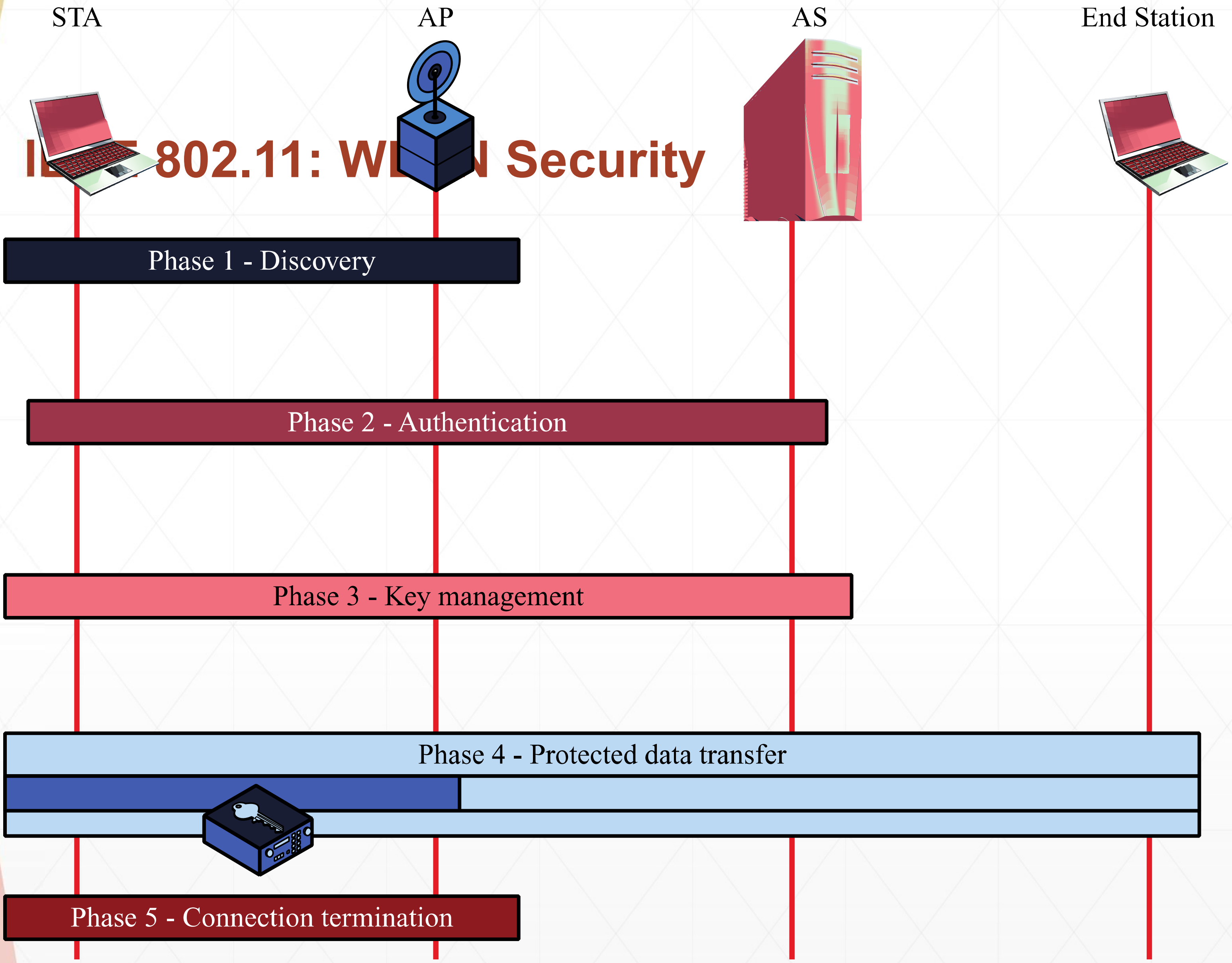
IEEE 802.11: Element of IEEE 802.i


Robust Security Network (RSN)
Services
Protocols
Access control
Authentication and key generation
Confidentialiy, data origin authentication and integrity and replay protection
IEEE 802.1 Port-based Access Control
Extensible Authentication Protocol (EAP)
TKIP
CCMP

Services and Protocols

CCMP	=	Counter Mode with Cipher Block Chaining MAC Protocol
TKIP	=	Temporal Key Integrity Protocol

IEEE 802.11: WLAN Security



STA

AP

AS

End Station

Phase 1 - Discovery

Phase 2 - Authentication

Phase 3 - Key management

Phase 4 - Protected data transfer

Phase 5 - Connection termination

IEEE 802.11i : Phases of Operation

- Discovery
  - STA uses Beacons and Probe Response to identify the AP to which it wishes to communicate
- Authentication
  - STA and AS prove their identities to each other
- Key generation and distribution
  - Access point (AP) and STA perform several operations to generate several cryptographic keys and distribute them on AP and STA
- Protected data transfer
  - Frame exchanges between STA and other end STA. Secure data transfer only occur between STA and AP
- Connection Termination

IEEE 802.11i : Phases of Operation: Discovery

- Discovery
  - STA uses Beacons and Probe Response to identify the AP to which it wishes to communicate
  - Operations :
    - Network and security capability discovery
      - STA may be passively listen or actively request RSN IE (Information Element) broadcasted through Beacon frame
    - Open system authentication
      - To maintain backward compatibility with IEEE 802.11 state machine
    - Association
      - STA associate to the access point using Association frame

IEEE 802.11i : Phases of Operation: Authentication

- Authentication
  - Enables mutual authentication between STA and authentication server (AS)
  - Uses IEEE 802.1X : Port-Based Network Access Control standard that adopts Extensible Authentication Protocol. This standard uses following terms
    - Supplicant corresponds to STA, Authenticator corresponds to AP
    - Authentication Server generally corresponds to separate devices accessible through Distribution System
  - Following phases take place
    - Connect to AS
    - EAP exchange
    - Secure Key Delivery
      - AS will generate master session key known as Authentication, Authorization and Accounting (AAA) key
      - This key will be used to generate cryptographic key in subsequent phase

IEEE 802.11i : Phases of Operation

- Key Management Phase
  - During this phase, a variety of cryptographic keys are generated and distributed to STAs
  - Two types of keys :
    - Pairwise keys : used for communication between STA and an AP
    - Group keys : used for multicast communication
- Protected Data Transfer
  - Only provide secure data transfer between AP and STA
  - Defines two schemes. Both provides message integrity and data confidentiality services
    - Temporal Key Integrity Protocol (TKIP)
      - Implemented in older wireless devises, that only requires software change
    - Counter Mode-CBC MAC protocol (CCMP)
      - Implemented in newer, hardware capable wireless devices
- Connection termination

IEEE 802.11i : Phases of Operation

- Key Management Phase
  - During this phase, a variety of cryptographic keys are generated and distributed to STAs
  - Two types of keys :
    - Pairwise keys : used for communication between STA and an AP
    - Group keys : used for multicast communication
- Protected Data Transfer
  - Only provide secure data transfer between AP and STA
  - Defines two schemes. Both provides message integrity and data confidentiality services
    - Temporal Key Integrity Protocol (TKIP)
      - Implemented in older wireless devises, that only requires software change
    - Counter Mode-CBC MAC protocol (CCMP)
      - Implemented in newer, hardware capable wireless devices
- Connection termination