Wireless Local Area Networks (WLAN)

Part 1

Based on:

- Ivan Marsic: Computer Networks, Sec. 1.5.3 (Moodle)
- B. Cory &W. Stalling (2016), Wireless Communication Networks and Systems, Chapter 11 Wireless LAN Technology
- IEEE 802.11-2012 standard (Moodle)
- Wikipedia
- (add relevant frames to services)

Learning Outcomes

On completion of LT04 and LT05:

- Explain the roles of layers in the IEEE802.11 architecture.
- Describe the services provided by IEEE 802.11
- Explain the use backoff, interframe spacing, point coordination, and distributed coordination for MAC layer operation of IEEE 802.11.
- Describe the main methods used to improve throughput in IEEE 802.11n, IEEE 802.11ac, and IEEE802.11ad.
- Explain the IEEE802.11i WLAN security procedures.

Wireless LANs

- Wireless LANs are an indispensable adjunct to traditional wired LANs,
- They satisfy requirements for:
  - mobility,
  - relocation,
  - ad hoc networking, and
  - coverage of locations difficult to wire.

Wireless LAN Class Index

- Wireless LAN's
  - Wireless LAN applications
  - Nomadic Access and Ad Hoc Networking
  - Wireless LAN requirements
  - Wireless LAN Technology
- Infrared LAN's
  - Strengths & Weaknesses

Wireless LAN Class Index

  - Transmission Techniques
- Spread Spectrum LAN’s
  - Configuration
  - Transmission Issues
- Narrowband Microwave LAN’s
  - Licensed Narrowband RF
  - Unlicensed Narrowband RF

Wireless LAN applications

- Early wireless LAN products, were marketed as substitutes for traditional wired LANs
- In a number of environments, there is a role for the wireless LAN as an alternative to a wired LAN.

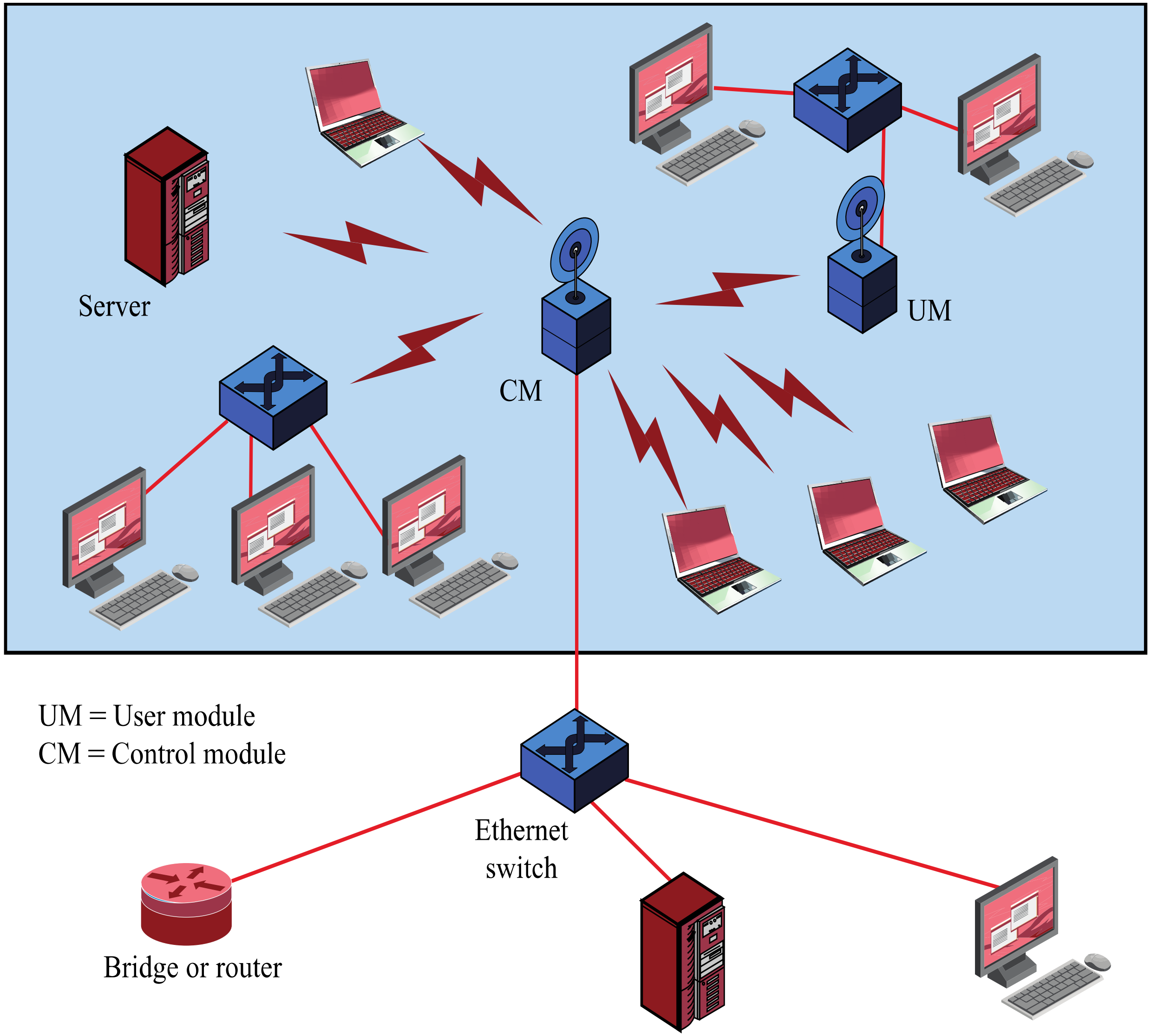
Wireless LAN applications

- Buildings with large open areas (manufacturing plants, stock exchange trading floors, warehouses).
- Historical buildings with insufficient twisted pair and where drilling holes for new wiring is prohibited.
- Small offices where installation and maintenance of wired LANs are not economical.

Wireless LAN applications

- In all of these cases, a wireless LAN provides an effective and more attractive alternative.
- In most of these cases, an organization will also have a wired LAN to support servers and some stationary workstations.

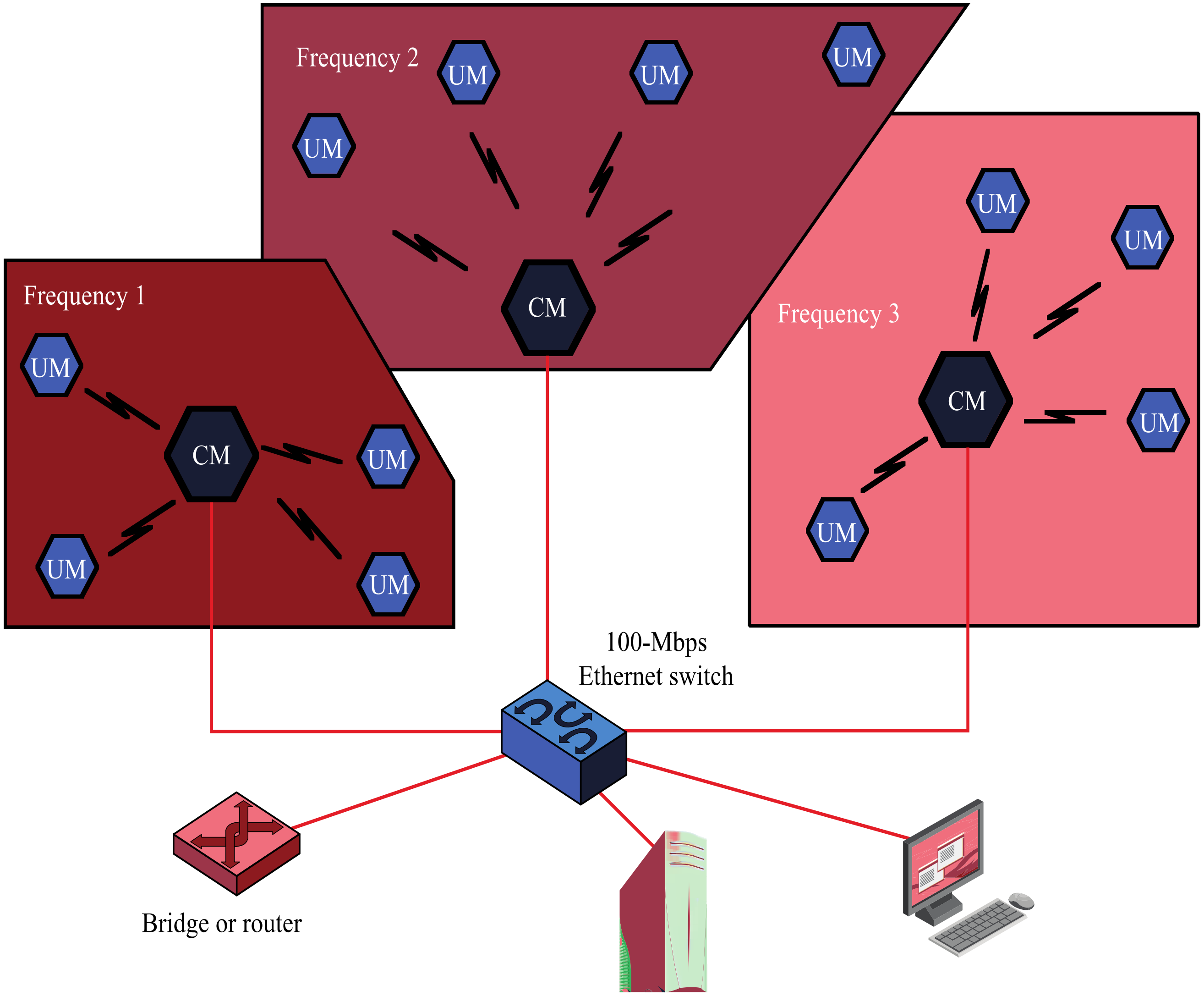
Example Single-Cell Wireless LAN Configuration



UM = User module
CM = Control module

- Multiple-cell wireless LAN
  - Multiple CMs connected by a wired LAN
  - Creates many issues for balancing cell loading and providing best connections for Ums

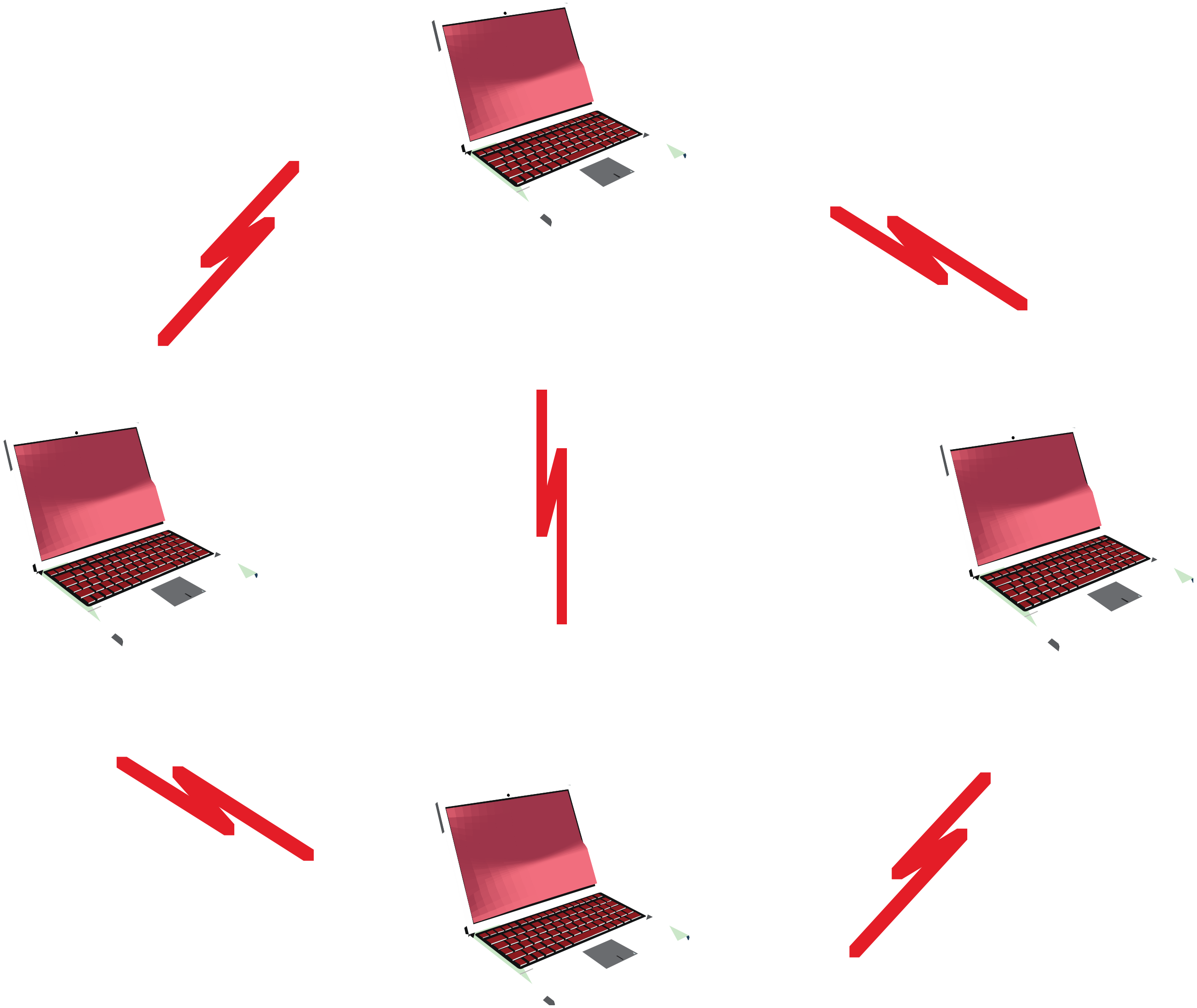
Example Multiple-Cell Wireless LAN Configuration



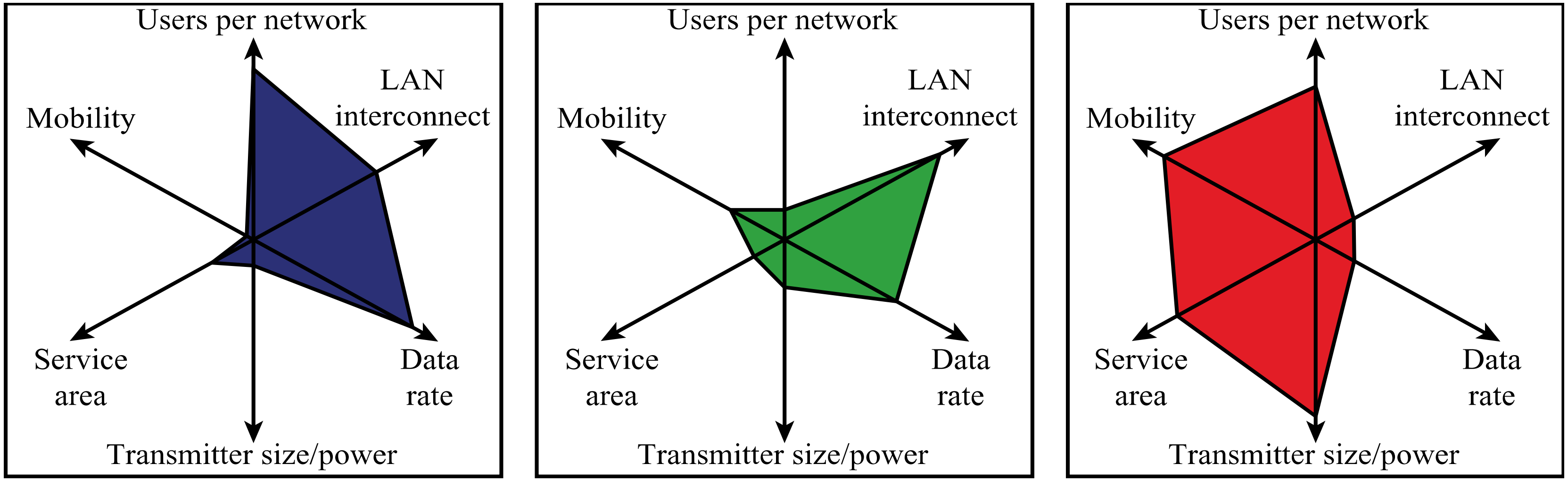
Ad Hoc Networking

- Temporary peer-to-peer network set up to meet immediate need
  - Peer-to-peer, no centralized server
  - May be a temporary network
  - Wireless connectivity provided by WLAN or Bluetooth, ZigBee, etc.
- Example:
  - Group of employees with laptops convene for a meeting; employees link computers in a temporary network for duration of meeting

Ad Hoc Wireless LAN Configuration



Kiviat Graphs for Data Networks



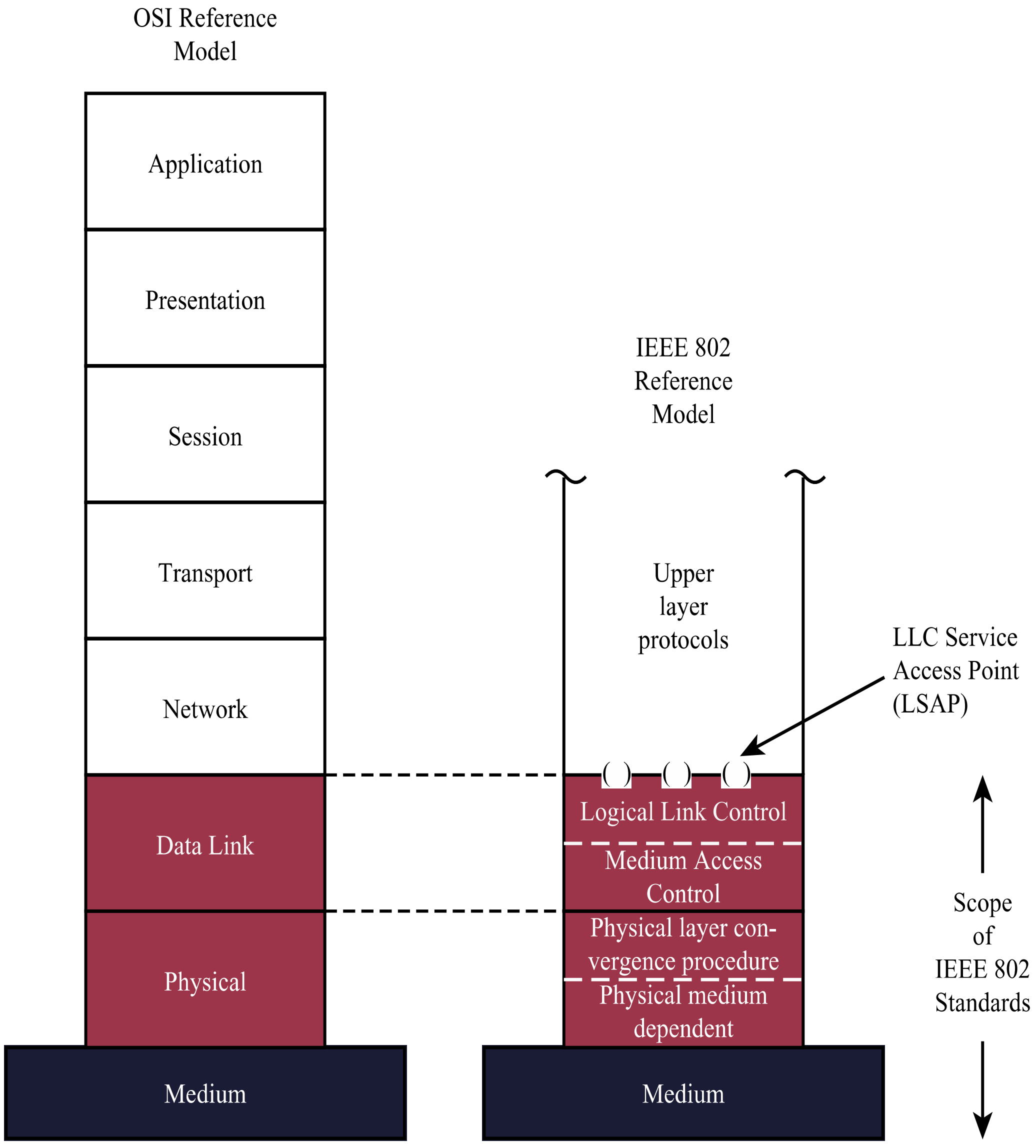
(a) Wired LANs **(b) Wireless LANs** **(c) Mobile data networks**

KG provides a pictorial means of comparing systems along multiple variables. The variables are laid out at equal angular intervals. A given system is defined by one point on each variable; these points are connected to yield a shape that is characteristic of that system

Protocol architecture

- Developed by the IEEE 802.11 working group
- Uses layering of protocols
- LAN protocols focus on the lower layers of the OSI model
  - Relates OSI with 802.11
  - Called the IEEE 802 reference model

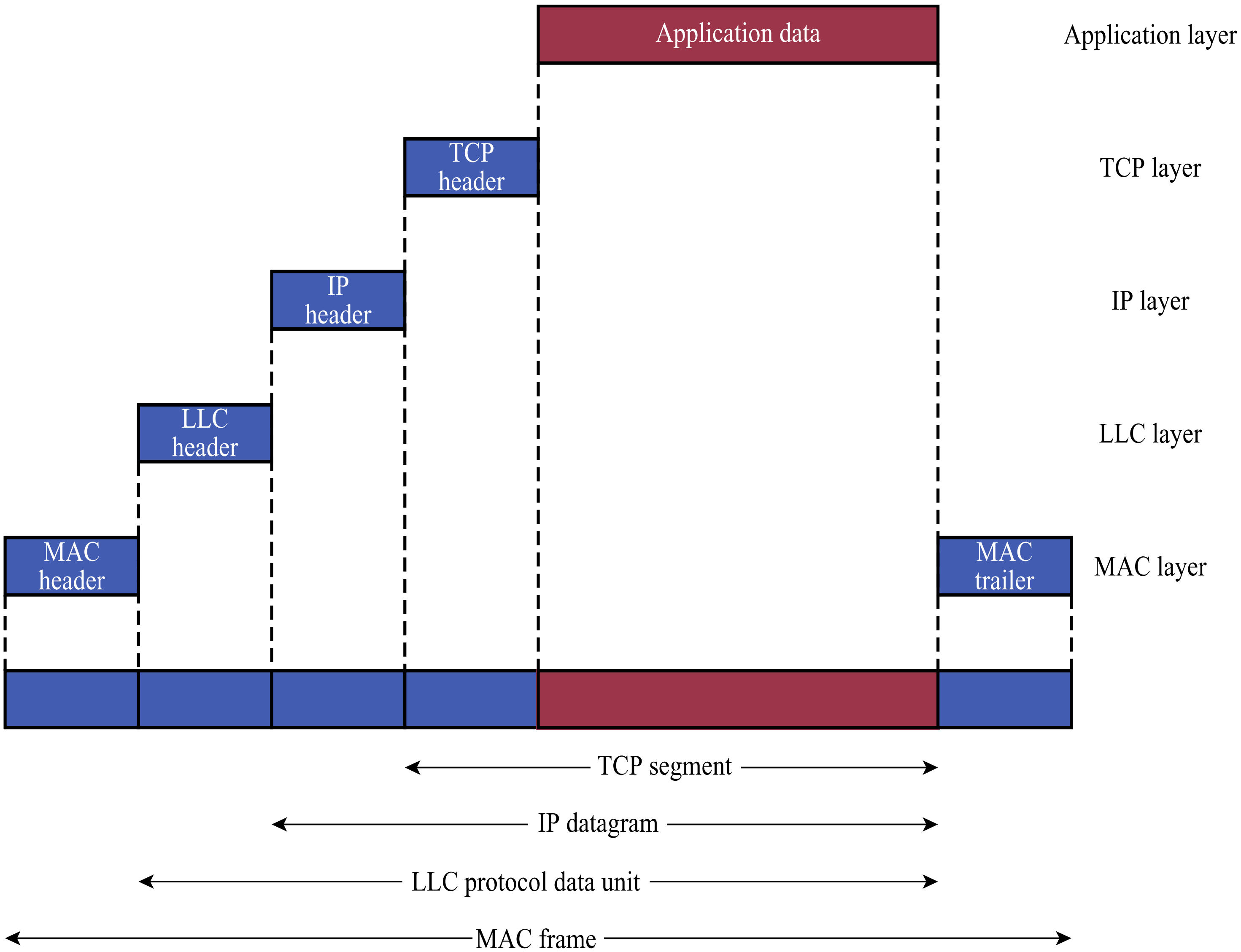
IEEE 802 Protocol Layers Compared to OSI Model



Protocol Architecture

- Functions of physical layer:
  - Encoding/decoding of signals
  - Preamble generation/removal (for synchronization)
  - Bit transmission/reception
  - Includes specification of the transmission medium
- Sublayers
  - Physical medium dependent sublayer (PMD)
    - Transmitting and receiving user data through a wireless medium
  - Physical layer convergence procedure (PLCP)
    - Mapping 802.11 MAC layer protocol data units (MPDUs) into a framing format
    - Sending and receiving between stations using same PMD sublayer

IEEE 802 Protocols in Context



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

Dominant Wireless Network Standards

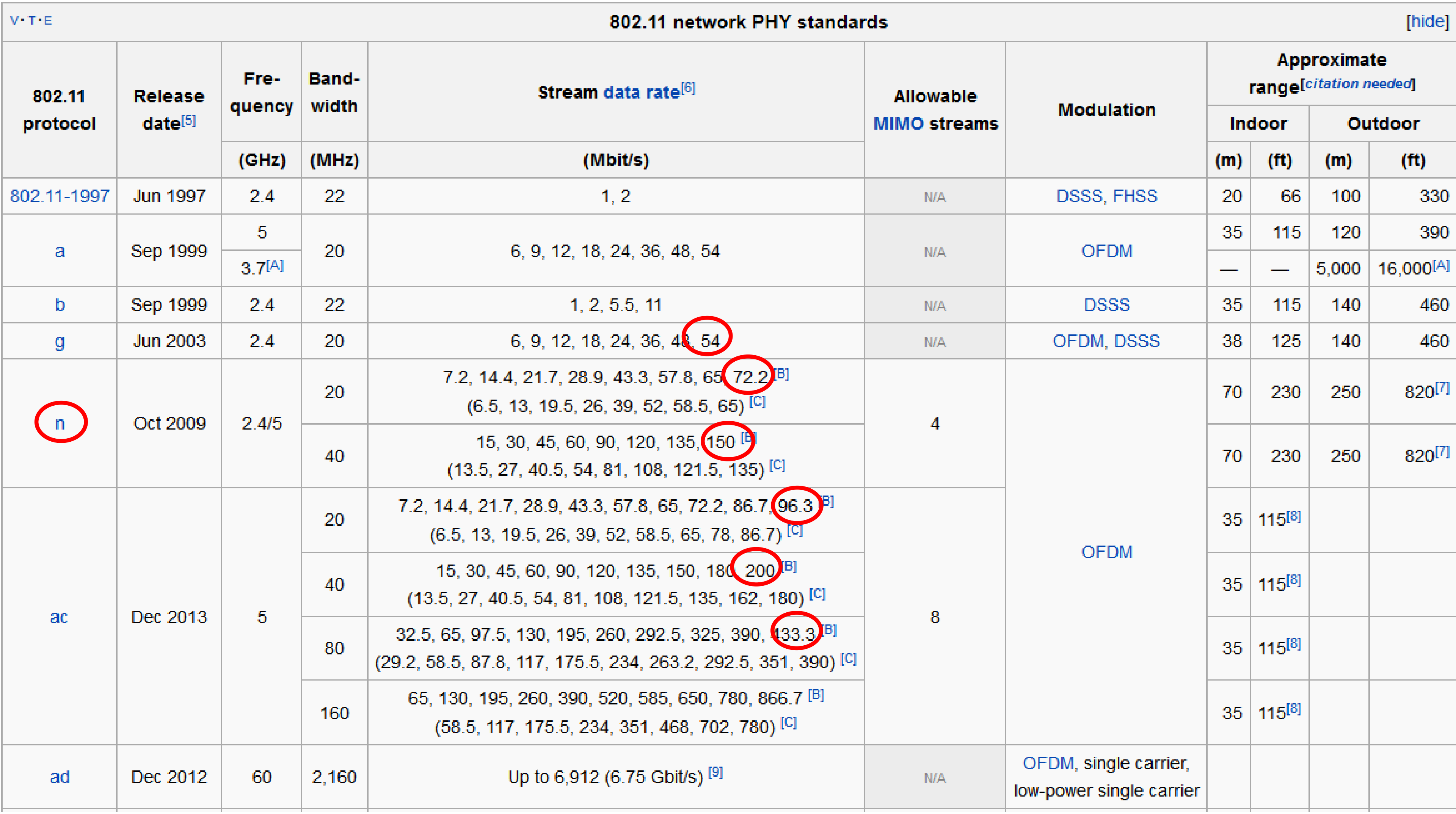
Common Name	Family	Primary use	Radio Tech	Downstream (Mb/s)	Upstream (Mb/s)	Note
WiFi	802.11	WLAN	OFDM MIMO	Up to 600		
HSPA+	3GPP	3G+ Networks	CDMA/FDD MIMO	Up to 300	Up to 150	Mobile users
LTE (advanced)	3GPP	4G Networks	**OFDMA, SC-FDMA** FDD/TDD MIMO	Up to 300 (1Gb/s)	Up to 75	Fixed and mobile users
WiMAX2	802.16m	Wireless MAN	OFDMA FDD/TDD MIMO	Up to 365 (1Gb/s)	Up to 376 (1Gb/s)	Fixed and mobile users

- OFDM – Orthogonal Frequency-Division Multiplexing
- OFDMA – Orthogonal Frequency-Division Multiple Access
- SC-FDMA – Single Carrier Frequency-Division Multiple Access
- CDMA – Code Division Multiple Access
- T/FDD – Time/Frequency Division Duplexing

Wireless LAN Standards

Wireless Local Area Network (WLAN)

- Wireless Local Area Networks (WLANs) are typically extension of the wired part of the LANs.
- **IEEE 802.11** is a set of standards for WLANs operating in the 2.4 and 5 GHz frequency bands.
- **IEEE 802.11-2012** is the current version of the standard which includes a number of amendments added over time.
- The popular amendments included in the 2012 version describe **802.11g**, **802.11n** and **802.11s** (mesh) protocols.
- **Wi-Fi** is a trademark of the **Wi-Fi Alliance** **(WiFi Aware –New Version) (https://www.youtube.com/user/WiFiAlliance)**
- Manufacturers may use this trademark to brand certified products that belong to a class of WLAN devices based on the IEEE 802.11 standards
- The term *Wi-Fi* is often used as a synonym for IEEE 802.11 WLAN technology.



V·T·E 802.11 network PHY standards [hide]

802.11 protocol	Release date[5]	Frequency	Bandwidth	Stream data rate[6]	Allowable MIMO streams	Modulation	Approximate range[citation needed]			
							Indoor		Outdoor	
		(GHz)	(MHz)	(Mbit/s)			(m)	(ft)	(m)	(ft)
802.11-1997	Jun 1997	2.4	22	1, 2	N/A	DSSS, FHSS	20	66	100	330
a	Sep 1999	5	20	6, 9, 12, 18, 24, 36, 48, 54	N/A	OFDM	35	115	120	390
		3.7[A]					—	—	5,000	16,000[A]
b	Sep 1999	2.4	22	1, 2, 5.5, 11	N/A	DSSS	35	115	140	460
g	Jun 2003	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	N/A	OFDM, DSSS	38	125	140	460
n	Oct 2009	2.4/5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2[B] (6.5, 13, 19.5, 26, 39, 52, 58.5, 65) [C]	4	OFDM	70	230	250	820[7]
			40	15, 30, 45, 60, 90, 120, 135, 150 [B] (13.5, 27, 40.5, 54, 81, 108, 121.5, 135) [C]			70	230	250	820[7]
ac	Dec 2013	5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 86.7, 96.3 [B] (6.5, 13, 19.5, 26, 39, 52, 58.5, 65, 78, 86.7) [C]	8		35	115[8]		
			40	15, 30, 45, 60, 90, 120, 135, 150, 180, 200 [B] (13.5, 27, 40.5, 54, 81, 108, 121.5, 135, 162, 180) [C]			35	115[8]		
			80	32.5, 65, 97.5, 130, 195, 260, 292.5, 325, 390, 433.3 [B] (29.2, 58.5, 87.8, 117, 175.5, 234, 263.2, 292.5, 351, 390) [C]			35	115[8]		
			160	65, 130, 195, 260, 390, 520, 585, 650, 780, 866.7 [B] (58.5, 117, 175.5, 234, 351, 468, 702, 780) [C]			35	115[8]		
ad	Dec 2012	60	2,160	Up to 6,912 (6.75 Gbit/s) [9]	N/A	OFDM, single carrier, low-power single carrier				

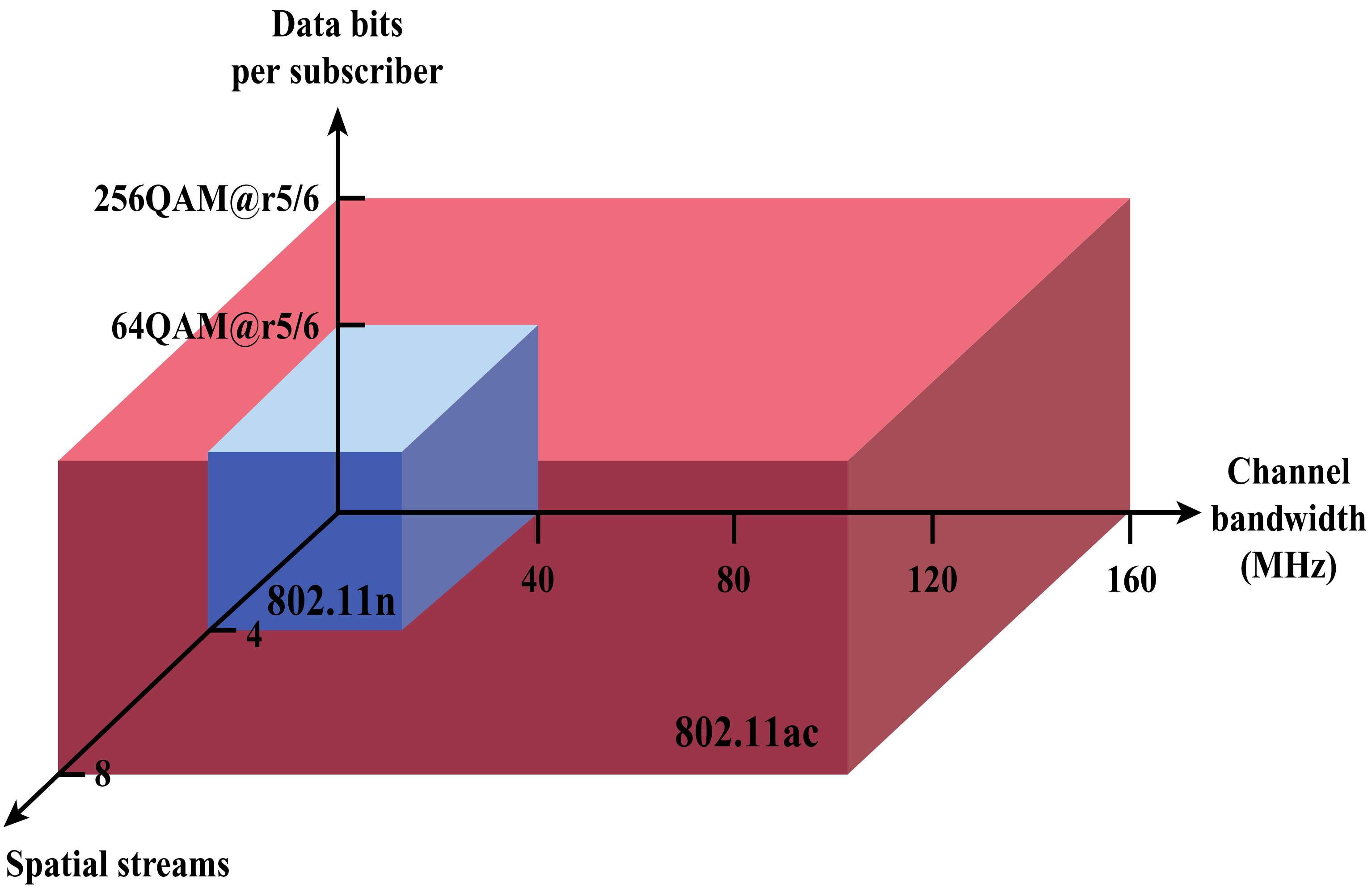
IEEE 802.11 wikipedia

DSSS - direct sequence spread spectrum,

FHSS - frequency-hopping spread spectrum,

OFDM - orthogonal frequency division multiplexing

IEEE 802.11 Performance Factors



Comments on the IEEE Std 802.11-2012

- A large, very detailed document covering all possible aspects of the **Medium Access Control** (MAC) and **Physical Layer** (PHY)
- Organized in chapters called clauses (contents)
- Annexes are either normative (must obey), or informative (explanations and clarifications)
- We will study in some detail Annex L (informative): Examples of encoding a frame for OFDM PHYs
- The list of definitions, acronyms, and abbreviations (clause 3) is included

Basic Architecture of 802.11 networks

- The basic element is the wireless **station** (STA)
- STA is the addressable unit described by the set of physical and operational characteristics.
- The **basic service set** (BSS) is the basic building block of an IEEE 802.11 LAN.

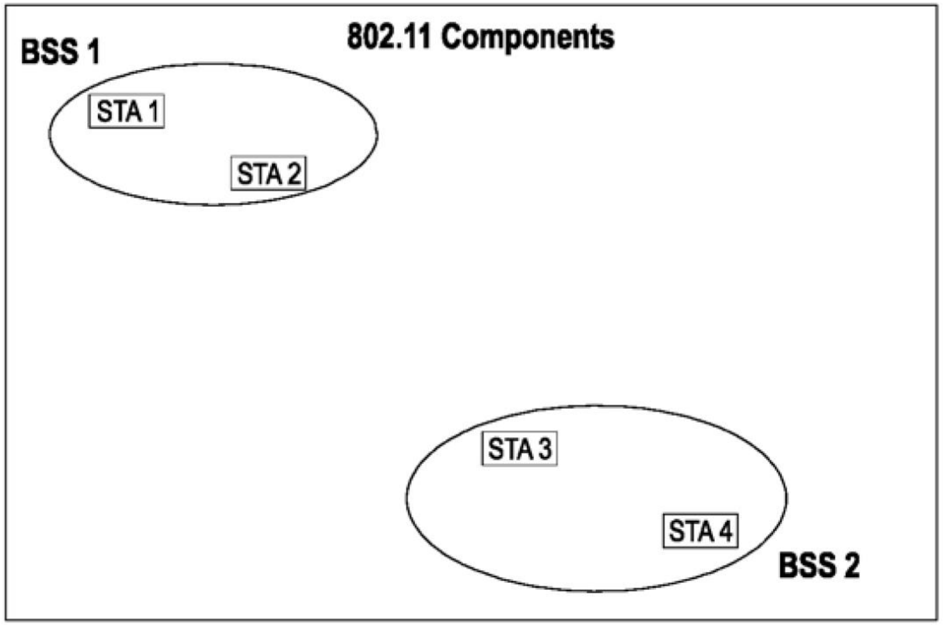


Figure 4-1—BSSs

- Figure 4-1 shows two BSSs, each of which has two STAs that are members of the BSS.
- The ovals represents the **coverage area** within which the member STAs of the BSS may communicate.

Independent and Infrastructure BSSs

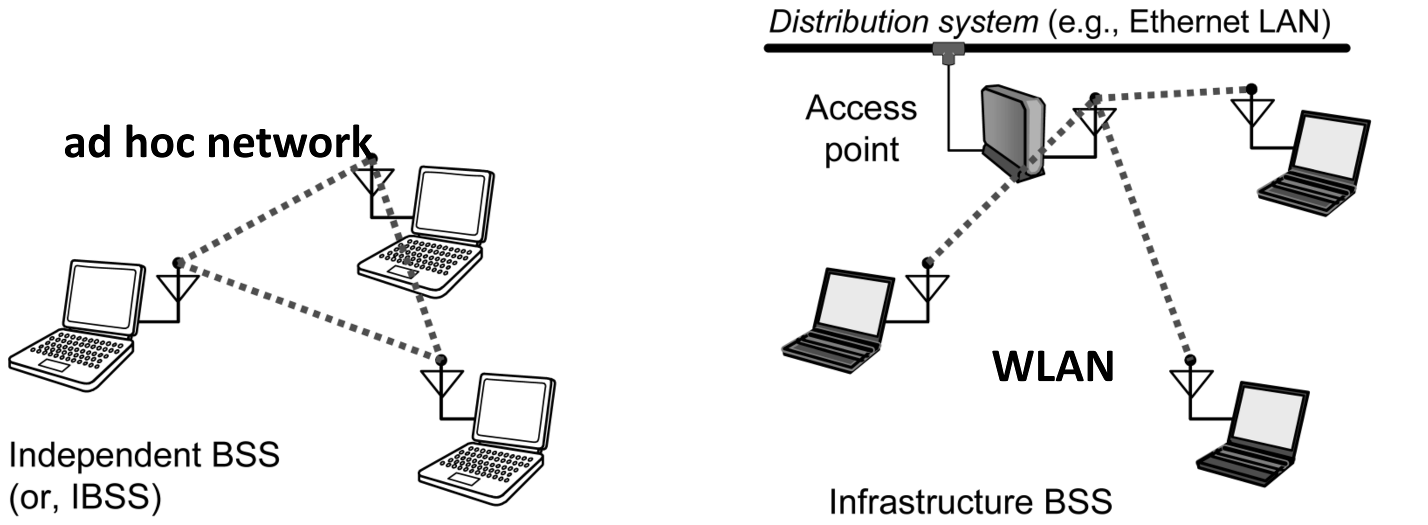


Figure 1-68: IEEE 802.11 (Wi-Fi) independent and infrastructure basic service sets (BSSs).

- The simplest type of IEEE 802.11 network is called an **Independent Basic Service Set** (IBSS) aka **ad hoc network**.
- All stations in IBSS can communicate with each other.
- **Infrastructure BSS** aka **Wireless Local Area Network** (WLAN): all mobile stations communicate only with an **Access Point** (AP)
- Therefore, communication between mobile stations in the same BSS takes place via the access point.

Membership of a BSS

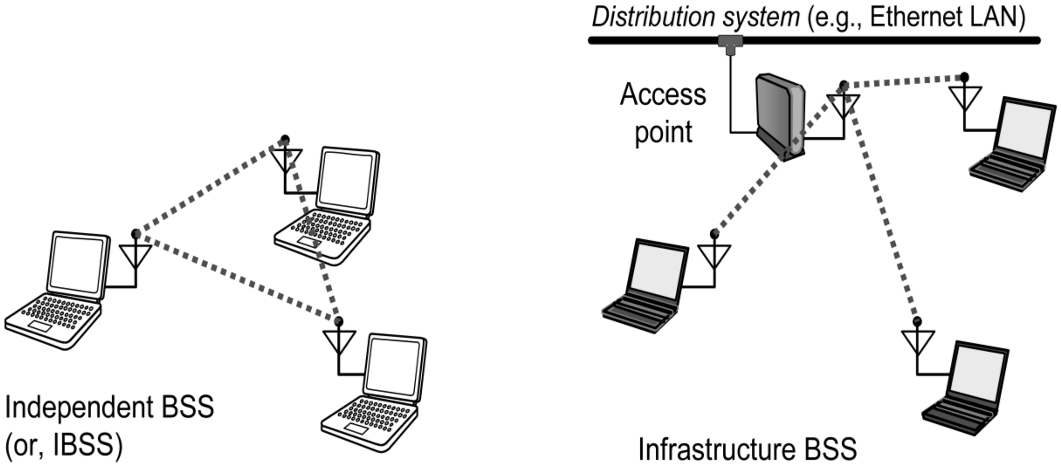

Distribution system (e.g., Ethernet LAN)
Access point
Independent BSS (or, IBSS)
Infrastructure BSS

Figure 1-68: IEEE 802.11 (Wi-Fi) independent and infrastructure basic service sets (BSSs).

- Membership of a BSS is dynamic: STAs turn on, turn off, come within the range, go out of the range.
- In general STAs and AP generate **Beacon frames** that advertise their presence and the set of operational characteristics
- To join an IBSS or an Infrastructure BSS the station follows the **synchronisation procedure**.

Components of an Infrastructure BSS

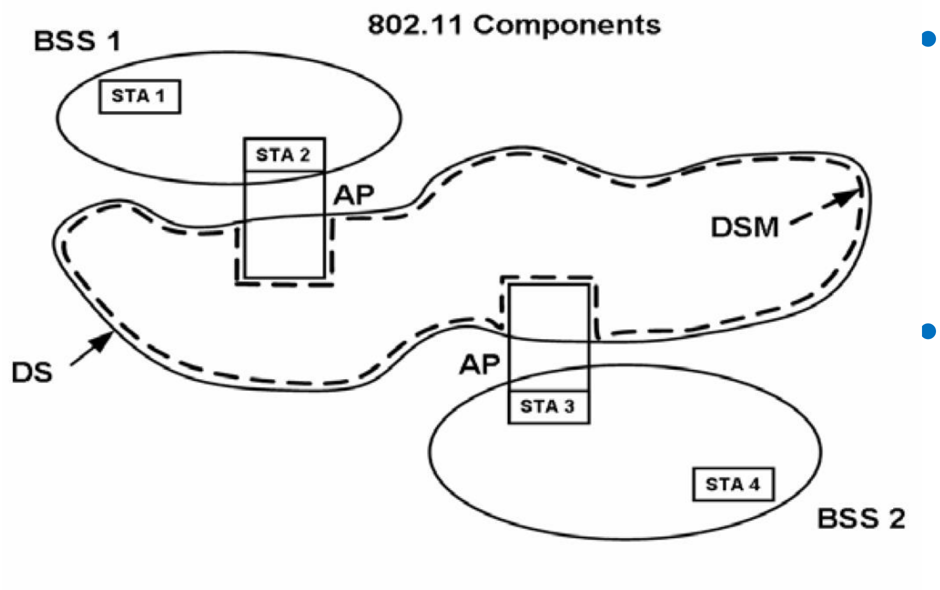
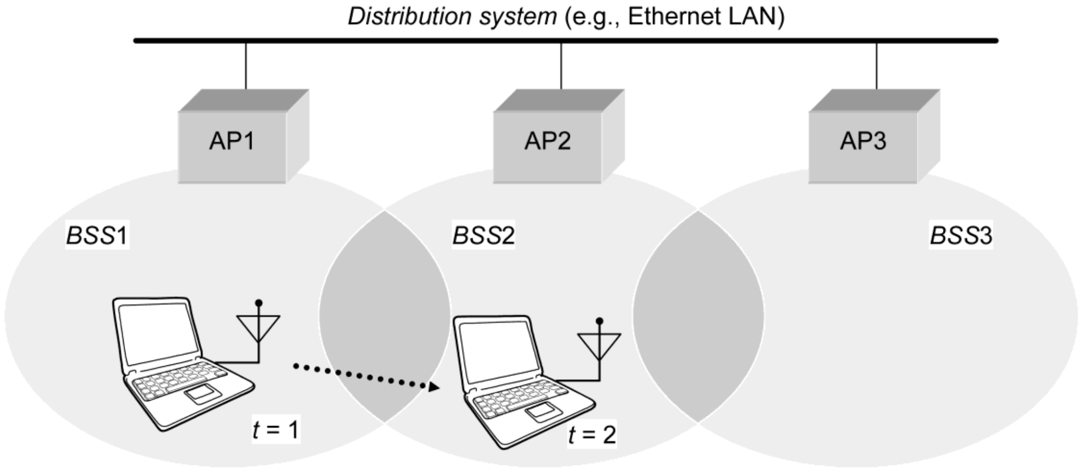


Figure 4-2—DSs and APs

- To build an infrastructure BSS we need:
  - An **Access Point** (AP)
  - A **Distribution system** DS
- The AP has all characteristics of a STA (including address) and additional features to get connected to the DS

- In other words, an access point is any entity that has STA functionality and enables access to the DS, via the **Wireless Medium** (WM) for associated STAs.
- The DS enables **mobile device support** by providing the **logical services** necessary to handle address to destination mapping and seamless integration of multiple BSSs.

Extended Service Set

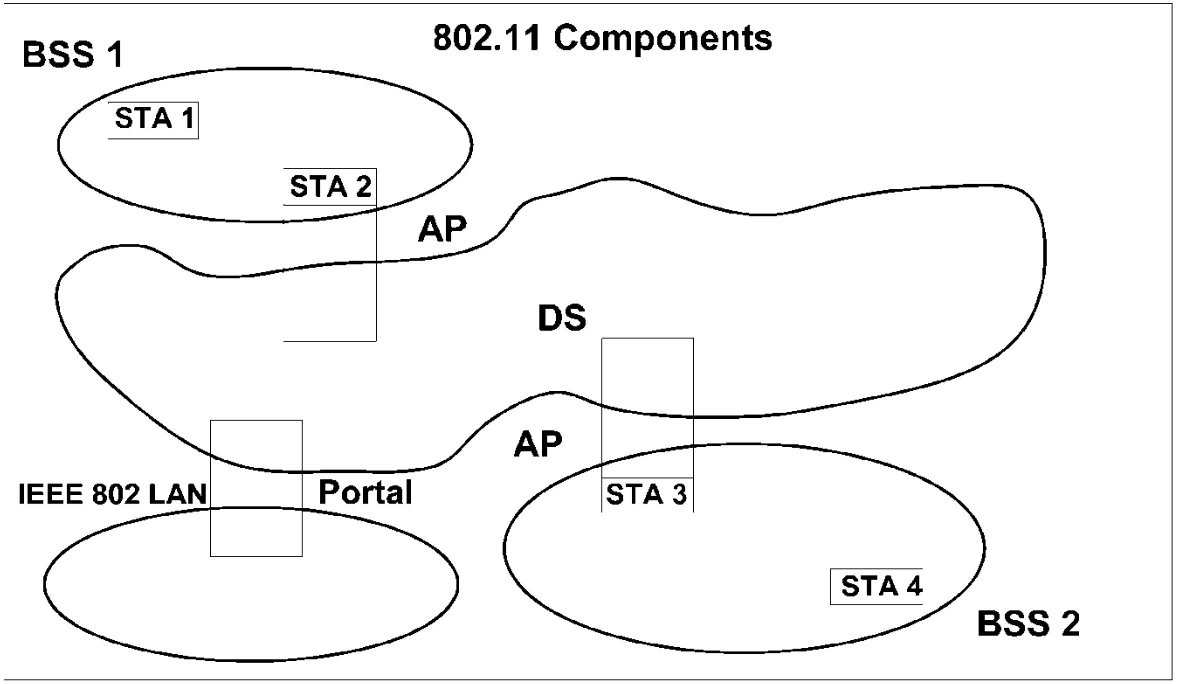


Extended service set (ESS) extends the range of mobility from a single BSS to any arbitrary range

- An ESS is a set of infrastructure BSSs, where the APs communicate among themselves via the DS in order to:
  - forward traffic from one BSS to another and
  - facilitate the roaming of mobile stations between the BSSs.
- The stations in an ESS see the wireless medium as a single layer-2 connection (e.g. Ethernet)
- Roaming between different ESSs is not supported by IEEE 802.11 and must be supported by a higher-level protocol, e.g., Mobile IP.

The portal – Integration with LANs

IEEE802.11-2012 Figure 4-6



The portal is the **logical point** at which MSDUs (MAC Service Data Unit) from an integrated non-IEEE-802.11 LAN enter the 802.11 Distribution System DS.

- The **integration service** at the portal is responsible for any addressing or frame format changes that might be required when frames pass between the DS and the integrated LAN.
- Typically the same device offers both the functions of an AP and a portal.

Subscription Service Provider Network (SSPN)

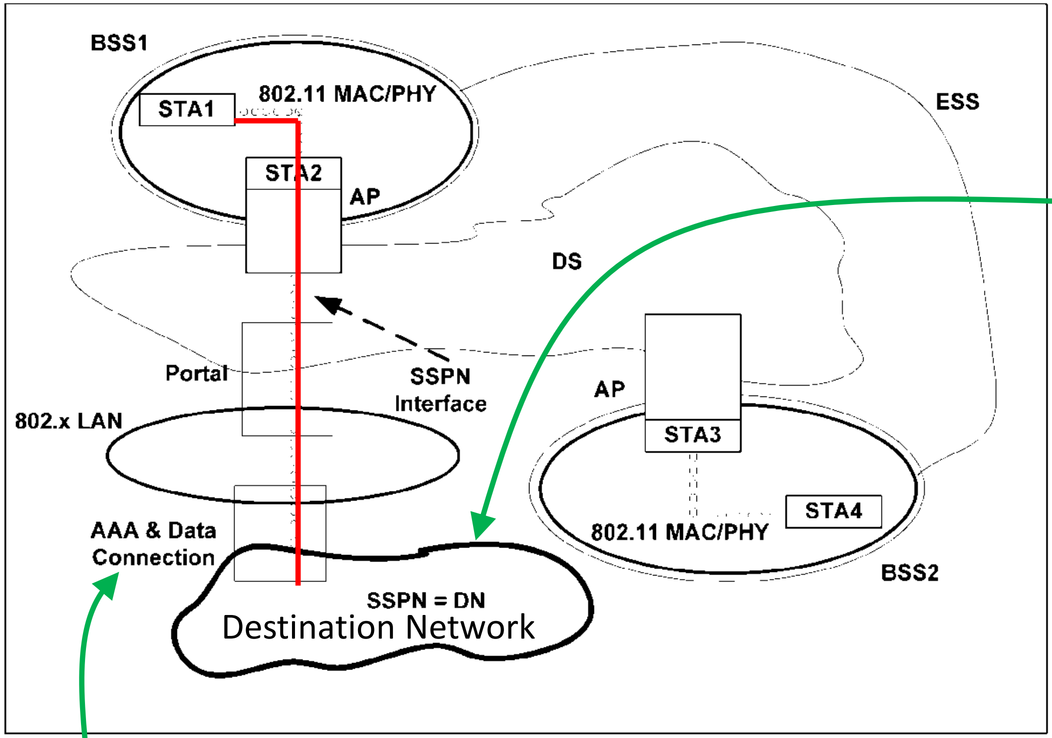


Figure 4-7—SSPN interface service architecture

- A station (STA1) might require to access a **Subscription Provider Network** (SSPN) for the services (data) it provides.
- The SSPN (DN) typically needs to authenticate and authorize the station, and charge money for the services provided.

- This is done by means of a **logical SSPN interface** that transparently connects the station through the **access point** and the **portal** to the subscription provider network and to its **AAA** (authentication, authorization and accounting) **server**.
- The protocol used to exchange this information is outside the scope of this standard.

Interworking Reference model (1)

Two layers facilitating the flow of data:

- **MAC** (Media Access Control) sublayer of the Data Link Layer
- Physical Layer (**PHY**):
  - **PLCP** (Physical Layer Convergence Procedure)
  - **PMD** (Physical Medium dependant)

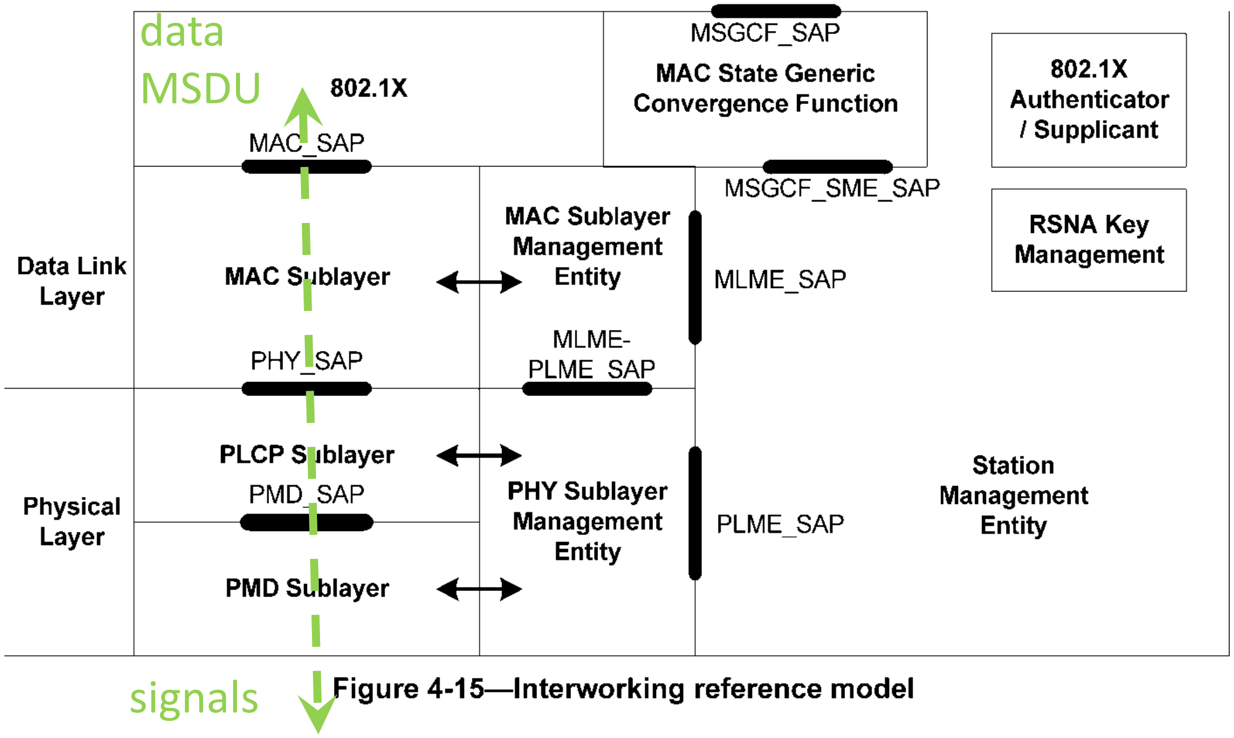


Figure 4-15—Interworking reference model

➢ Data flows through the SAPs (Service Access Points) through which the layers communicate

- MSDU – MAC layer Service Data Unit

Interworking Reference model (2)

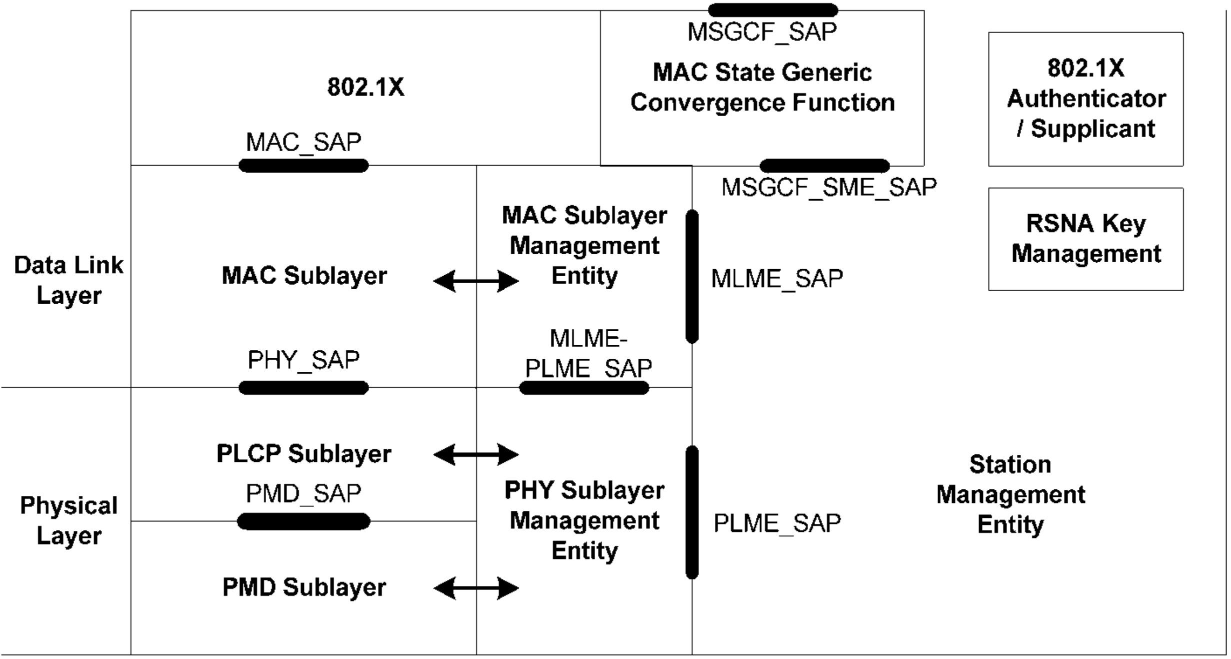


Figure 4-15—Interworking reference model

802.11X is an external data access and confidentiality protocol providing optional RSNA (Robust Security Network Association) services to the 802.11 STA

MSGCF – MAC state generic convergence function – correlates information from all management entities for the higher level entities

Two layers related Management Entities

- **MLME** (MAC subLayer Management Entity)
- **PLME** (PHY subLayer Management Entity)

SME – Station Management Entity

The management entities collect information about all aspects of data transmission and the status of the Station and set up parameters related to the station status.

Logical Service Interfaces

- IEEE Std 802.11 specifies ***services*** associated with different components of the architecture.
- There are two categories of services:
  - the station service (SS)
  - the distribution system service (DSS).

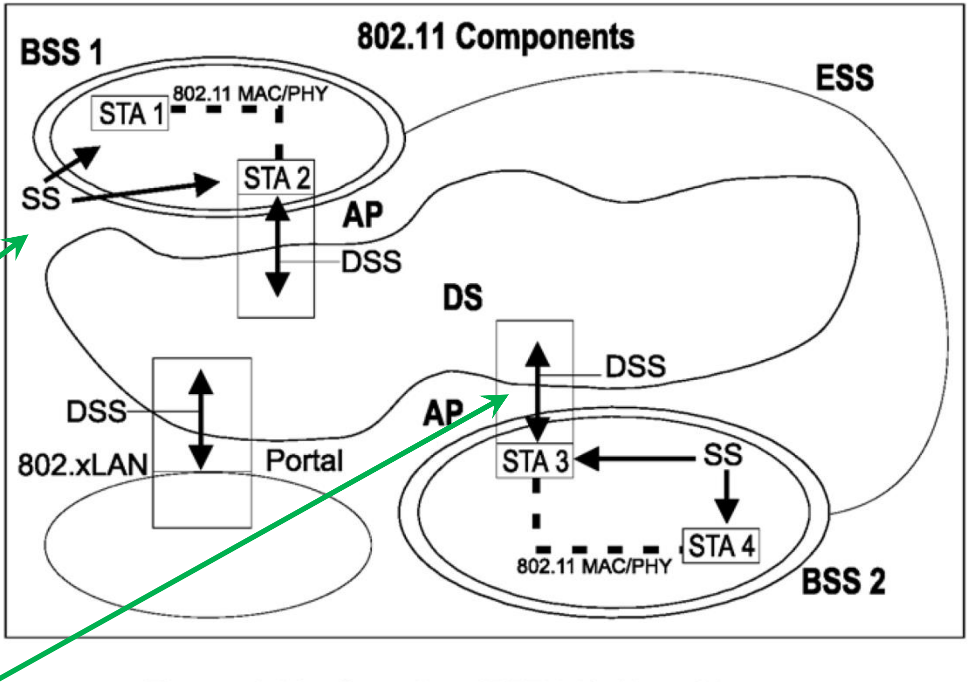


Figure 4-11—Complete IEEE 802.11 architecture

- Both categories of service are used by the MAC sublayer.

The Station (STA) Services (SS)

The SS (Station Services) are:

- present in every STA (including APs).
- specified for use by **MAC sublayer** entities.

  a) Authentication

  b) De-authentication

  c) Data confidentiality

  to control LAN access and confidentiality.

  d) MSDU delivery (MAC Service Data Unit)

  e) DFS (Dynamic Frequency Selection)

  f) TPC (Transmit Power Control)

  g) Higher layer timer synchronization (QoS facility only)

  h) QoS traffic scheduling (QoS facility only)

  QoS (Quality of Service) is related to timely delivery of packets

  i) Radio measurement

  j) DSE (Dynamic Station Enablement)

Distribution System (DS) service (DSS)

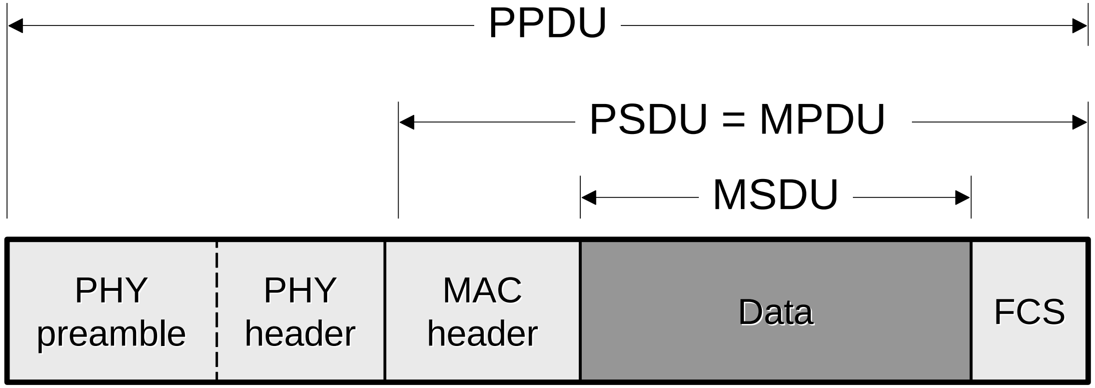
- The list of distribution system services (DSS):
  a) Association
  b) Disassociation
  c) Reassociation
  d) Distribution
  e) Integration
  f) QoS traffic scheduling (QoS facility only)
  g) DSE (dynamic station enablement)

Connection between STAs, AP, DS

Overview of the services

- Each of the services is supported by one or more **MAC frame** types.
- Some of the services are supported by MAC management messages and some by MAC data messages.
- All of the messages gain access to the WM via the MAC sublayer **medium access method**
- The MAC sublayer uses three types of messages (and related frames): — *data*, *management*, and *control*
- The **data messages** are handled via the MAC data service path.
- MAC **management messages** are handled via the MAC management service path.
- MAC **control messages** are used to support the delivery of data and management messages.

Structure of the MAC and PHY frames:



PPDU

PSDU = MPDU

MSDU

PHY preamble | PHY header | MAC header | Data | FCS

Key:

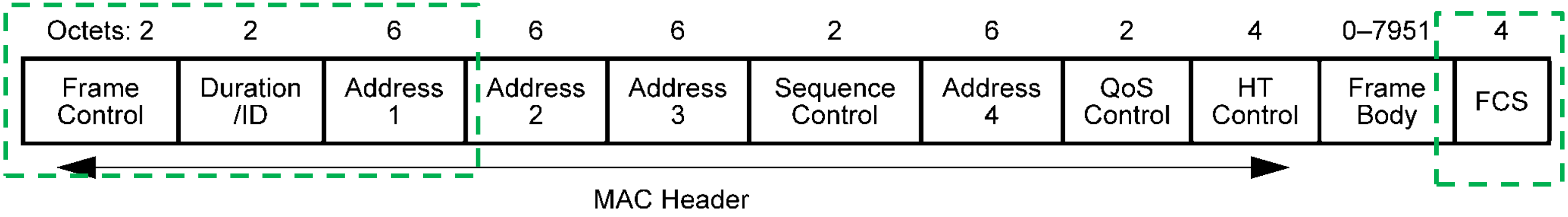
PPDU = PLCP protocol data unit
PSDU = PLCP service data unit
MPDU = MAC protocol data unit
MSDU = MAC service data unit

PLCP = physical (PHY) layer convergence procedure
MAC = medium access control

- MSDU with the MAC header and the FCS (Frame Check Sequence) form the MPDU
- MPDU is a Service Data Unit for the Physical Layer – PSDU
- PSDU with the header and the preamble prepended form the Protocol Data Unit PPDU
- MSDU length is not more than 2304/7951 bytes.
- MSDU frames can be aggregated to form a larger A-MSDU frame

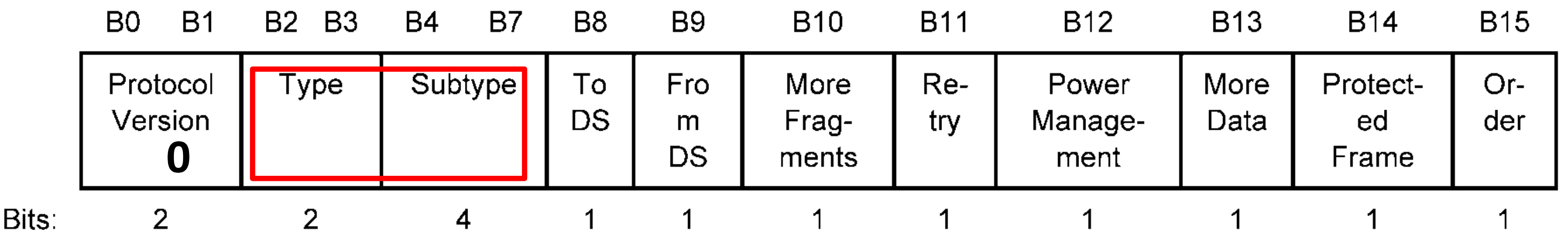
General MAC Frame format

Figure 8.1



Octets: 2	2	6	6	6	2	6	2	4	0–7951	4
Frame Control	Duration /ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	QoS Control	HT Control	Frame Body	FCS

- The first three fields (Frame Control, Duration/ID, and Address 1), 10 bytes, and the last field (FCS), 4 bytes, constitute the minimal frame format and are present in all frames.
- The fields Address 2, Address 3, Sequence Control, Address 4, QoS Control, HT Control, and Frame Body are present only in certain frame types and subtypes.
- There are three general types of frames related to three types of services and specified by 6 bits from the **Frame Control** field
  - Data Frames
  - Control Frames
  - Management Frames



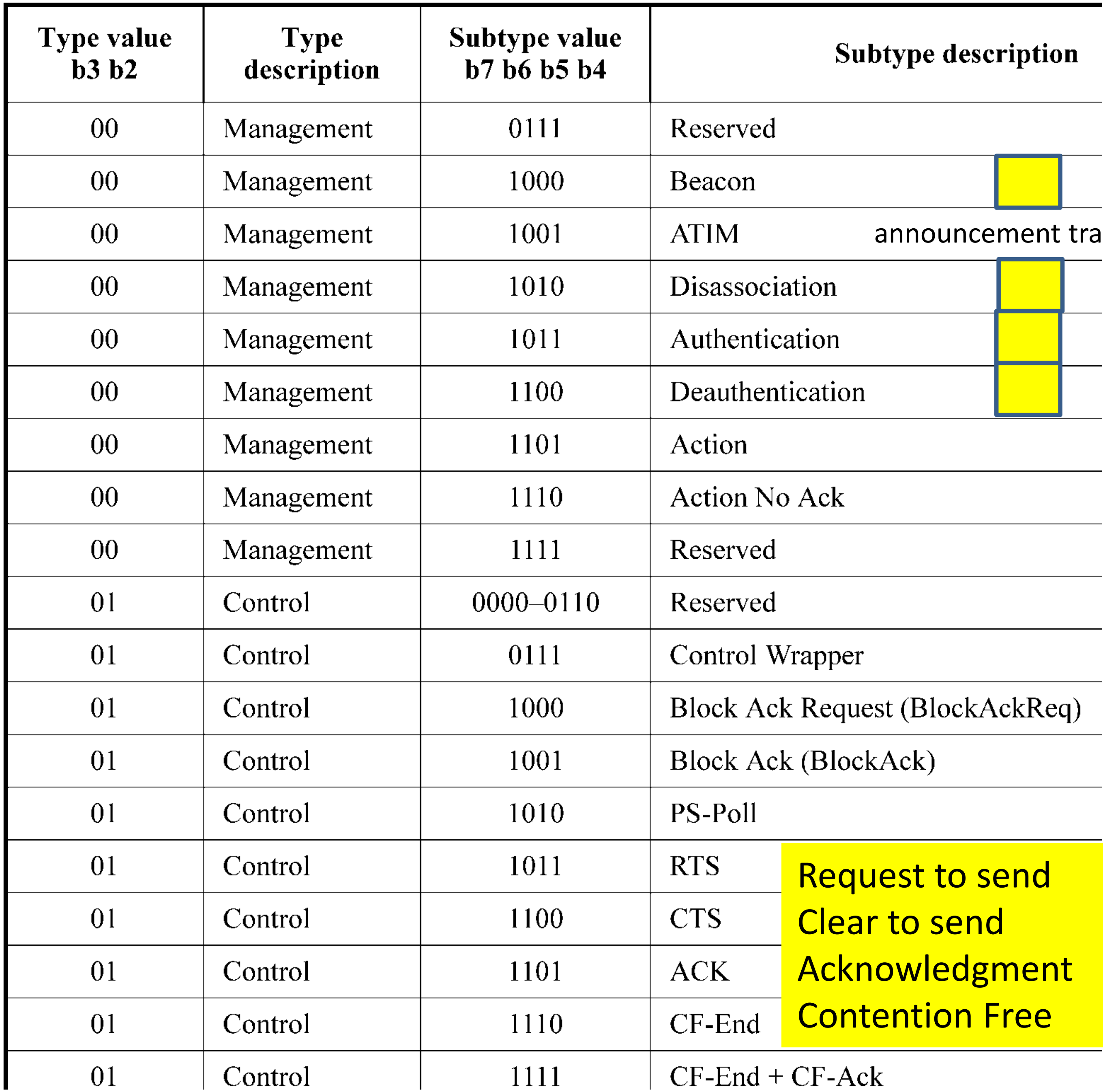
	B0 B1	B2 B3	B4 B7	B8	B9	B10	B11	B12	B13	B14	B15
	Protocol Version **0**	Type	Subtype	To DS	Fro m DS	More Frag- ments	Re- try	Power Manage- ment	More Data	Protect- ed Frame	Or- der
Bits:	2	2	4	1	1	1	1	1	1	1	1

Figure 8-2—Frame Control field

- Type-Subtype (6 bits) identify the function of the frame

Table 8-1—Valid type and subtype combinations

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
00	Management	0000	Association request
00	Management	0001	Association response
00	Management	0010	Reassociation request
00	Management	0011	Reassociation response
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	0110	Timing Advertisement

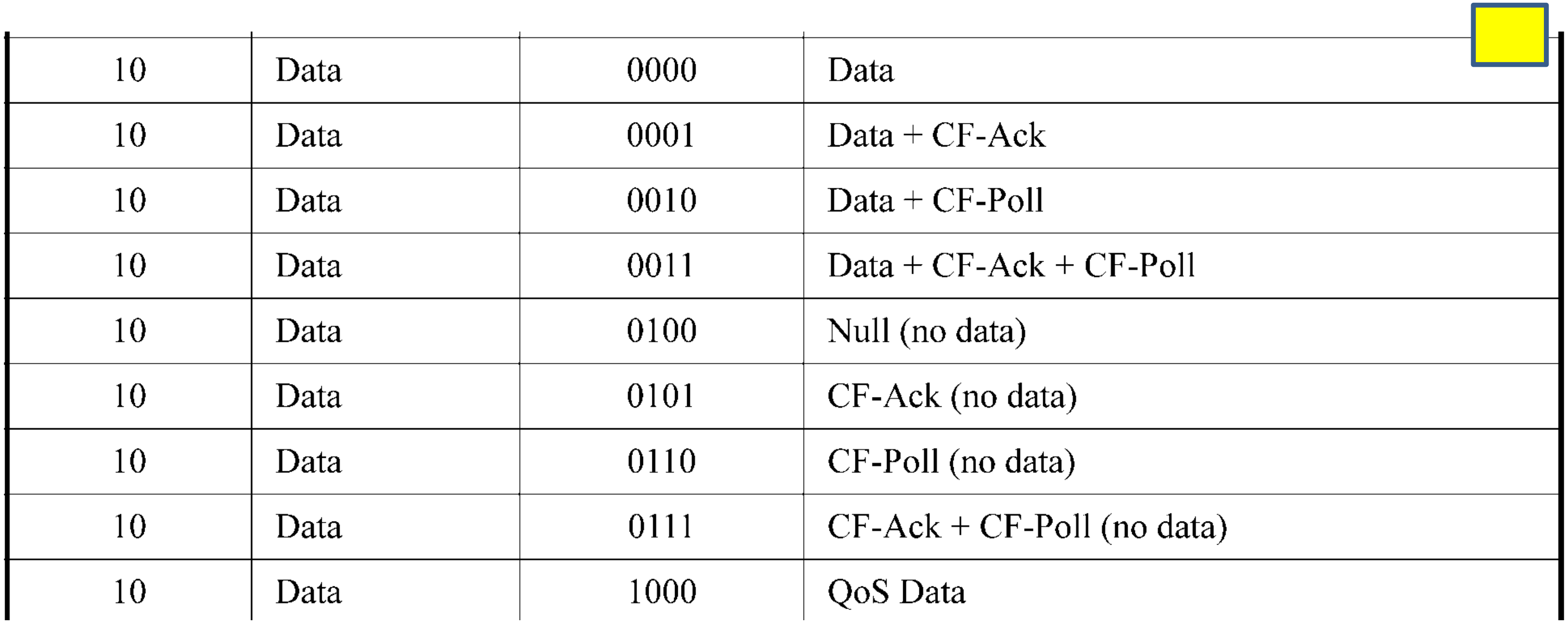


Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
00	Management	0111	Reserved
00	Management	1000	Beacon
00	Management	1001	ATIM
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101	Action
00	Management	1110	Action No Ack
00	Management	1111	Reserved
01	Control	0000–0110	Reserved
01	Control	0111	Control Wrapper
01	Control	1000	Block Ack Request (BlockAckReq)
01	Control	1001	Block Ack (BlockAck)
01	Control	1010	PS-Poll
01	Control	1011	RTS
01	Control	1100	CTS
01	Control	1101	ACK
01	Control	1110	CF-End
01	Control	1111	CF-End + CF-Ack

announcement traffic indication message

Request to send
Clear to send
Acknowledgment
Contention Free

Data Frames



10	Data	0000	Data
10	Data	0001	Data + CF-Ack
10	Data	0010	Data + CF-Poll
10	Data	0011	Data + CF-Ack + CF-Poll
10	Data	0100	Null (no data)
10	Data	0101	CF-Ack (no data)
10	Data	0110	CF-Poll (no data)
10	Data	0111	CF-Ack + CF-Poll (no data)
10	Data	1000	QoS Data

MAC Frame Control and the Duration/ID Fields

(ignore in first reading)

ToDS
FromDS

Indicate whether a data frame is headed for a DS.

Control and management frames set these values to zero.

All the data frames will have one of these bits set.

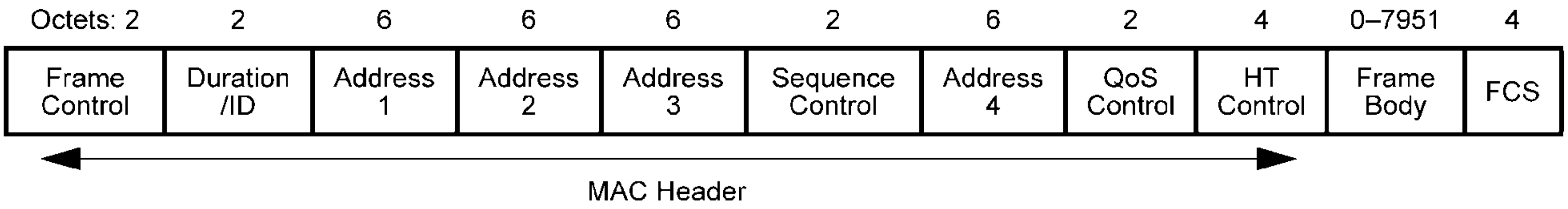
Communication within an IBSS network always set these bits to zero.

1 bit fields: More Fragments, Retry, Power Management, More Data, Protected Frame, Order (read about it)

2 bytes – Duration/ID field -- one of three forms:

Duration,
Contention-Free Period (CFP)
Association ID (AID)

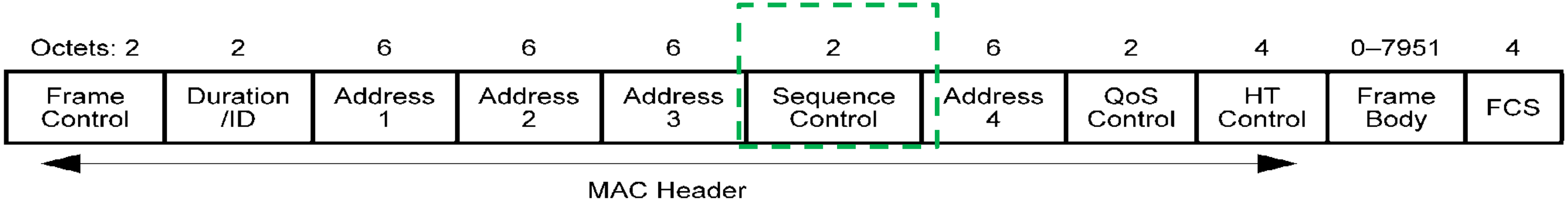
Address fields



Octets: 2	2	6	6	6	2	6	2	4	0–7951	4
Frame Control	Duration /ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	QoS Control	HT Control	Frame Body	FCS

- There are (at least) five different addressing information data used in exchange of frames:
  - the basic service set identifier (**BSSID**),
  - source address (**SA**),
  - destination address (**DA**),
  - transmitting STA address (**TA**),
  - receiving STA address (**RA**).
- The above addressing information is distributed in the four address fields available in the MAC frames
- Not all frames use all the address fields.
- Allocation of the addressing information to the address fields varies according to a specific frame type.

More MAC frame fields:

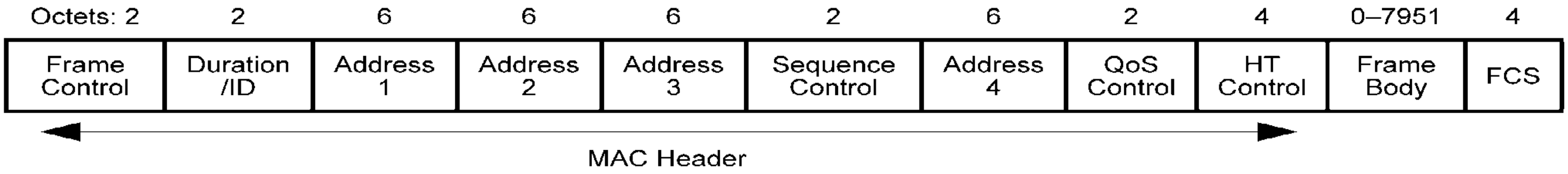


Octets: 2	2	6	6	6	2	6	2	4	0–7951	4
Frame Control	Duration /ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	QoS Control	HT Control	Frame Body	FCS

MAC Header

- The **Sequence Control** field is a two-byte section used for identifying message order as well as eliminating duplicate frames.
- The first 4 bits are used for the fragment number and the last 12 bits are the sequence number.
- An optional two-byte **Quality of Service** control field
- 4-byte HT (High Throughput) Control Field (used in .11n and up)

More MAC frame fields:



Octets: 2	2	6	6	6	2	6	2	4	0–7951	4
Frame Control	Duration /ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	QoS Control	HT Control	Frame Body	FCS

MAC Header

- The **Frame Body** field is variable in size, from 0 to 2304/7951 bytes plus any overhead from security encapsulation, plus possible **Mesh Control Field.**
- The **Frame Check Sequence** (FCS) aka the **Cyclic Redundancy Check** (CRC), is used to detect errors in the retrieved frames. (see sec. 8.2.4.8 FCS Field on Moodle)
- As frames are about to be sent the FCS is calculated and appended.
- When a station receives a frame it calculates the FCS of the frame and compare it to the one received.
- If they match, it is assumed that the frame was not distorted during transmission.

Beacon and the Probe Request Frames

- **Beacon frame:** is sent periodically from an access point to announce its presence and provide the SSID, and other parameters for STA/WNICs within range.
- **Probe request frame:** is sent from a station when it requires information from another station.
- **Probe response frame:** is sent back to the requesting STA and contains capability information, supported data rates, etc.
- In general every STA performs Radio Measurements to observe and gather data on radio link performance and on the radio environment.

Control Frames – ACK

- Control frames facilitate in the exchange of data frames between stations. Some common 802.11 control frames include:

Acknowledgement (ACK) frame:

- After receiving a data frame, the receiving station will send an ACK frame to the sending station if no errors are found.
- If the sending station doesn't receive an ACK frame within a predetermined period of time, the sending station will resend the frame.

Control Frames – RTS, CTS

- **Request to Send (RTS)** frame: The RTS and CTS frames provide an **optional collision reduction scheme** for access point with **hidden stations**.
- A station sends an RTS frame to an STA as the first step in a two-way handshake required before sending data frames.
- **Clear to Send (CTS)** frame: A station responds to an RTS frame with a CTS frame.
- It provides clearance for the requesting station to send a data frame.
- The CTS provides collision control management by including a **time value for which all other stations are to hold off** transmission while the requesting stations transmits.

Distribution (1)

- This is the primary service delivered by DS and used by STAs
- It is conceptually invoked by **every data message** to or from an STA operating **in an ESS** (when the frame is sent via the DS).

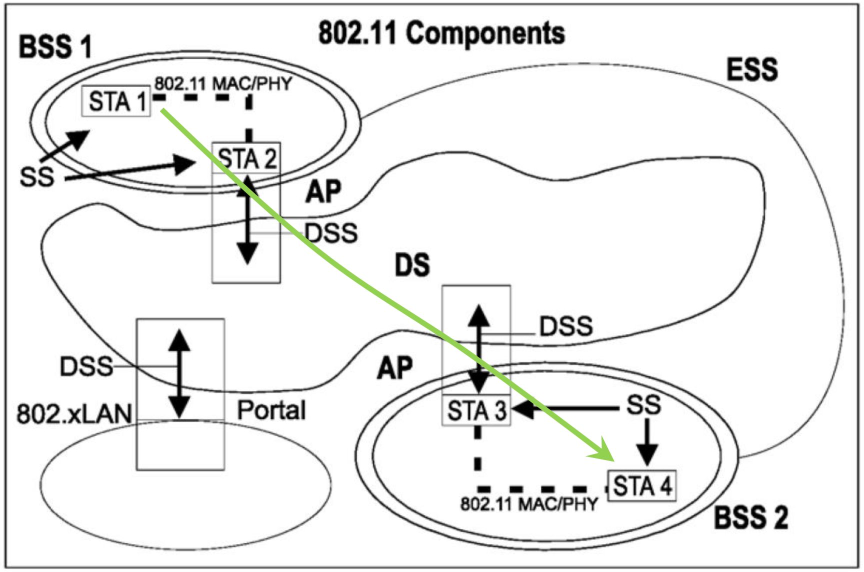


Figure 4-11—Complete IEEE 802.11 architecture

- Consider a data message being sent from STA 1 (BSS1) to STA 4 (BSS2)
- The message is sent from STA 1 and received by STA 2 (the “input” AP).
- The AP gives the message to the distribution service of the DS.

- It is the job of the distribution service to deliver the message within the DS in such a way that it arrives at the appropriate DS destination for the intended recipient.

Distribution (2)

- In this example, the message is distributed to STA 3 (the "output" AP) and STA 3 accesses the WM to send the message to STA 4 (the intended destination).
- How the message is distributed within the DS is not specified by IEEE Std 802.11.
- All IEEE Std 802.11 is required to do is to provide the DS with enough information for the DS to be able to determine the "output" point that corresponds to the intended recipient.
- The necessary information is provided to the DS by the three **association related services** (association, reassociation, and disassociation).

Integration (through a portal)

- If the distribution service determines that the intended recipient of a message is a member of an integrated LAN, the “output” point of the DS would be a **portal** instead of an AP.
- Messages that are distributed to a portal invoke the Integration service (conceptually after the distribution service).
- The Integration service is responsible for delivering a message from the DSMedia to the integrated LAN media (including any required media or address space translations).
- Messages received from an integrated LAN (via a portal) by the DS for an IEEE 802.11 STA invoke the Integration service before the message is distributed by the distribution service.

Association

- To deliver a message within a DS, the distribution service needs to know which AP to access for the given STA.
- Before a STA is allowed to send a data message via an AP, it first **becomes associated with the AP.**
- The association service provides the **STA to AP mapping** to the DS.
- The DS uses this information to accomplish its message distribution service.
- An STA learns what APs are present and what operational capabilities are available from each of those APs and then invokes the association service to establish an association.

Association Frames

- **Association request frame:** is sent from a station.
- It enables the access point to allocate resources and synchronize.
- The frame carries information about the STA including **supported data rates** and the **SSID** of the network the station wishes to associate with.
- If the request is accepted, the Access Point reserves memory and establishes an **association ID** for the STA.
- **Association response frame:** is sent from an Access Point to a station containing the acceptance or rejection to an association request.
- If it is an acceptance, the frame will contain information such as an **association ID** and **supported data rates**.

Reassociation

- Reassociation is needed to support the mobility of STA between BSS belonging to an ESS
- The reassociation service is invoked to “move” a current association from one AP to another.
- This keeps the DS informed of the current mapping between AP and STA as the STA moves from BSS to BSS within an ESS.
- Reassociation also enables changing association attributes of an established association while the STA remains associated with the same AP.
- Reassociation is always initiated by the mobile STA.

Disassociation

- The disassociation service is invoked when an existing association is to be terminated.
- In an ESS, this tells the DS to void existing association information.
- The disassociation service may be invoked by either party to an association (non-AP STA or AP).
- APs may disassociate STAs to enable the AP to be removed from a network for service or for other reasons.
- STAs attempt to disassociate when they leave a network.
- However, the MAC protocol does not depend on STAs invoking the disassociation service.
- (MAC management is designed to accommodate loss of communication with an associated STA.)

Access control and data confidentiality services

- Two services, access control and data confidentiality, are required for 802.11 to provide functionality equivalent to wired LANs.
- A **wired LAN** design assumes the physically closed and controlled nature of wired media which is not the case in an 802.11 WLAN
- One option is to use an external **RSNA** (Robust Security Network Association) based on the IEEE 802.1X services.
- The IEEE 802.11 station management entity (SME) provides authentication key management via an exchange of IEEE 802.1X EAPOL-Key frames. (Extensible Authentication Protocol over LANs)
- Data confidentiality and data integrity are provided by RSN key management together with the enhanced data cryptographic encapsulation mechanisms.

802.11 authentication and data confidentiality

- 802.11 authentication (an SS – STA service) operates at the link level between 802.11 STAs.
- 802.11 does not provide either end-to-end (message origin to message destination) or user-to-user authentication.
- The authentication service may be used by all STAs to establish their identity to STAs with which they communicate, in both ESS and IBSS networks.
- If a mutually acceptable level of authentication has not been established between two STAs, an association is not established.
- IEEE 802.11 defines four 802.11 authentication methods:
  - Open System authentication,
  - Shared Key authentication,
  - FT (fast transition) authentication,
  - simultaneous authentication of equals (SAE).

802.11 authentication methods

1. Open System authentication admits any STA to the DS.
2. Shared Key authentication relies on WEP to demonstrate knowledge of a WEP encryption key.
3. FT authentication relies on keys derived during the initial mobility domain association to authenticate the stations (Clause 12).
4. SAE authentication uses finite field cryptography to prove knowledge of a shared password.

- The IEEE 802.11 authentication mechanism also allows definition of new authentication methods.

802.11 Data Confidentiality

- By default STAs send unprotected frames
- The encryption is provided by the station’s confidentiality service
- IEEE Std 802.11 provides several cryptographic algorithms to protect data traffic, including: WEP, TKIP, and CCMP.
- WEP and TKIP are based on the ARC4 algorithm,
- CCMP is based on the advanced encryption standard (AES).
- A means is provided for STAs to select the algorithm(s) to be used for a given association.
- IEEE Std 802.11 provides one security protocol, CCMP, for protection of individually addressed robust management frames.

End of today’s Lecture 4 – Wireless LAN PART 1

Next week’s lecture 5 – Wireless LAN PART 2