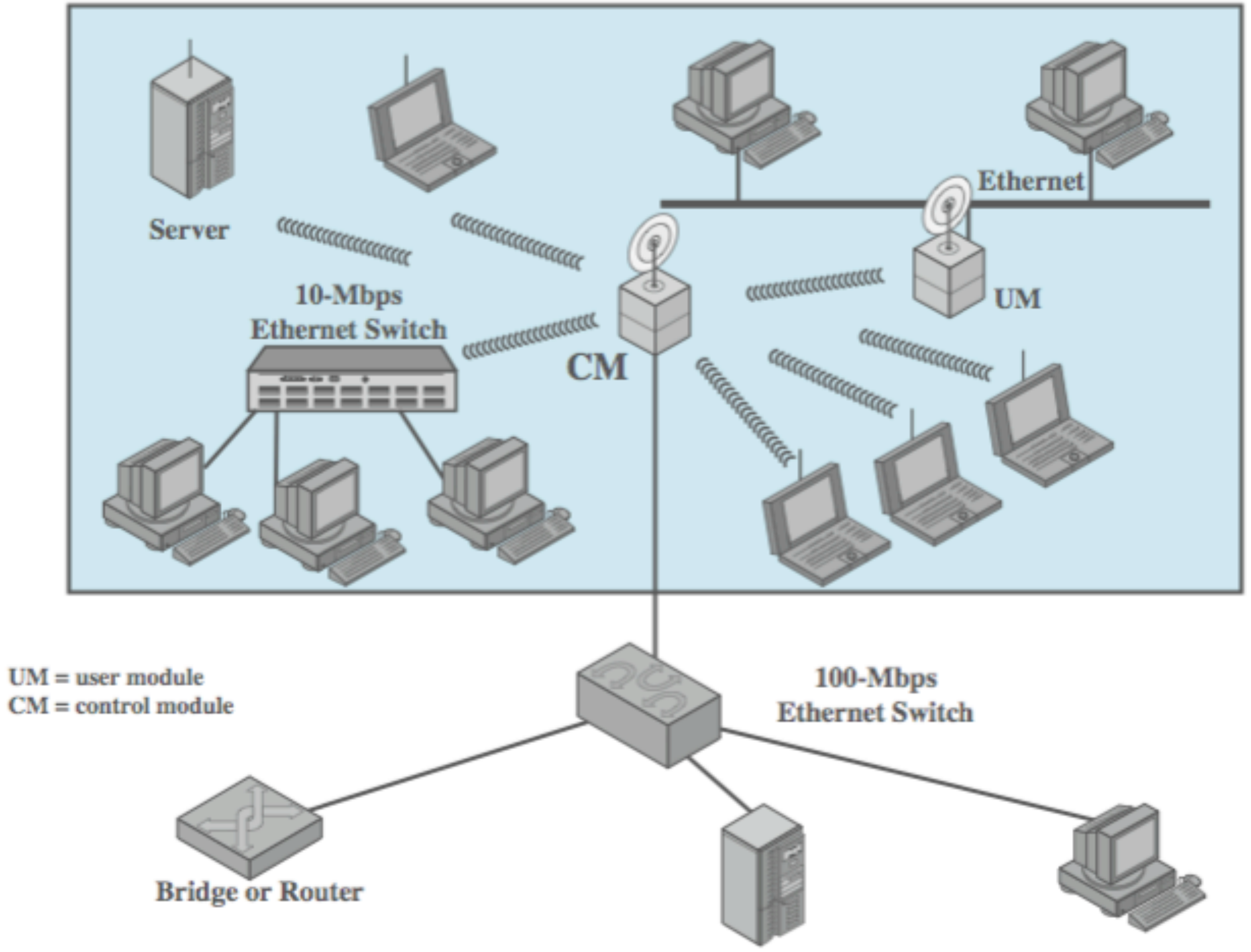
Wireless LANs

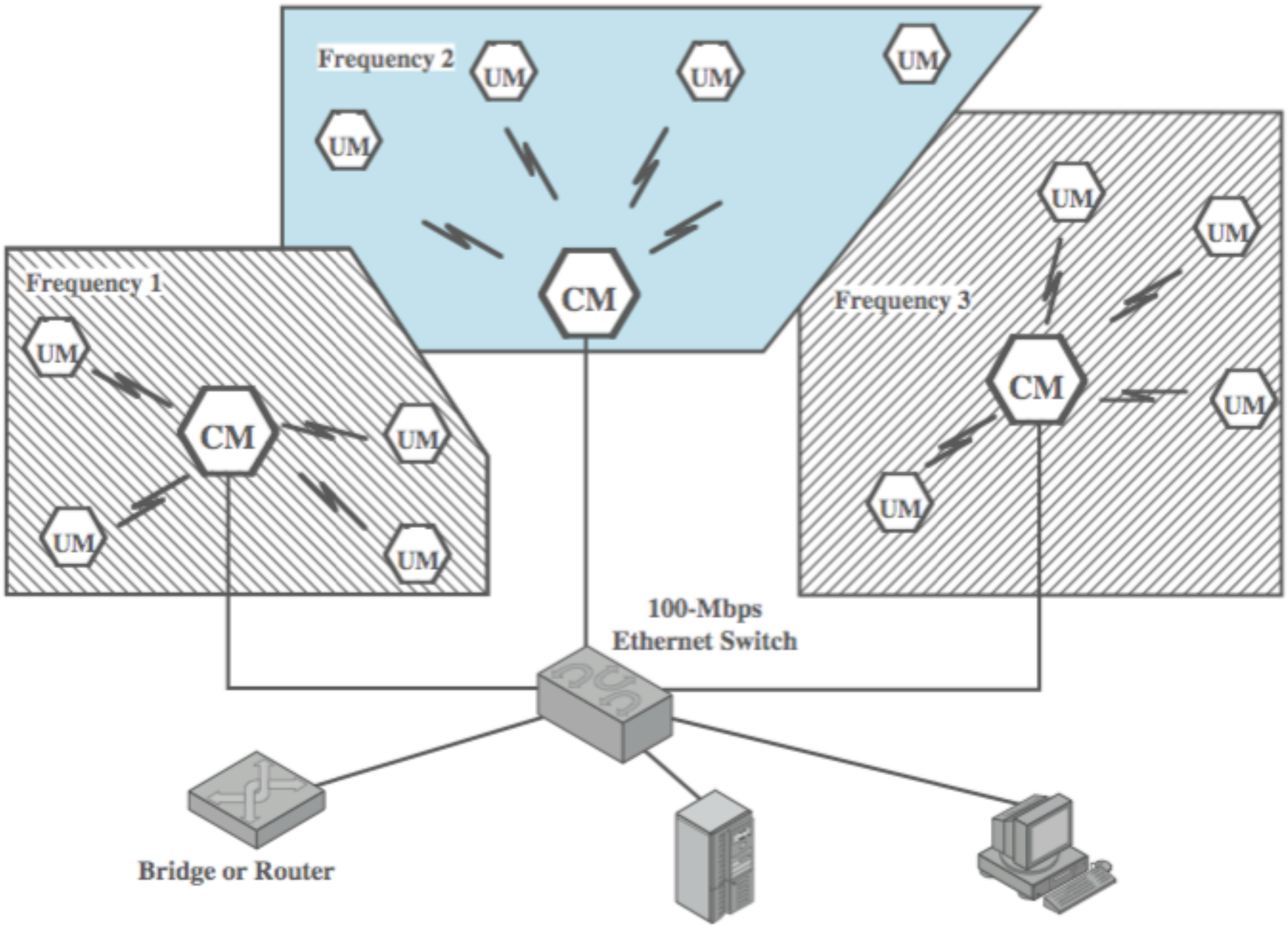
Overview of Wireless LANs

- use wireless transmission medium
- issues of high prices, low data rates, occupational safety concerns, & licensing requirements now addressed
- key application areas:
  - LAN extension
  - cross-building interconnect
  - nomadic access
  - ad hoc networking

Single Cell LAN Extension



Multi Cell LAN Extension



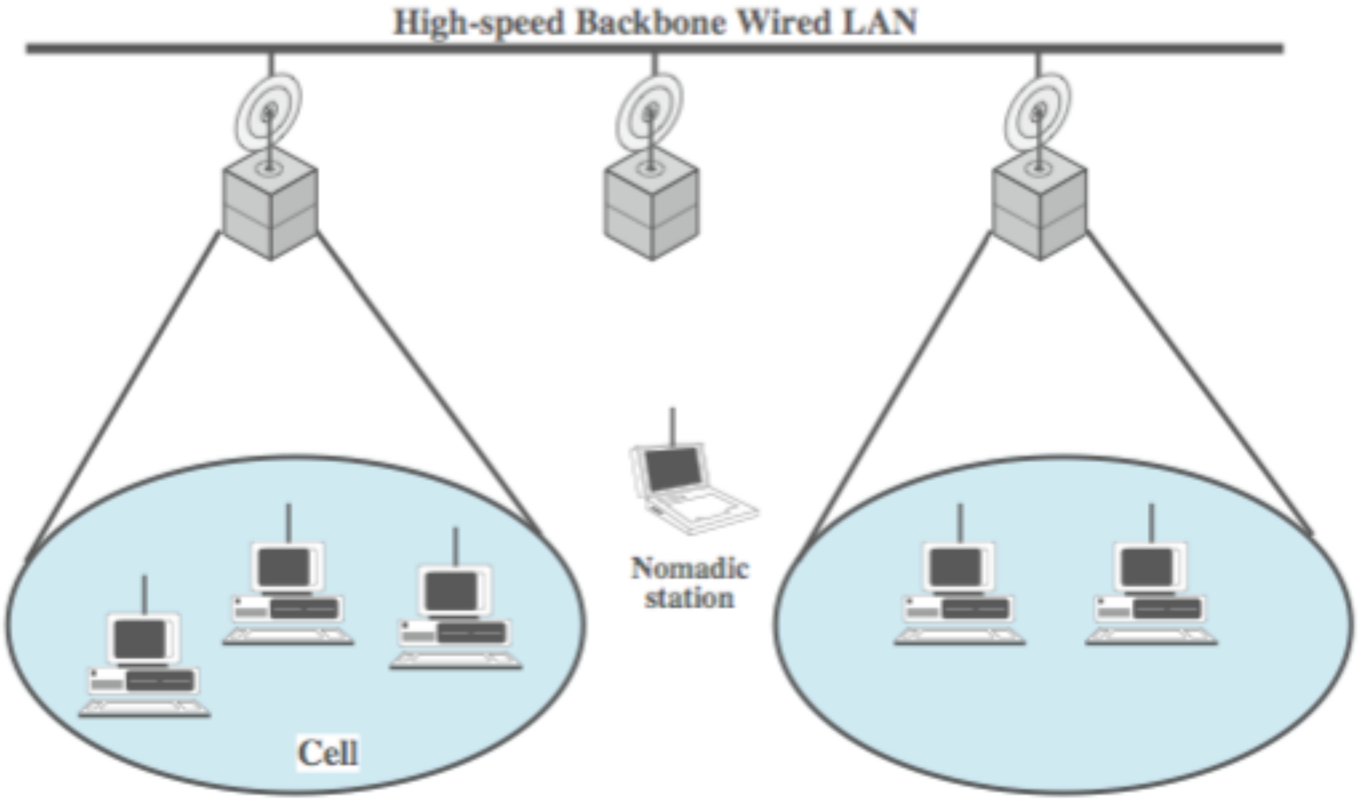
Cross-Building Interconnect

- connect LANs in nearby buildings
- point-to-point wireless link
    - Not a LAN per se
- connect bridges or routers

Nomadic Access

- link LAN hub & mobile data terminal
  - laptop or notepad computer
  - enable employee to transfer data from portable computer to server
- also useful in extended environment such as campus or cluster of buildings
  - users move around with portable computers
  - may wish access to servers on wired LAN

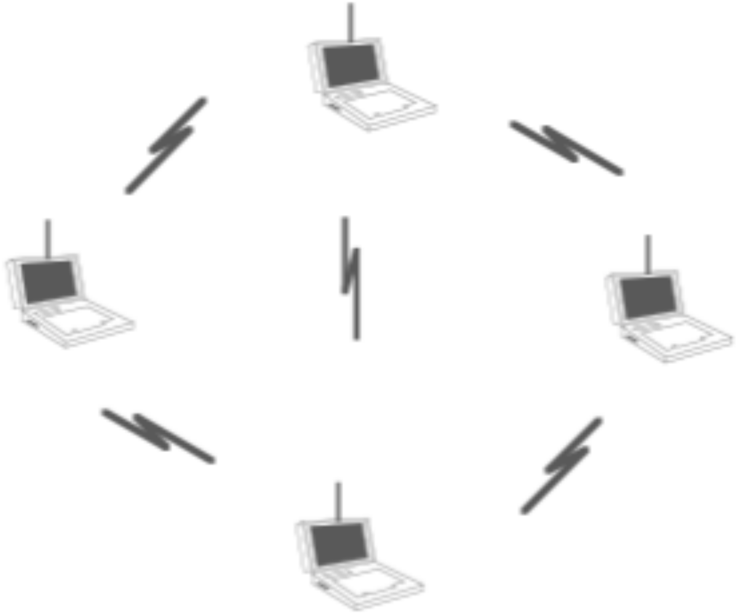
Infrastructure Wireless LAN



(a) Infrastructure Wireless LAN

Ad Hoc Networking

- temporary peer-to-peer network



(b) Ad hoc LAN

Wireless LAN Requirements

- throughput - efficient use wireless medium
- no of nodes - hundreds of nodes across multiple cells
- connection to backbone LAN - using control modules
- service area - 100 to 300 m
- low power consumption - for long battery life on mobiles
- transmission robustness and security
- collocated network operation
- license-free operation
- handoff/roaming
- dynamic configuration - addition, deletion, and relocation of end systems without disruption to users

Technology

- infrared (IR) LANs
  - individual cell of IR LAN limited to single room
  - IR light does not penetrate opaque walls
- spread spectrum LANs
  - mostly operate in ISM (industrial, scientific, and medical) bands
  - no Federal Communications Commission (FCC) licensing is required in USA
- narrowband microwave
  - microwave frequencies but not use spread spectrum
  - some require FCC licensing

Infrared LANs

- constructed using infrared portion of spectrum
- strengths
  - spectrum virtually unlimited hence high rates possible
  - unregulated spectrum
  - infrared shares some properties of visible light
    - reflection covers room, walls isolate networks
  - inexpensive and simple
- weaknesses
  - background radiation, e.g. sunlight, indoor lighting
  - power limited by concerns for eye safety and power consumption

Infrared LANs
Transmission Techniques

- directed-beam IR
  - point-to-point links
  - range depends on power and focusing
  - for indoor use can set up token ring LAN
  - IR transceivers positioned so data circulates in ring
- omnidirectional
  - single base station with line of sight to other stations
  - acts as a multiport repeater
  - other stations use directional beam to it
- diffused configuration
  - stations focused / aimed at diffusely reflecting ceiling

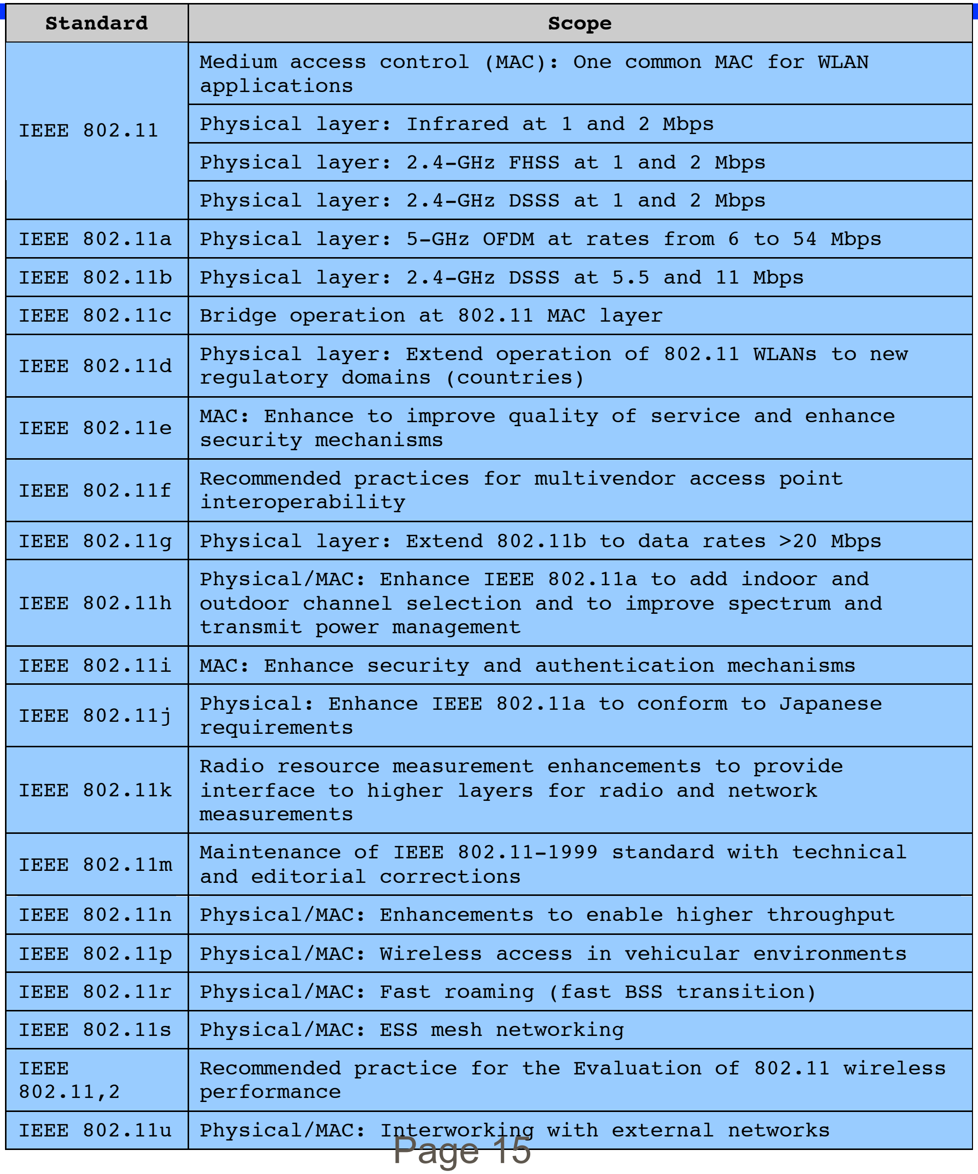
Spread Spectrum LAN Configuration

- usually use multiple-cell arrangement
- adjacent cells use different center frequencies
- configurations:
  - hub
    - connected to wired LAN
    - connect to stations on wired LAN and in other cells
    - may do automatic handoff
  - peer-to-peer
    - no hub
    - MAC algorithm such as CSMA used to control access
    - for ad hoc LANs

Spread Spectrum LANs Transmission Issues

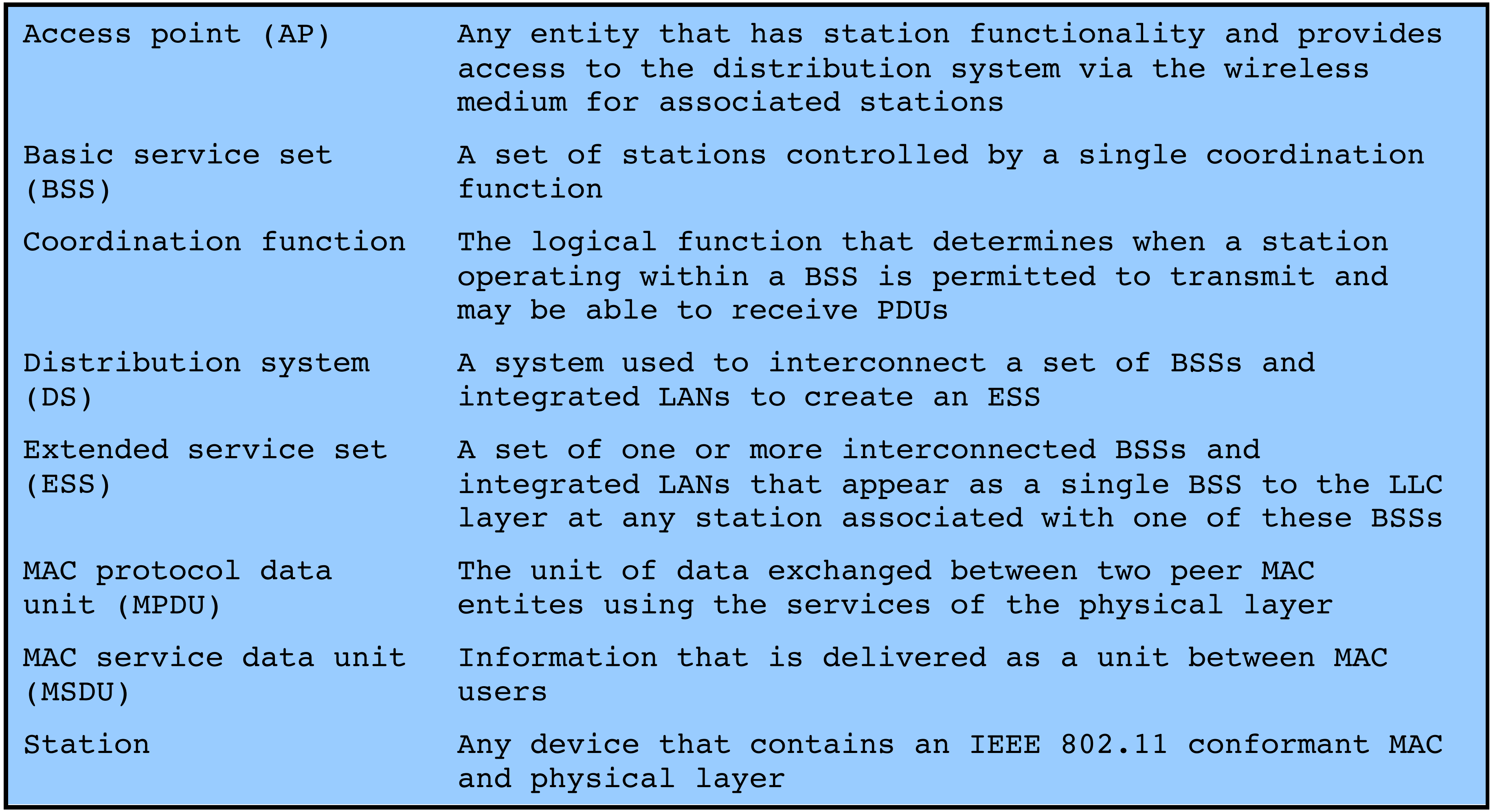
- licensing regulations differ between countries
- USA FCC allows in ISM band:
  - —spread spectrum (1W), very low power (0.5W)
    - 902 - 928 MHz (915-MHz band)
    - 2.4 - 2.4835 GHz (2.4-GHz band)
    - 5.725 - 5.825 GHz (5.8-GHz band)
  - —2.4 GHz also in Europe and Japan
- interference
  - —many devices around 900 MHz: cordless telephones, wireless microphones, and amateur radio
  - —fewer devices at 2.4 GHz; microwave oven
  - —little competition at 5.8 GHz

IEEE 802 Standards



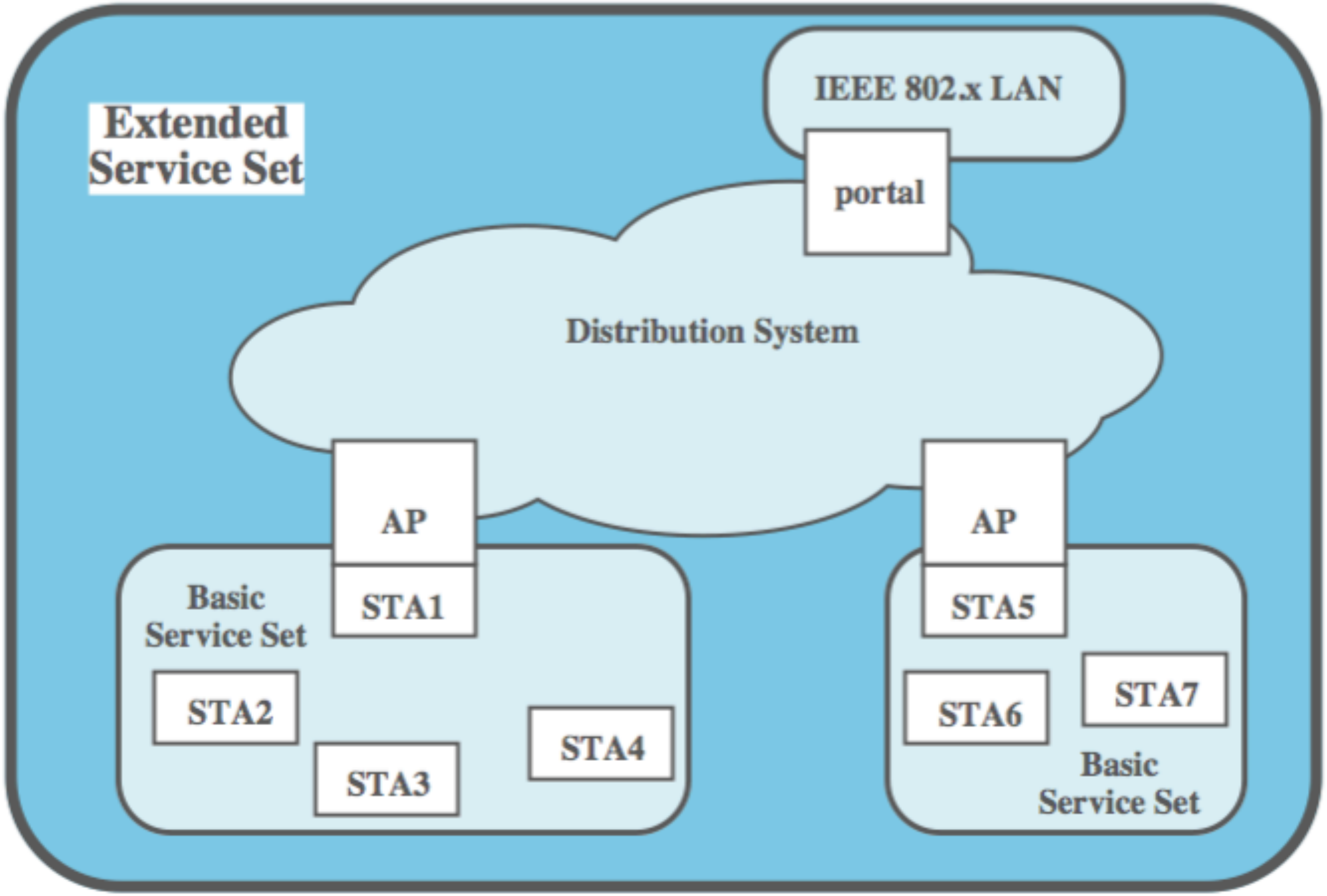
Standard	Scope
IEEE 802.11	Medium access control (MAC): One common MAC for WLAN applications
	Physical layer: Infrared at 1 and 2 Mbps
	Physical layer: 2.4-GHz FHSS at 1 and 2 Mbps
	Physical layer: 2.4-GHz DSSS at 1 and 2 Mbps
IEEE 802.11a	Physical layer: 5-GHz OFDM at rates from 6 to 54 Mbps
IEEE 802.11b	Physical layer: 2.4-GHz DSSS at 5.5 and 11 Mbps
IEEE 802.11c	Bridge operation at 802.11 MAC layer
IEEE 802.11d	Physical layer: Extend operation of 802.11 WLANs to new regulatory domains (countries)
IEEE 802.11e	MAC: Enhance to improve quality of service and enhance security mechanisms
IEEE 802.11f	Recommended practices for multivendor access point interoperability
IEEE 802.11g	Physical layer: Extend 802.11b to data rates >20 Mbps
IEEE 802.11h	Physical/MAC: Enhance IEEE 802.11a to add indoor and outdoor channel selection and to improve spectrum and transmit power management
IEEE 802.11i	MAC: Enhance security and authentication mechanisms
IEEE 802.11j	Physical: Enhance IEEE 802.11a to conform to Japanese requirements
IEEE 802.11k	Radio resource measurement enhancements to provide interface to higher layers for radio and network measurements
IEEE 802.11m	Maintenance of IEEE 802.11-1999 standard with technical and editorial corrections
IEEE 802.11n	Physical/MAC: Enhancements to enable higher throughput
IEEE 802.11p	Physical/MAC: Wireless access in vehicular environments
IEEE 802.11r	Physical/MAC: Fast roaming (fast BSS transition)
IEEE 802.11s	Physical/MAC: ESS mesh networking
IEEE 802.11,2	Recommended practice for the Evaluation of 802.11 wireless performance
IEEE 802.11u	Physical/MAC: Interworking with external networks

IEEE 802 Terminology



Access point (AP)	Any entity that has station functionality and provides access to the distribution system via the wireless medium for associated stations
Basic service set (BSS)	A set of stations controlled by a single coordination function
Coordination function	The logical function that determines when a station operating within a BSS is permitted to transmit and may be able to receive PDUs
Distribution system (DS)	A system used to interconnect a set of BSSs and integrated LANs to create an ESS
Extended service set (ESS)	A set of one or more interconnected BSSs and integrated LANs that appear as a single BSS to the LLC layer at any station associated with one of these BSSs
MAC protocol data unit (MPDU)	The unit of data exchanged between two peer MAC entites using the services of the physical layer
MAC service data unit (MSDU)	Information that is delivered as a unit between MAC users
Station	Any device that contains an IEEE 802.11 conformant MAC and physical layer

IEEE 802.11 Architecture



STA = station
AP = access point

IEEE 802.11 - BSS

- basic service set (BSS) building block
- may be isolated
- may connect to backbone distribution system (DS) through access point (AP)
- BSS generally corresponds to cell
- DS can be switch, wired network, or wireless network
- have independent BSS (IBSS) with no AP

Extended Service Set (ESS)

- possible configurations:
  - simplest is each station belongs to single BSS
  - can have two BSSs overlap
  - a station can participate in more than one BSS
  - association between station and BSS dynamic
- ESS is two or more BSS interconnected by DS
- appears as single logical LAN to LLC

IEEE 802 Services

Service	Provider	Used to support
Association	Distribution system	MSDU delivery
Authentication	Station	LAN access and security
Deauthentication	Station	LAN access and security
Dissassociation	Distribution system	MSDU delivery
Distribution	Distribution system	MSDU delivery
Integration	Distribution system	MSDU delivery
MSDU delivery	Station	MSDU delivery
Privacy	Station	LAN access and security
Reassocation	Distribution system	MSDU delivery

Services - Message Distribution

- distribution service
  - primary service used by stations to exchange MAC frames when frame must traverse DS
  - if stations in same BSS, distribution service logically goes through single AP of that BSS
- integration service
  - enables transfer of data between 802.11 LAN station and one on an integrated 802.x LAN

Association Related Services

- DS requires info about stations within ESS
- provided by association-related services
- station must associate before communicating
- 3 mobility transition types:
  - no transition - stationary or in single BSS
  - BSS transition - between BSS in same ESS
  - ESS transition: between BSS in different ESS

Association Related Services

- DS needs identity of destination station
  - stations must maintain association with AP within current BSS
- 3 services relate to this requirement:
  - Association - establishes initial association between station and AP
  - Reassociation - to transfer an association to another AP
  - Disassociation - by station or AP

Medium Access Control

- MAC layer covers three functional areas
  - reliable data delivery
  - access control
  - security

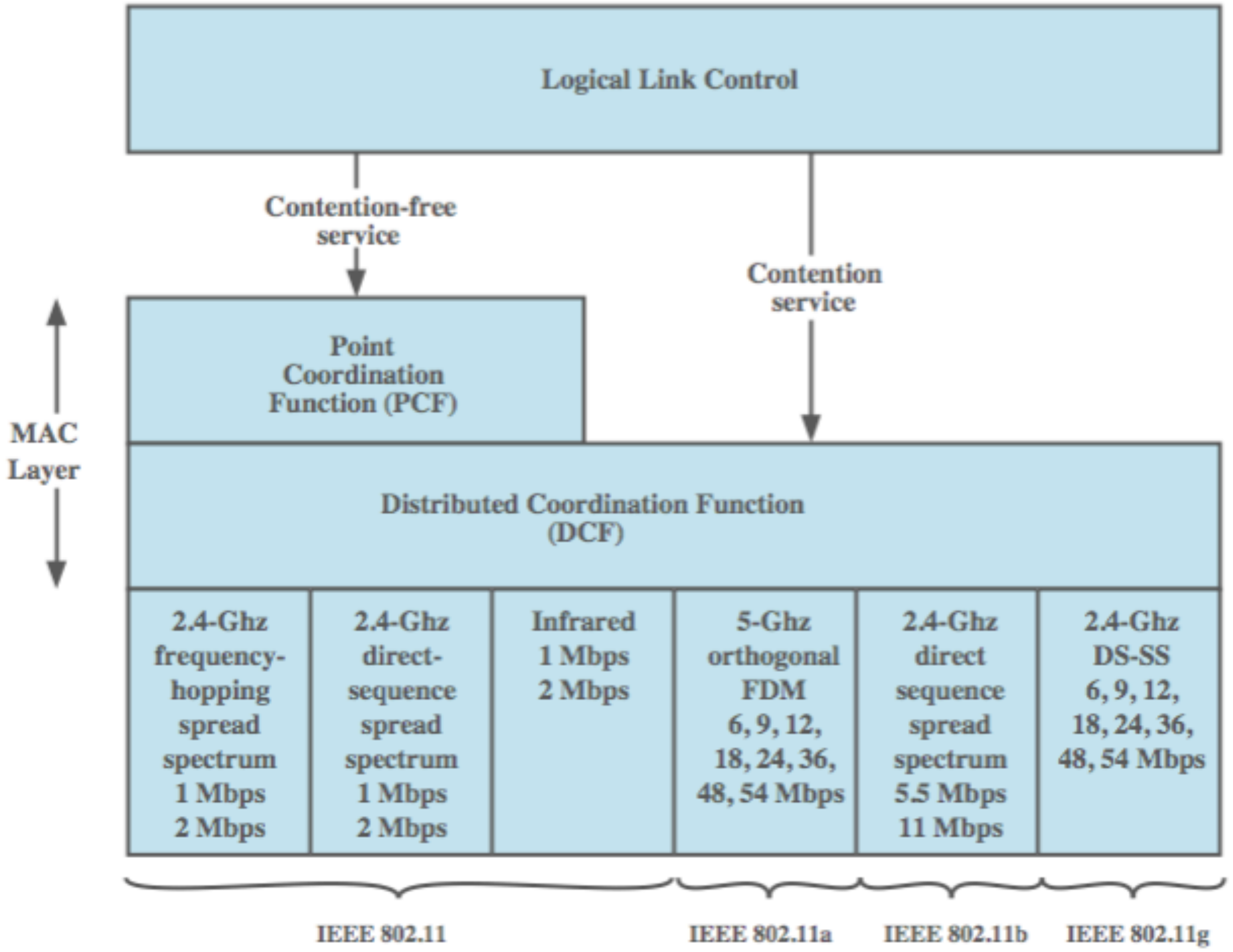
Reliable Data Delivery

- 802.11 physical / MAC layers unreliable
  - noise, interference, and other propagation effects result in loss of frames
  - even with error-correction codes, frames may not successfully be received
- can be dealt with at a higher layer, e.g. TCP
- more efficient to deal with errors at MAC level
- 802.11 includes frame exchange protocol
  - station receiving frame returns acknowledgment (ACK) frame
  - exchange treated as atomic unit
  - if no ACK within short period of time, retransmit

Four Frame Exchange

- can use four-frame exchange for better reliability
  - source issues a Request to Send (RTS) frame to dest
  - destination responds with Clear to Send (CTS)
  - after receiving CTS, source transmits data
  - destination responds with ACK
- RTS alerts all stations within range of source that exchange is under way
- CTS alerts all stations within range of destination
- other stations don't transmit to avoid collision
- RTS/CTS exchange is required function of MAC but may be disabled

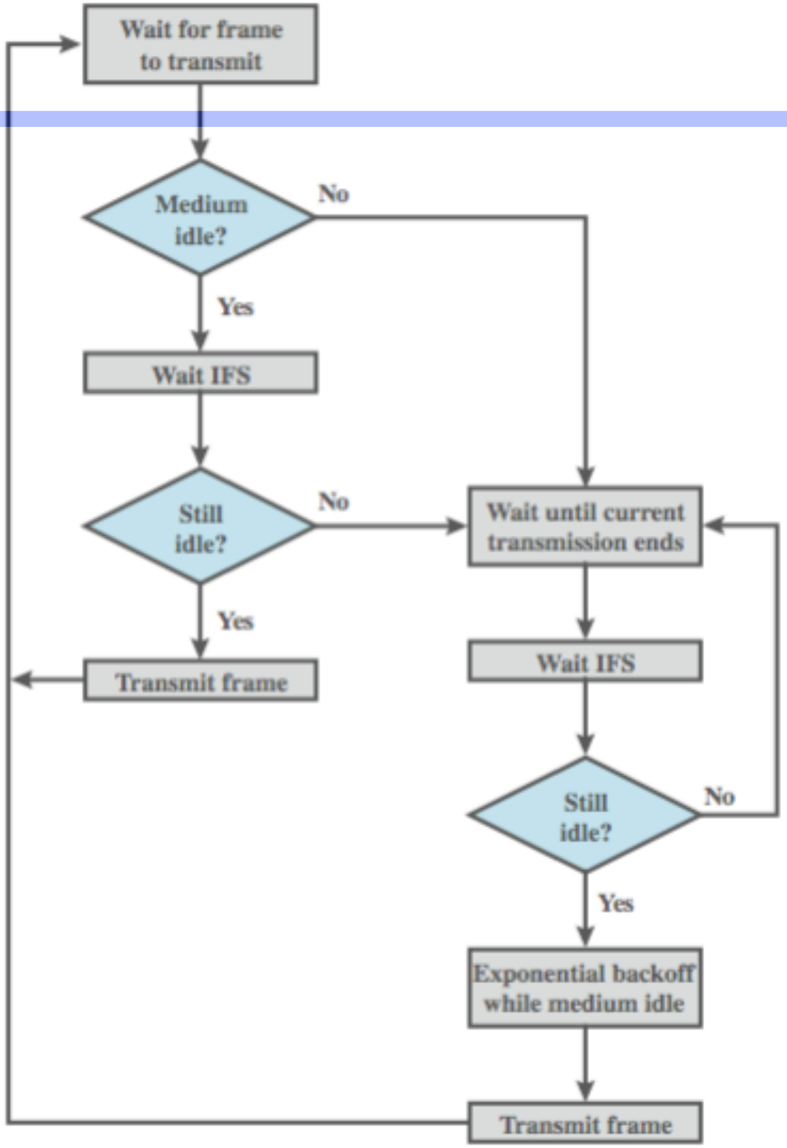
Media Access Control


Logical Link Control
Contention-free service
Contention service
Point Coordination Function (PCF)
MAC Layer
Distributed Coordination Function (DCF)
2.4-Ghz frequency-hopping spread spectrum 1 Mbps 2 Mbps
2.4-Ghz direct-sequence spread spectrum 1 Mbps 2 Mbps
Infrared 1 Mbps 2 Mbps
5-Ghz orthogonal FDM 6, 9, 12, 18, 24, 36, 48, 54 Mbps
2.4-Ghz direct sequence spread spectrum 5.5 Mbps 11 Mbps
2.4-Ghz DS-SS 6, 9, 12, 18, 24, 36, 48, 54 Mbps
IEEE 802.11
IEEE 802.11a
IEEE 802.11b
IEEE 802.11g

Distributed Coordination Function

- DCF sublayer uses CSMA
  - if station has frame to send it listens to medium
  - if medium idle, station may transmit
  - else waits until current transmission complete
- no collision detection since on wireless network
- DCF includes delays that act as a priority scheme

IEEE 802.11 Medium Access Control Logic


Wait for frame to transmit
Medium idle?
No
Yes
Wait IFS
Still idle?
No
Yes
Transmit frame
Wait until current transmission ends
Wait IFS
Still idle?
No
Yes
Exponential backoff while medium idle
Transmit frame

Priority IFS Values

- IFS (**I**nter **F**rame **S**pace)
- SIFS (short IFS)
  - for all immediate response actions (see later)
- PIFS (point coordination function IFS)
  - used by the centralized controller in PCF scheme when issuing polls
- DIFS (distributed coordination function IFS)
  - used as minimum delay for asynchronous frames contending for access

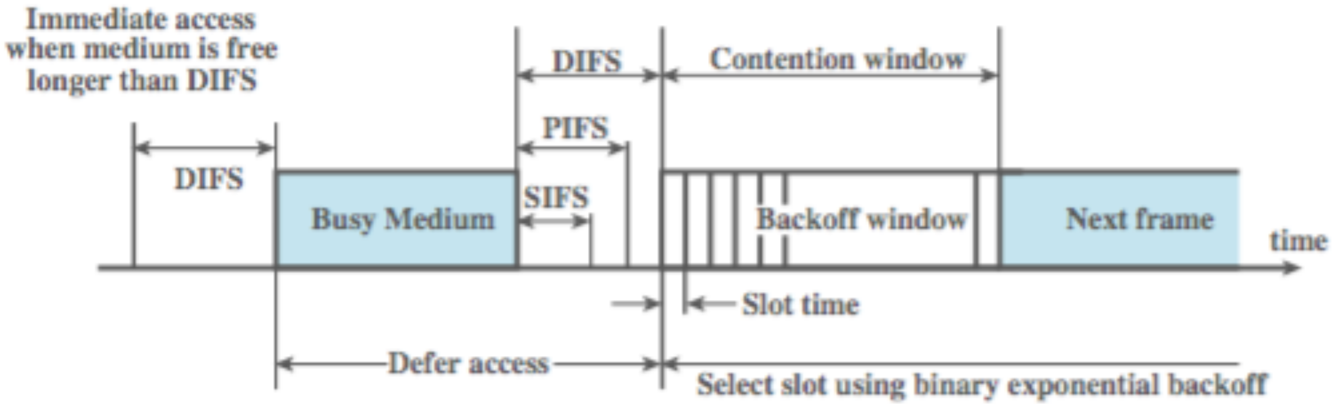
SIFS Use

- SIFS gives highest priority
  - over stations waiting PIFS or DIFS time
- SIFS used in following circumstances:
  - Acknowledgment (ACK)
    - station responds with ACK after waiting SIFS gap
    - for efficient collision detect & multi-frame transmission
  - Clear to Send (CTS)
    - station ensures data frame gets through by issuing RTS
    - and waits for CTS response from destination
  - Poll response
    - see Point coordination Function (PCF) discussion next

PIFS and DIFS Use

- PIFS used by centralized controller
  - for issuing polls
  - has precedence over normal contention traffic
  - but not SIFS
- DIFS used for all ordinary asynchronous traffic

IEEE 802.11 MAC Timing Basic Access Method

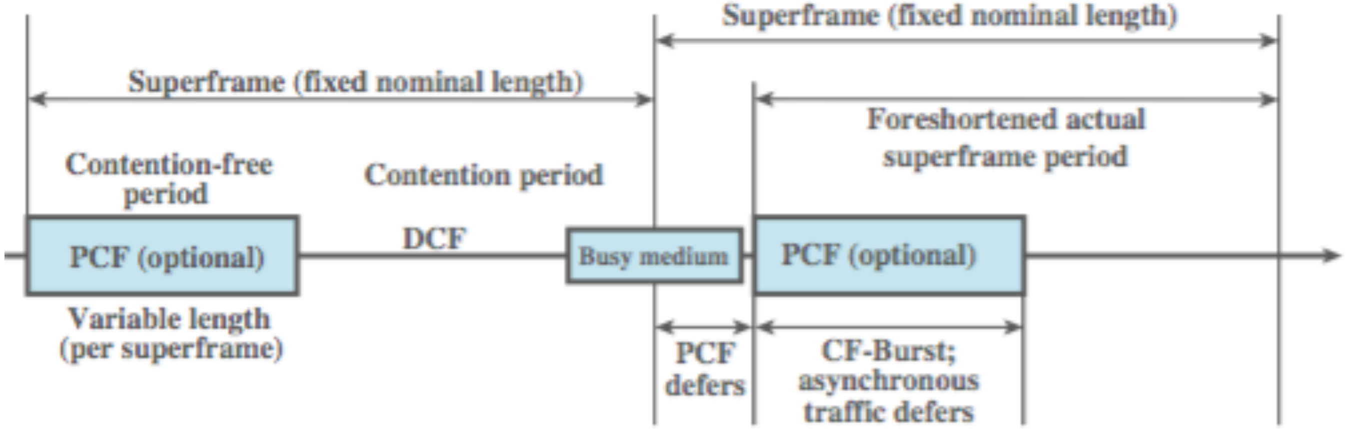


(a) Basic Access Method

Point Coordination Function (PCF)

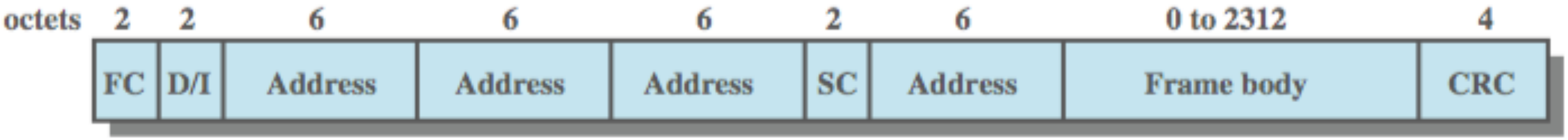
- alternative access method implemented on top of DCF
- polling by centralized polling master (point coordinator)
- uses PIFS when issuing polls
- point coordinator polls in round-robin to stations configured for polling
- when poll issued, polled station may respond using SIFS
- if point coordinator receives response, it issues another poll using PIFS
- if no response during expected turnaround time, coordinator issues poll
- coordinator could lock out async traffic by issuing polls
- have a superframe interval defined

PCF Superframe Timing


Superframe (fixed nominal length)
Superframe (fixed nominal length)
Foreshortened actual superframe period
Contention-free period
Contention period
DCF
PCF (optional)
Busy medium
PCF (optional)
Variable length (per superframe)
PCF defers
CF-Burst; asynchronous traffic defers

(b) PCF Superframe Construction

IEEE 802.11 MAC Frame Format



octets	2	2	6	6	6	2	6	0 to 2312	4
	FC	D/I	Address	Address	Address	SC	Address	Frame body	CRC

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

Control Frames

- Power Save-Poll (PS-Poll)
  - request AP transmit buffered frame when in power-saving mode
- Request to Send (RTS)
  - first frame in four-way frame exchange
- Clear to Send (CTS)
  - second frame in four-way exchange
- Acknowledgment (ACK)
- Contention-Free (CF)-end
  - announces end of contention-free period part of PCF
- CF-End + CF-Ack:
  - acknowledges CF-end to end contention-free period and release stations from associated restrictions

Data Frames – Data Carrying

- eight data frame subtypes, in two groups
- first four carry upper-level data
- Data
  - simplest data frame, contention or contention-free use
- Data + CF-Ack
  - carries data and acknowledges previously received data during contention-free period
- Data + CF-Poll
  - used by point coordinator to deliver data & req send
- Data + CF-Ack + CF-Poll
  - combines Data + CF-Ack and Data + CF-Poll

Data Frames – Not Data Carrying

- other four data frames do not carry user data
- Null Function
  - carries no data, polls, or acknowledgments
  - carries power mgmt bit in frame control field to AP
  - indicates station is changing to low-power state
- other three frames (CF-Ack, CF-Poll, CF-Ack + CF-Poll) same as corresponding frame in preceding list but without data

Management Frames

- used to manage communications between stations and Aps
- such as management of associations
    - requests, response, reassociation, dissociation, and authentication

802.11 Physical Layer

	802.11	802.11a	802.11b	802.11g
Available bandwidth	83.5 MHz	300 MHz	83.5 MHz	83.5 MHz
Unlicensed frequency of operation	2.4 - 2.4835 GHz DSSS, FHSS	5.15 - 5.35 GHz OFDM 5.725 - 5.825 GHz OFDM	2.4 - 2.4835 GHz DSSS	2.4 - 2.4835 GHz DSSS, OFDM
Number of non-overlapping channels	3 (indoor/outdoor)	4 indoor 4 (indoor/outdoor) 4 outdoor	3 (indoor/outdoor)	3 (indoor/outdoor)
Data rate per channel	1, 2 Mbps	6, 9, 12, 18, 24, 36, 48, 54 Mbps	1, 2, 5.5, 11 Mbps	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
Compatibility	802.11	Wi-Fi5	Wi-Fi	Wi-Fi at 11 Mbps and below

Original 802.11 Physical Layer - DSSS

- Direct-sequence spread spectrum (DSSS)
- 2.4 GHz ISM band at 1 Mbps and 2 Mbps
- up to seven channels, each 1 Mbps or 2 Mbps, can be used
- depends on bandwidth allocated by various national regulations
  - 13 in most European countries
  - one in Japan
- each channel bandwidth 5 MHz
- encoding scheme DBPSK for 1-Mbps and DQPSK for 2-Mbps using an 11-chip Barker seq

Original 802.11 Physical Layer - FHSS

- Frequency-hopping spread spectrum
  - 2.4 GHz ISM band at 1 Mbps and 2 Mbps
  - 23 channels in Japan
  - 70 channels in USA
  - signal hopping between multiple channels based on a pseudonoise sequence
  - 1-MHz channels are used
- hopping scheme adjustable
- two-level Gaussian FSK modulation for 1 Mbps
- four-level GFSK modulation used for 2 Mbps

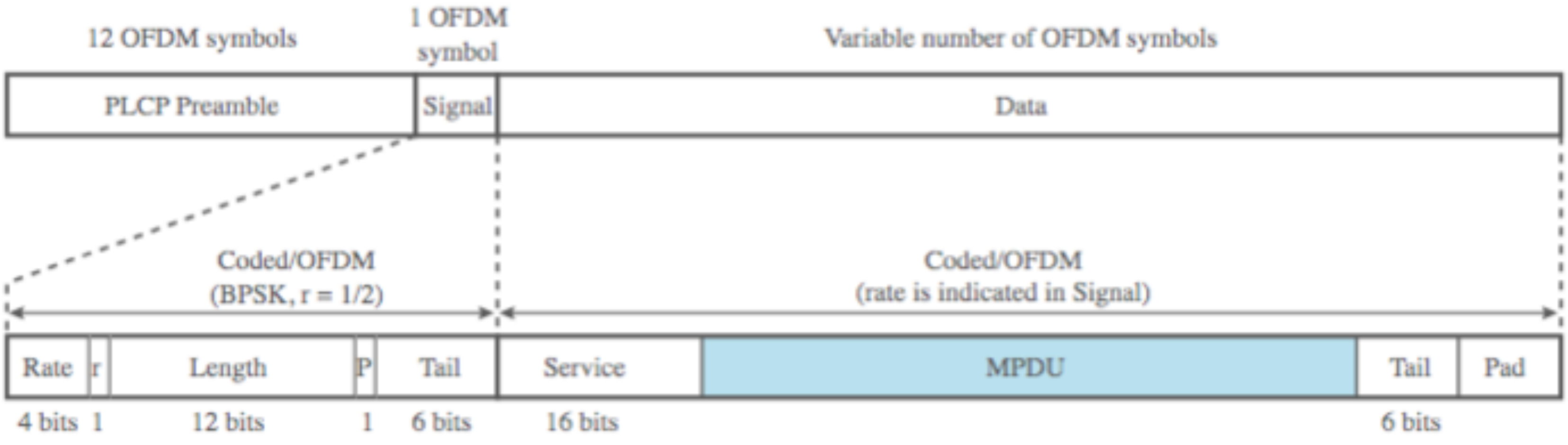
Original 802.11 Physical Layer – Infrared

- omnidirectional
- range up to 20 m
- 1 Mbps uses 16-PPM (pulse position modulation)
  - 4 data bit group mapped to one of 16-PPM symbols
  - each symbol a string of 16 bits
  - each 16-bit string has fifteen 0s and one binary 1
- 2-Mbps has each group of 2 data bits is mapped into one of four 4-bit sequences
  - each sequence consists of three 0s and one binary 1
- intensity modulation is used for transmission

802.11a

- uses 5-GHz band (different to other variants)
  - supports higher data rates, is less cluttered
- orthogonal frequency division multiplexing (OFDM)
  - multiple carrier signals at different frequencies
  - some bits on each channel
- up to 48 subcarriers modulated using BPSK, QPSK, 16-QAM, or 64-QAM
  - subcarrier frequency spacing 0.3125 MHz
  - convolutional code at rate of 1/2, 2/3, or 3/4 provides forward error correction
  - combination of modulation technique and coding rate determines data rate

802.11a Physical Frame

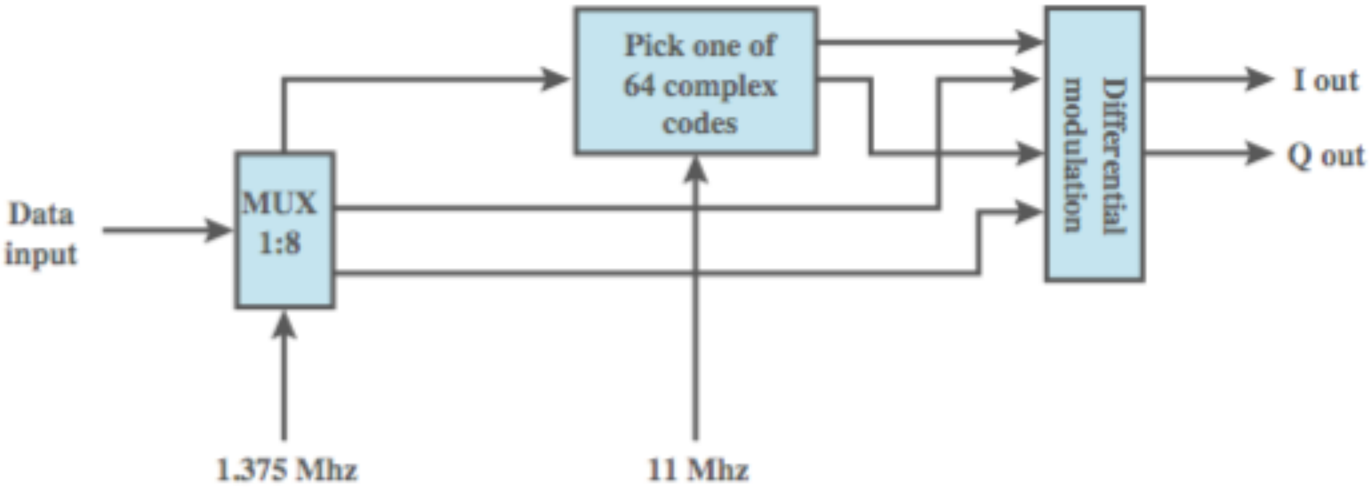


(a) IEEE 802.11a physical PDU

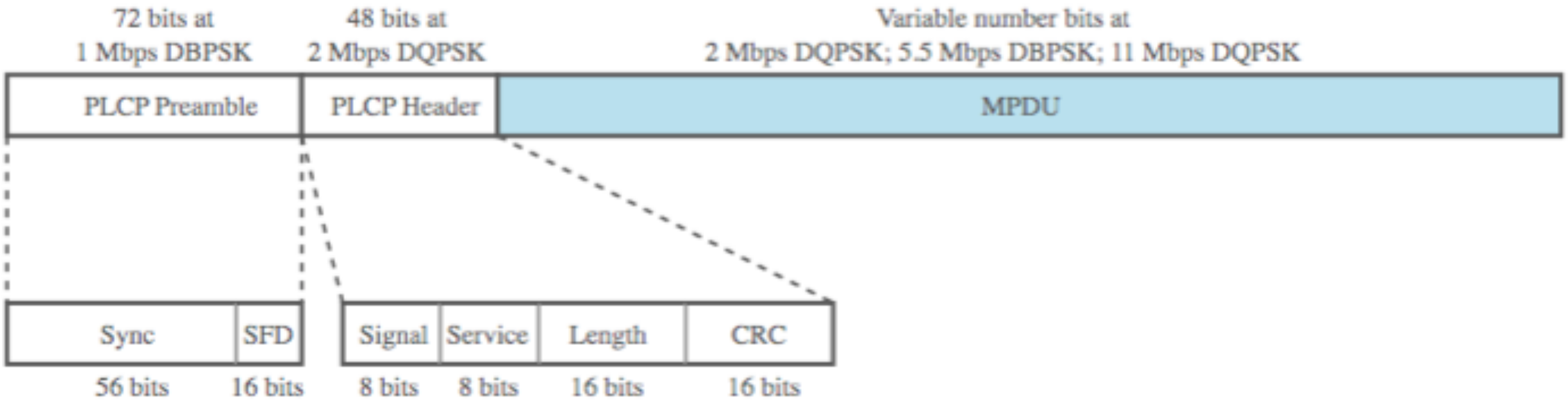
802.11b

- extension of 802.11 DS-SS scheme
  - with data rates of 5.5 and 11 Mbps
- chipping rate 11 MHz
  - same as original DS-SS scheme
  - Complementary Code Keying (CCK) modulation gives higher data rate with same bandwidth & chipping rate
  - also Packet Binary Convolutional Coding (PBCC) for future higher rate use

11-Mbps CCK Modulation Scheme



802.11b Physical Frame



(b) IEEE 802.11b physical PDU

802.11g

- higher-speed extension to 802.11b
- operates in 2.4GHz band
- compatible with 802.11b devices
- combines physical layer encoding techniques used in 802.11 and 802.11b to provide service at a variety of data rates
  - ERP-OFDM for 6, 9, 12, 18, 24, 36, 48, 54Mbps rates
  - ERP-PBCC for 22 & 33Mbps rates

Data Rate vs Distance (m)

Data Rate (Mbps)	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

Access and Privacy Services - Authentication

- authentication used to establish station identity
- wired LANs assume physical connection gives authority to use LAN
- not a valid assumption for wireless LANs
- 802.11 supports several authentication schemes
- does not mandate any particular scheme
- from relatively insecure handshaking to public-key encryption
- 802.11 requires mutually acceptable, successful authentication before association

Access and Privacy Services Deauthentication & Privacy

- Deauthentication
  - invoked whenever an existing authentication is to be terminated
- Privacy
  - used to prevent messages being read by others
  - 802.11 allows optional use of encryption
- Original WEP security features were weak
- Subsequently 802.11i and WPA alternatives evolved giving better security

Summary

- Wireless LAN alternatives
- IEEE 802.11 architecture and services
- 802.11 Media Access Control
- 802.11 Physical Layers
    - 802.11, 802.11a, 802.11b, 802.11g
- Security considerations