Introduction to IEEE 802.11: WiFi

Wireless Local Area Networking Standard

Speaker: Prof. A. Bruce McDonald
Re-configurable Wireless Networking Lab
Northeastern University, Dept. of Electrical and Computer Engineering

Outline

- Introduction to Wireless LANs
- IEEE 802.11 Architecture Overview
- IEEE 802.11 MAC Entity
- IEEE 802.11 PHY Entity
- IEEE 802.11 Security
- Enhancements coming with IEEE 802.11e
- Simulation Performance Results
- Conclusions & References

Introduction to Wireless LANs

- Wireless Technologies
  - Applications
  - Directions
- What is IEEE 802.11?
- What makes 802.11 popular?
- Current 802.11 Standards
- 802.11 Standards under Development
- Technology Status
- Technology Advantages and Applications

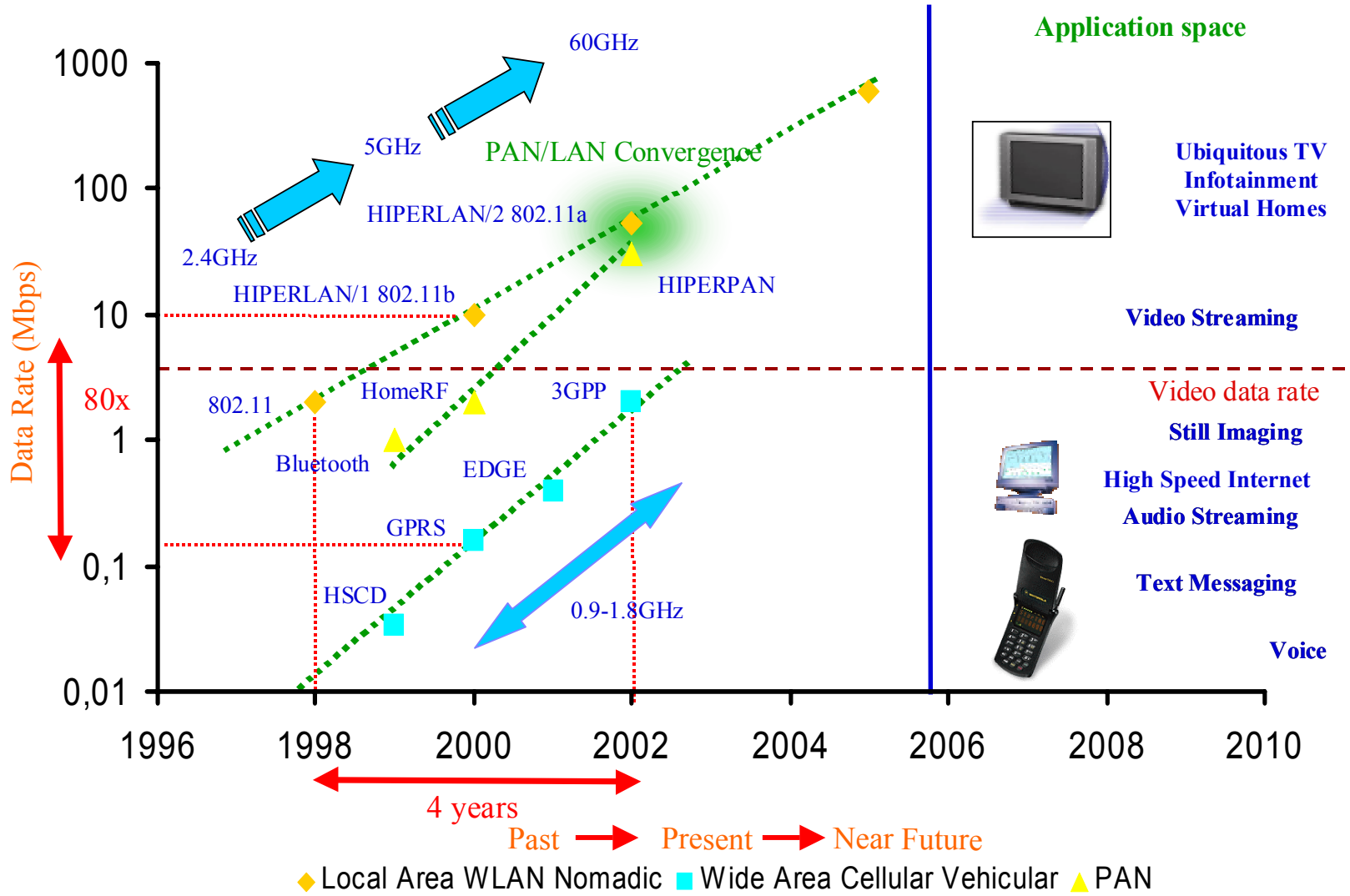
Applications of Wireless Technologies

- Wireless Communications technologies pervade our lives more than we may realize
  - Cell Phones
  - Telephone systems
  - Wireless LAN
  - Satellites
  - Garage Door openers
  - International communications
  - Medical Equipment
  - Electric Meter readings
  - Police and Firefighter

Directions of Wireless Technologies

- Moving to Higher Speed
  - 3G Cellular Systems → 2Mbps
  - IEEE802.11a → 54Mbps
- Becoming Smaller
  - Cellular Telephones now fit in wristwatches
  - Two chips encompass Bluetooth functionality
- Becoming Pervasive
  - In some European countries, 85 percent of the populace owns a cellular telephone
  - In the US, the home networking market is expected to be in the hundreds of millions

Directions of Wireless Technologies (cont.)



What is IEEE 802.11?

- Standard for wireless local area networks (wireless LANs)
- Developed in late 90s by IEEE
- Intended for home or office use (primarily indoor)
- 802.11 standard for the MAC and PHY layer
- Other standards (802.11a, 802.11b) for the physical layer
- Wireless version of the Ethernet (802.3) standard
  - Ethernet: CSMA/CD
  - WLAN: CSMA/CA

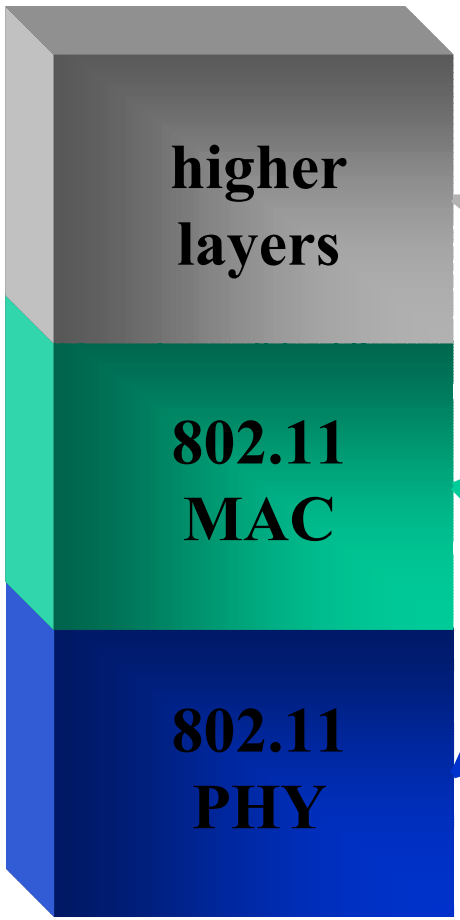
What makes IEEE 802.11 popular?

- Supported by a large number of vendors
- Transmission rates up to 11 Megabits per second and will be up to 54 Megabits per second
- Predicted to dominate the wireless networking market over lower bit rate technologies such as Bluetooth and HomeRF

802.11 Standard & Supplements

- IEEE 802.11-1997 base standard
  - also released as ANSI/ISO 8802-11 1999
- Base standard divided into two layers
  - medium access control (MAC) layer
  - physical (PHY) layer
- Standard supplements extend one of these layers or provide higher layer functions
- Supplements at different layers can be intermixed
  - 802.11e applies to 802.11b, 802.11a and 802.11g

802.11 Supplements



- 802.11a
  - 5 GHz OFDM
  - 54 Mbps
- 802.11b
  - 2.4GHz DSSS
  - 5.5, 11 Mbps
- 802.11c
  - bridging tables
- 802.11d
  - international roaming
- 802.11e
  - quality of service
- 802.11f
  - inter-access point protocols
- 802.11g
  - 2.4 GHz OFDM
  - 54 Mbps
- 802.11h
  - European regulatory extensions
- 802.11i
  - enhanced security

already approved under development

Technology Status

- Dominated the market rapidly
  - Starbucks has incorporated 802.11 in their coffee shops
  - McDonald's is deploying WLAN Hot Spots
  - Verizon is placing WLAN Access Points on their pay phones in NYC and offering free service to DSL clients
- Backed by companies such as Microsoft and Intel
- Wireless Ethernet Compatibility Alliance (WECA), also known WiFi Alliance, formed to certify 802.11 products
  - Has a large number of industry participants

Technological Advantages and Applications

- Advantages
  - Agreed upon IEEE standard that is accepted worldwide
  - Large number of commercial backers
  - Commercially available chipsets
  - High speed (11 Mbps) now and higher speed (54 Mbps) soon
- Applications
  - Home and Office Networking

802.11 Architecture

- Challenges of working in Wireless Environment
- Architecture Overview
- 802.11 Protocol Entities
- 802.11 Protocol Architecture
- 802.11 Configuration – Independent
- 802.11 Configuration – Infrastructure
  - Distribution System
  - Access Points

Challenges of working in Wireless Environment

- Difficult media
  - Interference and noise
  - quality varies over space and time
  - shared with "unwanted" 802.11 devices
  - shared with non-802 devices (unlicensed spectrum, microwave ovens)
- No assumption of full connectivity
  - "hidden node" problem
- Multiple international regulatory requirements

Challenges (continued)

- Mobility
  - variation in link reliability
  - battery usage: requires power management
  - want “seamless” connections
- Security
  - no physical boundaries
  - overlapping LANs

Architecture Overview

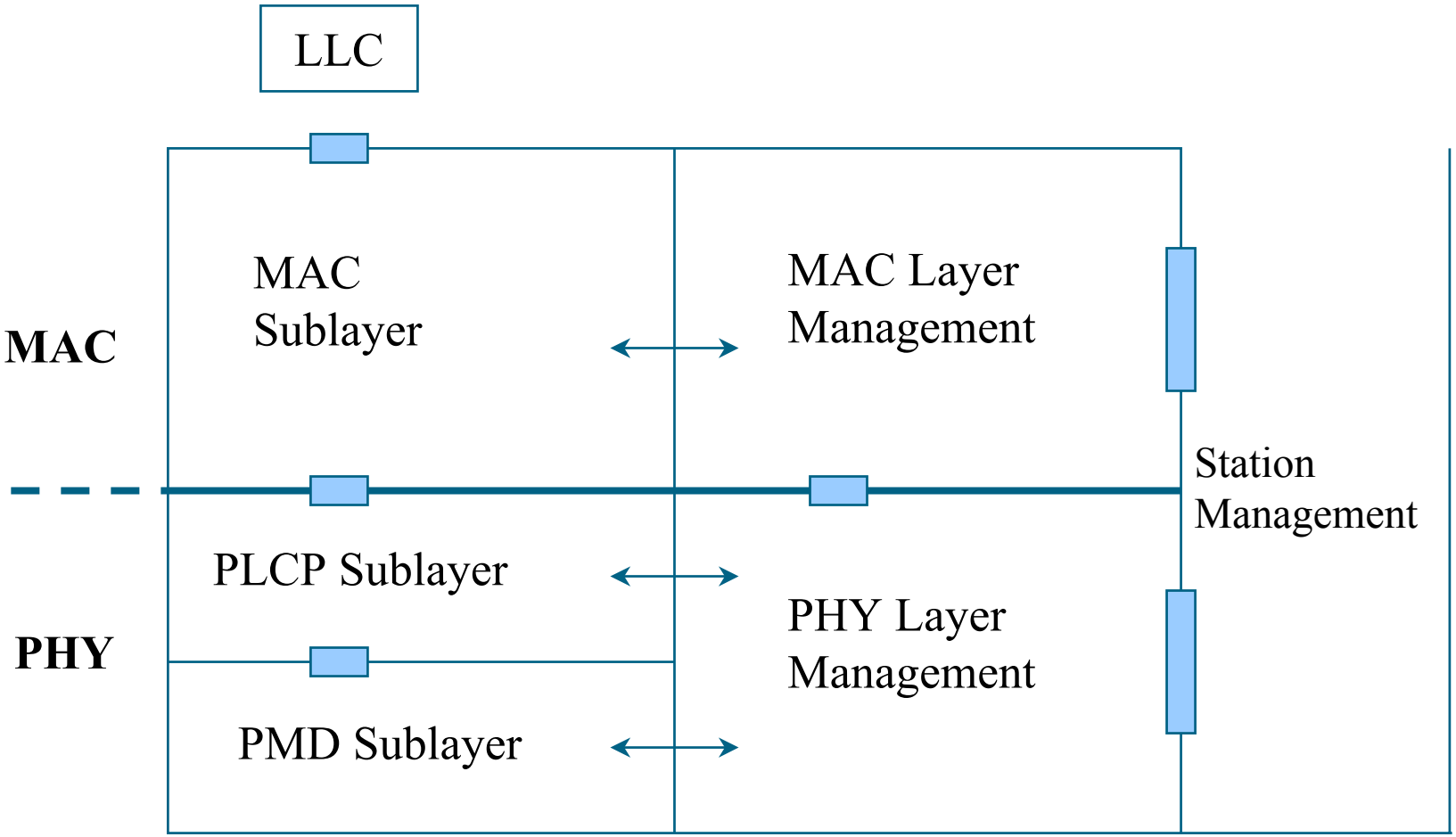
- One MAC supporting multiple PHYs
  - Frequency Hopping Spread Spectrum (FHSS)
  - Direct Sequence Spread Spectrum (DSSS)
  - Orthogonal Frequency Division Multiplexing (OFDM)
  - Infrared (IR)
- Two configurations
  - "independent" (ad hoc) and "infrastructure"
- CSMA/CA (collision avoidance) with optional "point coordination"

IEEE 802.11 Terminology

The 802.11 working group defined a number of key terms that would be required to implement the envisioned standard:

• Access Point	AP
• Basic Service Set	BSS
• Coordination Function	
• Distribution System	DS
• Extended Service Set	ESS
• MAC Protocol Data Unit	MPDU
• MAC Service Data Unit	MSDU
• Station	

802.11 Protocol Entities



LLC : Logical Link Control
PLCP : Physical Layer Convergence Protocol
PMD : Physical Medium Dependent Sublayer

802.11 Protocol Architecture

- MAC Entity
  - basic access mechanism
  - fragmentation
  - encryption
- MAC Layer Management Entity
  - synchronization
  - power management
  - roaming
  - MAC Management Information Base (MIB)
- Physical Layer Convergence Protocol (PLCP)
  - PHY-specific, supports common PHY Service Access Point (SAP)
  - provides Clear Channel Assessment (CCA) signal (carrier sense)

802.11 Protocol Architecture (cont.)

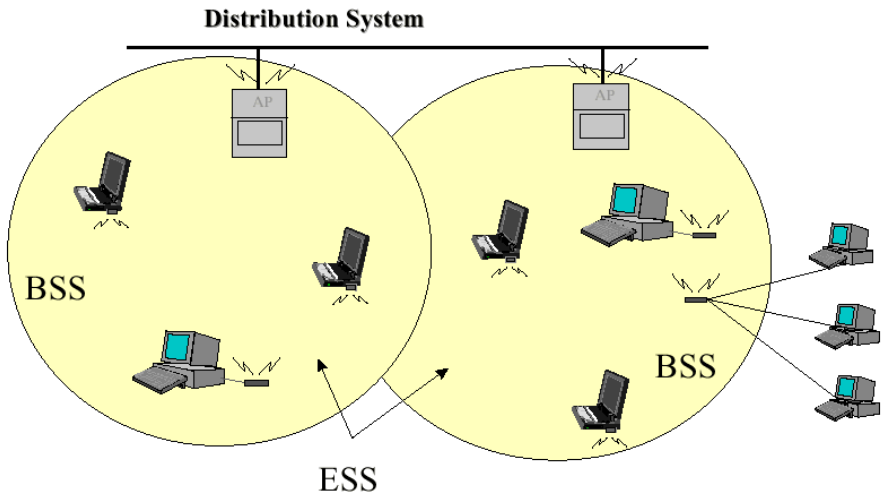
- Physical Medium Dependent Sublayer (PMD)
  - modulation and encoding
- PHY Layer Management
  - channel tuning
  - PHY MIB
- Station Management
  - interacts with both MAC and PHY management

IEEE 802.11 Architecture

The figure illustrates the major components of the IEEE 802.11 Architecture as developed by the working group.

- Multiple BSSs support associated stations.
- The stations may be mobile, thus, may move from BSS to BSS within an ESS that is connected by a DS.
- Access to a traditional 'wired' LAN is provided by a portal (not illustrated)

IEEE 802.11 Architecture



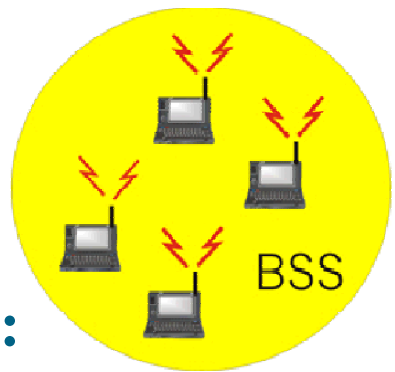
BSS:
The basic service set

The smallest building block of an 802.11 LAN is the BSS. It consists of stations executing the same MAC and competing for access to the shared medium. A BSS may be isolated or connect to a distributions system (DS) through an access point (AP)

- WM: Wireless medium used to transfer messages.
- ST: Station---an entity that utilizes the WM to obtain LAN services.
- BSS: A set of stations (cell) within mutual range or range of an AP.

IEEE 802.11 Architecture

Stations in a BSS:



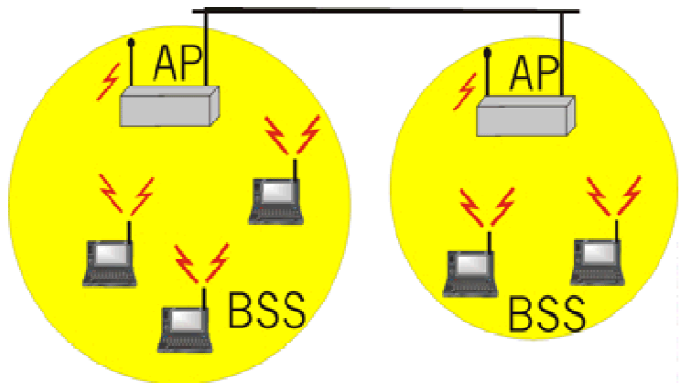
ESS:
The extended service set

A set of two or more BSSs interconnected by a distribution system (DS). The DS is typically a backbone wired LAN; however it can be any type of communications network.

- The ESS appears as single BSS to the LLC layer of any station(s) associated with any of the integrated BSSs.

IEEE 802.11 Architecture

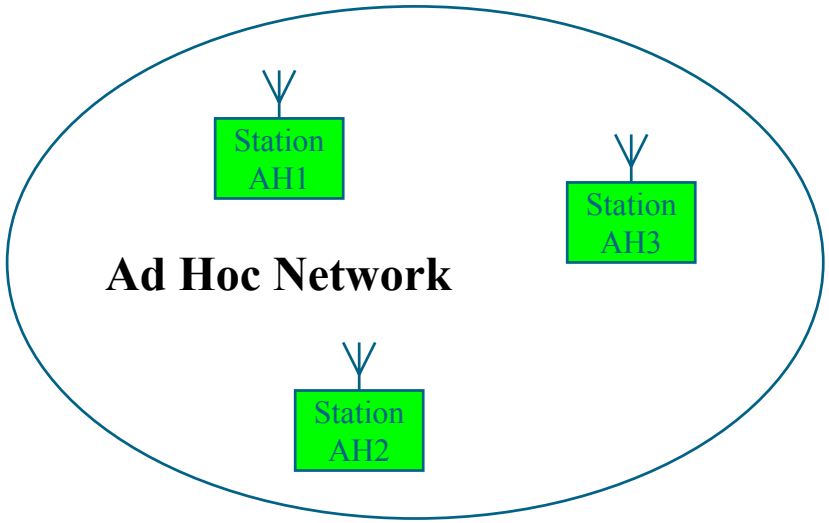
Simple example of an ESS



Distribution System

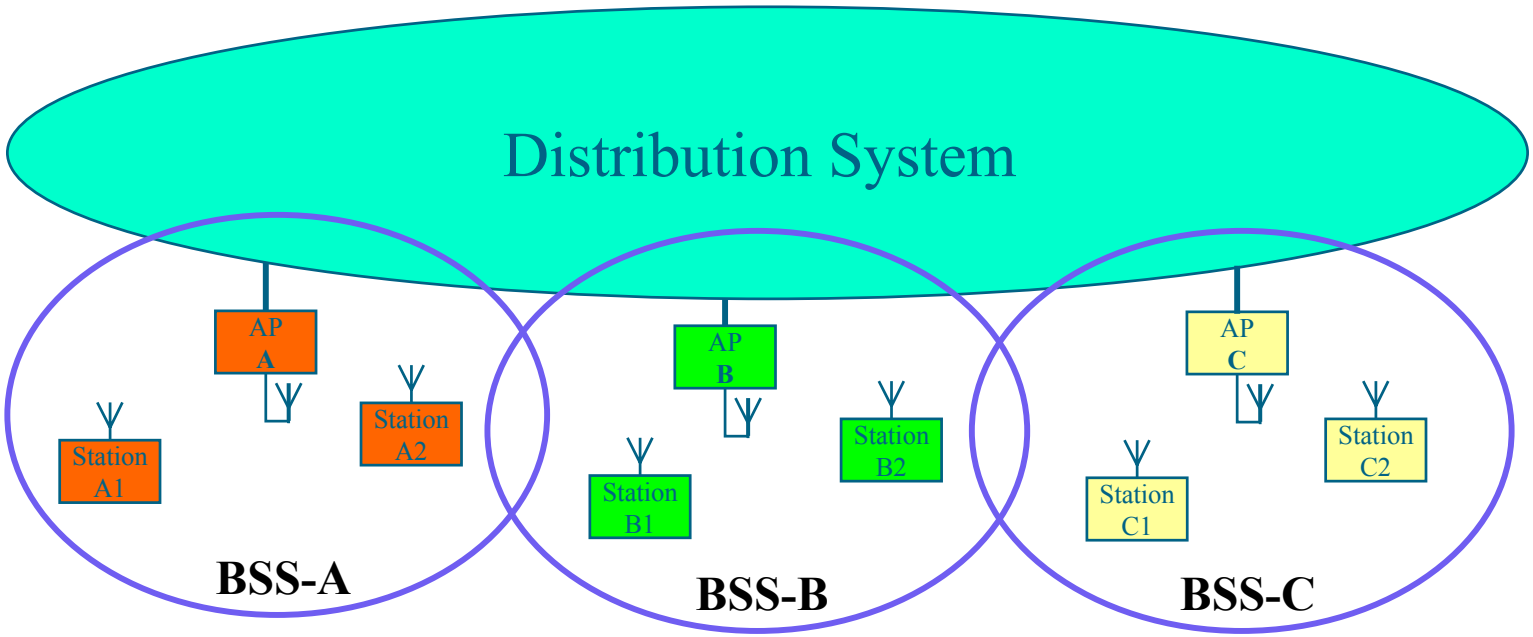
- Used to interconnect wireless "cells" to support roaming
  - Multiple BSS connected together form an ESS, Extended Service Set
  - BSSs must not cause channel level interference: 802.11b supports 11 channels; channel reuse must ensure that sufficient exists between BSSs utilizing the same channel.
  - Allows mobile stations to access to fixed resources as well
  - This is not network-layer mobility: all the stations in the ESS belong to the same IP network: "hand-off" between ESSs is a routing issue.
- Not part of 802.11 standard
  - Could be bridge IEEE LANs, wireless, other networks …

802.11 Configurations – Independent Ad Hoc Mode: Peer-to-peer



- Independent
  - Consists of one BSS
  - "Ad Hoc" network: no AP is used
  - Point-to-point communication: No Routing! (Must be provided above 802.11 which is a MAC protocol)
  - Limited coverage area

802.11 Configurations
Infrastructure mode: All communications through central AP



- Infrastructure
  - Access Points and stations
- Extension of wireless coverage area by Distribution System

IEEE 802.11 Service Model

IEEE 802.11 defines nine services to be provided by the wireless LAN to provide functionality that is roughly equivalent to that which is inherent in a wired LAN (theoretically ☺)

- The service provider may be the station or the distribution system.
- Station services are implemented in every 802.11 station including APs.
- Distribution services are provided between BSSs; these services may be implemented in an AP or in another specialized device attached to the DS.

IEEE 802.11 Services

802.11 Services

Three of the services are used to control LAN access and confidentiality. Six of the services are used to support delivery of MSDUs between stations. (Service;Provider;Used-to-Support)

Association	Distribution System	MSDU delivery
Authentication	Station	LAN access/security
Deauthentication	Station	LAN access/security
Disassociation	Distribution System	MSDU delivery
Distribution	Distribution System	MSDU delivery
Integration	Distribution System	MSDU delivery
MSDU Delivery	Station	MSDU delivery
Privacy	Station	LAN access/security
Reassociation	Distribution System	MSDU delivery

IEEE 802.11 Services

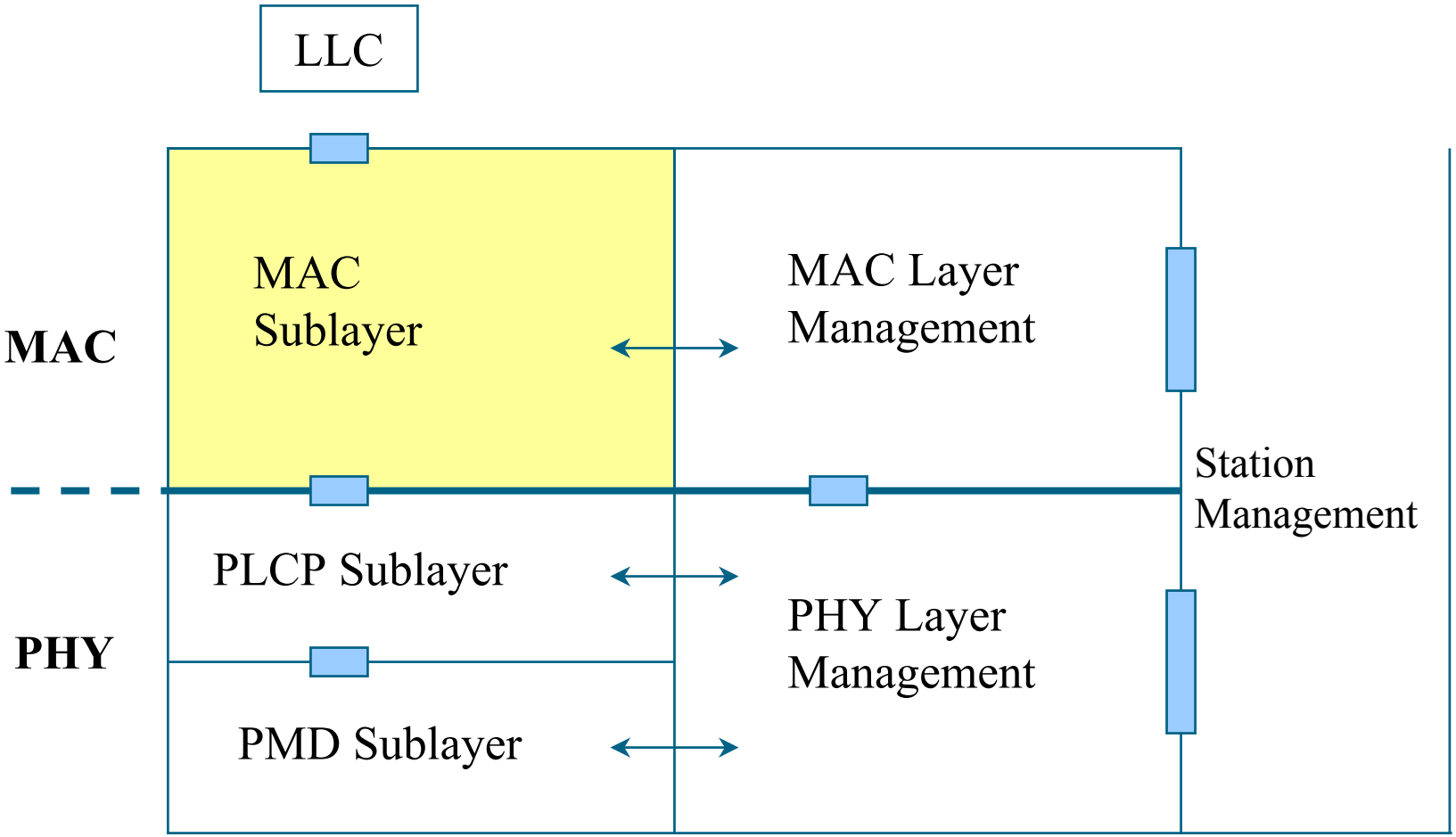
Access Points

- Stations select an AP and “associates” with it
- Support roaming
- Point Coordination Function (PCF)
- Provide other functions
  - time synchronization (beaconing)
  - power management support
- Traffic flow through AP

802.11 MAC Entity

- MAC Sublayer
  - Basic Access Protocol Features
  - CSMA/CA
  - RTS/CTS (Hidden Node Problem, Exposed Node Problem)
  - Optional Point Coordination Function (PCF)
  - Contention Free operation
  - PCF Burst
  - Fragmentation
  - Frame Formats
  - Privacy and Access Control
- MAC Management Layer
  - Synchronization
  - Power Management
  - Association and Reassociation

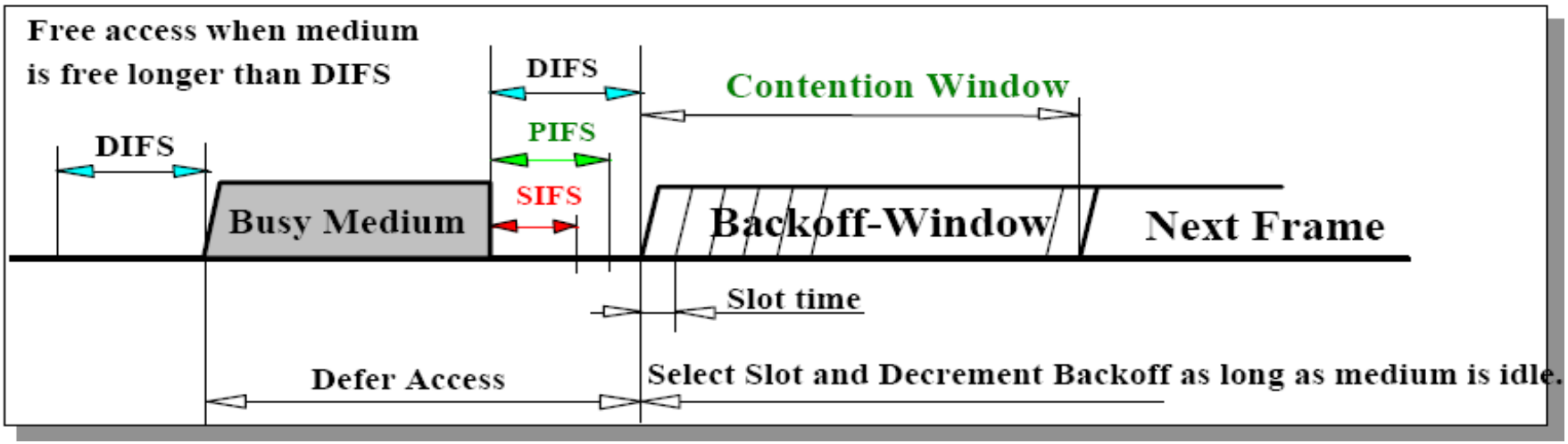
802.11 Protocol Entities



Basic Access Protocol Features

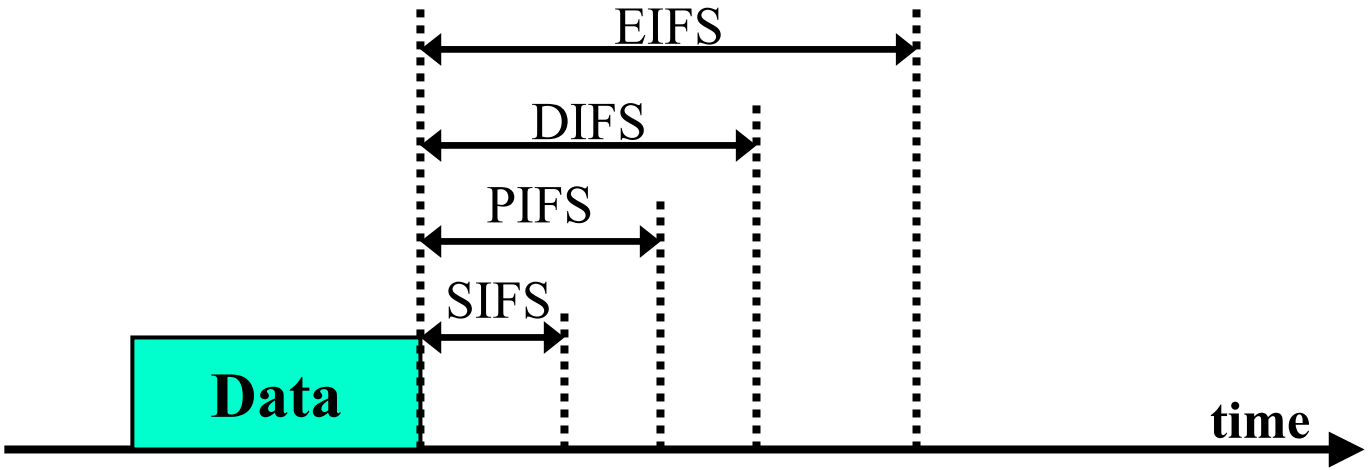
- Use Distributed Coordination Function (DCF) for efficient medium sharing without overlap restrictions
  - Use CSMA with Collision Avoidance derivative
  - Based on Carrier Sense function in PHY called *Clear Channel Assessment* (CCA)
- Robust for interference
  - **CSMA/CA + ACK** for unicast frames, with MAC level recovery
  - CSMA/CA for broadcast frames
- Parameterized use of RTS / CTS to provide a *Virtual Carrier Sense* function to protect against *Hidden Nodes*
  - Duration information distributed
- Includes fragmentation to cope with different PHY characteristics
- Frame formats to support the access scheme
  - For Infrastructure and Ad Hoc Network support
  - And Wireless Distribution System

CSMA/CA explained



- Reduce collision probability where mostly needed
  - Stations are waiting for medium to become free
  - Select Random Backoff after a Defer, resolving contention to avoid collisions
  - During deferral stations DO NOT decrement back-off timer
- Efficient Backoff algorithm stable at high loads
  - Exponential Backoff window increases for retransmissions
  - Backoff timer elapses only when medium is idle
- Implement different fixed priority levels
  - To allow immediate responses and PCF co-existence

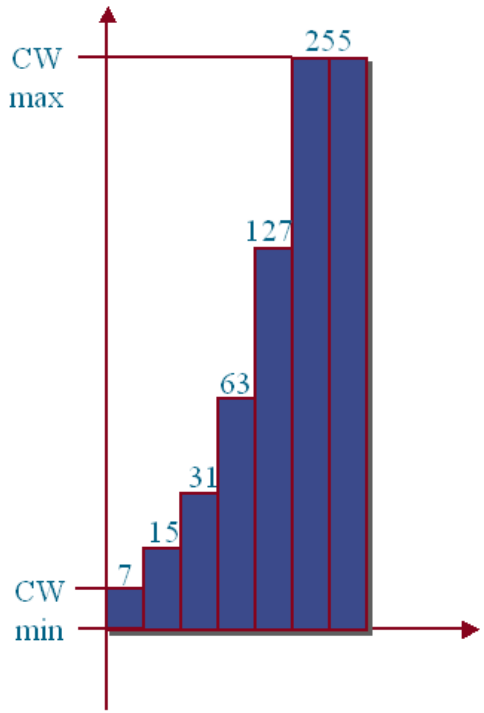
Access Spacing



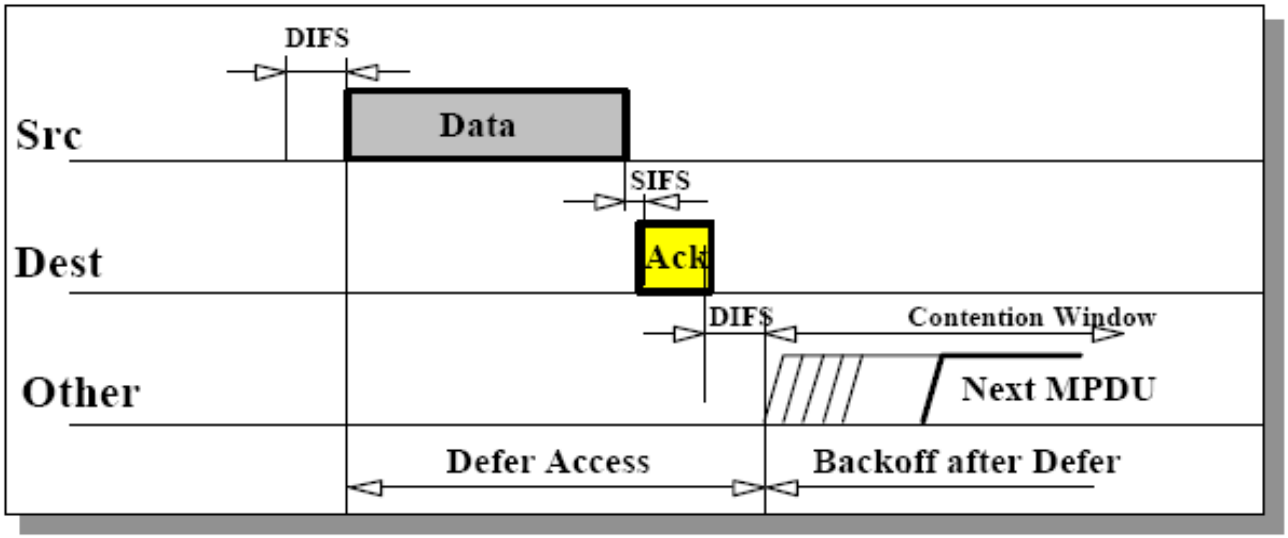
IFS	Interframe Space		
SIFS	Short IFS	Highest Priority	ACK,CTS, Poll Messages and Responses, CF-End
PIFS	PCF IFS	2nd priority	PCF Operation Mode (Beacon)
DIFS	DCF IFS	3rd priority	DCF Operation Mode (back-off, RTS)
EIFS	Extended IFS	Lowest priority	After detection of erroneous frame

Exponential Backoff

- If station tries to transmit and medium is busy, increase maximum *backoff time* exponentially
- Backoff Timer = Random () * Slot_Time
  - Random(): a pseudo random integer uniformly distributed over the interval [0, CW], where CW is a integer between CWmin and CWmax
    - newCW = oldCW * 2 + 1
  - Slot_Time: long enough for a station to detect if any other station has accessed the medium in that slot
- Exponential backoff executed:
  - First attempt at transmitting frame and medium was busy (initial window [0, CWmin])
  - For each retransmission (newCW computed)
  - After a successful transmission (window reduced to [0, CWmin])

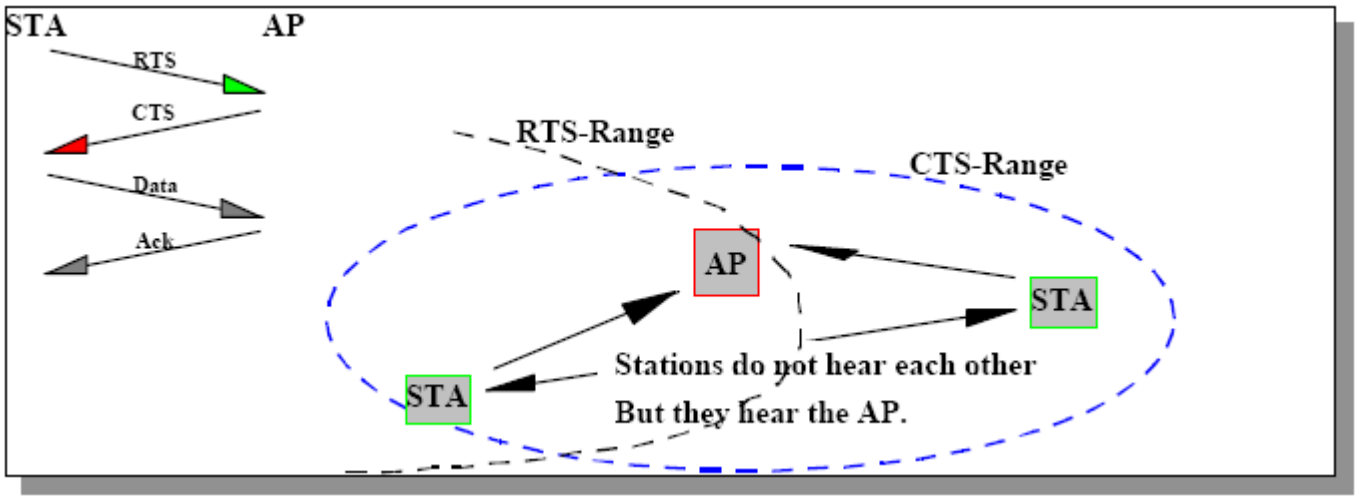


CSMA/CA + ACK protocol



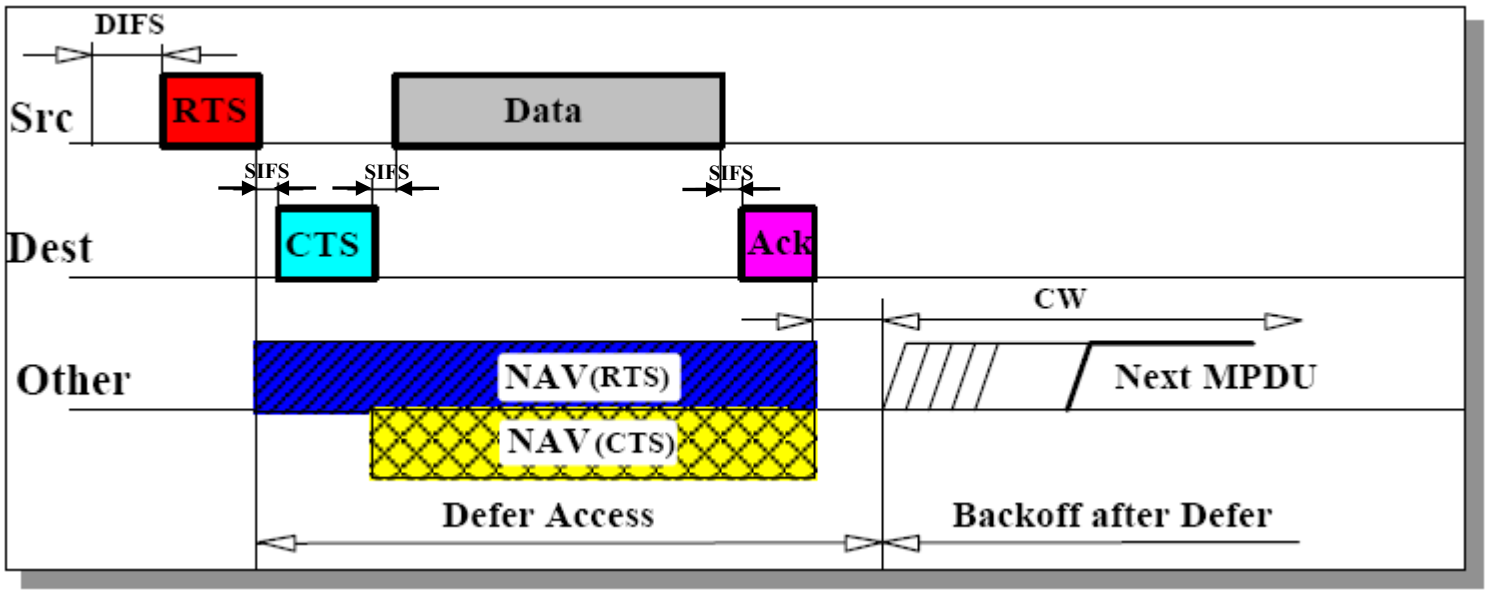
- Defer access based on Carrier Sense
  - CCA from PHY and Virtual Carrier Sense state
- Direct access when medium is sensed free longer than DIFS, otherwise defer and backoff
- Receiver of directed frames to return an ACK immediately when CRC correct
  - When no ACK received, then retransmit the frame after a random backoff (up to a maximum limit)
  - ACK is sent after SIFS (high priority)

"Hidden Node" Problem



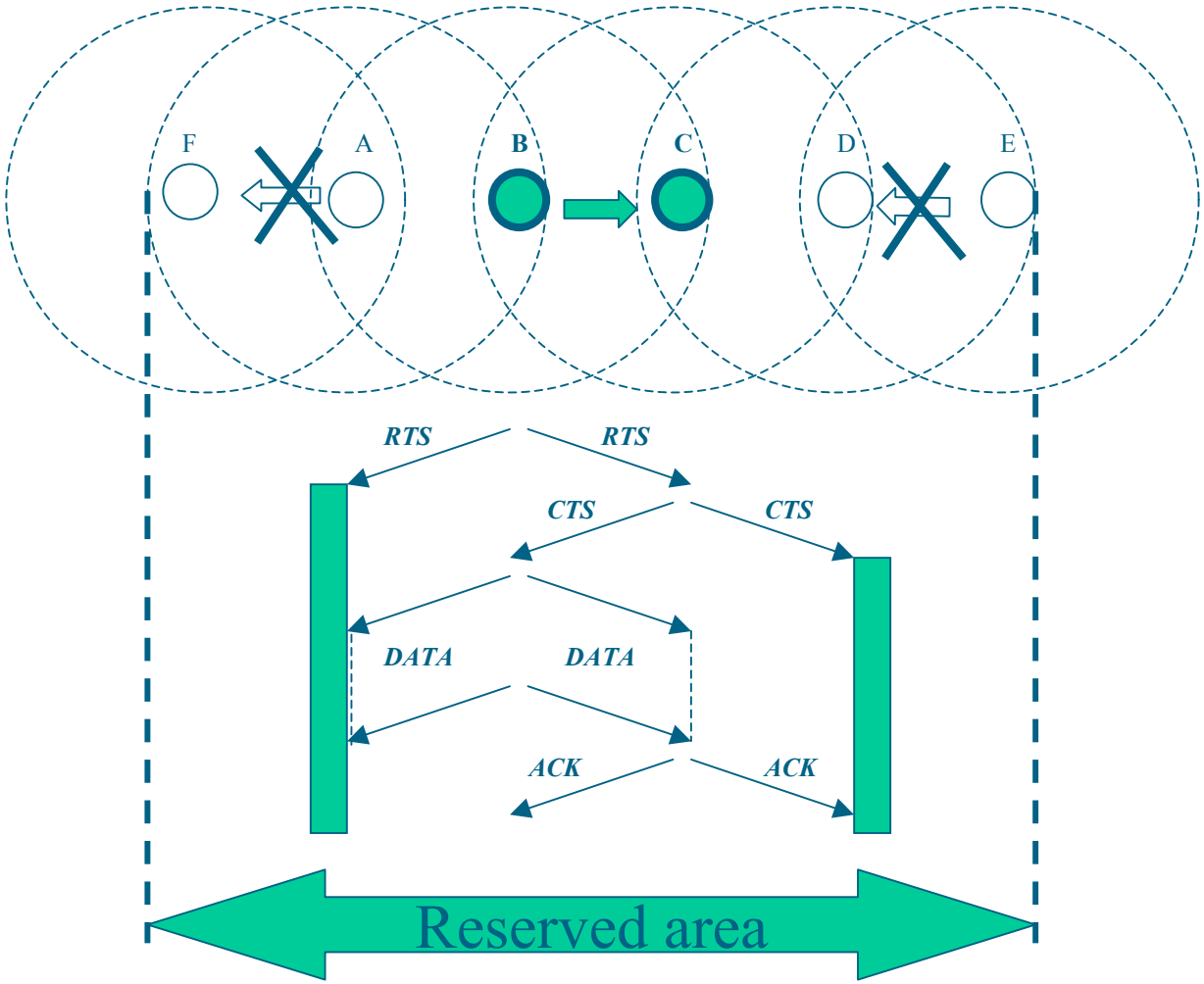
- Separate control frame exchange (RTS/CTS)
- Distribute duration around both Tx and Rx station

"Hidden Node" Provisions

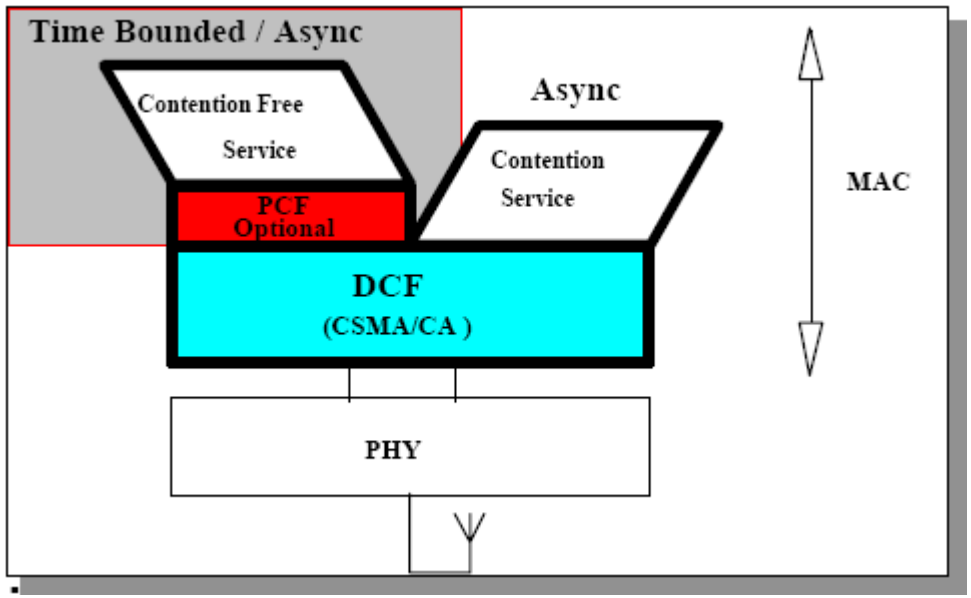


- *Duration* field in RTS and CTS frames distribute *Medium Reservation* information which is stored in a ***Network Allocation Vector*** *(NAV)*
- Defer on either NAV or "CCA" indicating ***Medium Busy***
- Use of RTS / CTS is optional but must be implemented
- Note use of high priority in CTS and ACK
- Note that NAV is a measure of TIME---not length; all control packets are sent at 1 Mbps so that all stations can hear them. Data may be sent at 1,2,5 or 11 Mbps in 802.11 b

“Exposed Node” Problem

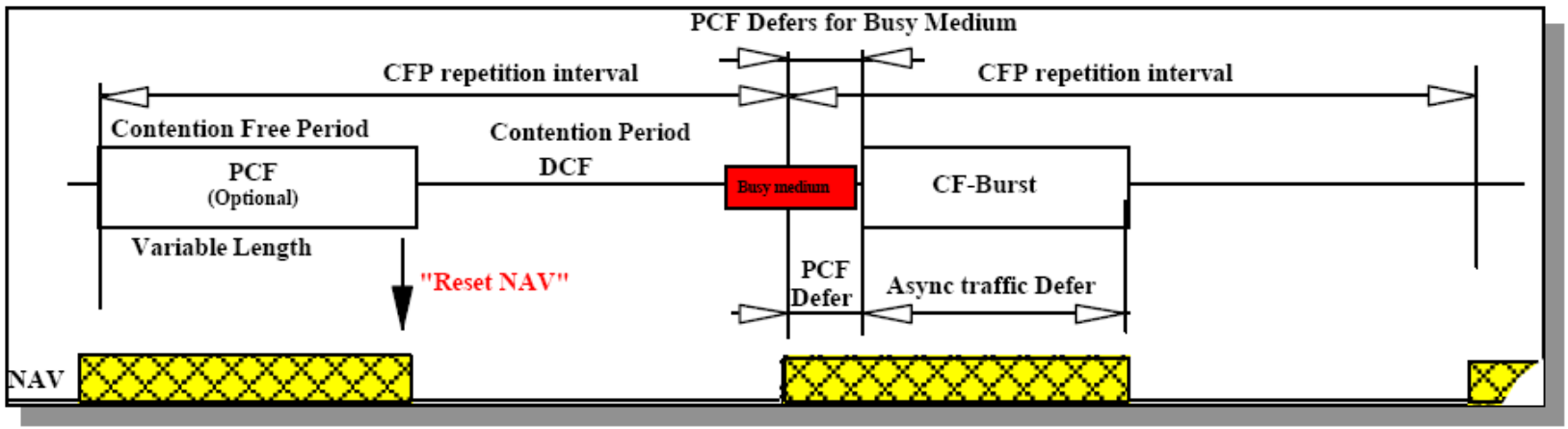


Optional Point Coordination Function (PCF)



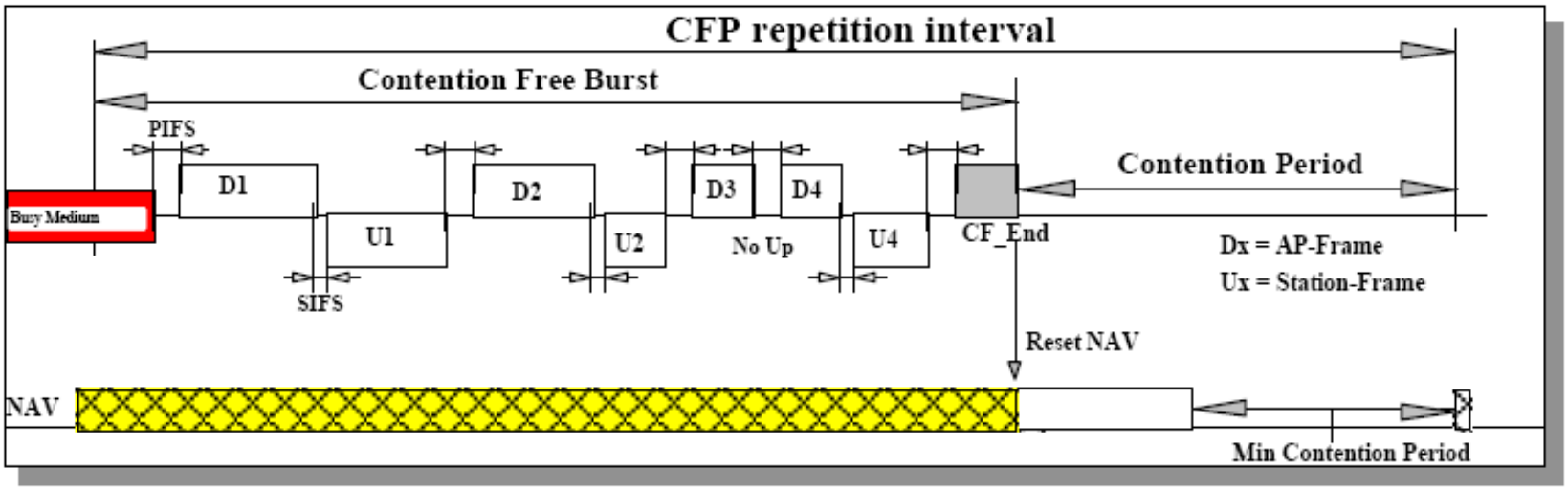
- Contention Free Service uses Point Coordination Function (PCF) on a DCF Foundation
  - lower transfer delay variations to support *Time Bounded Services*
  - Async Data, Voice or mixed implementations possible
  - Point Coordinator in AP
- Coexistence between Contention and optional Contention Free

Contention Free operation



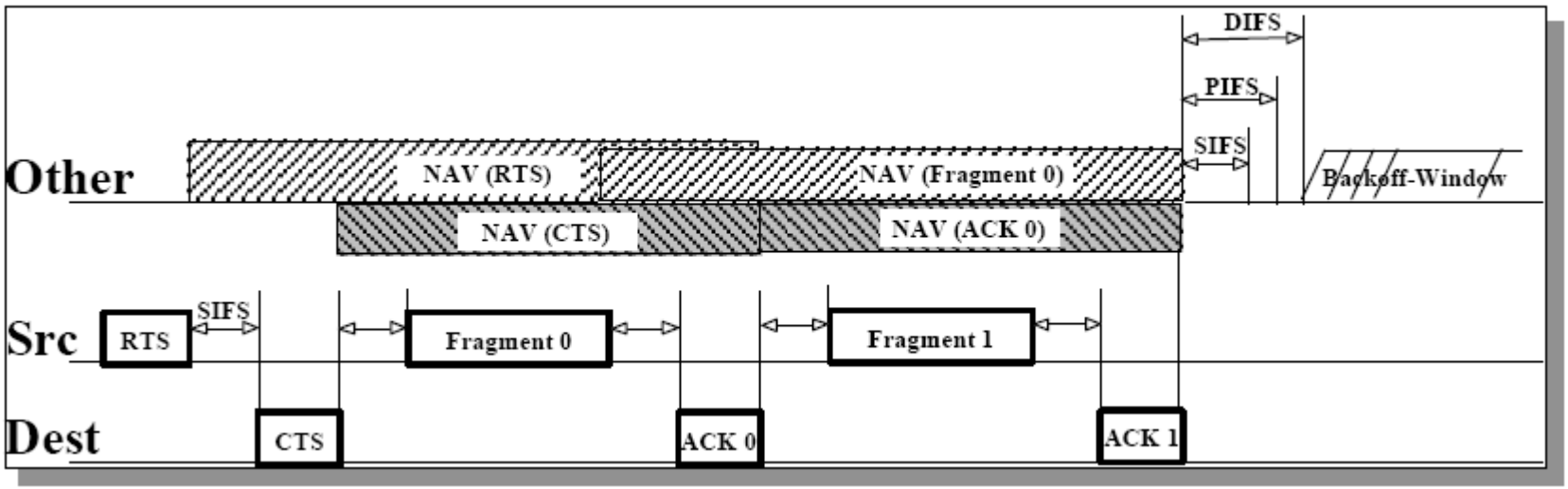
- Alternating *Contention Free* and *Contention* operation under PCF control
- NAV prevents *Contention* traffic until reset by the last PCF transfer
  - So variable length *Contention Free* period per interval
- Both PCF and DCF defer to each other causing PCF Burst start variations

PCF Burst



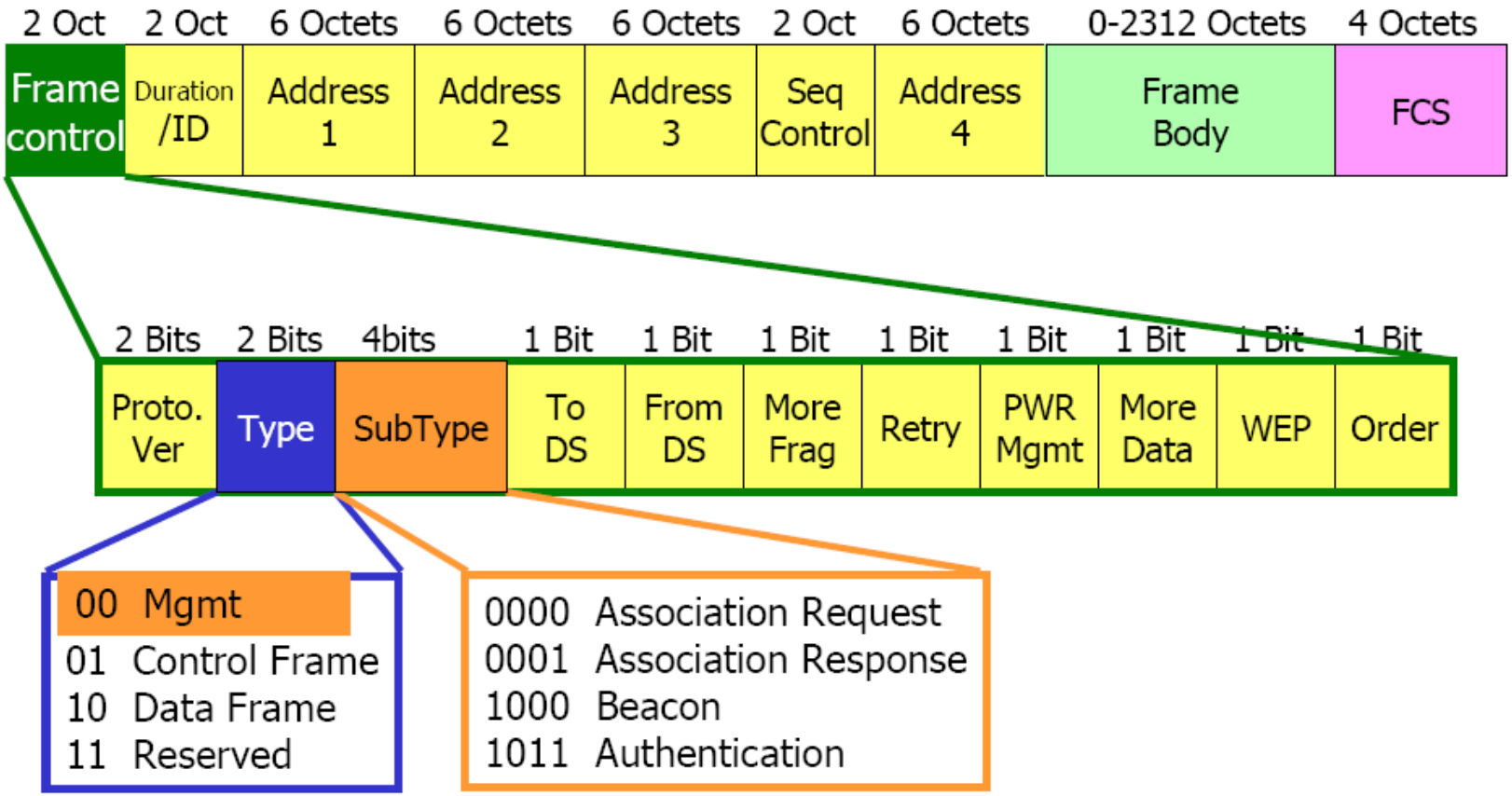
- CF-Burst by Polling bit in CF-Down frame
- Immediate response by Station on a CF_Poll
- Stations to maintain NAV to protect CF-traffic
- Responses can be variable length
- “Reset NAV” by last (CF_End) frame from AP
- "ACK Previous Frame" bit in Header

Fragmentation



- Individually acknowledged
  - for unicast frame only
- Random backoff and retransmission of failing fragment when no ACK is returned
- NAV to be set, for medium reservation mechanism

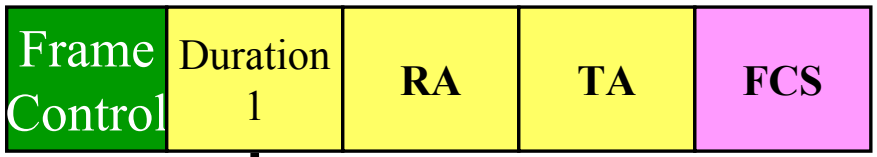
Frame Formats



- MAC header format differs for Type:
  - Control Frames
  - Management Frames
  - Data Frames

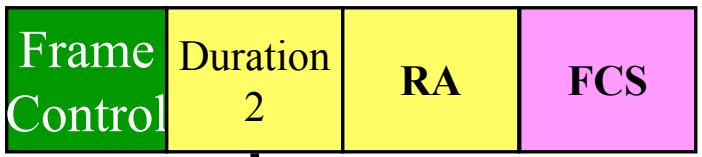
Control Frames: RTS-CTS-DATA-ACK

RTS frame



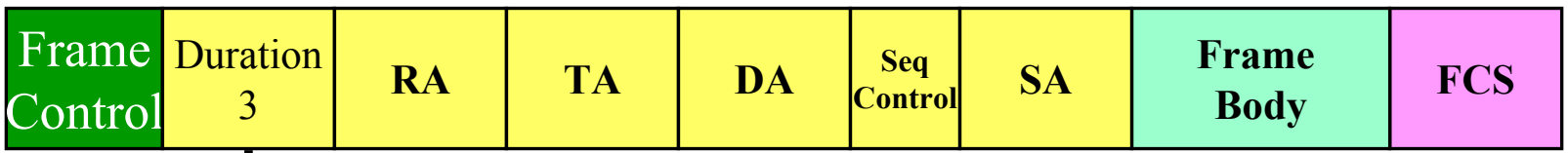
microsec = CTS + Data + ACK + 3SIFS

CTS frame



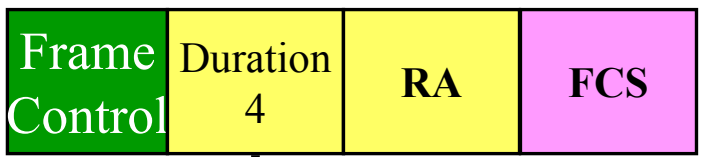
microsec = Duration 1 - CTS - SIFS

Data frame



microsec = Duration 2 – Data - SIFS

ACK frame



0

RA : Receiver Address
TA : Transmitter Address
DA : Destination Address
SA : Source Address
FCS : Frame Check sequence

Privacy and Access Control

- Goal of 802.11 is to provide "Wired Equivalent Privacy" (WEP)
  - Usable worldwide
- 802.11 provides for an Authentication mechanism
  - To aid in access control
  - Provisions for "OPEN", "Shared Key" or proprietary authentication extensions
- Optional (WEP) Privacy mechanism defined by 802.11
  - Limited for Station-to-Station traffic, so not "end to end"
    - embedded in the MAC entity
  - Only implements "Confidentiality" function
  - Only payload of Data frames are encrypted
    - encryption per MSDU basis

Access and privacy services

There are two characteristics of a wired LAN that are not inherent in a wireless LAN:

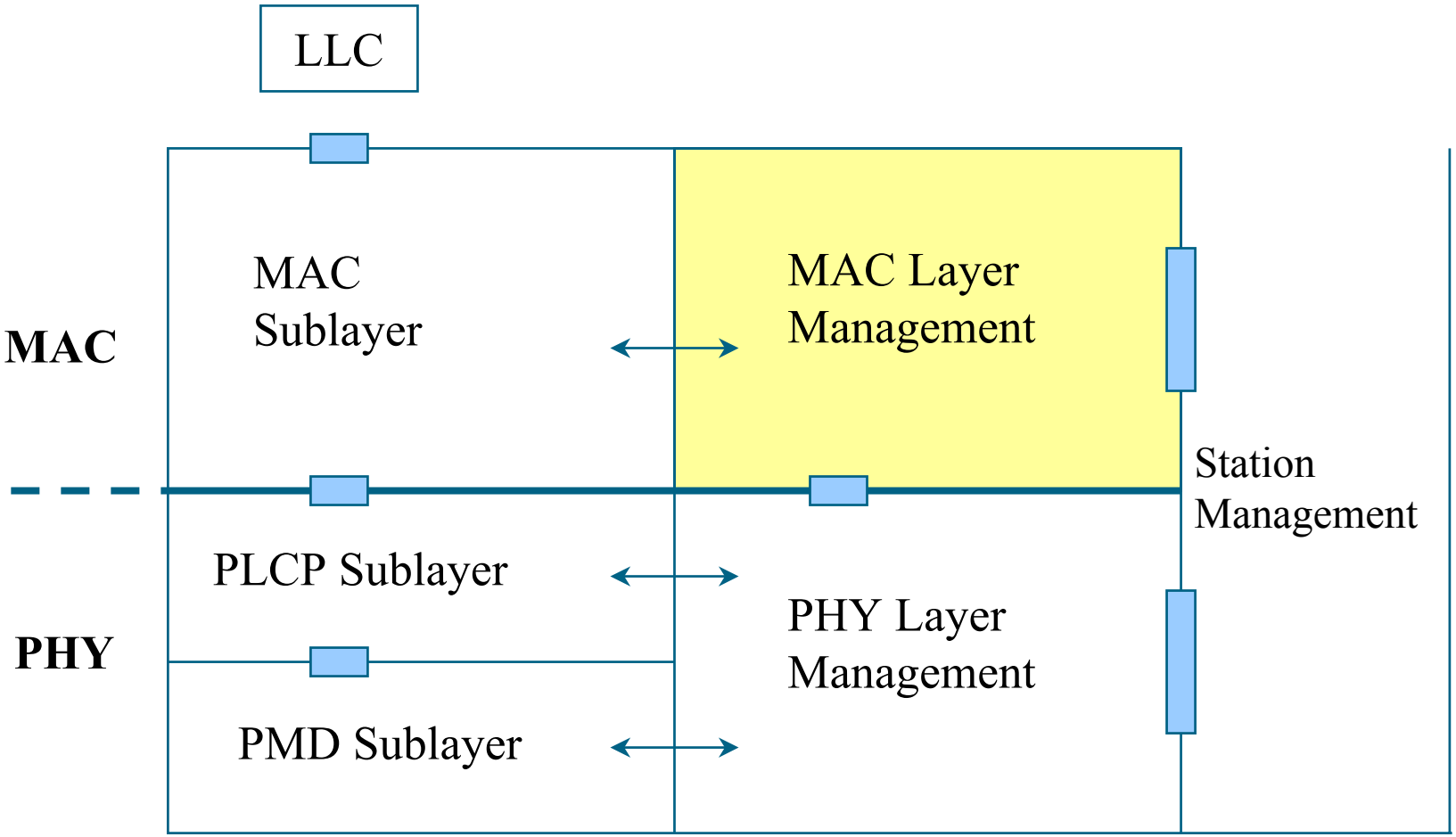
- In order to transmit on a wired LAN the station must be physically connected to the LAN: In a sense, this is a form of authentication inherent in a wired LAN.
- In order to receive a transmission from a station that is part of a wired LAN, the receiving station must be attached to that LAN: Thus, a wired LAN provides a degree of privacy.

Access and privacy services (2)

IEEE 802.11 defines three services to provide a wireless LAN with these two missing features:

- **Authentication:**.The authentication service is used by stations to establish their identity with stations they wish to communicate with. IEEE 802.11 supports several optional schemes: A station requires mutually acceptable, successful authentication before a station can associate with an AP
- **Deauthentication**: Invoked when existing authentication is terminated.
- **Privacy:** Used to prevent message contents from being read by an un-intended receiver. Standard provides optional use of encryption: WEP

MAC Layer Management



MAC Layer Management

- Synchronization
  - Finding and staying with a WLAN
  - Synchronization functions
    - TSF Timer, Beacon Generation
- Power Management
  - Sleeping without missing any messages
  - Power management functions
    - Periodic sleep, frame buffering, Traffic Indication Map
- Association and Reassociation
  - Joining a network
  - Roaming, moving from an AP to another
  - Scanning

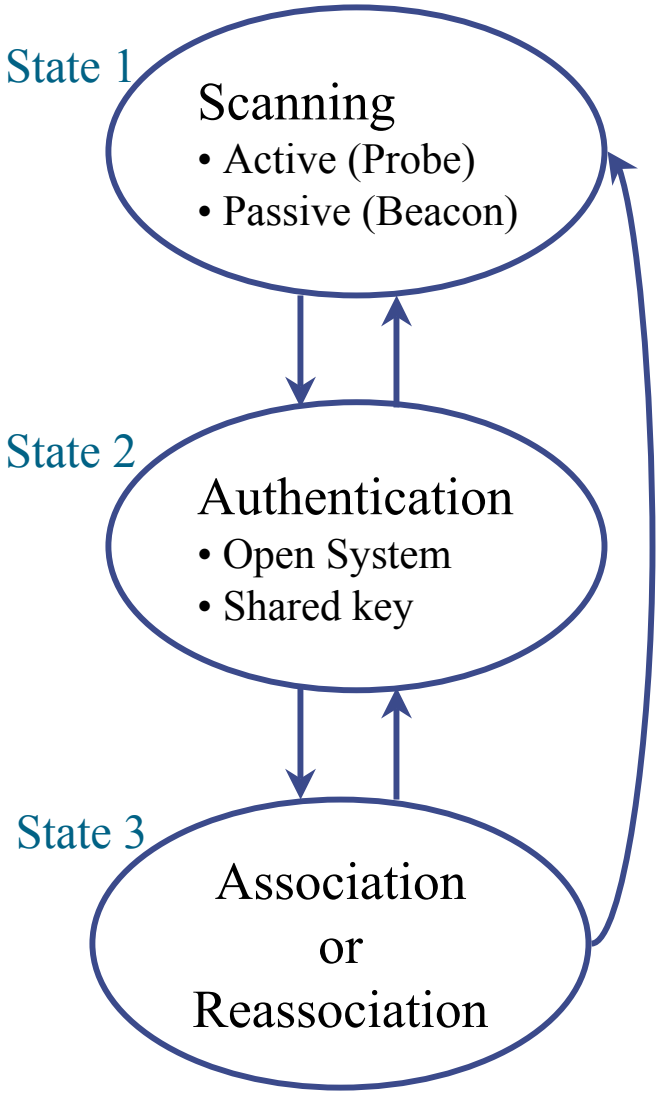
Synchronization in 802.11

- Timing Synchronization Function (TSF)
- Used for Power Management
  - Beacons sent at well-known intervals
  - All station timers in BSS are synchronized
- Used for Point Coordination Timing
  - TSF Timer used to predict start of Contention Free burst
- Used for Hop Timing for FH PHY
  - All Stations are synchronized, so they hop at the same time

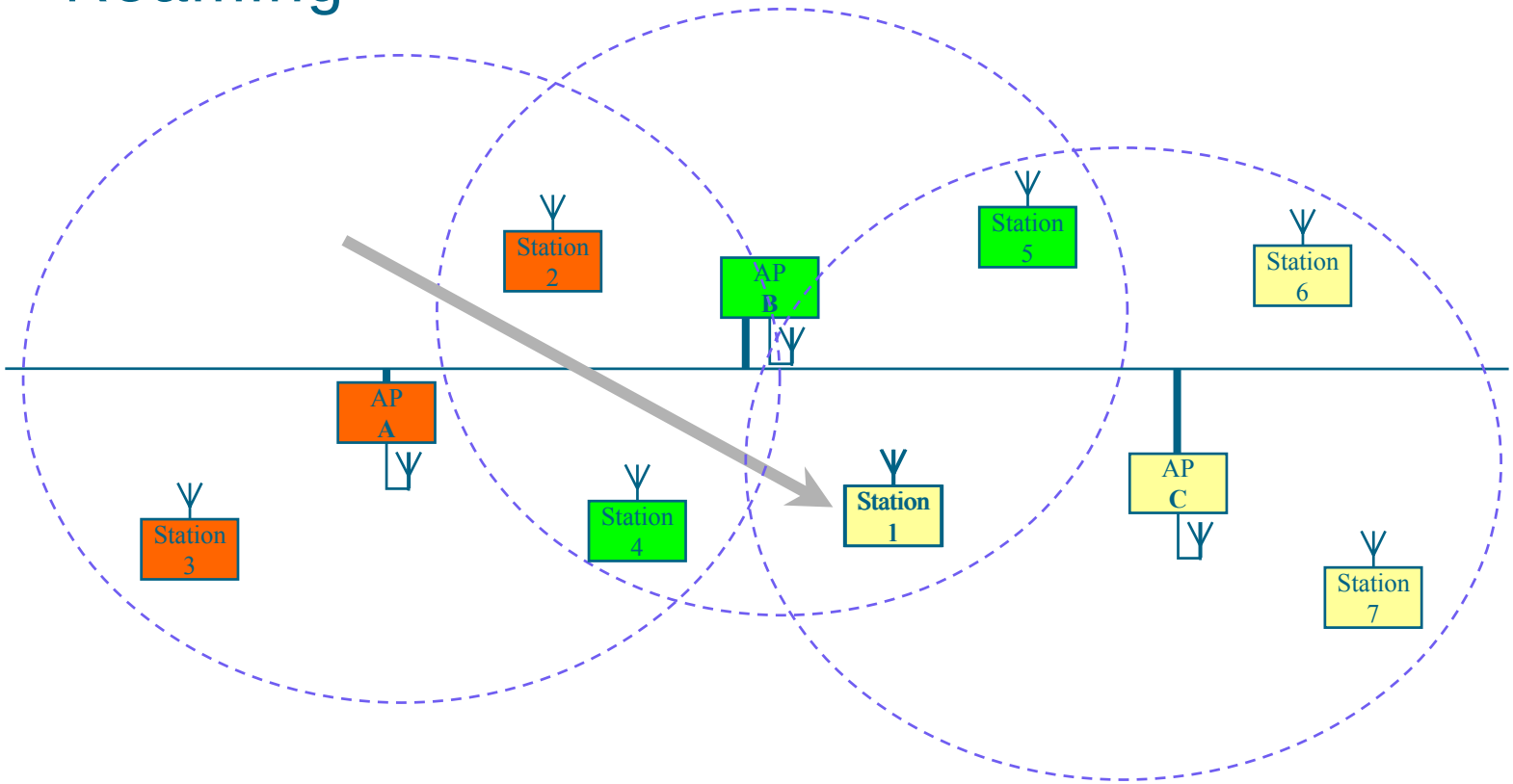
Power Management

- Mobile devices are battery powered.
  - *Power Management* is important for mobility
- Current LAN protocols assume stations are always ready to receive
  - Idle receive state dominates LAN adapter power consumption over time
- How can we power off during idle periods, yet maintain an active session?
- 802.11 Power Management Protocol:
  - Based on the fundamental transition strategy: *sleep on inactivity*
  - Messages are buffered at base stations
  - Mobile hosts wake up periodically to check for outstanding messages

Joining a Network



Roaming



- Mobile stations may leave…
  - the coverage area of their Access Point,
  - but they can get connected to another Access Point
- Reassociation allows station to continue operation

Association related services

Before DS can deliver data to or accept data from a station, that station must be *associated*: The set of related services support three transition types based on mobility.

- **No transition:** a station of this type is either stationary or moves only within the direct communications range of the communicating stations of a single BSS.
- **BSS transition:** defined as a station movement from one BSS to another BSS within the same ESS. Delivery of data to the station requires that the addressing capability be able to recognize the new location of the station.
- **ESS transition:** defined as a station movement from a BSS in one ESS to a BSS in another ESS. This requires upper-layer support and is beyond the scope of 802.11.

IEEE 802.11 Services

Association related services (2)

To deliver a message within a DS, the distribution service needs to know where the destination station is located: Specifically, the DS needs to know the identity of the AP to which the message should be delivered. There are three related services:

- **Association:** establishes initial association between a station and an AP.
- **Reassociation:** enables the transfer of an established association from one AP to another in the case of mobility.
- **Disassociation**: Notification that an existing association has been terminated (from the station or the AP).

IEEE 802.11 Services

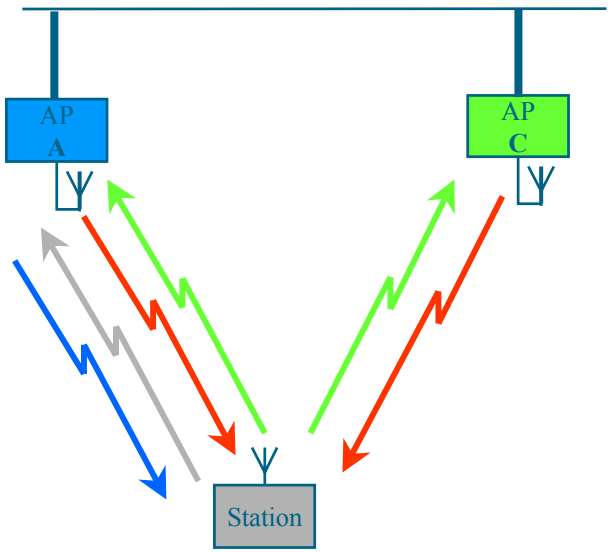
Roaming Approach

- Decide that link to its current AP is poor
- Use scanning function to find another AP
  - or use information from previous scans
- Send Reassociation Request to new AP
- If Reassociation Response is successful
  - then Roamed to the new AP
  - else Scan for another AP
- If AP accepts Reassociation Request
  - Indicate Reassociation to the Distribution System
  - Update Distribution System information
  - notify old AP through Distribution System

Scanning

- Scanning required for many functions
  - Finding and joining a network
  - Finding a new AP while roaming
  - Initializing an Independent BSS (ad hoc) network
- 802.11 MAC uses a common mechanism for all PHY technologies
  - Single or multichannel scanning
  - Passive scanning
    - Find networks simply by listening for beacons
  - Active scanning
    - On each channel, send a probe and wait for the response
- Beacon or probe response contains information necessary to join new network

Multi-channel and Active Scanning Example



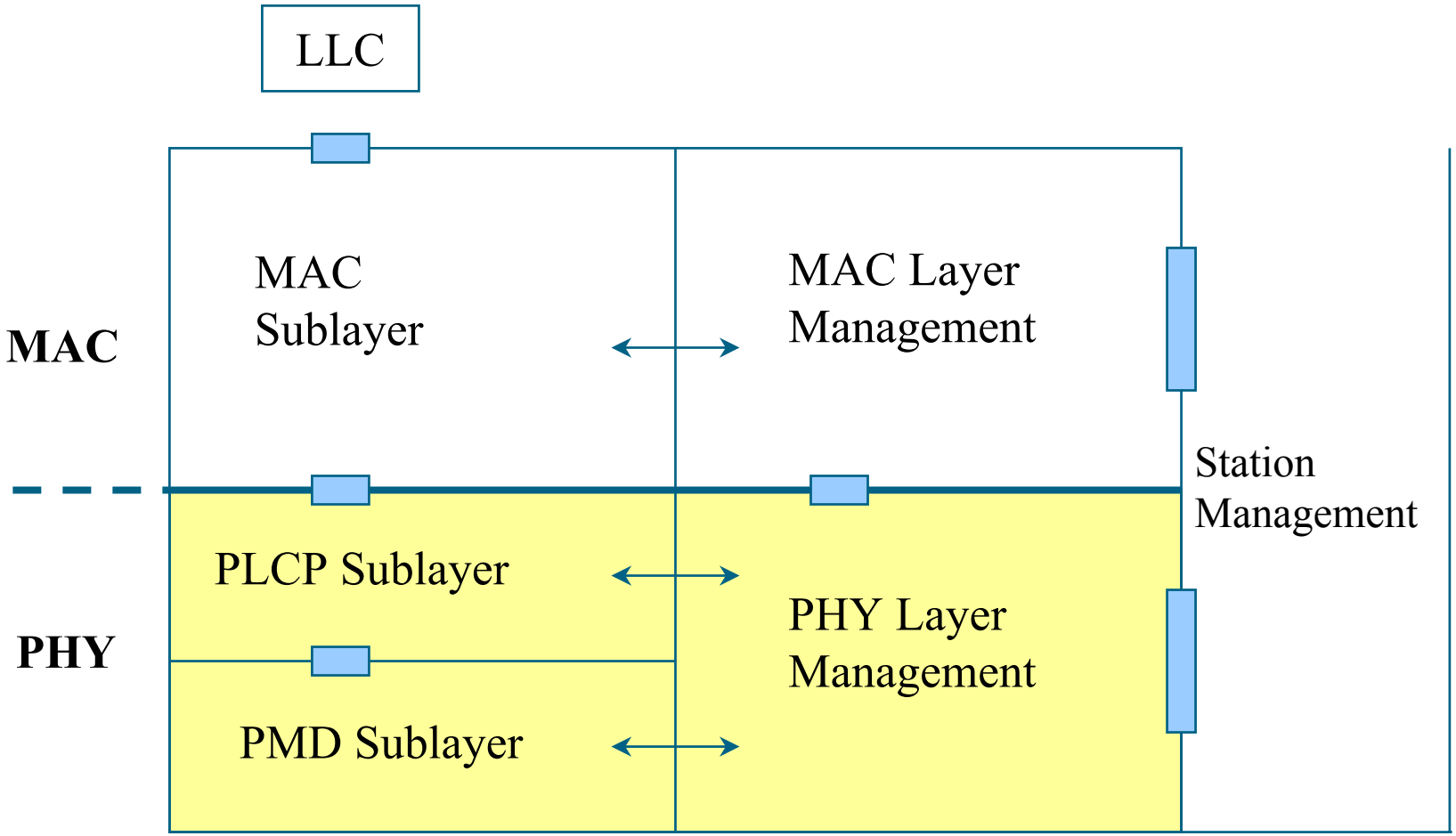
Steps to Association:

- Station send Probe
- APs send Probe Response
- Station selects best AP
- Station sends Association Request to selected AP, if the AP is good enough
- AP sends Association Response

802.11 PHY Entity

- Physical Layer Architecture
- Physical Layer Operations
- IEEE 802.11 Physical Layer
  - FHSS
  - DSSS
  - OFDM
  - IR

Physical Layer Architecture



PLCP Sublayer

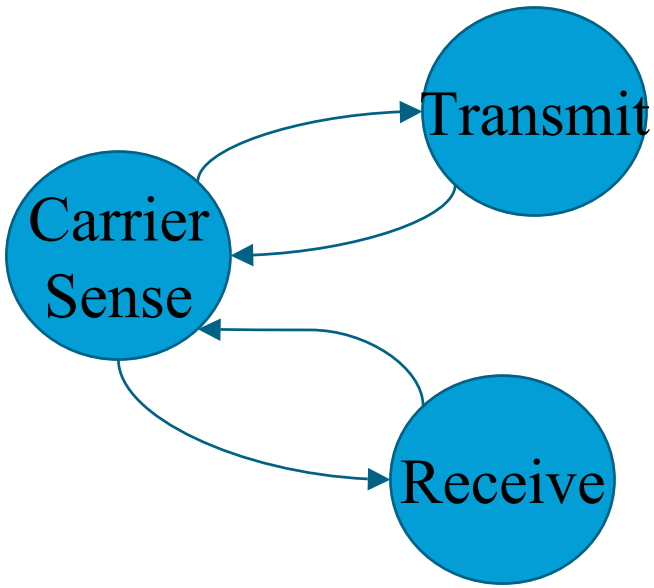
- Physical Layer Convergence Procedure
- Communicates to MAC via primitives through Physical Layer Service Access Point (SAP)
- Prepares PLCP protocol data unit (PPDU) (append fields to MPDU)
- PPDU provides for asynchronous transfer of MPDU between stations

PMD Sublayer

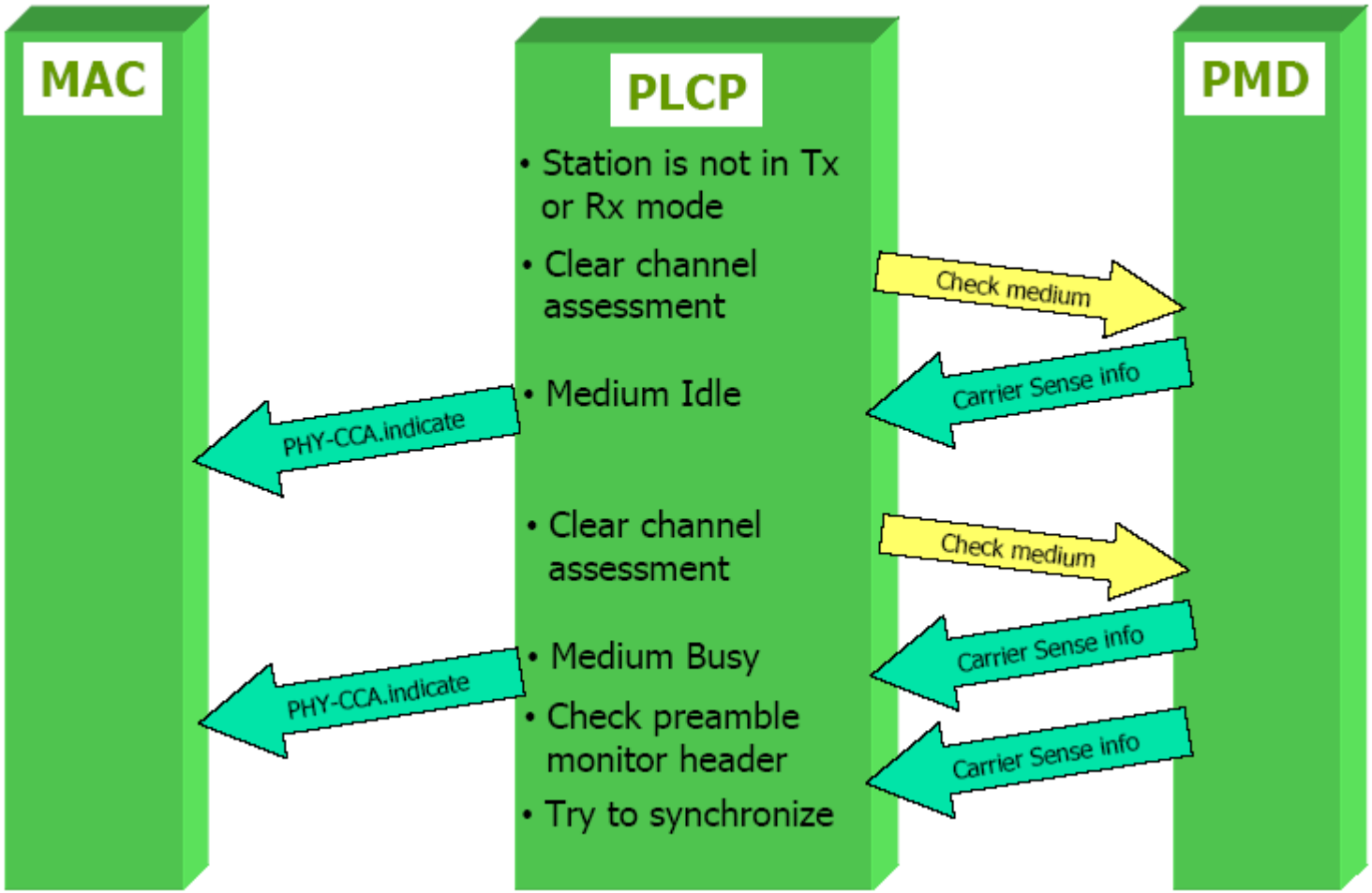
- Physical Medium Dependent
- Provides actual transmission and reception of Physical Layer entities through a wireless medium
- Interface directly to the medium
- Provides modulation and demodulation of the transmission frame

Physical Layer Operations

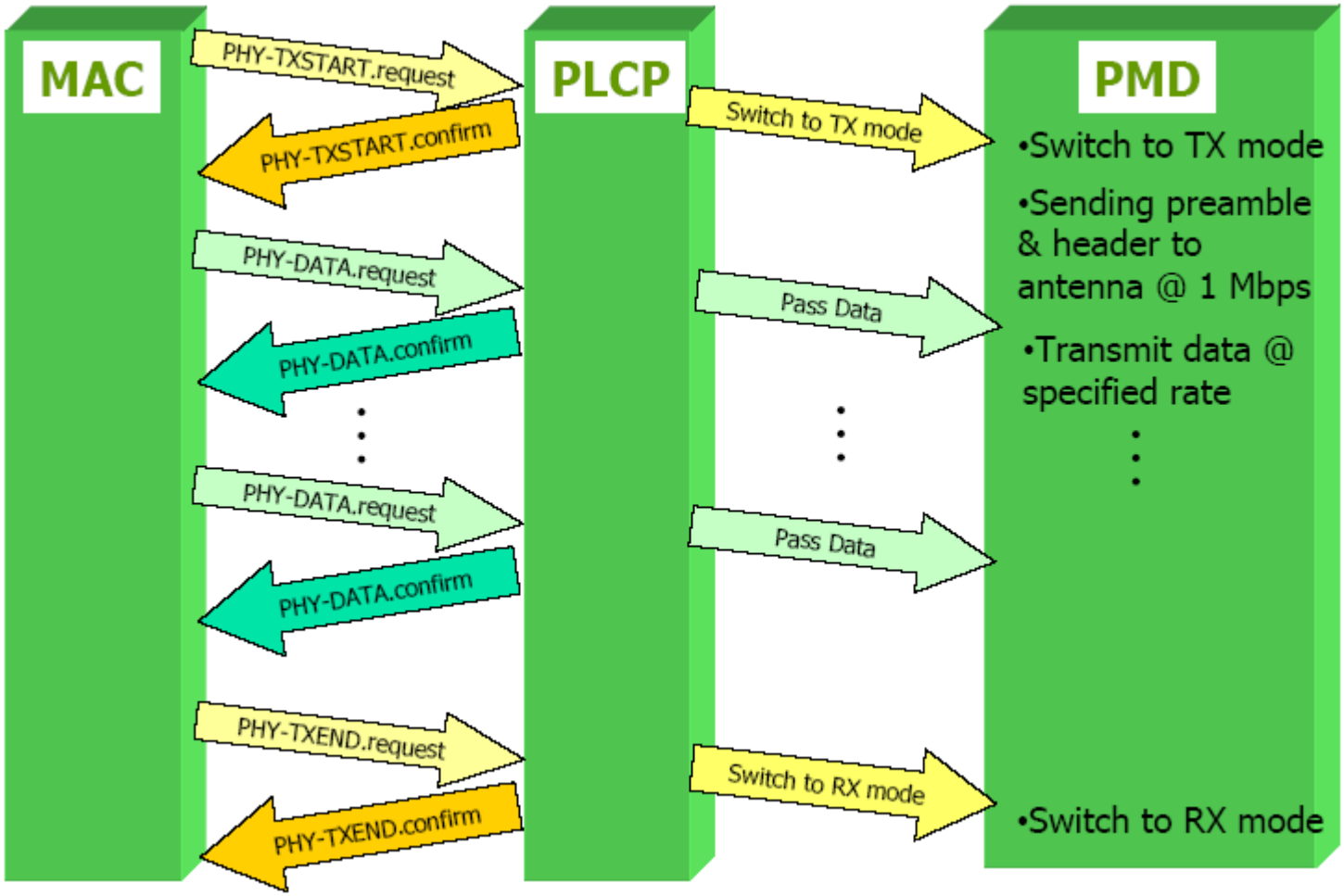
- A Three-State Machine
  - Carrier sense: determine the state of the medium
  - Transmit: send the data frame
  - Receive: receive the data frame



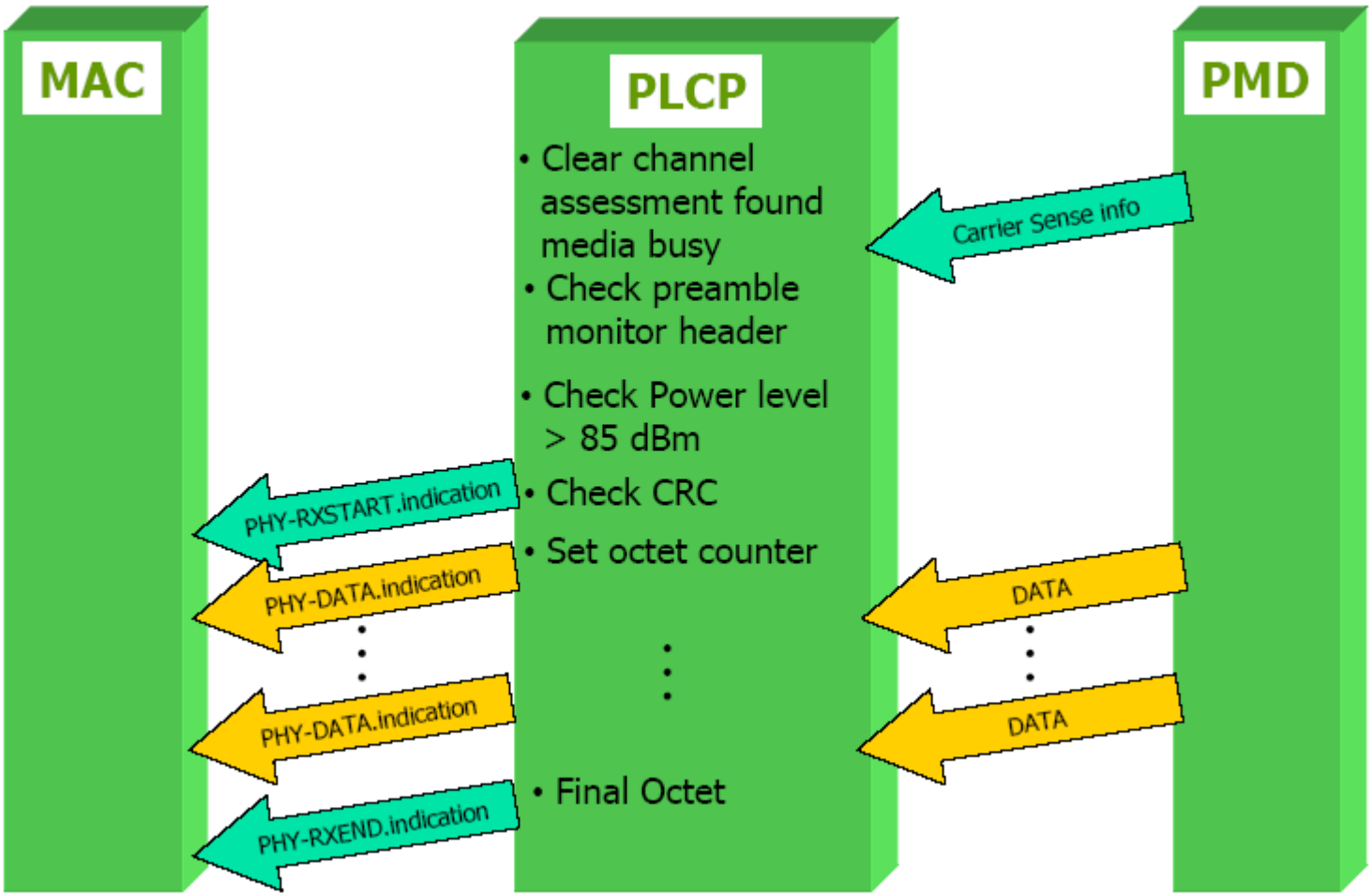
Carrier Sense Function



Transmit Function



Receive Function



IEEE 802.11 Physical Layer

- Frequency Hop Spread Spectrum
  - 2.4GHz band, 1 and 2 Mbps transmission
  - 2GFSK, 4GFSK
  - hop over 79 channels (North America)
- Direct Sequence Spread Spectrum
  - 2.4GHz band, 1, 2, 5.5 or 11 Mbps transmission
  - DBPSK, DQPSK
  - 11 chip Barker sequence
- Orthogonal Frequency Division Multiplexing
  - 2.4GHz & 5GHz, 6 to 54 Mbps
  - No Spread Spectrum
- Baseband IR
  - Diffuse infrared
  - 1 and 2 Mbps transmission, 16-PPM and 4-PPM

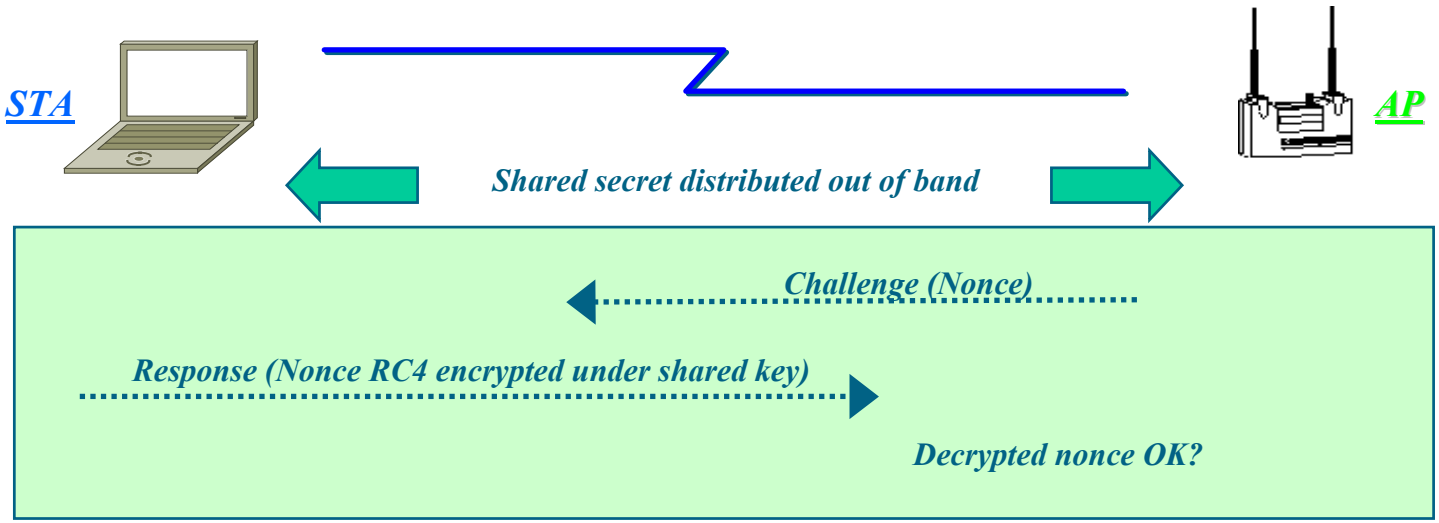
IEEE 802.11 Security

- 802.11 Security Today
- What's Wrong Today?
- 802.11i introducing New Security Mechanisms
- 802.11i: Proposed Authentication, Authorization, and Key Management

802.11 Security Today

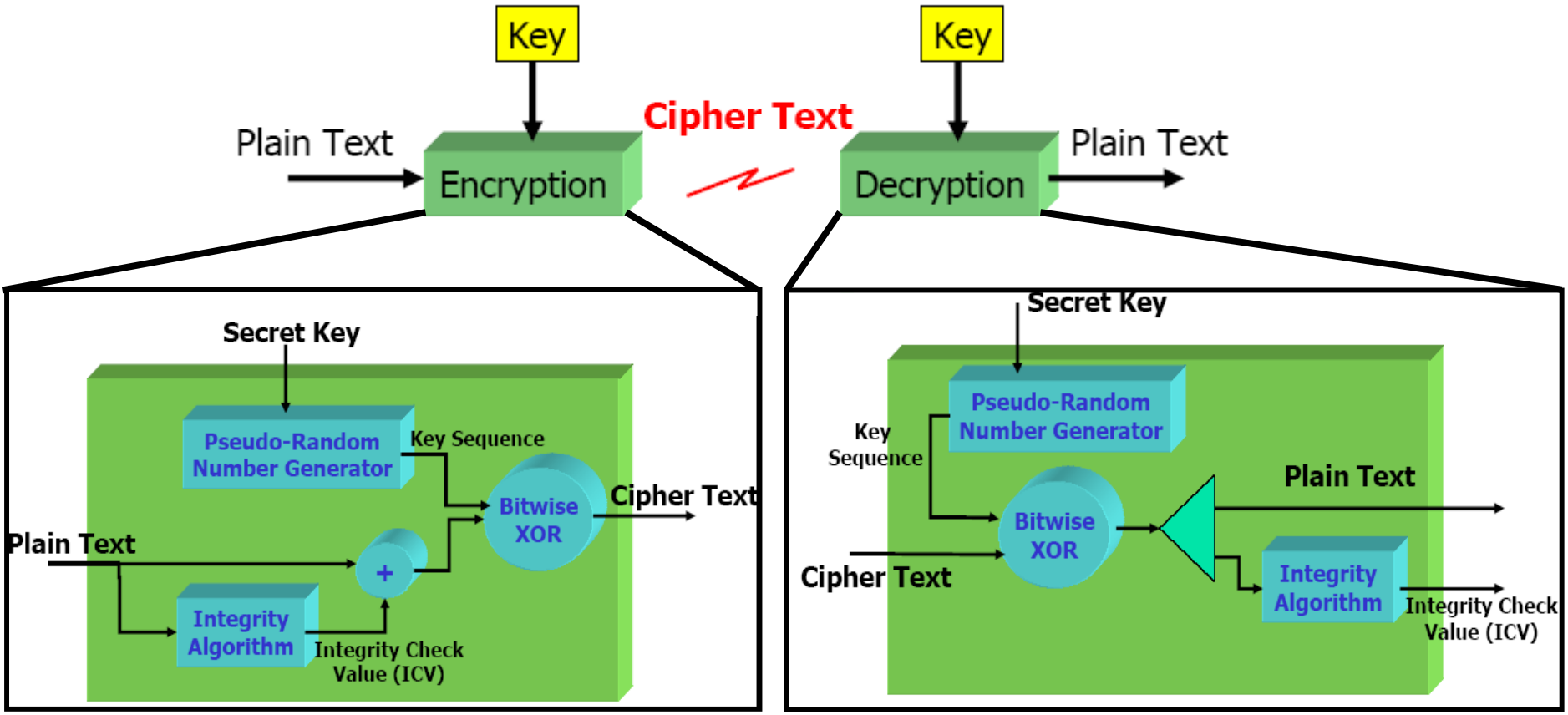
- Goals of existing 802.11 security
  - Create the privacy achieved by a wired network
    - Only prevent intellectual property from leaking through casual browsing
  - Simulate physical access control by denying access to unauthenticated stations
- Existing security consists of two subsystems
  - An authentication algorithm called Shared Key Authentication
  - A data encapsulation technique called ***W***ired ***E***quivalent ***P***rivacy (WEP)

Shared Key Authentication



- Authentication key distributed out-of-band
- Access Point generates a “randomly generated” challenge
- Station encrypts challenge using pre-shared secret

Wired Equivalent Privacy (WEP)



- Encryption Algorithm,RC4,
- Per-packet encryption key = 24-bit Initialization Vector(IV) concatenated to a pre-shared key
- WEP allows IV to be reused with any frame
- Data integrity provided by CRC-32 of the plaintext data (the “ICV”)
- Data and ICV are encrypted under the per-packet encryption key

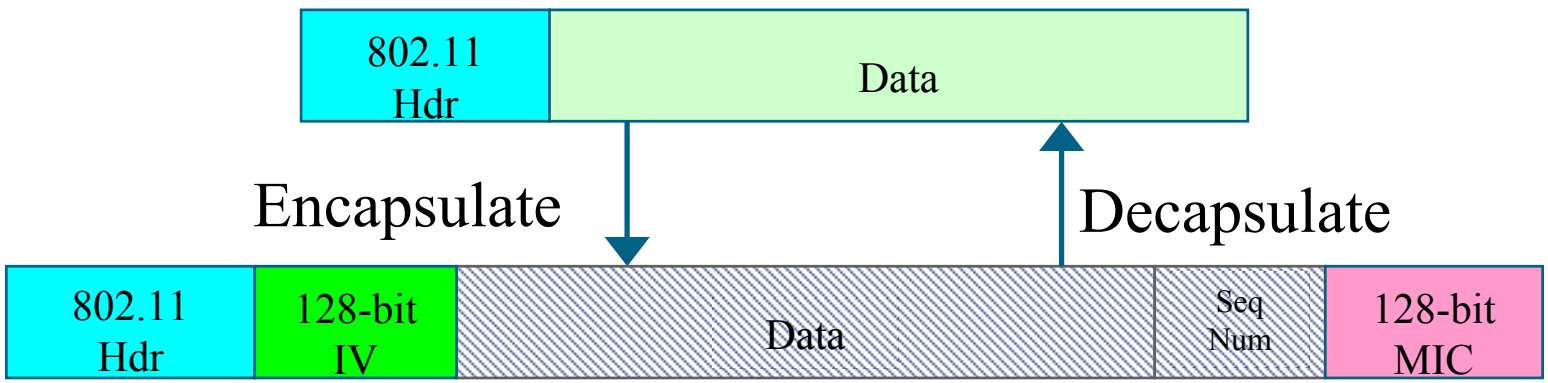
What is Wrong with 802.11 security?

- WEP
  - uses a synchronous cipher over a medium, where it is difficult to ensure synchronization during a complete session
  - concatenates the IV directly to the pre-shared key to produce a key for RC4, thus exposing the base-key to direct attack
  - only provides a method for authenticating stations to access points, not the other way around
  - Not robust enough to completely protect against eavesdropping
- No Secret Key distribution mechanism for sharing keys over an insecure medium
- very limited key-space for the IV since each packet needs to have a separate key for the network to be really secure
- CRC-32 used for message integrity is linear

802.11i introducing New Security Mechanisms

New Encryption:

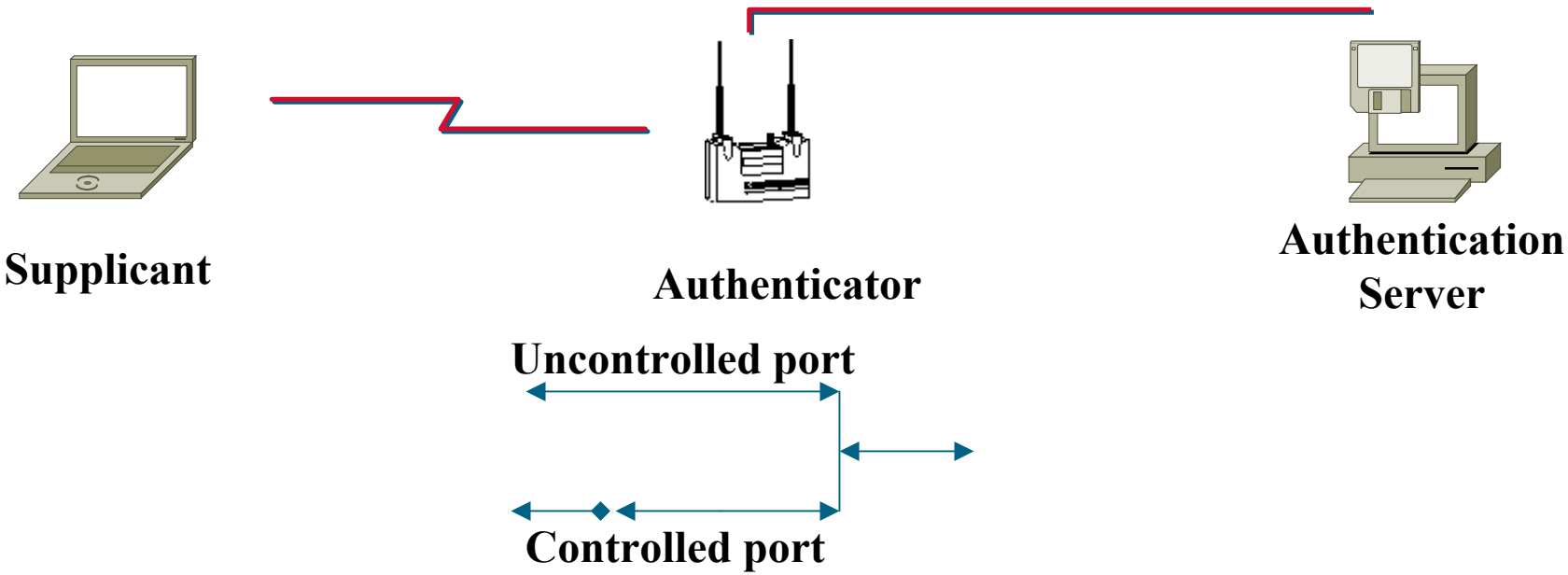
- Use Advanced Encryption Standard, AES-128, as the new cryptographic primitive
- Use AES in Offset Codebook Mode (OCB) mode
  - algorithm provides both privacy and data integrity
- Add session sequence number to avoid replay
- Map base key to session key
  - use OCB mode tag to compute session key, to minimize number of cryptographic primitives implemented



802.11i: Proposed Authentication, Authorization, and Key Management

- Based on existing protocols
  - Kerberos V (RFC 1510)
  - GSS-API (RFC 2743)
  - IAKERB (draft-ietf-cat-iakerb-05.txt)
  - EAP-GSS (draft-aboba-pppext-eapgss-02.txt)
  - EAP (RFC 2284)
  - 802.1X/EAPOL
- 802.11i enhancements
  - MAC security management
  - New model for authentication/association sequences

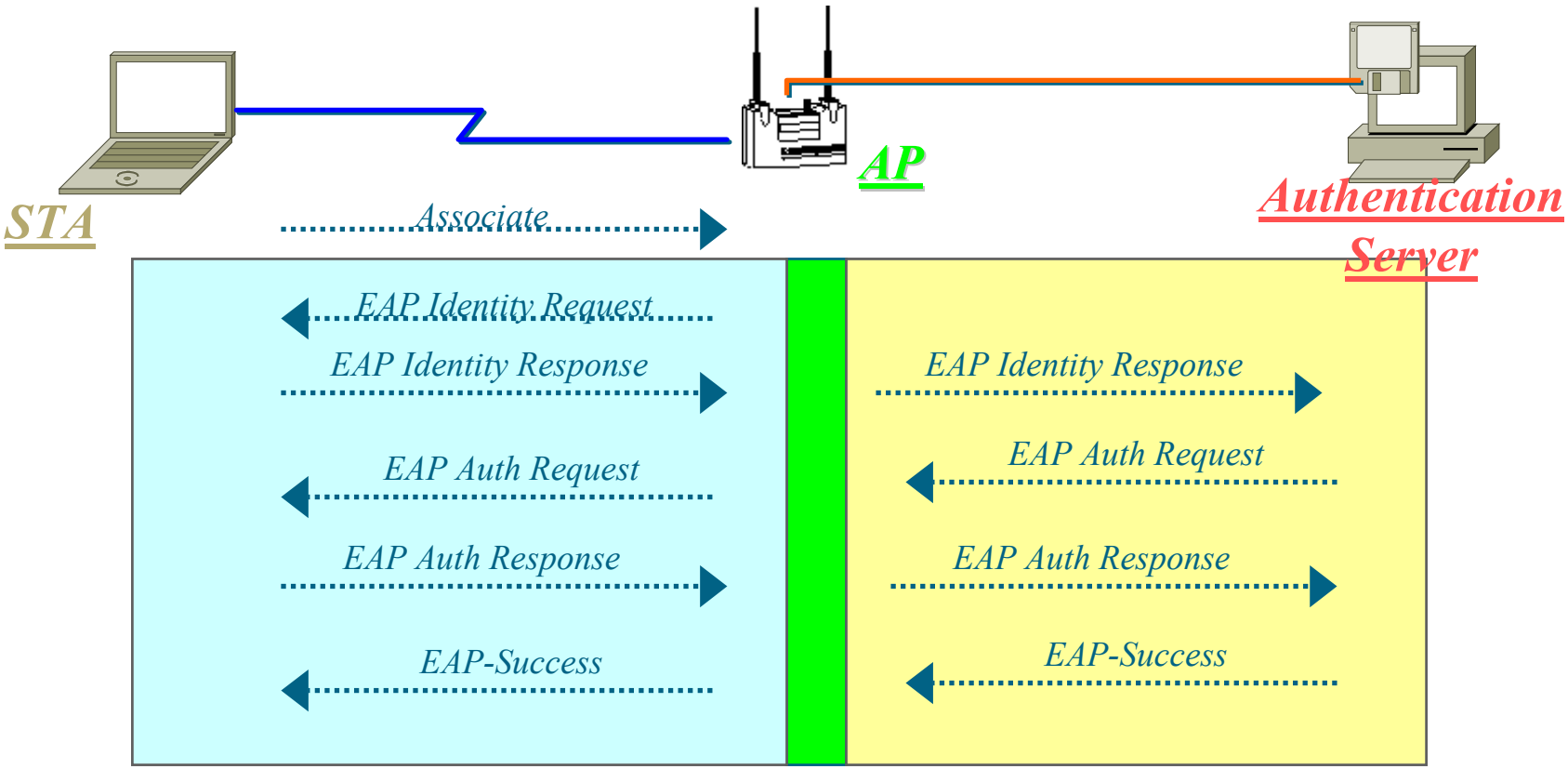
IEEE 802.1x Terminology



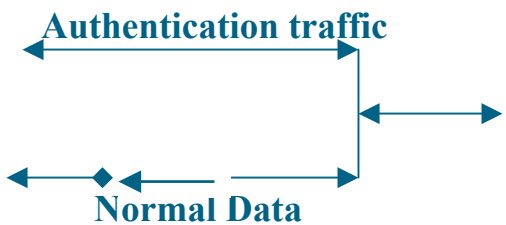
802.1x

- Created to control access to any 802 LAN
- Used as a transport for ***Extensible Authentication Protocol*** (EAP, RFC 2284)

802.1x Model



Port Status:



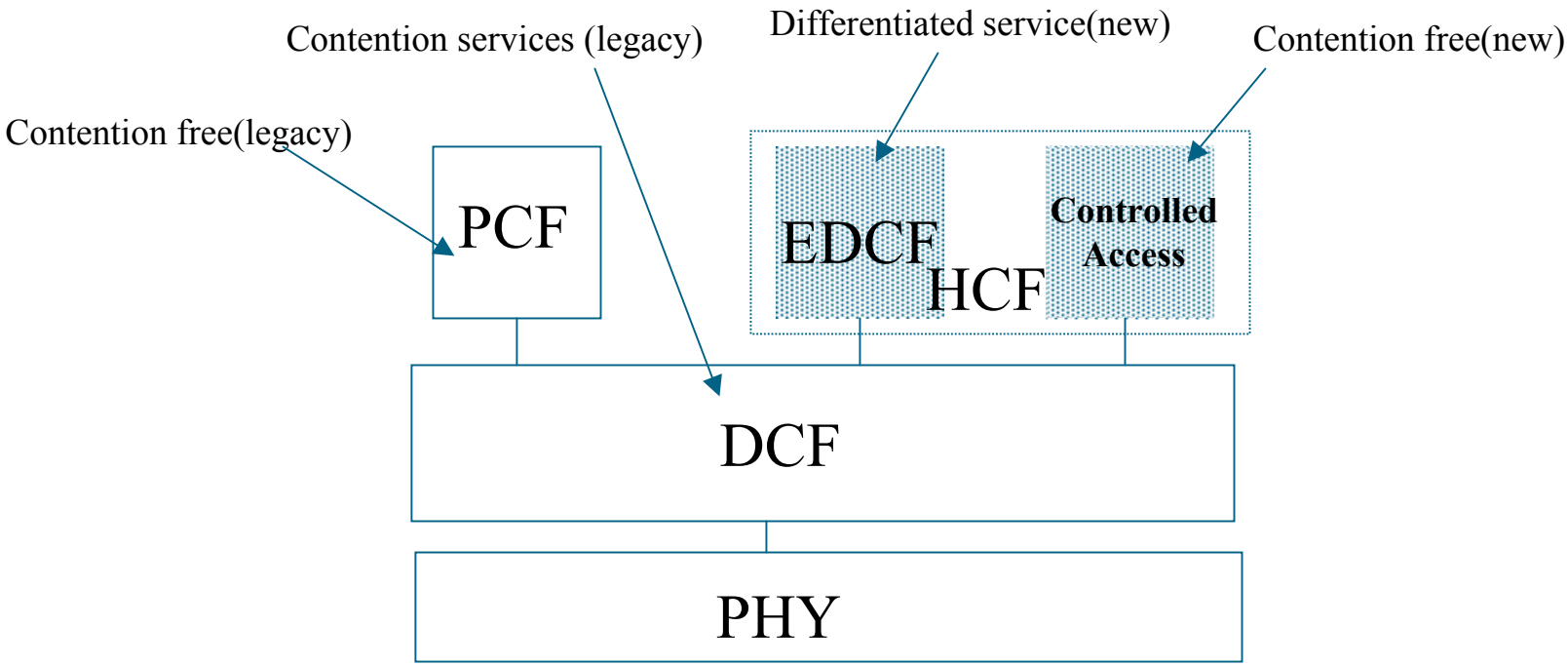
IEEE 802.11e

- The Draft 802.11e Standard Supplement
- IEEE 802.11e Protocol Entities
- EDCF

The Draft 802.11e Standard Supplement

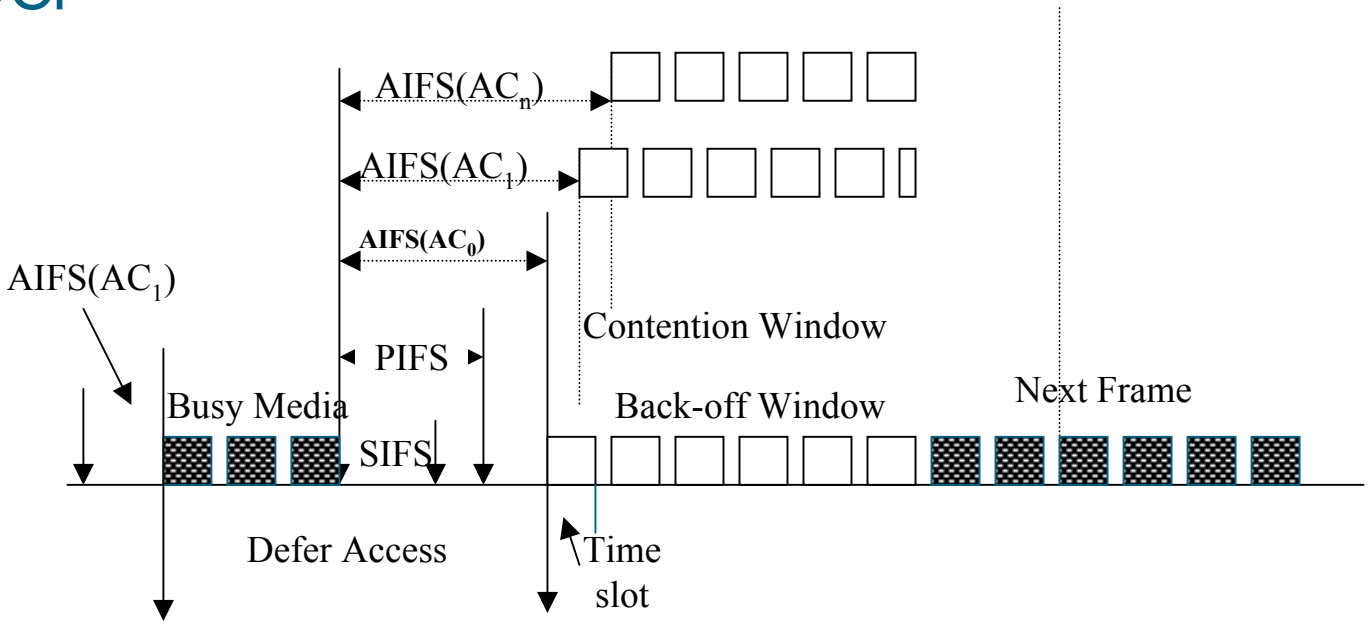
- Different requirements for high-layer applications such as data, video, and audio
  - Bandwidth
  - Delay
  - Jitter
  - Packet loss
- No differentiation mechanism to support the transmission of data streams with different Quality of Service (QoS) requirements in the DCF of IEEE802.11
- IEEE802.11 working group is currently developing 802.11e to support applications with QoS
- Focused on two applications:
  - A/V capability for consumer devices – need to handle at least three simultaneous DVD rate MPEG-2 channels, or one HDTV rate MPEG-2 channel over 802.11a
  - Managed QoS for corporate networks – provide prioritization that integrates with network management infrastructures
- Backward-compatible with existing systems; non-802.11e stations operate as best effort
  - consumers will still want to take their laptops home from work, and will expect to access multimedia applications

IEEE 802.11e Protocol Entities



- HCF: Hybrid CF
  - Both contention-based and controlled contention-free channel access methods in a single access protocol
  - Functions from the DCF and PCF with some enhanced QoS-specific mechanisms
- EDCF: Enhanced DCF
  - The contention based medium access method for HCF

EDCF



- 4 Access Class (AC) : 0,1,2,3 with different AIFS, and CWmin and CWmax parameters
- AIFS[AC]: Replaces DIFS by Arbitration IFS (AIFS) for different category of Access Class.
- AIFS[AC$_n$] = AIFS[AC]*slot-time + SIFS

EDCF Parameters of 4 classes

AC	CW_{min}	CW_{max}	AIFS
0	aCW_{min}	aCW_{max}	2
1	aCW_{min}	aCW_{max}	1
2	$(aCW_{min}+1)/2 -1$	aCW_{max}	1
3	$(aCW_{min}+1)/4 -1$	$(aCW_{max}+1)/2 -1$	1

Conclusion

- Wireless LANs will
  - Continue to become faster
  - Become embedded in our lives
  - Increase the average person's access to the world
- 802.11 is a widely accepted IEEE standard for wireless LANs
  - One of the most deployed wireless networks in the world
  - Highly likely to play major role in multimedia home networks and next-generation wireless communications
- 802.11 security doesn't meet any of its security objectives today
  - 802.11 Task Group I (TGi) is working to replace
    - Authentication scheme using 802.1X and Kerberos
    - Encryption scheme using AES in OCB mode
- 802.11e is based on over a decade of experience in design of WLAN protocols
  - Built from the ground up for real-world wireless conditions
  - Backward-compatible with 802.11

References

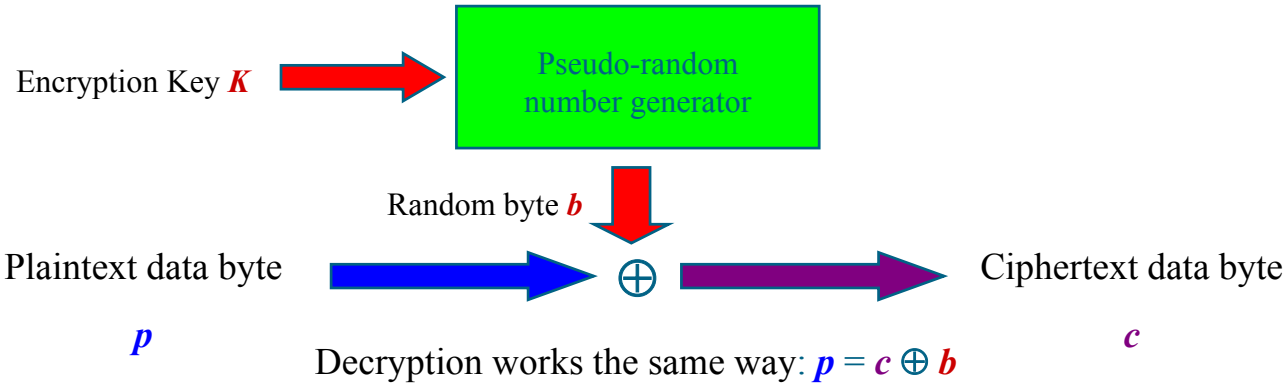
- Wireless LANs
  - http://grouper.ieee.org/groups/802/15/pub/2001/Sep01/Misc/MITWF.ppt
  - http://www.cat.utexas.edu/docs/Oct10TechMeeting/Wireless%20Communications.pdf
- 802.11 Protocol Standards
  - http://www.ieee802.org/11/
  - http://grouper.ieee.org/groups/802/11/main.html
- 802.11 Security
  - W. A. Arbaugh, "Your 802.11 Wireless Network has No Clothes", IEEE Wireless Communications, December 2002
  - http://grouper.ieee.org/groups/802/15/pub/2001/Mar01/01154r0P802-15_TG3-Overview-of-802-11-Security.ppt
- 802.11e
  - S. Mangold, "IEEE 802.11e Wireless LAN for Quality of Service"
  - D. Gu, "QoS Enhancement in IEE802.11 Wireless Local Area Networks", IEEE Communications Magazine, June 2003
- Performance Simulation Results
  - B. Giuseppe, "Performance Analysis of the IEEE 802.11 Distributed Coordination Function", IEEE Communications, March 2000
  - H. F. Chuan, "Performance Analysis of the IEEE 802.11 MAC Protocol", European Wireless 2002

Appendix

- Security
  - Properties of Vernam Ciphers
  - How to read WEP Encrypted Traffic
  - How to authentication without the key
  - Traffic modification
- 802.11e
  - Virtual Backoff
  - HCF

Properties of Vernam Ciphers

The WEP encryption algorithm RC4 is a Vernam Cipher:



Thought experiment 1: what happens when p_1 and p_2 are encrypted under the same "random" byte b?

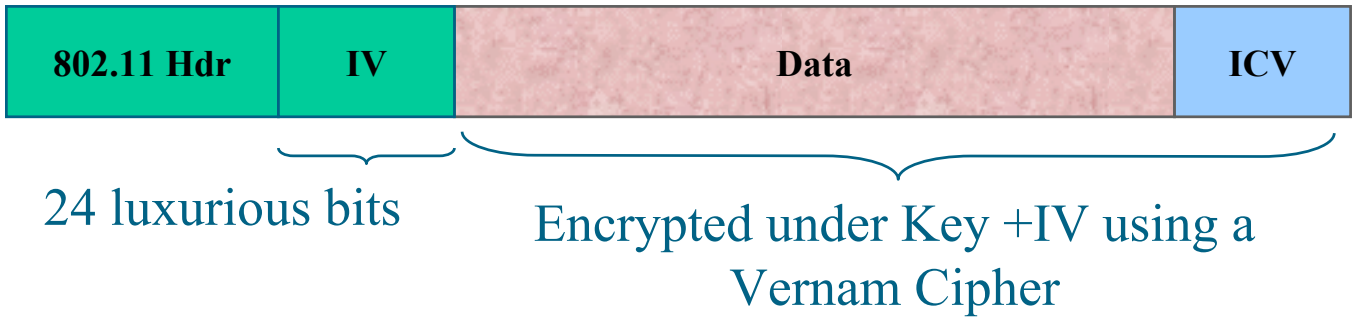
$$c_1 = p_1 \oplus b \qquad c_2 = p_2 \oplus b$$

Then:

$$c_1 \oplus c_2 = (p_1 \oplus b) \oplus (p_2 \oplus b) = p_1 \oplus p_2$$

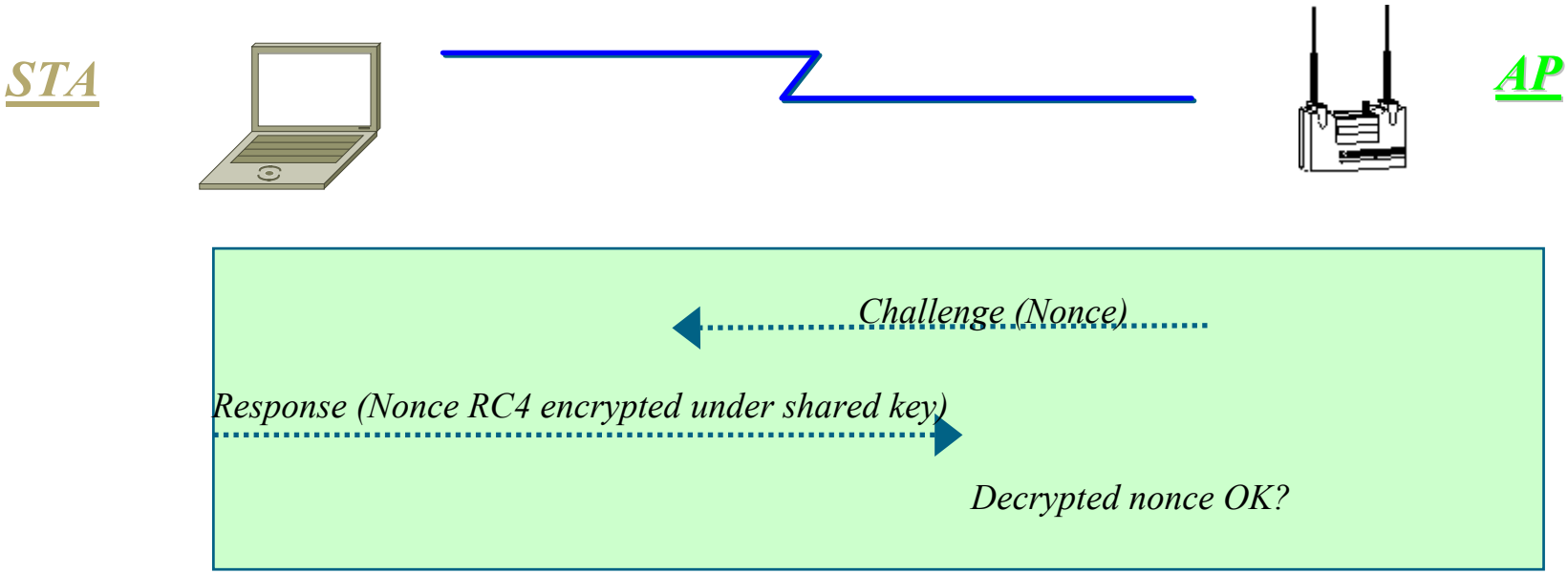
Conclusion: it is a very bad idea to encrypt any two bytes of data using the same byte output by a Vernam Cipher PRNG.

How to Read WEP Encrypted Traffic



- By the Birthday Paradox, probability P_n two packets will share same IV after n packets is $P_2 = 1/2^{24}$ after two frames and $P_n = P_{n-1} + (n-1)(1-P_{n-1})/ 2^{24}$ for n > 2.
- 50-percent chance of reuse of an IV value exists already after only 4823 packets!!!
- Pattern recognition can disentangle the XOR'd recovered plaintext.
- Recovered ICV can tell you when you've disentangled plaintext correctly.
- After only a few hours of observation, you can recover all 2^{24} key streams.
- Ways to accelerate the process:
  - Send spam into the network: no pattern recognition required!
  - Get the victim to send e-mail to you
    - The AP creates the plaintext for you!
  - Decrypt packets from one Station to another via an Access Point
    - If you know the plaintext on one leg of the journey, you can recover the key stream immediately on the other

How to Authenticate without the Key



- With our background, an easy attack is obvious:
  - Record one challenge/response with a sniffer
  - Use the challenge to decrypt the response and recover the key stream
  - Use the recovered key stream to encrypt any subsequent challenge

Traffic Modification

Vernam cipher thought experiment 2: how hard is it to change a genuine packet's data, so ICV won't detect the change?

Answer: Easy as pie

Represent an n-bit plaintext as an n-th degree polynomial:

$$\boldsymbol{p} = p_n x^n + p_{n-1} x^{n-1} + \ldots + p_0 x^0 \qquad (\text{each } p_i = 0 \text{ or } 1)$$

Then the plaintext with ICV can be represented as :

$$\boldsymbol{p}x^{32} + \mathrm{ICV}(\boldsymbol{p}) = \boldsymbol{p}_n x^{n+32} + \boldsymbol{p}_{n-1} x^{n-31} + \ldots + \boldsymbol{p}_0 x^{32} + \mathrm{ICV}(\boldsymbol{p})$$

If the n+32 bit RC4 key stream used to encrypt the body is represented by the n+32nd degree polynomial $\boldsymbol{b}$, then the encrypted message body is

$$\boldsymbol{p}x^{32} + \mathrm{ICV}(\boldsymbol{p}) + \boldsymbol{b}$$

But the ICV is linear, meaning for any polynomials p and q

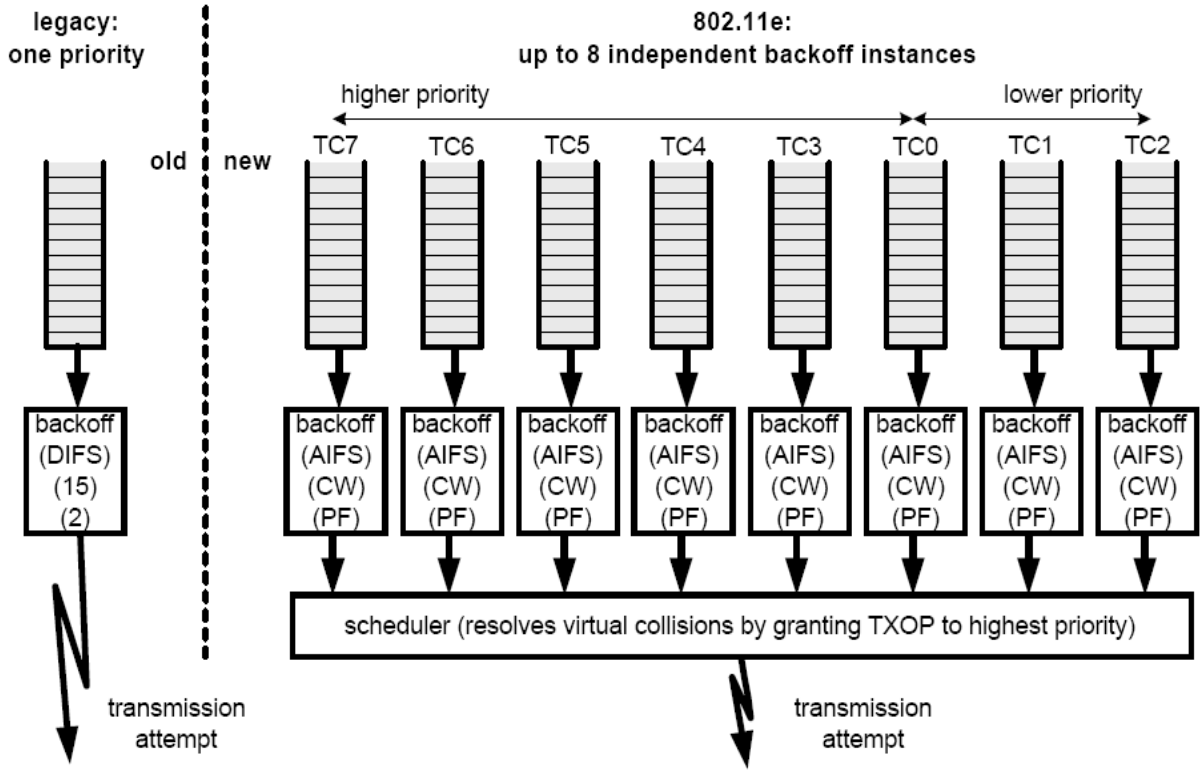
$$\mathbf{ICV}(\boldsymbol{p}+\boldsymbol{q}) = \mathbf{ICV}(\boldsymbol{p}) + \mathbf{ICV}(\boldsymbol{q})$$

This means that if q is an arbitrary nth degree polynomial, i.e., an arbitrary change in the underlying message data:

$$\begin{aligned}(\boldsymbol{p}+\boldsymbol{q})x^{32} + \mathrm{ICV}(\boldsymbol{p}+\boldsymbol{q}) + \boldsymbol{b} &= \boldsymbol{p}x^{32} + \boldsymbol{q}x^{32} + \mathrm{ICV}(\boldsymbol{p}) + \mathrm{ICV}(\boldsymbol{q}) + \boldsymbol{b} \\ &= ((\boldsymbol{p}x^{32} + \mathrm{ICV}(\boldsymbol{p})) + \boldsymbol{b}) + (\boldsymbol{q}x^{32} + \mathrm{ICV}(\boldsymbol{q}))\end{aligned}$$

Conclusion: Anyone can alter an WEP encapsulated packet in arbitrary ways without detection!!

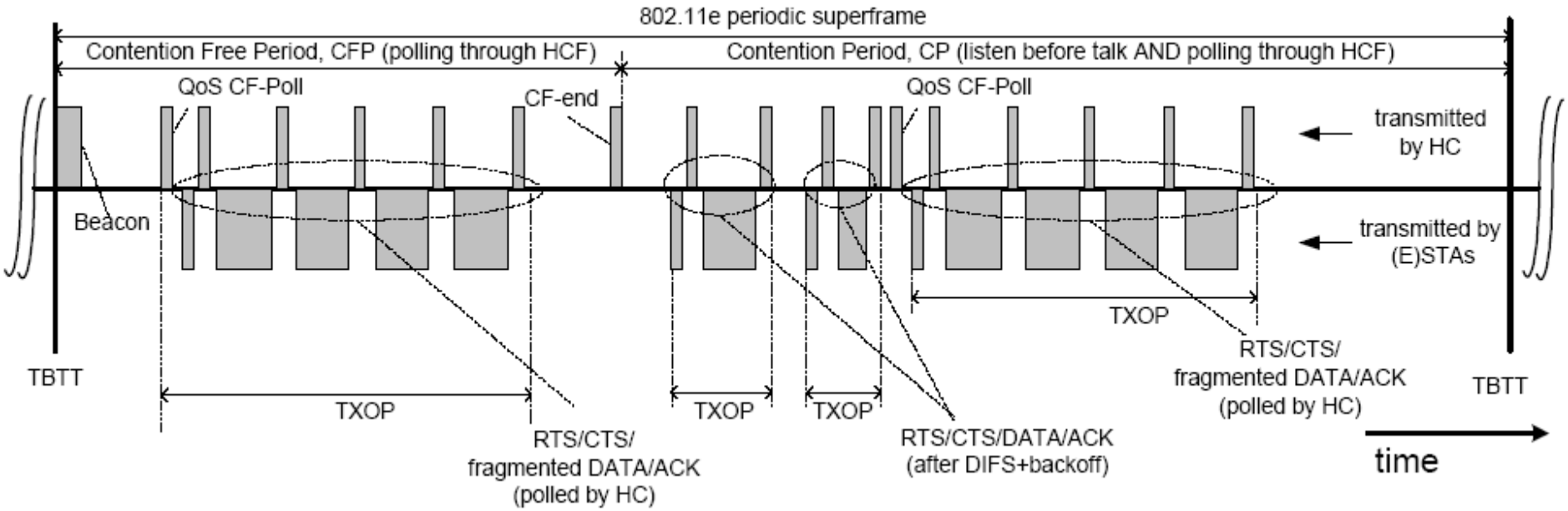
802.11e: Virtual Backoff



Priority	Access Category	Designation
2	0	Best Effort
1	0	Best Effort
0	0	Best Effort
3	1	Video probe
4	2	Video
5	2	Video
6	3	Voice
7	3	Voice

- 8 virtual stations inside a station
- Virtual Collision
- The scheduler grants the Transmission Opportunity (TXOP) to the TC with highest priority, out of the TCs that virtually collided within the station

802.11e: HCF



- Target Beacon Transition Time (TBTT) is announced in every beacon frame
- TXOP begins either
  - Available under EDCF
  - Receiving the QoS CF-Poll from the Hybrid Coordinator(HC)