

# Commercial Wireless Networking Explained

1 December 2009

Jack L. Burbank  
Jack.Burbank@jhuapl.edu



# Goals of this Tutorial

- To provide an overview of the commercial wireless networking landscape
  - *Comprehensive overview of commercial wireless networking technologies (layers 1 and 2)*
  - *Overview of relevant network layer technologies*
  
- What I hope you take away from this...
  - *A basic understanding of the most common commercial technologies*
  - *An understanding of what the various commercial technologies are, and what they are not*
    - *Capabilities*
    - *Usage cases*
    - *Drawbacks and limitations*
  - *Most importantly, an understanding that there is no ‘silver bullet’*
    - *Be skeptical of any claim of any technology that will ‘solve all our problems’...if it were that easy, it would have already been solved!*
    - *Likewise, approach any claim of the ‘total inadequacy’ of a technology with caution*
    - *Rather, all the technologies described here are tools*
      - *All have strengths, limitations, proper uses, and ill-advised uses*
      - *There is no ‘one size fits all’ solution*
    - *“Only a Sith deals in absolutes”, Obi-Wan Kenobi*

# Tutorial Overview

- Introduction and background
  - *Why do we need to be concerned about commercial wireless technologies?*
  - *Wireless networks, MANETs, Mobile IP, and NEMO*
  - *Difference between wired and wireless networks*
  - *Overview of the standards bodies*
  - *Brief review of some networking basics*
- Commercial wireless networking standards
  - *An architectural view of the commercial wireless networking domain*
  - *Wireless Local Area Networking: IEEE 802.11*
  - *Wireless Personal Area Networking: IEEE 802.15*
  - *Wireless Metropolitan Area Networking: IEEE 802.16*
- Wireless networking technologies at the network layer
  - *Mobile IP, NEMO, MANET routing*



# Introduction and Background

# Wireless Networking: A Brief History

- The first wireless network of record was introduced in 1971 at the University of Hawaii
  - *The ALOHNET research project*
  - *Connected seven campuses spread across four islands*
- Radio networking remained active in the US and Canada in the 1980's largely through the efforts of amateur radio hobbyists (hams) and the development of terminal node controllers (TNCs)
  - *TNCs were analogous to computer modems*
- In 1985, the Federal Communications Commission (FCC) authorized the public use of the Industrial, Scientific, and Medical (ISM) frequency bands
- In the late 1980's, the Institute of Electrical and Electronics Engineers (IEEE) 802 working group authorized a project for the development of a wireless local area network (WLAN) standard
- In 1994, Ericsson initiated project to study the feasibility of a low-power, low-cost radio interface to eliminate the cables from mobile phones and their accessories
- On November 18, 1997, the original 802.11 WLAN standard was published
- In 1998, the Bluetooth Special Interest Group was formed
- In 1999, initial Bluetooth specification was ratified (v1.0)
- In 2001, initial 802.16 specification was published

# The Enormous Commercial Success of Wireless Networks

- Commercial WLANs have experienced incredible success over the past 5 years
- The wireless Internet has evolved to provide connectivity to a variety of platforms, including Personal Digital Assistants (PDAs) and laptop computers, from a variety of locations, such as airports, coffee shops, and universities
- The most successful WLAN to date has been the IEEE 802.11 technology family and is now widely deployed worldwide
  - *Over 50,000 hot-spots worldwide in January 2004, over 100,000 in January 2006*
    - *Largest amount in Seoul: 2,056*
    - *Largest amount in United States: nearly 41,000*
      - Top US City: San Francisco, CA: 805
      - 30% of Americans use wireless networks, 60% of businesses
- And that trend is rapidly increasing at a non-linear rate...
  - *22.7 million 802.11 units shipped in 2003*
  - *10.99 million 802.11 units shipped in 3Q2004 alone!*
  - *Over 120 million 802.11 units shipped in 2005*
- Intel launched its *Centrino* wireless platform in 2003. The next wireless Intel platform will be *Sonoma*
  - *Currently over 130 notebook models with Centrino*
  - *Wireless-enabled notebooks represented 42% of all laptop sales in 2003*
  - *95% of all notebook sales wireless-enabled in 2006*
- This phenomenal upward trend is International:
  - *1.2 million wireless cards sold in Europe in 2004*
  - *Projected 5.7 million sales in Europe in 2008*
- Nearly 15 million mobile WiMAX, 90 million fixed WiMAX subscribers are forecast worldwide by 2009

\*All statistics from: <http://www.itfacts.biz>

## MANET, Nodal Mobility, and NEMO...

### lots of terms, lots of confusion

- **Mobile Ad-hoc Network (MANET):** ad-hoc networks (fixed or stationary) are those that can be formed in an immediate timeframe, without the need for pre-planning or configuration. Rather they form as needed. Addresses both network membership mobility and sub-network mobility
- **Nodal Mobility:** Network membership mobility (i.e. nodal mobility), but not sub-network mobility. (e.g. a network of mobile nodes, all moving relative to one another, but the point-of-attachment to the larger network is not moving – the network as a whole is not moving, at least as far as the larger network can tell). This is the focus of Mobile IP
- **Network Mobility (NEMO):** Mobility of a network in its entirety (not individual nodal mobility). (e.g. think of a collection of networked sensors on a vehicle. They are not moving relative to one another, but as a group they are moving relative to the rest of the network. This is the NEMO problem space.)
- Both NEMO and MIP are predicated upon the concept of a fixed infrastructure. Only the generalized MANET makes no assumptions regarding infrastructure.
  - *Note, however: even commercial MANET solutions are usually predicated upon some form of fixed infrastructure*

## Wired vs. Wireless...What's the Big Deal?

- **Low bandwidth** → limits raw link capacity
- **Poor channel quality** → data loss
- **Intermittent connectivity induced by terrain/environment and mobility** → (potentially rapidly) fluctuating network topology
- **Platform constraints** → limitations on size, weight, power, and complexity
- **Energy efficiency** → technology often implemented in devices with long design lifetimes
- **Environmental requirements (extreme temperatures and ruggedization)** → limits the deployable capability

# Overview of IEEE 802

- IEEE 802 is the “Local Area Network (LAN) and Metropolitan Area Network (MAN) standards committee”
  - *Working-group based*
  - *Develops PAN/LAN/MAN/WAN standards*
    - *Ethernet (IEEE 802.3)*
    - *Token Ring (IEEE 802.5)*
    - *Wireless Local Area Networks (LAN) (IEEE 802.11)*
    - *Wireless Personal Area Networks (PAN) (IEEE 802.15)*
    - *Broadband wireless networks (IEEE 802.16)*
    - *Mobile broadband wireless networks (IEEE 802.20)*

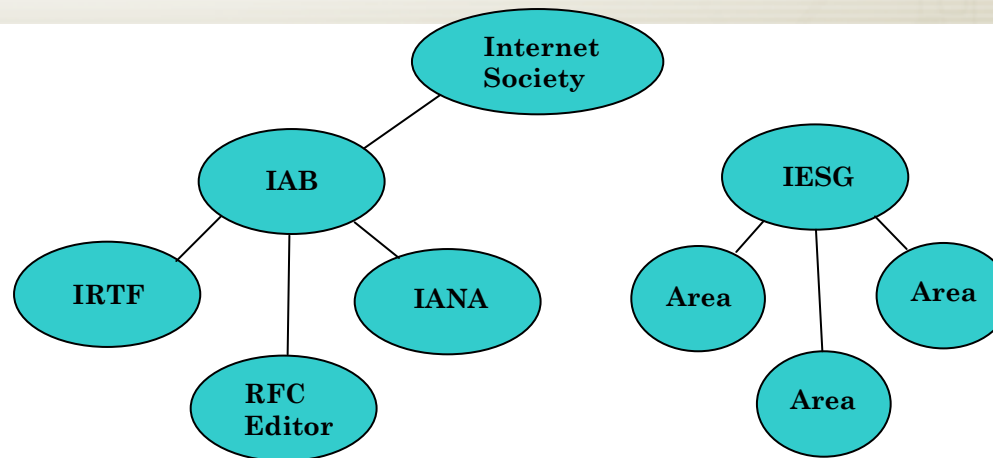
# IEEE 802 Standards Process

- Standards development activity begins in the form of a Study Group
- The members of the study group then decide if it wants to standardize a technology
- If so, it can then become a Task Group (TG)
- Before a TG can be formed, formal IEEE approval must be obtained
- IEEE approval requires two documents that have achieved working group consensus
  - *Project Authorization Request (PAR)*
    - *Delineates scope of proposed TG, goals, deliverables, etc.*
  - *'5 Criteria'*
    - *There are five criteria that must be met before a formal technology standards process can begin*
      - Broad Market Potential
      - Compatibility
      - Distinct Identity
      - Technical Feasibility
      - Economic Feasibility
- A typical timeline for a technology to become an 802 standard is typically 5-10 years

# Overview of IETF

- Primary organization engaged in the development of Internet standard specifications
- Formed in 1986
- IETF is not a 'formal' organization, no formal membership
- "Individuals, not companies"
- "Rough consensus and running code"
  - *Fundamentally different philosophy than IEEE*
  - *No formal voting*
  - *Predicated upon short design cycle*
    - *Implement, gain operational experience, feed back into next iteration of technology*
  - *IEEE characterized by formal membership, formal voting, much longer design cycle (typically)*

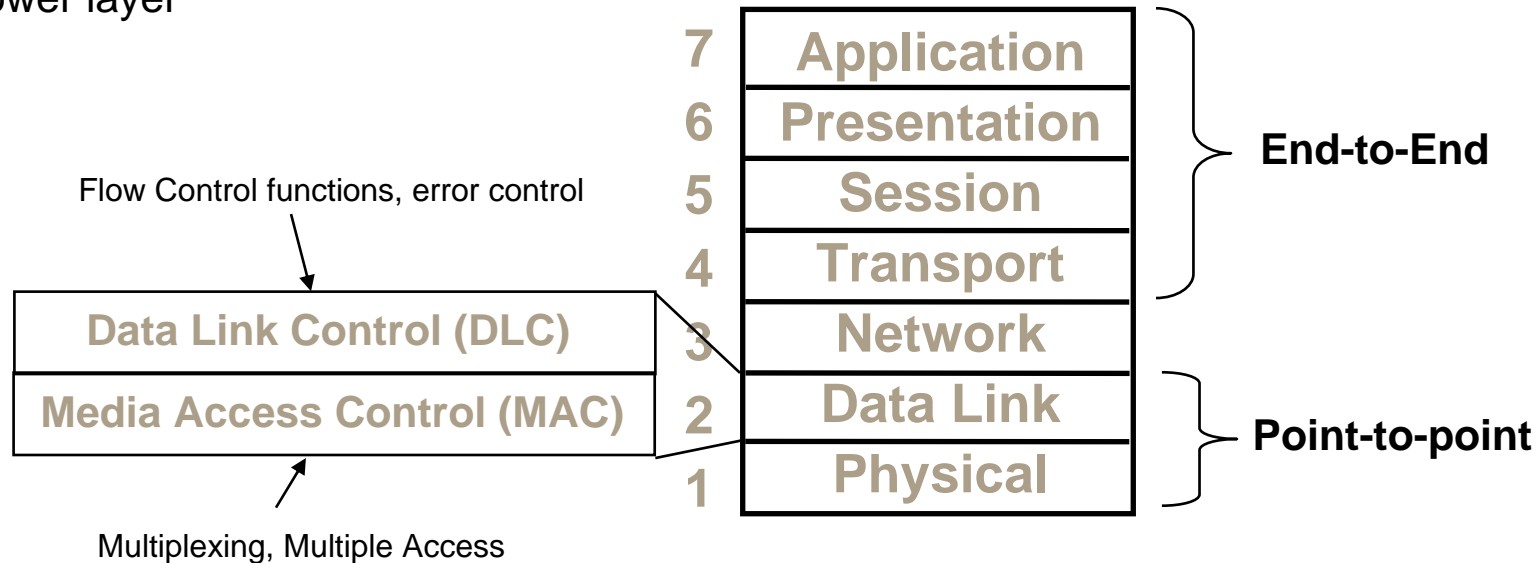
## Overview of IETF (continued)



- IETF divided into 8 areas (Internet, Operations and Management, Real-time Applications and Infrastructure, Routing, Security, Transport, Applications, General)
- Currently over 110 working groups (WGs) and BOFs
  - *Scope of WG, goals, deliverables delineated by IESG-approved charter*
- Oversight provided by Internet Engineering Steering Group (IESG) whose membership is Area Directors (ADs)
- Produces different types of documents in form of RFCs: Informational, Experimental, Standards-Track, Best Current Practice (BCP), Historical

# OSI Communications Reference Model

- The Open Systems Interconnection (OSI) communications reference model (OSIRM) is a commonly-used framework for digital communications between two end-points
- The OSI reference model employs a hierarchical structure of seven layers where each layer provides value-added service per the next-highest layer, and requests service from the next-lower layer



- Layer standards consist of:
  - *Service Definition: Describes the functions the layer performs and what services it provides (to the next upper layer)*
  - *Protocol Specification: Describes the procedures used within the layer, and between peer entities, to execute the functions defined by the service definition*

# What is a Protocol?

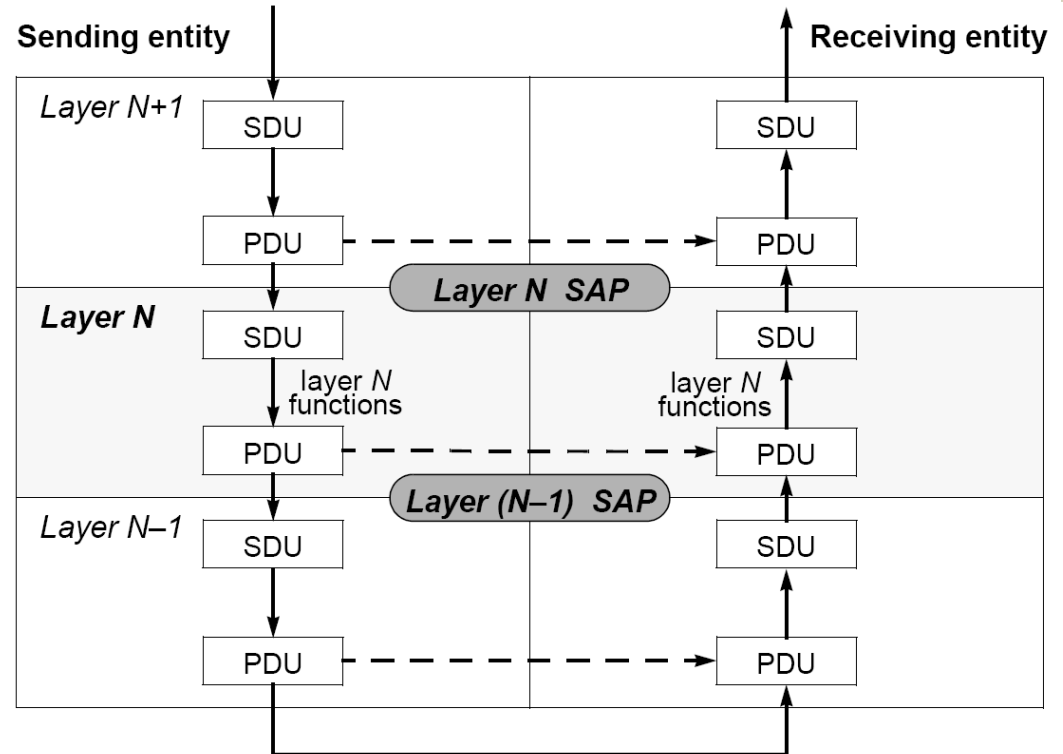
- A protocol is an agreement between the communicating parties on how communications is to proceed (i.e. selecting a language)
  - *In data communications, this generally defines the format of data, processing procedures, and agreed upon meaning of data values*
- Components of a protocol
  - *Service Data Unit (SDU): Consists of user data and control information created in the upper layers of the protocol stack*
    - *The information to be conveyed by that particular layer of the protocol stack*
  - *Protocol Control Information (PCI): Information exchanged by peer entities to perform certain tasks or settle on a format*
    - *The information that must be appended by the layer in order for that layer to successfully complete its functions*
  - *Protocol Data Unit (PDU): The combination of SDU and PCI*
    - *The information passed to the next-lower layer*
    - *This PDU is the SDU of the next-lower layer*

# Service Access Points and Primitives

- Interfaces between layers are provided through Service Access Points (SAPs)
  - *SAPs are standardized data interfaces between layers*
- Layers communicate with one another through the use of service primitives
  - *Set of messages required for operations*
    - *Request messages, status messages, response messages*

# Generic Layer Interactions

- Each layer (N+1) passes PDUs to the layer (N) below it
- Layer N adds an appropriate header (PCI) and passes a new PDU to layer N-1
- Encapsulated in this PDU is the PDU received from layer N
- This process is repeated to the bottom of the protocol stack
- The reverse process takes place at the receiver
  - Removal of PCI and passing up of original SDU



From Reference 3

# Layer Definitions

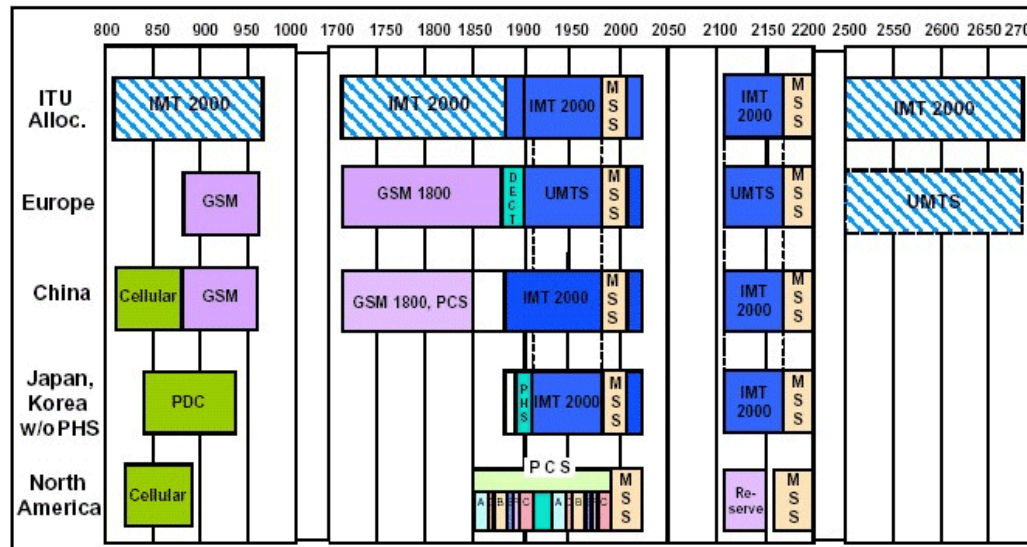
- **Network Layer** – defines the format and functions of headers and trailers that are added to SDUs so that packets can travel between source and destination network layer address over the end-to-end network. Responsible for establishing end-to-end (source, destination) path
- **Logical Link Control (LLC) Sublayer** - defines the format and functions of the PDU that is passed between service access points (SAPs) in the source and destination stations
- **MAC Sub-layer** - defines the format and functions of headers and trailers that are added to SDUs so that entire frames can travel between source and destination MAC addresses over the point-to-point network link. The MAC also defines the method by which the transmission medium is accessed.
- **Physical Layer** – defines the electrical and mechanical standards and signaling mechanisms



# Commercial Wireless Networking: The Big Picture...

# The Role of the ITU

- ITU began process of 3G standardization with its International Mobile Telecommunications (IMT-2000) initiative
- IMT-2000 standard loosely specifies requirements for 3G cellular networks
- However, IMT has expanded beyond cellular to encompass all wireless communications
- Technology proponents often put significant effort into having their technologies blessed as 'IMT compliant'
- Aside from marketing, why is it important to be 'IMT compliant'? Because many parts of the world allocate spectrum based on these characterizations

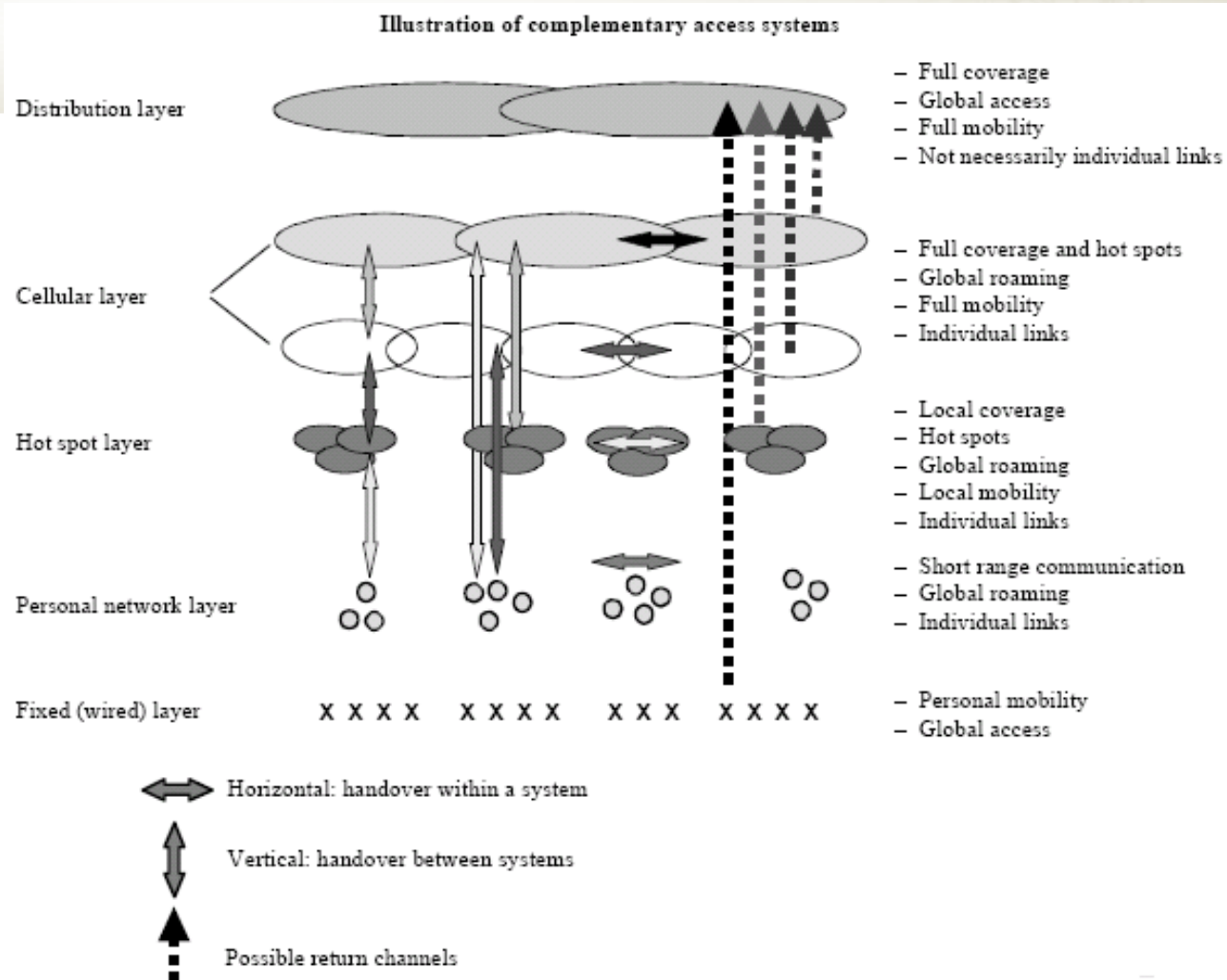


## IMT Activities within ITU

- **ITU-R:** Working Party (WP) 8F is responsible for the overall radio frequency (RF) spectrum and radio system aspects of IMT-2000 and beyond. It functions within the larger ITU-R Study Group (SG) 8 for issues related to the terrestrial component of IMT-2000 and beyond systems. Note that SG 8 also works issues related to the satellite component of IMT-2000 and beyond.
- **ITU-D:** Responsible for studies, activities, and direct assistance related to implementing IMT-2000 in developing countries.
- **ITU-T:** SG 19 is responsible for studies related to the networking aspects of IMT-2000, among other more general topics associated with wireless internetworking.



# IMT-2000 Layered Architecture



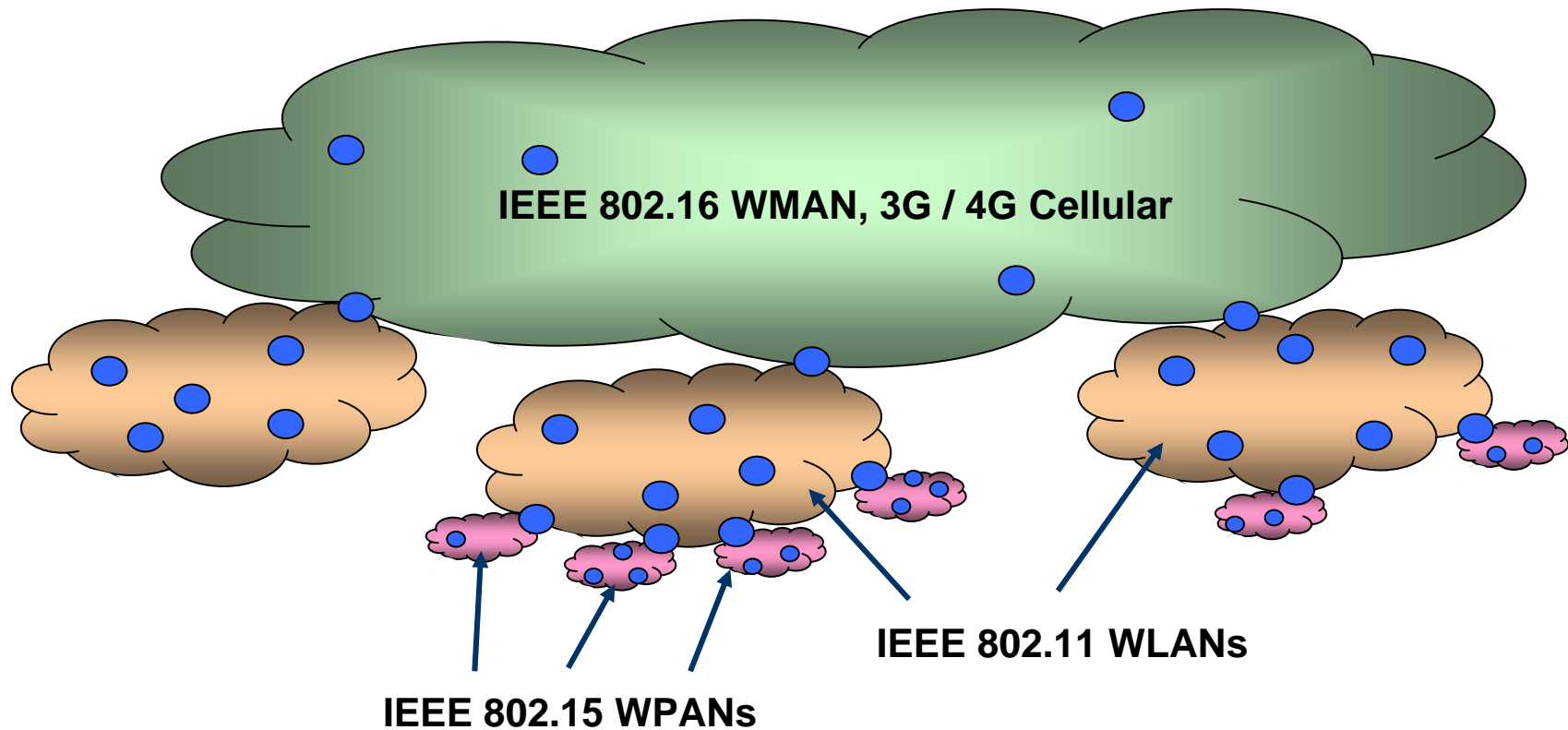
## IMT-2000 Threshold

- Candidate technology must meet set of requirements as defined by IMT
  - *Throughput, mobility, latency, handoff support, interface definition requirements*
  - *Requirements developed to meet each functional area of architecture*
- Example IMT-2000 cellular data rates

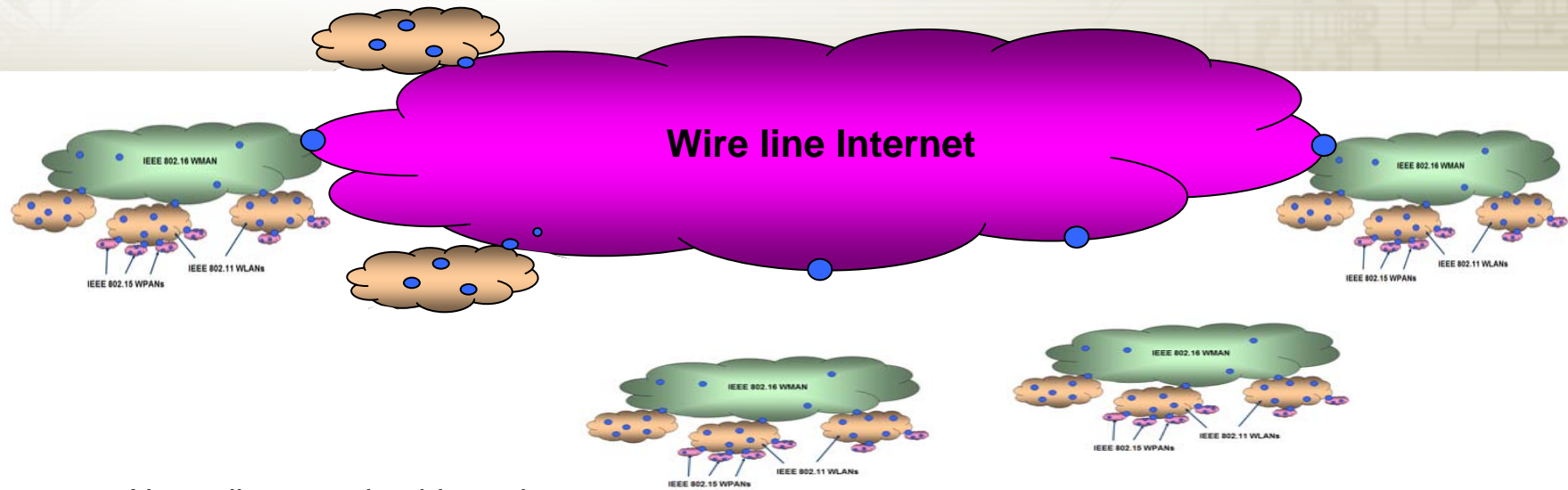
Platform	Data Rate
Outdoor stationary (0 mph)	2 Mbps
Pedestrian (3–4 mph)	384 kbps
Car or train (50–60 mph)	128 kbps

- IMT-Advanced, formerly known as ‘systems beyond IMT-2000’ sets higher functional requirements compared to IMT-2000
  - *e.g. approximately 100 Mbps for high mobility users and up to approximately 1 Gbps for low mobility users*

# Emerging Commercial Wireless Network Model



# The Emerging Wireless Internet (continued)

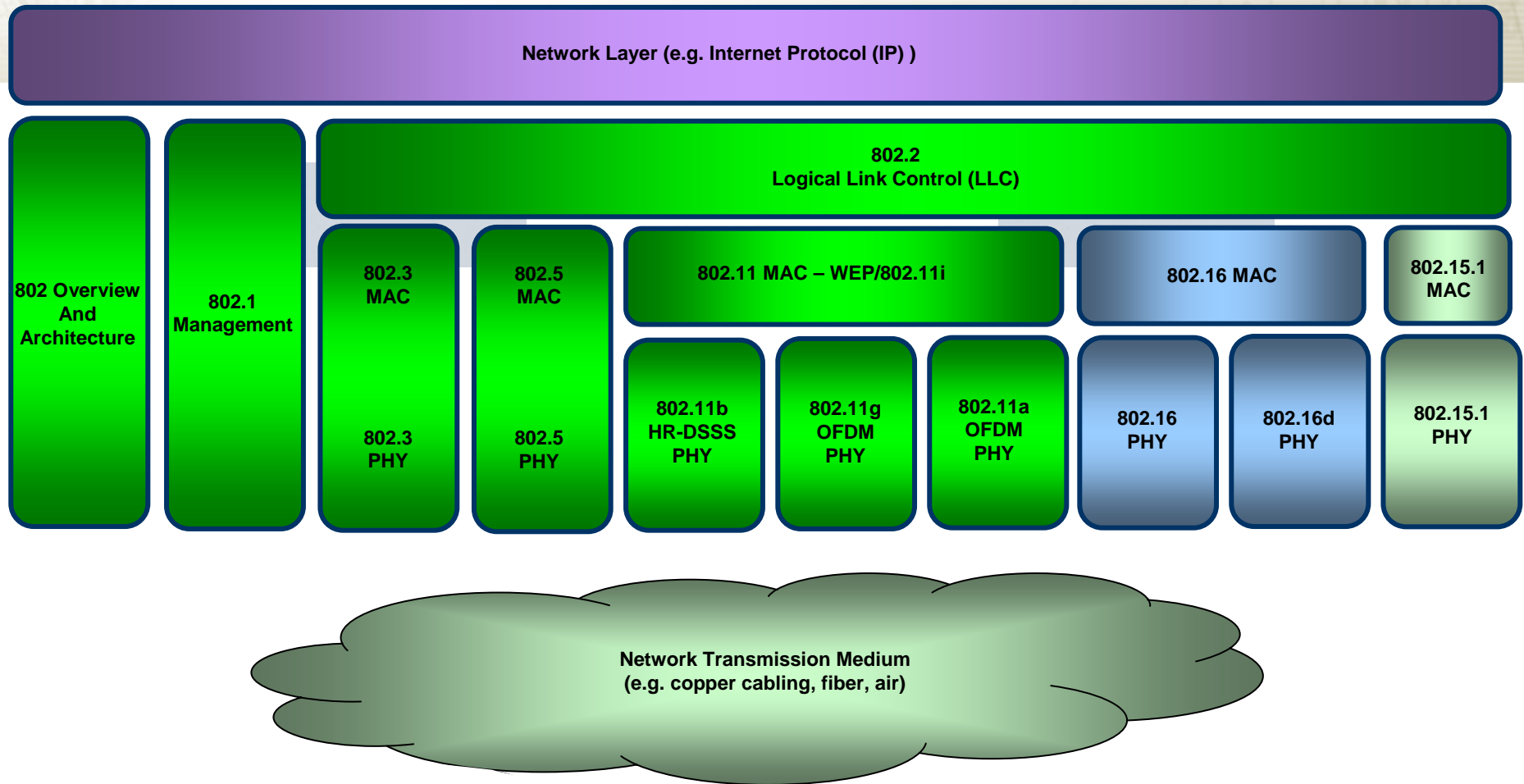


- Naturally-emerging hierarchy
  - 802.15 WPAN stub networks at bottom of hierarchy
  - 802.16 WMAN networks, 3G/4G cellular networks at top of wireless hierarchy, augmented by 802.22 in future
  - 802.11 WLANs envisioned to increasingly play role of transit network
- General trends:
  - Data rates increase towards bottom of hierarchy
    - Evolving towards Gbps solutions in WPAN domain, 100's Mbps solution in WLAN domain, 10's Mbps in WMAN domain
    - Not what you would expect as transit nature of network increases for higher levels of hierarchy
    - The exact opposite of the wired Internet
  - Mobility support less at bottom of hierarchy



# Commercial Wireless Networking Technologies

# IEEE 802 Family of Standards



NOTE: Non-exhaustive view of the IEEE 802 technology family

# IEEE 802 Wireless Technologies

- Conventional differentiator in technology classification is geographic range of operation
  - *PAN: spans up to 10's of feet*
  - *LAN: can span up to a few kilometers*
  - *MAN: spans 10's-100's of kilometers (i.e. a city)*
  - *WAN: spans a large distance, 100's-1000's kilometers (on the order of a country or continent)*
  - *It should be noted that this distinction is somewhat arbitrary*
    - *Technologies are designed for particular usage cases, but that doesn't exclude technologies from different applications (it just makes it more of a 'roll of the dice')*
      - *A good example is city-wide 802.11 deployments*
        - » *A LAN technology applied to a MAN scenario*
      - *Other examples of range-extending 802.11 for 100+ km*



# **IEEE 802.11: The Alphabet Soup that is the WLAN Technology Family**

# IEEE 802.11 Working Group

- Defines PHY and MAC layer protocols for WLANS
- “Task Groups” define different PHY implementations of the protocol, clarifications to current IEEE 802.11x standards, address Quality-of-Service (QoS), and security, among other issues.
- Common to the entire IEEE 802.11 Group:
  - *MAC Task Group: Defines the common IEEE 802.11 MAC which is compatible with all PHY implementations*
- Primary current Wireless LAN Standards:
  - *Task Group A (IEEE 802.11a): A PHY to operate in the Unlicensed National Information Infrastructure (UNII) band at 5.2 GHz*
  - *Task Group B (IEEE 802.11b): A PHY operating in the unlicensed Industrial, Scientific, and Medical band (ISM) at 2.4 GHz*
  - *Task Group G (IEEE 802.11g): A high-rate PHY extension to the IEEE 802.11b standard*
  - *Task Group I (IEEE 802.11i): Modification of the original MAC specification to enhance security and authentication*

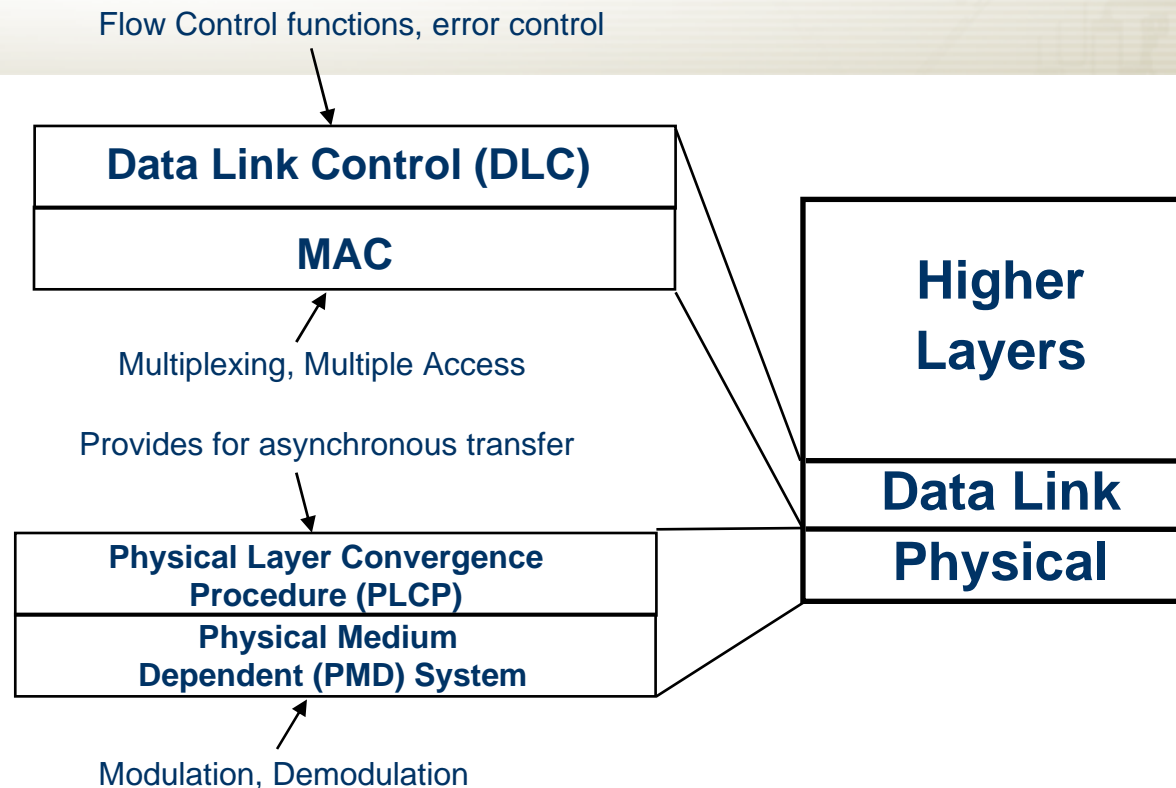
## “Wireless Fidelity”: The Business Side of 802.11

- “Wireless Fidelity” or “Wi-Fi” is an 802.11 marketing term that has become synonymous with 802.11 WLANs
- The Wi-Fi Alliance was formed in 1999 as a non-profit international organization to certify interoperability of 802.11 WLAN products
  - *Acts as an advocate for 802.11 technology*
  - *Heavily involvement in 802.11 technology advertisement*
- Over 200 member companies
- Over 1000 WLAN products have been certified by the Wi-Fi Alliance
  - *“Wi-Fi Certified” logos are found on 802.11 product packages*



Image taken from  
<http://www.wi-fi.org/OpenSection/index.asp>

# 802.11 Logical Architecture

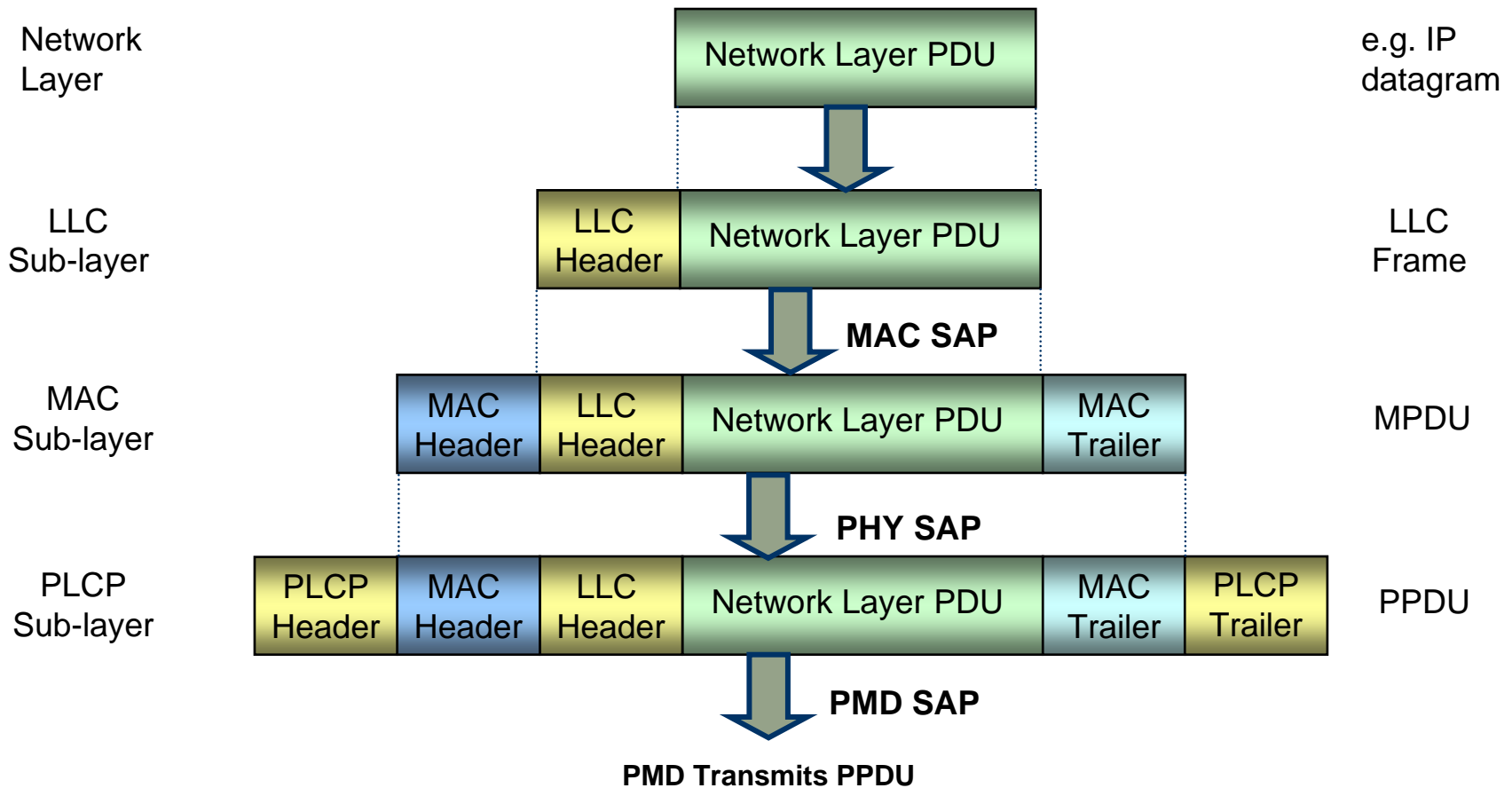


- 802.11 specifies MAC and PHY technologies
- 802.11 specifies DLC to be as specified by the IEEE 802.2 LLC standard
- 802.11 divides the PHY into two sub-layers, or 'functions': PLCP and PMD

## 802.11 Layer Functions

- LLC Sub-layer – provides flow control between point-to-point LLC peers
- MAC Sub-layer – provides access to the wireless medium, allows the radio to join an 802.11 network, and provides authentication and privacy
- PLCP Sub-layer – provides encapsulation of MAC SDUs (MSDUs) with control information to allow for asynchronous communications
- PMD Sub-Layer – transmits and receives PPDU over the specified air interface

# 802.11 Layer Interactions (continued)





# An IEEE 802.11 Wireless Network

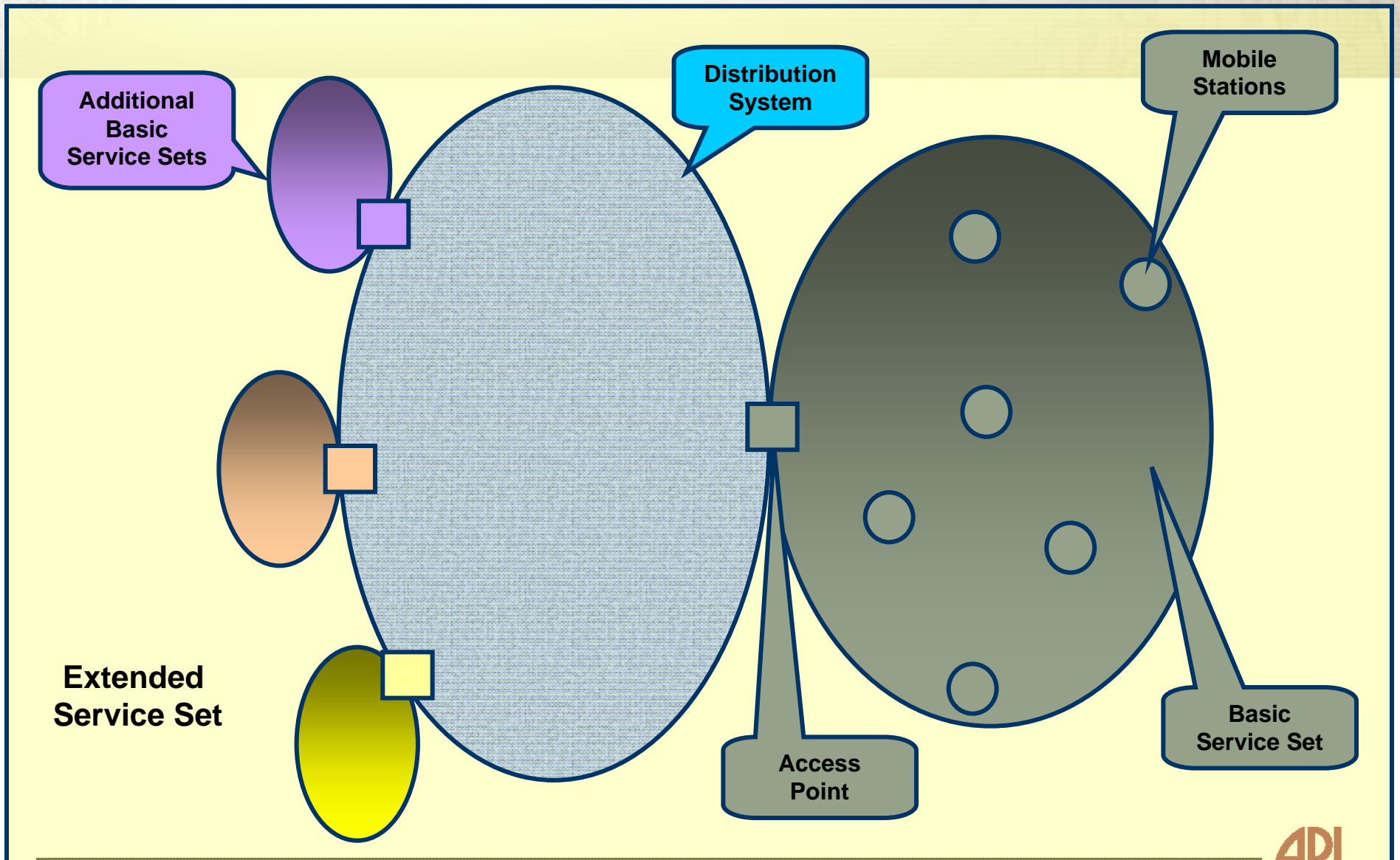
# Components of an 802.11 Network

- Four primary components of an 802.11 network:
  - *Access Points (APs)*
    - *Bridge the wireless network to the wired network*
  - *Mobile Stations (MSs)*
    - *Users of the network*
  - *Distribution System (DS)*
    - *Method by which multiple APs are interconnected to increase coverage*
  - *Wireless medium*
    - *Channel over which communications occur*

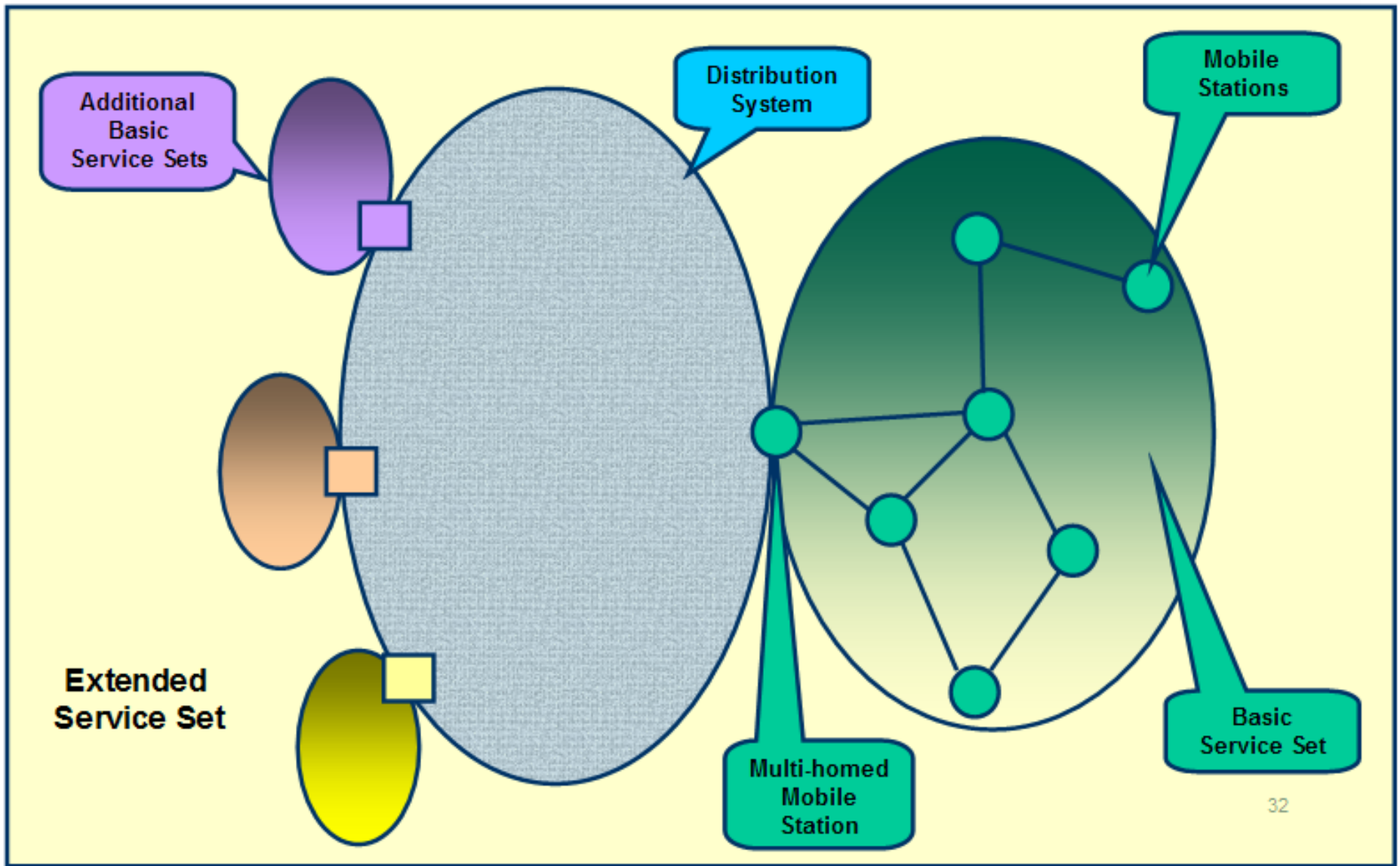
# The 802.11 Network

- The Basic Service Set (BSS) is the fundamental building block of an 802.11 network
  - *Consists of a group of MSs that communicate with each other*
  - *Coverage area of the BSS is referred to as the basic service area (BSA)*
- Two types of BSSs
  - *Infrastructural*
    - *All communications takes place through the AP*
    - *More common type of 802.11 network*
  - *Ad-hoc (or independent)*
    - *Mobile stations communicate directly to one another*
    - *Also known as independent BSS (IBSS)*
    - *Less common type of 802.11 network*
- Multiple BSSs can be inter-connected to form an Extended Service Set (ESS)
- BSSs are inter-connected through a DS
  - *DS method is not specified as part of the 802.11 standards*

# An 802.11 Network (Infrastructural View)



# An 802.11 Network (Ad-hoc View)



## The 802.11 Network (continued)

- Within the BSA, the required service set can be provided to a network node
  - *This required service set is the set of functions that the LLC sub-layer requires for sending MSDUs between two network nodes*
    - *Station Services*
      - Authentication, deauthentication, privacy, and MSDU delivery
    - *Distribution System Services (DSS)*
      - Association, disassociation, reassociation, distribution, and integration
- An ESS or BSS is identified by its Service Set Identity (SSID)
  - *SSID is a 0-32 byte identifier*
  - *Typically assigned a human readable ASCII character string*
  - *Referred to as the 802.11 network name*

# Joining the 802.11 Network

- A MS must first determine the presence of a network
- Two methods that a MS can employ for network detection
  - *Passive*
    - *The stations of a network periodically send out beacons on all channels to announce the presence of a network*
    - *An MS wishing to join the network can scan across all channels listening for these network beacons*
    - *Once a station detects the beacon, which contains required information such as its SSID, the station can begin the procedures required to join the network*
  - *Active*
    - *Alternatively, a MS can begin transmitting probes with the SSID of the network it wishes to join and then wait for a probe response*
    - *Upon receipt of a probe response, the MS can then begin joining the network*
    - *This is the method required if SSID broadcast suppression is employed by the network (see later discussion)*



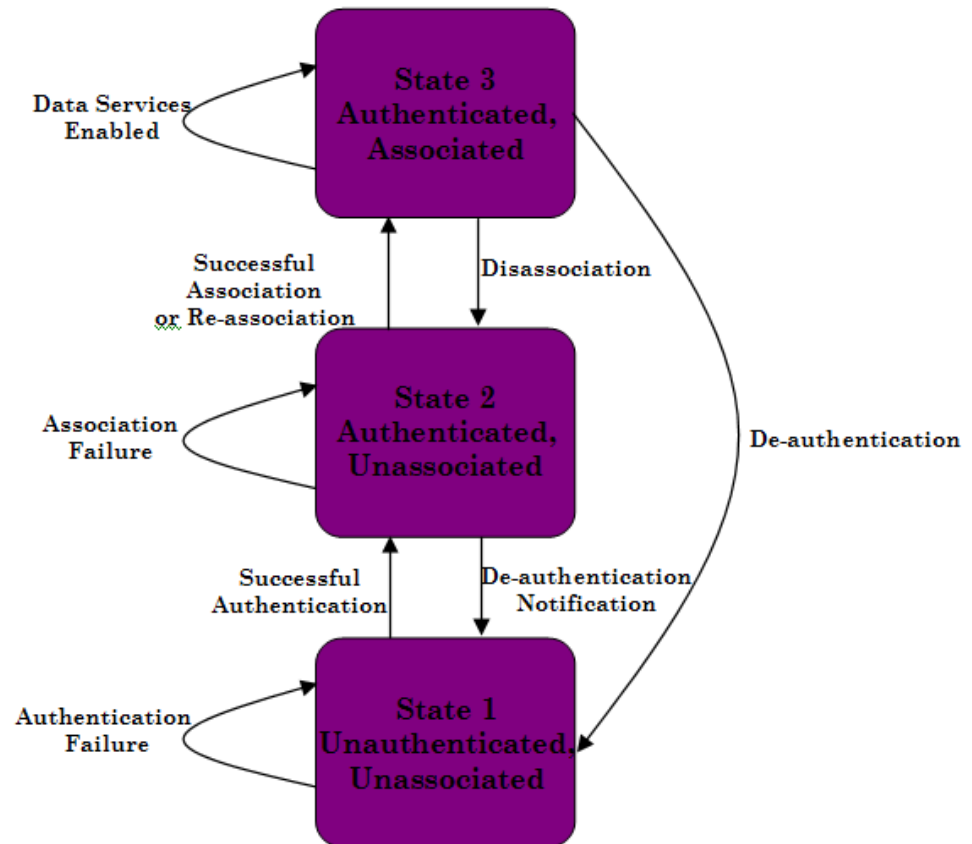
# The 802.11 MAC

## The 802.11 MAC: Introduction

- A common misperception is that the IEEE 802.11 MAC design is “wireless Ethernet”
  - *Certain aspects are similar to the IEEE 802.3 LAN standard,*
  - *However, the 802.11 MAC differs significantly from MAC designs of wired networks*
- There are four primary elements of the IEEE 802.11 MAC:
  - *Authentication and association procedures*
  - *Channel access procedures*
  - *Data flow control (DLC)*
  - *Framing mechanisms*

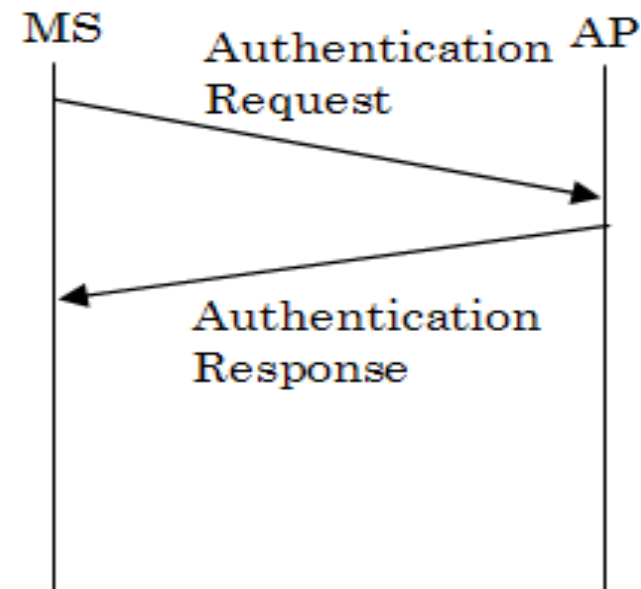
# Association and Authentication

- An MS must perform authentication and association before it can join the network
- Three states of existence
  - 1: *unauthenticated, unassociated*
    - Class 1 frames only
  - 2: *authenticated, unassociated*
    - Class 1, 2 frames only
  - 3: *authenticated, associated*
    - Class 1, 2, 3 frames
- MS can utilize data distribution services only once in State 3



## 802.11 Authentication Model

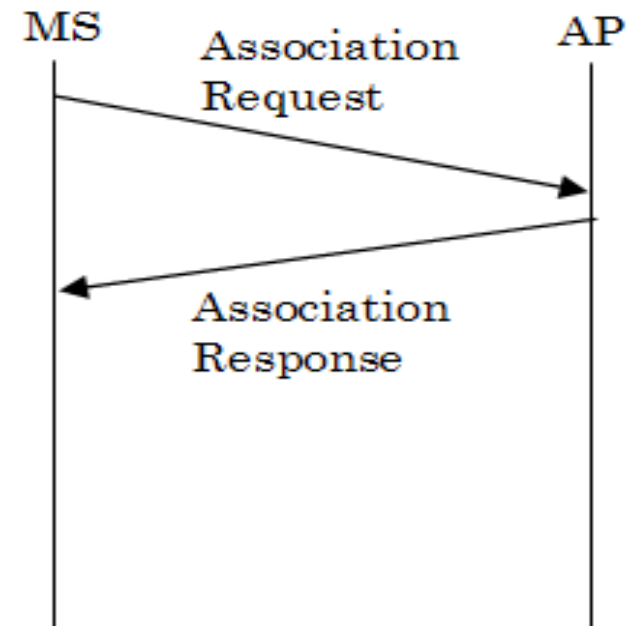
- Two methods of authentication
  - *Open-system*
    - *No credentials required*
  - *Shared-key*
- Intended to serve as an network access control mechanism
- Initiated by MS with an authentication request
- AP creates response
- Pre-configured shared-key uses a cryptographic key for this operation
  - *Four-frame operation for shared-key authentication*



NOTE: Authentication only supported for infrastructural mode

## 802.11 Association Model

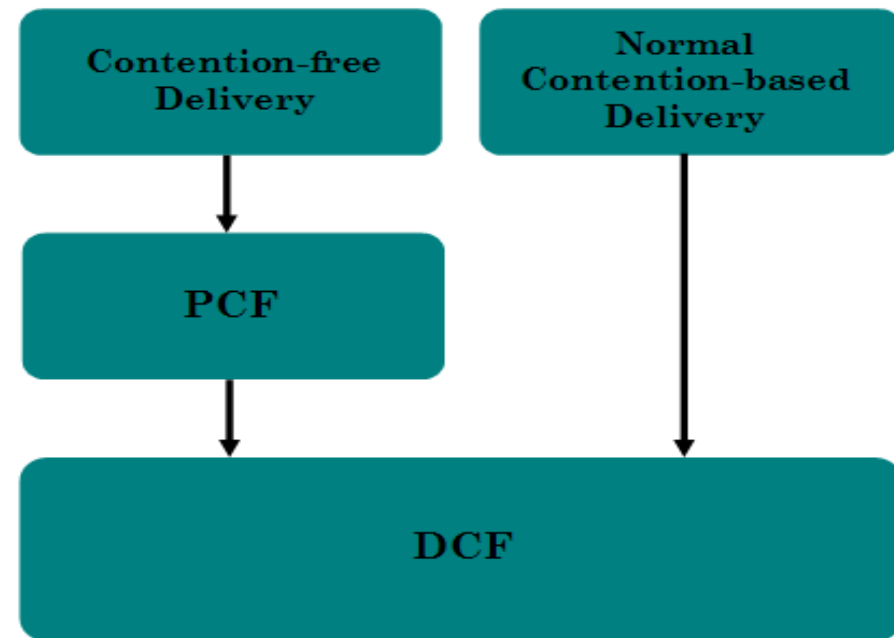
- Once authenticated, the MS initiates association with a request message
  - Includes the MAC address of the requesting node, the MAC address of the AP, and the SSID value
- AP responds with a response message
  - Result of association
  - Association identifier (AID)
- Association must occur before generated MAC layer frames can be passed up to higher networking layers
- Association enables network bookkeeping and frame forwarding
- Re-association occurs when the link is lost or MS moves to new AP
  - Re-association request and re-association response



NOTE: While according to the standard association applies to both ad-hoc and infrastructure modes, most devices operating in ad-hoc mode do not associate with each other

## 802.11 Channel Access

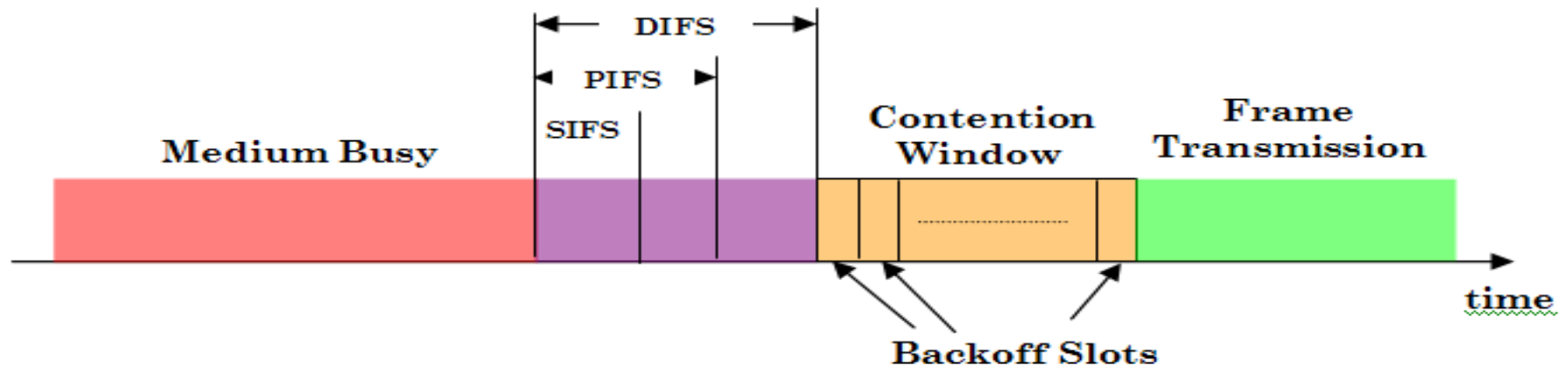
- Two methods by which an MS can access the wireless channel
  - *Contention-based access*
    - *Distributed Coordination Function (DCF)*
    - *Occurs in the contention period (CP)*
  - *Contention-free access*
    - *Point Coordination Function (PCF)*
    - *Occurs in the contention-free period (CFP)*
    - *Used within infrastructural networks only*
    - *Optional within standard*



# Contention-based Channel Access

- The 802.11 DCF is based upon Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA)
  - *CA reduces probability of collision between packets on a network with a shared medium*
  - *Different than Collision Detection (CD) implemented in 802.3*
- A node implementing CSMA/CA listens for network activity on the common channel through physical and virtual mechanisms
  - *Physical*
    - *Node listens for RF activity on the channel*
  - *Virtual*
    - *Uses Network Allocation Vector (NAV), which is a duration field contained within most frame types which can be used by nodes to reserve the wireless channel for a period of time by setting it to a non-zero value*
    - *Node passively receives other frames with flags that indicate end-of-frame sequence*
- A node can transmit data one of two ways:
  - *Transmits data frame*
  - *Transmits data frame using the RTS/CTS mechanism (see RTS/CTS discussion)*
- If collision occurs, waits a random time delay (exponential backoff) before repeating the process

# Inter-frame spacing



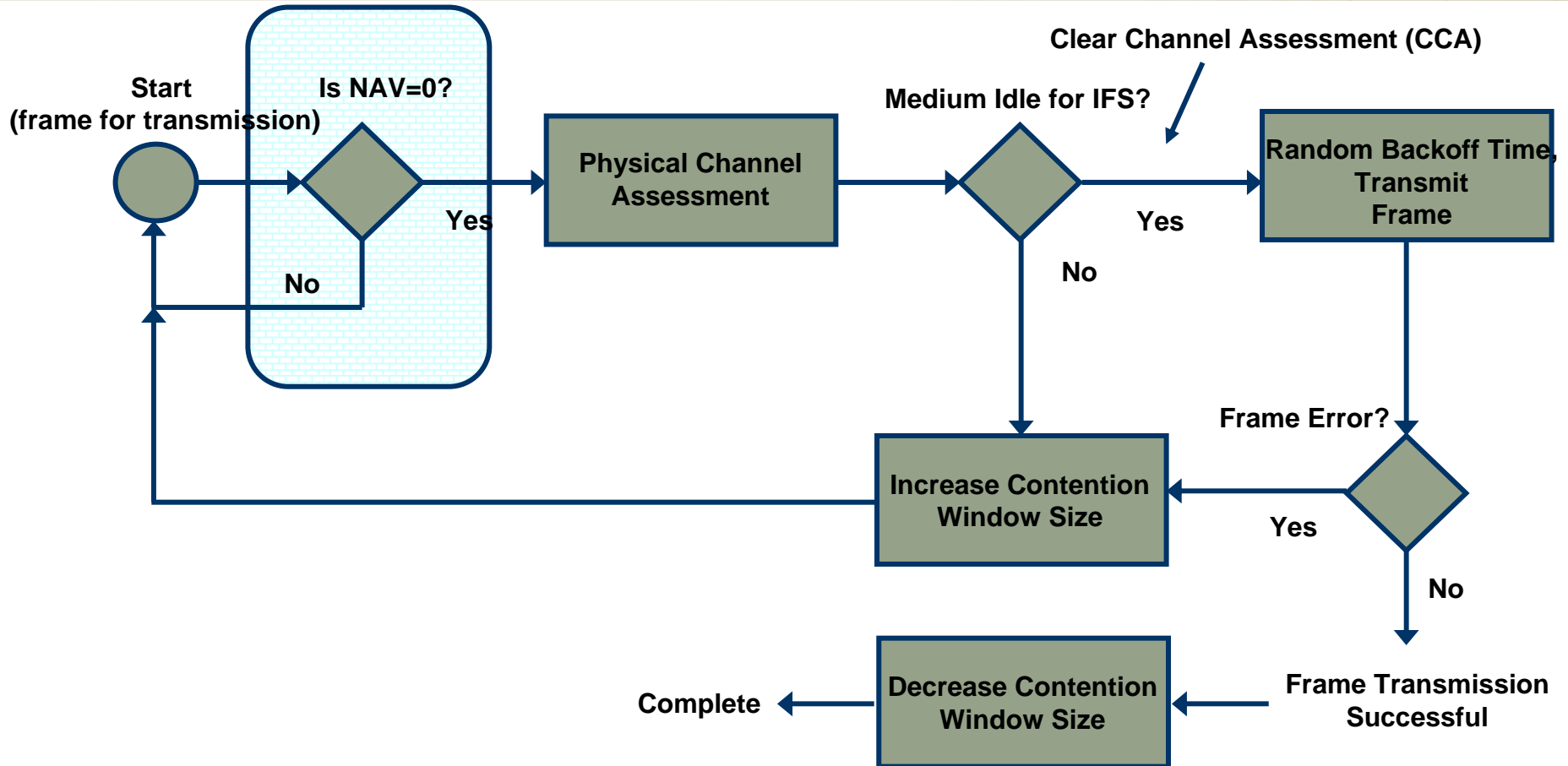
- The period of time for which the channel must be idle is determined by the Inter-frame spacing (IFS)
  - DCF inter-frame spacing (DIFS), PCF inter-frame spacing (PIFS), Short inter-frame spacing (SIFS), extended inter-frame spacing (EIFS)
    - SIFS used to give higher priority to more important messages, such as RTS/CTS frames, and positive acknowledgements
    - PIFS used by the PCF during the CFP
    - DIFS used by the DCF during the CP
    - EIFS used when there is an error during frame transmission

# Exponential Backoff

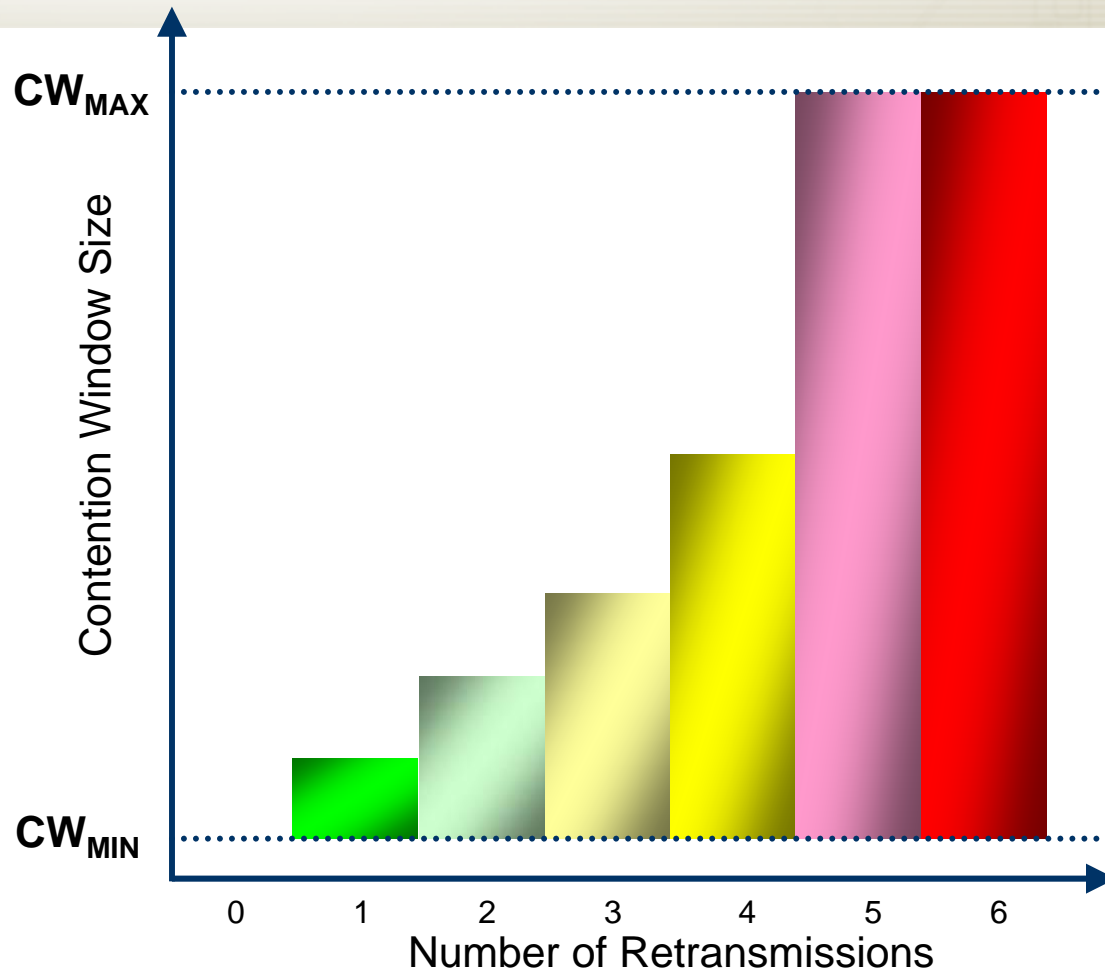
- Once the IFS has been observed, there is a 'backoff' or 'contention' window
  - *Divided into equal-length time slots*
  - *MS picks a random slot and waits for that time slot to attempt channel access*
- Contention window size is exponentially re-sized based upon transmission errors
  - *Contention window is sized  $2^{n-1}$ ,  $n \geq 1$ , with a maximum and minimum size*
  - *For each transmission error,  $n$  is incremented by 1*
  - *For each correct transmission,  $n$  is set to 1*
- Once the MS has waited the randomly-selected backoff time interval, the MS will determine if the medium is in use
  - *If not idle, the MS defers access*
  - *If idle, the MS will begin transmission*
  - *The rationale for random backoff is that after a busy time, multiple nodes may be waiting to transmit, and the introduction of a random time offset helps spread the initial traffic load, reducing collisions*

# DCF Operation

## Virtual Carrier Sensing



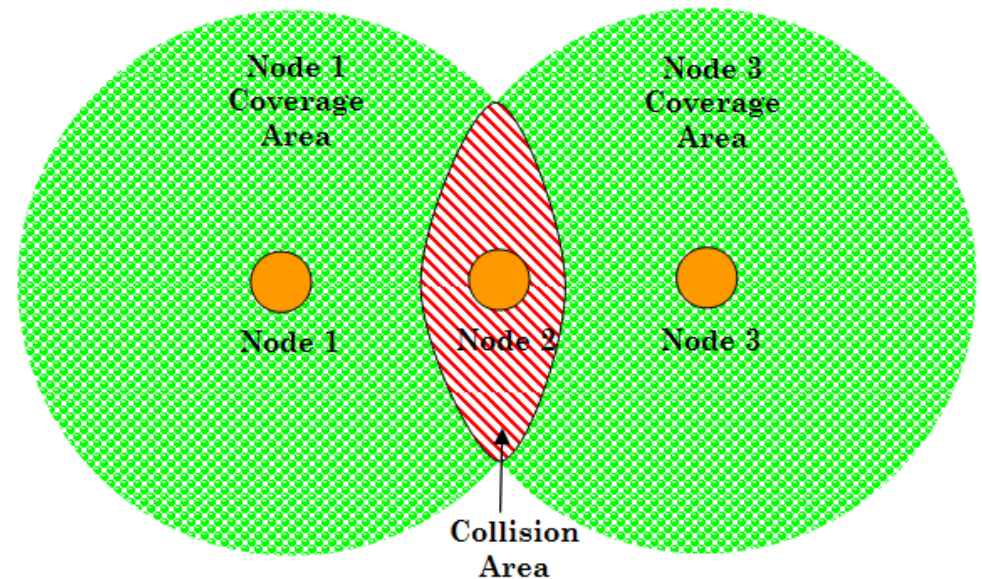
# Contention Window Size



\*Recreated from Reference 5

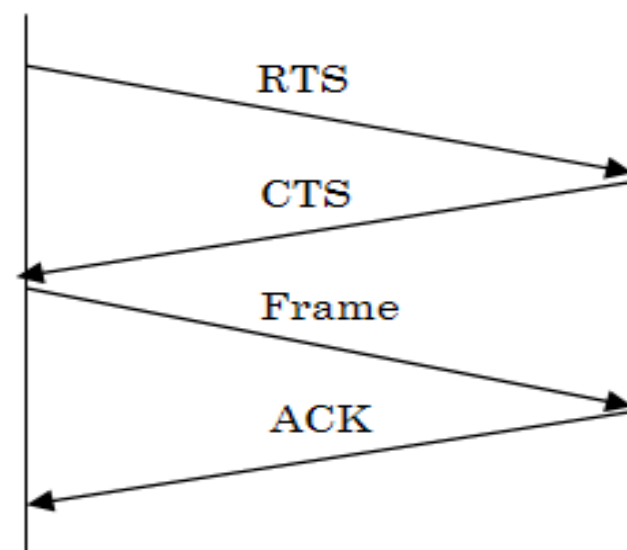
# The Hidden Node Problem

- The well-known 'hidden node problem' is caused by multiple nodes not within each other's sensing range, causing transmission collisions at intermediate nodes
  - A form of 'self jamming'
- This has led to the introduction of the Request to send (RTS) and Clear to send (CTS) to 'clear' out the area
  - Using this approach, nodes can reserve resources even within the CP



## Request to Send / Clear to Send

- Four-part process:
  - The transmitting MS sends a RTS which is received by all nodes within its transmission range
  - The receiving MS sends a CTS which is received by all nodes within its transmission range
    - Thus, all nodes within range of both nodes are made aware of the impending transmission
  - A data frame is then transmitted, followed by an acknowledgement
- This process is repeated for each data frame



- This leads to significant capacity usage inefficiency
  - Only used in certain cases
  - Governed by a configurable RTS Threshold
  - Frames that are larger than the threshold use the RTS/CTS mechanism

## Contention-Free Channel Access

- The 802.11 PCF is a centrally-enforced access scheme
  - AP arbitrates medium access among MSs
  - MSs can only transmit frames when they are granted permission to do so by the point coordinator (typically the AP)
    - *AP polls MSs on a polling list*
      - *Polling list populated with associated MSs*
  - Similar to IEEE 802.4 and 802.5 (token bus and token ring) token concepts
  - Periods of contention-free access alternate with periods of contention-free service
- 
- The PCF is an optional component of the 802.11 standard, and is not widely implemented

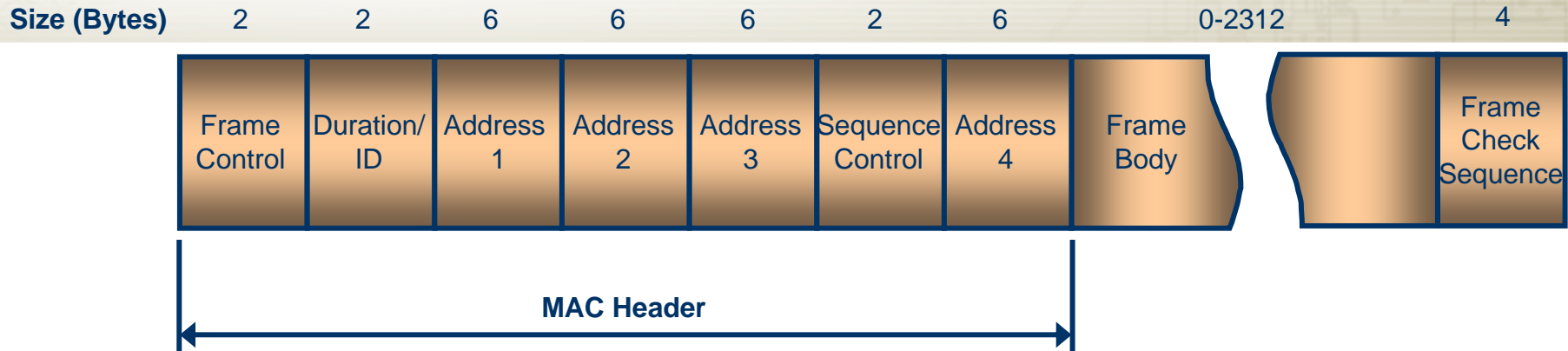
# Data Flow Control

- Point-to-point reliability provided through a data retransmission mechanism
  - *Only positive acknowledgements are employed*
- In an 802.11 network, the error detection and correction is the sole responsibility of the sender
  - *If a positive acknowledgement is not received, after a timeout the sender must retransmit until successful up to a configurable maximum number of retransmissions*
- Not all frames are subject to retransmission
  - *All unicast data must be acknowledged*
  - *All messages that are part of an 'atomic process' must be acknowledged*
- 802.11 performs fragmentation of higher-layer packets and some larger management frames to optimize performance
  - *A configurable fragmentation threshold is employed where packets larger than the threshold value is fragmented*
  - *Fragmentation threshold is typically set to be the same as the RTS threshold*

# Atomic Processes

- Atomic Process: a process that is a multi-frame exchange in which success is based upon the composite set of frame exchanges
- Examples of atomic processes
  - *Association*
  - *Authentication*
  - *RTS/CTS*
- The NAV is used by an MS to ensure that atomic operations are not interrupting, seizing the medium for the entire length of the atomic process

# 802.11 Framing: Generic Frame Format



- Differences from Ethernet MAC frames
  - 802.11 MAC frames do not include a length field
  - 802.11 MAC frames do not carry any type of preamble
  - Four addresses instead of two in an Ethernet MAC frame
    - Address 1: Destination address – analogous to destination address in Ethernet (the end user that passes information up the protocol stack)
    - Address 2: Source address – analogous to source address in Ethernet (originator of information)
    - Address 3: Receiver address – the final wireless station that should process the frame (e.g. AP)
    - Address 4: Transmitter address – the initial wireless station that placed the frame on the medium
      - This address is optional and is used only in wireless bridging applications

## 802.11 MAC Frame Fields

- Duration/ID – Identifies the duration of the next frame transmission (the NAV)
- Addresses – can be either individual or group addresses
  - *Multicast or broadcast group addresses*
- Sequence control – first four bits indicate fragment number, next 12 bits indicate sequence number
- Frame check sequence (FCS) – CRC-32 error detection field

# 802.11 Framing: Frame Control Field

Size (Bits)

2

2

4

1

1

1

1

1

1

1

Recreated from  
Reference 6



- Protocol version – currently set to 0 (only one MAC)
- Type – indicates whether the frame is management, control, or data
- Subtype – indicates the particular message
  - *E.g. subtype=0001 corresponds to an Association Response frame*
- To DS – indicates if frame is destined for DS
- From DS – indicates if frame originates from the DS
- More frag – indicates if additional fragments of an MSDU follows in subsequent frames
- Retry – indicates whether this is a retransmission
- Power Management – indicates the power management mode the sending station will assume after the current exchange
- More Data – indicates if the sending station has more data to send to the receiving station
- WEP – indicates whether the frame body has been WEP encrypted
- Order – indicates that frames must be processed in order

# Frame Types and Classes

- There are three types of 802.11 frames
  - *Management frames*
    - *Association-related frames*
    - *Probe-related frames*
    - *Beacons*
    - *Authentication-related frames*
  - *Control frames*
    - *RTS/CTS frames*
    - *Acknowledgement frames*
  - *Data frames*
- Three class of MAC frames
  - *Class 1*
    - *Most types of control frames, many management frames, select data frames*
  - *Class 2*
    - *Association requests and responses, re-association requests and responses, and disassociation frames*
  - *Class 3*
    - *Select control frames, select management frames, and most data frames*
- Exact frame formats vary across frame type and network operating mode (IBSS vs. Infrastructural)



## 802.11 Security Models



# Wired Equivalent Privacy

# WEP Overview

- WEP was introduced in the original IEEE 802.11 specification
- Goals of WEP
  - *Provide data integrity*
    - *Provided through a cyclic redundancy code (CRC)*
  - *Provide access control*
    - *Provided through WEP encryption*
  - *Provide confidentiality*
    - *Provided through WEP encryption*
- WEP security is available only in infrastructure-mode 802.11 networks
  - *Some vendors have implemented WEP for ad-hoc mode, but performance has often been reported as poor and unstable*

# WEP Encryption

- WEP is based on the RC4 algorithm
  - *A 24-bit Initialization Vector (IV) is processed through a function with a shared secret key.*
  - *The resulting key stream encrypts user data through an exclusive-OR operation*
- WEP, as defined by the 802.11b standard employs 40-bit shared secret keys
  - *Overall 64-bit key comes from 40-bit shared secret key and 24-bit IV*
  - *Small key size required to meet US Export Control laws in the early-mid 90's*

# WEP Vulnerability

- Well known that WEP key is far too small
  - *Small key size results in brute-force compromise in less than 5 hours (Reference 13)*
- WEP2 extended the size of the key to 104 bits
- Certain vendor implementations have extended WEP key size to 256 bits
- However, the WEP security model makes WEP vulnerable even with a key length of 1000 bits (Reference 13)
  - *Heavy re-use of keys*
    - *Encryption and authentication keys are identical*
  - *Lack of key management (no automated exchange or updating of keys)*
    - *Resulting lack of key updates puts networks at risk due to increased risk to crypto-analysis*
- Vulnerable to passive network sniffing
  - *Existence of automated tools that can determine WEP keys in as little as three hours in a fully automated fashion*
    - *Infamous example is AirSnort*
      - <http://airsnort.shmoo.com>

## WEP Vulnerability (continued)

- Lack of a sufficiently secure authentication mechanism
  - *As deployed, most WLANs employ open authentication*
  - *Shared-key authentication, however, is not secure*
- Shared-key authentication is a standard challenge-response system
- However, authentication is one-way
  - *Introduces well-known vulnerabilities*
    - *Man-in-the-middle attack*
    - *'Evil twin' attack*
- Poor authentication mechanism also introduces significant denial-of-service (DoS) vulnerabilities because of ability of unauthorized station from injecting frames into the network to attack proper MAC operation
  - *Example: constant transmission of association and de-association messages from an unauthorized node who has implemented a man-in-the-middle attack*

# Built-in Security Mechanisms

- SSID Broadcast Suppression
  - *To access the network, a MS must know the correct SSID*
  - *If this SSID is kept secret, it is equivalent to a network password*
  - *This provides rudimentary protection against the casual hacker*
  - *Can be defeated through standard password attack techniques*
- MAC Address Filtering
  - *This type of access control list (ACL) can be used to specifically define which computing platforms are allowed access to the network*
  - *This is a valid solution for small networks*
  - *However, quickly cumbersome for large networks*
  - *Can be overcome through eavesdropping*



# The 802.11i Security Model

## 802.11i: The Secure WLAN Technology

- 802.11i was ratified in mid-2004 and introduced as ‘the secure WLAN technology’ (Reference 14)
- 802.11i provides **significantly** enhanced security over 802.11 WEP networks
- Three key components within the 802.11i architecture
  - *Temporal Key Integrity Protocol (TKIP)*
  - *Counter-mode Cipher Block Chaining with Message Authentication Codes (CBC-MAC)*
  - *802.1x port authentication*

## 802.11i: TKIP

- TKIP designed as an immediate replacement for WEP
  - *Corrects well-known problems with small IVs and encryption keys*
- Employs RC4 encryption
- Employs a 48-bit IV
  - *Compared to the 24-bit IV of WEP*
- Employs a larger 128-bit encryption key
- Employs per-packet encryption
  - *A shared base key, the MS MAC address, and packet sequence number form a unique key for each packet*
  - *Considered much more secure by the industry*
- Periodically rotates the broadcast key
- While much more secure, TKIP is only a temporary solution to provide a quick-fix to the vulnerable WEP security architecture

## 802.11i: CCMP

- Counter mode with CBC-MAC Protocol (CCMP) employs the next-generation 128-bit advanced encryption standard (AES) in place of RC4
  - *The community considers AES to be a viable solution*
  - *CCMP is a required component of any 802.11i-compliant device*

## 802.11i: 802.1x

- Port-based authentication mechanism for Ethernet networks
  - *Employs Extensible Authentication Protocol (EAP)*
- As in WEP, a MS must authenticate before receiving full network access
- However, the AP performs two-way authentication
  - *Mitigates the man-in-the-middle attack*
- 802.11i also requires an authentication server within the network



# WiFi Protected Access

## WPA Overview

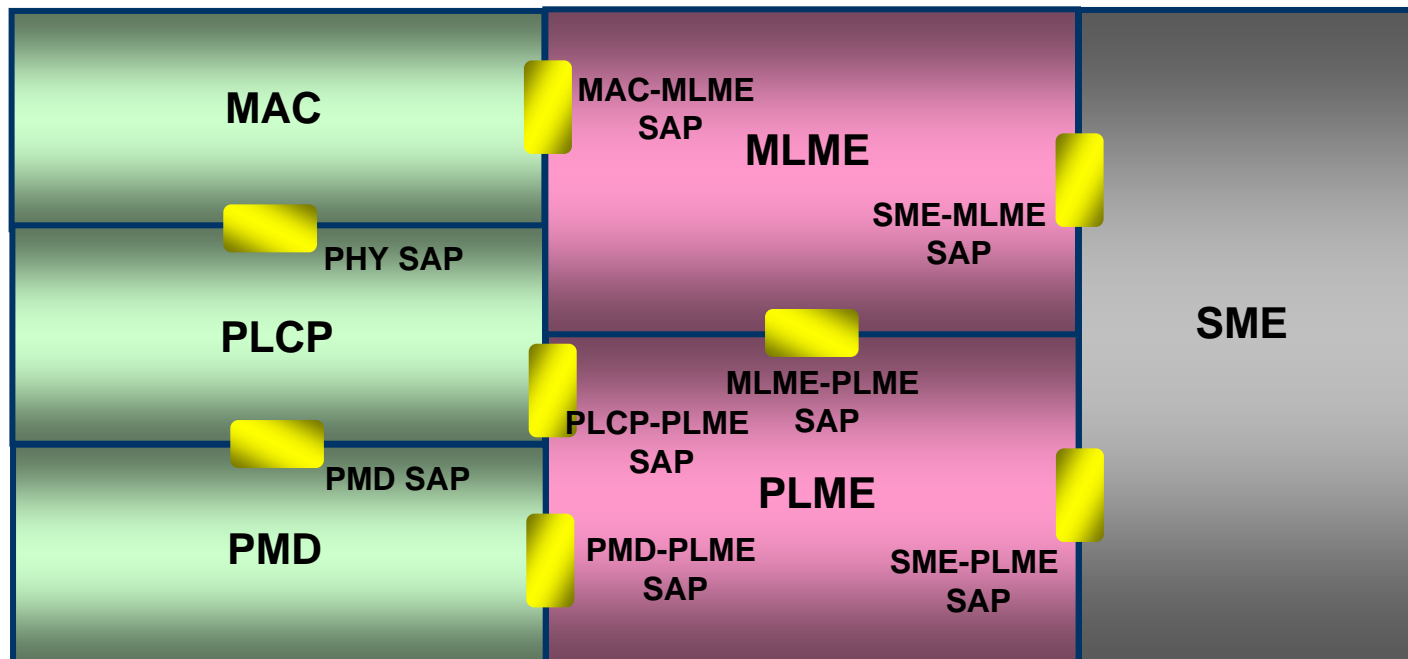
- WPA released by the WiFi Alliance
- WPA is a subset of 802.11i that was rushed to market to provide an immediate 'band-aid' to the significant vulnerabilities of WEP
  - *Employs TKIP*
- The second-generation WPA encryption standard, WPA2 (which is identical to 802.11i), will employ CCMP



# The 802.11 Management Model

# 802.11 Management

- The 802.11 management model contains three management entities:
  - *MAC Sub-layer Management Entity (MLME)*
  - *PHY Layer Management Entity (PLME)*
  - *Station Management Entity (SME)*
  - *These management entities communicate to one another and the data plane through SAPs, through which management functions can be invoked*



# Roles of 802.11 Management Entities

- MLME – provides the set of MAC management functions necessary for proper WLAN operation
- PLME – provides the set of PHY management functions necessary for proper WLAN operation
- SME – a layer-independent entity that is typically conceptualized in a separate management plane
  - *Gathers layer-dependent status from the various layer management entities*
  - *Sets values of layer-specific parameters*
  - *Exact SME functions are not specified in the 802.11 standards*
- Each 802.11 standard provides for specification of MLME and PLME functions and primitives
  - *MLME functions and primitives may vary across specifications*
  - *Model holds across technologies*

# An Example: OFDM PHY Service Parameter List

- The PLME interfaces to the MAC layer
  - *Primitives within the PLME include TXVECTOR and RXVECTOR*

Table 77 – RXVECTOR parameters

Parameter	Associate primitive	Value
LENGTH	PHY-RXSTART.indicate	1–4095
RSSI	PHY-RXSTART.indicate (RXVECTOR)	0–RSSI maximum
DATARATE	PHY-RXSTART.request (RXVECTOR)	6, 9, 12, 18, 24, 36, 48, and 54
SERVICE	PHY-RXSTART.request (RXVECTOR)	Null

Table 76 – TXVECTOR parameters

Parameter	Associate primitive	Value
LENGTH	PHY-TXSTART.request (TXVECTOR)	1–4095
DATARATE	PHY-TXSTART.request (TXVECTOR)	6, 9, 12, 18, 24, 36, 48, and 54 (Support of 6, 12, and 24 data rates is mandatory.)
SERVICE	PHY-TXSTART.request (TXVECTOR)	Scrambler initialization; 7 null bits + 9 reserved null bits
TXPWR_LEVEL	PHY-TXSTART.request (TXVECTOR)	1–8

\*Tables taken from [802OFDMREF]



# Emerging 802.11 Technologies

## Other IEEE 802.11 Flavors



- There is a variety of other task groups that are developing additional 802.11 WLAN standards that are of interest
  - *Task Group E (TGe): Modification of the MAC specification to improve and manage QoS, provide classes of service, and enhance security/authentication*
    - *Ratified in September 2005 as standard*
  - *Task Group S (TGs): Modification of the MAC to improve support of multi-hop mesh networking concepts*
  - *Task Group N (TGn): Modification of the MAC and PHY specification to improve throughput performance*
    - *MIMO technology*
  - *Task Group R (TGr): Modification of the MAC to improve mobility support*
  - *Task Group W (TGw): Extension of security features to management and control frames*



## 802.11e: Quality of Service

## The IEEE 802.11e Standard

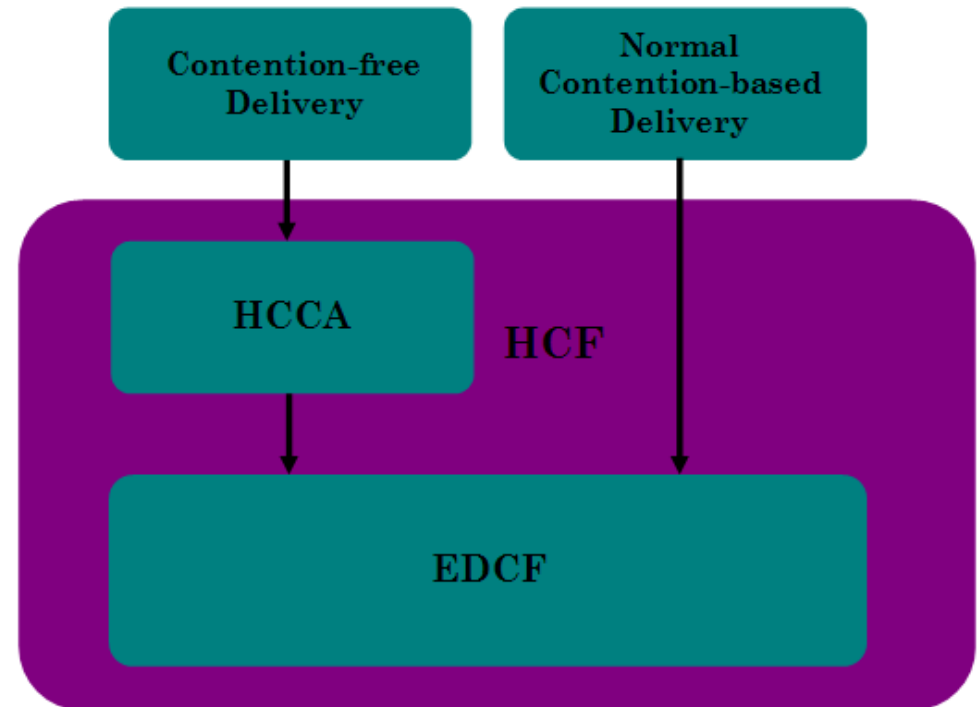
- Growing desire for WLANs to support QoS concepts in support of performance-sensitive multimedia applications (e.g. voice)
  - *Particularly as the Internet continues to develop QoS technologies*
- IEEE 802.11e standard is the IEEE effort to introduce QoS support into the 802.11 technology family (Reference 15)
- The 802.11e standard modifies the legacy 802.11 MAC specification, providing various modifications to both provide QoS support but also to enhance efficiency
- 802.11e interoperable with the legacy 802.11

## 802.11e Efficiency Enhancements

- The 802.11e MAC makes several modifications that provide efficiency benefits over the original 802.11 MAC
  - *The Transmission Opportunity (TXOP) and multiple frame transmissions*
    - *The original 802.11 MAC allowed for the transmission of a single frame for each channel access*
    - *The 802.11e MAC allows an MS to contend for a period of time (TXOP), during which multiple frames may be transmitted*
  - *The Direct Link Protocol (DLP)*
    - *Allows for direct MS-MS communications, even within infrastructural mode*
  - *Block acknowledgements*
    - *The original 802.11 MAC forces for an acknowledgement to be received before another frame can be transmitted (Stop-and-Go)*
    - *The 802.11e MAC allows for acknowledgements of multiple frames with a single message*

## 802.11e Channel Access

- The 802.11 MAC introduces a new access mechanism, the Hybrid Coordination Function (HCF)
  - Supports both PCF and DCF to enable full backwards compatibility
- Two methods by which an MS can access the wireless channel
  - Contention-based access
    - Enhanced (DCF) (EDCF)
  - Contention-free access
    - HCF Controlled Channel Access (HCCA)



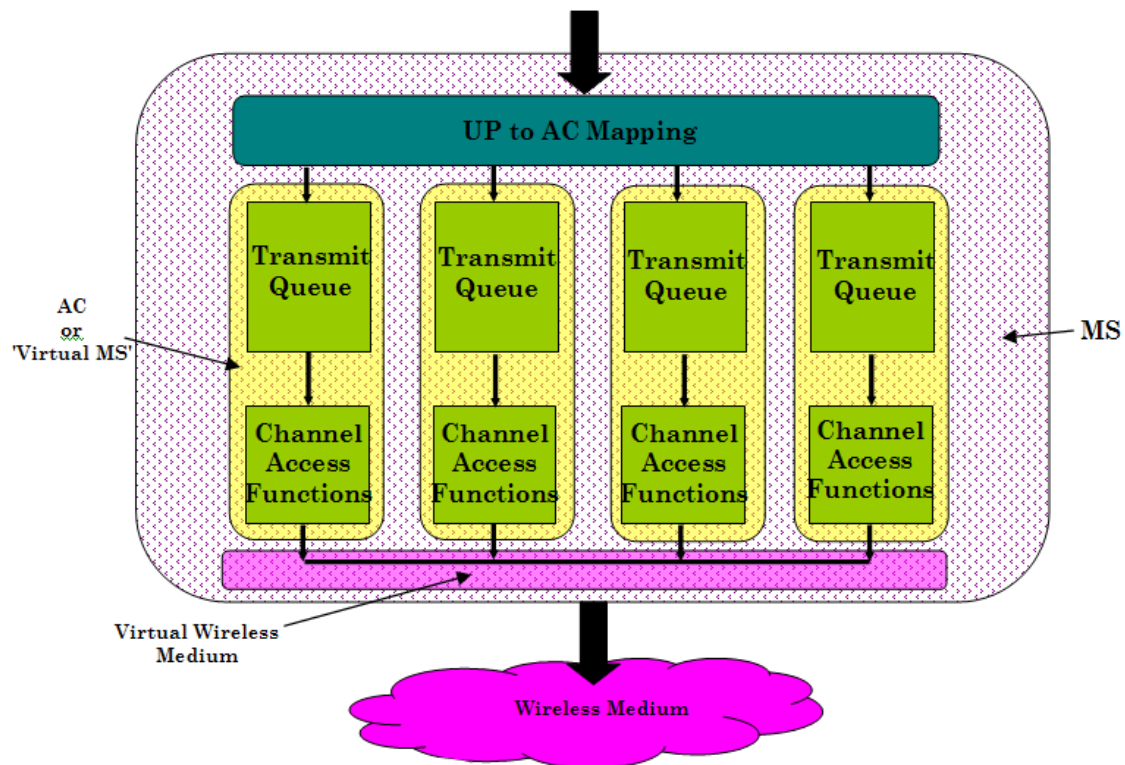
## 802.11e Contention-based Access

- QoS support is introduced through Traffic Categories (TCs)
  - A total of eight user priorities (UPs) are mapped to up to four access category (AC)

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

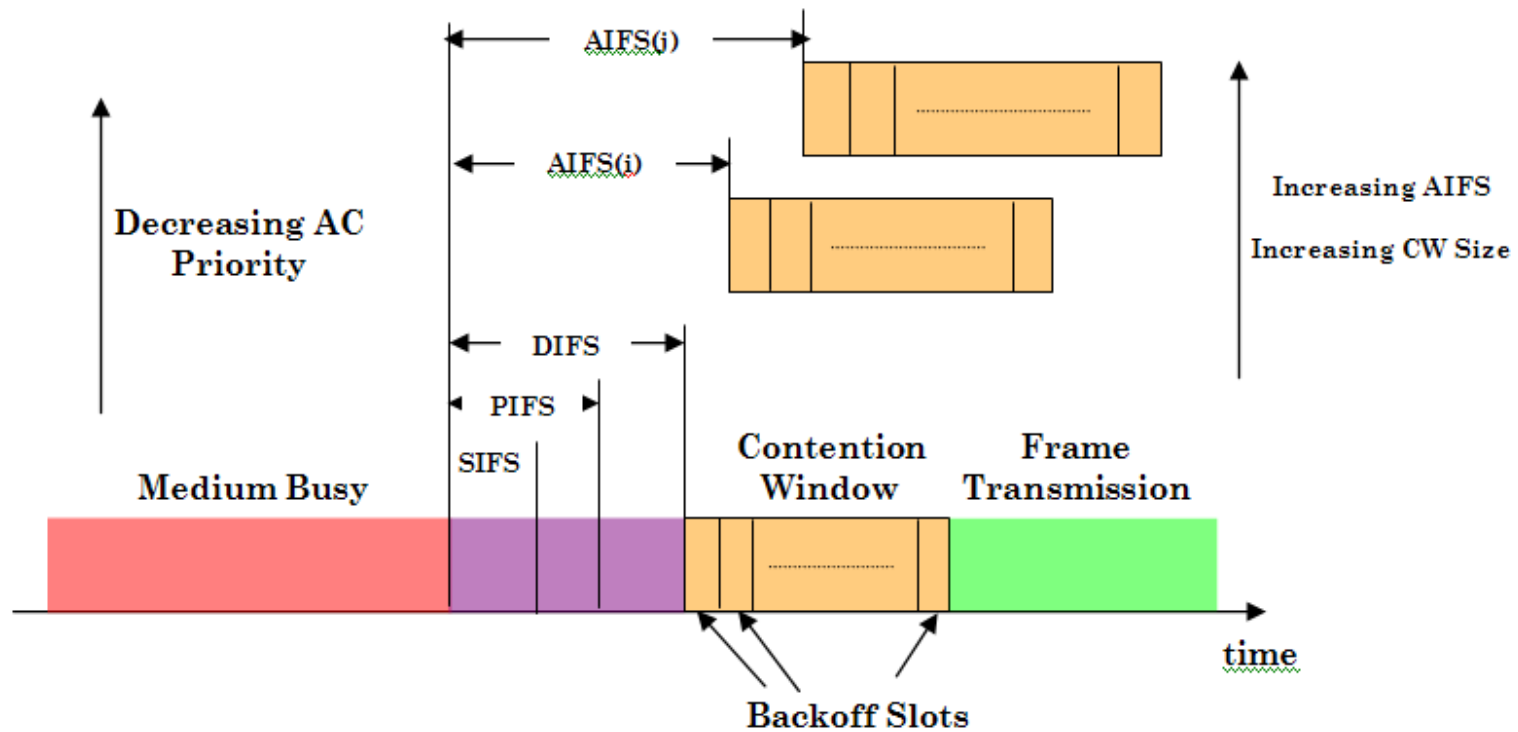
## 802.11e Reference Model

- Each AC is a 'virtual MS' (each virtual MS is analogous to the MS of the original MAC) that contends for the medium independently
- Each AC is configured independently



# The EDCF Mechanism

- Each AC (or virtual MS) implements an independent EDCF configured commensurate with data user priorities to provide preferential channel access





# IEEE 802.11n

## What is 802.11n?

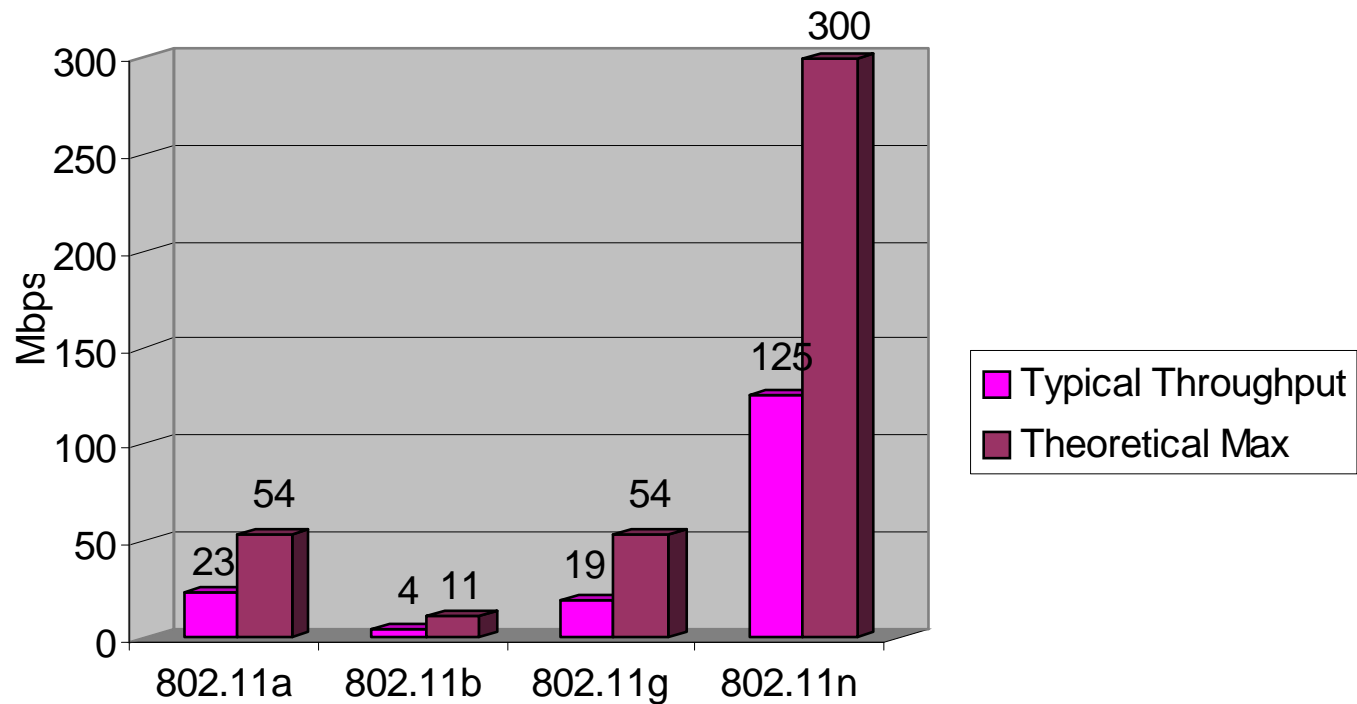
- MAC and PHY amendment to 802.11-2007 baseline specification
- Draft 2.0 802.11n technical specification approved in March 2007
- Design goal:
  - *300 Mbps at moderate ranges*
  - *802.11g-equivalent data rates at significantly greater ranges*
- Actually, similar/identical to 802.11a/g in many respects

# 802.11n – How it Compares with other flavors of 802.11

	802.11a	802.11b	802.11g	802.11n
Standard Approval	Sept. 1999	Sept. 1999	June 2003	Anticipated 2008
Available Bandwidth	580 MHz	83.5 MHz	83.5 MHz	83.5 MHz/580 MHz
Frequency Band of Operation	5 GHz	2.4 GHz	2.4 GHz	2.4 GHz/5 GHz
# of Non-overlapping Channels (US)	24	3	3	3/24
Data Rate per Channel	6-54 Mbps	1-11 Mbps	1-54 Mbps	1-600 Mbps
Modulation Type	Orthogonal Frequency Division Multiplexing (OFDM)	Direct Sequence Spread Spectrum (DSSS), Complimentary Code Keying (CCK)	DSSS, CCK, OFDM	DSSS, CCK, OFDM, MIMO-OFDM
Typical Ranges (Indoor/Outdoor)	~30m/~100m	~35m/~110m	~35m/~110m	~70m/~160m

# 802.11n – How it Compares with other flavors of 802.11

Typical Throughput vs. Theoretical Maximum



## Some Key Characteristics of 802.11n

Feature	802.11n
Backward Compatibility	802.11a/b/g using protection mechanisms
Available Bandwidth	83.5/580 MHz
Frequency Band of Operation	2.4 and 5 GHz
# of Non-overlapping Channels (US)	3/24
Channel Bandwidth	20 or 40 MHz (optional)
Theoretical Throughput per Channel	From 1 Mbps (b/g) to 600 Mbps (4x4 MIMO configuration, 40-MHz channel, 5/6 coding rate, 108 data sub-carriers, 2160 data bits per symbol)
Modulation Type	DSSS, CCK, OFDM, MIMO-OFDM, etc. The draft standard lists 77 different modulation and coding schemes (MCSs) indices.
Guard Intervals (GI)	400 and 800 nsec
MIMO Power Save	Limits power consumption penalty of MIMO by utilizing multiple antennas only on as-needed basis (required)
Aggregation	Improves efficiency by allowing transmission bursts of multiple data packets between overhead communication (required)
Reduced Inter-frame Spacing (RIFS)	One of several draft-n features designed to improve efficiency. Provides a shorter delay between OFDM transmissions than in 802.11a or g (required).
Greenfield Mode	Two new formats are defined for the PLCP (Physical Layer Convergence Protocol): the Mixed Mode and the Greenfield Mode. These two formats are called HT (High Throughput) formats. In addition to the HT formats, there is a legacy duplicate format that duplicates the 20 MHz legacy packet in two 20 MHz halves of a 40 MHz channel. So, the 802.11n physical layer operates in one of 3 modes in the time domain: Legacy mode, Mixed Mode or Greenfield Mode. Greenfield Mode improves efficiency by eliminating support for 802.11a/b/g devices in an all draft-n network (currently optional).



# IEEE 802.11n – An Overview of the Marketplace

# Types of 802.11n Radios

- Pre-n
  - *Proprietary products*
- 802.11b/g MIMO
  - *Application of adaptive beam-forming to existing 802.11b/g product lines*
  - *Backwards compatible with existing 802.11b/g products*
- Draft 1.0 n
  - *Poor interoperability, market 'failure'*
- Draft 2.0n
  - *When we say '802.11n', we mean this!*

# WiFi Alliance Certification and Deployment

- WiFi Alliance already certifying 802.11n radios based on Draft 2.0 802.11n specification
  - *Began June 2007*
- As of 27 August 2007, 78 products certified
- As of 18 February 2008, 223 products certified
- As of 8 September 2008, 397 products certified
  
- Rapid adoption by equipment vendors
  - *Over 50% of all chipsets currently shipped supports 802.11n*
  
- Deployment slow, however
  - *Current WiFi usage dominated by Internet access, which limits usefulness of 802.11n*
    - *End networks typically limited by Cable or DSL connection rates*
    - *Driving scenario eventually to be usage for in-home video distribution*

## Some 802.11n Product Trends

- Typical transmit powers of 100-300 mW are common
- Majority of IEEE 802.11n products support both 20 and 40 MHz channel bandwidths
- Majority of IEEE 802.11n products employ 2 or 3 antennas
- The majority of current IEEE 802.11n products employ 3 antennas
- The majority of current IEEE 802.11n products operate only in the 2.4 GHz ISM frequency band
- Emerging products increasingly support dual-band (2.4, 5 GHz) simultaneous operations



# Personal Area Networks

# Personal Area Network Overview

- The goal of WPANs are typically to 'remove the cables' from products
  - *The driving usage case for WPANs has historically been the 'cable-free PC'*
  - *In general, WPANs are envisioned to remove the need for most types of cabling of devices beyond power hook-ups*
    - *Cordless hands-free cellular head-sets*
    - *Cordless mice*
    - *Cordless keyboards*
    - *Cordless printers*
    - *Cordless speakers*
    - *Cordless televisions*
    - *Cordless stereos*

## IEEE 802.15

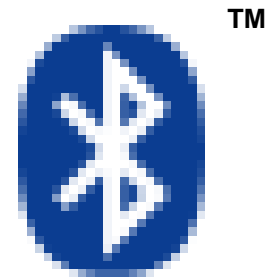
- The IEEE 802.15 working group defines Physical and MAC layer standards for Wireless Personal Area Networks (WPANs)
- There are currently six Task Groups
  - *TG1a – Provides PHY and MAC standards that matches the Bluetooth v1.2 specification (TG1 established the original formalized specification matching Bluetooth v1.1)*
  - *TG3a – Alternate high-rate PHY standard (goal is hundreds of Mbps up to 1 Gbps) (likely to employ Ultra Wideband (UWB) technology)*
  - *TG3b – MAC Amendment Task Group, aims to improve implementation and interoperability of the WPAN MAC in 802.15*
  - *TG4a – provides the alternate low rate PHY standard to provide enhanced precision ranging and location capability (UWB technology)*
  - *TG4b – A project for specific enhancements and clarifications to the older 802.15.4 standard (which was a low power standard to enable multi-month or multi-year operation)*
  - *TG5 – addressing issues related to WPAN mesh networking, including leveraging the concept to improve performance, battery life, and ease of network configuration*

# Bluetooth – A Quick Introduction

- Bluetooth was originally conceived by engineers at Ericsson
- In 1994, Ericsson initiated a project to study the feasibility of a low-power, low-cost radio interface to eliminate the cables mobile phones and their accessories
  - *Quickly realized its wider applicability*
- In 1998, the Bluetooth Special Interest Group (SIG) was formed
- Bluetooth standard developed by the Bluetooth SIG
  - *Chartered to define and promote Bluetooth technology as an interoperable, cross-platform technology for all device types*
  - *The Bluetooth SIG is an organization consisting of hundreds of telecommunications and computing companies*
    - *Founding members were Ericsson, Intel, Nokia, and Toshiba*
    - *There are now over 2,400 member companies from various fields*
      - Academia, consumer electronics, automotive, silicon, consulting, telecommunications
- Version 1.0 of Bluetooth was published in July 1999
- Now maintained in IEEE 802.15 WG (802.15.1)

## Bluetooth – The Name

- Harold Blaatand was the King of Denmark from approximately 940-985 A.D.
- During his reign, he united Denmark and Norway and brought Christianity to all of Scandinavia
- Blaatand translates, loosely, to 'Bluetooth'
- The origins of his name are unknown, but folklore has it that he was known by this name because of the bluish residue on his teeth due to his fondness for blueberries
- The Bluetooth SIG was hoping to unify multinational companies to accomplish a common technology and business goal
- Thus the SIG, which originated in Scandinavia, took on the symbolic name of the long-ago King that unified Scandinavia...the Bluetooth SIG
  - *The name stuck to the technology as well*
  - *The Bluetooth logo is inspired by the initials 'H.B.' for Harold Bluetooth*



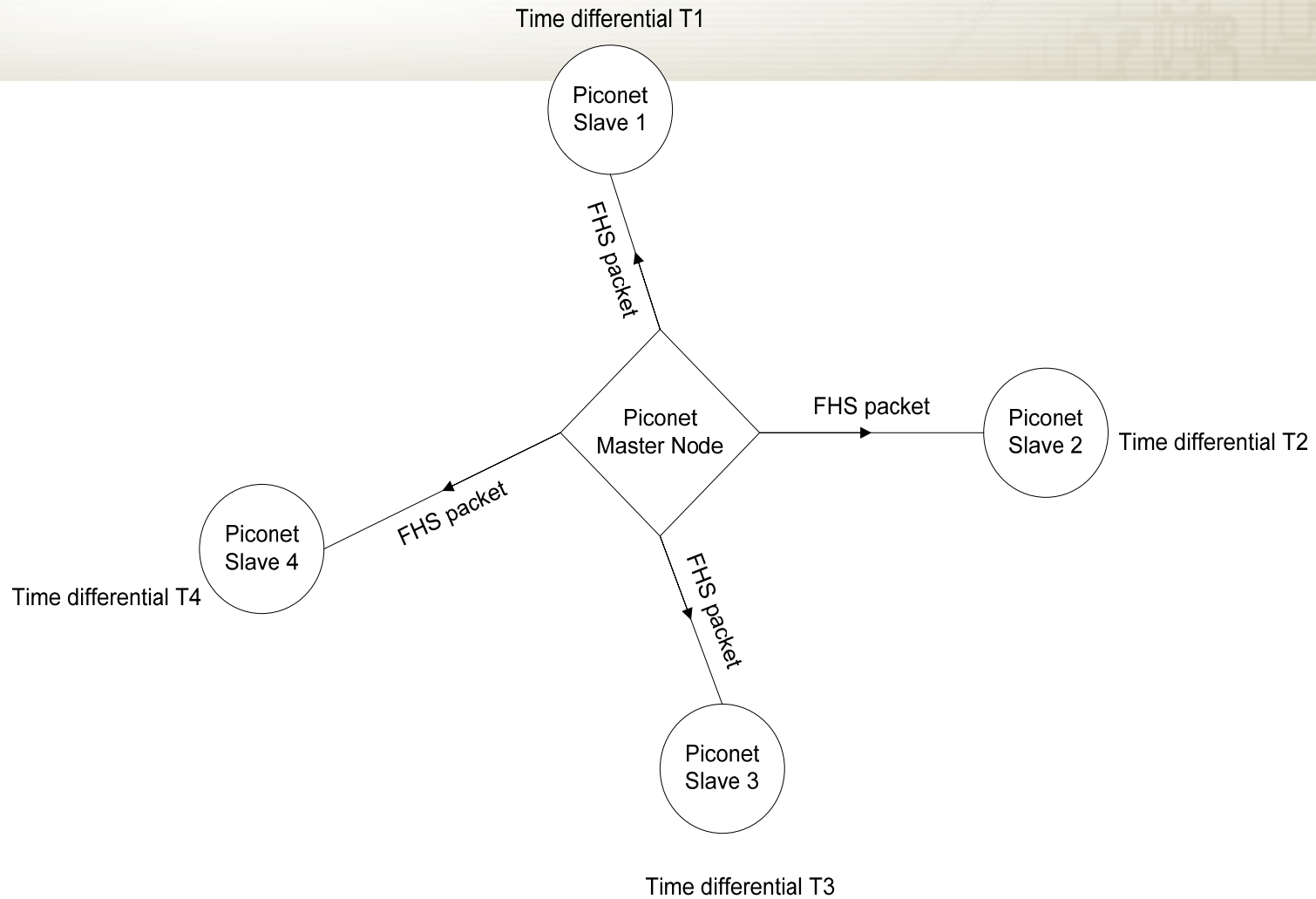
# Bluetooth – The Technology

- Bluetooth operates in the unlicensed 2.4 GHz ISM frequency band
  - *Same as 802.11b, 802.11g*
- Provides data rates of 400 kbps (symmetric) or 700 kbps (asymmetric)
- Frequency-hopping Spread Spectrum (FHSS) is employed
  - *A rate of up to 1600 hops per second over 79 one MHz channels (hops across the entire ISM band)*
- Modulation in Bluetooth is Gaussian Frequency Shift Keying (GFSK)
  - *FSK modulation that is passed through a Gaussian filter to ‘shape’ channel symbols*
  - *More spectrally efficient than FSK alone*
- Several error correction schemes are available
  - *Rate 1/3 and 2/3 FEC coding, and ARQ schemes*
- The waveform is very similar to the FHSS waveform of 802.11

# Bluetooth Networks

- Bluetooth forms 'piconets' or associations between nodes based on a particular hopping sequence
  - *All devices in a piconet hop together*
- A master-slave model is employed by Bluetooth
  - *Note role does not imply privilege, but only governs the synchronization of the FHSS communications between devices (master node determines frequency hopping pattern)*
  - *In most aspects, devices are peers*
- Within a piconet, there is a single master node
  - *Any node can be a master device*
  - *A node may be a master node on one connection, and a slave node on another connection*
- Its clock and Bluetooth device address (BD\_ADDR) are passed to slaves via frequency hop synchronization (FHS) packets
- The master BD\_ADDR is used to calculate the sequence of frequency hops required for all devices within the piconet to follow in order to communicate
- The master clock is used to decide which hop in the sequence is current (known as the hopping phase)
- All slave devices within the piconet use the differential between the master clock and their own to determine which frequency to use at any given time
- Each piconet operates on a unique frequency-hopping sequence

# Basic Hierarchy of a Single Bluetooth Piconet



# Bluetooth Networks

- Two types of network services offered
  - *Synchronous Connection Oriented (SCO)*
    - *In support of audio*
  - *Asynchronous Connectionless Link (ACL)*
- A master node can communicate with multiple slaves
  - *Up to 7 active slaves*
  - *Up to 255 parked slaves*
- Four modes of operation:
  - *Active – a slave is always listening for transmissions from the master*
    - *Most responsive, least power efficient*
  - *Sniff – a slave becomes active periodically (pre-arranged time schedule with master node)*
  - *Hold – similar to sniff time but more stringent ‘sleeping’ schedule*
  - *Park – maintains synchronization, but does not listen for packets at all*
    - *Least responsive, most power efficient*

# Bluetooth Physical Channels

- Physical channels in Bluetooth are characterized by a single RF combined with temporal parameters
- Two physical channels are used for communications between Bluetooth devices
  - *Basic piconet channel*
  - *Adapted piconet channel*
- Adapted piconet channel varies from the basic piconet channel in the following ways
  - *Transmitting frequencies for slaves are the same as the preceding master transmit frequency where the master frequency is recomputed with each packet transmitted by the master*
  - *Adapted type can utilize less than the 79 frequencies required for the basic piconet channel operation*
    - *Can adapt its frequency selection to mitigate frequency-selective fading*

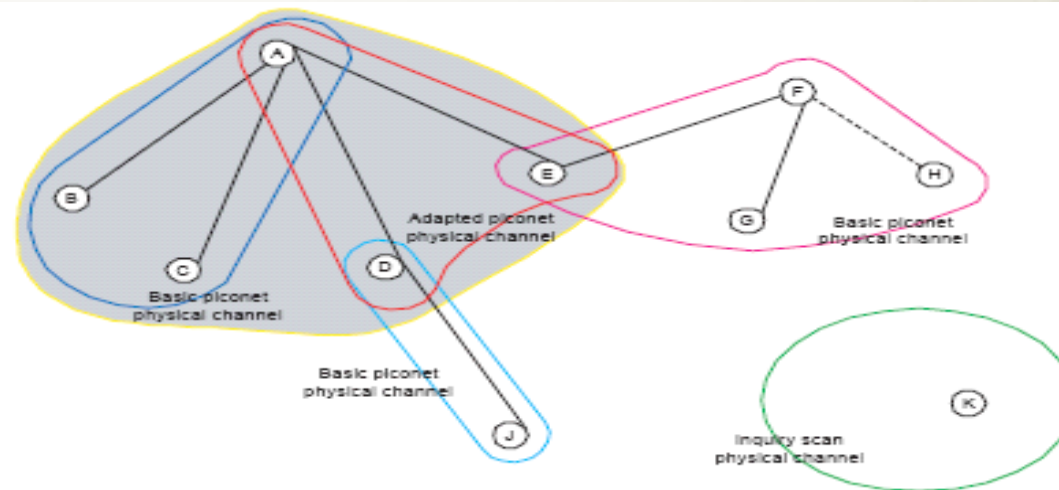
# Bluetooth Physical Channels

- Other physical channels defined within Bluetooth
  - *Inquiry Scan Channel*
    - *Used for device discovery within the Bluetooth domain*
  - *Page Scan Channel*
    - *Used for establishing connection between Bluetooth devices*

# Bluetooth Channelization

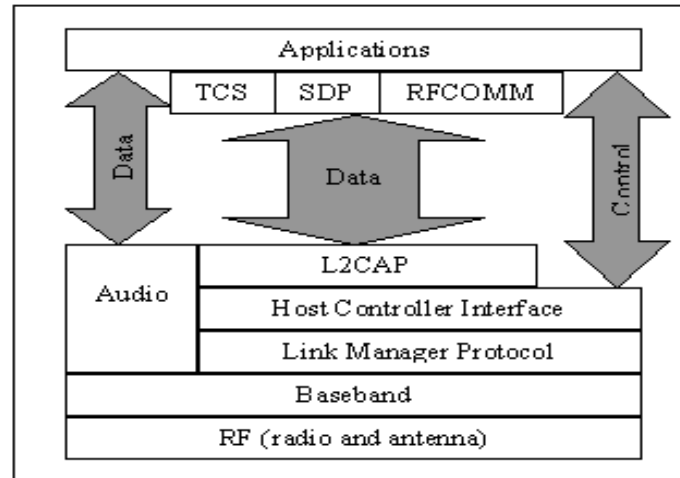
- The basic piconet channel is divided into time slots
  - *Each time slot is of length 625 microseconds*
- Time slots are numbered by the 27 most significant bits in the Bluetooth clock of the piconet master node
  - *Time slot numberings vary from 0 to  $2^{27}-1$*
- TDD is employed to allow the master and slave to alternate transmit/receive roles
- A Bluetooth frame consists of two packets
  - *Transmit followed by receive*
- The maximum packet length can extend over five time slots

# Bluetooth Piconets Utilizing Different Physical Channel Types



- Node E is participating in a basic piconet with nodes F, G, and H, while also participating in an adapted piconet with nodes A and D
- Nodes A, B, and C are participating in a separate basic piconet
- Node K has not joined any piconet and is only operating on the inquiry scan channel because there are no nodes within its range
- When nodes belong to multiple piconets, it may act as a bridge between them, forming a **scatternet**

# Bluetooth Protocol Stack

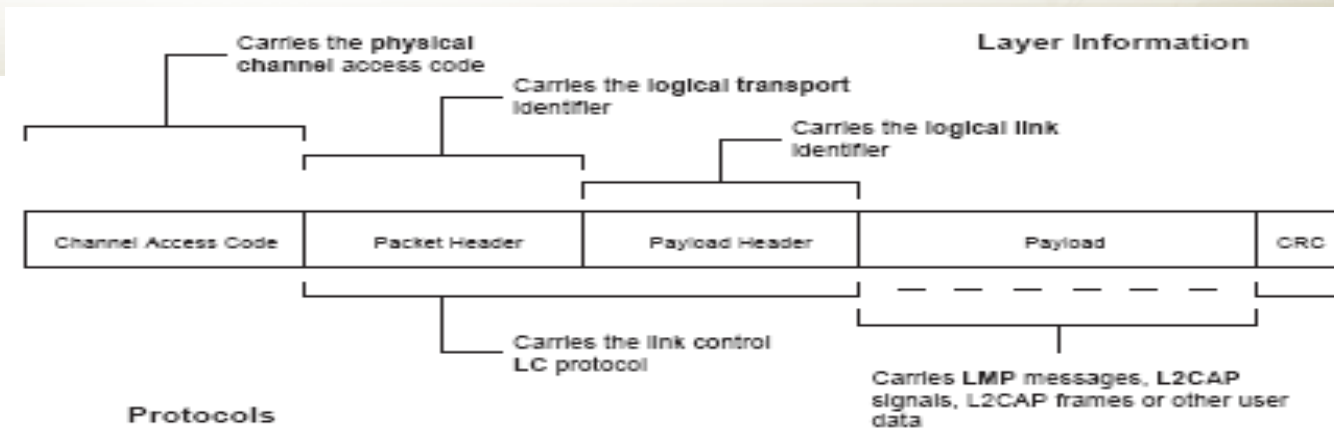


- Three groups within the Bluetooth protocol stack
  - *Transport protocol group*
    - *Layer 2 Control Access Protocol (L2CAP), HCI, Link Manager Protocol (LMP), baseband, radio*
  - *Middleware protocol group*
    - *TCS, Service Discovery Protocol (SDP), RFCOMM*
  - *Application group*

# Bluetooth Protocol Stack

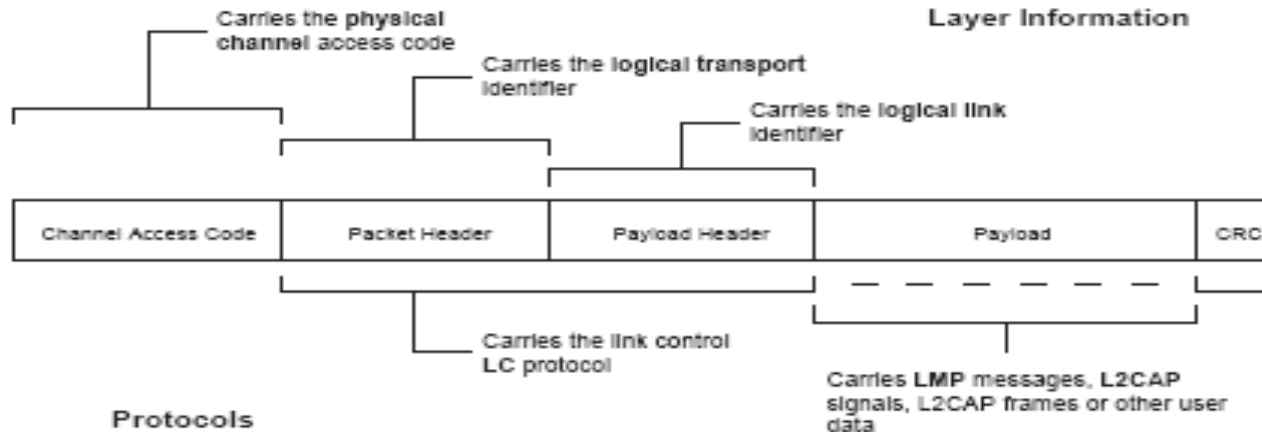
- Transport protocol group are protocols designed to allow Bluetooth devices to locate each other and to create, configure, and manage physical and logical links that allow higher layer protocols to pass data
  - *L2CAP – shields higher layer protocols and applications from the details of the lower layer transport protocols*
    - *Performs protocol multiplexing, segmentation and reassembly, admission control, coordinates communications parameters with lower layers in an attempt to maintain acceptable level of service*
    - *Supports connection-oriented and connectionless channels*
  - *LMP – negotiation of the properties of the air interface, including bandwidth allocation, authentication, encryption,*
  - *HCI – allows higher layers of the stack, including applications, to access the baseband, link manager, and other hardware registers through a standard interface*
- Middleware protocol group
  - *TCS – used for audio transport*
  - *SDP – informs higher layers about services available to them*
  - *RFCOMM – serial port emulation software*
- Application group – Application suite specifically designed to operate in Bluetooth environments

# Bluetooth Frame Format



- Generally, frames contain only the necessary fields required to complete a desired transmission
  - Thus, not all the fields shown above are used at all times
- Channel access code is included for all packets
  - Used to identify a particular physical channel and receiving nodes to ignore packets on a different physical channel
- The packet header contains the destination address (LT\_ADDR) for a node on the piconet and is used by each receiving device to determine if the packet is addressed to that device
  - It is also used to route across the piconet

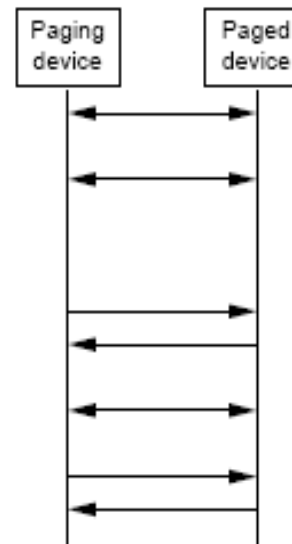
# Bluetooth Frame Format (continued)



- Payload header also includes a logical link identifier field used for routing and a length field to indicate the length of the payload
- L2CAP data within the payload field are used to multiplex the channel when more than two devices are active within the physical channel for the piconet
- CRC field used for error detection at the receiver

## Joining a Piconet

- In order to join a piconet, a device must be able to send packets on the page scan channel
- Any connectable device which is listening on this channel can receive such a page request and begin a sequence of transmissions that allows the two devices to associate and communicate
  - *Paging device becomes the default master of the resulting piconet*
- A device may be configured to automatically join a piconet upon detection or may be configured to accept only certain connections, or none at all.



Baseband page procedure

LMP procedures for clock offset request, LMP version, supported features, name request and/or detach.

LMP\_host\_connection\_req  
LMP\_accepted or LMP\_not\_accepted

LMP procedures for pairing, authentication and encryption.

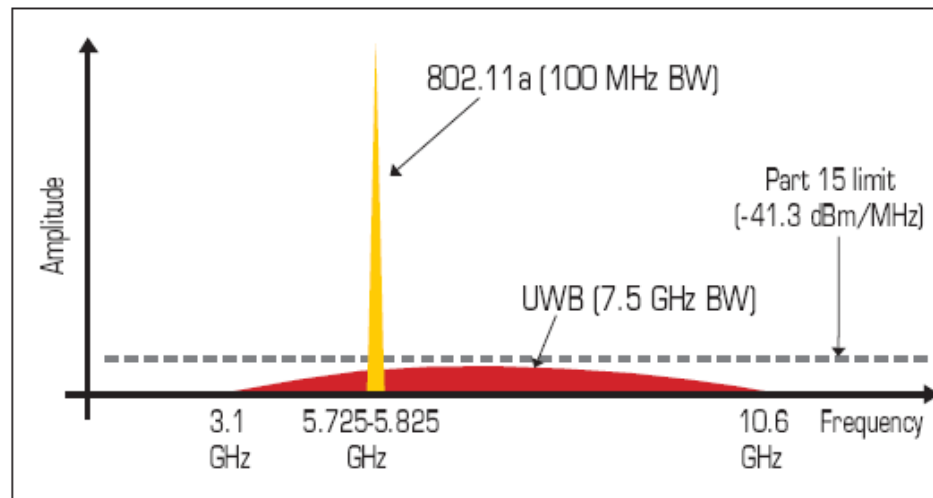
LMP\_setup\_complete  
LMP\_setup\_complete

# Bluetooth Security

- Bluetooth provides both authentication and privacy mechanisms
- Piconets may require one-way, two-way, or no authentication
- Authentication is based on a challenge-response algorithm
- Encryption is employed to provide privacy
  - *Shared secret key, with lengths of up to 128 bits*
  
- Bluetooth is not considered 'secure' in the strictest sense
- Relies heavily upon short-range nature of technology to provide protection
  - *Conventional wisdom is that unauthorized entry into the piconet would require operation within 10's of feet of the devices, thus making physical security more prominent in the overall network security plan*
  - *However, this conventional wisdom may be under challenge*

# Ultra Wideband Overview

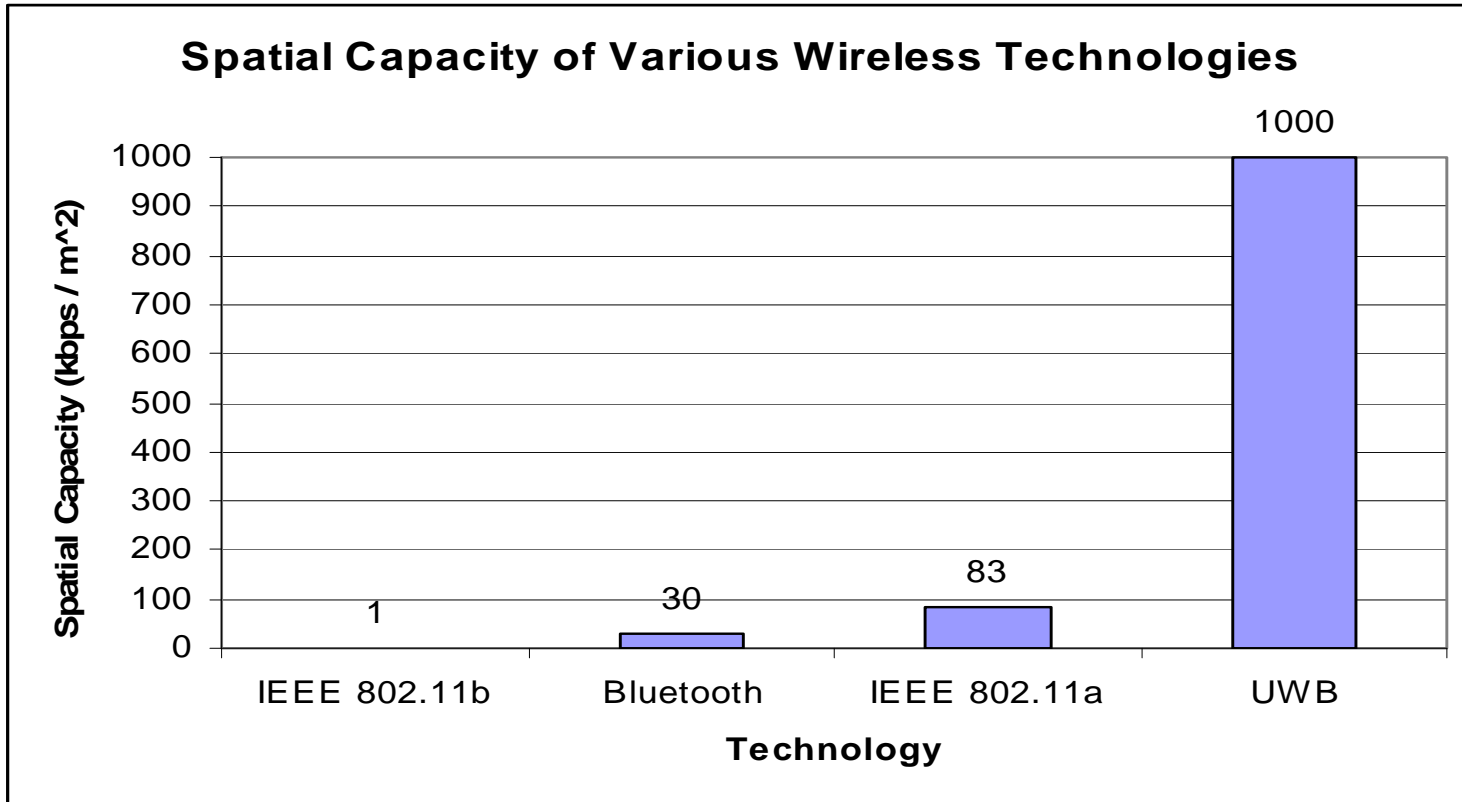
- UWB technology was originally developed in the 1960s during the height of the cold war for both American and Soviet purposes
- However, commercial interest in UWB has increased dramatically over the past 5-10 years
- The Federal Communications Commission defines UWB as any waveform whose fractional bandwidth is greater than 20% or greater than 500 MHz
- UWB waveforms are generated through the creation of very narrow time pulses that spread energy across a very large range of frequencies



## Ultra Wideband Overview (continued)

- Exhibits very good performance in terms of both detectability and robustness against interference (both intentional and unintentional)
- Over short distances (up to 10s of feet), data rates on the order of several hundred Mbps are achievable
  - *However, increasing power may enable UWB signals to propagate farther in space*
    - *Very low power density, to avoid interference*
      - UWB splashes across many allocated frequency bands and must be 'in the noise' such that they do not interfere with existing signals

# UWB Capacity Estimates Relative to other Technologies



\*Intel Labs

# Ultra Wideband Standardization

- Most notable method is in the 802.15.3a task group, which is developing the next-generation high-data rate WPAN standard
  - *Envisioned technology is Bluetooth MAC and network model with new high-rate UWB physical layer*
- However, this working group failed to produce a standard
  - *Two technology proposals on table from two consortiums*
  - *Competing consortiums continued to prevent acceptance of technology and brought progress to a standstill.*
  - *802.15.3a PAR withdrawn in early 2006*
- Will likely be *several* years before a UWB-based WPAN standard emerges
- Consortiums that are competing in 802.15.3a are now independently bringing products to market
  - *220 Mbps products on market now*
  - *440 Mbps products on market now*
  - *1 Gbps products entering market now*
    - *This large bandwidth could enable an entire new generation of wireless devices*

# Ultra Wideband Standardization

- Marketplace will decide de facto standard, and will likely come back to IEEE for formal standardization after-the-fact
  - *WiMedia Alliance vs. UWB Forum*
    - *WiMedia Alliance has really already won this battle (Wireless USB)*
- WiMedia Alliance developing Wireless USB technology
  - *500 MHz “UWB”*
  - *However, not really UWB*
    - *OFDM – composite narrowband signal*
  - *Unclear if many of the most compelling qualities of UWB are preserved using this approach*

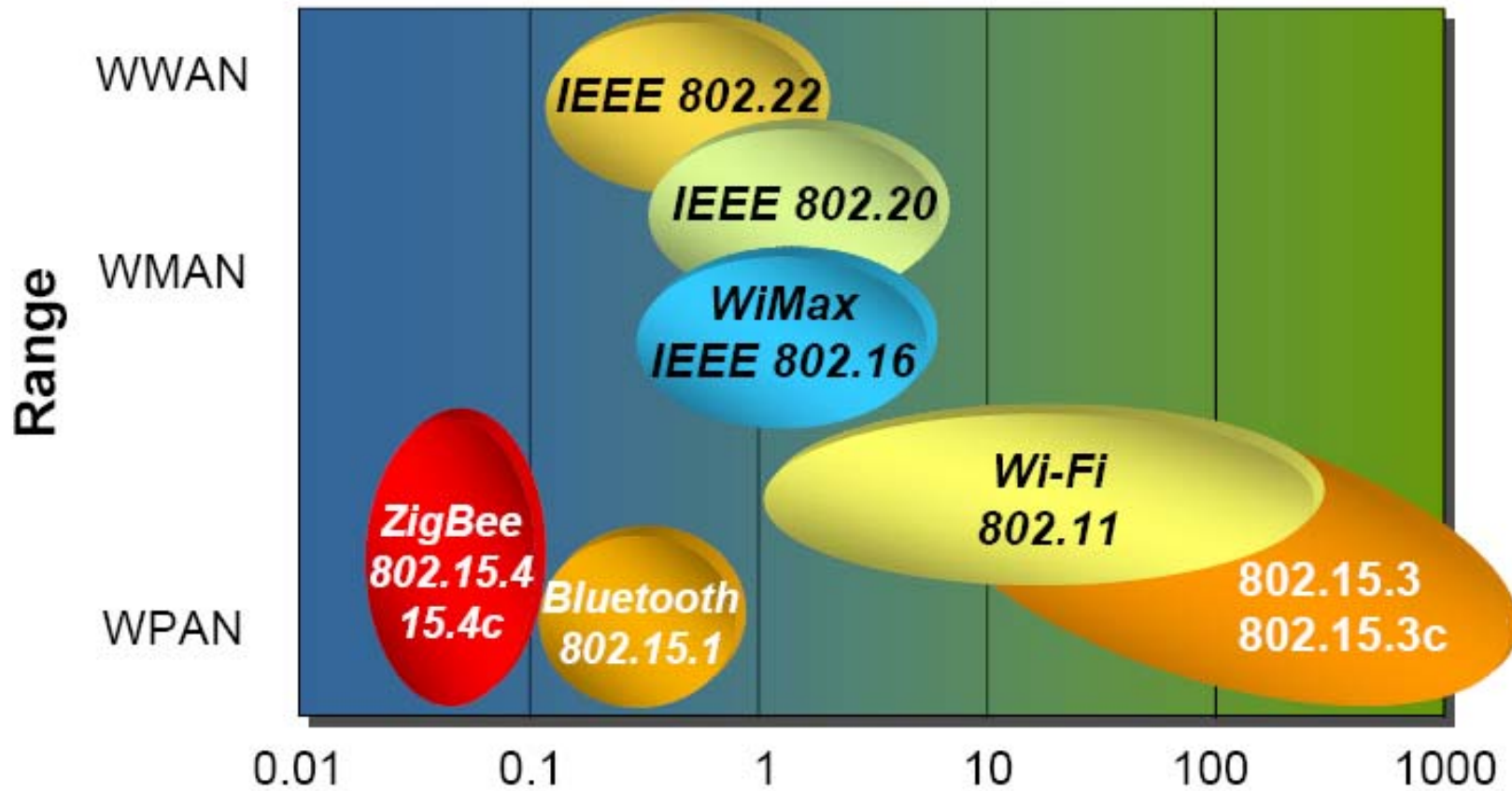
# ZigBee: WPAN Sensor Networking

- ZigBee developed by ZigBee Alliance as standardized remote sensor and control network technology
  - *Advanced metering, medical sensing and monitoring, home automation, building automation, and industrial automation*

Market Name	ZigBee®	---	Wi-Fi™	Bluetooth™
Standard	802.15.4	GSM/GPRS CDMA/1xRTT	802.11b	802.15.1
Application Focus	Monitoring & Control	Wide Area Voice & Data	Web, Email, Video	Cable Replacement
System Resources	4KB - 32KB	16MB+	1MB+	250KB+
Battery Life (days)	100 - 1,000+	1-7	.5 - 5	1 - 7
Network Size	Unlimited (2 <sup>64</sup> )	1	32	7
Bandwidth (KB/s)	20 - 250	64 - 128+	11,000+	720
Transmission Range (meters)	1 - 100+	1,000+	1 - 100	1 - 10+
Success Metrics	Reliability, Power, Cost	Reach, Quality	Speed, Flexibility	Cost, Convenience

**\*Taken from ZigBee Alliance website**

# ZigBee – How it Compares



\*Taken from ZigBee Alliance website

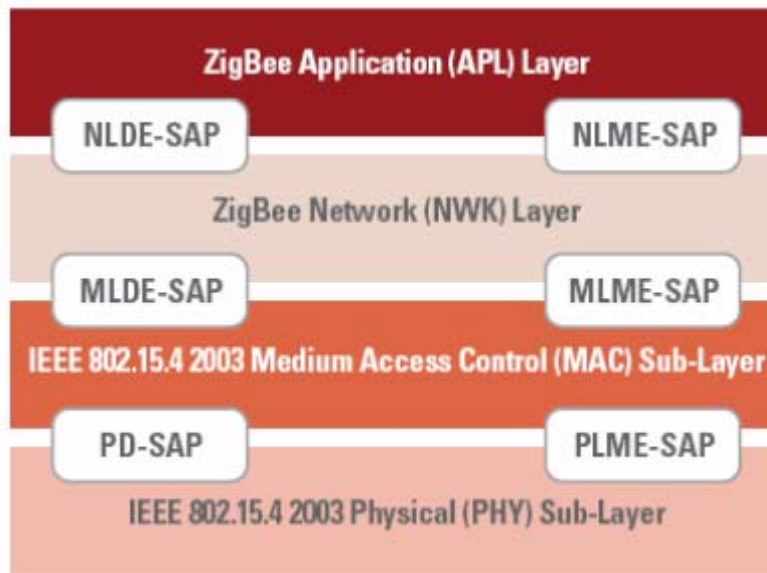
# ZigBee Alliance

- From the Zigbee Alliance web site... "The Zigbee Alliance is an association of companies working together to enable reliable, cost-effective, low-power, wirelessly networked, monitoring and control products based on an open global standard
- Technology based on 802.15.4 standard
- The charter of the Zigbee Alliance is:
  - *Definition of network, security, and application software layers*
  - *Interoperability and conformance testing specifications*
  - *Promotion of Zigbee brand products*
  - *Involvement in technology evolution*
- Zigbee Alliance is analogous to the WiFi Alliance
  - *Membership is company based and is closed, for-fee*

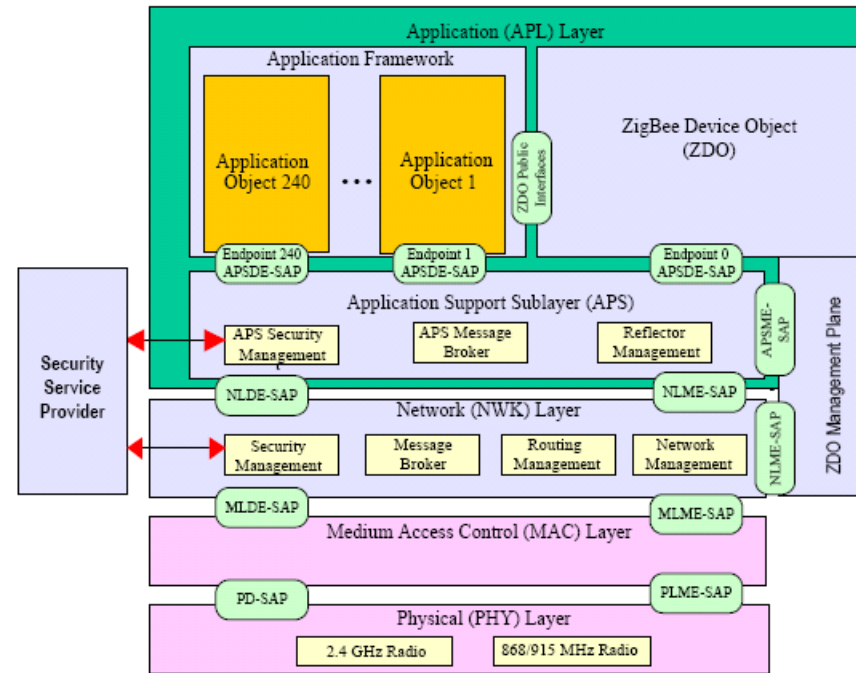


Specification	Protocol Version	Comment
Current	0x02	Backwards compatibility with ZigBee 2006 required. Backwards compatibility with ZigBee 2004 not required.
ZigBee 2006	0x02	Backwards compatibility with ZigBee 2004 not required.
ZigBee 2004	0x01	Original ZigBee version.

# ZigBee Protocol Stack

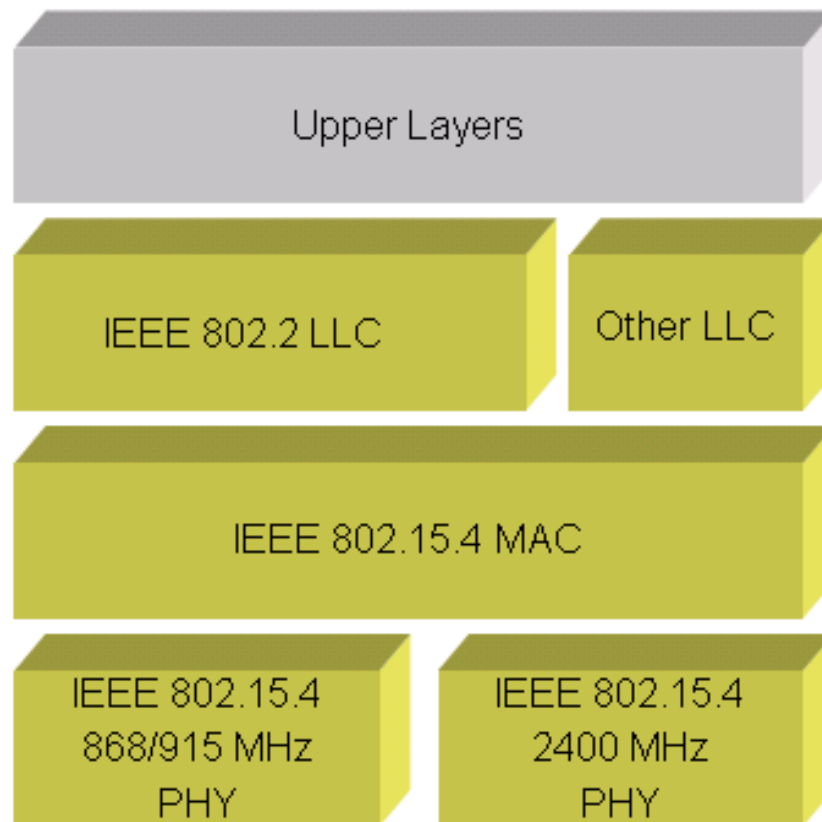


- IEEE 802.15.4 defined
- ZigBee™ Alliance defined
- End manufacturer defined
- Layer function
- Layer interface

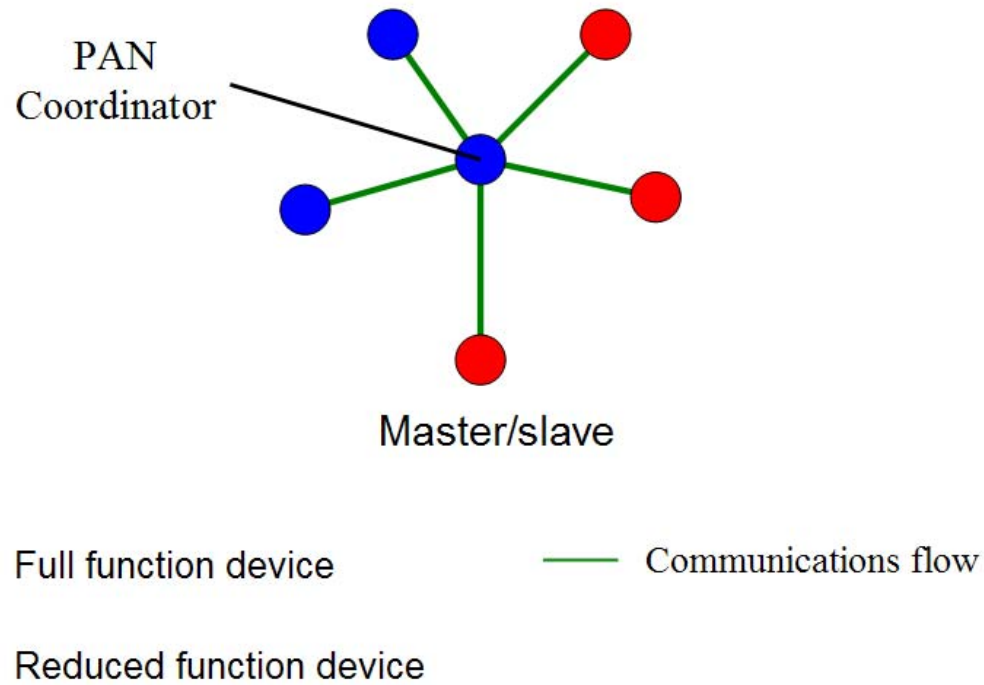


site

## 802.15.4 Logical Architecture

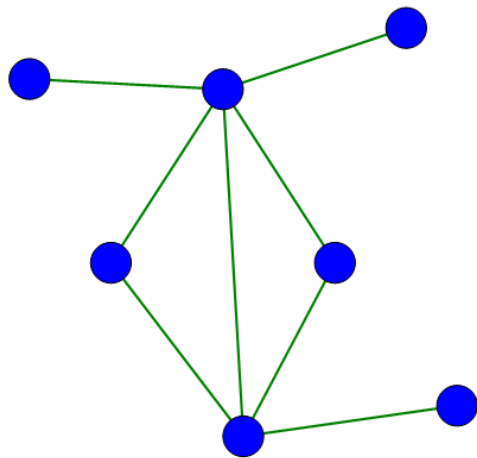


## 802.15.4 Networking



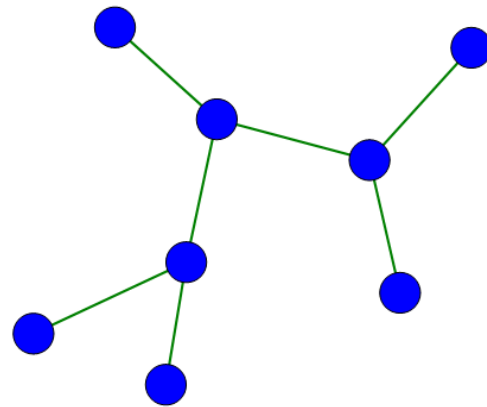
- Two types of 802.15.4 nodes:
  - *Full Function Devices (FFDs)*
  - *Reduced Function Devices (RFDs)*

## 802.15.4 Networking



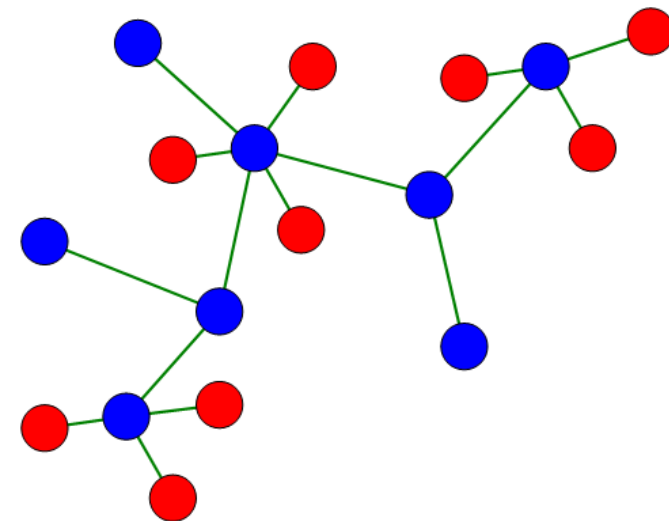
Point to point

● Full function device



Cluster tree

— Communications flow

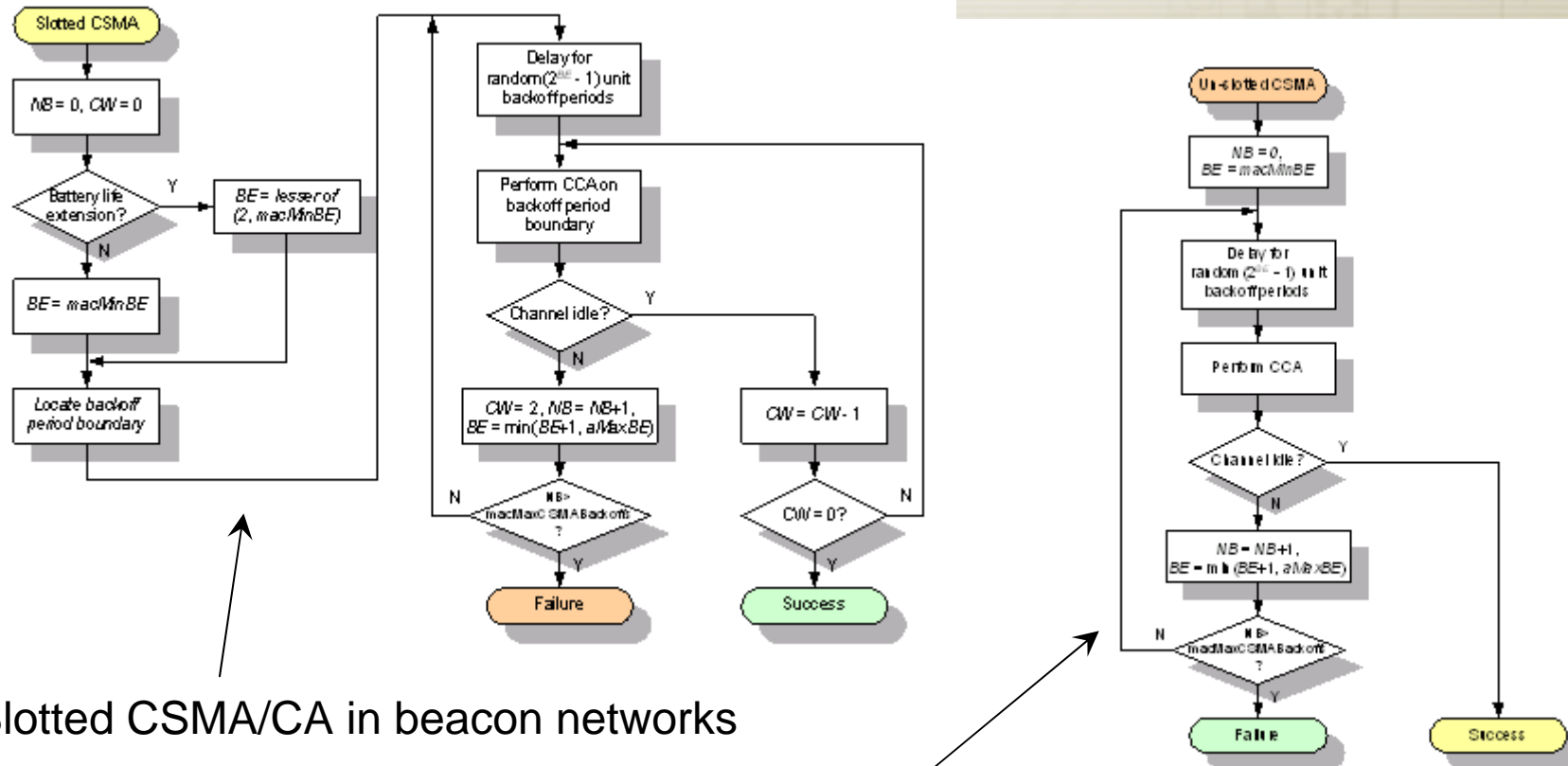


● Full function device — Communications flow

● Reduced function device

- Two topologies supported
  - *Point-to-Point (or mesh)*
  - *Cluster*
- Two types of roles in network
  - *ZigBee coordinator*
  - *ZigBee router*

# 802.15.4 Multiple Access



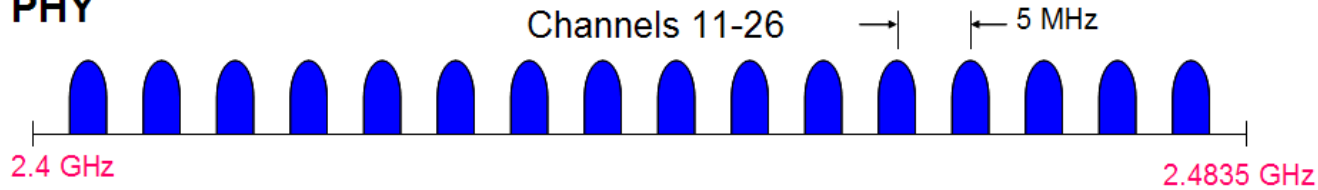
- Slotted CSMA/CA in beacon networks
- Non-slotted CSMA/CA in non-beacon networks

# 802.15.4 PHY

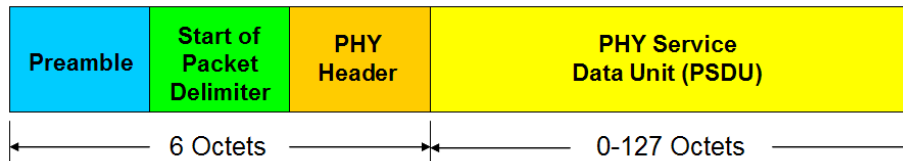
## 868MHz / 915MHz PHY



## 2.4 GHz PHY



Band (MHz)	Chip Rate (k)	Modulation	Bit Rate (k)	Symbol Rate (k)
868-868.6	300	BPSK	20	20
902-928	600	BPSK	40	40
2400-2483.5	2000	O-QPSK	250	62.5





# **802.16: Metropolitan Area Networks**

## An Introduction to IEEE 802.16

- Broadband wireless access (BWA) products and solutions have existed for quite some time
- Historically focused on providing high-rate connectivity between fixed stationary sites
  - *E.g. building-to-building bridging, connectivity to remote sites such as broadcast towers*
- However, these solutions have been proprietary in nature
  - *Poor interoperability, high cost due to lack of economy of scale*
- The IEEE 802.16 WMAN technology family is intended to provide a standard BWA solution in order to provide 'broadband wireless to the masses'

## The Hype of 802.16

- 802.16 is highly anticipated and has been called by some as ‘the next great wireless technology’
  - *Seen by some as threat to long-term viability of existing wireless technologies, such as IEEE 802.11, broadband residential technologies, such as DSL and cable, and by even more as a significant threat to 3G cellular technologies*
  - *More often, viewed as a powerful complimentary technology to these various tools*
- Regardless, much excitement, and hype, surrounds this technology
  - *“802.16 will solve all our problems”*
  - *Exaggerated claims of capabilities → high capacity (tens or hundreds of Mbps), long ranges (tens of miles), strong QoS, mobility support....and all at once!*
  - *Misunderstanding and misrepresentation*
  - *Indeed, 802.16 is emerging as a powerful technology that will help address a variety of issues in the overall problem space, but once again, there is no ‘silver bullet’*
  - *Remember the words of Obi-Wan Kenobi...*

# WiMAX is Worldwide?

- [Intel to Help Bring WiMAX to Southeast Asia](#) > [telecommunications ...](#) Daily bulletin of telecommunications related news. [www.teleclick.ca/2005/09/intel-to-help-bring-wimax-to-southeast-asia/](http://www.teleclick.ca/2005/09/intel-to-help-bring-wimax-to-southeast-asia/)
- [Promise of WiMAX to Deliver Quick, Economic Broadband in ...](#) File Format: PDF/Adobe Acrobat - [View as HTML](#) data and voice services to developing countries throughout Central and South America, the WiMAX Forum™, will host its first-ever WiMAX Pavilion at TelEXPO ...
- [Taking Wireless to The Max: WiMAX Outlook 2005 - 2010: Russia ...](#) "WiMAX Outlook 2005 - 2010, Russia", analyzes WiMAX opportunities in Russia. It includes a useful set of market data and recommendations in order to help ... [www.researchandmarkets.com/reportinfo.asp?report\\_id=300264](http://www.researchandmarkets.com/reportinfo.asp?report_id=300264)
- [Future of WiMAX - Service Providers Perspective: North America ...](#) Taking Wireless to The Max: WiMAX Outlook 2005 - 2010, North Africa · Taking Wireless to The Max: WiMAX Outlook 2005 - 2010, Central America ... [www.researchandmarkets.com/reportinfo.asp?report\\_id=311192](http://www.researchandmarkets.com/reportinfo.asp?report_id=311192)
- [WiMAX World Europe](#) This is why WiMAX World Europe Conference and Expo comes at an exceptionally ... WiMAX World Europe will offer the same high level of speakers and depth of ... [www.wimaxworldeurope.com/](http://www.wimaxworldeurope.com/)
- [picoChip R&D Facilities for 3G and WiMAX in China](#) 3G Phones, News, 3G Reviews, Forum, 3G Store, Games, 3G Newsletter and more. Daily 3g news and thousands of 3g press and industry articles via 3g search ... [www.3g.co.uk/PR/Sept2004/8294.htm](http://www.3g.co.uk/PR/Sept2004/8294.htm)
- [WiMAX/BWA in Africa — WiMAX Africa](#) remains the least connected continent in the world. Things are changing however. [www.wimax.com/commentary/spotlight/wimaxspotlight2005\\_06\\_15\\_part1](http://www.wimax.com/commentary/spotlight/wimaxspotlight2005_06_15_part1) - 33k -

[www.wisegorilla.com](http://www.wisegorilla.com)

# WiMAX Deployments (February 2007)



## 802.16 vs. WiMAX

- WiMAX Forum was formed in April 2001 as a non-profit international organization to certify conformance and interoperability of products based on the IEEE 802.16 and ETSI HiperMAN standards
  - *Also heavily involved as an advocate for 802.16 technology*
- The term WiMAX is a marketing term that has become synonymous with 802.16
  - *Much the same way Wi-Fi is synonymous with IEEE 802.11*
- “WiMAX Certified” logo will certainly be a key criterion for market viability
- People talk about the “WiMAX standard”
  - *Refers to the set of capabilities within 802.16 that will be tested for conformance and interoperability*
  - *Will heavily influence which pieces of 802.16 see significant implementation and deployment*

## 802.16 Technology Specifications

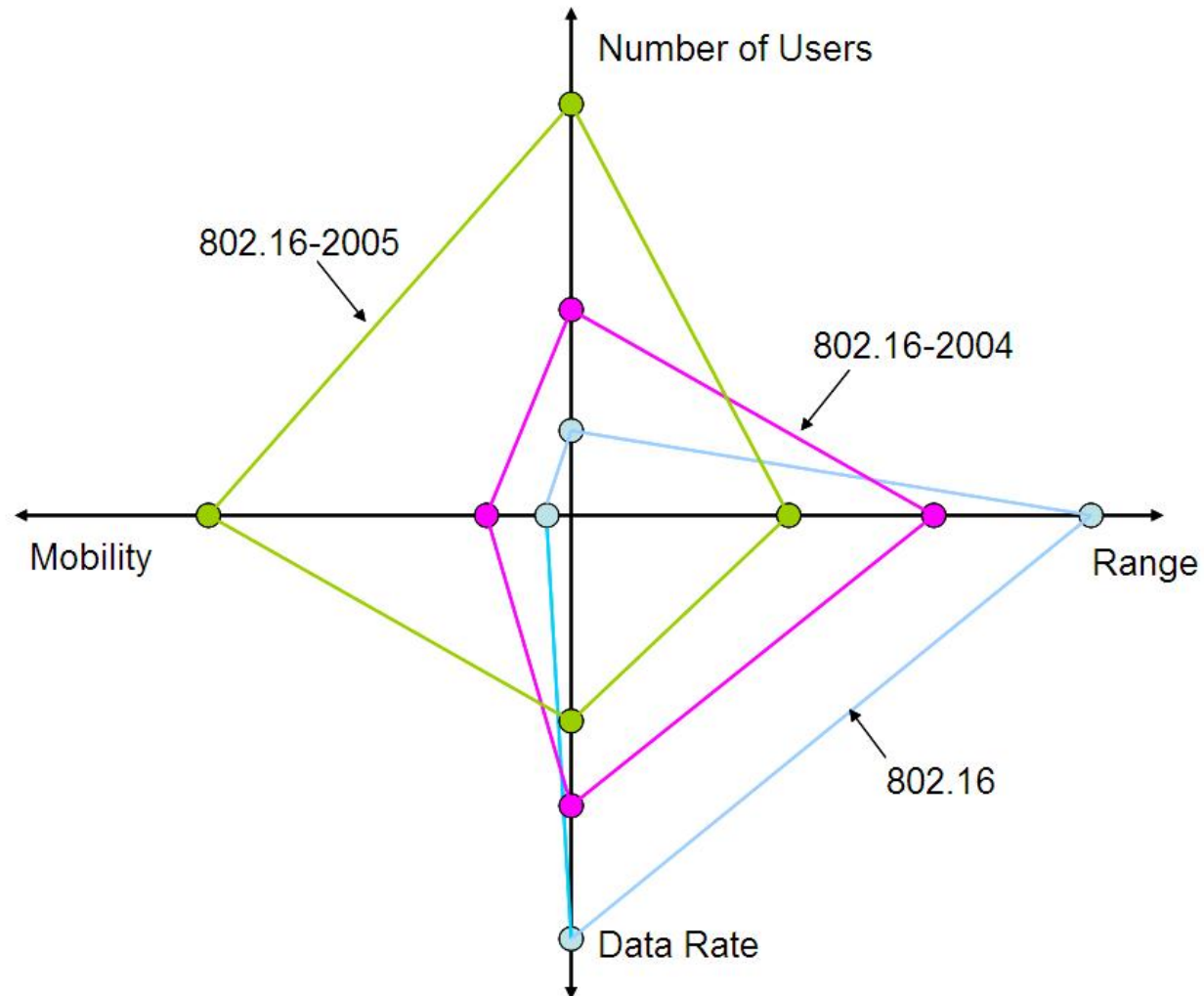
Specification	Year of Ratification	Description
802.16	2001	MAC and PHY definition for fixed broadband wireless access in the 10- to 66-GHz frequency bands
802.16a	2003	Amendment to the original specification; contains new PHY definitions for the 2- to 11-GHz frequency bands. Also includes mesh network modes of operation.
802.16c	2002	System profiles for 10- to 66-GHz operations
802.16d	2004	802.16-2004 is considered the base 802.16 fixed broadband wireless specification. Contains 802.16, 802.16a, and 802.16d (various MAC enhancements).
802.16e	2005	Amendment to the 802.16d specification to provide explicit support for mobility
802.16f	2005	802.16 Management Information Base

- Fixed WiMAX: based on 802.16d
- Mobile WiMAX: 802.16e
- 'Pre-WiMAX': based on 802.16a (or proprietary)
- While 802.16e will provide formal mobility support, there are usage cases of 802.16d (or at least 802.16-like) networks have been used in mobile environments
  - *E.g. communications to passenger trains*
    - *802.16 for off-train communications with 802.11 network service within train*
- 802.16d has also been shown to support 'nomadic mobility'
  - *Equivalent to 'on-the-halt' communications*

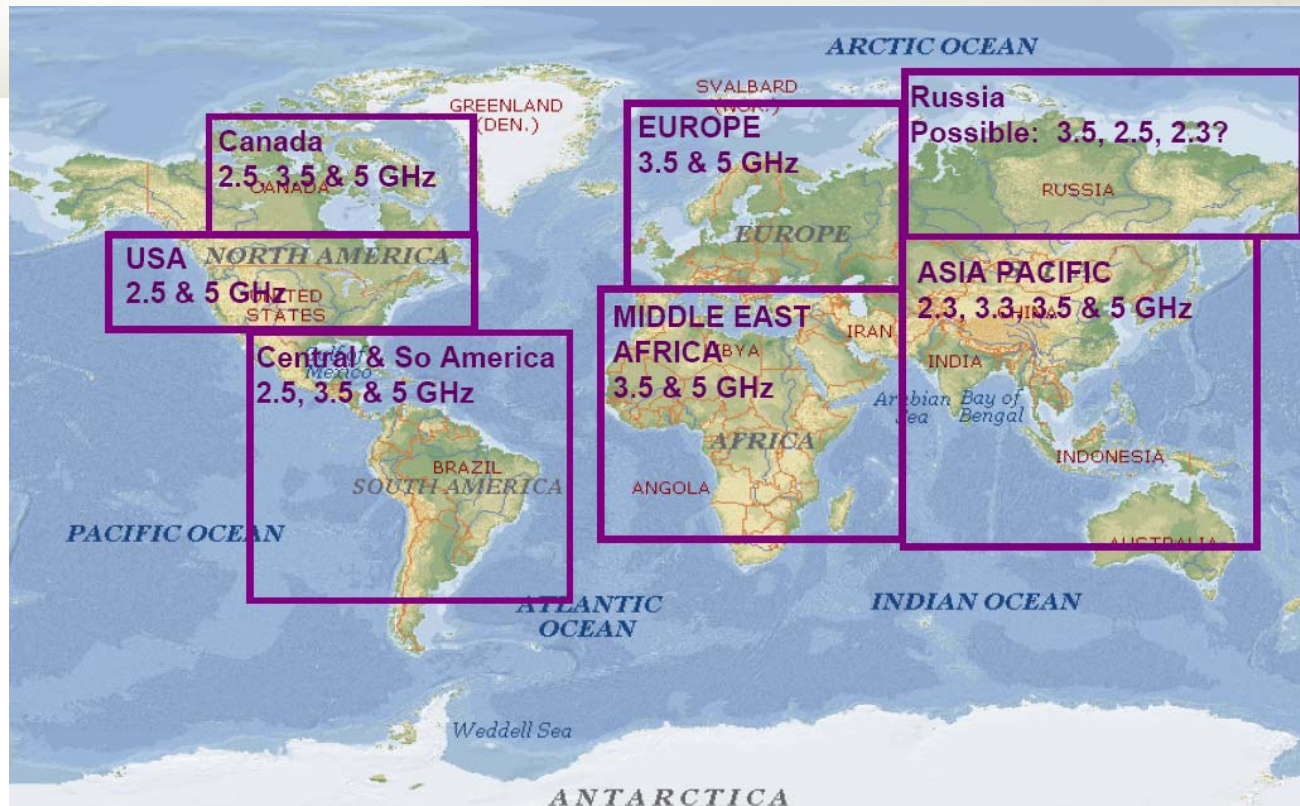
## Other Various 802.16 (and related) Technology Specifications

Specification	Year of Ratification	Description
802.16g	2007	Network management (management plane control procedures)
802.16h	In Progress	Coexistence in license exempt frequency bands
802.16i	Withdrawn	Mobile WiMAX Management Information Base; withdrawn; will be incorporated directly into 802.16-2008.
802.16j	In Progress	Multi-hop Operation
802.16k	In Progress	Bridging Amendment
802.20	In Progress	Mobile broadband wireless access standards group. Initially formed as a study group within the 802.16 Working Group; it consisted of a group of individuals who wished to develop a new technology focused solely on mobility.
WiBRO	N/A	Korean wireless broadband standard that has been incorporated into the 802.16e standard

# The Evolution of WiMAX

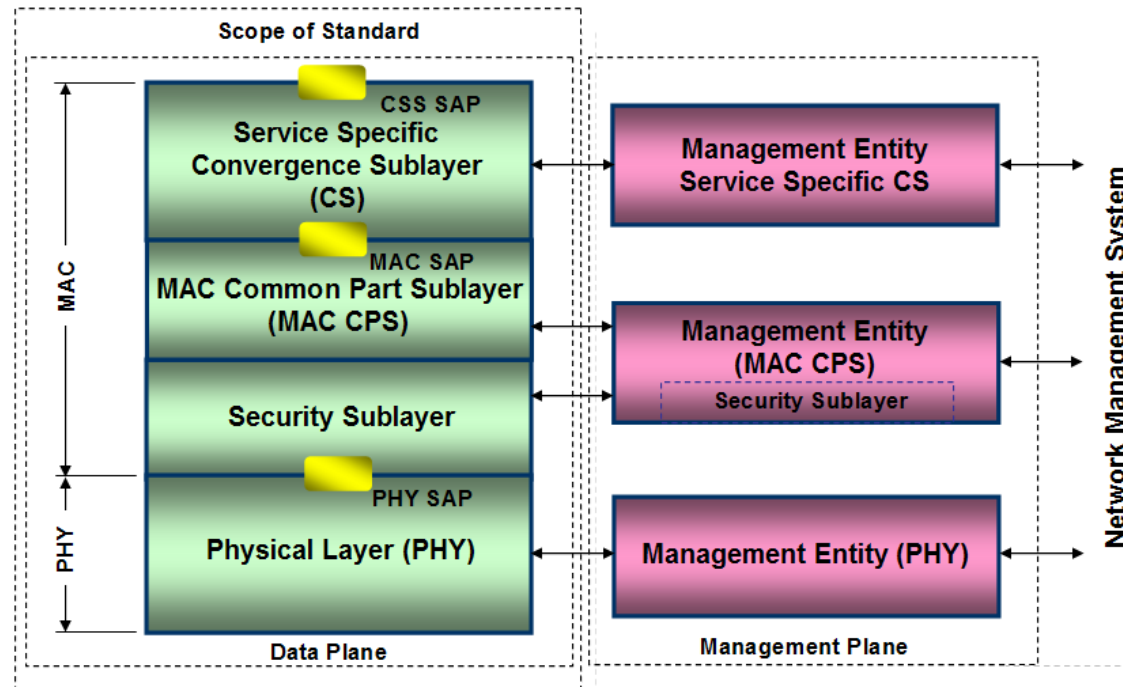


# WiMAX Frequency Bands



- Fixed WiMAX: primarily 3.5 GHz
- Mobile WiMAX: primarily expected to be 2.5 GHz
  - Also 2.3 GHz (WiBro)

# The Logical Architecture of 802.16



- The MAC sub-layer is sub-divided into three sublayers
  - *Convergence sub-layer (CS)*
  - *Common part sub-layer (CPS)*
  - *Security sub-layer*

## The 802.16 Convergence Sub-layer

- The CS aims to enable 802.16 to better accommodate higher-layer protocols placed above the MAC
- 802.16 specification assumes there will be two predominant types of traffic transported across the 802.16 network: ATM and Ethernet
- Consequently, two CS specifications: ATM and packet
- CS receives data frames from higher layer and classifies the frame
  - *Classification is the process by which data received from the higher-layers is associated with a particular connection*
- Based upon classification, CS can perform additional processing, such as Payload Header Compression (PHC)
- The CS is separate from the remainder of the 802.16 MAC so that vendors that wish to support other protocols can develop specialized CSs

## 802.16 Service Flows

- Central to 802.16 is the concept of a service flow, or **connection**
- 802.16 is connection-oriented but not in the traditional meaning of the term
- Traffic flows are all associated with connections
- An SS has (potentially) multiple connections established with the BS, each delineated by a **connection ID (CID)**
  - *Relatively static in nature, and have particular transmission and medium access characteristics associated with them*
  - *CID is 16 bits in length allowing for a total of 64000 connections within each uplink and downlink channel*
    - *However, implementations likely limit this number to hundreds*
- Association of traffic with a CID is a function of the classifier, which is a rule-set within the CS
  - *Can be based on multiple factors, such as priority, source MAC address, and destination MAC address*

## The 802.16 Common Part Sub-layer

- The CPS is the central piece of the 802.16 MAC
- Provided functions
  - *Duplexing*
  - *Network entry and initialization*
  - *Framing*
  - *QoS*
  - *Channel access*
- One of the most common criticisms of 802.16 is the complexity of the MAC (largely the CPS)
- We'll return to the CPS in more detail...

## The 802.16 Security Sub-layer

- Also referred to as the privacy sub-layer
- Two primary goals:
  - *Providing subscribers with privacy across the wireless network*
  - *Providing operators with strong protection from theft of service*
- More on 802.16 security in a bit...



## An 802.16 Wireless Network

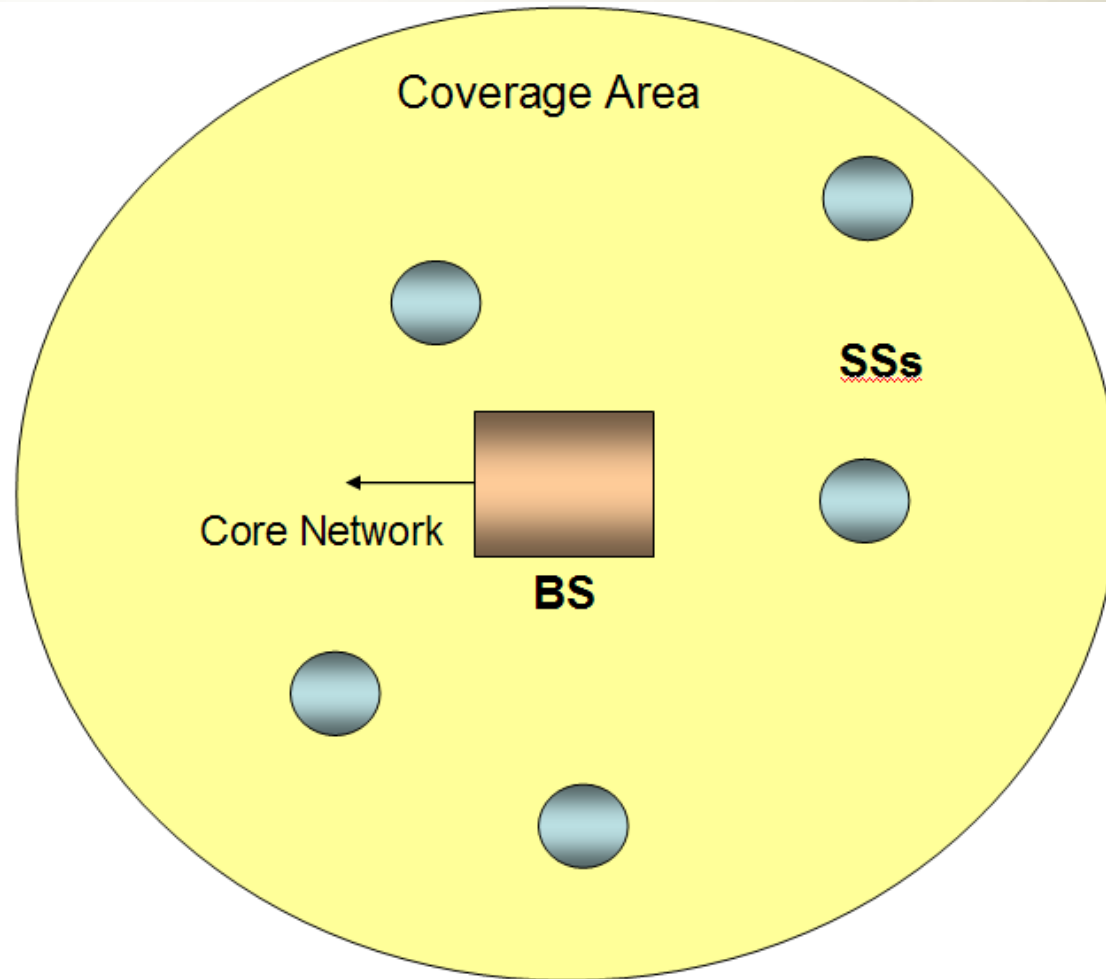
# Components of an 802.16 Network

- Four primary components of an 802.16 network:
  - *Base Stations (BSs)*
    - *Bridge the wireless network to the wired network*
    - *Almost every aspect of the 802.16 network is controlled by the BS*
      - *Highly centralized control and management*
  - *Subscriber Stations (SSs)*
    - *Users of the network*
  - *Core Network*
    - *Method by which multiple BSs are interconnected to increase coverage*
    - *Analogous to DS of 802.11*
  - *Wireless medium*
    - *Channel over which communications occur*

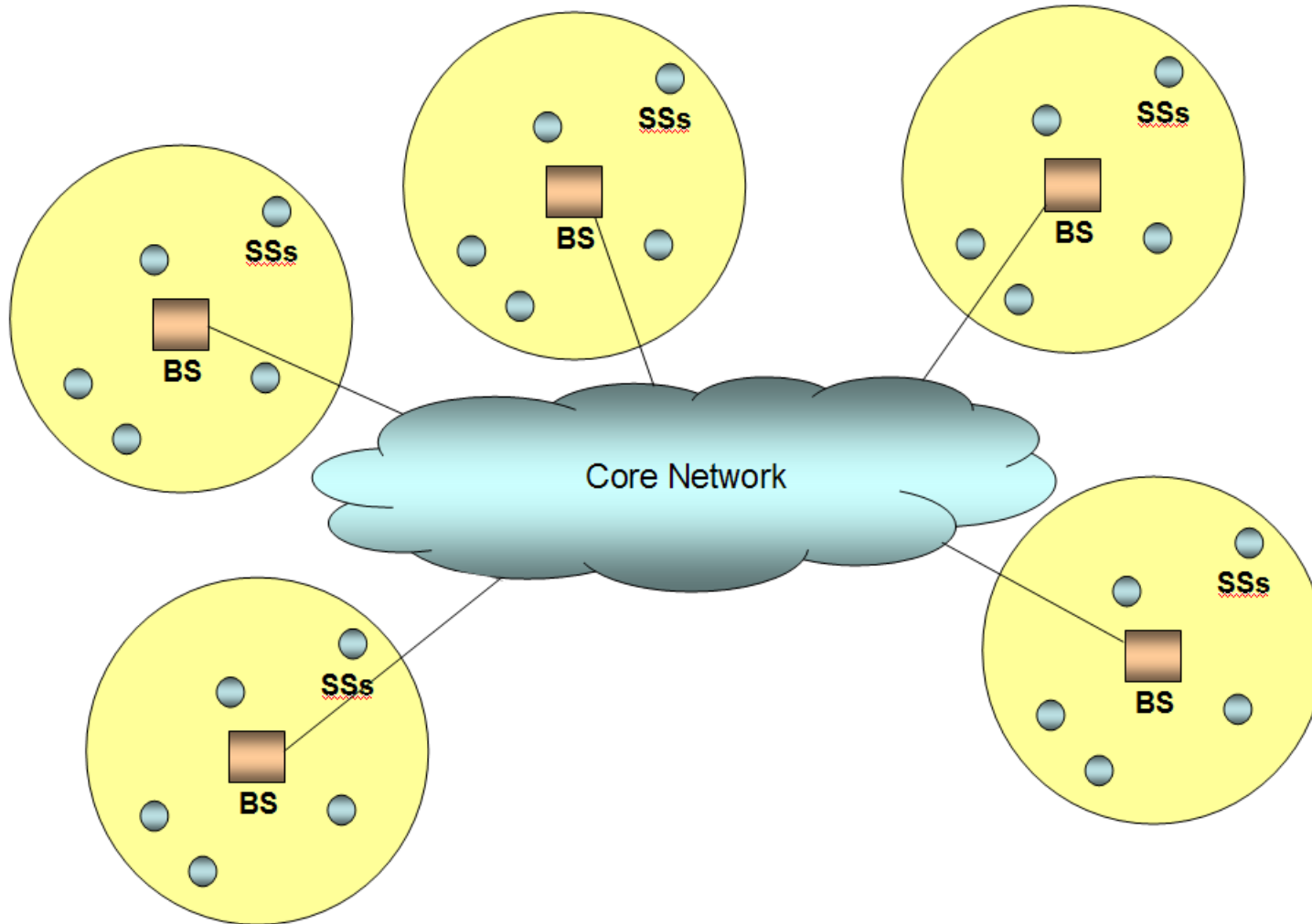
## The 802.16 Network

- An 802.16 coverage area, or 'cell', is the fundamental building block of an 802.16 network
  - *Consists of a single BS and one or more SS*
- Multiple coverage areas can be inter-connected to form a larger network
- Coverage areas are inter-connected through a core network
  - *Core network method is not specified as part of the 802.16 standard(s)*
  
- BS-to-SS link is referred to as the *downlink*
- SS-to-BS link is referred to as the *uplink*

# 802.16 Coverage Area



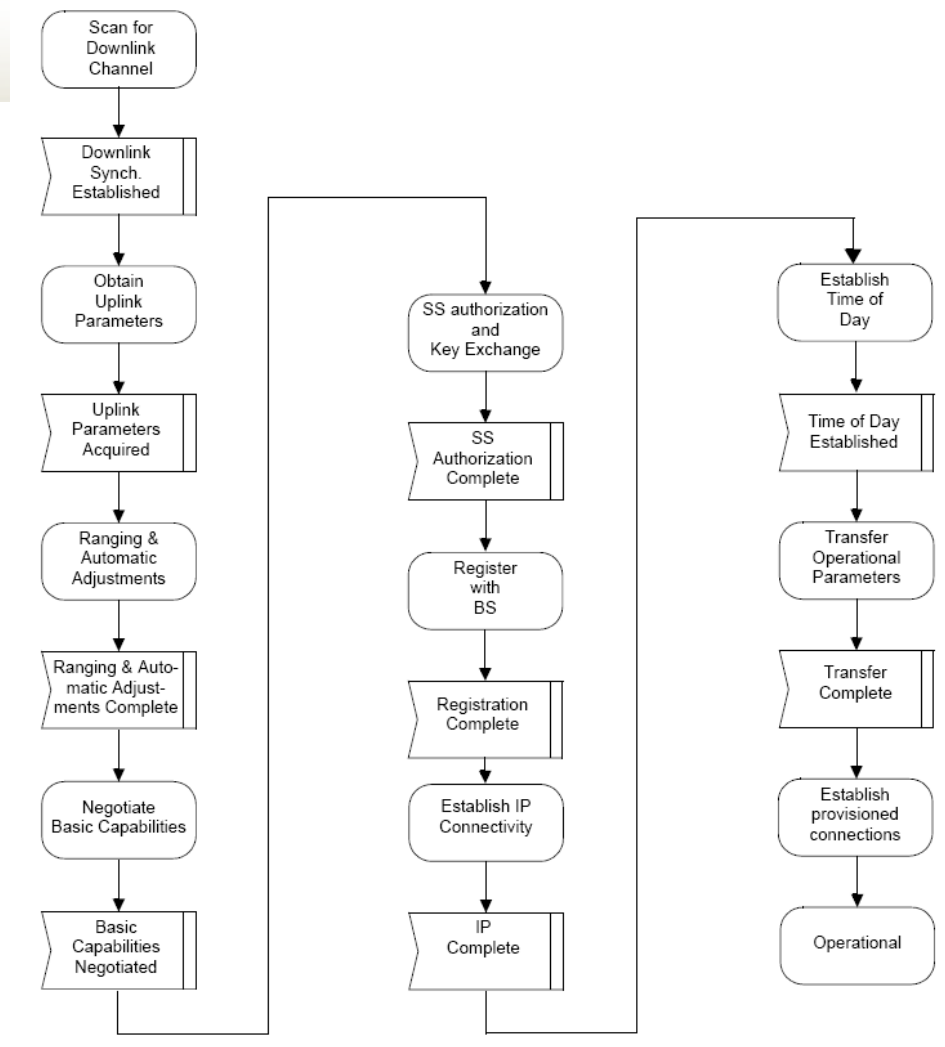
# The 802.16 Network



# Joining the 802.16 Network

- Several steps that must be taken before an SS can join an 802.16 network:
  - *Acquisition of downlink signal*
    - *SS will use last known valid operational parameters*
    - *If not found, the SS will search across all downlink channels*
  - *Obtain uplink parameters from the UL-MAP messages*
  - *The ranging process*
    - *Process that allows stations to calibrate the performance of their PHYs based on current channel conditions*
    - *Optimal power settings, timing and frequency synchronization*
  - *Network entry request*
  - *Authentication and cryptographic key exchange*
  - *Obtain IP configuration via DHCP*
- There is also a sub-channelized network entry procedure that may be used
  - *The SS chooses a particular sub-channel and sends specialized messages to the BS*
  - *In place to mitigate the large contention that can take place for initial ranging and logon*

# Network Entry Process

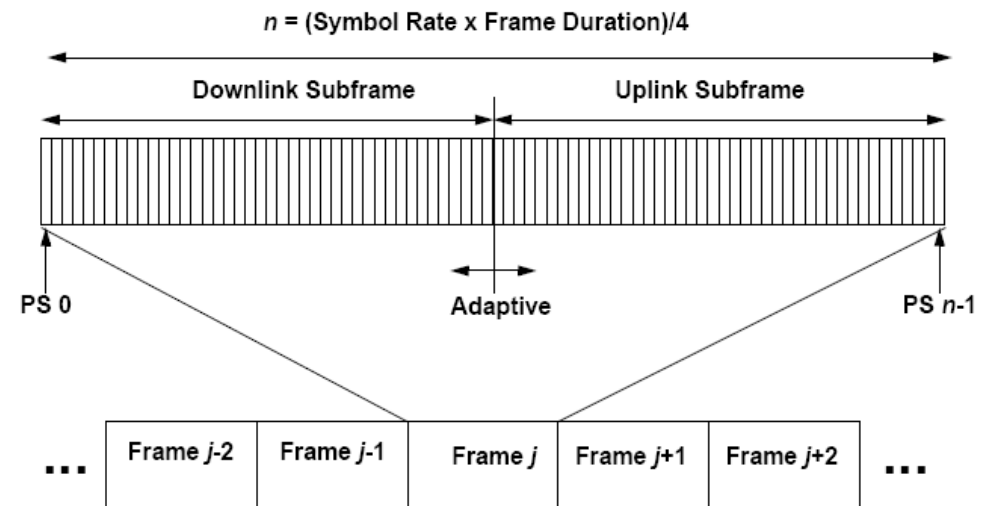


# Duplexing

- Duplexing – how the uplink and downlink channels are separated
- 802.16 provides two methods of duplexing:
  - *Time Division Duplexing (TDD) and Frequency Division Duplexing (FDD)*
- TDD:
  - *Wireless medium is divided in the time domain*
  - *Periods of time are allocated for uplink and downlink communications, respectively*
  - *Occupies only a single frequency channel*
- 802.16-2004 defines a frame to be “A structured data sequence of fixed duration used by some PHY specifications. A frame may contain both an uplink sub-frame and a downlink sub-frame.”
  - *Confused? So is the specification as it uses ‘frame’ to mean multiple things*
  - *We’ll use the terms ‘channel frame’ and data frame.*
    - *Channel frames refer to the logical groupings of TDMA channel timeslots*
    - *Data frame refers to a PDU*

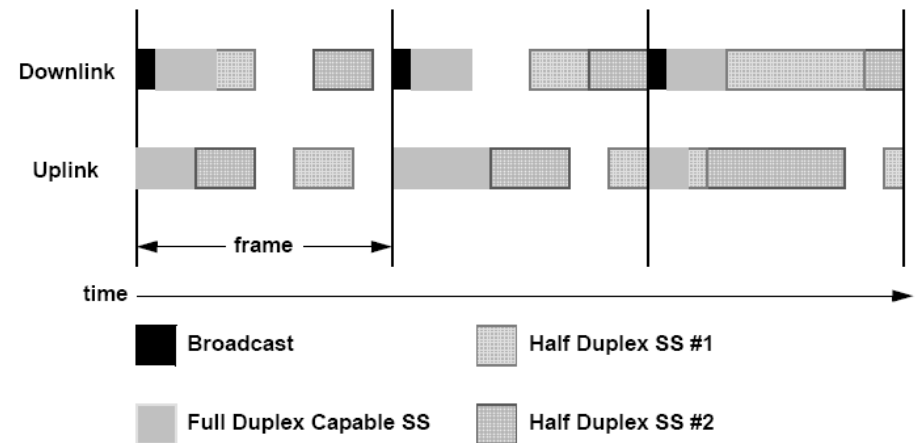
# Time Division Duplexing

- The channel frame is fixed in duration and contains one uplink and one downlink *sub-frame*
- Channel frame is divided into an integer number of timeslots
- The fractional bandwidth provided to the uplink and downlink is controlled by system parameters
- Important note: When TDD is employed, 802.16 is a half-duplex technology

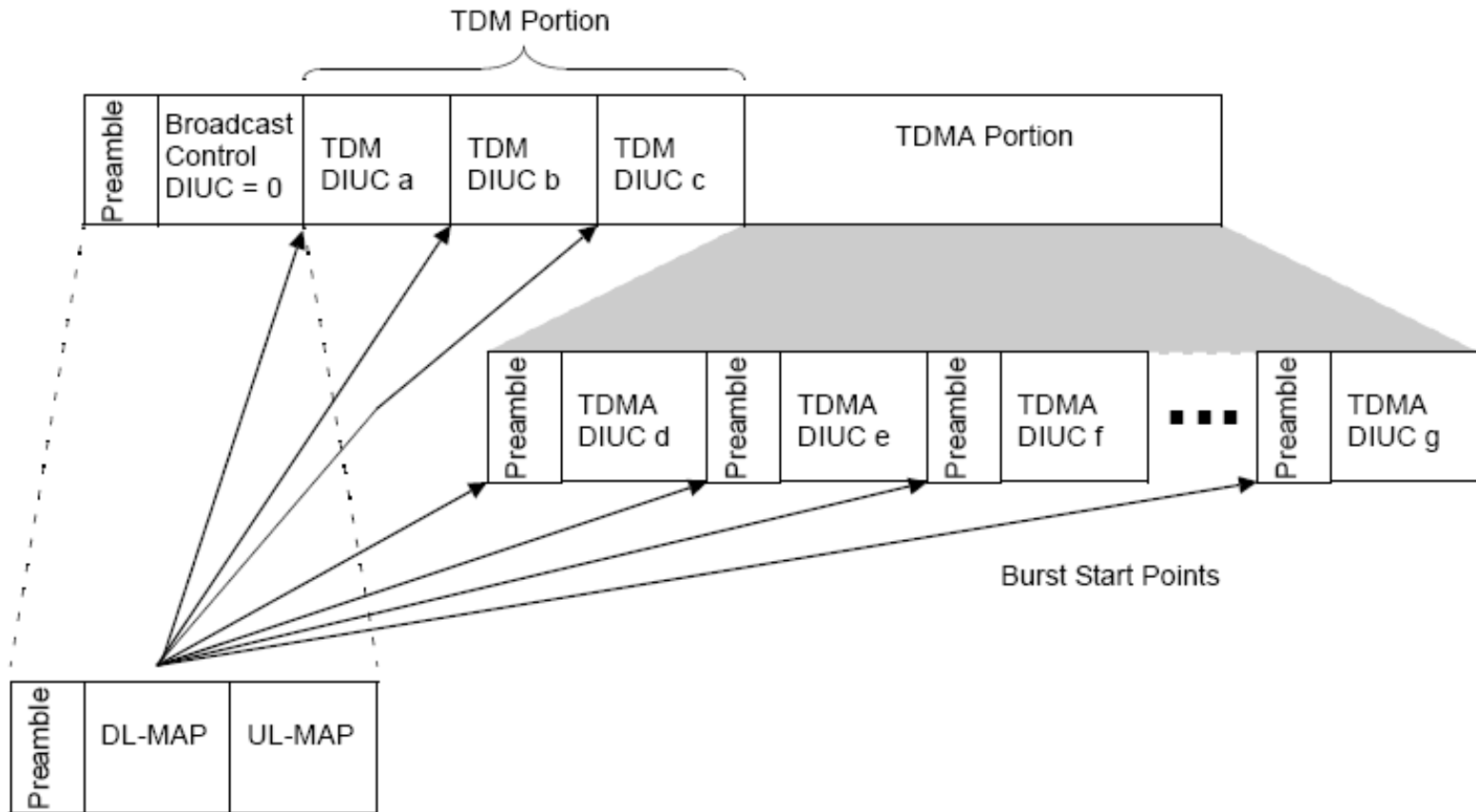


# Frequency Division Duplexing

- In FDD, the uplink and downlink transmissions are separated in frequency
- Since they can overlap in time, when FDD is employed 802.16 is a full-duplex technology
- FDD has disadvantage of having static assignments of uplink and downlink
  - *Making the system somewhat less flexible than TDD*
- FDD also has advantages
  - *Facilitating the use of different modulations on the uplink and downlink*
  - *Support of both full-duplex and half-duplex SSs*

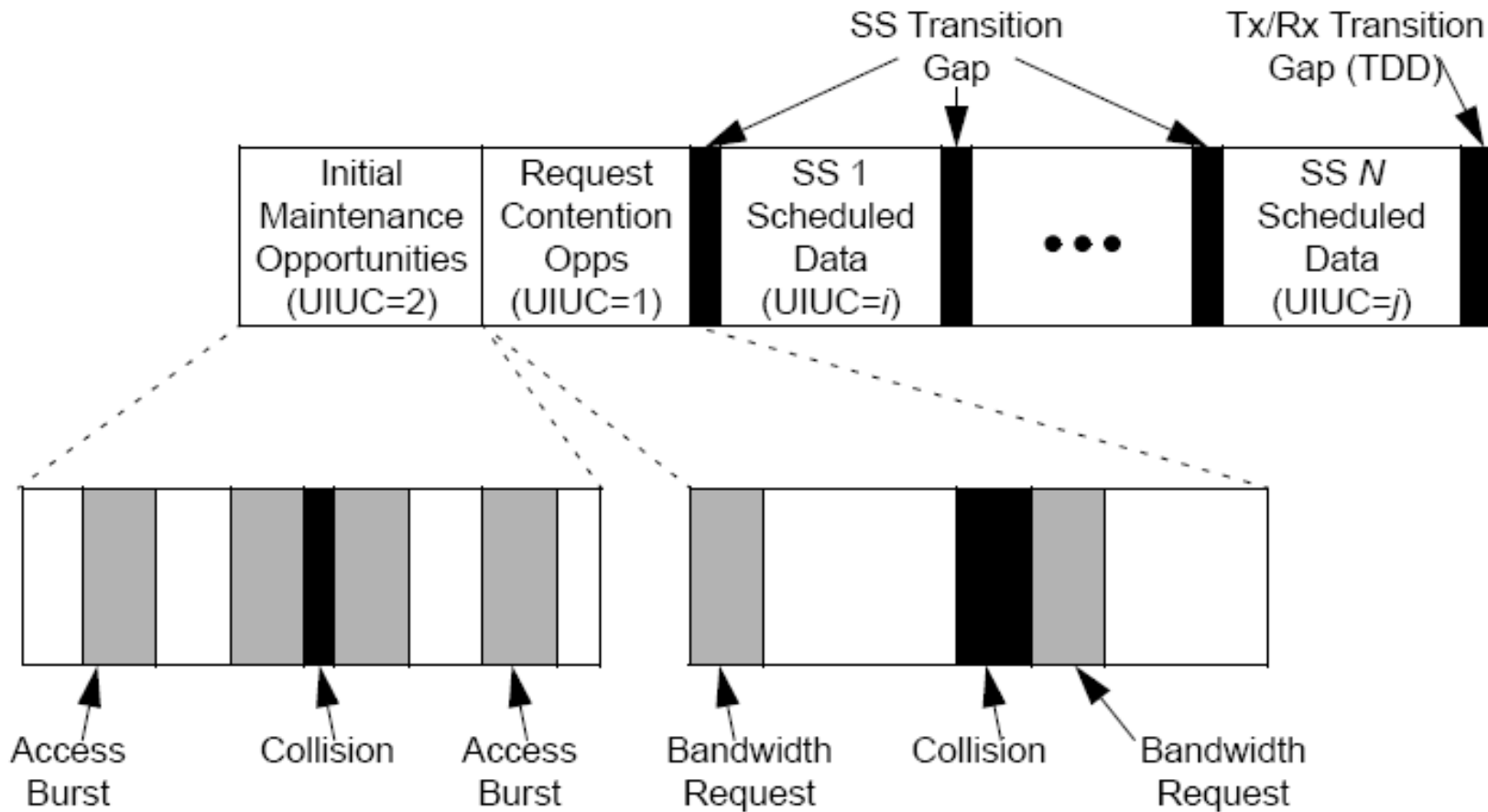


# Channelization and Channel Access – Downlink Sub-Frame Structure



# Channelization and Channel Access

## - Uplink Sub-Frame Structure



# MAPs and Bursts

- Each downlink frame begins with a control message
  - *Informs SSs of the modulation and coding of the various timeslots in the downlink frame*
  - *Referred to as the **downlink map (DL-MAP)***
  - *Required because 802.16 incorporates adaptive control of modulation and coding to accommodate changing channel conditions*
- A **burst** is a unit of data transfer for which the transmission characteristics remain constant
  - **Downlink bursts** *refer to transfers from a BS to a SS*
  - **Uplink bursts** *refer to transfers from a SS to a BS*
- The DL-MAP contains **burst profiles**, which is a set of parameters that describes the transmission properties associated with an **interval usage code (IUC)**
  - *Profile contains parameters such as modulation type, forward error control (FEC) type, preamble length, guard times*
  - *Must be updated every frame, because profiles can be modified on a burst-by-burst basis*

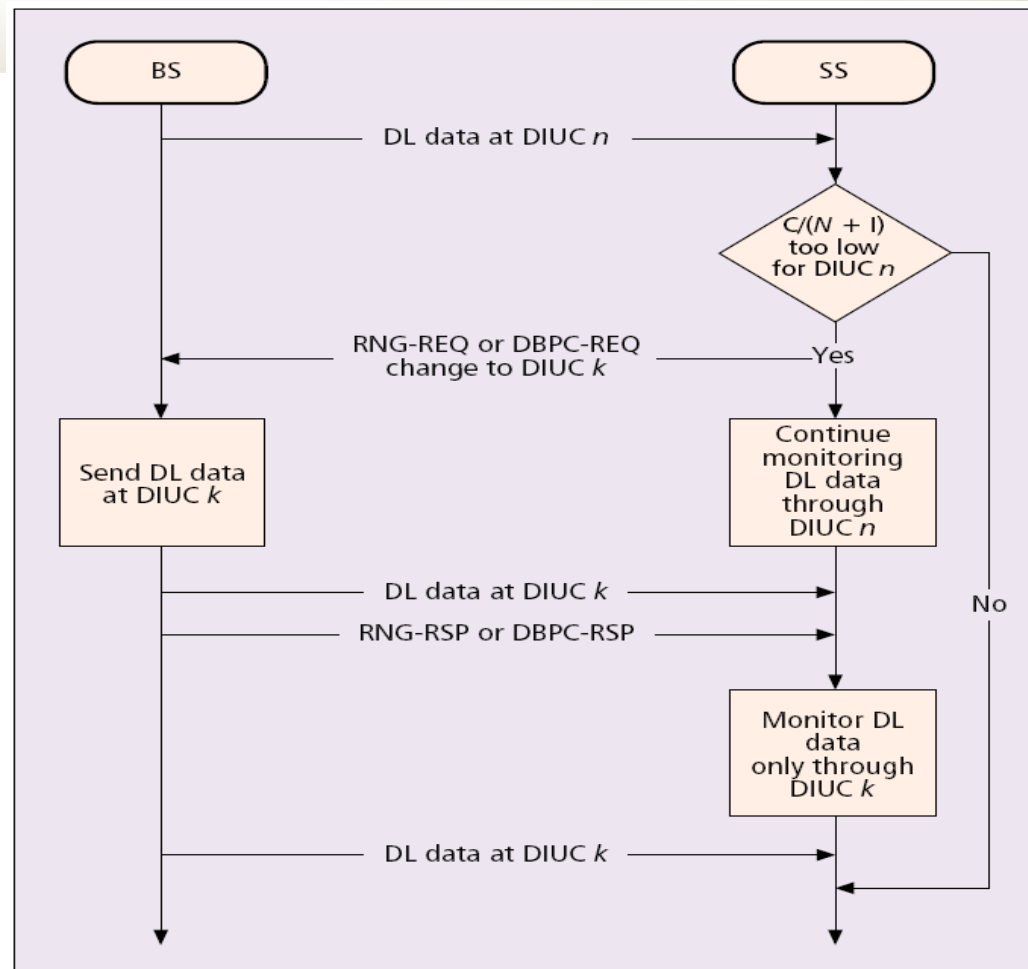
## MAPs and Bursts (continued)

- Downlink burst profiles controlled solely by the BS
  - *Indicated to the SS through **Downlink Interval Usage Codes (DIUCs)***
    - *Fields within Information Elements (IEs) of the DL-MAP*
- An SS can determine the proper communications configuration by mapping the DIUC to locally stored downlink burst profiles
  - *The BS merely informs the SS what burst profile to use for proper reception of data destined for that station*
- Locally-stored burst profiles within the SS can be modified as required through the periodic transmission of **channel descriptor** messages which essentially configure an SS with a set of burst profiles

## MAPs and Bursts (continued)

- Each uplink frame begins with an uplink control message (UL-MAP), which contains uplink burst profile information
- UL-MAP is fundamentally different than the DL-MAP in that it is the mechanism through which bandwidth is allocated to the SS
- UL-MAP informs the SS which timeslots they are allowed to use for that uplink frame
- ***Uplink Interval Usage Codes (UIUCs)*** within the UL-MAP indicates to the SS which uplink burst profiles to use
- The BS is in complete control of this process
- BS may negotiate downlink burst profiles based upon received quality
- But, still ultimately the decision of the BS what transmission characteristics the SS employs

# The Burst Profile Negotiation...



# Bandwidth Negotiation and Allocation

- There are two types of SSs
  - *Those that can accept bandwidth allocations on a grant per connection (GPC) basis*
  - *Those that can accept bandwidth allocations on a grant per SS (GPSS) basis*
- GPSS type of SS is responsible for managing bandwidth allocations to its various data flows
  - *Allows for increased flexibility by allowing the SS to ‘steal bandwidth’ from connections to augment other connections as necessary*
  - *Also ties bandwidth allocation to a priority queuing scheme*
  - *Can request aggregate bandwidth as required from the BS, and then manage the particular data flows independent of the BS*
- In the GPC case, performance a particular data flow experiences is largely independent of the SS
- GPSS generally outperforms GPC
- GPC SSs are less complex

## Bandwidth Negotiation and Allocation (continued)

- SSs typically request bandwidth incrementally as capacity requirements change over time
- However, SSs can request aggregate bandwidths from the BS so that the BS has a better idea of the actual bandwidth needs of the SS
- Bandwidth requests can be made by SS through two methods
  - *Requests during bandwidth request periods dedicated to the SS*
  - *Requests during contention periods*
- Method is determined by the BS
  - *Dictated by the time period in which the BS sends the polling message indicating the upcoming bandwidth request period*

## Quality of Service in 802.16

- QoS support provided through the concept of *service classes*
- Service flow properties are grouped into named service classes (globally well known)
  - *Upper-layer entities can request service flows with desired QoS parameters*
- Requests from higher layers for a particular type of service flow communicates a variety of performance requirements to the system
- QoS parameters considered within 802.16 standard include priority, minimum traffic rate, maximum sustained traffic rate, maximum traffic burst, maximum latency, and maximum tolerable jitter
- QoS parameters are used to influence a variety of system attributes
  - *MAC scheduling functions, bandwidth requests and allocations, and burst profiles*
  - *Influence is both on uplink and downlink*
- Special signaling mechanisms provided in the standard such that QoS-enabled service flows can be dynamically established as required
  - *Used to inform 802.16 the level of service required, which will influence the treatment of that service flow*

## 802.16 Security

- Security provided by the security sub-layer
  - *Also referred to as the privacy sub-layer*
- Privacy provided by encryption of the link between the BS and SS
- Service flows are encrypted within the entire network
- IEEE 802.16 privacy protocol based on the Privacy Key Management (PKM) protocol of the DOCSIS BPI+ specification
  - *However, enhanced to support Advanced Encryption Standard (AES)*
- PKM is based on the concept of security associations (SAs)
  - *Every SS establishes at least one SA during initialization*
  - *Every connection is mapped to an SA, either at setup time or dynamically during operation*
- PKM protocol uses X.509 digital certificates with RSA public key encryption for SS authentication and authorization key exchange
  - *Each SS contains a manufacturer-issued and factory-installed X.509 digital certificate*
  - *Certificates link the 48-bit MAC address of the SS and its public RSA key*

## 802.16 Security (continued)

- Certificates sent to the BS by the SS in authorization request and authentication information messages
- BS verifies the identify of the SS by checking the certificate via database lookup
  - *Also uses this credential to lookup the authorization level of the SS*
- If SS is authorized to join the network, the BS will transmit an Authorization Key (AK) encrypted with the SS's public key
- Traffic encryption employs DES in CBC mode with mandatory 56-bit keys
- Initialization vector is dependent upon frame counter (i.e. differs from frame to frame)
- Traffic Encryption Keys (TEKs) are exchanged using 3-DES with a key exchange key (KEK) derived from the authorization key
- PKM messages are authenticated using the Hashed Message Authentication Code (HMAC) protocol with SHA-1

## 802.16 Physical Layer

### ■ WiMAN-SC2

- *Primary air interface for Pre-WiMAX*
- *Channel bandwidths of 20-25 MHz in US, 28 MHz in Europe*
- *QPSK, 16-QAM, 64 QAM modulation*

### ■ WiMAN-OFDM

- *Primary air interface for Fixed WiMAX*
- *256-pt FFT OFDM*
- *Channel bandwidths: multiples of 1.25, 1.5, 1.75, 2.0 MHz*
  - *Fixed WiMAX: 3.5 MHz, 5 MHz, 7 MHz, 10 MHz*
- *BPSK, QPSK, 16-QAM, 64-QAM*
- *FEC: Reed-Solomon (outer) with convolutional (inner)*
  - *Overall coding rates:  $\frac{1}{2}$ ,  $\frac{2}{3}$ ,  $\frac{3}{4}$*
  - *Optional turbo coding (puncturing to achieve code rate targets) but not widely implemented*
- *TDMA channel access with frame durations of 2.5-20 ms*

Of Primary Interest –  
what People are Implementing  
and Deploying

### ■ WiMAN-OFDMA

- *Optional – not implemented in most current products*
- *Similar to primary air interface of Mobile WiMAX*
- *Multiple access provided by dynamic assignment of subset of OFDM sub-carriers to individual receivers*

## 2-11 WiMAN-OFDM Air Interface: Key Parameters

Channel bandwidth $BW$ <sup>1)</sup>	1.25 MHz to 28 MHz
Sampling frequency $F_s$ <sup>1)</sup>	1.72 MHz to 32 MHz
Sampling factor $n$	$8/7, 88/75, 144/125$ ( $316/275, 57/50$ )
FFT size $N_{FFT}$	256
Subcarrier spacing $\Delta f$	$F_s / N_{FFT}$
Useful symbol time $T_b$	$1 / \Delta f$
Cyclic prefix (CP) time $T_g$	$G \cdot T_b$
Guard period ratio $G$	$3/4, 1/8, 1/16, 1/32$
OFDM symbol time $T_s$	$T_b + T_g$
Number of used subcarriers $N_{used}$	200
Pilot carriers	8 (fixed location <sup>2)</sup> )
Guard subcarriers $N_{Guard, left} / N_{Guard, right}$	28 left, 27 right

1) Discrete values

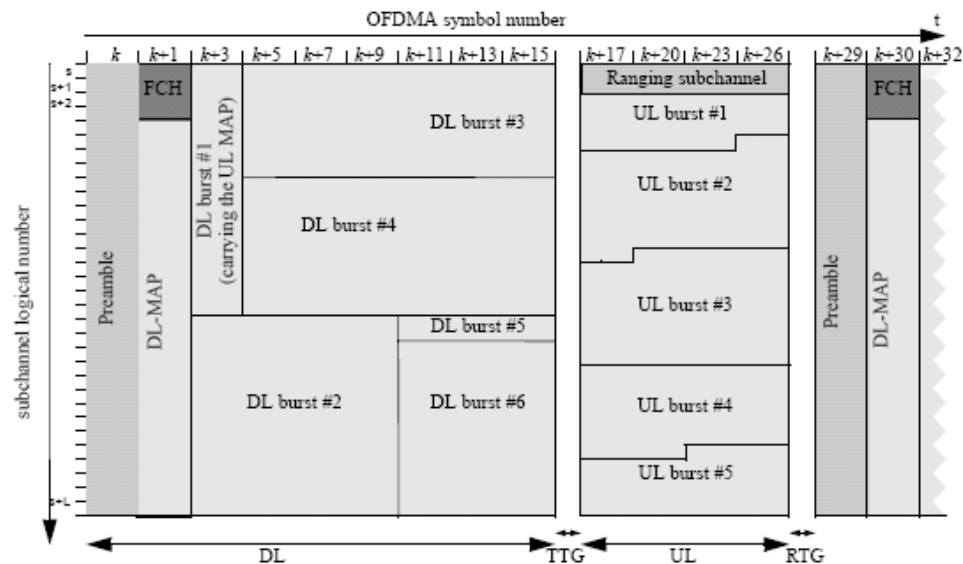
2)  $\pm 13, \pm 38, \pm 63, \pm 88$  – see also [1], Table 213

## IEEE 802.16e – Mobile WiMAX

- New Orthogonal Frequency Division Multiple Access (OFDMA) PHY
- Advanced Antenna System (AAS) support
- New Forward Error Control (FEC)
- Hybrid Automatic Repeat Request (H-ARQ)
- Handover support (in the form of new MAC message types)
- New security mechanisms
- New optional MAC messages
- New bandwidth request mechanisms
- Modified bandwidth allocation mechanisms
- New device types and characteristics
- Dwindling role of Frequency Division Duplexing (FDD)
- Sleep modes

# Mobile WiMAX - OFDMA

- Fixed WiMAX:** bandwidth is allocated in terms of time. A subscriber is allowed to utilize the channel for a given period of time, as defined by a number of OFDM symbols.
- Mobile WiMAX:** bandwidth is allocated in terms of time and frequency. A subscriber is allowed to utilize the channel for a given period of time, as defined by a number of OFDM symbols, and for a given set of frequencies, as defined by a set of OFDM subcarriers.





# WiMAX – An Overview of the Marketplace

## The Current WiMAX Market

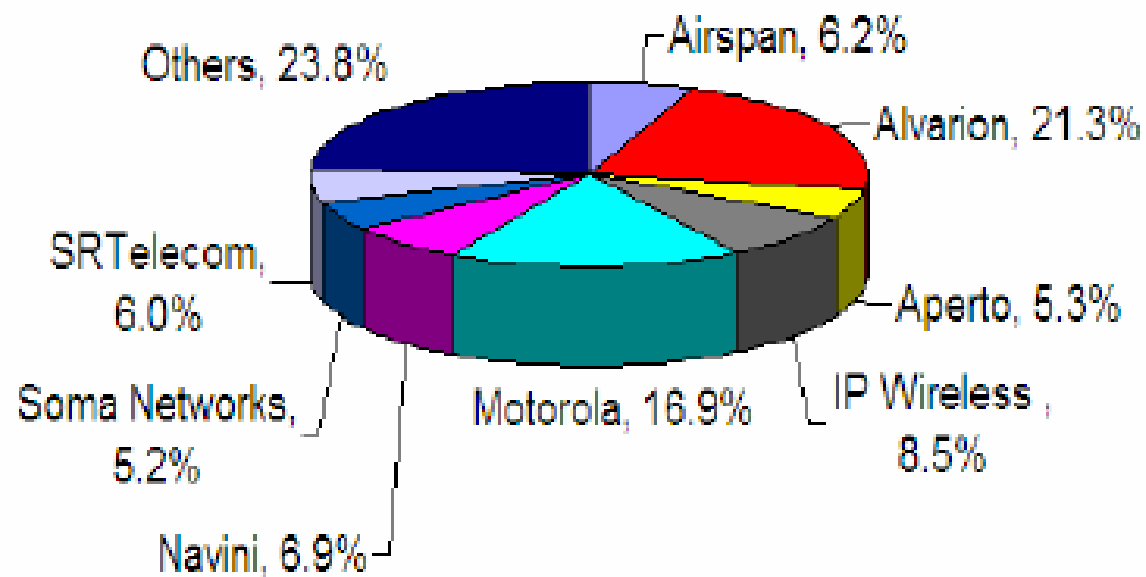
- There are a multitude of products on the market that are advertised as 802.16 or WiMAX products
- Note: there are currently a limited number of WiMAX (or guaranteed 802.16) products currently available on the market
  - *WiMAX Forum issued first certifications just in 2006 for fixed equipment at 3.5 GHz*
  - *Certifications in other frequency bands yet to emerge*
- Market relatively immature, small market penetration
  - *About 1 million subscribers worldwide*
- Costs still relatively high (\$200-\$500 per subscriber)
- SWaP profiles still large (WiMAX subscribers larger than most WiFi APs)
- Lack of testing and analysis tools

## WiMAX-Certified Products (as of May 2007)

	Vendor	Base Station	CPE	Profile
1	Airspan	MacroMAX Macro Modular Base Station	EasyST and ProST	3.5GHz 3.5MHz (FDD)
2	Alvarion	and MicroBS	BreezeMAX PRO CPE and Si	3.5GHz 3.5MHz (FDD)
3	Aperto Networks	PacketMAX 5000	PacketMAX 100 and 300	3.5GHz 3.5MHz TDD
4	Axxcelera	ExcelMax BS	ExcelMAX Full Duplex CPE	3.5 GHz-3.5 MHz FDD
5	Proxim	Tsunami MP16 3500		3.5GHz, 3.5MHz, TDD
6	Redline Communications	RedMAX AN-100U	RedMAX SS	3.5GHz 3.5MHz TDD
7	Sequans Communications	SQN2010-RD	SQN 1010-RD (FDD)	3.5 GHz - 3.5MHz FDD and TDD
8	Selex Communications	YSEMAX	WRY035-C	3.5GHz TDD 3.5MHz
9	Siemens	WayMAX@vantage	Gigaset SE461 WiMAX	3.5GHz-3.5 MHz H-FDD
10	SR Telecom	Symmetry BS	SSU5000 Symmetry SS	3.5 GHz 3.5 MHz, FDD
11	Telsima	StarMAX 4120	StarMAX 2140	3.5GHz-3.5MHz TDD
12	Wavesat		Wavesat miniMAX 3.5GHz	3.5GHz 3.5MHz TDD and FDD

# WiMAX Market Breakdown (2006)

## 2006 Expected Market Share Breakdown

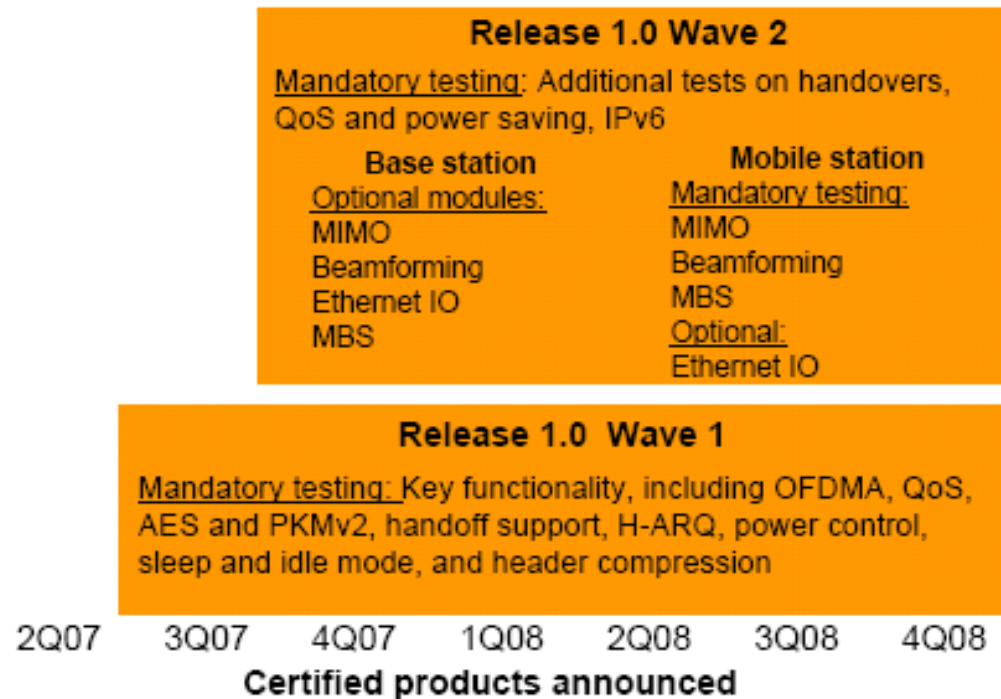
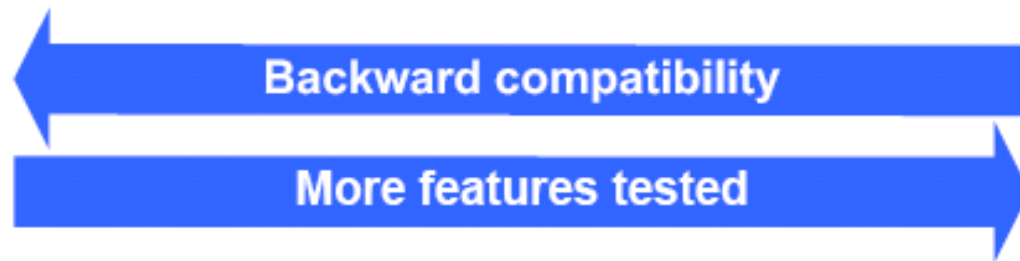


# Mobile WiMAX Certification

- All certifications to date have been Fixed WiMAX
- Mobile WiMAX certifications to begin later in 2007
  - *Schedule almost assured to slip well into 2008 given previous track record and requirements of testing*
- Mobile WiMAX certifications in two ‘waves’
  - *Wave 1: Bandclass 1.A*
    - *2.3 GHz, TDD, 8.75 MHz channel (WiBro)*
  - *Wave 2: Bandclass 3.A*
    - *2.496-2.69 GHz, TDD, 5, 10 MHz channels*
    - *Sprint, Clearwire strong proponents of this profile*

Band Class		1	2	3	4	5		
Frequency Range [GHz]		2.3-2.4	2.305-2.320 2.345-2.360	2.496-2.690	3.3-3.4	3.4-3.8	3.4-3.6	3.6-3.8
Duplex		TDD	TDD	TDD	TDD	TDD	TDD	TDD
Channel Bandwidth [MHz]	3.5 MHz							
	5 MHz		2.A	3.A	4.A	5.A	5L.A	5H.A
	7 MHz					5.B	5L.B	5H.B
	8.75 MHz	1.A						
	10 MHz			3.A				

# Mobile WiMAX Certification



# How Big Will WiMAX Be? - Issues Surrounding WiMAX

- Significant hype will likely result in short-term success
  - *Particularly in Greenfield scenarios and developing regions*
- Longer-term is cloudy for numerous reasons
  - *Lack of a common global frequency*
    - *Multi-mode devices keep costs higher*
  - *Lack of mobility at 3.5 GHz*
    - *License holders prevented from providing mobile services*
  - *Poor coexistence of FDD and TDD*
    - *Greatly complicates network planning*
    - *Complicates Fixed to Mobile migration*
  - *Poor ability to migrate from Fixed to Mobile WiMAX*
    - *Fixed and Mobile WiMAX do not interoperate*
    - *CPEs generally not software upgradeable*
  - *Fixed WiMAX vs. Mobile WiMAX*
    - *A service provider must choose, likely can't do both*

# How Big Will WiMAX Be? - Issues Surrounding WiMAX

- Lack of unlicensed Mobile WiMAX
  - *A key to WiFi success is unlicensed nature of technology*
    - *Facilitated growth of technology as commodity*
    - *Not much opportunity for service provider, but great for equipment vendors*
  - *Missing out on a potentially large market here*
- Lack of concrete differentiators
  - *Hype built mostly on marketing*
  - *Proponents point to the many innovative technologies incorporated within WiMAX*
    - *MIMO*
    - *H-ARQ*
    - *OFDMA*
  - *However, even proponents cannot clearly differentiate themselves from cellular competitors in terms of performance or capabilities*
    - *The biggest selling point is the promise of lower cost*

# How Big Will WiMAX Be?

## Advantages of WiMAX

- Industry support
  - *A lot of key companies really, really want WiMAX to succeed*
- Potential no-cost CPE in future
  - *A no-cost CPE is an enormous advantage*
    - *A big reason for the success of WiFi*

# How Big Will WiMAX Be? Final Analysis

- Envisioned timeline:
  - 1-3 years – *Fixed WiMAX deployments continue to grow rapidly worldwide, mostly in developing and undeveloped regions. Small-scale Mobile WiMAX deployments (region-specific trials) in developed markets (e.g. United States, Europe).*
  - 3-5 years – *Moderate Fixed WiMAX deployments, most likely infrastructural or fixed wireless local loop type of deployments. Large-scale Mobile WiMAX deployments in undeveloped and developing regions, continued small-scale deployment in developing*
  - 5+ years – *Emergence of next-generation WiMAX (based on upcoming 802.16m) deployments begin, real competition to incumbent cellular providers*
    - *Real question that will impact long-term deployment scale: Will Mobile WiMAX be deployed in large numbers before LTE solutions become available*



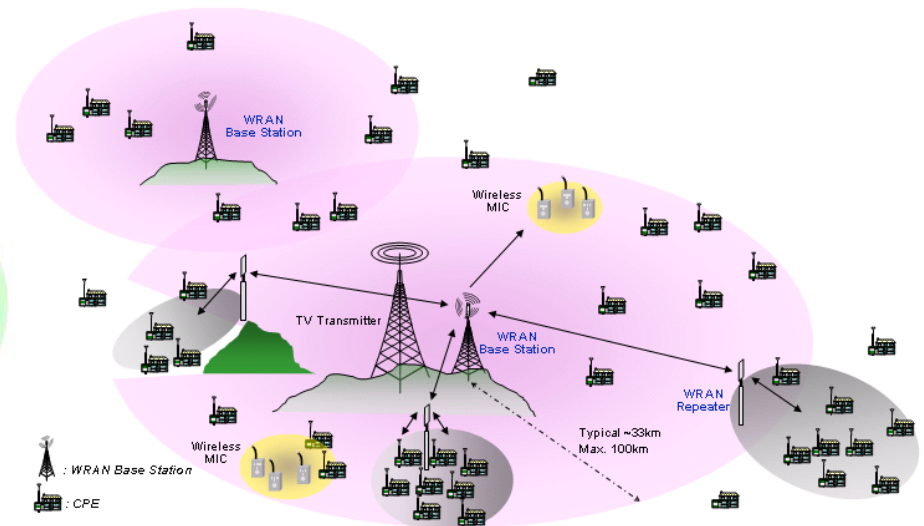
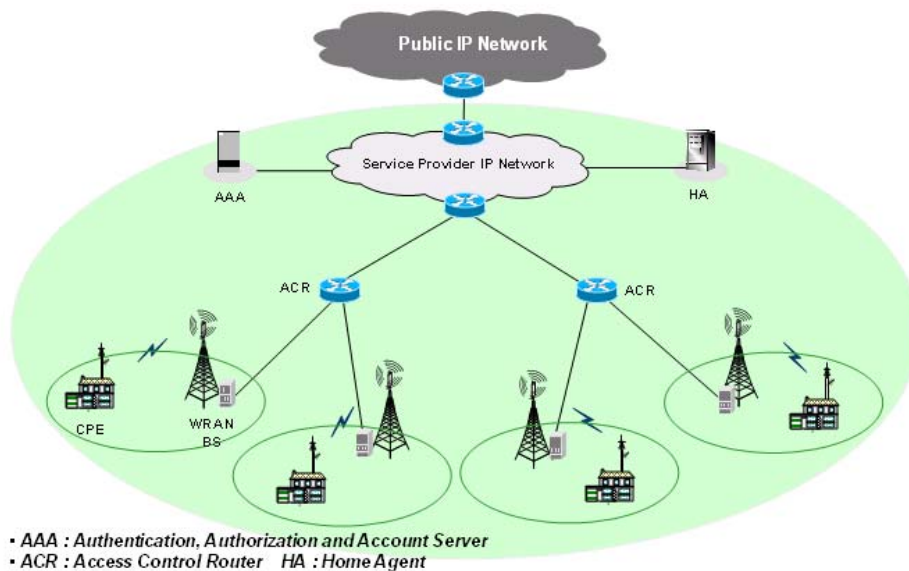
# 802.22: Cognitive Radio

# Cognitive Radio Background

- Ever increasing demand for increasing wireless capabilities has led to shortage of RF spectrum
- Problem is exacerbated by the way in which spectrum is managed
  - *Spectrum allocated for particular types of services*
  - *Licenses for usage are static in nature*
  - *Result is that spectrum is unavailable for use even if it is not used by license holder*
  - *Has led to considerable inefficiency in spectrum utilization and created an under-supply of spectrum*
- Issue temporarily alleviated with unlicensed spectrum usage
  - *Spectral congestion in these bands*
- This has led to the concept of cognitive radio

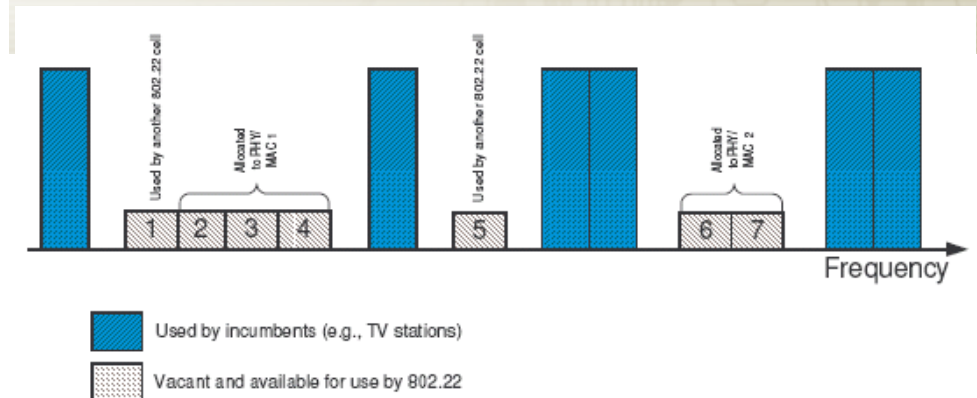
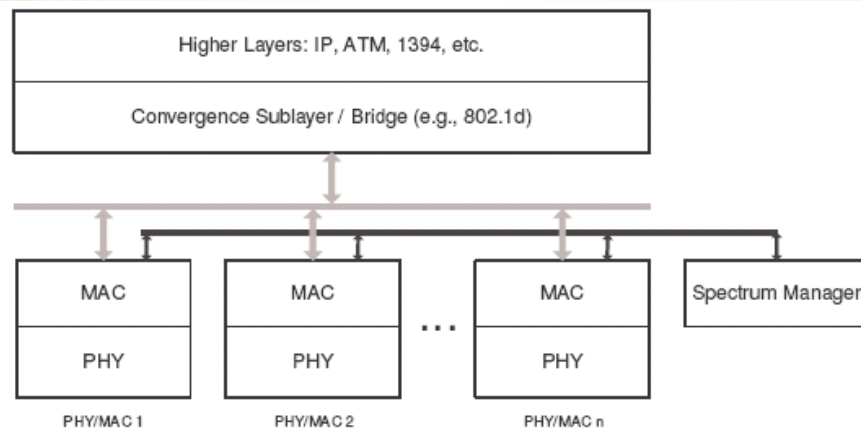
# IEEE 802.22

- IEEE 802.22 WG will specify the air interface, including MAC and PHY, of fixed point-to-multipoint wireless regional area networks (WRANs) operating in the VHR and UHF TV broadcast bands from 54 MHz to 862 MHz
- Utilize spectral white space found in many regions by providing access to these frequency bands on an unlicensed basis
- Fundamental tenant is protection of incumbents
  - *Secondary users operate strictly on a non-interference basis*



\*Images taken from Reference 23

# IEEE 802.22 Overview



- 802.22 network node maintains awareness of environment to determine presence of incumbents
- Chooses unused spectrum so that impact to incumbent users are minimized
- Evacuation of spectrum if incumbent user comes online

# IEEE 802.22 PHY

Parameters	Specification	Remark
Frequency range	54~862 MHz	
Service coverage	Typical range 33 km	
Bandwidth	Mandatory: 6, 7, 8 MHz	Optional fractional use of TV channel and channel bonding up to 3 contiguous TV channels. Channel aggregation of non-contiguous channels.
Data rate	Maximum: 72.6 Mbps Minimum: 4.8 Mbps	Maximum of 23 Mbps for 6 MHz
Spectral Efficiency	Maximum: 4.03 bits/s/Hz Minimum: 0.81 bits/s/Hz	Single TV channel BW of 6 MHz
Modulation	QPSK, 16QAM, 64QAM mandatory	
Transmit power	Default 4W EIRP	
Multiple Access	Adaptive OFDMA	Partial bandwidth allocation
FFT Mode	2K mandatory	1K / 4K optional, 2K / 4K / 6K for channel bonding
Cyclic Prefix Mode	$\frac{1}{4}$ , $\frac{1}{8}$ , $\frac{1}{16}$ , $\frac{1}{32}$	
Duplex	TDD mandatory	FDD supported
Network topology	Point-to-Multipoint Network	



## Other Technologies Not Discussed Here

## Other Technologies not discussed here...

- IEEE 802.20
  - *Not-so-distant cousin of 802.16*
  - *Still emerging, standardization efforts have been plagued with problems*
- ETSI HIPERMAN, HIPERLAN, HIPERLAN\2, HIPERPAN
  - *Often considered technological superior to IEEE solutions, few implementations*
- Cellular communications
  - *Very important in commercial landscape*
  - *Not covered here for sake of time, but important nonetheless...*



# Wireless Networking at the Network Layer

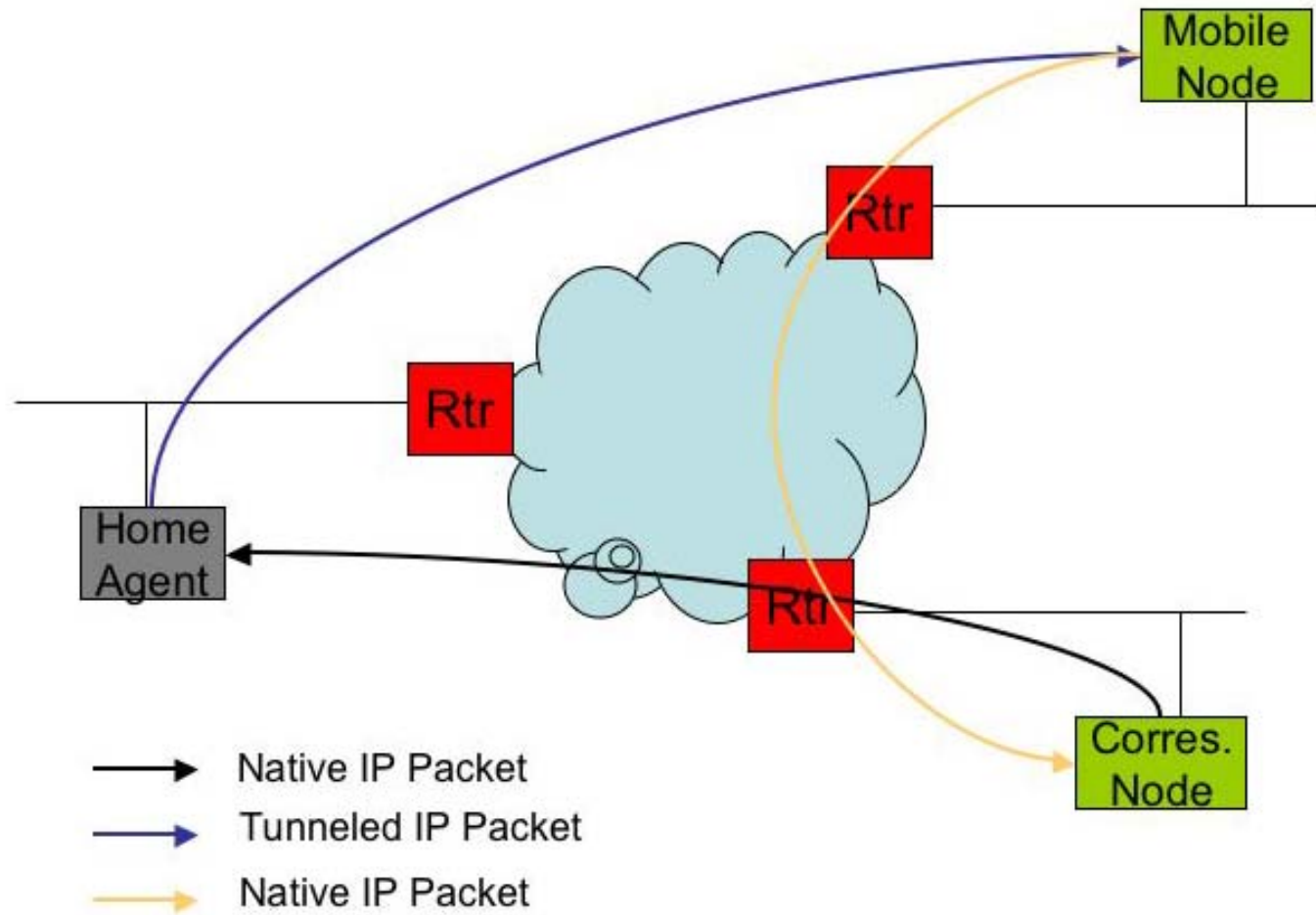


# Mobile IP

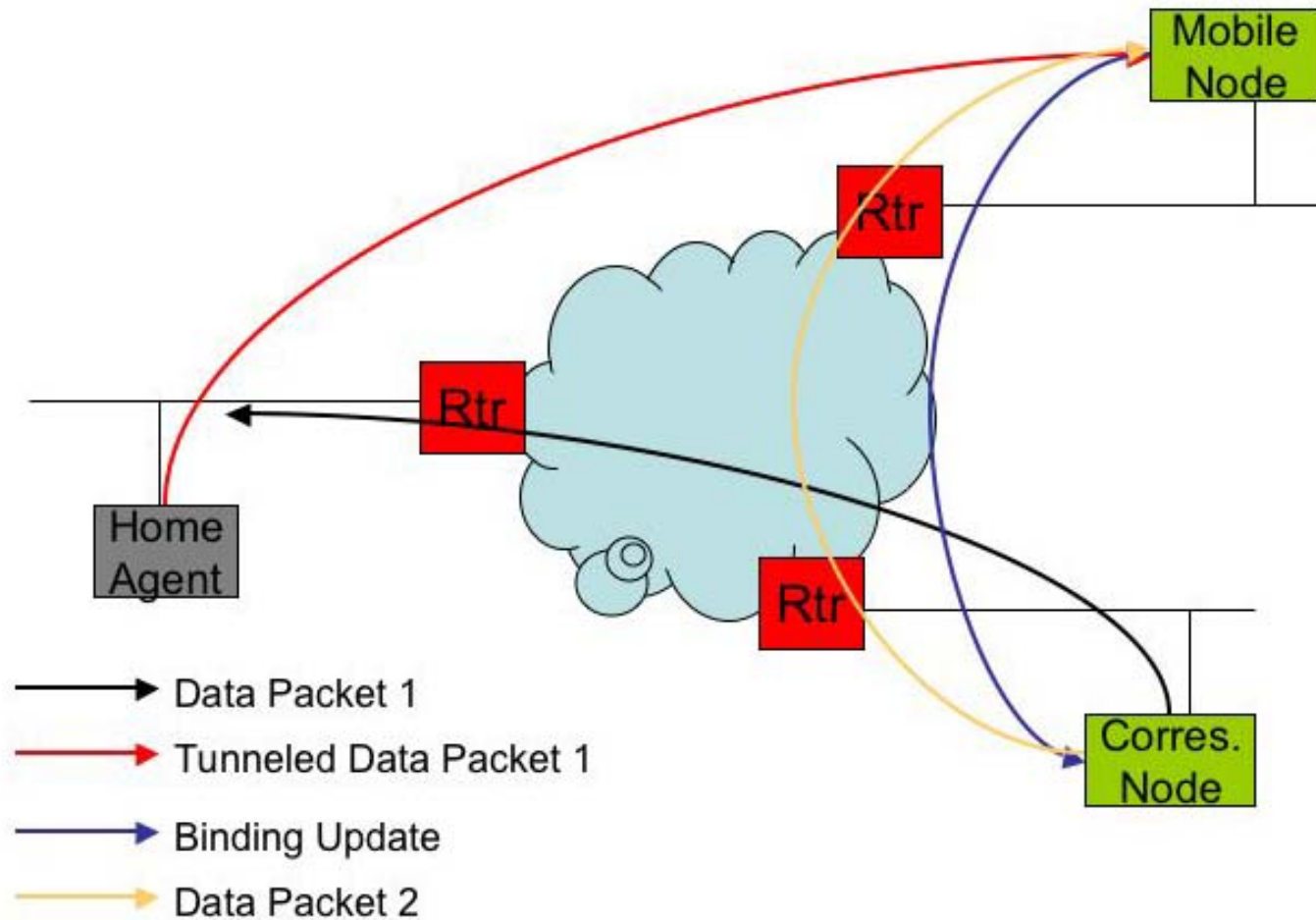
# Mobile IP - Introduction

- Developed within the MIPv4 and MIPv6 Working Groups of the IETF (Internet Area)
  - *MIPv4 for IPv4 mobility support, MIPv6 for IPv6 mobility support*
    - *RFC 3344 and RFC 3775, respectively*
    - *Similar model, but key differences*
    - *Common statement: “IPv6 provides better mobility support than IPv4”*
      - *Generally true, but only IF mobility extensions are implemented*
- Focused on support of individual node mobility (Mobile Node)
- Goal is to make mobility of node transparent to outside networks
- Key concepts:
  - *Two IP Addresses: Home Address (HoA) and Care-of Address (CoA)*
    - *MN is permanently associated with a ‘Home Network’*
    - *As MN point of attachment moves to different subnetworks, CoA are assigned to it*
  - *Home Agent (HA): located within MN’s home network and acts as proxy for MN*
  - *Binding Update (BU): message from MN that informs CoA*
  - *Correspondence Node (CN): Node in different sub-network wishing to communicate with MN*

# Mobile IP Model



# Mobile IP – Optimized Routing





# NEMO

## NEMO – An Overview

- Developed within the NEMO Working Group of the IETF (Internet Area)
- Focused on support of sub-network mobility
  - *Note, not all nodes in network even need to be aware of mobility*
- Goal is to make mobility of entire network transparent to outside networks
- RFC 3963 (the base NEMO specification) reuses the MIPv6 model
- Abstracts the concept of HA and MN and introduces the concept of a Mobile Router (MR)
  - *MR is the point of attachment to the larger network*
- In NEMO model, MR is the MN
- HA in the larger, fixed network acts as proxy for entire network
- MR obtains a CoA, and informs HA of the CoA in BU
  - *CoA used as tunnel endpoint*
- All traffic destined to that CoA prefix traverses tunnel



# MANET Routing

# MANET Routing

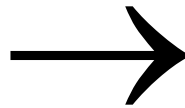
- There are two fundamental types of MANET routing protocols developed to date within the MANET Working Group of the IETF (Routing Area):
  - *Reactive*
    - *Routes are discovered as needed*
    - *Network state information not maintained*
    - *Forwarding state maintained as long as data traffic is utilizing path*
    - *Distance vector routing protocols*
    - *General strengths: reduced overhead (less routing messages), scalability, simplicity*
    - *General weaknesses: latency associated with route establishment, poor route selection due to distance vector approach in wireless environment*
  - *Proactive*
    - *Operate in manner similar to traditional routing protocols*
    - *Link-state routing protocols*
    - *Network state information maintained through distribution of Link State Advertisements*
    - *Allows for immediate forwarding of data packets*
    - *General strengths: low latency associated with route establishment*
    - *General weakness: increased overhead, convergence issues, scalability*
  - *Hybrid approaches have also been proposed in literature*

# MANET Routing

- MANET WG has developed four protocols published as Experimental RFCs:
  - *Proactive*
    - *Optimized Link State Routing (OLSR)*
    - *Topology-based Reverse-path Forwarding (TBRPF)*
  - *Reactive*
    - *Dynamic Source Routing (DSR)*
    - *Ad-hoc On-demand Distance Vector (AODV)*
- Two emerging protocols of choice: AODV, OLSR
- MANET WG is currently working towards two protocols (one proactive, one reactive) to publish as standards
  - *DYnamic MANET On-demand (DYMO)*
    - *“Son of AODV”*
  - *OLSRv2*



## Pointers to Additional Sources of Information



## Some Additional Reading

- [1] *802.11 Wireless Networks: The Definite Guide*, Matthew S. Gast, O'Reilly, 2002.
- [2] *Wireless LANs: Implementing High Performance IEEE 802.11 Networks*, Jim Geier, Sams, 2001.
- [3] *Wireless Communications Standards: A Study of IEEE 802.11, 802.15, and 802.16*, Todor Cooklev, IEEE Press, 2004.
- [4] *Bluetooth Revealed*, Brent Miller, Prentice Hall, 2002.

## Some Websites of Interest

- 1) 802.11 WG Home Page  
<http://www.ieee802.org/11/>
- 2) Wi-Fi Alliance  
<http://www.wi-fi.org/OpenSection/index.asp>
- 3) 802.11 Industry News  
<http://www.wi-fiplanet.com/>
- 4) Wireless Networking Statistics and Trends  
<http://www.itfacts.biz/index.php?id=P630>
- 5) Wi-Fi Deployment Data  
<http://www.wi-fihotspotlist.com/>
- 6) Wi-Fi Security  
<http://www.wardrive.net/>
- 7) 802.16 WG Home Page  
<http://www.ieee802.org/16/>
- 8) WiMAX Forum  
[www.wimaxforum.org](http://www.wimaxforum.org)
- 9) 802.16 Industry News  
<http://www.80216news.com>
- 10) Official Bluetooth WebSite  
<http://www.bluetooth.com>
- 11) Bluetooth Industry News  
[http://www.10meters.com/bluetooth\\_news.html](http://www.10meters.com/bluetooth_news.html)
- 12) 802.15 WG Home Page  
<http://www.ieee802.org/15/>



## Acronyms and Abbreviations

# Abbreviations and Acronyms

- AC – Access Category
- ACL – Access Control List
- ACL – Asynchronous Connectionless Link
- AES – Advanced Encryption Standard
- AID – Association Identifier
- AK – Authorization Key
- AODV – Ad-hoc On-demand Distance Vector
- AP – Access Point
- ASCII – American Standard Code for Information Interchange
- Bps – Bits per second
- BPSK – Binary Phase Shift Keying
- BS – Base Station
- BSA – Basic Service Area

## Abbreviations and Acronyms (continued)

- BSS – Basic Service Set
- BU – Binding Update
- BWA – Broadband Wireless Access
- CBC-MAC – Counter-mode Cipher Block Chaining with Message Authentication Codes
- CCK – Complimentary Code Keying
- CCMP – CBC-MAC Protocol
- CFP – Contention-Free Period
- CID – Connection ID
- CN – Correspondence Node
- CoA – Care-of Address
- COTS – Commercial-off-the-shelf
- CP – Contention Period
- CPS – Common Part Sub-layer
- CRC – Cyclic Redundancy Code

## Abbreviations and Acronyms (continued)

- CS – Convergence Sub-layer
- CSMA – Carrier Sense Multiple Access
- CSMA / CD – Carrier Sense Multiple Access / Collision Detection
- CSMA/CA – Carrier Sense Multiple Access / Collision Avoidance
- CTS – Clear to Send
- CW – Contention Window
- DARPA – Defense Advanced Research Projects Agency
- D-BPSK – Differential Binary Phase Shift Keying
- DCF – Distributed Coordination Function
- DFC – Data Flow Control
- DHSS – Direct Sequence Spread Spectrum
- DIFS – DCF Inter-frame Spacing
- DIUC – Downlink Interval Usage Code
- DLC – Data Link Control

## Abbreviations and Acronyms (continued)

- DLP – Direct Link Protocol
- DoS – Denial of Service
- D-QPSK – Differential Quaternary Phase Shift Keying
- DS – Distribution System
- DSR – Dynamic Source Routing
- DSSS – Direct Sequence Spread Spectrum
- DYMO – Dynamic MANET On-Demand
- EAP – Extensible Authentication Protocol
- EDCF – Enhanced DCF
- EIFS – Extended Inter-frame Spacing
- ESS – Extended Service Set
- FEC – Forward Error Control
- FCC – Federal Communications Commission
- FCS – Frame Check Sequence

## Abbreviations and Acronyms (continued)

- FHS – Frequency Hop Synchronization
- FHSS – Frequency Hopping Spread Spectrum
- GFSK – Gaussian Frequency Shift Keying (GFSK)
- GPC – Grant Per Connection
- GPSS – Grand Per Subscriber Station
- HA – Home Agent
- HCCA – HCF Controlled Channel Access
- HCF – Hybrid Coordination Function
- HMAC – Hashed Message Authentication Code
- HoA – Home Address
- HR – High-rate
- HR-DSSS – High-rate DSSS
- IEEE - Institute of Electrical and Electronics Engineers
- IESG – Internet Engineering Steering Group

## Abbreviations and Acronyms (continued)

- IETF – Internet Engineering Task Force
- IFS – Inter-frame Spacing
- IP – Internet Protocol
- ISM – Industrial, Scientific, and Medical
- IUC – Interval Usage Code
- IV – Initialization Vector
- KEK – Key Exchange Key
- L2CAP - Layer 2 Control Access Protocol
- LAN – Local Area Network
- LLC – Logical Link Control
- LMP - Link Manager Protocol
- LSA – Link State Advertisement
- MAC – Medium Access Control
- MAN – Metropolitan Area Network

## Abbreviations and Acronyms (continued)

- MANET – Mobile Ad-hoc Network
- MIP – Mobile IP
- MLME – MAC Sub-layer Management Entity
- MPDU – MAC Protocol Data Units
- MR – Mobile Router
- MS – Mobile Station
- MSDU – MAC Service Data Units
- NAV – Network Allocation Vector
- NEMO – Network Mobility
- OFDM – Orthogonal Frequency Division Multiplexing
- OSI – Open Systems Interconnection
- OSIRM – OSI Reference Model
- PAN – Personal Area Network
- PAR – Project Authorization Request

## Abbreviations and Acronyms (continued)

- PCF – Point Coordination Function
- PCI – Protocol Control Information
- PDA – Personal Digital Assistant
- PDU – Protocol Data Unit
- PHC – Payload Header Compression
- PHY – Physical Layer
- PIFS – PCF Inter-frame Spacing
- PKM – Privacy Key Management
- PLCP – Physical Layer Convergence Procedure
- PLME – PHY Layer Management Entity
- PMD – Physical Medium Dependent
- PPDU – PLCP Protocol Data Units
- PPM – Pulse Position Modulation
- PPP – Point to Point Protocol

## Abbreviations and Acronyms (continued)

- QAM - Quadrature Amplitude Modulation
- OLSR – Optimized Link State Routing
- QPSK – Quaternary Phase Shift Keying
- R&D – Research and Development
- RF – Radio Frequency
- RTS – Request to Send
- SA – Security Association
- SAP – Service Access Point
- SCO – Synchronous Connection Oriented
- SDU – Service Data Unit
- SDP - Service Discovery Protocol
- SG – Study Group
- SIFS – Short Inter-frame Spacing
- SIG – Special Interest Group

## Abbreviations and Acronyms (continued)

- SME – Station Management Entity
- SS – Service Set
- SS – Subscriber Station
- SSID – Service Set Identity
- TBRPF – Topology-based Reverse-path Forwarding
- TC – Traffic Category
- TEK – Traffic Encryption Key
- TG – Task Group
- TGe – Task Group E
- TGn – Task Group N
- TGr – Task Group R
- TGs – Task Group S
- TKIP – Temporal Key Integrity Protocol
- TNC – Terminal Node Controllers

## Abbreviations and Acronyms (continued)

- TXOP – Transmission Opportunity
- UIUC – Uplink Interval Usage Code
- U-NII – Unlicensed-National Information Infrastructure
- UP – User Priority
- UWB – Ultra Wideband
- WAN – Wide Area Network
- WAPI - WLAN Authentication and Privacy Infrastructure
- WEP – Wired Equivalent Privacy
- Wi-Fi – Wireless Fidelity
- WLAN – Wireless Local Area Network
- WMAN – Wireless Metropolitan Area Network
- WPA – Wireless Protected Access
- WPAN – Wireless Personal Area Network
- WRAN – Wireless Regional Area Network



## References

## List of References

- [1] "The Evolution of Untethered Communications", Committee of Evolution of Untethered Communications, National Research Council, 1997.
- [2] Secretary of Defense Memorandum, "Specifications and Standards - A New Way of Doing Business", Department of Defense, Washington DC, June 1994.
- [3] IEEE 802.16-2001, "IEEE Standard for Local and Metropolitan Area Networks - Part 16: Air Interface for Fixed Broadband Wireless Access Systems," 6 December 2001.
- [4] IEEE 802.2, "Part 2: Logical Link Control," 1998 (R2003).
- [5] 802.11 Wireless Networks: The Definitive Guide, First Edition, Matthew S. Gast, O'Reilly & Associated, April 2002.
- [6] Wireless LANS: Implementing High Performance IEEE 802.11 Networks, Second Edition, Jim Geier, Sams Publishing, 2002.
- [7] IEEE 802.11-1999, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," 1999.
- [8] IEEE 802.11b-1999, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band," 1999.

## List of References (continued)

- [9] M.J.E. Golay, "Static Multi-slit Spectrometry and it's Applications to the Panoramic Display of Infrared Spectra", J. Opt. Soc. Am, Vol 41, No. 7, p. 468-472, July 1951.
- [10] IEEE 802.11a-1999, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High-Speed Physical Layer in the 5 GHz Band," 1999.
- [11] "Orthogonal Frequency Division Multiplexing for Wireless Networks: Standard 802.11a," Anabil Luis Intini, University of California Santa Barbara, December 2000.
- [12] IEEE 802.11g-2003, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High-Speed Physical Layer in the 2.4 GHz Band," 2003.
- [13] Brandon Brown, "802.11: The Security Difference between b and I," *IEEE Potentials*, Vol. 22, No. 4, pp. 23-27, October/November 2003.
- [14] IEEE 802.11i-2004, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Medium Access Control (MAC) Security Enhancements," 2004.

## List of References (continued)

- [15] IEEE 802.11e draft/D4.0, "Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Medium Access Control (MAC) Enhancements for Quality of Service," November 2002.
- [16] IEEE 802.16a-2001, "IEEE Standard for Local and Metropolitan Area Networks - Part 16: Air Interface for Fixed Broadband Wireless Access Systems - Amendment 2: Medium Access Control Modifications and Additional Physical Layer Specifications for 2-11 GHz," 1 April 2003.
- [17] IEEE 802.16c-2001, "IEEE Standard for Local and Metropolitan Area Networks - Amendment 1: Detailed System Profiles for 10-66 GHz," 15 January 2003.
- [18] IEEE 802.16-2004, "IEEE Standard for Local and Metropolitan Area Networks - Air Interface for Fixed Broadband Wireless Access Systems," 1 October 2004.
- [19] Carl Eklund, et al., "IEEE Standard 802.16: A Technical Overview of the WirelessMAN Air Interface for Broadband Wireless Access," IEEE Communications Magazine, June 2002.

## List of References (continued)

- [20] William T. Kasch and Jack L. Burbank, "The Application of Commercial WLAN Technologies for Military Operations," Proceedings of the 2004 Virginia Tech/MPRG Wireless Personal Communications Symposium, 9-11 June 2004.
- [21] Jack L. Burbank and William T. Kasch, "COTS Communications Technologies for DoD Applications: Challenges and Limitations," Proceedings of the 2004 IEEE Military Communications (MILCOM) Conference, October 2004.
- [22] Jack L. Burbank, et al., "Key Challenges of Military Tactical Networking and the Elusive Promise of MANET Technology," to appear in the IEEE Communications Magazine, November 2006.
- [23] Carlos Cordeiro, et al., "IEEE 802.22: The First Worldwide Wireless Standard based on Cognitive Radios," 2005 First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN), 8-11 November 2005, pp. 328-337.