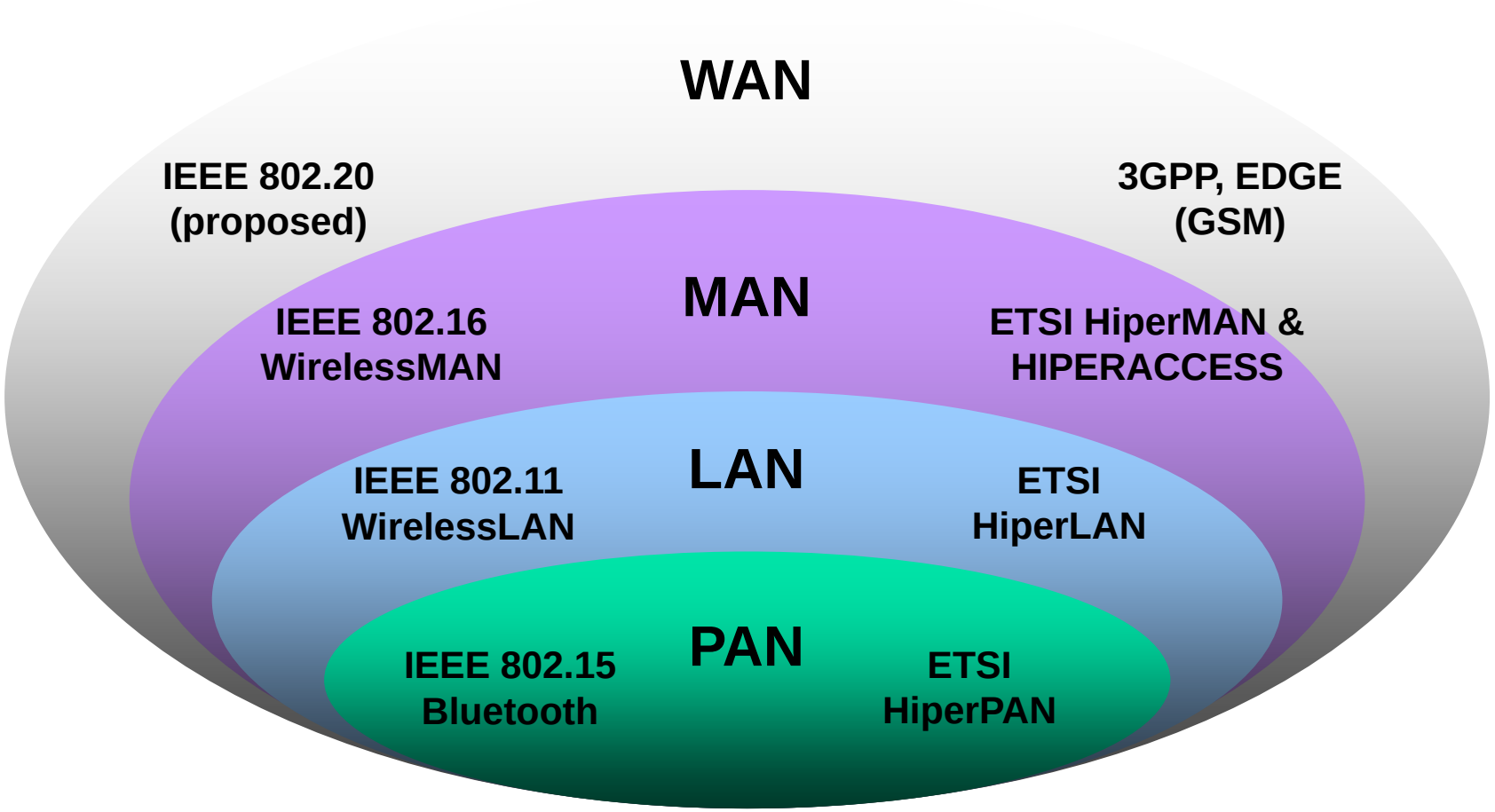
WiMAX & 802.16

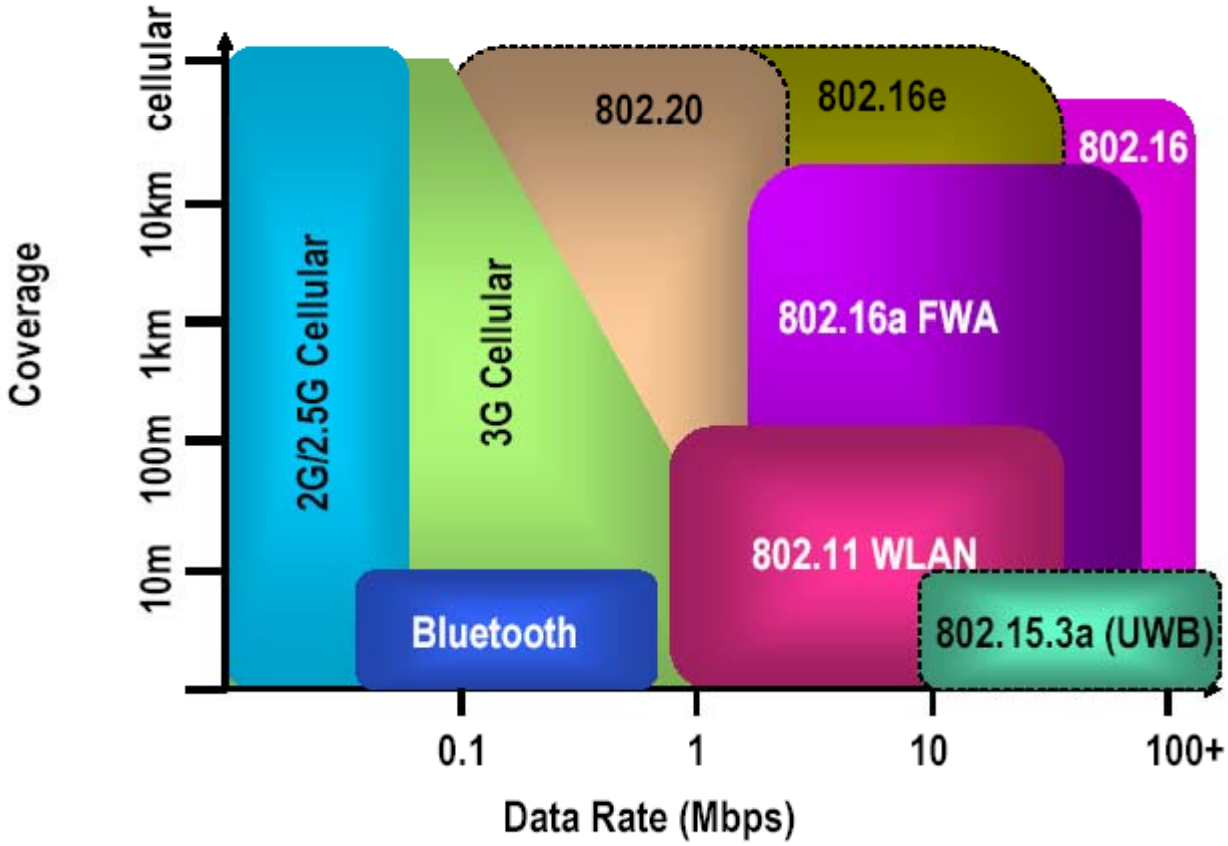
WIMAX?

- **Worldwide Interoperability for Microwave Access (**for license-exempt and licensed MAN operation), popularly known as **WiMax**, is the name for IEEE standard 802.16.
- "The first mile" or "the last mile"
- Within the city: Wireless access range of up to 31 miles;
  - Secure system that offers voice and video.
  - A non line-of-light broadband wireless standard capable of transmitting massive information over long distances
  - Aims to provide high-throughput wireless broadband connections over long distances
- Support different application classes – at the same time
  - Interactive gaming
  - VOIP & video conferencing
  - Streaming media (real time)
  - Web browsing & instant messaging
  - Media content download (store & forward**)**

Global Wireless Standards



WIRELESS STANDARDS: COVERAGE & RATE



Wireless Platforms





Fixed

Licensed and Unlicensed
E1/ T1 & DSL level service

- **Enterprise / Backhaul** → **802.16 HiperMAN**
- **Residential access** → **802.16 HiperMAN**

Portable

Licensed and Unlicensed
Consumer DSL level service

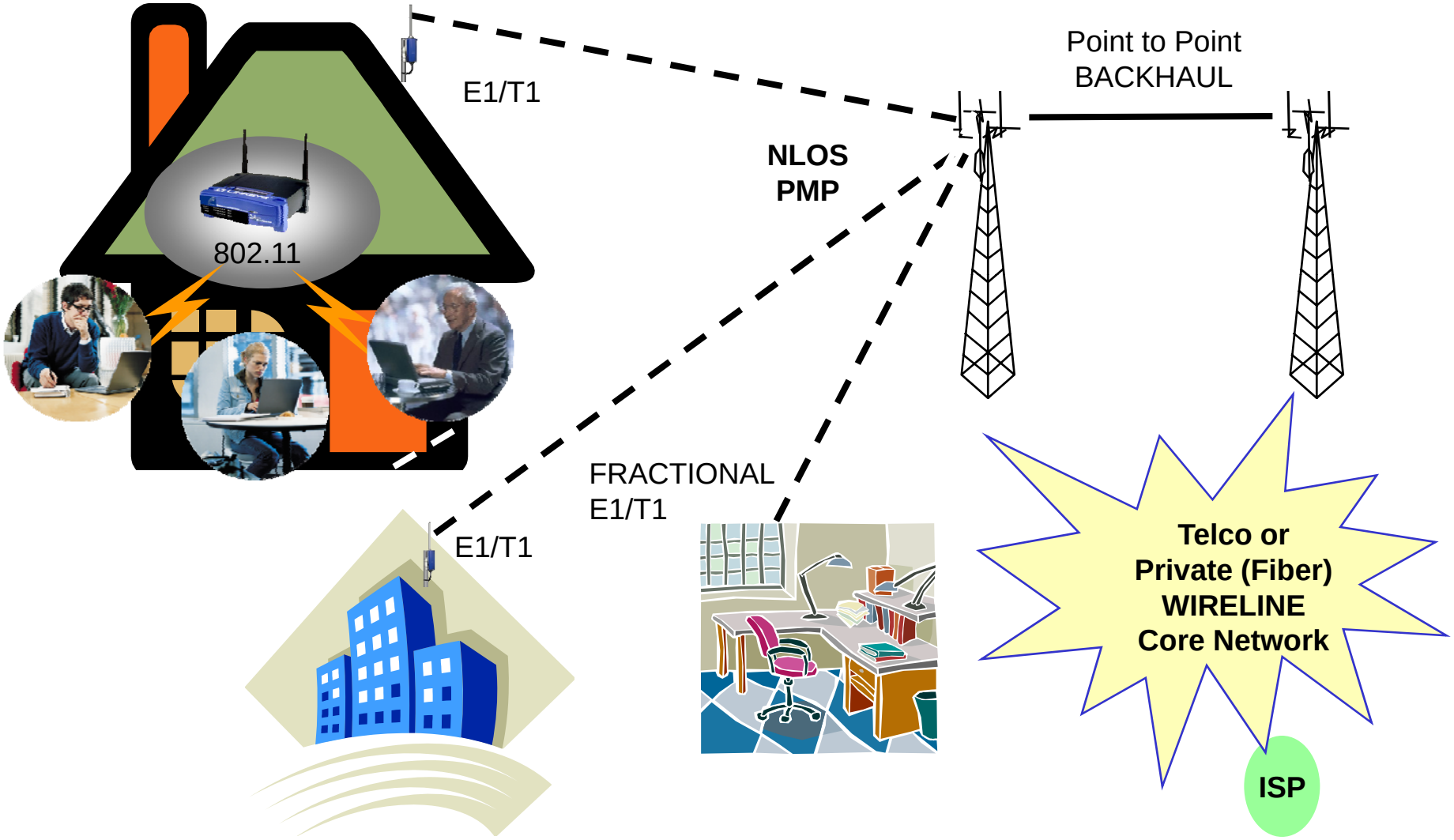
- **Destination based** → **802.11 Hot Spots**
- **Nomadic** → **802.16e**

Mobile

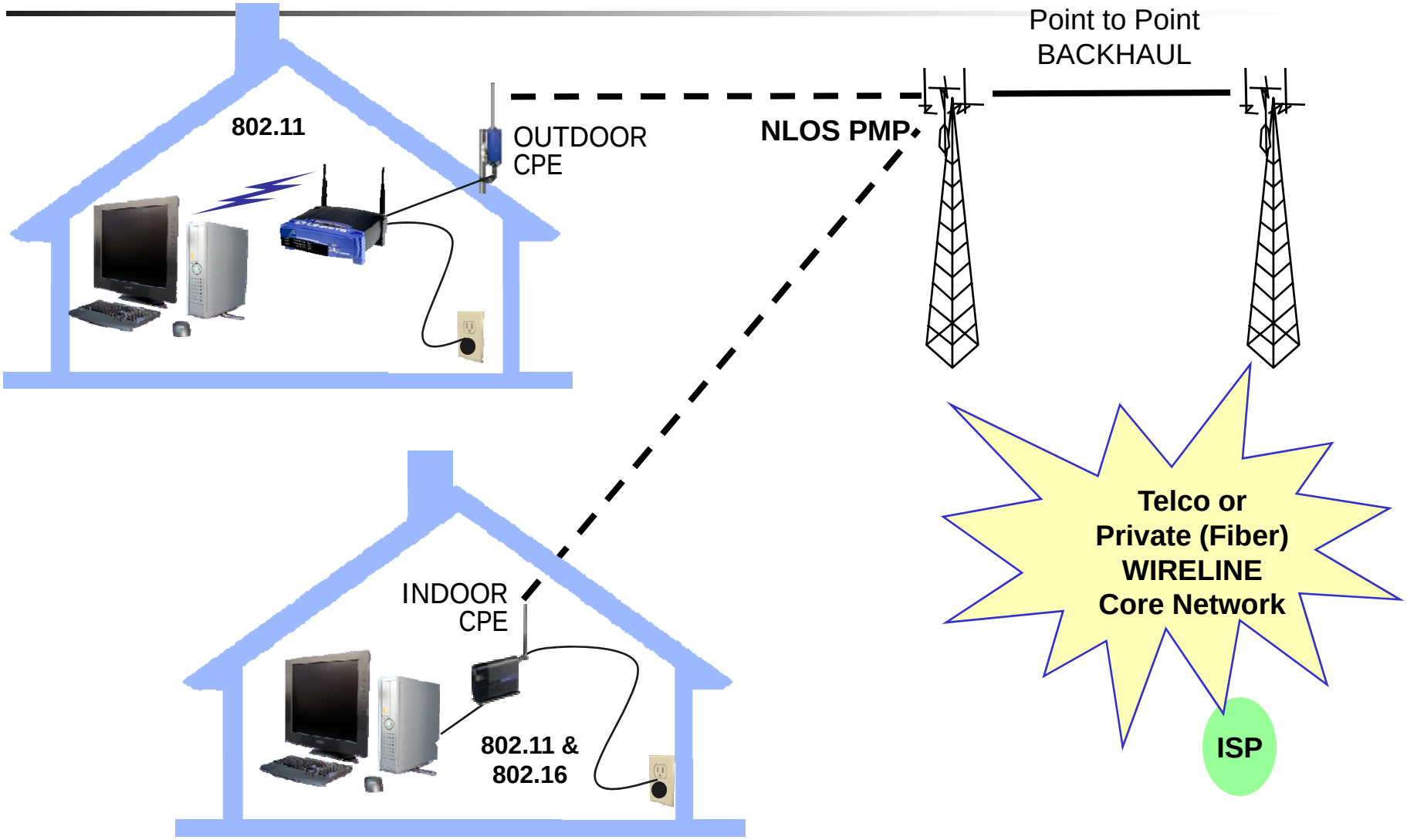
Licensed
Wideband Data Rates

- **Cellular Wideband** → **2.5G, 3G**

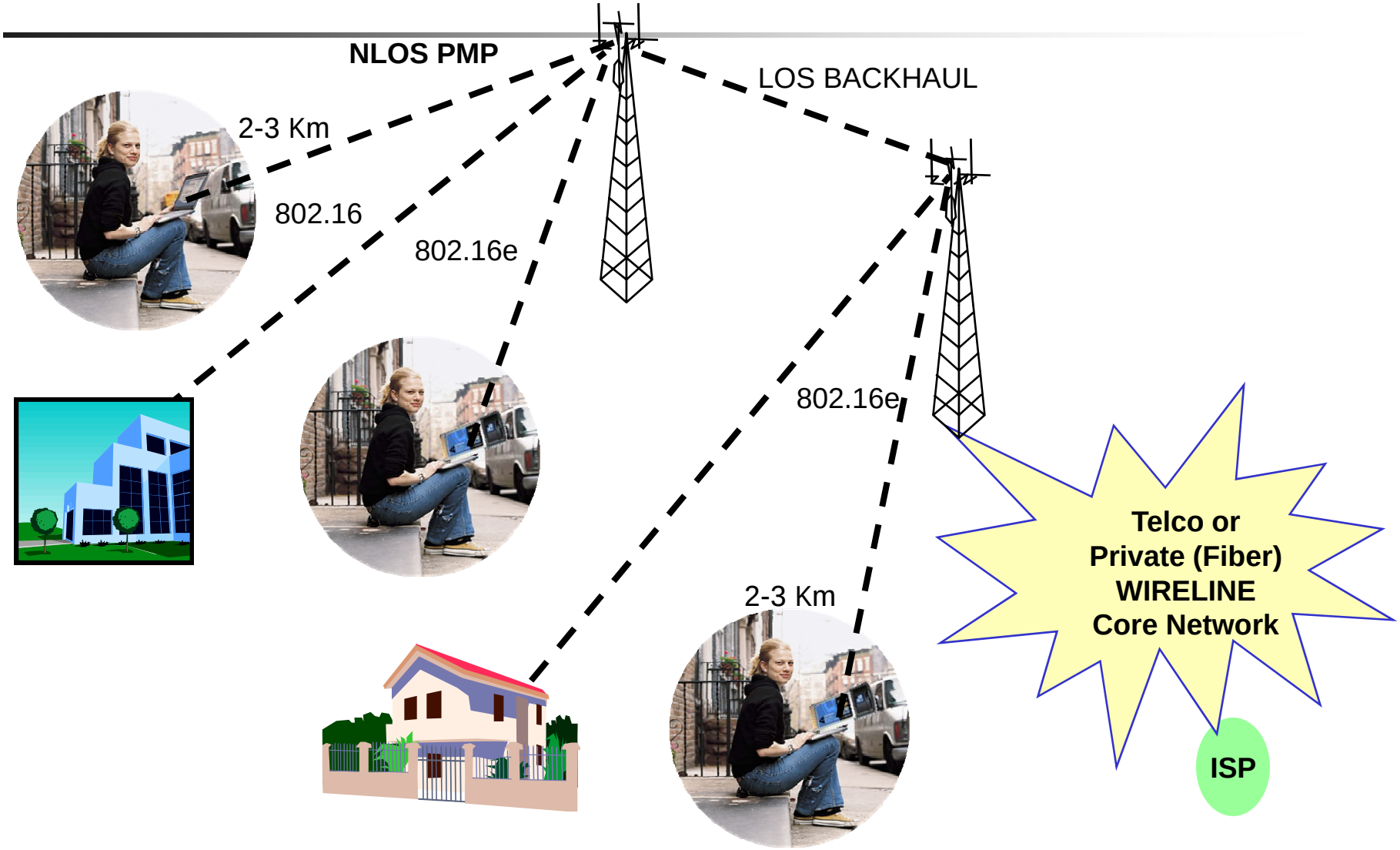
802.16 for Business Backhaul



802.16 for broadband residential Last Mile Access



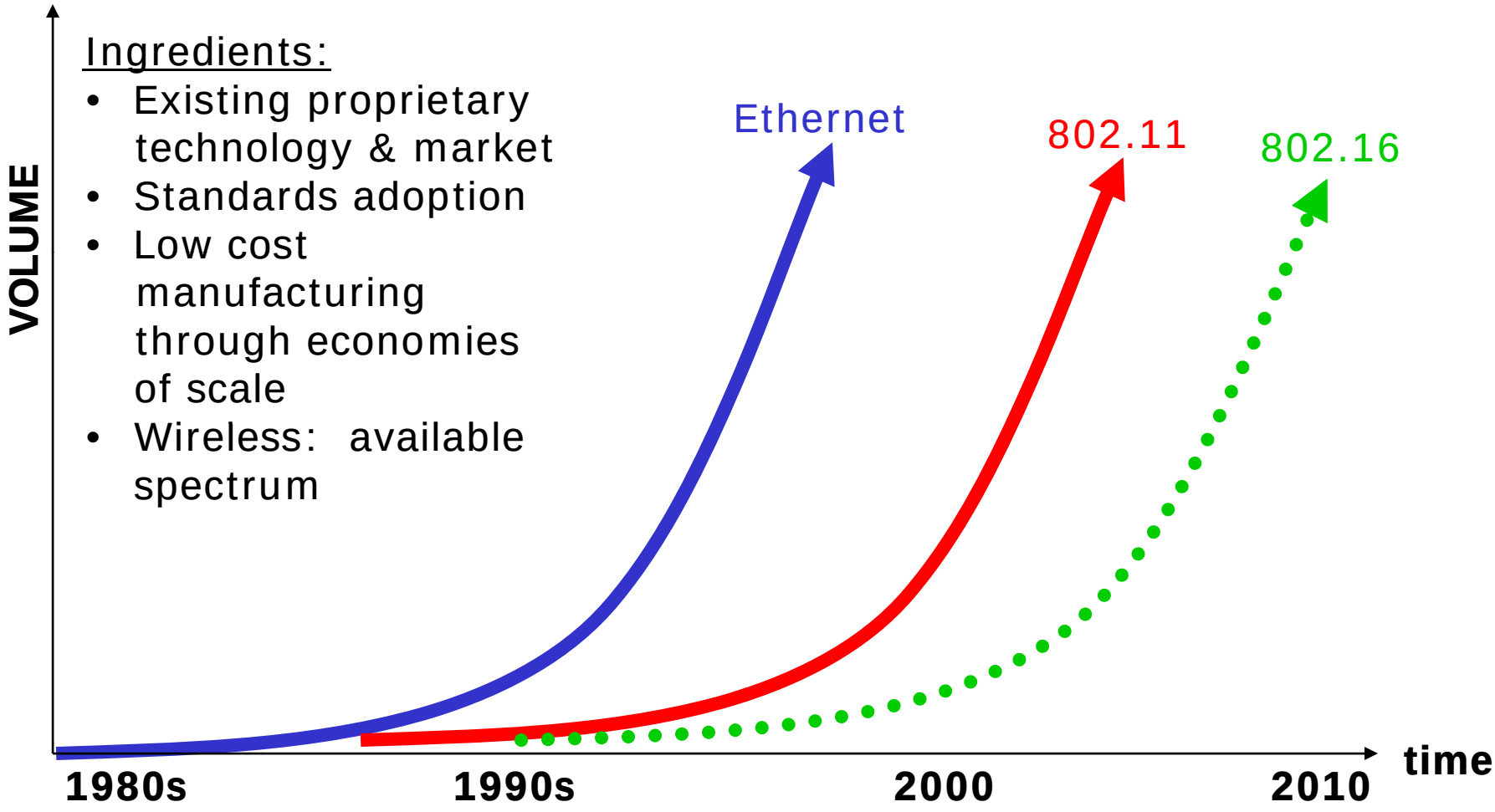
802.16e for Nomadic / Portable



802.16: applications & opportunities

- 802.16c designed for outdoor, long range, carrier class applications:High throughput, non line of sight propagation, scalability for up to 1000's of users, QoS
- 802.16e extension enables nomadic capabilities for laptops: Broadband connectivity beyond hot spots
- Supports both licensed and license-exempt spectrum
- Applicable in many markets – from dense urban environments to rural areas: Where there is no existing or poor wired infrastructure
- PTTs in developing regions
  - Mainly APAC, Eastern/Central Europe, Middle East, Africa, SA
  - Provide basic/broadband voice and internet connection to residential subscribers
- PTTs, ILECs, CLECs and ISPs in developed regions
  - Mainly in Europe & NA but also in more affluent regions of emerging economy countries
  - A new true broadband “last-mile” market play opportunity
    - Capture new subscribers
    - Upgrade existing dial-up/DSL subscribers
  - Provide enhanced services of high-speed internet, multiple voice lines to residential, mid-tier businesses and Hot-Spots’ backhaul

802.16: Expected Growth



BWA MARKET IS GLOBAL BUT HAS BEEN MIS-SERVED

Past Problems with BWA Solutions: Why has BWA not taken off?

- Lack of competitive multi-vendor system market
  - Pre-Standard: Expensive and proprietary systems, Proprietary, vertical solutions, No volume silicon market
  - High recurring costs to service providers
- Line-of-Sight limitations on deployment
  - Limited market penetration
- Unconvincing ROI models to service providers

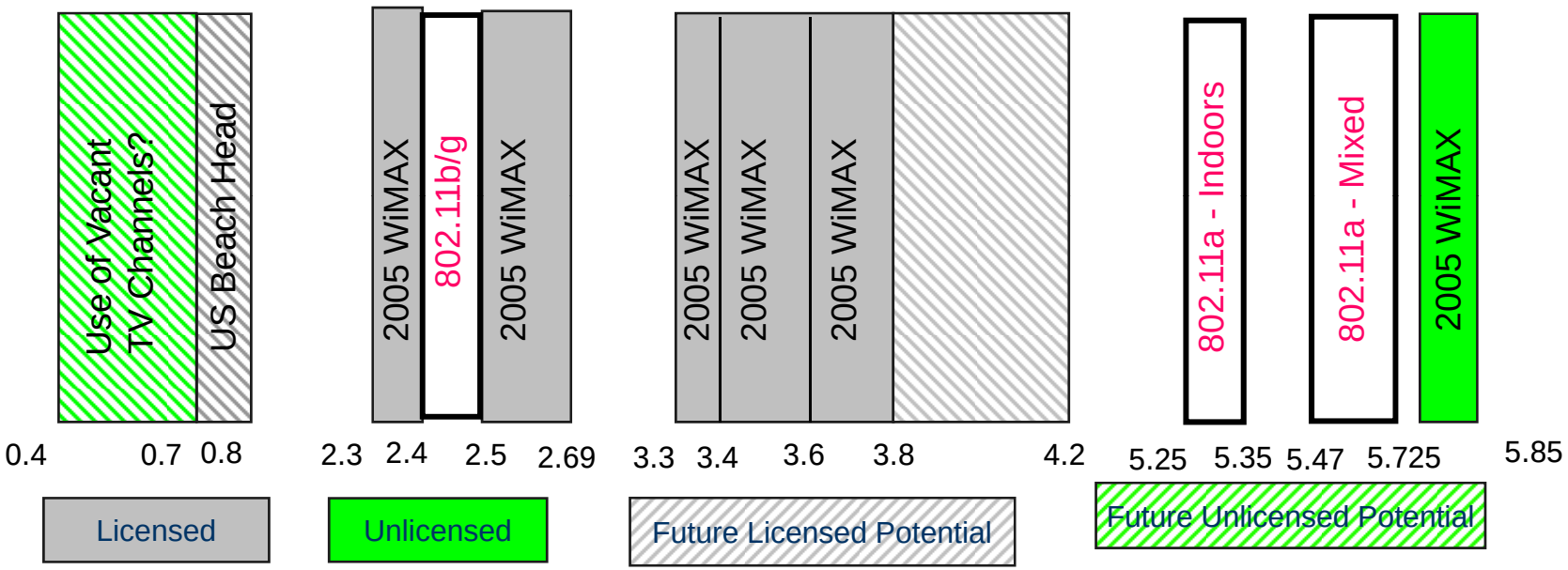
IEEE 802.16 / WiMAX Solution

- Standardization: Allows for multi-vendor system level interoperability
- Economies of scale
- Creates a competitive system vendors market environment
- Guarantees non line-of-sight operation to maximize market penetration
- Supports operation in multiple frequency bands for multiple countries
- Provides for strong economic foundations and ROI models to facilitate
  - Subscriber Unit @ <$300
  - Base Station Unit @ <$10K
  - Flexible service models from few high bandwidth to thousands of low bandwidth subscribers per base-station
  - Supports voice, video and data with full QoS requirements

IEEE 802.16 Standard

	802.16	802.16a/HiperMAN	802.16e
Completed	December 2001	January 2003 (802.16a) 802.16REVd: Q3'04	December 2005
Spectrum	10 - 66 GHz	< 11 GHz	< 11 GHz
Channel Conditions	Line of Sight	Non Line of Sight	Non Line of Sight
Bit Rate	32–134 Mbps in 28MHz	Up to 75 Mbps in 20MHz	peak DL up to 63 Mbps/sector and peak UL up to 28 Mbps/sector in 10MHz
Modulation	QPSK, 16QAM and 64QAM	OFDM 256 sub-carriers QPSK, 16QAM, 64QAM	OFDMA OFDM
Mobility	Fixed	Fixed, Portable	Mobility: Nomadic, Pedestrian, High-speed
Channel Bandwidth	20, 25 and 28 MHz	Scalable 1.25 to 20 MHz	Same as 802.16a with UL sub-channels
Typical Cell Radius	2-5 km	7 to 10 km, Max range 50 km	2-5 km

WiMAX Target Spectrum



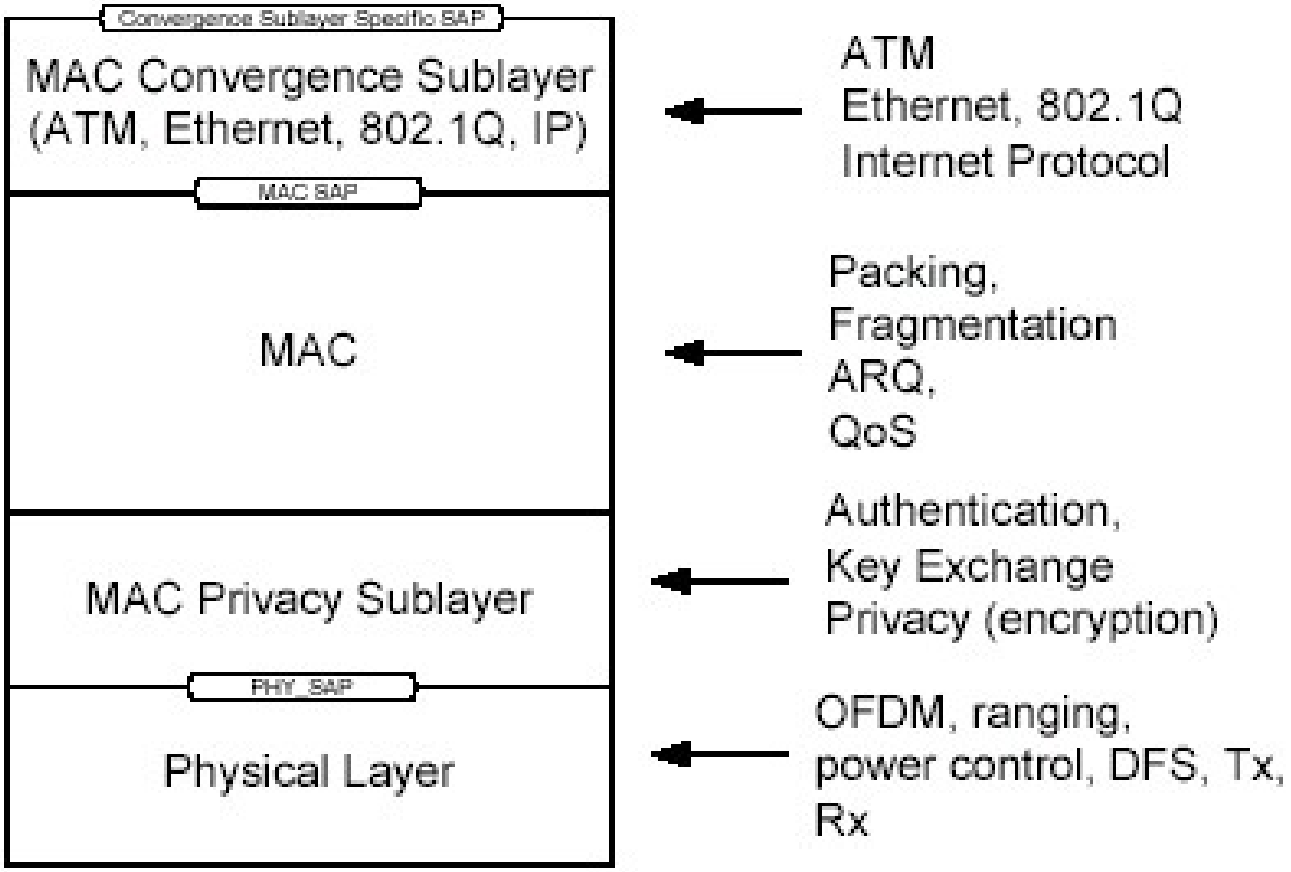
Baud Rates & Channel Size (10-66 GHz)

- Flexible plan - allows equipment manufactures to choose according to spectrum requirements

		Bit Rate (Mb/s)		
		QPSK	16-QAM	64-QAM
Channel BW	Symbol Rate			
20	16	32	64	96
25	20	40	80	120
28	22.4	44.8	89.6	134.4

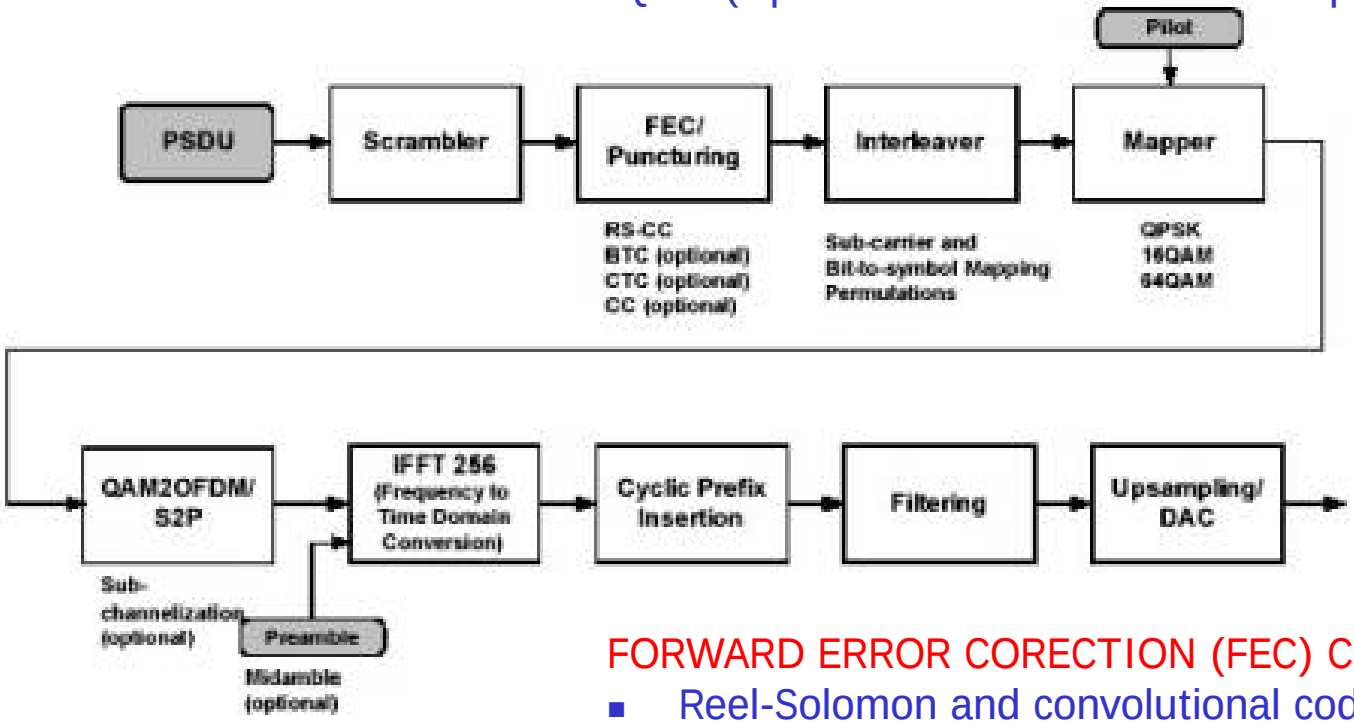
	CHANNEL BANDWIDTH (MHz)	MAX RATE (Mbps)	EFFICIENCY (bps/Hz)
CDMA2000	1.25	2	<1.6
EDGE	0.2	0.384	<1.9
802.11a	20	54	< 2.7
802.16a	3, 3.5, 6, 7, 10, 14, 20	70 (63 in 14)	<5 (4.5)

layers of the 802.16 protocol



transmitter signal processing

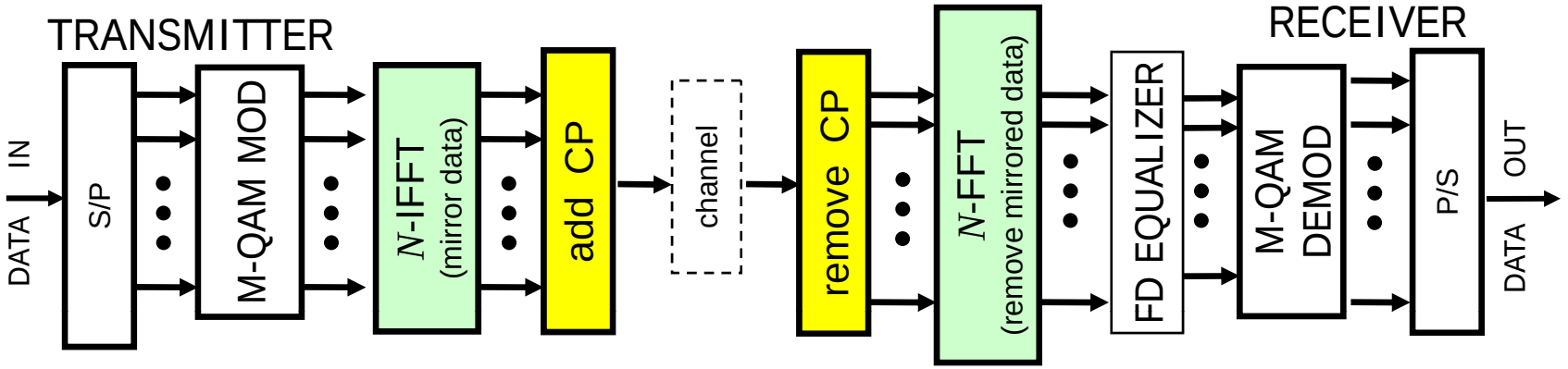
Gray-coded M-QAM: M=4, 16 (Mandatory for Downlink, Optional for Uplink),
64QAM (Optional for both Downlink & Uplink)

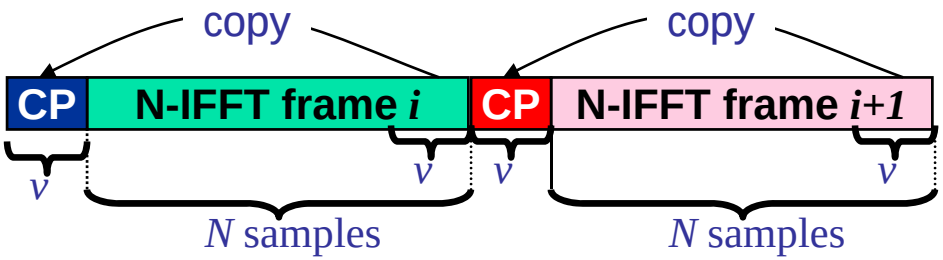


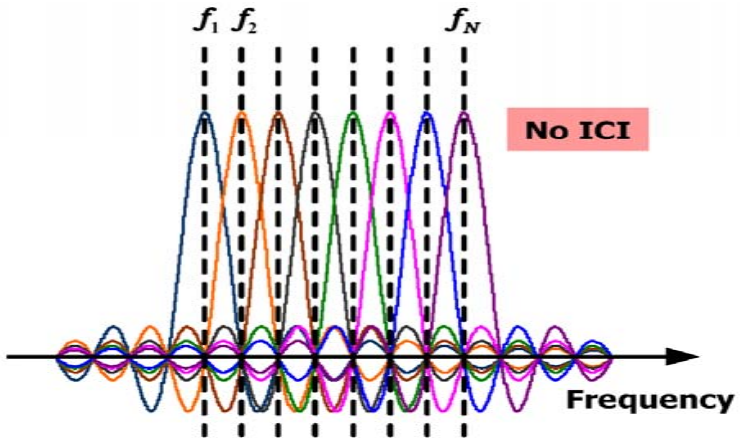
FORWARD ERROR CORECTION (FEC) CODING

- Reel-Solomon and convolutional coding: mandatory
- RS defined over GF(256) with t= 0,1,...,16
- Turbo Product Codes (TPC) are optional

ORTHOGONAL FREQUENCY-DIVISION MULTIPLEXING (OFDM)

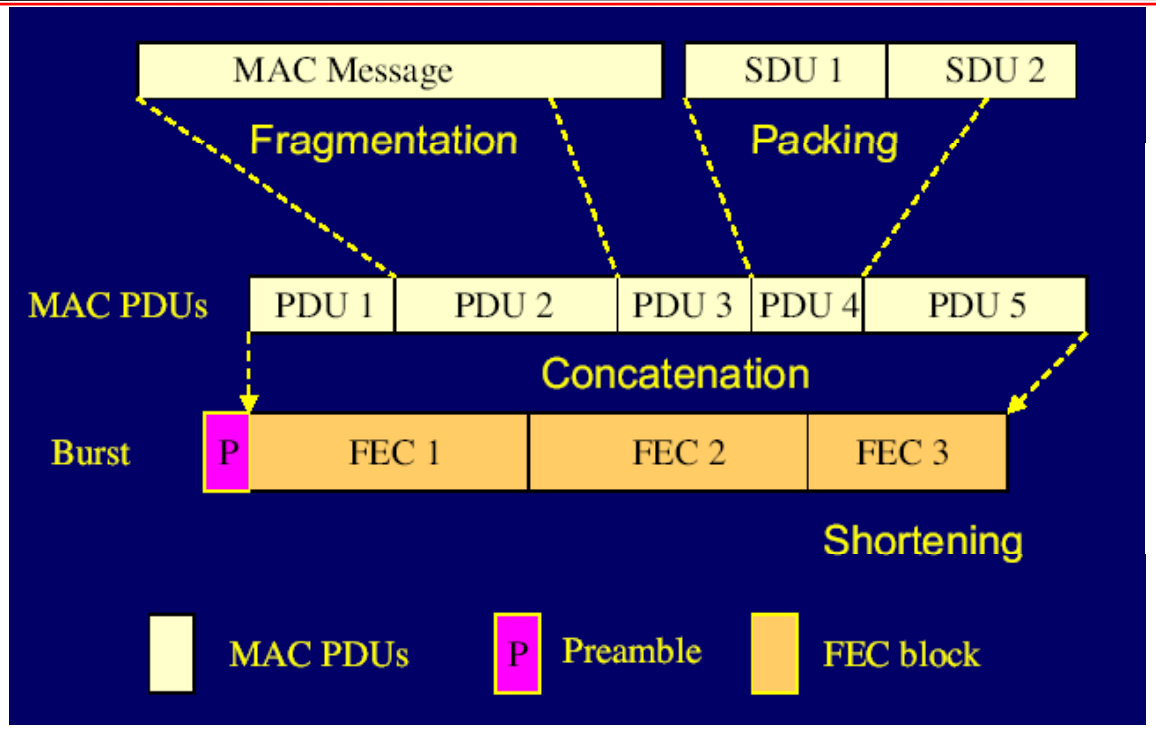






- TRANSMITTER AND RECEIVER ARE PERFECTLY SYNCHRONIZED
- THE FADING IS SLOW ENOUGH FOR THE CHANNEL TO BE CONSIDERED CONSTANT DURING ONE SYMBOL INTERVAL

ADAPTIVE BURST TRANSMISSION



MAC PDU and BURST

Adaptive Modulation and FEC (AMC) dynamically assigned according to link conditions

- Burst by burst, per subscriber station
- Trade-off capacity vs. robustness in real time

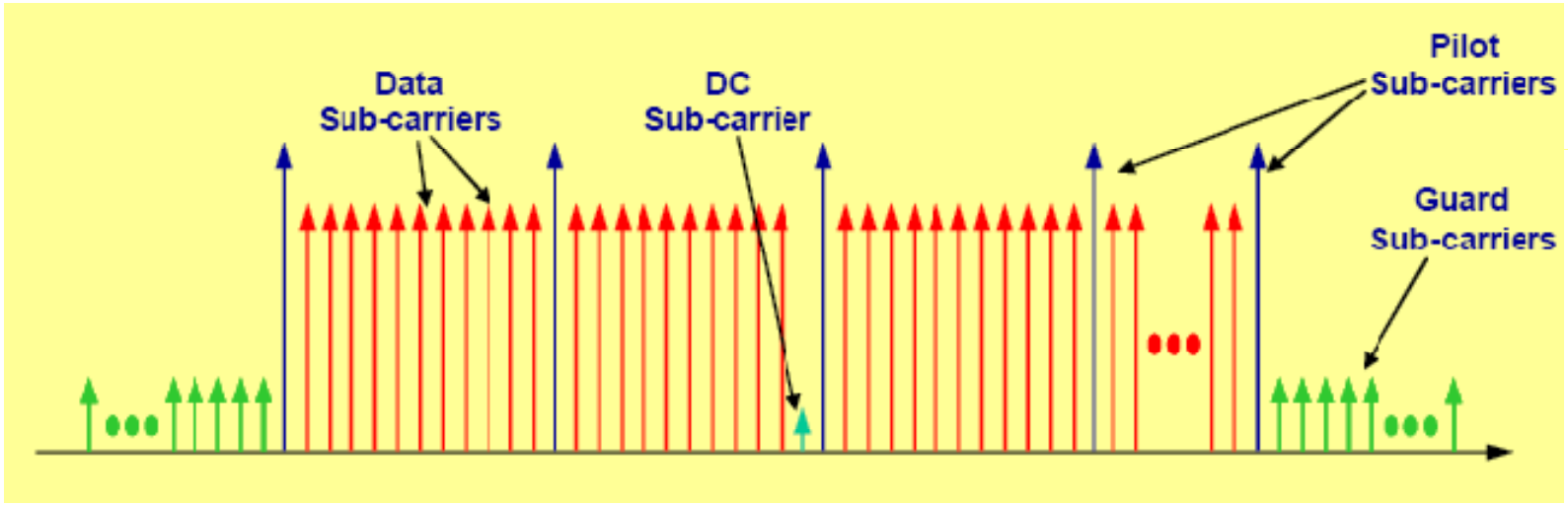
Preambles based on 16 symbol CAZAC sequences

- Burst profile for downlink broadcast channel is well-known and robust
- Other burst profiles can be configured “on the fly”
- SS capabilities recognized at registration

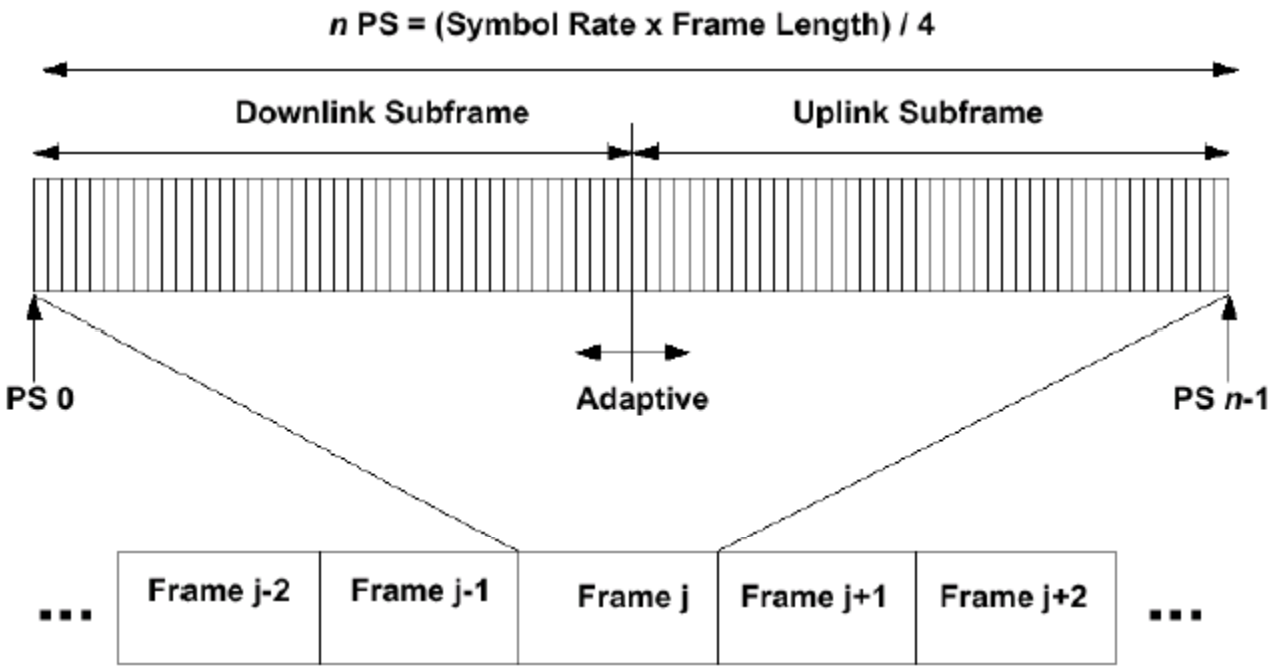
QUICK COMPARISON

Function	802.16a	802.11a/g	802.15.3a
Reed Solomon	(N = 256, K = 239) T= 8	None	None
Convolutional	K = 7, R=1/2	K = 7, R=1/2, 2/3, 3/4, g0133,g171	K=7, R=1/3
Modulation	4, 16, 64QAM	2, 4, 16, 64QAM	QPSK
Rate	<=75Mbps	6-54Mbps	55- 480 Mbps, 55, 110, 200 Man.
FFT	256 (2048 OFDMA)	64	128
OFDM Subcarriers	200	52	122
license status	Both	unlicensed only	3 bands not ISM bands
Transmission format	TDD/FDD	TDD	TDD
MIMO	Optional	None	None
BW	1.25-20MHz	Fixed 20 MHz	3 bands, 528MHz/ea
Packet size	1 - 4095 bytes	1 - 4095 bytes	1 - 4095 bytes
Scrambler	X15 + X14 + 1	X7 + X4 + 1	X15 + X14 + 1
Interleaver Block per OFDM symbol	Yes	Yes	Yes
PLCP Preamble	variable short or long	12 symbols	30 symbols
Ranging	Yes	None	None

OFDMA Sub-Carrier Structure



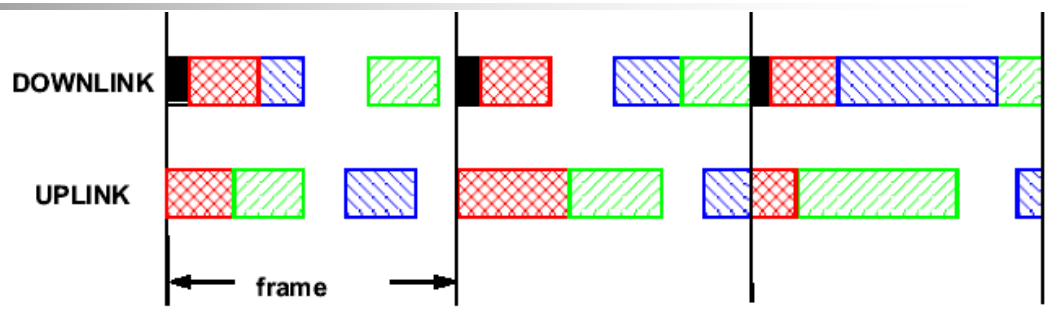
TDD Frame Structure (10-66 GHz)



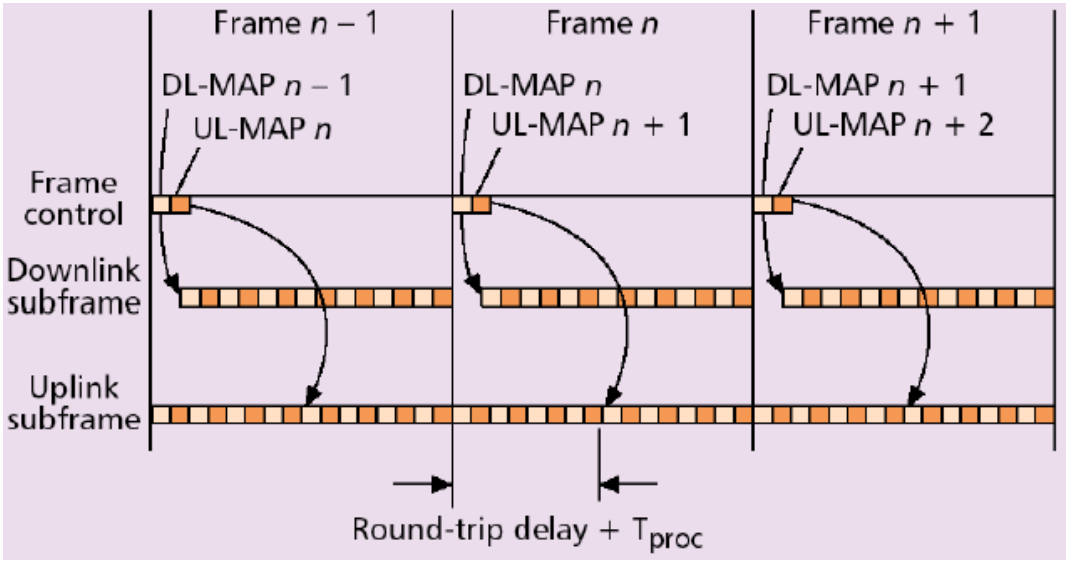
- Frame duration: 1 ms
- Physical Slot (PS) = 4 Modulation symbols. Depending on modulation, a PS contains 1, 2, or 3 bytes
- Allocation process is done in terms of PS

Burst FDD Framing

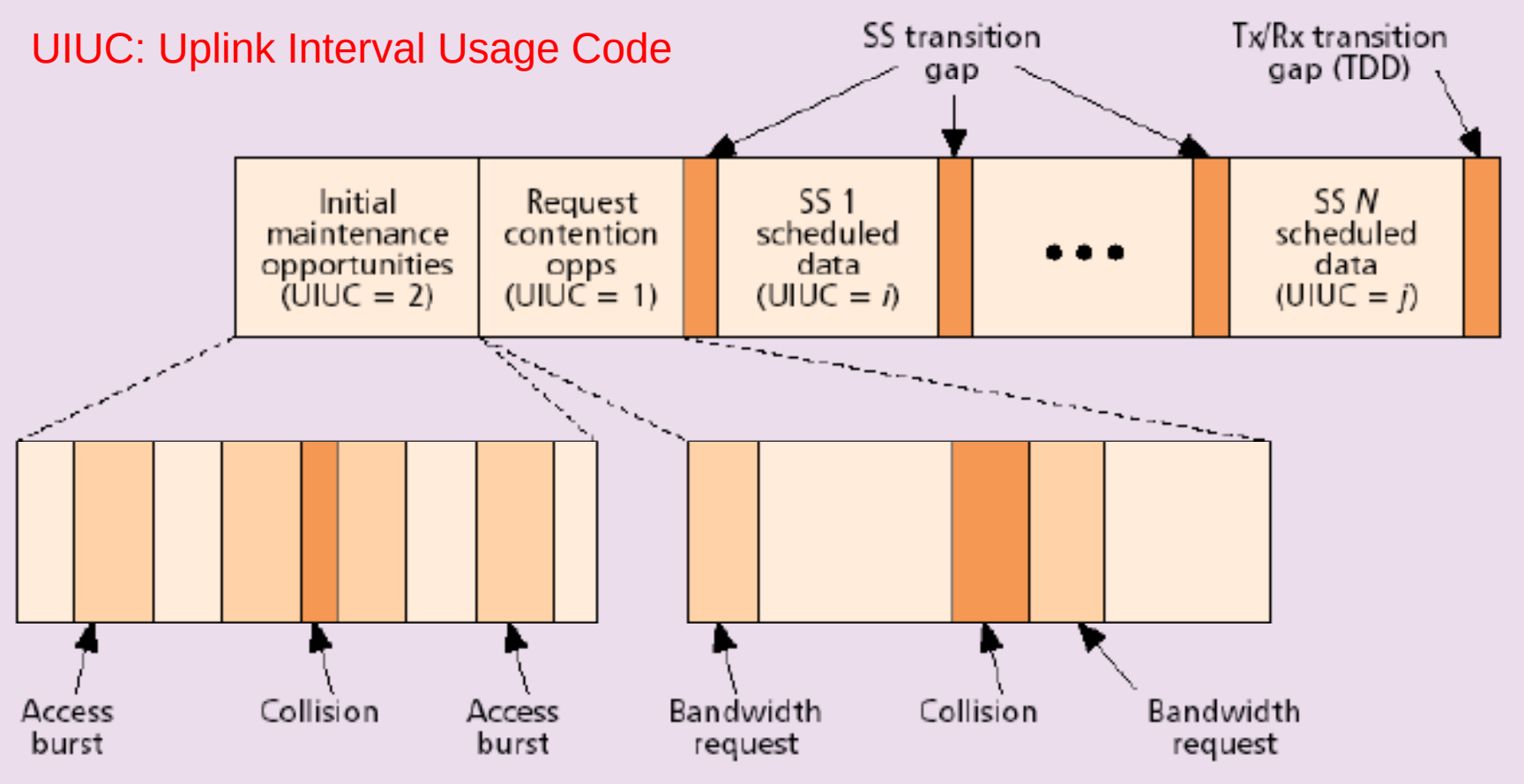
Allows scheduling flexibility



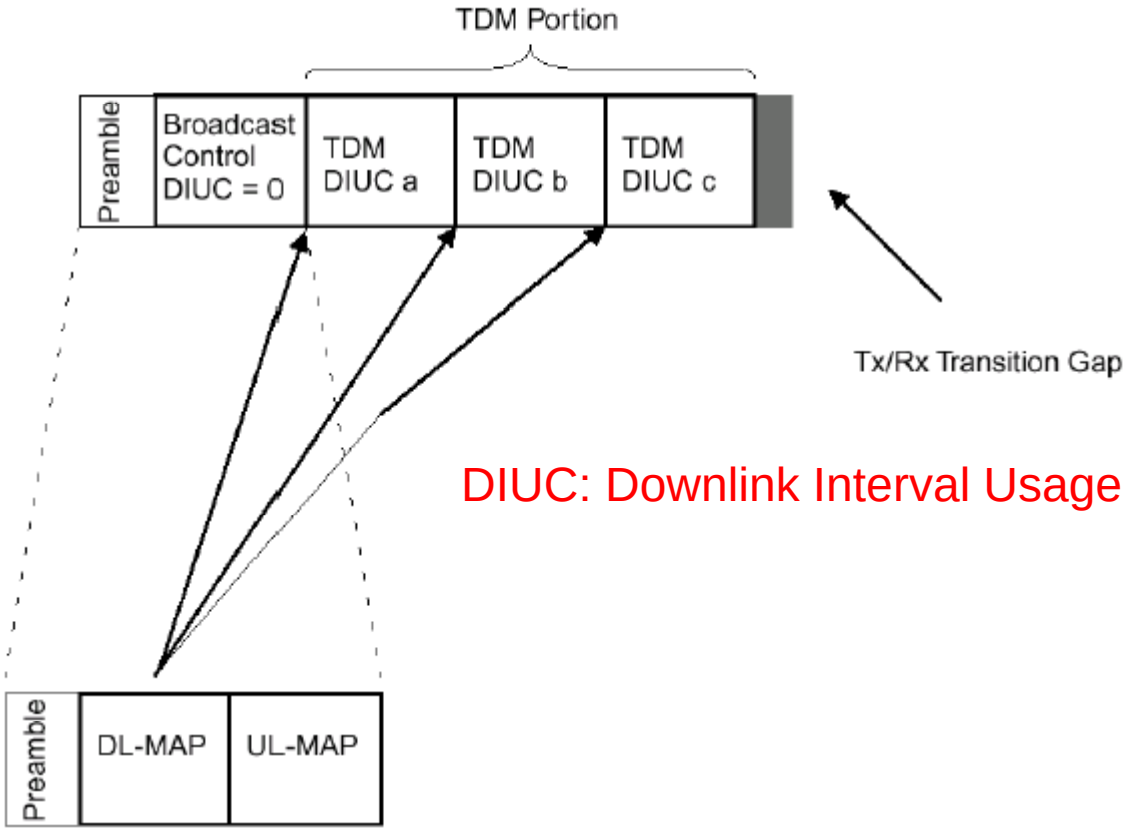
FDD Uplink Subframe: Minimum Advance



Typical Uplink Subframe (TDD or FDD)

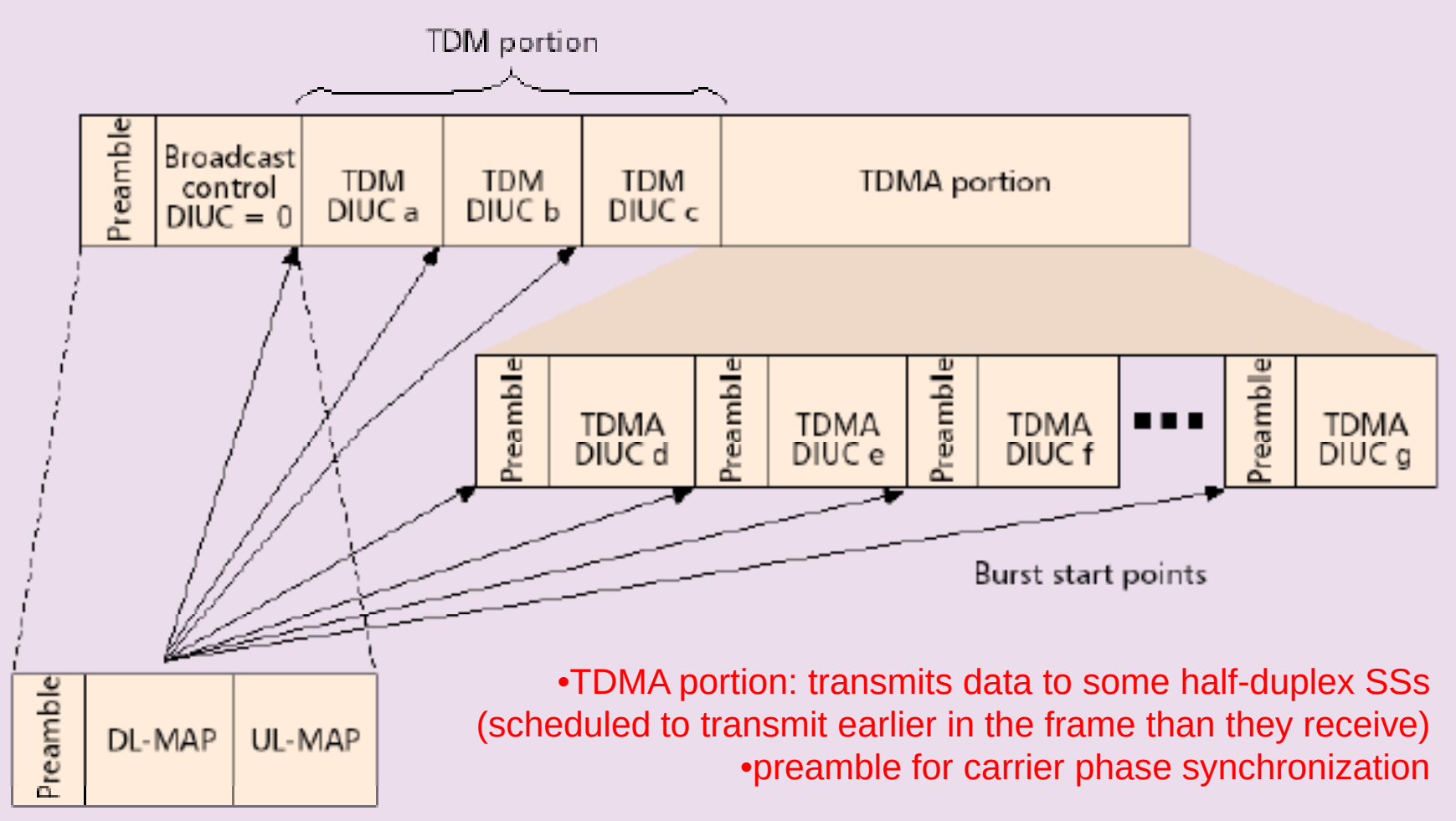


TDD Downlink Subframe



DIUC: Downlink Interval Usage Code

FDD Downlink Subframe



•TDMA portion: transmits data to some half-duplex SSs (scheduled to transmit earlier in the frame than they receive)

•preamble for carrier phase synchronization

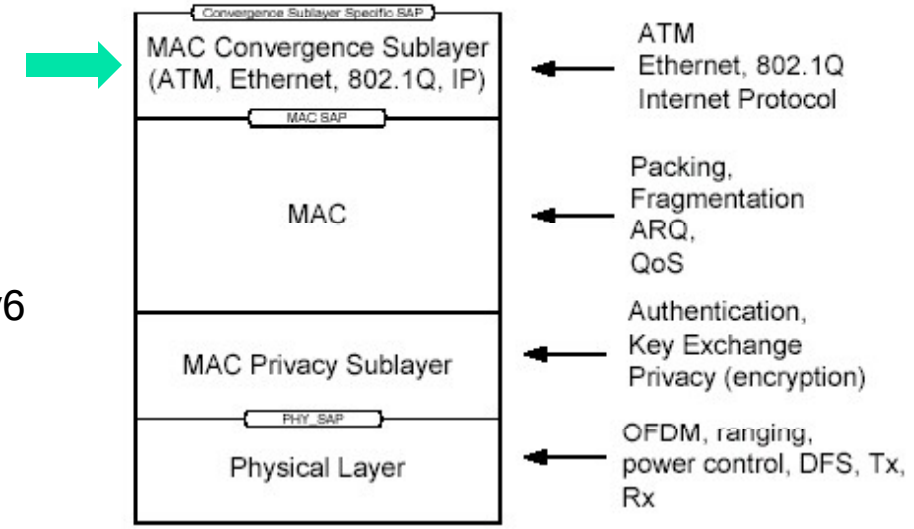
Convergence Sublayer

ATM Convergence Sublayer

- Support for:
  - VP (Virtual Path) switched connections
  - VC (Virtual Channel) switched connections
- Support for end-to-end signaling of dynamically created connections: SVCs, soft PVCs
- ATM header suppression
- Full QoS support

Packet Convergence Sublayer

- Initial support for Ethernet, IPv4, and IPv6
- Payload header suppression
- generic plus IP-specific
- Full QoS support
- Possible future support for: PPP, MPLS, ...



802.16 MAC: Overview

- Broadband services: Very high bit rates, downlink and uplink:
  - High bandwidth, hundreds of users per channel
  - Likelihood of terminal being shared
  - Base Station may be heavily loaded
  - Continuous and burst traffic
- Supports multiple 802.16 PHY alternatives: Adaptive mod, TDD/FDD; single-carrier, OFDM/OFDMA, etc.
- Protocol-Independent Engine: Convergence layers to Ethernet, IPv4, IPv6, ATM, …
- A range of QoS requirements: UGS, rt-PS, Ert-PS, nrt-PS, BE, with granularity within classes
- Connection-oriented
- Security, Authentication and Privacy
- Relationship to DOCSIS

Service Classes: applications and QoS specs

Unsolicited Grant Service (UGS):

- Applications: CBR-like service flows for constant bit-rate (CBR) or CBR-like service flows (SFs), e.g., T1/E1, VoIP
- QoS Specifications: Max Sustained Rate, Max Latency Tolerance, Jitter Tolerance

Real-time Polling Service (rtPS):

- for rt-VBR-like service flows, e.g., Streaming Audio or Video (MPEG)
- QoS Specifications: Min Reserved Rate, Max Sustained Rate, Max Latency Tolerance, Traffic Priority

Extended Real-Time Packet Service (ErtPS):

- Voice with Activity Detection (VoIP)
- QoS Specifications: Min Reserved Rate, Max Sustained Rate, Max Latency Tolerance, Jitter Tolerance, Traffic Priority

Non-real-time Polling Service (nrtPS):

- for non-real-time service flows with better than best effort service, e.g., bandwidth-intensive file transfer, File Transfer Protocol (FTP)
- QoS Specifications: Min Reserved Rate, Max Sustained Rate, Traffic Priority

Best Effort (BE):

- Generic data Data Transfer, Web Browsing, e.g. HTTP, SMTP, etc.
- QoS Specifications: Max Sustained Rate, Traffic Priority

Service Services: Operation

Unsolicited Grant Services (UGS):

- No explicit bandwidth requests issued by SS Prohibited from using any contention requests
- No unicast request opportunity provided
- May include a Grant Management (GM) sub-header containing
- Slip indicator: indicates that there is an backlog in the buffer due to clock skew or loss of maps
- Poll-me bit: indicates that the terminal needs to be polled (allows for not polling terminals with UGS-only services).

Real-time Polling Services (rtPS):

- Prohibited from using any contention requests
- Terminals polled frequently enough to meet the delay requirements of SFs
- Bandwidth requested with BW request messages (a special MAC PDU header)

nrt Services:

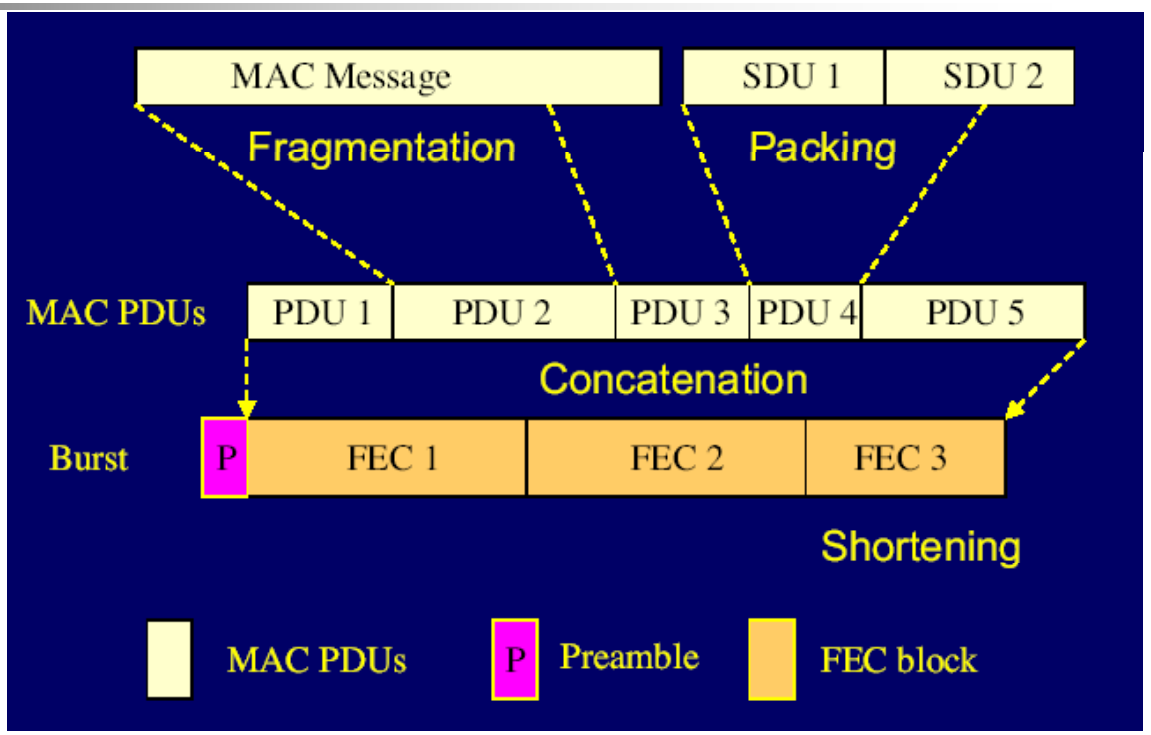
- May use Grant Management sub-header: new request can be piggybacked with each transmitted PDU
- allowed to use contention requests
- may use Grant Management sub-header
- new request can be piggybacked with each transmitted PDU

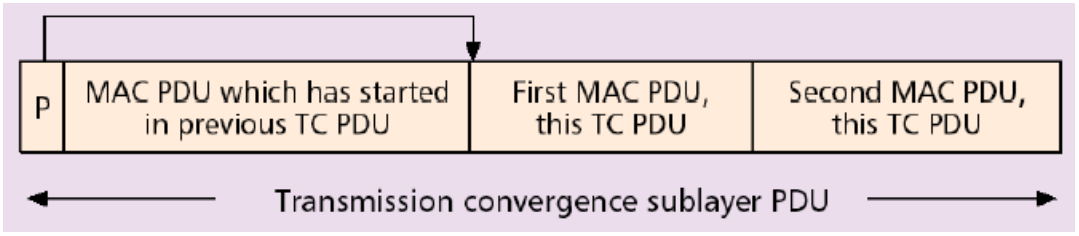
802.16 MAC

- controls access of the BS and SS
- timing is based on consecutive frames that are divided into slots:
  - Both frames and individual slots within the frames can be varied on a frame-by-frame basis, under the control of a scheduler in the BS to allow effective dynamic resource allocation in order to meet the demands of the active connections with their granted QoS properties.
- provides a connection-oriented service to upper layers of the protocol stack. Connections have QoS characteristics that are granted and maintained by the MAC. The QoS parameters for a connection can be varied by the SS making requests to the BS to change them while a connection is maintained.
- QoS service in the 802.16 MAC service takes one of four forms: constant bit rate grant, real time polling, non-real-time polling, and best effort.
- Media access control packet data units (MPDUs) are transmitted in on-air PHY slots. Within these MPDUs, MAC service data units (MSDUs) are transmitted. MSDUs are the packets transferred between the top of the MAC and the layer above.
- MPDUs are the packets transferred between the bottom of the MAC and the PHY layer below.

MAC PDU Transmission

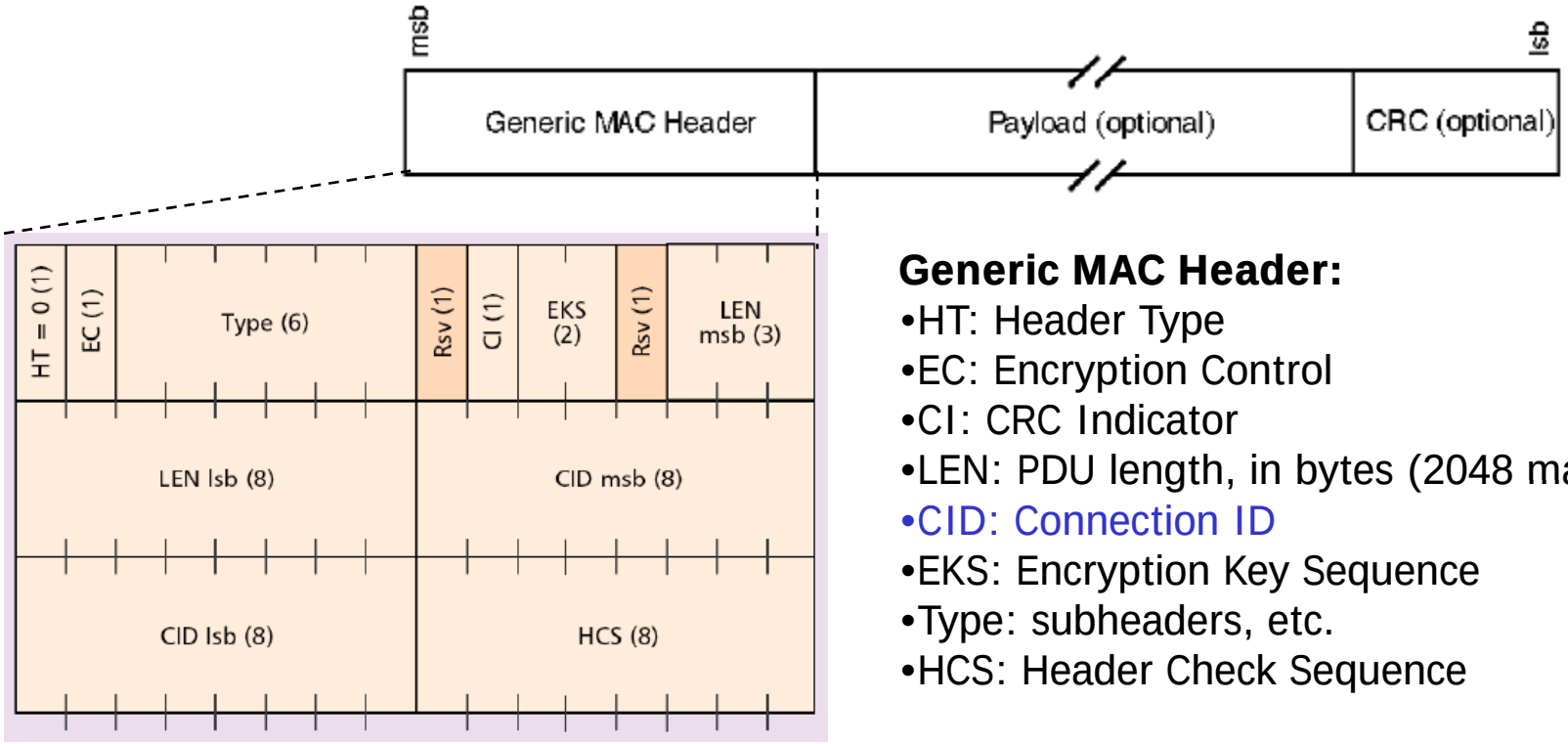
- Service Data Unit (SDU): Data units exchanged between adjacent layers
- Protocol Data Unit (PDU): Data units exchanged between peer entities
- MAC PDUs are transmitted in PHY bursts
- A single PHY burst can contain multiple MAC PDUs
- The PHY burst can contain multiple FEC blocks
- MAC PDUs may span FEC block boundaries
- The **TC (transmission convergence) layer** between the MAC and the PHY allows for capturing the start of the next MAC PDU in case of erroneous FEC blocks





MAC PDU format

- One or more MAC sub-headers may be part of the payload
- The presence of sub-headers is indicated by a Type field in the Generic MAC header



Generic MAC Header:

- HT: Header Type
- EC: Encryption Control
- CI: CRC Indicator
- LEN: PDU length, in bytes (2048 max)
- CID: Connection ID
- EKS: Encryption Key Sequence
- Type: subheaders, etc.
- HCS: Header Check Sequence

MAC Addressing

- SS has 48-bit IEEE MAC Address
- BS has 48-bit Base Station ID
  - Not a MAC address
  - 24-bit operator indicator
- 16-bit Connection ID (CID): Used in MAC PDUs
- Connection and Connection ID: a unidirectional mapping between MAC peers over the airlink (uniquely identified by a CID)
- Service Flow and Service Flow ID: a connection that on a connection that provides a particular QoS (uniquely identified by a SFID)

Fragmentation & Packing

Fragmentation: Partitioning a MAC SDU into fragments transported in multiple MAC PDUs

- Each connection can be in only a single fragmentation state at any time state at any time
- Contents of the fragmentation sub-header:
  - 2-bit Fragmentation Control (FC): Unfragmented, Last fragment, First fragment, Continuing fragment
  - 3-bit Fragmentation Sequence Number (FSN):
    - required to detect missing continuing fragments
    - continuous counter across SDUs

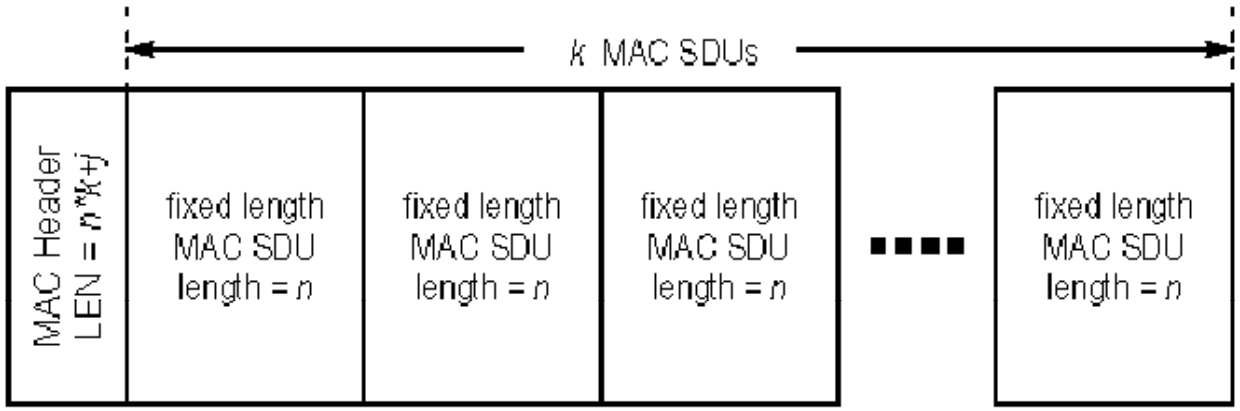
Packing: process of combining multiple MAC SDUs into a single MAC PDU

- with variable length MAC SDUs, packed PDU contains a 2-byte sub-header for each packed SDU (or fragment thereof):
  - Length of the SDU: 11 bits
  - 2 bits fragmentation control (FC): 2 bits
  - fragmentation sequence number (FS): 3 bits
- with fixed length MAC SDUs, no packing sub-header needed

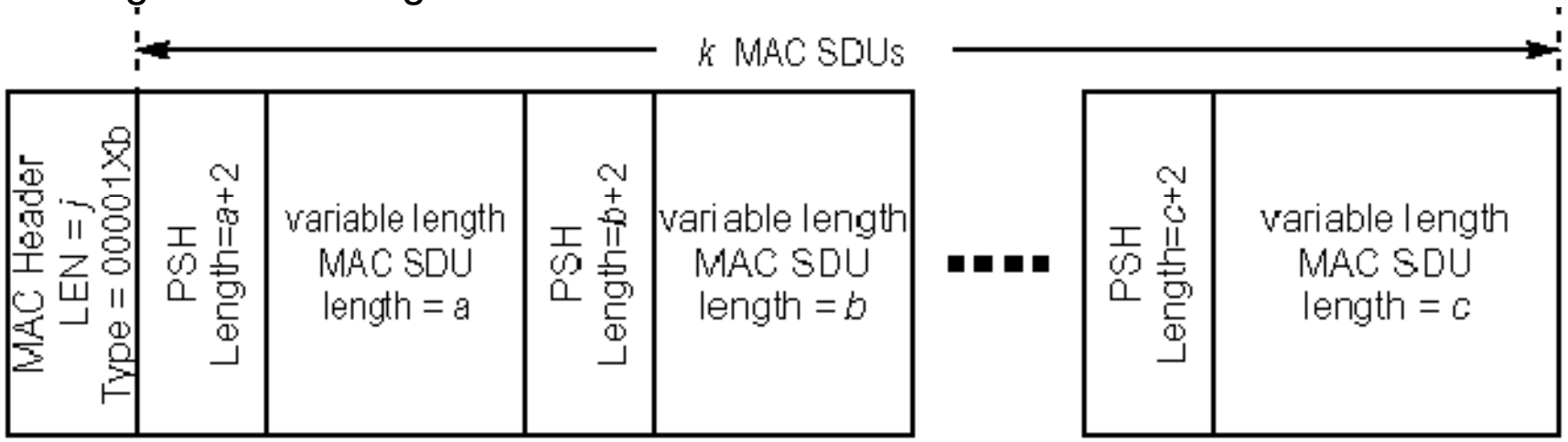
Packing and fragmentation can be combined to save system bandwidth

Packing Examples

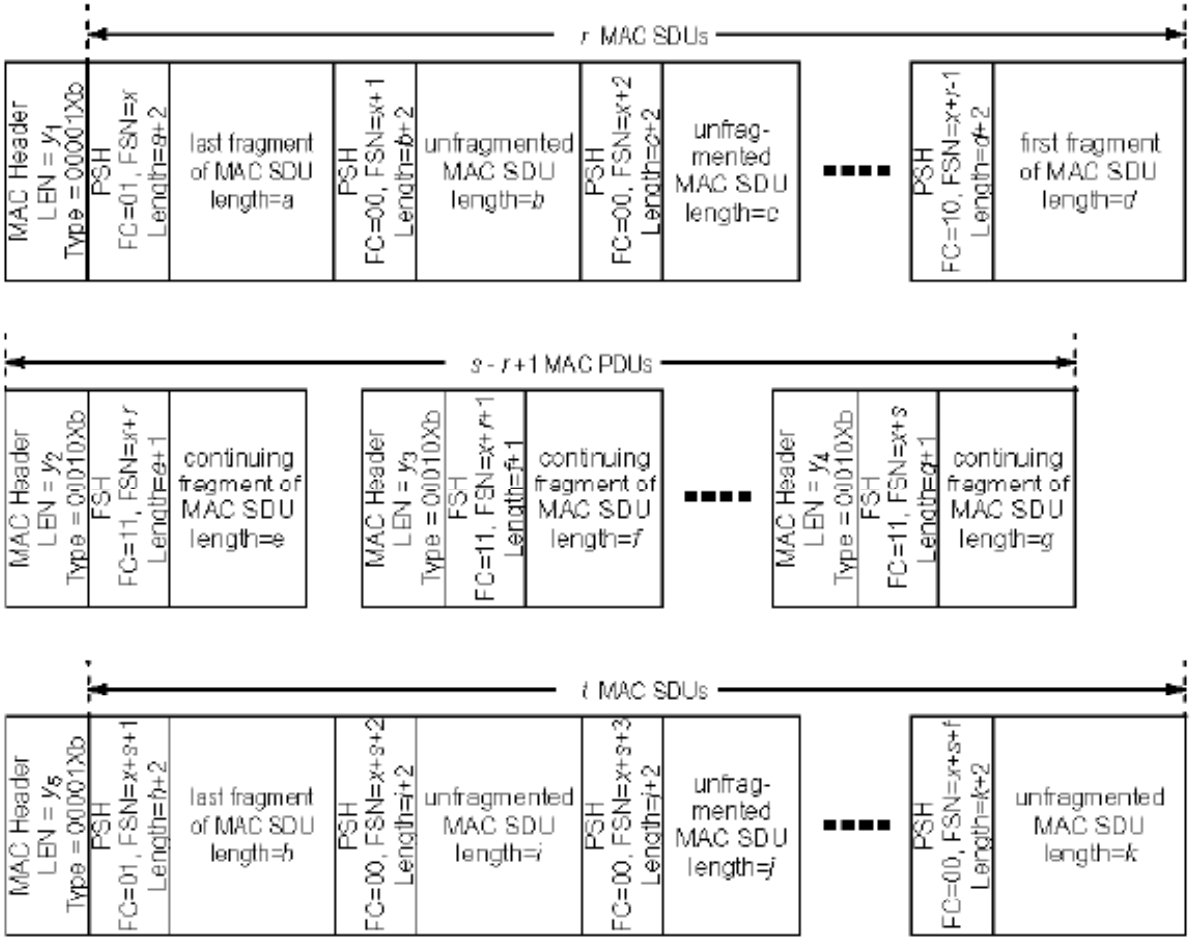
Packing Fixed-Length SDUs



Packing Variable-Length SDUs



Packing with Fragmentation: example



DOWNLINK TRANSMISSION

- Two kinds of bursts: TDM and TDMA, identified by a DIUC (Downlink Interval Usage Code)
- TDMA bursts have resync preamble
- Each terminal listens to all bursts at its operational IUC, or at a more robust one, except when told to transmit
- Each burst may contain data for several terminals
- SS must recognize the PDUs with known CIDs

Downlink Map (DL-MAP) message defines usage of downlink and contains carrier-specific data

- DL-MAP is first message in each frame
- Decoding very time-critical typically done in hardware
- Entries denote instants when the burst profile changes

Downlink Channel Descriptor: Used for advertising downlink burst profiles

- Each burst profile has mandatory exit threshold and minimum entry threshold
- Burst profile of DL broadcast channel is well-known
- All others are acquired
- Burst profiles can be changed on the fly without interrupting the service interrupting the service
- Not intended as 'super-adaptive' modulation
- Establishes association between DIUC and actual PHY parameters

UPLINK TRANSMISSION

- Transmissions in contention slots:
  - Bandwidth requests
  - Transmissions in initial ranging slots Ranging Requests (RNG-REQ)
  - Contention resolved using truncated exponential backoff

Bursts defined by UIUCs:

- Transmissions allocated by the UL-MAP message
- All transmissions have synchronization preamble
- Ideally, all data from a single SS is concatenated into a single PHY burst

Uplink Channel Descriptor regularly sent to defines uplink burst profiles

- All Uplink Burst profiles are acquired
- Burst profiles can be changed on the fly
- Establishes association between UIUC and actual PHY parameters

Uplink Map (UL-MAP) message defines usage of the uplink. It contains the "grants" addressed to the SS

- Time given in **mini-slots**:
  - **mini-slot** (in terms of an integer of physical slots) is the unit of uplink bandwidth allocation
  - in 10-66 GHz PHY, physical slot is 4 symbols
  - Time expressed as arrival time at BS

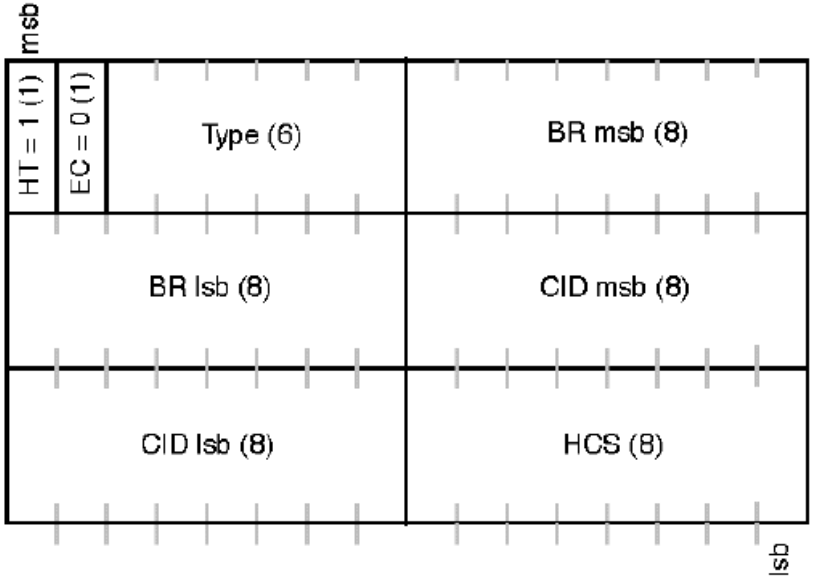
Request/Grant Scheme

- Self Correcting
- No acknowledgement
- Grants (given as durations durations) are carried in the UL-MAP messages
- SS needs to convert the time to amount of data using information about the UIUC
- Bandwidth Requests are always per Connection
- Grants are either per Connection (GPC) or per Subscriber Station (GPSS)
- Bandwidth Grant per Subscriber Station (GPSS)
  - Base station grants bandwidth to the subscriber station
  - Subscriber station may re-distribute bandwidth among its connections, maintaining QoS and service-level agreements
  - Suitable for many connections per terminal; off-loading base station's work
  - Allows more sophisticated reaction to QoS needs
  - Low overhead but requires intelligent subscriber station
  - Mandatory for P802.16 10-66 GHz PHY
- Bandwidth Grant per Connection (GPC)
  - Base station grants bandwidth to a connection
  - Mostly suitable for **few users** per subscriber station
  - Higher overhead, but allows simpler subscriber station

Bandwidth Request

- Come from the Connection
- Several kinds of requests:
  - Implicit requests (UGS): No actual messages, negotiated at connection setup
  - BW request messages : Uses the special BW request header
- Requests up to 32 KB with a single message
- Incremental or aggregate, as indicated by MAC header
- Piggybacked request (for non-UGS services only)
- Presented in GM sub-header and always incremental
- Up to 32 KB per request for the CID
- Poll-Me bit (for UGS services only)

- Used by the SS to request a bandwidth poll for non-UGS services
  - HT: Header Type
  - EC: Encryption Control
  - Type: subheaders, etc.
  - BR: Bandwidth req, in bytes (64k max)
  - CID: Connection ID
  - EKS: Encryption Key Sequence
  - HCS: Header Check Sequence



Maintaining QoS in GPSS

- Semi-distributed approach
- BS sees the requests for each connection; based on this, grants bandwidth (BW) to the SSs (maintaining QoS and fairness)
- SS scheduler maintains QoS among its connections and is responsible to share the BW among the connections (maintaining QoS and fairness)
- Algorithm in BS and SS can be very different; SS may use BW in a way unforeseen by the BS

SS Initialization & Ranging

Initialization

- Scan for downlink channel and establish synchronization with the BS
- Obtain transmit parameters (from UCD message)
- Perform ranging
- Negotiate basic capabilities
- Authorize SS and perform key exchange
- Perform registration
- Establish IP connectivity
- Establish time of day
- Transfer operational parameters
- Set up connections

Ranging

- For uplink transmissions, times are measured at BS
- At startup, SS sends a RNG-REQ in a ranging window
- BS measures arrival time and signal power; calculates required advance and power adjustment
- BS sends adjustment in RNG-RSP
- SS adjusts advance and power; sends new RNG-REQ Loop is continued until power and timing is ok

Registration & Connection

Registration: a form of capability negotiation

- SS sends a list of capabilities and parts of the configuration file to the BS in the REG-REQ message
- BS replies with the REG-RSP message tells which capabilities are supported/allowed tells
- SS acknowledges the REG-RSP with REG-ACK message

Initial Connection Setup:

- In multiple DSA-REQ messages, BS passes to the SS Service Flow Encodings containing either
  - full definition of service attributes (omitting defaultable items if desired)
  - service class name (ASCII string which is known at the BS and which indirectly specifies a set of QoS Parameters)
- SS replies with DSA-RSP messages

IP connectivity and configuration file download:

- IP connectivity established via DHCP
- Configuration file downloaded via TFTP contains provisioned information & operational parameters

Privacy and Security

- Secures over-the-air transmissions
- Designed to allow new/multiple encryption algorithms
- Authentication
  - X.509 certificates with RSA
  - Strong authentication of SSs (prevents theft of service)
  - Prevents cloning
- Data encryption
  - Currently 56-bit DES in CBC (cypher block chaining) mode
  - Initialization Vector (IV) based on frame number
- Message authentication
- Most important MAC management messages authenticated with one-way hashing (HMAC with SHA-1)

Security Associations

- A set of privacy information shared by a BS and one or more of its client SSs in order to support secured communications
- possibility of multicast SA's including Traffic Encryption Keys (TEKs) and CBC IVs
- Security Association Establishment
  - Primary SA established during initial registration
  - other SAs may be provisioned or dynamically created within the within the BS

SS Authorization

- **Authentication and Authorization:**
  - SS manufacturer's X.509 certificate binds the SS's public key to its other identifying information
  - Trust relation assumed between equipment manufacturer and network operator
  - Possibility to accommodate "root authority" if required
- **Authorization Key Update Protocol:**
  - The SS is responsible for maintaining valid keys
  - Two active AKs with overlapping lifetimes at all times
  - Reauthorization process done periodically: AK lifetime (7 days) & grace time timer (1 hr)

Encryption

Traffic Encryption Key Management:

- Authoriztion Key (AK) established with RSA
- Key Encryption Key (symmetric) derived from AK
- Encryption Keys (TEK) exchanged with symmetric algorithm negotiated at SA establishment (currently only 3-DES supported)
- Two sets of overlapping keying material maintained
- No explicit key acknowledgements
- Key synchronization maintained by 2-bit key sequence number in the MAC PDU header

Data Encryption:

- DES in CBC mode with IV derived from the frame number
- Hooks defined for other stronger algorithms, e.g. AES
- Two simultaneous keys with overlapping and offset lifetimes allow for uninterrupted service
- Key sequence number carried in MAC header
- Only MAC PDU payload (including sub-headers) is encrypted
- Management messages are unencrypted