The 802.16 WirelessMAN™ MAC: It's Done, but What Is It?

creating the IEEE 802.16 WirelessMAN™ Standard for Wireless Metropolitan Area Networks

http://WirelessMAN.org

Presentation Authors

- Roger B. Marks, NIST (Chair, 802.16)
- Carl Eklund, Nokia (802.16 TG1 MAC Chair)
- Ken Stanwood, Ensemble Communications
- Stanley Wang, Ensemble Communications

Outline

- Overview: IEEE 802.16 Air Interface Standard
  - P802.16: Air Interface (MAC and 10 - 66 GHz PHY)
  - P802.16a: Amendment, 2-11 GHz (licensed)
  - P802.16b: Amendment, (license-exempt)
- PHY considerations in the 802.16 MAC
- The 802.16 MAC as defined in P802.16/D5
- MAC Enhancements under development

IEEE 802.16 History

- Sponsors
  - IEEE Computer Society
  - IEEE Microwave Theory and Techniques Society
- Project Development: Summer 1998
- IEEE 802 Tutorial: November 1998
- IEEE Study Group
  - November 1998-March 1999

- Session #1: July 1999
- Session #16: November 2001

IEEE 802.16 by the Numbers

- 163 Members
- 67 “Potential Members”
- 62 Official Observers
- 700 different individuals have attended a session
- 2.8 Million file downloads in year 2000
- Members and Potential Members from
  - 10 countries
  - >110 companies

IEEE 802.16 Projects

- **Air Interface (PHYs with common MAC)**
  - **P802.16: 10-66 GHz**
    - Completed IEEE Sponsor Ballot
    - On RevCom agenda for December 5, 2001
  - **P802.16a: 2-11 GHz**
    - Licensed bands only
    - Expect OK to launch WG Letter Ballot this week
  - **P802.16b: 5-6 GHz**
    - License-exempt ("WirelessHUMAN™")
    - Expect OK to launch WG Letter Ballot this week
- **Coexistence**
  - **IEEE 802.16.2 (10-66 GHz)**
    - Published in September 2001
  - **P802.16.2a: amendment w/ 2-11 GHz licensed**

IEEE P802.16

Standard Air Interface for Fixed Broadband Wireless Access Systems

IEEE P802.16 History

- July-September, 1999: Functional Requirements
- November 1999: Proposals (14 for MAC)
- January 2000: 2 Consolidated Proposals
  - 1 MAC proposal based on DOCSIS
  - 1 not
- May 2000: Plan to Merge 2 Proposals
- August 2000: Rev. 0
- until February 2001: Working Group Review
  - formal comment process
- February-August 2001: WG Letter Ballot
- August-October 2001: IEEE Sponsor Ballot
- 5 December 2001: RevCom approval agenda

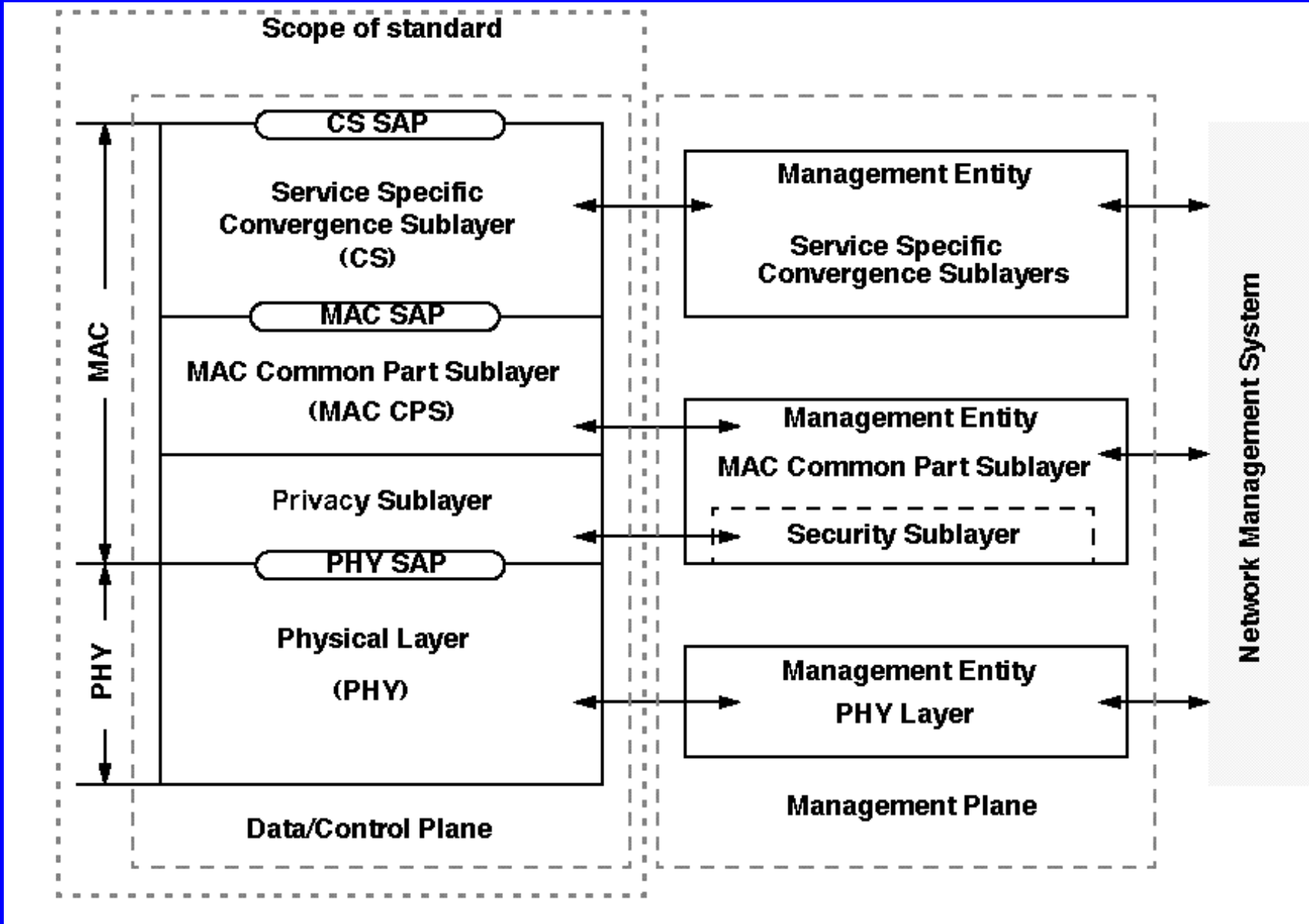
P802.16 Scope

Specifies the air interface, including the medium access control layer (MAC) and physical layer (PHY), of fixed point-to-multipoint broadband wireless access systems providing multiple services. The medium access control layer is capable of supporting multiple physical layer specifications optimized for the frequency bands of the application. The standard includes a particular physical layer specification broadly applicable to systems operating between 10 and 66 GHz.

Point-to-Multipoint Wireless MAN: not a LAN

- Base Station (BS) connected to public networks
- BS serves Subscriber Stations (SSs)
  - BS and SS are stationary
  - SS typically serves a building (business or residence)
  - provide SS with first-mile access to public networks
- Multiple services, with different QoS priority, simultaneously

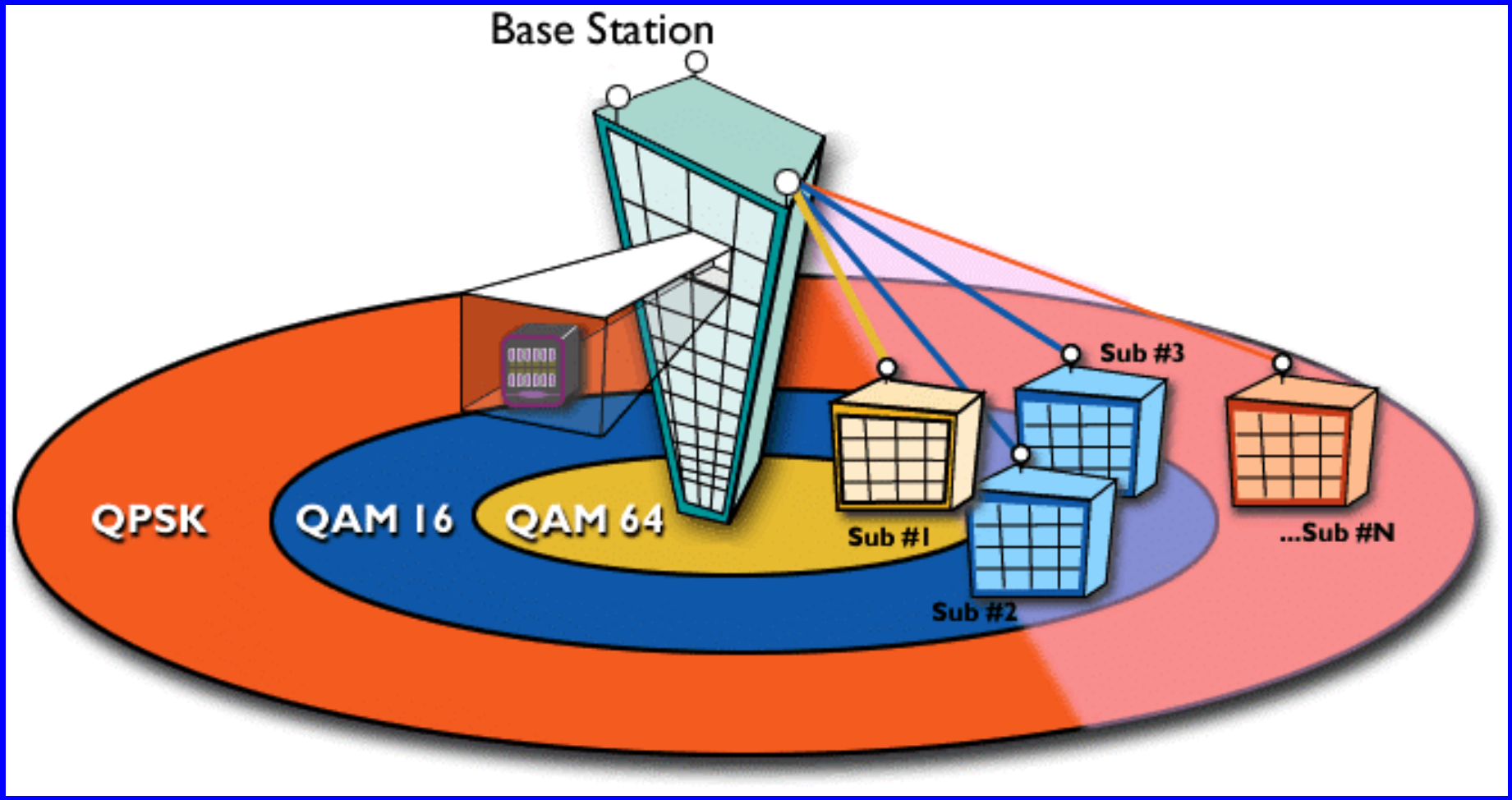
Reference Model



PHY Considerations that Effect the MAC (10-66 GHz)

- Broadband Channels
  - Wide channels (20, 25, or 28 MHz)
  - High capacity – Downlink **AND** Uplink
- Multiple Access
  - TDM/TDMA
  - High rate burst modems
- Adaptive Burst Profiles on Uplink and Downlink
- Duplex scheme agnostic
  - Time-Division Duplex (TDD)
  - Frequency-Division Duplex (FDD) [including Burst FDD]
    - Support for Half-Duplex Terminals

Adaptive PHY



(burst-by-burst adaptivity not shown)

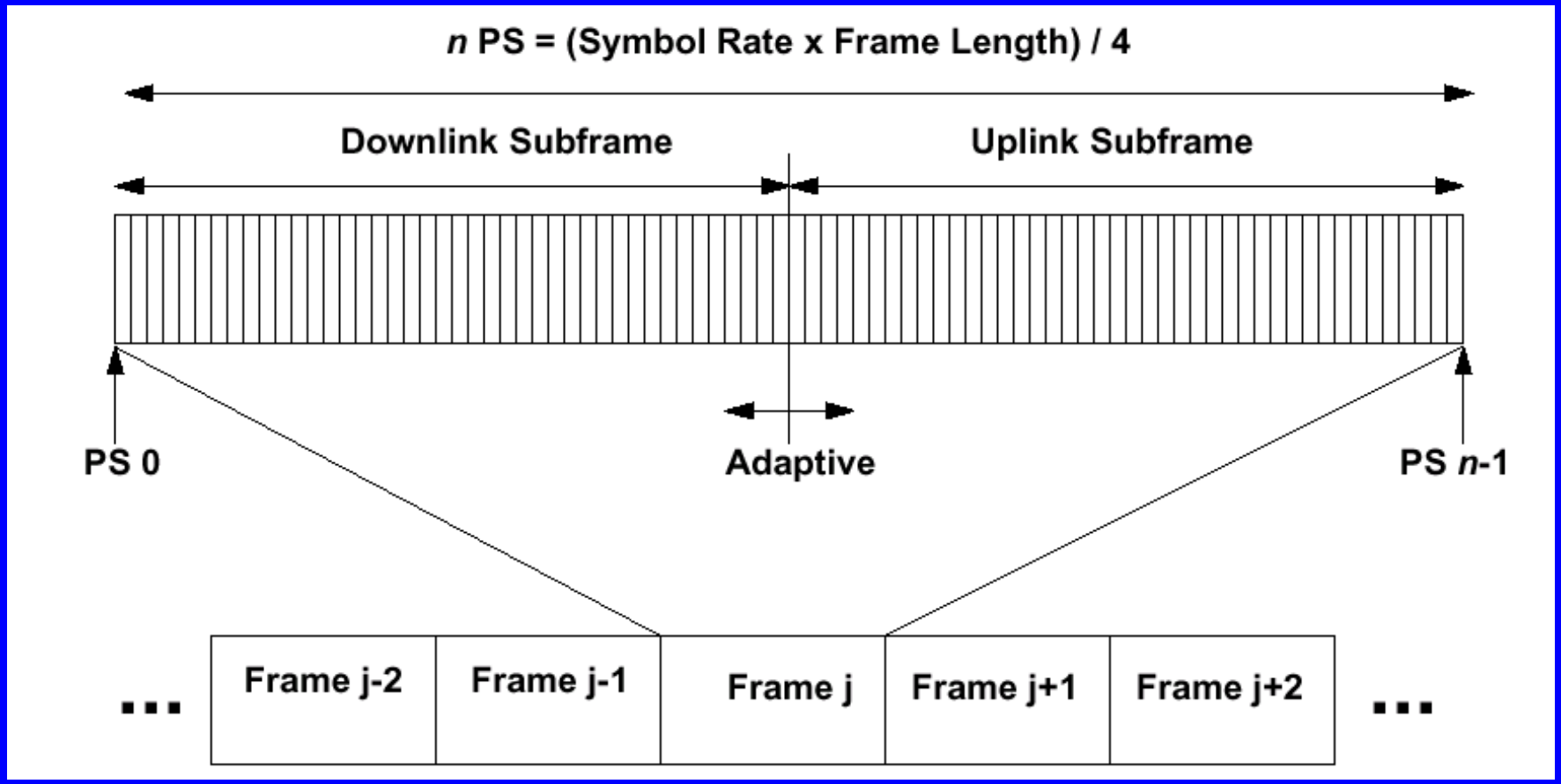
Adaptive Burst Profiles

- Burst profile
  - Modulation and FEC
- Dynamically assigned according to link conditions
  - Burst by burst, per subscriber station
  - Trade-off capacity vs. robustness in **real time**
- Roughly doubled capacity for the same cell area
- Burst profile for downlink broadcast channel is well-known
  - All other burst profiles could be configured “on the fly”
  - Subscriber station capabilities recognized at registration

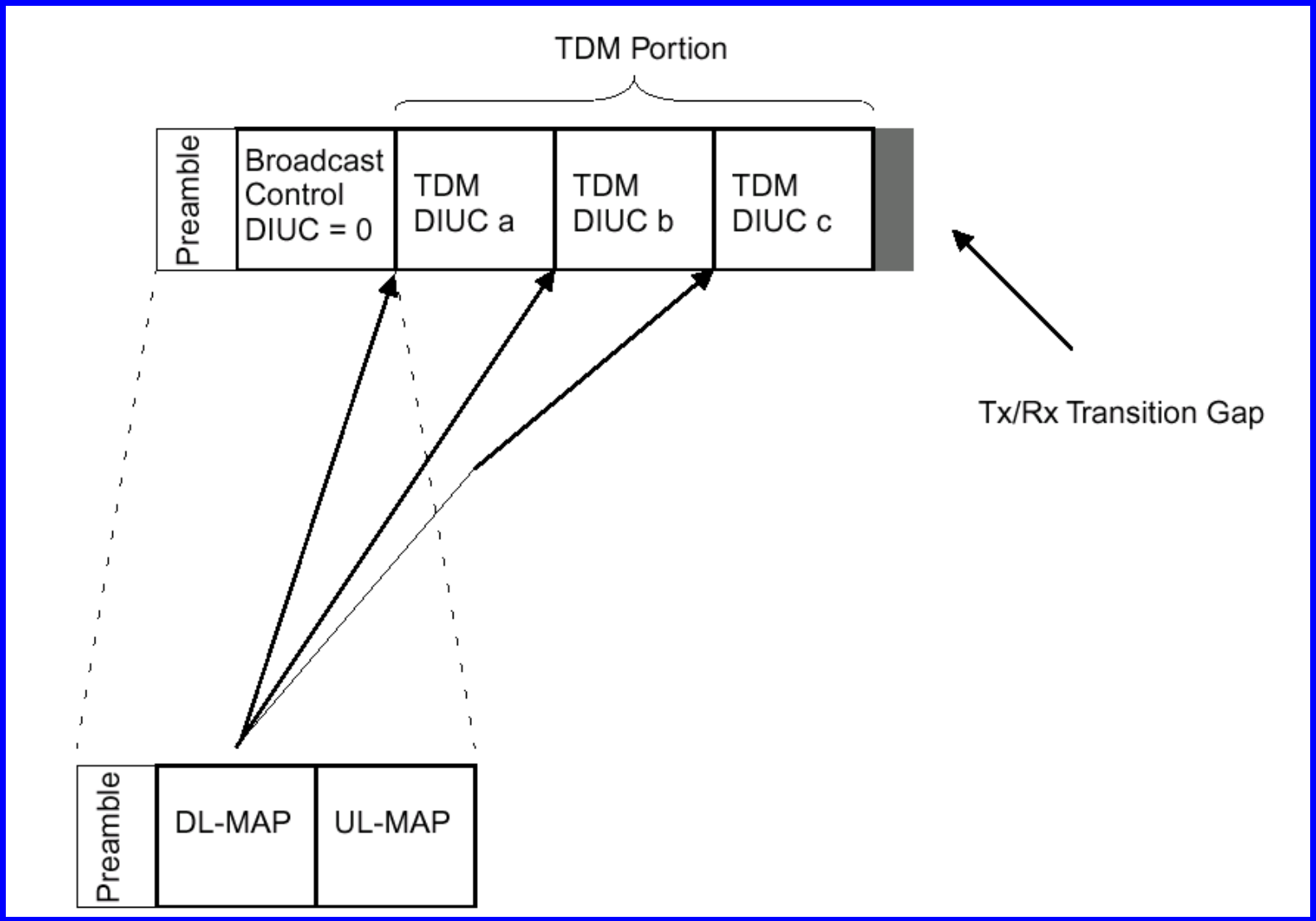
Duplex Scheme Support

- On downlink, SS is associated with a specific burst
- On uplink, SS is allotted a variable length time slot for their transmissions
- Time-Division Duplex (TDD)
  - Downlink & Uplink time share the same RF channel
  - Dynamic asymmetry
  - SS does not transmit & receive simultaneously (low cost)
- Frequency-Division Duplex (FDD)
  - Downlink & Uplink on separate RF channels
  - Static asymmetry
  - Half-duplex SSs supported
    - SS does not transmit & receive simultaneously (low cost)

TDD Frame (10-66 GHz)

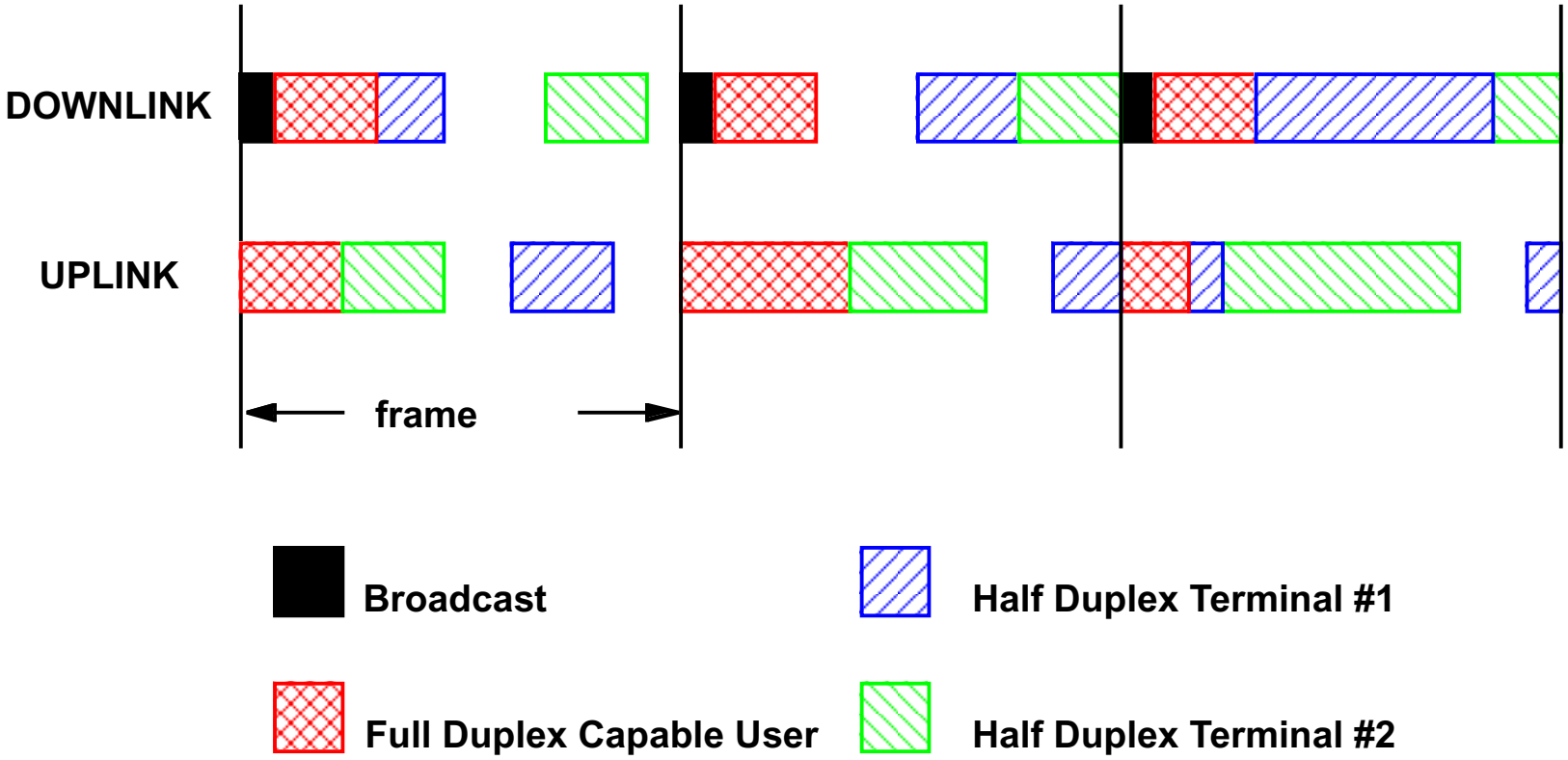


TDD Downlink Subframe



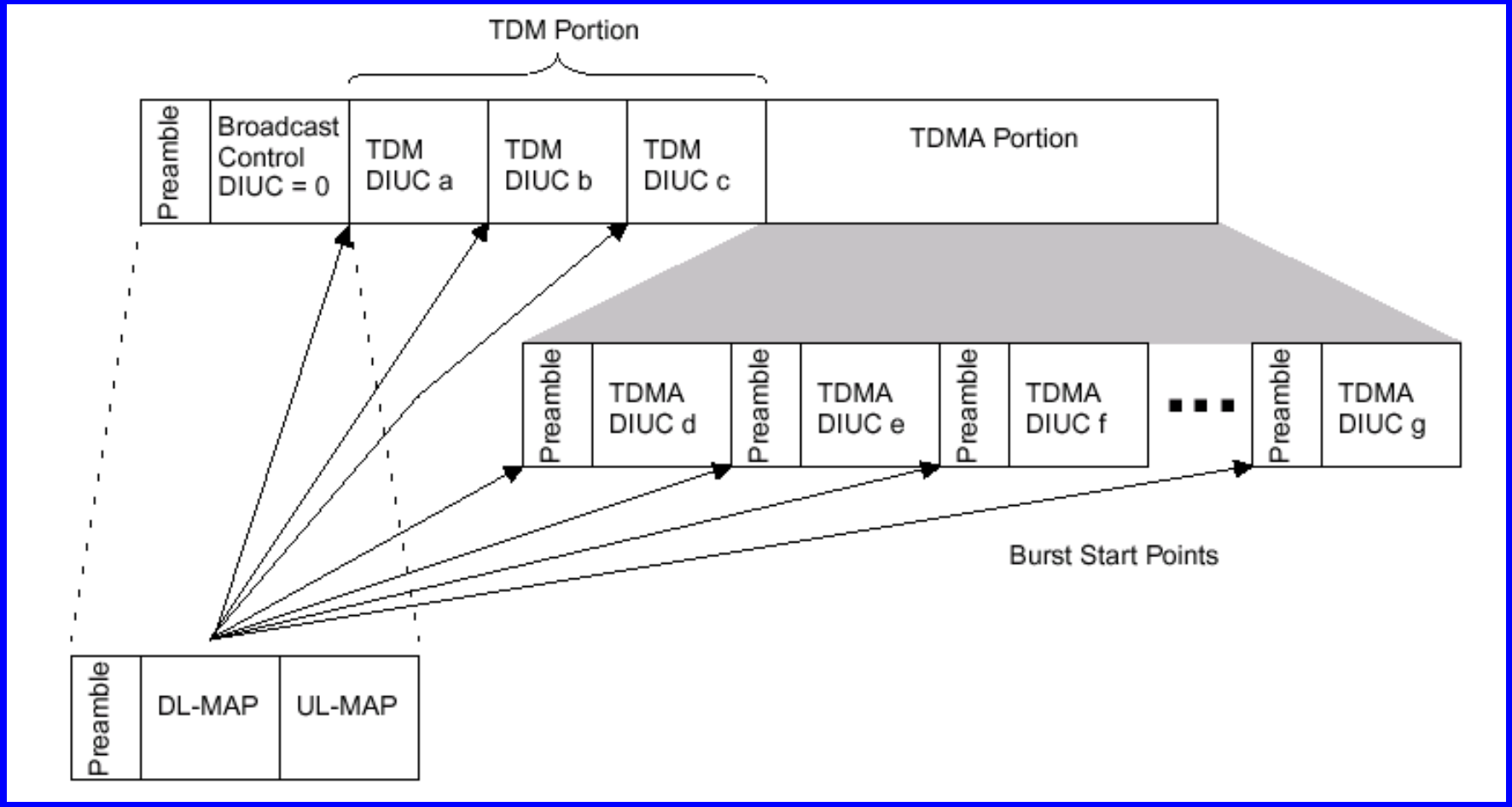
DIUC: Downlink Interval Usage Code

Burst FDD Framing



Allows scheduling flexibility

FDD Downlink Subframe



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

- Need preamble to re-sync (carrier phase)

Baud Rates & Channel Size (10-66 GHz)

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

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

MAC Requirements

- Provide Network Access
- Address the **Wireless** environment
  - e.g., very efficient use of spectrum
- Broadband services
  - Very high bit rates, downlink and uplink
  - A range of QoS requirements
  - Ethernet, IPv4, IPv6, ATM, ...
- Likelihood of terminal being shared
  - Base Station may be heavily loaded
- Security
- Protocol-Independent Engine
  - Convergence layers to ATM, IP, Ethernet, ...
- Support both TDD and FDD in the PHY

802.16 MAC: Overview

- Point-to-Multipoint
- Metropolitan Area Network
- Connection-oriented
- Supports difficult user environments
  - High bandwidth, hundreds of users per channel
  - Continuous and burst traffic
  - Very efficient use of spectrum
- Protocol-Independent core (ATM, IP, Ethernet, …)
- Balances between stability of contentionless and efficiency of contention-based operation
- Flexible QoS offerings
  - CBR, rt-VBR, nrt-VBR, BE, with granularity within classes
- Supports multiple 802.16 PHYs

Relationship to DOCSIS

- Management
  - Dynamic service “editing” protocol (Add/Change/Delete)
  - Management message payload format
- Security
  - Authentication and Privacy
- Polling categories
- Initial Access
  - Slightly modified allowing terminal capability negotiation

- Core MAC protocol engine is new design for Wireless Metropolitan Area Networks

Definitions

- **Service Data Unit (SDU)**
  - Data units exchanged between adjacent layers
- **Protocol Data Unit (PDU)**
  - Data units exchanged between peer entities
- **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 unidirectional flow of MAC PDUs on a connection that provides a particular QoS (uniquely identified by a SFID)

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
  - etc.

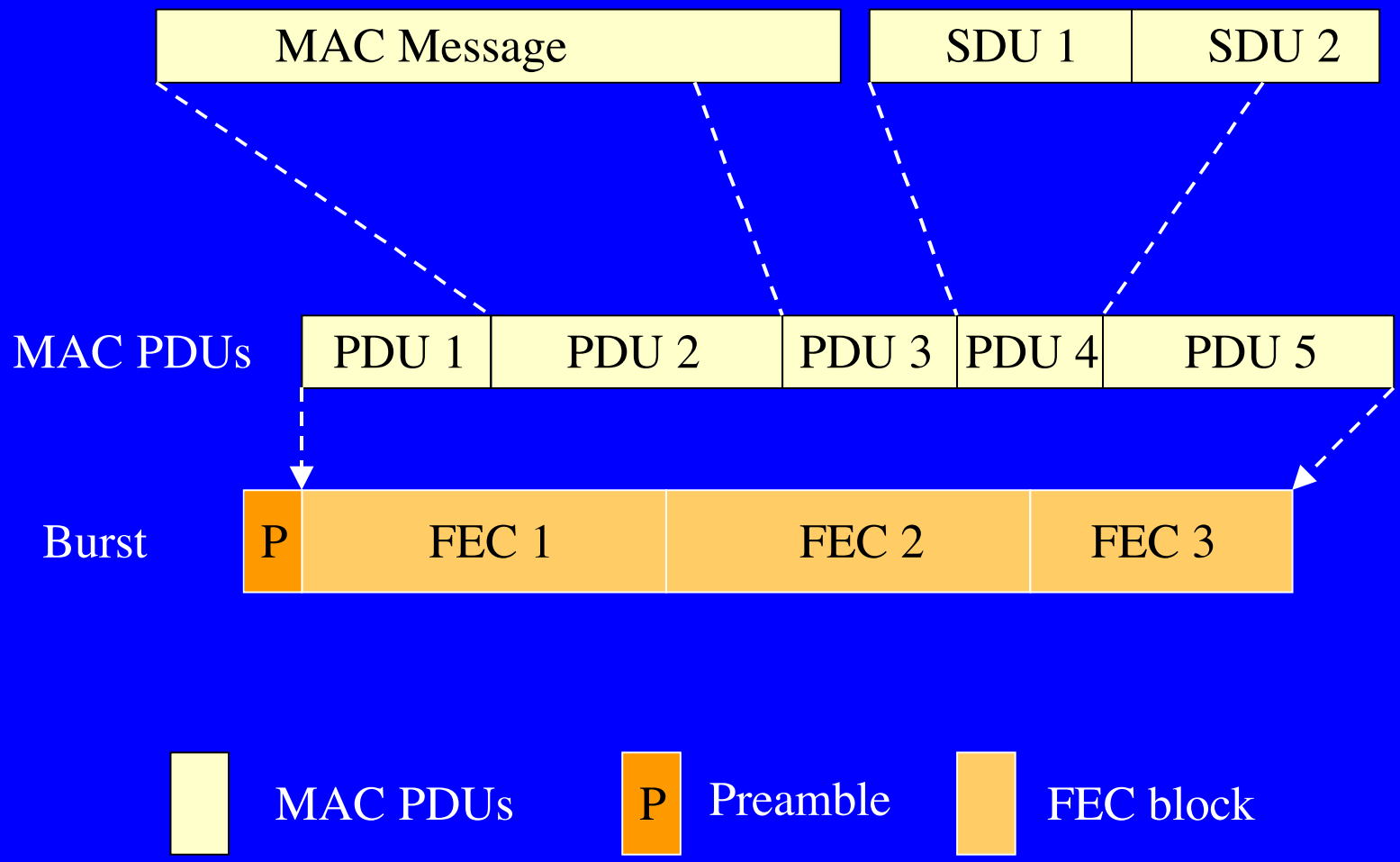
MAC Addressing

- 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

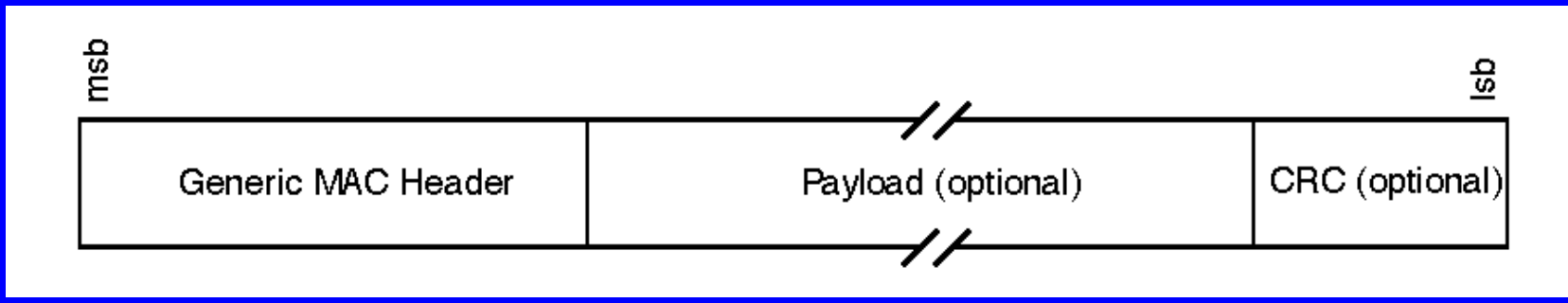
MAC PDU Transmission

- MAC PDUs are transmitted in PHY bursts
- A single PHY burst can contain multiple *Concatenated* MAC PDUs
- The PHY burst can contain multiple FEC blocks
- MAC PDUs may span FEC block boundaries
- The TC 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 Transmission

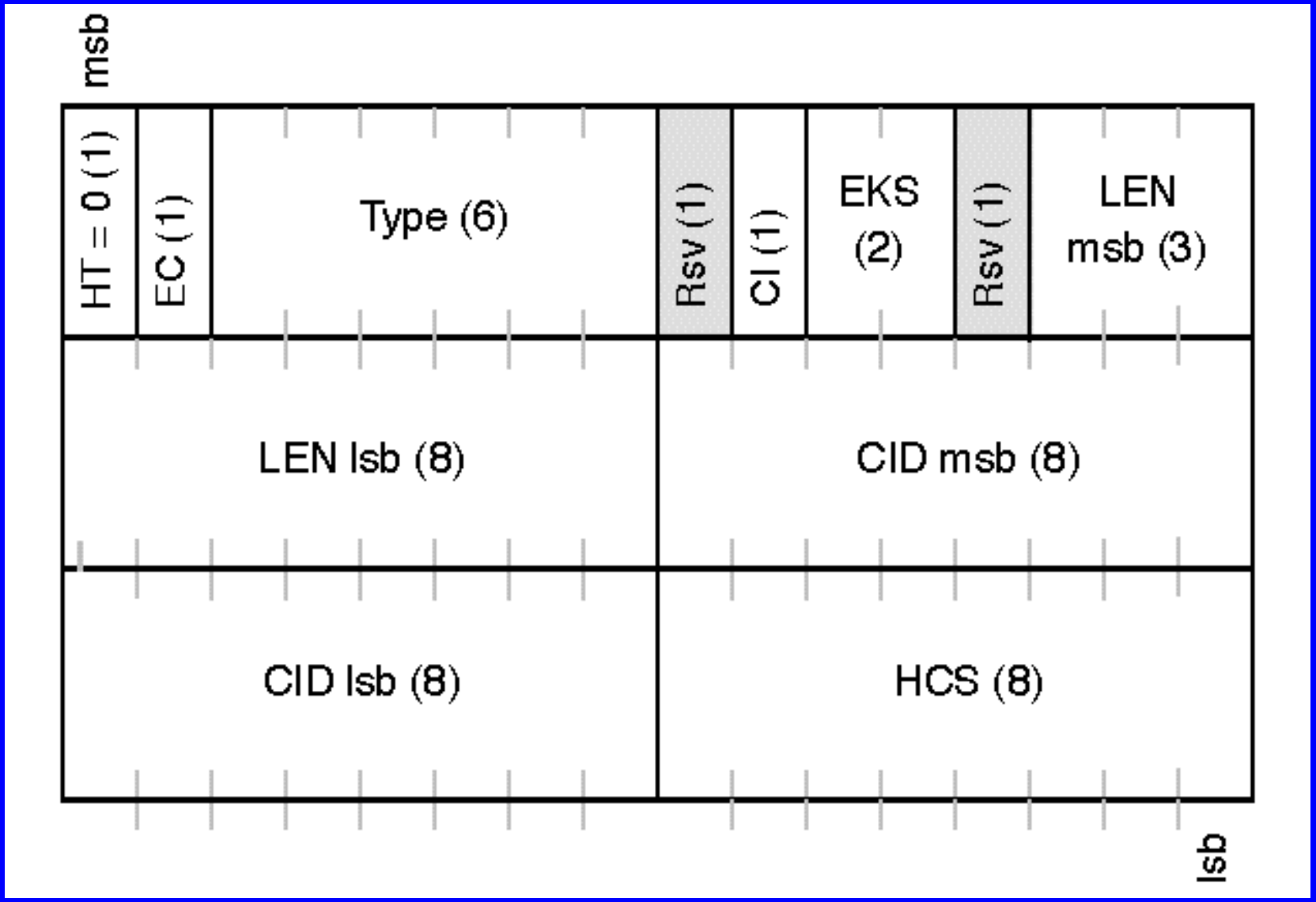


MAC PDU format



- The Generic MAC header has fixed 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



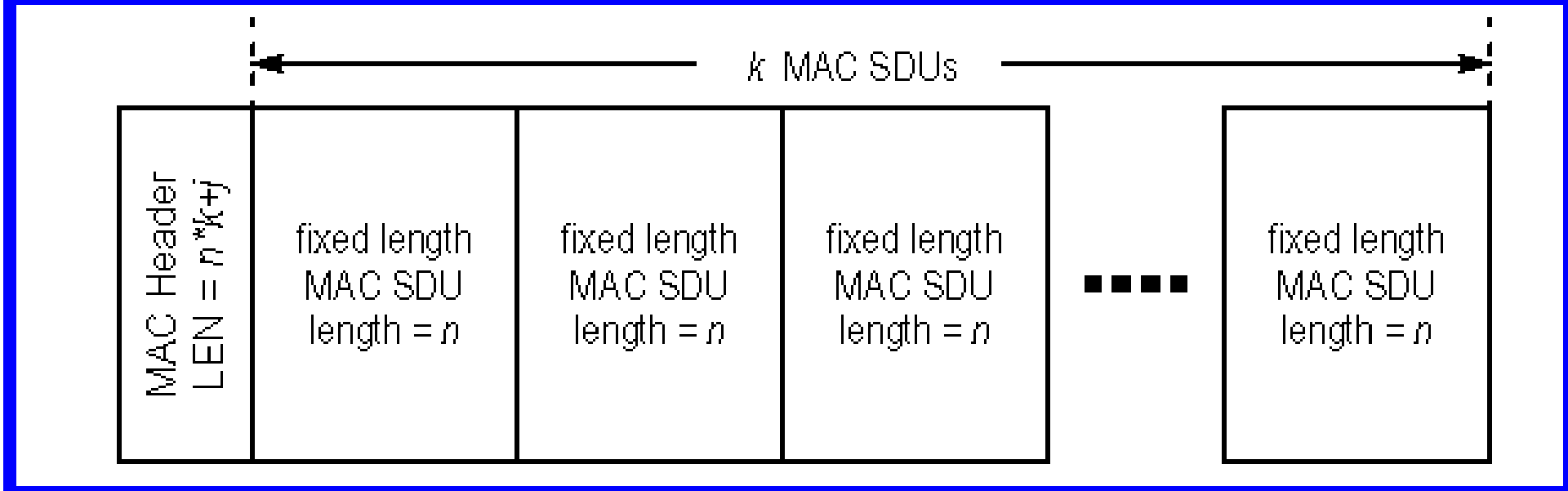
Fragmentation

- Partitioning a MAC SDU into fragments transported in multiple MAC PDUs
- Each connection can be in only a single fragmentation state at any time
- 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

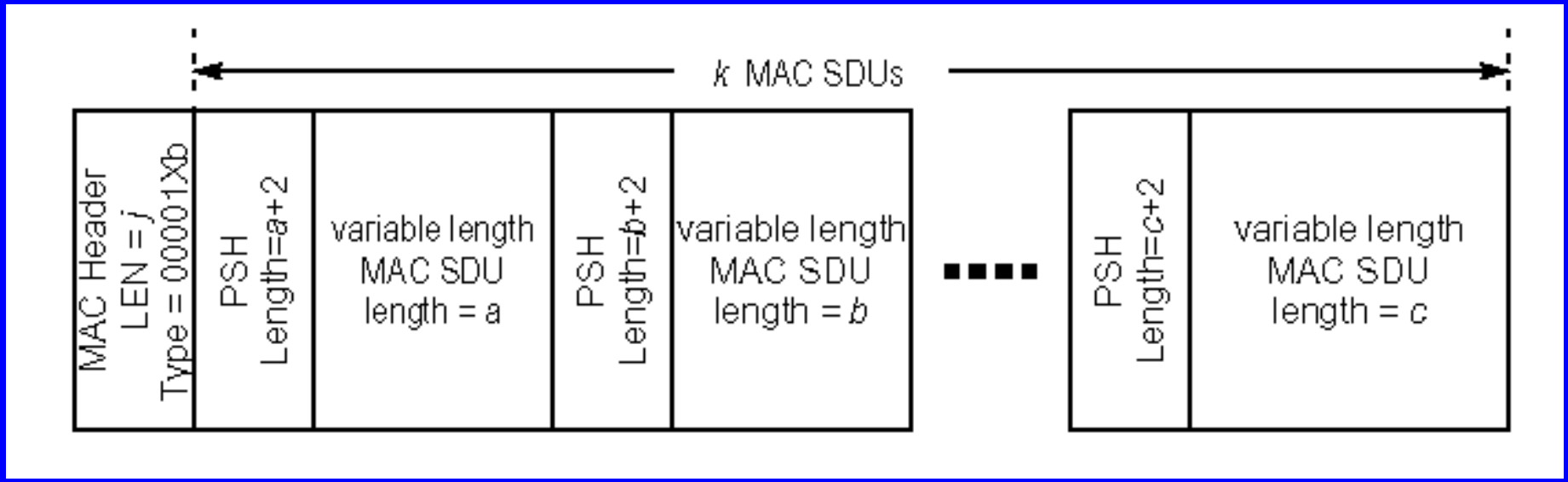
Packing

- The process of combining multiple MAC SDUs (or fragments thereof) into a single MAC PDU
- On connections with variable length MAC SDUs
  - Packed PDU contains a sub-header for each packed SDU (or fragment thereof)
- On connections with fixed length MAC SDUs
  - No packing sub-header needed
- Packing and fragmentation can be combined
- Can, in certain situations, save up to 10% of system bandwidth

Packing Fixed-Length SDUs

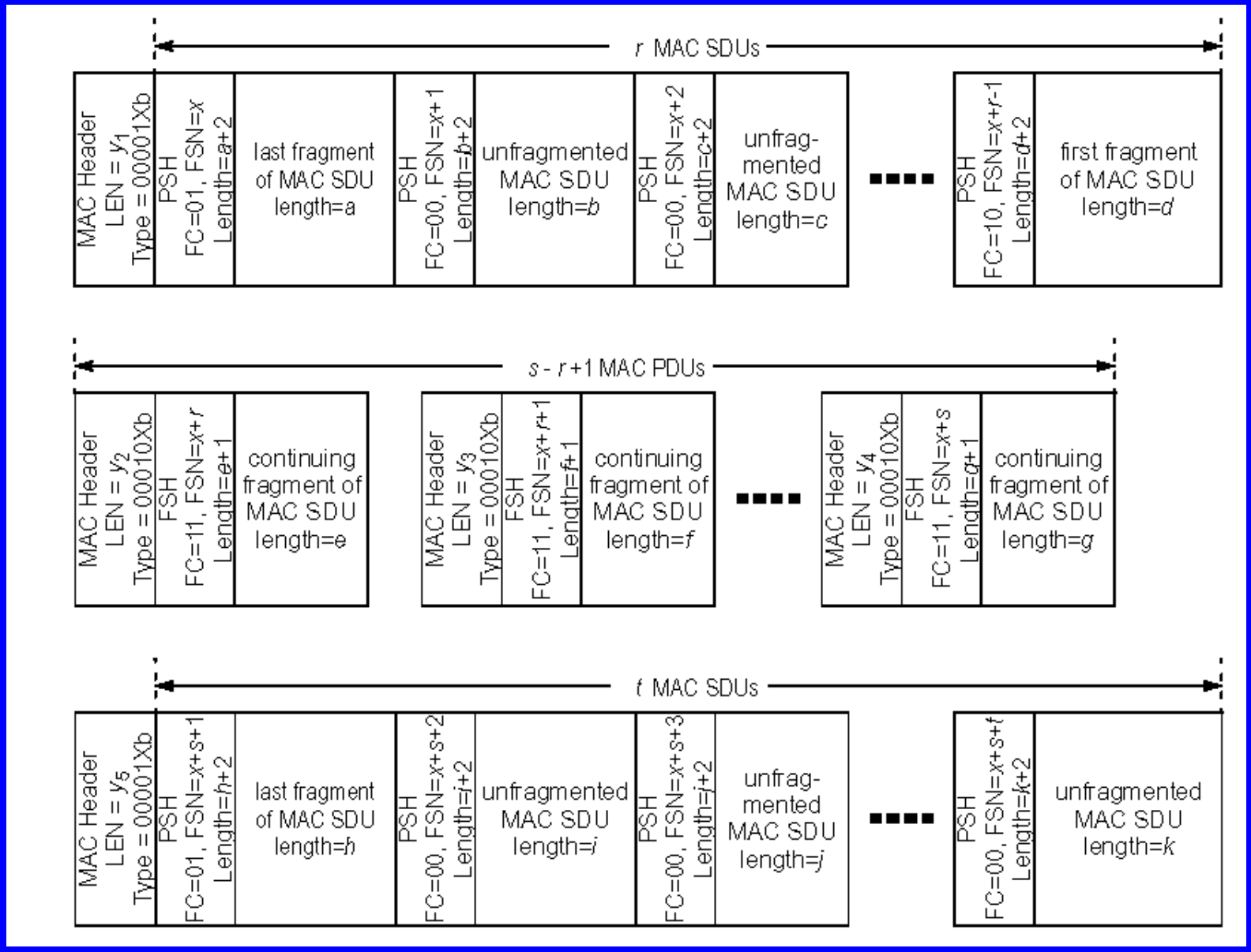


Packing Variable-Length SDUs



- 2 Byte Packing Sub-Header before each SDU
  - Length of the SDU: 11 bits
  - fragmentation control (FC): 2 bits
  - fragmentation sequence number (FS): 3 bits

Packing with Fragmentation



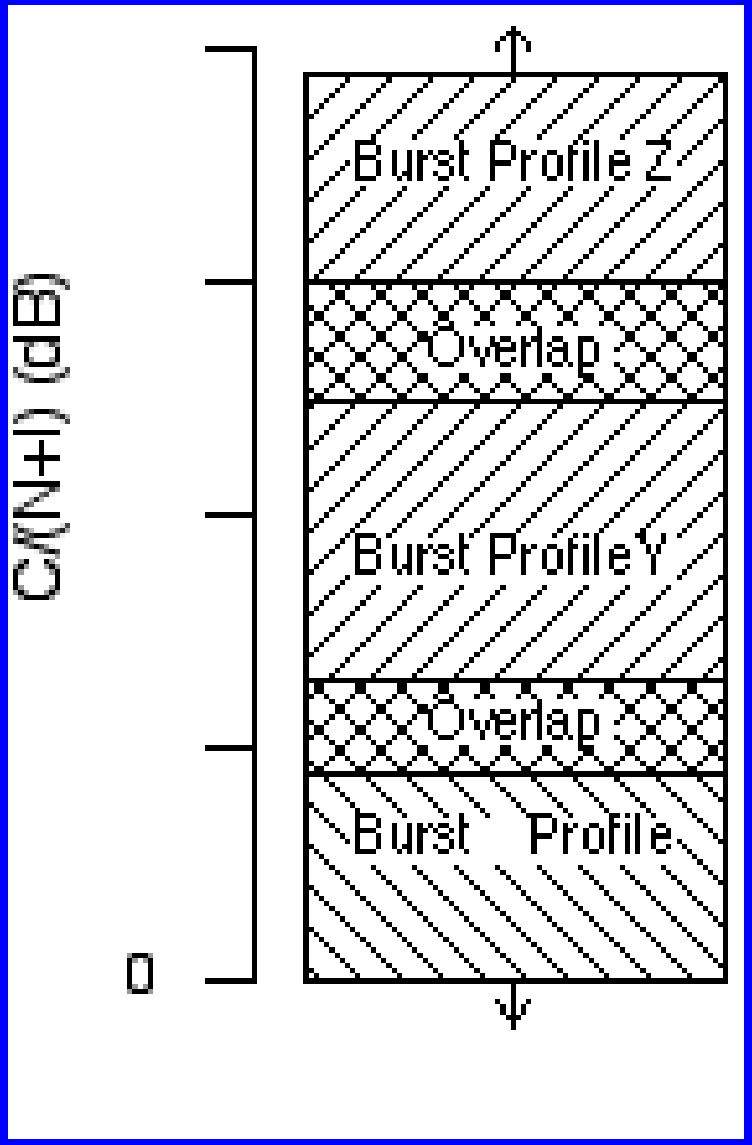
Downlink transmissions

- Two kinds of bursts: TDM and TDMA
- All bursts are identified by a DIUC
  - Downlink Interval Usage Code
- TDMA bursts have resync preamble
  - allows for more flexible scheduling
- 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
- DL-MAP message signals downlink usage

Downlink Channel Descriptor

- Used for advertising downlink burst profiles
- 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
  - Not intended as 'super-adaptive' modulation
- Establishes association between DIUC and actual PHY parameters

Burst profiles



- Each burst profile has mandatory exit threshold and minimum entry threshold
- SS allowed to request a less robust DIUC once above the minimum entry level
- SS must request fall back to more robust DIUC once at mandatory exit threshold
- Requests to change DIUC done with DBPC-REQ or RNG-REQ messages

Downlink Map Message

- 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

Uplink Transmissions

- Invited transmissions
- Transmissions in contention slots
  - Bandwidth requests
  - Contention resolved using truncated exponential backoff
- 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

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

Uplink MAP Message

- UL-MAP message defines usage of the uplink
- Contains the "grants"
- Grants addressed to the SS
- Time given in mini-slots
  - unit of uplink bandwidth allocation
  - 2^m physical slots
    - in 10-66 GHz PHY, physical slot is 4 symbols
- Time expressed as arrival time at BS

Classes of Uplink Service

Characteristic of the Service Flow

- Unsolicited Grant Services (UGS)
  - for constant bit-rate (CBR) or CBR-like service flows (SFs) such as T1/E1
- Real-time Polling Services (rtPS)
  - for rt-VBR-like SFs such as MPEG video
- Non-real-time Polling Services (nrtPS)
  - for nrt SFs with better than best effort service such as bandwidth-intensive file transfer
- Best Effort (BE)
  - for best-effort traffic

Uplink 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).

Uplink Services - rtPS

- Intended for rt-VBR-like service flows such as MPEG video
- Prohibited from using any contention requests
- Terminals polled frequently enough to meet the delay requirements of the SFs
- Bandwidth requested with BW request messages (a special MAC PDU header)
- May use Grant Management sub-header
  - new request can be piggybacked with each transmitted PDU

Uplink Service - nrtPS

- Intended for non-real-time service flows with better than best effort service
  - e.g. bandwidth-intensive file transfer
- Works like rt-polling except that polls are issued less frequently
- Allowed to use contention requests
- May use Grant Management sub-header
  - new request can be piggybacked with each transmitted PDU

Uplink Service - BE

- Generic data
  - e.g. HTTP, SMTP, etc.
- No QoS guarantees
- Allowed to use contention requests
- May use Grant Management sub-header
  - new request can be piggybacked with each transmitted PDU

Request/Grant Scheme

- Self Correcting
  - No acknowledgement
  - All errors are handled in the same way, i.e., periodical aggregate requests
- Bandwidth Requests are always per Connection
- Grants are either per Connection (GPC) or per Subscriber Station (GPSS)
  - Grants (given as durations) are carried in the UL-MAP messages
  - SS needs to convert the time to amount of data using information about the UIUC

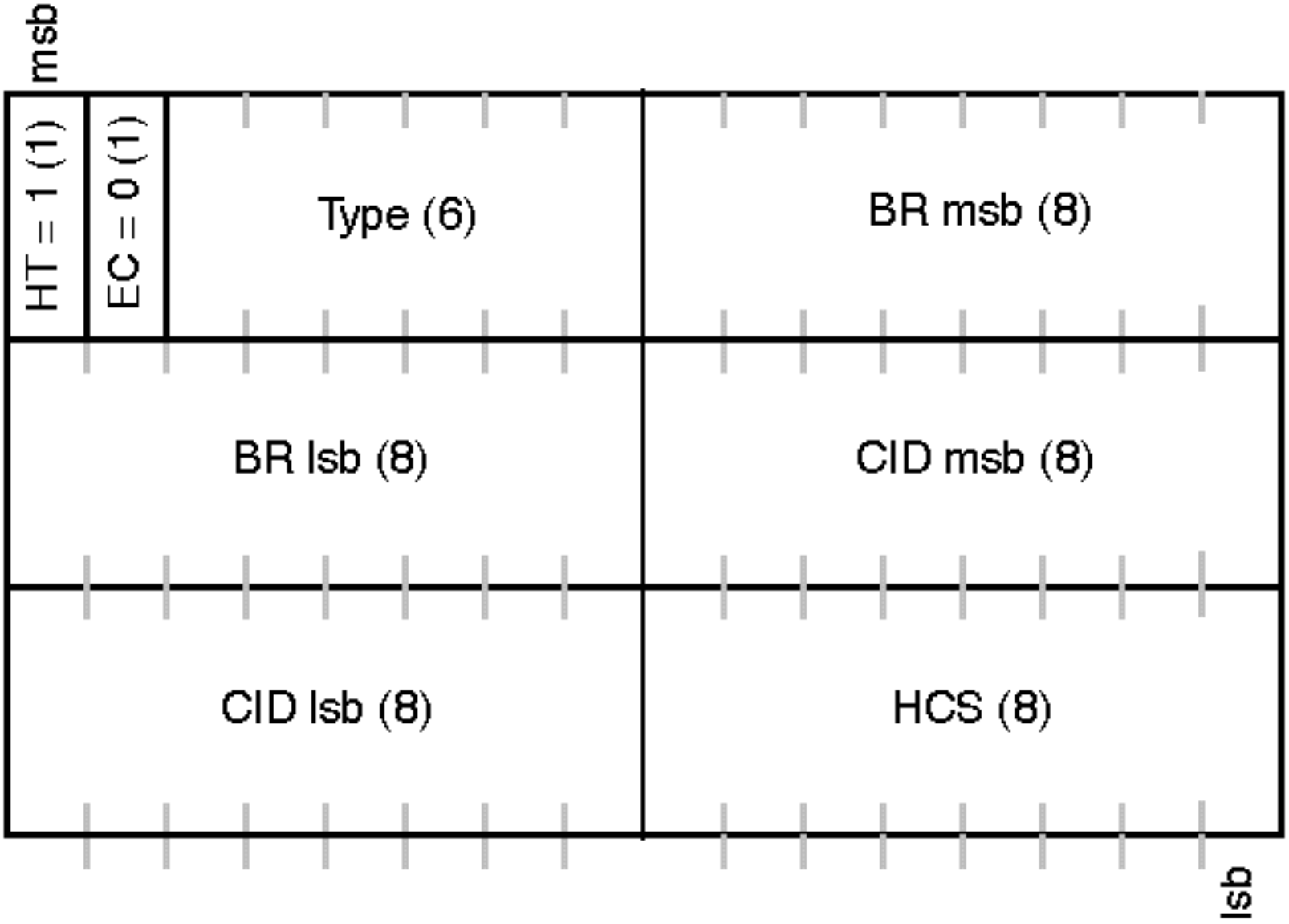
GPSS vs. GPC

- 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 Requests

- 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

BW Request Message



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

- 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

- Registration is 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
- SS acknowledges the REG-RSP with REG-ACK message

IP connectivity and configuration file download

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

Initial Connection Setup

- BS passes Service Flow Encodings to the SS in multiple DSA-REQ messages
- SS replies with DSA-RSP messages
- Service Flow Encodings contain 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

Privacy and Encryption

- Secures over-the-air transmissions
- Authentication
  - X.509 certificates with RSA PKCS
  - Strong authentication of SSs (prevents theft of service)
  - Prevents cloning
- Data encryption
  - Currently 56-bit DES in CBC mode
  - IV based on frame number
  - Easily exportable
- Message authentication
  - Key MAC management messages authenticated with one-way hashing (HMAC with SHA-1)
- Designed to allow new/multiple encryption algorithms
- Protocol descends from BPI+ (from DOCSIS)

Security Associations

- A set of privacy information
  - shared by a BS and one or more of its client SSs share in order to support secured communications
  - includes traffic encryption keys and CBC IVs
- Security Association Establishment
  - Primary SA established during initial registration
  - other SAs may be provisioned or dynamically created within the BS.

Key Management Messages

PKM Message	*Description*
Authentication Information	contains the manufacturer s X.509 Certificate, issued by an external authority.
Authorization Request	sent from an SS to its BS to request an AK and list of authorized SAIDs.
Authorization Reply	sent from a BS to an SS to reply an AK and a list of authorized SAIDs
Authorization Reject	send from a BS to an SS in rejection of an *Authorization Request* message sent by the SS.
Authorization Invalid	send from a BS to an SS as an unsolicited indication or a response to a message received from that SS.
Key Request	sent from an SS to its BS requesting a TEK for the privacy of one of its authorized SAIDs.
Key Reply	sent from a BS to an SS carrying the two active sets of traffic keying material for the SAID.
Key Reject	sent from a BS to an SS indicating that the SAID is no longer valid and no key will be sent.
TEK Invalid	sent from a BS to an SS if it determines that the SS encrypted uplink traffic with an invalid TEK.
SA Add	sent from a BS to an SS to establish one or more additional SAs.

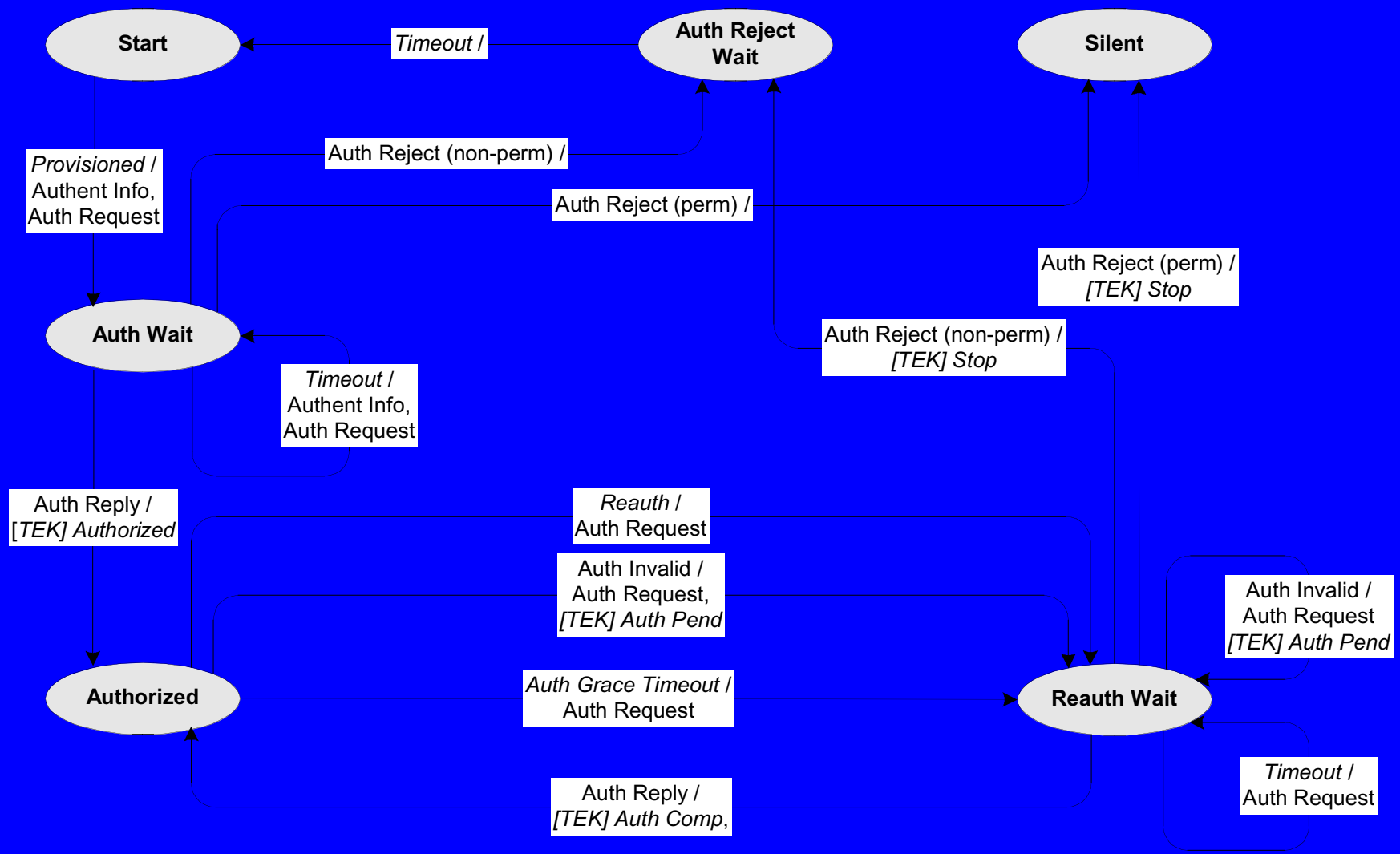
SS Authorization

- Authentication and Authorization
  - SS manufacturer's X.509 certificate binding 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)

Auth. FSM Transition Matrix

State ˚Event or Rcvd msg	(A) Start	(B) Auth Wait	(C) Authorized	(D) Reauth Wait	(E) Auth Reject Wait	(F) Silent
(1) Provisioned	Auth Wait	˚	˚	˚	˚	˚
(2) Auth Reject (non-perm)	˚	Auth Reject Wait	˚	Auth Reject Wait	˚	˚
(3) Auth Reject (perm)	˚	Silent	˚	Silent	˚	˚
(4) Auth Reply	˚	Authorized	˚	Authorized	˚	˚
(5) Timeout	˚	Auth Wait	˚	Reauth Wait	Start	˚
(6) Auth Grace Timeout	˚	˚	Reauth Wait	˚	˚	˚
(7) Auth Invalid	˚	˚	Reauth Wait	Reauth Wait	˚	˚
(8) Reauth	˚	˚	Reauth Wait	˚	˚	˚

Auth. FSM Flow Diagram



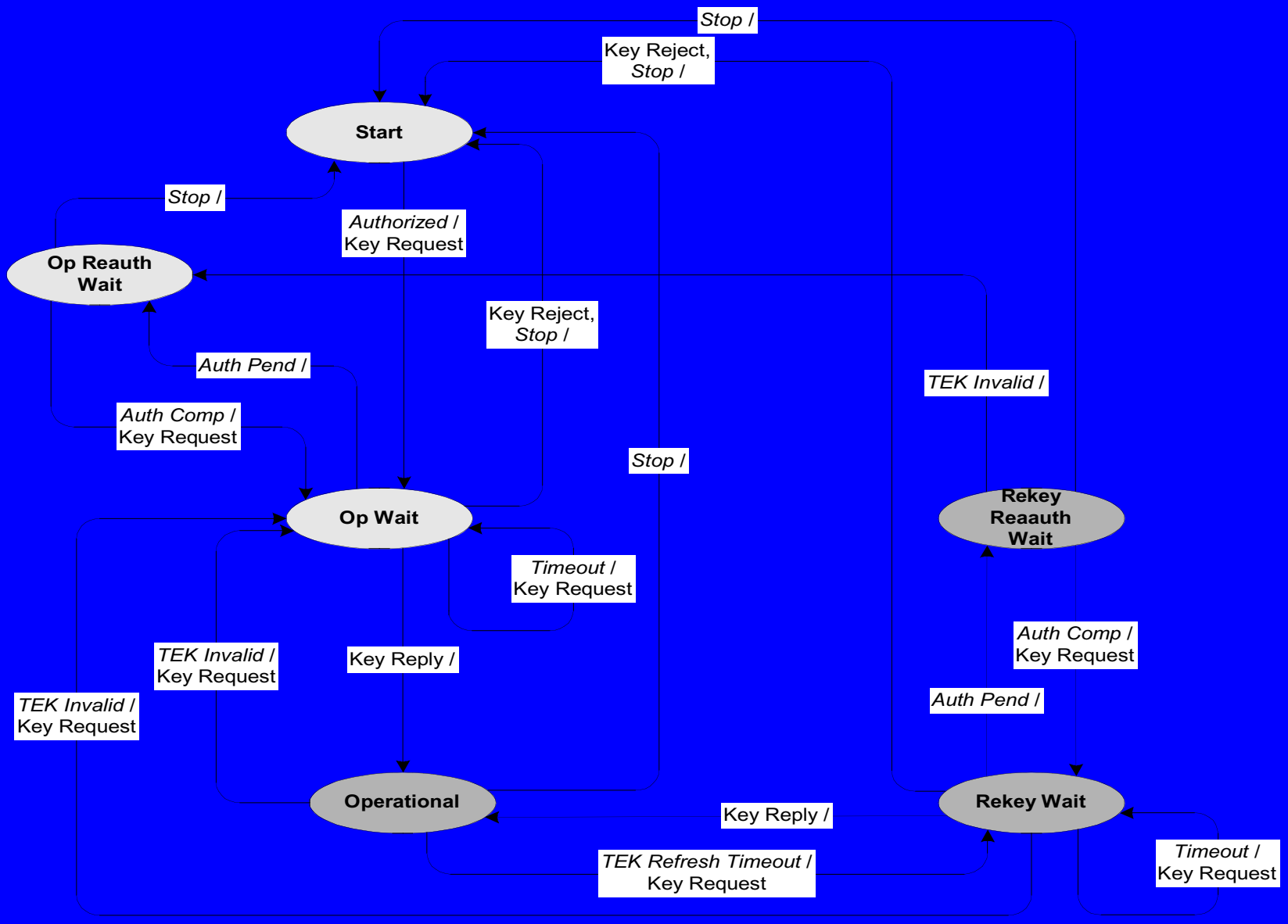
Traffic Encryption Key Management

- Two-level key exchange protocol
  - Key Encryption Key (symmetric) established with RSA
  - Traffic Encryption Keys (TEK) exhanged 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
- Traffic Encryption Key Exchange Protocol
  - Defined by the TEK FSM Transition Matrix

TEK FSM Transition Matrix

State Event or Rcvd msg	(A) Start	(B) Op Wait	(C) Op Reauth Wait	(D) Opera- tional	(E) Rekey Wait	(F) Rekey Reaut Wait
(1) Stop	◦	Start	Start	Start	Start	Start
(2) Authorized	Op Wait	◦	◦	◦	◦	◦
(3) Auth Pend	◦	Op Reauth Wait	◦	◦	Rekey Reauth Wait	◦
(4) Auth Comp	◦	◦	Op Wait	◦	◦	Rekey Wait
(5) TEK Invalid	◦	◦	◦	Op Wait	Op Wait	Op Reauth Wait
(6) Timeout	◦	Op Wait	◦	◦	Rekey Wait	◦
(7) TEK Refresh Timeout	◦	◦	◦	Rekey Wait	◦	◦
(8) Key Reply	◦	Operationa l	◦	◦	Operationa l	◦
(9) Key Reject	◦	Start	◦	◦	Start	◦

TEK FSM Flow Diagram



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
  - Rules for key usage
    - AP: encryption (older key), decryption (both keys)
    - AT: encryption (newer key), decryption (both keys)
- Key sequence number carried in MAC header
- Only MAC PDU payload (including sub-headers) is encrypted
- Management messages are unencrypted

Amendment Project IEEE P802.16a

Media Access Control Modifications and Additional Physical Layer for 2-11 GHz

Amendment Project
IEEE P802.16b

Media Access Control Modifications and Additional Physical Layer for License-Exempt Frequencies

Wireless High-Speed Unlicensed Metropolitan Area Network ("WirelessHUMAN™")

Key 802.16a/802.16b Enhancements

- OFDM Support
- ARQ
- 802.16b Mesh Mode
  - Optional topology
  - Subscriber-to-Subscriber communications

BWA in ETSI BRAN

- HIPERACCESS
  - Above 11 GHz
  - HIPERACCESS began before 802.16
  - Difficulty in resolving processes
  - IEEE now well ahead in schedule
- HIPERMAN
  - Below 11 GHz
  - IEEE went first
  - Signs of healthy cooperation
  - Recently selected 802.16 MAC as baseline

Summary

- The IEEE 802.16 WirelessMAN Air Interface, designed within the 802.16 Working Group, addresses worldwide BWA market needs.
- The outcome is due to successful cooperation between BWA leaders.
- The 802.16 MAC is flexible and powerful enough to support any fixed BWA technology variant in any spectrum in any market.
- The 802.16 Air Interface provides great opportunities for vendor differentiation, at both the base station and subscriber station, without compromising interoperability.

IEEE 802.16 Resources

IEEE 802.16 Working Group on Broadband Wireless Access

info, documents, email lists, etc:

http://WirelessMAN.org