Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Introduction to IP-OFDMA and 8F/1065**
Date Submitted	**2007-03-13**
Source(s)	Scott Probasco Nokia, Inc. scott.probasco@nokia.com
Re:	
Abstract	This contribution contains a presentation to the IP-OFDMA Evaluation Group Coordination Meeting. It provides an introduction to IP-OFDMA and 8F/1065
Purpose	For Information.
Notice	This document has been prepared to assist IEEE 802.16. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.
Release	The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.16.
Patent Policy and Procedures	The contributor is familiar with the IEEE 802.16 Patent Policy and Procedures (Version 1.0) <http://ieee802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, if there is technical justification in the opinion of the standards-developing committee and provided the IEEE receives assurance from the patent holder that it will license applicants under reasonable terms and conditions for the purpose of implementing the standard." Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair <mailto:r.b.marks@ieee.org > as early as possible, in written or electronic form, of any patents (granted or under application) that may cover technology that is under consideration by or has been approved by IEEE 802.16. The Chair will disclose this notification via the IEEE 802.16 web site <http://ieee802.org/16/ipr/patents/notices>.

Overview of 1065

- Attachment 1: cover sheet
- Attachment 2: proposed edits to M.1457
- Attachment 3: description template

Overview 1065

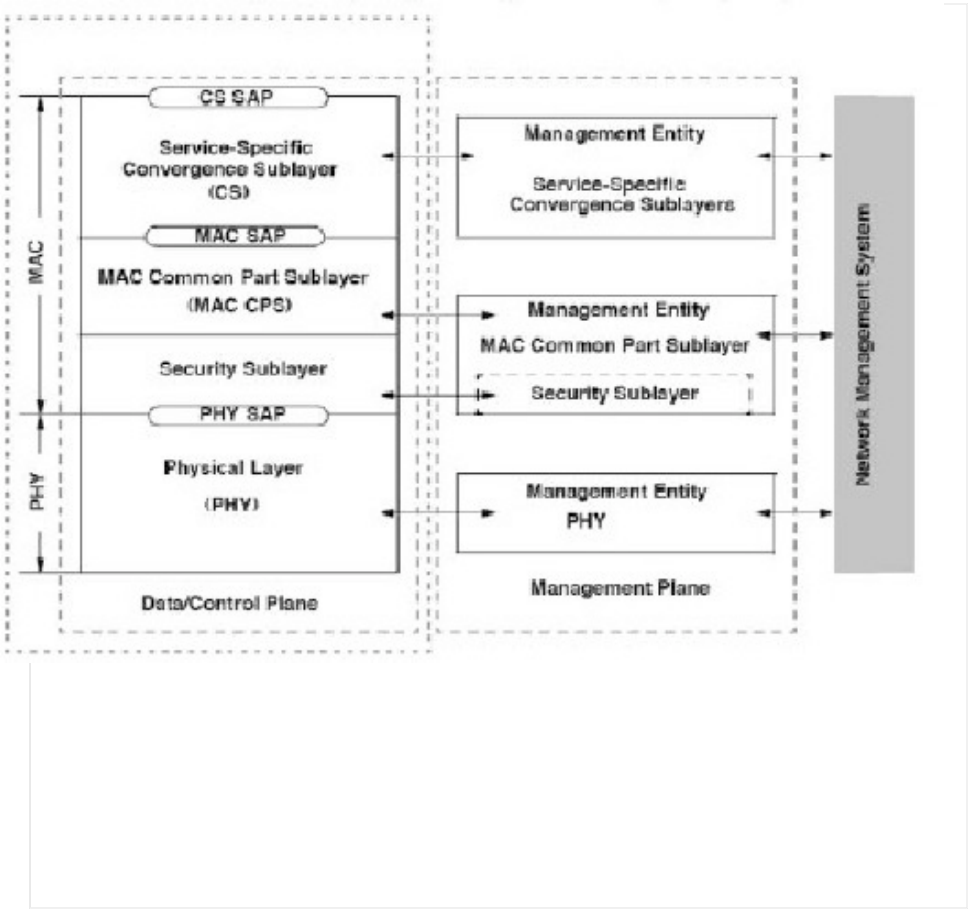
- 5.6.1.1 Introduction

- IEEE Std 802.16 developed and maintained by IEEE 802.16 WG
- IEEE Std 802.16 fully harmonized with ETSI TS 102 177 v1.3.2, ETSI TS 102 178 v1.3.2, and ETSI TS 102 210 v1.2.1
  - Included to F.1763 (earlier, limited version for fixed services only)
  - Included to M.[8A/BWA]
- IP-OFDMA
  - DLC: MAC+LLC, PtMP, typically IP packets
  - PHY: 5 or 10 MHz, special case of Wireless MAN-OFDMA
  - TDD mode only

Overview 1065

- 5.6.1.2 Radio access network architecture

- IP-OFDMA radio interface specifies Layers 1 and 2
  - Flexible to support networks for fixed, nomadic or fully mobile use
  - Compatible with network architectures defined in ITU-T Q.1701
  - Mobile WiMAX End-to-End System Architecture makes optimum use of IP-OFDMA



Overview 1065

- Attachment 3: description template

Overview 1065

- 5.6.1.5 Smart Antennas

- beamforming, space-time coding, and spatial multiplexing
- increase the cell size, data throughput, and spectral efficiency

- These techniques reduce the sensitivity of the system to fading and multipath transmission effects.

Overview 1065

- 5.6.1.4.3 Security

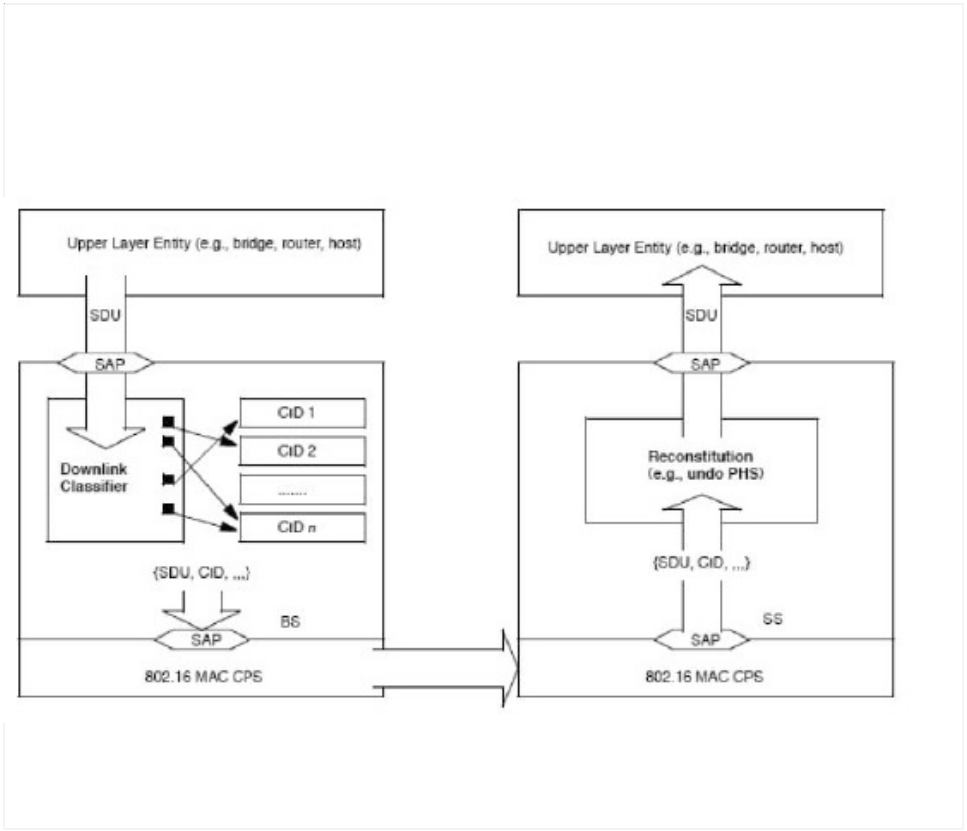
- strong encryption, decryption, mutual authentication, and secure key exchange
- Separate sub-layer facilitates upgrades. Key functionality internal to the sub-layer is also modular, to provide easy maintenance upgrade.
- IP-OFDMA security sub-layer utilizes a security association (SA)
  - a set of information shared between the transmitter and receiver
  - Each SA contains information on the cryptographic suite used for that SA and may also contain keys, such as the traffic encryption keys (TEKs), key lifetimes and other associated state information
  - MAC PDUs are mapped to an SA

Overview 1065

- 5.6.1.4 Layer 2: Medium access control layer (MAC)

- E.g. radio resource control, radio link control, error detection and retransmission, QoS, security, sleep mode, and handover

- A connection identifier (CID) is assigned to designate each connection.
- MAC uses the CID to identify all information exchanged between BS and SS, including management and broadcast data.
- CID provides a simple and direct way to differentiate traffic.
- All MAC-level QoS functions, such as the classifier and QoS scheduler, use the CID to identify and differentiate traffic in order to maintain the service level and fairness among connections



- Encapsulate (fragment, pack)
- MAC header uses flexible sub-headers (fragmentation, packing, grant management)

Overview 1065

- 5.6.1.4 cont.

- Resource allocation controlled by BS
- BS schedules DL, QoS information provided in CS
- SS schedules UL
  - Resource requests initiated by connection
  - BS grants to SS, not connection
  - distributed management and local resource allocation minimizes over-the-air negotiation; rescheduling decisions are made quickly and effectively

- PHY uses AMC, MAC handle RRC control, managing the modulation and coding selection at the SS through interactive message exchange based on monitoring the ratio of carrier signal to noise and interference.

- Energy Conseration in SS: sleep mode, idle mode

- Three types of handover: Hard Handover, Fast Base Station Switching, Macro Diversity

QoS category	Typical applications	QoS specifications
UGS Unsolicited Grant Service	VoIP	Maximum Sustained Rate Maximum Latency Tolerance Jitter Tolerance
rtPS Real-Time Packet Service	Streaming Audio or Video	Minimum Reserved Rate Maximum Sustained Rate Maximum Latency Tolerance Traffic Priority
ErtPS Extended Real-Time Packet Service	Voice with Activity Detection (VoIP)	Minimum Reserved Rate Maximum Sustained Rate Maximum Latency Tolerance Jitter Tolerance Traffic Priority
nrtPS Non-Real-Time Packet Service	File Transfer Protocol (FTP)	Minimum Reserved Rate Maximum Sustained Rate Traffic Priority
BE Best-Effort Service	Data Transfer, Web Browsing, etc.	Maximum Sustained Rate Traffic Priority

Overview 1065

- 5.6.1.4.3 Security

- strong encryption, decryption, mutual authentication, and secure key exchange
- Separate sub-layer facilitates upgrades. Key functionality internal to the sub-layer is also modular, to provide easy maintenance upgrade.
- IP-OFDMA security sub-layer utilizes a security association (SA)
  - a set of information shared between the transmitter and receiver
  - Each SA contains information on the cryptographic suite used for that SA and may also contain keys, such as the traffic encryption keys (TEKs), key lifetimes and other associated state information
  - MAC PDUs are mapped to an SA

Overview 1065

- 5.6.1.5 Smart Antennas

- beamforming, space-time coding, and spatial multiplexing
- increase the cell size, data throughput, and spectral efficiency

- These techniques reduce the sensitivity of the system to fading and multipath transmission effects.

Overview 1065

- Attachment 3: description template