WiMax

www.techalone.com
ABSTRACT

In recent years, Broadband technology has rapidly become an established, global commodity required by a high percentage of the population. The demand has risen rapidly, with a worldwide installed base of 57 million lines in 2002 rising to an estimated 80 million lines by the end of 2003. This healthy growth curve is expected to continue steadily over the next few years and reach the 200 million mark by 2006. DSL operators, who initially focused their deployments in densely-populated urban and metropolitan areas, are now challenged to provide broadband services in suburban and rural areas where new markets are quickly taking root. Governments are prioritizing broadband as a key political objective for all citizens to overcome the “broadband gap” also known as “digital divide”.

Wireless DSL (WDSL) offers an effective, complementary solution to wireline DSL, allowing DSL operators to provide broadband service to additional areas and populations that would otherwise find themselves outside the broadband loop. Government regulatory bodies are realizing the inherent worth in wireless technologies as a means for solving digital-divide challenges in the last mile and have accordingly initiated a deregulation process in recent years for both licensed and unlicensed bands to support this application. Recent technological advancements and the formation of a global standard and interoperability forum - WiMAX, set the stage for WDSL to take a significant role in the broadband market. Revenues from services delivered via Broadband Wireless Access have already reached $323 million and are expected to jump to $1.75 billion.
INTRODUCTION

There are several ways to get a fast Internet connection to the middle of nowhere. Until not too long ago, the only answer would have been "cable" — that is, laying lines. Cable TV companies, who would be the ones to do this, had been weighing the costs and benefits. However this would have taken years for the investment to pay off. So while cable companies might be leading the market for broadband access to most people (of the 41% of Americans who have high-speed Internet access, almost two-thirds get it from their cable company), they don't do as well to rural areas. And governments that try to require cable companies to lay the wires find themselves battling to force the companies to take new customers.

Would DSL be a means of achieving this requisite of broadband and bridging the digital divide?

The lines are already there, but the equipment wasn't always the latest and greatest, even then. Sending voice was not a matter of big concern, but upgrading the system to handle DSL would mean upgrading the central offices that would have to handle the data coming from all those farms.

The most rattling affair is that there are plenty of places in cities that can't handle DSL, let alone the country side. Despite this, we’ll still read about new projects to lay cable out to smaller communities, either by phone companies, cable companies, or someone else. Is this a waste of money? Probably because cables are on their way out. Another way to get broadband to rural communities is the way many folks get their TV: satellite, which offers download speeds of about 500 Kbps —faster than a modem, but at
best half as fast as DSL — through a satellite dish. But you really, really have to want it. The system costs $600 to start, then $60 a month by the services provided by DIRECWAY in the US. There are other wireless ways to get broadband access.

MCI ("Microwave Communications Inc.") was originally formed to compete with AT & T by using microwave towers to transmit voice signals across the US. Unlike a radio (or a Wi-Fi connection), those towers send the signal in a straight line — unidirectional instead of omni directional. That's sometimes called fixed wireless or point-to-point wireless. One popular standard for this is called LMDS: local multipoint distribution system. Two buildings up to several miles apart would have microwave antennas pointing at each other. One (in, say, the urban area) would be connected to the Internet in the usual way, via some kind of wire; the other (in the rural area you want to connect) would send and receive data over the microwave link, and then be connected to homes and farms via cables. Those cables would be much shorter and less expensive, with the bulk of the transmission being done through the ether.

WiMAX:

WiMax delivers broadband to a large area via towers, just like cell phones. This enables your laptop to have high-speed access in any of the hot spots. Instead of yet another cable coming to your home, there would be yet another antenna on the cell-phone tower. This is definitely a point towards broadband service in rural areas. First get the signal to the area, either with a single cable (instead of one to each user) or via a point-to-point wireless system. Then put up a tower or two, and the whole area is online. This saves the trouble of digging lots of trenches, or of putting up wires that are prone to storm damage.

However there is one promising technology that still uses cables to deliver a broadband signal to, well, wherever. It doesn't require laying any new wires (like cable Internet), and it doesn't require overhauling a lot of existing systems (like DSL). It's BPL:
(broadband over power lines). As the name suggests, it piggybacks a high speed data signal on those ubiquitous power lines. Those aren't the low-voltage ones that come to your house, but the medium-voltages ones that travel from neighborhood to neighborhood. The signal, like those power lines, can travel a long way thanks to "regenerators" that not only pass the data along, but clean the signal so it doesn't degrade over distance. That means the signal can travel as long as the lines do. Those regenerators can also include Wi-Fi antennas, so if you space them properly they can be placed near homes and farms and whatnot. You can also connect a cable to one to take the signal to the door if you don't feel like going the W-Fi way.

However there have been certain hiccups in the case of BPL. Unlike some early (and ongoing) attempts to do Internet through power lines, BPL doesn't go into individual homes. That's because in order to do so, the signal would have to make its way through a transformer and through a circuit-breaker box, both of which play havoc with it. The result is that the data get through, but much more slowly than leaving the power line before the transformer.

Combine BPL with Wi-Fi, WiMAX, or even (short) cables, and we have an inexpensive way to get the power of the Internet down on the farm using the power of power.

WiMAX is revolutionizing the broadband wireless world, enabling the formation of a global mass-market wireless industry. Putting the WiMAX revolution in the bigger context of the broadband industry, this paper portrays the recent acceleration stage of the Broadband Wireless Access market, determined by the need for broadband connectivity and by the following drivers:

A) The worldwide deregulation process  
B) The standardization progression; and  
C) Revolutionary wireless technology.
Deregulation:

Creating new opportunities on the horizon

A major driver impacting the broadband wireless explosion is the advent of global telecom deregulation, opening up the telecommunications/Internet access industries to a host of new players. As more and more countries enable carriers and service providers to operate in a variety of frequencies, new and lucrative broadband access markets are springing up everywhere. Wireless technology requires the use of frequencies contained within a given spectrum to transfer voice and data. Governments allocate a specific range of that spectrum to incumbent and competitive carriers, as well as cellular operators, ISPs, and other service providers, enabling them to launch a variety of broadband initiatives based exclusively on wireless networking solutions.

There are two main types of spectrum allocation: licensed and unlicensed.

- Licensed frequencies are typically awarded through an auction or “beauty contest” to those who present the soundest business plans to the regulatory authorities overseeing the process.
- Unlicensed frequencies allow multiple service providers to utilize the same section of the spectrum and compete with each other for customers.

Standardization:

WiMAX - Worldwide Interoperability for Microwave Access

The WiMAX Forum is a non-profit trade organization, founded in April 2002 by leading vendors of wireless access equipment and telecommunications components. The
Forum's mission is to lay the groundwork for an industry-wide acceptance and implementation of the IEEE 802.16 and ETSI HiperMAN standard, covering the 2-11 GHz bands for Wireless Metropolitan Area Networks (Wireless MAN). The Forum hopes to jump-start this crucial industry by establishing rigorous definitions for testing and certifying products for interoperability compliance. The issuing of a “WiMAX-Certified” label will serve as a seal of approval that a particular vendor’s system or component fully corresponds to the technological specifications set forth by the new Wireless MAN protocol.

In order to ensure the success of wireless technology as a stable, viable and cost effective alternative for delivering broadband access services in the last mile, the introduction of industry standards is essential. The companies that have already joined the WiMAX Forum represent over 75% of revenues in the global BWA market. Moreover, membership of the WiMAX Forum is not limited to industry leading BWA providers; numerous multinational enterprises like Intel and Fujitsu have also joined the WiMAX Forum. The Forum represents a cross-industry group of valued partners, including chip set manufacturers, component makers and service providers. All of these organizations recognize the long-term benefits of working with standardized, interoperable equipment and are committed to the design, development and implementation of WiMAX-compliant solutions.

OVERVIEW OF THE 802.16 IEEE STANDARDS

The 802.16 standard, amended by the IEEE to cover frequency bands in the range between 2 GHz and 11 GHz, specifies a metropolitan area networking protocol that will enable a wireless alternative for cable, DSL and T1 level services for last mile broadband access, as well as providing backhaul for 801.11 hotspots.
The new 802.16a standard specifies a protocol that among other things supports low latency applications such as voice and video, provides broadband connectivity without requiring a direct line of sight between subscriber terminals and the base station (BTS) and will support hundreds if not thousands of subscribers from a single BTS. The standard will help accelerate the introduction of wireless broadband equipment into the marketplace, speeding up last-mile broadband deployment worldwide by enabling service providers to increase system performance and reliability while reducing their equipment costs and investment risks.

However it has been shown repeatedly that adoption of a standard does not always lead to adoption by the intended market. For a market to be truly enabled, products must be certified that they do adhere to the standard first, and once certified it must also be shown that they interoperate. Interoperability means the end user can buy the brand they like, with the features they want, and know it will work with all other like certified products.

For the Broadband Wireless Access (BWA) market and its 802.16 standard, this role is played by the Worldwide Microwave Interoperability Forum or WiMAX. WiMAX is instrumental in removing the barrier in adopting the standard by assuring demonstrable interoperability between system components developed by OEMs. WiMAX will develop conformance and interoperability test plans, select certification labs and will host interoperability events for IEEE 802.16 equipment vendors.

Satisfying the growing demand for BWA in underserved markets has been a continuing challenge for service providers, due to the absence of a truly global standard. A standard that would enable companies to build systems that will effectively reach underserved business and residential markets in a manner that supports infrastructure build outs comparable to cable, DSL, and fiber. For years, the wildly successful 802.11x or WiFi wireless LAN technology has been used in BWA applications along with a host of proprietary based solutions. When the
WLAN technology was examined closely, it was evident that the overall design and feature set available was not well suited for outdoor BWA applications. It could be done, it is being done, but with limited capacity in terms of bandwidth and subscribers, range and a host of other issues made it clear this approach while a great fit for indoor WLAN was a poor fit for outdoor BWA.

**WiMAX and the IEEE 802.16a PHY Layer**

The first version of the 802.16 standard released addressed Line-of-Sight (LOS) environments at high frequency bands operating in the 10-66 GHz range, whereas the recently adopted amendment, the 802.16a standard, is designed for systems operating in bands between 2 GHz and 11 GHz. The significant difference between these two frequency bands lies in the ability to support Non-Line-of-Sight (NLOS) operation in the lower frequencies, something that is not possible in higher bands. Consequently, the 802.16a amendment to the standard opened up the opportunity for major changes to the PHY layer specifications specifically to address the needs of the 2-11 GHz bands. This is achieved through the introduction of three new PHY-layer specifications (a new Single Carrier PHY, a 256 point FFT OFDM PHY, and a 2048 point FFT OFDMA PHY): major changes to the PHY layer specification as compared to the upper frequency, as well as significant MAC-layer enhancements. Although multiple PHYs are specified as in the 802.11 suite of standards (few recall that infrared and frequency hopping were and are part of the base 802.11 standard), the WiMAX Forum has determined that the first interoperable test plans and eventual certification will support the 256 point FFT OFDM PHY (which is common between 802.16a and ETSI HiperMAN), with the others to be developed as the market requires.

The OFDM signaling format was selected in preference to competing formats such as CDMA due to its ability to support NLOS performance while maintaining a high
level of spectral efficiency maximizing the use of available spectrum. In the case of CDMA (prevalent in 2G and 3G standards), the RF bandwidth must be much larger than the data throughput, in order to maintain processing gain adequate to overcome interference. This is clearly impractical for broadband wireless below 11 GHz, since for example, data rates up to 70 Mbps would require RF bandwidths exceeding 200 MHz to deliver comparable processing gains and NLOS performance.

Some of the other PHY layer features of 802.16a that are instrumental in giving this technology the power to deliver robust performance in a broad range of channel environments are; flexible channel widths, adaptive burst profiles, forward error correction with concatenated Reed-Solomon and convolutional encoding, optional AAS (advanced antenna systems) to improve range/capacity, DFS (dynamic frequency selection)-which helps in minimizing interference, and STC (space-time coding) to enhance performance in fading environments through spatial diversity.

Table 1 gives a high level overview of some of the PHY layer features of the IEEE 802.16a standard.
Every wireless network operates fundamentally in a shared medium and as such that requires a mechanism for controlling access by subscriber units to the medium.

The 802.16a standard uses a slotted TDMA protocol scheduled by the BTS to allocate capacity to subscribers in a point-to-multipoint network topology. While this on the surface sounds like a one line, technical throwaway statement, it has a huge impact on how the system operates and what services it can deploy. By starting with a TDMA approach with intelligent scheduling, WiMAX systems will be able to deliver not only high speed data with SLAs, but latency sensitive services such as voice and video or database access are also supported. The standard delivers QoS beyond mere prioritization, a technique that is very limited in effectiveness as traffic load and the number of subscribers increases. The MAC layer in WiMAX certified systems has also

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>256 point FFT OFDM waveform</td>
<td>• Built in support for addressing multipath in outdoor LOS and NLOS environments</td>
</tr>
<tr>
<td>Adaptive Modulation and variable error correction encoding per RF burst</td>
<td>• Ensures a robust RF link while maximizing the number of bits/ second for each subscriber unit.</td>
</tr>
<tr>
<td>TDD and FDD duplexing support</td>
<td>• Address varying worldwide regulations where one or both may be allowed</td>
</tr>
<tr>
<td>Flexible Channel sizes (e.g. 3.5MHz, 5MHz, 10MHz, etc)</td>
<td>• Provides the flexibility necessary to operate in many different frequency bands with varying channel requirements around the world.</td>
</tr>
<tr>
<td>Designed to support smart antenna systems</td>
<td>• Smart antennas are fast becoming more affordable, and as these costs come down their ability to suppress interference and increase system gain will become important in BWA deployments.</td>
</tr>
</tbody>
</table>
been designed to address the harsh physical layer environment where interference, fast fading and other phenomena are prevalent in outdoor operation.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>TDM/TDMA Scheduled Uplink/Downlink frames.</td>
<td>• Efficient bandwidth usage</td>
</tr>
<tr>
<td>Scalable from 1 to hundreds of subscribers</td>
<td>• Allows cost effective deployments by supporting enough subs to deliver a robust business case</td>
</tr>
<tr>
<td>Connection-oriented</td>
<td>• Per Connection QoS</td>
</tr>
<tr>
<td>QoS support</td>
<td>• Faster packet routing and forwarding</td>
</tr>
<tr>
<td>Continuous Grant</td>
<td>• Low latency for delay sensitive services (TDM Voice, VoIP)</td>
</tr>
<tr>
<td>Real Time Variable Bit Rate</td>
<td>• Optimal transport for VBR traffic(e.g., video)</td>
</tr>
<tr>
<td>Non Real Time Variable Bit Rate</td>
<td>• Data prioritization</td>
</tr>
<tr>
<td>Automatic Retransmission request (ARQ)</td>
<td>• Improves end-to-end performance by hiding RF layer induced errors from upper layer protocols</td>
</tr>
<tr>
<td>Support for adaptive modulation</td>
<td>• Enables highest data rates allowed by channel conditions, improving system capacity</td>
</tr>
<tr>
<td>Security and encryption (Triple DES)</td>
<td>• Protects user privacy</td>
</tr>
<tr>
<td>Automatic Power control</td>
<td>• Enables cellular deployments by minimizing self interference</td>
</tr>
</tbody>
</table>
WHY WiMAX?

The low POTS penetration and the low quality of the copper pair prevent mass scale DSL deployment and foster the need for alternate broadband technologies. In this context, WiMAX is positioned as an excellent option. Moreover, the possibility of offering broadband services in combination with voice services will gradually lead to narrowband WLL substitution. WiMAX is of interest for large enterprises with several locations in the same metropolitan area. WiMAX will permit Operator's bypass under license conditions: building a metropolitan private network of IP lines at a very low cost (no civil works). The comparison to leased lines rental fee is in favor of Wimax even for two sites only.

Deployment topologies

Several topology and backhauling options are to be supported on the WiMAX base stations: wire line backhauling (typically over Ethernet), microwave Point-to-Point connection, as well as WiMAX backhaul. With the latter option, the base station has the capability to backhaul itself. This can be achieved by reserving part of the bandwidth normally used for the end-user traffic and using it for backhauling purposes.
**WiMAX for Portable Internet**

*WiMAX, the natural complement to mobile and Wi-Fi networks* Mobile networks offer full mobility, nation-wide coverage, voice support and moderate data rates. WiMAX can then be positioned as a complementary solution by offering higher bandwidth when required, in particular in dense urban areas. Public WLAN, while offering clear benefits, is limited in coverage and mobility capabilities. WiMAX by-passes these limitations and offers broadband connectivity in larger areas (hot zones). Wi-Fi and WiMAX solutions are also complementary, with Wi-Fi being more adapted for short-range, indoor connections (in particular in the enterprise and at home) and WiMAX for long-range outdoor connections.
**The WiMAX CPE**

In most cases, a simple plug and play terminal, similar to a DSL modem, provides connectivity. For customers located several kilometers from the WiMAX base station, a self-install outdoor antenna may be required to improve transmission quality. To serve isolated customers, a directive antenna pointing to the WiMAX base station may be required. For customers requesting voice in addition to broadband services, specific CPE will allow the connection of standard or VoIP phones. Ultimately, WiMAX chipset will be embedded in data-centric devices.

**Operator's business case**

WiMAX is of interest for incumbent, alternate, and mobile operators. Some business cases are possible.

- The incumbent operators can use the wireless technology as a complement to DSL, allowing them to offer DSL-like services in remote, low density areas that cannot be served with DSL.

- For alternate operators, the wireless technology is the solution for a competitive high-speed Internet and voice offering bypassing the landline facilities, with applicability in urban or sub-urban areas.

- The larger opportunity will come with the Portable Internet usage, complementing fixed and mobile solution in urban and suburban areas. Therefore it will enhance the business case by giving access to a large potential of end users.

**WiMAX, the obvious choice for operators**
By integrating WiMAX into their networks, mobile operators can boost their service with high bandwidth, when necessary, the same applications (messaging, agenda, location-based services) being offered on both networks with a single billing and subscriber profile. Mobile operators can also reuse existing radio sites and backhauling equipment to facilitate the deployment of WiMAX. Fixed operators, incumbent or alternate, will offer nomadic and Portable Internet usage as an addition to their fixed access offering to complement their DSL and Wi-Fi bundle. For those having deployed WiMAX for fixed access, this is also a natural evolution of their offering.

**WiMAX Technology Challenge**

**WiMAX, more flexibility and security**

Unlike WLAN, WiMAX provides a media access control (MAC) layer that uses a grant-request mechanism to authorize the exchange of data. This feature allows better exploitation of the radio resources, in particular with smart antennas, and independent management of the traffic of every user. This simplifies the support of real-time and voice applications. One of the inhibitors to widespread deployment of WLAN was the poor security feature of the first releases. WiMAX proposes the full range of security features to ensure secured data exchange:

- Terminal authentication by exchanging certificates to prevent rogue devices,
- User authentication using the Extensible Authentication Protocol (EAP),
- Data encryption using the Data Encryption Standard (DES) or Advanced Encryption Standard (AES), both much more robust than the Wireless
Equivalent Privacy (WEP) initially used by WLAN. Furthermore, each service is encrypted with its own security association and private keys.

**WiMAX, a very efficient radio solution**

WiMAX must be able to provide a reliable service over long distances to customers using indoor terminals or PC cards (like today's WLAN cards). These requirements, with limited transmit power to comply with health requirements, will limit the link budget. Sub-channeling in uplink and smart antennas at the base station has to overcome these constraints. The WiMAX system relies on a new radio physical (PHY) layer and appropriate MAC layer to support all demands driven by the target applications. The PHY layer modulation is based on OFDMA, in combination with a centralized MAC layer for optimized resource allocation and support of QoS for different types of services (VoIP, real-time and non-real-time services, best effort). The OFDMA PHY layer is well adapted to the NLOS propagation environment in the 2 - 11 GHz frequency range. It is inherently robust when it comes to handling the significant delay spread caused by the typical NLOS reflections. Together with adaptive modulation, which is applied to each subscriber individually according to the radio channel capability, OFDMA can provide a high spectral efficiency of about 3 - 4 bit/s/Hz.

However, in contrast to single carrier modulation, the OFDMA signal has an increased peak: average ratio and increased frequency accuracy requirements. Therefore, selection of appropriate power amplifiers and frequency recovery concepts are crucial. WiMAX provides flexibility in terms of channelization, carrier frequency, and duplex mode (TDD and FDD) to meet a variety of requirements for available spectrum resources and targeted services. An important and very challenging function of the WiMAX system is the support of various advanced antenna techniques, which are essential to provide high spectral efficiency, capacity, system performance, and reliability:
 Beam forming using smart antennas provides additional gain to bridge long distances or to increase indoor coverage; it reduces inter-cell interference and improves frequency reuse.

 Transmit diversity and MIMO techniques using multiple antennas take advantage of multipath reflections to improve reliability and capacity.

**System performance**

Table 2 gives typical cell size and throughput at 3.5 GHz in various configuration and environments.

<table>
<thead>
<tr>
<th>Environment</th>
<th>Typical cell size</th>
<th>Sector throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>Urban indoor (NLOS)</td>
<td>1 km (5/8 miles)</td>
<td>21 Mbit/s w. 10 MHz channel</td>
</tr>
<tr>
<td>Suburban indoor (NLOS)</td>
<td>2.5 km (1.5 miles)</td>
<td>22 Mbit/s w. 10 MHz channel</td>
</tr>
<tr>
<td>Suburban outdoor (LOS)</td>
<td>7 km (4 miles)</td>
<td>22 Mbit/s w. 10 MHz channel</td>
</tr>
<tr>
<td>Rural indoor (NLOS)</td>
<td>5 km (3 miles)</td>
<td>4.5 Mbit/s w. 3.5 MHz channel</td>
</tr>
<tr>
<td>Rural outdoor (LOS)</td>
<td>15 km (9 miles)</td>
<td>4.5 Mbit/s w. 3.5 MHz channel</td>
</tr>
</tbody>
</table>

**WiMAX Spectrum and Regulation Issues**

WiMAX-compliant equipment will be allowed to operate in both licensed and unlicensed bands. The minimum channel bandwidth for WiMAX usage is 1.75 MHz per channel, while 10 MHz is considered as an optimum. Although 2.4 GHz and 5 GHz non-licensed bands are largely available, their usage could be limited to trials because of the risks of interference preventing QoS commitments.

The 2.5 and 3.5 GHz licensed bands will be the most common bands for WiMAX applications. It should be noted that the 5 GHz band is also partially licensed in some
countries. Most countries have already allocated licensed spectrum, generally to alternate operators. Nevertheless large quantities of spectrum are still in a process of allocation, and some countries have not even defined any WiMAX licensed bands yet. WiMAX is designed to accommodate either Frequency Division Duplexing (FDD), which is more suited to enterprise traffic, or Time Division Duplexing (TDD), which is more adapted to asymmetrical traffic. Cohabitation of FDD and TDD techniques is possible within the same bands, provided guard bands are implemented.

TECHNICAL ASPECTS OF WiMAX

MEDIUM ACCESS CONTROL

The IEEE 802.16 MAC protocol was designed for point-to-multipoint broadband wireless access applications. It addresses the need for very high bit rates, both uplink (to the BS) and downlink (from the BS). Access and bandwidth allocation algorithms must accommodate hundreds of terminals per channel, with terminals that may be shared by multiple end users. The services required by these end users are varied in their nature and include legacy time-division multiplex (TDM) voice and data, Internet Protocol (IP) connectivity, and packetized voice over IP (VoIP). To support this variety of services, the 802.16 MAC must accommodate both continuous and bursty traffic. Additionally, these services expect to be assigned QoS in keeping with the traffic types. The 802.16 MAC provides a wide range of service types analogous to the classic asynchronous transfer mode (ATM) service categories as well as newer categories such as guaranteed frame rate (GFR).

The 802.16 MAC protocol must also support a variety of backhaul requirements, including both asynchronous transfer mode (ATM) and packet-based protocols. Convergence sublayers are used to map the transport-layer-specific traffic to a MAC that
is flexible enough to efficiently carry any traffic type. Through such features as payload header suppression, packing, and fragmentation, the convergence sublayers and MAC work together to carry traffic in a form that is often more efficient than the original transport mechanism. Issues of transport efficiency are also addressed at the interface between the MAC and the physical layer (PHY). For example, the modulation and coding schemes are specified in a burst profile that may be adjusted adaptively for each burst to each subscriber station. The MAC can make use of bandwidth-efficient burst profiles under favorable link conditions but shift to more reliable, although less efficient, alternatives as required to support the planned 99.999 percent link availability.

The request-grant mechanism is designed to be scalable, efficient, and self-correcting. The 802.16 access system does not lose efficiency when presented with multiple connections per terminal, multiple QoS levels per terminal, and a large number of statistically multiplexed users. It takes advantage of a wide variety of request mechanisms, balancing the stability of contention less access with the efficiency of contention-oriented access. While extensive bandwidth allocation and QoS mechanisms are provided, the details of scheduling and reservation management are left unstandardized and provide an important mechanism for vendors to differentiate their equipment. Along with the fundamental task of allocating bandwidth and transporting data, the MAC includes a privacy sub layer that provides authentication of network access and connection establishment to avoid theft of service, and it provides key exchange and encryption for data privacy. To accommodate the more demanding physical environment and different service requirements of the frequencies between 2 and 11 GHz, the 802.16a project is upgrading the MAC to provide automatic repeat request (ARQ) and support for mesh, rather than only point-to-multipoint, network architectures.

THE PHYSICAL LAYER

10–66 GHz — In the design of the PHY specification for 10–66 GHz, line-of-sight propagation was deemed a practical necessity. With this condition assumed, single-
carrier modulation was easily selected; the air interface is designated “Wireless MAN-SC.” Many fundamental design challenges remained, however. Because of the point-to-multipoint architecture, the BS basically transmits a TDM signal, with individual subscriber stations allocated time slots serially. Access in the uplink direction is by time-division multiple accesses (TDMA). Following extensive discussions regarding duplexing, a burst design was selected that allows both time division duplexing (TDD), in which the uplink and downlink share a channel but do not transmit simultaneously, and frequency-division duplexing (FDD), in which the uplink and downlink operate on separate channels, sometimes simultaneously. This burst design allows both TDD and FDD to be handled in a similar fashion. Support for half-duplex FDD subscriber stations, which may be less expensive since they do not simultaneously transmit and receive, was added at the expense of some slight complexity. Both TDD and FDD alternatives support adaptive burst profiles in which modulation and coding options may be dynamically assigned on a burst-by-burst basis.

**2–11 GHz** — The 2–11 GHz bands, both licensed and license-exempt, are addressed in IEEE Project 802.16a. The standard is in ballot but is not yet complete. The draft currently specifies that compliant systems implement one of three air interface specifications, each of which provides for interoperability. Design of the 2–11 GHz physical layer is driven by the need for non-line-of-sight (NLOS) operation. Because residential applications are expected, rooftops may be too low for a clear sight line to a BS antenna, possibly due to obstruction by trees. Therefore, significant multipath propagation must be expected. Furthermore, outdoor-mounted antennas are expensive due to both hardware and installation costs.

The three 2–11 GHz air interface specifications in 802.16a Draft 3 are:

- **WirelessMAN-SC2**: This uses a single-carrier modulation format.
- **Wireless MAN-OFDM**: This uses orthogonal frequency-division multiplexing with a 256-point transform. Access is by TDMA. This air interface is mandatory for license exempt bands.
Wireless MAN-OFDMA: This uses orthogonal frequency-division multiple access with a 2048-point transform. In this system, multiple access is provided by addressing a subset of the multiple carriers to individual receivers.

Because of the propagation requirements, the use of advanced antenna systems is supported. It is premature to speculate on further specifics of the 802.16a amendment prior to its completion. While the draft seems to have reached a level of maturity, the contents could change significantly in balloting. Modes could even be deleted or added.

PHYSICAL LAYER DETAILS

The PHY specification defined for 10–66 GHz uses burst single-carrier modulation with adaptive burst profiling in which transmission parameters, including the modulation and coding schemes, may be adjusted individually to each subscriber station (SS) on a frame-by-frame basis. Both TDD and burst FDD variants are defined. Channel bandwidths of 20 or 25 MHz (typical U.S. allocation) or 28 MHz (typical European allocation) are specified, along with Nyquist square-root raised-cosine pulse shaping with a rolloff factor of 0.25. Randomization is performed for spectral shaping and to ensure bit transitions for clock recovery.

The forward error correction (FEC) used is Reed-Solomon GF(256), with variable block size and error correction capabilities. This is paired with an inner block convolutional code to robustly transmit critical data, such as frame control and initial accesses. The FEC options are paired with quadrature phase shift keying (QPSK), 16-state quadrature amplitude modulation (16-QAM), and 64-state QAM (64-QAM) to form burst profiles of varying robustness and efficiency. If the last FEC block is not filled, that block may be shortened. Shortening in both the uplink and downlink is controlled by the BS and is implicitly communicated in the uplink map (ULMAP) and downlink map (DL-MAP). The system uses a frame of 0.5, 1, or 2 ms. This frame is divided into physical slots for the purpose of bandwidth allocation and identification of PHY transitions.
physical slot is defined to be 4 QAM symbols. In the TDD variant of the PHY, the uplink sub frame follows the downlink sub frame on the same carrier frequency.

In the FDD variant, the uplink and downlink sub frames are coincident in time but are carried on separate frequencies. The downlink sub frame is shown in the following figure.

![Figure 1. The downlink subframe structure.](image)

The downlink sub frame starts with a frame control section that contains the DL-MAP for the current downlink frame as well as the ULMAP for a specified time in the future. The downlink map specifies when physical layer transitions (modulation and FEC changes) occur within the downlink sub frame. The downlink sub frame typically contains a TDM portion immediately following the frame control section.

Downlink data are transmitted to each SS using a negotiated burst profile. The data are transmitted in order of decreasing robustness to allow SSs to receive their data before being presented with a burst profile that could cause them to lose synchronization with the downlink. In FDD systems, the TDM portion may be followed by a TDMA segment that includes an extra preamble at the start of each new burst profile. This feature allows better support of half-duplex SSs.

In an efficiently scheduled FDD system with many half-duplex SSs, some may need to transmit earlier in the frame than they receive. Due to their half-duplex nature, these SSs lose synchronization with the downlink. The TDMA preamble allows them to
regain synchronization. Due to the dynamics of bandwidth demand for the variety of services that may be active, the mixture and duration of burst profiles and the presence or absence of a TDMA portion vary dynamically from frame to frame. Since the recipient SS is implicitly indicated in the MAC headers rather than in the DL-MAP, SSs listen to all portions of the downlink sub frame they are capable of receiving. For full-duplex SSs, this means receiving all burst profiles of equal or greater robustness than they have negotiated with the BS. A typical uplink sub frame for the 10–66 GHz PHY is shown in the following figure.

Unlike the downlink, the UL-MAP grants bandwidth to specific SSs. The SSs transmit in their assigned allocation using the burst profile specified by the Uplink Interval Usage Code (UIUC) in the UL-MAP entry granting them bandwidth. The uplink sub frame may also contain contention-based allocations for initial system access and broadcast or multicast bandwidth requests. The access opportunities for initial system access are sized to allow extra guard time for SSs that have not resolved the transmit time advance necessary to offset the round-trip delay to the BS. Between the PHY and MAC is a transmission convergence (TC) sub layer. This layer performs the transformation of variable length MAC protocol data units (PDUs) into the fixed length FEC blocks (plus possibly a shortened block at the end) of each burst. The TC layer has a PDU sized to fit
in the FEC block currently being filled. It starts with a pointer indicating where the next MAC PDU header starts within the FEC block. This is shown in the following figure.

![Figure 3. TC PDU format.](image)

The TC PDU format allows resynchronization to the next MAC PDU in the event that the previous FEC block had irrecoverable errors. Without the TC layer, a receiving SS or BS would potentially lose the entire remainder of a burst when an irrecoverable bit error occurred.

**MEDIUM ACCESS CONTROL DETAILS**

The MAC includes service-specific convergence sub layers that interface to higher layers, above the core MAC common part sub layer that carries out the key MAC functions. Below the common part sub layer is the privacy sub layer.

**SERVICE-SPECIFIC CONVERGENCE SUBLAYERS**

**COMMON PART SUBLAYER**

**Introduction and General Architecture** — In general, the 802.16 MAC is designed to support a point-to-multipoint architecture with a central BS handling multiple independent sectors simultaneously. On the downlink, data to SSs are multiplexed in
TDM fashion. The uplink is shared between SSs in TDMA fashion. The 802.16 MAC is connection-oriented. All services, including inherently connectionless services, are mapped to a connection. This provides a mechanism for requesting bandwidth, associating QoS and traffic parameters, transporting and routing data to the appropriate convergence sublayer, and all other actions associated with the contractual terms of the service. Connections are referenced with 16-bit connection identifiers (CIDs) and may require continuously granted bandwidth or bandwidth on demand. As will be described, both are accommodated. Each SS has a standard 48-bit MAC address, but this serves mainly as an equipment identifier, since the primary addresses used during operation are the CIDs. Upon entering the network, the SS is assigned three management connections in each direction. These three connections reflect the three different QoS requirements used by different management levels. The first of these is the basic connection, which is used for the transfer of short, time-critical MAC and radio link control (RLC) messages. The primary management connection is used to transfer longer, more delay-tolerant messages such as those used for authentication and connection setup. The secondary management connection is used for the transfer of standards-based management messages such as Dynamic Host Configuration Protocol (DHCP), Trivial File Transfer Protocol (TFTP), and Simple Network Management Protocol (SNMP). In addition to these management SSs are allocated transport connections for the contracted services. Transport connections are unidirectional to facilitate different uplink and downlink QoS and traffic parameters; they are typically assigned to services in pairs. The MAC reserves additional connections for other purposes. One connection is reserved for contention-based initial access. Another is reserved for broadcast transmissions in the downlink as well as for signaling broadcast contention-based polling of SS bandwidth needs. Additional connections are reserved for multicast, rather than broadcast, contention-based polling. SSs may be instructed to join multicast polling groups associated with these multicast polling connections.

MAC PDU Formats
The MAC PDU is the data unit exchanged between the MAC layers of the BS and its SSs. A MAC PDU consists of a fixed-length MAC header, a variable-length payload, and an optional cyclic redundancy check (CRC). Two header formats, distinguished by the HT field, are defined: the generic header (as shown in the following figure) and the bandwidth request header.

![Figure 4. Format of generic header for MAC PDU.](image)

Except for bandwidth request MAC PDUs, which contain no payload, MAC PDUs contain either MAC management messages or convergence sublayer data.

Three types of MAC subheader may be present. The grant management subheader is used by an SS to convey bandwidth management needs to its BS. The fragmentation subheader contains information that indicates the presence and orientation in the payload of any fragments of SDUs. The packing subheader is used to indicate the packing of multiple SDUs into a single PDU. The grant management and fragmentation subheaders may be inserted in MAC PDUs immediately following the generic header if so indicated by the Type field. The packing subheader may be inserted before each MAC SDU if so indicated by the Type field. More details are provided below.
Transmission of MAC PDUs

The IEEE 802.16 MAC supports various higher-layer protocols such as ATM or IP. Incoming MAC SDUs from corresponding convergence sublayers are formatted according to the MAC PDU format, possibly with fragmentation and/or packing, before being conveyed over one or more connections in accordance with the MAC protocol. After traversing the airlink, MAC PDUs are reconstructed back into the original MAC SDUs so that the format modifications performed by the MAC layer protocol are transparent to the receiving entity.

IEEE 802.16 takes advantage of incorporating the packing and fragmentation processes with the bandwidth allocation process to maximize the flexibility, efficiency, and effectiveness of both. Fragmentation is the process in which a MAC SDU is divided into one or more MAC SDU fragments. Packing is the process in which multiple MAC SDUs are packed into a single MAC PDU payload. Both processes may be initiated by either a BS for a downlink connection or an SS for an uplink connection. IEEE 802.16 allows simultaneous fragmentation and packing for efficient use of the bandwidth.

PHY Support and Frame Structure

The IEEE 802.16 MAC supports both TDD and FDD. In FDD, both continuous and burst downlinks are supported. Continuous downlinks allow for certain robustness enhancement techniques, such as interleaving. Burst downlinks (either FDD or TDD) allow the use of more advanced robustness and capacity enhancement techniques, such as subscriber-level adaptive burst profiling and advanced antenna systems. The MAC builds the downlink subframe starting with a frame control section containing the DL-MAP and UL-MAP messages. These indicate PHY transitions on the downlink as well as bandwidth allocations and burst profiles on the uplink. The DL-MAP is always applicable to the current frame and is always at least two FEC blocks long. The first PHY transition is expressed in the first FEC block, to allow adequate processing time. In both
TDD and FDD systems, the ULMAp provides allocations starting no later than the next downlink frame. The UL-MAP can, however, allocate starting in the current frame as long as processing times and round-trip delays are observed. The minimum time between receipt and applicability of the UL-MAP for an FDD system is shown in the following figure

![Figure 5. Minimum FDD map relevance.](image)

### Radio Link Control

The advanced technology of the 802.16 PHY requires equally advanced radio link control (RLC), particularly the capability of the PHY to transition from one burst profile to another. The RLC must control this capability as well as the traditional RLC functions of power control and ranging. RLC begins with periodic BS broadcast of the burst profiles that have been chosen for the uplink and downlink. The particular burst profiles used on a channel are chosen based on a number of factors, such as rain region and equipment capabilities. Burst profiles for the downlink are each tagged with a Downlink Interval Usage Code (DIUC). Those for the uplink are each tagged with an Uplink Interval Usage Code (UIUC).

During initial access, the SS performs initial power leveling and ranging using ranging request (RNG-REQ) messages transmitted in initial maintenance windows. The adjustments to the SS’s transmit time advance, as well as power adjustments, are returned...
to the SS in ranging response (RNG-RSP) messages. For ongoing ranging and power adjustments, the BS may transmit unsolicited RNG-RSP messages commanding the SS to adjust its power or timing. During initial ranging, the SS also requests to be served in the downlink via a particular burst profile by transmitting its choice of DIUC to the BS. The choice is based on received downlink signal quality measurements performed by the SS before and during initial ranging.

The BS may confirm or reject the choice in the ranging response. Similarly, the BS monitors the quality of the uplink signal it receives from the SS. The BS commands the SS to use a particular uplink burst profile simply by including the appropriate burst profile UIUC with the SS’s grants in ULMAP messages. After initial determination of uplink and downlink burst profiles between the BS and a particular SS, RLC continues to monitor and control the burst profiles. Harsher environmental conditions, such as rain fades, can force the SS to request a more robust burst profile. Alternatively, exceptionally good weather may allow an SS to temporarily operate with a more efficient burst profile. The RLC continues to adapt the SS’s current UL and DL burst profiles, ever striving to achieve a balance between robustness and efficiency. Because the BS is in control and directly monitors the uplink signal quality, the protocol for changing the uplink burst profile for an SS is simple: the BS merely specifies the profile’s associated UIUC whenever granting the SS bandwidth in a frame. This eliminates the need for an acknowledgment, since the SS will always receive either both the UIUC and the grant or neither. Hence, no chance of uplink burst profile Mismatch between the BS and SS exists.

In the downlink, the SS is the entity that monitors the quality of the receive signal and therefore knows when its downlink burst profile should change. The BS, however, is the entity in control of the change. There are two methods available to the SS to request a change in downlink burst profile, depending on whether the SS operates in the grant per connection (GPC) or grant per SS (GPSS) mode (see “Bandwidth Requests and Grants”). The first method would typically apply (based on the discretion of the BS scheduling
algorithm) only to GPC SSs. In this case, the BS may periodically allocate a station maintenance interval to the SS.

The SS can use the RNG-REQ message to request a change in downlink burst profile. The preferred method is for the SS to transmit a downlink burst profile change request (DBPC-REQ). In this case, which is always an option for GPSS SSs and can be an option for GPC SSs, the BS responds with a downlink burst profile change response (DBPC-RSP) message confirming or denying the change. Because messages may be lost due to irrecoverable bit errors, the protocols for changing an SS’s downlink burst profile must be carefully structured.

The order of the burst profile change actions is different when transitioning to a more robust burst profile than when transitioning to a less robust one. The standard takes advantage of the fact that an SS is always required to listen to more robust portions of the downlink as well as the profile that was negotiated.

Uplink Scheduling Services

Each connection in the uplink direction is mapped to a scheduling service. Each scheduling service is associated with a set of rules imposed on the BS scheduler responsible for allocating the uplink capacity and the request-grant protocol between the SS and the BS. The detailed specification of the rules and the scheduling service used for a particular uplink connection is negotiated at connection setup time.

The scheduling services in IEEE 802.16 are based on those defined for cable modems in the DOCSIS standard Unsolicited grant service (UGS) is tailored for carrying services that generate fixed units of data periodically. Here the BS schedules regularly, in a preemptive manner, grants of the size negotiated at connection setup, without an explicit request from the SS. This eliminates the overhead and latency of bandwidth
requests in order to meet the delay and delay jitter requirements of the underlying service. A practical limit on the delay jitter is set by the frame duration. If more stringent jitter requirements are to be met, output buffering is needed.

Services that typically would be carried on a connection with UGS service include ATM constant bit rate (CBR) and E1/T1 over ATM. When used with UGS, the grant management subheader includes the poll-me bit (see “Bandwidth Requests and Grants”) as well as the slip indicator flag, which allows the SS to report that the transmission queue is backlogged due to factors such as lost grants or clock skew between the IEEE 802.16 system and the outside network. The BS, upon detecting the slip indicator flag, can allocate some additional capacity to the SS, allowing it to recover the normal queue state. Connections configured with UGS are not allowed to utilize random access opportunities for requests.

The real-time polling service is designed to meet the needs of services that are dynamic in nature, but offers periodic dedicated request opportunities to meet real-time requirements. Because the SS issues explicit requests, the protocol overhead and latency is increased, but this capacity is granted only according to the real need of the connection. The real-time polling service is well suited for connections carrying services such as VoIP or streaming video or audio. The non-real-time polling service is almost identical to the real-time polling service except that connections may utilize random access transmit opportunities for sending bandwidth requests. Typically, services carried on these connections tolerate longer delays and are rather insensitive to delay jitter. The non-real-time polling service is suitable for Internet access with a minimum guaranteed rate and for ATM GFR connections. A best effort service has also been defined.

Neither throughput nor delay guarantees are provided. The SS sends requests for bandwidth in either random access slots or dedicated transmission opportunities. The occurrence of dedicated opportunities is subject to network load, and the SS cannot rely on their presence.
Bandwidth Requests and Grants

The IEEE 802.16 MAC accommodates two classes of SS, differentiated by their ability to accept bandwidth grants simply for a connection or for the SS as a whole. Both classes of SS request bandwidth per connection to allow the BS uplink scheduling algorithm to properly consider QoS when allocating bandwidth. With the grant per connection (GPC) class of SS, bandwidth is granted explicitly to a connection, and the SS uses the grant only for that connection. RLC and other management protocols use bandwidth explicitly allocated to the management connections.

With the grant per SS (GPSS) class, SSs are granted bandwidth aggregated into a single grant to the SS itself. The GPSS SS needs to be more intelligent in its handling of QoS. It will typically use the bandwidth for the connection that requested it, but need not. For instance, if the QoS situation at the SS has changed since the last request, the SS has the option of sending the higher QoS data along with a request to replace this bandwidth stolen from a lower QoS connection.

The SS could also use some of the bandwidth to react more quickly to changing environmental conditions by sending, for instance, a DBPC-REQ message. The two classes of SS allow a trade-off between simplicity and efficiency. The need to explicitly grant extra bandwidth for RLC and requests, coupled with the likelihood of more than one entry per SS, makes GPC less efficient and scalable than GPSS. Additionally, the ability of the GPSS SS to react more quickly to the needs of the PHY and those of connections enhances system performance. GPSS is the only class of SS allowed with the 10–66 GHz PHY.

With both classes of grants, the IEEE 802.16 MAC uses a self-correcting protocol rather than an acknowledged protocol. This method uses less bandwidth. Furthermore, acknowledged protocols can take additional time, potentially adding delay. There are a
number of reasons the bandwidth requested by an SS for a connection may not be available:

- The BS did not see the request due to irrecoverable PHY errors or collision of a contention-based reservation.
- The SS did not see the grant due to irrecoverable PHY errors.
- The BS did not have sufficient bandwidth available.
- The GPSS SS used the bandwidth for another purpose.

In the self-correcting protocol, all of these anomalies are treated the same. After a timeout appropriate for the QoS of the connection (or immediately, if the bandwidth was stolen by the SS for another purpose), the SS simply requests again. For efficiency, most bandwidth requests are incremental; that is, the SS asks for more bandwidth for a connection. However, for the self-correcting bandwidth request/grant mechanism to work correctly the bandwidth requests must occasionally be aggregate; that is, the SS informs the BS of its total current bandwidth needs for a connection. This allows the BS to reset its perception of the SS’s needs without a complicated protocol acknowledging the use of granted bandwidth. The SS has a plethora of ways to request bandwidth, combining the determinism of unicast polling with the responsiveness of contention-based requests and the efficiency of unsolicited bandwidth. For continuous bandwidth demand, such as with CBR T1/E1 data, the SS need not request bandwidth; the BS grants it unsolicited.

To short-circuit the normal polling cycle, any SS with a connection running UGS can use the poll-me bit in the grant management subheader to let the BS know it needs to be polled for bandwidth needs on another connection. The BS may choose to save bandwidth by polling SSs that have unsolicited grant services only when they have set the poll-me bit.

A more conventional way to request bandwidth is to send a bandwidth request MAC PDU that consists of simply the bandwidth request header and no payload. GPSS SSs can send this in any bandwidth allocation they receive. GPC terminals can send it in
either a request interval or a data grant interval allocated to their basic connection. A closely related method of requesting data is to use a grant management subheader to piggyback a request for additional bandwidth for the same connection within a MAC PDU. In addition to polling individual SSs, the BS may issue a broadcast poll by allocating a request interval to the broadcast CID. Similarly, the standard provides a protocol for forming multicast groups to give finer control to contention based polling. Due to the nondeterministic delay that can be caused by collisions and retries, contention based request are allowed for only for certain lower QoS class of services.

**Channel Acquisition**

The MAC protocol includes an initialization procedure designed to eliminate the need for manual configuration. Upon installation, an SS begins scanning its frequency list to find an operating channel. It may be programmed to register with a specified BS, referring to a programmable BS ID broadcast by each. This feature is useful in dense deployments where the SS might hear a secondary BS due to selective fading or when the SS picks up a sidelobe of a nearby BS antenna. After deciding on which channel or channel pair to attempt communication, the SS tries to synchronize to the downlink transmission by detecting the periodic frame preambles. Once the physical layer is synchronized, the SS will look for the periodically broadcast DCD and UCD messages that enable the SS to learn the modulation and FEC schemes used on the carrier.

**Initial Ranging and Negotiation of SS Capabilities**

Upon learning what parameters to use for its initial ranging transmissions, the SS will look for initial ranging opportunities by scanning the UL-MAP messages present in every frame. The SS uses a truncated exponential backoff algorithm to determine which initial ranging slot it will use to send a ranging request message. The SS will send the burst using the minimum power setting and will try again with increasingly higher transmission power if it does not receive a ranging response. Based on the arrival time of the initial ranging request and the measured power of the signal, the BS commands a
timing advance and a power adjustment to the SS in the ranging response. The response also provides the SS with the basic and primary management CIDs. Once the timing advance of the SS transmissions has been correctly determined, the ranging procedure for fine-tuning the power can be performed using invited transmissions.

All transmissions up to this point are made using the most robust, and thus least efficient, burst profile. To avoid wasting capacity, the SS next reports its PHY capabilities, including the modulation and coding schemes it supports and whether, in an FDD system, it is half-duplex or full-duplex. The BS, in its response, can deny the use of any capability reported by the SS.

SS Authentication and Registration

Each SS contains both a manufacturer-issued factory-installed X.509 digital certificate and the certificate of the manufacturer. These certificates, which establish a link between the 48-bit MAC address of the SS and its public RSA key, are sent to the BS by the SS in the Authorization Request and Authentication Information messages. The network is able to verify the identity of the SS by checking the certificates and can subsequently check the level of authorization of the SS.

If the SS is authorized to join the network, the BS will respond to its request with an Authorization Reply containing an Authorization Key (AK) encrypted with the register with the network. This will establish the secondary management connection of the SS and determine capabilities related to connection setup and MAC operation. The version of IP used on the secondary management connection is also determined during registration.

IP Connectivity

After registration, the SS attains an IP address via DHCP and establishes the time of day via the Internet Time Protocol. The DHCP server also provides the address of the TFTP server from which the SS can request
a configuration file. This file provides a standard interface for providing vendor-specific configuration information.

**Connection Setup**

IEEE 802.16 uses the concept of service flows to define unidirectional transport of packets on either downlink or uplink. Service flows are characterized by a set of QoS parameters such as latency and jitter. To most efficiently utilize network resources such as bandwidth and memory, 802.16 adopts a two-phase activation model in which resources assigned to a particular admitted service flow may not be actually committed until the service flow is activated. Each admitted or active service flow is mapped to a MAC connection with a unique CID.

In general, service flows in IEEE 802.16 are preprovisioned, and setup of the service flows is initiated by the BS during SS initialization. However, service flows can also be dynamically established by either the BS or the SS. The SS typically initiates service flows only if there is a dynamically signaled connection, such as a switched virtual connection (SVC) from an ATM network. The establishment of service flows is performed via a three-way handshaking protocol in which the request for service flow establishment is responded to and the response acknowledged. In addition to dynamic service establishment, IEEE 802.16 also supports dynamic service changes in which service flow parameters are renegotiated. Like dynamic service flow establishment, service flow changes also follow a similar three-way handshaking protocol.

**Privacy Sublayer**

IEEE 802.16’s privacy protocol is based on the Privacy Key Management (PKM) protocol of the DOCSIS BPI+ specification but has been enhanced to fit seamlessly into the IEEE 802.16 MAC protocol and to better accommodate stronger cryptographic methods, such as the recently approved Advanced Encryption Standard.
Security Associations

PKM is built around the concept of security associations (SAs). The SA is a set of cryptographic methods and the associated keying material; that is, it contains the information about which algorithms to apply, which key to use, and so on. Every SS establishes at least one SA during initialization. Each connection, with the exception of the basic and primary management connections, is mapped to an SA either at connection setup time or dynamically during operation.

Cryptographic Methods

Currently, the PKM protocol uses X.509 digital certificates with RSA public key encryption for SS authentication and authorization key exchange. For traffic encryption, the Data Encryption Standard (DES) running in the cipher block chaining (CBC) mode with 56-bit keys is currently mandated. The CBC initialization vector is dependent on the frame counter and differs from frame to frame. To reduce the number of computationally intensive public key operations during normal operation, the transmission encryption keys are exchanged using 3DES with a key exchange key derived from the authorization key. The PKM protocol messages themselves are authenticated using the Hashed Message Authentication Code (HMAC) protocol with SHA-1. In addition, message authentication in vital MAC functions, such as the connection setup, is provided by the PKM protocol.

WiMAX Focuses on Interoperability

WiMAX (the Worldwide Interoperability for Microwave Access Forum) aims in promoting the adoption of IEEE 802.16 compliant equipment by operators of broadband wireless access systems. The organization is working to facilitate the deployment of
broadband wireless networks based on the IEEE 802.16 standard by helping to ensure the compatibility and interoperability of broadband wireless access equipment. In this regard, the philosophy of WiMAX for the wireless MAN is comparable to that of the Wi-Fi* Alliance in promoting the IEEE 802.11 standard for wireless LANs.

In an effort to bring interoperability to broadband Wireless Access, WiMAX is focusing its efforts on establishing a unique subset of baseline features grouped in what is referred to as “System Profiles” that all compliant equipment must satisfy. These profiles will establish a baseline protocol that allows equipment from multiple vendors to interoperate, and that also provides system integrators and service providers with the ability to purchase equipment from more than one supplier. System Profiles can address the regulatory spectrum constraints faced by operators in different geographies. For example, a service provider in Europe operating in the 3.5 GHz band who has been allocated 14 MHz of spectrum is likely to want equipment that supports 3.5 and/or 7 MHz channel bandwidths and TDD (time-division duplex) or FDD (frequency-division duplex) operation. Similarly, a WISP in the U.S. using license exempt spectrum in the 5.8 GHz UNII band may desire equipment that supports TDD and a 10 MHz bandwidth.

WiMAX will establish a structured compliance procedure based upon the proven test methodology specified by ISO/IEC 9646. The process starts with standardized Test Purposes written in English, which are then translated into Standardized Abstract Test Suites in a language called TTCN3. In parallel, the Test Purposes are also used as input to generate test tables referred to as the PICS (Protocol Implementation Conformance Statement) pro forma. The end result is a complete set of test tools that WiMAX will make available to equipment developers so they can design in conformance and interoperability during the earliest possible phase of product development.

Typically, this activity will begin when the first integrated prototype becomes available. Ultimately, the WiMAX suite of conformance tests, in conjunction with interoperability events, will enable service providers to choose from multiple vendors of broadband wireless access equipment that conforms to the IEEE 802.16a standard and that is optimized for their unique operating environment. Internationally, WiMAX will work with ETSI, the European Telecommunications Standards Institute, to develop
similar test suites for the ETSI HIPERMAN standard for European broadband wireless metropolitan area access.

IEEE 802.20 (Mobile-Fi) (Mobile Broadband Wireless Access Working Group)

IEEE 802.20 mission: Develop the specification for an efficient packet based air interface that is optimized for the transport of IP-based services. IEEE 802.20 scope: Specification of physical and medium access control layers of an air interface for interoperable mobile broadband wireless access systems, in licensed bands below 3.5GHz, optimized for IP data transport, with peak data rates per user in excess of 1Mbps. It supports various vehicular mobility classes up to 250 Km/h in a MAN environment and targets spectral efficiencies, sustained user data rates and numbers of active users that are all significantly higher than achieved by existing mobile systems.

“One key feature of 4G and B3G systems is likely to be the availability of much higher data rates than those in third generation systems. Higher spectral efficiency and lower cost per transmitted bit are other key requirements. Additional important expected features are increased flexibility of mobile terminals and networks, multimedia services and high speed data connections. A future convergence with digital broadcasting systems is yet another expected feature. The use of multiple transmit and receive antennas for achieving radio links with increased reliability and efficiency will probably also be a feature of such future systems. Also multiple access schemes that would be able to efficiently share high capacity of these systems among different users in an asynchronous channel.

802.16 aspects
➢ First standard (April 2002) defines the air interface for systems intended “to provide network access to homes, small businesses, and commercial buildings as an alternative to traditional wired connections”.

➢ Can economically serve up to 60 customers with T-speed (1.5Mbps) connections (and) can provide a feasible backhaul for connecting wireless LAN hotspots.

➢ Point-to-multipoint in 10-66 GHz range at data rates up to 120 Mbps. Generally line of sight with range up to 30 miles (802.16a extends to non line of sight operation in 2-11GHz range.)

➢ Medium access layer uses TDMA for both upstream and downstream transmissions. Supports both FDD (freq. division duplex) and TDD (time division duplex) operational modes.

➢ Up to 134 Mbps in 28 MHz channel (in 10-66 GHz air interface)

➢ QoS for multiple services (IPv4, IPv6, ATM, Ethernet, …)

➢ Frame-by-frame bandwidth on demand

➢ Comprehensive security

➢ Multiple frequency allocations from 2-66 GHz; OFDM and OFDMA for non line of sight applications

➢ TDD and FDD

➢ Link adaptation: adaptive modulation and coding, subscriber by subscriber, burst by burst, uplink and downlink

1) Point to multipoint topology, with mesh extensions

2) Support for adaptive antennas and space-time coding

3) New extensions to mobility

802.16a MODULATION
Retains single-carrier access method of original 802.16 for special purpose networks.

- Adds 256-carrier OFDM layer.
- Defines 2048-carrier OFDM (orthogonal freq. division multiple access) layer “which offers advanced multiplexing in tiered MANs and supports selective multicast applications”
- Spectral efficiency up to 5 bits/sec/Hz.

Differentiating the IEEE 802.16a and 802.11 Standards
- Wi-Fi versus WiMAX Scalability

At the PHY layer the standard supports flexible RF channel bandwidths and reuse of these channels (frequency reuse) as a way to increase cell capacity as the network grows. The standard also specifies support for automatic transmit power control and channel quality measurements as additional PHY layer tools to support cell planning/deployment and efficient spectrum use. Operators can re-allocate spectrum through sectorization and cell splitting as the number of subscribers grows. Also, support for multiple channel bandwidths enables equipment makers to provide a means to address the unique government spectrum use and allocation regulations faced by operators in diverse international markets.

The IEEE 802.16a standard specifies channel sizes ranging form 1.75MHz up to 20MHz with many options in between. Wi-Fi based products on the other hand require at least 20MHz for each channel (22MHz in the 2.4GHz band for 802.11b), and have specified only the license exempt bands 2.4GHz ISM, 5GHz ISM and 5GHz UNII for operation.

In the MAC layer, the CSMA/CA foundation of 802.11, basically a wireless Ethernet protocol, scales about as well as does Ethernet. That is to say - poorly. Just as in an Ethernet LAN, more users results in a geometric reduction of throughput, so does the
CSMA/CA MAC for WLANs. In contrast the MAC layer in the 802.16 standard has been designed to scale from one up to 100's of users within one RF channel, a feat the 802.11 MAC was ever designed for and is incapable of supporting.

Coverage

The BWA standard is designed for optimal performance in all types of propagation environments, including LOS, near LOS and NLOS environments, and delivers reliable robust performance even in cases where extreme link pathologies have been introduced. The robust OFDM waveform supports high spectral efficiency (bits per second per Hertz) over ranges from 2 to 40 kilometers with up to 70 Mbps in a single RF channel. Advanced topologies (mesh networks) and antenna techniques (beam-forming, STC, antenna diversity) can be employed to improve coverage even further.

These advanced techniques can also be used to increase spectral efficiency, capacity, reuse, and average and peak throughput per RF channel. In addition, not all OFDM is the same. The OFDM designed for BWA has in it the ability to support longer range transmissions and the multi-path or reflections encountered. In contrast, WLANs and 802.11 systems have at their core either a basic CDMA approach or use OFDM with a much different design, and have as a requirement low power consumption limiting the range. OFDM in the WLAN was created with the vision of the systems covering tens and maybe a few hundreds of meters versus 802.16 which is designed for higher power and an OFDM approach that supports deployments in the tens of kilometers.

QoS

The 802.16a MAC relies on a Grant/Request protocol for access to the medium and it supports differentiated service levels (e.g., dedicated T1/E1 for business and best effort for residential). The protocol employs TDM data streams on the DL (downlink) and TDMA on the UL (uplink), with the hooks for a centralized scheduler to support delay-sensitive services like voice and video.
By assuring collision-free data access to the channel, the 16a MAC improves total system throughput and bandwidth efficiency, in comparison with contention-based access techniques like the CSMA-CA protocol used in WLANs. The 16a MAC also assures bounded delay on the data (CSMA-CA by contrast, offers no guarantees on delay). The TDM/TDMA access technique also ensures easier support for multicast and broadcast services. With a CSMA/CA approach at its core, WLANs in their current implementation will never be able to deliver the QoS of a BWA, 802.16 system.

The WiMAX Forum-Interoperability for 802.16 Compliant Systems

Establishment of a standard is critical to mass adoption of a given technology; however by itself a standard is not enough. The 802.11b WLAN standard was ratified in 1999, however it did not reach mass adoption until the introduction of the Wi-Fi Alliance and certified, interoperable equipment was available in 2001. In order to bring interoperability to the Broadband Wireless Access space, the WiMAX Forum is focused on establishing a unique subset of baseline features grouped in what is referred to as "System Profiles" that all compliant equipment must satisfy. These profiles and a suite of test protocols will establish a baseline interoperable protocol, allowing multiple vendors' equipment to interoperate; with the net result being System Integrators and Service Providers will have option to purchase equipment from more than one supplier. Profiles can address, for example, the regulatory spectrum constraints faced by operators in different geographies. For example, a service provider in Europe operating in the 3.5 GHz band, who has been allocated 14 MHz of spectrum, is likely to want equipment that supports 3.5 and/or 7 MHz channel bandwidths and, depending on regulatory requirements, TDD (time-division duplex) or FDD (frequency-division duplex) operation. Similarly, a WISP (Wireless Internet Service Provider) in the
U.S. using license-exempt spectrum in the 5.8GHz UNII band might desire equipment that supports TDD and a 10 MHz bandwidth.

WiMAX is establishing a structured compliance procedure based upon the proven test methodology specified by ISO/IEC 9646. The process starts with standardized Test Purposes written in English, which are then translated into Standardized Abstract Test Suites in a language called TTCN. In parallel with the Test Purposes, the Test Purposes are also used as input to generate test tables referred to as the PICS (Protocol Implementation Conformance Statement) Proforma is generated. The end result is a complete set of test tools that WiMAX will make available to equipment developers so they can design-in conformance and interoperability during the earliest possible phase of product development. Typically, this activity will commence when the first integrated prototype becomes available.

Ultimately, the WiMAX Forum suite of conformance tests, in conjunction with interoperability testing, will enable service providers to choose from multiple vendors offering broadband wireless access equipment conforming to the IEEE 802.16a standard, that is optimized for their unique operating environment.
CONCLUSION

The latest developments in the IEEE 802.16 group are driving a broadband wireless access revolution thanks to a standard with unique technical characteristics. In parallel, the WiMAX forum, backed by industry leaders, helps the widespread adoption of broadband wireless access by establishing a brand for the technology. Initially, WiMAX will bridge the digital divide and thanks to competitive equipment prices, the scope of WiMAX deployment will broaden to cover markets where the low POTS penetration, high DSL unbundling costs, or poor copper quality have acted as a brake on extensive high-speed Internet and voice over broadband. WiMAX will reach its peak by making Portable Internet a reality.

When WiMAX chipsets are integrated into laptops and other portable devices, it will provide high-speed data services on the move, extending today's limited coverage of public WLAN to metropolitan areas. Integrated into new generation networks with seamless roaming between various accesses, it will enable endusers to enjoy an "Always Best Connected" experience. The combination of these capabilities makes WiMAX attractive for a wide diversity of people: fixed operators, mobile operators and wireless ISPs, but also for many vertical markets and local authorities. Alcatel, the worldwide broadband market leader with a market share in excess of 37%, is committed to offer complete support across the entire investment and operational cycle required for successful deployment of WiMAX services.