



Intel[®] Technology Journal

WiMAX

Global, Interoperable Broadband Wireless Networks: Extending WiMAX Technology to Mobility

Global, Interoperable Broadband Wireless Networks: Extending WiMAX Technology to Mobility

Ed Agis, Intel Communications Group, Intel Corporation
Henry Mitchel, Intel Communications Group, Intel Corporation
Shlomo Ovadia, Intel Communications Group, Intel Corporation
Selim Aissi, Corporate Technology Group, Intel Corporation
Sanjay Bakshi, Corporate Technology Group, Intel Corporation
Prakash Iyer, Corporate Technology Group, Intel Corporation
Masud Kibria, Corporate Technology Group, Intel Corporation
Christopher Rogers, Corporate Technology Group, Intel Corporation
James Tsai, Corporate Technology Group, Intel Corporation

Index words: 802.16, WiMAX, OFDM, OFDMA, portability, mobility, broadband wireless architecture, PKM, WiMAX certification, interoperability

ABSTRACT

IEEE* 802.16 is an emerging global broadband wireless access standard capable of delivering multiple megabits of shared data throughput supporting fixed, portable, and mobile operation. The standard offers a great deal of design flexibility including support for licensed and license-exempt frequency bands, channel widths ranging from 1.25 to 20 MHz, Quality of Service (QoS) establishment on a per-connection basis, strong security primitives, multicast support, and low latency/low packet loss handovers¹. Mass deployments of Subscriber Stations (SS) and Access Points² (AP) for portable and mobile services are expected to be based on scalable Orthogonal Frequency Division Multiplexing with Multiple Access (OFDMA). A broad range of network operators are anticipated to deploy such systems in licensed frequencies below 11 GHz. However, universal acceptance of 802.16 for portable and mobile use is contingent on the Industry's development, acceptance,

and conformance to two complementary aspects of the IEEE 802.16 air interface standards work: (1) development and adoption of an open and extensible end-to-end architecture framework and specification that is agnostic to incumbent operator backend networks; and (2) a means for ensuring spec-compliant and vendor interoperable equipment to support cost-effective deployments and give users the capability to roam across networks established by different network operators. A common architecture framework and standardized compliance testing mechanisms based on a suite of PHY and MAC profiles will enable multivendor interoperability supporting different deployment and use-case scenarios. In this paper, we describe Intel's 802.16 architecture vision and the Worldwide Interoperability Microwave Access (WiMAX) certification process to address these two important market needs.

INTRODUCTION

IEEE 802.16 is an emerging suite of air interface standards for combined fixed, portable, and Mobile Broadband Wireless Access (MBWA). Initially conceived as a radio standard to enable cost-effective last-mile broadband connectivity to those not served by wired broadband such as cable or DSL, the specifications are evolving to target a broader market opportunity for mobile, high-speed broadband applications. The promise of realizing a low-cost, broadly interoperable wide-area data network that supports portable and mobile usage

*Other brands and names are the property of their respective owners

¹ Optimization of PHY and MAC handover primitives is ongoing in the 802.16e Task Group and is expected to be completed by the end of 2004.

² In this paper the term Access Point is synonymous with Base Station, and an AP can be logically broken into a combination of one APC and one or more APTs.

could have significant end-user benefits. Notably, this network can complement and extend the Wi-Fi hotspot usage model to provide broader Internet Protocol (IP) data service coverage and roaming that has so far eluded current 3G systems, due to system cost and complexity.

The 802.16-2004 [1] standard to be published later this year supersedes all previous versions as the base standard and specifies networks for the current fixed access market segment. The 802.16e [2] amendment and the soon to be approved 802.16f and 802.16g task groups will amend the base specification to enable not just fixed, but also portable and mobile operation in frequency bands below 6 GHz.

802.16 is optimized to deliver high, bursty data rates to Subscriber Stations (SS) but the sophisticated Medium Access Control (MAC) architecture can simultaneously support real-time multimedia and isochronous applications such as Voice Over IP (VoIP) as well. This means that IEEE 802.16 is uniquely positioned to extend broadband wireless beyond the limits of today's Wi-Fi systems, both in distance and in the ability to support applications requiring advanced Quality of Service (QoS) such as VoIP, streaming video, and on-line gaming.

The technology is expected to be adopted by different incumbent operator types—for example, Wireless Internet Service Providers (WISPs), cellular operators (CDMA and WCDMA), and wireline broadband providers. Each of these operators will approach the market with different business models, each based on their current markets and perceived opportunities for broadband wireless as well as different requirements for integration with existing (legacy) networks. As a result, 802.16 network deployments face the challenging task of needing to adapt to different network architectures while still supporting standardized components and interfaces for multivendor interoperability.

This paper is organized into two main sections. The first section presents Intel's deployment vision and architecture framework for 802.16. The architecture and usage is presented as a two-stage evolution: initially combining fixed access with portability and scaling up to evolve to full mobility. The framework is based on several core principles:

- Support for different Radio Access Network (RAN) topologies.
- Well-defined interfaces to enable 802.16 RAN architecture independence while enabling seamless

integration and interworking with Wi-Fi, 3GPP³ and 3GPP2 networks.

- Leverage open, Internet Engineering Task Force (IETF)-defined IP technologies to build scalable all-IP 802.16 access networks using Common Off The Shelf (COTS) equipment.
- Support for IPv4 and IPv6 clients and application servers; recommending use of IPv6 in the infrastructure.
- Functional extensibility to support future migration to full mobility and delivery of rich broadband multimedia.

In the second section, the WiMAX certification process with its key building blocks is reviewed. The WiMAX certification process, which is being established by the WiMAX Forum, enables multivendor interoperability of subscriber systems and access points for this ecosystem.

BROADBAND WIRELESS DEPLOYMENT SCENARIOS

Initial deployments of IEEE 802.16 standards-based networks will likely target fixed access connectivity to unserved and underserved markets where wireline broadband services are insufficient to fulfill the market need for high-bandwidth Internet connectivity. Pre-standards implementations exist today that are beginning to address this fixed access service environment. Standardization will help accelerate the ramp for these fixed access solutions by providing interoperability amongst equipment and economies of scale resulting from high-volume standards-based components.

As IEEE 802.16 solutions evolve to address portable and mobile applications, the required features and performance of the system will increase. Beyond fixed access service, even larger market opportunities exist for providing cost-effective broadband data services to users on the go. Initially this includes portable connectivity for customers who are not within reach of their existing fixed broadband or WLAN service options. This type of service is characterized by access that is unwired but stationary in most cases, albeit with some limited provisions for user mobility during the connection. In this manner, 802.16 can be seen as augmenting coverage of 802.11 for private and public service networks and cost effectively extending hotspot availability to wider ranges of

³ 3GPP – Third Generation Partnership Project – a collaborative effort between ARIB, CCSA, ETSI, ATIS, TTA, and TTC to develop 3G telecommunications standards. 3GPP2 is a similar collaborative effort between ANSI, TTA and EIA-41.

coverage. Based on this described capability, this phase of deployment is referred to as “Portability with Simple Mobility.”

The next phase of functionality, known as “Full Mobility” provides incremental support for low latency, low packet loss real-time handovers between APs at speeds of 120 km/hr or higher, both within a network and between networks. This will deliver a rich end-user experience for high-quality multimedia applications. Figure 1 summarizes Intel’s deployment evolution vision of the 802.16 standard.

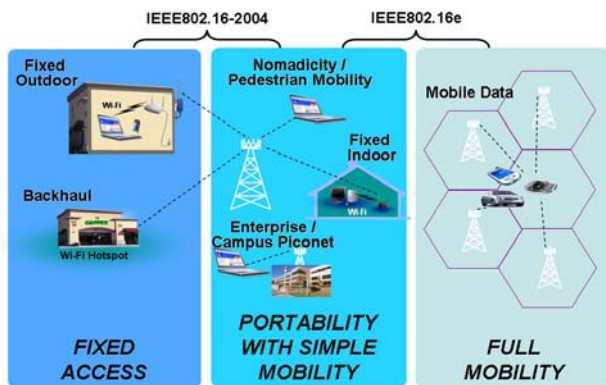


Figure 1: 802.16 standards and deployment evolution

To support the incremental functionality beyond fixed access deployment, there are required enhancements to both the air interface and network infrastructure. Both of these enhancements must also be standardized before interoperable services meeting end user demands can be realized. To understand these requirements, we need to examine usage models and service models for each stage of 802.16 deployment. From these usage expectations, we can then draw conclusions about required system capabilities that must be driven into the end-to-end architecture, interfaces, and network features. The usage evolution is depicted in Figure 2.

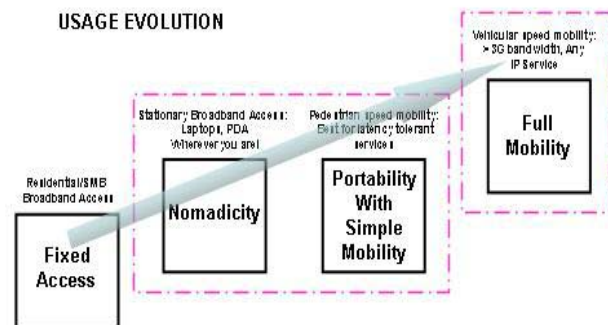


Figure 2: Usage evolution

Service and consumer usage of 802.16 for fixed access is expected to mirror that of fixed wireline service with many of the standards-based requirements being confined to the air interface. Because communication takes place via wireless links from customer premises equipment to remote Non Line of Sight (NLOS) APs, requirements for link security are increased beyond those needed for wireline service. The security mechanisms within the IEEE 802.16-2004 standard may be adequate for fixed access service, but need to be enhanced for portable and mobile applications.

An additional challenge for the fixed access air interface—as well as subsequent portable and mobile service—is the need to establish high-performance radio links capable of data rates comparable to wired broadband service, using equipment that can be self installed indoors by users, as is the case for DSL and cable modems. Doing so requires advanced Physical (PHY) layer techniques to achieve link margins capable of supporting high throughput in NLOS environments.

As 802.16 technology evolves to address portable and mobile service, so do the feature requirements of the air interface and RAN network, interoperability demands, and interworking with other dissimilar networks like Wi-Fi and 3G. The simple fact that mobile clients can dynamically associate and perform handover across APs crossing large, possibly discontinuous geographic regions and operator domains, drives the need for a number of network-related enhancements.

The simplest case of portable service (referred to as Nomadicity) involves a user transporting an 802.16 modem to a different location. Provided this visited location is served by wireless broadband service, in this

scenario, the user re-authenticates and manually re-establishes new IP connections and is afforded broadband service at the visited location.

This usage enhancement over fixed access requires enhancements to security such as strong mutual authentication between the user/client device and the network AP supporting a flexible choice of credential types. Portable and mobile devices need a means for authenticating trusted APs and detecting rogue APs. Such mutual authentication is not present in the fixed access standard. Also a common centralized mechanism for user authentication is needed as users may move between different APs within an IP prefix or subnet, or across APs in different subnets, or even roam to other service providers in different locales.

The next stage, portability with simple mobility, describes a more automated management of IP connections with session persistence or automatic reestablishment following transitions between APs. This incremental enhancement allows for more user transparent mobility and is suitable for latency tolerant applications such as TCP [13]; it does not provide adequate handover performance for delay and packet loss sensitive real-time applications such as VoIP.

In the fully mobile scenario, user expectations for connectivity are comparable to those experienced in 3G voice/data systems. Users may be moving while simultaneously engaging in a broadband data access or multimedia streaming session. The need to support low latency and low packet loss handovers of data streams as users transition from one AP to another is clearly a challenging task. For mobile data services, users will not easily adapt their service expectations because of environmental limitations that are technically challenging but not directly relevant to the user (such as being stationary or moving). For these reasons, the network and air interface must be designed up front to anticipate these user expectations and deliver accordingly.

THE 802.16 RADIO-SCALING TO FULL MOBILITY

The 802.16 standard provides an excellent framework upon which systems can be built to satisfy the broad spectrum of usage models described above. Of the three PHY layers supported in the standard, scalable OFDMA is the most versatile and the one preferred for operation across channel widths ranging from 1.75 MHz to 20 MHz. Single Carrier Access (SCa) will likely be considered for backhaul links while OFDM with 256-point Fast Fourier Transform (FFT) is best suited for Fixed Access in up to 10 MHz channel widths. Scalable OFDMA supports features (enhanced over OFDM) that

are especially suited for high-speed mobile operation such as Downlink (DL) and Uplink (UL) subchannelization, fixed subcarrier spacing (by maintaining constant ratio of FFT size to channel width), and reduced overhead for Cyclic Prefix (CP) by keeping its duration constant at $1/8^{\text{th}}$ the OFDMA symbol duration.

The 802.16 MAC is designed for Point-to-Multipoint (PMP) applications and is based on Collision Sense Multiple Access with Collision Avoidance (CSMA/CA). The 802.16 AP MAC manages UL and DL resources including Transmit and Receive scheduling. The MAC incorporates several features suitable for a broad range of applications at different mobility rates, such as the following:

- Four service classes—Unsolicited Grant Service (UGS), real-time Polling Service (rtPS), non-real-time Polling Service (nrtPS), and Best Effort (BE).
- Header suppression, packing, and fragmentation for efficient use of spectrum.
- Privacy Key Management (PKM) for MAC layer security. PKM version 2 incorporates support for Extensible Authentication Protocol (EAP).
- Broadcast and Multicast support.
- Manageability primitives.
- High-speed handover and mobility management primitives.
- Three power management levels: Normal Operation, Sleep, and Idle (with paging support).

These features combined with the inherent benefits of scalable OFDMA make 802.16 suitable for high-speed data and bursty or isochronous IP multimedia applications.

REQUIREMENTS AND TENETS FOR A GLOBAL INTEROPERABLE END-TO-END ARCHITECTURE FRAMEWORK

The architecture framework presented in this paper is based on the following requirements:

- **Applicability:** The architecture shall be applicable to licensed and license-exempt 802.16 deployments.
- **Service Provider Categories:** The architecture, especially the RAN, shall be suitable for adoption by all incumbent operator types, examples of which were listed earlier.

- **Harmonization/Interworking:** The architecture shall lend itself to integration with an existing IP operator core network (e.g., DSL, cable, or 3G) via interfaces that are IP-based and not operator-domain specific. This permits reuse of mobile client software across operator domains.
- **Provisioning and Management:** The architecture shall accommodate a variety of online and offline client provisioning, enrollment, and management schemes based on open, broadly deployable Industry standards.
- **IP Connectivity:** The architecture shall support a mix of IPv4 and IPv6 network interconnects and communication endpoints and a variety of standard IP context management schemes.
- **IP Services:** The architecture shall support a broad range of TCP and UDP real-time and non-real-time applications.
- **Security:** The architecture shall support Subscriber Station (SS) authorization, strong bilateral user authentication based on a variety of authentication mechanisms such as username/password, X.509 certificates, Subscriber Identity Module (SIM), Universal SIM (USIM), Removable User Identity Module (RUIM), and provide services such as data integrity, data replay protection, data confidentiality, and non-repudiation using the maximum key lengths permissible under global export regulations.
- **Mobility Management:** The architecture shall scale from fixed access to fully mobile operation scenarios with scalable infrastructure evolution, eventually supporting low latency (< 100 msec) and virtually zero packet loss handovers at mobility speeds of 120 km/hr or higher.
- **IP Connectivity:** The architecture shall support a mix of IPv4 and IPv6 network interconnects and communication endpoints and a variety of standard IP context management schemes.

The architecture framework is based on the following principles:

- Extensive use of IETF standards for IP routing, AAA, QoS and traffic engineering protocols in the RAN and integration with an operator's IP core/data center, enabling multivendor infrastructure interoperability.
- Functional decomposition that supports mixed operation and scaling up from NLOS portable operation to seamless mobility across RAN clouds spanning multiple IP subnets or prefixes.

- RAN architecture independence from an operator IP core or other interconnected networks.
- Loosely coupled interworking with 3G and Wi-Fi networks.
- An end-to-end security framework that is compatible with Wi-Fi, supporting credential reuse and similar consistent use of AAA protocols.

END-TO-END ARCHITECTURE EVOLUTION

Figure 3 conceptually depicts the architecture evolution for 802.16. A basic 802.16-2004-based Fixed Access (indoor⁴ and outdoor) deployment is typically accomplished via a static provisioning relationship between an SS and an 802.16 AP. The collection of APs and interconnecting routers or switches comprising the RAN can be logically viewed as a contiguous cloud with no inter-AP mobility requirements from an SS perspective. The RAN(s) interconnect via a logically centralized operator IP core network to one or more external networks as shown. The operator IP core may host services such as IP address management, Domain Name Service (DNS) [12], media switching between IP packet-switched data and Public Switched Telephony Network (PSTN) circuit-switched data, 2.5G/3G/Wi-Fi harmonization and interworking, and VPN services (provider hosted or transit).

Going from Fixed access to Portability with Simple Mobility involving the use of Mobile SSs (MSS) such as laptops and Personal Device Assistants (PDA) introduces network infrastructure changes such as the need to support break-before-make micro- and macro-mobility⁵ handovers across APs with relaxed handover packet loss and latency⁶ (less than two seconds), cross-operator roaming, and the need to support reuse of user and MSS credentials across logically partitioned RAN clouds.

Going from Portability to Full Mobility requires support in the RAN for low (~zero) packet loss and low latency (<100 msec) make-before-break handovers and mechanisms such as Idle mode with paging for extended low-power operation.

⁴ Indoor operation may require use of Beam Forming or Multiple Input Multiple Output (MIMO) Advanced Antenna Systems (AAS) which are supported in the 802.16 standard.

⁵ Micro-mobility refers to handovers between APs within the same IP prefix or subnet domain. Macro-mobility refers to handovers across APs in different IP prefix or subnet domains.

⁶ Latency may be unacceptable for real-time IP services such as VoIP during handovers but acceptable for TCP and VPN services as well as store-and-forward multimedia services.

An important design consideration is QoS. Fixed Access and Portable usage models need only support acceptable QoS guarantees for stationary usage scenarios. Portability introduces the requirement to transfer the Service Level Agreement (SLA) across APs involved in a handover, although QoS may be relaxed during handovers. Full Mobility requires consistent QoS in all operating modes, including handovers. The 802.16 RAN will need to deliver Bandwidth and/or QoS on Demand as needed to support diverse real-time and non-real-time services over the 802.16 RAN. Besides the traditional Best Effort forwarding, the RAN will need to handle latency intolerant traffic generated by applications such as VoIP and interactive games.

The decoupling of the RAN from an operator IP core network permits incremental migration to fully mobile operation. An operator must however give due consideration to the RAN topology (such as coverage overlap, user capacity, and range) to ensure that the physical network is future-proof for such an evolution.

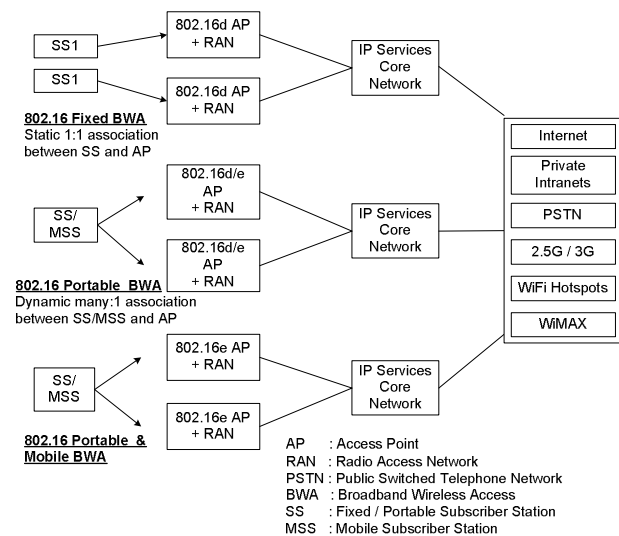


Figure 3: 802.16 architecture evolution

END-TO-END REFERENCE ARCHITECTURE

Figure 4 depicts an end-to-end reference architecture for 802.16. Various functional entities and interoperability interfaces are identified. The network essentially decomposes into three major functional aggregations: the 802.16 SS/MSS, the 802.16 RAN, and interconnect to various operator IP core and application provider networks. The IP core network a) manages the resources of the 802.16 RAN, and b) provides core network services such as address management, authentication, service authorization, and provisioning for 802.16 SS/MSSs.

The reference architecture, especially interconnectivity in the RAN and interconnects to remote IP networks, is based on extensive use of native IP suite of protocols that in turn can deliver desired economies of scale. In the sections below, we describe three logical entities: the Radio Network Serving Node (RNSN), AP, and SS/MSS. We also briefly describe the interoperability interfaces identified in Figure 4.

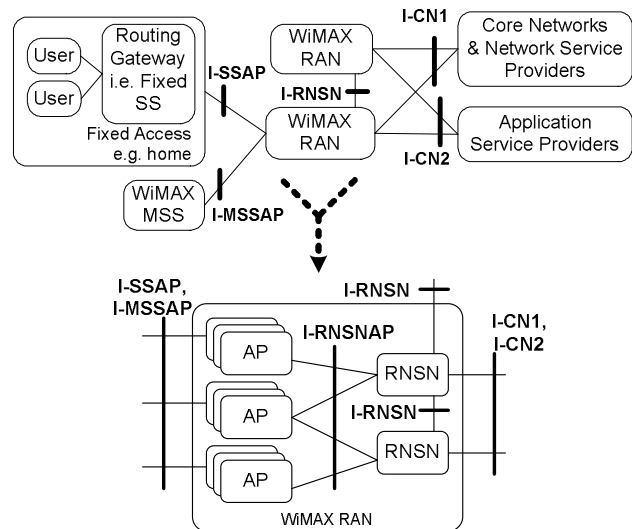


Figure 4: 802.16 reference architecture

Radio Network Serving Node (RNSN)

A Radio Network Service Node (RNSN) is a logical network entity that interfaces the RAN with the operator IP core network, Application Service Provider (ASP) networks, and other service networks such as IP Multimedia Subsystems (IMS), remote Enterprise Intranets, PSTN, and the Internet. Each RNSN instance manages a cloud of APs across a hybrid wireline/wireless backhaul network and is responsible for Radio Resource Management (RRM), data forwarding, and interconnects to back-end networks. Functions such as QoS, mobility, and security are cooperatively managed as a network of managed APs. An RNSN may also host RAN-specific centralized functions such as paging groups and macro mobility agents, an example of which is a Mobile IP (MIP) Foreign Agent (FA), and so on. An RNSN may be rendered on a convenient network infrastructure platform such as a Packet Data Gateway (PDG) [5] in 3GPP networks or a Packet Data Serving Node (PDSN) in a 3GPP2 network or on a standalone router platform.

Access Point (AP)

An 802.16 Access Point (referred to in the 802.16 standard as a base station) is a logical entity that provides the necessary over-the-air standards-compliant

functionality including SS/MSS admission control and all RRM and UL/DL scheduling.

We envision a number of AP/RAN topologies as depicted in Figure 5.

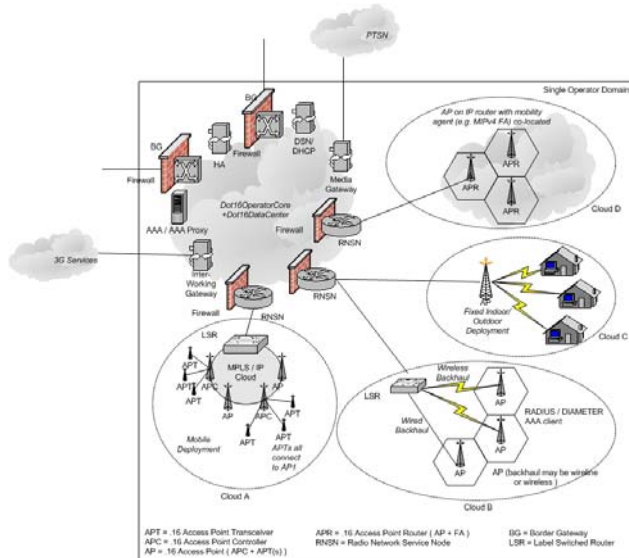


Figure 5: 802.16 RAN topologies

An AP may form a subnet/prefix boundary as indicated by an AP Router (APR) in the figure. An AP may be implemented as an integrated MAC/PHY entity or may take on a more distributed architecture involving an AP Controller (APC) and AP Transceivers (APT) that would render cells in groups.

A combination of an APC with one or more APT instances may render a multisector cell. Where multiple APTs are managed by an APC, the APC may host a common MAC instance across all APTs or a dedicated MAC instance for each APT. An APC would typically localize all micromobility functions across its managed APTs and as such would support all relevant 802.16 PHY, MAC, and Convergence Sublayer (CS) Service Access Point (SAP) primitives. An APC may also host optional wireless link services such as header suppression, payload compression, and MSS paging.

An AP hosting more than one logical APC instance can optimize control and management plane functions across all hosted instances. Factors such as projected scalability requirements (coverage, user density), degree of mobility, and need for incremental network growth would drive an operator's choices between the different AP configurations. However, the architecture framework is agnostic to specific RAN topologies and can support a mix of all possible variants simultaneously.

Mobile/Fixed Subscriber Station (MSS/SS)

Mobile and Fixed SSs form the third most important functional aggregation in the end-to-end framework. We envision that most operator networks would, over time, have to support a mix of SSs with varying degrees of mobility support.

INTEROPERABILITY INTERFACES

Figure 4 identified several key interoperability interfaces within the end-to-end framework. The functionality and purpose of each of these interfaces is discussed below. All interfaces are bi-directional unless noted otherwise.

I-SSAP and I-MSSAP

This is the control, data, management and service plane interface between fixed-only or mobile SSs and 802.16 APs. The functions supported over this interface include, but are not limited to the following:

- SS/MSS connectivity provisioning and admission control
- Over-the-air and end-to-end security
- Mobility management
- Device management
- UL and DL data exchange
- Authorization and tunneling for specialized IP services
- Application layer end-to-end signaling
- Advanced functions such as power management (paging), compression, data reliability

As noted earlier, the 802.16 standard presents a rich selection of optional features that in turn presents significant interoperability challenges to the Industry. We expect the WiMAX Forum to define profiles targeting operation in specific frequency bands, channel widths, PHY modes, and duplexing modes to drive multivendor interoperability. All such applicable profiles will be incorporated in the I-SSAP and I-MSSAP interfaces.

I-CN1 and I-CN2

I-CN1 represents the control, data, and management planes between 802.16 RANs and an operator's core network (with interfaces in turn to other remote networks). I-CN2 represents control, management, and service planes to ASP networks. Both of these interfaces are exposed by the RNSN and enable a consistent all-IP interface to diverse core networks. The functions modeled over this interface may be provided by a cluster

of servers, for example, DHCP, DNS, IMS Core Network components such as Proxy-Call Session Control Function (P-CSCF), Interrogating-CSCF (I-CSCF), Serving-CSCF (S-CSCF), Media Gateway (MGW), and so on. These interfaces may also host IP tunnels to carry data between provider networks.

The functions supported over this interface include, but are not limited to the following:

- Assignment of traffic engineering parameters for provisioned QoS for both control and data plane traffic.
- User authentication via AAA intermediaries and servers.
- Services authorization, access control, and charging.
- IP connectivity management and security (for example, domain firewall).
- Troubleshooting network access problems, application-specific problems and RAN event handling.
- Data traffic and macro mobility management.

I-RNSN

This is the control, data, and management plane interface between two RNSNs that logically may demarcate two RAN clouds. The interface typically handles inter-RNSN mobility management control and data plane traffic (including temporary data tunneling between RNSNs serving Serving and Target APs during handovers).

I-RNSNAP

This is the control, data, and management plane interface between an AP (or any of its control plane variants) and an RNSN. This interface demarcates the two endpoints of the RAN across which intra-RAN micro- and macro-mobility functions are performed. The interface also supports functions such as paging.

Mobility Management

The 802.16-2004 standard defines a BS as a single sector entity supporting one frequency assignment. The 802.16e amendment defines MAC message primitives to support network or MSS initiated handovers. The very basic handover scenario for a real-world multisector AP would be an inter-sector handover. The amendment defines handover optimization flags representing levels of handover context information that is shared between neighbor AP entities (sector line cards in a multisector AP or between the sector line cards in two different APs). The optimization flags consequently enable modeling of all possible handover scenarios from the most basic nomadic access scenario (where no network entry context is shared between APs across a handover) to scenarios involving inter-subnet, inter-frequency assignment, Idle

mode, and inter-physical AP handovers. Furthermore, optional advanced features such as Soft handover (with PHY layer macro diversity) and Fast Base Station Switching are being defined to support zero packet loss, low latency inter-sector handovers. The design goal for mobility management is to build on these primitives to deliver the desired handover performance. Fixed access and nomadic access require no handover support. Portability implies fast intra-RAN switching with potential data loss during handovers and even more latency and data loss during inter-subnet handovers. Full mobility requires zero/low packet loss and low latency handovers that are acceptable to real-time applications such as VoIP.

The end-to-end reference architecture classifies mobility management into macro-mobility and micro-mobility as illustrated in Figure 6. Within the RAN, this paper recommends the use of Multiprotocol Label Switching (MPLS) [11] or IP-in-IP tunneling with Diffserv [10] provisioned QoS to switch data paths across traffic engineered backhaul links during handovers for micro-mobility. With MPLS, we recommend fast pre-provisioned Label Switched Paths (LSP) switching between the RNSN and AP/APC that perform the role of Label Edge Routers (LER). Efficient MAC layer handover triggers and limited micro-mobility signaling would be used to initiate traffic forwarding/multiple unicasting and switching to minimize handover latency and data loss between RNSN and AP/APC. For macro-mobility this paper recommends the use of SIP mobility for real-time low-latency interactive applications such as VoIP, and Mobile IP for all other generic applications. In the case of SIP mobility, an IMS can overlay on top of the end-to-end framework via the RNSN defined above.

The RAN can leverage the IP Differentiated Services QoS model or MPLS-based traffic engineering technologies to provide appropriate forwarding treatment to end-user traffic flows as they traverse between an RNSN and APs.

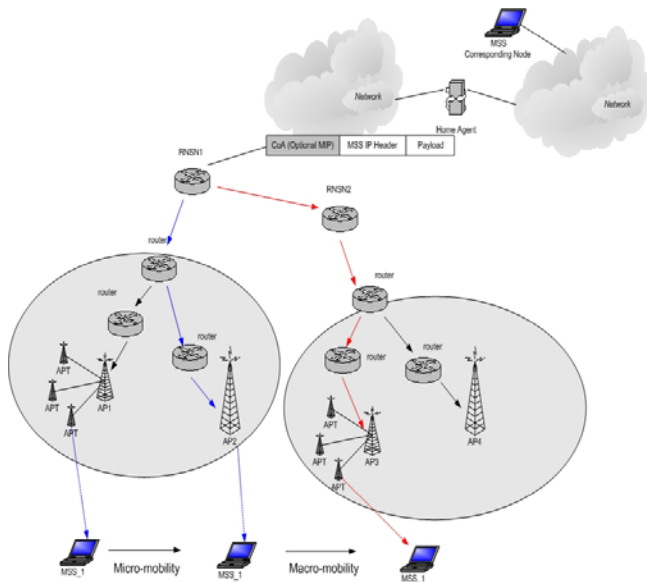


Figure 6: Mobility management

Harmonization and Interworking with Public Wi-Fi and 3G Networks

As noted earlier, different incumbent operators are likely to deploy 802.16 networks either as a data overlay network or as a standalone broadband access network. Integration with an existing operator network would involve either harmonization or interworking as defined below.

Interworking implies a technical and business relationship between operators owning homogenous or heterogeneous networks enabling subscribers to authenticate/authorize to their home operator network via the “visited” network and utilize system functions and IP services offered by both networks.

Harmonization on the other hand is a situation where two or more homogeneous or heterogeneous networks owned by an operator are offered as an integrated network to users.

The document http://www.intel.com/technology/IWS/WLAN_study.pdf describes Intel’s proposed interworking framework for public Wi-Fi hotspots. We recommend adopting and extending the same principles for inter-operator 802.16 interworking, supporting the following goals:

- An operator type-agnostic one-bill roaming (via common, extensible RADIUS [6] and DIAMETER [7] accounting primitives) framework across 802.16 networks—eventually leading to seamless IP services mobility across these networks.

- Support reuse of credentials and cryptographically strong bilateral authentication and session key management across these networks.
- A provisioning and access framework for advanced IP services that is compatible with the architecture for Wi-Fi hotspots.
- Enable offering of multiple IP services with attributes such as provisioned bandwidths, SLAs, QoS, and variable tariff profiles.

The all-IP architecture framework for Wi-Fi hotspots and 802.16 permit both loosely and tightly coupled harmonization scenarios. Figure 7 conceptually depicts these two forms of interworking.

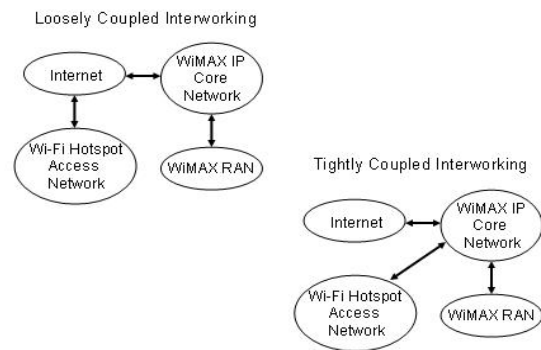


Figure 7: Loose and tight coupling of Wi-Fi and 802.16 networks

The loosely coupled framework is preferred in scenarios involving interworking between 802.16 networks and Wi-Fi hotspots managed by different operators. Other technical considerations are similar to what has been proposed for Wi-Fi roaming and inter-operator interworking in the reference cited above.

This paper recommends a loosely coupled integration approach for 802.16 and 2.5G/3G networks. Both 3GPP [4, 5] and 3GPP2 have ongoing efforts to develop an interworking architecture between Wi-Fi hotspots and 2.5G/3G networks. The loosely coupled interworking model is consistent with the developments in these two organizations. Figure 8 depicts the interworking model for 3GPP and 3GPP2 networks.

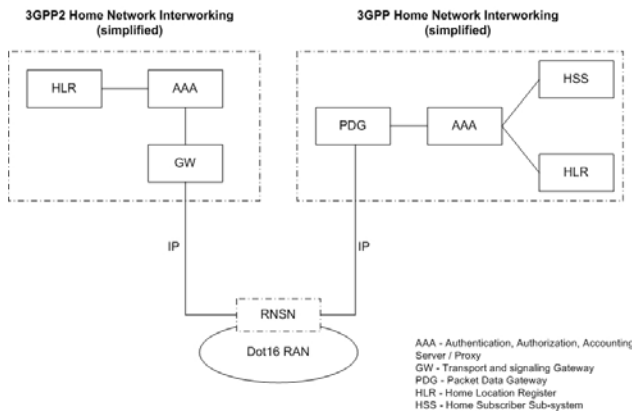


Figure 8: Reference model for 802.16 interworking with 2.5G/3G

3GPP has defined a Public Wi-Fi IP interworking entity called the Packet Data Gateway (PDG) to be incorporated in Release 6. With adaptations as needed based on functional requirements, the PDG can serve as the ingress to the operator IP core network (the 802.16 core network).

3GPP2 has a similar ongoing effort for Wi-Fi-3GPP2 interworking and will also identify a transport and signaling gateway that essentially supports integration of a 802.16 RAN into a 3GPP2 IP core network.

Note that while the RNSN is shown as a separate logical entity in Figure 8, most if not all of its functions on the IP core interconnect interface may be entirely subsumed by the PDG or PDSN while functions on the RAN interface may be subsumed by one or more APs.

End-to-End Security

Figure 9 conceptually depicts end-to-end Authentication, Authorization, and Accounting (AAA) on 802.16 networks supporting portability and fully mobile operations. The figure borrows terminology from Wi-Fi and is built on the three-party protocol (PKM v2) foundation being defined in 802.16e.

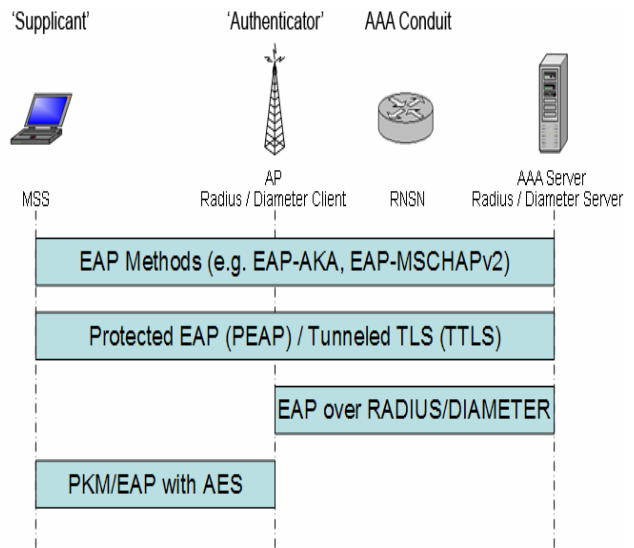


Figure 9: 802.16 security framework

As shown in this figure, over-the-air authentication and encryption (security association) is established using the PKM-EAP protocol. Extensible Authentication Protocol (EAP) is carried over RADIUS or DIAMETER to the AAA backend. The use of EAP enables support for cryptographically strong key-deriving methods such as EAP-AKA and EAP-MSCHAPv2. Intel also recommends using an end-to-end tunneling protocol such as Protected EAP (PEAP) or Tunneled TLS (TTLS) to afford mutual authentication and 128-bit or better Transport Layer Security (TLS) encryption to further enhance end-to-end security (especially in situations where cryptographically weaker EAP methods may be deployed). The AP or APC or APR serves as the “Authenticator” and hosts a RADIUS or DIAMETER AAA client. All AAA sessions are terminated on an AAA server that may be in the operator’s IP core network or an external IP network in roaming scenarios. The RNSN is merely a conduit for the AAA messages and does not play a significant role in the AAA process. In some instances, the network may employ an AAA aggregator/intermediary but the architecture is not impacted in those cases. Additionally, the RNSN may host a firewall to filter downstream traffic to a RAN.

THE WIMAX FORUM

In order for the defined IEEE 802.16 broadband wireless network architecture to become a reality, service providers must be assured that multivendor BS/SS interoperability is verified by an independent certification lab. The WiMAX Forum is a non-profit consortium of broadband wireless system vendors, service providers, component suppliers, and operators focused on enabling the development and deployment of interoperable

broadband wireless products around the world. Today, the consortium is focused on the development of conformance, interoperability, and certification of APs and SSs for Non Line of Sight (NLOS) operation below 11 GHz based on the IEEE 802.16 standard.

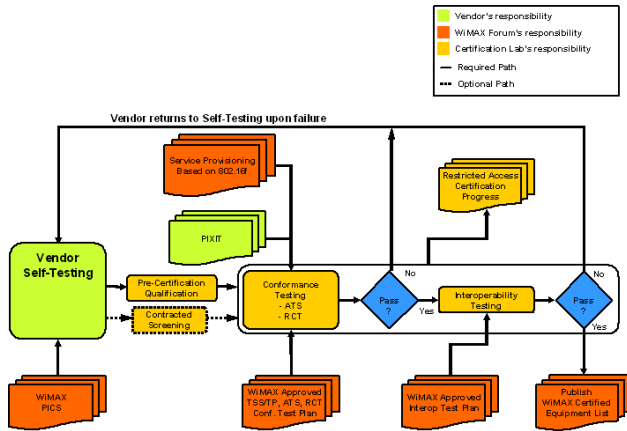


Figure 10: WiMAX certification process (preliminary)

The following section is divided into two main parts. First, the WiMAX conformance and interoperability processes are explained, and the WiMAX system profiles for certification are discussed. Second, the challenges facing the WiMAX certification process, including certification lab set-up and the development of the WiMAX protocol analyzer, are discussed.

WIMAX CERTIFICATION PROCESS

Conformance vs. Interoperability

WiMAX conformance should not be confused with interoperability. However, the combination of these two types of testing make up what is commonly referred to as certification testing. WiMAX conformance testing can be done by either the certification lab or another test lab and is a process where BS and SS manufacturers will be testing their pre-production or production units to ensure that they perform in accordance with the specifications called out in the WiMAX Protocol Implementation Conformance Specification (PICS) document. Based on the results of conformance testing, BS/SS vendors may choose to modify their hardware and/or firmware and formally re-submit these units for conformance testing. The conformance testing process may be subject to a vendor's personal interpretation of the IEEE standard, but the BS/SS units must pass all mandatory and prohibited test conditions called out by the test plan for a specific system profile.

On the other hand, WiMAX interoperability is a multivendor (≥ 3) test process hosted by the certification

lab to test the performance of BS and/or SS from one vendor to transmit and receive data bursts from another vendor BS and/or SS based on the WiMAX PICS. Figure 10 shows the preliminary WiMAX certification process with its components. First, the vendor submits BS/SS to the certification lab for Pre-Certification Qualification testing where a subset of the WiMAX conformance and interoperability test cases is done. These test results are used to determine if the vendor products are ready to start the formal WiMAX conformance testing process. Upon successful completion of the conformance testing, the certification lab can start full interoperability testing. However, if the vendor BS/SS failed some of the test cases, the vendor must first fix or make the necessary changes to his products (BS, SS) and provide the upgraded BS/SS with the self-test results to the certification lab before additional conformance and regulatory testing can be done. If the BS/SS vendor fails the interoperability testing, the vendor must make the necessary firmware/software modifications and then re-submit his products with the self-test results for a partial conformance testing depending on the type of failure and the required modification. The end goal is to show service providers and end users that as *WiMAX Forum Certified* hardware becomes available, service providers will have the option to mix and match different BSs and SSs from different vendors in their network in their deployments. Upon successful completion of the described process flow, the WiMAX Forum would then grant and publish a vendor's product as *WiMAX Forum Certified*. It should be pointed out that each BS/SS must also pass regulatory testing, which is an independent parallel process to the WiMAX certification process.

Abstract Test Suite Process

The WiMAX Forum is working on the development of numerous process and procedural test documents under the umbrella of the IEEE 802.16 standard. The key WiMAX test documents are as follows:

- Protocol Implementation Conformance Specification (PICS) in a table format.
- Test Purposes and Test Suite Structure (TP and TSS).
- Radio Conformance Test Specification (RCT).
- Protocol Implementation eXtra Information for Testing (IXIT) in a table format.

Figure 11 shows how these test documents are used in the development of a standardized Abstract Test Suite (ATS). The ATS is the culmination of test scripts written in a Tree and Tabular Combined Notation (TTCN) language. The end product of the ATS are test scripts for

conformance and interoperability testing under a number of test conditions called out in the PICS document for a specified WiMAX system profile. The development of the first set of available test scripts is planned for the fourth quarter of 2004. With available test scripts, the manual WiMAX certification testing will eventually become an automated process.

WiMAX System Profiles

As previously mentioned WiMAX defines interoperable system profiles between the BS and SS, which are targeted for licensed and licensed-exempt frequency bands used around the world. Table 1 lists only the first stage of the basic system profiles that will be used for WiMAX certification. This list is limited initially to 3.5 GHz licensed (international) and 5.8 GHz license-exempt frequency bands. Data bursts can be transmitted using either FDD or TDD schemes. In the TDD scheme, both the UL and DL share the same channel, but do not transmit simultaneously, and in the FDD scheme, the UL and DL operate on different channels, sometimes simultaneously. The second stage of profiles is pending regulatory and service providers contributions. WiMAX system profiles with 5 MHz channel bandwidth at 2.5 GHz frequency band (i.e., MMDS) using either TDD or FDD schemes are planned to be added in the second stage.

Table 1: First-stage system profiles for WiMAX certification

1st Stage Profile Configuration	Profile Name
3.5GHz, TDD, 7MHz	3.5T1
3.5GHz, TDD 3.5MHz	3.5T2
3.5GHz, FDD, 3.5MHz	3.5F1
3.5GHz, FDD, 7MHz	3.5F2
5.8GHz, TDD, 10MHz	5.8T

What is Certified?

As described above, certification is a combination of conformance and interoperability testing scripts based on selected profiles with test conditions specified from the PICS document. The selection of test cases for certification is currently in development by the WiMAX Forum. Development of the certification program is one of the many activities under the auspices of the WiMAX Certification Working Group (CWG). Certification testing is intended only for complete systems such as a BS or an SS, not individual solution components such as radio chips or software stacks. The introduction of BS/SS reference designs may also be considered for testing to show that the design conforms to the IEEE 802.16 specification and is interoperable with other *WiMAX Forum Certified* equipment, but will not preclude any requirement for a system vendor using components from the reference design from having to submit their product for certification testing. For portable and mobile platforms, various vendors are expected to client-based cards introduce later on that plug into a notebook or another portable platform. Such products will necessitate submission of the client-based cards with a notebook for testing similar to what has been done by a Wi-Fi certification lab. While much work still needs to be done, as the IEEE 802.16e standard becomes more stable, the working groups within the WiMAX Forum will continue to lay the framework for test integration and certification in migrating from supporting IEEE 802.16d towards the introduction of IEEE 802.16e-based products.

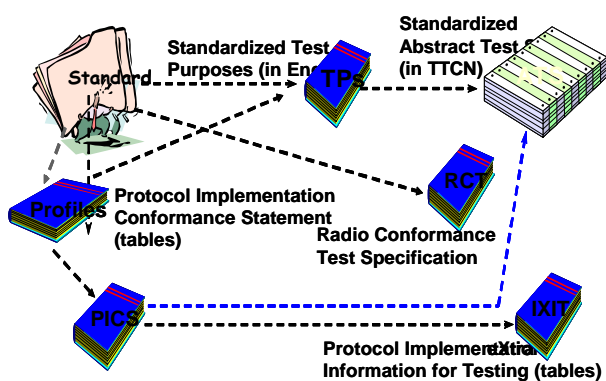


Figure 11: Abstract test suite development process

Certification Challenges

There are two main challenges facing the WiMAX certification process. The first challenge is to establish a

margins that are comparable to wide area wireless systems, IEEE 802.16 is uniquely positioned to extend broadband wireless beyond the small islands of service afforded by Wi-Fi systems today. Incremental evolution, from Fixed access to Portability and then to Full Mobility, with laptops and PDAs enabled with IEEE 802.16, furthers Intel's vision of coupling wireless connectivity and computing in a single processor platform. The set of ongoing activities outlined in this article, a PHY and MAC layer specification that unites the market behind a common set of standards, a flexible end-to-end network architecture that is coupled with a coherent service vision, and an efficient certification process that enables interoperability, are key enablers for realizing the WiMAX vision.

ACKNOWLEDGMENTS

The authors thank Gerald Lebizay, Glenn Begis, Tim Teckman, and David Putzolu for their review of this paper.

REFERENCES

- [1] "Part 16: Air Interface for Fixed Broadband Wireless Access Systems," *IEEETM P802.16-REVd/D5-2004*.
- [2] "Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems," *IEEETM P802.16e/D3-2004*.
- [3] "WiMAX PICS for WirelessMAN-OFDM and WirelessHUMAN(-OFDM) Rev.7f (2004)."
- [4] "3GPP TS 22.234-Requirements on 3GPP System to WLAN Interworking (Release 6)."
- [5] "3GPP TS 23.234-3GPP system to WLAN Interworking; System Description (Release 6)."
- [6] RFC 2865, "Remote Authentication Dial In User Service," Related RFCs at <http://www.freeradius.org/rfc/>*
- [7] RFC 3588, "DIAMETER base protocol."
- [8] RFC 3344, "IP Mobility support for IPv4."
- [9] RFC 3775, "Mobility support in IPv6."
- [10] RFC 2475, "An architecture for differentiated services."
- [11] RFC 3031, "Multiprotocol label switching architecture."
- [12] DNS RFCs can be found at <http://www.dns.net/dnsrd/rfc/>*
- [13] RFC 793, "Transmission Control Protocol."

AUTHORS' BIOGRAPHIES

Ed Agis is a market development manager for the Wireless Broadband Division (WBD) at Intel Corporation. He is also the co-chair of the WiMAX Forum Certification Working Group and a member of the WiMAX Technical and Marketing Working Groups. Ed holds a B.Sc. degree from the Air Force Academy graduating Magna cum Laude as well as a Masters of Business Administration in Management and another in Operations/Product Marketing from Amber University. His e-mail is ed.agis at intel.com.

Henry Mitchel is a systems architect in Intel's Modular Communications Platform Division within the Communications Infrastructure Group specializing in chip architectures, firmware, protocols, and standards, and their impacts on systems architecture. Prior to joining Intel he was director of R&D at DataStorm Technologies, Inc., makers of PROCOMM PLUS*. He holds a BS degree from the Massachusetts Institute of Technology and an MS degree from the University of Missouri. His e-mail is henry.mitchel at intel.com.

Shlomo Ovadia received a Ph.D. degree in Optical Sciences from the Optical Sciences Center, University of Arizona in 1984. He held various technical positions at IBM, Bellcore, and General Instruments before joining Intel in 2000 as principal architect in CTG, where he was leading the effort on the architecture, design, and development of optical burst switching in enterprise networks. Currently at ICG, Shlomo is leading Intel's WiMAX interoperability and certification effort for IEEE 802.16d/e-based wireless products. He is the author of a recently published book titled *Broadband Cable TV Access Networks: From Technologies to Applications* (Prentice Hall, 2001). He is a senior member of IEEE/LEOS/COMSOC with more than 70 technical publications and conference presentations. He is the holder of 35 patents, and his personal biography is included in the Millennium edition of *Who's Who in Science and Engineering* (2000/2001). His e-mail is shlomo.ovadia at intel.com.

Selim Aissi is lead MID and security architect in the Virtualization and Trust Lab at Intel's Corporate Technology Group. He also leads standards efforts in 3GPP. Before joining Intel in 1999, he worked at the University of Michigan, General Dynamics' M1A2 Battlefield Tank Division, General Motors' Embedded Controller Excellence Center, and Applied Dynamics International. Selim serves on the review board of several

* Other brands and names are the property of their respective owners.

publications and conferences, including ACM CCS, ACM SWS, and he is the vice-chair of the Security and Management (SAM) Conference. He holds a Ph.D. degree in Aerospace Engineering from the University of Michigan and is a senior member of the IEEE and ACM. His e-mail is selim.aissi at intel.com.

Sanjay Bakshi is an 802.16e network architect in Intel's Mobile Networking Lab within the Corporate Technology Group. Prior to joining the Mobile Networking Lab, Sanjay was engineering manager and architect in the Performance Networking Lab within the Corporate Technology Group. He has led a number of projects related to the usage of the Intel Internet Exchange Processor in various fields such as IP routing, MPLS, 3G wireless, and next-generation control plane architecture. Sanjay received his B.E. degree in Computer Science from the Regional Engineering College, Tiruchirapalli, India. His e-mail is sanjay.bakshi at intel.com.

Prakash Iyer is a senior staff architect in Intel's Mobile Networking Lab within the Corporate Technology Group. He is an active member of the IEEE 802.16 Working Group including chair for the Handoff Adhoc group. He leads standards efforts in the IEEE, IETF, 3GPP, and 3GPP2 on heterogeneous wireless interworking and directs architecture, prototyping, and simulation efforts for seamless networking—including 802.11 and 802.16. He holds B.S. degrees in Physics and Electrical and Computer Engineering and an M.S. degree in Computer Science. His e-mail is prakash.iyer at intel.com.

Masud Kibria is 802.16e initiative manager within Intel's Communications Technology Lab focused on the technical validation of 802.16e. Prior to joining Intel, Masud led various strategic projects at AT&T Wireless including WCDMA evolution to HSDPA, Interoperability for 2.5G/3G Networks, WLAN, Wireless-PBX, emerging technology feasibility studies, etc. Previously, he has worked on various theoretical and practical aspects of coverage, capacity, and interference for mobile wireless systems and has led regional teams in WWAN design, implementation, and operation. Masud received his BSEE degree from the University of Maryland. His e-mail is masud.kibria at intel.com.

Christopher B. Rogers is a WWAN technology strategist within Intel's Communications Technology Labs. Prior to his current focus on 802.16 technology, he was marketing director and co-founder of Intel's Ultrawideband Wireless Group and has also held business development and marketing roles in other WPAN- and WWAN-related businesses within Intel. Chris is a member of IEEE 802.15 and 802.16 and chairs an

industry specifications subgroup for mobile broadband wireless architecture. He received his Bachelors degree in engineering from Georgia Institute of Technology and holds an MBA degree from Carnegie Mellon University. His e-mail is chris.b.rogers at intel.com.

James Tsai is a wireless network and mobile platform architect in Intel's Mobile Networking Lab within the Corporate Technology Group. His research work has focused on wireless network architectures (Wi-Fi, WiMAX, and WWAN) and next-generation mobile platform technologies such as extended mobile access technology and multi-radio subsystems. He received his B.S degree in Electrical Engineering from the Chinese Culture University in Taiwan and an M.S. degree in Computer Science from Columbia University. His e-mail is james.tsai at intel.com.

Copyright © Intel Corporation 2004. This publication was downloaded from <http://developer.intel.com/>.

Legal notices at <http://www.intel.com/sites/corporate/tradmarx.htm>.

THIS PAGE INTENTIONALLY LEFT BLANK

For further information visit:

developer.intel.com/technology/itj/index.htm