CHAPTER

1

Introduction to MVPN

Contracting margins and revenues per user, cost-based competition, and focus on customer retention rather than acquisitions are all signs that mobile telephony is not likely to show significant revenue growth—comparable to that enjoyed over the past decade—over the next several years. Service providers are therefore forced to look for innovative ways to invest in new technologies, which can potentially become the next growth enablers. For instance, in recent years much attention has been paid to "mobile Internet" services, which are believed to pose a significant revenue-generation potential for service providers.

This belief was in part responsible for the massive investment in spectrum for next-generation radio access technologies, with the potential to support higher data rates for mobile Internet services, commonly known as *third generation* (3G). More recently, service providers have recognized that Internet access per se may not justify the significant investments they made. As a result, the search is back on for innovative ways to generate revenues by using the new service capabilities offered by the deployment of packet-data-based systems such as General Packet Radio Service (GPRS), Universal Mobile Telecommunication System (UMTS), or CDMA2000 (CDMA stands for Code Division Multiple Access). So far, it is

apparent that the most promising kind of services mix traditional mobile voice capabilities and new location-based and messaging services. Such systems must provide users personalized and predictable access to private networks where they can belong to communities of interest for both business and leisure, such as corporate networks or instant messaging groups.

The value of such networks to the customers appears to be strictly related to:

- Ensuring secure network access with predictable performance
- Making sure that access to such networks is exclusive to members with appropriate permissions.

These service requirements are compelling service providers to use Mobile Virtual Private Networking (MVPN), which we define as the emulation of private secure mobile data networks over generally insecure shared mobile and wireless facilities. This definition is based on a number of assumptions:

- Data user mobility is defined as uninterrupted connectivity or the ability to stay connected and communicate to a possibly remote data network while changing the network access medium or points of attachment.
- Despite MVPN service is usually provided over wireless media, and in fact, this book is written about VPN implementation over various wireless access systems. We make clear distinction between "mobile" and "wireless," since these terms have different meanings and we believe that for our purposes "mobile" is more accurate and inclusive (see Chapter 5 for more discussion on wireless versus mobile).
- The term "wireless facilities" refers to current and future generations of cellular systems of interest such as Global System for Mobile Communications (GSM), CDMA2000, Time Division Multiple Access (TDMA), and UMTS, wireless networks such as Wireless LANs (WLANs), and overlay wireless packet data systems such as GPRS.

A simple visualization of MVPN can be found in Figure 1.1, which shows secure tunnels connecting a mobile device with a variety of private networks over multiple shared public networks, such as the Internet and an arbitrary cellular wireless system or WLAN network.

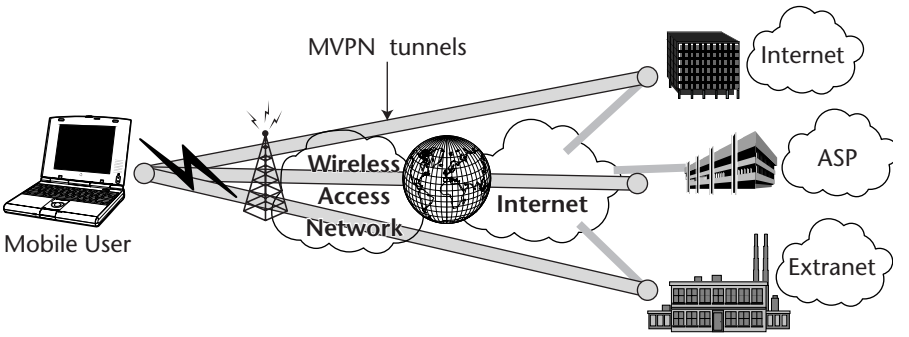

Figure 1.1 Example of Mobile Virtual Private Networking.

In this chapter we concentrate on business and standardization issues as an introduction to topics addressed in the rest of the book. The first half of this chapter discusses the MVPN business case and marketplace, explaining what benefits this technology can bring to service providers and their customers. We start with the discussion of pervasive mobility and its consequences, moving on to MVPN history and business case. The section ends with an overview of MVPN market segments and stakeholders. The second half of the chapter examines the current wireless data standardization status and trends and provides the reader with a reference to the standard documents usage and retrieval from various standard body repositories. The reader will become familiar with standards organizations such as 3GPP, 3GPP2, and the Internet Engineering Task Force (IETF), along with their standardization processes. An understanding of what a given standard body does within the landscape of mobile networking will be helpful to the reader for the remainder of the book.

The Era of Pervasive Mobility

We are fortunate to be witnessing the beginning of an era of *pervasive mobility*, when access to information resources will not be determined by the availability or type of network access technology but rather by factors such as the desire, necessity, and eligibility to obtain information or services. Information and services will be requested and accessed not only by individuals but also by virtual and physical entities such as automated

manufacturing processes, "smart" vending machines, information-collecting devices such as utility meters, intelligent cash registers, highway toll stations, security systems, and medical equipment. (See Chapter 9 for some anticipated next-generation services scenarios.) Remote network access service characteristics will not be dependent on geographical location, but rather on the existence of proper roaming and service agreements between home and visited data networks, allowing for home service profile retrieval into foreign networks. When proper agreements are in place, mobile entities or individuals will be able to receive services identical to those available in their "home" networking environments while roaming foreign networks.

Pervasive Mobility Drivers

So what drives the need for pervasive mobility, or permanently available uninterrupted on-demand connectivity? The most important drivers are productivity gains via advancing IT technology, the rise of the Internet, the ever-increasing speed of evolution of mobile devices, cellular and noncellular network coverage, and plummeting costs of cellular wireless service.

Increase in Productivity

The changing role of information technology in corporations and institutions throughout the world was responsible for major productivity gains in the workplace during the last decade of the twentieth century. That was, of course, accompanied by the rise of the Internet, which brought together masses of information and united disparate communities of interest all over the world. However, massive computerization also brought total dependence on computing and information resources often available only at a limited number of select locations, such as corporate headquarters or data centers. The newly available services, so indispensable to users in their offices, are more and more often requested from remote locations such as satellite or home offices, customer sites, and from the road. These needs in turn drive demand for global network roaming and ubiquitous remote network access. The uncertainty of the location where the user will require access imposes the need for mobile (dynamic) private connectivity to the home network to be available throughout a wide area (also referred to as ubiquitous access).

Mobile Device Evolution

It is hard to underestimate the role of personal communication and computing devices—such as Personal Digital Assistants (PDAs), smart mobile phones, and laptop computers leaving the factory with multiple built-in wireless interfaces—in the evolution of mobile communications. Plummeting prices, increasing user-friendliness, and feature richness are now making these devices not only increasingly available and desirable for ever-increasing groups of mobile professionals, but often indispensable.

The latest example of such devices is a slew of PDAs and PDA-based mobile phones that are approaching earlier-generation desktop computers in memory and processing power. Manufacturers like HP, Toshiba, Sony, Nokia, and Palm are leading this trend. These small, low-powered wonders can support multiple modes of wireless communications (Infrared, Bluetooth, WLAN, and GPRS or CDMA2000), VPN clients, and a micro-browser bundled with the operating system. This combination of features makes them ideal for secure access to remote corporate networks.

Cellular Systems Advances

The third driver for pervasive mobility is the rapid build-out and consolidation of cellular systems resulting in more and more uniform wide-area wireless coverage and increasingly inexpensive services. Cellular coverage has become so widespread and inexpensive that it is driving other technologies out of business. This resulted in a situation where *alternative* wide-area wireless access systems, such as satellite, had been deemed unnecessary by a paying public whose low demand forced them into bankruptcy or niche markets. Good examples of those are now defunct satellite operator Iridium and Inmarsat, which is forced to specialize on maritime navigation. In fact, cellular service in some areas, ranging from highly saturated European and Japanese markets to developing nations completely lacking landline infrastructure, became so ubiquitous and affordable that it began to replace landline phone service.

Mobile Lifestyles and Workplaces

These and other technological advances account for the rise of pervasive mobility, which in turn continues to bring profound ongoing changes to our society, lifestyle, and workplace in how we communicate, how we

receive information and news, and how we process the information. The 90's and the first years of the new millennium were essential in the formation of mobile technology. The way our society now uses cellular wireless networking and, specifically, wireless data technologies such as short messaging service (SMS) is the best indicator of these changes. From teenagers using SMS for "secret" communications to professionals in Japan using i-mode devices for banking services, wireless data users are fast approaching voice users in numbers and generated revenues. In fact, it is expected that wireless data will become the leading driving force of telecommunications in the coming decade.

Stopping short of producing yet another set of arguments in favor of this technology to add to the numerous articles and books already written, let's now turn our attention to the main subject of this book. In our view the next "hot" mobile technology will involve wireless data as a foundation for specialized services like location-based service, private environments, mobile-commerce (m-commerce), and MVPN. We discuss these services further in Chapter 9. For now, we start our discussion of MVPN by taking a brief tour of VPN history, then outlining Mobile VPN business case.

Background on VPN

Virtual Private Networks were originally defined and first applied in voice communications. For years, phone companies delivered voice services using what they called "Virtual Private Networks," despite the fact that there wasn't—and still isn't—much that is "virtual" about them. In fact, even today just about any software-defined user group provisioned over any physical medium is considered VPN by the phone companies. The term is still in use even though Public Switched Telephone Network (PSTN) facilities are owned by the phone companies, thus making the technology essentially a private network used for offering user group services.

With the rise of data communication, the term VPN was adopted by data networking industry and was given a new, more accurate meaning. So-called traditional data VPNs were initially created with dedicated link layer networking technologies such as Frame Relay PVC (Permanent Virtual Circuit) or ATM VC (ATM stands for Asynchronous Transfer Mode) links, established between individual hosts or networks. In roughly 10 years following the advent of these technologies, data VPNs typically have been implemented in this fashion with the main goal of replacing less efficient private networks based on dedicated end-to-end leased facilities.

NOTE **Interestingly, later on both ATM and Frame Relay were gradually reclassified as private networking technologies, mainly on the grounds that while these networks were shared, they nevertheless were privately owned. This also made sense for marketing purposes; ATM and FR services could be equated to those available through the use of truly private, dedicated technologies, such as leased lines, thereby promoting these new data transport methods.**

As the use of the public Internet Protocol (IP) networks such as the Internet quickly gained public interest and market acceptance, a new generation of VPN services based on network layer technologies has been introduced to the market. Like traditional VPNs, IP VPNs utilize shared facilities to emulate private networks and deliver reliable, secure services to end users. During the initial IP VPN technology trials, equipment manufacturers and standards organizations such as the IETF came up with a number of encapsulation and encryption techniques (more on those in Chapter 2) in an effort to deliver on the promised cost advantages and complexity reduction [Yuan2001], without compromising security requirements many potential VPN customers have. The proprietary mechanisms like Layer Two Forwarding (L2F) devised by Cisco and Point-to-Point Tunneling Protocol (PPTP) introduced by Microsoft include such early examples. Ultimately, the industry settled on the use of standard based technologies such as IPSec, L2TP, Generic Routing Encapsulation (GRE), and Multi-Protocol Label Switching (MPLS), among others (details are also in Chapter 2). Common authentication and accounting methods largely based on the RADIUS protocol previously defined to satisfy the demand for centralized subscriber management in the remote dial-up industry were also selected and standardized for use with IP VPN. Mobile wireless VPNs are the latest members of this group.

MVPN Business Case

Mobile VPN is a data service that can be provided within any system or network supporting authenticated (most often wireless) access to a data network. Let's look at MVPN business case as a combination of VPN and wireless data business cases and analyze its value for operators, in the form of revenue and marketing potentials, and customers, as a vehicle for delivery of new services and functionality. Based on our findings, we will look at MVPN market from both service provider and customer perspectives and evaluate the MVPN benefits and values proposition for specific customer and provider segments.

Moving to Mobile VPN

The Internet, now accessible from almost anyplace where telephone lines, cellular service, or satellite services are available, has fundamentally changed the way we communicate and access information and services. The Internet is rapidly becoming the medium of choice for business communications. However, it is a public shared network, whereas business communications requires private secure facilities. That means if the Internet is to be used for private communications, the user information transported over it must be somehow secured.

Suites of networking and security technologies were devised in response to this requirement and quickly became popular methods for conducting private communications over the Internet or any other shared IP networking medium. These were known as IP VPN technologies. In the course of wireless networks' development, the requirement of mobility became more and more stringent in the provisioning of IP VPN services. This fostered research, standards efforts, and the development of MVPN technologies in the industry. Today, operators are preparing business plans and architectures to support a variety of MVPN offerings to serve the needs of their business and institutional customers.

Wireless Communications with MVPN

For wireless operators deploying latest-generation cellular systems based on packet-switched data such as GPRS and CDMA2000, and especially those targeting *business* customers for significant portion of their revenue stream, the importance of services based on MVPN technologies is hard to underestimate. For operators, MVPN is not only one of the required technologies for business customers' private network access but also a foundation for other services requiring interaction with private networks such as m-commerce, virtual presence and gaming applications, and multimedia applications (which includes Voice over IP-based services).

The benefits of deploying Mobile VPNs for businesses and institutions include:

- Uninterrupted, media and location-independent connectivity to private networks
- Seamless private network access mobility
- Connectivity to a particular Internet service provider (ISP) or application service provider (ASP)

- Mobile remote access outsourcing possibilities
- Secure m-commerce enabler
- Constant remote-workers reachability
- Higher cost-effectiveness

As a result, businesses, which already had a positive experience with wireline VPN services, are now looking to wireless operators for extending these services into wireless environments. In our view, during the next few years as the latest generations of cellular systems and other wireless technologies take off, an enormous market opportunity awaits wireless carriers who can meet demands for services requiring private network access.

MVPN as a Differentiation Tool

Mobile VPN is a powerful differentiation tool especially for service providers dedicating a significant portion of their offerings to serving business customers. But why is differentiation so important? During the last few decades, we witnessed the cellular communications gradually rise from luxury item and status symbol to necessary tool and then abruptly become a commodity. Commoditization is undesirable for any industry. But it is also a natural part of almost any product life cycle and is no stranger to the wireless telecommunications. As Internet-based Web services boomed in recent years, ubiquitous and fast Internet access became an immediate goal of the wireless data industry as well. However, wireless data services consisting mainly of Internet access are considered as generic as today's cellular voice services, and face price-based competition that is already hurting wireless voice revenues. Subscribers will not have enough incentive to stay with a particular carrier for reasons other than pricing. The situation is further complicated by the ease of switching from one carrier to another, known by operators as *customer churn*, which has plagued the wireless industry since its inception.

MVPN seems to be one of the likely answers to these problems. Since MVPN technology is highly customizable and can be implemented in different flavors to accommodate different customers needs, the MVPN service offerings can also be packaged and marketed differently by different wireless operators. That means they would be able to offer more "sticky" or unique services, and therefore prevent price-driven customer churn. This is especially true for large institutions and enterprises expected to make unique MVPN services from different wireless operators an integral part of their IT infrastructures.

Mobile VPN Market and Stakeholders

Having touched on the MVPN overall value proposition and its significance in the wireless market, let's now turn to MVPN market segments. The MVPN market, like any other market, consists of buyers (private network access customers) and sellers (wireless carriers and other service providers) who engage in transactions concerning a particular product or product category (private network access in mobile environment in our case) [Kotler1999]. Let's now look at each group, taking into account the benefits of MVPN and different deployment strategies more suitable to different customers and providers.

MVPN Service Providers

MVPN service providers can be loosely classified into three major groups:

- Wireless operators
- Mobile Virtual Private Operators (MVNOs) and other subcontractors and resellers
- Wireline Internet service providers (surprise!)

The wireless operators group includes carriers, offering both actual network-based MVPN services as well as the business-quality Internet access with properties suitable for stable end-to-end VPN to be created between the customer's mobile equipment and the customer's VPN gateways. (See Chapter 5 for details on the difference between end-to-end and network-based VPN types.) Wireless carriers are by far the largest MVPN service provider group. This is not surprising, since the wireless carriers own both the spectrum licenses and the radio infrastructure. For network-based MVPN offerings, wireless carriers would have to establish proper agreements with the enterprises and institutions defining trust relationships, legal liabilities, quality of services, availability, and other parameters. If the enterprise chooses an end-to-end VPN method, the role of wireless carriers would be to support an end-to-end MVPN-compatible IP addressing scheme based on the use of publicly routable IP addresses or appropriately designed private address translation mechanisms. Of course, in the case of end-to-end VPN, wireless carriers might be bypassed altogether and might not even be aware of private communication taking place over their infrastructure, since by the nature of end-to-end VPN, packets transmitted between tunnel endpoints are encrypted and bear only end-to-end significance. This makes network-based service more attractive to wireless carriers; they can introduce a multitude of offerings with high

revenue-generating potentials and institute more control over the mobile subscribers.

The second category of potential MVPN providers includes Mobile Virtual Network Operators (MVNOs) and other wireless service subcontractors, such as those engaged in infrastructure-sharing agreements (the radio access network and the spectrum license normally belong to their business partners). This group should be especially interested in network-based VPN services for the same reasons as regular wireless carriers. In addition, when the end-to-end VPN option is selected by the MVNO's corporate customers, MVNO's role would be much restricted and revenues would be likely marginal, since the middle-man role the MVNO targets would be quite limited. So MVNOs are even more likely to strive to add as much value as possible by implementing intelligent services in the network. (More discussion on MVNOs is provided in Chapter 9.)

The last service provider group, which might be considered unlikely by some, includes traditional wireline Internet service providers. This group can participate in providing network-based MVPN service through agreements with wireless operators, which often allow the latter to use highly developed IP infrastructures of the former. The benefits of offering MVPN service for this group mostly lies not in new revenue-generating capabilities but in product line extension—that is, in augmenting their traditional wireline offerings with newly available MVPN options. This allows wireline ISPs to become one-stop service providers for their traditional customers regardless of the network access method (wireless or wireline). We also need to stress that *wireline* service providers in some countries are starting to drive the deployment of a WLAN-based hot-spot coverage infrastructure, thus seeking as much independence as possible from *cellular* wireless operators and at the same time trying to compete with them in wireless high-speed data services.

MVPN Customers

The benefits of deploying Mobile VPNs are as significant for customers as they are for service providers. MVPNs provide remote workers with constant, media-independent connectivity to corporate networks or to the ISPs and ASPs of their choice. MVPNs enable corporations to outsource mobile remote access, and in some cases can completely replace *wireline* remote access infrastructures—thereby eliminating the costs of purchasing and supporting the remote access equipment while allowing private networks to maintain full control over user address assignments, authentication, and security (see Chapter 5).

Let's take a closer look at the potential MVPN users and their requirements. Generally, they can be classified into the following main categories:

- Small businesses
- Large enterprises
- Institutions, both government and academic
- Applications service providers (ASPs)

The following sections look at each user category in more depth.

Small Businesses

The main motivation for small businesses to use MVPN is primarily convenience and its cost-cutting abilities. MVPN is generally used by small businesses for remote access to centralize information resources, email access, and the monitoring of certain events, such as medical monitoring and utility billing. MVPN service for small business is more likely to be achieved via end-to-end connectivity, which does not require the establishment of complex agreements with wireless carriers. Instead, the responsible personnel must make sure that employees and partners are provided with the business class wireless Internet access with proper qualities to support end-to-end MVPN service.

Another reason why end-to-end VPN is more likely to be utilized within this segment is its relative ease of implementation and low price. To support this service, the remote workers must be provided with mobile devices equipped with off-the-shelf or proprietary VPN clients and security software and equipment such as IPSec protocol stacks and RSA SecureID cards. Often clients are bundled with operating systems—for example, IPSec clients are bundled with Microsoft Windows 2000 used with laptop computers (more in Chapter 8).

Enterprises

The main reason larger enterprises would be interested in MVPN is the potential productivity gains and increased personnel reachability. Cost cutting and ease of deployment will remain secondary issues. In an enterprise, MVPN services are most likely outsourced via an agreement or a number of agreements with wireless carriers, which are responsible for providing remote employees and partners of an enterprise with specific types and classes of MVPN services. In this situation, all types of MVPN can be used with equally good results as long as they satisfy cost, security, convenience, ease of support, and other requirements of an enterprise.

Generally, large enterprises are not as cost-sensitive as small businesses or government institutions. They often desire state-of-the-art services for their remote mobile workers—such as high-speed mobile data access and special security arrangements—which require a variety of MVPN technologies; network-based ones often being the most suitable. Usually, enterprise IT departments require to be involved in many aspects of the services provided by carriers, which, for instance, would allow them to retain control over policy provisioning, authentication, or IP address assignment. In these situations, open management interfaces, as well as carefully structured provisioning arrangements, are critical.

Institutions

Government and other public institutions might be interested in MVPN services for reasons different from those motivating the private sector. For example, telecommuting is encouraged by the US government primarily not for cost-cutting reasons but to reduce pollution by eliminating daily travel to work. Home offices are becoming more and more popular with many public institutions. This trend, however, requires large-scale remote access mechanisms such as landline IP VPN combined with MVPN for workers on the road.

Service requirements of a government institution often can be rather unpredictable and unexpected (anyone in the private sector who has dealt with government customers can attest to this), often for a good reason or at least with good intentions. For that reason, flexibility in MVPN offerings and technologies should be the key when dealing with public institutions of various sizes and functions. For example, security requirements can often be very strong and far exceed those customary for private sector.

On the other hand, government institutions are often required to be especially cost-conscious and must structure their spending according to yearly plans.[1] This prompts the use of very detailed service level agreements between government institutions and wireless carriers defining all the up-front prices and the services these prices would buy. Offering compulsory VPN service also relieves an institution from the responsibility of participating in VPN setup, provisioning, and maintenance—all of which can be outsourced to wireless carriers and their partners.

Academic and medical institutions are usually bound by similar goals of careful use of often substantial resources and the desire to use the latest technology available to achieve certain unique objectives such as support for telecommunications research projects or remote patient diagnostics. MVPN requirements for this group often have the attributes of both large

[1] 5-year plans were used in some countries in the past without much success.

enterprises and public institutions. For this reason, the approach that should be taken by wireless carriers should be one of diversity. Often the service presenting the right features might consist of a combination of offerings and unique arrangements, such as a combination of end-to-end and network-based VPN services, use of granular per-flow policies, and unique arrangements for traffic differentiation and service bundling.

Application Service Providers

This class of MVPN customers will grow as the wireless carriers take advantage of application packages offered by their wireline partners or content providers. These players must rely on dedicated private virtual networks so that the control of access to the services they offer can be easily enforced, and business class and predictable network access makes the user experience in accessing the services they offer uniform. ASP VPN offerings also come with advanced accounting features, so that the wireless provider and the partners can mutually exchange correlated traffic and content usage data and apply to these discounting policies and offer services like trend analysis and customer-behavior monitoring. These MVPNs allow members to access ASP services and offer subscription-based access to a host of services in a service bundle without forcing customers to perform individual authentication procedures.

Wireless Data Standards

It is no doubt that interoperability and multivendor-based solutions is one of the key market requirements in telecommunications industry today. In particular, compliance to standards has always been one of the main requirements to MVPN solutions, since they potentially span multiple networks (access, transit ISP, customer) and are inherently bound to interoperability between wireless access devices and the access network infrastructure to allow for global roaming. It is therefore necessary to have a good understanding of the standard bodies we will be referencing in the book.

The need to produce standards for the advent of the next generation of wireless systems prompted the foundation of a number of Standard Definition Organizations (SDOs) during the last few years. Third-generation wireless systems requirements were originally defined by the ITU (International Telecommunications Union, a United Nations-associated organization) within the IMT-2000 framework (International Mobile Telecommunications). Aside from defining some technological and spectrum requirements for the

radio transmission technologies that could be considered candidate for 3G services, the IMT-2000 framework defined service requirements such as the support of global roaming.

This forced all the parties (manufacturers and operators) involved in standards setting to evolve the standardization bodies at a global level. The result was the creation of the Third-Generation Partnership Project (3GPP) organization and later the foundation of a mirror organization (not without a touch of irony in the name) called 3GPP2. Before we define the scope and organization of these SDOs, we should step back and look at the landscape of cellular-industry-related standards organizations before the advent of the 3GPP and 3GPP2.

Regional Standards Organizations

Aside from international organizations such as the ITU, which had almost no influence on the definition of cellular wireless systems, each region in the world had its own standard-setting bodies devoted to this technology. The GSM system in the 900- and 1800-MHz spectrum was defined by European Telecommunications Standards Institute (ETSI) and later was also adopted by the Telecommunications Industry Association (TIA) T1-P1 committee in North America for the 1900-MHz spectrum (dedicated to PCS, or Personal Communications Services). TIA has also defined a host of other cellular systems in the North American region, both analog and digital. Japan, in contrast to the rest of the world, defined its own digital cellular system called Personal Digital Communications (PDC). The Japanese standard bodies are the Association of Radio Industries and Businesses (ARIB) and the Telecommunication Technology Committee (TTC). These standards bodies also influence the decision making in the rest of the Pacific Rim—with the exception of Korea and China, which have their own organizations (the Korean Telecommunications Technology Association and China Wireless Telecommunication Standards Group, respectively).

Each of these organizations were defining regional standards incompatible with standards defined by other organizations, with the exception of the GSM 1900-MHz system, that would allow GSM 900 and 1800 customers to roam to North America using a tri-band phone. It was clear that this model could not work anymore, as the need to standardize 3G systems guaranteeing global roaming arose. In an ideal world, a single new organization defining a single system for the whole world would have been a logical solution. Of course, we don't live in a perfect world. Instead, the spectrum allocation for the 3G services in Europe and Japan was in the 1900- to 2100-MHz region, which was already partially used by the PCS

services in the North American region. This situation, together with a different migration paths to 3G and different core network technologies used in the existing European GSM and the North American CDMA systems, led to even more profound mutual incompatibilities, not entirely by chance, right from the birth of two distinct SDOs for third-generation systems: 3GPP and 3GPP2.

3GPP

3GPP is an agreement between regional telecommunications standards bodies known as O*rganizational Partners*. Currently, the 3GPP Organizational Partners are ARIB, China Wireless Telecommunication Standard Group (CWTS), ETSI, T1, Telecommunications Technology Association (TTA), and Telecommunication Technology Committee (TTC). 3GPP was created in December 1998 when the partners signed the Third-Generation Partnership Project Agreement. A company can be a member of 3GPP providing that it meets the rules defined for 3GPP membership.

A second category of partnership was created within the project: *market representation partners*. These are organizations and industry focus groups driven by objectives based on long-term needs of their member companies. At a certain stage, these partners decide it is important to have 3GPP hear their opinion as a group, rather than disseminate this opinion via the individual member companies. One of these groups, the 3G.IP industry focus group, has been particularly influential in driving the standardization of the evolution of the 3GPP system's specifications toward an IP-based, multimedia-capable system.

The intended purpose of 3GPP was to define technical specifications and technical reports for a 3G Mobile System based on an evolution of the GSM core network. This included the radio access technologies that were selected for 3G services based on the GSM core network: W-CDMA-based Universal Terrestrial Radio Access (UTRA) in its Frequency Division Duplex (FDD) and Time Division Duplex (TDD) modes. Later it became evident that it would make sense to extend the scope of 3GPP to include the maintenance and evolution of the Global System for Mobile communication (GSM) technical specifications and technical reports, and the related radio access technologies and services, General Packet Radio Service (GPRS) and Enhanced Data rates for GSM Evolution (EDGE). Now 3GPP has taken over the roles for which ETSI had been responsible.

The work of 3GPP is organized into Technical Standardization Groups (TSGs), which in turn are organized into Working Groups (WGs). The rules of operation of a TSG are specified in the technical report 3G TS 21.900 "Technical Specification Group Working Methods."

Following is the list of current TSGs groups comprising 3GPP:

- TSG-SA (System and Architecture) defines the systems aspects and coordinates the technical work of all other groups from a systems perspective. It includes five WGs:
  - SA1 handles requirements.
  - SA2 Systems handles architecture.
  - SA3 handles security.
  - SA4 Voice handles multimedia coding.
  - SA5 handles charging.
- TSG-CN (Core Network) specifies the evolution of the core network. There are five Working Groups in TSG CN:
  - CN1 addresses the protocols between the user equipment (UE, also known as terminal, mobile phone, or mobile station) and the core network [specifically the node in the core network that dialogues with terminals in order to manage UE mobility and allow the mobile station (MS) to set up and receive calls].
  - CN2 specifies the interaction of the mobile network with intelligent network functionality and services.
  - CN3 defines the interworking of the mobile network with external networks, such as the PSTN, or packet data networks, such as the Internet.
  - CN4 specifies core network protocols.
  - CN5 specifies application programming interfaces and protocols used to access network services from third-party application providers.
- TSG-RAN (Radio Access Network) defines the UMTS Terrestrial Radio Access Network (UTRAN). It is composed of four WGs:
  - RAN-1 is devoted to radio physical layer protocol specification.
  - RAN-2 handles the specification of the radio link layer.
  - RAN-3 defines the Iu interface (that is, the interface between the radio access network and the core network).
  - RAN 4 addresses pure radio aspects.
- TSG-GERAN (GSM Evolution RAN) defines specifications for the evolution of the GSM Radio Access Network. It is composed of five Working Groups:

  - GERAN1 is devoted to radio aspects.
  - GERAN2 addresses protocol aspects.
  - GERAN3 is devoted to GSM Base Station Subsystem testing OA&M.
  - GERAN4 specifies radio aspects of terminal testing.
  - GERAN5 WG5 addresses protocol aspects of terminal testing.
- TSG-(T) (Terminals) specifies terminal aspects. It includes three WGs:
  - T1 addresses test specifications for interoperability
  - T2 specifies terminal capabilities
  - T3 specifies the UMTS Subscriber Identity Module (SIM), which is a chipcard that enables subscriber identity authentication, terminal portability, and execution of simple applications.
- A Project Coordination Group (PCG) has the role of determining rules of operation of the body and defining its working procedures.

3GPP specifications are delivered in *releases*. Initially, ETSI released specifications every year and assigned names accordingly. The first release of UMTS specifications (which was also a GSM specifications release, because of the role of GSM maintenance and evolution that 3GPP took over) was named Release 99. Later, as soon as the following release 2000 development plan had to be articulated, the decision was made to lift the constraint binding 3GPP specifications releases to a year and instead use functionality-based releases. 3GPP releases are now named with a release number different from the year the release was issued, starting from year 2000. The first release issued under this new naming convention was named Release 4, the second Release 5, and so on. The counter started from 4 because the specification version number was 3.*x*.*y* (where *x* and *y* are generic-figure placeholders) for Release 99, and the decision was made to increment the first number in the version number of a specification at every release.

Release 99 defines the basic UMTS features associated with the circuit-switched and packet-switched services UMTS provides. Release 4 enhances the circuit services part of the system to use the latest developments in media gateways and media gateway controllers' technologies, and Release 5 introduces the support of multimedia services over the packet-switched part of the system.

Release 6 will introduce, among other features, multicast and broadcast capabilities that make the delivery of multicast content economically

viable. Note that by pure coincidence the issue of a release happens every year, so the completion of the R5 specification is 2002, and Release 6 specification is expected to be completed in 2003.

3GPP Documents and Standardization Process

3GPP produces specifications that result in two sets in permanent documents: technical reports (TRs) and technical specifications (TSs). A TR is a permanent document that records a Working Group activity, such as the investigation on the feasibility of introduction of some feature in the specifications. A TS is the actual document specifying the behavior of network nodes and the definition of protocols used in 3GPP-compliant systems.

The three kinds of technical specifications are as follows:

- Stage 1 specifications outline service and functional requirements and are based on the input from the operators. SA1 is the WG within TSG-SA that normally generates all Stage 1 documents for 3GPP.
- Stage 2 specifications address system-level and architectural-level requirements that the protocols specified by 3GPP should meet. These are the documents where all the strategic directions and political decisions are formalized. Normally, SA2 within TSG takes the role of generating the most high-level Stage 2 documents, while when more specific competence is required on the protocol level, other WGs define Stage 2 documents.
- Stage 3 documents are the actual 3GPP protocols specifications.

Generating a TS is a formal process. In the first phase, interested companies, led by a document rapporteur or group of rapporteurs, contribute heavily to generate a first draft of the document. The document is generated by a WG by consensus. When the draft document is ready, a WG submits it to the TSG plenary for approval. After the approval, the document is promoted to a higher level of stability. The WG submits the document again to the TSG plenary, suggesting that it is stable enough to enter the change control phase. In this stage of a document's lifetime, companies can change the document only by submitting a formal change request (CR). A specification belongs at any given time to a release. When a release is "frozen," changes to the document can be approved only by general consensus or because there are serious system operation problems if the document does not change. A document can evolve over a number of releases, until 3GPP decides to withdraw a specification starting from a 3GPP release.

Documents (better known as temporary documents, as opposed to TSs and TRs, which are permanent documents) submitted by interested companies are discussed at WG meetings. A set of output documents is the result of consensus of the WG meetings. This set of documents is forwarded to the TSG plenary, where normally they are approved (or companies that feel their voice was not adequately heard at the WG level can ask for changes or the rejection of one or more of them). When documents are approved by a TSG plenary, the content is normally transferred to a permanent document. Thus, after every TSG plenary the version number of the documents under the control of a TSG changes.

3GPP2

3GPP2 is a collaboration agreement among standard definition organizations interested in developing specifications for the 3G systems evolving from an ANSI-41-based core network, set up in February 1999 for the same reasons that led to the creation of 3GPP to define specifications for 3G systems evolving from the map-based GSM core network. The Organizational Partners that are currently members of 3GPP2 are ARIB, CWTS, TIA, TTA, TTC, and Market Representation Partners (MRP).

Much like 3GPP, 3GPP2 felt the need to allow the market to bring organized input to their standardization activities. 3GPP2 Market Representation Partners (MRP) are organizations that can offer market advice to 3GPP2 and bring into 3GPP2 a consensus view of market requirements (e.g., services, features, and functionality) falling within the 3GPP2 scope.

Following is a list of current MRPs:

- CDMA Development Group (CDG)
- Mobile Wireless Internet Forum (MWIF)
- IPv6 Forum

In particular, MWIF has been proposing strongly the evolution of the 3GPP2 systems specification to an IP-based multimedia-capable system (much like 3G.IP in the 3GPP arena).

The operation of 3GPP2 is guided by the Steering Committee.

The actual work in 3GPP2 is performed by TSGs. The TSGs responsible for generating the technical specification documents of 3GPP2 are as follows:

- TSG-A (Access Network Interface) is responsible for the specifications of interfaces between the radio access network and core network, as well as within the access network for capabilities like intervendor handoff.

- TSG-C (CDMA2000) is responsible for the radio access part, including its internal structure, of systems based on 3GPP2 specifications. Specifically, it is responsible for requirements, functions, and interfaces for the CDMA2000 infrastructure and user terminal equipment. This includes radio layer 1, 2, and 3 specifications, mobile and base station performance and test specifications, support for enhanced privacy, authentication and encryption, and digital speech and video codecs. It also addresses the mobile station-to-adapter interfaces and other ancillary interfaces.
- TSG-N (ANSI-41, Wireless Intelligent Network) is responsible for the specifications of the core network part of systems based on 3GPP2 specifications. These include core network internal interfaces for call-associated and noncall-associated signaling, evolution of the core network for intersystem operation within the ANSI-41 family member, Virtual Home Environment (VHE) procedures, user identity module (UIM) support (detachable and integrated), and support for enhanced privacy, authentication, encryption, and other security aspects.
- TSG-P (Wireless Packet Data Networking) is responsible for the specifications of packet data networking for 3GPP2 systems. These include Wireless IP services (including IP Mobility Management), Wireless IP network architecture design, Voice over IP, public Internet and secure private network access, packet data accounting, multimedia, and quality of service (QoS) methods. This group is strongly influenced by MRPs like MWIF. An ad hoc *TSG All IP* has been created to satisfy the MWIF requirements for an All IP-based system.
- TSG-R (Interface of 3GPP Radio Access Technology to 3G Core Network evolved from ANSI-41) is responsible for the Inter-Working Function specification of Interface of 3GPP Radio Access Technology (i.e., UTRAN) to 3G Core Network to an evolved ANSI-41 core network. It also addresses handoff between cdmaOne and UTRA radio technologies and roaming between ANSI-41 and GSM core networks. TSG-S (Systems and Services Aspects) is responsible for the development of service capability requirements for systems based on 3GPP2 specifications. It is also responsible for architectural issues as required to coordinate service development across the various TSGs.

3GPP2 Documents and Standardization Process

3GPP2 produces technical specifications and reports similarly to 3GPP. TSG-S defines feature and system requirements. These, much in the same

way as in 3GPP, are referred to as Stage 1 requirements. Technical specifications and reports are developed in the TSGs. The specifications are developed in two stages:

- Stage 2 is a high-level overview of the implementation of a feature or service in the 3GPP2 architecture, including message flow diagrams.
- Stage 3 is the text and the associated information for the final technical specification.

Once a specification or report is technically stable and complete, the TSG approves the document as *baseline text*. The document undergoes a verification and validation (V&V) process. Once this V&V process has been passed, the document can be approved for publication by the TSG.

After a TSG approves a document, it forwards the document to the 3GPP2 Secretariat. The 3GPP2 Secretariat opens a 15-day comment period. If no comments are received, the document is published as an official 3GPP2 publication. The Organizational Partners (TIA, TTC) can subsequently handle the document according to regional standards approval processes. Once this review is complete, any comments are sent to the originating 3GPP2 TSG. The document then undergoes an update process. The updated document is then base-lined, subjected to V&V, and approved by the TSG as necessary. The process described previously is then repeated.

Internet Engineering Task Force

Since most data applications in wireless networks are IP-based, it comes as no surprise that the IETF and the protocols it specifies are becoming increasingly relevant to the wireless data industry. The IETF is organized in areas that organize technically related Working Groups. The current IETF areas are as follows:

- *Applications Area* deals with applications and application protocols like presence and instant messaging, network time protocol, calendaring, and scheduling.
- *General Area* addresses topics related to the general operation of the IETF, such as rules setting.
- *Routing Area* specifies routing protocols and their applicability.
- *Internet Area* defines IP protocol-related matters, such as the definition of its evolution, the support of network services such as PPP, and IP host configuration. Recently, it took on the role of specifying the Mobile IP protocol from the Routing Area, since Mobile IP is now perceived as a mobile remote IP network access technology, rather than a routing protocol.

- *Operations and Management Area* defines network management aspects and protocols, such as the well-known Simple Network Management Protocol (SNMP) and its evolution.
- *Security Area* addresses Internet security aspects.
- *Sub-IP Area* is devoted to the definition of technologies and protocols that normally are located at a layer below IP in the protocol stack and are devoted to the provision of services such as VPNs, traffic engineering, and transport of link layers or even circuit emulation.
- *Transport Area* is responsible for the definition of transport-related matters, such as QoS, transport-level protocols (for instance, recently transport protocols for carrying signaling was defined), and congestion control.

Each of these areas is led by one or two *area directors*. Area directors and the IETF chair are members of the Internet Engineering Steering Group (IESG), which has the role of standards quality evaluation and can strongly influence the transition of an Internet Draft to proposed standards RFC status, by returning it to the WG until it attains an adequate level of quality to be published. The following section explains this role in greater detail.

IETF Documents and Standardization Process

The IETF standardization process is quite different from that of the 3GPP. First, no company can officially be an IETF member. IETF membership is only allowed for engineers and scientists or students interested in the evolution of the Internet. These individuals, however, are more often than not sponsored by companies and organization, whose interests are therefore indirectly represented.

Second, there is no actual formal document evaluation process. When an individual deems something is needed to add functionality to the Internet, he or she (possibly with multiple other coauthors) submits an Internet Draft to the relevant IETF Working Group. If no appropriate WG exists, interested individuals may set up one with IESG approval, going through a *bird-of-feather* (BoF) first round of discussion to gauge consensus on the need of the WG and its scope. Normally this takes place at an IETF meeting (there are three IETF meetings for each calendar year). It should be noted that once a WG is set up, individuals can summit Internet Drafts and discuss them on a WG mailing list. All the decisions are taken on the mailing list, based on evidence of "rough consensus" and some proof of having "running code" that testifies that the protocol being developed really works.

Once the WG is sufficiently happy with an Internet Draft evolved through amendments from the mailing list, the WG submits the draft to the IESG for their review. When the IESG has no further comments, the document is published as a Request for Comments (RFC) document. An RFC can be just an informational document, which documents something some group of individuals do or a protocol they use, or a standard track document, for instance, a protocol that is going to be generally used in the Internet.

In addition, there are different levels of standards track document. Initially, a standards track RFC is a *proposed standard*. Then, after some years of operational experience and with the evidence of at least two independent interoperable implementations, an RFC can become a *draft standard*. A draft standard RFC normally is a very stable document. After many years of operation, the IETF may elect to promote a draft standard RFC to the status of *Internet standard*. Other times, when the protocol becomes obsolete and no more widely used, the RFC can become "historical." Sometimes, if a WG or IESG needs to publish some rules or practices used in the Internet or in the IETF, they publish a *Best Current Practice* (BCP) RFC.

NOTE **An individual may ask the IESG to evaluate directly a document he or she has produced, to document something that is relevant to the Internet operation. For instance, you might ask them to look at a proprietary protocol that happened to become widespread in the Internet, because it is supported by a dominant vendor of a popular internetworking device. The IESG may decide to approve recording the document as an informational RFC. Sometimes vendors misuse this option to advertise their own proprietary solutions as IETF standards.**

IEEE 802 LAN/MAN Standards Committee

The Institute of Electrical and Electronics Engineers (IEEE) defines standards for local area networking in the IEEE P802 LAN/MAN standards committee, part of the IEEE Standards Association (IEEE-SA). In recent years, the IEEE 802.11 WG has defined a standard for Wireless LAN, known as the 802.11 standard. This is a very promising set of standards, and it is creating a serious competitor (or a complementing technology, depending on the way the industry looks at it) to 3G technologies in serving network access in hot-spot areas such as airports, hotels, and train stations (more on this in Chapter 9). The IEEE 802.11 WG is organized into Task Groups (TGs). Each Task Group takes care of the standardization of a particular aspect of the WLAN technology, and they are the authors of the

standards documents. Following is a list of 802.11 TGs, directly derived from the IEEE standards Web site:

MAC Task Group. [The scope of this project] is to develop one common MAC for Wireless Local Area Networks (WLANs) applications, in conjunction with the PHY Task Group work. Work has been completed on the ISO/IEC version of the original Standard, published as 8802-11: 1999 (ISO/IEC) (IEEE Std. 802.11, 1999 Edition).

PHY Task Group. The scope of the project is to develop three PHYs for Wireless Local Area Networks (WLANs) applications, using Infrared (IR), 2.4-GHz Frequency Hopping Spread Spectrum (FHSS), and 2.4-GHz Direct Sequence Spread Spectrum (DSSS), in conjunction with the one common MAC Task Group work. Work has been completed and is now part of the original Standard. Work has been completed on the ISO/IEC version of the original Standard, published as 8802-11: 1999 (ISO/IEC) (IEEE Std. 802.11, 1999 Edition).

Task Group a. The scope of the project is to develop a PHY to operate in the newly allocated UNII band. Work has been completed on the ISO/IEC version of the original Standard as an amendment, published as 8802-11: 1999 (E)/Amd 1: 2000 (ISO/IEC) (IEEE Std. 802.11a-1999 Edition).

Task Group b. The scope of the project is to develop a standard for a higher rate PHY in the 2.4-GHz band. Work has been completed and is now part of the Standard as an amendment, published as IEEE Std. 802.11b-1999.

Task Group b-cor1. The scope of this project is to correct deficiencies in the MIB definition of 802.11b. As the MIB is currently defined in 802.11b, it is not possible to compile an interoperable MIB. This project will correct the deficiencies in the MIB. It is an ongoing Task Group.

Task Group c. [This project] adds a subclause under 2.5 Support of the Internal Sub-Layer Service by specific MAC Procedures to cover bridge operation with IEEE 802.11 MACs. This supplement to ISO/IEC 10038 (IEEE 802.1D) will be developed by the 802.11 Working Group in cooperation with the IEEE 802.1 Working Group. Work has been completed and is now part of the ISO/IEC 10038 (IEEE 802.1D) Standard.

Task Group d. This supplement will define the physical layer requirements (channelization, hopping patterns, new values for current MIB attributes, and other requirements) to extend the operation of 802.11 WLANs to new regulatory domains (countries). It is an ongoing task.

Task Group e. This Task Group is expected to enhance the 802.11 Medium Access Control (MAC) to improve and manage Quality of Service, provide classes of service, and enhanced security and authentication mechanisms. [It will] consider efficiency enhancements in the areas of the Distributed Coordination Function (DCF) and Point Coordination Function (PCF). These enhancements, in combination with recent improvements in PHY capabilities from 802.11a and 802.11b, will increase overall system performance, and expand the application space for 802.11. Example applications include transport of voice, audio and video over 802.11 wireless networks, video conferencing, media stream distribution, enhanced security applications, and mobile and nomadic access applications. The security part of the TGe PAR (Project Authorization Request) was moved to the ongoing TGi PAR as of May 2001 [PARs are discussed in greater detail in the next section].

Task Group f. [This Task Group] develops recommended practices for an Inter-Access Point Protocol (IAPP), which provides the necessary capabilities to achieve multivendor Access Point interoperability across a Distribution System supporting IEEE P802.11 Wireless LAN Links. It is an ongoing TG.

Task Group g. The scope of this project is to develop a higher speed(s) PHY extension to the 802.11b standard. The new standard shall be compatible with the IEEE 802.11 MAC. The maximum PHY data rate targeted by this project shall be at least 20 Mbit/s. The new extension shall implement all mandatory portions of the IEEE 802.11b PHY standard. The current 802.11b standard already defines the basic rates of 1, 2, 5.5, and 11 Mbit/s. The proposed project targets further developing the provisions for enhanced data rate capability of 802.11b networks. It is an ongoing TG.

Task Group h. [The scope of this project is to enhance] the 802.11 Medium Access Control (MAC) standard and 802.11a High Speed Physical Layer (PHY) in the 5-GHz Band supplement to the standard; to add indoor and outdoor channel selection for 5-GHz license exempt bands in Europe; and to enhance channel energy measurement and reporting mechanisms to improve spectrum and transmit power management (per CEPT and subsequent EU committee or body ruling incorporating CEPT Recommendation ERC 99/23). It is an ongoing project.

Task Group i. [The scope of the project is to enhance the 802.11 Medium Access Control (MAC), thereby enhancing] security and authentication mechanisms. It is an ongoing project.

It is now possible to buy a WLAN PCMCIA card or an *access point* based on compliance with one or more of the documents authored by the task groups. Wireless Ethernet Compatibility Alliance (WECA) is an industry forum charged with the mission of certifying interoperability of IEEE 802.11 products. The WECA determines the criteria for compliance, based on references to the appropriate documents generated by IEEE 802.11 TGs.

IEEE Documents and Standardization Process

The creation of a new IEEE standard happens via a Standards Project. This must be sponsored by a member of the IEEE SA Standardization Board. An IEEE Standards Project may be:

New. A document that does not replace or substantially modify another standard

Revision. A document that updates or replaces an existing IEEE standard

Amendment. An addendum or a substantive change to an exiting IEEE standard

Corrigenda. A document that contains only substantive corrections to an existing IEEE standard

Each project must be authorized by the board after a Project Authorization Request (PAR)—which defines the scope of the project—has been submitted. Once the project is approved, it has to generate a draft document, which will later undergo a ballot, before being approved as an IEEE standard by the Review Committee, or *Revcom*. The Revcom makes recommendations to the IEEE-SA Standards Board on the approval or disapproval of documents submitted to IEEE-SA Standards Board.

IEEE standards can be classified in four ways:

Standards. These documents specify mandatory requirements.

Recommended practices. These documents clarify procedures and positions preferred by IEEE.

Guides. These define a set of alternative approaches, but no strict recommendations are made.

Trial-use documents. Valid for up to 2 years, these documents may belong to any of the preceding categories.

Every 5 years an IEEE standard has to undergo a *reaffirmation* process to confirm its validity. The IEEE process is summarized in Figure 1.2.

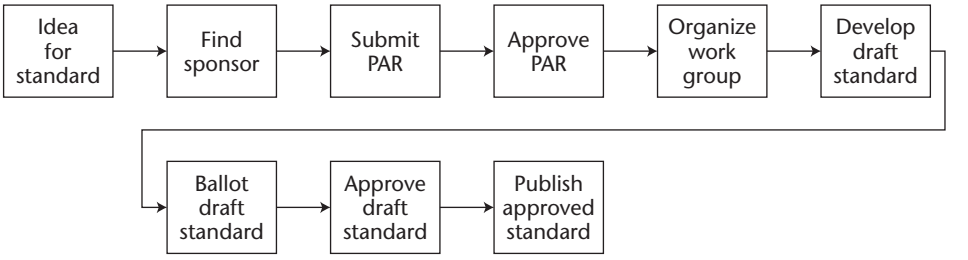

Figure 1.2 The IEEE standards process.

Finding Standards Documents Online

Throughout the book we frequently reference standards documents, and you are invited to probe further when you find a topic in which you are particularly interested. Fortunately, most of the documents are available via the Internet. Table 1.1 includes links to the Web sites where the standards documents we refer to can be downloaded.

Table 1.1 Resources on the Web

STANDARDS BODY	URL
3GPP	http://www.3gpp.org
3GPP2	http://www.3gpp2.org
IETF	http://www.ietf.org
IEEE 802.11 WG	http://grouper.ieee.org/groups/802/11/

Summary

In this chapter we introduced and defined what MVPN is, providing a market perspective that includes the customer drivers and key players, along with their needs for using MVPN technologies. We then stressed the importance of standards in MVPN solutions and provided a brief outline of the key standards bodies, specifying protocols and systems involved in MVPN technologies. In Chapters 2, 3, and 4, we provide a complete overview of the wireless systems and networking technologies required to understand MVPN technology. Readers who are already comfortable with data networking VPN technologies and wireless systems may want to skip ahead to Chapter 5.