Bridging Wireless Protocols

John W. Noerenberg II, Qualcomm, Inc.

ABSTRACT

The lingua franca of the Internet is TCP/IP, and wireless devices are learning to speak this language. But what is the "wireless Internet?" There are a number of different answers to this question. The question poses problems for equipment manufacturers, service providers, and users alike. We desire seamless access to the Internet, and in order to have that, all these different modes must operate transparently for users. This article discusses how TIA/EIA standard IS-856 cellular data (1xEV) can be married with IEEE 802.11b wireless data to enable wide-area Internet access for service providers and users. The article outlines the system used at the December 2000 IETF meeting and discusses its implications.

INTRODUCTION: WHY BRIDGE WIRELESS PROTOCOLS?

Both 802.11 and Telecommunications Industry Association/Electronics Industry Alliance (TIA/EIA) IS-856 are wireless networking protocols. However, each meets different goals. Devices for short-range 802.11 wireless networks are rapidly proliferating. Wireless network providers (carriers) are eager to deploy high-speed wireless data protocols such as IS-856 that complement their wireless voice networks. The IS-856 standard is integrated into the protocols for code-division multiple access (CDMA) networks. Finding an effective means to connect 802.11 devices to increasingly available high-data-rate cellular networks answers the need of users for 802.11 devices to take advantage of the eventual ubiquity of high-speed cellular networks.

The 802.11 and IS-856 protocols have similar architectures. Wireless stations are untethered. Both use similar modulation techniques for moving bits of data through the wireless medium. Both provide medium access control (MAC) to manage the physical and data link layers of the open systems interconnect (OSI) protocol model. Access points mediate access to other networks. Each has protocols for handing off between access points a station's logical connections as stations move into different coverage regions. Both are well adapted to support higher layers of the TCP/IP protocol stack.

However, significant differences exist as well. The differences arise from the different design goals these protocols serve. The 802.11 standard is designed to build short-range wireless local area networks (WLANs), where the maximum distance between stations is on the order of 100 m. While IS-856 supports LANs, the range of over which stations communicate is tens of kilometers. The IS-856 standard is designed to be an integral part of a cellular communication network that operates in licensed frequency bands assigned specifically for cellular communication. Networks of 802.11 devices use unlicensed frequency bands and must work in spite of the possibility of other nearby devices using the same radio spectrum for purposes other than data communication.

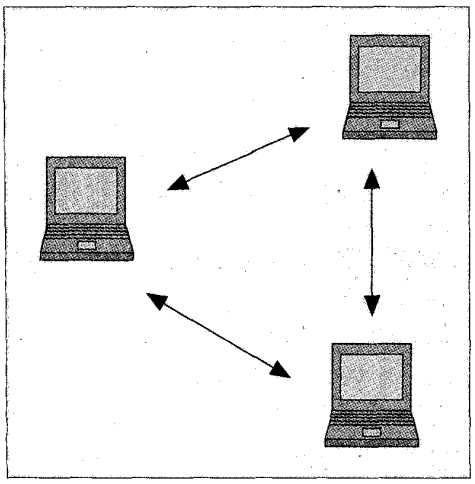
These differences, principally the difference in range, fostered the idea that these two wireless systems could be combined to complement each other. Another factor behind this idea is the proliferation of 802.11-capable devices and the desire of their users to connect to the Internet via their Internet service provider (ISP). We have demonstrated how 802.11 networks and IS-856 networks can be bridged to facilitate user demand for this connectivity as they range through an IS-856 network with their 802.11 device.

Connecting the two protocols is quite straightforward. It can be done simply because these protocol designs complement each other in key ways. This article provides overviews of how IS-856 and 802.11b manage the wireless medium. Following the overview, the technique used to bridge the protocols is described. The article concludes with some suggestions on how an ISP can take advantage of these techniques to offer wide-area access to its subscribers who are using 802.11 devices.

OVERVIEW OF 802.11 ARCHITECTURE

The introduction to this article listed a number of similarities and differences between IS-856 networks and 802.11 networks. The differences are primarily due to the way in which each wireless protocol is used. Networks of 802.11 devices are short-range wireless networks. Today, typical

0163-6804/01/$10.00 © 2001 IEEE



■ **Figure 1.** *Independent basic service set.*

applications for 802.11 protocols provide wireless access to TCP/IP networks for laptop computers. The 802.11 protocols aren't limited to this kind of application. Any group of devices designed to share access to a common short-range communication medium can be built on 802.11's services. In the future, devices designed for particular tasks that incorporate communication with other nearby devices will be able to take advantage of 802.11's services in ad hoc networks. Some of these devices may simultaneously be part of the more structured environment of the Internet. This will have important implications when a single user or group of nearby users has a variety of devices that could interact for the benefit of their owners.

Devices able to take advantage of a wireless network will use TCP/IP protocols as their means to exchange information with other devices. Because 802.11 defines MAC protocols, which correspond to the data link and physical layers of the OSI model, 802.11 is well suited to provide the basic connection on which the rest of the TCP/IP protocol stack depends.

This aspect of 802.11 enables it to fit neatly with IS-856 networks. For example, an IS-856 network could easily provide the backbone needed to connect a number of separate 802.11 networks into a single network domain. This idea is explored later when the particular architecture used for the IETF network is described.

IEEE MAC Protocol for Wireless LANs

One of the fundamental design goals for 802.11 is to provide services that are consistent with the services of 802.3 networks. This makes the peculiarities of wireless communication irrelevant to higher layers of the protocol stack. The 802.11 MAC protocols take care of the housekeeping associated with devices moving within the 802.11 WLAN. From the point of view of the IP layer, communication via wireless with 802.11 is no different than communication over an 802.3 data link, fiber, asynchronous transfer mode (ATM), or any other data link service. Because these different media are capable of different data rates, users can perceive differences in performance. But any well-designed application will operate successfully over all these media. This greatly reduces complexity for application designers. Reduced complexity results in more reliable and more robust applications, more rapid development by designers, and broader utility for users.

Designed for Multiple Scenarios

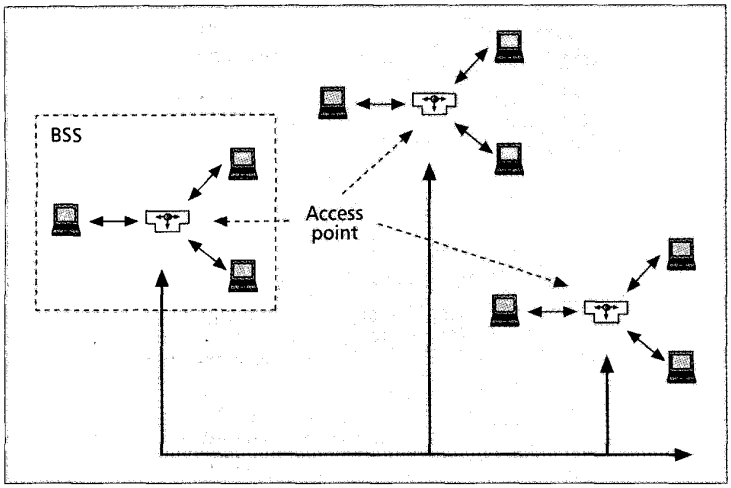
The fundamental organizational unit of an 802.11 network is called a basic service set (BSS). The members of a BSS are the wireless stations that share a specific 802.11 WLAN. How a BSS connects to other networks defines the variants.

A BSS not connecting to another network is termed an independent BSS or iBSS (Fig. 1). An iBSS uses MAC protocols to establish how its members share the medium. There can be no hidden nodes in an iBSS. Each member must be able to communicate directly with all other members without relays. An iBSS is ideal for a collection of personal devices that move with the owner. For example, a PDA, laptop, cell phone, CD or DVD player, or video and/or audio recorder could be members of an individual's personal network of communication devices. An 802.11 network connecting them would provide an individual user with a rich array of ways to communicate with others. Another example might be a coffee maker, alarm clock, lawn sprinkler controller, home security cameras, home entertainment systems, and a personal computer. A network made up of these devices could turn on the coffee maker when the alarm goes off in the morning. It would allow a homeowner to water the grass from his/her easy chair, and make sure he or she is not watering the sidewalk, or turn the sprinklers on the burglar while calling the police and playing recordings of large dogs barking.

When a BSS connects with another network via an access point, it is termed an *infrastructure BSS*. Because this is the most common configuration today, the acronym BSS usually implies an infrastructure BSS. The access point is both a member of the BSS and mediates access to other networks on behalf the rest of the BSS. Generally, the members of the BSS beside the access point are personal computers. To facilitate coverage of a campus within the same 802.11 network, a group of BSSs, called an *extended service set* (ESS), define how access points hand off connections for members of the network as stations move between access points. The access points are connected by backbone links that provide the medium for the handoff protocol (Fig. 2).

The 802.11 standard supports simultaneous existence of iBSS and BSS networks. It provides means for labeling networks and conditioning access so they can operate without interfering with each other. It is entirely reasonable that the computers mentioned in the iBSS examples above could participate simultaneously in a private 802.11 network and an infrastructure 802.11 network providing Internet access. While this

One of the fundamental design goals for 802.11 is to provide services that are consistent with the services of 802.3 networks. This makes the peculiarities of wireless communication irrelevant to higher layers of the protocol stack.



■ **Figure 2.** *Extended service set.*

idea has fascinating possibilities, further discussion is beyond the scope of this article.

MAC Layer Protocols

The 802.11 standard consists of several MAC layer protocols to provide the variety of services necessary for the kinds of wireless networks just described. A Beacon protocol enables a BSS or iBSS to organize its communication. The Beacon information contains the network label information so 802.11 devices can discover the networks that exist within range of their antennae. The Beacon establishes the timing intervals of the network. Timing intervals mediate how stations access the medium. For an iBSS, once timing and network identity are determined, stations may exchange data. For a BSS, there are two additional groups of services to manage traffic.

Distribution Services and Station Services

The nine services for a BSS are grouped into distribution services and station services. There are five distribution services and four station services.

Distribution Services

Distribution services manage traffic within a BSS and transfer traffic beyond the BSS. They provide roaming capability so a wireless station can move between the BSSs in an ESS. The five services are association, reassociation, disassociation, distribution and integration.

Association creates a logical connection between a wireless station and the access point. Once association is established, the access point will deliver, buffer, or forward traffic for a wireless station. The association service is used when a wireless station first joins a BSS or when a sufficiently long enough period has elapsed with no communication between the access point and the wireless station.

Reassociation is similar to association. A wireless station uses reassociation when moving between access points. A wireless station moving into an access point's coverage notifies the new access point with a reassociation request identifying the access point previously serving the wireless station. The new access point then contacts the prior access point for any traffic that has been buffered for the wireless station.

Either the wireless station or the access point can use disassociation. A wireless station sends a disassociation message when it is leaving the BSS. An access point may send a disassociation message to a wireless station if it is going offline or has no resources to handle the wireless station. In the latter circumstance, a wireless station may attempt to associate with a different access point, provided there is one in range.

Access points use the distribution service to forward frames received from wireless station in its BSS. Frames may be forwarded to another station within the BSS, to another station within an ESS, or to a router for delivery to a destination outside the WLAN.

Integration and distribution provide a portal to non-802.11 networks. Integration takes an 802.11 frame and recasts it as a frame for a different type of data link service such as Ethernet.

Station Services

While distribution services enable wireless stations and access points to establish communication, station services grant permission to use a BSS and accomplish delivery of data in the BSS. The four services are authentication, deauthentication, privacy, and data delivery.

Authentication, deauthentication, and privacy are potentially valuable. However, as Arbaugh, Shankar, and Wan have outlined in their recent paper [5], the current definition of these services cannot be relied on to protect access to the WLAN. In lieu of these limitations, there are alternative means, such as IPSec [6], to ensure the integrity of IP traffic sent across an 802.11 WLAN. More detailed discussion of these issues is beyond the scope of this article.

Of these services, data delivery is the most important. It provides reliable delivery of datagrams while minimizing duplication and reordering. It is the essential service for moving data across the WLAN. Data delivery, distribution, and management services are the essential services provided by the MAC layer of 802.11.

802.11: Versatile Wireless Environment

The MAC protocols provided by 802.11 permit the creation of a variety of short-range wireless networks. These networks range from ad hoc collections of stations to integral subnets of a complex internetworking structure. The flexibility of 802.11 may well obviate the need for other protocol stacks for personal devices. Regardless, 802.11's easy adaptability for TCP/IP networking has proven its value for large communities. It is for one such large community, the Internet Engineering Task Force (IETF), combining the strengths of 802.11 and IS-856 proved to be especially valuable.

An Overview of IS-856 Access Network Architecture

This overview describes how the wireless station and the access network provide transparent data transmission for the logical sessions between the wireless station and the Internet.

The description is based on a prototype implementation of the architecture. A scalable implementation would differ in some respects from the prototype, particularly with regard to methods for authentication and authorization of wireless stations. The description notes those details and offers alternatives more suitable for commercial implementation.

CDMA cellular networks are spread spectrum packet radio networks. Originally, the CDMA protocol was designed for efficient transmission of packets carrying voice data. Voice has different constraints than efficient data transmission. Voice transmission minimizes delay times at the cost of some data fidelity. The human ear is more tolerant of a little distortion than it is of delay. For data transmission, nearly the reverse is true. Errors in data bits increase packet retransmission that hurts overall network throughput.

In a CDMA network, the base station sends data to wireless stations over the forward link. Wireless stations use the reverse link to communicate to the base station. The IS-856 standard uses CDMA's reverse link packet structure retaining compatibility with voice traffic. The forward link packet structure is different, but the modulation techniques are the same, preserving compatibility in the forward link. However, management techniques for voice traffic and for data traffic differ considerably. A voice call comprises a single CDMA connection during which the call begins and ends. Packet data transmission comprises multiple CDMA connections, so that the CDMA network is used only when the wireless station must exchange data with the rest of the network. A single logical network session — a browser session or an e-mail exchange — will consist of a number of CDMA connections.

In the prototype IS-856 system all wireless stations were known, so registration of the wireless station in the network was simplified. In a commercial system, IS-856 systems would use the Remote Authentication Dial-In User Service (RADIUS) [4] to manage the registration and configuration information a particular access network would need. RADIUS is not the technique used to register cellular phones in CDMA networks. The carrier would unify its accounting and billing for data upstream of the systems using RADIUS with other systems used to account for voice traffic.

The RADIUS protocol is a means to authenticate connections to a data network and optionally provide configuration information to the device making the connection. When a user of a wireless station begins a session with an ISP, the wireless station and a network access server (NAS) exchange a series of messages that identify the user, and obtain parameters configuring the Point-to-Point Protocol (PPP) session used between the station and the access network. The network access server may rely on databases further upstream for authentication information it needs when the station attempts to connect.

Asymmetric Data Paths

To provide maximum data throughput for all wireless stations in the network, IS-856 uses asymmetric data paths. This is not unlike the asymmetry between forward and reverse links in CDMA voice systems. By taking this approach to a packet data network, it is possible to provide higher forward link burst rates than reverse link data rates. The user model for wireless stations assumes reverse link data demand is similar to demand at the terminals of wired networks. The forward link to the wireless station is capable of transmitting bursts up to 2.4 Mb/s. The reverse link provides a constant data rate of up to 153.6 kb/s for each station. These data rates are comparable to those typically found on cable networks such as Time Warner's Road Runner service or Cox@Home.

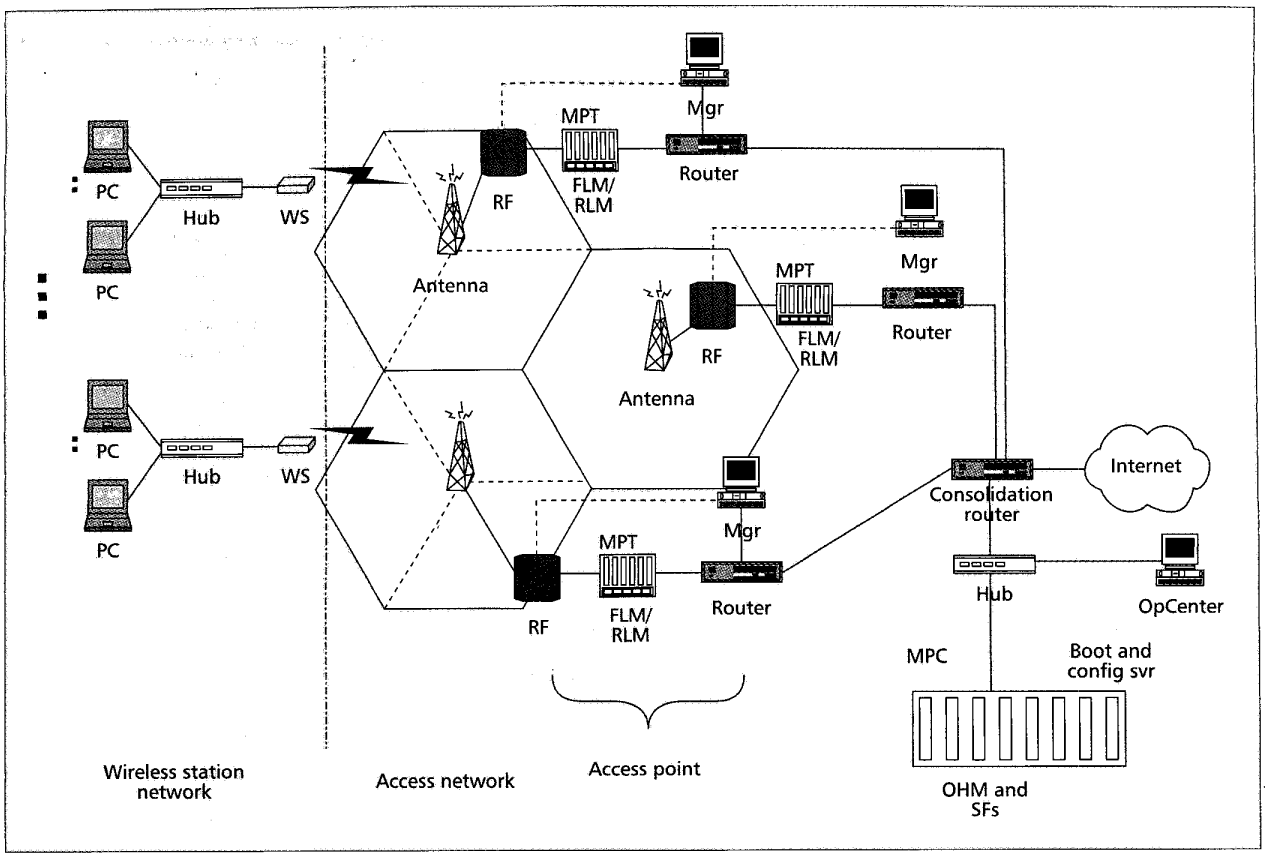
Access Network and Wireless Stations

The carrier's access network mediates connections between wireless stations and the Internet by providing access points in each sector. The access network is a private network, invisible and transparent from the point of view of devices connected to the wireless station or from the Internet beyond the access network. Access networks manage the IP space for all wireless stations in the carrier's service area. Besides transporting data, the access network includes monitoring and maintenance capabilities.

The access network and the wireless station use PPP as their data link protocol. PPP is carried over the radio channel using the Radio Link Protocol (RLP) of IS-856. [1, sec. 3] RLP minimizes data loss and packet retransmission in order to provide an interface to the wireless medium with error rates that meet or exceed the requirements for adequate PPP performance.

In the prototype, each wireless station manages a local subnet. This subnet is part of the IP space assigned to the prototype system, not part of the access network. In a commercial implementation using the same approach, the subnet managed by the wireless station would be part of an ISP's IP space. Using the Dynamic Host Configuration Protocol (DHCP), the wireless station distributes the IP space it manages, and transfers TCP/IP traffic between the devices, the wireless station services, and the access point. Because the wireless station handles the PPP connection, downstream devices don't need to. They simply function as they would ordinarily in a TCP/IP LAN. The wireless station and access point cooperate to shield devices from the PPP session and to permit persistent TCP/IP sessions, independent of the CDMA connections. This helps optimize the use of the CDMA network resources in a way that is transparent to the user.

Access networks manage the IP space for all wireless stations in the carrier's service area. Besides transporting data, the access network includes monitoring and maintenance capabilities.



■ **Figure 3.** *The access network.*

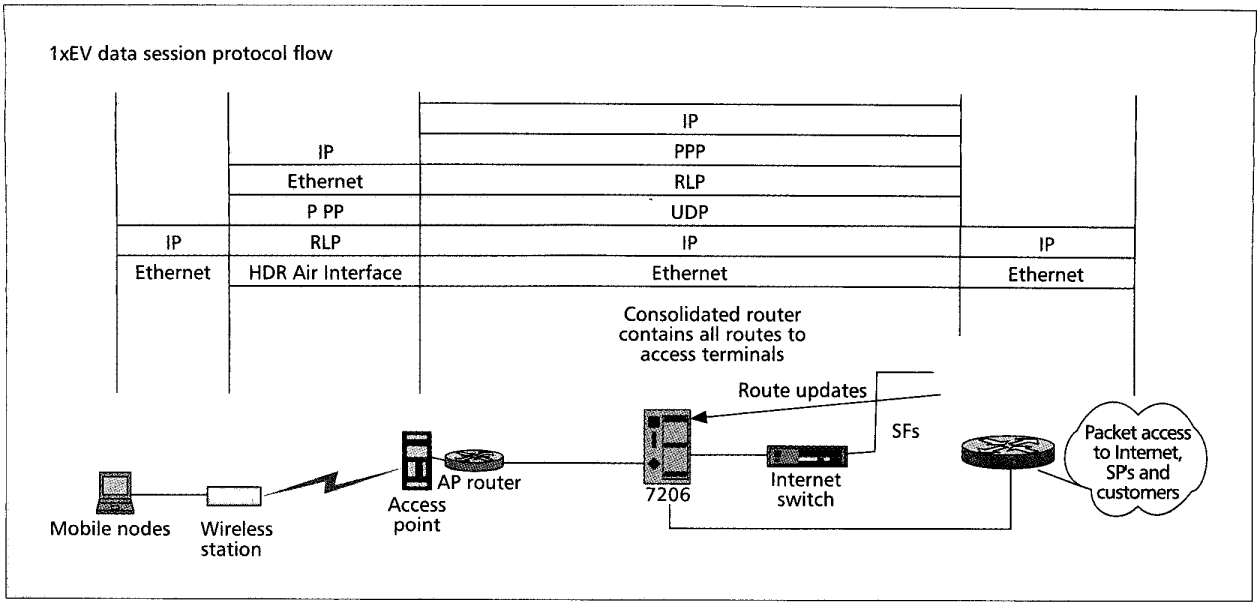
ACCESS NETWORK ARCHITECTURE

Figure 3 shows the connection between a wireless station (WS in the figure) and the access network, and the access network's internal structure. The access network consists of several subsystems. The principal systems are the consolidation router, modem pool controller (MPC), and access point. User Datagram Protocol/Internet Protocol (UDP/IP) is used within the access network to connect subsystems. These will be described below. While this is a description of a prototype architecture, most of the same components and functions must be present in a commercial system. Because this is a prototype, configuration information storage and maintenance is simplified.

The consolidation router creates the boundary between the access network and the rest of the Internet. It provides routing information to the Internet for all wireless stations managed by the access network. It also routes traffic within the access network, ensuring that private traffic stays within the access network. Routes for user devices to the Internet are derived from information maintained by the MPC.

The MPC is the heart of the access network. It houses the configuration server (CS), overhead manager (OHM), and a set of selector functions (SFs). The MPC uses the OHM and SFs to manage the state of wireless stations within all of the cells served by the access network. The OHM's primary role is to assign an SF for use during a wireless station session. In the prototype, the OHM also delivers configuration information it obtains from a static database in the configuration server. In a commercial system, the configuration server would interact with the RADIUS authentication, authorization, and accounting (AAA) server to obtain the necessary information for its database. When a wireless station registers with an access network (via some access point), the access point notifies the OHM about the wireless station. The OHM assigns an SF to manage the wireless station connection. In a commercial implementation, the SFs may retrieve wireless station parameters from either the configuration server database or directly from the AAA server. The SF cooperates with the wireless station to maintain PPP state. The SF encapsulates the PPP packet in RLP, then forwards it via UDP to the access point. The SF also updates the consolidation router with current routing information for the wireless station. When a wireless station moves between access points by moving into a new sector, the SFs for each access point update the wireless station routes for the consolidation router.

An IS-856 access point divides into two structures, a local router and modulation equipment connecting the access network to the cellular network. An access point shares its modulation equipment among a number of wireless stations. Over time, the wireless stations served by an access point will change.



■ **Figure 4.** *Access network protocol flow.*

The local router within the access point enables the modulation equipment to connect to the rest of the access network regardless of how resources are assigned to wireless stations. The modulation equipment consists of pairs of forward link module/reverse link modules (FLM/RLMs) and an RF adapter. Collectively, this is called the modem pool transceiver (MPT). Each FLM and RLM is an IP device on the access network LAN. The RF adapter connects FLMs and RLMs to the RF system of the CDMA base station.

An FLM receive packets destined for wireless stations. It provides the network and datalink layer interface performing intermediate modulation of the data. After the intermediate frequency (IF) stage, it hands the data stream to the RF adapter for broadcast in the cell sector. An RLM performs the inverse process. It receives an IF stream from the RF adapter, demodulates the data, and forms it into a packet, forwarding it to the SF.

Figure 4 shows how the access network uses UDP to encapsulate packets that are exchanged between the wireless station and the Internet. The red IP datagram contains the user data flowing to and from the mobile node. The other protocol layers in the diagram show the encapsulation used to make the access network transparent to the Internet and to devices connected to the wireless station. An IS-856 system preserves the PPP state between a wireless station and an SF. This must be accomplished despite movement of wireless stations between sectors and, consequently, between access points. The access network preserves this information by using UDP to wrap the entire packet down to the RLP layer. If a wireless station changes access points, the SF updates its internal route to the new FLM/RLM. In this way, the SF and the wireless station can maintain PPP state, regardless of how the wireless station moves between sectors.

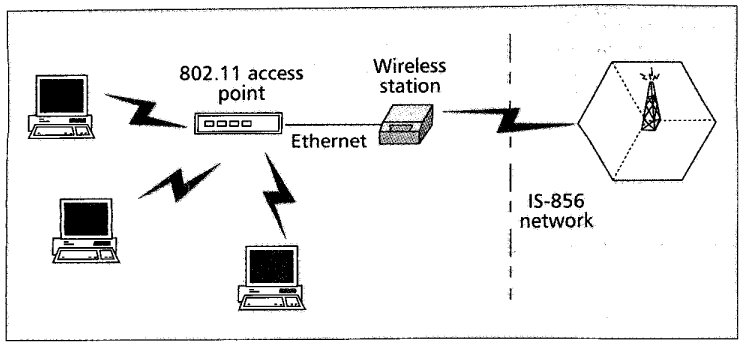
Over the Air Operation Summary

A typical IS-856 session between a wireless station and the Internet is described below. In addition, some aspects of IS-856 networks that enable a carrier to support multiple ISPs are noted.

In a full-scale implementation, the configuration server functions as a RADIUS client to obtain information about wireless stations appearing in range of the access network. The configuration server may cache information about wireless stations to optimize use of RADIUS.

A wireless station requests a session with the carrier's network by announcing its presence to an access point. As in CDMA voice systems, the access point requests an SF and authentication of the wireless station. Once an SF and modulation resources are assigned and the wireless station is authenticated, the SF and wireless station establish the PPP channel. The SF maintains the wireless station's PPP state in the absence of any traffic from the wireless station allowing the CDMA system to drop CDMA connections without terminating the wireless station's IP sessions. The OHM stores an idle timer value. When there is no reverse link traffic within this time period, the SF will drop the CDMA connection but maintain the PPP state (until the PPP session terminates). When the wireless station sends new traffic, a new CDMA connection starts, and the SF maintaining the wireless station relays the traffic to the consolidation router. Similarly, for forward link traffic, if there is no CDMA connection established between the SF and the wireless station, the SF will signal the FLM to create a connection in order to forward traffic to the wireless station.

A carrier provides IS-856 service by installing an access network and populating an AAA database with information about wireless stations served by the access network. In the proto-



■ **Figure 5.** *Hotel network connection.*

type, each wireless station was capable of managing a small IP space of its own allowing each wireless station to create a local network connected to the wireless station. There is no requirement all wireless stations described in the accounting database use contiguous IP space. This provides tremendous flexibility for both users and carriers. Each user can have a small LAN associated with the wireless station. As the number of TCP/IP devices proliferates, this is a powerful concept.

Carriers could serve any number of ISPs by leasing access to the wireless network for the IP space the ISP assigns for wireless access. Alternatively, a carrier could serve as the ISP and manage the IP space for all the wireless stations registered with its network. The policy that is followed is not constrained by the architecture of the IS-856 network.

Regardless of how the IP space is administered, each wireless station in an IS-856 network is capable of distributing IP addresses it manages. Combining this ability with the utility of 802.11 and the ubiquity of 802.11 devices in the large community of an IETF meeting provided a powerful demonstration of bridging 802.11protocols with an IS-856 network.

49TH IETF MEETING NETWORK

The IETF relies heavily on Internet communication for developing the protocols that are essential for the smooth operation of the Internet and for protocols for new services that can be provided over the Internet. The IETF meets thrice yearly for face-to-face working group meetings to assist the work carried out by members over the Internet. An essential part of every IETF meeting is the increasingly misnamed "Terminal Room." The Terminal Room is a LAN created for the meeting to provide Internet access to attendees, and to members who cannot attend in person. Until recently, the LAN for each meeting provided wired access throughout the meeting areas of the hotel where meetings are held. The last few meetings have experienced an explosion in demand for 802.11 wireless access as more attendees employ 802.11 wireless networks at home. As a result, attendees have come to expect 802.11 coverage throughout the meeting areas of the main hotel.

As the number of people attending IETF meetings has grown, the result is that typically the meeting hotel can no longer provide enough hotel rooms for all the attendees. Secondary hotels are used for the overflow. However, extending the meeting network to the secondary hotels has not been possible, putting attendees staying at the secondary hotels at a distinct disadvantage.

The design of the network for the 49th meeting in San Diego demonstrated a solution for the access problem in the secondary hotels, assuming that many attendees in the secondary hotels would have 802.11 cards for their laptop computers. By combining a prototype IS-856 network with 802.11 access points in these hotels, adequate access for those attendees was provided (Fig. 5).

An 802.11 BSS was installed in each secondary hotel. The 802.11 access point was connected to a prototype Qualcomm IS-856 wireless station via a short 10baseT Ethernet cable. Each IS-856 wireless station was assigned an IP address range from the prototype network it could distribute to the 802.11 cards of attendees' laptops. The 802.11 access point provided BSS housekeeping and the IS-856 wireless network provided the backbone links connecting the 802.11 networks. It wasn't a true ESS, because users could not roam between BSSs and preserve their network address. However, in principle, there is nothing to prevent the forwarding necessary for an ESS.

During the meeting some attendees were equipped with an IS-856 wireless station for their individual use. This was done to compare the performance of individual use of the IS-856 network with the shared access provided by connecting an 802.11b network to the Internet via the IS-856 network. An 802.11b network provides data rates comparable to 10 Mb/s wired networks. Because users of the 802.11 BSSs reported similar performance when a single IS-856 wireless station was shared among multiple users, this experiment demonstrated that an IS-856 network provides an adequate backbone for an 802.11b ESS.

Figure 6 shows a sample of the average data rates of both individual and shared IS-856 wireless stations operating during the meeting. One can see from the chart that forward and reverse data rates are comparable. Users of the shared wireless station in the 802.11 BSSs didn't seem appreciably affected by difference in data rates between 802.11b and IS-856. We regularly saw a dozen or more users sharing access to the IS-856 wireless station via the bridge. When we interviewed the users later, they were enthusiastic in their ability to access the net via the bridge. Based on their feedback on the performance of the prototype, using IS-856 wireless links as a backbone for an 802.11 ESS is promising.

CONCLUSIONS

The 802.11 standard has provided a very popular method for individual wireless access to the Internet. The quasi-ESS built with an IS-856 backbone offers interesting possibilities for practical systems. Both carriers and ISPs will face increasing demand from their customers for wireless Internet access. There are at least two approaches that exploit the ease with which an 802.11 net can be bridged with an IS-856 backbone.

One possibility is that carriers will provide both ISP and infrastructure services. Carriers will succeed in this approach as long as they are adept at providing a wide range of services and support demanded by their consumer subscribers. As successful ISPs have discovered, service and support demand for consumer Internet access will extend well beyond the demands of simply providing wireless Internet access.

Another possibility is that carriers will concentrate solely on building the infrastructure to transport data. ISPs will purchase wireless access much as they purchase wired transport today. In this scenario carriers would serve a more homogeneous set of customers consisting of ISPs with similar requirements. The ISP will focus on serving its specialized community of subscribers and take advantage of its knowledge of its customers to provide consumer subscribers with attractive services and support tailored to their tastes.

It is difficult to predict which of these scenarios will dominate the future of wireless Internet access, or if some wholly different model will appear. It is certain, however, that the cost effectiveness of deploying IS-856 and the high consumer demand for 802.11-based devices will lead to the use of both wireless protocols to satisfy demand for access to the wireless Internet.

ACKNOWLEDGMENTS

The author would like to thank his colleagues at Qualcomm and Cisco for their assistance with the development of the 49th IETF meeting network and the writing of this article. In particular, Paul Bender answered my numerous questions, and provided important insights into IS-856 as well as thoughtful commentary on early drafts of this article. Katy Bendel patiently explained the intricacies of an IS-856 access network. Jon Detra, Abhijeet Basain, and David Clapp provided the data on the performance of the bridges during the meeting. The author also would like to thank Phil Karn who originally proposed the idea of using the IS-856 prototype network to serve remote 802.11 users.

BIBLIOGRAPHY

[1] "cdma2000 High Rate Packet Data Air Interface Specification," 3GPP2, http://www.3gpp2.org/Public_html/specs/C.S0024.pdf., Sept 2000.

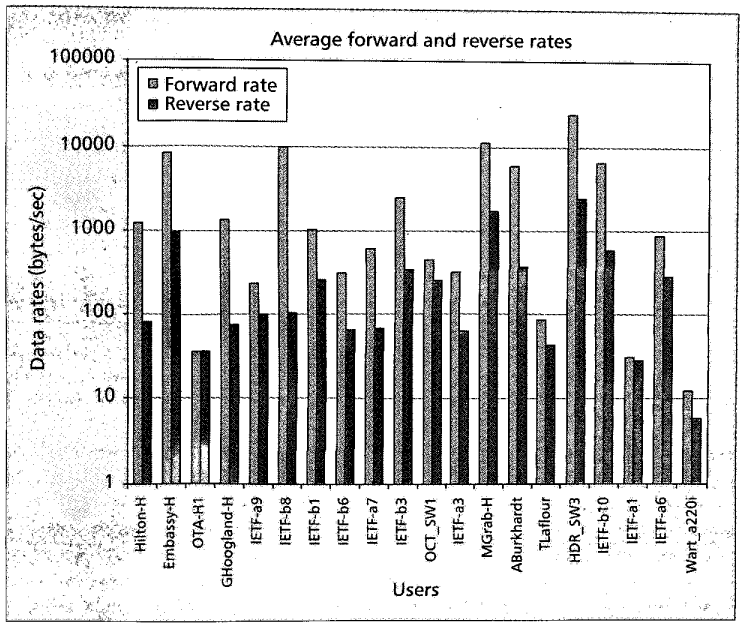


Figure 6. *Aggregate data rates.*

[2] "LAN MAN Standards of the IEEE Computer Society. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, IEEE Standard 802.11, 1999 Edition," 1999.

[3] O'Hara and Petrick, *802.11 Handbook, A Designer's Companion*, IEEE Press, Dec .1999.

[4] Rigney, Rubens, Simpons, and Willens, "Remote Authentication Dial In User Service (RADIUS)," RFC 2138, ftp://ftp.ietf.org/rfc/rfc2138.txt, Apr. 1997.

[5] Arbaugh, Shankar, and Wan, "Your Wireless Network Has No Clothes," Univ. of MD, http://www.cs.umd.edu/~waa/wireless.pdf, Mar. 2001.

[6] Atkinson and Kent, "Security Architecture for the Internet Protocol," RFC 2401, ftp://ftp.ietf.org/rfc/rfc2401.txt, Nov. 1998.

BIOGRAPHY

JOHN W. NOERENBERG, II (jwn2@qualcomm.com) is a principal engineer for Qualcomm, Inc, and has been designing and implementing Internet protocols since 1989. Prior to 1989 he spent a number of years developing wireless network protocols with Linkabit Corporation. He contributed to the design of the MIME protocol, and led the commercial development of the e-mail program Eudora. He is also engaged in cryptographic work chairing the IETF OpenPGP working group. With Qualcomm, he contributed to the design and implementation of the corporate network, and recently returned to working on wireless data protocols. He holds a B.S.E.E degree from Purdue University.