OFFICE OF THE MANAGER
NATIONAL COMMUNICATIONS SYSTEM
TECHNICAL
NOTES

AUGUST 2000 *TECHNOLOGY AND PROGRAMS DIVISION* VOLUME 7, NUMBER 4

Wireless IP—Internet Without Wires

by Ray Young

INTRODUCTION

The wireless telecommunications industry is actively developing a new generation of products that merge new data services into the mobile handset. In addition, the emerging Wireless Intelligent Network (WIN) standard allows smart devices and specialized services to be added to the cellular network. Also, consumers' desire to maintain their full suite of services as they roam outside their home service area has created a demand for interoperable data technologies. Service providers are merging their circuit-switched networks with their packet-switched networks. These developments, in turn, have led to the extension of the Internet Protocol (IP) to the next generation of mobile handsets, called third generation (3G). All these trends are creating a demand for wireless IP.

This Technical Note explores wireless IP from its roots in the Mobile IP standard, defines the emerging architecture, and projects wireless IP's impact on National Security and Emergency Preparedness (NS/EP) communications.

WHAT'S THE PROBLEM?

IP was not originally designed with mobility in mind. A device attached to an IP network is given a static address to identify itself to other entities on the network. When the device is moved to a new network, it is generally assigned a new address.

Cellular phones and mobile Internet devices using IP, however, may move from one base station (BS) to another or one mobile switching center (MSC) to another during a conversation/data session, or the subscriber may roam out of the home network service area. Nevertheless, the subscriber's home network must seamlessly track the subscriber's services and the mobile handset's IP address to relay incoming packets.

MOBILE IP

To deal with this problem, the Internet Engineering Task Force (IETF) drafted the Mobile IP standard, Request for Comments (RFC) 2002.[1] This protocol creates a mechanism for delivering packets to an object on the network. If the object changes its point of attachment to the network, packets to be delivered to the object are forwarded to its new location.

Figure 1 depicts at a high level how communications occur over an IP network using Mobile IP. The mobile node is assigned to a home agent (HA). The HA is a router on the mobile node's home network that maintains current location information about the node. When the mobile node moves to another network, called a foreign network, a foreign agent (FA) registers the mobile node, receives data from the HA, and delivers the data destined for the node.

In Mobile IP, the mobile node moves from its home network to a foreign network and registers with the FA. The FA assigns a "care of" address to the mobile node, which is stored with the HA. When another object or Internet service sends packets to the mobile node, the HA uses the "care of" address and forwards the packets to the FA. The FA delivers the packets to the mobile node.

Although wireless communication between a device and a network is common, mobility does not necessarily mean a wireless communication path exists. The Mobile IP RFC does not solve all the problems presented by emerging 3G networks; therefore, additional wireless IP protocols are under development by the IETF and other standards-forming bodies.

ARCHITECTURE/FUNCTIONAL DESCRIPTION

Wireless IP will provide mobile subscribers with 3G communications and data transfers of up to 384 kilobytes / second. Figure 2 describes the emerging architecture for Wireless IP.[2] This model assumes the mobile handset is not in the subscriber's home network. The mobile handset connects via the air link to the radio network (RN) (base station and / or base station controller). The RN connects to the Visiting Location Register (VLR), which uses the Signaling System 7 (SS7) network and signaling to gain subscriber information from the Home Location Register (HLR) within the subscriber's home network. The RN also connects to the Public Data Switched Network (PDSN), which maintains the connection through the Public Data Network to the subscriber's home network. The PDSN is equivalent to the FA in Mobile IP. Authentication services are pro-

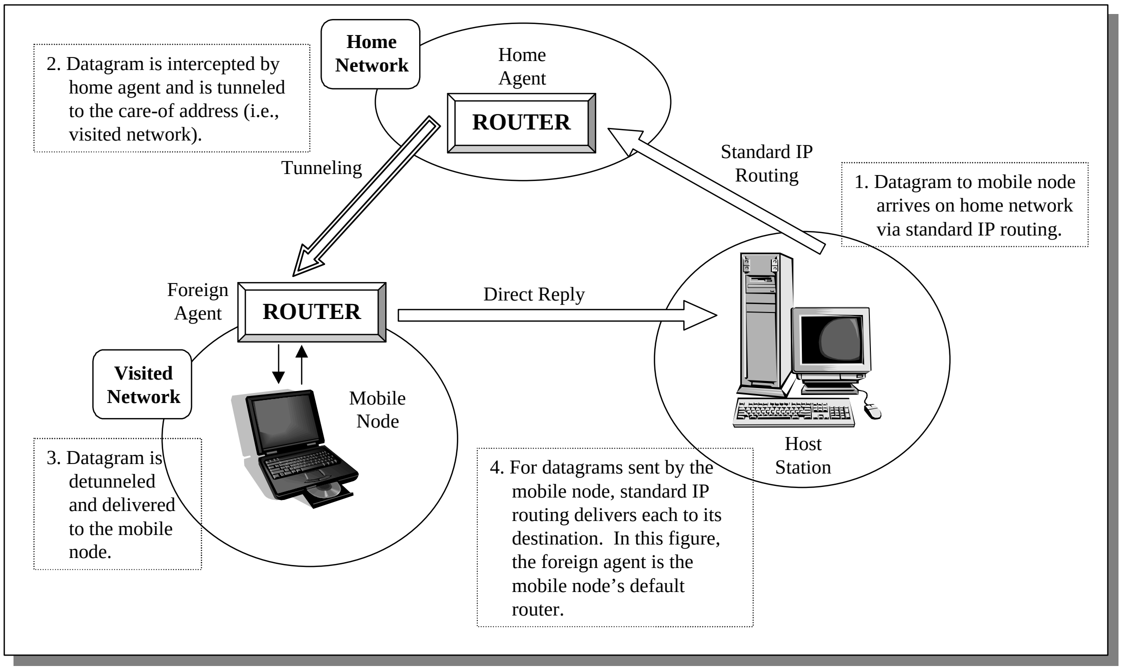

Home Network
Home Agent
ROUTER
2. Datagram is intercepted by home agent and is tunneled to the care-of address (i.e., visited network).
Tunneling
Standard IP Routing
1. Datagram to mobile node arrives on home network via standard IP routing.
Foreign Agent
ROUTER
Direct Reply
Visited Network
Mobile Node
Host Station
3. Datagram is detunneled and delivered to the mobile node.
4. For datagrams sent by the mobile node, standard IP routing delivers each to its destination. In this figure, the foreign agent is the mobile node's default router.

Figure 1. Mobile IP Architecture

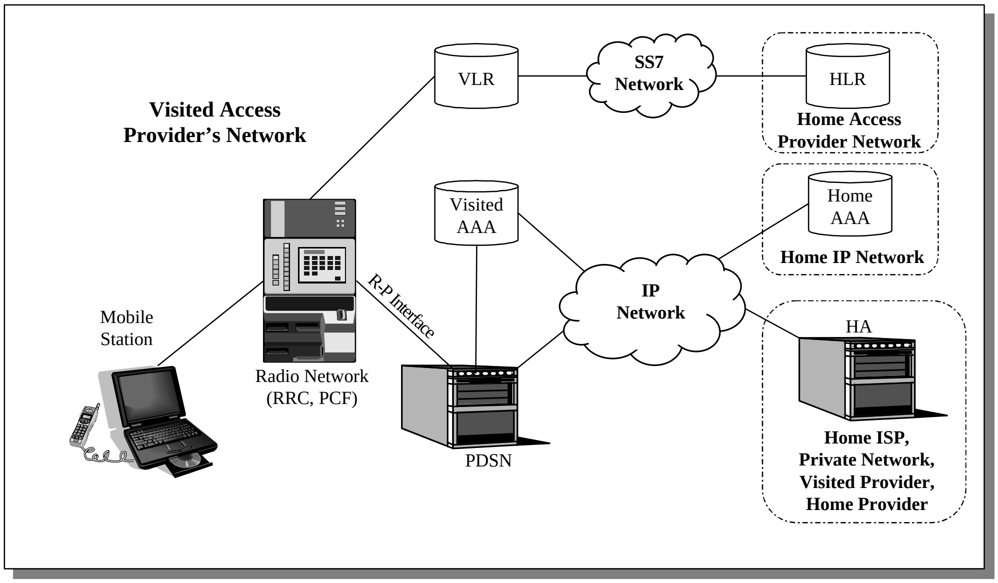

VLR
SS7 Network
HLR
Home Access Provider Network
Visited Access Provider's Network
Visited AAA
Home AAA
Home IP Network
R-P Interface
IP Network
HA
Mobile Station
Radio Network (RRC, PCF)
PDSN
Home ISP, Private Network, Visited Provider, Home Provider

Figure 2. Architecture Model for Mobile IP

vided through the Visited Authentication, Authorization, and Accounting (AAA) node in concert with the Home AAA node. The HA serves the same function as in the Mobile IP RFC.

PROTOCOL ARCHITECTURE LAYERS

Figure 3[2,3] describes the Protocol Reference Model for Mobile IP. Logically, the layer 1 connection between the mobile station (MS) and the RN is the air link. The air link will be defined by one of the emerging 3G RF standards. The physical link with the other entities depends on the service providers' hardware choices. Generally, the backbone connections are now fiber optic cables using Asynchronous Transfer Mode (ATM) and frame relay to transport packets.

The Medium Access Control (MAC) layer controls and manages common resources (e.g., packet data channels) between the MSs and the RN. MAC controls synchronization and implements Quality of Service (QOS) requirements. The Link Access Control (LAC) layer is responsible for ensuring that data transmitted between the MS and RN is segmented, transmitted, and reassembled correctly.

The Point-to-Point Protocol (PPP)[4] is a data-link network layer protocol that enables

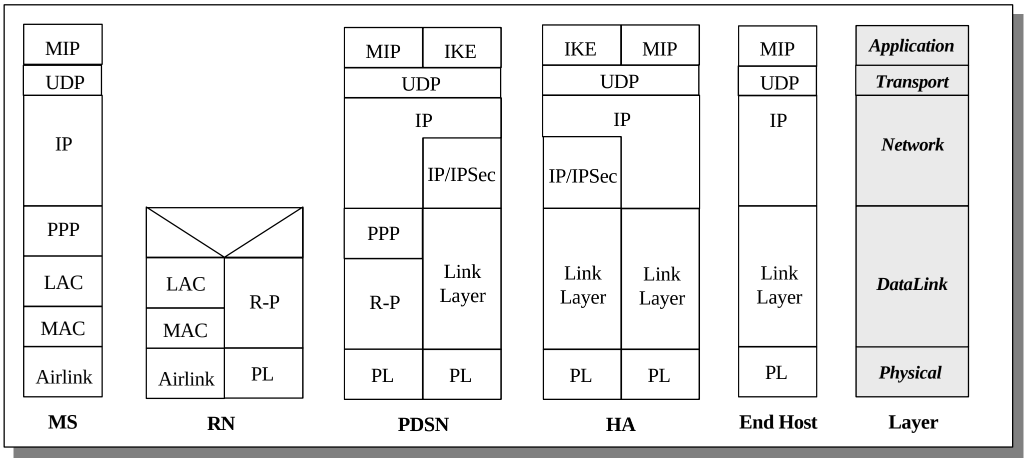


Figure 3. Protocol Reference Model for Mobile IP

multiple protocols to be transported between points on a network. The protocol is bidirectional, allowing various kinds of network nodes to communicate asynchronously.

The radio-packet (R-P) interface is the link between the RN and the PDSN. Here, the radio-dependant part of the network connects with packet data network elements. The R-P interface maintains the logical connection for the communication session. The R-P session must remain intact, even when no data packets are being passed between the MS and the HA. When the MS moves from one RN to another, the R-P session moves to the new RN. However, if the MS moves to another PDSN, a new R-P session is established. The MS and PDSN establish a PPP link after the RN and PDSN establish the R-P link.

Wireless IP uses the User Datagram Protocol (UDP) at the Transport level. This connectionless protocol is fast because no acknowledgement of packets' receipt is needed.

Riding on top of these layers is the Application layer. For example, the Mobile IP and Internet Key Exchange (IKE) protocols work on the Application layer.

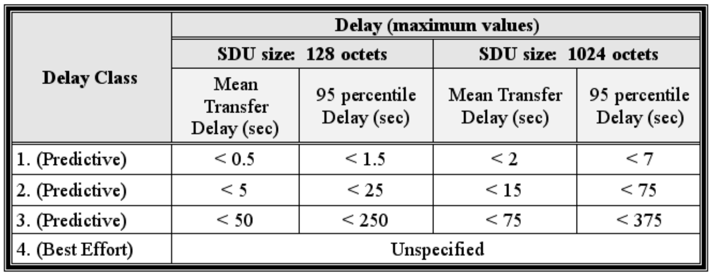
QOS AND SLAS

QOS is an important component of wireless IP. Different kinds of communications can handle different QOS levels. QOS measures Internet traffic; specifically, it quantifies the delay, throughput, and reliability that an Internet packet or packet stream is receiving. Packet streams are often delayed by network congestion. Congestion can occur anywhere in the call path, affecting the MSC, BS, or handset.

A subscriber negotiates with a service provider for the desired QOS, which is quantified in a service level agreement (SLA). An SLA is a contract between the user and service provider that specifies the level of service (i.e., bandwidth, loss rate, and delays) and the type of treatment and routing the Internet traffic will receive. It also specifies times of service availability and describes how the service will be measured and billed.

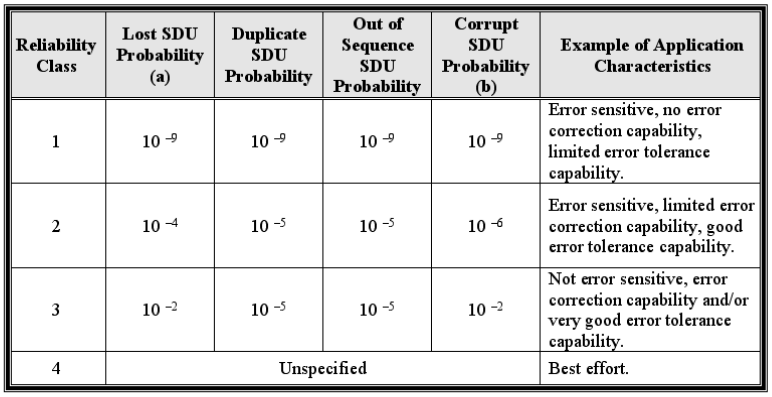
QOS IMPLEMENTATION FOR WIRELESS IP

Tables 1 and 2[5] illustrate how an SLA might be translated into a wireless IP network. Actual implementations may vary from values shown in the tables.



Delay Class	Delay (maximum values)			
	SDU size: 128 octets		SDU size: 1024 octets	
	Mean Transfer Delay (sec)	95 percentile Delay (sec)	Mean Transfer Delay (sec)	95 percentile Delay (sec)
1. (Predictive)	< 0.5	< 1.5	< 2	< 7
2. (Predictive)	< 5	< 25	< 15	< 75
3. (Predictive)	< 50	< 250	< 75	< 375
4. (Best Effort)	Unspecified			

Table 1. Delay Classes

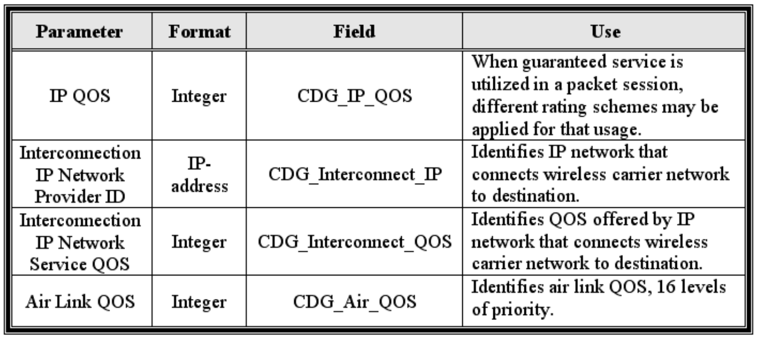


Reliability Class	Lost SDU Probability (a)	Duplicate SDU Probability	Out of Sequence SDU Probability	Corrupt SDU Probability (b)	Example of Application Characteristics
1	10^{-9}	10^{-9}	10^{-9}	10^{-9}	Error sensitive, no error correction capability, limited error tolerance capability.
2	10^{-4}	10^{-5}	10^{-5}	10^{-6}	Error sensitive, limited error correction capability, good error tolerance capability.
3	10^{-2}	10^{-5}	10^{-5}	10^{-2}	Not error sensitive, error correction capability and/or very good error tolerance capability.
4	Unspecified				Best effort.

Table 2. Reliability Classes

General Packet Radio Service (GPRS), a GSM implementation of wireless IP, gives subscribers a choice of one of three priority levels for any one of five classes, including service precedence, reliability, delay, peak throughput, or mean throughput.

A CDMA2000 type of wireless IP that uses Remote Authentication Dial-in User Service (RADIUS) offers a different QOS implemen tation. The User Data Record (UDR) has a QOS field with four subfields. This means CDMA2000 can provide a finer granularity of QOS treatment. Table 3[3] provides additional details about the RADIUS QOS implementation. Clearly, CDMA2000 provides improved mechanisms for identifying priority traffic and tools for developing priority services.



Parameter	Format	Field	Use
IP QOS	Integer	CDG_IP_QOS	When guaranteed service is utilized in a packet session, different rating schemes may be applied for that usage.
Interconnection IP Network Provider ID	IP-address	CDG_Interconnect_IP	Identifies IP network that connects wireless carrier network to destination.
Interconnection IP Network Service QOS	Integer	CDG_Interconnect_QOS	Identifies QOS offered by IP network that connects wireless carrier network to destination.
Air Link QOS	Integer	CDG_Air_QOS	Identifies air link QOS, 16 levels of priority.

Table 3. Quality of Service Field Definition

Security Mechanisms

Wireless IP would be incomplete without security. Generally, security involves ensuring the integrity of control messages. Access to an RN can be secured through encryption and authentication of the MS.

An MS initially registers with the visiting PDSN. The PDSN can use any means internal to the network to initially register and authenticate the MS. Using a form of public key encryption (IKE, for example), the HA and PDSN establish a security relationship. A reverse tunnel is deployed in addition to the tunnel IPSEC establishes. By using a reverse tunnel, data packets are encrypted in both directions between endpoints. An MS and the MS's home network share a key or security relationship known only to each other. The HA authenticates the MS using this relationship. After the HA authenticates the MS, the MS and PDSN begin their data session. The PDSN uses a key made up of the network, the mobile's IP address, and the time stamp to identify the MS and encrypt MS packets.[6,7]

When a mobile node sends data to its HA, a filter (e.g., firewall) may discard the incoming packets because they contain a source address internal to the home network. Reverse tunneling is one technique used to circumvent this problem. Reverse tunneling creates a secure path from the PDSN to the HA, and the MS uses the PDSN's "care of" address as its source address. As a result, the mobile's location is hidden as it traverses the IP network, providing an extra layer of privacy for the subscriber.

IKE provides a generic ability to establish keys for encryption between network entities (e.g., PDSN and HA). The difficulty with key exchanges is that both sides of the exchange have no previous relationship and the keys need to be created without any observer, "the man in the middle," being able to discover the key as both sides complete their negotiation. If an adversary gains the encryption key, the network becomes vulnerable to replay attacks, false registrations, and phony control messages (e.g., handovers or sign-offs).

IPSEC provides security for mobile IP data packets through two kinds of services. First, it ensures the authenticity and integrity of the data header. Also, it ensures the confidentiality of the packet's data. Together, both IPSEC services provide end-to-end encryption and security for IP traffic.

Developing Work

Active standardization of wireless IP is occurring in national and international standards bodies. Companies are eager to deploy interoperable standards in their emerg-

ing wireless data products.
In the IETF, work is continuing to adapt the Mobile IP protocol to the needs of the emerging 3G technologies. For example, protocols under development optimize routes and support reverse tunneling. Work is ongoing to extend wireless IP to IP version 6 (IPv6). Work is in development to provide security through AAA, registration, and unique challenges.

Outside the IETF, the International Telecommunications Union (ITU) is standardizing the 3G network protocols and air interfaces. Work is ongoing to produce regional implementations of 3G in 3G partnership projects (3GPP for GSM and 3GPP2 for the American National Standards Institute [ANSI]-41 networks). Nationally, T1 is standardizing GPRS through its Wireless/Mobility Systems and Services standards body (T1P1). The Telecommunications Industry Association (TIA) is standardizing wireless IP protocols through its Adjunct Wireless Packet Data Technology standards body (TR45.6), including CDMA2000.

The National Communications System (NCS) is approaching wireless IP from two fronts. First, work is in progress to provide WIN queuing at the access and egress parts of the network. Also, the NCS is working with industry to ensure NS/EP requirements are included in network elements. Efforts will be needed to ensure wireless service providers' networks support NS/EP requirements. Next, the Government Emergency Telecommunication Service (GETS) will need to work with service providers to develop NS/EP-based SLAs.

NS/EP communications will be greatly enhanced by wireless IP products. Initially, subscribers could receive text messages, but eventually, the mobile handset will become a video teleconferencing tool. The subscriber could receive maps and photos and transmit real-time video of disaster scenes.

The NCS is exploring how NS/EP communications can navigate congested IP networks as circuit-switched networks are merged with packet-switched systems. NS/EP communications are becoming increasingly dependent on wireless systems, and therefore, developing wireless solutions is becoming increasingly important. The NCS is actively working with industry to explore how NS/EP requirements can be included in emerging standards.

References

1. Perkins, C., "IP Mobility Support," RFC 2002, October 1996.
2. "Wireless IP Architecture Based on IETF Protocols," PN-4286-A (to be published as TIA/EIA/TSB-115), February 10, 2000. (Subject to change)
3. "Wireless IP Network Standard," PN-4732 (to be published as a TIA/EIA Interim Standard), January 13, 2000. (Subject to change)
4. Simpson, W., "The Point-to-Point Protocol," RFC 1661, July 1994.
5. "Issues Relating to Adapting the PCS 1900 GPRS Network To Support Wireless Internet Protocol Telephony," Draft Technical Report, T1P1.5/2000-096, January 22, 2000. (Subject to change)
6. Campbell, A., "Cellular IP," Internet Draft, Internet Engineering Task Force, January 2000. (Subject to change)
7. Khan, Irfan, "Draft Technical Report on Mobile IP for PCS 1900 Networks," T1P1.5/99-120r4, July 1999. (Subject to change)

For further information, please contact:

Ray Young
National Communications System
Technology and Programs Division (N2)
701 South Court House Road
Arlington, VA 22204-2198