Secure access and roaming between wireless local and wide area networks.

Christopher Couper, IT Architect
Jyrki (Jeri) Korkki, Global Solution Manager
### Contents

2 Executive summary
4 Wireless LANs are becoming commonplace
5 Wireless LAN standards
6 Types of wireless LANs
9 Security and authentication in wireless LAN environments
15 Wireless wide area networks
16 Seamless roaming
18 Mobile IP
25 IBM WebSphere® Everyplace Connection Manager
29 Security considerations while roaming
30 IBM WebSphere Everyplace Connection Manager provides seamless roaming over the enterprise firewall
32 Summary
34 About the authors
36 Endnotes

### Executive summary

In the past few years, the prevalence of wireless local area networks (LANs) has increased dramatically. Companies are now starting to implement wireless LANs as a convenient network access method to enable workforce mobility within their buildings and campuses. The ratification of the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standards, lower prices and rapid progress to higher data rates have put the promise of truly mobile high-speed computing within reach. Wireless LANs allow companies to lower their infrastructure costs. They can save on cabling costs in new, to-be-expanded and to-be-renovated buildings. Companies can also save office space through “hot desking” mobile users, and can facilitate temporary LANs for peak season and special projects.

In the public space, hotels, airports, convention centers and even restaurants are putting in wireless LAN hotspots to facilitate high-speed access to the Internet for their customers. This could be a revenue generation scheme or a means of providing enhanced customer service, all applying to the mobile road warrior or business professional that needs high-speed access while away from the traditional office. The objectives of deploying wireless LANs could also include providing services to an increasing number of data-hungry consumers, for example, to allow them to download streaming video or music files in public places.

More and more business professionals are installing wireless LANs in their homes to extend the high-speed broadband access anywhere and to avoid cabling private residences. Reasonably priced combinations of DSL (digital subscriber line) and cable modems, routers, firewalls and wireless LAN access points have come to the market.
Where wireless LANs are not available, the 2.5G and 3G wireless networks can provide the means of communication. While not providing the same speed as wireless LANs, even at speeds around 56 kbps they can still provide an acceptable wireless alternative to wired dial-up access.

To provide a seamless end-user experience between wireless LAN hotspots and wireless wide area networks (WANs), various roaming solutions are appearing on the marketplace. This paper will examine two methods of providing consistent wireless access regardless of the end user’s work location and means of connection. We will also discuss wireless network standards and technologies, examine the security aspects of wireless networks, and look into some of the technologies and issues regarding secure access and roaming between wireless networks.

An ideal communications solution for the business user would allow him or her to connect without wires and at high speed to the company intranet and to the Internet from virtually anywhere—from home, when on the road, from cafes, restaurants and hotels, while visiting customers and at the office (see Figure 1—Ideal communications solution).
Wireless LANs are becoming commonplace

Wireless LANs are becoming the preferred way to connect to the company intranet and even to the public Internet. Not only do they provide end users with the flexibility to be able to work virtually anywhere within their coverage area, but they can also significantly reduce network implementation and running costs. Companies around the world are beginning to receive pressure from their mobile employees to provide wireless LANs.

On the road, the “road warriors,” workers who rarely work in a traditional office or whose work location changes frequently, can get high-speed access to the Internet through public wireless LANs. This may be in the waiting area or a lounge of an airport, a hotel room or convention center, or even their favorite coffeehouse. In short, it may be anywhere that the mobile worker can find a few minutes of free time to catch up with work and can take advantage of a high-speed network connection to replicate e-mail, upload and download large files, access enterprise applications, participate in chat sessions and access the Internet.

Wireless LANs are made up of several components (see Figure 2—Wireless LAN components and security solutions):

- Built-in wireless LAN adapters or removable wireless LAN PC cards that enable mobile devices to communicate without wires
- Access points that connect wireless devices to a wired Ethernet network
- Wired Ethernet backbone network for the wireless LAN access points
- Security infrastructure components, such as access controllers and authentication servers, which are used to authenticate users and control their access to the network. Note that the security in wireless LANs can also be provided with virtual private network (VPN) technology, which is discussed later in this paper.
- Service provisioning, billing and settlement systems for public wireless LANs.

Various components make up a wireless LAN, from LAN adapters for PCs and mobile devices, to the Ethernet backbone network that connects the access points.
Wireless LAN standards

The IEEE 802.11 has become a de facto standard for wireless LANs. This standard has several variants. The IEEE 802.11b—often called “Wi-Fi” or wireless fidelity—is the current, most widely deployed standard, operating in the 2.4 GHz frequency band and enabling wireless data transmission up to 11 Mbps.

The IEEE 802.11a is a more recent standard, and may eventually overtake the current 802.11b standard—although it is expected that the current 802.11b standard will hold its dominant position for some time due to its widespread use. There will also be some wireless LAN base stations with dual radio systems that allow the two systems to be used concurrently. The new 802.11a standard offers data transmission speeds up to 54 Mbps. It operates in the 5 GHz frequency band where there is less radio frequency interference and where there are eight non-overlapping radio channels, as compared to the three non-overlapping channels that are available in the 2.4 GHz band. These additional channels allow more systems to overlap in the same physical space, or they can be used to increase the total aggregated data transmission capacity by deploying parallel wireless LAN access points. 802.11a standard-based wireless LAN equipment arrived in the North American market in the beginning of 2002.
Europe has been developing its own high-speed wireless LAN standard, the HiperLAN/2. There are currently no commercial HiperLAN/2 products on the market, and therefore, its future remains unclear. In 2002, some European telecommunications administrators started to issue licenses that allow the use of 802.11a-compliant wireless LAN equipment. There will also be a variant of 802.11a that is specifically designed for Europe and that meets the European regulations. This new standard, known as 802.11h, is expected to become available during 2003.

The most recent IEEE wireless LAN standard—802.11g—is an attempt to refresh the 802.11b standard. Like 802.11b, the 802.11g standard operates in the 2.4 GHz frequency band but uses a new modulation technique (OFDM—orthogonal frequency division multiplexing) that enables higher speeds. Market adoption of the 802.11g standard is still unclear, and at the time of this writing, there are no commercial 802.11g-based products on the market.

Types of wireless LANs

Wireless LANs can be characterized by their usage: enterprise wireless LANs; public wireless LANs in public places; and public wireless LANs inside companies and enterprises (semi-public).

Enterprise wireless LANs

While not getting the same attention in the media as public wireless LANs, more enterprise wireless LANs are installed each day than any other type of wireless LAN. Many of the world's largest corporations have mobile workforces at least a portion of which depend on enterprise wireless LANs as their means of connectivity to the corporate intranet.
Unfortunately, wireless LANs are not always under the control of corporate IT departments, nor do the users strictly adhere to corporate IT standards—which presents a serious security problem. With the cost of wireless LAN access points dropping close to a few hundred dollars (US$), it has become inexpensive to install a small workgroup wireless LAN for a handful of users. The hardware prices for small workgroup wireless LAN installations are going below US$1,000, well below many departments’ discretionary spending limits. In addition, for small work areas with one or two access points, installation can be as simple as setting them in place, providing power and hooking them up to the corporate network with an Ethernet cable.

IBM recommends that enterprise wireless LANs be integrated into an overall corporate intranet network and adhere to corporate network security standards and strategies. Wireless LANs need to be safeguarded so that unauthorized persons from the outside cannot use them to access the company intranet. The over-the-air interface must be encrypted, and there must be a secure access control system that will help prevent unauthorized use of the wireless LAN network. This will also allow for consistency in access, usage and security across the corporation, as well as ease of maintenance. If each department were to deploy their wireless LANs without adhering to the overall corporate framework, it would most likely result in spiraling costs and non-secure systems, and access and usage would be limited between sites, or worse, workgroups. This would hinder the communications of the users that visit their different corporate sites during occasional work sessions or during temporary assignments. Having a consistent corporate standard and implementation strategy for wireless LANs will not only help support security and uniform access, but will also reduce the overall costs and support requirements within an enterprise.
Public wireless LANs are becoming commonplace in locations such as hotels and airports, and are becoming more widely deployed in other public places, such as government buildings, libraries and even street corners.

Having a public wireless LAN can provide a venue owner with a competitive advantage over establishments that do not have that capability, because it gives consumers an incentive to choose that establishment over others.

Public wireless LANs
Public wireless LANs are being implemented by service providers and even venue owners such as hotels and restaurants by themselves. These networks provide high-speed access to the Internet for mobile professionals and consumers. Public wireless LAN hotspots are appearing in locations such as airports, hotels and convention centers but could eventually include other public spaces, such as government buildings, libraries, hospitals, parks, and even street corners. Many establishments such as restaurants and shopping malls are installing public wireless LANs to increase their clientele as well as to invite extended visits that potentially increase overall sales per visit. Communities are beginning to deploy public wireless LANs as a means of providing information to their citizenry.

The revenue models for public wireless LANs may be direct, by charging for the access time, may be given away for free, or may be hidden in nonrelated charges in order to increase some other revenue opportunity. For example, a hotel may provide wireless LAN access in its hotel rooms, restaurants and meeting rooms for no additional charge in an attempt to guarantee certain usage of their property, or may bundle it within a package price. A wireless LAN could also be provided as an incentive to use a certain establishment’s services, giving that establishment a competitive edge over those that do not provide such a service. For example, a restaurant may provide a wireless LAN in its banquet room to entice organizations to hold their large meetings there. In fact, in some cases the public wireless LAN could be the major reason why a client visits an establishment—and then buys its products or services as an afterthought.
Access to the Internet in public wireless LANs can be controlled either by means of a user id and password or by means of some more sophisticated method, such as a smart card or SIM (subscriber identity module) card—a physical token in the user’s possession. The end-user data security is ultimately the end user’s responsibility, but responsible public wireless LAN service providers should do their utmost to advise their customers about data security in public wireless LANs.

Public wireless LANs inside companies and enterprises
A public wireless LAN may also be deployed inside an enterprise to give wireless high-speed connectivity to a select set of visitors that are generally well known to the organization, such as contractors and business partners. This type of public wireless LAN, even though it is physically inside the corporate premises, is installed outside the company firewall. Access to it is controlled as with any other public wireless LAN, i.e., through user id and password. Public wireless LANs inside company premises provide high-speed Internet connectivity to visitors, allowing users to access their own intranets using security-rich VPN tunnels through the Internet.

Security and authentication in wireless LAN environments
Security in wireless LANs is more demanding than in wired networks. Wireless LANs use radio waves, and radio waves do not respect the physical boundaries of an organization’s property. For example, it may be possible to stand along a public thoroughfare adjacent to a building with a wireless LAN installation and receive the signals from it. In Europe, wall chalkers have written on the outside of buildings, telling hackers the addresses of unsecured wireless LANs. Appropriate security measures have to be put in place to protect wireless LAN installations and to control who can access them.
Enterprise wireless LANs are extending the corporate intranet, which makes security of paramount concern. In public wireless LANs, access control and user authorization are enforced to ensure that the users pay for their access to the network. This is generally the model in public wireless LANs. However, in some special cases, access and authorization may not be enforced at all, giving anyone free access to the wireless LAN. In some unfortunate cases this is not by design, but instead due to an unknowing wireless LAN installer or administrator incorrectly configuring the wireless LAN.

There are special tools, sometimes called “sniffers,” that can identify wireless LANs around them. We have seen examples where businesses have not properly restricted access to their networks. There are also known cases where people have been able to access these wireless LANs and use them to “surf” the Internet (and possibly also the corporate intranet) without the company’s permission or knowledge.

Security and access control are two independent aspects of the wireless LAN environment, but they need to be implemented together in a coordinated fashion. In this section we will look at the various security and user authentication methods that can be used to control and limit access to the wireless LAN. We will cover the most frequently used methods and indicate the pros and cons of each.
Protecting wireless LANs

As simple as wireless LANs are to install, security-rich enterprise wireless LAN systems are far from easy to deploy. If a wireless LAN is deployed incorrectly, it can jeopardize the corporation’s IT assets and security. Enterprise wireless LAN designers need to consider not only access and availability issues, but also security. While an Ethernet LAN is generally considered protected by its physical location within enterprise buildings, wireless LAN signals do not respect the building walls. They often penetrate the physical boundaries of buildings.

Earlier security methods that were built into the 802.11 standard, such as SSID (service set identifier)—a unique key to identify devices that belong to a given network; MAC (medium access control) filtering—setting filters to the access points that allow only devices with a defined MAC address to access the network; and the use of a static WEP (wireless equivalent privacy) key—a static encryption key that has to be installed in all wireless LAN stations and access points—are considered to provide low levels of security features and should only be used with some higher-level security solutions such as VPN.

There are multiple ways to improve wireless LAN security. The two most commonly used solutions are 802.1x standard-based security and virtual private networks.

IEEE 802.1x-based security

The IEEE 802.1x standard-based security solution makes use of the physical access characteristics that are built into the network infrastructure components. Wireless LAN access points can play the part of an authenticator. When users want to access the wireless LAN network, access points challenge them to show their credentials. A small supplicant code needs to be installed into the wireless LAN devices to facilitate the end-user interaction, i.e., to request that a user enter his user id and password or to handle some stronger means of authentication such as reading a smart card.
Secure access and roaming between wireless local and wide area networks.

Highlights

With 802.1x-based security, wireless LAN access points can be used to authenticate users dynamically, with every access attempt/session.

When an access point receives the user’s credentials, it forwards them to the authentication server (RADIUS server) and asks it to authenticate the user. If the access point receives authorization, it will create a dynamic WEP key and allow the user to access the network. The dynamic WEP key is used for only that particular user and that session. Data between the device and an access point is then encrypted using the dynamically created WEP key. As an added security measure, the system can be configured to continuously change the WEP key (during a user’s session) to make it even harder to break into the network.

Wireless LAN components and security solutions

![Diagram of wireless LAN components and security solutions](image)
Virtual private network technology provides a security-enhanced mechanism for authenticating users and encrypting the information that flows on the network. VPN technology can also be used to protect wireless LANs. With the VPN solution, the wireless LAN network, including access points and their Ethernet backbone, is implemented as a separate network outside the company firewall. The wireless LAN network may be physically inside the company premises but it is logically outside the company firewall, and all traffic from the wireless LAN has to pass through the firewall or through a VPN gateway to reach the company intranet.

If there are multiple physically separated locations, there may also be a need to deploy multiple VPN gateways so that the gateways do not become traffic bottlenecks. This may increase the network infrastructure costs—and this is one of the reasons why IT managers are often looking into 802.1x standard-based solutions for enterprise wireless LAN deployments.

A VPN solution is considered by many to be more secure than the 802.1x-based solution. There is also one more additional benefit on the VPN based wireless LAN security solution: users always have the same user interface and method of logging into the intranet, regardless of whether they are connecting to the office wireless LAN, working from home, working at a public wireless LAN hotspot or connecting through a wireless wide area network connection.
Secure access and roaming between wireless local and wide area networks.

Highlights

In summary, VPN technology can be used to provide security features to wireless LANs and to outside corporate communication consistently and uniformly. There are multiple types of VPNs. Although many feel that the industry standard IPsec provides the best VPN functionality, that may not always be the case. For example, IPsec has no “knowledge” of the roaming characteristics that may have been implemented. Because of this, it may interfere with network access during certain sessions. Before implementing any mobile VPN solution, it is crucial to make sure that all the desired features will be supported. Most importantly, any VPN should include a strong encryption mechanism, such as triple Data Encryption Standard (DES).

Personal firewalls and virus protection

While 802.1x and VPNs protect the information that is being transmitted across the air interface, they do not protect the end user’s device itself. For example, a hacker could obtain the IP address of an end user’s computer and gain access to it through an IP connection. This would be outside of what the VPN or 802.1x can control. The unauthorized user could gain access to the computer and its data files, or could install worms or other viruses. Also, the users themselves could jeopardize the security of their computers by unknowingly accepting viruses, especially in e-mail messages.

These problems are not unique to wireless LANs, but are endemic to all forms of communication between computers. However, 802.1x and VPNs do not negate the need for either personal firewalls or virus software. In wired and wireless LANs alike, both of these features should be included in a security-rich design and implementation of the end user’s device.
Wireless wide area networks

Outside the reach of the enterprise wireless LAN, and where public wireless LAN hotspots are not available, the 2.5G and future 3G and 4G wireless wide area networks can fulfill the mobile data communication needs. The 2.5 networks are currently being deployed worldwide, and 3G and 4G networks are expected to be commercially available in a few years.

While wireless LANs have become more prevalent and provide the first choice of wireless connectivity for many, their short range and the currently limited availability of public wireless LAN hotspots means large gaps in coverage, even in metropolitan areas. Wireless wide area networks such as CDMA, GPRS and future UMTS can fill these gaps by providing similar levels of service, although at slower speeds. As time moves on, wireless wide area networks are expected to increase their speeds and provide a more complementary solution to the wireless LAN. Nonetheless, even at today’s speeds (see Table 1), wireless WANs can play a role in providing mobile data for the users that need it “on the road.”

Table 1

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Technology</th>
<th>Initial Speed</th>
<th>Timeframe</th>
<th>Geographies</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDPD</td>
<td>Cellular Digital Packet Data</td>
<td>19.2 kbps</td>
<td>Now</td>
<td>NA</td>
</tr>
<tr>
<td>GPRS</td>
<td>General Packet Radio Services</td>
<td>20–56 kbps (114 kbps max)</td>
<td>Now</td>
<td>EMEA, AP, NA</td>
</tr>
<tr>
<td>iDEN</td>
<td>Integrated Digital Enhanced Network</td>
<td>64 kbps</td>
<td>Now</td>
<td>NA</td>
</tr>
<tr>
<td>CDMA 1XRTT</td>
<td>Code-Division Multiple Access 1XRTT</td>
<td>144 kbps (307 kbps max)</td>
<td>2002</td>
<td>NA, some AP</td>
</tr>
<tr>
<td>CDMA2000 1xEVDO</td>
<td>CDMA2000 1xEV-DO</td>
<td>2 Mbps max</td>
<td>2003</td>
<td>NA, some AP</td>
</tr>
<tr>
<td>UMTS</td>
<td>Universal Mobile Telecommunications Service</td>
<td>384 kbps (2 Mbps max)</td>
<td>2003</td>
<td>AP, EMEA</td>
</tr>
<tr>
<td>UWB</td>
<td>Ultra Wideband Network</td>
<td>1–10 Mbps</td>
<td>2003–2004</td>
<td>NA</td>
</tr>
</tbody>
</table>
Secure access and roaming between wireless local and wide area networks.

For more information, please see the IBM White Paper, “Exploiting the full opportunity of 2.5 and 3G networks,” IBM Corporation, October 2001 (G580-3852-00).

**Seamless roaming**

Each computer or device on the company intranet or on the Internet has a unique IP address that is used in all communications with that device. IP addresses are divided into two parts: the first part identifies the network to which the device belongs, and the second part is its unique address within that network. When the current IP addressing schema was created, the computers were stationary. Because the IP address identifies the network to which a computer belongs, a user cannot move his computer or device to another network or subnetwork without renewing the IP address. When he changes his IP address, the user loses his existing session and his communication partner is no longer able to find him.

To provide an uninterrupted and seamless roaming experience between networks—be they wired networks such as Ethernet or ADSL, wireless LAN or wireless WAN—some kind of roaming solution is needed.

---

**Highlights**

The current IP addressing schema assumed that computers would remain stationary, and was not designed to accommodate the connectivity needs of mobile users.
In this paper, we define “seamless roaming” as the ability to maintain the current state of an end-user session unchanged, even if the mobile device changes its physical network connection and moves between IP networks on an enterprise intranet or moves to any type of wireless or wired IP network outside the enterprise firewall. Without the seamless roaming capability, users would:

- Lose their sessions when moving between IP subnetworks, wired Ethernet and wireless LAN or wireless WAN, or moving between wireless LAN hotspots
- Need to restart applications after roaming from one type of network to another
- Obtain and present a new IP address to their applications every time they reconnected
- Need to reestablish their VPN connections
- Potentially lose data when roaming from one network to another
- Lose time in reestablishing connections when moving out of range of current connections.

There are different types of wireless roaming solutions available on the market, and more are in development. In this paper, we focus on two roaming solutions: Mobile IP and the WebSphere Everyplace Connection Manager from IBM.

Please note that, even if a seamless roaming solution can keep the end user’s session alive when he roams from one network to another, it does not remove the need for the end user to be authenticated to the network that he is roaming into. That is, if a user roams from the enterprise Ethernet into the enterprise wireless LAN with 802.1x-based security, he will still need to log on to the wireless LAN network.
Similarly, if the user roams from a wireless WAN to a public wireless LAN, he will need to log on to the public wireless LAN. This is done either by using a user id and password or through SIM card-based authentication. In public wireless LANs that use SIM-based authentication, the logon can be automated. Whenever the device comes to the coverage area of a public wireless LAN and the user wants to communicate, the access point and access controller can read the SIM information and authenticate the device.

The statements above are based on the assumption that all communications adapters are concurrently active. If users need to stop and start communications adapters or remove and insert PC cards, their organizations should be looking to install a utility program that allows configuration changes on the fly. One good example of such a utility program is IBM Access Connections, which ships with IBM ThinkPad® notebook computers. It allows users to dynamically change their communications configuration with a point-and-click.

Note also that the seamless roaming capability does raise some security issues, as the mobile devices will then work as a conduit into the company intranet, as discussed later in this paper.

**Mobile IP**

Mobile IP is an emerging standard from the Internet Engineering Task Force (IETF). While originally conceived to support CDMA networks, it can be applied to any wireless network provided that adequate hardware support is available. Today, vendors such as Cisco Systems, ipUnplugged, Nokia and Lucent Technologies have announced or demonstrated Mobile IP-based roaming solutions. Mobile IP requires upgrades to the network infrastructure.
In general, on an IP network, packets are transported from their source to their destination by routers that forward data packets from incoming network interfaces to outbound network interfaces according to information obtained via routing protocols. The routing information is stored in routing tables.

Mobile IP is an enhancement to the IP routing infrastructure that provides forwarding of traffic to mobile users. It uses what are referred to as “agents” in the user’s home network and in all foreign networks that support Mobile IP. When the users move to remote networks, the Mobile IP client in their mobile devices—called the mobile node (MN)—registers its presence with the foreign agent (FA) in this “visited” network. The foreign agent signals the presence of a mobile node back to its home agent (HA), and from there on, the home agent “knows” to forward the data packets to the mobile device via the foreign agent in the remote network.

The basic entities constituting a Mobile IP-aware network are:

- **Mobile Node (MN)**—Mobile IP client code in the mobile device that has an IP address, such as a notebook computer or a handheld device.
- **Foreign Agent (FA)**—A piece of microcode, typically in the router on a visited network. The foreign agent will work as a proxy to the visiting mobile node and will forward and receive data packets from its home agent or from its corresponding node.
- **Home Agent (HA)**—Another piece of microcode in the router on the user’s home network. The home agent converses with the foreign agents and routes the data packets according to the mobile node’s then-current location.
- **Correspondent Node (CN)**—Any computer outside the user’s home network with which the mobile node is corresponding. The home and foreign agents will handle the routing of data packets between the mobile node and the correspondent node.
Foreign agents are distributed around the network in the visited networks to provide roaming capability. The home agent sits in the home network and acts as a coordinator between the mobile nodes, foreign agents and correspondent nodes.

Every mobile node is allocated a home address in its home network. Every time the mobile node moves, it is required to register as a guest with a foreign agent in the visited network. It will be given a “care-of” address that it communicates to its home agent.
Highlights

Mobile IP reverse tunneling
Figure 4 shows the Mobile IP network elements, but it does not illustrate how the agents manage the mobile user's session. Basically, routing tunnels are set up between foreign agents and the home agent to support data traffic from the mobile node to and from the home network and to correspondent nodes external to the home network.

![Mobile IP reverse tunneling diagram](image)

The most common approach to managing the mobile user’s session is reverse (two-way) tunneling.

The most common approach is reverse or two-way tunneling. This is not the only option, but it is the most practical when dealing with enterprise users as in most cases when the computer or an application with which the mobile node needs to communicate resides on the home network. With reverse tunneling, the home agent will encapsulate packets bound to its mobile nodes and then route them appropriately to the foreign agent of the network where the mobile node is visiting. The home IP address of the mobile node is contained within the routed message. When the foreign agent receives the packet, it recognizes that it is a Mobile IP packet bound to a visiting mobile node. The foreign agent strips the routing information and forwards the message on to the mobile node using its temporary care-of address within the visited network.
Secure access and roaming between wireless local and wide area networks.

### Highlights

Reverse tunneling does not encrypt data packets, so a VPN solution is still required with Mobile IP to ensure data privacy and security.

Control and ownership of the interconnected networks in a Mobile IP solution will depend in part on the placement of the home and foreign agents.

The reverse takes place for messages originating from the mobile node, where the foreign agent encapsulates the message and forwards it to the home agent for further routing. Note that this is not message encapsulation and tunneling like that which takes place with a VPN. Data packets in the Mobile IP tunnels are not encrypted; the tunneling is only used to route the data packets between agents. A VPN solution needs to be added on top of the Mobile IP solution to provide data privacy and security.

**Placement of foreign and home agents in a Mobile IP solution**

Where the home and foreign agents are placed makes a significant difference in who controls and owns the interconnected networks and how they are managed and maintained. It also has a significant impact on the traffic in the network.

Ideally, the home agent would be placed into the user’s “home network,” which—in the case of an enterprise—would mean placing it into the company intranet, inside the company firewall. The home agent would then be able to facilitate roaming to mobile nodes within the boundaries of the intranet—assuming that the routers in all subnetworks have foreign agents.

While Mobile IP is fairly straightforward to implement inside the enterprise intranet—requiring only a router upgrade to support it—implementations that cross the enterprise firewall and moreover would provide seamless roaming across the firewall, are more difficult to put in place.

There are some techniques that allow firewall traversal for Mobile IP, so that the mobile node could reside outside in the public network and be communicating with correspondent nodes that are inside the private intranet. For this to work, the mobile node would have to negotiate access through the firewall and to construct a protected tunnel into its home network. This technique allows the mobile node to maintain its “virtual home address” outside the firewall—even though its physical IP address has changed.
Without going into the technical details—and challenges—of this solution, it should be noted that this type of Mobile IP implementation would be owned and controlled by the enterprise. The enterprise owns the home agent and mobile nodes, and just uses the service provider’s network to access the home network.

To place home agents and foreign agents into separate networks owned by different service providers and companies would present multiple security challenges. Opening up the company intranet for public view is not an option. The organization would have to have a separate “cloud of interconnected Mobile IP networks” that is isolated from its intranet with a firewall.

To set up a Mobile IP solution that spans multiple networks that are owned by different parties would require bilateral agreements, shared authentication and shared network management between network owners. This would be an administrative and contractual challenge. The question is, where would this kind of solution be needed?

One likely scenario for Mobile IP implementation is that a service provider could offer it to provide seamless roaming between wireless networks, e.g., between a wireless WAN (CDMA, GPRS or 3G) and a public wireless LAN.

In this type of solution, the foreign agents would reside on the service provider’s CDMA, GPRS or 3G networks and on the public wireless LAN networks. Foreign agents in these networks regularly broadcast agent advertisements. When the visiting mobile node receives the advertisement, it can see the foreign agent’s IP address and thus it can request a care-of address for itself. Once it has received an address, it will tell its home agent its new care-of address.

Where home and foreign agents are placed has security ramifications, and raises administrative and contractual challenges as well.

Service providers may be able to offer seamless roaming between wireless networks, which could ease shared-ownership issues.
If the home agent is placed into the service provider’s network, it is the service provider that controls the address space and provides routing services to mobile nodes. The service provider would then have to have a protected VPN tunnel to “pipe” the sessions to its enterprise customer. This solution works between the service provider’s wireless networks, but it does not provide seamless roaming between the intranet and the outside networks.

To add that capability, either mobile nodes would need to be able to use VPN to “tunnel out” from the intranet to the home agent at the service provider network, or the enterprise wireless LANs would need to be placed outside the company firewall and foreign agents installed into these networks. The challenge with both configurations is that all traffic would be routed out to the home agent in the service provider’s network—and should the corresponding node be in the intranet, as is likely with enterprise applications, the traffic would have to flow back again to the VPN gateway (or firewall) on the edge of the enterprise network.

Although this solution would work, it would be a wasteful use of trunk line capacity and the trunk, the home agent and the VPN gateway may become a bottleneck.

If the service provider offered this type of Mobile IP roaming solution, it would only work within its own network until other service providers had implemented Mobile IP and made bilateral agreements for shared authentication and network management. User cross-authentication and billing would become a formidable task in such a solution.
IBM WebSphere Everyplace Connection Manager

IBM is fully committed to international standards, and IBM Networking Services helps its enterprise and service provider customers to implement Mobile IP in their networks. However, IBM also provides another seamless roaming solution to its customers. This solution allows mobile users to roam inside the company intranet from subnet to subnet and to roam from the intranet to the public Internet or any other IP network, and back again.

The IBM WebSphere Everyplace Connection Manager allows mobile devices, such as Microsoft® Windows® workstations and PocketPCs to roam seamlessly between any wired and wireless networks. No modifications are needed to the networks. The solution can be installed at the enterprise, or a service provider can use it to provide seamless roaming to its customers. The IBM WebSphere Everyplace Connection Manager supports a variety of communications protocols and networks, as can be seen in Table 2.

Table 2—WebSphere Everyplace Connection Manager supported networks

<table>
<thead>
<tr>
<th>Cellular Networks:</th>
<th>LAN Connections:</th>
<th>Public Packet-Radio Networks:</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDMA</td>
<td>Wireless LAN—802.11 Ethernet Token Ring</td>
<td>GPRS (GSM Worldwide)</td>
</tr>
<tr>
<td>AMPS &amp; N-AMPS</td>
<td></td>
<td>CDPD and CS-CDPD</td>
</tr>
<tr>
<td>GSM</td>
<td></td>
<td>DataTAC 4000 (US)</td>
</tr>
<tr>
<td>iDEN</td>
<td></td>
<td>DataTAC 5000 (Europe)</td>
</tr>
<tr>
<td>PCS 1900</td>
<td></td>
<td>Modacom (Germany)</td>
</tr>
<tr>
<td>PDC (Japan)</td>
<td></td>
<td>DataTAC 6000 (Asia)</td>
</tr>
<tr>
<td>PHS (Japan)</td>
<td></td>
<td>DataTAC/IP</td>
</tr>
<tr>
<td>TDMA</td>
<td></td>
<td>Mobitex (Worldwide)</td>
</tr>
<tr>
<td>TDMA</td>
<td></td>
<td>Mobitex/IP (US)</td>
</tr>
<tr>
<td>SMS-C Connections:</td>
<td>Internet Connections:</td>
<td>PDC-Packet (Japan)</td>
</tr>
<tr>
<td>SMPP</td>
<td>Cable Modem</td>
<td></td>
</tr>
<tr>
<td>SMTP</td>
<td>DSL</td>
<td></td>
</tr>
<tr>
<td>SNPP</td>
<td>ISDN</td>
<td></td>
</tr>
<tr>
<td>UCP</td>
<td>ISP</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dial Connections:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DIAL/TCP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ISDN</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PPP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PSTN (POTS)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Secure access and roaming between wireless local and wide area networks.

Client devices can have one or more communications adapters of any type indicated in Table 2. For example, an IBM ThinkPad notebook computer may have a built-in Ethernet adapter, a built-in dial-up modem, a built-in wireless LAN adapter and a CDMA network card in its Personal Computer Memory Card International Association (PCMCIA) slot. The IBM WebSphere Everyplace Connection Client code in the ThinkPad notebook computer, together with the gateway at the user’s home network, manages the connectivity through the different physical networks. They establish and control the IP session. For the user and for applications, the IP session appears seamless even though the underlying physical network may be changed at will.

In the example shown in Figure 6 (see next page), the client device has three physical network adapters: wired Ethernet, wireless LAN (802.11b), and wireless WAN (CDMA 1x). Each communications adapter is configured to the operating system and is operational. The communications adapters themselves may not be active, depending on user selection and whether or not the adapter is connected to the network or the network coverage is available to the adapter.

The IBM WebSphere Everyplace Connection Manager adds a fourth element—a virtual device driver—to the system. It is this device driver that the applications are in communications with at any given time.

To see how this works, let’s study an example. A user starts his session while connected to the wired Ethernet network in his office or cubicle. Moving to a conference room to attend a team meeting, the user disconnects the Ethernet cable and loses his connection to the network. The wireless LAN connection, which was active but not in session with the user’s applications, then becomes the new preferred network connection for the mobile device. This would all be controlled by the IBM WebSphere Everyplace Connection Client. Because the IBM WebSphere Everyplace Connection Client provides a virtual device driver to the applications, the user would not lose his session even though the physical network connection changed.
Furthermore, the user could then leave the building and the CDMA network would then provide the connectivity after the wireless LAN adapter had lost its signal. Again, the IBM WebSphere Everyplace Connection Manager would take control and seamlessly make the transition. The application would not be “aware” that the physical network had changed again. However, as the network speed changed from high-speed wireless LAN to lower-speed WAN, the user would most likely notice somewhat longer response times.

In more technical terms (see Figure 6), applications interface with the TCP/IP communications stack (1), but rather than interfacing with the network device drivers, the TCP/IP communications stack interfaces with (2) the special device driver provided with the WebSphere Everyplace Connection Client. The IBM WebSphere Everyplace Connection Manager device driver is a virtual device driver that interfaces with the “real” device drivers (3) that support different communications adapters (4).
Secure access and roaming between wireless local and wide area networks.

Highlights

With the IBM WebSphere Everyplace Connection Manager, users can control in which order to use the communications adapters. There is also an optional application programming interface (API) that allows applications to determine the state of the virtual and physical connections and to control the switching of the communications adapters.

In addition to providing virtually seamless roaming, the IBM WebSphere Everyplace Connection Manager also helps reduce data transmission costs over wireless wide area networks. It is designed to provide efficient data compression and optimize session transport for IP-based wireless networks, including 2.5G and 3G networks. It also helps enable optimized IP transport over non-IP wireless packet networks. This functionality helps improve speed, enhance the reliability of wireless communication and improve the end-user experience.

The reliability of the IBM WebSphere Everyplace Connection Manager can be improved further through gateway clustering, and gateways can be distributed across multiple sites, to scale with the customer’s needs. The IBM WebSphere Everyplace Connection Manager supports High Availability Cluster Multiprocessing (HACMP) to provide around-the-clock availability and reliability.

Security with WebSphere Everyplace Connection Manager

The IBM WebSphere Everyplace Connection Manager is designed to provide not only virtually seamless roaming between communications networks, but also enhanced security. It provides strong authentication, and supports RSA Secure ID authentication. Customers can choose from an extensive cryptographic library, which includes DES, Triple DES, RC5 and AES (later in 2002), to provide end-to-end encryption of all data between the mobile device and the intranet network.
Security considerations while roaming

There are a number of security considerations that need to be addressed in roaming solutions. Networks have different levels of security. Very few companies today implement access control or encryption in their in-building Ethernet networks. Physical control over access into the building is considered to be a sufficient security measure. Encryption of data in the Ethernet networks can be done, but it would dramatically increase the cost of the networks. On the other hand—even if the risk of inside attacks is always there—a properly designed, managed and monitored switched Ethernet network offers fewer opportunities for eavesdropping. One of the key security rules, obviously, is that all the active network components be kept in locked wiring cabinets.

As discussed earlier, companies are implementing 802.1x-based security solutions for wireless LANs inside the corporate premises because, in several cases, it becomes cheaper than installing a VPN solution.

Let’s take another look at the example we used before. A user is inside the company premises, starts a session while connected to the Ethernet, stops the connection, unplugs the Ethernet cable and starts using the wireless LAN with 802.1x-based security. In the Ethernet, there was neither authentication nor encryption. With 802.1x-secured wireless LAN, the access point does not let the user in until he has entered his credentials, i.e., his user id and password. Once the user has been authenticated, he is let into the network and his session data is encrypted using the WEP key.

Both Mobile IP and IBM WebSphere Everyplace Connection Manager solutions are able to handle this roaming scenario as the security is managed below the IP protocol stack by the supplicant code and by the wireless LAN access point.
Secure access and roaming between wireless local and wide area networks.

Highlights

It starts getting more difficult when users want to roam from within the enterprise to the Internet or to other outside networks. There they need to cross the enterprise’s protective firewall, change the IP address space and activate VPN tunneling. This is a tall order for the Mobile IP solution.

**IBM WebSphere Everyplace Connection Manager provides seamless roaming over the enterprise firewall**

IBM WebSphere Everyplace Connection Manager can do this. It is designed to provide security-rich, virtually seamless roaming between IP subnets within the enterprise intranet, and it allows users to seamlessly roam from inside the company intranet to the public Internet and back.

Mobile users who spend most of their time outside the company premises and only infrequently come to the office can start and leave their WebSphere Everyplace Connection Client permanently on, or they can set it to auto-start with their system. When they are outside the company premises, mobile users can select any available means of connectivity to the Internet and the WebSphere Everyplace Connection Client safeguards the connection, provides traffic optimization and allows virtually seamless roaming between different networks.

When the user comes inside company premises, he maintains his IP session when he connects to the wireless LAN or to the Ethernet. Obviously, with the 802.1x-secured wireless LAN, the user first needs to sign on to the network. This can be done transparently by utilizing the inherent API service built into the WebSphere Everyplace Connection Client.
In the example above (see Figure 7), all traffic, whether from outside or inside the company firewall, is routed to the IBM WebSphere Everyplace Connection Manager at the edge of the enterprise intranet. This is not the most efficient use of the network, as the sessions from 802.1x-secured wireless LANs and wired LANs inside the company intranet would need to first exit the intranet to reach the WebSphere Everyplace Connection Manager. However, with this solution the user would always have the same method and user interface to connect to the network regardless of whether they are in the office, working remotely from home or on the road.

*With IBM WebSphere Everyplace Connection Manager, users have a consistent method and interface for connecting to the network, whether they are at home, in the office or on the road.*
In the seamless roaming scenario depicted above, the IBM WebSphere Everyplace Connection Manager maintains a persistent session regardless of changes in the mode of connection and the underlying network infrastructure. This also means that there is a persistent VPN connection from the device to the company intranet. Because the mobile device is now always connected to the enterprise intranet, appropriate security measures must be implemented at the device level to prevent unauthorized access to the enterprise intranet.

To prevent looping out of and back into the company intranet, the user would just have to switch off the IBM WebSphere Everyplace Connection Client and then he would be reconnected directly to the intranet. Obviously switching off and on the WebSphere Everyplace Connection Client would disrupt the sessions.

If the user spends most of his time inside the company premises, he should not start the WebSphere Everyplace Connection Client, but should instead use a direct connection to the wireless LAN or to the Ethernet.

Summary

Wireless LANs are quickly becoming the favorite choice for enterprise and consumer connectivity, including use in homes, businesses and in public places.

While IEEE 802.11b—”Wi-Fi”—is the predominant standard in wireless LAN solutions, increasing pressure for more throughput and less interference is providing a market for a new standard, IEEE 802.11a. This standard delivers up to five times the throughput of the current Wi-Fi standard, and less interference with other networks and devices.
Security in wireless LANs is a serious issue. Every company should be aware of it and take appropriate measures to secure their wireless LAN networks. Unfortunately, some organizations are unaware of how best to implement wireless LAN security and this has led to some widely published security exposures.

Security features of wireless LANs can be enhanced with a good design, well-planned installation, high-quality products and an appropriate network management system.

IBM Networking Services is one of the world’s largest enterprise network builders, specialized in designing and implementing security-rich, industrial-strength networks. IBM Networking Services can help customers design and deploy security-enhanced and manageable wireless LAN networks.

Today more than ever, users are seeing a need for more than one method of communication. IBM ThinkPad notebook computers have multiple communications capabilities built into the devices, thus allowing multiple simultaneous communications to take place.

Roaming between networks is emerging as one of the basic tenets of connectivity. Roaming solutions give users an environment where switching the underlying network infrastructure, or temporary network outages, do not disrupt their application sessions. To users, the connectivity appears seamless; they can move from one location to another and from one network to another while maintaining their sessions.

Current standards treat mobility and security as separate issues. The standards are not well synchronized to support an ideal connectivity solution. Organizations need to plan ahead and configure their networks for optimal use based on the characteristics of their user base.
As time moves forward, we expect to see more interplay from the standards bodies between these two areas. In the meantime, the IBM WebSphere Everyplace Connection Manager is designed to provide a solution for the enterprises and service providers that need seamless, security-rich, robust and scalable roaming capability in wireless networks.

About the authors

Christopher C. Couper

Christopher (Chris) Couper, IT Architect, is responsible for the worldwide development of wireless e-business solutions. Mr. Couper joined IBM in 1982 as a Systems Engineer specializing in communications and peer-oriented computing. Mr. Couper has extensive knowledge and experience in communications product development and deployment of wireless and LAN-based products. Mr. Couper is the recipient of a number of significant intellectual property awards within IBM for communications. Mr. Couper has extensive experience in the field deploying various communications solutions as well as supporting business and operational support systems (BSS and OSS) to enterprises as well as telecommunications companies worldwide. Mr. Couper is an IBM Certified IT Architect and a member of the IBM Americas Architect Board. Mr. Couper is also a member of the prestigious IBM Academy of Technology. Mr. Couper is currently working in the IBM Wireless e-business Solutions organization in White Plains, NY.
Jyrki Korkki

Jyrki (Jeri) Korkki, global solution manager, is responsible for the worldwide wireless e-business services development for IBM Networking Services. Mr. Korkki joined IBM in 1972 as a telecommunications engineer with practical experience in early cellular telephone system design and military aviation communications. In addition to having 30 years of networking experience, he was also the technical lead for the task force that created the IBM internal e-business architecture. Drawing on the extensive knowledge gained from that assignment and working in the capacity of senior consultant to IBM customers, Mr. Korkki has contributed to multiple large e-business transformation engagements. Mr. Korkki also helps develop and teach courses on networking and wireless solutions. After starting his career in his native Finland, Mr. Korkki worked in multiple IBM locations, including the IBM La Gaude research facility in France, several U.S. locations and the IBM EMEA (Europe/Middle East/Africa) education facility in La Hulpe, Belgium. Mr. Korkki currently is based in the IBM European headquarters in Paris, France.
Examples worldwide include American Airlines Admiral Clubs, Starbucks Coffee stores, and multiple U.S. and European airports.

“3G” is short for third-generation wireless network. 3G personal and business wireless technology is expected to become available between the years 2003 and 2005. The third generation, as its name suggests, follows the first and second generation (2G) in wireless communications. The 1G period began in the late 1970s and lasted through the 1980s. The present mobile voice networks are second-generation networks that are now being updated for higher-speed mobile data. These new mobile data networks are called 2.5G networks.

As is the case with the Ethernet, each wireless LAN adapter and access point has a unique MAC address allocated to it and “burned” into its hardware at the time of manufacturing.

IPsec—Internet Protocol Security—is a developing standard for security at the network or packet-processing layer of the communications network. IPsec is especially useful for implementing virtual private networks and remote user access control to intranet networks.

DES—Data Encryption Standard—is a widely used method of data encryption using a private (secret) key. It has been judged so difficult to break by the U.S. government that it has been restricted for exportation to other countries. DES originated at IBM in 1977 and has been adopted by the U.S. Department of Defense.

“4G” is short for fourth-generation wireless network, and refers to new broadband mobile communications networks that are expected to follow the still non-existent 3G network. The major distinction of 4G over 3G networks is increased data transmission rates: the 4G network data rates are expected to reach 20–40 Mbps.

A subnet—short for subnetwork—is a small, separately identifiable part of the company’s intranet. Typically, a subnet contains computers at one geographic location, in one building, or in a local area network. By dividing its intranet into subnets, a company can connect to the Internet with a single shared network address. Without “subnetting” its intranet, the company could get multiple connections to the Internet, one for each of its physically separate subnetworks, but this would also require an unnecessary use of network numbers that the Internet would have to assign. It would also require that Internet routing tables on gateways outside the company would need to know about and have to manage routing that could and should be handled within a company.

API—application programming interface—is a specific method by which a programmer writing an application program can make requests to IBM WebSphere Everyplace Connection Manager.

RC5 is a fast block cipher designed by Ronald Rivest for RSA Data Security (now RSA Security) in 1994. It is a parameterized algorithm with a variable block size, a variable key size, and a variable number of rounds.

AES—Advanced Encryption Standard—is an encryption algorithm for securing sensitive but unclassified material by U.S. government agencies and, as a likely consequence, may eventually become the de facto encryption standard for commercial transactions in the private sector.