IBM Pervasive Computing
February 2003

Enhancing General Packet Radio Service Performance with IBM WebSphere Everyplace Connection Manager

Arshad Bahl, Marketing Manager, IBM Pervasive Computing Systems

Pierre Secondo, IBM STSM, Mobile e-business, Europe

Alexandre Signoret, Sales Specialist for telecom, IBM WebSphere

Executive Summary

Today, many mobile telephone providers have successfully deployed General Packet Radio Service (GPRS) networks for their customers. Business enterprises are also considering GPRS networks as a viable wireless extension to their own data networks. Service providers and enterprise IT departments are forming strategic partnerships that deliver a robust wireless network based on GPRS.

This white paper was written with the IBM Business Partners (such as a Service Provider) in mind who provide wireless solutions to their enterprise customers. The paper describes how GPRS performance can be significantly enhanced for enterprises, through the use of the *IBM WebSphere Everyplace Connection Manager (WECM)*.

IBM's WECM addresses these issues that are on the top of the mind of current GPRS users – total cost of ownership, security, performance, and session management. Additionally, real-life scenarios and test results are used to illustrate the cost savings gained by deploying IBM WECM. Although the tests are conducted on a GPRS network, the results apply to all 2.5G and 3G networks.

Using WECM's compression functions, 2.5G and 3G network service providers can now transmit data more efficiently, thereby freeing up the limited bandwidth for additional value-added services.

In addition to WWANs, wireless Local Area Networks (hotspots) deployment has been significant and continues at a dramatic rate. Enterprises are now starting to implement wireless LANs as a convenient network access method within their offices and campuses, leading to lower infrastructure deployment costs. Additionally, public space hotels, airports, convention centers and even restaurants are putting in wireless LAN hotspots for their customers to use while they visit their properties.

The total coverage gained by having the WWANs and wireless LANs coverage now paints a very compelling wireless story for enterprises who want to ensure always-on coverage. IBM's WECM allows seamless roaming to users switching between wireless LAN hotspots and the WWANs.

IBM has been conducting GPRS connectivity and performance testing in most European countries with GPRS availability. Various WECM testing configurations were exercised and specific GPRS services, such as Cegetel's Internet mobile service (IMS), were tested. A variety of wireless devices, including laptops, PDAs, and telephones have been used. All performance measurements were conducted using a laptop loaded with the WECM Wireless Client.

These tests were conducted on an SFR GPRS network. SFR is a partner in the Vodafone group, deploying GPRS services throughout Europe. This paper highlights the findings and the implications of the test results.

Wireless Wide Area Networks

Wireless Wide Area Networks (WWANs) consist of technologies such as Cellular Digital Packet Data (CDPD), GPRS, and Universal Mobile Telecommunications Service (UMTS). *Table 1* lists the key technologies, geographies, and deployment timeframes.

Acronym	Technology	Initial Speed	Initial Geographies
CDPD	Cellular Digital Packet Data	19.2 kbps	NA
GPRS	General Packet Radio Service	56 kbps (114 kbps max)	EMEA, AP
IDEN	Integrated Digital Enhanced Network	64 kbps	NA
CDMA 1XRTT	Code Division Multiple Access 1XRTT	144 kbps (307 kbps max)	NA, some AP
CDMA2000 1xEVDO	CDMA2000 1xEV-DO	2 Mbps	NA, some AP
UMTS	Universal Mobile Telecommunications Service	384 kbps (2 Mbps max)	AP, EMEA
UWB	Ultra Wideband Network	1-10 Mbps	NA

Table 1 - Wireless WAN Technology - Protocols

General Packet Radio Service (GPRS)

For Global System for Mobile communication (GSM) operators, the first key step on the road to 3G is the deployment of *GPRS*, the 2.5G technology that introduces non-voice packet switching to the GSM network. The GPRS infrastructure is essentially an extension of a GSM network, offering data rates of up to 115 kbps by providing a means to aggregate radio channels for higher data bandwidth, with initial user data rates of typically 40-50 kbps. GPRS facilitates the introduction of several new applications that have not previously been available over GSM networks due to the limitations in the speed of circuit switched data (at 9.6 kbps). GPRS overlays a packet-based air interface on the existing circuit-switched GSM network. GSM operators need only add a few new infrastructure nodes and upgrade software in some existing network elements.

GPRS is also designed for deployment on mobile networks based on the IS-136 TDMA standard, popular in North and South America. TDMA operators (such as AT&T Wireless and Cingular Wireless in the USA) are in the process of moving to GSM/GPRS in their migration to providing 2.5G and 3G services.

See Appendix A for additional network details.

Wireless Local Area Networks

In the past few years, the proliferation of Wireless Local Area Networks has increased dramatically. Wireless LAN applications include those used by end users, enterprises, public wireless LANs inside enterprises, and public wireless LANs in public places (such as hotspots in cafés). Enterprises are now starting to implement WLANs as a convenient network access method within their offices and campuses. WLANs allow companies to lower their infrastructure costs, saving on cabling in new, to-be-expanded, and to-be-renovated buildings.

The Toronto Police Service, deploying IBM WECM in their police cruisers, has created WLAN "hotspots" at numerous locations in Toronto where the officers can drive up and replicate data-intensive files. When they are away from these hotspots, they are still able to access data over the WWAN networks.

In the public space, hotels, airports, convention centers, and even restaurants are providing wireless LAN hotspots for their customers[1]. Service providers are studying this market as a new revenue channel for existing GPRS customers. Combining GPRS and Wi-fi seamless roaming allows mobile road warriors or business professionals' constant access to high-speed data access while away from the traditional office.

Security with WWANs and WLANs

Security in Wireless LANs and Wireless WANs is more demanding than in traditional wired local area networks. Wireless LANs use radio waves, which are not limited to the physical boundaries of an enterprise. For example, drivers on a public thoroughfare adjacent to a Wireless LAN installation could receive its signals. Appropriate security measures have to be put in place to secure wireless LAN installations. Authentication, or the authorization of a wireless LAN system, is a prerequisite. Enterprise WLANs are extending the corporate Intranet wirelessly and therefore security is paramount. In public wireless LANs, access and authorization is enforced to insure that the user pays for network access.

[1] Examples include American Airlines' Admiral Clubs, Starbucks Coffee, and the Singapore Airport

Virtual Private Network (VPN) technology provides a highly-secure mechanism for authenticating users and encrypting information on a network -- wireless or wireline. For example, a mobile employee with a dialup modem or Ethernet connection between a hotel room and a local Internet Service Provider (ISP) can use VPN to securely access the company intranet. Encrypted data insures that sensitive information won't fall into the wrong hands. VPN technology provides security to wireless networks and external corporate communications consistently and uniformly.

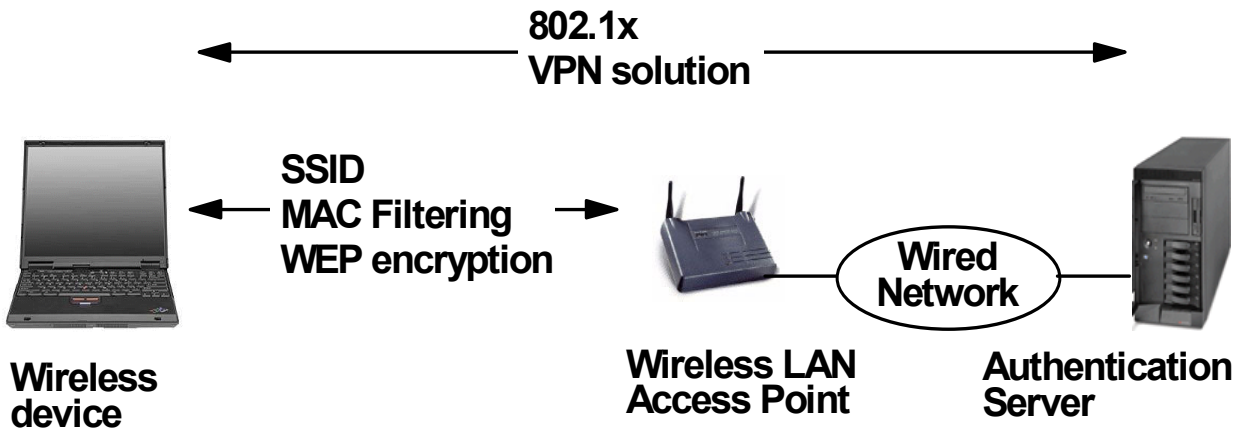

Figure 1: IBM WebSphere Everyplace Connection Manager provides the ability to connect to a company Intranet from various locations with seamless roaming

Wireless, Cross-Network Roaming

Wireless, seamless, cross-network roaming solution allows the end-user to maintain session even when the mobile device changes its network connection from an IP sub-network on an enterprise intranet to any type of wireless network outside the enterprise firewall *(see Figure 1)*.

Without seamless roaming, a mobile user would:

- Lose the session when moving between a wireless LAN sub-network, wireless LAN, or wireless WAN network (such as GPRS), or between wireless LAN hotspots (such as enterprises Wi-Fi)
- Need to restart applications after roaming from one type of network to another
- Obtain and present a new IP address to applications whenever reconnecting
- Need to re-establish a VPN connection
- Potentially lose data when roaming from one network to another

- Lose time in re-establishing connections when moving out-of-range of current connections

The growth of GPRS and WLANs will enable the mobile employee to stay connected virtually anywhere and move seamlessly from one network to the other. *(Another IBM white paper[2] provides details on secure access and cross-network roaming).*

Enterprise Expectations

Enterprise IT managers are concened about:

- Data flow performance and delivery
- Security and privacy of their networks
- User comfort and overall performance of a new network

It is critical that data privacy be guaranteed. GPRS privacy must also be compatible with existing enterprise IT security schemes. IT providers and mobile operators must address the security challenge together to ensure confidence in their end-to-end secured wireless solutions.

Enterprises also want their WWANs and WLANs to provide a familiar user experience that is like existing wired networks. Until now, most existing IT applications were designed for high-speed LANs; GPRS transmission rates didn't provide the performance of wired modems. That made access to some applications impractical over WWANs such as GPRS. For example, accessing an intranet home page or a custom database designed for a high-speed intranet can be tedious at a lower transmission rate. Enterprises were specifically seeking an ability to dynamically compress the GPRS data flow.

Enterprises also want robust, stable, end-to-end connections, despite the conditions that generally characterize radio connections with mobile devices.

Since GPRS may not be accessible in all locations, wireless LANs can fill coverage gaps for the mobile enterprise employee. It is critical that applications work seamlessly across the WWANs, WLANs and wired networks so that mobile workers can chose the best one available – with the right mix of price and function -- whether they are using ADSL at home, GPRS on the road, or WLANs in hotels.

Data flow on a wireless network is not considered as stable as on a wired network. IT infrastructures must provide tools to handle connectivity challenges, assuring a consistent user experience over time.

---

[2] "Secure Access and Roaming Between Wireless Local and Wide Area Networks" by Jyrki Korkki and Christopher Couper.

IBM WebSphere Everyplace Connection Manager

IBM has developed a solution that addresses the need for enterprises and service providers interested in giving their employees and customers secure connectivity to critical applications. *IBM WebSphere Everyplace Connection Manager (WECM)* provides industry-leading security, data flow optimization, and improved session stability over wired and wireless networks. IBM WECM also provides seamless cross-network roaming, allowing mobile users to switch between wired networks, WLANs and WWANs without having to restart their applications *(see Figure 2)*

IBM WECM enables enterprises to extend their existing applications to mobile workers using a variety of handheld and mobile computers. It allows the mobile professional to connect over a wide range of wireline and wireless networks, offering the broadest choice of cost and coverage options. WECM's architecture shields applications and application developers from the unique idiosyncrasies of wireless networks. WECM employs compression and optimization techniques to compensate for the high latency and low bandwidth typically seen on today's networks. It also allows the transport of IP data over non-IP wireless infrastructures.

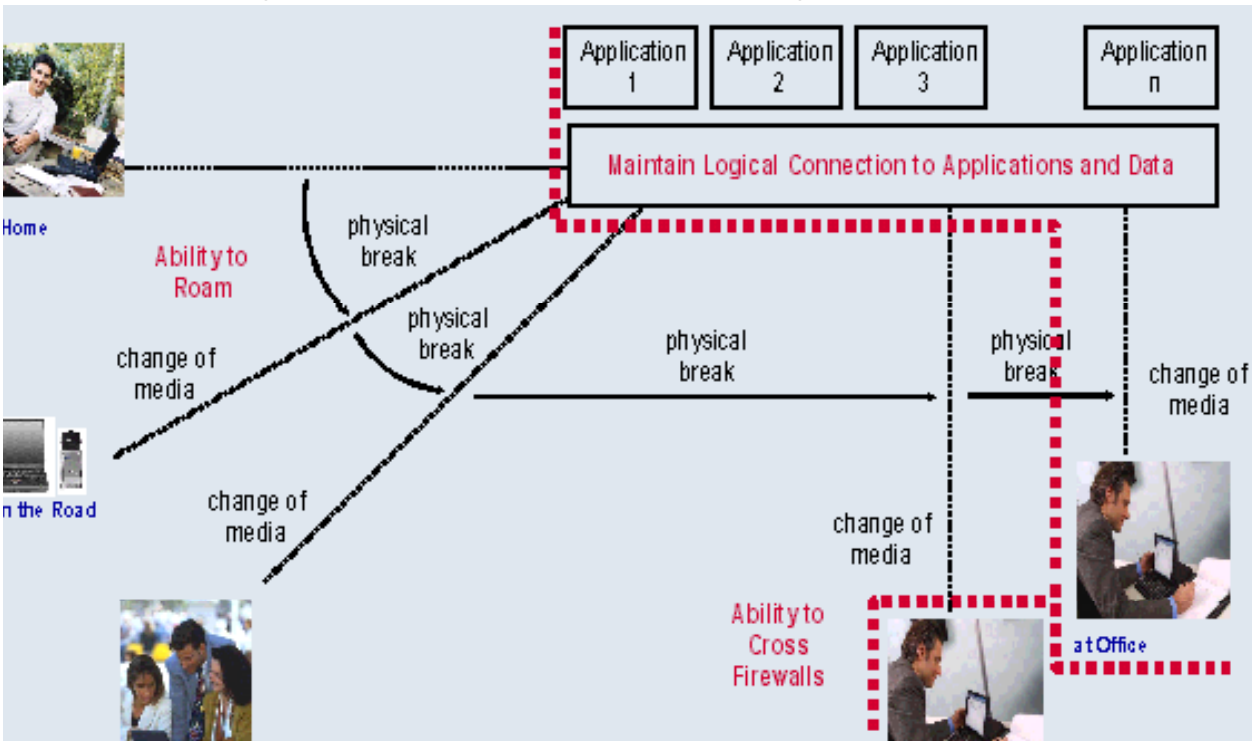

Figure 2: Seamless, Cross-Networking Roaming with IBM

A mobile professional can use WECM to access business applications and retrieve critical customer information while travelling. Cellular networks can be used in addition to 802.11 wireless LANs in hotels, airports, and other public spaces. WECM supports dynamic switching between IP-based connections such as 802.11 and GPRS or CDPD.

A comprehensive range of network protocols have been tested with WECM v4.2. In addition to public network access, WECM also provides support for private radio networks. This allows it to be used by a wide variety of customers who have special security needs such as public safety and law enforcement. WECM also supports secure data access by both WAP and non-WAP clients over a wide range of international wireless network technologies, as well as LAN and WAN wireline networks.

WECM is an ideal solution for mobile service providers, since it enables wireless access from WAP-enabled devices and can handle SMS messages. WECM is highly scalable to accommodate large numbers of subscribers. It employs strong encryption technology to ensure data through public networks is protected. Its recently-added seamless roaming

capability allows service providers to gain a competitive advantage by adding value-added services and entering the new "hotspot" marketplace.

WECM provides the ability to send application-generated alerts and notifications to devices capable of receiving SMS messages, SMTP e-mail messages or pagers. It provides a rich, well-documented API that separates message generation from message delivery. Applications do not need to format messages for specific networks or devices. Data generated by an application is simply sent through an API with the required delivery information; the messaging service formats and delivers each message. This provides maximum flexibility in delivering messages across the broadest set of networks and devices -- without writing or re-writing applications.

Figure 3 illustrates WECM's end-to-end capabilities.

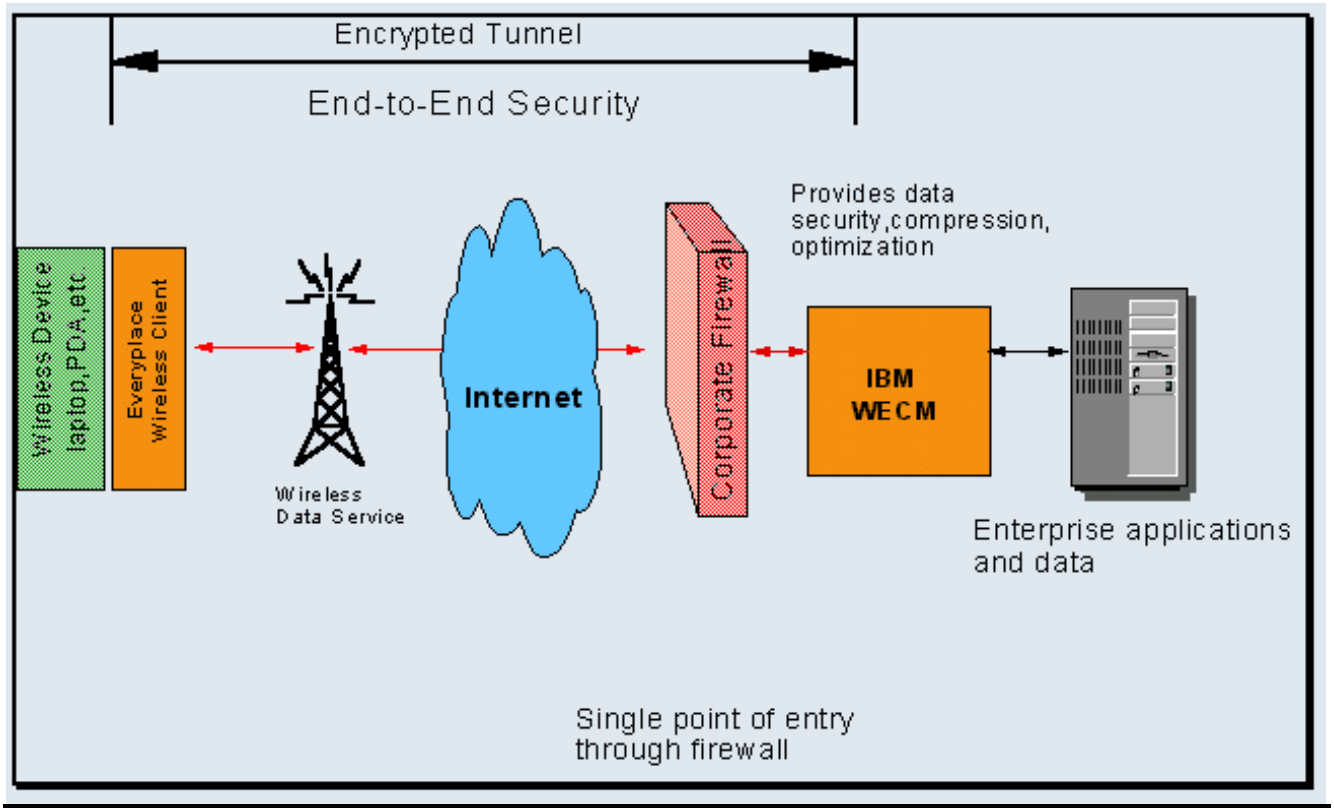

Figure 3: WECM's End-to-End Security

The three main components of IBM WECM are its *Gateway, Gatekeeper,* and Mobility *Client*.

Gateway

IBM WECM Gateway provides a TCP/IP interface to wireless and wired networks. It integrates all supported networks within a single host and can connect radio networks to any wireline network. Mobile devices can link to the same wireless gateway and use the same applications, regardless of the radio network used. Users with various application requirements dependent upon transmission costs, coverage areas, or available devices can select the best network for their needs.

The *Remote Access Gateway* uses the Wireless Client to extend IP applications to mobile devices over a variety of international wireless and wireline networks. It not only extends enterprise networks to a mobile workforce; it also enables carriers and service providers to offer IP applications to their customers over wireless networks.

Gatekeeper

The WECM Wireless Gatekeeper provides a Java technology-based administrator console, which serves as an easy-to-use administrative interface. It enables the remote definition and configuration of wireless gateways, registers users and mobile devices, and performs routine administrative tasks. Data is stored in the Lightweight Directory Access Protocol (LDAP) format.

This component can also be used to configure WECM as a messaging gateway by supporting the delivery and receipt of short messages to and from client devices.

Mobility Client

IBM Wireless Mobility Client software runs locally on mobile devices, providing a full-function interface to communicate with WECM. It offers enhanced functionality, improved performance, and security-rich operations.

WECM gives service providers a set of tools that can improve and increase customer relationship management (CRM). It is capable of

- Providing secure, two-way user authentication and data encryption
- Improving network response times
- Reducing data overload with data compression and header reduction
- Maintaining and restoring dial-up connections automatically

WECM Key Value Propositions

Data Optimization

WECM reduces data transmission costs over wireless networks by providing efficient data compression, connectivity management, and optimal session transport for IP-based wireless networks, including 2.5G and 3G. WECM also optimizes IP transport over non-IP wireless packet networks, leading to improved speed, reliability, and user interaction.

Data optimization can be described as four basic techniques:

- The first technique *compresses* data before IP packets are sent. The size of each packet is reduced without any impact on its contents. Compression increases the data rate of wireless networks and decreases the data transmitted, thereby potentially reducing transmission costs.
- The second technique works for TCP traffic by *reducing* the 40-byte TCP headers to an average of 3 to 5 bytes. This decreases the data transmitted over a wireless network.
- The third technique *optimizes* TCP retransmissions. TCP communications over wireless links often cause packet retransmissions because of the high latency and small bandwidth available.
- A final technique, known as *short hold mode* reduces air time on connection-oriented wireless networks and PSTNs. With short hold mode enabled, there is no physical connection over the mobile network, but there is a virtual one. If the wireless client or wireless gateway attempts to transmit an IP packet, one of these components re-establishes the connection and starts the transmission immediately. As a result, this technique can lower connection fees.

Security and privacy of networks

WECM has several ways to enforce the security of networks, applications, and data. Remote access gateways and wireless clients work together to establish secure communications between them by using two-way *authentication* and *data encryption*.

- *Authentication* is the process of allowing users at each end of a communications link to establish identities with each other. Authentication is required to encrypt the communication link between a remote access gateway and wireless client. The basic mechanism for authentication is the mutual presentation of a secret key, a process

known as *bi-directional authentication*. In addition to this two-party key distribution, a remote access gateway can use third-party RADIUS servers. Remote access gateway and wireless clients authenticate each other without sending passwords over the air.

- *Encryption* is the process of converting data using a secret code, so it can remain private until decrypted. Because the communication link might not be private, data should be encrypted before sent. Encryption helps prevent unauthorized access to data by transforming it into an unintelligible form, so that the original data cannot be obtained without a decrypting process. Remote access gateways encrypt data using the session key exchanged during authentication. This process double-encrypts traffic between a wireless client and the remote access gateway.

The wireless client can choose from among several forms of encryption. All are known as strong "symmetric key" encryption algorithms:

- *Digital Encryption Standard (DES)* is a block cipher that has been a commercial encryption standard in the USA for many years.
- *RC5* is an alternative to DES and is a block cipher proprietary to RSA Data Security, Inc.
- *Triple-DES* is a block cipher that executes DES three times. This is the strongest type of encryption supported by the wireless client.
- *Advanced Encryption Standards (AES)*
- *FIPS140-2* compliance to meet the most stringent U.S. Government security standards

Session Persistence

WECM supports dynamic roaming across physical networks without breaking application sessions, enabling mobile users on Windows workstations or PocketPCs to roam seamlessly between multiple wired or wireless networks offered by multiple service providers. No modifications are needed to the service providers' networks. The solution can be installed at an enterprise or service provider to provide seamless roaming for employees or customers. WECM supports a variety of communications protocols and networks, as shown in Appendix A.

Cellular Networks:	LAN Connections:	Public Packet-Radio Networks:
CDMA	Wireless LAN -802.11	GPRS (GSM Worldwide)
AMPS & N-AMPS	Ethernet	CDPD and CS-CDPD
GSM	Token Ring	DataTAC 4000 (US)
iDEN		DataTAC 5000 (Europe)
PCS 1900	Internet Connections:	Modacom (Germany)
PDC (Japan)	Cable Modem	DataTAC 6000 (Asia)
PHS (Japan)	DSL	DataTAC/IP
TDMA	ISDN	Mobitex (Worldwide)
	ISP	Mobitex/IP (US)
SMS-C Connections:	Dial Connections:	PDC-Packet (Japan)
SMPP	DIAL/TCP	
SMTP	ISDN	
SNPP	PPP	
UCP	PSTN (POTS)	
		Packet Satellite Network:
		Norcom

Table 1: WECM-supported networks and connection types

Multiple Network Choices

An extensive selection of global wireless and wireline network technologies are accessible by WECM, including cellular networks, public packet-radio networks, Internet connections, dial-up connections, private packet networks, satellite networks, and LAN connections. WECM is hardware, vendor, and media independent. *(See Table 1)*

Scalable and Reliable

WECM supports gateway clustering, and can distribute across multiple sites, to scale with mobile needs. In addition, it uses High Availability Cluster Multiprocessing (HACMP) to provide 24x7 reliability.

WECM over GPRS: Performance Testing

In partnership with various European telecom operators and major enterprises, IBM conducted testing of WECM over a GPRS network. Various testing configurations were exercised and specific GPRS services such as Cegetel's Internet Mobile Service (IMS) were tested. Also, several devices including laptops, PDAs and mobile phones were tested. However, all performance measurements were run on a laptop loaded with the WECM Wireless Client.

The tests presented here were conducted on an SFR GPRS Network. SFR is a partner of the Vodafone group, a provider of GPRS service throughout Europe.

Test Configuration

The configuration shown in *Figure 4* has been used to test a variety of files including text, Web pages, log files, dump files, etc. For the test, the WECM client ran on an IBM ThinkPad (model T23), equipped with a Nokia D211 PCMCIA GPRS card for access of the GPRS network.

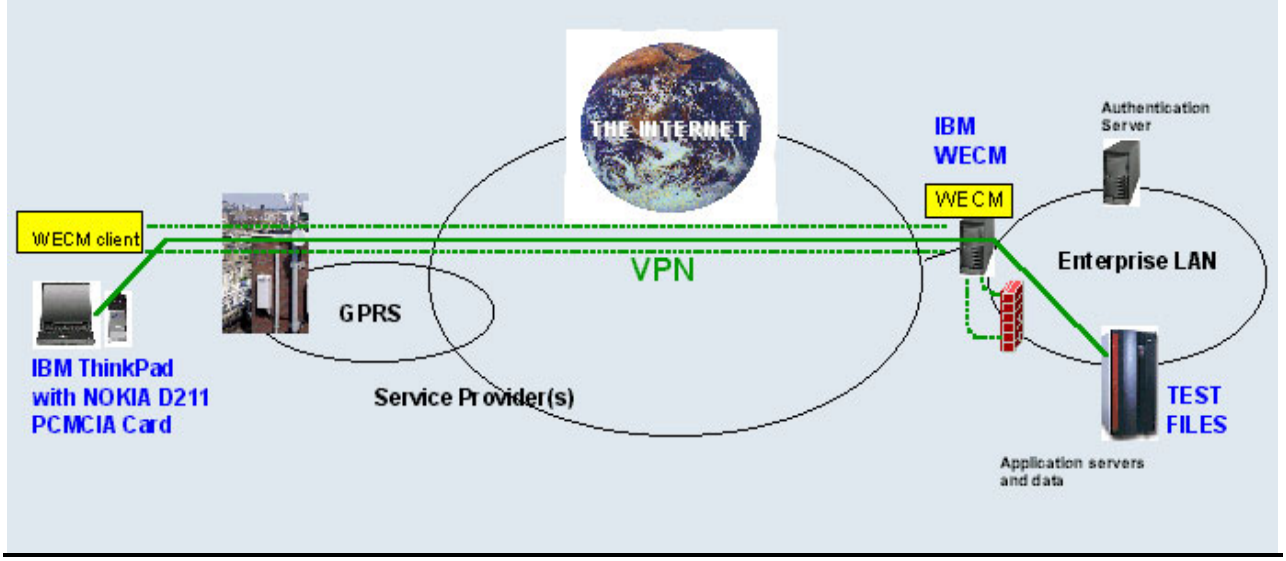

Figure 4: Test Configuration

The tests were run with the following WECM security and compression options:

- Triple DES encryption
- Standard WECM compression

The tests consisted of downloading (FTP or HTT) files from a server to the terminal, of various types and sizes *(S),* while measuring the size of the file sent over the air *(s)*, and the transfer time *(t)* to compute the observed throughput.

- FTP Get a 14,142 byte application small log file
- FTP Get a 291,324 byte application medium size Log file
- FTP Get a 972,931 byte System DB Log file
- FTP Get a 77,165 byte Configuration file
- FTP Get a 2,660,206 byte System Log file
- HTTP Get a 340,646 byte HTML file

(Content from http://performance.toast.net: "medium compression")

Results and Implications

Size of the File in server memory (S) in bytes	Size of the File transmitted over the GPRS network. (s)	Performance Enhancement	Experienced throughput In Kbps/s
14,142	4,525	312%	45.12
291,324	119,443	244%	54.23
972,931	318,018	306%	60.64
77,165	32,190	240%	44.24
2,660,206	948,266	280%	55.28

Table 2: Test Results

Based on the test results in *Table 2*, the three key implications are:

- VPN operations using IBM WECM result in gain (ratio of S/s) ranging from 2.4 to 3 for most of the transferred file types. This translates to a reduction of the transmitted volume and generally in GPRS, a reduction of the transmission cost by a factor of 240% to 300%. For example, assume an enterprise with 200 mobile workers each transmitting 1 Mb of data per day assuming a minimum cost of $4 per MB. This means a yearly cost to the enterprise of around $160,000. If we apply an average gain of 270% by using WECM, the resulting cost for the enterprise would drop to around $60,000, realizing an annual saving of $100,000
- Data throughput, and therefore the response time, are dramatically improved. On average, the test throughput was 49 Kbps, compared to the real network throughput of 15 to 20 Kbps (over 100% gain in throughput).
- As a result of the security and compression benefits, the tests demonstrated a very high VPN resiliancy, permitting a better session stability when on the move. Data sessions are significantly less disruptive when using WECM to run instant messaging, heavy file downloads, and Web transactions -- even in a full mobility environment.

WECM Deployment Scenarios

Several potential case scenarios are possible when deploying WECM, enabling enterprises and mobile operators to find the best-fitted solution in terms of costs, security, responsibility, deployment time and maintenance type.

A - WECM within Enterprise Premises

In the following scenario, a service provider provided a communication channel using IBM WECM VPN, for end-to-end security. This model makes the enterprise 100%-independent from the operator's network in terms of security and management. The enterprise can choose from multiple telecom suppliers with no impact on the mobile application.

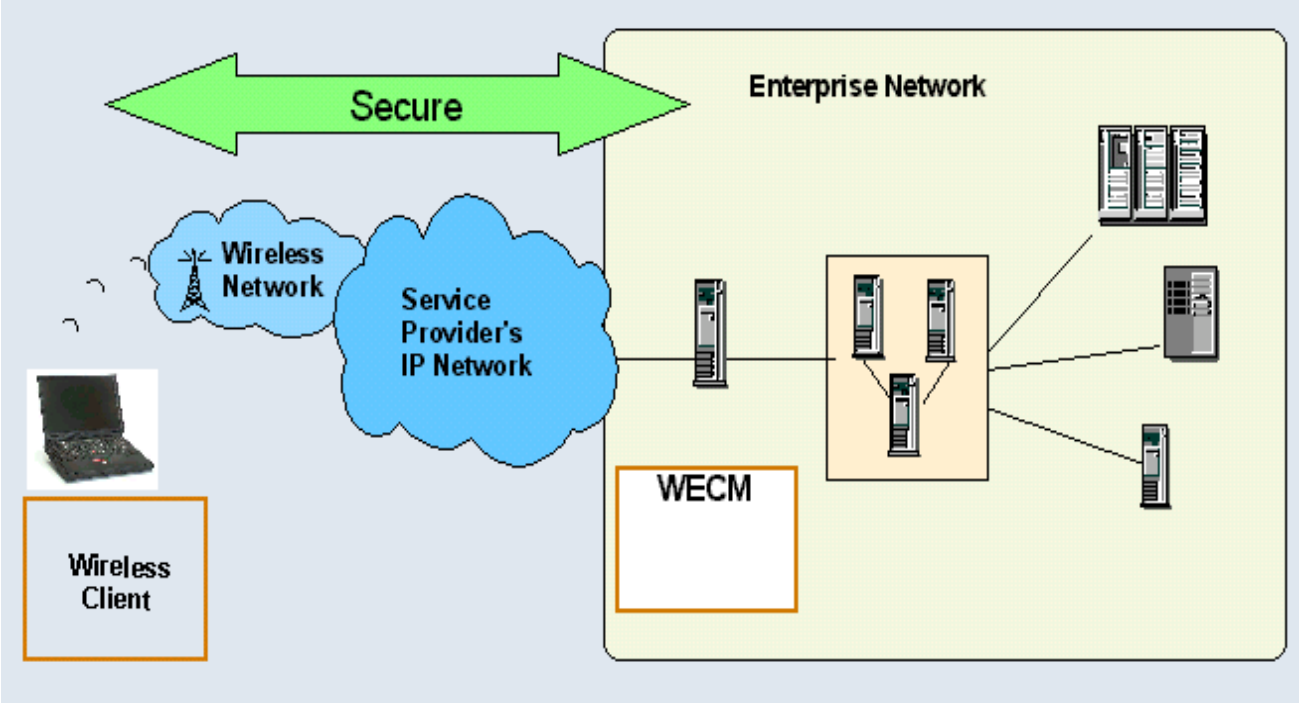

Figure 5: WECM in the Enterprise (Case "A")

User scenario example

"I was a speaker at a conference held at a resort a few hours away. My trip to the conference was via trains and taxi. My laptop had a GPRS card and the IBM WECM Client installed. I was running late, so when my taxi arrived, I grabbed my laptop and headed out the door, without shutting down the work I was doing. I simply disconnected from the WLAN I was on and plugged in my GPRS card. In the taxi, I connected to a

GPRS network and continued to download my presentation and synchronize my e-mail while enroute to the train station.

“Since it was a large file, the download continued while I was on the train, and I was also able to use Lotus Notes Sametime and communicate with my technical team on some last-minute details. Entering a long tunnel, I lost GPRS coverage, but WECM, using its session persistance feature, kept the session alive. Leaving the tunnel, the replication continued without having to log back on.

“The high security level (triple DES and AES) provided by WECM conforms to my company’s security policy, so I can securely gain access to the company intranet and also access my personal bank account.

“As I reached the resort, I realized that it was equipped with a WLAN, and I found it more data efficient to switch over to its higher bandwidth capability. Later, my speech went well, although I did get a tricky question from the audience. I delayed my answer until the end of the speech, contacting a specialist using instant messaging to get an immediate answer.”

B - WECM Hosted at a Service Provider

In this case, the service provider hosts WECM and security is insured by two concatenated secure pipes. A key benefit is that the operator can provide on-the-fly services depending of the type of data. However, this configuration may not satisfy some customers because of the secure channel break at the service provider premises.

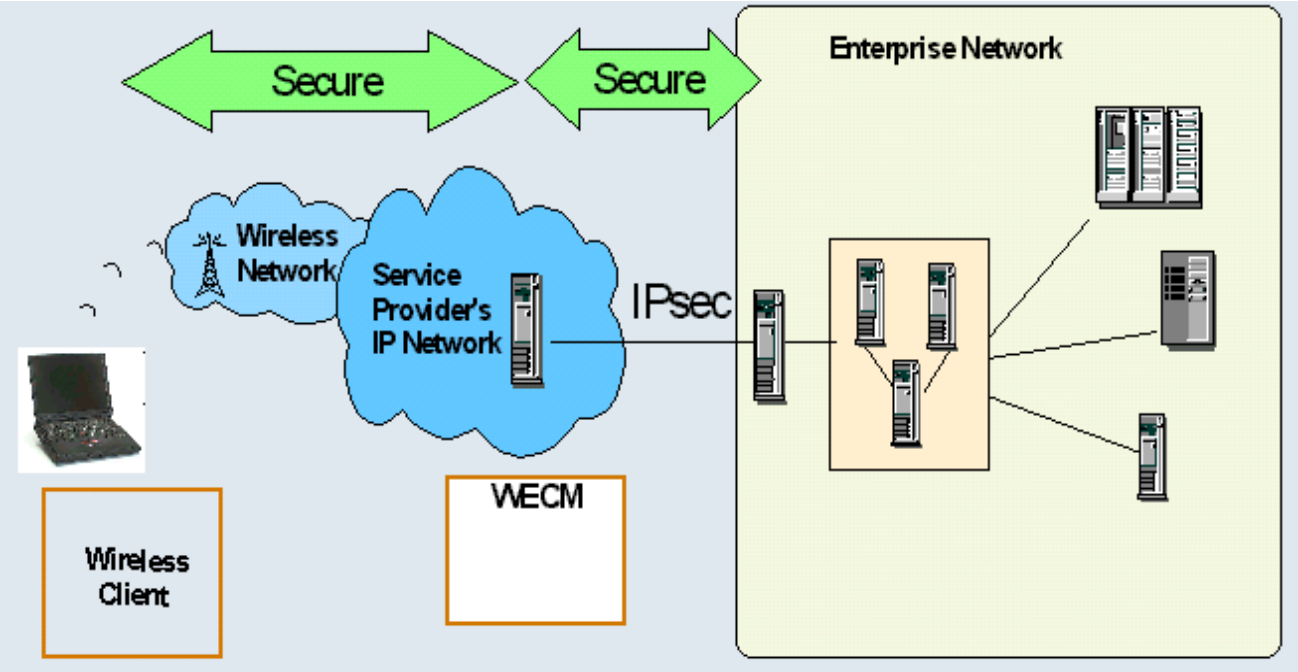

Figure 6: WECM Hosted at the Service Provider (Case "B")

C - WECM at Service Provider with End-to-end Security

Here, the service provider is hosting a WECM "Principal Node", and each customer is hosting a WECM "Subordinate Node". The security is insured by single end-to-end secure pipes for each customer. Key benefits are:

- Each customer enterprise is granted data confidentiality
- The service provider can insure central management of the Subordinate WECM
- The service provider can offer enterprise VPN service via a single shared WECM

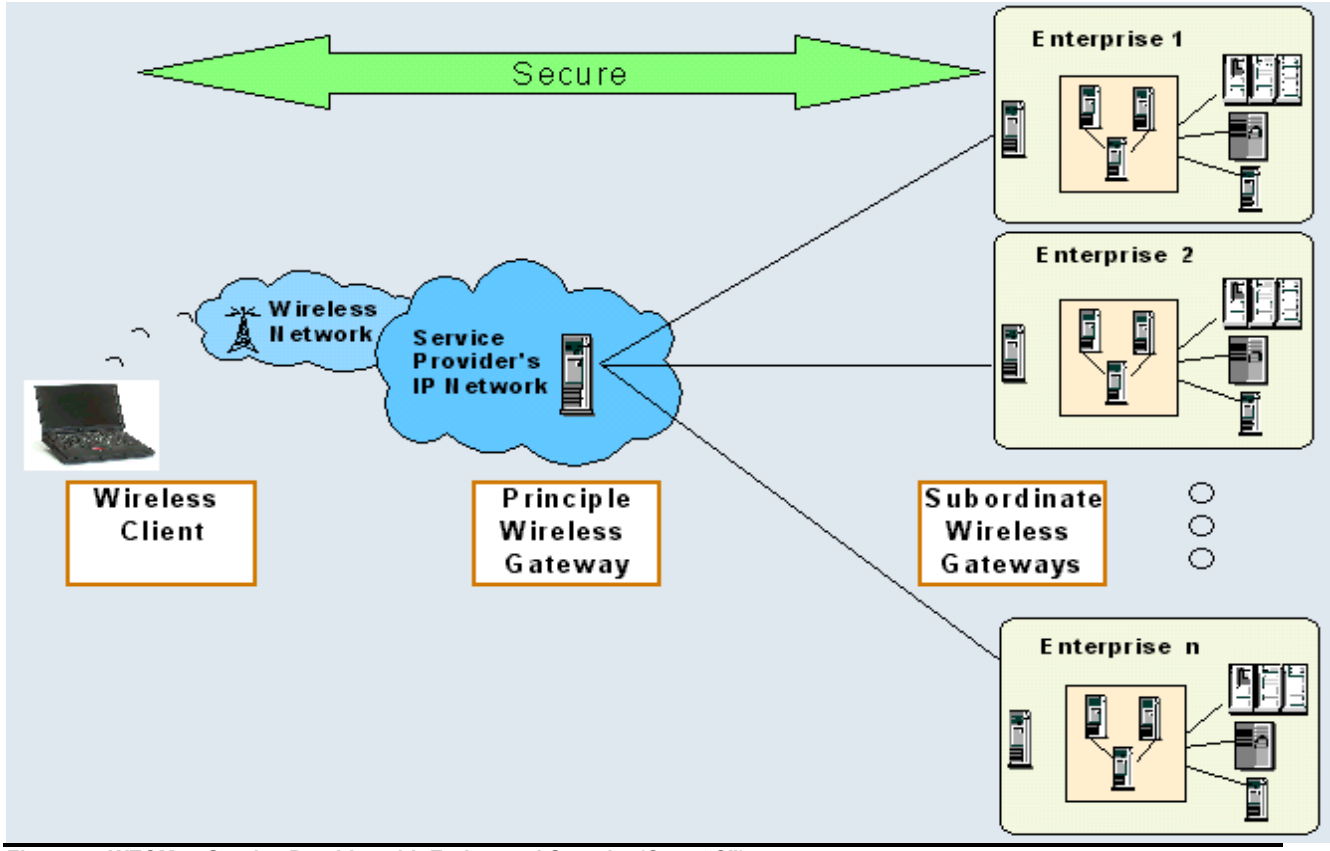

Figure 7: WECM at Service Provider with End-to-end Security (Case "C")

Summary

In this paper we have shown how IBM WECM and Wireless Client software can enhance the GPRS services offered by mobile service providers. These enhancements are required by enterprises for running mobile office applications. Key features that enterprises are looking for and provided by WECM include - end to end security and privacy, data flow optimization, reductions in transmission costs, data session persistence, and an overall improvement of the mobile enterprise user experience.

Moreover, WECM provides seamless network roaming and deployment flexibility, that both service providers and enterprises can take advantage of to further enhance and optimize e-business applications.

Appendix A

Cellular Digital Packet Data (CDPD)

CDPD is a wireless packet data network, and, as its name implies, sends packets of data over dedicated channels as an overlay on the existing AMPS cellular network at speeds up to 19.2 kbps. CDPD infrastructure was first deployed in 1995. Three IBM employees originally filed CDPD patents in 1991. IBM and the wireless carriers developed the initial CDPD specifications. CDPD was originally designed to utilize channel capacity not being used for voice transmission, but has evolved to using dedicated channels for more consistent performance. CDPD is available in some locations internationally, but its main deployment is in the USA, where coverage varies (about 50 percent of the population) and is concentrated around approximately 100 cities. CDPD provides native TCP/IP support, facilitating integration of third party applications.

CDMA2000 1xEVDO

Evolution beyond 2.5G to 3G within 1xRTT includes *CDMA2000 1xEV* (EVolution) that further increases packet data rates in the CDMA 1.25 MHz channel or carrier.

Beyond CDMA2000 1xRTT lies *CDMA2000 3xRTT*, or *3xMC* (multi-carrier), so named because it uses three 1.25 MHz channels (plus guard bands) for 5 MHz of bandwidth, with speeds of up to 2 Mbps. CDMA2000 3xRTT is currently being worked on in the standards bodies and may be approved for implementation in the 2003 to 2005 timeframe.

Universal Mobile Telecommunications Service (UMTS)

The European Telecommunications Standard Institute (ETSI) choose *UMTS* to define the 3G system when positioned in the 2.1 GHz band, used in Europe and other parts of the world where these frequencies are available. By providing broadband, packet-based transmission of text, digitized voice, video, and multimedia, UMTS allows many more applications to be introduced to a worldwide base of users and provides the vital link between today's GSM systems and IMT–2000. UMTS increases transmission speeds to 2 Mbps per mobile user and establishes a global roaming standard. Once UTMS is fully implemented, computer and phone users can be continually attached to the Internet and have the same set of roaming capabilities wherever they travel. Until then, users can have multi-mode devices that switch to the currently available technology (such as GSM 900 and 1800) where UMTS is not yet available. UMTS is being developed by the Third-Generation Partnership Project (3GPP), a joint venture of several standards-developing organizations around the world.

Ultra Wideband (UWB) Network

Ultra Wideband radio is a revolutionary wireless technology for transmitting digital data over a wide spectrum of frequency bands using very low power. It can transmit data at very high rates for wireless local area network applications. UWB technology is currently being studied and commercial products are still in the future, but UWB communication devices could be used to wirelessly distribute services such as phone, cable, and computer networking throughout a building or home. They could also be used by police, fire, and rescue personnel to provide covert, secure communications.

Credits and Resources

Special thanks to
- Christophe Boulangé, IBM wireless e-business architect for telecommunication
- Nicolas Poujardieu, EMEA PVC Technical Sales, EWG Specialist.

Find out more about IBM WebSphere Everyplace Connection Manager and IBM WebSphere Everyplace Access at:

Ibm.com/pvc

Learn about short-messaging support provided by the IBM WebSphere Everyplace Connection Manager in "IBM WebSphere Everyplace Connection Manager: Short-messaging support in the WebSphere Everyplace Suite" (WebSphere Developer Domain, April 2001)

Tour the developerWorks Wireless zone for more resources.

References

Rigney, C., et al. April 1997. *Remote Authentication Dial In User Service (RADIUS)*. The Internet Engineering Task Force. Internet. 22 April 2002.

WAP Forum. February 1999. *Wireless Application Protocol Wireless Transport Layer Security Specification11-February-1999* . WAP Forum. Internet. 22 April 2002.

Rivest, R. April 1992. *The MD5 Message-Digest Algorithm* . The Internet Engineering Task Force. Internet. 22 April 2002.

Jussi Rautpalo, Helsinki University of Technology : *GPRS Security – Secure Remote Connections over GPRS* Internet, 24 Nov. 2000.

Henry Welborn Software Engineer, IBM. *Secure for sure: Securing wireless communication with the IBM WebSphere Everyplace Connection Manager*. IBM internet,12 July 2002

Notices

This paper discusses strategy and plans which are subject to change because of IBM business and technical judgments.

All statements regarding IBM future direction or intent are subject to change or withdrawal without notice and represent goals and objectives only.

References in this publication to IBM products or services do not imply that IBM intends to make them available in any other countries.

Performance results obtained in other environments may vary significantly from your results. There is no guarantee that these measurements will be the same on your systems.

Trademarks

IBM, the IBM logo and WebSphere are trademarks of International Business Machines Corporation in the United States, other countries, or both.
Linux is a registered trademark of Linus Torvalds
Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.

IBM Corporation
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
02-14-03