Security-enhanced IBM solution for mobile enterprises and Service Providers
April 2003

WebSphere Everyplace Connection Manager: increasing mobile security, reducing wireless costs

Dennis Anderson
Fred Christensen
IBM Pervasive Computing

Contents

Executive summary

As companies expand mobile applications, key executives face a complex array of challenges. The number of WiFi hotspots, for example, is expected to quadruple by 2005 and a new generation of mobile devices is spurring rapid data usage. Gartner reports "that despite the falling prices for voice services, most enterprises deploying mobile applications in 2003 will find that the monthly costs for wireless data services and the total cost of ownership for their mobile solutions will exceed expectations by at least 30 percent. (0.7 probability)[1]"

To address these issues, IBM designed WebSphere Everyplace Connection Manager for optimizing bandwidth, reducing costs, ensuring security and roaming seamlessly across a wide range of networks. WebSphere Everyplace Connection Manager creates a mobile Virtual Private Network (VPN) that encrypts data, while optimizing performance and reducing transmission costs. The platform also integrates with an exhaustive range of Internet Protocol (IP) and non-IP networks, server hardware, device operating systems and mobile security options. This paper analyzes WebSphere Everyplace Connection Manager by focusing on advanced capabilities in:

- Cross network roaming, data compression and bandwidth optimization
- Mobile VPN, strong authentication and federal encryption certifications
- Secure mobile access via Secure Sockets Layer (SSL) and Wireless Transport Layer Security (WTLS) industry standards
- Push-based and two-way messaging for Wireless Access Protocol (WAP), Short Message Services (SMS), packet radio and paging networks
- Sensing, selecting and prioritizing network connections
- High Availability Cluster Multiprocessing (HACMP) and distributed administration

[1] Gartner, Five Steps to Contain Mobile Data Costs, by William Clark, February, 2003.

The WebSphere Everyplace Connection Manager solution allows mobile users to roam between virtually any wired or wireless network.

WebSphere Everyplace Connection Manager — an overview

Despite advances in wireless data networks, companies face mounting pressure to manage costs, coverage, and security for their mobile workforce. WebSphere Everyplace Connection Manager is designed to protect sensitive data, optimize network traffic, provide wireless messaging and enable seamless roaming. The technology is a distributed, scalable, multipurpose communications platform allowing a wide choice of wireless networks, server hardware, mobile devices, operating systems and industry standards.

From an architectural perspective, the WebSphere Everyplace Connection Manager platform is constructed of three components – Mobility Client, Connection Manager server and Distributed Administration. The net result is that users enjoy "always on" connectivity across divergent networks at lower cost and higher data rates. Key features include:

Feature	Advantage
Wireless network data optimization	• Improves data communication efficiency for VPN networking over wireless, reducing data volume and costly overhead
Authentication	• 2-party strong authentication verifies both server and client
Encryption	• Advanced Encryption Standard executes faster than 3DES
Cross-network roaming	• Mobile VPN and applications persist when switching networks
Thin client secure access options	• Supports phones and devices with no IBM client software via HTTPS and WTLS industry standards
SMS gateway and push services	• Same product configurable as full featured SMS gateway • Messaging SDK supporting :Java™, C, C++
Server integration	• Integrates with existing AAA via Radius support, directories via LDAP and ODBC databases
Reliability and scalability	• Server has 24x7 reliability with scalable, distributed design

WebSphere Everyplace Connection Manager also includes a wide variety of messaging and push features for WAP and Short Messaging Services, one-way and two-way paging, and messaging over packet radio networks. The platform is a mature fifth-generation software with load balancing cluster configurations, distributed management, hardware fail-over and support from the largest professional services group in the world.

Seamless roaming is the ability to maintain the current state and security of an end-user session, even if the mobile device changes networks.

Mobile persistence and secure network roaming

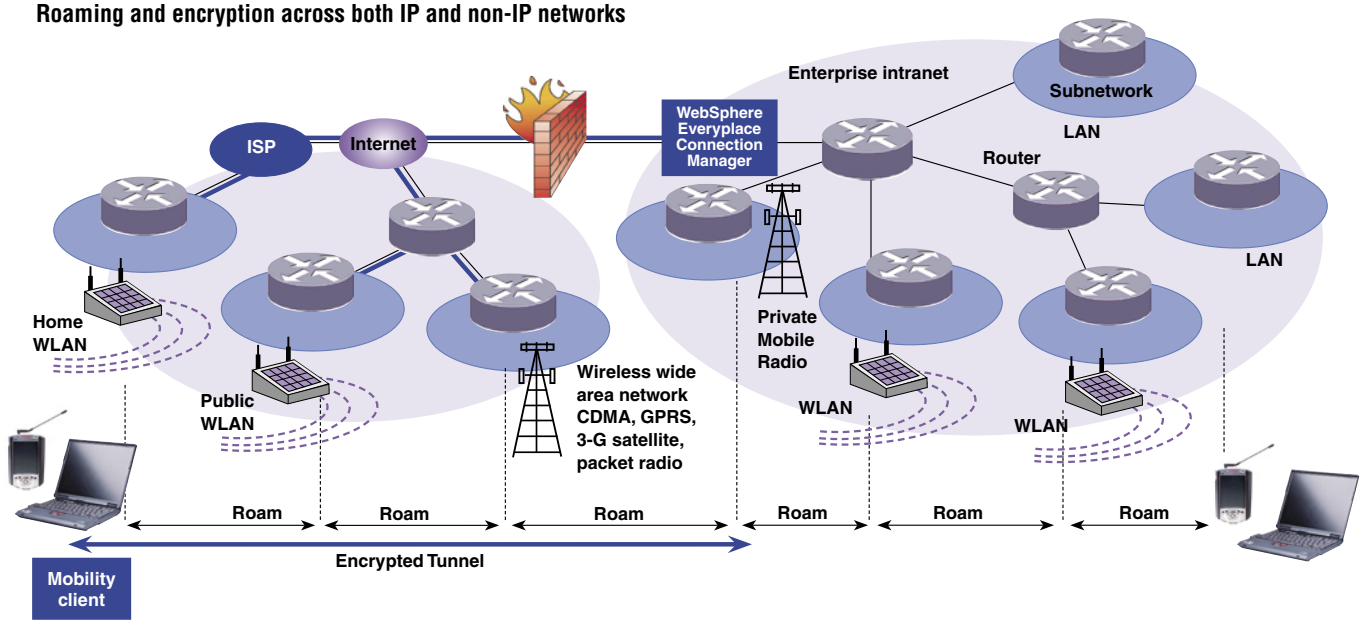
Companies moving beyond basic e-mail, SMS and personal information management (PIM) need to match security privileges, connection frequency, total data and network costs against a multi-network environment. Maintaining persistence, authentication and encryption across these boundaries is a daunting task. To simplify that environment, WebSphere Everyplace Connection Manager can increase user productivity by not requiring login and re-initialization of the application whenever roaming occurs.

Persistence allows switching physical networks, while preserving both the VPN connection and application session. In shifting from home Digital Subscriber Line (DSL) to office LAN, cellular or WiFi hotspot, users remain connected and encrypted from device to enterprise. Without roaming, that same user would lose their session and be forced to restart the application, re-authenticate to the firewall, obtain a new IP address, renew the VPN connection and restart the application. This is particularly important in instant messaging sessions, where dropping connections effectively means losing the entire conversation string.

Roaming across non-IP, packet radio networks is a key capability in WebSphere Everyplace Connection Manager.

Roaming is accomplished via a software layer that isolates the application from the physical network interface, implements a persistent IP network interface and routes application traffic through that new interface. This permits the Mobility Client VPN to dynamically select networks and smoothly roam without breaking session integrity.

Roaming and encryption across both IP and non-IP networks



In addition to providing virtually seamless roaming between wired and wireless networks, WebSphere Everyplace Connection Manager enables a secure, encrypted tunnel.

Network connections

Cellular Networks:
CDMA
TDMA
GSM CSD, SMS
PCS 1900
PDC (Japan)
PHS (Japan)
CDMA2000, 1XRTT, eVDO
GPRS (GSM)
UMTS
PDC-P (Japan)
iDEN
CDPD and CS-CDPD
AMPS & N-AMPS

SMS-C Connections:
SMPP
SMTP
SNPP
UCP

W-LAN, W-PAN:
802.11b
802.11a
Bluetooth

LAN Connections:
Ethernet
Token Ring

Internet Connections:
Cable Modem
ADSL/DSL
ISDN
ISP

Dial Connections:
DIAL/TCP
ISDN
PPP
PSTN (POTS)

Public Non-IP Radio Networks:
DataTAC 4000 (US)
DataTAC/IP
DataTAC 5000 (Europe)
Modacom (Germany)
DataTAC 6000 (Asia)
DataTAC/IP
Mobitex (Worldwide)
Mobitex/IP (US)

Private Packet Radio Networks:
Dataradio
Motorola Private Radio
(DataTAC)

Satellite Networks:
Norcom
Wireless Matrix

Unmatched mobile security

WebSphere Everyplace Connection Manager features multiple levels of authentication and encryption to assure identity of the user, prevent unauthorized access and protect data privacy. In addition to the mobile VPN option, Connection Manager incorporates Secure Socket Layer connectivity, Wireless Transport Layer Security and Point-to-Point Protocol remote access standard from PPP clients. A symmetric encryption key is used to encode or decode data with varying key lengths, the strongest being the 256-bit key used in the Advanced Encryption Standard (AES). To ensure data privacy and protection, customers can choose from Data Encryption Standard (DES), Triple DES, RC5, AES and other algorithms.

WebSphere Everyplace Connection Manager includes FIPS certification for government and military applications.

Compared to traditional Internet Protocol Security (IPSec) VPNs or special purpose mobile middleware, the IBM approach has a number of compelling advantages:

Comparative overview

Mobility Client feature	IBM WebSphere Everyplace Connection Manager	Traditional IPSec VPN
End-to-end encryption	✔	✔
Seamless, cross-network roaming IP and non-IP networks	✔	
Secure IP routing through non-IP networks	✔	
Network address translation	✔	
Bi-directional, two-factor authentication	✔	✔
Header reduction, IP data compression and filtering to reduce packet overhead	✔	
TCP protocol optimization to minimize costly retransmissions due to network latency	✔	
Dynamic disconnect/reconnect	✔	
Performance tuning profiles customizable for differences in connection technologies	✔	
Support for Microsoft® CE.Net, Windows®, Pocket PC, Win CE, Palm OS and Linux	✔	✔

Connection Manager validates users against corporate LDAP directory servers, as well as Remote Authentication Dial-In User Service (RADIUS)-compliant authentication servers. To ensure proper strength of the shared-secret key, comprehensive password policy rules are enforced at Connection Manager. The latest release has been enhanced for two-factor authentication by tying user credentials with hardware identifiers, such as hardware serial number, modem network address, or call line identifier. Connection Manager can also verify valid X.509 client certificates, comparing the information in the certificate against a trusted certificate authority.

For government and military clients, WebSphere Everyplace Connection Manager is certified for the Federal Information Processing Standard (FIPS) 140-2 (under review), 197, 46-3, 186-2 and 180-1 standards. The cryptographic libraries used by IBM have been tested and verified for U.S. and Canadian Federal agencies, an important attribute for deploying mission-critical, highly secure mobile applications.

Data transmission costs may be reduced as a result of the WebSphere Everyplace Connection Manager's efficient data compression.

Optimizing bandwidth to reduce costs

In recent tests, WebSphere Everyplace Connection Manager increased effective throughput on a GPRS network by over 60 percent. To accomplish this, the Mobility Client and Connection Manager implement advanced data compression, byte reduction and minimization of Transmission Control Protocol (TCP) retransmissions to reduce data loads and increase effective bandwidth. The platform has also been demonstrated to improve session stability for instant messaging, heavy file downloads and Web transactions. Assuming an average monthly charge of $50 for GPRS services and a 20 percent annual drop in prices, 200 users consuming 40 megabytes per month each could save up to $75,000 in the first year alone.

Broad-scale messaging services

WebSphere Everyplace Connection Manager Messaging Service also includes a powerful messaging gateway with support for an impressive range of WAP phones, SMS phones and pagers. A WebSphere Everyplace Connection Manager Toolkit and application program interface (API) are available to create push applications by simply specifying the address type. Connection Manager hides the complex details of message encoding specific protocols for each network and connections to the network from the developer.

These messaging services are tightly integrated with WebSphere Everyplace Access, a complementary product. Included in that platform is Intelligent Notification Services (INS), which utilizes messaging services for push alerts. INS monitors information from a variety of sources, recognizes when an event occurs and notifies workers via cell phone, pager or personal digital assistant (PDA). A "Stock-Out Alert" from an INS-enabled supply chain application, for example, can issue messages when inventory reaches critical levels.

Optimizing throughput over GPRS networks

Data type	File size Kb	File size over GPRS after WebSphere Everyplace Connection Manager	Percent reduction	Realized throughput Kb/S
App Log File (small)	14	5	64%	45
App Log File (small)	291	119	59%	54
App Log File (large)	973	318	67%	61
System Configure File	77	32	58%	44
HTML File	2,660	948	64%	55

Net savings for 200 employees = $75,000 in Y1

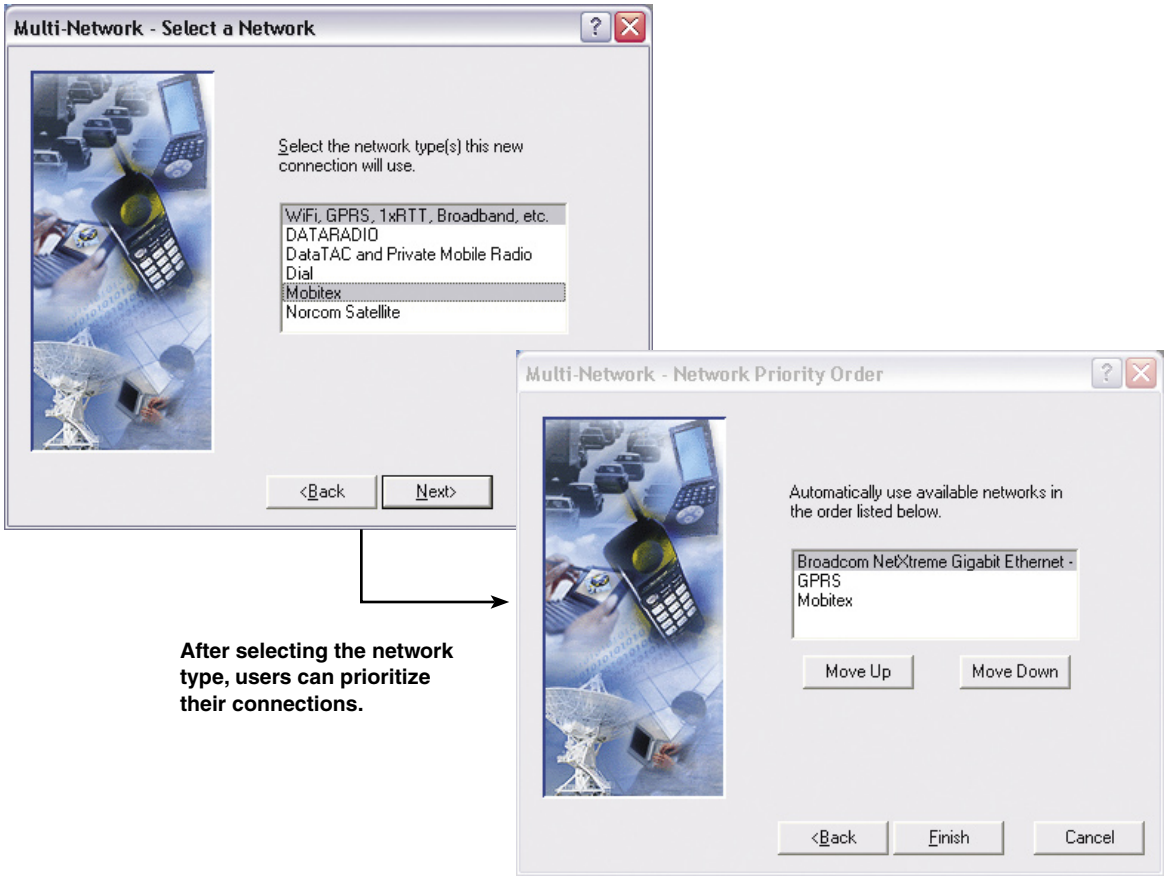
Assumptions	
Average increase in realized throughput	63%
Number of mobile employees	200
Expected mobile data use per month (MB)	40
Expected growth in mobile data usage	0%
Monthly bill in USD (AT&T Wireless GPRS)	$50
Annual drop in data prices	20%

WebSphere Everyplace Connection Manager offers mobile users continuous wireless network access for virtually uninterrupted communications, data protection and increased productivity.

Enhancing the user experience

To simplify network selection, WebSphere Everyplace Connection Manager Version 5.0 features a powerful graphical user interface that steps the user through a list of connections and prioritizes them from high to low. When a higher priority connection becomes available, WebSphere Everyplace Connection Manager automatically senses and switches to that network. And when a new connection is discovered, the Mobility Client queries users, dynamically defines the new network interface, adds that option, opens the interface and switches connections depending on priority.

Prioritizing networks for roaming



After selecting the network type, users can prioritize their connections.

Architecture

WebSphere Everyplace Connection Manager is a complete wireless and wireline mobile access platform for extending e-business solutions, or any IP-based applications, securely and efficiently to mobile users. The architecture comprises three distinct components, each designed to run on multi-vendor hardware and operating system platforms: Connection Manager server, Mobility Client and Distributed Administration.

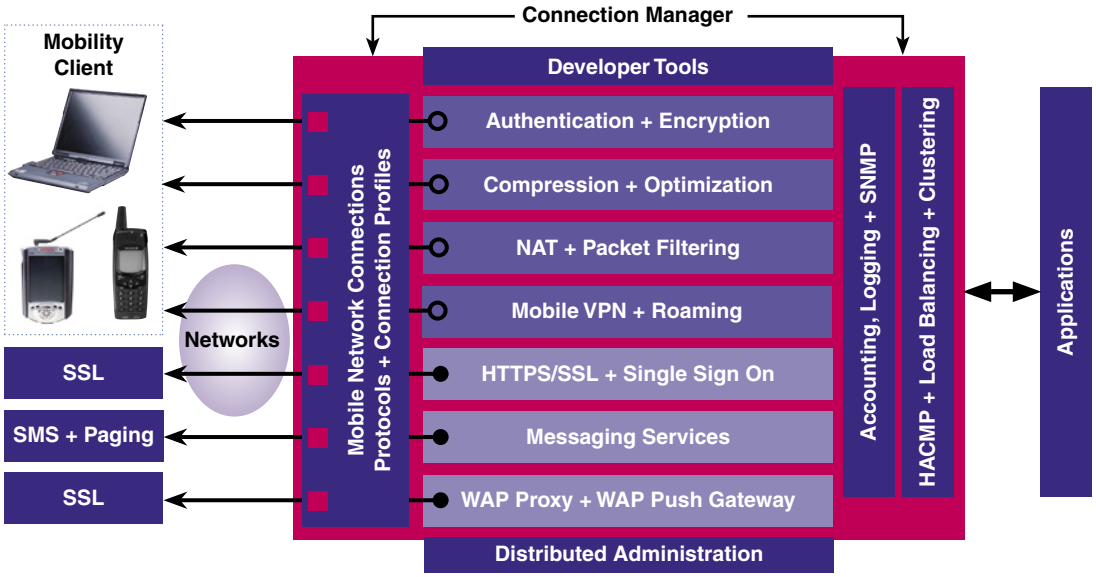
Mobility Client

Mobility Client runs locally on the device, establishes an optimized mobile VPN and enables cross-network roaming. Once Mobility Client authenticates to Connection Manager, a VPN is established and the device securely joins the enterprise intranet.

Mobility Client also includes a toolkit and APIs to create network-aware applications. One type of application, for example, selects the exact type of data to transmit based on type of connectivity, costs and bandwidth. Another can monitor Wi-Fi signal strength, decide to start a GPRS connection and roam to GPRS before Wi-Fi connectivity is lost.

Connection Manager

Connection Manager supports a comprehensive spectrum of communication protocols for both IP and non-IP networks, indicated in the chart on page five. Flexible connectivity is created by configuring multiple Mobile Network Connections (MNC) for any combination of public or private physical networks. Unlike conventional VPNs, each MNC can be tuned for optimal performance, compensating for latency, link speed and other characteristics that vary across different communication technologies.



Mobile Network Interfaces and IP Addressing

WebSphere Everyplace Connection Manager also implements Mobile Network Interfaces (MNI) through which the operating system IP layer communicates with all supported wireless, dial or wireline networks. The platform controls one or more IP subnets of users whose traffic is routed through the appropriate MNI. IP addresses can be assigned on either a static basis or via Dynamic Host Configuration Protocol to support a pool of dynamically assigned addresses.

Each network interface in WebSphere Everyplace Connection Manager can be fine-tuned to control traffic flow.

In order to reduce and control data traffic, each MNI can be customized with packet filtering or packet mapping. The built-in Network Address Translation feature helps manage scarce corporate IP addresses, expanding the number of addressable Mobility Clients to 64,000 for every real IP address.

HTTP/HTTPS Access Service

For mobile devices with an SSL-capable browser, Connection Manager also supports either unsecured Hypertext Transfer Protocol (HTTP) or authenticated Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) connectivity. To enable Single Sign On through Web servers or portals, WebSphere Everyplace Connection Manager Version 5.0 adds Light Weight Third Party Authentication token support.

Messaging services

Connection Manager includes extensive messaging services that implement a wide range of Service Provider connectivity options. Short messaging and one-way or two-way messaging needs are well covered over a wide variety of protocols:

- SMPP – Short Message Peer to Peer over X.25 and TCP/IP
- UCP – Universal Computer Protocol over X.25 and TCP/IP
- WCTP – Wireless Communication Transfer Protocol over TCP/IP
- SNPP – Simple Network Paging Protocol over TCP/IP
- SMTP – Simple Mail Transfer Protocol over TCP/IP
- WAP Proxy Services

WAP Proxy and Push Proxy Gateway

As an option, WebSphere Everyplace Connection Manager incorporates a WAP 1.2.x compliant WAP Proxy and Push Proxy gateway.

Distributed Administration

Administration of single or multiple Connection Managers is simplified with a Java remote console and portlets in the IBM WebSphere Portal Server. This includes defining several levels of administration delegation, each with separate access or change permissions, permitting flexibility to match organizational needs.

All administration and configuration data resides in a common Lightweight Directory Access Protocol (LDAP) directory. Remote Gatekeeper administration communicates securely to the Connection Managers via Extensible Markup Language (XML) over SSL connections.

Recommendations

As data usage, network options and security vulnerabilities grow, companies need to simplify their communications architecture, reduce costs and enforce corporate security policies. In order to take advantage of the benefits in WebSphere Everyplace Connection Manager, firms should consider a five-point plan for deploying a mobile enterprise and managing user connectivity:

1. Conduct an assessment to appraise current wireless security levels, risks, connectivity challenges, user behavior and mobility costs
2. Define an appropriate mobile architecture, security principles, cost targets and network option
3. Model both current and future network, device, application and user need
4. Design and deploy an end-to-end communications platform vs. a patchwork architecture
5. Partner with a leading vendor on the basis of product capabilities, partnerships, future roadmap, financial stability and services expertise

Summary

Given pressures to increase productivity while reducing costs, roaming and security and optimization between networks are emerging as basic tenets of connectivity. With the IBM platform, connectivity can be seamless as the workforce changes locations or networks while maintaining a secure, encrypted session.

IBM, as a leader in wireless e-business and with nearly 150,000 IBM Global Services professionals in 170 countries, can assist you with aspects of Wireless LAN, Public WLAN and seamless roaming. IBM can help enterprises, as well as Service Providers, deploy wireless networks and provide seamless, secure roaming for their employees and customers.

For more information

To learn more about IBM Pervasive Computing and WebSphere Everyplace Connection Manager, visit: **ibm.com**/software/pervasive/products/mobile_sols/connection_manager.shtml

IBM Corporation
Department LG9A
8051 Congress Avenue
Boca Raton, Florida 33487

Produced in the United States of America
04-03