IBM WebSphere Everyplace Suite v1.1

White Paper

18th October 2000

Bob Beck
Mike McGinnis

The authors wish to express appreciation to the following team members for their tremendous assistance in creating this paper:

Dennis Anderson	Paul Bercow	Keith Carter
Tom Covalla	Jim Crosskey	Patty Dudek
Peter Goss	Gary Hand	Wendy Ling
Dave Locke	Karen Momenee	Mark Pozefsky
Sandeep Singhal	Keith Taylor	John Turek

Table of Contents

1.0 Objectives

The primary objective of this paper is to describe the features, functions and benefits of WebSphere Everyplace Suite for the benefit of IBM's sales teams and IBM's customers. This document therefore is intended to be a combined sales enablement tool and customer reference.

To support this objective, the content of this document is biased towards a relatively non-technical, value-based perspective rather than a deeply technical, architecture-based level.

The scope of the document is such that the reader will attain a level of understanding down to component level depth which spans across the whole breadth of the suite. On reading through this document, readers should be able to understand what WebSphere Everyplace Suite does, how it does it, and what business value it delivers. This document will be regularly maintained and the latest version will always be found on the IBM Pervasive Computing Web site at www.ibm.com/pvc within the "Tools and resources" section. The authors suggest you check back here regularly.

2.0 Introduction

Nearly five years ago, in a ten year outlook study, IBM identified the single largest opportunity for the corporation over the next ten years. At the time, we were imagining that the Internet would become the preferred medium for a myriad of communication and commerce activities, and that rather than PC's being the dominant access point, a whole new class of client devices would emerge. Today, these devices are not only an everyday reality, for example Wireless Application Protocol phones (WAP phones), Personal Digital Assistants or PDAs, and Internet devices, but their adoption by companies for business purposes is growing rapidly. IBM uses the term "pervasive computing" to describe the actions, behavior and opportunities that would be experienced by IBM and its customers during this new phase of computing.

At about the same time, IBM was focused on another transition; the e-business transition. The amount of hardware, software and services revenue which are now attributed to e-business activities shows that this transition is nearly complete. Our business today, and into the future, is e-business. And in that future lies even more opportunity than we've ever imagined, due in large part to the very same things we envisaged five years ago. The rate at which the Internet is "going mobile" is faster than almost anyone could have imagined. For example, NTT DoCoMo's *iMode* service crossed the proverbial "chasm" as if it were a small crack with around half a million new subscribers being added per month recently.

The high and relentlessly increasing level of cell phone penetration together with the dawn of broadband wireless services are enabling data access, collaboration and transactions to be conducted on the move and without wires.

Today, many businesses have already recognised how these mobile Internet technologies will affect their marketplace and have responded quickly by deploying enterprise-class mobile e-business solutions. IBM has been in the thick of the action from the start, helping organizations such as Banesto, Delta Air Lines, Ethicon, Handelsbanken, Swissair, Telus and dozens of other leading enterprises extend their existing e-business solutions to reach the emerging mobile e-business economy. This is the second wave of e-business and it's happening today.

As with any emerging opportunity of this magnitude there are an almost unlimited number of ways in which a company can choose to engage. IBM has chosen to focus on the intelligent middleware, services and hardware that make it easy to extend web applications, enterprise applications and all forms of data to a virtually unpredictable set of devices. Starting with the basic concepts from our outlook study, added to our extensive mobile Internet engagement experience, we've architected, developed and integrated a set of software and services that make it easy for our e-business customers to extend their applications to the Pervasive Computing domain.

IBM's mobile e-business strategy is based on our customers' desire to reach a new class of client devices by extending their existing e-business infrastructure. This protects and enhances the value of their existing e-business investments while simultaneously minimizing the time-to-market for a commercial deployment.

We've also made a number of strategic decisions which set the tone for most of our current go-to-market activities. Major handset and communications infrastructure suppliers are our partners. Carriers and service providers are our customers, and possibly, also our partners. Large enterprises are our customers. Business partners such as web integrators and system integrators are channels for our software and hardware. Independent Software Vendors, ISV partners are our "pizzazz". We endorse the competitive playing field that comes with open standards and we invest heavily in both initiating and extending industry standards which are important to us. These simple facts are the backbone of our strategy and help to shape our tactics.

Besides extending the reach of existing e-business applications to mobile users, mobile Internet technologies will give rise to an entirely new class of value-added applications offering "location-based

services". Imagine being able to call a cab, find a restaurant or order take away food, or locate a car breakdown recovery service in an unknown destination at the press of a few buttons on your cell phone. In the near future, the location sensing capabilities of emerging wireless technologies will be able to accurately pinpoint your position from your cell phone or wireless PDA and put you in touch with services and products in your immediate vicinity.

2.1 Modern e-Business

The modern e-Business environment consists of a three-tier system:

- The **Web Server** receives inbound HyperText Transport Protocol, or HTTP requests, manages communication sessions, and routes requests to the appropriate application server(s).
- The **Web Application Server** executes the business logic, manages application sessions, and interacts with the back-end systems.
- The **back-end systems** include various internal and external services (e.g. data, transactions, payments) and various auxiliary services (e-mail, collaboration, directory, etc.) that form the core business processes of the e-business solution.

Pervasive computing is about connecting a wide variety of client devices (such as PDAs, cellular phones, automotive computers, home gateways, wearable computers, as well as traditional PCs) to a modern Web environment, and enabling interaction and e-business to occur via technology which is virtually invisible to the end user. When compared to e-business solutions that today connect desktop PCs to these servers, pervasive computing introduces the following unique requirements:

- **Generate and process different types of input/output content:** some devices have only text capabilities, others also have graphical capabilities, and others may add or be limited to audio capabilities. The industry is separating content from presentation using eXtensible Markup Language (XML). Pervasive middleware must be capable of generating and processing multiple types of markup languages such as subsets of HyperText Markup Language or HTML such as HTML 3.2, and CompactHTML or other XML presentation languages such as Wireless Markup Language (WML) and VoiceXML.
- **Customize content and distribution based on user, device, and network characteristics:** Content delivered to pervasive devices needs to be personalized, not only to reflect the user's content preferences (content selection and filtering), but also to reflect the environment (reduce content size to match network bandwidth, re-format content to match particular target device). Simply selecting the right markup language is insufficient, because different pervasive devices will present that content differently.
- **Support asynchronous client-server messaging and data synchronization:** Pervasive devices, unlike desktop PCs, typically are not always connected to the network. Instead, they need to be able to queue outbound requests and asynchronously receive messages delivered from the network. Similarly, pervasive devices typically contain a local data store that can be modified off-line and therefore must be synchronized with the primary data server.
- **Enable alternative access protocols such as the Wireless Application Protocol (WAP):** The pervasive device space is dominated by both non-Internet Protocol (non-IP) network protocols that are particularly optimized for wireless connectivity, as well as Internet Protocol capable networks. To address the diverse international variety of cellular, packet radio, and satellite protocols, the industry is rallying around the Wireless Application Protocol standard for network and device independent wireless Internet access. In the future, devices may communicate using various optimized TCP/IP dialects.
- **Manage the device from the network to reduce support costs and enhance user experience:** Pervasive devices are often accessed by non-computer-literate users or by mobile workers who are far removed from the physical control of the enterprise IT department. Consequently, extremely

easy-to-use device management is needed to upgrade client software, detect or even predict device faults, and perform other management functions on behalf of inexperienced user.

- **Virtual private network (VPN) and security services:** Pervasive devices typically connect to the enterprise using various public carrier networks. To access enterprise content or personal data, the device needs to be assured of end-to-end security that prevents data being observed or altered by unauthorised users.

To meet these requirements, a service provider or enterprise needs to install an infrastructure server between the pervasive devices and the servers that those devices need to access. This infrastructure server (hereafter referred to as the pervasive ***WebSphere Everyplace Suite*** provides the necessary connectivity, content manipulation, synchronization and management functions required to support pervasive devices.

2.2 WebSphere Everyplace Suite

WebSphere Everyplace Suite has been designed in response to a set of fundamental business objectives which existing and prospective customers have told us they need:

- ✓ Preserve existing investment by integrating into existing applications and subsystems easily.
- ✓ Increase customer loyalty for greater retention and/or less churn.
- ✓ Deploy new services quickly and cost effectively.
- ✓ Support future (unknown) client devices quickly and cost effectively.
- ✓ Adjust end-user experience appropriate to multiple client devices.
- ✓ Provide end-to-end security, with minimal end-user disruption.
- ✓ Provide usage information appropriate to existing accounting and billing systems.

IBM WebSphere Everyplace Suite addresses these needs for two major customer sets:

- **Service Providers** such as telecommunications companies, Internet Service Providers and Application Service Providers which are providing access to data and applications
- **Enterprises** of all kinds which are providing access to customers, employees and/or suppliers to data and applications which reside within their intranet domain.

3.0 Overview

3.1 WebSphere Everyplace Suite

One of IBM's great strengths in technology is the investment it has made in its Research and Development Laboratories. Increasingly, customers are interested in "First of a Kind" solutions that provide differentiation in the market place. IBM can provide customers with that differentiation through the work that has both been completed and is ongoing in its labs all over the world.

An example of such a solution is IBM WebSphere Everyplace Suite, an integrated, end-to-end middleware solution for mobile e-business. WebSphere Everyplace Suite provides the functions necessary to enable data access and the extension of e-business applications to the new class of client devices such as WAP phones and PDAs (as well as the installed base of mobile computers running Windows clients.

Uniquely, WebSphere Everyplace Suite combines "First of a Kind" differentiation with quality and reliability through the use of IBM technologies that have already been proven in customer environments around the world. Packaging these technologies into an integrated offering brings value to the customer through simplified pricing and ordering, easier installation and configuration, together with a common security and accounting architecture.

WebSphere Everyplace Suite consists of the following major functional areas:

Connectivity:

- ✓ **Everyplace Wireless Gateway:** Provides security-rich wired and wireless connectivity between the IT network and the Communications Network (e.g. Cellular networks including GSM, CDMA, TDMA, PDC, PHS, iDEN, AMPS; Packet Radio networks including GPRS, CDPD, DatatTAC, Mobitex; plus satelite; and Wireline environments including DSL, cable modems, Internet Service Providers, ISDN, Dial, and LAN). In addition, provides protocol translation as a WAP gateway, information push as a WAP push proxy gateway, and support for short messaging (SMS).

Content Adaptation:

- ✓ **WebSphere Transcoding Publisher.** Transforms arbitrary content into a form that can be presented on a device that is different from the originally intended target, such as changing HTML content intended for desktop PCs to WML content suitable for the new class of smartphones.
- ✓ **MQSeries Everyplace:** Enables pervasive devices to queue messages, and assure their completion once and only once, in a security-rich and efficient manner in both connected and disconnected end user scenarios.
- ✓ **Everyplace Synchronization Manager:** Enables pervasive devices to operate applications "off-line", and synchronize the results of their activities with a server database when connectivity is re-established.

Management Services:

- ✓ **Tivoli Personalized Services Manager:** Provides a comprehensive set of management services including content personalization, enrollment, self-care, customer care, interfaces to external billing systems, reporting, software distribution and update.

Security:

- ✓ **Everyplace Authentication Server:** Provides the user and device authentication capabilities which enable a single, device-independent user log-on, and pass-through of authentication information to web application servers.
- ✓ **Client Authentication and Encryption:** IBM is a recognized leader in the industry on the issue of security and privacy. To that end, the Everyplace Wireless Gateway is designed to enable comprehensive end-to-end security, within the constraints of the devices being used. Where

standards exist to accomplish this task, IBM supports the standards. Where no standards exist, the Everyplace Wireless Gateway provides alternatives which are time tested and acceptable to the worlds leading companies. Details of our support for various clients are as follows:

- **WAP Clients:** The Everyplace Wireless Gateway utilizes WAP Transport Layer Security (WTLS) for communication between a WAP enabled device and the Everyplace Wireless Gateway. The gateway supports WAP basic authentication and data privacy via several WTLS encryption algorithm options. Security for WAP devices is an area of high activity for the WAP Forum, and IBM, as an active member of the WAP Forum is working to both shape the specification, and rapidly bring to market, advances in this area as they become standards.

- **Windows and Windows CE Clients:** Through a small piece of code which is installed directly on these platforms, the Everyplace Wireless Gateway provides bi-directional authentication with key distribution using a minimal number of messages over the network. This is a security protocol called Two-Party Key Distribution Protocol (2PKDP). In addition, the Everyplace Wireless Gateway provides data privacy on these platforms via encryption/decryption support for communications coming into and going out of WebSphere Everyplace Suite, with a choice of either DES, Triple DES or RC5 encryption algorithms, as explained later.

- **PPP Clients (e.g. Palm devices):** The Everyplace Wireless Gateway enables PPP clients to communicate with the gateway using either PAP or CHAP authentication.

✓ **Firewall support:** Support for integrating IBM SecureWay Firewall and popular 3rd party firewalls to protect against unauthorized access and viruses.

✓ **Virtual Private Network support:** Support for integrating theIBM Virtual Private Network feature of the IBM SecureWay Firewall to extend an enterprise's private intranet across a public network, such as the Internet, and to create a private connection with security through a private IP tunnel.

Performance Optimization:

✓ **Everyplace Wireless Client/Gateway:** For Windows and Windows CE-based clients, provides wireless optimizations for standard IP communications including header reduction, IP packet compression, IP filtering, and TCP protocol optimization to address wireless network latency and constrained bandwidth.

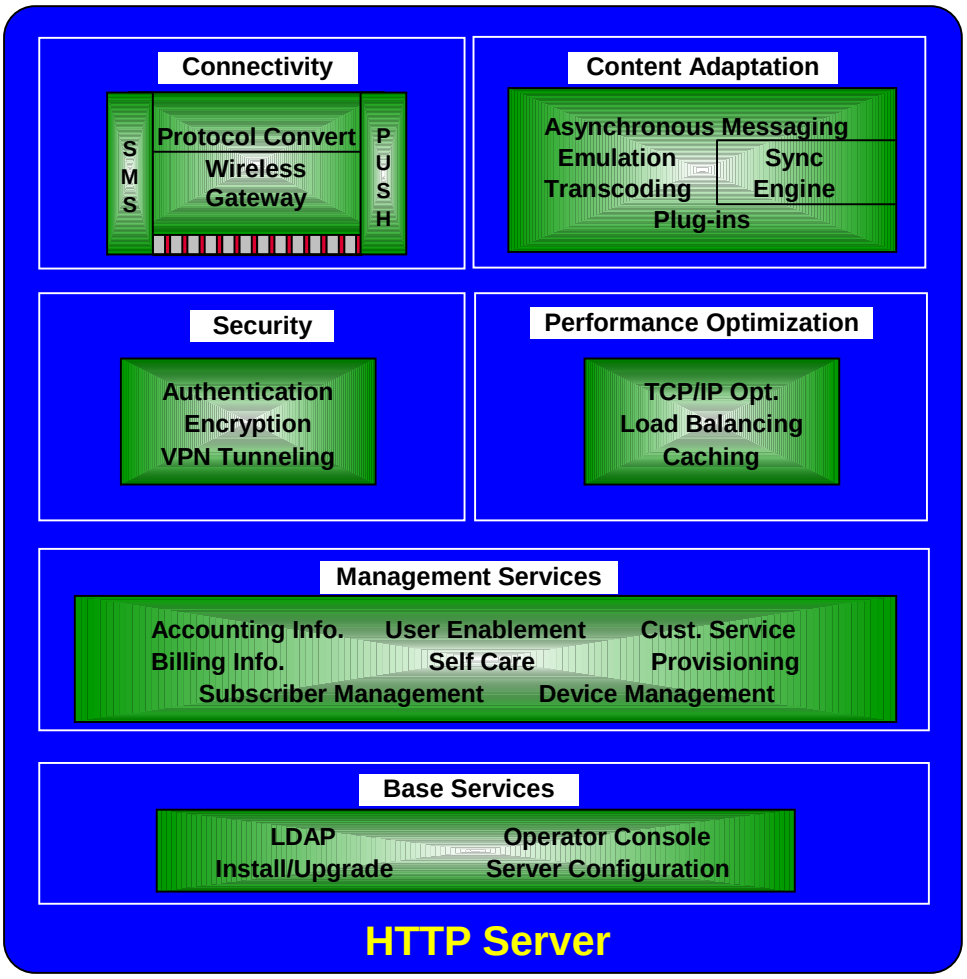
✓ **WebSphere Edge Server:** Provides highly scalable caching functions on a server to reduce bandwidth costs and improve response times when processing URLs. In addition, WebSphere Edge Server dynamically monitors and load-balances activity across the set of WebSphere Everyplace Suite processors which are deployed in a configuration.

Base (Common) Services:

✓ **Secureway Directory:** A central LDAP repository which contains runtime information about active sessions, users, devices, and networks. This database makes it easy for the various components of WebSphere Everyplace Suite (and any server that is added to the configuration) to access the runtime information centrally, without having to replicate the data in other repositories.

✓ **Everyplace Suite Console:** Provides a single console for system administrators to perform installation and diagnostic procedures, administrative procedures, and system maintenance procedures.

In the intial release, WebSphere Everyplace Suite will be available on AIX and Solaris operating platforms.

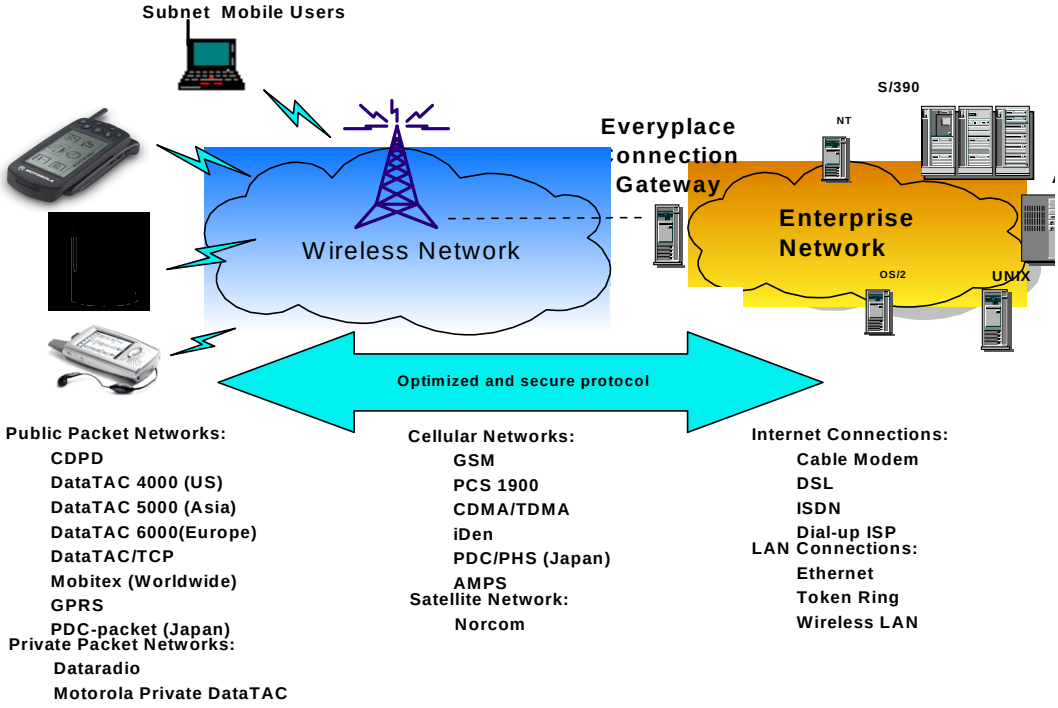

Connectivity
SMS
Protocol Convert
Wireless
Gateway
PUSH
Content Adaptation
Asynchronous Messaging
Emulation
Transcoding
Sync
Engine
Plug-ins
Security
Authentication
Encryption
VPN Tunneling
Performance Optimization
TCP/IP Opt.
Load Balancing
Caching
Management Services
Accounting Info.
User Enablement
Cust. Service
Billing Info.
Self Care
Provisioning
Subscriber Management
Device Management
Base Services
LDAP
Operator Console
Install/Upgrade
Server Configuration
HTTP Server

4.0 Connectivity

4.1 Everyplace Wireless Gateway

4.1.1 Description

Everyplace Wireless Gateway is a distributed, highly scalable, multipurpose UNIX communications platform that supports optimized, security-rich data access by both Wireless Application Protocol (WAP) and non-WAP clients over a wide range of international wireless network technologies, as well as local area (LAN) and wide area (WAN) wireline networks.



Everyplace Wireless Gateway includes the following features:

- ✓ **Support for the WAP Version 1.2 standard** (as defined by the WAP Forum).
- ✓ **SMS information "push"** capability to client devices.
- ✓ **IBM SecureWay wireless technology** which supports standard Internet Protocols (IP) efficiently and with security over both IP and non-IP wireless bearer networks.
- ✓ **Distributed Gateway design** using dynamic clusters of gateways to balance load and improve availability and allowing multiple gateways to access end user and network configuration information from a central, highly scalable LDAP-based repository.

Everyplace Wireless Gateway is made up of several key components:

- ✓ **Everyplace Wireless Gateway:** which provides a security-rich, high performance TCP/IP communications interface between a broad range of devices and a variety of wireless, dial-up, and LAN networks.

- ✓ **Everyplace Wireless Gatekeeper:** a Java™ based administrator's console to the Wireless Gateway and to wireless resources that enables centralized or distributed remote administration.

- ✓ **Everyplace Wireless Client:** wireless client code which, when installed onto a device, enables wireless device access through the Everyplace Wireless Gateway with full performance optimization and security functionality.

4.1.2 Everyplace Wireless Gateway

Everyplace Wireless Gateway integrates all supported international networks within a single UNIX gateway. Its ability to connect radio networks to wireline networks means that all supported devices, whether they be mobile or static, can access the network and applicationsvia the same wireless gateway, regardless of the cellular or radio network. Users with different application needs (based on transmission costs, coverage, or devices) can select the best wireless network for their situation. Mobile users can use wired networks as well, such as an ISP connection or an ethernet in the hotel room, and gain secure access through the gateway to their applications.

Applications that use TCP/IP and/or WAP may communicate over the wireless gateway. Everyplace Wireless Gateway and Client not only can be used for efficiently extending enterprise networks with security to the wireless world, but can also be used by carriers and service provider companies to allow them to offer wireless IP extensions to their customers.

The multipurpose design of Everyplace Wireless Gateway enables it to be configured to support a variety of communications modes, including:

- ✓ **WAP wireless communications**
- ✓ **Optimized TCP/IP wireless and wireline communications**
- ✓ **SMS push proxy**

4.1.2.1 WAP wireless communications

When Everyplace Wireless Gateway is configured as a WAP gateway, it performs the protocol conversions to provide communication between WAP clients and the e-business web servers.

The WAP gateway support includes:

- ✓ Compliance with the WAP Version 1.2 standard, as defined by the WAP Forum, including the push proxy gateway capabilities
- ✓ Persistent storage of cookies on behalf of WAP clients.
- ✓ Security features based on the WAP Wireless Transport Layer Security (WTLS) protocol between WAP clients and the WAP gateway.
- ✓ Security-rich HTTP (HTTPS) requests to Web servers using Secure Sockets Layer (SSL) made on behalf of WAP clients.
- ✓ A choice of encryption algorithms and key strengths for both key exchange and bulk encryption methods.

- ✓ WAP user Authentication integrated with the Everyplace Authentication Server, and the LDAP directory in the Everyplace Suite, or optionally with a 3rd party RADIUS server. Certificate authentication for WAP 1.2 compliant clients is also supported.
- ✓ Interfaces to IP capable networks such as Cellular Circuit-Switched Data and IP Packet based networks, as well as SMS network types. For example, SMS-SMPP and SMS-UCP.
- ✓ Network Management of WAP Gateway via Simple Network Management Protocol (SNMP) standards.
- ✓ Accounting records are stored in a ODBC relational database allowing external applications easy access to billing data.

4.1.2.2 Optimized TCP/IP wireless and wireline communications

In this configuration, the Everyplace Wireless Gateway integrates data access from wireless and wireline networks. TCP/IP applications may use either wireless networks and wireline networks. Using TCP/IP further integrates communication under a common interface layer that shields all network-specific details from the user application and addresses the wireless environment issues. Functions that address the mobile and wireless environment include network-specific enhancements such IP tunneling through non-IP wireless networks, header reduction, IP data compression and filtering, data encryption for privacy, bidirectional authentication of both the client and the gateway, TCP protocol optimization for network latency, dynamic connection suspend/resume for reducing connect time charges and recovery from inadvertently dropped connections, and a rich set of diagnostic, logging, accounting and management functions..

Everyplace Wireless Gateway supports a wide range of wireless and wireline networks, including:

Cellular Networks
- AMPS and N-AMPS
- CDMA
- TDMA
- GSM
- iDEN
- PCS 1900
- PCD (Japan)
- PHS (Japan

Public Packet-Radio Networks
- CDPD and CS-CDPD
- DataTAC 4000 (US)
- DataTAC 5000 (Europe)
- Modacom (Germany)
- DataTAC 6000 (Asia)
- DataTAC/IP
- GPRS (GSM)
- Mobitex (Worldwide)
- Mobitex/IP (US)
- PDC-P (Japan)

Internet Connections
- Cable Modem
- DSL
- ISP

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

Private Packet Networks
- Dataradio
- Motorola Private DataTAC

Satellite Networks
- Norcom

LAN Connections
- Ethernet
- Token Ring
- Wireless Lan

4.1.2.3 Push proxy gateway

When Everyplace Wireless Gateway is configured to be a push proxy gateway (PPG), it enables a Web application server to push (send without a synchronous request) content from a wired network to a WAP client in a wireless network. With a push operation, users are able to get information without having to request that information. Examples of push messages might be news, stock quotes, weather, broadcast messages, and notification of events such as e-mail arrival.

A push operation starts when a Push Initiator application (PI) transmits content to a PPG for subsequent delivery to a client using the Push Access Protocol (PAP). PAP messages, which carry control information, content, and optionally client capabilities information, are contained in XML documents that are exchanged over HTTP between the PI and the PPG. The push proxy gateway validates the incoming push messages. If the content is accepted for delivery, the PPG either initiates or makes use of existing wireless session protocol (WSP) sessions to deliver the push message to a WAP client.

You can configure only one push proxy gateway per wireless gateway.

4.1.3 Everyplace Wireless Gatekeeper

Everyplace Wireless Gatekeeper is an easy-to-use administrative interface that enables you to remotely define and manage any number of Everyplace Wireless Gateways from a variety of platforms, such as AIX, Windows 95, Windows 98, Windows NT, Windows 2000, Linux, and Solaris.

Through Everyplace Wireless Gatekeeper, you can configure wireless gateways, register users and mobile devices, specify logging and tracing controls, and perform other administrative tasks. The administration and configuration data is stored in the Everyplace Suite LDAP directory. Multiple Wireless Gatekeepers can be defined to flexibly distribute administrative permissions and responsibilities. If you use the Wireless Gateway exclusively to support WAP clients, you can configure Everyplace Wireless Gatekeeper to display only WAP-related resources, thereby simplifying the administration process.

4.1.4 Everyplace Wireless Client

The Everyplace Wireless Client is software that runs locally on the Windows and Windows CE-based mobile devices. The Client code enables the interface to the wireless/wireline modems or adapters, optimizes with security the applications' IP data communications, implements dynamic connection suspend/resume, and provides a full function interface for starting and stopping communication with Everyplace Wireless Gateway. After the authenticated network connection to the Gateway is made, the Gateway assigns the client IP address (intranet or internet) and via the Everyplace Wireless Client, the IP applications on the mobile device can run wirelessly using the standard TCP/IP provided by the operating system on the mobile device. The enhanced functionality offered by the Everyplace Wireless Client, in conjunction with the Everyplace Wireless Gateway, enables improved performance and security.Since the Everyplace Wireless Client is positioned below TCP/IP, network-specific details can be shielded from view inside a common interface layer. To the end user or application developer, or administrator, a radio network becomes just another network that does not require any specialized communication protocols or programming. Standard IP routing is supported, even over non-IP wireless bearer networks, permitting unbroken, end-to-end TCP sessions between applications on the mobile device and the application servers in the enterprise network.

The Everyplace Wireless Client is supported for use on devices running Windows CE, Windows 95, Windows 98, Windows NT, and Windows 2000. See section 4.1.8 for further information.

4.1.5 Support for WAP clients

The Everyplace Wireless Gateway, when configured as a WAP Gateway, provides connectivity for multi-vendor WAP 1.1 and WAP 1.2 client devices. For WAP client support no Everyplace Wireless Client software needs to be present on the mobile device. WAP cell phones and WAP PDAs can connect to Everyplace Wireless Gateway using a WAP microbrowser. The Everyplace Wireless Gateway fully supports the WAP Wireless Session Protocol (WSP) to link the WAP microbrowser with connection-oriented and connectionless, security-enriched and non-secure, WAP services. The performance optimization and security functionality for this mode of connection is that provided by the WAP standard.

The administration and management of WAP devices and users connecting through the Everyplace Wireless Gateway are integrated with the Everyplace Suite LDAP directory and the Tivoli management functions. See section 4.1.8 for further information.

4.1.6 Support for standard PPP clients

Another broad category of mobile client connectivty that is supported by the Everyplace Wireless Gateway comprises all devices that can establish a Point to Point Protocol (PPP) connection to the gateway as the Network Access Server. For this PPP client support, no Everyplace Wireless Client software needs to be present on the mobile device. With PPP connections, performance optimization is much less and security functionality is restricted to authentication (no encryption). With PPP connections, you will not receive the benefits of the Everyplace Wireless Client such as efficient logon, data encryption, header reduction, IP data compresssion, connection suspend/resume, or non-IP wireless network support.

To authenticate native-PPP clients, Everyplace Wireless Gateway implements both the challenge-handshake authentication protocol (CHAP) or the ubiquitous password authentication protocol (PAP) that exchanges passwords in the clear. By using the Everyplace Wireless Gateway this PAP or CHAP user authentication support is integrated with Everyplace Authentication or other 3rd party RADIUS servers. The administration of users, IP addresses, network configuration, etc. via the Wireless Gatekeeper is also integrated with the Everyplace Suite LDAP directory. The Gateway can also perform outbound-only TCP protocol optimization to PPP clients as well as integrated network management and logging/accounting.. See section 4.1.8 for further information.

4.1.7 Value

- ✓Companies can efficiently extend their e-business IP networks and applications with security out to mobile devices over wireless and wireline networks.
- ✓Companies can support multiple networks (both wired and wireless), which enables mobile users to use the network that meets their individual needs and cost objectives.
- ✓Everyplace Wireless Gateway supports applications using industry-standard sockets programming interface, so users do not need to learn special programming interfaces or proprietary tools and protocols. In effect, TCP/IP applications can run unchanged with wireless networks.
- ✓The comprehensive network access solution features bi-directional user and server authentication and data encryption for security.

- ✓Everyplace Wireless Gateway data compression and header reduction helps enable faster response times and lower data volumes over the network..
- ✓Everyplace Wireless Gateway automatically disconnects from connection-oriented dial networks during idle periods and reconnects for new data transmissions. This lowers connection fees and preserves a virtual connection when the physical connection is dropped accidentally or intentionally.
- ✓Everyplace Wireless Gateway provides its own Java™ user interface that enables easy setup and configuration across multiple platforms.

4.1.8 Device Support Summary

Since the Everyplace Wireless Gateway is a multi-purpose gateway, "support" of a device can be defined in various ways:

X: WebSphere Everyplace Suite has wireless client code on that device for security-rich and connectivity and optimization functions.

Y: The Gateway can support that device as a standard PPP-capable client, adding the connectivity and somewhat less optimization, and security via authentication only, but not data encryption (with no IBM code needed on the device).

Z: The Gateway can support that device as a WAP-capable client (with no IBM code needed on the device).

The Everyplace Wireless Gateway client device support is defined in these terms, as follows:

Windows CE V2.0 (HPC)	X, Y, Z (w/WAP browser)
Windows CE V2.1.1 (HPC Pro)	X, Y, Z (w/WAP browser)
Windows CE (PPC)	Y, Z (w/WAP browser)
Windows CE V3.0	Y, Z (w/WAP browser)
Windows 95, Windows 98, Windows NT, Windows 2000	X, Y, Z (w/WAP browser)
PalmOS	Y, Z (w/WAP browser)
EPOC	Y, Z (w/WAP browser)
WAP 1.1 cell phones	Z (w/WAP browser
WAP 1.2 cell phones	Z (w/WAP browser
QNX/Neutrino	Y, Z (w/WAP browser)

5.0 Content Adaptation

5.1 WebSphere Transcoding Publisher

5.1.1 Description

Transcoding is the process of transforming content from one format into another, including conversion between alternative screen sizes or window sizes and aspect ratios so that the content can be displayed on a wide and growing variety of devices. Both enterprise and web content may be filtered, transformed, converted, or reformatted to enable it to be universally accessed by a variety of devices, to exploit specific application requirements for content customization, and to enable personalization of general content. Moreover, this content may be delivered over a wide range of networks and, as a result, the network bandwidth and latency encountered will vary greatly.

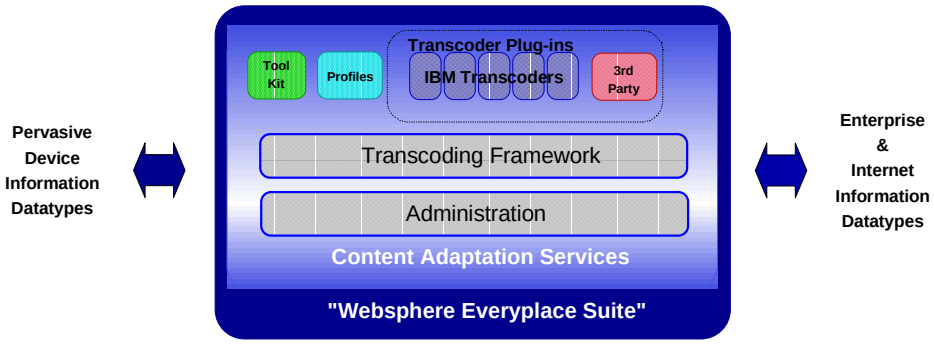
WebSphere Transcoding Publisher offers the following features:

- ✓ A pluggable framework that hosts third-party and IBM-provided transformation plug-ins, or transcoders. New transcoders can be added and can interact with existing transcoders. All plug-ins can leverage a set of core services, such as the ability to acquire preference information in order to respond to different requests for different users or different devices.

- ✓ A base set of transcoder plug-ins that transform content. For example, one of the transcoders can select and apply the appropriate Extensible Stylesheet Language (XSL) stylesheet to transcode an Extensible Markup Language (XML) document for rendering on a particular device. The framework can also host transcoders for other purposes, such as personalizing Web pages, transcoding printable documents for Web viewing, and converting from legacy formats such as AFP (Advanced Function Presentation) to Internet formats such as the World-Wide Web Consortium (W3C) Scalable Vector Graphics (SVG). Other examples include converting HTML for display on Palm, EPOC or Windows CE devices, image re-sizing, and converting HTML to imode.

- ✓ Administrator control over configuration information and preference profiles. Administrators can also view and control message and trace logging.

- ✓ The IBM Transcoding Technology toolkit. This is a developer's toolkit which contains a set of samples, instructions, documentation and procedures to enable you to easily build and implement your own custom transcoder plug-ins. Custom transcoder plug-ins can be used to process additional data formats, to support new pervasive client devices, to extract the most important elements of a particular full screen application for display on a pervasive client device, or to improve the transcoding associated with specific Web applications.



5.1.2 Value

As the use of the Web becomes more ubiquitous in peoples' work and home lives, there are an increasing number of requirements which WebSphere Transcoding Publisher can easily satisfy:

✓ **Legacy Data**
WebSphere Transcoding Publisher enables easy mobile access to legacy data. This is crucial to enterprises as their workforces become more mobile and widespread in order to penetrate new e-business markets.

✓ **New Standards**
Isolating the content presentation from the application enables existing applications to exploit emerging presentation trends, such as Scalable Vector Graphics (SVG), without requiring the application to be rewritten.

✓ **Pervasive Devices**
In the same way, transcoding allows developers to exploit the capabilities of new client devices as they emerge, without re-writing the application.

✓ **Freedom of Choice**
Transcoding enables customers to choose from a wider range of client devices.

5.1.3 Device Support

WebSphere Transcoding Publisher supports pre-EPOC WAP cell phones, i-mode, EPOC (requires device profile), PalmOS, QNX/Neutrino (requires device profile), Windows CE, Windows 95, Windows 98, Windows NT and Windows 2000 device platforms.

5.2 MQSeries Everyplace

5.2.1 Description

MQSeries Everyplace provides MQSeries-compatible messaging in lightweight devices, designed with an emphasis on the frugal use of system resources, both in the messaging device and over the associated client network link. It supports a variety of client operating systems, including operation in an e-Java or Java virtual machine. It inherits all the trusted benefits of MQSeries: industrial strength messaging, reliable communications, and once-only delivery, and in addition provides rock solid encryption and end-to-end security, plus an optimized data stream, all essential in a mobile communication environment.

MQSeries Everyplace can be configured to support a variety of different message queuing styles. Where minimal use of system resources is required, especially on the mobile device, it can be configured to provide capability similar to that of a conventional MQSeries client, i.e. synchronous messaging. MQSeries Everyplace allows mobile workers to access applications on any of the 35-plus platforms of an MQSeries network, MQSeries Integrator, and MQSeries Workflow. Virtually wherever they are, they can access corporate data, and fully participate in business processes such as publish/subscribe.

MQSeries Everyplace provides a high security level as standard with a selection of compression, authentication and encryption options. Enhanced security is available as an additional feature.

MQSeries Everyplace integrates many of the functions that require application programming in other MQSeries family members. Thus encryption and compression are built-in. Similarly, MQSeries Everyplace efficiently supports both reliable and unreliable communications (e.g. local area networks, PSTN over land lines or mobile links, and communications over selected packet radio networks). This communication support is designed to operate with a minimum of user intervention, with system entities such as adapters,channels and transmission queues being effectively hidden from users, programmers and administrators.

MQSeries Everyplace consists of gateway code that runs on the server and device code that executes on the mobile device, which may be a hand-held, a laptop, a monitoring device or an unattended device like a server.

Simplest configurations consist of devices and one or more gateways, and no MQSeries nodes. Applications run on the device and communicate with applications on the gateway. As installations grow, and requirements increase, adding connectivity to an MQSeries network is simple. The gateway automatically handles the data stream and, if necessary, protocol conversion to allow the device to communicate with new or existing, unchanged MQSeries applications. In this mode, the gateway multiplexes multiple device attachment to an MQSeries network.

MQSeries Everyplace on the device can run as a queue manager, constantly available for communications, but storing messages if the connection to the gateway is not available. Configuration and administration is minimal and is intended to be pre-defined, carried out at installation time, done locally through programming or performed remotely.

5.2.2 Value

✓ Dependable application-to-application communication from a variety of mobile devices.
✓ Once-only delivery with prioritization and application-controlled rules.
✓ Efficient use of resources - small footprint, optimised datastreams.
✓ Enables synchronous and asynchronous (disconnected) operations.
✓ Built-in security and encryption.
✓ Transparent to user.
✓ Supports multiple device types within a single MQSeries network.
✓ Simple to start with small configurations, easy extension to existing MQSeries applications.

5.2.3 Device Support

MQSeries Everyplace is available for the following client platforms:

- Any platform that runs the IBM VisualAge Micro Edition virtual machines
  QNX/Neutrino
  Palm OS
  Hard Hat Linux
  Red Hat Linux
- Any platform that runs a Sun-certified Java Virtual Machine (1.1 level)
  Windows CE, Windows 95, Windows 98, Windows NT and Windows 2000

5.3 Everyplace Synchronization Manager

5.3.1 Description

Everyplace Synchronization Manager allows organizations to transfer information from multiple hand-held devices directly to corporate databases without the need to synchronize via the PC. It enables 2-way relational database synchronization with any ODBC database source, 2-way file transfer, and the remote installation of applications.

Everyplace Synchronization Manager also supports direct synchronization with Lotus Notes and Microsoft Exchange for server based synchronization of e-mail, calendars, contacts and tasks.

Finally, Everyplace Synchronization Manager provides the support for synchronizing relational database information between a server relational database and IBM's DB2 Everyplace, a compact relational database for PalmOS and Windows CE platforms.

The end users of the mobile devices need only know how to operate whichever simple 'line-of-business' application they have running on their device. To remotely connect to the server, they simply press the 'Connect' button on the Everyplace Synchronization Manager client software which runs on their mobile device. Everyplace Synchronization Manager then automatically performs the communications tasks, the transfers of information, and so on.

All of these transfers are supported over networking infrastructures that support IP, i.e. Wireless GSM, Internet, as well as standard Local Area Networks (LANs) and Wide Area Networks (WANs). Additionally, the product utilizes a Visual Basic (VB) Scripting engine that enables a company to "plug" its core business logic components directly into their server. Events handled by these components can then be automatically triggered by the data that is being transmitted from the remote hand-held devices. For example, this would allow remotely transmitted orders to be directly launched into a company's workflow system.

As well as logging all transactions by each user, the system captures machine statistics and enables preemptive, problem management, all of which maximizes management control.

5.3.2 Value

Deploying Everyplace Synchronization Manager can increase customer satisfaction by equipping mobile customer-contact personnel with vital information related to their customers. Customers will perceive faster responsiveness, higher credibility and more value in the relationship.

Specifically, with Everyplace Synchronization Manager, users can access and perform updates with applications including:

- ✓ Authentication may be done using the existing authentication capabilities of WebSphere Everyplace Suite.
- ✓ Users can access Notes databases for mail, calendar, address book, to-do lists, memos or corporate application databases.
- ✓ Users can access Microsoft Exchange for mail, calendar, address book or to-do lists.
- ✓ Access to corporate relational databases supporting ODBC Version 4.
- ✓ Binary files can be transferred to handheld devices.
- ✓ Server-based e-mail attachments can be sent to Windows CE devices provided a corresponding converter for the type of file exists
- ✓ Handheld program and data files can be backed up and restored to each device.
- ✓ Each client can establish size limitation parameters for the amount of mail and calendar information they receive.

- ✓ Each client can connect with the Everyplace Synchronization Manager server while cradled to the user's desktop system, eliminating the need to dial while at the home office.
- ✓ Synchronize relational database information between DB2 Everyplace and a server or mainframe relational database.

5.3.3 Device Support

Everyplace Synchronisation Manager supports the EPOC, PalmOS and Windows CE device platforms.

6.0 Management Services

6.1 Tivoli Personalized Services Manager

6.1.1 Description

TPSM is an integrated solution that enables businesses to manage subscribers and their pervasive devices. TPSM provides the following functions:

✓**Subscriber Management Services**
✓**Device Management Services**
✓**Administrator Console**
✓**Support for integration with 3rd party Subscription Management Databases**

6.1.1.1 Subscriber Management Services

Subscriber Management provides a full range of support services, including enrollment, provisioning, self-care, customer care, and billing interfaces:

- ✓ Customer Care application enables subscriber enrollment by end-users and administrators and allows administrator to perform subsequent updates such as checking the statistics of an account, e.g. how much time is spent connected or how much has been charged to the account.
- ✓ Subscriber Self-Care application lets end-users self-enroll and later update these values as well as checking a subset of the statistics possible within the Customer Care application.
- ✓ Accounting of user access.
- ✓ **Customizable portal** by Webmasters, with personalized pages depending on subscriber and device preferences.
- ✓ **Data provisioning** to and from external service provider applications.
- ✓ **Toolkits** to ease the integration with other (optional) service management components that may be chosen, such as billing systems or portal engines.
- ✓ **Subscriber grouping** allows the service provider to categorize end users into various levels such as realms, groups and business accounts.
- ✓ **Subscriber data** such as name, address, hobbies, advertising profile, etc..

✓

✓6.1.1.2 Device Management Services

Device Management provides services to support management of client devices such as screen-phones, PCs, PDAs, and other portable devices with network access. Services include software distribution, device identification, inventory, and remote configuration. Device vendors can extend the framework through a toolkit, enabling the services provided by TPSM to be extended to their specific devices. Features include:

- ✓ **Device Identification services** to identify the device when it joins the network.
- ✓ **Enrollment / Initial device setup** provides any initial setup required by the device before, during, and after the enrollment process.
- ✓ **Device configuration** provides services for saving and restoring device configuration information for applications such as dialer, web browser, mail and TCP/IP.
- ✓ **Rest page management** is a type of software configuration for device-resident initial start page. The rest page may contain clickable icons, and advertising remotely changed by the ISP. DMS provides a way to distribute rest pages to devices.
- ✓ **Software package definition**: name, version, hardware and software prerequisites.
- ✓ **Software distribution** with ability to distribute to certain groups of users, or to users that have specific offerings.

6.1.1.3 Integration with 3rd Party Subscription Management Systems

Integration with 3rd party subscription management systems can be accomplished using the TPSM Transaction facility, Device Resource API and Job API.

6.1.1.4 Accounting

TPSM supplies a programming interface through which a 24-byte accounting record can be generated and provided to a 3rd party billing engine. This capability can be used to customize event tracking and billing for each WebSphere Everyplace Suite end-user.

6.1.1.5 Administrator Console

TPSM provides an administration console that enables management of subscribers and devices. It supports the following operations:

- ✓ Management of devices, device groups and device-specific software resources.
- ✓ Scheduled distribution of software and device configuration to groups of devices.
- ✓ Device-class specific configuration panels.
- ✓ Job-profile based distribution mechanism.
- ✓ Error log viewing.
- ✓ Viewing of device and software inventory.
- ✓ First-connection mechanism to automatically configure newly created devices.

6.1.2 Value

- ✓ Enables you to create a personalized service environment for each subscriber based on their device, their profile, the content they see, and the business offering they subscribe to.
- ✓ Allows you to quickly define new business offerings and make them rapidly available to new subscribers.
- ✓ Reduces the costs associated with self-care and automated device management.

6.1.3 Device Support

Within WebSphere Everyplace Suite, TPSM supports the PalmOS, QNX/Neutrino and Windows CE device platforms.

7.0 Security

7.1 Everyplace Encryption

7.1.1 Description

The WebSphere Everyplace Wireless Gateway supports three types of clients:

- ✓ Everyplace Wireless Clients
- ✓ WAP Clients
- ✓ PPP Clients

7.1.1.1 Everyplace Wireless Clients

Traditional remote access authentication is a uni-directional authentication process in which the remote access gateway must determine whether or not the the client requesting a session is valid. But looking at this process from the other direction, there is no authentication of the gateway by the client. Given that the client requesting a session has submitted a user id and password, how does the client know that it is communicating with a valid gateway? If in fact this gateway is an impostor, the client's id and password have now been intercepted. The impostor can now gain access through the authentic gateway with the intercepted user id and password. To help prevent this situation, it is important to securely authenticate both parties of a remote connection.

IBM addressed this security issue by developing the Two Party Key Distribution Protocol (2PKDP), a sophisticated authentication protocol which enables the advanced bi-directional authentication process used by the Everyplace Wireless Gateway and the Everyplace Wireless Client.

The authentication process is effectively a challenge/response dialogue between Everyplace Wireless Gateway and Client. This process involves two keys, a *secret key* (user password) and a *session key* (encryption password). When a client is configured by the gateway administrator, it is assigned a secret key which is then stored in an encrypted manner on the gateway and communicated (by phone, secure e-mail, mail, etc) to the end-user so that it is known only to both parties. The authentication process is initiated when, as the first step of establishing a session, the client requests a *challenge packet* from the gateway. The gateway then sends the challenge packet which contains a hidden session key. The client can only compute the session key if it knows the secret key, in which case it will respond to the gateway indicating its knowledge of the secret key and the session key. The gateway will then acknowledge a correct response from the client and accept the client's request for a session. It should be noted that the secret key is never transmitted during the authentication process or at any other time. In this way, IBM's 2PKDP security technology directly addresses the security risks associated with uni-directional authentication and their associated transmission of passwords.

7.1.1.2 WAP Clients

The Wireless Application Protocol is a set of defacto standards for the presentation and delivery of wireless information on mobile phones and other types of wireless terminals. The Everyplace Wireless Gateway supports the WAP 1.2 specification. As part of WAP 1.2, Internet security is extended to wireless phones through the use of the Wireless Transport Layer Security specification (WTLS). WTLS was designed to allow for security-rich transactions without requiring the handsets to have the same level of processing power and memory as desk top systems. WTLS is the equivalent of SSL for wireless devices.

7.1.1.3 PPP Clients

A Point-to-Point Protocol (PPP) client is also supported by the Everyplace Wireless Gateway. A client using PPP may authenticate itself using either the Password Authentication Protocol (PAP) or the Challenge Handshake Authentication Protocol (CHAP) using a user id and password.

For each type of client, authentication is a prerequisite for the encryption of communication between the gateway and client. Encryption helps to prevent inappropriate access to the data exchanged between the gateway and client by transforming the transmitted data into an unintelligible form using the session key exchanged during the authentication process. With this process, encrypted data can only be decrypted by someone who possesses the session key.

Everyplace Wireless Gateway supports three different, commonly used encryption algorithms, DES, Triple DES and RC5. When the client software is installed on a workstation, the administrator must choose the type of encryption that is desired, either DES, Triple RC5 or no encryption. If data encryption is enabled on the client, then all IP packets flowing between the gateway and client will be encrypted with either DES, Triple DES or RC5.

There are three security options to help protect your network, applications and data:

Client validation
This option determines what validation is required when a wireless client initiates a session with Everyplace Wireless Gateway. Whenever a client logs in to the gateway, the gateway must have a user name to associate with that client session. This name will be used for logging and tracing. The user name can be identified in several ways: it can be entered at the client, derived from the identifier of the mobile device being used, or it can be a default value.

Administrator access
With the gatekeeper function, you can organise your wireless resources into operational units, and then specify the types of access that each administrator has to each type of resource in each unit. By planning the organisational structure of your resources, you can give administrators as much or as little access as you wish.

This option is independent of the device and so applies equally to all pervasive devices, including wired PDAs, for example.

Data traffic control
For security purposes and to avoid transmitting packets to a wireless client which shouldn't receive them, Everyplace Wireless Gateway provides for packet filtering mechanisms. Packet filtering also reduces the traffic on the wireless link. Filtering mechanisms may also be used to restrict or explicitly permit selected mobile users to access specific IP address ranges.

7.1.2 Value

Through advanced security technologies, Everyplace Encryption provides data protection against unauthorised access while being transmitted between the Everyplace Wireless Gateway and the client device. Everyplace Encryption also protects stored data, applications and networks from unauthorised access through the gateway.

7.2 Firewall Support

7.2.1 Description

Firewalls are frequently at the heart of a well architected security scheme. Rather than disrupting an existing security architecture by providing an integrated firewall, WebSphere Everyplace Suite is specifically designed to integrate easily and quickly with IBM Secureway Firewall (available separately as an optional purchase) and firewall products from other vendors such as Check Point.

7.2.2 Value

Companies can take advantage of WebSphere Everyplace Suite's firewall support to establish an infrastructure that will enable safer, more secure e-business by controlling communications to and from the Internet.

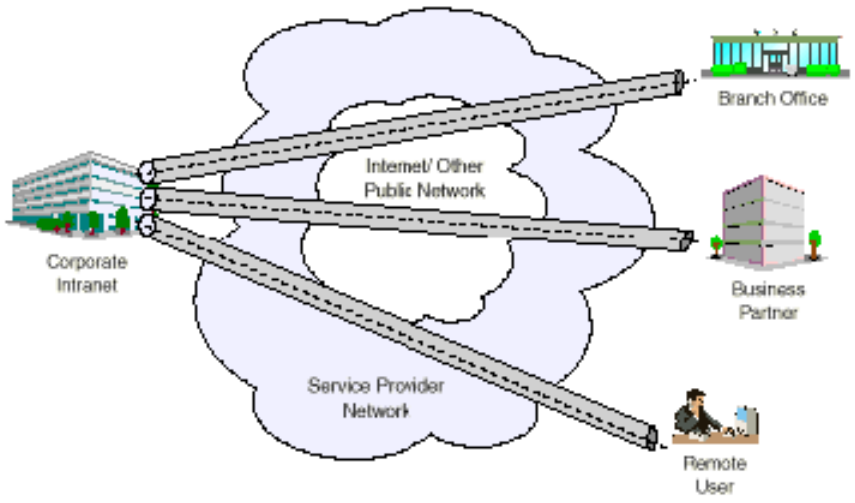
7.3 Virtual Private Network Support

7.3.1 Description

WebSphere Everyplace Suite is designed to integrate with the Virtual Private Network feature of the IBM Secureway Firewall (available separately as an optional purchase) and as such includes the advanced security technologies that are essential to constructing a safer virtual private network (VPN):

- ✓ **IP Security** (IPSec) provides end-to-end protection as well as segment-by-segment protection. Based on the work of the Internet Engineering Task Force, IBM chose to incorporate IPSec support into its WebSphere Everyplace Suite and Virtual Private Network products.
- ✓ **Layer-2 tunnelling** and **remote access authentication servers** provide the necessary additional flexibility to apply adequate security to any given VPN configuration.

The popularity of the Internet as a far reaching, low-cost backbone infrastructure, has led many companies to consider constructing a secure VPN over the public Internet. A VPN is an extension of a private intranet across a public network, such as the Internet, to create a more secure privateconnection through a private "tunnel", as shown in the diagram below.



7.3.2 Value

With WebSphere Everyplace Suite and Virtual Private Networks, companies can now more safely and cost-effectively extend the reach of their applications and data across the world through the implementation of security-rich VPN solutions.

Internet service providers (ISPs) offer cost-effective access to the Internet (via direct lines or local telephone numbers), enabling companies to eliminate their current, expensive, leased lines, long-distance calls, and toll-free telephone numbers. A 1997 VPN Research Report, by Infonetics Research, Inc., estimates savings from 20% to 47% of wide area network (WAN) costs by replacing leased lines to remote sites with VPNs. And, for remote access VPNs, savings can be 60% to 80% of corporate remote access dial-up costs. Additionally, Internet access is available world-wide where other connectivity alternatives may not be available.

8.0 Performance Optimization

8.1 WebSphere Edge Server

8.1.1 Edge Server Caching Proxy

The Edge Server Caching Proxy provides highly scalable caching functions associated with receiving requests and serving URLs. With tuneable caching capable of supporting high cache hit rates, this component can help reduce bandwidth costs and provide more consistently rapid customer response times. Using Edge Server Caching Proxy, "Unable to Connect to Server errors", which today are so frequent, can be reduced.

Edge Server Caching Proxy is a proxy server, which means that it assumes the responsibility for retrieving Internet data for multiple browser clients. Client requests are sent to the Web servers through the proxy. In other words, the client may be configured to send its request to the proxy first, and then it is the proxy that forwards the client's request to the Web server, acting on behalf of the originating client. The Web server does not even see the IP address of the client in the packet headers, but only the IP address of the proxy server. Once the proxy receives the information from the Web server, it forwards the information to the requesting client.

A traditional proxy server receives a request for a URL from a client and then forwards the request to the destination Web server. Edge Server Caching Proxy uses an innovative caching scheme from IBM Research Laboratories. Its highly configurable design allows you to customise its advanced caching features to suit your own needs. For example, Edge Server Caching Proxy allows you to specify which of the Web pages and documents it retrieves are to be cached, when the information on a page will expire, how large to make the cache and when to update it. Edge Server Caching Proxy can then serve subsequent requests for cached documents from its local cache. The benefit here is that the client device receives the required information faster while bandwidth utilisation and associated costs are reduced.

When used in conjunction with Edge Server Load Balancer, WebSphere Everyplace Suite becomes a massively scalable solution.

8.1.1.1 Optimisation

The Edge Server Caching Proxy cache design provides a very efficient mapping of URLs onto the cache file system. This provides quicker retrieval of cached objects, more efficient use of disk space within the cache, and quicker cache garbage collection. The cache also uses write-behind techniques for greater throughput. Additionally, Edge Server Caching Proxy now includes caching of Domain Name Server (DNS) lookup results, giving quicker response time and further reducing network load.

The caching proxy function provided by Edge Server Caching Proxy is valuable to service providers and enterprises needing to optimise line costs and performance associated with accessing remote Web sites. Customers that can benefit from using the caching and proxy function of a caching proxy server include:

- ✓ **Service providers** needing to provide good response time to clients from Web sites accessible only via expensive or distant links that experience significant propagation delay time. They need to be able to provide non-disruptive access to information on servers located within their networks as well as those external to their networks. For example, many ISPs must have infrastructures capable of cost-effective expansion to handle growth rates greater than 10% per month.
- ✓ **Enterprises** wanting to optimise wide-area line usage.

8.1.1.2 Value

Edge Server Caching Proxy provides a valuable and scalable solution to some of the major traffic management problems. These are the main benefits it offers:

- ✓ Reduction of costs and constraints on network bandwidth, particularly during periods of peak concurrent activity.
- ✓ Scalable infrastructure that provides cost-effective growth paths and high capacity potential with minimum redesign or disruption.

Edge Server Caching Proxy provides these benefits irrespective of browser type. For example, WAP phone browsers, PalmOS browsers and EPOC browsers each receive equal benefit from Edge Server Caching Proxy.

8.1.2 Edge Server Load Balancer

The number of users and networks connected to the Internet is growing exponentially. This growth is causing problems of scale that can limit users' access to popular sites. Currently, network administrators are using numerous methods to try to maximise access. Some of these methods allow users to choose a different server at random if an earlier choice is slow or not responding. This approach is cumbersome and inefficient. Another method is the standard "round-robin", in which the DNS server selects TCP servers in turn to handle requests. This approach is better, but still inefficient because it blindly forwards traffic without any consideration of the server workload. Even if a server fails, requests will continue to be sent to it, and users will experience serious access problems.

The need for a more powerful solution has resulted in the development of Edge Server Load Balancer. It offers numerous benefits over earlier and present day competing solutions. Edge Server Load Balancer is a server that dynamically monitors and balances TCP servers and applications in real time. The main function of the load balancing component is that it allows heavily accessed Web sites to increase capacity, since multiple TCP servers can be dynamically linked in a single entity that appears in the network as a single logical server. This load balancing software improves the performance of servers by distributing TCP/IP session requests in a more intelligent way than the standard round-robin.

Edge Server Load Balancer is derived from a proven IBM technology used to load balance TCP traffic on many of today's most active web sites, including some that have been used to support some of the highest profile sporting events over the past few years. Examples include the Web sites for the Masters Golf Tournament, Wimbledon Tennis Championship, French Open Tennis Championship, U.S. Open Tennis Tournament, the ACM Chess Challenge sites (Gary Kasparov vs IBM's Deep Blue chess playing super-computer), and the Olympic Games Web sites, which have withstood many thousands of hits per minute.

Edge Server Load Balancer is very useful for applications such as e-mail servers, World Wide Web (WWW) servers, distributed parallel database queries, and many other TCP/IP applications. When used with web servers, it can help maximise the potential of a web site by providing a powerful, flexible, and scalable solution to ensure that the site remains responsive to incoming requests. Edge Server Load Balancer also increases availability by performing "dynamic take-over" if a server fails. This allows the server to be taken out of service for maintenance or reconfiguration without disrupting end-user availability.

Within WebSphere Everyplace Suite, Edge Server Load Balancer is used to balance the load across servers performing the same kind of function. For example, a WebSphere Everyplace Suite configuration may require multiple processors to execute its TPSM or WebSphere Transcoding Publisher components. In these scenarios, Edge Server Load Balancer will distribute each of the loads (TPSM or WebSphere Transcoding Publisher) across like-function servers so as to provide very high levels of availability.

Edge Server Load Balancer consists of three sub components that can be used separately or together to provide superior load-balancing results:

- ✓ Dispatcher
  You can use the Dispatcher component by itself to balance the load on servers within a local area network (LAN) or wide area network (WAN) using a number of weights and measurements that are dynamically set by Dispatcher. This function provides load balancing at a level of specific services, such as HTTP, FTP, SSL, NNTP, POP3, SMTP, and Telnet. It does not use a DNS server to map domain names to IP addresses.

- ✓ Interactive Session Support
  You can use the ISS component by itself to balance the load on servers within a local or wide area network using a DNS round-robin approach or a more advanced user-specified approach. Load balancing is performed at the machine level. ISS can also be used to provide server load information to a Dispatcher machine. When used for load balancing, ISS works in conjunction with the DNS server to map DNS names of ISS services to IP addresses. When used to provide server load information, a DNS is not required.
- ✓ Content Based Routing
  The CBR component works along with Edge Server Caching Proxy to load balance client Web requests to specified servers; the routing is determined by comparing the content of the request to rules that have been defined in the CBR component.

8.1.2.1 Value

- ✓ **Scalability**
  As the number of client requests increases, you can add servers dynamically, providing support for millions of requests per day on multiple servers.

- ✓ **Efficient use of equipment**
  Load balancing ensures that each group of servers makes optimum use of its resources by minimising the hot-spots that frequently occur with a standard round-robin method.

- ✓ **Easy integration**
  Edge Server Load Balancer uses standard TCP/IP protocols. You can add it to your existing network without making any physical changes to the network (provided the servers are all on LANs). It is simple to install and configure.

- ✓ **Low overhead**
  Edge Server Load Balancer needs only to look at the inbound client-to-server flows. It does not need to see the outbound server-to-client flows. This significantly reduces its impact on the application compared with other approaches and can result in improved network performance.

- ✓ **Non-invasive technology**
  Edge Server Load Balancer does not modify any packets, nor does it require any modifications to the operating system on which it runs.

- ✓ **Content Based Routing**
  CBR gives an Edge Server Caching Proxy administrator the ability to proxy requests to specific servers based on the content requested.

- ✓ **High Availability**
  The Dispatcher component of Edge Server Load Balancer offers built-in high availability, utilising a standby machine that remains ready at all times to take over load balancing should the primary Dispatcher machine fail.

ISS is intrinsically highly available. All the nodes in an ISS configuration work together to eliminate any single point of failure within ISS.

CBR does not offer a high availability feature, but multiple CBR machines can be load balanced by an additional Edge Server Load Balancer machine; if a CBR machine should unexpectedly fail, the Edge Server Load Balancer server realises it and directs traffic around the failing machine. This way, CBR high availability can be achieved as well.

- ✓ **Collocation option**
  The Dispatcher component can be installed on the same machine where one of the application servers reside. This option is particularly useful if you want your Web site to benefit from the high availability and scalability options of the Load Balancing component with a minimal investment. The collocation option is currently available on AIX and Solaris platforms.

8.2 Gateway Optimisation

Everyplace Wireless Gateway optimises communication over the wireless link by implementing a range of optimisation techniques that reduce traffic:

Compression enables the size of each IP packet to be reduced in a way that it can completely be restored at the receiver. This is done without having any knowledge of the content of the IP packet. This increases the effective data rate of the wireless network. It also decreases the amount of data to be transmitted and therefore transmission costs in most cases.

TCP Header Reduction minimises redundancy in TCP traffic. TCP normally adds a 40-byte header to each packet it transmits. But for a point-to-point connection between the Gateway and Client, some of the fields in the TCP header are redundant and can be removed. Everyplace Wireless Gateway removes these redundant header fields.

Retransmission Optimisation reduces the number of packet retransmissions over TCP. This common and wasteful problem is caused by insufficient bandwidth availability or high latency over the wireless link. Retransmission optimisation in the Gateway and Client addresses this problem.

Short Hold Mode helps reduce air time on connection-oriented wireless networks and PSTN. In short-hold mode there is no established physical connection over the mobile network, but client and gateway remain *virtually* connected. If the client or gateway is requested by the IP stack to transmit an IP packet, this component will re-establish the physical connection and start the transmission immediately. Short-hold mode is entered when there is no traffic on the line for a certain amount of time. Both the Gateway and Client have a timer configured after which the short-hold mode will be initiated. To enter the short-hold mode, one party simply hangs up the line.

Short-hold mode is also useful when the connection set-up time is relatively short (as in GSM networks connected to the gateway over ISDN - roughly 10 seconds) and for recovering from connection breakdowns on cellular switched networks. Since none of the parties in a wireless connection can determine if short-hold mode has been entered due to the fact that the opposite party intended to, or the connection was interrupted by the wireless network provider, the connection will automatically recover when one party wants to transmit a packet.

9.0 Base (Common) Services

WebSphere Everyplace Suite is integrated around two key base services:

- ✓ A central directory which stores runtime information
- ✓ A single, unified console which provides a common view of all aspects of the suite.

9.1 SecureWay Directory

SecureWay Directory is a highly scalable and robust Lightweight Directory Access Protocol (LDAP) directory server that is integrated into WebSphere Everyplace Suite. This LDAP database is the central repository for the various categories of runtime information that are necessary to support an active user of WebSphere Everyplace Suite.

SecureWay Directory is optimised for read access by multiple applications and consequently brings performance and scaleability benefits to WebSphere Everyplace Suite while avoiding the high costs associated with maintaining multiple databases. For example, new servers can be added to a WebSphere Everyplace Suite configuration without having to duplicate the runtime database.

9.2 Everyplace Suite Console

Everyplace Suite Console provides a single web-based operator console for WebSphere Everyplace Suite that provides navigation and integration across the subcomponent consoles, such as the Everyplace Wireless Gateway and TPSM consoles for example.

Specifically, Everyplace Suite Console enables system administrators to perform the following procedures from a single interface:

- ✓ Installation
- ✓ Configuration
- ✓ Diagnostics
- ✓ Administration
- ✓ System maintenance

It should be noted that the WebSphere Everyplace Suite installation program is designed to permit any combination of its components to be installed on any machine. We do not force any minimum set or combination to be installed.

10.0 Trademarks and Disclaimer

10.1 Trademarks

Java is a trademark or registered trademark of Sun Microsystems, Inc. in the United States and other countries.

Windows, Windows NT, Windows CE and Windows 2000 are trademarks of Microsoft Corporation. Other company, product, and service names may be trademarks or service marks of others.

10.2 Disclaimer

IBM reserves the right to alter specifications and other product information without prior notice. This publication could include technical inaccuracies and typographical errors. Reference herein to IBM products and services do not imply that IBM intends to make them available in all countries. IBM provides this publication “as is” without warranty of any kind, either express or implied, including the implied warranties of merchantability or fitness for a particular purpose. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions; therefore, this disclaimer may not apply to you.