

Cingular Wireless



Configuration Orange Paper
Cisco Wireless VPN

Data Connect
Enterprise Solutions



Configuration White Paper – Cisco Wireless VPN

Cingular would like to thank Cisco for their contribution to and validation of the information contained within this document.

Table of Contents

Overview	3
Assumptions.....	7
Step One:.....	8
(Optional)	9
Step Two:	9
Step Three:	12
Additional Support.....	13
Appendix A - Definitions	15

Conventions Used in this Guide

Throughout this guide there are several conventions that are used to make it easier for you to identify notes and examples. They are as follows:



NOTE: This icon/symbol is used to identify a note regarding previous text.



EXAMPLE: This icon/symbol is used to identify an example regarding previous text.

LEGAL NOTICE

This document is intended to help with your configuration of the Data Connect service to work with your enterprise VPN. No warranties express or implied are hereby created. This document is not a part of your contract for Cingular Service. All company, brand, and product names are referenced for identification purposes only and may be trademarks that are the sole property of their respective owners.

Copyright © 2003 Cingular Wireless All rights reserved. Version 1.0



Configuration White Paper – Cisco Wireless VPN

Overview This paper addresses enterprise management's business requirements for connectivity between wireless subscriber mobile devices and the corporate enterprise network. Cellular network features and benefits that have recently been made available (2.5G) and which continue to evolve (3G) provide increasingly effective connectivity to the enterprise for mobile users. Secure, wireless communications between laptops and PDA's is now possible by implementing the recommendations highlighted in this paper.

Enterprise Security Evolution: VPN Enterprises have become more global, with workforces that are both mobile and geographically dispersed. Many such enterprises have facilities across the United States and around the world. In this environment of continual evolution, enterprises share a common requirement: define and implement an effective method for maintaining secure, reliable, and effective communications between the enterprise and virtually any user location.

As the popularity of the Internet continues to grow, businesses increasingly turn to it as a means of extending their own private networks. Intranets, which largely comprise the private enterprise connectivity infrastructure and which require secure, password-protected access, are typically deployed for use only by company employees and other similar closed user groups. Now, many enterprises are enabling **VPNs**, or **Virtual Private Networks**, to accommodate the secure connectivity requirements of mobile employees and distant offices. VPNs provide required functionality and valuable benefits to the enterprise, including the following:

- **Security** - The highest level of security using advanced encryption and authentication protocols that protect data from unauthorized access.
- **Savings** - Organizations utilize cost-effective third- party Internet transport to connect remote offices and users to the main corporate site, eliminating expensive, dedicated WAN links and modem banks.
- **Scalability** - Corporations utilize easy-to-provision and scale Internet ISP infrastructure and devices. Thus, increasing their capacity without adding significant infrastructure investment.

Numerous third party solutions (e.g. Cisco) are now available to provide secure VPN connectivity for remote workers and branch offices using standard IP Security (IPsec) technology.



Configuration White Paper – Cisco Wireless VPN

Increasing the ROI of Existing VPN Investment

Cingular understands the enterprise need to effectively support remote workers with secure corporate network connectivity. By wirelessly enabling the corporate Intranet, the enterprise can expand VPN benefits to include:

- **Mobility** - A company can provide secure Intranet access to remote and mobile workers. This secure connectivity can offer greater employee uptime, productivity enhancements, reduced need for multiple information input, better support of remote/telecommuter workers, and reduced transit time and costs for remote workers.
- **Increased ROI** - Increase the ROI of existing VPN investments by extending the corporate network into the wireless environment, helping companies increase productivity, effectiveness, and support of remote and mobile workers.

VPN Overview

In providing a wireless VPN solution, it is important to recognize that the IPsec standards were originally developed and optimized for providing the high level of security and privacy demanded by global enterprises on landline based networks. IPsec was not necessarily optimized for efficient operation over wide area wireless data networks such as those currently available from wireless carriers including Cingular Wireless. Consideration of the basic elements of the wireless VPN will help clarify. Figure 1 below shows the elements of the Wireless VPN.

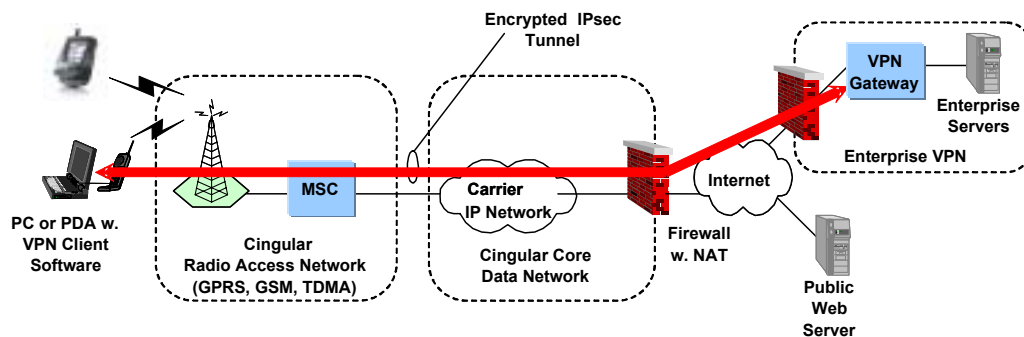


Figure 1

This example illustrates a “user-initiated” VPN where the secure tunnel spans the entire distance between the mobile device and the enterprise Intranet. At the highest level, the typical VPN solution consists of a remote user with a laptop or PDA computing device, with a VPN client; an enterprise network (Intranet) protected from the public Internet by a VPN firewall; and a public wireless data network that can provide connectivity between the remote user and the public Internet.

While working together, all of these elements provide secure communications across the public wireless data network and the public Internet. The remote computer employs a software product called a VPN Client. This software encrypts the network traffic before it leaves the computer, and forwards all of this traffic to a single IP address of the VPN server which is inside their secure enterprise network. The VPN server performs the reverse function of the VPN Client, de-encrypting the traffic and routing the original IP packet to its final destinations inside the enterprise. The VPN server authenticates the VPN Client before allowing this connection, verifying the identity of the remote user via a password, secure token, or public certificate.



Configuration White Paper – Cisco Wireless VPN

Client / Server

Users of third party VPN Client/Server products (e.g. Cisco) can securely communicate over the wired Internet, or wireless data networks such as that used by Cingular Wireless' Data Connect service. Some of the challenges of supporting these third-party VPN products over a wide-area wireless data network are discussed in the following section.

Wireless VPN Challenges

There are two key challenges for users of commercial VPN client / server products over a public wireless network:

1. Operation through a firewall with Network Address Translation (NAT)
2. Bandwidth Overhead penalties caused by IPsec

The Cingular Wireless data network protects its wireless users and its own network infrastructure from unauthorized access and attacks by using a firewall at its boundary with the public Internet. Similar to other wireless service providers, Cingular is sensitive to the need to conserve the dwindling pool of available public IP addresses while serving millions of wireless subscribers. Hence this firewall also employs Network Address Translation (NAT) to convert the mobile device's private IP address into a shared public IP address as its data crosses into the public Internet. In addition, the NAT function also helps to further protect mobile users by masking their actual IP addresses from exposure on the public Internet.

NAT technology is commonly employed in most Cable and DSL access equipment (Linksys, D-Link) used by high speed Internet home subscribers today. The IPsec standards have been enhanced in recent years to operate correctly over a NAT connection, but this requires most third party VPN client / server users to verify that their VPN client and server settings are configured to support this mode correctly. NOTE: Detailed instructions on how to ensure your Cisco VPN operation is configured* correctly over Cingular's Data Connect network is outlined later in within this document.

The issue of bandwidth overhead caused by VPN client solutions arises primarily from the additional headers added to every packet by the VPN software. The figure below shows that the most common IPsec configuration used by VPN clients will add 62 bytes to every packet sent or received by a VPN user. Figure 2 below shows IPsec Tunnel Mode with UDP Encapsulation, and indicative of 30% or more overhead caused by IPsec encryption.

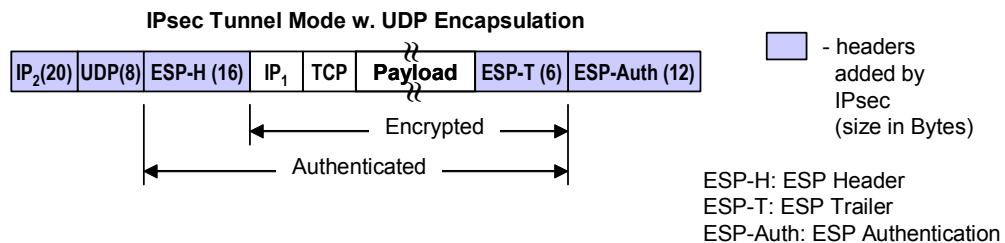


Figure 2



Configuration White Paper – Cisco Wireless VPN

IPsec

IPsec encryption equates to a 30% (or more) reduction in the bandwidth available to the user over a network already challenged for bandwidth with respect to a non-wireless network such as DSL. Figure 3 below also shows 30% or more overhead caused by IPsec encryption.

Connection Type	Raw Link Bandwidth (Overhead Included)	Overhead	Net VPN Bandwidth (30% Overhead Subtracted)
TDMA Circuit Switched	9.6 Kbps	30% or more	6.7 Kbps
GSM Circuit Switched	14.4 Kbps	30% or more	10.1 Kbps
GPRS	30 - 40 Kbps	30% or more	21 - 28 Kbps
EDGE	60 - 90Kbps	30% or more	42 - 63Kbps

Figure 3


Cingular recognizes this bandwidth impact, and is working to provide additional solutions. They are:

- Recommendations from Cingular regarding how to configure* your Cisco VPN to take advantage of data compression capabilities inherent in those VPN server and clients (see later sections of this paper). These compression capabilities can help to regain performance loss caused by the VPN overhead.
- Solutions in the near future that offer and/or support enterprise Data Acceleration products. These products will counteract the impacts of VPN overhead, providing additional optimized throughput performance significantly above that which would otherwise be realized.

The remainder of this document provides information on how to configure existing Cisco wireline VPN solutions to function efficiently with Cingular Data Connect



Configuration White Paper – Cisco Wireless VPN

 **Note: The configuration changes recommended in this document are only required to ensure efficient operation over the Cingular Wireless network – these changes do not have any negative impact on the privacy or security of your enterprise data.**

Setup and Configuration of Cisco VPN

Assumptions

Prior to installing and configuring the VPN and QLM Clients on the PC or PDA device, the following assumptions should be considered

1. Cisco VPN Tunnel Server (version 3.6.7 or greater) has been installed, configured, connected to the Internet, and tested across a wired network connection with a Cisco VPN Client
2. Cisco VPN Client (version 3.6.3 or greater) has been installed, configured and tested to work across a wired connection.
3. Cingular recommended data capable phone / pc-card and corresponding data kit have been procured.
4. The user's SIM card (GSM only) has been provisioned for GPRS Wireless Internet Express (or Wireless Internet if CSD connection is being used).
5. Cingular QuickLink Mobile (QLM) Client has been installed from CD and Internet connectivity has been tested.



Configuration White Paper – Cisco Wireless VPN



Three Steps to Setting up VPN

Step One:


Configuring the Cisco VPN Server for Cingular's Network

NAT support must be enabled on the Cisco VPN Concentrator.

Use the following procedure to configure NAT transparent mode on the VPN Concentrator.

- 1)  On the VPN Concentrator, go to Configuration > User Management > Groups.
- 2)  To add a group, select Add. To modify an existing group, select it and click Modify.

Click the IPsec tab, check IPsec through NAT and configure the IPsec through NAT UDP Port. The default port for IPsec through NAT is 10000 (source and destination), but this setting may be changed

 **This completes the modifications that are needed to enable the Cisco VPN Server to establish secure connectivity using Cingular Data Connect service.**

For additional information on NAT configuration, go to:
http://www.cisco.com/warp/customer/471/nat_trans.pdf

http://www.cisco.com/en/US/products/sw/secursw/ps2276/products_configuration_example09186a008010edf4.shtml




(Optional)

Setup and Configuration of Cisco VPN Server Connection Compression

Cingular recommends that you configure your Cisco VPN to take advantage of data compression capabilities inherent in the Cisco VPN server and client (include actual location of this info). These compression capabilities can help to regain performance loss caused by the VPN overhead.

If a new profile is created that will be unique to wireless VPN users, it may be appropriate to enable “IP Compression” in order to provide improved performance for your wireless VPN users. You can find the “IPComp” setting for your group under:

 **Configuration > User Management > Groups > your_group_name > IPsec**

On the Cisco 3000 concentrator.



Enabling IP compression has an impact on the total user capacity of the VPN concentrator. To that end it is not recommended to enable this option for a Group that includes a large number of users, or users who are near the rated concentrator capacity. In addition, do **not** enable this option for Groups containing users who will also be using broadband access networks to connect to the enterprise VPN. If it is decided to enable compression for the wireless VPN Group, simply change the “IPComp” setting from “None” to “LZS”. (**Note:** For questions relating to the option indicated above, please contact local Cisco Customer Support)


 **This optional step completes the modifications that are needed to enable Compression within the Cisco VPN Server.**

Step Two:

Configuring the Cisco VPN Client for Cingular’s Network

To configure the Cisco VPN Client to establish a secure tunnel across the Cingular Wireless network, two primary activities need to take place:

- 3)  Cingular and Cisco both recommend Maximum Transmission Unit (MTU)* must be set to 1300
- 4)  Cisco VPN Client must be configured for IPsec over UDP to support NAT.



 *MTU sizing affects fragmentation of IPsec and IPsec through NAT mode packets to your connection destination. Fragmentation increases with larger sizes (e.g 1400+). To prevent fragmentation, it is recommended that MTU be 1400 or smaller. Fragmentation and reassembly of packets at the destination causes slower tunnel performance, and many firewalls do not let fragments through.

The following diagrams are provided to assist the enterprise user with configuring the MTU and UDP encapsulation of Ipsec. However, as versions change, screens may be modified. Please refer to the Cisco Documentation for the latest procedures that are available at: <http://www.cisco.com>



Configuration White Paper – Cisco Wireless VPN

Step 2 Cont.

1.  Modify the MTU, click on the SetMTU icon under the Cisco VPN Client tab.
2.  Select the “Cingular Wireless Internet Express” (GPRS), or “Cingular Wireless Internet” (CSD) Network Adapter and select 1300. Click OK. .

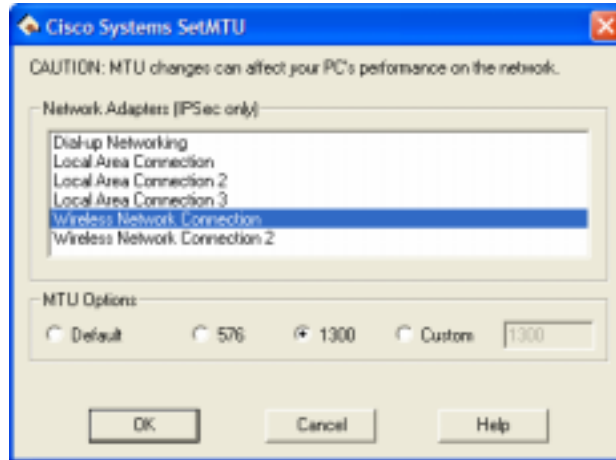




Diagram 1: MODIFYING MTU

1.  Select the Options; and then select properties
2.  Select the “Allow IPsec over UDP (NAT/PAT). Timeout should be set to 90 seconds.



Configuration White Paper – Cisco Wireless VPN

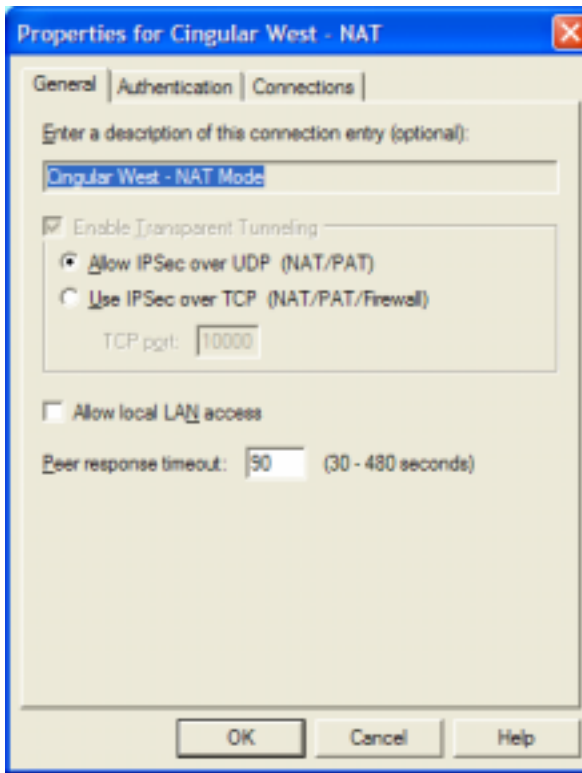



Diagram 2: ENABLING NAT SUPPORT (UDP ENCAPSULATION OF IPSEC)

Step 2 Cont

 This step completes the modifications that are needed to enable the Cisco VPN Client to establish secure connectivity using Cingular Data Connect service.

Additional information is available on the following

Installing and troubleshooting the Cisco VPN client: http://www.cisco.com/en/US/products/sw/secursw/ps2308/products_administration_guide_chapter09186a00800ecaa2.html



Configuration White Paper – Cisco Wireless VPN

Step Three:


Setup of the Cingular *Data Connect* – QuickLink Mobile current version:


(Please note: To setup the QLM for the first time, you should reference the Quick Start Guide that is included with the purchase of any Mobile Office Kit or Data Connect PC Card.)

To configure QLM to work with the Cisco VPN Client, you may need to disable Data Acceleration per the following instructions. Note: the user can re-enable this option later if they want to initiate a non-VPN connection.

 Launch the QuickLink Mobile application.

Click the QLM "Menu" button, select "Preferences", and then click on the "Data Acceleration" tab.

 In that tab, un-check the "Data Acceleration" option (since the network acceleration can not provide any benefit for the encrypted VPN connection). Note that the user can re-check this option later if they want to initiate a non-VPN connection.

 Select the account type ("Cingular Wireless Internet Express" for GPRS, or "Cingular Wireless Internet" for CSD) and click the Connect button to start a wireless session



This completes the modifications that are needed to enable the Data Connect - QLM Client to establish secure connectivity using Cingular Data Connect service.

Establishing the VPN Connection:

Once the wireless connection is active; all the user needs to do is to select the Cisco VPN Dialer and click "Connect" to establish the secure VPN tunnel

Cingular Continues to Develop Better Solutions

Cingular is dedicated to effectively addressing the needs of the enterprise customer. As part of that effort, Cingular is developing solutions that will offer and/or support an Enterprise Data Acceleration product which will counteract all of the VPN overhead, and provide additional acceleration above and beyond that so that the wireless VPN session will have better performance than a normal non-accelerated session would have without a VPN.



Additional Support

Additional Cisco VPN information and support is available from the following sources:

Cisco VPN Client User Guide:

http://www.cisco.com/application/pdf/en/us/guest/products/ps3866/c1629/ccmigrati on_09186a00800b6217.pdf

Cisco VPN Client Datasheet and Feature Comparison:

http://www.cisco.com/warp/public/cc/pd/vpnc/vpncl/prodlit/clvpn_ds.pdf

Cisco VPN Client Q&As:

http://www.cisco.com/en/US/products/sw/secursw/ps2138/products_qanda_item09186a00800925ee.shtml

NAT Configuration:

http://www.cisco.com/warp/customer/471/nat_trans.pdf or
http://www.cisco.com/en/US/products/sw/secursw/ps2276/products_configuration_example09186a008010edf4.shtml

Cisco Technical Assistance Center (TAC) Web Site

Use the Cisco TAC Web Site to resolve P3 and P4 issues, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

<http://www.cisco.com/tac>

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register: <http://www.cisco.com/register/>

If a Cisco.com registered user cannot resolve technical issues by using the Cisco TAC Web Site, a case can be opened online by using the TAC Case Open tool at this URL: <http://www.cisco.com/tac/caseopen>

Cingular recommends that P3 and P4 cases be opened through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When contacting the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case. To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>



Configuration White Paper – Cisco Wireless VPN

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number

Still have VPN questions?

For questions regarding your VPN solution, call:

Cisco Customer Service: 800-553-NETS

Cisco Tech Assistance Center: 800-553-2447

For questions regarding your Cingular Wireless service:

Cingular Customer Service: 1-866-CINGULAR (mention key words “VPN with Data Connect ”)



Appendix A - Definitions

Term	Definition
2.5G	Two and a half Generation wireless network.
3G	Third Generation wireless network.
APN	Access Point Name. The service description and routing for GPRS data for application use.
CSD	Circuit Switched Data. Cingular operates at 9.6kb on both TDMA and GSM networks. Cingular's product name for CSD is Wireless Internet.
Data Connect	Data Connect is Cingular's service that provides CSD and GPRS network access via Laptop or PDA's to Direct IP via Cingular or to an ISP of the user's choice via PSTN dial-up. Data Connect is not a separate offering and is a service <u>included</u> in the Wireless Internet or Wireless Internet Express, and Wireless Internet Express – Pay Per Use offerings.
DSL	Digital Subscriber Line - high speed Internet access technology using standard copper phone wires into a home or business.
EDGE	Enhanced Data for GSM Evolution - new higher speed evolution of GPRS / GSM data.
ESP	Encapsulating Security Protocol – a protocol used by IPsec for secure communications.
GPRS	<p>General Packet Radio Service. General Packet Radio Service is the packet data transmission or bearer service for GSM networks. GPRS is provisioned via specific APN profiles.</p> <p>Cingular runs its GPRS in parallel with its existing GSM networks. It uses the same basic radio station infrastructure as the GSM network and complements, not replaces, existing WAP, SMS, and CSD technologies.</p> <p>Benefits of GPRS include the following:</p> <ul style="list-style-type: none"> • An “Always Registered” platform is provided for a large range of new applications. • Potential access speeds can provide up to 10 times faster connections than the current CSD methods. • A subscriber can connect to the network in roughly half the time compared to CSD modem connect time. • GPRS speeds generally vary between 10 and 40 kilobits per second, depending upon network conditions. • Subscribers can seamlessly toggle between voice and data without losing their data connections. <p>Cingular's product name for GPRS is Wireless Internet Express or Wireless Internet Express – Pay Per Use.</p>
GSM	Global System for Mobile (Communications) – a digital wireless network technology.
IP	Internet Protocol
IPsec	Internet Protocol Security
ISP	Internet Service Provider



Configuration White Paper – Cisco Wireless VPN

Kbps	Kilobits per second – 1024 bits per second.
MTU	Maximum Transmission Unit – the maximum size of a packet that will be sent over a network link.
NAT	Network Address Translation is the translation of an Internet Protocol address used within one network to a different IP address known within another network. One network is designated the <i>inside</i> network and the other is the <i>outside</i> . Typically, a company maps its local inside network addresses to one or more global outside IP addresses and unmaps the global IP addresses on incoming packets back into local IP addresses. This helps ensure security since each outgoing or incoming request must go through a translation process that also offers the opportunity to qualify or authenticate the request or match it to a previous request. NAT also conserves on the number of global IP addresses that a company needs and it lets the company use a single IP address in its communication with the world.
P1, P2, P3, P4	Priority 1-4 – the severity classification of a network trouble ticket by Cisco Systems.
PAT	Port Address Translation - a function provided by some routers which allows hosts on a LAN to communicate with the rest of a network (such as the Internet) without revealing their own private IP address . All outbound packets have their IP address translated to the routers external IP address. Replies come back to the router which then translates them back into the private IP address of the original host for final delivery.
PDA	Personal Digital Assistant – a handheld computing device.
PSTN	Public Switched Telephone Network.
QLM	QuickLink Mobile – the Cingular network dialer client which is installed on the mobile laptop or PDA, used for Data Connect.
ROI	Return on Investment
SIM	Subscriber Identity Module – used in GSM and GPRS mobile devices.
SMS	Short Message Service
TCP	Transport Control Protocol
TDMA	Time Division Multiple Access – a digital wireless network technology.
UDP	User Datagram Protocol
URL	Uniform Resource Locator – a world wide web address.
VPN	Virtual Private Network - A Virtual Private Network (VPN) is an extension of an enterprise's private intranet across the Internet or other public network. It creates a secure private "tunnel" through the Internet to the other partner.
VPN Client	Cisco's VPN product which runs on the end user's PC or PDA.
WAN	Wide Area Network – a network which spans a wide geographical area.
WAP	Wireless Application Protocol
Wireless Internet	Cingular's offering name for TDMA and GSM CSD networks to use WAP and Data Connect services. This service includes SMS capabilities.
Wireless Internet Express	Cingular's offering name for GPRS networks to use WAP and Data Connect services. This offering includes the CSD and SMS capabilities.