WHITE PAPER

# Mobility Services Platform (MSP)
# Using MSP in Wide Area Networks (Carriers)

# Table of Contents

***Using MSP in Wide Area Networks (Carriers) is a technical brief that provides general information which may aid in planning management of mobile deployments with MSP over Wide Area Networks and more specifically commercial GSM and/or CDMA carrier networks.***

# About This Document

## Overview

Topics covered in this guide are as follows:

- **Chapter 1, Wireless Data Technologies**, a brief summary of available wireless data technologies available via commercial carriers and a comparison of data throughputs.
- **Chapter 2, Wireless Data IP Overview (Carrier Agnostic)**, a brief summary on IP Addressing options available through carrier data plans. The descriptions apply to both GSM and CDMA carrier networks. Relevant impacts for mobile deployments that use MSP (especially remote control) are outlined.
- **Chapter 3, GSM Wireless Data Networks and MSP**, a brief summary of some options generally available from GSM carriers through data plans and their impacts for the mobile enterprise. Some recommended network planning scenarios are presented with regards to MSP.
- **Chapter 4, CDMA Wireless Data Networks and MSP**, a brief summary of some options generally available from CDMA carriers through data plans and their impacts for the mobile enterprise. Some recommended network planning scenarios are presented with regards to MSP.
- **Chapter 5, Bandwidth Considerations and MSP**, a brief summary of bandwidth and throughput considerations for various tasks associated with managing mobile devices with MSP.

## Related Document

- Mobility Services Platform 3.1 User's Guide, p/n 72E-100158-04

# Chapter 1 Wireless Data Technologies

## Wireless Data Technology Overview

Wireless Data as a commercial carrier offering has adopted various wireless standards and has evolved over time with technology improvements in what are called "Generations", or "G" (i.e. 1G, 2G, etc). With each technology improvement introduces higher data rates, additional features, and network enhancements. Figure 1 summarizes some of the technology standards and their evolution path.

GSM (Global System for Mobile Communications) is the dominant global standard for cellular communications. GSM originated in Europe in the late 1980's and has since pervaded international markets. On a global level, GSM represents 80% of global digital subscribers. In the United States the largest wireless carriers for GSM are Cingular (now AT&T) and T-Mobile. GSM data services are defined as Edge, GPRS, UMTS and HSDPA.

CDMA (Code Division Multiple Access) is a digital technology developed by Qualcomm and delivered by various wireless carriers (mostly in North America). CDMA is "spread spectrum" technology allowing many users to occupy the same time and frequency allocations in a given band/space. The CDMA air interface is used in both 2G and 3G networks. It offers good secure coverage in the United States where the largest carriers are Verizon, Sprint, and Alltel. Coverage outside of North America for CDMA is generally not as prevalent as GSM coverage.

The dominant cellular/wireless data technologies in North America and in the rest of the world are based on Code Division Multiple Access (CDMA) and Global System for Mobile communication (GSM). This document focuses on these two technologies as they are the most widely deployed. 4G technologies are currently in development and generally not commercially available (2008). Figure 2 summarizes the overall data throughput limits for the various technologies.

## Wireless Data Technologies and MSP

MSP operates and manages Motorola Mobile Devices through a client/server architecture using IP communication. MSP is network technology agnostic. In other words, wide area networks as implemented and made available through carrier networks can be used as a communication channel for the enterprise to manage their mobile deployments through MSP. Proper planning and coordination with carriers in constructing an appropriate data plan, understanding the relevant interfaces, and generating an appropriate IP addressing scheme are important for managing mobile devices with MSP. This whitepaper covers some of these areas to aid in planning. Close coordination with the carrier and/or data plan supplier should be sought prior to using MSP in carrier based networks.

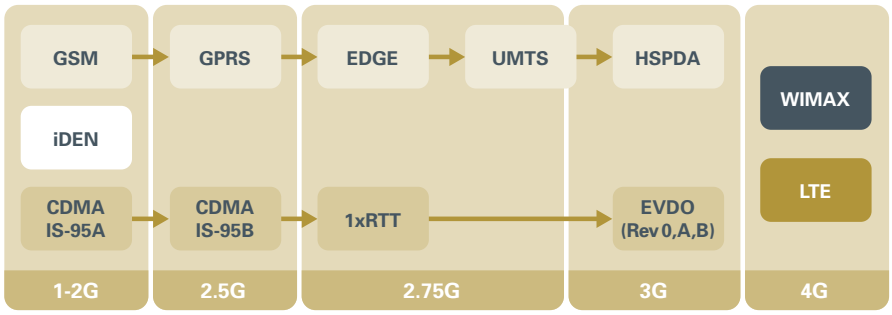


**Figure 1: Wireless Data Technology Evolution Roadmap**

| Standard | Generation | Max Downlink Mbits/S | Max Uplink Mbits/S | Typical Downlink Mbits/S |
|---|---|---|---|---|
| CDMA RTT 1X | 2G | 0.3072 | 0.1536 | 0.1250 |
| CDMA EVDO Rev. 0 | 2.75G | 2.4580 | 0.1536 | 0.7500 |
| CDMA EVDO Rev. A | 3G | 3.100 | 1.800 | 1.000 |
| CDMA EVDO Rev. B | 3G | 4.900 | 1.800 | 2.000 |
| GSM GPRS Class 10 | 2.5G | 0.0856 | 0.0428 | 0.1400 |
| GSM EDGE type 2 | 2.5G | 0.4736 | 0.0473 | 0.3400 |
| GSM EDGE Evolution | 2.5G | 1.8944 | 0.0947 | 0.7500 |
| UMTS | 3G | 0.3840 | 0.3840 | 0.2500 |
| HSDPA | 3G | 14.400 | 0.3840 | 3.0000 |
| WiMAX 802.16e | 4G | 70.00 | 70.00 | >10.00 |
| LTE | 4G | 70.00 | 70.00 | >10.00 |

**Figure 2: Data Throughput Summary by Technology Type**

# Chapter 2 Wireless Data IP Overview (Carrier Agnostic)

## IP Addressing Overview

IP Addresses are numbered addresses that are used to locate and communicate to network elements. IP addresses are managed and created by the Internet Assigned Numbers Authority (IANA). The IANA allocates blocks of addresses to regional internet registries who in turn allocate smaller blocks to internet service providers and enterprises. IP addresses can be public or private. Additionally, IP addresses can be statically or dynamically allocated.

**Public and Private IP Address**
Public IPs are unique addresses allocated by the IANA and routable over the general internet and allow network elements to be resolved and reachable on the general internet. Certain ranges of internet addresses are considered Private IP addresses and not routable over the general internet. Private IP addresses can be reused in private networks, are not unique, and not registered with the IANA. Network elements assigned a private IP address are generally not reachable from the general internet There exist mechanisms to allow this (i.e. NAT port mapping) but are generally not common. Public IP addresses incur a cost and may not be as secure as a network element assigned a private IP address since they are reachable from the general internet. Private IP addresses are free to use but are limited in that without additional networking are not reachable over the general internet.

Mobile wireless data connections initiated by the mobile device that require access to the general internet may be assigned a Public or a Private IP address. Mobile wireless data connections initiated by a host from the general internet communicating to the mobile device require that the mobile device be assigned a Public IP address. For MSP, the Remote Control feature is a host initiated connection to the mobile device and in many cases a Public IP address is required for the mobile device. In this case a host initiated connection is an IP connection between the console PC used by the IT administrator (client) to the mobile device (acting as a server) — Not necessarily the MSP server itself. Exceptions exist for some networking configurations (i.e. VPN, fixed end connections with private networking).

**Static and Dynamic IP Address**
A network element may be assigned a static IP address meaning that the IP address is fixed over time. A dynamic IP addresses typically is managed by the network infrastructure through a DHCP server where a pool of addresses are available and when requested by a network

element a dynamic (usually time limited) IP address is assigned from the pool. For network elements using dynamic IP address assignment their IP address may change over time and are shared among network elements. By default carriers typically use dynamic IP address assignment to more efficiently use available IP addresses and simplify management of IP addresses.

**Dynamic DNS Service**
A Dynamic DNS Service maps a static hostname to a remote device and is able to resolve the mobile device IP address for dynamically allocated managed IP addresses. Carriers may be able to supply such a service. MSP does not require nor would it use such a service but a Dynamic DNS service may be useful for other line of business applications.

## Fixed End Connectivity

Carriers (both CDMA and GSM based) generally can provide through value added services a fixed end connection to the enterprise. A fixed end connection is a dedicated secure direct connection from the customer's enterprise network to the wireless data network supplied by the carrier. Enterprise mobile devices through custom carrier services may provide a virtual private network through a fixed end connection to the enterprise. A fixed end connection may add a level of security and control for the enterprise. Some fixed end connection options include:

- **Virtual Private Network**
  A virtual private network is an encrypted channel from the carrier wireless network (radio access network) through IPSec or SSL over the general internet. A virtual private network may be relatively inexpensive when compared to a direct circuit.
- **Direct Circuit (or Frame Relay)**
  A direct circuit (i.e. frame relay, T1, T3, etc.) is a direct channel to the enterprise bypassing the general internet. A direct connection provides full routing control and allows enterprises to use Private IPs for carriers that support Private IPs for mobile devices. Redundant direct connections may enhance availability.

# Chapter 3 GSM Based Wireless Data Networks

## GSM Based Wireless Data Network Deployments

The following sections provide information specific to GSM related wireless data networks (i.e. GPRS, UMTS, and HSPDA) with discussion related to using MSP.

### Data Access Point Name (APN)

Access Point Names (APN) are utilized in GSM related wireless data network standards (i.e GPRS, UMTS, HSPDA). An Access Point Name (APN) and are assigned and managed by the GSM carriers. An APN identifies an external network that is accessible from a mobile device. An APN has several attributes associated with it that define how you can access the external network. APNs are a named item that identifies the details, capabilities, and limits assigned to a wireless data connection. An APN specifies how mobile devices connect, their assigned quality of service, what communication is available to external networks, what fixed end connections to use, and what value-added services the mobile device has access to. Typically GSM carriers support several APNs that fall into three general categories:

- **Default APN**
  A Default APN is a general purpose APN for general internet access which typically comes by default with a standard data plan. Quality of Service, security settings, and IP addressing schemes are well known by carrier (see carrier specific discussion below). Username and password are hard coded and well known for access. A default APN is usually the easiest to setup and typically the most economical.
- **Special Purpose APN**
  A Special Purpose APN is an APN pre-created by the carrier with incremental features different than the Default APN to address other customer segments that may require different capabilities from those provided by the Default APN. Carriers can provide information on any Special Purpose APNs they may have available along with the relevant wireless data connection details.
- **Custom APN**
  A Custom Purpose APN is an APN created and managed by a carrier specifically for a customer. Many options are available with a custom APN including: Quality of Service, security settings, IP address planning, access control, and network connectivity options. With a custom APN security and access control can be serviced by the carrier or provided by the customer. Custom APNs usually require a setup fee, take time to create, and may have more recurring expenses.

A summary of options related to APNs are summarized in Figure 3. In later sections some recommendations are provided related to mobile enterprise deployments that use MSP to manage mobile devices in GSM based networks.

## GSM Related Wide Area Network Mobile IP Addressing

Although GSM carriers are bound by relevant technology standards for wireless data, all wireless carriers operate slightly differently in some details related to IP Addressing as it relates to mobile data

| Feature | Default APN | Special Purpose APN | Custom APN |
|---|---|---|---|
| Use Case | Public Shared APN | Shared APN with Incremental Features | APN assigned specifically for Customer |
| Implementation Time | Minutes | Week | Weeks |
| Cost | Included in Standard Plans | Incremental Cost | Higher Setup Cost and possible additional recurring cost |
| Firewall Rules | Predefined | Predefined | Customizable |
| Typical IP Addressing Scheme | Fixed, Typically Dynamically Assigned, Private* or Public IP | Predefined but Several Options Dynamic, Static Private*, Public | Customizable |
| Fixed End Connectivity | Internet Only | Internet Only | Internet, Network VPN, Frame Relay/Fiber/T1 |
| Security | Carrier Provided (pretty open) | Carrier Provided | Customizable (Managed by Carrier or Customer) |
| Access Control | One (fixed) Username and Password for Access | Username and Password Managed by Carrier | Custom Access (Managed by Carrier or Customer) |
| Quality of Service | Default | Fixed by Carrier (Can be higher) | Customizable |

**Figure 3: APN Categories and Key Differences (GSM Networks)**

plans. GSM carriers in general can provide a host of options and close coordination with a carrier may be pursued to customize enterprise mobile device IP planning and allocation. Provided below are some guidelines for GSM carriers based on currently available information (2008).

One important item when planning carrier based IP addressing is that the Remote Control feature in MSP requires mobile devices to be reachable (Public IPs) if the MSP administrator PC is not on the same private LAN as the mobile device. IP addresses can be dynamic or static as MSP tracks IP addresses for devices but the mobile device must have a routable (Public) IP address for MSP to perform Remote Control in a network that uses the general internet without a virtual private network. Other MSP features do not require a Public IP address since all other IP connections are initiated and established by the devices.

**Private IP Addresses in Wireless Data Networks**
This is the default IP addressing solution on many GPRS/EDGE/UMTS/HSPDA networks (including the AT&T data network). If you choose this option, your mobile devices will be dynamically assigned a private IP address. Users can access WAP applications and the Internet. Combine this option with a VPN, and devices can access corporate content-such as enterprise email or corporate intranet sites-from behind a firewall.

Ability to use Remote Control option in MSP will not be available with Private IP addresses unless the MSP administrator console is located in the same private network as the applicable mobile device. One way to achieve this is to use a virtual private network (VPN).

## Example Pricing Structure for GSM Based IP Plans

Example costs associated with data plan setup for a specific carrier are provided in Figure 4 (2007). This is meant as an example as carriers change pricing guidelines over time and region. Please consult directly with carriers to obtain up to date pricing information.

| IP Plan Type | One Time Setup Charge | Monthly Charge |
|---|---|---|
| Private IPs — Dynamically Assigned | No Additional Charge | No Additional Charge |
| Public IPs — Dynamically Assigned | $500 | No Additional Charge |
| Static Public IPs | $500 | $3 per static IP |
| Customer Provided Public IPs | No Additional Charge (from carrier). Costs to obtain Public IPs | No Additional Charge |
| Custom APN Setup | $500 | Varies |

**Figure 4: Example Pricing Structure for IP Plans (AT&T GPRS Data Plan)**

**Public IP Addresses in Wireless Data Networks**
Public IP addresses can be dynamically assigned or assigned from a designated range of addresses for a specific business. Choosing a block of public IPs allows enterprises to enhance corporate security by adding a fixed block of wireless device IPs for access to the enterprise firewall. Public IP addresses can be purchased in convenient block quantities (from 28 to 1020). Businesses of any size can implement an IP-based security method to access data from behind a firewall.

GSM based carriers can typically obtain public IPs for a fee or businesses can obtain public IPs by some other means and communicate those to the carrier for configuration. Ability to use Remote Control option in MSP is available with devices assigned Public IP addresses (dynamically or statically assigned).

**Static IP Addresses in Wireless Data Networks**
Business critical applications that require a fixed IP address require statically assigned IP addresses. With static IP addresses, a business can designate a range of public IP addresses to be assigned to their mobile users. Each time a mobile user signs on to the wireless data network, the network assigns the same IP address to the device from the designated range. GSM carriers typically provide a convenient Web interface to manage the assignment of specific IP addresses to mobile devices. Static IP addresses can be purchased in blocks ranging from 28 to 1020 IPs.

**Customer Provided IP Addresses**
Enterprises typically can provide their own IP address block to the carrier for your mobile data configuration essentially extending your company's local area network to include the carrier network. This allows for simpler firewall configuration, as well as mobile device identification.

The enterprise should choose an IP plan to best fit their wireless data needs and coordinate with the carrier to construct the appropriate data plan. Using Public IPs, a virtual private network (with Private IPs), or a mobile private network is a requirement for using the Remote Control feature with MSP. Dynamic assignment may be more efficient use of IP Addresses. Alternatively, statically assigned (or a range of enterprise Public IPs — Customer or Carrier provided) may enhance enterprise security through well known IPs.

## GSM Carrier Networks and MSP Network Planning

This section outlines various possible networking configurations for management of mobile devices using MSP in GSM based wireless data networks. Implications, costs, relative complexity, options, and recommendations are summarized for each

networking configuration. Each enterprise should work with their selected carrier to understand and plan an appropriate network configuration to meet the varying needs of their enterprise.

### Standard Carrier APN Configuration

The Standard Carrier APN Configuration (see Figure 5) uses the default data plan provided by the carrier. Typical default settings are: private IP dynamically assigned (for GPRS/EDGE/UMTS/HSPDA), static username/password access, general internet access, and general internet access unsecured. This is the typical case at present since it is lowest cost and easiest to implement. It is also the least secure and provides minimal amount of control from the Enterprise. Using the Standard APN for a wireless carrier, you generally get connectivity, directly or indirectly, to the Internet. Without using a virtual private network in this particular configuration the Remote Control Feature in MSP will not be available.

### Key Points Related to Standard Carrier APN

- Mobile users can access the general internet (i.e. browse yahoo).
- If private IP assignment is used mobile termination is not available therefore the Remote Control Feature for MSP will not be available.
- Least secure networking option for the mobile devices. Especially if Public IP assignment is used.
- Typically the least expensive and least complex solution to implement with the least amount of setup time.
- Typically cannot filter and control access to the Enterprise MSP backend system based on device.
- Default Private IP dynamically assigned.
- Hard coded username/password for APN access.
- Shared networking with all subscribers (not just enterprise subscribers).
- Potential for "Man in the Middle" security compromises

### Recommendations for using MSP with Standard Carrier APN

- For relay server communication utilize secure FTP (FTPS) with server certificate validation and certificates installed on the mobile devices.
- Appropriately firewall and secure access to the enterprise networks (and especially the Relay Servers) within the enterprise.
- Implement mobile device to enterprise network VPN (see the VPN section). Although this option requires VPN to be up and running on the mobile device in order to manage the device with MSP.

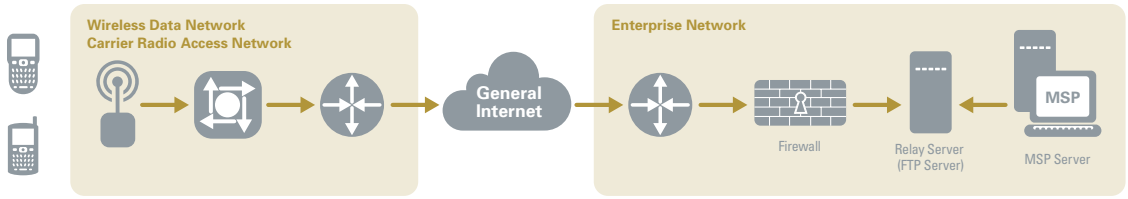


**Figure 5: Standard Carrier APN Configuration (Using General Internet)**

## Custom Carrier APN Configuration with Mobile Private Network

The Custom Carrier APN Configuration (see Figure 6) with Mobile Private Network (MPN) provides a significant amount of control, security, and flexibility for the mobile enterprise related to mobile device to enterprise communication in general and more specifically the communication MSP uses to manage mobile devices. GSM carriers can customize a solution for the mobile enterprise through a Custom APN. Setup time, complexity, and cost are typically more than the Standard APN but enterprises may require the control and customization that such a solution provides.

For the Custom Carrier APN with Mobile Private Network the enterprise devices network traffic is isolated from the general subscriber population and routed to the enterprise directly over a fixed end connection (typically encrypted between the carrier and the enterprise via IPSEC encryption).

### Key Points Related to Custom Carrier APN with MPN

- Mobile users IP traffic is not mixed with general subscribers and does not utilize the general internet.
- Mobile users IP traffic is always routed through the enterprise. The enterprise can limit general internet access by requiring proxy servers as needed.
- Private, Public, Dynamic, Static, and continuous block of IP addresses all available as required.
- Most secure networking option for the mobile devices with the exception of endpoint VPN between the enterprise and mobile devices (although VPN can be used as well for added security).
- Typically the most expensive and most complex solution to implement with the most amount of setup time.
- Ability to customize network access control at the carrier, enterprise, or both.
- Carrier may be able to provide intrusion detection, firewall, and access control services.
- Typically able to scale quality of service as needed.
- Positions the enterprise to take advantage of enhanced services and future carrier offerings.

### Recommendations for using MSP with Custom Carrier APN with MPN

- For relay server communication standard (clear) FTP may be used.
- Appropriately firewall and secure access to the enterprise networks (and especially the Relay Servers) within the enterprise via IP address filtering and appropriate access control.
- VPN is not needed in many cases but adds an extra level of security.

Each enterprise should work with their selected GSM carrier to understand and plan an appropriate network configuration to meet the varying needs of their enterprise.

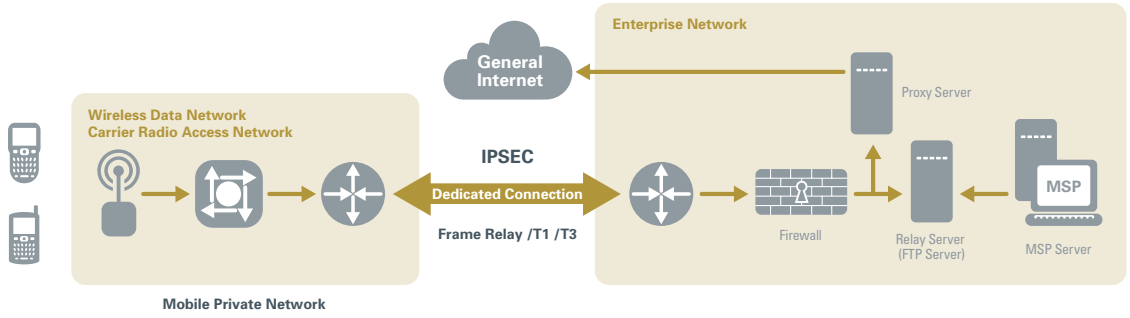


**Figure 6: Custom Carrier APN Configuration with Mobile Private Network**

# Chapter 4 CDMA Wireless Data Networks

## CDMA Based Wireless Data Network Deployments

The following sections provide information specific to CDMA related wireless data networks (i.e. EVDO rev. 0, rev. A., and rev. B) with discussion related to using MSP.

### CDMA Related Wide Area Network Mobile IP Addressing

Although CDMA carriers are bound by relevant technology standards for wireless data, all wireless carriers operate slightly differently in some details related to IP Addressing as it relates to mobile data plans. CDMA carriers in general can provide a host of options and close coordination with a carrier may be pursued to customize enterprise mobile device IP planning and allocation. Provided below are some guidelines for CDMA carriers based on currently available information (2008).

One important item when planning carrier based IP addressing is that the Remote Control feature in MSP requires mobile devices to be reachable (Public IPs) if the MSP administrator PC is not on the same private LAN as the mobile device. IP addresses can be dynamic or static as MSP tracks IP addresses for devices but the mobile device must have a routable (Public) IP address for MSP to perform Remote Control in a network that uses the general internet without a virtual private network. Other MSP features do not require a Public IP address since all other IP connections are initiated and established by the devices.

**Private IP Addresses in Wireless Data Networks**
In CDMA private IP addresses are usually available as a customized service from the carrier through a mobile private network (MPN). There is usually a setup cost and a setup time associated with assignment of a private IP address as part of a wireless data plan through a CDMA carrier. If you choose this option, your mobile devices can be assigned private IP addresses dynamically or statically as chosen by the enterprise. A mobile private network provides the most control for the enterprise as all mobile devices IP traffic is routed to the enterprise as assignment of a private IP address in a CDMA network requires a fixed end connection between the carrier and the enterprise.

Ability to use Remote Control option in MSP with a mobile private network will function correctly since more than likely the MSP administrator console is located in the same private network as the applicable mobile device.

**Public IP Addresses in Wireless Data Networks**
Public IP addresses assigned dynamically are the default configuration for standard CDMA wireless data plans. Public IP addresses can be dynamically assigned or assigned from a designated range of addresses for a specific business. Choosing a block of public IPs allows enterprises to enhance corporate security by adding a fixed block of wireless device IPs for access to the enterprise firewall. Public IP addresses can be purchased in convenient block quantities (from 28 to 1020). Businesses of any size can implement an IP-based security method to access data from behind a firewall. Ability to use Remote Control option in MSP is available with devices assigned Public IP addresses (dynamically or statically assigned).

**Static IP Addresses in Wireless Data Networks**
Business critical applications that require a fixed IP address require statically assigned IP addresses. With static IP addresses, a business can designate a range of public IP addresses to be assigned to their mobile users. Each time a mobile user signs on to the wireless data network, the network assigns the same IP address to the device from the designated range. Static IP addresses can be purchased in blocks ranging from 28 to 1020 IPs.

**Customer Provided IP Addresses**
Enterprises typically can provide their own IP address block to the carrier for your mobile data configuration essentially extending your company's local area network to include the carrier network. This allows for simpler firewall configuration, as well as mobile device identification.

## Example Pricing Structure for CDMA Based IP Plans

Example costs associated with data plan setup for a specific carrier are provided in Figure 7 (2008). This is meant as an example as carriers change pricing guidelines over time and region. Please consult directly with carriers to obtain up to date pricing information.

| IP Plan Type | One Time Setup Charge | Monthly Charge |
|---|---|---|
| Private IPs — Dynamically Assigned | $500 | No Additional Charge |
| Public IPs — Dynamically Assigned | No Additional Charge | No Additional Charge |
| Static Public IPs | $500 | No Additional Charge |
| Customer Provided Public IPs | No Additional Charge (from carrier). Costs to obtain Public IPs | No Additional Charge |
| Mobile Private Network Setup | Varies | Varies |

**Figure 7: Example Pricing Structure for IP Plans (Verizon EVDO Data Plan)**

The enterprise should choose an IP plan to best fit their wireless data needs and coordinate with the carrier to construct the appropriate data plan. Using Public IPs, a virtual private network (with Private IPs), or a mobile private network is a requirement for using the Remote Control feature with MSP. Dynamic assignment may be more efficient use of IP Addresses. Alternatively, statically assigned (or a range of enterprise Public IPs — Customer or Carrier provided) may enhance enterprise security through well known IPs.

# Wide Area Networks and MSP Network Planning

This section outlines various possible networking configurations for management of mobile devices using MSP. Implications, costs, relative complexity, options, and recommendations are summarized for each networking configuration. Each enterprise should work with their selected carrier to understand and plan an appropriate network configuration to meet the varying needs of their enterprise.

### Standard Data Plan Configuration

The standard data plan configuration (see Figure 8) is the default data plan provided by the carrier. Typical default settings for CDMA are: public IP addresses dynamically assigned, general internet access, and general internet access unsecured. This is the typical case at present since it is lowest cost and easiest to implement. It is also the least secure and provides minimal amount of control from the Enterprise. Using the default data plan for a CDMA wireless carrier, you generally get connectivity, directly or indirectly, to the Internet. The Remote Control feature in MSP should work with the CDMA default data plan since dynamic public IP addresses are assigned.

### Key Points Related to Standard Data Plan

- Mobile users can access the general internet (i.e. browse yahoo).
- Least secure networking option for the mobile devices.
- Typically the least expensive and least complex solution to implement with the least amount of setup time.
- Typically cannot filter and control access to the Enterprise MSP backend system based on device.
- Default Public IP dynamically assigned.
- Shared networking with all subscribers (not just enterprise subscribers).
- Potential for "Man in the Middle" security compromises.

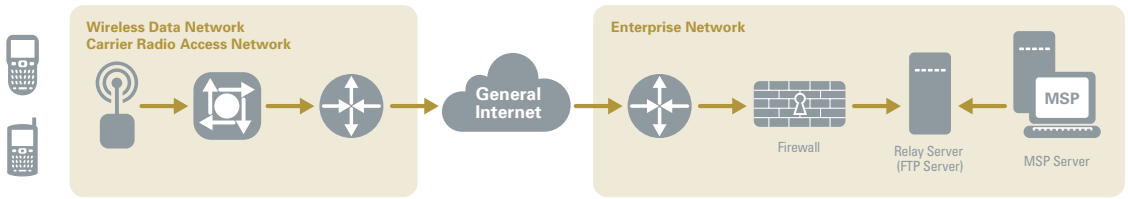


**Figure 8: Standard Data Plan Configuration (Using General Internet)**

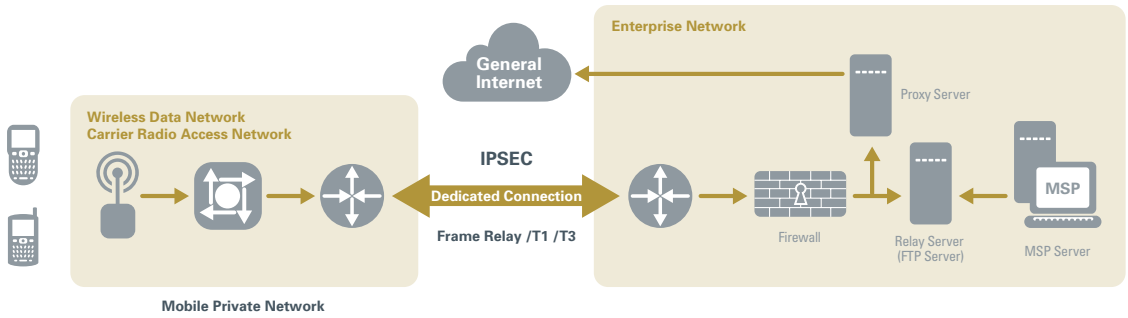


**Figure 9: Configuration with Mobile Private Network**

### Recommendations for using MSP with Standard Data Plan

- For relay server communication utilize secure FTP (FTPS) with server certificate validation and certificates installed on the mobile devices.
- Appropriately firewall and secure access to the enterprise networks (and especially the Relay Servers) within the enterprise.
- Implement mobile device to enterprise network VPN (see the VPN section). Although this option requires VPN to be up and running on the mobile device in order to manage the device with MSP.

### Custom Carrier Configuration with Mobile Private Network

A CDMA carrier (i.e. Verizon Wireless) can provide a customized Mobile Private Network (MPN) — see Figure 9. A MPN provides a significant amount of control, security, and flexibility for the mobile enterprise related to mobile device to enterprise communication in general and more specifically the communication MSP uses to manage mobile devices. Setup time, complexity, and cost are typically more than the Standard data plan but enterprises may require the control and customization that such a solution provides.

For the Mobile Private Network the enterprise devices network traffic is isolated from the general subscriber population and routed to the enterprise directly over a fixed end connection (typically encrypted between the carrier and the enterprise via IPSEC encryption).

### Key Points Related to Custom MPN

- Mobile users IP traffic is not mixed with general subscribers and does not utilize the general internet.
- Mobile users IP traffic is always routed through the enterprise. The enterprise can limit general internet access by requiring proxy servers as needed.
- Private, (dynamic or static), and continuous block of IP addresses all available as required.
- Most secure networking option for the mobile devices with the exception of endpoint VPN between the enterprise and mobile devices (although VPN can be used as well for added security).
- Typically the most expensive and most complex solution to implement with the most amount of setup time.
- Ability to customize network access control at the carrier, enterprise, or both.
- Carrier may be able to provide intrusion detection, firewall, mobile IP, and access control services.
- Typically able to scale quality of service as needed.
- Positions the enterprise to take advantage of enhanced services and future carrier offerings.

### Recommendations for using MSP with Custom MPN

- For relay server communication standard (clear) FTP may be used.
- Appropriately firewall and secure access to the enterprise networks (and especially the Relay Servers) within the enterprise via IP address filtering and appropriate access control.
- VPN is not needed in many cases but adds an extra level of security.

Each enterprise should work with their selected CDMA carrier to understand and plan an appropriate network configuration to meet the varying needs of their enterprise.

# Chapter 5 Bandwidth Considerations and MSP

## Bandwidth and Throughput Planning for MSP

This section provides details related to data bandwidth and throughput associated with various tasks that may be performed by MSP in the course of managing mobile devices. Understanding data transfer requirements for managing devices with MSP will aid in choosing a carrier data plan and related MSP configuration that may allow MSP to run more efficiently in carrier based wireless data networks.

As a note, we discuss bandwidth and throughput needs from the perspective of the mobile device. It is assumed required bandwidth and throughput is present in the wired backhaul infrastructure network (i.e. relay server to MSP Server and from the backhaul of the carrier to applicable relay servers) and the limiting factor is the bandwidth and throughput available in the carrier based wireless data network. Figure 9 summarizes bandwidth and throughput guidelines for various MSP features. Combining features is additive. The bandwidth outlined does not account for line of business applications and only considers data requirements for MSP.

### MSP Management Tasks and Corresponding Data Traffic

Managing mobile devices in MSP and the tasks associated with mobile device to relay server interactions (most MSP features) and administrator console to mobile device (for remote control) are described below. For each category a discussion of required bandwidth, relevant MSP configuration, and recommendations are given.

**Mobile Device Check-In Interactions**

At periodic intervals the MSP client software on the device attempts to check in with the MSP relay server and if updated information is available on the mobile device a file is transferred from the mobile device to the relay server containing associated device information. The default check in period for MSP is set to fifteen minutes but is configurable by the MSP administrators on a device, group, or entire fleet basis. The associated data transferred includes the file and related overhead. A file is only transferred if relevant information on the mobile device has changed. Any custom attributes added by the MSP administrator to be tracked can add to the file size being transferred during check in.

### Bandwidth Related Items for Mobile Device Check In

- About 3.1 KB of data may be uploaded from the mobile device to the relay server during MSP client check in (only if MSP detects the file to transfer has changed which may be seldom — otherwise the data transfer is about 0.1 KB at each check in interval that the device is on). Additional custom attributes to be tracked increase the data to be transferred during MSP client check in.
- The default MSP client check in interval is 15 minutes but is configurable by the MSP administrator to other intervals (i.e. each hour, day, week, etc.).
- Worst case for a default check in interval and a mobile device always on with a relevant check in change being reported each interval 9 MB of data may be transferred in a month related to

MSP client check in. A more typical case would be much less than 9 MB of data transferred in a month related to MSP client check in.

- Real time throughput is not needed to perform mobile device check in.

**Staging and Provisioning**
MSP provides the ability to stage and provision software, settings, files, and any other relevant commands and logic to load these items as part of staging and provisioning. The bandwidth required for staging and provisioning is directly proportional with the underlying packages being provisioned. Large software applications require more data to be transferred (i.e. an OS image). MSP provides the capability to limit provisioning such that provisioning only takes place on a particular network. As an example, provisioning can be configured to only occur when a device is currently connected to a high bandwidth WIFI network and to not occur when connected to a wide area network (carrier).

### Bandwidth Related Items for Staging and Provisioning

- Amount of data transferred is directly proportional to underlying package sizes.
- MSP can be configured to only provision in particular network types (i.e. WIFI) which will limit the data transfer needed on a wide area network.
- If many packages are planned to be provisioned using the wide area carrier network an unlimited data plan may be an appropriate option.
- Real time throughput is not needed to perform staging and provisioning.

**Mobile Device Monitoring**
MSP provides the ability for the enterprise to configure mobile devices to report important characteristics on a periodic basis including battery, memory, scanner, CPU, and many others. Zero up to many of these characteristics can be configured to be reported. Reporting these characteristics requires periodic file transfer to the relay server. The period at which these characteristics are reported is governed by the MSP check in period. The MSP check in period is fifteen minutes by default but is configurable by the MSP administrators on a device, group, or entire fleet basis.

### Bandwidth Related Items for Mobile Device Monitoring

- The amount of data transferred for monitoring is directly proportional to the number of characteristics being collected on the device. From no data up to a maximum of about 1 KB every fifteen minutes (if all characteristics are collected at fifteen minute intervals, device is always on, and connected to the network) may be transferred. At this level about 3 MB of data will be transferred from the mobile device to the relay server every month.
- The collection period may be set individually by characteristic to fifteen minute or hour intervals.
- Real time throughput is not needed to perform mobile device monitoring.

| MSP Feature Area | Bandwidth Guidelines (minimum per month) | Throughput Guidelines (minimum technology) |
|---|---|---|
| Mobile Device Check In | 9MB | N/A |
| Mobile Device Staging and Provisioning (if using over wide area networks)* | Unlimited | N/A |
| Mobile Device Monitoring | 3MB | N/A |
| Mobile Device Remote Control | (See Note 2) | GSM GPRS EDGE<br>CDMA EVDO Rev. 0 |

* MSP can be configured to not use wide area networks for provisioning if desired

Note 2: Remote Control may be used seldom and may not be built into the data plan with the thought that if remote control were used data plan overages for that device would be incurred.

**Figure 10: Recommended Guideline by Feature (Data Requirements are Additive)**

### Mobile Device Remote Control

Remote control in MSP is an on demand feature where an MSP administrator can selectively take control, view the display, and interact with a mobile device. The amount of bandwidth required for a remote control session is directly proportional with the length and the level of remote control performed on a device. The granularity and color depth rendered during a remote control session is configurable and lower color depth results in less data transfer. The remote control feature is a real time interaction and throughput is a factor in making remote control interactions usable. From testing and experience it is recommended that minimum throughput is required (see Figure 10) to make remote control sessions appear nearly real time.

### Bandwidth Related Items for Mobile Device Check In

- Amount of data transferred is directly proportional to the length and level of interaction related to particular remote control sessions.
- The granularity and color depth rendered during a remote control session is configurable and lower color depth results in less data transfer.
- A minimum throughput level of about 200 kbs provides near real time remote control interactions. A minimum of a GSM based GPRS EDGE connections or CDMA EVDO Rev. 0 connections are good candidates for utilizing remote control over wide area networks.

# Summary

Deploying MSP over a Wide Area Wireless network requires careful consideration of many factors. This whitepaper covers some of these areas to aid in planning. In addition, other factors that should be considered when deploying MSP:

**Carrier Selection** — GSM and CDMA providers both offer high speed data services. Selection of the Carrier will depend mostly on the Enterprise Customer as they frequently have large corporate agreements with one or more Wireless Providers. A mix of both GSM and CDMA technologies is not uncommon.

**Coverage** — GSM and CDMA providers usually offer excellent coverage in urban areas. Rural infrastructure can vary widely. High speed data services for instance may not be offered in rural service areas. Packet Data Roaming between networks may also have impacts on service. It is important to consider where the mobile user will operate in order to make a recommendation on the Carrier that should be used.

**Cost** — The cost of Data Plans vary from carrier to carrier. Additionally, added services discussed in this document may incur additional one time and/or recurring charges (i.e. fixed end connections, IP address assignment, enhanced security services, etc). Again, since many large Enterprises use one of more carriers for voice services these costs could be substantially discounted from published prices. Carriers are moving towards flat-rate "all you can eat" plans that include both voice and unlimited data. Enterprise rates for these services can be very aggressive.

**Planned Utilization of MSP Features** — Data capacity requirements related to features used in MSP along with enterprise requirements to utilize the remote control feature in MSP will have an impact on carrier data plan architecture and planning.

**Line of Business Data Protection** — Carriers will typically offer enhanced security services that can be used by the enterprise for additional cost. The enterprise may also implement virtual private networking solutions to enhance line of business data protection (including MSP client to enterprise communication).

***Careful planning is the key to a successful roll-out of MSP.***

**Motorola, Inc.**
One Motorola Plaza
Holtsville, New York 11742-1300
http://www.symbol.com


motorola.com

Part number WP-MSPWAN. Printed in USA 06/08. 