Digi Connect® Application Guide
Cellular IP Connections (Uncovered)

Introduction

When connecting remote devices to a cellular network, users must take into account the requirements of the application and the available IP addressing schemes available by the wireless telco. Specifically, consideration must be given in wireless solutions regarding which side of the connection initiates communication. Each wireless carrier handles usage and management of IP addresses differently; therefore customers must be prepared to carefully examine the type of IP connectivity options available and make sure that they work with the targeted application.

The purpose of this paper is to help users understand the IP connectivity options available and steer them towards the best solution based on:

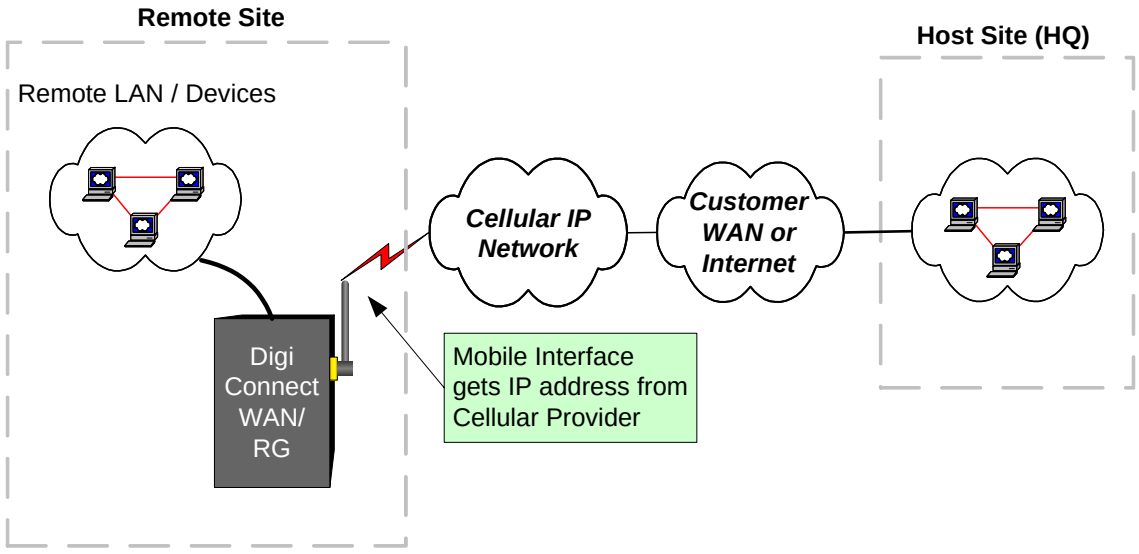
- Type of Cellular Application
  - Mobile Originated vs. Mobile Terminated
- IP Addressing Schemes
  - Static vs. Dynamic
  - Private vs. Public
- IP Addressing on GSM Networks
- IP Addressing on CDMA Networks

Mobile Applications

In order to establish what type of application your scenario falls into, you must first ask yourself:

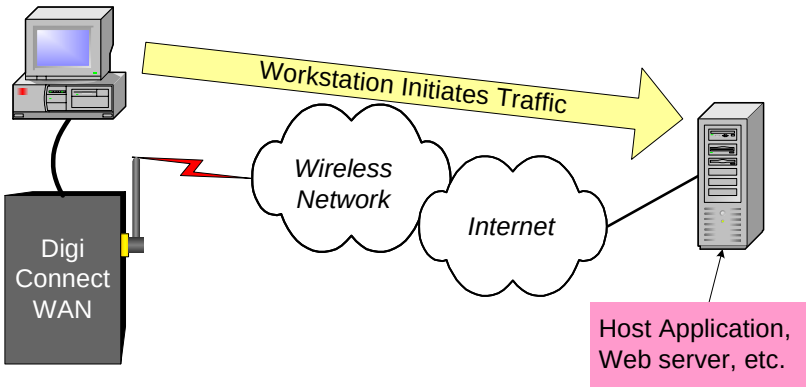
> *"Where is the traffic originating from?"* or said differently, *"Which end is the first to initiate the connection?"*

Consider this simple diagram:

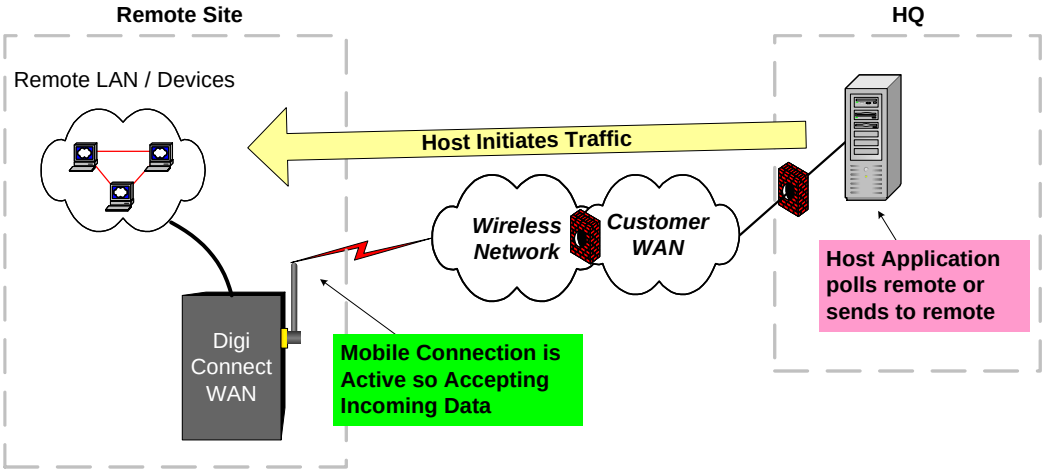


The answer would fall among these three possible applications:

- Mobile Originated – *Remote device makes first communication.*
  A remote device or workstation *initiates* an out-going data connection. This connection could be terminated by a host application at headquarters (HQ) or a remote web server (i.e., web browsing). Some carriers refer to this as *mobile originated* data. Another typical example of mobile originated data is a client-to-site VPN.



- Mobile Terminated – *Host makes first communication.*
  A host application at HQ *requests* information from the remote devices and/or workstations. In this case the remote site must *terminate* the IP connection. This is sometimes called *mobile terminated* data. Common applications include telemetry, SCADA and other forms of polling.



- Both Mobile Originated and Terminated.
  Two common examples are site-to-site VPN and telemetry applications where the host polls the remote while the remote is able to proactively send out alarms.

Why is this important? Devices like the Digi Connect wireless products obtain their IP address from the cellular network. Cellular data providers have various plans that provide different IP addressing options. For example,many plans provide only private IP addresses. Other plans may provide public IP addresses, but the may block via firewall any incoming traffic from outside the cellular network.

IP addressing and security options are very important items to consider when working with your cellular provider. This document is intended to help you and your provider determine which IP addressing and security schemes are needed. Engage your provider's technical staff early in the process to ensure a smooth transition to utilizing cellular IP traffic. This will make your "un-tethered" IP connectivity experience a pleasant one.

Wireless Carrier IP Addressing Schemes

Although every wireless telco offers different IP addressing options, they all fall into one of the categories below:

Public vs. Private IP Addresses

If you have a Mobile Terminated application, your solution requires a routable (or reachable) IP address, meaning the host must be able to access to the remote IP address. One way to accomplish this is with a Public IP address. A public IP address is an IP that is generally reachable by anyone on the Internet. A private IP address, on the other hand, is an IP that is not directly accessible over the Internet.

[Note in some instances a wireless telco can provide Mobile Terminated connections using private IP addresses. These cases are usually where the customer has a dedicated private connection from their network to the wireless provider. These plans are more expensive and availability of these plans varies by provider.]

A common problem with public IP's is that wireless carriers have a limit to the number of IP addresses they are capable of issuing, therefore public IP's can be very expensive. Because of this most IP addresses associated with wireless data plans actually hand out private IP addresses that are not reachable by others around the Internet.

In general private IP's do allow the remote devices access to the Internet. Therefore private IP addresses work just fine for Mobile Originated applications.

Static vs. Dynamic IP Addresses

The demand for public IP addresses continues to grow, however there are only a finite number of public IP addresses available. To help alleviate the shortage of IP addresses, wireless carriers have resorted to handing out dynamic IP addresses instead of static (fixed)/public addresses to solve the problem.

With dynamic IPs, each device is given an IP address for a limited period of time, which is usually no more than a few hours, then the IP address is changed. By using dynamic IP addressing schemes, carriers effectively solve their problem of not having a sufficient quantity of fixed IP addresses to meet market demand. This however creates a challenge for the users with mobile terminated applications who need a fixed address to target.

Fortunately, solutions to all of the challenges above are available using Digi products and Digi partner technology. First, the network connection type between the carrier network infrastructure and the customers' data center can provide some flexibility. For example, a frame relay or VPN connection between the carrier network and the customer's data center allows remote devices to use private IP address assignments for mobile terminated application connections.

Dynamic DNS Services

Additionally, Dynamic Domain Name Services (DDNS) solve the problem associated ever changing dynamic IP addresses in applications where customers require a mobile terminated connection. A DDNS server maps a static hostname to the remote device, so that no matter how often the IP address of that device changes, the hostname still points to the same device.

Some carriers offer network specific DDNS servers. Digi also offers a cross-network DDNS solution through its Digi Connectware® Manager platform. This feature allows the devices to report IP address changes to the Digi Connectware Manager server which in turn sends updates to a designated DNS server. This DDNS architecture approach also utilizes "keep-alive messages" between the device and Digi Connectware Manager to maintain current IP address accuracy.

See the DDNS white paper at http://www.digi.com/pdf/wp_dynamicIP.pdf? for more details on how Digi Connectware Manager works with DDNS.

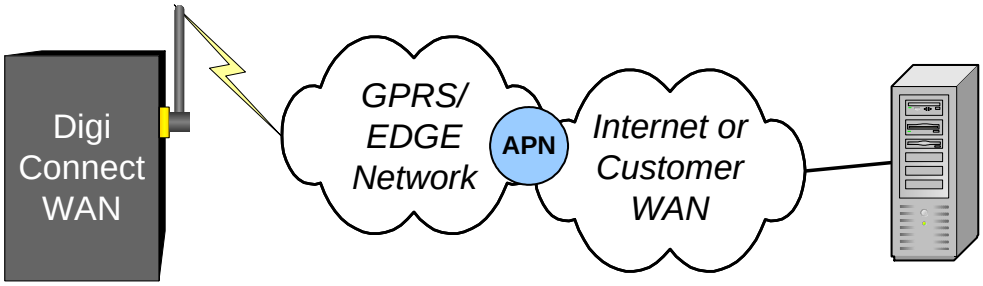
IP Addressing on GSM Networks

[Note: The following data is specific to the U.S. Cingular network; however, it is applicable to any GSM network, although some of the APN names may have a different name. Please check with your wireless telco for specific IP addressing options and details.]

GSM GPRS/EDGE cellular data networks use a mechanism called an APN (Access Point Name) to determine how a Mobile Station (MS), in this case a Digi Connect WAN or Digi Connect® RG, communicates via the GSM network to a host site (i.e., how the carrier network passes IP traffic to the host network). An APN determines what IP addresses are assigned to the mobile station, what security methods are used, and how the GSM data network connects to the customer's network.

APNs are general-purpose and are available to multiple customers or can be customized for particular customers to address unique requirements.

The APN essentially terminates the mobile IP session and connects to the customer's network. For example:



The various GSM providers all use APNs but implement them differently. For example, some by default will not allow mobile terminated connections while others use RADIUS servers and require user name/password authentication in addition to SIM authentication.

Cingular® Blue (formerly AT&T Wireless) provides multiple options for IP addressing, including public, private, customer-supplied and network-assigned IP addresses. Various

options are available for static and dynamic IP addresses. Dynamic DNS naming is also supported in certain APN types.

Following is a typical sequence used to create an IP connection on a GSM network:

1. Digi Connect WAN/RG comes online and gets a signal from the tower.
2. As long as there is a signal, and a SIM card has been inserted into the Digi Connect device, and the Digi Connect device has been properly configured to match the SIM/APN provisioning, the Digi Connect device will "dial" the GSM network with a pre-determined dial string. This dial string tells the GSM network how to handle the connection. The user does not need to know how to configure the dial-string.
3. The SIM and provisioning info, along with optional username/password, is sent to the GSM network. This information is used to determine which APN to use. (The provisioning can be changed without the need to replace the SIM card.)
4. The APN sends an IP address back to the Digi Connect device which is used on its mobile interface.
5. The PPP link is established (also called a PDP context) and IP traffic starts.

Cingular APN Types

Here we will focus on the Digi Connect WAN/RG when used with the Cingular network. As stated above, the different GSM providers have varying APN types, so it is important to check with your provider for available options

Cingular Blue offers four main APN types:

- Proxy
- Public
- Internet
- Custom

Proxy and Public APNs: These APN types are for outgoing, mobile originated data only. No incoming, mobile terminate data connections are permitted. The only difference in these two APN types are that proxy uses a Cingular provided private IP address while public gets a public IP address.

Internet APN: The Internet APN allows incoming mobile terminated connections as well as mobile originated. IP addresses are dynamic Internet, Cingular-provided public addresses. An address maps to Dynamic DNS name in the convention of 1[phone_number].internet.mycingular.com (e.g. 15055551212.internet.mycingular.com). These mobile connections are visible on the public Internet so security and traffic blocking need to be taken into consideration. The customer back-end connection only needs to provide Internet access.

Custom APN: A custom APN is just that – custom. In this case the end-customer works with Cingular to determine the appropriate settings for:

- IP addressing requirements: Are public IP addresses required? If so, who provides the addresses – Cingular or the customer? Do these addresses need to be static?
- Connection from Cingular to customer network: Cingular can provide the following connectivity options from their network to the customer's network, depending on security and cost requirements:
    - Dedicated frame relay connection where the Cingular-to-customer connection is not publicly accessible.
    - Internet VPN connection where the Cingular-to-customer connection is via IPsec VPN.
    - Internet connection: Can be lower cost if security requirements allow such connections as no security is provided by Cingular.

Cingular Orange offers similar APN types, but with fewer options than Cingular Blue. Private custom APNs are available that can provide static mobile terminated IP addresses. In this case the mobile device traffic never touches the Internet. Orange APNs also typically require user name/password for authentication via RADIUS AAA servers.

Other GSM Providers: Digi Connect WAN/RG devices support most domestic and international GSM GPRS/EDGE networks that provide IP routing. Other carriers with built-in support include SunCom, Rogers, T-Mobile, Petrocom, as well as a custom selection. IP addressing schemes and connectivity options vary amongst these providers, so please check with your provider for details.

IP Addressing on CDMA Networks

Note: The following information is specific to the Sprint network but is relevant to most CDMA networks. Please check with your wireless telco for specific IP addressing options and details.

Unlike GSM, CDMA does not use a SIM card for authentication and provisioning. Instead, activations are based on parameters entered in the device configuration and serial number information from the device itself.

As with most GSM IP data networks, CDMA IP networks were designed for outbound, mobile originated data connections. This means many provide private and public IP addresses which are dynamically assigned each time they log onto the network.

Sprint provides two data services: Vision and DataLink. Vision is what is used for most mobile applications and features the dynamic public IP addressing scheme. It is similar to the Internet APN offered by Cingular (above).

The Sprint PCS DataLink program is a custom program offered to create a more secure, more integrated option for customers. It is similar to the Cingular Custom APN (above) and provides solutions via frame relay or VPN into Sprint, as well as static IP options. DataLink is an enterprise solution, which is an extension of Sprint's consumer-oriented Vision data service.

Enterprise authentication is done via AAA (Authentication, Authorization and Accounting) services.

The default Sprint DataLink IP address is a dynamic public IP address. The mobile IP network option offers a static IP address constant for the duration of the mobile session.

Mobile terminated connections for dynamic IP networks must be handled by a dynamic DNS capability. Each time the wireless device authenticates with the enterprise AAA server, the device's current IP address is discovered and can be used to update a DNS server. Alternatively, Digi Connectware Manager can also provide DNS server updates.

Another way of providing static IP addresses is via Sprint partners such as Motient or NPhase who offer programs for allowing mobile terminated applications over CDMA (and GSM) networks.

More information on Sprint's DataLink service is available at http://www.sprint.com/business/products/products/dataLink_tabC.jsp.