Choosing a Cellular Solution for Connecting Devices to a WWAN

Dana Lee, Senior Product Manager
dana.lee@moxa.com

Recent developments in the wireless and industrial automation fields have spurred businesses to consider using wireless technologies to connect remote devices. In the past, using wireless for communicating between remote devices or remote offices and the central office was not feasible due to problems with cost, speed, and reliability. However, wireless technologies have already reached a level of sophistication that makes wireless technology a feasible solution for a variety of applications.

Cellular Technology for WWAN Applications

Cellular technology is currently the most popular choice for implementing wireless WAN applications. This is because of the extended range and coverage that cellular technology offers.

Cellular technology is usually classified into the two standards that are widely used in various parts of the world today—GSM/GPRS and CDMA. Current estimates put the global market shares for GSM/GPRS and CDMA at 80% and 20%, respectively. The GSM/GPRS standards comprise several generations, with each generation offering higher data rates than the previous one.

The following table lists the various GSM/GPRS generations, and the data rates supported by each generation.

	2G	2.5G	3G	3.5G

Released on May 1, 2008

Moxa manufactures one of the world's leading brands of device networking solutions. Products include industrial embedded computers, industrial Ethernet switches, serial device servers, multiport serial boards, embedded device servers, and remote I/O products. Our products are key components of many networking applications, including industrial automation, manufacturing, POS, and medical treatment facilities.

How to contact Moxa

Tel:	1-714-528-6777
Fax:	1-714-528-6778
Web:	www.moxa.com
Email:	info@moxa.com

MOXA®

This document was produced by the Moxa Technical Writing Center (TWC). Please send your comments or suggestions about this or other Moxa documents to twc@moxa.com.

GSM Standard	GSM	GPRS/EDGE	UMTS (WCDMA)	HSDPA/HSUPA
Data Rate (Kbps)	9.6	54.2/237	384	>1800

With the increase in data rates and reliability that cellular technologies (especially GSM/GPRS) now offer, they are becoming the primary data communication method for a number of industrial automation applications.

Types of Cellular Products for WWAN Applications

To understand which cellular solution you need for your wireless WAN application, you need to know what options are available in the market and the specific applications or environments they were designed for.

Cellular Modules

A cellular module is a supplementary module (or add-on) that provides a device with basic cellular capability. The module enables the attached device to connect to the cellular network using simple AT commands. Cellular modules are primarily used to enable host devices to send data back to the central office. In real-world applications, cellular modules are used as a backup data communication channel that can be used if the telephone service is unavailable or disconnected.

Cellular modules are developed by companies such as Siemens, Wavecom, and Telit, and are used by hardware vendors that want to add basic cellular capability to their own devices, such as machines, gateway devices, and routers. The modules usually come with a serial interface to support 2G and 2.5 standards, or a USB interface to support 3G and 3.5G standards.

Cellular Modems

A cellular modem is a device that connects to intelligent serial devices to enable them to send and receive data over the cellular network (typically GSM/GPRS). Smart vending machines and automated teller machines (ATMs) are examples of intelligent serial devices that use cellular modems to send data back to and receive commands from a remote host.

Some cellular modems also support short message service (SMS) mode for data acquisition or simple control. For example, a machine operator can configure a device to send an SMS message when its status changes, or an engineer can change the LED display on a highway by sending an SMS message to the device.

Cellular modems operate in the voice channel and use one of two available data modes—Circuit Switched Data (CSD) and Packet Switched Data (PSD).

- CSD was traditionally used for data exchange, and works the same as dial-up modem-to-modem communication. With CSD, once a circuit connection is made, the connection is reserved exclusively for its users, and charges are based on the duration of the connection. This can be both inefficient and costly for some data applications. With Internet connections, for example, more time is spent reading information than is spent exchanging data, but you are still billed for the time spent reading. Many corporate email services address this problem by charging users only for the time they are downloading data, after which the user works offline.
- PSD is a technology where the communication "pipe" is shared by multiple users. Data is sent to a specific address after a short delay, in which the delay depends on the number of users as well as the level of priority requested for the information. Billing is based on the volume of data rather than the duration of the connection. PSD is the same method used for Internet communication. Since it maximizes the use of the network, it will eventually be used even for voice communication, with high priority assigned to that form of traffic.

Cellular IP Modems

In addition to intelligent serial devices, other simpler devices such as meters, LED displays, and detectors, may also need to send and receive data through the cellular network. However, since these are so-called "dumb" devices, they cannot be programmed to send and receive data automatically, and they cannot initiate TCP/IP connections. Non-intelligent devices such as these can still be connected to the cellular network using a cellular IP modem.

Cellular IP modems are similar to cellular modems in that they can enable devices to transmit data over a cellular network. However, whereas cellular modems can only connect devices to the cellular network, cellular IP modems come with a full TCP/IP stack that allows them to connect to other TCP/IP devices and networks, and also have an embedded operating system that allows them to be programmed to perform automated tasks. Simply put, IP modems provide non-intelligent devices with dialup capability, and allow the devices to initiate a data connection to the cellular network to send and receive data from the device. By using cellular IP modems, even non-IP serial devices, such as utility meters, can exchange data with IP-based devices and networks.

Advanced cellular IP modems also come with a number of operation modes that enable users to integrate these modems quickly and easily into their applications without needing to modify their software. Operation modes such as TCP server, TCP client, and RealCOM give users a great deal of flexibility by allowing them to enable only the modes that their applications require.

Cellular Routers

Cellular routers, also known as 3G routers, are devices that connect remote LANs and remote Ethernet devices to the cellular network. Cellular routers are similar to cellular IP modems in that they come with a full TCP/IP stack that enables connected IP-based devices to be integrated with other IP-based devices and networks across the cellular network.

Cellular routers are typically deployed as the primary WAN link in areas or applications (such as environmental monitoring) where using wired connections is costly or not feasible. In areas that can be wired, cellular routers can also be installed as a backup communication link in case the primary cabled link fails. Since these cellular routers are typically deployed at remote gateways, some advanced models also provide built-in network security features, such as VPN and firewalls, that are integrated into gateway devices.

NOTE: Moxa provides several wireless products for industrial applications. For details, please visit our website at www.moxa.com, or contact the author, Dana Lee, at support@moxa.com.

Disclaimer

This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied by law, including implied warranties and conditions of merchantability, or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form for any purpose, without our prior written permission.

Moxa White Paper

Considerations for Deploying Wireless Applications across Cellular Networks

Dana Lee, Senior Product Manager
dana.lee@moxa.com

Are you in the process of designing applications that require accessing devices over the cellular network? If so, then there are some key issues that you should consider. The three most important considerations are:

- IP Connectivity
- Cost
- Security

IP Connectivity

Cellular devices that connect remote sites to a central office must each be configured with a unique IP address obtained from the cellular network provider, and since cellular companies offer different options for obtaining IP addresses, you must carefully consider which subscription plan is best for your type of application. The factors you should consider are:

- Origin of Traffic
- Public vs. Private IP Addresses
- Static vs. Dynamic IP Addresses
- Dynamic DNS

Released on June 1, 2008

Moxa manufactures one of the world’s leading brands of device networking solutions. Products include industrial embedded computers, industrial Ethernet switches, serial device servers, multiport serial boards, embedded device servers, and remote I/O solutions. Our products are key components of many networking applications, including industrial automation, manufacturing, POS, and medical treatment facilities.

How to contact Moxa

Tel:	1-714-528-6777
Fax:	1-714-528-6778
Web:	www.moxa.com
Email:	info@moxa.com

This document was produced by the Moxa Technical Writing Center (TWC). Please send your comments or suggestions about this or other Moxa documents to twc@moxa.com.

Determining your needs precisely can help you choose the best possible cellular provider and subscription plan, and help ensure the success of your project.

Origin of Traffic

Applications that require using the cellular network to connect a central office to one or more remote sites can be categorized by determining where the traffic originates from. Connections are either initiated by the remote sites, or they are initiated by the central office.

- **Remote site initiates the connection:** This is often referred to as a "mobile originated application." Wireless WANs, for example, often use a mobile originated application, since connections to the server in the home office are initiated by devices at the remote sites.
- **Central office initiates the connection:** This is often referred to as a mobile terminated application. Applications for which a host (or master) located in the central office initiate connections with remote (or slave) devices use a mobile terminated application.

Public vs. Private IP Addresses

As you are probably aware, only a limited number of public IP addresses are available, and for this reason, many providers of cellular service do NOT provide public IP addresses for connecting a SIM card to the Internet. How does the inability to obtain a public IP address for your SIM cards affect your application? The answer to this question depends on whether you are setting up a "mobile originated application" or "mobile terminated application."

- **Mobile originated applications** do NOT require using public IP addresses for your remote devices. This is because the devices themselves initiate each connection. (The situation is similar to connecting from a private LAN, such as the one in your office, to the Internet. You can connect out to public hosts on the Internet, but the same hosts would not be able to initiate a direct connection to your office computer.)

- **Mobile terminated applications** generally require that each of your remote devices is configured with a unique public IP address. This should make sense, since if a device is configured with a private IP address, a host computer in your central office would be unable to find the private IP on the public Internet.

Based on this assessment it would seem that it is nearly impossible to set up a "mobile terminated application," since such an application should require one or more public IP addresses.

The good news is that cellular device vendors have begun developing solutions that allow you to deploy "mobile terminated applications" without needing to obtain public IP addresses for your remote cellular devices. A good example is the "Reverse Real COM mode" built into Moxa's OnCell cellular IP modems. The OnCell is installed at the remote site, and then uses Reverse Real COM mode to ensure that the central office computers will always be able to reach the remote device, even if the device is configured with a private IP address.

Reverse Real COM mode uses a mechanism similar to port mapping to enable remote devices that use private IP addresses to remain accessible to external hosts. When Reverse Real COM mode is enabled, the Moxa driver that comes with the device establishes a transparent connection from the remote device to the network host by mapping the device's serial port to a local COM port on the host.

Static vs. Dynamic IP Addresses

Another issue to consider is the difference between using static and dynamic IP addresses. Because of the limited number of public IP addresses that are available, some cellular providers now offer service plans that use dynamic IP addresses instead of static or fixed IP addresses.

When using dynamic IP addressing, your remote device is assigned a public IP address, but the particular IP address that is assigned could change frequently. Although dynamic IP address service plans get around the problem of limited availability of public IP addresses, they still present a problem for mobile terminated applications, since the IP addresses of the remote devices change frequently and unpredictably.

Dynamic DNS

If you are deploying a mobile terminated application, using a Dynamic Domain Name Service (DDNS) provides a way to get around the dynamic IP address and private IP address problems. A DDNS server works by mapping a static host name to the remote device, so that regardless of how often the IP address of the device changes, the host name can be used to locate the device. By using a DDNS, the remote device will be reachable over the Internet even after the IP address of the device changes.

Advanced cellular devices that support DDNS are now available to keep your remote devices accessible over the Internet. For example, Moxa's OnCell cellular IP modems support a number of operation modes that make use of a DDNS to keep your devices visible over the Internet.

- **Real COM Mode:** If your service provider assigns a public IP address (either fixed or dynamic) to your cellular device, you can enable the DDNS function and Real COM mode to ensure that other devices on the Internet can connect to your device using its domain name. This will ensure that your device is reachable over the Internet even when the device's public IP address gets updated. Note that you will need to register your device with a DDNS.

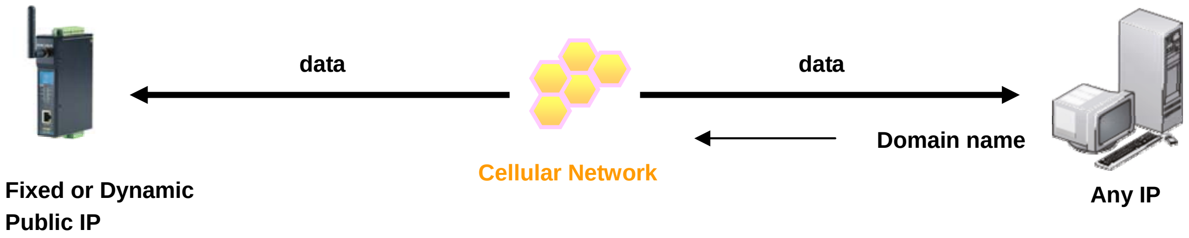

Figure 1: Real COM Mode & DDNS Enabled

- **Reverse Real COM Mode:** If your service provider assigns a private IP address (either fixed or dynamic) to your cellular device, configuring the device for Reverse Real COM mode is another way to ensure continuous connectivity from the device to the remote host, even when the device's IP address changes. With Reverse Real COM mode, the driver that comes with the Moxa device establishes a transparent connection from the serial device to the host side by mapping the serial port to a local COM port on the host computer.

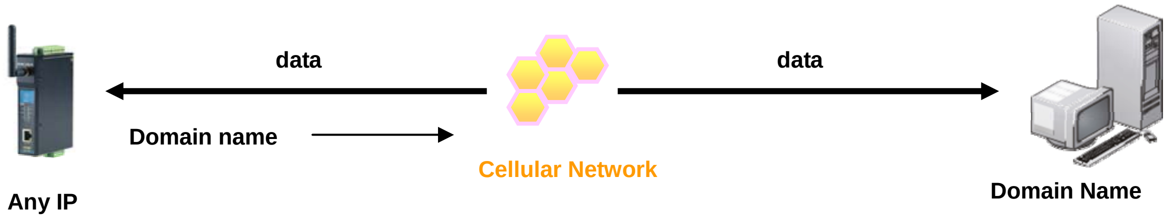

Figure 2: Reverse Real COM Mode

- **TCP Server Mode:** If your service provider assigns a public IP address (either fixed or dynamic) to your cellular device, and your control center is using a TCP client, you can enable the DDNS function and TCP server mode to enable other devices on the Internet to connect to your device using its domain name. This will ensure that your device will remain reachable even when its public IP address is updated. Note that you will need to register your device with a DDNS.

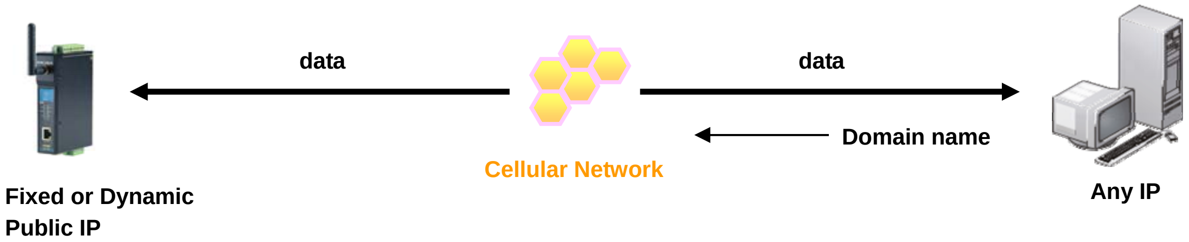

Figure 3: TCP Server Mode & DDNS Enabled

- **TCP Client Mode:** If your control center is using a dynamic public IP address, you can register the host with a DDNS server and enable TCP client mode on the cellular device so that it can connect to the control center using its domain name. This will ensure that your device is reachable even when the host's public IP address is updated. Note that you will need to register your host with a DDNS server.

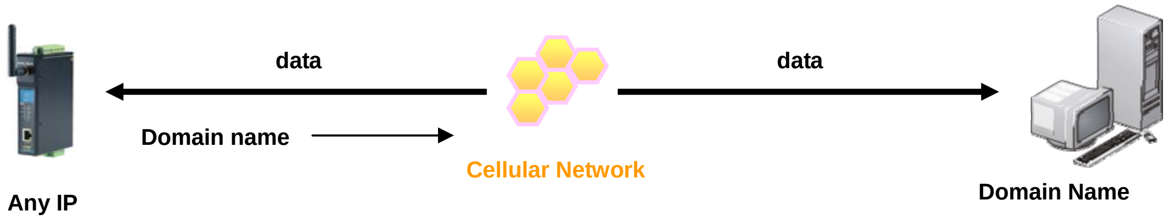

Figure 4: TCP Client Mode

- **UDP Mode:** If your service provider assigns a public IP address (either fixed or dynamic) to your cellular device and your control center is the side that initiates the connection, you can enable the DDNS function and UDP mode to allow other devices on the Internet to connect to your device using its domain name. This will ensure that your device is reachable even when its public IP address is updated. Note that you will need to register your device and your host with a DDNS server.

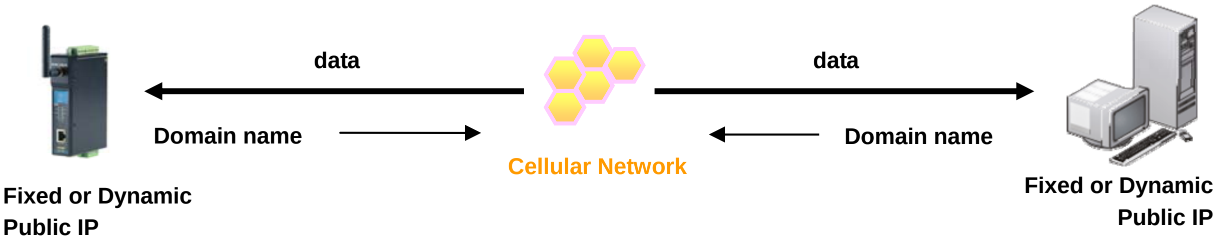

Figure 5: UDP Mode & DDNS Enabled

Cost

Cost is another important factor to consider when deploying wireless applications over the cellular network, particularly since the cost of subscribing to different cellular plans can vary considerably. By considering all the options and then choosing the plan best suited for your application, you can make sure that you're only paying for the service that you need

In addition, you can also look for cellular devices that provide multiple connection types. Moxa's OnCell cellular IP modems, for example, support the following connection options to allow you to make better use of your cellular service plan.

- **Always On:** Use this option to maintain a continuous cellular connection between the device and the cellular network, even when data is not being transmitted. If you are connecting to a GPRS network and your application requires frequent data transfer, then this connection type is recommended. GPRS service plans bill by the volume of data packets sent during the monthly billing cycle.

- **Inactivity Time:** When using this option, the connection between the device and the cellular network disconnects automatically when the connection has been idle for a specified period of time. If your device sends data infrequently, regardless of whether it is connected to a GSM or GPRS network, this connection type is recommended.
- **Remote Host Recovered:** This option can be used to establish a backup or secondary connection that is automatically enabled whenever the Ethernet data connection fails. If your cellular device sends and receives critical data, this connection type is recommended.

The table below lists the connection types that Moxa recommends based on the characteristics and requirements of your devices.

Type of Cellular Network	Characteristic/Requirement	Required Operation Mode		
		Always On	***Inactivity Time***	***Remote Host Recovered***
GSM	Discounted cellular rates	√	---	---
	Normal cellular rates	---	√	---
	Infrequent data transfer	---	√	---
	Frequent data transfer	√	---	---
	Cellular connection is used as backup (Ethernet is primary)	---	---	√
GPRS	Discounted/normal cellular rates	√	---	---
	Infrequent data transfer	---	√	---
	Frequent data transfer	√	---	---
	Cellular connection is used as backup (Ethernet is primary)	---	---	√

Table 1: Recommended Connection Types

Device Functions that Generate Data Packets

Cellular devices typically send out keep-alive packets at configurable time intervals. If you use the "Always On" connection type and you are connecting the device to a GPRS network, then these keep-alive packets will count towards your data packet usage. As indicated in the following table, other functions also contribute to data packet usage.

Function	Options	Description
Link Quality Report	Enable	Disconnects the device if the link noise exceeds a certain threshold. This function performs a link quality check every three minutes.
	Disable (default)	No packets are sent since the device does not perform a link quality check.
Auto IP Report to Host	Enable	Reports the IP address of the device to a remote host based on the configured interval (useful if your device is using a dynamic IP address).
	"blank"	No packets are sent.
TCP Alive Check Time	Set to greater than 0	Defines the time interval during which the device will wait for a response to its "keep-alive" packets. If no response is received, the device will terminate the TCP connection.
	Set to "0"	No packets are sent.
Time Server	"server name"	Once you specify a time server for the device, the device will connect to that server every ten minutes to request the current time.
	"blank"	No packets are sent.

Table 2: Functions that Contribute to Packet Usage

Security

Security is an important consideration for any application that requires sending data over a public network. This is especially critical when your application involves remote devices that you may not always have access to. Two essential security requirements are:

- Ensure the security of data that is sent and received.

- Ensure that remote devices can be managed over a secure connection

Advanced cellular devices, including Moxa's OnCell products, should come with the following security features built in:

- End-to-end security between the remote site and the central office via SSL/HTTPS.
- Access Control List to prevent unauthorized IP addresses from connecting to a device.
- Password security.
- Blocking of certain management services, such as Telnet.
- Use of secure protocols for managing the device.
- SMS authentication.

Summary

As with any type of deployment, good preparation is essential to ensure the success of your cellular application. Part of the preparation includes looking into the primary considerations that will affect the success of your planned deployment.

In deploying wireless applications across a cellular network, there three primary issues that you need to consider: IP connectivity, cost, and security. Fortunately, some cellular devices now have built-in functions that can help you overcome these issues.

Cellular devices developed by Moxa, for example, now have advanced IP addressing functions that help ensure that your device remains reachable by other devices on the Internet, even if it is using a private or dynamic IP address. Moxa's products also support a number of connection types (always on, inactivity time, and remote host recovered) to provide you with a degree of flexibility in choosing the optimum data plan for your wireless application. Security issues, which are of significant concern when deploying remote devices, can also be handled by some of the security features (such as data encryption, SSL, and SMS authentication) built into Moxa devices.

NOTE: Moxa provides several industrial-grade cellular solutions. For details, please visit our website at www.moxa.com, or contact the author, Dana Lee, at support@moxa.com.

Disclaimer

This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied by law, including implied warranties and conditions of merchantability, or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form for any purpose, without our prior written permission.