

What you don't know about industrial GSM/GPRS modem communications

A White Paper presented by:

Ira Sharp
Product Marketing Lead Specialist
Phoenix Contact
P.O. Box 4100
Harrisburg, PA 17111-0100
Phone: 717-944-1300
Fax: 717-944-1625
Website: www.phoenixcontact.com



What you don't know about industrial GSM/GPRS modem communications

Key concepts:

- Several factors must be considered when using cellular communications in an industrial application
- GPRS networks provide better architecture than GSM for M2M and other industrial applications
- GSM networks can be used for SMS alarm notification communications
- With the proper modem and wireless service, three types of GPRS communication are possible: Dynamic IP, Virtual Static IP (VSIP) and Virtual Static IP with VPN

Introduction

Cellular communications are becoming increasingly popular in industrial process applications where traditional wired and wireless communications are not possible. The cellular network provides access to devices anywhere a cellular connection exists. However, when using cellular communications, a number of things must be considered to ensure solid network communications.

Many cellular networks like AT&T do not permit M2M (machine to machine), or continuous "always on" connections, without specific modem approval. To achieve the needed approval, the modem must first comply with PTCRB (PCS Type Certification Review Board), which verifies the modem will not cause harm to the cellular network. After receiving the PTCRB approval, the modem can then be approved by specific carriers such as AT&T. Without the PTCRB and carrier approvals, the carrier reserves the right to disable any unauthorized devices on the cellular network rendering remote modems inaccessible.

In the United States, carriers like AT&T typically do not allow the use of "voice" networks like GSM (Global System for Mobile communications) for M2M data communication applications. This is because modems could monopolize network bandwidth, thus reducing network access for the carrier's typical customers. However, it is also advantageous for the user of cellular modems to avoid using the GSM network because of billing methods. GSM network users are billed by time, which can become very costly when transmitting data, as connection times are generally lengthy. One exception to this is the use of SMS (Short Message Services), which is communication that takes place on GSM networks in the form commonly called "Text Messages."

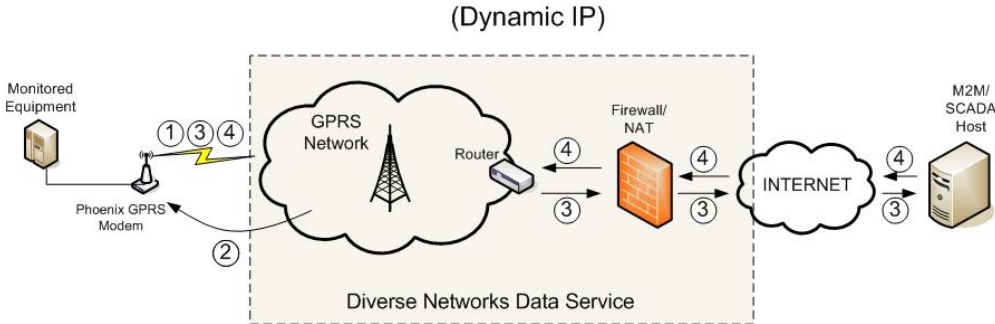
Text messages for remote site monitoring can be a very easy to deploy use of the cellular network to transmit alarm notification from remote locations. Industrial modems include digital input connections that will initiate a pre-programmed message to be sent to a pre-programmed phone number, thereby notifying a technician or operator of an alarm condition. Additionally, AT commands can be used via this communication method to initiate a digital output on the modem or to reset alarm enunciations.

Data networks, such as GPRS (General Packet Radio Service), are designed to provide better network architecture for data communications. Data networks offer an always-on connection and provide billing based on the amount of data sent, not the time spent connected. To create a successful communications system using the GPRS network, special considerations must be taken. With the proper modem and wireless service, industrial users can use three types of GPRS communications: dynamic IP, virtual static IP and virtual static IP with VPN.

Dynamic IP

If the application requires that the remote device (connected to the modem) will periodically report in with status updates or report by exception, the dynamic IP service can be used. GPRS data networks are designed under the assumption that client modems inside the GPRS network will attempt to connect to a host device outside of the network. The client modems are protected by placing a firewall between the modem and the Internet, where the hosts are expected to reside. In this scenario, a host may only respond to client requests, and may not initiate communication to the client.

The client is assigned a dynamic IP address on the Internet, which may change each time it contacts the host. Firewalls, using a process known as port mapping, may assign the same IP address to many different client modems at the same time. Therefore, the client modem will have to identify itself when it connects to a host. How it does this is application- or protocol-specific. The host must have a fixed IP address (or domain name) on the Internet, so that the client knows where to find it. The network diagram below is an example of how a Dynamic IP service will communicate to a host device.



The monitored equipment will communicate via RS-232 to the modem identifying that a network connection must be made. This is done via a socket dial (see below).

- Step 1:** The remote modem will request an IP address from the GPRS network.
- Step 2:** The GPRS network will provide a dynamic IP address to the modem for some lease period (this is typically limited to two to four hours).
- Step 3:** The remote modem will connect to the SCADA host. It is important to understand that the SCADA host must have access to the Internet with the application port opened and ready to communicate.
- Step 4:** The SCADA host replies to the modem request, creating a connection between the SCADA host and the remote GPRS modem.

This connection will remain, provided there is data flow. After a period of no data flow, the connection will be broken, and the modem will no longer be accessible to the SCADA host.

In this scenario, the remote device will report data on a scheduled interval or by exception, or it might check in with the host at scheduled intervals to see if the host needs to communicate with it. The modem will drop off the GPRS network when it is idle for an extended period.

This is the simplest type of service. It will require that the device connected to the modem is capable of sending some initialization strings to the modem in order to open the GPRS connection. Using this method, it is possible to send data to multiple hosts by changing the destination IP address in the initialization string. Using a Phoenix Contact modem as an example, the following structure would be used:

AT#SKTD="type", "port", "addr"

Type	0 TCP (default) 1 UDP
Port	0...65535 Number of the remote port. Default: 1023
Addr	Enter the IP address of the host using the format "xxx.xxx.xxx.xxx". A URL can also be entered as an alternative.

Virtual Static IP

Most data acquisition and control host applications do not expect a device to contact them. Rather, the host expects to contact the remote device whenever it needs to collect data or send commands. For this to work, the host must know where to find the device. There are two common methods for accomplishing this.

One approach is to assign each device a fixed Internet address (or domain name). One major drawback to this approach is that the device will become accessible to anyone on the Internet and will have to protect itself from unauthorized access. Also, Internet IP addresses are a finite resource that can be hard to justify if the number of devices to be accessed is in the hundreds or thousands. The device(s) must also be intelligent enough to make sure they are always attached to the GPRS network, as the network will still disconnect them if they are idle for an extended period.

Another approach is to set up a private connection to the service provider that bypasses the firewall. This way, the remote devices (and the host) are protected from the Internet, and the remote devices can be assigned fixed internal addresses. Because this approach requires specialized hardware and knowledge, it can be more expensive and time-consuming to set up. It is recommended only for larger deployments, and the device(s) still need to be intelligent to keep themselves connected to the GPRS network.

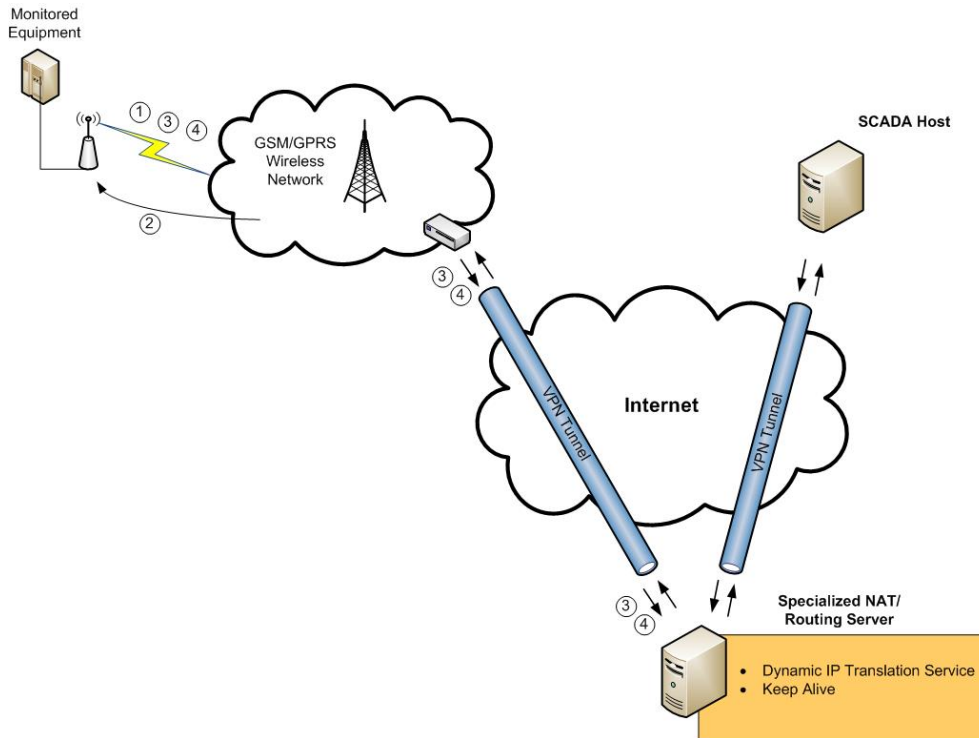
The most robust approach is called Virtual Static IP (VSIP). With VSIP, smaller deployments can be assigned fixed Internet addresses that are protected behind a firewall so that only a designated host can access these devices. The devices are still assigned dynamic addresses, but these addresses are tracked so they can always be mapped to the fixed address. The device will be given a special internal address to contact the host. A useful side effect of maintaining this mapping process is that the device will stay attached to the GPRS network, so no intelligence is required in the remote device to maintain the connection.

This service is very flexible. It will allow the modem to act as both a server and a client device, so the functions offered by the dynamic IP service can also be used with VSIP. The VSIP service will allow a host to communicate to a modem, since the IP addresses are now static. Modbus applications will require this type of service to allow the master host device to poll the slaves in the field.

Virtual Static IP with VPN

The VSIP with VPN service is identical to the VSIP service with the addition of a VPN connection. The VPN setup is established with the modem user's IT department and the wireless service provider once the setup is completed. The IT department manages the users. There can be multiple users with access to the modem and remote device while maintaining one static IP address as the host. It also allows users to be mobile and have access to the modem data from anywhere in the world.

The network diagram below shows how a Virtual Static IP service maintains communications.



The process starts when the modem is powered on, or if it loses connection at any given time.

Step 1: The remote modem will request an IP address from the GPRS network.

Step 2: A dynamic IP address is assigned to the modem from the GPRS network.

Step 3: The address is sent to the specialized NAT/routing server, which will map the VSIP (Virtual Static IP) to the newly acquired dynamic IP address of the modem.

Step 4: A keep-alive message is periodically sent from the modem monitoring the dynamic IP for an extended period of time.

Performing Steps 1-4 allows the remote monitoring equipment to be accessible at all times through the routing server. This allows a connection to be made from the remote device to the SCADA host or from the SCADA host to the remote equipment as needed through the secure VPN tunnel.

Phoenix Contact and Stanza Systems have partnered to provide reliable GPRS communications for industrial applications. By using a Phoenix Contact modem in conjunction with Stanza Systems Diversenet wireless service, industrial users have easy access to all three types of communication: dynamic IP, virtual static IP and virtual static IP with VPN.

Conclusion

Cellular communications can be an efficient means of accessing devices that are not accessible by traditional means. When using cellular modems, it is essential that they are PTCRB- and carrier-approved to ensure modems will not be taken offline.

Data communications may appear challenging over the GPRS network, but with proper planning and an understanding of the different means of communications, it can be very effective.

About Phoenix Contact

Phoenix Contact is a world leader in electrical connection, electronic interface and industrial automation technologies. Phoenix Contact GmbH & Co. KG, Blomberg, Germany, operates 46 international subsidiaries, including Phoenix Contact USA in Middletown, Pa. Global sales exceed more than 1 billion euro annually. Phoenix Contact's formal Integrated Management System is registered to ISO quality, environmental and safety standards (ISO 9001:2008,14001:2004 and 18001:2007).

About Stanza Systems

Stanza Systems, Inc. provides data solutions and custom software development services that help companies benefit from the latest infrastructure monitoring technology. Stanza Systems has specialized expertise dealing with wireless and wired network engineering, real-time application integration, SCADA systems, network security, and service delivery management. Stanza is uniquely positioned to offer end-to-end M2M solutions for a wide range of information on demand needs including SCADA, meter reading, distribution system operations, asset management and general data gathering.