Overcoming IP Address Issues with GPRS Remote Monitoring and Alarm Systems

Stanley Liu, Product Manager

stanley.liu@moxa.com

GPRS is a communication technology that allows data acquisition systems to overcome the difficulty of cabling for wide area remote sites. GPRS applications are becoming more and more prevalent due to the ease with which they can be implemented, but the dynamic IP address issues associated with GPRS networking continue to frustrate system integrators.

For wide coverage areas and hard-to-wire locations for remote monitoring and alarm applications, such as traditional river monitoring systems, construction is difficult because river environments are not well suited for using wire or fiber transmission lines. In comparison, GPRS technology gives system integrators an excellent alternative. In addition to being easy to set up and configure, the cost of operating a GPRS monitoring system can be substantially lower, since the cost is directly proportional to the volume of the data and the frequency with which it is transmitted.

Although GPRS technology makes it easier and more convenient to set up a river monitoring system, the fact that most GPRS devices use dynamic IP addresses can be somewhat frustrating. What this means is that telecom service providers (commonly referred to as carriers) often assign temporary IP addresses to their clients to access the Internet.

Released on April 22, 2009

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.

Compared with static IP addresses, using dynamic IP addresses make it difficult for the control centers to keep in constant contact with remote devices.

The Traditional Polling Architecture of GPRS Networks

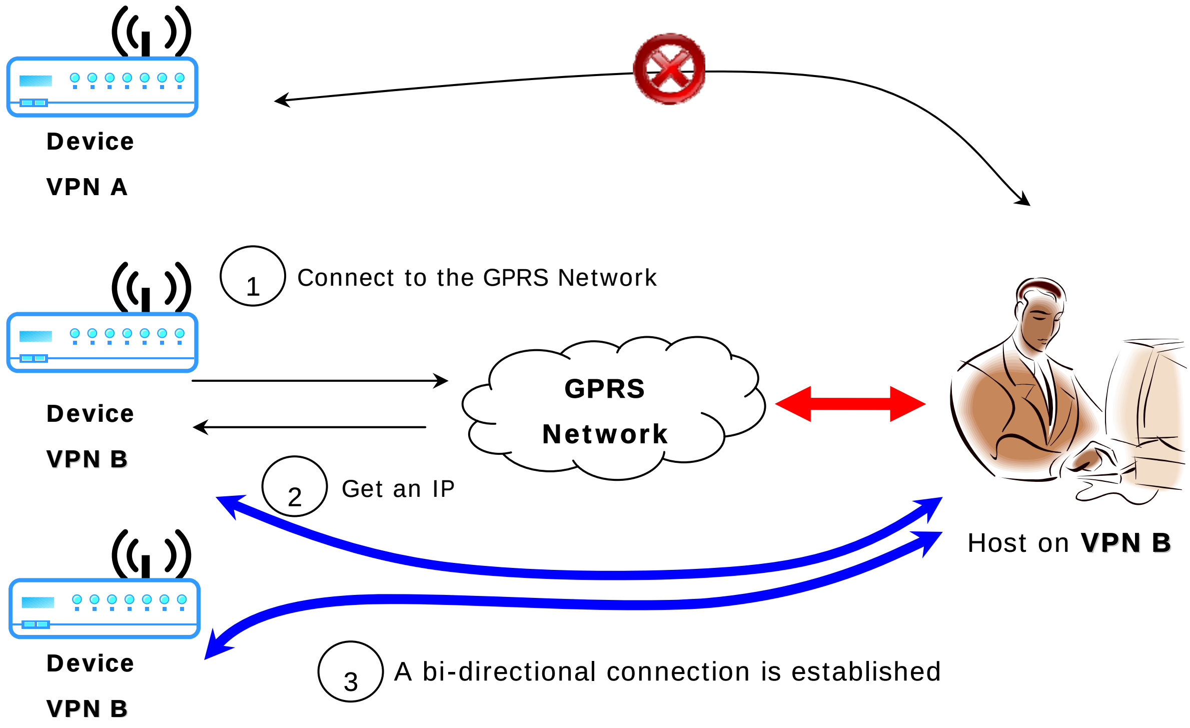
Traditional monitoring and alarm systems use a polling architecture that will only work properly if the host knows the IP addresses of the I/O devices used by the system. The trouble with I/O devices with GPRS capability is that the devices receive a different IP address every time they connect to the GPRS network. Three distinct solutions have been developed to tackle this obstacle:

Solution 1: Public Static IP Address

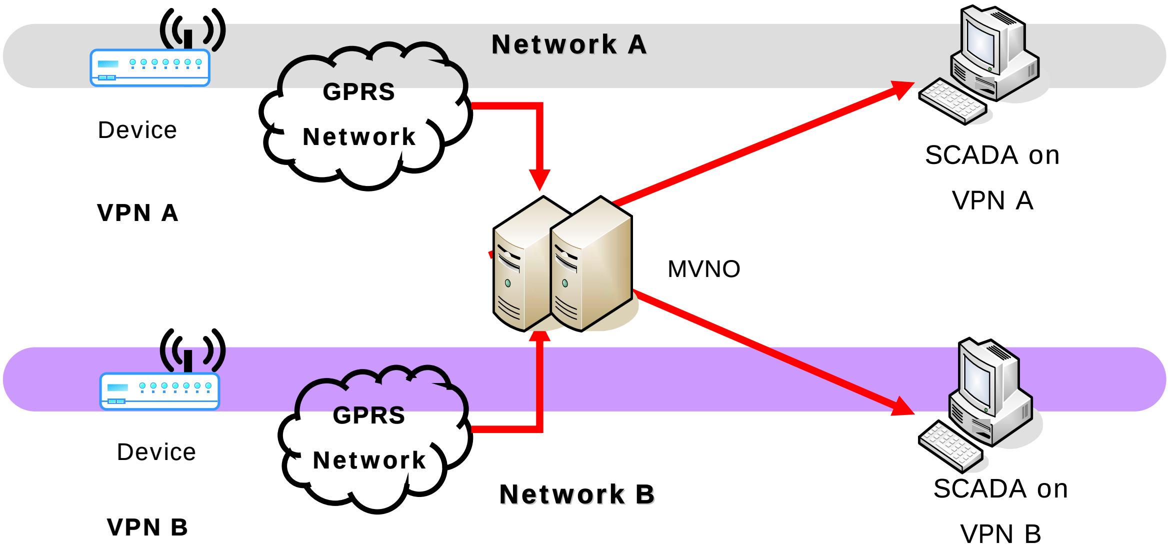
The first choice is to get a public static IP address; some carriers can assign a static IP address to a specific SIM card. This way, all the I/O devices will have their own static IP address and the entire system will operate in the same manner as a traditional monitoring system that uses physical wiring. Perhaps the main benefit of this solution is that it behaves the same as a wired solution. However, not all carriers offer this kind of service, and when they do the cost is relatively high.

Solution 2: VPN Service Provided by Carrier / MVNO

A VPN (Virtual Private Network) is a secure LAN solution that groups specific devices together. VPN has two major functions—security and grouping—and for the GPRS world the VPN grouping concept solves the dynamic IP address issues. The grouping of the devices into one private network prevents unauthorized persons from accessing the data. For this VPN solution, customers are required to buy a number of different GPRS on-line services, and to apply for access to a Virtual Private Network (VPN). When the GPRS device dials up, the carrier will assign a private IP address to it and because the private IP address is on the same network segment as the host, the host and devices can maintain bi-directional communication using a polling architecture.


Device
VPN A
1
Connect to the GPRS Network
Device
VPN B
GPRS
Network
2
Get an IP
Host on VPN B
Device
VPN B
3
A bi-directional connection is established

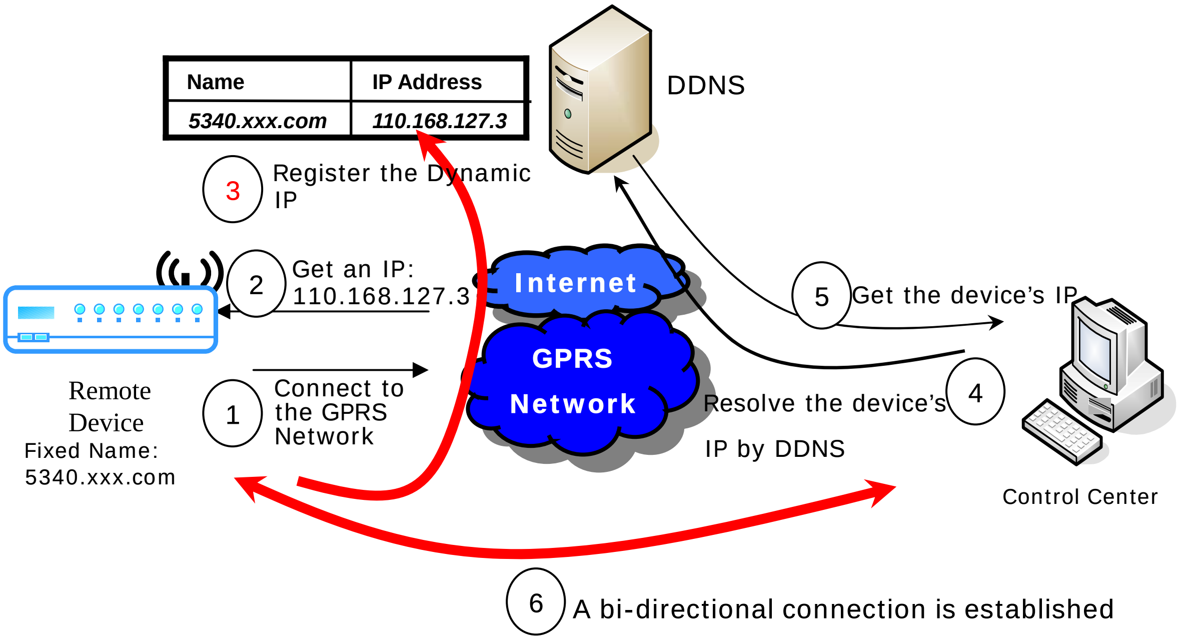
Since most carriers do not offer basic service packages for enterprise clients, many enterprise clients turn to **mobile virtual network operators (MVNO)**. MVNOs are companies that provide mobile phone services, but they do not have their own licensed frequency allocation of the radio spectrum, and may not have the infrastructure needed to provide cellular telephone services. In fact, an MVNO acquires numerous GPRS services and then rents them out to customers who are looking for a small number of IP addresses. In general, MVNOs will also set up a VPN server to divide their clients into different groups.



Unfortunately, some countries do not have MVNOs, and some carriers do not provide VPN services. For this reason, this solution may be unfeasible for some users.

Solution 3: DDNS

Using dynamic IP addresses is often necessary since many ISPs do not provide static IP addresses, or because the cost of obtaining a static IP address is too expensive. The Dynamic Domain Name System (DDNS) is used to convert a device's name into a dynamic IP address so that remote devices can communicate with the control center using a fixed domain name. DDNS is one type of DNS server. The difference between DDNS and DNS is that DDNS takes care of the Dynamic IP address of a device, and DNS the static IP address. With most remote GPRS devices, you need to apply for a hostname for each of the devices handled by the DDNS server. When GPRS devices get an IP from the carrier, they will automatically connect to the GPRS network. Each time a GPRS device's built-in DDNS client gets a new IP address, it will send the IP address to the DDNS sever. The mapping table in the DDNS server is refreshed each time the DDNS receives a new IP address from the devices.



Name	IP Address
5340.xxx.com	*110.168.127.3*

The host can find a device's IP address from the DDNS's mapping table by looking up the device's hostname. For this solution there are two concerns: (1) A majority of DDNS servers do not have standard protocols to implement IP address updates, which makes it difficult for GPRS devices to provide client APs to the DDNS. (2) The quality of the service; as DDNS service is usually provided by a third party service provider, the system may crash when the DDNS loses connection or is being maintained. In addition, it may be necessary to pay a premium to the DDNS service provider for better quality of service.

The Pros and Cons of Polling

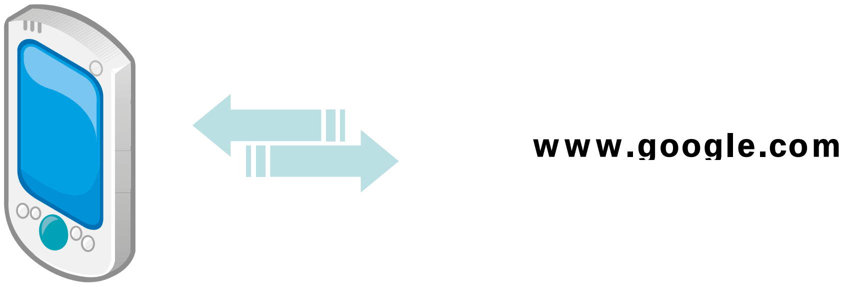
The advantage of polling architecture is that it operates in the same manner as wired Ethernet environments. In order to implement these solutions, we need a third party, such as a carrier or MVNO/DDNS service provider. For the most part, the solutions will require time and money, and collaborating with third parties to find a suitable means of implementing your GPRS remote monitoring and alarming system.

Pros and Cons for each solution.

Solution	Pros	Cons
Public Static IP Address	Same behavior as wired Ethernet	Cost is high Not readily available
VPN	Same behavior as wired Ethernet.	Needs third party service providers Needs time to create the system
DDNS	Uses hostnames to resolve the dynamic IP issue	Extra cost is required Not all devices support DDNS client

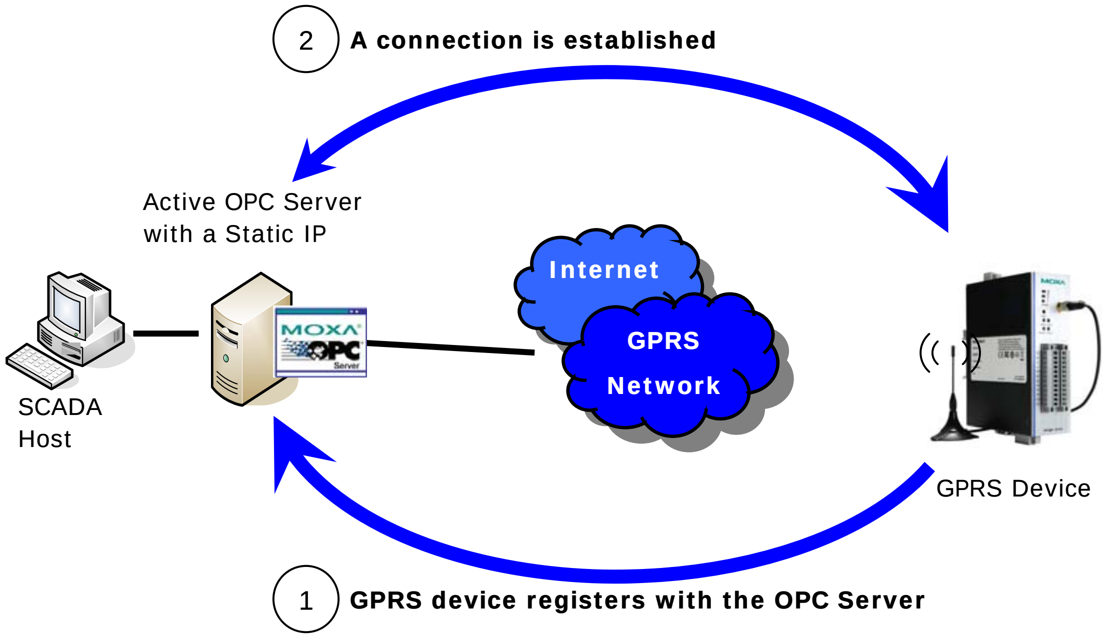
New Push Architecture for GPRS Networks

Push Architecture is a mobile centric solution. Service providers such as web portals and e-mail servers use a fixed domain name. Clients such as mobile phones get information from these service providers by “pushing” the connection request to the Web and e-mail servers, and when a connection is established, the communication is bi-directional.



Unlike the so-called polling architecture, push technology makes bi-directional communication possible for GPRS networks that are using either a dynamic or a static IP address. A remote device with front-end intelligence can report its I/O status to the host and connect to the GPRS network when it needs to.

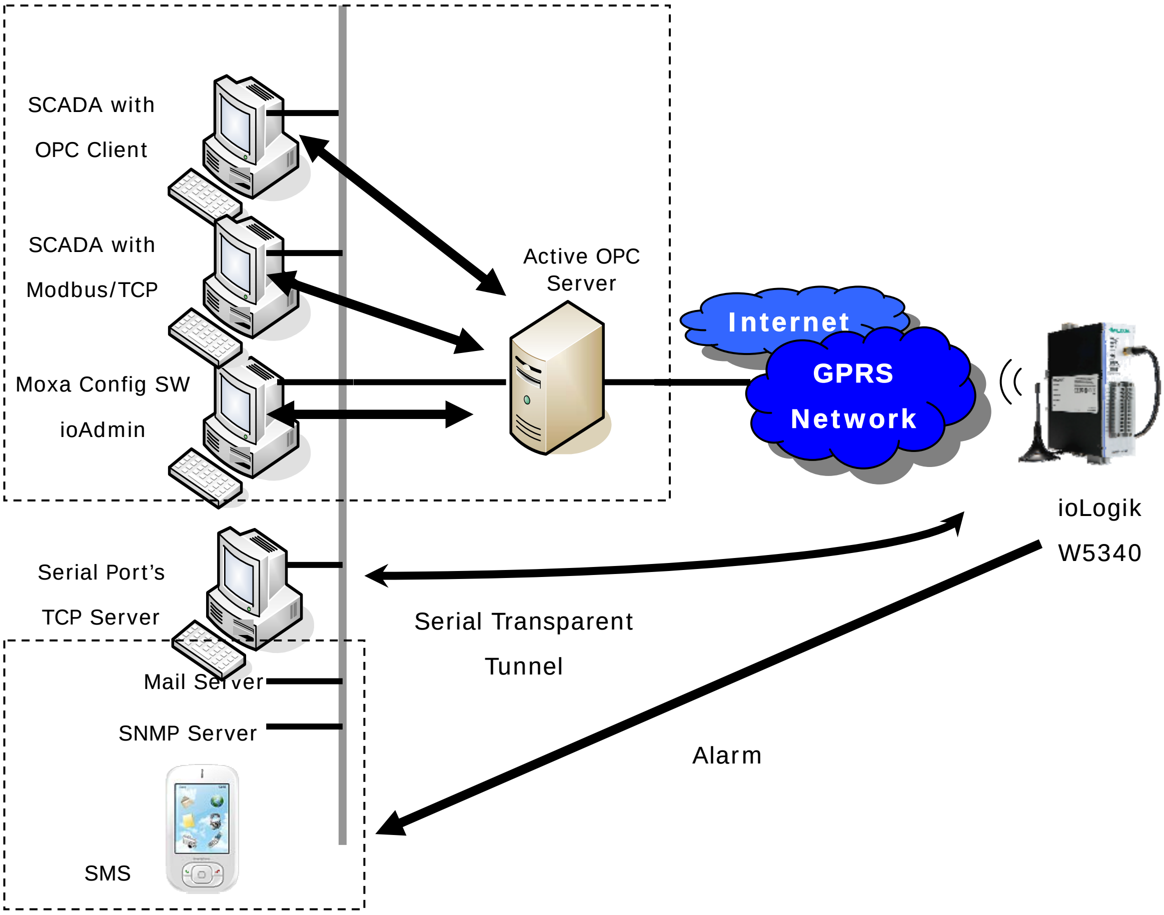
Since Moxa's Active OPC Server supports push technology, our GPRS I/O family of products creates a software-based gateway that makes communications easier. By using a static IP address on the Active OPC Server, the GPRS I/O device can connect to the GPRS network and Active OPC Server without needing to worry about the IP address issues. The topology is described below:



Compared with polling architecture, push technology not only solves the IP address issues but also reduces network loading as well as bandwidth consumption.

Moxa's ioLogik W5340 Active GPRS I/Os takes full advantage of all the benefits of the push technology and Active OPC Server. What Active GPRS I/O and Active OPC Server provide are:

1. SCADA Data Acquisition by OPC protocol.
2. SCADA Data Acquisition by Modbus/TCP protocol.
3. ioAdmin.exe: active GPRS I/O's configuration software.



Alarm messages, such as e-mail and SNMP trap or user definable TCP/UDP raw packets, can all be actively pushed to e-mail servers, SNMP trap servers, or TCP/UDP servers. SMS can be pushed from the Active GPRS I/O to an engineer's cellular phone.

Active OPC Server is an exceptionally powerful gateway for Active GPRS I/O and plays the role of managing IP addresses, GPRS I/O device names, data acquisition gateways, and configuration gateways. This is truly the easiest solution for the GPRS industry to eliminate IP address and communication problems.

Benefits of Using Active GPRS I/O

Moxa's W5340 Active GPRS I/O devices come equipped with 4 analog inputs, 8 software configurable DI/Os, and 2 relay outputs. In addition, the built-in GPRS communication, front-end intelligence, and data logging function give users the advantage of a highly integrated solution. The W5340 also features a 3-in-1 serial port (RS-232/422/485) for connecting field serial devices such as instruments or meters. The benefits of using Active GPRS I/O include:

- **A cost-effective solution for GPRS telemetry applications.**
- **The best choice for solving the dynamic IP issue:** whether the IP is public or private, dynamic or static.
- **Easy installation:** with Active OPC's support, the W5340 can push IP addresses and I/O status to Active OPC Server.
- **Flexible Event Handling** thanks to the Click&Go logic inside.
- **Rich Alarm functions:** SMS, SNMP trap, and e-mail.
- **Lower bandwidth consumption:** push architecture reduces bandwidth by 80% compared to the polling architecture.
- **Faster response time** because of push technology and event handling
- **Data Logging:** Local data logged to SD card and pushed to host by TFTP.

Conclusion

Remote monitoring and alarm systems used in water distribution, pipeline management, and environmental monitoring applications must be capable of covering a wide area and function reliably. Most importantly, the cost must be affordable. A remote monitoring and alarm solution with Moxa's Active GPRS I/O devices and Active OPC Server help users overcome the frustrations associated with using dynamic IP addresses, and makes it extremely easy to connect to SCADA systems.

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.