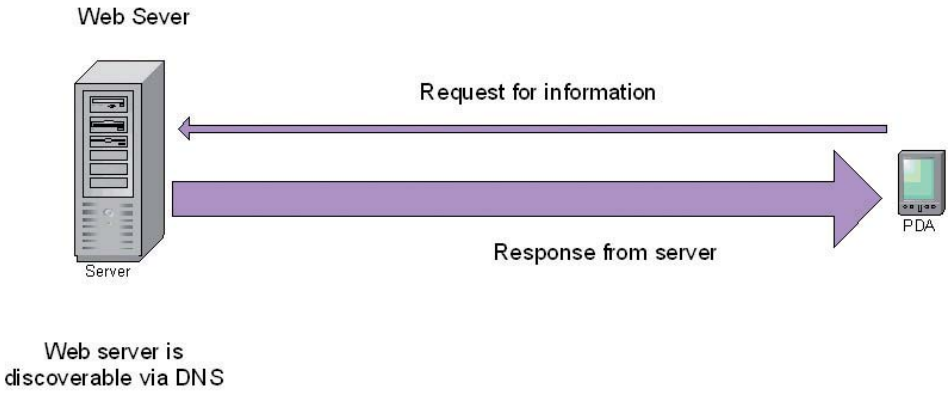
IP Connectivity over GPRS & 3G mobile networks

Introduction

This white paper will attempt to describe how a telemetry or control system can be implemented over the GPRS & 3G (UMTS) mobile networks.

Mobile Networks

The IP provision within the mobile service provider networks is designed around the need for WEB access from a mobile device. This can be seen in the asymmetric architecture of the up and down link with the bias being on the downlink having more bandwidth than the up link. The idea being that the handset or PDA will issue small requests for data to a server on the internet. The sever in turn will send large amounts of data in response to the request in the form of HTML pages or data files.



With this design criterion there is no real need for the handset or PDA (client) to have a static IP address. All requests for data transfer will be initiated from the client. The servers on the wider internet will have ether a static IP address or can be discovered using DNS (Domain Name System).

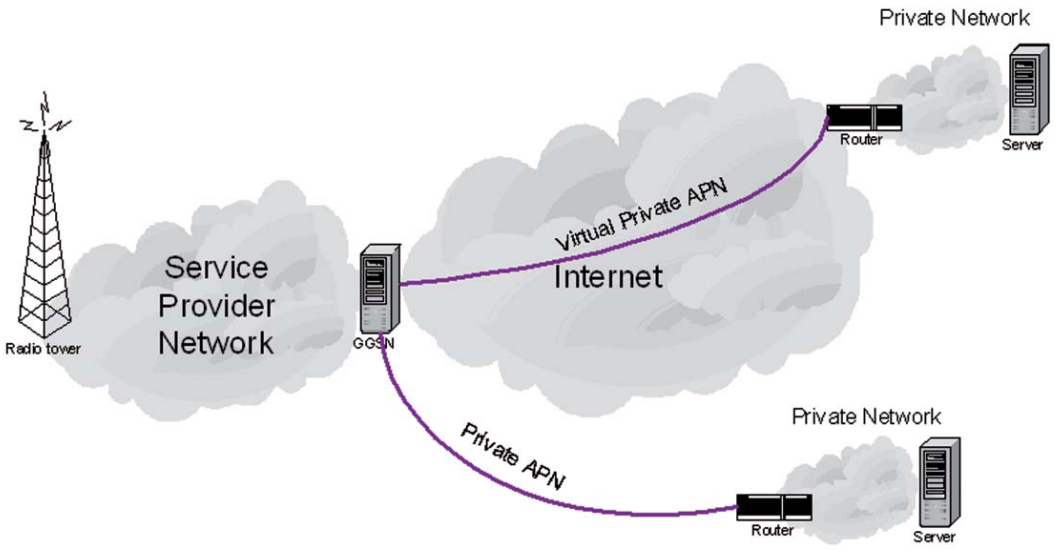
Another consideration for this type of architecture is the billing model and the need to conserve bandwidth within the service provider's network. The current billing model is to charge for each byte or Mb sent over the network to and from a device. To protect the subscribers on the network from being maliciously attacked by port scanners or "ping of death" attacks and to conserve the bandwidth within the service provides' network the GPRS and 3G networks are protect by a NAT interface between the service providers network and the internet. The NAT interface know as a GGSN (Gateway GPRS Service Node), will allow connections to be initiated from the service provider's network out to a server on the internet. The GGSN will prevent any attempt to initiate a connection from the internet into the service provider's network even if a devices IP address is known.

The mobile provider's network can be considered to be a private network, because the IP addresses issued internally by the mobile service provider are not directly accessible from the internet, in much the same way as laptops and PC on a company network cannot be directly accessed from the internet. Therefore it is not usually possible to directly access devices on the mobile network. There are exceptions, for example it is possible to get a static ip address from the service providers in Poland and some other providers in Europe. In France it is possible when using the Orange network to register the current IP address of a mobile device on a DDNS server (Dynamic Domain Name Server).

This architecture works well from a client/server WEB browsing perspective, where the servers are located externally to the service provider's network. However this type of architecture does not usually work for peer to peer communications within the service provider's network or with the requirement to open a socket to a remote device on service provider's network from a client on the internet. Again there are exceptions for peer to peer communications within a Service provider's network. You will need to check with the local service provider.

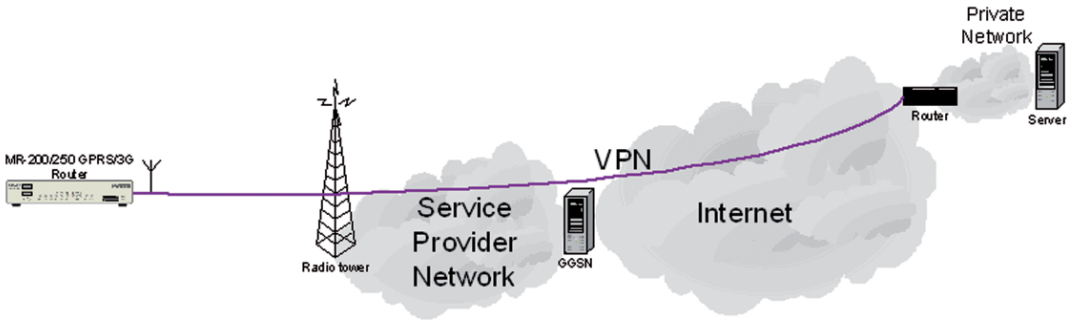
For a pier to pier connection to be established at least one end of a link must have a static or a discoverable IP address. Since the service providers do not generally support a DDNS service with the network, we must rely on a device having a static IP address. Currently the most common way a static IP address can be issued is via a third party supplier or via the provision of a private APN.

The provision of static IP address via a third party supplier or a private or Virtual private APN can also be used to overcome the restrictions imposed by the NAT interface. The third party supplier and the private APN can provide a direct connection to the service provider's network, bypassing the NAT interface and allowing clients external to the service provider's network access to IP addresses within the service provider's network. Because the device addresses are now static, a client external to the service provider's can open and close sockets via the third party connection or APN whenever there is a requirement. Equally the devices on the service provider's network can establish a connection to the external servers as required via the APN.



Although the APN does allow direct access to the service provider's network, access is limited to only the IP addresses and group of SIM cards within the assigned range for the APN. It is not possible to have access to the wider range of variable IP addresses or SIM cards that form the majority of the users on the service provider's network. Equally the IP address and SIM cards outside those allocated to the APN cannot get access to the APN. A SIM card will have to be provisioned or assigned to the Private APN before it can be accessed over the APN. It is not possible to pick any SIM card and get access to the closed group even if the correct credentials were known.

The requirement for static IP addresses can be negated by using devices with inherently more IP intelligence and functionality, such as the Westermo MR-200 and MR-250 which can work with static or variable IP addresses. These devices fall firmly in the category of routers. The key issue is the ability to support VPN (Virtual Private Network) tunnels originating from the router on the service provider's network to a router with an accessible static or discoverable IP address outside of the service provider's network on the internet or APN.



Conclusion

Whilst the provision of static IP addresses does offer a way of getting access to a remote site over GPRS or 3G, it does come at a high cost in most countries around the world. The alternative of using VPN opens up a huge range of possibilities in terms topology and reductions in running costs, but does require a little more thought at the system design stage. There are a number of other key factors that need to be taken into consideration. The local network coverage, the positioning of antennas and the length of the antenna feed cables all need to be considered for a system to operate successfully.

Ray Lock
Technical Director
Westermo UK