Hybrid GPRS/3G, ADSL Wide Area Networking systems

Introduction

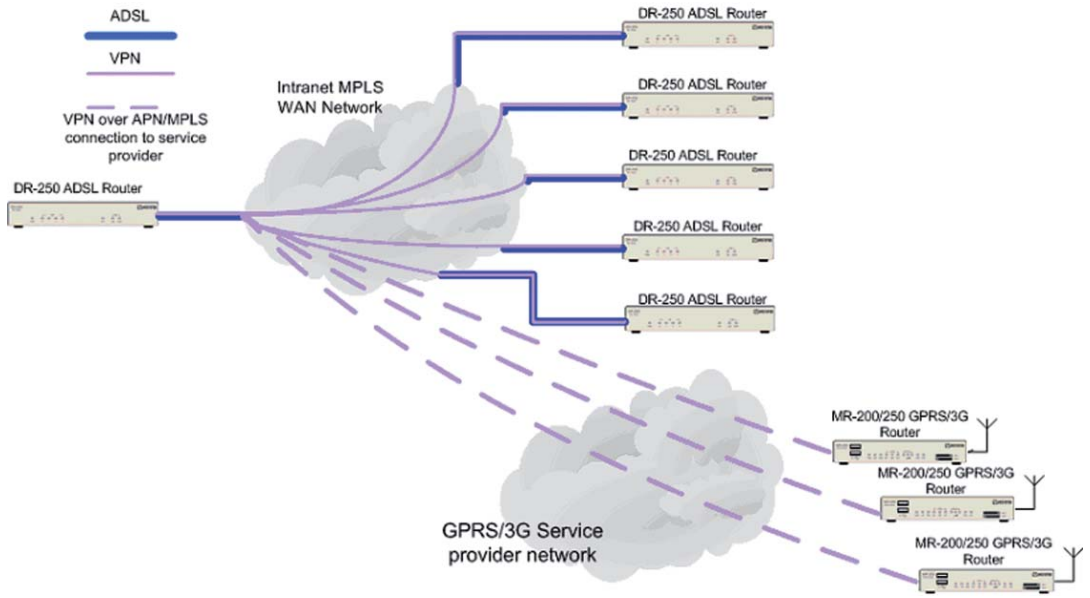
This white paper will attempt to describe how control networks can be implemented over WAN technologies such as GPRS, 3G (UMTS) and ADSL. Although the white paper will primarily discuss these technologies the principles can be applied to any IP environment connected over any media.

Hybrid Systems

The communications requirements for ever more complex control and monitoring schemes for utilities or industrial processes will not necessarily be met by any one technology alone. Coverage issues on mobile networks and bandwidth limitations will require an alternative media such as ADSL to be used to create links to some locations. By using IP as the transport and addressing mechanism the various remote locations can be seen as just nodes on a large WAN.

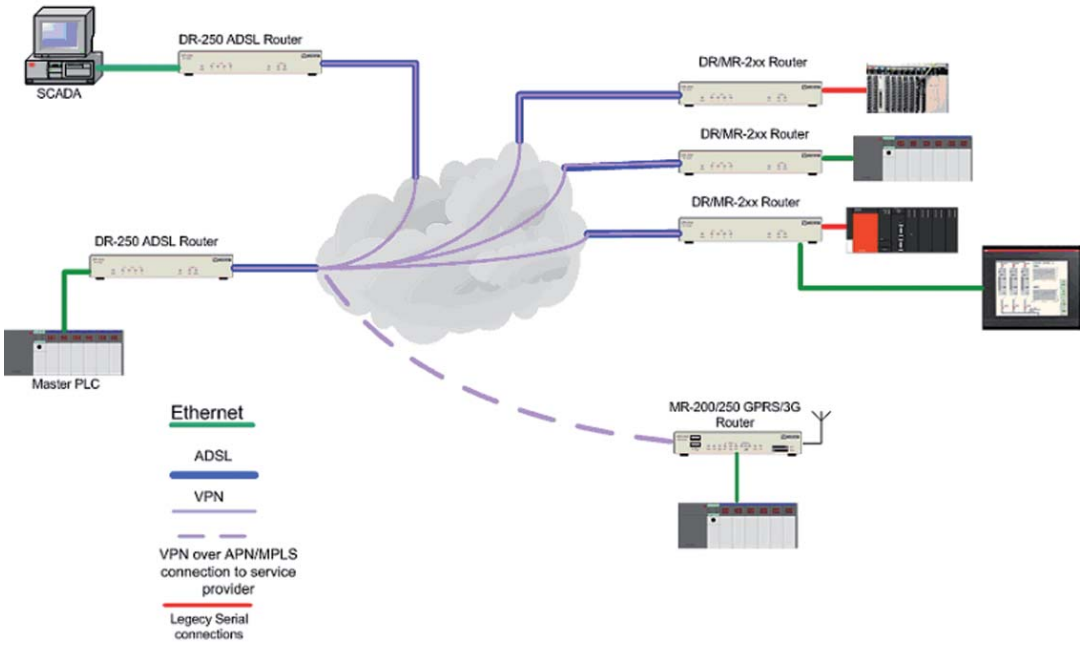
The media used to connect to a site can be seen as irrelevant and only the latency and bandwidth need to be considered. Hybrid systems that use multiple media types to provide the transport layer between sites would be a solution.

Wide area Telemetry network communications



The example below is a hybrid solution in a control environment. In this example a number of remote locations are linked to a central SCADA system over various types of media. Traditionally the solution to this type of system would have been to use analogue leased lines or x.21 connection.
These media are limited in bandwidth and costly to maintain and rent from telecoms providers. The hybrid ADSL/ GPRS/3G offer greater flexibility and bandwidth.

Control system over WAN networks

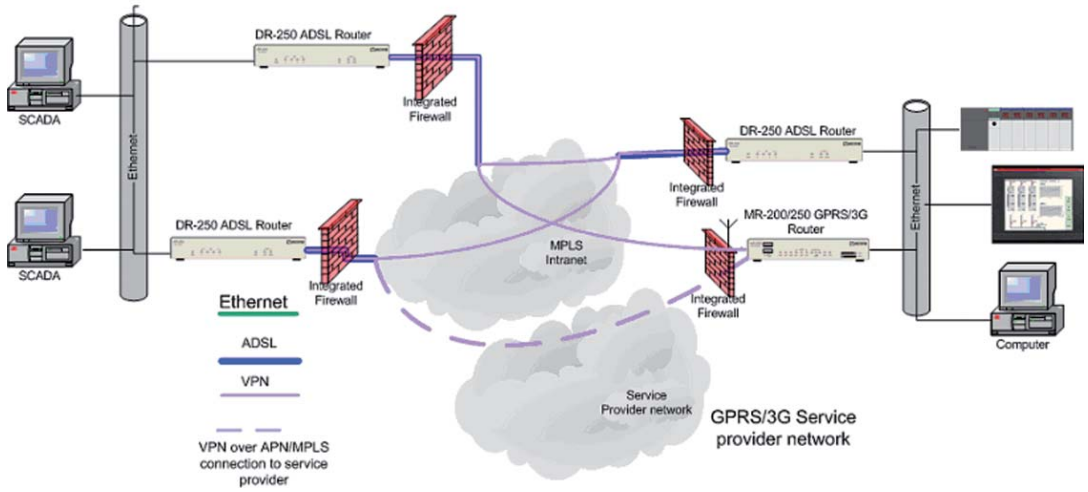


In this example the links between sites will be over VPN's (Virtual Private Networks). Effectively the VPN is the replacement for a leased line. To increase security the VPN's are secured using DES, 3DES or AES encryption.

Redundant or fail over communication

In some critical applications a single media connection or single interconnecting tunnel can be seen as a "Single Point of Weakness". Within the IP environment such concerns can be overcome by using multiple media connections and multiple VPN tunnels to interconnect the sites to provide redundant or fail over communications.

Dual Redundant VPN communications



Security

Security is always a concern when using the internet as part of the interconnection media. The treats are not just hacking or denial of service. There is a real concern on the part of national governments that any communications sent over a third party communication supplier is encrypted.

There are many ways to enhance the network security both internally and externally. External vulnerabilities can be dealt by using a wires only MPLS (Multi Protocol Label Switching) ADSL type intranet connection. This type of connection is readily available from ADSL and other service providers. Using an MPLS based service will ensure that traffic over the WAN is segregated from the internet. Typically it will not be possible to access the Internet from within the MPLS segment. Equally it is not possible to connect to any of the IP addresses within the MPLS segment from the internet. Outbound GPRS and 3G connections can be segregated from the internet by using a private or virtual APN (see white paper on IP Connectivity over GPRS/3G for more detail). The down side to MPLS and APN segregation is cost. The service providers will charge a premium as they will need to configure and maintain the segregation and to a degree dedicate bandwidth to the service.

When the Internet is used as part of the media or infrastructure other measures can be used to secure the traffic. By using IPSEC encrypted VPN's the traffic across a VPN will be encrypted using the most sophisticated encryption algorithms currently available. The Westermo MR and DR series routers support state of the art DES, 3DES and AES 128/256 bit encryption. The downside is that heavily encrypted traffic uses more bandwidth and processing power. The net effect of the extra bandwidth and processing is a reduction in throughput over a given link.

Security vulnerabilities from inside the network can be negated by using the state-full inspection firewall build into the Westermo MR and DR router. By setting specific rules to limit the access through the firewall, only site relevant data can pass. Any attempt to attack the network from within will be thwarted. The Firewall also provides an effective barrier to attack from the WAN or Internet side. For example the Firewall in the Westermo MR and DR routers can be configured to appear to be totally silent on the internet and respond only to authorised traffic. With such a configuration in place, WEB crawling software designed to find weakness and vulnerabilities will move on to the next IP address in their search list.

Conclusion

In conclusion it can be seen that by using hybrid combination of media it is possible to create fast flexible and resilient networks, ether over dedicated MPLS based infrastructure or the internet. The networks can be secured against attack from both internal and external sources. The less obvious benefit is a reduction in costs due to the move away from dedicated high cost circuits such as leased lines or X.21.