Virtual Private Networking over MPDS

inmarsat

VPN configuration over MPDS

Most companies now support a Virtual Private Networking (VPN) technology so that staff can securely access the corporate network while away from the office. The VPN enables access to the entire LAN, not just email.

The configuration for the remote mobile device (e.g. client software on the userís PC) is largely done by the VPN server they connect into. The corporate IT department will create a profile or configuration for the remote device/user and this will either by downloaded to the device, or requested by the user software on first connection.

In the case of client software, some user verification might be required the first time a connection is made.

MPDS provides a direct connection to the Internet, exactly as if a dial-up connection had been made through a standard Internet Service Provider. Thus, there is no extra or special configuration to enable VPN over MPDS. If a standard VPN connection cannot be made, it is worth contacting your LESO to ensure that there are no restrictions in place for your connection that might stop the VPN connection from working.

VPNs with MPDS

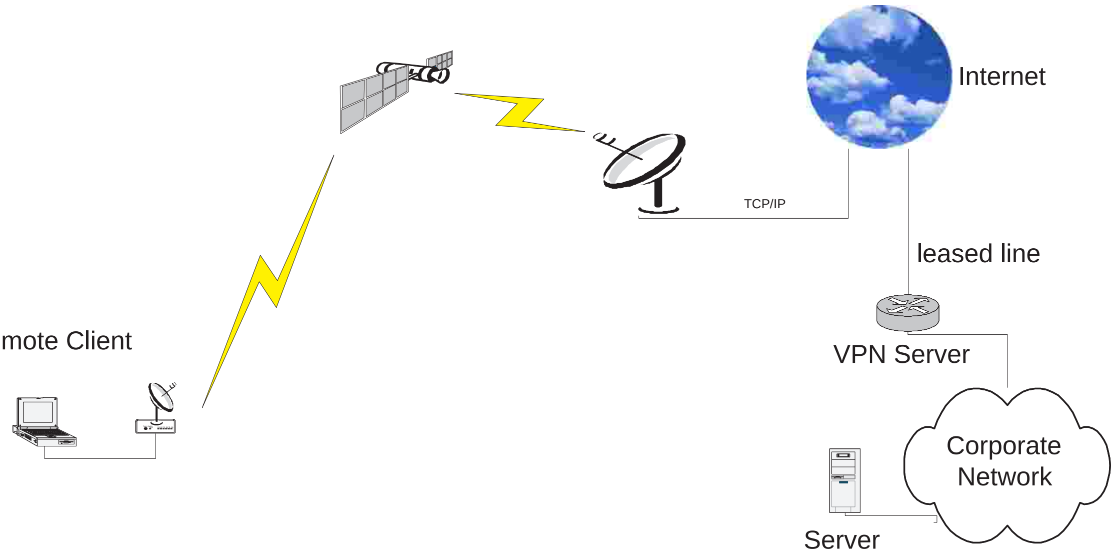
Some Inmarsat LESOs provide VPN services for their customers. By providing this service at the LESO, data traffic between the MES and the LESO is not part of the VPN. This traffic is secured by the standard mechanisms used within the MPDS network, and means that no extra overhead is introduced by further encryption and encapsulation of packets. However, no additional protection for the satellite hop is provided by such a partial VPN approach. An end-to-end VPN creates a distinct overhead, but also can provide better security on the satellite link.

MPDS example solutions

A VPN is likely to be configured in one or two ways, which are discussed in the following sections:

- Point to point VPN
- Client to Server VPN

Point to Point VPN



Point to point VPN

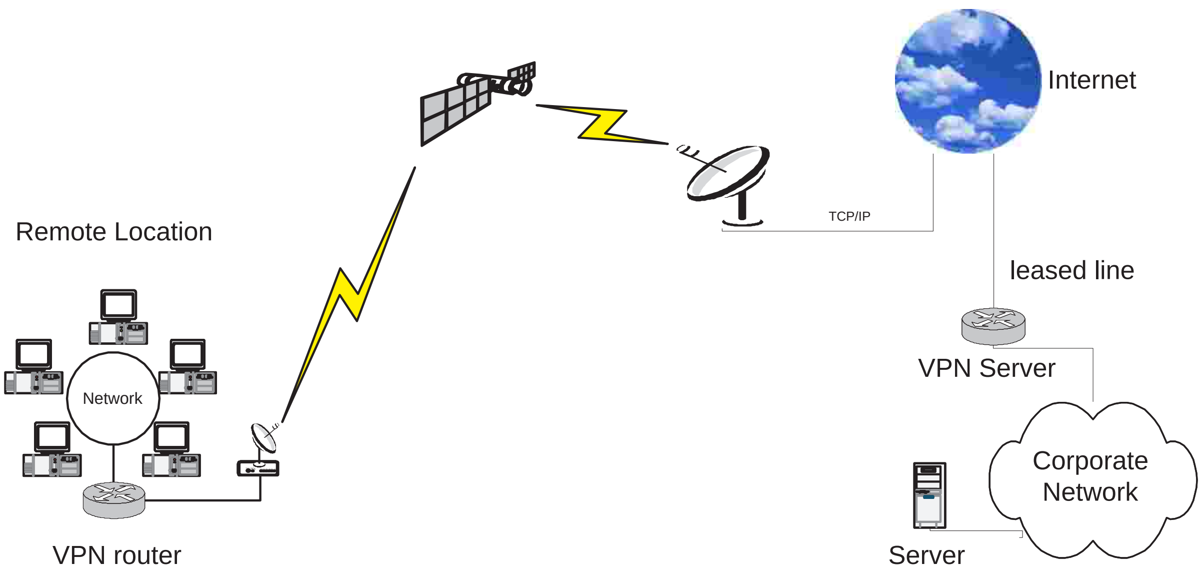
A point to point VPN solution is usually used when connecting two sites, or a remote site to a head quarters. The remote site may have one or more PCs, printers and other equipment connected using a LAN. The point to point VPN is set-up by a VPN capable router which connects to a VPN server at head quarters and provides a VPN tunnel for all traffic between the remote LAN and the HQ's network.

Clearly a point to point VPN solution is ideally suited for remote LANs connecting into corporate head-quarters. There are a number of hardware solutions on the market, the most commonly used being Cisco routers. For the above scenario, a Cisco VPN concentrator is required at corporate head quarters, such as the Cisco 2600 range, (with VPN capability) or the Cisco PIX range, which are combined firewall/VPN servers. At the remote site, a router such as the Cisco 1700 may be used.

Client to server VPN

A client to server VPN solution is used when individual clients are connecting in separately to a central site. The above solution may be used for individual clients, but it involves equipping each client with a router. Thus it is more common to use some VPN client software on the client lap-top.

Client to Server VPN



Commonly used VPN client software is:

- Cisco SecureClient; which connects a remote user into a Cisco VPN server
- Checkpoint VPN client; which connects a remote user into a Checkpoint Firewall with VPN capability
- Microsoft Windows; is capable of connecting to a number of VPN servers

The client software chosen is largely dependant on the existing infrastructure of the corporate network. The existing corporate firewall is probably upgradeable to support VPN connections, and thus the appropriate client software is used.

About VPNs

A VPN aims to provide a secure tunnel, over another (insecure) network. This enables secure traffic to be sent over the Internet, by running a 'virtual' network over the top. When used over MPDS, it ensures that data is secured from the device attached to the MPDS terminal, all the way to the VPN server, based inside the corporate network.

The use of VPNs is becoming more common, largely because of the availability of VPN protocols and technologies in the Microsoft operating systems. In addition, there are many other companies that provide VPN technologies for Microsoft and other platforms.

VPNs use two main standards:

- PPTP (Point to Point Tunnelling protocol)
- IPSEC (Internet Protocol Security)

Point to Point Tunnelling protocol

PPTP was designed by a consortium including Ascend, 3com, Telematics, US Robotics and Microsoft. The protocol was designed as an encapsulation method to enable other network protocols to be transmitted over a TCP/IP network. The ability to encrypt the tunnelled data was added later, and led to the protocol being used as a method of setting up a VPN.

The specification allows for a number of encryption and authentication methods, but most systems use the Microsoft solutions, which have some limitations, depending on the version used.

Initial versions of Microsoft PPTP relied on the users domain password in order to create an encryption key. As the domain passwords are frequently less than 10 characters, the generated encryption keys cannot be as secure as a key created randomly, from much longer strings.

Later versions of Microsoft VPN solutions have alleviated some of these problems, but remain to some extend backwardly compatible, and thus clients can request older methods of security, which may result in less effective data encryption.

Internet Protocol Security

IPSEC is an evolving Internet standard that enables IP packets to be both signed and encrypted. An IP packet consists of a header and a data payload, both of which can provide potentially useful information for an attacker. IPSEC provides mechanisms to encrypt and sign the data payload, as well as sign the headers, so that source and destination addresses can be trusted.

IPSEC can also be used in a tunnel mode, which encapsulates the whole IP packet inside another, after encrypting the whole packet (both header and data). This is frequently used where packets are transmitted over networks utilising NAT (Network address translation) systems, which change the headers of packets as they pass through.

VPN Advantages and Disadvantages

As VPNs must encrypt and decrypt all packets, this can put a considerable load on the VPN server (and client), as well as on the corporate network and Internet connection. VPN servers are either hardware solutions (encrypting routers), firewall solutions (plug-in modules for firewalls), or software solutions. In all cases, an overhead is placed on the network, but clearly a hardware solution can best cope with the processor power needed to run strong encryption algorithms.

VPNs provide a tunnel for data traffic. This entails taking each data packet, encrypting it, and placing it inside another data packet. Its not hard to see that, for a full packet, encrypting it will increase its size, and placing this larger amount of data inside another packet will again increase the overall traffic sent over the network. For networks like MPDS, where data traffic should be kept to a minimum for cost reasons, this should be remembered.