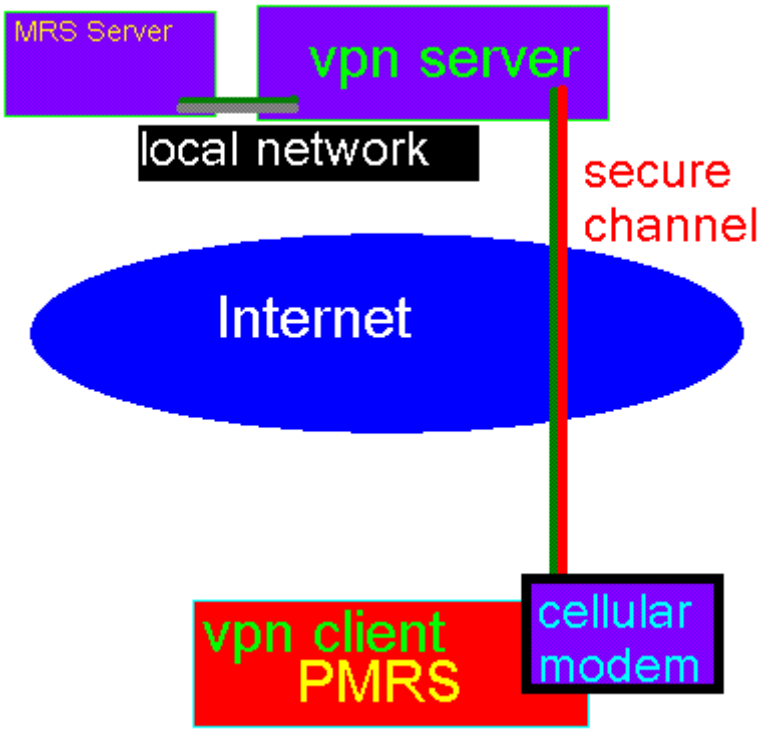
PMRS with Open VPN

This document describes connecting and using the PMRS devices with an Open VPN server. It applies to firmware version 5.0.0.3 of the PMRS devices.

The PMRS units model 101 and 102 (not including MRS-400 and PMRS-100) versions 5.0.0.2 and above include a configurable Open VPN client version 2.3.2. This built-in Open VPN client is capable of connecting to an Open VPN server using the PMRS built-in cellular modem connection.

It connects using the default Open-VPN settings of UDP port 1194 and creates a virtual network over this connection. This virtual network can be encrypted using TLS if provided with the authentication parameters: RSA certificate, key, and CA certificate. TLS supports a number of ciphers, including DES (40 bits), 3DES (168 bits), AES (256 bits) and RC4 (128 bits). The selected encryption cipher is a result of the negotiation between the TLS client and the TLS server.



In order to have the PMRS media connection encrypted as part of the VPN, it must use the virtual network addresses instead of the internet addresses in the MRS Connection section of the Device Config Utility. Either the PMRS is a client that connects to an MRS Server using its virtual address (in the remote address field), or it is a server (local server selection) and the MRS Client will use the virtual address of the PMRS device to connect there. When using the virtual network addresses, it is possible to have a PMRS working as a server with a known virtual address even if it receives a dynamic or private address from the cellular provider.

The following parameters are configurable using the PMRS Device Configuration utility for tuning the Open-VPN connection:

Device Config Name	Open-VPN Name	Description
VPN Type	-	Enables selecting Open-VPN as the type of the VPN. If “None” is selected, the VPN will be disabled.
External Address	remote	The address of the Open-VPN server. This address must be accessible from the cellular network.
Existing/Routing network	dev tap/tun	Whether the VPN bridges two existing local networks with existing addresses, or being a network tunnel with new addresses.
Address configuration method (bridge)	-	Use “None”. This setting is actually controlled by the VPN server.
Manual Configuration (bridge)	-	Not to be used. These settings are actually controlled by the VPN server.
Local Address (tunnel)	ifconfig	Host address in the VPN.
Remote Address (tunnel)	ifconfig	VPN Server address in the VPN.
Certificate	cert	TLS certificate (with public key) of the PMRS device in the VPN.
Private Key	key	TLS Private key of the PMRS device in the VPN.
Certification Authority Certificate	ca	TLS certificate (with public key) of the certification authority used by the VPN server.

In addition to configuring these parameters above, one must also check the “Enable VPN” box in the modem section of the device configuration utility. That will enable using this VPN for the cellular connection.

Read the Open-VPN manual for more information about configuring Open-VPN.