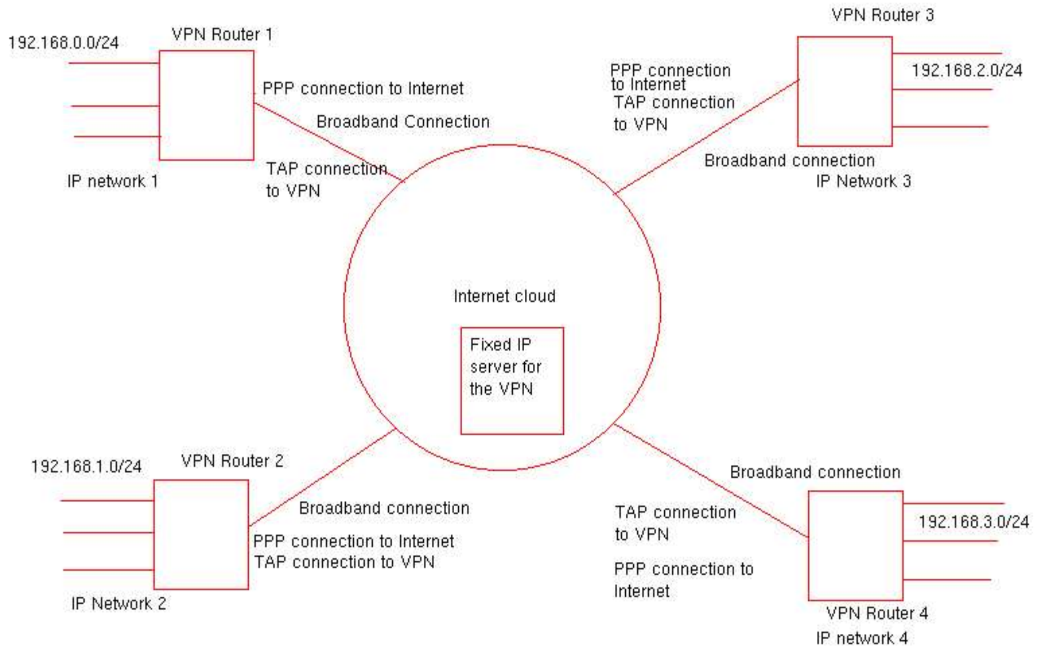
How to connect your distributed networks via the Internet using a VPN.

Problem statement:
I have a number of offices across the country. I need to be able to link them up, but I can not afford Diginet lines between all my offices. The cheapest Diginet solution of 64k is also too slow to make it worth my while. I would like to use ADSL, but there are no static IP addresses that can be allocated to me. Dynamic DNS also lags too long for updates to make a broadband connection viable for me.

Solution:
By using a VPN (Virtual Private Network), you can use the broadband connection of your choice. Each branch office needs a VPN router that is connected to your broadband Internet access point. Your internal private IP network will be accessible via the VPN interface on your router.

Dynamics of the VPN.



As can be seen, the local Internet connections make use of public IP addresses obtained from the ISP. The internal networks make use of private IP addresses. The fixed IP address server on the Internet is used to control access to the VPN as follows: Say VPN node 1 connects to the Internet to establish a connection to the VPN. The fixed IP server contains the Certificate authority's certificate as well as the client's certificate. The client presents the keys to the server. If it is accepted by the server, a virtual TAP device is created on the client, with a private IP address, say 10.10.1.1 on the server and 10.10.1.2 on the client. If node 2 connects successfully, it will be assigned IP address 10.10.1.3. Assume for the explanation that a class C network was configured with a net mask of 255.255.255.0. Therefore there can be 254 nodes on the VPN.

The nodes can now communicate their routing tables to each other. There will now be two class C networks on each machine, one the local network and the other the TAP network. Logically each local network is only one hop away, no matter how many physical hops are in between.

Because it is a TAP interface with a class C network, the traffic needs not be directed through the VPN server, but directly to the remote node acting as a router for the requested network.

All nodes are monitored by the server and each node monitors it's own connection as well. Should the connection go down on a node, it will immediately restart the connection, renegotiate the certificates and re-establish the connection. This can be set to ping every 15 seconds, for instance. If an ADSL connection is used, you will get an effective 512/256k throughput through the system. Should the ADSL fail, a backup system like ISDN can be used as a backup. This system will eliminate the need for specialised equipment like Cisco routers, which can be the cause of extended downtime in the case of failure. Each VPN/Internet router is a normal generic computer loaded with Linux and a VPN client and hardware failures can be rectified within minutes.

All the local networks use the PPP connection for normal Internet traffic.

All data running across the VPN is encrypted with 1024 bits and data compression is accomplished with the LZO algorithm.

Connectivity costs can be greatly reduced because all connections are just local Internet connections, instead of expensive dedicated data lines. Security is greatly enhanced due to the fact that no data will be accepted unless a valid certificate is offered. The VPN also runs on private IP addresses, making it invisible on the Internet

Contact details:
Email: tommy@netsurfers.co.za
Telephone: 041 922 8891
Cellphone: 082 436 9324