6.1 Introduction to VPN

Virtual Private Networks (VPNs) are a common way to connect remotely to a network in a secure fashion. A VPN creates a private network connection over the Internet to connect remote sites or users together. Instead of using a dedicated connection, a VPN uses virtual connections routed through the Internet from the remote site or user to the private network. Security is accomplished by encrypting all the transmissions.

A VPN allows a remote user to have network access, just as if it was local to the private network. This does not only connect the user to the network as if the user were local, but it also makes the connection secure. Due to the fact that most organisations have many employees traveling and working from home, remote network access has become an important security concern. Users want access and administrators want security. The VPN is the current standard that offers both.

To accomplish its purpose, the VPN must emulate a direct network connection. This means it must provide both the same level of access and the same level of security as a direct connection. To emulate a dedicated point-to-point link, data is encapsulated, or wrapped, with a header that provides routing information allowing it to transmit across the Internet to reach its destination. This creates a virtual network connection between the two points. The data being sent is also encrypted, thus making that virtual network private.

A VPN does not require separate technology or direct cabling. It is a virtual private network, which means it can use existing connections to provide a secure connection. In most cases it is used through normal Internet connections.

A variety of methods are available for connecting one computer to another. Once upon a time it was common to dial up to an ISP via a phone modem. Nowadays cable modems, cellular devices, and other mechanisms are more common. All of these methods have something in common: they are not inherently secure. Any data that is sent back and forth is unencrypted. What is more, it is a fact that anyone can use a packet sniffer to intercept and view the data. Finally, neither end is authenticated. This means you cannot be completely certain who you are really sending data to or receiving data from. The VPN provides an answer to these issues.

This sort of arrangement is generally acceptable for an ISP. The customers connecting simply want a channel to the Internet and do not need to connect directly or securely to a specific network. However, this setup is inadequate for remote users that attempt to connect to an organisation’s network. In such cases the private and secure connection that a VPN provides is critical.

Individual remote users are not the only users of VPN technology. Many larger organisations have offices in various locations. Achieving reliable and secure site-to-site connectivity for such organisations is an important issue. The various branch offices must be connected to the central corporate network through tunnels that transport traffic over the Internet.

Using VPN technology for site-to-site connectivity enables a branch office with multiple links to move away from an expensive, dedicated data line and to simply utilize existing Internet connections.