What Is A Virtual Private Network?

By Robert Moskowitz
ICSA / Network Computing

I've come to appreciate the fact that virtual private networking means different things to different people. In fact, there is a major disconnect among vendors and consumers in our communications industry on this item. After much thought, I have some ideas to share--and a few more buzzwords for you to digest. The debate comprises three questions: What is virtual? What constitutes privacy? And is it a network?

Virtualosity Webster's Dictionary defines virtual as "being such practically or in effect, although not in actual fact or name." So for something to be a virtual network, it should act like a network, yet not be one. It's a wonder then that anyone could classify only some networks as virtual since all networks are virtual to some extent. Perhaps we can make the separation based on physical wiring. If there are real wires among all of the nodes, then the network is not virtual. Based on this determination, WANs have been virtual since the telcos stopped provisioning T1 circuits on conditioned copper and started using channelized T3 circuits instead.

Perhaps a better determinant is whether the network connections are on-demand or dedicated. An on-demand network is made of connections that can be controlled by network administrators, instead of their telecom partners. A network made of connections controlled by a third party like a telco, ISP or telecom analyst is a dedicated network. At some point in this type of network, administrators lose control of the physical network, sometimes right past the building hubs. Thus, for all practical purposes, on-demand networks are built above the network layer because this is the only place accessible to network administrators for their entire network.

Pssst! Got a Secret? What is private for one person is all too often very public for the next. Over the years I've heard of numerous cases of tapped lease circuits, both legally and illegally. We shouldn't use the word private when we mean secure. After all, my front yard is private, yet open for viewing to anyone who wants to see my weedy lawn. Private is defined by Webster's as "of, belonging to, or concerning a particular person or group; not common or general." So a private network is one where you acquire exclusive use of the network links. This is contrasted with a public network where the ownership or payment is dispersed across all of the network residents.

A secure network is an altogether different type of network. Secure networks might be private or public. Security is rarely accomplished in the manner in which the network is provisioned, unless you have armed guards patrolling the wires. In many cases, only the WAN links are secured as a part of their provisioning. This type of secured networking is done with encrypting hardware that delivers security just below the network layer. Secure networking can be more consistently provisioned above the network layer, just like on-demand networking.

This little exercise provides us with a handful of interesting network types. The most common special type of network found is the DPN (dedicated private network). A DPN is what you get almost every time you order a WAN from a third party (regardless of the method--leased circuits, frame relay or ATM) or build your LAN with ATM switches instead of wiring hubs. These technologies let the telecom analyst specify which devices actually have data paths between them, which may be different from the actual physical wiring. Thus a private network, again, is where the data paths are defined by someone for someone and these can consist of physical wiring or specific data links over shared wiring.
This type of private network is different from DSNs (dedicated secure networks), which are standard for banks and military operations. A few companies have implemented DSNs for their international links because of industrial espionage concerns. In a DSN, the WAN links are secured with link-layer or physical-layer encryption devices. The new trends, however are for ONs (on-demand public networks) and OSNs (on-demand secure networks).

Networks When You Need Them The concept behind on-demand networking is that the node can join the network for any desired function at any time, for any length of time. The common approach is to tunnel IP within IP with some layer in between to provide the on-demand management. Two technologies are emerging for this: L2TP (Layer 2 Tunneling Protocol) and IPSec (IP Security Protocol).

L2TP combines a number of existing technologies to create manageable on-demand networks. For the most part, L2TP does not claim to offer security. There are two proposals for gaining security: using IPSec in its transport mode or using a much weaker--though in some cases adequate--PPP security. L2TP, as its name implies, tunnels a link-layer protocol over IP. This allows for support of multiple protocols over an IP network, such as IPX or AppleTalk. The connection management protocol within L2 TP lets the network administrator control the valid L2TP links. L2TP is targeted for remote clients, but some servers, routers and gateways will support it for network-to-network links. L2TP may not be common in firewall products as its security is not recognized as fully secure.

IPSec provides network-level security for IP. Its management protocol, ISAKMP/Oakley, is also a security protocol and protects against man-in-the-middle attacks during the connection setup. IPSec in hosts as OS components or BITS ("bump in the stacks") implementations can work with gateway or router implementations, such as BITW ("bump in the wire") to create secured, on-demand network connections. The distinction between L2TP and IPSec is an important one. L2TP supports on-demand connections that can be secured. IPSec provides security that supports on-demand connections.

Choices to Make Instead of shopping for a virtual private network, now you can shop for a DPN, DSN, ON or OSN, according to whatever suits your networking needs. You can mix and match to provide the most cost-effective networking for your organization, instead of buying what's marketed most effectively to your management. If someone out there can propose more pronounceable terms than OSNs, let me know. I'm always looking for better ways to express what's really happening in networking.

Robert Moskowitz is a senior technical director at the International Computer Security Association and a member of the Internet Architecture Board (IAB). He can be reached at rgm@htt-consult.com.