Total Private Network Solution to Overcome the Limits of Packet Encryption VPN Performance via Satellite

White Paper

April 2006

Abstract
This paper explains the source of severe throughput degradation experienced by IPSec and other data communication protocols over a satellite link. It describes a specialized hardware solution that enables highly efficient end-to-end private network performance over satellite circuits despite inherently lengthy signal propagation delay. Details are provided on features and functionality of this innovative technology.

Virtual Private Networks
A Virtual Private Network (VPN) allows users to communicate and access information securely over the public Internet and other IP based networks. VPNs operate as seamlessly and securely as a true private network, but take advantage of the ubiquitous global coverage of the Internet. Secure virtual connections or “tunnels” are established only when needed to provide network connectivity for a closed user community. IPSec (IP Security) is a protocol suite widely used for VPN solutions that allows secure exchange of data packets at the IP layer. Using encryption and other technology, VPNs typically support four important areas: authentication, confidentiality of information, access control, and data integrity. Most VPN solutions are suited for intranet, extranet, site-to-site and remote access configurations.

Satellite Communication
Satellite communication technology has been available for many years and is an ideal medium for simultaneously disseminating information to many users, linking remote geographical locations, and providing connectivity to wide coverage areas. Via radio transmission, impressive data rates can be obtained using high capacity transponder channels. As the demand from businesses for broadband data services increases, satellite communication is well positioned to address this need. DSL and ISDN fulfill much of the demand in a cost-effective manner, but these services are not available throughout all of North America and the world. A small satellite antenna or VSAT (Very Small Aperture Terminal) can be placed virtually anywhere to provide high-speed connectivity for remote offices or single users.
**Satellite Signal Propagation Delay**

Satellite communication technology is based on electromagnetic waves passing between earth-based antennas and a radio transceiver in space. This is the same fundamental principle used by terrestrial microwave systems, with the notable exception that signals must travel a much greater distance between satellite antennas on the ground and a repeater in orbit. In order for a satellite in space to appear stationary relative to the earth’s rotation, it is placed in a geostationary or geosynchronous orbit. This represents a distance of approximately 22,300 miles from the surface of the earth. Even though electromagnetic waves travel at the speed of light, roughly 186,000 miles/sec, the lengthy distance introduces a relatively long latency period. This delay can dramatically affect performance of certain data communication protocols that were designed to operate on terrestrial based networks.

The time for a signal to travel from one satellite earth station to another is nearly ¼ second, which can be computed by dividing the total distance traveled by the speed of signal propagation. A return transaction doubles the total transit time, increasing it to almost ½ a second. For comparison, a round-trip terrestrial transaction using copper or fiber mediums between New York and London requires approximately 0.038 seconds, well over 10 times quicker than via satellite. Transactions requiring less distance between nodes are considerably faster. These calculations exclude additional time required for processing by electronic equipment at the originating, receiving, and repeater stations, which adds to the total delay. In practice, round trip transaction time is typically at least 700 milliseconds.

**TCP/IP over Satellite**

Internet and World Wide Web connectivity is made possible through use of the TCP/IP protocol suite. TCP is a connection oriented end-to-end communication protocol that enables reliable transport of data between network nodes. In short, the protocol functions by breaking an electronic file into small packets of data, sending them along with control information, and then waiting for acknowledgements indicating they were received successfully before more data is sent. The process of sending data and receiving acknowledgements is normally rapid and quite efficient. TCP uses a mechanism called slow-start to ascertain the maximum data rate of a channel upon initial connection setup. After sending a packet, it waits for an acknowledgement. When a response is received, an increasing number of packets are sent in the next transmission and the process continues in a similar manner. When a positive acknowledgement for a data packet is not received within a set time period, the rate at which subsequent packets are transmitted is slowed down in an attempt to optimize throughput.

There are well-understood and long-standing technological problems preventing optimal TCP communication over satellite links. TCP was designed to function most effectively on common terrestrial-based networks that exhibit much shorter round-trip latency than that of a satellite channel. In fact, the intrinsic ½ second
round-trip delay for a satellite circuit exceeds the timeout period during which TCP expects an acknowledgement. Because of this, the protocol assumes there is network congestion and will continue sending all subsequent transmissions at a slow rate, never escaping slow-start mode.

**Protocol Acceleration**

Given the widespread use of TCP/IP and satellite communication technology, solutions have been developed to compensate for the effects of space segment latency. Performance enhancement proxies, most commonly in the form of TCP accelerators, isolate the satellite portion of a circuit from the terrestrial leg, thereby avoiding adverse effects of a high latency satellite link. Caching and pre-fetching allows configuration parameters, such as window size, for each portion of the circuit to be optimized independently. This, in effect, allows signal propagation delay to be hidden from the originator. Since packet acknowledgements are returned rapidly by a terrestrial link, TCP quickly moves out of slow-start mode and builds to a fast processing speed. Under ideal conditions, acceleration technology allows satellite users to obtain throughput performance equivalent to a comparable terrestrial circuit since the effects of signal propagation delay are essentially negated.

**IPSec and Acceleration**

Though IPSec VPNs are built to operate atop an IP infrastructure, they cannot capitalize on acceleration benefits due to protocol design and the manner in which encryption is employed. Since IP Security data is transmitted using an IPSec packet type—not a TCP/IP packet format—they simply cannot be interpreted by TCP protocol acceleration methods. Furthermore, IPSec encrypts and encapsulates not only data, but also the TCP and IP headers that are needed in clear text by acceleration logic to function properly. Due to these factors, protocol acceleration functionality is rendered useless and IPSec packets traverse performance enhancement proxies without any action being taken. They are then forced to make a time-consuming journey over the satellite channel to a receiving node where they can be decrypted, at which point acknowledgements are generated and sent back over the satellite circuit to the originator. The round-trip satellite connection adds over a ½ second delay between packet transmission and acknowledgement—a long time in the realm of electronic data communications. Since this same process takes place for every IPSec packet, the effects of propagation delay and processing time accumulate and are manifested in the form of significantly reduced throughput of up to fifty percent.

Due to protocol design and the laws of physics, IPSec cannot escape the adverse impact on throughput resulting from satellite circuit latency. The ability to locally accelerate a remote receiver is not feasible and throughput is consequently limited by the need to acknowledge each data packet individually over a satellite link.

**Total Private Network Technology**

Ground Control’s Total Private Network technology circumvents performance
problems experienced by IPSec and other network layer protocols when subjected to satellite circuit propagation delay. Utilizing true private network connections via satellite and not operating at the network level where IPSec functions, Ground Control’s technology takes advantage of a satellite network’s existing protocol acceleration capabilities and other performance enhancement techniques.

Figure 1 provides a high level overview of the path for sending data from a user’s client application to a secure server residing in a trusted environment. With Ground Control’s solution, all user data and sensitive addressing information traversing the satellite link is fully encrypted at the transport layer using constantly changing Triple DES (3DES) session keys.

When the client receives data and associated communication information (such as an IP hostname and address header) from an application, it is packaged and prepared for transmission. This information becomes the payload of a standard TCP/IP packet destined for the corporate network. After traversing the satellite link to the NOC, the acceleration server receives the packet, un-packages the payload and performs validity checks. In this manner, the payload is never hidden from the acceleration server, providing it with the required header information. Once validated, the acceleration server interprets the TCP control information, sends an acknowledgement to the originator, and forwards (proxies) the message on to the final destination. Immediately after the originator receives a positive acknowledgement, it transmits the next packet—while previous ones are in transit over the satellite channel—and the process continues. Since this happens rapidly, TCP quickly moves out of slow-start mode and builds to the fastest rate supported by the connection. TCP acknowledgements returned from
the receiving node are intercepted by the acceleration server and discarded before they can reach the originator since they would be duplicates.

It is important to realize that the Total Private Network architecture is provided from a client’s system to the corporate network, thereby ensuring end-to-end protection. This is possible because of the private circuit and/or VPN connection based architecture that allows a highly secure path to be maintained from an end user all the way to the target destination.

Since Total Private Network technology allows packets to appear as standard TCP/IP traffic, they are not subject to NAT (Network Address Translation) issues or firewall traversal problems commonly encountered with IPSec VPNs. These areas are a source of implementation and ongoing maintenance headaches that make deployment and management of a VPN a time-consuming chore requiring skilled network technicians. Corporate network addressing can be passed all the way to the client machine to ensure transparent network activity.

Total Private Network technology has no performance degradation as its payload data is unencrypted TCP/IP traffic over satellite.

**Conclusion**

By operating with the Total Private Network architecture and leveraging a satellite network’s TCP protocol acceleration capabilities, Ground Control’s Total Private Network technology is able to deliver impressive throughput efficiency over high latency satellite links. Secure network connectivity is provided from an end user all the way into a corporate environment without exposing any user data or sensitive addressing information.

Ground Control is a leading provider of high-speed Internet to mobile or stationary professionals. We specialize in HughesNet (formerly known as Direcway) satellite Internet and we’re the leading provider of HughesNet Total Private Network architecture. Our Galileo VSAT system is for the performance minded and is also available for use separately or in addition to our HughesNet offering. Our Magellan MSS product line provides mobility to the Total Private Network technology and makes any vehicle, truck or RV into a mobile office.

There are many questions to ask and answer when setting up a Total Private Network and we highly recommend that you speak with a sales engineer at Ground Control for more information. Please visit www.groundcontrol.com or call 800-773-7168.