

Enterprise VPNs: Choose Performance, Reliability, and Low Cost

IT executives are always asked to provide more with less, particularly in this challenging economic environment. There is constant pressure to deliver business applications with higher performance (speed and reliability) at a lower cost. For the distributed enterprise, there have typically been two choices for Wide-Area Network (WAN) Virtual Private Network (VPN) solutions—broadband VPNs or an MPLS solution. What if there were a new third alternative that offered more performance at a better price point than either of these two approaches?

This white paper compares the costs and risks associated with traditional broadband VPN and MPLS approaches, followed by an examination of a new high-availability VPN solution from Hughes. The Hughes solution overcomes the drawbacks associated with traditional broadband IP-VPN and T1-WANs, delivering unprecedented availability, high-performance bandwidth, and robust security—all at a competitive price point.

The Challenge

Companies that rely on WAN-VPNs need extremely reliable, high-performance connectivity in order to keep revenue flowing, customers satisfied, and operations running. These communication links are especially crucial for distributed enterprises in the retail, financial, hospitality, and insurance industries.

As business applications outgrow the capabilities of existing WAN connections, IT executives need to upgrade their networks in order to increase throughputs while improving overall reliability, availability, and security—all within justifiable costs.

Traditional Approaches and Their Drawbacks

Companies typically are presented with a choice between conventional broadband VPNs (DSL, cable, or some variant) or a T1-based MPLS solution. With a broadband VPN approach, it's possible to achieve good performance at low cost, but reliability may suffer. An MPLS solution offers good performance and better reliability, but costs will be much higher.

The T1-MPLS Option

Over the past few years, carriers have evolved from legacy frame relay to IP offerings such as MPLS. However, the last mile access is still usually a standard T1, or, to a limited extent, T3 and Ethernet.¹ And while application bandwidth demands have increased significantly over the past few years,² network pricing has remained high. Typical T1 access costs \$450-\$600 per month or higher, depending on network service.³

MPLS is considered highly reliable and secure, and the technology also scales well, providing increased capacity on demand. However, it's very expensive to roll out MPLS across hundreds, let alone thousands of distributed sites.

The Broadband VPN Option

Broadband VPNs, like DSL and cable, are much less costly than T1, but they have a reputation for being difficult to deploy and manage. In the past, the technologies also lacked the reliability and performance necessary for enterprise-critical applications and data. By leveraging DSL and cable technology as part of a 'hybrid approach' to managed VPNs, innovative solutions are beginning to appear that overcome many of these disadvantages.

¹ 55% of all VPN connections utilize T1 access, ENS, Vertical Systems Group, 2008

² Bandwidth requirements expected to grow 35-50% for the near-medium term, Gartner, 2008

³ ENS, Vertical Systems Group, 2008

A New Approach

What is needed is a new approach—a WAN-VPN solution that delivers the performance of MPLS, but at a broadband VPN price. Key attributes should include the following:

- **High performance/bandwidth** for rapid processing of enterprise-critical applications
- **High reliability/availability and redundancy** to eliminate costly downtime
- **Robust security** to ensure privacy and protection across the network
- **Low cost** which is crucial in good times as well as bad

Fortunately, due to new creative technology improvements, companies no longer have to choose between “broadband VPNs with limitations” and “expensive MPLS.” It’s now possible to achieve better-than-MPLS reliability and performance at DSL-type prices. Gartner, the respected industry analyst, recommends enterprises adopt “hybrid WANs that combine multiple technologies and networks in parallel” in order to achieve improved reliability, among other advantages.⁴

HughesNet® High-Availability VPN

The HughesNet High-Availability VPN solution combines low-cost broadband access with redundant, broadband wireless coverage to yield network availability that is unrivaled in the industry. This is achieved by exploiting three technology trends:

- Advances in broadband access, performance, and service management capabilities
- New, built-in WAN optimization capabilities
- Redundant, dual-independent broadband paths

The HughesNet High-Availability VPN offers companies an integrated managed network solution that meshes broadband wireline connectivity with redundant broadband wireless (satellite or EVDO) coverage. As illustrated in Table 1, the result is an enterprise network “triple-play” that features higher performance, better reliability, and lower cost than T1-based private networks.

Criteria	T1-MPLS VPN	HughesNet High-Availability VPN
Bandwidth	1.5 Mbps	1.5–5 Mbps*
Availability	99.8%	99.9–99.99%
Managed Enterprise-Grade Service Delivery	Yes	Yes
Security	Via private network and network-based security	Via security access router, data encryption, and network-based security
Class of Service	Typically 4–6	4 data classes
Multicast Support	Limited	Fully scalable
WAN Optimization	Overlay service with external appliance and additional cost	Integral, no additional cost
Cost	\$400–\$800 monthly per site	\$200–\$400 monthly per site

*Multiple access links to each location. Includes benefits of WAN optimization

Table 1 - Comparison of T1-MPLS VPN and HughesNet High-Availability VPN

⁴ Cost Cutting by Rightsizing Network Reliability, Gartner, 2008

Customers have the flexibility to choose any combination of wireline, wireless, and satellite access technologies at each site based on their unique business requirements. For example, the network design could include a primary DSL site connection coupled with redundant satellite coverage. Or, primary T1s could be deployed with redundant EVDO wireless. The HughesNet High-Availability VPN solution is technology agnostic. No matter what technology combinations are chosen, customers receive a complete, managed solution that includes end-to-end network status visibility, proactive monitoring features and fault-management capabilities.

The advantages remain the same, regardless of the technology combination:

- More bandwidth and better application performance
- Dramatically enhanced network reliability
- Robust security
- Low cost

As a result, revenue streams and operational performance are protected while bandwidth increases significantly and security is strengthened. In addition, the HughesNet solution can be readily modified as the enterprise expands or network requirements change.

Improved Reliability

The HughesNet High-Availability VPN solution provisions dual independent broadband paths at each site, boosting network availability to near 100% levels. Broadband path failure is detected in real-time, and automatic switch-over reroutes traffic within seconds. The configuration and management of the customer premises routers (customer premise equipment or CPE), including failure detection and switchover, are integral parts of the HughesNet managed service. The routers continually monitor the status of the WAN links, reporting the health of each link and failure detection. In the event of a failure—of either the link or a router, the system automatically triggers re-routing of all traffic to the redundant operational connection. This ensures that the remote location stays on-line and can still deliver mission-critical applications.

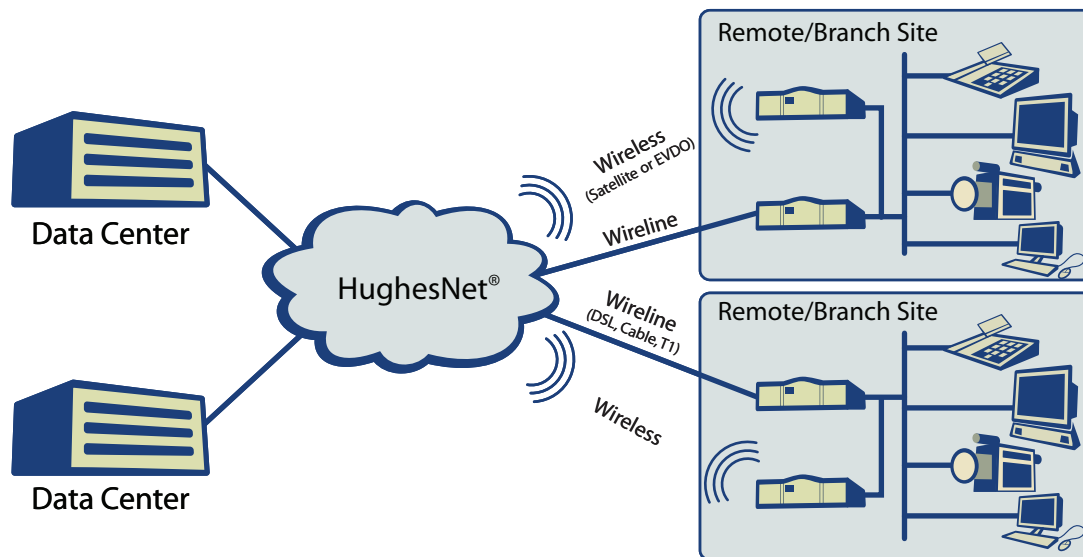


Figure 1. HughesNet High-Availability VPN

Scalable Bandwidth

In addition to high availability, dual broadband access links deliver increased bandwidth that is scalable. As illustrated in Figure 2, the two broadband links can be utilized to accomplish application level load balancing, which improves performance without increasing costs. This approach eliminates costly wireline upgrades since the second co-primary wireless link can handle the additional bandwidth required. As a result, bandwidth is available as application demands increase.

With application-based prioritization and routing, both broadband access links can be leveraged to deliver up to 3 Mbps downstream to each location—twice as fast as T1 access. Furthermore, HughesNet WAN Optimization⁵ applies sophisticated data reduction techniques to improve usable WAN throughput—up to 5 Mbps downstream to each location. Additional compression and protocol overhead reduction techniques trim data streams by 50-90%, depending on user traffic.

HughesNet Dual-Access Advantages

- Savings up to 30% over traditional T1-MPLS solutions
- Application-level channel bonding delivers 3 Mbps performance
- WAN optimization increases performance to 5 Mbps
- Compression and protocol overhead reduction reduce data streams by 50-90% (traffic dependent)

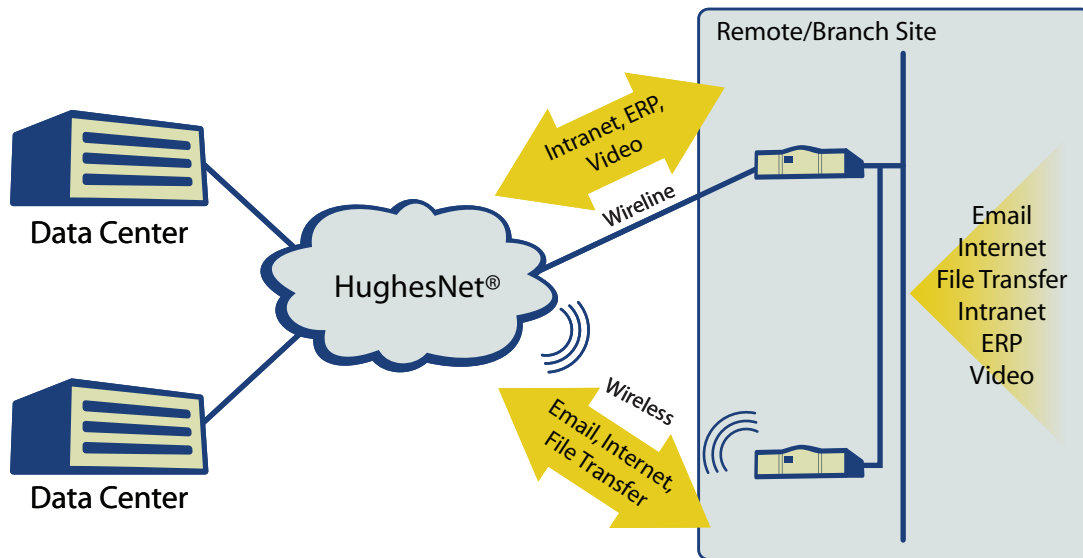


Figure 2. HughesNet Bandwidth Scalability

Network Security

HughesNet services include a robust end-to-end security architecture that exceeds customer privacy and security requirements. At the networking layer, IPSec with AES encryption is utilized to secure all data from the remote site. Hughes has also developed its own customer premise routers to dramatically improve service delivery and security. The Hughes HN7700S-R router supports both wireline and wireless WAN access. Unlike typical routers, the HN7700S-R is not an Internet access router. It's a secure tunneling router that uses the Internet as a transport. Between the router and a specialized IP gateway within the Hughes network operations center (NOC), Hughes establishes, maintains, and monitors an AES IPSec tunnel. The router's access control list (ACL) enforces the rule that all traffic is sent only over the AES IPSec tunnel to/from the Hughes NOC.

⁵ Hughes WAN Optimization: A New Approach, Hughes, December 2008.

Management of the remote router is also very secure. All management traffic is transmitted within the AES IPsec tunnel, inclusive of ICMP pings which are used to determine up/down status of the remote site. This ensures that an out-of-band attacker cannot compromise the network via the router's WAN connection. Only packets which are successfully decrypted and authenticated may be used by the management software. In addition, a Hughes-proprietary SDL (simple data link) protocol is used to communicate configuration information.

Optional network-based managed security services, such as managed firewall and filtering capabilities are also available to further enhance the network security of each branch location.

The overall architecture and implementation approach of the HughesNet service has been certified as PCI compliant. By following PCI standards, Hughes maintains strong protection for customer traffic and network security. Customers can also be assured knowing that Hughes follows ISO quality business practices and procedures for implementation, monitoring, and change management. For further HughesNet security information, see *Hughes Broadband VPN End-to-End Security Enabled by HN7700S-R*, Hughes, February 2009.

Application Performance

The HughesNet solution uses application-aware WAN optimization technology to ensure consistent, high-performance application delivery. In addition, application level traffic shaping matches business priorities to network bandwidth allocation at peak hours. When bandwidth hungry applications (real-time, non-real time, and recreational) run over 100 Mbps+ LANs and meet the relatively low speed WAN access, prioritization and traffic shaping are crucial. These technologies maintain the performance of key business applications without forcing companies to expand access bandwidth.

Like MPLS, the HughesNet solution offers Class of Service (CoS) settings to prioritize certain applications over others, depending the needs of the business. The HughesNet solution also maps to MPLS code points to ensure interoperability with existing MPLS networks. As a result, CoS parameters can be set across the network to distinguish high-priority traffic (such as point-of-sale, email, and business critical application data) from lower priority traffic (CRM, payroll, or possibly recreational traffic that should not be on the network, such as YouTube videos, Facebook activity, and music downloading).

Generally, WAN optimization refers to network utilization optimization and application acceleration. The goal is to deliver 'LAN-like' performance over the WAN. For the past 15 years Hughes has been a pioneer in the development of WAN optimization technology leading to many patents. The HughesNet High-Availability VPN solution uses a *symmetrical architecture*⁶ approach for effective bandwidth control and acceleration, with a Hughes HN7700S-R enterprise-class router deployed at each remote location. The solution delivers WAN optimization functionality such as:

- **Application Prioritization and Traffic Shaping:** With the growth in remote applications as well as recreational traffic, demand for WAN bandwidth will often exceed available bandwidth at branch sites. Instead of traditional traffic engineering approaches that attempt to manage traffic levels, a more efficient method is to use prioritization to ensure business critical applications are provided preferential access to WAN bandwidth. The HughesNet solution provides four levels of CoS priority. Traffic flows are classified via a variety of rules, such as application type, TCP ports, or IP addresses.
- **Application Acceleration:** Protocol acceleration is an effective method for delivering excellent application performance by minimizing or eliminating the effects of latency and jitter on commonly used protocols. TCP, for instance, is susceptible to significant performance degradation due to well known issues, such as slow-start and window scaling. While these have no user-perceivable impact on LANs, their effect becomes more pronounced in WANs. The HughesNet solution incorporates both TCP and HTTP/HTTPS (web and secure web) acceleration functionality. Application acceleration occurs transparently to the end user application systems.
- **Data Reduction:** Data reduction refers to the decrease or elimination of redundant data over the WAN. The technique delivers significant benefits in terms of WAN bandwidth efficiency. Hughes has incorporated two forms of data

⁶ A symmetrical architecture is one where the WAN optimization appliance or software is present at the end user premises. An asymmetrical architecture is a network or data center-based approach without any additional appliance at the remote site. The former approach is more powerful, while traditionally more expensive, whereas the cloud-based approach reduces overall costs but is more limited in its functionality.

reduction to maximize these gains compression and protocol overhead removal. Both are transparent to the end systems. Stateful, content-aware compression provides lossless compression gains of up to 10 times, depending on the actual traffic content.

Protocol overhead removal significantly reduces TCP and application level overhead through the use of local TCP termination. The Hughes router at each remote location terminates TCP sessions locally and uses a high-efficiency WAN protocol to transfer the data to the destination where the reverse process occurs. An advanced form of protocol overhead reduction is also incorporated at the HTTP level to significantly reduce bandwidth required for web requests. These data reduction techniques are built into the HughesNet solution at no additional cost. In contrast, these data reduction techniques are an additional cost (as hardware and service upgrades) when implemented with competitive solutions. They are not commonly available with off-the-shelf solutions. For example, a managed VPN service purchased from a traditional telco provider does not automatically include WAN optimization, compression, and acceleration features. Costly additional third-party equipment is usually necessary. This equipment is usually managed by the telco provider or the customer IT team.

For further information, see *Hughes WAN Optimization: A New Approach*, Hughes, December 2008.

Additional HughesNet Benefits

Broadband Anywhere

Hughes uniquely provides cost-effective broadband VPN service throughout North America using broadband satellite technology, and is available anywhere with a view of the southern sky. In those areas where DSL and cable are not available, wireline providers often deploy expensive T1 circuits, which can drive up costs significantly. The high-throughput HughesNet satellite service already supports thousands of businesses in North America, with international services available in Europe, India, and Brazil. This is the same proven satellite technology that industry leading retailers, grocery stores and major gas station brands rely on every day to run their businesses.

In addition, satellite broadband guards against service failures due to disruptions on the ground from stray back-hoes, earthquakes, hurricanes or other natural disasters, provided emergency power is available at the sites. Satellite bypasses the entire wireline footprint. Whatever is happening on the ground does not affect the ability to deliver broadband service via satellite. Satellite technology combined with landline broadband results in a completely diverse, dual-path solution.

IP Multicast for Scalable Content Delivery

IP multicast provides an ideal mechanism for scalable content delivery to a group or all remote branch locations at one time. Unlike competing solutions that offer limited or no multicast capability, the HughesNet service delivers software or virus updates, and rich media content for employee training or digital signage purposes at the push of a button. Multicast saves on valuable WAN resources since the content packages are delivered simultaneously rather than in successive transmissions to each location, which is typical of unicast wireline solutions. Hughes offers a comprehensive solution that includes the technology and service components necessary to deliver a fully managed multicast solution.

The following services are available:

- **Content Distribution:** The HughesNet service leverages satellite IP technology for a highly scalable content distribution system. Any content, streaming or data files can be transmitted over the network to thousands of recipients simultaneously. As a result, customers can distribute content cost effectively and efficiently.
- **Managed Digital Signage:** The HughesNet service efficiently delivers IP and MPEG video for customer branding and promotions as part of a networked digital signage solution. This type of solution is used in retail networks to impact the buyer at the point of purchase to improve sales. Hughes can provide a turnkey service including network design, equipment installation, and maintenance, as well as end-to-end 'content-to-screen' network management.

- **Business IPTV:** HughesNet Business IPTV is a centrally managed service for the distribution of training modules and other video communications to one or multiple locations through live video broadcasts or on-demand playback. The service reduces travel costs and helps companies more effectively manage employee training and compliance.

In many cases, these IP multicast services can be added to the HughesNet High-Availability VPN solution with little or no additional hardware or software costs.

Summary: Choose all Three – Performance, Reliability & Low Cost

Until recently, IT executives had to make a number of enterprise network upgrade trades-offs to get the performance and reliability they needed, at a cost they could afford. Today, however, new broadband VPN solutions are offering a compelling alternative—high-bandwidth and excellent network reliability at a very reasonable cost.

Hughes leverages its own technology and service delivery to offer 'MPLS-like' performance as part of a managed network service at prices more comparable to broadband VPN. By choosing Hughes, customers don't have to sacrifice performance and availability for cost or vice-versa.

The HughesNet High-Availability VPN solution is already successfully providing services to a number of leading distributed enterprises. In all, over 150 enterprises with more than 225,000 sites rely on Hughes to meet their mission-critical private network requirements. To learn more about HughesNet High-Availability VPN and how it applies to your specific connectivity circumstances, please call 1-866-251-2795 or visit www.enterprise.hughesnet.com.

Proprietary Statement

All rights reserved. This publication and its contents are proprietary to Hughes Network Systems, LLC. No part of this publication may be reproduced in any form or by any means without the written permission of Hughes Network Systems, LLC, 11717 Exploration Lane, Germantown, Maryland 20876.