White Paper

HUGHES

HughesNet® High Availability VPN

HughesNet High Availability VPNs provide a nationwide solution expressly designed to deliver cost-effective, highly available IP networking for distributed enterprises using physically diverse access technologies.

HughesNet®

SEP 2009

www.hughes.com

HUGHES

HughesNet® High Availability VPN

Overview

HughesNet High Availability VPNs provide a nationwide solution expressly designed to deliver cost-effective, highly available IP networking for distributed enterprises.

HughesNet High Availability VPNs achieve superior reliability by integrating two broadband access paths—wireline (DSL, cable, T1) and wireless (3G or satellite) at each remote location. The combination of these route-diverse access technologies ensures that connectivity is available in the event of a failure of either path. In addition, the solution allows both paths to be active simultaneously in delivering the combined throughputs of each access.

Managed router service is a fundamental functionality of the HughesNet High Availability VPN service, with Hughes providing operational management of all aspects of the end-to-end service. This service, combined with scalable bandwidth, high availability, and favorable economics, makes the HughesNet High Availability VPN a very compelling option for the distributed enterprise.

Benefits

Achieving consistent high availability at a reasonable cost has traditionally been difficult to accomplish. Although a carrier's backbone network can be made highly resilient by use of redundancy and subsecond switchovers can often achieve 99.999 percent availability, the Achilles' heel of most distributed enterprise networks remains the access loop or the "last mile." Achieving truly diverse access with an all-terrestrial enterprise network requires careful planning involving conduit separation, dual entrances, connectivity to two central offices, and comprehensive analysis to ensure that no common path exists upstream—often on a site-by-site basis. Any common element between the two paths defeats high availability by becoming a common point of failure. By leveraging widely available broadband access, the HughesNet High Availability VPN solution provides a nationwide service that can deliver this objective in a cost-effective fashion.

HughesNet High Availability VPN offers a number of valuable benefits:

- **Highly Resilient:** Use of physically diverse access technologies (wired and wireless) results in a highly available network. At the remote location, failures are detected automatically, and switchover occurs within minutes of the failure detection.
- **Scalable Bandwidth:** Co-prime access architecture provides the combined throughput of both access paths to the site—up to multi-Mbps based on service plans selected.
- **Performance:** Policy-based routing provides intelligent load sharing capabilities, whereby specific applications are mapped to the access lines. In addition, Hughes' integral WAN optimization provides superior application performance and improved network throughput on both links.
- **Cost-Effective:** Use of widely available broadband access technologies produces a very economical design, which is a fraction of the cost of a leased line network.
- **Nationwide Coverage:** Not only is the service available anywhere in the U.S., but there is almost no per-site design and analysis required. This enables ready deployment throughout the distributed enterprise.
- **Security:** An array of connectivity and configuration options enables customers to deploy a private network requiring no encryption to utilize the Internet with a VPN. The Hughes solution can be deployed in a PCI-compliant architecture.

Architecture Overview

Figure 1 provides a high-level view of the underlying architecture for HughesNet High Availability VPN. It shows a network where some sites are deployed with high availability configurations along with other lower value sites with single access.

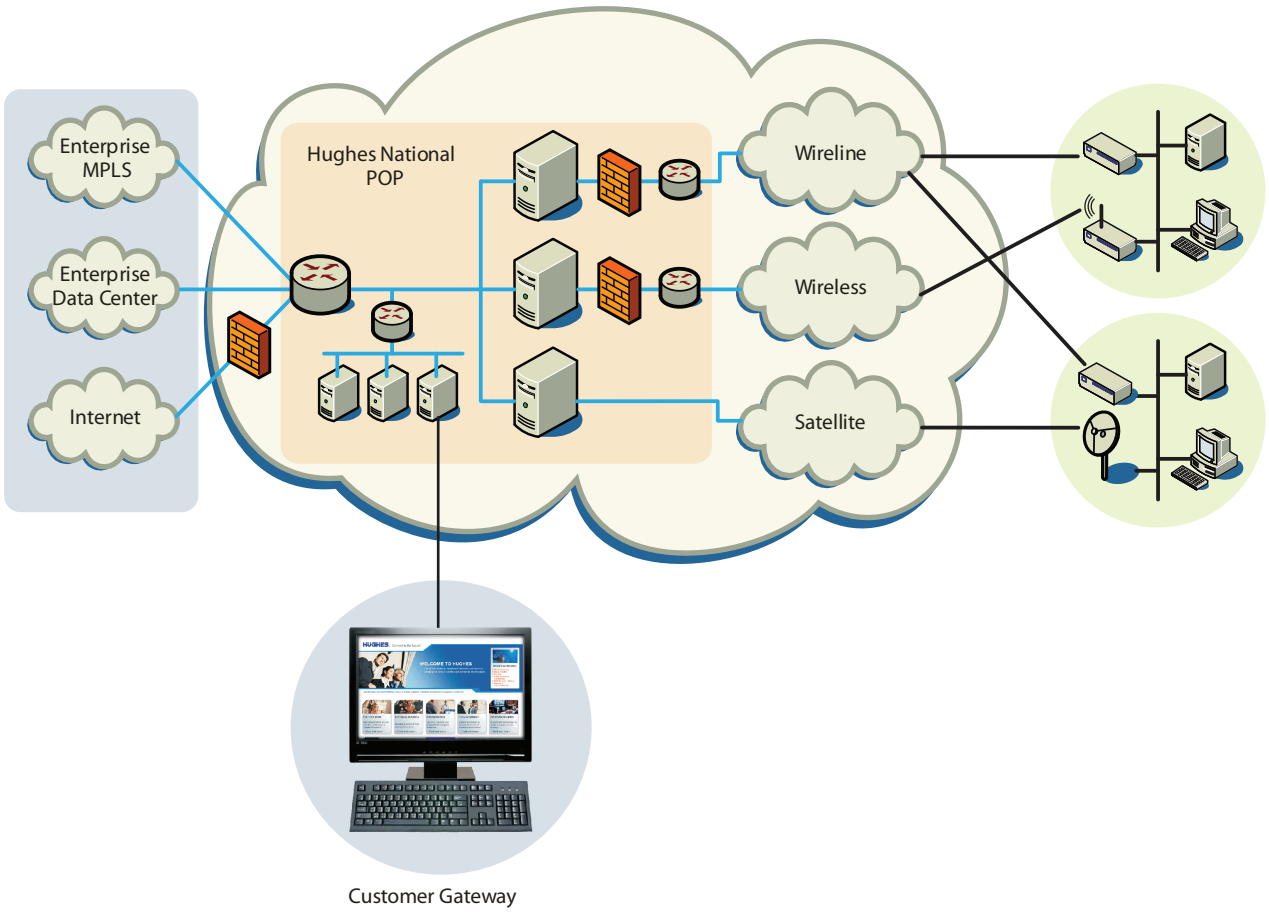


Figure 1. Overview of HughesNet High Availability VPN Architecture

Site Configuration

Figure 2 shows a typical site configuration. The devices on the site are configured to use a single virtual router IP address for the upstream gateway. One of the Hughes managed routers is the primary and performs Policy Based Routing (PBR) to determine the upstream path. In the event of a failure of this router or its associated access path, the second router asserts control and becomes the primary router. End-user devices continue to use the same IP address, and the switchovers are generally transparent to these devices.

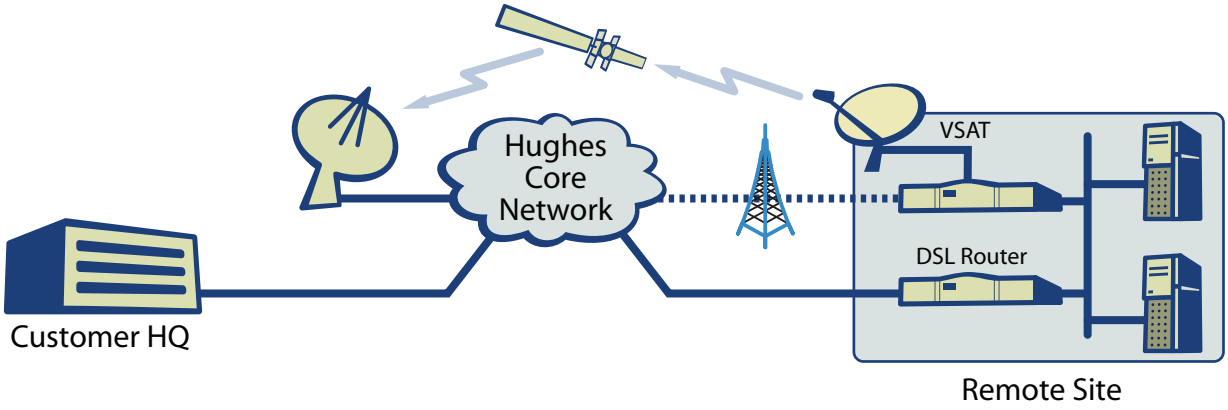


Figure 2. High Availability Site Configuration

Resilience Options

Access Network and Router Resilience

The access network is the primary source of network problems in a distributed enterprise network. A HughesNet High Availability VPN mitigates failures in the access network by using truly route-diverse connectivity from each remote site. Automated switching of traffic between the wired and wireless paths ensures that connectivity is available at all times. In the event of a failure in either path, traffic is rerouted over the other path. The influx of additional traffic on the backup path is controlled by configuring appropriate prioritization within the local routers to ensure that mission-critical traffic will have the highest priority. The time between the failure of an access path to the switchover of all traffic to the other path is dependent upon the overall network configuration but typically takes place within 3 minutes.

Note that in addition to the access network resilience, this solution also provides redundancy in case of a router failure.

Complete End-to-End Resilience

For customers requiring an even higher level of network resilience, HughesNet High Availability VPN provides an option to maintain separation of all network elements from the remote location all the way to the customer's data center. This is achieved by architecting two geographically separate paths across the Hughes network back to the customer's data center.

WAN Optimization

WAN optimization refers to a suite of capabilities that optimizes network utilization and accelerates a broad range of applications accessed by distributed enterprise users using a variety of methods, such as:

- Traffic management methods that give priority to mission-critical applications and related traffic during "rush hour" congestion
- TCP and other protocol-specific acceleration algorithms to minimize the effects of network latency
- File and object caching with "pre-fetch" mechanisms to speed up response times
- Data reduction techniques, including compression and protocol redundancy removal, to improve network throughput

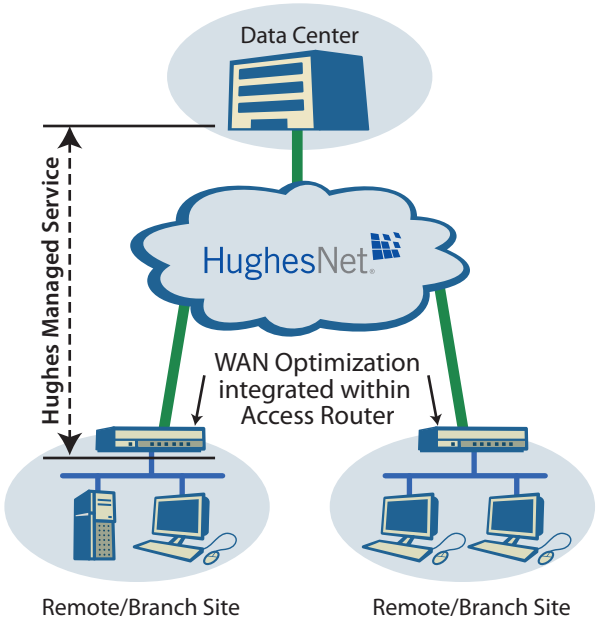
The benefits of WAN optimization generally have been limited to large locations. However, increased broadband access options are now available at the most remote and smallest of branches in a typical multisite distributed enterprise. With a cost-effective WAN optimization solution, all sites in the network can realize improved application performance and network throughput.

Hughes' Approach to WAN Optimization

The HughesNet WAN Optimization offering is graphically depicted in Figure 3. The solution uses a symmetrical architectural approach for effective bandwidth control and acceleration, with a Hughes HN7700S-R enterprise-class router deployed at each remote location. The HN7700S-R integrates a multiaccess router with WAN optimization technology. The combination of lower CPE investment, as well as managed service delivery, makes it highly suitable for deployment over broadband VPNs.

For further details, refer to the WAN Optimization-Enabled HughesNet Managed VPN white paper.

Figure 3. Overview of HughesNet WAN Optimization Service



Performance Improvement

HughesNet WAN optimization brings significant application acceleration benefits. Table 1 shows the performance benefits of FTP and HTTP over DSL and EVDO access utilizing the powerful HN7700S-R enterprise class router.

Table 1. HN7700S-R Performance Advantage

Application	Technology	HughesNet Performance Benefit (Approximate)
FTP	DSL (upload/download)	90% / 30%
	EVDO (upload/download)	140% / 20%
HTTP	DSL	60%
	EVDO	110%

The FTP test consisted of numerous transmissions with varying file sizes and file types, each with different compressibility. The HTTP test measured response time performance of hundreds of Web sites and represents the average of those tests.

HughesNet Managed Services Description

HughesNet High Availability VPN is offered as a fully managed service. As such, Hughes serves as the single point of contact for the full scope of end-to-end services surrounding the offering. HughesNet Managed Network Services includes a full suite of services in two broad categories: service management and network management.

In the service management component, HughesNet Managed Services includes network design, implementation planning, site installation and provisioning, network rollout, customer support/help desk, on-site maintenance, and centralized billing. An experienced program manager is assigned to each customer to ensure efficient and responsive service delivery and management. Network management includes network operations, configuration management, proactive fault monitoring and management, performance management, and reporting.

Service and network management functions are integrated through the use of sophisticated, proprietary Hughes technology to provide superior delivery to the customer. For example, proactive fault monitoring is integrated with the Customer Help Desk and on-site maintenance to provide rapid fault resolution. The Hughes Customer Gateway, accessible to both Hughes internal support staff and customer personnel, serves as a single portal to all HughesNet Managed Services.

The HughesNet Managed Services call center provides customers with several help desk options, with Tier 3 included in the standard managed services package. The use of advanced network tools enables Hughes Help Desk operators to resolve many issues remotely. In the event that on-site service is required, Hughes uses its nationwide field maintenance organization to provide local coverage, including the option of a 4-hour response time to most geographic locations.

Service Level Agreements

HughesNet High Availability VPN provides committed service levels, backed by a Service Level Agreement (SLA). The following parameters are covered by the SLA:

- Network Availability
- Data Delivery Ratio
- Throughput
- Time to Install
- Time to Restore
- Round-Trip Latency

In terms of network availability, HughesNet High Availability VPNs can be designed for up to 99.99% availability.

Summary

Since it first began serving the mission-critical networking needs of the enterprise market over 20 years ago, Hughes' customer base has grown to include over 150 leading US enterprises encompassing more than 225,000 remote locations that rely on Hughes to meet their mission-critical private network requirements. Hughes ranks as a top three IP VPN provider in the U.S., alongside companies like AT&T and Verizon.*

With HughesNet High Availability VPNs, Hughes has leveraged its core competencies of unparalleled experience in managing large mission-critical networks, developing industry leading technology in satellite data networks, networking tools, and business processes to offer customers an unmatched solution for achieving cost-effective, ultra high-availability connectivity for widely distributed networks. The combination of transport technologies and fully managed service delivery allows clients unsurpassed availability, coverage, convenience, and favorable economics.

Hughes' unique blend of experience, advanced technology, and enhanced support services ensures customers superior support for even the most complex and demanding mission-critical applications. Further, the flexibility and scalability of HughesNet Managed Network Services assure customers that they will enjoy a level of reliability, performance, and economics that will support the long-term needs of their businesses.

**Vertical Systems Group 2009, 2008 U.S. IP VPN Service Site Share.*

Appendix: Access Technologies Supported

xDSL

xDSL represents the different types of DSL routinely deployed as part of the HughesNet High Availability VPN service. These include shared line ADSL, dedicated line ADSL, SDSL, and IDSL. The nature of DSL technology is such that the supportable bandwidth decreases as the distance increases between the customer site and the Central Office (CO).

ADSL is supported in two versions—shared and dedicated. In shared line ADSL, the data portion of the traffic shares the DSL line with the voice traffic. The data and voice utilize different frequencies on the line so both traffic types can coexist. With dedicated line ADSL, there is no voice on the line, and only the data portion is available. This is also known as "bare" DSL, "naked" DSL, or "dry loop" DSL.

SDSL is a symmetrical DSL line that provides the same upload speed as download speed. SDSL only comes in a dedicated line; hence, there is no sharing of the data traffic with voice. SDSL has less coverage than ADSL.

IDSL is an ISDN-based DSL service providing symmetrical 144 kbps bandwidth. This service only operates on a dedicated line and has the broadest coverage of any DSL technology.

DSL services can be deployed in either a private Layer 2 environment or as a VPN in a Layer 3 environment. Table A-1 shows the different speeds for the various DSL offerings.

Technology	Upstream Burst Rate (kbps)	Downstream Burst Rate (Mbps)
ADSL	Typical: 128, 384	Typical: .768, 1.5, 3.0
SDSL	Typical: 128, 256, 384, 768, 1.536	Typical: .128, .256, .384, .768, 1.536
IDSL	144	.144

Table A-1. xDSL

Satellite

By its nature, satellite service is available anywhere there is a clear view of the southern sky. An indoor satellite router at the remote premises receives and transmits via standard RJ6 cabling to a compact exterior radio and antenna package.

Satellite bandwidth to each individual site is configured using HughesNet standard Enterprise Service Plans, which provide a variety of data throughputs, from 1 to 5 Mbps on the downstream up to 1 Mbps on the upstream.

Hughes' satellite routers also incorporate sophisticated acceleration technologies that deliver high performance on TCP and Web traffic. In addition to acceleration, performance is further enhanced through the integrated application of lossless compression. The acceleration and compression occur transparently to the end application.

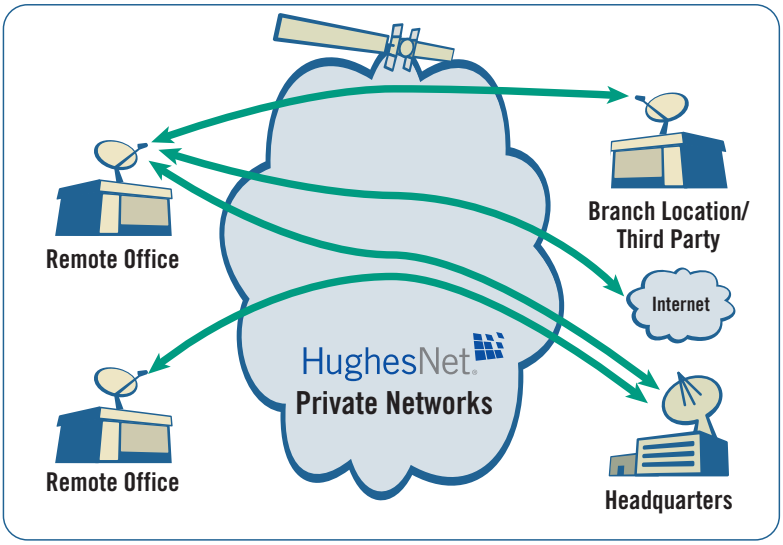


Figure A-1. Satellite Data Network Architecture

HughesNet satellite access also supports multiple Classes of Service (CoS), allocating different priorities and treatment of each for the applications they carry. Figure A-2 shows various CoS supported from the same site.

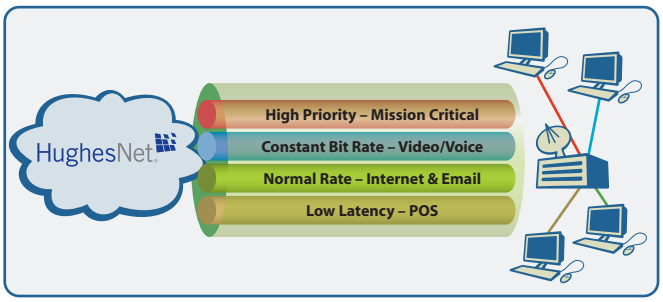


Figure A-2. SPACEWAY® 3 Ka-band CoS levels

Cable

Cable sites are deployed in a Layer 3 architecture where the traffic traverses the Internet and a VPN is implemented to ensure security. Typical bandwidths provided start at 128 kbps or 256 kbps on the upload and 1.5 Mbps on the download.

T1/Fractional T1

Leased line connectivity can be deployed in a Layer 2 or Layer 3 environment. Typically, the Layer 2 implementation involves Frame Relay, whereas a Layer 3 network connects to the Internet, and a VPN is implemented to ensure security. Typical bandwidths provided are T1 and fractional T1.

Wireless

Hughes supports 3G terrestrial wireless access based on EVDO. Most of the sites likely would be provisioned with EVDO Rev. A as it supports the fastest speeds, although individual sites may sync up to higher speeds or fall back to lower speeds, namely EVDO Rev 0 or 1x RTT, depending on signal strength and related factors. Wireless implementations are supported in a Layer 3 model with a managed VPN to ensure security.

Table A-2 shows the different speeds supported by the different wireless technologies.

Technology	Upload	Download
1xRTT	60–80 kbps	60–80 kbps
EVDO, Rev. 0	60–70 kbps	400–700 kbps
EVDO, Rev. A	300–400 kbps	450–800 kbps

Table A-2. Wireless Technology Average Bandwidth

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.

HUGHES, HughesNet, IPOS, SPACEWAY 3, TurboPage, AiReach, Broadband Unbound, and Connect to the future are trademarks of Hughes Network Systems, LLC. All other trademarks are the property of their respective owners.