

Transforming the Agency Network

Managed SD-WAN Delivers Long Sought-After Results: More Bandwidth, Higher Availability, and Cloud Readiness—at Lower Costs

MPLS networks are being challenged by demands of modern IT—a steep rise in video usage, adoption of Cloud applications, and nonstop application availability, to name a few. These stem from the “digitalization” of the modern enterprise and the seismic shift toward the adoption of Cloud-based and rich-media applications. Often, these new applications are not introduced through IT or network teams, causing unpredictable bandwidth strains and degrading application and agency performance. That is especially problematic for the legacy dedicated networks that are still common throughout the public sector.

Today’s widely distributed agency is seeking a cost-effective way to transform the architecture of their Wide Area Network (WAN) so that it is capable of delivering higher performance, better resiliency, nonstop application availability, and iron-clad security. The Software-Defined Wide Area Network (SD-WAN) and use of broadband access have emerged as critical and cost-effective solutions to meet these needs, especially in times of budgetary uncertainty.

Yet the implementation of SD-WAN is not without challenges. The solution leverages broadband access at each site, which can be a daunting management task for large organizations, particularly those with highly distributed branch locations. These branches can often be limited in terms of connectivity options (e.g., transport type and available speeds). This variability at the branch sites causes further network complexity, requiring optimization measures to conform to available bandwidth without stressing the network and reducing performance during peak use times.

The key to unleashing an SD-WAN solution across a widely distributed agency is to procure it from a proven and trusted managed network services provider that also offers advanced broadband optimization tools and technologies. Such a solution provides significant benefits over traditional MPLS networks, including Cloud readiness, high performance, improved network and application availability, flexibility, security and, most importantly, cost savings.

The Challenges

Budget cuts are a serious and ongoing concern for the vast majority of government agencies. And yet the drive for modernization across government IT is increasing with the rising adoption of new devices, Cloud-based applications, and video content that are required for more efficient operations.

In a recent 3-year period, there was a 150% increase in bandwidth demand per site based on analysis of Hughes enterprise customers. Rising demand for bandwidth, without a rising supply leads to network congestion and degraded performance. Such congestion, especially during daily peak times, can also degrade individual branch productivity by as much as 25%. Since many of today’s applications are becoming increasingly mission-critical, agency enterprises are growing dependent on their being “always-on” and available without disruption across the network—from the branch sites, to headquarters, to the data center locations.

Here are some of the networking challenges faced by organizations as they modernize their IT:

- **Legacy network technology:** Traditional WAN architectures were not designed with the Internet in mind. Cloud data traffic involves regular access to the Internet, which can cause application performance to suffer from latency issues as it is passed through data centers and multiple expensive T1 links.
- **Expensive and limited transport options:** The primary technology supporting access to MPLS at most sites is a T1 circuit and 1.5 Mbps is not sufficient for most Cloud applications. Adding more transport capacity by upgrading to Ethernet access or procuring additional T1 lines to increase bandwidth is a costly proposition, especially when employing distributed networks with numerous branch sites.
- **Inefficient redundancy structures:** Since backup WAN links usually become active only when an outage occurs, there is often unused, yet paid-for, bandwidth available every month going to waste.
- **Network complexity:** Large and complex legacy networks require manually configured rules for classifying and prioritizing application traffic. In addition, cumbersome change management processes for complex networks require a deep roster of skilled (and expensive) IT and network engineering staff to effectively manage the network.

The Managed SD-WAN Solution

SD-WAN is the next-generation network solution for organizations seeking greater agility and improved operational efficiencies. And yet, for government agencies—which are often highly distributed enterprises—there are some unique deployment challenges. Chief among them is the fact that branch sites can have vastly different broadband access types and service providers, which can further complicate network performance and management.

Deploying broadband to networked sites is without question a beneficial move thanks to its cost-effectiveness. However, not

all broadband is created equal for all locations. There will likely still be sites that get higher or lower access speeds than other sites. To solve this, new optimization tools have come to market, thanks to the steady rise in broadband adoption and the realization that traditional Quality of Service (QoS) techniques used over legacy network technologies will not produce the same results when applied to broadband. The ability to optimize broadband is now paramount to having a consistent user experience across all network locations.

With a managed SD-WAN solution, the Managed Service Provider (MSP) can provide the agency with one partner to manage all of the access technologies and service providers, streamlining network operations. However, the MSP should do more than just manage service providers and apply appropriate path control rules. This is because there will likely be locations that can still only get one type of access technology. To account for these sites, the MSP can apply software-driven technologies and tools to optimize broadband performance. These tools can enable a virtual expansion of bandwidth without having to actually procure additional bandwidth—contributing to improved application performance and cost savings. The latest SD-WAN optimization technologies can also be integrated into an existing network and configured to work with any access transport technology.

SD-WAN solutions apply optimization algorithms not just to prioritize traffic routing but also application workloads so they can be processed faster and more efficiently to optimize bandwidth efficiency and usage. On top of that, data compression techniques help relieve network congestion and improve application performance. Multiple optimization techniques work together to deliver a dramatic improvement to the branch user's experience.

Managed SD-WAN solutions also make it easier for agencies to scale their network operations to support changing requirements or growth, without the financial burdens of investing in new, expensive T1 lines. By leveraging access to a wide variety of broadband transport technologies, agencies can get all their sites connected, regardless of their geographic location.

MSPs with proven experience supporting large government agencies are best equipped to achieve and maintain compliance with all applicable federal policies and standards, especially those related to security. They are equally adept at assessing agency-specific requirements and tailoring solutions accordingly. Deploying broadband across agency networks also means accounting for a different risk environment than with MPLS T1 lines. However, qualified MSPs can deliver robust managed security solutions within the SD-WAN environment. Depending on agency requirements, there are managed security solutions that can deliver everything from foundational levels of network security all the way to enhanced 24/7 monitoring with threat mitigation and analysis via an MSP Security Operations Center (SOC).

In addition to SD-WAN management and standards compliance, MSPs handle the delivery and support of all related customer premise equipment items, such as network routers, firewalls, Intrusion Detection Systems and Prevention Systems (IDS/IPS), Data Service Units (DSU), Channel Service Units (CSU), out-of-band modems, Indoor Units or Outdoor Units (IDU/ODU), and any other service-enabling devices required to connect to the network. In most instances, MSPs should match or tailor their

change control processes to complement the agency network operations, so that there is a predictable approach to network installations, moves, additions, and changes. In essence, the managed

SD-WAN is not a one-size-fits-all solution but one that is thoroughly designed to meet specific agency requirements.

The Hughes Solution

Hughes is the third largest MSP in the US when it comes to the number of IP VPN end points managed, and, as such, it is able to leverage its experience and culture of innovation to transform outdated legacy networks into powerful, secure, enterprise-grade networks. Hughes enables agencies to meet the digitized needs of today's users and helps highly distributed organizations overcome common SD-WAN deployment challenges to realize their full potential. In this scenario, Hughes, as the MSP, takes full responsibility for end-to-end operation and around-the-clock monitoring of the network via one of its Security Operations Centers (SOC). As the MSP, Hughes works directly with customers and in full transparency to keep them informed as well as provide 24/7 access to a dedicated customer network dashboard.

Hughes managed SD-WAN incorporates its novel suite of advanced broadband optimization tools called ActiveTechnologies™. The suite consists of four primary optimization tools:

ActivePath™

Hughes ActivePath ensures that the performance of each branch's WAN as a whole is always maximized by continuously comparing each link's real-time characteristics with application performance thresholds and directing traffic in the optimal direction. This allows application performance to inherit the characteristics of the best-performing path. As an additional enhancement, mission-critical traffic, such as VoIP, can be duplicated on two WANs without resetting TCP connections and minimizing the impact to the end user during path transitions.

ActiveQoS™

Hughes ActiveQoS leverages premises-based intelligence, compensating for the unpredictable bandwidth changes in broadband networks. ActiveQoS automatically adjusts upstream and downstream bandwidth settings for each WAN connection based on the real-time measured end-to-end capacity of the entire path between the branch and the data center. This measurement is achieved efficiently without generating synthetic traffic in the presence of user traffic and is updated within seconds of changing network conditions.

ActiveClassifier™

Hughes ActiveClassifier is an IP flow-based packet classifier that works both in the upstream and downstream directions independently and eliminates the administrative overhead of defining rules in the network. It intelligently classifies traffic according to its QoS needs, ensuring that real-time and interactive applications receive the appropriate prioritization automatically, while new applications being added to the network are effortlessly blended in.

ActiveCompression™

Hughes ActiveCompression technology dramatically increases the virtual or effective bandwidth available at branch locations by improving throughput and application performance without incurring the expense of increasing the access link speed. This technology employs an innovative two-stage compression algorithm for optimum compression gain. The result is improved performance for the end user and more available bandwidth for applications.

In an independent evaluation by The Tolly Group, Hughes ActiveTechnologies demonstrated highly effective prioritization of transactional traffic (a 5X improvement) and multiple Web-based applications (a 7X improvement) on a congested broadband transport. These improvements resulted in significantly faster application processing times and an improved end user experience.

In short, the Hughes managed SD-WAN solution:

- Enables optimized Internet access with strong perimeter security to enable secure access to the Cloud
- Is transport technology-agnostic (DSL, cable, fiber, 4G LTE, satellite, etc.) to ensure benefits are realized all the way to the network edge
- Leverages ActiveTechnologies to automatically adjust as the broadband network varies to ensure optimal performance
- Delivers high availability of modern bandwidth-hungry applications
- Improves the branch user's experience with reliable application performance
- Enables easy integration into existing network topologies
- Provides critical intelligent path control with brownout protection and ample redundancy
- Delivers a scalable and cost-effective replacement for legacy WAN architectures
- Provides support to all sites as a single MSP, eliminating multivendor management

Conclusion

As government enterprises at all levels grapple with how best to manage tight budgetary resources while simultaneously meeting increasingly complex network demands, they are noticing that branch locations are taxed by sluggish transmissions between sites and have an inability to support new bandwidth-intensive applications. On top of application performance and availability, there are a rapidly growing number of devices connecting to the network, making network security vital.

While the emergence of SD-WAN is promising, large and widely distributed agencies would be best served by exploring this technology within the context of managed services that are capable of delivering its full potential. With a managed SD-WAN, agencies will discover a viable and cost-effective solution that provides significant benefits over traditional private networks. These benefits include Cloud readiness, high performance, improved network and application availability, flexibility, and, most importantly, security and cost savings.

Technical Specifications to Consider for Managed SD-WAN Solutions

Below are common technical tasks and services to be considered for a high-quality managed SD-WAN solution.

- WAN optimization technologies
 - Application classification and prioritization
 - QoS and flow control
 - Dynamic path selection
 - Application-agnostic TCP acceleration for higher latency links
 - Data compression for emails, office files, and unencrypted workloads
 - Caching for repetitive downloading of common files and assets
- Network engineering design services, implementation, management, and maintenance
- Provisioning, managing, and maintaining all end-point premises equipment and service-enabling equipment
- 24/7 network and security operations support and monitoring
- Management and monitoring of firewalls, including content filtering, Intrusion Detection and Prevention Systems (IDS/PS), and antimalware protection
- Integration with the agency's service desk, if applicable
- Engineering support and coordination for the provisioning of services
- Timely and accurate response to agency requests for status, information, performance, and service-level compliance reports
- Troubleshooting tools and analytics reporting for all broadband access technologies (including DSL, cable, fiber, Ethernet, 3G-4G, LTE wireless, microwave, and satellite)
- Field maintenance and troubleshooting of service issues
- Scalable bandwidth (high-capacity access) in increments up to 155 Mbps to agency field offices
 - Multiple broadband links may be used to accommodate required bandwidth
 - Provide full network capacity insights
 - Real-time monitoring of links with dynamic balancing for better performance
- Tier I (Basic), Tier II, or Tier III Help Desk Support

VPN Support

- IPSec, AES encryption
- Networking/routing configuration
- Multiple WAN link support, DHCP, policy-based routing, RIP, OSPF, BGP, and multicast
- IPv4 support for operations and security components. (e.g., firewall, DNS, transport mode, SIP, dynamic routing)

Transforming the Agency Network

- VLAN tagging (802.1Q), including separate VLAN interfaces, QoS, CoS
- Group-based authentication and scheduling
- Network security and access control
- Flow-based antivirus/antispymware protection
- Web filtering, including HTTP/HTTPS and MIME content header filtering. Be able to block Java Applet, cookies, and Active X
- Application control (e.g., MSN, Facebook, Skype, Yahoo) regardless of port or protocol
- Antispam support for SMTP/SMTSPS, POP3/POP3S, IMAP/IMAPS
- MIME header check
- Keyword/phrase filtering
- IP address black/white list
- Wi-Fi access for guests and guest LAN services

Network Monitoring and Customer Care

- Customer Care Portal or Enterprise Web Access Portal integrated across all access types and sites that provides a comprehensive and often real-time view into:
 - Trouble tickets
 - Installation activities
 - Status of network elements and other fault management data
 - Performance Management reports (such as Network Usage, Inventory, Rogue Device, Uptime, New User, User Session, and Device Summary)
 - Historical reports for traffic analysis and trends, peak usage time, capacity planning, etc.
 - Configuration error alerts (default password enablement, wireless association information, detailed user tracking, and session history)

VPN Converged Services

- Converged multiservice ports to provide local private and public networking to maximize SaaS/Cloud performance without the need for separate circuits
- End-to-end SLAs with key performance metrics and remedies
- Network-based VPN concentrators to support secure remote access, secure Web/email gateway, and secure Internet breakout
- Converged multiservice ports to allow for flexible bandwidth and future-proofing site connectivity
- Access to major Cloud providers to support Cloud applications for real-time QoS
- Single ASN to allow control over network functions on a global basis
- Layer 3 routing protocols that remain private and secure

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.

Visit government.hughes.com/sdwan to learn more.



www.hughes.com

11717 Exploration Lane
Germantown, MD 20876 USA

TRANSFORMING THE AGENCY NETWORK
Hughes Network Systems, LLC. HUGHES is a registered trademark of Hughes Network Systems, LLC.
All information is subject to change. All rights reserved. H58901 JUL 17