Lippis Report

White Paper

WAN Advantage: New Thinking in Branch Office and WAN Edge Design plus Services

Secure and Increase Collaboration and

Application Performance to Reduce Corporate Cost

by

Nicholas John Lippis III
President, Lippis Consulting

March 2009

Table of Contents

Abstract

Along with a turbulent macro economic cycle comes business rationalization and in networking the wide area offers a unique opportunity to deliver value both in terms of operational efficiency and business initiative alignment. Advances in network-embedded, software- based WAN Services such as security, unified communications (UC) and WAN optimization are starting to deliver the same type of application experience and management tools to control application performance that was once only available over the LAN. But the wide area network has been pieced together, usually site by site, without a comprehensive plan. This lack of planning is most acute in branch-office-to-WAN and data center connections as geographically distributed branches are connected with inconsistent WAN Services and indigenous WAN transport. IT planners are being offered an opportunity to implement a common set of WAN Services embedded within routers such as UC, WAN optimization, security etc., between branch, headquarter and data center sites which promise to lower operational spend, align business initiatives and policy while delivering Local Area Network (LAN)-like application performance. This paper presents a strategy for common WAN Services embedded in routers connecting branch offices to data centers and larger corporate sites that speed up workflow and business process for all employees independent of geographic location.

1. Macro Corporate Trends Driving New WAN Design

There are multiple business and technology trends that are now interacting and forcing IT planners to rethink their wide area network (WAN) design. The macroeconomic downturn has proven once and for all that business and its processes are global. With economic globalization and the current turbulence people are required to collaborate more closely, more frequently and across greater distances than at any other point in time. At the same time IT leaders have been consolidating IT service delivery into data centers as well as consolidating their number of data centers. Data center consolidation offers large economic efficiency but places greater distance between data, applications and end-users, putting great strain on application performance. Corporate green initiatives have driven up the number of home and mobile workers to the point that 15% of traffic flows to and from mobile workers and data centers. Adding more pressure, WANs have historically been designed in a piecemeal fashion with little to no regard for delivering consistent WAN Services among sites. Add heightened security plus compliance requirements to new applications such as web 2.0, video conferencing, mobility, etc., and the result is unprecedented demands on the WAN to keep a corporation productive. At a time when WAN performance needs to be optimized and tuned as carefully as Local Area Networks (LANs) performance, it unfortunately is more difficult than ever to accomplish. These trends, if not addressed, will invariably have a negative impact on application performance and corporate productivity, especially among WAN-connected branch offices, larger corporate sites and data centers, since 41% of network traffic now flows to and from branch offices.

Increased traffic load, application load, collaboration, distance, separation of data and applications and security/compliance requirements are all dynamics that are completely altering the design requirements for the WAN. To address these dynamics, IT leaders need to deploy consistent WAN Services so that tuning/controlling/optimizing of WAN Services and applications across all sites connected via the WAN are performed uniformly, saving both time and money while increasing corporate value. Having consistency in application optimization, collaboration, and security WAN Services, among corporate sites large and small, combine to form a WAN Advantage that enables business and IT leaders to boost collaboration throughout their business, strengthen security, speed access to data and ideas, optimize application performance end-to-end, and ultimately cut operating costs. In this paper we focus on the WAN Edge that connects branches to larger sites and data centers; however the concepts and subsequent principles can be applied to other corporate WAN areas.
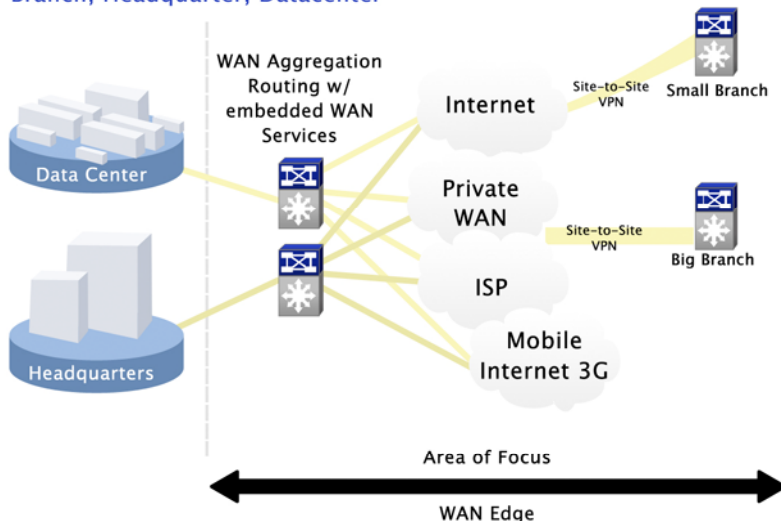
A. WANs Slow To Keep Pace

The telecommunication service providers have done a good job introducing new WAN Services such as 3G wireless, broadband services, metro ethernet, extending access arrangements for MPLS and Frame Relay, et al. But wide area bandwidth has not kept pace with the rapid advance of LAN bandwidth and application demand where wide area connections are often at least one to two orders of magnitude (10 to 100 times) slower than the LANs they connect. This bandwidth mismatch is the root cause of slow application response time and poor voice and video user experience resulting in diminished productivity. In addition to WAN bandwidth being slow to keep pace, so too has WAN Service delivery. To defend against security breaches, optimize application performance plus gain the benefits of unified communications and collaboration IT leaders have been forced to deploy a series of appliances in each branch office thanks to a lack of common WAN Service delivery options. Deficits in WAN bandwidth and service delivery increase complexity, which drives up life-cycle management cost and makes IT service delivery difficult.
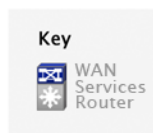
Nowhere is the deficit in WAN bandwidth and services more acute than in connecting branch offices to larger corporate sites and data centers, as the complexity it creates is magnified. This magnification is due to the fact that branches are widely distributed over large geographic areas resulting in a lack of WAN bandwidth consistency, meaning that some branch offices may connect at broadband speeds while others use frame relay; still others use MPLS or private lines, etc., while WAN Service appliances pile up in each branch. While IT leaders have limited control over WAN bandwidth provisioned by telecom service providers they do have total control over WAN Service delivery, which in turn exploits and manages WAN bandwidth. In short, WAN Service management is the key to complexity reduction and the basis for new thinking in WAN design.
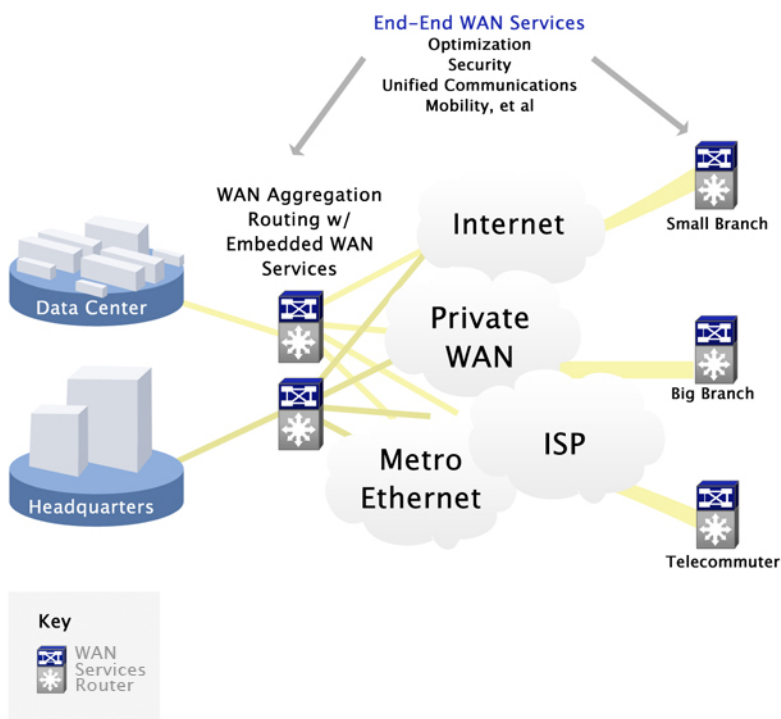
Cisco's WAN Advantage

[Listen to the Podcast](#)

2. New WAN Requirements

Before we dive into WAN Services let's quickly review the new WAN Edge requirements. All of the above-mentioned business and technology changes and drives can be summed up in the following four WAN requirements:

1) **Reduce Complexity:**   The first requirement is to reduce complexity by exploiting common WAN Services between branch office and WAN aggregation routers located either in data centers or larger feeder sites.   This requirement is central to gain economies of scale and greater Return on Investment (ROI) by aligning branch requirements with consistency in WAN Services policy.

2) **Defend and Mitigate Security Threats:** Network security is top of mind and concern to business and IT leaders, especially during the economic downturn where exploits have spiked.   To defend against external and internal threats the WAN is required to implement a series of security services such as VPN, access control and traffic monitoring.   The WAN has three roles to play here: 1) virtualized security services to reduce the number of appliances easing its management; 2) reducing security capital and operational spend while maintaining a high level of defense; and 3) delivering compliance reporting to avoid penalties associated with legislative and regulatory exposure.

3) **Improved User Experience of Collaborative Applications:**   Branch WAN connections have historically been designed to support corporate applications. But with both the increased need for communications and collaboration driven by their economic benefits and business imperatives, branch WAN connections are required to support voice and video services that are reliable, stable and operate at a level which promotes their use and productivity advantages. That is the elimination of choppy and/or dropped video conferencing and voice sessions.

WAN Services Logical Overlay

4) **LAN-Like Application Response Time:** While LAN and WAN bandwidth alignment will not occur any time soon, WAN Services especially in the area of WAN optimization can significantly improve application response time and resiliency to the point where applications operating over the WAN can respond as if they were hosted on a local disk drive. Fundamental here is the ability for users to be productive using corporate applications that increasingly access data from fewer and distant data centers.

Addressing these four requirements will increase the IT experience of branch office employees allowing them to be productive while reducing IT operational cost and complexity.

3. Essential WAN Services

To deliver on the requirements a set of common WAN Services needs to be available in both branch office and WAN aggregation routers, which are typically located within data centers and larger corporate sites.   This consistency in the WAN Services phase is akin to LAN evolution, maturity and value.

Thanks to WAN Services, WAN performance can approach that of LANs. In fact WAN Services are evolving in a similar manner to that of LANs. During the 1990s there were competing LAN standards such as Token Ring, Ethernet, FDDI, ATM, et al., each supporting a specific number of protocols such as IP, DECnet, LAT, IPX, AppleTalk, IP, OSI, VINES, etc. After the bridge vs routing and token ring vs ethernet and

OSI vs IP debates, a consistency of one physical LAN standard, that being ethernet, and one data protocol, that being IP, emerged. Multi-protocol routing/bridging over ethernet in particular supported all data protocols as multiple logical networks that flowed over one physical infrastructure which over time migrated to IP, taming a largely complex LAN environment. Multi-protocol routing/bridging was the enabling technology that rationalized LAN standards and data protocols.

There may not be a single WAN physical service such as ethernet any time soon but just as multi-protocol routing simplified LANs so too will WAN Services as it manages and masks the inconsistencies in different wide area facilities and injects value. In short WAN Services provide a set of logical components that rationalize a messy WAN world and replace it with user experience consistency and uniformed IT management and security. To bring the discussion down to product level, it's Cisco's ISR and ASR 1000, 3Com's 5000 and 6000, Juniper's J and M Series, Nortel's Secure Routers, HP ProCurve's 7000dl Series and others which offer the promise of consistent WAN Services. Of the above list only a few offer routers, which deliver consistent WAN Services at the branch office and the Enterprise WAN edge/aggregation respectively, thanks to a shared common software code enabling these routers to collaborate via protocol exchanges across the wide area. Part of this common WAN Services software code is based upon standards such as IPSec, SSL, MPLS, SIP (Session Initiation Protocol), Real Time Protocol (RTP), etc., while other aspects are company specific such as Cisco's GET-VPN which simplifies the provisioning and management of VPN.

While there are a growing number of WAN Services we'll focus on the three most important or essential ones, those being security, unified communications and WAN optimization that support the above WAN requirements. Again to gain the value of these WAN Services there must be consistency in their offering between branch and WAN aggregation routers, which reduce complexity, thus addressing the first WAN requirement. We address the remaining WAN Services in the same order as the WAN requirements presented.

Network/IT Security: To readily adapt to new business requirements, reduce qualification time for new deployments, proactively monitor and provide pervasive integrated security services, meet and comply with federal or industry regulations requiring confidential communications, ASR 1000, for example, can be deployed as a Secure WAN Aggregation router with integrated firewall, IPsec encryption and a wide range of VPN termination options. In addition access control such as Network Access Control (NAC), IDS/IPS Intrusion Detection Services /Intrusion Protection Services and Network Foundation Protection (NFP) deliver defenses to mitigate both internal and external security threats. Traffic monitoring through quality of service (QoS), Netflow and event logging ensure application performance and provide security forensics data. The key to security as a WAN Service is that it's implemented end-to-end within branch office and WAN aggregation routers enabling a uniformed deployment, management environment and secure user experience network wide.

Unified Communications Video and Telepresence: The WAN requires increased collaboration frequency over larger distances to support unified communication (UC) plus video and telepresense services. There are specific WAN Services that ensure the user UC and video experience remains excellent even while other applications compete for WAN resources and/or during network disruption such as backhoe fade, etc. UC as a WAN Service means that most, if not all, UC features are embedded into routers, removing the requirement for additional hardware and providing common network and communications management and user collaborative experience network-wide. In a Cisco environment, UC as a WAN Service includes Cisco's UC Manager Express (**UCME**) which sets up and tears down calls; its Survivable Remote Site Telephony (**SRST**), which provides redundant call control in the remote branch office; Cisco Unity Express (**CUE**) voice messaging and greeting services, Unified Messaging Gateway (**UMG**) for voice messaging, Cisco Unified Border Element (**CUBE**) software which provides connectivity between enterprise UC Session Initiation Protocol (**SIP**) trunks to the public-switched telephone network (**PSTN**) and Cisco Session Border Control (**SBC**) software to control, secure, and manage real-time IP multimedia traffic across enterprise and service provider network borders.

WAN Optimization: WAN optimization is a WAN Service that is embedded as a series of application optimization features/functions within branch and WAN aggregation routers that strive to deliver local drive response time to applications that are delivered over the WAN. WAN optimization services include WAN optimization and traffic classification. In a Cisco environment WAN optimization services include software components such as Wide Area Application Services (WAAS) which accelerate applications over the WAN. Web Cache Communication Protocol v2 (WCCPv2) serves as a general purpose transparent interception mechanism for any IP-based protocol such as web traffic and redirects it to local caching devices and Performance Routing (PfR), which selects the best path for each application based upon advanced criteria such as reachability, delay, loss, jitter, and Mean Opinion Score (MOS).

Classifying and marking applications is both a security and application optimization benefit. The following two protocols span both the security and WAN optimization categories of WAN Services. To intelligently identify and classify applications and guarantee them a minimum amount of bandwidth, policy routed, or marked for preferential treatment, deep packet inspection software such as Network-Based Application Recognition (NBAR) is used. Conversely non-critical applications may be marked for best effort service, policed, or blocked. In addition Flexible Packet Matching (FPM) protects against existing and emerging threats at network entry points using granular Layer 2-7 pattern matching deep within packet header or payload to provide a rapid first line of defense against network threats and notable worms and viruses. FPM also ensures application optimization so that worms and viruses do not propagate and fill up WAN links causing business-critical applications to suffer performance loss.

Application monitoring is also important to WAN optimization and security services. QoS and Netflow was addressed earlier, but one other feature is IP Service Level Agreements (SLAs) which ensure that business-critical IP data, voice, and video applications adhere to SLA levels by measuring application performance both on an end-to-end and at the IP layer.

There are more WAN Services such as mobility and others to come over the next business cycle. The value WAN Services delivers is rooted in the fact that WAN Services are logical components embedded into the wide area simplifying IT operations, accelerating the absorption of innovation and delivering end-user performance consistently independent upon their physical location.

4, The New WAN Advantage

A. Old World WAN

Traditionally, connecting branch offices to larger corporate facilities and data centers has been implemented in a piecemeal fashion, meaning that most IT organizations have not architected or designed the WAN Edge as a holistic solution. For these firms branch office WAN connections are a mixture of disparate transport services; their routers have little to no WAN Service consistent with headquarter and data center aggregation routers while the branch offices are populated with special purpose WAN Services appliances. This lack of planning results in much higher IT capital and operational spend. But more troubling is that poor business performance results, thanks to inconsistent application performance and branch IT delivery difficulty especially of new collaboration services and tools.

Compounding this trend has been the increased intelligence that resides within branch routers, placing a greater service load on aggregation routers, which in turn requires the aggregation routers to be more intelligent. To gain efficiency the WAN Service feature cycle between branch and aggregation routers needs to be in synch. In most cases however, IT hasn't considered the branch WAN as an end-to-end application supporting infrastructure. Most consider the branch WAN as a point in a network and provision needs from that perspective, which unfortunately contributes to the above WAN Services misalignment cycle and subsequent business difficulty implications as this thinking drives IT to a point product approach.

This piecemeal approach reviews requirements in isolation which drives questions such as, what do we need in this branch? what do we need at this corporate headquarters? Over a short period of time this leads to bottlenecks, better security in some branches than others, and becomes complex and difficult to manage, change and grow as the system becomes populated with an assortment of disparate devices all with their own management systems, upgrade paths and patch requirements.

B. New World WAN Advantage

The new approach to WAN design is based upon business initiatives and user experience expectations independent of geographic location. This shift from piecemeal to end-to-end design considers secure access to corporate data, applications, people, ideas, etc., from anywhere. This approach requires a comprehensive, cohesive WAN design with end-to-end support for services, because after all, a network delivers applications and application performance governs a user's experience and productivity.

The new WAN should deliver a consistent user experience in the same way as LANs do, by switches and routers offering a common set of LAN services. For the new WAN, considerations of WAN bandwidth plus a common set of WAN Services between branch and aggregation routers delivered end-to-end can result in consistent user experience. This is primarily achieved through a common set of tools that provide network operations with access to tune/tweak/optimization/configure WAN Services throughout branch offices and aggregation sites so that a user's experience is the same, independent of location, LAN and/or WAN. With well over 6 million Cisco ISRs in production and most firms running sophisticated applications and services in the branch, it's only logical that these ISRs be terminated at an aggregation router over the WAN equipped with common WAN Services to achieve a WAN Advantage. The table below illustrates the shift from old WAN to new WAN design attributes.

5. Business and IT Results and Value

What is the value of the WAN Advantage? From a business perspective the WAN Advantage aligns WAN resources with business priorities, initiatives and process. The WAN Advantage can deliver an excellent user experience with real time collaboration services including reliable video conferencing from anywhere to anywhere, excellent application response and access to data so that employees work **differently and better.** For example, travel requirements plummet as does this expense line item and executive wear and tear thanks to video conferencing and telepresence and in the process the business model changes too.   A WAN Advantage implementation that enables secure web conferencing, UC, video conferencing and local hard drive application performance enables data centers to consolidate without application performance degrading, and faster business processes to take place in global operations thanks to collaboration services.

From an IT operations perspective value is gained by delivering consistent security, UC and application performance services across all branch offices through a single management interface, and WAN fabric. WAN Security Services deployed via the WAN Advantage ensures regulatory compliance avoiding federal and/or state government fines plus consistent defenses and mitigation against exploits throughout all branch offices. Consistent WAN Service delivery offers powerful economies of scale, as service rollouts across the enterprise are dramatically simplified and uniform, saving IT operations time and delivering speed of deployment.

For example, Chad Halilton, Director of IS and Technology at FreeMantleMedia North America, one of the largest international creators and producers of entertainment brands in the world, deployed the WAN Advantage. According to Chad, "Out-tasking aspects of voice network management to a managed service provider frees up time for me to focus on other IT projects. I did not need to learn new skills to manage the voice system because Cisco Unified Communications Manager Express runs on a Cisco Integrated Services Router, which we already used for our data network." FreeMantleMedia/ WAN Advantage improved employee collaboration with conferencing, reduced communications costs by 50% (a 10 month ROI), increased network resiliency and application availability to employees, reduced IT complexity, management, and support costs and realized faster adds, moves and changes in addition to added flexibility for global projects.

Because WAN Services are integrated or embedded into routers a series of additional benefits are gained. For example, embedded WAN Services reduce energy consumption by displacing the large number of appliances scattered through numerous branch offices contributing to corporate Green initiatives. In addition capital cost and branch office IT footprint are reduced too.   Servicing is simplified as well via remote network management, eliminating truck rolls and their associated cost.

Old to New WAN Attributes

Old Wide Area Network	New Wide Area Network
Disparate Branch & WAN Edge Services Experience	Homogenous & Consistent Services Experience
Inefficient Use of WAN Transport & Poor Application Performance	WAN & Application Performance Optimized for Voice, Video, Data
Racks of Appliances for WAN Services	WAN Services Embedded within Routing
Not Architected, Piecemeal	Architected/Designed End-to-End
High Capital & Operational Cost	Efficient TCO: Capital, Ops & Transport
Difficult/Expensive to Add UC & Collaboration	Integrated into Embedded WAN Services

Much of the above benefits are realized when IT designers and architects consider the network as part of the application. During application development and delivery, IT architects who consider how applications are to be delivered over the WAN and factor their response time, reliability, security, bandwidth needs and other attributes into WAN design deliver better user experiences.

6. Seven WAN Design Principals

Guiding principles are helpful in evolving a network gradually during major design decision points rather than a total replacement. To meet that end we offer the following seven guiding principles, which over time will result in a fully WAN Advantage implementation complete with the business and IT benefits discussed above.

Principal One: Deploy Consistent WAN Services: Does the branch office and aggregation routers being installed have consistent and compatible WAN Services and share a common software image/code base to deliver WAN Services across the WAN.

Principle Two: Consider WAN Services During Branch Application Design: When developing or reviewing applications for branch office deployments consider WAN attributes such as bandwidth and WAN Services to ensure application performance and resiliency.   In short consider the WAN as a critical component in IT application life cycle.

Principle Three: Consider the WAN as an End-to-End Application Delivery Service: Avoid viewing a branch office as a point on the network, but view the WAN as a comprehensive application delivery platform.   This will move IT away from point product discussions and toward an architected solution, which will hasten development and improve performance. The question to ask when considering this principle is: Has the WAN been designed to support the new application across all branch offices? If the answer is yes then it's been architected; if the answer is no then the group is developing and deploying applications piecemeal.

Principle Four: Deploy Embedded WAN Services First, Special Appliances Second: Before deploying an essential WAN Service such as security, UC, WAN optimization, etc., as an appliance, first consider if the WAN Service is embedded into an existing branch office and aggregation routing platform.

Principle Five: Appliances Last Resort: If a WAN Service is not available as an embedded service within branch and/or aggregation router only then deploy the appliance. When comparing WAN Services as an appliance versus an embedded service, only deploy the appliance in the case where there are specific features or functions that are must haves and not available in the embedded WAN Service.

Principle Six: 3 Year WAN Transport Service Review: While this principle is slightly off topic, it's important because adhering to it will save the corporation significant expense dollars while increasing WAN bandwidth, thus increasing application performance value to a WAN Advantage deployment. WAN transport services should be put out to competitive bid at least every three years.

Principle Seven: Broadband First: For new branch offices, seek broadband connections first before alternative WAN transport services. With US broadband services past the 50% of total household threshold level and over $7B available in the US stimulus bill for further broadband deployment it's a safe bet that broadband services will only improve and become more pervasive over time. Therefore, when considering WAN bandwidth for branch office sites demand broadband first from service providers and other transport services second.

7. Recommendations

Use the above principles during design decisions and include representatives from various IT groups. Using the above principles, ask the team each principle and discuss it to ensure that all agree the principle is being met. Over time consistent WAN Services will be realized, user experience will improve, design decisions will become routine, speeding up application delivery and business alignment. In addition to the above principles the following recommendations are offered which focus specifically on WAN Services at the WAN Edge. Consider the following:

1. Nonstop Forwarding To Boost Redundancy/Availability: Consider redundancy and fail-over capability across switching, routing, tunneling, WAN access, etc. With new services such as UC and video being massively adopted, convergence time or the time to recover from a WAN transport outage needs to occur within tens of milliseconds.

2. Consistent WAN Optimization and Performance Routing: Consider the consistent implementation of WAN optimization and performance routing between branch and aggregation routing.

3. VPN and WAN Scalability: Consider scale when designing a WAN that connects a large number of branch offices into a set of aggregation routers. Scale such as bandwidth and VPN support can be limiting factors. Aggregation router VPN service in particular should scale up toward 20,000 tunnels to support multiple VPNs per branch as well as mobile users.

4. Consider Integrated Management: Consider network management that integrates WAN Services configuration, troubleshooting, fault isolation as well as security management including threat reporting and compliance reporting. Management that provides constant audits to ensure QoS should be considered as well, as a means to monitor application performance.

5. Consistent Application of QoS/Encryption/Security Across Routers and Tunnels: Consider consistency of Services across different branches especially with QoS, security, routing and switching. Ensure that security policy enforcement is the same at headquarters, data centers and branch levels.

6. Confidentiality And Integrity: As aggregation routers support widely geographically distributed branch offices and mobile users, confidentially and integrity are important security attributes to be considered as part of the WAN security service. Confidentiality ensures that authorized individuals, processes, or systems only have access to information. Identification, authentication, and authorization through access controls maintain information confidentiality. Encrypting information also supports confidentiality by limiting information usability in the event it is viewed while encrypted. Integrity means that information should be protected from intentional, unauthorized, or accidental changes.

About Nick Lippis

Nicholas J. Lippis III is a world-renowned authority on advanced IP networks, communications and their benefits to business objectives. He is the publisher of the Lippis Report, a resource for network and IT business decision leaders to which over 40,000 business and IT executive leaders subscribe. Its Lippis Report podcasts have been downloaded over 80,000 times; i-Tunes reports that listeners also download the Wall Street Journal's Money Matters, Business Week's Climbing the Ladder, The Economist and The Harvard Business Review's IdeaCast. Mr. Lippis is currently working with clients to transform their converged networks into a business platform.

He has advised numerous Global 2000 firms on network architecture, design, implementation, vendor selection and budgeting, with clients including Barclays Bank, Microsoft, Kaiser Permanente, Sprint, Worldcom, Cigitel, Cisco Systems, Nortel Networks, Lucent Technologies, 3Com, Avaya, Eastman Kodak Company, Federal Deposit Insurance Corporation (FDIC), Hughes Aerospace, Liberty Mutual, Schering-Plough, Camp Dresser McKee and many others. He works exclusively with CIOs and their direct reports. Mr. Lippis possesses a unique perspective of market forces and trends occurring within the computer networking industry derived from his experience with both supply and demand side clients.