A Lippis Consulting Industry Paper

A Guide to Cloud-Ready Branch Office Networking

Is Your Wide Area Network Cloud Ready?

By Nicholas John Lippis III
President, Lippis Consulting

July, 2012

Introduction: The Branch Office Wide Area Network Is Not Ready For Cloud

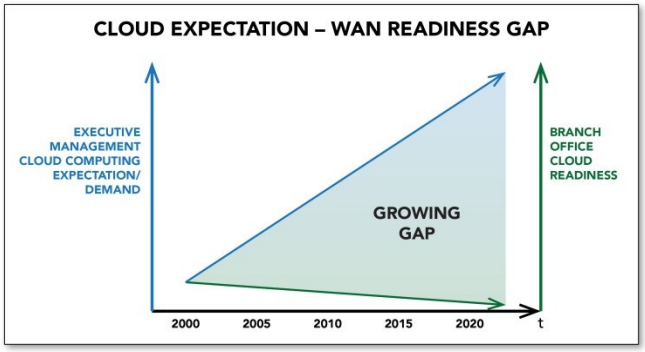
Over the past several years, computing has accelerated its fantastic pace of innovation that has manifested into cloud and mobile computing. There are numerous metrics that have tracked these trends to show their increasingly mainstream acceptance. But the most telling set of data comes from supporting technologies or approaches that are no longer able to support both legacy and the new cloud plus mobile computing models. Wide area networking or in particular, the approach to branch office wide area networking, is in need of an overhaul as its current form does not support cloud computing. This is particularly troubling as nearly 55% of a corporation's employees reside in branch offices and are now, in essence, cut off from secure cloud computing, experience poor cloud application performance and cost their corporation more money than needed.

Over the past 10 to 15 years, branch office wide area networking was primarily built with MPLS (Multiprotocol Label Switching) links connecting branch offices to data centers. Network intelligence or routing was placed on both ends of this transport service. All traffic flowed between branch and data center in a north-south flow. Internet traffic is backhauled from branch to data center only to be re-directed to an internet connection at the data center, consuming MPLS bandwidth that could be used for other applications and driving up its cost. This model does not provide for cloud-computing access; it's not cloud aware, and as such, user experience of cloud services suffer. In addition, in the current branch office model, there are limited cloud security services, and its operational model is outdated and expensive. As if this was bad enough, the reality is that it's only going to get worse as cloud computing forces more structural changes of business process and branch networking.

Cloud computing has evolved at a breakneck pace, changing the way organizations do business. For example, in the financial services industry, small boutique broker firms are placing servers strategically in the cloud very close to an exchange center to drastically reduce NICS Transaction Number (NTN) stock transaction times, where milliseconds saved is millions of dollars made. This levels the playing field between boutique and large-scale transaction brokerage firms and in the process, provides better customer service. The retail industry was hit hard during the 2008-2009 recession, with the largest number of bankruptcies plus liquidations, and still struggles. To reduce branch cost and be more customer responsive, IT business leaders have increasingly placed corporate applications into the cloud. In short, various industries are on different journeys to the cloud, but for the many that have started their journey, they have been rewarded with tremendous benefits of lower cost, increased flexibility and agility.

In fact, in a study commissioned by Cisco of 1,300 global IT professionals across 13 countries, researchers found that there is a four times increase in the number of IT executives who expect to have more than 50% of their applications in the cloud by the end of 2012. Of this same group, 37% consider a cloud-ready WAN to be the most important infrastructure for cloud computing ahead of a virtualized data center or their Service Provider providing appropriate Service Level Agreement or SLA.

Cloud computing deployment decisions are both top down, CEO/CIO, and bottom up, Line of Business or LoB, driven. In many instances, a CIO's cloud objectives are provided to IT management to implement, but the current state of the WAN is not ready for large-scale cloud deployment. There has been a growing gap between executive management cloud expectations and branch office network cloud readiness. This gap is being realized in an increasing number of obstacles or roadblocks, thanks to WAN challenges to cloud deployments. The main WAN challenges are lack of performance, need for better security and management, meaning better monitoring and visibility tools with deployment flexibility to achieve operational savings at scale.



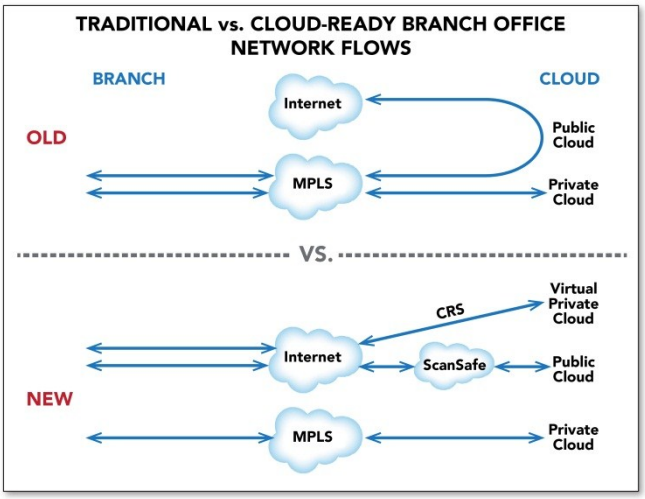
It's surprising that so many IT executives focus on server and storage infrastructure being ready when envisioning cloud deployments and omit their WAN. Re-architecting the branch office WAN can close the Cloud Expectation-WAN Readiness gap. As such, the WAN is about to experience an architectural shift to eliminate the challenges of cloud performance, security and management.

A few examples of how the Cloud Expectation-WAN Readiness gap is an impediment to cloud deployment are presented here. In private cloud scenarios, many firms have implemented Virtual Desktop Infrastructure or VDI pilots, but have not expanded deployments more widely due to WAN challenges. VDI in branch offices over high latency, low bandwidth WANs creates unique challenges as every user-virtual desktop interaction, whether it's a keystroke, mouse

control, video, screen capture, et cetera, has to traverse the WAN every time the user accesses the virtual desktop. Consider that a typical VDI session requires approximately 500 kbps, thus a typical branch WAN link may support only 20 DVI. Also simple human reaction time is between 160 to 190 milliseconds, meaning an excellent VDI experience will result if latency is contained to within this range. Therefore, WAN latency becomes a major performance challenge, impeding VDI pilots from moving to wide-spread deployment, and robbing corporations of its benefits.

A VDI pilot phase may include five to 10 virtual desktops in a few branch offices, which perform to expectation, but as the number of virtual desktops scale up, the Cloud Expectation-WAN Readiness gap hits, resulting in bottlenecks that drive a recalculation of MPLS bandwidth needed per branch connection to guarantee user experience and assure traditional applications, such as Oracle CRM, perform as well or better than thick clients. Most IT business leaders abandon their VDI pilots at this point, as the cost to overcome the WAN performance challenge becomes prohibitive for large-scale deployment, even though they believe VDI offers better security and centralized control of patches, software updates and access.

In public cloud scenarios, backhauling or hairpinning is the main WAN challenge. As mentioned above, hairpinning is the use of an MPLS network that connects branch offices to data centers for Internet traffic. In essence, Internet traffic travels from branch office to data center, only to be forwarded to internet access within the data center, consuming MPLS bandwidth for public cloud services. This approach is very prevalent, as some studies have observed that 90% of branch offices hairpin their Internet traffic due to a lack of cloud security and old habits are hard to die. Obviously, hairpinning consumes MPLS bandwidth, an expensive service, and robs other applications of this bandwidth. Hairpinning is not sustainable as more applications are being moved to the public cloud at speed; it's only a matter of time that hairpinning will be a major cause of poor user/application experience as it consumes a greater percentage of traffic flowing over the MPLS branch-data center network.



Cloud-Ready Branch Office Network Requirements

A cloud-ready branch office network needs to close the Cloud Expectation-WAN Readiness gap by delivering 1) the right experience for the endpoint device, 2) a secure cloud connection at scale and 3) application visibility and monitoring.

Right Experience for the Endpoint Device: A cloud-ready branch needs to deliver the right user performance/experience to various endpoint devices while they're accessing different cloud services, such as public, private, virtual private or hybrid.

Secure Cloud at Scale: A cloud-ready branch needs to provide safe, secure and scalable access to the cloud; that is, security from user devices to cloud.

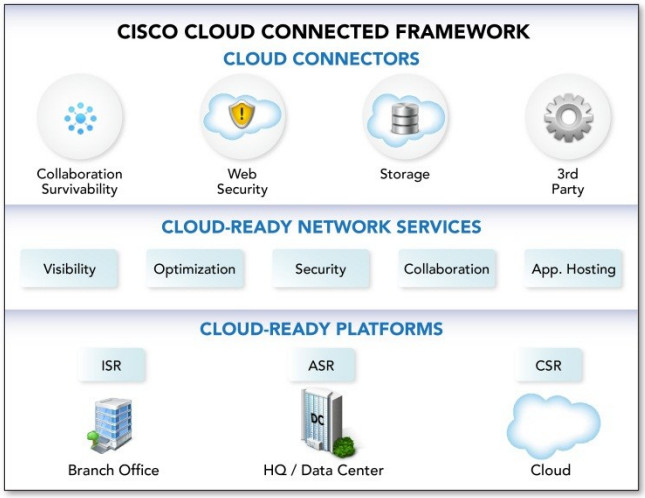
Visibility and Monitoring: A cloud-ready branch needs to provide a set of visibility and monitoring tools that deliver application visibility across data center, branch and cloud(s) so that IT architects can deploy resources efficiently and flexibly to optimize and simplify operations. The desired outcome here is to lower operational expense and headcount growth to manage IT infrastructure.

As Cisco systems is, by far, the largest provider of branch office network equipment, a focus on its latest investments to address the above and provide the industry a cloud- aware and friendly branch office network environment is provided. The following profiles the Cisco Cloud Connected solution for branch office networks.

Cisco Cloud Connected Framework

Cisco has developed a framework with deep product underpinnings that depicts its approach to a cloud-connected branch office. There are four components to the framework, including Cloud-Ready Platforms, Cloud-Ready Network Services, Cloud Connectors and lastly, Integrated Management and Policy. Note that there are no new hardware platforms in the Cloud Connect Framework; all new

components are software based to ease deployment at speed and scale. The underlying infrastructure is cloud ready.



Cloud-Ready Platforms: The Cloud-Ready Platforms are Cisco's Integrated Services Router or ISR G2 for branch offices, Aggregation Services Router or ASR 1000 for headquarters/data center plus internet access, and the new CSR or Cloud Services Router for the cloud. The CSR platform is a virtualized version of the ASR IOS XE image. It will eliminate most traffic hairpinning/backhauling by delivering secure connectivity directly to the cloud from the remote sites.

Cloud-Ready Network Services: Network services are software that run on various platforms. Cisco has invested in a set of existing network services to assure they are cloud-aware in five key areas, including *Visibility* for cloud applications, *Optimization* for cloud-specific applications, *Security* to eliminate hairpinning. As an increasing number of collaborative applications are now hosted in the cloud, the *Collaboration* network service provides increased access efficiency. Finally, the *Application Hosting* network service brings the same operational efficiency and deployment flexibility enjoyed in the data center to the branch office or remote site by offering a more powerful hosting option in the ISR G2. The Application Hosting network service provides IT architects the design option to host applications close to users to increase user experience/performance and reduce MPLS/WAN north-south traffic flows.

Cloud Connectors: The Cloud Connectors are a new set of solutions designed to solve challenges for specific cloud services. Currently, there are four Cloud Connector categories including *Collaboration Survivability, Web Security, Storage* and *third party*. These are but just the first set of Cloud Connectors from Cisco as there are many more in development at Cisco, as well as partners since Cisco has developed a Cloud Connector ecosystem. This is an integral part of Cisco's Software-Defined Networking (SDN) strategy where the rich intelligence of Cisco's networking platforms can be harnessed through open APIs called OnePK. OnePK enables organizations to build their own software solutions to improve services to their customers, employees and partners. For example, third-party partner, Ctera, uses the OnePK API to offer a Storage Connector that provides secure access to cloud-based storage. Cloud Connectors are software modules that currently reside on ISR G2platforms.

In its first Cisco Cloud Connect announcement, there are three connectors, a connector ecosystem, updated network services plus a new platform being launched. In addition, there is a new focus of investment at Cisco on inter-platform communication/collaboration engineered to deliver cloud-based services that improve user experience, increase cloud security and simplify operations. As the network is the only IT component that processes all traffic flows, it's also the appropriate resource to set and enforce policies to control application traffic. Therefore, all platforms will be participating in traffic statistic data collection to gain increased visibility and control of IT resources. All of the above can be summarized as the WAN is being re-invented to support cloud computing with Cisco Cloud Connected for the branch office, closing the Cloud Expectation-WAN Readiness gap.

Putting Cisco Cloud Connected Solution to Work

Gaining optimal user experience is one of the three gaps to close in the Cloud Expectation-WAN Readiness chasm. As an example of the new software tools available to increase user experience in a Cisco Cloud Connected branch office environment, the following network services and connectors are employed on the ISR G2 and ASR 1000 platforms.

1. Application Visibility and Control or **AVC Network Service** on the ISR G2 and ASR 1000 to provide granular application visibility and control
2. **AppNav for WAAS Network Service** for flexible scaling of application optimization
3. Hosted Collaboration Solution or **HCS Connector** for survivability

Increasing user experience is usually a two-step process of 1) figuring out what application are flowing over the network and 2) optimizing their performance.

Application Visibility and Control or AVC Network Service

The underlying AVC technology is Cisco's NBAR2 or Network-Based Application Recognition, Flexible NetFlow or NetFlow V9, and Performance Routing or PfR, all working in unison to provide granular visibility of 1,000-plus applications. Network traffic statistics and application visibility information is aggregated in the ISR and ASR and exported in a standardized format of Flexible NetFlow or NetFlow V9 to

Cisco Prime Assurance Manager, or a third-party tool, for graphing and reporting. AVC provides IT planning with application identification/recognition/awareness, such as YouTube, Citrix XenDesktop, video conferencing, etc., that is traversing between branch to data center. A report is generated, detailing all branch offices with their various applications in use, including top talkers, network utilization, bandwidth requirements, etc. NetOps can then optimize the network, making it more effective for certain high-priority business vertical applications. Since AVC is an embedded instrumentation capability on the ISR and ASR 1000 platforms, IT organizations do not need to deploy probes for collecting granular application performance and management statistics.

AppNav Network Service to Optimize Application Performance

Once application visibility is obtained, the second step is to optimize application performance. This is accomplished with Cisco's WAAS or Wide Area Application Services product, which is available in a range of form factors from appliances, integrated solution on ISR G2 to virtualized versions called vWAAS that run on Cisco's UCS and other virtualization-enabled servers. Cloud services are driving the need for new WAN optimization solutions that can intelligently pool and provision resources, elastically, in a simplified manner, with better manageability for private, public and virtual private cloud deployments. For example, "bring your own device" (B.Y.O.D) requires local mobile connectivity while application flow into the private cloud increases to support email, web connections, virtual desktops, business applications, etc. To deliver and maintain excellent user experience, the ability to rapidly and transparently add private and/or virtual private cloud WAN optimization at the head-end is paramount.

As WAAS is a WAN optimization and load balancing network service that is deployed in branch offices and data centers, the need to be able to pool this resource and control it to strengthen its ability to optimize application performance at scale has become a significant need. Cisco introduced AppNav for this purpose as controlling a single virtual pool of WAN optimization network service can be used effectively in terms of load balancing including traffic redirection, classification and flow distribution. Further, AppNav is a major reduction of operational complexity, thanks to transparent scaling, clustering plus its configuration and monitoring is integrated with WAAS Central Manager 5.0.

Cisco AppNav technology virtualizes WAN optimization resources in the data center by pooling them into one elastic resource in a manner that is policy based and on demand with scale and performance. It integrates with Cisco WAAS physical and virtual network infrastructure, supporting more than a million connections, providing investment protection, as well as expands WAN optimization service to meet future demands. AppNav enables IT operations to optimize application performance at scale that may sprawl across branch, cloud and/or enterprise data center. While this virtual pool can get quite large, AppNav's management tool provides operations with tight, yet flexible, control.

AppNav optimizes applications that are implemented in large-scale cloud deployments, including a private, VPC (Virtual Private Cloud) or public cloud, by pooling WAN optimization appliances, independent upon their form factor. That is, AppNav is backward compatible with older WAAS appliances while being forward compatible with the new Cisco WAVE (Wide Area Virtualization Engine) appliance plus vWAAS implementations. Once a virtual pool of WAAS is established via AppNav, IT designers can split the pool in various ways. For example, a portion of the pool can be allocated on a per application basis so that a set of WAN optimization appliances optimize only a certain type of application, or the pool can be split based upon policies, such as organizational structure, including HR, finance, engineering, manufacturing, etc., or even geographic locations.

AppNav effectively uses existing WAN optimization resources and adds more when required without needing to change or reconfigure portions of the network. That is, NetOps do not have to reconfigure IP addresses or change network state when WAN optimization is added or removed; a huge complexity reduction as AppNav eliminates the time, inconvenience and process previously required to install additional WAN Optimization service.

In addition, AppNav optimizes applications across data centers. Consider an enterprise that utilizes a Freeware appliance in its private cloud and requires to cloud burst a workload, load balance off an application, etc. Certain workloads can be moved to a VPC environment with vWAAS so that all WAN optimization is included in the virtual pool created by AppNav. AppNav also runs on the new CSR in a multi-tenant hosted cloud environment providing multiple VPCs. An enterprise can now scale and use various types of clouds, knowing that they can optimize applications across all cloud scenarios, thanks to AppNav's ability to abstract WAN optimization into a virtual pool(s).

AppNav is available as part of Cisco WAAS Software Release 5.0 and in three form factors providing deployment flexibility. It's available in the Cisco WAVE appliances, CSR platform as a software solution and in the near future, on the ASR 1000 platform Series Routers built into IOS XE. Note that IT architects can implement AppNav in one of the three, or in all three, deployment options.

Optimizing VDI via AppNav

Scaling VDI pilots to larger-scale implementations confronts the Cloud Expectation-WAN Readiness performance gap. As VDI pilots start to scale, NetOps would deploy additional WAN optimization at the head-end, thanks to increased traffic. With the AppNav software module implemented, it automatically identifies the new WAAS appliance. When AppNav is implemented, policy is defined by NetOps to instruct the use of its virtual pool. Therefore, when the new WAAS appliance is deployed, AppNav uses this policy to automatically optimize application traffic—in this case, its virtual desktop traffic from a branch office, for example. AppNav will start load balancing based upon a new larger pool consisting of the previous WAN optimization pool plus the newly implemented WAAS resource—enabling scale with growth. Note that previous to AppNav, NetOps would have to change the layer 3 IP addresses on each WAAS and manually input policies in each WAN optimization device. Further, the above-mentioned new WAAS appliance could have been implemented in a virtual private cloud or simply private cloud, and the AppNav module would operate the same.

Survivability HCS Connector on ISR G2

The HCS connector is the Survivable Remote Site Telephony or SRST solution but it now works with Cisco's Host Collaboration Solution (HCS) that was introduced in December 2011. In the event of a communication disruption, such as a brownout, WAN congestion or WAN link failure, the HCS connector on the ISR G2 assures that branch office voice over IP calls continue uninterrupted. This is accomplished by retaining the calls occurring between branch offices, or if PSTN (public switched telephone network) back up is in place, by transferring those calls over the PSTN. HCS is critical for call centers, financial services, retail stores and any office that provides call support for customers.

The above demonstrates an example of Cisco's Cloud Connected for branch office networking components and how they can be put to work to optimize user experience by gaining application visibility and control, optimizing application performance and assuring non-interrupted real-time communication services.

Cloud Security

Increasing cloud-access security is also one of the three gaps to close in the Cloud Expectation-WAN Readiness chasm. As an example of the new software tools available to increase cloud access security in a Cisco Cloud Connected branch office environment, the following network services and connectors are employed on the ISR G2, ASR 1000 and the new CSR platforms:

1. **ScanSafe Connector** on the ISR G2 to provide cloud-based security.
2. **FlexVPN Network Service** on the ISR G2, ASR 1000 and CSR for unified VPN configuration for cloud access.

To increase security, Cisco has developed the new CSR platform. CSR is a virtualized platform that runs on any virtualized server, such as Cisco's UCS, HP, Dell, IBM, etc.—in essence any machine that runs VMware ESXi Hypervisor or Citrix XenServer. CSR soon will run also on top of Microsoft's Hyper-V. CSR can be used within private, public or virtual private cloud computing environments, but it offers unique advantages when used with VPC offerings.

CSR provides two primary functions: virtual security services and a control point. First, for those IT business leaders who are placing applications in a VPC environment, CSR provides a strategic control point. VPC providers such as Amazon, Terremark, Microsoft's Azure, etc., provide IT leaders with the ability to define a virtual network topology that closely resembles a traditional network that one might operate in their own datacenter. IT departments have complete control over their virtual networking environment, including selection of IP address range, creation of subnets, and configuration of route tables and network gateways. With CSR, IT architects can spin up a virtual machine that runs as a router and securely terminate their VPN connections from branch offices and/or remote users directly.

This offers a fundamental change in how branch office and remote access networking is designed. It eliminates the expense and overhead of back-hauling/hairpinning cloud bound traffic from branch offices to centrally-located internet access points over the corporate MPLS network. In short, it frees up this bandwidth for private cloud applications. CSR enables an easy, efficient and scalable way of providing direct secure access to a VPC environment while reducing MPLS bandwidth consumption.

We expect content service providers and others to utilize the combination of CSR plus VPC in the creation of a variety of services to meet the needs primarily of the Small- to Medium-size Business (SMB) and the large enterprise market too. In this market, CSR creates a low barrier of entry as dedicated networking platforms are not required, enabling an efficient deployment model based upon market need, be it peak traffic, number of customers, etc. One or many network acting VMs can be easily deployed when needed, and accordingly, CSRs can be associated with a set of customers providing a clear demarcation point. With the CSR as a control point for each customer's virtual network within a VPC, it will largely contribute to meeting compliance

requirements for many vertical industries such as healthcare, financial services, etc.

Within a private cloud, generally corporations will have a head-end terminating VPN connection such as the ASR 1000, reducing the need for CSR. However, in a VPC environment, the corporation or VPC customer does not have their own infrastructure in place for their enterprise; therefore, CSR provides the control point for which most, if not all, IT business leaders are looking.

In addition to CSR, Cisco's secure cloud access services include the ScanSafe Connector on ISR G2. The ScanSafe Connector on ISR G2 redirects Internet and cloud-destined traffic via a local broadband internet connection to cloud-based Cisco ScanSafe solution where IT managers have a centralized control point to implement policy, enforcement and mitigate risks across branch offices. ScanSafe eliminates hairpinning as the ISR G2 forwards Internet and cloud-destined traffic over broadband versus MPLS connection.

The third solution for Cisco's secure cloud access services is its FlexVPN on the ISR G2, ASR 1000 and CSR routing platforms. FlexVPN simplifies the configuration and management of a range of underlying VPN technologies, such as DMVPN, IPsec VPN, Remote Access VPN, etc. FlexVPN abstracts these underlying VPN technologies and provides a consistent way of configuration and management at a platform level.

The above demonstrates Cisco's Cloud Connected for branch office networking components to secure cloud access, and in the process, offer IT designers the secure use of VPCs. With the use of CSR plus ScanSafe, hairpinning can be all but removed, assuring that only private cloud traffic flows over the MPLS network. FlexVPN reduces operational cost and tasks by providing a common set of configuration and management tools for all types of VPN tunnels.

Simplifying Operations

There are three product underpinnings for Cisco's Cloud Connected Framework goal of simplifying operations. These include the next generation UCS Express or the UCS E-Series, which is available as a single or doublewide ISR G2 module that runs a quad-core or six-core Intel Xeon CPU, centralized traffic and application monitoring via Cisco Prime Assurance Manager or PAM, and a new form factor for the ASR called the ASR 1002-X to deliver on-demand performance and scale.

First, the UCS E-Series provides higher performance than the UCS Express so as to run multiple Cisco, plus third-party, network services and applications simultaneously. The UCS E-Series is a virtualized application-hosting platform supporting VMware hypervisor and Microsoft Hyper-V. For example, network services, such as vWLC (virtual Wireless LAN Controller), vWAAS, Infoblox, Sage ACT plus a wide range of other Cisco, and third-party solutions, can run simultaneously on UCS E-Series. From a management point of view, the virtualization layer can be managed via VMware's vCenter with UCS hardware managed via Cisco's CIMC or Chassis Integrated Management Controller for UCS controller management. The simplification is derived from a single model of managing all UCS deployments that span between data centers and branch offices while providing infrastructure consolidation for branch offices, thanks to virtualized application hosting on ISR G2 routers.

Second, Cisco Prime Assurance Manager (PAM) provides a front-end tool for the AVC network service mentioned above that presents traffic data and application visibility information for centralized analysis and reporting. To gain application visibility into the wireless LAN network within the branch office, Cisco's 3600 Aironet Access Point was enhanced from a cloud perspective to provide monitoring of cloud and business applications traversing throughout the branch office. PAM provides a single pane-of-glass for monitoring plus centrally identifying, prioritizing and controlling applications.

Third, the ASR 1002-X is a new form factor for the ASR 1000, which provides an on-demand performance upgrade without the need to install a new forwarding processor or acquire new hardware. A nearly seven times increase in ASR performance is gained through a software-license upgrade. Once the software license is upgraded via remote access, a performance increase of between five to 36 GB can be realized. The ASR 1002-X offers a pay-as-you-go model, eliminating a rip-and-replace process every time the need to increase throughput or bandwidth is required at the WAN head-end.

All of the above is tied into providing tools, deployment flexibility plus management and monitoring options to simplify operations and lower its cost.

Pulling It All Together

Cisco Cloud Connected Solution offers an entirely new set of design options for various types of industry sectors. It enables options that simply were not possible previously that leverage the strength and benefits of cloud computing along with proven features and functions Cisco developed for branch office networking. The following are a few examples.

Consider a retail store with an advertising campaign residing in a Terremark server in a VPC. With Cisco Cloud Connected, the retail store could run a redundant advertising campaign application on the UCS E-Series server providing survivability. Therefore, in the event of a brownout where VPC access could be cut-off, the advertising campaign will still proceed uninterrupted, thanks to local application

hosting. Further, with Cisco's HCS Connector on the ISR G2 voice over, IP calls are assured uninterrupted service in the event of network congestion or a brownout.

From a PCI-compliance perspective, many retailers utilize the company "Square" to host their point of sale or PoS applications in a VPC environment. To assure the retailer is PCI compliant, its credit card transactions are securely transmitted by terminating the VPN connections on a CSR router that resides within a VPC. The retailer has direct access and control of its VPC environment to assure PCI compliance and reporting while also reducing its PCI infrastructure cost.

Retail Banking

In the banking industry, an increasing number of teller applications are being hosted on virtual desktops, thanks to excellent user experience. The network is key to delivering this experience, assuming that the bank is running ISR G2 with AVC providing applications visibility while Citrix-Ready WAAS optimizes the virtual desktops. Branch bank VPN connections are terminated securely in their private cloud using the ASR 1000 with FlexVPN, offering simplified configuration and management of all VPNs. NetOps utilizes Cisco PAM, which is fed traffic statistics from AVC to control, prioritize and monitor applications.

In the branch bank, a customer is engaged with a mortgage-refinancing agent who surfs the web to serve up a list of refinancing options. The agent is accessing web pages that are safe and securely accessed, thanks to the ScanSafe connector that, again, resides on the same ISR G2 that fronts the branch office.

Education

A university has deployed FlexVPN on an ASR 1002-X and WAAS with Context-Aware DRE or Data Redundancy Elimination plus AppNav on an ISR G2. Consider the University of Phoenix or any university that delivers class and course work on-line by broadcasting lectures to multiple sites. To assure that the video content is optimized across many branch offices, the university deploys WAAS Context-Aware DRE that transmits only new content minimizing video bandwidth use, while the many WAN optimization network services are pooled and managed with AppNav. Video lectures are transmitted securely over VPNs, thanks to FlexVPN on the ASR 1002-X router.

Recommendations:

The Cisco Cloud Connected for branch office networking re-defines wide area networking in the age of cloud computing. Cisco has provided a set of cloud connectors, cloud-enhanced network services plus the new CSR platform that provides IT architects the tools to close the Cloud Expectation-WAN Readiness Gap. With the exception of the UCS E-Series module on the ISR G2, all other network services and cloud connectors are software additions to the ISR and ASR platforms, enabling rapid deployment and cloud readiness to branch office networking. The cloud connector ecosystem developed as part of Cisco's OnePK SDN environment can be utilized by enterprises, service providers, cloud providers and development partners to utilize network intelligence and build software solutions on top of routing and switching platforms for providing innovative solutions to their customers, employees and partners. It's hopeful that the Cisco Cloud Connected solution and its ecosystem will close the Cloud Expectation-WAN Readiness gap for most, and enable Cisco and partners to quickly implement solutions that keep pace with fast-moving cloud computing.

The following recommendations are offered:

- ✓ Assess the branch office network for cloud readiness. If it's not cloud ready, then consider implementing many of the software modules associated with Cisco Cloud Connected Solution.
- ✓ Start to use AVC by implementing it within the ISR G2 and ASR 1000 with reporting to either Cisco PAM or their third-party Flexible NetFlow compliant reporting packages to gain application visibility.
- ✓ With application visibility gained, utilize AppNav to pool distributed WAN optimization network services to optimize prioritized applications performance.
- ✓ Implement broadband access at branch offices with an eye toward removing Internet traffic from MPLS backbone networks to broadband infrastructure.
- ✓ Start to eliminate hairpinning by experimenting with the ScanSafe Connector.
- ✓ Experiment with VPC solutions and the CSR control point as VPC is a fast- growing cloud computing option.
- ✓ Consider using FlexVPN to manage existing VPNs and to configure new ones.

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 makers to which over 35,000 executive IT business leaders subscribe. Its Lippis Report podcasts have been downloaded over 180,000 times; ITunes 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 design their private and public virtualized data center cloud computing network architectures to reap maximum business value and outcome. He has advised numerous Global 2000 firms on network architecture, design, implementation, vendor selection and budgeting, with clients including Barclays Bank, Eastman Kodak Company, Federal Deposit Insurance Corporation (FDIC), Hughes Aerospace, Liberty Mutual, Schering-Plough, Camp Dresser McKee, the state of Alaska, Microsoft, Kaiser Permanente, Sprint, Worldcom, Cisco Systems, Hewlett Packet, IBM, Avaya 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.

Mr. Lippis received the prestigious Boston University College of Engineering Alumni award for advancing the profession. He has been named one of the top 40 most powerful and influential people in the networking industry by Network World. TechTarget, an industry on-line publication, has named him a network design guru while Network Computing Magazine has called him a star IT guru.

Mr. Lippis founded Strategic Networks Consulting, Inc., a well-respected and influential computer networking industry-consulting concern, which was purchased by Softbank/Ziff-Davis in 1996. He is a frequent keynote speaker at industry events and is widely quoted in the business and industry press. He serves on the Dean of Boston University's College of Engineering Board of Advisors as well as many start-up venture firms' advisory boards. He delivered the commencement speech to Boston University College of Engineering graduates in 2007. Mr. Lippis received his Bachelor of Science in Electrical Engineering and his Master of Science in Systems Engineering from Boston University. His Masters' thesis work included selected technical courses and advisors from Massachusetts Institute of Technology on optical communications and computing.