A Lippis Consulting Industry Paper

A Software-Defined Networking Approach to Branch Office Routing

By Nicholas John Lippis III
President, Lippis Consulting

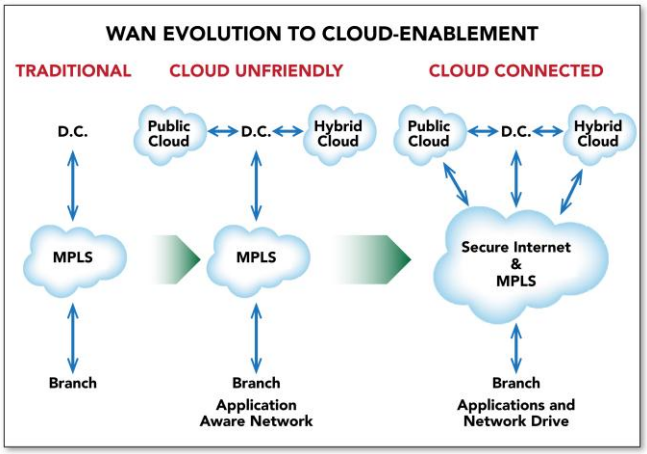
February, 2013

New Computing Model Drives New Network Architecture

Cloud and mobile computing deployment has accelerated at a fantastic pace over the last five years, changing the economics of where computing and storage are located, how applications are written and accessed, and most importantly, how corporate computing automates business processes. The pace of change in cloud and mobile computing has been much faster than the evolution of wide area networking, which is now on the critical path to reaping the rewards of modern computing and its favorable business outcomes. Wide area networking or in particular, the approach to branch office WAN design, is in need of an overhaul as its current form does not support cloud computing.

Over the past 10 plus years, branch office WAN design was primarily built with MPLS (Multiprotocol Label Switching) links connecting branch offices routers to data centers. All traffic passed 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. But network design is shifting from making more WAN bandwidth "available to applications" toward "applications becoming aware of network resources available." This shift in thinking and network design approach affords applications to exploit or best utilize network resources to increase performance and thus user experience.

Without applications being network aware, the current branch office network model will stay cloud unfriendly. What this means is that current branch office networks do not provide effective cloud-computing access; it's not cloud aware, and as such, user experience of applications hosted in cloud services suffer. In addition, branch office networks are limited in cloud security services, and its operational model is outdated and expensive. As if this was not bad enough, the reality is that it's only going to get worse as cloud computing forces more structural changes of business processes and branch office networking.

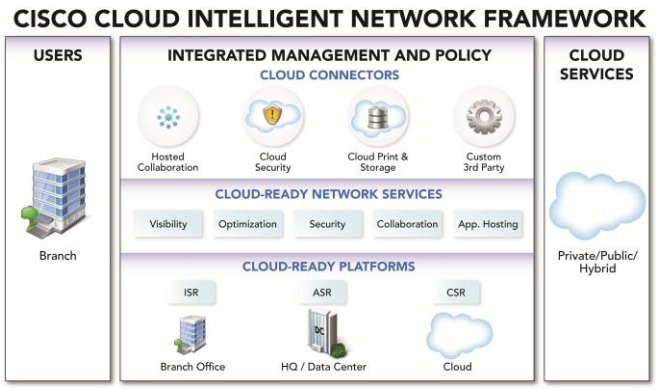


Wide area networking needs to evolve, both in transport and intelligence, to support IT business leaders' cloud and mobile computing initiatives. In short, there is a new era in wide area networking emerging where applications are aware and gain knowledge of the WAN to drive intelligent decisions that increase application performance and utilization. Consider a storage backup application that has network utilization knowledge, which it uses to transport backup data over the WAN during low traffic utilization periods. Wide area networking needs to provide applications network intelligence to serve the new transitions IT business leaders are demanding. Wide area networking needs to be more flexible so that IT leaders can easily move, change or expand availability of their application portfolio mix as business requires. The corporate WAN can deliver optimal performance to assure businesses stay productive without excessive capital, operational and WAN bandwidth costs by enabling applications with network information to best utilize its services.

The new WAN is not only providing a transport service, but exposing state information to applications so that better decisions in application delivery are made. Note that networks have been application aware for some time; that is, networks have been able to detect application signatures within network traffic and perform some action, such as define quality of service, monitor services, control and/or apply security policy, etc. But in the cloud-connected branch office network model, applications are aware of the network which opens up an entirely new set of cloud-enabled services through software-defined networking or SDN. Applications equipped with network intelligence are able to exploit and utilize both corporate WAN and Internet access bandwidth securely, increase application performance and reduce WAN cost too. As security has been one of the main concerns in slowing cloud deployments, a cloud-enabled WAN should deliver consistent security and operations regardless of where an application is accessed from, either public or private clouds.

Cisco Cloud Intelligent Network

During the summer of 2012, Cisco launched its Cloud Intelligent Network Framework, which offers a platform for delivering innovation into branch office wide area networking for optimal experience, pervasive security and simplified operations. Cisco's Cloud Intelligent Network Framework is rooted in deep product underpinnings and 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. In this white paper, we focus on Cloud Connectors as they are the mechanism to enable cloud services in the branch offices in which applications become network aware.



Cloud Connectors

As the industry is in the early stages of cloud and mobile computing, it's not known what unforeseen changes and opportunities may occur. Cisco's Cloud Intelligent Network Framework provides its Cloud Connectors technology and partner program that delivers an ecosystem of partners that are rapidly adding innovation and value to cloud-enabled branch office wide area networking. It's the Cloud Connectors that allow networking to catch up with the pace of change in cloud and mobile computing to support a modern application portfolio mix.

As example of a Cloud Connector delivering value, consider a corporate user requesting a YouTube video to be displayed on her/his virtualized desktop interface or VDI. In a VDI environment, bandwidth use is relatively low as mouse clicks and keyboard strokes are sent to the data center while display changes are sent back to the user. But video has a different traffic profile with large bandwidth and low latency required. Distributing this traffic type via a VDI session is highly likely to negatively impact all VDI sessions suddenly. This scenario could also arise due to high network congestion. Traditionally, network engineers have control knobs to assign quality of service (QoS) to different traffic types so that one endpoint doesn't degrade application performance of others. Further, VDI introduces specific challenges, such as traffic encryption, that does not allow standard QoS to work efficiently. So how can you assure fairness in a VDI environment? The Cloud Connector approach is to enable interaction between the network and application. For example, the application could inform the end user of a potential negative impact of his/her action to others if he/she watches a YouTube video on a VDI screen, or the application may suggest that the user postpone usage to a later time when he/she will receive a better experience without impacting business critical traffic.

Another example of how applications, users and networks can interact is a billboard exchange. Consider shopping in a mall with a smartphone. The Wireless Local Area Network (WLAN) can leverage location services and notification features to deliver a different user experience. You may enter a retail store looking for a special gift and decide to search for it on your smartphone. Your smartphone, leveraging your location and search information, may display locations close by that have inventory of the gift, pricing and potentially, relevant promotions specific to your location opportunities. This is an example of a stronger tie between application and network location services that's dynamic and occurs in real time.

Cloud Connectors are a result of the Cisco ONE initiative to create an open networking environment that exposes network features, state and functions to applications. Cisco ONE is Cisco's Software-Defined Networking (SDN) strategy and initiative. Within Cisco ONE, an important Application Programming Interface or API has been made available called onePK (ONE Platform Kit), which provides programmers access to select network features and functions. In short, onePK abstracts the network so that applications and/or programmers can call upon network resources and provide network statistics state, such as congestion levels, etc. Cloud Connectors enhance and enable cloud-based applications to operate more efficiently over networks while the onePK API allows application providers to leverage the network for optimal application delivery.

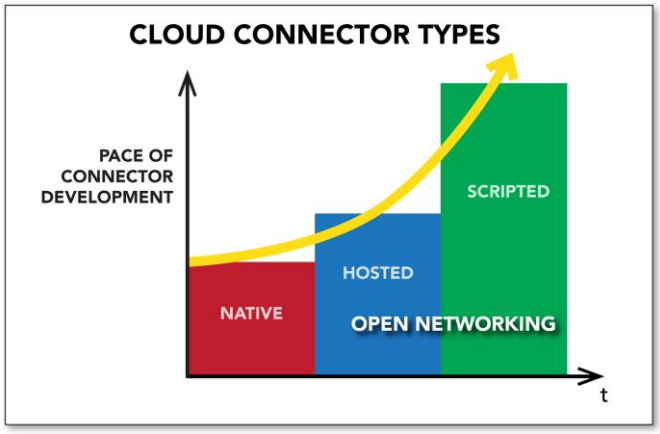
A key point to note is that while the industry has focused on Open Networking and SDN as a data center set of technologies, Cisco, through its Cloud Connectors, shows how pervasive SDN is in that Cisco is using it to add value to its branch office networking portfolio, in addition to campus and data center assets.

Cloud Connectors offer increased flexibility and a major injection point of innovation so more features and functions can be added to existing network investment. From an operational cost reduction point of view, Cloud Connectors enable business continuity, consistent and optimized use of network resources for enhanced user experience, plus simplified application deployment. There are Cloud Connectors that focus on increasing application performance too.

Cloud Connectors are responsible for delivering a cloud-enabled next generation network that requires much more application deployment flexibility. They ensure that application performance and user experience is optimal while business operations are not compromised as cloud services are added to the corporate application portfolio mix. The bottom line is that Cloud Connectors are applications enabled by the Cisco ONE framework that deliver cloud-ready branch offices.

Cloud Connector Types

To address the wide range of Cloud Connector requirements, Cisco has segmented its Cloud Connectors into three categories. They are 1) Native, 2) Hosted via Cisco or 3rd party and 3) Scripted, which is a future Cloud Connector category. A native Cloud Connector is one that is integrated into IOS or IOS-XE. The WebEx CCA, Cloud Web Security and HCS Survivability are in this category. The hosted Cloud Connectors reside on a Cisco ISR G2 2900 or 3900, which support Cisco Server blades, such as the UCS-E (Unified Computing System) Series. The third Cloud Connector type is the scripted Cloud Connectors that leverage Cisco's onePK API, which will open up the network to an innovative set of new cloud-enabled services. Both hosted and scripted Cloud Connectors may use Cisco's onePK API.



Native Cloud Connectors

Survivability HCS Cloud Connector on Cisco ISR G2: The HCS Cloud Connector supports Survivable Remote Site Telephony or SRST solution for Cisco Hosted 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 Cloud Connector on the Cisco ISR G2 assures that branch office voice over IP continues to make calls. This is accomplished by allowing branch users to continue making calls leveraging the public switched telephone network (PSTN) for backup. HCS is critical for call centers, financial services, retail stores and any office that provides call support for customers.

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

Hosted Cloud Connectors

Hosted Cloud Connectors are currently for the Cisco ISR 2900 and 3900 series of products as they are capable of hosting compute blades such as the UCS Express or the UCS E-Series Server blades. The UCS E-Series is available as a single or doublewide ISR G2 module that runs a quad-core or six-core Intel Sandy Bridge processors with as much as 48 GB of RAM and 3 TB of storage. UCS E-Series provides higher performance than the UCS Express so as to run multiple Cisco, plus third-party network services, applications and Cloud Connectors simultaneously. From a management point of view, the virtualization layer of the UCS-E can be managed via VMware's vCenter with UCS hardware managed via Cisco's CIMC or Chassis Integrated Management Controller for UCS controller management. Simplification is derived by a single management point for managing all UCS deployments that span data centers and branch offices. In addition, branch office infrastructure consolidation is realized, thanks to virtualized application hosting on Cisco ISR G2 routers.

The lights-out management capabilities of the UCS-E Series and Cisco ISR G2 enables multiple Cloud Connectors to run simultaneously per branch and of course, different branches can run different Cloud Connectors based upon unique requirements. Below are examples of hosted Cloud Connectors.

Xerox Mobile Print Cloud Connector: Third-party Cloud Connectors include integration and collaboration between Cisco and partners such as Xerox. Xerox, for instance, has developed two Cloud Connectors: one for private and one for public clouds.

The concept behind Xerox's Cloud Connector is to provide print services to mobile users equipped with an iPhone and/or iPad, for example. Consider that you enter a business equipped with your iOS device, and you need to print a document. The Xerox public Cloud Connector can provide a printer code that can be entered into a Xerox printer keypad where your document, email, spreadsheet, etc., will be printed. Once the code is entered into the Xerox printer, the iOS device and printer are bonded, granting a range of print services. The public cloud connector discovers local printers for the Xerox Cloud Print service and acts as a gateway and informant so that BYOD users know which printers are available for printing. A Xerox software agent runs locally on a UCS E-Series blade server communicating with Xerox Cloud Print services that facilitates printing for BYOD users.

The private Cloud Connector provides all required services to print including job processing in the ISR G2. This provides

the flexibility for customers to decide whether they prefer the job processing to be done in their own premises. Similar to the public cloud connector, the private cloud connector leverages the UCS E-Series blade server to provide the mobile printing services. Both public and private cloud connectors offer mobile-app as well as email based printing.

Amazon Storage Gateway Connector: The Amazon Cloud Connector is another great example of how Cisco is delivering value in its Cloud Intelligent Network Framework. Amazon's Simple Storage Service or Amazon S3 developed a Cloud Connector to leverage Cisco's storage gateway that resides on a Cisco ISR G2. The Amazon Cloud Connector allows branch office applications to experience S3 with responsiveness that is LAN like, thanks to caching. An application can be using 10 TB of information but practically only 1 TB could be available in the branch. The Amazon Cloud Connector provides the application with the other 9 TB via cache over the WAN. Access is very affordable, too, with cloud storage as low as 10 cents per GB per month. The latest Amazon pricing can be found here.

Asigra Cloud Backup Connector: For a cloud-based agentless backup solution, Cisco has worked with Asigra to develop a Cloud Connector. The Asigra Cloud Connector enables multiple back-up solutions to improve data recoverability and business continuity. For example, an employee may have changed his/her SalesForce.com schema, wiping out previous information during backup. The Asigra Cloud Backup Connector can recreate and recover the lost information as well as other information in branch applications. The Asigra Cloud Backup Connector ensures anytime/anywhere recovery of data on servers, VMs and mobile devices. It runs on a Cisco 2921 ISR G2.

There are a wide range of storage related Cloud Connectors that offer seamless and reliable backup and file services. In addition to Asigra and Amazon, CTERA, Maginatics, Panzura and Unitrends all offer storage connectors.

VMware VDI Connector: Cisco and VMware are collaborating to develop a Cloud Connector that provides business continuity services for VDI users. The first connector assist in re-establishing VDI sessions, be it in the branch or cloud which is very helpful in the case of high latency or connectivity issues. Consider that an employee has developed an important presentation on a VDI terminal, and he/she needs to present it very shortly, such as in five minutes. Then suddenly he/she loses the VDI session! This VDI Cloud Connector can spawn a VDI session directly to the local branch Cisco ISR G2 router's VDI server to re-establish the VDI service. While this is a manual procedure today requiring a phone call to IT, over time, this Cloud Connector will be automated in that it will provide a cached way to continue with the presentation and address latency or other network performance issues.

The Desktone connector empowers service providers and enterprises to deliver virtual desktops remotely managed from the cloud. In addition, Atlantis Computing increases VDI density and accelerates Cisco "office-in-a-box" performance. There will be more VDI Cloud Connectors from a wide range of virtualization vendors plus a focus on VDI acceleration.

Infoblox Network Services Connector: In the business continuity area, a Cloud Connector is available to assure cloud-based services are accessible in the event that a DHCP server operation is interrupted. Cisco has worked with Infoblox to develop the Infoblox Network Services Connector. In the event that a corporation's DHCP server crashes, access to data center applications from the branch office would be disrupted as IP addressing and resolution services would be unavailable and connectivity interrupted. This Cloud Connector assures branch office survivability by providing local IP services for VMs and physical devices providing continuous provisioning when data centers are unreachable. The Infoblox Network Services Connector is based upon the Infoblox vNIOS and Trinzic DD running on a Cisco ISR-G2 with UCS-E Series.

Ping Identity Cloud Connector: In identity management, Cisco worked with Ping Identity to create a Cloud Connector to facilitate the creation of trust between two or more parties. Consider an organization that works with re-sellers and suppliers that need access to the organization's IT systems. The typical challenge is how to manage identity of all parties that the organization is working with especially considering the dynamics of people being granted access then denied as they transition to new roles and responsibilities. This Cloud Connector allows partners to manage their users' identity, so that in the case of termination, an employee's cloud services accounts can be transitioned, deleted or terminated rapidly, thanks to the identity Cloud Connector at the reseller/supplier's premise establishing the trust relationship with the connector counterpart located in the data center of the IT organization.

Another use of the identity Cloud Connector provides a single sign-on at the point of network access that grants admission to IT resources uniquely for each user. A user presents credentials at the point of network access, which is then applied to grant access to select IT resources that is regulated by policy. This trust relationship could carry over to all applications that the organization uses independent upon private or public cloud. The identity Cloud Connector provides identity services through credential management.

In short, the identity Cloud Connector manages identity and trust relationships by securely hosting user credentials to a wide variety of public and private cloud application services.

This identity Cloud Connector is made possible by Cisco working with partner Ping Identity and Cisco onePK API.

Security: SecureLogix's Cloud Connector protects voice networks with business policies that control inbound and outbound usage. Voice security capabilities, such as the ability to shut down anomalistic call behavior including denial of service attack, flood of call connections, etc., are included. Look for new data protection Cloud Connectors in the near future.

Collaboration: The Nevotek Collaboration Cloud Connector is focused on the hospitality sector by connecting IP phone systems to hotel provisioning services. The Cloud Connector facilitates auto provisioning of collaboration services triggered upon check-in and check-out room allocation, voice mailbox set up, room phone establishment, Internet connection, etc. Pre-IP phones did a good job connecting into provisioning systems, but IP phones have lagged. This connector bridges that gap and enables hotel operators to move costly local IT operations of smaller hotels into the cloud.

Digital Signage: The Industry Weapon Cloud Connector facilitates the distribution and cache of content to be displayed on digital signage at branch offices. Each branch will now have localized content pertinent to its clientele while maintaining centralized management to push content across different locations. This Cloud Connector provides a greater range of digital signage display options and increases content display performance as it's cached locally in the branch. It can continue to stream content even in the event of a connectivity issue between display and video source.

Transportation: The Setel Hellas Transportation Cloud Connector specializes in optimization of network services, such as security, satellite connectivity, voice services, plus business transactions for large ships in transit. The Setel Hellas Cloud Connector can be managed via private or public clouds.

A complete list of Cloud Connectors can be found here.

Hosted and Scripted Cloud Connector Evolution

Hosted Cloud Connectors are likely to expand in functionality by leveraging Cisco's onePK API to script enhancements. Hosted connectors can address different development use cases than scripted connectors. For example, a company that has built a hosted connector may utilize the Cisco onePK API abstraction of network capabilities to add network functions, such as congestion state, identity, etc., to their hosted connector. Scripted connectors are new standalone code, which is typically developed rapidly from a zero scripted in a software environment, such as Python.

For example, a developer of scripted Cloud Connector for a school may restrict student access to inappropriate YouTube content. YouTube content can be restricted with the inclusion of a tag in the traffic flow, which triggers YouTube to filter video request so that students only access adequate content. If a student requests inappropriate YouTube content, the network will display a message such as "this content is restricted" to the student's computer. This scripted Cloud Connector consists of a few lines of code that's implemented independent upon school grounds location and requires no client software to be installed on student endpoints.

There are some 21 Cloud Connectors available today, with more in development at Cisco, as well as partners though its Cloud Connector ecosystem. This is an integral part of Cisco's SDN strategy where the rich intelligence of Cisco's networking platforms can be harnessed through Cisco onePK API, which enables organizations to build their own software solutions to improve services to their customers, employees and partners.

The Cloud Connector ecosystem is designed to foster third-party development of Cloud Connectors for hosted and scripted connectors. The development environment for scripted Cloud Connectors will be available for both third party as well as IT departments over time to leverage with the ability to favorably modify applications to meet unique requirements. The scripting environment is network centric. In today's networks, IT has control over network behavior, but to modify network behavior for an application, an understanding of how a network operates is required, which is detailed and intricate. A bridge between the needs of an application(s) and/or application developers and its interaction with the network needs to be built. This is a new concept to the IT community as hosted and scripted Cloud Connectors enable applications to be network aware.

Cloud Connector Value Proposition

Over the next several quarters, expect that Cisco will build upon its base of Cloud Connectors and add connectors that deliver QoS and application optimization, identity services, authentication services, deep transaction inspection, location services, access control, network visibility, policy and configuration. In short, Cisco is well into building its Cloud Connector portfolio.

The Cloud Connector operational model is simply turn it on, and automated services are delivered to end-users. For example, the Cloud Web Security Connector, once engaged, automatically directs public cloud-destined traffic to the cloud directly from branch office Internet connection securely, protecting BYOD and corporate devices with no additional client software installation required. This connector also increases application performance as backhauling public

cloud traffic over an MPLS network to the data center Internet connection is avoided.

Cloud Connector Cisco Partner Value

Cisco is building a large Cloud Connector portfolio that contains value propositions for various stakeholders. For partners, Cloud Connector capabilities offer a new go-to-market opportunity. Network equipment channel partners typically enjoy relationships with network team management. As Cloud Connectors impact application performance, cloud services, business continuity, branch office business process and WAN design, the range of solutions partners can now offer network team management has expanded and so, too, will its customer conversations.

Cisco cloud services' partners can now differentiate WAN services offered by optimizing existing WAN solutions for cloud application delivery. For those offering cloud services, it too can be enhanced with business continuity for voice, web, VDI, DHCP, etc. Some partners will find that they can now be in a position to offer one-stop shopping for a more complete or holistic cloud solution.

The above Cloud Connectors discussed are just a sample of the new cloud-enabled branch office WAN options. The scripting environment with its ability to abstract and expose network functionality and services for network teams, partners and Managed Service Providers or MSPs to leverage, promises to deliver Cloud Connectors to market at a pace that is sure to be faster than the networking industry has delivered.

Cloud Connector Cisco Customer Value

The Cloud Connector value proposition for Cisco customers and prospects is based upon capturing cloud computing scale, application mobility, cost advantage, investment protection, etc., value and putting it to work for your corporation. Cloud Connectors augment application value with network awareness, which will not only add features to applications but also deliver key business requirements such as security, business continuity, application performance productivity, etc. Corporate computing is undergoing a tremendous transition, thanks to BYOD, cloud services and virtualized data centers. Cisco's Cloud Connectors promise to increase the pace of network innovation by delivering a platform for rapid delivery of network solutions that keep pace with computing changes and customer challenges.

The Cloud-Enabled Branch Office

Cisco's Cloud Intelligent Network Framework and in particular, its Cloud Connectors offer a means to increase adoption of cloud services by injecting innovation into branch office networking at the same or greater pace of mobile and cloud computing deployment. Existing Cloud Connectors increase application performance by eliminating backhaul, increase cloud security through Cloud Web Security, deliver business continuity solutions for voice, data retrieval, DHCP and VDI sessions while offering new capabilities, such as smartphone printing, cloud storage and much more to come. In addition, Cloud Connectors are packaged as part of the Cisco ISR G2 and UCS-E Series, which eliminates additional branch office footprint need and deployment concerns that are most often found with multiple component solutions. Cisco's Cloud Intelligent Network Framework is not only cloud-enabling the branch office, it promises to deliver a range of new services and capabilities that are sourced from Cisco, its partners and IT departments, thanks to Cisco's onePK APIs, compute platforms and router extensibility.

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 200,000 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. He is also the co-founder and conference chair of the Open Networking User Group, which sponsors a bi-annual meeting of over 200 IT business leaders of large enterprises. Mr. Lippis is currently working with clients to design their private and public virtualized data center cloud computing network architectures with open networking technologies 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.