A Lippis Consulting Industry Paper

A New Holistic Approach to Enterprise Network Management

Integrated Wire, Wireless and Policy Management

By Nicholas John Lippis III
President, Lippis Consulting

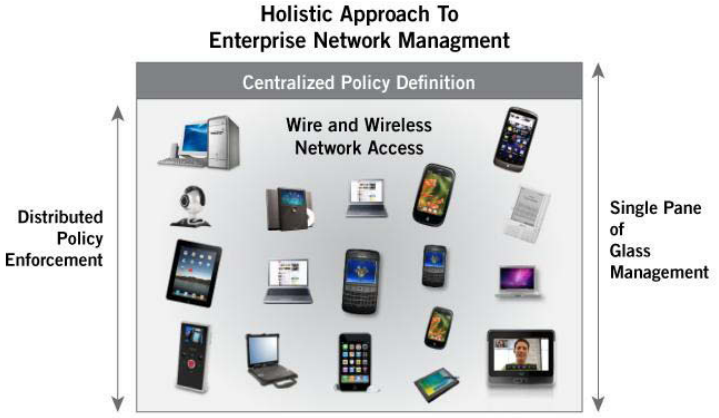
July, 2011

Abstract:

IT business leaders are demanding a unified policy-driven management strategy for network access and security, mobile endpoints including iPads, tablets and smartphones. A holistic network approach is the unification of these management assets to simplify operations and shift control to IT leaders. A holistic network approach from Cisco Systems is to streamline NetOps through the automated orchestration of policy, management and infrastructure. In this model, network administrators will not have to access multiple different management systems to collect data, correlate it manually and then attempt to identify problem location. One management system, Cisco Prime NCS with integrated links to ISE, delivers this service to NetOps, drastically improving network visibility and reducing troubleshooting time through a client- or user-focused approach to managing corporate networks in the age of mobile and cloud computing.

Introduction

Network infrastructure has been changing at one of the fastest paces in its twenty-five- plus year history, thanks to the introduction of mobile endpoints such as laptops, iPhones, iPads and Android-based smartphones. Mobile computing, with no signs of abatement, has driven the huge growth in Wireless Local Area Networking or WLANs. But wired and wireless networks did not share a common management system, leaving IT operational groups with separate views of wired and wireless networks



and the devices they connected, and frustrating operations' management and troubleshooting tasks. Modern enterprise networking is focused on providing a holistic infrastructure that connects wired and wireless devices while providing network operations a 360-degree view of all network users and their associated connected endpoints.

Much like a national transportation system that provides rules of the road and distributed enforcement to assure proper use, IT business managers are being provided centralized policy definition tools to do the same in enterprise networking. In short, enterprise network best practices are to provide one wired and wireless network to connect mobile and fixed endpoints while providing IT operations with a single pane of glass management system with centralized policy control. As the old adage goes, you can't manage what you can't measure. For networking, this means connecting all user and non-user devices, both wired and wireless, into one network with one management system equipped with centralized policy creation and monitoring.

To grasp the magnitude of this expansion of mobile networking, consider the following statistics. The smartphone market nearly doubled year-over-year in Q4 2010, to about 101 million units, according to Canalys. According to RBC analyst Mike Abramsky, only 0.3% of the Earth's inhabitants owned a tablet at the end of 2010, and he projects a vast market for these devices. Combined, the smartphone and tablet user base is approximately 394 million worldwide versus other markets, such as TV subscriptions (600 million), total PCs (1.3 billion) and mobile subscribers (5.1 billion). According to RBC, there will be more than 400 million tablet users alone, worldwide, by 2014, including 185 million tablets sold in 2014.

What's startling is the acceleration of adoption and resulting IT rate of change. Apple is on track to sell 8 million iPads for the 2011 June quarter—its best quarter of iPad sales and a 74% increase over last quarter. According to Apple, it sold 200 million iOS devices, which is less than half the market of mobile devices. In addition, both IDC and Gartner have cut their estimates for global PC sales this year, due in part to the growing popularity of tablets like Apple's iPad over small laptops. Gartner predicts that PC sales are to grow 9.3 percent this year, down from its previous forecast of 10.5 percent. IDC expects worldwide PC shipments to increase just 4.2 percent

this year, down from its February estimate of 7.1 percent. While both differ in their growth projections, both do agree that PC unit sales growth is declining, thanks to the demand in smartphones and tablet mobile computing.

Mobile Computing Changes Business Processes

What this means for IT business leaders is that their network infrastructure needs to be able to support a growing population of mobile devices plus new business processes and dynamics. For example, healthcare providers are using mobile tablets and iPads to look at x-rays, check medication interactions and view patient medical histories. In the future, more emergency room providers such as Allscripts, NextGen, Greenway, eClinicalWorks and others will write native iPad applications to allow providers to routinely lookup up full patient histories, order procedures and medications, view diagnostic images and even communicate with patients via their iPads. By communicate, they mean everything from text messages to video chat. Dr. Roger Haley, kidney specialist at Kaweah Delta Health Care District in Visalia, said, “This is going to make my day easier and patient safety better because not only now I don’t have to find a work station to do what I need to do. What I need to do I can do it right there, right then, right now.” Higher education is also using mobile devices for taking attendance, collecting data, reading scholarly articles, recording notes, using textbook tools, planning lectures, etc.

But while high growth is in mobile devices connected via WLANs, an increase in non-user types of wired devices is being plugged into corporate networks too. These non-user devices are printers, video surveillance, wireless access points, etc., attempting to access the network and IT assets. According to Multimedia Content and Services, revenue from shipments of IP video surveillance cameras nearly doubled in 2005 and continued to grow at a Compound Annual Growth Rate of 87.9 percent from 2004 to 2010, to reach $3.9 billion.

A New Model to Manage Enterprise Networks

What is clear from the market is that employees, customers, partners and suppliers need access to the enterprise network, and thanks to consumerization of IT, they have access to the technology and tools to do so with and without IT’s blessing. From an IT perspective, the imperative is to bring all interested parties onto the corporate network with appropriate security and access to IT resources. This means managing the corporate network like a single access network versus a fragmented wired and wireless network. By having all users and endpoints on a single network with a range of access methods then IT operations can create policies that transcend the entire network, touching every endpoint and application, creating unique profiles and privileges for users and their devices to be productive while using the enterprise network.

This approach to holistic networking empowers IT administrators and users alike to be productive, innovative and creative using the endpoints they require to do their job while providing a well-managed and secure infrastructure. This holistic approach also allows IT to deliver services in new ways without the network infrastructure being an exploit mechanism. What is fundamental to this approach is a single pane of glass for wired and wireless network management, a centralized identity engine to define policy and a network equipped with the tools to enforce policy.

A Shift from Network Device to User-Focused Management

To achieve this vision of increased access flexibility and IT control, network management is shifting away from network device-oriented management to users and their endpoints. For example, from a network management console, Network Operations (NetOps) can search for a user’s name, which will display the endpoints connected to the network associated with that user. These endpoints can be wired or wireless. Consider that Bob has three devices connected to the network; two are wireless and one is wired. The wireless devices are connected properly with no issues, but the wired device is experiencing an authorization failure, because the organization is slowly adopting 802.1x on the wired network. IT may have

created a policy that does not allow personal assets on the network or allows restricted access, for example. With the context of identity information, IT is able to identify what the device is and allow fine control over its behavior on the network.

The context is that NetOps is provided a 360-degree view of a single holistic network that allows it to view users and their devices for quicker troubleshooting and overall network management efficiency.

Enabling the Shift to User-Focused Management

In order to move from the traditional device-focused approach of network management to this new user-focused management approach requires tools and systems that meet certain criteria.

Über-view of the Network: NetOps needs to combine visibility of both wired and wireless networks. Key metrics regarding how users access the network and the impact these users have on the access infrastructure must be clear. On the wired side, bandwidth breakdowns, top switches, device uptime, etc., should be easily understood, while on the wireless side, WLAN type, protocol, access method, upstream and downstream bandwidth is equally important. Solutions that provide a dashboard that allows one quick assessment and view of network dynamics on both sides of wired and wireless networking deliver significant returns in this regard.

Viewing Wired and Wireless Clients: As the end-user utilizes both wired and wireless devices, both organization provided and consumer grade, NetOps needs a consolidated view of wired and wireless clients more than ever before. However, having just a converged view may not be enough; the ability to quickly switch between different network views and to drill down on a particular area can result in substantial improvement in how quickly client issues are resolved.

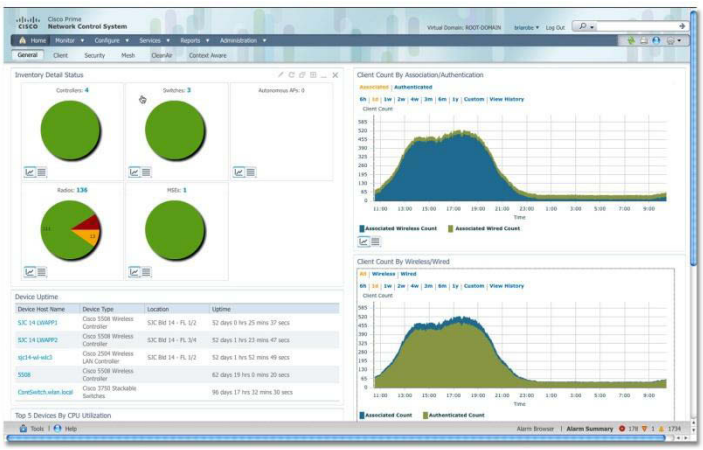
WiFi Network Type: NetOps needs to have visibility into users/clients and endpoints on the network. For example, a distribution view that may show 60 percent of clients on the 5 gigahertz bandwidth in 802.11n would show a well-designed client distribution as the 5gigahertz band is a less crowded spectrum than 2.4 gigahertz space. This view can quickly show how effective the wireless network meets end-user need. As we know, not all organizations have moved to 802.11n so the solution views should also support legacy WiFi types such as 802.11a, b, c frequencies.

Wired Networks: NetOps can similarly understand the distribution of wired bandwidth use across clients with a utilization view of the number of 1GbE versus 100MbE versus 10MbE ports, etc.

Traffic Distribution: An interesting and valuable view would be top usage charts such as the top clients on SSIDs or top clients on switches. This easy access to traffic distribution information would aid in capacity planning so that NetOps knows whether to grow or reduce capacity or repurpose devices. Additionally, the ability to view the number of clients and bandwidth usage trends for specific time frames can aid in seeing how network usage is changing to better plan for additional devices coming online. For example, if the average client count on the network is multiplying by two or three week over week, NetOps can then clearly recognize when they need to add more network infrastructure resources and plan accordingly.

Posture Data Pulled In: Having the ability to view posture and profile information regarding certain clients or client types for users/clients on the network enables a clear understanding if a user is not able to access the network due to a network access problem or if it is by design, thanks to policies purposely put in place.

From a network vendor point of view most are focused upon wired or wireless management with a few discussing a combined network management offering. Cisco Systems is unique in that its Cisco Prime Network Control System (NCS) network management



product provides a single pane of glass for wired and wireless management organized around users, endpoints and network devices. Most importantly, though, is that Cisco Prime NCS and the Cisco Identity Services Engine or ISE, platform that offers centralized policy definition, are linked and share information so as to hasten the pace of user network access troubleshooting, which is a huge helpdesk pain point.

Cisco Prime NCS is part of Cisco's Prime network management strategy that seeks to reduce operational cost through simplification.

The Cisco Prime for Enterprise strategy is built on a service-centric foundation and a set of common operational attributes. Each Cisco Prime for Enterprise product includes one or more of the six common operational attributes:

- Consistent usability across all products is delivered through an intuitive user interface and optimized operator methodology.
- Guided workflows and automated troubleshooting tools based on Cisco Validated Designs and best practices developed from Cisco knowledge including Cisco Smart Business Architecture (SBA).
- The ability to automate and augment the lifecycle process required to manage an end-to-end network.
- Day-one device support for new devices and technologies developed by Cisco.
- Cisco smart interactions deliver personalized automated self-help tools.
- Deployment of products as either physical or virtual appliances.

The Cisco Prime for Enterprise portfolio of products simplify network management, improve operations efficiency, reduce errors and make the delivery of services on the network more predictable.

Cisco Prime Network Control System (NCS)

With troubleshooting client connectivity issues being one of the biggest IT pain points, Cisco Prime NCS offers access to crucial information speeding resolution. As mentioned above, when a user calls a help desk with the issue of not being able to access information needed, all the help desk representative needs to do is enter a search for the individual's user name. This is far simpler than relying on the end-user to provide a MAC or IP address that often requires time-consuming help desk intervention.

Based on the user name, Cisco Prime NCS displays the number of devices associated with the user and reveals which devices, wired or wireless, have potential problems. This streamlined process minimizes the guesswork associated with finding the cause of the problem. Faster troubleshooting enables first-tier support to solve more problems, without escalation, which allows end-users to get back online faster, thus maintaining employee productivity. This is the power of converged user and access visibility for wired and wireless networks with identity integration, enabled by Cisco Prime NCS and Cisco ISE.

Centralized Policy Definition-Distributed Enforcement

A centralized policy engine whose rules are enforced throughout the network offers IT operations significant simplification. Any person and their associated endpoint may be offered access to network resources anywhere, but only if certain rules are followed and enforced. Cisco's SecureX architecture provides the framework and tools for context- based policy rule definition, user and device authentication, profiling and posture assessment plus troubleshooting and ongoing monitoring of policy enforcement. ISE is Cisco's new centralized policy engine that combines much of the policy features and attributes of Cisco's ACS (Access Control Server) and NAC (Network Access Control) profiler, guest, manager and server simplifying policy rule definition and enforcement. It also offers a unified view of policy management. TrustSec 2.0 is the enforcement mechanism of policy rules into network elements enabling wide distribution of policy enforcement.

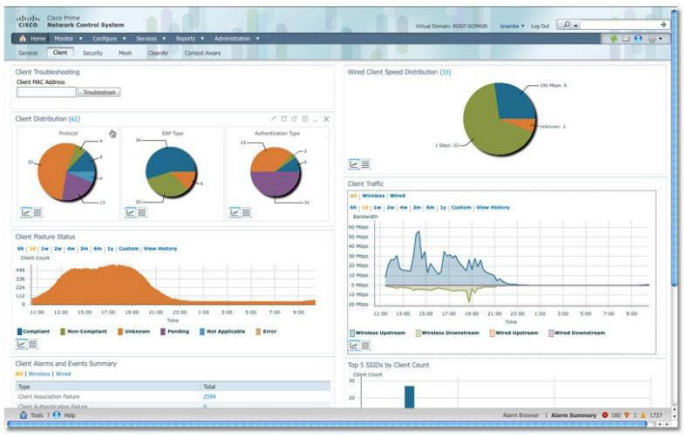
Cisco SecureX Architecture enforces security policies based on the full context of the network access situation. This next-generation, context-aware security architecture meets the evolving security needs of borderless network environments. For example, contextual information such as user and endpoint

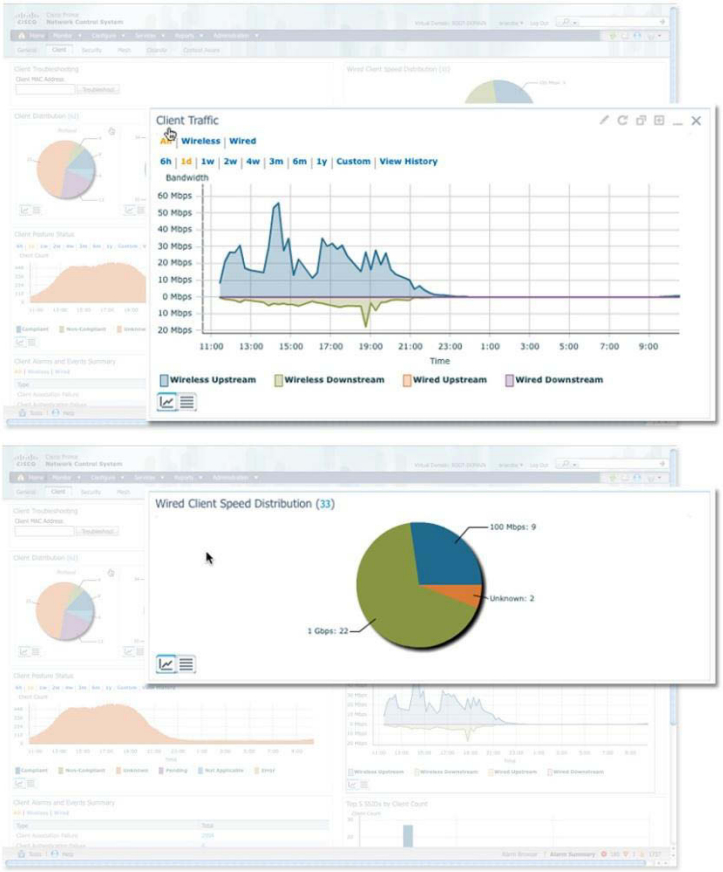
identity, application(s) being used, time-of-day and location is used to determine if network access is allowed or denied.

ISE acts as the source or "brain" for centralized enterprise network policy while TrustSec 2.0 provides a range of access control capabilities or the 'braun' to enforce these polices. Access control can be based on the user role, the type of endpoint, the posture state of the endpoint, or a range of other attributes. These attributes are used to make intelligent decisions as to who and what can access production services, restricted services or even be denied access. In addition, the network can “tag” a user’s data stream, so that as the stream transverses throughout the enterprise IT infrastructure, the network can enforce defined policy independent upon the stream’s destination(s). For example, once the user has passed access control, should this user decide to search for a payroll server location, the network may recognize that he/she is not allowed access, thanks to defined policy, and the network can drop the requests and log the event.

Cisco Prime NCS plus ISE = Holistic Network Management and User Flexibility

With the combination of Cisco Prime NCS and ISE, IT can assure access for any mobile endpoint, plus fixed user and non-user devices that are wired into the corporate network. With all endpoints connected into a common network infrastructure, ISE can be put to work to control and protect IT assets in ways that were not previously possible. ISE provides policy to mitigate and protect the new mobile workload and workforce on the network while Cisco Prime NCS provides operational efficiency to manage both wired and wireless infrastructure with a common set of views and tools for NetOps to be more effective.





Link between Cisco Prime NCS and ISE

The power of this holistic network management system is highlighted during troubleshooting user problems as described in the “Bob” example above. Expanding on Bob’s trouble ticket, after NetOps searches his name in Cisco Prime NCS, NetOps is provided a list of client devices and network connections associated with Bob’s endpoints. NetOps can drill down into each endpoint and network link. The same is available in ISE to view policy for each endpoint associated with Bob.

ISE policy integration into Cisco Prime NCS provides data information that is collected and correlated in terms of the type of endpoint with contextually-rich identity, well beyond simple user and device type afforded through the radius protocol, for example. An ISE API provides the vehicle to populate this information into NCS, making the data much richer with identity and access correlated through the NCS management solution.

For Bob's trouble ticket, Cisco Prime NCS's troubleshooting tool provides visibility to network connections and determines if there is a network connectivity or security issue. With a network connectivity problem ruled out, NetOps can then pull ISE information to determine if Bob may **not** have authorization to access certain IT assets and thus his access was blocked. To help guide the process, the NetOps Operator is presented recommendations as to how to resolve the issue, orienting them in the right direction to resolve the problem.

The key point to consider is that Bob's trouble resolution scenario started with troubleshooting a user issue, NOT troubleshooting a wired or wireless device issue. This is fundamental as most users are simultaneously connected to both wired and wireless networks. This combination of Cisco Prime NCS and

ISE is also a platform that other innovations will be spawned from, adding value to NetOps. Innovations, such as pre- and post-access control, distributed sensing and defenses, could be added to this platform.

Recommendations

The following recommendations are offered to IT business leaders for their consideration:

1) Define policies or rules of proper use of network resources for all employees, partners, customers, contractors and guests.
2) Consider defining different policies based on device type, i.e., laptops having full access versus tablet having limited access.
3) Seek to configure a centralized policy engine with the above rules and the ability to easily adjust policies. Start with a pilot as this will be a trial-and-error process.

Integrate wired and wireless LAN management to provide a single access network managed via a single pane of glass. Here, too, start with a pilot to gain skill sets and learnings of managing a holistic network. Unified management and centralized policy deployment may start simultaneously or in sequence.

4) With unified WLAN/Wired LAN management and a centralized identity engine past the pilot phase, consider piloting the interconnection of both. This assumes that a link between policy and management is supported. Choose a vendor that has this linkage available.
5) Expand pilot. With experience gained both in terms of technology skills and organization procedures defined, expand the pilot at pace. Carefully monitor help desk activity to measure defined rules, assuring that access is not too restrictive.

Conclusion

The corporate network will increasingly provide both posture assessment and enforcement. Defenses will become highly distributed throughout all aspects of the network to close vulnerabilities at the point of access. This will mitigate an exploit before its passes beyond a port independent of whether that port is wired or wireless.

This holistic network approach from Cisco is designed to streamline NetOps through the automated orchestration of policy, management and infrastructure. In this model, network administrators will not have to access multiple different management systems to collect data, correlate it manually, and then attempt to figure out the location of a problem. One management system, Cisco Prime NCS with integrated links to ISE, delivers this service.

To build a holistic network management approach with Cisco Prime NCS and ISE could be achieved by migrating from existing Cisco Wireless Control System and Cisco ACS and NAC systems. If these products are already being used to manage a corporate network, then software updates will add value and features to this powerful new unified approach to network management. After a detailed review of Cisco Prime NCS and ISE, it's recommended that IT departments pilot this unified management solution to ascertain its utility within their corporate network.

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 160,000 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, Cigital, 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 online 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 Master's thesis work included selected technical courses and advisors from Massachusetts Institute of Technology on optical communications and computing.