Lippis Report 221:

HP Invests Heavy in Unified Wired and Wireless Network Infrastructure

By Nicholas John Lippis III
President, Lippis Consulting
August, 2014
Ever since the introduction of the first iPhone in 2007, mobile computing has never been the same. In just six short years, the smartphone industry is selling nearly 500 million devices a quarter, according to Gartner, and there will be 50 billion devices, including laptops, smartphones, iPads, tablets, non-IT devices, etc., connected to wireless networks by 2020. For the past several years, BYOD or Bring Your Own Device projects have been the largest budget spends for IT departments worldwide, thanks to each user connecting up to three devices on average with Wi-Fi being the preferred wireless network service. As mobility connectivity has been on the rise, wired connections to enterprise networks are still growing, albeit at a slower pace than prior to 2010. From a network design, operations and management perspective, these networks evolved at different paces and with separate management and operational models. The networking industry has been working to unify or converge wired and wireless management to ease operations, increase security and user experience. In particular, increasing complexity or operational cost is driving the need for unified wired and wireless, in addition to the increased use of Software as a Service (SaaS) or cloud computing as a more flexible IT service delivery model. In this Lippis Report Research Note, we review HP’s approach to unified wired and wireless networking.

**FlexNetwork**

With the increasing number of mobile devices being connected to enterprise wireless networks, the enterprise network needs to easily adapt to support both wired and wireless access connections so that IT departments can migrate from wired to wireless at the pace of their user base and business requirements. HP’s FlexNetwork is a converged architecture that spans from data center to network edge. The FlexNetwork architecture consists of three components: 1) FlexFabric, 2) FlexCampus and 3) FlexBranch, all of which are wrapped in HP’s FlexManagement.

For unified access, its HP’s FlexCampus that unifies wired and wireless network management in the campus and branch. FlexCampus strives to provide a consistent user and NetOps experience independent of wired and wireless network use. Unified management is delivered by HP’s single-pane-of-glass management system that provides operational visibility from data center to network edge or branch. This management system provides management and monitoring tools for physical and virtual networks plus wired and wireless network.

HP is one of only a few firms that offer a full comprehensive portfolio suite of both network switches and Wi-Fi gear. Its offering spans from cloud-based offerings for SMB and remote offices to on-premise solutions for medium to large enterprises, all of which are equipped with single-pane-of-glass management. HP’s Cloud-Managed Network Solution for SMB and distributed offices offers cloud-based network management of Wi-Fi gear, such as the HP 365, HP 355 and HP 350. HP claims that the solution lowers total cost of ownership by reducing the need for onsite IT staff and lowering upfront costs by up to 30 percent with a pay-per-use cloud service model.

For on-premise solutions, HP has optimized its portfolio architecture for both centralized and distributed forwarding, which reduces network latency to support the huge growth in video flows, as well as real-time voice applications to avoid controller bottleneck issues. From a security perspective, HP offers pervasive security with best-in-class threat protection through integration with its TippingPoint IPS or Intrusion Prevention System. Key to its security services is comprehensive identity-based access end point security for wired and wireless that’s consistent across the network and can be enforced via multi-vendor environments.

**Small and Medium Business Solutions**

The diagram shows HP’s controller portfolio. The MSM720 is its lower end product that supports 10 to 40 access points. This is a stand-alone appliance targeted at the mid-market that also sports a consistent Operating System (OS) with HP’s mid-market switching gear. Consistent access policies are applied through HP’s Intelligent Management Center or IMC.
Increasing in capacity to 200 access points is HP’s MSM760 controller, which is also a stand-alone appliance. The MSM775 supports two access modes, regular access and roaming services with teaming for reliability and seamless failover of mobility services.

**HP’s Unified Portfolio**

The unified portfolio starts with the MSM775 that offers similar capabilities of the appliances, but is an integrated appliance in HP’s 5400 and 8200 modular switches. The MSM775 sports Layer 2 and 3 roaming, 240 access points and all the features found in the MSM720 and 760 appliances. The MSM775 can be configured for scale up to 800 access points, thanks to teaming or virtual teaming. A virtual team is managed with a single IP address, which is great for reliability as the failover time of a lost IP address is less than 30 seconds. Virtual teaming and N+1 hardware redundancy further increases high availability to assure clients are not disconnected during periods of disruption.

From an architecture point of view, the HP enterprise unified wired and wireless network solution offers two forwarding capabilities. With intelligent access points at the edge of the network, the network can operate in centralized access control, where all traffic is sent to the controller for processing. In addition, the network can leverage the intelligent access points at the

edge of the network to directly forward traffic to end destinations without passing through the controller. And a third model is distributed forwarding, with centralized authentication, where traffic requiring authentication, such as PCI flows, are directed to the controller, while regular traffic is forwarded from the access points to destinations.

For branch office environments, HP offers a unified wired and wireless switch solution in the HP 830, which is a single form factor supporting both wired and wireless connections. For large enterprise networks, HP’s 10500/7500 Unified Wired-WLAN Module plugs into its large 10500 and the 7500 modular switches.

Going forward, HP’s product development strategy is to unify the access layer with products in the portfolio. In short, HP is unifying policy, media access and management at the access layer much like it has done in its mid-market platforms, but now it’s bringing that functionality to the large enterprise. In addition, there is a consistency in operating system, too, across wired and wireless networks.

A notable feature of the HP wireless offering is Wi-Fi Clear Connect RF optimization, which optimizes the radio resource for capacity and performance with automatic power and channel assignments. In addition, automated client load
balancing is provided based on the number of clients per access points, or on traffic load. Airtime fairness optimizes performance or throughput to provide equal airtime to different clients, whether clients are a, b, g or ac end point radios. The HP wireless solution provides interference detection and mitigation so that if the wireless network detects interference on a specific channel, it can perform automatic channel changing, or NetOps can perform this manually. Interference mitigation is supported on HP's access points where a sensor detects and classifies the interference. All of the above represents next generation RRM in that WLAN capacity, and performance is optimized with automatic power and channel assignments, client load balancing and airtime fairness to the end user experience and increased visibility with detection, reporting and mitigation of poor RF performance conditions.

Large Enterprise Unified Solution

The large enterprise solution consists of the HP 10500/7500 unified wired and wireless blade that integrates in HP’s 10500 or 7500 modular switching platforms. This solution can scale to support up to 1,024 access points, and 20,000 clients per module. Depending on the switch, for example, the HP 10512 can support 11 HP 10500/7500 Unified Wired-WLAN Modules in a single switch that scales to 11,000 access points and 220,000 clients. The HP 870 supports 1,536 APs and 30,000 users while the HP 850 supports 512 APs and 10,000 users for overlay wireless deployments. And, these particular platforms sport several redundancy modes: N+1, N+N, and 1+1. 1+1 delivers sub-second failover of mobility services in either centralized and local forwarding mode and ensures continuity of services with 802.1x hot back up.

In addition to scale and high reliability, unified security, end point admission defense plus end-to-end quality of service is integrated and common across wired and wireless access. This HP platform supports full IPv4 and IPv6 so that NetOps doesn’t need to change the controller when upgrading from v4 to v6 as the controller operates in dual stack mode. Depending on the network, v4 or v6 traffic can be tunneled too.

The HP 10500/7500 Unified Wired-WLAN Module, and the HP 870 and HP 850 unified Wired-WLAN Appliances support a set of high-density features, including channel reuse and adaptive rate control. Adaptive rate control is environment aware to adjust transmit rate of access points accordingly. They work with the HP 830 unified access switch, or remote access points in the branches, so that they can be provisioned for local forwarding mode for example and access point-to-controller switch over, thanks to HP’s dual link and fast fault detection feature.

In the branch environment, the HP 830 is a single device with integrated controller and Ethernet switching functions, providing unified access, unified security policies and end-to-end quality of service. The HP 830 supports flexible forwarding to optimize traffic flow, Wi-Fi Clear Connect that’s similar to features found in large enterprise, Layer 2 and Layer 3 roaming. Being in the branch, the HP 830 supports N+1 and N+N redundancy.

For higher speed Wi-Fi access bandwidth, the new HP 560 and 517 IEEE 802.11ac wireless APs enable organizations to support the growing number of mobile devices, while improving user experience with speeds three times faster than 802.11n. The HP 560 access points will also be OpenFlow-enabled, empowering customers to leverage SDN applications without having to rip and replace existing infrastructure.

Single-pane-of-glass Management

Integrated wired and wireless management is one of the most important aspects of a unified product portfolio. HP focuses its investment in the intelligent management center or IMC. IMC is based on a modular service-oriented architecture, so modules can be added as needed. IMC provides management, not only of a HP portfolio, but also multi-vendor network management. IMC can manage some 6,000 devices from 220 manufacturers that includes wired, and now supports Cisco and Aruba wireless devices. The platform offers the capability for network admission control and onboarding of mobile devices. Centralized security policy that spans wired and wireless
devices is a fundamental feature set of IMC as a unified wired-wireless management platform. Therefore, NetOps will have the capability to troubleshoot across wired and wireless networks and to view device security policies to ascertain if an access problem is security policy related or a network/device problem.

The IMC security and policy engine is designed for multi-vendor environments. IMC provides network traffic monitoring and complete visibility of BYOD traffic, so NetOps can view which users are accessing the network, how much bandwidth they are using, etc., so to provide NetOps the ability to set policies for network use and acceptable behavior. Security posture check and agent controls are assessed at network access time, providing end point admission defense. HP’s security posture check feature is based upon the integration with MDM vendors. IMC end point admission defense relies on MDM information on device posture and health before granting access to the network.

What’s different about HP’s IMC is that all of the above is offered in a single tool, as most vendors offer separate platforms for policy enforcement, network management, etc., and in most cases, management and security solutions are not-multivendor. For example, HP’s access control is offered through IMC, called IMC User Access Manager, which is a software module to IMC. It provides the ability to onboard mobile devices to a self-participation portal that uses advanced device fingerprinting to identify the type of device being onboarded, the software releases of the end point and MAC address.

The IMC User Access Manager then provisions the device and assigns the user to a specific VLAN and applies consistent policies depending upon guests or employee access so NetOps can design different policies based on the type of user, type of device, as well as device location. Access can be denied, for example, based on location, for example. Once onboarded, NetOps needs a monitoring capability. The IMC User Access Manager module integrates with HP’s TippingPoint IPS so if a device is infected with malware, IMC will quarantine the device into an isolated VLAN. For good standing onboarded mobile devices, NetOps can monitor user behavior and access history, as well as review traffic analysis. The HP BYOD solution provides visibility to what users are accessing and how much bandwidth they are using. Then NetOps can optimize performance with the tools mentioned above.

Software-Defined Networking

Software-Defined Networking or SDN will play an important role in unified wired and wireless networking moving forward. SDN-enabled unified wired and wireless networks increase network agility and simplify deployment, enabling customers to derive business value from the network. HP has integrated OpenFlow into most of their switches and in the process, found a way to integrate Network Protector into the onboarding and day-to-day security monitoring aspects of networking.

For example, when a new packet enters an HP OpenFlow switch, it forwards the packet to the HP SDN Controller where not only its flow is determined, but its security posture is assessed as well. HP Network Protector is a SDN security application that mitigates threats based on reputation. All new flows are compared to a reputation database or RepDV before a flow is programmed into a switch and traffic permitted to flow. All DNS requests are also compared to the RepDV.

The Network Protector security application in an SDN context is a great bottom-up deployment example in that the controller and all OpenFlow switches become an enforcement mechanism to mitigate threats before they turn into flows. The Network Protector security application runs on the controller providing real-time network threat protection. Network Protector leverages HP TippingPoint intellectual property via its DV labs, which contains a reputation database. The Network Protector security application can protect an enterprise from over 1,500,000 different botnets, malware and spyware, independent of their source, that is over wired or wireless network access.

The Network Protector security application is an HP lead product developed across multiple HP
groups as it contains TippingPoint intellectual property, integration with ArcSight to provide threat visibility and log entry correlation capability plus HP’s SDN controller. ArcSight alerts are correlated across numerous network-attached devices so as to identify anomalous behavior. The Sentinel security application will have both ArcSight anomalous behavior identification plus reputation data from DV labs to mitigate threats at the point before a flow is created. One can see how this may evolve to add HP Fortify for triage and fix outbreaks quickly, for example. HP is rolling out next generation SDN-based services that are unified to address both wired and wireless network access with the same approach it has taken to security with Network Protector.

For example, according to HP, the new HP Location Aware SDN application locates any wireless-enabled device indoors with approximately two meter accuracy—up to five times more accurate than competing alternatives. Powered by technology developed at HP Labs, HP Location Aware enables a wide range of new context-aware retail, asset management and security applications. This application will be integrated with the HP Virtual Application Networks (VAN) SDN controller and is designed to help businesses transform wireless LAN infrastructure into revenue-generating vehicles.

Case in point, HP Communications and Media Solutions (CMS), leveraging Big Data Analytics and Location Aware technology, has developed a proof-of-concept application called SmartShopper. SmartShopper enables enterprises to tighten relationships with customers and monetize the network delivering real-time, location-based offers to customers’ smartphones. Using HP’s location- and context-aware Telco Big Data and Analytics technology, organizations can increase sales by personalizing the shopping experience and drive revenue through targeted promotion of relevant products.

For unified communications, the HP Network Optimizer SDN Application for Microsoft Lync enables automated provisioning of network policy and quality of service to provide an enhanced user experience. The Network Optimizer Application dynamically provisions the end-to-end network path and Quality of Service (QoS) policy via the HP VAN SDN Controller, reducing the need for manual, device-by-device configuration via CLI, which simplifies policy deployment and reduces the likelihood of human errors.

IT management can now get ahead of the BYOD curve as networking vendors are delivering unified wired and wireless solutions that deliver common solutions that span policy, management, monitoring, troubleshooting and security at scale. HP’s approach is comprehensive, thanks to its broad portfolio of switching and WLAN products. Its IMC offering is unique in that it’s multivendor and new large feature sets are offered, as modules allowing a buy-what-you-need model. But most compelling is that NetOps gains consistent and common view of the wired and wireless network that’s integrated into policy and security. By providing a common or unified approach to deploying and managing wired and wireless networking, IT can then provide connectivity based upon user needs, so that as WLAN connections grow and wired connections growth slows, IT is afforded a seamless method to manage this transition. HP is unifying the bulk of its product portfolio and leveraging SDN to eliminate the gap between wired and wireless networking.
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.