A Lippis Consulting Industry Paper

Cisco Preps ACI for General Availability: What to Expect

By Nicholas John Lippis III
President, Lippis Consulting

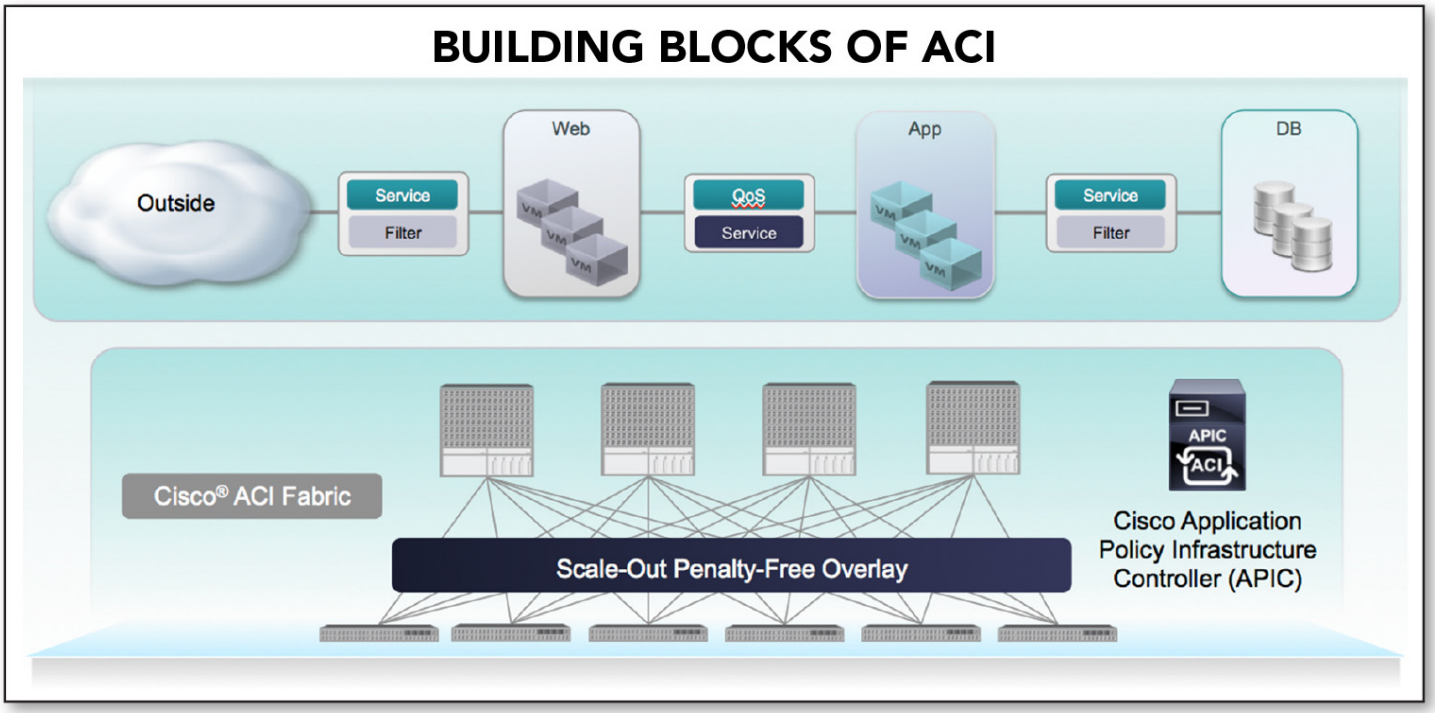
August, 2014

One of the biggest networking events this August is the general availability of Cisco's ACI or Application Centric Infrastructure. Cisco has been shipping its Nexus 9000 series of switches in what is called "standalone mode," which is an ultra-fast data center Ethernet switch, since November 2013. Nexus 9000 orders tripled from 180 in Q3 to 580 at the end of Cisco's fiscal fourth quarter. Cisco promised as part of the Nexus 9000 release that these switches can be deployed in what it calls "ACI fabric mode." ACI fabric mode promises to reduce operational cost, increase agility and link applications to network infrastructure like never before. The manifestation of fabric mode is ACI, and it's now entering general availability. In this Lippis Report Research Note, we take a look at ACI from a point of view of what it can do for data center architects today.

There are three basic building blocks to ACI: 1) a policy model which is an organizing principle for how to group devices into container-like constructs, and describe how they connect, 2) the APIC or Application Policy Infrastructure Controller that provides a single point of management and repository for all described policies and 3) the ACI fabric which is an abstraction of all physical and virtual network devices that make up the ACI fabric. Here's a quick refresher on the three ACI components.

world. The policy for describing the connectivity needs for this application can be defined directly using Group-Based Policies within ACI, but the model could also be very generic too. The policy could be used to define security-oriented policies where an outside (remote site and internet traffic) group connects to the DMZ group, which then connects to the inside group, for example. Alternatively, a GBP could even model how most networks are described today, in terms of VLANs and/or subnets, which would map into various groups. Ultimately, Cisco would like to expose different interested parties to this Group-Based Policy concept so that a **Cisco Certified Internetwork Expert** (CCIE) or a networking genius isn't needed to create connectivity. An administrator would simply express this "group of things" connects to another "group of things." Cisco calls these arbitrary "groups of things" with the terminology End Point Group (EPG), and represents a collection of physical or virtual endpoints. That is an EPG could be physical services, bare-metal servers, virtual machines across multiple different hypervisors, etc. The point is that Cisco can place "things" into groups fairly flexibly, regardless of where they are across the entire ACI fabric.

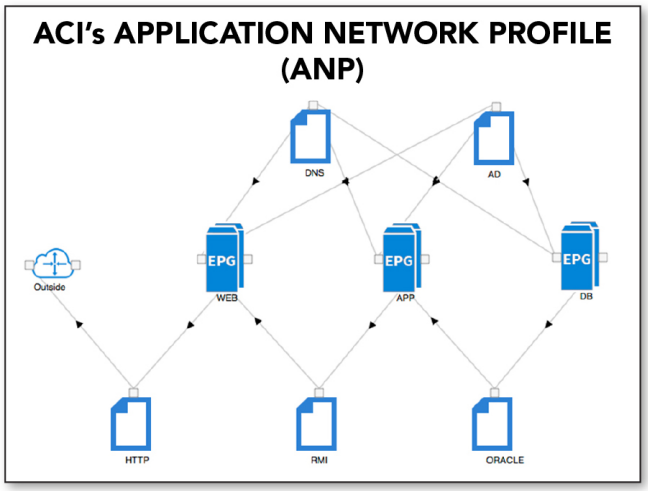
Another core concept in ACI's policy model is the ability to define the relationship between EPGs. This relationship is



Policy Model: ACI's policy model creates a new way of describing connectivity via what Cisco calls the "Group-Based Policy" (GBP) concept. Cisco's policy model provides a generic way of describing how things connect. As an example, consider a typical three-tiered application deployed in a data center that may consist of a Web front-end tier, a middle-ware application tier, and a back-end database tier; this application may also need connectivity from the outside

called a "contract" and describes what can flow or what connectivity methods are allowed between different EPGs. A contract can consist of a specific protocol (or set of protocols) that would be allowed to flow between groups, or it could also be used to stitch in a Layer 4-7 service graph to apply network services, such as a firewall, load balancer etc., to the connectivity between groups.

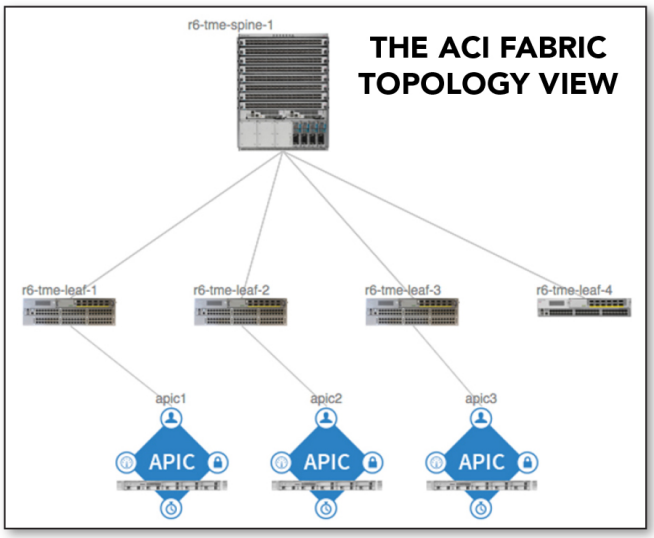
From a SecOps perspective, the ACI policy model essentially implements a white-list model for security, which is vastly different to today's implementation of ACLs. In today's networking mode, NetOps assumes anything can communicate, but only those that can't should be locked down with ACLs; this follows a black-list model for security. In essence, the entire ACI fabric can be seen as operationally identical to a large distributed context-based firewall, which is enforcing policies holistically across the entire data center.



Cisco contains these definitions of EPGs, contracts and outside networks into something called an Application Network Profile (ANP). These ANPs are completely abstracted/de-coupled from any underlying physical/virtual infrastructure, and hence can be copied to a completely different ACI fabric and re-instantiated again. This makes life very easy to define application connectivity globally across multiple pods or sites without the application administrator needing to understand the details of how a given fabric is architected.

APIC: ACI policies are described in the APIC or Application Policy Infrastructure Controller. The APIC is a cluster of UCS C-series x86 1RU rack servers and provides a single point of management and repository for all the described policies, and any other policies to provision, administer, monitor and troubleshoot the fabric; according to Cisco everything is now a policy! Note that APIC is not used for forwarding or lookups. As a matter of fact, once policies are described within APIC, it can be completely removed, and everything will keep functioning, but this point is to emphasize that the APIC is not needed during forwarding operations.

In fact, Cisco does not recommend completely removing the entire APIC cluster as administrators would not be able to modify policies until at least one APIC is re-attached. The APIC cluster is completely redundant and load-balancing at the same time, with a recommended steady-state of three APIC appliances forming the cluster.



The entire ACI system models everything as an object, and lays these objects out in what Cisco calls a "distributed Management Information Tree" or dMIT so that individual objects inherit properties (security privileges, attributes, etc.) from their parent objects. These objects are in turn exposed northbound to the rest of the world via the APIC through a number of means, including REST (XML/JSON) APIs, Graphical User Interface (GUI) or a command line shell that resembles a Linux BASH environment. Alternatively, Cisco also offers additional Software Development Kits (SDKs) for those that wish to develop applications to interact directly with the ACI policy model. At General Availability (GA), Cisco is shipping and supporting a Python SDK, but tells us that a Ruby variant and even a C# variant is in the works.

ACI Fabric: The ACI fabric is essentially a collection of physical and virtual devices that make up the network fabric, processing all data plane functions, such as lookups, forwarding, policy enforcement, etc. These devices may be providing forwarding services, such as switches and routers, and/or layer 4 through 7 network services, such as firewalls, load balancers, etc.

At the heart of the ACI fabric are Cisco's new flagship Nexus 9000 series data center switches, which are configured in a Spine-Leaf topology, providing scale-out connectivity, performance, resiliency and flexibility. At the time of GA, Cisco offers two variants of Leaf switches:

- Nexus 9396PX – 48 Ports of 1/10G SFP+ with an additional 12 Ports of 40G QSFP uplinks
- Nexus 93128TX – 96 Ports of 1/10G Base-T with an additional 8 Ports of 40G QSFP uplinks

Cisco also offers the following two variants of Spine switches:

- Nexus 9336PQ – 36 Ports of 40G QSFP links to the Leaf switches
- Nexus 9508 – Up to 288 Ports of 40G QSFP links to the Leaf switches

Cisco has also committed to supporting additional form factors of both Spine and Leaf switches, including 1RU Leaf switches, as well as both smaller (4-slot Nexus 9504) and larger (16-slot Nexus 9516) Spine switches in the near future.

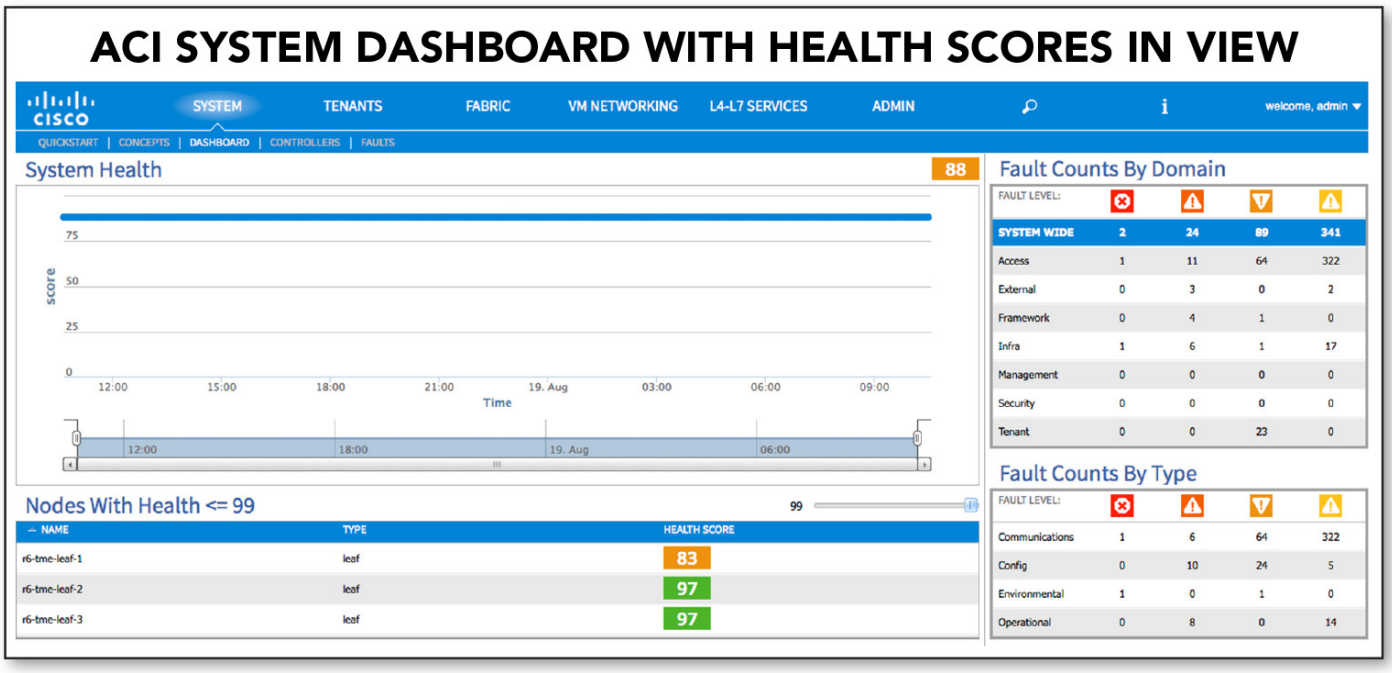
From a network design standpoint, all devices connect to the leaf switches. The only devices that connect into the Spine switches are other leaf switches. Under the covers, Cisco runs IPv4 routing across the fabric as its "underlay" protocol and leverages a hardware Virtual eXtensible LAN (VXLAN) "overlay" encapsulation to provide any-to-any L2/L3 bridging and routing across the entire ACI fabric.

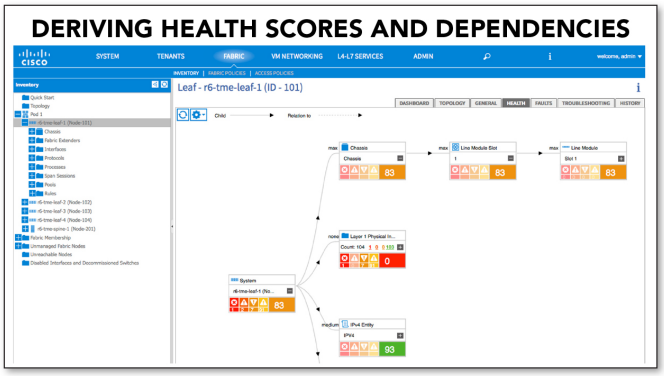
An important note is that the ACI fabric is also able to control any Virtual Switches (vSwitches) residing across different hypervisors with which it integrates—be it VMware via vCenter, Microsoft via SCVMM (System Center Virtual Machine Manager) running Windows Server 2012 R2 or OVS via OpenStack (supporting Ubuntu and RedHat variants). Also, the ACI fabric is able to control network services through plugins Cisco calls "Device Packages," and allows the APIC to facilitate the orchestration, automation and chaining of L4-7 services; polices are extended down to these network services so that administrators do not need to manage these devices separately. Hence, the ACI fabric extends beyond Cisco's Nexus 9000 platforms, but also encompasses all other services with which it integrates.

Operationalizing ACI: Health Scores

What's fundamental to Cisco's approach to ACI is that with this general release, it's offering a set of tools that will help data center administrators operationalize a Cisco ACI deployment. One of these tools is called Health Scores. In addition to providing a streamlined way to provision the ACI fabric, Cisco wanted to add a lot of value to day-two operations; that is day-to-day management and operations. After the ACI is configured and set-up, administrators need to monitor and understand how well the fabric is tracking to expectations, or how the fabric is behaving, or misbehaving. Enter "health scores," which provide different administrators with an elegant way to drill down to very discreet measurements of health trouble spots. As mentioned above, since all devices within the ACI fabric are essentially objects, ACI can measure and assign a health score to most objects since these objects are laid out in an object tree. Health scores can also be "rolled-up" the tree, so that an aggregate per-tenant score, or an entire fabric score can be reported and collected. It's a fractal model that provides a high level score and lets the administrator drill down to devices and components or functions on devices, such as a port or even at the protocol level.

For example, the entire ACI fabric may have a 99% health score, which is very good, but then changes as something within the fabric degrades. It could be errors on ports, a port gone down, or a VM on an ESX host measuring very high CPU cycle consumption. As faults occur, they start triggering off events, which lead to a degradation in health scores of discrete objects and a visual clue to administrators. These scores are rolled up the tree, and eventually the entire fabric health score will start decreasing as underlying object scores decrease. Those who support and operationalize networks in data centers understand it's very difficult to triage down to a problem's source without having good context. The health scores provide context and a grading system with the best score being 100.





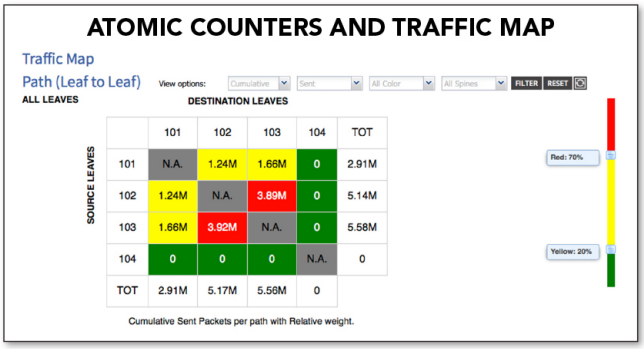
Some NetOps personnel may think that they can create a similar system to health score by executing scripts to automate the collection and processing of regular network statistics, but this is a tall order. True, one can hide a lot of complexity of existing networking through scripts, but imagine developing scripts on every individual operational aspect of the network. It's not only difficult requiring serious DevOps skillsets; it's not scalable across a large environment too. What Cisco did with ACI is even before creating the hardware and software in the system, it developed the object oriented data model for ACI to support these functions. This model not only supports the provisioning and deletion when administrators create and remove objects, but it also delivers on-going information of individual objects' attributes, allowing administrators to monitor object status. It's more scalable, and should add tremendous value, especially in OpEx savings plus speeding up time to resolution when issues occur.

Visibility and Troubleshooting: Atomic Counters

Another important operational feature is what Cisco calls "atomic counters"; a troubleshooting and analytical tool. Atomic counters are exposed in a few ways, but essentially Cisco has included atomic counters as a specific functionality in its hardware to avoid a performance penalty when enabled. Cisco has also committed that atomic counters would also be extended to Cisco's software switch—the Application Virtual Switch (AVS) and potentially exist in other open software switches too. So what do atomic counters do? Essentially their function is very simple, but extremely valuable. Atomic counters count every packet that enters and leaves the fabric but they also provide contextualization into the packet count.

Traditionally, it's been very difficult to gain visibility into the motion of traffic flows within networks. The ACI fabric seeks to change that with atomic counters that track or trace flows as they ingress and egress the fabric around and within the policy groupings mentioned above. Packets entering the ACI fabric are tagged at the first ingress point on the fabric, and these tags are stripped at egress. These tagged packets are the source of atomic counters' flow tracing and counting. With atomic counters, administrators will know very quickly whether or not the fabric has dropped packets for a given ingress/egress leaf pair (what Cisco calls a "path"), or even between a given ingress/egress uplink port pairs (what Cisco calls a "trail"). This information provides a way for administrators to track packet/flow information end-to-end within the fabric and to scope those flows between sources and destinations.

Cisco has created a neat graphic to display atomic counters' data collection in the form a heat or traffic map to show overall utilization percentages of flows between different paths and trails. Different utilizations are color coded to provide areas with high/medium/low utilization levels. This information is helpful to understanding if there are packet drops in the fabric and as a planning tool to understand where to place additional workload onto the fabric.



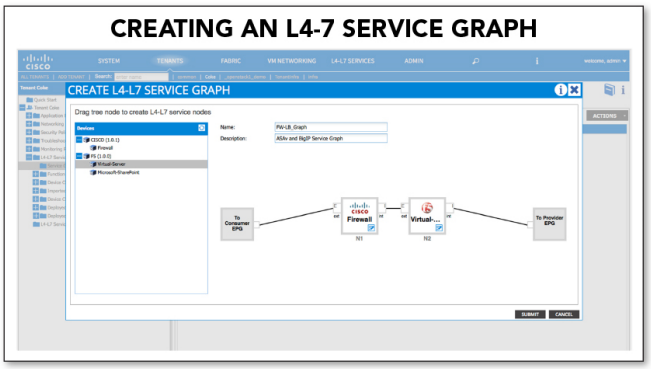
One of the biggest challenges in diagnosing network problems occurs when NetOps has to correlate information from multiple different devices and management systems. It's very common for NetOps personnel to have to interact with different devices, running a series of CLI commands such as "show ip arp," "show mac-address"…, and then attempt to trace all of this information, usually on a sheet of paper to understand the network path. The drill down capability of atomic counters allows operations staff to bypass this tedious and time-consuming process and go straight to the problem's source. Atomic counters can be used in these scenarios to assist in end-to-end system troubleshooting, allowing administrators to filter on specific tenants, EPGs, endpoints, etc., they are interested in, and count only those packets that match the criteria specified.

Attaching Applications to Network Services

Of high interest on infrastructure administrators' minds is how to attach Application Network Profiles (ANPs) to network services where L4-7 network services may be instantiated as a physical appliance, virtualized form factors or a combination of both. ACI provides multiple ways to address this design problem, while minimizing the number of management points down to one. To attach a L4-7 network service to an ANP, the administrator does not have to interact with different device interfaces or management systems. As L4-7 services are modeled as part of the ACI fabric, Cisco basically architected those services inside the same group-based policy model as discussed above. An

additional huge benefit to the ACI fabric model of attaching L4-7 services to ANPs is that L4-7 services can be location independent; that is, these services can be attached anywhere in the fabric so that when the administrator attaches the service function to the ANP, the fabric figures out automatically where they are located and provisions any corresponding encapsulations to those service nodes to automate data path forwarding.

Cisco models these L4-7 service functions as a Service Graph, and may contain one or more service functions (Firewall, Load Balancer, etc.). These Service Graphs can then be stitched into the definition of the ANP to reflect the desired ANP behavior.



For example, by associating L4-7 Service Graphs to the ANP, the administrator or security auditor can understand, at a high level, all traffic matching on HTTP/S destined to the Web EPG in the ACI fabric needs to first pass through a particular Firewall Service Graph. Or before a flow enters the back-end database EPG, it needs to pass through a load balancing Service Graph. The Cisco ACI approach to ANP attachment to network services mitigates one of the largest time sinks in the IT service delivery chain, where it takes minutes to spin up a VM but weeks or months to configure the network and L4-7 network services. At the time of writing, Cisco ACI provides integration with Cisco ASA and ASAv firewalls plus Citrix and F5 Load Balancers. Device packages for each of these service nodes are available on the respective vendors' sites.

Cisco has committed to working with over a dozen L4-7 services vendors for delivery of additional device packages. For the most updated list of ACI ecosystem partners, refer to Cisco's ACI page at http://www.cisco.com/go/aci

Service Chaining and Replication

For integrating L4-7 services, there are two basic approaches: leverage physical network services and divide them up logically into multiple contexts for each tenant, or dedicate individual virtual services per tenant.

ACI is able to support both approaches as most IT organizations and cloud providers have needs for both. For example, in most enterprises, before traffic enters the enterprise application definition, it must pass through a perimeter firewall. This firewall function is typically very well controlled and highly secured, almost like an air gap in spacecraft or submarines. But in recent years, it's been qualified that one doesn't need an actual, physical air gap, but most SecOps want a physical device that stands as that policy control point. In this scenario, ACI is able to integrate Cisco and other vendors' firewall platforms, as they should be able to attach into the ACI fabric. Organizations that have more stringent security controls prefer this architectural model as they don't have as much trust for virtualized firewalls to guard against threats at the DMZ. They are most comfortable leveraging their existing Cisco ASA, Check Point firewall, Juniper SRX, or Palo Alto Networks firewalls. APIC allows these IT organizations to leverage their existing physical firewall investment by plugging them directly into the ACI fabric, thus incorporating its functionality and provision policies via APIC.

There is growing interest in locking down or segmenting communication between different tiers of applications; this is where the ACI policy model contributes from a scale and performance perspective. Since policies are defined through the ANP, such policies are rendered throughout the infrastructure and enforced at the first entry point into the ACI fabric, providing distributed firewall functionality across all ANPs.

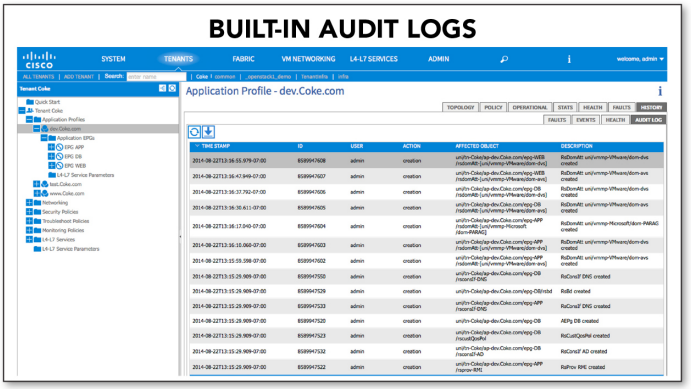
Dedicated individual virtual services per tenant are supported within ACI much like physical form factor appliances. Cloud service providers have a strong desire to set up and dedicate an instance of a virtual firewall, load balancer, etc., for every tenant it hosts, so it may be controlled and individually managed by each tenant. Many IT organizations apply the tenant concept to individual business units, for example. However, with virtual network services, there is an additional necessary step to deploy the virtual firewall or load balancer, which is to provide appropriate version control, and install the correct licenses. This is commonly known as Virtual Services Lifecycle management. Cisco partners with Embrane to incorporate this functionality in its ACI offering.

A Huge Leap forward for IT Systems' Auditors

A major benefit to the explicit definition of EPGs and "contracts" is that it provides administrators and IT auditors the ability to easily audit what policy has been instantiated versus what the original intent of the application owner was/is. It's no secret that systems policy documentation is sparse at best in most IT organizations, and when it does exist, maintaining accuracy and updating such documents becomes a huge IT administrator overhead. Additionally, the original applications or platform owner may have moved on to different roles or have left the company altogether, leaving a significant knowledge gap. Those who have had to re-derive the intent of the application/platform owner from retrieving and reviewing switch/router/firewall/load-balancer

configurations realize that it's a costly, daunting and time-consuming process.

This is a huge area where ACI plays an important role. Since ACI policies are expressed in higher-level abstracted terms, IT auditors are able to quickly understand the intent of the application owner simply by looking at the ANP. The auditor does not need to trace/correlate detailed network and services configuration files to understand the over-arching application policies. Additionally, Cisco has implemented a very detailed audit log for objects that are modified, indicating the timestamp, user, object and description of what was modified for complete traceability.



Multi-Hypervisor Tunneling and Interoperability

Fundamentally, ACI provides connectivity, but the means of connecting devices is changing as applications span both physical and virtual environments. Although there has been a steady increase in the migration from physical to virtual workloads, there is still the inevitable requirement that virtual workloads need to communicate with bare-metal hosted workloads. Furthermore, in the past year, there has been a huge increase in the interest to investigate container-based workloads to further optimize performance and reduce processing overhead. The network has always been an underlying normalization point for IT assets and computing models since all workloads leverage the network for connectivity. ACI seeks to become the new foundation in the normalization of these different workloads, that being in both connectivity and policy.

The space that needs normalization most today is in virtualized networking, with different hypervisor offerings providing different methods to manage virtual networks with support of various data plane encapsulations (VLAN, VXLAN, NVGRE, etc.). There is an increasing number of environments that are looking to deploy multi-hypervisor environments, and with this trend, companies need to look towards a holistic way to manage these disparate environments as well as their respective underlying encapsulations.

Cisco ACI provides direct integration with VMware's vCenter and OpenStack Icehouse release, running Ubuntu KVM with its GA release of software. Cisco has committed to support Microsoft's SCVMM, Microsoft AzurePack, and Red Hat KVM with OpenStack in the near future. By integrating multi-hypervisors with ACI, the APIC becomes the central point of management for both physical and virtual network policies, and the ACI fabric becomes a distributed encapsulation normalization point for multiple encapsulation types (VLAN, VXLAN, NVGRE), providing administrators the flexibility to terminate, interpret and remap different encapsulations into and amongst each other. These encapsulations are also orchestrated by the APIC so the network or VM administrator does not need to coordinate tag bindings. When packets enter the ACI fabric, these unique encapsulation tags are stripped off and are either re-attached at egress or translated to the destination hypervisor encapsulation scheme providing multi-hypervisor connectivity.

Integration with these Virtual Machine Managers (VMMs) allows the administrator to treat physical and virtual workloads exactly the same; by leveraging the ACI policy model. When administrators create application tiers, security zones or anything that binds to an EPG, these groups are essentially pushed out to the underlaying physical and virtual devices. In VMWare's vCenter, the APIC pushes EPGs out as VMWare port groups. In Microsoft's SCVMM, the APIC pushes EPGs out as VM Networks, and with OpenStack, APIC pushes EPGs as simple networks.

As an example, consider a VMWare ESX Hypervisor that's using VXLAN; it tags all packets via VXLAN, but it needs to communicate to two other ESX Hypervisors that use VLAN encapsulation. The ACI fabric performs VLAN translation, or VXLAN-to-VLAN bridging and routing, so these packets can transcend across subnets. In short, ACI provides full VLAN, VXLAN termination, normalization and routing functions at hardware performance.

Host or Network Approach to Virtual Tunneling Schemas Normalization

ACI provides a different architectural approach than hypervisor-only networking. In the hypervisor-only approach, network functions are implemented in the hypervisor. This starts with the tagging and policy enforcement mechanisms in the hypervisor, providing end-to-end knowledge of the virtual network at the hypervisor-level. In this model, every host that is tunneled to—that is, the tunnel endpoints—needs to be of the same vertical stack, such as VMWare, Microsoft or whatever virtual tunneling schemas are being used. The virtual tunneling schemas need to be coordinated across every other hypervisor host in the connectivity domain. This means that essentially workloads need to be virtualized and paired with the exact same hypervisor as well. There is little or no interoperability between hypervisor management systems that allows a mixing and matching of encapsulations and policies. Further, to connect to bare-metal (non-virtualized) servers, for example, a physical switch in the

network needs to understand that same virtual tunneling schemas, and requires deep integration with the hypervisor management systems so their encapsulations and policies can be coordinated/orchestrated.

A further challenge for production deployments is that data center administrators now need to test and validate not only the physical underlying fabric (the "underlay"), but they would then need to leverage another set of tools to validate the virtual networks (the "overlay"), essentially doubling the amount of qualification time it takes to bring the overall network infrastructure into a production-ready deployment.

Rather than driving the coordination at the host level, ACI uses the network to coordinate virtual tunneling schemas, thus providing normalization at every leaf node. As network nodes are the normalization point in ACI, it provides full connectivity and policies for all devices, be it physical, virtual or containers that plug in to the network. To operationalize the ACI fabric into a production-ready deployment, the data center administrator only has to test and validate the ACI fabric, as it combines both the underlay and overlay into the same plane, saving much time in qualifying the end-to-end solution.

Therefore, the choice most architects are confronted with now is this: 1) leverage the network as a normalization point for both connectivity and policy, and qualify the physical and virtual network together, 2) virtualize everything and mandate that every host run exactly the same hypervisor across the entire data center and double the amount of qualification time, and/or 3) run multiple overlay networks that don't interoperate between hypervisors and/or bare-metal servers, adding the appropriate qualification cycles.

In the ACI model, applications can span Microsoft Hyper-V, VMWare ESX and Ubuntu/RedHat KVM as well as bare-metal servers. In this model, part of a web application can be hosted on ESX running VXLAN, the application can be hosted on Hyper-V with its databases on KVM and bare metal with connectivity, and policies provided to all through a single point of management. If there is a desire for true choice and flexibility in data center infrastructure, then ACI is a great fit.

Conclusion

Cisco viewed the problems IT executives are experiencing with managing modern day data center infrastructure and developed a new approach that seeks to reduce operational cost, hasten IT delivery, span physical and virtual IT assets plus provide multi-hypervisor support and interoperability. Cisco kept the one true design principle of networking—to support all applications and workloads, and to be a general-purpose infrastructure that can be customized around connectivity via policy, automation and programmability. This new approach is Application Centric Infrastructure, and with it, Cisco has developed some of the deepest new thinking that the networking industry has seen in nearly 25 years. While it may take time for the industry to fully embrace ACI, what most will find is that Cisco is providing a new model of networking that poses valuable technological innovations that's much easier to control and manage than today's device-oriented networks. The result should be OpEx relief in the short term plus architecture for next-generation data center infrastructures that will be the basis to move the world economies forward another 25 years in the long term.

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.