Building a Real-World Data Center with Cisco Application Centric Infrastructure (ACI)

Customer Insights

Table of Contents

Executive Summary

Edison has followed the development and use of Cisco's Application Centric Infrastructure (ACI) over the past five years. Cisco ACI delivers an intent-based networking framework to enable agility in the datacenter. It captures higher-level business and user intent in the form of a policy and translates this intent into the network constructs necessary to dynamically provision the network, security, and infrastructure services.

While ACI is an innovative approach to the challenges of traditional networks from scale, operations and management, security, and agility perspectives, we were interested to see how the promise of new technological approach manifested themselves in the market and how it has been applied to solve business challenges.

The following paper provides an overview of traditional network challenges, a summary of how Cisco ACI solves these challenges, and most importantly, how actual customers feel about the product, their migration journey, and realization of benefits.

ACI has lived up to the promise of efficient network operations, enhanced security, increased scale and ultimately a more agile and flexible infrastructure. One significant takeaway is that potential customers need to look at what others have done in order to minimize effort and maximize benefit. To that end, a section on best practices is provided.

Challenges with Traditional Networks

As discussed previously, the customer-driven digital marketplace is placing high demands on resources, both IT infrastructure and personnel. The following specific challenges need to be overcome before IT can respond appropriately.

- **Not cloud ready or able** – traditional networks and architectures are not designed for today's hybrid IT or cloud environments. Specifically, they are not designed to be on-demand nor self-serve. As customers move to a hybrid IT environment, they want to ensure they have the same level of control and can maintain consistent policies across their end to end infrastructure.

- **Manually intensive** – without pervasive network operations automation, there is a reliance on restrictive manual configuration efforts. In many cases, configurations cannot be templated, forcing time-consuming, redevelopment. Additionally, these time consuming manual operations can result in human errors causing delay and further frustration, especially in an environment where resources are not necessarily scaling accordingly with network scale and complexity.

- **Not application centric** – traditional network infrastructure does not support an intelligent architecture designed specifically to respond to the needs of the applications which in turn drive the business intent. Specifically, the business owners and their application developers need instant access to network resources and ultimately want to deploy their applications in a simple and timely manner. They need an agile, highly available network that can deliver application requirements in an automated manner.

- **Restrictive Hub-Spoke Architecture** – traditional hub-and-spoke networks implicitly create silos which make it difficult to place any workload anywhere. Traditional hub-and-spoke architectures satisfied the requirements of a north-south traffic pattern, but do not support the traffic shift created by the need for data sharing from machine to machine (east-west traffic pattern).

- **Global Requirements** – since most traditional networks were designed to support local traffic, the migration towards global expansion and the need towards centralized management cannot be supported efficiently or cost-effectively. One of the biggest challenges customers face is the need to scale their network while maintaining a sound high availability and network reliability strategy. Eliminating a single fault domain and creating a simpler management environment is key to business continuity success.

- **No ROI** – most traditional networks are difficult to extend due to aging hardware limitations, and inability to support open APIs to easily integrate 3rd party products resulting in a near-zero return on investment.

- **Lack of Intent** – Lack of consistent policy in the network can cause unwanted experiences ranging from manual human errors, security breaches and network outages resulting in a loss of revenue and excessive frustration. With limited IT resources and a rapid application development environment, an intent-based network creates an operationally efficient network and accelerates time to market.

Why Customers Should Look at ACI?

Designed for the Cloud

Cisco ACI is specifically designed to support private, public and hybrid clouds or cloud-like networking infrastructure. OpenStack, Kubernetes, Bare-metal cloud providers, VMware vRealize, and Microsoft AzurePack are currently supported. Support for AWS, Microsoft Azure and Google Cloud are underway.

Cisco ACI comes out-of-the-box with an abstracted representation of network connectivity though the group-based policy model. This feature is extremely attractive in cloud deployments because a main requirement for such deployments is the capability to abstract the complexity of the network infrastructure so that it is not visible to the consumer of the cloud service

On-Demand Self-Service

Single-pane-of-glass, easy-to-use GUI, network automation and group-based policy profiles make it possible for network operations and less technical personnel to provision resources as needed.

Broad Network Access

Cisco ACI is designed to support access across the network from anywhere, regardless of where the computing facilities are located.

Resource Pooling

Cisco Application Policy Infrastructure Controller (APIC) API enables applications to directly connect with a secure, shared, high-performance resource pool that includes network, compute, and storage capabilities.

Rapid Elasticity

By separating infrastructure from the things that infrastructure supports (namely applications, security policies and IT services), enables organizations to spend more time managing group-based policies than the individual devices themselves. This makes it easy to quickly change network configurations or provision new services in step with business requirements.

Application-centric

Network that serves the needs of the application. Applications today behave differently, are highly virtualized, run on multiple hypervisors, and are more distributed than ever.[1] Applications require rapid and continuous delivery, shifting the communication needs within the data center. This new model is a transformation in data center design and scale, IT infrastructure management, provisioning, and consumption. Ease of provisioning and speed are now critical performance metrics for data center network infrastructure that supports physical, virtual, and cloud environments - without compromising scalability or security.

Network-centric vs Application-centric

Just to demonstrate the flexibility of Cisco ACI, the ACI policy model allows customers to use a network-centric (traditional) approach when moving to ACI.

Customers can gradually port their current network way of operating to the ACI fabric and then move to an application centric model over time.

In ACI, all endpoints connected to the fabric will belong to a group. These groups are defined in ACI as End Point Groups (EPGs).

In an application-centric approach, EPGs are application groups (webservers, appservers, etc.). Different application groups can belong to the same IP subnet or a single application group can belong to multiple subnets. The application group is to a degree decoupled from tradition network constructs.

In a network-centric approach, an EPG represents a VLAN and IP subnet (EPG=VLAN=Subnet) which matches the current network configurations. Both an application-centric approach and a network-centric approach can used simultaneously as this is just leveraging the flexibility of the abstracted policy model.

Automation Leads to Agility

Cisco ACI provides complete automated provisioning and management of the network infrastructure. Administrators can transparently add spine or leaf nodes to the Cisco ACI fabric without any configuration on the devices themselves. Provisioning of ecosystem partner solutions is also fully automated through the group-based policy model on Cisco Application Policy Infrastructure Controller (APIC), so the end user doesn't need to manually and

---

[1] https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-733800.html

individually manage those devices and systems. Day-two management of these devices and systems is also enabled through Cisco APIC.

Leaf-spine Architecture

With an ACI Fabric, administrators can transparently add spine or leaf nodes to the existing network without the need to physically configure the devices themselves.

Cross Geography Support

Multi-site – enables global connectivity with scale and seamless disaster recovery allowing for an active-active data center environment for applications.

Open with a Rich Ecosystem

Cisco ACI has a strong support ecosystem consisting of product design, partners and 3rd party application integration.

- Cisco gives you options by building on open APIs, open sources, open standards, and open ecosystems.

- Cisco works closely with 65+ ecosystem partners including F5, Citrix, and Fortinet. Support App model – users can write their own apps.

Foundation for Intent-Based Networking

As stated earlier, ACI provides the foundation for an intent-based network by enforcing intent in the form of policy across the network.

Companies Interviewed

Interviews were conducted with three of the first end-users of Cisco ACI. The first, Cisco's Global Infrastructure Services was picked as it demonstrates that Cisco uses its own products and services. The last two represent the first two Cisco ACI clients.

Cisco's Global Infrastructure Services

One of the first installations of ACI. A clear example of a company using its own products to support critical business practices, namely, "walk-the-talk". They worked very closely with ACI development teams as they implemented and used the product set so their improvements could be passed onto new clients as they started on their own migration paths. Global Infrastructure Services (GIS) is using ACI to enhance 25 datacenters representing 60K virtual/physical servers. As of October 2017, they were 95% completed. Edison interviewed one of the lead Principal Engineers in the Global Infrastructure Services team.

Pulsant

UK based, hybrid IT solutions and cloud hosting provider. Another early adopter. They were focused on the improving internal operational capabilities and customer service delivery. As of October 2017, they had deployed ACI in three of fifteen locations, two of which are their main cloud service data centers. Edison interviewed two people namely, Head of Connectivity and Network Operations.

Vecozo

Dutch based, healthcare administrative digital data exchange support. One of Cisco ACI's first commercial clients. They decided to implement ACI in conjunction with their new data center and focused on enhancing their disaster recovery capabilities. As of October 2017, they were 85% completed. Edison interviewed three people namely, Team Leader, ICT Architect and Senior System & Network Administrator.

Customer Drivers/Benefits/Results

To get a first-hand perspective from three different end-users of Cisco ACI, Edison interviewed key personnel. The results of those interviews are presented below.

Each of the companies interviewed provided their own specific perspectives on drivers or why they decided to explore and implement ACI, and what benefits were realized.

Efficient Network Operations

One of the key reasons for migrating to Cisco ACI, was to simplify network operations so tasks could be easily repeatable, not require in-depth technical skills to perform common tasks, make it possible to manage a growing network without increasing personnel resources, and reduce network outages.

Cisco – tasks become easier, less effort, less issues, faster response

- "A lot of tasks become easier when it came to performing basic operations".

- "Using ACI, we have seen reductions in the provisioning effort - we need less people and/or less time to build things on ACI. You can build automation software on top of ACI".

- "The number of issues associated with provisioning were significantly reduced using ACI. Outages were reduced (part of this was human error). You can credit it to ACI, but some of it was due to the software Cisco built on top of ACI to make sure this was done with high integrity".

- "ACI added a programmable network that could more easily fit into our cloud and orchestration network."

- "We were able to build scripts for application developers so they could deploy applications faster on the network".

Pulsant – central control, automation enabled, self-checking changes, simple to use

- "ACI delivers a single Fabric to do it all. From an operational point of view, we went from needing to manage 100's of switches individually; to one single Fabric that collapses everything, virtual and physical workloads, together in a secure way. Incredible".

- "Now, every single solution on the market has automation. But I always put emphasis on something that is called simple-automation vs. complicated-automation. With ACI all you need to do is ask. It's an intent-based kind of infrastructure".

- "Once you deliver information or your intent to ACI double checks it for you. If you're not overwriting configuration that already existed, it then pushes it into the switches. Then the switches do the same thing. From a code point of view that's simplified as well. If you want to automate your data center, and if you don't have a huge amount of experience in scripting, ACI is a perfect way to introduce your infrastructure engineering teams to safe automation".

- "After you've done the physical racking and stacking, you can also use a new switch within minutes, just by using existing policies, adding a switch to the Fabric takes no time at all".

- "In terms of deploying customers, we use the RESTful API, and we have a bunch of Python scripts that we've written for our standard products. So, whether it's some transit we're delivering to the cloud, or if it's some transit we deliver to just a couple of physical ports for a colocation customer, we can provision that now within seconds as opposed to minutes, due to automation. This is also true for setting up new customers".

- "ACI opened the door because it's simple, because it has a GUI. Suddenly provisioning is not necessarily performed by network engineers. Others don't understand the technical details, they know what IP is, they don't understand EGP, they don't understand ISA. They don't have to understand it. All they need to do, is work on the high-level abstraction. And that allowed us to [reduce] costs on new staff members; new senior staff members".

Vecozo – reduced provisioning time, reduced operational effort

- "Minimized technical issues associated with moving from one data center to another, timing, storage, etc. ".

- "It used to take 2-3 weeks for to setup a new environment. Even though we aren't fully automated on the network, it now takes a couple of days".

- "We have two admins. Now we can do a bit of it with a smaller team. Previously, we had to create VLAN, configure firewalls, internet, manually. We now have a tool where a colleague can create contracts by themselves."

- "The scope of work became more realistic for network employees. With the use of UCS director, we want to be able to press one button and create a three-tier application topology with the front-backend and database server. With the use of UCS director, ACI and some storage on the back, it's a lot easier to do the work. From requiring Network Specialists for all tasks to general tasks that can be performed by other disciplines such as Storage Administrators".

Enhanced Security

Security is a critical function in any network. The ability to microsegment coupled with other functions and features makes Cisco ACI very secure.

Cisco – interface with other security approaches, easy to pinpoint vulnerabilities

- "ACI is not the only thing that we use for security. Yes, there is improvement. Takes a lot of focus to secure our business-critical apps with high-confidential info and apps that are internet facing – a fair amount of applications. More and more attacks are coming from the inside.

- Data modeling, tenancy, is closer to how application people think, and is closer to how we can start building security in our data center network.

- Previously, we were restricted by our network constructs. It is very easy for us to do now, using API's, where we query our systems and know exactly what part of our network is carved out for which applications. These are the security mechanisms that we built around. The way that ACI has modeled itself is beyond traditional networking and we think that it can be used from both cloud and security perspectives."

Vecozo – improved microsegmentation features

- "Previous infrastructure was microsegmented, and ACI enabled us to do it in a more standardized manner so it would be less of an effort".

Pulsant – role-based network access, open network

- "From a cloud and storage point of view we have, 3 tiers, cloud and storage. We enabled them safe access to the APIC. So, some engineers have read only access where they can troubleshoot ACI, cloud problems for example, before escalating to network operations, again saving operational time.

- "Solution architects have read only access, so that they are able to analyze the customer's solution while advising them on expanding their solutions. So again, it's openness. I refer to it as network openness."

Increased Flexibility, Scalability

Pulsant – virtual/physical workload parity, single pane-of-glass management

- "In the past we wondered, "How are we connecting our virtual workloads and physical workloads?" ACI collapses everything up to a level, everything has an endpoint in ACI, therefore we don't have those problems completely at this stage".

- "You have a single screen – health and logical connections display".

Vecozo – reduced operational effort, highly scalable network

- "Amount of effort we had to put into new services was increasing over time. ACI would enable us to do this with much less effort. Because of the "Spine-and-Leaf" architecture, the new network is highly scalable - we now have something that can carry us forward five years or more".

Improved, Measureable ROI

Unlike many projects of this scope, Cisco ACI project ROI was measureable and, on average, met initial expectations.

Cisco – realized anticipated savings, more to come

- "ROI. We have quantified now. We anticipated savings when we proposed ACI for CIO. Was it worth the time we invested in ACI? We have revisited the anticipated measures. In some cases, they were better and others not as much. There are other areas where we need to wait a bit longer before we realize anticipated savings".

Simplified Cloud Integration

Cisco ACI was built for the cloud. As such it easily integrates with all cloud types, public, private, hybrid) as well as many of the popular technologies, i.e., OpenStack, Kubernetes, VMware vRealize, and Microsoft AzurePack. Others (AWS, Azure and Google Cloud Platform) will be released soon.

Pulsant – integration with cloud service providers

- "Integration with the cloud. We are using VMware now, but are investigating OpenStack. We are now integrating with Azure and AWS and all the other major players in the market as well and our ACI network will help make the integration much easier".

Best Practices

As the interviews were conducted, several best-practices emerged. They are presented below.

- **Fully understand Cisco ACI and IBN approach BEFORE acquisition.** It is critical to fully understand the scope of this effort and the impact on people, process and technology before making a commitment. One of the key reasons a project fails is due to unrealized expectations. It is critical that all participants from stakeholders to administrators to users understand the effort and impact of this decision.

  We include IBN here as it is a logical next step in infrastructure development and as such the end-user should be aware of its capabilities and how it may improve the overall network infrastructure and its operation. .

- **Expand implementation team to include application developers, network and cloud personnel.** Application-centric mode adoption requires either collaboration with application teams or leveraging cloud orchestrators – this unlocks the complete value of ACI.

- **Train. Train. Train.** Invest in learning – ACI bring in some new concepts, while building upon well-known network constructs. There have been use cases where the end-user learns something towards the end of implementation that might have either helped them to do something better or to take advantage of new functions/features without the need to start over.

- **Expedite Migration by Initially Using Network-Centric Approach** – As stated previously, customers can configure their new network using the same approach, network-centric, they are using now. This can speed up the migration, allow customers to take advantage of what ACI has to offer and then, when they are more comfortable, move, expand or migrate parts of their network using the application-centric approach.

Summary and Recommendations

This paper focuses on Cisco ACI, the need for it, how it addresses those needs and most importantly customer perspectives on what motivated them to acquire it and the realized benefits.

Why ACI?

Very simply, our conclusions based on customer interactions, Cisco ACI delivers the most secure, open, and comprehensive Software-Defined Networking (SDN) data center solution. It radically simplifies, optimizes, and accelerates infrastructure deployment and governance, and expedites the application deployment lifecycle. It supports a hybrid IT infrastructure: on premise and multi-cloud environments.

What makes it unique is its architecture. It was designed to support an application-centric environment so it can easily respond to the changing demands of today's data center to support physical, virtual and container environments simultaneously without compromising scalability or security.

ACI is built on a leaf-and-spine network architecture, supports any workload, anywhere. Management is software based so the devices are not affected when there is a need to expand or reconfigure.

Cisco ACI has a strong support ecosystem (65+ partners) building on open APIs, open sources and open standards.

Customer Perspectives

An in-depth customer perspective of the effort to evaluate, implement and benefit realization was obtained by interviewing three of the first end-users of Cisco ACI. The first, Cisco's Global Infrastructure Services was picked as it demonstrates that Cisco uses its own products and services. The last two represent the first two Cisco ACI clients.

Efficient Network Operations

- Tasks become easier, less effort, less issues, faster response

- Central control, automation enabled, self-checking changes, simple to use

- Reduced provisioning time, reduced operational effort

Enhanced Security

- Whitelist policy driving a zero-trust architecture

- Improved multi-tenant security with microsegmentation

- Security across the Cloud

- Industry compliance with certification for Federal Government, Retail, Finance and Healthcare.

Increased Flexibility, Scaling

- Integrated virtual/physical network with a single pane-of-glass management

- Hypervisor independent solution supporting any workload type: physical bare-metal servers, virtual machines and/or containers.

- Reduced operational effort through automation delivering a highly scalable network

Improved Measureable ROI

- Elastic scale and growth through open APIs providing seamless integration with 3rd party vendor solutions.

Simplified Cloud Integration

- Integration with cloud service providers

Cross Geographical Support

- Improved disaster recovery, improved geographical support

Best Practices

As a part of the interview process, best practices were identified and recorded. Some of the more notable are:

- Fully understand Cisco ACI/IBN capabilities before beginning to build the new infrastructure. This enables the end-user to maximize the benefits using Cisco ACI.

- Involve multiple groups in the development and implementation. Include, but not limited to, application teams and/or cloud orchestrators.

- Training, training, training. Cisco ACI is built on unique architecture that requires a novel approach to network design and operation.

Recommendations

Adopting Cisco ACI is like taking a giant leap forward. By doing so you are committing to a new approach, new technology, changes in process, changes in expectations, and a significant amount of initial effort.

However, based on a review of the approach, technology and realized customer benefits it proved to be worthwhile as it equipped the organization with an infrastructure that can meet current and future business requirements, namely growth, scale, and change effectively and efficiently.

Another significant attribute of ACI is its foundational role in Cisco's Intent-Based Networking strategy and provides a path to build on Cisco's innovative roadmap and solutions going forward. This not only protects and enhances the investment in ACI, it also assures that the high-level of business-value will be maintained.

Edison highly recommends that organizations that are looking to compete effectively now and in the future in this digital economy need to seriously consider Cisco ACI.