White Paper

Organizational Impact of Cisco Application Centric Infrastructure on IT Departments

What You Will Learn

Cisco® Application Centric Infrastructure (ACI) is an innovative and open architecture for data center networking and security that delivers significant value through increased agility, automation, security, and workload mobility and lower total cost of ownership (TCO). ACI supports flexible operating models within an IT department and enables customers to gain immediate value from ACI deployments without requiring changes to organizational structure, processes, or skill sets to operationalize ACI in the environment.

This document describes a variety of operating models for IT departments using ACI. It also describes the associated benefits and organizational impact of ACI as derived from Cisco's experience with several ACI customers as well as Cisco's internal IT ACI deployment.

State of the Data Center

User demands and changing application requirements require a different approach that is simple, more agile, and application centric. Applications today behave differently, are highly virtualized, run on multiple hypervisors, and are more distributed than ever.

Developed differently, these 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.

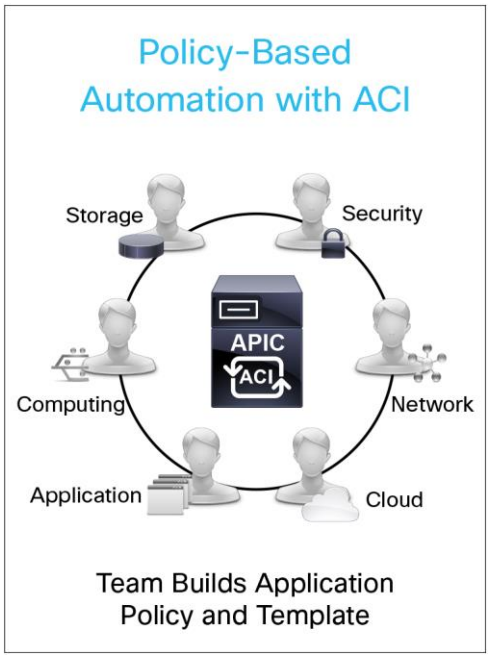
Today's solutions lack an application-centric approach. The use of virtual overlays on top of physical layers has increased complexity by adding policies, services, and devices. Traditional software-define networking (SDN) solutions are network centric and based on constructs that replicate networking functions that already exist.

Cisco ACI Vision

Cisco ACI for the data center is an innovative, highly secure architecture that delivers centralized application-based policy automation, management, and visibility for physical and virtual networks.

A critical architectural component of ACI is the Cisco Application Policy Infrastructure Controller (APIC). This component provides a single touchpoint for all configuration, management, and operational tasks, including policy definition and health monitoring. By providing a common framework, it unifies applications, networking, cloud, and security teams in the definition of application requirements (Figure 1).

Figure 1. IT Teams Collaborate to Define Application-Centric Policy



With traditional IT departments are under pressure to be more agile and to provide better outcomes to the business, a new model for operations has emerged: Fast IT. Cisco ACI can enable Fast IT by providing a common policy-based model across the entire ACI-ready infrastructure, drastically reducing costs and complexity.

Operating Models for IT Department with Cisco ACI

Cisco ACI supports an evolutionary approach to the transformation of an organization's IT operating model to support future cloud and DevOps deployments. The organization can gain immediate value from ACI without the need to make changes to its current IT operating model.

This section outlines three main operating models for an IT department using ACI and presents use cases and their associated organizational impact and benefits. Note that the operating models are not ACI technology modes of operation, but are operating models for an IT department using ACI. This discussion is based on Cisco's experience with ACI customers as well as Cisco's internal IT deployment.

Model 1: Network-Centric ACI Deployment

This operating model for an organization with ACI doesn't require any changes to the organization structure or processes. In this scenario, customers deploy ACI fabric as their next-generation data center network to enable a 10- and 40-Gbps access and aggregation network. The network is optimized for east-west data center traffic to support virtualized, dynamic environments as well as nonvirtualized workloads. Network teams can start managing the ACI fabric using the built-in APIC GUI and command-line interface (CLI) options without API-based automation. They can also use the library of Python scripts from GitHub even without knowing Python and can use the community-developed commands.

This mode of ACI deployment doesn't involve any changes to the IT organization structure or processes. It does not require new roles other than incremental training on ACI technology innovations for the network engineering and operations teams. Network engineers can continue to manually configure their ACI fabric using the APIC GUI and CLI. VLANs and access control lists (ACLs) can be directly mapped to the ACI model with endpoint groups (EPGs) and contracts. Network operations teams can continue to use existing network management tools (syslog, Simple Network Management Protocol [SNMP], etc.) to manage the network in conjunction with the option to use APIC to supplement the existing operation monitoring tools. The only difference is that configuration and monitoring operations are now performed centrally on the APIC instead of using the less scalable and more error-prone device-by-device approach that most networks rely on today

Benefits of this mode of operation include:

- No change to existing IT department structure or processes
- Next-generation high-speed 10- and 40-Gbps data center network with quality of service (QoS) optimized for data center east-west application traffic patterns and heterogeneous (virtualized and bare-metal) environments
- Workload mobility and flexibility, with placement of computing and storage resources anywhere in the data center
- Capability to manage the fabric as a whole instead of using device-centric operations
- Capability to monitor the network as a whole using APIC in addition to the existing operation monitoring tools; APIC offers new monitoring and troubleshooting tools such as health scores and atomic counters
- Lower TCO and a common network that can be shared securely across multiple tenants in the data center
- Centralized auditing of configuration changes

Model 2: Network Automation with Cisco ACI

This operating model for an IT department with ACI is suited for customers who want to automate their network provisioning for specific use cases such as complex enterprise applications or big data without significantly changing their operating model for IT. The organizational impact in terms of organizational changes is minimal in this mode of ACI deployment and doesn't require changes to organization structures or the addition of new roles. Existing IT staff can simply acquire and develop incremental skills in the area of network programming, using Python or Representational State Transfer (REST) APIs for example.

That new skill set quickly enhances the efficiency of existing teams, allowing them to automate network configuration tasks for specific target use cases. Common network tasks that can be automated using APIC APIs include creation of VLANs and subnets, configuration of interfaces, and definition of external connectivity. Using code-generation tools freely distributed by Cisco, even nonprogrammers can very quickly reap the benefits of network automation and start creating a library of automated tasks. In this mode of deployment, ACI policy objects can easily be mapped to existing network-centric constructs (for example, **EPG=VLAN**).

Benefits of this mode of operation include:

- No change to existing IT department structure or roles, and minimal change to IT processes
- Workload mobility and flexibility, with placement of computing and storage resources anywhere in the data center
- Capability to manage the fabric as a whole instead of using device-centric operations

- Capability to monitor the network as a whole using APIC in addition to the existing operation monitoring tools; APIC offers new monitoring and troubleshooting tools such as health scores and atomic counters
- Lower TCO and a common network that can be shared across multiple tenants in the data center
- Centralized auditing of configuration changes
- Reduced application downtime in the event of network-related changes
- Faster application deployment and improved efficiency for specific target use cases through network automation

Model 3: Policy-Based Management with Cisco ACI

This operating model for an IT department with ACI is targeted at customer use cases such as private clouds and development and operations (DevOps) in which a high degree of integrated automation (for example, using OpenStack) across computing, storage, network, security, and Layer 4 through 7 network services is required. For the private cloud use case, IT can offer self-service for end users to consume ACI resources through a portal so that those end users can request and provision their own service infrastructure on demand.

Customers who want to deploy ACI for private clouds can benefit from this mode of operation. Prior to ACI, customers may have already made some organization changes to better align IT with cloud initiatives. No additional ACI-specific changes are needed beyond the organizational changes that the IT department may need to make for its private cloud initiatives. Some of the organizational changes that customers have made to better align IT teams with private cloud initiatives are summarized here:

- Organization structure: Customers typically form a new cloud team within the IT environment to coordinate requirements for their private cloud initiatives across multiple IT teams, such as networking, storage, and computing teams. No significant changes are made to the existing network, computing, security, and storage teams.
- New roles and responsibilities: A cloud team is created that includes the following roles:
  - Architect: Evaluates business value, defines process changes, and develops strategic roadmap for IT over the next two to three years
  - Designer: Selects technologies for automation and designs application infrastructure
  - Engineer: Develops code and designs the GUI and portal
- Change management: Change management typically involves an approval process for network configuration changes, and several days can be needed to get the necessary approvals. In a private cloud environment, this process can become a bottleneck when the network provisioning for a tenant or application can be automated to complete the changes in a few minutes. To enable agility, organizations may need to make changes to the data center infrastructure change-management process. Those changes can help ensure that network configuration modifications for changes enabled by automation aren't slowed by the approval process.

Benefits of this mode of operation include:

- Workload mobility and flexibility, with placement of computing and storage resources anywhere in the data center
- Capability to manage the fabric as a whole instead of using device-centric operations
- Capability to monitor the network as a whole using APIC in addition to the existing operation monitoring tools; APIC offers new monitoring and troubleshooting tools such as health scores and atomic counters

- Lower TCO and a common network that can be shared across multiple tenants in the data center
- Reduced application downtime for network-related changes
- Rapid application deployment and agility through programmability and integrated automation
- Centralized auditing of configuration changes
- Enhanced data center security for east-west application traffic, with microsegmentation to contain threats and prevent threats from spreading laterally across tenants and applications inside the data center
- Direct visibility into the health of the application infrastructure, benefitting application owners
- Template-based configuration, which increases efficiency and enables self-service

Benefits and Impact of Operating Models

Table 1 summarizes the operating models for IT departments using ACI along with associated use cases and organizational impact on IT teams.

Table 1. Operating Models for IT Departments Using Cisco ACI

	Network-Centric ACI Deployment	Network Automation with ACI	Policy-Based Management with ACI
Target Use Cases	New data center network, virtualized environments, multitenancy, and 10- and 40-Gbps access and aggregation layers	Enterprise application deployment, big data, and development and testing automation	Private cloud and DevOps
Organizational Structure	No changes	No changes	Add cloud and DevOps teams; no changes to other existing IT teams
Organizational Process	No changes	Some changes to process to enable automated network provisioning	Process changes to enable agility for cloud and DevOps deployments
Organizational Roles and Responsibilities	No changes	No changes	No changes to current IT roles; add team roles for cloud (cloud architect, service designer, engineer, etc.)
Organizational Skills	No changes	Network teams augment their skills to enable network automation (for example, Python, scripting)	New skill sets for team roles; collaboration with other teams to gather application requirements; work with various teams to define and enforce policy

Conclusion

Cisco ACI allows organizations to employ flexible operating models for IT teams and quickly gain value from ACI deployments. IT departments can gain immediate value from ACI without the need for changes to their existing organizational structure or processes, and the IT department skill set and processes can evolve according to the organization's use cases. This document describes the main operating models for an IT department using ACI, based on ACI customer deployments. It also presents target use cases and their associated benefits and organizational impact.

For More Information

Refer to the Cisco ACI website: http://www.cisco.com/go/aci.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-733800-00 01/15