The bridge to possible

# Cisco Application Centric Infrastructure (Cisco ACI)

The bridge to possible

## Challenges networks face today

The pace of digital innovation is surging across the digital ecosystem in the post-pandemic era, resulting in a sharp expansion of applications and cloud usage. Experiences such as 8K ultra-high-definition video streaming, immersive Virtual Reality (VR) and Augmented Reality (AR) applications, gaming, self-driving vehicles, high-frequency stock trading, automation driven by AI/ML systems, IoT, and use cases with 5G networks are expected to be agile and secure by enterprises. In response, organizations are adopting software-defined networking frameworks in order to attain agility within the network across the data center and cloud and improve their business outcomes.

Today, networking is the foundation for modern applications, connecting microservices, functions, and data into mission-critical business services across a hybrid and multicloud world.

## Cisco's premier SDN solution

How does Cisco® Application Centric Infrastructure (Cisco ACI®) play into this networking continuum? Cisco ACI can operate with our Nexus® Dashboard Platform, enabling agility and resiliency in hybrid-cloud and multicloud environments. It captures higher-level business and user intent in the form of a policy and translates this policy into the network constructs necessary to dynamically provision the network, security, and infrastructure services.

Cisco ACI, the industry's most secure, open, and comprehensive Software-Defined Networking (SDN) solution, enables automation that accelerates infrastructure deployment and governance, simplifies management to easily move workloads across a multifabric and multicloud frameworks, and proactively secures against risk arising from anywhere. It radically simplifies, optimizes, and expedites the application deployment lifecycle.

Modern data centers are dynamic. IT operations must meet the expectations of quality-of-service business needs in a rapidly changing environment. Cisco ACI transforms IT operations from reactive to proactive with a highly intelligent set of software capabilities that analyze every component of the data center to ensure business intent, guarantee reliability, and identify performance issues in the network before they happen.

As applications have become more pervasive across the enterprise network, IT professionals are looking to build solutions for consistent policy and encryption from the campus to the cloud.

## Cisco ACI benefits

To keep up with the massive influx of data and the increased demands on the network for speed and agility, networking professionals are learning to broker, connect, build, and govern their networks not only in the data center, but also across a vast cloud landscape.

Cisco ACI was built to simplify the IT infrastructure and operations by automating the network, providing pervasive security, and helping accelerate businesses to move to a cloud or multicloud environment.

With Cisco ACI, customers can manage complexity, maximize business benefits, and deploy workloads in any location, small and large, on premises and remote locations, in private and public clouds, satellite data centers, and 5G-enabled telecom edges.

The main benefits of Cisco ACI include the following:

**Accelerate network operations**

Cisco ACI provides a flexible and yet highly available network that allows agile application deployment within a site, across sites, and across global data centers while removing the need for complex Data Center Interconnect (DCI) infrastructure.

- Empower the 400G to 800G evolution.
- Be provided with centralized network management and visibility, with full automation and real-time network health monitoring.
- Have seamless integration of underlay and overlay networks.
- Employ open northbound APIs to provide flexibility for DevOps teams and ecosystem partner integration.
- Use a common platform for managing physical and virtual environments.
- Automate IT workflows and have flexible application deployment.
- Expand network reach and extend mobility domains using standards-based extensions.

**Securely expand to multicloud**

- Employ a secure cloud-ready SDN solution.
- Create business continuity and provide disaster recovery.
- Get inherent security with a zero-trust allow list model and innovative features in policy enforcement, microsegmentation, and analytics.
- Be provided with integrated security with Cisco security products and ecosystem partners.
- Have a consistent security posture at scale across a multicloud environment.

**Deliver superior experience**

- Benefit from operational simplicity, with common policy, management, and operation models across application, network, and security resources.
- Use flexible deployment models.
- Be provided with single policy and seamless connectivity across any data center and public cloud.
- Employ container networking enabled by integration with OpenStack, OpenShift, Kubernetes, and Cisco UCS® Director.
- Have open APIs and a programmable SDN fabric, with 65+ ecosystem partners including Infrastructure as Code (IaC).
- Have the power to scale.

## Cisco Nexus Dashboard platform

Cisco Nexus Dashboard provides a single automation platform to access operational services and tools for the data center and network. You can deploy policy and connectivity automation, visibility and analytics tools, and traffic aggregation capability using the Cisco Nexus Dashboard platform. It becomes even more of a collaborative focal point with the inclusion of operations-critical, third-party applications and tools. The platform drives the adoption of cloud-native application practices, which provide the following benefits:

- Easy to use
  - Customizable role-based UI view to provide a focused view on network operators' use cases.
  - Single Sign-On (SSO) for a seamless user experience across operation services.
  - Single console for health monitoring and quick service turnup.
- Easy to scale
  - High availability, scale-out operations from a single dashboard.
  - Scale use cases, leveraging flexible deployment options.
  - Operations that span across on-premises, multicloud, and edge networks.
- Easy to maintain
  - Seamless integration and lifecycle management of operational services.
  - Onboarding and managing operational services across on-premises, cloud, and hybrid environments.
  - Single point of integration for critical third-party applications and tools.

## Cisco Nexus Dashboard visibility and analytics

Cisco Nexus Dashboard gives customers the ability to monitor and analyze their fabric in real time to identify anomalies, provide root-cause analysis and capacity planning, and accelerate troubleshooting. By tracking historical context, collecting and processing hardware and software telemetry data, and correlating customer designs with Cisco best-practices, customers can get excellent visibility and awareness of issues affecting their environment and take corrective actions.

## Cisco Nexus Dashboard policy and connectivity automation

Cisco Nexus Dashboard provides a single point of provisioning for multiple Cisco ACI fabrics operating in a coordinated way. When this solution is combined with the latest networking enhancements of Cisco ACI, organizations can manage extension network elements such as Virtual Routing and Forwarding (VRF) instances, bridge domains, and subnets across multiple fabrics. It enables centralized policy and security controls across geographically distributed fabrics and very large scaled-out fabrics with automation and operations from a common point, allowing for a global cloud-scale infrastructure.

## Cisco ACI building blocks

Cisco ACI and architectural solutions are built with the following building blocks:

- Cisco Application Policy Infrastructure Controller (APIC).
- Cisco Nexus 9000 Series spine and leaf switches for Cisco ACI.

## Cisco Application Policy Infrastructure Controller (APIC)

The infrastructure controller is the main architectural component of the Cisco ACI solution. It is the unified point of automation and management for the Cisco ACI fabric, policy enforcement, and health monitoring. The APIC appliance is a centralized, clustered controller that optimizes performance and unifies the operation of physical and virtual environments. The controller manages and operates a scalable multitenant Cisco ACI fabric.

The main features of the Cisco APIC include the following:

- Application-centric network policies.
- Data-model-based declarative provisioning.
- Application and topology monitoring and troubleshooting.

- Third-party integration Layer-4 through Layer-7 (L4-L7) services.
  - VMware vCenter.
  - Nutanix Prism and AHV.
  - Microsoft Hyper-V, Microsoft System Center Virtual Machine Manager (SCVMM), and Azure Pack.
  - Open vSwitch (OVS), OpenStack, and OpenShift.
  - Kubernetes.
- Image management (spine and leaf).
- Cisco ACI inventory and configuration.
- Implementation of a distributed framework across a cluster of appliances.
- Health scores for critically managed objects (tenants, application profiles, switches, etc).
- Fault, event, and performance management.

The controller framework enables broad ecosystem and industry interoperability with Cisco ACI. It enables interoperability between a Cisco ACI environment and management, orchestration, virtualization, and L4-L7 services from a broad range of vendors.

## Cisco Nexus 9000 Series spine and leaf switches for Cisco ACI

Cisco Nexus 9300 and 9500 series switches support Cisco ACI. Organizations can use them as spine or leaf switches to take full advantage of an automated, policy-based, systems-management approach.

Cisco Nexus 9000 Series Switches include modular and fixed 1 to 400 Gigabit Ethernet switch configurations that are designed to operate either in NX-OS mode for compatibility and consistency with the current Cisco Nexus switches (using Cisco NX-OS Software) or in ACI mode to take full advantage of Cisco ACI application-policy-based services and infrastructure automation features. This dual-function capability provides customers with investment protection and ease of migration to Cisco ACI through a software upgrade.

# Cisco ACI deployment models

Cisco ACI consists of the following architectural solutions:

- Virtual APIC (vAPIC) in AWS
- Virtual APIC (vAPIC) for VMware
- Cisco ACI Multi-Pod
- Cisco ACI physical remote leaf
- Cisco Mini ACI Fabric

## APIC deployment models

### Cisco Application Policy Infrastructure Controller (APIC) appliance

The Cisco Application Policy Infrastructure Controller (APIC) is the main architectural component of the Cisco ACI solution. It is the unified point of automation and management for the Cisco ACI fabric, policy enforcement, and health monitoring. The APIC appliance is a centralized, clustered controller that optimizes performance and unifies the operation of physical and virtual environments. The controller manages and operates a scalable multitenant Cisco ACI fabric.

### Virtual APIC (vAPIC)

For those ACI deployments where physical APIC appliances might be impractical, APIC can also run as a VM form factor in an existing ESXi/VMware footprint. Operators can take advantage of unused capacity CPU, memory, and storage on ESXi clusters while also leveraging well-known virtualization life-cycle management techniques such as VMware's VMotion and Dynamic Resource Scheduler to optimize APIC performance, availability, and serviceability. Also, vAPIC enables ACI deployments where rack-space is constrained, such as marine, hospitality, or ruggedized environments.

For customers desiring to operate their on-premises ACI deployments through the cloud, the Cisco Virtual APIC (vAPIC) can be deployed in AWS, enabling operators to benefit from cloud-based implementation. This approach offers advantages such as reduced power consumption, TCO, and the capability to leverage cloud-spend minimums.

**Cisco ACI Multi-Pod**

Cisco ACI Multi-Pod is part of the "single APIC cluster/single domain" family of solutions; a single APIC cluster is deployed to manage all the different ACI networks that are interconnected. These separate ACI networks are called "pods," and each of them looks like a regular two-tier, spine-leaf topology. The same APIC cluster can manage several pods, and, to increase the resiliency of the solution, the various controller nodes that make up the cluster can be deployed across different pods.

**Hybrid and multicloud**

IT organizations approach their multicloud strategy by breaking it down into three pieces:

- **First:** Take stock and make a plan across their teams and technologies. Optimize what they have, adopt new skills, and modernize to meet new requirements. Establish the connections, security, and processes to create a highway for rapid change and delivery of new services.
- **Second:** Extend the data center where it needs to go. IT can become the one-stop-shop for private and public resources and to make them secure, consistent, and seamless for their environment.
- **Third:** Optimize, because "good multicloud starts at home." For those workloads and data to land securely and efficiently on premises they need private and hybrid cloud platforms that offer self-service consumption and the ability to move workloads seamlessly from private cloud to public cloud and the edge.

**How Cisco ACI can help**

Cisco ACI occupies a unique position in a cloud ecosystem because clouds ultimately depend on the network that uses them. For cloud builders, we make complete automation with a software-defined physical infrastructure in ACI. ACI, as a multicloud software solution, puts people in control of their public and private cloud resources in a secure way using single pane of glass management. IT teams can easily connect and manage infrastructure anywhere, from core to edge.

**Expected outcomes:**

- **Increase value of IT team.** Data center infrastructure and operations teams become builders and brokers of services that can offer the right mix of performance, security, cost, location to line-of-business stakeholders, on premises in the core data center or at remote sites, or in the public cloud. Developers and application architects can operate with a consistent development and runtime environment whether on premises or in the cloud.
- **Accelerate change while protecting the business.** The connections, security, and processes are established to create the highway for rapid change and agile delivery of new services.
- **Multicloud continuity.** Infrastructure resources are managed at any location at any scale to support new initiatives in IoT and mobility, and AI/ML technology is taken out of the equation so that application deployment is driven by business needs and cost considerations, not by technology limitations.

**Cisco ACI remote leaf**

With Cisco ACI physical remote leaf, customers can place a regular leaf switch in a remote or satellite location and connect back to the spine switch in the main (on-premises) location and, in turn, extend Cisco ACI policy into the remote or satellite location. By doing so, customers can also take advantage of all the benefits of the physical remote leaf, from diverse interfaces to superior performance, and scale and built-in encryption.

# Cisco ACI example capabilities and uses

**Security through microsegmentation and zero-trust network policy model**

Reduce attack surfaces and enhance your network security with a zero-trust model, microsegmentation, line-rate encryption, continuous compliance with business rules, and ensuring network security policy.

**Business outcomes:**

- Visibility of network and security changes that meet compliance requirements.
- Reduction of risk.
- Increased availability.
- Reduction of security incidents and number of unplanned changes.

**Unified network management and operations**

Simplify your network and save time by using unified management and embedded tools for operations, enabling you to scale more efficiently while automation ensures consistency.

**Business outcomes:**

- One place to easily understand the data center's network, health, performance, redundancy, troubleshooting, and operational status.
- Reduction in time for provisioning, configuration, troubleshooting, and upgrades.
- Reduction in configuration errors.

**Private cloud networking**

Accelerate your business with a private-cloud-ready data center network that provides simple integrations with the most popular virtualization platforms to give you cloud-like agility internally.

**Business outcomes:**

- Agility to change network elements supporting applications, in lockstep with the application real-time lifecycle.
- Reduction in time for business applications to be delivered and deployed.
- Reduction in time for network move, add, change, and delete.

**Automation and integrations**

Optimize your network administration workflows by leveraging programmability with APIs and/or integration with ecosystem partners to save time, reduce errors, and accelerate your rate of change.

**Business outcomes:**

- Doing more with less by leveraging the enhanced capabilities of API automation and service insertion that drive operational efficiencies.
- Reduction in operational costs by automating routine tasks.
- More resource time for projects to advance the business.

**Geographic diversity and Business Continuity/Disaster Recovery (BC/DR)**

Protect your business by enabling workload portability between multiple data centers, ensuring always-on applications, simplifying migrations, and contributing to BC/DR plans.

**Business outcomes:**

- Application availability at all times, regardless of data-center maintenance, migration, capacity, or other service interruptions.
- Reduced risk of downtime.

**Public- and hybrid-cloud integration**

Accelerate your adoption of a multicloud environment while providing consistent network and security policies within the data center and in the public cloud.

**Business outcomes:**

- Enabling the business to gain agility from using the public cloud while reducing risk by uniformly applying network and security rules using the same toolset regardless of deployment.

- Time savings.
- Acceleration of time to market.
- Reduction in hybrid cloud connection errors.
- CapEx reduction.

## Popular Cisco ACI integrations

**Utilize Cisco Infrastructure-as-Code (IaC) integrated solutions with HashiCorp Terraform and Red Hat Ansible**

Infrastructure as Code (IaC) is an innovative approach to building application and software infrastructure by using code. IaC enables automated provisioning and management of the full technology stack by translating manual, repetitive tasks into reusable, robust, and distributable code. IaC relies on practices that have been successfully used for years in software development, such as versioning, automated testing, release tagging, continuous delivery, etc.

Cisco Data Center Network (DCN) IaC solutions cover integrations with common third-party tools from HashiCorp such as Terraform and Red Hat Ansible. These solutions enable customers to empower application services to define network and security requirements at the infrastructure layer in an automated and fully synchronized manner. With this approach, you can embrace a DevOps model by accelerating applications deployment and optimize network compliance in a safe and predictable manner.

**Benefits of IaC**

- Scalability and reliability.
- Automation and agility.
- Higher ROI and lower TCO.

**Cisco ACI and Cisco SD-WAN integration**

Cisco offers ACI and SD-WAN integration for branch offices (network edge). This is an integral component of customers' cloud journey, which requires secure, policy-driven interconnects between the data center and branch offices that are a cost-efficient alternative to provisioning dedicated connections. Through this integration, customers can now automate a WAN path selection between the branch office and the on-premises data center based on application policy.

For example, traffic from a stock trader in a branch office in Chicago can be automatically sent over the fastest possible WAN link to access the trading application hosted in a data center in New York, based on the application policies and SLAs configured.

**Cisco ACI and AppDynamics assurance integration**

Digital transformation is a complex team effort across business and IT, requiring end-to-end application management and awareness. AppDynamics® provides IT teams with the application-layer visibility and monitoring required in an intent-based architecture to validate that IT and business policies are being implemented across the network. Cisco ACI and AppDynamics integration provides dynamic correlation between application and network constructs. This combined solution provides high-quality application performance monitoring, a richer diagnostic capability for application and network performance, and faster root-cause analysis of problems, with fast triage, sent quickly to appropriate team members – for example, whether a given problem pertains to an application or to the network.

This integration does the following:

- Dynamically maps the application and service components to the Cisco ACI network elements, thus providing a shared view of the application and infrastructure across teams.
- Provides a dynamic view of application use in the infrastructure for the network operations team.
- Provides a cross-launch for application teams to correlate network and application fault and performance data.
- Baselines application health statuses in AppDynamics by correlating the Cisco ACI network's health and faults.

Customers are on a continuous quest to correlate application service-level management with infrastructure monitoring. This new integration will significantly reduce the time it takes to identify and troubleshoot end-to-end application performance issues.

**Cisco ACI and Cisco Campus (Cisco Catalyst and Cisco ISE)**

The combined solution of Cisco ACI and Cisco Campus (comprising Cisco ISE and Cisco Catalyst®) unifies the mapping of segmentation policies based on the user's security profile as they access resources within the data center and campus/branch. This enables security administrators to manage end-to-end, user-to-application segmentation seamlessly, using dynamic, human-readable group information. As a result, any unauthorized or suspicious access to resources and potential threats can quickly be controlled and remediated.

**Cisco ACI and Cisco SD-Access integration**

Hyper-distributed applications and highly mobile users, increased cybersecurity threats, and increased regulatory requirements make network segmentation a must for reducing risk and achieving better compliance. Policy integration between Cisco ACI and Cisco SD-Access allows the marrying of Cisco ACI's application-based microsegmentation in the data center with Cisco SD-Access's user-group-based segmentation across the campus and branch. This integration automates the mapping and enforcement of segmentation policy based on the user's security profile as they access resources within the data center. It enables security administrators to manage segmentation seamlessly from end to end, user to application. A common and consistent identity-based microsegmentation capability is provided from the user to the application. As a result of this integration, the attack surface is greatly reduced, and any unauthorized or suspicious access to resources and potential threats can quickly be controlled and remediated. The solution is fully qualified for up to 25,000 Cisco SD-Access campus users, with plans to expand scale as needed by our customers.

**Cisco ACI and ServiceNow**

Enterprises are increasingly embracing a multicloud strategy to deliver applications with the intent to accelerate innovation and reduce costs. However, this strategy brings in its wake inherent challenges in application agility and security. Enterprises demand business services to be up and running rapidly to serve their end users. End users often demand that IT departments quickly and flexibly offer services that can help them get their jobs done. This goal leaves many IT teams struggling to maintain the business services needed to help ensure that end users remain productive. Some of the challenges they face in helping ensure the uptime of critical business services include:

- A manual service mapping process that can take weeks or months, depending on service complexity.
- Lack of correlation between infrastructure changes and the business services they support.
- Disconnected infrastructure tools and portals for change management and troubleshooting.
- Inefficient root-cause analysis for service outages as a result of inaccurate service maps.

Cisco ACI integration with ServiceNow automates the discovery, application to business service mapping, firmware management, and provisioning of the Cisco ACI fabric from the ServiceNow instance.

Integrating Cisco ACI with ServiceNow delivers visibility and automation from the application tier down to the physical infrastructure, improving the speed and efficiency of IT provisioning, management, and troubleshooting, including:

- Faster troubleshooting and root-cause analysis.

- Improved operational efficiency.
- Reduced TCO.

**Cisco ACI and Kubernetes**

Cisco ACI is designed to offer policy-based automation, security, mobility, and visibility for application workloads regardless of whether they run on bare-metal servers, hypervisors, or Linux containers. The Cisco ACI system-level approach extends the support for Linux containers by providing tight integration of Kubernetes, a popular container orchestration platform, and the Cisco ACI platform.

This integration allows Cisco ACI to provide a ready-to-use, secure networking environment for Kubernetes. The integration maintains the simplicity of the user experience in deploying, scaling, and managing containerized applications while still offering the controls, visibility, security, and isolation required by an enterprise.

The Cisco ACI and Kubernetes solution offers the following benefits:

- Flexible approach to policy.
- Automated, integrated load-balancing services.
- Secure multitenancy.
- Visibility and telemetry information.

## Cisco ACI open ecosystem

Table 1. Features of the Cisco ACI open ecosystem

| Feature | Description |
|---|---|
| Third-party integration enabled by open APIs | Avoid vendor lock-in and expand choice and flexibility to build your own data center solution. |
| Jointly certified software solutions with ecosystem partners | Employ a best-in-class SDN ecosystem with more than 65 technology partners, with partners publishing a certification matrix to guide customers to install and upgrade compatible software versions. |
| L4-L7 service integration through service chaining | Deploy multivendor service graphs with a Cisco ACI integration mode of your choice to meet your operational and organizational needs. |

The bridge to possible

## Cisco Capital

**Flexible payment solutions to help you achieve your objectives.**

Cisco Capital® makes it easier to get the right technology to achieve your objectives, enable business transformation and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services and complementary third-party equipment in easy, predictable payments. Learn more.

## For more information

### Use the following links for additional information:

- Cisco ACI website
- Cisco APIC Data Sheet
- Cisco Nexus 9000 Series Switches Data Sheets
- Cisco ACI Multi-Site White Paper
- Cisco ACI Remote Leaf Switches
- Data Center and Cloud Networking Case Studies
- Download Cisco ACI software
- Cisco Application Centric Infrastructure Ordering Guide



C22-741487-07 06/24