Cisco Application Centric Infrastructure

What’s Inside

- At a glance: Cisco ACI solution
- Main benefits
- Cisco ACI building blocks
- Main features
  - Fabric Management and Automation
  - Network Security
  - Virtualization and Containers
  - Open Ecosystem
  - Streaming Telemetry
  - Fabric Extension and Deployment options
- For more information

At a Glance: Cisco ACI Solution

Cisco® Application Centric Infrastructure (Cisco ACI™) is the industry’s most secure, open, and comprehensive Software-Defined Networking (SDN) solution. It radically simplifies, optimizes, and accelerates infrastructure deployment and governance and expedites the application deployment lifecycle.

Cisco ACI implements Cisco’s intent-based networking framework. It captures higher-level business and user intent in the form of a policy and converts this intent into the network constructs necessary to dynamically provision the network, security, and infrastructure services. It uses a holistic systems-based approach, with tight integration between hardware and software and physical and virtual elements, an open ecosystem model, and innovative Cisco customer Application-Specific Integrated Circuits (ASICs) to enable unique business value for modern data centers. This unique approach uses a common policy-based operating model across the network, drastically reducing the cost and complexity of operating your network.

Main Benefits

With Cisco ACI, you can build a better network anywhere.
Cisco ACI is the only SDN solution that is hypervisor independent; works cohesively with all types of workloads including virtual machines, physical bare-metal servers, and containers; and extends seamlessly from your on-premises data center to remote small-scale data centers and even across geographically dispersed multiple data centers.

You truly get a Cisco ACI Anywhere solution: with one intent, using any hypervisor, for any workload, in any location (coming up shortly), and in any cloud (future).

The main benefits of Cisco ACI include the following:

**Optimize Your Network**

- Operational simplicity, with common policy, management, and operation models across application, network, and security resources
- 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
- Centralized network management and visibility with full automation and real-time network health monitoring
- Seamless integration of underlay and overlay
- Open northbound APIs to provide flexibility for DevOps teams and ecosystem partner integration
- An SDN solution at cloud scale
- Common platform for managing physical and virtual environments
Protect Your Business

- Business continuity and disaster recovery
- Secure networking with a zero-trust security model and innovative security features such as microsegmentation
- Security at cloud scale with hardware performance

Accelerate Multi-cloud (future)

- Single policy and seamless connectivity across any data center and public cloud
- Any hypervisor, any workload, any location, any cloud
- Cloud automation enabled by integration with vRealize, AzurePck, OpenStack, UCS Director

Cisco ACI Building Blocks

The Cisco ACI solution consists of the following building blocks (Figure 2):

- Cisco Application Policy Infrastructure Controller (APIC)
- Cisco ACI multisite virtual appliance
- Cisco Nexus® 9000 Series spine and leaf switches for Cisco ACI
- Cisco Application Virtual Switch (AVS)

Figure 2. Cisco ACI Architectural Building Blocks
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 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 and vShield
  - Microsoft Hyper-V, System Center Virtual Machine Manager (SCVMM), and Azure Pack
  - Open Virtual Switch (OVS) and OpenStack
  - Kubernetes
- Image management (spine and leaf)
- Cisco ACI inventory and configuration
- Implementation on a distributed framework across a cluster of appliances
- Health scores for critical managed objects (tenants, application profiles, switches, etc.)
- Fault, event, and performance management
- Cisco Application Virtual Switch (AVS), which can be used as a virtual leaf switch

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 ACI Multi-Site Virtual Appliance

The Cisco ACI multisite appliance provides a single point of provisioning for multiple Cisco ACI fabrics operating in a coordinated way. When this appliance 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. Centralized policy and security controls across geographically distributed fabrics and very large scaled-out fabrics at a single site enable automation and operations from a common point for global cloud-scale infrastructure.

The main features of the multisite solution include the following:

- Single point of administration for multiple Cisco ACI fabrics
- Capability to map tenants, applications, and associated networks to specific availability domains within the Cisco ACI multisite
- Change control across multiple fabrics, allowing staging, testing, and if required, clean backout of any policy changes
- Automatic configuration and management of fabric network interconnects across an IP backbone

**Cisco Nexus 9000 Series Spine and Leaf Switches for Cisco ACI**

Cisco Nexus 9300 and 9500 platform 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, 10, 25, 40, 50, and 100 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 Application Virtual Switch**

Cisco AVS is a hypervisor-resident virtual network switch that is specifically designed for the Cisco ACI architecture. AVS provides feature support for the Cisco ACI policy model, full switching capabilities, and more advanced telemetry features.

Main features include the following:

- Purpose-built, virtual network edge for Cisco ACI fabric architecture
- Integration with the Cisco ACI management and orchestration platform to automate virtual network provisioning and application services deployments
- High performance and throughput
- Integrated visibility of both physical and virtual workloads and network paths
- Open APIs to extend the software-based control and orchestration of the virtual network fabric

AVS offers:

- Single point of management and control for both physical and virtual workloads and infrastructure
- Optimal traffic steering to application services
- Seamless workload mobility
- Support for all leading hypervisors with a consistent operational model across implementations for simplified operations in heterogeneous data centers

**Main Features**

This section summarizes the main features of the Cisco ACI solution.

Cisco ACI brings differentiated benefits in four areas, shown in Figure 3.
Table 1 summarizes the Cisco ACI fabric management features.

Table 1. Fabric Management and Automation Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Touchless provisioning</td>
<td>Bootstrap your network with topology autodiscovery, automated leaf configuration, and infrastructure addressing using industry-standard protocols.</td>
</tr>
<tr>
<td>Centralized fabric management</td>
<td>Manage your network and L4-L7 service nodes through APIC for single-pane management. Every single task can be performed through the APIC GUI, Command-Line Interface (CLI), and northbound open representational state transfer (REST) APIs. Cisco ACI offers a single access point to an NX-OS style of CLI on the APIC and access to all switches in the fabric.</td>
</tr>
<tr>
<td>Network virtualization</td>
<td>Employ an integrated approach to network virtualization with segmentation implemented at both the software and hardware layers.</td>
</tr>
<tr>
<td>Scalable multitenancy</td>
<td>A Virtual Extensible LAN (VXLAN)–enabled overlay approach provides a cloud-scale multitenant fabric with a significantly large network segment space.</td>
</tr>
<tr>
<td>Policy enforcement</td>
<td>Cisco ACI captures your intent in the form of a policy between and within endpoint groups and dynamically enforces it across the fabric leaf switches, according to the location to which the endpoint moves.</td>
</tr>
<tr>
<td>Workload mobility</td>
<td>The Cisco ACI policy model and VXLAN-based overlay jointly support workload mobility in which security policies travel to wherever application workloads move.</td>
</tr>
<tr>
<td>Real-time monitoring and troubleshooting</td>
<td>You can now troubleshoot faster with health scores. A health score is a real-time weighted score abstracting various types of faults at the tenant, pod, application, and system levels. Know process-level performance with CPU and memory utilization indexes. Debug the data path with protocol, bridge domain, VLAN, and interface-level statistics and atomic counters. Divert traffic though Cisco Switched Port Analyzer (SPAN), Encapsulated Remote SPAN (ERSSPAN), or Copy Service features. The capacity dashboard provides visual cues about hardware resource utilization in the Cisco ACI fabric. Stream your traffic from Cisco Nexus 9000 Series Switches hardware sensors to the Cisco Tetration Analytics™ platform for pervasive visibility into applications through big data analytics. Troubleshoot wizard for easy network troubleshooting. Heat map of resources. The EP (Endpoint) Tracker feature allows you to quickly see the location of the endpoint, the Endpoint...</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Graceful Insertion and Removal (GIR)</td>
<td>Perform device upgrades and maintenance by gracefully isolating the node from the fabric and reinserting it into the network after the maintenance window with little to no traffic impact.</td>
</tr>
</tbody>
</table>

Group (EPG) it belongs to, the VLAN encapsulation used, and any state transitions.
### Feature Description

**API-based automation and orchestration**
The APIC’s open northbound APIs allow Cisco ACI to interoperate with products such as Cisco UCS Director, Cisco Cloud Center, and Cisco Tetration Analytics plus many third-party products. Avoid vendor lock-in and gain control and visibility for the network fabric using our application policy framework.

**High availability**
Operate the APIC cluster in active-standby mode. The APIC provides split-brain detection. Deploy multipod and multisite solutions. Get N-way spine redundancy. Deploy APIC cluster software rolling upgrades and downgrades. Site ID recovery helps recover the configuration state of APIC from the operational state of ACI network.

**Multiple software versions in fabric**
To ease network migration and upgrades, you can use Cisco ACI fabric nodes with different qualified software versions at the same time.

### Virtualization and Containers

Table 2 summarizes the Cisco ACI virtualization and container features.

**Table 2. Virtualization and Container Features**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual machine networking</td>
<td>Consistently enforce policies across both virtual and physical workloads managed by hypervisors from multiple vendors.</td>
</tr>
<tr>
<td>Virtual Machine Manager (VMM) domain profiles</td>
<td>Enable virtual machine mobility and placement of workloads anywhere in the Cisco ACI fabric.</td>
</tr>
<tr>
<td>OpenStack integration</td>
<td>Employ fully distributed Neutron networking, your choice of Neutron APIs or group-based policy, and OpenStack-aware visibility within the fabric.</td>
</tr>
</tbody>
</table>

### Network Security

Table 3 summarizes the Cisco ACI security features.

**Table 3. Security Features**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zero-trust security model</td>
<td>The Cisco ACI whitelist-based policy model supports zero-trust security architecture. It assumes no default trust between entities regardless of the location of the entity.</td>
</tr>
<tr>
<td>Role-Based Access Control (RBAC)</td>
<td>Achieve true multitenant isolation with custom RBAC rules on the APIC. The APIC provides access according to a user’s roles, privilege types, and security domain tags.</td>
</tr>
<tr>
<td>Microsegmentation</td>
<td>Reduce your network’s attach surface by reducing the possibilities for lateral movement in the event of a security breach. Cisco ACI microsegmentation allows you to formulate a custom security group of virtual machine endpoints based on various virtual machine-level attributes, tags, etc.</td>
</tr>
<tr>
<td>Cisco TrustSec® integration</td>
<td>Address breaches, segmentation, and compliance challenges by sharing policy groups between networks enabled for Cisco TrustSec and Cisco ACI data centers. Provide consistent security policy management across the enterprise by using user roles and device types together with application context anywhere in the network. This integration simplifies security design, operations, and compliance.</td>
</tr>
<tr>
<td>Secure user authentication</td>
<td>Get local authentication with password and RBAC rules. The APIC also supports secure user authentication using TACACS+, RADIUS, and Lightweight Directory Access Protocol (LDAP).</td>
</tr>
<tr>
<td>Audit support and logging</td>
<td>Audit all user access and configuration changes in the system.</td>
</tr>
</tbody>
</table>
### Feature Description

**Secure Virtual Desktop Infrastructure (VDI)**

Deploy large scale VDI leveraging user identity based ACI micro-segmentation in conjunction with Cisco FirePOWER.

**Automatic Remediation**

Automatically quarantine and remediate the threats using a closed security feedback loop between Cisco ACI and Cisco Sourcefire.

**First-hop security**

Mitigate security threats such as Man-In-The-Middle attack (MITM) attacks and IP theft. The first-hop security feature lets you build a secure endpoint database by controlling address assignment and derived operations such as duplicate address detection and address resolution.

**Multifactor authentication**

Authenticate access to the APIC only when the user has successfully passed a 2-step authentication process.

**Endpoint authentication**

Secure your network by authenticating every device that wants to attach to your data center network.

---

**Open Ecosystem**

Table 4 Summarizes the Features of the Cisco ACI Open Ecosystem.

#### Table 4. Open Ecosystem Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Third-party integration enabled by open APIs</strong></td>
<td>Avoid vendor lock-in and expand choice and flexibility to build your own data center solution.</td>
</tr>
<tr>
<td><strong>Jointly certified software solutions with ecosystem partners</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>L4-L7 service integration through service chaining</strong></td>
<td>Deploy multivendor service graphs with a Cisco ACI integration mode of your choice to meet your operational and organizational needs.</td>
</tr>
</tbody>
</table>
| **Cisco ACI App Center** | Cisco ACI applications help you get the best applications for Cisco ACI in an efficient way. The Cisco ACI App Center:  
  - Accelerates innovations related to the Cisco ACI open ecosystem  
  - Enables Cisco internal partners, customers, and third-party developers to add value to Cisco ACI networks  
  - Allows customers to efficiently extract value from their networking investments |

---

**Streaming Telemetry**

Table 5 summarizes the Cisco ACI streaming telemetry features.

#### Table 5. Streaming Telemetry Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tetration sensor support</strong></td>
<td>Stream your traffic from Cisco Nexus 9000 Series Switches hardware sensors to the Cisco Tetration Analytics platform for pervasive visibility into applications through big data analytics.</td>
</tr>
<tr>
<td><strong>Cisco NetFlow</strong></td>
<td>Monitor data traffic flowing through your Cisco ACI fabric. Monitoring provides a metering base for applications, traffic accounting, use-based network billing, and network planning. This feature also provides denial-of-service monitoring capabilities.</td>
</tr>
</tbody>
</table>
Fabric Extension and Deployment Options

The fundamental design of Cisco ACI includes control-plane and data-plane disaggregation and fault isolation. The main benefit of this model is that the operational state of the Cisco ACI fabric’s control plane (the APIC cluster) does not affect data-path forwarding within the Cisco ACI network.

Cisco ACI provides various fabric deployment options to meet your objectives, summarized in Table 6.

**Table 6. Fabric Extension and Deployment Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stretched fabric</td>
<td>You can use the same control planes and data planes stretched across multiple sites. This deployment with transit leaf switches supports a partial mesh design that connects Cisco ACI leaf and spine switches distributed in multiple locations. Though the fabric is stretched across different geographical locations, it constitutes one fault domain.</td>
</tr>
<tr>
<td>Multipod</td>
<td>You can use partial fault isolation with one control plane but isolated data planes across pods. A multipod solution allows a single APIC cluster to manage multiple Cisco ACI fabrics in which each fabric is a pod. The multipod fabric can be between different floors or buildings within a campus or a local metropolitan region. Each pod is a localized fault domain.</td>
</tr>
<tr>
<td>Multisite</td>
<td>You can use complete fault isolation with an isolated control plane and data plane at every site. A multisite solution provides one management view and policy extension across your data centers, whether they are in same building or around the world. It simplifies the management of multiple data centers by offering a single operational domain with enhanced availability and flexibility.</td>
</tr>
</tbody>
</table>

For More Information

Use the following links for additional information.

<table>
<thead>
<tr>
<th>Link</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco ACI Ordering Guide</td>
<td>Click here</td>
</tr>
<tr>
<td>Cisco APIC Datasheet</td>
<td>Click here</td>
</tr>
<tr>
<td>Cisco Nexus 9000 Series Switches data sheet</td>
<td>Click here</td>
</tr>
<tr>
<td>Cisco AVS data sheet</td>
<td>Click here</td>
</tr>
<tr>
<td>Cisco ACI solution general details</td>
<td>Click here</td>
</tr>
<tr>
<td>Technical white papers</td>
<td>Click here</td>
</tr>
<tr>
<td>Case studies</td>
<td>Click here</td>
</tr>
<tr>
<td>Solution overviews</td>
<td>Click here</td>
</tr>
<tr>
<td>YouTube video tutorials</td>
<td>Click here</td>
</tr>
<tr>
<td>Release notes for Cisco ACI and APIC solutions</td>
<td>Click here</td>
</tr>
<tr>
<td>Release notes for Cisco Nexus 9000 Series Switches</td>
<td>Click here</td>
</tr>
<tr>
<td>Download Cisco ACI software</td>
<td>Click here</td>
</tr>
</tbody>
</table>

Cisco Capital

Financing to Help You Achieve Your Objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there’s just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.