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 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. 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.
Benefits

Cisco ACI is the industry leading SDN solution that provides policy driven automation through an integrated underlay and overlay, is hypervisor agnostic; and extends policy automation to any workload—including virtual machines, physical bare-metal servers, and containers.

Cisco ACI Anywhere is a comprehensive solution: with one intent, using any hypervisor, for any workload, in any location, and in any cloud.

Cisco ‘ACI Anywhere’ offers a set of capabilities that enable seamless connectivity between on-premises data center, remote small-scale data centers, and geographically dispersed multiple data centers under a single pane of policy orchestration. In future, these capabilities will extend to public cloud as well.

With Cisco ACI, you can build a better network anywhere.

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 accelerated by hardware

**Accelerate multi-cloud**

- 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, AzurePack, OpenStack, OpenShift, Kubernetes, and 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 Nexus® 9000 Series spine and leaf switches for Cisco ACI
- Cisco ACI MultiPod
- Cisco ACI Multi-Site Orchestrator
- Cisco ACI Virtual Edge (AVE)
- Cisco ACI Physical Remote Leaf
- Cisco ACI Virtual Pod (vPod)
- Cisco ACI Mini Fabric

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 vRealize
  - Microsoft Hyper-V, System Center Virtual Machine Manager (SCVMM), and AzurePack
  - 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

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 9000 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, 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 ACI MultiPod

ACI MultiPod is part of the “Single APIC Cluster/Single Domain” family of solutions as a single APIC cluster is deployed to manage all the different ACI networks that are interconnected. These separate ACI networks are named “Pods” and each of them looks like a regular two-tiers 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.

Cisco ACI Multi-Site Orchestrator

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 ACI Virtual Edge

Cisco ACI Virtual Edge is the next generation of the Application Virtual Switch for Cisco ACI environments. Cisco ACI Virtual Edge is a hypervisor-independent distributed service VM that leverages the native distributed virtual switch that belongs to the hypervisor. Cisco ACI Virtual Edge runs in user-space, operates as a virtual leaf, and is managed by the Cisco Application Policy Infrastructure Controller (APIC).
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

Cisco ACI Virtual Edge benefits:

- Hypervisor independent distributed service VM that leverages the distributed virtual switch of the hypervisor
- ACI policy model for virtual workloads and policy consistency with physical environment
- Seamless workload mobility
- Ability to secure east-west traffic using micro segmentation
- Maintain distributed firewall policies across virtual machine moves

Cisco ACI Virtual Pod

The Cisco ACI Virtual Pod architecture is an extension of the ACI architecture in the virtual infrastructure space. A Virtual Pod consists of a management cluster [Virtual Spines (vSpines), Virtual Leafs (vLeafs)] and ACI Virtual Edge (AVE) instances that are deployed on a hypervisor infrastructure. The main use-case of ACI Virtual Pod is the ability to extend an existing ACI policy domain in a location that cannot accommodate the addition of a physical ACI component. These locations can be baremetal cloud extensions, brownfield deployments, remote locations and Co-Lo facilities. Virtual Pods are managed by the APIC in the On-Prem datacenter. The Virtual Pod interconnects with the physical ACI fabric using a generic IP Network (IPN). Thus the Cisco ACI Virtual Pod deployment remains functionally a single fabric, with all the nodes deployed across the physical and virtual Pods under the control of a single APIC cluster.

Cisco ACI Physical Remote Leaf

With Cisco ACI Physical Remote Leaf, customers can place a regular leaf switch in a remote/satellite location and connect back to the Spine switch in the main (on premise) location and in turn extend ACI policy into the remote/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 Core Features

This section summarizes the main features of the Cisco ACI solution. Cisco ACI brings differentiated benefits in four areas, shown in Figure 3.

Figure 3. Cisco ACI benefits

---

**Cisco ACI Mini Fabric**

With the introduction of Cisco Mini ACI Fabric customers can now leverage an optimized ACI solution for their small-scale deployments. This solution comprises of APIC-CLUSTER-XS (1 physical and 2 virtual controllers) along with 2 spines and a minimum of 2 and maximum of 4 leaves.

Solution overview

Cisco public

On-premises ACI Data Center

Remote Location

Policy extension from On-premise DC

Logical Connection to Spine (BGP-EVPN)

IP Network

Virtual Pod

Hypervisor

ACI Virtual Edge

Virtual Spine

vSpine

vLeaf

vLeaf

Leaf 2 - 48 ports

Leaf 1 - 48 ports

Leaf 1 - 48 ports

Leaf 2 - 48 ports

No. of Leafs

2-4

No. of Spines

2

No. of Tenants

25

No. of EPs

20,000

No. of BDs

1000

No. of EPGs

1000

No. of VRFs

25

Physical APIC

1

Virtual APIC

2

© 2018 Cisco and/or its affiliates. All rights reserved.
### Fabric management and automation

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.</td>
</tr>
<tr>
<td></td>
<td>Every single task can be performed through the APIC GUI, Command-Line Interface (CLI), and northbound open Representational State Transfer (REST) APIs.</td>
</tr>
<tr>
<td></td>
<td>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 trouble shooting</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.</td>
</tr>
<tr>
<td></td>
<td>Know process-level performance with CPU and memory utilization indexes.</td>
</tr>
<tr>
<td></td>
<td>Debug the data path with protocol, bridge domain, VLAN, and interface-level statistics and atomic counters.</td>
</tr>
<tr>
<td></td>
<td>Divert traffic though Cisco Switched Port Analyzer (SPAN), Encapsulated Remote SPAN (ERSPAN), or Copy Service features.</td>
</tr>
<tr>
<td></td>
<td>The capacity dashboard provides visual cues about hardware resource utilization in the Cisco ACI fabric.</td>
</tr>
<tr>
<td></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></td>
<td>Troubleshoot wizard for easy network troubleshooting.</td>
</tr>
<tr>
<td></td>
<td>Heat map of resources.</td>
</tr>
<tr>
<td></td>
<td>The EP (Endpoint) Tracker feature allows you to quickly see the location of the endpoint, the Endpoint Gr(EPG) it belongs to, the VLAN encapsulation used, and any state transitions.</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>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>API-based automation and orchestration</td>
<td>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.</td>
</tr>
<tr>
<td>High availability</td>
<td>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.</td>
</tr>
<tr>
<td>Multiple software versions in fabric</td>
<td>To ease network migration and upgrades, you can use Cisco ACI fabric nodes with different qualified software versions at the same time.</td>
</tr>
<tr>
<td>Policy Based Redirect</td>
<td>ACI Policy Based Redirect (PBR) enables provisioning service appliances, such as firewalls or load balancers, as managed or unmanaged nodes without needing a Layer 4 to Layer 7 package. PBR simplifies the deployment of service appliances by enabling the provisioning consumer and provider endpoint groups to be all in the same Virtual Redirect and Forwarding (VRF) instances.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Virtualization and containers**

Table 2 summarizes the Cisco ACI 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>
## Solution overview

Cisco public

© 2018 Cisco and/or its affiliates. All rights reserved.

### OpenShift Integration

Cisco ACI integrates with the OpenShift container application platform. OpenShift platform simplifies deployments of containers for both development and production workloads. Cisco ACI provides foundational networking optimized for performance, scale and availability of OpenShift Container platform.

### Microsoft Windows Azure Pack Integration

Cisco ACI integrates with Microsoft Windows Azure Pack to provide a self-service experience for the tenant. Cisco ACI with Microsoft Windows Azure Pack for Windows Server is a collection of Microsoft Azure technologies that include the following capabilities: Management portal for tenants; Management port for administrators; Service Management API.

### RedHat Virtualization

Cisco ACI integration with RedHat Virtualization helps in further enhancing the network management capabilities of the platform. This solution will enable the next generation cloud deployments that drive business agility and lower operational costs.

Cisco and Red Hat offer a certified, supported turn-key ACI based OpenStack solution. This solution enables customers to deploy the full range of service and deployment models with OpenStack to meet the most demanding needs of cloud deployments.

### Pivotal Cloud Foundry

Cisco ACI integration with Pivotal Cloud Foundry enables customers to use all Cisco ACI security and policy features in Pivotal Cloud Foundry.

### Kubernetes and OpenShift Nested in OpenStack VMs

The ACI Containers solution brings native ACI support to container orchestration systems. The ACI Containers Nested in OpenStack VMs will support the deployment of the ACI Containers solution inside OpenStack VMs. Cisco APIC serves as the normalization point for common policy and provides one place for administering it. This solution preserves the design of the ACI Container solution for Bare-Metal servers and adapts it to run inside OpenStack VMs.

### Network security

Table 3 summarizes the Cisco ACI security features.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kubernetes and OpenShift Nested in OpenStack VMs</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>
</tbody>
</table>

© 2018 Cisco and/or its affiliates. All rights reserved.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>Multifactor authentication</td>
<td>Authenticate access to the APIC only when the user has successfully passed a 2-step authentication process.</td>
</tr>
<tr>
<td>Endpoint authentication</td>
<td>Secure your network by authenticating every device that wants to attach to your data center network.</td>
</tr>
<tr>
<td>Dot1x Authentication</td>
<td>Cisco ACI supports IEEE 802.1x port-based authentication mechanism to prevent unauthorized devices from gaining access to the network.</td>
</tr>
<tr>
<td>MAC SEC</td>
<td>Cisco ACI supports the IEEE 802.1AE Standards based Layer-2 hop by hop encryption that provides data confidentiality and integrity for media access independent protocols.</td>
</tr>
<tr>
<td>RSA Two-Factor Authentication</td>
<td>Cisco ACI Provides token based password and multi-factor authentication and Identity Assurance for access to APIC. Supports multiple levels of authentication including two-factor authentication, Multi-Factor Authentication (MFA), email authentication or mobile MFA.</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) and SAML. Audit support and logging</td>
</tr>
<tr>
<td>Secure Virtual Desktop Infrastructure (VDI)</td>
<td>Deploy large scale VDI leveraging user identify based ACI micro-segmentation in conjunction with Cisco FirePOWER.</td>
</tr>
<tr>
<td>Automatic Remediation</td>
<td>Automatically quarantine and remediate the threats using a closed security feedback loop between Cisco ACI and Cisco Sourcefire.</td>
</tr>
<tr>
<td>First-hop security</td>
<td>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.</td>
</tr>
<tr>
<td>CloudSec</td>
<td>Cisco ACI provides industry’s first encrypted VXLAN Overlay for Inter-Site traffic. The Spine to Spine encryption technology provides Controller based key generation along with linerate encryption of traffic going across Multi-Site ACI fabrics.</td>
</tr>
</tbody>
</table>
ACI 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 stretch the ACI fabric across multiple geographies using the stretched fabric deployment model. 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>Multi-Pod</td>
<td>ACI Multi-pod allows you to enable isolation one of control plane and data planes across multiple pods. A multipod solution allows a single APIC cluster to manage multiple pods. 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>Multi-Site</td>
<td>ACI Multi-site allows you to automate the connectivity between multiple sites under a single policy domain, while providing isolation of control plane and data plane at every site. This requires the deployment of the ACI Multi-site orchestrator that composes and coordinates policy across sites, and also provides visibility into the health of infrastructure across sites. 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>
<tr>
<td>Physical Remote Leaf</td>
<td>ACI ‘Remote Leaf’ extends the policy driven automation functions to a remote location (or satellite datacenters) by deploying a pair of Nexus 9K leafs, connected to the on-prem datacenter over an IP network. These remote leafs are managed by the APIC in the On-Prem datacenter.</td>
</tr>
<tr>
<td>Virtual Pod (vPod)</td>
<td>The Cisco ACI Virtual Pod architecture is an extension of the Multi-Pod architecture in the virtual infrastructure space. A Virtual Pod consists of a management cluster [Virtual Spines(vSpines), Virtual Leafs (vLeafs)] and ACI Virtual Edge (AVE) instances that are deployed on an existing hypervisor infrastructure. The main use-case of ACI Virtual Pod is the ability to extend an existing ACI policy domain in a location that cannot accommodate the addition of a physical ACI component. These locations can be baremetal cloud extensions, brownfield deployments, remote locations and Co-Lo facilities. Virtual Pods are managed by the APIC in the On-Prem datacenter.</td>
</tr>
</tbody>
</table>
Figure 4 shows Cisco ACI certifications.

Figure 4. Certifications

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>Third-party integration enabled by open APIs</td>
<td>Avoid vendor lock-in and expand choice and flexibility to build your own data center solution. 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. Deploy multivendor service graphs with a Cisco ACI integration mode of your choice to meet your operational and organizational needs.</td>
</tr>
<tr>
<td>Jointly certified software solutions with ecosystem partners</td>
<td>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</td>
</tr>
<tr>
<td>L4-L7 service integration through service chaining</td>
<td></td>
</tr>
<tr>
<td>Cisco ACI App Center</td>
<td></td>
</tr>
</tbody>
</table>

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>Tetration sensor support</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>Cisco NetFlow</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>
<tr>
<td>Network Insight Resources</td>
<td>The Network Insight Resources App is a platform for predictive analytics, streaming telemetry data for networking fabrics and providing flow level telemetry information. The App provides system metrics, statistical data correlation, fabric anomaly detection and flow triage information along with fabric resource utilization.</td>
</tr>
</tbody>
</table>
For more information

Use the following links for additional information.

- Cisco ACI Overview
- Cisco ACI Ordering Guide
- Cisco APIC Datasheet
- Cisco Nexus 9000 Series Switches datasheet
- Cisco ACI Virtual Edge data sheet
- Cisco ACI Multi Site White paper
- Cisco ACI Remote Leaf
- Technical white papers
- Case studies
- Solution overviews
- YouTube video tutorials
- Release notes for Cisco ACI and APIC solutions
- Release notes for Cisco Nexus 9000 Series Switches
- Download Cisco ACI software

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.