Cisco Application Centric Infrastructure (Cisco ACI)



© 2026 Cisco and/or its affiliates. All rights reserved.

Challenges networks face today

The pace of digital innovation is surging across the digital ecosystem with the unprecedented growth of AI, resulting in a sharp expansion of applications and cloud usage. Enterprises now demand agility and security to support 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 5G use cases.

To meet these demands, organizations are adopting software-defined networking frameworks. These frameworks allow you to attain true network agility across the data center and cloud, improving 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 operates seamlessly with Nexus® Dashboard, on-premises managed Nexus One, enabling agility and resiliency in hybrid and complex enviornments It captures 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.

As the industry's most secure, open, and comprehensive Software-Defined Networking (SDN) solution, Cisco ACI delivers automation that accelerates infrastructure deployment and governance. It simplifies management, allowing easy movement of workloads across a multifabric and hybrid frameworks, while proactively securing against risk arising from anywhere. This 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 datacenter.

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 is built to simplify the IT infrastructure and operations by automating the network, providing pervasive security, and helping accelerate businesses to operate in complex hybrid environments.

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.

© 2026 Cisco and/or its affiliates. All rights reserved.

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, removing the need for complex Data Center Interconnect (DCI) infrastructure.

- **Empower the 400G to 800G evolution:** make your infrastructure future ready with high-speed connectivity
- **Centralized visibility and automation:** gain full automation and real-time network health monitoring
- **Seamless Provisioning:** unify underlay and overlay networks, bootstrapped APIC clustering for seamless operations
- **Open API ecosystem:** leverage open northbound APIs for flexibility with DevOps teams and third-party integrations
- **Common platform:** manage physical and virtual environments from a single place
- **Automated workflows:** simplify IT tasks and enable flexible application deployment
- **Expanded reach:** extend mobility domains using standards-based extensions
- **Seamless connectivity with Cisco Nexus One:** enable any-to-any connectivity between ACI and VXLAN EVPN fabrics with consistent policy extensions
- **Enhanced load balancing:** improve performance with DLB, fabric, and L3 port-channel support, customizable thresholds using superior forwarding mechanisms, and per-packet load balancing
- **Hybrid APIC clusters:** enable seamless co-existence and interoperability between physical and virtual APICs
- **AI/ML readiness:** support high-bandwidth, scalable, and deterministic connectivity required for modern AI/ML workloads.

Securely expand to hybrid environments

- **AI/ML ready SDN:** employ a secure and robust solution designed for general purpose and AI/ML ready data center
- **Business continuity:** ensure robust disaster recovery and continuity planning
- **Inherent security:** benefit from a zero-trust allow-list model, advanced policy enforcement, microsegmentation, and analytics
- **Integrated security:** seamlessly integrate with Cisco security products and ecosystem partners
- **Consistent security posture:** scale across a multicloud environment in a secure manner

Deliver superior experience

- **Operational simplicity:** utilize common policy, management, and operation models across application, network, and security resources
- **Flexible deployment:** adapt to your specific needs with versatile deployment models
- **Unified Policy:** ensure single policy and seamless connectivity across any data center and public cloud
- **Container networking:** integrate with OpenStack, OpenShift, Kubernetes, and Cisco UCS® Director
- **Programmability:** access open APIs and a programmable SDN fabric, with 65+ ecosystem partners including Infrastructure as Code (IaC)
- **Optimized upgrades:** benefit from faster APIC reboot times, centralized workflows for cluster upgrades, and support for APIC CIMC upgrades directly through the APIC
- **Operational efficiency:** improve efficiency with enhanced support for mixed (dual) software versions across ACI fabrics
- **Scalability:** harness the power to scale as your business grows

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Nexus Dashboard, on-premises managed Nexus One

Cisco Nexus Dashboard provides a unified automation and operations platform for data center networking. As the on-premises operational model of Nexus One, it can deploy policy and connectivity automation, provide visibility and analytics, and traffic aggregation. This platform becomes a collaborative focal point by including operations-critical, third-party applications and tools. The platform drives the adoption of cloud-native application practices, offering 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.

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Nexus Dashboard visibility and analytics

Gain real-time monitoring and analysis of your fabric to identify anomalies, perform root-cause analysis, 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, allowing for proactive corrective actions.

Cisco Nexus Dashboard policy and connectivity automation

Provision multiple Cisco ACI fabrics from a single point. Combined with the latest Cisco ACI enhancements, organizations can manage 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, allowing for a global cloud-scale infrastructure.

Cisco ACI building blocks

Cisco ACI and architectural solutions are built in two primary building blocks:

- Cisco Application Policy Infrastructure Controller (APIC)
- Cisco N9000 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.

Key features of Cisco APIC:

- Application-centric network policies.
- Object tree 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 ensures broad ecosystem interoperability, connecting Cisco ACI with management, orchestration, virtualization, and L4-L7 services from a broad range of vendors.

Cisco N9000 Series spine and leaf switches for Cisco ACI

Cisco N9300, N9400, and N9500 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 N9000 Series Switches include modular and fixed 1 to 400 to 800 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) for VMware
- Virtual APIC (vAPIC) for Nutanix
- 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.

© 2026 Cisco and/or its affiliates. All rights reserved.

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.

© 2026 Cisco and/or its affiliates. All rights reserved.

- **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.

With its remote leaf resiliency feature, it groups multiple RLs that form fully meshed BGP EVPN sessions to share routing information, ensuring local traffic continues despite WAN or main POD failures, using a standards-based EVPN approach.

Cisco ACI capabilities and use-cases

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.

© 2026 Cisco and/or its affiliates. All rights reserved.

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 Protection and OpEx reduction.

Cisco Nexus One: next-generation data center architecture

- With Cisco Nexus One, Cisco ACI fabrics are unified with Cisco NX-OS VXLAN EVPN fabrics under a common operational and policy model, enabling customers to extend consistent networking and segmentation across both ACI and non-ACI domains while leveraging open standards.
- This interoperability is enabled through **ACI Border Gateway (BGW)** nodes, which act as the standards-based interconnection points between ACI and external VXLAN EVPN domains using BGP EVPN. ACI BGWs securely exchange routing, reachability, and segmentation information, allowing ACI Endpoint Groups (EPGs) and VRFs to be extended beyond the ACI fabric without altering internal fabric behavior or policy constructs.
- ACI under Nexus One continues to support its established multi-pod, multi-site, and remote-leaf deployment models, with policy and connectivity automation orchestrated centrally through Cisco Nexus Dashboard. The Nexus One unified fabric experience brings seamless interoperability, centralized visibility, and consistent microsegmentation and security policies across heterogeneous data center fabrics.

© 2026 Cisco and/or its affiliates. All rights reserved.

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 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

© 2026 Cisco and/or its affiliates. All rights reserved.

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.

© 2026 Cisco and/or its affiliates. All rights reserved.

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 and Nutanix

Cisco ACI integrates with Nutanix to provide consistent, policy-driven networking and operational visibility for virtualized workloads running on Nutanix AHV. Through integration with the Cisco APIC and Nutanix Prism, Cisco ACI enables centralized visibility into Nutanix clusters, including hosts, virtual machines, subnets, and networking constructs, while maintaining ACI as the authoritative control point for fabric policy and connectivity.

This integration allows customers to align ACI endpoint groups and network policies with Nutanix-managed virtual networks, simplifying workload onboarding and reducing manual network configuration. The result is a unified operational model that preserves a clear separation of responsibilities, with ACI for network and security policy and Nutanix for compute and storage, while delivering consistent connectivity, governance, and automation across physical and virtual infrastructure.

Cisco ACI and Isovalent

Cisco ACI integrates with the Isovalent® Enterprise Platform to deliver enhanced cloud-native networking, security, and observability for Kubernetes workloads alongside traditional ACI and Nexus deployments. The Isovalent Enterprise solution uses eBPF-based Cilium technology to extend identity-aware networking, policy enforcement, and detailed visibility into Kubernetes clusters while preserving ACI's centralized policy and fabric control.

Through this integration, ACI and Isovalent jointly enable consistent network policy alignment from the physical infrastructure to containerized applications, allowing seamless connectivity between Kubernetes services and other data-center workloads. This approach provides enriched telemetry and security insights for cloud-native environments without sacrificing the deterministic, high-performance characteristics of Cisco's underlay and overlay fabrics, enabling customers to unify traditional and modern application networking across a hybrid infrastructure.

© 2026 Cisco and/or its affiliates. All rights reserved.

For more information

Use the following links for additional information:

- Cisco ACI website.
- Cisco APIC Data Sheet.
- Cisco N9000 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.
- Cisco Nexus One.
- Guide: Designing Isovalent Enterprise for Cisco ACI & Nexus.

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.

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.

© 2026 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

C22-741487-09 09/26