Cisco Virtual Managed Services

SD-WAN Made Simple for Service Providers

Cisco' **Virtual Managed Services (VMS)** is a cloud native solution for service providers to automate, innovate and accelerate SD-WAN services to their business customers. This platform allows services providers to:

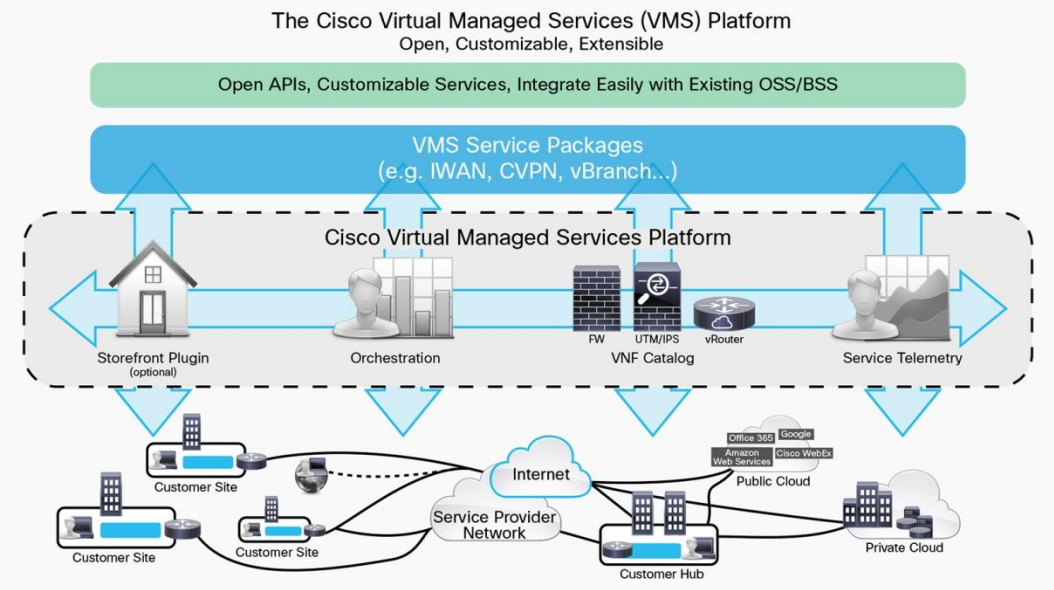
- Increase market share
- Create highly differentiated services
- Reduce cost and risk
- Deploy services faster
- Add new customers with minimal costs
- Leverage existing IT portal investments

Product Overview

Cisco's VMS and service packages deliver a turn-key solution that allows network operators to rapidly and cost effectively deliver new services to business customers.

VMS enables service providers to onboard new customers in minutes vs weeks, or months. It includes a suite of service-level packages, such as SD-WAN, and provides an open architecture for easy integration into existing systems. These service packages can be customized and new ones created using the VMS Software Development Kit.

Figure 1. The VMS Platform: How it works



Solution Components:

Service packages: A suite of prepackaged, or operator-defined, use cases that deliver the combination of business logic that uses components from the VMS solution for service delivery.

- Storefront plug-in: Customer-facing self-service portal that provides a full graphical interface for creating, ordering, customizing, managing, and activating a cloud service offering. It also provides an operator-facing portal with a dashboard application for virtual managed services operations and APIs for integration with the operator's operations support system and business support system (OSS/BSS).
- Orchestration platform: This platform enables automation of network service delivery. It uses the model-based Cisco Network Services Orchestrator (NSO) software to automate the dynamic provisioning of physical, virtual, and software assets required to create services. It uses the Cisco Elastic Services Controller (ESC) to automate virtual network functions (VNFs) lifecycle management.
- VNF catalog: Certified Cisco and third-party VNFs that can be integrated into new and existing service packages.
- Service telemetry: A data collection and distribution component that provides monitoring, health status, proactive alerts, and key performance indicators (KPIs) for end-to-end services and devices.
- Open APIs and SDK that allow every function utilized within VMS to be driven via the rich API provided as part of the system. Any function exposed via the user interface can be driven via API calls. The software development kit enables operators to build their own services integrated with VMS and offer them directly to tenants.

Automate, Innovate, and Accelerate

VMS enables to service provider to rapidly create and deploy highly differentiated and automated services:

- Secure Multi-Tenant Cloud Management with simplified orchestration, tenant self-service, assurance and analytics.
- Turn-key solution rapidly creates new services and modifies existing services, instantly from the Cloud.
- Cloud-native scalable architecture provides carrier class availability and Virtualized Infrastructure Manager (VIM) independence for ease of deployment.
- Open APIs easily integrate service workflows into existing BSS and OSS systems.

Primary Features

Service providers need to efficiently contain cost while finding new revenue streams. In order to cope with approximately 50% YoY network bandwidth growth and while leveraging key improvements in internet performance, service providers have also had to adjust to increasing pressure to reduce OpEx while relatively flat revenue. Cisco has developed these key features in VMS to simplify and accelerate service delivery while also opening up a wide array of new revenue streams.

Suite of Prevalidated Customizable Business Service Packages

Fast time to market and time to revenue are essential to service providers. The VMS solution offers multiple prepackaged and prevalidated business services. These packages support all the business and technical logic for the user interface, service orchestration, service assurance, VNFs, and underlying infrastructure. For example, cloud VPN service-level packages support secure site-to-site VPN, firewall, and web security services.

Multitenant Cloud-Native Architecture

VMS is a multitenant solution that scales with the needs of the service provider from initial installs to wide-scale deployment across the entire customer base. As a cloud-native and open system, it uses a containerized architecture consisting of multivendor network services orchestration enabled by Cisco NSO and open-source technologies such as Kubernetes. It supports standards-based YANG for service modeling, NETCONF, and representational state transfer (REST) APIs for management of multivendor physical and virtual elements. The openness and flexibility of VMS enable you to extend existing service packages and develop your own virtualized managed service offers across your infrastructure.

Customer Self-Service Portal

The comprehensive user experience provides day 0 planning, day 1 provisioning, and day 2 monitoring and assurance. It enables customers to more quickly order what they need when they need it; especially useful for new branch offices, businesses entering new markets, and organizations that need to make seasonal changes. The portal reduces customer acquisition costs and IT operating costs through simplicity and an extensible experience.

Operator Portal

The web-based operator portal is built to deliver many service provider managed services securely across many customers, offering the network operator a complete view of all customers or an individual customer. VMS provides secure role-based access control (RBAC) and Identity Management(IDM) integration that is built throughout the solution.

Service Extensions

The service extension feature enables an operator to add custom configurations to the service model via simple text file edits. This enables operators to implement their own configurations for management functions such as SNMP, AAA, and TACACS or add end-user configurations such as protocol authentication that might not be part of the standard model. Through the use of the service extension feature, the user interface and APIs are automatically updated to support these newly configurable parameters.

Zero-Touch CPE Provisioning

Automated, hands-free provisioning of the branch CPE eliminates the need for service calls and allows services to be rolled out more quickly.

Service Packages

1. **Cloud Managed IWAN:** our SD-WAN solution for service providers offers a scalable, multi-tenant solution for delivering SD-WAN services.
2. **Cloud VPN with Virtual Converged Edge:** offers service providers a simple way to offer customers a site-to-site and remote access VPN connectivity service.

Why SD-WAN is important

The global SD-WAN market is forecasted to reach $6B by 2020. Cisco is taking SD-WAN to another level with IWAN. In order to fully capitalize on the market potential, you will need a software-defined services solution that allows your business to:

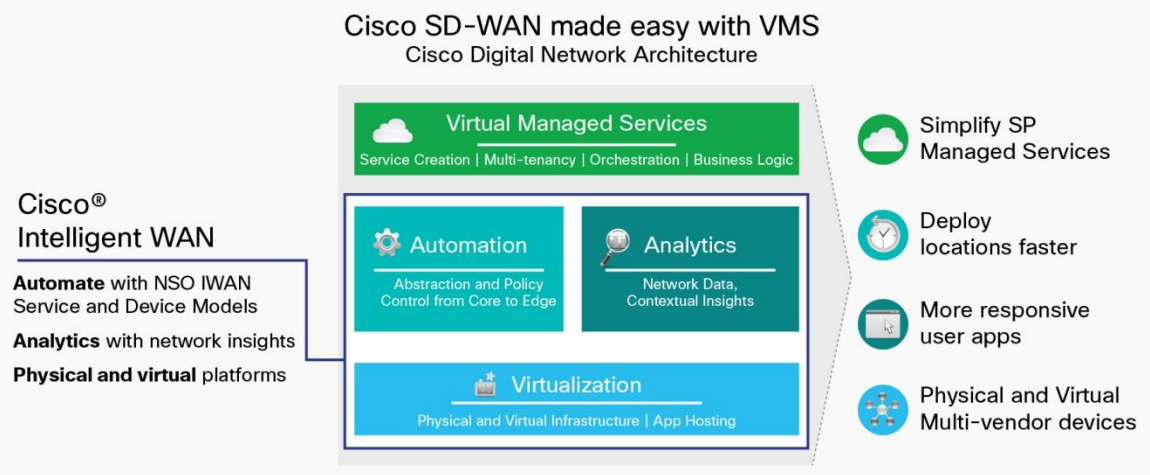
- Automate – Deploy SD-WAN and enable it in minutes across any infrastructure
- Innovate – With your own services offering, integrated into existing IT workflows
- Accelerate – Generate revenue through a customer portal that delivers service packs like SD-WAN

How our Cloud Managed IWAN service can help

Cisco's Cloud Managed IWAN delivers an SD-WAN solution that leverages Cisco's Intelligent WAN enterprise service offering and packages it in a scalable, multi-tenant solution for network operators. IWAN is a comprehensive set of traffic control and security features for the wide-area network that has been integrated into Cisco branch-office routers. IWAN supplies you with all the business-grade capabilities of an MPLS VPN—for example, quality of service (QoS), WAN optimization, and VPN tunneling—that you can put to work using less-expensive connections. VMS delivers a cloud-managed IWAN service that dynamically routes your traffic prioritized by application, endpoint, and network conditions for best-quality experiences. This VMS SD-WAN use case uses the same architecture as IWAN 2.0, with hub border router and master controller functions located in the enterprise data center, complemented by branch devices. These hub and branch locations are connected by an overlay VPN with the following characteristics:

- Transport independent, works over any network supplying IP connectivity.
- Internet traffic offload at each branch location to place traffic on the optimal transport available.
  - Securely encrypted.
  - Identifies applications and makes sure that each application gets the transport SLA it requires from available resources on the network.
  - Self-healing and -optimizing network that continually monitors performance to automatically place workloads on the best path.

Figure 2.

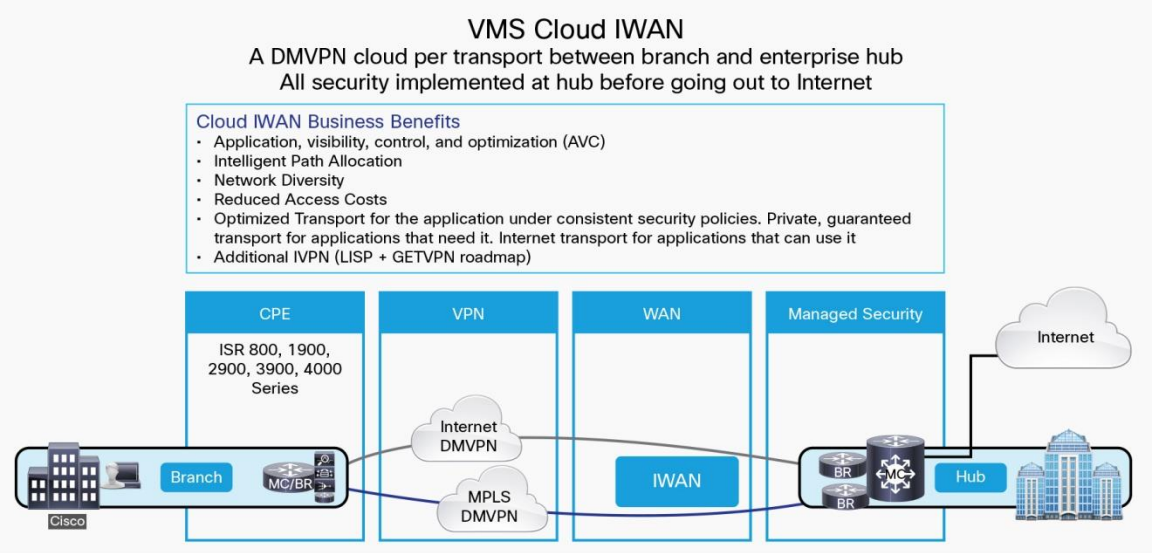


These SD-WAN benefits are delivered via the VMS cloud-managed IWAN, including these features:

- Initial topology contains three devices at the enterprise hub location, a border router for Internet and a border router for MPLS transport, with a master controller. The topology supported at the branch is a single router with one MPLS and one Internet connection.
- Graphical representation of performance (loss, latency, and jitter) for application classes, service and device health (memory and CPU utilization), top applications, and bandwidth consumed.
- User-selectable QoS policy.
- User-selectable and customizable performance routing policy to implement intelligent path control.

- User-selectable business relevance value on a per application basis that can be modified from the default settings for each tenant.
- A CPE configuration synchronization feature that enables an operator to implement additional device configuration during troubleshooting and copy that additional configuration to the system database. This maintains synchronization between the VMS system and the deployed devices, maintaining a single view of device configuration.

Figure 3.



Technical Details

VMS Cloud Managed IWAN Features	Description
Topologies	
Hub and Spoke Hybrid Transport Topology	Hub and Spoke connectivity between Hub site and Branch site utilizing dual path hybrid transport (one mpls plus one internet path).
Three Router Hub	IWAN hub with dedicated routers for functionality and scale. A dedicated PfR Master Controller router along with dedicated Border Routers for MPLS and Internet Transport Networks.
Single router branch	A single router deployed at branch site combining site Master Controller as well as MPLS and Internet Border router functions for the Branch site.
Hub Redundancy	Deploy a Primary Hub, and add a secondary Hub for Hub site redundancy.
Customization	
Customize application business-relevance	Enables the user to change the business relevance of any NBAR2 known application (Relevant, irrelevant, or default) thereby permitting each business to identify which applications are and are not relevant to their business needs. Application which are identified as irrelevant to the business will receive lower preference on the network (see Intelligent Path Control below).
Service Extensions to add to provisioned device CLI	Enables upload of an XML file to insert custom configuration into the orchestrated device. Auto generates form entry field for any required data collection required for configuration.
Sync from CPE feature to absorb manually provisioned CLI	Enables operator to change CLI directly on the router, for example during troubleshooting and sync that configuration to the orchestration database.
Transport	
Ethernet	Only ethernet interface support.
DMVPN Overlay	Topology overlaid with Dynamic Multipoint VPN tunnels for site-to-sites transport.
Application visibility	Graphs for last one hour or last 8 hours can be displayed for all, or selectable traffic classes.
NBAR2 Application Classification	NBAR2 is used to classify the application traffic on ingress at LAN interface.

VMS Cloud Managed IWAN Features	Description
Loss per class	Detect & present a view of the loss per traffic class.
Latency per class	Detect & present a view of the latency per traffic class.
Jitter per class	Detect & present a view of the jitter per traffic class.
Device & Site reporting	
Bandwidth utilization	Bandwidth graphs per hour or last 8 hours available for bandwidth utilization of all WAN links.
CPU utilization	Graph of CPU utilization for last hour or eight hours.
Memory utilization	Graph of memory utilization of the router for last hour or 8 hours.
Link availability	Graph identifying availability of an MPLS or Internet transport interface.
DMVPN overlay Tunnel availability	Graph identifying availability of DMVPN Tunnels over the MPLS or Internet transport.
Top 10 Applications	Graph identifying the 10 ten applications in use per site.
QoS	
Apply SP defined QoS policy per interface	Enables SP to define supported QoS policies and for the tenant to select from the list of supported policies their preferred option.
Intelligent Path Control	
Select MPLS, Internet, none or blackhole per traffic Category	Defines the preferred and backup path for the 6 traffic class categories per RFC 4594 as MPLS, Internet none (which is load balanced) or blackhole (which means drop).
Change the Business Relevance for any NBAR2 known application	Search for any application known by NBAR2, and change the business relevance for any application. Applications which are irrelevant to the business will receive lower priority. Applications which are relevant to the business will be receive a priority classification according to RFC 4594.
Security	
FlexVPN for DMVPN Tunnels	FlexVPN used to secure DMVPN overlay tunnels.
TACACS+ Support	TACACS+ Support for Router AAA.
Per Tenant Router & FlexVPN Tunnel Security Profile	Per Tenant Settings for Router Credentials as well as per FlexVPN DMVPN Security Profile.
User Interface	
Tenant order and configure experience	Order workflow to place and order for a CPE and configure the CPE qith required data.
Tenant monitor via map view and drill down	Tenant can see all sites on a map, and drill down into each one for detailed performance reporting.
SP monitor views for service and devices	SP can see a view of all customers, services and devices provisioned on the system and drill down into each one.
Service, device and overlay status and health	Bar chart view of service, overlay and interface health for one or 8 hour views.
IWAN Router Platform Support	
ISR4451, ASR1001-X, ASR1002-X Support for Hub Routers	Hub Devices supported are ISR4451, ASR1001-X, ASR1002-X.
ISR4000 Series, ISR G2 Series Support for Branch Routers	Branch Devices supported are ISR 4000 Series, ISR 3900 Series, ISR 2900 Series, ISR 1900 Series (non-W), as well as ISR 892FSP and ISR 899G from the ISR 890 Series.
IOS XE Support of 3.16.2S/15.5(3)S2 for ISR 4K and ASR1K Series Routers	Support for IOS XE 3.16.2S/15.5(3)S2 or newer maintenance release within 15.5(3)S train.
IOS Support of 15.5(3)M2a for ISR G2 Series Routers	Support for IOS 15.5(3)M2a or newer maintenance release within 15.5(3)M train.

Cloud VPN Service Package with Virtual Converged Edge

The Cloud VPN service packages offers service providers a simple way to offer customers a site-to-site and remote access VPN connectivity service. This configuration has an advanced option that allows interconnections, regardless of the WAN access method used. It provides secure enterprise access enhanced with Cisco web security. This gives a service provider various options to offer business customers:

- managed access to multiple sites as well as unmanaged access
- remote access
- mobile worker access

This service package is flexible and efficient in how it offers Internet access service. It also combines web security with a common DMZ for all enterprise traffic accessing the Internet.

Benefits and Features

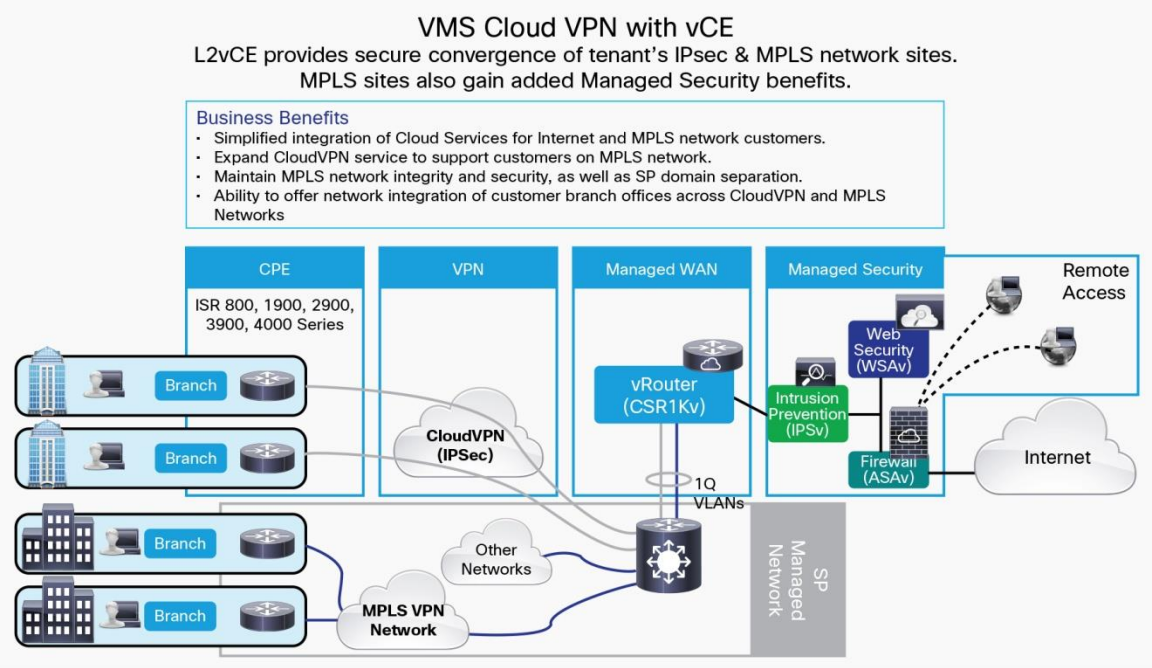
- An enterprise can unify their corporate network by inter-connecting sites through a Cloud VPN vRouter.
- All CPE based enterprise sites can communicate with each other through the vRouter utilizing a Hub-n-Spoke topology.
- All traffic traversing the Hub-n-Spoke topology is secured through encryption across Flex-VPN based IPSec tunnels.
- Mobile users securely access the enterprise using an SSL VPN session terminating on a DMZ providing FW and NAT services.
- All Internet traffic, generating from enterprise CPE based sites or mobile users can be redirect to a virtual Web security appliance (vWSA) for high touch Web access while using a common DMZ.
- By aggregating Internet access, the enterprise can manage Web and general Internet access through a common service policies based on traffic type.
- The Virtual Converged Edge (vCE) functionality allows legacy sites connected via MPLS networks to participate in the Cloud VPN service, in addition to Internet connected sites.

Technical Details

VMS Cloud VPN with Virtual Converged Edge Features	Description
Available on NFVI or Metacloud	• The ability to provide CVPN service across both IPSesc and MPLS attached circuit. This offer is available when VMS is installed on premise. (It is possible in some hosted environments with additional equipment). • Enables secure internet (via VNFs) and NFV services for MPLS sites. • The vCE service will be providing a L2 VLAN transport pre-existing MPLS private network.
Supported VNFs: ASAv, WSA, and AnyConnect	• CVPN Provides additional Virtual Network Function that can be attached to the basic VPN Service. • Cisco Web Security Appliance (WSA) with optional enhanced features (licensed separately). ◦ Sophos. ◦ Advanced Malware Protection (AMP). ◦ McAfee virus protection. • Cisco Adaptive Security Appliance (ASA) firewall functions and remote access. • Cisco AnyConnect Remote client to facilitate remote connection services.

VMS Cloud VPN with Virtual Converged Edge Features	Description
Firewall policy provisioning	• Allows the tenant to make Basic firewall rule changes on the ASAv from VMS portal. • Control traffic sourcing from Inside network to the outside internet. • Control port-forwarding mechanisms to access servers sitting in the inside network (Outside to Inside Port-forwarding).
LTE CPE support	• Support LTE as a primary path for network connectivity. • Integrating CISCO ISR 819/899 CPE support.
Up to 500 Mbps throughput per customer	• Increased CVPN throughput. Customers can order 500Mbps bandwidth.
Up to 750 ASAv remote access users	• Tenant may order 1 to 750- remote VPN Access Users.

Figure 4.



VMS Licensing

Table 1.

VMS Component	Description	License
VMS solution server licenses NSO, ESC, and VMS software integration framework (SIF)	Foundation licenses for the VMS solution, allowing orchestration and automation of the virtual network functions and service policies.	One- or three-year prepaid term license per data center (includes HA license) with three levels of technical support
User interface	Allows improved end-customer experience, e-commerce capabilities, real-time network monitoring, and an operator administrative user interface (portal).	One- or three-year prepaid term license per data center with three levels of technical support
CPE/IWAN orchestration	Enables the VMS NSO, ESC, and VMS SIF to control the end-customer CPE device. A CPE or IWAN orchestration license is required for any CPE device orchestrated by the Cisco VMS solution.	One- or three-year prepaid term license per device with three levels of technical support

VMS Component	Description	License
Cloud VPN Foundation Service Package	Site-to-site IPSec VPN use case service package. Includes 1 VNF (CSR), orchestration, function packs, VM lifecycle management, and SDN capabilities.	One- or three-year prepaid term license per end customer instance with three levels of technical support **Or** Monthly postpaid utility billing based on metered consumption
Cloud VPN Advanced Service Package	Site-to-site IPSec VPN with firewall use case service package. Includes 2 VNFs (CSR and ASAv), orchestration, function packs, VM lifecycle management, and SDN capabilities. Includes ability to add optional VNFs, including web security (WSAv) and/or remote access SSL VPN users.	One- or three-year prepaid term license per end customer instance with three levels of technical support **Or** Monthly postpaid utility billing based on metered consumption

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.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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

Printed in USA C78-738671-01 04/17