Data Sheet

Cisco Nexus 1000V Series Switches for VMware vSphere

Product Overview

Cisco Nexus® 1000V Series Switches provide a comprehensive and extensible architectural platform for virtual machine (VM) and cloud networking. The switches are designed to accelerate server virtualization and multitenant cloud deployments in a secure and operationally transparent manner. Integrated into the VMware vSphere hypervisor and fully compatible with VMware vCloud Director, the Cisco Nexus 1000V Series provides:

- Advanced virtual machine networking based on Cisco® NX-OS Software operating system and IEEE 802.1q switching technology
- Cisco vPath technology for efficient and optimized integration of virtual network services
- Enhanced Virtual extensible LAN (Enhanced VXLAN), supporting cloud networking
- VXLAN gateway for interconnecting VXLAN segments with traditional VLAN segments

These capabilities help ensure that the virtual machine is a basic building block of the data center, with full switching capabilities and a variety of Layer 4 through 7 services in both dedicated and multitenant cloud environments. VXLAN capabilities make sure that the, network isolation among virtual machines can scale beyond traditional VLANs for cloud-scale networking.

Advanced Virtual Machine Networking using Cisco Nexus 1000V Series

The Cisco Nexus 1000V Series Switches are virtual machine access switches for the VMware vSphere environments running the Cisco NX-OS operating system. Operating inside the VMware ESX or ESXi hypervisors, the Cisco Nexus 1000V Series provides:

- Policy-based virtual machine connectivity
- Mobile virtual machine security and network policy
- Nondisruptive operational model for your server virtualization and networking teams

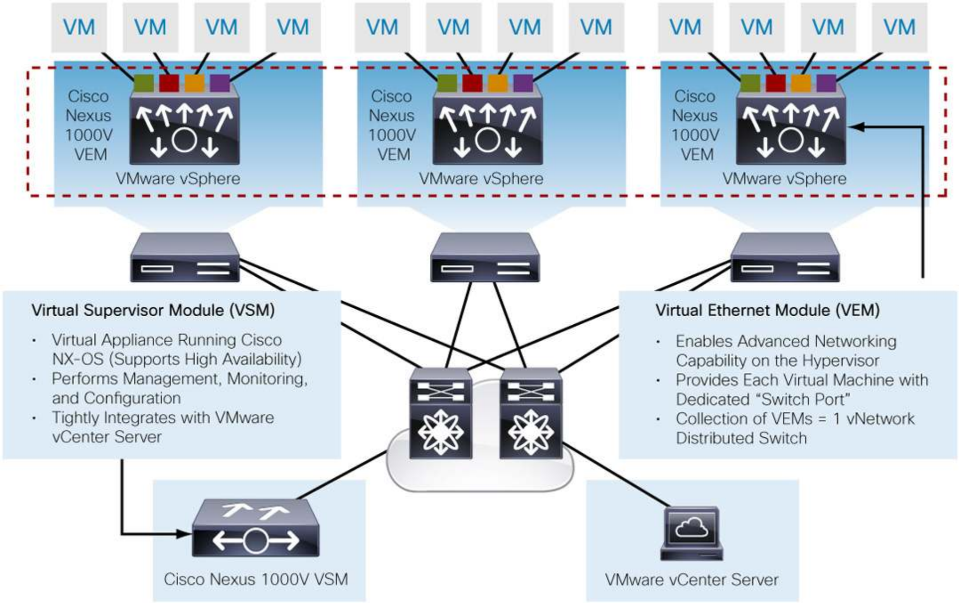
When server virtualization is deployed in the data center, virtual servers typically are not managed the same way as physical servers. Server virtualization is treated as a special deployment, leading to longer deployment time, with a greater degree of coordination among server, network, storage, and security administrators. With the Cisco Nexus 1000V Series, you can have a consistent networking feature set and provisioning process all the way from the virtual machine access layer to the core of the data center network infrastructure. Virtual servers can now use the same network configuration, security policy, diagnostic tools, and operational models as their physical server counterparts attached to dedicated physical network ports. Virtualization administrators can access predefined network policies that follow mobile virtual machines to ensure proper connectivity saving valuable time to focus on virtual machine administration. This comprehensive set of capabilities helps you to deploy server virtualization faster and realize its benefits sooner.

Developed in close collaboration with VMware, the Cisco Nexus 1000V Series is certified by VMware to be compatible with VMware vSphere, vCenter, vCloud Director, ESX, and ESXi, and many other VMware vSphere features. You can use the Cisco Nexus 1000V Series to manage your virtual machine connectivity with confidence in the integrity of the server virtualization and cloud infrastructure.

Product Architecture

The Cisco Nexus 1000V Series Switch has two major components: the virtual Ethernet module (VEM), which runs inside the hypervisor, and the external virtual supervisor module (VSM), which manages the VEMs (Figure 1).

Figure 1. Cisco Nexus 1000V Series Architecture


VM
VM
VM
VM
Cisco Nexus 1000V VEM
VMware vSphere
Virtual Supervisor Module (VSM)
• Virtual Appliance Running Cisco NX-OS (Supports High Availability)
• Performs Management, Monitoring, and Configuration
• Tightly Integrates with VMware vCenter Server
Virtual Ethernet Module (VEM)
• Enables Advanced Networking Capability on the Hypervisor
• Provides Each Virtual Machine with Dedicated "Switch Port"
• Collection of VEMs = 1 vNetwork Distributed Switch
Cisco Nexus 1000V VSM
VMware vCenter Server

Virtual Ethernet Module

The Cisco Nexus 1000V Series VEM runs as part of the VMware ESX or ESXi kernel and replaces the VMware Virtual Switch functionality. The VEM uses the VMware vNetwork Distributed Switch (vDS) API, which was developed jointly by Cisco and VMware, to provide advanced networking capability to virtual machines. This level of integration helps ensure that the Cisco Nexus 1000V Series is fully aware of all server virtualization events, such as VMware vMotion and Distributed Resource Scheduler (DRS). The VEM takes configuration information from the VSM and performs Layer 2 switching and advanced networking functions:

- PortChannels
- Quality of service (QoS)
- Security: Private VLAN, access control lists (ACLs), and port security
- Monitoring: NetFlow, Switch Port Analyzer (SPAN), and Encapsulated Remote SPAN (ERSPAN)

In the event of loss of communication with the VSM, the VEM has Nonstop Forwarding (NSF) capability to continue to switch traffic based on the last known configuration. Thus, the VEM provides advanced switching with data center reliability for the server virtualization environment.

Virtual Supervisor Module

The Cisco Nexus 1000V Series VSM controls multiple VEMs as one logical modular switch. Instead of physical line-card modules, the VSM supports multiple VEMs running in software inside the physical servers. Configuration is performed through the VSM and is automatically propagated to the VEMs. Instead of configuring soft switches inside the hypervisor on a host-by-host basis, administrators can define configurations for immediate use on all VEMs being managed by the VSM, from a single interface.

By using the capabilities of Cisco NX-OS, the Cisco Nexus 1000V Series provides:

- Flexibility and scalability: port profiles, a new Cisco NX-OS feature, provides configuration of ports by category, enabling the solution to scale to a large number of ports. Common software can run all areas of the data center network, including the LAN and SAN.
- High availability: Synchronized, redundant VSMs enable rapid, stateful failover and help ensure an always-available virtual machine network.
- Manageability: The Cisco Nexus 1000V Series can be accessed through the Cisco command-line interface (CLI), Simple Network Management Protocol (SNMP), XML API, and CiscoWorks LAN Management Solution (LMS).

The VSM is also integrated with VMware vCenter Server so that the virtualization administrator can take advantage of the network configuration in the Cisco Nexus 1000V Series.

Essential and Advanced Editions

Starting with the new Cisco Nexus 1000V Series Software Release 2.1, the Cisco Nexus 1000V Series will be offered in two editions: Essential and Advanced.

- Essential Edition: Available at no cost, the Cisco Nexus 1000V Essential Edition provides all the Layer 2 networking features needed to connect virtual applications to the network and integrate into VMware environments, including VXLAN capability, Cisco vPath service insertion, integration with VMware vCloud Director, and a plug-in for management and monitoring in VMware vCenter Server. This free version will enable rapid, low-risk adoption of Cisco's virtual network technology environments. Cisco Technical Assistance Center (TAC) support is optional but recommended.
- Advanced Edition: This is available at the same price as Cisco Nexus 1000V Series Software Release 1.x, the Advanced Edition includes:
    - Cisco Virtual Security Gateway (VSG) for Nexus 1000V Series Switch, a virtual firewall with visibility into virtual machine attributes to build sophisticated compliance policies and logical trust zones between applications (Cisco VSG previously was sold as a separate product).
    - Support for advanced security capabilities, such as Dynamic Host Configuration Protocol (DHCP) snooping, IP source guard, Dynamic Address Resolution Protocol (ARP) Inspection, and Cisco TrustSec® security group access (SGA).
    - VXLAN gateway.

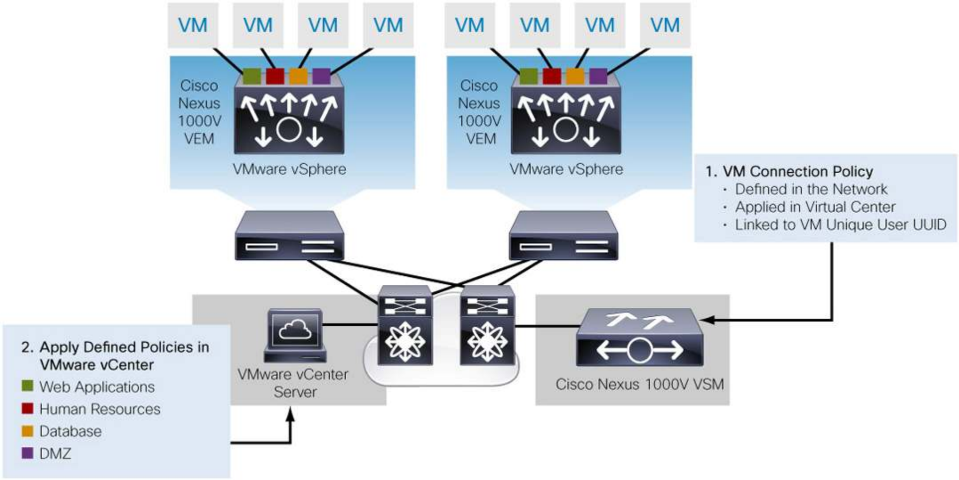
Features and Benefits

The Cisco Nexus 1000V Series provides a common management model for both physical and virtual network infrastructures that includes policy-based virtual machine connectivity, mobility of virtual machine security and network properties, overlay networking with VXLAN, representational state transfer (REST) APIs, and a nondisruptive operational model.

Policy-Based Virtual Machine Connectivity

To complement the ease of creating and provisioning virtual machines, the Cisco Nexus 1000V Series includes the Port profile feature to address the dynamic nature of server virtualization from the network's perspective (Figure 2). Port profiles enable you to define virtual machine network policies for different types or classes of virtual machines from the VSM and then apply the profiles to individual virtual machine virtual NICs (vNICs) through the VMware vCenter GUI for transparent provisioning of network resources. Port profiles are a scalable mechanism for configuring networks with large numbers of virtual machines.

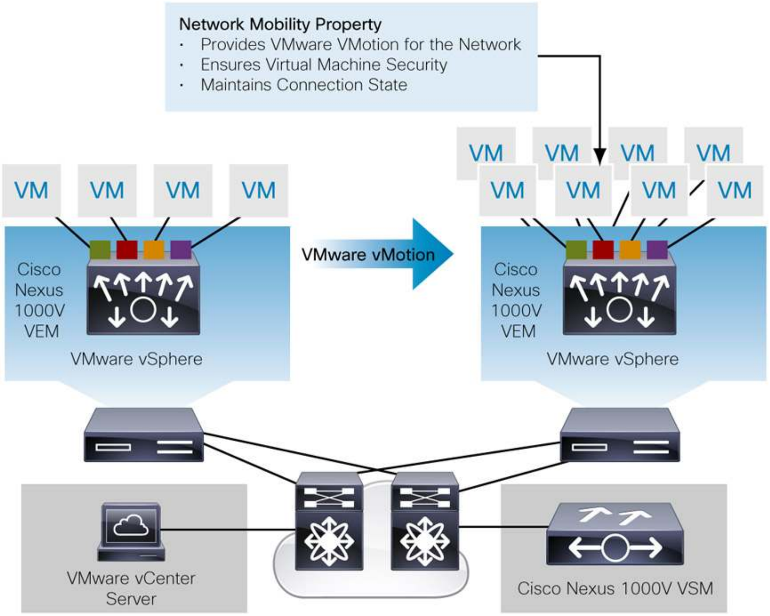
Figure 2. Policy-Based Virtual Machine Connectivity



Mobility of Virtual Machine Security and Network Properties

Network and security policies defined in the port profile follow the virtual machine throughout its lifecycle, whether it is being migrated from one server to another (Figure 3), suspended, hibernated, or restarted. In addition to migrating the policy, the VSM also moves the virtual machine’s network state, such as the port counters and flow statistics. Virtual machines participating in traffic monitoring activities, such as Cisco NetFlow or ERSPAN, can continue these activities uninterrupted by VMware vMotion operations. When a specific port profile is updated, the Cisco Nexus 1000V Series automatically provides live updates to all of the virtual ports using that same port profile. With the ability to migrate network and security policies through VMware vMotion, regulatory compliance is much easier to enforce with the Cisco Nexus 1000V Series, because the security policy is defined in the same way as physical servers and constantly enforced by the switch.

Figure 3. Mobility of Network and Security Properties

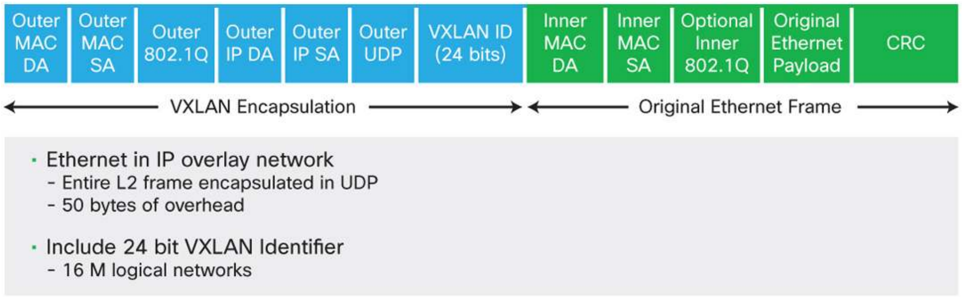

Network Mobility Property
- Provides VMware VMotion for the Network
- Ensures Virtual Machine Security
- Maintains Connection State
VM
VMware vMotion
Cisco Nexus 1000V VEM
VMware vSphere
VMware vCenter Server
Cisco Nexus 1000V VSM

Cloud Networking with Enhanced VXLAN

Cloud-based computing, which requires support for large number of customers and applications, demands even more scalable networks. In particular, each tenant, and even each application within each tenant, requires its own network that is logically isolated from other networks. While traditional servers typically have unique network addresses to help ensure proper communication, VMware vCloud Director duplicates the addresses of virtual machines for each instance of the application. Hence, VMware vCloud Director requires a dedicated logical network for each instance of the application.

Because of this increased need for logical networks, Cisco introduced Virtual Extensible Local Area Network (VXLAN) in the Cisco Nexus 1000V Series. With VXLAN, when a virtual machine sends a frame, it is encapsulated in a UDP packet along with a 24-bit segment identifier that uniquely identifies the bridge domain and provides a dedicated logical network (Figure 10). VXLAN enables an architectural maximum of over 16 M logical networks, supporting large cloud deployments.

Figure 4. Virtual Extensible Local Area Network (VXLAN)

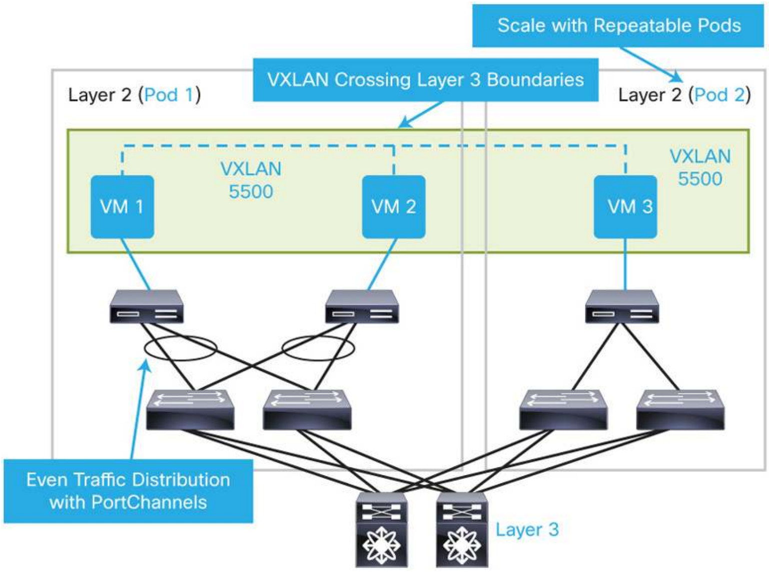


- Ethernet in IP overlay network
  - Entire L2 frame encapsulated in UDP
  - 50 bytes of overhead
- Include 24 bit VXLAN Identifier
  - 16 M logical networks

The Cisco Nexus 1000V Series with VXLAN is fully integrated with VMware vCloud Director, allowing instant provisioning of the new segments. In addition, customers using VXLAN gain the following benefits (Figure 11).

- Because of the Layer 3 nature of UDP, VXLAN traffic can cross Layer 3 boundaries.
- New servers, to accommodate the elastic demands of cloud computing, can be added in different Layer 2 domains. Therefore, VXLAN enables architecture to scale the cloud with repeatable pods.
- Cisco Nexus 1000V with VXLAN provides a consistent operational model from the physical network to the cloud.
- Cloud providers can customize the network policy on a per-tenant basis, allowing differentiated cloud service offerings.
- VXLAN provides efficient use of links in Port Channels with the UDP encapsulation.

Figure 5. Cisco Nexus 1000V Series with VXLAN Benefits


Scale with Repeatable Pods
VXLAN Crossing Layer 3 Boundaries
Layer 2 (Pod 1)
Layer 2 (Pod 2)
VXLAN 5500
VXLAN 5500
VM 1
VM 2
VM 3
Even Traffic Distribution with PortChannels
Layer 3

Enhancements to VXLAN

- Multicast-less mode: VXLAN functions on Cisco Nexus 1000V Series are enhanced to support a multicast-independent solution while preserving the flooding behavior. In this mode, the ingress node replicates the flooded frames instead of depending on the multicast configuration in the physical infrastructure. Each replicated frame is encapsulated in a IP-UDP packet and is sent as a unicast packet to the destination VTEP. The VSM helps identify all the network nodes currently active in a bridge domain.
- Unicast Flood-less mode: VXLAN uses traditional flood-and-learn behavior to learn the MAC addresses of the virtual machines. If the destination MAC address of a frame is unknown, the packet is flooded in the VXLAN segment. In the virtual environment, the VEM knows the MAC address when the virtual machine is attached to the network. This information can be used to learn the MAC address of all the devices in the segment. This capability can eliminate the need to flood to find the frames with unknown MAC addresses.
- VXLAN Trunk Mapping: This feature enables the user to specify the IEEE 802.1q tag to VXLAN segment associations and attach them to the interface. The interface will be part of the mapped VXLAN segments, and any traffic to and from the VXLAN segment is mapped to the corresponding IEEE 802.1q tag.

- Multiple MAC Mode: With this feature, the VEM at the new location generates a special frame to refresh the Layer 2 table entries. This refresh helps ensure that Layer 2 table entries are relearned with the new location from subsequent frames. Until the MAC address is learned, other VEMs will flood the frames, including the new location.

VXLAN Gateway

The VXLAN gateway provides a mechanism for combining a traditional VLAN-based segment with a VXLAN segment to form a single broadcast domain. This mechanism enables the virtual machines in a VXLAN segment to communicate with physical servers, physical service nodes, and physical network nodes such as Layer 3 routes present on the VLAN segments.

The Cisco Nexus 1000V Series provides the VXLAN gateway as a service node running on the Cisco Nexus 1010, 1010-X, 1110-X, and 1110-S appliances. The service node is integrated with the Cisco Nexus 1000V Series Switch and appears as a module on the Cisco Nexus 1000V Series Switch with a common control and management plane. All the provisioning and management of the gateway function is performed on the VSM.

REST API

Cisco NX-OS Release 4.2(1)SV2(1.1) introduced REST APIs, which are used by the virtual computing web client to access Cisco Nexus 1000V Series information such as virtual interfaces and port profiles. The current release introduces dynamic in-field upgradability of these APIs at the infrastructure level using Cisco NX-OS support for plug-ins. New CLI commands are available to manage the REST API plug-in. This plug-in is provided to the customer as a Cisco Connection Online or developer.cisco.com download. Contact your account representative for more details.

The intended use case for these dynamic REST API plug-ins offers a way to provide more API capability to VSMs in service, which may be useful for presenting new information to hypervisor managers or for presenting new deployment integration requirements critical to customers that become known after Cisco Connection Online posting of the current Cisco Nexus 1000V Series firmware release. Another use is to upgrade Release 2.2 in the field with APIs that offer read-write capability of, for example, port profiles. As in the previous release, read-only APIs are provided for the following along with the base Cisco Nexus 1000V Series firmware:

- Uplink
- Limits
- vNIC
- Port profile
- VEM
- Summary (firmware version, etc.)
- License

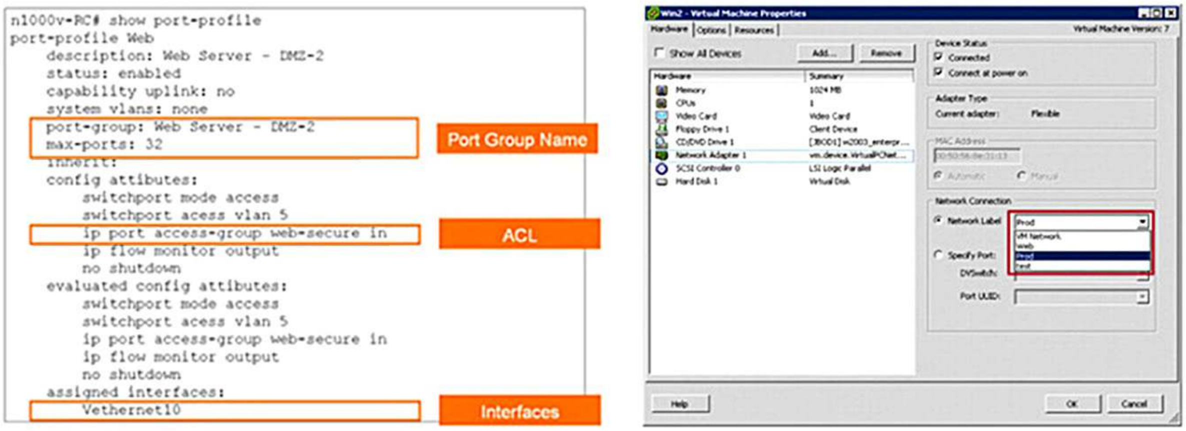
Reinstallation of a REST API plug-in does not affect service for any VSM function except for a brief service interruption at the API endpoint during the uninstallation of the existing plug-in and installation of the new one.

Nondisruptive Operational Model

Because of its close integration with VMware vCenter Server, the Cisco Nexus 1000V Series allows virtualization administrators to continue using VMware tools to provision virtual machines. At the same time, network administrators can provision and operate the virtual machine network the same way they do the physical network using Cisco CLI and SNMP along with tools such as ERSPAN and NetFlow (Figure 4). While both teams work independently, using familiar tools, the Cisco Nexus 1000V Series enforces consistent configuration and policy throughout the server virtualization environment. This level of integration lowers the cost of ownership while supporting various organizational boundaries among server, network, security, and storage teams.

Inside VMware vCenter Server, virtual machines are configured as before. Instead of defining network configuration in VMware vCenter Server, port profiles defined on the VSM are displayed by VMware vCenter as port groups. Virtualization administrators can take advantage of preconfigured port groups and focus on virtual machine management, while network administrators can use port profiles to apply policy for a large number of ports at the same time. Together, both teams can deploy server virtualization more efficiently and with lower operational cost.

Figure 6. Nondisruptive Operational Model



```
n1000v-RC# show port-profile
port-profile Web
    description: Web Server - DMZ-2
    status: enabled
    capability uplink: no
    system vlans: none
    port-group: Web Server - DMZ-2
    max-ports: 32
    inherit:
    config attibutes:
        switchport mode access
        switchport acess vlan 5
        ip port access-group web-secure in
        ip flow monitor output
        no shutdown
    evaluated config attibutes:
        switchport mode access
        switchport acess vlan 5
        ip port access-group web-secure in
        ip flow monitor output
        no shutdown
    assigned interfaces:
        Vethernet10
```

Win2 - Virtual Machine Properties

Virtual Machine Version: 7

Hardware	Summary
Memory	1024 MB
CPUs	1
Video Card	Video Card
Floppy Drive 1	Client Device
CD/DVD Drive 1	[JBOD1] w2003_enterpr...
Network Adapter 1	vm.device.VirtualPCNet...
SCSI Controller 0	LSI Logic Parallel
Hard Disk 1	Virtual Disk

Device Status
☑ Connected
☑ Connect at power on

Adapter Type
Current adapter: Flexible

Network Connection
● Network Label: Prod
○ Specify Port:

Network Administrator View of Network Policy

Virtualization Administrator Applying Network Policy

Virtualized Network Services with Cisco vPath

In addition to virtual machine switching, the Cisco Nexus 1000V Series supports Cisco vPath to provide a single architecture supporting multiple Layer 4 through 7 network services. In the Cisco vPath architecture, Virtual Service Nodes can provide a variety of network services, such as virtual firewall, load balancing, and WAN acceleration. Specifically, the Cisco vPath architecture provides:

- Intelligent traffic steering:
    - Redirect traffic from server requesting network service to the virtual service node (VSN)
    - Extend port profile to include network service profile
- Flexible deployment:
    - Each VSN can serve multiple physical servers
    - VSN can be hosted on a separate or dedicated server

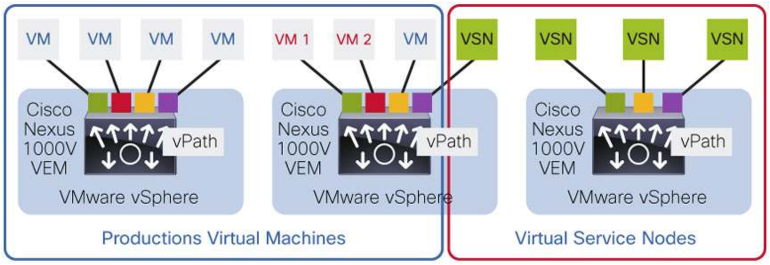
- Network service acceleration:
  - Network Service Decision Caching: Cisco Nexus 1000V Series remembers network service policy from prior traffic, reducing traffic steering
  - Performance of virtual network services can be accelerated through enforcement in the hypervisor kernel

In Figure 5, when VM 1 sends a packet to VM 2 requiring virtualized network services, the VEM forwards the request to a VSN, possibly on a different host. The VSN responds to the originating VEM with the suitable action: for example, sending or dropping packets in this flow. The original VEM caches and executes the decision that the VSN requested. For future packets from VM 1 to VM 2, the VEM can implement the virtualized network service without requests to the VSN. Hence, the VEM:

- Implements the virtualized network service decision
- Accelerates network service because it is running in the hypervisor kernel
- Scales network service because the VEM is on every hypervisor host

In addition, the VSN can be placed on any host, providing greater flexibility and separation of production workload and network services. In fact, the vPath architecture is designed to support a variety of network services.

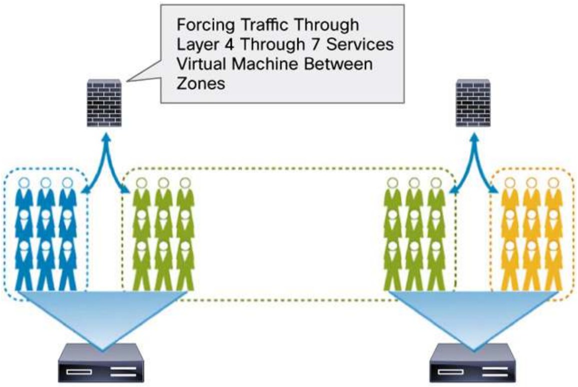
Figure 7. Cisco vPath Architecture



The first VSN to use vPath is the Cisco Virtual Security Gateway (VSG). Cisco VSG enforces attribute-based security policies for single and multitenant environments. Because Cisco VSG is offered as a virtual appliance, customers can scale its deployment with the vPath architecture and by deploying more Cisco VSG appliances on demand.

For customers that have Layer 4 through 7 services virtual machines that do not support vPath, Cisco Nexus 1000V Series can provide policy-based provisioning through virtual service domains (VSDs). A VSD groups virtual machines, which may be on multiple servers, into zones and forces traffic traveling between zones through a Layer 4 through 7 services virtual machine, such as a firewall, including VMware vShield Zones (Figure 6). This extensible capability makes the Cisco Nexus 1000V Series much easier to use with a variety of Layer 4 through 7 services.

Figure 8. Virtual Service Domain


Forcing Traffic Through Layer 4 Through 7 Services Virtual Machine Between Zones

Cisco ASA1000V

The Cisco ASA1000V enables a broad set of multitenant workloads that have varied security profiles to share a common infrastructure in a virtual data center. By associating one or more virtual machines in a network with distinct security profiles, the Cisco ASA1000V helps ensure that access to and from these virtual machines is controlled and monitored through established security policies.

Integrated with the Cisco Nexus 1000V Series Switches and Cisco Prime Network Services Controller, the Cisco ASA1000Vallows administrative segregation across security and server teams that enables collaboration, eliminates administrative errors, and simplifies audits.

Cisco Nexus 1100 Series Cloud Services Platform

Deploying a VSM as a virtual appliance is one approach. However, for network administrators who prefer a dedicated computing appliance for hosting the VSM and other virtual networking services, Cisco offers the Nexus 1110-X and 1110-S Cloud Services Platforms. The Virtual Security Gateway (VSG), Network Analysis Module (NAM), Data Center Network Manager (DCNM), VXLAN Gateway, and Imperva Web Application Firewall (WAF) are other networking services that can be hosted on the Cloud Services Platform. The appliances are deployed in pairs for High Availability (HA) in production environments. (Figure 9).

Figure 9. Cisco Nexus 1110-X Cloud Services Platform

With the Cisco Nexus 1110-X and 1110-S, network administrators no longer have to rely on server administrators to run VSMs and other virtual services to manage their virtual switching infrastructure. Hence, server and network administrators can reduce the complexity and interdependency of a virtualized data center deployment. See http://www.cisco.com/go/1100 for additional information on the Nexus 1100 Series Cloud Services Platform.

Optimization for Server Virtualization and Cloud Deployment

Differentiated Quality of Service

Today, network interfaces are often dedicated to a particular type of traffic, such as VMware Console or vMotion. With the Cisco Nexus 1000V Series, all the network interface cards (NICs) on the server can be treated as a single logical channel with QoS attached to each type of traffic. With VMware vSphere Version 4.1, the Cisco Nexus 1000V Series can even provide different service-level agreements (SLAs) for production virtual machines. Consequently, the bandwidth to the server can be more efficiently utilized with virtualization of network-intensive applications.

Secure Desktop Virtualization

The number of virtual machines running on a server is increasing quickly, especially in a virtual desktop environment, similar to the way that CPU performance follows Moore's Law. With a large population of virtual machines on a server, an infected virtual machine can quickly spread a virus or malware to other virtual machines on the same server. VMware vMotion can then migrate an infected virtual machine to another server, spreading the virus. Consequently, virtual machines must have the same security policy as physical servers.

The Cisco Nexus 1000V Series includes the Cisco Integrated Security features that are found on Cisco physical switches to prevent a variety of attack scenarios (Table 1). For example, a rogue virtual machine can spoof its MAC and IP addresses so that it appears to be an existing production virtual machine, send a rogue ARP transaction mimicking the way that VMware vMotion announces the location of a migrated virtual machine, and divert traffic from the production virtual machine to the rogue virtual machine. With Cisco Integrated Security features, this type of attack can easily be prevented with simple networking policy. Because server virtualization is being used for desktop and server workloads, it is critical that this type of security feature be deployed for the proper operation of a virtualized environment.

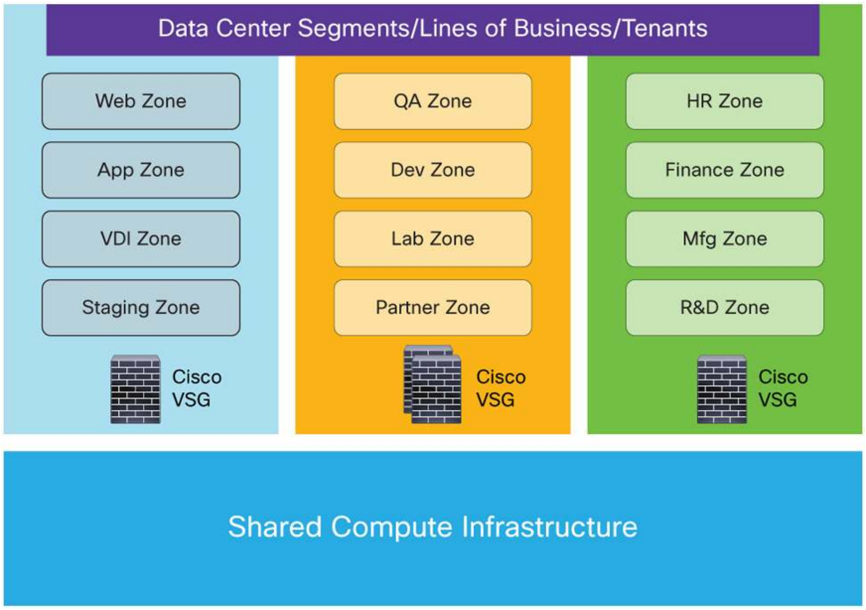
Table 1. Cisco Integrated Security Features

Feature	Capability	Prevents
Cisco TrustSec	• Cisco TrustSec uniquely provides a policy-based platform, the Cisco Identity Services Engine (ISE), that offers integrated posture, profiling, and guest services to make context-aware access control decisions	• Insecure access • Compromising of data and resources
Port security	• Restricts MAC addresses on a port	• MAC address spoofing by rogue virtual machine
IP source guard	• Maps IP addresses to MAC addresses	• IP and MAC address spoofing
Dynamic ARP Inspection	• Monitors virtual machine ARP transactions, which are also used for VMware vMotion	• ARP cache poisoning on other virtual machines, hosts, and network devices
DHCP snooping	• Prevents DHCP client requests from reaching untrusted entities • Prevents untrusted entities from acting as DHCP servers • Rate-limits DHCP requests to prevent denial-of-service (DoS) attacks	• Rogue DHCP servers • Denial of service to DHCP services

Secure Multitenancy

With the capabilities of server virtualization, customers can consolidate disparate workloads onto a single set of computing infrastructure. However, these workloads must be logically separated for either administrative or regulatory compliance purposes. With the introduction of a virtual firewall, such as Cisco VSG, this logical isolation can be achieved easily and efficiently. In fact, in this type of deployment, workloads can be dynamically created depending on the business demands. As shown in Figure 9, the Cisco Nexus 1000V Series with Cisco vPath supports this type of deployment with Cisco VSG and allows customers to build their own private clouds within the enterprise.

Figure 10. Secure Multitenancy with Cisco Nexus 1000V Series Supporting Cisco VSG



Cisco NX-OS Software Overview

Cisco NX-OS Software is a data-center-class operating system built with modularity, resiliency, and serviceability at its foundation. Based on the industry-proven Cisco MDS 9000 SAN-OS Software, Cisco NX-OS Software helps ensure continuous availability and sets the standard for mission-critical data center environments. The self-healing and highly modular design of Cisco NX-OS makes zero-impact operations a reality and delivers exceptional operational flexibility. Focused on the requirements of the data center, Cisco NX-OS provides a comprehensive feature set that fulfills the Ethernet and storage networking requirements of present and future data centers. With a CLI like that of Cisco IOS® Software, Cisco NX-OS provides state-of-the-art implementations of relevant networking standards as well as a variety of true data-center-class Cisco innovations.

Cisco NX-OS Software Features and Benefits

- Software compatibility: Cisco NX-OS Software Release 4.0 interoperates with Cisco products running any variant of the Cisco IOS Software operating system. Cisco NX-OS Software Release 4.0 also interoperates with any networking OS that conforms to the networking standards listed as supported in this data sheet.
- Common software throughout the data center: Cisco NX-OS simplifies the data center operating environment and provides a unified OS designed to run all areas of the data center network, including the LAN, SAN, and Layer 4 through 7 network services.
- Modular software design: Cisco NX-OS modular processes are instantiated on demand, each in a separate protected memory space. Thus, processes are started and system resources allocated only when a feature is enabled. The modular processes are governed by a real-time preemptive scheduler that helps ensure the timely processing of critical functions.

- In-Service Software Upgrade (ISSU): The Cisco Nexus 1000V Series helps to enable server and network administrators to transparently upgrade the VEM and VSM software, reducing downtime and allowing customers to integrate the newest features and functions with little or no negative effect on network operations. Network and server administrators can upgrade the VSM and VEM during different maintenance windows or in batches and continue operation of the Cisco Nexus 1000V Series. The VMware vCenter Server and Cisco Nexus1000V Series can be upgraded at the same time.
- Quick development of enhancements and problem fixes: The modularity of Cisco NX-OS allows new features, enhancements, and problem fixes to be integrated into the software quickly. Thus, modular fixes can be developed, tested, and delivered in a short time span.
- SNMP and XML API: Cisco NX-OS complies with SNMPv1, v2, and v3. A comprehensive collection of MIBs is supported. Cisco NX-OS also has a full-featured, documented XML API, enabling integration with third-party management tools.
- Role-Based Access Control (RBAC): With RBAC, Cisco NX-OS allows administrators to limit access to switch operations by assigning roles to users. Administrators can customize and restrict access to the users who require it.

Product Specifications

VMware Product Compatibility

The Cisco Nexus 1000V Series is VMware Ready Certified to be compatible with VMware vSphere as a vNetwork Distributed Switch with support for VMware ESX and ESXi hypervisors and integration with VMware vCenter Server.

VMware vSphere Feature Compatibility

The Cisco Nexus 1000V Series is supported with the following VMware vSphere features:

- VMware vMotion
- VMware Distributed Resource Scheduler (DRS)
- VMware High Availability (HA)
- VMware Storage vMotion
- VMware Fault Tolerance (FT)
- VMware Update Manager
- VMware vShield Zones
- VMware Auto Deploy

Maximum Supported Configurations

- 128 VMware ESX or ESXi hosts per VSM
- 4096 virtual Ethernet ports per VMware vDS, with 300 virtual Ethernet ports per physical host
- 2048 active VLANs
- 2048 active VXLANs
- 2048 port profiles
- 32 physical NICs per physical host
- 256 PortChannels per VMware vDS, with 8 PortChannels per physical host

Layer 2 Features

- Layer 2 switch ports and VLAN trunks
- IEEE 802.1q VLAN encapsulation
- Link Aggregation Control Protocol (LACP): IEEE 802.3ad
- Advanced PortChannel hashing based on Layer 2, 3, and 4 information
  - Source MAC address (default)
  - Virtual port ID
  - Destination IP address and Layer 4 port
  - Destination IP address, Layer 4 port, and VLAN
  - Destination IP address and VLAN
  - Destination MAC address
  - Destination Layer 4 port
  - Source and destination IP addresses and Layer 4 port
  - Source and destination IP addresses, Layer 4 port, and VLAN
  - Source and destination IP addresses and VLAN
  - Source and destination MAC addresses
  - Source and destination Layer 4 port
  - Source IP address and Layer 4 port
  - Source IP address, Layer 4 port, and VLAN
  - Source IP address and VLAN
  - Source MAC address
  - Source Layer 4 port
  - VLAN only
- Virtual PortChannel Host Mode
- Private VLANs with Promiscuous, Isolated, and Community ports
- Private VLAN on trunks
- Internet Group Management Protocol (IGMP) Snooping Versions 1, 2, and 3
- Jumbo-frame support; up to 9216 bytes
- Integrated loop prevention with Bridge Protocol Data Unit (BDPU) filter without running Spanning Tree Protocol

QoS Including Virtual Machine Granularity

- Classification
  - Access group (ACL)
  - IEEE 802.1p CoS
  - IP Type of Service: IP precedence or DSCP (RFC 2474)
  - User Datagram Protocol (UDP) ports
  - Packet length

- Marking
    - Two Rate Three Color Marker (RFC 2698)
    - IEEE 802.1p CoS marking
    - IP Type of Service: IP precedence or DSCP (RFC 2474)
- Traffic policing (transmit- and receive-rate limiting)
- Class-based Weighted Fair Queuing (only on VMware vSphere 4.1 or later versions)
- Modular QoS CLI (MQC) compliance

Security

- Ingress and egress ACLs on Ethernet and virtual Ethernet ports
- Standard and extended Layer 2 ACLs:
    - MAC address and IPv4
    - Source MAC address
    - Destination MAC address
    - EtherType
    - VLAN
    - Class of service (CoS)
- Standard and extended Layer 3 and 4 ACLs:
    - Source IP
    - Destination IP
    - DSCP
    - Precedence
    - Protocol (TCP, UDP, Internet Control Message Protocol [ICMP], and IGMP)
    - Source port
    - Destination port
    - TCP flags
    - ICMP and IGMP types
    - ICMP code
- Port-based ACLs (PACLs)
- Named ACLs
- ACL statistics
- Cisco Integrated Security Features
    - Port security
    - IP source guard
    - Dynamic ARP inspection
    - DHCP snooping
- Virtual Service Domain for Layer 4 through 7 services virtual machine

Virtualized Network Services Support

- Cisco vPath with Layer 2 and Layer 3 support for connectivity between Virtual Ethernet Module and Virtual Service Node
- Virtual Service Domain

VXLAN

- Scalable network isolation
- Fully integrated with VMware vCloud Director
- Port statistics
- Port security
- ACL
- QoS
- Cisco vPath
- Multicast-less mode
- Unicast Flood-less mode
- VXLAN Trunk Mode
- Multi Mac Mode

High Availability

- Stateful supervisor failover: Synchronized redundant supervisors are always ready for failover while maintaining a consistent and reliable state.
- Nonstop forwarding: Forwarding continues despite loss of communication between the VSM and VEM.
- Process survivability: Critical processes run independently for ease of isolation, fault containment, and upgrading. Processes can restart independently in milliseconds without losing state information, affecting data forwarding, or affecting adjacent devices or services.
- Redundant VSM support across two datacenters: VSM can be distributed across two Datacenters.
- Branch-office VEM support: This feature extends the datacenter to branch office with support for hosts in branch offices and VSMs in the central datacenter.

Management

- VSM installation wizard for virtualization and network administrators
  - Installs VSM on its own VEM
  - Creates physical NIC port profiles
  - Configures VSM high availability
  - Configures VSM-to-VEM communication options
- VMware vCenter plug-in
  - Provides holistic view of the virtual network from VMware vCenter Server
  - Installs directly into VMware vCenter
  - Provides dashboard view
  - Provides license use view

  - Provides switch and host view
- Installer application
  - Is a simple piece of software for a PC
  - Provides single-pane view for entire installation process
  - Installs both VSM and VEM
  - Supports deployment of redundant VSMs
- VMware vTracker support
  - Adds visibility into the virtual and physical networks
  - Provides views of VMware vMotion, VLAN, and upstream network
  - Provides views of virtual machine information, virtual machine vNIC, and module physical NIC (pNIC)
- Layer 2 and 3 connectivity between VSM and VEM
- Cisco NX-OS CLI console
- ISSU
- SPAN: Local port mirroring of physical interface, PortChannel, VLAN, and port profile
- Enhanced Remote SPAN (ERSPAN) Type III: Remote port mirroring
- NetFlow Version 9 with NetFlow Data Export (NDE)
- Cisco Discovery Protocol Versions 1 and 2
- ACL Logging
- SNMP (read) v1, v2, and v3
- SNMP ACL
- XML API support
- Enhanced SNMP MIB support
- SSH v2
- Telnet
- Authentication, authorization, and accounting (AAA)
- TACACS+
- RADIUS
- Cisco TrustSec
  - SGT
  - SGT Exchange Protocol over TCP (SXP)
- Syslog
  - Includes VMware vMotion events
- RBAC
- Ingress and egress packet counters per interface
- Network Time Protocol (NTP) RFC 1305
- Domain Name Services (DNS) for management interfaces
- CiscoWorks LMS v3.1, v3.0.1, and v2.6 with Service Pack 1 (SP1)

SNMP MIBs

- Generic MIBs
  - CISCO-TC
  - SNMPv2-MIB
  - SNMP-COMMUNITY-MIB
  - SNMP-FRAMEWORK-MIB
  - SNMP-NOTIFICATION-MIB
  - SNMP-TARGET-MIB
- Configuration MIBs
  - ENTITY-MIB
  - IF-MIB
  - CISCO-ENTITY-EXT-MIB
  - CISCO-ENTITY-FRU-CONTROL-MIB
  - CISCO-FLASH-MIB
  - CISCO-IMAGE-MIB
  - CISCO-CONFIG-COPY-MIB
  - CISCO-ENTITY-VENDORTYPE-OID-MIB
  - ETHERLIKE-MIB
  - CISCO-LAG-MIB
  - MIB-II
- Monitoring MIBs
  - NOTIFICATION-LOG-MIB
  - CISCO-PROCESS-MIB
  - CISCO-VIRTUAL-NIC-MIB
- Security MIBs
  - CISCO-AAA-SERVER-MIB
  - CISCO-COMMON-MGMT-MIB
  - CISCO-PRIVATE-VLAN-MIB
- Miscellaneous MIBs
  - CISCO-CDP-MIB
  - CISCO-LICENSE-MGR-MIB
  - CISCO-ENTITY-ASSET-MIB

Supported Standards

Table 2 presents IEEE compliance information, and Table 3 presents RFC compliance information.

Table 2. IEEE Compliance

Standard	Description
IEEE 802.1p	CoS tagging for Ethernet frames
IEEE 802.1q	VLAN tagging
IEEE 802.3	Ethernet
IEEE 802.3ad	Link Aggregation Control Protocol (LACP)

Table 3. RFC Compliance

Standard	Description
IP Services	
RFC 768	User Data Protocol (UDP)
RFC 791	IP
RFC 792	Internet Control Message Protocol (ICMP)
RFC 793	TCP
RFC 826	Address Resolution Protocol (ARP)
RFC 854	Telnet
RFC 894	IP over Ethernet
RFC 1305	Network Time Protocol Version 3
RFC 1492	TACACS+
RFC 1591	Domain Name System (DNS) Client
RFC 2068	HTTP server
RFC 2138	RADIUS authentication
RFC 2139	RADIUS accounting
IP Multicast	
RFC 1112	IGMPv1 snooping
RFC 2236	IGMPv2 snooping
RFC 3376	IGMPv3 snooping
Quality of Service	
RFC 2474	DSCP marking
RFC 2698	Two Rate Three Color Marker

System Requirements

- VMware vSphere Enterprise Plus Version 4.1 or later; supports VMware vSphere 5.5
- Compatible with VMware vCloud Director 1.5 or later
- Cisco Nexus 1000V Series VSM
  - VSM can be deployed as a virtual machine on VMware ESX or ESXi 3.5U2 or later or ESX or ESXi 4.0
  - Hard disk: 3 GB
  - RAM: 2 GB
  - 1 virtual CPU at 1.5 GHz
- Cisco Nexus 1000V Series VEM
  - VMware ESX or ESXi 4.0 or later
  - Hard disk space: 6.5 MB
  - RAM: 150 MB
- Number of VLANs for Layer 2 connectivity between VSM and VEM: 1
- Server on VMware Hardware Compatibility List (http://www.vmware.com/go/hcl)
- Compatible with any upstream physical switches, including all Cisco Nexus and Cisco Catalyst® switches as well as Ethernet switches from other vendors
- VXLAN requires physical switches supporting multicast (RFC 2236)

Licensing and Ordering Information

The Cisco Nexus 1000V Series is licensed based on the number of physical CPUs on the server on which the VEM is running. Table 4 presents ordering formation for the Cisco Nexus 1000V Series.

Table 4. Cisco Nexus 1000V Series Ordering Information

Part Number	Description
N1K-VLCPU-01=	Nexus 1000V Paper CPU License Qty 1-Pack
N1K-VLCPU-04=	Nexus 1000V Paper CPU License Qty 4-Pack
N1K-VLCPU-16=	Nexus 1000V Paper CPU License Qty 16-Pack
N1K-VLCPU-32=	Nexus 1000V Paper CPU License Qty 32-Pack
L-N1K-VLCPU-01=	Nexus 1000V eDelivery CPU License Qty 1-Pack
L-N1K-VLCPU-04=	Nexus 1000V eDelivery CPU License Qty 4-Pack
L-N1K-VLCPU-16=	Nexus 1000V eDelivery CPU License Qty 16-Pack
L-N1K-VLCPU-32=	Nexus 1000V eDelivery CPU License Qty 32-Pack

Warranty

The Cisco Nexus 1000V Series has a 90-day limited software warranty. For more information about the Cisco Nexus 1000V Series warranty, see http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html.

Service and Support

Cisco Software Application Support plus Upgrades (SASU) is a comprehensive support service that helps you maintain and enhance the availability, security, and performance of your business-critical applications. Cisco SASU includes the following resources:

- Software updates and upgrades: The Cisco SASU service provides timely, uninterrupted access to software updates and upgrades to help you keep existing systems stable and network release levels current. Update releases, including major upgrade releases that may include significant architectural changes and new capabilities for your licensed feature set, are available by software download from Cisco.com or by CD-ROM shipment.
- Cisco TAC: Cisco TAC engineers provide accurate, rapid diagnosis and resolution of software application problems to help you reduce outages and performance degradation. These specialized software application experts are trained to support the Cisco Nexus 1000V Series. Their expertise is available to you 24 hours a day, 365 days a year, by telephone, fax, email, or the Internet.
- Online support: Cisco SASU provides access to a wide range of online tools and communities to help you resolve problems quickly, support business continuity, and improve competitiveness.

For More Information

- For more information about the Cisco Nexus 1000V Series, visit http://www.cisco.com/go/nexus1000v.
- For more information about the Cisco Nexus 1100 Series Cloud Services Platform, visit http://www.cisco.com/go/1100.
- For more information about Cisco Virtual Security Gateway, visit http://www.cisco.com/go/vsg.
- For more information about Cisco Nexus 1000V community, visit http:www.cisco.com/go/nexus1000vcommunity.
- For more information about Cisco NX-OS Software, visit http://www.cisco.com/go/nxos.
- For more information about VMware vSphere, visit http://www.vmware.com/go/vsphere.
- For more information about VMware vCloud Director, visit http://www.vmware.com/products/vcloud-director/.
- For more information about how Cisco and VMware are working together, visit http://www.vmware.com/cisco.
- Nexus 1000V is also available for Microsoft Hyper-V. For more information, visit http://www.cisco.com/en/US/products/ps13056/index.html.

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 C78-492971-16 09/13