

# Cisco Nexus 1010 Virtual Services Appliance Version 2.2

## Deployment Guide

June 2013

---

<a href="#">Overview</a>	3
<a href="#">Audience</a>	3
<a href="#">Introduction</a>	3
<a href="#">Cisco Nexus 1010 and 1010-X Components</a>	4
<a href="#">High Availability</a>	5
<a href="#">Network Connectivity</a>	6
<a href="#">Management VLAN</a>	7
<a href="#">Control VLAN</a>	7
<a href="#">Network Connectivity Options</a>	7
<a href="#">Network Connection Option 1</a>	7
<a href="#">Network Connection Option 2</a>	8
<a href="#">Network Connection Option 3</a>	10
<a href="#">Network Connection Option 4</a>	11
<a href="#">Network Option 5 (Flexible Network)</a>	13
<a href="#">Deployment Considerations</a>	15
<a href="#">Topology Examples</a>	16
<a href="#">Cisco Nexus 1000V Backup and Restore Procedure</a>	20
<a href="#">Virtual Service Blade Support</a>	21
<a href="#">Feature Enhancements</a>	22
<a href="#">Appendix A: Quick Configuration Guide</a>	22
<a href="#">Cisco Nexus 5000 Series Upstream Configurations</a>	23
<a href="#">Primary Cisco Nexus 1010 Setup</a>	24
<a href="#">Secondary Cisco Nexus 1010 Setup</a>	27
<a href="#">Verify Cisco Nexus 1010 Setup</a>	28
<a href="#">Instantiate Cisco Nexus 1000V VSM (First VSB)</a>	29
<a href="#">Verify Cisco Nexus 1000V VSB</a>	30
<a href="#">Cisco Nexus 1010 Technical Documentation</a>	31
<a href="#">For More Information</a>	31

---

## Overview

This document provides design guidelines for deploying the Cisco Nexus™ 1010 Virtual Services Appliance. For detailed feature-level configuration documentations, please refer to the respective Cisco® product configuration guides found at [Cisco.com/go/1010](http://Cisco.com/go/1010). Links to additional information can be found in the “For More Information” section of this document.

## Audience

This document is intended for network architects, network engineers, virtualization administrators, and server administrators interested in understanding and deploying the Cisco Nexus 1000V Virtual Access Switch utilizing the Cisco Nexus 1010 in a Cisco data center environment.

## Introduction

The Cisco Nexus® 1010 Virtual Services Appliance (Figure 1) is a member of the Cisco Nexus 1000V Series Switches portfolio. It hosts the Nexus 1000V Virtual Supervisor Modules (VSMs) and provides support for Virtual Service Blades (VSBs) to offer a more comprehensive solution for virtual access switching. Because the Cisco Nexus 1010 provides dedicated hardware for the VSM, it makes virtual access switch deployment easier for the network administrator. In addition, support for additional VSBs such as the Virtual Security Gateway (VSG), the Cisco Prime Network Analysis Modules (NAM), the Data Center Network Manager (DCNM) makes the Cisco Nexus 1010 a crucial component of a virtual access switch solution.

**Figure 1.** Cisco Nexus 1010 Virtual Services Appliance



## Member of Cisco Nexus 1000 Family

Cisco Nexus® 1000V Series Switches are virtual machine access switches. They are intelligent switches designed for hypervisor environments running the Cisco® NX-OS Software operating system. Operating inside the hypervisor, the Cisco Nexus 1000V Series supports server virtualization technology to provide:

- Policy-based virtual machine connectivity
- Mobile virtual machine security and network policy
- Non-disruptive operational model for 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 times, with a greater degree of coordination needed 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 operation models as their physical server counterparts attached to dedicated physical network ports. Virtualization administrators can access a predefined network policy that follows mobile virtual machines to help ensure proper connectivity, saving valuable

---

time to all you to focus on virtual machine administration. This comprehensive set of capabilities helps you deploy server virtualization and achieve its benefits more quickly.

## Cisco Nexus 1010 and 1010-X Components

The Cisco Nexus 1010 offers a physical platform for deploying and managing the Cisco Nexus 1000V VSMs and other virtual services. For the Cisco Nexus 1010, the platform refers to the physical server coupled with the Cisco Nexus 1010 Manager software, which houses multiple Cisco VSBs.

### Cisco Nexus 1010 Physical Components

The physical components of the Cisco Nexus 1010 are based on the Cisco UCS™ C200M2 High-Density Rack-Mount Server containing:

- Two Intel X5650 processors, with 2.66 GHz and 6 cores
- Four 4-GB RDIMM RAM
- Two 500-GB SATA-II HDD
- One Broadcom Quad Port Gigabit Ethernet 5709 network interface card (NIC)
- One serial port
- One rail kit

### Cisco Nexus 1010-X Physical Components

The physical components of the Cisco Nexus 1010-X are based on the Cisco UCS C200M2 physical appliance containing:

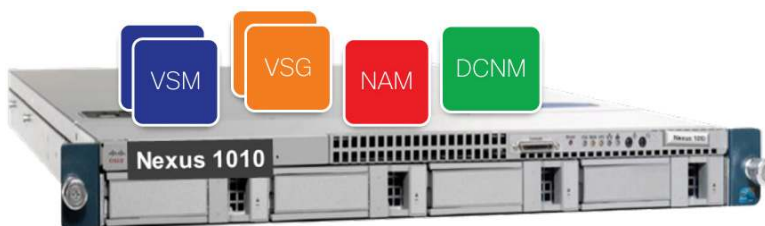
- Two Intel X5650, with 2.66 GHz and 6 cores
- Six 8-GB RDIMM RAM
- Two 2-terabyte (TB) SAS HDD
- One Broadcom Quad Port Gigabit Ethernet 5709 NIC
- One serial port
- One rail kit

### Virtual Service Blade

A VSB provides expansion capabilities so that new services can be added to the Nexus 1010 in the future. The Cisco Nexus 1010 Manager enables customers to install, configure, and manage various VSBs. Currently, four VSBs are supported: VSM, VSG, NAM, and DCNM.

The Cisco Nexus 1010 can host up to six VSBs and the Cisco Nexus 1010-X can host up to ten VSBs, where the VSM is one of those VSBs. Each VSM can manage a group of up to 64 Cisco Virtual Ethernet Modules (VEMs). From a network management perspective, a VSM and the VEMs make up a virtual switch. The Cisco Nexus 1010 and the multiple VSMs it hosts are viewed as a cluster of switches (Figure 2).

**Figure 2.** Cisco Nexus 1010 with four VSBs: VSMs, VSGs, NAM, and DCNM



Support is provided for both Layer 2 and Layer 3 communication between the VSMs on the Cisco Nexus 1010 and the VEMs that it will control.

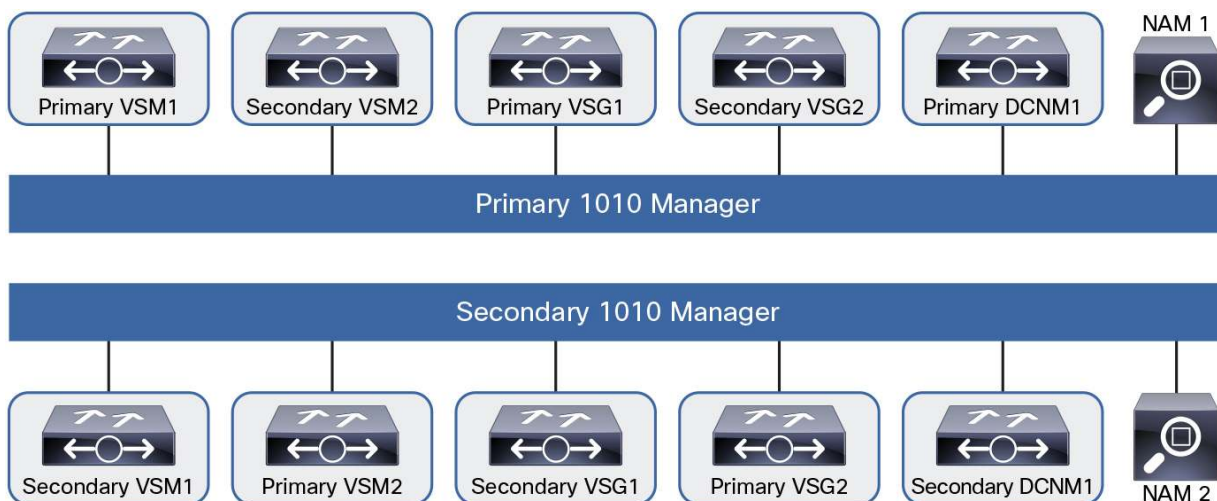
More information and recommendations about the use of Layer 2 and Layer 3 connectivity between VSMs and VEMs can be found in the Cisco Nexus 1000V deployment guide.

### High Availability

#### Cisco Nexus 1010 High Availability

To achieve high availability, you should deploy redundant Cisco Nexus 1010 appliances, with one Cisco Nexus 1010 as the primary and the second Cisco Nexus 1010 as the secondary device. The two appliances run in an active-standby configuration to offer high availability for both management and VSB deployments. Certain virtual services, such as Cisco NAMs, do not support high availability. Please refer to the particular VSB to determine whether it supports high availability. Figure 3 shows the built-in high availability for both the VSMs and VSGs.

**Figure 3.** Cisco Nexus 1010 High-Availability(HA) pair



If one Cisco Nexus 1010 were to fail, management automatically fails over to the other Cisco Nexus 1010 without disruption of traffic or operations. For two Cisco Nexus 1010 appliances to form a high-availability pair, the control VLAN and domain ID of both Cisco Nexus 1010 appliances must match.

Another high-availability feature built into the Cisco Nexus 1010 is the capability of the Cisco Nexus 1010 Manager to automatically distribute the placement of the active VSMs across the two appliances. This feature helps balance the distribution of traffic and reduce the size of the potential fault domain.

The pairing of the Cisco Nexus 1010 appliances must match the hardware platform. A Cisco Nexus 1010 must be paired with another identical Cisco Nexus 1010 platform; mixing of platforms is not supported such as mixing a 1010 with a 1010-X.

### VSM High Availability

High availability is also configured for the redundant VSBs that are created on the Cisco Nexus 1010.

Not every VSB is the primary module on the primary Cisco Nexus 1010. With connectivity between the primary and secondary Cisco Nexus 1010 appliances, access through a serial connection to any virtual service is maintained. When one Cisco Nexus 1010 fails, the remaining Cisco Nexus 1010 becomes active, and all virtual services in the standby state on that Cisco Nexus 1010 become active automatically.

A virtual service can be removed completely from both redundant Cisco Nexus 1010 appliances, or from only one. If one of the redundant pair of virtual services becomes unusable, it can be removed from the Cisco Nexus 1010 platform on which it resides. This approach facilitates recovery by preserving the remaining virtual service in the pair. Use of this service may be needed if a new instance of the service must be provisioned.

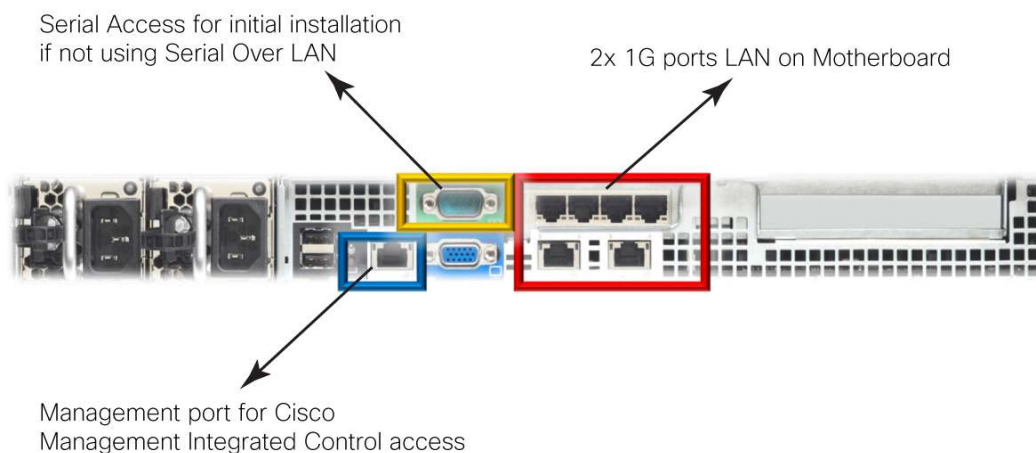
You should create redundant VSMs on the Cisco Nexus 1010 with the Cisco Nexus 1000V software image. The current version is bundled as an ISO image and included in the Cisco Nexus 1010 bootflash:repository folder. The image is copied to a new VSM service when it is created. After you have created the first VSM, you can use that software image to create additional VSMs. You can upgrade VSMs to a new release of Cisco Nexus 1000V as needed.

For more information about VSM high availability, see the [Cisco Nexus 1000V High Availability and Redundancy Configuration Guide](#).

### Network Connectivity

The Cisco Nexus 1010 has six 1 Gigabit Ethernet interfaces available for network connectivity: two 1 Gigabit Ethernet LAN-on-motherboard (LOM) interfaces and four 1 Gigabit Ethernet interfaces, available through a PCI card (Figure 4).

**Figure 4.** Backside of Nexus 1010



Four types of traffic flow through these interfaces: management, control, packet, and VSB data traffic. The Cisco Nexus 1010 is not in the data path of everyday virtual machine data traffic. However, when Cisco NAM or VSG

VSBs are deployed, data traffic from selected virtual machines will flow to the Cisco Nexus 1010 to be processed by the respective network service. The decision to use or not use these other VSBs influences the choice of network connectivity option used for connecting the Cisco Nexus 1010 to the network.

### Management VLAN

The Cisco Nexus 1010 and its hosted Cisco Nexus 1000V VSMs share the same management VLAN. Unlike the control and packet VLANs, which are set when a virtual service is created, the management VLAN is inherited. The mgmt0 interface on the VSM needs to be on the same subnet as the mgmt0 interface that the Cisco Nexus 1010 uses. Note that the management VLAN is inherited from the Cisco Nexus 1010. If it is changed, the change is applied to both the Cisco Nexus 1010 and all its hosted Cisco Nexus 1000V VSMs.

### Control VLAN

The control VLAN is a Layer 2 interface used for communication between the redundant Cisco Nexus 1010 appliances. This interface handles low-level control packets such as heartbeats as well as any configuration data that needs to be exchanged between the Cisco Nexus 1010 appliances.

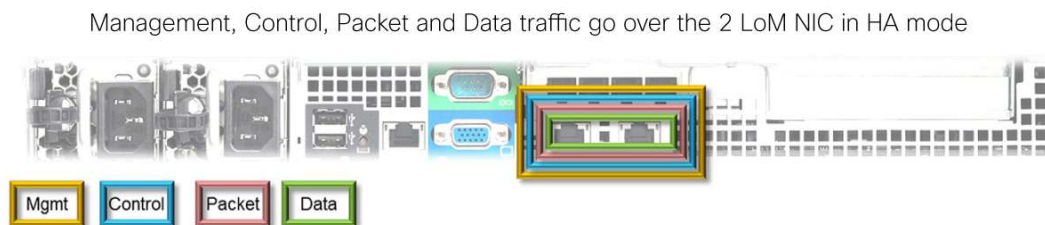
### Network Connectivity Options

The interfaces on the Cisco Nexus 1010 can be connected to the network in five ways. The choice of the best connectivity option, or uplink type, for the Cisco Nexus 1010 depends on the customer's needs and requirements. When the Cisco Nexus 1010 is first initialized, the setup script requests some basic configuration information, including selection of the network connectivity option. This section explains the five uplink types (or network connectivity options) and discusses best practices for choosing the best option.

#### Network Connection Option 1

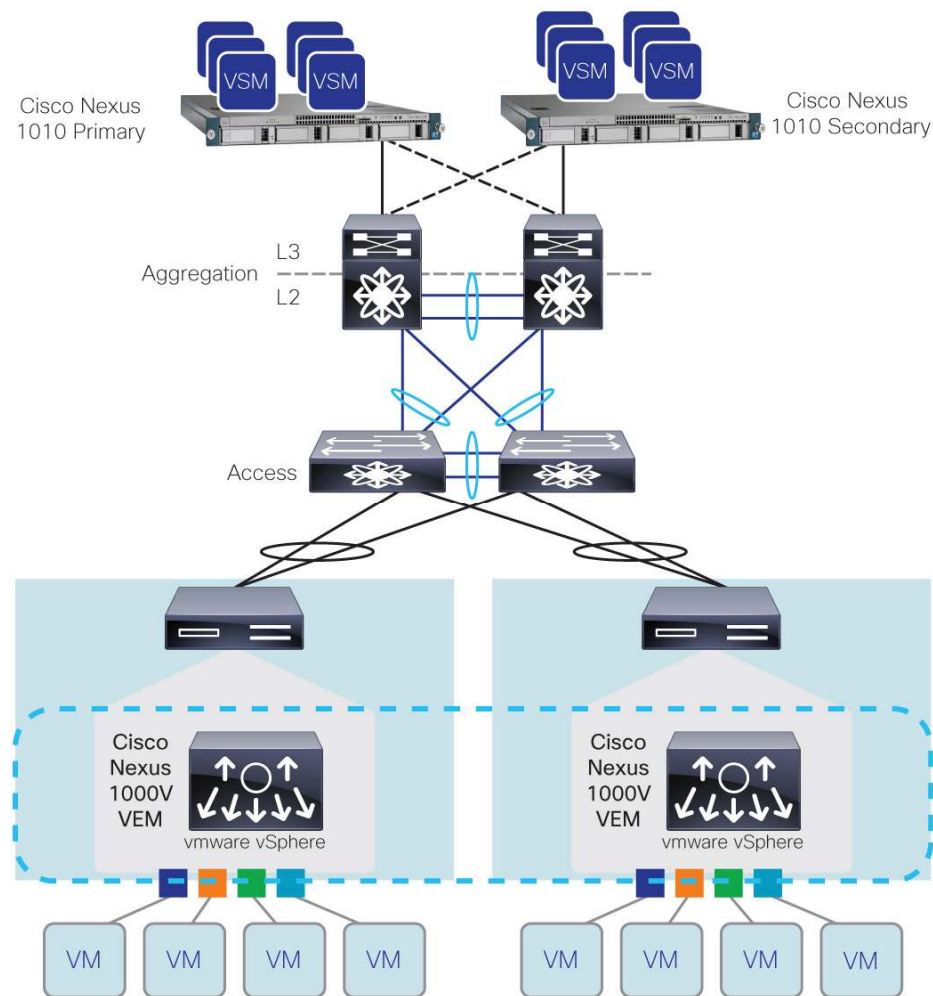
Option 1, the simplest way of connecting the Cisco Nexus 1010 to the network, uses the two LOM interfaces to carry all traffic types: management, control, packet, and data. In this configuration, each uplink connects to two different upstream switches to provide redundancy (Figure 5).

**Figure 5.** Network Connection Option 1



Option 1 is preferred in cases in which customers are not using a Cisco NAM and therefore have little or no data traffic traversing the uplinks to the Cisco Nexus 1010. This option is commonly used when the Cisco Nexus 1010 is used only for VSMs. The management, control, packet, and data traffic can all use different VLANs, although this is not a requirement. This option is recommended for the simplest configuration and lowest risk of misconfiguration (Figure 6).

**Figure 6.** Option 1 Configuration



**Note:** The LOM ports are active-standby only and cannot be part of a PortChannel or virtual PortChannel (vPC).

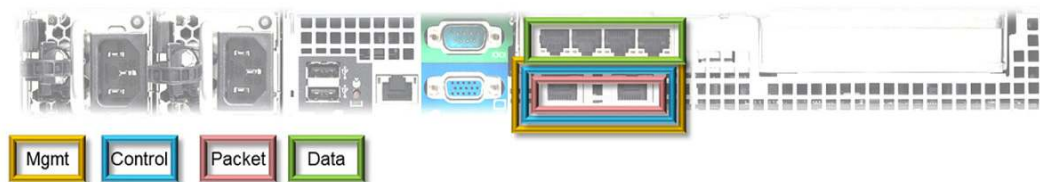
#### Network Connection Option 2

Option 2 uses the two LOM interfaces to carry management, control, and packet traffic. The other four interfaces on the PCI card carry only data traffic. In this configuration, the two interfaces used for management, control, and packet traffic should be connected to two separate upstream switches for redundancy. In addition, the four ports used for data traffic should be split between two upstream switches for redundancy. Not all four interfaces are required, and their use depends on bandwidth requirements. Use a minimum of two interfaces that are also connected to two separate physical switches. In addition, if multichassis EtherChannel is available, that technology is preferred, to provide additional bandwidth and redundancy (Figure 7).



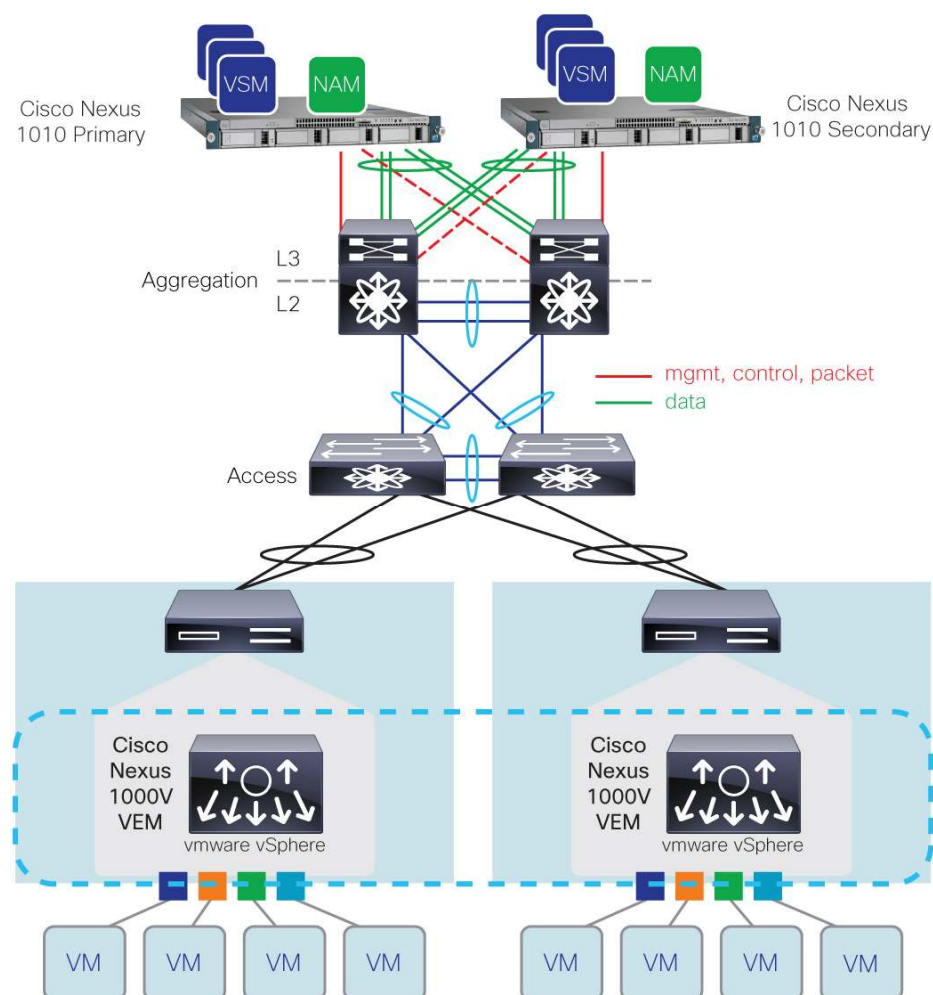
**Figure 7.** Network Connection Option 2

Management, Control and Packet Traffic are over the 2 LoM uplink  
Data Traffic over the 4 remaining ports



Option 2 is well suited for customers who are deploying a Cisco NAM in the Cisco Nexus 1010. The management, control, and packet traffic is kept physically separate from the data traffic, helping ensure that data traffic does not divert cycles from the other traffic. Of the four available connectivity options, option 2 provides the most dedicated bandwidth for Cisco NAM traffic and should be used by customers who want to increase the Cisco NAM capabilities (Figure 8).

**Figure 8.** Option 2 Configuration



This option is ideal for customers who are deploying a NAM module within the 1010. The management, control and packet traffic is kept physically separate from the data traffic ensuring that data traffic does not steal cycles from the other traffic. Out of the four available connectivity options, this option provides the most dedicated bandwidth for NAM traffic and should be used by customers who want to maximize the NAM capabilities.

**Note:** The 4-port NIC adapter does support PortChannel and vPC capabilities and can provide added bandwidth utilization and redundancy. This example showed the use of a PortChannel, but a vPC configuration would also be valid.

### Network Connection Option 3

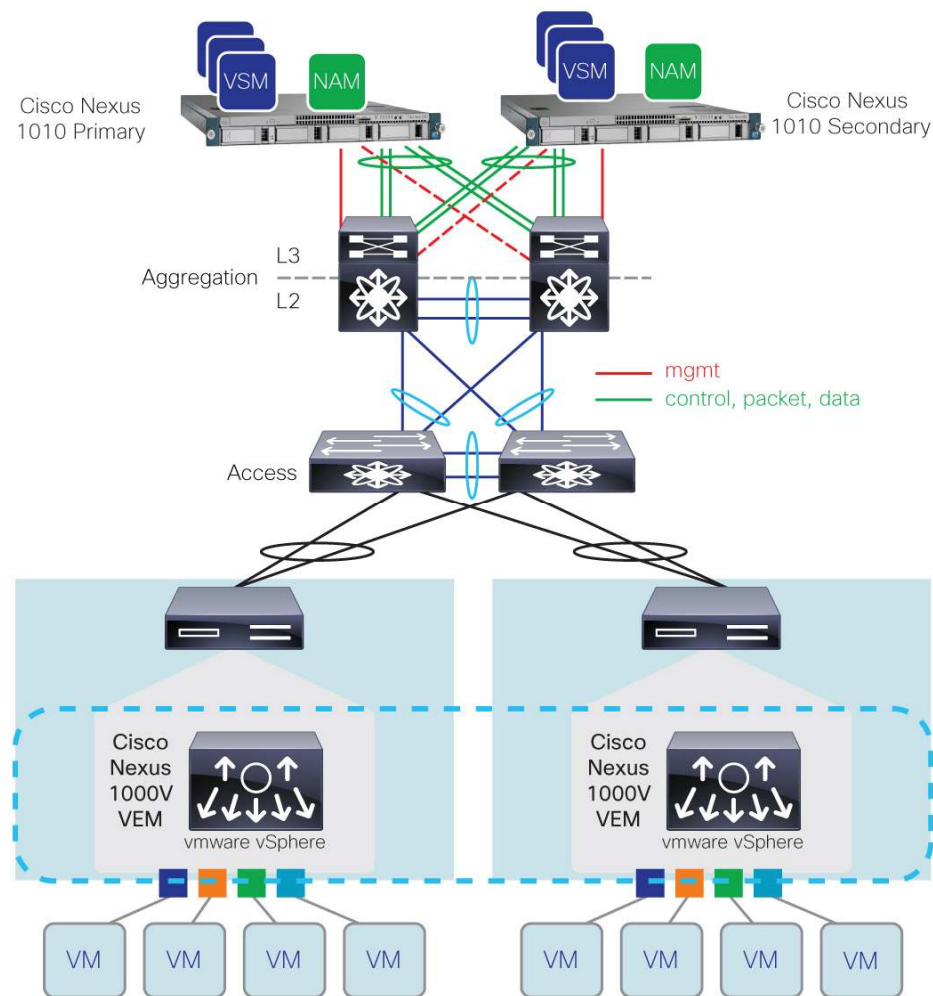
Option 3 uses the two LOM interfaces for management traffic only, and it uses the four interfaces on the PCI card to carry control, packet, and data traffic. In this configuration, the two management interfaces should be connected to two separate upstream switches for redundancy. In addition, the four ports used for control, packet, and data traffic should be split between two upstream switches for redundancy (Figure 9).

**Figure 9.** Network Connection Option 3



Option 3 is well suited for customers who are deploying a Cisco NAM in the Cisco Nexus 1010 but require a separate management network. Because there is little control and packet traffic, customers can still use most of the bandwidth from the four 1 Gigabit Ethernet interfaces for Cisco NAM traffic. This option is recommended for most deployments because it provides the flexibility to handle both currently supported and future VSBs (Figure 10).

**Figure 10.** Option 3 Configuration



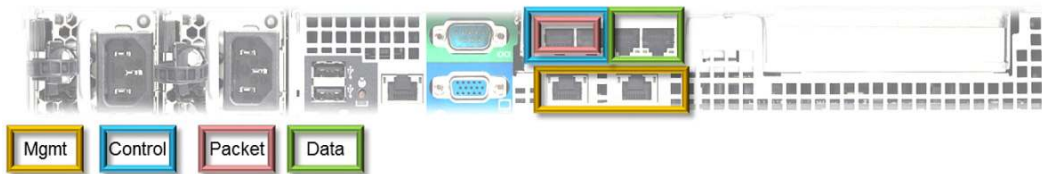
**Note:** Physical connectivity does not change for this network option. As in the PortChannel configuration for network option 2, a vPC configuration is also valid.

#### Network Connection Option 4

Option 4 uses the two LOM interfaces for management traffic, two of the four PCI interfaces for control and packet traffic, and the other two PCI interfaces for data traffic. Each of these pairs of interfaces should be split between two upstream switches for redundancy (Figure 11).

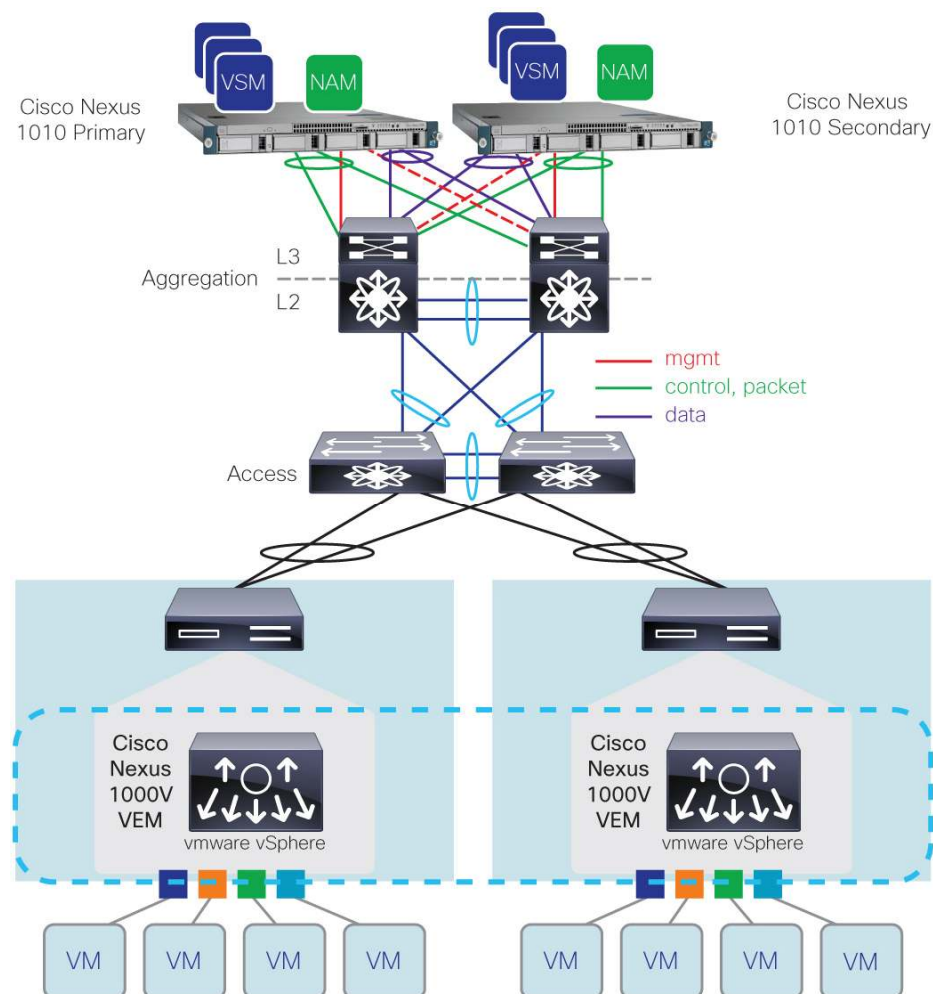
**Figure 11.** Network Connection Option 4

Management over the 2 LoM uplink  
Control, Packet over port 3 and 4  
Data over port 5 and 6



Option 4 is well suited for customers who want to use the Cisco NAM but require separate data and control networks. Separating the control from the data network helps ensure that Cisco NAM traffic does not divert cycles from control traffic and therefore affect connectivity (Figure 12).

**Figure 12.** Option 4 Configuration



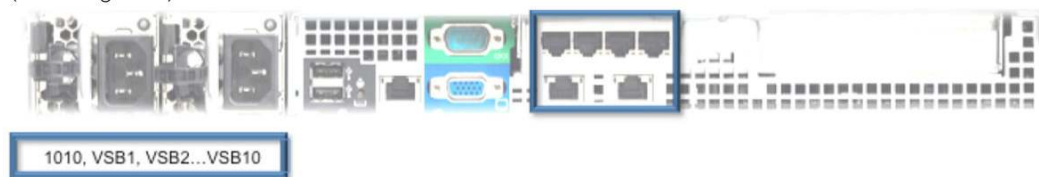
**Note:** Since each type of traffic uses two physical interfaces, a vPC is recommended if possible. Otherwise, a regular PortChannel configuration should be used, but the two physical links need to connect to a single upstream switch.

#### Network Option 5 (Flexible Network)

The addition of this “Flexible Network” option, users can now have a more flexible deployment of their VSBs on the Nexus 1010. Because of this option, there is no longer a classification of what ports allows what type of traffic (i.e. management, control and data) flows through these ports. One of the key advantages this option provides is to define a VSB to utilize a particular interface. This gives a more granular level of traffic engineering in case of security purposes. An example of this would be where a VSM VSB for production will utilize an interface connected to the production network, while another VSM VSB is created for the DMZ, which will have another interface connected to the DMZ network. The diagram below depicts 2 of the possible options with the flexible network’s traffic flow options (Figure 13).

**Figure 13.** Network Connection Option 5

All Nexus 1010 and VSB traffic go over all 6 NICs  
(including LoM) in HA mode



OR

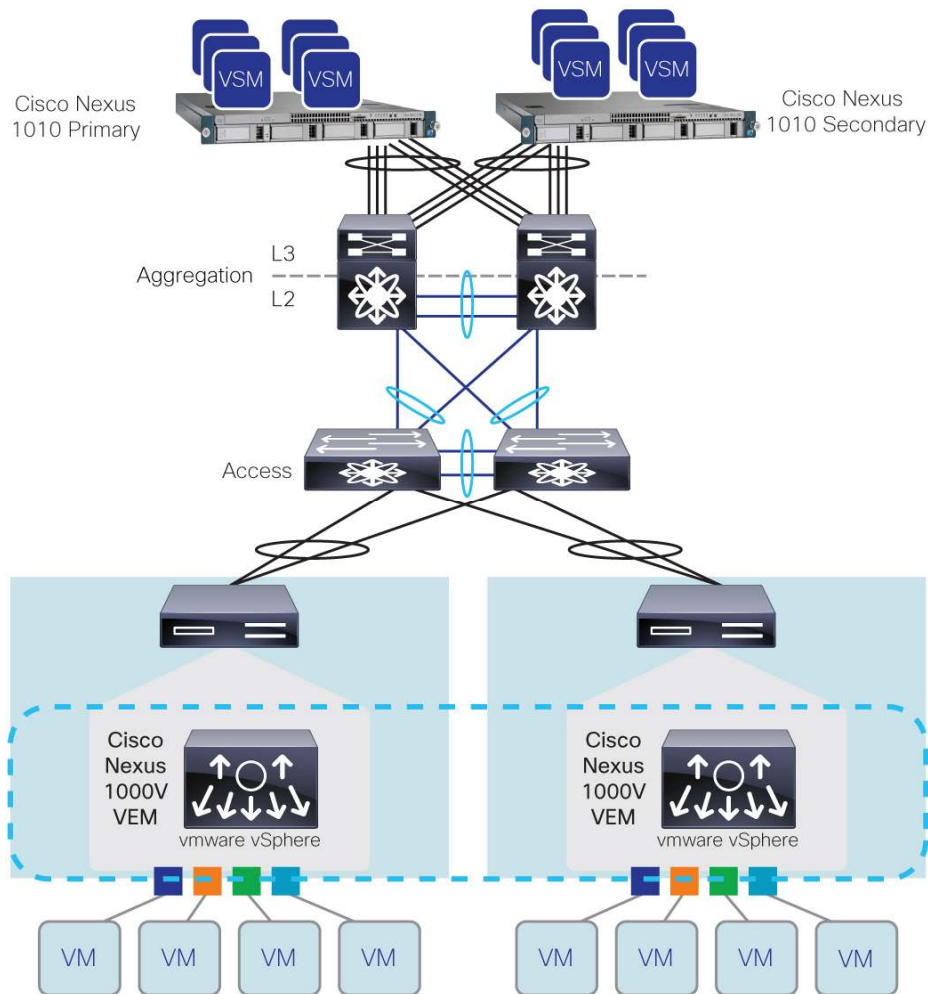
Particular VSB to a particular interface



**Note:** These are 2 possible options but other options are possible that are a mix of the combination shown.

Another feature enhancement with the 4.2(1)SP1(4) release is the capability to port-channel the LAN on Motherboard (LoM) interfaces as well, along with the other 4 GE interfaces. With this enhancement, this can simplify configuration for the network connectivity, which is shown in diagram below (Figure 14).

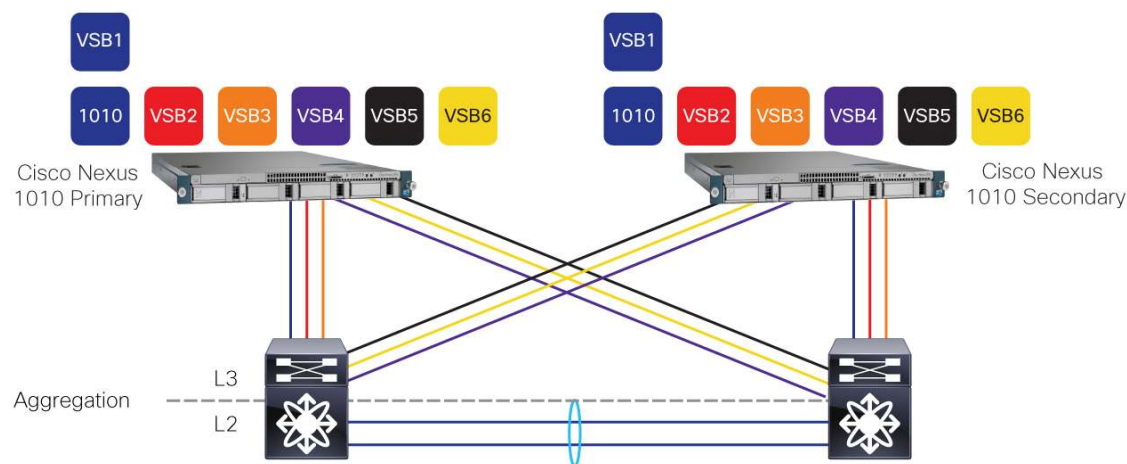
**Figure 14.** Option 5 Configuration



On the other end of the configuration options, it is possible to dedicate a single interface for a particular VSB. Since there is only six physical interfaces on the Nexus 1010 and one of the interfaces need to be utilized by the Nexus 1010 communication, which will mean there are 5 available interfaces to host dedicated VSBs. The diagram below depicts a possible connectivity for this option (Figure 15).



**Figure 15.** Option 5 Connectivity



**Note:** With support of up to 10x VSBs on the 1010-X, some of the interfaces may have multiple VSBs share the same interface. Also, for VSBs that do not support HA (i.e. NAM and DCNM for example), will not have redundancy if there is no NIC redundancy from the Nexus 1010/1010-X perspective.

This flexible option is the best option for users that want more control on designing the VSBs for optimized flexibility and redundancy.

### Deployment Considerations

The Cisco Nexus 1010 offers many deployment benefits. First, because the Cisco Nexus 1010 is an appliance owned and operated by the network team, deployment no longer depends on collaboration by network, storage, and virtualization operations teams. Instead, the Cisco Nexus 1010 can be installed and deployed in the same way as any networking device.

Another benefit is the flexibility as to where the Cisco Nexus 1010 can be inserted into the network. The previous section discussed the four options for connecting the Cisco Nexus 1010 to the network. These methods can be used throughout various areas of the network. Typically, Cisco Nexus 1010 appliances will be deployed within a central management domain. Often, this location can be where other network appliances, such as Cisco Application Control Engine (ACE), Cisco Wide Area Application Services (WAAS), and Cisco NAM appliances, are deployed.

Typically, the Cisco Nexus 1010 is best deployed at the aggregation layer of the network so that it can host a larger set of servers. Because the architecture of the Cisco Nexus 5000 Series Switches and Cisco Nexus 2000 Series Fabric Extenders supports up to 1152 servers, deploying the Cisco Nexus 1010 on the Cisco Nexus 2000 Series provides a large pool of servers supported on a single point of management of those servers, while also treating the Cisco Nexus 1010 as a virtual switch connected to the Cisco Nexus 5000 and 2000 Series architecture.

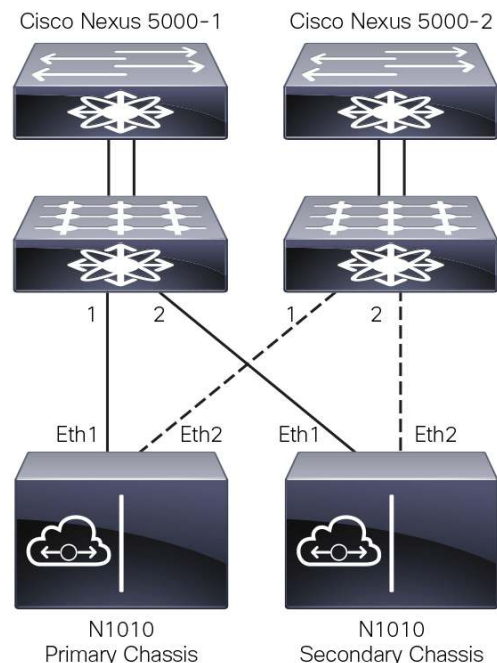
Because the Cisco Nexus 1010 uses 1 Gigabit Ethernet interfaces to connect to the network, a fabric extender provides an optimal connectivity solution. Connecting a Cisco Nexus 1010 to a Cisco Nexus Family switch or fabric extender module helps simplify deployment by running the same operating system, Cisco NX-OS, on both devices.

## Topology Examples

The following topology examples use the premise of connecting the Cisco Nexus 1010 directly to Cisco Nexus 2000 Series Fabric Extenders on a Cisco Nexus 5000 Series parent switch. The vPC technology on the Cisco Nexus 5000 and 7000 Series Switches (or any other switch that supports multichassis EtherChannel technology) can be used to increase bandwidth utilization on uplink types that support Link Aggregation Control Protocol (LACP) PortChannels.

This section discusses the four uplink types in the context of connection to upstream switches that use Cisco Nexus 2000 Series Fabric Extenders. Note that this discussion can also apply when you connect to other upstream switches.

### Uplink Type 1



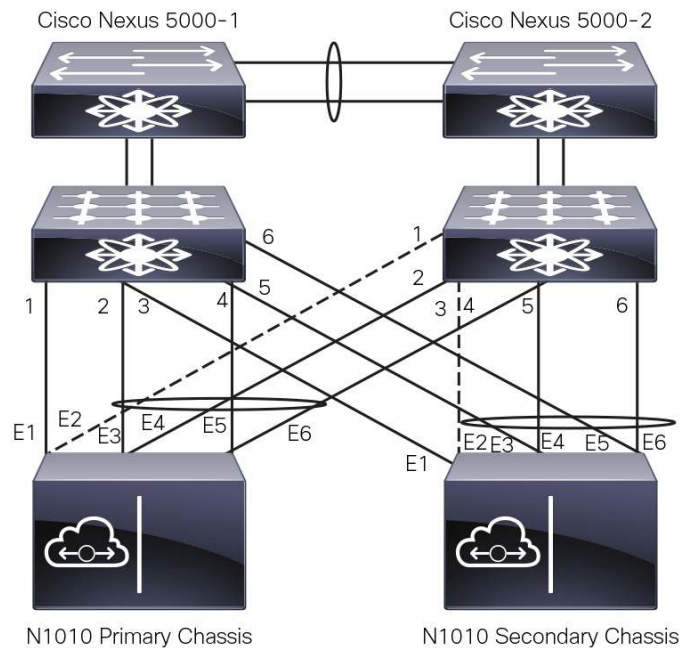
In this topology, all traffic (management, control, and VSB data) is switched out at an effective bandwidth of 1 Gbps. Both ports on the Cisco Nexus 1010, Eth1 and Eth2, are teamed to form an active-standby pair. This uplink type is simplistic and does not require any PortChannel or LACP configuration on the upstream switches. The upstream Cisco Nexus 5000 Series configuration would look similar to the following for the access ports to which the Cisco Nexus 1010 connects.

#### Nexus 5000-1 and Nexus 5000-2 Configuration

```
interface ethernet 101/1/1-2
switchport mode trunk                                !-- multiple vlans trunked across link
switchport trunk allowed vlan 170,250-251            !--only allow mgmt, control and data
                                                       vlans
spanning-tree port type edge trunk                   !-- enable portfast edge
```



## Uplink Type 2



In this topology, management and control traffic is switched out of the first two Ethernet interfaces. Ethernet 1 and 2 are forwarding as an active-standby pair, just as in uplink type 1. However, VSB data traffic is carried out of Ethernet interfaces 3 through 6. If vPC (or similar clustering) is used on the upstream switches, the effective combined bandwidth is 5 Gbps for each Cisco Nexus 1010. This uplink type is well suited when more non-VSM VSBs, such as Cisco NAM or VSG, are used, because there is more bandwidth for the VSB data traffic to use.

Here, LACP PortChannel technology is used on the upstream switches to give each Cisco Nexus 1010 its own PortChannel across the two Cisco Nexus 5000 Series Switches. The configuration upstream would look similar to the following.

### Nexus 5000-1 and Nexus 5000-2 Configuration

```
interface ethernet 101/1/1, 101/1/3
switchport mode trunk                                |-- multiple vlans trunked across link
switchport trunk allowed vlan 170,250                |-- only allow mgmt and control vlans
spanning-tree port type edge trunk                    |-- enable portfast edge

interface ethernet 101/1/2, 101/1/4
switchport mode trunk                                |-- multiple vlans trunked across link
switchport trunk allowed vlan 251                    |-- only allow data vlan(s)
spanning-tree port type edge trunk                    |-- enable portfast edge
channel-group 1010 mode active                         |-- add interface to port-channel

interface port-channel 1010                            |-- this is a unique vpc for N1010
vpc 1010                                                Primary

interface ethernet 101/1/5, 101/1/6
```

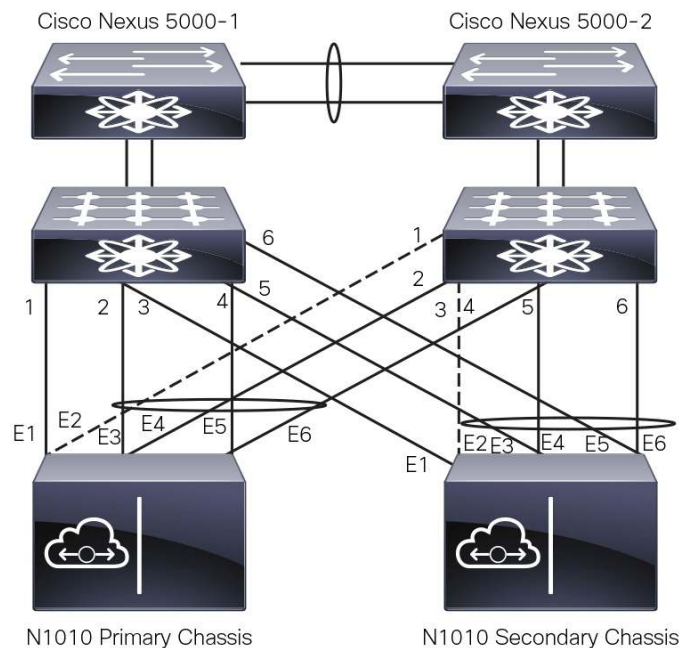
```

switchport mode trunk                                !-- multiple vlans trunked across link
switchport trunk allowed vlan 251                   !-- only allow data vlan(s)
spanning-tree port type edge trunk                  !-- enable portfast edge
channel-group 1011 mode active                       !-- add interface to port-channel

interface port-channel 1011                          !-- this is a unique vpc for N1010
vpc 1011                                              Secondary

```

### Uplink Type 3



Uplink type 3 is physically identical to uplink type 2 because it uses all the Ethernet interfaces available. The difference is in the way that the traffic is carried across these interfaces. In this topology, management traffic is switched out of the first two Ethernet interfaces. Ethernet 1 and 2 are forwarding as an active-standby pair, just as in the other uplink types. However, both control and VSB data traffic is carried out of Ethernet interfaces 3 through 6. If vPC (or similar clustering) is used on the upstream switches, the effective combined bandwidth is 5 Gbps for each Cisco Nexus 1010. This uplink type is well suited when multiple VSM VSBs are used because it allows the VSM traffic to be shared with other VSBs. This type also provides the flexibility to add either VSM VSBs or different additional VSBs in the future while increasing bandwidth utilization for all VSBs.

Here, LACP PortChannel technology is used on the upstream switches to give each Cisco Nexus 1010 its own PortChannel across the two Cisco Nexus 5000 Series Switches. The configuration upstream would look similar to the following.

#### Nexus 5000-1 and Nexus 5000-2 Configuration

```

interface ethernet 101/1/1, 101/1/3
switchport mode trunk                                !-- multiple vlans trunked across link
switchport trunk allowed vlan 170                   !-- only allow mgmt vlan
spanning-tree port type edge trunk                  !-- enable portfast edge

```

```

interface ethernet 101/1/2, 101/1/4
switchport mode trunk                                !-- multiple vlans trunked across link
switchport trunk allowed vlan 250-251                !-- only allow control and data vlans
spanning-tree port type edge trunk                   !-- enable portfast edge
channel-group 1010 mode active                        !-- add interface to port-channel

interface port-channel 1010                           !-- this is a unique vpc for N1010
vpc 1010                                              Primary

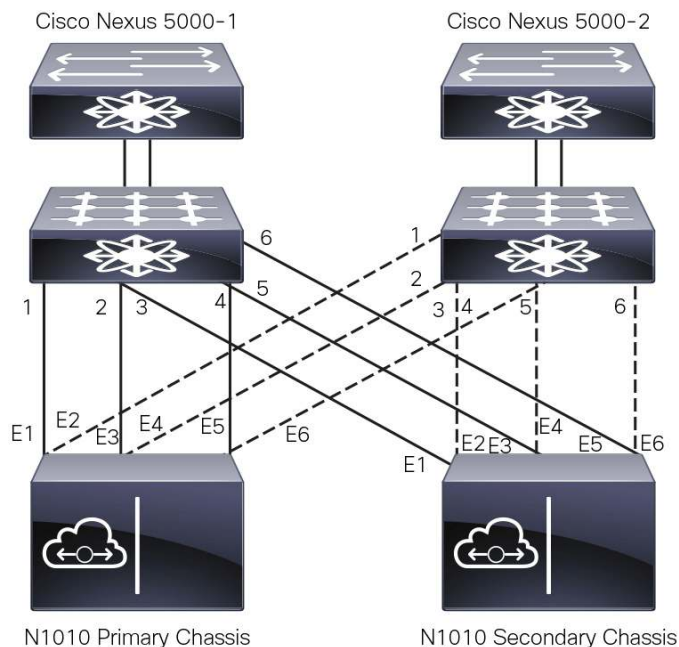
interface ethernet 101/1/5, 101/1/6
switchport mode trunk                                !-- multiple vlans trunked across link
switchport trunk allowed vlan 250-251                !-- only allow control and data vlans
spanning-tree port type edge trunk                   !-- enable portfast edge
channel-group 1011 mode active                        !-- add interface to port-channel

interface port-channel 1011                           !-- this is a unique vpc for N1010
vpc 1011                                              Secondary

```

#### Uplink Type 4

Figure 16 shows another option for deploying the Cisco Nexus 1010 in the aggregation layer or the Layer 2 and 3 boundary of the network. The VSMs residing on the Cisco Nexus 1010 and the hosts that are managed by the VSMs can be connected over Layer 2 or 3 as explained in the previous sections. Best practices regarding the choice of Layer 2 or Layer 3 connectivity between the VSMs and VEMs can be found in the Cisco Nexus 1000V deployment guide.



---

Here, LACP PortChannel technology is not used on the upstream switches. The configuration upstream would look similar to the following.

#### Nexus 5000-1 and Nexus 5000-2 Configuration

```
interface ethernet 101/1/1, 101/1/3
switchport mode trunk
switchport trunk allowed vlan 170          !-- multiple mgmt vlan(s) trunked
across link
spanning-tree port type edge trunk        !-- enable portfast edge

interface ethernet 101/1/2, 101/1/4
switchport mode trunk
switchport trunk allowed vlan 250          !-- multiple Control vlans trunked
across link
spanning-tree port type edge trunk        !-- enable portfast edge

interface ethernet 101/1/5, 101/1/6
switchport mode trunk
switchport trunk allowed vlan 251          !-- multiple VSB data vlans trunked
across
spanning-tree port type edge trunk        !-- enable portfast edge
```

#### Uplink Type 5

This uplink type is for the flexible network option and can be a mix of a combination of any of the above uplink types.

### Cisco Nexus 1000V Backup and Restore Procedure

With the release of Cisco Nexus 1000V Version 4.2(1)SV1(4a) and Cisco Nexus 1010 Version 4.2(1)SP1(3) firmware, you can now back up and restore network configurations of the Cisco Nexus 1000V. Depending on the type of disaster that has occurred, restoration of the network configurations or VSM instance is now possible in this new release. Here are the high-level steps for the VSM installed on the Cisco Nexus 1010.

#### Backup Procedures

1. Shut down the secondary or standby VSM VSB.
2. Export that VSB to remote storage.
3. Back up the running configuration of the Cisco Nexus 1000V to a remote server or site.
  - a. Copy the running configuration often or whenever network the configuration has changed.
4. Power back on the secondary or standby VSM.

#### Restore Procedures

1. Completely remove the Cisco Nexus 1000V VSB if it is still on the Cisco Nexus 1010.
2. Create a new Cisco Nexus 1000V VSB.
  - a. Import a backup Cisco Nexus 1000V instance to the new VSB.
  - b. Verify that the Cisco Nexus 1000V instance is operational.
3. Restore the backup network configuration as the running configuration.

- a. Verify that the port profiles and configurations are correct.
- b. Verify that the virtual machines are connected to the appropriate port profiles.
- c. Create a backup configuration of the running configuration after the environment has stabilized.

As a best practice, back up configurations to a remote site and not on the bootflash drive of the Cisco Nexus 1000V VSM. The configuration can be stored on the bootflash drive, but it is good to have another copy remotely as well.

## Virtual Service Blade Support

With the introduction of the Cisco Nexus 1010, the platform supports up to four VSBs. As of Cisco Nexus 1010 Version 4.2(1)SP1(3), up to six VSBs are supported on the Cisco Nexus 1010, and under Release 4.2(1)SP1(4) up to ten VSBs are supported on the Cisco Nexus 1010-X. The Cisco NAM was the second VSB, along with the VSM to be supported on the Cisco Nexus 1010. With the Cisco Nexus 1010 Version 4.2(1)SP1(3) software release, additional service blades are supported, such as Cisco VSG and DCNM. Each of these service blades counts toward the supported number of VSBs with this software release. The table below shows the weight of each virtual service in the Cisco Nexus 1010 and 1010-X platforms.

### Nexus 1010 Maximum Supported Configurations (Up to 6x VSBs Total; see weighting matrix)

- 6x Cisco Nexus 1000V VSMs, each capable of managing 64x ESX/ESXi hosts for a total of 384x VMware ESX/ESXi hosts
- 6x Cisco VSG VSBs

### Nexus 1010-X Maximum Supported Configurations [Up to 10x VSBs Total Using Cisco Nexus 1010 Release 4.2(1)SP1(4) and later; see weighting matrix]

- 10x Cisco Nexus 1000V VSMs, each capable of managing 64x ESX or ESXi for a total of 640x VMware ESX/ESXi hosts
- 10x Cisco VSG VSBs

Weighting Matrix (to determine max capacity of various VSBs on the Nexus 1010 and 1010-X)

	VSM	VSG	NAM	DCNM	Total Weighting
Nexus 1010 and 1010-X Release 4.2(1)SP1(3)	1	1	2	2	<=6
Nexus 1010 Release 4.2(1)SP1(4)	1	1	2	2	<=6
Nexus 1010-X Release 4.2(1)SP1(4)	1	1	2	2	<=10

### Example Nexus 1010 configurations:

- 6x VSMs
- 6x VSGs
- 3x VSMs, 3x VSGs
- 1x VSM, 1x VSG, 1x NAM, 1x DCNM

### Example Nexus 1010-X configurations with Release 4.2(1)SP1(4):

- 10x VSMs
- 10x VSGs

- 5x VSMs, 5x VSGs
- 3x VSMs, 3x VSGs, 1x NAM, 1x DCNM

## Feature Enhancements

With the release of NX-OS 4.2(1)SP1(4), the following are enhancement features that improves on the usability of the Nexus 1010 solution. Below are a list of these features and a brief explanation of each enhancement.

- OVA Support
- Native VLAN
- Different Management Network per VSB

### **OVA Support:**

When deploying the virtual service blade (VSB), the image format supported is ISO. With now the added support of the format of OVA, this will allow users to deploy a VSB from a VMware Virtual Machine file format. A common use case would be for migration of the VSM as a VM onto the Nexus 1010.

### **Native VLAN:**

In prior release of the Nexus 1010, native vlan was not supported for the network ports. With the release of 4.2(1)SP1(4), it is now possible to configure native vlan on the upstream switch. Without support of native vlan, all types of traffic had to be tagged to a particular vlan. This is typically focused toward management traffic. Now with this support of native vlan, network administrators can configure the physical access switch as trunk with a native vlan, designed for the network traffic.

### **Different Management Network per VSB:**

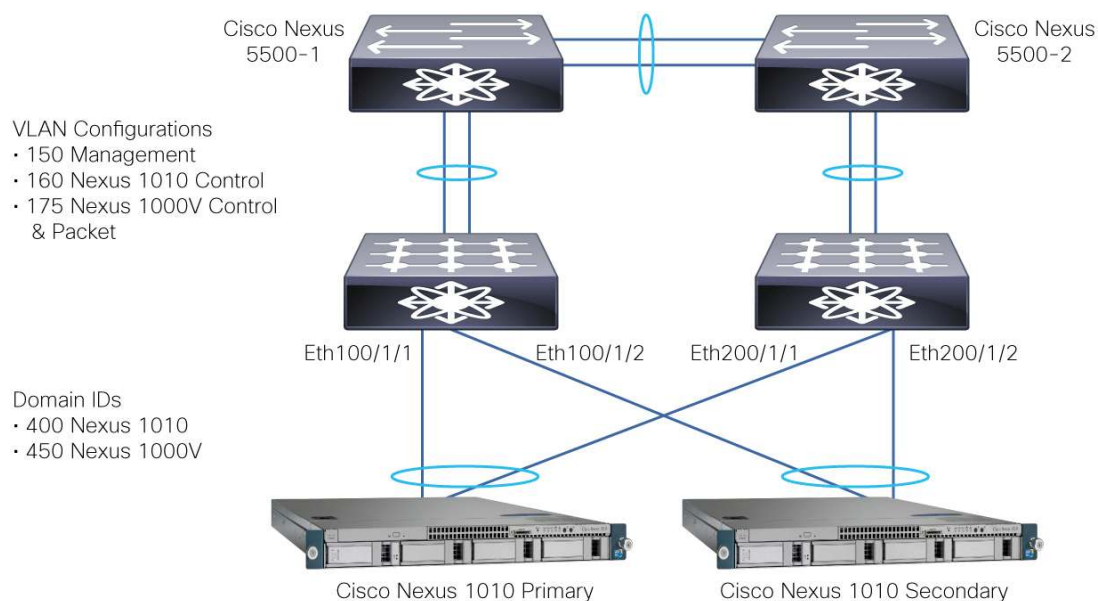
In previous releases, the management network for the Nexus 1010 and all of the VSBs had to reside on the same VLAN and subnet. With the 4.2(1)SP1(4) release, each of the VSBs management interfaces can reside on different VLANs and different subnets. This provides a more robust deployment of various VSBs that resides on the Nexus 1010.

## Appendix A: Quick Configuration Guide

This appendix provides a quick configuration guide for instantiating a VSM on the Cisco Nexus 1010. The example uses network connectivity option 1. This quick configuration does not show how to register the VSM to VMware vCenter, nor does it show how to add a VMware ESX or ESXi server as a VEM. All those steps are standard in configuring the Cisco Nexus 1000V and are independent of the platform for which the VSM is installed (either as a virtual machine or on the Cisco Nexus 1010).

Figure 16 shows the network connection used for this example.

**Figure 16.** Network Connection for Configuration Example



### Cisco Nexus 5000 Series Upstream Configurations

With the Cisco Nexus 1010 using network connectivity option 1, the following example will create a PortChannel of the two physical LOM interfaces on the Cisco Nexus 1010. This PortChannel will allow only the necessary VLANs for the environment. Here is the configuration output of the Cisco Nexus 5500 platform:

```
5548-1# show running-config interface port-channel 101
```

```
!Command: show running-config interface port-channel101
```

```
!Time: Mon Sep 5 23:05:11 2011
```

```
version 5.0(3)N2(1)
```

```
interface port-channel101
```

```
switchport mode trunk
```

```
switchport trunk allowed vlan 150, 160, 175
```

```
spanning-tree port type edge trunk
```

```
5548-1# show running-config interface ethernet100/1/1-2
```

```
!Command: show running-config interface Ethernet100/1/1-2
```

```
!Time: Mon Sep 5 23:08:04 2011
```

```
version 5.0(3)N2(1)
```

```
interface Ethernet100/1/1
```

```
switchport mode trunk
```

```

switchport trunk allowed vlan 150, 160, 175
spanning-tree port type edge trunk
channel-group 101

```

```

interface Ethernet100/1/2
switchport mode trunk
switchport trunk allowed vlan 150, 160, 175
spanning-tree port type edge trunk
channel-group 101

```

**Note:** The configuration of the Cisco Nexus 5500 platform will be similar. The PortChannel interface number can be different, but the port configuration and VLAN information should be the same.

Verify that the PortChannel interface is up with the following command:

```

5548-1# show port-channel summary
Flags:    D - Down                P - Up in port-channel (members)
          I - Individual          H - Hot-standby (LACP only)
          s - Suspended           r - Module-removed
          S - Switched            R - Routed
          U - Up (port-channel)

```

Group	Port-Channel	Type	Protocol	Member Ports
101	Po101(SU)	Eth	NONE	Eth100/1/21(P) Eth100/1/22(P)

### Primary Cisco Nexus 1010 Setup

With the upstream access switch configured in preparation for the Cisco Nexus 1010, power on the Cisco Nexus 1010. Follow these steps to set up the primary Cisco Nexus 1010:

- When asked, enter and confirm the administrator password.  
---- System Admin Account Setup ----  
Enter the password for "admin":  
Confirm the password for "admin":
- When asked, enter the high-availability role. If you do not specify a role, then **primary** is assigned.  
Enter HA role[primary/secondary]: **primary**

**Note:** The high-availability standalone role is not supported for the Cisco Nexus 1010.

- When asked, enter the uplink type.

**Note:** After you configure an uplink type, the only way to modify it is to reload the software.

Enter network-uplink type <1-4>:

- Ports 1-2 carry all management, control and data vlans



- 
2. Ports 1-2 management and control, ports 3-6 data
  3. Ports 1-2 management, ports 3-6 control and data
  4. Ports 1-2 management, ports 3-4 control, ports 5-6 data
  4. When asked, enter the VLAN ID for the control VLAN.  
Enter control vlan <1-3967, 4048-4093>: **160**
  5. When asked, enter the domain ID.  
Enter the domain id<1-4095>: **400**
  6. When asked, enter the VLAN ID for the management VLAN.  
Enter management vlan <1-3967, 4048-4093>: 150  
Saving boot configuration. Please wait...

[#####] 100%

---- Basic System Configuration Dialog ----

This setup utility guides you through the basic configuration of the system. Setup configures only enough connectivity for management of the system.

Press Enter at any time to skip a dialog box. Press Ctrl-C at any time to skip the remaining dialog boxes.

7. When asked if you want to enter the basic configuration dialog box, respond yes.  
Would you like to enter the basic configuration dialog (yes/no): **yes**

---- Basic System Configuration Dialog ----

This setup utility guides you through the basic configuration of the system. Setup configures only enough connectivity for management of the system.

**Note:** Setup is mainly used for configuring the system initially, when no configuration is present, so setup always assumes system defaults and not the current system configuration values.

Press Enter at any time to skip a dialog box. Press Ctrl-C at any time to skip the remaining dialog boxes.

8. When asked to create another login account, answer no.  
Create another login account (yes/no) [n]: **no**
9. When asked to configure a read-only SNMP community string, answer no.  
Configure read-only SNMP community string (yes/no) [n]: **no**
10. When asked to configure a read-write SNMP community string, answer no.  
Configure read-write SNMP community string (yes/no) [n]: **no**
11. Enter a name for the appliance.  
Enter the VSA name [Nexus1010]: **Nexus1010**

12. When asked to configure out-of-band management, answer yes and then enter the management 0 IPv4 address.

This is the IP address of the management interface that appears as the mgmt0 port on the appliance.

Continue with Out-of-band (mgmt0) management configuration? [yes/no] [y]: **yes**

Mgmt0 IPv4 address: **10.78.109.67**

13. When asked to configure the default gateway, answer yes.

Configure the default-gateway: (yes/no) [y]: **yes**

IPv4 address of the default gateway: **10.78.109.1**

14. When asked to configure advanced IP options, answer no.

Configure Advanced IP options (yes/no)? [n]: **no**

15. When asked to enable the telnet service, answer yes.

Enable the telnet service? (yes/no) [y]: **yes**

16. When asked to enable the SSH service, answer yes and then enter the key type and number of key bits.

Enable the ssh service? (yes/no) [y]: **yes**

Type of ssh key you would like to generate (dsa/rsa): **rsa**

Number of key bits <768-2048>: **1024**

17. When asked to configure the Network Time Protocol (NTP) server, answer no.

The configuration is summarized.

Configure NTP server? (yes/no) [n]: **no**

The following configuration will be applied:

```
Switchname Nexus1010
interface Mgmt0
ip address 10.78.109.67 255.255.255.0
no shutdown
telnet server enable
ssh key rsa 1024 force
ssh server enable
svs-domain
control vlan 160
domain id 400
```

18. Do one of the following:

- If you do not want to edit the configuration answer no and continue with the next step.
- If you want to edit the configuration, answer yes and return to Step 8 to revisit each command.

Would you like to edit the configuration? (yes/no) [n]: **no**

19. When asked to use and save this configuration, answer yes.

**Caution:** If you do not save the configuration now, then none of your changes will be part of the configuration the next time the switch is rebooted. Enter yes to save the new configuration. This entry helps ensure that the kickstart and system images are also automatically configured.

---

Use this configuration and save it? (yes/no) [y]: **yes**

[#####] 100%

20. You have completed this procedure.

### Secondary Cisco Nexus 1010 Setup

With the primary Cisco Nexus 1010 configured, power on the secondary Cisco Nexus 1010 and follow these steps:

1. When asked, enter and confirm the administrator password.

---- System Admin Account Setup ----

Enter the password for "admin":

Confirm the password for "admin":

2. When asked, enter the high-availability role.

Enter HA role[primary/secondary]: **secondary**

3. When asked, enter the uplink type.

Enter network-uplink type <1-4>:

1. Ports 1-2 carry all management, control and data vlans

2. Ports 1-2 management and control, ports 3-6 data

3. Ports 1-2 management, ports 3-6 control and data

4. Ports 1-2 management, ports 3-4 control, ports 5-6 data

4. When asked, enter the VLAN ID for the control VLAN.

Enter control vlan <1-3967, 4048-4093>: **160**

5. When asked, enter the domain ID.

Enter the domain id<1-4095>: **400**

6. When asked, enter the VLAN ID for the management VLAN.

Enter management vlan <1-3967, 4048-4093>: **150**

Saving boot configuration. Please wait...

[#####] 100%

System is going to reboot to configure network uplinks

HA mode set to secondary. Rebooting now...

7. You have completed this procedure.

### Verify Cisco Nexus 1010 Setup

Run the following command on the Cisco Nexus 1010 to validate the status of the Cisco Nexus 1010:

```
Nexus1010# show system redundancy status
```

Redundancy role

-----

administrative: primary  
operational: primary

Redundancy mode

-----

administrative: HA  
operational: HA

This supervisor (sup-1)

-----

Redundancy state: Active  
Supervisor state: Active  
Internal state: Active with HA standby

Other supervisor (sup-2)

-----

Redundancy state: Standby  
Supervisor state: HA standby  
Internal state: HA standby

Verify that the Cisco Nexus 1000V VSM ISO is in the bootflash:repository directory:

Nexus1010# dir bootflash:repository

16384	Aug 02 11:34:09 2011	lost+found/
183412736	Aug 03 15:09:26 2011	nam-app-x86_64.5-1-1.iso
<b>127037440</b>	<b>Aug 03 12:56:39 2011</b>	<b>nexus-1000v.4.2.1.SV1.4a.iso</b>
9498	Aug 10 08:00:09 2011	ovf-env-va-1.xml
5705	Aug 06 20:22:52 2011	ovf-env-va-2.xml
4096	Aug 06 18:29:19 2011	unpack_dir/
651	Aug 10 08:00:10 2011	vmpresults.txt

Usage for bootflash://sup-local

308875264 bytes used  
3682504704 bytes free  
3991379968 bytes total

### Instantiate Cisco Nexus 1000V VSM (First VSB)

The Cisco Nexus 1010 is now configured in high-availability mode, and the Cisco Nexus 1000V ISO image is downloaded to the bootflash:repository directory, so creation of the first Cisco Nexus 1000V can begin. The following configuration steps show how to do this.

Nexus1010# **configuration terminal**

Nexus1010(config)# **virtual-service-blade VSM1**

```

Nexus1010(config-vs-b-config)# virtual-service-blade-type new nexus-
1000v.4.2.1.SV1.4a.iso
Nexus1010(config -vsb-config)# interface control vlan 175
Nexus1010(config -vsb-config)# interface packet vlan 175
Nexus1010(config -vsb-config)# no shutdown
Nexus1010(config -vsb-config)# enable
Enter vsb image: [nexus-1000v.4.2.1.SV1.4a.iso] <Press Enter>
Enter domain id[1-4095]: 450
Management IP version [V4/V6]: [V4] <Press Enter>
Enter Management IP address: 10.78.109.69
Enter Management subnet mask: 255.255.255.0
IPv4 address of the default gateway: 10.78.109.1
Enter HostName: VSM1
Enter the password for 'admin': <Enter password>
Nexus1010(config-vs-b-config)# show virtual-service-blade summary

```

Name	Role	State	Nexus1010-Module
VSM1	PRIMARY	VSB DEPLOY IN PROGRESS	Nexus1010-PRIMARY
VSM1	SECONDARY	VSB NOT PRESENT	Nexus1010-SECONDARY

**Note:** When you run the **enable** command, the Cisco Nexus 1010 will automatically deploy both VSMS (primary and secondary) to the appropriate Cisco Nexus 1010 appliance after the script is completed. This process will take a few minutes. Check the status of the deployment; the final state of the VSB should have the following output:

```

Nexus1010# show virtual-service-blade summary
-----
Name                Role        State                Nexus1010-Module
-----
VSM1                PRIMARY    VSB POWERED ON      Nexus1010-PRIMARY
VSM1                SECONDARY  VSB POWERED ON      Nexus1010-SECONDARY

```

### Verify Cisco Nexus 1000V VSB

When the Cisco Nexus 1000V VSB is finished powering on, from the Cisco Nexus 1010 console, log into the Cisco Nexus 1000V instance and verify that both the primary and secondary VSMS are up and operational. To do so, follow these steps:

```

Nexus 1010# login virtual-service-blade VSM1

```

**Note:** You will need to press the Enter key to see the login prompt.

Telnet escape character is '^\'.

Trying 127.1.0.18...

Connected to 127.1.0.18.

Escape character is '^\'.

Nexus 1000v Switch

VSM1 login:

Cisco Nexus Operating System (NX-OS) Software

TAC support: <http://www.cisco.com/tac>

Copyright (c) 2002-2011, Cisco Systems, Inc. All rights reserved.

The copyrights to certain works contained in this software are owned by other third parties and used and distributed under license. Certain components of this software are licensed under the GNU General Public License (GPL) version 2.0 or the GNU Lesser General Public License (LGPL) Version 2.1. A copy of each such license is available at

<http://www.opensource.org/licenses/gpl-2.0.php> and

<http://www.opensource.org/licenses/lgpl-2.1.php>

VSM1# **show module**

Mod	Ports	Module-Type	Model	Status
1	0	Virtual Supervisor Module	Nexus1000V	active *
2	0	Virtual Supervisor Module	Nexus1000V	ha-standby

Mod	Sw	Hw
1	4.2(1)SV1(4a)	0.0
2	4.2(1)SV1(4a)	0.0

Mod	MAC-Address(es)	Serial-Num
1	00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8	NA
2	00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8	NA

Mod	Server-IP	Server-UUID	Server-Name
1	10.29.172.51	NA	NA
2	10.29.172.51	NA	NA

\* this terminal session

VSM1#

## Cisco Nexus 1010 Technical Documentation

- [Release Notes](#)
- [Installation Workflow](#)
- [Hardware Installation Guide](#)

- 
- [Software Installation and Upgrade Guide](#)
  - [Nexus 1010 Deployment Guide](#)
  - [Configuration Guide](#)
  - [Command Reference](#)
  - [Password Recovery Guide](#)
  - [All Nexus 1010 and Nexus 1000V Technical Documentation](#)

### For More Information

- Cisco Nexus 1010 and 1010-X: <http://www.cisco.com/go/1010>
- Cisco Nexus 1000V product information: <http://www.cisco.com/go/1000v>
- Cisco Nexus 1000V technical documentation: <http://www.cisco.com/go/1000vdocs>
- Cisco Nexus 1000V community: <http://www.cisco.com/go/1000vcommunity>
- Free evaluation of the Nexus 1000V: <http://www.cisco.com/go/1000veval>
- Cisco Virtual Security Gateway: <http://www.cisco.com/go/vsg>
- Cisco Prime Network Services Controller: <http://www.cisco.com/go/services-controller>
- Cisco Prime Network Analysis Module VSB: <http://www.cisco.com/go/1000nam>
- Cisco Data Center Network Manager LAN VSB: <http://www.cisco.com/go/dcnm>



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](http://www.cisco.com/go/offices).

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](http://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)