Cisco Nexus 1010 Virtual Services Appliance

Deployment Guide

Contents

Overview

This document provides design guidelines for deploying the Cisco Nexus® 1010 Virtual Services Appliance. For detailed configuration documentation, please refer to the respective Cisco® product configuration guides found at http://www.cisco.com. Links to the product configuration guides 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 VMware vSphere hosts 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, which hosts the Cisco Nexus 1000V Virtual Supervisor Module (VSM) and supports virtual service blades to provide 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 much easier for the network administrator. In addition, support for additional virtual service blades such as the Cisco Nexus 1000V Network Analysis Module (NAM) Virtual Service Blade makes the Cisco Nexus 1010 an indispensable component of a virtual access switch solution.

Figure 1. Cisco Nexus 1010 Virtual Services Appliance

Cisco Nexus 1000V Series

Cisco Nexus 1000V Series Switches are intelligent virtual machine access switches designed for VMware vSphere environments running the Cisco NX-OS Software operating system. Operating within the VMware ESX hypervisor, the Cisco Nexus 1000V Series supports Cisco Virtual Network Link (VN-Link) server virtualization technology to provide:

- Policy-based virtual machine connectivity
- Mobile virtual machine security and network policy
- Nondisruptive operating 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 and a greater need for 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 policy that follows mobile virtual machines to help ensure proper connectivity, saving valuable time to focus on virtual machine administration. This comprehensive set of capabilities helps you deploy server virtualization faster and achieve its benefits sooner.

Cisco Nexus 1010 Components

The Cisco Nexus 1010 offers a physical platform for deploying and managing the Cisco Nexus 1000V VSM and other virtual services. The Cisco Nexus 1010 platform includes the physical server coupled with the Cisco Nexus 1010 Manager software, which houses multiple virtual service blades.

Physical Components

The physical components of the Cisco Nexus 1010 are based on the Cisco UCS C200 M1 High-Density Rack-Mount Server physical appliance containing:

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

Virtual Service Blade

Virtual service blades provide expansion capabilities, enabling new services to be added to the Cisco Nexus 1010 in the future. The Cisco Nexus 1010 Manager enables customers to install, configure, and manage various virtual service blades. Currently, two types of virtual service blades are supported: the Cisco Nexus 1000V VSM and the virtual NAM.

The Cisco Nexus 1010 can host up to four VSMs, each controlling a group of up to 64 virtual Ethernet modules (VEMs). From a network management perspective, a VSM and the VEMs it controls make up a virtual switch, and the Cisco Nexus 1010 and the multiple virtual switches it hosts are viewed as a cluster of switches.

Both Layer 2 and 3 connectivity between the VSMs that reside on the Cisco Nexus 1010 and the VEMs that it will control are supported. Regardless of which method is used, all VSMs on a single Cisco Nexus 1010 must use the same connectivity option. If Layer 3 control is used, the VEMs can reside in different Layer 3 domains.

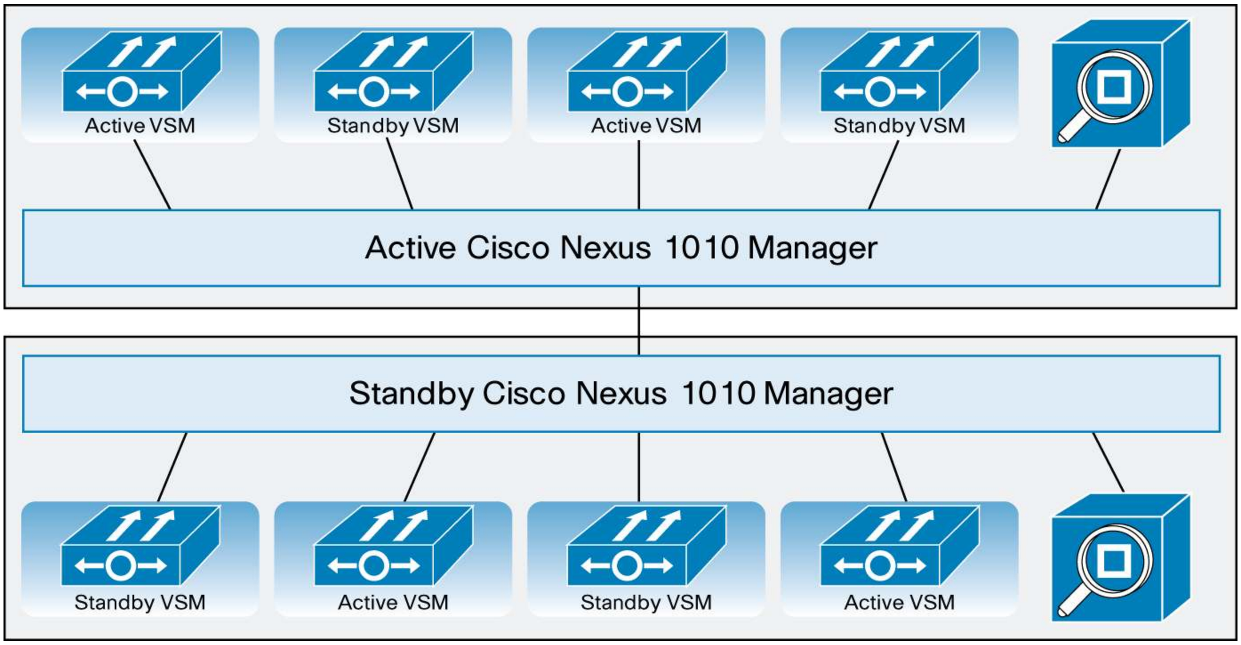
For more information and recommendations about when to use Layer 2 or Layer 3 connectivity between VSMs and VEMs, see the Cisco Nexus 1000V deployment guide.

High Availability

Cisco Nexus 1010 High Availability

Two redundant Cisco Nexus 1010 appliances should be deployed to achieve high availability, with one Cisco Nexus 1010 used as the primary appliance, and the second Cisco Nexus 1010 used as the secondary appliance. The two appliances will run in an active-standby setup to offer high availability from both the management and deployment sides. Figure 2 shows how high availability is built into the Cisco Nexus 1010 Manager.

Figure 2. Cisco Nexus 1010 High Availability



If one Cisco Nexus 1010 were to fail, management would automatically failover to the other Cisco Nexus 1010 without disruption of traffic or operations. For two Cisco Nexus 1010 appliances to form a high-availability pairing, 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 potential fault domain.

VSM High Availability

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

Not all virtual services blades are active on the active Cisco Nexus 1010. As long as the active and standby Cisco Nexus 1010 appliances are connected, access through a serial connection is maintained to any virtual service. 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 on their own.

A virtual service can be removed completely from both redundant Cisco Nexus 1010 appliances, or from only one. If one of a redundant pair of virtual services becomes unusable, it can be removed from just the Cisco Nexus 1010 on which it resides. This feature aids recovery by preserving the remaining virtual service in the pair. Removal of just the failed service may be necessary 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 Series 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 the VSM is created. After the first VSM is created, that software image can be used to create additional VSMs. Upgrading VSMs to a new release of the Cisco Nexus 1000V Series is available as needed.

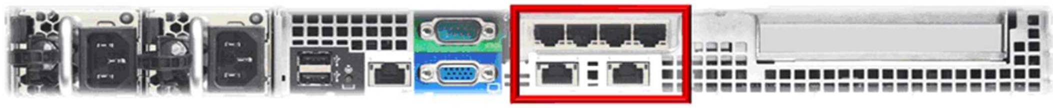
For more information about VSM high availability, see the Cisco Nexus 1000V High Availability and Redundancy Configuration Guide, Release 4.0(4)SV1(3).

http://www.cisco.com/en/US/partner/docs/switches/datacenter/nexus1000/sw/4_0_4_s_v_1_3/high_availability/configuration/guide/n1000v_ha_preface.html.

Network Connectivity

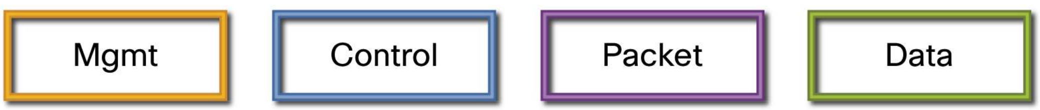
The Cisco Nexus 1010 has six Gigabit Ethernet interfaces available for network connectivity: two Gigabit Ethernet LAN interfaces on the motherboard, and four Gigabit Ethernet interfaces available through a PCI card (Figure 3).

Figure 3. Cisco Nexus 1010 Network Interfaces



Four types of traffic flows through these interfaces: management, control, packet, and data traffic. The Cisco Nexus 1010 does not reside in the data path of normal virtual machine data traffic (Figure 4). However, when the Cisco Nexus 1000V NAM Virtual Service Blade is deployed, data traffic from the selected virtual machines will flow to the Cisco Nexus 1010 to be analyzed. The decision to use or not use the NAM is one factor that influences which network connectivity option should be used to connect the Cisco Nexus 1010 to the network.

Figure 4. Color Code for Various Cisco Nexus 1010 Traffic



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.

Do not change the management VLAN on a virtual service. Since the management VLAN is inherited from the Cisco Nexus 1010, if you change it, 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.

Connectivity Options

The interfaces on the Cisco Nexus 1010 can be connected to the network in four ways. The best connectivity option for the Cisco Nexus 1010 in a particular situation depends on the customer’s needs and requirements. This section explains the four connectivity options and discusses best practices for choosing which option to deploy.

Option 1

The simplest way to connect the Cisco Nexus 1010 to the network is to use the two lights-out management (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. LOM Interfaces Carry All Traffic for the Cisco Nexus 1010

This option is preferred in cases in which customers are not using a NAM and therefore will have little or no data traffic traversing the uplinks to the Cisco Nexus 1010. The management, control, packet, and data traffic can all be using different VLANs; however, this is not a requirement. If the NAM is not currently in use, this option is recommended because it is the simplest configuration and has the lowest risk of misconfiguration.

Option 2

The second option uses the two LOM interfaces to carry management and control traffic. The other four interfaces on the PCI card would be used to carry 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 divided between two upstream switches for redundancy (Figure 6).

Figure 6. LOM Interfaces for Management and Control and Other 4 NICs for Data Traffic

This option is ideal for customers who are deploying a NAM within the Cisco Nexus 1010. The management and control traffic is kept physically separate from the data traffic, helping ensure that data traffic does not steal cycles from control traffic. 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.

Option 3

The third option uses the two LOM interfaces for management traffic, and the four interfaces on the PCI card are used 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 divided between two upstream switches for redundancy (Figure 7).

Figure 7. LOM Interfaces for Management and Other 4 NICs for Control, Packet and Data Traffic

This option is ideal for customers who are deploying a NAM within the Cisco Nexus 1010 but require a separate management network. Because control traffic is minimal, customers can still use most of the bandwidth from the four Gigabit Ethernet interfaces for NAM traffic.

Option 4

The fourth option 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 divided between two upstream switches for redundancy (Figure 8).

Figure 8. LOM Interfaces for Management, 2 NICs for Control and Packet and 2 NICs for Data Traffic

This option is ideal for customers who want to use a NAM but require separate data and control networks. Separating the control traffic from the data network helps ensure that NAM traffic will never steal cycles from control traffic and therefore affect connectivity.

Deployment Considerations

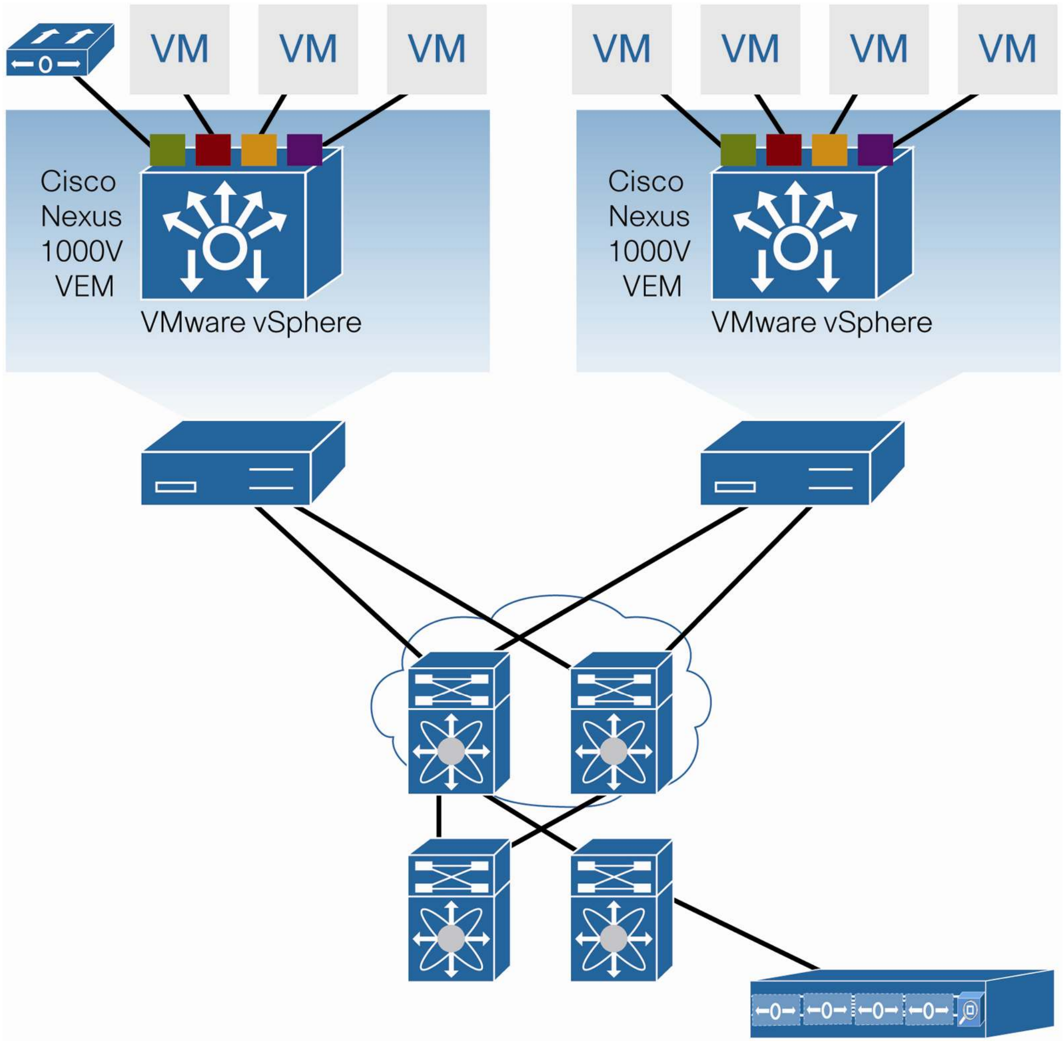
Deployment of the Cisco Nexus 1010 offers many benefits. First, because the Cisco Nexus 1010 appliance is owned and operated by the network team, deployment no longer depends on collaboration with the network, storage, and virtualization operations teams. Instead, the Cisco Nexus 1010 can be installed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

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

One option for deployment is to connect the Cisco Nexus 1010 appliance to Cisco Nexus 2000 Series Fabric Extenders or Cisco Nexus 5000 Series Switches at the access layer. Because the Cisco Nexus 1010 uses 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 helps simplify deployment by running the same operating system: Cisco NX-OS.

Figure 9 shows another option for deploying the Cisco Nexus 1010 at the aggregation layer or the Layer 2 and Layer 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 Layer 3 as explained in the previous sections. For best practices regarding Layer 2 and Layer 3 connectivity between the VSMs and VEMs, see the Cisco Nexus 1000V deployment guide.

Figure 9. Cisco Nexus 1010 Deployment at the Aggregation Layer



For More Information

For more information about the Cisco Nexus 1000V Series, please refer to the following URLs:

- 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

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 C07-603623-00 06/10

