



Newer Cisco SBA Guides Available

This guide is part of an older series of Cisco Smart Business Architecture designs. To access the latest Cisco SBA Guides, go to <http://www.cisco.com/go/sba>

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.





SBA

BORDERLESS
NETWORKS

DEPLOYMENT
GUIDE

LAN and Data Center Collapsed Core Using Cisco Nexus 7000 Deployment Guide

● ● ● SMART BUSINESS ARCHITECTURE

August 2012 Series

Preface

Who Should Read This Guide

This Cisco® Smart Business Architecture (SBA) guide is for people who fill a variety of roles:

- Systems engineers who need standard procedures for implementing solutions
- Project managers who create statements of work for Cisco SBA implementations
- Sales partners who sell new technology or who create implementation documentation
- Trainers who need material for classroom instruction or on-the-job training

In general, you can also use Cisco SBA guides to improve consistency among engineers and deployments, as well as to improve scoping and costing of deployment jobs.

Release Series

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

The Release Notes for a series provides a summary of additions and changes made in the series.

All Cisco SBA guides include the series name on the cover and at the bottom left of each page. We name the series for the month and year that we release them, as follows:

month year Series

For example, the series of guides that we released in August 2012 are the “August 2012 Series”.

You can find the most recent series of SBA guides at the following sites:

Customer access: <http://www.cisco.com/go/sba>

Partner access: <http://www.cisco.com/go/sbachannel>

How to Read Commands

Many Cisco SBA guides provide specific details about how to configure Cisco network devices that run Cisco IOS, Cisco NX-OS, or other operating systems that you configure at a command-line interface (CLI). This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

Commands that specify a value for a variable appear as follows:

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

```
class-map [highest class name]
```

Commands shown in an interactive example, such as a script or when the command prompt is included, appear as follows:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
wrr-queue random-detect max-threshold 1 100 100 100 100 100  
100 100 100
```

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

```
interface Vlan64  
ip address 10.5.204.5 255.255.255.0
```

Comments and Questions

If you would like to comment on a guide or ask questions, please use the [SBA feedback form](#).

If you would like to be notified when new comments are posted, an RSS feed is available from the SBA customer and partner pages.

Table of Contents

What's In This SBA Guide.....	1	Summary	12
Route to Success	1	For Additional Information.	12
About This Guide	1	Appendix A: Product List	13
Introduction.....	2	Appendix B: Configuration Files.....	14
Business Overview.....	2	Nexus 7000 Core Switch 1	14
Technology Overview.....	2	Nexus 7000 Core Switch 2.....	18
Deployment Details.....	6	Appendix B: Changes.....	23
Configuring the Core Layer	6		

What's In This SBA Guide

Cisco SBA Borderless Networks

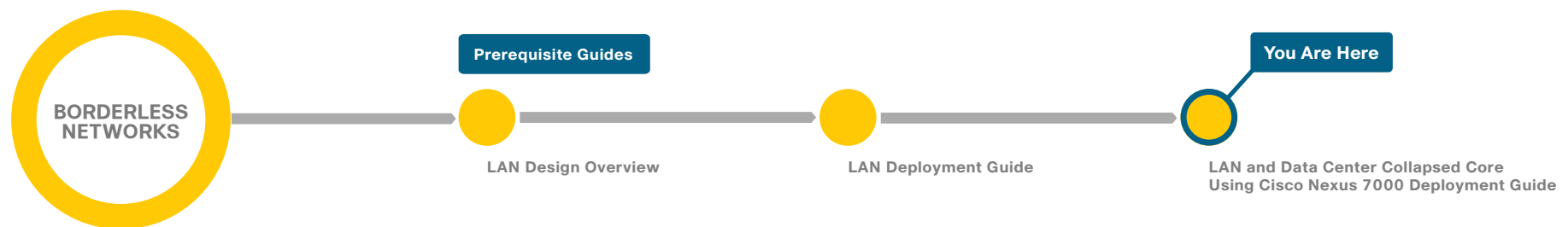
Cisco SBA helps you design and quickly deploy a full-service business network. A Cisco SBA deployment is prescriptive, out-of-the-box, scalable, and flexible.

Cisco SBA incorporates LAN, WAN, wireless, security, data center, application optimization, and unified communication technologies—tested together as a complete system. This component-level approach simplifies system integration of multiple technologies, allowing you to select solutions that solve your organization's problems—without worrying about the technical complexity.

Cisco SBA Borderless Networks is a comprehensive network design targeted at organizations with up to 10,000 connected users. The SBA Borderless Network architecture incorporates wired and wireless local area network (LAN) access, wide-area network (WAN) connectivity, WAN application optimization, and Internet edge security infrastructure.

Route to Success

To ensure your success when implementing the designs in this guide, you should first read any guides that this guide depends upon—shown to the left of this guide on the route below. As you read this guide, specific prerequisites are cited where they are applicable.



About This Guide

This *deployment guide* contains one or more deployment chapters, which each include the following sections:

- **Business Overview**—Describes the business use case for the design. Business decision makers may find this section especially useful.
- **Technology Overview**—Describes the technical design for the business use case, including an introduction to the Cisco products that make up the design. Technical decision makers can use this section to understand how the design works.
- **Deployment Details**—Provides step-by-step instructions for deploying and configuring the design. Systems engineers can use this section to get the design up and running quickly and reliably.

You can find the most recent series of Cisco SBA guides at the following sites:

Customer access: <http://www.cisco.com/go/sba>

Partner access: <http://www.cisco.com/go/sbachannel>

Introduction

Business Overview

As the LAN environment at a larger facility grows, it often creates the need to use multiple LAN distribution layer blocks. As the number of required distribution layer blocks in a facility grows beyond two or three, a solution is required to reduce the complexity and cost of fully meshing all interconnectivity while maintaining a design that provides a reliable infrastructure.

When an organization has a large primary site, the organization's primary data center is often located there also. If the data center is large enough that it also includes multiple distribution layer blocks, then the data center also needs a solution for scaling interconnectivity.

The similarities between the needs of the campus and the data center present an opportunity to consolidate the needs into a single set of devices, which can save both operational and equipment costs.

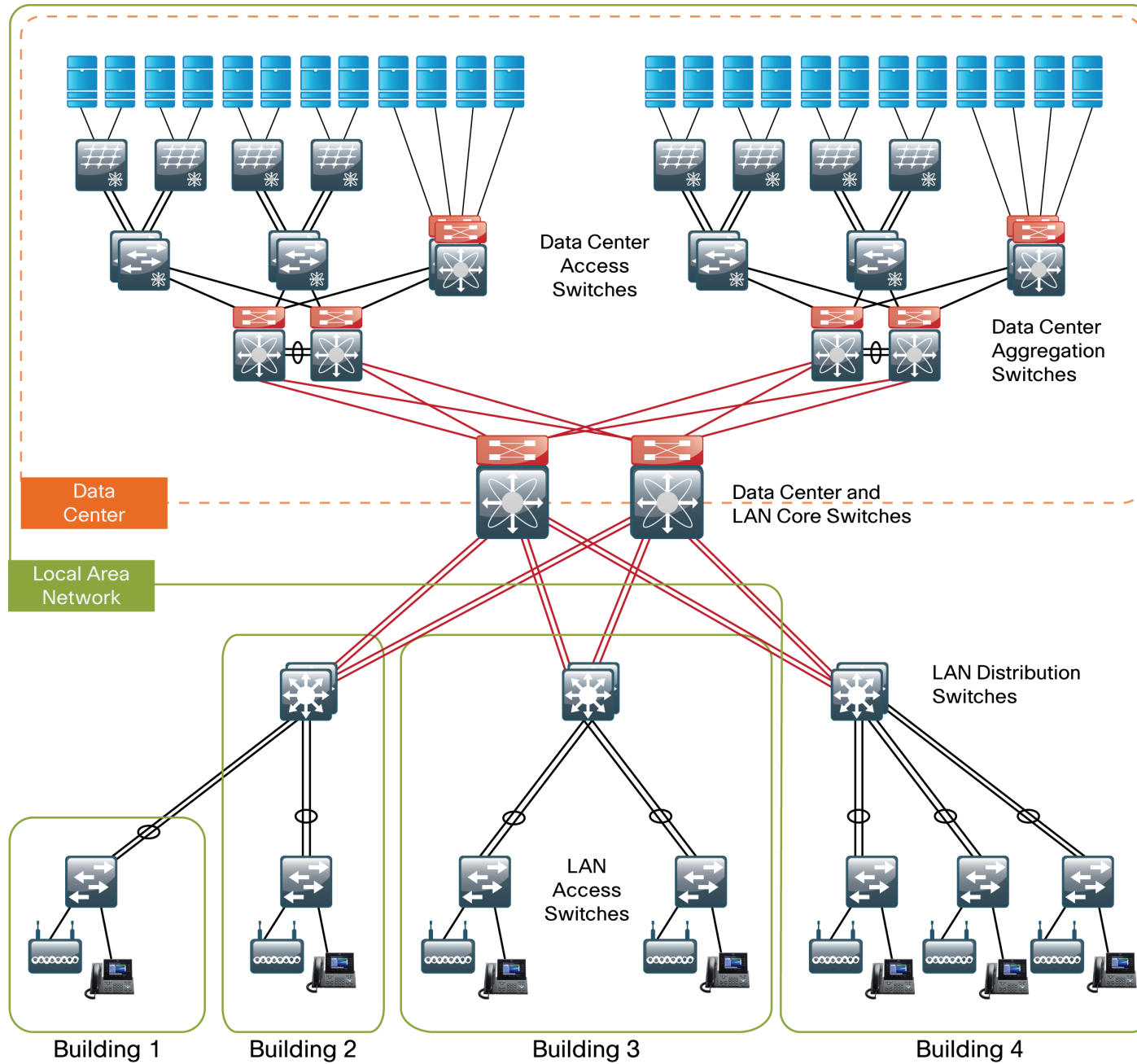
Technology Overview

Cisco has a rich tradition of building scalable and robust LAN and campus networks using the Cisco® Catalyst switch line. The Catalyst 6500 series switch has a long history as the flagship of large campus aggregation and core layer networks. As of 2008, state-of-the-art data center networks started using Cisco Nexus family switching products. Specifically, data center aggregation (also referred to as distribution), and core layers are built using the Cisco Nexus 7000 Series switch.

The Cisco Nexus 7000 Series delivers high performance, port density, availability, and resiliency with a comprehensive feature set targeted for the core of data center and campus LAN networks. The Cisco Nexus 7000 Series switch effectively addresses data center core and aggregation requirements, such as a high-density 10 Gigabit Ethernet interface, robust Layer 3 protocols, and a zero-service disruption architecture. In environments where the core device also acts as a data center interconnect (DCI) platform, the Cisco Nexus 7000 Series switch supports Overlay Transport Virtualization (OTV), an industry solution that enables the extension of Layer 2 over Layer 3 networks, without the operational complexities of other interconnect solutions.

Outside of the data center, the Cisco Nexus 7000 can also be used in the core layer of the campus LAN. The main driver for using the Cisco Nexus 7000 Series in the core of a campus LAN network is the ability to collapse the LAN and the data center core, which usually are on separate pairs of devices, onto a single pair of Cisco Nexus 7000 Series switches. Figure 1 shows a collapsed view of the data center and LAN core.

Figure 1 - Collapsed data center and LAN core

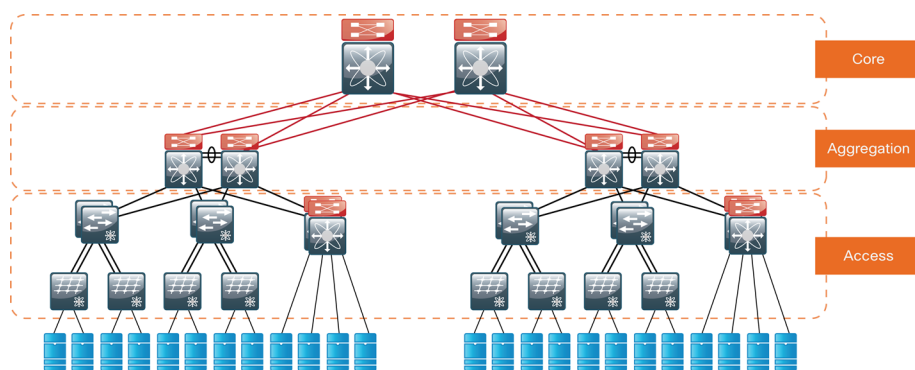


The Cisco Nexus 7000 Series switch is uniquely positioned as the platform to support a consolidated campus LAN and data center core because of its high 10 Gigabit Ethernet density, resiliency and high availability, and extensive support of virtualization.

With higher density and the potential for combining multiple layers, the bar for availability and resiliency moves higher. From a high-availability standpoint, the Cisco Nexus 7000 Series is a very robust and resilient platform. In addition to the resiliency that is built into every hardware component of the Cisco Nexus 7000 Series, its operating system, Cisco NX-OS, provides a unique, highly-resilient capability that supports non-stop packet forwarding, even in the event of a software upgrade, with the hitless in-service software upgrade (ISSU) feature. Furthermore, Cisco NX-OS on the Cisco Nexus 7000 Series supports graceful restart as well as non-stop routing (NSR) functionalities for routing protocols. The operating system is capable of detecting and restarting a faulty process, without disrupting the other operations of the switch. The zero-service disruption architecture of the Cisco Nexus 7000 Series switch is paramount with a collapsed LAN and data center core, where infrastructure failure or maintenance windows can have a broad impact.

In a data center network with a three-tier architecture (see Figure 2), the Cisco Nexus 7000 Series switch is the state-of-the-art Layer 3 switch for the core and aggregation layers. Typically the aggregation layer is the Layer 2 or Layer 3 boundary.

Figure 2 - Three-tier data center architecture



Virtual device contexts (VDCs) allow a Cisco Nexus 7000 Series switch to be carved up into logically separate devices. Each of those entities can be managed separately to allow operational independence and isolation from each other. This isolation can be useful for environments where layers of networks may be physically combined while logically staying independent or where organizational units have to be separated from a management and configuration access standpoint (such as for compliance reasons).

For example, a data center core and aggregation can fall into one pair of switches. To still follow the hierarchical network model as well as to respect operational boundaries, device virtualization can be used via a virtual device context (VDC), which is the first control-plane virtualization in a network device. Using the Cisco Nexus 7000 Series Supervisor Module 1, a single switch can be carved up into a maximum of four logical switches (that is, four VDCs), where resources such as interfaces, memory, and so on are explicitly allocated to the respective VDC. Besides offering consolidation and operational benefits, the configuration of VDCs offers flexible separation and distribution of resources. The hardware and software isolation per VDC not only delineates administrative contexts, but also allows scaling the overall systems. The virtualization capabilities of VDCs are key to deploying a collapsed LAN and data center core on a single Cisco Nexus 7000 Series switch with multiple logical cores.

The aggregation layer usually acts as a Layer 2 or Layer 3 boundary. Along with routing technologies, the Cisco Nexus 7000 Series switch offers flexible switching functionalities, such as virtual Port Channels (vPC), rapid spanning tree, and Port Channels that are all handled in a stateful fashion to guarantee a very high level of system reliability.

Core Layer Architecture

The core layer of the LAN is a critical part of the scalable network, yet by design, it is one of the simplest. Like the distribution layer, the core layer aggregates connectivity, but for multiple distribution layers instead of access layers. As networks grow beyond three distribution layers in a single location, a core layer should be used to optimize the design.

Beyond the simple aggregation of connectivity, the core layer serves to reduce the number of paths between distribution layers, which in turn lowers the time required to converge the network after a failure. By upgrading bandwidth between a distribution layer and the core, multiple distribution layer blocks can benefit from the increase versus the need to upgrade the bandwidth to every other device in a design without a core. The core layer is especially relevant to designs where the data center resources might be collocated with the LAN.

In large modular and scalable LAN designs, a core layer is used to aggregate multiple user connectivity distribution layer blocks. In designs with a collocated data center, the core provides high speed fanout connectivity to the rest of the network. The core layer also serves as the interconnect for the Wide Area Network (WAN) and Internet Edge distribution layer blocks. Because of this central point of connectivity for all data flows, the core is part of the backbone IP routing address space and is designed to be highly resilient to protect from component-, power-, or operational-induced outages.

The core layer in the SBA LAN design is based on two physically and logically separate switches. Connectivity to and from the core should be Layer 3 only. No VLANs should span the core to drive increased resiliency and stability. Since the core does not need to provide the same services or boundaries that the distribution layer does, the two-box design does not significantly increase the complexity of the solution. The core layer should not contain highly complex or high-touch services that require constant care and tuning to avoid downtime required by complex configuration changes, increased software upgrades for new services, or links that toggle up/down as part of normal operations like user endpoint connectivity.

The core is built on dual switches to provide a completely separate control plane housed on each switch, which provides redundant logic, line cards, hardware, and power for the backbone operation. Each distribution layer block, router, or other appliance connecting to the core should be dual-homed with an EtherChannel or link to each core switch. This dual homed approach provides Equal Cost Multiple Path (ECMP) load sharing of IP traffic across links for traffic traversing the core, and fast failover based on either EtherChannel or ECMP alternate routes without waiting for routing protocol topology changes to propagate the network.

The core is designed to be high speed and provides for connectivity ranging from Gigabit Ethernet, Gigabit EtherChannel, 10 Gigabit Ethernet, and up to 10 Gigabit EtherChannel. The core can provide non-blocking bandwidth based on design and configuration. EtherChannel links homed to a switch should be spread across line cards when possible.

The collapsed core Nexus 7000 switches should be provisioned with dual supervisors. A Nexus 7000 system provisioned with dual supervisors is capable of supporting Stateful Switchover (SSO) and Nonstop Forwarding (NSF) for completely hitless In-Service Software Upgrades (ISSU). SSO can help protect the core in the event of control plane hardware or software failures. NSF provides enhanced Layer 3 resilience for dual supervisor based systems.

Attaching the Data Center Aggregation Layer

The links from the core layer facing the data center aggregation or distribution layer are configured in the same way as the links facing campus distribution layers. More specifically these are routed Layer 3 interfaces with point-to-point subnets and a routing configuration as outlined below.

The data center aggregation layer configuration follows a similar model as the campus distribution layer. Integration of services such as firewalling, intrusion prevention and load-balancing are typically added. Design guide references and sample configurations for using the Cisco Nexus 7000 Series switch in the data center aggregation layer are listed at the end of this document.

Deployment Details

This chapter describes the configuration for the core layer using the Cisco Nexus 7000 Series. Only the core layer relevant features are described. The core layer is typically a Layer 3 configured device; therefore, deployment details of Cisco Nexus 7000 Series Layer 2 features, such as spanning tree, VLAN Trunking Protocol (VTP), and virtual Port Channel (vPC), are intentionally omitted. For those scenarios that require having spanning tree as a safeguard, Rapid Spanning Tree Protocol (RSTP) is enabled by default on the Cisco Nexus 7000 Series switch and does not require any additional configuration.

The core layer design is based on dual switches; therefore, programming of the core devices is symmetrical for simplicity except IP addressing for interfaces and services that must be unique in the network. Because we cover the global configuration options in detail in the access layer section, the commands are listed here for easy reference.

Process

Configuring the Core Layer

1. Configure LAN Switch Universal Settings
2. Core Layer Switch Global Configuration
3. Configure IP Multicast Routing
4. Connect to Distribution Layer

Some platforms require a one-time, initial configuration before you configure the features and services of the switch. The initial configuration includes installing the appropriate license and enabling feature commands or enabling a grace period for trying or testing features.

Software license prerequisites

The Cisco Nexus 7000 Series offers a simplified software management mechanism based on software licenses. These licenses are enforceable on a chassis basis and enable a full suite of functionalities. As the core layer is characterized by a Layer 3 configuration, the Cisco Nexus 7000 Series switch requires the Enterprise LAN license, which enables routing functionalities.

The VDC configuration is not included in this addendum. However, for those deployments where VDC is recommended, the Advanced LAN license needs to be installed. Other baseline features (such as QoS and Layer 2) do not require any additional licenses.

Feature commands

Due to the modular nature of Cisco NX-OS, processes are only started when a feature is enabled. As a result, commands and command chains only show up after the feature has been enabled. For licensed features, the feature **feature-name** command can only be used after the appropriate license is installed. For trial and testing purposes, there is a grace period of 120 days during which all features can be tried within the system. To enable this grace period, use the **license grace-period** command.

Procedure 1

Configure LAN Switch Universal Settings

Within this design, there are features and services that are common across all LAN switches regardless of the type of platform or role in the network. These are system settings that simplify and secure the management of the solution.

This procedure provides examples for some of those settings. The actual settings and values depend on your current network configuration.



Tech Tip

The device management configuration in this section assumes the Nexus 7000 is being deployed in a non-VDC environment that is using the default VDC. If the deployment requires multiple VDCs, some of the management variables may also need to exist in the configured VDCs. For more information, design guide references and sample configurations are listed at the end of this document.

Table 1 - Examples of common network services used in the deployment

Network Service	Address
Domain Name	cisco.local
Multicast Rendezvous Point (RP)	10.4.40.254
Authentication Control System	10.4.48.15
Network Time Protocol Server	10.4.48.17
ELGRP Autonomous System (AS)	100
IP Multicast Range	239.1.0.0/16

Step 1: Configure the device hostname.

```
hostname [hostname]
```

Step 2: Configure device management protocols.

Secure Shell (SSH) is an application and a protocol that provide a secure replacement to Remote Shell (RSH) and Telnet. Secure management access is enabled through the use of the SSH protocol. The protocol is encrypted for privacy.

SSH is enabled by default and does not require any specific configuration. Cisco NX-OS can store SSH authentication keys and, therefore, simplify the login process while still using strong authentication. Non-secure protocols like Telnet are disabled by default. SSH requires a domain name to be set.

```
ip domain-name cisco.local
```

Simple Network Management Protocol (SNMP) is enabled to allow a network management system (NMS) to manage the network infrastructure devices. SNMPv2c is configured for both a read-only (network-operator) and read-write (network-admin) community string.

```
snmp-server community cisco group network-operator
snmp-server community cisco123 group network-admin
```

Step 3: Configure secure user authentication.

Authentication, authorization, and accounting (AAA) is enabled for access control. All management access to the network infrastructure devices is controlled with AAA. The Cisco Authentication Control System is the AAA server used in this architecture. Configuration of ACS is discussed in the *Cisco SBA—Borderless Networks Device Management Using ACS Deployment Guide*.

TACACS+ is the primary protocol used to authenticate management logins on the infrastructure devices to the AAA server. A local AAA user database is also defined each network infrastructure device to provide a fallback authentication source in case the centralized TACACS+ server is unavailable.

```
feature tacacs+
username admin password cisco123 role network-admin
tacacs-server host 10.4.48.15 key SecretKey
aaa group server tacacs+ tacacs
    server 10.4.48.15
aaa authentication login default group tacacs
```

Step 4: If you have a network where network operational support is centralized, you can increase network security by using an access list to limit the networks that can access your device. In this example, only devices on the 10.4.48.0/24 network will be able to access the device via SSH or SNMP.

```
ip access-list vty-acl-in
    permit tcp 10.4.48.0/24 any eq 22
line vty
    ip access-class vty-acl-in in
!
ip access-list snmp-acl
    permit udp 10.4.48.0/24 any eq snmp
snmp-server community cisco use-acl snmp-acl
snmp-server community cisco123 use-acl snmp-acl
```



Tech Tip

If you configure an access-list on the vty interface, you may lose the ability to use ssh to login from one router to the next for hop-by-hop troubleshooting.

Step 5: Configure a synchronized clock for management.

The Network Time Protocol (NTP) is designed to synchronize a network of devices. An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two devices to within a millisecond of one another.

Network devices should be programmed to synchronize to a local NTP server in the network. The local NTP server typically references a more accurate clock feed from an outside source. Configuring console messages, logs, and debug output on switches, routers, and other devices in the network to provide time stamps on output allows cross-referencing of events in a network.

On the Cisco Nexus 7000, NTP can only be configured in the default VDC. To configure NTP in Cisco NX-OS, use the following feature command and specify the NTP server. The example also shows how to enable the correct time zone and daylight savings settings.

```
ntp server 10.4.48.17
clock timezone PST -8 0
clock summer-time PDT 1 Sunday March 02:00 1 Sunday November
02:00 60
!
logging timestamp milliseconds
```

Step 6: Configure device resiliency features.

UniDirectional Link Detection (UDLD) is a Layer 2 protocol that enables devices connected through fiber-optic or twisted-pair Ethernet cables to monitor the physical configuration of the cables and detect when a unidirectional link exists. When UDLD detects a unidirectional link, it disables the affected port and alerts you. Unidirectional links can cause a variety of

problems, including spanning-tree loops, black holes, and non-deterministic forwarding. In addition, UDLD enables faster link failure detection and quick reconvergence of port trunks, especially with fiber, which can be susceptible to unidirectional failures.

In normal mode, if the link state of the port is determined to be unidirectional, then the port continues to forward traffic normally, but the port is marked as undetermined. The port cycles through the regular spanning tree protocol states and continues to forward traffic. In aggressive mode, the port enters the error disabled state (errdisable) and effectively shuts down. To recover from errdisable, you have to shut down and restart the port by issuing the **shutdown** and **no shutdown** commands. UDLD does not function any differently for either mode. The same messages are sent, and the same messages are expected to be received. The modes only differ in the way that UDLD reacts to a unidirectional link failure.

After the UDLD feature is turned on, UDLD operation is automatically enabled in the global configuration.

```
feature udld
```

Step 7: Configure events to log to console.

With the Nexus 7000, you can use system message logging variables to control the destination and to filter the severity level of messages that system processes generate. You can configure logging to terminal console sessions, a log monitor file, and to syslog servers on remote systems.

By default, logging of messages for events, such as link up/down, Enhanced Interior Gateway Routing Protocol (EIGRP) and Protocol Independent Multicast (PIM) neighbor status changes, are enabled to log to the logging monitor file. To display these message types to the console port as well, you must set the console port speed to operate at 38400 bps or greater, and change the console logging level to include level 5 (notifications).

```
logging console 5
line console
speed 38400
```

Procedure 2 Core Layer Switch Global Configuration

Step 1: Configure an in-band management interface.

The loopback interface is a logical interface that is always reachable as long as the device is powered on and any IP interface is reachable to the network. Because of this capability, the loopback address is the best way to manage the switch in-band. Layer-3 process and features are also bound to the loopback interface to ensure processes resiliency.

The loopback address is commonly a host address with a 32-bit address mask. Allocate the loopback address from the core IP address block.

```
interface loopback 0
  ip address [ip address]/32
```

After the IP loopback interface is created, you can tie SNMP to that interface address.

```
snmp-server source-interface trap loopback 0
```

Step 2: Configure IP unicast routing.

You must enter the **feature eigrp** command to enable this feature. All the EIGRP configuration commands appear only after the feature is enabled.

Cisco NX-OS routing configuration follows an interface-centric model. Instead of adding networks to be advertised via network statements, EIGRP is enabled on a per-interface-basis. Each Layer 3 interface that carries a network that may be advertised via EIGRP requires the `ip router eigrp` statement. In this configuration, the only parameter configured under the EIGRP process (`router eigrp 100`) is the router-ID. The loopback 0 IP address is used for the EIGRP router ID.

```
feature eigrp
router eigrp 100
  router-id [ip address of loopback 0]
interface loopback 0
  ip router eigrp 100
```

Quality of Service

The core layer quality of service (QoS) configuration honors the QoS values present in the traffic because classification and marking of traffic has already happened at the edge of the network. For traffic not hitting any congestion point when traversing through the core, the original QoS (DSCP) values are preserved and not altered. In case congestion occurs once traffic travels through the core, a reclassification or markdown can occur.

A Cisco Nexus 7000 Series switch has QoS enabled by default. All interfaces are configured to be trusted, which means that the QoS values present in the IP packets are honored for queuing and scheduling. By default then, no QoS configuration is required in the core.

Procedure 3 Configure IP Multicast Routing

IP Multicast allows a single IP data stream to be sent from a single source to multiple receivers and be replicated by the infrastructure (that is, routers and switches). Using IP Multicast is much more efficient than multiple unicast streams or a broadcast stream that would propagate everywhere. IP Telephony Music on Hold and IP Video Broadcast Streaming are two examples of IP Multicast applications.

To receive a particular IP Multicast data stream, end hosts must join a multicast group by sending an Internet Group Management Protocol (IGMP) message to their local multicast router. In a traditional IP Multicast design, the local router consults another router in the network that is acting as an RP to map receivers to active sources so they can join their streams.

The RP is a control-plane operation that should be placed in the core of the network or close to the IP Multicast sources on a pair of Layer 3 switches or routers. In this design, which is based on pim sparse mode multicast operation, Cisco uses Anycast RP to provide a simple yet scalable way to provide a highly resilient RP environment.

Step 1: Enable PIM.

To enable operations and commands required for IP Multicast operation you must first enable the feature.

```
feature pim
```

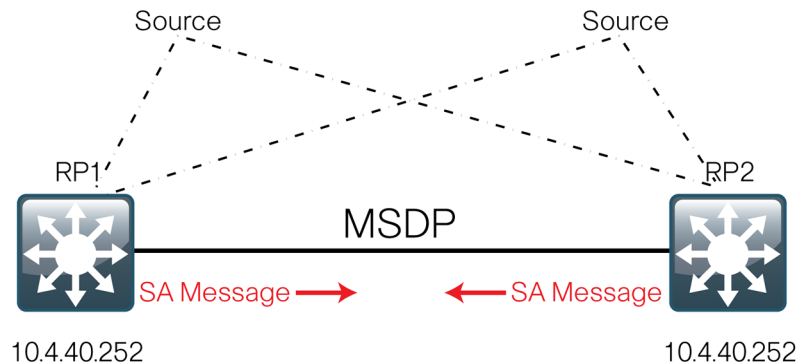

Step 2: Configure loopback interface for RP.

To enable Anycast RP operation, the first step is to configure a second loopback interface on each of the core switches. The key is that this second loopback interface has the same IP address on both core switches and uses a host address mask (32 bits). All routers then point to this common IP address on **loopback 1** for the RP. We configured the RP address from the core IP address space.

```
interface loopback 1
 ip address 10.4.40.252/32
 ip pim sparse-mode
 ip router eigrp 100
```

Step 3: Configure Multicast Source Discovery Protocol (MSDP).

The final step for the Anycast RP configuration is to enable MSDP to run between the two core RP switches.



To enable MSDP, you must use unique addresses at each end of the link; therefore, we use the loopback 1 addresses of each core router to configure the MSDP session. Enter the **feature msdp** command first to enable the feature.

On core switch #1:

```
feature msdp
 ip msdp originator-id loopback 0
 ip msdp peer 10.4.40.253 connect-source loopback 0
 ! The IP address for the listed above is the core switch #2
 loopback
```

On core switch #2:

```
feature msdp
 ip msdp originator-id loopback 0
 ip msdp peer 10.4.40.254 connect-source loopback 0
 ! The IP address for the listed above is the core switch #1
 loopback
```

The MSDP configuration is complete and convergence around a failed RP is now as fast as the unicast routing protocol (EIGRP) convergence. You can see the MSDP protocol session activate later as you enable the routing links between the core switches and the distribution layer blocks that establish Layer 3 connectivity. Use the **show ip msdp summary** command for verification.

Every Layer 3 switch and router must know the address of the IP multicast RP, including the core switches that are serving as the RP. This design uses AutoRP to announce candidate RPs, which are the core switches, to the rest of the network.

Step 4: Configure AutoRP candidate RPs.

The **send-rp-announce** command in conjunction with the **group-list** option advertises the RP address, with the multicast range the device is willing to serve, as a candidate RP to the AutoRP mapping agents.

```
ip pim send-rp-announce loopback 1 group-list 239.1.0.0/16
```

Step 5: Configure AutoRP mapping agent.

The AutoRP mapping agent listens for candidate RPs and then advertises to the rest of the network the list of available RPs. The **send-rp-discovery** command enables the core switches to act as AutoRP mapping agents.

```
ip pim send-rp-discovery loopback 0 scope 32
 ip pim register-source loopback 0
```

Step 6: Configure devices to listen to AutoRP announcements.

All network devices in the organization, including the RPs, must be configured to listen to the AutoRP announcements from the mapping agents.

```
ip pim auto-rp listen
```

In the event that you add a core layer to your existing network and the RP is currently configured on a distribution layer, you may want to move the RP to the core.

With Anycast RP, you can move the RP to a new location by programming the RP address on the loopback 1 interfaces at the new location, and then enabling and establishing IP multicast, MSDP peering, and AutoRP.

All remote routers learn the location of the new RP identities that are advertising the same RP address, which simplifies the move and reduces disruption to the IP multicast environment.

All Layer 3 interfaces in the network must be enabled for sparse mode multicast operation.

```
interface loopback 0
  ip pim sparse-mode
```

Procedure 4 Connect to Distribution Layer

In this design, links in the core layer are configured as point-to-point Layer 3 routed links or Layer 3 routed EtherChannels.

If you are using the Cisco Catalyst 6500 VSS 4T system in the distribution layer, Cisco recommends that all peer-connected links are EtherChannel links. EtherChannel to the Catalyst 6500 VSS provides for optimal forwarding because a packet that is received on the switch is forwarded out a link on that same switch in normal operation instead of traversing the VSL link.

Other benefits of EtherChannel to any single physical or logical device are that it makes it easier for you to grow bandwidth without changing the topology and that a single link failure uses EtherChannel recovery versus using Equal-cost multi-path (ECMP) or a routing topology change to reroute the data flows for fastest recovery.

Since the core links are point-to-point routed links, use 30-bit IP address subnets and masks, and do not use Switched Virtual Interfaces (SVI).

Step 1: For Layer 3 connected devices that do not require EtherChannel, configure routed interfaces with the IP address directly on the physical interface, and do not use an SVI.

```
interface ethernet [number]
  no switchport
  logging event link-status
  ip address [ip address] / [mask]
  ip pim sparse-mode
  ip router eigrp 100
```

Step 2: (Optional) When creating a Layer 3 EtherChannel (also referred to as a port channel) you can create the logical port-channel interface first. Before you can create a port-channel that uses LACP protocol, you must first enable the LACP feature command.

```
feature lacp
interface port-channel [number]
  no switchport
  ip address [ip address] / [mask]
  ip pim sparse-mode
  ip router eigrp 100
```

Step 3: Configure the physical interfaces to tie to the logical port channel by using the **channel-group** command. The number for the port channel and the channel group match for every unique port channel you build.



Reader Tip

Note that Cisco NX-OS labels all Ethernet interfaces as interface ethernet regardless of the actual interface speed. This style of labeling is different than IOS, which uses interface GigabitEthernet, interface TenGigabitEthernet and so on.

```
interface ethernet [interface 1] - [interface 2]
  channel-group [number] mode active
```

Make sure you enter the **no shutdown** command to bring up the port channel interface and the channel member interfaces to an operational state.

Summary

The Cisco Nexus 7000 Series is a key platform for the data center and campus core deployments.

Built around the flexible and scalable Cisco NX-OS operating system, the Cisco Nexus 7000 Series combines hardware and software to deliver unprecedented high availability. Full hardware redundancy and sophisticated mechanisms for recovering from failure conditions make the Cisco Nexus 7000 Series a very robust, zero-downtime platform for core networks for both scenarios of collapsed data center and campus core or separate cores.

The VDC technology provides a variety of benefits ranging from simplified operations, hardware and software resources separation, virtualization, and consolidation. While relevant to all the core architectures, VDC adds great value in a collapsed core environment. In this scenario, each VDC can virtualize a core device, presenting the physical switch as multiple logical devices with their own unique set of VLANs, IP routing tables, VRFs, and physical interfaces.

Furthermore, scalable and efficient multicast capabilities, along with a flexible QoS model, enable the Cisco Nexus 7000 Series to embrace the Cisco Medianet solution.

For Additional Information

Cisco NX-OS Product Page: <http://www.cisco.com/go/nxos>

Cisco NX-OS / IOS Comparison: http://docwiki.cisco.com/wiki/Cisco_Nexus_7000_NX-OS/IOS_Comparison_Tech_Notes

Cisco Nexus 7000 Series Product Page: <http://www.cisco.com/go/nexus7000>

Cisco Nexus 7000 Series Product Documentation: http://www.cisco.com/en/US/products/ps9402/tsd_products_support_series_home.html

Medianet on Cisco.com: <http://www.cisco.com/go/medianet>

Borderless Networks: <http://www.cisco.com/go/borderless>

Data Center Design and Configuration documents:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/DC_3_0/DC-3_0_IPInfra.html

http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/nx_7000_dc.html

Appendix A: Product List

Core Layer

Functional Area	Product Description	Part Numbers	Software
Core Switch	Nexus 7000 C7010 (10 Slot), Chassis	N7K-C7010	5.2(4)
	Nexus 7000 C7009 (9 Slot), Chassis	N7K-C7009	
	Nexus 7000 Series Supervisor Module Includes External 8Gb flash	N7K-SUP1	
	Nexus 7000 48-port GigE Mod (SFP)	N7K-M148GS-11L	
	Nexus 7000 32-port 10 GigE Module	N7K-M132XP-12L	
	Nexus 7000 8-port 10 GigE Ethernet Module X2	N7K-M108X2-12L	

Appendix B: Configuration Files

Nexus 7000 Core Switch 1

```
version 5.2(4)
hostname N7010-1
vdc N7010-1 id 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource monitor-session minimum 0 maximum 2
  limit-resource monitor-session-erspan-dst minimum 0 maximum 23
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 96 maximum 96
  limit-resource u6route-mem minimum 24 maximum 24
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8

feature tacacs+
feature pim
feature msdp
feature eigrp
feature udld
feature lacp

username admin password 5 $1$1YiN9ceM$sciBUhPWLdJgNc/XkkLln/
role network-admin
ip domain-lookup
ip domain-name cisco.local
tacacs-server host 10.4.48.15 key 7 "VagwwtFjq"
aaa group server tacacs+ tacacs
  server 10.4.48.15
ip access-list snmp-acl
```

```
10 permit udp 10.4.48.0/24 any eq snmp
ip access-list vty-acl-in
  10 permit tcp 10.4.48.0/24 any eq 22
copp profile strict
snmp-server user admin network-admin auth md5
0xcad0ba9f139f27f1266c4750f0e6f861
  priv 0xcad0ba9f139f27f1266c4750f0e6f861 localizedkey
rmon event 1 log trap public description FATAL(1) owner PMON@
FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@
CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@
ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@
WARNING
rmon event 5 log trap public description INFORMATION(5) owner
PMON@INFO
snmp-server community cisco123 group network-admin
snmp-server community cisco group network-operator
snmp-server community cisco123 use-acl snmp-acl
snmp-server community cisco use-acl snmp-acl
ntp server 10.4.48.17
aaa authentication login default group tacacs

vrf context management
  ip route 0.0.0.0/0 10.194.112.65
vlan 1

interface port-channel30
  description Etherchannel link to D6500VSS
  ip address 10.4.40.9/30
  ip router eigrp 100
  ip pim sparse-mode

interface port-channel31
  description Connection to D3750X
  ip address 10.4.40.13/30
```



```
ip router eigrp 100
ip pim sparse-mode

interface Ethernet1/1
  channel-group 31 mode active
  no shutdown

interface Ethernet1/2
  channel-group 31 mode active
  no shutdown

interface Ethernet1/3

interface Ethernet1/4

interface Ethernet1/5
  no shutdown

interface Ethernet1/6

interface Ethernet1/7

interface Ethernet1/8

interface Ethernet1/9

interface Ethernet1/10

interface Ethernet1/11

interface Ethernet1/12

interface Ethernet1/13

interface Ethernet1/14

interface Ethernet1/15
```

```
interface Ethernet1/16

interface Ethernet1/17

interface Ethernet1/18

interface Ethernet1/19

interface Ethernet1/20

interface Ethernet1/21

interface Ethernet1/22

interface Ethernet1/23

interface Ethernet1/24

interface Ethernet1/25

interface Ethernet1/26

interface Ethernet1/27

interface Ethernet1/28

interface Ethernet1/29

interface Ethernet1/30

interface Ethernet1/31

interface Ethernet1/32

interface Ethernet1/33
```

```

interface Ethernet1/34

interface Ethernet1/35

interface Ethernet1/36

interface Ethernet1/37

interface Ethernet1/38

interface Ethernet1/39

interface Ethernet1/40

interface Ethernet1/41

interface Ethernet1/42

interface Ethernet1/43

interface Ethernet1/44

interface Ethernet1/45

interface Ethernet1/46

interface Ethernet1/47

interface Ethernet1/48

interface Ethernet4/1
    channel-group 30 mode active
    no shutdown

interface Ethernet4/2
    channel-group 30 mode active
    no shutdown

```

```

interface Ethernet4/3
    description IE-D3750X Ten1/1/1
    ip address 10.4.40.65/30
    ip router eigrp 100
    ip pim sparse-mode
    no shutdown

interface Ethernet4/4
    no shutdown

interface Ethernet4/5
    description D4507 Te1/12
    ip address 10.4.40.17/30
    ip router eigrp 100
    ip pim sparse-mode
    no shutdown

interface Ethernet4/6
    description WAN-D3750X Te2/1/1
    ip address 10.4.40.41/30
    ip router eigrp 100
    ip pim sparse-mode
    no shutdown

interface Ethernet4/7
    description Link to DC5548UPa Eth1/19
    ip address 10.4.40.49/30
    ip router eigrp 100
    ip pim sparse-mode
    no shutdown

interface Ethernet4/8
    description Link to DC5548UPb Eth1/19
    ip address 10.4.40.53/30
    ip router eigrp 100
    ip pim sparse-mode

```

```

no shutdown

interface Ethernet4/9

interface Ethernet4/10

interface Ethernet4/11

interface Ethernet4/12

interface Ethernet4/13

interface Ethernet4/14

interface Ethernet4/15

interface Ethernet4/16

interface Ethernet4/17

interface Ethernet4/18

interface Ethernet4/19

interface Ethernet4/20

interface Ethernet4/21

interface Ethernet4/22

interface Ethernet4/23

interface Ethernet4/24

interface Ethernet4/25

interface Ethernet4/26

```

```

interface Ethernet4/27

interface Ethernet4/28

interface Ethernet4/29

interface Ethernet4/30

interface Ethernet4/31

interface Ethernet4/32

interface mgmt0
    ip address 10.194.112.124/26

interface loopback0
    ip address 10.4.40.254/32
    ip router eigrp 100
    ip pim sparse-mode

interface loopback1
    ip address 10.4.40.252/32
    ip router eigrp 100
    ip pim sparse-mode
clock timezone PST -8 0
clock summer-time PDT 1 Sunday March 02:00 1 Sunday November
02:00 60
line console
    speed 38400
line vty
    access-class vty-acl-in in
boot kickstart bootflash:/n7000-s1-kickstart.5.2.4.bin sup-1
boot system bootflash:/n7000-s1-dk9.5.2.4.bin sup-1
boot kickstart bootflash:/n7000-s1-kickstart.5.2.4.bin sup-2
boot system bootflash:/n7000-s1-dk9.5.2.4.bin sup-2
router eigrp 100

```

```

router-id 10.4.40.254
ip pim send-rp-announce loopback1 group-list 239.1.0.0/16
ip pim send-rp-discovery loopback0 scope 32
ip pim ssm range 232.0.0.0/8
ip pim auto-rp listen
ip pim register-source loopback0
ip msdp originator-id loopback0
ip msdp peer 10.4.40.253 connect-source loopback0
logging timestamp milliseconds
logging console 5

```

Nexus 7000 Core Switch 2

```

version 5.2(4)
hostname N7010-2
vdc N7010-2 id 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource monitor-session minimum 0 maximum 2
  limit-resource monitor-session-erspan-dst minimum 0 maximum 23
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 96 maximum 96
  limit-resource u6route-mem minimum 24 maximum 24
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8

feature tacacs+
feature pim
feature msdp
feature eigrp
feature udld
feature lacp

username admin password 5 $1$T9PmvjPW$5cr3kG/b/ge5ZfZOPUztq0
role network-admin
ip domain-lookup
ip domain-name cisco.local
tacacs-server host 10.4.48.15 key 7 "VagwvtFjq"

```

```

aaa group server tacacs+ tacacs
  server 10.4.48.15
ip access-list snmp-acl
  10 permit udp 10.4.48.0/24 any eq snmp
ip access-list vty-acl-in
  10 permit tcp 10.4.48.0/24 any eq 22
copp profile strict
snmp-server user admin network-admin auth md5
0x9954a999e815a8422e2b5865a310105b
  priv 0x9954a999e815a8422e2b5865a310105b localizedkey
rmon event 1 log trap public description FATAL(1) owner PMON@
FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@
CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@
ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@
WARNING
rmon event 5 log trap public description INFORMATION(5) owner
PMON@INFO
snmp-server community cisco123 group network-admin
snmp-server community cisco group network-operator
snmp-server community cisco123 use-acl snmp-acl
snmp-server community cisco use-acl snmp-acl
ntp server 10.4.48.17
aaa authentication login default group tacacs

vrf context management
  ip route 0.0.0.0/0 10.194.112.65
vlan 1

interface port-channel35
  description 10GbEtherchannel link to D6500VSS
  ip address 10.4.40.21/30
  ip router eigrp 100
  ip pim sparse-mode

```

```
interface port-channel36
  description Connection to D3750X
  ip address 10.4.40.25/30
  ip router eigrp 100
  ip pim sparse-mode
```

```
interface Ethernet1/1
  channel-group 36 mode active
  no shutdown
```

```
interface Ethernet1/2
  channel-group 36 mode active
  no shutdown
```

```
interface Ethernet1/3
```

```
interface Ethernet1/4
```

```
interface Ethernet1/5
```

```
interface Ethernet1/6
```

```
interface Ethernet1/7
```

```
interface Ethernet1/8
```

```
interface Ethernet1/9
```

```
interface Ethernet1/10
```

```
interface Ethernet1/11
```

```
interface Ethernet1/12
```

```
interface Ethernet1/13
```

```
interface Ethernet1/14
```

```
interface Ethernet1/15
```

```
interface Ethernet1/16
```

```
interface Ethernet1/17
```

```
interface Ethernet1/18
```

```
interface Ethernet1/19
```

```
interface Ethernet1/20
```

```
interface Ethernet1/21
```

```
interface Ethernet1/22
```

```
interface Ethernet1/23
```

```
interface Ethernet1/24
```

```
interface Ethernet1/25
```

```
interface Ethernet1/26
```

```
interface Ethernet1/27
```

```
interface Ethernet1/28
```

```
interface Ethernet1/29
```

```
interface Ethernet1/30
```

```
interface Ethernet1/31
```

```
interface Ethernet1/32
```



```

interface Ethernet1/33
    channel-group 35 mode active
    no shutdown

interface Ethernet1/34

interface Ethernet1/35

interface Ethernet1/36

interface Ethernet1/37

interface Ethernet1/38

interface Ethernet1/39

interface Ethernet1/40

interface Ethernet1/41

interface Ethernet1/42

interface Ethernet1/43

interface Ethernet1/44

interface Ethernet1/45

interface Ethernet1/46

interface Ethernet1/47

interface Ethernet1/48

interface Ethernet4/1
    channel-group 35 mode active
    no shutdown

interface Ethernet4/2

interface Ethernet4/3
    description IE-D3750X Ten2/1/1
    ip address 10.4.40.69/30
    ip router eigrp 100
    ip pim sparse-mode
    no shutdown

interface Ethernet4/4

interface Ethernet4/5
    description D4507 Ten1/12
    ip address 10.4.40.29/30
    ip router eigrp 100
    ip pim sparse-mode
    no shutdown

interface Ethernet4/6
    description WAN-D3750X Tel1/1/1
    ip address 10.4.40.45/30
    ip router eigrp 100
    ip pim sparse-mode
    no shutdown

interface Ethernet4/7
    description Connection to DC5548UPa Eth1/20
    ip address 10.4.40.57/30
    ip router eigrp 100
    ip pim sparse-mode
    no shutdown

interface Ethernet4/8
    description Connection to DC5548UPb Eth1/20
    ip address 10.4.40.61/30
    ip router eigrp 100

```

```

ip pim sparse-mode
no shutdown

interface Ethernet4/9

interface Ethernet4/10

interface Ethernet4/11

interface Ethernet4/12

interface Ethernet4/13

interface Ethernet4/14

interface Ethernet4/15

interface Ethernet4/16

interface Ethernet4/17

interface Ethernet4/18

interface Ethernet4/19

interface Ethernet4/20

interface Ethernet4/21

interface Ethernet4/22

interface Ethernet4/23

interface Ethernet4/24

interface Ethernet4/25

```

```

interface Ethernet4/26

interface Ethernet4/27

interface Ethernet4/28

interface Ethernet4/29

interface Ethernet4/30

interface Ethernet4/31

interface Ethernet4/32

interface mgmt0
    ip address 10.194.112.125/26

interface loopback0
    ip address 10.4.40.253/32
    ip router eigrp 100
    ip pim sparse-mode

interface loopback1
    ip address 10.4.40.252/32
    ip router eigrp 100
    ip pim sparse-mode
clock timezone PST -8 0
clock summer-time PDT 1 Sunday March 02:00 1 Sunday November
02:00 60
line console
    speed 38400
line vty
    access-class vty-acl-in in
boot kickstart bootflash:/n7000-s1-kickstart.5.2.4.bin sup-1
boot system bootflash:/n7000-s1-dk9.5.2.4.bin sup-1
boot kickstart bootflash:/n7000-s1-kickstart.5.2.4.bin sup-2
boot system bootflash:/n7000-s1-dk9.5.2.4.bin sup-2

```

```
router eigrp 100
  router-id 10.4.40.253
ip pim send-rp-announce loopback1 group-list 239.1.0.0/16
ip pim send-rp-discovery loopback0 scope 32
ip pim ssm range 232.0.0.0/8
ip pim auto-rp listen
ip pim register-source loopback0
ip msdp originator-id loopback0
ip msdp peer 10.4.40.254 connect-source loopback0
logging timestamp milliseconds
```

Notes

Appendix B: Changes

This appendix summarizes the changes to this guide since the previous Cisco SBA series.

- To the Configure LAN Switch Universal Settings process, we integrated an optional step to control SSH and SNMP access to the switch.
- In the product list, we replaced all non-XL I/O modules to XL.

Notes

Feedback

Click [here](#) to provide feedback to Cisco SBA.



SMART BUSINESS ARCHITECTURE

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2012 Cisco Systems, Inc. All rights reserved.



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.

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