NX-OS and Cisco Nexus Switching
Next-Generation Data Center Architectures

The complete guide to planning, configuring, managing, and troubleshooting NX-OS in enterprise environments

Kevin Corbin, CCIE® No. 11577
Ron Fuller, CCIE No. 5851
David Jansen, CCIE No. 5952
Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Corporate and Government Sales

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, and branding interests. For more information, please contact: U.S. Corporate and Government Sales 1-800-382-3419 corpsales@pearsontechgroup.com

For sales outside the United States please contact: International Sales international@pearsoned.com

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers’ feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher Paul Boger
Associate Publisher Dave Dusthimer
Executive Editor Brett Bartow
Managing Editor Sandra Schroeder
Project Editor Seth Kerney
Editorial Assistant Vanessa Evans
Interior and Cover Designer Louisa Adair
Composition Mark Shirar

Manager, Global Certification Erik Ullanderson
Business Operation Manager, Cisco Press Anand Sundaram
Senior Development Editor Christopher Cleveland
Copy Editor Apostrophe Editing Services
Technical Editors Phil Davis, Eric Murray
Indexer WordWise Publishing Services
Proofreader Water Crest Publishing
Dedications

Kevin Corbin: I would like to dedicate this book to my parents. You have loved and supported me through all my endeavors. Mom, you instilled in me a work ethic that has been at the root of everything I have done. Dad, you taught me perseverance, and that the only time something is impossible is when you think it is. Nothing that I will ever accomplish would have been possible without both of you, I love you.

Ron Fuller: This book is dedicated to my loving wife Julie and my awesome children: Max, Sydney, Veronica, and Lil Bubba. Thank you for showing me the world through your perspective and helping me appreciate the things I would have otherwise taken for granted. I can't thank you enough for believing in me when I told you I was going to write another book. Your support and encouragement has and always will be the key to any success I enjoy. Thank you for your love and support.

David Jansen: This book is dedicated to my loving wife Jenise and my three children: Kaitlyn, Joshua, and Jacob. You are the inspiration that gave me the dedication and determination to complete this project. Kaitlyn, Joshua, Jacob, you are three amazing kids, you are learning the skills to be the best at what you do and accomplish anything; keep up the great work. Thank you for all your love and support; I could not have completed this without your help, support, and understanding. I'm so grateful to God, who gives endurance, encouragement, and motivation to complete such a large project like this.
About the Authors

Kevin Corbin, CCIE No. 11577, is a technology solutions architect with Cisco. In this role for three years, Kevin works with Enterprise customers to help them develop their next-generation data center architectures. Kevin has more than 14 years of server and networking experience including routing, switching, security, and content networking. Kevin has also held multiple certifications from Microsoft, Citrix, HP, Novell, and VMWare. Prior to joining Cisco, Kevin worked for many large enterprises and most recently in a consulting capacity for large enterprise customers.

Ron Fuller, CCIE No. 5851 (Routing and Switching/Storage Networking), is a technical solutions architect for Cisco specializing in data center architectures. He has 19 years of experience in the industry and has held certifications from Novell, HP, Microsoft, ISC2, SNIA, and Cisco. His focus is working with Enterprise customers to address their challenges with comprehensive end-to-end data center architectures. He lives in Ohio with his wife and three wonderful children and enjoys travel and auto racing.

David Jansen, CCIE No. 5952, is a technical solutions architect for Data Center for Central Area. David has more than 20 years experience in the information technology industry. He has held multiple certifications from Microsoft, Novell, Checkpoint, and Cisco. His focus is to work with Enterprise customers to address end-to-end data center Enterprise architectures. David has been with Cisco for 12 years and working as a Technical Solutions Architect for 4 years and has provided unique experiences helping customers build architectures for Enterprise data centers. David has also been instrumental in developing data center interconnect solutions to address L2 requirements between multiple data centers to meet application clusters and virtualization requirements. David has been presenting data center interconnect at Cisco Live for 3 years. David holds a B.S.E. degree in computer science from the University of Michigan (Go Blue!) and an M.A. degree in adult education from Central Michigan University.

About the Technical Reviewers

Phil Davis, CCIE No. 2021, is a technical solutions architect with Cisco, specializing in routing and switching and data center technologies. Phil has been with Cisco for more than 10 years and has more than 17 years of experience in the industry. Phil currently uses his expertise with Enterprise customers designing their data center and multiprotocol network architectures. Phil holds multiple certifications, including VMware’s VCP, and is often presenting on many of today’s top technologies. Phil lives near Cincinnati, Ohio, with his wife and two children.

Eric Murray is a network engineer for a large healthcare company. He has more than 15 years experience with designing, implementing, and maintaining Cisco Enterprise networks in the fast-paced healthcare and manufacturing industries. Eric has implemented several Nexus data center network designs and migrations and is a subject matter expert in utilizing Nexus 7000, 5000, and 2000 series switches. Eric is currently involved with designing, testing, implementing, and providing technical support for a Cisco Unified Communications solution. Eric also has extensive experience in multiprotocol WAN and data center LAN environments utilizing Cisco switching and routing platforms.
Acknowledgments

Kevin Corbin: I would like to first thank my co-authors Ron Fuller and David Jansen. I truly enjoy working with you on a day-to-day basis, and I am truly honored to have the opportunity to collaborate with you, and to even be considered in the same league as you guys. You are both rock stars. I would also like to recognize Steve McQuerry for his role in getting me involved in this project and providing coaching throughout this process.

I would like to thank the Cisco Press team, specifically Brett Bartow and Chris Cleveland. Thank you for being patient with me as I got ramped up for the project and keeping me motivated to make this project a reality. To Phil Davis and Eric Murray, thank you for keeping us honest throughout your review process.

The development of this content would not have been possible without a significant amount of access to equipment, and I’d like to thank Hongjun Ma and Jon Blunt for their commitment to ensure that gear was available and accessible to me.

Working at Cisco has opened up a world of opportunity for me and challenged me on almost a daily basis to accomplish things that I never could have imagined that I was capable of. For this I would be remiss if I didn't give my most sincere thanks to Joel Ekis for opening the door; Gary McNiel for taking a chance on me; and Scott Sprinkle and Jason Heiling for their support throughout my time at Cisco.

Ron Fuller: First I’d like to thank my co-authors Dave Jansen and Kevin Corbin. Dave, thank you for being such a good friend, a trusted co-worker, and a leader in our organization. You set the bar the rest of us try to reach. It has been great sharing a brain with you, and I look forward to more challenges and fun. Keep the goat rodeos coming! Kevin, thank you for stepping in to help complete this project. You are awesome to work with and your technical acumen is top-notch. People like you and Dave are the reason I love my job.

I’d like to thank Brett Bartow for his (almost) infinite patience with this project. It is a huge undertaking and his persistence and understanding and encouragement were greatly appreciated.

Chris Cleveland, it has been a pleasure working with you. Your guidance on the formatting and consistency makes the book something we all can be proud of. Thank you for making three propeller heads from Cisco look good.

To our technical editors, Phil Davis and Eric Murray—wow, you guys are picky! Thank you for the detail-oriented work and assistance making the book accurate and concise.

To Jeff Raymond, Marty Ma, and Charlie Lewis—thank you for allowing us access to the hardware. This book wouldn't have been possible without your help.

I’d like to thank my manager, Bill Taylor, for his support throughout this project and understanding. You are a great manager and I truly enjoy working for you. Thanks for the opportunity and the support you’ve provided over the last five years. (Time flies when you are having fun!)

To my family, thank you for the many times you wanted me to do something and hearing about a book on things you don't get to see. Your understanding and support through the weekends and late nights are truly appreciated.
For the extended teams at Cisco—thank you for responding to my many emails and calls no matter how inane you thought they were. There was a method to the madness—I think. Working with a world-class organization like this makes coming to work a pleasure.

Finally, I want to thank God for the gifts he has given me and the opportunity to do what I love to do with people I enjoy to support my family. I couldn’t ask for more.

David Jansen: This is my second book, and it has been a tremendous honor to work with the great people at Cisco Press. There are so many people to thank, I’m not sure where to begin. I’ll start with Brett Bartow: Thank you for getting me started in the writing industry; this is something I enjoy doing. I appreciate your patience and tolerance on this project. I really appreciate you keeping me on track to complete the project in a timely manner, as we have missed several completion dates.

First, I would like to thank my friend and co-authors Ron Fuller and Kevin Corbin. I can’t think of two better people to work with to complete such a project. Cisco is one of the most amazing places I’ve ever worked, and it’s people like you, who are wicked smart and a lot of fun to work with, that make it such a great place. I look forward to working on other projects in the future. I am truly blessed by having both of you as a co-worker and friend. I look forward to continue to work with you and grow the friendship into the future.

Chris Cleveland, again it was a pleasure to work with you. Your expertise, professionalism, and follow-up as a development editor is unsurpassed; thank you for your hard work and quick turn-around; this helped to meet the deadlines set forth.

To our technical editors—Phil Davis and Eric Murray—thank you for the time, sharp eyes, and excellent comments/feedback. It was a pleasure having you as part of the team.

Thank you to Jeff Raymond, Marty Ma, Lincoln Dale, and Ben Basler from Data Center Business Unit (DCBU) to provide access to hardware to complete this book. Also, thank you Charlie Lewis in RTP CPOC for scheduling hardware to complete this book as well.

Thanks to my manager at Cisco, Bill Taylor—I appreciate your guidance and your trust in my ability to juggle the many work tasks along with extra projects like working on a book.

I would like to thank the heavy metal music world out there—it allowed me to stay focused when burning the midnight oil; I would not have been able to complete this without loud rock ‘n roll music. Thank you.

I want to thank my family for their support and understanding while I was working on this project late at night and being patient with me when my lack of rest may have made me a little less than pleasant to be around.

Most important, I would like to thank God for giving me the ability to complete such a task with dedication and determination and for providing me the skills, knowledge, and health needed to be successful in such a demanding profession.
Contents

Foreword xiv
Introduction xv

Chapter 1  Introduction to Cisco NX-OS  1
NX-OS Overview  1
  NX-OS Supported Platforms  3
  Cisco NX-OS and Cisco IOS Comparison  3
NX-OS User Modes  5
  EXEC Command Mode  6
  Global Configuration Command Mode  6
  Interface Configuration Command Mode  7
Management Interfaces  8
  Controller Processor (Supervisor Module)  8
  Connectivity Management Processor (CMP)  9
  Telnet  11
  SSH  12
  XML  14
  SNMP  14
  DCNM  19
Managing System Files  20
  File Systems  21
    Configuration Files: Configuration Rollback  25
  Operating System Files  27
Virtual Device Contexts (VDCs)  28
  VDC Configuration  29
Troubleshooting  33
  show Commands  33
  debug Commands  34
Topology  34
Further Reading  35

Chapter 2  Layer 2 Support and Configurations  37
Layer 2 Overview  37
  Store-and-Forward Switching  38
  Cut-Through Switching  38
  Fabric Extension via the Nexus 2000  38
  Configuring Nexus 2000 Using Static Pinning  39
  Nexus 2000 Static Pinning Verification  41
  Configuring Nexus 2000 Using Port-Channels  45
Chapter 4  **IP Multicast Configuration**  171

Multicast Operation  171
- Multicast Distribution Trees  172
- Reverse Path Forwarding  174
- Protocol Independent Multicast (PIM)  174
- RPs  176

PIM Configuration on Nexus 7000  177
- Configuring Static RPs  180
- Configuring BSRs  182
- Configuring Auto-RP  184
- Configuring Anycast-RP  186
- Configuring SSM and Static RPF  188

IGMP Operation  189
- IGMP Configuration on Nexus 7000  190
- IGMP Configuration on Nexus 5000  194
- IGMP Configuration on Nexus 1000V  195
- MSDP Configuration on Nexus 7000  197

Summary  199

Chapter 5  **Security**  201

Configuring RADIUS  202
- RADIUS Configuration Distribution  205

Configuring TACACS+  211
- Enabling TACACS+  212

Configuring SSH  221

Configuring Cisco TrustSec  224
- Layer 2 Solutions Between Data Centers  231

Configuring IP ACLs  232

Configuring MAC ACLs  234
Configuring VLAN ACLs 236
Configuring Port Security 237
    Security Violations and Actions 240
Configuring DHCP Snooping 242
Configuring Dynamic ARP Inspection 246
    Dynamic ARP Inspection Trust State 247
Configuring IP Source Guard 250
Configuring Keychain Management 252
Configuring Traffic Storm Control 253
Configuring Unicast RPF 255
Configuring Control Plane Policing 257
Configuring Rate Limits 266
SNMPv3 271
Summary 278

Chapter 6  High Availability 279
Physical Redundancy 279
    Redundant Power Supplies 280
    Redundant Cooling System 282
    Redundant Supervisors 285
    Redundant Ethernet Out-of-Band (EOBC) 286
    Redundant Fabric Modules 286
Generic Online Diagnostics 287
    Bootup Diagnostics 288
    Runtime Diagnostics 289
    On-Demand Diagnostics 294
NX-OS High-Availability Architecture 295
Process Modularity 295
Process Restart 297
Stateful Switchover 297
Nonstop Forwarding 299
In-Service Software Upgrades 299
Summary 309

Chapter 7  Embedded Serviceability Features 311
SPAN 311
    SPAN on Nexus 7000 312
    Configuring SPAN on Nexus 7000 313
    SPAN on Nexus 5000 318
    Configuring SPAN on Nexus 5000 319
Icons Used in This Book

- **Nexus 7000**
- **Nexus 5000**
- **Nexus 2000 Fabric Extender**
- **Nexus 1000 Series**
- **ASR 1000 Series**
- **Router**
- **Network Management Appliance**
- **Web Server**
- **Laptop**
- **Server**
- **PC**
- **Network Cloud**
- **Ethernet Connection**
- **Serial Line Connection**

Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a `show` command).

- **Italic** indicates arguments for which you supply actual values.

- Vertical bars (|) separate alternative, mutually exclusive elements.

- Square brackets ([ ] ) indicate an optional element.

- Braces ( { } ) indicate a required choice.

- Braces within brackets ( { [ ] } ) indicate a required choice within an optional element.
Foreword

More than five years ago, Cisco had the vision of unifying the fabrics in the data center to enable consolidation, virtualization, and automation. Cisco gathered input from customers and partners, and feedback from TAC and the sales team, to begin the design of the Nexus series of switches. With the launch of the Nexus 7000 in 2008, the years of planning, discussion, and hard work paid off as this new platform was released to our customers. The Nexus 5000, Nexus 2000, and Nexus 1000V quickly followed, providing a comprehensive end-to-end data center architecture designed to solve the emerging challenges faced in the ever-changing space that is the data center.

Supporting key innovations that make the 24×7×365 highly available data center a reality, while aligning with the increased demands of virtualization, the Nexus portfolio is truly game-changing. These innovations span the breadth of the product line and encompass both hardware and software changes. A subset includes capabilities such as In-Service Software Upgrade (ISSU), virtual device contexts (vDC), virtual Port Channels (vPC), VN-Link, and Unified Fabric for Fibre Channel over Ethernet (FCoE). This breadth of new capabilities brings increased efficiencies to how data center networks are designed, engineered, and operated.

To that end, a book like the one you are reading will hopefully become a convenient reference for best practices deployment of these new technologies. It is written by three of our Enterprise data center technology solutions architects, who work with our customers on a daily basis and help them develop next-generation data center architectures. Their breadth of experience makes them perfect candidates to drive a project such as this.

We hope that as you read this book and learn more about the Nexus series of switches, and NX-OS specifically, you’ll see the years of effort that made this product the Cisco flagship data center operating system now and in the years to come. Enjoy!

Umesh Mahajan, VP/GM
Ram Velaga, VP Product Management
Data Center Switching Technology Group
Cisco, San Jose
Introduction

The modern data center is rapidly changing and evolving to support the current and future demands of technology. At the center of this change is the network—the single entity that connects everything and touches all components of the data center. With that in mind, Cisco has launched a new series of switches, Nexus, based on a revolutionary new operating system, NX-OS, to meet these changes and provide a platform with the scalability, reliability, and comprehensive feature set required in the next generation data center.

The purpose of this book is to provide a guide for the network administrator who might not be familiar with Nexus and NX-OS. It is intended to be used as a “go-to” resource for concise information on the most commonly used aspects of NX-OS across the Nexus 7000, 5000, and 1000V platforms.

Goals and Methods

The goal of this book is to provide best practice configurations to common internetworking scenarios involving Nexus products. Having been network administrators ourselves, we are conscious of the pressures and challenges with finding accurate and relevant information, especially on new technology. We intend this book to be a resource the network administrator reaches for first.

Although there might be more than one way to accomplish a networking requirement, we focused on the best way that minimizes operational complexity and maximizes supportability. We realize and respect that there might be corner-case scenarios that call for configurations not described in this book but sincerely hope we address the vast majority of common configurations.

Who Should Read This Book?

This book is targeted for the network administrator, consultant, or student looking for assistance with NX-OS configuration. It covers the three major Cisco Nexus products and highlights key features of them in a way that makes it easy for the reader to digest and implement.

How This Book Is Organized

This book has been organized following the OSI system model for the initial chapters starting with Layer 2 and then moving to Layer 3. We then add in network-based services such as IP multicast, security, and high availability. Next the embedded serviceability features of NX-OS are explored before moving to emerging data center architecture, Unified Fabrics. Last, and certainly not least, we focus on Nexus 1000V and its capability to provide insight, consistent network policy, and simplified administration to virtualized environments.
Chapters 1 through 9 cover the following topics:

- **Chapter 1, “Introduction to Cisco NX-OS”**: Provides the reader with the foundation for building NX-OS configurations including command-line interface (CLI) differences, virtualization capabilities, and basic file system management.

- **Chapter 2, “Layer 2 Support and Configurations”**: Focuses on the comprehensive suite of Layer 2 technologies supported by NX-OS including vPC and Spanning Tree Protocol.

- **Chapter 3, “Layer 3 Support and Configurations”**: Delves into the three most common network Layer 3 protocols including EIGRP, OSPF, and BGP. Additionally HSRP, GLBP, and VRRP are discussed.

- **Chapter 4, “IP Multicast Configuration”**: Provides the reader the information needed to configure IP Multicast protocols such as PIM, Auto-RP, and MSDP.

- **Chapter 5, “Security”**: Focuses on the rich set of security protocols available in NX-OS including CTS, ACLs, CoPP, DAI, and more.

- **Chapter 6, “High Availability”**: Delves into the high-availability features built into NX-OS including ISSU, stateful process restart, stateful switchover, and non-stop forwarding.

- **Chapter 7, “Embedded Serviceability Features”**: Provides the reader with the ability to leverage the embedded serviceability components in NX-OS including SPAN, configuration checkpoints and rollback, packet analysis, and Smart Call Home.

- **Chapter 8, “Unified Fabric”**: Explores the industry leading capability for Nexus switches to unify storage and Ethernet fabrics with a focus on FCoE, NPV, and NPIV.

- **Chapter 9, “Nexus 1000V”**: Enables the reader to implement Nexus 1000V in a virtualized environment to maximum effect leveraging the VSM, VEM, and port profiles.
This chapter provides an introduction and overview of NX-OS and a comparison between traditional IOS and NX-OS configurations and terminology. The following sections will be covered in this chapter:

- NX-OS Overview
- NX-OS User Modes
- Management Interfaces
- Managing System Files

**NX-OS Overview**

Cisco built the next-generation data center-class operating system designed for maximum scalability and application availability. The NX-OS data center-class operating system was built with modularity, resiliency, and serviceability at its foundation. NX-OS is based on the industry-proven Cisco Storage Area Network Operating System (SAN-OS) Software and helps ensure continuous availability to set the standard for mission-critical data center environments. The self-healing and highly modular design of Cisco NX-OS enables for operational excellence increasing the service levels and enabling exceptional operational flexibility. Several advantages of Cisco NX-OS include the following:

- Unified data center operating system
- Robust and rich feature set with a variety of Cisco innovations
- Flexibility and scalability
- Modularity
- Virtualization
- Resiliency
IPv4 and IPv6 IP routing and multicast features

Comprehensive security, availability, serviceability, and management features

Key features and benefits of NX-OS include

- **Virtual device contexts (VDC):** Cisco Nexus 7000 Series switches can be segmented into virtual devices based on customer requirements. VDCs offer several benefits such as fault isolation, administration plane, separation of data traffic, and enhanced security.

- **Virtual Port Channels (vPC):** Enables a server or switch to use an EtherChannel across two upstream switches without an STP-blocked port to enable use of all available uplink bandwidth.

- **Continuous system operation:** Maintenance, upgrades, and software certification can be performed without service interruptions due to the modular nature of NX-OS and features such as In-Service Software Upgrade (ISSU) and the capability for processes to restart dynamically.

- **Security:** Cisco NX-OS provides outstanding data confidentiality and integrity, supporting standard IEEE 802.1AE link-layer cryptography with 128-bit Advanced Encryption Standard (AES) cryptography. In addition to CTS, there are many additional security features such as access control lists (ACL) and port-security, for example.

- **Base services:** The default license that ships with NX-OS covers Layer 2 protocols including such features such as Spanning Tree, virtual LANs (VLAN), Private VLANs, and Unidirectional Link Detection (UDLD).

- **Enterprise Services Package:** Provides Layer 3 protocols such as Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (ISIS), Enhanced Interior Gateway Routing Protocol (EIGRP), Policy-Based Routing (PBR), Protocol Independent Multicast (PIM), and Generic Routing Encapsulation (GRE).

- **Advanced Services Package:** Provides Virtual Device Contexts (VDC), Cisco Trustsec (CTS), and Overlay Transport Virtualization (OTV).

- **Transport Services License:** Provides Overlay Transport Virtualization (OTV) and Multiprotocol Label Switching (MPLS) (when available).

Example 1-1 shows the simplicity of installing the NX-OS license file.

**Example 1-1  Displaying and Installing the NX-OS License File**

| Once a license file is obtained from Cisco.com and copied to flash, it can be installed for the chassis. |
| Displaying the host-id for License File Creation on Cisco.com: |
NX-OS offers feature testing for a 120-day grace period. Here is how to enable a 120-day grace period:

congo(config)# license grace-period

The feature is disabled after the 120-day grace period begins. The license grace period is enabled only for the default admin VDC, VDC1.

Using the grace period enables customers to test, configure, and fully operate a feature without the need for a license to be purchased. This is particularly helpful for testing a feature prior to purchasing a license.

NX-OS Supported Platforms

NX-OS data center-class operating system, designed for maximum scalability and application availability, has a wide variety of platform support, including the following:

- Nexus 7000
- Nexus 5000
- Nexus 2000
- Nexus 1000V
- Cisco MDS 9000
- Cisco Unified Computing System (UCS)
- Nexus 4000

Cisco NX-OS and Cisco IOS Comparison

If you are familiar with traditional Cisco IOS command-line interface (CLI), the CLI for NX-OS is similar to Cisco IOS. There are key differences that should be understood prior to working with NX-OS, however:

- When you first log into NX-OS, you go directly into EXEC mode.
- NX-OS has a setup utility that enables a user to specify the system defaults, perform basic configuration, and apply a predefined Control Plane Policing (CoPP) security policy.
- NX-OS uses a feature-based license model. An Enterprise or Advanced Services license is required depending on the features required.

- A 120-day license grace period is supported for testing, but features are automatically removed from the configuration after the expiration date is reached.

- NX-OS has the capability to enable and disable features such as OSPF, BGP, and so on via the `feature` configuration command. Configuration and verification commands are not available until you enable the specific feature.

- Interfaces are labeled in the configuration as Ethernet. There aren’t any speed designations in the interface name. Interface speed is dynamically learned and reflected in the appropriate `show` commands and interface metrics.

- NX-OS supports Virtual Device Contexts (VDC), which enable a physical device to be partitioned into logical devices. When you log in for the first time, you are in the default VDC.

- The Cisco NX-OS has two preconfigured instances of VPN Routing Forwarding (VRF) by default (management, default). By default, all Layer 3 interfaces and routing protocols exist in the default VRF. The mgmt0 interface exists in the management VRF and is accessible from any VDC. If VDCs are configured, each VDC has a unique IP address for the mgmt0 interface.

- Secure Shell version 2 (SSHv2) is enabled by default. (Telnet is disabled by default.)

- Default login administrator user is predefined as admin; a password has to be specified when the system is first powered up. With NX-OS, you must enter a username and password; you cannot disable the username and password login. In contrast, in IOS you can simply type a password; you can optionally set the login to require the use of a username.

- NX-OS uses a kickstart image and a system image. Both images are identified in the configuration file as the kickstart and system boot variables; this is the same as the Cisco Multilayer Director Switch (MDS) Fibre Channel switches running SAN-OS.

- NX-OS removed the `write memory` command; use the `copy running-config startup-config`; there is also the alias command syntax.

- The default Spanning Tree mode in NX-OS is Rapid-PVST+.

**Caution**  In NX-OS, you have to enable features such as OSPF, BGP, and CTS; if you remove a feature via the `no` feature command, all relevant commands related to that feature are removed from the running configuration.

For example, when configuring vty timeouts and session limits, consider Example 1-2, which illustrates the difference between IOS and NX-OS syntax.
Example 1-2  *vty Configurations and Session Limits, Comparing the Differences Between Traditional IOS and NX-OS*

<table>
<thead>
<tr>
<th>IOS:</th>
<th>NX-OS:</th>
</tr>
</thead>
<tbody>
<tr>
<td>congo#</td>
<td>congo(config)#</td>
</tr>
<tr>
<td>congo(config)# line vty 0 9</td>
<td>congo(config)# line vty</td>
</tr>
<tr>
<td>congo(config)# exec-timeout 15 0</td>
<td>congo(config)# session-limit 10</td>
</tr>
<tr>
<td>congo(config)# login</td>
<td>congo(config)# exec-timeout 15</td>
</tr>
<tr>
<td>congo# copy running-config startup-config</td>
<td>congo# copy running-config startup-config</td>
</tr>
</tbody>
</table>

NX-OS User Modes

Cisco NX-OS CLI is divided into command modes, which define the actions available to the user. Command modes are “nested” and must be accessed in sequence. As you navigate from one command mode to another, an increasingly larger set of commands become available. All commands in a higher command mode are accessible from lower command modes. For example, the `show` commands are available from any configuration command mode. Figure 1-1 shows how command access builds from EXEC mode to global configuration mode.

Figure 1-1  *NX-OS Command Access from EXEC Mode to Global Configuration Mode*
EXEC Command Mode

When you first log in, Cisco NX-OS Software places you in EXEC mode. As demonstrated in Example 1-3, the commands available in EXEC mode include the `show` commands that display device status and configuration information, the `clear` commands, and other commands that perform actions that you do not save in the device configuration.

Example 1-3  Cisco NX-OS EXEC Mode

```
Congo# show interface ethernet 1/15
Ethernet1/15 is down (SFP not inserted)
   Hardware: 10000 Ethernet, address: 001b.54c2.bbc1 (bia 001b.54c1.e4da)
   MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec,
       reliability 255/255, txload 1/255, rxload 1/255
   Encapsulation ARPA
   auto-duplex, auto-speed
   Beacon is turned off
   Auto-Negotiation is turned off
   Input flow-control is off, output flow-control is off
   Switchport monitor is off
   Last link flapped never
   Last clearing of 'show interface' counters never
   30 seconds input rate 0 bits/sec, 0 packets/sec
   30 seconds output rate 0 bits/sec, 0 packets/sec
   Load-Interval #2: 5 minute (300 seconds)
       input rate 0 bps, 0 pps; output rate 0 bps, 0 pps
   L3 in Switched:
       ucast: 0 pkts, 0 bytes - mcast: 0 pkts, 0 bytes
   L3 out Switched:
       ucast: 0 pkts, 0 bytes - mcast: 0 pkts, 0 bytes
! Output omitted for brevity

Congo#
```

Global Configuration Command Mode

Global configuration mode provides access to the broadest range of commands. The term *global* indicates characteristics or features that affect the device as a whole. You can enter commands in global configuration mode to configure your device globally or enter more specific configuration modes to configure specific elements such as interfaces or protocols as demonstrated here:

```
Nx7000# config
Nx7000(config)# interface ethernet 1/15
```
Chapter 1: Introduction to Cisco NX-OS

Interface Configuration Command Mode

One example of a specific configuration mode that you enter from global configuration mode is interface configuration mode. To configure interfaces on your device, you must specify the interface and enter interface configuration mode.

You must enable many features on a per-interface basis. Interface configuration commands modify the operation of the interfaces on the device, such as Ethernet interfaces or management interfaces (mgmt 0).

Example 1-4 demonstrates moving between the different command modes in NX-OS.

Example 1-4  Interface Ethernet1/5 Is a 10Gigabit Ethernet Interface—Show How the Interface Is Designated at Ethernet and Not Interface Ten1/15.

```
congo# conf t
congo(config)# interface ethernet 1/15
congo(config-if)# exit
Congo# show interface ethernet 1/15
Ethernet1/15 is down (SFP not inserted)
   Hardware: 10000 Ethernet, address: 001b.54c2.bbc1 (bia 001b.54c1.e4da)
   MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec,
       reliability 255/255, txload 1/255, rxload 1/255
   Encapsulation ARPA
   auto-duplex, auto-speed
   Beacon is turned off
   Auto-Negotiation is turned off
   Input flow-control is off, output flow-control is off
   Switchport monitor is off
   Last link flapped never
   Last clearing of "show interface" counters never
   30 seconds input rate 0 bits/sec, 0 packets/sec
   30 seconds output rate 0 bits/sec, 0 packets/sec
   Load-Interval #2: 5 minute (300 seconds)
       input rate 0 bps, 0 pps; output rate 0 bps, 0 pps
   L3 in Switched:
       ucast: 0 pkts, 0 bytes · mcast: 0 pkts, 0 bytes
   L3 out Switched:
       ucast: 0 pkts, 0 bytes · mcast: 0 pkts, 0 bytes

Congo#
```

NX-OS supports different Ethernet interface types such as Gigabit Ethernet and 10-Gigabit Ethernet interfaces. All interfaces are referred to Ethernet; NX-OS does not designate Gigabit or 10-Gigabit Ethernet interfaces. In Example 1-4, interface 1/15 is a 10-Gigabit Ethernet interface.
Management Interfaces

NX-OS has many different type of management interfaces, all of which the following section covers:

- **Controller Processor (CP)/Supervisor**: Has both the management plane and control plane and is critical to the operation of the network.

- **Connectivity Management Processor (CMP)**: Provides a second network interface to the device for use even when the CP is not reachable. The CMP interface is used for out-of-band management and monitoring; the CMP interface is independent from the primary operating system.

- **MGMT0**: Provides true out-of-band management through a dedicated interface and VRF to ensure 100 percent isolation from either control plane or data plane. MGMT0 enables you to manage the devices by the IPv4 or IPv6 address on the MGMT0 interface; the mgmt0 interface is a 10/100/1000 Ethernet interface. When implementing Virtual port-channel (vPC), a best practice is to use the MGMT0 interface for the VPC keepalive link.

- **Telnet**: Provides an unsecure management connection to the NX-OS device.

- **SSH**: Provides a secure management connection to the NX-OS device.

- **Extended Markup Language (XML) management interfaces**: Use the XML-based Network Configuration Protocol (NETCONF) that enables management, monitoring, and communication over the interface with an XML management tool or program.

- **Simple Network Management Protocol (SNMP)**: Used by management systems to monitor and configure devices via a set of standards for communication over the TCP/IP protocol.

Controller Processor (Supervisor Module)

The Cisco Nexus 7000 series supervisor module is designed to deliver scalable control plane and management functions for the Cisco Nexus 7000 Series chassis. The Nexus 7000 supervisor module is based on an Intel dual-core processor that enables a scalable control plane. The supervisor modules controls the Layer 2 and Layer 3 services, redundancy capabilities, configuration management, status monitoring, power, and environmental management. The supervisor module also provides centralized arbitration to the system fabric for all line cards. The fully distributed forwarding architecture enables the supervisor to support transparent upgrades to higher forwarding capacity-capable I/O and fabric modules. Two supervisors are required for a fully redundant system, with one supervisor module running as the active device and the other in hot standby mode, providing exceptional high-availability features in data center-class products. Additional features and benefits of the Nexus 7000 supervisor modules to meet demanding data center requirements follow:
- Active and standby supervisor.
- In-Service Software Upgrade (ISSU) with dual supervisor modules.
- Virtual output queuing (VoQ), which is a quality of service (QoS)-aware lossless fabric, avoids the problems associated with head-of-line blocking.
- USB interfaces that enable access to USB flash memory devices for software image loading and recovery.
- Central arbitration that provides symmetrical control of the flow of traffic through the switch fabric helps ensure transparent switchover with no losses.
- Segmented and redundant out-of-band provisioning and management paths.
- Virtualization of the management plane via Virtual Device Contexts (vDC).
- Integrated diagnostics and protocol decoding with an embedded control plane packet analyzer; this is based on the Wireshark open source. (No additional licenses are required.)
- Fully decoupled control plane and data plane with no hardware forwarding on the module.
- Distributed forwarding architecture, enabling independent upgrades of the supervisor and fabric.
- With Central arbitration and VoQ, this enables for Unified Fabric.
- Transparent upgrade capacity and capability; designed to support 40-Gigabit and 100-Gigabit Ethernet.
- System locator and beacon LEDs for simplified operations.
- Dedicated out-of-band management processor for “lights out” management.

**Connectivity Management Processor (CMP)**

The supervisor incorporates an innovative dedicated connectivity management processor (CMP) to support remote management and troubleshooting of the complete system. The CMP provides a complete out-of-band management and monitoring capability independent from the primary operating system. The CMP enables *lights out* management of the supervisor module, all modules, and the Cisco Nexus 7000 Series system without the need for separate terminal servers with the associated additional complexity and cost. The CMP delivers the remote control through its own dedicated processor, memory, and boot flash memory and a separate Ethernet management port. The CMP can reset all system components, including power supplies; it can also reset the host supervisor module to which it is attached, enabling a complete system restart.

The CMP offers many benefits, including the following:

- Dedicated processor and memory, and boot flash.
- The CMP interface can reset all the system components, which include power, supervisor module, and system restart.
An independent remote system management and monitoring capability enables lights out management of the system.

Remote monitoring of supervisor status and initiation of resets that removes the need for separate terminal server devices for out-of-band management.

System reset while retaining out-of-band Ethernet connectivity, which reduces the need for onsite support during system maintenance.

Capability to remotely view boot-time messages during the entire boot process.

Capability to initiate a complete system power shutdown and restart, which eliminates the need for local operator intervention to reset power for devices.

Login authentication, which provides secure access to the out-of-band management environment.

Access to supervisor logs that enables rapid detection and prevention of potential system problems.

Capability to take full console control of the supervisor.

Complete control is delivered to the operating environment.

Example 1-5 shows how to connect to the CMP interface and the available show commands available from the CMP interface. Also, note the escape sequence of “~,” to get back to the main NX-OS interface. You can also connect from the CMP back to the CP module.

**Example 1-5  Connecting to the CMP Interface, Displaying Available show Commands**

```
N7010-1# attach cmp
Connected
Escape character is ‘~’, [tilde comma]

N7010-1-cmp5 login: admin
Password:
Last login: Tue Aug 11 23:58:12 2009 on ttyS1

N7010-1-cmp5# attach cp
This command will disconnect the front-panel console on this supervisor, and will clear all console attach sessions on the CP - proceed(y/n)? y
N7010-1#

N7010-1# attach cmp
Connected
Escape character is ‘~’, [tilde comma]

N7010-1-cmp5 login: admin
Password:
Last login: Wed Aug 12 00:06:12 2009 on ttyS1
```
Telnet

NX-OS enables for Telnet server and client. The Telnet protocol enables TCP/IP terminal connections to a host. Telnet enables a user at one site to establish a TCP connection to a login server at another site and then passes the keystrokes from one device to the other. Telnet can accept either an IP address or a domain name as the remote device address.

Note Remember that the Telnet server is disabled by default in NX-OS.

The Telnet server is disabled by default on an NX-OS device. Example 1-6 demonstrates how to enable a Telnet server in NX-OS.

Example 1-6  Enabling a Telnet Server in NX-OS

```
N7010-1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
N7010-1(config)# feature telnet
N7010-1(config)# show telnet server
telnet service enabled
N7010-1(config)# copy running-config startup-config
[########################################] 100%
```
SSH

NX-OS supports SSH Server and SSH Client. Use SSH server to enable an SSH client to make a secure, encrypted connection to a Cisco NX-OS device; SSH uses strong encryption for authentication. The SSH server in Cisco NX-OS Software can interoperate with publicly and commercially available SSH clients. The user authentication mechanisms supported for SSH are Remote Authentication Dial-In User Service (RADIUS), Terminal Access Controller Access Control System Plus (TACACS+), and the use of locally stored usernames and passwords.

The SSH client application enables the SSH protocol to provide device authentication and encryption. The SSH client enables a Cisco NX-OS device to make a secure, encrypted connection to another Cisco NX-OS device or to any other device that runs the SSH server.

SSH requires server keys for secure communications to the Cisco NX-OS device. You can use SSH server keys for the following SSH options:

- SSH version 2 using Rivest, Shamir, and Adelman (RSA) public-key cryptography
- SSH version 2 using the Digital System Algorithm (DSA)

Be sure to have an SSH server key-pair with the appropriate version before allowing the SSH service. You can generate the SSH server key-pair according to the SSH client version used. The SSH service accepts two types of key-pairs for use by SSH version 2:

- The *dsa* option generates the DSA key-pair for the SSH version 2 protocol.
- The *rsa* option generates the RSA key-pair for the SSH version 2 protocol.

By default, Cisco NX-OS Software generates an RSA key using 1024 bits.

SSH supports the following public key formats:

- OpenSSH
- IETF Secure Shell (SECSH)

Example 1-7 demonstrates how to enable SSH server and configure the SSH server keys.

**Example 1-7  Enabling SSH Server and Configuring SSH Server Keys**

```bash
N7010-1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
N7010-1(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled
N7010-1(config)# ssh key rsa 2048
generating rsa key(2048 bits)....
```
generated rsa key
N7010-1(config)# feature ssh
N7010-1(config)# exit
N7010-1# show ssh key

ssh-rsa AAAAB3NzaC1yc2EAAAADAQADAQADAQABH/mq1gQbfhhsjBmm65ksgfQb3Mb3qbwUbNlc
AA6fjJCgdHuf3kJox/hjgPDChJQoSkUXHjES1V59OhZP/Nh1BRBq0TGRr+hfdAssD3wG5oPkywgM4+bR/
ssCzoj6jVG4ItGmF/Pip4pr3dqsMzR21DXSKK/tdj7bipWky1wSkYQzZwatIVPIXRqTJY7L9a+JqVIJEA
0Q1JM1lwZ5YbxcB2GKNCM2x2BZ14okVg180CCJg7vmn+8Rq10Q5jNAPeb9kFw9nsPj/r5xFc1RcS
KeQbdYaJItU6cX1Ts1RnKj1WewCglA26dEaGdawMVuftgu0uM97VC0xZPQ==

bitcount:2048
fingerprint:

N7010-1# show ssh server

ssh version 2 is enabled

N7010-1(config)# username nxos-admin password C1sc0123!

N7010-1(config)# username nxos-admin sshkey ssh-rsa

N7010-1(config)# show user-account

user:admin
this user account has no expiry date
roles:network-admin

user:nxos-admin
this user account has no expiry date
roles:network-operator
ssh public key: ssh-rsa
AAAAB3NzaC1yc2EAAAADAQADAQADAQABH/mq1gQbfhhsjBmm65ksgfQb3Mb3qbwUbNlc
AA6fjJCgdHuf3kJox/hjgPDChJQoSkUXHjES1V59OhZP/Nh1BRBq0TGRr+hfdAssD3wG5oPkywgM4+bR/
ssCzoj6jVG4ItGmF/Pip4pr3dqsMzR21DXSKK/tdj7b
ip.

XML

NX-OS has a robust XML management interface, which can be used to configure the entire switch. The interface uses the XML-based Network Configuration Protocol (NETCONF) that enables you to manage devices and communicate over the interface with an XML management tool or a program. NETCONF is based on RFC 4741 and the NX-OS implementation requires you to use a Secure Shell (SSH) session for communication with the device.

NETCONF is implemented with an XML Schema (XSD) that enables you to enclose device configuration elements within a remote procedure call (RPC) message. From within an RPC message, you select one of the NETCONF operations that matches the type of command that you want the device to execute. You can configure the entire set of CLI commands on the device with NETCONF.

The XML management interface does not require any additional licensing. XML management is included with no additional charge.

XML/NETCONF can be enabled via a web2.0/ajax browser application that uses XML/NETCONF to pull all statistics off all interfaces on the Nexus 7000 running NX-OS in a dynamically updating table.

Figures 1-2, 1-3, and 1-4 demonstrate sample output from the XML/NETCONF interface.

SNMP

The Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network.

SNMP has different versions such as SNMPv1, v2, and v3. Each SNMP version has different security models or levels. Most Enterprise customers are looking to implement SNMPv3 because it offers encryption to pass management information (or traffic) across the network. The security level determines if an SNMP message needs to be protected and authenticated. Various security levels exist within a security model:

- **noAuthNoPriv**: Security level that does not provide authentication or encryption.
- **authNoPriv**: Security level that provides authentication but does not provide encryption.
- **authPriv**: Security level that provides both authentication and encryption.

![Figure 1-2](image1.png)

**Figure 1-2** Obtaining NX-OS Real-Time Interface Statistics via NETCONF/XML. The IP Address Entered Is the NX-OS mgmt0 Interface.

![Figure 1-3](image2.png)

**Figure 1-3** Login Results to the NX-OS Devices via NETCONF/XML.
Cisco NX-OS supports the following SNMP standards:

- **SNMPv1**: Simple community-string based access.
- **SNMPv2c**: RFC 2575-based group access that can be tied into RBAC model.
- **SNMPv3**: Enables for two independent security mechanisms, authentication (Hashed Message Authentication leveraging either Secure Hash Algorithm [SHA-1] or Message Digest 5 [MD5] algorithms) and encryption (Data Encryption Standard [DES] as the default and Advanced Encryption Standard [AES]) to ensure secure communication between NMS station and N7K/NX-OS. Both mechanisms are implemented as demonstrated in Example 1-8.

As NX-OS is truly modular and highly available, the NX-OS implementation of SNMP supports stateless restarts for SNMP. NX-OS has also implemented virtualization support for SNMP; NX-OS supports one instance of SNMP per virtual device context (VDC). SNMP is also VRF-aware, which allows you to configure SNMP to use a particular VRF to reach the network management host.

Example 1-8 demonstrates how to enable SNMPv3 on NX-OS.

**Example 1-8  Enabling SNMPv3 on NX-OS**

```
N7010-1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
N7010-1(config)# snmp-server user NMS auth sha Cisc0123! priv Cisc0123! engineID
```
N7010-1(config)# snmp-server host 10.100.22.254 informs version 3 auth NMS
N7010-1(config)# snmp-server community public ro
N7010-1(config)# snmp-server community nxos rw
N7010-1(config)# show snmp
sys contact:
sys location:
0 SNMP packets input
   0 Bad SNMP versions
   0 Unknown community name
   0 Illegal operation for community name supplied
   0 Encoding errors
   0 Number of requested variables
   0 Number of altered variables
   0 Get-request PDUs
   0 Get-next PDUs
   0 Set-request PDUs
   0 No such name PDU
   0 Bad value PDU
   0 Read Only PDU
   0 General errors
   0 Get Responses
45 SNMP packets output
   45 Trap PDU
   0 Too big errors
   0 No such name errors
   0 Bad values errors
   0 General errors
   0 Get Requests
   0 Get Next Requests
   0 Set Requests
   0 Get Responses
   0 Silent drops

<table>
<thead>
<tr>
<th>Community</th>
<th>Group / Access</th>
<th>context</th>
<th>acl_filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>nxos</td>
<td>network-admin</td>
<td>-------</td>
<td>----------</td>
</tr>
<tr>
<td>public</td>
<td>network-operator</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SNMP USERS

<table>
<thead>
<tr>
<th>User</th>
<th>Auth</th>
<th>Priv(enforce)</th>
<th>Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td></td>
<td>md5</td>
<td>network-admin</td>
</tr>
<tr>
<td>User</td>
<td>Auth</td>
<td>Priv</td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>------</td>
<td>------</td>
<td></td>
</tr>
<tr>
<td>NMS</td>
<td>sha</td>
<td>des</td>
<td></td>
</tr>
<tr>
<td>(EngineID 0:0:0:63:0:1:0:10:20:15:10:3)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SNMP Tcp Authentication Flag : Enabled.

Port Monitor : enabled

Policy Name : default

Admin status : Not Active

Oper status : Not Active

Port type : All Ports

---

<table>
<thead>
<tr>
<th>Counter event</th>
<th>Threshold</th>
<th>Interval</th>
<th>Rising Threshold event</th>
<th>Falling Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link Loss Yes</td>
<td>Delta</td>
<td>60</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>Sync Loss Yes</td>
<td>Delta</td>
<td>60</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>Protocol Error Yes</td>
<td>Delta</td>
<td>60</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Signal Loss Yes</td>
<td>Delta</td>
<td>60</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>Invalid Words Yes</td>
<td>Delta</td>
<td>60</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Invalid CRC's Yes</td>
<td>Delta</td>
<td>60</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>RX Performance Yes</td>
<td>Delta</td>
<td>60</td>
<td>2147483648</td>
<td>4</td>
</tr>
<tr>
<td>TX Performance Yes</td>
<td>Delta</td>
<td>60</td>
<td>2147483648</td>
<td>4</td>
</tr>
</tbody>
</table>

SNMP protocol : Enabled

Context [Protocol instance, VRF, Topology]

N7010-1# show snmp user
DCNM

Cisco Data Center Network Manager (DCNM) is a management solution that supports NX-OS devices. DCNM maximizes the overall data center infrastructure uptime and reliability, which improves service levels. Focused on the operational management requirements of the data center, DCNM provides a robust framework and rich feature set that fulfills the switching, application, automation, provisioning, and services needs of today's data centers and tomorrow's data center requirements.

DCNM is a client-server application supporting a Java-based client-server application. The DCNM client communicates with the DCNM server only, never directly with managed Cisco NX-OS devices. The DCNM server uses the XML management interface of Cisco NX-OS devices to manage and monitor them. The XML management interface is a programmatic method based on the NETCONF protocol that complements the CLI functionality.

DCNM has a robust configuration and feature support on the NX-OS platform. The following features can be configured, provisioned, and monitored through DCNM enterprise management:

- Physical ports
- Port channels and virtual port channels (vPC)
- Loopback and management interfaces
- VLAN network interfaces (sometimes referred to as switched virtual interfaces [SVI])
- VLAN and private VLAN (PVLAN)
- Spanning Tree Protocol, including Rapid Spanning Tree (RST) and Multi-Instance Spanning Tree Protocol (MST)
- Virtual Device Contexts
- Gateway Load Balancing Protocol (GLBP) and object tracking
- Hot Standby Router Protocol (HSRP)
- Access control lists
- IEEE 802.1X
- Authentication, authorization, and accounting (AAA)
- Role-based access control
- Dynamic Host Configuration Protocol (DHCP) snooping
- Dynamic Address Resolution Protocol (ARP) inspection
- IP Source Guard
- Traffic storm control
- Port security
- Hardware resource utilization with Ternary Content Addressable Memory (TCAM) statistics
- Switched Port Analyzer (SPAN)

DCNM also includes end-end enterprise visibility including topology views, event browsers, configuration change management, device operating system management, hardware asset inventory, logging, and statistical data collection management.

### Managing System Files

Directories can be created on bootflash: and external flash memory (slot0:, usb1:, and usb2:); you can also navigate through these directories and use them for files. Files can be created and accessed on bootflash:, volatile:, slot0:, usb1:, and usb2: file systems. Files can be accessed only on the system: file systems. Debug file system can be used for debug log files specified in the `debug logfile` command. System image files, from remote servers using FTP, Secure Copy (SCP), Secure Shell FTP (SFTP), and TFTP can also be downloaded.
File Systems

Table 1-1 outlines the parameters for the syntax for specifying a local file system, which is:

```
filesystem://[module/]
```

Example 1-9 demonstrates some file system commands and how to copy a file.

### Table 1-1 Syntax forSpecifying a Local File System

<table>
<thead>
<tr>
<th>File System Name</th>
<th>Module</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bootflash</td>
<td>sup-active</td>
<td>Internal CompactFlash memory located on the active supervisor module used for storing image files, configuration files, and other miscellaneous files. The initial default directory is bootflash.</td>
</tr>
<tr>
<td></td>
<td>sup-local</td>
<td></td>
</tr>
<tr>
<td>Bootflash</td>
<td>sup-standby</td>
<td>Internal CompactFlash memory located on the standby supervisor module used for storing image files, configuration files, and other miscellaneous files.</td>
</tr>
<tr>
<td></td>
<td>sup-remote</td>
<td></td>
</tr>
<tr>
<td>slot0</td>
<td>Not applicable</td>
<td>External CompactFlash memory installed in a supervisor module used for storing system images, configuration files, and other miscellaneous files.</td>
</tr>
<tr>
<td>volatile</td>
<td>Not applicable</td>
<td>Volatile random-access memory (VRAM) located on a supervisor module used for temporary or pending changes.</td>
</tr>
<tr>
<td>Nvram</td>
<td>Not applicable</td>
<td>Nonvolatile random-access memory (NVRAM) located on a supervisor module used for storing the startup-configuration file.</td>
</tr>
<tr>
<td>Log</td>
<td>Not applicable</td>
<td>Memory on the active supervisor that stores logging file statistics.</td>
</tr>
<tr>
<td>system</td>
<td>Not applicable</td>
<td>Memory on a supervisor module used for storing the running-configuration file.</td>
</tr>
<tr>
<td>debug</td>
<td>Not applicable</td>
<td>Memory on a supervisor module used for debug logs.</td>
</tr>
<tr>
<td>usb1</td>
<td>Not applicable</td>
<td>External USB flash memory installed in a supervisor module used for storing image files, configuration files, and other miscellaneous files.</td>
</tr>
<tr>
<td>usb2</td>
<td>Not applicable</td>
<td>External USB flash memory installed in a supervisor module used for storing image files, configuration files, and other miscellaneous files.</td>
</tr>
</tbody>
</table>
Example 1-9  File System Commands/Copying a File

N7010-1# dir bootflash:
311  Jun 20 05:15:05 2009  MDS20090619155920643.lic
309  Jun 20 05:15:56 2009  MDS20090619155929839.lic
2470887 Aug 01 08:13:35 2009  dp42
8533440 Apr 17 23:17:14 2009  lacp_tech_all.log
308249 Aug 01 09:08:39 2009  libcmd.so
134  Jun 19 23:06:53 2009  libglbp.log
175  Jun 20 04:14:22 2009  libotm.log
49152  Jun 19 22:50:53 2009  lost+found/
87081184 Jan 02 06:21:20 2008  congo-s1-dk9.4.0.2.bin
8775513 Dec 11 13:35:25 2008  congo-s1-dk9.4.0.4.bin
92000595 Apr 16 21:55:19 2009  congo-s1-dk9.4.1.4.bin
92645614 Apr 08 06:08:35 2009  congo-s1-dk9.4.1.5.bin
9204757 Jun 02 04:29:19 2009  congo-s1-dk9.4.1.5E2.bin
99851395 Aug 03 05:17:46 2009  congo-s1-dk9.4.2.0.601.bin
100122301 Aug 12 04:42:13 2009  congo-s1-dk9.4.2.1.bin
9965740 Jan 02 06:21:29 2008  congo-s1-epld.4.0.2.img
9730124 Dec 11 13:42:30 2008  congo-s1-epld.4.0.4.img
23584768 Apr 02 23:47:26 2009  eem_script.cfg
23785984 Dec 11 13:34:37 2008  congo-s1-kickstart.4.0.2.bin
24718848 Apr 16 21:52:40 2009  congo-s1-kickstart.4.1.4.bin
25173504 Apr 08 06:00:57 2009  congo-s1-kickstart.4.1.5.bin
25333248 Aug 03 05:18:37 2009  congo-s1-kickstart.4.2.0.601.bin
25234944 Aug 12 04:40:52 2009  congo-s1-kickstart.4.2.1.bin
12558 Aug 01 08:51:22 2009  shrun
916893 Apr 17 23:23:03 2009  stp_tech.og
4096 Dec 11 14:04:50 2008  vdc_2/
4096 Dec 11 14:04:50 2008  vdc_3/
4096 Dec 11 14:04:50 2008  vdc_4/
592649 Apr 17 23:18:16 2009  vpc_tech.log
942 Jul 10 09:45:27 2009  wireshark

Usage for bootflash://sup-local
98236816 bytes used
827592704 bytes free
1008999520 bytes total

N7010-1# dir bootflash://sup-remote
12349 Dec 05 02:15:33 2008  7k-1.vdc-all.run
4096 Apr 04 06:45:28 2009  eem/
18180 Apr 02 23:47:26 2009  eem_script.cfg
99851395 Aug 03 05:20:20 2009  congo-s1-dk9.4.2.0.601.bin
100122301 Aug 12 04:46:18 2009  congo-s1-dk9.4.2.1.bin
<table>
<thead>
<tr>
<th>Time</th>
<th>Date</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>19021</td>
<td>Apr 03</td>
<td>eem_script_counters.cfg</td>
</tr>
<tr>
<td>19781</td>
<td>Apr 05</td>
<td>eem_script_iptrack.cfg</td>
</tr>
<tr>
<td>29104</td>
<td>Jun 19</td>
<td>ethpm_act_logs.log</td>
</tr>
<tr>
<td>0</td>
<td>Jun 19</td>
<td>ethpm_syslogs.log</td>
</tr>
<tr>
<td>175</td>
<td>Jun 20</td>
<td>libotm.log</td>
</tr>
<tr>
<td>49152</td>
<td>Jun 19</td>
<td>lost+found/</td>
</tr>
<tr>
<td>4775113</td>
<td>Apr 07</td>
<td>congo-s1-dk9.4.0.4.bin</td>
</tr>
<tr>
<td>92000595</td>
<td>Apr 16</td>
<td>congo-s1-dk9.4.1.4.bin</td>
</tr>
<tr>
<td>92645614</td>
<td>Apr 08</td>
<td>congo-s1-dk9.4.1.5.bin</td>
</tr>
<tr>
<td>92004757</td>
<td>Jun 02</td>
<td>congo-s1-dk9.4.1.5E2.bin</td>
</tr>
<tr>
<td>10993389</td>
<td>Mar 22</td>
<td>congo-s1-epld.4.1.3.33.img</td>
</tr>
<tr>
<td>23785984</td>
<td>Apr 07</td>
<td>congo-s1-kickstart.4.0.4.bin</td>
</tr>
<tr>
<td>24718848</td>
<td>Apr 16</td>
<td>congo-s1-kickstart.4.1.4.bin</td>
</tr>
<tr>
<td>25173504</td>
<td>Apr 08</td>
<td>congo-s1-kickstart.4.1.5.bin</td>
</tr>
<tr>
<td>23936512</td>
<td>Jun 02</td>
<td>congo-s1-kickstart.4.1.5E2.bin</td>
</tr>
<tr>
<td>25333248</td>
<td>Aug 03</td>
<td>congo-s1-kickstart.4.2.0.601.bin</td>
</tr>
<tr>
<td>25234944</td>
<td>Aug 12</td>
<td>congo-s1-kickstart.4.2.1.bin</td>
</tr>
<tr>
<td>310</td>
<td>Sep 19</td>
<td>n7k-rhs-1.lic</td>
</tr>
<tr>
<td>12699</td>
<td>Jan 23</td>
<td>run_vpc_jan22</td>
</tr>
<tr>
<td>11562</td>
<td>Mar 13</td>
<td>startup-robert-cfg</td>
</tr>
<tr>
<td>16008</td>
<td>Mar 12</td>
<td>startup-vss-cfg</td>
</tr>
<tr>
<td>17315</td>
<td>Mar 19</td>
<td>startup-vss-cfg_roberto_mar18</td>
</tr>
<tr>
<td>99</td>
<td>Apr 04</td>
<td>test1</td>
</tr>
<tr>
<td>9991</td>
<td>Jun 19</td>
<td>vdc.cfg</td>
</tr>
<tr>
<td>4096</td>
<td>Jan 22</td>
<td>vdc_2/</td>
</tr>
<tr>
<td>4096</td>
<td>Jan 22</td>
<td>vdc_3/</td>
</tr>
<tr>
<td>4096</td>
<td>Sep 11</td>
<td>vdc_4/</td>
</tr>
<tr>
<td>111096</td>
<td>Dec 20</td>
<td>vpc.cap</td>
</tr>
<tr>
<td>0</td>
<td>Feb 03</td>
<td>vpc_hw_check_disable</td>
</tr>
<tr>
<td>18166</td>
<td>Apr 03</td>
<td>vpc_vss_apr02</td>
</tr>
<tr>
<td>18223</td>
<td>Apr 02</td>
<td>vss_vpc_apr2</td>
</tr>
</tbody>
</table>

Usage for bootflash://sup-remote
863535104 bytes used
94636416 bytes free
1800999520 bytes total

N7010-1# copy bootflash://sup
bootflash://sup-1/ bootflash://sup-active/ bootflash://sup-remote/
bootflash://sup-2/ bootflash://sup-local/ bootflash://sup-standby/

N7010-1# copy bootflash://sup-local/congo-s1-epld.4.0.4.img bootflash://sup-remote/congo-s1-epld.4.0.4.img

N7010-1# dir bootflash://sup-remote
<table>
<thead>
<tr>
<th>File Name</th>
<th>Date</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>7k-1-vdc-all.run</td>
<td>Dec 05 02:15:33 2008</td>
<td>12349</td>
</tr>
<tr>
<td>eem/</td>
<td>Apr 04 06:45:28 2009</td>
<td>4096</td>
</tr>
<tr>
<td>eem_script.cfg</td>
<td>Apr 02 23:47:26 2009</td>
<td>18180</td>
</tr>
<tr>
<td>eem_script_counters.cfg</td>
<td>Apr 03 21:04:50 2009</td>
<td>19021</td>
</tr>
<tr>
<td>eem_script_iptrack.cfg</td>
<td>Apr 05 23:30:51 2009</td>
<td>19781</td>
</tr>
<tr>
<td>ethpm_act_logs.log</td>
<td>Jun 19 22:44:51 2009</td>
<td>12699</td>
</tr>
<tr>
<td>ethpm_syslogs.log</td>
<td>Jun 19 22:44:51 2009</td>
<td>11562</td>
</tr>
<tr>
<td>libotm.log</td>
<td>Jun 19 22:38:45 2009</td>
<td>49152</td>
</tr>
<tr>
<td>lost+found/</td>
<td>Jun 20 04:14:37 2009</td>
<td>175</td>
</tr>
<tr>
<td>congo-s1-dk9.4.0.4.bin</td>
<td>Jun 19 22:44:51 2009</td>
<td>4096</td>
</tr>
<tr>
<td>congo-s1-dk9.4.1.4.bin</td>
<td>Jun 19 22:44:51 2009</td>
<td>4096</td>
</tr>
<tr>
<td>congo-s1-dk9.4.1.5.bin</td>
<td>Jun 19 22:44:51 2009</td>
<td>4096</td>
</tr>
<tr>
<td>congo-s1-dk9.4.1.5E2.bin</td>
<td>Jun 19 22:44:51 2009</td>
<td>4096</td>
</tr>
<tr>
<td>congo-s1-dk9.4.2.0.601.bin</td>
<td>Jun 19 22:44:51 2009</td>
<td>4096</td>
</tr>
<tr>
<td>congo-s1-dk9.4.2.1.bin</td>
<td>Jun 19 22:44:51 2009</td>
<td>4096</td>
</tr>
<tr>
<td>congo-s1-epld.4.0.4.img</td>
<td>Jun 19 22:44:51 2009</td>
<td>4096</td>
</tr>
<tr>
<td>congo-s1-epld.4.1.3.33.img</td>
<td>Jun 19 22:44:51 2009</td>
<td>4096</td>
</tr>
<tr>
<td>congo-s1-kickstart.4.0.4.bin</td>
<td>Jun 19 22:44:51 2009</td>
<td>4096</td>
</tr>
<tr>
<td>congo-s1-kickstart.4.1.4.bin</td>
<td>Jun 19 22:44:51 2009</td>
<td>4096</td>
</tr>
<tr>
<td>congo-s1-kickstart.4.1.5.bin</td>
<td>Jun 19 22:44:51 2009</td>
<td>4096</td>
</tr>
<tr>
<td>congo-s1-kickstart.4.1.5E2.bin</td>
<td>Jun 19 22:44:51 2009</td>
<td>4096</td>
</tr>
<tr>
<td>congo-s1-kickstart.4.2.0.601.bin</td>
<td>Jun 19 22:44:51 2009</td>
<td>4096</td>
</tr>
<tr>
<td>congo-s1-kickstart.4.2.1.bin</td>
<td>Jun 19 22:44:51 2009</td>
<td>4096</td>
</tr>
<tr>
<td>n7k-rhs-1.lic</td>
<td>Sep 19 03:58:55 2008</td>
<td>310</td>
</tr>
<tr>
<td>run_vpc_jan22</td>
<td>Jan 23 14:02:52 2009</td>
<td>12699</td>
</tr>
<tr>
<td>startup-robert-cfg</td>
<td>Mar 13 07:52:42 2009</td>
<td>11562</td>
</tr>
<tr>
<td>startup-vss-cfg</td>
<td>Mar 12 02:02:40 2009</td>
<td>16008</td>
</tr>
<tr>
<td>startup-vss-cfg_roberto_mar18</td>
<td>Mar 12 02:02:40 2009</td>
<td>17315</td>
</tr>
<tr>
<td>test1</td>
<td>Apr 04 06:51:15 2009</td>
<td>99</td>
</tr>
<tr>
<td>vdc.cfg</td>
<td>Jun 19 23:12:48 2009</td>
<td>9991</td>
</tr>
<tr>
<td>vdc_2/</td>
<td>Jan 22 13:37:57 2009</td>
<td>4096</td>
</tr>
<tr>
<td>vdc_3/</td>
<td>Jan 22 00:40:57 2009</td>
<td>4096</td>
</tr>
<tr>
<td>vdc_4/</td>
<td>Sep 11 12:54:10 2008</td>
<td>4096</td>
</tr>
<tr>
<td>vpc.cap</td>
<td>Dec 20 04:40:17 2008</td>
<td>111096</td>
</tr>
<tr>
<td>vpc_hw_check_disable</td>
<td>Feb 03 08:02:14 2009</td>
<td>18166</td>
</tr>
<tr>
<td>vpc_vss_apr02</td>
<td>Apr 03 03:24:22 2009</td>
<td>18223</td>
</tr>
</tbody>
</table>

Usage for bootflash://sup-remote
873283584 bytes used
936615936 bytes free
1000899520 bytes total
N7010-1#
Configuration Files: Configuration Rollback

The configuration rollback feature enables you to take a snapshot, or checkpoint, of the Cisco NX-OS configuration and then reapply that configuration to your device at any point without having to reload the device. Rollback allows any authorized administrator to apply this checkpoint configuration without requiring expert knowledge of the features configured in the checkpoint.

You can create a checkpoint copy of the current running configuration at any time. Cisco NX-OS saves this checkpoint as an ASCII file that you can use to roll back the running configuration to the checkpoint configuration at a future time. You can create multiple checkpoints to save different versions of your running configuration.

When you roll back the running configuration, you can trigger the following rollback types:

- **Atomic**: Implement the rollback only if no errors occur. This is the default rollback type.
- **Best-effort**: Implement a rollback and skip any errors.
- **Stop-at-first-failure**: Implement a rollback that stops if an error occurs.

When you are ready to roll back to a checkpoint configuration, you can view the changes that will be applied to your current running configuration before committing to the rollback operation. If an error occurs during the rollback operation, you can choose to cancel the operation or ignore the error and proceed with the rollback. If you cancel the operation, Cisco NX-OS provides a list of changes already applied before the error occurred. You need to clean up these changes manually.

Configuration rollback limitations are as follows:

- Allowed to create up to ten checkpoint copies per VDC.
- You are not allowed to apply a checkpoint file of one VDC into another VDC.
- You are not allowed to apply a checkpoint configuration in a nondefault VDC if there is a change in the global configuration portion of the running configuration compared to the checkpoint configuration.
- The checkpoint filenames must be 75 characters or less.
- You are not allowed to start a checkpoint filename with the word `auto`.
- You cannot name a checkpoint file with `summary` or any abbreviation of the word `summary`.
- Only one user can perform a checkpoint, rollback, or copy the running configuration to the startup configuration at the same time in a VDC.
- After execution of `write erase` and `reload` commands, checkpoints are deleted. You can use the `clear checkpoint database` command to clear out all checkpoint files.
- Rollback fails for NetFlow if during rollback you try to modify a record that is programmed in the hardware.
Although rollback is not supported for checkpoints across software versions, users can perform rollback at their own discretion and can use the best-effort mode to recover from errors.

When checkpoints are created on bootflash, differences with the running-system configuration cannot be performed before performing the rollback, and the system reports “No Changes.”

Example 1-10 demonstrates how to create a configuration rollback.

**Note** You need to make sure you are in the correct VDC. If you need to change VDCs, use the `switchto vdc` syntax.

---

**Example 1-10 Creating a Configuration Rollback**

```
N7010-1# checkpoint changes
............Done
N7010-1# show diff rollback-patch checkpoint changes running-config
Collecting Running-Config
Generating Rollback Patch
Rollback Patch is Empty
N7010-1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
N7010-1(config)# no snmp-server user nxos-admin
N7010-1(config)# exit
N7010-1# show diff rollback-patch checkpoint changes running-config
Collecting Running-Config
Generating Rollback Patch
!!
no username nxos-admin sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAADg
f3KJ
ox/hjgPDCkJ0d-
kUXHjE1V590hZP/NHlBrBq0TGRr+hfdAssD3wG5oPkywgM4+bR/ssCzoj6jVG41tGmfp4pr3dqsMzR2iDXSK
K/tdJ7bipWKy1wSkYqzzwatzlV1XRqTJY7L9a+JqVIJEAn00JMJ10wZ5YbxcBC2GKnKCM2x2BZ14okVg180CCJg
7vmn+8Rq1005JnAPNe9kFw9nsPj/r5xFc1RcSKeQbdYAJItU6cX1TslRnKj1WwCgIa26dEaGdawMvUfTg
u0uM
97VC0xZPQ==
no username nxos-admin
N7010-1# rollback running-config checkpoint changes
Note: Applying config in parallel may fail Rollback verification
Collecting Running-Config
Generating Rollback Patch
Executing Rollback Patch
```
Chapter 1: Introduction to Cisco NX-OS

Generating Running-config for verification
Generating Patch for verification

N7010-1# show snmp user nxos-admin

SNMP USER

<table>
<thead>
<tr>
<th>User</th>
<th>Auth</th>
<th>Priv(enforce)</th>
<th>Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>nxos-admin</td>
<td>sha</td>
<td>des(no)</td>
<td>network-operator</td>
</tr>
</tbody>
</table>

You can also enable specific SNMP traps:

N7010-1(config)# snmp-server enable traps eigrp
N7010-1(config)# snmp-server enable traps callhome
N7010-1(config)# snmp-server enable traps link
N7010-1(config)# exit
N7010-1#

Operating System Files

Cisco NX-OS Software consists of three images:

- The kickstart image, contains the Linux kernel, basic drivers, and initial file system.
- The system image contains the system software, infrastructure, Layers 4 through 7.
- The Erasable Programmable Logic Device (EPLD) image: EPLDs are found on the Nexus 7000 currently shipping I/O modules. EPLD images are not released frequently; even if an EPLD image is released, the network administrator is not forced to upgrade to the new image. EPLD image upgrades for I/O modules disrupt traffic going through the I/O module. The I/O module powers down briefly during the upgrade. The EPLD image upgrades are performed one module at a time.

On the Nexus 7000 with dual-supervisor modules installed, NX-OS supports in-service software upgrades (ISSU). NX-OS ISSU upgrades are performed without disrupting data traffic. If the upgrade requires EPLD to be installed onto the line cards that causes a disruption of data traffic, the NX-OS software warns you before proceeding so that you can stop the upgrade and reschedule it to a time that minimizes the impact on your network.

NX-OS ISSU updates the following images:

- Kickstart image
- System image
- Supervisor module BIOS
- Data module image
The ISSU process performs a certain sequence of events, as outlined here:

**Step 1.** Upgrade the BIOS on the active and standby supervisor modules and the line cards (data cards/nonsupervisor modules).

**Step 2.** Bring up the standby supervisor module with the new kickstart and system images.

**Step 3.** Switch over from the active supervisor module to the upgraded standby supervisor module.

**Step 4.** Bring up the old active supervisor module with the new kickstart image and the new system image.

**Step 5.** Upgrade the CMP on both supervisor modules.

**Step 6.** Perform nondisruptive image upgrade for line card (data cards/nonsupervisor modules), one at a time.

**Step 7.** ISSU upgrade is complete.

**Virtual Device Contexts (VDCs)**

The Nexus 7000 NX-OS software supports Virtual Device Contexts (VDCs), VDC(s) allow the partitioning of a single physical Nexus 7000 device into multiple logical devices. This logical separation provides the following benefits:

- Administrative and management separation
- Change and failure domain isolation from other VDCs
- Address, VLAN, VRF, and vPC isolation

Each VDC appears as a unique device and allows for separate Roles-Based Access Control Management (RBAC) per VDC. This enables VDCs to be administered by different administrators while still maintaining a rich, granular RBAC capability. With this functionality, each administrator can define virtual routing and forwarding instance (VRF) names and VLAN IDs independent of those used in other VDCs safely with the knowledge that VDCs maintain their own unique software processes, configuration, and dataplane forwarding tables.

Each VDC also maintains an individual high-availability (HA) policy that defines the action that the system will take when a failure occurs within a VDC. Depending on the hardware configuration of the system, there are various actions that can be performed. In a single supervisor system, the VDC can be shut down, restarted, or the supervisor can
be reloaded. In a redundant supervisor configuration, the VDC can be shut down, restarted, or a supervisor switchover can be initiated.

**Note**  Refer to Chapter 6, “High Availability,” for additional details.

There are components that are shared between VDC(s), which include the following:

- A single instance of the kernel which supports all of the processes and VDCs.
- Supervisor modules
- Fabric modules
- Power supplies
- Fan trays
- System fan trays
- CMP
- CoPP
- Hardware SPAN resources

Figure 1-5 shows the logical segmentation with VDCs on the Nexus 7000. A common use case is horizontal consolidation to reduce the quantity of physical switches at the data center aggregation layer. In Figure 1-5, there are two physical Nexus 7000 chassis; the logical VDC layout is also shown.

**VDC Configuration**

This section shows the required steps to creating a VDC; once the VDC is created, you will assign resources to the VDC. VDC(s) are always created from the default admin VDC context, VDC context 1.

**Note**  The maximum number of VDCs that can be configured per Nexus 7000 chassis is four; the default VDC (VDC 1) and three additional VDC(s).

Example 1-11 shows how to configure the VDC core on Egypt.

**Example 1-11  Creating VDC “core” on Egypt**

```plaintext
egypt(config)# vdc core
Note: Creating VDC, one moment please ...
egypt# show vdc
vdc_id  vdc_name  state  mac
```
Table 1-5

<table>
<thead>
<tr>
<th>VDC Name</th>
<th>State</th>
<th>MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>egypt</td>
<td>active</td>
<td>00:1b:54:c2:38:c1</td>
</tr>
<tr>
<td>core</td>
<td>active</td>
<td>00:1b:54:c2:38:c2</td>
</tr>
</tbody>
</table>

```bash
egypt# show vdc core detail
vdc id: 2
vdc name: core
vdc state: active
vdc mac address: 00:1b:54:c2:38:c2
vdc ha policy: RESTART
vdc dual-sup ha policy: SWITCHOVER
vdc boot Order: 2
vdc create time: Mon Feb 22 13:11:59 2010
vdc reload count: 1
vdc restart count: 0
egypt#
```

Figure 1-5  Logical Segmentation with VDCs on the Nexus 7000
Once the VDC is created, you now have to assign physical interfaces to the VDC. Depending on the Ethernet modules installed in the switch, interface allocation is supported as follows:

The 32-port 10-Gigabit Ethernet Module (N7K-M132XP-12), interfaces can be allocated on a per port-group basis; there are eight port-groups. For example, port-group 1 are interfaces e1, e3, e5, e7; port-group 2 are interfaces e2, e4, e6, e8.

The 48-port 10/100/1000 I/O Module (N7K-M148GT-11) can be allocated on a per-port basis.

The 48-port 1000BaseX I/O Module (N7K-M148GS-11) can be allocated on a per-port basis.

A future module, N7K-D132XP-15, interfaces will be allocated per 2 ports per VDC.

Note: It is not possible to virtualize a physical interface and associate the resulting logical interfaces to different VDCs. A supported configuration is to virtualize a physical interface and associate the resulting logical interfaces with different VRFs or VLANs. By default, all physical ports belong to the default VDC.

Example 1-12 demonstrates how to allocate interfaces to a VDC.

**Example 1-12 Allocating Interfaces to a VDC**

```bash
egypt(config)# vdc core
egypt(config-vdc)# allocate interface Ethernet1/17
egypt(config-vdc)# allocate interface Ethernet1/18
```

To verify the interfaces allocation, enter the show vdc membership command as demonstrated in Example 1-13.

**Example 1-13 Verifying Interface Allocation to a VDC**

```bash
egypt(config-vdc)# show vdc membership
vdc_id: 1 vdc_name: egypt interfaces:
  Ethernet1/26          Ethernet1/28          Ethernet1/30
  Ethernet1/32          Ethernet2/2           Ethernet2/4
  Ethernet2/6           Ethernet2/8           Ethernet2/26
  Ethernet2/28          Ethernet2/30          Ethernet2/32
  Ethernet3/4           Ethernet3/5           Ethernet3/6
  Ethernet3/7           Ethernet3/8           Ethernet3/9
```
In addition to interfaces, other physical resources can be allocated to an individual VDC, including IPv4 route memory, IPv6 route memory, port-channels, and SPAN sessions. Configuring these values prevents a single VDC from monopolizing system resources. Example 1-14 demonstrates how to accomplish this.

Example 1-14 Allocating System Resources

```
egypt(config)# vdc core
egypt(config-vdc)# limit-resource port-channel minimum 32 maximum equal-to-min
egypt(config-vdc)# limit-resource u4route-mem minimum 32 maximum equal-to-min
egypt(config-vdc)# limit-resource u6route-mem minimum 32 maximum equal-to-min
egypt(config-vdc)# limit-resource vlan minimum 32 maximum equal-to-min
egypt(config-vdc)# limit-resource vrf minimum 32 maximum equal-to-min
```

Defining the VDC HA policy is also done within the VDC configuration sub-mode. Use the ha-policy command to define the HA policy for a VDC as demonstrated in Example 1-15.
**Example 1-15  Changing the HA Policy for a VDC**

```plaintext
egypt(config)# vdc core
egypt(config-vdc)# ha-policy dual-sup bringdown
```

The HA policy will depend based on the use-case or VDC role. For example, if you have dual-supervisor modules in the Nexus 7000 chassis or if the VDC role is development/test, the VDC HA policy may be to just shut down the VDC. If the VDC role is for the core and aggregation use case the HA policy would be switchover.

**Troubleshooting**

The troubleshooting sections introduce basic concepts, methodology, and general troubleshooting guidelines for problems that might occur when configuring and using Cisco NX-OS.

**show Commands**

Table 1-2 lists sample EXEC commands showing the differences between IOS and NX-OS.

<table>
<thead>
<tr>
<th>Operation</th>
<th>IOS</th>
<th>NX-OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays the running configuration</td>
<td>show running-config</td>
<td>show running-config</td>
</tr>
<tr>
<td>Displays the startup configuration</td>
<td>show startup-config</td>
<td>show startup-config</td>
</tr>
<tr>
<td>Displays the status of a specified port-channel interface</td>
<td>show etherchannel #</td>
<td>show port channel #</td>
</tr>
<tr>
<td>Displays the current boot variables</td>
<td>show boot</td>
<td>show boot</td>
</tr>
<tr>
<td>Displays all environmental parameters</td>
<td>show environment</td>
<td>show environment</td>
</tr>
<tr>
<td>Displays the percentage of fabric utilized per module</td>
<td>show fabric utilization</td>
<td>show hardware fabric-utilization [detail]</td>
</tr>
<tr>
<td>Displays the supervisors high-availability status</td>
<td>show redundancy</td>
<td>show system redundancy status</td>
</tr>
<tr>
<td>Displays CPU and memory usage data</td>
<td>show process cpu</td>
<td>show system resources</td>
</tr>
<tr>
<td>Displays specific VRF information</td>
<td>show ip vrf name</td>
<td>show vrf name</td>
</tr>
</tbody>
</table>
**debug Commands**

Cisco NX-OS supports an extensive debugging feature set for actively troubleshooting a network. Using the CLI, you can enable debugging modes for each feature and view a real-time updated activity log of the control protocol exchanges. Each log entry has a timestamp and is listed chronologically. You can limit access to the debug feature through the CLI roles mechanism to partition access on a per-role basis. Although the `debug` commands show real-time information, you can use the `show` commands to list historical and real-time information.

**Caution**  Use the `debug` commands only under the guidance of your Cisco technical support representative because `debug` commands can impact your network/device performance. Save `debug` messages to a special log file, which is more secure and easier to process than sending the `debug` output to the console.

By using the `?` option, you can see the options that are available for any feature. A log entry is created for each entered command in addition to the actual `debug` output. The `debug` output shows a timestamped account of the activity that occurred between the local device and other adjacent devices.

You can use the `debug` facility to track events, internal messages, and protocol errors. However, you should be careful when using the `debug` utility in a production environment because some options might prevent access to the device by generating too many messages to the console or creating CPU-intensive events that could seriously affect network performance.

You can filter out unwanted `debug` information by using the `debug-filter` command. The `debug-filter` command enables you to limit the `debug` information produced by related `debug` commands.

Example 1-16 limits EIGRP hello packet `debug` information to Ethernet interface 1/1.

**Example 1-16  Filtering debug Information**

```
switch# debug-filter ip eigrp interface ethernet 1/1
switch# debug eigrp packets hello
```

**Topology**

Throughout the book, you see a common topology for demonstration purposes. Figure 1-6 depicts the physical topology.
Further Reading

NX-OS Feature Navigator: http://tinyurl.com/2btvax
NX-OS Nexus 7000 Supported MIB List: http://tinyurl.com/pzh4gg
NX-OS Nexus 5000 Supported MIB List: http://tinyurl.com/q4pqp5
NX-OS Nexus 1000V Supported MIB List: http://tinyurl.com/nu22mx
Numerics

10-Gigabit Ethernets, 362-363

A

AAA (Authentication, Authorization, and Accounting), 202
access
  groups, 233
  switch configuration, 57
access control lists. See ACLs
accounting, 202
ACLs (access control lists), 2
  interfaces, applying, 233
  IP configuration, 232-234
  MAC configuration, 234-236
  sequence numbers, modifying, 236
  VLAN configuration, 236-237
actions
  process restarts, 297
  security, 240-242
active zoneset verification, 371

adding
  email servers, 349
  ports to VLANs, 52
  static IP source entries, 252
  static secure MAC addresses, 239
  SVIs, 101
  VEMs, 406-414
  VLANs, 50
addresses
  BGP, 140
  IP management, 54
  MAC, 38
    DHCP snooping, 245
    enabling sticky learning, 238
    maximum number of, 241
  OSPF summary, 122
Advanced Encryption Standard. See AES
advantages of Cisco NX-OS, 1
advertisements, networks, 117, 148-150
AES (Advanced Encryption Standard), 2, 224
allocation
  interfaces to VDCs, 31
  system resources, 32
alphanumeric process IDs, 116
alphanumeric tags
  applying, 101
  EIGRP summarization, 104
  stub routing, 107
analyzers, embedded, 331-342
Any Source Multicast (ASM), 172, 176
Anycast-RP, 177, 186-188
APIs (application programming interfaces), 376
application-specific integrated circuit (ASIC), 38
applications, WireShark, 229
applying
  ACLs
    to interfaces, 233
    to VLANs, 248
  alphanumeric tags, 101
  VACLs, 237
architecture
  HA, 295
  Nexus 1000V, 377
areas, OSPF, 118
ASIC (application-specific integrated circuit), 38
ASM (Any Source Multicast), 172, 176
assignment
  ports, 83
  SNMPv3 users to multiple roles, 273
  VLAN memberships, 52-53
association, keychains, 252
atomic mode, 350
atomic rollback, 25
attribute-value (AV) pairs, 202
authentication, 202. See also security
  BGP, 144-145
  clear-text, 156
  consoles, 204
  EIGRP, 108
  local, 209
  OSPF, 128
  PIM, 179
  SNMPv3, 271
  TACACS+ configuration, 215
  Telnet, 217
Authentication, Authorization, and Accounting (AAA), 202
authorization, 202
Auto-RP, 177
  configuration, 184-186
autonomous-system as-number command, 100
AV (attribute-value) pairs, 202
availability, 2.
  See also HA (high availability)

B

backward congestion notification (BCN), 364
bandwidth, unicast storm control configuration, 255
BCN (backward congestion notification), 364
best-effort
  modes, 350
  rollbacks, 25
BGP (Border Gateway Protocol), 2, 137-152
  configuration, 137-140
Graceful Restart, 295
metrics, modifying routing, 150-151
neighbors, 141-144
networks, advertisements, 148-150
peer templates, 146-147
redistribution of prefix lists, 149
security, 144-145
verification of configuration, 151
Bidir (Bidirectional), 172
Bidirectional (Bidir), 172
Bootflash, 21
Bootstrap Routers. See BSRs
bootup diagnostics, 288
Border Gateway Protocol. See BGP
BPDUFilter, 73
BPDUGuard, 73-74
BPDUs (Bridge Protocol Data Units), 63
Bridge Assurance, 76-77
Bridge Protocol Data Units. See BPDUs
broadcasts
storm verification, 253
suppression, 55
BSRs (Bootstrap Routers), 182-184
bypassing bootup diagnostics, 288

C

CAM (Content Addressable Memory), 38
capturing traffic to files, 334
CE (Customer Edge), 231
Certificate Security Warning Dialog Box, 395
CFS (Cisco Fabric Services), 205, 349
distribution, 207
TACACS+ distribution, 213
channels
compatibility, 83
Etherchannels, 39
port-channels, Nexus 200, 45
ports
flow control, 85
virtual, 39
characteristics of port profiles, 430-431
checkpoint configuration, 25, 350-352
Cisco Fabric Services. See CFS
Cisco IOS, comparison to, 3-5
Cisco Technical Assistance Center (TAC), 294, 343
Cisco TrustSec. See CTS
Class of Service (CoS), 363
clear-text authentication, 156
CLI (command-line interface), 156
CMP (connectivity management processor), 9-11, 285
CNAs (Converged Network Adapters), 365
command-line interface. See CLI
commands
AAA, 205
autonomous-system as-number, 100
debug, 34
debug-filter, 34
EXEC setup, 389
rate limiting, 267
show, 33
show vlan, 53
Smart Call Home Alerts, 343
switchto vdc, 221
vlan vlan-id configuration, 50
vlan vlan-range, 50
common data center topology, 60

communities
  SNMP, 274
  VLANs, 55

comparison to Cisco IOS, 3-5

compatibility of channels, 83

components
  SPAN, 311-326
  VDCs, 29

configuration
  access to switches, 57
  ACLs
    IP, 232-234
    MAC, 234-236
    VLANs, 236-237
  Anycast-RP, 186-188
  Auto-RP, 184-186
  BGP, 137-140, 151
  BSRs, 182-184
  checkpoints, 350-352
  Cisco TrustSec, 224-231
  CoPP, 257-266
  DAI, 246-250
  default routes, 131
  ERSPAN port profiles, 327
  FC uplinks, 370
  FCoE, 369-373
  GLBP, 163-170, 165
  HSRP, 152-158
  IP
    multicast, 171-172
    Source Guard, 250-252
  keychains, 107, 156, 252-253
  LACP, 83
  Layer 2, 37-38, 78-87
  Layer 3, 97-170

MD5 authentication, 127
  monitor sessions, 314
  MST, 65-69
  NetFlow, 353-359
  Nexus 1000V, IGMP, 195-197
  Nexus 2000
    port-channels, 45
    static pinning, 41-45
  Nexus 5000
    IGMP, 194-195
    Unified Fabric, 364-367
  Nexus 7000
    IGMP, 190-194
    MSDP, 197
    PIM, 177-189
  notification receivers, 274
  OSPFv2, 114-120
  passive interfaces, 102
  ports
    costs, 70
    security, 237-242
  power redundancy, 280
  PVLANs, 55-58
  RADIUS, 202-212, 205-212
  Rapid-PVST+, 60
  rate limits, 266-271
  rollbacks, 25-27, 350-352
  RPF, 255-257
  Smart Call Home, 347-350
  SNMPv3, 271-278
  SPAN
    Nexus 1000V, 323-326
    Nexus 5000, 319-323
    Nexus 7000, 312-323
  SPT parameters, 69-72
  SSH, 221-223
SSM, 188-189
static RPF, 188-189
static RPs, 180-182
STP bridge priority, 62
TACACS+, 211-220
traffic storm control, 253-255
trunk interfaces, 52
UDLD, 94
unicast traffic storm control, 254
uplink profiles, 405-407
VDCs, 29-33
VLANs, 50-51, 53-54
vPCs, 88
VRRP, 158-162, 160-161
congestion, 363
connections, CMP interfaces, 10
Connectivity Management Processor. See CMP
consistency, forwarding tables, 49
console authentication, 204
consolidation, I/O, 361
Ethernet, 362
Content Addressable Memory (CAM), 38
Control Plane Policing. See CoPP
Controller Processor (supervisor module), 8
Converged Network Adapters (CNAs), 365
cooling system redundancy, 282-285
CoPP (Control Plane Policing), 3
configuration, 257-266
copying files, 22-24
CoS (Class of Service), 363
cost of port configuration, 70
cryptography, AES, 224
CTS (Cisco TrustSec), 2
configuration, 224-231
Layer 2 solutions, 231
VLANs, confirming, 228
Customer Edge. See CE
cut-through switching, 38

D

DAI (Dynamic ARP Inspection), 246-250
trust state, 247-250
Data Center Bridging, 363
Data Center Bridging Capability Exchange (DCBX), 364
Data Center Interconnect, 231
Data Center Network Manager (DCNM), 19-20
DCBX (Data Center Bridging Capability Exchange), 364
DCNM (Data Center Network Manager), 19-20
debug commands, 34
debug logs, 21
debug-filter command, 34
defaults
route configuration, 131
runtime diagnostics schedules, 291
SPT costs, 69
STP timers, 63
defining
flow exporters, 355
prefix lists, 110, 130
PVLANs, 56
route maps, 111
STP port types, 78
dense wavelength division multiplexing. See DWDM
deployment
AAA services, 203
VSM, 388
Designated Forwarders (DFs), 176
destination MAC (DMAC), 38
destination ports, ERSpan, 326
detection, VLAN BPDUs, 77
DFs (Designated Forwarders), 176
DHCP (Dynamic Host Configuration Protocol) snooping, 242-246
diagnostics
bootup, 288
GOLD, 287-294
on-demand, 294
runtime, 289-293
dialog boxes, Certificate Security Warning, 395
Diffusing Update Algorithm (DUAL), 98
Digital System Algorithm (DSA), 12
disabling
BPDUFilter, 73
LinkUp/LinkDown SNMP notifications, 275
LoopGuard, 75
port profiles, 430
RootGuard, 75
dispute mechanisms, 76
Distributed Resource Scheduler (DRS), 376
distribution
CFS, 207
TACACS+, 213
trees, IP multicast, 172-175
DMAC (destination MAC), 38
dotted-decimal notation, configuring BGP, 139
DRS (Distributed Resource Scheduler), 376
DSA (Digital System Algorithm), 12
DUAL (Diffusing Update Algorithm), 98
Dynamic ARP Inspection. See DAI
Dynamic Host Configuration Protocol. See DHCP

E

EACACS+ (Terminal Access Controller Access Control device Plus)
eBGP (external BGP), 142
edge ports, 77
egress traffic, rate limits, 267
EIGRP (Enhanced Interior Gateway Routing Protocol), 2, 170-114
enabling, 99
operations, 98
redistribution, 109-114
security, 107-109
stub routing, 106-107
summarization, 103-106
email servers, adding, 349
embedded serviceability features, 311-312
analyzers, 331-342
configuration checkpoints and rollbacks, 350-352
ERSpan on Nexus 1000V, 326-331
NetFlow, 353-359
Smart Call Home, 342-350
SPAN, 325-326
enabling
authentication, 156
BGP, 138
Bridge Assurance, 76
CTS, 224
DAI, 247
DHCP snooping, 242
EIGRP, 99
FCoE, 367
GLBP, 163
HSRP, 153
IGMP, 191
IP Source Guard, 251
LoopGuard, 75
MDS ports, 369
MSDP, 198
NetFlow, 354
NPV, 368
OSPF, 115
peer-gateway, 94
PIM, 178
port profiles, 430
port security, 238
PVLANs, 56
RADIUS, 205
RootGuard, 74
SNMP notifications, 277
SSH, 221
sticky learning, 238
TACACSp, 212
Telnet, 414
TrunkFast, 78
vPCs, 88
VRRP, 159
VTP, 51
Encapsulated Remote SPAN. See ERSpan
end-to-end privacy, 224
Enhanced Interior Gateway Routing Protocol. See EIGRP
enhanced transmission selection (ETS), 363
entering ACL configurations, 236
EOBC (Ethernet Out-of-Band) redundancy, 286
EPLD (Erasable Programmable Logic Device), 27
Erasable Programmable Logic Device (EPLD), 27
errdisable action, 240
ERSPAN (Encapsulated Remote SPAN), 326-331
Nexus 1000V, 376
sessions, 324
ESX vSphere hosts, adding VEM, 406-414
Ethalyzer, 230
Etherchannels, 39
Ethernet Out-of-Band. See EOBC
Ethernets
10-Gigabit, 362-364
DHCP snooping, 245
FCoE, 364
I/O consolidation, 362
multicast storm control verification, 254
support, 7
Unified Fabric, 362-364
ETS (enhanced transmission selection), 363
EXEC mode, 6
EXEC setup command, 389
Extensible Markup Language. See XML
external BGP (eBGP), 142
encryption, enforcing SNMP messages, 272
Fabric Discoveries (FDISC), 368
Fabric Extenders, Nexus 2000, 38-40
fabric login (FLOGI), 368
fabric module redundancy, 286-287
failures
diagnostics, 293. See also diagnostics
fans, 282
processes, 299
fans, verification, 282
FC uplinks, configuration, 370
FC-LS (Fibre Channel Link Services), 368
FCID (Fibre Channel Identification), 367
FCoE (Fibre Channel over Ethernet), 318, 364
configuration, 369-373
licenses, 366
FCS (frame check sequence), 38
FDISC (Fabric Discoveries), 368
FHRP (First Hop Redundancy Protocol), 98, 152-170
Fibre Channel, 318
Fibre Channel Identification (FCID), 367
Fibre Channel Link Services (FC-LS), 368
field replaceable unit (FRU), 282
FIFO (First In First Out), 38
files
copying, 22-24
operating systems, 27-28
systems
management, 20-28
specifying local, 21
traffic, capturing, 334

filtering
BPDUFilter, 73
DAI, 248
debug information, 34
messages, 346
First Hop Redundancy Protocols. See FHRP
First In First Out (FIFO), 38
fixed limit options, 112, 134
flexibility, 1
FLOGI (fabric login), 368
flow control, port channels, 85
flow records, creating, 354
forward-delay timers, 63
forwarding
Layer 2
Nexus 7000, 48
verification, 48-49
NSF, 299
RPF, 174, 255-257
tables, consistency, 49
frame check sequence (FCS), 38
frames, PAUSE implementation, 363
FRU (field replaceable unit), 282
full redundancy scheme, 280

Gateway Load Balancing Protocol. See GLBP
Generic Online Diagnostics. See GOLD
Generic Routing Encapsulation. See GRE
Generic Routing Encapsulation (GRE), 324
GLBP (Gateway Load Balancing Protocol), 98, 152
c configuration, 163-170
preemption, 164-165
priority, 164-165
secondary support, 169-170
security, 166-169
verification, 165
global configuration command mode, 6
global TACACS+ secret key configuration, 213
GOLD (Generic Online Diagnostics), 287-294
Graceful Restart (BGP), 295
GRE (Generic Routing Encapsulation), 2, 324
grid redundancy, 280
groups
access, 233
range configuration, 181
servers, 215
Smart Call Home Alerts, 343
GUIs (graphical user interfaces), Nexus 1000V installation, 399-400

H

HA (high availability), 279
architecture, 295
nonstop forwarding, 299
physical redundancy, 279-287
policies, 29
processes
  modularity, 295-296
  restarting, 297
stateful switchover, 297-298
VSM, 421-429
hello packets, 117

hello timers, 63
  PIM, 179
high availability
hostnames, modifying VSM, 414-421
hosts
  links, 79
  servers, 214
  standard, 79
  virtualization, 78
HSRP (Hot Standby Router Protocol), 98
  configuration, 152-158
  MD5, 156
  preemption, 154-155
  priority, 154-155
  secondary support, 157-158
  security, 155-1
hypervisor, 375-376, 380

I

I/O consolidation, 361, 362
IANA (Internet Assigned Number Authority), 172
iBGP (internal BGP), 141
IDS (Intrusion Detection Systems), 312
IETF (Internet Engineering Task Force), 114, 137
IGMP (Internet Group Management Protocol), 171
  enabling, 191
Nexus 1000V
  configuration, 195-197
  snooping, 196
Nexus 5000
  configuration, 194-195
  snooping, 194
Nexus 7000

configuration, 190-194
snooping, 194
operations, 189-190
versions, modifying, 192

images, updating, 27

implementation of PAUSE frames, 363

In-Service Software Upgrades. See ISSUs

inheritance, port profiles, 431

installation, Nexus 1000V

GUIs, 399-400
licenses, 412
VSM, 382-429

instances, EIGRP, 99. See also EIGRP

intercepts, DAI, 248

interface configuration command
mode, 7

interfaces

ACLs, applying, 233
APIs, 376
EIGRP, 109
Ethernet support, 7
GUIs, 399-400
IGMP, enabling, 191
IP Source Guard, enabling, 251

Layer 2

configuration, 78-87
DAI trust state configuration, 247

enabling port security, 238
management, 8-20
multicast storm control configuration, 254

passive

configuration, 102
OSPF, 119

security violations, 241
source, SNMP, 275
SVIs, 57
TACACS+, 216
Telnet, 11
VDCs, allocation to, 31

intermediate System-to-Intermediate System. See ISIS

internal BGP (iBGP), 141
internal VLAN usage, 50

Internet Assigned Number Authority (IANA), 172

Internet Engineering Task Force (IETF), 114, 137

Internet Group Management Protocol. See IGMP

Internet Protocol. See IP

interprocess communication (IPC), 295

Intrusion Detection Systems (IDS), 312

Intrusion Prevention Systems (IPS), 312

IP (Internet Protocol)

ACL configuration, 232-234
address management, 54

multicast

configuration, 171-172
distribution trees, 172-175
operations, 171-177
PIM, 174-176
RPF, 174

Source Guard configuration, 250-252
static source entries, adding, 252

IPC (interprocess communication), 295

IPS (Intrusion Prevention Systems), 312
ISIS (Intermediate System-to-Intermediate System), 2
isolated VLANs, 55
ISSUs (In-Service Software Upgrades), 2, 285, 299-308

K
keychains
configuration, 107, 156
management, 252-253
keys
AAA, 202. See also AAA; security
global TACACS+ secret key configuration, 213
servers, 214
generating, 222
SSH, 221

L
LACP (Link Aggregation Control Protocol), 82
configuration, 83
Last In First Out (LIFO), 38
Layer 2
configuration, 37-38
CTS, 231
forwarding
Nexus 7000, 48
verification, 48-49
interfaces
configuration, 78-87
DAI trust state configuration, 247
enabling port security, 238
IP Source Guard, enabling, 251
overview, 37-49
support, 37-48
Layer 3
configuration, 97-170
rate limits, 269
support, 97-170
licenses
FCoE, 366
Nexus 1000V installation, 412
VSM, 383
LIFO (Last In First Out), 38
limitations
number
of captured frames, 339
of redistributed routes, 135
of prefixes, 112
of rollbacks, 25
rate configuration, 266-271
of sessions
ERSPAN, 324
Nexus 5000 SPAN, 319
Nexus 7000 SPAN, 313
line card runtime diagnostics, 290
Link Aggregation Control Protocol. See LACP
links, virtualization hosts, 79
LinkUp/LinkDown SNMP notifications, disabling, 275
lists
prefixes
BGP redistribution, 149
defining, 110, 130
VLANs, 237
load distribution, verification, 86
local authentication, 209
local file systems, specifying, 21
logs, DAI, 248
loop prevention, 381
LoopGuard, 75-76

MAC (Media Access Control), 38
ACL configuration, 234-236
addresses
  
  DHCP snooping, 245
  maximum number of, 241
sticky learning, enabling, 238

management
ACLs, 232
features, 2
interfaces, 8-20
IP addresses, 54
keychain, 252-253
Session Manager, 233
system files, 20-28
System Manager, 295

manual installation, Nexus 1000V
  VSM, 382-399

mapping
PVLANs, 58
routes, defining, 111, 130
max-age timers, 63
maximum number of MAC addresses, 241
maximum retries (process restarts), 297

MBGP (Multiprotocol Border Gateway Protocol), 171
MD5 (Message Digest 5), 127
HSRP, 156

MDS ports, enabling, 369

Media Access Control. See MAC


membership, VLANs, 52-53
message and transaction services (MTS), 295

Message Digest 5. See MD5

messages
  debug, 34
  filtering, 346
  SYSLOG, 274

metrics, modifying BGP routing, 150-151

Microsoft Windows Server, CNAs, 365

minimum lifetimes (process restarts), 297

misconfiguration, MST, 66

modes
  user, 5-7
  EXEC, 6
  global configuration, 6
  interface configuration command, 7

  VTP devices, 51

modification
ACL sequence numbers, 236
diagnostic parameters, 293
IGMP versions, 192
routing, BGP metrics, 150-151
Smart Call Home alert groups, 348
STP timers, 64
VSM hostnames, 414-421

modularity, 1
  processes, 295-296

modules, fabric, 286-287

monitor ports, SPAN, 314
monitor sessions
  configuration, 314
  ERSpan, 330
MPLS (Multiprotocol Label Switching), 2
  CTS, 231
MSDP (Multicast Source Discovery Protocol), 171
  enabling, 198
  Nexus 7000 configuration, 197
MST (Multiple Spanning Tree), 59
  configuration, 65-69
  verification, 69
MTS (message and transaction services), 295
Multicast Source Discovery Protocol.
  See MSDP
multicasting, 2. See also IP multicast
Multiple Spanning Tree (MST), 59
  multiple VLANs, creating, 50
Multiprotocol Border Gateway Protocol. See MBGP
Multiprotocol Label Switching. See MPLS

N

N+1 (ps-redundant) scheme, 280
N-Port ID Virtualization. See NPIV
N-Port Virtualization. See NPV
neighbors
  BGP, 141-144
  eBGP, 142
  EIGRP, 98
  iBGP, 141
  OSPF stub, 124
NETCONF (Network Configuration Protocol), 14
NetFlow, 353-359
Network Configuration Protocol (NETCONF), 14
networks
  advertisements, 117
  advertisements, BGP, 148-150
  ports, 77
Nexus 1000V, 375
  GUI installation, 399-400
  hypervisor, 375-376, 380
  IGMP configuration, 195-197
  license installation, 412
  NetFlow, 357-359
  port profiles, 429-439
  SPAN, 323-326
  switching, 379-381
  system overview, 376-379
  VSM installation, 382-429
  vSphere, 361-376
Nexus 2000
  Fabric Extenders, 38-40
  port-channels, 45
  static pinning verification, 41-45
Nexus 5000
  IGMP configuration, 194-195
  SPAN, 318-323
  Unified Fabric configuration, 364-367
Nexus 7000
  IGMP configuration, 190-194
  Layer 2 forwarding, 48
  Layer 3, 97-170
  MSDP configuration, 197
  NetFlow, 354-357
  PIM, 177-189
  redundant power supplies, 280
SPAN, 312-318
VTP support, 51
nonredundant (combined) scheme, 280
nonstop forwarding (NSF), 299
nonvolatile random-access memory (NVRAM), 21
normal ports, 77
not-so-stubby-area (NSSA), 123
notifications
  congestion, 363
  LinkUp/LinkDown SNMP, disabling, 275
  receiver configuration, 274
  SNMP, enabling, 277
NPIV (N-Port ID Virtualization), 367
NPV (N-Port Virtualization), 367-369
NSF (nonstop forwarding), 299
NSSA (not-so-stubby-area), 123
numeric process IDs, 116
NVRAM (nonvolatile random-access memory), 21

OSM (Original Storage Manufacturer), 367
OSPF (Open Shortest Path First), 2, 114-137
  redistribution, 129-137
  security, 127-129
  stub routing, 123
  summarization, 120-123
OSPFv2 (Open Shortest Path First version 2) configuration, 114-120
OTV (Overlay Transport Virtualization), 2
OVA/ OVF (Open Virtualization Appliance / Open Virtualization Format) method, 382
Overlay Transport Virtualization (OTV), 2

P
packets, hello, 117
parameters
  diagnostics, 293
  SPT, 69-72
  VTP, 51
partitions, VDCs, 28. See also VDCs
passive interfaces
  configuration, 102
  OSPF, 119
paths, RPF, 255-257
PAUSE frames, implementation, 363
PBR (Policy-Based Routing), 2
peer configurations, MSDP, 199
peer templates, BGP, 146-147
Peer-Gateway, vPCs, 94
Persistent Storage Service (PSS), 295
PFC (priority-based flow control), 363

on-demand diagnostics, 294
Open Shortest Path First. See OSPF
Open Virtualization Appliance / Open Virtualization Format (OVA/OVF) method, 382
operating systems
  files, 27-28
  overview of, 1-5
operations
  EIGRP, 98
  IGMP, 189-190
  IP multicast, 171-177
physical redundancy, 279-287
See also redundancy
PIM (Protocol Independent Multicast), 2, 171
IP multicast, 174-176
Nexus 7000 configuration, 177-189
ping tests, 229
pinning, static, 39, 41-45
platforms, support, 3
plug-ins, VSM, 393
policies, CoPP, 258
policing, CoPP configuration, 257-266
Policy-Based Routing (PBR), 2
port-channels
Nexus 200, 45
ports, assigning, 83
ports
assignment, 83
channels, flow control, 85
costs, configuration, 70
ERSPAN, 326
FCoE, 364
MDS, enabling, 369
monitor, 314
priority, 72
profiles, 80, 429-439
SD, 322
security configuration, 237-242
SPAN, 312
STP types, 77-78
trunks, 79
VEM virtual, 380
VLANs, adding, 52
vmk, 327
power supply redundancy, 280-282
preemption
GLBP, 164-165
HSRP, 154-155
VRRP, 160
prefix lists
BGP redistribution, 149
defining, 110, 130
prevention, loops, 381
priority
GLBP, 164-165
HSRP, 154-155
MST configuration, 68
ports, 72
VRRP, 160
priority-based flow control (PFC), 363
privacy
end-to-end, 224
SNMPv3, 271
private VLANs. See PVLANs
processes
BGP configuration, 139
failures, 299
modularity, 295-296
restarting, 297
profiles
ports, 80, 429-439
uplink, 405-407
protect action, 240
Protocol Independent Multicast. See PIM
pseudo-wire (PW), 231
PSS (Persistent Storage Service), 295
PVLANs (private VLANs), 37, 54-59
access switch configuration, 57
configuration, 55-58
synchronization, 67
PW (pseudo-wire), 231
QCN (quantized congestion notification), 363
QoS (quality of service), 376
port profiles, 437
quality of service. See QoS
quantized congestion notification (QCN), 363

R
RADIUS (Remote Authentication Dial-In User Service), 12
configuration, 202-212
ranges, groups, 181
Rapid Per-VLAN Spanning Tree, 59
Rapid-PVST+ configuration, 60
rate limitations, configuration, 266-271
RBAC (Roles Based Access Control Management), 28
recalculation, spanning-tree, 64
receivers, notification, 274
redistribution
BGP prefix lists, 149
EIGRP, 109-114
OSPF, 129-137
redundancy
cooling systems, 282-285
EOBC, 286
fabric modules, 286-287
grids, 280
physical, 279-287
power supplies, 280-282
supervisors, 285-286, 297
Remote Authentication Dial-In User Service. See RADIUS
Remote SPAN (RSPAN), 312
removing
RootGuard, 75
VLANs, 53
Rendezvous Points. See RPs
Requests for Comments (RFCs), 114
requirements, PVLAN configurations, 55
resiliency, 1
resource allocation, 32
restarting processes, 297
restrict action, 240
Reverse Path Forwarding (RPF), 174
reviewing
EIGRP configurations, 113
OSPF configurations, 136
summarization, 105
RFCs (Requests for Comments), 114
RIP (Routing Information Protocol), 98
Rivest, Shamir, and Adelman (RSA) public-key cryptography, 12
Roles Based Access Control Management (RBAC), 28
rollback configuration, 25-27, 350-352
RootGuard, 74-75
routers
BSRs, 182-184
IDs
BGP, 140
configuration, 117
routes
default configuration, 131
maps, defining, 111, 130
routing, 2
BGP metrics, 150-151
OSPF, 116
stub

EIGRP, 106-107
OSPF, 123
Routing Information Protocol. See RIP
RPF (Reverse Path Forwarding), 174
RPF (Unicast Reverse Path Forwarding), 255-257
RPs (Rendezvous Points), 172, 176-177
static configuration, 180-182
RSA (Rivest, Shamir, and Adelman)
public-key cryptography, 12
RSPAN (Remote SPAN), 312
runtime diagnostics, 289-293

S

SAN-OS (Storage Area Network Operating System), 1
SANs (storage-area networks), 363
saving debug messages, 34
scalability, 1
ACL management, 232
SD (SPAN Destination) ports, 322
secondary support
GLBP, 169-170
HSRP, 157-158
VRRP, 162
secret keys, 213
Secure Shell. See SSH
security, 2, 201-202
actions, 240-242
BGP, 144-145
CoPP, 257-266
CTS, 224-231
DAI, 246-250
DHCP snooping, 242-246
EIGRP, 107-109
GLBP, 166-169
HSRP, 155-157
IP ACLs, 232-234
IP Source Guard, 250-252
keychain management, 252-253
MAC ACLs, 234-236
OSPF, 127-129
ports, 237-242
PVLANs, 54
RADIUS, 202-212
rate limitations, 266-271
SNMPv3, 271-278
SSH, 221-223
TACACS+, 211-220
traffic storm control, 253-255
unicast RPF, 255-257
violations, 240-242
VLAN ACLs, 236-237
VRRP, 161
sequence numbers, modifying ACLs, 236
servers
email, adding, 349
groups, 215
hosts, 214
keys, 214

generating, 222
SSH, 221
Microsoft Windows Server, CNAs, 365
telnet, 11
vCenter Server, 396
Service Level Agreements. See SLAs
serviceability, 2
Session Manager, 233
sessions
ERSPAN, 324
monitor, configuration, 314
Nexus 5000 SPAN, 319
Nexus 7000 SPAN, 313
Shortest Path Tree (SPT), 172
show commands, 33
show vlan command, 53
shutdown action, 240
Simple Network Management Protocol. See SNMP
SLAs (Service Level Agreements), 279
slot0, 21
Smart Call Home, 342-350
smooth round trip time (SRTT), 98
snapshot configuration, 25-27
SNMP (Simple Network Management Protocol), 14-19
 communities, 274
notifications, enabling, 277
SNMPv3 (Simple Network Management Protocol version 3) configuration, 271-278
snooping
DHCP, 242-246
IGMP, 190
 Nexus 1000V, 196
 Nexus 5000, 194
 Nexus 7000, 194
Source Guard, IP configuration, 250-252
source interfaces
SNMP, 275
TACACS+, 216
source ports
ERSPAN, 326
SPAN, 312
Source Specific Multicast. See SSM
SPAN (Switched Port Analyzer), 311-326
 Nexus 1000V, 323-326, 376
 Nexus 5000, 318-323
 Nexus 7000, 312-318
SPAN Destination (SD) ports, 322
Spanning Tree Protocol. See STP
spanning-tree root keyword, 61
specification
local file systems, 21
STP diameters, 64
VTP parameters, 51
SPT (Shortest Path Tree), 172
parameters, 69-72
tools, 72-77
SRTT (smooth round trip time), 98
SSH (Secure Shell), 12-14
customization, 221-223
enabling, 221
TACACS+ configuration, 215
SSM (Source Specific Multicast), 171, 172, 176, 188-189
SSO (Stateful Switchover), 285
standard hosts, 79
state, trust, 247-250
stateful process restart, 297
stateful switchover, HA, 297-298
Stateful Switchover (SSO), 285
static IP source entries, adding, 252
static MAC entries, creating, 48
static pinning, 39
 verification, 41-45
static RP configuration, 180-182
static RPF, 188-189
static secure MAC addresses, 239
sticky learning, 238
stop-at-first failure mode, 350
stop-at-first failure rollback, 25
Storage Area Network Operating System (SAN-OS), 1
storage-area networks (SANs), 363
store-and-forward switching, 38
storm control, traffic configuration, 253-255
STP (Spanning Tree Protocol), 2, 59-87
port types, 77-78
root verification, 70
timers, 63-65
stub routing
  EIGRP, 106-107
  OSPF, 123
subdomains, PVLANs, 55
subnets
  GLBP, 169-170
  HSRP, 157-158
  VRRP, 162
summarization
  EIGRP, 103-106
  OSPF, 120-123
supervisors
  module (Controller Processor), 8
  redundancy, 285-286, 297
  runtime diagnostics, 289
  switchover, 297
support
  Ethernets, 7
  GLBP, 169-170
  HSRP, 157-158
  Layer 2, 37-38
  Layer 3, 97-170
  PIM, 176
  platforms, 3
  VRRP, 162
SVIs (switched virtual interfaces), 57
  adding, 101
  GLBP configurations on, 164
  HSRP configuration on, 153
  VRRP configuration on, 159
SWDM (dense wavelength division multiplexing), 231
Switched Port Analyzer. See SPAN
switched virtual interfaces. See SVIs
switches
  access, configuration, 57
  Layer 3, 97. See also Layer 3
  RADIUS verification, 206
  SPAN, 312
  TACACS+ CFS configuration distribution, 216
switching
  Nexus 1000V, 379-381
  store-and-forward, 38
switchovers
  stateful, 297-298
  supervisors, 297
switchto vdc command, 221
synchronization, PVLANs, 67
SYSLOG messages, 274
  Smart Call Home mapping, 346
system file management, 20-28
system generated checkpoints, 350
system image compatibility and impact, 299
System Manager, 295
system overview, Nexus 1000V, 376-379
system resource allocation, 32

T

tables
  CAM, 38
  forwarding, consistency, 49
TAC (Cisco Technical Assistance Center), 294, 343
TACACS+ (Terminal Access Controller Access Control System Plus), 12
  CFS distribution, 213
  configuration, 211-220
  enabling, 212
tags, alphanumeric, 101
TCP (Transmission Control Protocol), 363
Telnet, 11
  authentication, 217
  enabling, 414
  TACACS+ configuration, 215
temperature, fans, 282
templates, peer, 146-147
Terminal Access Controller Access Control System Plus (TACACS+), 12
tests, ping, 229
thresholds, temperature, 283
timers
  hello, PIM, 179
  process failures, 299
  STP, 63-65
tools
  BPDUFilter, 73
  BPDUGuard, 73-74
  Bridge Assurance, 76-77
  dispute mechanisms, 76
  LoopGuard, 75-76
  RootGuard, 74-75
  SPT, 72-77
topologies, 34
  BGP configurations, 138
  CTS, 224
  DHCP snooping, 243
  FCoE, 366, 369
  GLBP configurations, 163
  HSRP configurations, 153
  IGMP snooping, 195
  MSDP configurations, 198
  Nexus 1000V SPAN, 324
  Nexus 2000, 40
  Nexus 5000 SPAN, 319
  OSPFv2 configuration, 115
  Port-Channels, 45
  PVLANs, 56
  security, 204
  SPAN, 313
  STP, 60
  VRRP configurations, 158
traffic
  congestion, 363
  egress, rate limits, 267
  files, capturing, 334
  storm control configuration, 253-255
Transmission Control Protocol (TCP), 363
trees, distribution, 172-175
triggering rollback types, 25
troubleshooting, 33-34. See also diagnostics
  GOLD, 287-294
  SPAN, 311-326
TrunkFast, enabling, 78
trunks
  interfaces, creating, 52
  ports, 79
trust, state, 247-250
TrustSec. See CTS
types
  ports, 77-78
  rollback, 25

U

UDLD (Undirectional Link Detection), 2, 37, 94-96
uncontrolled redistribution, 132
Undirectional Link Detection. See UDLD
Unicast Reverse Path Forwarding. See RPF
unicast traffic storm control configuration, 254
unified data center operating systems, 1
Unified Fabric, 361
  Ethernets, 362-364
  FCoE configuration, 369-373
  Nexus 5000 configuration, 364-367
  NPV, 367-369
  overview of, 361-362
unique device IDs, CTS configuration, 225
updating images, 27
upgrades, ISSUs, 299-308. See also ISSUs
uplinks
  FC configuration, 370
  profiles, creating, 405-407
usb1/usb2, 21
user modes, 5-7
  EXEC, 6
  global configuration, 6
  interface configuration command, 7

V

validation, DAI, 248
cCenter Server, 396
VDCs (virtual device contexts), 2, 4, 28-33
  configuration, 29-33
  SPAN, 312
vDS (vNetwork Distributed Switch), 376
VEMs (Virtual Ethernet Modules), 323, 376, 379-381
  adding, 406-414
  port profiles, 429-439
verification
  active zonesets, 371
  advertised networks, 148
  BGP
    authentication, 144
    configuration, 151
    peer templates, 146
  broadcast storms, 253
  CTS, 227
  DAI, 249
  DHCP snooping, 245
eBGP neighbors, 143
EIGRP, 109
fabric module status and utilization, 286
fans, 282
GLBP configuration, 165
HSRP status, 155
HSRP, MD5 authentication, 157
keychain association and management, 252
Layer 2 forwarding, 48-49
load distribution, 86
MAC ACLs, 235
MST, 66, 68, 69
multicast storm control, 254
OSPF
  authentication, 129
  summarization, 121
ports
  profiles, 433
  security, 238
power redundancy, 280
PVLAN configuration, 58
RADIUS, 206
rate-limit settings, 267
redistributed routes, 133
redistribution, 111
Session Managers, 233
SSH, 222
static pinning, 41-45
STP, 62
stub routing, 107
supervisor redundancy, 285
systems
  image compatibility and impact, 299
  temperature, 283
totally stub status on neighbors, 126
VLAN configuration, 53-54
VRRP configuration, 160-161
verification FCoE, licenses, 366
versions, IGMP, 192
viewing
  BGP configurations, 152
MAC address tables, 49
monitor session configurations, 315
MST verification, 66
OSPF configurations, 136
VRRP, 161
violations, security, 240-242
virtual device contexts. See VDCs
Virtual Ethernet Module (VEM), 323, 376
virtual LANs. See VLANs
virtual machines. See VMs
Virtual Port Channels. See vPCs
virtual port channels, 39
Virtual Router Redundancy Protocol. See VRRP
virtual routing and forwarding (VRF), 28
virtual storage area network (VSAN), 318, 367
Virtual Supervisor Module. See VSM
virtualization, 1
  hosts, 78
  links, 79
VLAN Trunking Protocol. See VTP
VLANs (virtual LANs), 2, 37, 50-54
  ACL configuration, 236-237
  configuration, 50-51
  CTS, confirming, 228
  DAI, 247
  DHCP snooping, 244
  FCoE, 371
  membership, assigning, 52-53
  removing, 53
  SPAN, 317
  verification, 53-54
  VSM, 398
VMs (virtual machines), 376
VMware, 376

Kernel Port (vmk) ports, 327
vCenter Server, 396

vNetwork Distributed Switch. See vDS

volatile, 21
vPCs (Virtual Port Channels), 2, 37, 87-94

Peer-Gateway, 94

VPN Routing Forwarding (VRF), 4
VRF (virtual routing and forwarding), 28
VRF (VPN Routing Forwarding), 4
VRRP (Virtual Router Redundancy Protocol), 98, 152
configuration, 158-162
preemption, 160
priority, 160
secondary support, 162
security, 161

VSAN (virtual storage area network), 318, 367
VSD (XML Schema), 14
VSM (Virtual Supervisor Module), 327, 376
HA, 421-429
hostnames, modifying, 414-421
Nexus 1000V, 382-429

vSphere, 361-376
vSphere, ESX hosts, 406-414

VTP (VLAN Trunking Protocol), 51

W

warnings, 112, 134
wide-open redistribution, 132
WINS (Windows Internet Naming Services), 333
WireShark application, 229
withdraw options, 112, 135

X

XML (Extensible Markup Language), 14-16, 343
XML Schema (XSD), 14