



Cisco Networks

Engineers' Handbook of Routing, Switching,
and Security with IOS, NX-OS, and ASA

—
Second Edition
—

Chris Carthern
William Wilson
Noel Rivera

Apress®

Cisco Networks

Engineers' Handbook of Routing, Switching,
and Security with IOS, NX-OS, and ASA

Second Edition



Chris Carthern
William Wilson
Noel Rivera

Apress®

Cisco Networks: Engineers' Handbook of Routing, Switching, and Security with IOS, NX-OS, and ASA

Chris Carthern
Bangkok, Krung Thep, Thailand

William Wilson
FPO, AP, USA

Noel Rivera
APO, AE, USA

ISBN-13 (pbk): 978-1-4842-6671-7
<https://doi.org/10.1007/978-1-4842-6672-4>

ISBN-13 (electronic): 978-1-4842-6672-4

Copyright © 2021 by Chris Carthern and William Wilson and Noel Rivera

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

Trademarked names, logos, and images may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, logo, or image we use the names, logos, and images only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Aditee Mirashi
Development Editor: Matthew Moodie
Coordinating Editor: Aditee Mirashi

Cover designed by eStudioCalamar

Cover image designed by Freepik (www.freepik.com)

Distributed to the book trade worldwide by Springer Science+Business Media New York, 1 New York Plaza, Suite 4600, New York, NY 10004-1562, USA. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail booktranslations@springernature.com; for reprint, paperback, or audio rights, please e-mail bookpermissions@springernature.com.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at <http://www.apress.com/bulk-sales>.

Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub via the book's product page, located at www.apress.com/978-1-4842-6671-7. For more detailed information, please visit <http://www.apress.com/source-code>.

Printed on acid-free paper

This book is dedicated to Chadwick Boseman who was a real-life superhero who inspired generations to take up the mantle and make sure his legacy lives on through us. Wakanda Forever.

Table of Contents

About the Authors.....xxv

About the Technical Reviewerxxvii

Acknowledgmentsxxix

Introductionxxxi

■ **Chapter 1: Introduction to Practical Networking..... 1**

 Tools of the Trade 1

 Open Systems Interconnection (OSI) Model 3

 Physical Layer 7

 Data Link Layer 8

 Network Layer 9

 Transport Layer 10

 Connection-Oriented..... 10

 Session Layer 10

 Presentation Layer 11

 Application Layer..... 11

 The OSI Model: Bringing It All Together 12

 TCP/IP..... 13

 TCP/IP Application Layer..... 14

 TCP/IP Transport Layer 14

 TCP/IP Internet Layer 15

 TCP/IP Network Interface Layer..... 16

 Reliability 17

Three-Way Handshake and Connection Termination	18
User Datagram Protocol.....	19
Port Numbers	20
Types of Networks	21
Personal Area Network	21
Local Area Network	21
Campus Area Network	21
Metropolitan Area Network.....	21
Wide Area Network	22
Wireless Wide Area Network	22
Virtual Private Network.....	22
Hierarchical Internetwork Model	23
Software-Defined Networking Overview	24
Software-Defined Network Control Models	24
Summary	24
■ Chapter 2: The Physical Medium	27
Layer 1	27
Standards	28
Cables.....	29
Twisted Pair Cable	29
Coaxial Cable	31
Fiber-Optic Cabling	32
Fiber-Optic Transmission Rates	33
Wireless Communication	33
Ethernet.....	34
Duplex	34
Time Division Duplexing	35
Frequency Division Duplexing	35
Autonegotiation	35
Unidirectional Link Detection	37

Common Issues	37
Duplex Mismatch	37
Bad Connector Terminations	38
Summary	38
■ Chapter 3: Data Link Layer	39
Protocols	39
The Address Resolution Protocol (ARP)	39
The Reverse Address Resolution Protocol (RARP)	42
Link Layer Functions	42
Framing	42
Addressing	42
Synchronizing	43
Flow Control	43
Link Layer Discovery Protocol (LLDP)	44
Class of Endpoints	44
LLDP Benefits	45
Cisco Discovery Protocol (CDP)	48
Address Resolution Mapping on IPv6 Networks	52
Summary	57
■ Chapter 4: The Network Layer with IP	59
IP Addressing (Public vs. Private)	60
Public	60
Private	60
IPv4	60
Class A	61
Class B	61
Class C	61
IPv4 Packet Header	61

IPv6	63
IPv6 Addresses	63
IPv6 Packet Header.....	64
Classless Inter-Domain Routing	65
Subnetting.....	65
Subnet Mask.....	66
A Simple Guide to Subnetting.....	66
Variable-Length Subnet Masking	69
Classful Subnetting.....	71
VLSM Subnetting	71
Subnetting Exercises.....	72
Subnetting Exercise Answers.....	75
Exercise 1 Answers	75
Exercise 2 Answers	75
Exercise 3 Answers	76
Exercise 4 Answers	76
Summary	77
■ Chapter 5: Intermediate LAN Switching	79
Cisco Console Access.....	79
Configuration Help	82
Displaying the Running Configuration	83
Configuring the Router	84
Switching	86
Link Aggregation Group (LAG)	86
Spanning Tree Protocol	91
Why Do You Need STP?.....	91
How STP Works	91
Bridge Protocol Data Units.....	92
Rapid Spanning Tree Protocol.....	93

Virtual Logical Network (VLAN).....	96
VLAN Configuration.....	97
IOU1 Configuration.....	98
Trunking	103
Trunk Configuration	105
Routing Between VLANs	107
Routing VLAN Configurations.....	108
VLAN Trunking Protocol	109
VTP Modes.....	109
VTP Pruning	110
VTP Configuration	110
Multiple Spanning Tree Protocol.....	113
MSTP Configuration.....	115
Summary.....	121
Exercises	121
Exercise Answers	127
Exercise 1	127
Exercise 2	128
Exercise 3	129
Exercise 4	130
Exercise 5	134
Exercise 6	136
■ Chapter 6: Routing.....	141
Static Routing.....	141
The Process of Routing.....	142
Default Routing	146
Testing Connectivity.....	146
Dynamic Routing Protocols	148
Distance-Vector Routing Protocol.....	149
Link-State Routing Protocol.....	149
Hybrid Routing Protocol.....	150

RIP	150
RIP Configuration	150
Authentication	152
EIGRP	156
OSPF	162
Configuring OSPF	166
Router ID	171
IS-IS	172
IS-IS Addressing	173
IS-IS Configuration	173
Link-State Packet Database	177
Authentication	179
Passive Interfaces	182
IS-IS Adjacency	183
BGP	183
BGP Configuration	184
Administrative Distance	189
RIP	189
EIGRP	190
OSPF	190
IS-IS	191
BGP	191
Summary	191
Exercises	192
Exercise Answers	195
Exercise 1	195
Exercise 2	197
Exercise 3	200
Exercise 4	202
Exercise 5	207
Exercise 6	208

■ Chapter 7: Introduction to Tools and Automation.....	211
Tools Overview	211
Introduction to Prime Infrastructure	211
Hands-On Experience and Limitations	213
Introduction to Identity Services Engine	214
Introduction to Software-Defined WAN and vManage	214
Introduction to Digital Network Architecture	215
Introduction to Application Centric Infrastructure	216
Vendor-Agnostic Automation Tools	217
Summary	217
■ Chapter 8: Basic Switch and Router Troubleshooting	219
Troubleshooting	219
Documenting Your Network	219
First Things First: Identify the Problem	220
Physical Medium and Ethernet	222
VLANs and Trunks	225
EtherChannel	229
VTP	232
Spanning Tree	234
Routing	237
Static Routing	237
Dynamic Routing	240
Summary	268
Exercises	268
Exercise Answers	275
Exercise 1	275
Exercise 2	276
Exercise 3	279
Exercise 4	282

Exercise 5	284
Exercise 6	286
Exercise 7	288
■ Chapter 9: Network Address Translation and Dynamic Host Configuration Protocol.....	291
NAT	291
Static NAT	292
Dynamic NAT	293
Port Address Translation (PAT)	294
DHCP	296
DHCP Process	297
Setting Up a Router As a DHCP Client.....	297
Setting Up a Router to Send a Request to a DHCP Server	298
Setting Up a RouterAs a DHCP Server	299
Summary	301
Exercises	301
Exercise Answers	303
Exercise 1	303
Exercise 2	304
Exercise 3	306
Exercise 4	307
■ Chapter 10: Management Plane	309
The Management Plane Defined	310
Authentication and Authorization Basics.....	310
User Accounts.....	313
Password Recovery	314
Banners	317
Management Sessions	318
Telnet	318
SSH.....	319
Console and Auxiliary Lines.....	321

Disabling Services	321
Disabled Services	321
Disabled Services on Interfaces	322
Authentication, Authorization, and Accounting (AAA)	322
RADIUS	323
TACACS+	330
Certificate-Based Authentication and Authorization	334
Monitoring/Logging	338
Simple Network Management Protocol	339
Syslog	342
Prime Infrastructure Overview	344
Introduction to Netconf	346
Exercises	346
Exercise Answers	347
Exercise 1	347
Exercise 2	348
Exercise 3	348
Summary	348
■ Chapter 11: Data Plane	349
Traffic Protocols	349
Filters and Introduction to Data Plane Security	351
State Machines	354
Stateful Protocols	358
Stateless Protocols	362
NetFlow and sFlow	363
Exercises	369
Summary	371

■ Chapter 12: Control Plane	373
Layer 2	373
Layer 2 and 3 Interaction.....	376
Routing Protocols	377
Interior Gateway Protocols	377
Exterior Gateway Protocols.....	394
Protocol-Independent Multicasting	401
Domain Name System.....	405
Network Time Protocol	408
Tools for Control Plane Management	412
Exercises	416
Preliminary Work	416
OSPF	417
BGP	418
NTP	419
Exercise Answers	419
Preliminary Configurations	420
OSPF	424
BGP	427
NTP	432
Named Mode EIGRP with Authentication	434
Multicast.....	436
Summary	438
■ Chapter 13: Introduction to Availability	439
High Availability	439
Layer 3 Multipathing	440
First Hop Redundancy Protocol (FHRP)	441
HSRP	441
VRRP	445
GLBP	447

Multilinks.....	451
Availability Exercises.....	453
Exercise Answers	455
Exercise 1	455
Exercise 2	457
Exercise 3	458
Summary	461
■ Chapter 14: Advanced Routing	463
EIGRP	463
Unicast.....	464
Summarization	464
Load Balancing	465
EIGRP Stub.....	465
Traffic Engineering with EIGRP	465
Authentication	466
Multiarea and Advanced OSPF	467
Summarization	468
OSPF Stub.....	469
Cost Manipulation.....	469
OSPF Virtual Link	470
Authentication	472
Policy-Based Routing Using Route Maps	472
Redistribution	475
RIP Redistribution Overview	476
EIGRP Redistribution Overview.....	476
OSPF Redistribution Overview	478
BGP Redistribution Overview	479
Avoiding Loops and Suboptimal Routing.....	480

BGP	481
Address Families	481
Peer Groups and Templates	481
Dynamic Neighbors	484
Next Hop Issues with iBGP	486
Anycast	486
Traffic Engineering with BGP	487
IPv6 Routing	489
EIGRPv6	491
OSPFv3	494
DHCPv6	496
NAT and IPV6	499
GRE Tunnels	504
BGP Issues	506
IPsec	506
Router8 Configuration	509
Router9 Configuration	511
IKEv2	512
Summary	525
Advanced Routing Exercises	525
Exercise 1: EIGRP and OSFP Redistribution	525
Exercise 2: GRE and IPSEC	525
Exercise 3: IKEv2	526
Exercise 4: BGP	526
Exercise 5: IPv6 OSPF and EIGRP Redistribution	527
Exercise Answers	528
Exercise 1	528
Exercise 2	529
Exercise 3	532
Exercise 4	534
Exercise 5	536

■ Chapter 15: QoS	541
Intro to QoS	541
Classifications and Markings	543
Policing and Shaping.....	554
QoS on Tunnels and Subinterfaces.....	577
IPv6 QoS	577
QoS Design Strategies.....	579
Exercise.....	581
■ Chapter 16: Advanced Security	583
Private VLANs	584
Use Case	584
Promiscuous vs. Community vs. Isolated	584
Configuration	585
Using Access Lists.....	586
Extended ACL.....	586
VACL.....	588
PACL	589
ARP and DHCP Snooping	590
Identity Services Engine.....	595
ISE and 802.1x.....	595
AAA	619
Advanced Security Exercises	627
Exercise 1: Extended ACL Exercises	627
Exercise 2: AAA Exercises.....	628
Exercise Answers	628
Exercise 1	628
Exercise 2	629
Summary.....	630

■ Chapter 17: Advanced Troubleshooting	631
Access Control List.....	631
VACL	634
PACL	635
Network Address Translation.....	635
Static NAT	636
Dynamic NAT	641
Overload	645
HSRP, VRRP, and GLBP	646
HSRP	647
VRRP	649
EIGRP	651
OSPF.....	655
BGP.....	658
Neighbor Relationships.....	658
Missing Prefixes	660
Route Redistribution.....	665
EIGRP	665
OSPF	668
GRE Tunnels.....	671
Recursive Routing.....	673
IPsec.....	674
Transform Mismatch.....	675
Key Mismatch	679
IPv6	680
Summary.....	689
Advanced Troubleshooting Exercises	689
Router1 Configuration.....	695
Router2 Configuration.....	696

Exercise Answers	697
Exercise 1	697
Exercise 2	699
Exercise 3	702
■ Chapter 18: Effective Network Management.....	705
Sample Network.....	705
Logs.....	706
Simple Network Management Protocol.....	708
Service-Level Agreements and Embedded Event Manager	715
sFlow and NetFlow Tools.....	718
Intrusion Detection and Prevention Systems	719
Management and Design of Management Data	722
Exercises	726
Syslog	726
SNMP	727
Service Policy	727
Exercise Answers	727
Initial Configuration	727
Syslog	728
SNMP	729
Service Policy	729
Summary	730
■ Chapter 19: Data Center and NX-OS	731
Fabric Design	731
NX-OS.....	732
NX-OSv	734
VLAN	735
Configuring a Non-routed VLAN.....	735
Configuring a VLAN As a Routed Switched Virtual Interface (SVI).....	735
VLAN Trunking Protocol	736

Nexus Routing	737
EIGRP	737
OSPF	741
BGP	745
Virtual Routing and Forwarding Contexts	747
Port Channels	751
Virtual Port Channels	757
Port Profiles	759
FEX	759
First Hop Redundancy Protocols	760
HSRP	760
VRRP	762
Nexus Security	763
Local User Accounts	764
TACACS+	765
Control Plane Policing	767
Network Virtualization	768
Virtual Device Context (VDC)	768
Overlay Transport Virtualization	768
Virtual Extensible LANs Overview	771
Application Centric Infrastructure Overview	772
NX-OS Exercise	772
Exercise Answer	773
Summary	775
■ Chapter 20: Wireless LAN (WLAN)	777
Wireless LANs (WLANs)	777
Wireless Standards	777
Wireless Components	778
Wireless Access Points	778
Wireless Controllers/Switches	778

Installing a WLAN	778
Wireless Site Survey.....	779
Access Point Installation.....	779
Access Point Configuration.....	780
WLAN Controller Installation.....	780
WLAN Controller Configuration	780
Security	792
Encryption and Authentication.....	792
Cisco ISE.....	795
Cisco ISE and WLAN.....	795
Wireless Setup Wizard	797
Hotspot Wizard	802
BYOD Wizard	806
Cisco Prime	811
Wireless Network Monitoring	814
Prime Infrastructure Maps.....	817
Prime Infrastructure Configuration	822
Threats and Vulnerabilities	825
Summary	826
Wireless Exercise	826
Exercise Answers	827
Exercise 1	827
■ Chapter 21: Firepower	835
Testing Policies in a Safe Environment	835
Management Access and Configuration.....	836
Initial Setup	836
Objects Overview.....	846
Device Configuration Overview.....	847
System Configuration and Platform Settings.....	879
External Authentication	882

Monitoring Overview	887
Management Console	887
Remote Syslog.....	889
eStreamer.....	891
Health Policies.....	893
Access Policies.....	895
Baselining and Discovery	895
Access Policy Basics	896
Application-Based Rules.....	901
Intrusion Policies Introduction	902
Intrusion Policy Tuning	904
Virtual Private Networks.....	909
Site to Site	909
Remote Access	919
Troubleshooting.....	928
Summary.....	932
■ Chapter 22: Introduction to Network Penetration Testing	933
Overview	933
Reconnaissance and Scanning	933
Vulnerability Assessment.....	938
Exploitation.....	942
The Human Factor	949
Summary.....	950
■ Chapter 23: Multiprotocol Label Switching	951
Multiprotocol Label Switching Basics	951
Label Protocols	962
LDP Security and Best Practices	964
LDP Verification	967

Layer 3 MPLS VPN	969
Site-to-Site VPN	972
Shared Extranet	984
Leaking Prefixes	988
Layer 2 MPLS VPN	990
IPv6 over MPLS	1000
Exercises	1003
MPLS Backbone	1003
Site-to-Site VPN	1004
Leak to CustomerB	1004
Tunneling IPv6	1005
Exercise Answers	1005
MPLS Backbone	1006
Site-to-Site VPN	1008
Leak to CustomerB	1011
Tunneling IPv6	1013
Summary	1016
■ Chapter 24: DMVPN	1017
DMVPN	1017
Phase 1	1018
Phase 2	1022
Phase 3	1025
Phase 3 with IPsec	1028
Phase 3 with OSPF	1029
FlexVPN	1031
Single-DMVPN Dual Hub	1034
Dual-DMVPN Dual Hub	1038
Summary	1043

DMVPN Exercises	1043
Exercise 1: DMVPN Phase 3 with BGP	1043
Exercise 2: IPsec.....	1043
Exercise 3: FlexVPN	1044
Exercise Answers	1044
Exercise 1: DMVPN Phase 3 with BGP	1044
Exercise 2: IPsec.....	1047
Exercise 3: FlexVPN	1048
■ Index.....	1053

About the Authors



Chris Carthern is a senior network engineer with 15 years of experience in the network engineering field. He is responsible for designing, implementing, and maintaining wide area and campus area networks. Carthern obtained his BS (honors) in computer science from Morehouse College and his MS in systems engineering from the University of Maryland, Baltimore County (UMBC). He holds the following certifications: Cisco Certified Network Professional (CCNP), Certified Information Systems Security Professional (CISSP), and Brocade Certified Network Professional (BCNP).



Dr. William Wilson is a senior network consulting engineer. He specializes in the optimization of routing and in security. He is responsible for assisting customers with resolving complex architectural and operation issues. He holds a bachelor's degree in mathematics from the University of Colorado. His doctorate is in computer science with a focus on applications of artificial intelligence in information security. He maintains the following certifications: CCIE Routing and Switching, CCIE Security, all of the CCNP tracks, Cisco DevNet Professional, VCP-NV, Certified Ethical Hacker, CISSP, MCSE, and PMP.

Noel Rivera is a systems architect with CACI who specializes in communications networks, IT security, and infrastructure automation. He has worked at NASA, DoD, Lockheed Martin, and CACI. Mr. Rivera holds a bachelor's degree in electrical engineering from the University of Puerto Rico at Mayaguez and two master's degrees, one in electrical engineering and another in computer science, from Johns Hopkins University. Mr. Rivera holds the following certifications: Cisco Certified Internetwork Expert in Routing and Switching (CCIE-RS), Cisco Certified Internetwork Expert in Security (CCIE-SEC), Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), Juniper Networks Certified Service Provider Professional (JNCIP-SP), Juniper Networks Certified Cloud Professional (JNCIP-Cloud), VMWare Certified Data Center Virtualization Professional (VCP-DCV), VMWare Certified Network Virtualization Professional (VCP-NV), and ITILv3. He is currently working on his Juniper Networks Certified Service Provider Expert certification (JNCIE-SP) and Microsoft Azure Solutions Architect Expert certification.

About the Technical Reviewer

Marc Julian has graduated from the University of Maryland, Baltimore County, with a Bachelor of Science in information systems. He is currently working at Cisco Systems Inc. as a network consulting engineer. He is CompTIA Network+ certified, CCNA R&S certified, and CCNP R&S certified. He will continue to work on receiving IT certifications such as Cisco certifications, MCSE certifications, and CWNA certifications.

Acknowledgments

Special thanks to my coauthors for your contributions to this book. I'm extremely grateful to my parents, Taylor and Lisa, and sister, Breanna, for all the support you have given me and the importance you placed on higher education. To my best friend, Tony Aaron II, I would like to express my deepest appreciation for the endless support. Thanks should also go to our technical reviewer, Marc Julian, for all the feedback on the content and exercises in the book; this book is better because of your diligent reviews. Lastly, I very much appreciate my publisher, Apress, for valuing our first edition and trusting us to complete a second. For anyone I missed, thank you all for your support and helping me become a better engineer.

—Chris Carthern

Introduction

Cisco Networks, Second Edition is a practical guide and desk reference for Cisco engineers. For beginning and experienced network engineers tasked with building LAN (local area network), WAN (wide area network), and data center connections, this book lays out clear directions for installing, configuring, and troubleshooting networks with Cisco devices. What is new in this edition includes discussions about software-defined (SD) networks and building Dynamic Multipoint VPNs (DMVPNs) using IPsec (Internet Protocol Security) Virtual Private Networks (VPNs). A new chapter on Quality of Service (QoS) has been added to teach managing network resources by prioritizing specific types of network traffic. The second edition has an updated wireless section which focuses on an updated controller and integration with Cisco Identity Services Engine (ISE) and Cisco Prime Infrastructure. The Cisco Firepower Next-Generation Firewall (NGFW) will also be covered. The emphasis throughout is on solving the real-world challenges engineers face in configuring network devices, rather than on exhaustive descriptions of hardware features.

This practical desk companion doubles as a comprehensive overview of the basic knowledge and skills needed by CCNA and CCNP exam takers. It distills a comprehensive library of cheat sheets, lab configurations, and advanced commands that the authors assembled as senior network engineers. Prior familiarity with Cisco routing and switching is desirable but not necessary, as the authors start their book with a review of network basics and move on to configuring routers and switches from a beginner level. The purpose of this book is to provide a practical guide for network engineers who work with Cisco devices on a daily basis. This book is not a Cisco certification guide, but you will learn key concepts that will be on exams to include the CCNA and CCNP. This book intends to be a day-to-day reference for the daily tasks you perform as a network engineer.

This book will cover advanced topics such as configuring wireless networks, securing your networks, and covering best practices. Learn how to strengthen your networks with VPNs and security devices and deployment using Cisco Identity Services Engine (ISE). By the end of the book, you will have mastered deploying Cisco networks.

CHAPTER 1



Introduction to Practical Networking

This chapter begins by discussing a few of the tools that you will use throughout the book. Next, we cover the OSI (Open Systems Interconnection) model and discuss how it relates to networking. We talk about all seven layers of the OSI model. Then we move on to the TCP/IP model and show its relation to the OSI model. We end the chapter discussing well-known port numbers, the different types of networks, and Cisco's hierarchical internetwork model.

So you want to become a good network engineer? Let us give you some advice: do not believe that you know everything there is to know about networking. No matter what certifications or years of experience you have, there will always be gaps in knowledge and people who know or have experienced issues that you may not have. Troubleshoot issues systematically from layer to layer. Use your resources—such as this book! You can never have too many resources at your disposal in your toolbox. Do not be afraid to ask for help. Do not be ashamed because you cannot resolve a problem. That is why we have teams of engineers. Everyone has their expertise, and we must use each to our advantage. Remember when dealing with networks, it is always better to have a second pair of eyes and another brain to help resolve issues quickly. This will help you save time and stop you from working in circles. You want to know how you can become a good network engineer? Start by reading this book and complete the lab exercises to reinforce what you have learned. The rest will come from experience on the job. Practice makes perfect!

Tools of the Trade

The best way to learn is by doing, and the best way to remember is by repetition. In order to learn real-life network designs and issues, it is best to have a lab. You can have a real or a virtual lab; however, it is more cost effective to have a virtual lab. In modern times, almost all vendors have implementations of their devices in virtual machines (VMs), many of them with significant trial periods that allow you to learn the basics of the technology. However, if you or your organization can afford, it is always best to have a lab with real physical devices since virtual devices have limitations or do not implement all features of the real physical devices.

To become proficient at anything, practice is needed, and to be efficient, tools are needed. Our tool of choice to practice and simulate network topologies is the Emulated Virtual Environment Next Generation, or EVE-NG for short. The reason why EVE-NG is our tool of choice is its clientless approach and HTML-based user interface. EVE-NG supports a wide range of virtual machine templates for fast virtual machine editing and instantiation, Docker containers, HTML5 device console, and VNC/RDP display over a VNC/RDP client or via HTML5; and it's a multiuser environment with independent pods per user and user teaming possibilities. Additionally, Wireshark is integrated into EVE-NG to facilitate packet captures (PCAPs) and

protocol studies. If you run EVE-NG on a dedicated server, you can access your lab on the go and interact with the devices via the HTML5 console or the HTML5 thin client desktop; alternatively, you can VPN into your network for a native console feel. Figure 1-1 displays an example network using EVE-NG.

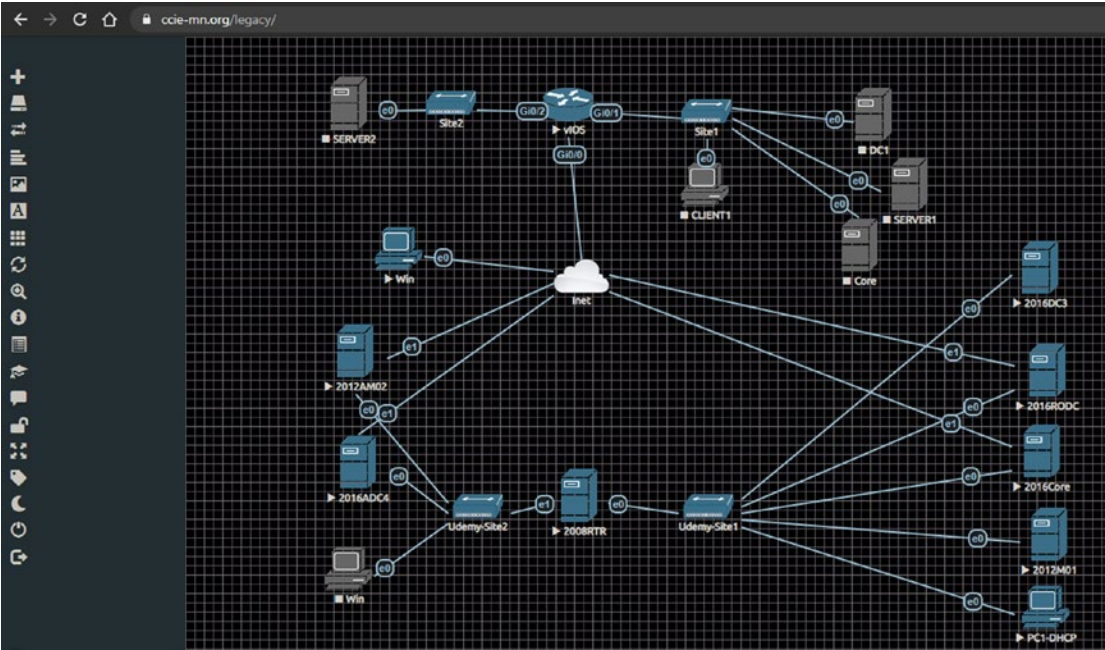


Figure 1-1. EVE-NG web-based UI

Another great simulation environment tool is the Graphical Network Simulator-3 (GNS3), and our tool of choice to peek into the network packets is Wireshark. There are other tools that you can use, but we found these two to be the easiest and most straightforward. Just in case you want to look at other options, a quick Internet search for “network simulators” and “network sniffers” will provide a list of the available alternatives to GNS3 and Wireshark, respectively.

GNS3 provides a simple all-in-one distribution that integrates Wireshark, VirtualBox, Qemu, and Dynamips among other tools, allowing simulation of network devices and virtualized workstations or servers. A simple visit to www.gns3.com and www.wireshark.org or a search on YouTube will glean vast amounts of information on how to use the tools. You need to be able to get an IOS (Internetwork Operating System) image; do not violate any license agreements. We will use GNS3 and Wireshark exclusively throughout this book.

Cisco Packet Tracer is a network simulation tool that allows you to simulate the configuring, operation, and troubleshooting of network devices. For more information, visit www.netacad.com/web/about-us/cisco-packet-tracer.

Cisco Virtual Internet Routing Lab (VIRL) is a network simulation tool that uses virtual machines running the same IOS as Cisco’s routers and switches. It allows you to configure and test real-world networks using IOS, IOS-XE, IOS-XR, and NX-OS. For more information, visit <http://virl.cisco.com>. For the 1.x branch of the application, VIRL was the name of the personal product, and Cisco Modeling Labs (CML) was the corporate version. In version 2.0, the names were merged, and VIRL is being renamed to CML Personal Edition. CML 2.0 Personal Edition is a significant improvement over VIRL 1.x. It replaced the thick client with an HTML5 interface and made several efficiency updates. It is available at <https://learningnetworkstore.cisco.com/cisco-modeling-labs-personal/cisco-cml-personal>.