



ICND2

Curriculum

200-105

Interconnecting Cisco Networking Devices Part 2
Version 3.0

Labs powered by



Interconnecting Cisco Networking Devices Part 2

200-105 Curriculum

Boson[®] NetSim

NETWORK SIMULATOR

25 Century Blvd., Ste. 500, Nashville, TN 37214 | Boson.com

The labs referenced in this book have been printed in the Boson Lab Guide, which is included with the purchase of the curriculum. These labs can be performed with real Cisco hardware or in the Boson NetSim Network Simulator version 9 or later. To learn more about the benefits of using NetSim or to purchase the software, please visit www.boson.com/netsim.

Copyright © 2016 Boson Software, LLC. All rights reserved. Boson, Boson NetSim, Boson Network Simulator, and Boson Software are trademarks or registered trademarks of Boson Software, LLC. Catalyst, Cisco, and Cisco IOS are trademarks or registered trademarks of Cisco Systems, Inc. in the United States and certain other countries. Media elements, including images and clip art, are the property of Microsoft. All other trademarks and/or registered trademarks are the property of their respective owners. Any use of a third-party trademark does not constitute a challenge to said mark. Any use of a product name or company name herein does not imply any sponsorship of, recommendation of, endorsement of, or affiliation with Boson, its licensors, licensees, partners, affiliates, and/or publishers.

Module 1: Cisco Device Management.....	1
Overview.....	2
Objectives.....	2
Understanding the IOS Boot Process.....	3
Loading IOS Images.....	4
Changing the IOS Image Load Location.....	5
Upgrading IOS.....	6
Troubleshooting IOS Upgrades.....	7
Understanding and Modifying the Configuration Register.....	8
Using the Configuration Register for Password Recovery.....	10
Managing Configuration Files.....	12
Managing Licensing.....	13
Using SNMP to Manage Licenses.....	14
Review Question 1.....	15
Review Question 2.....	17
Lab Exercises.....	19
Module 2: Troubleshooting Networks.....	21
Overview.....	22
Objectives.....	22
Understanding the Systematic Approach.....	23
Understanding Troubleshooting Techniques.....	25
Understanding the OSI Model.....	25
Implementing the OSI Techniques.....	26
<i>The Bottom Up Troubleshooting Technique.....</i>	<i>26</i>
<i>The Top Down Troubleshooting Technique.....</i>	<i>26</i>
<i>The Divide and Conquer Troubleshooting Technique.....</i>	<i>27</i>
Implementing the Non-OSI Techniques.....	28
<i>The Follow the Path Troubleshooting Technique.....</i>	<i>28</i>
<i>The Move the Problem Troubleshooting Technique.....</i>	<i>28</i>
<i>The Spot the Difference Troubleshooting Technique.....</i>	<i>29</i>
Understanding show Commands.....	30
Understanding debug Commands.....	32
Understanding Syslog.....	33
Configuring Log Severity Levels.....	34
Understanding the ping Command.....	35
Understanding the tracert Command.....	37
Monitoring LAN Traffic with SPAN.....	39
Understanding IP SLAs.....	41
Configuring IP SLA Echo.....	42
Understanding SNMP.....	44
Configuring SNMP.....	45
Using SNMP Data.....	47
Understanding NetFlow.....	48
Using NetFlow Data.....	49

Content in these modules is available in the full version of the curriculum. Please visit www.boson.com for more information.

Configuring NetFlow	50
Verifying NetFlow.....	51
Analyzing NetFlow Data	54
Solving Common Network Problems.....	56
Troubleshooting Connectivity.....	57
Troubleshooting Physical Layer Connectivity	58
Troubleshooting Data Link Layer Connectivity.....	60
Troubleshooting Network Layer Connectivity	61
Network Addressing	62
IPv4 Connectivity	63
IPv6 Connectivity	64
Path Selection	65
InterVLAN Routing	68
Troubleshooting Beyond Layer 3	70
Troubleshooting Layer 4	71
Using Telnet to Troubleshoot Layer 4.....	72
Resolving Layer 4 Connectivity.....	73
Troubleshooting Beyond Layer 4	74
Review Question 1.....	77
Review Question 2.....	79
Review Question 3.....	81
Lab Exercises	83

Content in these modules is available in the full version of the curriculum. Please visit www.boson.com for more information.

Module 3: Network Addressing..... 85

Overview.....	86
Objectives	87
Understanding IPv4 Subnets	88
Understanding IPv4 Subnetting	89
Understanding VLSMs.....	90
Understanding IPv6 Addressing	93
IPv6 Address Composition.....	94
IPv6 Address Prefixes	95
IPv6 Address Types	96
IPv6 Address Configuration	98
EUI-64 Interface IDs	99
Review Question 1.....	101
Review Question 2.....	103
Lab Exercises	105

Module 4: VLANs and Trunking 107

Overview.....	108
Objectives	108
What Do VLANs Do?.....	109
Creating and Configuring VLANs	111
Verifying VLANs	112
Configuring Access Ports.....	113

Verifying VLAN Membership	114
Understanding Trunk Ports	115
Configuring Trunk Ports	117
Verifying Trunk Ports	119
Understanding the Voice VLAN	121
Configuring the Voice VLAN	123
Understanding and Configuring DTP	124
Common VLAN and Trunk Problems	126
Review Question 1	127
Review Question 2	129
Lab Exercises	131
Module 5: Spanning Tree Protocol.....	133
Overview.....	134
Objectives.....	134
Understanding STP	135
Root Switch Election	136
Verifying the Root Switch	139
Path Costs	142
Determining Port Costs	143
Root Port	143
Designated Port.....	143
STP Port States.....	144
STP Timers.....	145
Understanding RSTP	146
Differences Between STP and RSTP	147
Understanding RSTP Port States.....	149
RSTP Alternate and Backup Port Roles.....	150
Understanding Cisco Implementations of STP	151
Per-VLAN Spanning Tree Plus	152
PVST+ Bridge IDs.....	153
Per-VLAN Rapid Spanning Tree Plus.....	154
Multiple Spanning Tree Protocol.....	155
Cisco Enhancements to STP	156
PortFast.....	157
BPDU Guard	158
Loop Guard.....	159
Root Guard	160
Review Question 1	161
Review Question 2.....	163
Lab Exercises	165
Module 6: Advanced Switch Redundancy.....	167
Overview.....	168
Objectives.....	168
Understanding EtherChannel	169

Content in these modules is available in the full version of the curriculum. Please visit www.boson.com for more information.

Understanding EtherChannel Protocols.....	170
Understanding PAgP and LACP Modes.....	171
<i>The On Mode</i>	171
<i>PAgP Modes</i>	171
<i>LACP Modes</i>	172
Configuring EtherChannel	173
Configuring PAgP EtherChannel	175
Configuring LACP EtherChannel.....	176
Understanding EtherChannel's Effects on STP	177
Verifying EtherChannel.....	179
Troubleshooting EtherChannel	181
Aggregation Protocol Mismatches.....	181
Bundle Configuration Mismatches.....	183
Understanding Gateway Redundancy	184
Understanding HSRP	186
Understanding Virtual MAC Addresses	188
Configuring HSRP	189
Configuring Preemption and Interface Tracking.....	190
Configuring Multigroup HSRP	192
Configuring HSRP on EtherChannel.....	194
Understanding GLBP	196
Configuring GLBP.....	197
Configuring GLBP Options	198
Verifying GLBP	200
Review Question 1.....	203
Review Question 2.....	205
Lab Exercises	207

Content in these modules is available in the full version of the curriculum. Please visit www.boson.com for more information.

Module 7: Access Layer Security..... 209

Overview.....	210
Objectives	210
Establishing Written Security Policies.....	211
Securing Access.....	212
Restricting Physical Access to a Switch.....	213
Creating Secure Passwords for Console and Remote Access	214
ACL Review	215
<i>Configuring IPv4 ACLs to Control Remote Access</i>	216
<i>Configuring IPv4 ACLs to Control Interface Access</i>	217
<i>Configuring IPv6 ACLs to Control Remote Access</i>	219
<i>Configuring IPv6 ACLs to Control Interface Access</i>	220
Creating a Secure Password for Privileged EXEC Mode Access	221
Encrypting Passwords on the Switch	222
Disabling or Replacing Vulnerable Services	223
Securing Vulnerable Services	225
Configuring Warning Banners	226
Securing Switch Ports	227

Disabling Unused Ports.....	228
Securing Trunk and Access Ports.....	229
Restricting Ports by Client MAC Address.....	230
Verifying Port Security.....	233
Understanding 802.1X Port-based Authentication.....	235
<i>How 802.1X Port-based Authentication Works</i>	236
<i>Configuring 802.1X Port-based Authentication</i>	237
Authenticating with AAA.....	238
RADIUS vs. TACACS+.....	239
Configuring AAA.....	240
Configuring RADIUS.....	241
Configuring TACACS+.....	243
Securing VLAN 1.....	245
Securing VTP.....	246
Securing Spanning Tree Protocol.....	249
Configuring Root Guard.....	250
Configuring BPDU Guard.....	251
Logging.....	252
Configuring Accurate Time.....	253
Configuring Log Severity Levels.....	254
Configuring and Using a Logging Server.....	255
Review Question 1.....	257
Review Question 2.....	259
Lab Exercises.....	261
Module 8: Routing Fundamentals.....	263
Overview.....	264
Objectives.....	264
Understanding Router Path Selection.....	265
Layer 3 Forwarding.....	266
Understanding Static Routes.....	267
Understanding IPv6 Static Routes.....	269
Understanding Dynamic Routes.....	270
Understanding AD.....	271
Understanding Routing Metrics.....	273
Understanding Autonomous Systems.....	274
Understanding Routing Protocols.....	275
Understanding the Types of IGPs.....	276
Understanding Distance-Vector Routing Protocols.....	277
Learning Distance-Vector Routes.....	278
Updating Distance-Vector Routes.....	279
Preventing Distance-Vector Problems.....	280
Understanding the Counting to Infinity Problem.....	281
<i>Understanding Maximum Counts</i>	283
Understanding Routing Loops.....	284
<i>Preventing Routing Loops</i>	285

Content in these modules is available in the full version of the curriculum. Please visit www.boson.com for more information.

Understanding Link-State Routing Protocols	286
Understanding Link-State Relationships	287
Understanding the LSDB	288
Learning Link-State Routes	289
Understanding Passive Interfaces	290
Review Question 1	293
Review Question 2	295
Lab Exercises	297
Module 9: EIGRP Configuration	299
Overview	300
Objectives	300
Understanding EIGRP	301
Understanding EIGRP Router IDs	302
Understanding EIGRP Adjacencies	303
Configuring Hello and Hold Timers	304
Understanding EIGRP Path Selection	305
Understanding Advertised Distance and Feasible Distance	308
Understanding EIGRP Tables	310
Configuring EIGRP	312
Verifying and Troubleshooting EIGRP	314
Understanding EIGRP Load Balancing	316
Using Variance to Load Balance EIGRP	317
Understanding EIGRP Route Summarization	319
Review Question 1	321
Review Question 2	323
Review Question 3	325
Review Question 4	327
Lab Exercises	329
Module 10: OSPF Configuration	331
Overview	332
Objectives	333
Understanding OSPF	334
Understanding OSPF Areas	336
Understanding Nonbackbone Areas	337
Understanding Single-Area and Multiarea Configurations	338
Understanding OSPF Router Roles	339
Autonomous System Boundary Routers	339
Area Border Routers	339
Backbone and Nonbackbone Routers	340
Choosing Between OSPF and EIGRP	341
Configuring OSPF	342
Configuring Single-Area OSPFv2	343
Configuring Multiarea OSPFv2	343
Configuring Areas in OSPFv3	344

Content in these modules is available in the full version of the curriculum. Please visit www.boson.com for more information.

Verifying OSPF	345
Understanding OSPF Router IDs	347
Understanding OSPF Adjacencies	348
Understanding DR and BDR Elections	350
Understanding the LSDB	351
Verifying OSPF Adjacencies	353
Verifying OSPF Link States	356
Troubleshooting OSPF Adjacencies	357
Using Cost to Load Balance OSPF	359
Review Question 1	363
Review Question 2	365
Review Question 3	367
Lab Exercises	369
Module 11: PPP WANs	371
Overview	372
Objectives	372
Implementing PPP	373
Establishing PPP Links	374
Configuring PPP on an Interface	375
Configuring PPP Authentication	377
Configuring Router Host Names, User Names, and Passwords	378
Configuring PAP Authentication	379
Configuring CHAP Authentication	381
Configuring PAP and CHAP on the Same Interface	382
Implementing MLP	383
Creating a Multilink Bundle	384
Verifying a Multilink Bundle	385
Implementing PPPoE	386
How PPPoE Works	387
Configuring PPPoE	389
Verifying PPPoE	390
Review Question 1	391
Review Question 2	393
Lab Exercises	395
Module 12: eBGP Configuration	397
Overview	398
Objectives	398
Understanding BGP	399
Autonomous Systems	400
eBGP vs. iBGP	401
Single-Homed, Dual-Homed, and Multihomed ASes	402
Path-Vector Algorithm	404
Configuring Single-Homed eBGP	406
Creating a BGP Routing Process	407

Content in these modules is available in the full version of the curriculum. Please visit www.boson.com for more information.

Specifying Local Networks to Advertise.....	408
Configuring Peer Information.....	409
Verifying Single-Homed eBGP.....	410
Examining the Local BGP Configuration.....	410
Examining the BGP Routing Process.....	411
Examining Detailed Peer Information.....	411
Examining BGP Routing Information.....	412
Examining BGP Routes.....	413
Review Question 1.....	415
Review Question 2.....	417
Review Question 3.....	420
Lab Exercises.....	423
Module 13: Secure VPNs and Tunneling.....	425
Overview.....	426
Objectives.....	426
Understanding the Purpose of a VPN.....	427
The Two Types of VPNs.....	428
Understanding Site-to-Site VPNs.....	429
Understanding Remote Access VPNs.....	431
Understanding the IPSec Protocol.....	433
IPSec Data Integrity Methods.....	435
IPSec Authentication Methods.....	436
Understanding GRE Tunnels.....	437
Differences Between Secure VPNs and GRE Tunnels.....	438
Configuring GRE Tunnels.....	439
Verifying GRE Tunnels.....	443
Review Question 1.....	445
Review Question 2.....	447
Review Question 3.....	449
Review Question 4.....	451
Lab Exercises.....	453
Module 14: Intelligent Networks.....	455
Overview.....	456
Objectives.....	457
Understanding Cloud Computing.....	458
Cloud Computing Benefits.....	459
Infrastructure as a Service.....	460
Platform as a Service.....	461
Software as a Service.....	462
Understanding SDNs.....	463
Understanding the SDN Planes.....	464
Understanding Cisco APIC.....	465
The Northbound API.....	466

Content in these modules is available in the full version of the curriculum. Please visit www.boson.com for more information.

Cisco Intelligent WAN.....	467
The Southbound API.....	468
Understanding Switch Stacking.....	469
Connecting StackWise Cables.....	470
Understanding the Stack Master.....	471
Review Question 1.....	473
Review Question 2.....	475
Review Question 3.....	477
Module 15: Quality of Service	479
Overview.....	480
Objectives.....	480
Network Traffic	481
Voice Traffic.....	482
Video Traffic	484
Data Traffic.....	485
Understanding Congestion	486
Normal Traffic Flow	487
Buffers and Memory Pools.....	488
Congested Traffic Flow.....	489
Traffic Classification and Marking.....	490
Policing and Shaping (Pre-ICND2).....	491
Understanding Marking	493
Congestion Management.....	494
Queuing Mechanisms.....	495
Scheduling Mechanisms	497
Congestion Avoidance.....	498
Policing and Shaping	500
Review Question 1.....	501
Review Question 2.....	503
Review Question 3.....	505
Index	507

Content in these modules is available in the full version of the curriculum. Please visit www.boson.com for more information.

Module 1

Cisco Device Management

Cisco Device Management Overview

- Boot process
- Configuration register
- Managing files
- Licensing
- Backing up
- Recovering



Overview

You can configure and manage Cisco devices by using the IOS software that ships with the devices. It is important to understand the process each device goes through, from the initial startup of a device to backing up its running configuration; each process is an important contribution toward ensuring an efficiently managed network. As a network evolves, this understanding will assist you as you make necessary changes to the configuration so that optimal configuration and peak performance of the network are consistently achieved.

In this module, you will learn about the basics of Cisco IOS as well as the options for configuring and managing the IOS on a device. You will also learn about how to install and manage licensing on Cisco devices.

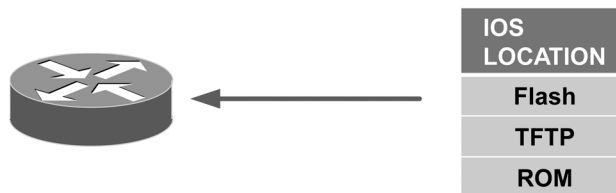
Objectives

After completing this module, you should have the basic knowledge required to complete all of the following tasks:

- Understand the boot process for Cisco devices.
- Understand and modify the configuration register.
- Manage IOS image files and configuration files.
- Activate, install, back up, and uninstall Cisco software licenses.

Understanding the IOS Boot Process

- Loading IOS images
- Changing the IOS image load location
- Upgrading IOS



Understanding the IOS Boot Process

When a Cisco device is started, it performs the following actions:

1. The device performs power-on self test (POST) checks.
2. The bootstrap program is loaded and executed.
3. The bootstrap program loads an IOS image.
4. The IOS loads a configuration file from non-volatile random access memory (NVRAM) and places it into dynamic random access memory (DRAM) for operation; if no configuration file is present, the device starts the System Configuration Dialog.
5. The device is placed in user EXEC mode.

This section covers the details of step 3, loading an IOS image. For a Cisco device to function, it must be able to load an IOS image. These images can be stored locally in flash memory or remotely on a network server; in addition, a limited IOS image is stored in read-only memory (ROM) and will be used if a full IOS image cannot be found.

Loading IOS Images

- Images can be loaded from:
 - Flash memory
 - A TFTP server
- By default, images will be loaded from flash memory
- Devices can be configured to load images from a TFTP server

Loading IOS Images

A full version of the Cisco IOS can be loaded at startup from flash memory or from a Trivial File Transfer Protocol (TFTP) server. The Cisco IOS is normally located in flash memory. If the flash memory is empty or the file system is corrupt, you will receive an error message stating `boot: cannot open "flash:"`.

By default, when a Cisco device is unable to locate a valid Cisco IOS image in flash memory during the boot process, it will attempt to locate a valid IOS image on a TFTP server on the local network. If it cannot locate a TFTP server, it will enter ROM monitor (ROMmon) mode. When a router enters ROMmon mode, the `rommon>` prompt will be displayed instead of the standard prompt that is displayed on devices that are properly configured. The device will then load a limited version of the IOS from ROM.

ROM does not contain a full version of the Cisco IOS. The boot image loaded from ROM will enable you to download a valid IOS image from a specific TFTP server. To load a boot image while the router is in ROMmon mode, you should issue the **confreg 0x2101** command from the `rommon>` prompt. Then you should issue the **reset** command to force the router to boot to the boot image. You can then configure one of the device's local area network (LAN) interfaces to connect to a network containing a TFTP server that stores a valid IOS image.

After downloading the IOS image, you should change the configuration register setting back to 0x2102, which will enable the router to boot to the new IOS image.

Changing the IOS Image Load Location

- The **boot system** command is used to change the IOS load location
- Load from flash:
 - **boot system flash** *[filename]*
- Load from TFTP:
 - **boot system tftp** *filename [ip-address]*
- Load from ROM:
 - **boot system rom**

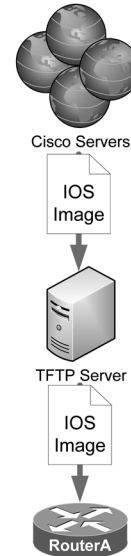
Changing the IOS Image Load Location

You can modify where a Cisco device loads the IOS from by issuing the **boot system** command. The **boot system flash** *[filename]* command configures the device to load the designated IOS from flash memory; if you do not specify the *filename*, the first bootable IOS image is loaded. The **boot system** [**tftp**] *filename [ip-address]* command configures the device to load the designated IOS from a TFTP server; if you do not specify the *ip-address*, the IP broadcast address of 255.255.255.255 will be used. The **boot system rom** command configures the device to load the IOS from ROM. If you issue multiple **boot system** commands, the router will attempt to load the IOS in the order that you issued the commands.

NVRAM is used to store configuration files. If no configuration file is present in NVRAM, the device will start the System Configuration Dialog, or setup mode. Alternatively, to enter setup mode, you could issue the **setup** command. The System Configuration Dialog enables you to configure basic settings, such as the host name, the enable password, the enable secret password, the virtual terminal (VTY) password, and interface IP addressing information.

Upgrading IOS

1. Configure a TFTP server
2. Download the IOS image from Cisco to TFTP
3. Verify TFTP server connectivity from the device
4. Issue the **copy tftp flash** command on the device
5. Check the IOS version and configuration register value
6. Reload the device



Upgrading IOS

You might need to upgrade IOS on a Cisco router or switch when you need additional features that are not available in the version of IOS that you are currently using. Before you can upgrade IOS, you must configure a TFTP server at a network location that can be accessed by the router or switch. The TFTP server can be run from any supported device on the network as long as the router or switch to be upgraded can connect to the device. You can verify that the TFTP server is reachable from the device to be upgraded by issuing the **ping ip-address** command on the device, where *ip-address* is the IP address of the TFTP server.

After you configure the TFTP server, you should download the new version of IOS from Cisco's website. You can use the [Cisco Feature Navigator](#) on Cisco's site to determine which version of IOS you need based on the hardware you have, the flash memory that is installed in the hardware, and the feature set that you want to implement. You should issue the **show version** command or the **show flash** command on the device to be upgraded to verify that enough flash memory space is available to support the new image.

After you download the new version of IOS to the TFTP server, you should issue the **copy tftp flash** command on the device to be upgraded to begin the upgrade process. After you issue the **copy tftp flash** command, you will be prompted to provide the IP address of the TFTP server, the filename of the IOS image that you want to copy, and the filename that you want to use for the IOS image on the device to be upgraded.

After you have entered the appropriate information at the prompts, IOS will display the `Erase flash: before copying? [confirm]` prompt. If you confirm that you want to erase flash memory, everything that is currently stored in flash memory will be erased before the new IOS image is copied. You can choose to not erase flash memory before copying the new image. However, you should first ensure that enough space exists in flash memory to store both the new IOS image and the current flash memory contents.

After you have either confirmed or dismissed the erase prompt, the file copy process begins. Depending on the size of the IOS image and the speed of the connection to the TFTP server, the copy process can take several minutes. The copy process is tracked by a series of ! symbols that are repeated as data is transferred.

After the data has been transferred, you should issue the **show version** command to verify that the configuration register is set to the default value of 0x2102. In addition, you should issue the **dir flash:** command to view the contents of flash memory. If the first file listed in flash memory is not the new IOS image, you might need to issue the **no boot system** command followed by the **boot system filename** command, where *filename* is the name of the new IOS image. The **boot system** command ensures that the device finds the correct IOS image upon reload.

Finally, you should issue the **reload** command to reboot the router or switch with the new IOS image. After the device reboots, you should issue the **show version** command to ensure that the correct version of IOS is running on the device.

Troubleshooting IOS Upgrades

Two common problems can occur during an IOS upgrade procedure: lack of flash memory space and lack of connectivity to the TFTP server. For example, if you were attempting to copy a new image named `newimage.bin` to a device that did not have enough free flash memory to support the new image, you might see the following message:

```
%Error copying tftp://10.10.10.10/newimage.bin
(Not enough space on device)
```

The error message above indicates that the **copy tftp flash** command was not able to copy a file named `newimage.bin` from a TFTP server with the IP address 10.10.10.10 because there was not enough space in flash memory to accommodate the file.

If you were attempting to copy an image named `newimage.bin` from a TFTP server that was either down or unreachable on the network, you might see the following message:

```
%Error opening tftp://10.10.10.10/newimage.bin (Timed out)
```

The error message above indicates that the **copy tftp flash** command was not able to connect to the TFTP server at 10.10.10.10 to retrieve the file named `newimage.bin`.

To avoid problems such as those described above, always check flash memory space limitations before attempting to upgrade IOS. In addition, use the **ping** command to verify that the device being upgraded can connect to the TFTP server.

Understanding and Modifying the Configuration Register

- The configuration register can determine how a router boots, the speed of the console, and what options are enabled while booting
- Issue the **show version** command to view the current configuration register setting
- Issue the **config-register** command to change the configuration register setting

Understanding and Modifying the Configuration Register

The configuration register can be changed to modify how a Cisco device boots. For example, you can configure the device to boot to ROM, to a bootstrap prompt, or to IOS. You can also modify the configuration register to change the console speed for terminal emulation sessions or to cause the device to disable boot messages. To view the current configuration register setting, you should issue the **show version** command. To change the configuration register setting, you should issue the **config-register** *value* command, where *value* is a hexadecimal value preceded by **0x**.

By default, the configuration register value is set to **0x2102**. This setting configures the device to boot normally, which means it boots to the IOS image stored in flash memory if a valid image exists. If a valid image does not exist, the device will boot to ROM. This value also configures a console speed of 9600 baud for terminal emulation sessions.

Other commonly used configuration register values include the following:

- **0x2101** – configures the device to boot to the bootstrap program, which is a program that can be used to run diagnostics on the router. This setting configures the device to boot using a speed of 9600 baud.
- **0x2120** – configures the device to boot to a `rommon>` prompt. When at a `rommon>` prompt, you can load a boot image, which will enable you to download a valid IOS image from a TFTP server.
- **0x2122** – configures the device to boot to an IOS image stored in flash memory, if one exists in flash memory. Otherwise, the device boots into ROM. The console speed when this setting is configured will be 19200 baud.

- **0x2142** – configures the device to disregard the contents of NVRAM when the router is rebooted. With this setting, any configuration information will be ignored and you will be prompted to create an initial configuration for the router.
- **0x3122** – configures the device to boot to an IOS image if a valid image exists. Otherwise, the device boots into ROM. This setting will also configure the device to boot using a console speed of 57600 baud.

Using the Configuration Register for Password Recovery

- Boot to flash memory
- Load the NVRAM configuration
- Reset or record any forgotten passwords
- Save the new configuration to NVRAM
- Boot to NVRAM



Using the Configuration Register for Password Recovery

The ability to modify how the device boots can be useful in emergencies, such as when you need to recover or change the enable password on a device for which the enable password has been lost. For example, if you had forgotten the enable password to a Cisco router named Router1, you could use a console cable to connect a terminal to the router, access the Router1 console, and perform the following steps:

1. Issue the **show version** command from user EXEC mode, and record the value of the configuration register. You will need to restore the router's configuration register to this value after you have completed the password recovery process.
2. Power cycle the device, and press the Break key on the terminal's keyboard within one minute after power is restored. This should boot the device into ROMmon mode.
3. In ROMmon mode, configure the device to boot from flash memory by issuing the **confreg 0x2142** command. Note that the ROMmon mode command for modifying the configuration register is different than the command you issue in global configuration mode. The **config-register value** command does not work in ROMmon mode.
4. Type **reset** to reboot the router.
5. You might be prompted with the configuration setup script because the 0x2142 configuration register setting disregards the contents of NVRAM. Press Ctrl+C on the keyboard after reboot to cancel the setup procedure.
6. From the console prompt, enter privileged EXEC mode by issuing the **enable** command. Because the router has ignored the NVRAM configuration, you should not be prompted for a password.
7. In privileged EXEC mode, issue the **copy startup-config running-config** command, which will load the contents of NVRAM into the running configuration. The router will remain in privileged EXEC mode.

After the router has loaded the configuration from NVRAM, you can either issue the **show running-config** command to display unencrypted passwords or you can place the device into global configuration mode and issue the appropriate commands to modify any encrypted or unencrypted passwords. You might also need to issue the **no shutdown** command on any interfaces that should be in the up state when the device is rebooted and the configuration is loaded.

Next, you should issue the **config-register 0x2102** command in global configuration mode to configure the device to boot from NVRAM. Finally, issue the **copy running-config startup-config** command from privileged EXEC mode to ensure that the configuration changes are saved to NVRAM and reboot the router.

Managing Configuration Files

- Loading IOS configuration files
 - From a TFTP server
 - **copy tftp running-config**
 - From NVRAM
 - **copy startup-config running-config**
- Saving IOS configuration files
 - To a TFTP server
 - **copy startup-config tftp**
 - To NVRAM
 - **copy running-config startup-config**

Managing Configuration Files

Cisco IOS provides the ability to load or save configuration files. Configuration files can be loaded from local storage, such as NVRAM, or from a remote location, such as a TFTP server. The **service config** command must be issued to load configuration files from a TFTP server. When the **service config** command is issued, the device will attempt to download the configuration files by using the default broadcast IP address of 255.255.255.255. To change this default, you should issue the **boot network url** and **boot host url** commands, where *url* is the complete Uniform Resource Locator (URL) of the configuration file on the TFTP server, including any user names and passwords.

Configuration files can also be saved to a TFTP server or to NVRAM. For example, if you make changes to a configuration file, you can save the changes to NVRAM so that the changes are loaded the next time the device is restarted.

To load an existing IOS configuration file, you should issue the **copy tftp running-config** command or the **copy startup-config running-config** command. Issuing the **copy tftp running-config** command replaces the current configuration with the configuration file stored on the TFTP server. Conversely, you could issue the **copy startup-config running-config** command to replace the current configuration with the configuration that is stored in NVRAM. Loading an existing configuration allows you to revert to a previous configuration in the event that you have made a number of changes that you want to erase.

To save the current running configuration file, you should issue either the **copy running-config startup-config** command or the **copy startup-config tftp** command. The **copy running-config startup-config** command is used to save the currently running configuration file to NVRAM. Running configurations, in addition to the running IOS software, are stored in DRAM. DRAM stores the routing tables, switching cache, and packet data when the device is in operation. The **copy startup-config tftp** command stores the current startup configuration file to a TFTP server.

Managing Licensing

- Pre-installed activated licenses
 - Permanent license for purchased features
 - No activation required
- Pre-installed inactive licenses
 - Evaluation licenses for additional features
 - Activate using the **license boot module** command
- New purchases
 - New software packages and product features can be activated with:
 - CLM
 - CLI – **license install** command
 - SNMP

Managing Licensing

Cisco devices come with a permanent license installed for the features you selected when you ordered the device; no activation is required for those feature sets. If you need to know which licenses are available on a device, the Cisco License Manager (CLM), the **show version** command, or the **show license** command can provide information about the licenses on a system. That information includes a list of the features that are enabled by using a permanent license, the features that are enabled by using a temporary license, and the features that are inactive.

Most Cisco devices come with evaluation, or temporary, licenses for the additional software and features supported by the device that were not initially purchased with the device. In order to test any given feature, you need to activate the temporary license for that feature by using the **license boot module** command. If you determine that you want to continue using the feature, you will first need to purchase the software package or device feature from cisco.com. When you make a purchase, you will receive a product activation key (PAK), which you will use along with the product ID and serial number of the device in order to obtain a license file. Once you have registered the purchased software package or device feature, you can use the CLM, the Cisco IOS command-line interface (CLI), or Simple Network Management Protocol (SNMP) to install and manage active licenses.

After permanent licenses have been installed and activated, you can use the **license save** command to make copies of the licenses for backup and recovery purposes. To remove a license from a device, use the **license clear** command. If a permanent license needs to be reinstalled after the **license clear** command has been issued, use the **license install** command along with the copy of the license previously made using the **license save** command. Temporary and built-in licenses cannot be removed by using the **license clear** command and therefore do not require a reinstall process.

Using SNMP to Manage Licenses

- Remotely monitor and manage network devices
- **snmp-server enable traps license** command
- SNMP license activation MIB

Using SNMP to Manage Licenses

Some devices can use an SNMP agent, such as the Cisco IOS Software Activation feature, which will allow installation of licenses by using SNMP. The SNMP agent accesses the CISCO-LICENSE-MGMT-MIB on the device to determine which licenses are active. The CISCO-LICENSE-MGMT-MIB is a management information base (MIB) that contains information about Cisco licenses available on the device.

This use of an SNMP agent offers administrators an additional method of license installation and increases flexibility in managing licenses. SNMP is typically used to remotely monitor and manage network devices by collecting statistical data about those devices. SNMP uses User Datagram Protocol (UDP) ports 161 and 162 by default.

SNMP version 1 (SNMPv1) and SNMPv2 use community strings to provide authentication. However, neither SNMPv1 nor SNMPv2 uses encryption; all data and community strings are sent in clear text. A malicious user can sniff an SNMP community string and use it to access and modify network devices. SNMPv3 is an enhancement to the SNMP protocol that uses encryption to provide confidentiality, integrity, and authentication.

To enable SNMP licensing notifications, you can use the **snmp-server enable traps** command with the **license** keyword by itself or in conjunction with the keywords **deploy**, **error**, **imagelevel**, or **usage**, depending on the level of information desired.

Review Question 1

You issue the **show version** command on a router and observe the following line at the end of the output:

```
Configuration register is 0x2102
```

Which of the following will occur as a result of this configuration the next time that the router is booted?

- A. The router will boot into ROMmon mode using a console speed of 9600 baud.
- B. The router will boot into the bootstrap program.
- C. The router will boot normally using a console speed of 9600 baud.
- D. The router will boot normally using a console speed of 19200 baud.
- E. The router will boot into ROMmon mode using a console speed of 19200 baud.
- F. The router will boot normally using a console speed of 57600 baud.

Review Question 1

You issue the **show version** command on a router and observe the following line at the end of the output:

```
Configuration register is 0x2102
```

Which of the following will occur as a result of this configuration the next time that the router is booted?

- A. The router will boot into ROMmon mode using a console speed of 9600 baud.
- B. The router will boot into the bootstrap program.
- C. The router will boot normally using a console speed of 9600 baud.
- D. The router will boot normally using a console speed of 19200 baud.
- E. The router will boot into ROMmon mode using a console speed of 19200 baud.
- F. The router will boot normally using a console speed of 57600 baud.

By default, the configuration register value is set to **0x2102**. This setting configures the router to boot normally, which means it boots to the IOS image stored in flash memory if a valid image exists. If a valid image does not exist, the router will boot to read-only memory (ROM). This value also configures a console speed of 9600 baud for terminal emulation sessions.

The configuration register can be changed to modify how a router boots. For example, by changing the configuration register setting, you can configure the router to boot to ROM, to a bootstrap prompt, or to the IOS. You can also modify the configuration register to change the console speed for terminal emulation sessions or to cause the router to disable boot messages. To view the current configuration register setting, you should issue the **show version** command. To change the configuration register setting, you should issue the **config-register value** command, where *value* is a hexadecimal value preceded by **0x**.

Review Question 2

From which locations can a full version of the Cisco IOS be loaded at startup?

- A. flash memory
- B. a TFTP server
- C. ROM
- D. NVRAM

Review Question 2

From which locations can a full version of the Cisco IOS be loaded at startup?

- A. flash memory
- B. a TFTP server
- C. ROM
- D. NVRAM

A full version of the Cisco IOS can be loaded at startup from flash memory or from a Trivial File Transfer Protocol (TFTP) server. The Cisco IOS is normally located in flash memory. If the flash memory is empty or the file system is corrupt, you will receive an error message stating `boot: cannot open "flash:"`. The router will then attempt to load IOS from a TFTP server. If IOS cannot be loaded from a TFTP server, the device will load a limited version of the IOS from read-only memory (ROM). ROM does not contain a full version of the Cisco IOS.

Lab Exercises

Module 1: Cisco Device Management

Lab 1.1 – Device Management

Labs powered by

NetSim[®]
NETWORK SIMULATOR[®]

The labs referenced in this book have been printed in the Boson Lab Guide, which is included with the purchase of the curriculum. These labs can be performed with real Cisco hardware or in the Boson NetSim Network Simulator. To learn more about the benefits of using NetSim or to purchase the software, please visit www.boson.com/netsim.

Certification Candidates

Boson Software's ExSim-Max practice exams are designed to simulate the complete exam experience. These practice exams have been written by in-house authors who have over 30 years combined experience writing practice exams. ExSim-Max is designed to simulate the live exam, including topics covered, question types, question difficulty, and time allowed, so you know what to expect. To learn more about ExSim-Max practice exams, please visit www.boson.com/exsim-max-practice-exams or contact Boson Software.

Organizational and Volume Customers

Boson Software's outstanding IT training tools serve the skill development needs of organizations such as colleges, technical training educators, corporations, and governmental agencies. If your organization would like to inquire about volume opportunities and discounts, please contact Boson Software at orgsales@boson.com.

Contact Information

E-Mail: support@boson.com
Phone: 877-333-EXAM (3926)
615-889-0121
Fax: 615-889-0122
Address: 25 Century Blvd., Ste. 500
Nashville, TN 37214





B o s o n . c o m

8 7 7 . 3 3 3 . 3 9 2 6 s u p p o r t @ b o s o n . c o m

© Copyright 2016 Boson Software, LLC. All rights reserved.