



TSHOOT

Curriculum

300-135

Labs powered by



TSHOOT

300-135 Curriculum



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 11 or later. To learn more about the benefits of using NetSim or to purchase the software, please visit www.boson.com/netsim.

Copyright © 2017 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: Disaster Recovery	1
Overview	2
Objectives	2
Have a Plan.....	3
Build Redundancy.....	4
Ensure Availability.....	5
Manually Copying the Configuration	6
Manually Copying the Configuration with Encryption.....	7
Creating an Archive.....	8
Verifying Archives and Restoring Configurations.....	9
Document the Network	10
Topology Diagrams.....	11
Cisco Information-Gathering Tools	13
show arp	14
show cdp neighbors	15
show interfaces	16
show ip route	17
show mac-address-table	18
show version	19
Windows Information-Gathering Tools	20
ipconfig /all	21
arp -a	22
tracert -d	23
route print	24
Mac OS, UNIX, and Linux Information-Gathering Tools.....	25
ifconfig -a	26
traceroute	27
route -n	28
Review Question 1.....	29
Review Question 2.....	31
Module 2: Troubleshooting Tools and Techniques	33
Overview	34
Objectives	34
Understanding the Systematic Approach	35
Gather Facts and Consider the Possibilities	37
Understanding the ping Command.....	38
Using Extended Pings for Other Tests.....	38
Using Ping to Troubleshoot.....	40
Create an Action Plan	41
Where Does the Device Function?	42
Implement an Action Plan with OSI.....	43
<i>The Bottom Up Troubleshooting Technique</i>	43

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

<i>The Top Down Troubleshooting Technique</i>	43
<i>The Divide and Conquer Troubleshooting Technique</i>	43
Implement a Non-OSI Action Plan	45
<i>The Follow the Path Troubleshooting Technique</i>	45
<i>The Move the Problem Troubleshooting Technique</i>	45
<i>The Spot the Difference Troubleshooting Technique</i>	46
Observe Results	47
Understanding show Commands	48
Understanding debug Commands.....	50
Understanding Syslog	52
Configuring Log Severity Levels.....	54
Document the Solution	55
Monitoring Networks	56
Monitoring LAN Traffic with SPAN.....	57
Understanding IP SLAs	59
Configuring IP SLA Echo	60
Verifying and Troubleshooting IP SLAs.....	62
Understanding SNMP	63
Configuring NetFlow	64
Using SNMP Data	66
Understanding NetFlow	68
Using NetFlow Data.....	69
Configuring NetFlow	70
<i>Verifying NetFlow</i>	71
<i>Analyzing NetFlow Data</i>	74
Solving Common Network Problems.....	76
Troubleshooting Connectivity.....	77
Troubleshooting Physical Layer Connectivity.....	78
Troubleshooting Data Link Layer Connectivity	80
Contacting Cisco TAC.....	81
Review Question 1.....	83
Review Question 2.....	85
Review Question 3.....	87
Lab Exercises	89
Module 3: Troubleshooting Layer 3 and Beyond	91
Overview	92
Objectives	92
Troubleshooting Network Layer Connectivity	93
Network Addressing	94
IPv4 Connectivity	96
IPv6 Connectivity	97
Path Selection	98

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

<i>Path Selection and Proxy ARP Configuration</i>	100
<i>Path Selection and Routing Protocols</i>	101
Troubleshooting Beyond Layer 3	102
Troubleshooting Layer 4	103
User Datagram Protocol	104
Transmission Control Protocol	105
The TCP Three-way Handshake	106
Windowing	108
Sliding Windowing	109
Using Telnet to Troubleshoot Layer 4	110
Resolving Layer 4 Connectivity	111
Troubleshooting Beyond Layer 4	112
Review Question 1	113
Review Question 2	115
Module 4: Basic Network Services Troubleshooting	117
Overview	118
Objectives	118
Content in these modules is available in the full version of the curriculum. Please visit www.boson.com for more information.	119
Remote Management Problems	120
Configuration Fallbacks	121
Configuring Fallback Timeouts	122
Reviewing Configuration Changes	124
CDP and LLDP	125
Disabling and Enabling CDP	126
Disabling and Enabling LLDP	127
Verifying CDP and LLDP Configurations	128
Displaying CDP and LLDP Neighbors	130
Displaying CDP and LLDP Information About Specific Devices	131
Displaying CDP and LLDP Information About Advertisements	132
Debugging CDP and LLDP	133
DHCP	134
Troubleshooting IP Address Conflicts	135
Troubleshooting Exhausted DHCP Pools	136
Debugging DHCP	137
DHCP Servers on Remote Subnets	138
Configuring a DHCP Server	139
Configuring DHCP Server Options	140
Configuring Automatic IPv6 Addressing on Clients	141
SLAAC	141
Stateless DHCPv6	142
Stateful DHCPv6	142
DHCP Snooping	143

Configuring DHCP Snooping	144
DNS	145
Configuring a DNS Client	146
Configuring a DNS Server.....	147
Other Causes of DNS Problems	148
NTP	149
Common Causes of NTP Problems	150
How NTP Stratum Works	151
Configuring NTP.....	152
Configuring the System Clock and NTP.....	153
Authenticating NTP Time Sources	155
NAT/PAT.....	156
Causes of Common NAT/PAT Problems	157
Commands for Troubleshooting NAT	158
NAT/PAT Address Terminology	160
Configuring Interfaces for NAT/PAT	161
NAT NVI Configurations	162
NAT Translation Methods	163
Configuring Static NAT.....	164
Dynamic NAT	165
Configuring Dynamic NAT	166
PAT	169
Configuring PAT.....	170
Review Question 1.....	173
Review Question 2.....	175
Lab Exercises	177
Module 5: Basic Security.....	179
Overview.....	180
Objectives	180
Protecting Assets.....	181
Securing Cisco Devices.....	182
Warning Banners	183
Login Banners	184
MOTD Banners.....	185
EXEC Banners	186
Securing Configurations	187
Logging	188
Configuring Accurate Time.....	189
Configuring Log Severity Levels.....	190
Configuring and Using a Logging Server	191
Securing Access.....	192

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

Requiring Authentication	193
Configuring Privilege Levels	194
Configuring Roles	195
Configuring RBAC CLI Access	196
<i>Configuring Users</i>	197
<i>Requiring Complex Passwords</i>	199
Configuring Encrypted Management Access	200
Configuring an Enable Password	202
Troubleshooting Access	204
Authenticating with AAA	205
AAA Authentication	206
RADIUS vs. TACACS+	207
<i>Configuring AAA and RADIUS</i>	208
<i>Configuring AAA and TACACS+</i>	210
Configuring Authorization and Accounting	212
Troubleshooting AAA	213
Understanding ACLs	214
Understanding Wildcard Masks	215
Configuring Standard ACLs	216
Configuring Extended ACLs	219
Understanding ACL Sequencing	223
Applying ACLs to an Interface	226
Verifying and Troubleshooting ACLs	228
Review Question 1	229
Review Question 2	231
Lab Exercises	233
Module 6: Switch Troubleshooting	235
Overview	236
Objectives	236
Troubleshooting STP Commands	237
STP Troubleshooting Requirements	241
Common Causes of STP Problems	242
Understanding STP	243
<i>Root Bridge Election</i>	244
<i>Path Costs</i>	247
<i>Determining Port Roles</i>	248
<i>STP Port States</i>	249
<i>STP Timers</i>	250
Understanding RSTP	251
<i>Differences Between STP and RSTP</i>	252
<i>Understanding RSTP Port States</i>	254
<i>RSTP Alternate and Backup Port Roles</i>	255

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

Understanding Cisco Implementations of STP	256
Per-VLAN Spanning Tree Plus	257
PVST+ Bridge IDs.....	258
Per-VLAN Rapid Spanning Tree Plus.....	259
Multiple Spanning Tree Protocol.....	260
MST Regions.....	261
MST Instances	262
Cisco STP Toolkit.....	263
UplinkFast.....	264
BackboneFast.....	265
PortFast.....	266
BPDU Guard	267
BPDU Filter.....	268
Loop Guard.....	269
UDLD.....	270
Root Guard	271
Trunk Troubleshooting Commands	272
Troubleshooting Trunk Ports	274
Configuring Trunk Ports	275
How DTP Negotiates Trunks	276
How DTP Negotiates Trunks	278
VLAN Troubleshooting Commands	280
Troubleshooting VLANs	281
Common Causes of VLAN Problems.....	282
Common Causes of Native VLAN Problems.....	283
VLAN Hopping	284
<i>Mitigating VLAN Hopping</i>	285
VTP Troubleshooting Commands.....	286
Common Causes of VTP Problems	287
Understanding and Configuring VTP	288
<i>VTP Domains</i>	289
<i>VTP Version</i>	290
<i>VTP Modes</i>	291
<i>VTP Operation</i>	292
<i>VTP Pruning</i>	294
Port Security Troubleshooting Commands	295
Common Causes of Port Security Problems.....	297
Restricting Ports by MAC Address	298
Error-Disabled Ports.....	301
Review Question 1	305
Review Question 2.....	307
Lab Exercises	309

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

Module 7: Multilayer Switch Troubleshooting	311
Overview	312
Objectives	312
Understanding Multilayer Switches.....	313
Default Routes	314
Configuring a Default Route on a Multilayer Switch	315
Verifying a Default Route on a Multilayer Switch	316
InterVLAN Routing.....	317
Troubleshooting InterVLAN Routing.....	319
Understanding EtherChannel.....	320
Commands for Troubleshooting EtherChannel	321
Understanding EtherChannel Protocols	323
Understanding PAgP and LACP Modes.....	324
<i>The On Mode</i>	324
<i>PAgP Modes</i>	324
<i>LACP Modes</i>	325
Troubleshooting EtherChannel.....	326
<i>Aggregation Protocol Mismatches</i>	327
<i>Bundle Configuration Mismatches</i>	328
HSRP	330
HSRP Versions.....	331
Understanding Virtual MAC Addresses.....	332
HSRP Hello Packets.....	333
HSRP Hello and Hold Timers.....	334
Configuring HSRP and Timers.....	335
Configuring Preemption.....	336
Configuring Interface Tracking	338
Configuring HSRP Object Tracking.....	340
Understanding HSRP States.....	341
Configuring Multigroup HSRP	342
HSRP Authentication.....	344
<i>Configuring HSRP Authentication</i>	345
Verifying HSRP	346
Troubleshooting HSRP	348
Understanding VRRP	349
Differences from HSRP	350
VRRP Timers	351
Configuring VRRP	352
Configuring VRRP Object Tracking.....	353
VRRP Authentication.....	354
<i>Configuring VRRP Authentication</i>	356
Verifying VRRP	357
Troubleshooting VRRP.....	358

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

Understanding GLBP	359
The AVG	360
<i>AVG States</i>	361
GLBP Virtual MAC Addresses	362
The AVF	363
<i>AVF States</i>	364
How GLBP Load Balancing Works	365
GLBP Hello Packets	367
How GLBP Failover Works	368
<i>AVG Failover</i>	368
<i>AVF Failover</i>	368
Configuring GLBP	369
Configuring GLBP Timers	371
Configuring GLBP Object Tracking	372
Configuring GLBP Authentication	373
Verifying GLBP	374
Troubleshooting GLBP	376
Review Question 1	377
Review Question 2	379
Lab Exercises	381
Module 8: Router Troubleshooting	383
Overview	384
Objectives	384
Routing Sources	385
Troubleshooting Commands for Routing Sources	386
Understanding Passive Interfaces	388
Redistribution	389
Redistribution Best Practices	390
Causes of Redistribution Problems	391
Distribution Lists	392
Seed Metrics	393
<i>Assigning Seed Metrics</i>	395
Redistribution Design Considerations	396
<i>Redistribution – RIP</i>	397
<i>Redistribution – OSPF</i>	398
<i>Redistribution – EIGRP</i>	400
<i>Verifying Redistribution</i>	402
Route Maps	403
Administrative Distance	404
Troubleshooting Commands for Redistribution	406
GRE Tunnels	408
Causes of GRE Tunnel Problems	409

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

Understanding GRE Tunnels.....	410
Configuring GRE Tunnels.....	412
Troubleshooting Commands for GRE Tunnels.....	416
Review Question 1.....	419
Review Question 2.....	421
Lab Exercises.....	423
Module 9: Troubleshooting Routing Protocols.....	425
Overview.....	426
Objectives.....	426
Understanding Autonomous Systems.....	427
Understanding Routing Protocols.....	428
Understanding the Types of IGP.....	429
Understanding Distance-Vector Routing Protocols.....	430
Learning Distance-Vector Routes.....	431
Updating Distance-Vector Routes.....	432
Preventing Distance-Vector Problems.....	433
Understanding the Counting to Infinity Problem.....	434
Understanding Routing Loops.....	436
Preventing Routing Loops.....	437
Understanding Link-State Routing Protocols.....	439
Understanding Link-State Relationships.....	440
Understanding the LSDB.....	441
Learning Link-State Routes.....	442
BGP.....	443
Troubleshooting Commands for BGP.....	444
Common Causes of BGP Problems.....	448
Configuring Peer Information.....	449
Configuring BGP Authentication.....	451
BGP Transit AS.....	452
BGP Route Filtering Mechanisms.....	453
Prefix Lists.....	454
How Prefix Lists Match Routes.....	455
ip prefix-list Command.....	456
Understanding le and ge Values.....	457
Examples of le and ge Values.....	458
neighbor prefix-list Command.....	459
Editing Prefix Lists.....	460
Verifying Prefix Lists.....	461
BGP Attributes and Path Selection.....	462
BGP Attributes.....	463
BGP Path Selection.....	465

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

MP-BGP.....	466
Troubleshooting Commands for MP-BGP	467
Common Causes of MP-BGP Problems	468
Configuring MP-BGP.....	469
RIPng.....	471
Troubleshooting Commands for RIPng	472
Common Causes of RIPng Problems	473
Configuring Basic RIPng	474
EIGRP	475
Understanding EIGRP	476
Basic Troubleshooting Commands for EIGRP	477
Understanding EIGRP Tables	479
Common Causes of EIGRP Adjacency Problems.....	481
Understanding EIGRP Adjacencies	482
Understanding EIGRP Passive Interfaces	483
Configuring EIGRP.....	484
<i>Configuring EIGRP in Named Mode.....</i>	<i>486</i>
<i>Configuring EIGRP Authentication</i>	<i>487</i>
<i>Configuring EIGRP Stub Routers.....</i>	<i>489</i>
<i>Using Variance to Load Balance EIGRP</i>	<i>490</i>
Troubleshooting Commands for EIGRP Summarization	493
Understanding EIGRP Route Summarization	494
Common Causes of EIGRP Summarization Problems	495
Troubleshooting Commands for EIGRP Stubs.....	496
Understanding EIGRP Stubs.....	497
Common Causes of EIGRP Stub Problems.....	498
Configuring EIGRP Stubs.....	499
EIGRP for IPv6	500
Understanding EIGRP for IPv6	501
Basic Troubleshooting Commands for EIGRP for IPv6.....	502
Troubleshooting EIGRP for IPv6 Tables.....	504
Configuring EIGRP for IPv6	506
OSPF	508
Troubleshooting Commands for OSPF	509
Understanding OSPF Router IDs	512
Understanding OSPF	513
Configuring OSPF	514
<i>Configuring Single-Area OSPFv2</i>	<i>514</i>
<i>The Importance of the Backbone Area.....</i>	<i>515</i>
<i>Configuring Multiarea OSPFv2.....</i>	<i>515</i>
Understanding OSPF Adjacencies.....	517
Understanding DR and BDR Elections.....	519
Understanding the LSDB.....	520

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

Common Causes of OSPF Adjacency Problems	522
<i>Troubleshooting Commands for OSPF Adjacencies</i>	526
OSPF Stub Areas	530
<i>Troubleshooting Commands for OSPF Stub Areas</i>	531
<i>Configuring OSPF Stub Areas</i>	533
OSPFv3	534
Troubleshooting Commands for OSPFv3.....	535
Understanding OSPFv3.....	538
Common Causes of OSPFv3 Problems	539
Configuring OSPFv3	540
Review Question 1	541
Review Question 2	543
Lab Exercises	545
Module 10: Preparing for the TSHOOT Exam.....	547
Overview	548
Objectives	548
Preparing for the TSHOOT Exam.....	549
Lab Exercises	551
Index	555

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

Module 1

Disaster Recovery

Disaster Recovery Overview

- Have a plan
- Build redundancy into the network
- Ensure availability of tools and backups
- Document the network



Overview

Network systems face several threats from both internal and external sources. Although some of these threats may not be malicious, they can all disrupt the operation of network devices. This module explores general methods of preparing for and recovering from disaster.

Objectives

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

- Have a plan.
- Build redundancy into the network.
- Ensure the availability of tools and backups.
- Document the network.

Have a Plan

- Three phases of recovery:
 - Activation
 - Execution
 - Reconstitution
- Know how to get replacement hardware
- Know software versions and configurations
- Know licensing
- Know installation procedures



Have a Plan

It is important to have a plan for disaster recovery before a disaster occurs. In the event of a disaster, an organization's administrators must know where to go to get the information they need and what to do with it when they have it. Encountering a disaster without a plan in place could create chaos within an organization and lead to decisions that are not in the best interests of restoring operations.

There are three phases of the disaster recovery process:

- Activation
- Execution
- Reconstitution

The activation phase of disaster recovery is the phase in which the effects of a disaster are examined and reported. This phase is critical for comprehending the scope of the disaster and communicating the effects through appropriate channels within an organization.

The execution phase of disaster recovery is the phase in which the deployment of planned procedures for mitigating the effects of a disaster occur. For example, you might need to replace destroyed hardware during the execution phase of a disaster recovery plan. In that case, your organization's execution plan would need to have clear documentation regarding how to obtain replacement hardware, what software is installed on the given hardware, what licenses the organization has for the given software, and how to install the hardware and software.

The reconstitution phase of disaster recovery is the phase in which the execution phase is complete. In this phase, the organization is considered restored and normal operations can resume.

Build Redundancy

- Create redundancy at critical network points
- Verify that there are no single points of failure



Build Redundancy

A single point of failure is a system component that would make a resource unavailable if it were to fail. A system that does not have a single point of failure is considered fault-tolerant. Redundant components provide fault tolerance by assuming the workload of another component if the primary component fails. Implementing fault-tolerant devices and systems, or redundancy, at critical network points mitigates flaws in service reliability or design reliability.

For example, a firewall connected to multiple Internet service providers (ISPs) is a single point of failure. If the firewall were to fail, network devices would not be able to communicate with the ISPs. Connecting multiple firewalls to multiple ISPs would allow continued ISP access if a firewall were to fail. At a network level, the use of redundant Internet connections, the use of redundant routes to a destination, and the use of First-Hop Redundancy Protocols (FHRPs) on redundant hardware can aid in eliminating single points of failure.

Ensure Availability

- Create regular backups
 - Local copies
 - Copies at disaster recovery facilities
- Back up configurations after each change
 - Manually copy the configuration
 - Regularly archive the configuration
 - Automatically archive the configuration
- Verify archives with **show archive** command



Ensure Availability

Redundant hardware and software installation media are not enough to ensure availability in case of disaster. You should also create regular backups of data generated by applications and users. You should store those backups in two places: on-location for quick and convenient access and off-site in case the local facility is destroyed or becomes inaccessible during a disaster. Regular backups stored in more than one location ensure that up-to-date copies of company data are always available. Ensuring availability also means having backups of network device configurations readily available to deploy in case network hardware is accidentally wiped or destroyed and replaced with redundant hardware.

Manually Copying the Configuration

Storing credentials for an FTP server

```
RouterA(config)#ip ftp username admin
RouterA(config)#ip ftp password myftppassword
```

Copying a running configuration to an FTP server

```
RouterA#copy running-config ftp
Address or name of remote host []? 192.168.51.50
Destination filename [routera-config]?
```

Copying a running-configuration to an FTP server with a single command

```
RouterA#copy running-config ftp://admin:myftppassword@192.168.51.50
Address or name of remote host [192.168.51.50]?
Destination filename [routera-config]?
```

Manually Copying the Configuration

The configurations of Cisco devices like routers and switches can be manually copied from those devices to other locations for backup by issuing the **copy** command from privileged EXEC mode. For example, you could issue the **copy running-config ftp** command to copy the configuration to a File Transfer Protocol (FTP) server.

The **copy** command prompts you for server information and credentials. Alternatively, you can store FTP server credentials locally so that you do not need to issue them each time you issue the **copy running-config ftp** command. Issuing the **ip ftp username admin** command in global configuration mode stores the FTP server user name **admin** locally. Issuing the **ip ftp password myftppassword** command in global configuration mode stores the FTP server password **myftppassword** locally. If you then issue the **copy running-config ftp** command, the user name of **admin** and the password of **myftppassword** is automatically used as the FTP server credentials. However, you would still be prompted for the FTP server IP address and the file name you want to use for the backup configuration's destination.

Finally, it is possible to specify the FTP server credentials and destination IP address as parameters to the **copy** command. For example, the **copy running-config ftp://admin:myftppassword@192.168.51.50** command connects to the FTP server at 192.168.51.50 by using a user name of **admin** and a password of **myftppassword**. A destination file name is still required.

It is also possible to use Trivial FTP (TFTP), Hypertext Transfer Protocol (HTTP), or HTTP Secure (HTTPS) instead of FTP. To use TFTP, replace the **ftp** keyword with the **tftp** keyword. To use HTTP, replace the **ftp** keyword with the **http** keyword. To use HTTPS, replace the **ftp** keyword with the **https** keyword. Unlike TFTP, FTP, and HTTP, information transmitted by using HTTPS is encrypted.

Manually Copying the Configuration with Encryption

Configuring an IP domain name

```
RouterA(config)#ip domain boson.com
```

Configuring a user name and password

```
RouterA(config)#username admin privilege 15 password mysshpassword
```

Configuring SSH

```
RouterA(config)#crypto key generate rsa
RouterA(config)#ip ssh time-out 90
RouterA(config)#ip ssh authentication-retries 3
```

Enabling SCP

```
RouterA(config)#ip scp server enable
```

Copying a file from flash memory to a remote SSH server

```
RouterA#copy flash: scp:
Source filename []? backupA.txt
Address or name of remote host []? 192.168.51.50
Destination username [Router]? secure
Destination filename [backupA.txt]?
Writing backupA.txt
Password:
```

Manually Copying the Configuration with Encryption

It is important to note that traffic is not encrypted when copying a configuration by using FTP or TFTP. To encrypt traffic between the source and destination, you first need to configure Secure Shell (SSH) and then use Secure Copy (SCP). To configure SSH, you must first have configured a host name and a domain name on the device. You can issue the **ip domain name** command to configure a domain name. After you have configured the host name and domain name, you can issue the **crypto key generate rsa** command to create an encryption key for SSH.

Unlike FTP, SSH on Cisco devices can use the local user database as a source for credentials to remote servers. You can add users and credentials to the local user database by issuing the **username user-name privilege privilege-level password password** command from global configuration mode. For example, issuing the command **username admin privilege 15 password mysshpassword** creates a user named **admin** that has a password of **mysshpassword** and a Cisco IOS privilege level of 15. If you want to ensure password encryption in the running configuration, you can issue the command with the **secret** keyword in place of the password keyword. If you issue the **password** keyword and the **password** encryption service is not running, the password string is stored as plain text.

After configuring SSH, you should enable SCP by issuing the **ip scp server enable** command from global configuration mode. You can customize some behavior of SSH sessions by issuing the **ip ssh time-out seconds** command and the **ip ssh authentication-retries number-of-retries** command from global configuration mode.

Finally, you can issue the **copy flash: scp:** command from privileged EXEC mode to copy a file from a Cisco device's flash memory by using SCP. The **copy** command prompts you for the source and destination file names, the destination IP address, and the destination credentials.

Creating an Archive

Creating an archive

```
RouterA(config)#archive
```

Configuring an archive destination path with credentials

```
RouterA(config-archive)#path ftp://admin:myftppassword@192.168.51.50/$t$h
```

Configuring an archive to occur at regular intervals

```
RouterA(config-archive)#time-period 10080
```

Configuring an archive to occur automatically when the running-config is written

```
RouterA(config-archive)#write-memory
```

Manually archiving a running configuration

```
RouterA#archive config
```

Creating an Archive

In addition to manually copying configurations to remote locations, it is possible to establish an automatic archiving of configurations at regular intervals. Before you can automatically copy configuration files, you must configure an archive. To configure an archive, you should first issue the **archive** command in global configuration mode. The **archive** command places the device into archive configuration mode.

At a minimum, the archive you configure must contain a path to the destination. You can create an archive path by issuing the **path path** command along with either the **\$h** variable or the **\$t** variable from archive configuration mode. Placing the **\$h** variable at the end of a path ensures that the destination file name is the same as the source host name. Placing the **\$t** variable at the end of a path ensures that the destination file name is the same as the date and time that the archive occurred. For example, the **path ftp://admin:myftppassword@192.168.51.50/\$t\$h** command ensures that an archive with a file name based on the source host name and archive date and time is copied to the FTP server at 192.168.51.50. Furthermore, the user name of **admin** and the password of **myftppassword** are used as credentials to access the FTP server. If the **\$t** variable is not specified, the archive is named by using a version number, starting with 1. The higher the version number, the more recent the archive.

To ensure the automatic creation of an archive at regular intervals, you can configure the **time-period minutes** command in archive configuration mode. For example, the **time-period 1620** command would ensure that a copy of the configuration is automatically archived every 24 hours. Issuing the **time-period 10080** command would ensure that a copy of the configuration is archived once per week.

If you issue the **write-memory** command in archive configuration mode, the archive creation occurs each time you store the running configuration in the device's non-volatile random-access memory (NVRAM). You can manually create an archive at any time, regardless of whether the **write-memory** command has been issued, by issuing the **archive config** command from privileged EXEC mode.

Verifying Archives and Restoring Configurations

Verifying archive configuration and history

```
RouterA#show archive
```

Copying a file from a TFTP server to flash memory

```
RouterA#copy tftp flash
Address or name of remote host []? 192.168.51.50
Source filename [routera-config]?
Destination filename [routera-config]?
Accessing tftp://192.168.51.50/routera-config...
Erase flash: before copying? [confirm]
Erasing the filesystem will remove all files! Continue? [confirm]
```

Copying a file from flash to the startup configuration

```
RouterA#copy flash:routera-config startup-config
Destination filename [startup-config]?
```

Replacing a configuration without reloading the device

```
RouterA#configure replace flash:routera-config list
```

Verifying Archives and Restoring Configurations

You can verify the results of manual and automatic archiving of configurations on a Cisco device by issuing the **show archive** command from privileged EXEC mode. The output of the **show archive** command displays the name of the next archive file in addition to an enumerated history of archives. The most recent archive is annotated with the <- Most Recent marker in the output.

There are several ways to restore a configuration that has been backed up to a remote location. One way is to manually copy the file to the Cisco device's flash memory by issuing the **copy** command. For example, the **copy tftp flash** command prompts you for the IP address of the source TFTP server, the source file name, the destination file name, and the erasure of flash memory. You can then copy the source file from flash memory to the startup configuration by issuing the **copy flash:filename startup-config** command from privileged EXEC mode. After you copy a file to the startup configuration, you must issue the **reload** command to load the configuration into memory.

Another means of restoring a backed-up configuration is to issue the **configure replace flash:filename [list]** command, where filename is the name of the file that you have copied to flash memory. The **configure replace** command detects the differences between the running configuration and the file with which you are replacing it. It then issues the correct commands to replace the running configuration with the new one. You can see the commands issued by the replace feature if you issue the command with the **list** keyword. By issuing the **configure replace** command, you can thus bypass the need to issue the **reload** command. However, the **configure replace** command cannot be used in every circumstance.

Document the Network

- Topology diagrams
- Documentation process



Document the Network

Network documentation is an invaluable tool for administrators when troubleshooting or performing disaster recovery. Up-to-date documentation provides administrators with an easy reference for the flow of traffic through a network. In addition, documentation enables administrators to immediately determine what devices are installed in different types of network hardware, what software versions are running on the hardware, and what addressing schemes are in use on the hardware.

Topology Diagrams

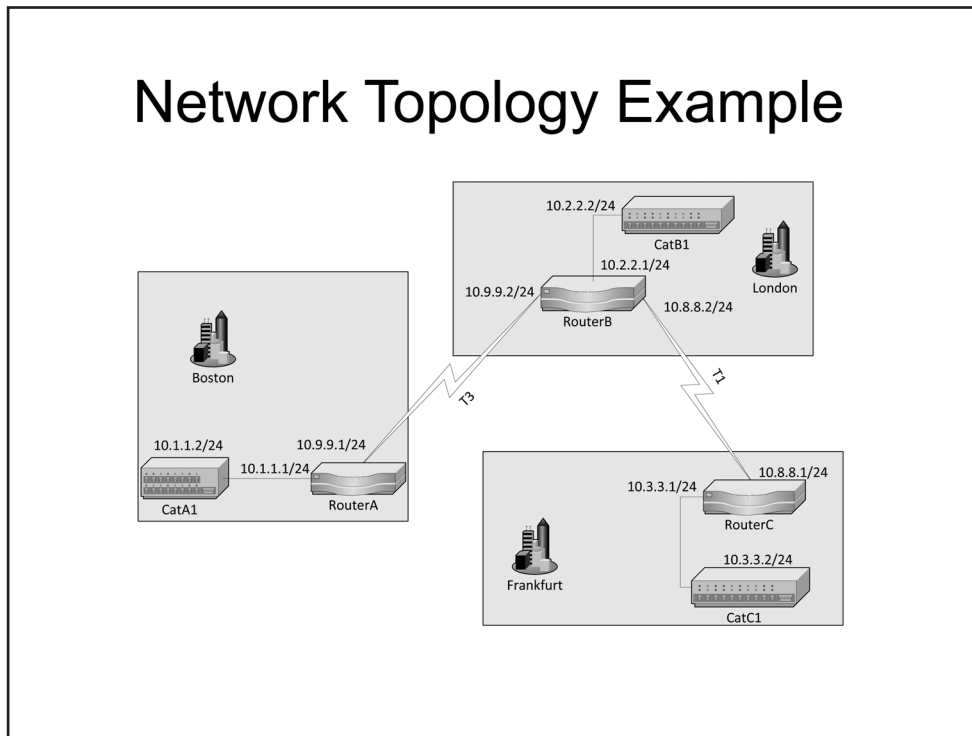
- Graphical diagram of your network
- Include:
 - Device names
 - WAN and LAN connections
 - VLAN, MAC, EtherChannel, and trunks
 - IP addresses, subnet masks, and routing protocols

Topology Diagrams

A topology diagram is a graphical representation of your company's network hardware and how it is connected. Each network device is represented along with configuration information, such as:

- Device name
- Network connection type
- Virtual LAN (VLAN), EtherChannel, and trunk information
- Media Access Control (MAC) and IP addressing information, including subnet masks
- Routing protocols, including autonomous system (AS) and area information

If the network spans multiple geographical areas, those areas should likewise be represented in the diagram.



In the example network topology diagram above, the network is divided into three geographical areas: Boston, London, and Frankfurt. Each geographical area is represented by a gray rectangle. Boston's RouterA is connected to London's RouterB by using a T3 line. The two routers operate on the 10.9.9.0/24 network, wherein RouterA has been assigned an IP address of 10.9.9.1 and RouterB has been assigned an IP address of 10.9.9.2.

London's RouterB is connected to Frankfurt's RouterC by using a T1 line. Each router on the link is operating in the 10.8.8.0/24 network, wherein RouterB has an IP address of 10.8.8.2 and RouterC has an IP address of 10.8.8.1.

The switch named CatA1 in Boston provides connectivity to the 10.1.1.0/24 network. The switch has an IP address of 10.1.1.2 and is connected by using Ethernet to the RouterA interface with the IP address of 10.1.1.1. Similarly, the switch named CatB1 in London provides connectivity to the 10.2.2.0/24 network. The switch has an IP address of 10.2.2.2 and is connected by using Ethernet to the RouterA interface with the IP address of 10.2.2.1. Finally, the switch named CatC1 in Frankfurt provides connectivity to the 10.3.3.0/24 network. The switch has an IP address of 10.3.3.2 and is connected by using Ethernet to the RouterA interface with the IP address of 10.3.3.1.

Cisco Information-Gathering Tools

- **show arp**
- **show cdp neighbors**
- **show interfaces**
- **show ip route**
- **show mac-address-table**
- **show version**



Cisco Information-Gathering Tools

Cisco IOS **show** commands provide information about a device or network activity that is static or collected over a period. You should typically issue **show** commands in privileged EXEC mode. Similar to other command-line interface (CLI) systems, many IOS **show** commands can be modified to produce variations of information or more detail about specific information. There are several **show** commands that can be useful for documenting a network device.

show arp

Displaying the ARP table on a router

```
RouterA#show arp
Protocol Address      Age (min)  Hardware Addr  Type   Interface
Internet 10.1.1.1      -          000C.3962.6232 ARPA   FastEthernet0/0
Internet 10.1.1.2      13         000C.8499.1947 ARPA   FastEthernet0/0
```

show arp

The Address Resolution Protocol (ARP) table contains a list of IP addresses mapped to MAC addresses. When a host knows the IP address of a remote destination but not the destination MAC address, it broadcasts an ARP request. When a Cisco router receives an ARP request for a device located on a remote network, the router replies to the ARP request with the MAC address of the router interface that is local to the sending host, indicating that the host should send the packet to the Cisco router. In effect, the router accepts responsibility for delivering the data to the remote destination. The router then uses the information stored in its ARP table to forward the data it receives to the correct destination.

show cdp neighbors

Displaying a Cisco router's neighbor information

```
RouterA#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID    Local Intrfce    Holdtme    Capability    Platform    Port ID
boson-1      Gig 0/1          117        S I           WS-C2960-2  Gig 0/1
boson-2      Gig 0/2          143        S I           WS-C2960-4  Gig 0/1
boson-3      Fas 0/3          102        R S I         1841        Fas 0/1
boson-4      Fas 0/4          133        R S I         1841        Fas 0/2
```

Displaying a Cisco switch's detailed neighbor information

```
SwitchA#show cdp neighbors detail
-----
Device ID: boson-1
Entry address(es):
  IP address: 10.1.2.3
Platform: WS-C2960-24TT-L, Capabilities: Switch IGMP
Interface: GigabitEthernet0/1, Port ID (outgoing port): GigabitEthernet0/10
Holdtime : 117 sec

Version :
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(25)SEE2, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Tue 08-Nov-06 15:20 by smithc

advertisement version: 2
VTP Management Domain: 'boson'
Native VLAN: 1
Duplex: full
Management address(es):
```

show cdp neighbors

You can issue the **show cdp neighbors** command on a device to view a list of information about the directly connected Cisco devices that are sending Cisco Discovery Protocol (CDP) updates to the device. The type of information displayed by the **show cdp neighbors** command includes the following:

- The device ID of the neighboring device
- The capabilities of the neighboring device
- The product number of the neighboring device
- The hold time
- The local interface
- The remote interface

You can view more detailed information about neighboring devices by issuing the **show cdp neighbors detail** command. In addition to providing the same information as found in the **show cdp neighbors** command, the **show cdp neighbors detail** command displays the following information:

- The Layer 3 address of the neighboring device
- The native VLAN
- The VLAN Trunking Protocol (VTP) domain

show interfaces

Displaying information about the FastEthernet 0/1 interface

```
SwitchA#show interfaces fastethernet 0/1
FastEthernet0/1 is up, line protocol is up
  Hardware is X2345, address is 00c0.1234.5678
  Internet address is 10.10.10.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  Auto-duplex, Auto-speed
  Last input 0:00:05, output 0:00:03, output hang never
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    119641 packets input, 21282118 bytes, 0 no buffer
    Received 92561 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 input packets with dribble condition detected
    149712 packets output, 14562789 bytes, 0 underruns
    0 output errors, 1 collisions, 5 interface resets
    0 babbles, 0 late collision, 7 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
```

Displaying interface descriptions on a router

```
RouterA#show interfaces description
Interface      Status      Protocol    Description
Fa0/0          up          up          To Internet
Fa0/1          up          up          To LAN
```

show interfaces

You can issue the **show interfaces** command to view information about the interfaces configured on a switch. The types of information displayed by issuing the **show interfaces** command include the status of interfaces, the IP address assigned to interfaces, the speed configured on the interfaces, and how many packets have been sent and received by the interfaces. In addition, you can view counts of how many times certain errors, such as cyclic redundancy check (CRC) errors, have occurred on the interface.

The syntax of the **show interfaces** command is **show interfaces** [*type number*], where the *type* and *number* parameters are optional. Using this syntax, you should issue the **show interfaces fastethernet 0/1** command to view information about interface FastEthernet 0/1.

A number of keywords can modify the output of the **show interfaces** command. For example, the **show interfaces description** command lists the device's interfaces and their statuses in a table format along with any text descriptions assigned to the interfaces.

show ip route

Verifying that a route is in the routing table

```
RouterA#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route

Gateway of last resort 192.168.1.2 to network 0.0.0.0

C    192.168.1.0 is directly connected, FastEthernet0/0
S    192.168.13.0 [1/0] via 192.168.2.2
C    192.168.2.0 is directly connected, FastEthernet0/1
R    192.168.10.0 [120/1] via 192.168.1.2, 00:06:17, FastEthernet0/0
S*   0.0.0.0 [1/0] via 192.168.1.2
```

show ip route

A router makes forwarding decisions based on the network information in its routing table. This network information typically originates from several different sources. For example, some of the information is configured manually, whereas other information is dynamically learned from other routers. Every route listed in the routing table belongs to one of the following general types:

- Directly connected routes
- Static routes
- Dynamic routes
- Default routes

You can use the **show ip route** command to view the contents of the routing table. Each entry in the routing table has the following components:

- Routing protocol code
- Network prefix and mask
- Next-hop IP address or interface

show mac-address-table

Displaying the MAC address table on a switch

```
SwitchA#show mac-address-table
      Mac Address Table
-----
Vlan  Mac Address      Type      Ports
----  -
1     000C.8908.7663    DYNAMIC   Fa0/2
1     000C.3962.6232    DYNAMIC   Fa0/1
```

show mac-address-table

The **show mac-address-table** command can be useful when trying to locate where a device is on the network, such as a rogue Dynamic Host Configuration Protocol (DHCP) server or wireless access point (WAP). If the MAC address is known, you can issue the **show mac-address-table mac-address** command to filter the output so that only information about that MAC address is displayed. Issuing the command without the *mac-address* parameter displays the entire MAC address table.

show version

Displaying IOS version information on a router

```
RouterA#show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IS-M), Version 12.0(7)T, RELEASE SOFTWARE (fc2)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Tue 07-Dec-99 02:21 by phanguye
Image text-base: 0x80008088, data-base: 0x80C524F8

ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)

Router uptime is 5 minutes
System returned to ROM by reload
System image file is "flash:c2600-is-mz.120-7.T"

cisco 2611 (MPC860) processor (revision 0x202) with 26624K/6144K bytes of memory.
Processor board ID JAB046372NK (8372799384)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
2 Ethernet/IEEE 802.3 interface(s)
2 Serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash partition 1 (Read/Write)
8192K bytes of processor board System flash partition 2 (Read/Write)

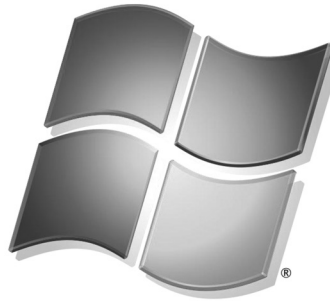
Configuration register is 0x2102
```

show version

The **show version** command provides information about the version of IOS that is running on a Cisco device. You can also use **show version** to determine whether enough random-access memory (RAM) exists on the device to support an IOS upgrade and to view the configuration register, which determines the order of the device boot process.

Windows Information-Gathering Tools

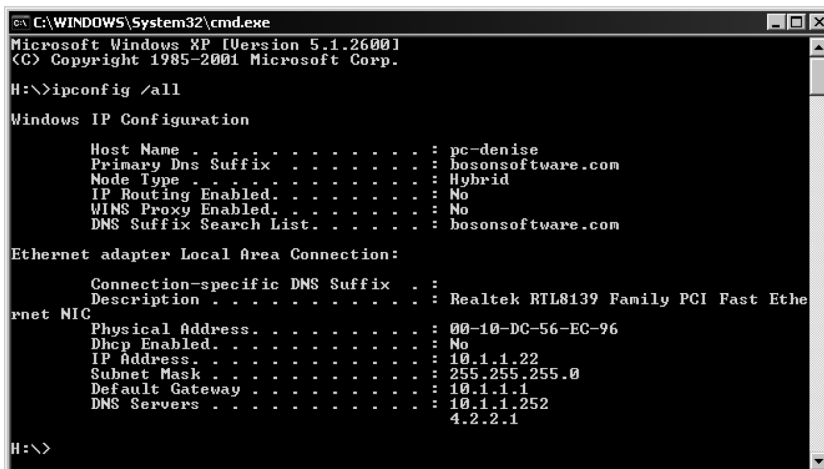
- **ipconfig /all**
- **arp -a**
- **tracert -d**
- **route print**



Windows Information-Gathering Tools

Complete disaster recovery documentation means that you should gather information about servers and end-user devices, not only the devices that are responsible for the network itself. Therefore, you should know how to gather important data from a variety of hardware and software. Many organizations use Microsoft Windows as both a server and a client operating system (OS). Therefore, you should know how to obtain network addressing and location information from Windows devices.

ipconfig /all



```
C:\WINDOWS\System32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

H:\>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : pc-denise
    Primary Dns Suffix . . . . . : bosonsoftware.com
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
    DNS Suffix Search List. . . . . : bosonsoftware.com

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . . :
    Description . . . . . : Realtek RTL8139 Family PCI Fast Eth
ernet NIC
    Physical Address. . . . . : 00-10-DC-56-EC-96
    Dhcp Enabled. . . . . : No
    IP Address. . . . . : 10.1.1.22
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.1.1.1
    DNS Servers . . . . . : 10.1.1.252
                           4.2.2.1

H:\>
```

ipconfig /all

The **ipconfig** command is a Windows command that is used to display a Windows computer's IP settings. Issuing the **ipconfig** command with the **/all** switch displays information about the computer's network interfaces, including the interface name, description, MAC address, IP address, subnet mask, default gateway, and Domain Name System (DNS) servers configured on the computer. You can also use **ipconfig /all** to determine whether a Windows computer has obtained its IP address by using DHCP. The **ipconfig** command supports several other switches that can be useful for troubleshooting, including the **/release** and **/renew** switches, which release and attempt to renew DHCP leases.

arp -a

```
Command Prompt
C:\>arp -a
Interface: 10.1.1.189 --- 0x2
Internet Address      Physical Address      Type
10.1.1.249            00-90-27-16-f0-4a    dynamic
10.1.1.252            00-04-75-e2-ff-91    dynamic
C:\>arp /?
Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr]

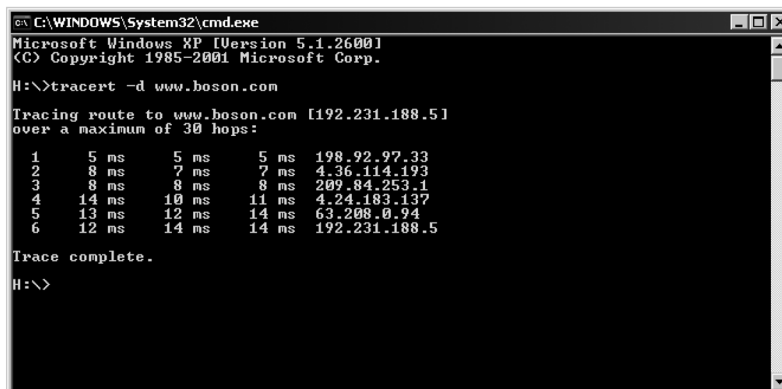
-a          Displays current ARP entries by interrogating the current
           protocol data.  If inet_addr is specified, the IP and Physical
           addresses for only the specified computer are displayed.  If
           more than one network interface uses ARP, entries for each ARP
           table are displayed.
-g          Same as -a.
inet_addr  Specifies an internet address.
-N if_addr Displays the ARP entries for the network interface specified
           by if_addr.
-d          Deletes the host specified by inet_addr.  inet_addr may be
           wildcarded with * to delete all hosts.
-s          Adds the host and associates the Internet address inet_addr
           with the Physical address eth_addr.  The Physical address is
           given as 6 hexadecimal bytes separated by hyphens.  The entry
           is permanent.
eth_addr   Specifies a physical address.
if_addr    If present, this specifies the Internet address of the
           interface whose address translation table should be modified.
           If not present, the first applicable interface will be used.

Example:
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Adds a static entry.
> arp -a          .... Displays the arp table.
```

arp -a

The **arp -a** command is a Windows command that displays the contents of the ARP cache. The ARP cache contains a list of the MAC addresses with which the local computer has recently communicated and the IP address associated with each MAC address. Therefore, the ARP cache is useful for determining the MAC addresses of other devices with which the local computer has recently communicated.

tracert -d



```
C:\WINDOWS\System32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

H:\>tracert -d www.boson.com

Tracing route to www.boson.com [192.231.188.5]
over a maximum of 30 hops:
  0  5 ms    5 ms    5 ms   198.92.97.33
  1  8 ms    7 ms    7 ms   4.36.114.193
  2  8 ms    8 ms    8 ms   209.84.253.1
  3  14 ms   10 ms   11 ms   4.24.183.137
  4  13 ms   12 ms   14 ms   63.208.0.94
  5  12 ms   14 ms   14 ms   192.231.188.5

Trace complete.

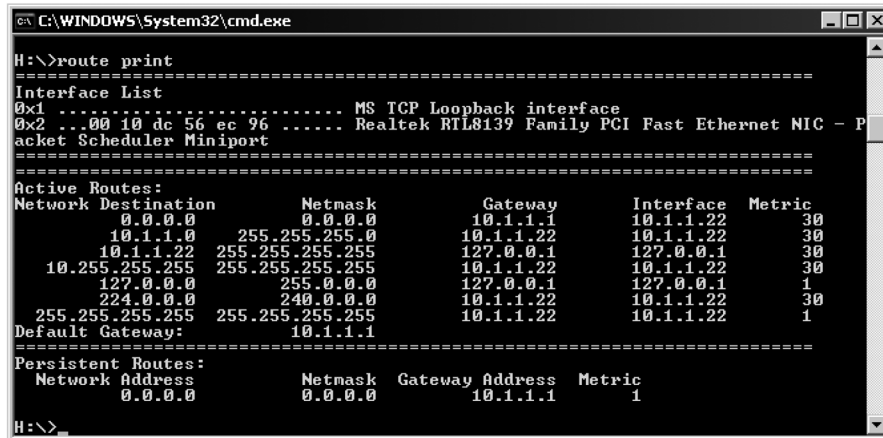
H:\>
```

tracert -d

The **tracert** command on Windows is similar to the **traceroute** command on Cisco devices. It can be used to determine the route taken by packets across an IP network as well as to troubleshoot router or bridge functionality. By default, Tracert attempts to use DNS to resolve IP addresses to host names along the path to the destination. Issuing the command with the **-d** switch disables that functionality. Tracert performs faster without the name resolution overhead.

Tracert sends Internet Control Message Protocol (ICMP) Echo packets to a destination on the network and then examines the Time Exceeded Messages (TEMs) returned by intermediate routers as well as the Echo Reply message returned by the destination. The **tracert** command can locate any potentially faulty routers or connections by determining where the packet has stopped on the network.

route print



```
C:\WINDOWS\System32\cmd.exe
H:\>route print
=====
Interface List
0x1 ..... MS TCP Loopback interface
0x2 ..00 10 dc 56 ec 96 ..... Realtek RTL8139 Family PCI Fast Ethernet NIC - P
acket Scheduler Miniport
=====
Active Routes:
Network Destination    Netmask          Gateway          Interface        Metric
0.0.0.0                0.0.0.0         10.1.1.1        10.1.1.22        30
10.1.1.0              255.255.255.0   10.1.1.22      10.1.1.22        30
10.1.1.22             255.255.255.255 127.0.0.1      127.0.0.1        30
10.255.255.255       255.255.255.255 10.1.1.22      10.1.1.22        30
127.0.0.0            255.0.0.0       127.0.0.1      127.0.0.1         1
224.0.0.0            240.0.0.0       10.1.1.22      10.1.1.22         30
255.255.255.255     255.255.255.255 10.1.1.22      10.1.1.22         1
Default Gateway:      10.1.1.1
=====
Persistent Routes:
Network Address        Netmask          Gateway Address  Metric
0.0.0.0                0.0.0.0         10.1.1.1         1
H:\>
```

route print

The **route** command displays and allows manipulation of routing tables stored on the local Windows device. When the **route** command is issued with the **print** command, the Windows device displays a list of the device's interfaces, the routing table, and persistent, or static, routes that have been configured on the device, such as a default gateway to the Internet. The routing table uses both IP version 4 (IPv4) and IP version 6 (IPv6) routes and includes the destination address, subnet mask, gateway, interface address, and metric for each route.

Mac OS, UNIX, and Linux Information-Gathering Tools

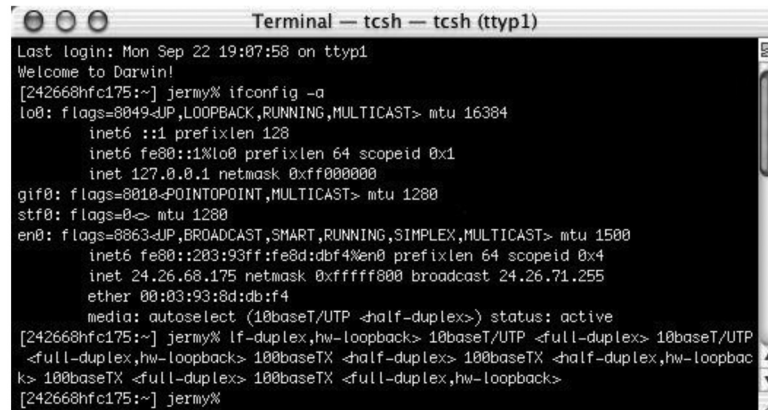
- **ifconfig -a**
- **traceroute**
- **route -n**



Mac OS, UNIX, and Linux Information-Gathering Tools

Although Windows computers are the dominant end-user devices in many industries, others use a more heterogeneous environment that might contain both Windows systems and Portable Operating System Interface (POSIX)-compliant systems, such as Mac OS, UNIX, and Linux.

ifconfig -a



```
Terminal — tcsh — tcsh (tty1)
Last login: Mon Sep 22 19:07:58 on tty1
Welcome to Darwin!
[242668hfc175:~] jerry% ifconfig -a
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
    inet6 ::1 prefixlen 128
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
    inet 127.0.0.1 netmask 0xffff0000
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    inet6 fe80::203:93ff:fe8d:dbf4%en0 prefixlen 64 scopeid 0x4
    inet 24.26.68.175 netmask 0xfffff800 broadcast 24.26.71.255
    ether 00:03:93:8d:db:f4
    media: autoselect (10baseT/UTP <-half-duplex>) status: active
[242668hfc175:~] jerry% if-duplex,hw-loopback> 10baseT/UTP <-full-duplex> 10baseT/UTP
<-full-duplex,hw-loopback> 100baseTX <-half-duplex> 100baseTX <-half-duplex,hw-loopbac
k> 100baseTX <-full-duplex> 100baseTX <-full-duplex,hw-loopback>
[242668hfc175:~] jerry%
```

ifconfig -a


The **ifconfig** command with the **-a** parameter is similar to the Windows **ipconfig** command with the **/all** switch. The **ipconfig -a** command displays a list of network interfaces along with information about the interface, such as its name, type, description, MAC address, network address, and status. The **ifconfig -a** command works similarly across Mac OS, Linux, and other POSIX-compliant OSes.

```
tracert
Terminal - tcsh - tcsh (tty1)
Last login: Mon Sep 22 08:30:15 on console
Welcome to Darwin!
[242668hfc175:~] jerry% traceroute www.boson.com
traceroute to www.boson.com (192.231.188.5), 30 hops max, 48 byte packets
 1  10.97.144.1 (10.97.144.1)  7.239 ms  10.127 ms  0.864 ms
 2  atm0-0-803.tamp1er1-rt11.tampobay.rr.com (65.32.111.22)  9.082 ms  9.4 ms  34.381 ms
 3  srp0-0.tamp1er1-rt11.tampobay.rr.com (65.32.9.228)  17.457 ms  13.283 ms  20.847 ms
 4  pop2-tby-p0-1.atdn.net (66.185.136.185)  9.37 ms  11.88 ms  28.287 ms
 5  bb1-tby-p0-1.atdn.net (66.185.136.176)  13.62 ms  10.617 ms  8.694 ms
 6  bb2-atm-p7-0.atdn.net (66.185.152.245)  26.875 ms  45.838 ms  28.335 ms
 7  pop2-atm-p5-0.atdn.net (66.185.138.43)  25.741 ms  27.74 ms  26.761 ms
 8  so-1-0.hsai.atlanta2.level3.net (66.185.138.34)  26.409 ms  25.794 ms  34.515 ms
 9  so-4-1-0.bbr1.atlanta1.level3.net (209.247.9.165)  27.85 ms  31.076 ms  28.284 ms
10  so-3-0-0.mp2.tampa1.level3.net (209.247.11.198)  68.259 ms  65.209 ms  56.632 ms
11  unknown.level3.net (64.159.1.158)  96.278 ms  62.373 ms  69.352 ms
12  unknown.level3.net (63.208.0.94)  58.997 ms  58.293 ms  58.556 ms
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
[242668hfc175:~] jerry%
```

traceroute

The **traceroute** command on a POSIX-compliant end-user device is similar to the Cisco **traceroute** command and the Microsoft Windows **tracert** command. It is used to determine the route taken by packets across an IP network as well as to troubleshoot router or bridge functionality. Also similar to Windows, DNS name resolution is typically on by default. To disable name resolution along the path to the destination, you should issue the **traceroute** command with the **-n** parameter.

route -n



```
Terminal — tcsh — tcsh (tty2)
Last login: Mon Sep 22 19:04:32 on tty2
Welcome to Darwin!
[242668hfc175:~] jermy% route -n get www.boson.com
route to: 192.231.188.5
destination: default
mask: default
gateway: 24.26.64.1
interface: en0
flags: <UP,GATEWAY_DONE,STATIC,PRCLONING>
recvpipe sendpipe ssthresh rtt,msec rttvar hopcount mtu expire
      0      0      0      0      0      0      1500      0
[242668hfc175:~] jermy%
```

route -n

On Mac OS devices, the **route** command is used to obtain information about a route to a specific destination. For example, issuing the command **route -n get www.boson.com** retrieves the IP address, subnet mask, and gateway used to reach the destination IP address that resolves to **www.boson.com**. Issuing the command with the **-n** parameter disables DNS name resolution.

It is important to note that the **route** command might not work the same way that other POSIX-compliant systems work. For example, many Linux and other Berkeley Software Distribution (BSD) UNIX systems allow you to display or modify the kernel routing table by issuing the **route** command without parameters. Mac OS does not allow you to issue the command without parameters. To see the kernel routing table on a Mac OS device, you should issue the **netstat -nr** command, which displays the routing table and disables DNS name resolution.

Review Question 1

Which of the following is not one of the three phases of recovery?

- A. activation
- B. execution
- C. reconstitution
- D. installation

Review Question 1

Which of the following is not one of the three phases of recovery?

- A. activation
- B. execution
- C. reconstitution
- D. installation**

Of the available choices, installation is not one of the three phases of recovery. There are three phases of the disaster recovery process:

- Activation
- Execution
- Reconstitution

The activation phase of disaster recovery is the phase in which the effects of a disaster are examined and reported. This phase is critical for comprehending the scope of the disaster and communicating the effects through appropriate channels within an organization.

The execution phase of disaster recovery is the phase in which the deployment of planned procedures for mitigating the effects of a disaster occur. For example, you might need to replace destroyed hardware during the execution phase of a disaster recovery plan. In that case, your organization's execution plan would need to have clear documentation regarding how to obtain replacement hardware, what software is installed on the given hardware, what licenses the organization has for the given software, and how to install the hardware and software.

The reconstitution phase of disaster recovery is the phase in which the execution phase completes. In this phase, the organization is considered restored and normal operations can resume.

Review Question 2

Which of the following is not a Microsoft Windows troubleshooting command?

- A. ipconfig /all**
- B. arp -a**
- C. traceroute -n www.boson.com**
- D. route print**

Review Question 2

Which of the following is not a Microsoft Windows troubleshooting command?

- A. `ipconfig /all`
- B. `arp -a`
- C. `tracert -n www.boson.com`**
- D. `route print`

Of the available choices, the **`tracert -n www.boson.com`** command is not a Microsoft Windows troubleshooting command. However, the **`tracert`** command on a Portable Operating System Interface (POSIX)-compliant end-user device is similar to the Microsoft Windows **`tracert`** command. It is used to determine the route taken by packets across an IP network as well as to troubleshoot router or bridge functionality. Also similar to Windows, Domain Name System (DNS) name resolution is typically on by default. To disable name resolution along the path to the destination, you should issue the **`tracert`** command with the **`-n`** parameter.

Index

Symbols

3DES (Triple Data Encryption Standard), 65, 201
 802.1D, 249, 251, 256, 257, 264–266
 802.1Q, 257, 276, 284, 285, 287, 306, 318
 802.1Q trunking, 276
 802.1s, 256, 260
 802.1w, 251, 253, 256, 259, 264–266
 802.1X, 207
 802.3ad, 323

A

AAA (Authentication, Authorization, and Accounting), 82, 180, 195, 196, 205–213
 ABR (area border router), 515
 ACK bit, 106
 ACL (access control list), 102, 111, 120, 122, 148, 157, 159, 167, 170, 176, 180, 204, 213–228, 230, 232, 348, 358, 376, 385, 391, 392, 395, 405, 407, 409, 453–455, 481, 522
 ACL sequencing, 223
 AD (administrative distance), 390, 404, 407, 480
 Address translation, 163, 166, 169
 AES (Advanced Encryption Standard), 65
 Application layer, 41, 43, 88, 104, 107
 Archive configuration mode, 8
 ARP (Address Resolution Protocol), 14, 96, 143, 330, 360
 ARP cache, 22, 143
 ARP poisoning, 143
 ARP replies, 143
 ARP requests, 14, 100, 360, 363, 365, 368
 ARP table, 14, 100
 AS (autonomous system), 11, 69, 394, 427, 444
 ASBR (autonomous system boundary router), 389
 ASN (autonomous system number), 73, 446, 481
 AuthNoPriv, 65
 AuthPriv, 65
 AUX (auxiliary), 193
 Availability, 2, 5, 59, 60, 276, 476
 AVF (active virtual forwarder), 360–366, 368, 372
 AVF states

- Active, 364
- Disabled, 364
- Initial, 364
- Listen, 364

 AVG (active virtual gateway), 360–363, 365–369, 372, 375
 AVG states

- Active, 361
- Disabled, 361
- Initial, 361
- Listen, 361

Speak, 361
 Standby, 361

B

BackboneFast, 238, 265, 266
 BGP (Border Gateway Protocol), 394, 426
 BID (bridge ID), 237, 242, 244–246, 258
 Binary, 215, 322
 Boson lab exercises, 89, 177, 233, 309, 381, 423, 545, 546, 551–553
 Bottom up troubleshooting technique, 43, 76, 88
 BPDU (bridge protocol data unit), 242, 244, 248–250, 252–255, 257, 261, 262, 265–269
 BPDU filter, 238, 268
 BPDU guard, 238, 267, 301
 BPDU packets, 252
 Brute-force attacks, 199
 BSD (Berkeley Software Distribution), 28

C

CAM (Content Addressable Memory), 368
 CCNP (Cisco Certified Network Professional), 548
 CDP (Cisco Discovery Protocol), 15, 49, 118, 125–128, 130–133, 174
 CDT (Central Daylight Time), 153
 Cisco FlowAnalyzer, 68
 Cisco IOS, 7, 13, 38, 40, 47, 86, 137, 187, 194, 195, 199, 201, 412
 Cisco NetFlow Collector, 68
 Cisco STP Toolkit, 238, 241, 263, 301
 Cisco Technical Assistance Center, 81, 82
 Cisco Technical Support, 50, 240
 CLI (command-line interface), 13, 48, 121, 123, 187, 196, 200, 454
 Commands

- aaa accounting, 212
- aaa authentication, 208, 209, 211
- aaa authorization, 212
- aaa group server radius, 209
- aaa group server tacacs+, 211
- aaa new-model, 196, 208
- access-list, 111, 167, 170, 195, 217, 218, 220–224, 228, 230, 232, 483
- address ipv4, 209, 210
- address prefix, 139
- archive, 8
- area virtual-link, 515
- arp -a, 22, 96
- banner, 183
- banner exec, 186
- banner incoming, 186
- banner login, 184

- banner motd, 185
- cdp enable, 126
- cdp run, 126
- channel-group mode, 378
- clear ip dhcp binding, 136
- clear ip dhcp conflict, 135
- clear ip nat translations, 159
- clear line, 204
- clock set, 153
- clock summer-time, 153
- clock timezone, 153
- commands, 196
- configure replace, 9, 120–124
- configure revert, 123
- copy, 6, 7, 120
- copy running-config ftp, 6
- copy running-config startup-config, 299
- copy tftp flash, 9
- crypto key generate rsa, 7, 200
- debug, 34, 47, 50–52
- debug condition, 50, 51
- debug ip nat, 159
- debug ip routing, 387
- debug ppp authentication, 51
- debug radius, 213
- debug spanning-tree events, 240
- debug tacacs+, 213
- default-metric, 395
- default-router, 140
- deny, 225
- disable, 194
- distance, 404, 405
- distribute-list, 392
- dns-server, 112, 140
- domain-name, 140
- duplex, 79
- enable, 194
- enable password, 202
- enable secret, 202
- enable view, 196
- encapsulation dot1q, 317
- end, 261
- errdisable recovery cause, 267, 303
- errdisable recovery cause bpduguard, 267
- errdisable recovery interval, 267, 300, 303
- exit, 194
- frequency, 60
- glbp authentication md5 key-string, 373
- glbp authentication text, 373
- glbp ip, 369
- glbp load-balancing, 370, 375
- glbp preempt, 369, 375
- glbp priority, 369, 375
- glbp timers, 371
- glbp weighting, 372
- glbp weighting track decrement, 372
- help, 194
- icmp-echo, 60
- ifconfig, 26
- instance vlan, 262
- interface, 317, 412
- interface range, 326, 378
- ip access-group, 226, 227
- ip access-list extended, 221, 222
- ip access-list standard, 217, 218, 224
- ip address, 94, 317, 342, 412–414, 516
- ipconfig, 21, 26, 137
- ip dhcp excluded-address, 135, 139
- ip dhcp pool, 139
- ip dhcp snooping, 144
- ip dns server, 147
- ip domain lookup, 112, 146
- ip domain name, 7, 146, 200
- ip flow, 70
- ip flow-export, 70
- ip ftp password, 6
- ip ftp username, 6
- ip host, 112, 147
- ip http-server, 201
- ip http secure-server, 201
- ip name-server, 112, 146
- ip nat inside, 161, 165, 167, 170
- ip nat outside, 161, 170
- ip nat pool, 167
- ip route, 315, 516
- ip scp server enable, 7
- ip sla schedule, 60
- ip ssh authentication-retries, 7
- ip ssh time-out, 7
- ip ssh version, 200, 201
- ipv6 address autoconfig, 141, 142
- ipv6 address dhcp, 142
- ipv6 host, 112, 147
- ipv6 nd other-config-flag, 140
- key, 210
- lldp enable, 127
- lldp run, 127
- logging console, 50, 54, 190, 191
- logging host, 52, 191
- logging trap, 54, 191
- login, 193
- login local, 197
- logout, 194
- match metric, 403
- monitor session, 57, 58
- name, 261
- netstat, 28
- network, 139

- ntp authenticate, 155
- ntp authentication-key, 155
- ntp master, 154
- ntp server, 153–155, 189
- ntp trusted-key, 155
- parser view, 196
- passive-interface, 388, 420, 483, 522
- password, 193, 196
- path, 8
- permit, 218, 222, 225, 230
- ping, 34, 37–40, 43, 44, 47, 59, 76, 77, 86, 88, 96, 97, 103, 110, 112, 148, 414, 415
- port, 210
- privilege, 194
- radius server, 208, 209
- redistribute, 389, 391, 397
- redistribute eigrp, 399
- redistribute metric, 395, 397, 398, 400
- redistribute ospf, 401
- redistribute rip, 400, 403
- redistribute route-map, 395
- release dhcp, 137
- reload, 9, 121, 122
- renew dhcp, 137
- revision, 261
- route, 24, 28
- router eigrp, 400, 483, 484, 486, 496, 506
- router ospf, 49, 398, 514, 516
- rule, 195
- secret, 196
- secure boot-config, 187
- secure boot-image, 187
- security password, 199
- server name, 209, 211
- service dhcp, 139
- service password-encryption, 193, 197, 203
- service tcp-small-servers, 200
- service timestamps, 52, 189
- service udp-small-servers, 200
- show, 34
- show access-lists, 159, 167, 170, 228, 407
- show archive, 9, 124
- show cdp, 128
- show cdp entry, 131
- show cdp interface, 128, 129
- show cdp neighbors, 15, 49, 130, 131
- show cdp traffic, 132, 133
- show clock, 152, 154
- show controllers, 49
- show debug condition, 51
- show errdisable detect, 302
- show errdisable recovery, 303, 304
- show etherchannel, 321, 322, 327, 328
- show file information, 49
- show file systems, 49
- show flash, 49
- show glbp, 374, 375
- show hosts, 147
- show interfaces, 16, 48, 49, 57, 78–80, 94, 111, 269, 271, 272, 275, 280, 295, 321, 416
- show ip access-lists, 111, 228
- show ip cache flow, 72
- show ip cache verbose flow, 72, 73
- show ip dhcp, 135, 136, 144
- show ip flow export, 71
- show ip flow interface, 71
- show ip interface, 416
- show ip interface brief, 49, 98, 280
- show ip nat statistics, 158
- show ip nat translations, 159, 165, 168, 170
- show ip ospf neighbors, 515
- show ip ospf virtual-links, 515
- show ip protocols, 101, 319, 407, 444, 477, 493, 509, 522
- show ip route, 17, 48, 49, 98, 316, 319, 386, 402, 406, 415, 480, 493, 510, 532
- show ip sla configuration, 62
- show ip sla statistics, 62
- show ip ssh, 200, 201
- show ipv6 access-lists, 111, 228
- show ipv6 interface, 49, 111
- show ipv6 interface brief, 49
- show ipv6 route, 49, 98, 472, 505
- show line, 204
- show lldp entry, 131
- show lldp interface, 129
- show lldp neighbors, 130, 131
- show lldp traffic, 132, 133
- show logging, 53, 191
- show mac-address-table, 18, 96, 280, 295
- show parser view, 196
- show pending, 261
- show port-security, 295
- show privilege, 194
- show role, 195
- show route-map, 407
- show running-config, 49, 147, 202, 203, 257, 259, 260, 327, 496, 522
- show snmp, 65
- show spanning-tree, 48, 237–239, 257, 259, 260, 264–268
- show standby, 346, 347
- show startup-config, 49
- show tech-support, 81, 82
- show udd, 270
- show user-account, 198
- show users, 198
- show version, 19, 49

- show vlan, 280, 286
- show vrrp, 357
- show vtp status, 286
- shutdown, 78, 300, 301, 321, 410
- snmp-server community, 64
- snmp-server contact, 64
- snmp-server enable traps, 66, 67
- snmp-server engineID, 65
- snmp-server host, 64, 65, 66
- snmp-server location, 64
- spanning-tree backbonefast, 265
- spanning-tree bpduguard enable, 267
- spanning-tree guard loop, 269
- spanning-tree link-type point-to-point, 252
- spanning-tree loopguard default, 269
- spanning-tree mode, 253, 257, 259, 260
- spanning-tree mode rapid-pvst, 253, 259
- spanning-tree mst configuration, 239, 261
- spanning-tree portfast, 266
- spanning-tree portfast bpduguard default, 268
- spanning-tree portfast bpduguard enable, 268
- spanning-tree portfast bpduguard default, 267
- spanning-tree portfast default, 266
- spanning-tree uplinkfast, 264
- spanning-tree vlan, 238, 246, 250
- speed, 79
- ssh, 201
- standby authentication md5 key-string, 345
- standby authentication text, 345
- standby ip, 335
- standby preempt, 336, 338, 347
- standby priority, 336
- standby timers, 335
- standby track, 338
- standby track decrement, 340
- standby version, 331
- switchport access vlan, 278
- switchport mode access, 278
- switchport mode dynamic auto, 279
- switchport mode dynamic desirable, 278
- switchport mode trunk, 276, 278
- switchport nonegotiate, 279
- switchport port-security, 298
- switchport port-security mac-address, 298, 299, 308
- switchport port-security maximum, 298, 308
- switchport port-security violation, 298, 300
- switchport trunk allowed vlan, 276, 277, 285, 294
- switchport trunk encapsulation, 276
- switchport trunk native vlan, 275, 276, 285
- switchport trunk pruning vlan, 277
- tacacs server, 210, 211
- telnet, 110, 112, 114, 148, 194
- terminal monitor, 50

- time-period, 8
- traceroute, 23, 27, 32, 34, 37, 40, 45, 47, 76, 77, 86, 96, 97, 103, 112, 407, 550
- tracert, 23, 27, 32, 76
- track, 340
- track interface, 353, 372
- transport input, 201
- tunnel destination, 413
- tunnel mode, 412, 413
- tunnel source, 413
- udld enable, 270
- udld port, 270
- udld reset, 270
- username, 7, 197, 203
- username password, 208
- variance, 407
- vlan dot1q tag native, 285
- vrrp authentication md5, 356
- vrrp authentication text, 356
- vrrp ip, 352
- vrrp preempt, 352
- vrrp priority, 352
- vrrp track decrement, 353
- vtp domain, 289
- vtp mode, 291
- vtp password, 289
- vtp pruning, 294
- vtp version, 290
- write-memory, 8

CPU load, 50**CPU usage, 228****CRC (cyclic redundancy check), 16, 78****CS-MARS (Cisco Security Monitoring, Analysis, and Response System), 68****CST (Central Standard Time), 153****CST (Common Spanning Tree), 258****D****Data Link layer, 41–44, 77, 80, 88, 125****DCE (data communications equipment), 49, 79****DES (Data Encryption Standard), 65, 201****DF (do-not-fragment), 39, 414****DHCP (Dynamic Host Configuration Protocol), 18, 21, 118, 134–140, 143, 144, 176****DHCP leases, 21, 136****DHCP snooping, 143–144****DHCPv6 (Dynamic Host Configuration Protocol version 6), 139–142****DHCPv6 servers, 139, 140, 142****Disaster recovery, 1–32**

- Activation phase, 3, 30

- Execution phase, 3, 30

- Reconstitution phase, 3, 30

Distribution lists, 392
Divide and conquer troubleshooting technique, 43, 44, 76, 88
DNS (Domain Name System), 21, 23, 27, 28, 32, 38, 102, 103, 110, 112, 114, 118, 140, 142, 145–148, 150, 160, 200
DNS clients, 112, 145–148
DNS name resolution, 27, 28
DoS (Denial of Service), 344
DSP (digital signal processing), 67
DST (Daylight Saving Time), 153
DTE (data terminal equipment), 49, 79
DTP (Dynamic Trunking Protocol), 236, 278
Dynamic auto mode, 278
Dynamic desirable mode, 278, 279
Dynamic NAT, 163, 166–177

E

EIGRP (Enhanced Interior Gateway Routing Protocol), 99, 388, 393, 396, 397, 399–407, 420, 422, 426, 428, 429, 440, 453, 475–491, 493–508, 538, 542, 549, 550
Encrypted management access, 200
ERSPAN (Encapsulated Remote Switched Port Analyzer), 58
EtherChannel, 11, 320
EtherChannel Misconfiguration Guard, 238
EtherChannel On mode, 324, 378
Extended ACL configuration mode, 221, 222
Extended ACLs, 219
Extended ping mode, 38

F

Fallback timeout, 121–123
FHRP (First-Hop Redundancy Protocol), 4, 312, 349, 350, 380
Flash memory, 7, 9, 49, 82, 293
Follow the path troubleshooting technique, 45
Frame Relay, 80
FTP (File Transfer Protocol), 6–8, 140, 181, 221
Full-duplex mode, 79

G

Gateway of last resort, 98, 314–316, 474
GET-BULK operation, 66
GET-NEXT operation, 66
GETBULK, 63
GET operation, 66
GLBP (Gateway Load Balancing Protocol), 312, 359, 360, 362, 363, 365–376, 380
GLBP load balancing

Host-dependent, 366
Round-robin, 366
Weighted, 366
Global configuration mode, 6–8, 52, 54, 57, 60, 64, 126, 139, 144, 146, 147, 153–155, 184–187, 189, 195–197, 199–201, 208, 210, 212, 253, 257, 264–270, 289–291, 294, 412, 474, 484, 506, 514, 540
Global unicast addresses, 141
GPS (global positioning system), 149
GRE (Generic Routing Encapsulation), 384, 408–414, 515
GRE tunnels, 408–423

H

Half-duplex mode, 79, 252
HDLC (High-level Data Link Control), 80
Hello packets, 330, 331, 333, 334, 336, 341, 350, 351, 367, 440, 476, 478, 479, 482, 483, 496, 497, 501, 503, 511, 513, 517, 518, 522, 524, 525, 544
Hexadecimal format, 332
HMAC (Hash-based Message Authentication Code), 65
HSRP (Hot Standby Router Protocol), 312, 330–360, 367, 369, 370, 372, 373, 380
HSRP states, 341
 Active, 341
 Initial, 341
 Learn, 341
 Listen, 341
 Speak, 341
 Standby, 341
HSRPv1 (Hot Standby Router Protocol version 1), 331–335
HSRPv2 (Hot Standby Router Protocol version 2), 331–335, 367
HTTP (Hypertext Transfer Protocol), 6, 75, 103, 110, 111, 112, 114, 181, 200, 201, 221
HTTPS (Hypertext Transfer Protocol Secure), 6, 200, 201

I

ICMP (Internet Control Message Protocol), 23, 38, 86, 94, 220, 314
ICMP Destination Unreachable message, 40, 86, 104, 314
ICMP Echo packets, 23, 38, 86
ICMP Echo Reply message, 23, 38, 86
ICMP Echo requests, 59, 270
ICMP traffic, 52, 111
IDS (Intrusion Detection System), 181, 182
IEEE (Institute of Electrical and Electronics Engineers), 125, 174, 251, 256, 260, 323, 380

IETF (Internet Engineering Task Force), 207, 349, 354, 380, 443, 463
IGRP (Interior Gateway Routing Protocol), 99, 388, 393, 420, 422, 426, 542, 549
INFORM operation, 66
Inside global addresses, 159, 160, 165, 167, 170
Inside local addresses, 159, 160, 165, 171
Interface configuration mode, 70, 126, 144, 161, 252, 266–270, 275, 276, 285, 300, 331, 335, 352, 369, 370, 488, 494, 506, 514, 517, 522, 540
InterVLAN routing, 312, 317, 319
IP (Internet Protocol), 38, 479
IP addresses, 14, 23, 68, 72, 94, 95, 111, 135, 139, 140, 143, 145, 146, 156, 157, 160, 166, 167, 170, 176, 226, 352, 412, 482, 484, 507, 517, 519, 544
IPFlow, 68
IP routing, 100, 317, 318, 480
IPS (Intrusion Prevention System), 181
IPSec (IP Security), 157, 176, 410, 538
IP SLA configuration mode, 60
IP SLA Echo operation, 60
IPv4 (IP version 4), 24, 49, 93, 114, 139, 209, 331, 412, 443
IPv6 (IP version 6), 24, 38, 93, 114, 139, 426, 542, 544
ISP (Internet service provider), 4, 76, 77, 78, 338, 427
IST (internal spanning tree), 262

L

Lab exercises, 89, 177, 233, 309, 381, 423, 545, 546, 551–553
LACP (Link Aggregation Control Protocol), 322–325, 328, 378
 Active mode, 322, 325, 378
 Passive mode, 322, 325, 378
Layer 1, 41, 42, 49, 77, 78, 92, 527
Layer 2, 41, 42, 49, 58, 77, 80, 92, 119, 125, 236, 243, 277, 288, 312, 313, 317, 481, 527
Layer 3, 15, 41, 68, 77, 92–94, 96, 98, 102, 110–112, 125, 130, 145, 236, 312–314, 319, 330, 335, 369, 410, 412, 479
Layer 4, 41, 92, 102, 103, 110–112, 114, 169
Layer 5, 41
Layer 6, 41
Layer 7, 41, 103, 110, 114
Link-local address, 141
Linux, 25, 26, 28
LLDP (Link Layer Discovery Protocol), 118, 125, 127–133, 174
Logging, 188
Log severity levels, 54, 67, 190
Loop guard, 238, 269, 271

M

MAC (Media Access Control), 11, 96, 136, 242, 308, 330
MAC addresses, 14, 18, 21, 22, 26, 96, 97, 100, 143, 245, 246, 249, 252, 258, 280, 281, 295, 297–300, 308, 330, 332, 360, 362, 363, 365, 366, 368, 372, 375
Mac OS, 25, 26, 28
Many-to-many mapping, 163
Many-to-one mapping, 163
MD5 (Message Digest 5), 63, 65, 155, 202, 203, 261, 344, 345, 354–356, 373, 487–489, 538
MED (Media Endpoint Device), 125, 174
MED (multi-exit discriminator), 394, 462
MIB (management information base), 63, 64, 66
Microsoft Windows, 20, 27, 32, 38, 137
MOTD (Message-of-the-Day), 183, 185
Move the problem troubleshooting technique, 45
MST (Multiple Spanning Tree), 238, 256, 260
MST configuration mode, 261
MTU (maximum transmission unit), 409, 521
Multilayer switches, 313, 318

N

NAT (Network Address Translation), 118, 156–171, 176
NAT Transparency, 157, 176
NAT Traversal, 157, 176
NBMA (nonbroadcast multiaccess), 517, 523
NetFlow, 34, 56, 68–72, 74, 75
NetFlow Monitor, 68
NetSim labs, 89, 177, 233, 309, 381, 423, 545, 546, 551–553
Network layer, 41, 43, 44, 76, 77, 88, 93, 94, 445
NIC (network interface card), 42
NMS (network management system), 66
NoAuthNoPriv, 65
NTP (Network Time Protocol), 118, 149–155, 189
NTP clients, 149–155
NTP servers, 149–155, 189
NTP stratum, 150, 151
NVI (NAT virtual interface), 162, 165, 167, 170
NVRAM (non-volatile random-access memory), 8, 291, 293

O

OID (object ID), 63
One-to-one mapping, 163
OS (operating system), 20, 38, 104, 145, 195
OSI (Open Systems Interconnection), 41–45, 76–78, 88, 92, 93, 103, 111, 312, 313, 326, 412
OSI reference model

- Application layer, 41, 43, 88, 104, 107
- Data Link layer, 41–44, 77, 80, 88, 125
- Layer 1, 41, 42, 49, 77, 78, 92, 527
- Layer 2, 41, 42, 49, 58, 77, 80, 92, 119, 125, 236, 243, 277, 288, 312, 313, 317, 481, 527
- Layer 3, 15, 41, 68, 77, 92–94, 96, 98, 102, 110–112, 125, 130, 145, 236, 312–314, 319, 330, 335, 369, 410, 412, 479
- Layer 4, 41, 92, 102, 103, 110–112, 114, 169
- Layer 5, 41
- Layer 6, 41
- Layer 7, 41, 103, 110, 114
- Network layer, 41, 43, 44, 76, 77, 88, 93, 445
- Physical layer, 41–44, 77, 78, 88, 550
- Presentation layer, 41
- Session layer, 41, 107
- Transport layer, 41, 44, 88, 92, 102–105, 107, 482

OSPF (Open Shortest Path First), 49, 98–101, 388, 393, 394, 396, 398–407, 420, 426, 428, 429, 440, 442, 482, 505, 508–533, 538, 540, 544

Outside global addresses, 159, 160, 165, 168

Outside local addresses, 159, 160, 165, 168

P

PAgP (Port Aggregation Protocol), 322–324, 378

- Auto mode, 322, 324, 378

- Desirable mode, 322, 324, 378

PAT (Port Address Translation), 156, 157, 160, 161, 163, 169, 170

Path cost, 241, 247, 248

PBR (policy-based routing), 384, 403

PDU (Protocol Data Unit), 104, 106, 107

Physical layer, 41–44, 77, 78, 88, 550

Plixer Scrutinizer, 68

PoE (Power over Ethernet), 125, 174

Point-to-point links, 252

PortFast, 238, 266, 267, 268

Port priority, 241

POSIX (Portable Operating System Interface), 25–28, 32

PPP (Point-to-Point Protocol), 51, 80

Presentation layer, 41

Privileged EXEC mode, 6–9, 13, 40, 48, 50, 51, 53, 62, 68, 78, 111, 135–137, 144, 147, 153, 154, 191, 192, 194, 196, 202, 228, 238–240, 257, 259, 264–267, 269, 270, 271, 275, 321, 327, 346, 357, 374, 461, 467, 472, 488, 512, 521, 522, 527–529

Promiscuous ports, 57

Protocol Analyzer, 81

PVRST+ (Per-VLAN Rapid Spanning Tree Plus), 256, 259, 260

PVST+ (Per-VLAN Spanning Tree Plus), 256–260

R

RADIUS (Remote Authentication Dial-In User Service), 205–213

RAM (random-access memory), 8, 19, 49, 291, 479

RBAC (role-based CLI access), 196

Redistribution, 389

Redundancy, 2, 4, 312, 321, 328, 338, 349, 359, 380

RFC (Request for Comments), 160, 349, 354

- RFC 1918, 160

- RFC 2338, 354

- RFC 3768, 349, 354

- RFC 5798, 354

RIP (Routing Information Protocol), 420, 422

RIPv2 (Routing Information Protocol version 2), 388, 428, 429, 431, 432, 436, 471

RLQ (Root Link Query), 265

Root-bridge election, 246

Root bridges, 237–239, 242–248, 250, 252, 255, 257, 258, 265, 271

Root guard, 271

Root ports, 243, 248, 252, 253, 255, 264

Root view, 196

Router-on-a-stick, 317, 318

Router configuration mode, 388, 389, 392, 397, 398, 400, 404, 448, 449, 469, 470, 484, 490, 491, 494, 506, 507, 512, 514, 516, 540

Routing loops, 390, 437

RSPAN (Remote Switched Port Analyzer), 58

RSTP (Rapid Spanning Tree Protocol), 239, 251–256, 259, 260, 264–266

RSTP port roles

- Alternate, 255

- Backup, 255

RSTP port states

- Discarding, 254

- Forwarding, 254

- Learning, 254

S

SCP (Secure Copy), 7

SCTP (Stream Control Transmission Protocol), 70, 71

Session layer, 41, 107

SHA (Secure Hash Algorithm), 63, 65

SLA (Service Level Agreement), 56, 59–62, 340

SLAAC (Stateless Address Automatic Configuration), 141, 142

Sliding windowing, 109, 116

SMTP (Simple Mail Transfer Protocol), 110, 114

SNAT (stateful Network Address Translation), 366

SNMP (Simple Network Management Protocol), 34, 300

- SNMP agents, 63–66
- SNMP community strings, 63
- SNMP manager, 66
- SNMP security levels
 - AuthNoPriv, 65
 - AuthPriv, 65
 - NoAuthNoPriv, 65
- SNMP server, 66, 67
- SNMP traps, 66
- SNMPv1 (Simple Network Management Protocol version 1), 63, 65
- SNMPv2 (Simple Network Management Protocol version 2), 63
- SNMPv2c (Simple Network Management Protocol version 2 community strings), 63, 65, 66
- SNMPv3 (Simple Network Management Protocol version 3), 63, 65, 66
- SolarWinds Orion, 68, 74
- SPAN (Switched Port Analyzer), 56–58
- Spot the difference troubleshooting technique, 46
- SSH (Secure Shell), 7, 50, 118–120, 183, 200, 201, 204
- SSH v1 (Secure Shell version 1), 200, 201
- SSH v2 (Secure Shell version 2), 200, 201
- SSL (Secure Sockets Layer), 200
- STA (Spanning Tree Algorithm), 243, 247
- Standard ACL configuration mode, 217, 218, 224
- Standard ACLs, 216
- Stateful DHCPv6, 142
- Stateless DHCPv6, 142
- Static NAT, 163, 164, 165, 166
- STP (Spanning Tree Protocol), 44, 48, 88, 236–244, 248–260, 262–269, 271, 301, 320, 328, 329, 380
- STP port states
 - Blocking, 249
 - blocking, 329
 - Disabled, 249
 - Forwarding, 249
 - Learning, 249
 - Listening, 249
- STP Toolkit, 238, 241, 263, 301
- SVF (standby virtual forwarder), 363–365
- SVG (standby virtual gateway), 360, 361, 363, 365, 368, 372, 375
- Switch priority, 241, 245, 246, 271
- SYN bit, 106
- Syslog, 34, 52, 54, 191
- Systematic approach, 35

T

- TAC (Technical Assistance Center), 81
- TACACS+ (Terminal Access Controller-Access Control System Plus), 205–208, 210, 211, 213
- TACACS+ server configuration mode, 210

- TCP (Transmission Control Protocol), 38, 69, 92, 103, 105, 106, 108–112, 114, 116, 145, 148, 157, 171, 176, 200, 207, 210, 213, 220, 222, 226, 449, 470
- TCP flags, 69
- TCP three-way handshake, 105, 106
- TC While timer, 252
- Telnet, 50, 52, 92, 103, 110, 112, 114, 118, 119, 183, 185, 186, 200, 201, 203, 204
- Telnet session, 52, 110, 112
- TEM (Time Exceeded Message), 23, 40, 86
- TFTP (Trivial File Transfer Protocol), 6, 7, 9, 121, 123, 124, 140, 193
- TLV (type, length, and value), 125, 497
- Top down troubleshooting technique, 43, 88
- ToS (Type of Service), 68, 73
- Transport layer, 41, 44, 88, 92, 102–105, 107, 482
- TRAP operation, 66
- Troubleshooting tools and techniques, 33–90
 - Consider the possibilities, 35
 - Create an action plan, 36
 - Define the problem, 35, 36, 84
 - Document the solution, 36
 - Gather facts, 35
 - Implement an action plan, 36
 - Observe results, 36
- TTL (Time To Live), 40, 86

U

- UDLD (UniDirectional Link Detection), 270–271, 301
- UDP (User Datagram Protocol), 40, 65, 66, 70, 71, 86, 92, 103–105, 138, 145, 148, 150, 157, 176, 200, 207, 209, 213, 348, 358, 376, 471
- UNIX, 25, 28
- UplinkFast, 238, 264–266
- UTC (Coordinated Universal Time), 53, 152, 153, 189

V

- Virtual forwarders, 360, 361, 372
- VLAN (virtual LAN), 11, 48, 130, 236, 306, 317
- VLAN hopping attacks, 283, 284, 306
- VLAN ID, 57, 246, 258, 274, 277, 283, 285, 369
- VLAN tagging, 284, 285, 306
- VoIP (Voice over IP), 59, 118, 125, 140
- VPN (virtual private network), 157, 176, 410, 443
- VPN checksums, 157, 176
- VRF (VPN Routing and Forwarding), 162
- VRRP (Virtual Router Redundancy Protocol), 312, 349–359, 372, 373, 380
- VSPAN (Virtual-based Switched Port Analyzer), 58
- VTP (VLAN Trunking Protocol), 15, 130, 236, 277, 281, 286–294

VTP pruning, 277, 294

**VTY (virtual terminal), 119, 193, 197, 201, 203, 204,
208, 209, 211, 212**

W

WAP (wireless access point), 18

Warning banners, 183

Wildcard masks, 215

Windowing, 108

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 2017 Boson Software, LLC. All rights reserved.