TSHOOT

300-135 Curriculum
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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>2</td>
</tr>
<tr>
<td>Objectives</td>
<td>2</td>
</tr>
<tr>
<td>Have a Plan</td>
<td>3</td>
</tr>
<tr>
<td>Build Redundancy</td>
<td>4</td>
</tr>
<tr>
<td>Ensure Availability</td>
<td>5</td>
</tr>
<tr>
<td>Manually Copying the Configuration</td>
<td>6</td>
</tr>
<tr>
<td>Manually Copying the Configuration with Encryption</td>
<td>7</td>
</tr>
<tr>
<td>Creating an Archive</td>
<td>8</td>
</tr>
<tr>
<td>Verifying Archives and Restoring Configurations</td>
<td>9</td>
</tr>
<tr>
<td>Document the Network</td>
<td>10</td>
</tr>
<tr>
<td>Topology Diagrams</td>
<td>11</td>
</tr>
<tr>
<td>Cisco Information-Gathering Tools</td>
<td>13</td>
</tr>
<tr>
<td>show arp</td>
<td>14</td>
</tr>
<tr>
<td>show cdp neighbors</td>
<td>15</td>
</tr>
<tr>
<td>show interfaces</td>
<td>16</td>
</tr>
<tr>
<td>show ip route</td>
<td>17</td>
</tr>
<tr>
<td>show mac-address-table</td>
<td>18</td>
</tr>
<tr>
<td>show version</td>
<td>19</td>
</tr>
<tr>
<td>Windows Information-Gathering Tools</td>
<td>20</td>
</tr>
<tr>
<td>ipconfig /all</td>
<td>21</td>
</tr>
<tr>
<td>arp -a</td>
<td>22</td>
</tr>
<tr>
<td>tracert -d</td>
<td>23</td>
</tr>
<tr>
<td>route print</td>
<td>24</td>
</tr>
<tr>
<td>Mac OS, UNIX, and Linux Information-Gathering Tools</td>
<td>25</td>
</tr>
<tr>
<td>ifconfig -a</td>
<td>26</td>
</tr>
<tr>
<td>traceroute</td>
<td>27</td>
</tr>
<tr>
<td>route -n</td>
<td>28</td>
</tr>
<tr>
<td>Review Question 1</td>
<td>29</td>
</tr>
<tr>
<td>Review Question 2</td>
<td>31</td>
</tr>
</tbody>
</table>

### Module 2: Troubleshooting Tools and Techniques

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>34</td>
</tr>
<tr>
<td>Objectives</td>
<td>34</td>
</tr>
<tr>
<td>Understanding the Systematic Approach</td>
<td>35</td>
</tr>
<tr>
<td>Gather Facts and Consider the Possibilities</td>
<td>37</td>
</tr>
<tr>
<td>Understanding the ping Command</td>
<td>38</td>
</tr>
<tr>
<td>Create an Action Plan</td>
<td>41</td>
</tr>
<tr>
<td>Where Does the Device Function?</td>
<td>42</td>
</tr>
<tr>
<td>Implement an Action Plan with OSI</td>
<td>43</td>
</tr>
<tr>
<td>The Bottom Up Troubleshooting Technique</td>
<td>43</td>
</tr>
</tbody>
</table>
Module 3: Troubleshooting Layer 3 and Beyond

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.
# TSHOOT Table of Contents

## Module 4: Traffic Management

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring DHCP Snooping</td>
<td>144</td>
</tr>
<tr>
<td>DNS</td>
<td>145</td>
</tr>
<tr>
<td>Configuring a DNS Client</td>
<td>146</td>
</tr>
<tr>
<td>Configuring a DNS Server</td>
<td>147</td>
</tr>
<tr>
<td>Other Causes of DNS Problems</td>
<td>148</td>
</tr>
<tr>
<td>NTP</td>
<td>149</td>
</tr>
<tr>
<td>Common Causes of NTP Problems</td>
<td>150</td>
</tr>
<tr>
<td>How NTP Stratum Works</td>
<td>151</td>
</tr>
<tr>
<td>Configuring NTP</td>
<td>152</td>
</tr>
<tr>
<td>Configuring the System Clock and NTP</td>
<td>153</td>
</tr>
<tr>
<td>Authenticating NTP Time Sources</td>
<td>155</td>
</tr>
<tr>
<td>NAT/PAT</td>
<td>156</td>
</tr>
<tr>
<td>Causes of Common NAT/PAT Problems</td>
<td>157</td>
</tr>
<tr>
<td>Commands for Troubleshooting NAT</td>
<td>158</td>
</tr>
<tr>
<td>NAT/PAT Address Terminology</td>
<td>160</td>
</tr>
<tr>
<td>Configuring Interfaces for NAT/PAT</td>
<td>161</td>
</tr>
<tr>
<td>NAT NVI Configurations</td>
<td>162</td>
</tr>
<tr>
<td>NAT Translation Methods</td>
<td>163</td>
</tr>
<tr>
<td>Configuring Static NAT</td>
<td>164</td>
</tr>
<tr>
<td>Dynamic NAT</td>
<td>165</td>
</tr>
<tr>
<td>Configuring Dynamic NAT</td>
<td>166</td>
</tr>
<tr>
<td>PAT</td>
<td>167</td>
</tr>
<tr>
<td>Configuring PAT</td>
<td>168</td>
</tr>
<tr>
<td>Review Question 1</td>
<td>173</td>
</tr>
<tr>
<td>Review Question 2</td>
<td>175</td>
</tr>
<tr>
<td>Lab Exercises</td>
<td>177</td>
</tr>
</tbody>
</table>

## Module 5: Basic Security

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>180</td>
</tr>
<tr>
<td>Objectives</td>
<td>180</td>
</tr>
<tr>
<td>Protecting Assets</td>
<td>181</td>
</tr>
<tr>
<td>Securing Cisco Devices</td>
<td>182</td>
</tr>
<tr>
<td>Warning Banners</td>
<td>183</td>
</tr>
<tr>
<td>Login Banners</td>
<td>184</td>
</tr>
<tr>
<td>MOTD Banners</td>
<td>185</td>
</tr>
<tr>
<td>EXEC Banners</td>
<td>186</td>
</tr>
<tr>
<td>Securing Configurations</td>
<td>187</td>
</tr>
<tr>
<td>Logging</td>
<td>188</td>
</tr>
<tr>
<td>Configuring Accurate Time</td>
<td>189</td>
</tr>
<tr>
<td>Configuring Log Severity Levels</td>
<td>190</td>
</tr>
<tr>
<td>Configuring and Using a Logging Server</td>
<td>191</td>
</tr>
<tr>
<td>Securing Access</td>
<td>192</td>
</tr>
</tbody>
</table>

Content in these modules is available in the full version of the curriculum. Please visit www.boson.com for more information.
Content in these modules is available in the full version of the curriculum. Please visit www.boson.com for more information.
<table>
<thead>
<tr>
<th>Understanding Cisco Implementations of STP</th>
<th>256</th>
</tr>
</thead>
<tbody>
<tr>
<td>Per-VLAN Spanning Tree Plus</td>
<td>257</td>
</tr>
<tr>
<td>PVST+ Bridge IDs</td>
<td>258</td>
</tr>
<tr>
<td>Per-VLAN Rapid Spanning Tree Plus</td>
<td>259</td>
</tr>
<tr>
<td>Multiple Spanning Tree Protocol</td>
<td>260</td>
</tr>
<tr>
<td>MST Regions</td>
<td>261</td>
</tr>
<tr>
<td>MST Instances</td>
<td>262</td>
</tr>
<tr>
<td>Cisco STP Toolkit</td>
<td>263</td>
</tr>
<tr>
<td>UplinkFast</td>
<td>264</td>
</tr>
<tr>
<td>BackboneFast</td>
<td>265</td>
</tr>
<tr>
<td>PortFast</td>
<td>266</td>
</tr>
<tr>
<td>BPDU Guard</td>
<td>267</td>
</tr>
<tr>
<td>BPDU Filter</td>
<td>268</td>
</tr>
<tr>
<td>Loop Guard</td>
<td>269</td>
</tr>
<tr>
<td>UDLD</td>
<td>270</td>
</tr>
<tr>
<td>Root Guard</td>
<td>271</td>
</tr>
<tr>
<td>Trunk Troubleshooting Commands</td>
<td>272</td>
</tr>
<tr>
<td>Troubleshooting Trunk Ports</td>
<td>274</td>
</tr>
<tr>
<td>Configuring Trunk Ports</td>
<td>275</td>
</tr>
<tr>
<td>How DTP Negotiates Trunks</td>
<td>276</td>
</tr>
<tr>
<td>Content in these modules is available in the full version of the curriculum. Please visit <a href="http://www.boson.com">www.boson.com</a> for more information.</td>
<td></td>
</tr>
<tr>
<td>VLAN Troubleshooting Commands</td>
<td>280</td>
</tr>
<tr>
<td>Troubleshooting VLANs</td>
<td>281</td>
</tr>
<tr>
<td>Common Causes of VLAN Problems</td>
<td>282</td>
</tr>
<tr>
<td>Common Causes of Native VLAN Problems</td>
<td>283</td>
</tr>
<tr>
<td>VLAN Hopping</td>
<td>284</td>
</tr>
<tr>
<td>Mitigating VLAN Hopping</td>
<td>285</td>
</tr>
<tr>
<td>VTP Troubleshooting Commands</td>
<td>286</td>
</tr>
<tr>
<td>Common Causes of VTP Problems</td>
<td>287</td>
</tr>
<tr>
<td>Understanding and Configuring VTP</td>
<td>288</td>
</tr>
<tr>
<td>VTP Domains</td>
<td>289</td>
</tr>
<tr>
<td>VTP Version</td>
<td>290</td>
</tr>
<tr>
<td>VTP Modes</td>
<td>291</td>
</tr>
<tr>
<td>VTP Operation</td>
<td>292</td>
</tr>
<tr>
<td>VTP Pruning</td>
<td>294</td>
</tr>
<tr>
<td>Port Security Troubleshooting Commands</td>
<td>295</td>
</tr>
<tr>
<td>Common Causes of Port Security Problems</td>
<td>297</td>
</tr>
<tr>
<td>Restricting Ports by MAC Address</td>
<td>298</td>
</tr>
<tr>
<td>Error-Disabled Ports</td>
<td>301</td>
</tr>
<tr>
<td>Review Question 1</td>
<td>305</td>
</tr>
<tr>
<td>Review Question 2</td>
<td>307</td>
</tr>
<tr>
<td>Lab Exercises</td>
<td>309</td>
</tr>
</tbody>
</table>
Module 7: Multilayer Switch Troubleshooting

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
  The On Mode ......................................................................................................................................... 324
  PAgP Modes .......................................................................................................................................... 324
  LACP Modes .......................................................................................................................................... 325
Troubleshooting EtherChannel ................................................................................................................ 326
  Aggregation Protocol Mismatches ......................................................................................................... 327
  Bundle Configuration Mismatches .......................................................................................................... 328
HSRP Versions ....................................................................................................................................... 330
Understanding Virtual MAC Addresses ................................................................................................. 331
HSRP Hello Packets ............................................................................................................................... 332
HSRP Hello and Hold Timers .................................................................................................................. 333
Configuring HSRP and Timers ................................................................................................................ 334
Configuring Preemption .......................................................................................................................... 335
Configuring Interface Tracking .............................................................................................................. 337
Configuring HSRP Object Tracking ....................................................................................................... 338
Understanding HSRP States .................................................................................................................... 340
Configuring Multigroup HSRP ................................................................................................................ 341
HSRP Authentication ............................................................................................................................... 342
  Configuring HSRP Authentication ........................................................................................................ 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
  Configuring VRRP Authentication ........................................................................................................ 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.
Content in these modules is available in the full version of the curriculum. Please visit www.boson.com for more information.
Content in these modules is available in the full version of the curriculum. Please visit www.boson.com for more information.
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Causes of OSPF Adjacency Problems</td>
<td>522</td>
</tr>
<tr>
<td>Troubleshooting Commands for OSPF Adjacencies</td>
<td>526</td>
</tr>
<tr>
<td>OSPF Stub Areas</td>
<td>530</td>
</tr>
<tr>
<td>Troubleshooting Commands for OSPF Stub Areas</td>
<td>531</td>
</tr>
<tr>
<td>Configuring OSPF Stub Areas</td>
<td>533</td>
</tr>
<tr>
<td>OSPFv3</td>
<td>534</td>
</tr>
<tr>
<td>Troubleshooting Commands for OSPFv3</td>
<td>535</td>
</tr>
<tr>
<td>Understanding OSPFv3</td>
<td>538</td>
</tr>
<tr>
<td>Common Causes of OSPFv3 Problems</td>
<td>539</td>
</tr>
<tr>
<td>Configuring OSPFv3</td>
<td>540</td>
</tr>
<tr>
<td>Review Question 1</td>
<td>541</td>
</tr>
<tr>
<td>Review Question 2</td>
<td>543</td>
</tr>
<tr>
<td>Lab Exercises</td>
<td>545</td>
</tr>
<tr>
<td>Module 10: Preparing for the TSHOOT Exam</td>
<td>547</td>
</tr>
<tr>
<td>Overview</td>
<td>548</td>
</tr>
<tr>
<td>Objectives</td>
<td>548</td>
</tr>
<tr>
<td>Preparing for the TSHOOT Exam</td>
<td>549</td>
</tr>
<tr>
<td>Content in these modules is available in the full version of the</td>
<td>551</td>
</tr>
<tr>
<td>curriculum. Please visit <a href="http://www.boson.com">www.boson.com</a> for more information.</td>
<td>555</td>
</tr>
</tbody>
</table>
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

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

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

<table>
<thead>
<tr>
<th>Configuring an IP domain name</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>RouterA(config)#ip domain boson.com</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuring a user name and password</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>RouterA(config)#username admin privilege 15 password mysshpw</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuring SSH</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>RouterA(config)#crypto key generate rsa</code></td>
</tr>
<tr>
<td><code>RouterA(config)#ip ssh time-out 90</code></td>
</tr>
<tr>
<td><code>RouterA(config)#ip ssh authentication-retries 3</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Enabling SCP</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>RouterA(config)#ip scp server enable</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Copying a file from flash memory to a remote SSH server</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>RouterA#copy flash: scp:</code></td>
</tr>
<tr>
<td>Source filename [?]: <code>backup.txt</code></td>
</tr>
<tr>
<td>Address or name of remote host [?]: <code>192.168.51.50</code></td>
</tr>
<tr>
<td>Destination username [Router]? <code>secure</code></td>
</tr>
<tr>
<td>Destination filename [backup.txt]?</td>
</tr>
<tr>
<td>Writing <code>backup.txt</code></td>
</tr>
<tr>
<td>Password:</td>
</tr>
</tbody>
</table>

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 mysshpw** creates a user named admin that has a password of mysshpw 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

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` 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

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.
Topography 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

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.
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

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 0000.1234.5678
    Internet address is 10.10.10.1/24
    MTU 1500 bytes, BWM 100000 Kbit, SLT 1000 usec, rely 255/255, load 1/255
    Encapsulation ARPA, loopback not set, keepalive set (10 sec)
    Auto-negot, Auto-speed
    Last input 0:00:00, 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
    Queuing 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, 21282138 bytes, 0 no buffer
    Received 91361 broadcasts, 0 runs, 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, 1492789 bytes, 0 underrun
    0 output errors, 1 collisions, 5 interface resets
    0 packets, 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

<table>
<thead>
<tr>
<th>Interface</th>
<th>Status</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/0</td>
<td>up</td>
<td>up</td>
<td>To Internet</td>
</tr>
<tr>
<td>Fa0/1</td>
<td>up</td>
<td>up</td>
<td>To LAN</td>
</tr>
</tbody>
</table>

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 is 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 [10/1] 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

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.

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Mac Address</th>
<th>Type</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>000c.0908.7866</td>
<td>DYNAMIC</td>
<td>Fa0/2</td>
</tr>
<tr>
<td>1</td>
<td>000c.3962.6232</td>
<td>DYNAMIC</td>
<td>Fa0/1</td>
</tr>
</tbody>
</table>
show version

Displaying IOS version information on a router

Router#show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-12-M), Version 12.0(7)T, RELEASE SOFTWARE (fc2)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Tue 07-Dec-99 02:12 by phanque
Image text-base: 0x60000000, data-base: 0x80C524F0
ROM: System Bootstrap, Version 11.3(2)XX4, RELEASE SOFTWARE (fc1)

Router uptime is 5 minutes
System returned to ROM by reload
System image file is "Flash:2600-1a-mz.120-7.7"
cisco 2611 (MPC60) processor (revision 0x202) with 26624K/6144K bytes of memory.
Processor Board ID JMA06372926 (0375799384)
M680 processor; part number 0, mask 49
BRIDGING software,
X.25 software, Version 3.0.0.
2 Ethernet/IEEE 802.3 interface(s)
2 Serial/async/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.
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.
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.
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

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.
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.
The `ifconfig -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.
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

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
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`
Of the available choices, the **traceroute -n www.boson.com** command is not a Microsoft Windows troubleshooting command. However, the **traceroute** 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 **traceroute** 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 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

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
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 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 dhcp, 142
ipv6 address dhcp, 142
ipv6 address dhcp, 142
ipv6 address dhcp, 142
ipv6 host, 112, 147
ipv6 nd other-config-flag, 140
ipv6 nd other-config-flag, 140
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

© 2017 Boson Software, LLC
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
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 errdisnable detect, 302
show errdisnable 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 udl, 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 bd_pduguard 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 bpdusfilter default, 268
spanning-tree portfast bpdusfilter enable, 268
spanning-tree portfast bd_pduguard 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
trace route, 23, 27, 32, 34, 37, 40, 45, 47, 76, 77, 86, 96, 97, 103, 112, 407, 550
tracert, 23, 27, 32, 76
tunnel destination, 413
tunnel module, 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
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
Hexadecimal format, 332
HMAC (Hash-based Message Authentication Code), 65
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

M
MAC (Media Access Control), 11, 96, 136, 242, 308, 330
Mac OS, 25, 26, 28
Many-to-many mapping, 163
Many-to-one mapping, 163
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
NST (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
<table>
<thead>
<tr>
<th>P</th>
<th>S</th>
</tr>
</thead>
<tbody>
<tr>
<td>PAgP (Port Aggregation Protocol), 322–324, 378</td>
<td>SCP (Secure Copy), 7</td>
</tr>
<tr>
<td>Auto mode, 322, 324, 378</td>
<td>SCTP (Stream Control Transmission Protocol), 70, 71</td>
</tr>
<tr>
<td>Desirable mode, 322, 324, 378</td>
<td>Session layer, 41, 107</td>
</tr>
<tr>
<td>PAT (Port Address Translation), 156, 157, 160, 161, 163, 169, 170</td>
<td>SHA (Secure Hash Algorithm), 63, 65</td>
</tr>
<tr>
<td>Path cost, 241, 247, 248</td>
<td>SLA (Service Level Agreement), 56, 59–62, 340</td>
</tr>
<tr>
<td>PBR (policy-based routing), 384, 403</td>
<td>SLAAC (Stateless Address Automatic Configuration), 141, 142</td>
</tr>
<tr>
<td>PDU (Protocol Data Unit), 104, 106, 107</td>
<td>Sliding windowing, 109, 116</td>
</tr>
<tr>
<td>Physical layer, 41–44, 77, 78, 88, 550</td>
<td>SMTP (Simple Mail Transfer Protocol), 110, 114</td>
</tr>
<tr>
<td>Plixer Scrutinizer, 68</td>
<td>SNAT (stateful Network Address Translation), 366</td>
</tr>
<tr>
<td>PoE (Power over Ethernet), 125, 174</td>
<td>SNMP (Simple Network Management Protocol), 34, 300</td>
</tr>
<tr>
<td>Point-to-point links, 252</td>
<td>R</td>
</tr>
<tr>
<td>PortFast, 238, 266, 267, 268</td>
<td>RADIUS (Remote Authentication Dial-In User Service), 205–213</td>
</tr>
<tr>
<td>Port priority, 241</td>
<td>RAM (random-access memory), 8, 19, 49, 291, 479</td>
</tr>
<tr>
<td>POSIX (Portable Operating System Interface), 25–28, 32</td>
<td>RBAC (role-based CLI access), 196</td>
</tr>
<tr>
<td>PPP (Point-to-Point Protocol), 51, 80</td>
<td>Redistribution, 389</td>
</tr>
<tr>
<td>Presentation layer, 41</td>
<td>Redundancy, 2, 4, 312, 321, 328, 338, 349, 359, 380</td>
</tr>
<tr>
<td>Promiscuous ports, 57</td>
<td>RFC 1918, 160</td>
</tr>
<tr>
<td>Protocol Analyzer, 81</td>
<td>RFC 2338, 354</td>
</tr>
<tr>
<td>PVRST+ (Per-VLAN Rapid Spanning Tree Plus), 256, 259, 260</td>
<td>RFC 3768, 349, 354</td>
</tr>
<tr>
<td>PVST+ (Per-VLAN Spanning Tree Plus), 256–260</td>
<td>RFC 5798, 354</td>
</tr>
<tr>
<td>RIPv2 (Routing Information Protocol version 2), 388, 428, 429, 431, 432, 436, 471</td>
<td>RIP (Routing Information Protocol), 420, 422</td>
</tr>
<tr>
<td>RIPv2 (Routing Information Protocol), 420, 422</td>
<td>Root-bridge election, 246</td>
</tr>
<tr>
<td>Root guard, 271</td>
<td>Root ports, 243, 248, 252, 253, 255, 264</td>
</tr>
<tr>
<td>Root view, 196</td>
<td>Routing loops, 390, 437</td>
</tr>
<tr>
<td>Router-on-a-stick, 317, 318</td>
<td>RSPAN (Remote Switched Port Analyzer), 58</td>
</tr>
<tr>
<td>Router configuration mode, 388, 389, 392, 397, 398, 400, 404, 448, 449, 469, 470, 484, 490, 491, 494, 506, 507, 512, 514, 516, 540</td>
<td>RSTP (Rapid Spanning Tree Protocol), 239, 251–256, 259, 260, 264–266</td>
</tr>
<tr>
<td>RSTP port roles</td>
<td>RSTP port states</td>
</tr>
<tr>
<td></td>
<td>Alternate, 255</td>
</tr>
<tr>
<td></td>
<td>Backup, 255</td>
</tr>
<tr>
<td></td>
<td>Discarding, 254</td>
</tr>
<tr>
<td></td>
<td>Forwarding, 254</td>
</tr>
<tr>
<td></td>
<td>Learning, 254</td>
</tr>
<tr>
<td></td>
<td>562 © 2017 Boson Software, LLC</td>
</tr>
</tbody>
</table>
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 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
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 1D, 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](http://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

[Logo]