Boson®

TSHOOT
Curriculum

300-135

Labs powered by

NetSim®
NETWORK SIMULATOR®

Boson®

TSHOOT

300-135 Curriculum

LM20170830/BV1.0

Boson® NetSim® NETWORK SIMULATOR®

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

The labs referenced in this book have been printed in the Boson Lab Guide, which is included with the purchase of the curriculum. These labs can be performed with real Cisco hardware or in the Boson NetSim Network Simulator version 11 or later. To learn more about the benefits of using NetSim or to purchase the software, please visit www.boson.com/netsim.

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.

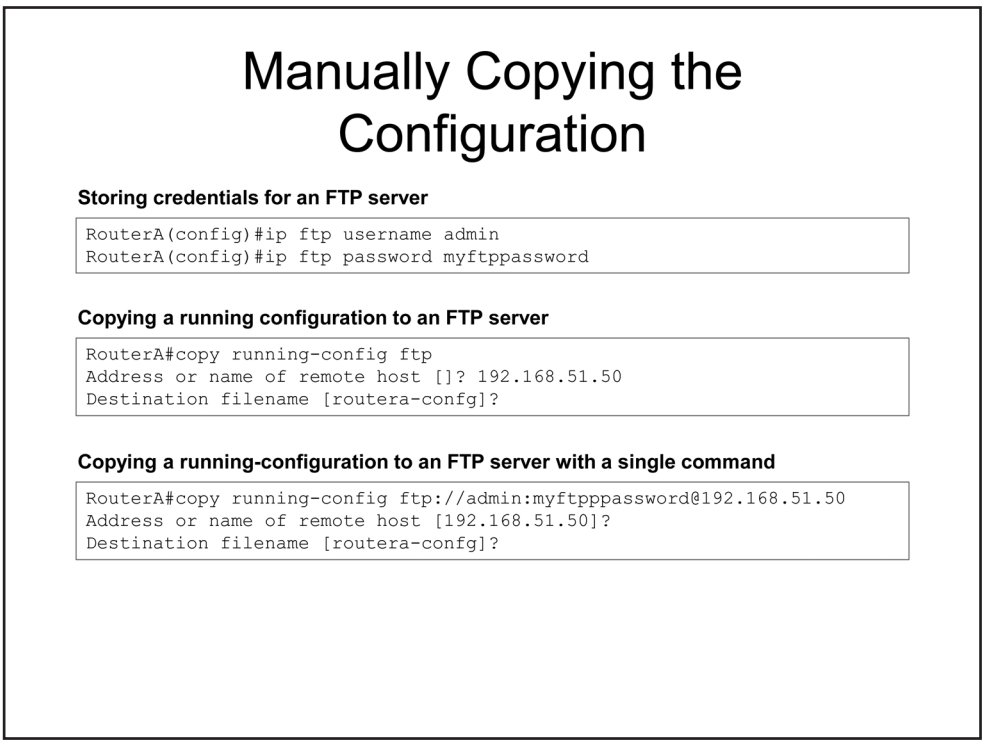
For example, a firewall connected to multiple Internet service providers (ISPs) is a single point of failure. If the firewall were to fail, network devices would not be able to communicate with the ISPs. Connecting multiple firewalls to multiple ISPs would allow continued ISP access if a firewall were 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.



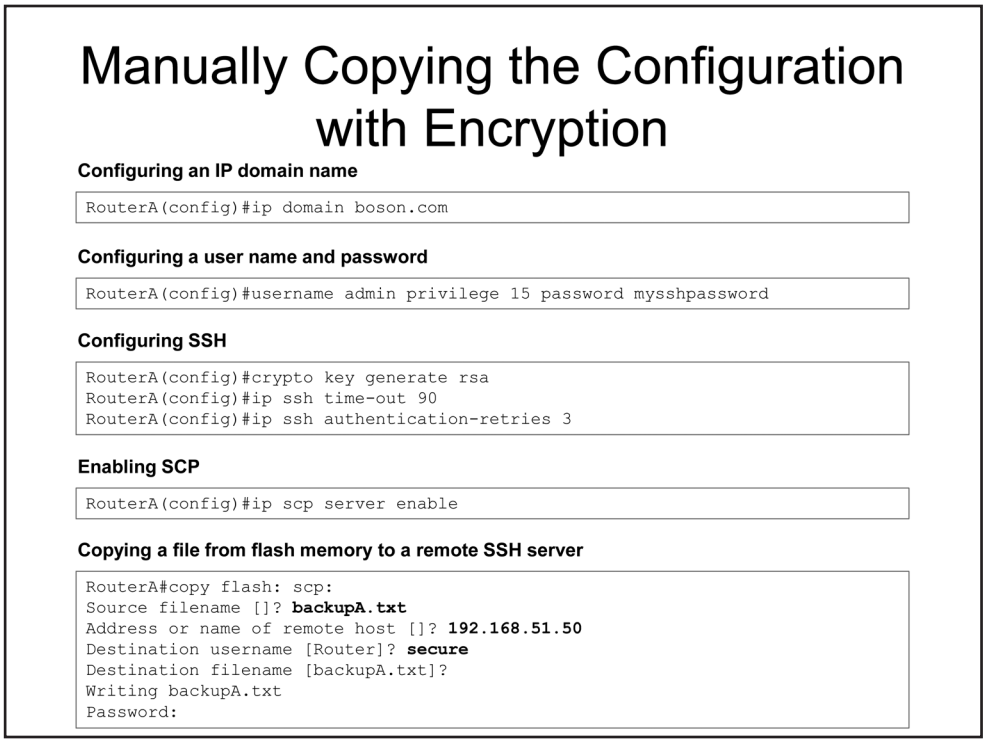
Manually Copying the Configuration

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.



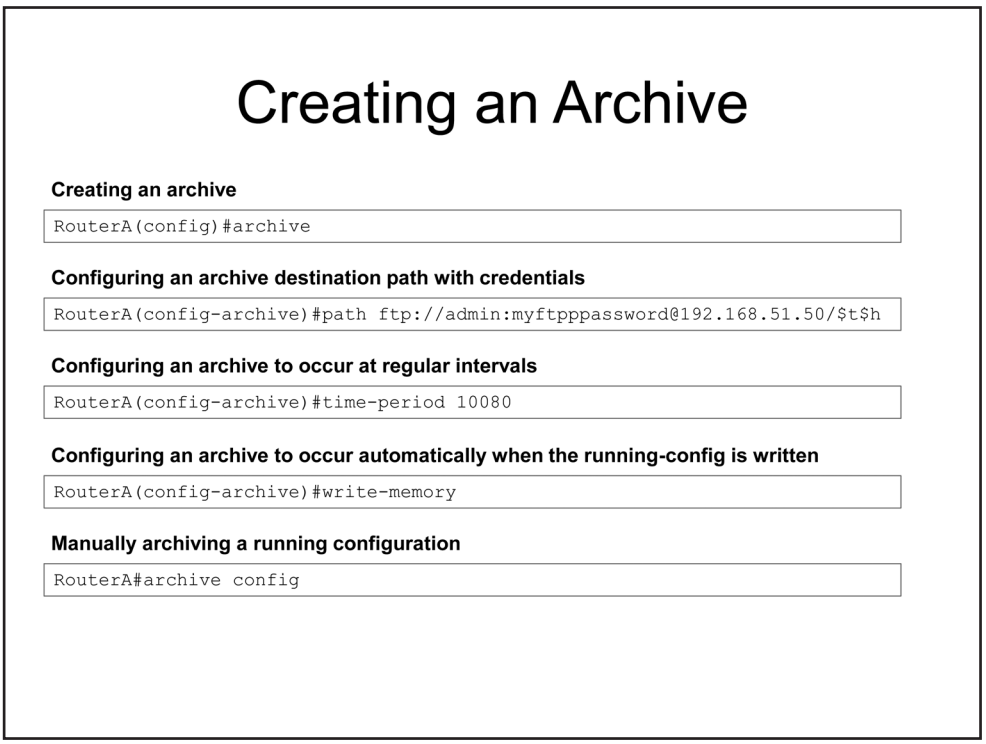
Manually Copying the Configuration with Encryption

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.



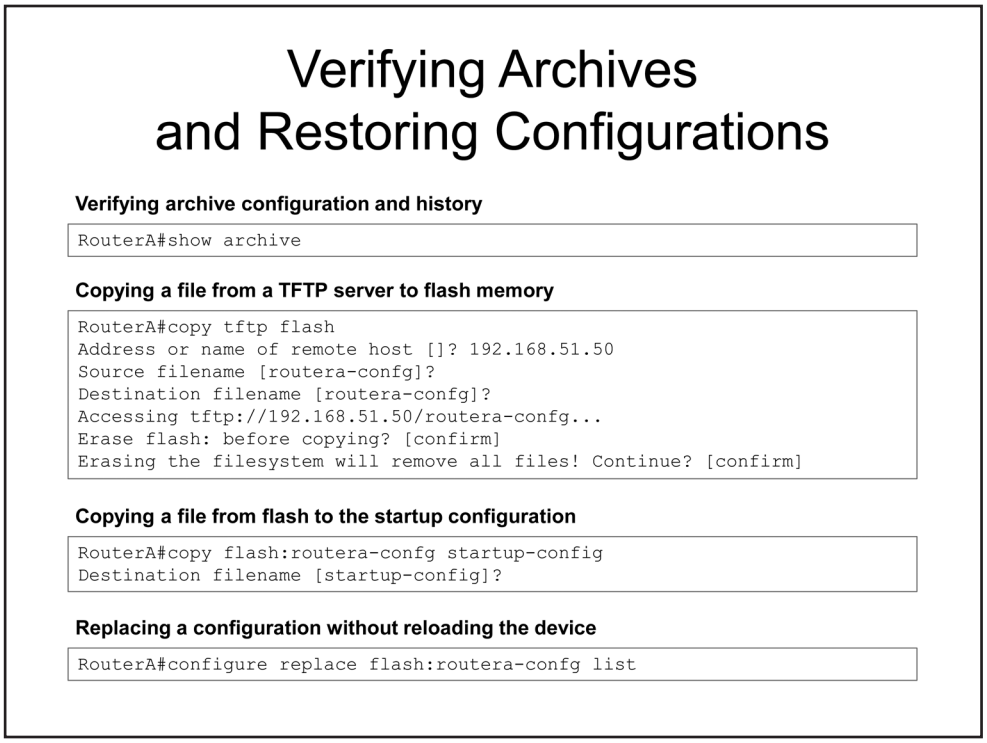
Creating an Archive

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/th** 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.

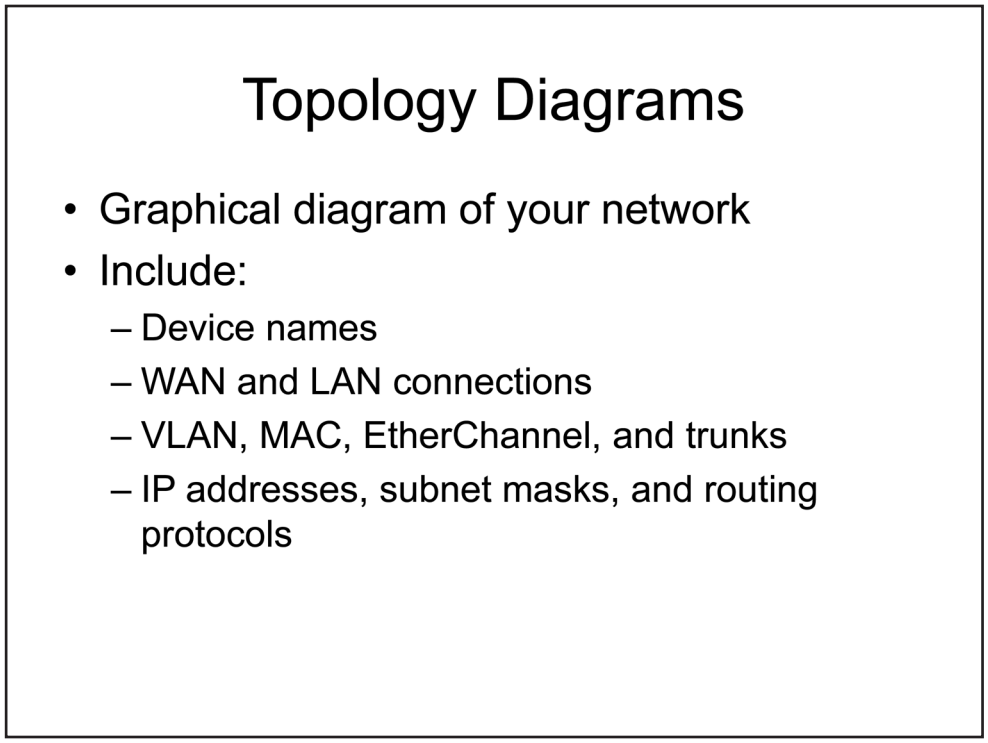
Another means of restoring a backed-up configuration is to issue the **configure replace flash:***filename* [**list**] command, where filename is the name of the file that you have copied to flash memory. The **configure replace** command detects the differences between the running configuration and 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.

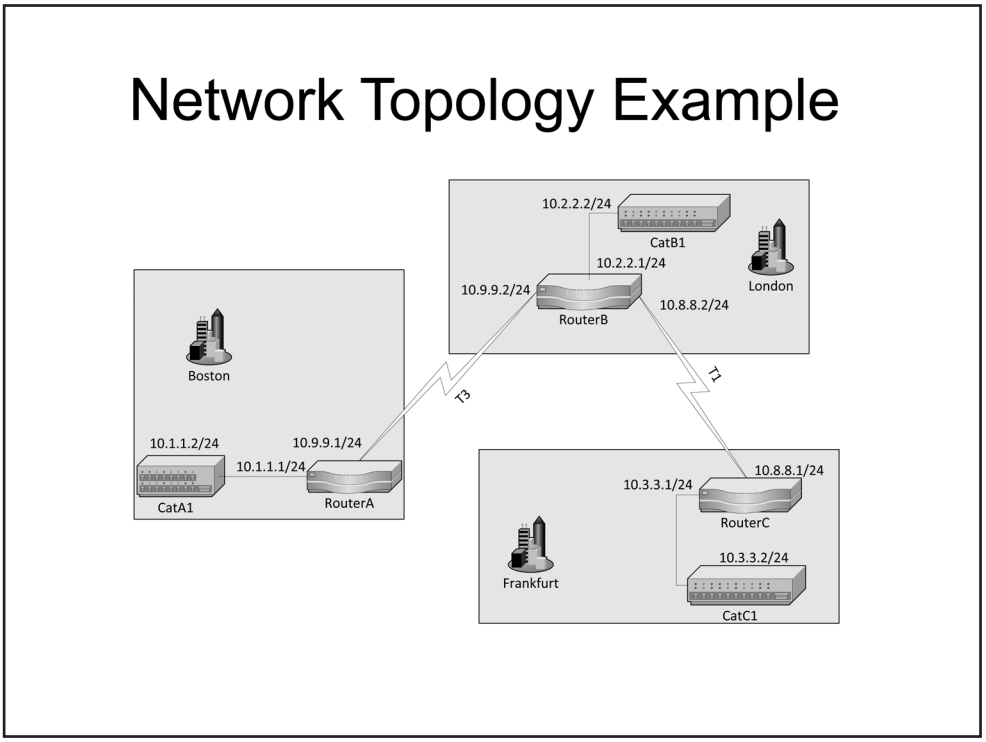


Topology Diagrams

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

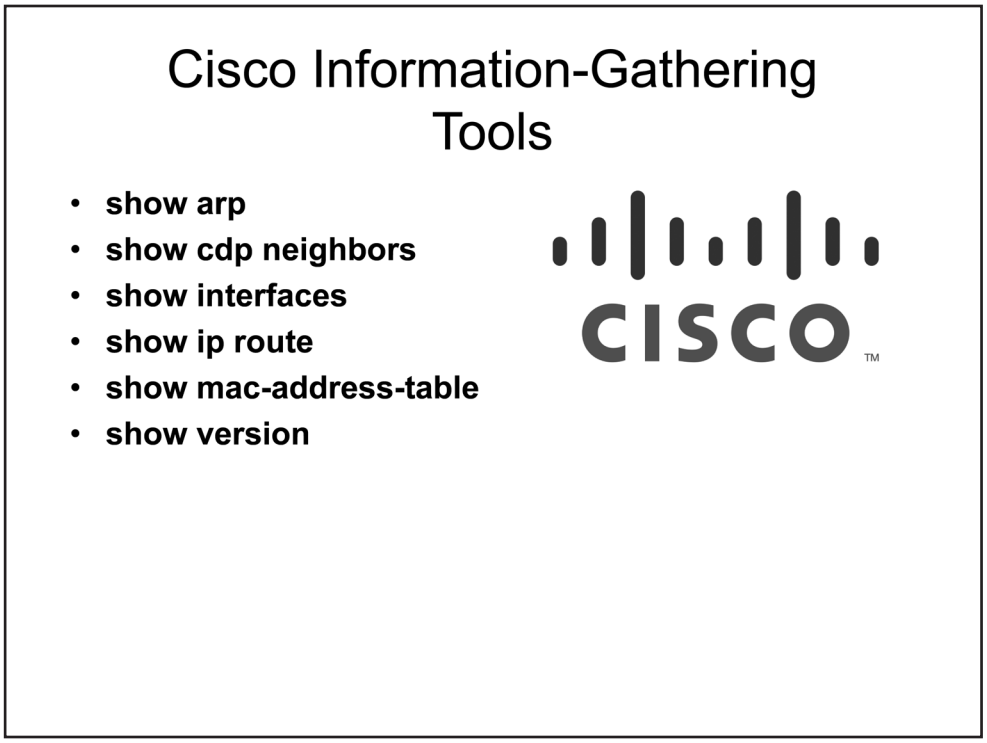
If the network spans multiple geographical areas, those areas should likewise be represented in the diagram.



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.

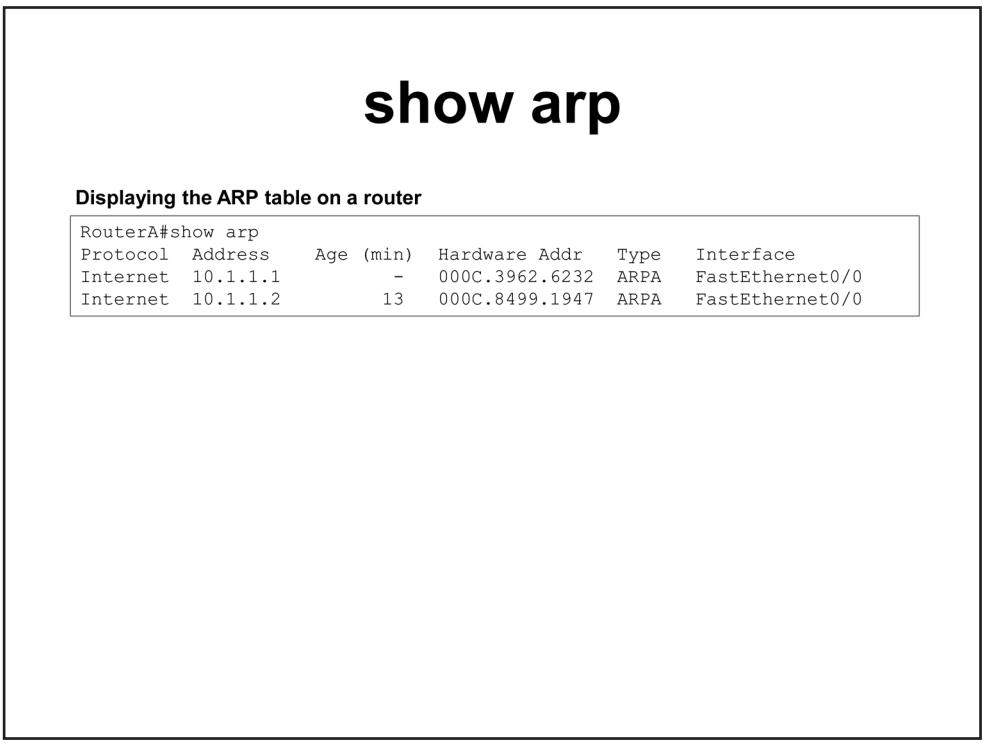
London's RouterB is connected to Frankfurt's RouterC by using a T1 line. Each router on the link is operating in the 10.8.8.0/24 network, wherein RouterB has an IP address of 10.8.8.2 and RouterC has an IP address of 10.8.8.1.

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.



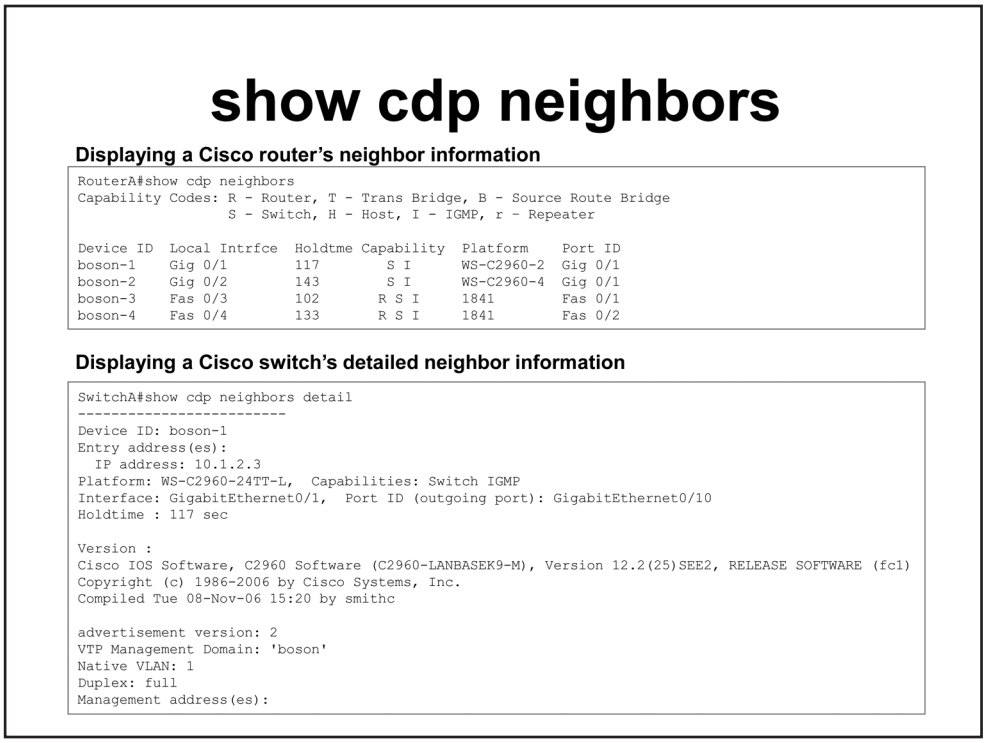
Cisco Information-Gathering Tools

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

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.



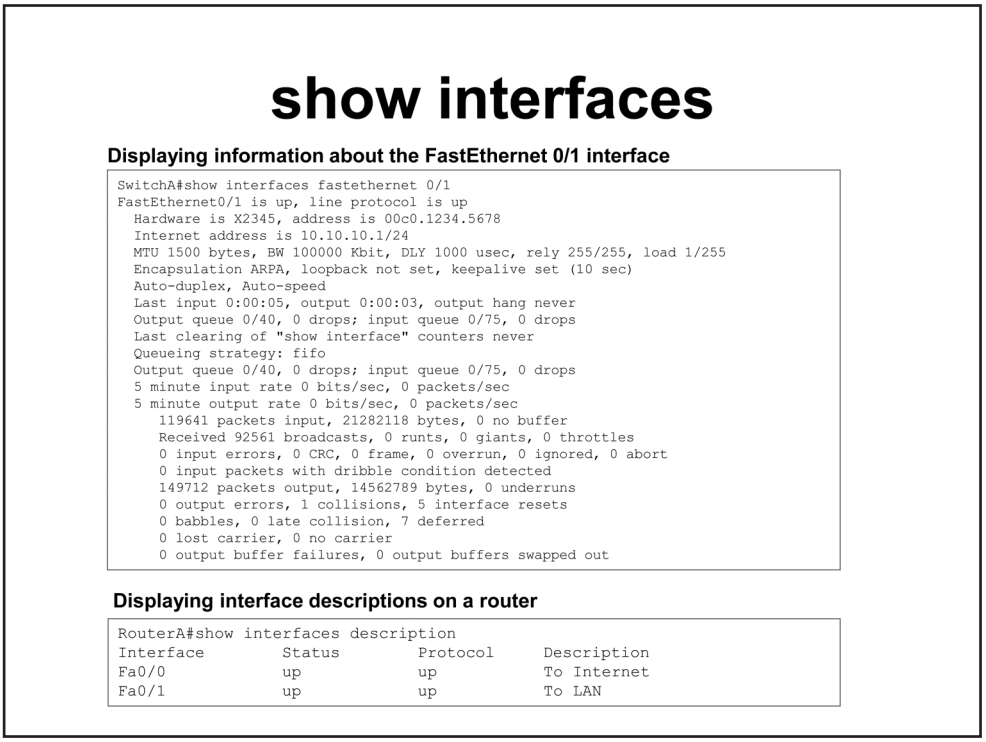
show cdp neighbors

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

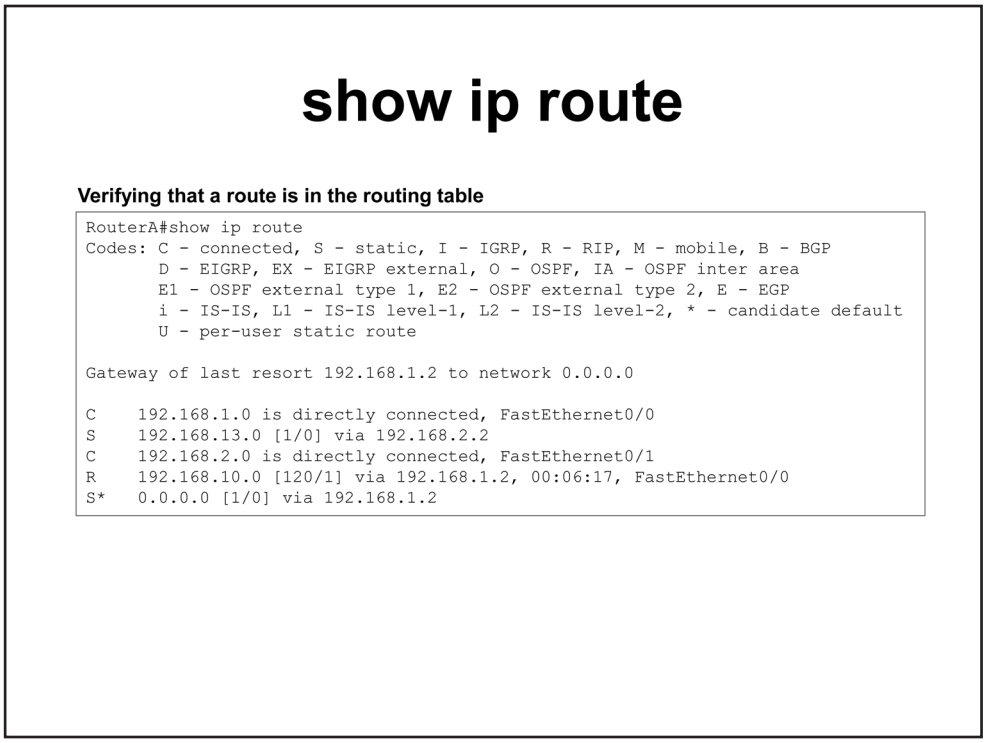


show interfaces

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.



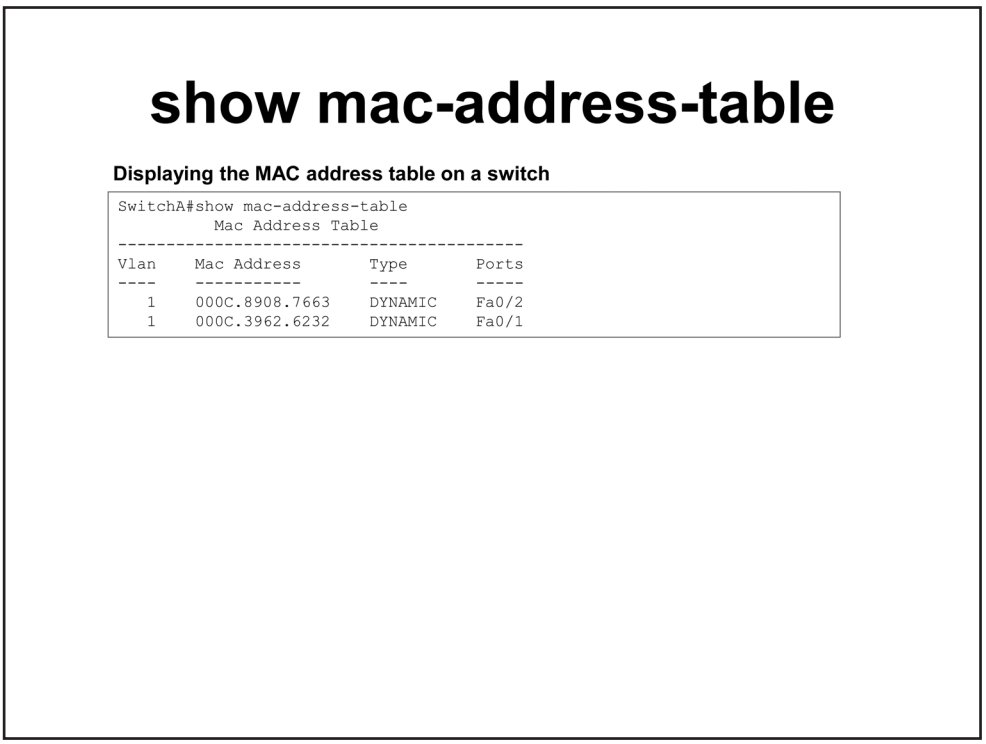
show ip route

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

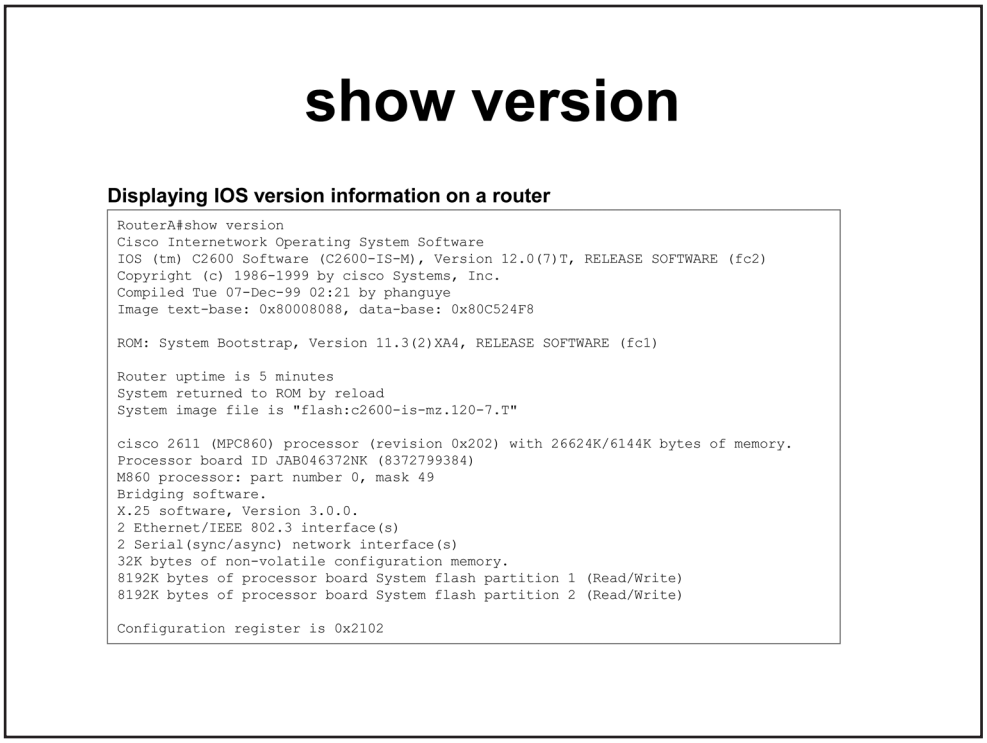
You can use the **show ip route** command to view the contents of the routing table. Each entry in the routing table has the following components:

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



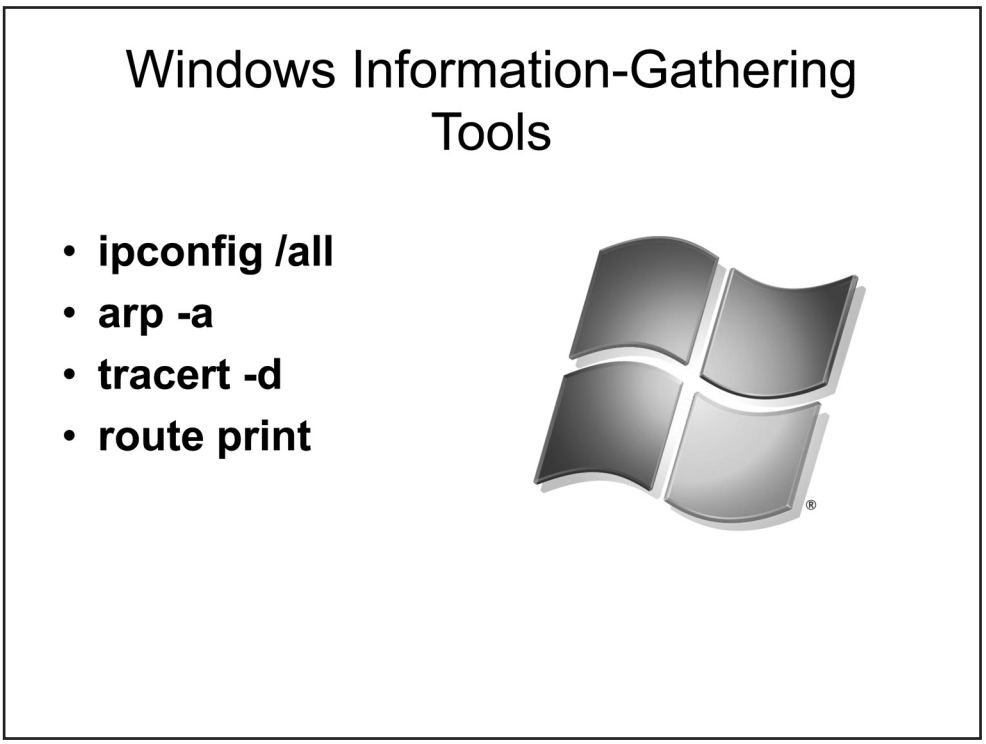
show mac-address-table

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.



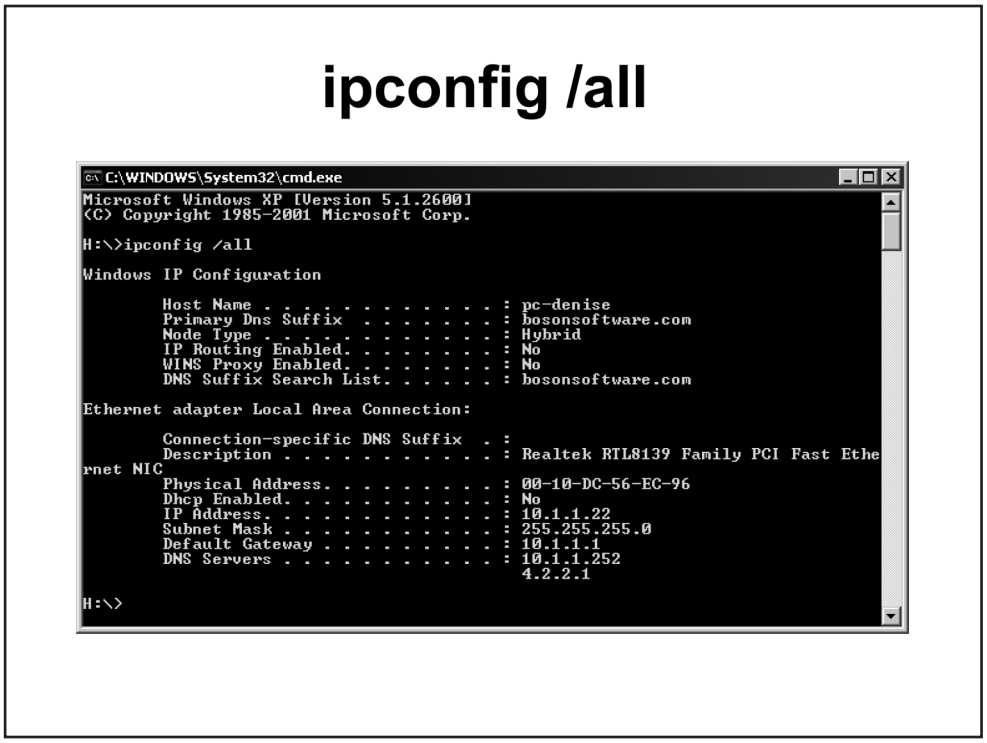
show version

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.



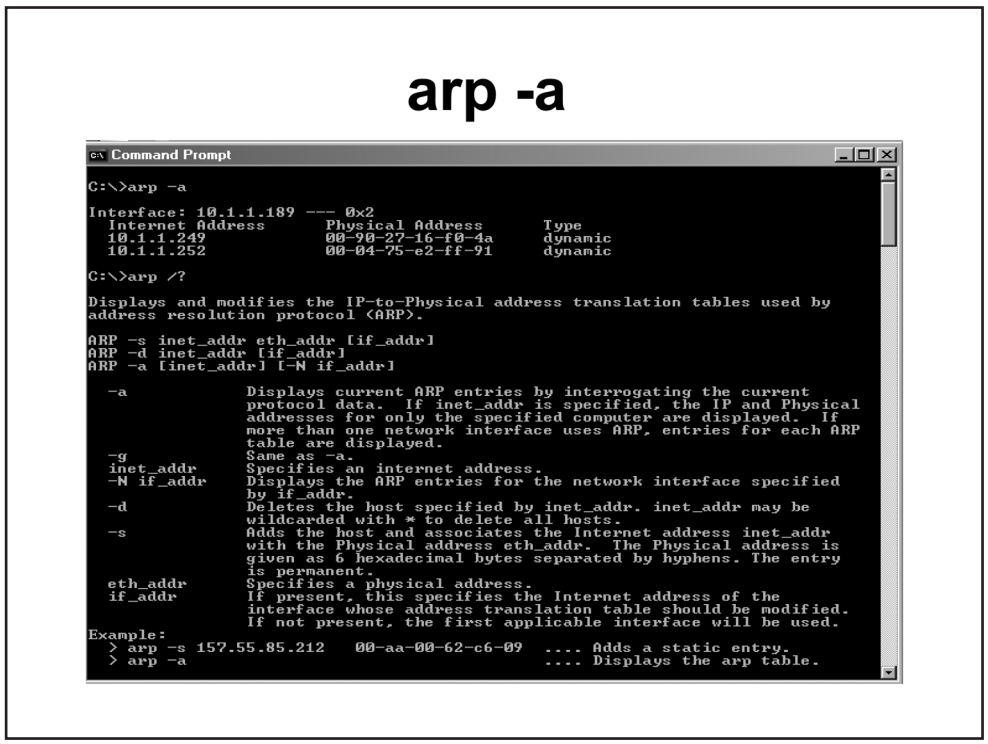
Windows Information-Gathering Tools

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.



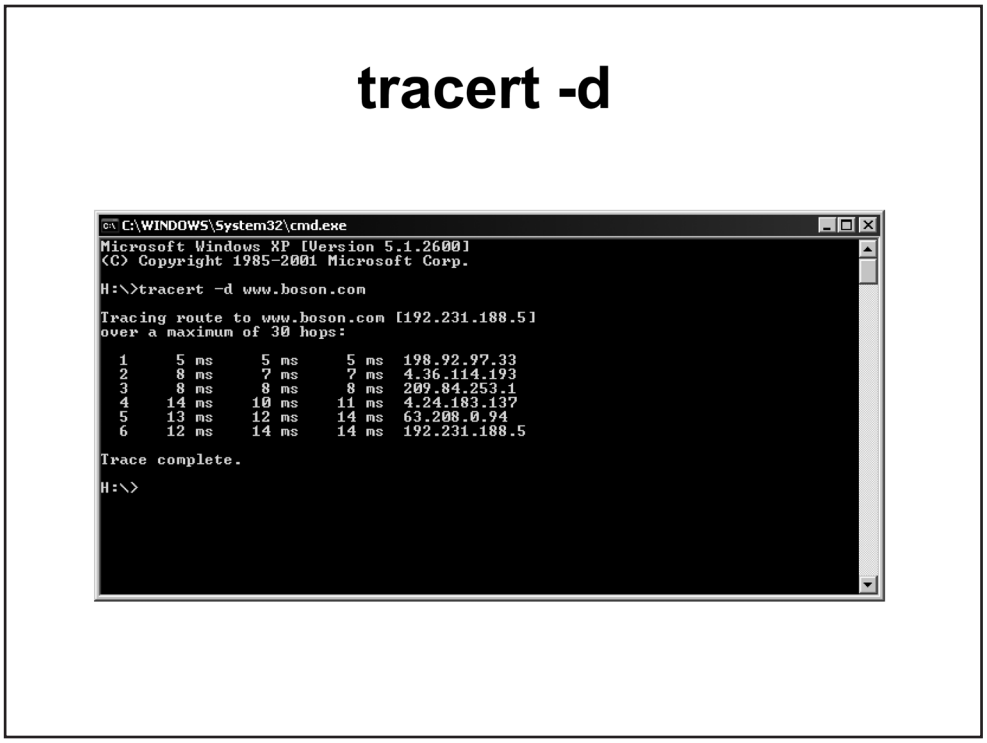
ipconfig /all

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

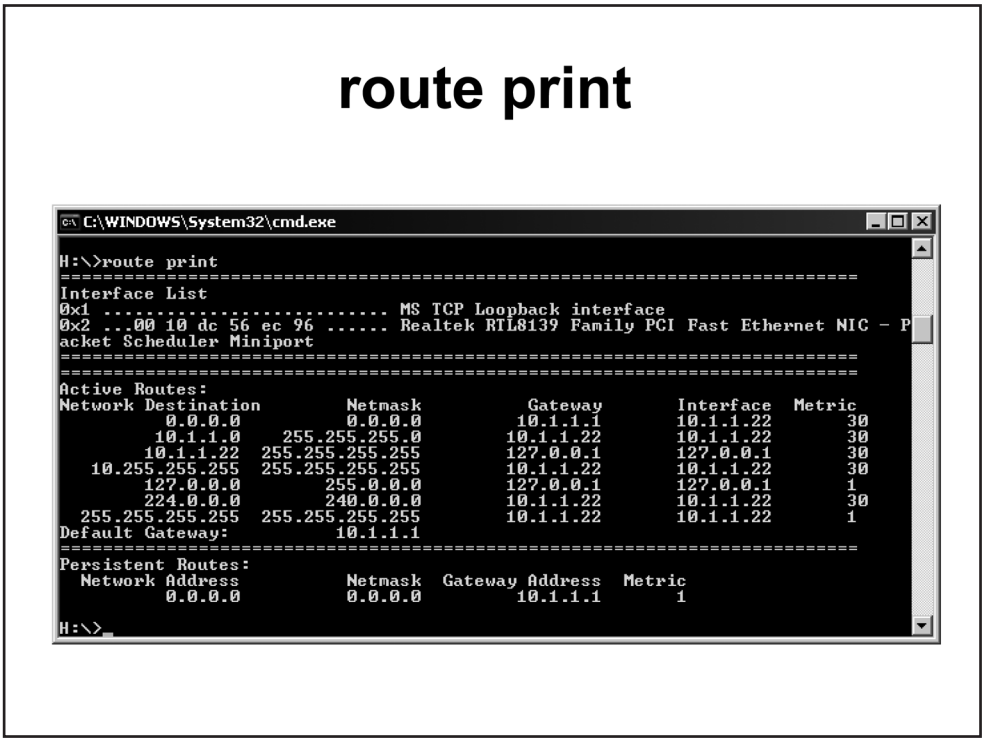
The **arp -a** command is a Windows command that displays the contents of the ARP cache. The ARP cache contains a list of the MAC addresses with which the local computer has recently communicated and the IP address associated with each MAC address. Therefore, the ARP cache is useful for determining the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



tracert -d

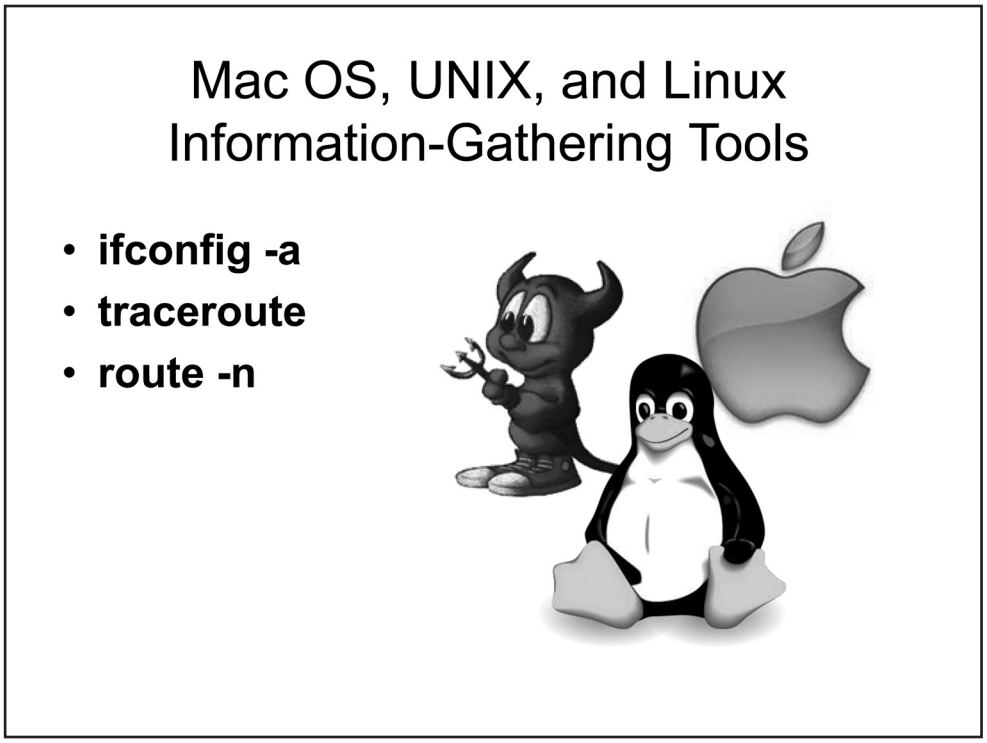
The **tracert** command on Windows is similar to the **traceroute** command on Cisco devices. It can be used to determine the route taken by packets across an IP network as well as to troubleshoot router or bridge functionality. By default, Tracert attempts to use DNS to resolve IP addresses to host 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.



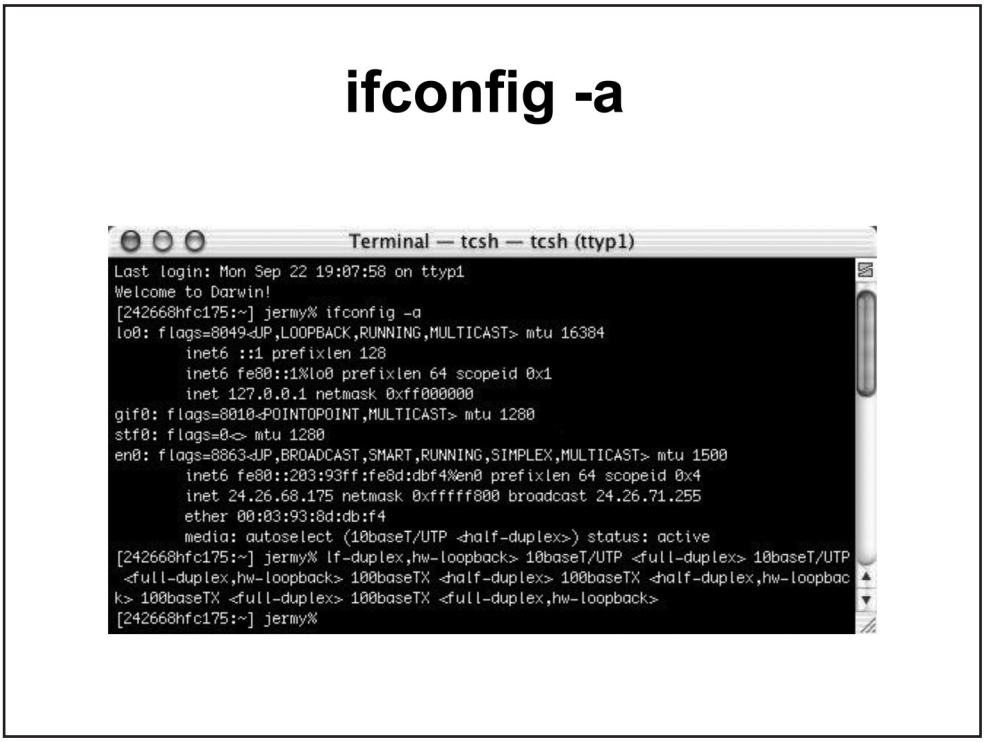
route print

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.



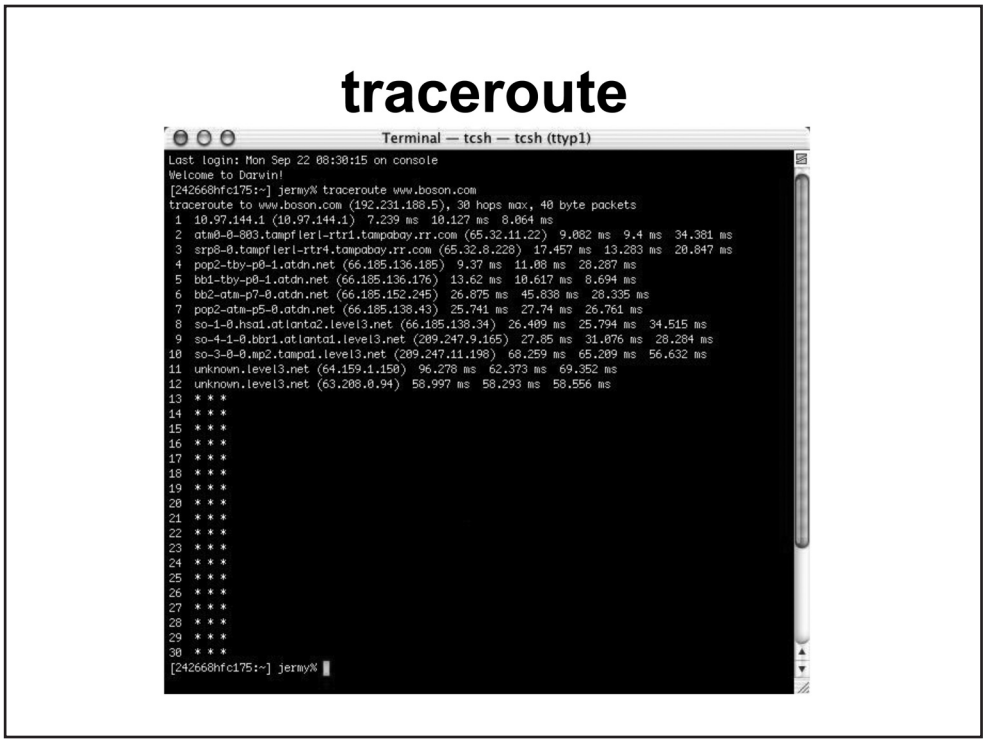
Mac OS, UNIX, and Linux Information-Gathering Tools

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.



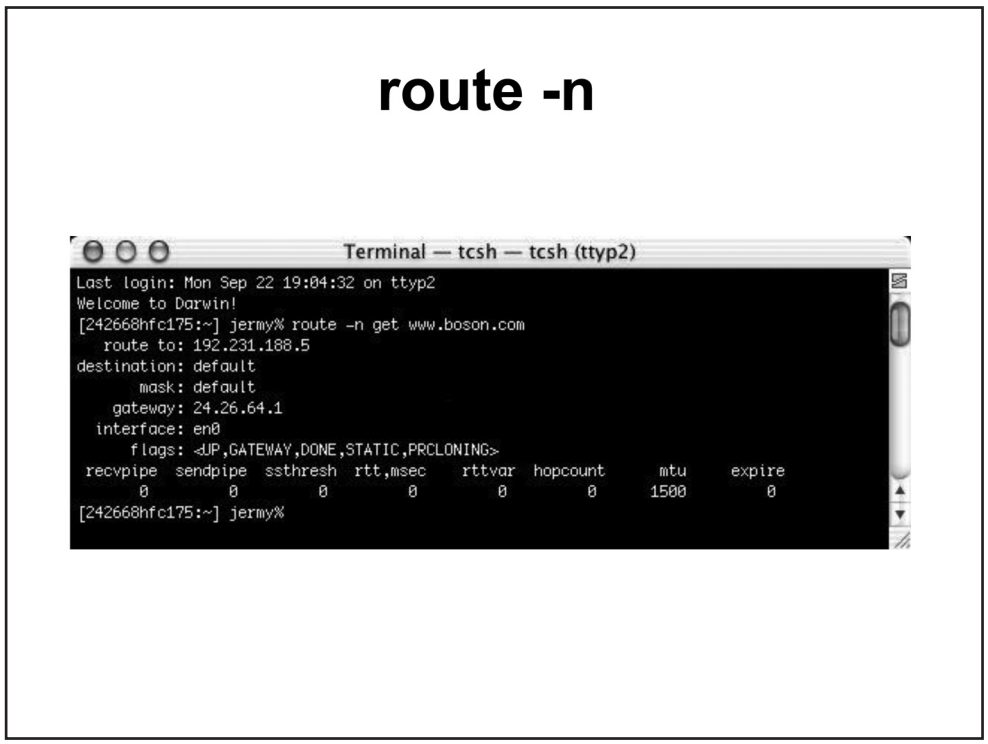
ifconfig -a

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.



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

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. 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

A

B

C

D

E

F

G

H

I

P

R

S

T

U

V

W

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

Boson.com

877.333.3926 support@boson.com