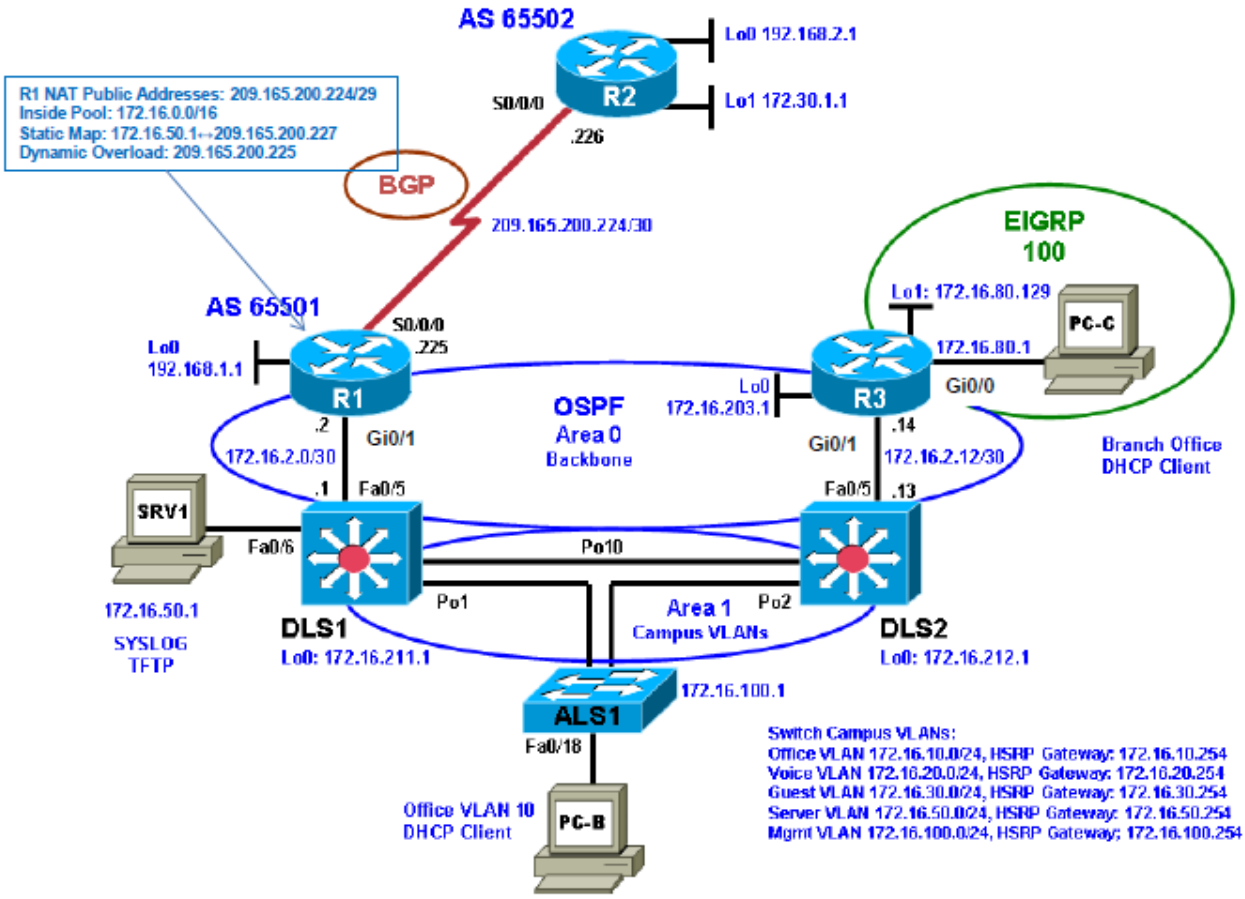
Cisco | Networking Academy®
Mind Wide Open™

Laboration 3

Troubleshooting Routing and IP Addressing

Topology



Objectives

Part 1: Erase the startup config and copy the Error configuration file from flash to the running config for each device.

Part 2: Troubleshoot and correct the errors in a routed network. Use basic commands and troubleshooting of the DHCP protocol.

Laboration Overview

This Laboration is a practical exercise for the course CCNP TSHOOT. In Part 1, you erase the existing configuration and load the error configs. In Part 2, you will find and correct errors related to routing. The last part in this laboration is to troubleshoot dynamic IP addressing with the DHCP protocol.

Required Resources

- 3 routers (Cisco IOS Release 15.4 Service or comparable)
- 2 multilayer switches and 1 access layer switch (Cisco IOS Release 15.0(2) or comparable with GigabitEthernet interfaces)
- SRV1 (Windows PC with a static IP address) with TFTP and syslog servers, plus an SSH client (PuTTY or comparable) and WireShark software
- PC-B (Windows PC—DHCP client) with PuTTY and WireShark software
- PC-C (Windows PC—DHCP client) with PuTTY and WireShark software
- Serial and Ethernet cables

Part 1: Load the Error Configuration Files to the Running Config

Step 1: Verify the existence and location of the error configuration files.

The error configuration file should be present at the desktop of the PCs in the lab room. Make sure you have access to this directory. If the directory and files are not present, contact your instructor.

Step 2: Erase the startup config from NVRAM.

Step 3: Delete the VLAN database from flash (switches only).

Step 4: Reload the device, but do *not* save the system configuration if prompted.

Step 5: When the device restarts, do not enter the initial configuration dialog, but terminate autoinstall if prompted.

Step 6: Copy the error device configuration file to the running configuration.

The format of these files is TSHOOT-xxxx-Lab3-Error-Cfg.txt, where *xxxx* is the name of the device.

Note: Although it is possible to copy the file to the startup config and reload the device, the RSA keys for SSH cannot be generated from the startup config.

Step 7: Copy the running config to the startup config.

Even if you see an Autosave message indicating that the running configuration has been saved to NVRAM, copy the running config to the startup config manually.

Note: If the device is rebooted at this point, you can log in remotely with the username **admin** and the password **adminpa55**. To access privileged EXEC mode, use the enable password **ciscoenpa55**.

Step 8: Repeat Steps 2 through 7 for all other devices in the network.

Step 9: Set the time on the NTP server R2.

Set the correct time on the NTP server R2 using the **`clock set`** command.

Step 10: Configure the PCs.

a. Configure SRV1 with the static IP address **172.16.50.1/24** and the default gateway **172.16.50.254**.

b. Start the syslog server and TFTP server on SRV1.

c. Configure PC-B and PC-C as DHCP clients.

d. Release and renew the DHCP leases on PC-B and PC-C.

Note: It is important to release and renew the DHCP leases on PC-B and PC-C because the PCs may have obtained a valid IP address previously and this could mask a problem.

Part 2: Troubleshoot and Correct the Errors

Step 1: Perform connectivity tests.

Use connectivity testing tools such as ping, traceroute, tracert (PC), and Cisco Discovery Protocol to determine the extent of connectivity loss. Use the following table to record the results of the connectivity tests. Be sure to ping from each PC to each network device interface and from each network device to every other network device using the various network addresses available, as shown in the IP Addressing table you created in Laboration 1.

Note: You can use the Ping Test table in Step 3 as a starting point.

Network Connectivity Test Table

Command	From Device/Interface/IP	To Device/Interface/IP	Result

Step 2: Document, resolve, and verify the issues discovered.

Using the tools available, such as **show** and **debug** commands, discover each problem, correct it, and document the corrective action taken. Use the Problem Resolution and Verification table to document the problem discovered, the affected devices, and the solution to the problem, including the commands used.

Note: For each device, after issuing corrective commands, copy the running config to the startup config.

Tip: If connecting from one device to another via Telnet, issue the **terminal monitor** command so that console and debug messages generated on the remote device can be viewed on the local console.

Problem Resolution and Verification Table

Device	Problem or Error Discovered	Corrective Action (commands used)	Verification Commands (more than one command can be used)
R1	Wrong network in OSPF	no network 172.16.0.2 0.0.0.3 area 0, network 172.16.2.0 0.0.0.3 area 0	show ip route, show ip ospf neighbors, show ip protocols, show run | begin ospf 1
R2	Wrong address for BGP neighbor	**no neighbor 209.165.200.225 remote-as 65501, neighbor 192.168.1.1 remote-as 65501, …**	**show ip bgp, show ip bgp neighbors, show ip route, show run | begin bgp**
R3	EIGRP routes missing in table, wrong AS number	**no redistribute eigrp 10 metric 100 subnets,** **redistribute eigrp 100 metric 100 subnets**	**Show ip route, show ip protocols, show run | begin ospf 1**
R3	No default gateway for DHCP	**default-router 172.16.80.1**	**Show ip dhcp bindings, show ip dhcp pool, show run | begin dhcp**
DLS1	Wrong IP address in DHCP pool	**no network 172.16.100.0 255.255.255.0, network 172.16.10.0 255.255.255.0**	**Show ip dhcp bindings, show ip dhcp pool**
DLS2	Missing network in OSPF	**network 172.16.2.12 0.0.0.3 area 0**	**show ip route, show ip protocols, show ip ospf neighbor, show run | begin ospf 1**

Notes

_____
_____
_____
_____
_____
_____
_____
_____

Step 3: Demonstrate basic network connectivity after correcting errors.

With all devices connected and all problems resolved, you should be able to ping from any device in the network to any other device. Perform pings according to the Ping Test table below.

Note: All pings in the table must be successful. If not, there are issues that need to be resolved.

Ping Test Table

From Device/Interface/IP	To Device/Interface/IP	Successful (Y/N)
PC-B	PC-C (DHCP 172.16.80.2)	
PC-B	HSRP default gateway (172.16.10.254)	
PC-B	SRV1 (172.16.50.1)	
PC-B	ALS1 mgmt (172.16.100.1)	
PC-B	DLS1 mgmt (172.16.100.252)	
PC-B	DLS2 mgmt (172.16.100.253)	
PC-B	R1 Gi0/1 (172.16.2.2)	
PC-B	R2 Lo1 (172.30.1.1)	
PC-B	R3 Gi0/1 (172.16.2.14)	
PC-C	R3 default gateway (172.16.80.1)	
PC-C	SRV1 (172.16.50.1)	
PC-C	ALS1 mgmt (172.16.100.1)	
PC-C	DLS1 mgmt (172.16.100.252)	
PC-C	DLS2 mgmt (172.16.100.253)	
PC-C	R1 Gi0/1 (172.16.2.2)	
PC-C	R2 Lo1 (172.30.1.1)	
PC-C	R3 Gi0/1 (172.16.2.14)	
ALS1 mgmt vlan 100 (172.16.100.1)	DLS1 mgmt (172.16.100.252)	
ALS1 mgmt vlan 100	DLS2 mgmt (172.16.100.253)	
ALS1 mgmt vlan 100	R1 Gi0/1 (172.16.2.2)	
ALS1 mgmt vlan 100	R2 Lo1 (172.30.1.1)	
ALS1 mgmt vlan 100	R3 Gi0/1 (172.16.2.14)	
R2	SRV1 (209.165.200.227)	

Notes

_____
_____
_____
_____
_____
_____
_____

Step 4: Demonstrate Telnet and SSH connectivity.

From PC-B, connect to each network device using Telnet (from the command prompt) and SSH (from an SSH client such as PuTTY) to verify remote management capability.

Note: Connecting to each device via Telnet and SSH must be successful. If not, there are issues that need to be resolved.

Remote Access Test Table

From Device	To Device/Interface/IP	Telnet (Y/N)	SSH (Y/N)
PC-B	ALS1 mgmt (172.16.100.1)		
PC-B	DLS1 mgmt (172.16.100.252)		
PC-B	DLS2 mgmt (172.16.100.253)		
PC-B	R1 Gi0/1 (172.16.2.2)		
PC-B	R2 S0/0/0 (209.165.200.226)		
PC-B	R3 Gi0/1 (172.16.2.14)		

Step 5: Demonstrate NTP functionality.

Check each network device to verify that it has synchronized with the NTP server R2.

Note: Each device must synchronize with the NTP server R2. If not, there are issues that need to be resolved.

NTP Synchronization Table

Device	NTP Status Synched (Y/N)
ALS1	
DLS1	
DLS2	
R1	
R2	
R3	

Step 6: Demonstrate network redundancy for PC-B after correcting errors.

a. Disable (shut down) DLS2 port channel Po2.

b. Ping from PC-B to all other devices in the network. Pings from PC-B to each of the other PCs and network devices must be successful. If not, there are issues that need to be resolved.

c. Renew and release the PC-B IP address. PC-B should be able to obtain an IP address on subnet 172.16.10.0/24. If not, there are issues that need to be resolved.

STP Redundancy Test Table

From Device/Interface/IP	To Device/Interface/IP	Result
PC-B	HSRP default gateway (172.16.10.254)	

PC-B	PC-C	
PC-B	SRV1 (172.16.50.1)	
PC-B	ALS1 mgmt (172.16.100.1)	
PC-B	DLS1 mgmt (172.16.100.252)	
PC-B	DLS2 mgmt (172.16.100.253)	
PC-B	R1 Gi0/1 (172.16.2.2)	
PC-B	R2 Lo1 (172.30.1.1)	
PC-B	R3 Gi0/1 (172.16.2.14)	

Notes:

_____
_____
_____
_____
_____
_____
_____

Command Summary

The table lists useful commands for this lab.

Command	Key Information Displayed
show spanning-tree vlan *vlan#*	Displays all essential parameters that affect the topology, such as the root port, designated ports, port state, and port type, as well as the spanning-tree mode being implemented.
show vlan brief	Displays a quick overview of all existing VLANs and the ports within them. Trunk ports are not listed.
show vlan id *vlan#*	Displays whether the VLAN exists and which ports are assigned to it. Includes the trunk ports on which the VLAN is allowed.
show ip interface vlan *vlan#*	Displays the SVI status, IP address, statistics, and IP Cisco Express Forwarding (CEF) information.
show ip route or **show ip route** *ip-addr*	Displays the entire routing table or information for a particular destination address.
show ip cef *ip-addr* **detail**	Displays the next hop and interface used for a particular destination address from the CEF table.
show ip cef exact-route src-*ip-addr dest-ip-addr*	Displays the next hop and interface used for a particular destination address from the CEF table.
show adjacency *int-type/#* **detail**	Displays information contained in the adjacency table for a next-hop IP address or interface.
show standby vlan *vlan#* **brief**	Verify active and standby roles and IP addresses for a particular VLAN for HSRP routers.

show standby brief	Verify active and standby roles and IP addresses for all VLANs on an HSRP router.
show ip eigrp interfaces	Displays interfaces that are participating in the EIGRP routing process. An interface does not need to be operational to be listed in the output.
show ip eigrp neighbors	Displays the EIGRP neighbor table to verify that all expected neighbor relationships are operational.
show ip eigrp topology *ip-addr net-mask*	Displays the EIGRP topology, which contains all routes that were received from all neighbors for a particular prefix.
debug eigrp packets	Displays real-time messages exchanged between EIGRP routers. **Caution:** Produces large amounts of output.
debug ip eigrp *as#* **neighbor** *ip-addr*	Displays real-time messages exchanged for a particular neighbor.
debug ip eigrp	Displays the processing of routing events by the router. **Caution:** Produces large amounts of output.
show ip ospf interface *type/#* **show ip ospf interface brief**	Displays interfaces that are participating in the OSPF routing process. An interface does not need to be operational to be listed in the command output.
show ip ospf neighbor	Displays the OSPF neighbor table to verify that all expected neighbor relationships are operational.
show ip ospf database router *router-id*	Verifies whether the directly connected routers properly advertise the destination network. Use this command to display the router (type-1) for the connected routers.
show ip ospf database external *subnet*	Verifies the availability of a specific type-5 external link-state advertisement (LSA) in the OSPF database. The *subnet* option is the subnet IP address of the prefix in which you are interested.
show ip ospf database summary *subnet*	Verifies the availability of a specific target network in a different area. The *subnet* option is the subnet IP address of the prefix in which you are interested.
show ip ospf database asbr-summary *router-id*	Verifies if a type-4 summary autonomous system (AS) boundary LSA exists for the Autonomous System Boundary Router (ASBR) with the specified router ID.
show system mtu	Displays the switch or router Maximum Transmission Unit (MTU), normally 1500 bytes. Mismatches in MTU can cause neighbor relationships to fail.
debug ip ospf packet	Displays the headers of OSPF packets as they are received by the router. Transmitted packets are not displayed. Packets are only shown for interfaces that are

	enabled for OSPF.
debug ip ospf adj	Displays all the different stages of the OSPF adjacency building process. It also reveals mismatches in the basic parameters contained in the OSPF packet header, such as area ID mismatches, the source being on the wrong subnet, or authentication mismatches. It does not reveal other mismatches in hello parameters, such as hello timers, subnet masks, or flags.
debug ip ospf events	Displays the same information that is displayed by the **debug ip ospf adj** command. In addition, it displays the transmission and reception of hello packets and reports mismatches in the hello parameters.
show ip bgp	Displays local and learned network entries in the BGP table with next hop, metric, local preference, weight, and AS path.
show ip bgp summary	Displays a summary of the BGP neighbor table. This command lists important BGP parameters, such as the AS number and router ID, statistics about the memory consumption of the various BGP data structures, and a brief overview of the configured neighbors and their state.
show ip bgp neighbors or **show ip bgp neighbor** *ip-address*	Displays parameters and extensive statistics about the peering session for all neighbors or for a particular neighbor address.
show ip bgp ***network mask***	Displays the contents of the BGP table for a specific prefix. The information is organized in the following manner: The entry for each available path in the table starts with the AS path attribute of the path, using the word “Local” to represent the empty AS path string.
debug ip tcp transactions	Displays TCP connection activity between peers. Can be used to investigate whether the TCP session is refused, established, and subsequently torn down again, or no response is received at all from the neighbor.
debug ip bgp	Displays the successive state transitions during the establishment of the BGP peering. If one of the peers decides to close the session because of a parameter problem, such as a mismatched AS number or an invalid router ID, the debug also displays information about the cause.
clear ip bgp *	Clears the contents of the BGP table.
show ip bgp *network mask* **longer prefixes**	Displays more specific prefixes present in the BGP table (including the prefix itself) that are contained in the prefix specified by the *network* and *mask* options.
show ip bgp neighbor *ip-address* **routes**	Displays all routes in the BGP table that were received from the neighbor specified by the *ip-address* option.

show ip bgp neighbor *ip-address* **advertised-routes**	Displays all routes in the BGP table that will be advertised to the neighbor specified by the *ip-address* option.
show ip bgp regexp *regular-expression*	Displays all routes from the BGP table that have an AS path string that is matched by the specified regular expression.
show ip nat statistics	Displays the NAT pool configuration information, boundaries (inside and outside interfaces), translation pool size, and usage statistics.
show ip nat translations	Displays all current translations (static and dynamic), including the initiating protocol as well as inside global, inside local, outside local, and outside global addresses.
debug ip icmp	Displays real-time information related to ping (echo request and echo reply) and other protocols that make use of ICMP.
debug ip nat	Displays real-time information related to NAT translation activity (static and dynamic).
clear ip nat translations *	Clears all dynamic translations.
clear ip nat statistics *	Clears NAT counters.
show ip dhcp server statistics	Displays DHCP pool activity from hosts requesting IP addressing.
show ip dhcp pool	Displays DHCP pool information, including the address range, number of excluded addresses, and lease activity.
show ip dhcp conflicts	Displays conflicts resulting from assigning addresses that are already assigned to a device interface in the same subnet or network.
show ip dhcp binding	Displays the IP address, hardware (MAC) address, and lease expiration for a DHCP address assignment.