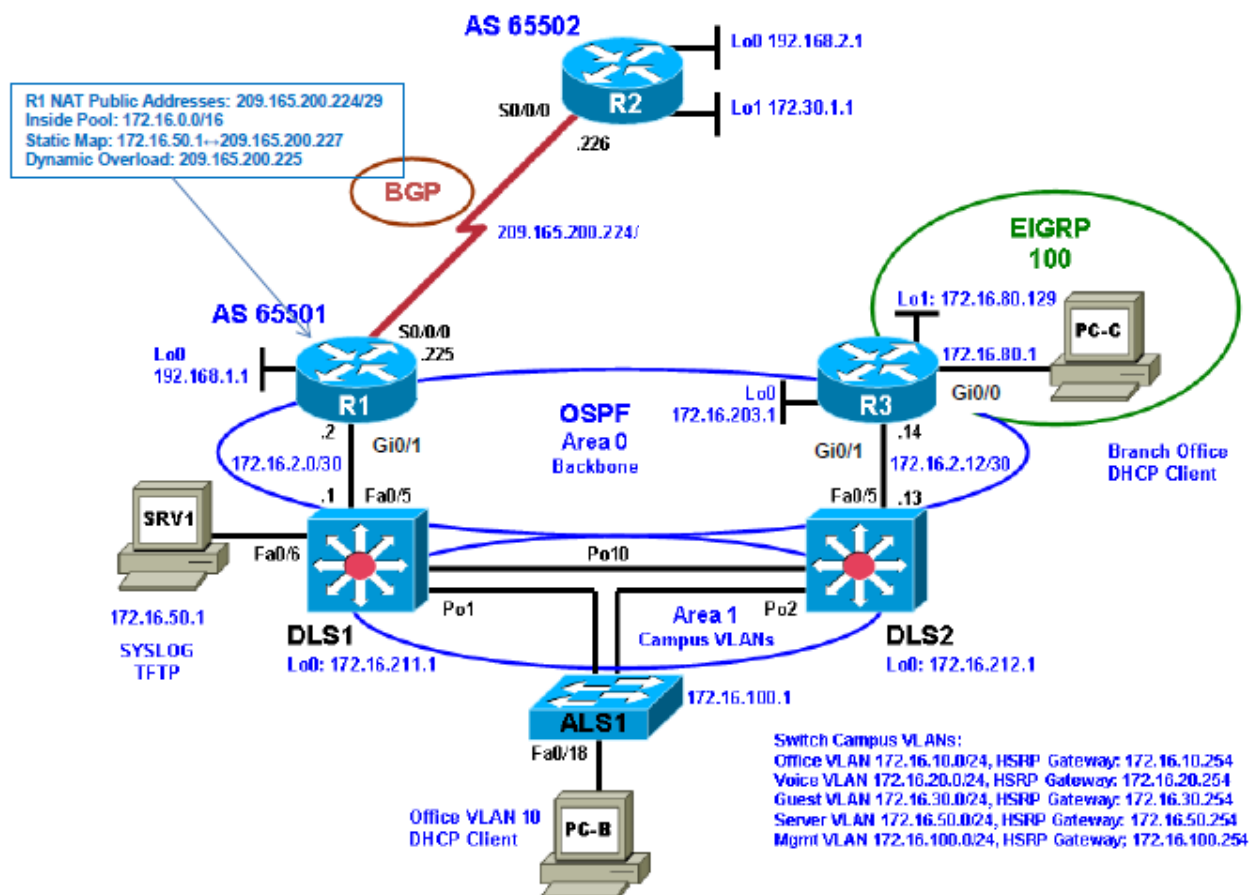


# Laboration Troubleshooting (Pass/Fail)

## Topology



### Objectives

Part 1: Erase the startup config and copy the basic configuration file to the running config for each device (config\_basic.zip).

Part 2: Troubleshoot and correct the errors in a routed network.

### Laboration Overview

This Laboration is a mandatory, practical exercise for the course Advanced Routing. 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.

### 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)
- 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 Basic Configuration Files to the Running Config

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

The basic configuration file should be present on the Course web page (config\_basic.zip). 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 basic device configuration file to the running configuration.

The format of these files is **TSHOOT-xxxx-Lab3-Base-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 PC-B and PC-C as DHCP clients.
- b. 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.

**Step 11: Verify Connectivity in the network.**

Use the table below to test the connectivity in your network. If all connectivity tests are successful, show your results for the instructor.

**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                              | 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                              | 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)               |                  |
|                                   |                                      |                  |

## 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.

**Note:** You can use the Ping Test table in the previous part as a starting point.

## Network Connectivity Test Table

[illegible]

### 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 |
|--------|-----------------------------|
|        |                             |

| Device | Corrective Action (commands used) |
|--------|-----------------------------------|
|        |                                   |

| Device | Verification Commands<br>(more than one command can be used) |
|--------|--|
|        |  |

**Notes**

---

---

---

---

---

---

---

---

**Step 3: Demonstrate basic network connectivity after correcting errors.**

With all devices connected and 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.

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

|            |  |
|------------|--|
| Name:      |  |
| ID-number: |  |
| PC:        |  |
| Pass/Fail: |  |

The table lists useful commands for this lab.

| Command  | Key Information Displayed  |
|--|--|
| <code>show spanning-tree vlan vlan#</code>                             | 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. |
| <code>show vlan brief</code>   | Displays a quick overview of all existing VLANs and the ports within them. Trunk ports are not listed.   |
| <code>show vlan id vlan#</code>  | Displays whether the VLAN exists and which ports are assigned to it. Includes the trunk ports on which the VLAN is allowed.  |
| <code>show ip interface vlan vlan#</code>                              | Displays the SVI status, IP address, statistics, and IP Cisco Express Forwarding (CEF) information.  |
| <code>show ip route</code><br>or<br><code>show ip route ip-addr</code> | Displays the entire routing table or information for a particular destination address.   |
| <code>show ip cef ip-addr detail</code>                                | Displays the next hop and interface used for a particular destination address from the CEF table.  |
| <code>show ip cef exact-route src-ip-addr dest-ip-addr</code>          | Displays the next hop and interface used for a particular destination address from the CEF table.  |
| <code>show adjacency int-type/# detail</code>                          | Displays information contained in the adjacency table for a next-hop IP address or interface.  |
| <code>show standby vlan vlan# brief</code>                             | Verify active and standby roles and IP addresses for a particular VLAN for HSRP routers.   |
| <code>show standby brief</code>  | Verify active and standby roles and IP addresses for all VLANs on an HSRP router.  |
| <code>show ip eigrp interfaces</code>                                  | Displays interfaces that are participating in the EIGRP routing process. An interface does not need to be operational to be listed in the output.                                    |
| <code>show ip eigrp neighbors</code>                                   | Displays the EIGRP neighbor table to verify that all expected neighbor relationships are operational.  |
| <code>show ip eigrp topology ip-addr net-mask</code>                   | Displays the EIGRP topology, which contains all routes that were received from all neighbors for a particular prefix.  |
| <code>debug eigrp packets</code>                                       | Displays real-time messages exchanged between EIGRP routers. <b>Caution:</b> Produces large amounts of output.   |
| <code>debug ip eigrp as# neighbor ip-addr</code>                       | Displays real-time messages exchanged for a particular neighbor.   |
| <code>debug ip eigrp</code>  | Displays the processing of routing events by the router.   |

|   |  |
|---|--|
|   | <b>Caution:</b> Produces large amounts of output.  |
| <pre>show ip ospf interface type/# show ip ospf interface brief</pre> | 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.   |
| <pre>show ip ospf neighbor</pre>                                      | Displays the OSPF neighbor table to verify that all expected neighbor relationships are operational.   |
| <pre>show ip ospf database router router-id</pre>                     | Verifies whether the directly connected routers properly advertise the destination network. Use this command to display the router (type-1) for the connected routers.   |
| <pre>show ip ospf database external subnet</pre>                      | Verifies the availability of a specific type-5 external link-state advertisement (LSA) in the OSPF database. The <i>subnet</i> option is the subnet IP address of the prefix in which you are interested.  |
| <pre>show ip ospf database summary subnet</pre>                       | Verifies the availability of a specific target network in a different area. The <i>subnet</i> option is the subnet IP address of the prefix in which you are interested.   |
| <pre>show ip ospf database asbr- summary router-id</pre>              | Verifies if a type-4 summary autonomous system (AS) boundary LSA exists for the Autonomous System Boundary Router (ASBR) with the specified router ID.   |
| <pre>show system mtu</pre>  | Displays the switch or router Maximum Transmission Unit (MTU), normally 1500 bytes. Mismatches in MTU can cause neighbor relationships to fail.  |
| <pre>debug ip ospf packet</pre>                                       | 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.   |
| <pre>debug ip ospf adj</pre>  | 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. |
| <pre>debug ip ospf events</pre>                                       | Displays the same information that is displayed by the <b>debug ip ospf adj</b> command. In addition, it displays the transmission and reception of hello packets and reports mismatches in the hello parameters.  |
| <pre>show ip bgp</pre>  | Displays local and learned network entries in the BGP table with next hop, metric, local preference, weight, and AS path.  |
| <pre>show ip bgp summary</pre>  | 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.  |
| <b>show ip bgp neighbors</b><br>or<br><b>show ip bgp neighbor <i>ip-address</i></b> | Displays parameters and extensive statistics about the peering session for all neighbors or for a particular neighbor address.   |
| <b>show ip bgp network mask</b>   | 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.      |
| <b>debug ip tcp transactions</b>  | 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.   |
| <b>debug ip bgp</b>   | 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. |
| <b>clear ip bgp *</b>   | Clears the contents of the BGP table.  |
| <b>show ip bgp network mask longer prefixes</b>                                     | Displays more specific prefixes present in the BGP table (including the prefix itself) that are contained in the prefix specified by the <i>network</i> and <i>mask</i> options.   |
| <b>show ip bgp neighbor <i>ip-address</i> routes</b>                                | Displays all routes in the BGP table that were received from the neighbor specified by the <i>ip-address</i> option.   |
| <b>show ip bgp neighbor <i>ip-address</i> advertised-routes</b>                     | Displays all routes in the BGP table that will be advertised to the neighbor specified by the <i>ip-address</i> option.  |
| <b>show ip bgp regexp <i>regular-expression</i></b>                                 | Displays all routes from the BGP table that have an AS path string that is matched by the specified regular expression.  |
| <b>show ip nat statistics</b>   | Displays the NAT pool configuration information, boundaries (inside and outside interfaces), translation pool size, and usage statistics.  |
| <b>show ip nat translations</b>   | Displays all current translations (static and dynamic), including the initiating protocol as well as inside global, inside local, outside local, and outside global addresses.   |
| <b>debug ip icmp</b>  | Displays real-time information related to ping (echo request and echo reply) and other protocols that make use of ICMP.  |
| <b>debug ip nat</b>   | Displays real-time information related to NAT translation activity (static and dynamic).   |
| <b>clear ip nat translations *</b>  | Clears all dynamic translations.   |



|   |  |
|---|--|
| <code>clear ip nat statistics *</code>      | Clears NAT counters.   |
| <code>show ip dhcp server statistics</code> | Displays DHCP pool activity from hosts requesting IP addressing.   |
| <code>show ip dhcp pool</code>              | Displays DHCP pool information, including the address range, number of excluded addresses, and lease activity.                       |
| <code>show ip dhcp conflicts</code>         | Displays conflicts resulting from assigning addresses that are already assigned to a device interface in the same subnet or network. |
| <code>show ip dhcp binding</code>           | Displays the IP address, hardware (MAC) address, and lease expiration for a DHCP address assignment.                                 |

## Physical Topology:

