Cisco | Networking Academy®
Mind Wide Open™

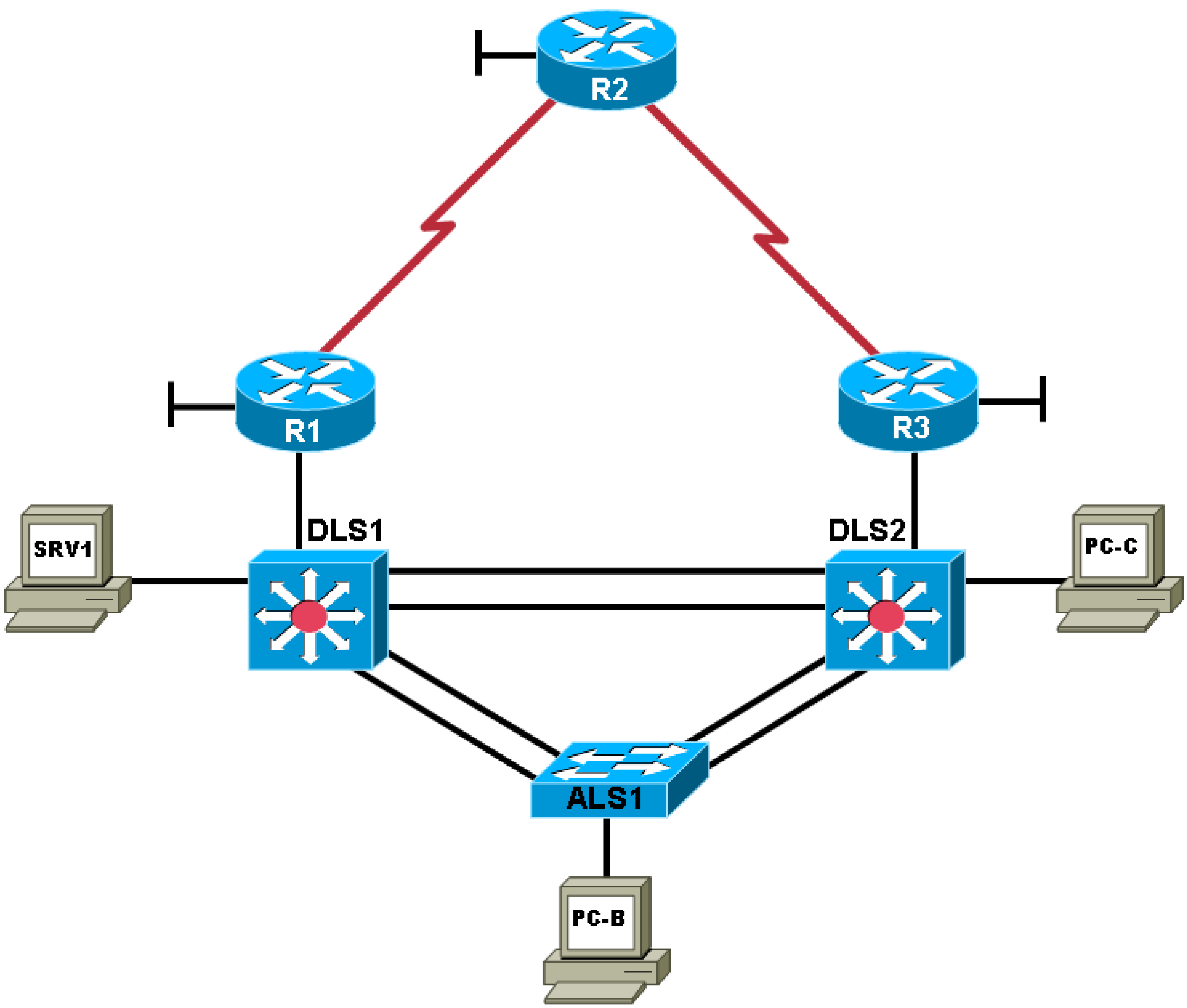
CCNP TSHOOT 6.0

Instructor Lab Manual

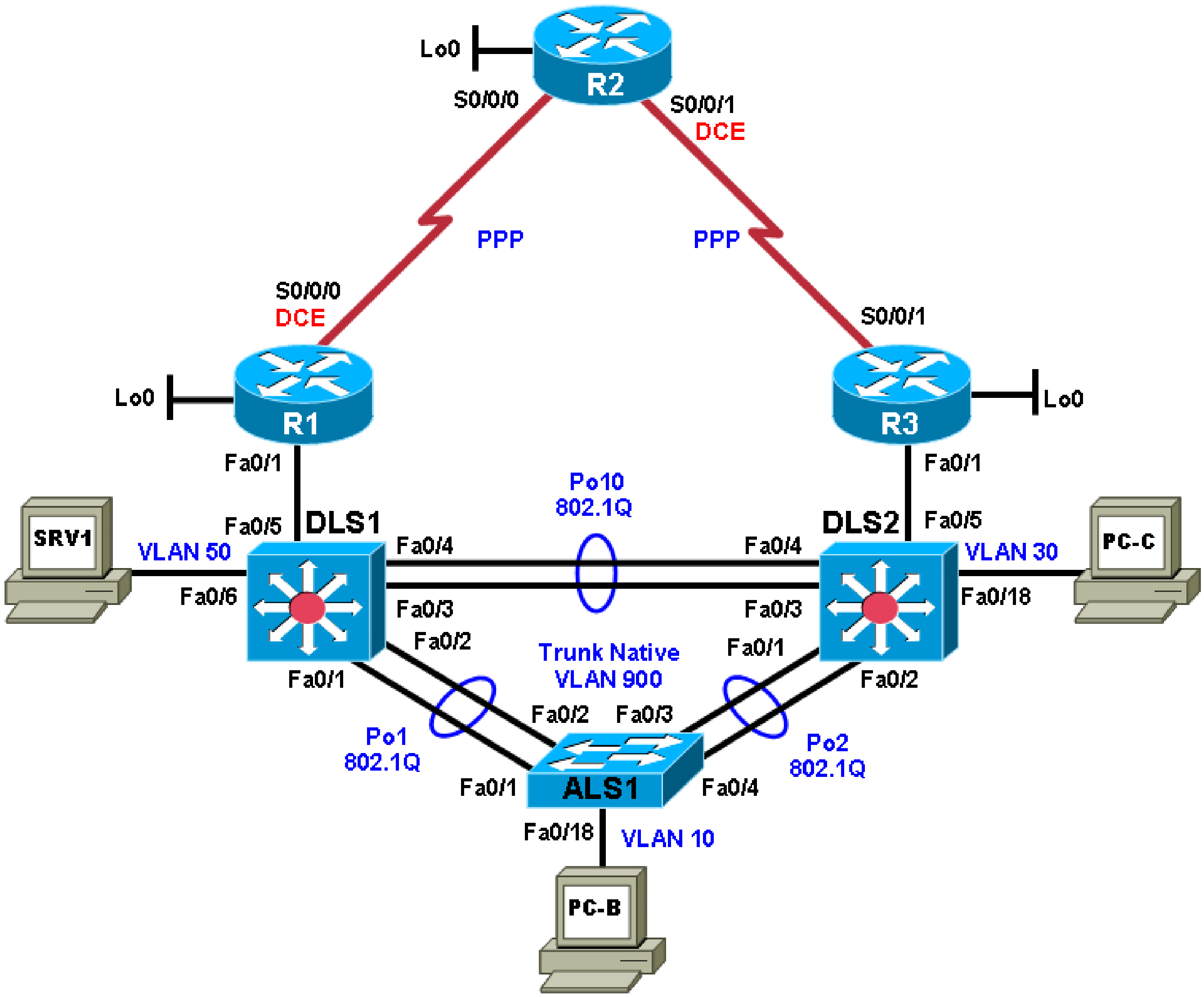
Chapter 3 Lab 3-1, Assembling Maintenance and Troubleshooting Tools **Instructor Version**

Physical Topology

Physical topology for STUDENT version of lab



Physical topology for INSTRUCTOR version of lab



Objectives

- Assign responsibility for a device or set of devices to team members (optional).
- Load the baseline configuration for all devices in the topology.
- Use available tools to document key device configuration parameters, such as the interfaces in use, IP addressing, routing protocols, VLANs, logging mechanisms, and security measures.
- Document the physical topology to support future troubleshooting tasks.
- Document the logical topology to support future troubleshooting tasks.

Background

You have been employed as a network engineering consultant by a company that has made a recent acquisition. The documentation for the acquired company's network is incomplete and outdated, so you need to inventory their network architecture both logically and physically, per company documentation standards. This will help you learn about the design and implementation of their network and ensure that you have access to up-to-date and accurate network documentation to reference during future troubleshooting procedures.

In this lab, you survey the baseline TSHOOT network. No problems are introduced in this lab. This network will evolve over time as changes and enhancements are made. You will analyze and document the current topology and device configuration parameters to develop familiarity with the baseline configurations and network connections. You will review and fill out the provided documentation as you evaluate the network. You will assess and assemble tools that can be used for future maintenance and troubleshooting tasks.

Note: This lab uses Cisco 1841 routers with Cisco IOS Release 12.4(24)T and the Advanced IP Services image c1841-advipservicesk9-mz.124-24.T.bin. The switches are Cisco WS-C2960-24TT-L with the Cisco IOS image c2960-lanbasek9-mz.122-46.SE.bin and Catalyst 3560-24PS with the Cisco IOS image c3560-advipservicesk9-mz.122-46.SE.bin. Other routers (such as 2801 and 2811), switches (such as 2950 or 3550), and Cisco IOS Software versions can be used if they have comparable capabilities and features. Depending on the router or switch model and Cisco IOS Software version, the commands available and output produced might vary from what is shown in this lab.

Instructor Notes:

- The lab topology should be pre-built prior to the students starting the lab. Ensure that all routers and switches (R1, R2, R3, ALS1, DLS1, and DLS2) have the course lab configuration files installed in flash. These can be downloaded from the Academy Connection web site. The baseline configurations for all devices are included at the end of this lab. Each configuration can be copied into a text file using the naming convention indicated in Task 2, Step 1.
- Each device should have a directory named “tshoot” in flash. This directory should contain the baseline configuration file for that device as well as configuration files for the other labs in this course.
- Instructors can use a TFTP server, USB drive, flash memory card, or other method at their discretion to initially copy all course configuration files into the flash:/tshoot directory for each device in the topology. This procedure is done once at the beginning of the course.
- For this lab and subsequent labs, the student is responsible for loading the baseline or trouble ticket configurations as required using the procedure described in Task 2.
- The baseline configuration file for each device and the final **show running-config** outputs are included at the end of this lab.
- Set the correct time on router R2, which serves as the primary NTP server for the lab network.

Required Resources

- 3 routers (Cisco 1841 with Cisco IOS Release 12.4(24)T1 Advanced IP Service or comparable)

  Instructor notes:

  The routers should have WIC-2T WAN modules, if available, rather than WIC-2A/S modules.
- 1 switch (Cisco 2960 with the Cisco IOS Release 12.2(46)SE C2960-LANBASEK9-M image or comparable)
- 2 switches (Cisco 3560 with the Cisco IOS Release 12.2(46)SE C3560-advipservicesK9-mz image or comparable)
- SRV1 (PC with static IP address): Windows XP, Vista, or Windows Server with RADIUS, TFTP, and syslog servers, plus an SSH client (PuTTY or comparable) and WireShark software

Instructor note: A RADIUS server is specified for SRV1, but it is not used with the baseline configuration in this lab. The WinRADIUS server is used in a subsequent troubleshooting lab, in which the installation process will be described.

- PC-B (DHCP client): Windows XP or Vista (with SSH client and WireShark software)
- PC-C (DHCP client): Windows XP or Vista (with SSH client and WireShark software)

- Serial and Ethernet cables, as shown in the topology
- Rollover cables to configure the routers and switches via the console

Instructor Notes:

- This lab is not a troubleshooting lab. It focuses on discovering the network, assembling documentation, and identifying available troubleshooting and maintenance tools. A large part of the documentation that students need for subsequent labs is included in the lab guide.
- The main purpose of this lab is to have students analyze the network design and implementation, familiarize themselves with the environment that they will be working in during the course, and assemble the documentation that they will need to troubleshoot effectively in subsequent labs.
- Students can work in teams of two or more, or can work individually from a remote environment. If the team consists of three people, each person can analyze and document one router and one switch. Each student can also work with a single device and use Telnet or SSH to access the other devices and map out the entire network, if time permits.
- The lab is divided into tasks. If time is a factor, Tasks 1 through 3 can be done in one session and Tasks 4 through 6 in a subsequent session.

  Task 1: Assign Responsibility for Each Device (optional)

  Task 2: Load the Baseline Device Configuration Files

  Task 3: Analyze and Document the Physical Lab Topology

  Task 4: Analyze and Document the Logical Lab Topology

  Task 5: Identify Troubleshooting and Maintenance Tools

  Task 6: Identify Implemented Security Measures

Task 1: Assign Responsibility for Each Device (optional)

Step 1: Review the lab topology together with your team members.

Step 2: Assign responsibility for each device to a team member.

a. The team member who has primary responsibility for a device is in control of the console of that device and changes to the device. No other team member should access the console, make changes to the device, or execute disruptive actions, such as reloading or debugging, without permission from the responsible team member.

b. All team members can access all devices via Telnet or SSH for nondisruptive diagnostic action without permission of the responsible team member. Responsibilities can be reassigned during later labs if necessary.

c. If working in teams, you can document responsibilities in the Device Responsibilities table.

Device Responsibilities Table

Device	Description	Responsible Team Member
R1	Core Router 1	Wayne
R2	ISP Router	Sonya
R3	Core Router 2	Bob
ALS1	Access Layer Switch 1	Wayne
DLS1	Distribution Layer Switch 1	Sonya
DLS2	Distribution Layer Switch 2	Bob
SRV1	TFTP, syslog	Wayne
PC-B	User PC	Sonya
PC-C	User PC	Bob

Task 2: Load the Baseline Device Configuration Files

Use the following procedure on each device in the network to load the baseline configuration. The procedure shown here is for a switch, but it is very similar to that of a router.

Note: The configs for this lab include **`ip host`** *`name ip-addr`* entries for all devices. This can be helpful in accessing devices using Telnet with this lab. The ip host entries are only provided in Lab 3-1 as the device IP addresses will change in subsequent labs.

Instructor Notes:

See the instructor note in the Background section at the beginning of the lab for additional information on initially copying the device config files to flash.

The baseline configurations used with this lab do not include some features that might be present in an enterprise network, such as NAT, ACLs, OSPF, and BGP. These features are implemented within the specific labs where they are introduced.

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

The lab configuration files for the course should be in flash under the tshoot directory for a given device. Use the **`show flash`** command to verify the presence of this directory. You can also verify the contents of the directory using the **`cd`** and **`dir`** commands. If the directory and files are not present, contact your instructor.

Note: When the **`show flash`** command is used on a switch, it lists the directories and files at the root directory but not the files within the directories. The following example uses the **`cd`** and **`dir`** commands on switch ALS1.

```
ALS1#show flash:

Directory of flash:/

    3  -rwx      916   Mar 1 1993 00:00:29 +00:00  vlan.dat
  619  -rwx     6582   Mar 1 1993 00:10:09 +00:00  config.text
    6  drwx      192   Oct 9 2009 13:00:50 +00:00  c2960-lanbasek9-mz.122-46.SE.bin
  622  drwx      128   Oct 9 2009 13:03:05 +00:00  tshoot


ALS1#cd tshoot
ALS1#dir
Directory of flash:/tshoot/

  623  -rwx        6582  Oct 9 2009 13:03:05 +00:00    Lab31-ALS1-Base-Cfg.txt
  624  -rwx        6578  Oct 9 2009 12:32:48 +00:00    Lab41-ALS1-TT-A-Cfg.txt
<output omitted>

Alternatively, you can see the contents of the directory by specifying its name
using the dir command. For example:

ALS1#dir flash:/tshoot
Directory of flash:/tshoot/

    5  -rwx        6515   Oct 9 2009 14:39:42 +00:00  Lab31-ALS1-Base-Cfg.txt
```

Note: When the **`show flash`** command is used on a router, it lists the directories and the files within them. The following example uses only the **`show flash`** command on router R1. The tshoot directory and its contents are listed.

```
R1#show flash:
-#- --length-- -----date/time------ path
1     38266988 Sep 24 2009 17:47:14 c1841-advipservicesk9-mz.124-24.T1.bin
2            0 Oct 09 2009 12:32:06 tshoot
3         2288 Oct 09 2009 12:32:48 tshoot/Lab31-R1-Base-Cfg.txt
<output omitted>
```

Instructor Notes:

- To create a directory in flash memory, use the **mkdir** {**flash: | slot0:**} command.

  Example: ALS1#**`mkdir flash:/tshoot`**

  ```
  Create directory filename [tshoot]?
  Created dir flash:/tshoot
  ```

- The following example shows how to copy a configuration file from a TFTP server at IP address 10.1.50.1 to the flash:/tshoot directory on ALS1:

  ALS1#**`copy tftp://10.1.50.1/Lab31-ALS1-Base-Cfg.txt flash:/tshoot`**

  Note: This assumes the configuration files are in the TFTP server default directory.

- You can view the contents of a particular file in flash using the UNIX or Cisco IOS **`more`** command. For example:

  ALS1#**more flash:/tshoot/Lab31-ALS1-Base-Cfg.txt**

  This command displays the contents of the file a page at a time.

Step 2: Erase the startup config from NVRAM.

```
ALS1#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
Erase of nvram: complete
```

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

```
ALS1#delete vlan.dat
Delete flash:vlan.dat? [confirm]
```

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

```
ALS1#reload

System configuration has been modified. Save? [yes/no]: no
Proceed with reload? [confirm]

*Oct   1 00:29:28.704: %SYS-5-RELOAD: Reload requested by console. Reload
Reason:  Reload command.
```

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

```
Press RETURN to get started!

         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no

Would you like to terminate autoinstall? [yes]: Enter
```

Step 6: Copy the specified lab device configuration file from flash to the running config.

```
Switch>enable
Switch#copy flash:/tshoot/Lab31-ALS1-Base-Cfg.txt running-config
Destination filename [running-config]? Enter

ALS1#
```

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.

Depending on the IOS version, AUTOSAVE may automatically save a copy of the running config to NVRAM for startup.

Note: AUTOSAVE does *not* copy the line con and vty configurations from the running config to the startup config. To ensure that the startup configuration is complete, you must copy manually.


```
ALS1#copy running-config startup-config
Building configuration...
[OK]
```

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

Step 8: Repeat Steps 1 through 7 for the other devices in the network.

Step 9: Configure the PCs.

a. Configure SRV1 with the static IP address 10.1.50.1/24 and the default gateway 10.1.50.254.

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

Step 10: Test basic network connectivity between devices.

a. Ping from PC-B to SRV1 at 10.1.50.1. Were the pings successful?

____

Yes

b. Ping from ALS1 to R2 at loopback 10.1.202.1. Were the pings successful?

____

Yes

Note: If the pings are not successful, contact your instructor.

Task 3: Analyze and Document the Physical Lab Topology

Note: At this time, only examine and document the physical connections. Documenting the logical topology, such as subnets, IP addresses, and routing protocols, is addressed in Task 4 of this lab.

Step 1: Review the physical topology diagram on page 1 of the lab.

Step 2: Use Cisco Discovery Protocol and show commands to verify the Layer 1 and Layer 2 connections of the lab topology.

a. Use the **show cdp** command to discover the interfaces associated with the physical connections. Fill in the correct device and interface designators in the following Device Links table and label them on the physical topology diagram on the first page of the lab.

```
ALS1#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
DLS2.tshoot.net  Fas 0/4           144          R S I     WS-C3560- Fas 0/2
DLS2.tshoot.net  Fas 0/3           144          R S I     WS-C3560- Fas 0/1
DLS1.tshoot.net  Fas 0/2           134          R S I     WS-C3560- Fas 0/2
DLS1.tshoot.net  Fas 0/1           134          R S I     WS-C3560- Fas 0/1

DLS1#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
R1.tshoot.net    Fas 0/5           164          R S I     1841      Fas 0/1
ALS1.tshoot.net  Fas 0/2           163           S I      WS-C2960- Fas 0/2
```



```
ALS1.tshoot.net  Fas 0/1           163           S I      WS-C2960- Fas 0/1
DLS2.tshoot.net  Fas 0/4           171         R S I      WS-C3560- Fas 0/4
DLS2.tshoot.net  Fas 0/3           170         R S I      WS-C3560- Fas 0/3
```

b. Review the configurations of the devices for using Layer 1 and Layer 2 features, such as trunks and EtherChannels. Fill in the information in the Device Links table and add it to the diagram. If a link is accounted for from one device to another, it is not necessary to repeat the entry from the other device. The first entry for ALS1, interface Fa0/1 is filled in as an example.

   Which other commands could you use to identify Layer 1 and Layer 2 characteristics?

   ____

   ____

   ____

   Answers will vary but could include: **`show run, show etherchannel summary, show int trunk, sh int switchport`**.

```
ALS1#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Po1         on               802.1q         trunking      900
Po2         on               802.1q         trunking      900

Port        Vlans allowed on trunk
Po1         10,20,30,100
Po2         10,20,30,100

ALS1#show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
---

1      Po1(SU)          -        Fa0/1(P)    Fa0/2(P)
2      Po2(SU)          -        Fa0/3(P)    Fa0/4(P)
```


Device Links Table

From Device	Interface	To Device	Interface	Layer 1 and 2 Features and Protocols Used
ALS1	Fa0/1	DLS1	Fa0/1	EtherChannel Po1, 802.1Q
ALS1	Fa0/2	DLS1	Fa0/2	EtherChannel Po1, 802.1Q
ALS1	Fa0/3	DLS2	Fa0/1	EtherChannel Po2, 802.1Q
ALS1	Fa0/4	DLS2	Fa0/2	EtherChannel Po2, 802.1Q
ALS1	Fa0/18	PC-B	NIC	100Base-T
DLS1	Fa0/3	DLS2	Fa0/3	EtherChannel Po10, 802.1Q
DLS1	Fa0/4	DLS2	Fa0/4	EtherChannel Po10, 802.1Q
DLS1	Fa0/5	R1	Fa0/1	100Base-T, DLS1 Fa0/5 is a routed L3 port (logical)
DLS1	Fa0/6	SRV1	NIC	100Base-T
DLS2	Fa0/5	R3	Fa0/1	100Base-T, DLS2 Fa0/5 is a routed L3 port (logical)
DLS2	Fa0/18	PC-C	NIC	100Base-T
R1	S0/0/0	R2	S0/0/0	WAN link, PPP
R2	S0/0/1	R3	S0/0/1	WAN link, PPP

c. Verify that all physical links shown in the diagram are operational. Which commands did you use?

____

____

Answers will vary but could include: **`show interfaces`, `show cdp neighbors`, `show interface status`, `show vlan`**.

Step 3: Map the VLANs used in the lab to the devices in the diagram.

Fill in the VLAN Definition table and label the physical topology diagram with the VLANs used for this topology. Identify all host devices that are members of each VLAN. The first entry for VLAN 10 is filled in as an example.

VLAN Definition Table

VLAN #	Name	Description	VLAN Members
10	OFFICE	Office VLAN	ALS1, DLS1, DLS2, PC-B
20	VOICE	Voice VLAN	ALS1, DLS1, DLS2
30	GUEST	Guest VLAN	ALS1, DLS1, DLS2, PC-C
50	SERVERS	Internal Servers	DLS1, DLS2, SRV1
100	MGMT	Management VLAN	ALS1, DLS1, DLS2
900	NATIVE	Trunk link VLAN	ALS1, DLS1, DLS2
999	UNUSED	Unused switch ports	ALS1, DLS1, DLS2

Step 4: Analyze spanning tree for the Layer 2 switched domain.

a. Analyze the spanning tree characteristics of the Layer 2 switched portion of the network. Which type of spanning-tree mode is implemented?

____

Rapid Per VLAN Spanning Tree (Rapid-PVST)

b. Which switch is the root switch for each VLAN, and what are the configured spanning-tree priorities?

____

____

____

Switch DLS1 is the root bridge for VLANs 10, 30, and 100. For these VLANs, the DLS1 priority is 24576, and the DLS2 priority is 28672. Switch DLS2 is the root bridge for VLANs 20 and 50. For these VLANs, The DLS1 priority is 28672, and the DLS2 priority is 24576.

c. What is the resulting spanning-tree topology for VLANs that have client devices connected?

____

____

____

____

For VLANs 10, 30, and 100, ALS1-Po1=Root/FWD, ALS1-Po2=Altn/BLK, DLS1-Po1=Desg/FWD, DLS1-Po10=Desg/FWD, DLS2-Po2=Desg/FWD, and DLS2-Po10=Root/FWD.

For VLANs 20 and 50, ALS1-Po1=Altn/BLK, ALS1-Po2=Root/FWD, DLS1-Po1=Desg/FWD, DLS1-Po10=Root /FWD, DLS2-Po2=Desg/FWD, and DLS2-Po10=Desg/FWD.

d. Which commands did you use to analyze the spanning-tree characteristics?

____

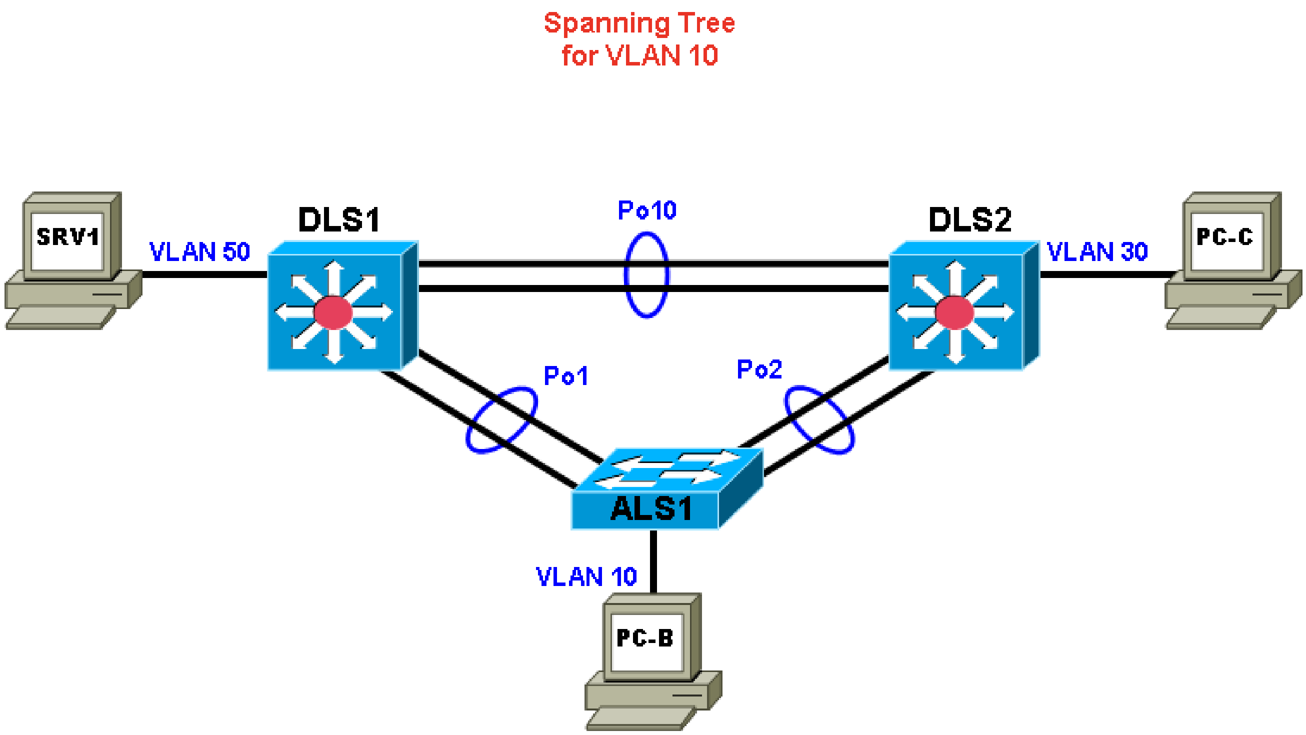
____

Answer will vary but could include **`show run`** and **`show spanning-tree vlan`** *`vlan-id`*.

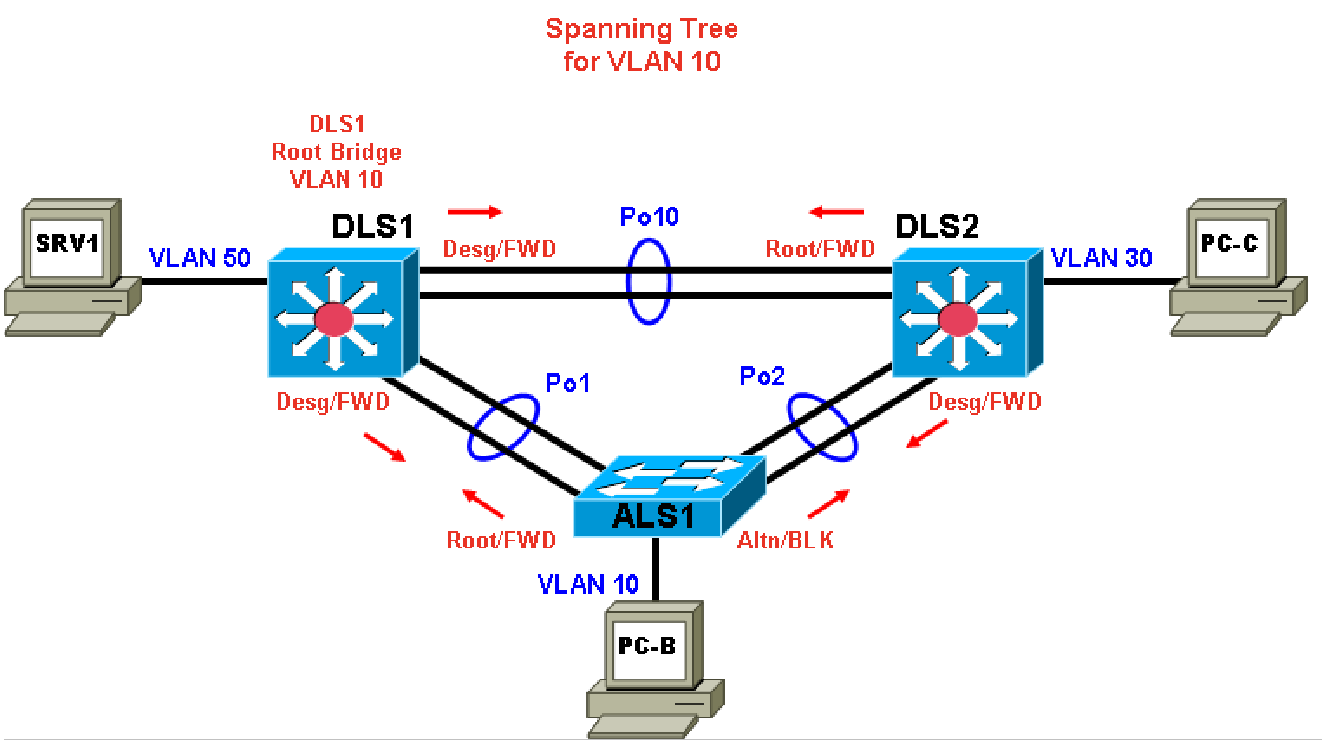
Step 5: Diagram the spanning tree for VLAN 10.

a. Label the STP role, port status, and direction for each port channel used in the physical topology diagram below.

VLAN 10 spanning tree for STUDENT version of lab



VLAN 10 spanning tree for INSTRUCTOR version of lab



Output for VLAN 10 on all three switches is shown as an example:

```
ALS1#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    24586
             Address     0017.5a5b.b400
             Cost        12
             Port        56 (Port-channel1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     001b.0c6d.8f00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------

Fa0/18              Desg FWD 19        128.18   P2p Edge
Po1                 Root FWD 12        128.56   P2p
Po2                 Altn BLK 12        128.64   P2p

DLS1#show spanning-tree vlan 10
```



```
VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    24586
             Address     0017.5a5b.b400
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24586  (priority 24576 sys-id-ext 10)
             Address     0017.5a5b.b400
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- -------------------------

Po1                 Desg FWD 12        128.56   P2p
Po10                Desg FWD 12        128.128  P2p


DLS2#sh spanning-tree vlan 10

VLAN0010
   Spanning tree enabled protocol rstp
     Root ID    Priority    24586
                Address     0017.5a5b.b400
                Cost        12
                Port        128 (Port-channel10)
                Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

     Bridge ID  Priority    28682  (priority 28672 sys-id-ext 10)
                Address     0017.5a53.a380
                Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
                Aging Time 300

   Interface           Role Sts Cost      Prio.Nbr Type
   ------------------- ---- --- --------- -------- ----------------------

   Po2                 Desg FWD 12        128.64   P2p
   Po10                Root FWD 12        128.128  P2p
```

b. If working as a team, discuss your findings with your teammates to ensure that all team members understand the physical and data link aspects of the network design.

Student Notes

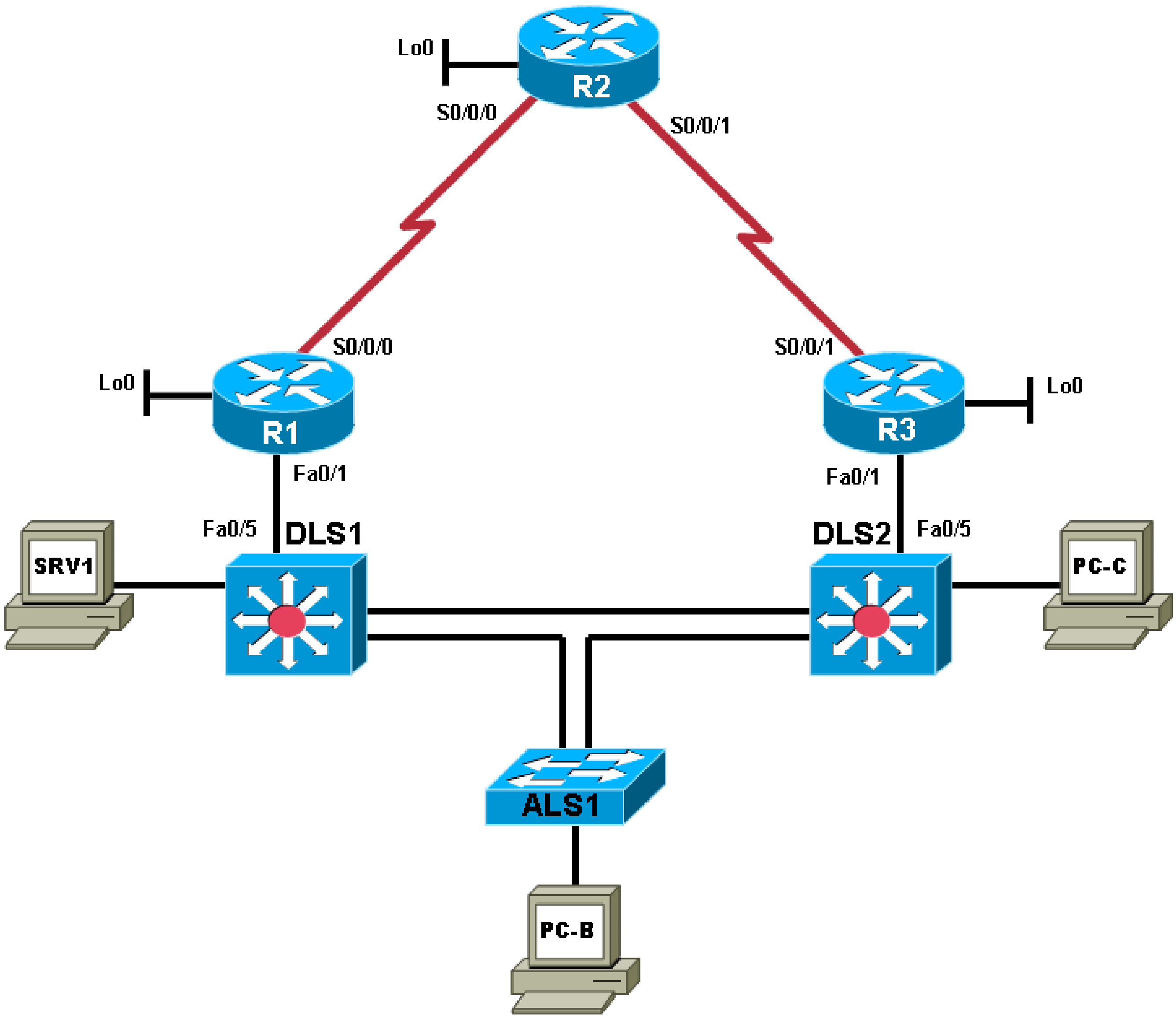
Use this space to make any additional notes regarding the physical configuration and the commands used.

Task 4: Analyze and Document the Logical Lab Topology

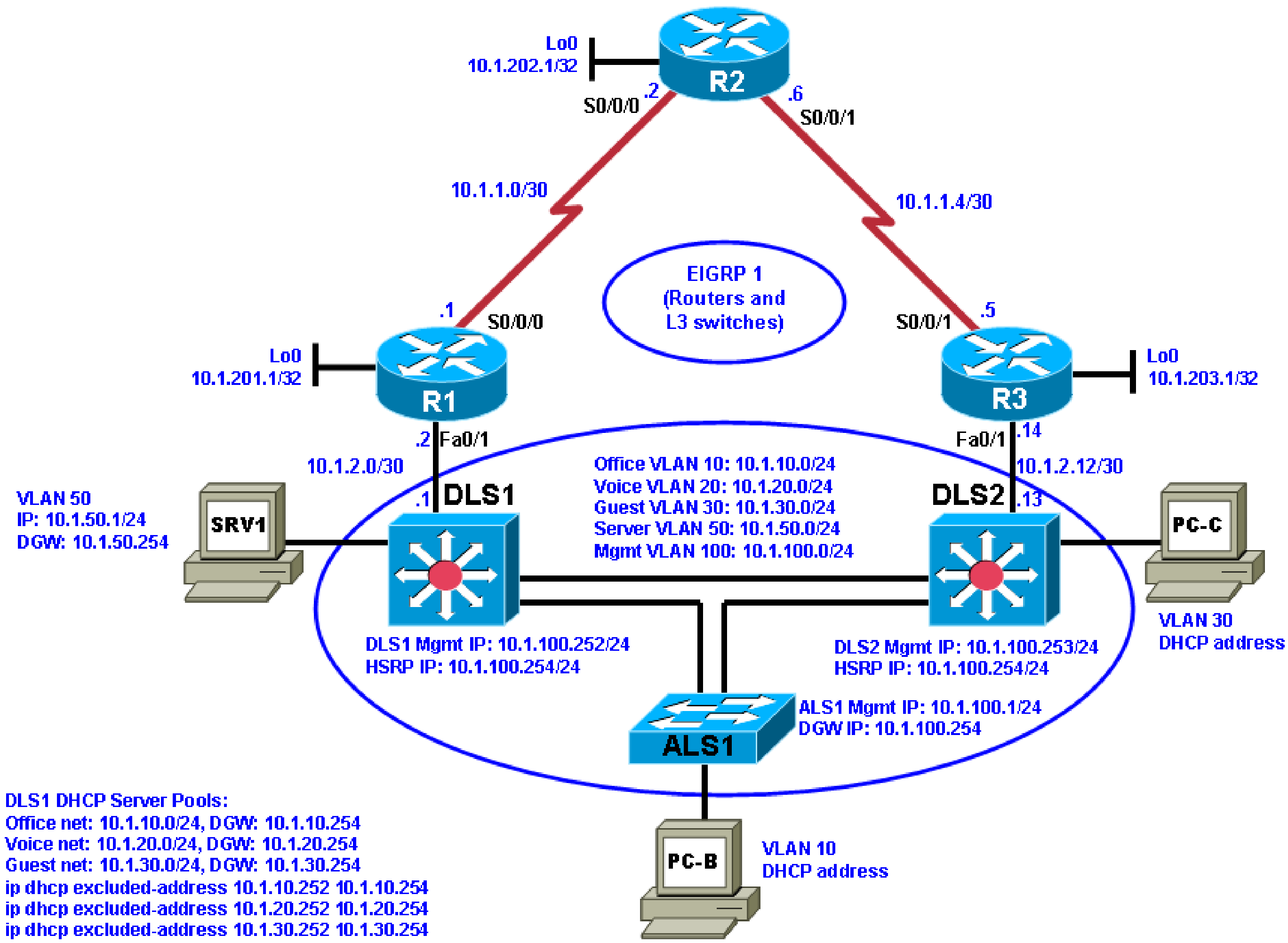
Step 1: Review the logical lab diagram and the subnets.

Review the IP subnets in the Subnet table for the VLANs and WAN links that are used in the lab network. Router interface designations from the physical topology diagram are provided.

Logical Topology for STUDENT version of lab



Logical Topology for INSTRUCTOR version of lab



Subnet Table

Description	Subnet	Prefix	Devices
VLANs			
Office VLAN 10	10.1.10.0	/24	PC-B
Voice VLAN 20	10.1.20.0	/24	N/A
Guest VLAN 30	10.1.30.0	/24	PC-C
Servers VLAN 50	10.1.50.0	/24	SRV1
Management VLAN	10.1.100.0	/24	ALS1, DLS1, DLS2
WAN Links			
DLS1 – R1	10.1.2.0	/30	DLS1 and R1 FE link
DLS2 – R3	10.1.2.12	/30	DLS2 and R3 FE link
R1 – R2	10.1.1.0	/30	R1 and R2 serial link
R2 – R3	10.1.1.4	/30	R2 and R3 serial link

Step 2: Map the subnet scheme to the logical diagram.

In the previous step, the subnets were documented in the Subnet table. Now document the host portion of the addresses. To document the host part, research the routing tables and interface IP addresses of all the devices. Document the management VLAN and interface addresses in the IP Address table and on the logical topology diagram. Use only the number of the last octet for IP addresses in the diagram. The device names and interfaces are listed to help identify the IP addresses. The entry for ALS1 VLAN 100 is shown as an example. If an interface is not in use, indicate this in the Additional Information column. Account for all interfaces on the routers.

IP Address Table

Device Name Abbreviation	Interface	Network Address and Prefix	Additional Information
ALS1	Vlan 100	10.1.100.1/24	SVI
DLS1	Vlan 100	10.1.100.252/24	SVI
DLS1	Fa0/5	10.1.2.1/30	Routed port to R1
DLS2	Vlan 100	10.1.100.253/24	SVI
DLS2	Fa0/5	10.1.2.13/30	Routed port to R3
R1	Fa0/0	N/A	Not used at this time
R1	Fa0/1	10.1.2.2/30	
R1	S0/0/0	10.1.1.1/30	
R1	S0/0/1	N/A	Not used at this time
R1	Loopback 0	10.1.201.1/32	
R2	Fa0/0	N/A	Not used at this time
R2	Fa0/1	N/A	Not used at this time
R2	S0/0/0	10.1.1.2/30	
R2	S0/0/1	10.1.1.6/30	
R2	Loopback 0	10.1.202.1/32	
R3	Fa0/0	N/A	Not used at this time
R3	Fa0/1	10.1.2.14/30	
R3	S0/0/0	N/A	Not used at this time
R3	S0/0/1	10.1.1.5/30	
R3	Loopback 0	10.1.203.1/32	
SRV1	NIC	10.1.50.1/24	Static address
PC-B	NIC	Varies	Address via DHCP
PC-C	NIC	Varies	Address via DHCP

Step 3: Analyze and document control plane logical configuration features.

Analyze the configurations of the devices for control plane features such as routing protocols, First Hop Redundancy Protocols (FHRPs), dynamic host configuration protocol (DHCP), and network address translation (NAT). Review, document, and discuss the following aspects of the logical network configuration.

a. Is dynamic or static routing being used?

dynamic

b. If dynamic, which routing protocol?

EIGRP

c. Are FHRPs in use, such as the Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), or Gateway Load Balancing Protocol (GLBP)? If yes, which one?

Yes. HSRP

d. What is the active router for all relevant VLANs?

DLS1 is the active router for VLANs 10, 30, and 100. DLS2 is the standby. DLS2 is the active router for VLANs 20 and 50, and DLS1 is the standby.

e. From the PC-B command prompt, issue the **tracert** command to router R2 loopback 0 at 10.1.202.1. What path did the packets take?

PC-B to DSL1 VLAN 10 IP address 10.1.10.252 (active HSRP router for VLAN 10) to R1 at 10.1.2.2 to R2 at 10.1.202.1.

```
C:\>tracert 10.1.202.1

Tracing route to 10.1.202.1 over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms 10.1.10.252
  2     1 ms    <1 ms    <1 ms 10.1.2.2
  3     7 ms     7 ms     7 ms 10.1.202.1

Trace complete.
```

f. Are any access lists used to filter traffic on the network? If yes, describe their function.

Not at this time.

g. Is DHCP in use? If yes, which DHCP server is used and for which VLANs present in the logical topology diagram?

Yes. DLS1 is the DHCP server for VLANs 10, 20, and 30.

h. If working as a team, discuss your findings with your teammates to ensure that all team members understand the high-level design of the network.

Notes

Use this space to make any additional notes regarding the logical configuration and the commands used.

Task 5: Identify Troubleshooting and Maintenance Tools

Step 1: Analyze device configurations for troubleshooting and maintenance features.

Analyze the configurations of the devices for services that support troubleshooting and maintenance, such as syslog, Simple Network Management Protocol (SNMP), and other network management features.

Step 2: Document the troubleshooting and maintenance features.

a. Document the troubleshooting and maintenance applications or tools in use with the network devices in the Troubleshooting and Maintenance Tools table. An entry for system logging is provided as an example.

Troubleshooting and Maintenance Tools Table

Configured Feature	Devices	Target Server	Target Tool or Application
System message logging	All	SRV1	Syslog server
Configuration archive	All	SRV1	TFTP server
SNMP traps	All	SRV1	Syslog server
NTP	All	R2	NTP server
NetFlow	R1 and R3	Local or SRV1	Local on the router or NetFlow Monitor on SRV1 (optional)

b. If working as a team, discuss your findings with your teammates to ensure that all team members know which maintenance and troubleshooting tools are available in the network.

Notes

Use this space to make any additional notes regarding troubleshooting and maintenance applications or tools.

Task 6: Identify the Security Measures Implemented

Step 1: Analyze device configurations for security-related features.

Analyze the configurations of your assigned devices for configuration options that help support a more secure network implementation, such as password security, login authentication, secure remote management, switch trunk and access port security, and VLANs. Record your entries in the Security Features table. An entry for password security is provided as an example.

Security Features Table

Security Feature Configured	Implementation Method or Commands
Password security	Enable secret, password encryption
Login authentication	AAA local database authentication
Secure remote management	SSH
Switch trunk port security	Switchport mode trunk, nonegotiate, unused native VLAN, VLANs allowed on trunk
Switch access port security	Switchport mode access, nonegotiate, PortFast, port security on ALS1 (max two sticky MAC addresses)
VLAN security	Unused ports placed in unused VLAN 999, VLANs allowed on trunk

Notes

Use this space to make any additional notes regarding security measures.

Note: Reference configurations for all devices are provided at the end of the lab. These are not the full **`show running-config`** output. Only the nondefault commands used to configure the devices are included (along with **`no shutdown`** on interfaces).

Lab Debrief Notes

Use this space to make notes of the key learning points that you picked up during the lab debrief discussions with your instructor. This can include alternate solutions, methods, and processes, procedure and communication improvements, as well as key commands and tools.

Note: This is your primary opportunity to document a baseline of the lab network before starting the troubleshooting exercises. During the debrief session, ask your instructor for clarification of any aspects of the network design and configurations that are unclear to you.

Instructor Notes: Presented here are points for the instructor to emphasize during the lab debriefing discussions.

Lab Design and Implementation: The focus of this lab is to allow the students to familiarize themselves with the lab environment. However, not all students might have the skills to independently map and analyze the network. Therefore, it is important that the instructor takes sufficient time to walk them through the physical and logical topology of the lab.

Be sure to review each major section (task) of the lab with the students to ensure that they have the network properly documented, both physically and logically.

The following details are important to point out:

- Process for loading device configuration files.
- The multiple commands that can be used to gather information. Discuss how different teams used different commands and how each of those commands revealed information about the network.
- Physical topology characteristics such as trunking protocols, WAN protocols, and EtherChannel.
- The spanning-tree topology and which switch is the root for each of the relevant VLANs.
- The use of routed ports and switch virtual interfaces (SVIs) and where they are used.
- The use of HSRP and which router performs the active role for each VLAN.
- Which routers or switches perform the role of DHCP server for which VLANs.
- Which maintenance and troubleshooting services have been implemented, such as NTP, TFTP, SNMP, syslog, archive, and NetFlow.
- Point out the use of the source interface SVI VLAN 100 on switches for logging, NTP, Telnet, SSH, and SNMP. The routers use source interface loopback 0 for logging, NTP, Telnet, SSH, SNMP, and NetFlow.
- Use of the archive utility in the configs, how it records versions of the running config, and how the path statement works to name files as they are sent to the TFTP server.
- Which security measures have been implemented, such as passwords, login authentication, trunks, and port VLANs.

Test points: Point out the main test points used in trouble tickets. The major Application Layer test used is browsing to a specific IP address. The major Network Layer tests are ping and traceroute to a specific IP address. Make clear that browsing the Internet should be possible from all clients. Most trouble tickets involve problems with lack of connectivity from one host or area of the network to another, resulting in the introduction of problems in the devices at OSI Layers 1, 2, 3, 4, and 7.

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1700	Fast Ethernet 0 (FA0)	Fast Ethernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
1800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2600	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)
2800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. Rather than try to list all the combinations of configurations for each router class, this table includes identifiers for the possible combinations of Ethernet and serial interfaces in the device. The table does not include any other type of interface, even though a specific router might contain one. An example of this is an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

Device Configurations

Important Instructor Note:

These are actual configuration commands (not running-config outputs) and include the **`no shutdown`** command for interfaces that should be up. Each device config can be copied from this lab and pasted into a text file and saved using the naming convention indicated in Task 2, Step 1 (for example, Lab31-ALS1-Base-Cfg.txt).

Each text file can then be copied to the device flash using TFTP, USB, flash card or another method. This preserves the **`no shutdown`** commands for interfaces. The file in flash can then be loaded into the running config using the procedure described in Task 2.

Caution: Pasting the configs into the running config and then copying them to flash does not preserve the **`no shutdown`** command for the interfaces, and they must be enabled manually.

Note: These configs include **`ip host`** *`name ip-addr`* entries for all devices. This can be helpful in accessing devices using Telnet with this lab. The ip host entries are only provided in this Lab 3-1 as the device IP addresses will change in subsequent labs.

Switch ALS1

```
!Lab 3-1 Switch ALS1 Baseline Config
!
hostname ALS1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
```



```
!
banner motd $*** Lab 3-1 Switch ALS1 Baseline Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip domain-name tshoot.net
ip host R1 10.1.2.2 10.1.1.1 10.1.201.1
ip host R2 10.1.1.2 10.1.1.6 10.1.202.1
ip host R3 10.1.1.5 10.1.2.14 10.1.203.1
ip host ALS1 10.1.100.1
ip host DLS1 10.1.100.252 10.1.2.1
ip host DLS2 10.1.100.253 10.1.2.13
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet

spanning-tree mode rapid-pvst
spanning-tree portfast default
!
interface Vlan1
 no ip address
 shutdown
!
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 100
 name MGMT
!
vlan 900
 name NATIVE
!
```



```
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel1
 description Channel to DLS1
 no shutdown
 !
interface Port-channel2
 description Channel to DLS2
 no shutdown
!
interface FastEthernet0/1
 description Channel to DLS1
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shutdown
!
interface FastEthernet0/2
 description Channel to DLS1
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shutdown
!
interface FastEthernet0/3
 description Channel to DLS2
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shutdown
!
interface FastEthernet0/4
 description Channel to DLS2
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shutdown
!
interface FastEthernet0/5
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/6
```



```
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown

interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
```

```
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description To PC-B
 switchport access vlan 10
 switchport mode access
 switchport voice vlan 20
 spanning-tree portfast
 switchport port-security
 switchport port-security maximum 2
 switchport port-security violation shutdown
 switchport port-security mac-address sticky
 no shut
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
```



```
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan100
 ip address 10.1.100.1 255.255.255.0
 no shutdown
!
ip default-gateway 10.1.100.254
!
ip http server
ip http secure-server
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server host 10.1.50.1 version 2c cisco
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps vlan-membership
```



```
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
  no transport input
!
ntp source Vlan100
ntp server 10.1.202.1
end
```

Switch DLS1

```
!Lab 3-1 Switch DLS1 Baseline Config
!
hostname DLS1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55

banner motd $*** Lab 3-1 Switch DLS1 Baseline Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
!
ip domain-name tshoot.net
ip host R1 10.1.2.2 10.1.1.1 10.1.201.1
ip host R2 10.1.1.2 10.1.1.6 10.1.202.1
ip host R3 10.1.1.5 10.1.2.14 10.1.203.1
ip host ALS1 10.1.100.1
ip host DLS1 10.1.100.252 10.1.2.1
ip host DLS2 10.1.100.253 10.1.2.13
!
ip dhcp excluded-address 10.1.10.252 10.1.10.254
ip dhcp excluded-address 10.1.20.252 10.1.20.254
ip dhcp excluded-address 10.1.30.252 10.1.30.254
```



```
!
ip dhcp pool OFFICE
   network 10.1.10.0 255.255.255.0
   default-router 10.1.10.254
   domain-name tshoot.net
!
ip dhcp pool VOICE
   network 10.1.20.0 255.255.255.0
   default-router 10.1.20.254
   domain-name tshoot.net
!
ip dhcp pool GUEST
   network 10.1.30.0 255.255.255.0
   default-router 10.1.30.254
   domain-name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 24576
spanning-tree vlan 20,50 priority 28672
!
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 100
 name MGMT
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
```



```
!
interface Port-channel1
 description Channel to ALS1
 no shut
!
interface Port-channel10
 description Channel to DLS2
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R1
 no switchport
 ip address 10.1.2.1 255.255.255.252
 speed 100
 duplex full
 spanning-tree bpduguard enable
 no shut
!
```

```
interface FastEthernet0/6
 description FE to SRV1
 switchport access vlan 50
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shut
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
```



```
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
```

```
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown

interface Vlan10
 ip address 10.1.10.252 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 priority 110
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.252 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.252 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 priority 110
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.252 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 preempt
!
```



```
interface Vlan100
 ip address 10.1.100.252 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 priority 110
 standby 100 preempt
!
router eigrp 1
 passive-interface default
 no passive-interface Fa0/5
 no auto-summary
 network 10.1.0.0 0.0.255.255
!
ip classless
ip http server
ip http secure-server
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server host 10.1.50.1 version 2c cisco
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 10.1.202.1
end
```

Switch DLS2

```
!Lab 3-1 Switch DLS2 Baseline Config
!
hostname DLS2
!
service timestamps debug datetime msec
service timestamps log datetime
service password-encryption
```



```
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 3-1 Switch DLS2 Baseline Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
ip domain-name tshoot.net
ip host R1 10.1.2.2 10.1.1.1 10.1.201.1
ip host R2 10.1.1.2 10.1.1.6 10.1.202.1
ip host R3 10.1.1.5 10.1.2.14 10.1.203.1
ip host ALS1 10.1.100.1
ip host DLS1 10.1.100.252 10.1.2.1
ip host DLS2 10.1.100.253 10.1.2.13
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
  path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 28672
spanning-tree vlan 20,50 priority 24576

vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
```



```
vlan 50
 name SERVERS
!
vlan 100
 name MGMT
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel2
 description Channel to ALS1
 no shut

interface Port-channel10
 description Channel to DLS1
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100
```



```
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R3
 no switchport
 ip address 10.1.2.13 255.255.255.252
 speed 100
 duplex full
 spanning-tree bpduguard enable
 no shut
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
```

```
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description FE to PC-C
 switchport access vlan 30
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
```

```
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 10.1.10.253 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.253 255.255.255.0
 standby 20 ip 10.1.20.254
```



```
 standby 20 priority 110
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.253 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.253 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 priority 110
 standby 50 preempt
!
interface Vlan100
 ip address 10.1.100.253 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 preempt
!
!
router eigrp 1
 passive-interface default
 no passive-interface Fa0/5
 no auto-summary
 network 10.1.0.0 0.0.255.255
!
ip classless
ip http server
ip http secure-server
!
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
```



```
!
ntp source Vlan100
ntp server 10.1.202.1
end
```

Router R1

```
!Lab 3-1 Router R1 Baseline Config
!
hostname R1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 3-1 Router R1 Baseline Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
ip host R1 10.1.2.2 10.1.1.1 10.1.201.1
ip host R2 10.1.1.2 10.1.1.6 10.1.202.1
ip host R3 10.1.1.5 10.1.2.14 10.1.203.1
ip host ALS1 10.1.100.1
ip host DLS1 10.1.100.252 10.1.2.1
ip host DLS2 10.1.100.253 10.1.2.13
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 10.1.201.1 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown
```



```
!
interface FastEthernet0/1
 description FE to DLS1
 ip address 10.1.2.2 255.255.255.252
 ip flow ingress
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
 description WAN link to R2 - 128k leased line
 ip address 10.1.1.1 255.255.255.252
 ip flow ingress
 encapsulation ppp
 clock rate 128000
  no shutdown
!
interface Serial0/0/1
 description WAN link to R3 (not used)
 no ip address
 shutdown
!
router eigrp 1
 passive-interface default
 no passive-interface FastEthernet0/1
 no passive-interface Serial0/0/0
 network 10.1.1.0 0.0.0.3
 network 10.1.2.0 0.0.0.3
 network 10.1.201.1 0.0.0.0
 no auto-summary
!
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
logging source-interface Loopback0
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
```

```
 transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 10.1.202.1
end
```

Router R2

```
!Lab 3-1 Router R2 Baseline Config
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
Hostname R2
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 3-1 Router R2 Baseline Config ***$
!
no ip domain lookup
ip host R1 10.1.2.2 10.1.1.1 10.1.201.1
ip host R2 10.1.1.2 10.1.1.6 10.1.202.1
ip host R3 10.1.1.5 10.1.2.14 10.1.203.1
ip host ALS1 10.1.100.1
ip host DLS1 10.1.100.252 10.1.2.1
ip host DLS2 10.1.100.253 10.1.2.13
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 10.1.202.1 255.255.255.255
!
```



```
interface FastEthernet0/0
 no ip address
 shutdown
!
interface FastEthernet0/1
 description optional connection for PC-C w/ static address
 no ip addr
 shutdown
!
interface Serial0/0/0
 description WAN link to R1 - 128k leased line
 ip address 10.1.1.2 255.255.255.252
 encapsulation ppp
 no shutdown

!
interface Serial0/0/1
 description WAN link to R3 - 128k leased line
 ip address 10.1.1.6 255.255.255.252
 clock rate 128000
 encapsulation ppp
 no shutdown
!
router eigrp 1
 passive-interface default
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
 network 10.1.1.0 0.0.0.3
 network 10.1.1.4 0.0.0.3
 network 10.1.202.1 0.0.0.0
 no auto-summary
!
ip http server
no ip http secure-server
!
logging source-interface Loopback0
logging 10.1.50.1
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
!
ntp master 3
 end
```

Router R3

```
!Lab 3-1 Router R3 Baseline Config
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 3-1 Router R3 Baseline Config ***$
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
no ip domain lookup
ip domain-name tshoot.net
ip host R1 10.1.2.2 10.1.1.1 10.1.201.1
ip host R2 10.1.1.2 10.1.1.6 10.1.202.1
ip host R3 10.1.1.5 10.1.2.14 10.1.203.1
ip host ALS1 10.1.100.1
ip host DLS1 10.1.100.252 10.1.2.1
ip host DLS2 10.1.100.253 10.1.2.13
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 10.1.203.1 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown

interface FastEthernet0/1
 description FE to DLS2
 ip address 10.1.2.14 255.255.255.252
 ip flow ingress
```



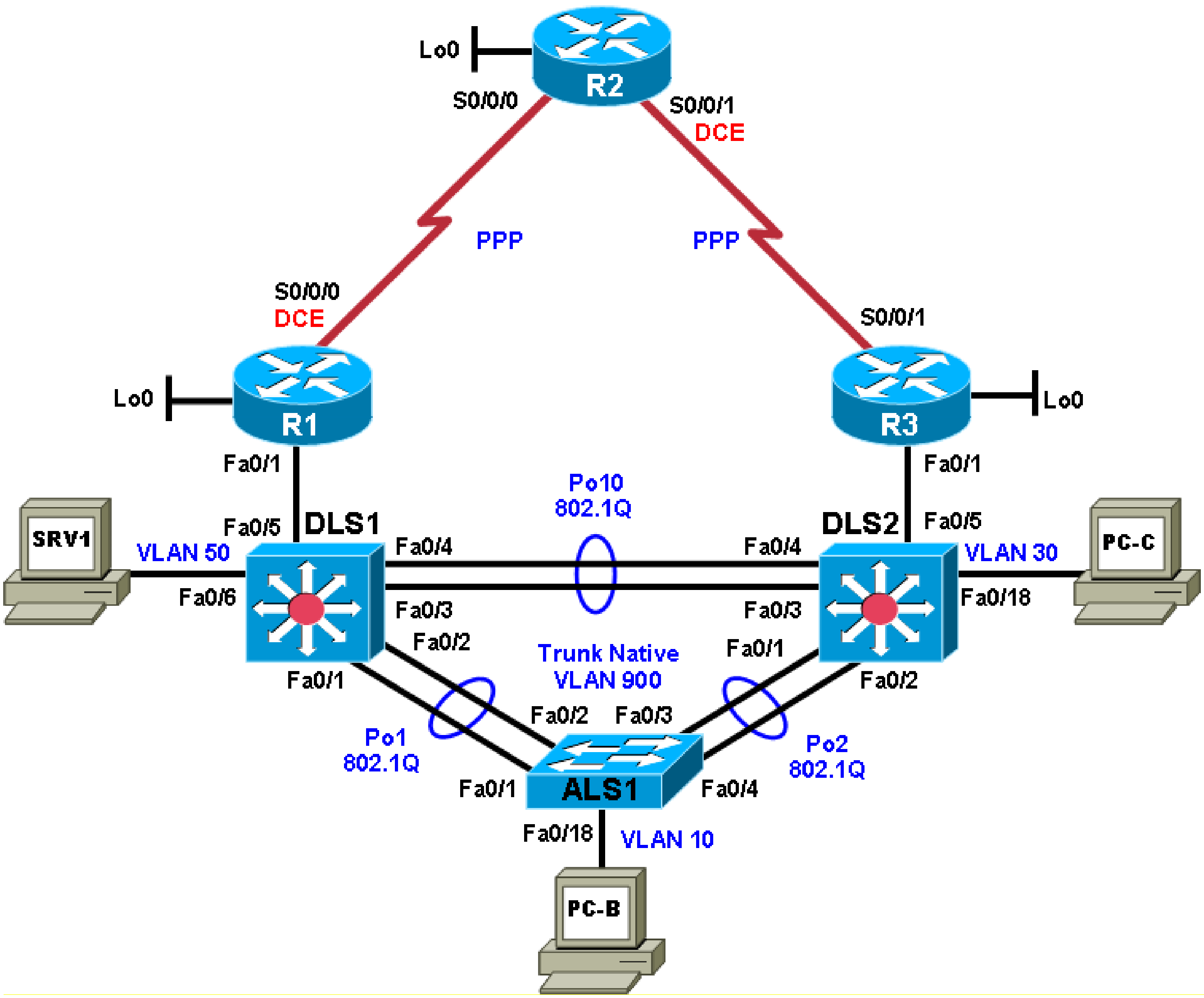
```
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
 description WAN link to R1 - (Not used)
 no ip address
 clock rate 128000
 encapsulation ppp
 shutdown
!
interface Serial0/0/1
 description WAN link to R2 - 128k leased line
 ip address 10.1.1.5 255.255.255.252
 ip flow ingress
 encapsulation ppp
 no shutdown
!
router eigrp 1
 passive-interface default
 no passive-interface FastEthernet0/1
 no passive-interface Serial0/0/1
 network 10.1.1.4 0.0.0.3
 network 10.1.2.12 0.0.0.3
 network 10.1.203.1 0.0.0.0
 no auto-summary
!
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
logging source-interface Loopback0
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
```



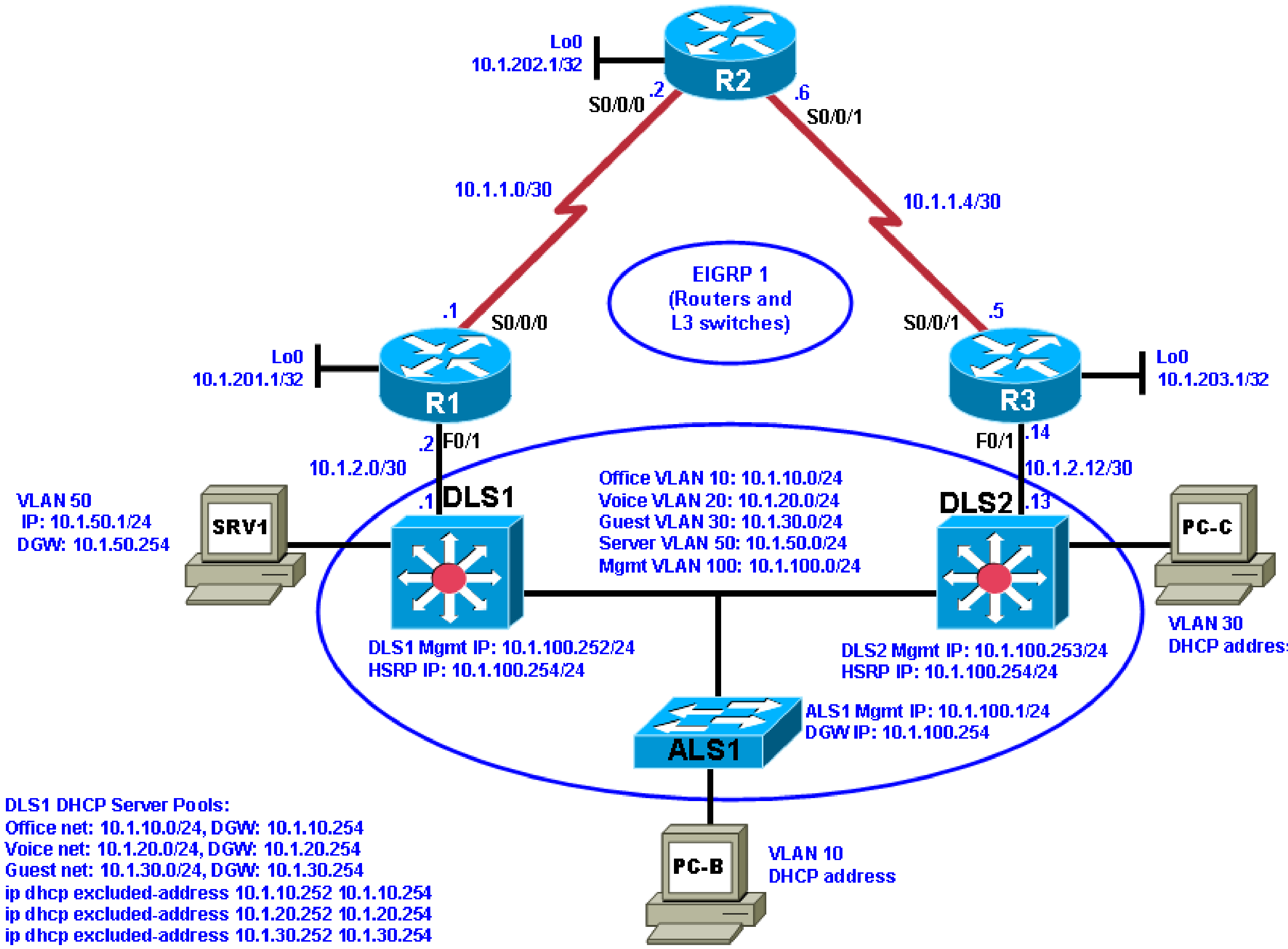
```
ntp server 10.1.202.1
end
```


Chapter 4 Lab 4-1, Layer 2 Connectivity and Spanning Tree **Instructor Version**

Physical Topology



Logical Topology



Objectives

- Load the device configuration files for each trouble ticket.
- Diagnose and resolve Layer 2 connectivity problems.
- Diagnose and resolve spanning-tree problems.
- Document the troubleshooting progress, configuration changes, and problem resolution.

Background

User computers, servers, and printers all connect to the access layer of the hierarchical model. With hundreds or thousands of hosts attached, access devices such as Layer 2 switches are a common source of networking issues. Physical and data-link problems at the access layer can include hardware, cabling, VLAN assignment, spanning tree, trunking protocol, or port security issues.

In this lab, you will troubleshoot various Layer 2 problems. For each task or trouble ticket, the scenario and symptoms are described. While troubleshooting, you will discover the cause of the problem, correct it, and then document the process and results.

Physical and Logical Topology Diagrams

The physical and logical topologies, including interface designations and IP addresses, are provided to assist the troubleshooting effort.

Lab Structure

This lab is divided into two main sections.

Section 1—Trouble Tickets and Troubleshooting Logs

This section includes multiple tasks. Each task is associated with a trouble ticket (TT) and introduces one or more errors on one or more devices. If time is a consideration, each task or trouble ticket can be performed independently.

Section 2—Troubleshooting Reference Information

This section provides general Layer 2 troubleshooting information that can be applied to any of the trouble tickets in this lab. Sample troubleshooting flows are provided, along with examples of useful commands and output. If time permits, it is recommended that you read through Section 2 prior to starting on the trouble tickets.

Note: This lab uses Cisco 1841 routers with Cisco IOS Release 12.4(24)T1 and the Advanced IP Services image c1841-advipservicesk9-mz.124-24.T1.bin. The switches are Cisco WS-C2960-24TT-L with the Cisco IOS image c2960-lanbasek9-mz.122-46.SE.bin and Catalyst 3560-24PS with the Cisco IOS image c3560-advipservicesk9-mz.122-46.SE.bin. Other routers (such as 2801 and 2811), switches (such as 2950 or 3550), and Cisco IOS Software versions can be used if they have comparable capabilities and features. Depending on the router or switch model and Cisco IOS Software version, the commands available and output produced might vary from what is shown in this lab.

Instructor note: Because the troubleshooting reference section is lengthy, it is advisable to have students read through it prior to starting the lab to become familiar with the troubleshooting flows and commands used. Consider assigning it as homework.

Note: Any changes made to the baseline configurations or topology (other than errors introduced) are noted in the trouble ticket so that you are aware of them prior to beginning the troubleshooting process.

Instructor Notes:

- The lab topology should be pre-built prior to the students starting the lab. Ensure that all routers and switches (R1, R2, R3, ALS1, DLS1, and DLS2) have the course lab configuration files installed in flash. You can download the files from the Academy Connection website.
- The device configurations that contain trouble ticket errors and modifications from the baseline are included at the end of the lab, and the errors in them are identified.
- Each device should have a directory named “tshoot” in flash. This directory contains the baseline configuration file for that device as well as the configuration files for the labs in this course. Refer to Lab 3-1 for instructions on creating the tshoot directory in flash.
- Instructors can use a TFTP server, USB drive, flash memory card or other method to copy all the course configuration files into the flash:/tshoot directory for each device in the topology.
- For this lab and subsequent labs, the student is responsible for loading the baseline or trouble ticket configurations as required using the procedure described in Lab 3-1.
- Set the correct time on router R2, which serves as the primary NTP server for the lab network.
- If time is an issue, each task (trouble ticket) can be performed independently.

Required Resources

- 3 routers (Cisco 1841 with Cisco IOS Release 12.4(24)T1 Advanced IP Service or comparable)
- 1 switch (Cisco 2960 with the Cisco IOS Release 12.2(46)SE C2960-LANBASEK9-M image or comparable)
- 2 switches (Cisco 3560 with the Cisco IOS Release 12.2(46)SE C3560-advipservicesK9-mz image or comparable)
- 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

Instructor Notes:

- This lab is divided into multiple tasks. Each task is associated with a trouble ticket (TT) and introduces one or more errors on one or more devices.
- Students can work individually or as a team. The problems introduced in this lab focus on the switching environment.
- Suggested actions and results presented during the troubleshooting process for each TT can be shared with the students during debrief or copies of the instructor version of the lab can be made available to the students to assist them in verifying their work.

Section 1—Trouble Tickets and Troubleshooting Logs

Task 1: Trouble Ticket Lab 4-1 TT-A

Instructor note: This trouble ticket involves access switch ALS1 issues related to an incorrect spanning-tree mode and a missing management VLAN.

Step 1: Review trouble ticket Lab 4-1 TT-A.

Late yesterday afternoon, access switch ALS1 failed, and you discovered that the power supply was not working. A junior colleague was tasked with replacing ALS1 with a comparable switch.

When you arrived this morning, you asked him how things went. He told you that he had stayed late trying to reconfigure ALS1, but was not entirely successful. Users on VLAN 10 have started to complain that they cannot get access to the network server SRV1, and you are unable to use Telnet to connect to ALS1 from SRV1. In addition, syslog messages from ALS1 are not being received on SRV1.

Your task is to diagnose the issues and restore switch ALS1 as a fully functional access switch on the network.

Step 2: Load the device trouble ticket configuration files for TT-A.

Using the procedure described in Lab 3-1, verify that the lab configuration files are present in flash. Load the configuration files indicated in the Device Configuration File table.

Note: The following device access methods are in effect after loading the configuration files:

- Console access requires no username or password.
- Telnet and SSH require username **admin** and password **adminpa55**.
- The enable password is **ciscoenpa55**.

Instructor note: Although it is not considered security best practice, the student can set the console and VTY line exec-timeout to 0 0 to facilitate performance of this lab.

Device Configuration File Table

Device Name	File to Load	Notes
ALS1	Lab41-ALS1-TT-A-Cfg.txt	This file contains configuration errors
DLS1	Lab41-DLS1-TT-A-Cfg.txt	This file is the same as the baseline
DLS2	Lab41-DLS2-TT-A-Cfg.txt	This file is the same as the baseline
R1	Lab41-R1-TT-A-Cfg.txt	This file is the same as the baseline
R2	Lab41-R2-TT-A-Cfg.txt	This file is the same as the baseline
R3	Lab41-R3-TT-A-Cfg.txt	This file is the same as the baseline
SRV1	N/A	Static IP: 10.1.50.1 Default gateway: 10.1.50.254
PC-B	N/A	DHCP (release and renew after loading device configurations)
PC-C	N/A	DHCP (release and renew after loading device configurations)

Instructor note: The student loads the “broken” TT configuration files for all devices even though only the configuration(s) indicated in the **Notes** column contains errors.

Step 3: Configure SRV1 and start the syslog and TFTP servers.

Ensure that SRV1 has static IP address 10.1.50.1 and default gateway 10.1.50.254.

Start the syslog server on SRV1, which is the syslog server for the entire network. When the network is properly configured, all devices send syslog messages to SRV1.

Start the TFTP server on SRV1, which is the archive server for the entire network. When the network is properly configured, all devices send archives of their running configurations to this server whenever the running config is copied to the startup config. Ensure that the default TFTP directory on SRV1 is set to the directory where you want to store the archives.

Instructor note: This lab uses tftpd32 for both TFTP and syslog. Other comparable tools can be used.

Step 4: Release and renew the DHCP leases on PC-B and PC-C.

Ensure that PC-B and PC-C are configured as DHCP clients.

After loading all TT-A device configuration files, issue the **ipconfig /release** and **ipconfig /renew** commands on PC-B and PC-C.

Note: Problems introduced into the network by the trouble ticket might prevent one or both of these PCs from acquiring an IP address. Do not assign either PC a static address.

Step 5: Outline the troubleshooting approach and validation steps.

Use this space to identify your troubleshooting approach and the key steps to verify that the problem is resolved. Troubleshooting approaches to select from include the follow-the-path, spot-the-differences, bottom-up, top-down, divide-and-conquer, shoot-from-the-hip, and move-the-problem methods.

Note: In addition to a specific approach, you can use the generic troubleshooting process described in the course, which can be found at the beginning of Section 2 of this lab.

____

____

____

____

____

____

The bottom-up or follow-the-path method can be used. Other methods are the top-down, divide-and-conquer, spot-the-differences, move-the-problem, and shoot-from-the-hip approaches.

Verification steps can include:

Switch ALS1 can be reached using Telnet from server SRV1.

PC-B, which is connected to switch ALS1, can acquire an IP address via DHCP.

PC-B, which is connected to switch ALS1, can ping server SRV1.

Syslog messages from ALS1 are received on SRV1.

Step 6: Record the troubleshooting process and configuration changes.

Note: Section 2 of this lab includes sample troubleshooting flows, useful commands, and examples of output.

Use this log to document your actions and results during the troubleshooting process. List the commands you used to gather information and, as you progress, record your thoughts as to what you think the problem might be and what actions you will take to correct the problems.

Device	Actions and Results

Responses will vary but could include:

- Pings from PC-B to SRV1 at 10.1.50.1 fail.
- Pings from PC-B to its default gateway 10.1.10.254 on DLS1 fail.
- A check of PC-B verifies that it is a DHCP client but has not acquired an IP address from DCHP server DLS1.
- Pings from ALS1 to DLS1 (10.1.100.252) and DLS2 (10.1.100.253) fail.

TT-A issue 1 – An incorrect spanning-tree mode is configured on ALS1

- The **`clear arp-cache`** and **`show arp`** commands on DLS1 and DLS2 indicate no Layer 3 connectivity between ALS1 and DLS1 or DLS2.

- The **`show cdp neighbors`** and **`show interfaces status`** commands on DLS1 and DLS2 indicate that the physical links to ALS1 are connected.
- The **`show spanning-tree`** command on DLS1 and DLS2 indicates that the spanning-tree mode is rapid per VLAN Spanning Tree (R-PVST) and that there is a separate instance for each VLAN.
- The **`show spanning-tree`** command on ALS1 indicates that the spanning-tree mode is Multiple Spanning Tree (MST) and that there is only one spanning-tree instance for all VLANs. Due to the inconsistency of spanning-tree modes between ALS1 and DLS1 and DLS2, both EtherChannels (Po1 and Po2) ports are put into a broken (BKN) state (not forwarding). This is because a successful cooperation of MST with R-PVST has certain prerequisites that have not been met in this topology.

Action: Change the spanning-tree mode on ALS1 to rapid PVST to enable the port channels to forward on a per spanning-tree basis. Refer to TT-A debrief for more information.

Pings from PC-B to SRV1 and other locations should now be successful.

TT-A issue 2 - Management VLAN 100 is missing on ALS1

- Telnet from SRV1 to switch ALS1 management address 10.1.100.1 fails.
- The **`show ip interface brief`** command on ALS1 indicates that the VLAN 100 SVI interface is configured with the correct IP address, but the protocol is down.
- The **`show vlan brief`** command on ALS1 indicates that the management VLAN 100 definition is missing.

Action: Add VLAN 100 with the name MGMT to switch ALS1. Refer to TT-A debrief for more information.

Verification: Using Telnet from SRV1 to ALS1 should now be successful. The logging source interface on ALS1 was set to SVI VLAN 100, so syslog messages can now be sent to SRV1.

Step 7: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with your instructor. The notes can include problems encountered, solutions applied, useful commands employed, alternate solutions, methods, and processes, and procedure and communication improvements.

____

____

____

____

____

____

____

Trouble ticket TT-A Debrief – Instructor Notes:

TT-A Issue 1

On switch ALS1, the spanning-tree mode was set to MST, causing the uplink ports to be placed in broken (BKN) spanning-tree state. This effectively blocks all traffic on the uplinks to switches DLS1 and DLS2. It prevents DHCP clients (PC-B, in this case) in VLAN 10 from getting their IP address information from DHCP server DLS1.

This issue can be remedied by issuing the following command on switch ALS1:

```
spanning-tree mode rapid-pvst
```


Note: If PC-B was rebooted, it might have acquired an autoconfigured IP address (169.254.x.x/16), but there is no default gateway. It might be necessary to issue the **`ipconfig /release`** and **`ipconfig /renew`** commands on DHCP clients after the network device problems are resolved to allow PC-B to acquire an IP address in the VLAN 10 subnet from DLS1.

TT-A Issue 2

You cannot use Telnet to connect to switch ALS1 from server SRV1 (or from any other point in the network) because VLAN 100, the management VLAN, is not present on switch ALS1. As a result, the VLAN interface on switch ASL1 for VLAN 100 will be down. SVI VLAN 100 has been assigned a valid IP address, but this does not affect the Layer 2 issues of the missing VLAN definition.

By issuing the following commands, the VLAN interface will become operational again, and connectivity to the management address of switch ALS1 will be restored:

```
vlan 100
  name MGMT
```

Task 2: Trouble Ticket Lab 4-1 TT-B

Instructor note: This trouble ticket involves DLS1 and DLS2 issues related to incorrect port channel trunk encapsulation.

Step 1: Review trouble ticket Lab 4-1 TT-B.

After an equipment failure, a network technician was asked to configure bundled Ethernet links between the ALS1 access switch and the two distribution layer switches in the network (DLS1 and DLS2). Shortly after the changes were made, users on ALS1 were unable to access the Internet (simulated by Lo0 on R2). You have been asked to look into the problem and have determined that you are able to ping the Internet from SRV1.

Your task is to diagnose the issues, allow hosts on ALS1 to connect to the Internet via DLS1 or DLS2, and verify that the switching environment redundant paths are functional.

Note: To simulate an Internet connection, you can ping the R2 Lo0 address at 10.1.202.1. Alternately, you can use the PC browser to connect to 10.1.202.1. You will then be prompted for a login to the router management GUI by R2. Enter the username **admin** and enable password **ciscoenpa55**.

Step 2: Load the device trouble ticket configuration files for TT-B.

Using the procedure described in Lab 3-1, verify that the lab configuration files are present in flash. Load the configuration files indicated in the Device Configuration File table.

Note: See Task 1, Step 2 for device access methods, usernames, and passwords after the configuration files have been loaded.

Device Configuration File Table

Device Name	File to Load	Notes
ALS1	Lab41-ALS1-TT-B-Cfg.txt	This file is the same as the baseline
DLS1	Lab41-DLS1-TT-B-Cfg.txt	This file contains configuration errors
DLS2	Lab41-DLS2-TT-B-Cfg.txt	This file contains configuration errors
R1	Lab41-R1-TT-B-Cfg.txt	This file is the same as the baseline
R2	Lab41-R2-TT-B-Cfg.txt	This file is the same as the baseline
R3	Lab41-R3-TT-B-Cfg.txt	This file is the same as the baseline
SRV1	N/A	Static IP: 10.1.50.1 Default gateway: 10.1.50.254
PC-B	N/A	DHCP (release and renew after loading device

		configurations)
PC-C	N/A	DHCP (release and renew after loading device configurations)

Step 3: Configure SRV1 and start the syslog and TFTP servers as described in Task 1.

Step 4: Reboot PC-B and PC-C or release and renew the DHCP lease as described in Task 1.

Step 5: Outline the troubleshooting approach and validation steps.

Use this space to identify your troubleshooting approach and the key steps to verify that the problem is resolved. . Troubleshooting approaches to select from include the follow-the-path, spot-the-differences, bottom-up, top-down, divide-and-conquer, shoot-from-the-hip, and move-the-problem methods.

Note: In addition to a specific approach, you can use the generic troubleshooting process described at the beginning of Section 2 of this lab.

____

____

____

____

____

The bottom-up or follow-the-path method can be used. Other methods are the top-down, divide-and-conquer, spot-the-differences, move-the-problem, and shoot-from-the-hip approaches.

Verification steps can include:

PC-B, which is connected to switch ALS1, can acquire an IP address via DHCP.

PC-B, which is connected to switch ALS1, can ping and browse the Internet via IP.

Using the **`show cdp neighbors`** command on ALS1 indicates that both DLS1 and DLS2 are neighbors.

Using the **`show etherchannel summary`** command indicates that trunks to both DLS1 and DLS2 are up and functional.

Further verification of the redundant switch paths could involve shutting down the port channel interface Po1 on DLS1 and pinging from PC-B to the Internet and then disabling the port channel interface Po2 on DLS2 and pinging from PC-B to the Internet.

Step 6: Record the troubleshooting process and configuration changes.

Note: Section 2 of this lab includes sample troubleshooting flows, useful commands, and examples of output.

Use this log to document your actions and results during the troubleshooting process. List the commands you used to gather information. As you progress, record what you think the problem might be and what actions you will take to correct the problem.

Device	Actions and Results

Device	Actions and Results

Answers will vary but could include:

- Pings from PC-B to R2 Lo0 (simulated ISP 10.1.202.1) fail.
- Pings from PC-B to its default gateway 10.1.10.254 on DLS1 fail.
- A check of PC-B verifies that it is a DHCP client but has not acquired an IP address from DCHP server DLS1.
- Pings from ALS1 to DLS1 (10.1.100.252) and DLS2 (10.1.100.253) fail.

TT-B issue 1 - Encapsulation is set to ISL on DLS1 port channel interface Po1.

- The **`clear arp-cache`** and **`show arp`** commands on DLS1 and DLS2 indicate no Layer 3 connectivity between ALS1 and DLS1 or DLS2.
- The **`show cdp neighbors`** command on ALS1 indicates that DLS1 and DLS2 are no longer its neighbors.
- The **`show cdp neighbors`** command on DLS1 indicates that DLS2 and R1 are neighbors.

- The **`show interfaces status`** command on DLS1 indicates that the physical links to ALS1 are connected.
- The **`show vlan id 10`** command on ALS1 and DLS1 indicates that VLAN 10 contains the correct ports.
- The **`show spanning-tree vlan 10`** command on ALS1 and DLS1 indicates that all port channels are designated and forwarding.
- The **`show interfaces trunk`** command on ALS1 indicates that Po1 (to DLS1) and Po2 (to DLS2) both use 802.1 encapsulation and native VLAN 900.
- The **`show interfaces trunk`** command on DLS1 indicates that Po1 (to ALS1) uses Inter-Switch Link (ISL) encapsulation, which is a mismatch with ALS1. No data frames will be transmitted.

Action: Change the encapsulation of DLS1 EtherChannel Po1 to 802.1Q (this also changes the physical ports). Refer to TT-B debrief for more information.

Verification: PC-B should acquire an IP address from DHCP server DLS1. You should now be able to ping from PC-B to its default gateway 10.1.10.254 on DLS1. PC-B now has access to the Internet (R2 Lo0 – 10.1.202.1).

TT-B issue 2 - Encapsulation is set to ISL on EtherChannel physical port interfaces.

- Next you must verify the existence of redundant paths from ALS1 to both DLS1 and DLS2.
- The **`show interfaces status`** command on DLS2 indicates that physical links to ALS1 are suspended.
- The **`show cdp neighbors`** command on ALS1 indicates that DLS1 is now a neighbor, but DLS2 is not.
- The **`show spanning-tree`** command on DLS2 does not show Po2 (to ALS1).
- The **`show interfaces trunk`** command on DLS2 does not show Po2 (to ALS1).
- The **`show etherchannel summary`** command on ALS1 indicates Po1 (to DLS1) and Po2 (to DLS2) as SU = Layer 2 and in use. All ports are P = bundled in the port channel.
- The **`show etherchannel summary`** command on DLS2 indicates Po2 (to ALS1) as SD = Layer 2 and down. Ports F0/1 and F0/2 are s = suspended.
- The **`show running-config interface po2`** command on DLS2 indicates that Po2 encapsulation is dot1q, the native VLAN is 900, and the trunks allowed are 10, 20, 30, 50, and 100.
- The **`show running-config interfaces F0/1`** and **`F0/2`** commands on DLS2 indicate that F0/1 encapsulation is ISL, the native VLAN is 900, and the trunk VLANs allowed are 10, 20, 30, 50, and 100. The physical port encapsulation is different than the port channel, which causes physical interfaces F0/1 and F0/2 to be suspended and the port channel interface to go down.

Action: Change the encapsulation on each physical interface to dot1q. Refer to TT-B debrief for more information.

Verification: The **`show cdp neighbors`** command on ALS1 now indicates that both DLS1 and DLS2 are neighbors. The **`show etherchannel summary`** command on DLS2 now indicates Po2 (to ALS1) as SU = Layer 2 and in use. Ports F0/1 and F0/2 are P = bundled in the port channel.

Step 7: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with your instructor. The notes can include problems encountered, solutions applied, useful commands employed, alternate solutions, methods and processes, and procedure and communication improvements.

Trouble Ticket TT-B Debrief – Instructor Notes

There are two separate problems with the uplinks between switch ALS1 and switches DLS1 and DLS2. The LAN is set up using redundant connections from switch ALS1 to switches DLS1 and DLS2. Therefore, lack of connectivity implies that there must be a problem with both redundant paths. To regain connectivity for the clients, only one of the two issues needs to be resolved. However, to regain the redundancy that is inherent in the physical network design, both issues must be diagnosed and resolved. Resolving one of the two problems might restore connectivity, but leaves a hidden issue. Proper verification should uncover both issues. If the trunk encapsulation problem is corrected on only DLS1 or DLS2, spanning tree adjusts the status of the ALS1 switch's Po1 and Po2 interfaces to account for the mismatch in the trunk encapsulation.

Ask the students if they found all issues and make them aware of the possibility of having hidden problems in a redundant network. Discuss which verification techniques could be used to find these types of issues.

TT-B Issue 1

On switch DLS1, the trunk encapsulation on the EtherChannel toward access switch ALS1 has been changed to ISL encapsulation. This causes all Layer 2 traffic on these links (including Cisco Discovery Protocol packets) to fail. Changing parameters on the port channel automatically changes them on the physical member ports, thus the parameter on the port channel and the individual ports remain consistent. The links stay up, and no errors other than potential oversized frames are recorded on the interfaces because ISL on DLS1 and 802.1Q on ALS1 are both using a valid Ethernet frame format. To remedy this situation, configure the following commands on DLS1:

```
interface Port-channel 1
    switchport trunk encapsulation dot1q
```

TT-B Issue 2

On switch DLS2, trunk encapsulation on the physical ports that are members of the EtherChannel toward the access switch have been changed to ISL encapsulation. The changing of physical port encapsulation causes an inconsistency between the configuration on the port channel 2 interface and the physical interfaces FastEthernet 0/1 and 0/2, which are members of the EtherChannel. This, in turn, causes the interfaces FastEthernet 0/1 and 0/2 to be suspended and the port channel interface to go down. To resolve this situation and restore the consistency between the configuration of the port channel interface and the FastEthernet interfaces, configure the following commands:

```
interface range FastEthernet 0/1 – 2
  switchport trunk encapsulation dot1q
```

Task 3: Trouble Ticket Lab 4-1 TT-C

Instructor note: This trouble ticket involves DLS2 with issues related to VLANs allowed on the trunk between the DLS2 switch and DLS1 and ALS1.

Step 1: Review trouble ticket Lab 4-1 TT-C.

This morning, the help desk received a call from an external consultant that needed access to the SRV1 guest account (simulated by ping). Her PC, PC-C, was plugged into one of the outlets that is patched to the guest VLAN on switch DLS2. However, she has not been able to get an IP address and cannot get onto the network.

Your task is to diagnose and solve this problem, making sure that the consultant gets access to SRV1.

Step 2: Load the device trouble ticket configuration files for TT-C.

Using the procedure described in Lab 3-1, verify that the lab configuration files are present in flash. Load the configuration files indicated in the Device Configuration File table.

Note: See Task 1, Step 2 for device access methods, usernames, and passwords after you have loaded the configuration files.

Device Configuration File Table

Device Name	File to Load	Notes
ALS1	Lab41-ALS1-TT-C-Cfg.txt	This file is the same as the baseline
DLS1	Lab41-DLS1-TT-C-Cfg.txt	This file is the same as the baseline
DLS2	Lab41-DLS2-TT-C-Cfg.txt	This file contains configuration errors
R1	Lab41-R1-TT-C-Cfg.txt	This file is the same as the baseline
R2	Lab41-R2-TT-C-Cfg.txt	This file is the same as the baseline
R3	Lab41-R3-TT-C-Cfg.txt	This file is the same as the baseline
SRV1	N/A	Static IP: 10.1.50.1 Default gateway: 10.1.50.254
PC-B	N/A	DHCP (release and renew after loading the device configurations)
PC-C	N/A	DHCP (release and renew after loading the device configurations)

Step 3: Configure SRV1 and start the syslog and TFTP servers, as described in Task 1.

Step 4: Reboot PC-B and PC-C or release and renew the DHCP lease, as described in Task 1.

Step 5: Outline the troubleshooting approach and validation steps.

Use this space to identify your troubleshooting approach and the key steps to verify that the problem is resolved. . Troubleshooting approaches to select from include the follow-the-path, spot-the-differences, bottom-up, top-down, divide-and-conquer, shoot-from-the-hip, and move-the-problem methods.

Note: In addition to a specific approach, you can use the generic troubleshooting process described at the beginning of Section 2 of this lab.

The bottom-up or follow-the-path method can be used. Other methods are the top-down, divide-and-conquer, spot-the-differences, move-the-problem, and shoot-from-the-hip approaches.

Verification steps can include:

PC-C, which is connected to switch DLS2, can acquire a VLAN 30 subnet IP address via DHCP.

PC-C, which is connected to switch DLS2, can access SRV1 using ping.

Using the **`show vlan`** and **`show interfaces trunk`** commands indicates that VLAN 30 is defined and allowed on both DLS2 trunks.

Step 6: Record the troubleshooting process and configuration changes.

Note: Section 2 of this lab includes sample troubleshooting flows, useful commands, and examples of output.

Use this log to document your actions and results during the troubleshooting process. List the commands you used to gather information. As you progress, record your thoughts as to what you think the problem might be and which actions you take to correct the problem.

Device	Actions and Results

Device	Actions and Results

Answers will vary but could include:

- Pings from PC-C on DLS2 to SRV1 fail.
- Pings from PC-C to its default (VLAN 30) gateway 10.1.30.254 fail.
- A check of PC-C verifies that it is a DHCP client but has not acquired an IP address from DCHP server DLS1.
- Pings from DLS2 (10.1.100.253) to ALS1 (10.1.100.1) and to DLS1 (10.1.100.252) are successful.
- The **`clear arp-cache`** and **`show arp`** commands on DLS2 indicate Layer 3 connectivity between ALS1 and DLS1 or DLS2.
- The **`show interfaces status`** command on DLS2 indicates that the physical links to ALS1 and DLS1 are connected.
- The **`show cdp neighbors`** command on DLS2 indicates that ALS1, DLS2, and R3 are neighbors.
- The **`show vlan brief`** command on DLS2 indicates that VLAN 30 exists and contains the port to which PC-C is connected (F0/18).
- The **`show spanning-tree vlan 30`** command on DLS2 indicates that the only port that is forwarding is F0/18. Port channel interfaces Po2 (to ALS1) and Po10 (to DLS1) are missing.
- The **`show interfaces trunk`** command on DLS2 indicates that EtherChannel trunk Po2 (to ALS1) allows VLANs 10, 20, and 100. DLS2 Po10 (to DLS1) allows 10, 20, 50 and 100. Neither trunk allows VLAN 30 (GUEST).
- The **`show running-config interface po2`** and **`show running-config interface po10`** commands on DLS2 confirm that Po2 encapsulation is dot1q and the native VLAN is 900. VLAN 30 (GUEST) is missing from the allowed VLANs on the trunks, which prevents packets from PC-C from traversing the DLS2 to DLS1 or DLS2 to ALS1 trunks.

Action: Add VLAN 30 to EtherChannel trunks Po2 and Po10 (this also changes the physical ports). Refer to TT-C debrief for more information.

Verification: You should now be able to ping from guest PC-C to SRV1.

Step 7: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with your instructor. The notes can include problems encountered, solutions applied, useful commands employed, alternate solutions and methods, and procedure and communication improvements.

Trouble Ticket TT-C Debrief – Instructor Notes

There are two problems with the trunk links between switches ALS1, DLS1, and DLS2. Neither trunk link allows VLAN 30 (the GUEST VLAN). To regain connectivity for the clients, only one of the two issues needs to be resolved. However, to regain the redundancy that is inherent in the physical network design, both issues must be diagnosed and resolved. Proper verification should uncover both issues.

Resolving one of the two problems might restore connectivity, but leaves a hidden issue. Ask the students if they found all issues and make them aware of the possibility of having hidden problems in a redundant network. Discuss which verification techniques could be used to find these types of issues.

TT-C Issue

The problem in this trouble ticket is caused by the omission of VLAN 30 (GUEST) from the list of allowed VLANs on the trunks between switches DLS2 and ALS1 and between switches DLS2 and DLS1.

This issue can be remedied by issuing the following commands on DLS2:

```
DLS2(config)#int po2
DLS2(config-if)#switchport trunk allowed vlan add 30
DLS2(config-if)#int po10
DLS2(config-if)#switchport trunk allowed vlan add 30
```

After adding VLAN 30 to the list of allowed VLANs, the PC-C should be able to get an IP address from router DLS1 via DHCP and ping SRV1.

Section 2—Troubleshooting Reference Information

General Troubleshooting Process

As a general guideline, you can use the following general troubleshooting process described in the course:

1. Define the problem (symptoms).
2. Gather information.
3. Analyze the information.
4. Propose a hypothesis (possible cause).
5. Test the hypothesis.
6. Eliminate or accept the hypothesis.
7. Solve the problem.
8. Document the problem.

Command Summary

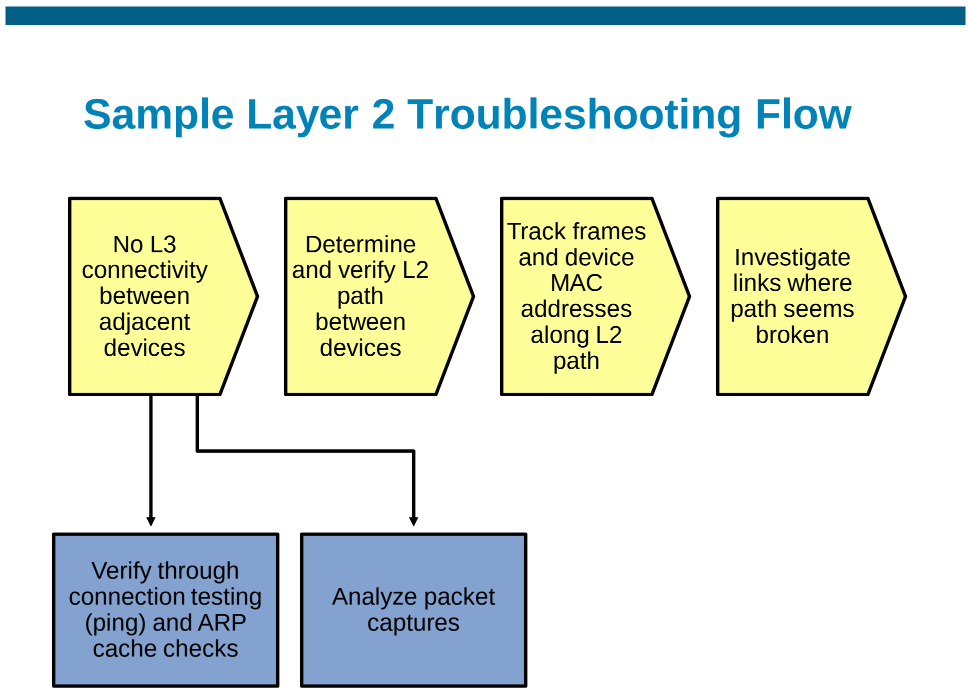
The table lists useful commands for this lab. The sample output is shown on following pages.

Command	Key Information Displayed
clear arp-cache	Clears ARP entries and resets aging.
show arp	Displays the IP address, MAC address, and interface.
show interfaces status	Displays link status, speed, duplex, trunk or VLAN membership, and interface descriptions.
show cdp neighbors (detail)	Displays device ID and type and confirms that a link is operational at the data link layer in both directions, including the sending and receiving ports. The **detail** option gives the remote device IP address.
show spanning-tree vlan *vlan#*	Displays all essential parameters that affect the topology, such as root port, designated ports, port state, and port type, as well as the spanning-tree mode implemented.
show spanning-tree inconsistentports	Displays a more detailed description of the type of port inconsistency and what might be causing it.
show spanning-tree summary	Displays the spanning-tree mode and the VLANs for which this switch is the root bridge. VLANs are listed along with the number of ports in various STP states.
show mac address-table address *mac-addr*	Displays the MAC address and interface entry in the table for the specified host.
show mac-address-table interface *intf-id*	Displays all MAC addresses that were learned on the specified port.
show vlan brief	Displays an 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, if so, which ports are assigned to it. Includes trunk ports on which the VLAN is allowed.
show interfaces *type/#*	Displays interface status, IP address/prefix, load, duplex, speed and packet statistics and errors.
show interfaces trunk	Displays all trunk ports, the operational status, trunk encapsulation, and native VLAN, as well as the list of allowed VLANs, active VLANs, and the VLANs in Spanning Tree Forwarding state for the trunk.
show interfaces *type/#* **switchport**	Checks all VLAN-related parameters for a specific interface (access ports and trunk ports).
show etherchannel summary	Displays port channels, the member ports, and flags indicating status.

Lab 4-1 Sample Troubleshooting Flows

The figure illustrates an example of a method that you could follow to diagnose and resolve Layer 2 problems.



Usually, you start troubleshooting the Layer 2 connectivity between devices because you have discovered that there is no Layer 3 connectivity between two adjacent Layer 2 hosts, such as two hosts in the same VLAN or a host and its default gateway. The following are typical symptoms that could lead you to start examining Layer 2 connectivity:

- Failing pings between adjacent devices. (This can also be caused by a host-based firewall that is blocking pings.)

- Address Resolution Protocol (ARP) failures. After clearing the ARP cache and triggering a connection attempt (for instance, by using ping), ARP entries show up as incomplete or are missing.
- Packets are not being received, which is shown by using a packet sniffer on the receiving host.

Confirm or Deny Layer 3 Connectivity

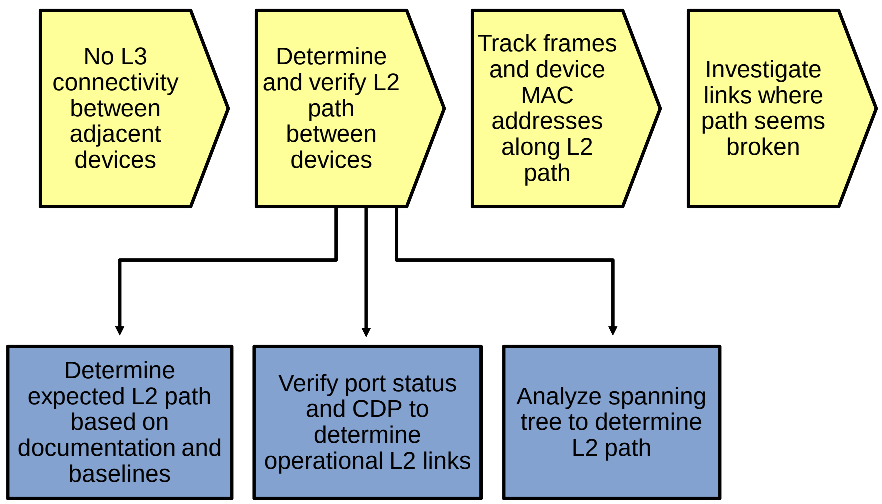
```
DLS1#ping 10.1.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.2.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

DLS1#clear arp-cache


DLS1#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.10.1               0   0007.e963.ce53  ARPA   Vlan10
Internet  10.1.2.1                -   0017.5a5b.b442  ARPA   FastEthernet0/5
Internet  10.1.50.1               0   0007.e963.ce53  ARPA   Vlan50
Internet  10.1.100.1              0   001b.0c6d.8f41  ARPA   Vlan100
Internet  10.1.100.254            -   0000.0c07.ac64  ARPA   Vlan100
Internet  10.1.100.253            0   0017.5a53.a3c1  ARPA   Vlan100
Internet  10.1.100.252            -   0017.5a5b.b441  ARPA   Vlan100
Internet  10.1.50.252             -   0017.5a5b.b446  ARPA   Vlan50
Internet  10.1.50.254             -   0000.0c07.ac32  ARPA   Vlan50
Internet  10.1.20.252             -   0017.5a5b.b444  ARPA   Vlan20
Internet  10.1.30.252             -   0017.5a5b.b445  ARPA   Vlan30
Internet  10.1.10.252             -   0017.5a5b.b443  ARPA   Vlan10
```

The most relevant fields in the output are the IP address, hardware address, and interface fields, because these give you the essential information that you are usually looking for when you issue the **show arp** command.

The age field is also relevant. By default, ARP entries are cached for four hours. To make sure that you are looking at current information, you can use the **clear arp-cache** command to flush existing entries from the cache.

If there is a "-" in the age field instead of a number, this entry is local to the switch. These entries represent locally configured IP and MAC addresses, and the switch will respond to ARP requests for these entries.

Sample Layer 2 Troubleshooting Flow



If you have determined that the problem is most likely a Layer 2 or Layer 1 problem, you want to reduce the scope of the potential failures. You can diagnose Layer 2 problems with the following common troubleshooting method:

- Determine the Layer 2 path. Based on documentation, baselines, and knowledge of your network in general, the first step is to determine the path that you would expect frames to follow between the affected hosts. Determining the expected traffic path beforehand helps you in two ways: It gives you a starting point for gathering information about what is actually happening on the network, and it makes it easier to spot abnormal behavior. The second step in determining the Layer 2 path is to follow the expected path and verify that the links on the expected path are actually up and forwarding traffic. If the actual traffic path is different from your expected path, this step might give you clues about the particular links or protocols that are failing and the cause of these failures.
- Track the flow of traffic across the Layer 2 path. By following the expected Layer 2 path and verifying that frames actually flow along that path, you can likely find the spot where the connectivity is failing.
- When you have found the spot where the connectivity is failing, examine the link or links where the path is broken. Now you can apply targeted troubleshooting commands to find the root cause of the problem. Even if you cannot find the underlying cause of the problem yourself, by reducing the scope of the problem, you have a better-defined problem that can be escalated to the next level of support.

Although there are many different approaches to troubleshooting Layer 2 problems, the elements mentioned above will most likely be part of any methodical approach. These elements are not necessarily executed in the presented order. Determining the expected path and verifying the actual path often go hand-in-hand.

To determine the traffic path between the affected hosts, you can combine knowledge from the following sources:

- **Documentation and baselines:** Documentation that was written during design and implementation usually contains information about the intended traffic paths between the hosts. If the documentation does not provide this information, you can usually reconstruct the expected flow of traffic by analyzing network diagrams and configurations.
- **Link status across the path:** A very straightforward check after you have determined the expected path of the traffic is to verify that all ports and links in the path are operational.

- **Spanning-tree topology:** In Layer 2 networks that have a level of redundancy built into the topology, analyze the operation of Spanning Tree Protocol (STP) to determine which of the available links will be used.

Verify Link Status

```
DLS1#show interfaces status

Port    Name              Status       Vlan     Duplex  Speed Type
Fa0/1   Channel to ALS1   connected    trunk    a-full  a-100 10/100BaseTX
Fa0/2   Channel to ALS1   connected    trunk    a-full  a-100 10/100BaseTX
Fa0/3   Channel to DLS2   connected    trunk    a-full  a-100 10/100BaseTX
Fa0/4   Channel to DLS2   connected    trunk    a-full  a-100 10/100BaseTX
Fa0/5   FE to R1          notconnect   routed     full    100 10/100BaseTX
Fa0/6   FE to SRV1        connected    50       a-full  a-100 10/100BaseTX
Fa0/7   Unused            disabled     999        auto   auto 10/100BaseTX
<output omitted>
Fa0/24  Unused            disabled     999        auto   auto 10/100BaseTX
Gi0/1   Unused            disabled     999        auto   auto Not Present
Gi0/2   Unused            disabled     999        auto   auto Not Present
Po1     Channel to ALS1   connected    trunk    a-full  a-100
Po10    Channel to DLS2   connected    trunk    a-full  a-100
```

To determine link status on switches, the **show interfaces status** command is useful because it gives a brief overview of all the interfaces on the switch as well as contains important elements, such as link status, speed, duplex, trunk or VLAN membership, and interface descriptions. If the link is up, the Status field shows “connected.” If it is down up, “notconnect” is in the Status field. If the link has been administratively shut down, the status is “disabled.”

```
DLS1#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
R1.tshoot.net    Fas 0/5           151          R S I     1841      Fas 0/1
ALS1.tshoot.net  Fas 0/2           153           S I      WS-C2960- Fas 0/2
ALS1.tshoot.net  Fas 0/1           153           S I      WS-C2960- Fas 0/1
DLS2.tshoot.net  Fas 0/4           172          R S I     WS-C3560- Fas 0/4
DLS2.tshoot.net  Fas 0/3           172          R S I     WS-C3560- Fas 0/3
```

If the Cisco Discovery Protocol is enabled between the switches and routers, you can use the **show cdp neighbor** command to confirm that a link is operational at the data link layer in both directions. Also, it is essential in uncovering cabling problems because it records both the sending and receiving ports, as can be seen in the output above.

Analyze Spanning Tree

```
ALS1#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    24586
             Address     0017.5a5b.b400
             Cost        12
             Port        56 (Port-channel1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     001b.0c6d.8f00
```



```
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------

Fa0/18              Desg FWD 19        128.18   P2p Edge
Po1                 Root FWD 12        128.56   P2p
Po2                 Altn BLK 12        128.64   P2p
```

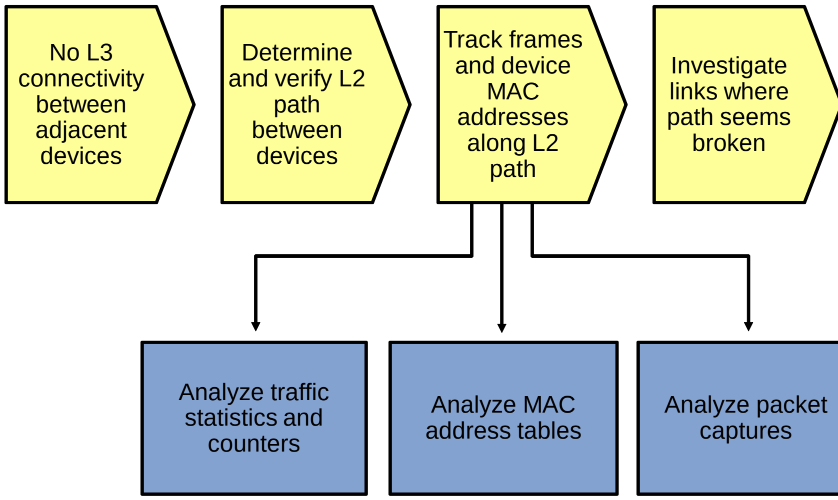
To analyze the spanning-tree topology and the consequences that STP has for the Layer 2 path, the **`show spanning-tree vlan`** *`vlan-id`* command is a good starting point. It lists all essential parameters that affect the topology, such as the root port, designated ports, port state, and port type.

Typical values for the port status field are BLK (blocking) and FWD (forwarding). You might also see LIS or LTN (listening), and LRN (learning) while STP is converging.

The states LBK (loopback), DWN (down), or BKN (broken) typically indicate problems. If the value is BKN, the Type field indicates what is causing the broken status. Possible values are ROOT_Inc, LOOP_Inc, PVID_Inc, TYPE_Inc, or PVST_Inc. To get a more detailed description of the type of inconsistency and what might be causing it, you can examine the output of the **`show spanning-tree inconsistentports`** command. Interface Type and information includes:

- P2p or Shr to indicate the link type (typically based on duplex status – P2p is full-duplex and Shr is half-duplex or shared Ethernet).
- Edge for edge (PortFast) ports.
- Bound for boundary ports when this switch is running 802.1s (MST) and the other switch is running a different spanning-tree variety. The output also indicates which other type of STP was detected on the port.
- Peer for peer ports when this switch is running Per VLAN Spanning Tree Plus (PVST+) or Per VLAN Rapid Spanning Tree Plus (PVRST+) and the other switch is running a different standard variety of STP (802.1D or 802.1s MST).

Sample Layer 2 Troubleshooting Flow



After you have determined the Layer 2 path between the two affected hosts, you can start tracking the traffic between the hosts as it is being switched along the path. The most direct approach to tracking the traffic is to capture packets at set points along the path by using a packet sniffer. Tracking packets in real time is a fairly intensive procedure, and technical limitations might restrict the links where traffic captures could be collected. However, it is the most definitive proof that traffic is or is not flowing along specific paths and links. A less labor-intensive method is to track the flow of traffic by analyzing MAC address tables or traffic statistics. These methods are less direct, because you are not looking at the actual traffic itself but at traces left by the passing of frames.

In a network that has not yet gone into production, packet statistics can help you see where traffic is flowing. On live networks, the test traffic that you are generating will be lost against the background of the live traffic patterns in most cases. However, if the switches that you are using have the capability to track packet statistics for access lists, you might be able to write an access list that matches the specific traffic that you are interested in and isolate the traffic statistics for that type of traffic.

A method of tracing traffic that can be used under all circumstances is analyzing the process of MAC address learning along the Layer 2 path. When a switch receives a frame on a particular port and for a particular VLAN, it records the source MAC address of that frame together with the port and VLAN in the MAC address table. Therefore, if the MAC address of the source host is recorded in a switch but not on the next switch in the path, it indicates a communication problem between these switches for the VLAN concerned, and the link between these switches should be examined.

Analyze MAC Address Tables

```
DLS1#show mac address-table

       Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 <Output omitted>
  50    0000.0c07.ac32    STATIC      CPU
  50    0007.e963.ce53    DYNAMIC     Fa0/6
```

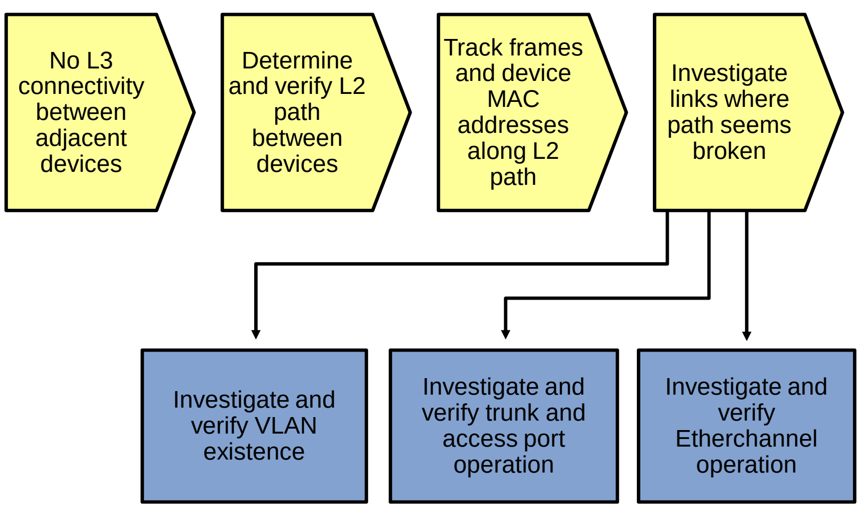
```
  50    0017.5a53.a385    DYNAMIC     Po10
  50    0017.5a53.a3c6    DYNAMIC     Po10
  10    0000.0c07.ac0a    DYNAMIC     Po10
  10    000b.db04.a5cd    DYNAMIC     Po1
  20    0000.0c07.ac14    DYNAMIC     Po10
  20    0017.5a53.a385    DYNAMIC     Po10
  30    0000.0c07.ac1e    DYNAMIC     Po10
 100    0000.0c07.ac64    STATIC      CPU
 100    0017.5a53.a3c1    DYNAMIC     Po10
 100    001b.0c6d.8f41    DYNAMIC     Po1
Total Mac Addresses for this criterion: 32


DLS1#show mac address-table address 0000.0c07.ac0a
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  10    0000.0c07.ac0a    DYNAMIC     Po10
Total Mac Addresses for this criterion: 1
```

You can use the **`show mac-address-table`** command to check the content of the MAC address table. Because this table usually contains hundreds to thousands of entries, you can narrow the results to find what you are looking for by using command options.

If you are looking for the MAC address of a specific host, use the **`show mac-address-table address`** *`mac-address`* option.

Another useful option is **`show mac-address-table interface`** *`intf-id`*, which shows which MAC addresses were learned on a specific port.

Sample Layer 2 Troubleshooting Flow



After you have found the spot in the Layer 2 path where one switch is learning the source MAC address and the next switch is not, examine the link between those two switches carefully.

When trying to determine what could cause the MAC address not to be learned on the next switch, consider the following questions:

- Does the VLAN exist on the next switch?
- Is there an operational trunk between the two switches?
- Is the VLAN allowed on the trunk between the switches?
- If an EtherChannel is between the switches, is the EtherChannel fully operational?

Verify VLAN Existence

```
ALS1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
10   OFFICE                           active    Fa0/18
20   VOICE                            active    Fa0/18
30   GUEST                            active
100  MGMT                             active
900  NATIVE                           active
999  UNUSED                           active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                Gi0/2
1002 fddi-default                             act/unsup
1003 token-ring-default                       act/unsup
1004 fddinet-default                          act/unsup
1005 trnet-default                            act/unsup
```

To get a quick overview of all existing VLANs, use the **show vlan brief** command. However, this command does not list the trunk ports. For instance, in the sample output above, trunk ports F0/1, F0/2, F0/3, and F0/4 are not listed. FastEthernet 0/18 is listed as the only port in VLANs 10 and 20.

```
ALS1#show vlan id 10

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
10   OFFICE                           active    Fa0/18, Po1, Po2

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
10   enet  100010     1500  -      -      -        -    -        0      0
```

To verify the existence of a particular VLAN on a switch, use the **show vlan id** *vlan-id* command. This command shows you whether the VLAN exists and which ports are assigned to it. This command includes trunk ports that the VLAN is allowed on. For the same VLAN 10 that was referenced in the previous output, you now see interface port channel 1 and port channel 2 listed as ports that are associated with VLAN 10.

Verify Trunk Operation

```
ALS1#show interfaces trunk
```

```
Port        Mode             Encapsulation  Status        Native vlan
Po1         on               802.1q         trunking      900
Po2         on               802.1q         trunking      900

Port        Vlans allowed on trunk
Po1         10,20,30,100
Po2         10,20,30,100

Port        Vlans allowed and active in management domain
Po1         10,20,30,100
Po2         10,20,30,100

Port        Vlans in spanning tree forwarding state and not pruned
Po1         10,30,100
Po2         20
```

The easiest way to get an overview of trunk operation is by using the **`show interface trunk`** command. Not only does it list trunk status, trunk encapsulation, and the native VLAN, but it also lists the allowed VLANs, active VLANs, and VLANs in Spanning Tree Forwarding state for the trunk. The last list can be very helpful in determining whether frames for a particular VLAN will be forwarded on a trunk.

For instance, in the example, you can see that both interface port channel 1 and port channel 2 allow VLANs 10, 20, 30, and 100, but VLANs 10, 30, and 100 are forwarded on port channel 1, while VLAN 20 is forwarded on port channel 2.

Verify VLAN Port Status

```
ALS1#show interfaces fastEthernet 0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (OFFICE)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 20 (VOICE)
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none

<Output Omitted>
```

To check all VLAN-related parameters for a specific interface, use the **`show interface`** *`intf-id`* **`switchport`** command. This command applies to access ports as well as trunk ports. For instance, in the example output, the port is configured as a static access port in VLAN 10, and VLAN 20 is assigned to the port as a voice VLAN.

Verify EtherChannel Operation

```
ALS1#show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

1      Po1(SU)          -        Fa0/1(P)    Fa0/2(P)
2      Po2(SU)          -        Fa0/3(P)    Fa0/4(P)
```

When an EtherChannel is configured between the switches and you suspect that EtherChannel operation could be causing the communication failure between the switches, you can verify this by using the **`show etherchannel summary`** command. Although the command output is fairly self-explanatory, the typical things to look for is the lowercase “s” flag, which indicates that a physical interface is suspended because of incompatibility with the other ports in the channel or the uppercase “D” flag, which indicates that an interface (physical or port channel) is down.

Reflection Questions

1. Which lab trouble tickets did you have the most difficulty with?

2. Would you change anything about the process that you used now that you see the resolution of the problem?

3. Which commands did you find most useful in diagnosing Layer 1 and Layer 2 issues? Add these to your toolbox for future use. Which commands did you find least useful?

Lab 4-1: References

If you need more information on the commands and their options, refer to the following references:

- Command References for Cisco Catalyst LAN Switches
Go to http://www.cisco.com/en/US/products/hw/switches/index.html. Then select Campus LAN and the product family that you are working with. The Command References are under the "Reference Guides" section.
- Virtual LANs and VLAN Trunking Protocol Troubleshooting Tech Notes
www.cisco.com/en/US/tech/tk389/tk689/tsd_technology_support_troubleshooting_technotes_list.html
- Spanning Tree Protocol Troubleshooting Tech Notes
www.cisco.com/en/US/tech/tk389/tk621/tsd_technology_support_troubleshooting_technotes_list.html
- EtherChannel Troubleshooting Tech Notes
www.cisco.com/en/US/tech/tk389/tk213/tsd_technology_support_troubleshooting_technotes_list.html

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1700	Fast Ethernet 0 (FA0)	Fast Ethernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
1800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2600	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)
2800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. Rather than try to list all the combinations of configurations for each router class, this table includes identifiers for the possible combinations of Ethernet and serial interfaces in the device. The table does not include any other type of interface, even though a specific router might contain one. An example of this is an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

Device Configurations (Instructor version)

Note: All device configurations are provided for TT-A, including those that are the same as the baseline as defined in Lab 3-1. The configs provided here are *not* running-config outputs. They can be used for cut-and-paste for TT-A and subsequent tickets. Where a config is noted as being the same as a previous one, the only change is in the MOTD, which identifies the Lab and TT. The errors in the configuration are commented and highlighted as red text.

Trouble Ticket - TT-A Configurations

Switch ALS1

```
!Lab 4-1 Switch ALS1 TT-A Config
!
hostname ALS1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 4-1 Switch ALS1 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024

archive
 log config
  logging size 50
  notify syslog contenttype plaintext
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet

spanning-tree mode mst
spanning-tree portfast default
!
interface Vlan1
 no ip address
 shutdown
!
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
```

Error: STP mode is set to mst, but should be rapid-pvst:

`spanning-tree mode rapid-pvst`

Error: Management VLAN 100 is missing:

```
vlan 100
 name MGMT
```

```
 name GUEST
!
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel1
 description Channel to DLS1
 no shutdown
  !
interface Port-channel2
 description Channel to DLS2
 no shutdown
!
interface FastEthernet0/1
 description Channel to DLS1
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shutdown
!
interface FastEthernet0/2
 description Channel to DLS1
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shutdown
!
interface FastEthernet0/3
 description Channel to DLS2
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shutdown
!
interface FastEthernet0/4
 description Channel to DLS2
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shutdown
!
interface FastEthernet0/5
 description Unused
```



```
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown

interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
```

```
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description To PC-B
 switchport access vlan 10
 switchport mode access
 switchport voice vlan 20
 spanning-tree portfast
 switchport port-security
 switchport port-security maximum 2
 switchport port-security violation shutdown
 switchport port-security mac-address sticky
 no shut
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
```

```
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan100
 ip address 10.1.100.1 255.255.255.0
 no shutdown
!
ip default-gateway 10.1.100.254
!
ip http server
ip http secure-server
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
```



```
snmp-server host 10.1.50.1 version 2c cisco
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps vlan-membership
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
  no transport input
!
ntp source Vlan100
ntp server 10.1.202.1
end
```

Switch DLS1

```
!Lab 4-1 Switch DLS1 TT-A Config
!
hostname DLS1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55

banner motd $*** Lab 4-1 Switch DLS1 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
!
ip domain name tshoot.net
!
ip dhcp excluded-address 10.1.10.252 10.1.10.254
ip dhcp excluded-address 10.1.20.252 10.1.20.254
```



```
ip dhcp excluded-address 10.1.30.252 10.1.30.254
!
ip dhcp pool OFFICE
   network 10.1.10.0 255.255.255.0
   default-router 10.1.10.254
   domain-name tshoot.net
!
ip dhcp pool VOICE
   network 10.1.20.0 255.255.255.0
   default-router 10.1.20.254
   domain-name tshoot.net
!
ip dhcp pool GUEST
   network 10.1.30.0 255.255.255.0
   default-router 10.1.30.254
   domain-name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 24576
spanning-tree vlan 20,50 priority 28672
!
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 100
 name MGMT
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
```



```
ip ssh source-interface Vlan100
!
interface Port-channel1
 description Channel to ALS1
 no shut
!
interface Port-channel10
 description Channel to DLS2
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R1
 no switchport
 ip address 10.1.2.1 255.255.255.252
 speed 100
 duplex full
 spanning-tree bpduguard enable
 no shut
```



```
!
interface FastEthernet0/6
 description FE to SRV1
 switchport access vlan 50
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shut
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
```

```
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
```



```
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown

interface Vlan10
 ip address 10.1.10.252 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 priority 110
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.252 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.252 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 priority 110
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.252 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 preempt
```



```
!
interface Vlan100
 ip address 10.1.100.252 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 priority 110
 standby 100 preempt
!
router eigrp 1
 passive-interface default
 no passive-interface Fa0/5
 no auto-summary
 network 10.1.0.0 0.0.255.255
!
ip classless
ip http server
ip http secure-server
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server host 10.1.50.1 version 2c cisco
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 10.1.202.1
end
```

Switch DLS2

```
!Lab 4-1 Switch DLS2 TT-A Config
!
hostname DLS2
!
service timestamps debug datetime msec
service timestamps log datetime
```



```
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 4-1 Switch DLS2 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
  path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 28672
spanning-tree vlan 20,50 priority 24576

vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 100
 name MGMT
```

```
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel2
 description Channel to ALS1
 no shut

interface Port-channel10
 description Channel to DLS1
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
```



```
interface FastEthernet0/5
 description FE to R3
 no switchport
 ip address 10.1.2.13 255.255.255.252
 speed 100
 duplex full
 spanning-tree bpduguard enable
 no shut
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
```



```
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description FE to PC-C
 switchport access vlan 30
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
```



```
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 10.1.10.253 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.253 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 priority 110
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.253 255.255.255.0
```



```
 standby 30 ip 10.1.30.254
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.253 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 priority 110
 standby 50 preempt
!
interface Vlan100
 ip address 10.1.100.253 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 preempt
!
!
router eigrp 1
 passive-interface default
 no passive-interface Fa0/5
 no auto-summary
 network 10.1.0.0 0.0.255.255
!
ip classless
ip http server
ip http secure-server
!
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 10.1.202.1
end
```

Router R1

```
!Lab 4-1 Router R1 TT-A Config
!
hostname R1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 4-1 Router R1 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 10.1.201.1 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown
!
interface FastEthernet0/1
 description FE to DLS1
 ip address 10.1.2.2 255.255.255.252
 ip flow ingress
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
 description WAN link to R2 - 128k leased line
```



```
 ip address 10.1.1.1 255.255.255.252
 ip flow ingress
 encapsulation ppp
 clock rate 128000
  no shutdown
!
interface Serial0/0/1
 description WAN link to R3 (not used)
 no ip address
 shutdown
!
router eigrp 1
 passive-interface default
 no passive-interface FastEthernet0/1
 no passive-interface Serial0/0/0
 network 10.1.1.0 0.0.0.3
 network 10.1.2.0 0.0.0.3
 network 10.1.201.1 0.0.0.0
 no auto-summary
!
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
logging source-interface Loopback0
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 10.1.202.1
end
```

Router R2

```
!Lab 4-1 Router R2 TT-A Config
!
```



```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
Hostname R2
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 4-1 Router R2 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 10.1.202.1 255.255.255.255
!
interface FastEthernet0/0
 shutdown
!
interface FastEthernet0/1
 shutdown
!
interface Serial0/0/0
 description WAN link to R1 - 128k leased line
 ip address 10.1.1.2 255.255.255.252
 encapsulation ppp
 no shutdown

!
interface Serial0/0/1
 description WAN link to R3 - 128k leased line
 ip address 10.1.1.6 255.255.255.252
 clock rate 128000
```



```
 encapsulation ppp
 no shutdown
!
router eigrp 1
 passive-interface default
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
 network 10.1.1.0 0.0.0.3
 network 10.1.1.4 0.0.0.3
 network 10.1.202.1 0.0.0.0
 no auto-summary
!
ip http server
no ip http secure-server
!
logging source-interface Loopback0
logging 10.1.50.1
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
!
ntp master 3
 end
```

Router R3

```
!Lab 4-1 Router R3 TT-A Config
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 4-1 Router R3 TT-A Config ***$
!
aaa new-model
```

```
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
no ip domain lookup
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 10.1.203.1 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown

interface FastEthernet0/1
 description FE to DLS2
 ip address 10.1.2.14 255.255.255.252
 ip flow ingress
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
 description WAN link to R1 - (Not used)
 no ip address
 clock rate 128000
 encapsulation ppp
 shutdown
!
interface Serial0/0/1
 description WAN link to R2 - 128k leased line
 ip address 10.1.1.5 255.255.255.252
 ip flow ingress
 encapsulation ppp
 no shutdown
!
router eigrp 1
 passive-interface default
 no passive-interface FastEthernet0/1
 no passive-interface Serial0/0/1
 network 10.1.1.4 0.0.0.3
 network 10.1.2.12 0.0.0.3
 network 10.1.203.1 0.0.0.0
```



```
 no auto-summary
!
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
logging source-interface Loopback0
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 10.1.202.1
end
```

Trouble Ticket - TT-B Configurations

Router R1 – Same as TT-A

Router R2 – Same as TT-A

Router R3 – Same as TT-A

Switch ALS1

```
!Lab 4-1 Switch ALS1 TT-B Config
!
hostname ALS1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384
```

```
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 4-1 Switch ALS1 TT-B Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet

spanning-tree mode rapid-pvst
spanning-tree portfast default
!
interface Vlan1
 no ip address
 shutdown
!
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 100
 name MGMT
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
```



```
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel1
 description Channel to DLS1
 no shutdown
 !
interface Port-channel2
 description Channel to DLS2
 no shutdown
!
interface FastEthernet0/1
 description Channel to DLS1
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shutdown
!
interface FastEthernet0/2
 description Channel to DLS1
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shutdown
!
interface FastEthernet0/3
 description Channel to DLS2
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shutdown
!
interface FastEthernet0/4
 description Channel to DLS2
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shutdown
!
interface FastEthernet0/5
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
```



```
 switchport nonegotiate
 shutdown

interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
```



```
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description To PC-B
 switchport access vlan 10
 switchport mode access
 switchport voice vlan 20
 spanning-tree portfast
 switchport port-security
 switchport port-security maximum 2
 switchport port-security violation shutdown
 switchport port-security mac-address sticky
 no shut
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
```

```
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan100
 ip address 10.1.100.1 255.255.255.0
 no shutdown
!
ip default-gateway 10.1.100.254
!
ip http server
ip http secure-server
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server host 10.1.50.1 version 2c cisco
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps vlan-membership
!
line con 0
 exec-timeout 60 0
```

```
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
  no transport input
!
ntp source Vlan100
ntp server 10.1.202.1
end
```

Switch DLS1

```
!Lab 4-1 Switch DLS1 TT-B Config
!
hostname DLS1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55

banner motd $*** Lab 4-1 Switch DLS1 TT-B Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip routing
!
ip subnet-zero
ip domain name tshoot.net
!
ip dhcp excluded-address 10.1.10.252 10.1.10.254
ip dhcp excluded-address 10.1.20.252 10.1.20.254
ip dhcp excluded-address 10.1.30.252 10.1.30.254
!
ip dhcp pool OFFICE
   network 10.1.10.0 255.255.255.0
   default-router 10.1.10.254
   domain-name tshoot.net
!
ip dhcp pool VOICE
```



```
   network 10.1.20.0 255.255.255.0
   default-router 10.1.20.254
   domain-name tshoot.net
!
ip dhcp pool GUEST
   network 10.1.30.0 255.255.255.0
   default-router 10.1.30.254
   domain-name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog contenttype plaintext
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 24576
spanning-tree vlan 20,50 priority 28672
!
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 100
 name MGMT
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel1
 description Channel to ALS1
 switchport trunk encapsulation isl
 no shut
!
interface Port-channel10
```

Error: Encapsulation is isl but should be dot1q.

Note: Changing the encapsulation on the port channel will change it on the physical interfaces.

```
interface Port-channel1
  switchport trunk encapsulation dot1q
```



```
 description Channel to DLS2
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation isl
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation isl
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R1
 no switchport
 ip address 10.1.2.1 255.255.255.252
 speed 100
 duplex full
 spanning-tree bpduguard enable
 no shut
!
interface FastEthernet0/6
 description FE to SRV1
 switchport access vlan 50
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
```



```
 no shut
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
```



```
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
```



```
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown

interface Vlan10
 ip address 10.1.10.252 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 priority 110
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.252 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.252 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 priority 110
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.252 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 preempt
!
interface Vlan100
 ip address 10.1.100.252 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 priority 110
 standby 100 preempt
!
```



```
router eigrp 1
 passive-interface default
 no passive-interface F0/5
 no auto-summary
 network 10.1.0.0 0.0.255.255
!
ip classless
ip http server
ip http secure-server
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server host 10.1.50.1 version 2c cisco
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 10.1.202.1
end
```

Switch DLS2

```
!Lab 4-1 Switch DLS2 TT-B Config
!
hostname DLS2
!
service timestamps debug datetime msec
service timestamps log datetime
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
```



```
banner motd $*** Lab 4-1 Switch DLS2 TT-B Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog contenttype plaintext
  hidekeys
  path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 28672
spanning-tree vlan 20,50 priority 24576

vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 100
 name MGMT
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
```



```
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 no shut
!
interface Port-channel10
 description Channel to DLS1
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation isl
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation isl
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R3
 no switchport
 ip address 10.1.2.13 255.255.255.252
 speed 100
 duplex full
```

Error: Encapsulation is set to isl on physical interfaces but port channel 2 is set to dot1q. Change to dot1q:

`switchport trunk encapsulation dot1q`

Error: Encapsulation is isl but should be dot1q:

`switchport trunk encapsulation dot1q`


```
 spanning-tree bpduguard enable
 no shut
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
```

```
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description FE to PC-C
 switchport access vlan 30
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
```



```
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 10.1.10.253 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.253 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 priority 110
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.253 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.253 255.255.255.0
 standby 50 ip 10.1.50.254
```



```
 standby 50 priority 110
 standby 50 preempt
!
interface Vlan100
 ip address 10.1.100.253 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 preempt
!
!
router eigrp 1
 passive-interface default
 no passive-interface F0/5
 no auto-summary
 network 10.1.0.0 0.0.255.255
!
ip classless
ip http server
ip http secure-server
!
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 10.1.202.1
end
```

Trouble Ticket - TT-C Configurations

Switch ALS1 - Same as TT-B

Switch DLS1 - Same as TT-A

Router R1 – Same as TT-A

Router R2 – Same as TT-A

Router R3 – Same as TT-A

Switch DLS2

```
!Lab 4-1 Switch DLS2 TT-C Config
!
hostname DLS2
!
service timestamps debug datetime msec
service timestamps log datetime
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 4-1 Switch DLS2 TT-C Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500

vtp domain TSHOOT
vtp mode transparent

ip subnet-zero
ip routing
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog contenttype plaintext
  hidekeys
  path tftp://10.1.50.1/$h-archive-config
 write-memory
```



```
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 28672
spanning-tree vlan 20,50 priority 24576

vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 100
 name MGMT
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel2
 description Channel to ALS1
 no shut
!
interface Port-channel10
 description Channel to DLS1
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
```

Error: VLAN 30 not allowed on trunks Po2 and Po10.

Note: Adding it to the port channel will add it to the physical interfaces.

```
interface Port-channel2
  switchport trunk allowed vlan add 30

interface Port-channel10
  switchport trunk allowed vlan add 30
```



```
!
interface FastEthernet0/3
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R3
 no switchport
 ip address 10.1.2.13 255.255.255.252
 speed 100
 duplex full
 spanning-tree bpduguard enable
 no shut
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
```



```
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description FE to PC-C
```

```
 switchport access vlan 30
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/2
 description Unused
 switchport access vlan 999
```



```
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 10.1.10.253 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.253 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 priority 110
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.253 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.253 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 priority 110
 standby 50 preempt
!
interface Vlan100
 ip address 10.1.100.253 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 preempt
!
!
router eigrp 1
 passive-interface default
 no passive-interface F0/5
 no auto-summary
 network 10.1.0.0 0.0.255.255
!
ip classless
ip http server
ip http secure-server
!
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
```

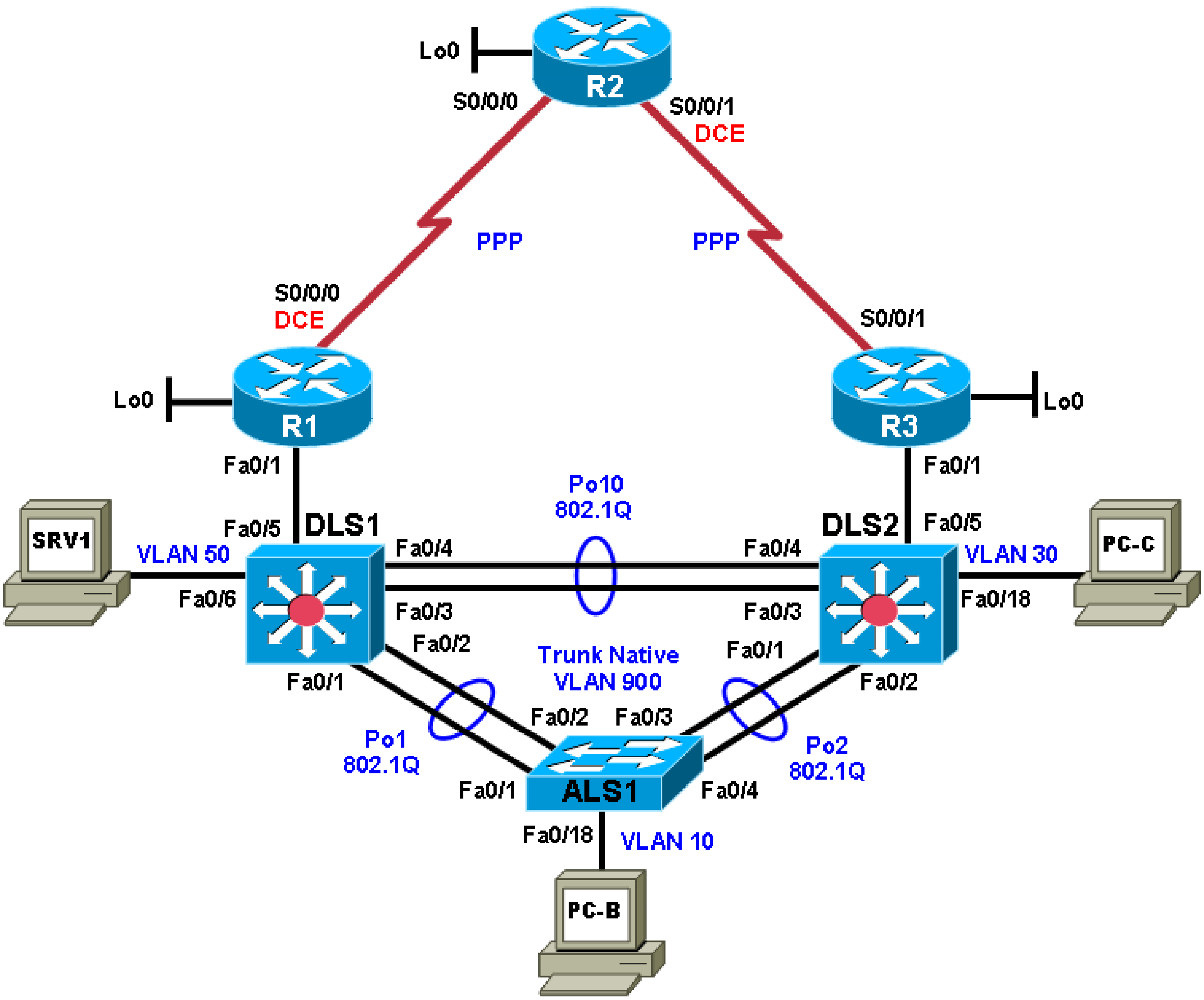


```
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 10.1.202.1
end
```

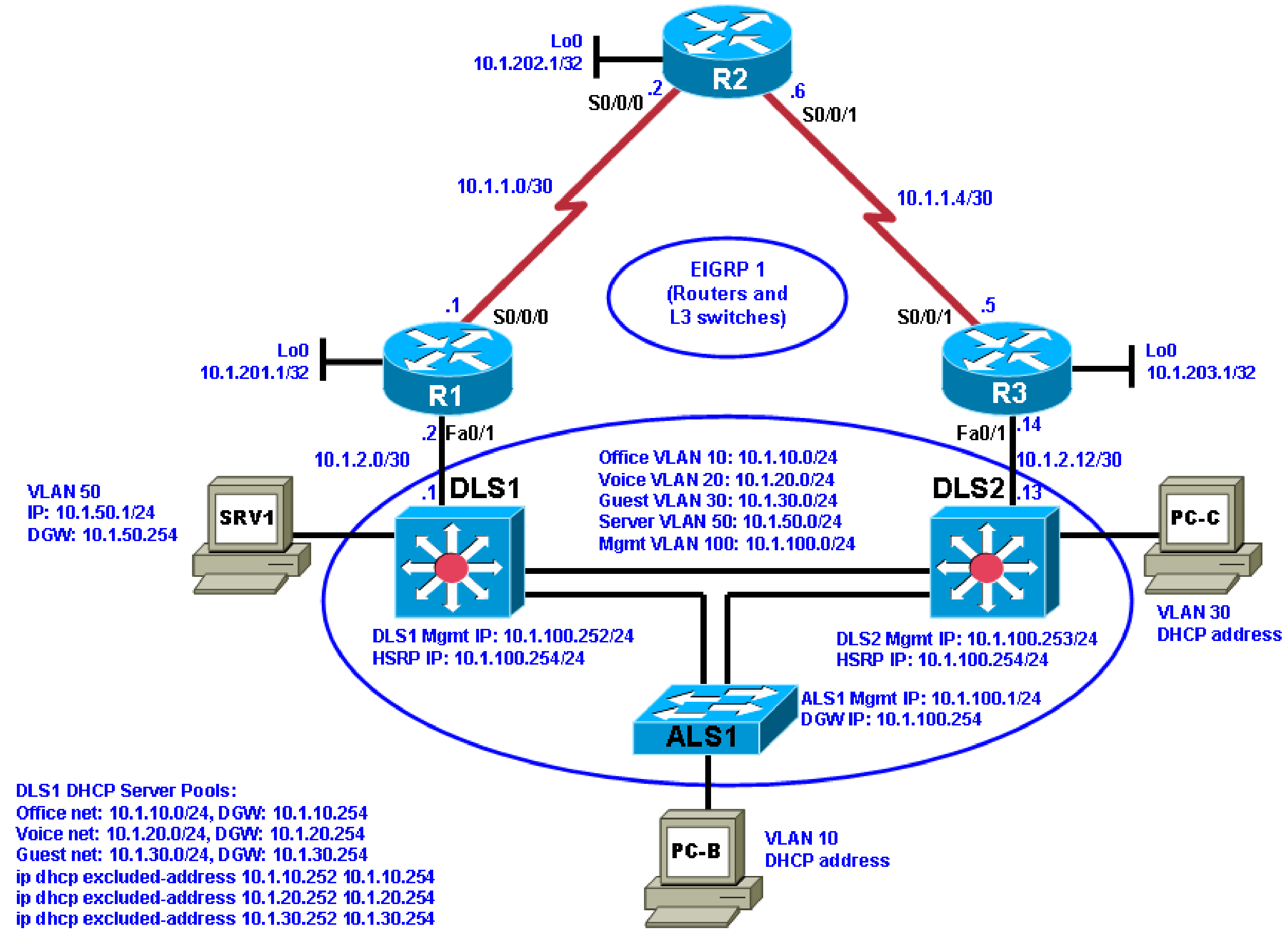
Chapter 4 Lab 4-2, Layer 3 Switching and First-Hop Redundancy

Instructor Version

Physical Topology



Logical Topology



Objectives

- Load the trouble ticket device configuration files for each trouble ticket.
- Diagnose and resolve problems related to switch virtual interfaces and multilayer switching.
- Diagnose and resolve problems related to First Hop Redundancy Protocols.
- Document troubleshooting progress, configuration changes, and problem resolution.

Background

Multilayer (Layer 3) switches have the capability to act as switches and routers when using switch virtual interfaces (SVIs), routed interfaces, and routing protocols. Layer 3 switches allow you to create SVIs or logical interfaces that represent a VLAN. They can also support routed physical interfaces. These versatile switches are frequently used as part of the LAN switch fabric and can be configured with a First Hop Redundancy Protocol (FHRP). Two or more Layer 3 switches (or routers) can provide redundant paths to the network edge for local hosts. A host is configured with a virtual default gateway address. If one of the gateways goes down, the other can take over for the client without the client's knowledge. Examples of FHRPs discussed in this course are Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), and Gateway Load Balancing Protocol (GLBP).

In this lab, you will troubleshoot problems related to Layer 3 switching and FHRPs, such as HSRP, including HSRP authentication. For each task or trouble ticket, the scenario and problem symptom is described. While troubleshooting, you will discover the cause of the problem, correct it, and then document the process and results.

Physical and Logical Topology Diagrams

The physical and logical topologies, including interface designations and IP addresses, are provided to assist the troubleshooting effort.

Lab Structure

This lab is divided into two main sections.

Section 1—Trouble Tickets and Troubleshooting Logs

This section includes multiple tasks. Each task is associated with a trouble ticket (TT) and introduces one or more errors on one or more devices. If time is a consideration, each task or trouble ticket can be performed independently.

Section 2—Troubleshooting Reference Information

This section provides general Layer 2 troubleshooting information that can be applied to any trouble ticket in this lab. Sample troubleshooting flows are provided, along with examples of useful commands and output. If time permits, it is recommended that you read through Section 2 prior to starting on the trouble tickets.

Instructor note: Because the troubleshooting reference section is lengthy, it is advisable to have students read through it prior to starting the lab to become familiar with the troubleshooting flows and commands used. Consider assigning it as homework.

This lab uses Cisco 1841 routers with Cisco IOS Release 12.4(24)T1 and the Advanced IP Services image c1841-advipservicesk9-mz.124-24.T1.bin. The switches are Cisco WS-C2960-24TT-L with the Cisco IOS image c2960-lanbasek9-mz.122-46.SE.bin and Catalyst 3560-24PS with the Cisco IOS image c3560-advipservicesk9-mz.122-46.SE.bin. Other routers (such as 2801 and 2811), switches (such as 2950 or 3550), and Cisco IOS Software versions can be used if they have comparable capabilities and features. Depending on the router or switch model and Cisco IOS Software version, the commands available and output produced might vary from what is shown in this lab.

Note: Any changes made to the baseline configurations or topology (other than errors introduced) are noted in the trouble ticket so that you are aware of them prior to beginning the troubleshooting process.

Instructor Notes:

- The lab topology should be pre-built prior to the students starting the lab. Ensure that all routers and switches (R1, R2, R3, ALS1, DLS1, and DLS2) have the course lab configuration files installed in flash. You can download the files from the Academy Connection website.
- The device configurations that contain trouble ticket errors and modifications from the baseline are included at the end of the lab, and the errors in them are identified.
- Each device has a directory named “tshoot” in flash. This directory contains the baseline configuration file for that device as well as the configuration files for the labs in this course. Refer to Lab 3-1 for instructions on creating the tshoot directory in flash.
- Instructors can use a TFTP server, USB drive, flash memory card, or other method to copy all the course configuration files into the flash:/tshoot directory for each device in the topology.
- The student is responsible for loading the baseline or trouble ticket configurations for all labs as required using the procedure described in Lab 3-1.
- Set the correct time on router R2, which serves as the primary NTP server for the lab network.
- If time is an issue, each task (trouble ticket) can be performed independently.

Required Resources

- 3 routers (Cisco 1841 with Cisco IOS Release 12.4(24)T1 Advanced IP Service or comparable)
- 1 switch (Cisco 2960 with the Cisco IOS Release 12.2(46)SE C2960-LANBASEK9-M image or comparable)

- 2 switches (Cisco 3560 with the Cisco IOS Release 12.2(46)SE C3560-advipservicesK9-mz image or comparable)
- 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 available
- PC-C (Windows PC—DHCP client) with PuTTY and WireShark software available
- Serial and Ethernet cables

Instructor Notes

- This lab is divided into multiple tasks. Each task is associated with a trouble ticket (TT) and introduces one or more errors on one or more devices.
- Students can work individually or as a team. The problems introduced focus on Layer 3 switching and the FHRP environment.
- Suggested actions and results presented during the troubleshooting process for each TT can be shared with the students during debrief or copies of the instructor version of the lab can be made available to the students to assist them in verifying their work.

Section 1—Trouble Tickets and Troubleshooting Logs

Task 1: Trouble Ticket Lab 4-2 TT-A

Instructor note: This trouble ticket involves ALS1 issues related to SVI status and addressing.

Step 1: Review trouble ticket Lab 4-2 TT-A.

Upon arriving at the office this morning, you find the following ticket in the system:

Switch ALS1 has been showing CRC errors on a group of eight ports for several days. It was suspected that hardware was the cause. During yesterday evening's maintenance window, the switch was replaced with a similar switch from the lab. After this replacement, clients could connect, and no errors were shown on the ports. However, making a backup of the ALS1 configuration to server SRV1 did not work, and no syslog messages from ALS1 are being received by SRV1. The switch is not reachable via Telnet or SSH from server SRV1. There was no time for further research yesterday so, because there is no impact to users, it was decided to leave the switch and pick up this issue the next day.

Your task is to diagnose the issue and restore connectivity between switch ALS1 and server SRV1. After resolving the problem, make a backup of the configuration to server SRV1.

Step 2: Load the device trouble ticket configuration files for TT-A.

Using the procedure described in Lab 3-1, verify that the lab configuration files are present in flash. Load the proper configuration files indicated in the Device Configuration File table.

Note: The following device access methods are in effect after loading the configuration files:

- Console access requires no username or password.
- Telnet and SSH require the username **admin** and password **adminpa55**.
- The **enable** password is **ciscoenpa55**.

Instructor note: Although it is not considered security best practice, the student can set the console and VTY line exec-timeout to 0 0 to facilitate performance of this lab.

Device Configuration File Table

Device Name	File to Load	Notes
ALS1	Lab42-ALS1-TT-A-Cfg.txt	This file contains configuration errors
DLS1	Lab42-DLS1-TT-A-Cfg.txt	This file is the same as the baseline
DLS2	Lab42-DLS2-TT-A-Cfg.txt	This file is the same as the baseline
R1	Lab42-R1-TT-A-Cfg.txt	This file is the same as the baseline
R2	Lab42-R2-TT-A-Cfg.txt	This file is the same as the baseline
R3	Lab42-R3-TT-A-Cfg.txt	This file is the same as the baseline
SRV1	N/A	Static IP: 10.1.50.1 Default gateway: 10.1.50.254
PC-B	N/A	DHCP (release and renew after loading device configurations)
PC-C	N/A	DHCP (release and renew after loading device configurations)

Instructor note: The student loads the "broken" TT configuration files for all devices, although only the configurations indicated in the **Notes** column have errors.

Step 3: Configure SRV1 and start the syslog and TFTP servers.

a. Ensure that SRV1 has the static IP address 10.1.50.1 and default gateway 10.1.50.254.

b. Start the syslog server on SRV1, which is the syslog server for the entire network. When the network is properly configured, all devices send syslog messages to SRV1.

c. Start the TFTP server on SRV1, which is the archive server for the entire network. When the network is properly configured, all devices send archives of their running configurations to this server whenever the running config is copied to the startup config. Ensure that the default TFTP directory on SRV1 is set to the directory where you want to store the archives.

Instructor note: This lab uses tftpd32 for both TFTP and syslog. Other comparable tools can be used.

Step 4: Release and renew the DHCP leases on PC-B and PC-C.

a. Ensure that PC-B and PC-C are configured as DHCP clients.

b. After loading all TT-A device configuration files, issue the **ipconfig /release** and **ipconfig /renew** commands on PC-B and PC-C. You might need to repeat this process after the TT problems have been resolved.

Note: Problems introduced into the network by the trouble ticket might prevent one or both of the PCs from acquiring an IP address. Do not assign either PC a static address.

Step 5: Outline the troubleshooting approach and validation steps.

Use this space to identify the troubleshooting approach that you plan to take and the key steps involved to verify that the problem is resolved. Troubleshooting approaches to select from include the follow-the-path, spot-the-differences, bottom-up, top-down, divide-and-conquer, shoot-from-the-hip, and move-the-problem methods.

Note: In addition to a specific approach, you can use the generic troubleshooting process described at the beginning of Section 2 of this lab.

____

____

____

____

____

____

The divide-and-conquer or shoot-from-the-hip method can be used. Other methods are the bottom-up, top-down, spot-the-differences, and move-the-problem approaches.

Verification steps can include:

Switch ALS1 can be reached by means of Telnet from server SRV1.

Syslog messages from ALS1 are being received on SRV1.

The ALS1 configuration can be copied to the TFTP server running on server SRV1.

Step 6: Record the troubleshooting process and configuration changes.

Note: Section 2 of this lab includes sample troubleshooting flows, useful commands, and examples of output.

Use this log to document your actions and results during the troubleshooting process. List the commands you used to gather information. As you progress, record your thoughts as to what you think the problem might be and which actions you take to correct the problem.

Device	Actions and Results

Responses will vary but could include:

- Pings from PC-B to SRV1 at 10.1.50.1 succeed.
- Pings from PC-B to its default gateway 10.1.10.254 on DLS1 succeed.
- Pings from PC-B to all other network devices succeed.
- Pings from ALS1 to DLS1 (10.1.100.252) and DLS2 (10.1.100.253) fail.
- Using Telnet from SRV1 to ALS1 (10.1.100.1) fails.
- Using Telnet from SRV1 to DLS1 (10.1.100.252) succeeds.

TT-A Issue - ALS1 management VLAN 100 SVI has been configured with an IP address that is not on the 10.1.0.0/16 network.

- The **`show spanning-tree`** command on ALS1, DLS1, and DLS2 indicates the correct spanning-tree mode of RSTP and a separate instance for each VLAN.

- The **`show vlan brief`** command on ALS1 indicates that the management VLAN 100 is defined and active.
- The **`show vlan id 100`** command on ALS1 indicates that the management VLAN 100 is defined and active and contains ports Po1 and Po2.
- The **`show ip interface brief`** command on ALS1 indicates that the VLAN 100 SVI status is up, and the protocol is up.
- The **`show ip interface vlan 100`** command on ALS1 indicates that the VLAN 100 SVI IP address is configured as 10.10.100.1/24, which is not part of the 10.1.0.0/16 network.
- Network documentation shows that the switch ALS1 VLAN 100 management IP address should be 10.1.100.1.

Action: Change the IP address for ALS1 VLAN 100 to the correct one shown in the network documentation. Refer to TT-A debrief for more information.

Verification: Using Telnet from SRV1 to ALS1 should now be successful. The logging source interface on ALS1 was set to SVI VLAN 100, so syslog messages can now be sent to SRV1.

Step 7: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with your instructor. The notes can include problems encountered, solutions applied, useful commands employed, alternate solutions, methods and processes, and procedure and communication improvements.

____

____

____

____

____

____

____

Trouble Ticket TT-A Debrief—Instructor Notes

TT-A Issue

The problem in this trouble ticket is because SVI VLAN 100 on ALS1 has been assigned an IP address (10.10.100.1/24) that is not part of the 10.1.0.0/16 network and cannot communicate with other devices using their management VLAN addresses. In addition, SRV1 is unable to use Telnet or ping to the switch at its presumed VLAN 100 management address of 10.1.100.1. A review of network documentation shows that the switch ALS1 VLAN 100 management IP address should on the 10.1.100.0/24 network. Even if the VLAN 100 IP address was on the 10.1.0.0/16 network, the network administrator would still be pinging the wrong address based on network documentation.

Because users can access all network resources via ping through switch ALS1, it is not likely to be a Layer 2 issue. However, SRV1 cannot ping or use Telnet to the switch at its management IP address. The switch cannot communicate with SRV1 for syslog and TFTP nor can it ping to any other network device at its management address. But SRV1 can ping the management IP address of all other network devices. This tends to point to a management VLAN issue with ALS1.

To solve the problem, issue the following command:

```
ALS1(config)#interface vlan 100
ALS1(config-if)#ip address 10.1.100.1 255.255.255.0
```


Task 2: Trouble Ticket Lab 4-2 TT-B

Instructor note: This trouble ticket involves DLS1 issues related to DHCP assigning an incorrect HSRP default gateway address and a mismatch of HSRP parameters between DLS1 and DLS2.

Step 1: Review trouble ticket Lab 4-2 TT-B.

During last Friday's maintenance window, a series of failover tests at headquarters and the branch offices were executed. It was discovered during a reboot of switch DLS1 that connectivity between clients in OFFICE VLAN 10 and the Internet was lost. After router DLS1 came back online, the clients regained connectivity. This was not the expected behavior, because the network provides gateway first-hop redundancy for clients in the OFFICE VLAN to ensure correct failover during outages.

If one of the HSRP switches fails, the hosts on the OFFICE VLAN should still be able to access the Internet (by pinging R2 Lo0 10.1.202.1 during the outage).

Step 2: Load the device trouble ticket configuration files for TT-B.

Using the procedure described in Lab 3-1, verify that the lab configuration files are present in flash. Load the proper configuration files indicated in the Device Configuration File table.

Note: See Task 1, Step 2 for device access methods, usernames, and passwords after the configuration files have been loaded.

Note: You can test the simulated Internet access by opening a browser and entering the IP address of the R2 Lo0 interface 10.1.202.1. You will be prompted for a username and password. You can gain access to the router GUI management interface by entering username **admin** and the enable password **ciscoenpa55**.

Device Configuration File Table

Device Name	File to Load	Notes
ALS1	Lab42-ALS1-TT-B-Cfg.txt	This file is the same as the baseline
DLS1	Lab42-DLS1-TT-B-Cfg.txt	This file contains configuration errors
DLS2	Lab42-DLS2-TT-B-Cfg.txt	This file contains configuration errors
R1	Lab42-R1-TT-B-Cfg.txt	This file is the same as the baseline
R2	Lab42-R2-TT-B-Cfg.txt	This file is the same as the baseline
R3	Lab42-R3-TT-B-Cfg.txt	This file is the same as the baseline
SRV1	N/A	Static IP: 10.1.50.1 Default gateway: 10.1.50.254
PC-B	N/A	DHCP (release and renew after loading device configurations)
PC-C	N/A	DHCP (release and renew after loading device configurations)

Step 3: Configure SRV1 and start the syslog and TFTP servers, as described in Task 1.

Step 4: Release and renew the DHCP leases on PC-B and PC-C, as described in Task 1.

Step 5: Outline the troubleshooting approach and validation steps.

Use this space to identify the troubleshooting approach that you plan to take and the key steps involved to verify that the problem is resolved. Troubleshooting approaches to select from include the follow-the-path, spot-the-differences, bottom-up, top-down, divide-and-conquer, shoot-from-the-hip, and move-the-problem methods.

Note: In addition to a specific approach, you can use the generic troubleshooting process described at the beginning of Section 2 of this lab.

The spot-the-differences or shoot-from-the-hip method can be used. Other methods are the bottom-up, top-down, divide-and-conquer, follow-the-path, and move-the-problem approaches.

Verification steps can include:

From PC-B (connected to switch ALS1) ping and browse the Internet using R2 Lo0 10.1.202.2 while DLS1 is being rebooted.

Step 6: Record the troubleshooting process and configuration changes.

Note: Section 2 of this lab includes sample troubleshooting flows, useful commands, and examples of output.

Use this log to document your actions and results during the troubleshooting process. List the commands you used to gather information. As you progress, record your thoughts as to what you think the problem might be and which actions you take to correct the problem.

Device	Actions and Results

TT-B Issue 1 - An incorrect HSRP default gateway address for VLAN 10 is assigned by DHCP server DLS1.

Answers will vary but could include:

Before rebooting the DLS1 primary HSRP router (device up and functioning):

- Pings from PC-B to the R2 simulated ISP Lo0 10.1.202.1 succeed.
- Tracert from PC-B to the R2 simulated ISP Lo0 10.1.202.1 succeeds and follows the path DLS1 (10.1.10.252) to R1 (10.1.2.2) to R2 (10.1.202.1).

When rebooting the DLS1 primary HSRP router (simulating a device failure):

Instructor note: You can also shut down the Po1 and Po10 port channel interfaces on DLS1 to simulate device failure.

- Pings from PC-B to the real IP address of the redundant router DLS2 10.1.10.253 succeed.
- Pings from PC-B to the virtual IP address 10.1.10.254 succeed.
- Pings from PC-B to the R2 simulated ISP Lo0 10.1.202.1 fail.
- Tracert from PC-B to the R2 simulated ISP Lo0 10.1.202.1 fails at first hop DLS1.
- There might be an issue with the routing protocol, but the **`show ip protocols`** command on DLS1 and DLS2 indicates that they are using EIGRP and routing for network 10.1.0.0/16.
- Also, the **`show ip route`** command on DLS1 and DLS2 indicates that a route exists to the R2 simulated ISP address 10.1.202.1 (learned via EIGRP).
- The **`show ip cef 10.1.202.1`** command on DLS1 indicates that the next hop is 10.1.2.2 via Fa 0/5.
- The **`show standby vlan 10`** command on DLS1 indicates that the virtual IP address for VLAN 10 is 10.1.10.254 and that DLS1 is the local active router. The standby router is DLS2, and its SVI VLAN 10 real IP address is 10.1.10.253.
- The **`show running-config interface vlan 10`** command on DLS1 indicates that the SVI VLAN 10 real IP address is 10.1.10.252 and that the virtual address is 10.1.10.254. Both are correct according to the network documentation.
- The **`ipconfig`** command on PC-B indicates that it is a DHCP client and that it is using the real IP address (10.1.10.252) of the primary VLAN 10 router DLS1 as its default gateway rather than the virtual VLAN IP address (10.1.10.254). This is okay as long as DLS1 is up, but it does not provide redundancy for VLAN 10 clients.
- A check of the network documentation indicates that DLS1 is the DHCP server for the network.
- The **`show running-config | beg dhcp`** command on DLS1 indicates that the IP DHCP pool OFFICE specifies a default router of 10.1.10.252, which is the real IP address of DLS1 SVI VLAN 10. It should specify the HSRP virtual IP address of 10.1.10.254.

Action: Change the default router for the OFFICE DHCP pool on DLS1 to 10.1.10.254. Refer to TT-B debrief for more information. On PC-B, issue the **`ipconfig /release`** and **`ipconfig /renew`** commands.

Verification: When DLS1 is reloaded (simulating an outage), packets are now routed through DLS2. Also, DLS2 now changes from standby to active and allows hosts on VLAN 10 to access the Internet via the backup.

TT-B Issue 2 - HSRP VLAN 100 parameters mismatch between DLS1 and DLS2.

VLAN 10 clients can now access the Internet, but you still cannot ping from switch ALS1 to DLS2 when DLS1 is reloaded to test the failover capability.

Answers will vary but could include:

When rebooting the DLS1 primary HSRP router (simulating a device failure):

- Pings from ALS1 to the real VLAN 100 IP address of the redundant router DLS2 10.1.100.253 succeed.
- Pings from ALS1 to the virtual VLAN 100 IP address 10.1.100.254 fail.
- When the primary router is down, if pings to the real IP address of the standby router are successful but pings to the virtual IP address fail, there might be a problem with the FHRP.
- When pinging from switch ALS1 to DLS2, they communicate using management VLAN 100.
- The **`show standby vlan 100`** command on DLS1 indicates that the group is 100 and that the state is active. The group name is hsrp-Vl100-100. The virtual IP address for VLAN 100 is 10.1.100.254, and DLS1 is the local active router. The standby router is unknown, indicating a problem with the HSRP configuration.
- The **`debug standby packets`** command on DLS1 indicates that the DLS1 is sending HSRP "hello out" messages from 10.1.100.252 for VLAN 100 Group 100, but no HSRP "hello in" messages are being received from DLS2 (10.1.100.253). The reverse is true for DLS2. The routers are not exchanging HSRP hello messages.
- The **`show running-config interface vlan 100`** command on DLS1 confirms that the SVI VLAN 100 real IP address is 10.1.10.252, and the virtual IP address is 10.1.100.254. The group number is 100.
- The **`show standby vlan 100`** command on DLS2 indicates that the group is 10 and that the state is active. The group name is hsrp-Vl100-10. The virtual IP address for VLAN 100 is 10.1.10.245, and DLS2 is the local active router. The standby router is unknown, indicating a problem with the HSRP configuration.
- The **`show running-config interface vlan 100`** command on DLS2 confirms that the SVI VLAN 100 real IP address is 10.1.10.253, and the virtual IP address is 10.1.100.245, which does not match the DLS1 configuration and is incorrect according to the network documentation. The standby group number is 10, which is also incorrect. It should be 100.
- A check of the network documentation indicates that the correct HSRP virtual IP address for VLAN 100 is 10.1.100.254.

Action: Change VLAN 100 on DLS1 to 10.1.100.254 and specify the standby group number 100, instead of 10. Refer to TT-B debrief for more information.

Verification: Now when DLS1 is reloaded (simulating an outage), ALS1 packets can still reach DLS2 using VLAN 100.

Step 7: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with your instructor. The notes can include problems encountered, solutions applied, and useful commands employed. It can also include alternate solutions, methods, and procedures and communication improvements.

Trouble Ticket TT-B Debrief—Instructor Notes

TT-B Issue 1

Connectivity between clients in VLAN 10 OFFICE and the Internet is lost when switch DLS1 is rebooted.

The problem with clients in VLAN 10 is caused by using the real IP address of Layer 3 switch DLS1 as the default gateway rather than the HSRP virtual IP address. The default gateway for clients is assigned via DHCP by DLS1.

The **`ipconfig`** command on PC-B indicated that it is a DHCP client, and it was using the real IP address (10.1.10.252) of the primary VLAN 10 router DLS1 as its default gateway rather than the virtual VLAN IP address (10.1.10.254). This provides connectivity as long as DLS1 is up, but it does not provide redundancy for VLAN 10 clients.

When DLS1 was up, the traceroute from PC-B to the R2 simulated ISP Lo0 10.1.202.1 succeeded and followed the path DLS1 (10.1.10.252) to R1 (10.1.2.2) to R2 (10.1.202.1). A trace to a location reports the real IP address of the hops on the path, not the virtual ones. Thus, the trace would have looked normal even though there might be problems with HSRP. However, when DLS1 goes down, the real IP address that PC-B was using as its default gateway is no longer available, and the traceroute fails at the first hop (DLS1).

To resolve this problem, the default gateway address that is assigned by DLS1 to VLAN 10 clients should be changed as follows:

```
ip dhcp pool OFFICE
   default-router 10.1.10.254
```

After this, the IP address on client PC-B should be released and renewed to force the client to update its default gateway.

TT-B Issue 2

Connectivity between ALS1 and DLS2 is lost when switch DLS1 is rebooted.

The second problem is caused by mismatched HSRP parameters between Layer 3 switches DLS1 and DLS2 for VLAN 100 MGMT. The HSRP group number and virtual IP address on DLS2 should be changed to match DLS1 as follows:

```
no interface vlan 100

interface vlan 100

 ip address 10.1.100.253 255.255.255.0

 standby 100 ip 10.1.100.254

 standby 100 preempt
```

Note: Additional HSRP group number information to share with students:

A problem in the HSRP configuration can be created when one router is configured using commands "standby x ip …", where “x” is the group number, while another router in the same network is configured using only "standby ip …", omitting the standby group number. Omitting the group number causes the router to create standby group 0. This will lead to two standby groups being created on a common network, both claiming the same virtual IP and MAC address. This problem is common and difficult to spot.

Task 3: Trouble Ticket Lab 4-2 TT-C

Instructor note: This trouble ticket involves DLS1 and DLS2 issues related to HSRP authentication.

Step 1: Review trouble ticket Lab 4-2 TT-C.

Your company has decided to use Message Digest 5 (MD5)-based authentication between the HSRP routers. A colleague of yours was asked to test the authentication using VLAN 100 MGMT (to avoid impact on end users) between DLS1 and DLS2. He started to configure the test late this afternoon but then left on vacation. Your task is to review and verify the implementation of HSRP authentication in VLAN 100 and fix any issues that remain.

Step 2: Load the device trouble ticket configuration files for TT-C.

Using the procedure described in Lab 3-1, verify that the lab configuration files are present in flash. Load the configuration files indicated in the Device Configuration File table.

Note: See Task 1, Step 2 for device access methods, usernames, and passwords after you have loaded the configuration files.

Device Configuration File Table

Device Name	File to Load	Notes
ALS1	Lab42-ALS1-TT-C-Cfg.txt	This file is the same as the baseline
DLS1	Lab42-DLS1-TT-C-Cfg.txt	This file contains configuration errors
DLS2	Lab42-DLS2-TT-C-Cfg.txt	This file contains configuration errors
R1	Lab42-R1-TT-C-Cfg.txt	This file is the same as the baseline
R2	Lab42-R2-TT-C-Cfg.txt	This file is the same as the baseline
R3	Lab42-R3-TT-C-Cfg.txt	This file is the same as the baseline
SRV1	N/A	Static IP: 10.1.50.1 Default gateway: 10.1.50.254
PC-B	N/A	DHCP
PC-C	N/A	DHCP

Step 3: Configure SRV1 and start the syslog and TFTP servers, as described in Task 1.

Step 4: Release and renew the DHCP leases on PC-B and PC-C, as described in Task 1.

Step 5: Outline the troubleshooting approach and validation steps.

Use this space to identify the troubleshooting approach you plan to take and the key steps to verify that the problem is resolved. Troubleshooting approaches to select from include the follow-the-path, spot-the-differences, bottom-up, top-down, divide-and-conquer, shoot-from-the-hip, and move-the-problem methods.

Note: In addition to a specific approach, you can use the generic troubleshooting process described at the beginning of Section 2 of this lab.

The spot-the-differences method or top-down method can be used. Other methods include the bottom-up, divide-and-conquer, shoot-from-the-hip, move-the-problem, and follow-the-path approaches.

Verification steps can include:

Syslog and console messages regarding HSRP authentication problems cease.

Using the **`show standby brief`** command on DLS1 and DLS2 reveals that they are now part of the same group and show correct active and standby roles.

Step 6: Record the troubleshooting process and configuration changes.

Note: Section 2 of this lab includes sample troubleshooting flows, useful commands, and examples of output.

Use this log to document your actions and results during the troubleshooting process. List the commands you used to gather information. As you progress, record your thoughts as to what you think the problem might be and which actions you take to correct the problem.

Note: You might need to issue the **ipconfig /release** and **ipconfig /renew** commands on DHCP clients after the network device problems are resolved.

Device	Actions and Results

Answers will vary but could include:

Syslog and console messages on DLS1 and DLS2 indicate that there is bad HSRP authentication between the two devices.

- The **show standby vlan 100** command on DLS1 indicates that the group is 100 and the state is active. The group name is hsrp-Vl100-100. The virtual IP address for VLAN 100 is 10.1.100.254, and DLS1 is the local active router. This is correct according to the network documentation. The standby router is unknown, indicating a problem with the HSRP configuration.
- The **show standby vlan 100** command on DLS2 indicates that the group is 100 and the state is active. The group name is hsrp-Vl100-100. The virtual IP address for VLAN 100 is 10.1.100.254, and DLS2 is the local active router. DLS2 has a lower HSRP priority than DLS1 and should be the standby for VLAN 100, not the active router. This is *not* correct according to network documentation. The standby router is unknown, indicating a problem with the HSRP configuration.
- The **show standby brief** command on DLS1 and DLS2 indicates that the standby roles and status for each device is correct for all other VLANs, but each router thinks it is the active router for VLAN 100 because it cannot communicate with the other router.
- The **debug standby packets** command on DLS1 indicates that DLS1 is sending HSRP "hello out" messages (from 10.1.100.252) for VLAN 100 Group 100 but hello messages from DLS2 are reported on DLS1 as "Grp 100 Auth failed for Hello pkt from 10.1.10.253."
- The **show running-config | beg standby** command on both DLS1 and DLS2 confirms that the SVI VLAN 100 is using MD5 authentication with a keychain of TEST. VLAN 100 on both devices appears to be configured correctly.
- The **show running-config | beg key** command on both DLS1 and DLS2 confirms that keychain TEST is configured with **key 1** with a key string that is password encrypted. It is not known what the key strings are, but they are most likely not the same and this is the problem.
- A check of the network documentation indicates that the key string was not documented.

Action: Change the keychain TEST on DLS2 to match DLS1 (**C1sc0** - uppercase C, numeral 1, lowercase s, lowercase c, zero). Refer to TT-C debrief for more information.

Validation: Syslog error messages should cease, and the two HSRP devices should be able to authenticate.

Step 7: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with your instructor. The notes can include the problems encountered, solutions applied, and useful commands employed. It could also include alternate solutions, methods, and procedures and communication improvements.

____

____

____

____

____

____

____

Trouble Ticket TT-C Debrief—Instructor Notes

TT-C Issue

The authentication failure between switches DLS1 and DLS2 is caused by a mismatch between the key strings that are configured on each switch. On switch DLS1, the key string uses a number 1 for the "i" in the string "C1sc0" while switch DLS2 uses a lowercase "l" for the "i" in the string "Clsc0." Changing the key on switch DLS1 to match switch DLS2, or vice versa, can solve this problem.

Note: The password encryption service prevents determining what the key string is when using the **show running-config** command. However, you can use the **show key chain** command to view the plain text key string.

```
DLS2(config)#service password-encryption

DLS2(config)#key chain TEST
DLS2(config-keychain)#key 1
DLS2(config-keychain-key)#key-string C1sc0
DLS2(config-keychain-key)#

DLS2#show run | include key

key chain TEST
 key 1
   key-string 7 106D580A0647
```

The **show key chain** command will display the plain text key string.

```
DLS2#show key chain
Key-chain TEST:
    key 1 -- text "C1sc0"
        accept lifetime (always valid) - (always valid) [valid now]
        send lifetime (always valid) - (always valid) [valid now]
```

To change the MD5 key string, use the following command on DLS2:

```
key chain TEST
 key 1
   key-string C1sc0
```

Note: Additional HSRP authentication information to share with students:

Using authentication for HSRP routers does not actually increase their security significantly. Authentication mismatch will cause the standby group to be partitioned with each router having a distinct MD5 password claiming to be the active router itself, leading to duplicate virtual IP and virtual MAC addresses. Also, the authentication cannot prevent anyone from assigning the virtual IP to himself, creating yet another address conflict. The authentication within first hop redundancy protocols is only of limited value. It has been deprecated and dropped from the current VRRP RFC though it is still supported in Cisco implementation. See RFC 3768, section 10.

Section 2—Troubleshooting Reference Information

General Troubleshooting Process

As a general guideline, you can use the following general troubleshooting process described in the course:

1. Define the problem (symptoms).
2. Gather information.
3. Analyze the information.
4. Propose a hypothesis (possible cause).
5. Test the hypothesis.
6. Eliminate or accept the hypothesis.
7. Solve the problem.
8. Document the problem.

Commands Summary

The table lists useful commands. The sample output is shown on the following pages.

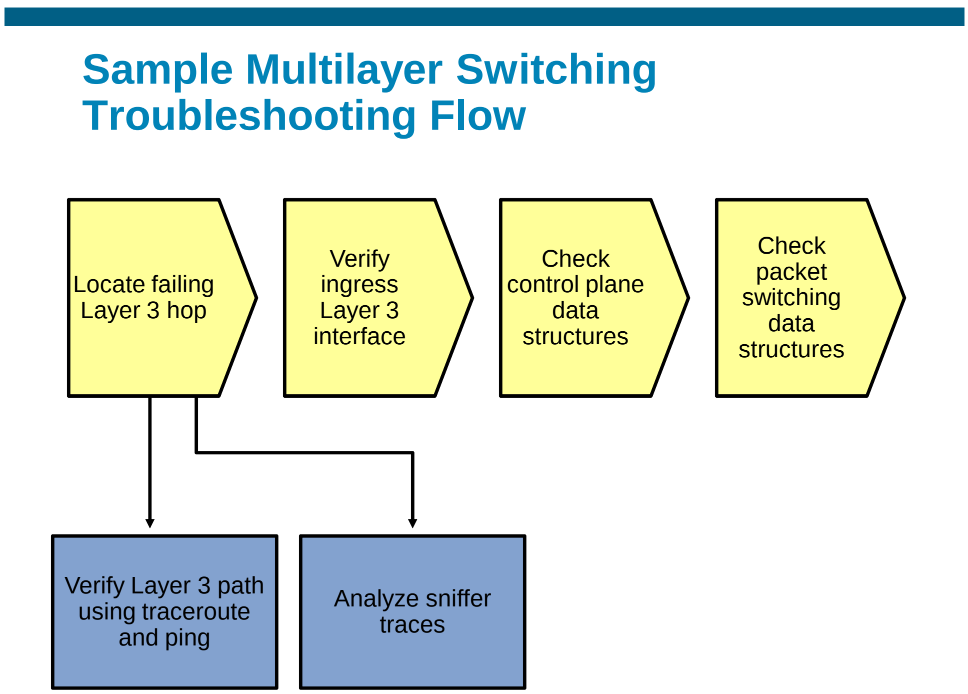
Command	Key Information Displayed
show spanning-tree vlan *vlan#*	Displays all essential parameters that affect the topology, such as the root port, designated ports, port state, and port type, as well as the spanning-tree mode being implemented.
show vlan brief	Displays a quick overview of all existing 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 interfaces vlan *vlan#*	Displays the SVI status, IP address, and statistics.
show ip route *ip-addr*	Displays the routing table information for a particular destination address.
show ip arp *ip-addr*	Displays the ARP table information for an IP address, including age, hardware address, and interface.
show interfaces *type/#* **| include bia**	Displays the MAC address of an interface on one output line.
show ip cef *ip-addr* **detail**	Displays the next hop and interface used for a particular destination address from the Cisco Express Forwarding table.
show adjacency *int-type/#* **detail**	Displays the information contained in the adjacency table for a next-hop IP address or interface.
show platform forward	Displays the hardware ternary content addressable memory (TCAM) information and exact forwarding behavior for a Layer 2 or Layer 3 switched frame.

	Note: Specific to the Catalyst 3560 and 3750 series of switches.
`show standby vlan` *`vlan#`* **`brief`**	Verify active and standby roles and IP addresses for a particular VLAN for HSRP routers.
`debug standby packets`	Displays real-time messages exchanged between HSRP routers.

Lab 4-2 Sample Troubleshooting Flows

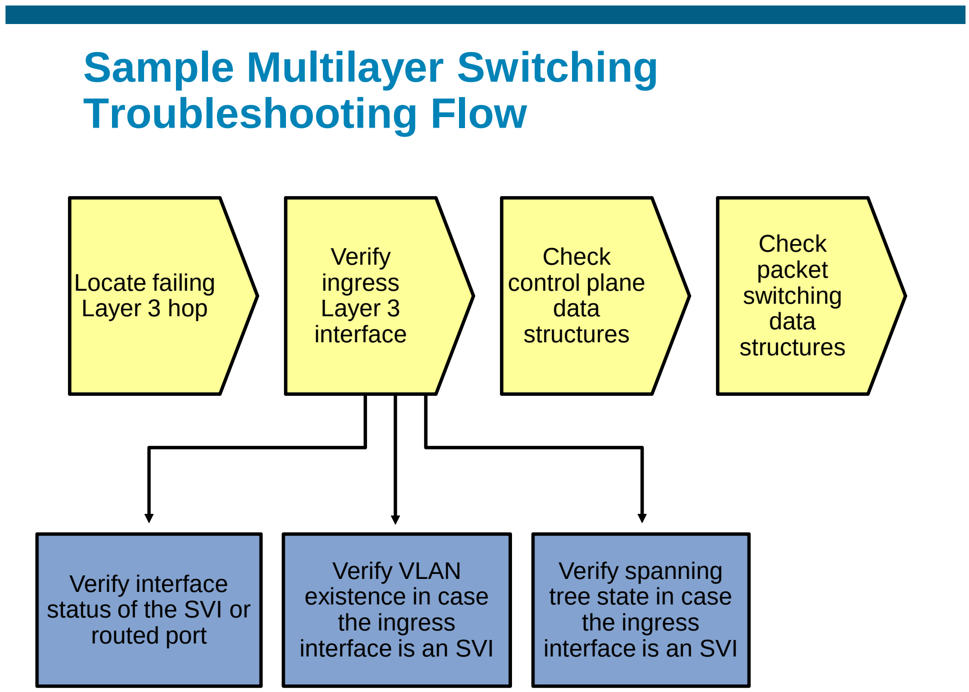
Troubleshooting Multilayer Switching

The figure illustrates an example of a method that you could follow to diagnose and resolve problems related to multilayer switching.



What is multilayer switching? In essence, a multilayer switch is a switch that is capable of switching Ethernet frames based on information in the Layer 2 and Layer 3 headers. Troubleshooting Layer 2 switching was covered in the previous lab exercise. This troubleshooting flow focuses on troubleshooting the process of switching Ethernet frames based on Layer 3 information.

Under which kind of circumstances do you start troubleshooting the multilayer switching process? Troubleshooting multilayer switching is just one of the steps in the bigger picture of troubleshooting network connectivity along a Layer 3 path. After you have determined—by using tools like traceroute or ping or through analysis of packet captures—that a particular hop in the Layer 3 path seems to be the point where packets start to get dropped and that hop is a multilayer switch, or when you are troubleshooting performance problems and you want to find the exact physical links on which packets travel, then start tracing and verifying the Layer 3 forwarding behavior of the multilayer switch that you suspect to be the cause of the problem.



Layer 3 packet switching generally consists of three major steps:

1. Receive the packet on a Layer 3 interface. This interface can either be a routed port or an SVI.
2. Perform a lookup in the hardware packet-switching data structures. Multilayer switches store packet-forwarding information in special TCAM data structures. The information contained in these data structures is compiled from the Cisco Express Forwarding data structures in the main memory of the route processor. These data structures are, in turn, derived from control plane tables, such as the routing table and the ARP cache.
3. Rewrite the frame and switch it to the outbound interface based on the information found in the TCAM.

Consequently, a straightforward approach to troubleshooting a Layer3 switching problem is to verify the components that are involved in this process. First, verify the ingress Layer 3 interface, then the control plane data structures and, subsequently, the packet-forwarding data structures. (Alternatively, you can perform these steps in the reverse order.)

If the ingress interface is a routed port, the first step in this process is simple because the Layer 3 and Layer 2 ports are identical. Verifying the physical interface status and the configured IP address and subnet mask for that interface is sufficient to determine the status of the Layer 3 ingress interface. However, if the ingress interface is an SVI, its status is not directly related to any particular physical interface.

Verify SVI Status (Missing VLAN)

```
DLS1#show vlan id 100
VLAN id 100 not found in current VLAN database


DLS1#show interfaces vlan 100
Vlan100 is down, line protocol is down
  Hardware is EtherSVI, address is 0017.5a5b.b441 (bia 0017.5a5b.b441)
  Internet address is 10.1.100.252/24

<Output Omitted>
```


A VLAN interface or SVI is up if there is at least one interface in the spanning-tree forwarding state for that VLAN. This implies that if an SVI is down, you should verify VLAN existence, VLAN port assignments, and the spanning-tree state for the SVI.

In the output above, you can see that a missing VLAN results in a VLAN interface that is in state “down, line protocol is down.”

Verify SVI Status (VLAN with No Port Assigned)

```
DLS1#show vlan id 100

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
100  MGMT                             active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
100  enet  100100     1500  -      -      -        -    -        0      0


DLS1#show interfaces vlan 100
Vlan100 is up, line protocol is down
  Hardware is EtherSVI, address is 0017.5a5b.b441 (bia 0017.5a5b.b441)
  Internet address is 10.1.100.252/24

<Output Omitted>
```

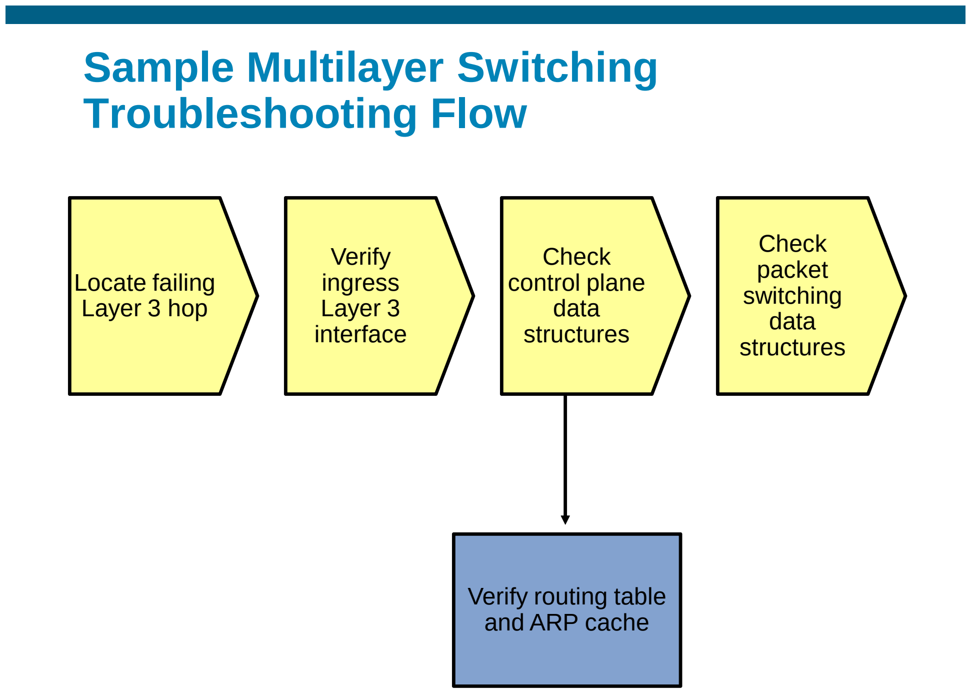
When the VLAN exists but no ports are assigned to that VLAN, the status of the SVI changes to “up, line protocol is down.”

Verify SVI Status (VLAN with No Port in Spanning-Tree Forwarding State)

```
DLS1#show spanning-tree vlan 100

<Output Omitted>

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------

Po1                 Desg LRN 12        128.56   P2p
Po10                Desg LRN 12        128.128  P2p

DLS1#show interfaces vlan 100
Vlan100 is up, line protocol is down
  Hardware is EtherSVI, address is 0017.5a5b.b441 (bia 0017.5a5b.b441)
  Internet address is 10.1.100.252/24

<Output Omitted>
```

Finally, if ports are assigned to the VLAN and at least one of these physical ports (trunk or access port) is up, one more condition needs to be met: The spanning-tree state for at least one of the ports needs to be forwarding. Under normal circumstances, if there is at least one interface assigned to a VLAN, an interface is in spanning-tree forwarding state. Either the switch is the root for the VLAN and all the ports assigned to the VLAN are designated ports and therefore forwarding, or the switch is not the root and it has a root port that is in forwarding state.

As a result, when you are troubleshooting a multilayer switching problem and you find that the ingress interface is an SVI and it is down, there is an underlying Layer 2 problem for that VLAN and you need to initiate a Layer 2 troubleshooting process.



Verify the Routing Table and ARP Cache

The next step in this process is to verify that the control plane information that is necessary to forward the packets is present. The two control plane data structures that are relevant to multilayer switching are the routing table and the ARP cache.

In this sample troubleshooting flow, the multilayer switching data structures for an Internet Control Message Protocol (ICMP) echo request traveling from source IP address 10.1.50.1 to destination IP address 10.1.202.1 is verified by using various **show** commands.

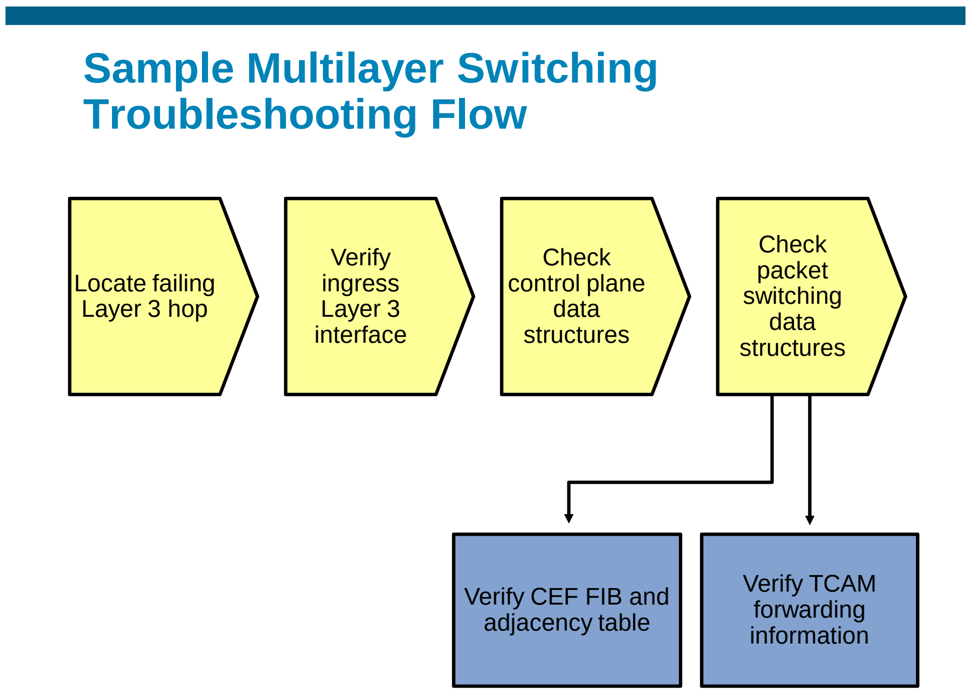
```
DLS1#show ip route 10.1.202.1
Routing entry for 10.1.202.1/32
  Known via "eigrp 1", distance 90, metric 2300416, type internal
  Redistributing via eigrp 1
  Last update from 10.1.2.2 on FastEthernet0/5, 02:41:16 ago
  Routing Descriptor Blocks:
  * 10.1.2.2, from 10.1.2.2, 02:41:16 ago, via FastEthernet0/5
      Route metric is 2300416, traffic share count is 1
      Total delay is 25100 microseconds, minimum bandwidth is 1544 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 2

DLS1#show ip arp 10.1.2.2
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.2.2              162   001b.530d.60b1  ARPA   FastEthernet0/5
DLS1#show interfaces FastEthernet 0/5 | include bia
  Hardware is Fast Ethernet, address is 0017.5a5b.b442 (bia 0017.5a5b.b442)
```

In the output, you can see that a route is found in the routing table for the destination IP address 10.1.202.1, and the next hop and outbound interface for packets with that destination are listed.

If the routing table does not contain an entry (specific prefix or default route) for the destination, the problem is not a packet-switching problem but a routing problem, and you should initiate a process to troubleshoot the routing operation on the control plane.

The ARP cache provides the destination MAC address for the next hop. If an ARP entry for the destination is missing or listed as incomplete, either the next hop listed in the route is not valid, or there is a Layer 2 problem between the multilayer switch and the next hop. In both cases, the problem is not really a multilayer switching problem, and you should investigate the routing operation on the control plane and the Layer 2 connectivity to the next hop first.

The final element that the router needs to rewrite a frame and switch it out is the source MAC address of the frame, which corresponds to the MAC address of the outbound Layer 3 interface.



When the control plane data structures have been verified, the next step in the multilayer switching troubleshooting process is to verify the data structures in software and hardware that are used to forward packets.

All recent Layer 3 switches use the Cisco Express Forwarding technology as the foundation for the multilayer switching process. The switches combine the information from the control plane data structure, such as the routing table and the ARP cache, into two different data structures: the Forwarding Information Base (FIB) and the adjacency table. These two data structures are stored in the main memory of the route processor. They are only used to forward packets that are not handled in hardware.

However, based on the information in the FIB and adjacency table, the hardware TCAM is populated, and the resulting TCAM information is what is eventually used to forward frames in hardware.

To verify the correct operation of the multilayer switching process, first verify that the control plane information is accurately reflected in the software FIB and adjacency table. Next, verify that the information from the FIB and adjacency table is correctly compiled into the TCAM.

Verify the FIB and Adjacency Table

```
DLS2#show ip cef 10.1.202.1
10.1.202.1/32
  nexthop 10.1.2.14 FastEthernet0/5

DLS2#show adjacency fastEthernet 0/5 detail
Protocol Interface                 Address
IP       FastEthernet0/5           10.1.2.14(19)
                                   0 packets, 0 bytes
```



```
epoch 0
sourced in sev-epoch 0
Encap length 14
001B530D6029 00175A53A3C2 0800
L2 destination address byte offset 0
L2 destination address byte length 6
Link-type after encap: ip
ARP
```

The **show ip cef** command can be used in a similar way as the **show ip route** command. When you specify a destination IP address as an option to the command, it lists the entry in the Cisco Express Forwarding FIB that matches that IP address. It also shows the next-hop IP address and egress interface, which serve as a pointer to the adjacency table.

The **show adjacency** command can be used to display the information contained in the adjacency table. The next-hop IP address or interface can be specified to select specific adjacencies. Adding the **detail** keyword to the command shows the frame rewrite information for packets that are switched through that adjacency. The frame rewrite information lists the complete Ethernet header. For the example in the output, this consists of the destination MAC address 001B.530D.6029 (which is the same MAC address that was listed as the MAC address of next hop 10.1.2.14 in the ARP cache), followed by the source MAC address 0017.5A53.A3C2 (which equals the MAC address of the egress interface F0/5), and finally, the Ethertype 0x0800 (which indicates that the protocol contained in the Ethernet frame is IP version 4).

The information displayed in these **show** commands should accurately reflect the information in the routing table and ARP cache.

Verify the Hardware TCAM Information

```
DLS2#show platform forward fa0/3 vlan 50 0017.5a5b.b405 0017.5a53.a385 ip 10.1.50.1
10.1.202.1 icmp 8 0
Ingress:
Global Port Number: 129, lpn: 4 Asic Number: 0
Source Vlan Id: Real 50, Mapped 5. L2EncapType 0, L3EncapType 0

<Output Omitted>

Egress: Asic 0, switch 1
        CPU queues: 7 14.
Source Vlan Id: Real 50, Mapped 5. L2EncapType 0, L3EncapType 0
portMap 0x1000, non-SPAN portMap 0x1000

<Output Omitted>

Port        Vlan      SrcMac           DstMac     Cos  Dscpv
Fa0/5       1006 0017.5a53.a385  0017.5a53.a3c2
```

Note: The **show platform forward** command shown in the above output is specific to the Catalyst 3560 and 3750 series of switches. Consult the documentation for the platform that you are working with to find similar commands to examine the content of the hardware forwarding data structures for the platform.

The **show platform forward** command consults the hardware TCAM information and displays the exact forwarding behavior for a Layer 2 or Layer 3 switched frame.

This command displays the exact forwarding behavior for a packet, taking into account all features that affect packet forwarding, including Cisco Express Forwarding load balancing, EtherChannel load balancing, and packet filtering using access control lists. Therefore, you must specify the exact content of all the relevant fields in the header of the packet.

In the example command output above, the following fields are specified:

- **Ingress interface:** In the example interface, FastEthernet 0/3 is specified as the ingress interface for the packet.
- **Ingress VLAN:** It is not necessary to specify this parameter if the port is an access port. For trunk ports, you must specify the VLAN that the frame is tagged with when it enters the ingress interface. VLAN 50 is specified as the ingress VLAN.
- **Source MAC address:** The source MAC address of the frame when it enters the switch needs to be specified. In the example, the address is 0017.5A5B.B405. This is the MAC address of the egress interface of the previous hop (DLS1 Fa0/3 MAC).
- **Destination MAC address:** The destination MAC address of the frame when it enters the switch needs to be specified. In the example, the address is 0017.5A53.A385 (DLS2 Fa0/3 MAC). For a Layer 3 switched packet, this address is the MAC address of the ingress Layer 3 interface (routed port or SVI).
- **Protocol:** This is not necessary for Layer 2 switched frames. For Layer 3 switching, the Layer 3 protocol that is used and the major fields in that protocol's header must be specified. In the example, IP is listed as the protocol.
- **Source IP address:** When IP is specified as the Layer 3 protocol, the source IP address of the packet must be specified. In the example, it is 10.1.50.1.
- **Destination IP address:** When IP is specified as the Layer 3 protocol, the destination IP address of the packet must be specified. In the example, it is 10.1.202.1.
- **IP protocol:** When IP is specified as the Layer 3 protocol, the protocol in the IP header, for example, TCP, UDP, or ICMP, must be specified. In the example, ICMP is specified because the example represents an ICMP echo request packet.
- **ICMP type and code:** When ICMP is specified as the protocol, the ICMP type and code values must be specified. When TCP or UDP is specified as the protocol, additional header fields that are appropriate for those protocols, such as source and destination port numbers, must be specified. In the example, ICMP type 8 and code 0 are specified to represent an echo request packet.

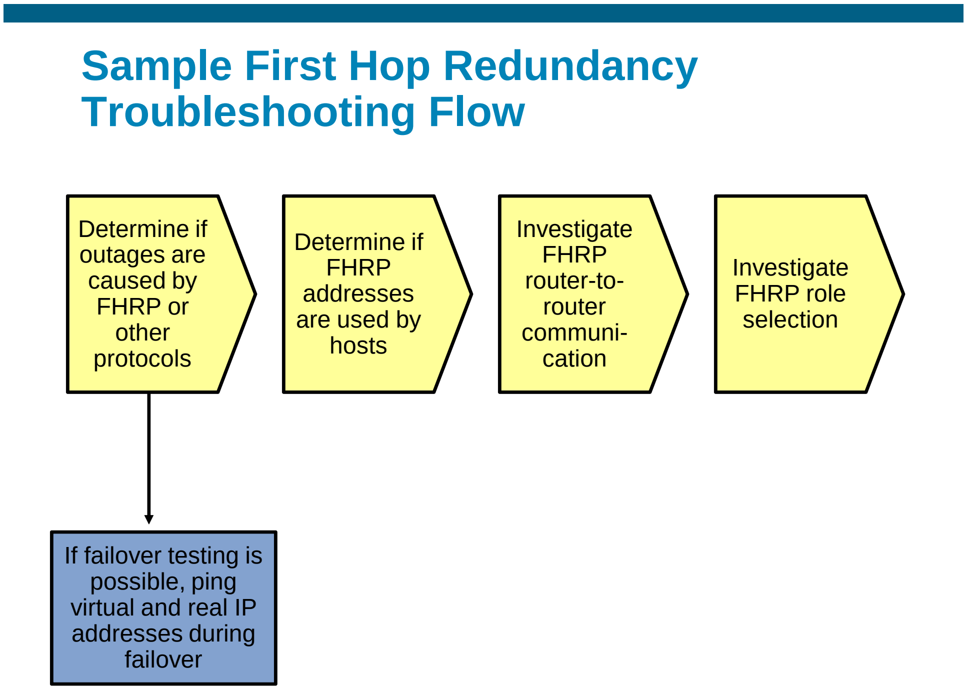
This command is very powerful because it shows you exactly how frames will be forwarded based on all features that affect forwarding behavior, such as load balancing, EtherChannel, and access control lists. Also, if a frame is dropped instead of forwarded, the command lists the reason why the frame is dropped.

What should you do if somewhere in this chain of verifying the control plane, you find an inconsistency between the software and hardware packet-forwarding data structures?

The process of building the FIB and adjacency table from the routing table and ARP cache, and subsequently populating the TCAM based on the FIB and adjacency table, is internal to the Cisco IOS software and not configurable. Whenever you find an instance where the information in these data structures is not consistent, open a case with the Cisco Technical Assistance Center (provided that you have a valid support contract for your device) to investigate and resolve the issue. As a workaround, you can try to clear the control plane data structures, such as the routing table and the ARP cache, for the particular entries that you are troubleshooting. This triggers both the control plane and the packet-forwarding data structures to be repopulated for those entries and, in certain cases, this might resolve the inconsistencies. However, this is only a workaround, not a real solution, because it only addresses the symptoms of the problem and not the underlying cause.

Troubleshooting First Hop Redundancy Protocols

The figure illustrates an example of a method that you could follow to diagnose and resolve problems related to FHRPs, such as HSRP, VRRP, and GLBP.



The most common reason to start troubleshooting FHRP behavior is because during an outage or a test, network connectivity is lost for longer than expected when a redundant device or link is temporarily disabled. In redundantly configured IP networks, a number of different protocols usually need to reconverge to recover from a failure. The FHRP that is used is just one of the protocols that could be the cause of the loss of connectivity. Other protocols that need to converge as well—and could be the cause of the problem—are routing protocols and Spanning Tree Protocol (STP).

So how do you determine if the FHRP is the problem?

If you have the opportunity to execute failover tests (for instance, during a scheduled maintenance window), a good way to determine if the problem is caused by the FHRP or by another protocol is by sending multiple continuous pings from a client that is using the virtual router as its default gateway. Ping to the virtual and real IP addresses of the routers that participate in the FHRP, and ping to an IP address of a host that is one or more router hops removed from the client. Observe and compare the behavior of the pings while you force a failover by disabling a device or a link.

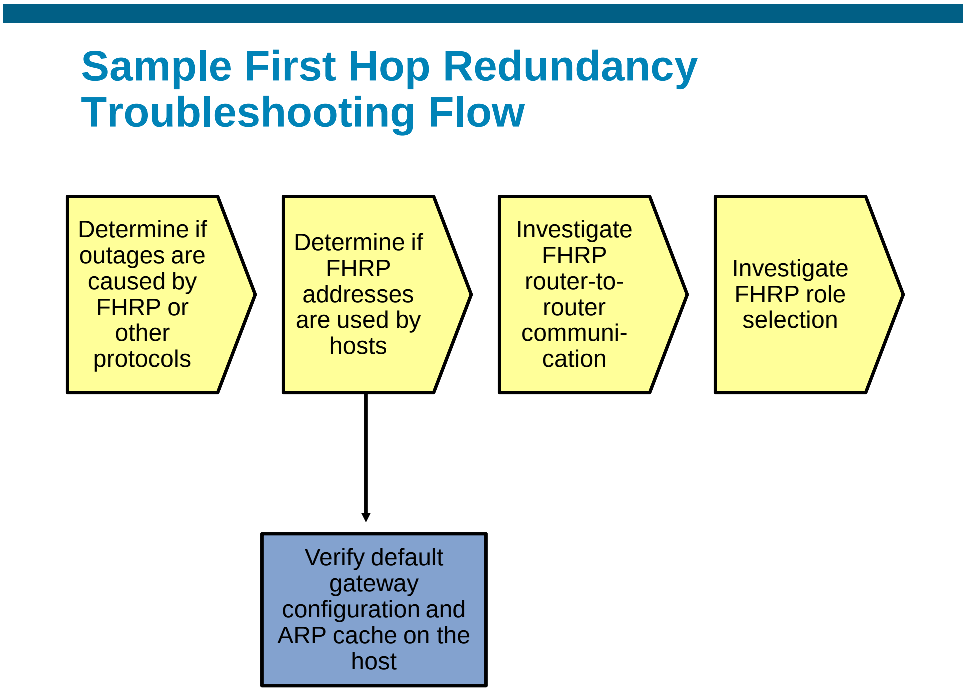
Based on the observed differences between the ping responses, you can draw conclusions about the likelihood that the problem is related to the FHRP or to any other protocols that are involved in the convergence. Here are a few examples:

- If you observe that the pings to the real IP address of the redundant router and the virtual IP address of the FHRP both fail at the same time and resume at the same time when you disable the primary router, assume that the problem is not related to the FHRP (because the FHRP does not affect the pings to the real IP address). The most likely cause in this scenario is the Layer 2 convergence for the VLAN, so you should start a Layer 2 troubleshooting procedure.
- If you observe that the pings to the real IP address of the redundant router do not suffer any packet loss, but pings to the virtual IP address fail, this strongly suggests that there is a problem with the FHRP.

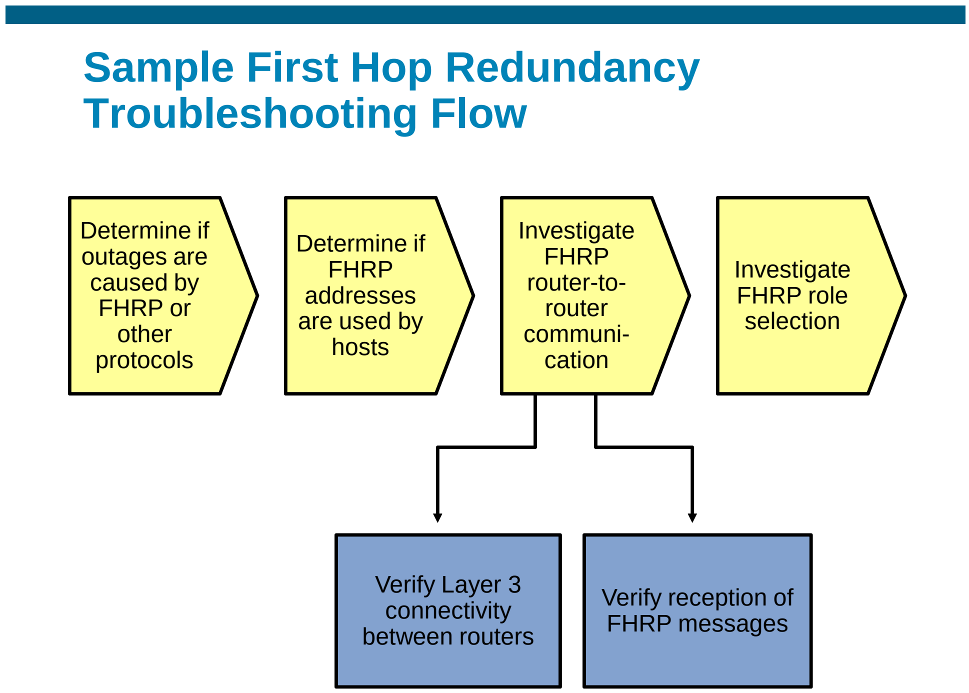
- If you observe that the pings to the real IP address of the redundant router and to the virtual IP address do not suffer packet loss, but the ping to the host further out in the network fails, this might indicate an issue with the routing protocol. Alternatively, it could indicate that the client is using the primary router address as its default gateway rather than the virtual IP address.

There are too many possible scenarios, combinations of ping results, and conclusions to list, but important clues can be gained in any scenario by comparing the differences between several pings during a failover.

If you have to troubleshoot without the opportunity to force failover for testing purposes, you might need to assume that the FHRP is the cause of the problem and carefully verify its implementation and operation, even if you cannot determine beforehand if this might be the cause of the problem.



Before starting to troubleshoot the FHRP itself, verify if the client is correctly using the virtual IP address and MAC address of the FHRP as its default gateway. This involves verifying the default gateway configuration (whether statically configured or learned via DHCP) and the ARP cache on the client to verify that both the virtual IP address and the virtual MAC address on the client match the expected values for the FHRP that is in use.



Many problems with FHRPs are caused by underlying problems in the Layer 3 connectivity between the routers. Therefore, a good next-step in the troubleshooting process is to verify that there is Layer 3 connectivity between all routers that are participating in the FHRP. Ping from each of the participating routers to the IP addresses of the other participating routers. If one of these pings fail, start a troubleshooting process to diagnose and resolve the Layer 3 connectivity issues between the routers before further investigating the FHRP.

When you have confirmed that there is Layer 3 connectivity between the participating routers in general, you must verify the proper transmission and reception of FHRP packets. To limit potential disruption, always use **show** commands to gather information before using **debug** commands.

Verify Reception of FHRP Messages

```
DLS1#show standby vlan 100 brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl100       100  110 P Active  local           10.1.100.253    10.1.100.254


DLS2#show standby vlan 100 brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl100       100  100 P Standby 10.1.100.252    local           10.1.100.254
```

This example shows how to confirm proper transmission and reception of HSRP messages. For GLBP or VRRP, the procedure is similar, although the command output is slightly different.

To confirm the proper reception of HSRP messages on all routers in the group, verify that all routers list an active and a standby router and that these roles are listed in a consistent way across all the routers. The **show standby brief** command is concise and still shows the most relevant information. As you can see in the example, switch DLS2 lists the IP address of switch DLS1 as the active router. As the standby router, it lists “local” to indicate that it considers itself to be the standby router. On switch DLS1, the situation is the opposite: The address of switch DLS2 is listed as the standby address, while the active router is listed as local. While you are verifying these roles, this is also a good opportunity to confirm that both the standby group number and the virtual IP address are configured in a consistent manner. Misconfiguration of these parameters is a common cause of HSRP problems.

```
DLS1#debug standby packets

DLS1#show logging | include Grp 100
Oct 26 15:29:00.049: HSRP: Vl100 Grp 100 Hello  in  10.1.100.253 Standby pri 100
vIP 10.1.100.254
Oct 26 15:29:01.659: HSRP: Vl100 Grp 100 Hello  out 10.1.100.252 Active  pri 110
vIP 10.1.100.254
```

Note: If you used Telnet, you cannot see the debug messages without using the **terminal monitor** command.

If you find inconsistencies in the output of the **show standby brief** commands, such as a missing standby router on one of the routers or multiple routers claiming the active or standby role for a group, this strongly suggests that there is a problem with the reception or interpretation of the HSRP messages on the routers. A **debug** command can now be used to investigate the transmission and reception of HSRP messages to gather more clues about the failure.

Before enabling a debug, first verify that the CPU of the device is not running at such high levels that adding the load of a debug would risk overloading the CPU. Secondly, it is always good to have a fallback plan to stop the debug when it unexpectedly starts to affect the performance of the device. For instance, you could open a second connection to the device and before you enable the debug in your primary session, type the **undebug all** command in the secondary session, but do not confirm it by pressing the Enter key yet. Another fallback scenario is to schedule a timed reload within a short time by using the **reload in** command. If you lose your connection to the device as a result of your debug, you can be assured that it will reload shortly and you will be able to reconnect to it. And finally, you should always refer to your organization's policies before executing any commands on a device that put the operation of the network at risk.

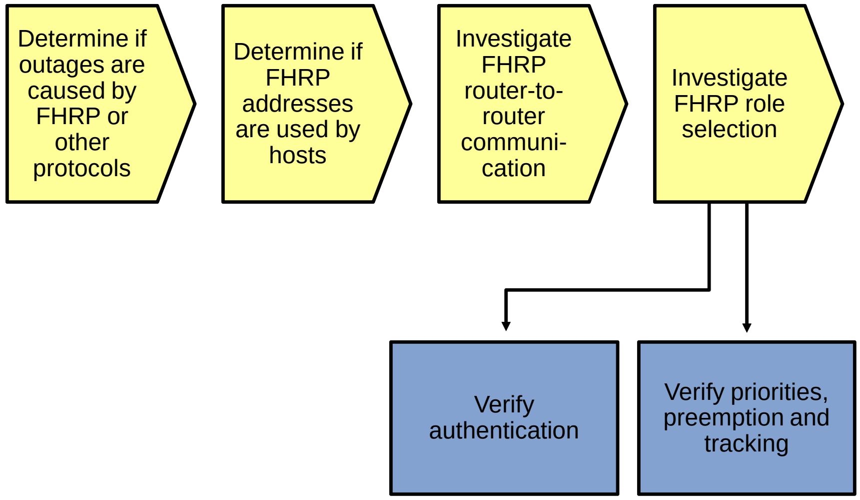
The **debug standby packets** command displays all HSRP packets sent or received by the device. This can quickly generate a lot of output, especially if you have configured many different HSRP groups or if you have tuned the hello timer to be shorter than the default value of three seconds. To make it easier to select the packets that you are interested in, you could use the technique shown in the example above. Instead of logging the debug output to the console or virtual terminal session, you can capture the output in a buffer in the device's RAM and then display the buffer's content by using the **show logging** command. The output of the command can then be filtered by using a regular expression to select the HSRP group that you are interested in.

In the example above, the output reveals that hellos are sent by this router and received from the other router. Just like the **show** commands in the previous output examples, execute the **debug** command on both routers to spot possible differences in behavior between the devices.

Do not forget to disable the debug by using the **no debug** command after you have gathered the information that you were interested in.

If these debugs reveal that HSRP protocol packets are not properly received on any router, check if access lists are blocking the packets. Given that you have already verified the Layer 3 connectivity between the devices, this problem should be on a higher layer.

Sample First Hop Redundancy Troubleshooting Flow



After you have established that FHRP messages are sent and received properly on all routers and still the FHRP does not perform as expected, the problem must be related to the role selection and transferring roles between routers during failover. You might need to verify two potential problem areas.

If the FHRP is using authentication and there is a mismatch between the authentication parameters, the devices will not accept each other's messages as valid when they are received. A typical symptom is that more than one router considers itself to be the active router for a group.

For all FHRPs, role selection is influenced by two parameters: priority and preemption. Tracking objects such as interfaces and routes can further alter these priorities. If an unexpected router is selected for the primary role at any point in the process, carefully analyze the priorities configured on the different devices and how they are affected by potential tracking options. However, to properly determine how properties behave during a failover, you must be able to force a failover, which means that you might need to postpone this type of testing until a regularly scheduled maintenance interval.

Reflection Questions

1. Which lab trouble tickets did you have the most difficulty with?

2. For the trouble tickets that you had difficulty with, would you change anything about the process that you used now that you see the resolution of the problem?

3. Which commands did you find most useful in diagnosing Layer 3 and HSRP issues? Add these to your toolbox for future use. Which commands did you find least useful?

References

If you need more information on the commands and their options, see the following references:

- Command References for Cisco Catalyst LAN Switches
Go to http://www.cisco.com/en/US/products/hw/switches/index.html. Then select product category (Campus LAN) and the model you are working with (for example 3560-E). The Command References for various IOS releases are under the "Reference Guides" section.
- Virtual LANs and VLAN Trunking Protocol Troubleshooting Tech Notes
www.cisco.com/en/US/tech/tk389/tk689/tsd_technology_support_troubleshooting_technotes_list.html
- Layer 3 Switching and Forwarding Troubleshooting Tech Notes
www.cisco.com/en/US/tech/tk389/tk815/tsd_technology_support_troubleshooting_technotes_list.html

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1700	Fast Ethernet 0 (FA0)	Fast Ethernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
1800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2600	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)
2800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. Rather than try to list all the combinations of configurations for each router class, this table includes identifiers for the possible combinations of Ethernet and serial interfaces in the device. The table does not include any other type of interface, even though a specific router might contain one. An example of this is an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

Device Configurations (Instructor version)

Note: All device configurations are provided for TT-A, including those that are the same as the baseline as defined in Lab 3-1. The configs provided here are *not* running-config outputs. They can be used for cut-and-paste for TT-A and subsequent tickets. Where a config is noted as being the same as a previous one, the only change is in the MOTD, which identifies the Lab and TT. The errors in the configuration are commented and highlighted as red text.

Trouble Ticket—TT-A Configurations

Switch ALS1

```
!Lab 4-2 Switch ALS1 TT-A Config
!
hostname ALS1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 4-2 Switch ALS1 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet

spanning-tree mode rapid-pvst
spanning-tree portfast default
!
interface Vlan1
 no ip address
 shutdown
!
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
```



```
vlan 30
 name GUEST
!
vlan 100
 name MGMT
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel1
 description Channel to DLS1
 no shutdown
 !
interface Port-channel2
 description Channel to DLS2
 no shutdown
!
interface FastEthernet0/1
 description Channel to DLS1
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shutdown
!
interface FastEthernet0/2
 description Channel to DLS1
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shutdown
!
interface FastEthernet0/3
 description Channel to DLS2
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shutdown
!
interface FastEthernet0/4
 description Channel to DLS2
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shutdown
```



```
!
interface FastEthernet0/5
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown

interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
```

```
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description To PC-B
 switchport access vlan 10
 switchport mode access
 switchport voice vlan 20
 spanning-tree portfast
 switchport port-security
 switchport port-security maximum 2
 switchport port-security violation shutdown
 switchport port-security mac-address sticky
 no shut
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
```

```
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan100
 ip address 10.10.100.1 255.255.255.0
 no shutdown
!
ip default-gateway 10.1.100.254
!
ip http server
ip http secure-server
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
```

Error: VLAN 100 SVI IP address is incorrect.

ip address 10.1.100.1 255.255.255.0


```
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server host 10.1.50.1 version 2c cisco
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps vlan-membership
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
  no transport input
!
ntp source Vlan100
ntp server 10.1.202.1
end
```

Switch DLS1

```
!Lab 4-2 Switch DLS1 TT-A Config
!
hostname DLS1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55

banner motd $*** Lab 4-2 Switch DLS1 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
!
ip domain name tshoot.net
ip host R1 10.1.2.2 10.1.1.1 10.1.201.1
```



```
ip host R2 10.1.1.2 10.1.1.6 10.1.202.1
ip host R3 10.1.1.5 10.1.2.14 10.1.203.1
ip host ALS1 10.1.100.1
ip host DLS1 10.1.100.252 10.1.2.1
ip host DLS2 10.1.100.253 10.1.2.13
!
ip dhcp excluded-address 10.1.10.252 10.1.10.254
ip dhcp excluded-address 10.1.20.252 10.1.20.254
ip dhcp excluded-address 10.1.30.252 10.1.30.254
!
ip dhcp pool OFFICE
   network 10.1.10.0 255.255.255.0
   default-router 10.1.10.254
   domain-name tshoot.net
!
ip dhcp pool VOICE
   network 10.1.20.0 255.255.255.0
   default-router 10.1.20.254
   domain-name tshoot.net
!
ip dhcp pool GUEST
   network 10.1.30.0 255.255.255.0
   default-router 10.1.30.254
   domain-name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 24576
spanning-tree vlan 20,50 priority 28672
!
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 100
 name MGMT
```



```
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel1
 description Channel to ALS1
 no shut
!
interface Port-channel10
 description Channel to DLS2
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
```

```
interface FastEthernet0/5
 description FE to R1
 no switchport
 ip address 10.1.2.1 255.255.255.252
 speed 100
 duplex full
 spanning-tree bpduguard enable
 no shut
!
interface FastEthernet0/6
 description FE to SRV1
 switchport access vlan 50
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shut
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
```



```
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
```

```
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown

interface Vlan10
 ip address 10.1.10.252 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 priority 110
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.252 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.252 255.255.255.0
```



```
 standby 30 ip 10.1.30.254
 standby 30 priority 110
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.252 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 preempt
!
interface Vlan100
 ip address 10.1.100.252 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 priority 110
 standby 100 preempt
!
router eigrp 1
 passive-interface default
 no passive-interface Fa0/5
 no auto-summary
 network 10.1.0.0 0.0.255.255
!
ip classless
ip http server
ip http secure-server
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server host 10.1.50.1 version 2c cisco
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 10.1.202.1
end
```


Switch DLS2

```
!Lab 4-2 Switch DLS2 TT-A Config
!
hostname DLS2
!
service timestamps debug datetime msec
service timestamps log datetime
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 4-2 Switch DLS2 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
ip domain name tshoot.net
ip host R1 10.1.2.2 10.1.1.1 10.1.201.1
ip host R2 10.1.1.2 10.1.1.6 10.1.202.1
ip host R3 10.1.1.5 10.1.2.14 10.1.203.1
ip host ALS1 10.1.100.1
ip host DLS1 10.1.100.252 10.1.2.1
ip host DLS2 10.1.100.253 10.1.2.13
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
  path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 28672
spanning-tree vlan 20,50 priority 24576
```



```
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 100
 name MGMT
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel2
 description Channel to ALS1
 no shut

interface Port-channel10
 description Channel to DLS1
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
```



```
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R3
 no switchport
 ip address 10.1.2.13 255.255.255.252
 speed 100
 duplex full
 spanning-tree bpduguard enable
 no shut
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
```

```
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description FE to PC-C
 switchport access vlan 30
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/19
```



```
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
```



```
!
interface Vlan10
 ip address 10.1.10.253 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.253 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 priority 110
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.253 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.253 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 priority 110
 standby 50 preempt
!
interface Vlan100
 ip address 10.1.100.253 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 preempt
!
!
router eigrp 1
 passive-interface default
 no passive-interface Fa0/5
 no auto-summary
 network 10.1.0.0 0.0.255.255
!
ip classless
ip http server
ip http secure-server
!
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 10.1.50.1 version 2c cisco
!
```



```
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 10.1.202.1
end
```

Router R1

```
!Lab 4-2 Router R1 TT-A Config
!
hostname R1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 4-2 Router R1 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
ip host R1 10.1.2.2 10.1.1.1 10.1.201.1
ip host R2 10.1.1.2 10.1.1.6 10.1.202.1
ip host R3 10.1.1.5 10.1.2.14 10.1.203.1
ip host ALS1 10.1.100.1
ip host DLS1 10.1.100.252 10.1.2.1
ip host DLS2 10.1.100.253 10.1.2.13
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
```



```
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 10.1.201.1 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown
!
interface FastEthernet0/1
 description FE to DLS1
 ip address 10.1.2.2 255.255.255.252
 ip flow ingress
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
 description WAN link to R2 - 128k leased line
 ip address 10.1.1.1 255.255.255.252
 ip flow ingress
 encapsulation ppp
 clock rate 128000
  no shutdown
!
interface Serial0/0/1
 description WAN link to R3 (not used)
 no ip address
 shutdown
!
router eigrp 1
 passive-interface default
 no passive-interface FastEthernet0/1
 no passive-interface Serial0/0/0
 network 10.1.1.0 0.0.0.3
 network 10.1.2.0 0.0.0.3
 network 10.1.201.1 0.0.0.0
 no auto-summary
!
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
logging source-interface Loopback0
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
```



```
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 10.1.202.1
end
```

Router R2

```
!Lab 4-2 Router R2 TT-A Config
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
Hostname R2
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 4-2 Router R2 TT-A Config ***$
!
no ip domain lookup
ip host R1 10.1.2.2 10.1.1.1 10.1.201.1
ip host R2 10.1.1.2 10.1.1.6 10.1.202.1
ip host R3 10.1.1.5 10.1.2.14 10.1.203.1
ip host ALS1 10.1.100.1
ip host DLS1 10.1.100.252 10.1.2.1
ip host DLS2 10.1.100.253 10.1.2.13
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
```



```
 write-memory
!
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 10.1.202.1 255.255.255.255
!
interface FastEthernet0/0
 shutdown
!
interface FastEthernet0/1
 shutdown
!
interface Serial0/0/0
 description WAN link to R1 - 128k leased line
 ip address 10.1.1.2 255.255.255.252
 encapsulation ppp
 no shutdown

!
interface Serial0/0/1
 description WAN link to R3 - 128k leased line
 ip address 10.1.1.6 255.255.255.252
 clock rate 128000
 encapsulation ppp
 no shutdown
!
router eigrp 1
 passive-interface default
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
 network 10.1.1.0 0.0.0.3
 network 10.1.1.4 0.0.0.3
 network 10.1.202.1 0.0.0.0
 no auto-summary
!
ip http server
no ip http secure-server
!
logging source-interface Loopback0
logging 10.1.50.1
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
```



```
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
!
ntp master 3
 end
```

Router R3

```
!Lab 4-2 Router R3 TT-A Config
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 4-2 Router R3 TT-A Config ***$
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
no ip domain lookup
ip domain name tshoot.net
ip host R1 10.1.2.2 10.1.1.1 10.1.201.1
ip host R2 10.1.1.2 10.1.1.6 10.1.202.1
ip host R3 10.1.1.5 10.1.2.14 10.1.203.1
ip host ALS1 10.1.100.1
ip host DLS1 10.1.100.252 10.1.2.1
ip host DLS2 10.1.100.253 10.1.2.13
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 10.1.203.1 255.255.255.255
!
interface FastEthernet0/0
```



```
 no ip address
 shutdown

interface FastEthernet0/1
 description FE to DLS2
 ip address 10.1.2.14 255.255.255.252
 ip flow ingress
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
 description WAN link to R1 - (Not used)
 no ip address
 clock rate 128000
 encapsulation ppp
 shutdown
!
interface Serial0/0/1
 description WAN link to R2 - 128k leased line
 ip address 10.1.1.5 255.255.255.252
 ip flow ingress
 encapsulation ppp
 no shutdown
!
router eigrp 1
 passive-interface default
 no passive-interface FastEthernet0/1
 no passive-interface Serial0/0/1
 network 10.1.1.4 0.0.0.3
 network 10.1.2.12 0.0.0.3
 network 10.1.203.1 0.0.0.0
 no auto-summary
!
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
logging source-interface Loopback0
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
```



```
 logging synchronous
line vty 0 4
 exec-timeout 60 0
transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 10.1.202.1
end
```

Trouble Ticket—TT-B Configurations

Router R1 – Same as TT-A

Router R2 – Same as TT-A

Router R3 – Same as TT-A

Switch ALS1

```
!Lab 4-2 Switch ALS1 TT-B Config
!
hostname ALS1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 4-2 Switch ALS1 TT-B Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip domain name tshoot.net
ip host R1 10.1.2.2 10.1.1.1 10.1.201.1
ip host R2 10.1.1.2 10.1.1.6 10.1.202.1
ip host R3 10.1.1.5 10.1.2.14 10.1.203.1
ip host ALS1 10.1.100.1
ip host DLS1 10.1.100.252 10.1.2.1
ip host DLS2 10.1.100.253 10.1.2.13
!
```



```
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet

spanning-tree mode rapid-pvst
spanning-tree portfast default
!
interface Vlan1
 no ip address
 shutdown
!
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 100
 name MGMT
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel1
 description Channel to DLS1
 no shutdown
 !
interface Port-channel2
 description Channel to DLS2
 no shutdown
!
interface FastEthernet0/1
 description Channel to DLS1
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shutdown
!
interface FastEthernet0/2
```

```
 description Channel to DLS1
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shutdown
!
interface FastEthernet0/3
 description Channel to DLS2
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shutdown
!
interface FastEthernet0/4
 description Channel to DLS2
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shutdown
!
interface FastEthernet0/5
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown

interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
```



```
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
```

```
!
interface FastEthernet0/18
 description To PC-B
 switchport access vlan 10
 switchport mode access
 switchport voice vlan 20
 spanning-tree portfast
 switchport port-security
 switchport port-security maximum 2
 switchport port-security violation shutdown
 switchport port-security mac-address sticky
 no shut
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/1
 description Unused
 switchport access vlan 999
```



```
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan100
 ip address 10.1.100.1 255.255.255.0
 no shutdown
!
ip default-gateway 10.1.100.254
!
ip http server
ip http secure-server
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server host 10.1.50.1 version 2c cisco
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps vlan-membership
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
  no transport input
!
ntp source Vlan100
ntp server 10.1.202.1
end
```

Switch DLS1

```
!Lab 4-2 Switch DLS1 TT-B Config
!
hostname DLS1
!
service timestamps debug datetime msec
```



```
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55

banner motd $*** Lab 4-2 Switch DLS1 TT-B Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
!
ip domain name tshoot.net
!
ip dhcp excluded-address 10.1.10.252 10.1.10.254
ip dhcp excluded-address 10.1.20.252 10.1.20.254
ip dhcp excluded-address 10.1.30.252 10.1.30.254
!
ip dhcp pool OFFICE
   network 10.1.10.0 255.255.255.0
   default-router 10.1.10.252
   domain-name tshoot.net
!
ip dhcp pool VOICE
   network 10.1.20.0 255.255.255.0
   default-router 10.1.20.254
   domain-name tshoot.net
!
ip dhcp pool GUEST
   network 10.1.30.0 255.255.255.0
   default-router 10.1.30.254
   domain-name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog contenttype plaintext
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
```

Error: Default router for OFFICE VLAN 10 provided by DHCP should be the HSRP standby address of 10.1.10.254.

`default-router 10.1.10.254`

```
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 24576
spanning-tree vlan 20,50 priority 28672
!
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 100
 name MGMT
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel1
 description Channel to ALS1
 no shut
!
interface Port-channel10
 description Channel to DLS2
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
```



```
!
interface FastEthernet0/3
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R1
 no switchport
 ip address 10.1.2.1 255.255.255.252
 speed 100
 duplex full
 spanning-tree bpduguard enable
 no shut
!
interface FastEthernet0/6
 description FE to SRV1
 switchport access vlan 50
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shut
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
```

```
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
```



```
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/2
 description Unused
 switchport access vlan 999
```



```
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown

interface Vlan10
 ip address 10.1.10.252 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 priority 110
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.252 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.252 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 priority 110
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.252 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 preempt
!
interface Vlan100
 ip address 10.1.100.252 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 priority 110
 standby 100 preempt
!
router eigrp 1
 passive-interface default
 no passive-interface Fa0/5
 no auto-summary
 network 10.1.0.0 0.0.255.255
!
ip classless
ip http server
ip http secure-server
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server host 10.1.50.1 version 2c cisco
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
```



```
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 10.1.202.1
end
```

Switch DLS2

```
!Lab 4-2 Switch DLS2 TT-B Config
!
hostname DLS2
!
service timestamps debug datetime msec
service timestamps log datetime
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 4-2 Switch DLS2 TT-B Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500

vtp domain TSHOOT
vtp mode transparent

ip subnet-zero
ip routing
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
```



```
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
  path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 28672
spanning-tree vlan 20,50 priority 24576

vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 100
 name MGMT
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel2
 description Channel to ALS1
 no shut

interface Port-channel10
 description Channel to DLS1
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/2
```

```
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R3
 no switchport
 ip address 10.1.2.13 255.255.255.252
 speed 100
 duplex full
 spanning-tree bpduguard enable
 no shut
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
```



```
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
```

```
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description FE to PC-C
 switchport access vlan 30
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/1
 description Unused
```



```
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 10.1.10.253 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.253 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 priority 110
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.253 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.253 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 priority 110
 standby 50 preempt
!
interface Vlan100
 ip address 10.1.100.253 255.255.255.0
 standby 10 ip 10.1.100.245
 standby 10 preempt
!
router eigrp 1
 passive-interface default
no passive-interface Fa0/5
 no auto-summary
 network 10.1.0.0 0.0.255.255
!
ip classless
ip http server
ip http secure-server
!
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
```

Error: Interface VLAN 100 standby group and standby IP address are incorrect.

```
interface Vlan100
 standby 100 ip 10.1.100.254
 standby 100 preempt
```

```
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 10.1.202.1
end
```

Trouble Ticket—TT-C Configurations

Switch ALS1 - Same as TT-B

Router R1 – Same as TT-A

Router R2 – Same as TT-A

Router R3 – Same as TT-A

Switch DLS1

```
!Lab 4-2 Switch DLS1 TT-C Config
!
hostname DLS1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55

banner motd $*** Lab 4-2 Switch DLS1 TT-C Config ***$
!
no ip domain lookup
!
```



```
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
!
ip domain name tshoot.net
!
key chain TEST
 key 1
   key-string C1sc0
!
ip dhcp excluded-address 10.1.10.252 10.1.10.254
ip dhcp excluded-address 10.1.20.252 10.1.20.254
ip dhcp excluded-address 10.1.30.252 10.1.30.254
!
ip dhcp pool OFFICE
   network 10.1.10.0 255.255.255.0
   default-router 10.1.10.254
   domain-name tshoot.net
!
ip dhcp pool VOICE
   network 10.1.20.0 255.255.255.0
   default-router 10.1.20.254
   domain-name tshoot.net
!
ip dhcp pool GUEST
   network 10.1.30.0 255.255.255.0
   default-router 10.1.30.254
   domain-name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog contenttype plaintext
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 24576
spanning-tree vlan 20,50 priority 28672
!
vlan 10
```



```
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 100
 name MGMT
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel1
 description Channel to ALS1
 no shut
!
interface Port-channel10
 description Channel to DLS2
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
```



```
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R1
 no switchport
 ip address 10.1.2.1 255.255.255.252
 speed 100
 duplex full
 spanning-tree bpduguard enable
 no shut
!
interface FastEthernet0/6
 description FE to SRV1
 switchport access vlan 50
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shut
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
```



```
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/19
 description Unused
```



```
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
```



```
interface Vlan10
 ip address 10.1.10.252 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 priority 110
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.252 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.252 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 priority 110
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.252 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 preempt
!
interface Vlan100
 ip address 10.1.100.252 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 priority 110
 standby 100 preempt
 standby 100 authentication md5 key-chain TEST
!
router eigrp 1
 passive-interface default
 no passive-interface Fa0/5
 no auto-summary
 network 10.1.0.0 0.0.255.255
!
ip classless
ip http server
ip http secure-server
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server host 10.1.50.1 version 2c cisco
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
!
```



```
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 10.1.202.1
end
```

Switch DLS2

```
!Lab 4-2 Switch DLS2 TT-C Config
!
hostname DLS2
!
service timestamps debug datetime msec
service timestamps log datetime
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 4-2 Switch DLS2 TT-C Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500

vtp domain TSHOOT
vtp mode transparent

ip subnet-zero
ip routing
ip domain name tshoot.net
!
key chain TEST
 key 1
   key-string Clsc0
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
```

Error: Key chain added but key-string does not match DLS1. The DLS1 key-string is C1sc0 (second character is a number 1). The DLS2 key-string is Clsc0 (second character is a lowercase L).

```
key chain TEST
 key 1
   key-string C1sc0
```



```
  logging size 50
  notify syslog
  hidekeys
  path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 28672
spanning-tree vlan 20,50 priority 24576

vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 100
 name MGMT
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel2
 description Channel to ALS1
 no shut

interface Port-channel10
 description Channel to DLS1
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
```

```
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R3
 no switchport
 ip address 10.1.2.13 255.255.255.252
 speed 100
 duplex full
 spanning-tree bpduguard enable
 no shut
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
```



```
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
```

```
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description FE to PC-C
 switchport access vlan 30
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
```



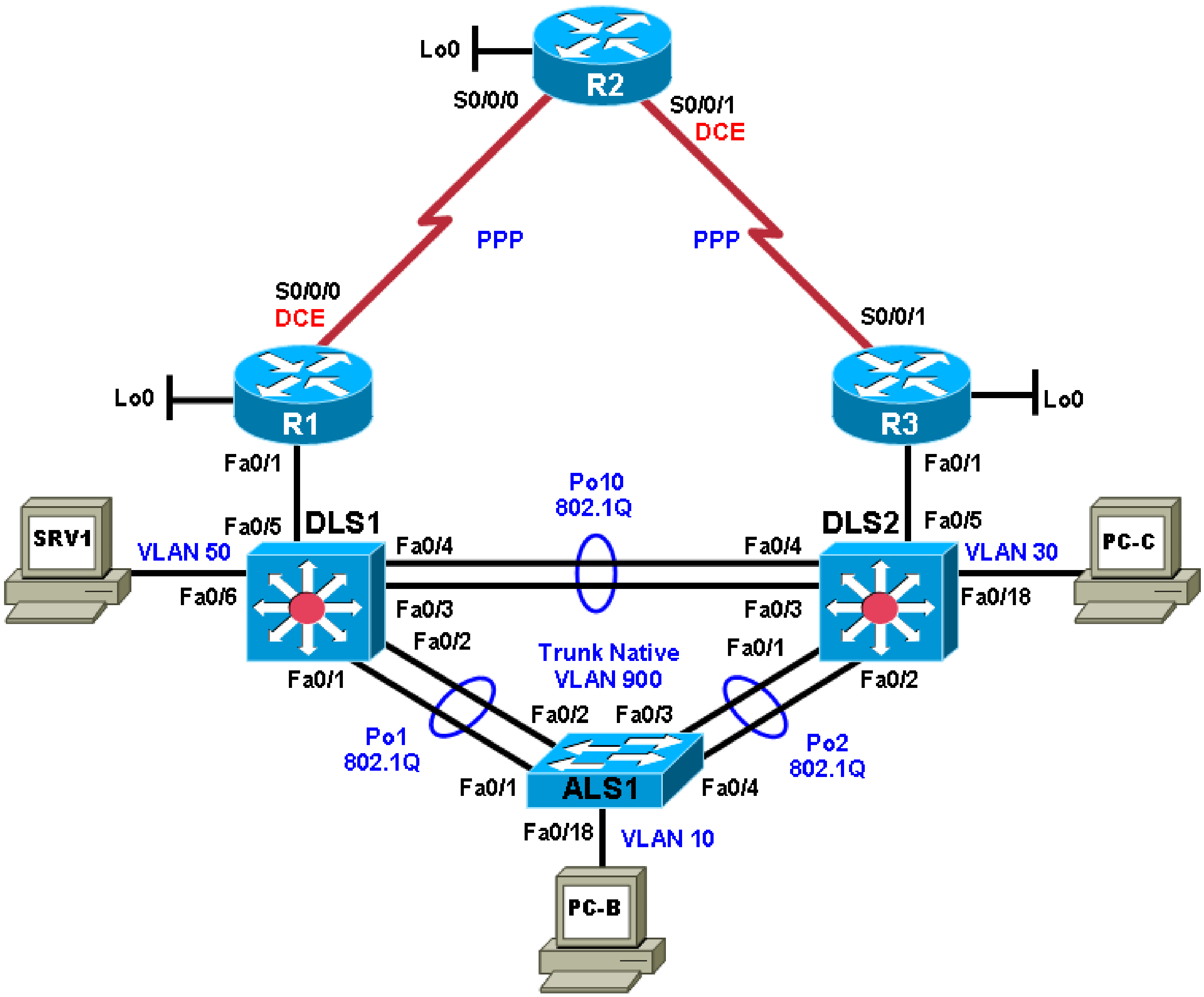
```
 shutdown
!
interface GigabitEthernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 10.1.10.253 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.253 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 priority 110
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.253 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.253 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 priority 110
 standby 50 preempt
!
interface Vlan100
 ip address 10.1.100.253 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 preempt
 standby 100 authentication md5 key-chain TEST
!
router eigrp 1
 passive-interface default
 no passive-interface Fa0/3
 no passive-interface Fa0/4
 no passive-interface Fa0/5
 no auto-summary
 network 10.1.0.0 0.0.255.255
!
ip classless
ip http server
ip http secure-server
!
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
```



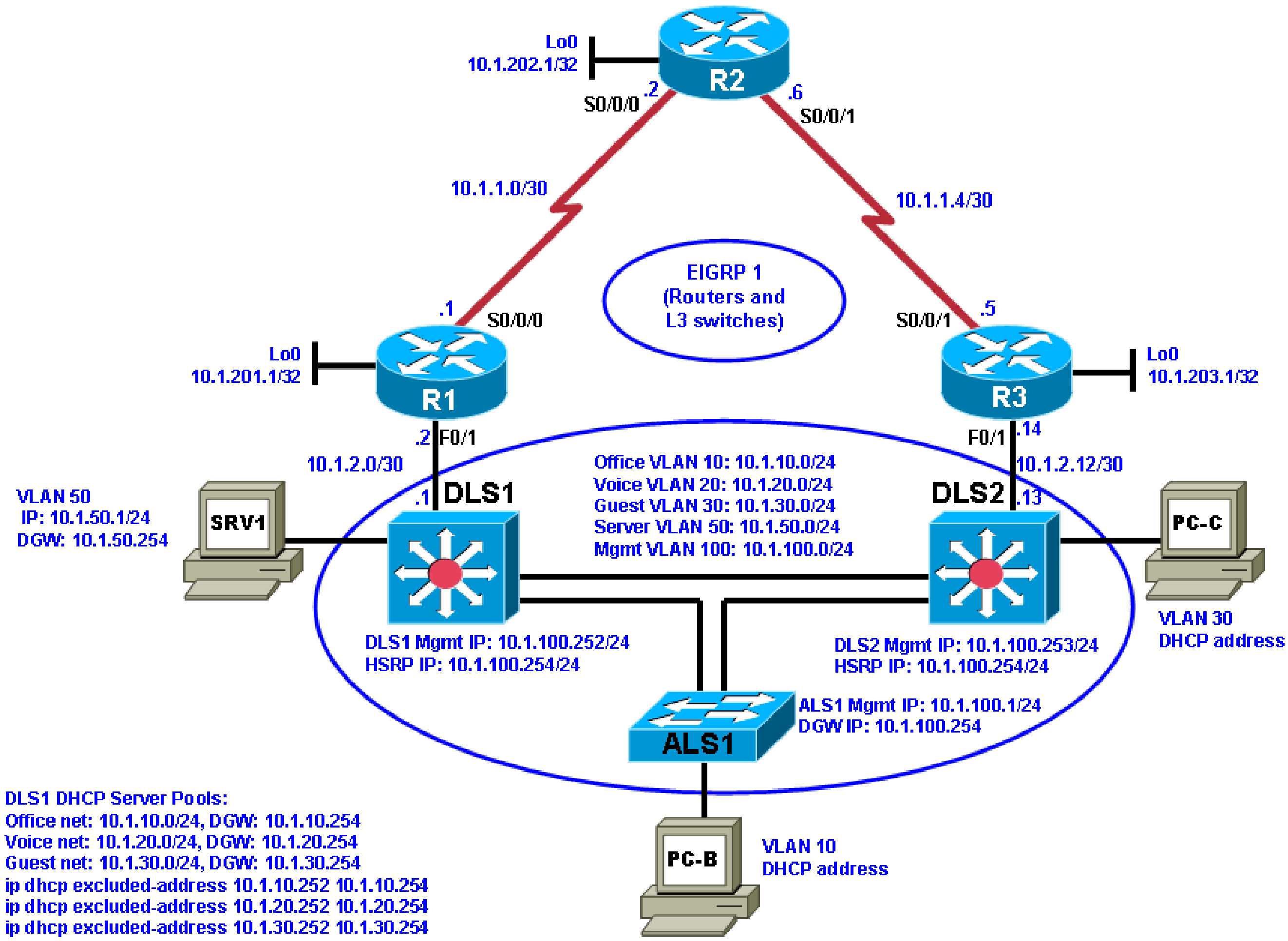
```
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 10.1.202.1
end
```

Chapter 5 Lab 5-1, Layer 3 Connectivity and EIGRP **Instructor Version**

Physical Topology



Logical Topology



Objectives

- Load the trouble ticket device configuration files for each trouble ticket.
- Diagnose and resolve problems related to network layer connectivity.
- Diagnose and resolve problems related to EIGRP.
- Document troubleshooting progress, configuration changes, and problem resolution.

Background

Because of the complexity of modern networks, Layer 3 routing issues are quite common and can also be difficult to troubleshoot. One of the most widely used enterprise routing protocols is Enhanced Interior Gateway Routing Protocol (EIGRP). It is a Cisco proprietary distance vector, classless routing protocol that was released in 1992 with Cisco IOS Release 9.21. EIGRP has features that are not commonly found in other distance vector routing protocols, such as the following:

- Reliable Transport Protocol (RTP)
- Bounded updates
- Diffusing Update Algorithm (DUAL)
- Establishing adjacencies

- Neighbor and topology tables

In this lab, you will troubleshoot problems related to Layer 3 connectivity and routing problems related to EIGRP.

For each task or trouble ticket, the trouble scenario and problem symptom are described. While troubleshooting, you will discover the cause of the problem, correct it, and then document the process and results.

Physical and Logical Topology Diagrams

The physical and logical topologies, including the interface designations and IP addresses, are provided to assist the troubleshooting effort.

Lab Structure

This lab is divided into two main sections.

Section 1—Trouble Tickets and Troubleshooting Logs

This section includes multiple tasks. Each task is associated with a trouble ticket (TT) and introduces one or more errors on one or more devices. If time is a consideration, each task or trouble ticket can be performed independently.

Section 2—Troubleshooting Reference Information

This section provides general Layer 3 and EIGRP troubleshooting information that can be applied to any trouble ticket in this lab. Sample troubleshooting flows are provided, along with examples of useful commands and output. If time permits, it is recommended that you read through Section 2 prior to starting on the trouble tickets.

Instructor note: Because the troubleshooting reference section is lengthy, ask students to read through it prior to starting the lab to become familiar with the troubleshooting flows and commands used in this lab. Consider assigning it as homework.

Note: This lab uses Cisco 1841 routers with Cisco IOS Release 12.4(24)T1 and the Advanced IP Services image c1841-advipservicesk9-mz.124-24.T1.bin. The switches are Cisco WS-C2960-24TT-L with the Cisco IOS image c2960-lanbasek9-mz.122-46.SE.bin and Catalyst 3560-24PS with the Cisco IOS image c3560-advipservicesk9-mz.122-46.SE.bin. Other routers (such as 2801 and 2811), switches (such as 2950 or 3550), and Cisco IOS Software versions can be used if they have comparable capabilities and features. Depending on the router or switch model and Cisco IOS Software version, the commands available and output produced might vary from what is shown in this lab.

Instructor Notes

- The lab topology should be pre-built prior to the students starting the lab. Ensure that all routers and switches (R1, R2, R3, ALS1, DLS1, and DLS2) have the course lab configuration files installed in flash. These can be downloaded from the Academy Connection website.
- The device configurations that contain trouble ticket errors or modifications from the baseline are included at the end of the lab, and the errors in them are identified.
- Each device should have a directory named “tshoot” in flash. This directory contains the baseline configuration file for that device as well as the configuration files for the labs. Refer to Lab 3-1 for instructions on creating the tshoot directory in flash.
- Instructors can use a TFTP server, USB drive, flash memory card, or other method to copy all the course configuration files into the flash:/tshoot directory for each device in the topology.
- For this and subsequent labs, the student is responsible for loading the trouble ticket configurations as required using the procedure described in Lab 3-1.
- Set the correct time on router R2, which serves as the primary NTP server for the lab network.
- If time is an issue, each task (trouble ticket) can be performed independently.

Required Resources

- 3 routers (Cisco 1841 with Cisco IOS Release 12.4(24)T1 Advanced IP Service or comparable)
- 1 switch (Cisco 2960 with the Cisco IOS Release 12.2(46)SE C2960-LANBASEK9-M image or comparable)
- 2 switches (Cisco 3560 with the Cisco IOS Release 12.2(46)SE C3560-advipservicesk9-mz image or comparable)
- 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

Instructor Notes

This lab is divided into multiple tasks. Each task is associated with a trouble ticket (TT) and introduces one or more errors on one or more devices.

Students can work individually or as a team. The problems introduced in this lab are related to Layer 3 switching and EIGRP.

Suggested actions and results presented during the troubleshooting process for each TT can be shared with the students during debrief or copies of the instructor version of the lab can be made available to the students to assist them in verifying their work.

Section 1—Trouble Tickets and Troubleshooting Logs

Task 1: Trouble Ticket Lab 5-1 TT-A

Instructor note: This trouble ticket involves DLS1 and DLS2 issues related to SVIs and addressing, as well as R2 issues related to network advertisement.

Step 1: Review trouble ticket Lab 5-1 TT-A.

Your company is interested in implementing an IP-based closed circuit television (CCTV) solution. Currently, different solutions and vendors are being evaluated. One of the vendors has offered to implement a pilot to show the capabilities of their solution. To keep the traffic associated with the CCTV solution separate from the regular network traffic, it will be implemented using a new VLAN (VLAN 70 corresponding to subnet 10.1.70.0/24). There must be communication between the test server (PC-C) and the office users on the LAN. In addition, branch workers on the R2 LAN (simulated by Lo0) must be able to access the internal CCTV server.

The vendor will come in tomorrow to install the client and server software. The network team has been asked to make sure that the new VLAN has been implemented and that there is IP connectivity between the local test client (PC-B) and the CCTV test server (PC-C) in the CCTV VLAN. You must also verify that there is connectivity between the remote test client (Lo0 on R2) and the CCTV test server. The test server requires a static IP address. One of your colleagues implemented the static address yesterday afternoon, but did not have time to test the implementation.

You have the following tasks:

- Configure the CCTV test server (PC-C).
- Verify the CCTV VLAN device configurations for the pilot.
- Ensure that the local and remote test clients can communicate with the CCTV test server before the vendor arrives to implement the CCTV pilot.
- Verify Hot Standby Router Protocol (HSRP) redundancy for CCTV VLAN 70.

Step 2: Load the device trouble ticket configuration files for TT-A.

Using the procedure described in Lab 3-1, verify that the lab configuration files are present in flash. Load the configuration files indicated in the Device Configuration File table.

Note: The following device access methods are in effect after loading the configuration files:

- Console access requires no username or password.
- Telnet and SSH require username **admin** and password **adminpa55**.
- The enable password is **ciscoenpa55**.

Instructor note: Although it is not considered security best practice, the student can set the console and VTY line exec-timeout to 0 0 to facilitate performance of this lab.

Device Configuration File Table

Device Name	File to Load	Notes
ALS1	Lab51-ALS1-TT-A-Cfg.txt	This file is the same as the baseline
DLS1	Lab51-DLS1-TT-A-Cfg.txt	This file contains configuration errors
DLS2	Lab51-DLS2-TT-A-Cfg.txt	This file contains configuration errors
R1	Lab51-R1-TT-A-Cfg.txt	This file is the same as the baseline
R2	Lab51-R2-TT-A-Cfg.txt	This file contains configuration errors
R3	Lab51-R3-TT-A-Cfg.txt	This file is the same as the baseline

SRV1	N/A	Static IP: 10.1.50.1 Default gateway: 10.1.50.254
PC-B	N/A	DHCP (test CCTV client)
PC-C	N/A	Static (test CCTV server)

Instructor note: The student loads the "broken" TT configuration files for all devices, even though only the configurations indicated in the Notes column contain errors.

Step 3: Configure the CCTV server IP address.

Configure the test server PC-C with a static IP address in the CCTV test VLAN subnet 10.1.70.0/24. According to the test plan, the default gateway should be the last usable IP address in the subnet.

Note: After this TT is completed, restore PC-C to its status as a DHCP client in VLAN 30.

Step 4: Release and renew the DHCP lease on PC-B.

Ensure that PC-B is configured as a DHCP client in the OFFICE VLAN.

After loading all TT-A device configuration files, issue the **ipconfig /release** and **ipconfig /renew** commands on PC-B.

Step 5: Outline the troubleshooting approach and validation steps.

Use this space to identify your troubleshooting approach and the key steps to verify that the problem is resolved. Troubleshooting approaches to select from include: follow-the-path, spot-the-differences, bottom-up, top-down, divide-and-conquer, shoot-from-the-hip, and move-the-problem.

Note: In addition to a specific approach, you can use the generic troubleshooting process described at the beginning of Section 2 of this lab.

____

____

____

____

____

The follow-the-path or the spot-the-differences approach can be used.

Verification steps can include:

- Local test client PC-B can ping test server PC-C.
- Remote test client (simulated by R2 Lo0) can ping test server PC-C.
- Connectivity tests can be accomplished with one Layer 3 switch down to verify redundancy.

Step 6: Record the troubleshooting process and configuration changes.

Note: Section 2 of this lab includes sample troubleshooting flows, useful commands, and examples of output.

Use this log to document your actions and results during the troubleshooting process. List the commands you used to gather information. As you progress, record what you think the problem might be and which actions you will take to correct the problem.

Device	Actions and Results

Responses will vary but could include:

- Pings from PC-B to the CCTV test server (PC-C) at the assigned static address (for example, 10.1.70.1) fail.
- Pings from PC-B to its default gateway 10.1.10.254 on DLS1 succeed.
- Pings from PC-B to all other network devices succeed.
- Pings from ALS1 to DLS1 (10.1.100.252) and DLS2 (10.1.100.253) succeed.
- Pings from ALS1 to the DLS1 VLAN 70 SVI address (10.1.70.252) fail.
- Pings from ALS1 to the DLS2 VLAN 70 SVI address (10.1.70.253) fail.
- Pings from R2 using Lo0 (10.1.202.1, the simulated remote branch client) as the source address to test the server (PC-C) at the assigned static address (for example, 10.1.70.1) fail.

TT-A Issue 1- DLS1 VLAN 70 was not added to trunk Po10.

The process suggested here tests local client access and HSRP redundancy first and then tests remote client access.

- The **`show vlan brief`** command on DLS1 indicates that the CCTV VLAN 70 is defined and active.
- The **`show vlan id 70`** command on DLS1 shows no ports carrying this VLAN.
- The **`show spanning-tree vlan 70`** command on DLS1 indicates that no spanning-tree instances exist for VLAN 70.

- The **show ip interface vlan 70** command on DLS1 indicates that the VLAN 70 SVI IP address is configured correctly as 10.1.70.252/24. The interface is up, but the protocol is down.
- The **show interfaces trunk** command on DLS1 indicates that VLAN 70 is not allowed on the trunk between DLS1 and DLS2.

Action: Add VLAN 70 as an allowed VLAN to interface Po10. This also adds VLAN 70 to the physical interfaces Fa0/3 and Fa0/4. Refer to TT-A debrief for more information.

Verification: The line protocol on interface VLAN 70 is up.

Verification: Pings from PC-B to the CCTV test server (PC-C) at the assigned static address (for example, 10.1.70.1) succeed.

TT-A Issue 2 - The DLS2 VLAN 70 IP address is not on the same subnet as DLS1, so there is no HSRP redundancy.

- The traceroute from PC-B to the test server PC-C shows a path through DLS1.
- Test local client FHRP redundancy by reloading DLS1 and pinging from PC-B to PC-C while DLS1 is reloading.
- Pings from PC-B to the CCTV test server (PC-C) at the assigned static address (for example, 10.1.70.1) fail.
- The **show standby vlan 70** command on DLS1 indicates that DLS1 is the active local HSRP router for VLAN 70 and that the standby router is unknown.
- The **show standby brief** command on DLS2 indicates that DLS2 is in the init state and that the standby router is unknown.
- The **show spanning-tree vlan 70** command on DLS2 indicates that interfaces F0/18 and Po10 are both designated and forwarding for VLAN 70.
- The **show ip interface vlan 70** command on DLS2 indicates that the VLAN 70 SVI IP address is configured incorrectly as 10.70.1.253/24 and is on a different subnet than DLS1 VLAN 70, so there is no HSRP redundancy.

Action: Change the VLAN 70 SVI IP address to be on the same subnet as DLS1 (for example, 10.1.70.253/24). Refer to TT-A debrief for more information.

Verification: Test local client FHRP redundancy by restarting DLS1 and pinging from PC-B to PC-C while DLS1 is reloading. Pings should be successful. The **show standby brief** command on DLS2 indicates that DLS2 is the active router for VLAN 70 and that the standby router is known (DLS1 is 10.1.70.252).

TT-A Issue 3 - R2 Lo0 has a network address that is not advertised by EIGRP.

- Pings from R2 using Lo0 (10.1.202.1—the simulated remote branch client) as the source address to the test server (PC-C) at the assigned static address (for example, 10.1.70.1) fail using the command **ping 10.1.70.1 source Lo0**.
- Pings from R2 using the default source address to the test server (PC-C) at the assigned static address (for example, 10.1.70.1) succeed using the command **ping 10.1.70.1**.
- The **show ip route** command on R2 indicates that the VLAN 70 network address 10.1.70.0/24 is in the routing table learned via EIGRP (D).
- The **show ip route** command on R2 indicates that the loopback0 IP address 10.1.202.1/32 is listed in the routing table as a directly connected network.
- The **show ip route 10.1.70.1** command on R2 indicates that there are two equal-cost routes to the 10.1.70.0/24 network.

- The **`show ip cef 10.1.70.1`** command confirms that the Cisco Express Forwarding database contains two next-hop entries: 10.1.1.1 via S0/0/0 and 10.1.1.5 via S0/0/1. R2 has two routes to the test server 10.1.70.1.
- The **`traceroute 10.1.70.1`** command on R2 confirms that there is a route and that ping requests are reaching the test server PC-C. However, the PC might not know how to send the ping replies back to R2.
- The **`show ip route`** command on DLS1 and DLS2 indicates that network address 10.1.202.1 (R2 Lo0 IP address) is not in either routing table and that no static or default route is present.
- The **`show run | begin eigrp`** command on R2 confirms that the Lo0 interface IP address 10.1.202.1/32 is not being advertised by EIGRP.

Action: Add the Lo0 interface IP address (10.1.202.1/32) to the EIGRP 1 process so that it will be advertised to DLS1 and DLS2. Refer to TT-A debrief for more information.

Verification: Pings from R2 using Lo0 (the simulated remote branch client) as the source address to the test server (PC-C) at the assigned static address (for example, 10.1.70.1) succeed using the command **`ping 10.1.70.1 source Lo0`**.

Step 7: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with your instructor. The notes can include problems encountered, solutions applied, useful commands employed, alternate solutions, methods and processes, and procedure and communication improvements.

____

____

____

____

____

____

____

Trouble Ticket TT-A Debrief—Instructor Notes

The problems in this trouble ticket are caused by several issues.

TT-A—Issue 1

The first issue is that the new CCTV test VLAN 70 is not allowed on the Po10 trunk between DLS1 and DLS2. This causes the SVI to be up/down.

To solve issue 1 problems, run the following command on DLS1:

```
DLS1(config)#interface port-channel10
DLS1(config-if)#switchport trunk allowed vlan 10,20,30,50,70,100
```

or

```
DLS1(config-if)#switchport trunk allowed vlan add 70
```

Note: If issue 1 on DLS1 is resolved before issue 2, the local client PC-B can reach the test server PC-C with one hop through DLS1 to DLS2.

TT-A—Issue 2

The second issue is that SVI VLAN 70 on DLS2 was configured with an IP address in a different network than DLS1. The switches cannot establish an HSRP relationship, and packets from PC-B cannot be routed directly from VLAN 10 to VLAN 70 through DLS2 (assuming that issue 1 still exists, and VLAN 70 is not allowed on interface Po10 of DLS1).

Issue 2 alone does not prevent the test client PC-B from communicating with the test server PC-C, unless DLS1 goes down. Then the client has no standby router. This might have gone unnoticed as a hidden issue due to the redundancy of the network.

To solve issue 2 problems, run the following commands on DLS2:

```
DLS2(config)#interface vlan 70
DLS2(config-if)#ip address 10.1.70.253 255.255.255.0
```

Note: If issue 2 on DLS2 is resolved before issue 1, the local client PC-B can reach the test server PC-C, but the packets must go through five hops: PC-B > DLS1 > R1 > R2 > R3 > DLS2 > PC-C.

TT-A—Issue 3

The third issue is not related to the CCTV test VLAN. It is a routing issue on R2. The remote branch CCTV test client Lo0 interface IP address is not included in the EIGRP networks to be advertised. Thus, DLS1 and DLS2 did not know of the route, and there was only one-way communication between R2 Lo0 and PC-C. Ping packets from the R2 source interface Lo0 could reach the test server PC-C, but they could not return, so the pings failed.

```
R2(config)#router eigrp 1
R2(config-router)#network 10.1.202.1 0.0.0.0
```

Task 2: Trouble Ticket Lab 5-1 TT-B

Instructor note: This trouble ticket involves issues related to interface settings on routers R1 and R3 resulting from an incorrect router restoration procedure.

Step 1: Review trouble ticket Lab 5-1 TT-B.

You receive an emergency call and are told that a short circuit caused a small fire in the server room. Routers R1 and R3, which were mounted in the same rack, were damaged. Luckily, you had two comparable spare routers in storage. When you arrive at the office, two of your colleagues have already installed the replacement routers, cabled them, and tried to restore the routers by cutting and pasting the configurations from the console. However, the routers are not operational when you come in.

You receive a call from the network administrator at the branch office (LAN simulated by R2 Lo0) asking about the loss of the WAN. His users cannot access server SRV1 at the central site. He has started to troubleshoot. You tell him what happened and ask him not to do anything until you have resolved the problem at the central site.

Your task is to check the configuration of routers R1 and R3 and restore the configurations as necessary to regain connectivity between the branch office and the central site across the WAN.

Step 2: Load the device trouble ticket configuration files for TT-B.

Using the procedure described in Lab 3-1, verify that the lab configuration files are present in flash. Load the configuration files indicated in the Device Configuration File table.

Note: See Task 1, Step 2 for device access methods, usernames, and passwords after the configuration files have been loaded.

Device Configuration File Table

Device Name	File to Load	Notes
ALS1	Lab51-ALS1-TT-B-Cfg.txt	This file is the same as the baseline
DLS1	Lab51-DLS1-TT-B-Cfg.txt	This file is the same as the baseline

DLS2	Lab51-DLS2-TT-B-Cfg.txt	This file is the same as the baseline
R1	Lab51-R1-TT-B-Cfg.txt	This file contains configuration errors
R2	Lab51-R2-TT-B-Cfg.txt	This file is the same as the baseline
R3	Lab51-R3-TT-B-Cfg.txt	This file contains configuration errors
SRV1	N/A	Static IP: 10.1.50.1 Default gateway: 10.1.50.254
PC-B	N/A	DHCP (release and renew after loading device configurations)
PC-C	N/A	DHCP (release and renew after loading device configurations)

Step 3: Configure SRV1 and start the syslog and TFTP servers, as described in Task 1.

Step 4: Release and renew the DHCP leases on PC-B and PC-C, as described in Task 1.

Step 5: Outline the troubleshooting approach and validation steps.

Use this space to identify your troubleshooting approach and the key steps to verify that the problem is resolved. Troubleshooting approaches to select from include: follow-the-path, spot-the-differences, bottom-up, top-down, divide-and-conquer, shoot-from-the-hip, and move-the-problem.

Note: In addition to a specific approach, you can use the generic troubleshooting process described at the beginning of Section 2 of this lab.

____

____

____

____

____

The follow-the-path or the spot-the-differences approach can be used.

Verification steps can include:

Users on the branch office LAN (simulated by R2 Lo0) can ping server SRV1.
Redundant EIGRP equal-cost paths exist from the R2 LAN to SRV1 via the R1 and R3 serial links.

Step 6: Record the troubleshooting process and configuration changes.

Note: Section 2 of this lab includes sample troubleshooting flows, useful commands, and examples of output.

Use this log to document your actions and results during the troubleshooting process. List the commands you used to gather information. As you progress, record what you think the problem might be and which actions you will take to correct the problem.

Device	Actions and Results

Device	Actions and Results

TT-B Issue 1 - The configurations were reversed when used to restore R1 and R3. R1 is now configured as R3, and R3 is configured as R1.

Responses will vary but could include:

- Pings from PC-B to SRV1 (10.1.50.1) succeed.
- Pings from PC-C to SRV1 (10.1.50.1) succeed.
- Pings from R2 using Lo0 (10.1.202.1—the simulated remote branch LAN user) as the source address to SRV1 (10.1.50.1) fail.
- EIGRP error messages on the router with prompt R1 (actually physical router R3) report that neighbor 10.1.2.13 is not on the common subnet for FastEthernet0/1. This router is connected to neighbor 10.1.2.13, which is DLS2.
- The **`show interfaces Fa0/1`** command on the router with prompt R1 (physical router R3) indicates that this router's Fa0/1 interface is configured with the IP address of the Fa0/1 interface connected to DLS1.
- The **`show ip route`** command on the router with prompt R1 (physical router R3) indicates that the routing table has no routes learned via EIGRP (D).
- The **`show ip protocols`** command on the router with prompt R1 (physical router R3) indicates that it is routing for the networks 10.1.1.0/30, 10.1.2.0/30, and 10.1.201.1/32. These networks should be advertised by the router connected to DLS1.
- EIGRP error messages on the router with prompt R3 (actually physical router R1) report that neighbor 10.1.2.1 is not on the common subnet for FastEthernet0/1. This router is connected to neighbor 10.1.2.1, which is actually DLS1.
- The **`show interfaces Fa0/1`** command on the router with prompt R3 (actually physical router R1) indicates that the router's Fa0/1 interface is configured with the IP address of the Fa0/1 interface connected to DLS2.

- The **`show ip route`** command on the router with prompt R3 indicates that the routing table has no routes learned via EIGRP (D).
- The **`show ip protocols`** command on the router with prompt R3 (actually R1) indicates that it is routing for the networks 10.1.1.4/30, 10.1.2.12/30, and 10.1.203.1/32. These network routes should be advertised by the router connected to DLS2.
- The configuration information in each router (R1 and R3) is the opposite of what it should be. It appears that the configurations between R1 and R3 have been accidently reversed.

Action: For each physical router, erase the startup config and reload the router. Configure the correct hostname, and configure Fa0/1 and the serial interface (S0/0/0 for R1 and S0/0/1 for R3) with the correct IP address and subnet mask, according to the network documentation. Enable the interfaces with the **`no shutdown`** command. Advertise the FastEthernet networks and serial networks under EIGRP. Refer to TT-B debrief for more information.

Note: For physical router R1, it is really only necessary to configure the Fa0/1 link and advertise it under EIGRP. However, R3 requires that all WAN links be functional to access the TFTP server SRV1.

Copy the correct backup (or archive) configuration from the TFTP server SRV1 to the startup config and reload the router. Another option is to use the **`configure replace`** command to overlay the existing running config. Additional information can be found in the TT-B debrief.

Verification: Pings from R2 using Lo0 (the simulated remote branch client) as the source address to SRV1 at the IP address 10.1.50.1 succeed using the command **`ping 10.1.50.1 source Lo0`**.

Step 7: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with your instructor. The notes can include problems encountered, solutions applied, useful commands employed, alternate solutions, methods and procedure, and procedure and communication improvements.

____

____

____

____

____

____

____

Trouble Ticket TT-B Debrief—Instructor Notes

TT-B Issue 1

The main problem in this trouble ticket is caused by the configuration of router R1 being loaded on router R3 and vice versa. This problem has multiple solutions. You can restore basic connectivity to the headquarters LAN and then load the correct configurations from the archive on the TFTP server. You can also fully reconfigure both routers based on the available documentation.

To restore connectivity to the headquarters LAN on router R1, correct the IP addresses on interfaces FastEthernet 0/1 and serial 0/0/0 and enable them under EIGRP. This can be achieved by issuing the following commands.

Note: For physical router R1 to gain access to SRV1, it is only necessary to configure the Fa0/1 interface and advertise it under EIGRP. However, R3 requires all WAN links and EIGRP functionality to access SRV1.

```
interface FastEthernet 0/1
```



```
 ip address 10.1.2.2 255.255.255.252
 no shut

interface Serial 0/0/0
 ip address 10.1.1.1 255.255.255.252
 encapsulation ppp
 clock rate 128000
 no shut

router eigrp 1
 network 10.1.2.0 0.0.0.3
 network 10.1.1.0 0.0.0.3
```

After running these commands, you can copy an archived backup configuration from the TFTP server SRV1 to the startup configuration and reload router R1.

In a similar manner, issuing the following commands restores LAN connectivity for router R3:

```
interface FastEthernet 0/1
 ip address 10.1.2.14 255.255.255.252
 no shut

interface Serial 0/0/1
 ip address 10.1.1.5 255.255.255.252
 encapsulation ppp
 no shut

router eigrp 1
 network 10.1.2.12 0.0.0.3
 network 10.1.1.4 0.0.0.3
```

After this configuration change, an archived backup configuration can also be copied from the TFTP server SRV1 to the startup configuration of router R3, and the router can be reloaded.

As a less disruptive alternative, you can use the **`configure replace`** command to replace the current running configuration with the archived backup configuration, without the need to reload. However, the routers can be reloaded with minimal disruption to network operation if the task is timed and coordinated properly.

If you do not have a good backup configuration to which to roll back, you can also fully reconfigure routers R1 and R3 based on the documentation and diagrams. The following commands represent a minimal list of the changes necessary to reconfigure routers R1 and R3 to match the original baseline configuration:

```
hostname R1
!
interface Loopback0
 ip address 10.1.201.1 255.255.255.255
!
interface FastEthernet0/1
 description FE to DLS1
 ip address 10.1.2.2 255.255.255.252
 no shutdown
!
interface Serial0/0/0
 description WAN link to R2 - 128k leased line
 ip address 10.1.1.1 255.255.255.252
 encapsulation ppp
 clock rate 128000
 no shutdown
```



```
interface Serial0/0/1
 no ip address
 shutdown
!
router eigrp 1
 no network 10.1.1.4 0.0.0.3
 no network 10.1.2.12 0.0.0.3
 no network 10.1.203.1 0.0.0.0

 network 10.1.1.0 0.0.0.3
 network 10.1.2.0 0.0.0.3
 network 10.1.201.1 0.0.0.0
 no auto-summary
!
```

In a similar manner, R3 can be reconfigured to match the original baseline configuration by issuing the following commands:

```
hostname R3
!
interface Loopback0
 ip address 10.1.203.1 255.255.255.255
!
interface FastEthernet0/1
 description FE to DLS2
 ip address 10.1.2.14 255.255.255.252
 no shutdown
!
interface Serial0/0/0
 no ip address
 shutdown

interface Serial0/0/1
 description WAN link to R2 - 128k leased line
 ip address 10.1.1.5 255.255.255.252
 encapsulation ppp
 no shutdown
!
router eigrp 1
 no network 10.1.1.0 0.0.0.3
 no network 10.1.2.0 0.0.0.3
 no network 10.1.201.1 0.0.0.0

 network 10.1.1.4 0.0.0.3
 network 10.1.2.12 0.0.0.3
 network 10.1.203.1 0.0.0.0
 no auto-summary
```

Task 3: Trouble Ticket Lab 5-1 TT-C

Instructor note: This trouble ticket involves issues related to EIGRP default route propagation on R2.

Step 1: Review trouble ticket Lab 5-1 TT-C.

A user on VLAN 10 (PC-B) called the help desk this morning because she does not have Internet access. When she tried to open a website (simulated by another Loopback Lo1 on R2 with address 209.165.200.225/30), she received an error message from her browser saying that it cannot display the web page. She can reach the internal server SRV1 without any problems.

One of your colleagues was working with the ISP to make some changes to the routing model used to access the ISP and the Internet. The ISP does not run EIGRP on its router. The colleague has called in sick today, but made some notes in the log about the ISP not running EIGRP on its router and not wanting R2 to attempt to establish an EIGRP neighbor relationship.

Your task is to diagnose and solve this problem and make sure that the user regains connectivity to the Internet.

Step 2: Load the device trouble ticket configuration files for TT-C.

Using the procedure described in Lab 3-1, verify that the lab configuration files are present in flash. Load the proper configuration files indicated in the Device Configuration File table.

Note: See Task 1, Step 2 for device access methods, usernames, and passwords after the configuration files have been loaded.

Device Configuration File Table

Device Name	File to Load	Notes
ALS1	Lab51-ALS1-TT-C-Cfg.txt	This file is the same as the baseline
DLS1	Lab51-DLS1-TT-C-Cfg.txt	This file is the same as the baseline
DLS2	Lab51-DLS2-TT-C-Cfg.txt	This file is the same as the baseline
R1	Lab51-R1-TT-C-Cfg.txt	This file is the same as the baseline
R2	Lab51-R2-TT-C-Cfg.txt	This file contains configuration errors
R3	Lab51-R3-TT-C-Cfg.txt	This file is the same as the baseline
SRV1	N/A	Static IP: 10.1.50.1 Default gateway: 10.1.50.254
PC-B	N/A	DHCP
PC-C	N/A	DHCP

Step 3: Configure SRV1 and start the syslog and TFTP servers, as described in Task 1.

Step 4: Release and renew the DHCP leases on PC-B and PC-C, as described in Task 1.

Step 5: Outline the troubleshooting approach and validation steps.

Use this space to identify your troubleshooting approach and the key steps to verify that the problem is resolved. Troubleshooting approaches to select from include: follow-the-path, spot-the-differences, bottom-up, top-down, divide-and-conquer, shoot-from-the-hip, and move-the-problem.

Note: In addition to a specific approach, you can use the generic troubleshooting process described at the beginning of Section 2 of this lab.

____

____

____

____

____

____

The follow-the-path or the spot-the-differences approach can be used.

Verification steps can include:

User PC-B in VLAN 10 can access the Internet via R2 Lo1 (209.165.200.225).

All EIGRP routers (R1, R2, R3, DLS1, and DLS2) have a route to the Internet (simulated by R2 Lo1).

Step 6: Record the troubleshooting process and configuration changes.

Note: Section 2 of this lab includes sample troubleshooting flows, useful commands, and examples of output.

Use this log to document your actions and results during the troubleshooting process. List the commands you used to gather information. As you progress, record what you think the problem might be and which actions you will take to correct the problems.

Device	Actions and Results

TT-C Issue 1 - A default route to the ISP (simulated by R2 link Lo1—209.165.200.225/30) was created to provide Internet access for the private network clients but was not redistributed to other EIGRP routers.

Responses will vary but could include:

- Browsing from PC-B to R2 using Lo0 (10.1.202.1) succeeds.
- Browsing from PC-B to R2 using Lo1 (209.165.200.225) fails.
- Pings from PC-B to R2 using Lo1 (209.165.200.225) fail.
- Pings from PC-C to R2 using Lo1 (209.165.200.225) fail.
- Pings from PC-B to SRV1 (10.1.50.1) succeed.
- Traceroute from PC-B to R2 Lo0 succeeds and takes path DLS1 > R1 > R2.
- Traceroute from PC-B to R2 Lo1 fails. DLS1 reports: “Destination host unreachable.”
- Traceroute from PC-C to R2 Lo1 fails. DLS2 reports: “Destination host unreachable.”
- The **`show ip protocols`** command on R2 indicates that it is routing for the networks 10.1.1.0/30, 10.1.1.4/30, and 10.1.202.1/32. According to the network documentation, these are the correct networks that should be advertised by R2.

- The **`show ip route`** command on DLS1 and DLS2 indicates that the routing table does not have a route to the simulated ISP 209.165.200.225/30 that was learned via EIGRP (D), but there are routes to all other networks in the topology.
- The **`show ip route`** command on R1 and R3 indicates that the routing table does not have a route to the simulated ISP 209.165.200.225/30 that was learned via EIGRP (D), but there are routes to all other networks in the topology.
- The **`show ip route`** command on R2 indicates that there is a route to the PC-B VLAN 10 subnet.
- The **`show ip route`** command on R2 indicates that there is a directly connected static default route (quad zero) to the ISP pointing to R2 Lo1.
- The **`show ip cef`** command on R2 indicates that network 209.165.200.225/30 is attached and the next hop is Lo1.
- The **`show run interface Lo1`** command indicates that this interface is identified as the simulated WAN link to the ISP.
- The **`show ip interface brief`** command indicates that interface Lo1 is up/up.
- A static default (quad zero) route to the Internet is defined on R2 (simulated ISP WAN—R2 Lo1), but none of the other routers in the EIGRP topology know about it.

Action: Redistribute the default route to the other EIGRP routers. This provides a path to the Internet for these routers, but it does not use Lo1 as an EIGRP interface to send hellos to the ISP. See the TT debrief notes for additional information. Refer to TT-C debrief for more information.

Verification: PC-B should now be able to access the Internet (via R2 Lo1), and all routers should have an external EIGRP (D*EX) route to 0.0.0.0/0 via their next hop. See notes in Step 5.

Step 7: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with your instructor. The notes can include problems encountered, solutions applied, useful commands employed, alternate solutions and methods, and procedure and communication improvements.

____

____

____

____

____

____

____

Trouble Ticket TT-C Debrief—Instructor Notes

TT-C Issue

The ISP has requested changes to R2 to use a default route to reach the next hop and will provide a static route for the return route. To address this, a quad zero default route to the ISP (using Lo1) was created. The problem in this ticket is caused by router R2 not advertising this route to the other EIGRP routers in the topology.

To correct the problem, the **`redistribute static`** command is added on R2 to EIGRP process 1 using the following commands:

```
router eigrp 1
  redistribute static
```

Note: Point out that connectivity between the internal clients (PC-B) and the Internet (represented by R2 Lo1 209.165.200.225/30) could have been provided by simply adding the subnet as a network to the EIGRP routing process on R2. This would install the route into every EIGRP routing table. However, it would enable the Lo1 interface (normally a serial or Ethernet interface) to begin sending hello messages to the ISP, which was not what the ISP had requested. Also, it would only provide connectivity to the specific address represented by Lo1. If host PC-B sent a packet to an address not in this topology (for example, 172.16.1.1), DLS1 would not know where to send it because there is no default route.

Task 4: Trouble Ticket Lab 5-1 TT-D

Instructor note: Issues related to the EIGRP neighbor relationship between DLS1 and DLS2.

Step 1: Review trouble ticket Lab 5-1 TT-D.

A contract worker called the help desk to report that he could not access the ISP email server (simulated by Lo0 on R2). He was working at a PC that is attached to a port in the GUEST VLAN (PC-C). You checked with the ISP and discovered that they had an unplanned outage, and the WAN link from R2 to R3 had gone down temporarily. Users in the OFFICE VLAN did not experience any loss of connectivity to the email server during the WAN link outage. Your expectation, if one of the WAN links went down, was that users in the GUEST VLAN would still be able to reach the server because of the redundancy in the network design.

Your colleague will replicate this scenario during the maintenance window this evening. You have agreed to help her diagnose the problem and propose a plan that can account for an outage in one of the WAN links to R2 so that guest users do not lose connectivity to the ISP mail server.

Your plan is to simulate the R3-to-R2 WAN link going down. You do not have administrative control over ISP router R2. You will test connectivity, determine the cause of the problem, and recommend which configuration changes to the devices could correct the issue.

Step 2: Load the device trouble ticket configuration files for TT-D.

Using the procedure described in Lab 3-1, verify that the lab configuration files are present in flash. Load the proper configuration files indicated in the Device Configuration File table.

Note: See Task 1, Step 2 for device access methods, usernames, and passwords after the configuration files have been loaded.

Device Configuration File Table

Device Name	File to Load	Notes
ALS1	Lab51-ALS1-TT-D-Cfg.txt	This file is the same as the baseline
DLS1	Lab51-DLS1-TT-D-Cfg.txt	This file is the same as the baseline. The source of the problem is the baseline configuration.
DLS2	Lab51-DLS2-TT-D-Cfg.txt	This file is the same as the baseline. The source of the problem is the baseline configuration.
R1	Lab51-R1-TT-D-Cfg.txt	This file is the same as the baseline
R2	Lab51-R2-TT-D-Cfg.txt	This file is the same as the baseline
R3	Lab51-R3-TT-D-Cfg.txt	This file is the same as the baseline
SRV1	N/A	Static IP: 10.1.50.1 Default gateway: 10.1.50.254
PC-B	N/A	DHCP
PC-C	N/A	DHCP

Step 3: Configure SRV1 and start the syslog and TFTP servers, as described in Task 1.

Step 4: Release and renew the DHCP leases on PC-B and PC-C, as described in Task 1.

Step 5: Outline the troubleshooting approach and validation steps.

Use this space to identify your troubleshooting approach and the key steps to verify that the problem is resolved. Troubleshooting approaches to select from include: follow-the-path, spot-the-differences, bottom-up, top-down, divide-and-conquer, shoot-from-the-hip, and move-the-problem.

Note: In addition to a specific approach, you can use the generic troubleshooting process described at the beginning of Section 2 of this lab.

____

____

____

____

____

____

The follow-the-path or the spot-the-differences approach can be used.

Verification steps can include:

- Switches DLS1 and DLS2 become neighbors and can exchange EIGRP routes to provide an alternate route if one of the WAN links is down.
- User PC-C in GUEST VLAN 30 can access the Internet via R2 Lo0 10.1.202.1 with the R2–R3 WAN link down. The plan is to shut down the S0/0/1 interface on R3 to simulate an outage on the R2–R3 WAN link. Then ping from PC-C in VLAN 30 to the R2 Lo0 interface to demonstrate connectivity with the direct link down.
- Traceroute from PC-C to R2 Lo0 with both WAN links up goes from PC-C to DLS2 to R3 to R2. With the R2–R3 WAN link down, the traceroute from PC-C goes from PC-C to DLS2 to DLS1 to R1 to R2.

Step 6: Record the troubleshooting process and configuration changes.

Note: Section 2 of this lab includes sample troubleshooting flows, useful commands, and examples of output.

Use this log to document your actions and results during the troubleshooting process. List the commands you used to gather information. As you progress, record what you think the problem might be and which actions you will take to correct the problems.

Device	Actions and Results

Device	Actions and Results

TT-D Issue - There is no Layer 3 link between DLS1 and DLS2, which means that they do not form an EIGRP neighbor relationship. This is part of the baseline configuration.

Responses will vary but could include:

With both WAN links up:

Pings from PC-C to R2 using Lo0 (10.1.202.1) succeed.

Traceroute from PC-C to R2 Lo0 succeeds and takes path DLS2 (10.1.30.253) > R3 (10.1.2.14) > R2 (10.1.202.1).

The **show ip route** command on DLS1 indicates that it has a route to R2 Lo0 (10.1.202.1) via its Fa0/5 interface.

The **show ip route** command on DLS2 indicates that it has a route to R2 Lo0 (10.1.202.1) via its Fa0/5 interface.

To simulate the down WAN link from R2–R3, shut down the R3 interface S0/0/1. With the R2–R3 WAN link down:

Pings from PC-C to R2 using Lo0 (10.1.202.1) fail. DLS2 reports: “Destination host unreachable.”

Traceroute from PC-C to R2 Lo0 fails. DLS2 reports: “Destination host unreachable.”

Pings from SRV1 to R2 using Lo0 (10.1.202.1) succeed.

Pings from PC-C to SRV1 succeed.

- The **show ip route** command on DLS1 indicates that it has a route to R2 Lo0 (10.1.202.1) via its Fa0/5 interface.
- The **show ip route** command on DLS2 indicates that it does *not* have a route to R2 Lo0 (10.1.202.1) via its Fa0/5 interface.
- The **show ip cef 10.1.202.1** command on DLS1 indicates that network 10.1.202.1 is accessible via local Fa0/5 with a next hop of 10.1.2.2 (R1 Fa0/1).
- The **show ip route** command on R2 indicates that there is a route to the PC-B VLAN 10 subnet.

Whether the R2–R3 link is up or down:

- The **show run | beg eigrp** command on DLS1 and DLS2 indicates that passive interface is enabled as a default, but interface Fa0/5 is configured as non-passive.
- The **debug eigrp packets hello** command on DLS2 indicates that hello messages are being sent and received from only neighbor R3 (10.1.2.14) via Fa0/5. This confirms that there is no EIGRP message exchanges between DLS1 and DLS2. If there were EIGRP messages, DLS1 could inform

DLS2 of its route to R2, and DLS2 could reach 10.1.202.1 through DLS1. The Fa0/3 and Fa0/4 ports on DLS1 and DLS2 comprise a Layer 2 trunk, and a Layer 3 relationship is needed for EIGRP neighbors to establish a relationship.

Action (Refer to TT-D debrief for additional information):

Option 1—Configure an existing VLAN (or newly created VLAN) on the existing Layer 2 EtherChannel as non-passive so that EIGRP messages can be exchanged.

Option 2—Configure the DLS1 to DLS2 EtherChannel (Po10) as a Layer 3 link. Po10, Fa0/3, and Fa0/4 on each switch must be non-switchport and non-passive.

Step 7: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with your instructor. The notes can include problems encountered, solutions applied, useful commands employed, alternate solutions and methods, and procedure and communication improvements.

____

____

____

____

____

Trouble Ticket TT-D Debrief—Instructor Notes

TT-D Issue

This issue is the result of the Layer 2 EtherChannel between DLS1 and DLS2 not allowing EIGRP message exchange.

This is not necessarily an error and could be the way the network was intended to function.

No errors are introduced to the baselines in this TT. On DLS1 and DLS2, under the EIGRP routing process, the **`passive-interface default`** command makes all interfaces passive (including all SVI VLAN interfaces), unless an interface is explicitly made non-passive using the **`no passive-interface`** *`interface`* command. With the baseline configuration, Fa0/5 is non-passive. Fa0/5 is a Layer 3 link (routed switch port). So EIGRP messages are only exchanged between DLS1 and R1 and between DLS2 and R3. EIGRP will not form a neighbor relationship over the DLS1–DLS2 link as it is currently configured. Hello messages are not exchanged over the Layer 2 Fa0/3 and Fa0/4 interfaces between DLS1 and DLS2 because no Layer 3 method of communication is non-passive.

As a result, DLS2 learns about all non-connected router networks via R3 (DLS1 learns them via R1). When the WAN link between R3 and R2 goes down, R3 no longer receives updates from R2, and DLS2 loses its route to R2. A Layer 3 construct between DLS1 and DLS2 addresses this issue. Thus, when the R2–R3 link goes down, PC-C and DLS2 still have a route to R2 via DLS1. The path is PC-C > DLS2 > DLS1 > R1 > R2.

Option 1—Configure an existing VLAN (for example, VLAN 100) or newly created VLAN (for example, VLAN 200) on the existing Layer 2 EtherChannel as non-passive under the EIGRP 1 routing process so that a neighbor relationship can be established and routes can be exchanged. This VLAN also becomes the main transit for traffic from the LAN to R1 and R3 and exchange routes between DLS1 and DLS2.

To use existing VLAN 100, use the following commands.

Switch DLS1

```
router eigrp 1
 no passive-interface vlan 100
```

Switch DLS2


```
router eigrp 1
 no passive-interface vlan 100
```

If a newly created VLAN is configured, it will need to be allowed on the Layer 2 EtherChannel. The SVI should be assigned an appropriate IP address for each switch and made non-passive under the EIGRP 1.

Option 2—Configure the DLS1 to DLS2 EtherChannel (Po10) as a Layer 3 link. Fa0/3 and Fa0/4 and Po10 on each switch must be non-switchport and non-passive under EIGRP. The Layer 3 EtherChannel (Po10) must be assigned an IP address in the same subnet on both devices. As long as the subnet is on the 10.1.0.0/16 network, it does not need to be added as a network under EIGRP.

Note: This option changes the logical and physical network topology and spanning-tree topology as the link is no longer an 802.1Q trunk and does not carry tagged VLAN traffic. Both options change the routing table entries, because DLS1 and DLS2 might provide better routes to some network addresses on R1 and R3. Some routes that would have been learned via Fa0/5 on DLS1 or DLS2 are learned via VLAN 100 from the opposite switch.

Option 2 can be configured using the following commands.

Switch DLS1

```
no interface Port-channel10

interface Port-channel10
 description Channel to DLS2
 no switchport
 ip address 10.1.3.1 255.255.255.252
 no shut

interface FastEthernet0/3
 description Channel to DLS2
 no switchport
 no ip address
 channel-group 10 mode on
 no shutdown

interface FastEthernet0/4
 description Channel to DLS2
 no switchport
 no ip address
 channel-group 10 mode on
 no shutdown

router eigrp 1
 no passive-interface FastEthernet0/3
 no passive-interface FastEthernet0/4
 no passive-interface Port-channel10
```

Switch DLS2

```
no interface Port-channel10

interface Port-channel10
 description Channel to DLS1
 no switchport
 ip address 10.1.3.2 255.255.255.252
 no shut
!
interface FastEthernet0/3
 description Channel to DLS1
```



```
 no switchport
 no ip address
 channel-group 10 mode on
 no shutdown
!
interface FastEthernet0/4
 description Channel to DLS1
 no switchport
 no ip address
 channel-group 10 mode on
 no shutdown

router eigrp 1
 no passive-interface FastEthernet0/3
 no passive-interface FastEthernet0/4
 no passive-interface Port-channel10
```

Task 5: Trouble Ticket Lab 5-1 TT-E

Instructor note: This trouble ticket involves issues related to improperly configured EIGRP authentication.

Step 1: Review trouble ticket Lab 5-1 TT-E.

A tech support intern on VLAN 30 (PC-C) called the help desk this Monday morning to report problems accessing certain areas of the network. It appears that the routers, R1, R2, and R3, are either down or unreachable.

Your company is in the process of testing various security measures to protect the network. Over the weekend, your IT staff worked on a project to secure EIGRP by implementing MD5 authentication. The staff was instructed to test the configuration over the weekend and reverse the implementation in the event that there were connectivity problems.

Your task is to ensure that the R1, R2 and R3 routers are online and reachable.

Step 2: Load the device trouble ticket configuration files for TT-E.

Using the procedure described in Lab 3-1, verify that the lab configuration files are present in flash. Load the proper configuration files indicated in the Device Configuration File table.

Note: See Task 1, Step 2 for device access methods, usernames, and passwords after the configuration files have been loaded.

Device Configuration File Table

Device Name	File to Load	Notes
ALS1	Lab51-ALS1-TT-E-Cfg.txt	This file is the same as the baseline
DLS1	Lab51-DLS1-TT-E-Cfg.txt	This file is the same as the baseline
DLS2	Lab51-DLS2-TT-E-Cfg.txt	This file is the same as the baseline
R1	Lab51-R1-TT-E-Cfg.txt	This file contains configuration errors
R2	Lab51-R2-TT-E-Cfg.txt	This file contains configuration errors
R3	Lab51-R3-TT-E-Cfg.txt	This file contains configuration errors
SRV1	N/A	Static IP: 10.1.50.1 Default gateway: 10.1.50.254
PC-B	N/A	DHCP
PC-C	N/A	DHCP

Step 3: Configure SRV1 and start the syslog and TFTP servers, as described in Task 1.

Step 4: Release and renew the DHCP leases on PC-B and PC-C, as described in Task 1.

Step 5: Outline the troubleshooting approach and validation steps.

Use this space to identify your troubleshooting approach and the key steps to verify that the problem is resolved. Troubleshooting approaches to select from include: follow-the-path, spot-the-differences, bottom-up, top-down, divide-and-conquer, shoot-from-the-hip, and move-the-problem.

Note: In addition to a specific approach, you can use the generic troubleshooting process described at the beginning of Section 2 of this lab.

____

____

____

____

____

____

The follow-the-path or the spot-the-differences approach can be used.

Verification steps can include:

Tech support staff who are using PC-B and PC-C can reach each other, but the routers are unreachable.

Step 6: Record the troubleshooting process and configuration changes.

Note: Section 2 of this lab includes sample troubleshooting flows, useful commands, and examples of output.

Use this log to document your actions and results during the troubleshooting process. List the commands you used to gather information. As you progress, record what you think the problem might be and which actions you will take to correct the problems.

Device	Actions and Results

Device	Actions and Results

TT-E Issue 1 – The EIGRP authentication was configured on R1, R2, and these two routers are sharing routes. However, there are still problems with the authentication configuration on R1 and R3. EIGRP authentication was not configured on DLS1 and DLS2, which prevents them from becoming neighbors with R1 and R3 respectively and explains why PC-B and PC-C cannot reach the R1, R2 and R3 loopback networks.

Responses will vary but could include:

- Browsing from PC-B to R2 using Lo0 (10.1.202.1) fails.
- Browsing from PC-B to R1 using Lo0 (10.1.201.1) fails.
- Pings from PC-C to R1 using Lo0 (10.1.201.1) fail.
- Pings from PC-C to R2 using Lo0 (10.1.202.1) fail.
- Pings from PC-B to SRV1 (10.1.50.1) succeed.
- Traceroute from PC-B to R2 Lo0 fails..
- Pings from R1 to R2 s0/0/1 interface succeed.
- Traceroute from PC-C to R2 Lo0 fails.
- The **`show ip protocols`** command on R2 indicates that it is routing for the networks 10.1.1.0/30, 10.1.1.4/30, and 10.1.202.1/32. According to the network documentation, these are the correct networks that should be advertised by R2.
- The **`show ip route`** command on DLS1 and DLS2 indicates that the routing table does not have routes to the networks on R1, R2,and R3 routers.
- The **`show ip route`** command on R1 and R2 indicates that the routing table does not have all the routes learned via EIGRP (D) to reach R3, DLS1 and DLS2.
- The **`show ip route`** command on R2 indicates that there are routes to R1.
- The **`show ip route`** command on R2 indicates that there are no routes learned via EIGRP for R3, DLS1 and DLS2..
- The **`show ip eigrp neighbors`** command on all the routers indicates the routers are unable to form adjacencies with all their neighboring routers.

Action:

Run the **`debug ip eigrp packets verbose`** command on the routers to check the EIGRP authentication messages for errors.

Check the interface authentication configuration commands for errors.

The key names used for EIGRP authentication are case-sensitive and must be the same on all routers for authentication to work properly.

Check to ensure that the EIGRP autonomous system number matches the autonomous system number used in the interface authentication.

Verification: PC-B and PC-C should now be able to access the R1, R2, and R3 routers..

Step 7: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with your instructor. The notes can include problems encountered, solutions applied, useful commands employed, alternate solutions and methods, and procedure and communication improvements.

____

____

____

____

____

____

____

Trouble Ticket TT-E Debrief—Instructor Notes

TT-E Issue

The authentication for the routing protocol is correctly configured on R2. However, there are issues with the configuration of authentication on R1 and R3. Further, the authentication could have either been removed from R1, R2 and R3, or added on DLS1 and DLS2.

To correct the problem, and have authentication:

On R1, the key "Secure" was typed in lowercase "secure." The key names are case sensitive. Change the configuration on interface Fa0/1 from:

```
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 secure
```

To:

```
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 Secure
```

On R3, the authentication configuration on the S0/0/1 and Fa0/1 interfaces had a typo. Change the AS number for EIGRP from 2 to the AS that the company uses, which is 1:

Change from:

```
ip authentication mode eigrp 2 md5
ip authentication key-chain eigrp 2 Secure
```

To:

```
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 Secure
```

On DLS1 and DLS2, add the following interface configuration commands to Fa0/5 interface:

```
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 Secure
```

Also, create the key on both DLSI and DLS2 using the global configuration commands:

```
key chain Secure
key 1
key-string Updatepa55
```


Section 2 – Troubleshooting Reference Information

General Troubleshooting Process

As a general guideline, you can use the following general troubleshooting process described in the course:

1. Define the problem (symptoms).
2. Gather information.
3. Analyze the information.
4. Propose a hypothesis (possible cause).
5. Test the hypothesis.
6. Eliminate or accept the hypothesis.
7. Solve the problem.
8. Document the problem.

Command Summary

The table lists useful commands for this lab. Sample output is shown on the following pages.

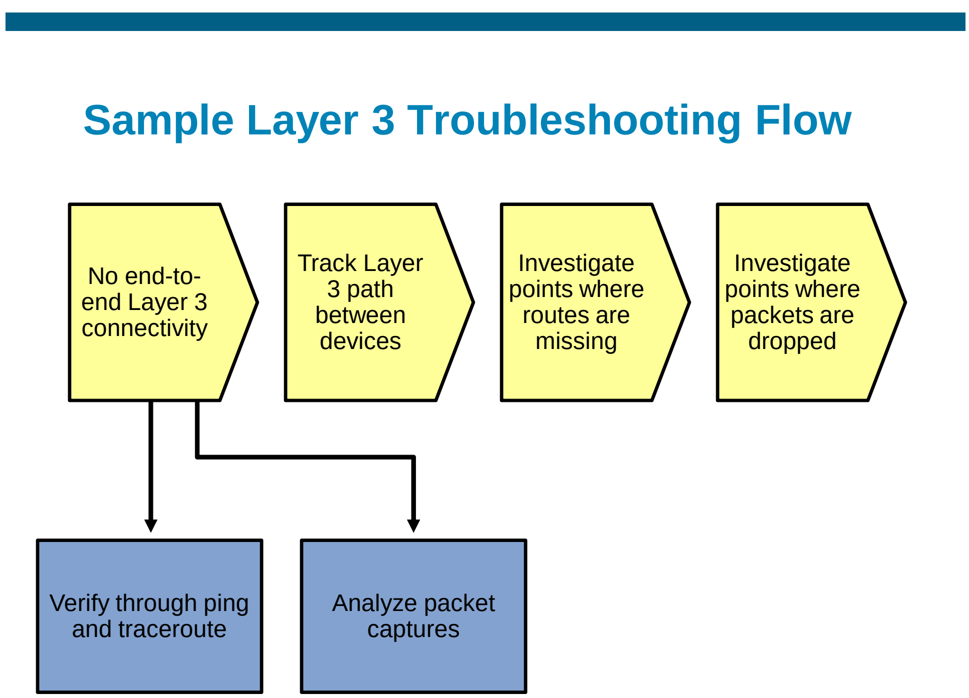
Command	Key Information Displayed
show spanning-tree vlan *vlan#*	Displays all essential parameters that affect the topology, such as the root port, designated ports, port state, and port type, as well as the spanning-tree mode being implemented.
show vlan brief	Displays a quick overview of all existing 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 *ip-addr*	Displays the routing table 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.

Lab 5-1 Sample Troubleshooting Flows

Troubleshooting IP Connectivity

The figure illustrates an example of a method that you could follow to diagnose and resolve problems related to IP connectivity.



Layer 3 is a common starting point for many troubleshooting procedures. An often applied method is the divide-and-conquer approach. When a user reports a problem concerning connectivity to a certain service or application running on a server, a good first step is to determine if there is end-to-end IP connectivity between the client and the server. If this is the case, you can focus on the higher layers of the Open Systems Interconnection (OSI) reference model.

End-to-end IP connectivity can be confirmed or denied by using the **`ping`** or **`traceroute`** commands. Almost every operating system supports these commands in some form, but the syntax might be slightly different for different operating systems.

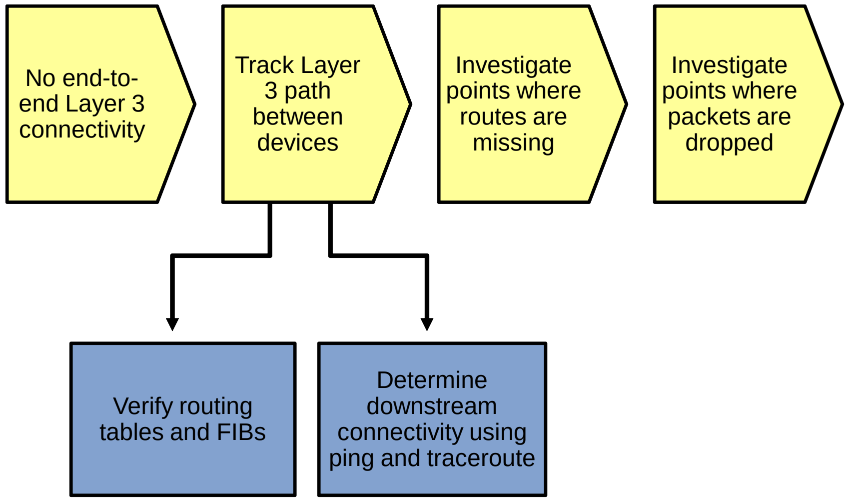
A prerequisite to using this method is that the appropriate Internet Control Message Protocol (ICMP) messages are allowed on the network and not blocked by any firewalls, including host-based firewalls on the destination host. If you cannot use ping and traceroute effectively, you might have to resort to analyzing traffic captures of the actual traffic flows to determine if packets can be sent at the network layer between the affected hosts.

Using the Correct Source Address

```
R2#ping 10.1.50.1 source Lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.50.1, timeout is 2 seconds:
Packet sent with a source address of 10.1.202.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/20/32 ms

R2#traceroute 10.1.50.1 source Lo0

Type escape sequence to abort.
Tracing the route to 10.1.50.1

  1 10.1.1.1 16 msec 16 msec 8 msec
  2 10.1.2.1 8 msec 16 msec 12 msec
  3 10.1.50.1 12 msec 12 msec 8 msec
```

Be aware that a successful ping or traceroute response is dependent on two things: the availability of a route to the destination and a route back to the source. Especially when running tests from the first-hop router in the path, make sure to specify the source address of the ping or traceroute. If you do not specify the source address, the router uses the IP address of the egress interface as the source for the packets. Using an address from a different source subnet than the client might lead you to reach wrong conclusions if the problem concerns the return path for the packets.

Sample Layer 3 Troubleshooting Flow



If you have determined that there is a problem with the end-to-end IP connectivity between the affected hosts, you want to reduce the scope of the problem and isolate the points in the path between the hosts where the connectivity is lost.

A commonly used method is to track the path of the packets. You can use the following method to diagnose end-to-end IP connectivity problems:

Determine the Layer 3 path. Based on documentation, baselines, and knowledge of your network in general, the first step is to determine the path that you would expect packets to follow between the affected hosts. Determining the expected traffic path beforehand helps in two ways. It provides a starting point for gathering information about what is happening on the network, and it makes it easier to spot abnormal behavior. The second step in determining the Layer 3 path is to follow the expected path and verify that the links on the path are up and forwarding traffic. If the actual traffic path is different from your expected path, this step might provide clues about which links or protocols are failing and the cause of these failures.

To track the path of the packets between the hosts, first track the path that is being used according to the control plane information. Start at the client and verify the IP address, subnet mask, and default gateway. Then go to the router that is listed as the default gateway and check which route is used for the destination IP address. Determine the next-hop router based on the information in the routing table. Connect to the next-hop router and repeat this procedure until you arrive at the router that is directly connected to the destination host. Then repeat the process for the route back from the destination to the source.

If the router has no route in the table for the destination network, you must diagnose the process that is the source of the routing information on this router, such as the routing protocol or static routes.

If you have verified that the routing information is present on the complete path from the source to the destination and from the destination back to the source but connectivity is failing, you must track the path again, but now determine at which point packets are being dropped. The likely causes for dropped packets are Layer 1 problems, Layer 2 problems, or Layer 3 to Layer 2 mapping problems. When you have determined the point where the packets are dropped, use the specific troubleshooting methods appropriate for the Layer 2 technology that is used on the egress interface.

These steps do not necessarily have to be taken in the order presented here. Often different aspects of this generic procedure are combined, and shortcuts can be taken based on the result. For instance, determining proper packet forwarding is often done in parallel with determining the routes by using ping to verify the reachability of the next-hop derived from the route or using ping and traceroute to the final destination from intermediate routers in the path.

If you find that a ping is successful from a particular point in the path, you know that routes to the destination must be available on all the downstream routers. You can then use traceroute to determine the path to the destination, instead of connecting to each router in the path. However, this method has a hidden assumption: Packets traveling to the same destination use the same path, regardless of their source. This is not necessarily the case in a redundant network with equal-cost paths to a certain destination. The source address is typically used as part of the load-balancing algorithm that determines the path used when equal-cost paths are available. It is important to determine the exact path for the actual source and destination IP address pair that is affected, especially in cases where control plane information is available in both directions but packets are dropped.

Verify the Routing Table

```
R2#show ip route 10.1.10.1
Routing entry for 10.1.10.0/24
  Known via "eigrp 1", distance 90, metric 2172672, type internal
  Redistributing via eigrp 1
  Last update from 10.1.1.5 on Serial0/0/1, 02:05:21 ago
  Routing Descriptor Blocks:
    10.1.1.5, from 10.1.1.5, 02:05:21 ago, via Serial0/0/1
      Route metric is 2172672, traffic share count is 1
      Total delay is 20110 microseconds, minimum bandwidth is 1544 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 2
  * 10.1.1.1, from 10.1.1.1, 02:05:21 ago, via Serial0/0/0
      Route metric is 2172672, traffic share count is 1
      Total delay is 20110 microseconds, minimum bandwidth is 1544 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 2
```

When you are troubleshooting IP connectivity to a specific destination IP address, you can use the **show ip route *ip-address*** command to determine the best prefix match for the IP address, the egress interface, and, for multipoint interfaces, the next-hop IP address. If multiple equal-cost paths are present, as can be seen in the example above, each entry is listed.

The routing source is also listed, such as directly connected, static, or the routing protocol. Additional control plane parameters that are associated with the route source, such as the administrative distance, routing protocol metrics, source router, and route age, are also displayed. To interpret these parameters, more detailed knowledge of the specific routing protocol is required. More detailed information can often be gathered from that specific protocol's data structures.

This command never displays the default route 0.0.0.0/0 as a match, even if it is the longest prefix match for a packet. Therefore, if this command displays the message "% Network not in table," you cannot conclude that packets will be dropped, so you need to verify if a default route is present by using the **show ip route 0.0.0.0 0.0.0.0** command.

Verify the Cisco Express Forwarding Information Base

```
R2#show ip cef 10.1.10.1
10.1.10.0/24
  nexthop 10.1.1.1 Serial0/0/0
  nexthop 10.1.1.5 Serial0/0/1
```

To see the best match for a specific IP address in the Forwarding Information Base (FIB), use the **show ip cef *ip-address*** command. This command lists the same forwarding information as the **show ip route** command but without the associated control plane information, such as routing protocol metrics, administrative distance, and so on. This command displays the default route 0.0.0.0/0 if it is the best match for the destination IP address. If the routing table for a route contains multiple entries, these same entries will also be present in the FIB.


```
DLS1#show ip cef exact-route 10.1.10.1 10.1.202.1
10.1.10.1 -> 10.1.202.1 => IP adj out of FastEthernet0/5, addr 10.1.2.2

R2#show ip cef exact-route 10.1.202.1 10.1.50.1
10.1.202.1 -> 10.1.50.1 => IP adj out of Serial0/0/0
```

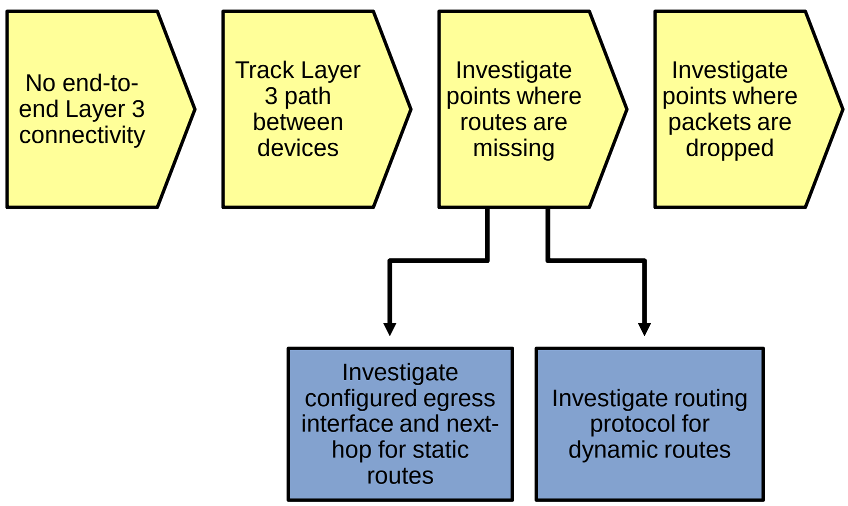
When you are tracing the packet flow between two specific hosts and the routing table and the FIB lists multiple entries (because there are multiple equal-cost paths), you must determine which entry is used to forward the packets associated with the specific source and destination IP address pair that you are troubleshooting. You can use the **show ip cef exact-route** command in these situations to determine the specific egress interface and next-hop IP address for the specific IP address pair.

On multilayer switches, instead of consulting the FIB that is stored in the main memory of the switch, you must consult the forwarding information stored in the hardware ternary content addressable memory (TCAM), because packet forwarding is handled by the TCAM, not the Cisco Express Forwarding FIB.

Although the FIB is used to compile the information that is loaded into the TCAM, the load-balancing algorithms that are used are different and do not necessarily yield the same result.

To learn more about the commands that can be used to verify the Layer 3 forwarding information contained in the TCAM, see the multilayer switching sections of the TSHOOT Student Guide and this Lab Guide.

Sample Layer 3 Troubleshooting Flow



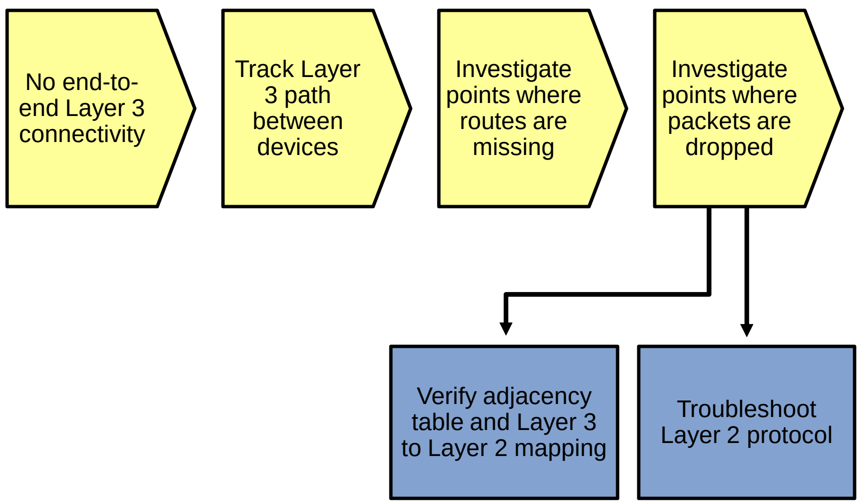
After you have found a point in the network where no route is present in the routing table for the destination IP address (or when analyzing the return path for the source IP address) of the session, you need to investigate what caused that route not to be installed in the routing table.

To correctly diagnose why a particular route is missing from the routing table, you first need to consult your documentation and baselines to find out what is the expected routing source. Is static routing or a routing protocol used on this router?

If a static route has been configured but it is not listed in the routing table, verify the status of the associated egress interface. If the egress interface for a static route is down, the route will not be installed in the routing table. If the route is not configured with an egress interface but with a next-hop IP address, the same rule applies. The router executes a recursive routing table lookup on the next hop for the static route. If no matching route and associated egress interface can be found for the configured next-hop IP address of the static route, the route is not installed in the routing table. If a match is found for the next-hop IP address, the static route is installed.

For dynamic routing protocols, you must initiate a troubleshooting process that is appropriate for that specific protocol and try to determine why the route was not learned on this router or, if it was learned, why it is not used.

Sample Layer 3 Troubleshooting Flow



If you have verified the presence of correct routing information along the paths in both directions but you find that packets are dropped at a certain hop in the path, you must diagnose the packet-forwarding process.

If a route is present in the routing table (and the FIB if Cisco Express Forwarding is used) but packets are not forwarded correctly, verify if a correct mapping between the IP next hop and the Layer 2 protocol is used on the egress interface. If the router cannot find all the necessary Layer 2 information to construct a frame to encapsulate a packet, it is dropped, even if the routing information is present in the routing table.

The exact command to verify the Layer 3-to-Layer 2 protocol mapping is dependent on the Layer 2 technology used on the egress interface. Examples are the **show ip arp** command for Ethernet networks and the **show frame-relay map** command for Frame Relay.

For more information about the exact command syntax, research the Layer 2 technology used in the configuration guides and command references on http://www.cisco.com.

If you find incorrect mappings, or if you find the mappings to be correct but frames are not forwarded correctly, initiate a Layer 2 troubleshooting procedure for the Layer 2 technology that is being used.

Verify the Adjacency Table

```
DLS1#show adjacency fa0/5 detail
Protocol Interface                 Address
IP       FastEthernet0/5           10.1.2.2(15)
                                   0 packets, 0 bytes
                                   epoch 0
                                   sourced in sev-epoch 0
                                   Encap length 14
                                   001B530D60B100175A5BB4420800
                                   L2 destination address byte offset 0
```



```
L2 destination address byte length 6
Link-type after encap: ip
ARP
```

Regardless of the Layer 2 technology, if Cisco Express Forwarding is used as the Layer 3 forwarding method, you can verify the availability of Layer 2 forwarding information using the **`show adjacency`** *`int-type/#`* **`detail`** command.

As can be seen in the example above, this command lists the Layer 2 frame header that is used to encapsulate packets transmitted via the listed adjacency. In this example, the frame header is 001B530D60B100175A5BB4420800, which is dissected as follows:

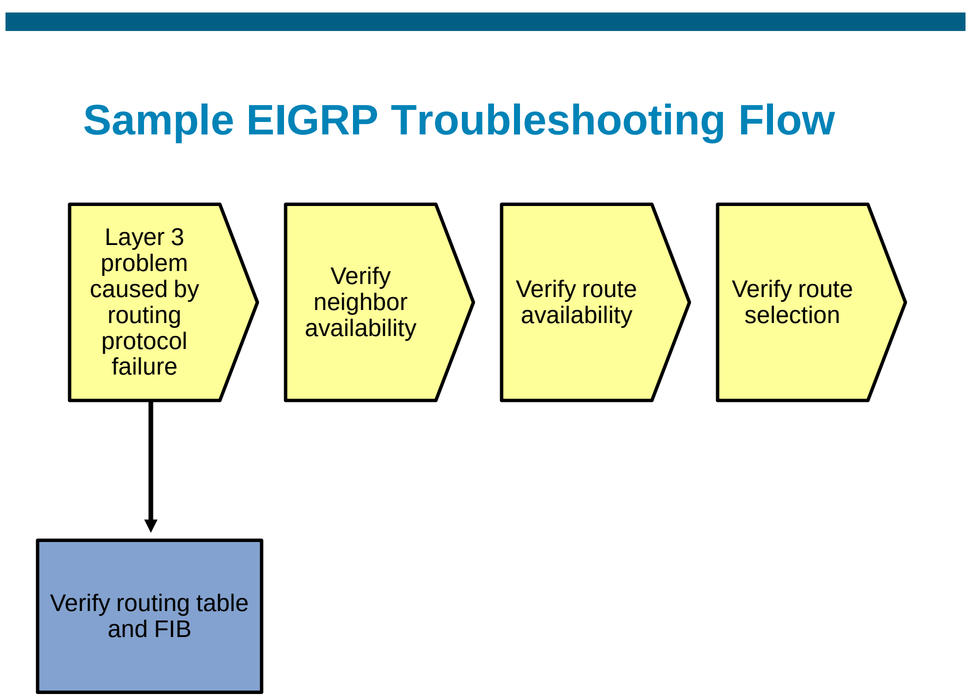
- **001B530D60B1** – This is the destination MAC address of the frame, which corresponds to the MAC address of the next hop 10.1.2.2.
- **00175A5BB442** – This is the source MAC address of the frame, which corresponds to the MAC address of interface FastEthernet 0/5.
- **0800** – This is the Ethernet type field, which indicates that the frame contains an IP packet, because Ethernet type value 0x800 is registered as the value for IP.

If you are troubleshooting a Layer 3 forwarding problem and the IP next hop and interface listed in the routing table are not present in the adjacency table, there is a problem with the Layer 3-to-Layer 2 mapping mechanisms.

If a Layer 2 frame header is listed in the adjacency table but the frames are not forwarded correctly across the Layer 2 medium, you must troubleshoot the underlying Layer 2 technology. The information contained in the header can be useful information when you start the Layer 2 troubleshooting process.

Troubleshooting EIGRP

The figure illustrates a method for diagnosing and resolving problems related to EIGRP.



The usual trigger to start investigating routing protocol operation is when you are troubleshooting IP connectivity to a particular destination and you find that the route to the destination network is missing from the routing table of one of the routers or that a different route than expected was selected to forward the packets to that destination.

To install a route into the routing table, each router that uses a routing protocol goes through several stages:

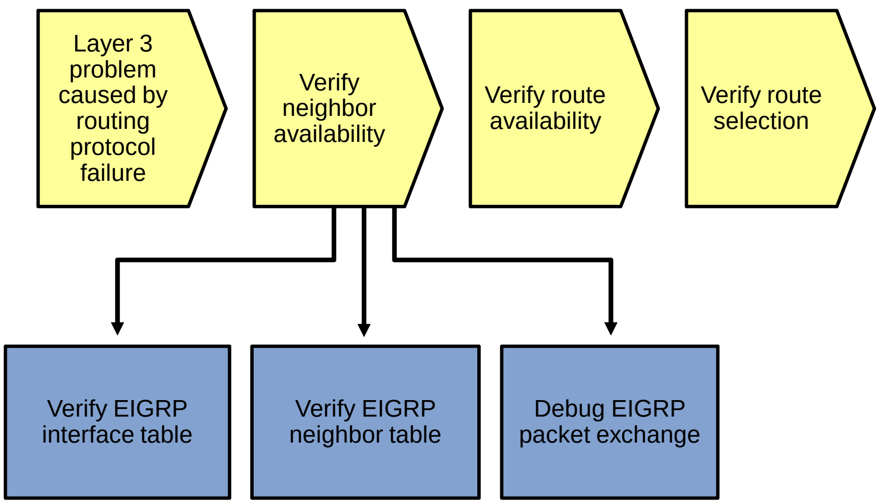
- Discover neighbors and establish a neighbor relationship.
- Exchange routing information with neighbors and store the received information in protocol specific data structures.
- Select the best route from the available routes and install it in the routing table.

Errors during any of these stages can cause routing information to be missing or incorrect routing information to be installed in the routing table.

The exact processes that take place, the data structures that are used, and the commands to gather information about these processes and data structures are protocol-specific, but the generic troubleshooting principles are similar for all routing protocols.

The order to perform the different stages is not important as long as a structured approach is used.

Sample EIGRP Troubleshooting Flow



EIGRP discovers and maintains neighbor relationships by using hello packets. Neighbors that are discovered are registered in the EIGRP neighbor table and remain in the neighbor table as long as hello packets are received. A neighbor is removed from the table when its hold time expires or when the interface on which the neighbor is registered goes down. The default EIGRP hello timer is 5 seconds for these interfaces:

- High-speed multipoint interfaces, such as Ethernet interfaces
- Point-to-point interfaces, such as the following:
  - Serial interfaces running PPP or High-Level Data Link Control (HDLC)
  - Point-to-point Frame Relay subinterfaces
  - Point-to-point ATM subinterfaces

The default hold time for these interfaces is 15 seconds. Each router advertises hello and hold timers that it uses in its hellos. Although it is recommended that the timers are changed in a consistent manner on all routers if they need to be tuned, they do not need to match between two routers to allow them to become neighbors.

Verify the EIGRP Interfaces

```
R1#show ip eigrp interfaces
IP-EIGRP interfaces for process 1

                        Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface        Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Se0/0/0            1        0/0        19       0/15          99           0
Fa0/1              1        0/0         8       0/1           50           0
```

Neighbors can only be discovered on an interface that is operational and has been activated for EIGRP processing. An interface is activated for EIGRP packet processing if the IP address of the interface is covered by one of the network statements in the **router eigrp** configuration and the interface is not configured as a passive interface. Use the **show ip eigrp interfaces** command to display the EIGRP interfaces. An interface does not need to be operational to be listed in the output. The operational status of the interface must be verified separately using the **show interfaces**, **show interface status,** or **show ip interfaces brief** command.

If an interface is not listed in the output of the **show ip eigrp interfaces** command as expected, verify the **network** and **passive-interface** commands under the **router eigrp** configuration.

Verify the EIGRP Neighbor Table

```
R1#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   10.1.2.1                Fa0/1             13 04:50:36    8   200  0  12
1   10.1.1.2                Se0/0/0           10 04:07:52   19   200  0  36
```

To verify that all expected neighbor relationships are operational, display the EIGRP neighbor table using the **show ip eigrp neighbors** command.

For troubleshooting purposes, the two most relevant columns in this output are Hold, which lists the number of seconds before a neighbor expires from the table, and Uptime, which lists how long this neighbor has been operational since it was last discovered. These two items can give you a good indication of the stability of the neighbor relationship. The uptime tells you for how long the neighbor relationship has been successfully maintained, while displaying the hold time several times in a row can tell you if hellos are being received in a timely fashion. Based on the default 5 second hello and 15 second hold time, the value in this column should be between 15 and 10 seconds, because it counts down and is reset to the hold time whenever a hello is received from the neighbor.

If the uptime of a neighbor is shorter than expected, verify the console or syslog logs for interface-related events or EIGRP neighbor-related events, such as the following (these are default message – not the result of debug):

```
Nov 2 06:25:01 EST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to down
Nov 2 06:25:02 EST: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to
down
Nov 2 06:25:02 EST: %DUAL-5-NBRCHANGE: EIGRP-IPv4:(1) 1: Neighbor 10.1.2.1
(FastEthernet0/1) is down: interface down
Nov 2 06:25:14 EST: %DUAL-5-NBRCHANGE: EIGRP-IPv4:(1) 1: Neighbor 10.1.2.1
(FastEthernet0/1) is up: new adjacency
Nov 2 06:25:16 EST: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
Nov 2 06:25:17 EST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up
```


Specifically, the %DUAL-5-NBRCHANGE messages are very useful in troubleshooting because they indicate why the neighbor was lost. In this case, it was caused by the interface going down.

Debug EIGRP Packet Exchange

If an expected neighbor is not listed in the neighbor table on a specific interface, and you have confirmed that the interface is operational and is listed in the interface table, use the **`debug eigrp packets`** command to display the transmission and reception of EIGRP packets in real time. This command can potentially generate a large amount of output, so be cautious about using it.

You can limit the output by specifying the packet type (update, request, query, reply, hello, ipxsap, probe, ack, stub, siaquery, or siareply). You can also add other conditions using the **`debug ip eigrp`** ***`as-number`*** command, such as limiting the output to a specific neighbor or network.

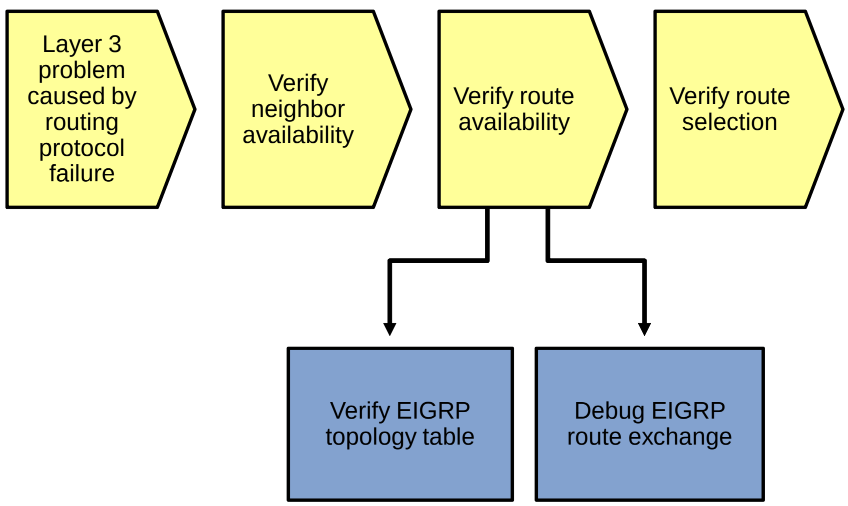
To further reduce the impact of the command, disable logging to the console and log to buffers in the router instead. You can then display the contents of the log buffer using the **`show logging`** command. The following example shows you how to use this technique:

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#no logging console
R1(config)#logging buffered 16384
R1(config)#^Z

R1#debug eigrp packets
EIGRP Packets debugging is on
    (UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY,
SIAREPLY)

R1#debug ip eigrp 1 neighbor 10.1.2.1
IP Neighbor target enabled on AS 1 for 10.1.2.1
IP-EIGRP Neighbor Target Events debugging is on

R1#clear logging
Clear logging buffer [confirm]

R1#show logging
Syslog logging: enabled (1 messages dropped, 108 messages rate-limited,
                0 flushes, 0 overruns, xml disabled, filtering disabled)
    Console logging: disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging: level debugging, 13924 messages logged, xml disabled,
                    filtering disabled
    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled

No active filter modules.

    Trap logging: level informational, 242 message lines logged
        Logging to 10.1.50.1(global) (udp port 514, audit disabled,  link up), 242
message lines logged, xml disabled,
               filtering disabled

Log Buffer (16384 bytes):

Nov 2 07:40:38.177 PDT: EIGRP: Received HELLO on FastEthernet0/1 nbr 10.1.2.1
```



```
Nov 2 07:40:38.177 PDT:   AS 1, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0 peerQ
un/rely 0/0
Nov 2 07:40:42.517 PDT: EIGRP: Received HELLO on FastEthernet0/1 nbr 10.1.2.1
Nov 2 07:40:42.517 PDT:   AS 1, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0 peerQ
un/rely 0/0
Nov 2 07:40:47.237 PDT: EIGRP: Received HELLO on FastEthernet0/1 nbr 10.1.2.1
Nov 2 07:40:47.237 PDT:   AS 1, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0 peerQ
un/rely 0/0
```

Sample EIGRP Troubleshooting Flow



After you have verified that neighbor relationships have been established as expected, verify that the route for the destination network that you are troubleshooting has been received correctly from all appropriate neighbors. EIGRP stores all routes that it receives from its neighbors in its topology table and then selects the best route from these routes to be installed in the routing table.

By investigating the available routes to the destination network in the topology table, you can see if all options that you expected were learned and if they have the correct associated metrics.

If routes are missing from the topology table, you might need to debug the EIGRP route exchange process to see if they were not received or if they were not entered into the topology table.

Verify the EIGRP Topology Table

```
R2#show ip eigrp topology 10.1.50.0 255.255.255.0
IP-EIGRP (AS 1): Topology entry for 10.1.50.0/24
  State is Passive, Query origin flag is 1, 2 Successor(s), FD is 2172672
  Routing Descriptor Blocks:
  10.1.1.1 (Serial0/0/0), from 10.1.1.1, Send flag is 0x0
      Composite metric is (2172672/28416), Route is Internal
      Vector metric:
        Minimum bandwidth is 1544 Kbit
        Total delay is 20110 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
```

```
        Hop count is 2
  10.1.1.5 (Serial0/0/1), from 10.1.1.5, Send flag is 0x0
      Composite metric is (2172672/28416), Route is Internal
      Vector metric:
        Minimum bandwidth is 1544 Kbit
        Total delay is 20110 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 2
```

The EIGRP topology table contains all routes that were received from all neighbors.

For each particular prefix, there might be the following three types of entries:

- **Successors** – These are the entries selected from the topology table as the best routes and installed in the routing table. For a router to be a successor, it must provide the lowest total metric (its advertised distance plus the metric of the link towards it) among all the routes in the topology table for that prefix. Also, the advertised distance to the prefix by that router must be strictly lower than the feasible distance (FD). Secondly, it will only be marked as a successor if it was actually installed in the routing table. If a competing route for that prefix, such as a static route, was installed in the routing table instead because it had a better administrative distance, the EIGRP route will not be marked as a successor.
- **Feasible successors** – These routers have a metric that is higher than the current lowest total metric for the prefix but still meet the feasibility condition. The feasibility condition is met if the advertised distance of the route is lower than the FD. This means that the route is considered a backup route and can be used immediately if the best route is lost, without needing to confirm its feasibility as a backup route through a query and reply process.
- **Possible successors** – These routers do not meet the feasibility condition. They are potential backup routes, but if the best route is lost, a query and reply process is necessary to confirm that they are valid and loop-free.

As an example, the content of the EIGRP topology table for network 10.1.50.0/24 is listed below and comments are interspersed with the output to help interpret the entries.

```
R2#show ip eigrp topology 10.1.50.0 255.255.255.0
IP-EIGRP (AS 1): Topology entry for 10.1.50.0/24
  State is Passive, Query origin flag is 1, 2 Successor(s), FD is 2172672
```

There are two successors for this prefix, and the FD is 2172672. This entry is the first successor, because its distance of 2172672 (the first number between the parentheses) towards the 10.1.50.0/24 network through 10.1.1.5 is also equal to the FD of 2172672.

```
Routing Descriptor Blocks:
  10.1.1.1 (Serial0/0/0), from 10.1.1.1, Send flag is 0x0
      Composite metric is (2172672/28416), Route is Internal
      Vector metric:
              Minimum bandwidth is 1544 Kbit
              Total delay is 20110 microseconds
              Reliability is 255/255
              Load is 1/255
              Minimum MTU is 1500
              Hop count is 2
```

This entry is the second successor, because its distance of 28416 is also equal to the FD of 28416.

```
10.1.1.5 (Serial0/0/0), from 10.1.1.5, Send flag is 0x0
      Composite metric is (2172672/28416), Route is Internal
      Vector metric:
            Minimum bandwidth is 1544 Kbit
```



```
                  Total delay is 20110 microseconds
                  Reliability is 255/255
                  Load is 1/255
                  Minimum MTU is 1500
                  Hop count is 2
```

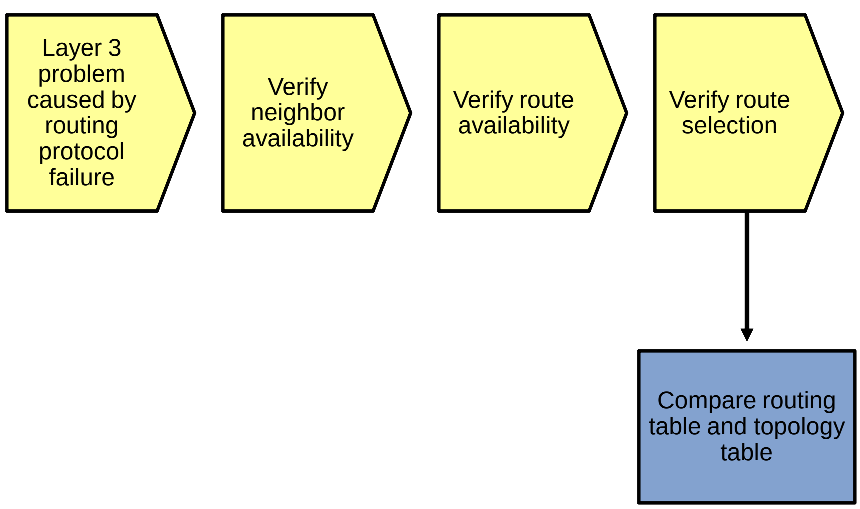
Verify the EIGRP Topology Table

```
R2#debug ip eigrp
IP-EIGRP Route Events debugging is on

R2#debug ip eigrp 1 neighbor 10.1.1.1
IP Neighbor target enabled on AS 1 for 10.1.1.1
IP-EIGRP Neighbor Target Events debugging is on

R2#clear ip eigrp neighbors 10.1.1.1
R2#
Nov  2 17:18:50.945: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.1.1.2 (Serial
0/0/0) is down: Interface Goodbye received
Nov  2 17:18:55.085: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.1.1.2 (Serial
0/0/0) is up: new adjacency
```

If you find expected route entries to be missing from the topology table, consider using the **debug ip eigrp** command to display the processing of routing events by the router. However, this command can produce a large number of messages and, as a result, has a high risk of disrupting the router's operation. Do not use this command unless guided by the Cisco TAC or in a nonoperational network, such as a lab network that you have built to reproduce a problem.

Like the **debug eigrp packets** command, you can limit the impact of this command by logging to buffers instead of the console and by limiting the output to specific neighbors or routes. Even then, extreme care should be taken.

Sample EIGRP Troubleshooting Flow



If you find that an EIGRP route for a specific destination network is available in the topology table, but a different route is present in the routing table, compare the value of the administrative distance of the route in the routing table to the value of the EIGRP route (which is 90 for internal routes and 170 for external routes, by default). If the distance of the EIGRP route is higher than the distance of the competing route, it will not be installed in the routing table.

Reflection Questions

1. Which lab trouble tickets did you have the most difficulty with?

2. For any of the trouble tickets, would you change anything about the process that you used now that you see the resolution of the problem?

3. Which commands did you find most useful in diagnosing Layer 3 and EIGRP issues? Add these to your toolbox for future use. Which commands did you find least useful?

References

If you need more information on the commands and their options, see the following references:

- IP Routing Protocol Command Reference

  http://www.cisco.com/cisco/web/support/index.html

- Cisco IOS IP Switching Command Reference

  http://www.cisco.com/en/US/docs/ios/ipswitch/command/reference/isw_book.html

- Enhanced Interior Gateway Routing Protocol Troubleshooting Tech Notes
  http://www.cisco.com/en/US/tech/tk365/tsd_technology_support_troubleshooting_technotes_list.html#anchor3

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1700	Fast Ethernet 0 (FA0)	Fast Ethernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
1800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2600	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)
2800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. Rather than try to list all the combinations of configurations for each router class, this table includes identifiers for the possible combinations of Ethernet and serial interfaces in the device. The table does not include any other type of interface, even though a specific router might contain one. An example of this is an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

Device Configurations (Instructor version)

Note: All device configurations are provided for TT-A, including those that are the same as the baseline as defined in Lab 3-1. The configs provided here are *not* running-config outputs. They can be used for cut-and-paste for TT-A and subsequent tickets. Where a config is noted as being the same as a previous one, the only change is in the MOTD, which identifies the Lab and TT. The errors in the configuration are commented and highlighted as red text.

Trouble Ticket—TT-A Configurations

Switch ALS1

```
!Lab 5-1 Switch ALS1 TT-A Config
```



```
!
hostname ALS1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 5-1 Switch ALS1 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet

spanning-tree mode rapid-pvst
spanning-tree portfast default
!
interface Vlan1
 no ip address
 shutdown
!
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 100
```



```
 name MGMT
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel1
 description Channel to DLS1
 no shutdown
 !
interface Port-channel2
 description Channel to DLS2
 no shutdown
!
interface FastEthernet0/1
 description Channel to DLS1
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shutdown
!
interface FastEthernet0/2
 description Channel to DLS1
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shutdown
!
interface FastEthernet0/3
 description Channel to DLS2
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shutdown
!
interface FastEthernet0/4
 description Channel to DLS2
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shutdown
!
interface FastEthernet0/5
 description Unused
 switchport access vlan 999
```



```
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown

interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
```

```
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description To PC-B
 switchport access vlan 10
 switchport mode access
 switchport voice vlan 20
 spanning-tree portfast
 switchport port-security
 switchport port-security maximum 2
 switchport port-security violation shutdown
 switchport port-security mac-address sticky
 no shut
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
```



```
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan100
 ip address 10.1.100.1 255.255.255.0
 no shutdown
!
ip default-gateway 10.1.100.254
!
ip http server
ip http secure-server
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server host 10.1.50.1 version 2c cisco
```



```
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps vlan-membership
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
  no transport input
!
ntp source Vlan100
ntp server 10.1.202.1
end
```

Switch DLS1

```
!Lab 5-1 Switch DLS1 TT-A Config
!
hostname DLS1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55

banner motd $*** Lab 5-1 Switch DLS1 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
!
ip domain name tshoot.net
!
ip dhcp excluded-address 10.1.10.252 10.1.10.254
ip dhcp excluded-address 10.1.20.252 10.1.20.254
```



```
ip dhcp excluded-address 10.1.30.252 10.1.30.254
!
ip dhcp pool OFFICE
   network 10.1.10.0 255.255.255.0
   default-router 10.1.10.254
   domain-name tshoot.net
!
ip dhcp pool VOICE
   network 10.1.20.0 255.255.255.0
   default-router 10.1.20.254
   domain-name tshoot.net
!
ip dhcp pool GUEST
   network 10.1.30.0 255.255.255.0
   default-router 10.1.30.254
   domain-name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog contenttype plaintext
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 24576
spanning-tree vlan 20,50 priority 28672
!
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 70
 name CCTV
!
vlan 100
 name MGMT
!
vlan 900
 name NATIVE
!
vlan 999
```

```
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel1
 description Channel to ALS1
 no shut
!
interface Port-channel10
 description Channel to DLS2
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100

switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R1
 no switchport
 ip address 10.1.2.1 255.255.255.252
```

Error: VLAN 70 is not allowed on trunk for Fa0/3 and Fa0/4. Add it for both interfaces.

switchport trunk allowed vlan add 70


```
 speed 100
 duplex full
 spanning-tree bpduguard enable
 no shut
!
interface FastEthernet0/6
 description FE to SRV1
 switchport access vlan 50
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shut
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
```



```
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
```



```
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 10.1.10.252 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 priority 110
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.252 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.252 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 priority 110
 standby 30 preempt
!
```

```
interface Vlan50
 ip address 10.1.50.252 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 preempt
!
interface Vlan70
 ip address 10.1.70.252 255.255.255.0
 standby 70 ip 10.1.70.254
 standby 70 preempt
!
interface Vlan100
 ip address 10.1.100.252 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 priority 110
 standby 100 preempt
!
router eigrp 1
 passive-interface default
 no passive-interface Fa0/5
 no auto-summary
 network 10.1.0.0 0.0.255.255
!
ip classless
ip http server
ip http secure-server
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO

snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server host 10.1.50.1 version 2c cisco
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 10.1.202.1
```



```
end
```

Switch DLS2

```
!Lab 5-1 Switch DLS2 TT-A Config
!
hostname DLS2
!
service timestamps debug datetime msec
service timestamps log datetime
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 5-1 Switch DLS2 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500

vtp domain TSHOOT
vtp mode transparent

ip subnet-zero
ip routing
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog contenttype plaintext
  hidekeys
  path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 28672
spanning-tree vlan 20,50 priority 24576

vlan 10
 name OFFICE
!
vlan 20
```



```
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 70
 name CCTV
!
vlan 100
 name MGMT
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel2
 description Channel to ALS1
 no shut
!
interface Port-channel10
 description Channel to DLS1
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,70,100
 switchport mode trunk
 switchport nonegotiate
```



```
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,70,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R3
 no switchport
 ip address 10.1.2.13 255.255.255.252
 speed 100
 duplex full
 spanning-tree bpduguard enable
 no shut
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
```



```
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description FE to PC-C
 switchport access vlan 70
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/19
 description Unused
```



```
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
```



```
interface Vlan10
 ip address 10.1.10.253 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.253 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 priority 110
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.253 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.253 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 priority 110
 standby 50 preempt
!
interface Vlan70
 ip address 10.70.1.253 255.255.255.0
 standby 70 ip 10.1.70.254
 standby 70 priority 110
 standby 70 preempt
!
interface Vlan100
 ip address 10.1.100.253 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 preempt
!
router eigrp 1
 passive-interface default
 no passive-interface Fa0/5
 no auto-summary
 network 10.1.0.0 0.0.255.255
!
ip classless
ip http server
ip http secure-server
!
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps hsrp
```

Error: Interface VLAN 70 address is not on 10.1.0.0/16 network.

```
interface VLAN 70
 ip address 10.1.70.253 255.255.255.0
```

```
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 10.1.202.1
end
```

Router R1

```
!Lab 5-1 Router R1 TT-A Config
!
hostname R1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 5-1 Router R1 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
```



```
!
interface Loopback0
 ip address 10.1.201.1 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown
!
interface FastEthernet0/1
 description FE to DLS1
 ip address 10.1.2.2 255.255.255.252
 ip flow ingress
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
 description WAN link to R2 - 128k leased line
 ip address 10.1.1.1 255.255.255.252
 ip flow ingress
 encapsulation ppp
 clock rate 128000
  no shutdown
!
interface Serial0/0/1
 description WAN link to R3 (not used)
 no ip address
 shutdown
!
router eigrp 1
 passive-interface default
 no passive-interface FastEthernet0/1
 no passive-interface Serial0/0/0
 network 10.1.1.0 0.0.0.3
 network 10.1.2.0 0.0.0.3
 network 10.1.201.1 0.0.0.0
 no auto-summary
!
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
logging source-interface Loopback0
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
```



```
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 10.1.202.1
end
```

Router R2

```
!Lab 5-1 Router R2 TT-A Config
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
Hostname R2
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 5-1 Router R2 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
```



```
 ip address 10.1.202.1 255.255.255.255
!
interface FastEthernet0/0
 shutdown
!
interface FastEthernet0/1
 shutdown
!
interface Serial0/0/0
 description WAN link to R1 - 128k leased line
 ip address 10.1.1.2 255.255.255.252
 encapsulation ppp
 no shutdown
 !
interface Serial0/0/1
 description WAN link to R3 - 128k leased line
 ip address 10.1.1.6 255.255.255.252
 clock rate 128000
 encapsulation ppp
 no shutdown
!
router eigrp 1
 passive-interface default
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
 network 10.1.1.0 0.0.0.3
 network 10.1.1.4 0.0.0.3
 no auto-summary
!
ip http server
no ip http secure-server
!
logging source-interface Loopback0
logging 10.1.50.1
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
!
ntp master 3
end
```

Error: Lo0 network 10.1.202.1 is not advertised under EIGRP.

```
router eigrp 1
 network 10.1.202.1 0.0.0.0
```


Router R3

```
!Lab 5-1 Router R3 TT-A Config
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 5-1 Router R3 TT-A Config ***$
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
no ip domain lookup
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 10.1.203.1 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown

interface FastEthernet0/1
 description FE to DLS2
 ip address 10.1.2.14 255.255.255.252
 ip flow ingress
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
 description WAN link to R1 - (Not used)
```



```
 no ip address
 clock rate 128000
 encapsulation ppp
 shutdown
!
interface Serial0/0/1
 description WAN link to R2 - 128k leased line
 ip address 10.1.1.5 255.255.255.252
 ip flow ingress
 encapsulation ppp
 no shutdown
!
router eigrp 1
 passive-interface default
 no passive-interface FastEthernet0/1
 no passive-interface Serial0/0/1
 network 10.1.1.4 0.0.0.3
 network 10.1.2.12 0.0.0.3
 network 10.1.203.1 0.0.0.0
 no auto-summary
!
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
logging source-interface Loopback0
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 10.1.202.1
end
```


Trouble Ticket—TT-B Configurations

Switch ALS1 - Same as TT-A

Switch DLS1

```
!Lab 5-1 Switch DLS1 TT-B Config
!
hostname DLS1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55

banner motd $*** Lab 5-1 Switch DLS1 TT-B Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
!
ip domain name tshoot.net
!
ip dhcp excluded-address 10.1.10.252 10.1.10.254
ip dhcp excluded-address 10.1.20.252 10.1.20.254
ip dhcp excluded-address 10.1.30.252 10.1.30.254
!
ip dhcp pool OFFICE
   network 10.1.10.0 255.255.255.0
   default-router 10.1.10.254
   domain-name tshoot.net
!
ip dhcp pool VOICE
   network 10.1.20.0 255.255.255.0
   default-router 10.1.20.254
   domain-name tshoot.net
!
ip dhcp pool GUEST
   network 10.1.30.0 255.255.255.0
   default-router 10.1.30.254
   domain-name tshoot.net
```

```
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 24576
spanning-tree vlan 20,50 priority 28672
!
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 100
 name MGMT
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel1
 description Channel to ALS1
 no shut
!
interface Port-channel10
 description Channel to DLS2
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
```



```
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R1
 no switchport
 ip address 10.1.2.1 255.255.255.252
 speed 100
 duplex full
 spanning-tree bpduguard enable
 no shut
!
interface FastEthernet0/6
 description FE to SRV1
 switchport access vlan 50
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shut
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
```



```
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
```

```
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
```



```
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown

interface Vlan10
 ip address 10.1.10.252 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 priority 110
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.252 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.252 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 priority 110
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.252 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 preempt
!
interface Vlan100
 ip address 10.1.100.252 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 priority 110
 standby 100 preempt
!
router eigrp 1
 passive-interface default
 no passive-interface Fa0/5
 no auto-summary
 network 10.1.0.0 0.0.255.255
!
ip classless
ip http server
ip http secure-server
```



```
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server host 10.1.50.1 version 2c cisco
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 10.1.202.1
end
```

Switch DLS2

```
!Lab 5-1 Switch DLS2 TT-B Config
!
hostname DLS2
!
service timestamps debug datetime msec
service timestamps log datetime
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 5-1 Switch DLS2 TT-B Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
```



```
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
  path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 28672
spanning-tree vlan 20,50 priority 24576

vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 100
 name MGMT
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel2
 description Channel to ALS1
 no shut

interface Port-channel10
 description Channel to DLS1
```



```
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R3
 no switchport
 ip address 10.1.2.13 255.255.255.252
 speed 100
 duplex full
 spanning-tree bpduguard enable
 no shut
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
```



```
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
```



```
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description FE to PC-C
 switchport access vlan 30
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
```



```
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 10.1.10.253 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.253 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 priority 110
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.253 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.253 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 priority 110
 standby 50 preempt
!
interface Vlan100
 ip address 10.1.100.253 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 preempt
!
!
router eigrp 1
```

```
 passive-interface default
 no passive-interface Fa0/5
 no auto-summary
 network 10.1.0.0 0.0.255.255
!
ip classless
ip http server
ip http secure-server
!
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 10.1.202.1
end
```

Router R1

Note: This is actually the configuration for R3.

```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
```



```
!
banner motd $*** Lab 5-1 Router R1 TT-B Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 10.1.203.1 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown

interface FastEthernet0/1
 description FE to DLS2
 ip address 10.1.2.14 255.255.255.252
 ip flow ingress
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
 description WAN link to R1 - (Not used)
 no ip address
 clock rate 128000
 encapsulation ppp
 shutdown
!
interface Serial0/0/1
 description WAN link to R2 - 128k leased line
 ip address 10.1.1.5 255.255.255.252
 ip flow ingress
 encapsulation ppp
 no shutdown
!
router eigrp 1
 passive-interface default
```



```
 no passive-interface FastEthernet0/1
 no passive-interface Serial0/0/1
 network 10.1.1.4 0.0.0.3
 network 10.1.2.12 0.0.0.3
 network 10.1.203.1 0.0.0.0
 no auto-summary
!
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
logging source-interface Loopback0
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 10.1.202.1
end
```

Router R2

```
!Lab 5-1 Router R2 TT-B Config
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
Hostname R2
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 5-1 Router R2 TT-B Config ***$
```



```
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 10.1.202.1 255.255.255.255
!
interface FastEthernet0/0
 shutdown
!
interface FastEthernet0/1
 shutdown
!
interface Serial0/0/0
 description WAN link to R1 - 128k leased line
 ip address 10.1.1.2 255.255.255.252
 encapsulation ppp
 no shutdown
!
interface Serial0/0/1
 description WAN link to R3 - 128k leased line
 ip address 10.1.1.6 255.255.255.252
 clock rate 128000
 encapsulation ppp
 no shutdown
!
router eigrp 1
 passive-interface default
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
 network 10.1.1.0 0.0.0.3
 network 10.1.1.4 0.0.0.3
 network 10.1.202.1 0.0.0.0
 no auto-summary
!
ip http server
```



```
no ip http secure-server
!
logging source-interface Loopback0
logging 10.1.50.1
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
!
ntp master 3
 end
!
```

Router R3

Note: This is actually the configuration for R1.

```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 5-1 Router R3 TT-B Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
```

```
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 10.1.201.1 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown
!
interface FastEthernet0/1
 description FE to DLS1
 ip address 10.1.2.2 255.255.255.252
 ip flow ingress
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
 description WAN link to R2 - 128k leased line
 ip address 10.1.1.1 255.255.255.252
 ip flow ingress
 encapsulation ppp
 clock rate 128000
  no shutdown
!
interface Serial0/0/1
 description WAN link to R3 (not used)
 no ip address
 shutdown
!
router eigrp 1
 passive-interface default
 no passive-interface FastEthernet0/1
 no passive-interface Serial0/0/0
 network 10.1.1.0 0.0.0.3
 network 10.1.2.0 0.0.0.3
 network 10.1.201.1 0.0.0.0
 no auto-summary
!
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
logging source-interface Loopback0
logging 10.1.50.1
!
snmp-server community cisco RO
```



```
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 10.1.202.1
end
```

Trouble Ticket—TT-C Configurations

Switch ALS1 - Same as TT-A

Switch DLS1 - Same as TT-B

Switch DLS2 - Same as TT-B

Router R1- Same as TT-A

Router R3 - Same as TT-A

Router R2

```
!Lab 5-1 Router R2 TT-C Config
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
Hostname R2
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 5-1 Router R2 TT-C Config ***$
```



```
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 10.1.202.1 255.255.255.255
!
interface Loopback1
 description Simulated WAN link to ISP
 ip address 209.165.200.225 255.255.255.252
!
interface FastEthernet0/0
 shutdown
!
interface FastEthernet0/1
 shutdown
!
interface Serial0/0/0
 description WAN link to R1 - 128k leased line
 ip address 10.1.1.2 255.255.255.252
 encapsulation ppp
 no shutdown
 !
interface Serial0/0/1
 description WAN link to R3 - 128k leased line
 ip address 10.1.1.6 255.255.255.252
 clock rate 128000
 encapsulation ppp
 no shutdown
!
router eigrp 1
 passive-interface default
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
 network 10.1.1.0 0.0.0.3
 network 10.1.1.4 0.0.0.3
```

Error: Default route to Lo1 is not being redistributed under EIGRP.

```
router eigrp 1
   redistribute static
```

```
 network 10.1.202.1 0.0.0.0
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 Loopback1
!
ip http server
no ip http secure-server
!
logging source-interface Loopback0
logging 10.1.50.1
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
!
ntp master 3
 end
```

Trouble Ticket—TT-D Configurations

Note: No errors are introduced with this trouble ticket. The issue is one of network design and desired functionality. All devices use the baseline configurations.

Trouble Ticket—TT-E Configurations

Switch ALS1 - Same as TT-A

Switch DLS1 - Same as TT-B (Config is provided with authentication commands)

Switch DLS2 - Same as TT-B (Config is provided with authentication commands)

Router R1

```
!Lab 5-1 Router R1 TT-E Config
!
hostname R1
!
```



```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 5-1 Router R1 TT-E Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
key chain Secure
 key 1
   key-string 7 Updatepa55
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 10.1.201.1 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown
!
interface FastEthernet0/1
 description FE to DLS1
 ip address 10.1.2.2 255.255.255.252
 ip flow ingress
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 secure
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
 description WAN link to R2 - 128k leased line
```

Error: Key name is incorrect for interface Fa0/1.

`interface FastEthernet0/1`

`ip authentication key-chain eigrp 1 Secure`


```
 ip address 10.1.1.1 255.255.255.252
 ip flow ingress
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 Secure
 encapsulation ppp
 clock rate 128000
  no shutdown
!
interface Serial0/0/1
 description WAN link to R3 (not used)
 no ip address
 shutdown
!
router eigrp 1
 passive-interface default
 no passive-interface FastEthernet0/1
 no passive-interface Serial0/0/0
 network 10.1.1.0 0.0.0.3
 network 10.1.2.0 0.0.0.3
 network 10.1.201.1 0.0.0.0
 no auto-summary
!
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
logging source-interface Loopback0
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 10.1.202.1
end
```

Router R2

```
!Lab 5-1 Router R2 TT-E Config
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
Hostname R2
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 5-1 Router R2 TT-E Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
key chain Secure
 key 1
   key-string Updatepa55
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 10.1.202.1 255.255.255.255
!
interface FastEthernet0/0
 shutdown
!
interface FastEthernet0/1
 shutdown
!
interface Serial0/0/0
 description WAN link to R1 - 128k leased line
 ip address 10.1.1.2 255.255.255.252
```



```
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 Secure
 encapsulation ppp
 no shutdown
!
interface Serial0/0/1
 description WAN link to R3 - 128k leased line
 ip address 10.1.1.6 255.255.255.252
 clock rate 128000
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 Secure
 encapsulation ppp
 no shutdown
!
router eigrp 1
 passive-interface default
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
 network 10.1.1.0 0.0.0.3
 network 10.1.1.4 0.0.0.3
 network 10.1.202.1 0.0.0.0
 no auto-summary
!
ip http server
no ip http secure-server
!
logging source-interface Loopback0
logging 10.1.50.1
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
!
ntp master 3
 end
!
```

Router R3

```
!Lab 5-1 Router R3 TT-E Config
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
```



```
!
hostname R3
!
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 5-1 Router R3 TT-E Config ***$
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
no ip domain lookup
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
key chain Secure
 key 1
   key-string Updatepa55
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 10.1.203.1 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown

interface FastEthernet0/1
 description FE to DLS2
 ip address 10.1.2.14 255.255.255.252
 ip flow ingress
ip authentication mode eigrp 2 md5
ip authentication key-chain eigrp 2 Secure
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
 description WAN link to R1 - (Not used)
 no ip address
```

Error: Wrong AS number for EIGRP authentication on interfaces Fa0/1 and S0/0/1. Fa0/1 commands are shown here.

interface FastEthernet0/1

ip authentication mode eigrp 1 md5

ip authentication key-chain eigrp 1 Secure

```
 clock rate 128000
 encapsulation ppp
 shutdown
!
interface Serial0/0/1
 description WAN link to R2 - 128k leased line
 ip address 10.1.1.5 255.255.255.252
 ip authentication mode eigrp 2 md5
 ip authentication key-chain eigrp 2 Secure
 ip flow ingress
 encapsulation ppp
 no shutdown
!
router eigrp 1
 passive-interface default
 no passive-interface FastEthernet0/1
 no passive-interface Serial0/0/1
 network 10.1.1.4 0.0.0.3
 network 10.1.2.12 0.0.0.3
 network 10.1.203.1 0.0.0.0
 no auto-summary
!
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
logging source-interface Loopback0
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 10.1.202.1
end

!Lab 5-1 Switch DLS1 TT-E Config
!
```


Switch DLS1

```
hostname DLS1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55

banner motd $*** Lab 5-1 Switch DLS1 TT-E Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
!
ip domain name tshoot.net
!
ip dhcp excluded-address 10.1.10.252 10.1.10.254
ip dhcp excluded-address 10.1.20.252 10.1.20.254
ip dhcp excluded-address 10.1.30.252 10.1.30.254
!


ip dhcp pool OFFICE
   network 10.1.10.0 255.255.255.0
   default-router 10.1.10.254
   domain-name tshoot.net
!
ip dhcp pool VOICE
   network 10.1.20.0 255.255.255.0
   default-router 10.1.20.254
   domain-name tshoot.net
!
ip dhcp pool GUEST
   network 10.1.30.0 255.255.255.0
   default-router 10.1.30.254
   domain-name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
```

Error: Key definition is missing.

```
key chain Secure
 key 1
  key-string Updatepa55
```



```
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog contenttype plaintext
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 24576
spanning-tree vlan 20,50 priority 28672
!
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 70
 name CCTV
!
vlan 100
 name MGMT
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel1
 description Channel to ALS1
 no shut
!
interface Port-channel10
 description Channel to DLS2
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
```



```
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100

switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R1
 no switchport
 ip address 10.1.2.1 255.255.255.252
 speed 100
 duplex full
 spanning-tree bpduguard enable
 no shut
!
interface FastEthernet0/6
 description FE to SRV1
 switchport access vlan 50
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shut
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
```

Error: EIGRP Authentication key is missing from Fa0/5.

ip authentication mode eigrp 1 md5

ip authentication key-chain eigrp 1 Secure


```
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
```

```
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
```

```
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 10.1.10.252 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 priority 110
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.252 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.252 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 priority 110
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.252 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 preempt
!
interface Vlan70
 ip address 10.1.70.252 255.255.255.0
 standby 70 ip 10.1.70.254
 standby 70 preempt
!
interface Vlan100
 ip address 10.1.100.252 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 priority 110
 standby 100 preempt
!
router eigrp 1
 passive-interface default
 no passive-interface Fa0/5
 no auto-summary
```



```
 network 10.1.0.0 0.0.255.255
!
ip classless
ip http server
ip http secure-server
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO

snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server host 10.1.50.1 version 2c cisco
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 10.1.202.1
end
```

Switch DLS2

```
!Lab 5-1 Switch DLS2 TT-E Config
!
hostname DLS2
!
service timestamps debug datetime msec
service timestamps log datetime
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 5-1 Switch DLS2 TT-E Config ***$
```



```
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
  path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 28672
spanning-tree vlan 20,50 priority 24576

vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 100
 name MGMT
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
```

Error: Key definition is missing.

```
key chain Secure
 key 1
  key-string Updatepa55
```



```
ip ssh source-interface Vlan100
!
interface Port-channel2
 description Channel to ALS1
 no shut

interface Port-channel10
 description Channel to DLS1
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R3
 no switchport
 ip address 10.1.2.13 255.255.255.252
 speed 100
 duplex full
 spanning-tree bpduguard enable
 no shut
```

Error: EIGRP Authentication key is missing from Fa0/5.

ip authentication mode eigrp 1 md5

ip authentication key-chain eigrp 1 Secure


```
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
```

```
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description FE to PC-C
 switchport access vlan 30
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
```

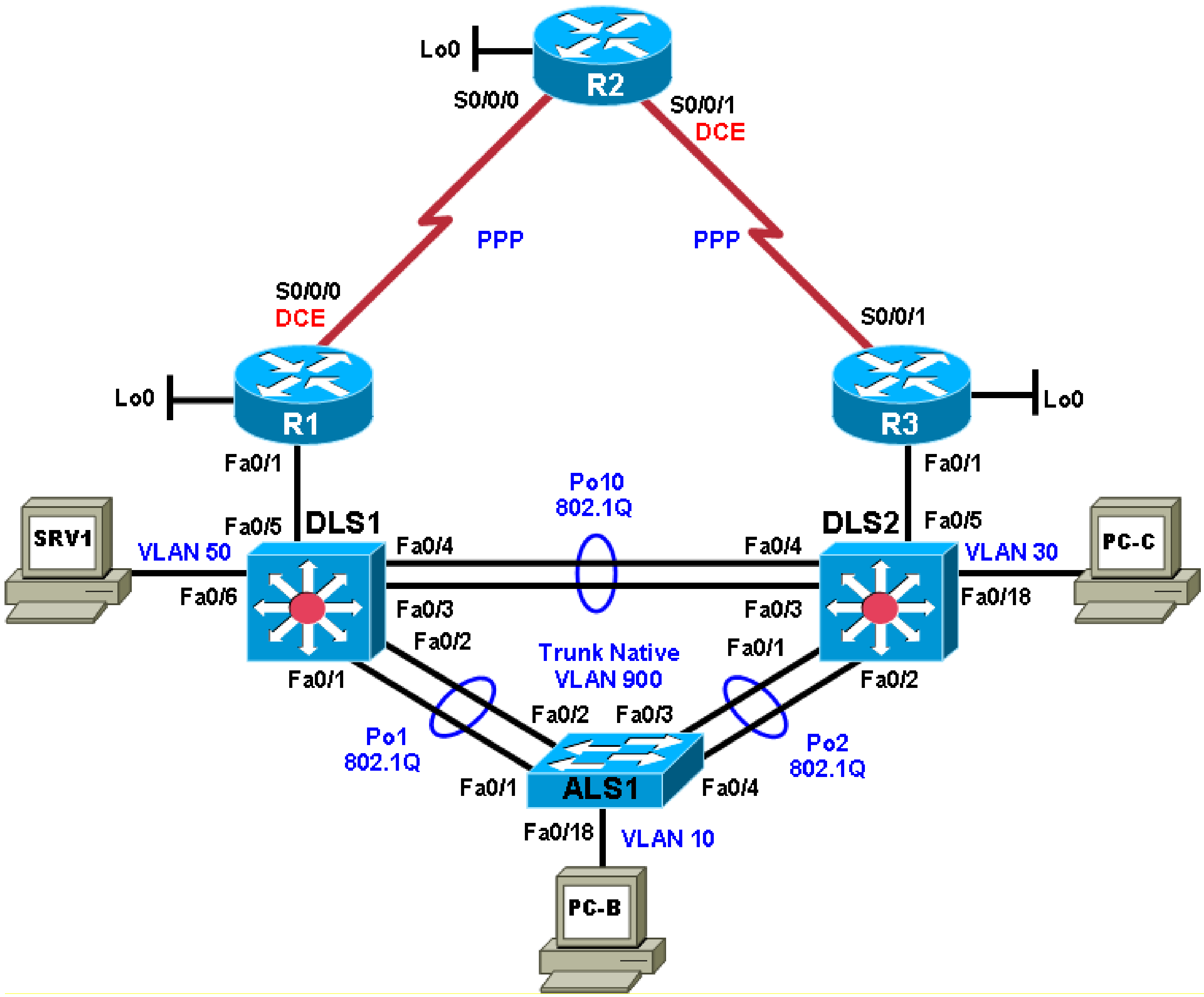


```
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 10.1.10.253 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.253 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 priority 110
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.253 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.253 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 priority 110
 standby 50 preempt
```

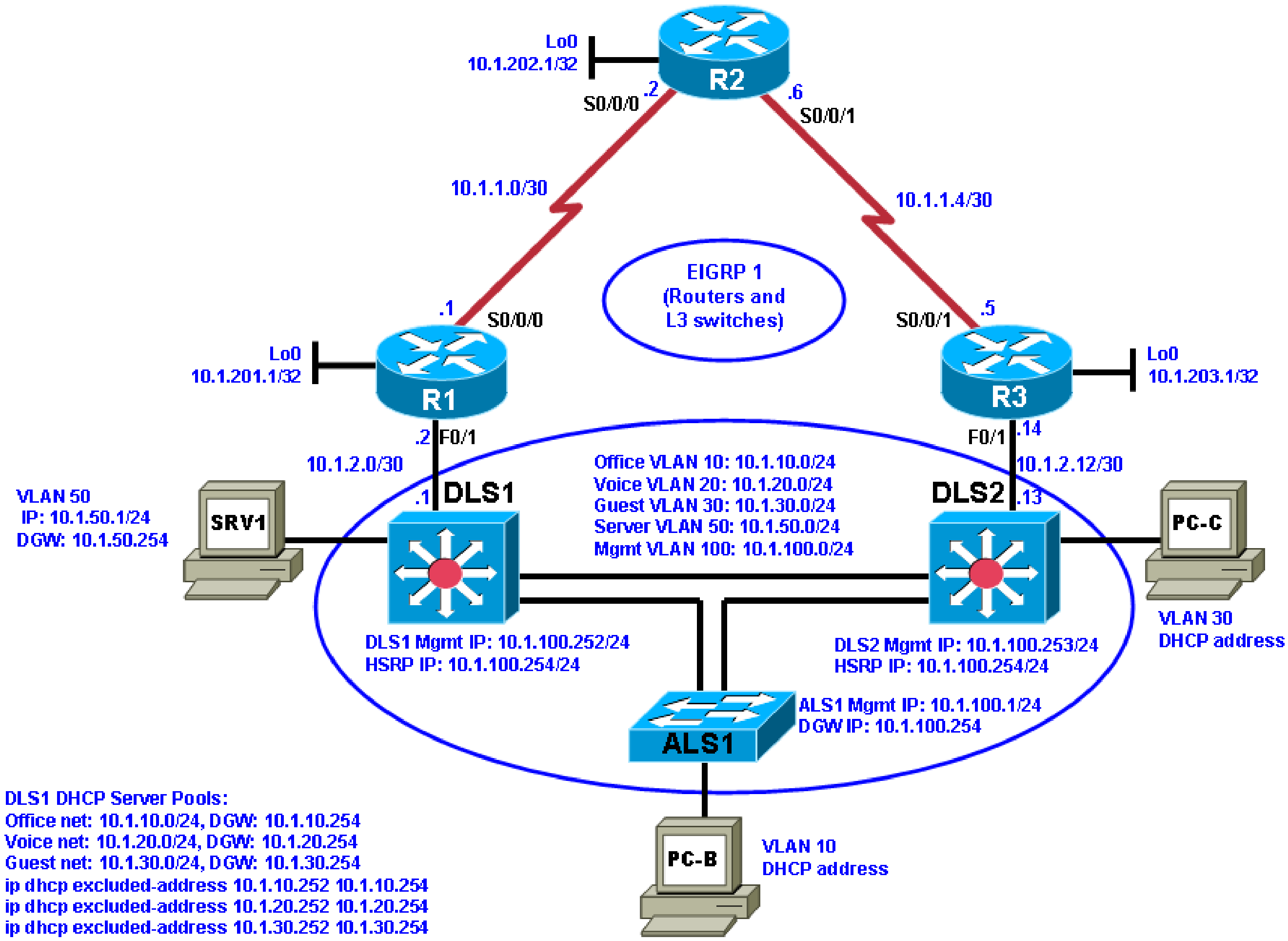
```
!
interface Vlan100
 ip address 10.1.100.253 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 preempt
!
!
router eigrp 1
 passive-interface default
 no passive-interface Fa0/5
 no auto-summary
 network 10.1.0.0 0.0.255.255
!
ip classless
ip http server
ip http secure-server
!
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 10.1.202.1
end
```


Chapter 5 Lab 5-2, OSPF and Route Redistribution Instructor Version

Physical Topology (Baseline)



Logical Topology (Baseline)



Objectives

- Load the trouble ticket device configuration files for each trouble ticket.
- Diagnose and resolve problems related to the OSPF routing protocol.
- Diagnose and resolve problems related to route redistribution.
- Document troubleshooting progress, configuration changes, and problem resolution.

Background

In this lab, you troubleshoot various problems related to the Open Shortest Path First (OSPF) routing protocol and route redistribution between routing protocols. For each task or trouble ticket, the trouble scenario and problem symptom are described. While troubleshooting, you will discover the cause of the problem, correct it, and then document the process and results.

Migrating from EIGRP to OSPF

Your company has decided to migrate from using Enhanced Interior Gateway Protocol (EIGRP) to OSPF as the routing protocol. This migration will be executed in two phases.

The engineering team planned and designed the migration, but the support team must support the new network, so they are involved in migrating the branch during Phase 2.

Phase 1—The headquarters central site campus is migrated to OSPF as well as one of the branch offices (simulated by Lo0 on R3). EIGRP is still used on the WAN toward the R2 branch office. On router R1, redistribution is configured between OSPF and EIGRP to ensure connectivity between headquarters and the branch office connected to R2.

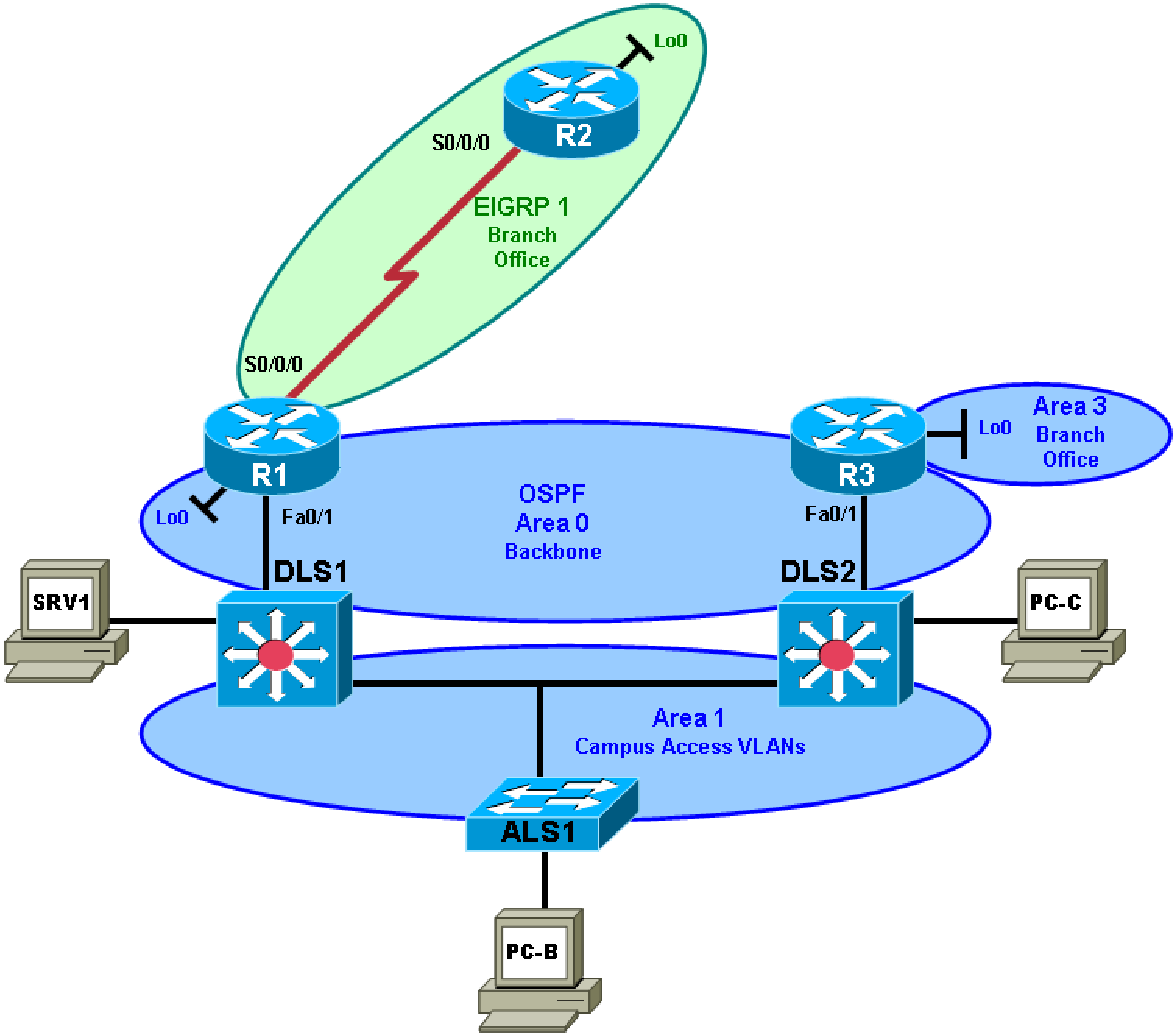
Phase 2—The R2 branch office (simulated by Lo0 on R2) is converted from EIGRP to OSPF, and all branch offices are migrated so that OSPF is used in the entire network. Each branch site is in a separate area that is configured as totally stubby.

Today is Saturday, and the engineering team has been busy implementing OSPF and removing EIGRP at the headquarters site. Although you have not taken part in the actual implementation, some of the senior engineers in the support team are on standby to assist during the verification and troubleshooting phase. Together with the engineering team, you will have to make the decision on Sunday to either accept the implementation or, if major issues are uncovered that would threaten the stability of the network, roll back to the original configurations.

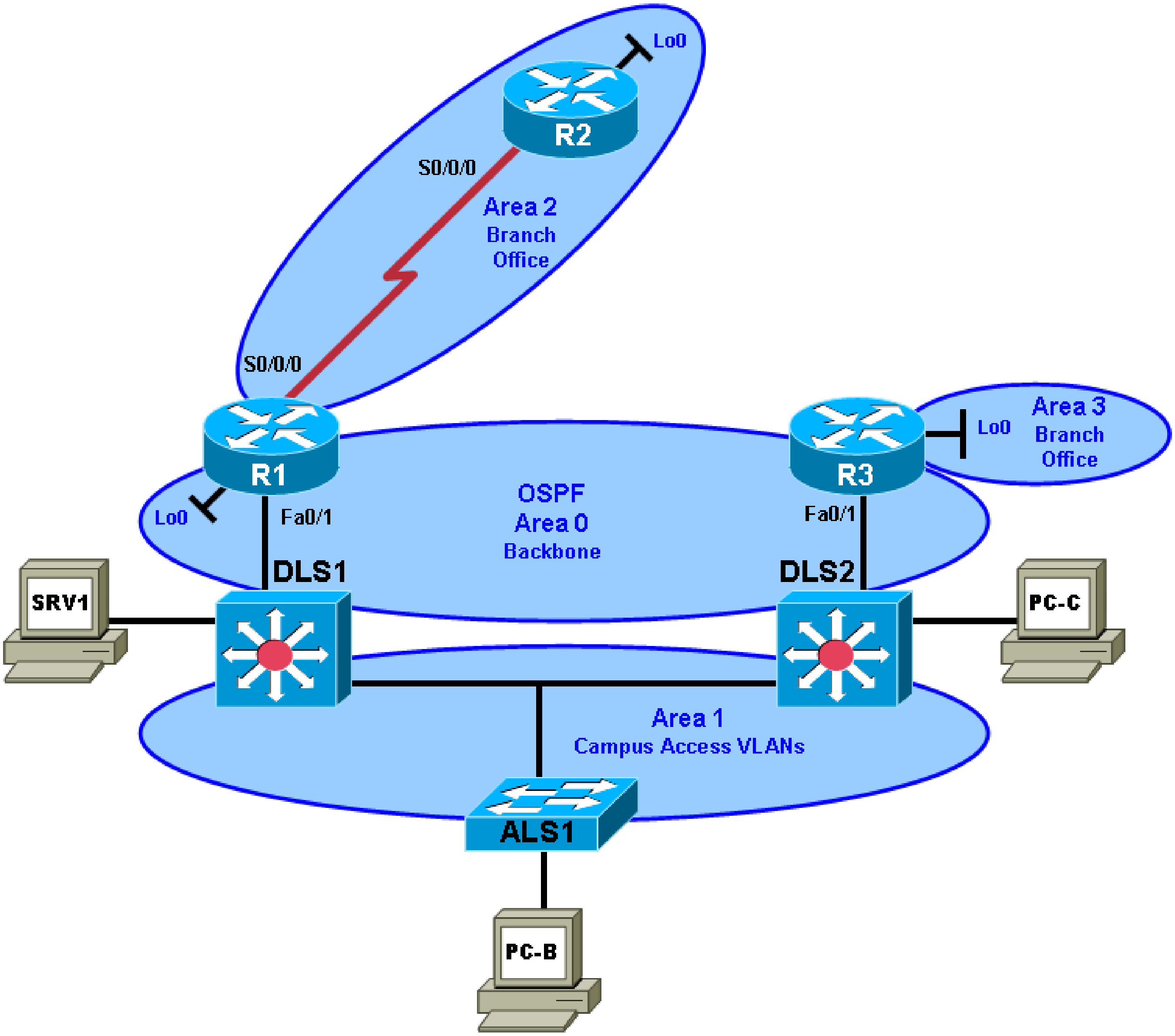
OSPF Network Design

Phases 1 and 2 of the OSPF design are depicted in the following figures. Backbone area 0 contains the FastEthernet interfaces on core Layer 3 switches DLS1 and DLS2 as well as those on routers R1 and R3. Area 0 also includes VLAN 200 and the corresponding SVI, which have been added to these two switches so that they can form an OSPF neighbor relationship and exchange routes. The headquarters campus access VLANs 10, 20, 30, and 50 and management VLAN 100 are in OSPF area 1. The R2 stub network is in area 2, and the R3 stub network is in area 3.

Phase 1 OSPF Network Design



Phase 2 OSPF Network Design



Test Plan

To test the branch connectivity using redistribution between EIGRP and OSPF and the eventual conversion to only OSPF, branch routers R2 and R3 have been specifically prepared for both of these scenarios. Router R2 functions as the default gateway for the R2 LAN, while router R3 is the default gateway for the R3 LAN. Router R2 runs EIGRP as usual. This allows testing the redistribution of EIGRP from the R2 branch office LAN (simulated by R2 Lo0) to OSPF area 0 and redistribution of OSPF into EIGRP using router R1 as an Autonomous System Border Router (ASBR). Router R3 is configured to run OSPF as an Area Border Router (ABR) between area 0 and area 3. The R3 branch office client is simulated by R3 Lo0).

At the end of Phase 1, when the network is fully converged, all OSPF routers should have EIGRP routes in their routing tables and EIGRP router R2 should have all OSPF routes in its routing table.

After the completion of Phase 2, all routers except R2 should have OSPF routes. Router R2 is totally stubby and should only have a default route to R1.

Note: Trouble ticket TT-A is related to the verification and acceptance of Phase 1 of the OSPF migration. Trouble tickets TT-B, C and D are related to the verification and acceptance of Phase 2 of the OSPF migration. Any interfaces that have been shut down on routers R2 and R3 should remain shut down for the duration of this lab exercise.

Physical and Logical Topology Diagrams

The physical and logical topologies for the existing EIGRP-based network are provided to assist the troubleshooting effort.

Lab Structure

This lab is divided into two main sections.

Section 1—Trouble Tickets and Troubleshooting Logs

This section includes multiple tasks. Each task is associated with a trouble ticket (TT) and introduces one or more errors on one or more devices. If time is a consideration, each task or trouble ticket can be performed independently.

Section 2—Troubleshooting Reference Information

This section provides OSPF and route redistribution troubleshooting information that can be applied to any trouble ticket in this lab. Sample troubleshooting flows are provided, along with examples of useful commands and output. If time permits, it is recommended that you read through Section 2 prior to starting on the trouble tickets.

Instructor note: Because the troubleshooting reference section is lengthy, ask students to read through it prior to starting the lab to become familiar with the troubleshooting flows and commands used in this lab. Consider assigning it as homework.

This lab uses Cisco 1841 routers with Cisco IOS Release 12.4(24)T1 and the Advanced IP Services image c1841-advipservicesk9-mz.124-24.T1.bin. The switches are Cisco WS-C2960-24TT-L with the Cisco IOS image c2960-lanbasek9-mz.122-46.SE.bin and Catalyst 3560-24PS with the Cisco IOS image c3560-advipservicesk9-mz.122-46.SE.bin. Other routers (such as 2801 and 2811), switches (such as 2950 or 3550), and Cisco IOS Software versions can be used if they have comparable capabilities and features. Depending on the router or switch model and Cisco IOS Software version, the commands available and output produced might vary from what is shown in this lab.

Note: Any changes made to the baseline configurations or topology (other than errors introduced) are noted in the trouble ticket so that you are aware of them prior to beginning the troubleshooting process.

Instructor Notes

- The lab topology should be pre-built prior to the students starting the lab. Ensure that all routers and switches (R1, R2, R3, ALS1, DLS1, and DLS2) have the course lab configuration files installed in flash. These can be downloaded from the Academy Connection web site.
- The device configurations that contain trouble ticket errors or modifications from the baseline are included at the end of the lab and the errors in them are identified.
- Each device has a directory named “tshoot” in flash. This directory contains the baseline configuration file for that device as well as configuration files for the labs in this course. Refer to Lab 3-1 for instructions on creating the tshoot directory in flash.
- Instructors can use a TFTP server, USB drive, flash memory card or other method to copy all the course configuration files into the flash:/tshoot directory for each device in the topology.

- The student is responsible for loading the trouble ticket configurations for all labs as required using the procedure described in Lab 3-1.
- Set the correct time on router R2, which serves as the primary NTP server for the lab network.
- If time is an issue, each task (trouble ticket) can be performed independently.

Required Resources

- 3 routers (Cisco 1841 with the Cisco IOS Release 12.4(24)T1 Advanced IP Service or comparable)
- 1 switch (Cisco 2960 with the Cisco IOS Release 12.2(46)SE C2960-LANBASEK9-M image or comparable)
- 2 switches (Cisco 3560 with the Cisco IOS Release 12.2(46)SE C3560-LANBASEK9-M image or comparable)
- SRV1 (Windows PC with 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

Instructor Notes:

- This lab is divided into multiple tasks. Each task is associated with a trouble ticket (TT) and introduces one or more errors on one or more devices.
- Students can work individually or as a team. The problems introduced in this lab are related to OSPF and route redistribution.
- Suggested actions and results presented during the troubleshooting process for each TT can be shared with the students during debrief or copies of the instructor version of the lab can be made available to the students to assist them in verifying their work.

Section 1—Trouble Tickets and Troubleshooting Logs

Task 1: Trouble Ticket Lab 5-2 TT-A

Instructor note: This trouble ticket involves device R1 and R2 issues related to OSPF and EIGRP route redistribution.

Step 1: Review trouble ticket Lab 5-2 TT-A.

After the completion of Phase 1—implementation of OSPF in the headquarters portion of the network and the redistribution between EIGRP and OSPF—the connectivity from the office LAN on the R2 branch router to server SRV1 at headquarters is tested. A ping from the R2 LAN client (sourced by Lo0 on R2) to server SRV1 fails.

Your task is to diagnose this problem and, if possible, resolve it. Connectivity from the R2 LAN to server SRV1 is mandatory to consider this phase of the migration successful.

Step 2: Load the device trouble ticket configuration files for TT-A.

Using the procedure described in Lab 3-1, verify that the lab configuration files are present in flash. Load the proper configuration files as indicated in the Device Configuration File table.

Note: The following device access methods are in effect after loading the configuration files:

- Console access requires no username or password.
- Telnet and SSH require username **admin** and password **adminpa55**.
- The enable password is **ciscoenpa55**.

Instructor note: Although it is not considered security best practice, the student can set the console and VTY line exec-timeout to 0 0 to facilitate performance of this lab.

Device Configuration File Table

Device Name	File to Load	Notes
ALS1	Lab52-ALS1-TT-A-Cfg.txt	This file is the same as the baseline
DLS1	Lab52-DLS1-TT-A-Cfg.txt	This file contains configurations different than the baseline
DLS2	Lab52-DLS2-TT-A-Cfg.txt	This file contains configurations different than the baseline
R1	Lab52-R1-TT-A-Cfg.txt	This file contains configuration errors.
R2	Lab52-R2-TT-A-Cfg.txt	This file contains configurations different than the baseline
R3	Lab52-R3-TT-A-Cfg.txt	This file contains configurations different than the baseline
SRV1	N/A	Static IP: 10.1.50.1 Default gateway: 10.1.50.254
PC-B	N/A	DHCP
PC-C	N/A	DHCP

Instructor note: The student loads the “broken” TT configuration files for all devices, even though only the configurations indicated in the Notes column contain errors.

Step 3: Configure SRV1 and start the syslog and TFTP servers.

Step 4: Release and renew the DHCP lease on PC-B.

Ensure that PC-B is configured as a DHCP client in the OFFICE VLAN.

After loading all TT-A device configuration files, issue the **ipconfig /release** and **ipconfig /renew** commands on PC-B.

Step 5: Outline the troubleshooting approach and validation steps.

Use this space to identify your troubleshooting approach and the key steps to verify that the problem is resolved. Troubleshooting approaches to select from include: follow-the-path, spot-the-differences, bottom-up, top-down, divide-and-conquer, shoot-from-the-hip, and move-the-problem.

Note: In addition to a specific approach, you can use the generic troubleshooting process described at the beginning of Section 2 of this lab.

The follow-the-path or spot-the-differences approach can be used.

Verification steps can include:

- The R2 LAN client (sourced by Lo0 on R2) in the EIGRP routing domain can ping server SRV1 in the OSPF routing domain.
- The R2 routing table shows external routes learned via R1 OSPF-to-EIGRP redistribution.
- The DLS1 routing table shows external routes learned via R1 EIGRP-to-OSPF redistribution.

Step 6: Record the troubleshooting process and configuration changes.

Note: Section 2 of this lab includes sample troubleshooting flows, useful commands, and examples of output.

Use this log to document your actions and results during the troubleshooting process. List the commands you used to gather information. As you progress, record what you think the problem might be and which actions you will take to correct the problem.

Device	Actions and Results

Device	Actions and Results

Responses will vary but could include:

- Pings from the R2 LAN client (sourced by Lo0 10.1.202.1 on R2) to server SRV1 fail.
- Pings from R2 (sourced by S0/0/0 10.1.1.2 on R2) to server SRV1 fail.
- Pings from R2 (sourced by S0/0/0 10.1.1.2 on R2) to R1 S0/0/0 (10.1.1.1) succeed.
- Pings from SRV1 to its default gateway VLAN 50 (10.1.50.254) on DLS1 succeed.
- Pings from SRV1 to all other network devices in the OSPF domain succeed.
- Pings from SRV1 to any R2 address (for example, 10.1.1.2) fails. DLS1 reports: “Destination host unreachable.”

TT-A Issue 1

R1 is not sending OSPF routes into the EIGRP AS. The redistribution of OSPF routes into EIGRP fails because no seed metric is specified for the **`redistribute ospf`** command under EIGRP.

- The **`show ip route 10.1.50.0 255.255.255.0`** command (SRV1 subnet) on R2 (in the EIGRP domain) indicates that the subnet is not in the routing table.
- The **`show ip route 10.1.50.1 255.255.255.0`** command on R1 indicates that the route is known via OSPF 1 and that it is redistributing via EIGRP, but it is not being advertised by EIGRP.
- A check of the OSPF migration plan indicates that server SRV1 is in OSPF area 1.
- The **`show ip ospf border-routers`** command indicates that R1 (ID 10.1.201.1) is configured as an ASBR in area 0 and that DLS1 (ID 10.1.211.1), DLS2 (ID 10.1.212.1) and R3 (ID 10.1.203.1) are configured as ABRs in area 0.
- The **`show ip route ospf`** command on R1 (ASBR) indicates that all routes from the OSPF network (both “O” and “IA”) are present in its routing table as well as a route to R2 Lo0 (10.1.202.1) learned via EIGRP (“D”).
- The **`show ip protocols`** command on R1 (ASBR) indicates that it is running both EIGRP 1 and OSPF 1, routing for the correct networks, and redistributing OSPF 1 under the EIGRP routing process.
- The **`show ip route`** command on R2 (in the EIGRP domain) indicates that there are no routes learned from the OSPF portion of the network via the redistribution point R1 (ASBR). It does not appear that R1 is redistributing OSPF routes properly into the EIGRP domain.

- The **show run | begin eigrp** command on R1 indicates that there is no seed metric specified with the **redistribute ospf 1** command under the EIGRP 1 routing process configuration, thus no OSPF routes will be redistributed into the EIGRP domain.

Action: Add a seed metric to the **redistribute ospf 1** command under the EIGRP 1 routing process so that OSPF routes will be injected into the EIGRP domain. See TT-A debrief for more information.

Verification: The R2 routing table now contains all the subnets from the OSPF domain (represented as external routes by code "D EX") learned via R1 OSPF-to-EIGRP redistribution. However, R2 Lo0 still cannot ping SRV1 at 10.1.50.1.

TT-A Issue 2

R1 is not sending EIGRP subnets to the OSPF domain because the keyword **subnets** was omitted from the **redistribute eigrp 1** command), which causes OSPF to only redistribute classful routes when redistributing from EIGRP into OSPF.

- The **show ip route eigrp** command on R1 (ASBR) indicates that there is an EIGRP ("D") route to the R2 Lo0 network 10.1.202.1/32, which was learned via R2, in its routing table with an AD of 90 and metric of 2297856.
- The **show ip route ospf** command on R1 (ASBR) indicates that all routes from the OSPF network (both "O" and "IA") are present in its routing table.
- The **show ip protocols** command on R1 indicates that it is redistributing external routes from EIGRP 1 under the OSPF routing process.
- The **show ip route 10.1.202.1 255.255.255.255** command on R1 indicates that the route is known via EIGRP 1 and that it is redistributing via OSPF but it is not being advertised by OSPF.
- The **show ip route 10.1.202.1** command on OSPF neighbor DLS1 indicates that no external (O E2) route to network 10.1.202.1/30 is in its routing table. DLS1 is not receiving redistributed EIGRP routes from ASBR R1.
- Only subnets of classful network 10.0.0.0/8 are advertised on R2 (10.1.1.0/30 and 10.1.202.1/32). Perhaps there is a problem with the redistribution, and only classful EIGRP networks are being advertised (no subnets).
- As a test, another loopback interface Lo1 is added to R2 with classful IP address 192.168.1.1/24. Network 192.168.1.0/24 is also added to the EIGRP 1 routing process.
- The **show ip route 192.168.1.0** command on DLS1 now indicates a routing entry redistributed by R1 for this classful network (external O E2), but there are still no routes to the R2 10.0.0.0/8 subnets.
- The **show run | begin router ospf** command on R1 indicates that the **redistribute eigrp 1** command under the OSPF routing process does not include the **subnets** option. As a result, DLS1 is not receiving redistributed EIGRP subnet routes from ASBR R1.

Action: Add the **subnets** option (and an optional seed metric) to the **redistribute ospf 1** command under the EIGRP 1 routing process so that OSPF routes will be injected into the EIGRP domain. See TT-A debrief for more information.

Verification: The DLS1 routing table now contains all the subnets from the EIGRP domain (represented as external routes by code "O E2") learned via R1 EIGRP-to-OSPF redistribution.

Verification: Pings from R2 using Lo0 (simulated remote branch client) as the source address to server SRV1 in VLAN 50 succeed using command: **ping 10.1.50.1 source Lo0** or **ping 10.1.50.1 source 10.1.202.1**.

Step 7: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with your instructor. The notes can include problems encountered, solutions applied, useful commands employed, alternate solutions and methods, and procedure and communication improvements.

Trouble Ticket TT-A Debrief—Instructor Notes

This trouble ticket has two different problems. The first issue prevents the redistribution of OSPF routes into EIGRP from working correctly. The second issue causes the redistribution in the other direction, from EIGRP into OSPF, to fail. Both issues need to be corrected to resolve this ticket.

TT-A—Issue 1

The redistribution from OSPF routes into EIGRP fails because no seed metric is specified for the redistribution. The default metric for EIGRP redistribution is set to infinity and causes the routes not to be redistributed into EIGRP. To resolve this problem, a correct seed metric needs to be specified for the redistribution from OSPF to EIGRP. The exact value of the seed metric is not important. If a different metric than the one presented here is used, the solution is likely to be correct as long as it has restored the connectivity for the simulated branch client (Lo0 on R2). The metric values chosen here are those associated with a high-speed T1 WAN link.

Correct redistribution of the OSPF routes into EIGRP can be accomplished by issuing the following commands on router R1:

```
router eigrp 1
 redistribute ospf 1 metric 1544 2000 255 1 1500
```

Be sure to discuss the values that are provided with the class during the TT debrief discussion. The following router command help output provides insight into the meaning of the metric variables used in the command:

```
R1(config-router)#redistribute ospf 1 metric ?
  <1-4294967295>  Bandwidth metric in Kbits per second

R1(config-router)#redistribute ospf 1 metric 1544 ?
  <0-4294967295>  EIGRP delay metric, in 10 microsecond units

R1(config-router)#redistribute ospf 1 metric 1544 2000 ?
  <0-255>  EIGRP reliability metric where 255 is 100% reliable

R1(config-router)#redistribute ospf 1 metric 1544 2000 255 ?
  <1-255>  EIGRP Effective bandwidth metric (Loading) where 255 is 100%
loaded

R1(config-router)#redistribute ospf 1 metric 1544 2000 255 1 ?
  <1-65535>  EIGRP MTU of the path

R1(config-router)#redistribute ospf 1 metric 1544 2000 255 1 1500
```

TT-A—Issue 2

The second problem is caused by the omission of the keyword **`subnets`** from the **`redistribute`** command, which is responsible for the redistribution from EIGRP into OSPF. As a result, OSPF will only redistribute classful routes. Because all routes in the R2 branch office are subnets of network 10.0.0.0, none of these routes will be redistributed.

In the possible troubleshooting process and configuration changes outlined in Step 6, a classful network 192.168.1.0/24 using Lo1 was configured on R2 to test the hypothesis and it was redistributed into the OSPF domain.

Correct the redistribution of the EIGRP routes into OSPF by issuing the following commands on router R1:

```
router ospf 1
 redistribute eigrp 1 metric 100 subnets
```

Although it is not necessary, it is good habit to specify a seed metric when configuring redistribution. At this point, connectivity from the branch office client (Lo0 on R2) should be restored.

Task 2: Trouble Ticket Lab 5-2 TT-B

Instructor note: This trouble ticket involves R1 and R2 issues related to OSPF area numbering and area types (for example, totally stubby).

Step 1: Review trouble ticket Lab 5-2 TT-B.

Phase 2 has been completed and all routers have been converted to OSPF. The connectivity from a branch office client on the R2 LAN (simulated by R2 Lo0) to server SRV1 at the central site is tested. A ping from the client on the R2 LAN (using source interface Lo0) to server SRV1 fails. The connectivity problem is not limited to SRV1. An attempt to connect to other headquarters servers also fails. Your task is to diagnose this problem and, if possible, resolve it. Connectivity from the branch client to server SRV1 is mandatory for this phase of the migration to be considered successful.

Note: Refer back to the implementation and test plan to review the requirements for Phase 2.

Step 2: Load the device trouble ticket configuration files for TT-B.

Using the procedure described in Lab 3-1, verify that the lab configuration files are present in flash. Load the proper configuration files as indicated in the Device Configuration File table.

Note: See Task 1, Step 2 for device access methods, usernames, and passwords after the configuration files have been loaded.

Device Configuration File Table

Device Name	File to Load	Notes
ALS1	Lab51-ALS1-TT-B-Cfg.txt	This file is the same as the baseline
DLS1	Lab51-DLS1-TT-B-Cfg.txt	This file contains configurations different than the baseline
DLS2	Lab51-DLS2-TT-B-Cfg.txt	This file contains configurations different than the baseline
R1	Lab51-R1-TT-B-Cfg.txt	This file contains configuration errors
R2	Lab51-R2-TT-B-Cfg.txt	This file contains configuration errors
R3	Lab51-R3-TT-B-Cfg.txt	This file contains configurations different than the baseline
SRV1	N/A	Static IP: 10.1.50.1 Default gateway: 10.1.50.254
PC-B	N/A	DHCP (release and renew after loading device configurations)
PC-C	N/A	DHCP (release and renew after loading device configurations)

Step 3: Configure SRV1 and start the syslog and TFTP servers.

Step 4: Release and renew the DHCP leases on PC-B and PC-C, as described in Task 1.

Step 5: Outline the troubleshooting approach and validation steps.

Use this space to identify your troubleshooting approach and the key steps to verify that the problem is resolved. Troubleshooting approaches to select from include: follow-the-path, spot-the-differences, bottom-up, top-down, divide-and-conquer, shoot-from-the-hip, and move-the-problem.

Note: In addition to a specific approach, you can use the generic troubleshooting process described at the beginning of Section 2 of this lab.

____

____

____

____

____

The follow-the-path or divide-and-conquer approach can be used.

Verification steps can include:

- Users on the R2 branch office LAN (simulated by R2 Lo0) can ping server SRV1.
- R1 and R2 become neighbors
- The R1 routing table contains all OSPF routes, but the branch office stub network R2 routing table contains only a default route to R1.

Step 6: Record the troubleshooting process and configuration changes.

Note: Section 2 of this lab includes sample troubleshooting flows, useful commands, and examples of output.

Use this log to document your actions and results during the troubleshooting process. List the commands you used to gather information. As you progress, record what you think the problem might be and which actions you will take to correct the problem.

Device	Actions and Results

Device	Actions and Results

Responses will vary but could include:

- Pings from the R2 LAN client (sourced by Lo0 10.1.202.1 on R2) to server SRV1 (10.1.50.1) fail.
- Pings from the R2 LAN client (sourced by Lo0 10.1.202.1 on R2) to R1 Fa0/1 (10.1.2.2) fail.
- Pings from R2 (sourced by S0/0/0 10.1.1.2 on R2) to server SRV1 fail.
- Pings from R2 (sourced by S0/0/0 10.1.1.2 on R2) to R1 S0/0/0 (10.1.1.1) succeed.
- Pings from SRV1 to its default gateway VLAN 50 (10.1.50.254) on DLS1 succeed.
- Pings from SRV1 to any R2 address (for example, 10.1.1.2) fails. DLS1 reports “Destination host unreachable.”
- Pings from SRV1 to all other network devices in the OSPF domain succeed.

TT-B Issue 1

R2 is configured with the incorrect OSPF area number, which does not match R1. This prevents them from becoming OSPF neighbors.

- The **`show ip route 10.1.50.0 255.255.255.0`** command (SRV1 subnet) on R2 (in the new OSPF area 2) indicates that the subnet is not in the routing table.
- A check of the OSPF migration plan indicates that server SRV1 is in OSPF area 1.
- The **`show ip route 10.1.50.1 255.255.255.0`** command on R1 indicates that the route is known via OSPF 1.
- The **`show ip route`** command on R2 indicates that no OSPF routes are present in its routing table.
- The **`show ip route ospf`** command on R1 (ABR) indicates that all routes from areas 0, 1, and 3 of the OSPF network (both “O” and “IA”) are present in its routing table, except routes to R2 in area 2 (Lo0 10.1.202.1).
- The **`show ip ospf neighbor`** command on R2 indicates that it has no OSPF neighbors.
- The **`show ip ospf neighbor`** command on R1 indicates that DLS1 is a neighbor (DR neighbor ID 10.1.211.1) but not R2.
- The **`show ip ospf interface brief`** command on R1 indicates that interfaces Lo0, Fa0/1, and S0/0/0 are participating in the OSPF process. Lo0 and Fa0/1 are in area 0, and S0/0/0 (WAN link to R2) is in area 2.
- The **`show ip ospf interface brief`** command on R2 indicates that interfaces Lo0 and S0/0/0 are participating in the OSPF process. Lo0 is in area 2, but S0/0/0 (WAN link to R1) is in area 22.

- The **`show ip ospf database router 10.1.202.1`** command on R2 indicates links to the two directly connected (stub) networks, but no link to another router.
- The **`debug ip ospf packet`** command on R2 produces no output, which indicates that it is not receiving valid hello packets from R1 (t:1 in the debug output refers to Type 1 Hello packets).
- The **`debug ip ospf packet`** command on R1 indicates that it is receiving OSPF version 2 (v:2) hello packets (t:1) via Fa0/1 from DLS1, but none from R2.
- The **`debug ip ospf adj`** command on R1 indicates that it received packets from R2 (10.1.1.2) via S0/0/0 in area 2, but there is a mismatch area 22 in the header from R2.
- The **`debug ip ospf events`** command on R1 provides more information. It indicates that R1 is sending hello packets to multicast address 224.0.0.5 in area 0 and area 2. It is receiving hello packets from DLS1 (10.1.211.1) via Fa0/1 in area 0. It is receiving packets from R2 (10.1.1.2) via S0/0/0 in area 2, but there is a mismatch area 22 in the header from R2.
- A check of the OSPF migration implementation plan shows that R2 S0/0/0 should be in area 2 along with Lo0.
- The **`show run | begin ospf 1`** command on R2 confirms that network 10.1.1.0 0.0.0.3 is defined in area 22. This prevents R1 and R2 from becoming neighbors.

Action: Change the area for network 10.1.1.0 0.0.0.3 to 2. See TT-B debrief notes for more information.

Verification: Pings from the R2 LAN client (sourced by Lo0 10.1.202.1 on R2) to server SRV1 (10.1.50.1) still fail. There must be another problem.

TT-B Issue 2

R1 area 2 is configured as a stub area, but on router R2, the area is not configured as a stub area. This prevents R1 and R2 from becoming OSPF neighbors.

- The **`show ip ospf interface brief`** command on R2 indicates that interfaces Lo0 and S0/0/0 are now both in area 2.
- The **`show ip ospf neighbor`** command on R2 indicates that it has no OSPF neighbors.
- The **`debug ip ospf packet`** command on R2 shows that hello packets are now being received from R1.
- The **`show ip route`** command on R2 indicates that there are still no OSPF routes in the R2 routing table.
- The **`debug ip ospf adj`** command on R1 indicates that there are no adjacency events to report.
- The **`debug ip ospf events`** command on R1 provides more information. It indicates that R1 is sending hello packets to multicast address 224.0.0.5 in area 0 and area 2. It is receiving hello packets from DLS1 (10.1.211.1) via Fa0/1 in area 0. It is receiving hello packets from R2 (10.1.1.2) via S0/0/0 in area 2, but there is a mismatch in the stub/transit area option bit.
- A check of the OSPF migration implementation plan shows that R2 area 2 should be a totally stubby area.
- The **`show run | begin ospf 1`** command on R1 confirms that area 2 is defined as a stub area.
- The **`show run | begin ospf 1`** command on R2 confirms that area 2 is *not* defined as a stub area. This prevents R1 and R2 from becoming neighbors.

Action: Change the area type for area 2 on R2 to stub to match R1. See TT-B debrief notes for more information.

Verification: Pings from the R2 LAN client (sourced by Lo0 10.1.202.1 on R2) to server SRV1 (10.1.50.1) succeed.

TT-B Issue 3

The branch office area 2 is not configured as a totally stubby area as specified in the OSPF implementation plan.

- The **`show ip route`** command indicates that the R2 routing table now contains all the subnets from the OSPF domain (represented as external routes by code "O IA"). There is also a default route injected by R1 to 0.0.0.0/0 via R1 S0/0/0 10.1.1.1. R1 area 2 and R2 area 2 are both configured as stub areas, but branch router R2 is still receiving all OSPF routes, which is unnecessary and does not meet the requirements of the implementation plan.
- The **`show run | begin ospf 1`** command on R1 and R2 confirms that area 2 has not been defined as a totally stubby area.

Action: On router R1, add the **`no-summary`** option to the **`area 2 stub`** command under OSPF process 1. See TT-B debrief notes for more information.

Verification: Pings from the R2 LAN client (sourced by Lo0 10.1.202.1 on R2) to server SRV1 (10.1.50.1) succeed. The **`show ip route`** command indicates that the R2 routing table now contains only a default route to 0.0.0.0/0 via R1 S0/0/0 10.1.1.1.

Step 7: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with your instructor. The notes can include problems encountered, solutions applied, useful commands employed, alternate solutions and methods, and procedure and communication improvements.

____

____

____

____

____

____

____

Trouble Ticket TT-B Debrief—Instructor Notes

This trouble ticket has two main issues. The problem is that router R2 does not succeed in establishing an OSPF neighbor relationship with router R1. The first issue is related to the OSPF area number defined. The second issue is a mismatch in the area type. Both issues need to be corrected to resolve this ticket. A third issue is related to the type of area defined for the branch office, but this issue does not result in a connectivity failure.

TT-B—Issue 1

The first issue is a mismatch between the area that is configured on router R2 for the WAN link (which is incorrectly configured as area 22, but should be area 2), and the area that is configured on router R1 (which is area 2). This issue alone prevents R2 from establishing an OSPF neighbor relationship with router R1. This problem can be resolved by issuing the following commands on R2:

```
router ospf 1
  network 10.1.1.0 0.0.0.3 area 2
  network 10.1.202.1 0.0.0.0 area 2
```

TT-B—Issue 2

The second issue is that area 2 is configured as a stub area on router R1, while on router R2, the area is not configured as a stub area. This issue alone prevents R2 from establishing an OSPF neighbor relationship with router R1. Correcting both issues allows R1 and R2 to become neighbors and provides connectivity between the branch office on R2 and SRV1 on the headquarters LAN.

This problem can be resolved by issuing the following commands on router R2:

```
router ospf 1
 area 2 stub
```

TT-B—Issue 3

Area 2 is configured as a stub area on both R1 and R2, but branch router R2 is still receiving all OSPF routes, which causes an unnecessary load on the R1–R2 WAN link and adds entries to the R2 routing table. In addition, this configuration does not conform to the requirements of the implementation plan, which states that "Each branch site will be in a separate area that is configured as totally stubby."

By making area 2 on R2 a stub area, the R2 routing table now contains all the subnets from the OSPF domain and a default route injected by R1 to 0.0.0.0/0 via R1 S0/0/0 10.1.1.1. With the default route, R2 does not need to have all the other routes in its routing table. To make area 2 totally stubby so that R2 only has a default route to R1, issue the following commands on router R1:

```
router ospf 1
  area 2 stub no-summary
```

Task 3: Trouble Ticket Lab 5-2 TT-C

Instructor note: This trouble ticket involves R3 and DLS2 issues related to mismatched OSPF hello and dead interval timers.

Step 1: Review trouble ticket Lab 5-2 TT-C.

After implementing OSPF, connectivity from the branch office on R3 (simulated by Lo0) to SRV1 is not working. A ping from PC-B to server SRV1 succeeds, but pings from R3 Lo0 to SRV1 fail.

Your task is to diagnose this problem and, if possible, resolve it. Connectivity from R3 branch office clients to server SRV1 is mandatory for this phase of the migration to be considered successful.

Step 2: Load the device trouble ticket configuration files for TT-C.

Using the procedure described in Lab 3-1, verify that the lab configuration files are present in flash. Load the proper configuration files as indicated in the Device Configuration File table.

Note: See Task 1, Step 2 for device access methods, usernames, and passwords after the configuration files have been loaded.

Device Configuration File Table

Device Name	File to Load	Notes
ALS1	Lab51-ALS1-TT-C-Cfg.txt	This file is the same as the baseline
DLS1	Lab51-DLS1-TT-C-Cfg.txt	This file contains configurations different than the baseline
DLS2	Lab51-DLS2-TT-C-Cfg.txt	This file contains configuration errors
R1	Lab51-R1-TT-C-Cfg.txt	This file contains configurations different than the baseline
R2	Lab51-R2-TT-C-Cfg.txt	This file contains configurations different than the baseline
R3	Lab51-R3-TT-C-Cfg.txt	This file contains configurations different than the baseline
SRV1	N/A	Static IP: 10.1.50.1 Default gateway: 10.1.50.254

PC-B	N/A	DHCP (release and renew after loading device configurations)
PC-C	N/A	DHCP (release and renew after loading device configurations)

Step 3: Configure SRV1 and start the syslog and TFTP servers, as described in Task 1.

Step 4: Release and renew the DHCP leases on PC-B and PC-C, as described in Task 1.

Step 5: Outline the troubleshooting approach and validation steps.

Use this space to identify your troubleshooting approach and the key steps to verify that the problem is resolved. Troubleshooting approaches to select from include: follow-the-path, spot-the-differences, bottom-up, top-down, divide-and-conquer, shoot-from-the-hip, and move-the-problem.

Note: In addition to a specific approach, you can use the generic troubleshooting process described at the beginning of Section 2 of this lab.

The follow-the-path or spot-the-differences approach can be used.

Verification steps can include:

- Users on the R3 branch office LAN (simulated by R3 Lo0) can ping server SRV1.
- R3 and DLS2 become OSPF neighbors.

Step 6: Record the troubleshooting process and configuration changes.

Note: Section 2 of this lab includes sample troubleshooting flows, useful commands, and examples of output.

Use this log to document your actions and results during the troubleshooting process. List the commands you used to gather information. As you progress, record what you think the problem might be and which actions you will take to correct the problem.

Device	Actions and Results

Device	Actions and Results

TT-C Issue 1

DLS2 is configured with hello and dead timers that do not match those on R3.

Responses will vary but could include:

- Pings from the R3 LAN client (sourced by Lo0 10.1.203.1 on R3) to server SRV1 (10.1.50.1) fail.
- Pings from the R3 LAN client (sourced by Lo0 10.1.203.1 on R3) to DLS1 Fa0/5 (10.1.2.13) fail.
- Pings from DLS2 to DLS1 succeed.
- Pings from DLS2 to SRV1 succeed.
- A check of the OSPF migration plan indicates that server SRV1 is in OSPF area 1.
- The **`show ip route`** command on DLS2 indicates that 10.1.50.0/24 is directly connected via VLAN 50, but there is no route to R3 Lo0 (10.1.203.1).
- The **`show ip route`** command on R3 indicates that no OSPF routes are present in its routing table.
- The **`show ip ospf neighbor`** command on R3 indicates that it has no OSPF neighbors.
- The **`show ip ospf neighbor`** command on DLS2 indicates that DLS1 is a neighbor (BDR neighbor ID 10.1.211.1) but not R3.
- The **`show ip ospf interface brief`** command on DLS2 indicates that interfaces Fa0/5 (link to R3), Lo0, and VLAN 200 are participating in the OSPF process and are all in area 0. Access VLANs (10, 20, 30, 50, and 100) are all in area 1.
- The **`show ip ospf interface brief`** command on R3 indicates that interfaces Fa0/1 (link to DLS2) and Lo0 are participating in the OSPF process. Fa0/1 is in area 0, and Lo0 is in area 3, per the implementation plan.
- The **`show ip ospf database router 10.1.203.1`** command on R3 indicates a link for area 3, but none for area 0.
- The **`debug ip ospf packet`** command on R3 indicates that it is receiving valid hello packets (t:1) from DLS2.
- The **`debug ip ospf adj`** command on R3 indicates no adjacency events.
- The **`debug ip ospf events`** command on R3 provides more information. It indicates that it is receiving hello packets from DLS2 (10.1.212.1) in area 0, but the hello timer parameters are mismatched. The dead interval received from DLS2 is 15 seconds, but the current R3 setting is 40 seconds. The hello interval received from DLS2 is 5 seconds, but the current R3 setting is 10 seconds. This prevents R1 and R2 from becoming neighbors.

- The **show ip ospf interface Fa0/1** (link to DLS2) command on R3 confirms that the hello interval setting is 10 seconds and the dead interval setting is 40 seconds.
- The **show ip ospf interface Fa0/5** (link to R3) command on DLS2 confirms that the hello interval setting is 5 seconds and the dead interval setting is 15 seconds.

Action: Change the hello interval and dead interval settings on DLS2 Fa0/5 to match those of R3 Fa0/1. See TT-C debrief notes for more information.

Verification: Pings from the R3 LAN client (sourced by Lo0 10.1.203.1 on R3) to server SRV1 (10.1.50.1) succeed.

Step 7: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with your instructor. The notes can include problems encountered, solutions applied, useful commands employed, alternate solutions and methods, and procedure and communication improvements.

____

____

____

____

____

____

____

Trouble Ticket TT-C Debrief—Instructor Notes

TT-C Issue 1

The problem in this ticket is caused by mismatched hello and dead timers on the link between switch DLS2 and router R3. The DLS2 switch timers were tuned to use 5 second hellos and a 15 second dead timer. R3 uses the default hello time of 10 seconds and dead time of 40 seconds. The trouble ticket introduction does not clearly state which timer values should be used. The solution presented here is to change the timers on switch DLS2 back to the default values. Changing the values on router R3 to match switch DLS2 is a valid solution as well. However, if you decide to use 5 second hellos and a 15 second dead timer on R3, you should consider changing the timers on all other interfaces in the network for consistency.

To reset the hello and dead timers to the default values on switch DLS2, issue the following commands:

```
interface FastEthernet 0/5
 default ip ospf hello-interval
 default ip ospf dead-interval
```


Task 4: Trouble Ticket Lab 5-2 TT-D

Instructor note: This trouble ticket involves issues on DLS1 and DLS2 related to OSPF passive interfaces and OSPF authentication.

Step 1: Review trouble ticket Lab 5-2 TT-D.

A recent security audit suggested that it would be best practice to secure the OSPF implementation by using MD5 authentication between the routers. Because this could complicate the implementation, it was decided that it was too late to include this now for all areas. However, to test the concept, it was decided to enable the authentication for area 0 for two devices. If the test is successful, the authentication will be added to other areas during the second phase of the implementation. If the test is not successful, a separate project will be initiated to implement the authentication.

One of your colleagues has enabled MD5 authentication for area 0 on VLAN 200, which is the link between the core switches DLS1 and DLS2 in area 0. Unfortunately, the neighbor relationship between DLS1 and DLS2 on VLAN 200 is not established.

Your task is to diagnose this problem and, if possible, resolve it. After correcting the OSPF neighbor relationship, verify that OSPF authentication between DLS1 and DLS2 is functioning correctly. You may disable the password encryption service during authentication testing.

Step 2: Load the device trouble ticket configuration files for TT-D.

Using the procedure described in Lab 3-1, verify that the lab configuration files are present in flash. Load the proper configuration files as indicated in the Device Configuration File table.

Note: See Task 1, Step 2 for device access methods, usernames, and passwords after the configuration files have been loaded.

Device Configuration File Table

Device Name	File to Load	Notes
ALS1	Lab51-ALS1-TT-D-Cfg.txt	This file is the same as the baseline
DLS1	Lab51-DLS1-TT-D-Cfg.txt	This file contains configuration errors
DLS2	Lab51-DLS2-TT-D-Cfg.txt	This file contains configuration errors
R1	Lab51-R1-TT-C-Cfg.txt	This file contains configurations different than the baseline
R2	Lab51-R2-TT-C-Cfg.txt	This file contains configurations different than the baseline
R3	Lab51-R3-TT-C-Cfg.txt	This file contains configurations different than the baseline
SRV1	N/A	Static IP: 10.1.50.1 Default gateway: 10.1.50.254
PC-B	N/A	DHCP
PC-C	N/A	DHCP

Step 3: Configure SRV1 and start the syslog and TFTP servers, as described in Task 1.

Step 4: Release and renew the DHCP leases on PC-B and PC-C, as described in Task 1.

Step 5: Outline the troubleshooting approach and validation steps.

Use this space to identify your troubleshooting approach and the key steps to verify that the problem is resolved. Troubleshooting approaches to select from include: follow-the-path, spot-the-differences, bottom-up, top-down, divide-and-conquer, shoot-from-the-hip, and move-the-problem.

Note: In addition to a specific approach, you can use the generic troubleshooting process described at the beginning of Section 2 of this lab.

The follow-the-path or spot-the-differences approach can be used.

Verification steps can include:

- Users on the R3 branch office LAN (simulated by R3 Lo0) can ping server SRV1.
- DLS1 and DLS2 become neighbors and exchange routes.
- DLS1 and DLS2 exchange OSPF authentication keys for area 0.

Step 6: Record the troubleshooting process and configuration changes.

Note: Section 2 of this lab includes sample troubleshooting flows, useful commands, and examples of output.

Use this log to document your actions and results during the troubleshooting process. List the commands you used to gather information. As you progress, record what you think the problem might be and which actions you will take to correct the problems.

Device	Actions and Results

TT-D Issue 1

The VLAN 200 interface on DLS1 is passive, so there is no communication between DLS1 and DLS2, which means they do not form an OSPF neighbor relationship.

Responses will vary but could include:

- Pings from the R3 LAN client (sourced by Lo0 10.1.203.1 on R3) to server SRV1 (10.1.50.1) fail.
- Pings from the R3 LAN client (sourced by Lo0 10.1.203.1 on R3) to DLS2 Fa0/5 (10.1.2.13) succeed.
- Pings from DLS2 to DLS1 succeed.
- Pings from DLS2 to SRV1 succeed.
- The **`show ip route`** command on DLS1 indicates that routes to R3 networks are missing from the routing table.
- The **`show ip route`** command on DLS2 indicates that routes to R1 and R2 networks are missing from the routing table.
- The **`show ip ospf neighbor`** command on DLS1 indicates that R1 is a neighbor (BDR neighbor ID 10.1.201.1) but not DLS2.
- The **`show ip ospf neighbor`** command on DLS2 indicates that R3 is a neighbor (BDR neighbor ID 10.1.203.1) but not DLS1.
- The **`show ip ospf interface brief`** command on DLS1 indicates that interface VLAN 200 is listed as an OSPF interface in area 0, and it is not down.
- The **`show ip ospf interface brief`** command on DLS2 indicates that interface VLAN 200 is listed as an OSPF interface in area 0, and it is not down.
- The **`show ip ospf interface vlan 200`** command on DLS1 indicates that no hellos are being sent on interface VLAN 200, and it is passive. The adjacent neighbor count for VLAN 200 is 0.
- The **`show ip ospf interface vlan 200`** command on DLS2 indicates that hellos are expected and the interface is not passive. The adjacent neighbor count for VLAN 200 is 0.
- The **`debug ip ospf packet`** command on DLS1 indicates that it is receiving valid hello packets (t:1) from R1.
- The **`debug ip ospf events`** command on DLS1 confirms that it is sending and receiving hello packets on Fa0/5 but not on interface VLAN 200. This prevents DLS1 and DLS2 from becoming neighbors.
- The **`debug ip ospf events`** command on DLS2 confirms that it is sending and receiving hello packets on Fa0/5 but only sending on interface VLAN 200.

Action: Configure the interface VLAN 200 command on DLS1 as non-passive. See TT-D debrief notes for more information.

Verification: Pings from the R3 LAN client (sourced by Lo0 10.1.203.1 on R3) to server SRV1 (10.1.50.1) succeed.

TT-D Issue 2

OSPF MD5 authentication with the password **ospfpa55** was configured for interface VLAN 200 on switches DLS1 and DLS2, but there is no authentication communication between the two switches.

Responses will vary but could include:

- Pings from the R3 LAN client (sourced by Lo0 10.1.203.1 on R3) to server SRV1 (10.1.50.1) succeed.
- The **`show ip route`** command on DLS1 and DLS2 indicates that all routes are present.
- The **`show ip ospf neighbor`** command on DLS1 indicates that DLS2 is a neighbor on VLAN 200.

Action: Test OSPF authentication by changing the MD5 password on switch DLS2 to observe error messages and verify that authentication is occurring. By changing the password on DLS2 to be different than DLS1, the two switches should no longer be OSPF neighbors if authentication is working correctly. Refer to TT-D debrief for more information.

- After changing the OSPF authentication password on DLS2, the **`show ip ospf neighbor`** command on DLS2 indicates that DLS1 is still a neighbor on VLAN 200, and no error messages were displayed when the DLS2 password was changed.
- The **`show ip route`** command on DLS1 and DLS2 indicates that all routes are present.
- The **`debug ip ospf packet`** command on DLS1 indicates that it is receiving valid hello packets (t:1) from R1 (no Fa0/5) and DLS1 (on VLAN 200), but the authentication flag is set to 0 (aut:0). No authentication is occurring.
- The **`show run | begin ospf 1`** command on DLS1 and DLS2 indicates that message-digest authentication for OSPF area 0 has not been enabled under the OSPF process.

Action: Enable message-digest authentication for area 0 under the OSPF 1 routing process on DLS1 and DLS2. Refer to TT-D debrief for more information.

Caution: This enables DLS1 and DLS2 to form a neighbor relationship over interface VLAN 200 but causes DLS1 to lose its neighbor relationship with R1, and DLS2 to lose its neighbor relationship with R3. Dead timer expiration messages confirm this.

Action: Enable message-digest authentication for area 0 under the OSPF 1 routing process on R1 and R3, and add the same message-digest key that was used on DLS1 and DLS2 VLAN 200 to R1 (Fa0/1) and R3 (Fa0/1). You must also configure the MD5 key on the DLS1 interface Fa0/5 and the DLS2 interface Fa0/5. This allows all routers in area 0 to authenticate. Refer to TT-D debrief for more information.

Verification: Area 0 devices DLS1, DLS2, R1, and R3 form neighbor relationships. The **`debug ip ospf packet`** command on DLS1 indicates that it is receiving valid hello packets (t:1) from R1 (on Fa0/5) and DLS2 (on VLAN 200), and the authentication flag is set to 2 (aut:2), which is MD5. Authentication is occurring.

Step 7: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with your instructor. The notes can include problems encountered, solutions applied, useful commands employed, alternate solutions and methods, and procedure and communication improvements.

____

____

____

____

____

____

____

Trouble Ticket TT-D Debrief—Instructor Notes

Two separate issues contribute to the problem in this ticket.

TT-D Issue 1

This issue is the result of the DLS1 VLAN 200 interface being passive and not allowing OSPF message exchange between DLS1 and DLS2.

The first issue is that all interfaces on DLS1 have been configured to be passive by default. Interfaces that interconnect OSPF devices must be specifically excluded from the default passive interface configuration. DLS2 is configured correctly so that this interface is non-passive. On switch DLS1, interface VLAN 200 has not been configured as an exception.

Issuing the following commands on switch DLS1 can solve this problem:

```
router ospf 1
 no passive-interface Vlan 200
```

TT-D Issue 2

This issue is the result of message-digest authentication for OSPF area 0 not being enabled on DLS1 or DLS2. (There is no authentication communication between the two switches.)

The second problem is caused by message-digest authentication for OSPF area 0 not being enabled on DLS1 or DLS2. OSPF MD5 authentication and password ospfpa55 were configured for interface VLAN 200 on switches DLS1 and DLS2, but this is not enough. Authentication must also be enabled for the area under the OSPF routing process. As a result, there is no authentication communication in the hello packets between the two switches.

Note: This problem does not cause a lack of connectivity.

To resolve this problem, you can enable message-digest authentication for OSPF area 0 on both DLS1 and DLS2:

```
router ospf 1
 area 0 authentication message-digest
```

Caution: This enables DLS1 and DLS2 to form a neighbor relationship over interface VLAN 200, but also causes DLS1 to lose its neighbor relationship with R1, and DLS2 to lose its neighbor relationship with R3. When OSPF neighbor authentication is enabled for an area, it must be enabled on all routers and interfaces participating on the area.

You can enable message-digest authentication for area 0 under the OSPF 1 routing process on R1 and R3 and add the same message-digest key that was used on DLS1 and DLS2 VLAN 200 to R1 (Fa0/1) and R3 (Fa0/1). You must also enable the MD5 key on DLS1 interface Fa0/5 and DLS2 interface Fa0/5. This allows all routers and switches in area 0 to use authentication. To enable message-digest authentication for OSPF area 0 on router R1 and R3, use the following commands:

```
router ospf 1
 area 0 authentication message-digest

interface Fa0/1
 ip ospf message-digest-key 1 md5 ospfpa55
```

Another option would be to enable the authentication on only DLS1 and DLS2, on an interface-specific basis, rather than on an area-wide basis. To implements MD5 authentication for only VLAN200, enter the following commands on DLS1 and DLS2:

```
interface vlan 200
  ip ospf authentication message-digest
```

This A debug ip ospf packet would reveal that VLAN 200 is then using MD5 authentication, but Fa0/5 still uses no authentication.

Section 2—Troubleshooting Reference Information

General Troubleshooting Process

As a general guideline, you can use the general troubleshooting process described in the course:

1. Define the problem (symptoms).
2. Gather information.
3. Analyze the information.
4. Propose a hypothesis (possible cause).
5. Test the hypothesis.
6. Eliminate or accept the hypothesis.
7. Solve the problem.
8. Document the problem.

Commands Summary

The table lists useful commands. Sample output is shown on the following pages.

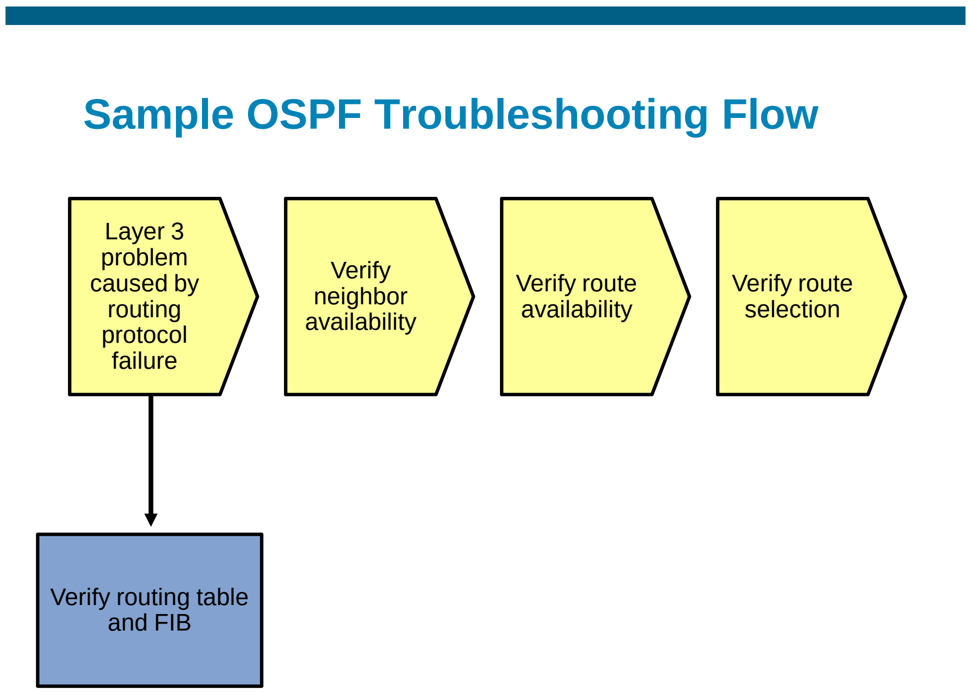
Command	Key Information Displayed
show ip route *ip-addr*	Displays the routing table information for a particular destination address.
show ip ospf interface *type/#* **show ip ospf interface brief**	Displays interfaces that are participating in the OSPF routing process. An interface does not need to 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.

Lab 5-2: Sample Troubleshooting Flows

Troubleshooting the OSPF Routing Protocol

The figure illustrates an example of a method that you could follow to diagnose and resolve problems related to the OSPF.



The usual trigger to start investigating routing protocol operation is when you are troubleshooting IP connectivity to a particular destination and you find that that the route to the destination network is missing from the routing table of one of the routers, or that a different route than expected was selected to forward the packets to that destination.

To install a route into the routing table, each router that uses a routing protocol goes through several stages:

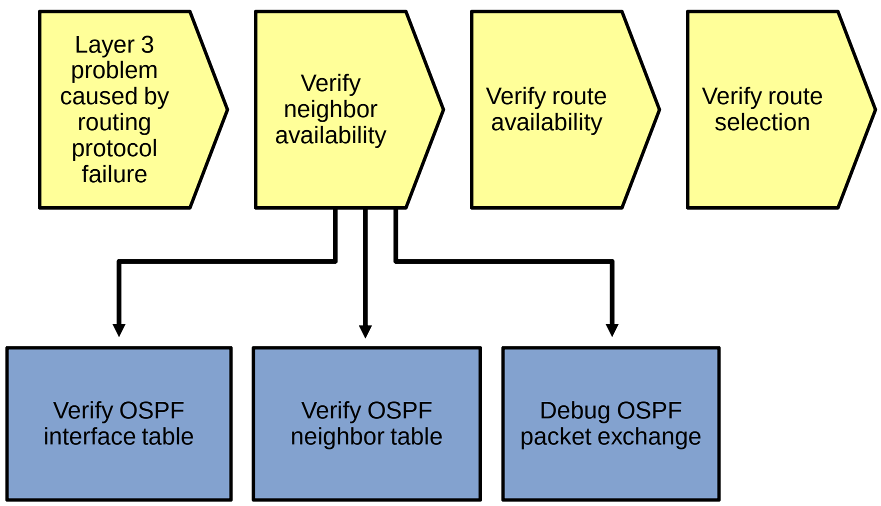
- Discovers neighbors and establishes a neighbor relationship.
- Exchanges routing information with neighbors and stores the received information in protocol-specific data structures.
- Selects the best route from the available routes and installs it in the routing table.

Errors during any of these stages can cause missing routing information or wrong routing information installed in the routing table.

The exact processes that take place, the data structures that are used, and the commands to gather information about these processes and data structures are protocol-specific, but the generic troubleshooting principles are similar for all routing protocols.

The order of verification of the different process stages is not important as long as a structured approach is used.

Sample OSPF Troubleshooting Flow



OSPF establishes and maintains neighbor relationships by using hello packets. Neighbors from which a hello packet is received are entered in the neighbor table. Subsequently, OSPF goes through the process of establishing an adjacency by transitioning through several stages in which the link-state database of the router are synchronized with its neighbor. After the completion of the database synchronization, the neighbors are considered to be fully adjacent, and both link-state updates and user traffic can be passed between the neighbors. The neighbor remains registered in the neighbor table as long as hello packets are received regularly. A neighbor is removed from the neighbor table when its dead time expires or when the interface on which the neighbor is registered goes down. The default OSPF hello timer is 10 seconds for point-to-point interfaces, such as serial interfaces running PPP or High-Level Data Link Control (HDLC), point-to-point Frame Relay or ATM subinterfaces, and broadcast-type interfaces such as Ethernet. The default dead time for these interfaces is 40 seconds. Each router advertises its hello and hold times in its hello packets, and the values must match for two routers to become neighbors.

Verify OSPF Interfaces


```
R1#show ip ospf interface brief
Interface     PID   area             IP Address/Mask    Cost  State Nbrs F/C
Lo0           1     0                10.1.201.1/32      1     P2P   0/0
Fa0/1         1     0                10.1.2.2/30        1     DR    1/1
Se0/0/0       1     2                10.1.1.1/30        64    P2P   1/1
```

Neighbors can only be discovered on an interface that has been enabled for OSPF and has not been configured as a passive interface. An interface can be enabled for OSPF in two ways. One way is if the IP address of the interface is covered by one of the **network** statements configured under the **router ospf** process, which assigns it to an area. Alternatively, an explicit **ip ospf** *process-id* **area** *area-id* command is configured on the interface, which assigns it to an area. To display a list of OSPF-enabled interfaces, use the **show ip ospf interface brief** command. This list includes interfaces that are down, which are marked as DOWN, and interfaces that have been configured as passive. However, passive interfaces are not easily recognizable in the output.

To verify whether an interface is passive, use the **show ip ospf interface** *interface-id* command. Instead of a short list, this command displays comprehensive details of the OSPF parameters and the operational state for the specified interface. This command is also useful to verify timer values, such as the hello and dead timers, which could prevent a neighbor relationship from being established.

```
R1#show ip ospf interface fastEthernet 0/1
FastEthernet0/1 is up, line protocol is up
  Internet Address 10.1.2.2/30, area 0
  Process ID 1, Router ID 10.1.201.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 10.1.201.1, Interface address 10.1.2.2
  No backup designated router on this network
  Timer intervals configured, hello 10, dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    No Hellos (Passive interface)
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

What does this mean from a troubleshooting standpoint?

If you find that an interface is not listed in the output of the **show ip ospf interface brief** command as expected, verify the **network** commands under the **router ospf** configuration.

If you find that an interface is listed but no neighbors are registered on the interface, verify that the interface was not marked as passive by issuing the **show ip ospf interface** *interface-id* command for that interface.

Verify the OSPF Neighbor Table

```
R1#show ip ospf neighbor

Neighbor ID     Pri   State          dead Time   Address         Interface
10.1.211.1        1   FULL/DR        00:00:31    10.1.2.1        FastEthernet0/1
10.1.202.1        0   FULL/  -       00:00:38    10.1.1.2        Serial0/0/0
```

```
DLS1>show ip ospf neighbor

Neighbor ID     Pri   State          dead Time   Address         Interface
```



```
10.1.212.1        1   FULL/DR       00:00:35    10.1.200.253  Vlan200
10.1.201.1        1   FULL/BDR      00:00:39    10.1.2.2      FastEthernet0/5
```

To verify that all expected neighbor relationships are operational, you can display the OSPF neighbor table using the **show ip ospf neighbor** command.

While two routers establish an adjacency and synchronize their link-state databases, they go through the following phases: Attempt (optional), Init, 2-Way, Exstart, Exchange, Loading, and Full. The expected state for a neighbor relationship is Full. The other states are transitory states, and a neighbor should not be stuck in any of those states for an extended period of time.

The only exception to this rule is a broadcast or nonbroadcast network with more than three routers. On these types of networks, a designated router (DR) and backup designated router (BDR) are elected, and all routers establish a full adjacency with the DR and BDR. Any two routers that are both not a DR or BDR (marked "DROTHER" in the **show** commands) do not transition any further than the two-way state.

In the example output, the device has two neighbors: neighbor 10.1.212.1, which is the DR, and neighbor 10.1.201.1, which is the BDR.

Debug OSPF Packet Exchange

```
DLS1#debug ip ospf packet
OSPF packet debugging is on
DLS1#
Nov  5 15:54:32.574: OSPF: rcv. v:2 t:1 l:48 rid:10.1.212.1
      aid:0.0.0.0 chk:8B98 aut:0 auk: from Vlan200
Nov  5 15:54:38.917: OSPF: rcv. v:2 t:1 l:48 rid:10.1.201.1
      aid:0.0.0.0 chk:2394 aut:0 auk: from FastEthernet0/5

R1#debug ip ospf packet
Nov  5 15:57:21.503: OSPF: rcv. v:2 t:1 l:48 rid:10.1.211.1
      aid:0.0.0.0 chk:2394 aut:0 auk: from FastEthernet0/1
Nov  5 15:57:22.443: OSPF: rcv. v:2 t:1 l:48 rid:10.1.202.1
      aid:0.0.0.2 chk:4497 aut:0 auk: from Serial0/0/0

In this highlighted sample output for R1, router ID 10.1.202.1 is in area 2
(aid:0.0.0.2) and the hello was received on interface Serial 0/0/0.
```

When an OSPF neighbor relationship is not properly established, you can use several **debug** commands to display events related to the establishment of neighbor relationships. The most elementary command is **debug ip ospf packet**, which displays the headers of OSPF packets as they are received by the router.

This command lists only received packets. Transmitted packets are not displayed. In addition, because interfaces that are not enabled for OSPF do not listen to the OSPF multicast addresses, packets are only shown for interfaces that are enabled for OSPF.

The following fields are the most relevant in the header description of these packets:

- Type (t): Lists the type of packet. Possible packet types are:
  - Type 1: Hello packets
  - Type 2: Database description packets
  - Type 3: Link-state request packets
  - Type 4: Link-state update packets
  - Type 5: Link-state acknowledgement packets
- Router ID (rid): Lists the ID of the sending router. This is usually not the same as the source address of the packet.

- Area ID (aid): The 32-bit area ID of the sending router is represented in dotted-decimal IP address format.
- Authentication (aut): Lists the authentication type. Possible types are:
  - Type 0: No (null) authentication
  - Type 1: Cleartext authentication
  - Type 2: Message Digest 5 (MD5) authentication
- Interface (from): Lists the interface on which the packet was received.

Note: Only successfully received and accepted packets are listed in the output of the **`debug ip ospf packet`** command. If there is a mismatch between essential parameters in the header, such as the area ID, authentication type, or authentication data between this router and the neighbor, the packets from that neighbor are silently discarded and not listed in the output of the debug.

The usefulness of this command for troubleshooting is limited because it does not display sent packets, packets received on an interface that is not enabled for OSPF, or packets that carry mismatched header information. However, because of the relatively limited amount of generated output, it can be used to confirm the reception of correct hellos from a neighbor.

Debug OSPF Adjacencies

In the following debug outputs, DLS1 interface Fa0/5 (link to R1) is shutdown and the OSPF adjacency terminates. When the DLS1 Fa0/5 interface is reactivated, an election occurs, DLS1 becomes the DR again and builds LSAs to send to R1. DLS1 and R1 establish a neighbor relationship and exchange OSPF database information.

```
DLS1#debug ip ospf adj
OSPF adjacency events debugging is on

DLS1(config)#interface fa0/5
DLS1(config-if)#shut

Nov  5 16:04:10.619: OSPF: Interface FastEthernet0/5 going Down
Nov  5 16:04:10.619: OSPF: 10.1.211.1 address 10.1.2.1 on FastEthernet0/5 is dea
d, state DOWN
Nov  5 16:04:10.619: OSPF: Neighbor change Event on interface FastEthernet0/5
Nov  5 16:04:10.619: OSPF: DR/BDR election on FastEthernet0/5
Nov  5 16:04:10.619: OSPF: Elect BDR 10.1.201.1
Nov  5 16:04:10.619: OSPF: Elect DR 10.1.201.1
Nov  5 16:04:10.619: OSPF: Elect BDR 10.1.201.1
Nov  5 16:04:10.619: OSPF: Elect DR 10.1.201.1
Nov  5 16:04:10.619
DLS1(config-if)#:        DR: 10.1.201.1 (Id)   BDR: 10.1.201.1 (Id)
Nov  5 16:04:10.619: OSPF: Flush network LSA immediately
Nov  5 16:04:10.619: OSPF: Remember old DR 10.1.211.1 (id)
Nov  5 16:04:10.619: OSPF: 10.1.201.1 address 10.1.2.2 on FastEthernet0/5 is dea
d, state DOWN
Nov  5 16:04:10.619: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.201.1 on FastEthernet0/
5 from FULL to DOWN, Neighbor Down: Interface down or detached
Nov  5 16:04:10.619: OSPF: Neighbor change Event on interface FastEthernet0/5
Nov  5 16:04:10.619: OSPF: DR/BDR election on FastEthernet0/5
Nov  5 16:04:10.619: OSPF: Elect BDR 0.0.0.0
Nov  5 16:04:10.619: OSPF: Elect DR 0.0.0.0
Nov  5 16:04:10.619:        DR: none    BDR: none
Nov  5 16:04:10.619: OSPF: Remember old DR 10.1.201.1 (id)
Nov  5 16:04:10.619: OSPF: [change notify] will poll [cnt 11] interface status f
or FastEthernet0/5
```



```
Nov  5 16:04:11.122: OSPF: We are not DR to build Net Lsa for interface FastEthe
rnet0/5
Nov  5 16:04:11.122: OSPF: Build network LSA for FastEthernet0/5, router ID 10.1
.211.1
Nov  5 16:04:11.122: OSPF: Build router LSA for area 0, router ID 10.1.211.1, se
q 0x80000012, process 1
Nov  5 16:04:12.599: %LINK-5-CHANGED: Interface FastEthernet0/5, changed state t
o administratively down
Nov  5 16:04:13.606: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEtherne
t0/5, changed state to down
Nov  5 16:04:20.628: OSPF: will poll [count 10] interface status for FastEtherne
t0/5
Nov  5 16:04:30.636: OSPF: will poll [count 9] interface status for FastEthernet
0/5
Nov  5 16:04:40.821: OSPF: will poll [count 8] interface status for FastEthernet
0/5
Nov  5 16:04:50.830: OSPF: will poll [count 7] interface status for FastEthernet
0/5
Nov  5 16:05:00.838: OSPF: will poll [count 6] interface status for FastEthernet
0/5
Nov  5 16:05:10.839: OSPF: will poll [count 5] interface status for FastEthernet
0/5
Nov  5 16:05:20.847: OSPF: will poll [count 4] interface status for FastEthernet
0/5
Nov  5 16:05:30.856: OSPF: will poll [count 3] interface status for FastEthernet
0/5
Nov  5 16:05:40.865: OSPF: will poll [count 2] interface status for FastEthernet
0/5
Nov  5 16:05:50.865: OSPF: will poll [count 1] interface status for FastEthernet
0/5

DLS1(config)#interface fa0/5
DLS1(config-if)#no shut

Nov  5 16:05:59.800: %LINK-3-UPDOWN: Interface FastEthernet0/5, changed state to
 up
Nov  5 16:05:59.800: OSPF: Interface FastEthernet0/5 going Up
Nov  5 16:05:59.800: OSPF: [change notify] will poll [cnt 11] interface status f
or FastEthernet0/5
Nov  5 16:06:00.303: OSPF: Build router LSA for area 0, router ID 10.1.211.1, se
q 0x80000013, process 1
Nov  5 16:06:00.807: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEtherne
t0/5, changed state to up
Nov  5 16:06:09.800: OSPF: will poll [count 10] interface status for FastEtherne
t0/5
Nov  5 16:06:09.800: OSPF: 2 Way Communication to 10.1.201.1 on FastEthernet0/5,
 state 2WAY
Nov  5 16:06:19.809: OSPF: will poll [count 9] interface status for FastEthernet
0/5
Nov  5 16:06:29.809: OSPF: will poll [count 8] interface status for FastEthernet
0/5
Nov  5 16:06:39.809: OSPF: end of Wait on interface FastEthernet0/5
Nov  5 16:06:39.809: OSPF: DR/BDR election on FastEthernet0/5
Nov  5 16:06:39.809: OSPF: Elect BDR 10.1.211.1
Nov  5 16:06:39.809: OSPF: Elect DR 10.1.211.1
Nov  5 16:06:39.809: OSPF: Elect BDR 10.1.201.1
Nov  5 16:06:39.809: OSPF: Elect DR 10.1.211.1
Nov  5 16:06:39.809:        DR: 10.1.211.1 (Id)   BDR: 10.1.201.1 (Id)
```



```
Nov  5 16:06:39.809: OSPF: Send DBD to 10.1.201.1 on FastEthernet0/5 seq 0x192E
opt 0x52 flag 0x7 len 32
Nov  5 16:06:39.818: OSPF: will poll [count 7] interface status for FastEthernet
0/5
Nov  5 16:06:40.313: OSPF: No full nbrs to build Net Lsa for interface FastEther
net0/5
Nov  5 16:06:42.209: OSPF: Rcv DBD from 10.1.201.1 on FastEthernet0/5 seq 0x8AC
opt 0x52 flag 0x7 len 32  mtu 1500 state EXSTART
Nov  5 16:06:42.209: OSPF: First DBD and we are not SLAVE
Nov  5 16:06:44.818: OSPF: Send DBD to 10.1.201.1 on FastEthernet0/5 seq 0x192E
opt 0x52 flag 0x7 len 32
Nov  5 16:06:44.818: OSPF: Retransmitting DBD to 10.1.201.1 on FastEthernet0/5 [
1]
Nov  5 16:06:44.818: OSPF: Rcv DBD from 10.1.201.1 on FastEthernet0/5 seq 0x192E
 opt 0x52 flag 0x2 len 432  mtu 1500 state EXSTART
Nov  5 16:06:44.818: OSPF: NBR Negotiation Done. We are the MASTER
Nov  5 16:06:44.818: OSPF: Send DBD to 10.1.201.1 on FastEthernet0/5 seq 0x192F
opt 0x52 flag 0x3 len 412
Nov  5 16:06:44.818: OSPF: Rcv DBD from 10.1.201.1 on FastEthernet0/5 seq 0x192F
 opt 0x52 flag 0x0 len 32  mtu 1500 state EXCHANGE
Nov  5 16:06:44.818: OSPF: Send DBD to 10.1.201.1 on FastEthernet0/5 seq 0x1930
opt 0x52 flag 0x1 len 32
Nov  5 16:06:44.818: OSPF: Send LS REQ to 10.1.201.1 length 24 LSA count 2
Nov  5 16:06:44.826: OSPF: Rcv LS REQ from 10.1.201.1 on FastEthernet0/5 length
36 LSA count 1
Nov  5 16:06:44.826: OSPF: Send UPD to 10.1.2.2 on FastEthernet0/5 length 64 LSA
 count 1
Nov  5 16:06:44.826: OSPF: Rcv DBD from 10.1.201.1 on FastEthernet0/5 seq 0x1930
 opt 0x52 flag 0x0 len 32  mtu 1500 state EXCHANGE
Nov  5 16:06:44.826: OSPF: Exchange Done with 10.1.201.1 on FastEthernet0/5
Nov  5 16:06:44.826: OSPF: Rcv LS UPD from 10.1.201.1 on FastEthernet0/5 length
108 LSA count 2
Nov  5 16:06:44.826: OSPF: No full nbrs to build Net Lsa for interface FastEther
net0/5
Nov  5 16:06:44.826: OSPF: Build network LSA for FastEthernet0/5, router ID 10.1
.211.1
Nov  5 16:06:44.826: OSPF: Synchronized with 10.1.201.1 on FastEthernet0/5, stat
e FULL
Nov  5 16:06:44.826: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.201.1 on FastEthernet0/
5 from LOADING to FULL, Loading Done
```

The **debug ip ospf adj** command is useful for troubleshooting OSPF neighbor-related events. It displays the different stages of the OSPF adjacency-building process as two neighbors transition from the init state to the full state. This command can be helpful in diagnosing problems in which a neighbor relationship is stuck in a particular stage of the adjacency-building process.

This command 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, however, reveal other mismatches in hello parameters, such as hello timers, subnet masks, or flags.

Debug OSPF Events

DLS2#**debug ip ospf events**

```
*Nov  5 03:03:11.043: OSPF: Send hello to 224.0.0.5 area 0 on FastEthernet0/5 fr
om 10.1.2.13
DLS2#
*Nov  5 03:03:13.551: OSPF: Send hello to 224.0.0.5 area 0 on Vlan200 from 10.1.
200.253
```



```
*Nov  5 03:03:13.845: OSPF: Rcv hello from 10.1.211.1 area 0 from Vlan200 10.1.2
00.252
*Nov  5 03:03:13.845: OSPF: End of hello processing
DLS2#
*Nov  5 03:03:16.051: OSPF: Send hello to 224.0.0.5 area 0 on FastEthernet0/5 fr
om 10.1.2.13
*Nov  5 03:03:16.286: OSPF: Rcv hello from 10.1.203.1 area 0 from FastEthernet0/
5 10.1.2.14
*Nov  5 03:03:16.286: OSPF: Mismatched hello parameters from 10.1.2.14
*Nov  5 03:03:16.286: OSPF: dead R 40 C 15, hello R 10 C 5  Mask R 255.255.255.2
52 C 255.255.255.252
DLS2#

DLS2#undebug all
All possible debugging has been turned off
DLS2#
*Nov  5 03:03:28: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.203.1 on FastEthernet0/5 f
rom FULL to DOWN, Neighbor Down: dead timer expired
```

A third **debug** command that can be useful in troubleshooting the establishment of OSPF neighbor relationships is **`debug ip ospf events`**. This command displays the same information that is displayed by the **`debug ip ospf adj`** command, but it also displays the transmission and reception of hello packets and reports mismatches in the hello parameters.

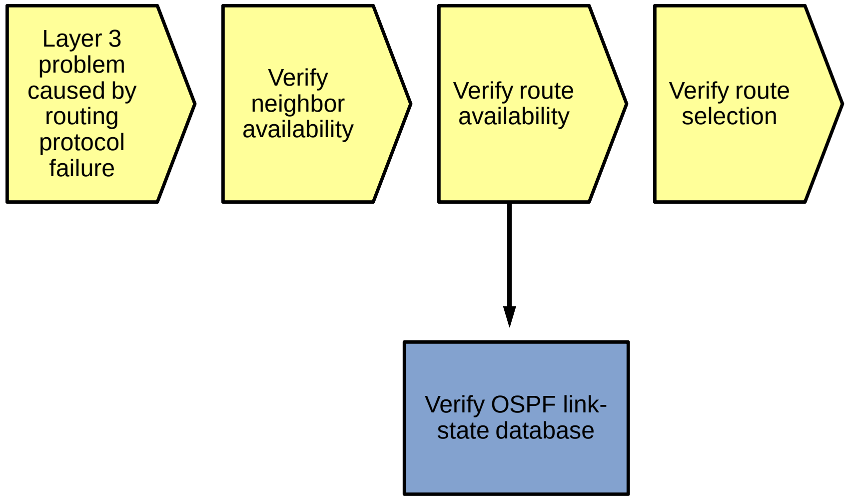
Confirming the transmission of hello packets by using this command can be useful because the **`debug ip ospf packet`** or **`debug ip ospf adj`** commands do not display the transmission of hello packets.

You can also use this command to display the reception of invalid hello packets. If there is a mismatch between the neighbors in the hello parameters that prevents the neighbor relationship from forming, this command displays the type of parameter mismatch and the value of the mismatched parameters. It displays mismatches for the following parameters:

- Hello and dead timers
- Area ID
- Subnet and subnet mask
- Authentication type and authentication data
- Flags that signify the area type, such as stub or not-so-stubby area (NSSA)

Because this command displays more events, it is often better to first enable the **`debug ip ospf adj`** command and only use the **`debug ip ospf event`** command if you did not get the information you need.

Sample OSPF Troubleshooting Flow



After you have verified that neighbor relationships have been established as expected, verify that the network topology information for the destination network that you are troubleshooting has been received correctly and entered into the OSPF link-state database.

The presence or absence of specific topology information in the OSPF link-state database can help isolate the source of the problem.

Verify the OSPF Link-State Database for Intra-Area Routes

```
DLS2#show ip ospf database router 10.1.212.1

            OSPF Router with ID (10.1.212.1) (Process ID 1)

                Router Link States (area 0)

  LS age: 60
  Options: (No TOS-capability, DC)
  LS Type: Router Links
  Link State ID: 10.1.212.1
  Advertising Router: 10.1.212.1
  LS Seq Number: 80000012
  Checksum: 0x592C
  Length: 60
  area Border Router
  Number of Links: 3

    Link connected to: a Stub Network
     (Link ID) Network/subnet number: 10.1.212.1
     (Link Data) Network Mask: 255.255.255.255
      Number of TOS metrics: 0
       TOS 0 Metrics: 1

    Link connected to: a Transit Network
     (Link ID) Designated Router address: 10.1.2.13
     (Link Data) Router Interface address: 10.1.2.13
```

```
      Number of TOS metrics: 0
       TOS 0 Metrics: 1
```

To decide which information to look for in the link-state database, you first need to discern in which type of route you are interested. If the destination network that you are troubleshooting is in the same area as the router from which you are troubleshooting, you know that the path to this destination network was derived from the type-1 and type-2 LSAs in the database of that area. To begin with, you can verify whether the directly connected routers properly advertise the destination network. To do this, display the router (type-1) for the connected routers by issuing the **show ip ospf database router** *router-id* command for these routers. To troubleshoot OSPF effectively, it is necessary to know the router IDs of all routers in your network, because these are used to identify a router in many of the OSPF **show** commands.

As part of the type-1 router LSA for a specific router, all subnets corresponding to a point-to-point link, loopback interface, or nontransit broadcast network (Ethernet) are listed as stub networks. If the target network is missing in this list, this indicates that the interface on the advertising router has not been enabled for OSPF.

In the example above subnet 10.1.212.1 is advertised by router 10.1.212.1 in area 0.

For transit networks, such as an Ethernet LAN with multiple routers attached, a link to the DR for the segment is listed. This points to the type-2 network LSA that contains the full topology information for the segment.

In the example above, this router is connected to a transit network with router 10.1.2.13 as the DR. Note that this IP address is the interface IP address of the DR, not the router ID.

```
DLS1#show ip ospf database network 10.1.2.13

            OSPF Router with ID (10.1.211.1) (Process ID 1)

                Net Link States (area 0)

  Routing Bit Set on this LSA
  LS age: 695
  Options: (No TOS-capability, DC)
  LS Type: Network Links
  Link State ID: 10.1.2.13 (address of Designated Router)
  Advertising Router: 10.1.212.1
  LS Seq Number: 80000004
  Checksum: 0xDBAA
  Length: 32
  Network Mask: /30
        Attached Router: 10.1.212.1
        Attached Router: 10.1.203.1
```

To display full information about a transit LAN, issue the **show ip ospf database network** *designated-router* command, using the IP address of the DR that was listed in the type-1 router LSA for one of the routers connected to the transit LAN. In the type-2 LSA, the DR advertises the subnet mask and connected routers for the segment. The connected routers are listed by their router ID values.

In the example above, a subnet mask of /30 is advertised for the transit LAN, and two connected routers are listed.

Verify the OSPF Link-State Database for Inter-Area Routes

```
DLS1>show ip ospf database summary 10.1.203.1

            OSPF Router with ID (10.1.211.1) (Process ID 1)

                Summary Net Link States (area 0)

  LS age: 577
  Options: (No TOS-capability, DC, Upward)
```



```
  LS Type: Summary Links(Network)
  Link State ID: 10.1.203.1 (summary Network Number)
  Advertising Router: 10.1.203.1
  LS Seq Number: 8000000B
  Checksum: 0x2A58
  Length: 28
  Network Mask: /32
        TOS: 0  Metric: 1
```

If the destination network that you are troubleshooting is in a different area than the area of the router from which you are troubleshooting, the router will not learn about this network through type-1 and type-2 LSAs because these are only used for intra-area routes. OSPF inter-area routes are calculated based on type-3 LSAs that are generated by the Area Border Routers (ABRs) for the area.

To verify the availability of a specific target network in a different area, you can use the **`show ip ospf database summary`** *`subnet`* command, where *`subnet`* is the subnet IP address of the prefix in which you are interested.

The type-3 summary LSA contains the subnet, mask, and cost of the targeted subnet and also lists the router ID of the ABR. If multiple ABRs are advertising the same network, all entries are listed.

In the example above, subnet 10.1.203.1/32 is advertised with a cost of 1 by ABR 10.1.203.1. The cost advertised by the ABR is the cost from the advertising ABR to the target network. When executing the Shortest Path First (SPF) algorithm, the router calculates its own cost to reach the ABR within the area and adds that to the cost advertised by the ABR.

If you do not find an entry for the target network, the next step is to connect to the ABR that you expected to be advertising the route and verify if the route is available there.

Verify the OSPF Link-State Database for External Routes

```
DLS1#show ip ospf database external 10.1.1.0

            OSPF Router with ID (10.1.211.1) (Process ID 1)

                Type-5 AS External Link States

  Routing Bit Set on this LSA
  LS age: 1196
  Options: (No TOS-capability, DC)
  LS Type: AS External Link
  Link State ID: 10.1.1.0 (External Network Number )
  Advertising Router: 10.1.201.1
  LS Seq Number: 80000006
  Checksum: 0x6804
  Length: 36
  Network Mask: /30
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 100
        Forward Address: 0.0.0.0
        External Route Tag: 0
```

If the destination network that you are troubleshooting did not originate in the OSPF network but was redistributed from a different source, the OSPF router learns about this network through type-5 external routes that are injected into the OSPF database by an Autonomous System Boundary Router (ASBR).

To verify the availability of a specific type-5 external LSA in the OSPF database, issue the **`show ip ospf database external`** *`subnet`* command, where *`subnet`* is the subnet IP address of the prefix in which you are interested.

The type-5 summary LSA contains the subnet, mask, metric type, and cost of the targeted subnet. In addition, it lists the router ID of the advertising ASBR. If multiple ASBRs are advertising the same network, all entries are listed.

In the example above, subnet 10.1.1.0/30 is advertised with a cost of 100 as a metric-type 2 external route by ASBR 10.1.201.1.

If you do not find an entry for the target network, the next step is to connect to the ASBR that you expected to be advertising the route and verify if the route is available. If the route is available but not advertised by the ASBR, troubleshoot the route redistribution process on that router.

```
DLS1#show ip ospf database router 10.1.201.1

            OSPF Router with ID (10.1.211.1) (Process ID 1)

                Router Link States (area 0)

  Routing Bit Set on this LSA
  LS age: 391
  Options: (No TOS-capability, DC)
  LS Type: Router Links
  Link State ID: 10.1.201.1
  Advertising Router: 10.1.201.1
  LS Seq Number: 8000000E
  Checksum: 0x1163
  Length: 48
  AS Boundary Router
  Number of Links: 2

<Output omitted>
```

Instead of connecting to the ASBR, the OSPF database can also be used to verify if any form of redistribution has been configured on the router that is supposed to be an ASBR. If that router is in the same area as the router from which you are troubleshooting, you can inspect the type-1 router LSA for the ASBR and verify that it advertises itself as an ASBR.

In the example above, the router 10.1.201.1 announces its ASBR status in its type-1 LSA. If the router does not advertise its ASBR status in its type-1 LSA, this indicates that redistribution has not been configured correctly on that router.

```
DLS1#show ip ospf database asbr-summary 10.1.201.1

            OSPF Router with ID (10.1.211.1) (Process ID 1)

                Summary ASB Link States (area 1)

  LS age: 723
  Options: (No TOS-capability, DC, Upward)
  LS Type: Summary Links(AS Boundary Router)
  Link State ID: 10.1.201.1 (AS Boundary Router address)
  Advertising Router: 10.1.211.1
  LS Seq Number: 8000000D
  Checksum: 0xF583
  Length: 28
  Network Mask: /0
        TOS: 0  Metric: 1
```

If the ASBR is not in the same area as the router from which you are troubleshooting, you do not have its type-1 LSA in the database of the router. As a result, you cannot verify its ASBR status by displaying the type-1 LSA. However, if an ASBR is available in a different area, the ABRs for the area generate a type-4 summary AS

Boundary (ASB) entry to announce the availability of the ASBR. The presence or absence of a type-4 entry can also yield a clue about the operation of the redistribution.

You can use the **`show ip ospf database asbr-summary`** *`router-id`* command to verify if a type-4 summary ASB LSA exists for the ASBR with the specified router ID.

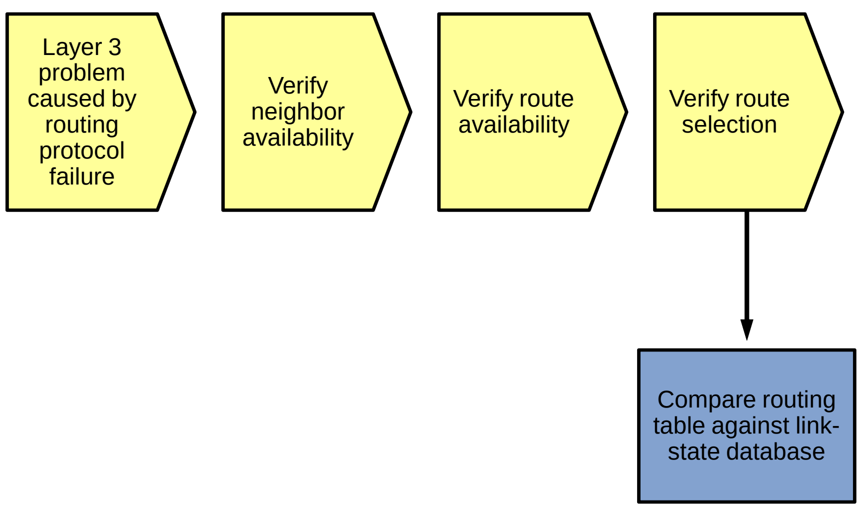
In the example above, ABR 10.1.211.1 announces the availability of ASBR 10.1.201.1.

```
DLS1#show ip ospf border-routers

OSPF Process 1 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 10.1.212.1 [1] via 10.1.200.253, Vlan200, ABR, area 0, SPF 5
i 10.1.201.1 [1] via 10.1.2.2, FastEthernet0/5, ASBR, area 0, SPF 5
i 10.1.203.1 [2] via 10.1.200.253, Vlan200, ABR, area 0, SPF 5
```

During the execution of the SPF algorithm, a router combines the information from the various LSAs that contain information about ABR and ASBR status and calculates the shortest paths to each ABR and ASBR. You can view the result of this calculation with the **`show ip ospf border-routers`** command.

In the example above, area 0 has two ABRs: 10.1.212.1 and 10.1.203.1. The cost to reach ABR 10.1.212.1 is 1, as can be seen from the number in the square brackets. The cost to reach ABR 10.1.203.1 is 2. The cost to reach ASBR 10.1.201.1 is 1. This cost is important to know because it is added to the cost advertised by these routers in their type-3 LSAs to obtain the total cost to the destination network.

Sample OSPF Troubleshooting Flow



If all appropriate entries are available in the OSPF link-state database, these should result in correct routes in the IP routing table after calculation of the SPF algorithm. Unfortunately, the results of the SPF algorithm for each individual route cannot be directly verified.

Keep in mind that OSPF competes with other routing sources to install routes in the routing table. Therefore, an OSPF route might not be installed in the routing table because a route with a better administrative distance from a different source is available.

Verify the MTU between OSPF Neighbors

Maximum Transmission Unit (MTU) mismatch between two OSPF neighbors is common when connecting together two multilayer switches of a different type (for example 3550 and 3560) or when interconnecting a multilayer switch with a router. Multilayer switches often have the system MTU set to 1504 bytes while routers typically use an MTU of 1500 bytes. An MTU mismatch usually causes two OSPF neighbors to remain stuck in EXSTART/EXCHANGE state, failing to create full adjacency.

Changes to the system MTU are made using the **`system mtu`** *`mtu-size`* command. The routing MTU can be changed using the **`system mtu routing`** *`mtu-size`* command. System MTU on a Cisco Catalyst 3560 switch can range from 1500-1998 bytes.

Note: Changes to MTU size will not take effect until the next reload is done.

MTU settings can be verified using the **`show interfaces`** or the **`show system mtu`** commands:

```
DLS2#show interfaces fastEthernet 0/5
FastEthernet0/5 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0017.5a53.a3c2 (bia 0017.5a53.a3c2)
  Description: FE to R3
  Internet address is 10.1.2.13/30
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255

DLS2#show system mtu

System MTU size is 1500 bytes
System Jumbo MTU size is 1500 bytes
Routing MTU size is 1500 bytes
```

OSPF Neighbor status can be verified using the **`show ip ospf neighbor`** command. In the example shown below, the system and system routing MTU for Layer 3 switch DLS2 has been changed to 1504 bytes. The MTU of the neighbors, DLS1 (10.1.211.1) and R3 (10.1.203.1) is set to the default of 1500 bytes.

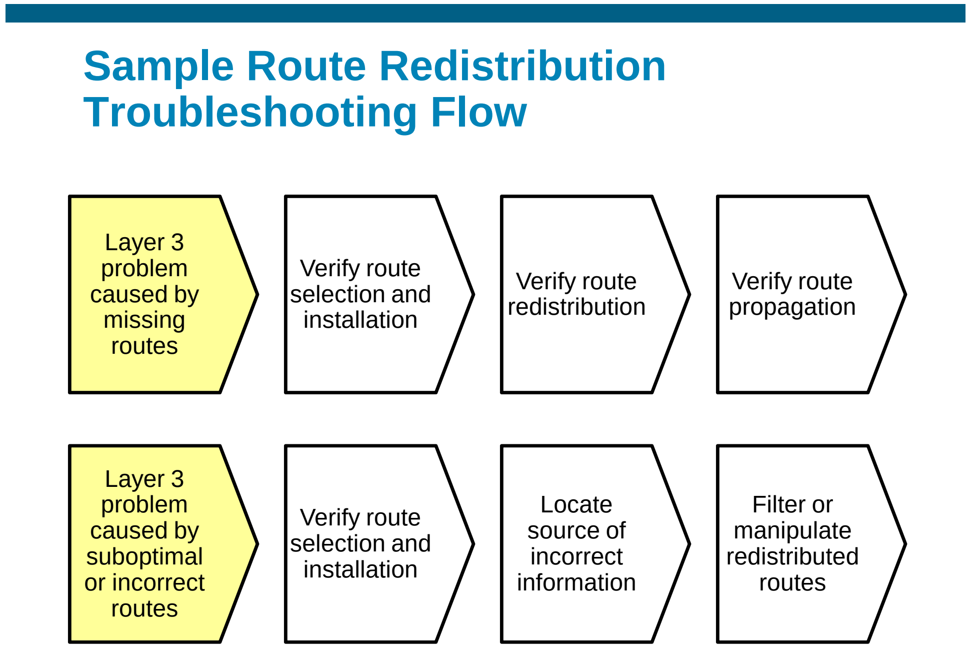
```
DLS2#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.1.211.1        1   EXSTART/BDR     00:00:38    10.1.200.252    Vlan200
10.1.203.1        1   EXSTART/BDR     00:00:37    10.1.2.14       FastEthernet0/5
```

Console messages:

```
DLS2#
%OSPF-5-ADJCHG: Process 1, Nbr 10.1.203.1 on FastEthernet0/5 from DOWN to
DOWN, Neighbor Down: Ignore timer expired
DLS2#
%OSPF-5-ADJCHG: Process 1, Nbr 10.1.211.1 on Vlan200 from EXSTART to DOWN,
Neighbor Down: Too many retransmissions
```

Troubleshooting Route Redistribution

The figure illustrates an example of a method that you can use to diagnose and resolve problems related to route redistribution.



When do you start troubleshooting route redistribution?

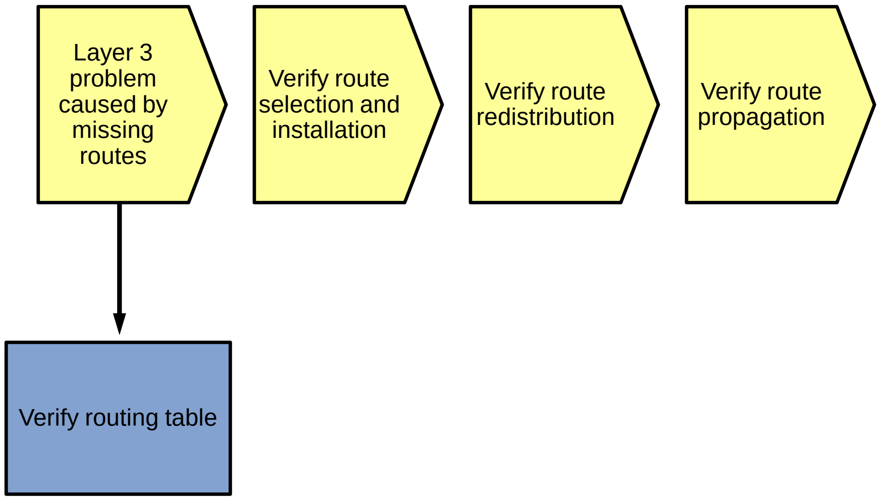
There are two major reasons to start troubleshooting the route redistribution. The first reason is when you are experiencing IP connectivity problems in an environment in which information from a specific routing domain is redistributed into a different routing domain and the connectivity problem is caused by a route from the source routing domain that is not available on one or more of the routers participating in the destination routing domain. In this scenario, the cause of the problem is that the exchange of routing information between the source routing domain and the destination routing domain is not working correctly.

Note: In this section, the terms *source* and *destination* are used to indicate the source and destination of the routing information, not the source and destination of a traffic flow.

The second reason to start troubleshooting route redistribution is if you are experiencing IP connectivity problems caused by the use of incorrect routing information by some of the routers in a network that use route redistribution. This behavior could be caused by routing information feedback or improper route selection.

Sample troubleshooting flows for each of these scenarios are provided in this section.

Sample Route Redistribution Troubleshooting Flow



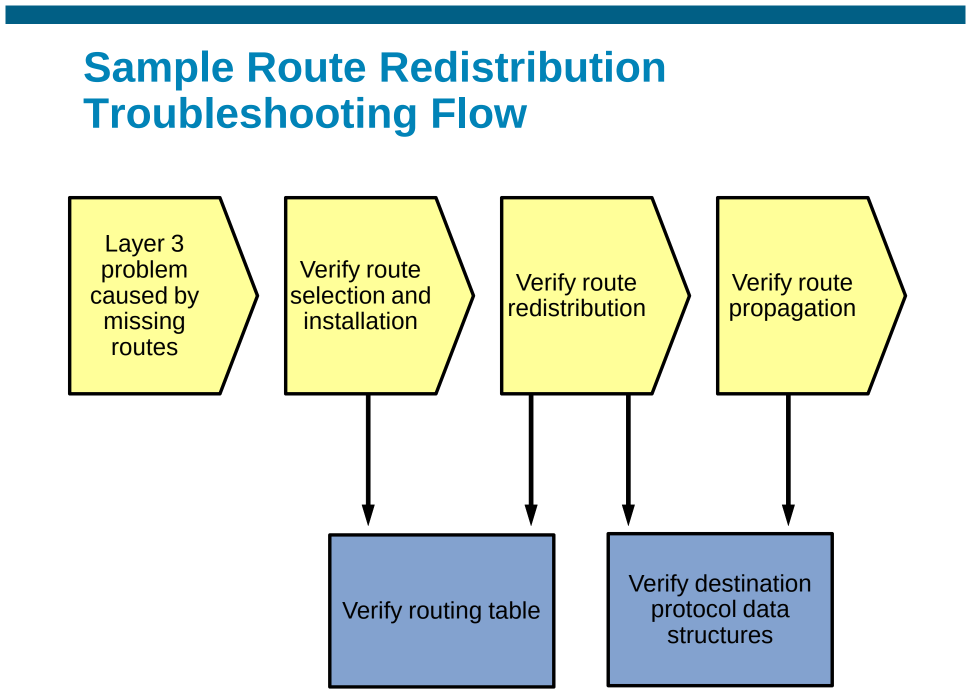
The first scenario in which you start troubleshooting route redistribution is when redistribution is configured and you are troubleshooting connectivity problems to a network in the source routing domain from a router in the destination routing domain. This type of problem is usually encountered during a generic IP connectivity troubleshooting process when a route is discovered missing from the routing table on one of the routers in the destination routing domain while the route is present in the routing tables of the routers in the source routing domain.

Troubleshooting redistribution consists of troubleshooting four generic areas:

- Source routing protocol
- Route selection and installation
- Redistribution
- Destination protocol

In this scenario, the reason to start troubleshooting the redistribution is when the route is available in the source routing domain but not in the destination routing domain. Therefore, the first step has already been taken at this point. If the route is not available everywhere in the source routing domain to begin with, there is no reason to start troubleshooting redistribution, but you should initiate a troubleshooting process for the source routing protocol first.

Therefore, we will start at the second step: troubleshooting route selection and installation.



There are not many tools that are specifically targeted at troubleshooting the redistribution process. The redistribution process takes routes from the routing table after they have been installed by the source routing protocol and then injects them into the destination protocol's data structures. Therefore, the main tools that are available to track this flow of information are the commands that allow you to examine the routing table and the destination protocol data structures.

After you have verified that the routes are injected into the destination protocol's data structures, you have finished troubleshooting the actual redistribution process. If the routes are not properly propagated by the destination protocol, initiate a troubleshooting process for the destination protocol.

The **show ip route 10.1.202.1 255.255.255.255** command on R1 indicates that the route is known via EIGRP 1 and is redistributing via OSPF, but it is not being advertised by OSPF.

```
R1#show ip route 10.1.202.1 255.255.255.255
Routing entry for 10.1.202.1/32
  Known via "eigrp 1", distance 90, metric 2297856, type internal
  Redistributing via eigrp 1, ospf 1
  Last update from 10.1.1.2 on Serial0/0/0, 07:02:16 ago
  Routing Descriptor Blocks:
  * 10.1.1.2, from 10.1.1.2, 07:02:16 ago, via Serial0/0/0
      Route metric is 2297856, traffic share count is 1
      Total delay is 25000 microseconds, minimum bandwidth is 1544 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
```

The **show ip route 10.1.203.1 255.255.255.255** command on R1 indicates that the route is known via EIGRP 1 and is redistributing via EIGRP. It is also being advertised by EIGRP 1.

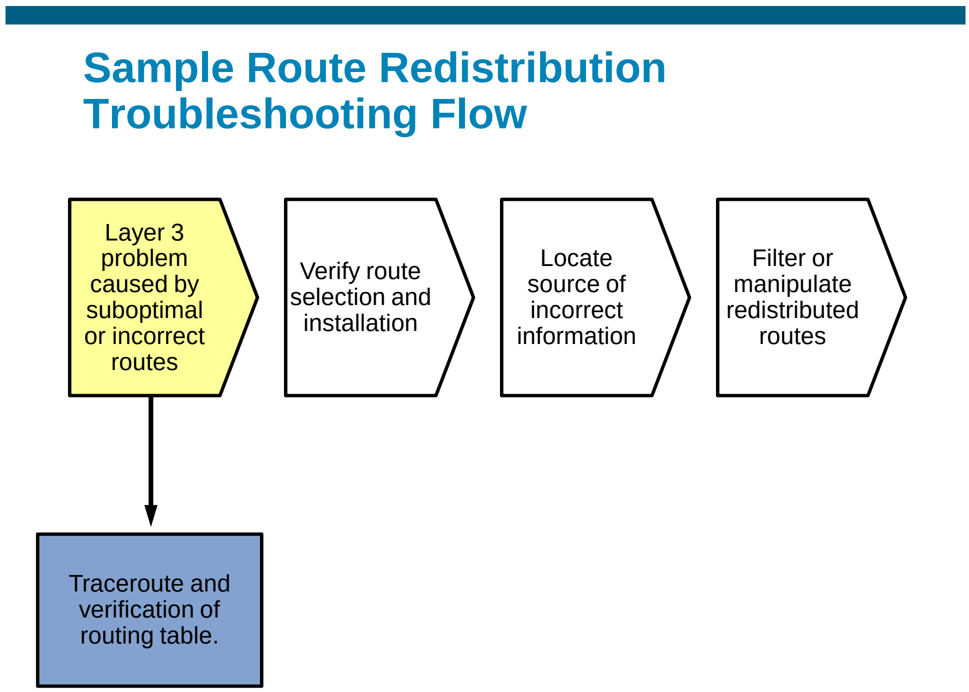
```
R1#show ip route 10.1.203.1 255.255.255.255
Routing entry for 10.1.203.1/32
  Known via "ospf 1", distance 110, metric 4, type inter area
  Redistributing via eigrp 1
  Advertised by eigrp 1 metric 1544 2000 255 1 1500
  Last update from 10.1.2.1 on FastEthernet0/1, 07:13:32 ago
  Routing Descriptor Blocks:
```



```
  * 10.1.2.1, from 10.1.203.1, 07:13:32 ago, via FastEthernet0/1
      Route metric is 4, traffic share count is 1
```

The best tool available in troubleshooting redistribution problems is the **`show ip route`** *`network mask`* command. Routes that are being redistributed and advertised to other routers by the destination protocol are marked with a line starting with "Advertised by" and then lists the destination protocol and any parameters configured on the redistribution statement, such as configured metrics and metric type.

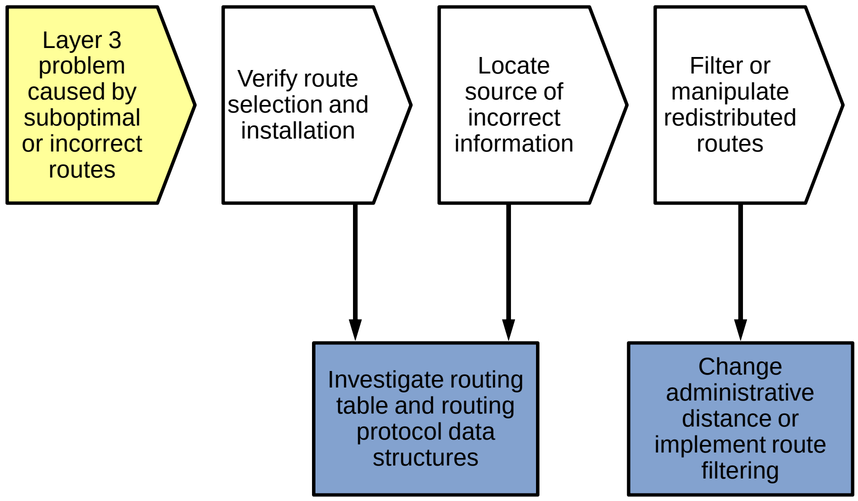
What makes this command useful is that it takes into account any route maps or distribute lists that are applied to the redistribution.



The second common scenario that might lead you to start troubleshooting route redistribution is when you discover that traffic is using unexpected suboptimal routes to reach certain destinations or that traffic enters a routing loop. This is often discovered while troubleshooting IP connectivity to a certain destination and using the **`show ip route`** and **`traceroute`** commands to track the flow of traffic. When you are redistributing routing information between routing protocols, you have to be aware that improper route selection or routing feedback can cause suboptimal paths to be used or traffic to enter a routing loop. Whenever you spot unexpected routing behavior in a network that uses redistribution, consider routing feedback or improper route selection as a possible cause.

A typical symptom of a redistribution problem is when the expected route is available on the router that you are troubleshooting, but it is not selected as the best route in the routing table. A route from a different protocol or a route of the same protocol but originated from a different source is selected as the best route and installed in the routing table.

Sample Route Redistribution Troubleshooting Flow



The first question to ask at this point is if the route is only improperly selected. In other words, you expected this route to be present but did not want it to be selected as the best route. If this is the case, you can manipulate the route selection process by changing the administrative distance. This can be done for all routes learned via a particular routing protocol or selectively using an access list.

If the route was not only improperly selected but should not have been present at all in the routing protocol data structures in this router, you must track the source of the route and use route-filtering techniques at the source to stop it from being advertised.

Verify the Routing Table

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 15 subnets, 3 masks
O IA    10.1.10.0/24 [110/2] via 10.1.2.1, 07:43:07, FastEthernet0/1
O       10.1.2.12/30 [110/3] via 10.1.2.1, 07:42:57, FastEthernet0/1
C       10.1.1.2/32 is directly connected, Serial0/0/0
C       10.1.2.0/30 is directly connected, FastEthernet0/1
C       10.1.1.0/30 is directly connected, Serial0/0/0
O IA    10.1.30.0/24 [110/2] via 10.1.2.1, 07:43:07, FastEthernet0/1
O IA    10.1.20.0/24 [110/2] via 10.1.2.1, 07:43:07, FastEthernet0/1
O IA    10.1.50.0/24 [110/2] via 10.1.2.1, 07:43:07, FastEthernet0/1
O IA    10.1.100.0/24 [110/2] via 10.1.2.1, 07:43:07, FastEthernet0/1
D       10.1.202.1/32 [90/2297856] via 10.1.1.2, 07:43:48, Serial0/0/0
O IA    10.1.203.1/32 [110/4] via 10.1.2.1, 07:42:57, FastEthernet0/1
C       10.1.201.1/32 is directly connected, Loopback0
```



```
O       10.1.200.0/24 [110/2] via 10.1.2.1, 07:43:00, FastEthernet0/1
O       10.1.211.1/32 [110/2] via 10.1.2.1, 07:43:10, FastEthernet0/1
O       10.1.212.1/32 [110/3] via 10.1.2.1, 07:43:00, FastEthernet0/1

R1#show ip route 10.1.50.0 255.255.255.0
Routing entry for 10.1.50.0/24
  Known via "ospf 1", distance 110, metric 2, type inter area
  Redistributing via eigrp 1
  Advertised by eigrp 1 metric 1544 2000 255 1 1500
  Last update from 10.1.2.1 on FastEthernet0/1, 07:42:07 ago
  Routing Descriptor Blocks:
  * 10.1.2.1, from 10.1.211.1, 07:42:07 ago, via FastEthernet0/1
      Route metric is 2, traffic share count is 1
```

The source of a route in the routing table is marked by the “from” field that follows the next-hop IP address. For distance vector protocols, the source and next-hop addresses are typically the same. For a link-state protocol, such as OSPF, this is the router that originated the LSA on which the route is based. By tracking the routing source from router to router, you can determine the point where the incorrect routing information is injected into the routing protocol’s data structures, and you can apply filtering to stop it from being propagated.

Reflection Questions

1. Which lab trouble tickets did you have the most difficulty with?

2. For any of the trouble tickets, would you change anything about the process that you used now that you see the resolution of the problem?

3. Which commands did you find most useful in diagnosing OSPF and redistribution issues? Add these to your toolbox for future use. Which commands did you find least useful?

4. What is required for routes to be redistributed from OSPF to EIGRP? From EIGRP to OSPF?

References

If you need more information on the commands and their options, see the following references:

- IP Routing Protocol Command Reference

  http://www.cisco.com/cisco/web/support/index.html

- Open Shortest Path First Troubleshooting Tech Notes
  http://www.cisco.com/en/US/tech/tk365/tsd_technology_support_troubleshooting_technotes_list.html#anchor8

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1700	Fast Ethernet 0 (FA0)	Fast Ethernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
1800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2600	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)
2800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. Rather than try to list all the combinations of configurations for each router class, this table includes identifiers for the possible combinations of Ethernet and serial interfaces in the device. The table does not include any other type of interface, even though a specific router might contain one. An example of this is an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

Device Configurations (Instructor version)

Note: All device configurations are provided for TT-A, including those that are the same as the baseline as defined in Lab 3-1. The configs provided here are *not* running-config outputs. They can be used for copy-and-paste for TT-A and subsequent tickets. Where a config is noted as being the same as a previous one, the only change is in the MOTD, which identifies the Lab and TT. The errors in the configuration are commented and highlighted as red text.

Trouble Ticket—TT-A Configurations

Switch ALS1

```
!Lab 5-2 Switch ALS1 TT-A Config
!
hostname ALS1
!
```



```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 5-2 Switch ALS1 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet

spanning-tree mode rapid-pvst
spanning-tree portfast default
!
interface Vlan1
 no ip address
 shutdown
!
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 100
 name MGMT
!
vlan 900
```



```
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel1
 description Channel to DLS1
 no shutdown
 !
interface Port-channel2
 description Channel to DLS2
 no shutdown
!
interface FastEthernet0/1
 description Channel to DLS1
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shutdown
!
interface FastEthernet0/2
 description Channel to DLS1
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shutdown
!
interface FastEthernet0/3
 description Channel to DLS2
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shutdown
!
interface FastEthernet0/4
 description Channel to DLS2
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shutdown
!
interface FastEthernet0/5
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
```



```
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown

interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
```



```
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description To PC-B
 switchport access vlan 10
 switchport mode access
 switchport voice vlan 20
 spanning-tree portfast
 switchport port-security
 switchport port-security maximum 2
 switchport port-security violation shutdown
 switchport port-security mac-address sticky
 no shut
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
```



```
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan100
 ip address 10.1.100.1 255.255.255.0
 no shutdown
!
ip default-gateway 10.1.100.254
!
ip http server
ip http secure-server
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server host 10.1.50.1 version 2c cisco
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
```

```
snmp-server enable traps port-security
snmp-server enable traps vlan-membership
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
  no transport input
!
ntp source Vlan100
ntp server 10.1.202.1
end
```

Switch DLS1

```
!Lab 5-2 Switch DLS1 TT-A Config
!
hostname DLS1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55

banner motd $*** Lab 5-2 Switch DLS1 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
!
ip domain name tshoot.net
!
ip dhcp excluded-address 10.1.10.252 10.1.10.254
ip dhcp excluded-address 10.1.20.252 10.1.20.254
ip dhcp excluded-address 10.1.30.252 10.1.30.254
!
ip dhcp pool OFFICE
   network 10.1.10.0 255.255.255.0
```



```
   default-router 10.1.10.254
   domain-name tshoot.net
!
ip dhcp pool VOICE
   network 10.1.20.0 255.255.255.0
   default-router 10.1.20.254
   domain-name tshoot.net
!
ip dhcp pool GUEST
   network 10.1.30.0 255.255.255.0
   default-router 10.1.30.254
   domain-name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog contenttype plaintext
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 24576
spanning-tree vlan 20,50 priority 28672
!
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
!
vlan 100
 name MGMT
!
vlan 200
 name TRANS
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
```

```
ip ssh source-interface Vlan100
!
interface Loopback0
 description OSPF router ID
 ip address 10.1.211.1 255.255.255.255
 ip ospf network point-to-point
!
interface Port-channel1
 description Channel to ALS1
 no shut
!
interface Port-channel10
 description Channel to DLS2
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R1
 no switchport
```

```
 ip address 10.1.2.1 255.255.255.252
 speed 100
 duplex full
 spanning-tree bpduguard enable
 no shut
!
interface FastEthernet0/6
 description FE to SRV1
 switchport access vlan 50
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shut
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
```



```
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
```



```
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 10.1.10.252 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 priority 110
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.252 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.252 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 priority 110
 standby 30 preempt
```



```
!
interface Vlan50
 ip address 10.1.50.252 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 preempt
!
interface Vlan100
 ip address 10.1.100.252 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 priority 110
 standby 100 preempt
!
interface Vlan200
 ip address 10.1.200.252 255.255.255.0
!
router ospf 1
 log-adjacency-changes
 passive-interface default
 no passive-interface Vlan200
 no passive-interface FastEthernet0/5
 network 10.1.2.0 0.0.0.3 area 0
 network 10.1.10.0 0.0.0.255 area 1
 network 10.1.20.0 0.0.0.255 area 1
 network 10.1.30.0 0.0.0.255 area 1
 network 10.1.50.0 0.0.0.255 area 1
 network 10.1.100.0 0.0.0.255 area 1
 network 10.1.200.0 0.0.0.255 area 0
 network 10.1.211.1 0.0.0.0 area 0
!
ip classless
ip http server
ip http secure-server
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
!
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server host 10.1.50.1 version 2c cisco
snmp-server enable traps ospf state-change
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
```

```
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 10.1.202.1
end
```

Switch DLS2

```
!Lab 5-2 Switch DLS2 TT-A Config
!
hostname DLS2
!
service timestamps debug datetime msec
service timestamps log datetime
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 5-2 Switch DLS2 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500

vtp domain TSHOOT
vtp mode transparent

ip subnet-zero
ip routing
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog contenttype plaintext
  hidekeys
  path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
```



```
spanning-tree vlan 10,30,100 priority 28672
spanning-tree vlan 20,50 priority 24576

vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
!
vlan 100
 name MGMT
!
vlan 200
 name TRANS
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Loopback0
 description OSPF router ID
 ip address 10.1.212.1 255.255.255.255
 ip ospf network point-to-point
!
interface Port-channel2
 description Channel to ALS1
 no shut
!
interface Port-channel10
 description Channel to DLS1
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
```

```
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R3
 no switchport
 ip address 10.1.2.13 255.255.255.252
 speed 100
 duplex full
 no shut
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
```



```
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
```



```
 shutdown
!
interface FastEthernet0/18
 description FE to PC-C
 switchport access vlan 30
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
```

```
!
interface GigabitEthernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 10.1.10.253 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.253 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 priority 110
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.253 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.253 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 priority 110
 standby 50 preempt
!
interface Vlan100
 ip address 10.1.100.253 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 preempt
!
interface Vlan200
 ip address 10.1.200.253 255.255.255.0
!
router ospf 1
 log-adjacency-changes
 passive-interface default
 no passive-interface Vlan200
 no passive-interface FastEthernet0/5
 network 10.1.2.12 0.0.0.3 area 0
 network 10.1.10.0 0.0.0.255 area 1
 network 10.1.20.0 0.0.0.255 area 1
 network 10.1.30.0 0.0.0.255 area 1
 network 10.1.50.0 0.0.0.255 area 1
 network 10.1.100.0 0.0.0.255 area 1
 network 10.1.200.0 0.0.0.255 area 0
 network 10.1.212.1 0.0.0.0 area 0
!
ip classless
ip http server
```



```
ip http secure-server
!
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps ospf state-change
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 10.1.202.1
end
```

Router R1

```
!Lab 5-2 Router R1 TT-A Config
!
hostname R1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 5-2 Router R1 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
```



```
!
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 10.1.201.1 255.255.255.255
 ip ospf network point-to-point
!
interface FastEthernet0/0
 no ip address
 shutdown
!
interface FastEthernet0/1
 description FE to DLS1
 ip address 10.1.2.2 255.255.255.252
 ip flow ingress
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
 description WAN link to R2 - 128k leased line
 ip address 10.1.1.1 255.255.255.252
 ip flow ingress
 encapsulation ppp
 clock rate 128000
  no shutdown
!
interface Serial0/0/1
 description WAN link to R3 (not used)
 no ip address
 shutdown
!
router eigrp 1
 redistribute ospf 1
 passive-interface default
 no passive-interface Serial0/0/0
 network 10.1.1.0 0.0.0.3
 no auto-summary
!
router ospf 1
 log-adjacency-changes
 redistribute eigrp 1
 passive-interface default
```

Error: Seed metric is not specified for redistribution.

redistribute ospf 1 metric 1544 2000 255 1 1500

Error: Metric and subnets option is not specified for redistribution.

redistribute eigrp 1 metric 100 subnets

Note: Metric 100 is optional, subnets is required.


```
 no passive-interface FastEthernet0/1
 no passive-interface Serial0/0/0
 no passive-interface Loopback0
 network 10.1.2.0 0.0.0.3 area 0
 network 10.1.201.1 0.0.0.0 area 0
!
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
logging source-interface Loopback0
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 10.1.202.1
end
```

Router R2

```
! Lab 5-2 Router R2 TT-A Config
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
Hostname R2
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 5-2 Router R2 TT-A Config ***$
!
no ip domain lookup
```



```
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 10.1.202.1 255.255.255.255

interface FastEthernet0/0
 shutdown
!
interface FastEthernet0/1
 shutdown
!
interface Serial0/0/0
 description WAN link to R1 - 128k leased line
 ip address 10.1.1.2 255.255.255.252
 encapsulation ppp
 no shutdown
!
interface Serial0/0/1
 description WAN link to R3 - 128k leased line – Not used for this lab
 ip address 10.1.1.6 255.255.255.252
 encapsulation ppp
 shutdown
!
router eigrp 1
 passive-interface default
 no passive-interface Serial0/0/0
 no passive-interface Loopback0
 network 10.1.1.0 0.0.0.3
 network 10.1.202.1 0.0.0.0
 no auto-summary
!
ip http server
no ip http secure-server
!
logging source-interface Loopback0
logging 10.1.50.1
```



```
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
!
ntp master 3
 end
```

Router R3

```
! Lab 5-2 Router R3 TT-A Config
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 5-2 Router R3 TT-A Config ***$
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
no ip domain lookup
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
```



```
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 10.1.203.1 255.255.255.255
 ip ospf network point-to-point
!
interface FastEthernet0/0
 no ip address
 shutdown

interface FastEthernet0/1
 description FE to DLS2
 ip address 10.1.2.14 255.255.255.252
 ip flow ingress
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
 description WAN link to R1 - (Not used)
 no ip address
 clock rate 128000
 encapsulation ppp
 shutdown
!
interface Serial0/0/1
 description WAN link to R2 - 128k leased line (Not used)
 ip address 10.1.1.5 255.255.255.252
 ip flow ingress
 encapsulation ppp
 shutdown
!
router ospf 1
area 3 stub no-summary
network 10.1.2.12 0.0.0.3 area 0
network 10.1.203.1 0.0.0.0 area 3
!
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
logging source-interface Loopback0
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps ospf state-change
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
```



```
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
line vty 0 4
 exec-timeout 60 0
transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 10.1.202.1
end
```

Trouble Ticket—TT-B Configurations

Switch ALS1 (Same as TT-A)

Switch DLS1 (Same as TT-A)

Switch DLS2 (Same as TT-A)

Router R3 (Same as TT-A)

Router R1

```
!Lab 5-2 Router R1 TT-B Config
!
hostname R1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 5-2 Router R1 TT-B Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
```



```
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 10.1.201.1 255.255.255.255
 ip ospf network point-to-point
!
interface FastEthernet0/0
 no ip address
 shutdown
!
interface FastEthernet0/1
 description FE to DLS1
 ip address 10.1.2.2 255.255.255.252
 ip flow ingress
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
 description WAN link to R2 - 128k leased line
 ip address 10.1.1.1 255.255.255.252
 ip flow ingress
 encapsulation ppp
 clock rate 128000
  no shutdown
!
interface Serial0/0/1
 description WAN link to R3 (not used)
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 area 2 stub
 passive-interface default
 no passive-interface FastEthernet0/1
 no passive-interface Serial0/0/0
 no passive-interface Loopback0
 network 10.1.1.0 0.0.0.3 area 2
 network 10.1.2.0 0.0.0.3 area 0
 network 10.1.201.1 0.0.0.0 area 0
!
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
logging source-interface Loopback0
```

Error: Area 2 should be configured as a totally stubby area.

`area 2 stub no-summary`


```
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 10.1.202.1
end
```

Router R2

```
! Lab 5-2 Router R2 TT-B Config
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
Hostname R2
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 5-2 Router R2 TT-B Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
```



```
   logging size 50
   notify syslog
   hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 10.1.202.1 255.255.255.255

interface FastEthernet0/0
 shutdown
!
interface FastEthernet0/1
 shutdown
!
interface Serial0/0/0
 description WAN link to R1 - 128k leased line
 ip address 10.1.1.2 255.255.255.252
 encapsulation ppp
 no shutdown
!
interface Serial0/0/1
 shutdown
!
router ospf 1
 log-adjacency-changes
 passive-interface default
 no passive-interface Serial0/0/0
 no passive-interface Loopback0
 network 10.1.1.0 0.0.0.3 area 22
 network 10.1.202.1 0.0.0.0 area 22
!
ip http server
no ip http secure-server
!
logging source-interface Loopback0
logging 10.1.50.1
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
```

Error: Area 22 should be area 2.

```
router ospf 1
  network 10.1.1.0 0.0.0.3 area 2
  network 10.1.202.1 0.0.0.0 area 2
```



```
!
ntp master 3
 end
```

Trouble Ticket—TT-C Configurations

Switch ALS1 (Same as TT-A)

Switch DLS1 (Same as TT-A)

Router R3 (Same as TT-A)

Switch DLS2

```
!Lab 5-2 Switch DLS2 TT-C Config
!
hostname DLS2
!
service timestamps debug datetime msec
service timestamps log datetime
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 5-2 Switch DLS2 TT-C Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500

vtp domain TSHOOT
vtp mode transparent

ip subnet-zero
ip routing
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog contenttype plaintext
  hidekeys
  path tftp://10.1.50.1/$h-archive-config
```

```
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 28672
spanning-tree vlan 20,50 priority 24576

vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
!
vlan 100
 name MGMT
!
vlan 200
 name TRANS
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Loopback0
 description OSPF router ID
 ip address 10.1.212.1 255.255.255.255
 ip ospf network point-to-point
!
interface Port-channel2
 description Channel to ALS1
 no shut
!
interface Port-channel10
 description Channel to DLS1
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
```



```
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R3
 no switchport
 ip address 10.1.2.13 255.255.255.252
 speed 100
 duplex full
 ip ospf hello-interval 5
 ip ospf dead-interval 15
 no shut
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
```

Error: Hello and dead timers are changed from the default.

```
interface FastEthernet 0/5
 default ip ospf hello-interval
 default ip ospf dead-interval
```



```
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
```



```
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description FE to PC-C
 switchport access vlan 30
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
```



```
!
interface GigabitEthernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 10.1.10.253 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.253 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 priority 110
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.253 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.253 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 priority 110
 standby 50 preempt
!
interface Vlan100
 ip address 10.1.100.253 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 preempt
!
interface Vlan200
 ip address 10.1.200.253 255.255.255.0
!
router ospf 1
 log-adjacency-changes
 passive-interface default
 no passive-interface Vlan200
 no passive-interface FastEthernet0/5
 network 10.1.2.12 0.0.0.3 area 0
 network 10.1.10.0 0.0.0.255 area 1
 network 10.1.20.0 0.0.0.255 area 1
 network 10.1.30.0 0.0.0.255 area 1
```

```
 network 10.1.50.0 0.0.0.255 area 1
 network 10.1.100.0 0.0.0.255 area 1
 network 10.1.200.0 0.0.0.255 area 0
 network 10.1.212.1 0.0.0.0 area 0
!
ip classless
ip http server
ip http secure-server
!
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps ospf state-change
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 10.1.202.1
end
```

Router R1

```
!Lab 5-2 Router R1 TT-C Config
!
hostname R1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
```



```
banner motd $*** Lab 5-2 Router R1 TT-C Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 10.1.201.1 255.255.255.255
 ip ospf network point-to-point
!
interface FastEthernet0/0
 no ip address
 shutdown
!
interface FastEthernet0/1
 description FE to DLS1
 ip address 10.1.2.2 255.255.255.252
 ip flow ingress
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
 description WAN link to R2 - 128k leased line
 ip address 10.1.1.1 255.255.255.252
 ip flow ingress
 encapsulation ppp
 clock rate 128000
  no shutdown
!
interface Serial0/0/1
 description WAN link to R3 (not used)
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 area 2 stub no-summary
```



```
 passive-interface default
 no passive-interface FastEthernet0/1
 no passive-interface Serial0/0/0
 no passive-interface Loopback0
 network 10.1.1.0 0.0.0.3 area 2
 network 10.1.2.0 0.0.0.3 area 0
 network 10.1.201.1 0.0.0.0 area 0
!
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
logging source-interface Loopback0
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 10.1.202.1
end
```

Router R2

```
! Lab 5-2 Router R2 TT-C Config
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
Hostname R2
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
```



```
banner motd $*** Lab 5-2 Router R2 TT-C Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 10.1.202.1 255.255.255.255

interface FastEthernet0/0
 shutdown
!
interface FastEthernet0/1
 shutdown
!
interface Serial0/0/0
 description WAN link to R1 - 128k leased line
 ip address 10.1.1.2 255.255.255.252
 encapsulation ppp
 no shutdown
!
interface Serial0/0/1
 description WAN link to R3 - 128k leased line – Not used for this lab
 ip address 10.1.1.6 255.255.255.252
 encapsulation ppp
 shutdown
!
router ospf 1
 log-adjacency-changes
 area 2 stub no-summary
 passive-interface default
 no passive-interface Serial0/0/0
 no passive-interface Loopback0
 network 10.1.1.0 0.0.0.3 area 2
 network 10.1.202.1 0.0.0.0 area 2
!
ip http server
```



```
no ip http secure-server
!
logging source-interface Loopback0
logging 10.1.50.1
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
!
ntp master 3
 end
```

Trouble Ticket—TT-D Configurations

Switch ALS1 (Same as TT-A)

Router R1 (Same as TT-C)

Router R2 (Same as TT-C)

Router R3 (Same as TT-A)

Switch DLS1

```
!Lab 5-2 Switch DLS1 TT-D Config
!
hostname DLS1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55

banner motd $*** Lab 5-2 Switch DLS1 TT-D Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
```



```
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
!
ip domain name tshoot.net
!
ip dhcp excluded-address 10.1.10.252 10.1.10.254
ip dhcp excluded-address 10.1.20.252 10.1.20.254
ip dhcp excluded-address 10.1.30.252 10.1.30.254
!
ip dhcp pool OFFICE
   network 10.1.10.0 255.255.255.0
   default-router 10.1.10.254
   domain-name tshoot.net
!
ip dhcp pool VOICE
   network 10.1.20.0 255.255.255.0
   default-router 10.1.20.254
   domain-name tshoot.net
!
ip dhcp pool GUEST
   network 10.1.30.0 255.255.255.0
   default-router 10.1.30.254
   domain-name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog contenttype plaintext
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 24576
spanning-tree vlan 20,50 priority 28672
!
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
```



```
 name GUEST
!
vlan 50
 name SERVERS
!
!
vlan 100
 name MGMT
!
vlan 200
 name TRANS
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
interface Loopback0
 description OSPF router ID
 ip address 10.1.211.1 255.255.255.255
 ip ospf network point-to-point
!
interface Port-channel1
 description Channel to ALS1
 no shut
!
interface Port-channel10
 description Channel to DLS2
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
```



```
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R1
 no switchport
 ip address 10.1.2.1 255.255.255.252
 speed 100
 duplex full
 no shut
!
interface FastEthernet0/6
 description FE to SRV1
 switchport access vlan 50
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shut
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
```



```
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/19
```

```
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
```



```
interface Vlan10
 ip address 10.1.10.252 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 priority 110
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.252 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.252 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 priority 110
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.252 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 preempt

!
interface Vlan100
 ip address 10.1.100.252 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 priority 110
 standby 100 preempt
!
interface Vlan200
 ip address 10.1.200.252 255.255.255.0
 ip ospf message-digest-key 1 md5 ospfpa55
!
router ospf 1
 log-adjacency-changes
 passive-interface default
 no passive-interface FastEthernet0/5
 network 10.1.2.0 0.0.0.3 area 0
 network 10.1.10.0 0.0.0.255 area 1
 network 10.1.20.0 0.0.0.255 area 1
 network 10.1.30.0 0.0.0.255 area 1
 network 10.1.50.0 0.0.0.255 area 1
 network 10.1.100.0 0.0.0.255 area 1
 network 10.1.200.0 0.0.0.255 area 0
 network 10.1.211.1 0.0.0.0 area 0

!
ip classless
ip http server
ip http secure-server
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
!
snmp-server community san-fran RW
```

Error: VLAN 200 should not be passive.

```
router ospf 1
 no passive-interface vlan 200
```

Error: OSPF authentication is not enabled in area 0.

```
router ospf 1
 area 0 authentication message-digest
```

OR (for just VLAN 200)

```
interface Vlan200
 ip ospf authentication message-digest
```



```
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server host 10.1.50.1 version 2c cisco
snmp-server enable traps ospf state-change
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 10.1.202.1
end
```

Switch DLS2

```
!Lab 5-2 Switch DLS2 TT-D Config
!
hostname DLS2
!
service timestamps debug datetime msec
service timestamps log datetime
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 5-2 Switch DLS2 TT-D Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500

vtp domain TSHOOT
vtp mode transparent

ip subnet-zero
```



```
ip routing
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog contenttype plaintext
  hidekeys
  path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 28672
spanning-tree vlan 20,50 priority 24576

vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
!
vlan 100
 name MGMT
!
vlan 200
 name TRANS
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Loopback0
 description OSPF router ID
 ip address 10.1.212.1 255.255.255.255
 ip ospf network point-to-point
!
interface Port-channel2
 description Channel to ALS1
 no shut
```



```
!
interface Port-channel10
 description Channel to DLS1
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R3
 no switchport
 ip address 10.1.2.13 255.255.255.252
 spanning-tree bpduguard enable
 speed 100
 duplex full
 no shut
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
```



```
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
```



```
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description FE to PC-C
 switchport access vlan 30
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
```



```
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 10.1.10.253 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.253 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 priority 110
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.253 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.253 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 priority 110
 standby 50 preempt
!
interface Vlan100
 ip address 10.1.100.253 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 preempt
```



```
!
interface Vlan200
 ip address 10.1.200.253 255.255.255.0
 ip ospf message-digest-key 1 md5 ospfpa55
!
router ospf 1
 log-adjacency-changes
 passive-interface default
 no passive-interface Vlan200
 no passive-interface FastEthernet0/5
 network 10.1.2.12 0.0.0.3 area 0
 network 10.1.10.0 0.0.0.255 area 1
 network 10.1.20.0 0.0.0.255 area 1
 network 10.1.30.0 0.0.0.255 area 1
 network 10.1.50.0 0.0.0.255 area 1
 network 10.1.100.0 0.0.0.255 area 1
 network 10.1.200.0 0.0.0.255 area 0
 network 10.1.212.1 0.0.0.0 area 0
!
ip classless
ip http server
ip http secure-server
!
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps ospf state-change
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 10.1.202.1
end
```

Error: OSPF authentication is not enabled in area 0.

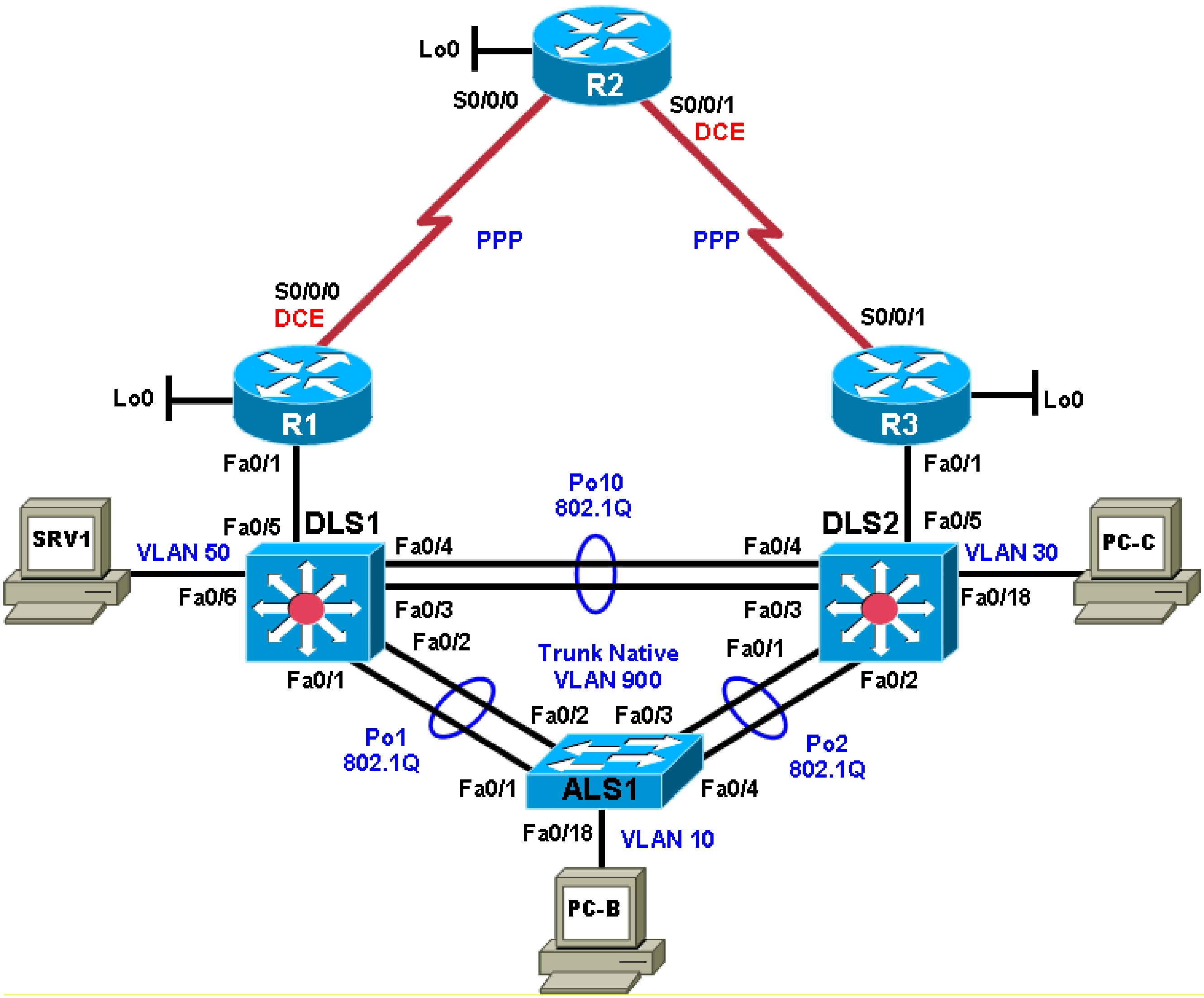
```
router ospf 1
 area 0 authentication message-digest
```

OR (for just VLAN 200)

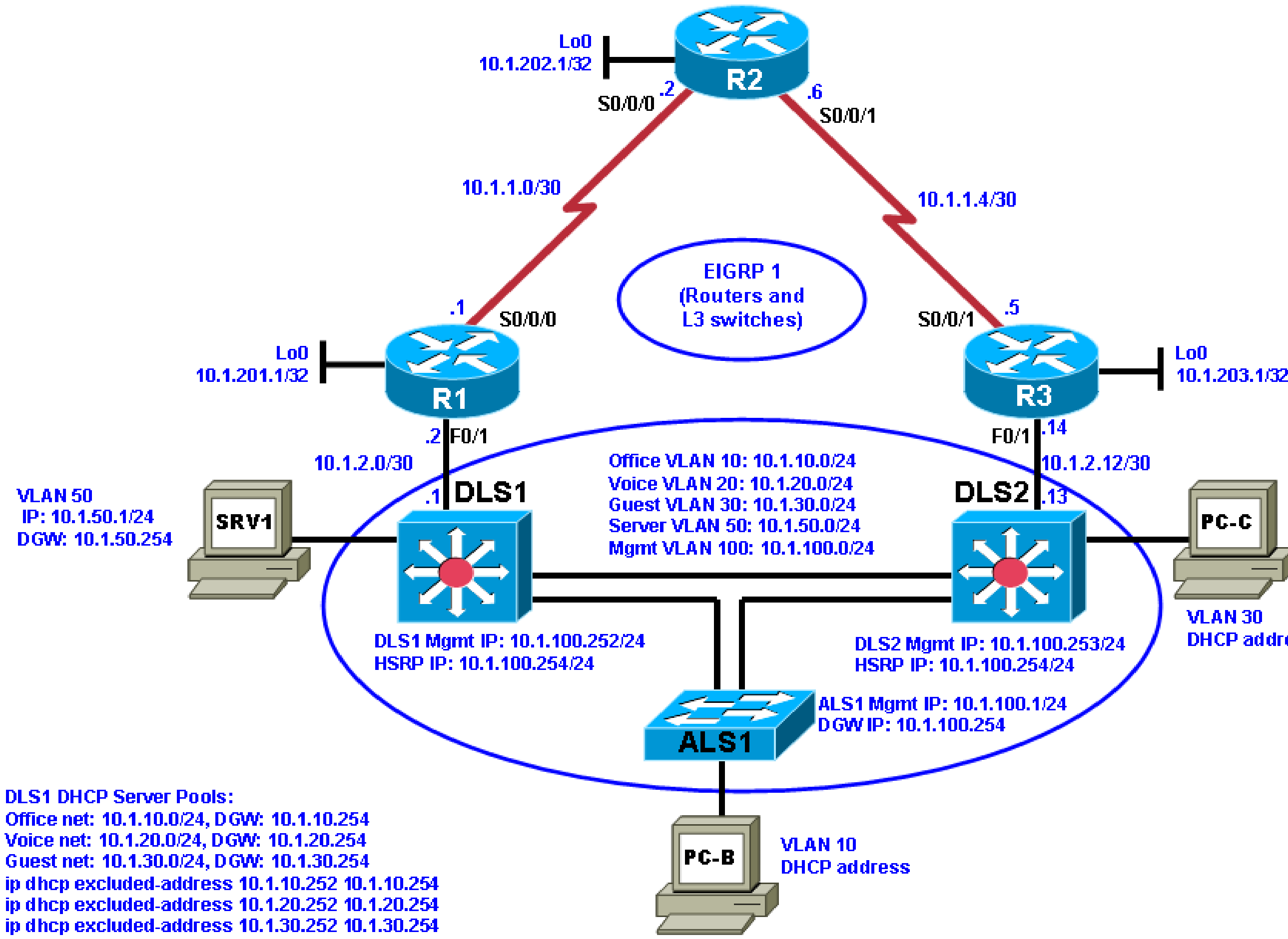
```
interface Vlan200
 ip ospf authentication message-digest
```

Chapter 5 Lab 5-3, BGP **Instructor Version**

Physical Topology (Baseline)



Logical Topology (Baseline)



Objectives

- Load the trouble ticket device configuration files for each trouble ticket.
- Diagnose and resolve problems related to the BGP exterior routing protocol.
- Document troubleshooting progress, configuration changes, and problem resolution.

Background

Border Gateway Protocol (BGP) is the most widely used exterior routing protocol on the Internet. It is the de facto standard for route (prefix) exchange between the autonomous systems (AS) of Internet service providers (ISPs). BGP can also be used between a customer network and one or more ISPs. In this lab, you will troubleshoot various problems related to BGP. For each task or trouble ticket, the trouble scenario and problem symptom are described. While troubleshooting, you will discover the cause of the problem, correct it, and then document the process and results.

Implementing BGP

Your company has decided to implement several new Internet-based services. The current web services that the company offers are hosted at an external data center. It has been decided to build an in-house data center from which the new services will be hosted. The servers that are currently externally hosted will also be moved to the new data center.

Your company currently has a single ISP for Internet access. You have obtained a registered AS number (65501) and address block 172.30.1.0/27, which will be used for the new services. After consulting with the

ISP, it has been decided to use BGP between the network edge router R1 and the ISP (R2). Upon successful completion of the BGP implementation, your company is considering adding another ISP for redundancy, but not as part of the current project.

Your support team has been working closely together with the engineering team to prepare the implementation. You have received confirmation from the ISP that they have prepared their router for the BGP implementation.

Router R1 will advertise the 172.30.1.0/27 IP address block to the ISP (R2). No other prefixes are allowed to be advertised. This ensures that only the assigned network address block will be received by the ISP. ISPs typically place filters on their edge routers to prevent customers from accidently announcing routes that do not belong to them.

The ISP router will send a default route to router R1 via BGP. The default route will be redistributed into Enhanced Interior Gateway Routing Protocol (EIGRP) by router R1. No other routes will be redistributed.

It is Friday evening, and the engineering team has just configured router R1 for BGP. To facilitate testing, a new hosted services VLAN and the corresponding subnet 172.30.1.0/27 will be created. All other devices, which have IP addresses in the 10.1.0.0/16 range, are using Network Address Translation (NAT), and their Internet access should not be affected by the BGP configuration.

You are on standby to assist in troubleshooting and testing the solution.

Implementation Plan

The implementation plan is in two phases.

Phase 1

During Phase 1, the link between edge router R1 and the existing ISP will be upgraded to a T1 leased line and converted to BGP. The remainder of the network will continue to use EIGRP. The 10.1.1.0/30 addressing on the R1-to-R2 serial WAN link will be changed to a public address (209.165.200.224/30) provided by the ISP. NAT will be used to translate the 10.1.0.0/16 internal private addresses to public address 209.165.200.225 using Port Address Translation (PAT). The loopback 0 address on R1 is also changed to 192.168.1.1.

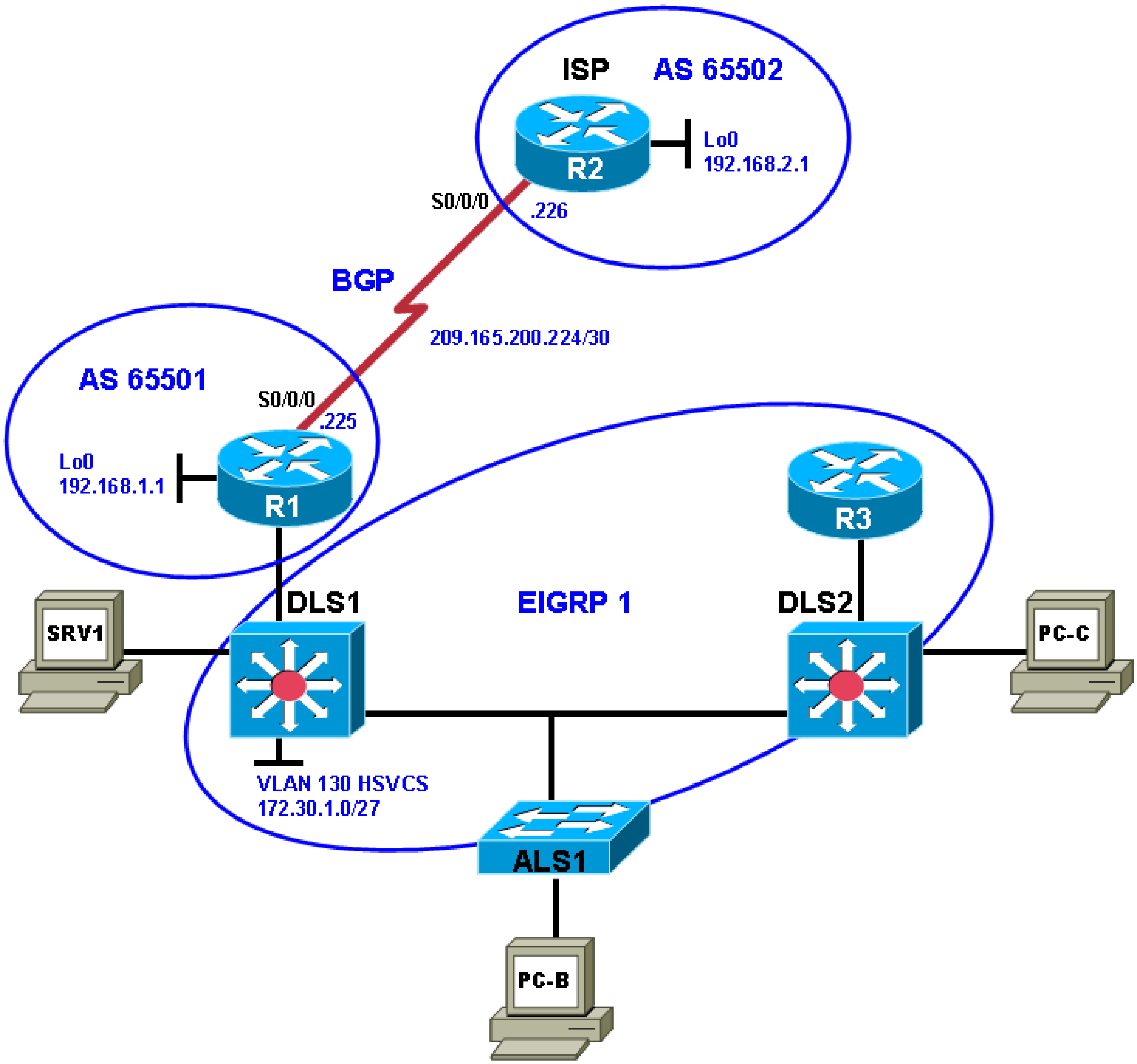
An external BGP peering will be established between router R1 and the ISP (R2). The ISP will advertise a default route to R1 via BGP. On router R1, redistribution of the default route will be configured between BGP and EIGRP to ensure connectivity between headquarters and the ISP.

Phase 2

During Phase 2, the hosted services VLAN 130 named HSVCS and the corresponding subnet 172.30.1.0/27 will be created on switch DLS1. A test server for the hosted services subnet will be installed, simulated by switch virtual interface (SVI) VLAN 130 172.30.1.1/27 on DLS1. A static route will be provided from R1 to DLS1 VLAN 130. Some services will be migrated to the new IP address block before moving them to the newly built datacenter.

BGP Network Design

The BGP design is outlined in the following figure. BGP AS 65501 is the company’s newly acquired AS number. The ISP AS is 65502.



Test Plan

In Phase 1, edge router R1 must become a BGP peer with the ISP, and the internal office clients must be able to access the Internet through the ISP. In Phase 2, the Internet clients must be able to access the hosted services network.

Note: Trouble ticket A is related to the verification and acceptance of BGP Phase 1. Trouble tickets B and C are related to the second phase of BGP conversion. Any interfaces that have been shut down on routers R2 and R3 should remain shut down for the duration of this lab exercise.

Physical and Logical Topology Diagrams

The physical and logical topologies for the existing EIGRP-based network are provided in this lab to assist the troubleshooting effort.

Lab Structure

This lab is divided into two main sections.

Section 1—Trouble Tickets and Troubleshooting Logs

This section includes multiple tasks. Each task is associated with a trouble ticket (TT) and introduces one or more errors on one or more devices. If time is a consideration, each task or trouble ticket can be performed independently.

Section 2—Troubleshooting Reference Information

This section provides general BGP troubleshooting information that can be applied to any trouble ticket in this lab. Sample troubleshooting flows are provided, along with examples of useful commands and output. If time permits, it is recommended that you read Section 2 prior to starting on the trouble tickets.

Instructor note: Because the troubleshooting reference section is lengthy, ask students to read through it prior to starting the lab to become familiar with the troubleshooting flows and commands used. Consider assigning it as homework.

Note: This lab uses Cisco 1841 routers with Cisco IOS Release 12.4(24)T1 and the Advanced IP Services image c1841-advipservicesk9-mz.124-24.T1.bin. The switches are Cisco WS-C2960-24TT-L with the Cisco IOS image c2960-lanbasek9-mz.122-46.SE.bin and Catalyst 3560-24PS with the Cisco IOS image c3560-advipservicesk9-mz.122-46.SE.bin. Other routers (such as 2801 and 2811), switches (such as 2950 or 3550), and Cisco IOS Software versions can be used if they have comparable capabilities and features. Depending on the router or switch model and Cisco IOS Software version, the commands available and output produced might vary from what is shown in this lab.

Instructor Notes

- The lab topology should be pre-built prior to the students starting the lab. Ensure that all routers and switches (R1, R2, R3, ALS1, DLS1, and DLS2) have the course lab configuration files installed in flash. These can be downloaded from the Academy Connection website.
- The device configurations that contain trouble ticket errors or modifications from the baseline are included at the end of the lab, and the errors in them are identified.
- Each device has a directory named “tshoot” in flash. This directory contains the baseline configuration file for that device as well as configuration files for the labs in this course. Refer to Lab 3-1 for instructions on creating the tshoot directory in flash.
- Instructors can use a TFTP server, USB drive, flash memory card, or other method to copy all the course configuration files into the flash:/tshoot directory for each device in the topology.
- The student is responsible for loading the trouble ticket configurations for all labs as required using the procedure described in Lab 3-1.
- Set the correct time on router R2, which serves as the primary NTP server for the lab network.
- If time is an issue, each task (trouble ticket) can be performed independently.

Required Resources

- 3 routers (Cisco 1841 with Cisco IOS Release 12.4(24)T1 Advanced IP Service or comparable)
- 1 switch (Cisco 2960 with the Cisco IOS Release 12.2(46)SE C2960-LANBASEK9-M image or comparable)
- 2 switches (Cisco 3560 with the Cisco IOS Release 12.2(46)SE C3560-LANBASEK9-M image or comparable)
- 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

Instructor Notes

- This lab is divided into multiple tasks. Each task is associated with a trouble ticket (TT) and introduces one or more errors on one or more devices.
- Students can work individually or as a team.
- Suggested actions and results presented during the troubleshooting process for each TT can be shared with the students during debrief or copies of the instructor version of the lab can be made available to the students to assist them in verifying their work.

Section 1—Trouble Tickets and Troubleshooting Logs

Task 1: Trouble Ticket Lab 5-3 TT-A

Instructor note: This trouble ticket involves issues related to the AS number and peer IP addressing on R1 that affect BGP peering on devices R1 and R2.

Step 1: Review trouble ticket Lab 5-3 TT-A.

After your colleague finished configuring BGP on edge router R1, you tested connectivity from PC-B in VLAN 10 to the ISP router to verify the configuration and peering between R1 and R2. This test failed. When you asked your colleague, he said he did not actually test the configuration from a client PC on the internal network. He suspected there was a problem with the ISP and contacted them to find out if there was an issue at their end. They stated that everything was correctly configured on router R2.

Your task is to diagnose the problem and verify that BGP is properly configured to enable BGP peering between router R1 and the ISP.

Step 2: Load the device trouble ticket configuration files for TT-A.

Using the procedure described in Lab 3-1, verify that the lab configuration files are present in flash and load the proper configuration files as indicated in the Device Configuration File table.

Note: The following device access methods are in effect after loading the configuration files:

- Console access requires no username or password.
- Telnet and SSH require username **admin** and password **adminpa55**.
- The enable password is **ciscoenpa55**.

Instructor note: Although it is not considered security best practice, the student can set the console and VTY line exec-timeout to 0 0 to facilitate performance of this lab.

Device Configuration File Table

Device Name	File to Load	Notes
ALS1	Lab53-ALS1-TT-A-Cfg.txt	This file contains configurations different than the baseline
DLS1	Lab53-DLS1-TT-A-Cfg.txt	This file contains configurations different than the baseline
DLS2	Lab53-DLS2-TT-A-Cfg.txt	This file contains configurations different than the baseline
R1	Lab53-R1-TT-A-Cfg.txt	This file contains configuration errors
R2	Lab53-R2-TT-A-Cfg.txt	This file contains configurations different than the baseline
R3	Lab53-R3-TT-A-Cfg.txt	This file contains configurations different than the baseline
SRV1	N/A	Static IP: 10.1.50.1 Default gateway: 10.1.50.254
PC-B	N/A	DHCP
PC-C	N/A	DHCP

Instructor note: The student loads the “broken” TT configuration files for all devices, even though only the configurations indicated in the Notes column contain errors.

Step 3: Configure SRV1 and start the syslog and TFTP servers.

Step 4: Release and renew the DHCP lease on PC-B.

a. Ensure that PC-B is configured as a DHCP client in the OFFICE VLAN.

b. After loading all TT-A device configuration files, issue the **ipconfig /release** and **ipconfig /renew** commands on PC-B.

Step 5: Outline the troubleshooting approach and validation steps.

Use this space to identify your troubleshooting approach and the key steps to verify that the problem is resolved. Troubleshooting approaches to select from include the follow-the-path, spot-the-differences, bottom-up, top-down, divide-and-conquer, shoot-from-the-hip, and move-the-problem methods.

Note: In addition to a specific approach, you can use the generic troubleshooting process described at the beginning of Section 2 of this lab.

___

___

___

___

___

___

The spot-the-differences or the follow-the-path method can be used. Other problem-solving methods are the bottom-up, top-down, divide-and-conquer, shoot-from-the-hip, and move-the-problem approaches.

Verification steps can include:

Edge router R1 forms a BGP peering relationship with the ISP (R2).

Office LAN client PC-B can access the Internet via the ISP (simulated by Lo0 on R2).

The R1 routing table shows a BGP advertised default route learned via BGP from ISP router R2.

Step 6: Record the troubleshooting process and configuration changes.

Note: Section 2 of this lab includes sample troubleshooting flows, useful commands, and examples of output.

Use this log to document your actions and results during the troubleshooting process. List the commands you used to gather information. As you progress, record what you think the problem might be and which actions you will take to correct the problem.

Device	Actions and Results

Device	Actions and Results

Responses will vary but could include:

- Pings from PC-B to R2 Lo0 address (192.168.2.1) fail. DLS1 reports: "Destination host unreachable."
- Pings from PC-B to its default gateway VLAN 10 (10.1.10.254) on DLS1 succeed.
- Pings from PC-B to all other network devices in the EIGRP domain succeed.
- Pings from R1 (sourced by Fa0/1) to R2 Lo0 address (192.168.2.1) succeed.

TT-A Issues

The R2 BGP neighbor address and the R2 AS number configured on R1 are not correct. This results in a peer relationship not being established.

- The **`show ip route`** command on R1 indicates that the default route to the ISP (R2) that should be learned from R2 is missing.
- The **`show ip bgp`** command on R1 confirms that there is no BGP network entry from another AS.
- The **`show ip interface brief`** command on R1 and R2 confirms that all interfaces that should be up are up.
- The **`show ip bgp summary`** command on R1 shows that no BGP messages have been sent or received from R1. The State/PfxRcd column is Active, which indicates no peering with R2. If peering is established, it shows a number indicating the number of prefixes received from the peer.
- The **`show ip bgp neighbors`** command on R1 indicates that no BGP Open messages have been sent or received and that the remote router ID is reported as 0.0.0.0. The Routing Information Base (RIB) does not have a route to 192.168.2.2, and there is no active TCP connection.
- The **`debug ip bgp`** command on R1 confirms peering has failed between R1 and R2.

  ```
  *Nov 13 11:39:05.853: BGP: 192.168.2.2 active open failed - route to peer
  is invalid, open active delayed 24335ms (35000ms max, 60% jitter)
  ```
- The **`show ip bgp summary`** command on R1 also indicates that the remote peer neighbor address is set to 192.168.2.2, and the remote AS is set to 65503. A check of the implementation plan and design diagram indicates that the ISP (R2) neighbor address should be 192.168.2.1, and the remote AS should be 65502.

- The **show run | begin bgp** command confirms the misconfiguration of BGP on R1, including the wrong AS for R1.

Action: Change the IP address for the remote BGP peer R2, specified under the BGP routing protocol on R1, to be that of R2 loopback0 (192.168.2.1). Also change the R1 AS to 65501 and the remote peer R2 AS to 65502. See TT-A debrief for more information.

Note: If only the remote peer IP address is corrected, console messages are displayed indicating that the peer is in the wrong AS.

```
*Nov 13 12:53:44.534: %BGP-3-NOTIFICATION: received from neighbor
192.168.2.1 2/2 (peer in wrong AS) 2 bytes FFDE
```

Verification: The console message indicates that peering is successful. The BGP default route to the ISP (R2) appears in the R1 routing table, and PC-B can now ping the ISP. The **show ip bgp** command indicates that R2 is a neighbor, BGP messages are being sent and received, and one prefix has been received.

```
R1#show ip bgp summary
BGP router identifier 192.168.1.1, local AS number 65501
<Output omitted>
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.2.1     4 65502      10      10        4    0    0 00:06:12        1
```

Step 7: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with your instructor. The notes can include problems encountered, solutions applied, useful commands employed, alternate solutions and methods, and procedure and communication improvements.

____

____

____

____

____

____

____

Trouble Ticket TT-A Debrief—Instructor Notes

Two problems in this trouble ticket prevent peering between customer router R1 and ISP router R2. The first reason that the peering is not established correctly is because an incorrect AS number has been configured for neighbor router R2 under the **router bgp** configuration on router R1. During session establishment, router R1 receives AS number 65502 in the OPEN message from router R2. The AS number does not match AS number 65503, the AS number that has been configured in the neighbor statement on R1 for router ISP (R2). As a result of this mismatch, router R1 immediately closes the session. Verification of the documentation reveals that the correct AS number for router R2 is 65502.

The second issue is that the IP address for remote peer R2 loopback0 is incorrectly specified as 192.168.2.2. The address should be 192.168.2.1. As a result, R1 has no route to peer R2 and open activity is delayed and periodically retried.

To correct these problems, use the following commands on router R1:

```
no router bgp 65502

router bgp 65501
 no synchronization
```



```
neighbor 192.168.2.1 remote-as 65502
neighbor 192.168.2.1 ebgp-multihop 2
neighbor 192.168.2.1 update-source Loopback0
```

By issuing the **no router bgp 65502** command on R1, the bgp redistribution configuration is removed from EIGRP. The result is that the BGP default route from R2 is not advertised within the EIGRP network. So you must also issue the following commands on R1:

```
router eigrp 1
 redistribute bgp 65501 metric 1544 2000 255 1 1500
```

Note: Discuss the **ebgp-multihop** option with students. There are no TTs related to this, but the option is used because the neighbor address specified is that of interface Lo0 on both routers, and Lo0 is also the update source. Peer addresses 192.168.1.1 (R1) and 192.168.2.1 (R2) are not directly connected.

Alternatively, if the BGP speakers are directly connected and are just peered using their loopback interfaces, the option **disable-connected-check** can be used instead of the **ebgp-multihop** option.

Task 2: Trouble Ticket Lab 5-3 TT-B

Instructor note: This trouble ticket involves R1 issues related to BGP route injection.

Step 1: Review trouble ticket Lab 5-3 TT-B.

The next step after the peering has been established is to test the new hosted services subnet, which has been created using VLAN 130. This subnet uses the 172.30.1.0/27 IP address block that was assigned to your company by the ISP. The subnet has been configured, and a test server has been installed (simulated by DLS1 SVI VLAN 130 - 172.30.1.1). Internet clients must be able to access the subnet from ISP router R2 (simulated by Lo0 192.168.2.1). Other hosts in the EIGRP 10.1.0.0/16 domain do not require access to the hosted services subnet.

Your task is to verify VLAN configuration and routing functionality. Also, verify that traffic from the Internet can be sent to the hosted network test server in VLAN 130 via R1 and that the return traffic can be received via ISP router R2.

Step 2: Load the device trouble ticket configuration files for TT-B.

Using the procedure described in Lab 3-1, verify that the lab configuration files are present in flash. Load the configuration files as indicated in the Device Configuration File table.

Note: See Task 1, Step 2 for device access methods, usernames, and passwords after the configuration files have been loaded.

Device Configuration File Table

Device Name	File to Load	Notes
ALS1	Lab53-ALS1-TT-B-Cfg.txt	This file contains configurations different than the baseline
DLS1	Lab53-DLS1-TT-B-Cfg.txt	This file contains configurations different than the baseline
DLS2	Lab53-DLS2-TT-B-Cfg.txt	This file contains configurations different than the baseline
R1	Lab53-R1-TT-B-Cfg.txt	This file contains configuration errors
R2	Lab53-R2-TT-B-Cfg.txt	This file contains configurations different than the baseline
R3	Lab53-R3-TT-B-Cfg.txt	This file contains configurations different than the baseline
SRV1	N/A	Static IP: 10.1.50.1

		Default gateway: 10.1.50.254
PC-B	N/A	DHCP
PC-C	N/A	DHCP

Step 3: Configure SRV1 and start the syslog and TFTP servers.

Step 4: Release and renew the DHCP leases on PC-B and PC-C, as described in Task 1.

Step 5: Outline the troubleshooting approach and validation steps.

Use this space to identify your troubleshooting approach and the key steps to verify that the problem is resolved. Troubleshooting approaches to select from include the follow-the-path, spot-the-differences, bottom-up, top-down, divide-and-conquer, shoot-from-the-hip, and move-the-problem methods.

Note: In addition to a specific approach, you can use the generic troubleshooting process described at the beginning of Section 2 of this lab.

____

____

____

____

____

The follow-the-path or the divide-and-conquer method can be used. Other problem-solving methods are the bottom-up, top-down, spot-the-differences method, shoot-from-the-hip, and move-the-problem approaches.

Verification steps can include:

- Internet users (simulated by Lo0 on R2) can access the IP block assigned to the test hosted services VLAN 130.
- The ISP (R2) routing table shows the advertised VLAN 130 subnet route learned via BGP from edge router R1.

Step 6: Record the troubleshooting process and configuration changes.

Note: Section 2 of this lab includes sample troubleshooting flows, useful commands, and examples of output.

Use this log to document your actions and results during the troubleshooting process. List the commands you used to gather information. As you progress, record what you think the problem might be and which actions you will take to correct the problem.

Device	Actions and Results

Device	Actions and Results

Responses will vary but could include:

- Pings from R2 (sourced by Lo0 192.168.2.1) to the simulated hosted server on DLS1 VLAN 130 (172.30.1.1) fail.
- Pings from R1 (sourced by Lo0 192.168.1.1) to the simulated hosted server on DLS1 VLAN 130 (172.30.1.1) fail.
- Pings from R1 (sourced by Lo0 192.168.1.1) to R2 Lo0 address (192.168.2.1) succeed.

TT-B Issue 1

There is no route from R1 to the VLAN 130 hosted network on DLS1 in the R1 routing table. This prevents the route from being injected into the BGP routing table and results in no route to VLAN 130 being learned via BGP on R2.

- The **`show ip bgp neighbors`** command on R1 indicates that it is a peer with R2.
- The **`show ip route`** command on R1 indicates that the default route to the ISP (R2) sent by R2 via BGP is present, and that the gateway of last resort is 192.168.2.1 to network 0.0.0.0. However, there is no route to the VLAN 130 hosted services network (172.30.1.0/27).
- The **`show ip bgp`** command on R1 confirms that the default route (network 0.0.0.0) to the ISP (R2) with a next hop of 192.168.2.1 (R2 Lo0) is listed, but the hosted network (172.30.1.0/27) is not.
- The **`show ip route`** command on R2 indicates that the hosted network (172.30.1.0/27) from R1 that should be advertised to the ISP is missing.
- The **`show ip bgp`** command on R2 confirms that only the default route is listed with a next hop of 0.0.0.0, and that there is no BGP network entry from another AS.
- The **`show ip interface brief`** on R1 and R2 indicates that all interfaces that should be up are up.
- The **`show ip route`** command on DLS1 indicates that the hosted network VLAN 130 (172.30.1.0/27) is correctly configured and directly connected.
- The **`show ip interface brief`** command on DLS1 indicates that SVI VLAN 130 is up/up and has the correct IP address.
- The **`show interface vlan 130`** command on DLS1 confirms that SVI VLAN 130 has the correct subnet mask.

- The **`show ip protocols`** command on DLS1 indicates that the VLAN 130 subnet is not advertised under EIGRP and that interface VLAN 130 is a passive interface. This could be viewed as a problem, but there is no need to advertise this subnet to all other devices in the EIGRP domain because the other hosts in the 10.1.0.0/16 network do not need access to it.
- Check R1 for a static route to VLAN 130 on R1 using the **`show run | begin ip route`** command. There is one static route to the R2 BGP neighbor Lo0 IP address, but no static route to DLS1 VLAN 130.

Action: Add a static route on R1 to DLS1 VLAN 130 172.30.1.0/27 via the DLS1 F0/5 IP address 10.1.2.1. See TT-B debrief for more information.

Verification: The route to DLS1 network 172.30.1.0/27 is now in the R1 routing table. However, the **`show ip bgp`** command on R1 indicates that the route is not listed in the BGP table, and that R2 does not have the BGP learned route in its routing table. There must be another problem.

TT-B Issue 2

The network statement specified for the hosted services VLAN under BGP is missing the mask option, which causes it to default to a classful address. This entry does not match the default route configured on R1 and results in no route to VLAN 130 being injected into the BGP table.

- The **`show run | begin bgp`** command on R1 indicates that there is a network statement for network 172.30.1.0. under BGP. However, no mask is specified. Therefore, BGP assumes it is a classful B address (/16). This network statement does not match the 172.30.1.0/27 static route in the R1 routing table and, as a result, R1 does not inject the route into the BGP table.

Action: Change the network statement under BGP to include the mask 255.255.255.224 so that it matches the route in the R1 routing table. See TT-B debrief for more information.

Verification:

- A console message indicates that BGP will look for the origin of the new route (in the R1 routing table).

```
*Nov 14 14:54:53.055: BGP: Applying map to find origin for 172.30.1.0/27
```

- The **`show ip bgp`** command on R1 indicates that the route is now listed in the BGP table, and R2 now has the BGP learned route 172.30.1.0/27 via next hop 192.168.1.1 (R1 Lo0) in its routing table.
- Pings sourced from the Internet (R2 Lo0) to the hosted services network on VLAN 130 (172.30.1.1) are successful.

Step 7: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with your instructor. The notes can include problems encountered, solutions applied, useful commands employed, alternate solutions and methods, and procedure and communication improvements.

____

____

____

____

____

____

____

Trouble Ticket TT-B Debrief—Instructor Notes

Two issues are preventing BGP from injecting the route to the hosted service networks on R1 so that R2 can receive it. The first is that there is no route in the R1 routing table. The second is that the network statement under BGP on R1 is too general and does not match the static route that will be added to the R1 routing table. For BGP to advertise a route, it must have an exact match in the routing table (either static, directly connected, or learned via a routing protocol).

TT-B—Issue 1

There must be a route to the target network in the R1 routing table for BGP to inject the route into the BGP table. There is no route (static or dynamic) to DLS1 VLAN 130 subnet 172.30.1.0/27 in the routing table for R1. The route could have been learned from DLS1 via EIGRP, but there is no need to advertise this subnet to all other devices in the EIGRP domain because the other hosts in the 10.1.0.0/16 network do not require access to it. This problem can corrected by adding a static route on R1 using the following command:

```
ip route 172.30.1.0 255.255.255.224 10.1.2.1
```

The route to DLS1 network 172.30.1.0/27 is now in the R1 routing table, but BGP is still not injecting the route into the R1 BGP table.

TT-B—Issue 2

A second problem in this ticket is that the network statement for this prefix, configured under the **router bgp** process on router R1, is not specific enough. BGP look for network with prefix 172.30.1.0 and with the default netmask 255.255.0.0 because no mask was specified. The required matching route in the routing table is not present. As a result, the prefix is not injected in the BGP table on router R1 and cannot be received via BGP by R2.

To resolve this issue, remove the less specific network statement under BGP and add a new network statement to include the mask 255.255.255.224 so that it matches the route in the R1 routing table.

```
router bgp 65501
 no network 172.30.1.0
 network 172.30.1.0 mask 255.255.255.224
```

Note: Point out that the default route configured on R2 (**`network 0.0.0.0`** command under BGP) to be advertised to R1 is only injected into the R2 BGP table because of the addition of the static default route to null0 (**`ip route 0.0.0.0 0.0.0.0 Null0`** command). The default route to null0 places the route in the R2 routing table. This is what allows it to be injected into the R2 BGP table and then passed to R1.

Task 3: Trouble Ticket Lab 5-3 TT-C

Instructor note: This trouble ticket involves R1 prefix advertisement and issues related to a prefix-list filter on R2.

Step 1: Review trouble ticket Lab 5-3 TT-C.

Your ISP uses prefix lists to ensure that customers do not announce routes that have not been officially assigned to them. This is critical for an ISP because if two customers were to accidently announce the same route as their own, it would create problems for both customers and the ISP. After you corrected the static route and BGP route injection issues on R1, one of your colleagues was working with the hosted services test network and made some changes. Now he can no longer ping from the hosted network test server (DLS1 VLAN 130) to the ISP. The ISP is also not receiving the advertisement for the hosted services subnet. Your task is to diagnose this problem and resolve it.

Step 2: Load the device trouble ticket configuration files for TT-C.

Using the procedure described in Lab 3-1, verify that the lab configuration files are present in flash. Load the proper configuration files as indicated in the Device Configuration File table.

Note: See Task 1, Step 2 for device access methods, usernames, and passwords after the configuration files have been loaded.

Device Configuration File Table

Device Name	File to Load	Notes
ALS1	Lab53-ALS1-TT-C-Cfg.txt	This file contains configurations different than the baseline
DLS1	Lab53-DLS1-TT-C-Cfg.txt	This file contains configurations different than the baseline
DLS2	Lab53-DLS2-TT-C-Cfg.txt	This file contains configurations different than the baseline
R1	Lab53-R1-TT-C-Cfg.txt	This file contains configuration errors
R2	Lab53-R2-TT-C-Cfg.txt	This file contains configurations different than the baseline
R3	Lab53-R3-TT-C-Cfg.txt	This file contains configurations different than the baseline
SRV1	N/A	Static IP: 10.1.50.1 Default gateway: 10.1.50.254
PC-B	N/A	DHCP
PC-C	N/A	DHCP

Step 3: Configure SRV1 and start the syslog and TFTP servers, as described in Task 1.

Step 4: Release and renew the DHCP leases on PC-B and PC-C, as described in Task 1.

Step 5: Outline the troubleshooting approach and validation steps.

Use this space to identify your troubleshooting approach and the key steps to verify that the problem is resolved. Troubleshooting approaches to select from include the follow-the-path, spot-the-differences, bottom-up, top-down, divide-and-conquer, shoot-from-the-hip, and move-the-problem methods.

Note: In addition to a specific approach, you can use the generic troubleshooting process described at the beginning of Section 2 of this lab.

____

____

____

____

____

____

The follow-the-path or the spot-the-differences method can be used. Other problem-solving methods are the bottom-up, top-down, divide-and-conquer, shoot-from-the-hip, and move-the-problem approaches.

Verification steps can include:

- Internet users (simulated by Lo0 on R2) can access the IP block assigned to the test hosted services VLAN 130.
- The ISP (R2) routing table shows the advertised VLAN 130 subnet route learned via BGP from edge router R1.

Step 6: Record the troubleshooting process and configuration changes.

Note: Section 2 of this lab includes sample troubleshooting flows, useful commands, and examples of output.

Use this log to document your actions and results during the troubleshooting process. List the commands you used to gather information. As you progress, record what you think the problem might be and which actions you will take to correct the problem.

Device	Actions and Results

Responses will vary but could include:

- Pings from R2 (sourced by Lo0 192.168.2.1) to the simulated hosted server on DLS1 VLAN 130 (172.30.1.1) fail.
- Pings from R1 (sourced by Lo0 192.168.1.1) to R2 Lo0 address (192.168.2.1) succeed.

TT-C Issues

R1 has been configured with a static route to DLS1 using an incorrect mask (/24 should be a /27). The network advertised under BGP on R1 is 172.30.1.0/24 but should be 172.30.1.0/27. The ISP has configured a prefix list filter that accepts only a network advertisement of 172.30.1.0/27 via BGP from the customer.

- The **`show ip bgp neighbors`** command on R1 indicates that it is a peer with R2.
- The **`show ip route`** command on R1 indicates that the default route to the ISP (R2) sent by R2 via BGP is present as well as a static route to the VLAN 130 hosted services network (172.30.1.0/24).
- The **`show ip bgp`** command on R1 confirms that the default route (network 0.0.0.0) to the ISP (R2) with a next hop of 192.168.2.1 (R2 Lo0) is listed as well as the hosted network 172.30.1.0/24 with a next hop of 10.1.2.1 (DLS1 Fa0/5).
- The **`show ip route`** command on R2 indicates that the hosted network from R1 that should be advertised to the ISP is missing.

- The **show ip bgp** command on R2 confirms that only the default route is listed with a next hop of 0.0.0.0 and no BGP network entry from the R1 AS.
- The **show ip interface brief** command on R1 and R2 indicates that all interfaces that should be up are up.
- The **show ip route** command on DLS1 indicates that the hosted network VLAN 130 (172.30.1.0/27) is correctly configured and directly connected.
- The **show ip interface brief** command on DLS1 indicates that SVI VLAN 130 is up and has the correct IP address.
- The **show interface vlan 130** command on DLS1 confirms that SVI VLAN 130 has the correct IP address (172.30.1.1) and subnet mask (/27).
- The **show run | begin bgp** command on R2 confirms that the ISP has configured a prefix list named **cust-ctrl** and has applied it inbound to any prefixes advertised by R1 (neighbor 192.168.1.1) on the R2 S0/0/0 interface, which will filter (block) BGP updates from any network other than 172.30.1.0/27.
- Referring back to the previous **show ip route** and **show ip bgp** command output on R1, we see that the network in the R1 routing table and the BGP table is 172.30.1.0/24 and not 172.30.1.0/27. Thus R1 is attempting to advertise a 256 (/24) address block instead of 32 (/27). The address block assigned to the customer is 172.30.1.0/27, not 172.30.1.0/24.

Action (See TT-C debrief for more information)**:**

- Change the static route on R1 to reference the 172.30.1.0/27 network (instead of 172.30.1.0/24).
- Change the BGP network statement mask on R1 to advertise the 172.30.1.0/27 network.

Verification:

- The **show ip bgp** command on R1 indicates that the 172.30.2.0/27 route is now listed in the BGP table, and R2 now has the BGP learned route 172.30.1.0/27 via next hop 192.168.1.1 (R1 Lo0) and the route is in its routing table.
- Pings sourced from the Internet (R2 Lo0 to VLAN 130 IP address 172.30.1.1) to the hosted service network on VLAN 130 (172.30.1.1) are successful.

Step 7: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with your instructor. The notes can include problems encountered, solutions applied, useful commands employed, alternate solutions and methods, and procedure and communication improvements.

____

____

____

____

____

____

____

Trouble Ticket TT-C Debrief—Instructor Notes

TT-C Issue 1

The problem in this ticket is caused by a mistake in the advertised prefix from the customer to the ISP. The ISP uses prefix lists to ensure that customers do not announce routes that have not been officially assigned to them.

ISPs do this to prevent customers from announcing routes that they do not own. They also typically include statements to exclude private IP addresses (like 10.0.0.0).

The ISP has configured a prefix list named **cust-ctrl** on R2 and has applied it inbound to any prefixes advertised by R1 (neighbor 192.168.1.1). This filter will block BGP updates from neighbor 192.168.1.1 for any network other than 172.30.1.0/27. This is accomplished by the following commands on R2:

```
ip prefix-list cust-ctrl seq 10 permit 172.30.1.0/27

router bgp 65502
neighbor 192.168.1.1 prefix-list cust-ctrl in
```

The customer's network administrator thought the hosted services network was a /24 rather than the correct /27. R1 was attempting to advertise a 256-address block (/24) instead of a 32-address block (/27). The address block assigned to the customer is 172.30.1.0/27, not 172.30.1.0/24. The ISP actually received the advertisement from R1, but it was rejected.

The solution is to change the static route on R1 to reference the 172.30.1.0/27 network (instead of 172.30.1.0/24) and to change the BGP network statement on R1 to advertise the 172.30.1.0/27 network. This can be accomplished by entering the following commands on R1:

```
no ip route 172.30.1.0 255.255.255.0 10.1.2.1
ip route 172.30.1.0 255.255.255.224 10.1.2.1

router bgp 65501
 no network 172.30.1.0 mask 255.255.255.0
 network 172.30.1.0 mask 255.255.255.224
```

Note: Simply changing the configurations might not be enough to have the configuration take effect. It might be necessary to either shut down an interface between the two routers or use the **`clear ip bgp *`** command on R1 and R2.

Section 2—Troubleshooting Reference Information

General Troubleshooting Process

As a general guideline, you can use the following general troubleshooting process described in the course.

1. Define the problem (symptoms).
2. Gather information.
3. Analyze the information.
4. Propose a hypothesis (possible cause).
5. Test the hypothesis.
6. Eliminate or accept the hypothesis.
7. Solve the problem.
8. Document the problem.

Command Summary

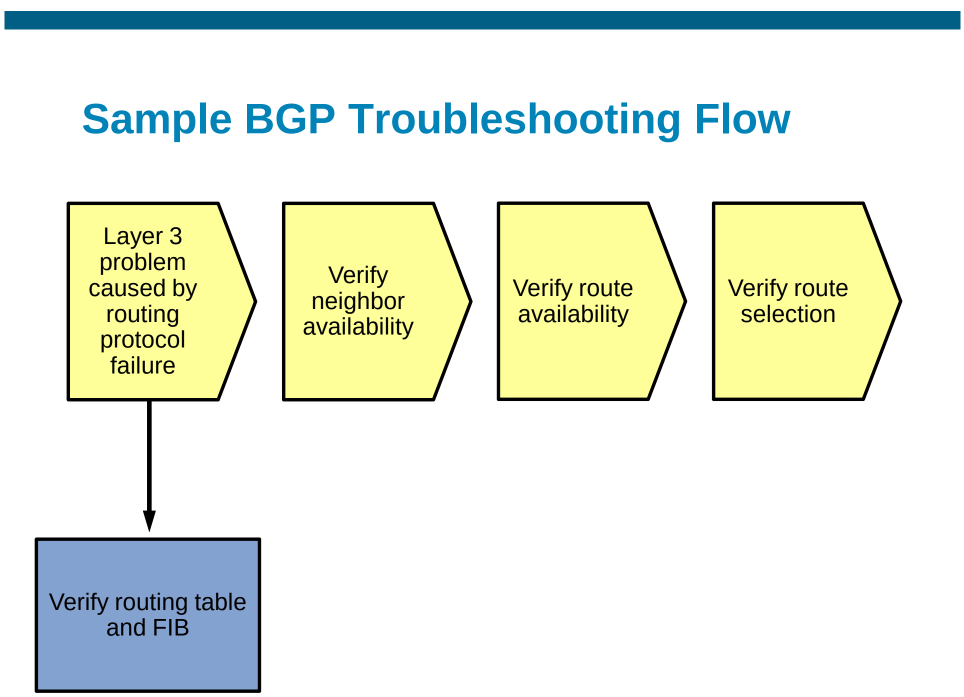
The table lists useful commands. Sample output is shown on the following pages.

Command	Key Information Displayed
show ip route or **show ip route** *ip-addr*	Displays the entire routing table or information for a particular destination address.
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.

Lab 5-3: Sample Troubleshooting Flows

The figure illustrates an example of a method that you could follow to diagnose and resolve problems related to BGP.



The typical trigger to start investigating BGP operation is when you are using BGP as an exterior gateway protocol to connect to other autonomous systems and you are troubleshooting IP connectivity to a destination in a different AS. Some reasons to start investigating BGP are if a route to the destination network is missing from the routing table of one of the routers, a different route than expected was selected to forward the packets to that destination, or return traffic from the other AS is not making it back to the source.

Troubleshooting problems with missing return traffic usually requires coordination with those responsible for the routing in the destination AS and possibly even intermediate autonomous systems. The only thing you can verify from within your own AS is if your routing information is correctly passed to the neighbor AS. Propagation of your routes beyond your direct peers cannot be verified without access to routers in other autonomous systems.

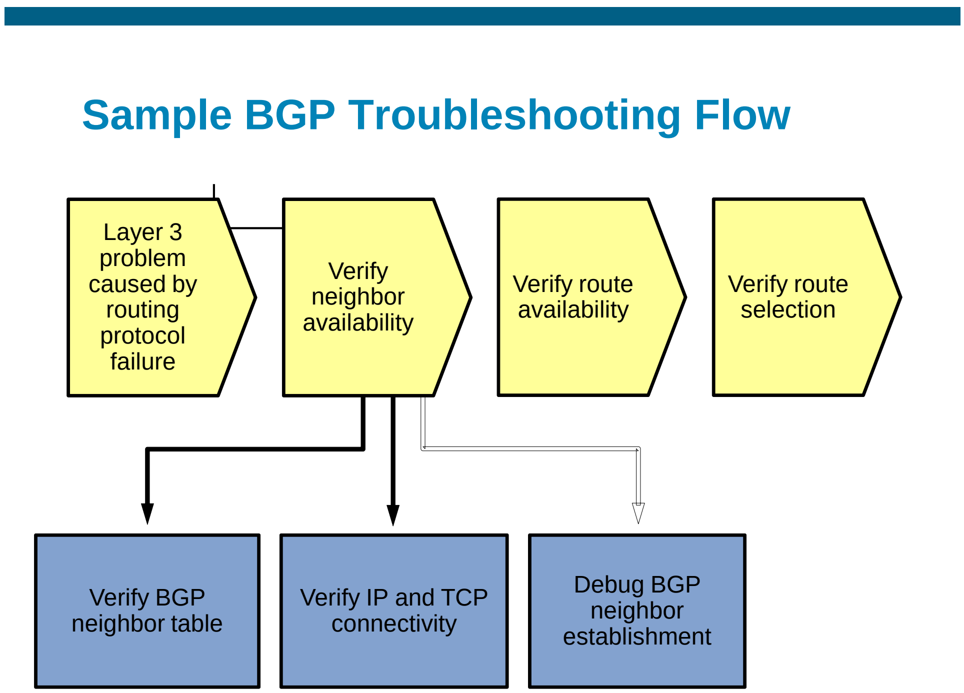
Therefore, this flow focuses mainly on troubleshooting traffic to a destination network in a different AS. However, commands that are helpful in troubleshooting route advertisement to a different AS are also highlighted, if appropriate.

To install a route into the routing table, each router that uses BGP goes through several stages:

1. Establish neighbor relationships with its configured neighbors.
2. Exchange routing information with neighbors and store the received information in the BGP table.
3. Select the best route from the available routes and install it in the routing table.

Errors during any of these stages can cause routing information to be missed or incorrect routing information to be installed in the routing table.

The order in which the different stages are verified is not important, as long as a structured approach is used.



BGP does not discover neighbors. Neighbor relationships are established based on an explicit configuration on both routers that participate in the peering session.

BGP uses TCP as a transport protocol. Establishing a peering relationship always starts with the establishment of a TCP session on port 179 between the configured neighbor IP addresses. By default, both neighbors attempt to initiate the TCP session to the configured IP address of the neighbor. When a router receives an incoming session request, it compares the source IP address of the session to its list of configured neighbors. It only accepts the session if the source IP address matches one of the IP addresses of its configured neighbors. Therefore, it is important that a router always sources the BGP packets that it sends to a specific neighbor from the IP address that has been configured as the neighbor IP address on the peer router. For neighbors that are directly connected on an interface, the correct source address is automatically used. For neighbors that are not directly connected, the appropriate source IP address for the session to a neighbor might need to be selected with the **`neighbor`** *`ip-address`* **`update-source`** *`interface-id`* command.

Verify the BGP Neighbor Table

```
R1#show ip bgp
BGP table version is 2, local router ID is 192.168.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 0.0.0.0          192.168.2.1              0             0 65502 i

R1#show ip bgp summary
BGP router identifier 192.168.1.1, local AS number 65501
BGP table version is 3, main routing table version 3
2 network entries using 264 bytes of memory
2 path entries using 104 bytes of memory
3/2 BGP path/bestpath attribute entries using 504 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory
BGP using 928 total bytes of memory
BGP activity 2/0 prefixes, 2/0 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.2.1     4 65502      36      36        3    0    0 00:33:01        1
```

To verify that all expected neighbor relationships are operational, you can display a summary of the BGP neighbor table using the **`show ip bgp summary`** command. 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.

For each neighbor, the configured IP address and AS of the neighbor are listed. The Up/Down column lists the time that has elapsed since the last state change. For a neighbor that is currently up, it lists the time elapsed since the session was established. For a neighbor that is down, it lists the time elapsed since the session was lost.

The most important column to verify the operational state of the neighbor is State/PfxRcd. This column can display the following values:

- **Idle** – Indicates that there is no session with the peer, and the router is not currently attempting to establish a session with the peer. The router is ready to accept incoming sessions.
- **Idle (Admin)** – Indicates that the session has been administratively shut down with the **`neighbor`** *`ip-address`* **`shutdown`** command.
- **Active** – The router is actively trying to open a TCP session with the neighbor. If it does not succeed in establishing the session, the router toggles between the Idle and Active states
- **Open Sent** – An Open message has been sent to the neighboring router containing the router ID, AS number, BGP version, hold timer, and capabilities.
- **Open Confirm** – An Open message from the neighbor has been received, the parameters in the message have been processed and accepted, and a hello message has been sent to acknowledge the acceptance of the neighbor’s Open message.

- **Number of received prefixes** – After an acknowledgment from the neighbor confirming the reception of this router's Open message, the state of the session moves to the Established state. At this point, the State/PfxRcd column does not list the state. It shows the number of prefixes that have been received from that neighbor and installed in the BGP table. The desired result is to see a number listed in this column, because that indicates that the session with the peer has been successfully established.

The Open Sent and Open Confirm states are transitory states. When the state for a neighbor toggles between Active and Idle, this indicates that the router is not successful in establishing a session with the neighbor.

You can use the **`show ip bgp neighbor`** *`ip-address`* command to display additional parameters and extensive statistics about the peering session. For more information about these parameters and statistics, see the BGP command references on www.cisco.com.

Verify IP and TCP Connectivity

```
R1#debug ip tcp transactions
TCP special event debugging is on

R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#no router bgp 65501
R1(config)#
*Nov 16 17:21:35.102: %BGP-5-ADJCHANGE: neighbor 192.168.2.1 Down BGP protocol i
nitialization
R1(config)#
*Nov 16 17:21:35.102: TCP0: state was ESTAB -> FINWAIT1 [179 -> 192.168.2.1(1188
9)]
*Nov 16 17:21:35.102: TCP0: sending FIN
*Nov 16 17:21:35.126: Released port 179 in Transport Port Agent for TCP IP type
0 delay 240000
*Nov 16 17:21:35.126: TCP0: state was LISTEN -> CLOSED [179 -> 192.168.2.1(0)]
*Nov 16 17:21:35.126: TCB 0x66EE8F34 destroyed
*Nov 16 17:21:35.138: TCP0: state was FINWAIT1 -> FINWAIT2 [179 -> 192.168.2.1(1
1889)]
*Nov 16 17:21:35.138: TCP0: FIN processed
*Nov 16 17:21:35.138: TCP0: state was FINWAIT2 -> TIMEWAIT [179 -> 192.168.2.1(1
1889)]
R1(config)#
*Nov 16 17:21:50.286: Reserved port 0 in Transport Port Agent for TCP IP type 0
*Nov 16 17:21:50.286: TCP: sending RST, seq 0, ack 2752306274
*Nov 16 17:21:50.286: TCP: sent RST to 192.168.2.1:41738 from 192.168.1.1:179
*Nov 16 17:21:50.290: Released port 0 in Transport Port Agent for TCP IP type 0
delay 240000
*Nov 16 17:21:50.290: TCP0: state was LISTEN -> CLOSED [0 -> UNKNOWN(0)]
*Nov 16 17:21:50.290: TCB 0x66F17E40 destroyed
R1(config)#
*Nov 16 17:21:55.006: Reserved port 0 in Transport Port Agent for TCP IP type 0
*Nov 16 17:21:55.006: TCP: sending RST, seq 0, ack 3974493125
*Nov 16 17:21:55.006: TCP: sent RST to 192.168.2.1:47416 from 192.168.1.1:179
*Nov 16 17:21:55.006: Released port 0 in Transport Port Agent for TCP IP type 0
delay 240000


R1(config)#router bgp 65501
R1(config-router)#no synchronization
R1(config-router)#bgp log-neighbor-changes
R1(config-router)#neighbor 192.168.2.1 remote-as 65502
R1(config-router)#neighbor 192.168.2.1 ebgp-multihop 2
```

```
R1(config-router)#neighbor 192.168.2.1 update-source Loopback0
*Nov 16 17:28:46.549: TCB65950C34 created
*Nov 16 17:28:46.549: TCB65950C34 setting property TCP_PMTU (38) 66A7C214
*Nov 16 17:28:46.549: TCB65950C34 setting property TCP_TOS (11) 66A7C220
*Nov 16 17:28:46.549: TCB65950C34 setting property TCP_VRFTABLEID (20) 66F233F8
*Nov 16 17:28:46.549: TCB65950C34 setting property TCP_IN_TTL (29) 66A7C200
*Nov 16 17:28:46.553: TCB65950C34 setting property TCP_OUT_TTL (30) 66A7C200
*Nov 16 17:28:46.553: TCB65950C34 setting property TCP_OUT_TTL (30) 66F2359A
*Nov 16 17:28:46.553: TCB65950C34 bound to UNKNOWN.179
*Nov 16 17:28:46.553: TCB65950C34 setting property TCP_ACCESS_CHECK (5) 60B47108

*Nov 16 17:28:46.553: TCB65950C34 setting property TCP_MD5KEY (4) 0
*Nov 16 17:28:46.553: Reserved port 179 in Transport Port Agent for TCP IP type
0
*Nov 16 17:28:46.553: TCB65950C34 listening with queue 1
*Nov 16 17:28:46.585: TCB65950C34 setting property TCP_IN_TTL (29) 66A7C278
*Nov 16 17:28:46.585: TCB65950C34 setting property TCP_OUT_TTL (30) 66A7C278
*Nov 16 17:28:46.585: TCB65950C34 setting property TCP_OUT_TTL (30) 66F2359A
R1(config-router)#
*Nov 16 17:28:50.581: TCB67096718 created
*Nov 16 17:28:50.581: TCB67096718 setting property TCP_VRFTABLEID (20) 66F233F8
*Nov 16 17:28:50.581: TCB67096718 setting property TCP_MD5KEY (4) 0
*Nov 16 17:28:50.581: TCB67096718 setting property TCP_ACK_RATE (32) 66F1B4D4
*Nov 16 17:28:50.581: TCB67096718 setting property TCP_TOS (11) 66F1B4C0
*Nov 16 17:28:50.581: TCB67096718 setting property TCP_PMTU (38) 66F1B48C
*Nov 16 17:28:50.581: TCB67096718 setting property TCP_IN_TTL (29) 66F1B478
*Nov 16 17:28:50.581: TCB67096718 setting property TCP_OUT_TTL (30) 66F1B478
*Nov 16 17:28:50.581: TCB67096718 setting property TCP_OUT_TTL (30) 66F2359A
*Nov 16 17:28:50.581: TCP: Random local port generated 30517, network 1
*Nov 16 17:28:50.581: TCB67096718 bound to 192.168.1.1.30517
*Nov 16 17:28:50.581: TCB67096718 setting property TCP_RTRANSTMO (31) 66F1B4D8
*Nov 16 17:28:50.581: Reserved port 30517 in Transport Port Agent for TCP IP typ
e 1
*Nov 16 17:28:50.581: TCP: sending SYN, seq 3632881552, ack 0
*Nov 16 17:28:50.581: TCP0: Connection to 192.168.2.1:179, advertising MSS 536
*Nov 16 17:28:50.585: TCP0: state was CLOSED -> SYNSENT [30517 -> 192.168.2.1(17
9)]
*Nov 16 17:28:50.593: TCP0: state was SYNSENT -> ESTAB [30517 -> 192.168.2.1(179
)]
*Nov 16 17:28:50.593: TCP: tcb 67096718 connection to 192.168.2.1:179, peer MSS
536, MSS is 536
*Nov 16 17:28:50.593: TCB67096718 connected to 192.168.2.1.179
*Nov 16 17:28:50.593: TCB67096718 setting property TCP_NO_DELAY (0) 66F1B4D8
*Nov 16 17:28:50.593: TCB67096718 setting property TCP_RTRANSTMO (31) 66F1B4D8
*Nov 16 17:28:50.621: %BGP-5-ADJCHANGE: neighbor 192.168.2.1 Up
R1(config-router)#
*Nov 16 17:28:50.821: TCP0: ACK timeout timer expired
R1(config-router)#do u all
All possible debugging has been turned off
```

If a session to one of the neighbors is not established correctly, you can take several steps to diagnose the issue. The first step is to test IP connectivity to the IP address of the neighbor by using the **ping** command. Make sure that you specify the same source interface that is used as the source interface for the BGP session. If the ping fails, initiate a troubleshooting process to first restore IP connectivity to the neighbor.

If the ping is successful, the next step is to determine whether the TCP session with the neighbor is established and successively torn down again, or if the TCP session is never established.

You can use the **`debug ip tcp transactions`** command to investigate whether the TCP session is refused (indicated by the reception of a TCP RST), established and subsequently torn down again (indicated by the normal TCP initiation and termination handshakes), or no response is received at all from the neighbor.

In the example output above, you can see that the TCP session to IP address 192.168.2.1 and TCP port 179 is refused by the peer, as indicated by the reception of the TCP RST from the peer. Clues like these can help eliminate possible problem causes. For instance, in this particular example, the output rules out an access list as the cause of the problem, because a TCP RST has been successfully received from the neighbor in response to the transmitted TCP SYN. In general, the fact that the peer refuses the session indicates that it does not recognize the session as coming from one of its configured neighbors. Possible causes are a missing neighbor statement or a mismatch between the configured IP address on the neighbor and the source IP address used by this router. Note that the source IP address and TCP port of the session are also displayed in the output of the debug as “bound to 192.168.1.1.30517.” You must work together with the party that manages the peer router to determine the exact cause of the problem.

Debug BGP Neighbor Establishment

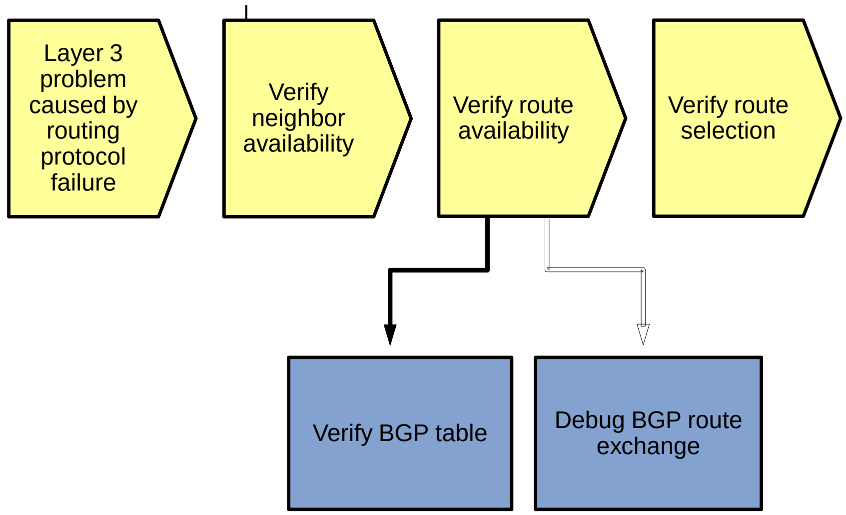
```
R1#debug ip bgp
BGP debugging is on for address family: IPv4 Unicast

R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface s0/0/0
R1(config-if)#shutdown
R1(config-if)#
*Nov 16 17:38:51.181: %LINK-5-CHANGED: Interface Serial0/0/0, changed state to a
dministratively down
*Nov 16 17:38:52.181: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/
0, changed state to down

R1(config-if)#do clear ip bgp 192.168.2.1
R1(config-if)#
*Nov 16 17:40:21.093: BGPNSF state: 192.168.2.1 went from nsf_not_active to nsf_
not_active
*Nov 16 17:40:21.093: BGP: 192.168.2.1 went from Established to Idle
*Nov 16 17:40:21.093: %BGP-5-ADJCHANGE: neighbor 192.168.2.1 Down User reset
R1(config-if)#
*Nov 16 17:40:21.093: BGP: 192.168.2.1 closing
R1(config-if)#
*Nov 16 17:40:22.973: BGP: 192.168.2.1 went from Idle to Active
*Nov 16 17:40:22.973: BGP: 192.168.2.1 active open failed - route to peer is inv
alid, open active delayed 26762ms (35000ms max, 60% jitter)


R1(config-if)#interface s0/0/0
R1(config-if)#no shutdown
R1(config-if)#
*Nov 16 17:40:51.041: %LINK-3-UPDOWN: Interface Serial0/0/0, changed state to up

R1(config-if)#
*Nov 16 17:40:52.045: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/
0, changed state to up
R1(config-if)#
*Nov 16 17:41:11.365: BGP: 192.168.2.1 open active, local address 192.168.1.1
*Nov 16 17:41:11.373: BGP: 192.168.2.1 read request no-op
*Nov 16 17:41:11.377: BGP: 192.168.2.1 went from Active to OpenSent
*Nov 16 17:41:11.377: BGP: 192.168.2.1 sending OPEN, version 4, my as: 65501, ho
ldtime 180 seconds
*Nov 16 17:41:11.377: BGP: 192.168.2.1 send message type 1, length (incl. header
```



```
) 53
*Nov 16 17:41:11.397: BGP: 192.168.2.1 rcv message type 1, length (excl. header)
 34
*Nov 16 17:41:11.397: BGP: 192.168.2.1 rcv OPEN, version 4, holdtime 180 seconds

*Nov 16 17:41:11.397: BGP: 192.168.2.1 rcv OPEN w/ OPTION parameter len: 24
*Nov 16 17:41:11.397: BGP: 192.168.2.1 rcvd OPEN w/ optional parameter type 2 (C
apability) len 6
*Nov 16 17:41:11.397: BGP: 192.168.2.1 OPEN has CAPABILITY code: 1, length 4
*Nov 16 17:41:11.397: BGP: 192.168.2.1 OPEN has MP_EXT CAP for afi/safi: 1/1
*Nov 16 17:41:11.397: BGP: 192.168.2.1 rcvd OPEN w/ optional parameter type 2 (C
apability) len 2
*Nov 16 17:41:11.397: BGP: 192.168.2.1 OPEN has CAPABILITY code: 128, length 0
*Nov 16 17:41:11.397: BGP: 192.168.2.1 OPEN has ROUTE-REFRESH capability(old) fo
r all address-families
*Nov 16 17:41:11.397: BGP: 192.168.2.1 rcvd OPEN w/ optional parameter type 2 (C
apability) len 2
*Nov 16 17:41:11.397: BGP: 192.168.2.1 OPEN has CAPABILITY code: 2, length 0
*Nov 16 17:41:11.397: BGP: 192.168.2.1 OPEN has ROUTE-REFRESH capability(new) fo
r all address-families
*Nov 16 17:41:11.397: BGP: 192.168.2.1 rcvd OPEN w/ optional parameter type 2 (C
apability) len 6
*Nov 16 17:41:11.397: BGP: 192.168.2.1 OPEN has CAPABILITY code: 65, length 4
*Nov 16 17:41:11.397: BGP: 192.168.2.1 OPEN has 4-byte ASN CAP for: 65502
BGP: 192.168.2.1 rcvd OPEN w/ remote AS 65502, 4-byte remote AS 65502
*Nov 16 17:41:11.401: BGP: 192.168.2.1 went from OpenSent to OpenConfirm
*Nov 16 17:41:11.405: BGP: 192.168.2.1 went from OpenConfirm to Established
*Nov 16 17:41:11.405: %BGP-5-ADJCHANGE: neighbor 192.168.2.1 Up
R1(config-if)#
*Nov 16 17:41:11.433: BGP_Router: unhandled major event code 128, minor 0
R1(config-if)#do u all
All possible debugging has been turned off
```

If the TCP session is successfully established but consecutively torn down again, the likely cause is that one of the BGP peers is rejecting one of the parameters in the received Open message from the peer. The **`debug ip bgp`** command 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 invalid router ID, the debug output displays information about the exact cause.

Sample BGP Troubleshooting Flow



After you have verified that neighbor relationships have been established as expected, verify that the route for the destination network that you are troubleshooting has been received correctly from all appropriate neighbors. BGP stores all routes that it receives from its neighbors in the BGP table and then selects the best route for each prefix to be installed in the routing table and advertised to other neighbors.

By investigating all available paths to the destination network in the BGP table, you can see if all the paths you expected to find are available. If multiple paths to the same prefix are listed, you can see which one was selected. In addition, you can see all the associated BGP attributes for the route, which can be useful to verify the path selection process and the results of the possible attribute manipulation by route maps that are used.

If routes are missing from the BGP table, you might need to debug the BGP route exchange process to see if they were not received or not entered into the BGP table.

Debug BGP Neighbor Establishment

```
R1#show ip bgp 0.0.0.0 0.0.0.0
BGP routing table entry for 0.0.0.0/0, version 4
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  65502
    192.168.2.1 from 192.168.2.1 (192.168.2.1)
      Origin IGP, metric 0, localpref 100, valid, external, best
```

In the output above, the prefix is 0.0.0.0/0, the AS path is 65502, and the next hop is 192.168.2.1.

```
R1#show ip bgp 172.30.1.0 255.255.255.224
BGP routing table entry for 172.30.1.0/27, version 5
Paths: (1 available, best #1, table Default-IP-Routing-Table)
Flag: 0x820
  Advertised to update-groups:
        1
  Local
    10.1.2.1 from 0.0.0.0 (192.168.1.1)
      Origin IGP, metric 0, localpref 100, weight 32768, valid, sourced, local,
```

```
R2>sh ip bgp 172.30.1.0/27
BGP routing table entry for 172.30.1.0/27, version 5
Paths: (1 available, best #1, table Default-IP-Routing-Table)
Flag: 0x820
  Not advertised to any peer
  65501
    192.168.1.1 from 192.168.1.1 (192.168.1.1)
      Origin IGP, metric 0, localpref 100, valid, external, best
```

The BGP table contains all routes that were received from all neighbors and were not denied by an incoming access list, prefix list, or route map. In the output for R2 above, the prefix is 172.30.1.0/27, the AS path is 65501 to the network, and the next hop is 192.168.1.1.

When you issue the **`show ip bgp`** *`network mask`* command to display the content 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). On the following lines, the other BGP attributes of the route, such as the next hop, origin code, and local preference, are listed. In addition, other information associated with the route is displayed. For example, the route is marked as internal if it was received from a BGP neighbor in the same AS. It is marked as external if it was received from a neighbor in a different AS. The path that was selected as the best path by the BGP path selection algorithm is marked as "best."

Note: The following section uses some sample output not produced from the equipment in this lab to demonstrate how to interpret the output of this command. This output is interspersed with comments that explain the important fields and their interpretation.

```
IRO1#show ip bgp 172.34.224.0 255.255.224.0
BGP routing table entry for 172.34.224.0/19, version 98
Paths: (2 available, best #1, table Default-IP-Routing-Table)
```

Two paths are available to reach prefix 172.34.224.0/19. The first path listed has been selected as the best path.

```
Advertised to update-groups:
    2
```

The best path is advertised to all neighbors in update group 2. Use the **`show ip bgp update-group`** command to view the neighbors that are members of a specific update group.

```
65525 65486
```

The first path has 65525 65486 as its AS path attribute, which indicates that the route has originated in AS 65486 and then passed to AS 65525, which subsequently passed it to this AS.

```
  192.168.224.254 from 192.168.224.254 (192.168.100.1)
```

The BGP next hop for this route is 192.168.224.254. The route was received from neighbor 192.168.224.254. The router ID of that neighbor is 192.168.100.1.

```
   Origin IGP, localpref 100, valid, external, best
```

The origin attribute for this route is IGP, and the local preference attribute has a value of 100. This route is a valid route received from an external BGP peer, and it has been selected as the best path.

```
 64566 65486
```

The second path has 64566 65486 as its AS path attribute, which indicates that the route has originated in AS 65486 and then passed to AS 64566, which subsequently passed it to this AS.


```
            172.24.244.86 (metric 30720) from 10.1.220.4 (10.1.220.4)
```

The BGP next hop for this route is 172.24.244.86, and the IGP metric to reach this next-hop IP address is 30720 (which is the EIGRP metric listed in the routing table to reach 172.24.244.86). The route was received from neighbor 10.1.220.4, and the router ID of that neighbor is also 10.1.220.4.

```
             Origin IGP, metric 0, localpref 100, valid, internal
```

The origin attribute for this route is IGP, the multi-exit discriminator (MED) attribute has a value of 0, and the local preference attribute has a value of 100. The route is a valid route received from an internal BGP peer.

For troubleshooting purposes, the AS path, next hop, and best path indicator are the most important fields in the output of this command. For a full description of all possible fields, see the BGP command references on www.cisco.com.

Instead of viewing a specific entry in the BGP table, it can also be useful to select a set of routes from the BGP table based on certain criteria. The Cisco IOS BGP command toolkit includes the following options to select specific routes from the BGP table:

- **`show ip bgp`** *`network mask`* **`longer-prefixes`** – Lists more specific prefixes present in the BGP table (including the prefix itself) that are contained in the *`network`* and *`mask`* options.
- **`show ip bgp neighbor`** *`ip-address`* **`routes`** – Lists 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`** – Lists 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`* – Selects all routes from the BGP table that have an AS path string that is matched by the specified regular expression.

For more information about how to match specific AS paths using regular expressions, see the "Understanding Regular Expressions" section in the *Cisco IOS Configuration Fundamentals Configuration Guide* at

http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_cli-basics_ps6350_TSD_Products_Configuration_Guide_Chapter.html#wp1002051

Debug BGP Route Exchange

```
R1#debug ip bgp update
BGP updates debugging is on for address family: IPv4 Unicast

R1#clear ip bgp *
R1#
*Nov 16 18:14:11.508: %BGP-5-ADJCHANGE: neighbor 192.168.2.1 Down User reset
R1#
*Nov 16 18:14:13.844: %BGP-5-ADJCHANGE: neighbor 192.168.2.1 Up
R1#
*Nov 16 18:14:13.860: BGP(0): 192.168.2.1 rcvd UPDATE w/ attr: nexthop 192.168.2
.1, origin i, metric 0, merged path 65502, AS_PATH
*Nov 16 18:14:13.860: BGP(0): 192.168.2.1 rcvd 0.0.0.0/0
*Nov 16 18:14:14.832: BGP(0): Revise route installing 1 of 1 routes for 0.0.0.0/
0 -> 192.168.2.1(main) to main IP table
R1#
*Nov 16 18:14:47.264: BGP(0): nettable_walker 172.30.1.0/27 route sourced locall
y
*Nov 16 18:14:47.268: BGP(0): 192.168.2.1 send UPDATE (format) 172.30.1.0/27, ne
xt 192.168.1.1, metric 0
```

If you find expected route entries to be missing from the BGP table, or you doubt whether the router is sending specific routes to a neighbor, consider using the **`debug ip bgp updates`** command to display the processing of BGP updates by the router. However, this command can generate a large number of messages, especially if your BGP table carries many routes. Consequently, it has a high risk of disrupting the router's operation. In production networks, you should take extreme care when using this command, and you should use command options to limit the output to the prefixes and neighbor that you are troubleshooting.

Note: The following section uses sample output not produced from the equipment in this lab to demonstrate how to limit the output of the **`debug ip bgp updates`** command by specifying a neighbor and using an access list to select only certain prefixes.

The commands are interspersed with comments that explain the procedure and output.

```
IRO1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
IRO1(config)#access-list 37 permit 172.17.76.0 0.0.3.255
IRO1(config)#^Z
IRO1#
```

An access list with number 37 is created. When used to filter BGP routes, this access list matches any prefix in the 172.17.76.0–172.17.79.0 IP range.

```
IRO1#debug ip bgp 192.168.224.254 updates 37
BGP updates debugging is on for access list 37 for neighbor
192.168.224.254 for address family: IPv4 Unicast
```

The debug is enabled for neighbor 192.168.224.254 and access list 37. Only update messages transmitted to or received from neighbor 192.168.224.254 that are permitted by access list 37 will be displayed.

```
IRO1#clear ip bgp 192.168.224.254 soft
```

A "soft" clear of BGP neighbor 192.168.224.254 is issued. As opposed to a "hard" clear, a soft clear does not tear down and restart the session completely. It just forces the routes between this router and the neighbor to be retransmitted.

```
IRO1#
Apr 29 06:36:57.549 PDT: BGP(0): 192.168.224.254 send UPDATE (format)
172.17.76.0/22, next 192.168.224.241, metric 0, path Local
```

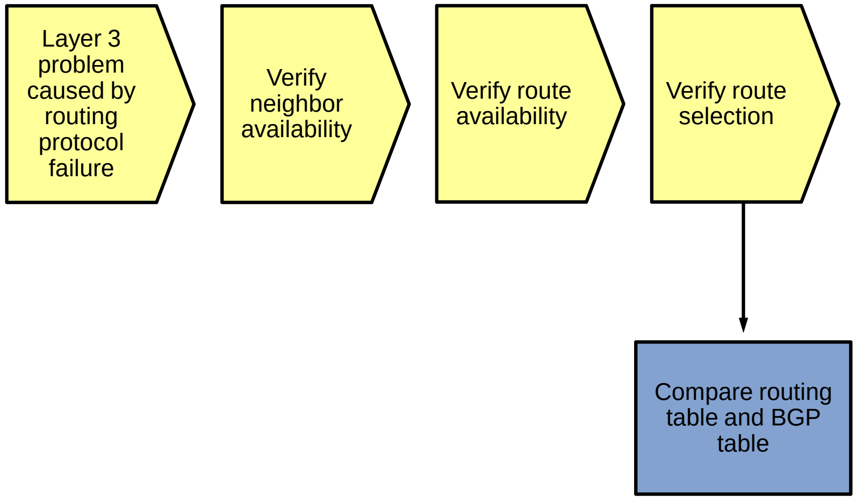
An update about prefix 172.17.76.0/22 is transmitted to neighbor 192.168.224.254. Note that both the neighbor and the prefix match the imposed restrictions.

```
Apr 29 06:36:57.553 PDT: BGP(0): 192.168.224.254 rcv UPDATE w/ attr:
nexthop 192.168.224.254, origin i, originator 0.0.0.0, path 65525 64568,
community , extended community
Apr 29 06:36:57.553 PDT: BGP(0): 192.168.224.254 rcv UPDATE about
172.17.76.0/22 -- DENIED due to: AS-PATH contains our own AS;
```

An update about prefix 172.17.76.0/22 is received but denied, because the AS path attribute contains this router's autonomous system (AS 64568).

Many more updates were sent between this router and its neighbor, but only updates that match the imposed restrictions were displayed, limiting the impact of the command.

Sample BGP Troubleshooting Flow



If you find that a route is available in the BGP table but not in the routing table, there are two possible explanations. Either BGP has not been able to select any of the paths as the best path, or it has selected a best path, but a competing route from a different source with a better administrative distance is present and has been installed in the routing table.

If none of the paths has been selected as the best path, this will be clearly visible in the BGP table, and clues about the cause of the best path selection failure can be gathered from the BGP table. For example, if none of the paths has a next hop that can be resolved in the IP routing table, “Inaccessible” is displayed instead of the IGP metric to reach the next hop. If the BGP synchronization rule is causing a route not to be installed in the routing table, “not synchronized” is displayed behind the route.

If a best path has been selected for the prefix but not installed in the routing table due to the presence of a competing route with a better administrative presence, the route is marked as a “RIB-failure” in the BGP table. To list all BGP routes that have not been installed in the routing table due to a RIB failure, use the **`show ip bgp rib-failure`** command.

Reflection Questions

1. Which lab trouble tickets did you have the most difficulty with?

2. Would you change anything about the process that you used for any of the trouble tickets now that you see the resolution of the problem?

3. Which commands did you find most useful in diagnosing BGP issues? Add these to your toolbox for future use. Which commands did you find least useful?

References

If you need more information on the commands and their options, see the following references:

- IP Routing Protocol Command Reference

  http://www.cisco.com/cisco/web/support/index.html

- Border Gateway Protocol Troubleshooting Tech Notes
  http://www.cisco.com/en/US/tech/tk365/tsd_technology_support_troubleshooting_technotes_list.html#anchor1

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1700	Fast Ethernet 0 (FA0)	Fast Ethernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
1800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2600	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)
2800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. Rather than try to list all the combinations of configurations for each router class, this table includes identifiers for the possible combinations of Ethernet and serial interfaces in the device. The table does not include any other type of interface, even though a specific router might contain one. An example of this is an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

Device Configurations (Instructor version)

Note: All device configurations are provided for TT-A. The configs provided here are *not* running-config outputs. They can be used for copy-and-paste for TT-A and subsequent tickets. Where a config is noted as being the same as a previous one, the only change is in the MOTD, which identifies the Lab and TT. The errors in the configuration are commented and highlighted as red text.

Trouble Ticket—TT-A Configurations

Switch ALS1

```
!Lab 5-3 Switch ALS1 TT-A Config
!
hostname ALS1
!
```



```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 5-3 Switch ALS1 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet

spanning-tree mode rapid-pvst
spanning-tree portfast default
!
interface Vlan1
 no ip address
 shutdown
!
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 100
 name MGMT
!
vlan 900
```



```
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel1
 description Channel to DLS1
 no shutdown
 !
interface Port-channel2
 description Channel to DLS2
 no shutdown
!
interface FastEthernet0/1
 description Channel to DLS1
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shutdown
!
interface FastEthernet0/2
 description Channel to DLS1
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shutdown
!
interface FastEthernet0/3
 description Channel to DLS2
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shutdown
!
interface FastEthernet0/4
 description Channel to DLS2
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shutdown
!
interface FastEthernet0/5
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
```



```
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown

interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
```

```
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description To PC-B
 switchport access vlan 10
 switchport mode access
 switchport voice vlan 20
 spanning-tree portfast
 switchport port-security
 switchport port-security maximum 2
 switchport port-security violation shutdown
 switchport port-security mac-address sticky
 no shut
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
```



```
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan100
 ip address 10.1.100.1 255.255.255.0
 no shutdown
!
ip default-gateway 10.1.100.254
!
ip http server
ip http secure-server
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server host 10.1.50.1 version 2c cisco
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
```

```
snmp-server enable traps port-security
snmp-server enable traps vlan-membership
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
  no transport input
!
ntp source Vlan100
ntp server 192.168.2.1
end
```

Switch DLS1

```
!Lab 5-3 Switch DLS1 TT-A Config
!
hostname DLS1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55

banner motd $*** Lab 5-3 Switch DLS1 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
!
ip domain name tshoot.net
!
ip dhcp excluded-address 10.1.10.252 10.1.10.254
ip dhcp excluded-address 10.1.20.252 10.1.20.254
ip dhcp excluded-address 10.1.30.252 10.1.30.254
!
ip dhcp pool OFFICE
   network 10.1.10.0 255.255.255.0
```



```
   default-router 10.1.10.254
   domain-name tshoot.net
!
ip dhcp pool VOICE
   network 10.1.20.0 255.255.255.0
   default-router 10.1.20.254
   domain-name tshoot.net
!
ip dhcp pool GUEST
   network 10.1.30.0 255.255.255.0
   default-router 10.1.30.254
   domain-name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 24576
spanning-tree vlan 20,50 priority 28672
!
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 100
 name MGMT
!
vlan 200
 name TRANS
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
```



```
!
interface Port-channel1
 description Channel to ALS1
 no shut
!
interface Port-channel10
 description Channel to DLS2
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R1
 no switchport
 ip address 10.1.2.1 255.255.255.252
 spanning-tree bpduguard enable
 speed 100
 duplex full
 no shut
!
```



```
interface FastEthernet0/6
 description FE to SRV1
 switchport access vlan 50
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shut
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
```

```
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
```

```
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown

interface Vlan10
 ip address 10.1.10.252 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 priority 110
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.252 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.252 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 priority 110
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.252 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 preempt
!
```



```
interface Vlan100
 ip address 10.1.100.252 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 priority 110
 standby 100 preempt
!
interface Vlan200
 ip address 10.1.200.252 255.255.255.0
!
router eigrp 1
 passive-interface default
 no passive-interface Fa0/5
 no passive-interface vlan200
 no auto-summary
 network 10.1.0.0 0.0.255.255
!
ip classless
ip http server
ip http secure-server
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server host 10.1.50.1 version 2c cisco
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 192.168.2.1
end
```

Switch DLS2

```
!Lab 5-3 Switch DLS2 TT-A Config
!
```



```
hostname DLS2
!
service timestamps debug datetime msec
service timestamps log datetime
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 5-3 Switch DLS2 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
  path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 28672
spanning-tree vlan 20,50 priority 24576

vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
```



```
 name SERVERS
!
vlan 100
 name MGMT
!
vlan 200
 name TRANS
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel2
 description Channel to ALS1
 no shut

interface Port-channel10
 description Channel to DLS1
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS1
 switchport trunk encapsulation dot1q
```



```
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R3
 no switchport
 ip address 10.1.2.13 255.255.255.252
 speed 100
 duplex full
 spanning-tree bpduguard enable
 no shutdown
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
```



```
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description FE to PC-C
 switchport access vlan 30
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
```



```
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 10.1.10.253 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 preempt
!
interface Vlan20
```



```
 ip address 10.1.20.253 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 priority 110
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.253 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.253 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 priority 110
 standby 50 preempt
!
interface Vlan100
 ip address 10.1.100.253 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 preempt
!
interface Vlan200
 ip address 10.1.200.253 255.255.255.0
!
router eigrp 1
 passive-interface default
 no passive-interface Fa0/5
 no passive-interface vlan200
 no auto-summary
 network 10.1.0.0 0.0.255.255
!
ip classless
ip http server
ip http secure-server
!
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
```



```
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 192.168.2.1
end
```

Router R1

```
!Lab 5-3 Router R1 TT-A Config
!
hostname R1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 5-3 Router R1 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 192.168.1.1 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown
```

```
!
interface FastEthernet0/1
 description FE to DLS1
 ip address 10.1.2.2 255.255.255.252
 ip flow ingress
 ip nat inside
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
 description WAN link to ISP R2
 ip address 209.165.200.225 255.255.255.252
 ip nat outside
 ip flow ingress
 encapsulation ppp
 clock rate 128000
 no shutdown
!
router eigrp 1
 redistribute bgp 65502 metric 1544 2000 255 1 1500
 passive-interface default
 no passive-interface FastEthernet0/1
 network 10.1.2.0 0.0.0.3
 no auto-summary
!
router bgp 65502
 no synchronization
 bgp log-neighbor-changes
 neighbor 192.168.2.2 remote-as 65503
 neighbor 192.168.2.2 ebgp-multihop 2
 neighbor 192.168.2.2 update-source Loopback0
 no auto-summary
!
ip route 192.168.2.1 255.255.255.255 209.165.200.226
!
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
ip nat inside source list 1 interface Serial0/0/0 overload
!
logging source-interface Loopback0
logging 10.1.50.1
!
access-list 1 permit 10.1.0.0 0.0.255.255
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
```

Error: Local AS should be 65501. Remote AS should be 65502 and neighbor IP should be 192.168.2.1.

```
no router bgp 65502
router bgp 65501
 no synchronization
 bgp log-neighbor-changes
 neighbor 192.168.2.1 remote-as 65502
 neighbor 192.168.2.1 ebgp-multihop 2
 neighbor 192.168.2.1 update-source Lo0
```



```
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 192.168.2.1
end
```

Router R2

```
!Lab 5-3 Router R2 TT-A Config
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
Hostname R2
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 5-3 Router R2 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 192.168.2.1 255.255.255.255
!
interface FastEthernet0/0
 shutdown
!
interface FastEthernet0/1
 shutdown
!
interface Serial0/0/0
```

```
 description WAN link to R1 – T1 leased line
 ip address 209.165.200.226 255.255.255.252
 encapsulation ppp
 no shutdown
!
router bgp 65502
 no synchronization
 bgp log-neighbor-changes
 network 0.0.0.0
 neighbor 192.168.1.1 remote-as 65501
 neighbor 192.168.1.1 ebgp-multihop 2
 neighbor 192.168.1.1 update-source Loopback0
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 Null0
ip route 192.168.1.1 255.255.255.255 209.165.200.225
!
ip http server
no ip http secure-server
!
logging source-interface Loopback0
logging 10.1.50.1
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
!
ntp master 3
 end
```

Router R3

```
!Lab 5-3 Router R3 TT-A Config
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
!
logging buffered 16384 debugging
enable secret ciscoenpa55
```



```
!
username admin secret adminpa55
!
banner motd $*** Lab 5-3 Router R3 TT-A Config ***$
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
no ip domain lookup
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 10.1.203.1 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown
!
interface FastEthernet0/1
 description FE to DLS2
 ip address 10.1.2.14 255.255.255.252
 ip flow ingress
 speed 100
 full-duplex
 no shutdown
!
router eigrp 1
 passive-interface default
 no passive-interface FastEthernet0/1
 network 10.1.2.12 0.0.0.3
 network 10.1.203.1 0.0.0.0
 no auto-summary
!
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
logging source-interface Loopback0
```



```
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 192.168.2.1
end
```

Trouble Ticket - TT-B Configurations

Switch ALS1—Same as TT-A

Router R2—Same as TT-A

Router R3—Same as TT-A

Switch DLS1

```
!Lab 5-3 Switch DLS1 TT-B Config
!
hostname DLS1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55

banner motd $*** Lab 5-3 Switch DLS1 TT-B Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
```

```
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
!
ip domain name tshoot.net
!
ip dhcp excluded-address 10.1.10.252 10.1.10.254
ip dhcp excluded-address 10.1.20.252 10.1.20.254
ip dhcp excluded-address 10.1.30.252 10.1.30.254
!
ip dhcp pool OFFICE
   network 10.1.10.0 255.255.255.0
   default-router 10.1.10.254
   domain-name tshoot.net
!
ip dhcp pool VOICE
   network 10.1.20.0 255.255.255.0
   default-router 10.1.20.254
   domain-name tshoot.net
!
ip dhcp pool GUEST
   network 10.1.30.0 255.255.255.0
   default-router 10.1.30.254
   domain-name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 24576
spanning-tree vlan 20,50 priority 28672
!
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
```



```
!
vlan 50
 name SERVERS
!
vlan 100
 name MGMT
!
vlan 130
 name HSVCS
!
vlan 200
 name TRANS
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel1
 description Channel to ALS1
 no shut
!
interface Port-channel10
 description Channel to DLS2
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,130,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
```

```
 no shut
!
interface FastEthernet0/4
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,130,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R1
 no switchport
 ip address 10.1.2.1 255.255.255.252
 spanning-tree bpduguard enable
 speed 100
 duplex full
 no shut
!
interface FastEthernet0/6
 description FE to SRV1
 switchport access vlan 50
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shut
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
```



```
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
```

```
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown

interface Vlan10
```

```
 ip address 10.1.10.252 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 priority 110
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.252 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.252 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 priority 110
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.252 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 preempt
!
interface Vlan100
 ip address 10.1.100.252 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 priority 110
 standby 100 preempt
!
interface Vlan130
 ip address 172.30.1.1 255.255.255.224
!
interface Vlan200
 ip address 10.1.200.252 255.255.255.0
!
router eigrp 1
 passive-interface default
 no passive-interface Fa0/5
 no passive-interface vlan200
 no auto-summary
 network 10.1.0.0 0.0.255.255
!
ip classless
ip http server
ip http secure-server
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server host 10.1.50.1 version 2c cisco
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
```



```
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 192.168.2.1
end
```

Switch DLS2

```
!Lab 5-3 Switch DLS2 TT-B Config
!
hostname DLS2
!
service timestamps debug datetime msec
service timestamps log datetime
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 5-3 Switch DLS2 TT-B Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
```



```
archive
 log config
  logging size 50
  notify syslog
  hidekeys
  path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 28672
spanning-tree vlan 20,50 priority 24576

vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 100
 name MGMT
!
vlan 130
 name HSVCS
!
vlan 200
 name TRANS
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel2
 description Channel to ALS1
 no shut

interface Port-channel10
 description Channel to DLS1
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
```



```
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,130,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,130,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R3
 no switchport
 ip address 10.1.2.13 255.255.255.252
 speed 100
 duplex full
 spanning-tree bpduguard enable
 no shutdown
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
```

```
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
```

```
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description FE to PC-C
 switchport access vlan 30
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
```



```
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 10.1.10.253 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.253 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 priority 110
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.253 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.253 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 priority 110
 standby 50 preempt
!
interface Vlan100
 ip address 10.1.100.253 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 preempt
!
interface Vlan200
 ip address 10.1.200.253 255.255.255.0
!
router eigrp 1
 passive-interface default
 no passive-interface Fa0/5
 no passive-interface vlan200
 no auto-summary
 network 10.1.0.0 0.0.255.255
!
```



```
ip classless
ip http server
ip http secure-server
!
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 192.168.2.1
end
```

Router R1

```
!Lab 5-3 Router R1 TT-B Config
!
hostname R1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 5-3 Router R1 TT-B Config ***$
!
no ip domain lookup
!
```



```
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 192.168.1.1 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown
!
interface FastEthernet0/1
 description FE to DLS1
 ip address 10.1.2.2 255.255.255.252
 ip flow ingress
 ip nat inside
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
 description WAN link to ISP R2 – T1 leased line
 ip address 209.165.200.225 255.255.255.252
 ip nat outside
 ip flow ingress
 encapsulation ppp
 clock rate 128000
  no shutdown
!
router eigrp 1
 redistribute bgp 65501 metric 1544 2000 255 1 1500
 passive-interface default
 no passive-interface FastEthernet0/1
 network 10.1.2.0 0.0.0.3
 no auto-summary
!
router bgp 65501
 no synchronization
 bgp log-neighbor-changes
 network 172.30.1.0
```

Error: Mask is not specified for network 172.30.1.0/27.

network 172.30.1.0 mask 255.255.255.224


```
 neighbor 192.168.2.1 remote-as 65502
 neighbor 192.168.2.1 ebgp-multihop 2
 neighbor 192.168.2.1 update-source Loopback0
 no auto-summary
!
ip route 192.168.2.1 255.255.255.255 209.165.200.226
!
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
ip nat inside source list 1 interface Serial0/0/0 overload
!
logging source-interface Loopback0
logging 10.1.50.1
!
access-list 1 permit 10.1.0.0 0.0.255.255
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 192.168.2.1
end
```

Error: Static route to subnet 172.30.1.0/27 on DLS1 is not specified.

ip route 172.30.1.0 255.255.255.224 10.1.2.1

Trouble Ticket—TT-C Configurations

Switch ALS1—Same as TT-A

Switch DLS1—Same as TT-B

Switch DLS2—Same as TT-B

Router R3—Same as TT-A

Router R1

```
!Lab 5-3 Router R1 TT-C Config
!
hostname R1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 5-3 Router R1 TT-C Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 192.168.1.1 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown
!
interface FastEthernet0/1
```



```
 description FE to DLS1
 ip address 10.1.2.2 255.255.255.252
 ip flow ingress
 ip nat inside
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
 description WAN link to ISP R2
 ip address 209.165.200.225 255.255.255.252
 ip nat outside
 ip flow ingress
 encapsulation ppp
 clock rate 128000
  no shutdown
!
router eigrp 1
 redistribute bgp 65501 metric 1544 2000 255 1 1500
 passive-interface default
 no passive-interface FastEthernet0/1
 network 10.1.2.0 0.0.0.3
 no auto-summary
!
router bgp 65501
 no synchronization
 bgp log-neighbor-changes
 network 172.30.1.0 mask 255.255.255.0
 neighbor 192.168.2.1 remote-as 65502
 neighbor 192.168.2.1 ebgp-multihop 2
 neighbor 192.168.2.1 update-source Loopback0
 no auto-summary
!
ip route 192.168.2.1 255.255.255.255 209.165.200.226
ip route 172.30.1.0 255.255.255.0 10.1.2.1
!
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
ip nat inside source list 1 interface Serial0/0/0 overload
!
logging source-interface Loopback0
logging 10.1.50.1
!
access-list 1 permit 10.1.0.0 0.0.255.255
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
```

Error: Wrong mask (/24) is specified for network 172.30.1.0/27 in network statement.

network 172.30.1.0 mask 255.255.255.224

Error: Wrong mask (/24) is on the static route to subnet 172.30.1.0/27.

ip route 172.30.1.0 255.255.255.224 10.1.2.1


```
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 192.168.2.1
end
```

Router R2

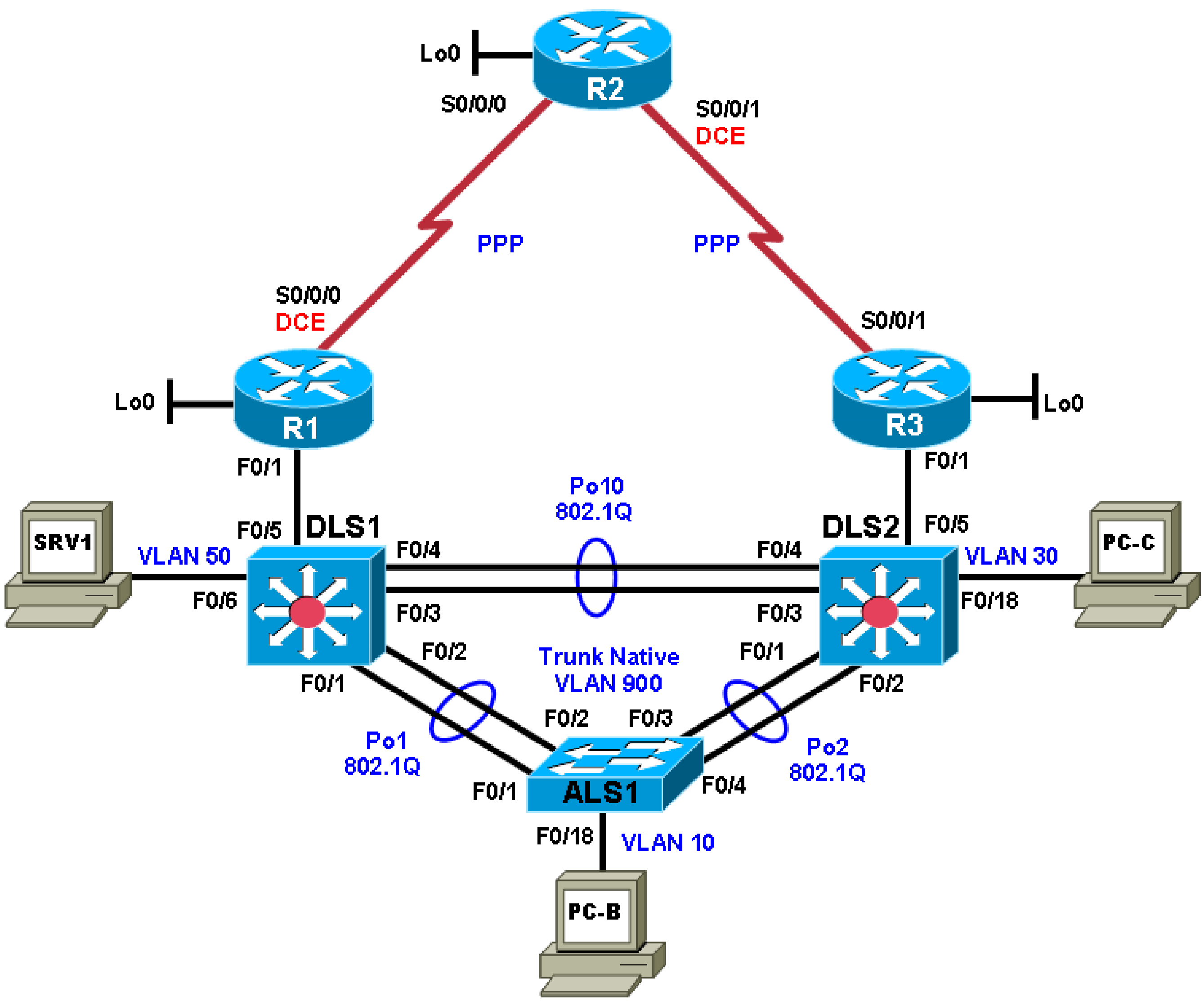
```
!Lab 5-3 Router R2 TT-C Config
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
Hostname R2
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 5-3 Router R2 TT-C Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 192.168.2.1 255.255.255.255
!
interface FastEthernet0/0
 shutdown
!
interface FastEthernet0/1
 shutdown
!
```



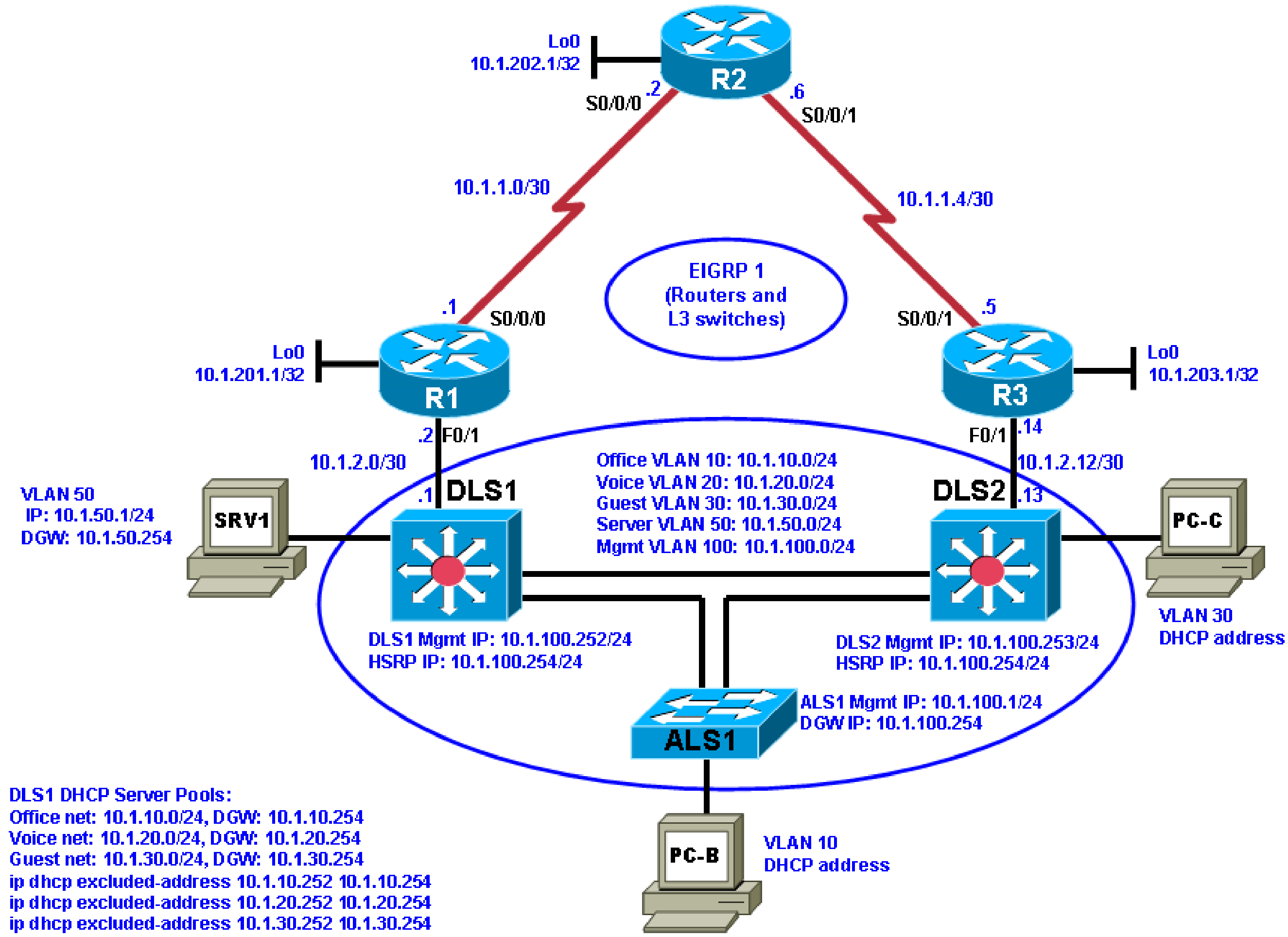
```
interface Serial0/0/0
 description WAN link to R1 – T1 leased line
 ip address 209.165.200.226 255.255.255.252
 encapsulation ppp
 no shutdown
!
interface Serial0/0/1
 shutdown
!
router bgp 65502
 no synchronization
 bgp log-neighbor-changes
 network 0.0.0.0
 neighbor 192.168.1.1 remote-as 65501
 neighbor 192.168.1.1 ebgp-multihop 2
 neighbor 192.168.1.1 update-source Loopback0
 neighbor 192.168.1.1 prefix-list cust-ctrl in
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 Null0
ip route 192.168.1.1 255.255.255.255 209.165.200.225
!
ip http server
no ip http secure-server
!
ip prefix-list cust-ctrl seq 10 permit 172.30.1.0/27
!
logging source-interface Loopback0
logging 10.1.50.1
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
!
ntp master 3
 end
```


Chapter 6 Lab 6-1, IP Addressing—NAT and DHCP Instructor Version

Physical Topology (Baseline)



Logical Topology (Baseline)



Objectives

- Load the device configuration files for each trouble ticket.
- Diagnose and resolve problems related to IP addressing and NAT.
- Diagnose and resolve problems related to IP addressing and DHCP.
- Document the troubleshooting progress, configuration changes, and problem resolution.

Background

Network Address Translation (NAT) is routinely employed in small and large networks. NAT preserves the public IPv4 address space and can provide a measure of security by using private addresses internally. Network layer connectivity issues associated with NAT can include address pool definition, pool depletion, address configuration, interface boundaries, and the type of NAT employed: static, dynamic, or Port Address Translation (PAT).

DHCP is the most common method of assigning IP addressing information to end-user clients. Network layer connectivity issues associated with DHCP include address pool definition, pool depletion, address and default gateway configuration, and server accessibility. In this lab, you will troubleshoot various problems related to NAT and DHCP.

For each task or trouble ticket, the trouble scenario and problem symptom are described. While troubleshooting, you will discover the cause of the problem, correct it, and then document the process and results.

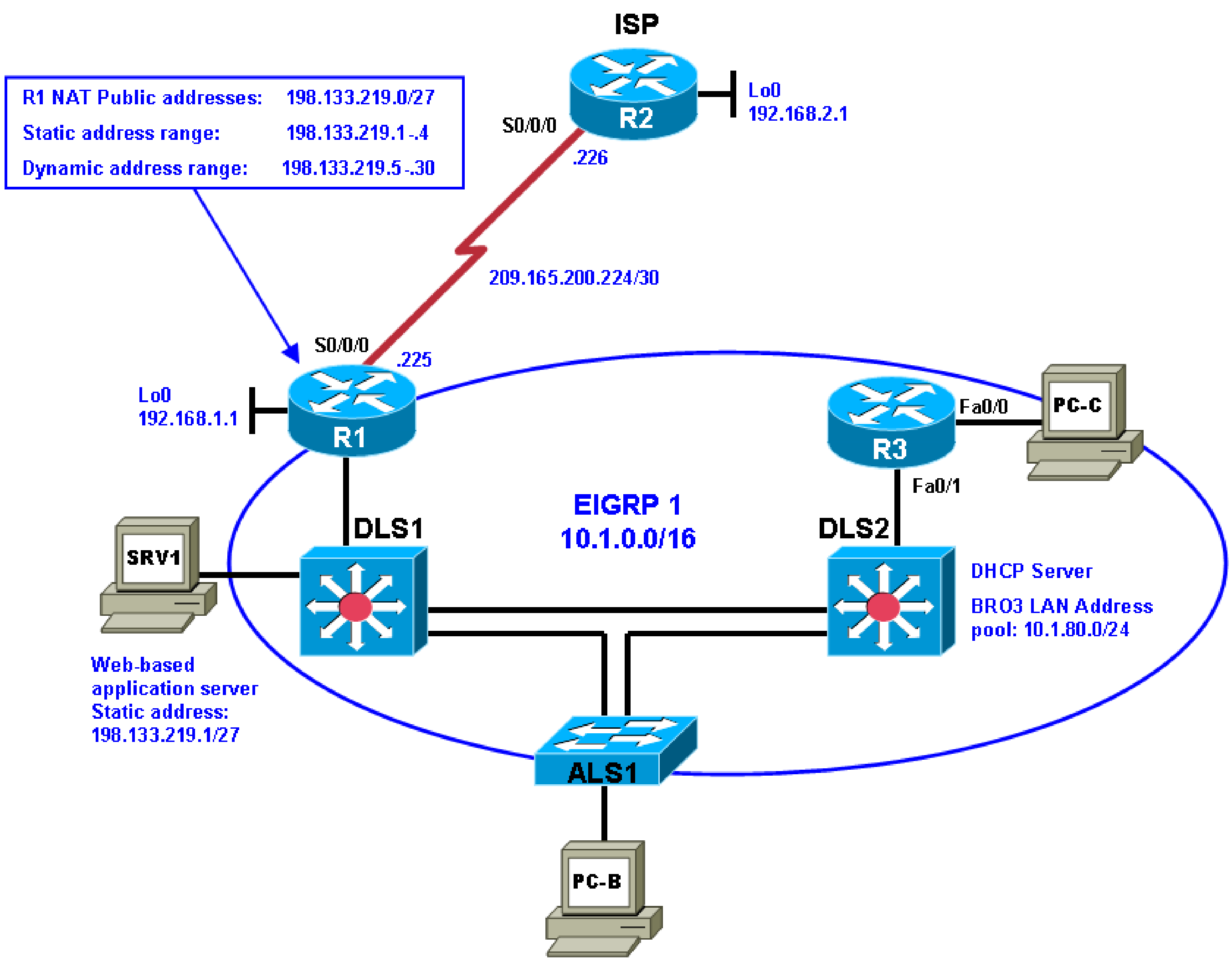
NAT and DHCP Configuration

Your company has decided not to implement a hosted services data center because of cost considerations. Because you will not be advertising a hosted services network, it was decided to discontinue the use of Border Gateway Protocol (BGP) in favor of a simple default static configuration.

Phase 1 (TT-A and TT-B): Dynamic NAT will be used for internal users accessing the Internet. Static NAT will give teleworkers access to some of the key internal servers. Your Internet service provider (ISP) has assigned a block of public addresses using prefix 198.133.219.0/27. These addresses will be used for dynamic NAT with the internal 10.1.0.0/16 network, as well as static NAT to specific servers. Server SRV1 will act as a test server that provides access to an internal web-based application for remote workers. Router R1 will have a default route to the ISP (R2) and will redistribute that route into Enhanced Interior Gateway Routing Protocol (EIGRP). The ISP will use a static route to the NAT public address pool on R1.

Phase 2 (TT-C): A second DHCP server will be added in TT-C to support the branch office router R3 LAN. Switch DLS2 will be configured to provide DHCP addresses to the R3 LAN clients. The following diagram provides information on the NAT (Phase 1) and DHCP (Phase 2) implementation.

Instructor note: Public address blocks 198.133.219.0/24 and 209.165.200.224/27 belong to Cisco Systems, Inc.



Physical and Logical Topology Diagrams

The baseline physical and logical topologies for the existing EIGRP-based network are provided in this lab to assist the troubleshooting effort.

Lab Structure

This lab is divided into two main sections.

Section 1—Trouble Tickets and Troubleshooting Logs

This section includes multiple tasks. Each task is associated with a trouble ticket (TT) and introduces one or more errors on one or more devices. If time is a consideration, each task or trouble ticket can be performed independently.

Section 2—Troubleshooting Reference Information

This section provides general troubleshooting information that can be applied to any of the trouble tickets in this lab. Examples of useful commands and output are provided. If time permits, it is recommended that you read through Section 2 prior to starting on the trouble tickets.

Instructor note: Because the troubleshooting reference section is lengthy, ask students to read through it prior to starting the lab to become familiar with the commands used in this lab. Consider assigning it as homework.

Note: This lab uses Cisco 1841 routers with Cisco IOS Release 12.4(24)T1 and the Advanced IP Services image c1841-advipservicesk9-mz.124-24.T1.bin. The switches are Cisco WS-C2960-24TT-L with the Cisco IOS image c2960-lanbasek9-mz.122-46.SE.bin and Catalyst 3560-24PS with the Cisco IOS image c3560-advipservicesk9-mz.122-46.SE.bin. Other routers (such as 2801 and 2811), switches (such as 2950 or 3550), and Cisco IOS Software versions can be used if they have comparable capabilities and features. Depending on the router or switch model and Cisco IOS Software version, the commands available and output produced might vary from what is shown in this lab.

Any changes made to configurations or topology (other than errors introduced) are noted in the lab and trouble tickets so that you are aware of them prior to beginning the troubleshooting process.

Instructor Notes

- The lab topology should be pre-built prior to the students starting the lab. Ensure that all routers and switches (R1, R2, R3, ALS1, DLS1, and DLS2) have the course lab configuration files installed in flash. You can download the files from the Academy Connection website.
- The device configurations that contain trouble ticket errors and modifications from the baseline are included at the end of the lab, and the errors in them are identified.
- Each device should have a directory named “tshoot” in flash. This directory contains the baseline configuration file for that device as well as the configuration files for the labs in this course. Refer to Lab 3-1 for instructions on creating the tshoot directory in flash.
- Instructors can use a TFTP server, USB drive, flash memory card, or other method to copy all the course configuration files into the flash:/tshoot directory for each device in the topology.
- The student is responsible for loading the baseline or trouble ticket configurations as required using the procedure described in Lab 3-1.
- Set the correct time on router R2, which serves as the primary NTP server for the lab network.
- If time is an issue, each task (trouble ticket) can be performed independently.

Required Resources

- 3 routers (Cisco 1841 with Cisco IOS Release 12.4(24)T1 Advanced IP Service or comparable)
- 1 switch (Cisco 2960 with the Cisco IOS Release 12.2(46)SE C2960-LANBASEK9-M image or comparable)

- 2 switches (Cisco 3560 with the Cisco IOS Release 12.2(46)SE C3560-advipservicesk9-mz image or comparable)
- SRV1 (Windows PC with 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

Instructor Notes

- This lab is divided into multiple tasks. Each task is associated with a trouble ticket (TT) and introduces one or more errors on one or more devices.
- Students can work individually or as a team.
- Suggested actions and results presented during the troubleshooting process for each TT can be shared with the students during debrief or copies of the instructor version of the lab can be made available to the students to assist them in verifying their work.

Section 1—Trouble Tickets and Troubleshooting Logs

Task 1: Trouble Ticket Lab 6-1 TT-A

Instructor note: This trouble ticket involves device R1 and issues related to the static and dynamic NAT configuration between the edge router and ISP.

Step 1: Review trouble ticket Lab 6-1 TT-A.

Your colleague has configured NAT on the edge router (R1), and the external users (simulated by R2 Lo0) can access the test server on the internal private network. However, host PC-B on the internal network cannot access the Internet. Your task is to diagnose the problem and verify that NAT is properly configured. In addition to external users accessing SRV1, internal users must also be able to access the Internet.

Step 2: Load the device trouble ticket configuration files for TT-A.

Using the procedure described in Lab 3-1, verify that the lab configuration files are present in flash. Load the proper configuration files as indicated in the Device Configuration File table.

Note: The following device access methods are in effect after loading the configuration files:

- Console access requires no username or password.
- Telnet and SSH require username **admin** and password **adminpa55**.
- The enable password is **ciscoenpa55**.

Instructor note: Although it is not considered security best practice, the enable secret and admin user passwords can be changed to something simpler to facilitate performance of this lab.

Device Configuration File Table

Device Name	File to Load	Notes
ALS1	Lab61-ALS1-TT-A-Cfg.txt	This file contains configurations different than the baseline
DLS1	Lab61-DLS1-TT-A-Cfg.txt	This file contains configurations different than the baseline
DLS2	Lab61-DLS2-TT-A-Cfg.txt	This file contains configurations different than the baseline
R1	Lab61-R1-TT-A-Cfg.txt	This file contains configuration errors
R2	Lab61-R2-TT-A-Cfg.txt	This file contains configurations different than the baseline
R3	Lab61-R3-TT-A-Cfg.txt	This file contains configurations different than the baseline
SRV1	N/A	Static IP: 10.1.50.1 Default gateway: 10.1.50.254
PC-B	N/A	DHCP
PC-C	N/A	DHCP

Instructor note: The student loads the “broken” TT configuration files for all devices, even though only the configurations indicated in the Notes column contain errors.

Step 3: Configure SRV1 and start the syslog and TFTP servers.

Step 4: Release and renew the DHCP leases.

a. Ensure that PC-B and PC-C are configured as a DHCP clients.

b. After loading all TT-A device configuration files, issue the **`ipconfig /release`** and **`ipconfig /renew`** commands on both PCs.

Note: This trouble ticket assumes that PC-C is in its standard location (connected to Fa0/18 on DLS2).

Step 5: Outline the troubleshooting approach and validation steps.

Use this space to identify your troubleshooting approach and the key steps to verify the problem is resolved. Troubleshooting approaches to select from include the follow-the-path, spot-the-differences, bottom-up, top-down, divide-and-conquer, shoot-from-the-hip, and move-the-problem methods.

Note: In addition to a specific approach, you can use the generic troubleshooting process described at the beginning of Section 2 of this lab.

____

____

____

____

____

____

The divide-and-conquer or follow-the-path method can be used. Other problem-solving methods are the bottom-up, top-down, spot-the-differences, shoot-from-the-hip, and move-the-problem approaches.

Verification steps can include:

- The R1 routing table shows a default route to the ISP and advertises it into EIGRP.
- Dynamic NAT allows office LAN client PC-B to access the Internet via the ISP (simulated by Lo0 on R2).
- Static NAT allows remote users on R2 (simulated by Lo0) to access the SRV1 server on the internal private network.

Step 6: Record the troubleshooting process and configuration changes.

Note: Section 2 of this lab includes useful commands and examples of output.

Use this log to document your actions and results during the troubleshooting process. List the commands you used to gather information. As you progress, record what you think the problem might be and the actions you take to correct the problem.

Device	Actions and Results

Device	Actions and Results

Responses will vary but could include:

- Pings from the external user (R2 Lo0 address 192.168.2.1) to the SRV1 static NAT address 198.133.219.1 succeed.
- Pings from R1 to the Internet (R2 Lo0 address 192.168.2.1) sourced by R1 Fa0/1 (10.1.2.2) fail.
- Pings from PC-B to the Internet (R2 Lo0 address 192.168.2.1) fail. R1 reports that "Destination host is unreachable."
- Pings from PC-B to its default gateway VLAN 10 (10.1.10.254) on DLS1 succeed.

TT-A Issue

The dynamic NAT statement on R1 does not specify that it applies to inside addresses. As a result, no translation of the internal 10.1.0.0/16 addresses takes place.

- The **`show ip route`** command on R1 indicates that the default route to the ISP (R2) is present. The **`show ip route`** command on DLS1 confirms that the default route has been received (D*EX 0.0.0.0/0 to R1 10.1.2.2).
- After test pings from R2 Lo0 to the SRV1 static address, the **`show ip nat translations`** command on R1 indicates an entry for the translation.

```
Pro Inside global     Inside local      Outside local      Outside global
icmp 198.133.219.1:5  10.1.50.1:5       209.165.200.226:5  209.165.200.226:5
```

- After test pings from PC-B (10.1.10.1) to R2 Lo0 (192.168.2.1), the **`show ip nat translations`** command indicates that there are no dynamic translations.
- The **`debug ip nat`** command issued on R1 shows no activity.
- The **`ping 198.133.219.1 source lo0 repeat 100`** command (SRV1 public address) is issued on R2. Return to R1 debug shows static NAT is occurring normally.

```
Nov 18 18:15:03.798: NAT*: s=192.168.2.1, d=198.133.219.1->10.1.50.1 [1183]
Nov 18 18:15:03.802: NAT*: s=10.1.50.1->198.133.219.1, d=192.168.2.1 [3151]
```

- The **`ping 192.168.2.1`** (R2 Lo0) command is issued from internal client PC-B. Debug output on R1 shows no dynamic NAT is occurring.

- The **debug ip icmp** command is issued on R2, and the ping from PC-B to R2 Lo0 shows echo replies being sent to destination 10.1.10.1 (PC-B). This confirms that there is no NAT occurring. R2 does not have a route to the 10.1.0.0/16 network.
- The **show run | include ip nat** command on R1 indicates that the NAT pool is defined, but the **ip nat source** statement does not specify that the addresses to be translated are inside.

Action: Add the **inside** keyword to the configuration. See TT-A debrief for more information.

Verification:

- Pings from an external user (R2 Lo0 address 192.168.2.1) to the SRV1 static NAT address 198.133.219.1 succeed.
- Pings from PC-B to the Internet (R2 Lo0 address 192.168.2.1) succeed.
- The **show ip nat translations** command on R1 indicates that translations are occurring from NTP requests (port 123) to R2 from internal devices such as DLS1 and others. These are being translated dynamically.

```
Pro Inside global      Inside local       Outside local      Outside global
udp 198.133.219.4:123  10.1.100.252:123   192.168.2.1:123    192.168.2.1:123
```

Step 7: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with your instructor. The notes can include problems encountered, solutions applied, useful commands employed, alternate solutions, methods, and processes, and procedure and communication improvements.

____

____

____

____

____

____

____

Trouble Ticket TT-A debrief—Instructor Notes

The problem in this trouble ticket is that the dynamic NAT statement on R1—**ip nat inside source list 1 pool public-addrs**—did not include the keyword **inside**. The **ip nat source** command is actually used in an alternate way of configuring NAT without specifying inside and outside domains. However, it is not used appropriately in this case, and as a result, no dynamic translation of the inside private addresses (10.1.0.0/16) to the public pool of addresses (198.133.219.0/27) takes place. Search for the document 'NAT Virtual Interface' on Cisco website for further information regarding the **ip nat source** command.

When this command is entered, it is accepted without the **inside** keyword. Omitting the **inside** keyword for dynamic NAT translation does not affect static NAT translation. This is why the external user (R2 Lo0) can still access the internal server SRV1 on VLAN 50. The internal address of SRV1 is 10.1.50.1, and the public static address is 198.133.219.1.

To correct the problem, use the following commands on router R1:

```
no ip nat source list 1 pool public-addrs
ip nat inside source list 1 pool public-addrs
```


Task 2: Trouble Ticket Lab 6-1 TT-B

Instructor note: This trouble ticket involves device R1 and issues related to the dynamic NAT pool and number of addresses available.

Step 1: Review trouble ticket Lab 6-1 TT-B.

The NAT configuration has been corrected, and dynamic NAT is now functioning between internal hosts and the ISP. However, some users have called the help desk stating that Internet access is inconsistent. Sometimes it works, and other times it does not. Your task is to diagnose the problem and correct it. At a minimum, propose a possible solution to the problem so that internal users can consistently access the Internet.

Step 2: Load the device trouble ticket configuration files for TT-B.

Using the procedure described in Lab 3-1, verify that the lab configuration files are present in flash. Load the proper configuration files as indicated in the Device Configuration File table.

Note: See Task 1, Step 2 for device access methods, usernames, and passwords after the configuration files have been loaded.

Device Configuration File Table

Device Name	File to Load	Notes
ALS1	Lab61-ALS1-TT-B-Cfg.txt	This file contains configurations different than the baseline
DLS1	Lab61-DLS1-TT-B-Cfg.txt	This file contains configurations different than the baseline
DLS2	Lab61-DLS2-TT-B-Cfg.txt	This file contains configurations different than the baseline
R1	Lab61-R1-TT-B-Cfg.txt	This file contains configuration errors.
R2	Lab61-R2-TT-B-Cfg.txt	This file contains configurations different than the baseline
R3	Lab61-R3-TT-B-Cfg.txt	This file contains configurations different than the baseline
SRV1	N/A	Static IP: 10.1.50.1 Default gateway: 10.1.50.254
PC-B	N/A	DHCP
PC-C	N/A	DHCP

Instructor note: The student loads the “broken” TT configuration files for all devices, even though only the configurations indicated in the Notes column contain errors.

Step 3: Configure SRV1 and start the syslog and TFTP servers.

Step 4: Release and renew the DHCP leases.

a. Ensure that PC-B and PC-C are configured as a DHCP clients.

b. After loading all TT-A device configuration files, issue the **`ipconfig /release`** and **`ipconfig /renew`** commands on both PCs.

Note: This trouble ticket assumes that PC-C is in its standard location (connected to Fa0/18 on DLS2).

Step 5: Outline the troubleshooting approach and validation steps.

Use this space to identify your troubleshooting approach and the key steps to verify that the problem is resolved. Troubleshooting approaches to select from include the follow-the-path, spot-the-differences, bottom-up, top-down, divide-and-conquer, shoot-from-the-hip, and move-the-problem methods.

Note: In addition to a specific approach, you can use the generic troubleshooting process described at the beginning of Section 2 of this lab.

____

____

____

____

____

____

The divide-and-conquer or follow-the-path method can be used. Other problem-solving methods are the bottom-up, top-down, spot-the-differences, shoot-from-the-hip, and move-the-problem approaches.

Verification steps can include:

- Dynamic NAT allows office LAN client PC-B consistent access to the Internet via the ISP (simulated by Lo0 on R2).
- Static NAT allows remote users on R2 (simulated by Lo0) to access the SRV1 server on the internal private network.

Step 6: Record the troubleshooting process and configuration changes.

Note: Section 2 of this lab includes sample troubleshooting flows, useful commands, and examples of output.

Use this log to document your actions and results during the troubleshooting process. List the commands you used to gather information. As you progress, record what you think the problem might be and the actions you take to correct the problem.

Device	Actions and Results

Device	Actions and Results

Responses will vary but could include:

- Pings from an external user (R2 Lo0 address 192.168.2.1) to the SRV1 static NAT address 198.133.219.1 succeed.
- Pings from R1 to the Internet (R2 Lo0 address 192.168.2.1) sourced by R1 Fa0/1 (10.1.2.2) fail occasionally.
- Pings from PC-B to the Internet (R2 Lo0 address 192.168.2.1) fail occasionally.
- Pings from PC-B to its default gateway VLAN 10 (10.1.10.254) on DLS1 succeed.

TT-B Issue

The dynamic NAT pool defined is very small and when all public addresses are taken, the next host that tries to access the Internet fails.

- After test ping and Telnet attempts from PC-B to R2 Lo0 fail, the **show ip nat translations** command on R1 indicates no entries for the translations. However, there are a number of other entries from internal network devices accessing the R2 NTP server (port 123).

```
Pro Inside global      Inside local       Outside local      Outside global
udp 198.133.219.6:123  10.1.2.14:123      192.168.2.1:123    192.168.2.1:123
--- 198.133.219.1      10.1.50.1          ---                ---
udp 198.133.219.5:123  10.1.100.1:123     192.168.2.1:123    192.168.2.1:123
udp 198.133.219.4:123  10.1.100.252:123   192.168.2.1:123    192.168.2.1:123
--- 198.133.219.3:123  10.1.100.253:123   192.168.2.1:123    192.168.2.1:123
```

- After test pings and Telnet attempts from PC-B to R2 Lo0 fail, the **debug ip nat** command on R1 indicates that translation was attempted but failed.

```
NAT: translation failed (A), dropping packet s=10.1.10.1 d=192.168.2.1
```

- The **ping 198.133.219.1 source lo0 repeat 100** command is issued on R2. Returning to R1 debug shows static NAT is occurring normally.

```
Nov 18 18:15:03.798: NAT*: s=192.168.2.1, d=198.133.219.1->10.1.50.1 [1183]
Nov 18 18:15:03.802: NAT*: s=10.1.50.1->198.133.219.1, d=192.168.2.1 [3151]
```

- Ping **192.168.2.1** (R2 Lo0) from PC-B. Debug shows no dynamic NAT is occurring.
- The **debug ip icmp** command entered on R1 and the ping from PC-B to R2 Lo0 shows host unreachable messages sent back to 10.1.10.1 (PC-B) from R1. No NAT is occurring.
- After test pings and Telnet attempts from PC-B to R2 Lo0 fail, the **show ip nat statistics** command on R1 indicates that the total number of addresses available in the address pool **public-addrs** is only four. Four addresses have been allocated, which is 100% of the addresses available. There are no more addresses to allocate. The pool shows multiple misses because clients are unable to obtain a public address for translation.

```
pool public-addrs: netmask 255.255.255.248
        start 198.133.219.3 end 198.133.219.6
```



```
        type generic, total addresses 4, allocated 4 (100%), misses 8
```

- The **`clear ip nat translation *`** command removes all dynamic translations and leaves the static translation to SRV1.
- A ping is issued from PC-B to the Internet (R2 Lo0 address 192.168.2.1). If the previous pings from PC-B to the Internet failed, this one now succeeds.

Note: After clearing the dynamic translations, if a ping from PC-B is done quickly before the network devices use up the addresses in the pool with NTP requests, a translation will be created for PC-B and will remain in effect until it is aged out. While the translation is active, PC-B can continue to ping the Internet.

- The **`show run | include ip nat (`**or **`show ip nat statistics`**) command on R1 indicates that the total number of NAT addresses is only six (mask is 255.255.255.248 or /29 = 8 addresses minus 2 = 6). The NAT pool **public-addrs** is assigned the starting address 198.133.219.3 and ending address 198.133.219.6 for a total of only four potential dynamic addresses. Addresses 198.133.219.1 and 198.133.219.2 have been reserved for static assignment to servers.

Action:

Option 1: If the NAT address pool was defined incorrectly, change the address range and mask to include the correct (larger) number of addresses.

Option 2: If the NAT address pool was defined correctly and is too small, obtain a larger address pool from the ISP.

Option 3: Use the NAT overload feature, which maps IP addresses and port numbers, allowing a small pool of addresses to be used for translation of many more devices. See TT-B debrief for more information.

Verification:

- If a larger pool is defined or overload is used, pings from PC-B to the Internet (R2 Lo0 address 192.168.2.1) succeed.
- The **`show ip nat translations`** command indicates that translations from PC-B (or other devices) resulting from ping, Telnet, or HTTP, are occurring as required.

Step 7: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with your instructor. The notes can include problems encountered, solutions applied, useful commands employed, alternate solutions, methods, and processes, and procedure and communication improvements.

____

____

____

____

____

____

____

Trouble Ticket TT-B Debrief—Instructor Notes

The problem in this trouble ticket is that the pool of public addresses available for dynamic translation is very small. It is being consumed by network devices (DLS1, DLS2, R3, and so on) making Network Time Protocol (NTP) requests of R2 (simulated ISP acting as the NTP server). When all public addresses are taken, the next host that tries to ping, telnet, or browse the Internet fails. NAT debugging indicates that translation is attempted but fails, and the packets are dropped.

Displaying NAT statistics shows that the total number of addresses available in the address pool **public-addrs** is only four. When all four addresses have been allocated (100% of available), there are no more addresses to allocate. Subsequent attempts to obtain a public address for translation result in multiple misses being reported. If the dynamic translations are cleared, PC-B and other internal hosts can obtain an address to access the Internet on a first come, first served basis, until the pool is depleted again.

A translation that is created remains in place until it is aged out. While the translation is active, the host or network device is able to continue to access the Internet. Because network devices, such as switch DLS1, continually request time updates from NTP server R2, the translation stays active and does not age out.

Note: Point out that the dynamic address depletion issue does not affect static translation for SRV1 because a statically mapped public address is reserved for this server.

There are several possible solutions to the problem.

Option 1: The network administrator defined the NAT address pool incorrectly. If that is the case, you can change the address range and mask to match the correct number of addresses assigned by the ISP.

Option 2: If the NAT address pool was defined correctly but is too small for the needs of the company, a larger address pool can be obtained from the ISP (at some cost).

For options 1 and 2, you can correct the problem by issuing the following commands on router R1:

```
R1(config)#no ip nat inside source list 1 pool public-addrs

Dynamic mapping in use, do you want to delete all entries? [no]: yes

R1(config)#no ip nat pool public-addrs 198.133.219.3 198.133.219.6 netmask
255.255.255.248
R1(config)#ip nat pool public-addrs 198.133.219.5 198.133.219.30 netmask
255.255.255.224

R1(config)#ip nat inside source list 1 pool public-addrs
```

Note: These commands create a pool of 26 usable addresses and reserve the first four addresses for static assignment to servers.

Option 3 (chosen): Use the NAT overload feature, which maps address and port number combinations and allows a small pool of addresses to be used for translation of many more internal addresses. This solution does not require purchasing additional addresses from the ISP.

For option 3, you can correct the problem by issuing the following commands on router R1:

```
R1(config)#no ip nat inside source list 1 pool public-addrs

Dynamic mapping in use, do you want to delete all entries? [no]: yes

R1(config)#ip nat inside source list 1 pool public-addrs overload
```

Note: Point out that changing NAT pools and other settings should be performed during a regular maintenance window, if possible, to minimize disruption of service and impact on users.

Task 3: Trouble Ticket Lab 6-1 TT-C

Instructor note: This trouble ticket involves DLS2 and R3 issues related to the DHCP server address pool definition, DHCP relay, and duplicate addressing.

Step 1: Review trouble ticket Lab 6-1 TT-C.

The company is expanding and opening a new branch office LAN that will be connected to router R3. It has been decided that switch DLS2 will provide DHCP services to this remote office. The branch office is represented by test host PC-C, which will be configured as a DHCP client. Your colleague says he has configured DHCP on DLS2 with a corresponding subnet and DHCP pool. However, test client PC-C has not been able to access server SRV1. The first address in the pool should be excluded because it is reserved for the R3 default gateway Fa0/0.

Your task is to verify VLAN configuration and DHCP services and that PC-C can access internal server SRV1.

Step 2: Load the device trouble ticket configuration files for TT-C.

Using the procedure described in Lab 3-1, verify that the lab configuration files are present in flash. Load the proper configuration files as indicated in the Device Configuration File table.

Note: See Task 1, Step 2 for device access methods, usernames, and passwords after the configuration files have been loaded.

Device Configuration File Table

Device Name	File to Load	Notes
ALS1	Lab61-ALS1-TT-C-Cfg.txt	This file contains configurations different than the baseline
DLS1	Lab61-DLS1-TT-C-Cfg.txt	This file contains configurations different than the baseline
DLS2	Lab61-DLS2-TT-C-Cfg.txt	This file contains configuration errors
R1	Lab61-R1-TT-C-Cfg.txt	This file contains configurations different than the baseline
R2	Lab61-R2-TT-C-Cfg.txt	This file contains configurations different than the baseline
R3	Lab61-R3-TT-C-Cfg.txt	This file contains configuration errors
SRV1	N/A	Static IP: 10.1.50.1 Default gateway: 10.1.50.254
PC-B	N/A	DHCP (release and renew after loading the device configurations)
PC-C	N/A	DHCP (release and renew after loading the device configurations)

Step 3: Configure SRV1 and start the syslog and TFTP servers.

Step 4: Release and renew the DHCP lease on PC-C.

a. Ensure that PC-C is configured as a DHCP client.

b. Connect PC-C to R3.

c. After loading all TT-C device configuration files, issue the **`ipconfig /release`** and **`ipconfig /renew`** commands on PC-C.

Step 5: Outline the troubleshooting approach and validation steps.

Use this space to identify your troubleshooting approach and the key steps to take to verify that the problem is resolved. Troubleshooting approaches to select from include the follow-the-path, spot-the-differences, bottom-up, top-down, divide-and-conquer, shoot-from-the-hip, and move-the-problem methods.

Note: In addition to a specific approach, you can use the generic troubleshooting process described at the beginning of Section 2 of this lab.

The follow-the-path or the divide-and-conquer method can be used. Other problem-solving methods are the bottom-up, top-down, spot-the-differences method, shoot-from-the-hip, and move-the-problem approaches.

Verification steps can include:

- PC-C receives an IP address from the DLS2 DHCP server on the 10.1.80.1/24 network.
- Pings from external PC-C to SRV1 (10.1.50.1) succeed.

Step 6: Record the troubleshooting process and configuration changes.

Note: Section 2 of this lab includes sample troubleshooting flows, useful commands, and examples of output.

Use this log to document your actions and results during the troubleshooting process. List the commands that you used to gather information. As you progress, record what you think the problem might be and the actions you take to correct the problem.

Device	Actions and Results

Responses will vary but could include:

- Pings from external PC-C to SRV1 (10.1.50.1) fail.
- Pings from PC-C to its default gateway (R3 Fa0/0 10.1.80.1) fail.
- Pings from R3 to DLS2 Fa0/5 (10.1.2.13) succeed.

TT-C Issue 1

By default, router R3 does not forward DHCP (broadcast) requests from PC-C, and a helper address is not configured on R3. As a result, PC-C cannot obtain its IP configuration from DHCP server DLS2.

- The **`show ip interface brief`** command on R3 indicates that interface Fa0/0 is UP/UP and is configured with the correct IP address (10.1.80.1).
- The **`show ip route`** command on R3 indicates that network 10.1.80.0/24 is directly connected.
- The **`show ip protocols`** command on R3 indicates that network 10.1.80.0/24 is advertised under EIGRP, as it should be. Interface Fa0/0 is listed as a passive interface, but this is not a problem because there is no need to advertise this network to the branch office LAN.
- Pings from R3 to DLS2 Fa0/5 (10.1.2.13) succeed.
- A check of PC-C confirms that it is configured as a DHCP client, but it has a Windows “Autoconfigure” address in the 169.254.0.0/16 range and has not received an IP address from a DHCP server.
- Issuing the **`ipconfig /release`** and **`ipconfig /renew`** commands at the PC-C command prompt does not result in PC-C obtaining an IP address.
- The **`show ip dhcp bindings`** command on DLS2 indicates that no IP addresses are associated with a client hardware (MAC) address.
- The **`show ip dhcp server statistics`** command on DLS2 indicates that no DHCPDISCOVER or DHCPREQUEST messages have been received, and no DHCPOFFER messages have been sent.
- The **`debug ip udp`** command on R3 indicates that UDP packets from the PC-C DHCP client (source address 0.0.0.0 port 68) are being broadcast, looking for a DHCP server (destination address 255.255.255.255 port 67). These are being received by R3, but they are not being forwarded to the DHCP server. There are no return packets from DLS2.

```
*Nov 20 15:53:29.606: UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67)
```

- Routers do not forward DHCP broadcasts by default. The **`show ip interface Fa0/0`** command on R3 indicates that no helper address is configured to assist PC-C by directing broadcasts to DLS2.

Action: Configure a helper address on the R3 interface Fa0/0 that directs broadcasts to the DHCP server DLS2 interface Fa0/5 (10.1.2.13). See the TT-C debrief for more information.

Verification:

- Issuing the **`ipconfig /release`** and **`ipconfig /renew`** commands at the PC-C command prompt does not result in PC-C obtaining an IP address. There must be another problem.
- Pings from external PC-C to SRV1 (10.1.50.1) fail. There must be another problem.

TT-C Issue 2

DHCP server DLS2 is configured to assign IP addresses in the 10.80.1.0/24 network instead of the 10.1.80.0/24 network. This results in PC-C not obtaining an IP address from the DHCP server.

- Pings from R3 to DLS2 Fa0/5 (10.1.2.13) succeed.
- A check of PC-C confirms that it is configured as a DHCP client, but it has an Autoconfigure address in the 169.254.0.0/16 range and has not received an IP address from a DHCP server.
- Issuing the **`ipconfig /release`** and **`ipconfig /renew`** commands at the PC-C command prompt does not result in PC-C obtaining an IP address.
- The **`show ip dhcp pool`** command on DLS2 indicates that pool BRO3 is defined with 254 total addresses, no leased addresses, and 3 excluded addresses.
- The **`debug ip dhcp server events`** command on DLS2 indicates that it is receiving DHCPDISCOVER messages and is sending notification of these messages to the R3 gateway IP

address 10.1.80.1 (giaddr). The debug on DLS2 also reports that no address pool corresponds to the R2 Fa0/0 IP address.

- The **show run | beg dhcp pool** command on DLS2 indicates that pool BRO3 is defined to assign addresses from the 10.80.1.0/24 range, but the default router address configured is the R3 Fa0/0 address of 10.1.80.1. The address range for the pool is incorrect. Even if DLS2 were able to assign PC-C an IP address from this pool, PC-C would not be able to communicate with its default gateway because they are on different networks.

Action: Change the network statement command on DLS2 to reference the correct range of 10.1.80.0/24. See TT-C debrief for more information.

Verification:

- PC-C receives an IP address from the DLS2 DHCP server on the 10.1.80.0/24 network.
- Pings from external PC-C to SRV1 (10.1.50.1) succeed.

TT-C Issue 3

DHCP server DLS2 is configured with an excluded address range of 10.1.80.252 to 10.1.80.254. The trouble ticket states that the default gateway on a subnet should be excluded (in this case, 10.1.80.1).

Note: This does not prevent PC-C from obtaining an IP address, but the address that it receives will be the next one in the range (10.1.80.2). The lack of exclusion for the R3 Fa0/0 IP address results in a duplicate address error being reported on DLS2.

```
*Nov 20 18:09:49.254: %IP-4-DUPADDR: Duplicate address 10.1.80.1 on
FastEthernet0/0, sourced
Nov 20 18:09:59: %DHCPD-4-DECLINE_CONFLICT: DHCP address conflict:  client
0100.0bdb.04a5.cd declined 10.1.80.1.
```

- The **show ip dhcp conflict** command on DLS2 indicates that the first IP address in the pool, 10.1.80.1, was already in use and was detected by ARP.

```
o  IP address        Detection method   Detection time          VRF
o  10.1.80.1         Gratuitous ARP     Nov 20 2009 06:09 PM
```

- Issuing the **ipconfig /release** and **ipconfig /renew** commands at the PC-C command prompt results in PC-C obtaining IP address 10.1.80.2 because 10.1.80.1 was in use.
- After correcting the BRO3 pool address range problem, pings from PC-C to DLS2 Fa0/5 (10.1.2.13) succeed.
- The **show run | beg dhcp pool** command on DLS2 indicates that the wrong addresses were excluded from the pool of assignable addresses.

Action: Change the DHCP excluded address statement on DLS2 to reference the IP address of R3 Fa0/0 (10.1.80.1). See TT-C debrief for more information.

Verification: PC-C receives IP address 10.1.80.2 from the DLS2 DHCP server.

Step 7: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with your instructor. The notes include problems encountered, solutions applied, useful commands employed, alternate solutions and methods, and procedure and communication improvements.

____

____

____

____

____

____

Trouble Ticket TT-C Debrief—Instructor Notes

This trouble ticket has three issues. The first two issues prevent the client from obtaining an IP address from the DHCP server. The third issue has to do with excluding the proper addresses from the DHCP pool.

TT-C Issue 1

DHCP discovery messages from the DHCP client are broadcasts. By default, routers do not forward DHCP broadcasts. As a result, PC-C in the branch office LAN connected to R3 cannot reach the DHCP server DLS2 at headquarters to obtain an IP address. Configuring a helper address on R3 assists PC-C by directing broadcasts to DLS2. Use the following commands to configure the helper address on R3 that points to the DLS2 Fa0/5 interface IP address.

```
interface FastEthernet0/0
 ip helper-address 10.1.2.13
```

This configuration allows DHCP discovery messages from PC-C to reach DLS2. However, PC-C still does not receive its IP address.

TT-C Issue 2

A second problem is the configuration of the DHCP pool on DLS2. DHCP server DLS2 is misconfigured to assign IP addresses in the 10.80.1.0/24 network instead of the 10.1.80.0/24 network. This results in PC-C not obtaining an IP address. DLS2 receives the PC-C DHCPDISCOVER messages relayed by R3 but compares the gateway IP address of R3 (10.1.80.1) to the misconfigured address range defined in the pool (10.80.1.0/24). They do not match, so DLS1 sends a message to R3 stating that no address pool corresponds to the R3 Fa0/0 IP address. As a result, the DHCP message exchange process with PC-C terminates, and no address is offered to PC-C.

Point out that even if DLS2 were able to assign PC-C an IP address from this pool, PC-C would not be able to communicate with its default gateway on R3 because they are on different networks.

To correct this problem, use the following command on DLS2 to remove the incorrect network pool definition and replace it with the correct one.

```
ip dhcp pool BRO3
 no network 10.80.1.0 255.255.255.0
 network 10.1.80.0 255.255.255.0

*Nov 20 18:09:49.254: %IP-4-DUPADDR: Duplicate address 10.1.80.1 on
FastEthernet0/0, sourced
Nov 20 18:09:59: %DHCPD-4-DECLINE_CONFLICT: DHCP address conflict:  client
0100.0bdb.04a5.cd declined 10.1.80.1.
```

Note the address conflict error on DLS2 when DLS2 tries to assign IP address 10.1.80.1 (R3 Fa0/0) to PC-C. This problem is addressed in the TT-C Issue 3 section.

What would happen if the IP address of R3 Fa0/0 were changed to 10.80.1.1/24? PC-C would be able to obtain an IP address but still would not be able to communicate with SRV1, because R3 does not advertise this network under EIGRP.

TT-C Issue 3

The third issue is related to the DHCP addresses excluded on DLS2. Address range 10.1.80.252 to 10.1.80.254 is being excluded, but this allows DLS2 to try to assign 10.1.80.1 the first address in the range, which belongs to R3 Fa0/0 and should be excluded. The trouble ticket states that the default gateway on a subnet should be excluded (in this case, 10.1.80.1).

The improper exclusion does not prevent PC-C from obtaining an IP address. When the problem in Issue 2 is resolved, the DHCP server selects the 10.1.80.1 address for potential assignment to PC-C, but before sending the DHCPOFFER, it first sends a series of pings to try to verify that the address is not already in use by some other device. In this case, it is used on R3's Fa0/0 interface, so the DHCP server realizes there is a conflict. The DHCP server then selects a different address for potential assignment to PC-C, runs the same ping tests, does not detect a conflict, and sends the DHCPOFFER to PC-C, with the offer containing this second address.

The address PC-C receives will be the next one in the range (10.1.80.2), but 10.1.80.1 will remain in a conflicted state.

```
*Nov 20 18:09:49.254: %IP-4-DUPADDR: Duplicate address 10.1.80.1 on
FastEthernet0/0, sourced
Nov 20 18:09:59: %DHCPD-4-DECLINE_CONFLICT: DHCP address conflict:  client
0100.0bdb.04a5.cd declined 10.1.80.1.
```

To correct this problem, issue the following commands on DLS2:

```
no ip dhcp excluded-address 10.1.80.252 10.1.80.254
ip dhcp excluded-address 10.1.80.1
```

Note: If servers, printers, or other devices are to be assigned static addresses on this subnet, a range can be specified to exclude these addresses.

To remove the conflicted addresses, issue this command:

```
clear ip dhcp conflict *
```

Section 2 Troubleshooting Reference Information

NAT command examples include verification of NAT boundaries, the type of NAT configured, NAT statistics, NAT translations, and debugging NAT translations.

DHCP examples include verification of the DHCP server configuration, address pools, DHCP server statistics, client configuration, and debugging DHCP activity.

General Troubleshooting Process

As a general guideline, you can use the following general troubleshooting process described in the course.

1. Define the problem (symptoms).
2. Gather information.
3. Analyze the information.
4. Propose a hypothesis (possible cause).
5. Test the hypothesis.
6. Eliminate or accept the hypothesis.
7. Solve the problem.
8. Document the problem.

Command Summary

The table lists useful commands for this lab. The sample output is shown on following pages.

Command	Key Information Displayed
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.
debug dhcp detail	Displays real-time information on a Cisco IOS DHCP client (router or switch).
debug ip dhcp server events	Displays real-time information for DHCP server process messages.
clear ip dhcp server statistics	Clears DHCP server statistics.
clear ip dhcp conflict *	Clears conflicted addresses.
show ip sockets	Displays the current connections for this server, including which services are running.

Sample Troubleshooting Output

NAT-related Commands

The following commands and output are samples from the devices in this lab.

```
R1#show ip nat translations
Pro Inside global       Inside local       Outside local      Outside global
icmp 198.133.219.7:512  10.1.10.1:512      192.168.2.1:512    192.168.2.1:512
---  198.133.219.7      10.1.10.1          ---                ---
---  198.133.219.1      10.1.50.1          ---                ---
udp  198.133.219.6:123  10.1.100.1:123     192.168.2.1:123    192.168.2.1:123
tcp  198.133.219.6:38711 10.1.100.1:38711  192.168.2.1:23     192.168.2.1:23
---  198.133.219.6      10.1.100.1         ---                ---
udp  198.133.219.4:123  10.1.100.252:123   192.168.2.1:123    192.168.2.1:123
---  198.133.219.4      10.1.100.252       ---                ---
tcp  198.133.219.3:1121 10.1.10.1:1121     192.168.2.1:80     192.168.2.1:80
---  198.133.219.3      10.1.10.1          ---                ---
udp  198.133.219.5:123  10.1.100.253:123   192.168.2.1:123    192.168.2.1:123
---  198.133.219.5      10.1.100.253       ---                ---
```

In the above example, the connections resulted from pings (ICMP port 512), NTP (UDP port 123), Telnet (TCP port 23), and HTTP (TCP port 80).

```
R1#show ip nat statistics
Total active translations: 7 (1 static, 6 dynamic; 2 extended)
Peak translations: 9, occurred 00:45:03 ago
Outside interfaces:
  Serial0/0/0
Inside interfaces:
  FastEthernet0/1
Hits: 2442  Misses: 0
CEF Translated packets: 2439, CEF Punted packets: 11
Expired translations: 15
Dynamic mappings:
-- Inside Source
[Id: 8] access-list 1 pool public-addrs refcount 6
 pool public-addrs: netmask 255.255.255.248
        start 198.133.219.3 end 198.133.219.6
        type generic, total addresses 4, allocated 4 (100%), misses 8
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```


The above output shows NAT pool configuration information, boundaries (inside and outside interfaces), translation pool size, and usage statistics.

```
R1#debug ip nat
IP NAT debugging is on
R1#terminal monitor
R1#
Nov 18 16:52:09.304: NAT*: s=10.1.10.1->198.133.219.6, d=192.168.2.1 [108]
Nov 18 16:52:09.316: NAT*: s=192.168.2.1, d=198.133.219.6->10.1.10.1 [108]
Nov 18 16:52:10.300: NAT*: s=10.1.10.1->198.133.219.6, d=192.168.2.1 [109]
Nov 18 16:52:10.308: NAT*: s=192.168.2.1, d=198.133.219.6->10.1.10.1 [109]
Nov 18 16:52:11.300: NAT*: s=10.1.10.1->198.133.219.6, d=192.168.2.1 [110]
Nov 18 16:52:11.308: NAT*: s=192.168.2.1, d=198.133.219.6->10.1.10.1 [110]
Nov 18 16:52:12.300: NAT*: s=10.1.10.1->198.133.219.6, d=192.168.2.1 [111]
Nov 18 16:52:12.312: NAT*: s=192.168.2.1, d=198.133.219.6->10.1.10.1 [111]
Nov 18 16:52:59.356: NAT*: s=10.1.100.252->198.133.219.4, d=192.168.2.1 [0]
Nov 18 16:52:59.368: NAT*: s=192.168.2.1, d=198.133.219.4->10.1.100.252 [0]
Nov 18 16:53:12.772: NAT: expiring 198.133.219.6 (10.1.10.1) icmp 512 (512)
Nov 18 16:53:47.140: NAT*: s=10.1.100.1->198.133.219.5, d=192.168.2.1 [0]
Nov 18 16:53:47.152: NAT*: s=192.168.2.1, d=198.133.219.5->10.1.100.1 [0]
Nov 18 16:53:53.992: NAT*: s=10.1.100.253->198.133.219.3, d=192.168.2.1 [0]
Nov 18 16:53:54.004: NAT*: s=192.168.2.1, d=198.133.219.3->10.1.100.253 [0]
```

This first output example of NAT debug shows dynamic NAT translation of test pings from internal host PC-B to simulated ISP R2, Lo0. Note that translations are aged out (expired) if the source host does not refresh the address assignment. The **`terminal monitor`** command was issued on R1 so that the debug output could be viewed from a Telnet connection.

```
R1#debug ip nat
IP NAT debugging is on
R1#
Nov 18 19:31:36.112: NAT: translation failed (A), dropping packet s=10.1.10.1 d=
192.168.2.1
Nov 18 19:31:37.108: NAT: translation failed (A), dropping packet s=10.1.10.1 d=
192.168.2.1
R1#
Nov 18 19:31:38.112: NAT: translation failed (A), dropping packet s=10.1.10.1 d=
192.168.2.1
R1#
Nov 18 19:31:39.112: NAT: translation failed (A), dropping packet s=10.1.10.1 d=
192.168.2.1
```

The above output example shows error messages reported on the NAT router because of pool depletion and the inability to assign a public source address to the packet being routed.

```
R1#debug ip icmp
ICMP packet debugging is on

Nov 18 19:50:50.879: ICMP: dst (192.168.2.1) host unreachable sent to 10.1.10.1
Nov 18 19:50:51.875: ICMP: dst (192.168.2.1) host unreachable sent to 10.1.10.1
R1#
Nov 18 19:50:52.879: ICMP: dst (192.168.2.1) host unreachable sent to 10.1.10.1
R1#
Nov 18 19:50:53.879: ICMP: dst (192.168.2.1) host unreachable sent to 10.1.10.1
```

The **`debug ip icmp`** output shows R1 responding to host PC-B with an error during a ping to the ISP because of the lack of NAT translation.

```
R2#debug ip icmp
Nov 18 18:29:31.381: ICMP: echo reply sent, src 192.168.2.1, dst 10.1.10.1
Nov 18 18:29:36.737: ICMP: echo reply sent, src 192.168.2.1, dst 10.1.10.1
Nov 18 18:29:41.745: ICMP: echo reply sent, src 192.168.2.1, dst 10.1.10.1
Nov 18 18:29:46.753: ICMP: echo reply sent, src 192.168.2.1, dst 10.1.10.1
```

The above output shows R2 sending replies to PC-B at the internal private address because of the lack of NAT translation.

DHCP-Related Commands

```
DLS2#show ip dhcp server statistics
Memory usage          15668
Address pools         1
Database agents       0
Automatic bindings    1
Manual bindings       0
Expired bindings      0
Malformed messages    0
Secure arp entries    0
Renew messages        2

Message               Received
BOOTREQUEST           0
DHCPDISCOVER          4
DHCPREQUEST           4
DHCPDECLINE           0
DHCPRELEASE           1
DHCPINFORM            0

Message               Sent
BOOTREPLY             0
DHCPOFFER             2
DHCPACK               4
DHCPNAK               0
```

The above output displays DHCP pool activity from hosts requesting IP addressing.

```
DLS2#show ip dhcp pool
Pool BRO3 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Excluded addresses             : 3
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased/Excluded/Total
 10.1.80.1            10.1.80.1        - 10.1.80.254       1     / 3     / 254
```

The above output displays DHCP pool information, including the address range, number of excluded addresses, and lease activity.

```
DLS2#show ip dhcp conflict
IP address        Detection method   Detection time          VRF
10.1.80.1         Gratuitous ARP     Nov 20 2009 06:09 PM
```


The above output displays an address conflict resulting from the attempted assignment of the 10.1.80.1 address. The server sends a ping for an address before it attempts to assign that address from the pool. Also, after the client is assigned an IP address by the DHCP server, it sends a Gratuitous ARP or test ARP for that address. If the address is already assigned to a device interface, the device to which it is assigned responds, and the DHCP server marks it as a conflicted address. Conflicted addresses can be cleared with the **`clear ip dhcp conflict *`** command.

```
DLS2#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
10.1.80.2           0100.0bdb.04a5.cd       Nov 21 2009 02:50 PM    Automatic
```

The above output displays the IP address, hardware (MAC) address, and lease expiration for a DHCP address assignment.

```
DLS2#debug ip dhcp server events
DHCP server event debugging is on.
DLS2#
Nov 20 15:20:31.653: DHCPD: Sending notification of TERMINATION:
Nov 20 15:20:31.653: DHCPD: address 10.1.80.2 mask 255.255.255.0
Nov 20 15:20:31.653: DHCPD: reason flags: RELEASE
Nov 20 15:20:31.653: DHCPD: htype 1 chaddr 000b.db04.a5cd
Nov 20 15:20:31.653: DHCPD: lease time remaining (secs) = 86356
Nov 20 15:20:31.653: DHCPD: interface = FastEthernet0/5
Nov 20 15:20:31.653: DHCPD: returned 10.1.80.2 to address pool BRO3.
DLS2#
Nov 20 15:20:46.226: DHCPD: Sending notification of DISCOVER:
Nov 20 15:20:46.226: DHCPD: htype 1 chaddr 000b.db04.a5cd
Nov 20 15:20:46.226:   DHCPD: giaddr = 10.1.80.1
Nov 20 15:20:46.226:   DHCPD: interface = FastEthernet0/5
Nov 20 15:20:46.226:   DHCPD: class id 4d53465420352e30
Nov 20 15:20:46.226:   DHCPD: Sending notification of DISCOVER:
Nov 20 15:20:46.226:   DHCPD: htype 1 chaddr 000b.db04.a5cd
Nov 20 15:20:46.226:   DHCPD: giaddr = 10.1.80.1
Nov 20 15:20:46.226:   DHCPD: interface = FastEthernet0/5
Nov 20 15:20:46.226:   DHCPD: class id 4d53465420352e30
Nov 20 15:20:48.239:   DHCPD: client requests 10.1.80.2.
Nov 20 15:20:48.239:   DHCPD: Adding binding to radix tree (10.1.80.2)
Nov 20 15:20:48.239:   DHCPD: Adding binding to hash tree
Nov 20 15:20:48.239:   DHCPD: assigned IP address 10.1.80.2 to client
0100.0bdb.04a5.cd. (471 0)
Nov 20 15:20:48.239:   DHCPD: Sending notification of ASSIGNMENT:
Nov 20 15:20:48.239:   DHCPD: address 10.1.80.2 mask 255.255.255.0
Nov 20 15:20:48.239:   DHCPD: htype 1 chaddr 000b.db04.a5cd
Nov 20 15:20:48.239:   DHCPD: lease time remaining (secs) = 86400
Nov 20 15:20:48.239:   DHCPD: interface = FastEthernet0/5

Nov 20 15:21:49.307: DHCPD: checking for expired leases.
```

The above output shows the process that the DHCP server goes through when a client issues the **`ipconfig /release`** and **`ipconfig /renew`** commands.

```
R3#debug ip udp
UDP packet debugging is on
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
```



```
R3(config)#int f0/0
R3(config-if)#no ip helper-address 10.1.2.13
R3(config-if)#
*Nov 20 15:53:29.606: UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length
=308
*Nov 20 15:53:32.606: UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length
=308
*Nov 20 15:53:41.610: UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length
=308
*Nov 20 15:53:57.614: UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length
=308
R3#
```

The above output shows the DHCP relay agent (R3) messages when a helper address is not configured. The UDP packets received are from the DHCP client (the source address is 0.0.0.0 port 68) searching for a DHCP server (the destination broadcast address is 255.255.255.255 port 67). There are no sent messages to the client because the broadcast is not forwarded to the DHCP server.

```
R3(config)#int f0/0
R3(config-if)#ip helper-address 10.1.2.13
R3(config-if)#
*Nov 20 15:54:19.547: Reserved port 67 in Transport Port Agent for UDP IP type 1
*Nov 20 15:54:34.035: UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length
=308
*Nov 20 15:54:34.035: UDP: sent src=10.1.80.1(67), dst=10.1.2.13(67), length=308
*Nov 20 15:54:36.043: UDP: rcvd src=10.1.2.13(67), dst=10.1.80.1(67), length=308
*Nov 20 15:54:36.047: UDP: sent src=0.0.0.0(67), dst=255.255.255.255(68), length
=308
*Nov 20 15:54:36.047: UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length
=324
*Nov 20 15:54:36.047: UDP: sent src=10.1.80.1(67), dst=10.1.2.13(67), length=324
*Nov 20 15:54:36.051: UDP: rcvd src=10.1.2.13(67), dst=10.1.80.1(67), length=308
*Nov 20 15:54:36.051: UDP: sent src=0.0.0.0(67), dst=255.255.255.255(68), length
=308
```

The above output shows the DHCP relay agent (R3) messages when a helper address is configured. The DHCP exchange between the server and the client are captured.

```
DLS2#show ip sockets
Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
 17   --listen--          10.1.200.253     1985   0   0 1001   0
 17 10.1.50.1        162 10.1.100.253    62682   0   0    0   0
 17   --listen--          10.1.200.253     1975   0   0   11   0
 17 10.1.80.1         67 10.1.200.253       67   0   0 2211   0
 17 0.0.0.0            0 10.1.200.253     2228   0   0  211   0
 17   --listen--          10.1.200.253      161   0   0    1   0
 17   --listen--          10.1.200.253      162   0   0   11   0
 17   --listen--          10.1.200.253    55485   0   0    1   0
 17   --listen--          --any--           161   0   0 20001   0
 17   --listen--          --any--           162   0   0 20011   0
 17   --listen--          --any--         61812   0   0 20001   0
 17   --listen--          10.1.200.253      123   0   0    1   0
 17 10.1.50.1        514 10.1.100.253    58346   0   0 400201   0
```

The above output displays the current connections for this server. The remote connection with R3 Fa0/0 (10.1.80.1) shows that the DHCP server is running on DLS2 and listening for requests on port 67 (DHCP server).

Reflection Questions

1. Which lab trouble tickets did you have the most difficulty with?

2. Would you change anything about the process that you used for any of the trouble tickets now that you see the resolution of the problem?

3. Which commands did you find most useful in diagnosing NAT and DHCP issues? Add these to your toolbox for future use. Which commands did you find least useful?

References

If you need more information on the commands and their options, see the following references:

- IP Routing Protocol Command Reference
  http://www.cisco.com/cisco/web/support/index.html
- Cisco IOS IP Switching Reference
  http://www.cisco.com/en/US/docs/ios/ipswitch/command/reference/isw_book.html
- Configuring Network Address Translation
  http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080094e77.shtml
- Configuring a Cisco IOS DHCP Server
  http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfdhcp.html

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1700	Fast Ethernet 0 (FA0)	Fast Ethernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
1800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2600	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)
2800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. Rather than try to list all the combinations of configurations for each router class, this table includes identifiers for the possible combinations of Ethernet and serial interfaces in the device. The table does not include any other type of interface, even though a specific router might contain one. An example of this is an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

Device Configurations (instructor version)

Note: All device configurations are provided for TT-A. The configs provided here are *not* running-config outputs. They can be used for copy-and-paste for TT-A and subsequent tickets. Where a config is noted as being the same as a previous one, the only change is in the MOTD, which identifies the Lab and TT. The errors in the configuration are commented and highlighted as red text.

Trouble Ticket - TT-A Configurations

Switch ALS1

```
!Lab 6-1 Switch ALS1 TT-A Config
!
```



```
hostname ALS1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 6-1 Switch ALS1 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet

spanning-tree mode rapid-pvst
spanning-tree portfast default
!
interface Vlan1
 no ip address
 shutdown
!
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 100
 name MGMT
```



```
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel1
 description Channel to DLS1
 no shutdown
 !
interface Port-channel2
 description Channel to DLS2
 no shutdown
!
interface FastEthernet0/1
 description Channel to DLS1
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shutdown
!
interface FastEthernet0/2
 description Channel to DLS1
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shutdown
!
interface FastEthernet0/3
 description Channel to DLS2
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shutdown
!
interface FastEthernet0/4
 description Channel to DLS2
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shutdown
!
interface FastEthernet0/5
 description Unused
 switchport access vlan 999
 switchport mode access
```



```
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown

interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
```



```
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description To PC-B
 switchport access vlan 10
 switchport mode access
 switchport voice vlan 20
 spanning-tree portfast
 switchport port-security
 switchport port-security maximum 2
 switchport port-security violation shutdown
 switchport port-security mac-address sticky
 no shut
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
```



```
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan100
 ip address 10.1.100.1 255.255.255.0
 no shutdown
!
ip default-gateway 10.1.100.254
!
ip http server
ip http secure-server
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server host 10.1.50.1 version 2c cisco
snmp-server enable traps vtp
```



```
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps vlan-membership
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
  no transport input
!
ntp source Vlan100
ntp server 192.168.2.1
end
```

Switch DLS1

```
!Lab 6-1 Switch DLS1 TT-A Config
!
hostname DLS1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55

banner motd $*** Lab 6-1 Switch DLS1 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
!
ip domain name tshoot.net
!
ip dhcp excluded-address 10.1.10.252 10.1.10.254
ip dhcp excluded-address 10.1.20.252 10.1.20.254
ip dhcp excluded-address 10.1.30.252 10.1.30.254
!
```



```
ip dhcp pool OFFICE
   network 10.1.10.0 255.255.255.0
   default-router 10.1.10.254
   domain-name tshoot.net
!
ip dhcp pool VOICE
   network 10.1.20.0 255.255.255.0
   default-router 10.1.20.254
   domain-name tshoot.net
!
ip dhcp pool GUEST
   network 10.1.30.0 255.255.255.0
   default-router 10.1.30.254
   domain-name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 24576
spanning-tree vlan 20,50 priority 28672
!
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 100
 name MGMT
!
vlan 200
 name TRANS
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
```



```
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel1
 description Channel to ALS1
 no shut
!
interface Port-channel10
 description Channel to DLS2
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R1
 no switchport
 ip address 10.1.2.1 255.255.255.252
 spanning-tree bpduguard enable
 speed 100
 duplex full
```

```
 no shut
!
interface FastEthernet0/6
 description FE to SRV1
 switchport access vlan 50
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shut
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
```

```
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
```



```
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown

interface Vlan10
 ip address 10.1.10.252 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 priority 110
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.252 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.252 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 priority 110
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.252 255.255.255.0
 standby 50 ip 10.1.50.254
```

```
 standby 50 preempt
!
interface Vlan100
 ip address 10.1.100.252 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 priority 110
 standby 100 preempt
!
interface Vlan200
 ip address 10.1.200.252 255.255.255.0
!
router eigrp 1
 passive-interface default
 no passive-interface Fa0/5
 no passive-interface vlan200
 no auto-summary
 network 10.1.0.0 0.0.255.255
!
ip classless
ip http server
ip http secure-server
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server host 10.1.50.1 version 2c cisco
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 192.168.2.1
end
```

Switch DLS2

```
!Lab 6-1 Switch DLS2 TT-A Config
```

```
!
hostname DLS2
!
service timestamps debug datetime msec
service timestamps log datetime
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 6-1 Switch DLS2 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
  path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 28672
spanning-tree vlan 20,50 priority 24576

vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
```

```
vlan 50
 name SERVERS
!
vlan 100
 name MGMT
!
vlan 200
 name TRANS
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel2
 description Channel to ALS1
 no shut

interface Port-channel10
 description Channel to DLS1
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS1
```



```
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R3
 no switchport
 ip address 10.1.2.13 255.255.255.252
 speed 100
 duplex full
 spanning-tree bpduguard enable
 no shutdown
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
```

```
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description FE to PC-C
 switchport access vlan 30
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
```



```
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 10.1.10.253 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 preempt
!
```

```
interface Vlan20
 ip address 10.1.20.253 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 priority 110
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.253 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.253 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 priority 110
 standby 50 preempt
!
interface Vlan100
 ip address 10.1.100.253 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 preempt
!
interface Vlan200
 ip address 10.1.200.253 255.255.255.0
!
router eigrp 1
 passive-interface default
 no passive-interface Fa0/5
 no passive-interface vlan200
 no auto-summary
 network 10.1.0.0 0.0.255.255
!
ip classless
ip http server
ip http secure-server
!
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
```



```
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 192.168.2.1
end
```

Router R1

```
!Lab 6-1 Router R1 TT-A Config
!
hostname R1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 6-1 Router R1 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 192.168.1.1 255.255.255.255
!
interface FastEthernet0/0
 no ip address
```



```
 shutdown
!
interface FastEthernet0/1
 description FE to DLS1
 ip address 10.1.2.2 255.255.255.252
 ip flow ingress
 ip nat inside
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
 description WAN link to ISP R2
 ip address 209.165.200.225 255.255.255.252
 ip nat outside
 ip flow ingress
 encapsulation ppp
 clock rate 128000
  no shutdown
!
interface Serial0/0/1
 description WAN link to R3 – Not used for this TT
 ip flow ingress
 encapsulation ppp
 clock rate 128000
 shutdown
!
router eigrp 1
 redistribute static
 passive-interface default
 no passive-interface FastEthernet0/1
 network 10.1.2.0 0.0.0.3
 network 192.168.1.1 0.0.0.0
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 209.165.200.226
!
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
ip nat pool public-addrs 198.133.219.5 198.133.219.30 netmask 255.255.255.224
ip nat source list 1 pool public-addrs
ip nat inside source static 10.1.50.1 198.133.219.1
!
logging source-interface Loopback0
logging 10.1.50.1
!
access-list 1 permit 10.1.0.0 0.0.255.255
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
```

Error: Inside is not specified on public-addrs pool statement.

no ip nat source list 1 pool public-addrs
ip nat inside source list 1 pool public-addrs


```
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 192.168.2.1
end
```

Router R2

```
!Lab 6-1 Router R2 TT-A Config
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
Hostname R2
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 6-1 Router R2 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
```



```
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 192.168.2.1 255.255.255.255
!
interface FastEthernet0/0
 shutdown
!
interface FastEthernet0/1
 shutdown
!
interface Serial0/0/0
 description WAN link to R1 – T1 leased line
 ip address 209.165.200.226 255.255.255.252
 encapsulation ppp
 no shutdown
!
interface Serial0/0/1
 shutdown
!
ip route 192.168.1.1 255.255.255.255 209.165.200.225
ip route 198.133.219.0 255.255.255.224 209.165.200.225
!
ip http server
no ip http secure-server
!
logging source-interface Loopback0
logging 10.1.50.1
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
!
ntp master 3
 end
```

Router R3

```
!Lab 6-1 Router R3 TT-A Config
!
service timestamps debug datetime msec
service timestamps log datetime msec
```

```
service password-encryption
!
hostname R3
!
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 6-1 Router R3 TT-A Config ***$
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
no ip domain lookup
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 10.1.203.1 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown
!
interface FastEthernet0/1
 description FE to DLS2
 ip address 10.1.2.14 255.255.255.252
 ip flow ingress
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
description WAN link to R1 – not used for this lab
 no ip address
 clock rate 128000
 shutdown
!
interface Serial0/0/1
 description WAN link to R2 - not used for this lab
```

```
 no ip address
 shutdown
!
router eigrp 1
 passive-interface default
 no passive-interface FastEthernet0/1
 network 10.1.2.12 0.0.0.3
 network 10.1.203.1 0.0.0.0
 no auto-summary
!
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
logging source-interface Loopback0
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 192.168.2.1
end
```

Trouble Ticket - TT-B Configs

Switch ALS1—Same as TT-A

Switch DLS1—Same as TT-A

Switch DLS2—Same as TT-A

Router R2—Same as TT-A

Router R3—Same as TT-A

Router R1

```
!Lab 6-1 Router R1 TT-B Config
!
hostname R1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 6-1 Router R1 TT-B Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 192.168.1.1 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown
```



```
!
interface FastEthernet0/1
 description FE to DLS1
 ip address 10.1.2.2 255.255.255.252
 ip flow ingress
 ip nat inside
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
 description WAN link to ISP R2
 ip address 209.165.200.225 255.255.255.252
 ip nat outside
 ip flow ingress
 encapsulation ppp
 clock rate 128000
  no shutdown
!
interface Serial0/0/1
 description WAN link to R3 – Not used for this TT
 ip flow ingress
 encapsulation ppp
 clock rate 128000
 shutdown
!
router eigrp 1
 redistribute static
 passive-interface default
 no passive-interface FastEthernet0/1
 network 10.1.2.0 0.0.0.3
 network 192.168.1.1 0.0.0.0
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 209.165.200.226
!
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
ip nat pool public-addrs 198.133.219.3 198.133.219.6 netmask 255.255.255.248
ip nat inside source list 1 pool public-addrs
ip nat inside source static 10.1.50.1 198.133.219.1
!
logging source-interface Loopback0
logging 10.1.50.1
!
access-list 1 permit 10.1.0.0 0.0.255.255
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
```

Error: NAT pool is very small. Configure overload on the pool.

no ip nat source list 1 pool public-addrs

ip nat inside source list 1 pool public-addrs overload


```
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 192.168.2.1
end
```

Trouble Ticket - TT-C Configs

Switch ALS1—Same as TT-A

Switch DLS1—Same as TT-A

Router R2—Same as TT-A

Router R1

```
!Lab 6-1 Router R1 TT-C Config
!
hostname R1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 6-1 Router R1 TT-C Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
```



```
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 192.168.1.1 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown
!
interface FastEthernet0/1
 description FE to DLS1
 ip address 10.1.2.2 255.255.255.252
 ip flow ingress
 ip nat inside
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
 description WAN link to ISP R2
 ip address 209.165.200.225 255.255.255.252
 ip nat outside
 ip flow ingress
 encapsulation ppp
 clock rate 128000
  no shutdown
!
interface Serial0/0/1
 description WAN link to R3 – Not used for this TT
 ip flow ingress
 encapsulation ppp
 clock rate 128000
 shutdown
!
router eigrp 1
 redistribute static
 passive-interface default
 no passive-interface FastEthernet0/1
 network 10.1.2.0 0.0.0.3
 network 192.168.1.1 0.0.0.0
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 209.165.200.226
!
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
```



```
ip flow-export destination 10.1.50.1 9996
!
ip nat pool public-addrs 198.133.219.5 198.133.219.30 netmask 255.255.255.224
ip nat inside source list 1 pool public-addrs overload
ip nat inside source static 10.1.50.1 198.133.219.1
!
logging source-interface Loopback0
logging 10.1.50.1
!
access-list 1 permit 10.1.0.0 0.0.255.255
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 192.168.2.1
end
```

Router R3

```
!Lab 6-1 Router R3 TT-C Config
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 6-1 Router R3 TT-C Config ***$
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
```



```
no ip domain lookup
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 10.1.203.1 255.255.255.255
!
interface FastEthernet0/0
 description FE to Branch office
 ip address 10.1.80.1 255.255.255.0
 no shutdown
!
interface FastEthernet0/1
 description FE to DLS2
 ip address 10.1.2.14 255.255.255.252
 ip flow ingress
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
description WAN link to R1 – not used for this lab
 no ip address
 clock rate 128000
 encapsulation ppp
 shutdown
!
interface Serial0/0/1
 description WAN link to R2 - not used for this lab
 no ip address
 encapsulation ppp
 shutdown
!
router eigrp 1
 passive-interface default
 no passive-interface FastEthernet0/1
 network 10.1.2.12 0.0.0.3
 network 10.1.80.0 0.0.0.255
 network 10.1.203.1 0.0.0.0
 no auto-summary
!
ip http server
no ip http secure-server
!
```

Error: Helper address is not configured on Fa0/0.

```
interface FastEthernet0/0
 ip helper-address 10.1.2.13
```



```
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
logging source-interface Loopback0
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 192.168.2.1
end
```

Switch DLS2

```
!Lab 6-1 Switch DLS2 TT-C Config
!
hostname DLS2
!
service timestamps debug datetime msec
service timestamps log datetime
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 6-1 Switch DLS2 TT-C Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
```



```
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
ip dhcp excluded-address 10.1.80.252 10.1.80.254
!
ip dhcp pool BRO3
   network 10.80.1.0 255.255.255.0
   default-router 10.1.80.1
   domain-name tshoot.net

!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
  path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 28672
spanning-tree vlan 20,50 priority 24576

vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 100
 name MGMT
!
vlan 200
 name TRANS
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
```

Error 1: Wrong addresses are excluded from the DHCP pool. R3 Fa0/0 IP address 10.1.80.1 should be excluded.

```
no ip dhcp excluded-address 10.1.80.252
10.1.80.254
ip dhcp excluded-address 10.1.80.1
```

Error 2: Wrong network address range is defined for pool. Change network to 10.1.80.0/24.

```
ip dhcp pool BRO3
 no network 10.80.1.0 255.255.255.0
 network 10.1.80.0 255.255.255.0
```



```
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel2
 description Channel to ALS1
 no shut

interface Port-channel10
 description Channel to DLS1
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R3
 no switchport
 ip address 10.1.2.13 255.255.255.252
 speed 100
 duplex full
 spanning-tree bpduguard enable
```



```
 no shutdown
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
```

```
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
```



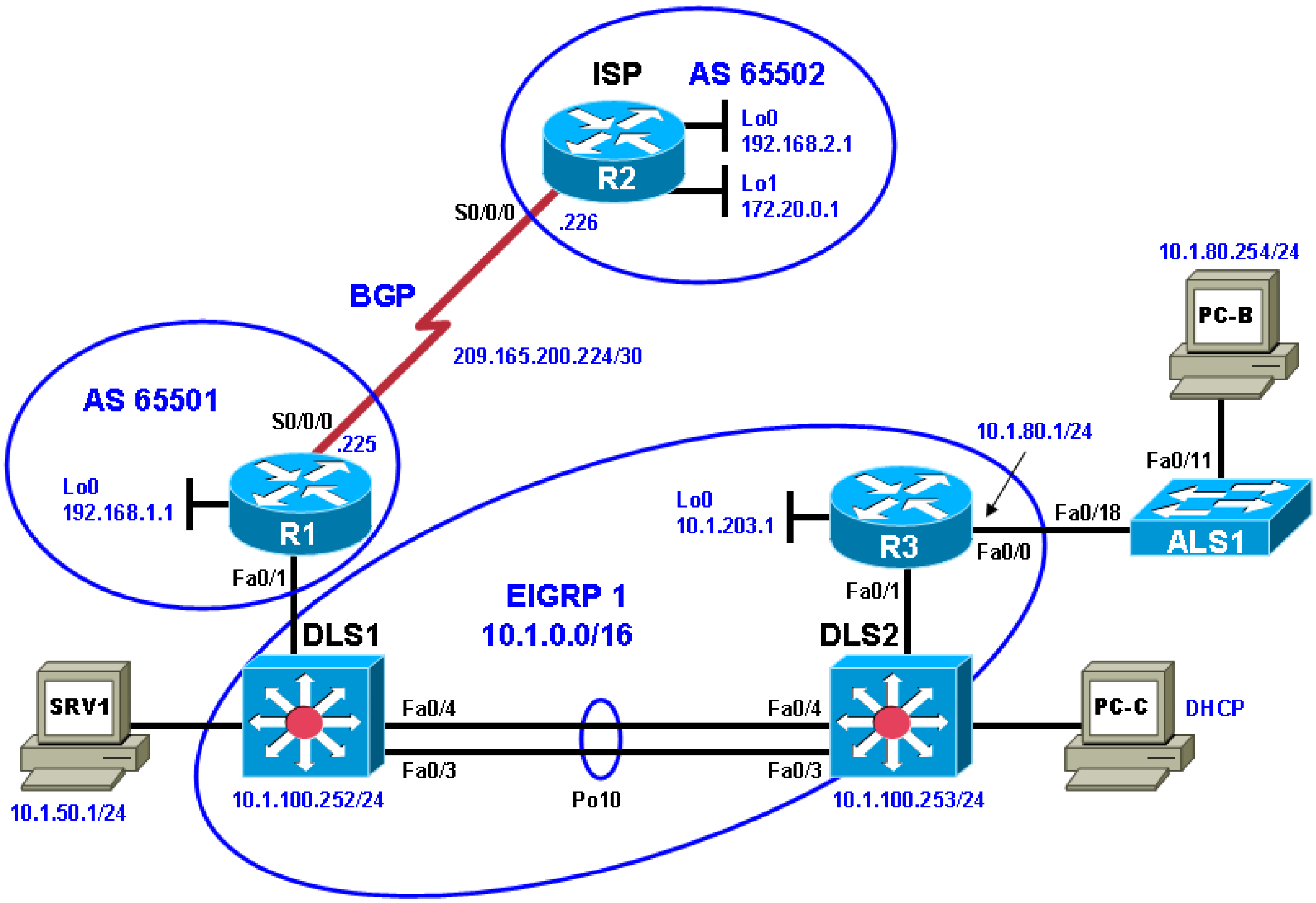
```
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 10.1.10.253 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.253 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 priority 110
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.253 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.253 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 priority 110
 standby 50 preempt
```



```
!
interface Vlan100
 ip address 10.1.100.253 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 preempt
!
interface Vlan200
 ip address 10.1.200.253 255.255.255.0
!
router eigrp 1
 passive-interface default
 no passive-interface Fa0/5
 no passive-interface vlan200
 no auto-summary
 network 10.1.0.0 0.0.255.255
!
ip classless
ip http server
ip http secure-server
!
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 192.168.2.1
end
```

Chapter 7 Lab 7-1, Router Performance **Instructor Version**

Lab Topology



Note: The topology for this lab moves access switch ALS1 to R3 and disconnects it from switches DLS1 and DLS2. This allows a load to be placed on R3 using ALS1 and DLS2. PC-B is moved to switch ALS1 port Fa0/11. Performance testing is done using Cisco IOS commands on R3 and pings from PC-B. Even though ALS1 is no longer attached to DSL1 and DLS2, VLAN 10 still exists. The interfaces for port channel 1 on DLS1 and port channel 2 on DLS2 are temporarily shutdown.

Objectives

- Load the trouble ticket device configuration files for each trouble ticket.
- Diagnose and resolve problems related to router performance, such as excessive CPU and memory utilization.
- Document troubleshooting progress, configuration changes, and problem resolution.

Background

A number of factors can affect router performance. In addition to heavy traffic loads, these can include suboptimal configurations for interfaces, WAN links, access lists, and routing protocols. In this activity, you troubleshoot various problems related to router performance and use Cisco IOS utilities to help diagnose the issues. For each task or trouble ticket, the trouble scenario and problem symptom is described. While troubleshooting, you will discover the cause of the problem, correct it, and then document the process and results.

Note: The focus of this lab is on the tools available to diagnose performance issues. The problems induced are intended to create symptoms in a lab environment and are not necessarily real-world examples. In addition to the information provided in Section 2, command examples and assistance are provided inline with the trouble tickets.

Lab Structure

This lab is divided into two main sections.

Section 1—Trouble Tickets and Troubleshooting Logs

This section includes multiple tasks. Each task is associated with a trouble ticket (TT) and introduces one or more errors on one or more devices. If time is a consideration, each task or trouble ticket can be performed independently.

Section 2—Troubleshooting Reference Information

This section provides a generic troubleshooting process and examples of useful commands and output. If time permits, it is recommended you read through Section 2 prior to starting on the trouble tickets.

Note: This lab uses Cisco 1841 routers with Cisco IOS Release 12.4(24)T1 and the Advanced IP Services image c1841-advipservicesk9-mz.124-24.T1.bin. The switches are Cisco WS-C2960-24TT-L with the Cisco IOS image c2960-lanbasek9-mz.122-46.SE.bin and Catalyst 3560-24PS with the Cisco IOS image c3560-advipservicesk9-mz.122-46.SE.bin. Other routers (such as 2801 and 2811), switches (such as 2950 or 3550), and Cisco IOS Software versions can be used if they have comparable capabilities and features. Depending on the router or switch model and Cisco IOS Software version, the commands available and output produced might vary from what is shown in this lab.

Instructor Notes

- The lab topology should be pre-built prior to the students starting the lab. Ensure that all routers and switches (R1, R2, R3, ALS1, DLS1, and DLS2) have the course lab configuration files installed in flash. You can download the files from the Academy Connection website.
- The device configurations that contain trouble ticket errors or modifications from the baseline are included at the end of the lab and the errors in them are identified.
- Each device has a directory named "tshoot" in flash. This directory contains the baseline configuration file for that device as well as configuration files for the labs in this course. Refer to Lab 3-1 for instructions on creating the tshoot directory in flash.
- Instructors can use a TFTP server, USB drive, flash memory card, or other method to copy all the course configuration files into the flash:/tshoot directory for each device in the topology.
- The student is responsible for loading the trouble ticket configurations for all labs as required using the procedure described in Lab 3-1.
- Set the correct time on router R2, which serves as the primary NTP server for the lab network.
- If time is an issue, each task (trouble ticket) can be performed independently.

Required Resources

- 3 routers (Cisco 1841 with the Cisco IOS Release 12.4(24)T1 Advanced IP Service or comparable)

- 1 switch (Cisco 2960 with the Cisco IOS Release 12.2(46)SE C2960-LANBASEK9-M image or comparable)
- 2 switches (Cisco 3560 with the Cisco IOS Release 12.2(46)SE C3560- advipservicesk9-mz image or comparable)
- SRV1 (Windows PC with 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

Instructor Notes

- This lab is divided into multiple tasks. Each task is associated with a trouble ticket (TT) and introduces one or more errors on one or more devices.
- Students can work individually or as a team.
- Suggested actions and results presented during the troubleshooting process for each TT can be shared with the students during debrief or copies of the instructor version of the lab can be made available to the students to assist them in verifying their work.

Section 1—Trouble Tickets and Troubleshooting Logs

Task 1: Trouble Ticket Lab 7-1 TT-A

Instructor note: This trouble ticket involves device R3 and issues related to process switching and a large access list that can cause high CPU utilization on a router.

In this lab, the Cisco IOS command **`ttcp`** is used to simulate a heavy traffic load between switches ALS1 and DLS2. The TTCP utility is a hidden, unsupported Cisco IOS command. This lab provides step-by-step assistance for using Cisco IOS performance diagnostic commands and the TTCP utility.

Note: Appendix A contains additional information on how to set up a PC as a client end device for TTCP.

A recommended approach to this lab is to follow a troubleshooting process that includes the following high-level tasks:

- Generate test traffic using the **`ping`** or **`ttcp`** command, as described in this task.
- Use **`ping`** to measure the performance between the headquarters and branch office. For example, ping from client PC-B to server SRV1.
- Examine the key performance indicators, such as interfaces, CPU, and memory on the routers, and look for symptoms associated with performance problems.
- Examine the routers for features and configurations that deviate from the baseline configurations and attempt to find the root cause of the problems.
- Address the issues causing the performance problems and test to verify that the performance has improved.

Step 1: Review trouble ticket Lab 7-1 TT-A.

It is Monday morning and as soon as you enter your office at headquarters, you receive a call from your colleague from the branch office (R3 LAN). She tells you that client (PC-B) applications report errors while connecting to the corporate server (SRV1) for large file transfers (simulated by TTCP). Your colleague suspects that there is performance degradation on the R3 router and has run some tests to verify this. She also has the baseline performance tests to compare with.

Another colleague who works the night shift has full access to the branch office devices. You suspect he might have made some configuration changes.

Your task is to diagnose the branch office problems and correct them.

Step 2: Load the device trouble ticket configuration files for TT-A.

Using the procedure described in Lab 3-1, verify that the lab configuration files are present in flash. Load the proper configuration files as indicated in the Device Configuration File Table.

Note: The following device access methods are in effect after loading the configuration files:

- Console access requires no username or password.
- Telnet and SSH require username **admin** and password **adminpa55**.
- The enable password is **ciscoenpa55**.

Instructor note: Although it is not considered a security best practice, the enable secret and admin user passwords can be changed to something simpler to facilitate access to devices in this lab.

Device Configuration File Table

Device Name	File to Load	Notes
ALS1	Lab71-ALS1-TT-A-Cfg.txt	This file contains configurations different than the baseline

DLS1	Lab71-DLS1-TT-A-Cfg.txt	This file contains configurations different than the baseline
DLS2	Lab71-DLS2-TT-A-Cfg.txt	This file contains configurations different than the baseline
R1	Lab71-R1-TT-A-Cfg.txt	This file contains configurations different than the baseline
R2	Lab71-R2-TT-A-Cfg.txt	This file contains configurations different than the baseline
R3	Lab71-R3-TT-A-Cfg.txt	This file contains configuration errors
SRV1	N/A	Static IP: 10.1.50.1/24 Default gateway: 10.1.50.254
PC-B	N/A	Static IP: 10.1.80.254/24 Default gateway: 10.1.80.1
PC-C	N/A	DHCP

Instructor note: The student loads the "broken" TT configuration files for all devices, even though only the configurations indicated in the Notes column contain errors.

Step 3: Configure PC-B.

Configure PC-B with static IP address 10.1.80.254/24 and default gateway 10.1.80.1.

Step 4: Test R3 performance without the TTCP load generator.

Use Cisco IOS commands and pings to record the router performance figures simulating a condition where no large file transfers are currently being transmitted from PC-B to SRV1. These results can be compared to the baseline output (selected baseline information is shown) and the output obtained when using the TTCP utility.

Note: Sample output is provided. Depending on your timing and the devices in use, the output and results may vary.

a. Ping from PC-B to SRV1 (10.1.50.1) and record the results here. Include minimum, maximum, and average round-trip times.

____

____

```
C:\>ping 10.1.50.1

Pinging 10.1.50.1 with 32 bytes of data:
Reply from 10.1.50.1: bytes=32 time=3ms TTL=64
Reply from 10.1.50.1: bytes=32 time=1ms TTL=64
Reply from 10.1.50.1: bytes=32 time=1ms TTL=64
Reply from 10.1.50.1: bytes=32 time=1ms TTL=64

Ping statistics for 10.1.50.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 1ms
```

b. Issue the **`show interfaces fa0/0`** command and note the transmit and receive loads (txload and rxload).

____

____


```
R3#show interfaces fa0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is Gt96k FE, address is 001b.530d.6028 (bia 001b.530d.6028)
  Internet address is 10.1.80.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

c. Issue the **show interfaces fa0/0 stats** command. Record the switching path and the packets in and out for processor and route cache.

____

____

```
R3#show interfaces fa0/0 stats

FastEthernet0/0
          Switching path    Pkts In   Chars In   Pkts Out  Chars Out
               Processor         50      16309        176      18457
             Route cache          1        159          0          0
                   Total         51      16468        176      18457

                   Total     116557   66924378     115034    6384079
```

d. Issue the **show interfaces fa0/0 summary** command for Fa0/0 and note the transmit (tx) and receive (rx) rates in bits per second and packets per second. With no load, there might be very little activity.

____

____

```
R3#show interfaces fa0/0 summary

 *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count

  Interface             IHQ   IQD  OHQ   OQD  RXBS RXPS  TXBS TXPS TRTL
------------------------------------------------------------------------
* FastEthernet0/0         0     0    0     0     0    1     0    0    0
```

e. Issue the **show processes cpu sorted** command on R3 and note the CPU utilization for five seconds, one minute, and five minutes. Also note that the processes running are sorted by highest CPU utilization.

____

____

```
   R3#show processes cpu sorted
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
 PID Runtime(ms)   Invoked  uSecs   5Sec   1Min   5Min TTY Process
 153           4   1366369      0  0.15%  0.12%  0.10%   0 HQF Shaper Backg

   2           0      7658      0  0.07%  0.02%  0.02%   0 Load Meter
```



```
   5           4          3   1333  0.00%  0.00%  0.00%   0 Pool Manager
<output omitted>
```

f. Generate some traffic by pinging from switch ALS1 to SRV1. From privileged EXEC mode on ALS1, issue the **`ping 10.1.50.1 repeat 1000 size 1000`** command. What are the minimum, maximum, and average round-trip times? Answers will vary.

____

____

```
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 1/4/9 ms
```

g. Quickly issue the **`show processes cpu sorted`** command on R3 again and note the CPU utilization for five seconds, one minute, and five minutes.

____

____

```
R3#show processes cpu sorted
CPU utilization for five seconds: 17%/5%; one minute: 3%; five minutes: 1%
 PID Runtime(ms)   Invoked  uSecs   5Sec   1Min   5Min TTY Process
  91        2308      4797    481 11.19%  2.10%  0.52%   0 IP Input

   3       13308      2477   5372  0.87%  0.18%  0.05%   0 Exec

 124          12       265     45  0.15%  0.03%  0.00%   0 TCP Timer

 153          20     93423      0  0.15%  0.12%  0.10%   0 HQF Shaper Backg

265        1280     11572    110  0.07%  0.01%  0.00%   0 IP-EIGRP: HELLO
<output omitted>
```

h. Issue the **`show processes cpu history`** command on R3 to see CPU utilization history in graph format. Note the CPU utilization for the last 60 seconds, last 60 minutes, and last 72 hours.

____

____

```
R3#show processes cpu history

R3   06:04:05 PM Monday Nov 30 2009 UTC



    1               11111                                  11111
100
 90
 80
 70
 60
 50
 40
 30
 20
 10
   0....5....1....1....2....2....3....3....4....4....5....5....6
             0    5    0    5    0    5    0    5    0    5    0
```

```
               CPU% per second (last 60 seconds)


    5  1          1  1                                      9
    511911111111119119413111111111111112111111211111111111829111
100                                                         *
 90                                                         *
 80                                                         *
 70                                                         *
 60 *                                                       *
 50 *                                                       *
 40 *                                                       *
 30 *                                                       *
 20 *  *          *  *                                      #
 10 *  *          *  *                                    * #
   0....5....1....1....2....2....3....3....4....4....5....5....6
             0    5    0    5    0    5    0    5    0    5    0
               CPU% per minute (last 60 minutes)
              * = maximum CPU%   # = average CPU%

    9
    9
100 *
 90 *
 80 *
 70 *
 60 *
 50 *
 40 *
 30 *
 20 *
 10 *
   0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
             0    5    0    5    0    5    0    5    0    5    0    5    0
                   CPU% per hour (last 72 hours)
                  * = maximum CPU%   # = average CPU%
```

Step 5: Generate loads on R3 using the TTCP utility.

For this trouble ticket, you can use the Cisco IOS command **`ttcp`** to simulate a heavy traffic load instead of performing large file transfers between the client (PC-B) and server SRV1 for testing. The TTCP utility consists of a client side and server side. Because this lab revolves around router performance, you can use the switches as test points.

Note: The **`ttcp`** command is a hidden, unsupported, privileged mode command, and it is not available for all Cisco IOS Software releases. For instance, some platforms require the Cisco IOS Enterprise feature set to perform this activity. For more information about TTCP, see the URL references provided at the end of the lab and in Appendix A.

To initiate a TTCP connection and generate test traffic from switch ALS1 at the branch office to switch DLS2 at headquarters, use the following procedure.

a. On DLS2, the device that will perform the receiving (server) side of the connection, issue the **`ttcp`** command. You are prompted for information about this connection. You can accept the default values or enter new values. You can also use the command line to enter all the parameters as one command. The command generated is shown after the last entry prompt.

   As TTCP waits for the transmitting (client) side to make a connection, the console screen freezes.

```
DLS2#ttcp
```



```
transmit or receive [receive]:
receive packets asynchronously [n]:
perform tcp half close [n]:
receive buflen [32768]:
bufalign [16384]:
bufoffset [0]:
port [5001]:
sinkmode [y]:
rcvwndsize [32768]:
ack frequency [0]:
delayed ACK [y]:
show tcp information at end [n]:

ttcp-r: buflen=32768, align=16384/0, port=5001
rcvwndsize=32768, delayedack=yes  tcp
```

b. On ALS1, the device that will perform the client side of the connection, you must specify that this side is the transmitting side because the default is to run in receive mode. You must also specify the IP address of the receiving side (DLS2) to initiate the connection.

```
ALS1#ttcp
transmit or receive [receive]: transmit
Target IP address: 10.1.100.253
calculate checksum during buffer write [y]:
perform tcp half close [n]:
send buflen [32768]:
send nbuf [2048]:
bufalign [16384]:
bufoffset [0]:
port [5001]:
sinkmode [y]:
buffering on writes [y]:
show tcp information at end [n]:

ttcp-t: buflen=32768, nbuf=2048, align=16384/0, port=5001  tcp  ->
10.1.100.253
ttcp-t: connect
ttcp-t: 67108864 bytes in 106812 ms (106.812 real seconds) (~613 kB/s) +++
ttcp-t: 2048 I/O calls
ttcp-t: 0 sleeps (0 ms total) (0 ms average)
```

The DLS2 (receive) side of the connection shows the following information when the transfer completes:

```
ttcp-r: accept from 10.1.80.251
ttcp-r: 67108864 bytes in 106837 ms (106.837 real seconds) (~613 kB/s) +++
ttcp-r: 43182 I/O calls
ttcp-r: 0 sleeps (0 ms total) (0 ms average)
```

Referring to the above results, the TTCP utility transmitted over 67 million bytes in approximately 106 seconds or about 613 Kilobytes per second (kB/s). As a comparison, the baseline configuration without the errors in this trouble ticket took approximately 70 seconds to transmit the same amount of data but at a rate of about 898 kB/s. Different devices and network links produce different results.

Note: You cannot issue any commands on the console of either device until the transfer finishes. The transmission can be interrupted at any point in time from the transmitting side using the key combination Ctrl-Shift-6.

Caution: This utility can overload a router with test traffic. It is not recommended to use it on production devices. Read the TTCP documentation before using the TTCP utility.

Step 6: Test R3 with load applied.

Note: For this lab, TTCP utility creates a load that lasts 60–120 seconds. The actual length of time depends on the capabilities of the devices and links being used.

On R3, use Cisco IOS commands and pings to record the router performance figures simulating a condition where large file transfers are being transmitted. These results can be compared to the baseline output (selected baseline information is shown) and the output obtained when using the TTCP utility.

Try to issue the following Cisco IOS commands on R3 while TTCP is generating traffic between ALS1 and DSL2. If it stops, restart the transmit-receive process between switches ALS1 and DLS2. You can also increase the length of time traffic runs by increasing the **`send buflen`** parameter, which defaults to 32768 (for example, you can increase it 65536 or higher).

a. While TTCP is running, ping from PC-B to SRV1 and record the minimum, maximum, and average round-trip results.

____

____

The times should be 10 times or more higher than without the TTCP load on R3.

```
C:\>ping 10.1.50.1

Pinging 10.1.50.1 with 32 bytes of data:
Reply from 10.1.50.1: bytes=32 time=39ms TTL=64
Reply from 10.1.50.1: bytes=32 time=38ms TTL=64
Reply from 10.1.50.1: bytes=32 time=38ms TTL=64
Reply from 10.1.50.1: bytes=32 time=38ms TTL=64

Ping statistics for 10.1.50.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 38ms, Maximum = 39ms, Average = 38ms
```

b. On Fa0/0, change the period over which the loads are computed to 30 seconds.

```
interface fa0/0
    load-interval 30
```

c. Issue the **`show interfaces fa0/0`** command and note the values for txload and rxload.

____

```
R3#show interfaces fa0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is Gt96k FE, address is 001b.530d.6028 (bia 001b.530d.6028)
  Internet address is 10.1.80.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 0/255, rxload 4/255
```

d. Issue the **`show interfaces fa0/0 stats`** command and record the switching path and the packets in and out for processor and route cache.

____

____


```
R3#show interfaces f0/0 stats
FastEthernet0/0
          Switching path    Pkts In   Chars In   Pkts Out  Chars Out
               Processor     134289   77529720     129782   10884700
             Route cache          1        159          0          0
                   Total     134290   77529879     129782   10884700
```

e. Issue the **`show interfaces summary`** command for Fa0/0 and record the transmit (tx) and receive (rx) rates in bits per second and packets per second. How do they compare to the rates when TTCP is not running?

____

____

Much higher.

```
R3#show interfaces f0/0 summary

 *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count

  Interface              IHQ   IQD  OHQ   OQD  RXBS RXPS  TXBS TXPS TRTL
------------------------------------------------------------------------
* FastEthernet0/0          0     0    0     0 969000  204 94000  201    0
```

f. While TTCP is transferring data, issue the **`show processes cpu sorted`** command on R3 and note the CPU utilization for five seconds, one minute, and five minutes. How do they compare with utilization when TTCP is not running?

____

Much higher

```
R3#show processes cpu sorted
CPU utilization for five seconds: 99%/29%; one minute: 77%; five minutes: 26%
 PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
  91      201824       20441       9873 69.50% 54.19% 18.26%   0 IP Input

<output omitted>
```

g. After the TTCP transfer process ends, issue the **`show processes cpu history`** command on R3 to see the CPU utilization history in graph format. Note the CPU utilization for the last 60 seconds, 60 minutes, and 72 hours. What is the maximum utilization shown?

____

Most likely 99%

```
R3#show processes cpu history

R3   07:54:09 PM Monday Nov 30 2009 UTC


 999988888
 99999999922222                    11111
```



```
100 ****
 90 *********
 80 *********
 70 *********
 60 *********
 50 *********
 40 *********
 30 *********
 20 *********
 10 *********
   0....5....1....1....2....2....3....3....4....4....5....5....6
             0    5    0    5    0    5    0    5    0    5    0
               CPU% per second (last 60 seconds)


            992                                      3
    1111111199811111211111112111111111121111112111111131111111111
100         *#
 90         *#
 80         ##
 70         ##
 60         ##
 50         ##
 40         ##
 30         ##*                                       *
 20         ##*                                       *
 10         ##*                                       *
   0....5....1....1....2....2....3....3....4....4....5....5....6
             0    5    0    5    0    5    0    5    0    5    0
               CPU% per minute (last 60 minutes)
              * = maximum CPU%   # = average CPU%


    99
    99
100 **
 90 **
 80 **
 70 **
 60 **
 50 **
 40 **
 30 **
 20 **
 10 **
   0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
             0    5    0    5    0    5    0    5    0    5    0    5    0
                   CPU% per hour (last 72 hours)
                  * = maximum CPU%   # = average CPU%
```

h. Issue the **show memory statistics** command and note the free memory and the amount used. Is there an issue with memory usage with this router?

No. Used memory is about 24 MB, and free memory is about 77 MB.

```
R3#show memory statistics
```



```
             Head    Total(b)   Used(b)     Free(b)   Lowest(b)  Largest(b)
Processor  64E822C0  101178688  24016328    77162360  75584536   75588172
      I/O  EAF00000   17825792   5421744    12404048  12363136   1238780
```

Step 7: Outline the troubleshooting approach and validation steps.

The following approach is recommended as a troubleshooting process:

1. Generate test traffic using the **`ping`** and **`ttcp`** commands, as described in this task.
2. Use **`ping`** to measure the performance between the headquarters and branch office. For example, ping from client PC-B to server SRV1.
3. Examine the key performance indicators, such as the interfaces, CPU and memory on the routers, and watch for symptoms associated with performance problems.
4. Examine the routers for features and configurations that deviate from the baseline configurations and attempt to find the root cause of the problems.
5. Address the issues causing the performance problems and test to verify that the performance has improved.

Step 8: Record the troubleshooting process and configuration changes.

Document your actions and results during the troubleshooting process. List the commands you used to gather information. As you progress, record what you think the problem might be and which actions you will take to correct the problem.

Device	Actions and Results

Responses will vary but could include:

- Pings from PC-B to SRV1 have minimum, average, and maximum times in a normal range.

TT-A Issue 1

Cisco Express Forwarding is disabled on router R3. This results in slow processing and forwarding of packets, especially with heavy traffic loads.

- Pings from PC-B to SRV1 take much longer than normal.
- The **`show processes cpu sorted`** command on R3 indicates that the CPU is heavily loaded.
- The **`show memory statistics`** command on R3 indicates that there is sufficient free memory.
- The **`show interfaces fa0/0 stats`** command on R3 indicates that the switching path being used is a processor and not a route cache.
- The **`show ip cef`** command on R3 confirms that Cisco Express Forwarding is not running (not globally enabled).
- The **`show ip int fa0/0`** command on R3 confirms that IP Cisco Express Forwarding switching is disabled.

Action: Enable IP Cisco Express Forwarding globally on R3 and configure the IP route cache on interfaces Fa0/0 and Fa0/1. See TT-A debrief for additional information.

Verification: Ping times and TTCP file transfer improve. TTCP transfer time decreases from 106 seconds to 89 seconds, and the transfer rate improves from 613 kB/s to 735 kB/s.

TT-A Issue 2

A very large, unnecessary access list is applied to R3 Fa0/0, which is causing slow processing and forwarding of packets, especially with heavy traffic loads.

- Pings from PC-B to SRV1 still take longer than normal.
- The **`show processes cpu sorted`** command on R3 indicates that the CPU is still heavily loaded when transferring large files.
- ACL match messages display on the R3 console as packets are permitted, indicating that a logging ACL is in place.
- The **`show run interface fa0/0`** command on R3 indicates that an ACL is applied inbound on Fa0/0.
- The **`show access-lists`** command on R3 confirms that a very large and unnecessary access list is configured.

Action: Remove the ACL from R3 and remove the reference to it from interface Fa0/0. See the TT-A debrief for additional information.

Verification:

- ACL log messages stop displaying on the R3 console.
- Ping times and TTCP file transfer improve. TTCP transfer time decreases from 89 seconds to 70 seconds and the transfer rate improves.

Step 9: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with your instructor. This can include problems encountered, solutions applied, useful commands, alternate solutions, methods, and processes, and procedure and communication improvements.

____

____

____

____

____

____

____

Trouble Ticket TT-A Debrief—Instructor Notes

This trouble ticket consists of two issues. The first issue is the use of process switching as the switching mode. The second issue is a large unnecessary access list, which causes high CPU utilization on the branch office router R3.

TT-A Issue 1

The IP Cisco Express Forwarding process on R3 was disabled globally and IP route caching was disabled on Fa0/0 and Fa0/1. To disable process switching and re-enable Cisco Express Forwarding, issue the following commands on R3.

```
ip cef

interface FastEthernet0/0
 ip route-cache

interface FastEthernet0/1
 ip route-cache
```

Note: Enabling IP CEF globally automatically enables route cache on all interfaces so the **`ip route-cache`** command on Fa0/0 and Fa0/1 is not required.

TT-A Issue 2

A large unnecessary standard access list (huge-acl) was configured that did not even specify the R3 LAN subnet (10.1.80.0/24). The R3 LAN traffic was only allowed after the entire ACL was processed and the **`permit any`** statement at the end matched the 10.1.80.0/24 traffic. This ACL needed to be removed from R3. To correct this problem, issue the following commands on R3:

```
interface FastEthernet 0/0
 no ip access-group huge-acl in

no ip access-list standard huge-acl
```

Task 2: Trouble Ticket Lab 7-1 TT-B

Instructor note: This trouble ticket involves R2 issues related to an inappropriate BGP configuration that can cause memory exhaustion on a router.

Step 1: Review trouble ticket Lab 7-1 TT-B.

After the Internet service provider (ISP) reconfigured Border Gateway Protocol (BGP) on router R2, you received complaints from branch office users on the R3 LAN about it being slow or having no connection at all to the partner servers outside the corporate network residing in the IP address block 172.20.0.0/16 (simulated by R2 Lo1).

You have access to the R1 and R2 routers. Your task is to diagnose the problem and verify that BGP is properly configured to minimize the impact on internal routing performance for devices such as R3, DLS1, and DLS2.

Step 2: Load the device trouble ticket configuration files for TT-B.

Using the procedure described in Lab 3-1, verify that the lab configuration files are present in flash. Load the proper configuration files as indicated in the Device Configuration File table.

Note: See Task 1, Step 2 for device access methods, usernames, and passwords after the configuration files have been loaded.

Device Configuration File Table

Device Name	File to Load	Notes
ALS1	Lab71-ALS1-TT-B-Cfg.txt	This file contains configurations different than the baseline
DLS1	Lab71-DLS1-TT-B-Cfg.txt	This file contains configurations different than the baseline
DLS2	Lab71-DLS2-TT-B-Cfg.txt	This file contains configurations different than the baseline
R1	Lab71-R1-TT-B-Cfg.txt	This file contains configurations different than the baseline
R2	Lab71-R2-TT-B-Cfg.txt	This file contains configuration errors
R3	Lab71-R3-TT-B-Cfg.txt	This file contains configurations different than the baseline
SRV1	N/A	Static IP: 10.1.50.1 Default gateway: 10.1.50.254
PC-B	N/A	Static IP: 10.1.80.254/24 Default gateway: 10.1.80.1
PC-C	N/A	DHCP

Step 3: Test R3 performance without the TTCP load generator.

Use Cisco IOS commands and pings to record the router performance figures simulating a condition in which no large file transfers are currently being transmitted. These results can be compared to the baseline output (selected baseline information is shown) and the output obtained when using the TTCP utility.

a. Ping from PC-B to R2 Lo1 (simulated remote server) and record the minimum, maximum, and average round-trip times.

____


```
C:\>ping 172.20.0.1

Pinging 172.20.0.1 with 32 bytes of data:
Reply from 172.20.0.1 : bytes=32 time=11ms TTL=64
Reply from 172.20.0.1 : bytes=32 time=10ms TTL=64
Reply from 172.20.0.1 : bytes=32 time=10ms TTL=64
Reply from 172.20.0.1 : bytes=32 time=10ms TTL=64

Ping statistics for 172.20.0.1 :
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 11ms, Average = 10ms
```

b. Issue the **show interfaces fa0/0** command and note the txload and rxload information.

____

```
R3#show interfaces fa0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is Gt96k FE, address is 001b.530d.6028 (bia 001b.530d.6028)
  Internet address is 10.1.80.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
<output omitted>
```

c. Issue the **show interfaces fa0/0 stats** command and record the switching path and the packets in and out for the processor and route cache.

____

```
R3#show interfaces fa0/0 stats
FastEthernet0/0
          Switching path    Pkts In   Chars In   Pkts Out  Chars Out
               Processor        831     356623       4075     408723
             Route cache     381399  221941950     375270   20282949
                   Total     382230  222298573     379345   20691672
```

d. Issue the **show processes cpu sorted** command on R3 and note the CPU utilization for five seconds, one minute, and five minutes.

____

```
R3#show processes cpu sorted
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
```

e. Generate some traffic by pinging from switch ALS1 to R2 Lo1. From privileged EXEC mode on ALS1, issue the **ping 172.20.0.1 repeat 100 size 1000** command. What are the round-trip minimum, average, and maximum times?

____(

Answers will vary.

Success rate is 100% (100/100), round-trip min/avg/max = 125/129/135 ms

f. While the ping is running, issue the **`show processes cpu sorted`** command on R3 again and note the CPU utilization for five seconds, one minute, and five minutes. Was there an increase? _______ Yes

```
   R3#show processes cpu sorted
CPU utilization for five seconds: 11%/11%; one minute: 6%; five minutes: 2%
   <output omitted>
```

g. Issue the **`show processes cpu history`** command on R3 to see the CPU history in graph format. Note the CPU utilization for the last 60 seconds, 60 minutes, and 72 hours. Does the CPU appear to be heavily loaded? ____________ No

```
R3#show processes cpu history


R3   04:08:25 PM Tuesday Dec 1 2009 UTC



                             11111     11111
100
 90
 80
 70
 60
 50
 40
 30
 20
 10
   0....5....1....1....2....2....3....3....4....4....5....5....6
             0    5    0    5    0    5    0    5    0    5    0
               CPU% per second (last 60 seconds)


                                                      5
    2111211111111111111111112111111111111111111111113111151111111
100
 90
 80
 70
 60                                                   *
 50                                                   *
 40                                                   *
 30                                                   *
 20                                                   *
 10                                                   *
   0....5....1....1....2....2....3....3....4....4....5....5....6
             0    5    0    5    0    5    0    5    0    5    0
               CPU% per minute (last 60 minutes)
              * = maximum CPU%   # = average CPU%


    344351
    251910
100
 90
```



```
 80
 70
 60
 50  *  *
 40  ****
 30 *****
 20 *****
 10 ******
   0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
             0    5    0    5    0    5    0    5    0    5    0    5    0
                   CPU% per hour (last 72 hours)
                  * = maximum CPU%   # = average CPU%
```

h. Issue the **show processes memory sorted** command on R3. Note the processes running and the holding amount of memory. The holding amount is the memory the process is currently using. The entries go from highest holding memory to lowest.

```
R3#show processes memory sorted
Processor Pool Total:  101178688 Used:   24024572 Free:   77154116
      I/O Pool Total:   17825792 Used:    5421728 Free:   12404064

 PID TTY  Allocated      Freed    Holding    Getbufs    Retbufs Process
   0   0   64042304   36231984   23552016          0          0 *Init*

  55   0     659620       1328     640292          0          0 USB Startup

   1   0     474960          0     482164          0          0 Chunk Manager

 219   0     469096      18304     436816          0          0 VLAN Manager

  25   0     260308          0     270512      99792          0 EEM ED Syslog

 170   0     218420        504     215916          0          0 Crypto HW
Proc

 221   0     196192          0     203396          0          0 EEM Server

 183   0     114340        532     123012          0          0 Crypto WUI

 167   0      76476        252      83428          0          0 HTTP Process
```

i. Issue the **show memory statistics** command on R3. Note the amount of used and free memory for the processor for later comparison. By comparing the amount of memory used to the baseline (shown below), you can determine how much is used when the trouble ticket issues are introduced. You can also compare this to the memory when running the TTCP utility. The baseline memory amounts and after the TT was loaded are provided here for comparison.

Note: As can be seen below, the trouble ticket issues cause an increase of nearly 70 KB of memory over the baseline. This is not enough to cause serious memory depletion issues with the router but serves to illustrate the type of problem that can occur in a lab environment. Actual results might be very different in a production environment.

Baseline

```
R3#show memory statistics
             Head    Total(b)   Used(b)     Free(b)   Lowest(b)  Largest(b)
```



```
Processor  64E822C0  101178688  24016328    77162360  75584536   75588172

      I/O  EAF00000   17825792   5421744    12404048  12363136   1238780
```

After TT Issues Are Introduced

```
R3#show memory statistics
             Head     Total(b)   Used(b)     Free(b)    Lowest(b)  Largest(b)

Processor   64E822C0 101178688  24085092    77093596    75584536    75579176

      I/O   EAF00000  17825792   5421744    12404048    12363136    1238780
```

Step 4: Generate loads on R3 using the TTCP utility.

To initiate a TTCP connection and generate test traffic from switch ALS1 at the branch office to switch DLS2 at headquarters, use the following procedure.

a. On switch DLS2 (receiver), enter the command sequence.

```
DLS2#ttcp
transmit or receive [receive]:
receive packets asynchronously [n]:
perform tcp half close [n]:
receive buflen [32768]:
bufalign [16384]:
bufoffset [0]:
port [5001]:
sinkmode [y]:
rcvwndsize [32768]:
ack frequency [0]:
delayed ACK [y]:
show tcp information at end [n]:

ttcp-r: buflen=32768, align=16384/0, port=5001
rcvwndsize=32768, delayedack=yes  tcp
```

b. On switch ALS1 (transmitter), enter the command sequence:

```
ALS1#ttcp
transmit or receive [receive]: transmit
Target IP address: 10.1.100.253
calculate checksum during buffer write [y]:
perform tcp half close [n]:
send buflen [32768]:
send nbuf [2048]:
bufalign [16384]:
bufoffset [0]:
port [5001]:
sinkmode [y]:
buffering on writes [y]:
show tcp information at end [n]:

ttcp-t: buflen=32768, nbuf=2048, align=16384/0, port=5001  tcp  ->
10.1.100.253
ttcp-t: connect

ttcp-t: 67108864 bytes in 68434 ms (68.434 real seconds) (~957 kB/s)
+++
```



```
ttcp-t: 2048 I/O calls
ttcp-t: 0 sleeps (0 ms total) (0 ms average)
```

c. Record the time required to complete the TTCP data transfer.

____

Note: Referring to the above results, the TTCP utility transmitted over 67 million bytes in approximately 68 seconds. This is comparable to the baseline performance, which indicates that this router is not significantly loaded. Different devices and network links will produce different results.

Step 5: Test R3 with load applied.

Note: In this lab, the TCP utility creates a load that lasts for about 60–120 seconds. The actual length of time depends on the capabilities of the devices and links in use.

Use Cisco IOS commands and pings to record the router performance figures simulating a condition in which large file transfers are currently being transmitted. These results can be compared to the baseline output (selected baseline information is shown) and the output obtained when using the TTCP utility.

a. Ping from PC-B to R2 Lo1 and record the results.

____

Include the minimum, maximum, and average round-trip times. The times should be about the same as without the TTCP load on R3.

```
C:\>ping 172.20.0.1

Pinging 172.20.0.1 with 32 bytes of data:
Reply from 172.20.0.1 : bytes=32 time=12ms TTL=64
Reply from 172.20.0.1 : bytes=32 time=11ms TTL=64
Reply from 172.20.0.1 : bytes=32 time=11ms TTL=64
Reply from 172.20.0.1 : bytes=32 time=11ms TTL=64

Ping statistics for 172.20.0.1 :
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 12ms, Average = 11ms
```

b. While TTCP is transferring data, issue the **`show processes cpu sorted`** command on R3 and note the CPU utilization for five seconds, one minute, and five minutes

____

```
R3#show processes cpu sorted
CPU utilization for five seconds: 10%/9%; one minute: 2%; five minutes: 1%
 PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process

<output omitted>
```

Based on the output above, you can see that R3 is not CPU bound.

c. Issue the **`show processes cpu history`** command on R3 to see the CPU history in graph format. Note the CPU utilization for the last 60 minutes and 72 hours.

```
R3#show processes cpu history

R3   05:46:25 PM Tuesday Dec 1 2009 UTC
```

```
<Output omitted>
                                  4          11
    111111111111111111111111111111911111111111011111111111111111
100
 90
 80
 70
 60
 50                               *
 40                               *
 30                               *
 20                               *
 10                               *          *#
   0....5....1....1....2....2....3....3....4....4....5....5....6
             0    5    0    5    0    5    0    5    0    5    0
               CPU% per minute (last 60 minutes)
              * = maximum CPU%   # = average CPU%


    35344351
    15251910
100
 90
 80
 70
 60  *
 50  * *  *
 40  * ****
 30 *******
 20 *******
 10 ********
   0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
             0    5    0    5    0    5    0    5    0    5    0    5    0
                   CPU% per hour (last 72 hours)
                  * = maximum CPU%   # = average CPU%
```

As with the output for the **show processes cpu sorted** command, you can see that R3 is not CPU bound.

d. Issue the **show memory statistics** command on R3. Note the amount of used and free memory for the processor. By comparing the amount of memory used to the baseline and the TT issues, you can determine how much is used when running the TTCP utility. The memory amounts for the baseline after the TT was loaded and while TTCP was running are shown here for comparison.

   Note: The trouble ticket issues cause an increase of nearly 70 KB of memory over the baseline. This is not enough to cause real memory depletion issues with the router but serves to illustrate the type of problem that can occur in a production environment. Running the TTCP load utility caused an increase of about 7 KB over the TT issues.

Baseline

```
R3#show memory statistics
             Head    Total(b)   Used(b)     Free(b)   Lowest(b)  Largest(b)

Processor  64E822C0  101178688  24016328    77162360  75584536   75588172

      I/O  EAF00000   17825792   5421744    12404048  12363136   1238780
```


After TT Issues Are Introduced

```
R3#show memory statistics
                Head    Total(b)     Used(b)     Free(b)   Lowest(b)  Largest(b)

Processor    64E822C0 101178688   24085092    77093596    75584536    75579176

      I/O    EAF00000  17825792    5421744    12404048    12363136    1238780
```

While Running TTCP

```
R3#show memory statistics
                Head    Total(b)     Used(b)     Free(b)   Lowest(b)  Largest(b)

Processor    64E822C0 101178688   24092388    77086300   75584536    75579176

      I/O    EAF00000  17825792    5424292    12401500   12363136    1238780
```

Step 6: Outline the troubleshooting approach and validation steps.

The following approach is recommended as a troubleshooting process:

1. Generate test traffic using the **`ping`** and **`ttcp`** commands, as described in this task.
2. Use **`ping`** to measure the performance between the headquarters and Internet or network servers. For example, ping from client PC-B to server SRV1, R1 or R2.
3. Examine the key performance indicators, such as the interfaces, CPU, and memory, on the routers and watch for symptoms associated with performance problems.
4. Examine the routers for features and configurations that deviate from the baseline configurations and attempt to find the root cause of the problems.
5. Address the issues causing the performance problems and test to verify that performance has improved.

Step 7: Record the troubleshooting process and configuration changes.

Use this log to document your actions and results during the troubleshooting process. List the commands you used to gather information. As you progress, record what you think the problem might be and which actions you will take to correct the problem.

Device	Actions and Results

Device	Actions and Results

Responses will vary but could include:

- Pings from PC-B to SRV1 indicate that the minimum, average, and maximum times are in a normal range.
- Actual improvements might be slight because of the high amount of memory available in the routers used and the lack of actual network traffic being passed.

TT-B Issue

Router R2 advertises over 100 prefixes to R1 via BGP. R1 then redistributes these routes to the other network devices via EIGRP. This results in excessive memory use on all network devices.

- Pings from PC-B to R2 Lo1 take longer than normal.
- Traceroute from PC-B to R2 Lo1 takes the expected route with consistent delay.
- The **`show processes cpu sorted`** command on R3 indicates that the CPU is not heavily loaded.
- The **`show memory statistics`** command on R3 indicates that there is sufficient memory free, but memory usage is significantly increased over the baseline.
- The **`show interfaces fa0/0 stats`** command on R3 indicates that the switching path being used is the more efficient route cache (Cisco Express Forwarding).
- The **`show ip route`** command on R3 shows a very large number of external routes to the partner 172.20.0.x networks, learned via EIGRP.
- The **`show ip route`** command on R1 shows the same large number of external routes to the partner 172.20.0.x networks, learned via BGP.
- The **`show ip protocols`** command on R1 indicates that R1 is redistributing BGP routes.
- The **`show ip bgp`** command on R2 indicates that R2 is injecting over 100 individual specific prefixes into the BGP process, which are picked up by BGP peer R1 and redistributed into the EIGRP domain.

Action: Configure an aggregate address on R2 that consolidates all the individual prefixes before sending them to R1. See the TT-B debrief for additional information.

Verification:

- Ping times improve slightly.
- Memory usage on R3 and other EIGRP devices decreases.

Step 8: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with your instructor. This can include problems encountered, solutions applied, useful commands employed, alternate solutions, methods, and processes, and procedure and communication improvements.

____

____

____

____

____

____

____

Trouble Ticket TT-B Debrief—Instructor Notes

TT-B Issue

This trouble ticket revolves around memory exhaustion on routers R1 and R3 and Layer 3 switches DLS1 and DLS2 caused by an inappropriate BGP configuration on R2. The memory exhaustion problems on R1 and R3 and the Layer 3 switches are caused by the large number of BGP prefixes sent to these routers. The most straightforward method to address this is to configure BGP route aggregation on router R2 for the 172.20.0.0/21 address block. To suppress the advertisement of all the more-specific prefixes, use the **`summary-only`** command option.

Note: Issue the **`show ip route`** command on R1 and R3 before and after correcting the TT-B problem on R2 to see the decrease in the number of routes in the routing table.

Issue the following commands on router R2:

```
router bgp 65502
 aggregate-address 172.20.0.0 255.255.248.0 summary-only
```

As an alternative you can also configure a prefix list or route map on router R1 to drop all prefixes, except for the major block as the updates are received. However, this is considered to be less efficient, because it still causes the updates to be sent to the router, even though they are discarded immediately after they are received.

Memory exhaustion issues involving BGP are quite common in production devices. A full Internet BGP routing table includes over 300,000 prefixes. Refer to the BGP routing table growth graph at the following URL: http://bgp.potaroo.net/

Section 2—Troubleshooting Reference Information

General Troubleshooting Process

As a general guideline, you can use the following general troubleshooting process described in the course.

1. Define the problem (symptoms).
2. Gather information.
3. Analyze the information.
4. Propose a hypothesis (possible cause).
5. Test the hypothesis.
6. Eliminate or accept the hypothesis.
7. Solve the problem.
8. Document the problem.

Command Summary

The table lists useful commands for this lab. The sample output is shown on following pages.

Command	Key Information Displayed
show interfaces *type/#*	Displays the interface IP address, subnet mask, MAC address, and load statistics.
show interfaces *type/# summary*	Displays a summary of input and output queues and packet transmit and receive rates.
show interfaces *type/#* **stats**	Displays the switching path and the number of characters or packets in and out for the processor and route cache (Cisco Express Forwarding).
show ip interface *type/#*	Displays primarily IP-related information for the interface, such as the helper address, multicast groups, and route cache processing status.
clear counters *type/#*	Clears the interface counters on an interface.
show processes cpu sorted	Displays short-term CPU utilization (five seconds, one minute, and five minutes). It also lists the currently running processes, sorted by the most CPU utilization to the least.
show processes cpu history	Displays long-term CPU utilization in a graph format for the last 60 seconds, 60 minutes, and 72 hours. Useful for analyzing CPU load over time.
show processes memory sorted	Displays memory CPU utilization (used and free) for the processor and I/O memory pools. The entries are sorted by the highest amount of holding memory used.
show memory statistics	Displays a summary of memory utilization (total, used, and free) for the processor and I/O memory pools. The lowest is the smallest amount of free memory since the last boot. The largest is the size of the largest available free block.
show ip cef	Displays all known prefix entries in the Cisco Express Forwarding Forwarding Information Base (FIB). The prefix, next-hop IP address, and the exit interface are shown. If

	Cisco Express Forwarding is not enabled, the output states this.

Display Interface Load, Statistics, and Forwarding Information

```
R3#show interfaces fastethernet 0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is Gt96k FE, address is 001b.530d.6028 (bia 001b.530d.6028)
  Internet address is 10.1.80.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 2/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 913000 bits/sec, 179 packets/sec
  5 minute output rate 62000 bits/sec, 175 packets/sec
     381659 packets input, 222009886 bytes
     Received 257 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     377267 packets output, 20429223 bytes, 0 underruns
     0 output errors, 0 collisions, 3 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

The output of the **show interfaces fastethernet 0/0** command above shows the IP address and mask, hardware (MAC) address, as well as the reliability, transmit (txload), receive (rxload), and details on packet input and output rates. The **summary** option shown below provides a quick view of input and output queues and bit per packet transmit and receive rates. As can be seen, there are no packets in the input and output queues.

```
R3#show interfaces fa0/0 summary

 *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count

  Interface              IHQ   IQD  OHQ   OQD  RXBS RXPS   TXBS TXPS TRTL
-------------------------------------------------------------------------
* FastEthernet0/0          0     0    0     0 969000   204 94000   201    0
```

```
R3#show interfaces fa0/0 stats
      FastEthernet0/0
```



```
                    Switching path    Pkts In   Chars In   Pkts Out  Chars Out
                         Processor        831     356623       4075     408723
                       Route cache     381399  221941950     375270   20282949
                             Total     382230  222298573     379345   20691672
```

The **stats** option shown above displays the switching path and the number of characters and packets in and out for processor and route cache (Cisco Express Forwarding). As can be seen, only a few packets have been process-switched and a very large number have been switched via the route cache (with Cisco Express Forwarding enabled).

```
R3#show ip interface fastethernet 0/0
FastEthernet0/0 is up, line protocol is up
  Internet address is 10.1.80.1/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is 10.1.2.13
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  Input features: Ingress-NetFlow, MCI Check
  Output features: Post-Ingress-NetFlow
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
```

The output from the **show ip interface fastethernet 0/0** command above shows primarily IP-related information for the interface. Note the helper address pointing to the switch DLS2 DHCP server IP address. This router interface has joined multicast group 224.0.0.10 for communication between EIGRP routers. Also note that Cisco Express Forwarding is enabled.

```
R1#show ip cef
```



```
Prefix              Next Hop             Interface
0.0.0.0/0           209.165.200.226      Serial0/0/0
0.0.0.0/8           drop
0.0.0.0/32          receive
10.1.2.0/30         attached             FastEthernet0/1
10.1.2.0/32         receive              FastEthernet0/1
10.1.2.1/32         attached             FastEthernet0/1
10.1.2.2/32         receive              FastEthernet0/1
10.1.2.3/32         receive              FastEthernet0/1
10.1.2.12/30        10.1.2.1             FastEthernet0/1
10.1.10.0/24        10.1.2.1             FastEthernet0/1
10.1.20.0/24        10.1.2.1             FastEthernet0/1
10.1.30.0/24        10.1.2.1             FastEthernet0/1
10.1.50.0/24        10.1.2.1             FastEthernet0/1
10.1.80.0/24        10.1.2.1             FastEthernet0/1
10.1.100.0/24       10.1.2.1             FastEthernet0/1
10.1.200.0/24       10.1.2.1             FastEthernet0/1
10.1.203.1/32       10.1.2.1             FastEthernet0/1
127.0.0.0/8         drop
172.20.0.0/21       209.165.200.226      Serial0/0/0
192.168.1.0/24      attached             Loopback0
192.168.1.0/32      receive              Loopback0
Prefix              Next Hop             Interface
192.168.1.1/32      receive              Loopback0
192.168.1.255/32    receive              Loopback0
192.168.2.1/32      209.165.200.226      Serial0/0/0
209.165.200.224/30  attached             Serial0/0/0
209.165.200.224/32  receive              Serial0/0/0
209.165.200.225/32  receive              Serial0/0/0
209.165.200.226/32  attached             Serial0/0/0
209.165.200.227/32  receive              Serial0/0/0
224.0.0.0/4         drop
224.0.0.0/24        receive
240.0.0.0/4         drop
255.255.255.255/32  receive
```

The output from the **show ip cef** command above shows all the known prefix entries in the Cisco Express Forwarding FIB. The prefix, next-hop IP address, and the exit interface are shown. If Cisco Express Forwarding is not enabled, the output states this.

Display CPU Load and Process Statistics

```
R3#show processes cpu sorted
CPU utilization for five seconds: 17%/5%; one minute: 3%; five minutes: 1%
 PID Runtime(ms)   Invoked  uSecs    5Sec   1Min   5Min TTY Process
  91        2308      4797    481 11.19%  2.10%  0.52%   0 IP Input

   3       13308      2477   5372  0.87%  0.18%  0.05%   0 Exec

 124          12       265     45  0.15%  0.03%  0.00%   0 TCP Timer

 153          20     93423      0  0.15%  0.12%  0.10%   0 HQF Shaper Backg

265         1280     11572    110  0.07%  0.01%  0.00%   0 IP-EIGRP: HELLO
<output omitted>
```

The output from the **`show processes cpu sorted`** command above shows short-term CPU utilization for the last five seconds, one minute, and five minutes. It also lists the currently running processes, sorted by the most CPU utilization to the least. This router CPU is not heavily loaded at this time (not CPU bound).

```
R3#show processes cpu history

R3   07:54:09 PM Monday Nov 30 2009 UTC


    999988888
    99999999922222                      11111
100 ****
 90 *********
 80 *********
 70 *********
 60 *********
 50 *********
 40 *********
 30 *********
 20 *********
 10 *********
   0....5....1....1....2....2....3....3....4....4....5....5....6
             0    5    0    5    0    5    0    5    0    5    0
               CPU% per second (last 60 seconds)


            992                                       3
    111111119981111121111111211111111112111111211111113111111111
100         *#
 90         *#
 80         ##
 70         ##
 60         ##
 50         ##
 40         ##
 30         ##*                                       *
 20         ##*                                       *
 10         ##*                                       *
   0....5....1....1....2....2....3....3....4....4....5....5....6
             0    5    0    5    0    5    0    5    0    5    0
               CPU% per minute (last 60 minutes)
              * = maximum CPU%   # = average CPU%


    99
    99
100 **
 90 **
 80 **
 70 **
 60 **
 50 **
 40 **
 30 **
 20 **
 10 **
   0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
```

```
             0    5    0    5    0    5    0    5    0    5    0    5    0
                   CPU% per hour (last 72 hours)
                  * = maximum CPU%   # = average CPU%
```

The output from the **show processes cpu history** command above shows long-term CPU utilization in a graph format for the last 60 seconds, 60 minutes, and 72 hours. This router CPU has been recently heavily loaded and is CPU bound at 99% utilization. Percent CPU utilization can hit 90% occasionally, but consistently high utilization over time can point to processing problems, such as access lists and large file transfers.

Display Memory Usage and Process Statistics

```
R3#show processes memory sorted
Processor Pool Total:  101226944 Used:   24015448 Free:   77211496
      I/O Pool Total:   17825792 Used:    5446544 Free:   12379248

 PID TTY  Allocated      Freed    Holding    Getbufs    Retbufs Process
   0   0   62860036   36235836   23615956          0          0 *Init*

  55   0     659528       1328     640200          0          0 USB Startup

   1   0     466000          0     473204          0          0 Chunk Manager

 219   0     469124      18304     436776          0          0 VLAN Manager

   0   0          0          0     420380          0          0 *MallocLite*

  25   0     260308          0     270512      99792          0 EEM ED Syslog

 170   0     218420        504     215916          0          0 Crypto HW Proc

 221   0     196192          0     203396          0          0 EEM Server

 183   0     114384        528     123060          0          0 Crypto WUI

 167   0      76544        252      83496          0          0 HTTP Process

  40   0      66536     153420      73340          0          0 IF-MGR control p

   3   0    7352228    7237092      66908          0          0 Exec

<output omitted>
```

The output from the **show processes memory sorted** command above shows memory utilization (used and free) for the processor and I/O memory pools. The holding amount is the amount of memory that the process is currently using. The entries are sorted by the highest amount of holding memory first.

```
R3#show processes memory sorted | include EIGRP
 265   0    1676448    7910464      24464          0          0 IP-EIGRP: PDM

 264   0          0          0      18200          0          0 IP-EIGRP Router

 266   0   19720032   13337320       7116          0          0 IP-EIGRP: HELLO
```

The list of processes output from this command can be lengthy. Use the pipe (|), as shown above, to filter the output and focus on specific processes. Search strings are case-sensitive.


```
R3#show memory statistics
                Head    Total(b)     Used(b)     Free(b)   Lowest(b)  Largest(b)

Processor   64E76640   101226944    23964420    77262524    76880040    76910312

      I/O   EAF00000    17825792     5421732    12404060    12376432    1240031
```

The output from the **show memory statistics** command above shows a summary of memory utilization (total, used, and free) for the processor and I/O memory pools. The lowest column is the smallest amount of free memory since the last boot. The largest column shows the size of the largest available free block.

Reflection Questions

1. Which lab trouble tickets did you have the most difficulty with?

____
____
____

2. Would you change anything about the process that you used for any of the trouble tickets now that you see the resolution of the problem?

____
____
____

3. Which commands did you find most useful in diagnosing router performance issues? Add these to your toolbox for future use. Which commands did you find least useful?

____
____
____

References

If you need more information on the commands and their options, see the following references:

- IP Routing Protocol Command Reference

  http://www.cisco.com/cisco/web/support/index.html

- Cisco IOS IP Switching Reference
  http://www.cisco.com/en/US/docs/ios/ipswitch/command/reference/isw_book.html

- TTCP information (also see Appendix A)
  http://www.cisco.com/en/US/tech/tk801/tk36/technologies_tech_note09186a0080094694.shtml

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1700	Fast Ethernet 0 (FA0)	Fast Ethernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
1800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2600	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)
2800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. Rather than try to list all the combinations of configurations for each router class, this table includes identifiers for the possible combinations of Ethernet and serial interfaces in the device. The table does not include any other type of interface, even though a specific router might contain one. An example of this is an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

Appendix A—Using a Windows PC as a TTCP End Device

a. Download the TTCP for Windows ttcpw program from the link provided at http://www.cisco.com/en/US/tech/tk801/tk36/technologies_tech_note09186a0080094694.shtml.

b. Expand the ZIP file in a folder to access the .exe and readme files.

c. Start the ttcpw program on the PC (in a DOS window), running as a receiver. Refer to the Readme file provided with the windows TTCP software for the appropriate syntax. An example is provided here.

```
C:\Cisco\TTCP>ttcpw -r -s ttcp-r: buflen=8192, nbuf=2048, align=16364/0,
port=5001 tcp ttcp-r: socket
```

d. Start the ttcp program on DLS2 running as a transmitter and specify the target IP address of the PC.

```
DLS2#ttcp
transmit or receive [receive]: transmit
Target IP address: 10.1.80.254
```



```
calculate checksum during buffer write [y]:
perform tcp half close [n]:
send buflen [32768]:
send nbuf [2048]:
bufalign [16384]:
bufoffset [0]:
port [5001]:
sinkmode [y]:
buffering on writes [y]:
show tcp information at end [n]:
```

e. When the transfer completes, you should see the results on the transmitter and receiver. The following output is from DLS2, the transmitter.

```
ttcp-t: buflen=32768, nbuf=2048, align=16384/0, port=5001  tcp  ->
10.1.80.254
ttcp-t: connect
ttcp-t: 67108864 bytes in 47622 ms (47.622 real seconds) (~1375 kB/s) +++
ttcp-t: 2048 I/O calls
ttcp-t: 0 sleeps (0 ms total) (0 ms average)
```

Device Configurations (instructor version)

Note: All device configurations are provided for TT-A. The configs provided here are *not* running-config outputs. They can be used for copy-and-paste for TT-A and subsequent tickets. Where a config is noted as being the same as a previous one, the only change is in the MOTD, which identifies the Lab and TT. The errors in the configuration are commented and highlighted as red text.

Trouble Ticket - TT-A Configurations

Switch ALS1

```
!Lab 7-1 Switch ALS1 TT-A Config
!
hostname ALS1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55

banner motd $*** Lab 7-1 Switch ALS1 TT-A Config ***$
!
aaa new-model
!
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
```



```
!
aaa session-id common
system mtu routing 1500
vtp domain TSHOOT
vtp mode transparent
ip subnet-zero
!
ip default-gateway 10.1.80.1
!
no ip domain-lookup
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
archive
 log config
  logging size 50
  notify syslog contenttype plaintext
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
spanning-tree portfast default
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan1
ip ssh source-interface Vlan1
!
interface FastEthernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/3
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/4
```



```
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/5
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description to PC-B
 switchport mode access
 switchport nonegotiate
 no shut
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
```



```
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description to R3
 switchport mode access
 spanning-tree portfast
 speed 100
 full-duplex
 no shut
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
```



```
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 ip address 10.1.80.251 255.255.255.0
 no ip route-cache
 no shutdown
!
ip http server
ip http secure-server
logging source-interface Vlan1
logging 10.1.50.1
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan1
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
```



```
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps vlan-membership
snmp-server host 10.1.50.1 version 2c cisco
!
control-plane
!
line con 0
 exec-timeout 60 0
 logging synchronous
 login authentication CONSOLE
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 transport input none
!
ntp clock-period 36032713
ntp source Vlan1
ntp server 192.168.2.1
end
```

Switch DLS1

```
!Lab 7-1 Switch DLS1 TT-A Config
!
hostname DLS1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55

banner motd $*** Lab 7-1 Switch DLS1 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
!
ip domain name tshoot.net
```



```
!
ip dhcp excluded-address 10.1.10.252 10.1.10.254
ip dhcp excluded-address 10.1.20.252 10.1.20.254
ip dhcp excluded-address 10.1.30.252 10.1.30.254
!
ip dhcp pool OFFICE
   network 10.1.10.0 255.255.255.0
   default-router 10.1.10.254
   domain-name tshoot.net
!
ip dhcp pool VOICE
   network 10.1.20.0 255.255.255.0
   default-router 10.1.20.254
   domain-name tshoot.net
!
ip dhcp pool GUEST
   network 10.1.30.0 255.255.255.0
   default-router 10.1.30.254
   domain-name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 24576
spanning-tree vlan 20,50 priority 28672
!
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 100
 name MGMT
!
vlan 200
 name TRANS
!
vlan 900
```



```
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel1
 description Channel to ALS1
 shutdown
!
interface Port-channel10
 description Channel to DLS2
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 shutdown
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 shutdown
!
interface FastEthernet0/3
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R1
```

```
 no switchport
 ip address 10.1.2.1 255.255.255.252
 spanning-tree bpduguard enable
 speed 100
 duplex full
 no shut
!
interface FastEthernet0/6
 description FE to SRV1
 switchport access vlan 50
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shut
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
```

```
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
```



```
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown

interface Vlan10
 ip address 10.1.10.252 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 priority 110
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.252 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.252 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 priority 110
```

```
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.252 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 preempt
!
interface Vlan100
 ip address 10.1.100.252 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 priority 110
 standby 100 preempt
!
interface Vlan200
 ip address 10.1.200.252 255.255.255.0
!
router eigrp 1
 passive-interface default
 no passive-interface Fa0/5
 no passive-interface vlan200
 no auto-summary
 network 10.1.0.0 0.0.255.255
!
ip classless
ip http server
ip http secure-server
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server host 10.1.50.1 version 2c cisco
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 192.168.2.1
```



```
end
```

Switch DLS2

```
!Lab 7-1 Switch DLS2 TT-A Config
!
hostname DLS2
!
service timestamps debug datetime msec
service timestamps log datetime
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 7-1 Switch DLS2 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
  path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 28672
spanning-tree vlan 20,50 priority 24576

vlan 10
 name OFFICE
!
```

```
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 100
 name MGMT
!
vlan 200
 name TRANS
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel2
 description Channel to ALS1
 shutdown

interface Port-channel10
 description Channel to DLS1
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 shutdown
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 shutdown
!
interface FastEthernet0/3
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
```



```
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R3
 no switchport
 ip address 10.1.2.13 255.255.255.252
 speed 100
 duplex full
 no shutdown
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
```



```
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description FE to PC-C
 switchport access vlan 30
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/19
 description Unused
```



```
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
```



```
interface Vlan10
 ip address 10.1.10.253 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.253 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 priority 110
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.253 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.253 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 priority 110
 standby 50 preempt
!
interface Vlan100
 ip address 10.1.100.253 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 preempt
!
interface Vlan200
 ip address 10.1.200.253 255.255.255.0
!
router eigrp 1
 passive-interface default
 no passive-interface Fa0/5
 no passive-interface vlan200
 no auto-summary
 network 10.1.0.0 0.0.255.255
!
ip classless
ip http server
ip http secure-server
!
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
```

```
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 192.168.2.1
end
```

Router R1

```
!Lab 7-1 Router R1 TT-A Config
!
hostname R1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 7-1 Router R1 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
```

```
interface Loopback0
 ip address 192.168.1.1 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown
!
interface FastEthernet0/1
 description FE to DLS1
 ip address 10.1.2.2 255.255.255.252
 ip flow ingress
 ip nat inside
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
 description WAN link to ISP R2
 ip address 209.165.200.225 255.255.255.252
 ip nat outside
 ip flow ingress
 encapsulation ppp
 clock rate 128000
  no shutdown
!
interface Serial0/0/1
 description WAN link to R3 – Not used for this TT
 no ip address
 encapsulation ppp
 clock rate 128000
 shutdown
!
router eigrp 1
 redistribute bgp 65501 metric 1544 2000 255 1 1500
 passive-interface default
 no passive-interface FastEthernet0/1
 network 10.1.2.0 0.0.0.3
 network 192.168.1.1 0.0.0.0
 redistribute static
 no auto-summary
!
router bgp 65501
 no synchronization
 bgp log-neighbor-changes
 neighbor 192.168.2.1 remote-as 65502
 neighbor 192.168.2.1 ebgp-multihop 2
 neighbor 192.168.2.1 update-source Loopback0
 no auto-summary
!
ip route 192.168.2.1 255.255.255.255 209.165.200.226
ip route 0.0.0.0 0.0.0.0 209.165.200.226
!
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
```



```
!
ip nat inside source list 1 interface Serial0/0/0 overload
!
logging source-interface Loopback0
logging 10.1.50.1
!
access-list 1 permit 10.1.0.0 0.0.255.255
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 192.168.2.1
end
```

Router R2

```
!Lab 7-1 Router R2 TT-A Config
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
Hostname R2
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 7-1 Router R2 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
```



```
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 192.168.2.1 255.255.255.255
!
interface FastEthernet0/0
 shutdown
!
interface FastEthernet0/1
 shutdown
!
interface Serial0/0/0
 description WAN link to R1 – T1 leased line
 ip address 209.165.200.226 255.255.255.252
 encapsulation ppp
 no shutdown
!
interface Serial0/0/1
 shutdown
!
router bgp 65502
 no synchronization
 bgp log-neighbor-changes
 neighbor 192.168.1.1 remote-as 65501
 neighbor 192.168.1.1 ebgp-multihop 2
 neighbor 192.168.1.1 update-source Loopback0
 network 192.168.2.1 mask 255.255.255.255
 no auto-summary
!
ip route 192.168.1.1 255.255.255.255 209.165.200.225
!
ip http server
no ip http secure-server
!
logging source-interface Loopback0
logging 10.1.50.1
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 logging synchronous
 login authentication CONSOLE
line vty 0 4
 exec-timeout 60 0
```



```
 transport input telnet ssh
!
ntp master 3
 end
```

Router R3

```
!Lab 7-1 Router R3 TT-A Config
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 7-1 Router R3 TT-A Config ***$
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!

no ip cef
no ip domain lookup
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 10.1.203.1 255.255.255.255
!
interface FastEthernet0/0
 description FE to ALS1
 ip address 10.1.80.1 255.255.255.0
 ip access-group huge-acl in
 ip helper-address 10.1.2.13
 ip flow ingress
 no ip route-cache
```

Error: IP cef is disabled. Reenable it.

ip cef

Errors: Huge-acl is applied to Fa0/0. Remove it. IP route cache is disabled. Reenable it.

```
interface FastEthernet0/0
 no ip access-group huge-acl in
 ip route-cache
```



```
 speed 100
 full-duplex
 no shutdown
!
interface FastEthernet0/1
 description FE to DLS2
 ip address 10.1.2.14 255.255.255.252
 ip flow ingress
 no ip route-cache
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
 description WAN link to R1 – not used
 no ip address
 clock rate 128000
 encapsulation ppp
 shutdown
!
interface Serial0/0/1
 description WAN link to R2 - not used
 no ip address
 encapsulation ppp
 shutdown
!
router eigrp 1
 passive-interface default
 no passive-interface FastEthernet0/1
 network 10.1.80.0 0.0.0.255
 network 10.1.2.12 0.0.0.3
 network 10.1.203.1 0.0.0.0
 no auto-summary
!
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
!
ip access-list standard huge-acl
 permit 10.1.0.0 0.0.0.15 log
 permit 10.1.0.16 0.0.0.15 log
 permit 10.1.0.32 0.0.0.15 log
 permit 10.1.0.48 0.0.0.15 log
 permit 10.1.0.64 0.0.0.15 log
 permit 10.1.0.80 0.0.0.15 log
 permit 10.1.0.96 0.0.0.15 log
 permit 10.1.0.112 0.0.0.15 log
 permit 10.1.0.128 0.0.0.15 log
 permit 10.1.0.144 0.0.0.15 log
 permit 10.1.0.160 0.0.0.15 log
 permit 10.1.0.176 0.0.0.15 log
 permit 10.1.0.192 0.0.0.15 log
 permit 10.1.0.208 0.0.0.15 log
 permit 10.1.0.224 0.0.0.15 log
```

Error: IP route cache is disabled. Reenable it.

```
interface FastEthernet0/0
 ip route-cache
```

Error: Huge-acl is defined here. Remove it from the router.

```
 no ip access-list standard huge-acl
```

```
 permit 10.1.0.240 0.0.0.15 log
 permit 10.1.1.0 0.0.0.15 log
 permit 10.1.1.16 0.0.0.15 log
 permit 10.1.1.32 0.0.0.15 log
 permit 10.1.1.48 0.0.0.15 log
 permit 10.1.1.64 0.0.0.15 log
 permit 10.1.1.80 0.0.0.15 log
 permit 10.1.1.96 0.0.0.15 log
 permit 10.1.1.112 0.0.0.15 log
 permit 10.1.1.128 0.0.0.15 log
 permit 10.1.1.144 0.0.0.15 log
 permit 10.1.1.160 0.0.0.15 log
 permit 10.1.1.176 0.0.0.15 log
 permit 10.1.1.192 0.0.0.15 log
 permit 10.1.1.208 0.0.0.15 log
 permit 10.1.1.224 0.0.0.15 log
 permit 10.1.1.240 0.0.0.15 log
 permit 10.1.2.0 0.0.0.15 log
 permit 10.1.2.16 0.0.0.15 log
 permit 10.1.2.32 0.0.0.15 log
 permit 10.1.2.48 0.0.0.15 log
 permit 10.1.2.64 0.0.0.15 log
 permit 10.1.2.80 0.0.0.15 log
 permit 10.1.2.96 0.0.0.15 log
 permit 10.1.2.112 0.0.0.15 log
 permit 10.1.2.128 0.0.0.15 log
 permit 10.1.2.144 0.0.0.15 log
 permit 10.1.2.160 0.0.0.15 log
 permit 10.1.2.176 0.0.0.15 log
 permit 10.1.2.192 0.0.0.15 log
 permit 10.1.2.208 0.0.0.15 log
 permit 10.1.2.224 0.0.0.15 log
 permit 10.1.2.240 0.0.0.15 log
 permit 10.1.3.0 0.0.0.15 log
 permit 10.1.3.16 0.0.0.15 log
 permit 10.1.3.32 0.0.0.15 log
 permit 10.1.3.48 0.0.0.15 log
 permit 10.1.3.64 0.0.0.15 log
 permit 10.1.3.80 0.0.0.15 log
 permit 10.1.3.96 0.0.0.15 log
 permit 10.1.3.112 0.0.0.15 log
 permit 10.1.3.128 0.0.0.15 log
 permit 10.1.3.144 0.0.0.15 log
 permit 10.1.3.160 0.0.0.15 log
 permit 10.1.3.176 0.0.0.15 log
 permit 10.1.3.192 0.0.0.15 log
 permit 10.1.3.208 0.0.0.15 log
 permit 10.1.3.224 0.0.0.15 log
 permit 10.1.3.240 0.0.0.15 log
 permit 10.1.4.0 0.0.0.15 log
 permit 10.1.4.16 0.0.0.15 log
 permit 10.1.4.32 0.0.0.15 log
 permit 10.1.4.48 0.0.0.15 log
 permit 10.1.4.64 0.0.0.15 log
 permit 10.1.4.80 0.0.0.15 log
 permit 10.1.4.96 0.0.0.15 log
 permit 10.1.4.112 0.0.0.15 log
 permit 10.1.4.128 0.0.0.15 log
```



```
 permit 10.1.4.144 0.0.0.15 log
 permit 10.1.4.160 0.0.0.15 log
 permit 10.1.4.176 0.0.0.15 log
 permit 10.1.4.192 0.0.0.15 log
 permit 10.1.4.208 0.0.0.15 log
 permit 10.1.4.224 0.0.0.15 log
 permit 10.1.4.240 0.0.0.15 log
 permit 10.1.5.0 0.0.0.15 log
 permit 10.1.5.16 0.0.0.15 log
 permit 10.1.5.32 0.0.0.15 log
 permit 10.1.5.48 0.0.0.15 log
 permit 10.1.5.64 0.0.0.15 log
 permit 10.1.5.80 0.0.0.15 log
 permit 10.1.5.96 0.0.0.15 log
 permit 10.1.5.112 0.0.0.15 log
 permit 10.1.5.128 0.0.0.15 log
 permit 10.1.5.144 0.0.0.15 log
 permit 10.1.5.160 0.0.0.15 log
 permit 10.1.5.176 0.0.0.15 log
 permit 10.1.5.192 0.0.0.15 log
 permit 10.1.5.208 0.0.0.15 log
 permit 10.1.5.224 0.0.0.15 log
 permit 10.1.5.240 0.0.0.15 log
 permit 10.1.6.0 0.0.0.15 log
 permit 10.1.6.16 0.0.0.15 log
 permit 10.1.6.32 0.0.0.15 log
 permit 10.1.6.48 0.0.0.15 log
 permit 10.1.6.64 0.0.0.15 log
 permit 10.1.6.80 0.0.0.15 log
 permit 10.1.6.96 0.0.0.15 log
 permit 10.1.6.112 0.0.0.15 log
 permit 10.1.6.128 0.0.0.15 log
 permit 10.1.6.144 0.0.0.15 log
 permit 10.1.6.160 0.0.0.15 log
 permit 10.1.6.176 0.0.0.15 log
 permit 10.1.6.192 0.0.0.15 log
 permit 10.1.6.208 0.0.0.15 log
 permit 10.1.6.224 0.0.0.15 log
 permit 10.1.6.240 0.0.0.15 log
 permit 10.1.7.0 0.0.0.15 log
 permit 10.1.7.16 0.0.0.15 log
 permit 10.1.7.32 0.0.0.15 log
 permit 10.1.7.48 0.0.0.15 log
 permit 10.1.7.64 0.0.0.15 log
 permit 10.1.7.80 0.0.0.15 log
 permit 10.1.7.96 0.0.0.15 log
 permit 10.1.7.112 0.0.0.15 log
 permit 10.1.7.128 0.0.0.15 log
 permit 10.1.7.144 0.0.0.15 log
 permit 10.1.7.160 0.0.0.15 log
 permit 10.1.7.176 0.0.0.15 log
 permit 10.1.7.192 0.0.0.15 log
 permit 10.1.7.208 0.0.0.15 log
 permit 10.1.7.224 0.0.0.15 log
 permit 10.1.7.240 0.0.0.15 log
 permit 10.1.8.0 0.0.0.15 log
 permit 10.1.8.16 0.0.0.15 log
 permit 10.1.8.32 0.0.0.15 log
```



```
 permit 10.1.8.48 0.0.0.15 log
 permit 10.1.8.64 0.0.0.15 log
 permit 10.1.8.80 0.0.0.15 log
 permit 10.1.8.96 0.0.0.15 log
 permit 10.1.8.112 0.0.0.15 log
 permit 10.1.8.128 0.0.0.15 log
 permit 10.1.8.144 0.0.0.15 log
 permit 10.1.9.0 0.0.0.15 log
 permit 10.1.9.16 0.0.0.15 log
 permit 10.1.9.32 0.0.0.15 log
 permit 10.1.9.48 0.0.0.15 log
 permit 10.1.9.64 0.0.0.15 log
 permit 10.1.9.80 0.0.0.15 log
 permit 10.1.9.96 0.0.0.15 log
 permit 10.1.9.112 0.0.0.15 log
 permit 10.1.9.128 0.0.0.15 log
 permit 10.1.9.144 0.0.0.15 log
 permit 10.1.9.160 0.0.0.15 log
 permit 10.1.9.176 0.0.0.15 log
 permit 10.1.9.192 0.0.0.15 log
 permit 10.1.9.208 0.0.0.15 log
 permit 10.1.9.224 0.0.0.15 log
 permit 10.1.9.240 0.0.0.15 log
 permit 10.1.10.0 0.0.0.15 log
 permit 10.1.10.16 0.0.0.15 log
 permit 10.1.10.32 0.0.0.15 log
 permit 10.1.10.48 0.0.0.15 log
 permit 10.1.10.64 0.0.0.15 log
 permit 10.1.10.80 0.0.0.15 log
 permit 10.1.10.96 0.0.0.15 log
 permit 10.1.10.112 0.0.0.15 log
 permit 10.1.10.128 0.0.0.15 log
 permit 10.1.10.144 0.0.0.15 log
 permit 10.1.10.160 0.0.0.15 log
 permit 10.1.10.176 0.0.0.15 log
 permit 10.1.10.192 0.0.0.15 log
 permit 10.1.10.208 0.0.0.15 log
 permit 10.1.10.224 0.0.0.15 log
 permit 10.1.10.240 0.0.0.15 log
 permit 10.1.11.0 0.0.0.15 log
 permit 10.1.11.16 0.0.0.15 log
 permit 10.1.11.32 0.0.0.15 log
 permit 10.1.11.48 0.0.0.15 log
 permit 10.1.11.64 0.0.0.15 log
 permit 10.1.11.80 0.0.0.15 log
 permit 10.1.13.144 0.0.0.15 log
 permit 10.1.13.160 0.0.0.15 log
 permit 10.1.13.176 0.0.0.15 log
 permit 10.1.13.192 0.0.0.15 log
 permit 10.1.13.208 0.0.0.15 log
 permit 10.1.13.224 0.0.0.15 log
 permit 10.1.13.240 0.0.0.15 log
 permit 10.1.14.0 0.0.0.15 log
 permit 10.1.14.16 0.0.0.15 log
 permit 10.1.14.32 0.0.0.15 log
 permit 10.1.14.48 0.0.0.15 log
 permit 10.1.14.64 0.0.0.15 log
 permit 10.1.14.80 0.0.0.15 log
```



```
 permit 10.1.14.96 0.0.0.15 log
 permit 10.1.14.112 0.0.0.15 log
 permit 10.1.14.128 0.0.0.15 log
 permit 10.1.14.144 0.0.0.15 log
 permit 10.1.14.160 0.0.0.15 log
 permit 10.1.14.176 0.0.0.15 log
 permit 10.1.14.192 0.0.0.15 log
 permit 10.1.14.208 0.0.0.15 log
 permit 10.1.14.224 0.0.0.15 log
 permit 10.1.14.240 0.0.0.15 log
 permit 10.1.15.0 0.0.0.15 log
 permit 10.1.15.16 0.0.0.15 log
 permit 10.1.15.32 0.0.0.15 log
 permit 10.1.15.48 0.0.0.15 log
 permit 10.1.15.64 0.0.0.15 log
 permit 10.1.15.80 0.0.0.15 log
 permit 10.1.15.96 0.0.0.15 log
 permit 10.1.15.112 0.0.0.15 log
 permit 10.1.15.128 0.0.0.15 log
 permit 10.1.15.144 0.0.0.15 log
 permit 10.1.15.160 0.0.0.15 log
 permit 10.1.15.176 0.0.0.15 log
 permit 10.1.15.192 0.0.0.15 log
 permit 10.1.18.32 0.0.0.15 log
 permit 10.1.18.48 0.0.0.15 log
 permit 10.1.18.64 0.0.0.15 log
 permit 10.1.18.80 0.0.0.15 log
 permit 10.1.18.96 0.0.0.15 log
 permit 10.1.18.112 0.0.0.15 log
 permit 10.1.18.128 0.0.0.15 log
 permit 10.1.18.144 0.0.0.15 log
 permit 10.1.18.160 0.0.0.15 log
 permit 10.1.18.176 0.0.0.15 log
 permit 10.1.18.192 0.0.0.15 log
 permit 10.1.18.208 0.0.0.15 log
 permit 10.1.18.224 0.0.0.15 log
 permit 10.1.18.240 0.0.0.15 log
 permit 10.1.19.0 0.0.0.15 log
 permit 10.1.19.16 0.0.0.15 log
 permit 10.1.19.32 0.0.0.15 log
 permit 10.1.19.48 0.0.0.15 log
 permit 10.1.19.64 0.0.0.15 log
 permit 10.1.19.80 0.0.0.15 log
 permit 10.1.19.96 0.0.0.15 log
 permit 10.1.19.112 0.0.0.15 log
 permit 10.1.19.128 0.0.0.15 log
 permit 10.1.19.144 0.0.0.15 log
 permit 10.1.19.160 0.0.0.15 log
 permit 10.1.19.176 0.0.0.15 log
 permit 10.1.19.192 0.0.0.15 log
 permit 10.1.19.208 0.0.0.15 log
 permit 10.1.19.224 0.0.0.15 log
 permit 10.1.19.240 0.0.0.15 log
 permit 10.1.20.0 0.0.0.15 log
 permit 10.1.20.16 0.0.0.15 log
 permit 10.1.20.32 0.0.0.15 log
 permit 10.1.20.48 0.0.0.15 log
 permit 10.1.20.64 0.0.0.15 log
```



```
 permit 10.1.20.80 0.0.0.15 log
 permit 10.1.20.96 0.0.0.15 log
 permit 10.1.22.192 0.0.0.15 log
 permit 10.1.22.208 0.0.0.15 log
 permit 10.1.22.224 0.0.0.15 log
 permit 10.1.22.240 0.0.0.15 log
 permit 10.1.23.0 0.0.0.15 log
 permit 10.1.23.16 0.0.0.15 log
 permit 10.1.23.32 0.0.0.15 log
 permit 10.1.23.48 0.0.0.15 log
 permit 10.1.23.64 0.0.0.15 log
 permit 10.1.23.80 0.0.0.15 log
 permit 10.1.23.96 0.0.0.15 log
 permit 10.1.23.112 0.0.0.15 log
 permit 10.1.23.128 0.0.0.15 log
 permit 10.1.23.144 0.0.0.15 log
 permit 10.1.23.160 0.0.0.15 log
 permit 10.1.23.176 0.0.0.15 log
 permit 10.1.23.192 0.0.0.15 log
 permit 10.1.23.208 0.0.0.15 log
 permit 10.1.23.224 0.0.0.15 log
 permit 10.1.23.240 0.0.0.15 log
 permit 10.1.24.0 0.0.0.15 log
 permit 10.1.24.16 0.0.0.15 log
 permit 10.1.24.32 0.0.0.15 log
 permit 10.1.24.48 0.0.0.15 log
 permit 10.1.24.64 0.0.0.15 log
 permit 10.1.24.80 0.0.0.15 log
 permit 10.1.24.96 0.0.0.15 log
 permit 10.1.24.112 0.0.0.15 log
 permit 10.1.24.128 0.0.0.15 log
 permit 10.1.24.144 0.0.0.15 log
 permit 10.1.24.160 0.0.0.15 log
 permit 10.1.24.176 0.0.0.15 log
 permit 10.1.24.192 0.0.0.15 log
 permit 10.1.24.208 0.0.0.15 log
 permit 10.1.24.224 0.0.0.15 log
 permit 10.1.24.240 0.0.0.15 log
 permit 10.1.25.0 0.0.0.15 log
 permit 10.1.27.80 0.0.0.15 log
 permit 10.1.27.96 0.0.0.15 log
 permit 10.1.27.112 0.0.0.15 log
 permit 10.1.27.128 0.0.0.15 log
 permit 10.1.27.144 0.0.0.15 log
 permit 10.1.27.160 0.0.0.15 log
 permit 10.1.27.176 0.0.0.15 log
 permit 10.1.27.192 0.0.0.15 log
 permit 10.1.27.208 0.0.0.15 log
 permit 10.1.27.224 0.0.0.15 log
 permit 10.1.27.240 0.0.0.15 log
 permit 10.1.28.0 0.0.0.15 log
 permit 10.1.28.16 0.0.0.15 log
 permit 10.1.28.32 0.0.0.15 log
 permit 10.1.28.48 0.0.0.15 log
 permit 10.1.28.64 0.0.0.15 log
 permit 10.1.28.80 0.0.0.15 log
 permit 10.1.28.96 0.0.0.15 log
 permit 10.1.28.112 0.0.0.15 log
```

```
 permit 10.1.28.128 0.0.0.15 log
 permit 10.1.28.144 0.0.0.15 log
 permit 10.1.28.160 0.0.0.15 log
 permit 10.1.28.176 0.0.0.15 log
 permit 10.1.28.192 0.0.0.15 log
 permit 10.1.28.208 0.0.0.15 log
 permit 10.1.28.224 0.0.0.15 log
 permit 10.1.28.240 0.0.0.15 log
 permit 10.1.29.0 0.0.0.15 log
 permit 10.1.29.16 0.0.0.15 log
 permit 10.1.29.32 0.0.0.15 log
 permit 10.1.29.48 0.0.0.15 log
 permit 10.1.29.64 0.0.0.15 log
 permit 10.1.29.80 0.0.0.15 log
 permit 10.1.29.96 0.0.0.15 log
 permit 10.1.29.112 0.0.0.15 log
 permit 10.1.29.128 0.0.0.15 log
 permit 10.1.31.224 0.0.0.15 log
 permit 10.1.31.240 0.0.0.15 log
 permit 10.1.32.0 0.0.0.15 log
 permit 10.1.32.16 0.0.0.15 log
 permit 10.1.32.32 0.0.0.15 log
 permit 10.1.32.48 0.0.0.15 log
 permit 10.1.32.64 0.0.0.15 log
 permit 10.1.32.80 0.0.0.15 log
 permit 10.1.32.96 0.0.0.15 log
 permit 10.1.32.112 0.0.0.15 log
 permit 10.1.32.128 0.0.0.15 log
 permit 10.1.32.144 0.0.0.15 log
 permit 10.1.32.160 0.0.0.15 log
 permit 10.1.32.176 0.0.0.15 log
 permit 10.1.32.192 0.0.0.15 log
 permit 10.1.32.208 0.0.0.15 log
 permit 10.1.32.224 0.0.0.15 log
 permit 10.1.32.240 0.0.0.15 log
 permit 10.1.33.0 0.0.0.15 log
 permit 10.1.33.16 0.0.0.15 log
 permit 10.1.33.32 0.0.0.15 log
 permit 10.1.33.48 0.0.0.15 log
 permit 10.1.33.64 0.0.0.15 log
 permit 10.1.33.80 0.0.0.15 log
 permit 10.1.33.96 0.0.0.15 log
 permit 10.1.33.112 0.0.0.15 log
 permit 10.1.33.128 0.0.0.15 log
 permit 10.1.33.144 0.0.0.15 log
 permit 10.1.33.160 0.0.0.15 log
 permit 10.1.33.176 0.0.0.15 log
 permit 10.1.33.192 0.0.0.15 log
 permit 10.1.33.208 0.0.0.15 log
 permit 10.1.33.224 0.0.0.15 log
 permit 10.1.33.240 0.0.0.15 log
 permit 10.1.34.0 0.0.0.15 log
 permit 10.1.34.16 0.0.0.15 log
 permit 10.1.36.112 0.0.0.15 log
 permit 10.1.36.128 0.0.0.15 log
 permit 10.1.36.144 0.0.0.15 log
 permit 10.1.36.160 0.0.0.15 log
 permit 10.1.36.176 0.0.0.15 log
```



```
 permit 10.1.36.192 0.0.0.15 log
 permit 10.1.36.208 0.0.0.15 log
 permit 10.1.36.224 0.0.0.15 log
 permit 10.1.36.240 0.0.0.15 log
 permit 10.1.37.0 0.0.0.15 log
 permit 10.1.37.16 0.0.0.15 log
 permit 10.1.37.32 0.0.0.15 log
 permit 10.1.37.48 0.0.0.15 log
 permit 10.1.37.64 0.0.0.15 log
 permit 10.1.37.80 0.0.0.15 log
 permit 10.1.37.96 0.0.0.15 log
 permit 10.1.37.112 0.0.0.15 log
 permit 10.1.37.128 0.0.0.15 log
 permit 10.1.37.144 0.0.0.15 log
 permit 10.1.37.160 0.0.0.15 log
 permit 10.1.37.176 0.0.0.15 log
 permit 10.1.37.192 0.0.0.15 log
 permit 10.1.37.208 0.0.0.15 log
 permit 10.1.37.224 0.0.0.15 log
 permit 10.1.37.240 0.0.0.15 log
 permit 10.1.38.0 0.0.0.15 log
 permit 10.1.38.16 0.0.0.15 log
 permit 10.1.38.32 0.0.0.15 log
 permit 10.1.38.48 0.0.0.15 log
 permit 10.1.38.64 0.0.0.15 log
 permit 10.1.38.80 0.0.0.15 log
 permit 10.1.38.96 0.0.0.15 log
 permit 10.1.38.112 0.0.0.15 log
 permit 10.1.38.128 0.0.0.15 log
 permit 10.1.38.144 0.0.0.15 log
 permit 10.1.38.160 0.0.0.15 log
 permit 10.1.38.176 0.0.0.15 log
 permit 10.1.41.16 0.0.0.15 log
 permit 10.1.41.32 0.0.0.15 log
 permit 10.1.41.48 0.0.0.15 log
 permit 10.1.41.64 0.0.0.15 log
 permit 10.1.41.80 0.0.0.15 log
 permit 10.1.41.96 0.0.0.15 log
 permit 10.1.41.112 0.0.0.15 log
 permit 10.1.41.128 0.0.0.15 log
 permit 10.1.41.144 0.0.0.15 log
 permit 10.1.41.160 0.0.0.15 log
 permit 10.1.41.176 0.0.0.15 log
 permit 10.1.41.192 0.0.0.15 log
 permit 10.1.41.208 0.0.0.15 log
 permit 10.1.41.224 0.0.0.15 log
 permit 10.1.41.240 0.0.0.15 log
 permit 10.1.42.0 0.0.0.15 log
 permit 10.1.42.16 0.0.0.15 log
 permit 10.1.42.32 0.0.0.15 log
 permit 10.1.42.48 0.0.0.15 log
 permit 10.1.42.64 0.0.0.15 log
 permit 10.1.42.80 0.0.0.15 log
 permit 10.1.42.96 0.0.0.15 log
 permit 10.1.42.112 0.0.0.15 log
 permit 10.1.42.128 0.0.0.15 log
 permit 10.1.42.144 0.0.0.15 log
 permit 10.1.42.160 0.0.0.15 log
```

```
 permit 10.1.42.176 0.0.0.15 log
 permit 10.1.42.192 0.0.0.15 log
 permit 10.1.42.208 0.0.0.15 log
 permit 10.1.42.224 0.0.0.15 log
 permit 10.1.42.240 0.0.0.15 log
 permit 10.1.43.0 0.0.0.15 log
 permit 10.1.43.16 0.0.0.15 log
 permit 10.1.43.32 0.0.0.15 log
 permit 10.1.43.48 0.0.0.15 log
 permit 10.1.43.64 0.0.0.15 log
 permit 10.1.45.160 0.0.0.15 log
 permit 10.1.45.176 0.0.0.15 log
 permit 10.1.45.192 0.0.0.15 log
 permit 10.1.45.208 0.0.0.15 log
 permit 10.1.45.224 0.0.0.15 log
 permit 10.1.45.240 0.0.0.15 log
 permit 10.1.46.0 0.0.0.15 log
 permit 10.1.46.16 0.0.0.15 log
 permit 10.1.46.32 0.0.0.15 log
 permit 10.1.46.48 0.0.0.15 log
 permit 10.1.46.64 0.0.0.15 log
 permit 10.1.46.80 0.0.0.15 log
 permit 10.1.46.96 0.0.0.15 log
 permit 10.1.46.112 0.0.0.15 log
 permit 10.1.46.128 0.0.0.15 log
 permit 10.1.46.144 0.0.0.15 log
 permit 10.1.46.160 0.0.0.15 log
 permit 10.1.46.176 0.0.0.15 log
 permit 10.1.46.192 0.0.0.15 log
 permit 10.1.46.208 0.0.0.15 log
 permit 10.1.46.224 0.0.0.15 log
 permit 10.1.46.240 0.0.0.15 log
 permit 10.1.47.0 0.0.0.15 log
 permit 10.1.47.16 0.0.0.15 log
 permit 10.1.47.32 0.0.0.15 log
 permit 10.1.47.48 0.0.0.15 log
 permit 10.1.47.64 0.0.0.15 log
 permit 10.1.47.80 0.0.0.15 log
 permit 10.1.47.96 0.0.0.15 log
 permit 10.1.47.112 0.0.0.15 log
 permit 10.1.47.128 0.0.0.15 log
 permit 10.1.47.144 0.0.0.15 log
 permit 10.1.47.160 0.0.0.15 log
 permit 10.1.47.176 0.0.0.15 log
 permit 10.1.47.192 0.0.0.15 log
 permit 10.1.47.208 0.0.0.15 log
 permit 10.1.47.224 0.0.0.15 log
 permit 10.1.50.48 0.0.0.15 log
 permit 10.1.50.64 0.0.0.15 log
 permit 10.1.50.80 0.0.0.15 log
 permit 10.1.50.96 0.0.0.15 log
 permit 10.1.50.112 0.0.0.15 log
 permit 10.1.50.128 0.0.0.15 log
 permit 10.1.50.144 0.0.0.15 log
 permit 10.1.50.160 0.0.0.15 log
 permit 10.1.50.176 0.0.0.15 log
 permit 10.1.50.192 0.0.0.15 log
 permit 10.1.50.208 0.0.0.15 log
```



```
permit 10.1.50.224 0.0.0.15 log
permit 10.1.50.240 0.0.0.15 log
permit 10.1.51.0 0.0.0.15 log
permit 10.1.51.16 0.0.0.15 log
permit 10.1.51.32 0.0.0.15 log
permit 10.1.51.48 0.0.0.15 log
permit 10.1.51.64 0.0.0.15 log
permit 10.1.51.80 0.0.0.15 log
permit 10.1.51.96 0.0.0.15 log
permit 10.1.51.112 0.0.0.15 log
permit 10.1.51.128 0.0.0.15 log
permit 10.1.51.144 0.0.0.15 log
permit 10.1.51.160 0.0.0.15 log
permit 10.1.51.176 0.0.0.15 log
permit 10.1.51.192 0.0.0.15 log
permit 10.1.51.208 0.0.0.15 log
permit 10.1.51.224 0.0.0.15 log
permit 10.1.51.240 0.0.0.15 log
permit 10.1.52.0 0.0.0.15 log
permit 10.1.52.16 0.0.0.15 log
permit 10.1.52.32 0.0.0.15 log
permit 10.1.52.48 0.0.0.15 log
permit 10.1.52.64 0.0.0.15 log
permit 10.1.52.80 0.0.0.15 log
permit 10.1.52.96 0.0.0.15 log
permit 10.1.54.192 0.0.0.15 log
permit 10.1.54.208 0.0.0.15 log
permit 10.1.54.224 0.0.0.15 log
permit 10.1.54.240 0.0.0.15 log
permit 10.1.55.0 0.0.0.15 log
permit 10.1.55.16 0.0.0.15 log
permit 10.1.55.32 0.0.0.15 log
permit 10.1.55.48 0.0.0.15 log
permit 10.1.55.64 0.0.0.15 log
permit 10.1.55.80 0.0.0.15 log
permit 10.1.55.96 0.0.0.15 log
permit 10.1.55.112 0.0.0.15 log
permit 10.1.55.128 0.0.0.15 log
permit 10.1.55.144 0.0.0.15 log
permit 10.1.55.160 0.0.0.15 log
permit 10.1.55.176 0.0.0.15 log
permit 10.1.55.192 0.0.0.15 log
permit 10.1.55.208 0.0.0.15 log
permit 10.1.55.224 0.0.0.15 log
permit 10.1.55.240 0.0.0.15 log
permit 10.1.56.0 0.0.0.15 log
permit 10.1.56.16 0.0.0.15 log
permit 10.1.56.32 0.0.0.15 log
permit 10.1.56.48 0.0.0.15 log
permit 10.1.56.64 0.0.0.15 log
permit 10.1.56.80 0.0.0.15 log
permit 10.1.56.96 0.0.0.15 log
permit 10.1.56.112 0.0.0.15 log
permit 10.1.56.128 0.0.0.15 log
permit 10.1.56.144 0.0.0.15 log
permit 10.1.56.160 0.0.0.15 log
permit 10.1.56.176 0.0.0.15 log
permit 10.1.56.192 0.0.0.15 log
```



```
 permit 10.1.56.208 0.0.0.15 log
 permit 10.1.56.224 0.0.0.15 log
 permit 10.1.59.80 0.0.0.15 log
 permit 10.1.59.96 0.0.0.15 log
 permit 10.1.59.112 0.0.0.15 log
 permit 10.1.59.128 0.0.0.15 log
 permit 10.1.59.144 0.0.0.15 log
 permit 10.1.59.160 0.0.0.15 log
 permit 10.1.59.176 0.0.0.15 log
 permit 10.1.59.192 0.0.0.15 log
 permit 10.1.59.208 0.0.0.15 log
 permit 10.1.59.224 0.0.0.15 log
 permit 10.1.59.240 0.0.0.15 log
 permit any log
!
logging source-interface Loopback0
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 logging synchronous
 login authentication CONSOLE
line vty 0 4
 exec-timeout 60 0
transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 192.168.2.1
end
```

Trouble Ticket - TT-B Configs

Switch ALS1—Same as TT-A

Switch DLS1—Same as TT-A

Switch DLS2—Same as TT-A

Router R1— Same as TT-A

Router R2

```
!Lab 7-1 Router R2 TT-A Config
!
```

```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
Hostname R2
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 7-1 Router R2 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 192.168.2.1 255.255.255.255
 no shut
!
interface Loopback1
 ip address 172.20.0.1 255.255.255.240
 no shut
!
interface FastEthernet0/0
 no ip address
 shutdown
!
interface FastEthernet0/1
 shutdown
!
interface Serial0/0/0
 description WAN link to R1 – T1 leased line
 ip address 209.165.200.226 255.255.255.252
 encapsulation ppp
 no shutdown

!
interface Serial0/0/1
 shutdown
!
router bgp 65502
 no synchronization
 bgp log-neighbor-changes
 neighbor 192.168.1.1 remote-as 65501
 neighbor 192.168.1.1 ebgp-multihop 2
```



```
 neighbor 192.168.1.1 update-source Loopback0
 no auto-summary
 network 192.168.2.1 mask 255.255.255.255
!
 network 172.20.0.0 mask 255.255.255.240
 network 172.20.0.16 mask 255.255.255.240
 network 172.20.0.32 mask 255.255.255.240
 network 172.20.0.48 mask 255.255.255.240
 network 172.20.0.64 mask 255.255.255.240
 network 172.20.0.80 mask 255.255.255.240
 network 172.20.0.96 mask 255.255.255.240
 network 172.20.0.112 mask 255.255.255.240
 network 172.20.0.128 mask 255.255.255.240
 network 172.20.0.144 mask 255.255.255.240
 network 172.20.0.160 mask 255.255.255.240
 network 172.20.0.176 mask 255.255.255.240
 network 172.20.0.192 mask 255.255.255.240
 network 172.20.0.208 mask 255.255.255.240
 network 172.20.0.224 mask 255.255.255.240
 network 172.20.0.240 mask 255.255.255.240
 network 172.20.1.0 mask 255.255.255.240
 network 172.20.1.16 mask 255.255.255.240
 network 172.20.1.32 mask 255.255.255.240
 network 172.20.1.48 mask 255.255.255.240
 network 172.20.1.64 mask 255.255.255.240
 network 172.20.1.80 mask 255.255.255.240
 network 172.20.1.96 mask 255.255.255.240
 network 172.20.1.112 mask 255.255.255.240
 network 172.20.1.128 mask 255.255.255.240
 network 172.20.1.144 mask 255.255.255.240
 network 172.20.1.160 mask 255.255.255.240
 network 172.20.1.176 mask 255.255.255.240
 network 172.20.1.192 mask 255.255.255.240
 network 172.20.1.208 mask 255.255.255.240
 network 172.20.1.224 mask 255.255.255.240
 network 172.20.1.240 mask 255.255.255.240
 network 172.20.2.0 mask 255.255.255.240
 network 172.20.2.16 mask 255.255.255.240
 network 172.20.2.32 mask 255.255.255.240
 network 172.20.2.48 mask 255.255.255.240
 network 172.20.2.64 mask 255.255.255.240
 network 172.20.2.80 mask 255.255.255.240
 network 172.20.2.96 mask 255.255.255.240
 network 172.20.2.112 mask 255.255.255.240
 network 172.20.2.128 mask 255.255.255.240
 network 172.20.2.144 mask 255.255.255.240
 network 172.20.2.160 mask 255.255.255.240
 network 172.20.2.176 mask 255.255.255.240
 network 172.20.2.192 mask 255.255.255.240
 network 172.20.2.208 mask 255.255.255.240
 network 172.20.2.224 mask 255.255.255.240
 network 172.20.2.240 mask 255.255.255.240
 network 172.20.3.0 mask 255.255.255.240
 network 172.20.3.16 mask 255.255.255.240
 network 172.20.3.32 mask 255.255.255.240
 network 172.20.3.48 mask 255.255.255.240
 network 172.20.3.64 mask 255.255.255.240
 network 172.20.3.80 mask 255.255.255.240
```

Error: Individual prefixes are advertised to R1. This is not really an error, but it causes excessive memory use on R1 and the downstream EIGRP routers.

The solution is to create an aggregate prefix that summarizes all of the individual prefixes into a single prefix.

```
router bgp 65502
 aggregate-address 172.20.0.0 255.255.248.0 summary-only
```



```
 network 172.20.3.96 mask 255.255.255.240
 network 172.20.3.112 mask 255.255.255.240
 network 172.20.3.128 mask 255.255.255.240
 network 172.20.3.144 mask 255.255.255.240
 network 172.20.3.160 mask 255.255.255.240
 network 172.20.3.176 mask 255.255.255.240
 network 172.20.3.192 mask 255.255.255.240
 network 172.20.3.208 mask 255.255.255.240
 network 172.20.3.224 mask 255.255.255.240
 network 172.20.3.240 mask 255.255.255.240
 network 172.20.4.0 mask 255.255.255.240
 network 172.20.4.16 mask 255.255.255.240
 network 172.20.4.32 mask 255.255.255.240
 network 172.20.4.48 mask 255.255.255.240
 network 172.20.4.64 mask 255.255.255.240
 network 172.20.4.80 mask 255.255.255.240
 network 172.20.4.96 mask 255.255.255.240
 network 172.20.4.112 mask 255.255.255.240
 network 172.20.4.128 mask 255.255.255.240
 network 172.20.4.144 mask 255.255.255.240
 network 172.20.4.160 mask 255.255.255.240
 network 172.20.4.176 mask 255.255.255.240
 network 172.20.4.192 mask 255.255.255.240
 network 172.20.4.208 mask 255.255.255.240
 network 172.20.4.224 mask 255.255.255.240
 network 172.20.4.240 mask 255.255.255.240
 network 172.20.5.0 mask 255.255.255.240
 network 172.20.5.16 mask 255.255.255.240
 network 172.20.5.32 mask 255.255.255.240
 network 172.20.5.48 mask 255.255.255.240
 network 172.20.5.64 mask 255.255.255.240
 network 172.20.5.80 mask 255.255.255.240
 network 172.20.5.96 mask 255.255.255.240
 network 172.20.5.112 mask 255.255.255.240
 network 172.20.5.128 mask 255.255.255.240
 network 172.20.5.144 mask 255.255.255.240
 network 172.20.5.160 mask 255.255.255.240
 network 172.20.5.176 mask 255.255.255.240
 network 172.20.5.192 mask 255.255.255.240
 network 172.20.5.208 mask 255.255.255.240
 network 172.20.5.224 mask 255.255.255.240
 network 172.20.5.240 mask 255.255.255.240
 network 172.20.6.0 mask 255.255.255.240
 network 172.20.6.16 mask 255.255.255.240
 network 172.20.6.32 mask 255.255.255.240
 network 172.20.6.48 mask 255.255.255.240
 network 172.20.6.64 mask 255.255.255.240
 network 172.20.6.80 mask 255.255.255.240
 network 172.20.6.96 mask 255.255.255.240
 network 172.20.6.112 mask 255.255.255.240
 network 172.20.6.128 mask 255.255.255.240
 network 172.20.6.144 mask 255.255.255.240
 network 172.20.6.160 mask 255.255.255.240
 network 172.20.6.176 mask 255.255.255.240
 network 172.20.6.192 mask 255.255.255.240
 network 172.20.6.208 mask 255.255.255.240
 network 172.20.6.224 mask 255.255.255.240
 network 172.20.6.240 mask 255.255.255.240
```



```
 network 172.20.7.0 mask 255.255.255.240
 network 172.20.7.16 mask 255.255.255.240
 network 172.20.7.32 mask 255.255.255.240
 network 172.20.7.48 mask 255.255.255.240
 network 172.20.7.64 mask 255.255.255.240
 network 172.20.7.80 mask 255.255.255.240
 network 172.20.7.96 mask 255.255.255.240
 network 172.20.7.112 mask 255.255.255.240
 network 172.20.7.128 mask 255.255.255.240
 network 172.20.7.144 mask 255.255.255.240
 network 172.20.7.160 mask 255.255.255.240
 network 172.20.7.176 mask 255.255.255.240
 network 172.20.7.192 mask 255.255.255.240
 network 172.20.7.208 mask 255.255.255.240
 network 172.20.7.224 mask 255.255.255.240
 network 172.20.7.240 mask 255.255.255.240
!
ip route 172.20.0.0 255.255.255.240 Null0
ip route 172.20.0.16 255.255.255.240 Null0
ip route 172.20.0.32 255.255.255.240 Null0
ip route 172.20.0.48 255.255.255.240 Null0
ip route 172.20.0.64 255.255.255.240 Null0
ip route 172.20.0.80 255.255.255.240 Null0
ip route 172.20.0.96 255.255.255.240 Null0
ip route 172.20.0.112 255.255.255.240 Null0
ip route 172.20.0.128 255.255.255.240 Null0
ip route 172.20.0.144 255.255.255.240 Null0
ip route 172.20.0.160 255.255.255.240 Null0
ip route 172.20.0.176 255.255.255.240 Null0
ip route 172.20.0.192 255.255.255.240 Null0
ip route 172.20.0.208 255.255.255.240 Null0
ip route 172.20.0.224 255.255.255.240 Null0
ip route 172.20.0.240 255.255.255.240 Null0
ip route 172.20.1.0 255.255.255.240 Null0
ip route 172.20.1.16 255.255.255.240 Null0
ip route 172.20.1.32 255.255.255.240 Null0
ip route 172.20.1.48 255.255.255.240 Null0
ip route 172.20.1.64 255.255.255.240 Null0
ip route 172.20.1.80 255.255.255.240 Null0
ip route 172.20.1.96 255.255.255.240 Null0
ip route 172.20.1.112 255.255.255.240 Null0
ip route 172.20.1.128 255.255.255.240 Null0
ip route 172.20.1.144 255.255.255.240 Null0
ip route 172.20.1.160 255.255.255.240 Null0
ip route 172.20.1.176 255.255.255.240 Null0
ip route 172.20.1.192 255.255.255.240 Null0
ip route 172.20.1.208 255.255.255.240 Null0
ip route 172.20.1.224 255.255.255.240 Null0
ip route 172.20.1.240 255.255.255.240 Null0
ip route 172.20.2.0 255.255.255.240 Null0
ip route 172.20.2.16 255.255.255.240 Null0
ip route 172.20.2.32 255.255.255.240 Null0
ip route 172.20.2.48 255.255.255.240 Null0
ip route 172.20.2.64 255.255.255.240 Null0
ip route 172.20.2.80 255.255.255.240 Null0
ip route 172.20.2.96 255.255.255.240 Null0
ip route 172.20.2.112 255.255.255.240 Null0
ip route 172.20.2.128 255.255.255.240 Null0
```

```
ip route 172.20.2.144 255.255.255.240 Null0
ip route 172.20.2.160 255.255.255.240 Null0
ip route 172.20.2.176 255.255.255.240 Null0
ip route 172.20.2.192 255.255.255.240 Null0
ip route 172.20.2.208 255.255.255.240 Null0
ip route 172.20.2.224 255.255.255.240 Null0
ip route 172.20.2.240 255.255.255.240 Null0
ip route 172.20.3.0 255.255.255.240 Null0
ip route 172.20.3.16 255.255.255.240 Null0
ip route 172.20.3.32 255.255.255.240 Null0
ip route 172.20.3.48 255.255.255.240 Null0
ip route 172.20.3.64 255.255.255.240 Null0
ip route 172.20.3.80 255.255.255.240 Null0
ip route 172.20.3.96 255.255.255.240 Null0
ip route 172.20.3.112 255.255.255.240 Null0
ip route 172.20.3.128 255.255.255.240 Null0
ip route 172.20.3.144 255.255.255.240 Null0
ip route 172.20.3.160 255.255.255.240 Null0
ip route 172.20.3.176 255.255.255.240 Null0
ip route 172.20.3.192 255.255.255.240 Null0
ip route 172.20.3.208 255.255.255.240 Null0
ip route 172.20.3.224 255.255.255.240 Null0
ip route 172.20.3.240 255.255.255.240 Null0
ip route 172.20.4.0 255.255.255.240 Null0
ip route 172.20.4.16 255.255.255.240 Null0
ip route 172.20.4.32 255.255.255.240 Null0
ip route 172.20.4.48 255.255.255.240 Null0
ip route 172.20.4.64 255.255.255.240 Null0
ip route 172.20.4.80 255.255.255.240 Null0
ip route 172.20.4.96 255.255.255.240 Null0
ip route 172.20.4.112 255.255.255.240 Null0
ip route 172.20.4.128 255.255.255.240 Null0
ip route 172.20.4.144 255.255.255.240 Null0
ip route 172.20.4.160 255.255.255.240 Null0
ip route 172.20.4.176 255.255.255.240 Null0
ip route 172.20.4.192 255.255.255.240 Null0
ip route 172.20.4.208 255.255.255.240 Null0
ip route 172.20.4.224 255.255.255.240 Null0
ip route 172.20.4.240 255.255.255.240 Null0
ip route 172.20.5.0 255.255.255.240 Null0
ip route 172.20.5.16 255.255.255.240 Null0
ip route 172.20.5.32 255.255.255.240 Null0
ip route 172.20.5.48 255.255.255.240 Null0
ip route 172.20.5.64 255.255.255.240 Null0
ip route 172.20.5.80 255.255.255.240 Null0
ip route 172.20.5.96 255.255.255.240 Null0
ip route 172.20.5.112 255.255.255.240 Null0
ip route 172.20.5.128 255.255.255.240 Null0
ip route 172.20.5.144 255.255.255.240 Null0
ip route 172.20.5.160 255.255.255.240 Null0
ip route 172.20.5.176 255.255.255.240 Null0
ip route 172.20.5.192 255.255.255.240 Null0
ip route 172.20.5.208 255.255.255.240 Null0
ip route 172.20.5.224 255.255.255.240 Null0
ip route 172.20.5.240 255.255.255.240 Null0
ip route 172.20.6.0 255.255.255.240 Null0
ip route 172.20.6.16 255.255.255.240 Null0
ip route 172.20.6.32 255.255.255.240 Null0
```



```
ip route 172.20.6.48 255.255.255.240 Null0
ip route 172.20.6.64 255.255.255.240 Null0
ip route 172.20.6.80 255.255.255.240 Null0
ip route 172.20.6.96 255.255.255.240 Null0
ip route 172.20.6.112 255.255.255.240 Null0
ip route 172.20.6.128 255.255.255.240 Null0
ip route 172.20.6.144 255.255.255.240 Null0
ip route 172.20.6.160 255.255.255.240 Null0
ip route 172.20.6.176 255.255.255.240 Null0
ip route 172.20.6.192 255.255.255.240 Null0
ip route 172.20.6.208 255.255.255.240 Null0
ip route 172.20.6.224 255.255.255.240 Null0
ip route 172.20.6.240 255.255.255.240 Null0
ip route 172.20.7.0 255.255.255.240 Null0
ip route 172.20.7.16 255.255.255.240 Null0
ip route 172.20.7.32 255.255.255.240 Null0
ip route 172.20.7.48 255.255.255.240 Null0
ip route 172.20.7.64 255.255.255.240 Null0
ip route 172.20.7.80 255.255.255.240 Null0
ip route 172.20.7.96 255.255.255.240 Null0
ip route 172.20.7.112 255.255.255.240 Null0
ip route 172.20.7.128 255.255.255.240 Null0
ip route 172.20.7.144 255.255.255.240 Null0
ip route 172.20.7.160 255.255.255.240 Null0
ip route 172.20.7.176 255.255.255.240 Null0
ip route 172.20.7.192 255.255.255.240 Null0
ip route 172.20.7.208 255.255.255.240 Null0
ip route 172.20.7.224 255.255.255.240 Null0
ip route 172.20.7.240 255.255.255.240 Null0
ip route 192.168.1.1 255.255.255.255 209.165.200.225
!
ip http server
no ip http secure-server
!
logging source-interface Loopback0
logging 10.1.50.1
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 logging synchronous
 login authentication CONSOLE
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
!
ntp master 3
 end
```

Router R3

```
!Lab 7-1 Router R3 TT-B Config
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 7-1 Router R3 TT-B Config ***$
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!

ip cef
no ip domain lookup
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 10.1.203.1 255.255.255.255
!
interface FastEthernet0/0
 description FE to ALS1
 ip address 10.1.80.1 255.255.255.0
 ip flow ingress
 speed 100
 full-duplex
 no shutdown
!
interface FastEthernet0/1
 description FE to DLS2
```



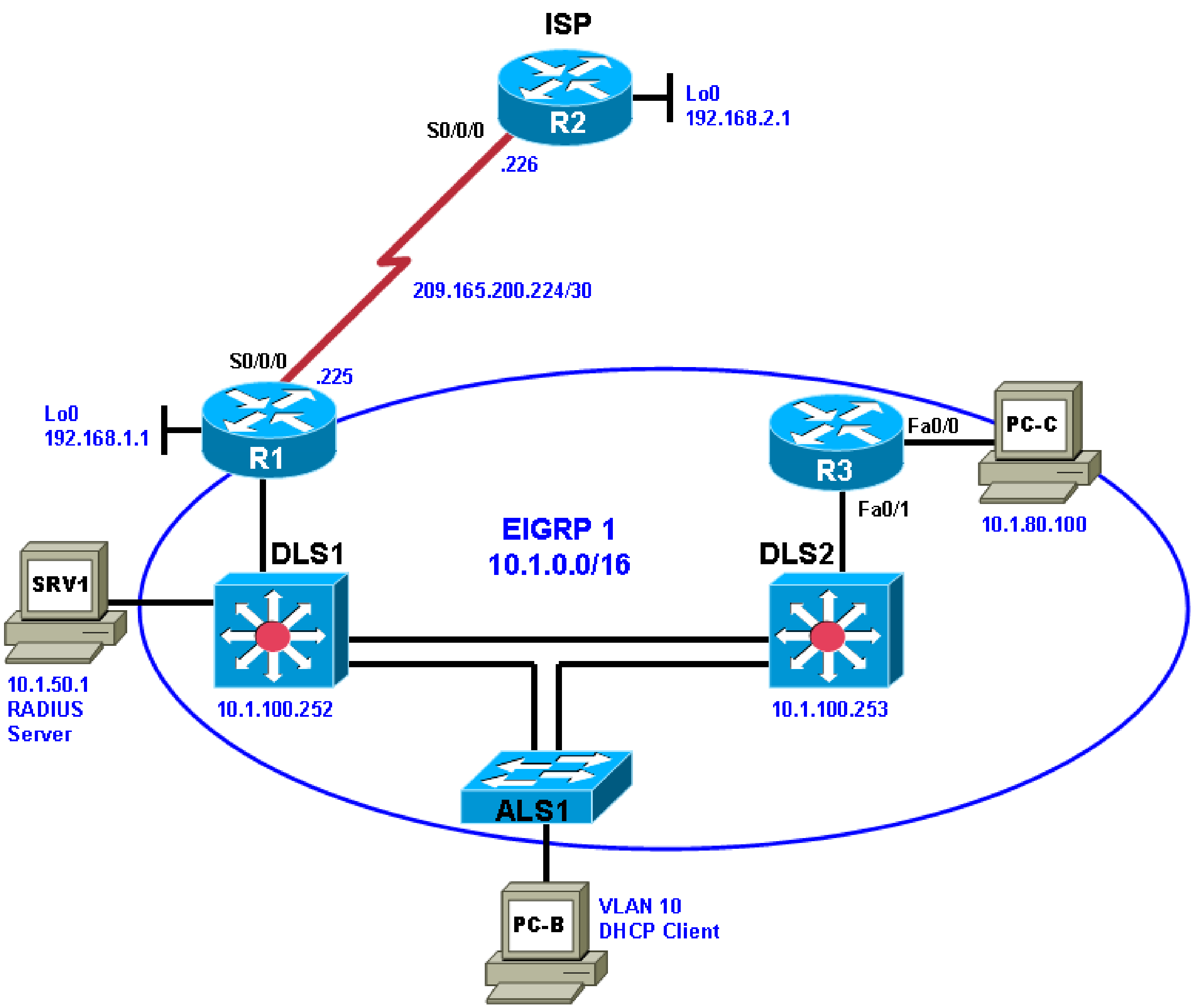
```
 ip address 10.1.2.14 255.255.255.252
 ip flow ingress
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
description WAN link to R1 – not used for this lab
 no ip address
 clock rate 128000
 encapsulation ppp
 shutdown
!
interface Serial0/0/1
 description WAN link to R2 - not used for this lab
 no ip address
 encapsulation ppp
 shutdown
!
router eigrp 1
 passive-interface default
 no passive-interface FastEthernet0/1
 network 10.1.80.0 0.0.0.255
 network 10.1.2.12 0.0.0.3
 network 10.1.203.1 0.0.0.0
 no auto-summary
!
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
logging source-interface Loopback0
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 logging synchronous
 login authentication CONSOLE
line vty 0 4
 exec-timeout 60 0
transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
```



```
ntp server 192.168.2.1
end
```


Chapter 9 Lab 9-1, Management Plane Security **Instructor Version**

Lab Topology



Objectives

- Load the device configuration files for each trouble ticket.
- Diagnose and resolve problems related to router and Layer 3 switch management plane security.
- Document the troubleshooting progress, configuration changes, and problem resolution.

Background

Routers and Layer 3 switches are typically segmented into three planes of operation, each with a clearly identified objective. The data plane (also called the forwarding plane) forwards user data packets. The control plane routes data correctly, and the management plane manages the network devices.

The management plane deals with the traffic used to access, manage, and monitor all the network elements. It supports all required provisioning, maintenance, and monitoring functions for the network. Like the other IP traffic planes, management plane traffic is handled in-band with all other IP traffic. Most service providers and many large enterprises also build separate, out-of-band (OOB) management networks to provide alternate reachability when the primary in-band IP path is not reachable.

Processes and protocols that are associated with this plane include Telnet, AAA, SSH, FTP, TFTP, SNMP, syslog, TACACS+, RADIUS, DNS, NetFlow, ROMMON, and other management protocols.

This lab focuses on management plane security issues related to SSH, AAA, and RADIUS for management access to routers and Layer 3 switches.

For each task or trouble ticket, the trouble scenario and problem symptom are described. While troubleshooting, you will discover the cause of the problem, correct it, and then document the process and results.

Note: Because TACACS+ is Cisco proprietary and is more complex to configure, this lab uses RADIUS instead of TACACS+. RADIUS is an Internet standard and several freeware versions are available. However, TACACS+ is generally considered to be superior to RADIUS because it offers increased functionality and encrypts messages between the server and client.

Lab Structure

This lab is divided into two main sections.

Section 1—Trouble Tickets and Troubleshooting Logs

This section includes two tasks. Each task is associated with a trouble ticket (TT) and introduces one or more errors on one or more devices. If time is a consideration, each task or trouble ticket can be performed independently.

Section 2—Troubleshooting Reference Information

This section provides general troubleshooting information that can be applied to any of the trouble tickets in this lab. Examples of useful commands and output are provided. If time permits, it is recommended that you read through Section 2 prior to starting on the trouble tickets.

Instructor note: Because the troubleshooting reference section is lengthy, ask students to read through it prior to starting the lab to become familiar with the commands used in this lab. Consider assigning it as homework.

Note: This lab uses Cisco 1841 routers with Cisco IOS Release 12.4(24)T1 and the Advanced IP Services image c1841-advipservicesk9-mz.124-24.T1.bin. The switches are Cisco WS-C2960-24TT-L with the Cisco IOS image c2960-lanbasek9-mz.122-46.SE.bin and Catalyst 3560-24PS with the Cisco IOS image c3560-advipservicesk9-mz.122-46.SE.bin. Other routers (such as 2801 and 2811), switches (such as 2950 or 3550), and Cisco IOS Software versions can be used if they have comparable capabilities and features. Depending on the router or switch model and Cisco IOS Software version, the commands available and output produced might vary from what is shown in this lab.

Any changes made to configurations or topology (other than errors introduced) are noted in the lab and trouble tickets so that you are aware of them prior to beginning the troubleshooting process.

Instructor Notes

- The lab topology should be pre-built prior to the students starting the lab. Ensure that all routers and switches (R1, R2, R3, ALS1, DLS1, and DLS2) have the course lab configuration files installed in flash. You can download the files from the Academy Connection website.
- The device configurations that contain trouble ticket errors and modifications from the baseline are included at the end of the lab, and the errors in them are identified.
- Each device should have a directory named "tshoot" in flash. This directory contains the baseline configuration file for that device as well as the configuration files for the labs in this course. Refer to Lab 3-1 for instructions on creating the tshoot directory in flash.
- Instructors can use a TFTP server, USB drive, flash memory card, or other method to copy all the course configuration files into the flash:/tshoot directory for each device in the topology.
- The student is responsible for loading the baseline or trouble ticket configurations as required using the procedure described in Lab 3-1.
- Set the correct time on router R2, which serves as the primary NTP server for the lab network.
- If time is an issue, each task (trouble ticket) can be performed independently.

Required Resources

- 3 routers (Cisco 1841 with Cisco IOS Release 12.4(24)T1 Advanced IP Service or comparable)
- 1 switch (Cisco 2960 with the Cisco IOS Release 12.2(46)SE C2960-LANBASEK9-M image or comparable)
- 2 switches (Cisco 3560 with the Cisco IOS Release 12.2(46)SE C3560-advipservicesk9-mz image or comparable)
- SRV1 (Windows PC with 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

Instructor Notes

- This lab is divided into multiple tasks. Each task is associated with a trouble ticket (TT) and introduces one or more errors on one or more devices.
- Students can work individually or as a team.
- Suggested actions and results presented during the troubleshooting process for each TT can be shared with the students during debrief or copies of the instructor version of the lab can be made available to the students to assist them in verifying their work.

Section 1—Trouble Tickets and Troubleshooting Logs

Task 1: Trouble Ticket Lab 9-1 TT-A

Instructor note: This trouble ticket involves device DLS1 and issues related to AAA access, Telnet, and the RADIUS server configuration (port numbers) for device access.

Step 1: Review trouble ticket Lab 9-1 TT-A.

As a security measure, your company has decided to implement centralized server-based AAA authentication for key network devices, such as routers and switches. The implementation plan specifies that RADIUS server software is to be installed on SRV1 (see Appendix A for the installation procedure). As a pilot, Layer 3 core switch DLS1 is to be configured with AAA to access the RADIUS server for login authentication. The implementation plan specifies RADIUS as the primary method of authentication, with local authentication as the backup method.

Your colleague has configured the RADIUS server on SRV1 and AAA login authentication on DLS1 but is having trouble accessing DLS1 when attempting to log in via Telnet from PC-B. On the RADIUS server, he has created a test username **raduser** with a password of **RadUserpass**.

He has asked for your help in diagnosing and solving the problem.

Note: The freeware server WinRadius is used for this trouble ticket.

Step 2: Load the device trouble ticket configuration files for TT-A.

Using the procedure described in Lab 3-1, verify that the lab configuration files are present in flash. Load the proper configuration files as indicated in the Device Configuration File table.

Note: The following device access methods are in effect after installing RADIUS on SRV1 and loading the configuration files:

- Console access requires no username or password.
- Telnet and SSH require username **admin** and password **adminpa55** (except for DLS1, which uses RADIUS).
- The enable password is **ciscoenpa55**.

Instructor note: Although it is not considered security best practice, the enable secret and admin user passwords can be changed to something simpler to facilitate performance of this lab.

Device Configuration File Table

Device Name	File to Load	Notes
ALS1	Lab91-ALS1-TT-A-Cfg.txt	This file contains configurations different than the baseline
DLS1	Lab91-DLS1-TT-A-Cfg.txt	This file contains configuration errors
DLS2	Lab91-DLS2-TT-A-Cfg.txt	This file contains configurations different than the baseline
R1	Lab91-R1-TT-A-Cfg.txt	This file contains configurations different than the baseline
R2	Lab91-R2-TT-A-Cfg.txt	This file contains configurations different than the baseline
R3	Lab91-R3-TT-A-Cfg.txt	This file contains configurations different than the baseline
SRV1	N/A	Static IP: 10.1.50.1/24 Default gateway: 10.1.50.254

PC-B	N/A	DHCP
PC-C	N/A	Static IP: 10.1.80.100/24 Default gateway: 10.1.80.1

Instructor note: The student loads the "broken" TT configuration files for all devices, even though only the configurations indicated in the Notes column contain errors.

Step 3: Configure SRV1 and start the RADIUS server.

Instructor note: The procedure for installing the WinRadius server is described in Appendix A.

a. Configure SRV1 with the static IP address 10.1.50.1/24 and default gateway 10.1.50.254.

b. Start the WinRadius server application on SRV1. If the WinRadius server is not installed, contact your instructor.

c. From the menu, select **Operation > Add User** and create a new user named **raduser** with a password of **RadUserpass.** Click **OK**.

   Note: Passwords are case-sensitive.

d. To clear the log on the WinRadius server, select **Log > Clear** from the main menu.

Note: If you exit the WinRadius server application and restart it, you must recreate the user **raduser**. A maximum of five users can be created using the free version of the software.

Step 4: Release and renew the DHCP lease on PC-B.

a. Ensure that PC-B is configured as a DHCP client in the OFFICE VLAN.

b. After loading all TT-A device configuration files, issue the **`ipconfig /release`** and **`ipconfig /renew`** commands on PC-B.

Step 5: Outline the troubleshooting approach and validation steps.

Use this space to identify your troubleshooting approach and the key steps to verify that the problem is resolved. Troubleshooting approaches to select from include the follow-the-path, spot-the-differences, bottom-up, top-down, divide-and-conquer, shoot-from-the-hip, and move-the-problem methods.

Note: In addition to a specific approach, you can use the generic troubleshooting process described at the beginning of Section 2 of this lab.

____

____

____

____

____

____

The bottom-up or divide-and-conquer method can be used. Other problem-solving methods are the top-down, follow-the-path, spot-the-differences, shoot-from-the-hip, and move-the-problem approaches.

Verification steps can include:

- PC-B can telnet to DLS1, and user **raduser** with password **RadUserpass** can be authenticated as a valid user by the RADIUS server on SRV1 when the server is available.

- PC-B can telnet to DLS1, and user **admin** with password **adminpa55** can be authenticated by the local database if the RADIUS server on SRV1 is not available.
- If you telnet to DLS1 and enter a username-password combination that is not in the RADIUS server database, you are denied access to DLS1.
- You can access the DLS1 console user EXEC mode directly without entering a username and password but must enter the enable secret password to gain access to privileged EXEC mode.
- Successful authentication messages display on the SRV1 RADIUS server.

Step 6: Record the troubleshooting process and configuration changes.

Note: Section 2 of this lab includes useful commands and examples of output.

Use this log to document your actions and results during the troubleshooting process. List the commands you used to gather information. As you progress, record what you think the problem might be and the actions you take to correct the problem.

Device	Actions and Results

Responses will vary but could include:

- Pings from PC-B to DLS1 succeed.
- Pings from DLS1 (10.1.100.252) to RADIUS server SRV1 (10.1.50.1) succeed.
- Telnet from PC-B to DLS1 is rejected.
- No login success or failure messages display on the SRV1 RADIUS server.

TT-A Issue 1

Telnet is not permitted on vty lines 0–4 (only SSH). As a result, DLS1 rejects all Telnet connection attempts.

- Telnet from PC-B to DLS1 is rejected with the message:

```
C:\>telnet 10.1.100.252
Connecting To 10.1.100.252...Could not open connection to the host, on port
23: Connect failed
```

- Telnet from DLS1 to R1 (192.168.1.1) is accepted.
- Pings from PC-B to DLS1 (10.1.100.252) verify Layer 3 connectivity.
- The **`show line vty 0`** command on DLS1 indicates that the allowed input transport is SSH but not Telnet. Allowed output transports are Telnet and SSH.
- The **`show run | begin vty`** command on DLS1 confirms that the only input transport allowed is SSH.

Action: Add the `telnet` keyword to vty lines 0–4. See the TT-A debrief for more information.

Verification: Telnet from PC-B to DLS1 makes the connection, and DLS1 prompts for user access verification. However, you cannot log in to DLS1 with the test user account **raduser**. There must be another problem.

TT-A Issue 2

The default ports used with the Cisco IOS software do not match the ones used by the WinRadius server on SRV1. As a result, the RADIUS server software running on SRV1 is not accessible.

- Attempts to log in to DLS1 using the RADIUS user account **raduser** fail.
- Attempts to log in to DLS1 using the local user account **admin** succeed but with significant delay.
- The **`show run | include aaa`** command on DLS1 indicates that the AAA Telnet is configured properly to try the RADIUS server first for authentication and then use the local user database as a backup if the RADIUS server is unavailable. This explains why you can log in as local user **admin** but with a delay.
- A check of the SRV1 RADIUS server verifies that WinRadius is running, but there are no log messages indicating successful or failed login attempts.
- Pings from DLS1 (10.1.100.252) to RADIUS server SRV1 (10.1.50.1) verify Layer 3 connectivity between DLS1 and SRV1.
- The **`show radius server-group all`** command on DLS1 indicates that host 10.1.50.1 (SRV1) is defined as the server, operating on ports 1645 and 1646.

```
Sever group radius
    Sharecount = 1  sg_unconfigured = FALSE
    Type = standard  Memlocks = 1
    Server(10.1.50.1:1645,1646) Transactions:
```

- The **`show radius statistics`** command on DLS1 indicates that multiple packets have been sent without responses, and multiple authentication timeouts have occurred.
- The **`show aaa servers`** command on DLS1 indicates that the RADIUS server is 10.1.50.1, and DLS1 is configured to use auth-port 1645 and acct-port 1646. There have been multiple authentication requests and an equal number of timeouts. There are multiple failures and no successes.
- When the **`debug radius authentication`** command on DLS1 is active, attempts to log in from PC-B as **raduser** with a password of **RadUserpass** fail.
- Debug messages indicate that DLS1 is attempting multiple retransmits, and the RADIUS server is not responding.

```
DLS1#
Dec  4 16:07:10.370: RADIUS: Retransmit to (10.1.50.1:1645,1646) for id 1645/5
Dec  4 16:07:25.370: %RADIUS-4-RADIUS_DEAD: RADIUS server 10.1.50.1:1645,1646 is
 not responding.
```



```
Dec  4 16:07:25.370: RADIUS: No response from (10.1.50.1:1645,1646) for id 1645/
5
```

- The **`show run | include radius-server`** command on DLS1 indicates that the RADIUS server key is specified, but because of password encryption, we cannot tell if it is correct. If the wrong password is specified on DLS1 for the RADIUS server on SRV1, DLS1 cannot communicate with the RADIUS server software.
- Display the WinRadius password and the default ports that the RADIUS server software is using by selecting **Settings > System** from the WinRadius main menu on SRV1.
- Changing the password to the one specified in WinRadius does not allow DLS1 to establish communication with the RADIUS server. There must be another problem.
- The WinRadius **Settings > System** screen shows that WinRadius is using ports 1812 and 1813 for authorization and accounting. What ports is DLS1 using?
- The **`show run | include radius-server`** command on DLS1 indicates that host 10.1.50.1 (SRV1) is specified as the RADIUS server and that DLS1 uses auth-port 1645 and acct-port 1646 to communicate with the RADIUS server software on DLS1. The port numbers do not match.
- the previous **`show radius statistics`** command output and debug message output on DLS1 shows that the RADIUS ports being used by DLS1 are 1645 and 1646. The port numbers do not match those of the RADIUS server.

Action: Change the RADIUS port numbers used on DLS1 to match those of the RADIUS server on SRV1 (1812 and 1813). See TT-A debrief for more information.

Verification:

- Telnet to DLS1. The login attempt with username **raduser** and password **RadUserpass** fails.
- Authentication OK message displays on the RADIUS server log screen for **raduser**.
- The Telnet session is immediately closed by DLS1. There must be another problem.

TT-A Issue 3

AAA authorization is configured on DLS1 for EXEC access. It defaults to local instead of TELNET-LINES for Telnet. This prevents the host that is using Telnet from accessing the EXEC prompt (user or privileged). As a result, the Telnet session is immediately closed by DLS1.

- Attempts to log in to DLS1 from PC-B using the RADIUS user account **raduser** fail. The Telnet session is immediately closed by DLS1 with the message “% Authorization failed. Connection to host lost.”
- An authentication OK message displays on the RADIUS server log screen, indicating that **raduser** is successfully authenticated.
- The **`debug radius authentication`** command on DLS1 reveals that **raduser** is accepted as a valid user and the response is sent to DLS1.

```
<some output omitted>
Dec  7 14:51:36.763: RADIUS:  authenticator DC E8 EB 1E AC AA 24 68
Dec  7 14:51:36.763: RADIUS:  User-Name           [1]   9   "raduser"
Dec  7 14:51:36.763: RADIUS:  User-Password       [2]   18  *
Dec  7 14:51:36.772: RADIUS:  NAS-Port-Id         [87]  6   "tty1"
Dec  7 14:51:36.772: RADIUS:  Calling-Station-Id  [31]  11  "10.1.10.1"
Dec  7 14:51:36.772: RADIUS:  NAS-IP-Address      [4]   6   10.1.50.252
Dec  7 14:51:36.772: RADIUS:  Received from id 1645/8 10.1.50.1:1812, Access-
Accept
```

- The **`debug aaa authentication`** command on DLS1 indicates that TELNET_LINES was the AAA method list used, but there is no indication of success or failure.

```
Dec  7 16:06:20.330: AAA/BIND(0000000D): Bind i/f
Dec  7 16:06:20.330: AAA/AUTHEN/LOGIN (0000000D): Pick method list
'TELNET_LINES’
```


- The **debug aaa authorization** command on DLS1 indicates that "default" was the pick method list used and authorization was not successful.

```
Dec  7 16:07:43.311: AAA/AUTHOR (0xE): Pick method list 'default' - FAIL
Dec  7 16:07:43.311: AAA/AUTHOR/EXEC(0000000E): Authorization FAILED
```

- Referring back to the Telnet session message on PC-B, "% Authorization failed," the problem is not with authentication but with authorization.
- The **show run | include aaa** command on DLS1 indicates that AAA for Telnet is configured properly to use the RADIUS server for authentication but not for authorization.
- The **aaa authorization exec default local** command requires that a user accessing the EXEC prompt be authorized using the local database. As soon as **raduser** is authenticated, it attempts to access the EXEC prompt on DLS1, but it is not authorized to do so and DLS1 closes the Telnet session.

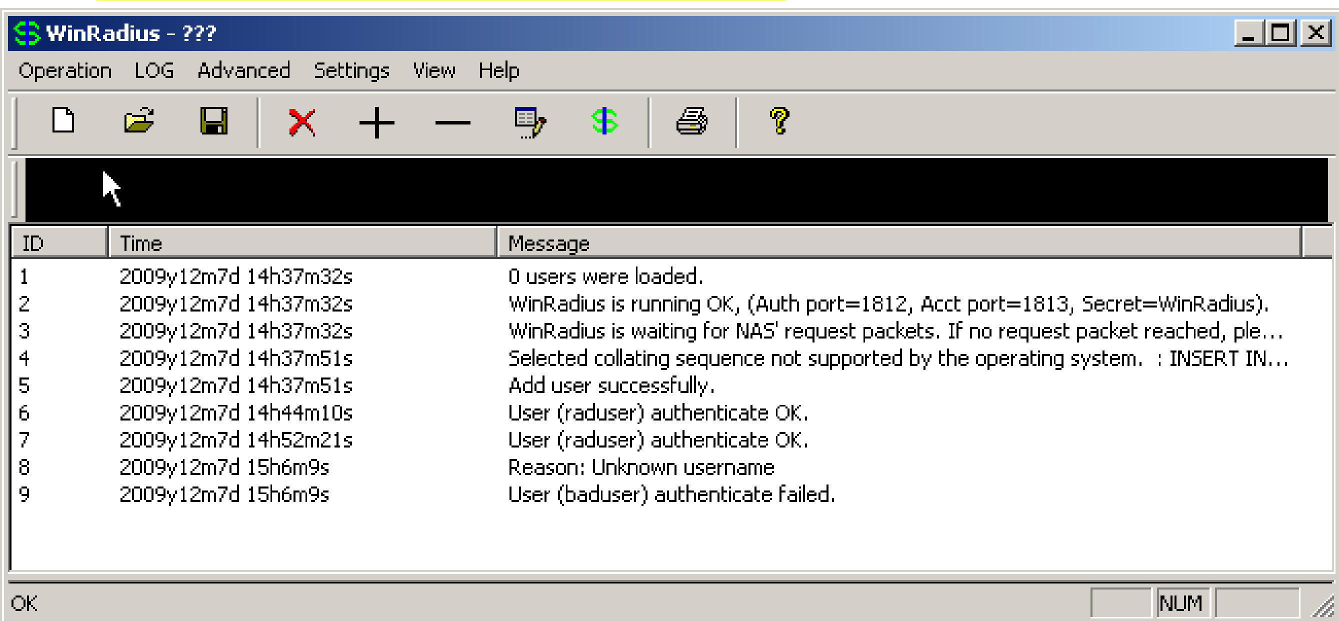
Action:

- Option 1: Add local user **admin** to the RADIUS server.
- Option 2: Configure AAA authorization on DLS1 for Telnet access.
- Option 3: Remove the requirement for AAA EXEC authorization from DLS1.
- See the TT-A debrief for more information.

Verification:

- Telnet to DLS1 from PC-B. Logging in with username **raduser** and password **RadUserpass** is successful.
- Telnet to DLS1. Logging in with an undefined username (example baduser, password badpass) fails with the message "Authentication failed."
- Authentication success and failure messages display on the RADIUS server log screen.

(WinRadius screenshot is for instructor version of lab.)



Step 7: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with your instructor. The notes can include problems encountered, solutions applied, useful commands employed, alternate solutions, methods, and processes, and procedure and communication improvements.

____

____

____

____

____

____

____

Trouble Ticket TT-A Debrief—Instructor Notes

This trouble ticket consists of three configuration issues that impact remote administrative access using Telnet.

TT-A Issue 1

The first problem is that Telnet is not permitted on vty lines 0–4 on DLS1 (only SSH is permitted). As a result, DLS1 rejects all Telnet connection attempts. To correct the problem, use the following commands on switch DLS1:

```
line vty 0 4
   transport input telnet ssh
```

TT-A Issue 2

The second problem is that the default RADIUS ports (1645 and 1646) used with the Cisco IOS Software do not match the ones used by the WinRadius server on SRV1 (1812 and 1813). As a result, the RADIUS server software running on SRV1 is not accessible to DLS1, and no RADIUS authentication can occur. However, local AAA authentication is specified as a fallback, which allows access if the RADIUS server is inaccessible for some reason. This assumes that a valid local username and password are known. If the RADIUS server is down, the RADIUS client (DLS1 in this case) will still try to authenticate the user via RADIUS first, resulting in a significant login delay.

Point out that the early deployment of RADIUS was done using UDP port number 1645 for authentication and 1646 for accounting, which conflicts with the datametrics service. Because of this conflict, RFC 2865 officially assigned port numbers 1812 and 1813 for RADIUS.

Unless specified otherwise, the Cisco IOS RADIUS configuration defaults to UDP port numbers 1645 and 1646. Either the router Cisco IOS port numbers must be changed to match the port number of the RADIUS server or the RADIUS server port numbers must be changed to match the port numbers of the Cisco IOS router.

To change the Cisco IOS port numbers to those used by the RADIUS server, issue the following commands on DLS1:

```
no radius-server host 10.1.50.1 auth-port 1645 acct-port 1646
radius-server host 10.1.50.1 auth-port 1812 acct-port 1813 key WinRadius
```

TT-A Issue 3

The third problem is that AAA authorization for EXEC access defaults to local instead of TELNET-LINES for Telnet. This prevents the host that is using Telnet from accessing the EXEC prompt (user or privileged) because the AAA policy specifies that EXEC access is only permitted if the user is locally defined.

Note: The messages on the RADIUS server indicate that the user is authenticated (OK) but the Telnet session is closed immediately by DLS1 and an error message is sent to the Telnet client that says: "% Authorization failed," and the connection to the DLS1 host is lost.

To remedy this problem, there are three options:

- Add local user **admin** and password **adminpa55** to the RADIUS server using the GUI.
- Remove the requirement for AAA EXEC authorization from DLS1.
  ```
  no aaa authorization exec default local
  ```
- Configure AAA authorization on DLS1 for use with Telnet access.
  ```
  no aaa authorization exec default local
  aaa authorization exec TELNET_LINES group radius local
  ```

Task 2: Trouble Ticket Lab 9-1 TT-B

Instructor note: This trouble ticket involves device R3 and issues related to ACLs, SSH access, and copying of configurations and RSA keys.

Step 1: Review trouble ticket Lab 9-1 TT-B.

As a further security measure, your company has decided to implement SSH and only allow vty access to key networking devices from specific management workstations. As a pilot, router R3 will be configured to allow SSH access from only PC-C (on the R3 LAN) and prevent remote access from any host other than PC-C. For testing purposes, host PC-C will be used as a management workstation and will be assigned a static address of 10.1.80.100. Login from PC-C to R3 must be authenticated by the RADIUS server running on SRV1. No other hosts in the network should be able to access R3 via SSH.

A colleague of yours configured an ACL and SSH access on R3, but due to sporadic hardware issues with R3, she decided to replace R3 with a comparable router. She says that she backed up the configuration from the old router to a USB flash drive and loaded it into the new router. Now she is unable to connect to R3 using SSH from PC-C.

On the RADIUS server, she created a test user named **raduser** with a password of **RadUserpass**. The implementation plan specifies RADIUS as the primary method of authentication with local authentication as the backup method.

She has asked for your help in diagnosing and solving the problem.

Step 2: Load the device trouble ticket configuration files for TT-B.

Using the procedure described in Lab 3-1, verify that the lab configuration files are present in flash. Load the proper configuration files as indicated in the Device Configuration File table.

Note: The following device access methods are in effect after installing RADIUS on SRV1 and loading the configuration files:

- Console access requires no username or password.
- Telnet and SSH require username **admin** and password **adminpa55** (except for R3).
- The enable password is **ciscoenpa55**.

Instructor note: Although it is not considered security best practice, the enable secret and admin user passwords can be changed to something simpler to facilitate performance of this lab.

Device Configuration File Table

Device Name	File to Load	Notes
ALS1	Lab91-ALS1-TT-B-Cfg.txt	This file contains configurations different than the baseline
DLS1	Lab91-DLS1-TT-B-Cfg.txt	This file contains configurations different than the baseline
DLS2	Lab91-DLS2-TT-B-Cfg.txt	This file contains configurations different than the baseline
R1	Lab91-R1-TT-B-Cfg.txt	This file contains configurations different than the baseline
R2	Lab91-R2-TT-B-Cfg.txt	This file contains configurations different than the baseline
R3	Lab91-R3-TT-B-Cfg.txt	This file contains configuration errors
SRV1	N/A	Static IP: 10.1.50.1/24 Default gateway: 10.1.50.254
PC-B	N/A	DHCP
PC-C	N/A	Static IP: 10.1.80.100/24 Default gateway: 10.1.80.1

Instructor note: The student loads the "broken" TT configuration files for all devices, even though only the configurations indicated in the Notes column contain errors.

Step 3: Configure SRV1 and start the RADIUS server.

Instructor note: The procedure for installing the WinRadius server is described in Appendix A.

a. Configure SRV1 with static IP address 10.1.50.1/24 and default gateway 10.1.50.254.

b. Start the WinRadius server application on SRV1. If the WinRadius server is not installed, contact your instructor.

c. Select **Operation > Add User** from the menu and create a new user named **raduser** with a password of **RadUserpass**. Click **OK**.

   Note: Passwords are case-sensitive.

d. To clear the log on the WinRadius server, select **Log > Clear** from the main menu.

Note: If you exit the WinRadius server application and restart it, you must recreate the user **raduser**. A maximum of five users can be created using the free version of the software.

Step 4: Configure a static IP address on PC-C.

a. Configure PC-C with static IP address 10.1.80.100, subnet mask 255.255.255.0, and default gateway 10.1.80.1.

b. Verify that PC-C has PuTTY (or comparable) SSH client software installed. If it does not, contact your instructor.

Step 5: Outline the troubleshooting approach and validation steps.

Use this space to identify your troubleshooting approach and the key steps to verify that the problem is resolved. Troubleshooting approaches to select from include the follow-the-path, spot-the-differences, bottom-up, top-down, divide-and-conquer, shoot-from-the-hip, and move-the-problem methods.

Note: In addition to a specific approach, you can use the generic troubleshooting process described at the beginning of Section 2 of this lab.

____

____

____

____

____

____

The divide-and-conquer or shoot-from-the-hip method can be used. Other problem-solving methods are the bottom-up, top-down, follow-the-path, spot-the-differences, and move-the-problem approaches.

Verification steps can include:

- Only PC-C can use SSH to access R3.
- The PC-C user login is authenticated as a valid user by the RADIUS server on SRV1 when the server is available.
- PC-C can use only SSH to access R3 and not Telnet.
- No other PCs can use SSH or Telnet to access R3.

Step 6: Record the troubleshooting process and configuration changes.

Note: Section 2 of this lab includes useful commands and examples of output.

Use this log to document your actions and results during the troubleshooting process. List the commands you used to gather information. As you progress, record what you think the problem might be and the actions you take to correct the problem.

Device	Actions and Results

Device	Actions and Results

Responses will vary but could include:

- Pings from PC-C to the R3 default gateway succeed.
- Pings from R3 to RADIUS server SRV1 (10.1.50.1) succeed.
- Using SSH from PC-C to R3 fails.

TT-B Issue 1

The backup running-config that was used to load R3 when it was replaced does not include the RSA keys that are required to support SSH. The RSA keys are not exportable, except when copying from the running-config to the startup-config. As a result, the SSH server is disabled, and R3 rejects all SSH attempts.

- SSH from PC-C to R3 using PuTTY is rejected with the message: `“Network error: Connection refused”`
- Telnet from PC-C to R3 using the command prompt also fails (as it should).
- The **`show line vty 0`** command on R3 indicates that the allowed input transport is SSH but not Telnet (as it should be).
- The **`show ip ssh`** command on R3 indicates that SSH is disabled on R3 and that it is necessary to create the RSA keys (of at least 768 bits).

Action: Create new RSA keys on R3 to support SSH. See the TT-B debrief for more information

Verification:

- SSH from PC-C to R3 opens the connection, R3 prompts for user access verification, and the RADIUS server authenticates the user.
- With additional testing, it is determined that you can connect via SSH to R3 from PC-B or DLS2, which should not be allowed. There must be another problem.

TT-B Issue 2

The ACL that is supposed to limit SSH access to R3 is not applied to the vty lines as it should be, but it is applied to the R3 F0/0 interface inbound. This allows any PC that can access R3 to use SSH to it if the user knows a valid username and password.

- Telnet from PC-B to R3 fails (it should).
- SSH from PC-B to R3 using PuTTY succeeds (it should not).
- SSH from DLS1 using the command **`ssh -l raduser 10.1.2.14`** prompts for a password and succeeds (it should not).
- The **`show ssh`** command on R3 indicates that there are multiple workstations (in addition to PC-C) connected to R3. Connections via SSH to R3 from PC-B, SRV1, or other hosts should not be allowed.
- The **`show users`** command on R3 indicates that there are multiple users logged in to R3.
- The **`show access-lists`** command on R3 verifies that an ACL that permits only PC-C (10.1.80.100) has been configured and that it has a number of matches against it.

- The **`show run | beg vty`** command on R3 confirms that the login authentication method list VTY_LINES is applied to the vty lines, and the only transport input allowed is SSH. The reference to ACL 1, which would limit access to only PC-B, is missing, but how did the ACL accumulate matches?
- The **`show run int fa0/0`** command on R3 indicates that the ACL is incorrectly applied to the R3 interface Fa0/0 inbound. This does not accomplish the goal of preventing vty access from workstations in the network other than PC-C.

Action: Remove the ACL from Fa0/0 and apply it to vty lines 0–4. See the TT-B debrief for more information

Verification: SSH from any host other than PC-C (PC-B or SRV1) to R3 fails. Only PC-C can connect to R3 via SSH.

Step 7: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with your instructor. The notes can include problems encountered, solutions applied, useful commands employed, alternate solutions, methods, and processes, and procedure and communication improvements.

____

____

____

____

____

____

____

Trouble Ticket TT-B Debrief—Instructor Notes

This trouble ticket consists of two configuration issues that affect remote administrative access using SSH.

TT-B Issue 1

The first problem is that the backup running-config that was used to load R3 does not have the RSA keys that are required for SSH. RSA keys are not stored in the configuration and are not transferred when you copy a configuration from one device to another. As a result, the SSH server is disabled, and R3 rejects all login attempts via SSH.

Note: The keys are stored in a separate non-volatile storage area when copying from the running-config to the startup-config so that they are available if the device is reloaded.

The **`show ip ssh`** command on R3 indicates that SSH is disabled on R3 and that it is necessary to create the RSA keys (of at least 768 bits). This can be accomplished using the following commands.

```
R3#show ip ssh
SSH Disabled - version 1.99
%Please create RSA keys (of at least 768 bits size) to enable SSH v2.
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits

R3(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R3.tshoot.net

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R3(config)#
```



```
*Dec  7 18:06:35.205: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Note: Be sure to copy the running-config to the startup-config after generating the RSA keys.

```
R3#copy running-config startup-config
```

TT-B Issue 2

The second problem is that the ACL that was created to limit SSH access to R3 is not applied to the vty lines as it should be, but it is applied to the R3 F0/0 interface inbound where it allows any type of traffic sourced from PC-C (10.1.80.1). It prevents traffic other than 10.1.80.1 from entering F0/0, but it does not control SSH attempts from other networks that are accessible via the F0/1 interface. This allows any PC that can access R3 to use SSH if the user knows a valid username and password.

To correct this problem, remove the ACL from FA0/0 and apply it to the vty lines using the following commands.

```
interface fastEthernet 0/0
 no ip access-group 1 in

line vty 0 4
 access-class 1 in
```

Section 2—Troubleshooting Reference Information

General Troubleshooting Process

As a general guideline, you can use the following general troubleshooting process described in the course.

1. Define the problem (symptoms).
2. Gather information.
3. Analyze the information.
4. Propose a hypothesis (possible cause).
5. Test the hypothesis.
6. Eliminate or accept the hypothesis.
7. Solve the problem.
8. Document the problem.

Command Summary

The table lists useful commands for this lab. The sample output is shown on following pages.

Command	Key Information Displayed
show line vty 0	Displays the physical serial interface characteristics of a vty line as well as the transport input and output allowed (for example: Telnet or SSH).
show users	Displays device lines in use (for example: con, vty 0, vty 1), the username logged in, and the IP address of the connected host.
show radius server-group all	Displays the RADIUS servers defined in the group specified (default group is radius). The server IP address and port numbers are listed.
show radius statistics	Displays the RADIUS message statistics for authentication and accounting communication between the network device and the RADIUS server. Output includes packets with and without responses, response delay, and timeouts. Source port numbers are also listed.
debug radius authentication	Displays real-time interaction and message exchange between the network device, the calling station, and the RADIUS server. Authentication success or failure is indicated.
show aaa servers	Displays AAA server host information, including type (RADIUS or TACACS), IP address, port numbers in use, and AAA requests, successes, and failures.
show aaa method-lists all	Displays the names of AAA method lists currently defined, the type of validation in use, and the sequence of application (for example: server group, local, or none).
debug aaa authentication	Displays the method list defined and being used for AAA authentication (for example: TELNET_LINES).
debug aaa authorization	Displays the method list defined and being used for AAA authorization.

debug aaa accounting	Displays the method list defined and being used for AAA accounting.
show ip ssh	Displays SSH status (enabled or disabled), version number, timeout, retries, and key size in use (for example: 1024 bits).
show ssh	Displays active SSH connections with username, version, mode, encryption, HMAC, and state of the connection.
sh access-lists	Displays currently configured ACLs with type (for example: standard, extended) and name if one is assigned. ACL statements are listed with the number of matches for each one.
show ip interface fa0/0	Displays IP-related interface information, including any inbound or outbound access lists configured.

Sample Troubleshooting Output

VTY Line-related Commands

The following commands and outputs are samples from the devices in this lab.

```
DLS1#show line vty 0
   Tty Typ     Tx/Rx    A Modem  Roty AccO AccI   Uses   Noise  Overruns   Int
     1 VTY              -    -      -    -    -      4       0     0/0       -

Line 1, Location: "", Type: ""
Length: 24 lines, Width: 80 columns
Baud rate (TX/RX) is 9600/9600
Status: Ready, No Exit Banner
Capabilities: none
Modem state: Ready
Special Chars: Escape  Hold  Stop  Start  Disconnect  Activation
                ^^x    none   -     -       none
Timeouts:      Idle EXEC    Idle Session   Modem Answer  Session    Dispatch
               01:00:00        never                        none     not set
                            Idle Session Disconnect Warning
                              never
                            Login-sequence User Response
                             00:00:30
                            Autoselect Initial Wait
                              not set
Modem type is unknown.
Session limit is not set.
Time since activation: never
Editing is enabled.
History is enabled, history size is 20.
DNS resolution in show commands is enabled
Full user help is disabled
Allowed input transports are ssh.
Allowed output transports are telnet ssh.
Preferred transport is telnet.
No output characters are padded
No special data dispatching characters
```


In the above example, DLS1 allows only SSH as an input transport protocol on vty lines, but it allows both SSH and Telnet on output.

```
R3#show users
    Line       User       Host(s)              Idle       Location
*  0 con 0                idle                 00:00:00
 194 vty 0     raduser    idle                 00:22:52 10.1.80.100
 195 vty 1     admin      idle                 00:00:22 10.1.50.1
```

In the above example, two users are logged in to R3 using the vty lines (could be Telnet or SSH), one from host 10.1.80.100 and one from host 10.1.50.1.

RADIUS-related Commands

```
DLS1#show radius server-group all
Sever group radius
    Sharecount = 1  sg_unconfigured = FALSE
    Type = standard  Memlocks = 1
    Server(10.1.50.1:1645,1646) Transactions:
    Authen: Not Available   Author:Not Available  Acct:Not Available
```

In the above example, DLS1 is configured to access a RADIUS server at IP address 10.1.50.1, using ports 1645 and 1646. No transaction have taken place.

```
DLS1#show radius statistics
                                  Auth.      Acct.       Both
         Maximum inQ length:         NA         NA          1
       Maximum waitQ length:         NA         NA          1
       Maximum doneQ length:         NA         NA          1
       Total responses seen:          0          0          0
     Packets with responses:          0          0          0
  Packets without responses:          4          0          4
 Average response delay(ms):          0          0          0
 Maximum response delay(ms):          0          0          0
  Number of Radius timeouts:         16          0         16
       Duplicate ID detects:          0          0          0
 Buffer Allocation Failures:          0          0          0
Maximum Buffer Size (bytes):         82          0         82
 Source Port Range: (2 ports only)
 1645 - 1646
 Last used Source Port/Identifier:
 1645/4
 1646/0
```

In the above example, DLS1 has attempted to contact the server 16 times (four attempted logins with four retries each), and all attempts have timed out due to lack of accessibility of the server.

```
DLS1#debug radius authentication
Radius protocol debugging is on
Radius protocol brief debugging is off
Radius protocol verbose debugging is off
Radius packet hex dump debugging is off
Radius packet protocol debugging is on
Radius packet retransmission debugging is off
Radius server fail-over debugging is off
Radius elog debugging is off
```


Login attempt with incorrect RADIUS ports specified on DLS1:

```
DLS1#
Dec  4 16:06:50.142: RADIUS/ENCODE(00000005): ask "Username: "
DLS1#
Dec  4 16:06:59.430: RADIUS/ENCODE(00000005): ask "Password: "
DLS1#
Dec  4 16:07:05.487: RADIUS/ENCODE(00000005):Orig. component type = EXEC
Dec  4 16:07:05.487: RADIUS:  AAA Unsupported Attr: interface         [170] 4

Dec  4 16:07:05.487: RADIUS:   74 74                [ tt]
Dec  4 16:07:05.487: RADIUS/ENCODE(00000005): dropping service type, "radius-server
attribute 6 on-for-login-auth" is off
Dec  4 16:07:05.487: RADIUS(00000005): Config NAS IP: 0.0.0.0
Dec  4 16:07:05.487: RADIUS/ENCODE(00000005): acct_session_id: 5
Dec  4 16:07:05.487: RADIUS(00000005): sending
Dec  4 16:07:05.487: RADIUS/ENCODE: Best Local IP-Address 10.1.50.252 for Radius
-Server 10.1.50.1
Dec  4 16:07:05.487: RADIUS(00000005): Send Access-Request to 10.1.50.1:1645 id
1645/5, len 82
Dec  4 16:07:05.487: RADIUS:  authenticator B5 DF D2 00 81 8A C0 08 - 5E 68 DA A
9 59 01 7A 00
Dec  4 16:07:05.487: RADIUS:  User-Name           [1]   9   "raduser"
Dec  4 16:07:05.487: RADIUS:  User-Password       [2]   18  *
Dec  4 16:07:05.487: RADIUS:  NAS-Port            [5]   6   1

DLS1#
Dec  4 16:07:05.487: RADIUS:  NAS-Port-Id         [87]  6   "tty1"
Dec  4 16:07:05.487: RADIUS:  NAS-Port-Type       [61]  6   Virtual
      [5]
Dec  4 16:07:05.487: RADIUS:  Calling-Station-Id  [31]  11  "10.1.10.1"
Dec  4 16:07:05.487: RADIUS:  NAS-IP-Address      [4]   6   10.1.50.252

DLS1#
Dec  4 16:07:10.370: RADIUS: Retransmit to (10.1.50.1:1645,1646) for id 1645/5
DLS1#
Dec  4 16:07:15.269: RADIUS: Retransmit to (10.1.50.1:1645,1646) for id 1645/5
DLS1#
Dec  4 16:07:20.403: RADIUS: Retransmit to (10.1.50.1:1645,1646) for id 1645/5
DLS1#
Dec  4 16:07:25.370: %RADIUS-4-RADIUS_DEAD: RADIUS server 10.1.50.1:1645,1646 is
 not responding.
Dec  4 16:07:25.370: %RADIUS-4-RADIUS_ALIVE: RADIUS server 10.1.50.1:1645,1646 h
as returned.
DLS1#
Dec  4 16:07:25.370: RADIUS: No response from (10.1.50.1:1645,1646) for id 1645/
5
Dec  4 16:07:25.370: RADIUS/DECODE: parse response no app start; FAIL
Dec  4 16:07:25.370: RADIUS/DECODE: parse response; FAIL
DLS1#
Dec  4 16:07:27.375: RADIUS/ENCODE(00000005): ask "Username: "
```

The above example shows the exchange between the RADIUS client and server when the client is using port numbers that do not match the server. Note the retransmits and the server dead messages.

Successful login from PC-B (using valid username raduser on the RADIUS server):


```
DLS1(config)#
Dec  6 17:04:47.577: RADIUS/ENCODE(0000000F): ask "Username: "
DLS1(config)#
Dec  6 17:04:55.715: RADIUS/ENCODE(0000000F): ask "Password: "
DLS1(config)#
Dec  6 17:05:05.439: RADIUS/ENCODE(0000000F):Orig. component type = EXEC
Dec  6 17:05:05.439: RADIUS:  AAA Unsupported Attr: interface         [170] 4

Dec  6 17:05:05.439: RADIUS:   74 74                [ tt]
Dec  6 17:05:05.439: RADIUS/ENCODE(0000000F): dropping service type, "radius-ser
ver attribute 6 on-for-login-auth" is off
Dec  6 17:05:05.439: RADIUS(0000000F): Config NAS IP: 0.0.0.0
Dec  6 17:05:05.439: RADIUS/ENCODE(0000000F): acct_session_id: 15
Dec  6 17:05:05.439: RADIUS(0000000F): se
DLS1(config)#nding
Dec  6 17:05:05.439: RADIUS/ENCODE: Best Local IP-Address 10.1.50.252 for Radius
-Server 10.1.50.1
Dec  6 17:05:05.439: RADIUS(0000000F): Send Access-Request to 10.1.50.1:1812 id
1645/12, len 82
Dec  6 17:05:05.439: RADIUS:  authenticator 7E D1 DF 37 75 69 EC 91 - 42 FC 2E 7
8 D7 9B 5B 3B
Dec  6 17:05:05.439: RADIUS:  User-Name           [1]   9   "raduser"
Dec  6 17:05:05.439: RADIUS:  User-Password       [2]   18  *
Dec  6 17:05:05.439: RADIUS:  NAS-Port            [5]   6   1
DLS1(config)#
Dec  6 17:05:05.439: RADIUS:  NAS-Port-Id         [87]  6   "tty1"
Dec  6 17:05:05.439: RADIUS:  NAS-Port-Type       [61]  6   Virtual
      [5]
Dec  6 17:05:05.439: RADIUS:  Calling-Station-Id  [31]  11  "10.1.10.1"
Dec  6 17:05:05.439: RADIUS:  NAS-IP-Address      [4]   6   10.1.50.252

Dec  6 17:05:05.447: RADIUS: Received from id 1645/12 10.1.50.1:1812, Access-Acc
ept, len 26
Dec  6 17:05:05.447: RADIUS:  authenticator 75 81 E4 CD 45 1D F6 14 - 5D 1F AD F
4 D4 83 D
DLS1(config)#5 FE
Dec  6 17:05:05.447: RADIUS:  Session-Timeout     [27]  6   9999999

Dec  6 17:05:05.447: RADIUS(0000000F): Received from id 1645/12
```

The above example shows the exchange between the RADIUS client and server when the client is using the same port numbers as the server and a legitimate user attempts to login. Note the Access-Accept message.

Unsuccessful login from PC-B (using invalid username baduser):

```
DLS1(config)#
Dec  6 17:10:00.346: RADIUS/ENCODE(00000010): ask "Username: "
DLS1(config)#
Dec  6 17:10:06.722: RADIUS/ENCODE(00000010): ask "Password: "
DLS1(config)#
Dec  6 17:10:16.580: RADIUS/ENCODE(00000010):Orig. component type = EXEC
Dec  6 17:10:16.580: RADIUS:  AAA Unsupported Attr: interface         [170] 4

Dec  6 17:10:16.580: RADIUS:   74 74                [ tt]
Dec  6 17:10:16.580: RADIUS/ENCODE(00000010): dropping service type, "radius-ser
ver attribute 6 on-for-login-auth" is off
```



```
Dec  6 17:10:16.580: RADIUS(00000010): Config NAS IP: 0.0.0.0
Dec  6 17:10:16.580: RADIUS/ENCODE(00000010): acct_session_id: 16
Dec  6 17:10:16.580: RADIUS(00000010): se
DLS1(config)#nding
Dec  6 17:10:16.580: RADIUS/ENCODE: Best Local IP-Address 10.1.50.252 for Radius
-Server 10.1.50.1
Dec  6 17:10:16.580: RADIUS(00000010): Send Access-Request to 10.1.50.1:1812 id
1645/13, len 82
Dec  6 17:10:16.580: RADIUS:  authenticator 17 3A 1D 34 81 4C F1 6F - 89 62 05 1
3 14 8F 33 4B
Dec  6 17:10:16.580: RADIUS:  User-Name           [1]   9   "baduser"
Dec  6 17:10:16.580: RADIUS:  User-Password       [2]   18  *
Dec  6 17:10:16.580: RADIUS:  NAS-Port            [5]   6   1
Dec  6 17:10:16.580: RADIUS:  NAS-Port-Id         [87]  6   "tty1"
Dec  6 17:10:16.580: RADIUS:  NAS-Port-Type       [61]  6   Virtual
      [5]
Dec  6 17:10:16.580: RADIUS:  Calling-Station-Id  [31]  11  "10.1.10.1"
Dec  6 17:10:16.580: RADIUS:  NAS-IP-Address      [4]   6   10.1.50.252

Dec  6 17:10:16.588: RADIUS: Received from id 1645/13 10.1.50.1:1812, Access-Rej
ect, len 20
Dec  6 17:10:16.588: RADIUS:  authenticator 81 34 66 76 58 03 AF 9B - CF D5 93 F
2 C6 13 6
DLS1(config)#7 7D
Dec  6 17:10:16.588: RADIUS(00000010): Received from id 1645/13
Dec  6 17:10:18.593: RADIUS/ENCODE(00000010): ask "Username: "
```

The above example shows the exchange between the RADIUS client and server when the client is using the same port numbers as the server and a bad login is attempted (nonexistent username and bad password). Note the Access-Reject message. Switch DLS1 then prompts immediately to allow entry of a correct username and password combination.

AAA-related Commands

Incorrect RADIUS port numbers:

```
DLS1#show aaa servers

RADIUS: id 2, priority 1, host 10.1.50.1, auth-port 1645, acct-port 1646
     State: current UP, duration 13752s, previous duration 0s
     Dead: total time 0s, count 0
     Quarantined: No
     Authen: request 8, timeouts 8
             Response: unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction: success 0, failure 2

<output omitted>
```

The above example shows that the AAA server is RADIUS and lists the IP address and ports defined on the client. Note the eight requests and eight timeouts, resulting in two failed authentication attempts.

Correct RADIUS port numbers:

```
R3#show aaa servers
RADIUS: id 1, priority 1, host 10.1.50.1, auth-port 1812, acct-port 1813
     State: current UP, duration 23188s, previous duration 0s
```



```
     Dead: total time 0s, count 0
     Quarantined: No
     Authen: request 0, timeouts 0, failover 0, retransmission 0
             Response: accept 0, reject 0, challenge 0
             Response: unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction: success 2, failure 0
             Throttled: transaction 0, timeout 0, failure 0
     Author: request 0, timeouts 0, failover 0, retransmission 0
             Response: accept 0, reject 0, challenge 0
             Response: unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction: success 0, failure 0
             Throttled: transaction 0, timeout 0, failure 0
     Account: request 0, timeouts 0, failover 0, retransmission 0
             Request: start 0, interim 0, stop 0
             Response: start 0, interim 0, stop 0
             Response: unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction: success 0, failure 0
             Throttled: transaction 0, timeout 0, failure 0
```

The above example shows that the AAA server is RADIUS and lists the IP address and ports defined on the client. Note the two successful authentication transactions.

```
R3#show aaa method-lists all
authen queue=AAA_ML_AUTHEN_LOGIN
  name=default valid=TRUE id=0 :state=ALIVE : LOCAL
  name=CONSOLE valid=TRUE id=2B000001 :state=ALIVE : NONE
  name=VTY_LINES valid=TRUE id=87000002 :state=ALIVE : SERVER_GROUP radius LOCAL

authen queue=AAA_ML_AUTHEN_ENABLE
authen queue=AAA_ML_AUTHEN_PPP
authen queue=AAA_ML_AUTHEN_SGBP
authen queue=AAA_ML_AUTHEN_ARAP
authen queue=AAA_ML_AUTHEN_DOT1X
authen queue=AAA_ML_AUTHEN_EAPOUDP
authen queue=AAA_ML_AUTHEN_8021X
permanent lists
  name=Permanent Enable None valid=TRUE id=0 :state=ALIVE : ENABLE  NONE
  name=Permanent Enable valid=TRUE id=0 :state=ALIVE : ENABLE
  name=Permanent None valid=TRUE id=0 :state=ALIVE : NONE
  name=Permanent Local valid=TRUE id=0 :state=ALIVE : LOCAL
author queue=AAA_ML_AUTHOR_SHELL
  name=VTY_LINES valid=TRUE id=61000003 :state=ALIVE : SERVER_GROUP radius LOCAL
<output omitted>
```

The above example shows the names of the AAA method lists currently defined, the type of validation in use, and the sequence of application (for example: server group, local, or none).

```
DLS1#debug aaa authentication
AAA Authentication debugging is on
DLS1#
Dec  7 15:48:21.869: AAA/BIND(0000000C): Bind i/f
Dec  7 15:48:21.869: AAA/AUTHEN/LOGIN (0000000C): Pick method list 'TELNET_LINES
'
```

The above example shows the method list defined and being used for AAA authentication (TELNET_LINES).


```
DLS1#debug aaa authorization
AAA Authorization debugging is on
DLS1#
Dec  7 16:06:34.836: AAA/AUTHOR (0xD): Pick method list 'default' - FAIL
Dec  7 16:06:34.844: AAA/AUTHOR/EXEC(0000000D): Authorization FAILED
```

The above example shows the method list defined and being used for AAA authorization (default). Note that the authorization attempt failed.

SSH-related Commands

```
R3#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits

R3#show ip ssh
SSH Disabled - version 1.99
%Please create RSA keys (of at least 768 bits size) to enable SSH v2.
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
```

The first example above shows the output when the RSA keys have been created and SSH is enabled. The second example shows the output when there are no RSA keys and SSH is disabled.

```
R3#show ssh
Connection Version Mode Encryption  Hmac         State                 Username
0          2.0     IN   aes256-cbc  hmac-sha1    Session started       raduser
0          2.0     OUT  aes256-cbc  hmac-sha1    Session started       raduser
1          2.0     IN   aes256-cbc  hmac-sha1    Session started       admin
1          2.0     OUT  aes256-cbc  hmac-sha1    Session started       admin
%No SSHv1 server connections running.
```

The above example shows active SSH connections with the username, version, mode, encryption, HMAC, and state of the connection.

ACL-related Commands

```
R3#show access-lists
Standard IP access list 1
    10 permit 10.1.80.100 (77 matches)
```

The above example shows the currently configured ACLs with the type, number (if one is assigned), statements, and the number of matches for each one.

```
R3#show ip interface fa0/0
FastEthernet0/0 is up, line protocol is up
  Internet address is 10.1.80.1/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is not set
```

```
  Inbound  access list is 1
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF switching turbo vector

<output omitted>
```

The above example shows IP-related interface information, including any inbound or outbound access lists configured

Reflection Questions

1. Which lab trouble tickets did you have the most difficulty with?

____
____
____

2. Would you change anything about the process that you used for any of the trouble tickets now that you see the resolution of the problem?

____
____
____

3. Which commands did you find most useful in diagnosing management plane security issues? Add these to your toolbox for future use. Which commands did you find least useful?

____
____
____

References

If you need more information on the commands and their options, see the following references:

- IP Routing Protocol
  http://www.cisco.com/cisco/web/support/index.html
- Cisco IOS IP Switching
  http://www.cisco.com/en/US/docs/ios/ipswitch/command/reference/isw_book.html
- Configuring SSH on Routers and Switches Running Cisco IOS Software
  http://www.cisco.com/en/US/tech/tk583/tk617/technologies_tech_note09186a00800949e2.shtml
- SSH FAQ
  http://www.cisco.com/en/US/tech/tk583/tk617/technologies_q_and_a_item09186a0080267e0f.shtml

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1700	Fast Ethernet 0 (FA0)	Fast Ethernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
1800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2600	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)
2800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. Rather than try to list all the combinations of configurations for each router class, this table includes identifiers for the possible combinations of Ethernet and serial interfaces in the device. The table does not include any other type of interface, even though a specific router might contain one. An example of this is an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

Appendix A—WinRadius Server Installation

Note: A WinRadius (or comparable) server should be installed on server SRV1 for this lab. If it is not, you can use the following procedure to download and install it. Check with your instructor if you have questions regarding the RADIUS server installation.

Step 1: Download the WinRadius software.

A number of RADIUS servers are available, both freeware and for sale. This lab uses WinRadius, a freeware standards-based RADIUS server that runs on Windows XP and most other Windows operating systems.

Note: The free version of the software can support only five usernames.

Step 2: Install the WinRadius software.

a. Create a folder named WinRadius on your desktop or other location in which to store the files.

b. Search the web for **winradius** and download the latest version from a trusted website.

Instructor note: The instructions provided in this lab are for WinRadius 4.0. However, you can use another RADIUS server if one is available.

c. Save the downloaded zip file in the folder created in Step 2a, and extract the zipped files to the same folder. There is no installation setup. The extracted WinRadius.exe file is executable.

d. You can create a shortcut on your desktop for WinRadius.exe.

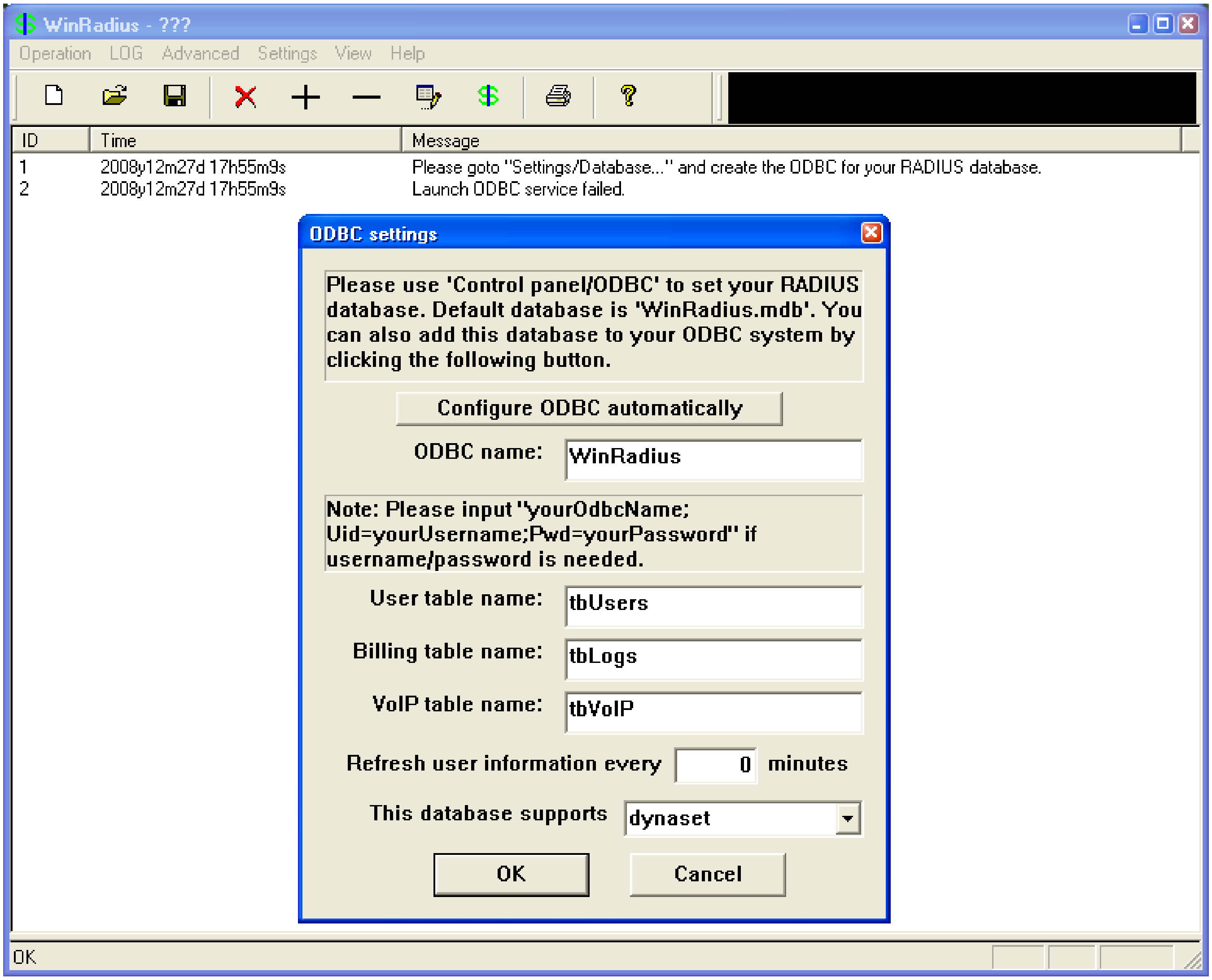
Step 3: Configure the WinRadius server database.

a. Start the WinRadius.exe application. WinRadius uses a local database in which it stores user information. When the application is started for the first time, the following messages are displayed:

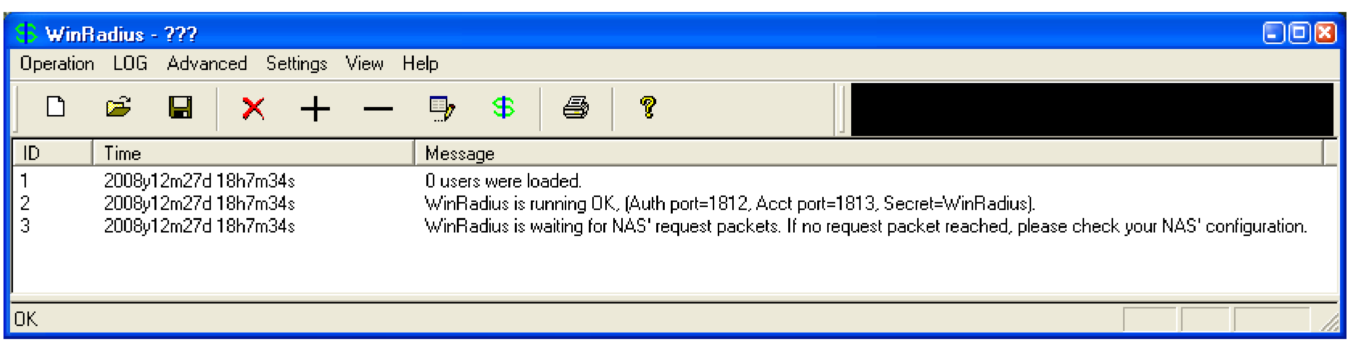
```
Please go to “Settings/Database and create the ODBC for your RADIUS
database.

Launch ODBC failed.
```

b. From the main menu, select **Settings > Database**.

c. Click the **Configure ODBC automatically** button and then click **OK**. You should see a message that the ODBC was created successfully. Exit WinRadius and restart the application for the changes to take effect.



d. When WinRadius starts again, you should see messages similar to the following:



Instructor note: WinRadius listens for authentication on port 1812 and accounting on port 1813.

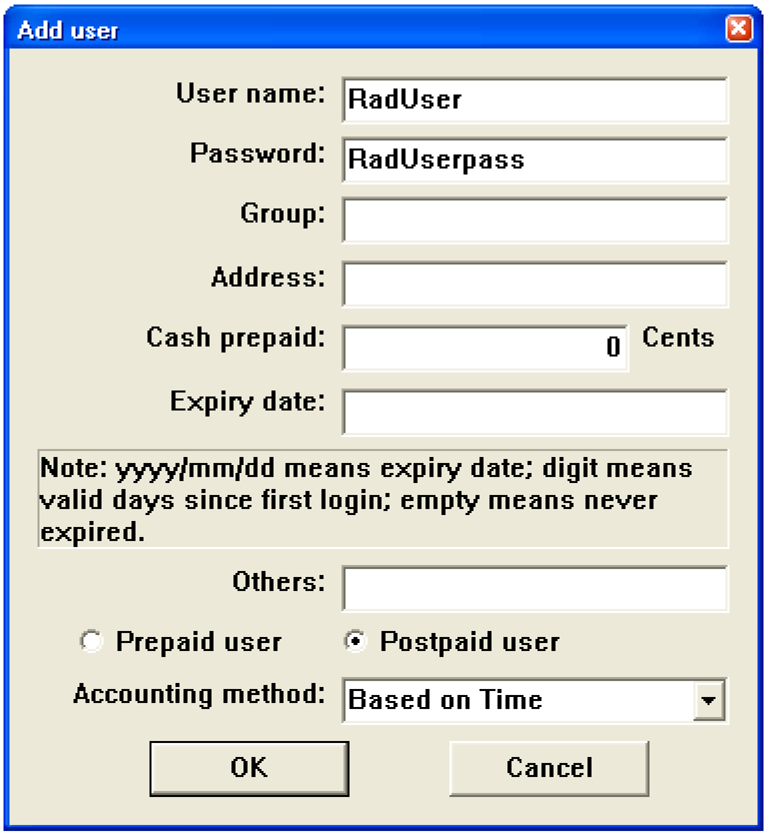
Step 4: Configure users and passwords on the WinRadius server.

Note: The free version of WinRadius can support only five usernames at a time. The usernames are lost if you exit the application and restart it. Any usernames created in previous sessions must be recreated. The first message in the previous screen shows that zero users were loaded. No users had been created prior to this, but this message is displayed each time WinRadius is started, regardless of whether users were created or not.

a. From the main menu, select **Operation > Add User.**

b. Enter the username **raduser** with a password of **RadUserpass.**

Note: The lab specifies the username **raduser** in lowercase. The example here creates user **RadUser**.



c. Click **OK**. You should see a message on the log screen that the user was added successfully.

Step 5: Clear the log display.

From the main menu, select **Log > Clear**.

Step 6: Test the new user added using the WinRadius test utility.

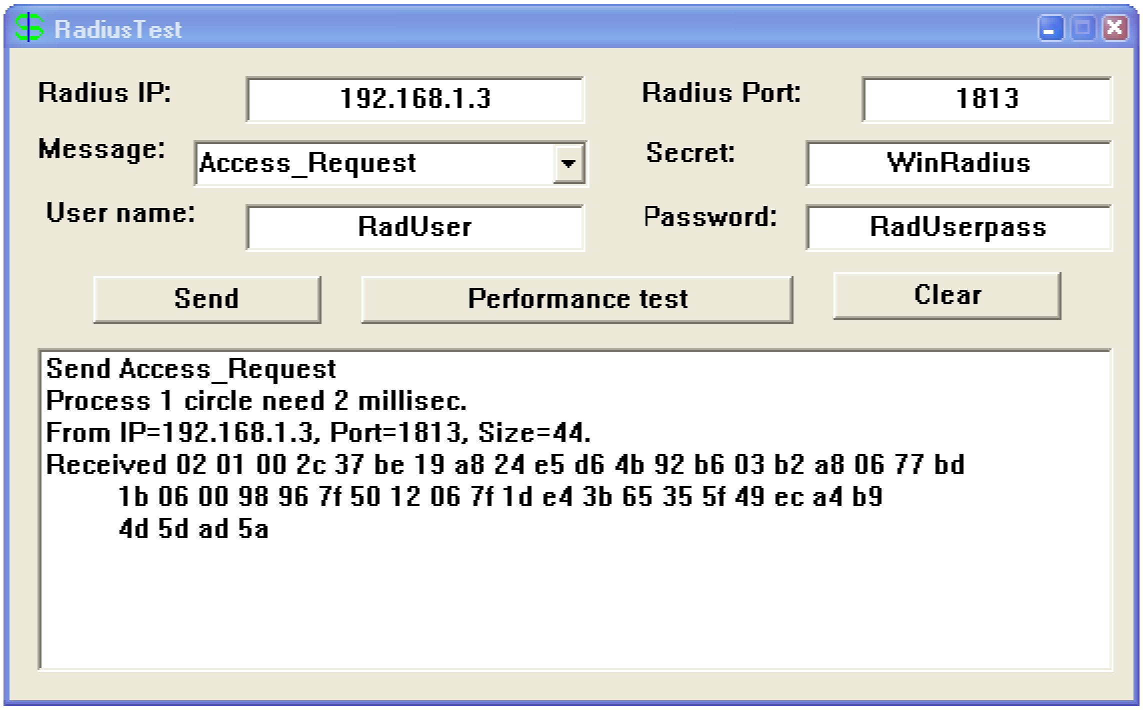
a. A WinRadius testing utility is included in the downloaded zip file. Navigate to the folder where you unzipped the WinRadius.zip file and locate the file named RadiusTest.exe.

b. Start the RadiusTest application, and enter the IP address of the RADIUS server. For this lab, the RADIUS server is SRV1, and the IP address is 10.1.50.1. The IP address of the RADIUS server in the example shown here is 192.168.1.3.

c. Enter username **raduser** and password **RadUserpass**. Do not change the default RADIUS port number of 1813 nor the RADIUS password of WinRadius.

Note: Be sure to use the IP address of SRV1 in this lab (10.1.50.1) when testing.

d. Click **Send** and you should see a Send Access_Request message indicating that the server at 10.1.50.1, port number 1813, received 44 hexadecimal characters. On the WinRadius log display, you should also see a message indicating that user raduser was authenticated successfully.



e. Close the RadiusTest application.

Device Configurations (instructor version)

Note: All device configurations are provided for TT-A. The configs provided here are *not* running-config outputs. They can be used for cut-and-paste for TT-A and subsequent tickets. Where a config is noted as being the same as a previous one, the only change is in the MOTD, which identifies the Lab and TT. The errors in the configuration are commented and highlighted as red text.

Trouble Ticket—TT-A Configurations

Switch ALS1

```
!Lab 9-1 Switch ALS1 TT-A Config
!
hostname ALS1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 9-1 Switch ALS1 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
```



```
spanning-tree mode rapid-pvst
spanning-tree portfast default
!
interface Vlan1
 no ip address
 shutdown
!
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 100
 name MGMT
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel1
 description Channel to DLS1
 no shutdown
 !
interface Port-channel2
 description Channel to DLS2
 no shutdown
!
interface FastEthernet0/1
 description Channel to DLS1
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shutdown
!
interface FastEthernet0/2
 description Channel to DLS1
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shutdown
!
interface FastEthernet0/3
 description Channel to DLS2
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
```



```
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shutdown
!
interface FastEthernet0/4
 description Channel to DLS2
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shutdown
!
interface FastEthernet0/5
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown

interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
```



```
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description To PC-B
 switchport access vlan 10
 switchport mode access
 switchport voice vlan 20
 spanning-tree portfast
 switchport port-security
 switchport port-security maximum 2
 switchport port-security violation shutdown
 switchport port-security mac-address sticky
 no shut
```



```
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan100
```



```
 ip address 10.1.100.1 255.255.255.0
 no shutdown
!
ip default-gateway 10.1.100.254
!
ip http server
ip http secure-server
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server host 10.1.50.1 version 2c cisco
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps vlan-membership
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
  no transport input
!
ntp source Vlan100
ntp server 192.168.2.1
end
```

Switch DLS1

```
!Lab 9-1 Switch DLS1 TT-A Config
!
hostname DLS1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55

banner motd $*** Lab 9-1 Switch DLS1 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
```



```
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authentication login TELNET_LINES group radius local
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
!
ip domain name tshoot.net
!
ip dhcp excluded-address 10.1.10.252 10.1.10.254
ip dhcp excluded-address 10.1.20.252 10.1.20.254
ip dhcp excluded-address 10.1.30.252 10.1.30.254
!
ip dhcp pool OFFICE
   network 10.1.10.0 255.255.255.0
   default-router 10.1.10.254
   domain-name tshoot.net
!
ip dhcp pool VOICE
   network 10.1.20.0 255.255.255.0
   default-router 10.1.20.254
   domain-name tshoot.net
!
ip dhcp pool GUEST
   network 10.1.30.0 255.255.255.0
   default-router 10.1.30.254
   domain-name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 24576
spanning-tree vlan 20,50 priority 28672
!
vlan 10
 name OFFICE
!
vlan 20
```

Error: AAA authorization for EXEC access defaults to local instead accessing RADIUS server for Telnet.

no aaa authorization exec default local

aaa authorization exec TELNET_LINES group radius local


```
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 100
 name MGMT
!
vlan 200
 name TRANS
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel1
 description Channel to ALS1
 no shut
!
interface Port-channel10
 description Channel to DLS2
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
```



```
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R1
 no switchport
 ip address 10.1.2.1 255.255.255.252
 speed 100
 duplex full
 spanning-tree bpduguard enable
 no shut
!
interface FastEthernet0/6
 description FE to SRV1
 switchport access vlan 50
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shut
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
```

```
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/19
 description Unused
```



```
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
```



```
interface Vlan10
 ip address 10.1.10.252 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 priority 110
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.252 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.252 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 priority 110
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.252 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 preempt
!
interface Vlan100
 ip address 10.1.100.252 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 priority 110
 standby 100 preempt
!
interface Vlan200
 ip address 10.1.200.252 255.255.255.0
!
router eigrp 1
 passive-interface default
 no passive-interface Fa0/5
 no passive-interface vlan200
 no auto-summary
 network 10.1.0.0 0.0.255.255
!
ip classless
ip http server
ip http secure-server
!
logging source-interface Vlan100
logging 10.1.50.1
radius-server host 10.1.50.1 key WinRadius
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server host 10.1.50.1 version 2c cisco
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps config
```

Error: The **radius-server host** command does not specify the ports used by the RADIUS server (1812 and 1813). The IOS default ports are 1645 and 1646. Remove the existing radius-server host and re-enter it with the correct ports.

no radius-server host 10.1.50.1 auth-port 1645 acct-port 1646

radius-server host 10.1.50.1 auth-port 1812 acct-port 1813 key WinRadius

```
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input ssh
 login authentication TELNET_LINES
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 192.168.2.1
end
```

Error: Telnet is not specified as an allowable input transport.

```
line vty 0 4
 transport input telnet ssh
```

Switch DLS2

```
!Lab 9-1 Switch DLS2 TT-A Config
!
hostname DLS2
!
service timestamps debug datetime msec
service timestamps log datetime
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 9-1 Switch DLS2 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
```



```
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
  path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 28672
spanning-tree vlan 20,50 priority 24576

vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 100
 name MGMT
!
vlan 200
 name TRANS
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel2
 description Channel to ALS1
 no shut

interface Port-channel10
 description Channel to DLS1
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
```



```
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R3
 no switchport
 ip address 10.1.2.13 255.255.255.252
 speed 100
 duplex full
 spanning-tree bpduguard enable
 no shutdown
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
```



```
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
```



```
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
```

```
interface GigabitEthernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 10.1.10.253 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.253 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 priority 110
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.253 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.253 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 priority 110
 standby 50 preempt
!
interface Vlan100
 ip address 10.1.100.253 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 preempt
!
interface Vlan200
 ip address 10.1.200.253 255.255.255.0
!
router eigrp 1
 passive-interface default
 no passive-interface Fa0/5
 no passive-interface vlan200
 no auto-summary
 network 10.1.0.0 0.0.255.255
!
ip classless
ip http server
ip http secure-server
```



```
!
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 192.168.2.1
end
```

Router R1

```
!Lab 9-1 Router R1 TT-A Config
!
hostname R1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 9-1 Router R1 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
```



```
!
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 192.168.1.1 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown
!
interface FastEthernet0/1
 description FE to DLS1
 ip address 10.1.2.2 255.255.255.252
 ip flow ingress
 ip nat inside
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
 description WAN link to ISP R2
 ip address 209.165.200.225 255.255.255.252
 ip nat outside
 ip flow ingress
 encapsulation ppp
 clock rate 128000
  no shutdown
!
interface Serial0/0/1
 shutdown
!
router eigrp 1
 redistribute static
 passive-interface default
 no passive-interface FastEthernet0/1
 network 10.1.2.0 0.0.0.3
 network 192.168.1.1 0.0.0.0
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 209.165.200.226
!
ip http server
no ip http secure-server
```



```
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
ip nat pool public-addrs 198.133.219.10 198.133.219.30 netmask 255.255.255.224
ip nat inside source list 1 pool public-addrs
ip nat inside source static 10.1.50.1 198.133.219.1
!
logging source-interface Loopback0
logging 10.1.50.1
!
access-list 1 permit 10.1.0.0 0.0.255.255
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 192.168.2.1
end
```

Router R2

```
!Lab 9-1 Router R2 TT-A Config
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
Hostname R2
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 9-1 Router R2 TT-A Config ***$
!
no ip domain lookup
!
```



```
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 192.168.2.1 255.255.255.255
!
interface FastEthernet0/0
 shutdown
!
interface FastEthernet0/1
 shutdown
!
interface Serial0/0/0
 description WAN link to R1 – T1 leased line
 ip address 209.165.200.226 255.255.255.252
 encapsulation ppp
 no shutdown
 !
interface Serial0/0/1
 shutdown
!
ip route 192.168.1.1 255.255.255.255 209.165.200.225
ip route 198.133.219.0 255.255.255.224 209.165.200.225
!
ip http server
no ip http secure-server
!
logging source-interface Loopback0
logging 10.1.50.1
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
```



```
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
!
ntp master 3
 end
```

Router R3

```
!Lab 9-1 Router R3 TT-A Config
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 9-1 Router R3 TT-A Config ***$
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
no ip domain lookup
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 10.1.203.1 255.255.255.255
!
interface FastEthernet0/0
```



```
 description FE to R3 LAN
 ip address 10.1.80.1 255.255.255.0
 ip flow ingress
 speed 100
 full-duplex
 no shutdown
!
interface FastEthernet0/1
 description FE to DLS2
 ip address 10.1.2.14 255.255.255.252
 ip flow ingress
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
description WAN link to R1 – not used for this lab
 no ip address
 clock rate 128000
 encapsulation ppp
 shutdown
!
interface Serial0/0/1
 description WAN link to R2 - not used for this lab
 no ip address
 encapsulation ppp
 shutdown
!
router eigrp 1
 passive-interface default
 no passive-interface FastEthernet0/1
 network 10.1.2.12 0.0.0.3
 network 10.1.80.0 0.0.0.255
 network 10.1.203.1 0.0.0.0
 no auto-summary
!
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
logging source-interface Loopback0
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
```



```
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 192.168.2.1
end
```

Trouble Ticket—TT-B Configurations

Switch ALS1—Same as TT-A

Switch DLS2—Same as TT-A

Router R1—Same as TT-A

Router R2—Same as TT-A

Switch DLS1

```
!Lab 9-1 Switch DLS1 TT-B Config
!
hostname DLS1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55

banner motd $*** Lab 9-1 Switch DLS1 TT-B Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authentication login TELNET_LINES group radius local
aaa authorization exec TELNET_LINES group radius local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
!
ip domain name tshoot.net
!
```



```
ip dhcp excluded-address 10.1.10.252 10.1.10.254
ip dhcp excluded-address 10.1.20.252 10.1.20.254
ip dhcp excluded-address 10.1.30.252 10.1.30.254
!
ip dhcp pool OFFICE
   network 10.1.10.0 255.255.255.0
   default-router 10.1.10.254
   domain-name tshoot.net
!
ip dhcp pool VOICE
   network 10.1.20.0 255.255.255.0
   default-router 10.1.20.254
   domain-name tshoot.net
!
ip dhcp pool GUEST
   network 10.1.30.0 255.255.255.0
   default-router 10.1.30.254
   domain-name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 24576
spanning-tree vlan 20,50 priority 28672
!
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 100
 name MGMT
!
vlan 200
 name TRANS
!
vlan 900
 name NATIVE
```

```
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel1
 description Channel to ALS1
 no shut
!
interface Port-channel10
 description Channel to DLS2
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R1
 no switchport
```

```
 ip address 10.1.2.1 255.255.255.252
 speed 100
 duplex full
 spanning-tree bpduguard enable
 no shut
!
interface FastEthernet0/6
 description FE to SRV1
 switchport access vlan 50
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shut
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
```



```
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
```

```
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown

interface Vlan10
 ip address 10.1.10.252 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 priority 110
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.252 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.252 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 priority 110
 standby 30 preempt
```

```
!
interface Vlan50
 ip address 10.1.50.252 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 preempt
!
interface Vlan100
 ip address 10.1.100.252 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 priority 110
 standby 100 preempt
!
interface Vlan200
 ip address 10.1.200.252 255.255.255.0
!
router eigrp 1
 passive-interface default
 no passive-interface Fa0/5
 no passive-interface vlan200
 no auto-summary
 network 10.1.0.0 0.0.255.255
!
ip classless
ip http server
ip http secure-server
!
logging source-interface Vlan100
logging 10.1.50.1
radius-server host 10.1.50.1 auth-port 1812 acct-port 1813 key WinRadius
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server host 10.1.50.1 version 2c cisco
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
 login authentication TELNET_LINES
line vty 5 15
 no transport input
!
ntp source Vlan100
```



```
ntp server 192.168.2.1
```

Router R3

```
!Lab 9-1 Router R3 TT-B Config
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 9-1 Router R3 TT-B Config ***$
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authentication login VTY_LINES group radius local
aaa authorization exec VTY_LINES group radius local
!
no ip domain lookup
ip domain name tshoot.net
!
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 10.1.203.1 255.255.255.255
!
interface FastEthernet0/0
 description FE to R3 LAN
 ip address 10.1.80.1 255.255.255.0
 ip access-group 1 in
 ip flow ingress
 duplex full
 speed 100
 no shutdown
!
interface FastEthernet0/1
 description FE to DLS2
 ip address 10.1.2.14 255.255.255.252
 ip flow ingress
```

Error: Command to generate RSA keys for SSH is missing.

`crypto key generate rsa general-keys modulus 1024`

Error: ACL 1 should not be applied to R3 Fa0/0.

```
interface FastEthernet0/0
 no ip access-group 1 in
```



```
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
description WAN link to R1 – not used for this lab
 no ip address
 clock rate 128000
 encapsulation ppp
 shutdown
!
interface Serial0/0/1
 description WAN link to R2 - not used for this lab
 no ip address
 encapsulation ppp
 shutdown
!
router eigrp 1
 passive-interface default
 no passive-interface FastEthernet0/1
 network 10.1.2.12 0.0.0.3
 network 10.1.80.0 0.0.0.255
 network 10.1.203.1 0.0.0.0
 no auto-summary
!
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
logging source-interface Loopback0
logging 10.1.50.1
access-list 1 permit host 10.1.80.100
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input ssh
 login authentication VTY_LINES
!
ntp source Loopback0
ntp update-calendar
```

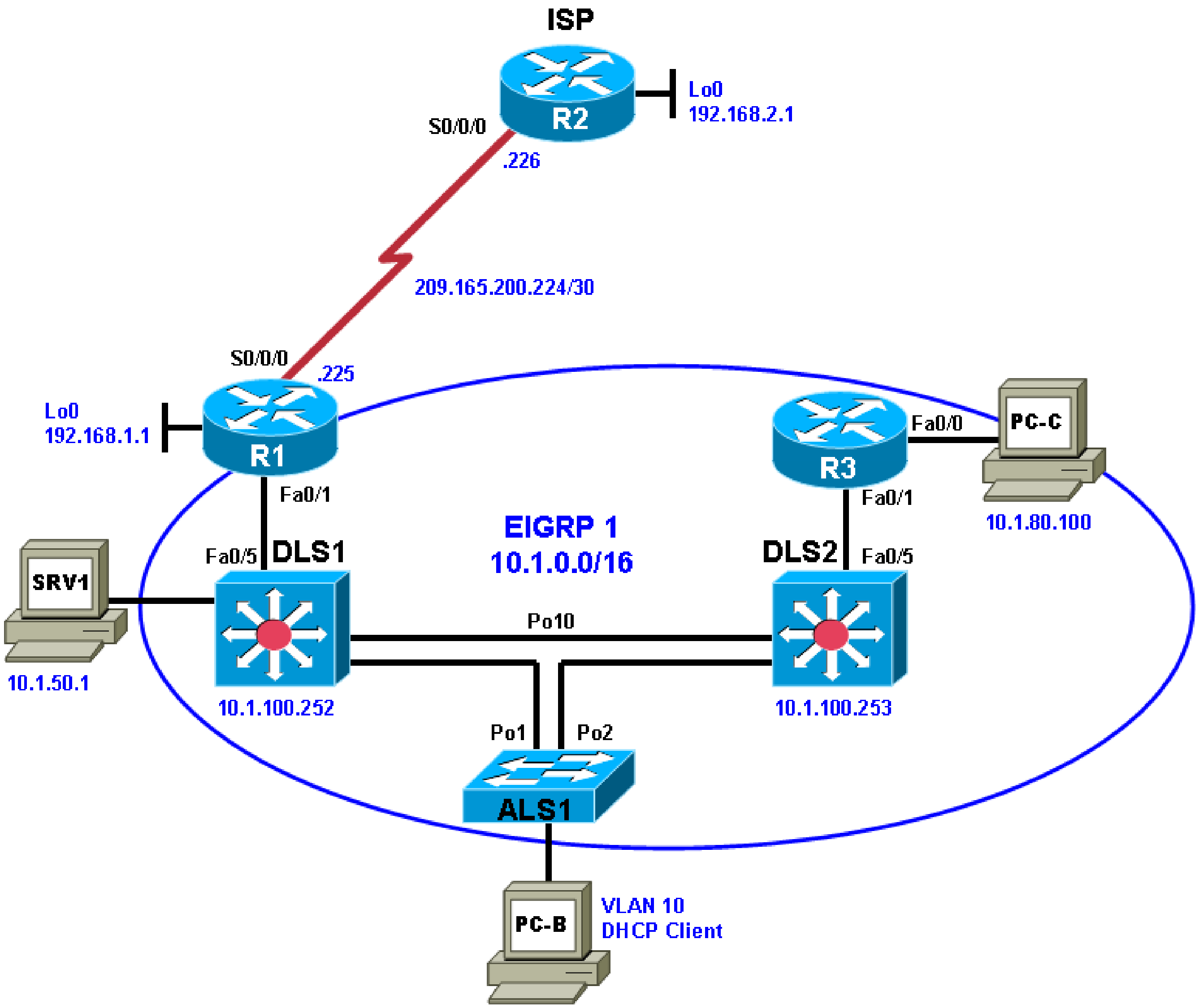
Error: ACL 1 is missing from VTY lines.

```
line vty 0 4
 access-class 1 in
```

```
ntp server 192.168.2.1
end
```


Chapter 9 Lab 9-2, Control Plane Security **Instructor Version**

Lab Topology



Objectives

- Load the device configuration files for each trouble ticket.
- Diagnose and resolve problems related to router and switch control plane security.
- Document the troubleshooting progress, configuration changes, and problem resolution.

Background

Routers and Layer 3 switches are typically segmented into three planes of operation, each with a clearly identified objective. The data plane (also called the forwarding plane) forwards user data packets. The control plane routes data correctly, and the management plane manages the network devices.

The control plane is typically associated with packets generated by the network elements themselves. End users typically do not interact with the control plane. Examples of Layer 3 control plane protocols and related security functions include neighbor authentication for routing protocols and HSRP. Examples of security-related Layer 2 control plane protocols include root guard, BPDU guard, DHCP snooping, Dynamic ARP Inspection, IP source guard, and the use of special VLANs for trunks and unused ports.

This lab focuses on control plane security issues related to DHCP snooping and EIGRP authentication for routers and Layer 3 switches.

For each task or trouble ticket, the trouble scenario and problem symptom is described. While troubleshooting, you will discover the cause of the problem, correct it, and then document the process and results.

Lab Structure

This lab is divided into two main sections.

Section 1—Trouble Tickets and Troubleshooting Logs

This section includes two tasks. Each task is associated with a trouble ticket (TT) and introduces one or more errors on one or more devices. If time is a consideration, each task or trouble ticket can be performed independently.

Section 2—Troubleshooting Reference Information

This section provides general troubleshooting information that can be applied to any of the trouble tickets in this lab. Examples of useful commands and output are provided. If time permits, it is recommended that you read through Section 2 prior to starting on the trouble tickets.

Instructor note: Because the troubleshooting reference section is lengthy, ask students to read through it prior to starting the lab to become familiar with the commands used in this lab. Consider assigning it as homework.

Note: This lab uses Cisco 1841 routers with Cisco IOS Release 12.4(24)T1 and the Advanced IP Services image c1841-advipservicesk9-mz.124-24.T1.bin. The switches are Cisco WS-C2960-24TT-L with the Cisco IOS image c2960-lanbasek9-mz.122-46.SE.bin and Catalyst 3560-24PS with the Cisco IOS image c3560-advipservicesk9-mz.122-46.SE.bin. Other routers (such as 2801 and 2811), switches (such as 2950 or 3550), and Cisco IOS Software versions can be used if they have comparable capabilities and features. Depending on the router or switch model and Cisco IOS Software version, the commands available and output produced might vary from what is shown in this lab.

Any changes made to configurations or topology (other than errors introduced) are noted in the lab and trouble tickets so that you are aware of them prior to beginning the troubleshooting process.

Instructor Notes

- The lab topology should be pre-built prior to the students starting the lab. Ensure that all routers and switches (R1, R2, R3, ALS1, DLS1, and DLS2) have the course lab configuration files installed in flash. You can download the files from the Academy Connection website.
- The device configurations that contain trouble ticket errors and modifications from the baseline are included at the end of the lab, and the errors in them are identified.
- Each device has a directory named “tshoot” in flash. This directory contains the baseline configuration file for that device as well as the configuration files for the labs in this course. Refer to Lab 3-1 for instructions on creating the tshoot directory in flash.

- Instructors can use a TFTP server, USB drive, flash memory card, or other method to copy all the course configuration files into the flash:/tshoot directory for each device in the topology.
- The student is responsible for loading the baseline or trouble ticket configurations as required using the procedure described in Lab 3-1.
- Set the correct time on router R2, which serves as the primary NTP server for the lab network.
- If time is an issue, each task (trouble ticket) can be performed independently.

Required Resources

- 3 routers (Cisco 1841 with Cisco IOS Release 12.4(24)T1 Advanced IP Service or comparable)
- 1 switch (Cisco 2960 with the Cisco IOS Release 12.2(46)SE C2960-LANBASEK9-M image or comparable)
- 2 switches (Cisco 3560 with the Cisco IOS Release 12.2(46)SE C3560-advipservicesk9-mz image or comparable)
- SRV1 (Windows PC with 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

Instructor Notes

- This lab is divided into multiple tasks. Each task is associated with a trouble ticket (TT) and introduces one or more errors on one or more devices.
- Students can work individually or as a team.
- Suggested actions and results presented during the troubleshooting process for each TT can be shared with the students during debrief or copies of the instructor version of the lab can be made available to the students to assist them in verifying their work.

Section 1—Trouble Tickets and Troubleshooting Logs

Task 1: Trouble Ticket Lab 9-2 TT-A

Instructor note: This trouble ticket involves devices ALS1 and DLS1 and issues related to DHCP snooping and trusted ports.

Step 1: Review trouble ticket Lab 9-2 TT-A.

As a security measure, your company has decided to implement DHCP snooping on access switches to prevent DHCP spoofing by unauthorized DHCP servers. For the pilot, the implementation plan specifies that the user VLAN 10 (OFFICE VLAN) on ASL1 be configured for DHCP snooping, and DHCP client PC-B be used as a test station. The test plan requires that the redundant switch topology failover allows VLAN 10 users to obtain an IP address from the DHCP server (DLS1) if one of the trunk links from ALS1 to DLS1 or DLS2 goes down.

Your colleague has configured DHCP snooping on ASL1, but now PC-B cannot access SRV1 or the Internet. He has asked for your help in diagnosing and solving the problem.

Step 2: Load the device trouble ticket configuration files for TT-A.

Using the procedure described in Lab 3-1, verify that the lab configuration files are present in flash. Load the proper configuration files as indicated in the Device Configuration File table.

Note: The following device access methods are in effect after loading the configuration files:

- Console access requires no username or password.
- Telnet and SSH require username **admin** and password **adminpa55**.
- The enable password is **ciscoenpa55**.

Instructor note: Although it is not considered security best practice, the enable secret and admin user passwords can be changed to something simpler to facilitate performance of this lab.

Device Configuration File Table

Device Name	File to Load	Notes
ALS1	Lab92-ALS1-TT-A-Cfg.txt	This file contains configuration errors
DLS1	Lab92-DLS1-TT-A-Cfg.txt	This file contains configuration errors
DLS2	Lab92-DLS2-TT-A-Cfg.txt	This file contains configurations different than the baseline
R1	Lab92-R1-TT-A-Cfg.txt	This file contains configurations different than the baseline
R2	Lab92-R2-TT-A-Cfg.txt	This file contains configurations different than the baseline
R3	Lab92-R3-TT-A-Cfg.txt	This file contains configurations different than the baseline
SRV1	N/A	Static IP: 10.1.50.1 Default gateway: 10.1.50.254
PC-B	N/A	DHCP
PC-C	N/A	Static IP: 10.1.80.100 Default gateway: 10.1.80.1

Instructor note: The student loads the “broken” TT configuration files for all devices, even though only the configurations indicated in the Notes column contain errors.

Step 3: Configure SRV1.

a. Configure SRV1 with static IP address 10.1.50.1/24 and default gateway 10.1.50.254.

Step 4: Release and renew the DHCP lease on PC-B.

a. Ensure that PC-B is configured as a DHCP client in the OFFICE VLAN.

b. After loading all TT-A device configuration files, issue the **`ipconfig /release`** and **`ipconfig /renew`** commands on PC-B.

Step 5: Outline the troubleshooting approach and validation steps.

Use this space to identify your troubleshooting approach and the key steps to verify that the problem is resolved. Troubleshooting approaches to select from include the follow-the-path, spot-the-differences, bottom-up, top-down, divide-and-conquer, shoot-from-the-hip, and move-the-problem methods.

Note: In addition to a specific approach, you can use the generic troubleshooting process described at the beginning of Section 2 of this lab.

____

____

____

____

____

____

The spot-the-differences or shoot-from-the-hip method can be used. Other problem-solving methods are the top-down, bottom-up, follow-the-path, divide-and-conquer, and move-the-problem approaches.

Verification steps can include:

- PC-B can obtain a VLAN 10 IP address from DHCP server DLS1.
- PC-B can ping SRV1 and the Internet (simulated by R2 Lo0).
- All DHCP traffic is permitted on port channels Po1 and Po2.
- If Po1 or Po2 on ALS1 goes down, the DHCP server on DLS1 is still reachable.
- A DCHP server attached to an ALS1 access port is not accessible by VLAN 10 clients.

Step 6: Record the troubleshooting process and configuration changes.

Note: Section 2 of this lab includes useful commands and examples of output.

Use this log to document your actions and results during the troubleshooting process. List the commands you used to gather information. As you progress, record what you think the problem might be and the actions you take to correct the problem.

Device	Actions and Results

Device	Actions and Results

Responses will vary but could include:

TT-A Issue 1

DHCP relay information from ALS1 is not trusted on DLS1. As a result, there is no access to the DLS1 DHCP server from ALS1 via ALS1 trusted port Po1 (Fa0/1 and Fa0/2).

- Pings from PC-B to SRV1 fail.
- Pings from PC-B to the DLS1 VLAN 10 default gateway fail.
- A check of PC-B indicates that it is a DHCP client but has not acquired an IP address from the DLS1 DHCP server.
- The **`show ip dhcp snooping`** command on ALS1 indicates that snooping is enabled and is configured on VLAN 10. Trunk interfaces Fa0/1 and Fa0/2 and port channel Po1 to DLS1 are trusted ports.
- The **`show run int po1`** command on ALS1 confirms that **`ip dhcp snooping trust`** is configured.
- After issuing the **`debug ip dhcp snooping packet`** command on ALS1 and then issuing the **`ipconfig /release`** and **`ipconfig /renew`** commands on PC-B, the debug output shows a DHCP DISCOVER broadcast received on ALS1 Fa0/18 from PC-B. However, there is no DHCP OFFER from DLS1 on Po1.
- The **`show ip dhcp snooping`** command on DLS1 indicates that DHCP snooping is not enabled.

Action: Enable DLS1 to trust DHCP relay information from ALS1 so that the DHCP server can respond to the ALS1 trusted port requests. It is not necessary to enable DHCP snooping on DLS1, although this would indirectly correct the problem. It is also not necessary to configure snooping for VLAN 10 on DLS1 nor is it required to make Po1 (Fa0/1 and Fa0/2) or Po10 (Fa0/3 and Fa0/4) on DLS1 trusted. See the TT-A debrief for more information.

Verification:

- PC-B can obtain an IP address in VLAN 10 from DHCP server DLS1.
- PC-B can ping SRV1 and the Internet (simulated by R2 Lo0).

- The **`debug ip dhcp snooping packet`** command on ALS1 and the **`ipconfig /release`** and **`ipconfig /renew`** commands on PC-B show all DHCP messages passing between Fa0/18 and Po1.
- If Po1 from ALS1 to DLS1 goes down, the DHCP server on DLS1 will *not* be reachable. There is a hidden problem related to redundancy.
- A DCHP server attached to an ALS1 access port will not be accessible by VLAN 10 clients. Note that this can only be tested if another DHCP server is available.

TT-A Issue 2

Po2 (Fa0/3 and Fa0/4) on ALS1 is not configured as a trusted interface. As a result, there is no access to the DLS1 DHCP server from ALS1 if trunk link Po1 goes down.

- PC-B can obtain a VLAN 10 IP address from DHCP server DLS1 as long as the Po1 link between ALS1 and DLS1 is up.
- Pings from PC-B to SRV1 succeed as long as the Po1 link between ALS1 and DLS1 is up, unless PC-B seeks to renew its IP address.
- If interface Po1 on ALS1 is shut down (simulating a link failure), and the **`ipconfig /release`** and **`ipconfig /renew`** commands are issued on PC-B, an IP address cannot be obtained from DHCP server DLS1 via the alternate path Po2.
- Pings from PC-B to SRV1 fail.
- The **`show ip dhcp snooping`** command on ALS1 indicates that snooping is enabled and is configured on VLAN 10. However, trunk interfaces Fa0/3 and Fa0/4 and port channel Po2 to DLS2 are not trusted ports.
- The **`show run int po2`** command on ALS1 confirms that **`ip dhcp snooping trust`** is not configured.

Action: Configure ALS1 interface Po2 (Fa0/3 and Fa0/4) to be trusted. It is not necessary to configure **`ip dhcp snooping`** on DLS2. See the TT-A debrief for more information.

Verification:

- PC-B can obtain a VLAN 10 IP address from DHCP server DLS1 when either link Po1 or Po2 is down.
- PC-B can ping SRV1 and the Internet (simulated by R2 Lo0).
- A DCHP server attached to an ALS1 access port is not accessible by VLAN 10 clients.

Step 7: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with your instructor. The notes can include problems encountered, solutions applied, useful commands employed, alternate solutions, methods, and processes, and procedure and communication improvements.

____

____

____

____

____

____

____

Trouble Ticket TT-A Debrief—Instructor Notes

This trouble ticket consists of two DHCP snooping issues that affect access to the DHCP server on DLS1.

TT-A Issue 1

The first problem is that DLS1 does not accept packets from ALS1 as a relay agent. As a result, there is no access to the DLS1 DHCP server from ALS1.

For each DHCP packet received on an untrusted port, ALS1 inserts a DHCP Option-82 (the Relay Agent Information Option). This option is used by ALS1 to identify itself and the port where the client is connected. However, it leaves the GIADDR field in the DHCP packet set to 0.0.0.0. DLS1 considers such DHCP packets to be invalid and drops them. This problem can be remedied by allowing DLS1 to accept DHCP packets with Option-82 present and having the GIADDR set to 0.0.0.0.

This can be accomplished in global configuration mode using the following command on DLS1. This allows PC-B to obtain a VLAN 10 IP address from DHCP server DLS1.

```
ip dhcp relay information trust-all
```

Alternatively, the command **`ip dhcp relay information trusted`** can be issued on individual routed interfaces (SVIs, physical interfaces).

Note: If Po1 from ALS1 to DLS1 goes down, the DHCP server on DLS1 will *not* be reachable. This is a hidden problem related to redundancy.

TT-A Issue 2

The second problem is that Po2 (Fa0/3 and Fa0/4) on ALS1 is not configured as a trusted interface. As a result, there is no access to the DLS1 DHCP server from ALS1 if trunk link Po1 goes down. Po2 is currently an ALS1 STP backup link. This problem does not prevent PC-B from receiving an IP address as long as the Po1 link is up. However, the lack of a backup link does not fulfill the failover requirement specified in the implementation test plan.

Configure ALS1 interface Po2 (Fa0/3 and Fa0/4) to be trusted. It is not necessary to configure **`ip dhcp snooping`** on DLS2, unless it has a port connection to a DHCP server. DLS2 is simply acting as a Layer 2 switch providing a backup path to the DLS1 DHCP server.

Issue the following command on ALS1:

```
interface Port-channel2
  ip dhcp snooping trust
```

Note: Configuring port channel Po2 as trusted automatically configures the physical ports that make up the port channel (Fa0/3 and Fa0/4).

Task 2: Trouble Ticket Lab 9-2 TT-B

Instructor note: This trouble ticket involves devices R3 and DLS2 and issues related to EIGRP router neighbor authentication.

Step 1: Review trouble ticket Lab 9-2 TT-B.

As another control plane security measure, your company has decided to implement MD5 authentication between EIGRP routers and Layer 3 switches. As a pilot, a colleague of yours configured MD5 authentication on Layer 3 switch DLS2 and router R3. Now branch office users on the R3 LAN (PC-C) cannot access SRV1 or the Internet. He has asked for your help in diagnosing and solving the problem.

Step 2: Load the device trouble ticket configuration files for TT-B.

Using the procedure described in Lab 3-1, verify that the lab configuration files are present in flash. Load the proper configuration files as indicated in the Device Configuration File table.

Note: The following device access methods are in effect after loading the configuration files:

- Console access requires no username or password.
- Telnet and SSH require username **admin** and password **adminpa55**.
- The enable password is **ciscoenpa55**.

Instructor note: Although it is not considered security best practice, the enable secret and admin user passwords can be changed to something simpler to facilitate performance of this lab.

Device Configuration File Table

Device Name	File to Load	Notes
ALS1	Lab92-ALS1-TT-B-Cfg.txt	This file contains configurations different than the baseline
DLS1	Lab92-DLS1-TT-B-Cfg.txt	This file contains configurations different than the baseline
DLS2	Lab92-DLS2-TT-B-Cfg.txt	This file contains configuration errors.
R1	Lab92-R1-TT-B-Cfg.txt	This file contains configurations different than the baseline
R2	Lab92-R2-TT-B-Cfg.txt	This file contains configurations different than the baseline
R3	Lab92-R3-TT-B-Cfg.txt	This file contains configuration errors
SRV1	N/A	Static IP: 10.1.50.1 Default gateway: 10.1.50.254
PC-B	N/A	DHCP
PC-C	N/A	Static IP: 10.1.80.100 Default gateway: 10.1.80.1

Instructor note: The student loads the “broken” TT configuration files for all devices, even though only the configurations indicated in the Notes column contain errors.

Step 3: Configure SRV1.

Configure SRV1 with static IP address 10.1.50.1/24 and default gateway 10.1.50.254.

Step 4: Configure a static IP address on PC-C.

Configure PC-C with static IP address 10.1.80.100, subnet mask 255.255.255.0, and default gateway 10.1.80.1.

Step 5: Outline the troubleshooting approach and validation steps.

Use this space to identify your troubleshooting approach and the key steps to verify that the problem is resolved. Troubleshooting approaches to select from include the follow-the-path, spot-the-differences, bottom-up, top-down, divide-and-conquer, shoot-from-the-hip, and move-the-problem methods.

Note: In addition to a specific approach, you can use the generic troubleshooting process described at the beginning of Section 2 of this lab.

The follow-the-path or shoot-from-the-hip method can be used. Other problem-solving methods are the bottom-up, top-down, spot-the-differences, follow-the-path, divide-and-conquer, and move-the-problem approaches.

Verification steps can include:

- PC-C can access SRV1 and the Internet.
- DLS2 and R3 establish a neighbor relationship.
- DLS2 and R3 exchange updates using MD5 authentication.

Step 6: Record the troubleshooting process and configuration changes.

Note: Section 2 of this lab includes useful commands and examples of output.

Use this log to document your actions and results during the troubleshooting process. List the commands you used to gather information. As you progress, record what you think the problem might be and the actions you take to correct the problem.

Device	Actions and Results

TT-B Issue 1

MD5 authentication on R3 is configured on Fa0/0. It should be on Fa0/1. There is no EIGRP authentication configured on Fa0/1, the neighbor interface that is adjacent to DLS2. As a result, no neighbor relationship formed between DLS2 and R3.

- Pings from PC-C to SRV1 and the Internet fail.
- Pings from PC-C to the R3 default gateway succeed.
- The **`show ip route`** command on R3 indicates that there are no routes learned via EIGRP.
- The **`show ip eigrp neighbors`** command on R3 indicates that it has not formed a neighbor relationship with DLS2.
- The **`show ip eigrp interfaces`** command on R3 indicates that interface Fa0/1 is an EIGRP interface but that there are no peers associated with it.
- The **`show ip eigrp interfaces detail`** command on R3 indicates that the authentication mode is not set on interface Fa0/1.
- The **`show run interface fa0/0`** command on R3 indicates that EIGRP MD5 authentication is configured on interface Fa0/0. However, Fa0/0 is not adjacent to R3 or any other another EIGRP device.

Action: Remove MD5 authentication from R3 interface Fa0/0 and configure it on Fa0/1. See the TT-B debrief for more information.

Verification:

- Pings from PC-C to SRV1 and the Internet fail.
- The **`show ip route`** command on R3 indicates that there are still no routes learned via EIGRP. There must be another problem.

TT-B Issue 2

The authentication key string specified for key chain EIGRPCHAIN on DLS2 does not match the one configured on R3.

- The **`show ip route`** command on R3 indicates that there are still no routes learned via EIGRP.
- The **`show ip eigrp neighbors`** command on R3 indicates that it has not formed a neighbor relationship with DLS2.
- The **`show ip eigrp interfaces detail`** command on R3 indicates that the authentication mode is MD5 and the key chain is EIGRPCHAIN for interface Fa0/1, the neighbor interface with DLS2.
- The **`show ip eigrp interfaces detail`** command on DLS2 indicates that the authentication mode is MD5 and the key chain is EIGRPCHAIN for interface Fa0/5, the neighbor interface with R3.
- The **`show run | begin key chain`** command on R3 and DLS2 indicates that the key chain EIGRPCHAIN is configured on both devices, but the key 1 key string is encrypted. It cannot be determined if the passwords are the same by viewing the running config.
- The **`show key chain`** command on R3 and DLS2 reveals that the key chains do not match and the one on DLS2 should be changed.

Action: Change key chain EIGRPCHAIN on DLS2 to match the one on R3. See the TT-B debrief for more information.

Verification:

- EIGRP console messages indicate that a new adjacency has formed.

```
Dec 11 19:20:43: %DUAL-5-NBRCHANGE: EIGRP-IPv4:(1) 1: Neighbor 10.1.2.14
 (FastEthernet0/5) is up: new adjacency
```


- The **`show ip eigrp neighbors`** command on R3 confirms that a neighbor relationship has been established with DLS2.
- The **`show ip route`** command on R3 indicates that all expected routes are present.
- Pings from PC-C to SRV1 and the Internet succeed.

Step 7: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with your instructor. The notes can include problems encountered, solutions applied, useful commands employed, alternate solutions, methods, and processes, and procedure and communication improvements.

____

____

____

____

____

____

____

Trouble Ticket TT-B Debrief—Instructor Notes

This trouble ticket consists of two configuration issues that prevent EIGRP adjacency between R3 and DLS2.

TT-B Issue 1

The first problem is that EIGRP MD5 authentication on R3 is configured on Fa0/0 when it should be configured on Fa0/1, the neighbor interface that is adjacent to DLS2. No EIGRP device is on the R3 LAN, and Fa0/0 is a passive interface. EIGRP MD5 authentication is configured on DLS2 Fa0/5. As a result, no adjacency is formed between DLS2 and R3.

Removing the MD5 authentication from R3 interface Fa0/0 and configuring it on Fa0/1 corrects this problem. Issue the following commands on R3:

```
interface fa0/0
 no ip authentication mode eigrp 1 md5
 no ip authentication key-chain eigrp 1 EIGRPCHAIN

interface fa0/1
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 EIGRPCHAIN
```

Note: The number “1” after the keyword **`eigrp`** in the above commands refers to the EIGRP AS number, not the key number (which is also 1).

TT-B Issue 2

The second problem in this trouble ticket is that the authentication key string specified for key chain EIGRPCHAIN on DLS2 does not match the one configured on R3. However, the key 1 key string on both devices is encrypted by the password encryption service and it cannot be determined if the passwords are the same by viewing the running config or startup config. To view the decrypted key for either device, use the **`show key chain`** command. To ensure that the key string is the same on R3 and DLS2, issue the following commands on DLS2.

```
key chain EIGRPCHAIN
```



```
key 1
 key-string eigrpkey
```

Note: Key strings are case-sensitive, and even the presence of a trailing space in one of them makes them different.

Section 2 Troubleshooting Reference Information

General Troubleshooting Process

As a general guideline, you can use the following general troubleshooting process described in the course.

1. Define the problem (symptoms).
2. Gather information.
3. Analyze the information.
4. Propose a hypothesis (possible cause).
5. Test the hypothesis.
6. Eliminate or accept the hypothesis.
7. Solve the problem.
8. Document the problem.

Command Summary

The table lists useful commands for this lab. The sample output is shown on following pages.

Command	Key Information Displayed
show ip dhcp snooping	Displays snooping status (enabled or not) and, if enabled, on which VLANs. Also shows which interfaces are trusted.
debug ip dhcp snooping packet	Displays real-time information on DHCP snooping activity and the client/server exchange.
debug ip dhcp server packet	Displays real-time information on DHCP on the client/server exchange from the server perspective.
show ip eigrp neighbors	Displays the IP address of EIGRP neighbors and the interface on which they were learned.
sh ip eigrp interfaces	Displays all interfaces participating in EIGRP for each AS and the number of peers associated with each interface.
show ip eigrp interfaces detail	Displays all interfaces participating in EIGRP for each AS along with the number of peers, hello interval, and the type of authentication (if configured).
debug eigrp packets	Displays real-time information on types of EIGRP packets exchange, which include authentication information.

Sample Troubleshooting Output

DHCP Snooping-related Commands

The following commands and outputs are provided as samples from the devices in this lab.

```
ALS1#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10
```



```
DHCP snooping is operational on following VLANs:
10
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
   circuit-id format: vlan-mod-port
    remote-id format: MAC
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                    Trusted     Rate limit (pps)
------------------------     -------     ----------------
FastEthernet0/1              yes         unlimited
FastEthernet0/2              yes         unlimited
FastEthernet0/3              yes         unlimited
FastEthernet0/4              yes         unlimited
Port-channel1                yes         unlimited
Port-channel2                yes         unlimited
```

In the above example, DHCP snooping is operational on ALS1 VLAN 10, and Fa0/1 through Fa0/4 (port channels Po1 and Po2) are trusted.

```
DLS1#show ip dhcp snooping
Switch DHCP snooping is disabled
DHCP snooping is configured on following VLANs:
none
DHCP snooping is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
   circuit-id format: vlan-mod-port
    remote-id format: MAC
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                    Trusted     Rate limit (pps)
------------------------     -------     ----------------
```

In the above example, Option 82 on untrusted port is not allowed, and no interfaces are trusted.

```
ALS1#debug ip dhcp snooping packet
DHCP Snooping Packet debugging is on
ALS1#
*Mar  1 09:04:48.215: DHCPSNOOP(hlfm_set_if_input): Setting if_input to Fa0/18 f
or pak.  Was not set
*Mar  1 09:04:48.215: DHCPSNOOP(hlfm_set_if_input): Clearing if_input for pak.
Was Fa0/18
*Mar  1 09:04:48.215: DHCPSNOOP(hlfm_set_if_input): Setting if_input to Fa0/18 f
or pak.  Was not set
*Mar  1 09:04:48.215: DHCP_SNOOPING: received new DHCP packet from input interfa
ce (FastEthernet0/18)
```



```
*Mar  1 09:04:48.215: DHCP_SNOOPING: process new DHCP packet, message type: DHCP
DISCOVER, input interface: Fa0/18, MAC da: ffff.ffff.ffff, MAC sa: 000b.db04.a5cd,
IP da: 255.255.255.255
, IP sa: 0.0.0.0, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 0.0.0.0, DHCP siaddr: 0.0.0
.0, DHCP giaddr: 0.0.0.0, DHCP chaddr: 000b.db04.a5cd
*Mar  1 09:04:48.215: DHCP_SNOOPING: add relay information option.
*Mar  1 09:04:48.215: DHCP_SNOOPING_SW: Encoding opt82 CID in vlan-mod-port form
at
*Mar  1 09:04:48.215: DHCP_SNOOPING_SW: Encoding opt82 RID in MAC address format

*Mar  1 09:04:48.215: DHCP_SNOOPING: binary dump of relay info option, length: 20
data:
0x52 0x12 0x1 0x6 0x0 0x4 0x0 0xA 0x1 0x12 0x2 0x8 0x0 0x6 0x0 0x1B 0xC 0x6D 0x8
F 0x0
*Mar  1 09:04:48.215: DHCP_SNOOPING_SW: bridge packet get invalid mat entry: FFF
F.FFFF.FFFF, packet is flooded to ingress VLAN: (10)
ALS1#
```

In the above example, a DHCP DISCOVER message with option 82 and GIADDR of 0.0.0.0 was sent to DLS1 but, because DLS1 does not trust this relay information a reply was not received from the DLS1 DHCP server.

```
ALS1#debug ip dhcp snooping packet
DHCP Snooping Packet debugging is on
ALS1#
*Mar  1 09:10:36.904: DHCPSNOOP(hlfm_set_if_input): Setting if_input to Fa0/18 f
or pak.  Was not set
*Mar  1 09:10:36.904: DHCPSNOOP(hlfm_set_if_input): Clearing if_input for pak.
Was Fa0/18
*Mar  1 09:10:36.904: DHCPSNOOP(hlfm_set_if_input): Setting if_input to Fa0/18 f
or pak.  Was not set
*Mar  1 09:10:36.904: DHCP_SNOOPING: received new DHCP packet from input interfa
ce (FastEthernet0/18)
*Mar  1 09:10:36.904: DHCP_SNOOPING: process new DHCP packet, message type: DHCP
DISCOVER, input interface: Fa0/18, MAC da: ffff.ffff.ffff, MAC sa: 000b.db04.a5cd,
IP da: 255.255.255.255
, IP sa: 0.0.0.0, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 0.0.0.0, DHCP siaddr: 0.0.0
.0, DHCP giaddr: 0.0.0.0, DHCP chaddr: 000b.db04.a5cd
*Mar  1 09:10:36.904: DHCP_SNOOPING: add relay information option.
*Mar  1 09:10:36.904: DHCP_SNOOPING_SW: Encoding opt82 CID in vlan-mod-port form
at
*Mar  1 09:10:36.904: DHCP_SNOOPING_SW: Encoding opt82 RID in MAC address format

*Mar  1 09:10:36.904: DHCP_SNOOPING: binary dump of relay info option, length: 20
data:
0x52 0x12 0x1 0x6 0x0 0x4 0x0 0xA 0x1 0x12 0x2 0x8 0x0 0x6 0x0 0x1B 0xC 0x6D 0x8
F 0x0
*Mar  1 09:10:36.904: DHCP_SNOOPING_SW: bridge packet get invalid mat entry: FFF
F.FFFF.FFFF, packet is flooded to ingress VLAN: (10)
*Mar  1 09:10:36.912: DHCPSNOOP(hlfm_set_if_input): Setting if_input to Po1 for
pak.  Was not set
*Mar  1 09:10:36.912: DHCPSNOOP(hlfm_set_if_input): Clearing if_input for pak.
Was Po1
*Mar  1 09:10:36.912: DHCPSNOOP(hlfm_set_if_input): Setting if_input to Po1 for
pak.  Was not set
*Mar  1 09:10:36.912: DHCP_SNOOPING: received new DHCP packet from input interfa
ce (Port-channel1)
```



```
*Mar  1 09:10:36.912: DHCP_SNOOPING: process new DHCP packet, message type: DHCP
OFFER, input interface: Po1, MAC da: ffff.ffff.ffff, MAC sa: 0017.5a5b.b443, IP
da: 255.255.255.255, IP sa: 10.1.10.252, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 10.1
.10.1, DHCP siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0, DHCP chaddr: 000b.db04.a5cd
*Mar  1 09:10:36.912: DHCP_SNOOPING: binary dump of option 82, length:
ALS1#20 data:
0x52 0x12 0x1 0x6 0x0 0x4 0x0 0xA 0x1 0x12 0x2 0x8 0x0 0x6 0x0 0x1B 0xC 0x6D 0x8
F 0x0
*Mar  1 09:10:36.912: DHCP_SNOOPING: binary dump of extracted circuit id, length
: 8 data:
0x1 0x6 0x0 0x4 0x0 0xA 0x1 0x12
*Mar  1 09:10:36.912: DHCP_SNOOPING: binary dump of extracted remote id, length:
 10 data:
0x2 0x8 0x0 0x6 0x0 0x1B 0xC 0x6D 0x8F 0x0
*Mar  1 09:10:36.912: DHCP_SNOOPING_SW: opt82 data indicates local packet
*Mar  1 09:10:36.912: DHCP_SNOOPING: remove relay information option.
*Mar
ALS1# 1 09:10:36.912: DHCP_SNOOPING: direct forward dhcp reply to output port: F
astEthernet0/18.
*Mar  1 09:10:36.912: DHCPSNOOP(hlfm_set_if_input): Setting if_input to Fa0/18 f
or pak.  Was not set
*Mar  1 09:10:36.912: DHCPSNOOP(hlfm_set_if_input): Clearing if_input for pak.
Was Fa0/18
*Mar  1 09:10:36.912: DHCPSNOOP(hlfm_set_if_input): Setting if_input to Fa0/18 f
or pak.  Was not set
*Mar  1 09:10:36.912: DHCP_SNOOPING: received new DHCP packet from input interfa
ce (FastEthernet0/18)
*Mar  1 09:10:36.91
ALS1#2: DHCP_SNOOPING: process new DHCP packet, message type: DHCPREQUEST, input
 interface: Fa0/18, MAC da: ffff.ffff.ffff, MAC sa: 000b.db04.a5cd, IP da: 255.2
55.255.255, IP sa: 0.0.0.0, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 0.0.0.0, DHCP sia
ddr: 0.0.0.0, DHCP giaddr: 0.0.0.0, DHCP chaddr: 000b.db04.a5cd
*Mar  1 09:10:36.912: DHCP_SNOOPING: add relay information option.
*Mar  1 09:10:36.912: DHCP_SNOOPING_SW: Encoding opt82 CID in vlan-mod-port form
at
*Mar  1 09:10:36.912: DHCP_SNOOPING_SW: Encoding opt82 RID
ALS1#in MAC address format
*Mar  1 09:10:36.912: DHCP_SNOOPING: binary dump of relay info option, length: 2
0 data:
0x52 0x12 0x1 0x6 0x0 0x4 0x0 0xA 0x1 0x12 0x2 0x8 0x0 0x6 0x0 0x1B 0xC 0x6D 0x8
F 0x0
*Mar  1 09:10:36.921: DHCP_SNOOPING_SW: bridge packet get invalid mat entry: FFF
F.FFFF.FFFF, packet is flooded to ingress VLAN: (10)
*Mar  1 09:10:36.921: DHCPSNOOP(hlfm_set_if_input): Setting if_input to Po1 for
pak.  Was not set
*Mar  1 09:10:36.921: DHCPSNOOP(hlfm_set_if_input): Clearing if_input for pak.
ALS1#  Was Po1
*Mar  1 09:10:36.921: DHCPSNOOP(hlfm_set_if_input): Setting if_input to Po1 for
pak.  Was not set
*Mar  1 09:10:36.921: DHCP_SNOOPING: received new DHCP packet from input interfa
ce (Port-channel1)
*Mar  1 09:10:36.921: DHCP_SNOOPING: process new DHCP packet, message type: DHCP
ACK, input interface: Po1, MAC da: ffff.ffff.ffff, MAC sa: 0017.5a5b.b443, IP da
: 255.255.255.255, IP sa: 10.1.10.252, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 10.1.1
0.1, DHCP siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0, DHCP chaddr:
ALS1# 000b.db04.a5cd
*Mar  1 09:10:36.921: DHCP_SNOOPING: binary dump of option 82, length: 20 data:
0x52 0x12 0x1 0x6 0x0 0x4 0x0 0xA 0x1 0x12 0x2 0x8 0x0 0x6 0x0 0x1B 0xC 0x6D 0x8
```



```
F 0x0
*Mar  1 09:10:36.921: DHCP_SNOOPING: binary dump of extracted circuit id, length
: 8 data:
0x1 0x6 0x0 0x4 0x0 0xA 0x1 0x12
*Mar  1 09:10:36.921: DHCP_SNOOPING: binary dump of extracted remote id, length:
 10 data:
0x2 0x8 0x0 0x6 0x0 0x1B 0xC 0x6D 0x8F 0x0
*Mar  1 09:10:36.921: DHCP_SNOOPING_SW: opt82 data indicates lo
ALS1#cal packet
*Mar  1 09:10:36.921: DHCP_SNOOPING_SW: opt82 data indicates local packet
*Mar  1 09:10:36.921: DHCP_SNOOPING: remove relay information option.
*Mar  1 09:10:36.921: DHCP_SNOOPING: direct forward dhcp reply to output port: F
astEthernet0/18.
ALS1#u all
All possible debugging has been turned off
ALS1#
```

In the above example, the **`ip dhcp relay information trust-all`** command was issued on DLS1. The DHCP DISCOVER message received on ALS1 interface Fa0/18 (from PC-B) and was forwarded to DLS1 to complete the DHCP exchange between PC-B and DLS1.

```
DLS1#debug ip dhcp server packet
DHCP server packet debugging is on.
Dec 11 14:14:25.024: DHCPD: Reload workspace interface Vlan10 tableid 0.
Dec 11 14:14:25.024: DHCPD: tableid for 10.1.10.252 on Vlan10 is 0
Dec 11 14:14:25.024: DHCPD: client's VPN is .
Dec 11 14:14:25.024: DHCPD: inconsistent relay information.
Dec 11 14:14:25.024: DHCPD: relay information option exists, but giaddr is zero
```

In the above example, with dhcp relay information from ALS1 and a GIADDR of 0.0.0.0, the relay information is inconsistent and DLS1 rejects the DHCP DISCOVER message from PC-B.

```
DLS1#debug ip dhcp server packet
DHCP server packet debugging is on.
Dec 11 14:28:13.118: DHCPD: Reload workspace interface Vlan10 tableid 0.
Dec 11 14:28:13.118: DHCPD: tableid for 10.1.10.252 on Vlan10 is 0
Dec 11 14:28:13.118: DHCPD: client's VPN is .
Dec 11 14:28:13.118: DHCPD: DHCPRELEASE message received from client 0100.0bdb.0
4a5.cd (10.1.10.1).
Dec 11 14:28:15.542: DHCPD: Reload workspace interface Vlan10 tableid 0.
Dec 11 14:28:15.542: DHCPD: tableid for 10.1.10.252 on Vlan10 is 0
Dec 11 14:28:15.542: DHCPD: client's VPN is .
Dec 11 14:28:15.542: DHCPD: using received relay info.
Dec 11 14:28:15.542: DHCPD: DHCPDISCOVER received from client 0100.0bdb.04a5.cd
on interface Vlan10.
Dec 11 14:28:15.542: DHCPD: using received relay info.
Dec 11 14:28:17.556: DHCPD: Sending DHCPOFFER to client 0100.0bdb.04a5.cd (10.1.
10.1).
Dec 11 14:28:17.556: DHCPD: Check for IPe on Vlan10
Dec 11 14:28:17.556: DHCPD: creating ARP entry (10.1.10.1, 000b.db04.a5cd).
Dec 11 14:28:17.556: DHCPD: unicasting BOOTREPLY to client 000b.db04.a5cd (10.1.
10.1).
Dec 11 14:28:17.556: DHCPD: Reload workspace interface Vlan10 tableid 0.
Dec 11 14:28:17.556: DHCPD: tableid for 10.1.10.252 on Vlan10 is 0
Dec 11 14:28:17.556: DHCPD: client's VPN is .
Dec 11 14:28:17.556: DHCPD: DHCPREQUEST received from client 0100.0bdb.04a5.cd.
```



```
Dec 11 14:28:17.556: DHCPD: Sending DHCPACK to client 0100.0bdb.04a5.cd (10.1.10
.1).
Dec 11 14:28:17.556: DHCPD: Check for IPe on Vlan10
Dec 11 14:28:17.556: DHCPD: creating ARP entry (10.1.10.1, 000b.db04.a5cd).
Dec 11 14:28:17.556: DHCPD: unicasting BOOTREPLY to client 000b.db04.a5cd (10.1.
10.1).
```

In the above example, with the **`ip dhcp relay information trust-all`** command issued on DLS1, the entire DHCP conversation between PC-B and the DLS1 server takes place, and PC-B is provided with an IP address.

EIGRP Authentication-related Commands

```
DLS2#show ip eigrp neighbors
EIGRP-IPv4:(1) neighbors for process 1
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
1   10.1.2.14               Fa0/5             13 00:20:59    1   200  0  29
0   10.1.200.252            Vl200             14 05:31:25    2   200  0  45
```

In the above example, DLS2 has two EIGRP neighbors, R3 (10.1.2.14) via Fa0/5 and DLS1 (10.1.200.252) via VLAN 200.

```
DLS2#show ip eigrp interfaces
EIGRP-IPv4:(1) interfaces for process 1

                        Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface        Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Vl200              1        0/0         2       0/1           50           0
Fa0/5              1        0/0         1       0/1           50           0
```

In the above example, DLS2 has two interfaces participating in the EIGRP process, VLAN 200 and Fa0/5. Both interfaces have a peer attached.

```
DLS2#show ip eigrp interfaces detail
EIGRP-IPv4:(1) interfaces for process 1

                        Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface        Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Vl200              1        0/0         1       0/1           50           0
  Hello interval is 5 sec
  Next xmit serial <none>
  Un/reliable mcasts: 0/18  Un/reliable ucasts: 22/9
  Mcast exceptions: 1  CR packets: 1  ACKs suppressed: 1
  Retransmissions sent: 1  Out-of-sequence rcvd: 0
  Topology-ids on interface - 0
  Authentication mode is not set

Fa0/5              0        0/0         0       0/1           50           0
  Hello interval is 5 sec
  Next xmit serial <none>
  Un/reliable mcasts: 0/18  Un/reliable ucasts: 9/25
  Mcast exceptions: 2  CR packets: 2  ACKs suppressed: 3
  Retransmissions sent: 6  Out-of-sequence rcvd: 1
  Topology-ids on interface - 0
```



```
  Authentication mode is md5,  key-chain is "EIGRPCHAIN"
```

In the above example, no authentication is configured on DLS2 interface VLAN 200. MD5 authentication is configured on interface Fa0/5 using key chain EIGRPCHAIN.

```
DLS2#debug eigrp packets
EIGRP Packets debugging is on
    (UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY,
SIAREPLY)
DLS2#
Dec 14 18:21:51.626: EIGRP: Sending HELLO on FastEthernet0/5
Dec 15 18:21:51.626:   AS 1, Flags 0x0, Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0
Dec 15 18:21:51.895: EIGRP: FastEthernet0/5: ignored packet from 10.1.2.14, opcode
= 5 (missing authentication)
Dec 15 18:21:52.255: EIGRP: Sending HELLO on Vlan200
Dec 15 18:21:52.255:   AS 1, Flags 0x0, Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0
Dec 15 18:21:54.495: EIGRP: Received HELLO on Vlan200 nbr 10.1.200.252
Dec 15 18:21:54.495:   AS 1, Flags 0x0, Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0
 peerQ un/rely 0/0

DLS2#debug eigrp packets
EIGRP Packets debugging is on
    (UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY,
SIAREPLY)

Dec 15 18:28:38.442: EIGRP: Sending UPDATE on FastEthernet0/5 tid 0
Dec 15 18:28:38.442:   AS 1, Flags 0x2, Seq 21/0 interfaceQ 2/0 iidbQ un/rely 0/
0 serno 1-10
Dec 15 18:28:38.442: EIGRP: received packet with MD5 authentication, key id = 1
Dec 15 18:28:38.442: EIGRP: Received HELLO on FastEthernet0/5 nbr 10.1.2.14
```

In the first debug example above, authentication is configured on DLS2 Fa0/5. However, it is not configured on R3 Fa0/1, and DLS2 ignores packets from R3. No authentication is required on VLAN 200, so DLS2 is able to send and receive hello messages with DLS1.

In the second debug example above, authentication is now configured on R3 Fa0/1, and DLS2 accepts hello packets from R3.

```
R3#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.1.2.13 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 9 subnets, 3 masks
D       10.1.10.0/24 [90/28416] via 10.1.2.13, 00:01:43, FastEthernet0/1
C       10.1.2.12/30 is directly connected, FastEthernet0/1
D       10.1.2.0/30 [90/30976] via 10.1.2.13, 00:01:43, FastEthernet0/1
D       10.1.30.0/24 [90/28416] via 10.1.2.13, 00:01:43, FastEthernet0/1
D       10.1.20.0/24 [90/28416] via 10.1.2.13, 00:01:43, FastEthernet0/1
```



```
D       10.1.50.0/24 [90/28416] via 10.1.2.13, 00:01:43, FastEthernet0/1
D       10.1.100.0/24 [90/28416] via 10.1.2.13, 00:01:43, FastEthernet0/1
C       10.1.203.1/32 is directly connected, Loopback0
D       10.1.200.0/24 [90/28416] via 10.1.2.13, 00:01:43, FastEthernet0/1
D    192.168.1.0/24 [90/158976] via 10.1.2.13, 00:01:43, FastEthernet0/1
D*EX 0.0.0.0/0 [170/2175232] via 10.1.2.13, 00:01:43, FastEthernet0/1
```

In the above example, all expected routes are present in the R3 routing table. This does not prove that authentication is occurring. However, it does indicate that either authentication is configured correctly for both adjacent interfaces, or it is not configured at all for both adjacent interfaces.

Reflection Questions

1. Which lab trouble tickets did you have the most difficulty with?

---

2. Would you change anything about the process that you used for any of the trouble tickets now that you see the resolution of the problem?

---

3. Which commands did you find most useful in diagnosing control plane security issues? Add these to your toolbox for future use. Which commands did you find least useful?

References

If you need more information on the commands and their options, see the following references

- IP Routing Protocol
  http://www.cisco.com/cisco/web/support/index.html
- Cisco IOS IP Switching

  http://www.cisco.com/en/US/docs/ios/ipswitch/command/reference/isw_book.html
- Configuring DHCP Features on a Cisco 2960 Switch
  http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_37_se/configuration/guide/swdhcp82.html
- Configuring EIGRP Message Authentication
  http://www.cisco.com/en/US/tech/tk365/technologies_configuration_example09186a00807f5a63.shtml

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1700	Fast Ethernet 0 (FA0)	Fast Ethernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
1800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2600	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)
2800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. Rather than try to list all the combinations of configurations for each router class, this table includes identifiers for the possible combinations of Ethernet and serial interfaces in the device. The table does not include any other type of interface, even though a specific router might contain one. An example of this is an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

Device Configurations (instructor version)

Note: All device configurations are provided for TT-A. The configs provided here are *not* running-config outputs. They can be used for cut-and-paste for TT-A and subsequent tickets. Where a config is noted as being the same as a previous one, the only change is in the MOTD, which identifies the Lab and TT. The errors in the configuration are commented and highlighted as red text.

Trouble Ticket—TT-A Configurations

Switch ALS1

```
!Lab 9-2 Switch ALS1 TT-A Config
!
hostname ALS1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 9-2 Switch ALS1 TT-A Config ***$
!
ip dhcp snooping vlan 10
ip dhcp snooping
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
```

```
spanning-tree mode rapid-pvst
spanning-tree portfast default
!
interface Vlan1
 no ip address
 shutdown
!
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 100
 name MGMT
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel1
 description Channel to DLS1
 ip dhcp snooping trust
 no shutdown
 !
interface Port-channel2
 description Channel to DLS2
 no shutdown
!
interface FastEthernet0/1
 description Channel to DLS1
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 ip dhcp snooping trust
 no shutdown
!
interface FastEthernet0/2
 description Channel to DLS1
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 ip dhcp snooping trust
 no shutdown
!
interface FastEthernet0/3
```

Error: Interface Po2 is not trusted. Add ip dhcp snooping trust to Po2 interface. This will automatically add it to member ports Fa0/3 and Fa0/4.

```
interface Port-channel2
 ip dhcp snooping trust
```

```
 description Channel to DLS2
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shutdown
!
interface FastEthernet0/4
 description Channel to DLS2
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shutdown
!
interface FastEthernet0/5
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown

interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
```



```
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description To PC-B
 switchport access vlan 10
 switchport mode access
 switchport voice vlan 20
 spanning-tree portfast
 switchport port-security
 switchport port-security maximum 2
```



```
 switchport port-security violation shutdown
 switchport port-security mac-address sticky
 no shut
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitetherneт0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
```

```
 shutdown
!
interface Vlan100
 ip address 10.1.100.1 255.255.255.0
 no shutdown
!
ip default-gateway 10.1.100.254
!
ip http server
ip http secure-server
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server host 10.1.50.1 version 2c cisco
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps vlan-membership
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
  no transport input
!
ntp source Vlan100
ntp server 192.168.2.1
end
```

Switch DLS1

```
!Lab 9-2 Switch DLS1 TT-A Config
!
hostname DLS1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55

banner motd $*** Lab 9-2 Switch DLS1 TT-A Config ***$
!
```



```
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
!
ip domain name tshoot.net
!
ip dhcp excluded-address 10.1.10.252 10.1.10.254
ip dhcp excluded-address 10.1.20.252 10.1.20.254
ip dhcp excluded-address 10.1.30.252 10.1.30.254
!
ip dhcp pool OFFICE
   network 10.1.10.0 255.255.255.0
   default-router 10.1.10.254
   domain-name tshoot.net
!
ip dhcp pool VOICE
   network 10.1.20.0 255.255.255.0
   default-router 10.1.20.254
   domain-name tshoot.net
!
ip dhcp pool GUEST
   network 10.1.30.0 255.255.255.0
   default-router 10.1.30.254
   domain-name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 24576
spanning-tree vlan 20,50 priority 28672
!
vlan 10
 name OFFICE
```

Error: DHCP relay information from ALS1 is not trusted.

`ip dhcp relay information trust-all`

```
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 100
 name MGMT
!
vlan 200
 name TRANS
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel1
 description Channel to ALS1
 no shut
!
interface Port-channel10
 description Channel to DLS2
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
```

```
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R1
 no switchport
 ip address 10.1.2.1 255.255.255.252
 speed 100
 duplex full
 spanning-tree bpduguard enable
 no shut
!
interface FastEthernet0/6
 description FE to SRV1
 switchport access vlan 50
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shut
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
```



```
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
```



```
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
```



```
 shutdown

interface Vlan10
 ip address 10.1.10.252 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 priority 110
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.252 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.252 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 priority 110
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.252 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 preempt
!
interface Vlan100
 ip address 10.1.100.252 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 priority 110
 standby 100 preempt
!
interface Vlan200
 ip address 10.1.200.252 255.255.255.0
!
router eigrp 1
 passive-interface default
 no passive-interface Fa0/5
 no passive-interface vlan200
 no auto-summary
 network 10.1.0.0 0.0.255.255
!
ip classless
ip http server
ip http secure-server
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server host 10.1.50.1 version 2c cisco
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
```



```
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 192.168.2.1
end
```

Switch DLS2

```
!Lab 9-2 Switch DLS2 TT-A Config
!
hostname DLS2
!
service timestamps debug datetime msec
service timestamps log datetime
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 9-2 Switch DLS2 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard!
!
```



```
archive
 log config
  logging size 50
  notify syslog
  hidekeys
  path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 28672
spanning-tree vlan 20,50 priority 24576

vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 100
 name MGMT
!
vlan 200
 name TRANS
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel2
 description Channel to ALS1
 no shut

interface Port-channel10
 description Channel to DLS1
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
```



```
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R3
 no switchport
 ip address 10.1.2.13 255.255.255.252
 speed 100
 duplex full
 spanning-tree bpduguard enable
 no shutdown
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
```

```
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
```

```
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/1
```

```
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 10.1.10.253 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.253 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 priority 110
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.253 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.253 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 priority 110
 standby 50 preempt
!
interface Vlan100
 ip address 10.1.100.253 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 preempt
!
interface Vlan200
 ip address 10.1.200.253 255.255.255.0
!
router eigrp 1
 passive-interface default
 no passive-interface Fa0/5
 no passive-interface vlan200
 no auto-summary
 network 10.1.0.0 0.0.255.255
!
ip classless
ip http server
ip http secure-server
!
```



```
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 192.168.2.1
end
```

Router R1

```
!Lab 9-2 Router R1 TT-A Config
!
hostname R1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 9-2 Router R1 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
```



```
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 192.168.1.1 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown
!
interface FastEthernet0/1
 description FE to DLS1
 ip address 10.1.2.2 255.255.255.252
 ip flow ingress
 ip nat inside
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
 description WAN link to ISP R2
 ip address 209.165.200.225 255.255.255.252
 ip nat outside
 ip flow ingress
 encapsulation ppp
 clock rate 128000
  no shutdown
!
interface Serial0/0/1
 shutdown
!
router eigrp 1
 redistribute static
 passive-interface default
 no passive-interface FastEthernet0/1
 network 10.1.2.0 0.0.0.3
 network 192.168.1.1 0.0.0.0
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 209.165.200.226
!
ip http server
no ip http secure-server
!
```

```
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
ip nat pool public-addrs 198.133.219.10 198.133.219.30 netmask 255.255.255.224
ip nat inside source list 1 pool public-addrs
ip nat inside source static 10.1.50.1 198.133.219.1
!
logging source-interface Loopback0
logging 10.1.50.1
!
access-list 1 permit 10.1.0.0 0.0.255.255
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 192.168.2.1
end
```

Router R2

```
!Lab 9-2 Router R2 TT-A Config
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
Hostname R2
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 9-2 Router R2 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
```



```
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 192.168.2.1 255.255.255.255
!
interface FastEthernet0/0
 shutdown
!
interface FastEthernet0/1
 shutdown
!
interface Serial0/0/0
 description WAN link to R1 – T1 leased line
 ip address 209.165.200.226 255.255.255.252
 encapsulation ppp
 no shutdown
 !
interface Serial0/0/1
 shutdown
!
ip route 192.168.1.1 255.255.255.255 209.165.200.225
ip route 198.133.219.0 255.255.255.224 209.165.200.225
!
ip http server
no ip http secure-server
!
logging source-interface Loopback0
logging 10.1.50.1
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
```

```
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
!
ntp master 3
 end
```

Router R3

```
!Lab 9-2 Router R3 TT-A Config
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 9-2 Router R3 TT-A Config ***$
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
no ip domain lookup
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 10.1.203.1 255.255.255.255
!
interface FastEthernet0/0
 description FE to R3 LAN
```



```
 ip address 10.1.80.1 255.255.255.0
 ip flow ingress
 speed 100
 full-duplex
 no shutdown
!
interface FastEthernet0/1
 description FE to DLS2
 ip address 10.1.2.14 255.255.255.252
 ip flow ingress
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
description WAN link to R1 – not used for this lab
 no ip address
 clock rate 128000
 encapsulation ppp
 shutdown
!
interface Serial0/0/1
 shutdown
!
router eigrp 1
 passive-interface default
 no passive-interface FastEthernet0/1
 network 10.1.2.12 0.0.0.3
 network 10.1.80.0 0.0.0.255
 network 10.1.203.1 0.0.0.0
 no auto-summary
!
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
logging source-interface Loopback0
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
```



```
 exec-timeout 60 0
transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 192.168.2.1
end
```

Trouble Ticket—TT-B Configurations

Router R1—Same as TT-A

Router R2—Same as TT-A

Switch ALS1

```
!Lab 9-2 Switch ALS1 TT-B Config
!
hostname ALS1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 9-2 Switch ALS1 TT-B Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
```



```
file prompt quiet

spanning-tree mode rapid-pvst
spanning-tree portfast default
!
interface Vlan1
 no ip address
 shutdown
!
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 100
 name MGMT
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel1
 description Channel to DLS1
 no shutdown
  !
interface Port-channel2
 description Channel to DLS2
 no shutdown
!
interface FastEthernet0/1
 description Channel to DLS1
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shutdown
!
interface FastEthernet0/2
 description Channel to DLS1
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shutdown
!
interface FastEthernet0/3
 description Channel to DLS2
```



```
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shutdown
!
interface FastEthernet0/4
 description Channel to DLS2
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shutdown
!
interface FastEthernet0/5
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown

interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
```



```
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description To PC-B
 switchport access vlan 10
 switchport mode access
 switchport voice vlan 20
 spanning-tree portfast
 switchport port-security
 switchport port-security maximum 2
 switchport port-security violation shutdown
```

```
 switchport port-security mac-address sticky
 no shut
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
```

```
!
interface Vlan100
 ip address 10.1.100.1 255.255.255.0
 no shutdown
!
ip default-gateway 10.1.100.254
!
ip http server
ip http secure-server
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server host 10.1.50.1 version 2c cisco
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps vlan-membership
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
  no transport input
!
ntp source Vlan100
ntp server 192.168.2.1
end
```

Switch DLS1

```
!Lab 9-2 Switch DLS1 TT-B Config
!
hostname DLS1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 9-2 Switch DLS1 TT-B Config ***$
!
no ip domain lookup
```

```
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
!
ip domain name tshoot.net
!
ip dhcp excluded-address 10.1.10.252 10.1.10.254
ip dhcp excluded-address 10.1.20.252 10.1.20.254
ip dhcp excluded-address 10.1.30.252 10.1.30.254
!
ip dhcp pool OFFICE
   network 10.1.10.0 255.255.255.0
   default-router 10.1.10.254
   domain-name tshoot.net
!
ip dhcp pool VOICE
   network 10.1.20.0 255.255.255.0
   default-router 10.1.20.254
   domain-name tshoot.net
!
ip dhcp pool GUEST
   network 10.1.30.0 255.255.255.0
   default-router 10.1.30.254
   domain-name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 24576
spanning-tree vlan 20,50 priority 28672
!
vlan 10
 name OFFICE
!
vlan 20
```



```
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 100
 name MGMT
!
vlan 200
 name TRANS
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel1
 description Channel to ALS1
 no shut
!
interface Port-channel10
 description Channel to DLS2
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
```



```
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R1
 no switchport
 ip address 10.1.2.1 255.255.255.252
 speed 100
 duplex full
 spanning-tree bpduguard enable
 no shut
!
interface FastEthernet0/6
 description FE to SRV1
 switchport access vlan 50
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shut
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
```



```
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/19
 description Unused
```



```
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
```



```
interface Vlan10
 ip address 10.1.10.252 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 priority 110
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.252 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.252 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 priority 110
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.252 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 preempt
!
interface Vlan100
 ip address 10.1.100.252 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 priority 110
 standby 100 preempt
!
interface Vlan200
 ip address 10.1.200.252 255.255.255.0
!
router eigrp 1
 passive-interface default
 no passive-interface Fa0/5
 no passive-interface vlan200
 no auto-summary
 network 10.1.0.0 0.0.255.255
!
ip classless
ip http server
ip http secure-server
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server host 10.1.50.1 version 2c cisco
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps config
snmp-server enable traps hsrp
```



```
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 192.168.2.1
end
```

Switch DLS2

```
!Lab 9-2 Switch DLS2 TT-B Config
!
hostname DLS2
!
service timestamps debug datetime msec
service timestamps log datetime
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 9-2 Switch DLS2 TT-B Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard!
!
key chain EIGRPCHAIN
 key 1
```

```
  key-string eigrpbadkey
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
  path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 28672
spanning-tree vlan 20,50 priority 24576

vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 100
 name MGMT
!
vlan 200
 name TRANS
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel2
 description Channel to ALS1
 no shut

interface Port-channel10
 description Channel to DLS1
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
```

Error: Key-string does not match R3 key-string. Change the key to match R3.

```
key chain EIGRPCHAIN
 key 1
  key-string eigrpkey
```

```
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R3
 no switchport
 ip address 10.1.2.13 255.255.255.252
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 EIGRPCHAIN
 speed 100
 duplex full
 spanning-tree bpduguard enable
 no shutdown
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
```



```
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
```

```
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown

interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
```



```
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 10.1.10.253 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.253 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 priority 110
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.253 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.253 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 priority 110
 standby 50 preempt
!
interface Vlan100
 ip address 10.1.100.253 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 preempt
!
interface Vlan200
 ip address 10.1.200.253 255.255.255.0
!
router eigrp 1
 passive-interface default
 no passive-interface Fa0/5
 no passive-interface vlan200
 no auto-summary
 network 10.1.0.0 0.0.255.255
!
```



```
ip classless
ip http server
ip http secure-server
!
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 192.168.2.1
end
```

Router R3

```
!Lab 9-2 Router R3 TT-B Config
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 9-2 Router R3 TT-B Config ***$
!
aaa new-model
aaa authentication login default local
```

```
aaa authentication login CONSOLE none
aaa authorization exec default local
!
no ip domain lookup
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
key chain EIGRPCHAIN
 key 1
   key-string eigrpkey
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 10.1.203.1 255.255.255.255
!
interface FastEthernet0/0
 description FE to R3 LAN
 ip address 10.1.80.1 255.255.255.0
 ip flow ingress
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 EIGRPCHAIN
 speed 100
 full-duplex
 no shutdown
!
interface FastEthernet0/1
 description FE to DLS2
 ip address 10.1.2.14 255.255.255.252
 ip flow ingress
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
description WAN link to R1 – not used for this lab
 no ip address
 clock rate 128000
 encapsulation ppp
 shutdown
!
interface Serial0/0/1
 shutdown
!
router eigrp 1
 passive-interface default
```

Error: EIGRP authentication should not be configured on Fa0/0. It should be on Fa0/1. Remove it from Fa0/0.

```
interface fa0/0
 no ip authentication mode eigrp 1 md5
 no ip authentication key-chain eigrp 1 EIGRPCHAIN
```

Error: EIGRP authentication is missing from Fa0/1. Add it to Fa0/1.

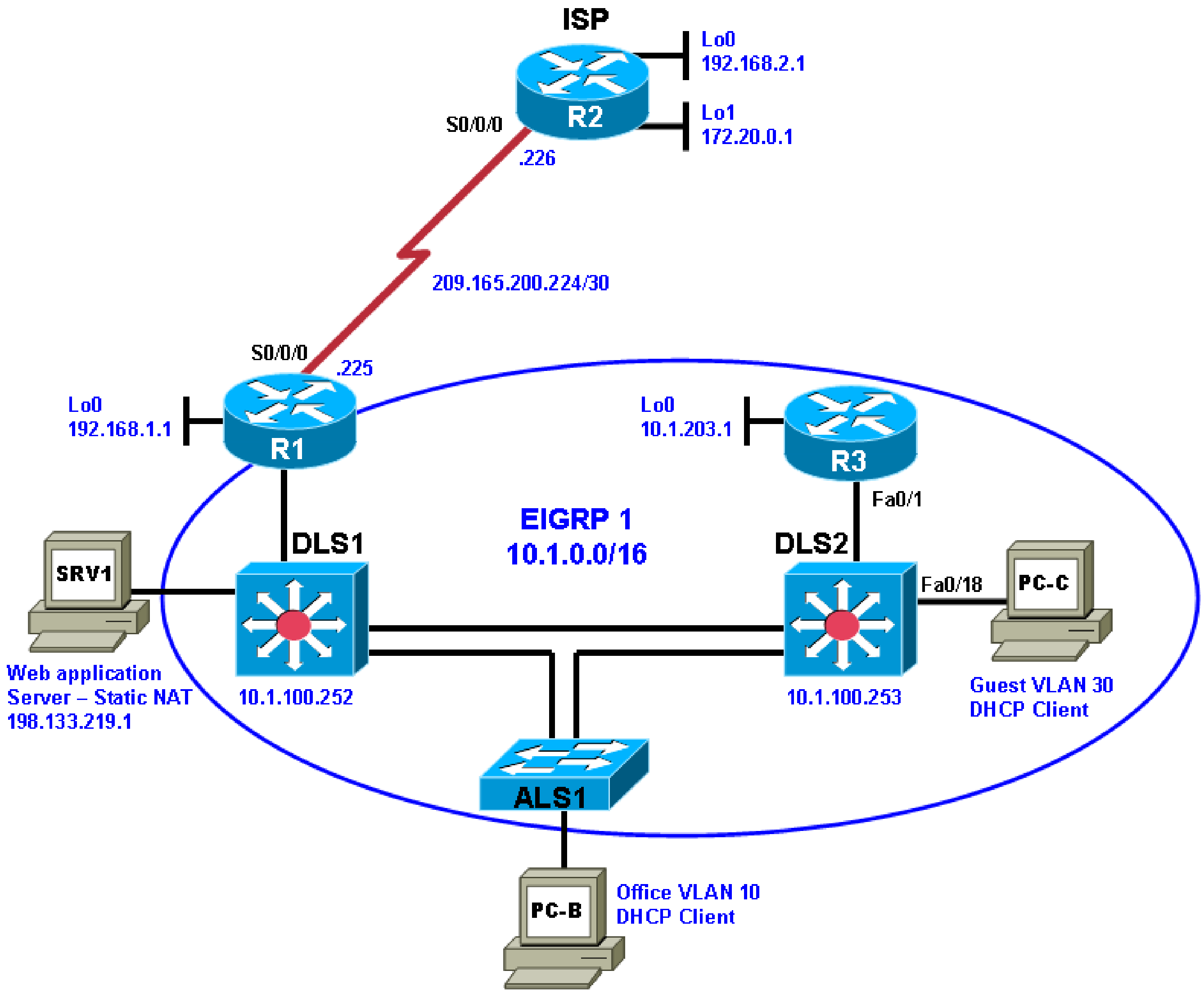
```
interface fa0/1
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 EIGRPCHAIN
```



```
 no passive-interface FastEthernet0/1
 network 10.1.2.12 0.0.0.3
 network 10.1.80.0 0.0.0.255
 network 10.1.203.1 0.0.0.0
 no auto-summary
!
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
logging source-interface Loopback0
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 192.168.2.1
end
```

Chapter 9 Lab 9-3, Data Plane Security **Instructor Version**

Lab Topology



Objectives

- Load the device configuration files for each trouble ticket.
- Diagnose and resolve problems related to router and switch data plane security.
- Document the troubleshooting progress, configuration changes, and problem resolution.

Background

Routers and Layer 3 switches are typically segmented into three planes of operation, each with a clearly identified objective. The data plane (also called the forwarding plane) forwards user data packets. The control plane routes data correctly. The management plane provides administrative access to network devices.

The data plane encompasses all “customer” application traffic. Customer traffic refers to traffic generated by hosts, clients, servers, and applications that are intended to use the network for the purpose of transport only. Data plane traffic should never have destination IP addresses that belong to any networking devices (routers or switches). Instead, data plane traffic should be sourced from and destined to other devices, such as PCs and servers, that are supported by the network. The primary job of the router or Layer 3 switch is to forward these packets downstream as quickly as possible. Routers and switches can inspect and filter traffic as part of the implementation of a security policy.

Examples of security features implemented on the data plane include ACLs, NAT, firewalls, IPS, switch port security, VLAN ACLs (VACLs), IP Source Guard, private VLANs, Storm Control, and VPNs.

This lab focuses on data plane security issues related to Cisco IOS stateful firewalls and VLAN ACLs for routers and Layer 3 switches.

For each task or trouble ticket, the trouble scenario and problem symptom are described. While troubleshooting, you will discover the cause of the problem, correct it, and then document the process and results.

Lab Structure

This lab is divided into two main sections.

Section 1—Trouble Tickets and Troubleshooting Logs

This section includes two tasks. Each task is associated with a trouble ticket (TT) and introduces one or more errors on one or more devices. If time is a consideration, each task or trouble ticket can be performed independently.

Section 2—Troubleshooting Reference Information

This section provides general troubleshooting information that can be applied to any of the trouble tickets in this lab. Examples of useful commands and output are provided. If time permits, it is recommended that you read through Section 2 prior to starting on the trouble tickets.

Instructor note: Because the troubleshooting reference section is lengthy, ask students to read through it prior to starting the lab to become familiar with the commands used in this lab. Consider assigning it as homework.

Note: This lab uses Cisco 1841 routers with Cisco IOS Release 12.4(24)T1 and the Advanced IP Services image c1841-advipservicesk9-mz.124-24.T1.bin. The switches are Cisco WS-C2960-24TT-L with the Cisco IOS image c2960-lanbasek9-mz.122-46.SE.bin and Catalyst 3560-24PS with the Cisco IOS image c3560-advipservicesk9-mz.122-46.SE.bin. Other routers (such as 2801 and 2811), switches (such as 2950 or 3550), and Cisco IOS Software versions can be used if they have comparable capabilities and features. Depending on the router or switch model and Cisco IOS Software version, the commands available and output produced might vary from what is shown in this lab.

Any changes made to configurations or topology (other than errors introduced) are noted in the lab and trouble tickets so that you are aware of them prior to beginning the troubleshooting process.

Instructor Notes

- The lab topology should be pre-built prior to the students starting the lab. Ensure that all routers and switches (R1, R2, R3, ALS1, DLS1, and DLS2) have the course lab configuration files installed in flash. You can download the files from the Academy Connection website.
- The device configurations that contain trouble ticket errors and modifications from the baseline are included at the end of the lab, and the errors in them are identified.

- Each device should have a directory named “tshoot” in flash. This directory contains the baseline configuration file for that device as well as the configuration files for the labs in this course. Refer to Lab 3-1 for instructions on creating the tshoot directory in flash.
- Instructors can use a TFTP server, USB drive, flash memory card or other method to copy all the course configuration files into the flash:/tshoot directory for each device in the topology.
- The student is responsible for loading the baseline or trouble ticket configurations as required using the procedure described in Lab 3-1.
- Set the correct time on router R2, which serves as the primary NTP server for the lab network.
- If time is an issue, each task (trouble ticket) can be performed independently.

Required Resources

- 3 routers (Cisco 1841 with Cisco IOS Release 12.4(24)T1 Advanced IP Service or comparable)
- 1 switch (Cisco 2960 with the Cisco IOS Release 12.2(46)SE C2960-LANBASEK9-M image or comparable)
- 2 switches (Cisco 3560 with the Cisco IOS Release 12.2(46)SE C3560-LANBASEK9-M image or comparable)
- SRV1 (Windows PC with 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

Instructor Notes

- This lab is divided into multiple tasks. Each task is associated with a trouble ticket (TT) and introduces one or more errors on one or more devices.
- Students can work individually or as a team.
- Suggested actions and results used during the troubleshooting process for each TT can be shared with the students during debrief or copies of the instructor version of the lab can be made available to the students to assist them in verifying their work.

Section 1—Trouble Tickets and Troubleshooting Logs

Task 1: Trouble Ticket Lab 9-3 TT-A

Instructor note: This trouble ticket involves device R1 and issues related to the Cisco IOS stateful firewall configuration.

Step 1: Review trouble ticket Lab 9-3 TT-A.

As a security measure, your company has decided to implement stateful packet inspection using a Cisco IOS firewall on edge router R1. The firewall will allow traffic from external hosts only if it is a response to a legitimate request from an internal host. The only exception is that Internet access to the internal SRV1 web-based application will be allowed. Internal users should be able to access the Internet (simulated by Lo1 on R2) using various protocols, such as ICMP, FTP, Telnet, DNS, and HTTP. The firewall implementation must work in conjunction with the dynamic NAT currently being employed on R1. In addition, internal network devices must be able to obtain the correct time from the ISP (R2).

You colleague has configured the firewall and the necessary access lists on R1. However, users on the office VLAN cannot access Internet websites, and remote users on the Internet cannot access the web-based application on SRV1. Your colleague has asked for your help in diagnosing and solving the problem.

Step 2: Load the device trouble ticket configuration files for TT-A.

Using the procedure described in Lab 3-1, verify that the lab configuration files are present in flash. Load the proper configuration files as indicated in the Device Configuration File table.

Note: The following device access methods are in effect after loading the configuration files:

- Console access requires no username or password.
- Telnet and SSH require username **admin** and password **adminpa55**.
- The enable password is **ciscoenpa55**.

Instructor note: Although it is not considered security best practice, the enable secret and admin user passwords can be changed to something simpler to facilitate performance of this lab.

Device Configuration File Table

Device Name	File to Load	Notes
ALS1	Lab93-ALS1-TT-A-Cfg.txt	This file contains configurations different than the baseline
DLS1	Lab93-DLS1-TT-A-Cfg.txt	This file contains configurations different than the baseline
DLS2	Lab93-DLS2-TT-A-Cfg.txt	This file contains configurations different than the baseline
R1	Lab93-R1-TT-A-Cfg.txt	This file contains configuration errors
R2	Lab93-R2-TT-A-Cfg.txt	This file contains configurations different than the baseline
R3	Lab93-R3-TT-A-Cfg.txt	This file contains configurations different than the baseline
SRV1	N/A	Static IP: 10.1.50.1 Default gateway: 10.1.50.254
PC-B	N/A	DHCP
PC-C	N/A	DHCP

Instructor note: The student loads the “broken” TT configuration files for all devices, even though only the configurations indicated in the Notes column contain errors.

Step 3: Configure SRV1.

Configure SRV1 with static IP address 10.1.50.1/24 and default gateway 10.1.50.254.

Step 4: Release and renew the DHCP lease on PC-B.

a. Ensure that PC-B is configured as a DHCP client in the OFFICE VLAN.

b. After loading all TT-A device configuration files, issue the **`ipconfig /release`** and **`ipconfig /renew`** commands on PC-B.

Step 5: Outline the troubleshooting approach and validation steps.

Use this space to identify your troubleshooting approach and the key steps to verify that the problem is resolved. Troubleshooting approaches to select from include the follow-the-path, spot-the-differences, bottom-up, top-down, divide-and-conquer, shoot-from-the-hip, and move-the-problem methods.

Note: In addition to a specific approach, you can use the generic troubleshooting process described at the beginning of Section 2 of this lab.

____

____

____

____

____

____

The spot-the-differences or shoot-from-the-hip method can be used. Other problem-solving methods are the top-down, bottom-up, follow-the-path, divide-and-conquer, and move-the-problem approaches.

Verification steps can include:

- PC-B can access the Internet (simulated R2 Lo1 172.20.0.1) using a web browser (assumes a web GUI on R2).
- Remote users on the Internet (simulated by R2 Lo1 172.20.0.1) can access SRV1 (verified by ping unless a web server is running on SRV1).
- R1 and other internal network devices can get NTP updates from R2 Lo0 IP address 192.168.2.1.

Step 6: Record the troubleshooting process and configuration changes.

Note: Section 2 of this lab includes useful commands and examples of output.

Use this log to document your actions and results during the troubleshooting process. List the commands you used to gather information. As you progress, record what you think the problem might be and the actions you take to correct the problem.

Device	Actions and Results

Device	Actions and Results

Responses will vary but could include:

TT-A Issue 1

HTTP is not specified for inspection by the firewall. As a result, no HTTP responses are allowed from external hosts to internal hosts when the internal hosts initiate web requests.

- Attempts to access Internet websites (simulated by R2 Lo1 172.20.0.1) from PC-B via a browser fail.
- Pings from PC-B to R2 Lo1 (172.20.0.1) succeed.
- Telnet attempts from PC-B to R2 Lo1 (172.20.0.1) succeed.
- The **`show ip nat translations`** command on R1 indicates that there is valid NAT translation for the ping, Telnet, and an attempted HTTP session from PC-B. It appears that NAT is functioning properly.
- Issuing the **`show ip inspect sessions`** command on R1 quickly after the pings indicates that a session exists for the ping and Telnet to R2 Lo1, but none for the web access attempt.
- The **`show run int s0/0/0`** command on R1 indicates that FW-ACL is applied correctly as incoming on S0/0/0, and inspection rule FW-inspect is applied correctly as outgoing on S0/0/0.
- The **`show ip inspect interfaces`** command on R1 confirms that an outgoing inspection rule named FW-inspect inspects FTP, SMTP, TFTP, DNS, ICMP, and Telnet is configured on S0/0/0. It does not inspect HTTP traffic, which is a requirement for an external web server (simulated by R2 Lo1 172.20.0.1) to respond to web requests from internal clients.

Action: Enable inspection of HTTP traffic. See the TT-A debrief for more information.

Verification: Attempts to access R2 Lo1 (172.20.0.1) from PC-B via a web browser succeed.

TT-A Issue 2

The R1 firewall ACL inbound on S0/0/0 does not permit remote users from the Internet (simulated by R2 Lo1) to access the SRV1 static NAT address (198.133.219.1). As a result, R2 cannot ping SRV1.

- Remote users on the Internet (R2 Lo1 172.20.0.1) cannot access SRV1 at static address 198.133.219.1 by ping or via a web browser. The command used is `R2#`**`ping 198.133.219.1 source Lo1`**.
- Pings to SRV1 (198.133.219.1) from any R2 interface or address fail.

Note: To actually test web access, a web server must be running on SRV1, but this is not a requirement for the lab.

- The **`show ip nat translations`** command on R1 indicates that there is a valid static NAT entry for the internal SRV1 IP address translation. The inside global address is 198.133.219.1, and the inside local address is 10.1.50.1.
- The **`show access-lists`** command on R1 indicates that there is an ACL named FW-ACL that denies all incoming traffic on S0/0/0, and there is a high number of matches on the **`deny ip any any`** statement.
- The **`clear ip access-list counters`** command on R1 resets the ACL counters, and the pings from R2 to R1 are repeated.
- The **`show access-lists`** command on R1 indicates that the number of matches increases by 5, which is the number of ping attempts. The ACL is blocking access to SRV1 from the Internet.

Note: The number of matches might increase by more than 5 as a result of other blocked traffic.

Action:

- Add a statement to FW-ACL on R1 that permits HTTP traffic (www or port 80) from any external address that is destined for SRV1.
- Add a statement to FW-ACL allowing ICMP (ping) for testing purposes.
- These entries must be before the **`deny ip any any`** statement. See the TT-A debrief for more information.

Verification: Remote users on the Internet (simulated by R2 Lo1 172.20.0.1) can access SRV1 at static address 198.133.219.1 by ping or via a web browser, if one is installed on SRV1.

TT-A Issue 3

NTP is not specified for inspection by the firewall. As a result, no NTP responses are allowed to NTP requests from internal devices, and ALS1, DLS1, DLS2, and R3 cannot synchronize their time with the R2 NTP server.

Note: NTP is a management plane issue. However, the problem is caused by data plane security measures.

- Pings from R1 to R2 at Lo0 (NTP address 192.168.2.1) fail.
- The **`show ip nat translations`** command on R1 indicates that there are entries for NTP requests, one for each internal device as it attempts to synchronize with the NTP server R2 at 192.168.2.1.
- The **`show ntp associations`** command on DLS1 indicates that R2 address 192.168.2.1 is configured as the NTP server, but the reference clock is still in the INIT state.
- The **`show ntp status`** command on DLS1 indicates that the clock is unsynchronized and that there is no reference clock IP address.
- The **`show ip inspect interfaces`** command on R1 confirms that rule FW-inspect inspects FTP, SMTP, TFTP, DNS, ICMP, Telnet, and HTTP. It does not inspect NTP traffic, which is a requirement for an external NTP server (R2) to respond to NTP requests from internal clients.

Action: Enable inspection of NTP traffic. See TT-A debrief for more information.

Verification:

- The **`show ntp associations`** command on DLS1, DLS2, ALS1, and R3 indicates that R2 address 192.168.2.1 is configured as the NTP server and is shown as the master (synced).

- The **show ntp status** command on R1 indicates that the clock is unsynchronized. There is no reference clock. There must be another problem.

TT-A Issue 4

R1 NTP requests to R2 are sourced from external interface S0/0/0 (IP address 209.165.200.225) or loopback 0 (IP address 192.168.1.1) if the command **ntp source Loopback0** is configured. In either case, they cannot be inspected by the stateful firewall, because they do not originate from inside the firewall. The stateful firewall rule FW-inspect now inspects NTP. However, the R1 firewall ACL inbound on S0/0/0 does not permit NTP responses from R2 to R1 NTP requests. R1 cannot peer with the R2 NTP server and obtain updates.

- The **show access-lists** command on R1 indicates that FW-ACL denies all incoming traffic on S0/0/0, and there is a high number of matches.
- After adding the **log** keyword to the end of the **deny ip any any** statement for FW-ACL, log messages are displayed on the R1 console, and the syslog server indicates that the ACL is blocking R2 NTP updates being sent to R1.

Action: Add a statement to FW-ACL on R1 that permits NTP traffic from the R2 NTP server IP address 192.168.2.1 to R1 (S0/0/0 or Lo0 IP address, depending on which is used as the NTP source). See the TT-A debrief for more information.

Verification:

- The **show ntp associations** command on R1 indicates that R2 address 192.168.2.1 is configured as the NTP server and is the master. The reference clock is the internal clock 127.127.1.1.
- The **show ntp status** command on R1 indicates that the clock is synchronized, the stratum is level 4, and the reference clock is 192.168.2.1.
- The FW-ACL **deny ip any any log** messages stop displaying on the console and syslog server.

Instructor note: NTP is a management plane, not a data plane issue. However, problems with NTP can stem from data plane security measures that are intended to control user access. NTP functionality for all network devices is part of the requirement specified in the implementation test plan.

Step 7: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with the instructor. The notes can include problems encountered, solutions applied, useful commands employed, alternate solutions, methods, and processes, and procedure and communication improvements.

____

____

____

____

____

____

____

Trouble Ticket TT-A Debrief—Instructor Notes

This trouble ticket consists of four network connectivity issues related to the Cisco IOS stateful firewall on R1 and the associated ACL.

TT-A Issue 1

HTTP is not specified for inspection by the stateful firewall FW-inspect. The traffic must be inspected on the way out for the inbound firewall ACL to be dynamically adjusted to permit the return traffic. As a result, no HTTP responses to internal host web requests are allowed to reach internal hosts. This has no effect on HTTP traffic between internal clients and internal web servers. Only HTTP traffic that passes through the firewall is affected.

Enable inspection of HTTP traffic using the following command on R1:

```
ip inspect name FW-inspect http
```

Note: The inspection rule FW-inspect is currently applied to S0/0/0 in the outbound direction. The inspection rule could also be applied incoming on R1 Fa0/1 because this is the only interface that connects to the internal network. If there is more than one inside interface, applying the rule to the external interface S0/0/0 provides a single exit and entry point for the network.

TT-A Issue 2

By default, the R1 firewall ACL FW-ACL that is applied inbound on S0/0/0 does not permit users from the Internet (simulated by R2 Lo1) to access the SRV1 static NAT address (198.133.219.1). As a result, R2 cannot access (ping or browse) SRV1. The ACL can be removed and recreated, or the necessary statements can be added to the existing ACL by sequence number. The single existing **deny ip any any** statement is sequence number 10.

Note: You can use the **show access-lists** command to see all ACLs configured and their current statement line numbers, as shown in the following example.

```
R1#show access-lists
Standard IP access list 1
    10 permit 10.1.0.0, wildcard bits 0.0.255.255
Extended IP access list FW-ACL
    10 deny ip any any
```

To allow external access to internal server SRV1 via HTTP (www) and ping (ICMP), use the following commands on R1:

```
ip access-list extended FW-ACL
 3 permit tcp any host 198.133.219.1 eq www
 5 permit icmp any host 198.133.219.1
```

TT-A Issue 3

NTP is not specified for inspection by the firewall, and no NTP updates are allowed in response to internal requests. As a result, DLS1, DLS2, ALS1, and R3 cannot synchronize their time with the R2 NTP server.

Enable inspection of NTP traffic using the following command on R1:

```
ip inspect name FW-inspect ntp
```

Note: NTP is a management plane, not a data plane issue. However, the problems stem from data plane security measures that are intended to control user access. NTP functionality for all network devices is part of the requirement specified in the implementation test plan. It not uncommon for firewalls to cause unintended consequences, such as NTP and routing protocol update issues.

TT-A Issue 4

The R1 firewall ACL inbound on S0/0/0 does not permit NTP responses from R2 to R1 NTP requests. As a result, R1 cannot peer with the R2 NTP server and obtain updates. R1 NTP requests are sourced from interface S0/0/0 by default (or loopback 0, if **`ntp source Lo0`** is configured) and not from the internal network (10.1.x.x/16). They are not inspected by the firewall. As a result, NTP update responses from R2 (192.168.2.1) are denied. All other NTP requests from internal devices are inspected, and responses are permitted if TT-A Issue 3 is corrected.

To allow NTP responses from R2 to R1, add a statement to FW-ACL on R1 that permits NTP traffic from the R2 NTP server IP address 192.168.2.1 to R1 (S0/0/0 or Lo0 IP address, depending on which is used).

Instructor Note: The **`ntp source Loopback0`** command can be an issue when copying configurations from flash. If the **`ntp source Loopback0`** command is configured on R1, the log message will be:

```
%SEC-6-IPACCESSLOGP: list FW-ACL denied udp 192.168.2.1(123) ->
192.168.1.1(123), 1 packet
```

Use the Lo0 IP address 192.168.1.1 if the **`ntp source Loopback0`** command is applied on R1.

```
ip access-list extended FW-ACL
 7 permit udp host 192.168.2.1 host 192.168.1.1 eq ntp
```

If the **`ntp source Loopback0`** command is not configured on R1, the log message will be:

```
%SEC-6-IPACCESSLOGP: list FW-ACL denied udp 192.168.2.1(123) ->
209.165.200.225(123), 1 packet
```

Use the S0/0/0 IP address 209.165.200.225 if the **`ntp source Loopback0`** command is not applied on R1:

```
ip access-list extended FW-ACL
 7 permit udp host 192.168.2.1 host 209.165.200.225 eq ntp
```

Note: The above commands allow only uninspected NTP traffic from R2 to reach R1. They do not affect NTP or other traffic from internal hosts that is inspected by the stateful firewall. If it is necessary to be able to use ping, Telnet, or SSH from R2 to R1, statements must be added to the FW-ACL to permit these protocols.

Note: When statement sequence numbers are inserted into the ACL, the next time the **`show access-lists`** command is used, they are renumbered by tens (10, 20, 30).

```
R1#show access-lists FW-ACL
Extended IP access list FW-ACL
    10 permit udp host 192.168.2.1 host 192.168.1.1 eq ntp
    20 permit tcp any host 198.133.219.1 eq www
    30 permit icmp any host 198.133.219.1
    40 deny ip any any log
```

Note: The **`log`** option in the above statement 40 **`deny ip any any log`** is normally used when testing or troubleshooting; not for production environments.

Task 2: Trouble Ticket Lab 9-3 TT-B

Instructor note: This trouble ticket involves device DLS2 and issues related to VLAN ACLs and user access.

Step 1: Review trouble ticket Lab 9-3 TT-B.

In a continuing effort to improve network data plane security, your company has decided to limit access for users on the guest VLAN 30 subnet (10.1.30.0/24). Guest VLAN users should not have access to any Office VLAN 10 or Server VLAN 50 resources. In addition, it will be necessary to prevent guests from pinging internal network switches. Although they will not have access to internal resources, guest users must be able to access the Internet from VLAN 30. Guest user PCs are DHCP clients (simulated by PC-C) that connect to the network from Layer 3 core switch DLS2 and obtain their IP addresses from DLS1.

Your colleague has configured a VLAN access control list (VACL) on DLS2 to limit guest access. After the VACL implementation, guests are prevented from accessing Office VLAN and Server VLAN resources, as expected. However, guest users are unable to access the Internet (simulated by R2 Lo1). Your colleague has asked for your help in diagnosing and solving the problem.

Step 2: Load the device trouble ticket configuration files for TT-B.

Using the procedure described in Lab 3-1, verify that the lab configuration files are present in flash. Load the proper configuration files as indicated in the Device Configuration File table.

Note: The following device access methods are in effect after loading the configuration files:

- Console access requires no username or password.
- Telnet and SSH require username **admin** and password **adminpa55**.
- The enable password is **ciscoenpa55**.

Instructor note: Although it is not considered security best practice, the enable secret and admin user passwords can be changed to something simpler to facilitate performance of this lab.

Device Configuration File Table

Device Name	File to Load	Notes
ALS1	Lab93-ALS1-TT-B-Cfg.txt	This file contains configurations different than the baseline
DLS1	Lab93-DLS1-TT-B-Cfg.txt	This file contains configurations different than the baseline
DLS2	Lab93-DLS2-TT-B-Cfg.txt	This file contains configuration errors
R1	Lab93-R1-TT-B-Cfg.txt	This file contains configurations different than the baseline
R2	Lab93-R2-TT-B-Cfg.txt	This file contains configurations different than the baseline
R3	Lab93-R3-TT-B-Cfg.txt	This file contains configurations different than the baseline
SRV1	N/A	Static IP: 10.1.50.1 Default gateway: 10.1.50.254
PC-B	N/A	DHCP
PC-C	N/A	DHCP

Instructor note: The student loads the “broken” TT configuration files for all devices, even though only the configurations indicated in the Notes column contain errors.

Step 3: Configure SRV1.

Configure SRV1 with static IP address 10.1.50.1/24 and default gateway 10.1.50.254.

Step 4: Release and renew the DHCP lease on PC-C.

After loading all TT-B device configuration files, issue the **`ipconfig /release`** and **`ipconfig /renew`** commands on PC-C.

Step 5: Outline the troubleshooting approach and validation steps.

Use this space to identify your troubleshooting approach and the key steps to verify that the problem is resolved. Troubleshooting approaches to select from include the follow-the-path, spot-the-differences, bottom-up, top-down, divide-and-conquer, shoot-from-the-hip, and move-the-problem methods.

Note: In addition to a specific approach, you can use the generic troubleshooting process described at the beginning of Section 2 of this lab.

____

____

____

____

____

____

The follow-the-path or shoot-from-the-hip method can be used. Other problem-solving methods are the bottom-up, top-down, spot-the-differences, divide-and-conquer, and move-the-problem approaches.

Verification steps can include:

- PC-C can access via ping the Internet (simulated by R2 Lo1, IP 172.20.0.1).
- PC-C should not be able to access SRV1 (server VLAN 50).
- PC-C should not be able to access PC-B (office VLAN 10).
- PC-C should not be able to access the DLS2 management address (mgmt VLAN 100: 10.1.100.253).

Step 6: Record the troubleshooting process and configuration changes.

Note: Section 2 of this lab includes useful commands and examples of output.

Use this log to document your actions and results during the troubleshooting process. List the commands you used to gather information. As you progress, record what you think the problem might be and the actions you take to correct the problem.

Device	Actions and Results

Device	Actions and Results

TT-B Issue 1

Access map BLOCK-GUEST is missing a statement that forwards traffic that is not matched in the GUEST-ACCESS-CTRL ACL. The result is that the implicit action “drop” is applied and denies all other traffic, including traffic destined for the Internet.

- Pings from PC-C to the Internet (simulated by R2 Lo1) fail.
- Pings from PC-C to the VLAN 30 default gateway 10.1.30.254 fail.
- A check of PC-C indicates that it is a DHCP client but has not been assigned a VLAN 30 IP address.
- The **`show ip route`** command on DLS2 indicates that all expected routes, including the EIGRP default, are present.
- The **`show ip interface brief`** command on DLS2 indicates that interface VLAN 30 is UP/UP.
- The **`show access-lists`** command on DLS2 indicates that extended IP access list GUEST-ACCESS-CTRL is configured, and it permits VLAN 30 traffic access to the office VLAN and the server VLAN. This is correct because it has the effect of selecting this traffic for subsequent denial.
- The **`show ip interface vlan 30 | include access`** command on DLS2 indicates that no access lists are applied to interface VLAN 30.
- The **`show ip interface fa0/18`** command on DLS2 indicates that interface Fa0/18 is UP/UP, and no access list is set.
- The **`show vlan access-map`** command on DLS2 indicates that access map BLOCK-GUEST is defined with a match clause for IP addresses that uses access list GUEST-ACCESS-CTRL. The action is to drop traffic that matches the ACL.
- The **`show vlan filter`** command on DLS2 indicates that VLAN map BLOCK-GUEST is filtering VLAN 30. It blocks traffic to the office and server VLANs (10 and 50), as it should. However, it does not include a statement to allow traffic destined for locations other than the office or server VLAN, such as the Internet. The implied **`deny any`** at the end of VLAN access map BLOCK-GUEST drops all traffic not matched by ACL GUEST-ACCESS-CTRL.

Action:

- Add another statement to **`vlan access-map BLOCK-GUEST`** that allows traffic destined for any location other than the office or server VLANs to be forwarded.
- Issue the **`ipconfig /release`** and **`ipconfig /renew`** commands on PC-C.
- See the TT-B debrief for more information.

Verification:

- PC-C is able to obtain a VLAN 30 IP address.
- Pings from PC-C to the Internet (simulated by R2 Lo1) succeed.

- Pings from PC-C to the VLAN 30 default gateway 10.1.30.254 succeed.
- Pings from PC-C to office VLAN 10 host PC-B fail.
- Pings from PC-C to server VLAN 50 host SRV1 fail.
- Pings from PC-C to DLS2 management address (mgmt VLAN 100: 10.1.100.253) succeed.

TT-B Issue 2

The access list GUEST-ACCESS-CTRL is missing a statement that permits (selects for blocking) traffic from Guest VLAN 30 that is destined for the management VLAN 100. This allows guest users to ping the network switches. Access to network devices by hosts in the guest VLAN is not permitted by the security policy.

- Pings from PC-C to VLAN 100 host DLS1 at management address 10.1.100.252 or another switch (ALS1 or DLS2) succeed. They should not.
- The **`show access-lists`** command on DLS2 indicates that extended IP access list GUEST-ACCESS-CTRL permits VLAN 30 traffic access to the office VLAN and the server VLAN, as it should. The access map uses the permit statements to block this traffic. However, the ACL does not specify traffic destined for management VLAN 100.

Action: Add statement 30 to the end of ACL GUEST-ACCESS-CTRL to permit (selects for blocking by the BLOCK-GUEST access map) traffic from the VLAN 30 subnet to any VLAN 100 IP address. See the TT-B debrief for more information.

Verification: Pings from PC-C to a switch management address, such as DLS1 at 10.1.100.252, fail, as they should.

Step 7: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with the instructor. The notes can include problems encountered, solutions applied, useful commands employed, alternate solutions, methods, and processes, and procedure and communication improvements.

____

____

____

____

____

____

____

Trouble Ticket TT-B Debrief—Instructor Notes

This trouble ticket consists of two network connectivity issues related to the VLAN access map on DLS2 and the associated ACL. These issues prevent guest VLAN users from accessing the Internet and do not prevent them from accessing internal switches.

TT-B Issue 1

Access map BLOCK-GUEST is missing a statement that forwards traffic that is not matched in the GUEST-ACCESS-CTRL ACL. The result is that the implicit drop action is applied, which denies all other traffic, including traffic destined for the Internet.

To correct this problem, add another statement that allows traffic destined for any location, other than the office or server VLAN, to be forwarded:


```
vlan access-map BLOCK-GUEST 20
  action forward
```

Note: Be sure to issue the **`ipconfig /release`** and **`ipconfig /renew`** commands on PC-C after the VACL changes to verify that it can access the DHCP server.

TT-B Issue 2

The access list GUEST-ACCESS-CTRL is missing a statement that permits (selects for blocking) traffic from Guest VLAN 30 that is destined for management VLAN 100. This allows guest users to ping the network switches, which they should not be able to do. Access to network devices by hosts in the guest VLAN is not permitted by the security policy.

To correct this problem, add a statement to the end of ACL GUEST-ACCESS-CTRL that permits traffic from the VLAN 30 subnet to any VLAN 100 IP address:

```
ip access-list extended GUEST-ACCESS-CTRL
  permit ip 10.1.30.0 0.0.0.255 10.1.100.0 0.0.0.255
```

Note: The requirements for TT-B state that users on the Guest VLAN should not be able to reach the VLAN 10, 50, and 100 networks. Note that DLS1 and DLS2 do have addresses on other interfaces as well - for VLANs 20 and 200. The solution above does not cover those other two subnets. It should contain similar entries that prevent communication between the 10.1.30.0 subnet and the 10.1.20.0 as well as 10.1.200.0 subnets.

```
ip access-list extended GUEST-ACCESS-CTRL
  permit ip 10.1.30.0 0.0.0.255 10.1.20.0 0.0.0.255
  permit ip 10.1.30.0 0.0.0.255 10.1.200.0 0.0.0.255
```


Section 2 Troubleshooting Reference Information

General Troubleshooting Process

As a general guideline, you can use the following general troubleshooting process described in the course.

1. Define the problem (symptoms).
2. Gather information.
3. Analyze the information.
4. Propose a hypothesis (possible cause).
5. Test the hypothesis.
6. Eliminate or accept the hypothesis.
7. Solve the problem.
8. Document the problem.

Command Summary

The table lists useful commands for this lab. The sample output is shown on following pages.

Command	Key Information Displayed
show ip inspect sessions	Displays established sessions with the source IP address and port number, protocol name, and destination IP address and port number.
show ip inspect config	Displays inspection rule configuration information, including rule name, session parameters, and protocols being inspected.
show ip inspect interfaces	Displays interfaces configured for inspection and inbound/outbound inspection rules, if set, and inbound/outbound access lists, if applied. Also displays protocols being inspected.
show access-lists *ACL#/name*	Displays all ACLs configured on a device, including the ACL number and name, the type of ACL (standard or extended), the statements in each ACL, and the number of matches accumulated for each statement.
show vlan access-map	Displays the name of any configured VLAN access maps, including the match clauses in each. An implied **deny all** match clause is in effect at the end of the access map.
show vlan filter	Displays the name of any configured VLAN access maps and the VLANs for which they are filtering traffic.
show clock	Displays the time and date kept by the device internal clock.
show ntp associations	Displays the configured NTP server IP address, reference clock in use, stratum level, and sync status.
show ntp status	Displays the clock synchronization status, stratum level, and reference clock IP address. Also shows the number of seconds since the last update was received from the reference clock.

Sample Troubleshooting Output

The following commands and outputs are provided as samples from the devices in this lab.

Cisco IOS Stateful Firewall-related Commands

```
R1#show ip inspect sessions
Established Sessions
 Session 657D5B98 (10.1.10.1:8)=>(172.20.0.1:0) icmp SIS_OPEN
 Session 657D5608 (10.1.10.1:1041)=>(172.20.0.1:23) telnet SIS_OPEN
```

In the example above, PC-B (10.1.10.1) has established two sessions to R2 Lo1 through the firewall, one for ping (ICMP) and one for Telnet.

```
R1#show ip inspect config
Session audit trail is disabled
Session alert is enabled
one-minute (sampling period) thresholds are [unlimited : unlimited] connections
max-incomplete sessions thresholds are [unlimited : unlimited]
max-incomplete tcp connections per host is unlimited. Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
tcp reassembly queue length 16; timeout 5 sec; memory-limit 1024 kilo bytes
dns-timeout is 5 sec
Inspection Rule Configuration
 Inspection name FW-inspect
    ftp alert is on audit-trail is off timeout 3600
    http alert is on audit-trail is off timeout 3600
    smtp max-data 20000000 alert is on audit-trail is off timeout 3600
    tftp alert is on audit-trail is off timeout 30
    dns alert is on audit-trail is off timeout 30
    icmp alert is on audit-trail is off timeout 10
    telnet alert is on audit-trail is off timeout 3600
    http alert is on audit-trail is off timeout 3600
    ntp alert is on audit-trail is off timeout 30
```

In the example above, a stateful firewall rule named FW-inspect has been configured that inspects FTP, HTTP, SMTP, TFTP, DNS, ICMP, HTTP, NTP, and Telnet traffic.

```
R1#show ip inspect interfaces
Interface Configuration
 Interface Serial0/0/0
  Inbound inspection rule is not set
  Outgoing inspection rule is FW-inspect
    ftp alert is on audit-trail is off timeout 3600
    http alert is on audit-trail is off timeout 3600
    smtp max-data 20000000 alert is on audit-trail is off timeout 3600
    tftp alert is on audit-trail is off timeout 30
    dns alert is on audit-trail is off timeout 30
    icmp alert is on audit-trail is off timeout 10
    telnet alert is on audit-trail is off timeout 3600
  Inbound access list is FW-ACL
  Outgoing access list is not set
```

In the example above, an outgoing inspection rule named FW-inspect has been configured on S0/0/0, and an access list FW-ACL is applied inbound on S0/0/0.

The example below shows the use of the Cisco IOS help function to display a partial listing of the protocols that can be inspected.

```
R1(config)#ip inspect name FW-inspect ?
  802-11-iapp        IEEE 802.11 WLANs WG IAPP
  ace-svr            ACE Server/Propagation
  appfw              Application Firewall
  appleqtc           Apple QuickTime
  bgp                Border Gateway Protocol
  biff               Bliff mail notification
  bittorrent         bittorrent
  bootpc             Bootstrap Protocol Client
  bootps             Bootstrap Protocol Server
  cddbp              CD Database Protocol
  cifs               CIFS
  cisco-fna          Cisco FNATIVE
  cisco-net-mgmt     cisco-net-mgmt
  cisco-svcs         cisco license/perf/GDP/X.25/ident svcs
  cisco-sys          Cisco SYSMAINT
  cisco-tdp          Cisco TDP
  cisco-tna          Cisco TNATIVE
  citrix             Citrix IMA/ADMIN/RTMP
  citriximaclient    Citrix IMA Client
  clp                Cisco Line Protocol
  creativepartnr     Creative Partnr
  creativeserver     Creative Server
  cuseeme            CUSeeMe Protocol
  daytime            Daytime (RFC 867)
  dbase              dBASE Unix
  dbcontrol_agent    Oracle dbControl Agent po
  ddns-v3            Dynamic DNS Version 3
  dhcp-failover      DHCP Failover
  directconnect      Direct Connect Version 2.0
  discard            Discard port
  dns                Domain Name Server
  dnsix              DNSIX Securit Attribute Token Map
  echo               Echo port
  edonkey            eDonkey
  entrust-svc-hdlr   Entrust KM/Admin Service Handler
  entrust-svcs       Entrust sps/aaas/aams
  esmtp              Extended SMTP
  exec               Remote Process Execution
  fasttrack          FastTrack Traffic - KaZaA, Morpheus, Gro
  fcip-port          FCIP
  finger             Finger
  fragment           IP fragment inspection
  ftp                File Transfer Protocol
  ftps               FTP over TLS/SSL
  gdoi               GDOI
  giop               Oracle GIOP/SSL
  gnutella           Gnutella Version2 Traffic - BearShare, S
  gopher             Gopher
  gtpv0              GPRS Tunneling Protocol Version 0
  gtpv1              GPRS Tunneling Protocol Version 1
  h323               H.323 Protocol (e.g, MS NetMeeting, Intel Video Phone)
  h323-annexe        H.323 Protocol AnnexE (e.g, MS NetMeetin
  h323-nxg           H.323 Protocol AnnexG
  hp-alarm-mgr       HP Performance data alarm manager
```



```
  hp-collector       HP Performance data collector
  hp-managed-node    HP Performance data managed node
  hsrp               Hot Standby Router Protocol
  http               HTTP Protocol
  https              Secure Hypertext Transfer Protocol
  ica                ica (Citrix)
  icabrowser         icabrowser (Citrix)
  icmp               ICMP Protocol
<output omitted>
```

ACL-related Commands

```
R1#show access-lists
Standard IP access list 1
    10 permit 10.1.0.0, wildcard bits 0.0.255.255 (18 matches)

Extended IP access list FW-ACL
    10 deny ip any any (29 matches)
```

In the above example, two ACLs are configured on R1: a standard numbered ACL that identities internal NAT hosts, and an extended named ACL that blocks all traffic for a given direction (inbound or outbound). Statements in both are accumulating matches.

```
R1#show access-lists FW-ACL
Extended IP access list FW-ACL
    10 permit icmp any host 198.133.219.1 (13 matches)
    20 permit tcp any host 198.133.219.1 eq www
    30 permit udp host 192.168.2.1 host 192.168.1.1 eq ntp
    40 deny ip any any log (299 matches)
```

In the above example, a specific named ACL is displayed. Note the log option on the **deny ip any any** statement. The use of this option produces logged message output on the console and syslog server, similar to that shown below. In this example, an NTP packet (port 123) from R2 to R1 is being denied.

```
Dec 19 20:23:29.691: %SEC-6-IPACCESSLOGP: list FW-ACL denied udp 192.168.2.1(123) -
> 192.168.1.1(123), 1 packet
```

Note: The **log** option is normally used when testing or troubleshooting; not for production environments.

VACL-related Commands

```
DLS2#show vlan access-map
Vlan access-map "BLOCK-GUEST"  10
  Match clauses:
    ip  address: GUEST-ACCESS-CTRL
  Action:
    drop
Vlan access-map "BLOCK-GUEST"  20
  Match clauses:
  Action:
    Forward
```

In the above example, access map BLOCK-GUEST has been configured with two match clauses. The first drops all traffic that matches the IP addresses specified in named ACL GUEST-ACCESS-CTRL. The second forwards all traffic that does not match the IP addresses specified in named ACL GUEST-ACCESS-CTRL. An implied **deny all** match clause is in effect at the end of the access map.

```
DLS2#show vlan filter
VLAN Map BLOCK-GUEST is filtering VLANs:
  30
```

In the above example, access map BLOCK-GUEST has been applied to VLAN 30 and is filtering traffic.

NAT-related Commands

```
R1#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 198.133.219.20:512 10.1.10.1:512     172.20.0.1:512     172.20.0.1:512
tcp 198.133.219.20:1043 10.1.10.1:1043    172.20.0.1:23      172.20.0.1:23
tcp 198.133.219.20:1046 10.1.10.1:1046    172.20.0.1:80      172.20.0.1:80
--- 198.133.219.1      10.1.50.1          ---                ---
udp 198.133.219.17:123 10.1.100.1:123     192.168.2.1:123    192.168.2.1:123
udp 198.133.219.18:123 10.1.100.252:123   192.168.2.1:123    192.168.2.1:123
udp 198.133.219.16:123 10.1.100.253:123   192.168.2.1:123    192.168.2.1:123
```

In the above example, PC-B (inside local 10.1.10.1) has initiated a ping (ICMP port 512), a Telnet session (TCP port 23), and a browser (HTTP) session (TCP port 80) to the external R2 Lo1 IP address 172.20.0.1. In addition, several internal devices have initiated NTP requests (UDP port 123) to NTP server R2 (192.168.2.1). Server SRV1 with IP address 10.1.50.1 has a NAT static mapping to public address 198.133.219.1.

NTP-related Commands

```
R2#show clock
*19:19:48.350 UTC Wed Dec 21 2009
```

```
R1#show ntp associations
  address         ref clock       st   when   poll reach  delay  offset   disp
 ~192.168.2.1     .INIT.          16   2258    256     0  0.000   0.000 15937.
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

R1#show ntp associations
  address         ref clock       st   when   poll reach  delay  offset   disp
*~192.168.2.1     127.127.1.1      3      3     64   377  0.000  -0.393  3.038
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```

In the first example above, R1 is configured to contact the NTP server R2 at 192.168.2.1, but the reference clock is in the INIT state, and R1 has not peered with R2. In the second example, R1 has peered with the NTP server R2 at 192.168.2.1, and the reference clock is now R1's internal clock (127.127.1.1).

```
R1#show ntp status
Clock is unsynchronized, stratum 16, no reference clock
nominal freq is 250.0000 Hz, actual freq is 250.0002 Hz, precision is 2**24
reference time is CED4F227.B352D730 (18:08:39.700 UTC Thu Dec 17 2009)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 0.02 msec, peer dispersion is 0.00 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -0.000000961 s/s
system poll interval is 64, last update was 2278 sec ago.

R1#show ntp status
```



```
Clock is synchronized, stratum 4, reference is 192.168.2.1
nominal freq is 250.0000 Hz, actual freq is 250.0002 Hz, precision is 2**24
reference time is CED63F93.9C972B04 (17:51:15.611 UTC Fri Dec 18 2009)
clock offset is -0.0003 msec, root delay is 0.01 msec
root dispersion is 0.00 msec, peer dispersion is 0.00 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -0.000000977 s/s
system poll interval is 64, last update was 20 sec ago.
```

In the first example above, the R1 clock is unsynchronized, and there is no reference clock. The stratum level defaults to 16 (the highest) when no NTP server is reachable. The last update occurred before the firewall was applied and blocked NTP. In the second example, the R1 clock is synchronized, and the reference clock is R2 192.168.2.1. The stratum level is now 4. The last update occurred very recently after the firewall was adjusted to allow NTP.

Reflection Questions

1. Which lab trouble tickets did you have the most difficulty with?

2. Would you change anything about the process that you used for any of the trouble tickets now that you see the resolution of the problem?

3. Which commands did you find most useful in diagnosing data plane security issues? Add these to your toolbox for future use. Which commands did you find least useful?

References

If you need more information on the commands and their options, see the following references:

- **IP Routing Protocol**
  http://www.cisco.com/cisco/web/support/index.html
- **Cisco IOS IP Switching**
  http://www.cisco.com/en/US/docs/ios/ipswitch/command/reference/isw_book.html
- **Configuring Cisco IOS Firewall with NAT**
  http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_configuration_example09186a008009445f.shtml
- **Configuring VLAN ACLs (VACLs)**
  http://www.cisco.com/en/US/docs/routers/7600/ios/12.2SXF/configuration/guide/vacl.html#wp1039754

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1700	Fast Ethernet 0 (FA0)	Fast Ethernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
1800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2600	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)
2800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface.				

Router Interface Summary
The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Device Configurations (instructor version)

Note: All device configurations are provided for TT-A. The configs provided here are *not* running-config outputs. They can be used for cut-and-paste for TT-A and subsequent tickets. Where a config is noted as being the same as a previous one, the only change is in the MOTD, which identifies the Lab and TT. The errors in the configuration are commented and highlighted as red text.

Trouble Ticket - TT-A Configurations

Switch ALS1

```
!Lab 9-3 Switch ALS1 TT-A Config
!
hostname ALS1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 9-3 Switch ALS1 TT-A Config ***$
!
ip dhcp snooping vlan 10
ip dhcp snooping
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
archive
 log config
  logging size 50
```



```
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet

spanning-tree mode rapid-pvst
spanning-tree portfast default
!
interface Vlan1
 no ip address
 shutdown
!
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 100
 name MGMT
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel1
 description Channel to DLS1
 no shutdown
 !
interface Port-channel2
 description Channel to DLS2
 no shutdown
!
interface FastEthernet0/1
 description Channel to DLS1
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 ip dhcp snooping trust
 no shutdown
!
interface FastEthernet0/2
 description Channel to DLS1
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
```



```
 channel-group 1 mode on
 ip dhcp snooping trust
 no shutdown
!
interface FastEthernet0/3
 description Channel to DLS2
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 ip dhcp snooping trust
 no shutdown
!
interface FastEthernet0/4
 description Channel to DLS2
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 ip dhcp snooping trust
 no shutdown
!
interface FastEthernet0/5
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown

interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
```

```
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
```



```
 description To PC-B
 switchport access vlan 10
 switchport mode access
 switchport voice vlan 20
 spanning-tree portfast
 switchport port-security
 switchport port-security maximum 2
 switchport port-security violation shutdown
 switchport port-security mac-address sticky
 no shut
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
```



```
 shutdown
!
interface gigabitethernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan100
 ip address 10.1.100.1 255.255.255.0
 no shutdown
!
ip default-gateway 10.1.100.254
!
ip http server
ip http secure-server
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server host 10.1.50.1 version 2c cisco
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps vlan-membership
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
  no transport input
!
ntp source Vlan100
ntp server 192.168.2.1
end
```

Switch DLS1

```
!Lab 9-3 Switch DLS1 TT-A Config
!
hostname DLS1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
```



```
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55

banner motd $*** Lab 9-3 Switch DLS1 TT-A Config ***$
!
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
!
ip domain name tshoot.net
!
ip dhcp relay information trust-all
!
ip dhcp excluded-address 10.1.10.252 10.1.10.254
ip dhcp excluded-address 10.1.20.252 10.1.20.254
ip dhcp excluded-address 10.1.30.252 10.1.30.254
!
ip dhcp pool OFFICE
   network 10.1.10.0 255.255.255.0
   default-router 10.1.10.254
   domain-name tshoot.net
!
ip dhcp pool VOICE
   network 10.1.20.0 255.255.255.0
   default-router 10.1.20.254
   domain-name tshoot.net
!
ip dhcp pool GUEST
   network 10.1.30.0 255.255.255.0
   default-router 10.1.30.254
   domain-name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
```



```
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 24576
spanning-tree vlan 20,50 priority 28672
!
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 100
 name MGMT
!
vlan 200
 name TRANS
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel1
 description Channel to ALS1
 no shut
!
interface Port-channel10
 description Channel to DLS2
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
```



```
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R1
 no switchport
 ip address 10.1.2.1 255.255.255.252
 spanning-tree bpduguard enable
 speed 100
 duplex full
 no shut
!
interface FastEthernet0/6
 description FE to SRV1
 switchport access vlan 50
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shut
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
```



```
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
```

```
 shutdown
!
interface FastEthernet0/18
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
```



```
interface gigabitethernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 10.1.10.252 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 priority 110
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.252 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.252 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 priority 110
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.252 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 preempt
!
interface Vlan100
 ip address 10.1.100.252 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 priority 110
 standby 100 preempt
!
interface Vlan200
 ip address 10.1.200.252 255.255.255.0
!
router eigrp 1
 passive-interface default
 no passive-interface Fa0/5
 no passive-interface vlan200
 no auto-summary
 network 10.1.0.0 0.0.255.255
!
ip classless
ip http server
ip http secure-server
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
```



```
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server host 10.1.50.1 version 2c cisco
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 192.168.2.1
end
```

Switch DLS2

```
!Lab 9-3 Switch DLS2 TT-A Config
!
hostname DLS2
!
service timestamps debug datetime msec
service timestamps log datetime
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 9-3 Switch DLS2 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
```



```
ip subnet-zero
ip routing
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
  path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 28672
spanning-tree vlan 20,50 priority 24576
!
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 100
 name MGMT
!
vlan 200
 name TRANS
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel2
 description Channel to ALS1
 no shut

interface Port-channel10
 description Channel to DLS1
 no shut
!
```



```
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R3
 no switchport
 ip address 10.1.2.13 255.255.255.252
 speed 100
 duplex full
 spanning-tree bpduguard enable
 no shutdown
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/7
 description Unused
```

```
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
```



```
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description FE to PC-C
 switchport access vlan 30
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
```



```
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 10.1.10.253 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.253 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 priority 110
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.253 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.253 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 priority 110
 standby 50 preempt
!
interface Vlan100
 ip address 10.1.100.253 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 preempt
!
interface Vlan200
 ip address 10.1.200.253 255.255.255.0
!
router eigrp 1
```



```
 passive-interface default
 no passive-interface Fa0/5
 no passive-interface vlan200
 no auto-summary
 network 10.1.0.0 0.0.255.255
!
ip classless
ip http server
ip http secure-server
!
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 192.168.2.1
end
```

Router R1

```
!Lab 9-3 Router R1 TT-A Config
!
hostname R1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
```



```
!
banner motd $*** Lab 9-3 Router R1 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
ip inspect name FW-inspect ftp
ip inspect name FW-inspect smtp
ip inspect name FW-inspect tftp
ip inspect name FW-inspect dns
ip inspect name FW-inspect icmp
ip inspect name FW-inspect telnet
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 192.168.1.1 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown
!
interface FastEthernet0/1
 description FE to DLS1
 ip address 10.1.2.2 255.255.255.252
 ip flow ingress
 ip nat inside
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
 description WAN link to ISP R2
 ip address 209.165.200.225 255.255.255.252
 ip access-group FW-ACL in
 ip nat outside
 ip inspect FW-inspect out
 ip flow ingress
 encapsulation ppp
 clock rate 128000
```

Error: HTTP and NTP are missing from the protocols to inspect.

```
ip inspect name FW-inspect http
ip inspect name FW-inspect ntp
```



```
  no shutdown
!
interface Serial0/0/1
 shutdown
!
router eigrp 1
 redistribute static
 passive-interface default
 no passive-interface FastEthernet0/1
 network 10.1.2.0 0.0.0.3
 network 192.168.1.1 0.0.0.0
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 209.165.200.226
!
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
ip nat pool public-addrs 198.133.219.10 198.133.219.30 netmask 255.255.255.224
ip nat inside source list 1 pool public-addrs
ip nat inside source static 10.1.50.1 198.133.219.1
!
ip access-list extended FW-ACL
 deny ip any any
!
logging source-interface Loopback0
logging 10.1.50.1
!
access-list 1 permit 10.1.0.0 0.0.255.255
!
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 192.168.2.1
end
```

Error: FW-ACL Permit statements are missing. (These are added by sequence number. The existing deny ip any any statement is seq #10):

* Allow external access to internal SRV1 via ping and HTTP.

```
ip access-list extended FW-ACL
 3 permit tcp any host 198.133.219.1 eq www
 5 permit icmp any host 198.133.219.1
```

* Allow NTP responses from R2 to R1.

```
 7 permit udp host 192.168.2.1 host 192.168.1.1 eq ntp
```


Router R2

```
!Lab 9-3 Router R2 TT-A Config
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
Hostname R2
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 9-3 Router R2 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 192.168.2.1 255.255.255.255
!
interface Loopback1
 ip address 172.20.0.1 255.255.255.248
!
interface FastEthernet0/0
 shutdown
!
interface FastEthernet0/1
 shutdown
!
interface Serial0/0/0
 description WAN link to R1 – T1 leased line
 ip address 209.165.200.226 255.255.255.252
```



```
 encapsulation ppp
 no shutdown

!
interface Serial0/0/1
 shutdown
!
ip route 192.168.1.1 255.255.255.255 209.165.200.225
ip route 198.133.219.0 255.255.255.224 209.165.200.225
!
ip http server
no ip http secure-server
!
logging source-interface Loopback0
logging 10.1.50.1
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 logging synchronous
 login authentication CONSOLE
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
!
ntp master 3
 end
```

Router R3

```
!Lab 9-3 Router R3 TT-A Config
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 9-3 Router R3 TT-A Config ***$
!
aaa new-model
aaa authentication login default local
```

```
aaa authentication login CONSOLE none
aaa authorization exec default local
!
no ip domain lookup
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 10.1.203.1 255.255.255.255
!
interface FastEthernet0/0
 description FE to R3 LAN
 ip address 10.1.80.1 255.255.255.0
 ip flow ingress
 speed 100
 full-duplex
 no shutdown
!
interface FastEthernet0/1
 description FE to DLS2
 ip address 10.1.2.14 255.255.255.252
 ip flow ingress
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
description WAN link to R1 – not used for this lab
 no ip address
 clock rate 128000
 encapsulation ppp
 shutdown
!
interface Serial0/0/1
 shutdown
!
router eigrp 1
 passive-interface default
 no passive-interface FastEthernet0/1
 network 10.1.2.12 0.0.0.3
 network 10.1.80.0 0.0.0.255
 network 10.1.203.1 0.0.0.0
 no auto-summary
!
```



```
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
logging source-interface Loopback0
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 logging synchronous
 login authentication CONSOLE
line vty 0 4
 exec-timeout 60 0
transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 192.168.2.1
end
```

Trouble Ticket - TT-B Configurations

Router R2—Same as TT-A

Router R3—Same as TT-A

Switch ALS1—Same as TT-A

Switch DLS1—Same as TT-A

Switch DLS2

```
!Lab 9-3 Switch DLS2 TT-B Config
!
hostname DLS2
!
service timestamps debug datetime msec
service timestamps log datetime
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
```

```
username admin secret adminpa55
!
banner motd $*** Lab 9-3 Switch DLS2 TT-B Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
  path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 28672
spanning-tree vlan 20,50 priority 24576
!
vlan access-map BLOCK-GUEST 10
 action drop
 match ip address GUEST-ACCESS-CTRL
!
vlan filter BLOCK-GUEST vlan-list 30
!
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 100
```

Error: Access map block-guest is missing a statement that forwards traffic that is not matched in the GUEST-ACCESS-CTRL ACL. Otherwise the implicit action drop statement is applied and denies all other traffic, including traffic destined for the Internet. Add statement 20.

```
vlan access-map BLOCK-GUEST 20
  action forward
```



```
 name MGMT
!
vlan 200
 name TRANS
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel2
 description Channel to ALS1
 no shut

interface Port-channel10
 description Channel to DLS1
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
```

```
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R3
 no switchport
 ip address 10.1.2.13 255.255.255.252
 speed 100
 duplex full
 spanning-tree bpduguard enable
 no shutdown
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
```



```
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description FE to PC-C
 switchport access vlan 30
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
```

```
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 10.1.10.253 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.253 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 priority 110
```

```
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.253 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.253 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 priority 110
 standby 50 preempt
!
interface Vlan100
 ip address 10.1.100.253 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 preempt
!
interface Vlan200
 ip address 10.1.200.253 255.255.255.0
!
router eigrp 1
 passive-interface default
 no passive-interface Fa0/5
 no passive-interface vlan200
 no auto-summary
 network 10.1.0.0 0.0.255.255
!
ip classless
ip http server
ip http secure-server
!
ip access-list extended GUEST-ACCESS-CTRL
 permit ip 10.1.30.0 0.0.0.255 10.1.10.0 0.0.0.255
 permit ip 10.1.30.0 0.0.0.255 10.1.50.0 0.0.0.255
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 logging synchronous
 login authentication CONSOLE
```

Error: The access list is missing a statement that permits (selects for blockage) traffic from Guest VLAN 30 that is destined for management VLAN 100. Add statement 30 to the end of the ACL.

```
ip access-list extended GUEST-ACCESS-CTRL
 permit ip 10.1.30.0 0.0.0.255 10.1.100.0 0.0.0.255
```



```
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 192.168.2.1
end
```

Router R1

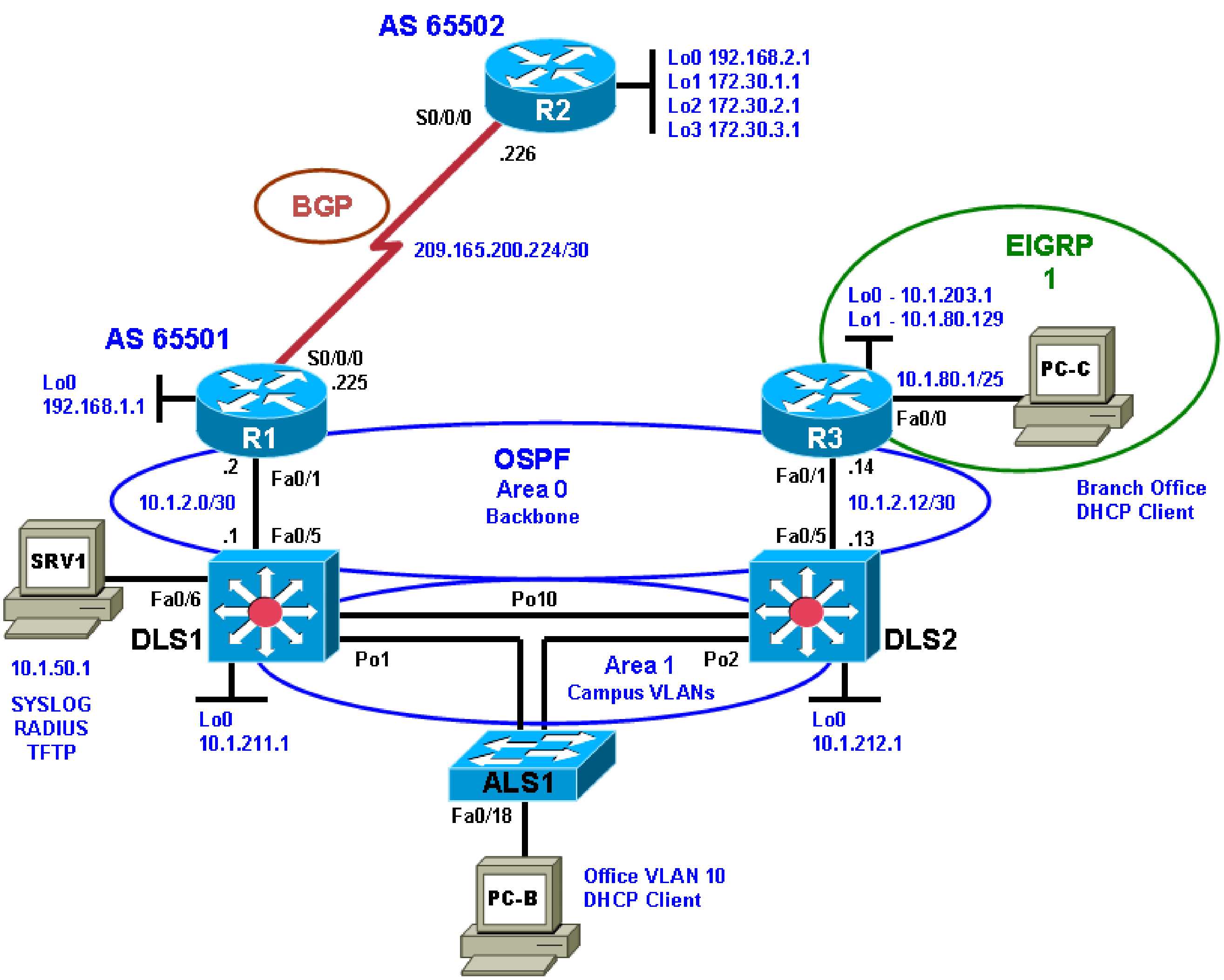
```
!Lab 9-3 Router R1 TT-B Config
!
hostname R1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 9-3 Router R1 TT-B Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
ip inspect name FW-inspect ftp
ip inspect name FW-inspect http
ip inspect name FW-inspect ntp
ip inspect name FW-inspect smtp
ip inspect name FW-inspect tftp
ip inspect name FW-inspect dns
ip inspect name FW-inspect icmp
ip inspect name FW-inspect telnet
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
```

```
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 192.168.1.1 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown
!
interface FastEthernet0/1
 description FE to DLS1
 ip address 10.1.2.2 255.255.255.252
 ip flow ingress
 ip nat inside
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
 description WAN link to ISP R2
 ip address 209.165.200.225 255.255.255.252
 ip access-group FW-ACL in
 ip nat outside
 ip inspect FW-inspect out
 ip flow ingress
 encapsulation ppp
 clock rate 128000
  no shutdown
!
interface Serial0/0/1
 shutdown
!
router eigrp 1
 redistribute static
 passive-interface default
 no passive-interface FastEthernet0/1
 network 10.1.2.0 0.0.0.3
 network 192.168.1.1 0.0.0.0
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 209.165.200.226
!
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
ip nat pool public-addrs 198.133.219.10 198.133.219.30 netmask 255.255.255.224
ip nat inside source list 1 pool public-addrs
ip nat inside source static 10.1.50.1 198.133.219.1
!
ip access-list extended FW-ACL
 permit tcp any host 198.133.219.1 eq www
 permit icmp any host 198.133.219.1
 permit udp host 192.168.2.1 host  192.168.1.1 eq ntp
```

```
 deny ip any any
!
logging source-interface Loopback0
logging 10.1.50.1
!
access-list 1 permit 10.1.0.0 0.0.255.255
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 192.168.2.1
end
```


Chapter 10 Lab 10-1, Troubleshooting Complex Environments Instructor Version

Lab Topology



Objectives

- Load the device configuration files for each trouble ticket.
- Diagnose and resolve problems related to features, protocols, or technology that could be encountered in a complex, integrated enterprise network.
- Document the troubleshooting progress, configuration changes, and problem resolution.

Background

This lab covers a range of problems and requires that you make use of the troubleshooting skills acquired throughout this course to resolve the routing and switching problems introduced. These trouble tickets are based on scenarios from previous labs. This lab focuses on routing and switching connectivity issues related to EtherChannel, STP, OSPF, EIGRP, and ACLs.

For each task or trouble ticket, the trouble scenario and problem symptom are described. While troubleshooting, you will discover the cause of the problem, correct it, and then document the process and results.

Trouble Tickets and Troubleshooting Logs

This lab includes four tasks. Each task is associated with a trouble ticket (TT) and introduces one or more errors on one or more devices. If time is a consideration, each task or trouble ticket can be performed independently.

Instructor note: Some suggested commands are provided for each trouble ticket but not a step-by-step solution and validation procedure as with previous labs. Solutions and discussions are included in the debrief for each TT. Students are expected to use the commands and troubleshooting procedures introduced in previous labs to diagnose the problems in this lab.

Troubleshooting Reference Information

A generic troubleshooting flow is provided for analysis. Suggested commands are provided for each trouble ticket. Refer to previous labs for specific troubleshooting flows, examples of additional commands and command output.

Note: This lab uses Cisco 1841 routers with Cisco IOS Release 12.4(24)T1 and the Advanced IP Services image c1841-advipservicesk9-mz.124-24.T1.bin. The switches are Cisco WS-C2960-24TT-L with the Cisco IOS image c2960-lanbasek9-mz.122-46.SE.bin and Catalyst 3560-24PS with the Cisco IOS image c3560-advipservicesk9-mz.122-46.SE.bin. Other routers (such as 2801 and 2811), switches (such as 2950 or 3550), and Cisco IOS Software versions can be used if they have comparable capabilities and features. Depending on the router or switch model and Cisco IOS Software version, the commands available and output produced might vary from what is shown in this lab.

Instructor Notes

- The lab topology should be pre-built prior to the students starting the lab. Ensure that all routers and switches (R1, R2, R3, ALS1, DLS1, and DLS2) have the course lab configuration files installed in flash. You can download the files from the Academy Connection website.
- The device configurations that contain trouble ticket errors and modifications from the baseline are included at the end of the lab, and the errors in them are identified.
- Each device should have a directory named “tshoot” in flash. This directory contains the baseline configuration file for that device as well as the configuration files for the labs in this course. Refer to Lab 3-1 for instructions on creating the tshoot directory in flash.
- Instructors can use a TFTP server, USB drive, flash memory card, or other method to copy all the course configuration files into the flash:/tshoot directory for each device in the topology.
- The student is responsible for loading the baseline or trouble ticket configurations as required using the procedure described in Lab 3-1.
- Set the correct time on router R2, which serves as the primary NTP server for the lab network.
- If time is an issue, each task (trouble ticket) can be performed independently.
- Students can work individually or as a team.

Required Resources

- 3 routers (Cisco 1841 with Cisco IOS Release 12.4(24)T1 Advanced IP Service or comparable)
- 1 switch (Cisco 2960 with the Cisco IOS Release 12.2(46)SE C2960-LANBASEK9-M image or comparable)
- 2 switches (Cisco 3560 with the Cisco IOS Release 12.2(46)SE C3560-advipservicesk9-mz image or comparable)
- SRV1 (Windows PC with 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

Instructor Notes

- This lab is divided into multiple tasks. Each task is associated with a trouble ticket (TT) and introduces one or more errors on one or more devices.
- Students can work individually or as a team.
- Suggested actions and results presented during the troubleshooting process for each TT can be shared with the students during debrief, or copies of the instructor version of the lab can be made available to the students to assist them in verifying their work.

Section 1—Trouble Tickets and Troubleshooting Logs

Task 1: Trouble Ticket Lab 10-1 TT-A

Instructor note: This trouble ticket involves ALS1 and DLS1 issues related to port channels and physical port VLAN issues.

Step 1: Review trouble ticket Lab 10-1 TT-A.

One of your colleagues mentioned that he had established a Telnet connection to switch ALS1 from PC-B and tested connectivity to server SRV1 via ping but was not successful. All switches in the network have a management address assigned, so he should be able to ping any device in the network. He asked for your help in determining the cause and resolving the issue.

Step 2: Load the device trouble ticket configuration files for TT-A.

Using the procedure described in Lab 3-1, verify that the lab configuration files are present in flash. Load the proper configuration files as indicated in the Device Configuration File table.

Note: The following device access methods are in effect after loading the configuration files:

- Console access requires no username or password.
- Telnet and SSH require username **admin** and password **adminpa55**.
- The enable password is **ciscoenpa55**.

Instructor note: Although it is not considered security best practice, the enable secret and admin user passwords can be changed to something simpler to facilitate performance of this lab.

Device Configuration File Table

Device Name	File to Load	Notes
ALS1	Lab101-ALS1-TT-A-Cfg.txt	This file contains configuration errors
DLS1	Lab101-DLS1-TT-A-Cfg.txt	This file contains configuration errors
DLS2	Lab101-DLS2-TT-A-Cfg.txt	This file contains configurations different than the baseline
R1	Lab101-R1-TT-A-Cfg.txt	This file contains configurations different than the baseline
R2	Lab101-R2-TT-A-Cfg.txt	This file contains configurations different than the baseline
R3	Lab101-R3-TT-A-Cfg.txt	This file contains configurations different than the baseline
SRV1	N/A	Static IP: 10.1.50.1 Default gateway: 10.1.50.254
PC-B	N/A	DHCP
PC-C	N/A	DHCP

Instructor note: The student loads the "broken" TT configuration files for all devices, even though only the configurations indicated in the Notes column contain errors.

Step 3: Configure SRV1 and start the syslog and TFTP servers.

a. Configure SRV1 with the static IP address 10.1.50.1/24 and default gateway 10.1.50.254.

b. Start the syslog server on SRV1 to monitor console messages from multiple devices.

c. Start the TFTP server on SRV1 to record device configuration changes.

Step 4: Release and renew the DHCP lease on PC-B and PC-C.

a. Ensure that PC-B is configured as a DHCP client in the OFFICE VLAN.

b. Ensure that PC-C is configured as a DHCP client in the R3 branch office LAN.

c. After loading all TT-A device configuration files, issue the **`ipconfig /release`** and **`ipconfig /renew`** commands on PC-B and PC-C.

Step 5: Outline the troubleshooting approach and validation steps.

Use this space to identify your troubleshooting approach and the key steps to verify that the problem is resolved. Troubleshooting approaches to select from include the follow-the-path, spot-the-differences, bottom-up, top-down, divide-and-conquer, shoot-from-the-hip, and move-the-problem methods.

Note: In addition to a specific approach, you can use the generic troubleshooting process described at the beginning of Section 2 of this lab.

____

____

____

____

____

____

The follow-the-path or shoot-from-the-hip method can be used. Other problem-solving methods are the top-down, bottom-up, follow-the-path, spot-the-differences, divide-and-conquer and move-the-problem approaches.

Verification steps can include:

- Switch ALS1 can ping SRV1.
- Switch ALS1 can ping DLS1.

Step 6: Record the troubleshooting process and configuration changes.

Use this log to document your actions and results during the troubleshooting process. List the commands you used to gather information. As you progress, record what you think the problem might be and the actions you take to correct the problem.

Note: Refer to the table of commands following this log, which might be helpful in troubleshooting this problem. You can also refer to Lab 4-1 for sample troubleshooting flows and additional commands.

Device	Actions and Results

Device	Actions and Results

Command	Key Information Displayed
show interfaces status	Displays link status, speed, duplex, trunk or VLAN membership, and interface descriptions.
show cdp neighbors [**detail**]	Displays detailed information about a neighbor (or neighbors) including network address, enabled protocols, hold time, and software version.
show spanning-tree vlan *vlan#*	Displays all essential parameters that affect the topology, such as root port, designated ports, port state, and port type, as well as the spanning-tree mode implemented.
show spanning-tree summary	Displays the spanning-tree mode and the VLANs for which this switch is the root bridge. VLANs are listed along with the number of ports in various STP states.
show vlan brief	Displays an 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 which trunk ports that the VLAN is allowed on.
show interfaces trunk	Displays all trunk ports, the operational status, trunk encapsulation, and native VLAN, as well as the list of allowed VLANs, active VLANs, and the VLANs in Spanning Tree Forwarding state for the trunk.
show interfaces *type/#*	Checks all VLAN-related parameters for a specific interface

`switchport`	(access ports and trunk ports).
`show etherchannel summary`	Displays port channels, member ports, and flags indicating status.

Step 7: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with the instructor. The notes can include problems encountered, solutions applied, useful commands employed, alternate solutions, methods, and processes, and procedure and communication improvements.

___

___

___

___

___

___

___

Trouble Ticket TT-A Debrief—Instructor Notes

The connectivity problem between switch ALS1 and server SRV1 was caused by two issues.

TT-A Issue 1

There is a mismatch in configuration between interface Po1 and interfaces Fast Ethernet 0/1 and 0/2 on switch ALS1. On interface Po1, the VLAN list configured allows VLAN 30 (the GUEST VLAN). Physical interfaces Fa0/1 and Fa0/2 do not allow VLAN 30. This causes the physical interfaces to be suspended, and the port channel interface to go down. To correct this problem, issue the following commands on switch ALS1:

```
interface range FastEthernet 0/1 – 2
  switchport trunk allowed vlan add 30
```

Note: This brings up interface Po1 on ALS1 and allows ALS1 to ping SRV1, but it does not address the issue of why ALS1 could not ping SRV1 via the backup link interface Po2.

Instead of adding these commands to interfaces Fast Ethernet 0/1 and 0/2, connectivity between ALS1 and server SRV1 can also be restored by removing the allowed VLAN list from interface Po1. However, this is not an acceptable solution because it is not in compliance with the established policies on the network, based on the fact that allowed VLAN lists are configured on all other trunks between the switches.

TT-A Issue 2

When ALS1 Po1 and physical ports Fa0/1 and Fa0/2 were shut down because of the VLAN mismatch, ALS1 should have been able to ping SRV1 through the STP backup link Po2 to DLS2 and then from DLS2 to DLS1 though Po10. However, the DLS1 Po10 trunk interface does not allow VLAN 100, which is the source of the ping (the switch ALS1 management address is 10.1.100.1).

To correct this problem, issue the following commands on switch DLS1:

```
interface Port-channel 10
  switchport trunk allowed vlan add 100
```

Note: This automatically adds VLAN 100 to the member interfaces Fa0/3 and Fa0/4.

Task 2: Trouble Ticket Lab 10-1 TT-B

Instructor note: This trouble ticket involves devices R1 and R2 and issues related to the OSPF and BGP default route redistribution and missing static routes.

Step 1: Review trouble ticket Lab 10-1 TT-B.

Many users on the network are experiencing problems when accessing the Internet. An office user who uses client PC-B reports that he cannot browse to a website at IP address 172.30.3.1 (simulated by R2 Lo3).

Your task is to restore connectivity from client PC-B to the Internet and ensure that the user can connect to 172.30.3.1 using ping or a web browser.

Step 2: Load the device trouble ticket configuration files for TT-B.

Using the procedure described in Lab 3-1, verify that the lab configuration files are present in flash. Load the proper configuration files as indicated in the Device Configuration File table.

Note: The following device access methods are in effect after loading the configuration files:

- Console access requires no username or password.
- Telnet and SSH require username **admin** and password **adminpa55**.
- The enable password is **ciscoenpa55**.

Instructor note: Although it is not considered security best practice, the enable secret and admin user passwords can be changed to something simpler to facilitate performance of this lab.

Device Configuration File Table

Device Name	File to Load	Notes
ALS1	Lab101-ALS1-TT-B-Cfg.txt	This file contains configurations different than the baseline
DLS1	Lab101-DLS1-TT-B-Cfg.txt	This file contains configurations different than the baseline
DLS2	Lab101-DLS2-TT-B-Cfg.txt	This file contains configurations different than the baseline
R1	Lab101-R1-TT-B-Cfg.txt	This file contains configuration errors
R2	Lab101-R2-TT-B-Cfg.txt	This file contains configuration errors
R3	Lab101-R3-TT-B-Cfg.txt	This file contains configurations different than the baseline
SRV1	N/A	Static IP: 10.1.50.1 Default gateway: 10.1.50.254
PC-B	N/A	DHCP
PC-C	N/A	DHCP

Instructor note: The student loads the “broken” TT configuration files for all devices, even though only the configurations indicated in the Notes column contain errors.

Step 3: Configure SRV1 and start the syslog and TFTP servers.

a. Configure SRV1 with the static IP address 10.1.50.1/24 and default gateway 10.1.50.254.

b. Start the syslog server on SRV1 to monitor console messages from multiple devices.

c. Start the TFTP server on SRV1 to record device configuration changes.

Step 4: Release and renew the DHCP lease on PC-B and PC-C.

a. Ensure that PC-B is configured as a DHCP client in the OFFICE VLAN.

b. Ensure that PC-C is configured as a DHCP client in the R3 branch office LAN.

c. After loading all TT-B device configuration files, issue the **`ipconfig /release`** and **`ipconfig /renew`** commands on PC-B and PC-C.

Step 5: Outline the troubleshooting approach and validation steps.

Use this space to identify your troubleshooting approach and the key steps to verify that the problem is resolved. Troubleshooting approaches to select from include the follow-the-path, spot-the-differences, bottom-up, top-down, divide-and-conquer, shoot-from-the-hip, and move-the-problem methods.

Note: In addition to a specific approach, you can use the generic troubleshooting process described at the beginning of Section 2 of this lab.

The follow-the-path or shoot-from-the-hip method can be used. Other problem-solving methods are the top-down, bottom-up, follow-the-path, spot-the-differences, divide-and-conquer and move-the-problem approaches.

Verification steps can include:

- PC-B can ping the Internet (R2 Lo1, Lo2 or Lo3).
- PC-B can browse to R2 Lo3 (172.30.3.1).
- All other devices in the internal OSPF and EIGRP networks can ping the Internet (R2 Lo1, Lo2, or Lo3).

Step 6: Record the troubleshooting process and configuration changes.

Use this log to document your actions and results during the troubleshooting process. List the commands you used to gather information. As you progress, record what you think the problem might be and the actions you take to correct the problem.

Note: In addition to the commands listed for TT-A, the table of commands following this log might be helpful in troubleshooting this problem. You can also refer to Labs 5-2 and 5-3 for sample troubleshooting flows and additional commands.

Device	Actions and Results

Device	Actions and Results

Command	Key Information Displayed
show ip route or **show ip route** *ip-addr*	Displays the entire routing table or information for a particular destination address.
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 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. 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	Displays parameters and extensive statistics about the peering session for all BGP neighbors.
show ip ospf database	Verifies the link types and link IDs for all areas in which this device participates.

Step 7: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with the instructor. The notes can include problems encountered, solutions applied, useful commands employed, alternate solutions, methods, and processes, and procedure and communication improvements.

____

____

____

____

____

____

____

Trouble Ticket TT-B Debrief—Instructor Notes

PC-B is unable to access the Internet (simulated by R2 Lo1, Lo2, and Lo3) because of two separate issues.

TT-B Issue 1

Router R1 is not redistributing the default route learned via BGP to other OSPF neighbors. As a result, DLS1 does not have a default route by which it can reach R2. To correct this problem, issue the following commands on router R1:

```
router ospf 1
 default-information originate
```

TT-B Issue 2

Correcting Issue 1 provides a default route to DLS1, but PC-B pings to R2 Lo3 are still not successful. The pings, sourced from the 10.1.0.0/16 network, are reaching R2, but R2 does not have a return route by which to reply. A static default route (0.0.0.0) or static to the 10.1.0.0 network is needed on R2 pointing to R1.

To correct this problem, issue the following command on router R2:

```
ip route 10.1.0.0 255.255.0.0 209.165.200.225
```

Task 3: Trouble Ticket Lab 10-1 TT-C

Instructor note: This trouble ticket involves devices DLS1, DLS2 and R3 issues related to OSPF neighbor relationships, as well as EIGRP route advertisement issues.

Step 1: Review trouble ticket Lab 10-1 TT-C.

The user of PC-C on the branch office network called the help desk and reported that she is unable to access SRV1 or the Internet. Your task is to restore connectivity from client PC-C to SRV1 and the Internet and ensure that the user can connect to 172.30.3.1 using ping or a web browser. The branch office administrator did some preliminary testing and reported that he cannot ping or use Telnet to DLS2 or any other network devices from R3. The capability to ping other devices from remote router R3 is a connectivity requirement for the network.

Step 2: Load the device trouble ticket configuration files for TT-C.

Using the procedure described in Lab 3-1, verify that the lab configuration files are present in flash. Load the proper configuration files as indicated in the Device Configuration File table.

Note: The following device access methods are in effect after loading the configuration files:

- Console access requires no username or password.
- Telnet and SSH require username **admin** and password **adminpa55**.
- The enable password is **ciscoenpa55**.

Instructor note: Although it is not considered security best practice, the enable secret and admin user passwords can be changed to something simpler to facilitate performance of this lab.

Device Configuration File Table

Device Name	File to Load	Notes
ALS1	Lab101-ALS1-TT-C-Cfg.txt	This file contains configurations different than the baseline
DLS1	Lab101-DLS1-TT-C-Cfg.txt	This file contains configurations different than the baseline
DLS2	Lab101-DLS2-TT-C-Cfg.txt	This file contains configuration errors
R1	Lab101-R1-TT-C-Cfg.txt	This file contains configurations different than the baseline
R2	Lab101-R2-TT-C-Cfg.txt	This file contains configurations different than the baseline
R3	Lab101-R3-TT-C-Cfg.txt	This file contains configuration errors
SRV1	N/A	Static IP: 10.1.50.1 Default gateway: 10.1.50.254
PC-B	N/A	DHCP
PC-C	N/A	DHCP

Instructor note: The student loads the “broken” TT configuration files for all devices, even though only the configurations indicated in the Notes column contain errors.

Step 3: Configure SRV1 and start the syslog and TFTP servers.

a. Configure SRV1 with the static IP address 10.1.50.1/24 and default gateway 10.1.50.254.

b. Start the syslog server on SRV1 to monitor console messages from multiple devices.

c. Start the TFTP server on SRV1 to record device configuration changes.

Step 4: Release and renew the DHCP lease on PC-B and PC-C.

a. Ensure that PC-B is configured as a DHCP client in the OFFICE VLAN.

b. Ensure that PC-C is configured as a DHCP client in the R3 branch office LAN.

c. After loading all TT-C device configuration files, issue the **`ipconfig /release`** and **`ipconfig /renew`** commands on PC-B and PC-C.

Step 5: Outline the troubleshooting approach and validation steps.

Use this space to identify your troubleshooting approach and the key steps to verify that the problem is resolved. Troubleshooting approaches to select from include follow-the-path, spot-the-differences, bottom-up, top-down, divide-and-conquer, shoot-from-the-hip, and move-the-problem methods.

Note: In addition to a specific approach, you can use the generic troubleshooting process described at the beginning of Section 2 of this lab.

____

____

____

____

____

____

The follow-the-path or spot-the-differences method can be used. Other problem-solving methods are the top-down, bottom-up, follow-the-path, shoot-from-the-hip, divide-and-conquer and move-the-problem approaches.

Verification steps can include:

- DLS1, DLS2, and R3 become OSPF neighbors and are able to exchange routes.
- PC-C can ping the Internet (R2 Lo1, Lo2, or Lo3).
- PC-C can ping SRV1 (10.1.50.1).
- R3 can ping and use traceroute to internal devices.
- R3 can establish Telnet and SSH connections to internal devices.
- R3 can access internal devices via syslog, SNMP, and NTP.

Step 6: Record the troubleshooting process and configuration changes.

Use this log to document your actions and results during the troubleshooting process. List the commands that you used to gather information. As you progress, record what you think the problem might be and the actions you take to correct the problem.

Note: In addition to the commands listed for TT-A and TT-B, the table of commands following this log might help you troubleshoot this problem. You can also refer to Lab 5-1 and the Chapter 9 labs for sample troubleshooting flows and additional commands.

Device	Actions and Results

Device	Actions and Results

Command	Key Information Displayed
show ip cef *ip-addr* **detail**	Displays the next hop and interface used for a particular destination address from the CEF table.
show standby brief	Verifies 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 access-lists *ACL#/name*	Displays all ACLs configured on a device, including the ACL number and name, the type (standard or extended), the statements, and the number of matches accumulated for each statement.
show ntp status	Displays the clock synchronization status, stratum level, and reference clock IP address. Also shows the number of seconds since the last update was received from the reference clock.

Step 7: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with the instructor. The notes can include problems encountered, solutions applied, useful commands employed, alternate solutions, methods, and processes, and procedure and communication improvements.

____

____

____

____

____

____

____

Trouble Ticket TT-C Debrief—Instructor Notes

PC-C is unable to access the Internet or SRV1 because of three separate issues.

TT-C Issue 1

The first problem is the duplicate OSPF router ID between Layer 3 switches DLS1 and DLS2. This causes DLS1 and DLS2 not to form an OSPF neighbor relationship, and no routes can be exchanged. The R3 networks are not known to DLS1, and the R1 and R2 (ISP) networks are not known to DLS2. In addition, DLS1 does not receive a default route.

This problem can be resolved by changing the OSPF router ID on DLS2 to the IP address that is configured on its loopback. This is accomplished by issuing the following commands on switch DLS2:

```
router ospf 1
 router-id 10.1.212.1

clear ip ospf process
```

Note: For the changes to take effect, you must also issue the **`clear ip ospf process`** command or reload the device. This enables DLS1 and DLS2 to form an OSPF neighbor relationship. However, other problems are preventing successful pings from PC-C.

The best choice for the router ID on DLS2 is the IP address of its loopback 0 interface 10.1.212.1. Choosing any other unique router ID or changing the router ID on router DLS1 to a unique value will also restore connectivity and is technically a correct solution. However, because all other routers use the IP address of their loopback 0 interface as their OSPF router ID, this is not considered a best practice.

TT-C Issue 2

The second problem is that R3 does not advertise the correct route to the R3 Fa0/0 LAN subnet under EIGRP. This prevents pings from PC-C to other areas from returning because the correct network to PC-C is not known by the other routers.

This problem can be resolved by removing the incorrect route and adding the correct route to the 10.1.80.0/25 network under EIGRP. This is accomplished by issuing the following commands on router R3:

```
router eigrp 1
  no network 10.1.81.0 0.0.0.127
  network 10.1.80.0 0.0.0.127
```

TT-C Issue 3

The third problem is an extended access list on DLS2 interface Fa0/5 that causes problems with management and control plane traffic. This access list was added to allow only traffic from the 10.1.80.0/24 network (Lo1 and Fa0/0 LANs) into the core network. However, the implicit “deny ip any any” at the end of the ACL also blocks R3 OSPF traffic to DLS2. The R3 OSPF address on the interface Fa0/1 is 10.1.2.14 and hellos from this address are not permitted by the ACL on DLS2 Fa0/5. This causes DLS2 and R3 not to form an OSPF neighbor relationship, and no routes can be exchanged. The R3 networks are not known to DLS1 and DLS2. The R1 and R2 (ISP) networks are not known to R3. In addition, R3 does not receive a default route.

This problem can be resolved by adding an OSPF protocol permit statement to the ACL on DLS2 using the following command on switch DLS2. The statement is added to the end of the ACL and permits OSPF traffic from any interface on R3.

```
access-list 101 permit ospf any any
```

Another issue is that network connectivity testing (ping and traceroute) as well as management (Telnet) and control plane (NTP) traffic are accidently blocked. After adding the above statement, access list 101 allows traffic from the R3 10.1.80.0/24 network to reach any other location in the internal network. It also permits OSPF traffic. However, the ACL does not permit R3 to ping DLS2 (or other internal network devices) using the default R3 IP source address 10.1.2.14 of interface Fa0/1. Additionally, no other device on the internal network can ping R3 unless they ping the R3 F0/0 or Lo0/1 interface IP address (so that ping replies have a source address on the 10.1.80.0/24 network). To correct this problem, add a statement to access list 101 permitting traffic from 10.1.2.14 (R3 Fa0/1):

```
access-list 101 permit ip 10.1.2.14 0.0.0.0 any
```

Note: If an extended ping is used on R3 to ping DLS2 Fa0/5 (10.1.2.13), and R3 F0/0 (address 10.1.80.1) is specified as the source interface, the ping will succeed.

```
R3#ping 10.1.2.13 source fa0/0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.2.13, timeout is 2 seconds:
Packet sent with a source address of 10.1.80.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

In addition, the ACL on DLS2 does not allow Telnet, SSH, syslog, NTP, or SNMP traffic from R3 to reach the necessary internal network devices via DLS2. All these protocols are sourced by R3 Lo0 (10.1.203.1). To correct this problem, add a statement to access list 101 permitting traffic from 10.1.203.1 (R3 Lo0).

```
access-list 101 permit ip 10.1.203.1 0.0.0.0 any
```

Note: If an extended Telnet is used on R3 to DLS2 Fa0/5 (10.1.2.13), and R3 F0/0 (address 10.1.80.1) is specified as the source interface, Telnet will succeed.

```
R3#telnet 10.1.2.13 /source-interface fa0/0
Trying 10.1.2.13 ... Open
*** Lab 10-1 Switch DLS2 TT-C Config ***
User Access Verification
Username:
```


Task 4: Trouble Ticket Lab 10-1 TT-D

Instructor note: This trouble ticket involves device R3 issues related to the router boot process and config register settings.

Step 1: Review trouble ticket Lab 10-1 TT-D.

The user of PC-C on the branch office network called the help desk again and reported that she is unable to access SRV1 or the Internet and she is pretty upset. You must restore access to these resources for this user.

Step 2: Load the device trouble ticket configuration files for TT-D.

Using the procedure described in Lab 3-1, verify that the lab configuration files are present in flash. Load the proper configuration files as indicated in the Device Configuration File table.

Note: The following device access methods are in effect after loading the configuration files:

- Console access requires no username or password.
- Telnet and SSH require username **admin** and password **adminpa55**.
- The enable password is **ciscoenpa55**.

Instructor note: Although it is not considered security best practice, the enable secret and admin user passwords can be changed to something simpler to facilitate performance of this lab.

Step 3: Restart router R3 after the TT-D file is loaded.

After loading the TT-D file into the running config for router R3 and then copying it to the startup config, use the `reload` command to restart the router.

Device Configuration File Table

Device Name	File to Load	Notes
ALS1	Lab101-ALS1-TT-D-Cfg.txt	This file contains configurations different than the baseline
DLS1	Lab101-DLS1-TT-D-Cfg.txt	This file contains configurations different than the baseline
DLS2	Lab101-DLS2-TT-D-Cfg.txt	This file contains configurations different than the baseline
R1	Lab101-R1-TT-D-Cfg.txt	This file contains configurations different than the baseline
R2	Lab101-R2-TT-D-Cfg.txt	This file contains configurations different than the baseline
R3	Lab101-R3-TT-D-Cfg.txt	This file contains configuration errors and the router must be restarted after it is loaded
SRV1	N/A	Static IP: 10.1.50.1 Default gateway: 10.1.50.254
PC-B	N/A	DHCP
PC-C	N/A	DHCP

Instructor note: The student loads the "broken" TT configuration files for all devices, even though only the configurations indicated in the Notes column contain errors.

Step 4: Configure SRV1 and start the syslog and TFTP servers.

a. Configure SRV1 with the static IP address 10.1.50.1/24 and default gateway 10.1.50.254.

b. Start the syslog server on SRV1 to monitor console messages from multiple devices.

c. Start the TFTP server on SRV1 to record device configuration changes.

Step 5: Release and renew the DHCP lease on PC-B and PC-C.

a. Ensure that PC-B is configured as a DHCP client in the OFFICE VLAN.

b. Ensure that PC-C is configured as a DHCP client in the R3 branch office LAN.

c. After loading all TT-D device configuration files, issue the **`ipconfig /release`** and **`ipconfig /renew`** commands on PC-B and PC-C.

Step 6: Outline the troubleshooting approach and validation steps.

Use this space to identify your troubleshooting approach and the key steps to verify that the problem is resolved. Troubleshooting approaches to select from include the follow-the-path, spot-the-differences, bottom-up, top-down, divide-and-conquer, shoot-from-the-hip, and move-the-problem methods.

Note: In addition to a specific approach, you can use the generic troubleshooting process described at the beginning of Section 2 of this lab.

____

____

____

____

____

____

The shoot-from-the-hip or follow-the-path method can be used. Other problem-solving methods are the top-down, bottom-up, follow-the-path, spot-the-differences, divide-and-conquer and move-the-problem approaches.

Verification steps can include:

- PC-C can ping the Internet (R2 Lo1, Lo2, or Lo3).
- PC-C can ping SRV1 (10.1.50.1).

Step 7: Record the troubleshooting process and configuration changes.

Use this log to document your actions and results during the troubleshooting process. List the commands that you used to gather information. As you progress, record what you think the problem might be and the actions you take to correct the problem.

Note: The table of commands following this log might help you troubleshoot this problem.

Device	Actions and Results

Device	Actions and Results

Command	Key Information Displayed
`show version`	Displays the device hardware and software status.
`dir flash:`	Displays the files and directories in flash memory.

Step 7: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with the instructor. The notes can include problems encountered, solutions applied, useful commands employed, alternate solutions, methods, and processes, and procedure and communication improvements.

____

____

____

____

____

____

____

Trouble Ticket TT-D Debrief—Instructor Notes

TT-D Issue

The configuration register has been set to 0x2100 on router R3, causing it to boot to ROM monitor mode instead of booting the Cisco IOS software. This simulates a potentially corrupted Cisco IOS image. There are two options to remedy this problem.

Option 1

a. Manually boot from a Cisco IOS image in flash memory, and change the configuration register value to its default value of 0x2102. To boot router R3 from ROM monitor mode, issue the following command:

```
boot flash:c1841-advipservicesk9-mz.124-24.T1.bin
```

Note: Replace the name of the Cisco IOS image file with the name of the file found in the flash of router R3. The files in flash can be listed from ROM monitor mode using the **`dir flash:`** command:

```
rommon 1 > dir flash:
program load complete, entry point: 0x8000f000, size: 0xcb80
Directory of flash:

2963     38266988  -rw-      c1841-advipservicesk9-mz.124-24.T1.bin
2        6389760   -rw-      sdm.tar
2079     931840    -rw-      es.tar
5389     1821      -rw-      sdmconfig-18xx.cfg
1977     415956    -rw-      sslclient-win-1.1.4.176.pkg
2307     1505280   -rw-      common.tar
2675     112640    -rw-      home.tar
2703     1038      -rw-      home.shtml
2704     527849    -rw-      128MB.sdf
2833     512000    -rw-      dg_sdm.tar
2958     2891      -rw-      running-config
1562     1697952   -rw-      securedesktop-ios-3.1.1.45-k9.pkg
2960     0         drw-      tshoot
```

b. To reset the configuration register to its default value of 0x2102, issue the following Cisco IOS command after the router has fully booted:

```
config-register 0x2102
```

c. Reload (or power cycle) the router.

Option 2

a. Change the config register value from ROM monitor before booting the Cisco IOS software by issuing the following command:

```
confreg 0x2102
```

b. Reload (or restart) the router or issue the **`reset`** command from ROM monitor mode.

Section 2 Troubleshooting Reference Information

This lab covers all the technologies that were practiced in the previous labs. Therefore, no specific additional troubleshooting flows are provided for this lab. Refer to the Sample Troubleshooting Flows sections in previous labs for examples of procedures for specific technologies.

General Troubleshooting Process

As a general guideline, you can use the following general troubleshooting process described in the course.

1. Define the problem (symptoms).
2. Gather information.
3. Analyze the information.
4. Propose a hypothesis (possible cause).
5. Test the hypothesis.
6. Eliminate or accept the hypothesis.
7. Solve the problem.
8. Document the problem.

Reflection Questions

1. Which lab trouble tickets did you have the most difficulty with?

2. Would you change anything about the process that you used for any of the trouble tickets now that you see the resolution of the problem?

3. Which commands did you find most useful in diagnosing issues?

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1700	Fast Ethernet 0 (FA0)	Fast Ethernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
1800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2600	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)
2800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

Device Configurations (instructor version)

Note: All device configurations are provided for TT-A. The configs provided here are *not* running-config outputs. They can be used for copy-and-paste for TT-A and subsequent tickets. Where a config is noted as being the same as a previous one, the only change is in the MOTD, which identifies the Lab and TT. The errors in the configuration are commented and highlighted as red text.

Trouble Ticket - TT-A Configurations

Switch ALS1

```
!Lab 10-1 Switch ALS1 TT-A Config
!
hostname ALS1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 10-1 Switch ALS1 TT-A Config ***$
!
ip dhcp snooping vlan 10
ip dhcp snooping
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
```

```
spanning-tree mode rapid-pvst
spanning-tree portfast default
!
interface Vlan1
 no ip address
 shutdown
!
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 100
 name MGMT
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel1
 description Channel to DLS1
 switchport trunk allowed vlan 10,20,30,100
 no shutdown
 !
interface Port-channel2
 description Channel to DLS2
 no shutdown
!
interface FastEthernet0/1
 description Channel to DLS1
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 ip dhcp snooping trust
 no shutdown
!
interface FastEthernet0/2
 description Channel to DLS1
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 ip dhcp snooping trust
 no shutdown
!
```

Error: List of allowed VLANs on Fa0/1 and Fa0/2 does not match those configured on the logical port channel Po1. VLAN 30 is missing.

```
interface range FastEthernet 0/1 – 2
 switchport trunk allowed vlan add 30
```

```
interface FastEthernet0/3
 description Channel to DLS2
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 ip dhcp snooping trust
 no shutdown
!
interface FastEthernet0/4
 description Channel to DLS2
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 ip dhcp snooping trust
 no shutdown
!
interface FastEthernet0/5
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown

interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
```

```
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description To PC-B
 switchport access vlan 10
 switchport mode access
 switchport voice vlan 20
```



```
 spanning-tree portfast
 switchport port-security
 switchport port-security maximum 2
 switchport port-security violation shutdown
 switchport port-security mac-address sticky
 no shut
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/2
 description Unused
```

```
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan100
 ip address 10.1.100.1 255.255.255.0
 no shutdown
!
ip default-gateway 10.1.100.254
!
ip http server
ip http secure-server
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server host 10.1.50.1 version 2c cisco
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps vlan-membership
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
  no transport input
!
ntp source Vlan100
ntp server 192.168.2.1
end
```

Switch DLS1

```
!Lab 10-1 Switch DLS1 TT-A Config
!
hostname DLS1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
```



```
banner motd $*** Lab 10-1 Switch DLS1 TT-A Config ***$
!
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
!
ip domain name tshoot.net
!
ip dhcp excluded-address 10.1.10.252 10.1.10.254
ip dhcp excluded-address 10.1.20.252 10.1.20.254
ip dhcp excluded-address 10.1.30.252 10.1.30.254
!
ip dhcp relay information trust-all
!
ip dhcp pool OFFICE
   network 10.1.10.0 255.255.255.0
   default-router 10.1.10.254
   domain-name tshoot.net
!
ip dhcp pool VOICE
   network 10.1.20.0 255.255.255.0
   default-router 10.1.20.254
   domain-name tshoot.net
!
ip dhcp pool GUEST
   network 10.1.30.0 255.255.255.0
   default-router 10.1.30.254
   domain-name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
```



```
spanning-tree vlan 10,30,100 priority 24576
spanning-tree vlan 20,50 priority 28672
!
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 100
 name MGMT
!
vlan 200
 name TRANS
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Loopback0
 description OSPF router ID
 ip address 10.1.211.1 255.255.255.255
 ip ospf network point-to-point
!
interface Port-channel1
 description Channel to ALS1
 no shut
!
interface Port-channel10
 description Channel to DLS2
 switchport trunk allowed vlan 10,20,30,50,200
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
```

Error: List of allowed VLANs on Po10 does not include management VLAN 100. Adding the VLAN to the port channel will automatically add it to interfaces F0/3 and Fa0/4.

```
interface Port-channel 10
 switchport trunk allowed vlan add 100
```



```
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R1
 no switchport
 ip address 10.1.2.1 255.255.255.252
 speed 100
 duplex full
 spanning-tree bpduguard enable
 no shut
!
interface FastEthernet0/6
 description FE to SRV1
 switchport access vlan 50
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shut
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
```



```
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
```



```
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
```



```
 shutdown
!
interface gigabitethernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 10.1.10.252 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 priority 110
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.252 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.252 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 priority 110
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.252 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 preempt
!
interface Vlan100
 ip address 10.1.100.252 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 priority 110
 standby 100 preempt
!
interface Vlan200
 ip address 10.1.200.252 255.255.255.0
!
router ospf 1
 log-adjacency-changes
 passive-interface default
 no passive-interface Vlan200
 no passive-interface FastEthernet0/5
 network 10.1.2.0 0.0.0.3 area 0
 network 10.1.10.0 0.0.0.255 area 1
 network 10.1.20.0 0.0.0.255 area 1
 network 10.1.30.0 0.0.0.255 area 1
 network 10.1.50.0 0.0.0.255 area 1
 network 10.1.100.0 0.0.0.255 area 1
 network 10.1.200.0 0.0.0.255 area 0
 network 10.1.211.1 0.0.0.0 area 0
```



```
!
ip classless
ip http server
ip http secure-server
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server host 10.1.50.1 version 2c cisco
snmp-server enable traps ospf state-change
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 192.168.2.1
end
```

Switch DLS2

```
!Lab 10-1 Switch DLS2 TT-A Config
!
hostname DLS2
!
service timestamps debug datetime msec
service timestamps log datetime
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 10-1 Switch DLS2 TT-A Config ***$
!
no ip domain lookup
!
```

```
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
  path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 28672
spanning-tree vlan 20,50 priority 24576
!
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 100
 name MGMT
!
vlan 200
 name TRANS
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
```



```
ip ssh source-interface Vlan100
!
interface Loopback0
 description OSPF router ID
 ip address 10.1.212.1 255.255.255.255
 ip ospf network point-to-point
!
interface Port-channel2
 description Channel to ALS1
 no shut

interface Port-channel10
 description Channel to DLS1
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R3
 no switchport
```

```
 ip address 10.1.2.13 255.255.255.252
 speed 100
 duplex full
 spanning-tree bpduguard enable
 no shutdown
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
```

```
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
```



```
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 10.1.10.253 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.253 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 priority 110
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.253 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 preempt
!
interface Vlan50
```



```
 ip address 10.1.50.253 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 priority 110
 standby 50 preempt
!
interface Vlan100
 ip address 10.1.100.253 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 preempt
!
interface Vlan200
 ip address 10.1.200.253 255.255.255.0
!
router ospf 1
 log-adjacency-changes
 passive-interface default
 no passive-interface Vlan200
 no passive-interface FastEthernet0/5
 network 10.1.2.12 0.0.0.3 area 0
 network 10.1.10.0 0.0.0.255 area 1
 network 10.1.20.0 0.0.0.255 area 1
 network 10.1.30.0 0.0.0.255 area 1
 network 10.1.50.0 0.0.0.255 area 1
 network 10.1.100.0 0.0.0.255 area 1
 network 10.1.200.0 0.0.0.255 area 0
 network 10.1.212.1 0.0.0.0 area 0
!
ip classless
ip http server
ip http secure-server
!
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps ospf state-change
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
```



```
 no transport input
!
ntp source Vlan100
ntp server 192.168.2.1
end
```

Router R1

```
!Lab 10-1 Router R1 TT-A Config
!
hostname R1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 10-1 Router R1 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 192.168.1.1 255.255.255.255
 ip ospf network point-to-point
!
interface FastEthernet0/0
 no ip address
 shutdown
!
interface FastEthernet0/1
 description FE to DLS1
```



```
 ip address 10.1.2.2 255.255.255.252
 ip flow ingress
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
 description WAN link to ISP R2
 ip address 209.165.200.225 255.255.255.252
 ip flow ingress
 encapsulation ppp
 clock rate 128000
 no shutdown
!
interface Serial0/0/1
 shutdown
!
router ospf 1
 log-adjacency-changes
 passive-interface default
 no passive-interface FastEthernet0/1
 no passive-interface Loopback0
 network 10.1.2.0 0.0.0.3 area 0
 network 192.168.1.1 0.0.0.0 area 0
 default-information originate always
!
router bgp 65501
 no synchronization
 bgp log-neighbor-changes
 neighbor 192.168.2.1 remote-as 65502
 neighbor 192.168.2.1 ebgp-multihop 2
 neighbor 192.168.2.1 update-source Loopback0
 no auto-summary
!
ip route 192.168.2.1 255.255.255.255 209.165.200.226
!
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
logging source-interface Loopback0
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps ospf state-change
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
```



```
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 192.168.2.1
end
```

Router R2

```
!Lab 10-1 Router R2 TT-A Config
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
Hostname R2
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 10-1 Router R2 TT-A Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 192.168.2.1 255.255.255.255
!
interface Loopback1
```



```
 ip address 172.30.1.1 255.255.255.255
!
interface Loopback2
 ip address 172.30.2.1 255.255.255.255
!
interface Loopback3
 ip address 172.30.3.1 255.255.255.255
!
interface FastEthernet0/0
 shutdown
!
interface FastEthernet0/1
 shutdown
!
interface Serial0/0/0
 description WAN link to R1 – T1 leased line
 ip address 209.165.200.226 255.255.255.252
 encapsulation ppp
 no shutdown
!
interface Serial0/0/1
 shutdown

router bgp 65502
 no synchronization
 bgp log-neighbor-changes
 network 0.0.0.0
 neighbor 192.168.1.1 remote-as 65501
 neighbor 192.168.1.1 ebgp-multihop 2
 neighbor 192.168.1.1 update-source Loopback0
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 null0
ip route 192.168.1.1 255.255.255.255 209.165.200.225
ip route 10.1.0.0 255.255.0.0 209.165.200.225
!
ip http server
no ip http secure-server
!
logging source-interface Loopback0
logging 10.1.50.1
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
```

```
!
ntp master 3
 end
```

Router R3

```
!Lab 10-1 Router R3 TT-A Config
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 10-1 Router R3 TT-A Config ***$
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
no ip domain lookup
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
ip dhcp excluded-address 10.1.80.1
ip dhcp excluded-address 10.1.80.129
!
ip dhcp pool R3-B1
   network 10.1.80.0 255.255.255.128
   default-router 10.1.80.1
   domain-name tshoot.net
!
ip dhcp pool R3-B2
   network 10.1.80.128 255.255.255.128
   default-router 10.1.80.129
   domain-name tshoot.net
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
```

```
!
interface Loopback0
 ip address 10.1.203.1 255.255.255.255
 ip ospf network point-to-point
!
interface Loopback1
description simulated R3-B2 LAN subnet
ip address 10.1.80.129 255.255.255.128
!
interface FastEthernet0/0
 description FE to R3-B1 LAN
 ip address 10.1.80.1 255.255.255.128
 ip flow ingress
 speed 100
 full-duplex
 no shutdown
!
interface FastEthernet0/1
 description FE to DLS2
 ip address 10.1.2.14 255.255.255.252
 ip flow ingress
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
description WAN link to R1 – not used for this lab
 no ip address
 clock rate 128000
 encapsulation ppp
 shutdown
!
interface Serial0/0/1
 description WAN link to R2 - not used for this lab
 no ip address
 encapsulation ppp
 shutdown
!
router eigrp 1
 redistribute ospf 1 metric 1544 2000 255 1 1500
 passive-interface default
 no passive-interface FastEthernet0/0
 no passive-interface loopback1
 network 10.1.80.0 0.0.0.127
 network 10.1.80.128 0.0.0.127
 no auto-summary
!
router ospf 1
 log-adjacency-changes
 redistribute eigrp 1 metric 100 subnets
 passive-interface default
 no passive-interface FastEthernet0/1
 network 10.1.2.12 0.0.0.3 area 0
 network 10.1.203.1 0.0.0.0 area 0
!
ip http server
no ip http secure-server
!
```



```
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
logging source-interface Loopback0
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 192.168.2.1
end
```

Trouble Ticket - TT-B Configurations

Router R3—Same as TT-A

Switch DLS2—Same as TT-A

Switch ALS1

```
!Lab 10-1 Switch ALS1 TT-B Config
!
hostname ALS1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 10-1 Switch ALS1 TT-B Config ***$
!
ip dhcp snooping vlan 10
ip dhcp snooping
```



```
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet

spanning-tree mode rapid-pvst
spanning-tree portfast default
!
interface Vlan1
 no ip address
 shutdown
!
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 100
 name MGMT
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Port-channel1
 description Channel to DLS1
 no shutdown
```



```
 !
interface Port-channel2
 description Channel to DLS2
 no shutdown
!
interface FastEthernet0/1
 description Channel to DLS1
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 ip dhcp snooping trust
 no shutdown
!
interface FastEthernet0/2
 description Channel to DLS1
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 ip dhcp snooping trust
 no shutdown
!
interface FastEthernet0/3
 description Channel to DLS2
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 ip dhcp snooping trust
 no shutdown
!
interface FastEthernet0/4
 description Channel to DLS2
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 ip dhcp snooping trust
 no shutdown
!
interface FastEthernet0/5
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
```

```
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
```



```
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description To PC-B
 switchport access vlan 10
 switchport mode access
 switchport voice vlan 20
 spanning-tree portfast
 switchport port-security
 switchport port-security maximum 2
 switchport port-security violation shutdown
 switchport port-security mac-address sticky
 no shut
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
```



```
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan100
 ip address 10.1.100.1 255.255.255.0
 no shutdown
!
ip default-gateway 10.1.100.254
!
ip http server
ip http secure-server
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server host 10.1.50.1 version 2c cisco
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps vlan-membership
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
```



```
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
  no transport input
!
ntp source Vlan100
ntp server 192.168.2.1
end
```

Switch DLS1

```
!Lab 10-1 Switch DLS1 TT-B Config
!
hostname DLS1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55

banner motd $*** Lab 10-1 Switch DLS1 TT-B Config ***$
!
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
!
ip domain name tshoot.net
!
ip dhcp excluded-address 10.1.10.252 10.1.10.254
ip dhcp excluded-address 10.1.20.252 10.1.20.254
ip dhcp excluded-address 10.1.30.252 10.1.30.254
!
ip dhcp relay information trust-all
!
ip dhcp pool OFFICE
   network 10.1.10.0 255.255.255.0
   default-router 10.1.10.254
   domain-name tshoot.net
!
ip dhcp pool VOICE
```



```
   network 10.1.20.0 255.255.255.0
   default-router 10.1.20.254
   domain-name tshoot.net
!
ip dhcp pool GUEST
   network 10.1.30.0 255.255.255.0
   default-router 10.1.30.254
   domain-name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 24576
spanning-tree vlan 20,50 priority 28672
!
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 100
 name MGMT
!
vlan 200
 name TRANS
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Loopback0
 description OSPF router ID
 ip address 10.1.211.1 255.255.255.255
```



```
 ip ospf network point-to-point
!
interface Port-channel1
 description Channel to ALS1
 no shut
!
interface Port-channel10
 description Channel to DLS2
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R1
 no switchport
 ip address 10.1.2.1 255.255.255.252
 speed 100
 duplex full
 spanning-tree bpduguard enable
 no shut
```



```
!
interface FastEthernet0/6
 description FE to SRV1
 switchport access vlan 50
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 no shut
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
```

```
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
```



```
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/1
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface gigabitethernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 10.1.10.252 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 priority 110
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.252 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.252 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 priority 110
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.252 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 preempt
```



```
!
interface Vlan100
 ip address 10.1.100.252 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 priority 110
 standby 100 preempt
!
interface Vlan200
 ip address 10.1.200.252 255.255.255.0
!
router ospf 1
 log-adjacency-changes
 passive-interface default
 no passive-interface Vlan200
 no passive-interface FastEthernet0/5
 network 10.1.2.0 0.0.0.3 area 0
 network 10.1.10.0 0.0.0.255 area 1
 network 10.1.20.0 0.0.0.255 area 1
 network 10.1.30.0 0.0.0.255 area 1
 network 10.1.50.0 0.0.0.255 area 1
 network 10.1.100.0 0.0.0.255 area 1
 network 10.1.200.0 0.0.0.255 area 0
 network 10.1.211.1 0.0.0.0 area 0
!
ip classless
ip http server
ip http secure-server
!
logging source-interface Vlan100
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server host 10.1.50.1 version 2c cisco
snmp-server enable traps ospf state-change
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
```



```
ntp server 192.168.2.1
end
```

Router R1

```
!Lab 10-1 Router R1 TT-B Config
!
hostname R1
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 10-1 Router R1 TT-B Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 192.168.1.1 255.255.255.255
 ip ospf network point-to-point
!
interface FastEthernet0/0
 no ip address
 shutdown
!
interface FastEthernet0/1
 description FE to DLS1
 ip address 10.1.2.2 255.255.255.252
 ip flow ingress
 speed 100
```

```
 full-duplex
 no shutdown
!
interface Serial0/0/0
 description WAN link to ISP R2
 ip address 209.165.200.225 255.255.255.252
 ip flow ingress
 encapsulation ppp
 clock rate 128000
 no shutdown
!
interface Serial0/0/1
 shutdown
!
router ospf 1
 log-adjacency-changes
 passive-interface default
 no passive-interface FastEthernet0/1
 no passive-interface Loopback0
 network 10.1.2.0 0.0.0.3 area 0
 network 192.168.1.1 0.0.0.0 area 0
!
router bgp 65501
 no synchronization
 bgp log-neighbor-changes
 neighbor 192.168.2.1 remote-as 65502
 neighbor 192.168.2.1 ebgp-multihop 2
 neighbor 192.168.2.1 update-source Loopback0
 no auto-summary
!
ip route 192.168.2.1 255.255.255.255 209.165.200.226
!
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
logging source-interface Loopback0
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps ospf state-change
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
```

Error: The **default-information originate** command is missing.

```
router ospf 1
  default-information originate
```



```
 exec-timeout 60 0
 transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 192.168.2.1
end
```

Router R2

```
!Lab 10-1 Router R2 TT-B Config
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
Hostname R2
!
logging buffered 16384 debugging
!
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 10-1 Router R2 TT-B Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 192.168.2.1 255.255.255.255
!
interface Loopback1
 ip address 172.30.1.1 255.255.255.255
!
interface Loopback2
```

```
 ip address 172.30.2.1 255.255.255.255
!
interface Loopback3
 ip address 172.30.3.1 255.255.255.255
!
interface FastEthernet0/0
 shutdown
!
interface FastEthernet0/1
 shutdown
!
interface Serial0/0/0
 description WAN link to R1 – T1 leased line
 ip address 209.165.200.226 255.255.255.252
 encapsulation ppp
 no shutdown
!
interface Serial0/0/1
 shutdown
!
router bgp 65502
 no synchronization
 bgp log-neighbor-changes
 network 0.0.0.0
 neighbor 192.168.1.1 remote-as 65501
 neighbor 192.168.1.1 ebgp-multihop 2
 neighbor 192.168.1.1 update-source Loopback0
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 null0
ip route 192.168.1.1 255.255.255.255 209.165.200.225
!
ip http server
no ip http secure-server
!
logging source-interface Loopback0
logging 10.1.50.1
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
!
ntp master 3
 end
```

Error: Static route to 10.1.0.0/16 network is missing.

ip route 10.1.0.0 255.255.0.0 209.165.200.225

Trouble Ticket - TT-C Configurations

Router R1—Same as TT-A

Router R2—Same as TT-A

Switch ALS1—Same as TT-B

Switch DLS1—Same as TT-B

Switch DLS2

```
!Lab 10-1 Switch DLS2 TT-C Config
!
hostname DLS2
!
service timestamps debug datetime msec
service timestamps log datetime
service password-encryption
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 10-1 Switch DLS2 TT-C Config ***$
!
no ip domain lookup
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
system mtu routing 1500
!
vtp domain TSHOOT
vtp mode transparent
!
ip subnet-zero
ip routing
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
errdisable recovery cause bpduguard
!
archive
 log config
  logging size 50
  notify syslog
  hidekeys
  path tftp://10.1.50.1/$h-archive-config
 write-memory
file prompt quiet
```

```
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,30,100 priority 28672
spanning-tree vlan 20,50 priority 24576
!
vlan 10
 name OFFICE
!
vlan 20
 name VOICE
!
vlan 30
 name GUEST
!
vlan 50
 name SERVERS
!
vlan 100
 name MGMT
!
vlan 200
 name TRANS
!
vlan 900
 name NATIVE
!
vlan 999
 name UNUSED
!
ip telnet source-interface Vlan100
ip ssh source-interface Vlan100
!
interface Loopback0
 description OSPF router ID
 ip address 10.1.212.1 255.255.255.255
 ip ospf network point-to-point
!
interface Port-channel2
 description Channel to ALS1
 no shut

interface Port-channel10
 description Channel to DLS1
 no shut
!
interface FastEthernet0/1
 description Channel to ALS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/2
 description Channel to ALS1
```

```
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode on
 no shut
!
interface FastEthernet0/3
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/4
 description Channel to DLS1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 10,20,30,50,100,200
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode on
 no shut
!
interface FastEthernet0/5
 description FE to R3
 no switchport
 ip address 10.1.2.13 255.255.255.252
 ip access-group 101 in
 speed 100
 duplex full
 spanning-tree bpduguard enable
 no shutdown
!
interface FastEthernet0/6
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/7
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/8
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
```

```
!
interface FastEthernet0/9
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/10
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/11
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/12
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/13
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/14
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/15
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/16
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/17
```



```
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/18
 description unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/19
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/20
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/21
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/22
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/23
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/24
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/1
 description Unused
 switchport access vlan 999
```



```
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet0/2
 description Unused
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 10.1.10.253 255.255.255.0
 standby 10 ip 10.1.10.254
 standby 10 preempt
!
interface Vlan20
 ip address 10.1.20.253 255.255.255.0
 standby 20 ip 10.1.20.254
 standby 20 priority 110
 standby 20 preempt
!
interface Vlan30
 ip address 10.1.30.253 255.255.255.0
 standby 30 ip 10.1.30.254
 standby 30 preempt
!
interface Vlan50
 ip address 10.1.50.253 255.255.255.0
 standby 50 ip 10.1.50.254
 standby 50 priority 110
 standby 50 preempt
!
interface Vlan100
 ip address 10.1.100.253 255.255.255.0
 standby 100 ip 10.1.100.254
 standby 100 preempt
!
interface Vlan200
 ip address 10.1.200.253 255.255.255.0
!
router ospf 1
 router-id 10.1.211.1
 log-adjacency-changes
 passive-interface default
 no passive-interface Vlan200
 no passive-interface FastEthernet0/5
 network 10.1.2.12 0.0.0.3 area 0
 network 10.1.10.0 0.0.0.255 area 1
 network 10.1.20.0 0.0.0.255 area 1
 network 10.1.30.0 0.0.0.255 area 1
 network 10.1.50.0 0.0.0.255 area 1
 network 10.1.100.0 0.0.0.255 area 1
 network 10.1.200.0 0.0.0.255 area 0
```

Error: Wrong router ID is configured. This is the DLS1 router ID which results in a duplicate. Change to the IP address of the DLS2 Loopback 0 interface.

```
router ospf 1
  router-id 10.1.212.1
```



```
 network 10.1.212.1 0.0.0.0 area 0
!
ip classless
ip http server
ip http secure-server
!
!
logging source-interface Vlan100
logging 10.1.50.1
!
access-list 101 permit ip 10.1.80.0 0.0.0.255 any
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Vlan100
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps ospf state-change
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
 transport input telnet ssh
line vty 5 15
 no transport input
!
ntp source Vlan100
ntp server 192.168.2.1
end
```

Error: ACL 101 does not permit the OSPF protocol. Add the following statement:

access-list 101 permit ospf any any

Error: ACL 101 does not permit ping or traceroute from R3 default Fa0/1 interface (10.1.2.14) to other network internal devices. Add the following statement:

access-list 101 permit ip host 10.1.2.14 any

Error: ACL 101 does not permit Telnet, SSH, NTP, SNMP or syslog from R3 Lo0 source interface (10.1.203.1) to other network internal devices. Add the following statement:

access-list 101 permit ip host 10.1.203.1 any

Router R3

```
!Lab 10-1 Router R3 TT-C Config
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
```



```
banner motd $*** Lab 10-1 Router R3 TT-C Config ***$
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
no ip domain lookup
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
ip dhcp excluded-address 10.1.80.1
ip dhcp excluded-address 10.1.80.129
!
ip dhcp pool R3-B1
   network 10.1.80.0 255.255.255.128
   default-router 10.1.80.1
   domain-name tshoot.net
!
ip dhcp pool R3-B2
   network 10.1.80.128 255.255.255.128
   default-router 10.1.80.129
   domain-name tshoot.net
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 10.1.203.1 255.255.255.255
 ip ospf network point-to-point
!
interface Loopback1
description simulated R3-B2 LAN subnet
ip address 10.1.80.129 255.255.255.128
!
interface FastEthernet0/0
 description FE to R3-B1 LAN
 ip address 10.1.80.1 255.255.255.128
 ip flow ingress
 speed 100
 full-duplex
 no shutdown
!
interface FastEthernet0/1
 description FE to DLS2
 ip address 10.1.2.14 255.255.255.252
 ip flow ingress
```



```
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
description WAN link to R1 – not used for this lab
 no ip address
 clock rate 128000
 encapsulation ppp
 shutdown
!
interface Serial0/0/1
 description WAN link to R2 - not used for this lab
 no ip address
 encapsulation ppp
 shutdown
!
router eigrp 1
 redistribute ospf 1 metric 1544 2000 255 1 1500
 passive-interface default
 no passive-interface FastEthernet0/0
 no passive-interface loopback1
 network 10.1.81.0 0.0.0.127
 network 10.1.80.128 0.0.0.127
 no auto-summary
!
router ospf 1
 log-adjacency-changes
 redistribute eigrp 1 metric 100 subnets
 passive-interface default
 no passive-interface FastEthernet0/1
 network 10.1.2.12 0.0.0.3 area 0
 network 10.1.203.1 0.0.0.0 area 0
!
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
logging source-interface Loopback0
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
```

Error: Wrong subnet is advertised under EIGRP.

```
router eigrp 1
 no network 10.1.81.0 0.0.0.127
 network 10.1.80.0 0.0.0.128
```

```
 logging synchronous
line vty 0 4
 exec-timeout 60 0
transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 192.168.2.1
end
```

Trouble Ticket - TT-D Configurations

Error: The config register for R3 is set to boot to ROM Monitor mode and not Cisco IOS.

Option 1:
a. Boot from ROM monitor
boot flash:c1841-advipservicesk9-mz.124-24.T1.bin
b. Issue the IOS command:
config-register 0x2102

Option 2:
a. Reset the config register from ROM monitor
confreg 0x2102
b. Reload the router or issue the **reset** command from ROM monitor mode.

Router R1—Same as TT-A

Router R2—Same as TT-A

Switch DLS2—Same as TT-A

Switch ALS1—Same as TT-B

Switch DLS1—Same as TT-B

Router R3

```
!Lab 10-1 Router R3 TT-D Config
!
config-register 0x2100
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
!
logging buffered 16384 debugging
enable secret ciscoenpa55
!
username admin secret adminpa55
!
banner motd $*** Lab 10-1 Router R3 TT-D Config ***$
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
!
no ip domain lookup
ip domain name tshoot.net
!
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
!
ip dhcp excluded-address 10.1.80.1
ip dhcp excluded-address 10.1.80.129
```



```
!
ip dhcp pool R3-B1
   network 10.1.80.0 255.255.255.128
   default-router 10.1.80.1
   domain-name tshoot.net
!
ip dhcp pool R3-B2
   network 10.1.80.128 255.255.255.128
   default-router 10.1.80.129
   domain-name tshoot.net
!
file prompt quiet
archive
 log config
  logging size 50
  notify syslog
  hidekeys
 path tftp://10.1.50.1/$h-archive-config
 write-memory
!
ip telnet source-interface Loopback0
ip ssh source-interface Loopback0
!
interface Loopback0
 ip address 10.1.203.1 255.255.255.255
 ip ospf network point-to-point
!
interface Loopback1
description simulated R3-B2 LAN subnet
ip address 10.1.80.129 255.255.255.128
!
interface FastEthernet0/0
 description FE to R3-B1 LAN
 ip address 10.1.80.1 255.255.255.128
 ip flow ingress
 speed 100
 full-duplex
 no shutdown
!
interface FastEthernet0/1
 description FE to DLS2
 ip address 10.1.2.14 255.255.255.252
 ip flow ingress
 speed 100
 full-duplex
 no shutdown
!
interface Serial0/0/0
description WAN link to R1 – not used for this lab
 no ip address
 clock rate 128000
 encapsulation ppp
 shutdown
!
interface Serial0/0/1
 description WAN link to R2 - not used for this lab
 no ip address
 encapsulation ppp
```

```
 shutdown
!
router eigrp 1
 redistribute ospf 1 metric 1544 2000 255 1 1500
 passive-interface default
 no passive-interface FastEthernet0/0
 no passive-interface loopback1
 network 10.1.80.0 0.0.0.127
 network 10.1.80.128 0.0.0.127
 no auto-summary
!
router ospf 1
 log-adjacency-changes
 redistribute eigrp 1 metric 100 subnets
 passive-interface default
 no passive-interface FastEthernet0/1
 network 10.1.2.12 0.0.0.3 area 0
 network 10.1.203.1 0.0.0.0 area 0
!
ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.50.1 9996
!
logging source-interface Loopback0
logging 10.1.50.1
!
snmp-server community cisco RO
snmp-server community san-fran RW
snmp-server trap-source Loopback0
snmp-server location TSHOOT Lab Facility
snmp-server contact support@tshoot.net
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps config
snmp-server enable traps cpu threshold
snmp-server host 10.1.50.1 version 2c cisco
!
line con 0
 exec-timeout 60 0
 login authentication CONSOLE
 logging synchronous
line vty 0 4
 exec-timeout 60 0
transport input telnet ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 192.168.2.1
end
```

