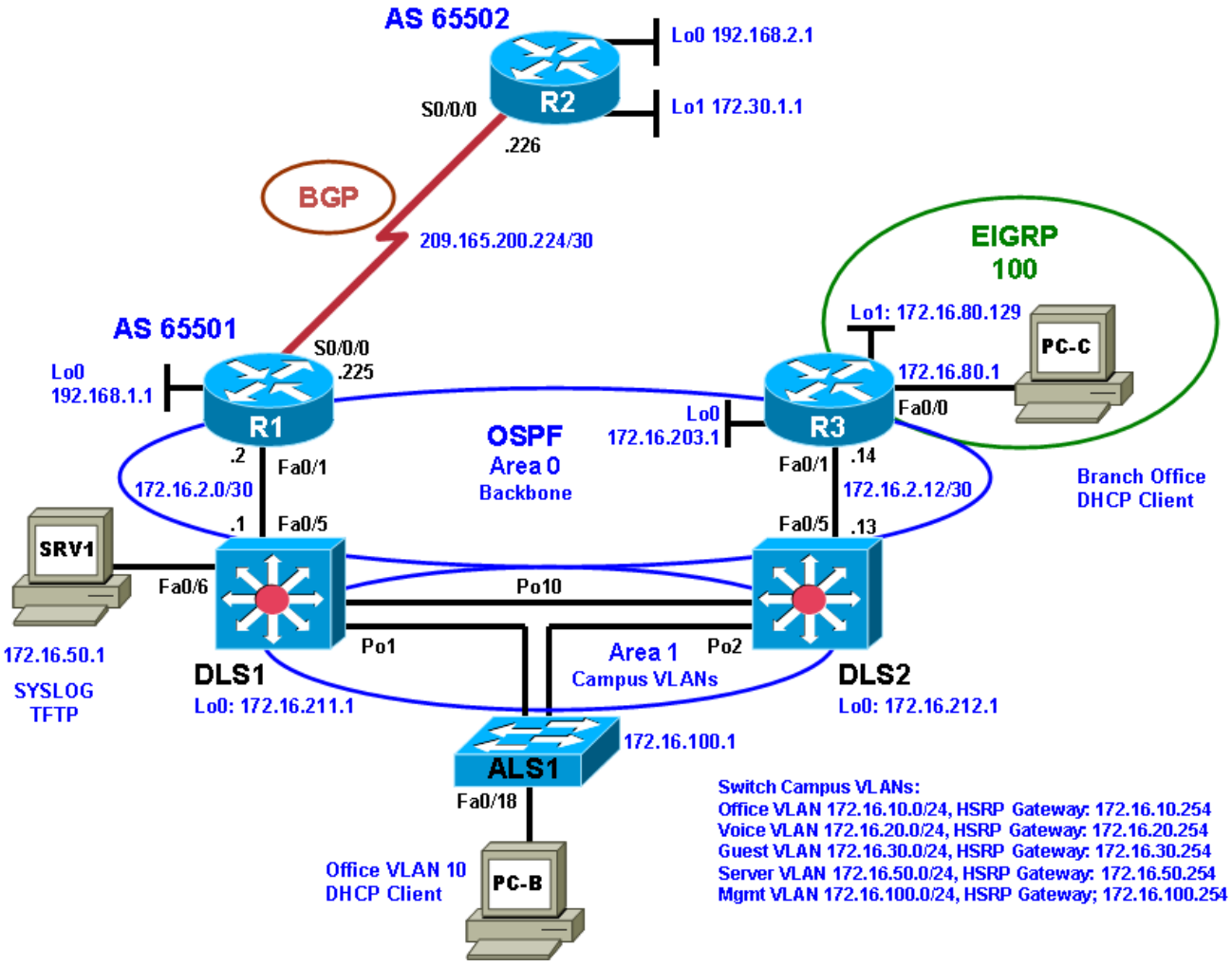
Laboration 4

Troubleshooting Problems related to Security

Topology



Objectives

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

Part 2: Troubleshoot and correct errors related to security in the Management Plane, Control Plane and Data Plane.

Laboration Overview

This Laboration is a practical exercise for the course CCNPv6 TSHOOT. In Part 1, you erase the existing configuration and load the error configs. In Part 2, you will find and correct errors related to security issues in the Management, Control and Data Plane.

In this laboration an ACL is applied in R3 to only allow ICMP and HTTP traffic from the directly connected LANs to all other networks.

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-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

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

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

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

Step 2: Erase the startup config from NVRAM.

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

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

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

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

The format of these files is TSHOOT-xxxx-Lab4-Error-Cfg.txt, where *xxxx* is the name of the device.

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

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

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

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

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

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

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

Step 10: Configure the PCs.

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

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

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

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

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

Part 2: Troubleshoot and Correct the Errors

Step 1: Perform connectivity tests.

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

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

Network Connectivity Test Table

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

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

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

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

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

Problem Resolution and Verification Table

Device	Problem or Error Discovered	Corrective Action (commands used)	Verification Commands (more than one command can be used)

Notes

_____

_____

_____

_____
_____
_____
_____
_____

Step 3: Demonstrate basic network connectivity after correcting errors.

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

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

Ping Test Table

From Device/Interface/IP	To Device/Interface/IP	Successful (Y/N)
PC-B	PC-C (DHCP 172.16.80.2)	
PC-B	HSRP default gateway (172.16.10.254)	
PC-B	SRV1 (172.16.50.1)	
PC-B	ALS1 mgmt (172.16.100.1)	
PC-B	DLS1 mgmt (172.16.100.252)	
PC-B	DLS2 mgmt (172.16.100.253)	
PC-B	R1 Fa0/1 (172.16.2.2)	
PC-B	R2 Lo1 (172.30.1.1)	
PC-B	R3 Fa0/1 (172.16.2.14)	
PC-C	R3 default gateway (172.16.80.1)	
PC-C	SRV1 (172.16.50.1)	
PC-C	ALS1 mgmt (172.16.100.1)	
PC-C	DLS1 mgmt (172.16.100.252)	
PC-C	DLS2 mgmt (172.16.100.253)	
PC-C	R1 Fa0/1 (172.16.2.2)	
PC-C	R2 Lo1 (172.30.1.1)	
PC-C	R3 Fa0/1 (172.16.2.14)	
ALS1 mgmt vlan 100 (172.16.100.1)	DLS1 mgmt (172.16.100.252)	
ALS1 mgmt vlan 100	DLS2 mgmt (172.16.100.253)	
ALS1 mgmt vlan 100	R1 Fa0/1 (172.16.2.2)	
ALS1 mgmt vlan 100	R2 Lo1 (172.30.1.1)	
ALS1 mgmt vlan 100	R3 Fa0/1 (172.16.2.14)	

Notes

_____
_____
_____
_____
_____
_____
_____

Step 4: Demonstrate Telnet and SSH connectivity.

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

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

Remote Access Test Table

From Device	To Device/Interface/IP	Telnet (Y/N)	SSH (Y/N)
PC-B	ALS1 mgmt (172.16.100.1)		
PC-B	DLS1 mgmt (172.16.100.252)		
PC-B	DLS2 mgmt (172.16.100.253)		
PC-B	R1 Fa0/1 (172.16.2.2)		
PC-B	R2 S0/0/0 (209.165.200.226)		
PC-B	R3 Fa0/1 (172.16.2.14)		

Step 5: Demonstrate NTP functionality.

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

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

NTP Synchronization Table

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

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

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

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

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

STP Redundancy Test Table

From Device/Interface/IP	To Device/Interface/IP	Result
PC-B	HSRP default gateway (172.16.10.254)	
PC-B	PC-C	
PC-B	SRV1 (172.16.50.1)	
PC-B	ALS1 mgmt (172.16.100.1)	
PC-B	DLS1 mgmt (172.16.100.252)	
PC-B	DLS2 mgmt (172.16.100.253)	
PC-B	R1 Fa0/1 (172.16.2.2)	
PC-B	R2 Lo1 (172.30.1.1)	
PC-B	R3 Fa0/1 (172.16.2.14)	

Notes:

_____
_____
_____
_____
_____
_____
_____

Command Summary

The table lists useful commands for this lab.

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.
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.
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.