Networking Academy
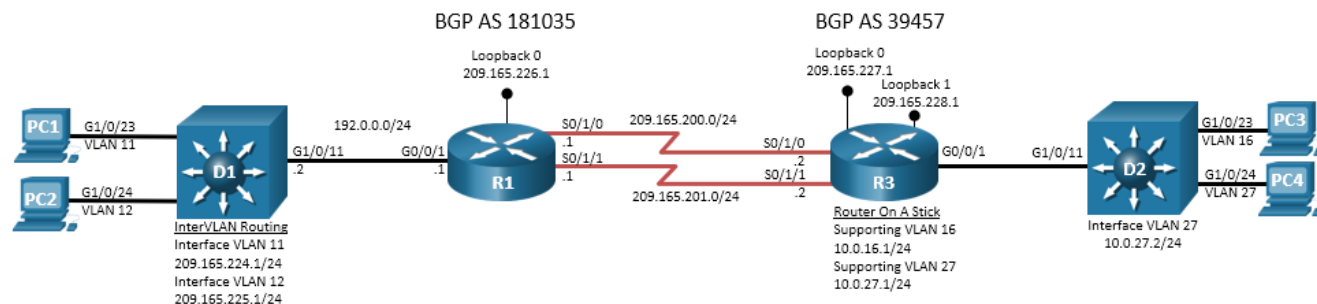
Lab - Troubleshoot IPv4 ACLs (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Answers: 21.1.2 Lab - Troubleshoot IPv4 ACLs

Topology

Addressing Table

Device	Interface	IP Address	Subnet Mask
R1	G0/0/1	192.0.0.1	255.255.255.0
	S0/1/0	209.165.200.1	255.255.255.0
	S0/1/1	209.165.201.1	255.255.255.0
	Loopback0	209.165.226.1	255.255.255.0
R3	G0/0/1.16	10.0.16.1	255.255.255.0
	G0/0/1.27	10.0.27.1	255.255.255.0
	S0/1/0	209.165.200.2	255.255.255.0
	S0/1/1	209.165.201.2	255.255.255.0
	Loopback0	209.165.227.1	255.255.255.0
	Loopback1	209.165.228.1	255.255.255.0
D1	G1/0/11	192.0.0.2	255.255.255.0
	VLAN 11	209.165.224.1	255.255.255.0
	VLAN 12	209.165.225.1	255.255.255.0
PC1	NIC	DHCP	
PC2	NIC	DHCP	
PC3	NIC	DHCP	
PC4	NIC	DHCP	

Objectives

Troubleshoot network issues related to the configuration and operation of ACLs for IPv4.

Background / Scenario

In this topology, R1 and D1 are OSPF neighbors, while R1 and R3 are BGP neighbors. Switch D1 provides inter-VLAN routing for two subnets. R3 provides inter-VLAN routing for two subnets, and switch D2 provides connectivity for the two VLANs supporting those subnets. The BGP relationship between R1 and R3 is established using EBGP multihop between the router's respective Loopback 0 interfaces. You will be loading configurations with intentional errors onto the network. Your tasks are to FIND the error(s), document your findings and the command(s) or method(s) used to fix them, FIX the issue(s) presented here and then test the network to ensure both of the following conditions are met:

1) the complaint received in the ticket is resolved

2) full reachability is restored

Note: The routers used with CCNP hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.4 (universalk9 image). The switches used in the labs are Cisco Catalyst 3650 with Cisco IOS XE Release 16.9.4 (universalk9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

Note: Make sure that the devices have been erased and have no startup configurations. If you are unsure, contact your instructor.

Instructor Note: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

Required Resources

- 2 Routers (Cisco 4221 with Cisco IOS XE Release 16.9.4 universal image or comparable)
- 2 Switches (Cisco 3560 with Cisco IOS XE Release 16.9.4 universal image or comparable)
- 4 PCs (Choice of operating system with terminal emulation program installed)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Instructions

Part 1: Trouble Ticket 21.1.2.1

Scenario:

A security consultant worked overnight making R1 and R3 compliant with RFC 1918. After the consultant finished the task, a business-critical connection between PC1 and PC3 is no longer operational. The task of finding and fixing the error(s) is now your job.

Use the commands listed below to load the configuration files for this trouble ticket:

Instructor Note: Commands for uploading the configuration are provided at the end of this document.

Device	Command
R1	`copy flash:/enarsi/21.1.2.1-r1-config.txt run`
R3	`copy flash:/enarsi/21.1.2.1-r3-config.txt run`

Device	Command
D1	`copy flash:/enarsi/21.1.2.1-d1-config.txt run`
D2	`copy flash:/enarsi/21.1.2.1-d2-config.txt run`

- PCs 1, 2, 3, and 4 receive their addressing via DHCP for IPv4.

- Passwords on all devices are **cisco12345**. If a username is required, use **admin**.

- When you have fixed the ticket, change the MOTD on EACH DEVICE using the following command:

  banner motd # This is $(hostname) FIXED from ticket <ticket number> #

- Then save the configuration by issuing the **wri** command (on each device).

- Inform your instructor that you are ready for the next ticket.

- After the instructor approves your solution for this ticket, issue the **reset.now** privileged EXEC command. This script will clear your configurations and reload the devices.

Instructor Notes:

Although the trouble ticket does not mention this, the student may also notice that PC2 and PC4 cannot communicate. The ticket came in from the users of the connection between PC1 and PC3. Therefore, that is the focus. Fixing the issue between PC1 and PC3 will also restore full connectivity between all PCs. This trouble ticket contains 1 intentional error. The NAT ACL on R3, named NAT-ELIGIBLE, is configured with the wrong wildcard mask, causing hosts in VLAN 16 and VLAN 27 not to qualify for NAT. Because those networks are not advertised in BGP and blocked at R1, PC3 cannot communicate with PC1.

The student may choose one of two methods to correct the error. They may either completely remove and replace the NAT-ELIGIBLE ACL, or they may edit the NAT-ELIGIBLE ACL and replace the errored statement.

The commands the use the latter method to fix these errors should be:

```
R3(config)# ip access-list standard NAT-ELIGIBLE
R3(config-std-nacl)# no 10
R3(config-std-nacl)# 10 permit 10.0.0.0 0.0.255.255
R3(config-std-nacl)# exit
R3(config)# end
```

Part 2: Trouble Ticket 21.1.2.2

Scenario:

A junior network administrator has attempted to tune access control lists to improve security. After doing so, PC2 is no longer able to communicate with devices with the IPv4 addresses 209.165.227.1 or 209.165.228.1. This problem needs to be solved to allow for business operations to continue.

Use the commands listed below to load the configuration files for this trouble ticket:

Instructor Note: Commands for uploading the configuration are provided at the end of this document.

Device	Command
R1	`copy flash:/enarsi/21.1.2.2-r1-config.txt run`
R3	`copy flash:/enarsi/21.1.2.2-r3-config.txt run`
D1	`copy flash:/enarsi/21.1.2.2-d1-config.txt run`
D2	`copy flash:/enarsi/21.1.2.2-d2-config.txt run`

- PCs 1, 2, 3, and 4 receive their addressing via DHCP for IPv4.

- Passwords on all devices are **cisco12345**. If a username is required, use **admin**.

- When you have fixed the ticket, change the MOTD on EACH DEVICE using the following command:

  banner motd # This is $(hostname) FIXED from ticket <ticket number> #

- Then save the configuration by issuing the **wri** command (on each device).

- Inform your instructor that you are ready for the next ticket.

- After the instructor approves your solution for this ticket, issue the **reset.now** privileged EXEC command. This script will clear your configurations and reload the devices.

Instructor Notes:

This trouble ticket contains 1 intentional error. An ACL called IPCHECK has been added inbound on R1. The wildcard mask does not include the VLAN 12 network, so PC2 and VLAN 12 are blocked.

The student may choose one of two methods to correct the error. They may either completely remove and replace the IPCHECK ACL, or they may edit the IPCHECK ACL and replace the errored statement, or add an additional statement to permit the VLAN 12 network.

The commands to replace the errored statement should be:

```
R1(config)# ip access-list extended IPCHECK
R1(config-std-nacl)# no 10
R1(config-std-nacl)# 10 permit ip 209.165.224.0 0.0.1.255 any
R1(config-std-nacl)# exit
R1(config)# end
```

The commands to add permission for VLAN 12 should be:

```
R1(config)# ip access-list extended IPCHECK
R1(config-std-nacl)# 15 permit ip 209.165.225.0 0.0.0.255 any
R1(config-std-nacl)# exit
R1(config)# end
```

Part 3: Trouble Ticket 21.1.2.3

Scenario:

Security is an important consideration in your network. Over the weekend, a junior network administrator was working to improve remote access security with BGP AS 181035. It is 8:00 Monday morning, and router R1 and switch D1 are refusing Telnet connections. You need to find and fix this error as soon as possible.

Use the commands listed below to load the configuration files for this trouble ticket:

Instructor Note: Commands for uploading the configuration are provided at the end of this document.

Device	Command
R1	`copy flash:/enarsi/21.1.2.3-r1-config.txt run`
R3	`copy flash:/enarsi/21.1.2.3-r3-config.txt run`
D1	`copy flash:/enarsi/21.1.2.3-d1-config.txt run`
D2	`copy flash:/enarsi/21.1.2.3-d2-config.txt run`

- PCs 1, 2, 3, and 4 receive their addressing via DHCP for IPv4.

- Passwords on all devices are **cisco12345**. If a username is required, use **admin**.

- When you have fixed the ticket, change the MOTD on EACH DEVICE using the following command:

  banner motd # This is $(hostname) FIXED from ticket <ticket number> #

- Then save the configuration by issuing the **wri** command (on each device).

- Inform your instructor that you are ready for the next ticket.

- After the instructor approves your solution for this ticket, issue the **reset.now** privileged EXEC command. This script will clear your configurations and reload the devices.

Instructor Notes:

This trouble ticket contains 1 intentional error that is repeated in two places. The junior administrator did not understand the commands to use for adding a time-range to an ACL, and subsequently made the time-ranges extremely restrictive. He thought he was denying access between midnight and five a.m., when the result of the configuration was to allow access between midnight and five a.m. only.

To correct the error, the student must completely remove and replace the time range REMOTE-CONTROL and then reassign the VTY-CONTROL access-list to the vty lines.

The commands to replace the errored time-range should be:

```
R1(config)# no time-range REMOTE-CONTROL
R1(config)# time-range REMOTE-CONTROL
R1(config-time-range)# periodic weekdays 05:00 to 23:59
R1(config-time-range)# periodic weekend 05:00 to 23:59
R1(config-time-range)# exit
R1(config)# line vty 0 4
R1(config-line)# access-class VTY-CONTROL in
R1(config-line)# exit
R1(config)# end

D1(config)# no time-range REMOTE-CONTROL
D1(config)# time-range REMOTE-CONTROL
D1(config-time-range)# periodic weekdays 05:00 to 23:59
D1(config-time-range)# periodic weekend 05:00 to 23:59
D1(config-time-range)# exit
D1(config)# line vty 0 4
D1(config-line)# access-class VTY-CONTROL in
D1(config-line)# exit
D1(config)# end
```

Router Interface Summary Table

Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

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.

Uploading Configuration Files

Use the commands below to create the configuration files on the lab devices for each trouble ticket in this lab. The TCL script commands help create and copy the configurations. However, the configuration commands could also be copied and pasted directly into global config mode on each device. Simply remove the TCL script commands, enter the **enable** and **configure t** commands on the device, and copy and paste the configuration commands.

Important: The device requires a folder in flash named **enarsi**. Use the **dir** command to verify. If the folder is missing, then create it using the **mkdir flash:/enarsi** privileged exec command. For all switches, make sure the vlan.dat file is set to the default. Use the **delete vlan.dat** privileged exec command, if necessary.

Reset scripts

These TCL scripts will completely clear and reload the device in preparation for the next ticket. Copy and paste the appropriate script to the appropriate device.

Router Reset Script

```
tclsh
puts [ open "flash:/enarsi/reset.tcl" w+ ] {
typeahead "\n"
copy running-config startup-config
typeahead "\n"
erase startup-config
puts "Reloading the router"
typeahead "\n"
reload
}
tclquit
```

D1/D2 (Cisco 3650) Reset Script - The default 3650 SDM template supports IPv6, so it is not set by this script.

```
tclsh
puts [ open "flash:/enarsi/reset.tcl" w+ ] {
typeahead "\n"
copy running-config startup-config
typeahead "\n"
erase startup-config
delete /force vlan.dat
puts "Reloading the switch"
typeahead "\n"
reload
}
tclquit
```

R1 Configuration File Scripts

! R1 - Trouble Ticket # 1

```
tclsh
puts [ open "flash:/enarsi/21.1.2.1-r1-config.txt" w+ ] {
hostname R1
no ip domain lookup
banner motd # This is R1, Trouble Ticket 21.1.2.1 #
enable secret cisco12345
username admin privilege 15 algorithm-type scrypt secret cisco12345
ip access-list extended IPCHECK
 permit ip 209.165.224.0 0.0.1.255 any
 permit ip 192.0.0.0 0.0.0.255 any
 exit
ip access-list standard BOGON-MARTIAN
 deny 10.0.0.0 0.255.255.255
 deny 172.16.0.0 0.31.255.255
 deny 192.168.0.0 0.0.255.255
 deny 127.0.0.0 0.255.255.255
 deny 192.0.0.0 0.0.0.255
 deny 209.165.224.0 0.0.0.255
 deny 209.165.225.0 0.0.0.255
 deny host 209.165.226.1
 permit any
 exit
interface g0/0/1
 ip address 192.0.0.1 255.255.255.0
 ip access-group IPCHECK in
 no shutdown
 exit
interface s0/1/0
 ip address 209.165.200.1 255.255.255.0
 ip access-group BOGON-MARTIAN in
```

```
 no shutdown
 exit
interface s0/1/1
 ip address 209.165.201.1 255.255.255.0
 ip access-group BOGON-MARTIAN in
 no shutdown
 exit
interface loopback 0
 ip address 209.165.226.1 255.255.255.255
 no shutdown
 exit
ip route 209.165.227.1 255.255.255.255 s0/1/0
ip route 209.165.227.1 255.255.255.255 s0/1/1
router ospf 1
 router-id 1.1.1.1
 network 192.0.0.0 0.0.0.255 area 0
 default-information originate always
 exit
router bgp 181035
 bgp router-id 209.165.226.1
 neighbor 209.165.227.1 remote-as 39457
 neighbor 209.165.227.1 update-source loopback 0
 neighbor 209.165.227.1 ebgp-multihop 3
 network 209.165.224.0 mask 255.255.255.0
 network 209.165.225.0 mask 255.255.255.0
 network 192.0.0.0 mask 255.255.255.0
 exit
time-range REMOTE-CONTROL
 periodic weekdays 05:00 to 23:59
 periodic weekend 05:00 to 23:59
 exit
ip access-list extended VTY-CONTROL
 permit ip 209.165.224.0 0.0.0.255 any time-range REMOTE-CONTROL
 deny ip any any log
 exit
line con 0
 logging synchronous
 exec-timeout 0 0
 exit
line vty 0 4
 login local
 transport input telnet
 exec-timeout 5 0
 access-class VTY-CONTROL in
 exit
```

```
alias exec reset.now tclsh flash:/enarsi/reset.tcl
end
}
tclquit
```

! R1 - Trouble Ticket # 2

```
tclsh
puts [ open "flash:/enarsi/21.1.2.2-r1-config.txt" w+ ] {
hostname R1
no ip domain lookup
banner motd # This is R1,  Trouble Ticket 21.1.2.2  #
enable secret cisco12345
username admin privilege 15 algorithm-type scrypt secret cisco12345
ip access-list extended IPCHECK
 permit ip 209.165.224.0 0.0.0.255 any
 permit ip 192.0.0.0 0.0.0.255 any
 exit
ip access-list standard BOGON-MARTIAN
 deny 10.0.0.0 0.255.255.255
 deny 172.16.0.0 0.31.255.255
 deny 192.168.0.0 0.0.255.255
 deny 127.0.0.0 0.255.255.255
 deny 192.0.0.0 0.0.0.255
 deny 209.165.224.0 0.0.0.255
 deny 209.165.225.0 0.0.0.255
 deny host 209.165.226.1
 permit any
 exit
interface g0/0/1
 ip address 192.0.0.1 255.255.255.0
 ip access-group IPCHECK in
 no shutdown
 exit
interface s0/1/0
 ip address 209.165.200.1 255.255.255.0
 ip access-group BOGON-MARTIAN in
 no shutdown
 exit
interface s0/1/1
 ip address 209.165.201.1 255.255.255.0
 ip access-group BOGON-MARTIAN in
 no shutdown
 exit
interface loopback 0
 ip address 209.165.226.1 255.255.255.255
 no shutdown
```

```
 exit
ip route 209.165.227.1 255.255.255.255 s0/1/0
ip route 209.165.227.1 255.255.255.255 s0/1/1
router ospf 1
 router-id 1.1.1.1
 network 192.0.0.0 0.0.0.255 area 0
 default-information originate always
 exit
router bgp 181035
 bgp router-id 209.165.226.1
 neighbor 209.165.227.1 remote-as 39457
 neighbor 209.165.227.1 update-source loopback 0
 neighbor 209.165.227.1 ebgp-multihop 3
 network 209.165.224.0 mask 255.255.255.0
 network 209.165.225.0 mask 255.255.255.0
 network 192.0.0.0 mask 255.255.255.0
 exit
time-range REMOTE-CONTROL
 periodic weekdays 05:00 to 23:59
 periodic weekend 05:00 to 23:59
 exit
ip access-list extended VTY-CONTROL
 permit ip 209.165.224.0 0.0.0.255 any time-range REMOTE-CONTROL
 deny ip any any log
 exit
line con 0
 logging synchronous
 exec-timeout 0 0
 exit
line vty 0 4
 login local
 transport input telnet
 exec-timeout 5 0
 access-class VTY-CONTROL in
 exit
alias exec reset.now tclsh flash:/enarsi/reset.tcl
end
}
tclquit
```

! R1 - Trouble Ticket # 3

```
tclsh
puts [ open "flash:/enarsi/21.1.2.3-r1-config.txt" w+ ] {
hostname R1
no ip domain lookup
banner motd # This is R1, Trouble Ticket 21.1.2.3 #
```

```
enable secret cisco12345
username admin privilege 15 algorithm-type scrypt secret cisco12345
ip access-list extended IPCHECK
 permit ip 209.165.224.0 0.0.1.255 any
 permit ip 192.0.0.0 0.0.0.255 any
 exit
ip access-list standard BOGON-MARTIAN
 deny 10.0.0.0 0.255.255.255
 deny 172.16.0.0 0.31.255.255
 deny 192.168.0.0 0.0.255.255
 deny 127.0.0.0 0.255.255.255
 deny 192.0.0.0 0.0.0.255
 deny 209.165.224.0 0.0.0.255
 deny 209.165.225.0 0.0.0.255
 deny host 209.165.226.1
 permit any
 exit
interface g0/0/1
 ip address 192.0.0.1 255.255.255.0
 ip access-group IPCHECK in
 no shutdown
 exit
interface s0/1/0
 ip address 209.165.200.1 255.255.255.0
 ip access-group BOGON-MARTIAN in
 no shutdown
 exit
interface s0/1/1
 ip address 209.165.201.1 255.255.255.0
 ip access-group BOGON-MARTIAN in
 no shutdown
 exit
interface loopback 0
 ip address 209.165.226.1 255.255.255.255
 no shutdown
 exit
ip route 209.165.227.1 255.255.255.255 s0/1/0
ip route 209.165.227.1 255.255.255.255 s0/1/1
router ospf 1
 router-id 1.1.1.1
 network 192.0.0.0 0.0.0.255 area 0
 default-information originate always
 exit
router bgp 181035
 bgp router-id 209.165.226.1
```

```
  neighbor 209.165.227.1 remote-as 39457
  neighbor 209.165.227.1 update-source loopback 0
  neighbor 209.165.227.1 ebgp-multihop 3
  network 209.165.224.0 mask 255.255.255.0
  network 209.165.225.0 mask 255.255.255.0
  network 192.0.0.0 mask 255.255.255.0
  exit
time-range REMOTE-CONTROL
 periodic weekdays 00:00 to 05:00
 periodic weekend 00:00 to 05:00
 exit
ip access-list extended VTY-CONTROL
 permit ip 209.165.224.0 0.0.0.255 any time-range REMOTE-CONTROL
 deny ip any any log
 exit
line con 0
 logging synchronous
 exec-timeout 0 0
 exit
line vty 0 4
 login local
 transport input telnet
 exec-timeout 5 0
 access-class VTY-CONTROL in
 exit
alias exec reset.now tclsh flash:/enarsi/reset.tcl
end
}
tclquit
```

R2 Configuration File Scripts - Not Used In This Lab

R3 Configuration File Scripts

! R3 - Trouble Ticket # 1

```
tclsh
puts [ open "flash:/enarsi/21.1.2.1-r3-config.txt" w+ ] {
hostname R3
no ip domain lookup
banner motd # This is R3, Trouble Ticket 21.1.2.1  #
enable secret cisco12345
username admin privilege 15 algorithm-type scrypt secret cisco12345
ip access-list standard BOGON-MARTIAN
 deny 10.0.0.0 0.255.255.255
 deny 172.16.0.0 0.31.255.255
 deny 192.168.0.0 0.0.255.255
```

```
  deny 127.0.0.0 0.255.255.255
  deny host 209.165.227.1
  deny host 209.165.228.1
 permit any
 exit
interface g0/0/1
 no ip address
 no shutdown
interface g0/0/1.16
 encapsulation dot1q 16
 ip address 10.0.16.1 255.255.255.0
 no shutdown
 exit
interface g0/0/1.27
 encapsulation dot1q 27
 ip address 10.0.27.1 255.255.255.0
 no shutdown
 exit
interface s0/1/0
 ip address 209.165.200.2 255.255.255.0
 ip access-group BOGON-MARTIAN in
 no shutdown
interface s0/1/1
 ip address 209.165.201.2 255.255.255.0
 ip access-group BOGON-MARTIAN in
 no shutdown
interface loopback 0
 ip address 209.165.227.1 255.255.255.255
 no shutdown
 exit
interface loopback 1
 ip address 209.165.228.1 255.255.255.255
 no shutdown
 exit
ip route 209.165.226.1 255.255.255.255 s0/1/0
ip route 209.165.226.1 255.255.255.255 s0/1/1
router bgp 39457
 bgp router-id 209.165.227.1
 neighbor 209.165.226.1 remote-as 181035
 neighbor 209.165.226.1 update-source loopback 0
 neighbor 209.165.226.1 ebgp-multihop 3
 network 209.165.228.1 mask 255.255.255.255
 exit
ip access-list standard NAT-ELIGIBLE
 permit 10.0.0.0 0.0.0.255
```

```
 deny any log
 exit
ip nat inside source list NAT-ELIGIBLE interface loopback 1 overload
ip dhcp excluded-address 10.0.16.1 10.0.16.5
ip dhcp excluded-address 10.0.27.1 10.0.27.5
ip dhcp pool NAT16
 network 10.0.16.0 255.255.255.0
 default-router 10.0.16.1
 exit
ip dhcp pool NAT27
 network 10.0.27.0 255.255.255.0
 default-router 10.0.27.1
 exit
interface s0/1/0
 ip nat outside
 exit
interface s0/1/1
 ip nat outside
 exit
interface g0/0/1.16
 ip nat inside
 exit
interface g0/0/1.27
 ip nat inside
 exit
line con 0
 logging synchronous
 exec-timeout 0 0
 exit
line vty 0 4
 login local
 transport input telnet
 exec-timeout 5 0
 exit
alias exec reset.now tclsh flash:/enarsi/reset.tcl
end
}
tclquit
```

! R3 - Trouble Ticket # 2

```
tclsh
puts [ open "flash:/enarsi/21.1.2.2-r3-config.txt" w+ ] {
hostname R3
no ip domain lookup
banner motd # This is R3, Trouble Ticket 21.1.2.2 #
enable secret cisco12345
```

```
username admin privilege 15 algorithm-type scrypt secret cisco12345
ip access-list standard BOGON-MARTIAN
 deny 10.0.0.0 0.255.255.255
 deny 172.16.0.0 0.31.255.255
 deny 192.168.0.0 0.0.255.255
 deny 127.0.0.0 0.255.255.255
 deny host 209.165.227.1
 deny host 209.165.228.1
 permit any
 exit
interface g0/0/1
 no ip address
 no shutdown
interface g0/0/1.16
 encapsulation dot1q 16
 ip address 10.0.16.1 255.255.255.0
 no shutdown
 exit
interface g0/0/1.27
 encapsulation dot1q 27
 ip address 10.0.27.1 255.255.255.0
 no shutdown
 exit
interface s0/1/0
 ip address 209.165.200.2 255.255.255.0
 ip access-group BOGON-MARTIAN in
 no shutdown
interface s0/1/1
 ip address 209.165.201.2 255.255.255.0
 ip access-group BOGON-MARTIAN in
 no shutdown
interface loopback 0
 ip address 209.165.227.1 255.255.255.255
 no shutdown
 exit
interface loopback 1
 ip address 209.165.228.1 255.255.255.255
 no shutdown
 exit
ip route 209.165.226.1 255.255.255.255 s0/1/0
ip route 209.165.226.1 255.255.255.255 s0/1/1
router bgp 39457
 bgp router-id 209.165.227.1
 neighbor 209.165.226.1 remote-as 181035
 neighbor 209.165.226.1 update-source loopback 0
```

```
 neighbor 209.165.226.1 ebgp-multihop 3
 network 209.165.228.1 mask 255.255.255.255
 exit
ip access-list standard NAT-ELIGIBLE
 permit 10.0.0.0 0.255.255.255
 deny any log
 exit
ip nat inside source list NAT-ELIGIBLE interface loopback 1 overload
ip dhcp excluded-address 10.0.16.1 10.0.16.5
ip dhcp excluded-address 10.0.27.1 10.0.27.5
ip dhcp pool NAT16
 network 10.0.16.0 255.255.255.0
 default-router 10.0.16.1
 exit
ip dhcp pool NAT27
 network 10.0.27.0 255.255.255.0
 default-router 10.0.27.1
 exit
interface s0/1/0
 ip nat outside
 exit
interface s0/1/1
 ip nat outside
 exit
interface g0/0/1.16
 ip nat inside
 exit
interface g0/0/1.27
 ip nat inside
 exit
line con 0
 logging synchronous
 exec-timeout 0 0
 exit
line vty 0 4
 login local
 transport input telnet
 exec-timeout 5 0
 exit
alias exec reset.now tclsh flash:/enarsi/reset.tcl
end
}
tclquit
```

! R3 - Trouble Ticket # 3

```
tclsh
```

```
puts [ open "flash:/enarsi/21.1.2.3-r3-config.txt" w+ ] {
hostname R3
no ip domain lookup
banner motd # This is R3, Trouble Ticket 21.1.2.3 #
enable secret cisco12345
username admin privilege 15 algorithm-type scrypt secret cisco12345
ip access-list standard BOGON-MARTIAN
 deny 10.0.0.0 0.255.255.255
 deny 172.16.0.0 0.31.255.255
 deny 192.168.0.0 0.0.255.255
 deny 127.0.0.0 0.255.255.255
 deny host 209.165.227.1
 deny host 209.165.228.1
 permit any
 exit
interface g0/0/1
 no ip address
 no shutdown
interface g0/0/1.16
 encapsulation dot1q 16
 ip address 10.0.16.1 255.255.255.0
 no shutdown
 exit
interface g0/0/1.27
 encapsulation dot1q 27
 ip address 10.0.27.1 255.255.255.0
 no shutdown
 exit
interface s0/1/0
 ip address 209.165.200.2 255.255.255.0
 ip access-group BOGON-MARTIAN in
 no shutdown
interface s0/1/1
 ip address 209.165.201.2 255.255.255.0
 ip access-group BOGON-MARTIAN in
 no shutdown
interface loopback 0
 ip address 209.165.227.1 255.255.255.255
 no shutdown
 exit
interface loopback 1
 ip address 209.165.228.1 255.255.255.255
 no shutdown
 exit
ip route 209.165.226.1 255.255.255.255 s0/1/0
```

```
ip route 209.165.226.1 255.255.255.255 s0/1/1
router bgp 39457
 bgp router-id 209.165.227.1
 neighbor 209.165.226.1 remote-as 181035
 neighbor 209.165.226.1 update-source loopback 0
 neighbor 209.165.226.1 ebgp-multihop 3
 network 209.165.228.1 mask 255.255.255.255
 exit
ip access-list standard NAT-ELIGIBLE
 permit 10.0.0.0 0.255.255.255
 deny any log
 exit
ip nat inside source list NAT-ELIGIBLE interface loopback 1 overload
ip dhcp excluded-address 10.0.16.1 10.0.16.5
ip dhcp excluded-address 10.0.27.1 10.0.27.5
ip dhcp pool NAT16
 network 10.0.16.0 255.255.255.0
 default-router 10.0.16.1
 exit
ip dhcp pool NAT27
 network 10.0.27.0 255.255.255.0
 default-router 10.0.27.1
 exit
interface s0/1/0
 ip nat outside
 exit
interface s0/1/1
 ip nat outside
 exit
interface g0/0/1.16
 ip nat inside
 exit
interface g0/0/1.27
 ip nat inside
 exit
line con 0
 logging synchronous
 exec-timeout 0 0
 exit
line vty 0 4
 login local
 transport input telnet
 exec-timeout 5 0
 exit
alias exec reset.now tclsh flash:/enarsi/reset.tcl
```

```
  end
  }
tclquit
```

D1 Configuration File Scripts

! D1 - Trouble Ticket # 1

```
tclsh
puts [ open "flash:/enarsi/21.1.2.1-d1-config.txt" w+ ] {
hostname D1
no ip domain lookup
ip routing
banner motd # This is D1, Trouble Ticket 21.1.2.1  #
enable secret cisco12345
username admin privilege 15 algorithm-type scrypt secret cisco12345
interface range g1/0/1-24
 switchport mode access
 shutdown
 exit
interface g1/0/11
 no switchport
 ip address 192.0.0.2 255.255.255.0
 no shutdown
 exit
interface vlan 11
 ip address 209.165.224.1 255.255.255.0
 no shutdown
 exit
interface vlan 12
 ip address 209.165.225.1 255.255.255.0
 no shutdown
 exit
interface g1/0/23
 switchport mode access
 switchport access vlan 11
 spanning-tree portfast
 no shutdown
 exit
interface g1/0/24
 switchport mode access
 switchport access vlan 12
 spanning-tree portfast
 no shutdown
 exit
router ospf 1
 router-id 131.131.131.131
```

```
  network 192.0.0.0 0.0.0.255 area 0
  network 209.165.224.0 0.0.1.255 area 0
  passive-interface vlan 11
  passive-interface vlan 12
  exit
 ip dhcp excluded-address 209.165.224.1 209.165.224.5
 ip dhcp excluded-address 209.165.225.1 209.165.225.5
 ip dhcp pool VLAN11
  network 209.165.224.0 255.255.255.0
  default-router 209.165.224.1
  exit
 ip dhcp pool VLAN12
  network 209.165.225.0 255.255.255.0
  default-router 209.165.225.1
  exit
 line con 0
  logging synchronous
  exec-timeout 0 0
  exit
 time-range REMOTE-CONTROL
  periodic weekdays 05:00 to 23:59
  periodic weekend 05:00 to 23:59
  exit
 ip access-list extended VTY-CONTROL
  permit ip 209.165.224.0 0.0.0.255 any time-range REMOTE-CONTROL
  deny ip any any log
  exit
 line vty 0 4
  login local
  transport input telnet
  exec-timeout 5 0
  access-class VTY-CONTROL in
  exit
 alias exec reset.now tclsh flash:/enarsi/reset.tcl
 end
 }
 tclquit
```

! D1 - Trouble Ticket # 2

```
 tclsh
 puts [ open "flash:/enarsi/21.1.2.2-d1-config.txt" w+ ] {
 hostname D1
 no ip domain lookup
 ip routing
 banner motd # This is D1, Trouble Ticket 21.1.2.2 #
 enable secret cisco12345
```

```
username admin privilege 15 algorithm-type scrypt secret cisco12345
interface range g1/0/1-24
 switchport mode access
 shutdown
 exit
interface g1/0/11
 no switchport
 ip address 192.0.0.2 255.255.255.0
 no shutdown
 exit
interface vlan 11
 ip address 209.165.224.1 255.255.255.0
 no shutdown
 exit
interface vlan 12
 ip address 209.165.225.1 255.255.255.0
 no shutdown
 exit
interface g1/0/23
 switchport mode access
 switchport access vlan 11
 spanning-tree portfast
 no shutdown
 exit
interface g1/0/24
 switchport mode access
 switchport access vlan 12
 spanning-tree portfast
 no shutdown
 exit
router ospf 1
 router-id 131.131.131.131
 network 192.0.0.0 0.0.0.255 area 0
 network 209.165.224.0 0.0.1.255 area 0
 passive-interface vlan 11
 passive-interface vlan 12
 exit
ip dhcp excluded-address 209.165.224.1 209.165.224.5
ip dhcp excluded-address 209.165.225.1 209.165.225.5
ip dhcp pool VLAN11
 network 209.165.224.0 255.255.255.0
 default-router 209.165.224.1
 exit
ip dhcp pool VLAN12
 network 209.165.225.0 255.255.255.0
```

```
  default-router 209.165.225.1
  exit
 line con 0
  logging synchronous
  exec-timeout 0 0
  exit
 time-range REMOTE-CONTROL
  periodic weekdays 05:00 to 23:59
  periodic weekend 05:00 to 23:59
  exit
 ip access-list extended VTY-CONTROL
  permit ip 209.165.224.0 0.0.0.255 any time-range REMOTE-CONTROL
  deny ip any any log
  exit
 line vty 0 4
  login local
  transport input telnet
  exec-timeout 5 0
  access-class VTY-CONTROL in
  exit
 alias exec reset.now tclsh flash:/enarsi/reset.tcl
 end
 }
 tclquit
```

! D1 - Trouble Ticket # 3

```
 tclsh
 puts [ open "flash:/enarsi/21.1.2.3-d1-config.txt" w+ ] {
 hostname D1
 no ip domain lookup
 ip routing
 banner motd # This is D1, Trouble Ticket 21.1.2.3 #
 enable secret cisco12345
 username admin privilege 15 algorithm-type scrypt secret cisco12345
 interface range g1/0/1-24
  switchport mode access
  shutdown
  exit
 interface g1/0/11
  no switchport
  ip address 192.0.0.2 255.255.255.0
  no shutdown
  exit
 interface vlan 11
  ip address 209.165.224.1 255.255.255.0
  no shutdown
```

```
 exit
interface vlan 12
 ip address 209.165.225.1 255.255.255.0
 no shutdown
 exit
interface g1/0/23
 switchport mode access
 switchport access vlan 11
 spanning-tree portfast
 no shutdown
 exit
interface g1/0/24
 switchport mode access
 switchport access vlan 12
 spanning-tree portfast
 no shutdown
 exit
router ospf 1
 router-id 131.131.131.131
 network 192.0.0.0 0.0.0.255 area 0
 network 209.165.224.0 0.0.1.255 area 0
 passive-interface vlan 11
 passive-interface vlan 12
 exit
ip dhcp excluded-address 209.165.224.1 209.165.224.5
ip dhcp excluded-address 209.165.225.1 209.165.225.5
ip dhcp pool VLAN11
 network 209.165.224.0 255.255.255.0
 default-router 209.165.224.1
 exit
ip dhcp pool VLAN12
 network 209.165.225.0 255.255.255.0
 default-router 209.165.225.1
 exit
line con 0
 logging synchronous
 exec-timeout 0 0
 exit
time-range REMOTE-CONTROL
 periodic weekdays 00:00 to 01:00
 periodic weekend 00:00 to 02:00
 exit
ip access-list extended VTY-CONTROL
 permit ip 209.165.224.0 0.0.0.255 any time-range REMOTE-CONTROL
 deny ip any any log
```

```
   exit
line vty 0 4
 login local
 transport input telnet
 exec-timeout 5 0
 access-class VTY-CONTROL in
 exit
alias exec reset.now tclsh flash:/enarsi/reset.tcl
end
}
tclquit
```

D2 Configuration File Scripts

! D2- Trouble Ticket # 1

```
tclsh
puts [ open "flash:/enarsi/21.1.2.1-d2-config.txt" w+ ] {
hostname D2
no ip domain lookup
ip routing
banner motd # This is D2, Trouble Ticket 21.1.2.1  #
enable secret cisco12345
username admin privilege 15 algorithm-type scrypt secret cisco12345
interface range g1/0/1-24
 switchport mode access
 shutdown
 exit
interface g1/0/11
 switchport mode trunk
 switchport nonegotiate
 no shutdown
 exit
interface g1/0/23
 switchport mode access
 switchport access vlan 16
 spanning-tree portfast
 no shutdown
 exit
interface g1/0/24
 switchport mode access
 switchport access vlan 27
 spanning-tree portfast
 no shutdown
 exit
interface vlan 16
 ip address 10.0.16.2 255.255.255.0
```

```
  no shutdown
  exit
interface vlan 27
 ip address 10.0.27.2 255.255.255.0
 no shutdown
 exit
ip default-gateway 10.0.27.1
line con 0
 logging synchronous
 exec-timeout 0 0
 exit
line vty 0 4
 login local
 transport input telnet
 exec-timeout 5 0
 exit
alias exec reset.now tclsh flash:/enarsi/reset.tcl
end
}
tclquit
```

! D2- Trouble Ticket # 2

```
tclsh
puts [ open "flash:/enarsi/21.1.2.2-d2-config.txt" w+ ] {
hostname D2
no ip domain lookup
ip routing
banner motd # This is D2, Trouble Ticket 21.1.2.2 #
enable secret cisco12345
username admin privilege 15 algorithm-type scrypt secret cisco12345
interface range g1/0/1-24
 switchport mode access
 shutdown
 exit
interface g1/0/11
 switchport mode trunk
 switchport nonegotiate
 no shutdown
 exit
interface g1/0/23
 switchport mode access
 switchport access vlan 16
 spanning-tree portfast
 no shutdown
 exit
interface g1/0/24
```

```
 switchport mode access
 switchport access vlan 27
 spanning-tree portfast
 no shutdown
 exit
interface vlan 27
 ip address 10.0.27.2 255.255.255.0
 no shutdown
 exit
ip default-gateway 10.0.27.1
line con 0
 logging synchronous
 exec-timeout 0 0
 exit
line vty 0 4
 login local
 transport input telnet
 exec-timeout 5 0
 exit
alias exec reset.now tclsh flash:/enarsi/reset.tcl
end
}
tclquit
```

! D2- Trouble Ticket # 3

```
tclsh
puts [ open "flash:/enarsi/21.1.2.3-d2-config.txt" w+ ] {
hostname D2
no ip domain lookup
ip routing
banner motd # This is D2, Trouble Ticket 21.1.2.3 #
enable secret cisco12345
username admin privilege 15 algorithm-type scrypt secret cisco12345
interface range g1/0/1-24
 switchport mode access
 shutdown
 exit
interface g1/0/11
 switchport mode trunk
 switchport nonegotiate
 no shutdown
 exit
interface g1/0/23
 switchport mode access
 switchport access vlan 16
 spanning-tree portfast
```

```
 no shutdown
 exit
interface g1/0/24
 switchport mode access
 switchport access vlan 27
 spanning-tree portfast
 no shutdown
 exit
interface vlan 27
 ip address 10.0.27.2 255.255.255.0
 no shutdown
 exit
ip default-gateway 10.0.27.1
line con 0
 logging synchronous
 exec-timeout 0 0
 exit
line vty 0 4
 login local
 transport input telnet
 exec-timeout 5 0
 exit
alias exec reset.now tclsh flash:/enarsi/reset.tcl
end
}
tclquit
```

A1 Configuration File Scripts - Not Used In This Lab