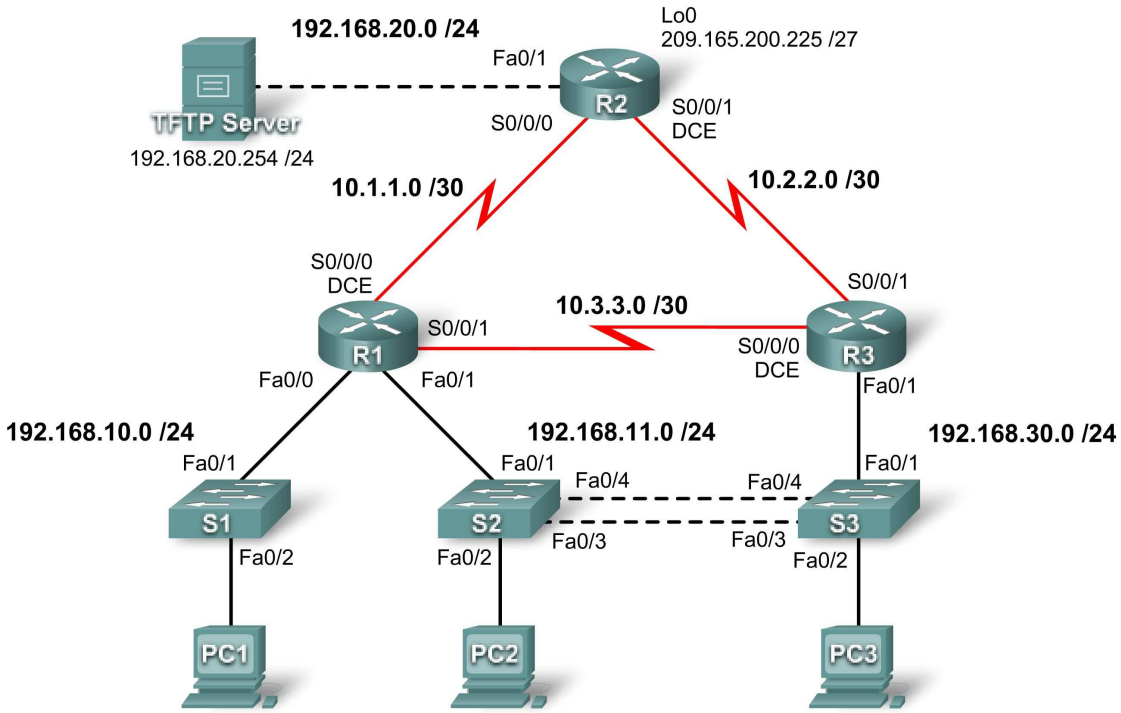
Lab 8.5.2: Troubleshooting Enterprise Networks 2

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.10.1	255.255.255.0	N/A
	Fa0/1	192.168.11.1	255.255.255.0	N/A
	S0/0	10.1.1.1	255.255.255.252	N/A
	S0/1	10.3.3.1	255.255.255.252	N/A
R2	Fa0/1	192.168.20.1	255.255.255.0	N/A
	S0/0	10.1.1.2	255.255.255.252	N/A
	S0/1	10.2.2.1	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	209.165.200.226
R3	Fa0/1	N/A	N/A	N/A
	Fa0/1.11	192.168.11.3	255.255.255.0	N/A
	Fa0/1.30	192.168.30.1	255.255.255.0	N/A
	S0/0	10.3.3.2	255.255.255.252	N/A
	S0/1	10.2.2.2	255.255.255.252	N/A
S1	VLAN10	DHCP		N/A
S2	VLAN11	192.168.11.2	255.255.255.0	N/A
S3	VLAN30	192.168.30.2	255.255.255.0	N/A
PC1	NIC	DHCP		
PC2	NIC	192.168.11.10	255.255.255.0	192.168.11.1

PC3	**NIC**	192.168.30.10	255.255.255.0	192.168.30.1
TFTP Server	**NIC**	192.168.20.254	255.255.255.0	192.168.20.1

Learning Objectives

Upon completion of this lab, you will be able to:

- Cable a network according to the topology diagram
- Erase the startup configuration and reload a router to the default state
- Load the routers and switches with supplied scripts
- Find and correct all network errors
- Document the corrected network

Scenario

For this lab, do not use login or password protection on any console lines to prevent accidental lockout. Use **ciscoccna** for all passwords in this lab.

Note: Because this lab is cumulative, you will be using all the knowledge and troubleshooting techniques that you have acquired from the previous material to successfully complete this lab.

Requirements

- S2 is the spanning-tree root for VLAN 11, and S3 is the spanning-tree root for VLAN 30.
- S3 is a VTP server with S2 as a client.
- The serial link between R1 and R2 is Frame Relay.
- The serial link between R2 and R3 uses HDLC encapsulation.
- The serial link between R1 and R3 is authenticated using CHAP.
- R2 must have secure login procedures because it is the Internet edge router.
- All vty lines, except those belonging to R2, allow connections only from the subnets shown in the topology diagram, excluding the public address.
- Source IP address spoofing should be prevented on all links that do not connect to other routers.
- Routing protocols must be used securely. EIGRP is used in this scenario.
- R3 must not be able to telnet to R2 through the directly connected serial link.
- R3 has access to both VLAN 11 and 30 via its Fast Ethernet port 0/1.
- The TFTP server should not get any traffic that has a source address outside the subnet. All devices have access to the TFTP server.
- All devices on the 192.168.10.0 subnet must be able to get their IP addresses from DHCP on R1. This includes S1.
- All addresses shown in diagram must be reachable from every device.

Task 1: Load Routers with the Supplied Scripts

```
!----------------------------------------
!                  R1
!----------------------------------------
no service password-encryption
!
hostname R1
!
```



```
boot-start-marker
boot-end-marker
!
security passwords min-length 6
enable secret ciscoccna
!
ip cef
!
ip dhcp pool Access1
   network 192.168.10.0 255.255.255.0
   default-router 192.168.10.1
!
no ip domain lookup
frame-relay switching
!
username R2 password ciscoccna
username ccna password ciscoccna
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 ip access-group Anti-spoofing out
 duplex auto
 speed auto
 no shutdown
!
interface FastEthernet0/1
 ip address 192.168.11.1 255.255.255.0
 duplex auto
 speed auto
 no shutdown
!
interface Serial0/0
 ip address 10.1.1.1 255.255.255.252
 encapsulation frame-relay
 no keepalive
 clockrate 128000
 frame-relay map ip 10.1.1.1 201
 frame-relay map ip 10.1.1.2 201 broadcast
 no frame-relay inverse-arp
 frame-relay intf-type dce
 no shutdown
!
interface Serial0/1
 ip address 10.3.3.1 255.255.255.0
 encapsulation ppp
 ppp authentication chap
 no shutdown
!
!
router eigrp 10
 passive-interface default
 no passive-interface FastEthernet0/0
 no passive-interface FastEthernet0/1
 no passive-interface Serial0/0
 no passive-interface Serial0/1
 network 10.1.1.0 0.0.0.255
```



```
 network 10.2.2.0 0.0.0.255
 network 192.168.10.0 0.0.0.255
 network 192.168.11.0 0.0.0.255
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 10.1.1.2
!
ip http server
!
ip access-list standard Anti-spoofing
 permit 192.168.10.0 0.0.0.255
 deny   any
ip access-list standard VTY
 permit 10.0.0.0 0.255.255.255
 permit 192.168.10.0 0.0.0.255
 permit 192.168.11.0 0.0.0.255
 permit 192.168.20.0 0.0.0.255
 permit 192.168.30.0 0.0.0.255
!
line con 0
 exec-timeout 5 0
 logging synchronous
line aux 0
line vty 0 4
 access-class VTY in
 login local
!
end
!----------------------------------------
!                  R2
!----------------------------------------
no service password-encryption
!
hostname R2
!
security passwords min-length 6
enable secret ciscoccna
!
aaa new-model
!
aaa authentication login local_auth local
aaa session-id common
!
ip cef
!
no ip domain lookup
!
username ccna password 0 ciscoccna
!
interface Loopback0
 ip address 209.165.200.225 255.255.255.224
 ip access-group private in
!
interface FastEthernet0/1
 ip address 192.168.20.1 255.255.255.0
 ip access-group TFTP out
```



```
 ip access-group Anti-spoofing in
 ip nat outside
 no shutdown
!
!
interface Serial0/0
 ip address 10.1.1.2 255.255.255.252
 ip nat inside
 encapsulation frame-relay
 no keepalive
 frame-relay map ip 10.1.1.1 201 broadcast
 frame-relay map ip 10.1.1.2 201
 no frame-relay inverse-arp
 no shutdown
!
interface Serial0/1
 ip address 10.2.2.1 255.255.255.252
 ip nat inside
 clockrate 128000
 no shutdown
!
!
router eigrp 100
passive-interface default
 no passive-interface FastEthernet0/1
 no passive-interface Serial0/0
 no passive-interface Serial0/1
 no passive interface lo0
 network 10.1.1.0 0.0.0.3
 network 10.2.2.0 0.0.0.3
 network 192.168.20.0 0.0.0.255
network 209.165.200.0 0.0.0.7
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 209.165.200.226
!
no ip http server
ip nat inside source list NAT interface FastEthernet0/0 overload
!
ip access-list standard Anti-spoofing
 permit 192.168.20.0 0.0.0.255
 deny   any
ip access-list standard NAT
 permit 10.0.0.0 0.255.255.255
 permit 192.168.0.0 0.0.255.255
ip access-list standard private
 deny   127.0.0.1
 deny   10.0.0.0 0.255.255.255
 deny   172.16.0.0 0.15.255.255
 deny   192.168.0.0 0.0.255.255
 permit any
!
ip access-list extended R3-telnet
 deny   tcp host 10.2.2.2 host 10.2.2.1 eq telnet
 deny   tcp host 10.3.3.2 host 10.2.2.1 eq telnet
 deny   tcp host 192.168.11.3 host 10.2.2.1 eq telnet
```



```
 deny   tcp host 192.168.30.1 host 10.2.2.1 eq telnet

!
ip access-list standard TFTP
 permit 192.168.20.0 0.0.0.255
!
control-plane
!
line con 0
 exec-timeout 5 0
 logging synchronous
line aux 0
 exec-timeout 15 0
 logging synchronous
 login authentication local_auth
 transport output telnet
line vty 0 4
 exec-timeout 15 0
 logging synchronous
 login authentication local_auth
 transport input telnet
!
end
!----------------------------------------
!                  R3
!----------------------------------------
no service password-encryption
!
hostname R3
!
security passwords min-length 6
!
no aaa new-model
!
ip cef
!
no ip domain lookup
!
username R1 password ciscoccna
username ccna password  ciscoccna
!
interface FastEthernet0/1
 no shutdown
!
interface FastEthernet0/1.11
 encapsulation dot1Q 11
 ip address 192.168.11.3 255.255.255.0
 no snmp trap link-status
!
interface FastEthernet0/1.30
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0
 ip access-group Anti-Spoofin in
  no shutdown
!
!
```



```
interface Serial0/0
 ip address 10.3.3.2 255.255.255.252
 encapsulation ppp
 ppp authentication pap
!
interface Serial0/1
 ip address 10.2.2.2 255.255.255.252
 no shutdown
!
router eigrp 10
 network 10.3.3.0 0.0.0.3
 network 10.2.2.0 0.0.0.3
 network 192.168.11.0 0.0.0.255
 network 192.168.30.0 0.0.0.255
 no auto-summary
!
ip classless
!
ip http server
!
ip access-list standard Anti-spoofing
 permit 192.168.30.0 0.0.0.255
 deny   any
ip access-list standard VTY
 permit 10.0.0.0 0.255.255.255
 permit 192.168.10.0 0.0.0.255
 permit 192.168.11.0 0.0.0.255
 permit 192.168.20.0 0.0.0.255
 permit 192.168.30.0 0.0.0.255
!
!
line con 0
 exec-timeout 5 0
 logging synchronous
line aux 0
 exec-timeout 15 0
 logging synchronous
line vty 0 4
 access-class VTY out
 exec-timeout 15 0
 logging synchronous
 login local
!
end
!----------------------------------------
!               S1
!----------------------------------------
no service password-encryption
!
hostname S1
!
security passwords min-length 6
enable secret ciscoccna
!
no aaa new-model
vtp domain CCNA_Troubleshooting
```



```
vtp mode transparent
vtp password ciscoccna
ip subnet-zero
!
no ip domain-lookup
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 10
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan10
 ip address dhcp
 no ip route-cache
!
ip default-gateway 192.168.10.1
ip http server
!
line con 0
 exec-timeout 5 0
 logging synchronous
line vty 0 4
 password ciscoccna
 login
line vty 5 15
 no login
!
end
!----------------------------------------
!                S2
!----------------------------------------
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname S2
!
security passwords min-length 6
enable secret ciscoccna
!
```



```
no aaa new-model
vtp domain CCNA_Troubleshooting
vtp mode Client
vtp password ciscoccna
ip subnet-zero
!
no ip domain-lookup
!
no file verify auto
!
spanning-tree mode mst
spanning-tree extend system-id
spanning-tree vlan 30 priority 4096
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
 switchport access vlan 11
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 11
 switchport mode access
!
interface FastEthernet0/3
 switchport trunk allowed vlan 11,30
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk allowed vlan 11,30
 switchport mode trunk
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan11
 ip address 192.168.11.2 255.255.255.0
 no ip route-cache
!
ip http server
!
control-plane
!
line con 0
 exec-timeout 5 0
 logging synchronous
line vty 0 4
 password ciscoccna
 login
line vty 5 15
 no login
!
end
!----------------------------------------
!               S3
```



```
!----------------------------------------
no service password-encryption
!
hostname S3
!
security passwords min-length 6
enable secret ciscoccna
!
no aaa new-model
vtp domain CCNA_Troubleshooting
vtp mode Server
vtp password ciscoccna
ip subnet-zero
!
no ip domain-lookup
!
no file verify auto
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 11 priority 4096
vlan internal allocation policy ascending
!
Vlan 11,30
!
interface FastEthernet0/1
 switchport trunk allowed vlan 11,30
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/3

 switchport trunk allowed vlan 11,30
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk allowed vlan 11,30
 switchport mode trunk
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan30
 ip address 192.168.30.2 255.255.255.0
 no ip route-cache
!
ip default-gateway 192.168.30.1
ip http server
!
line con 0
 exec-timeout 5 0
 logging synchronous
```



```
line vty 0 4
 password ciscoccna
 login
line vty 5 15
 no login
!
end
```

Task 2: Find and Correct All Network Errors

Task 3: Verify that Requirements Are Fully Met

Task 4: Document the Corrected Network

Task 5: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

