Cisco | Networking Academy®
Mind Wide Open™

Laboratório 8.5.2: Identificação e solução de problemas de rede da empresa 2

Diagrama de topologia

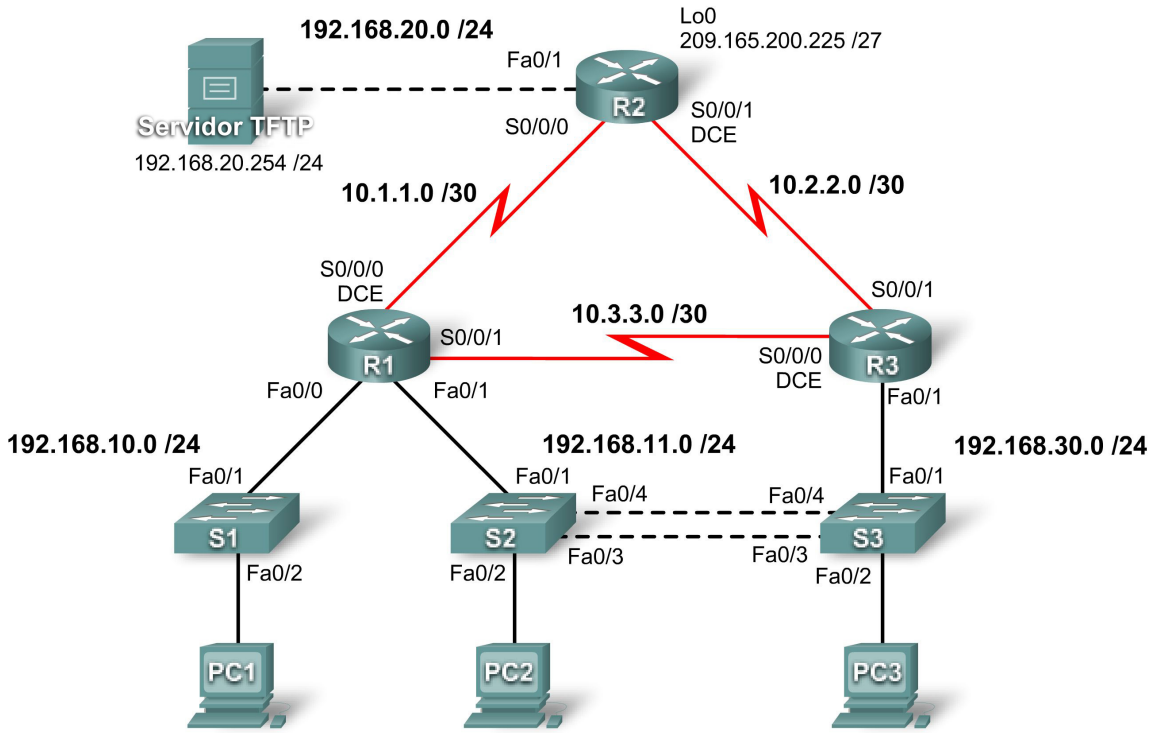

Tabela de endereçamento

Dispositivo	Interface	Endereço IP	Máscara de sub-rede	Gateway padrão
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
	S0/0/0	10.1.1.1	255.255.255.252	N/A
	S0/0/1	10.3.3.1	255.255.255.252	N/A
R2	**Fa0/1**	192.168.20.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	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
	S0/0/0	10.3.3.2	255.255.255.252	N/A
	S0/0/1	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	**Placa de rede**	DHCP		

All contents are Copyright © 1992–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

PC2	**Placa de rede**	192.168.11.10	255.255.255.0	192.168.11.1
PC3	**Placa de rede**	192.168.30.10	255.255.255.0	192.168.30.1
Servidor TFTP	**Placa de rede**	192.168.20.254	255.255.255.0	192.168.20.1

Objetivos de aprendizagem

Após concluir este laboratório, você será capaz de:

- Cabo de rede de acordo com o diagrama de topologia
- Apagar a configuração de inicialização e recarregar o estado padrão de um roteador
- Carregar os roteadores e os switches com scripts fornecidos
- Localizar e corrigir todos os erros de rede
- Documentar a rede corrigida

Cenário

Para este laboratório, não use a proteção por login ou senha em nenhuma linha de console para impedir o bloqueio acidental. Use **ciscoccna** para todas as senhas deste laboratório.

Nota: como este laboratório é cumulativo, você utilizará todo o conhecimento e as técnicas de identificação e solução de problemas aprendidas no material anterior para concluir este laboratório com êxito.

Requisitos

- S2 é a raiz de spanning tree para VLAN 11, e S3 é a raiz de spanning tree para VLAN 30.
- S3 é um servidor VTP com S2 como um cliente.
- O link serial entre R1 e R2 é Frame Relay.
- O link serial entre R2 e R3 usa encapsulamento HDLC.
- O link serial entre R1 e R3 é autenticado com o uso de CHAP.
- R2 deve ter procedimentos de login seguros por ser o roteador de extremidade da Internet.
- Todas as linhas vty, exceto as pertencentes a R2, só permitem conexões das sub-redes mostradas no diagrama de topologia, excluindo-se o endereço público.
- O spoofing do endereço IP de origem deve ser impedido em todos os links que não se conectam a outros roteadores.
- Os protocolos de roteamento devem ser usados com segurança. O EIGRP é usado neste cenário.
- R3 não deve ser capaz de executar telnet para R2 pelo link serial conectado diretamente.
- R3 tem acesso a VLANs 11 e 30 via porta Fast Ethernet 0/1.
- O servidor TFTP não deve obter nenhum tráfego que possua endereço de origem fora da sub-rede. Todos os dispositivos têm acesso ao servidor TFTP.
- Todos os dispositivos na sub-rede 192.168.10.0 devem ser capazes de obter os endereços IP de DHCP em R1. Isso inclui o S1.
- Todos os endereços mostrados no diagrama devem ser alcançáveis em todos os dispositivos.

All contents are Copyright © 1992–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Tarefa 1: Carregar os roteadores com os scripts fornecidos

```
!-----------------------------------------
!                  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 Serial0/0/0
 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 Serial0/0/1
 ip address 10.3.3.1 255.255.255.0
 encapsulation ppp
```

All contents are Copyright © 1992–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

```
 ppp authentication chap
 no shutdown
!
!
router eigrp 10
 passive-interface default
 no passive-interface FastEthernet0/0
 no passive-interface FastEthernet0/1
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
 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
```

All contents are Copyright © 1992–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

```
!
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 Serial0/0/0
 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 Serial0/0/1
 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 Serial0/0/0
 no passive-interface Serial0/0/1
 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
```

All contents are Copyright © 1992–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

```
 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
```

All contents are Copyright © 1992–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

```
 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 Serial0/0/0
 ip address 10.3.3.2 255.255.255.252
 encapsulation ppp
 ppp authentication pap
!
interface Serial0/0/1
 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
```

All contents are Copyright © 1992–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

```
 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 range FastEthernet0/3-24
!
interface GigabitEthernet0/1
 shutdown
!
interface GigabitEthernet0/2
 shutdown
!
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
```

All contents are Copyright © 1992–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

```
!
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
```

All contents are Copyright © 1992–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

```
!
interface range FastEthernet0/5-24
 shutdown
!
interface GigabitEthernet0/1
 shutdown
!
interface GigabitEthernet0/2
 shutdown
!
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
```

All contents are Copyright © 1992–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

```
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 range FastEthernet0/5-24
 shutdown
!
interface GigabitEthernet0/1
 shutdown
!
interface GigabitEthernet0/2
 shutdown
!
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
```

All contents are Copyright © 1992–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Tarefa 2: Localizar e corrigir todos erros de rede

Tarefa 3: Verificar se os requisitos foram totalmente atendidos

Tarefa 4: Documentar a rede corrigida

Tarefa 5: Limpar

Apague as configurações e recarregue os roteadores. Desconecte e guarde o cabeamento. Para hosts PC normalmente conectados a outras redes (como a LAN escolar ou a Internet), reconecte o cabeamento apropriado e restaure as configurações TCP/IP.

All contents are Copyright © 1992–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.