Atividade PT 2.4.6: Configurando a autenticação PAP e CHAP

Diagrama de topologia

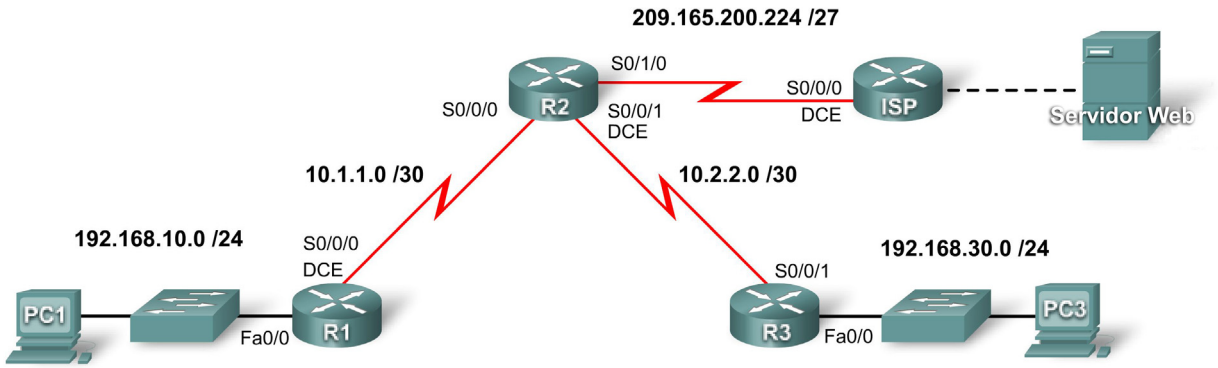

Tabela de endereçamento

Dispositivo	Interface	Endereço IP	Máscara de sub-rede
R1	Fa0/0	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.252
R2	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	255.255.255.252
R3	Fa0/0	192.168.30.1	255.255.255.0
	S0/0/0	10.2.2.2	255.255.255.252
ISP	S0/0/0	209.165.200.226	255.255.255.252
	Fa0/0	209.165.200.1	255.255.255.252
Servidor Web	Placa de rede	209.165.200.2	255.255.255.252
PC1	Placa de rede	192.168.10.10	255.255.255.0
PC3	Placa de rede	192.168.30.10	255.255.255.0

Objetivos de aprendizagem

- Configurar o roteamento OSPF.
- Configurar a autenticação PAP entre R1 e R2.
- Configurar a autenticação CHAP entre R3 e R2.

Introdução

O encapsulamento PPP permite dois tipos diferentes de autenticação: PAP (Password Authentication Protocol) e CHAP (Challenge Handshake Authentication Protocol). PAP utiliza uma senha em texto simples, e CHAP um hash unidirecional que fornece mais segurança que o PAP. Nesta atividade, você irá configurar PAP e CHAP e analisar a configuração de roteamento OSPF.

Tarefa 1: Configurar o roteamento OSPF

Etapa 1. Habilitar o OSPF em R1.

Com um *process-ID* **1**, utilize o comando **router ospf 1** para habilitar o roteamento OSPF.

Etapa 2. Configurar instruções de rede em R1.

No modo de configuração de roteador, adicione todas as redes conectadas a R1 utilizando o comando **network**. O parâmetro *area-id* OSPF é **0** para todas as instruções **network** desta topologia.

```
R1(config-router)#network 192.168.10.0 0.0.0.255 area 0
R1(config-router)#network 10.1.1.0 0.0.0.3 area 0
```

Etapa 3. Configurar as instruções network em R2 e R3.

Repita as etapas 1 e 2 para os roteadores R2 e R3. Utilize a tabela de endereçamento para determinar as instruções corretas. Em R2, *não* anuncie a rede 209.165.200.224/30. Você configurará uma rota padrão na próxima etapa.

Etapa 4. Estabelecer e redistribuir a rota padrão no OSPF.

- Em R2, crie uma rota estática padrão para ISP com o comando **ip route 0.0.0.0 0.0.0.0 s0/1/0**.
- No prompt do roteador, emita o comando **default-information originate** para incluir a rota estática nas atualizações OSPF enviadas de R2.

Etapa 5. Verificar a conectividade fim-a-fim.

A esta altura, na configuração, todos os dispositivos devem ser capazes de executar ping em todos os locais.

Clique em **Check results** e na guia **Connectivity Tests**. O status deve ser “Correct” para ambos os testes**.** As tabelas de roteamento de R1, R2 e R3 devem estar completas. R1 e R3 devem ter uma rota padrão, conforme mostrado na tabela de roteamento de R1 abaixo:

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
<saída do comando omitida>

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

     10.0.0.0/30 is subnetted, 2 subnets
C       10.1.1.0 is directly connected, Serial0/0/0
O       10.2.2.0 [110/128] via 10.1.1.2, 00:03:59, Serial0/0/0
C    192.168.10.0/24 is directly connected, FastEthernet0/0
O    192.168.30.0/24 [110/129] via 10.1.1.2, 00:02:19, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 10.1.1.2, 00:02:19, Serial0/0/0
```

Etapa 6. Verifique os resultados.

O percentual de conclusão deve ser 40%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 2: Configurar a autenticação PAP

Etapa 1. Configurar R1 para utilizar autenticação PAP com R2.

- Em R1, no modo de configuração global, digite o comando **username R2 password cisco123**. Esse comando permite ao roteador remoto, R2, se conectar a R1 durante a utilização da senha **cisco123**.
- Altere o tipo de encapsulamento na interface s0/0/0 de R1 para PPP utilizando o comando **encapsulation ppp**.
- Ainda na configuração da interface serial, configure a autenticação PAP com o comando **ppp authentication pap**.
- Configure o nome de usuário e a senha a serem enviados para R2 com o comando **ppp pap sent-username R1 password cisco123**. Embora o Packet Tracer não classifique o comando **ppp pap sent-username R1 password cisco123**, este é obrigatório para configurar com êxito uma autenticação PAP.
- Retorne ao modo exec privilegiado e utilize o comando **show ip interface brief** para observar se o link entre R1 e R2 já foi desativado.

```
R1(config)#username R2 password cisco123
R1(config)#interface s0/0/0
R1(config-if)#encapsulation ppp
R1(config-if)#ppp authentication pap
R1(config-if)#ppp pap sent-username R1 password cisco123
R1(config-if)#end
%SYS-5-CONFIG_I: Configured from console by console
R1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.10.1    YES manual up                    up
FastEthernet0/1        unassigned      YES manual administratively down down
Serial0/0/0            10.1.1.1        YES manual up                    down
Serial0/0/1            unassigned      YES manual administratively down
Vlan1                  unassigned      YES manual administratively down down
```

Etapa 2. Configurar R2 para utilizar a autenticação PAP com R1.

Repita a Etapa 1 para R2, usando o link serial para R1.

Lembre-se de que o nome utilizado no comando **username** *name* **password** *password* é sempre o nome
do roteador remoto, mas no comando **ppp pap sent-username** *name* **password** *password*, o nome é do roteador de origem.

Nota: embora o Packet Tracer ative o link, no equipamento real são necessários **shutdown** e **no shutdown** na interface para forçar a reautenticação do PAP. Você também pode simplesmente reiniciar os roteadores.

Etapa 3. Testar a conectividade entre o PC1 e o servidor Web.

Utilize o comando **show ip interface brief** para observar se o link entre R1 e R2 está ativado agora. Agora o acesso ao servidor Web de R1 deve ser restaurado. Testar enviando um ping do PC1 para o servidor Web.

```
R2#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES manual administratively down down
FastEthernet0/1        unassigned      YES manual administratively down down
Serial0/0/0            10.1.1.2        YES manual up                    up
Serial0/0/1            10.2.2.1        YES manual up                    up
Serial0/1/0            209.165.200.225 YES manual up                    up
Serial0/1/1            unassigned      YES manual administratively down down
Vlan1                  unassigned      YES manual administratively down down
```

Etapa 4. Verifique os resultados.

O percentual de conclusão deve ser de 70%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 3: Configurar a autenticação CHAP

Etapa 1. Configurar R3 para utilizar a autenticação CHAP com R2.

- No modo de configuração global de R3, digite **username R2 password cisco123**.
- Na interface s0/0/1, emita os comandos **encapsulation ppp** e **ppp authentication chap**, habilitando o encapsulamento PPP e a autenticação CHAP.
- Utilize o comando **show ip interface brief** para observar se o link entre R2 e R3 foi desativado.

```
R3(config)#username R2 password cisco123
R3(config)#interface s0/0/1
R3(config-if)#encapsulation ppp
R3(config-if)#ppp authentication chap
```

Etapa 2. Configurar R2 para utilizar a autenticação CHAP com R3.

Repita a Etapa 1 para R2, mas altere o nome de usuário para R3, porque R3 é o roteador remoto.

Etapa 3. Testar a conectividade entre o PC3 e o servidor Web.

Utilizando o comando **show ip interface brief**, você deve ver se o link entre R2 e R3 está ativado e se o PC3 pode executar ping no servidor Web.

Etapa 4. Verifique os resultados.

O percentual de conclusão deve ser de 100%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.