Atividade PT 4.3.2: Configurando a autenticação OSPF

Diagrama de topologia

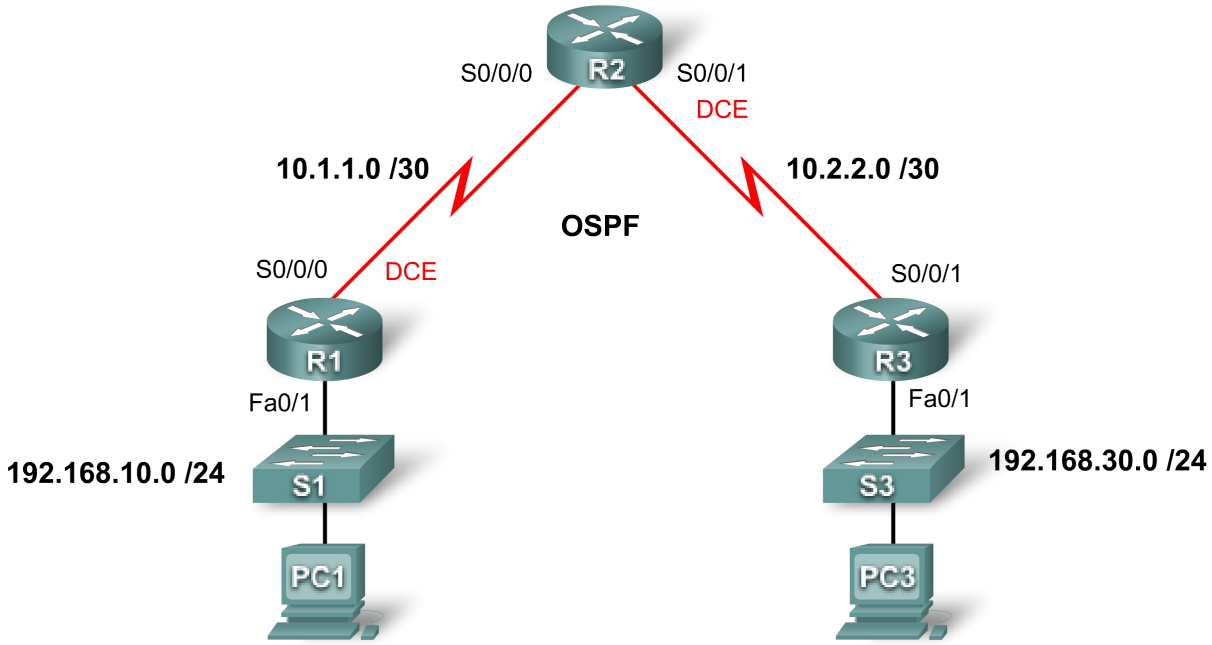

Tabela de endereçamento

Dispositivo	Interface	Endereço IP	Máscara de sub-rede
R1	**Fa0/1**	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
R3	**Fa0/1**	192.168.30.1	255.255.255.0
	S0/0/1	10.2.2.2	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

- Configure autenticação simples OSPF.
- Configurar autenticação OSPF MD5
- Testar conectividade.

Introdução

Esta atividade abrange a autenticação simples OSPF e a autenticação MD5 OSPF (resumo de mensagens 5). Você pode habilitar a autenticação em OSPF para trocar as informações sobre atualização de roteamento de uma maneira segura. Com autenticação simples, a senha é enviada em texto não criptografado pela rede. A autenticação simples é utilizada quando os dispositivos dentro de uma área não conseguem dar suporte à autenticação MD5 mais segura. Com autenticação de MD5, a senha não é enviada pela rede. MD5 é considerado o modo de autenticação OSPF mais seguro. Quando configurar a autenticação, você deve configurar uma área inteira com o mesmo tipo de autenticação. Nesta atividade, você irá configurar a autenticação simples entre R1 e R2 e a autenticação MD5 entre R2 e R3. Use as senhas **cisco** e **class** para acessar os modos de EXEC da CLI para roteadores.

Tarefa 1: Configurar autenticação simples OSPF

Etapa 1. Configurar R1 com autenticação simples OSPF.

Para habilitar a autenticação simples em R1, entre no modo de configuração do roteador utilizando o comando **router ospf 1** no prompt de configuração global. Em seguida, digite o comando **area 0 authentication** para habilitar a autenticação.

```
R1(config)#router ospf 1
R1(config-router)#area 0 authentication
00:02:30: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.1 on Serial0/0/0 from FULL to
DOWN, Neighbor Down: Dead timer expired
00:02:30: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.1 on Serial0/0/0 from FULL to
Down: Interface down or detached
```

Você acabará vendo uma mensagem de console com adjacência R2 desativada. R1 perde todas as rotas OSPF de sua tabela de roteamento até ser capaz de autenticar rotas com R2. Muito embora você ainda não tenha configurado uma senha, R1 está exigindo que os vizinhos utilizem autenticação em mensagens e atualizações de roteamento OSPF.

O comando **area 0 authentication** habilita a autenticação em todas as interfaces na área 0. Utilizar apenas esse comando funciona com R1, porque não precisa dar suporte a todos os outros tipos de autenticação.

Para configurar R1 com uma senha de autenticação simples, entre no modo de configuração da interface do link que se conecta a R2. Em seguida, utilize o comando **ip ospf authentication-key cisco123**. Esse comando define a senha de autenticação como **cisco123**.

```
R1(config-router)#interface S0/0/0
R1(config-if)#ip ospf authentication-key cisco123
```

Etapa 2. Configurar R2 com a autenticação simples OSPF.

Você configurou a autenticação em R1 para a área inteira. Como R2 dará suporte a autenticações simples e MD5, os comandos são digitados no nível da interface.

Entre no modo de configuração de interface de S0/0/0. Especifique que você está utilizando a autenticação simples com o comando **ip ospf authentication**. Em seguida, utilize o comando **ip ospf authentication-key cisco123** para definir a senha de autenticação como **cisco123**.

```
R2(config)#interface S0/0/0
R2(config-if)#ip ospf authentication
R2(config-if)#ip ospf authentication-key cisco123
00:07:45: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.1 on Serial0/0/0 from
EXCHANGE to FULL, Exchange Done
```


Quando concluir essas tarefas de configuração, você deverá ver uma mensagem da console indicando que a adjacência foi restabelecida entre R1 e R2. As rotas OSPF são reinstaladas na tabela de roteamento.

Etapa 3. Verifique os resultados.

O percentual de conclusão deve ser 50%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 2: Configurar autenticação OSPF MD5

Etapa 1. Configurar R3 com autenticação OSPF MD5.

Para habilitar a autenticação MD5 em R3, entre no modo de configuração do roteador utilizando o comando **router ospf 1** no prompt de configuração global. Em seguida, emita o comando **area 0 authentication message-digest** para habilitar a autenticação.

```
R3(config)#router ospf 1
R3(config-router)#area 0 authentication message-digest
00:10:00: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.1 on Serial0/0/1 from FULL to
DOWN, Neighbor Down: Dead timer expired
00:10:00: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.1 on Serial0/0/1 from FULL to
Down: Interface down or detached
```

Você acabará vendo uma mensagem de console com adjacência R2 desativada. R3 perde todas as rotas OSPF de sua tabela de roteamento até ser capaz de autenticar rotas com R2.

Para configurar R3 com a senha de autenticação MD5, entre no modo de configuração da interface do link que se conecta a R2. Em seguida, utilize o comando **ip ospf message-digest-key 1 md5 cisco123**. Esse comando define a senha de autenticação OSPF como **cisco123**, protegida com o algoritmo MD5.

```
R3(config-router)#interface S0/0/1
R3(config-if)#ip ospf message-digest-key 1 md5 cisco123
```

Etapa 2. Configurar R2 com autenticação OSPF MD5.

Em R2, entre no modo de configuração da interface do link que se conecta a R3. Digite o comando **ip ospf authentication message-digest** para habilitar a autenticação MD5. Esse comando é necessário em R2 porque esse roteador está utilizando dois tipos de autenticação.

Em seguida, emita o comando **ip ospf message-digest-key 1 md5 cisco123** para definir a senha de autenticação como **cisco123**.

```
R2(config)#interface S0/0/1
R2(config-if)#ip ospf authentication message-digest
R2(config-if)#ip ospf message-digest-key 1 md5 cisco123
00:13:51: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on Serial0/0/1 from
EXCHANGE to FULL, Exchange Done
```

Depois de inserir esse comando, aguarde um momento até que os roteadores possam convergir. Você deve ver uma mensagem da console em R2 e R3 indicando que a adjacência do vizinho foi restabelecida. Você pode confirmar se R2 reinstalou as rotas OSPF e se R2 tem R3 como um vizinho OSPF.

```
R2#show ip route
<saída do comando omitida>

Gateway of last resort is not set
```



```
     10.0.0.0/30 is subnetted, 2 subnets
C       10.1.1.0 is directly connected, Serial0/0/0
C       10.2.2.0 is directly connected, Serial0/0/1
O    192.168.10.0/24 [110/65] via 10.1.1.1, 00:06:13, Serial0/0/0
O    192.168.30.0/24 [110/65] via 10.2.2.2, 00:00:07, Serial0/0/1

R2#show ip ospf neighbor
Neighbor ID     Pri   State           Dead time   Address         Interface
192.168.10.1      1   FULL/-          00:00:32    10.1.1.1        Serial0/0/0
192.168.30.1      1   FULL/-          00:00:37    10.2.2.2        Serial0/0/1
```

Etapa 3. Verifique os resultados.

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

Tarefa 3: Testar conectividade

Agora a autenticação deve ser configurada corretamente em todos os três roteadores, logo PC1 não deve ter nenhuma dificuldade na execução de ping em PC3. Clique em **Check Results** e em **Connectivity Tests** para ver se há êxito.

