Exercice PT 4.3.2 : configuration de l'authentification OSPF

Diagramme de topologie

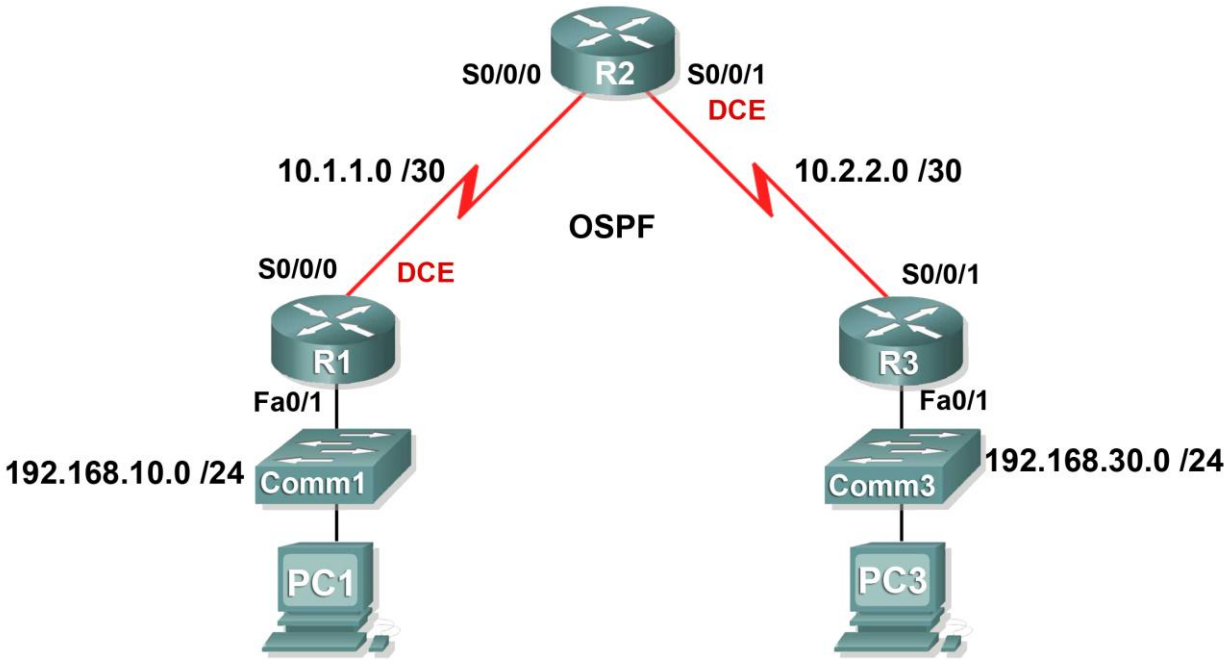

Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau
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	**Carte réseau**	192.168.10.10	255.255.255.0
PC3	**Carte réseau**	192.168.30.10	255.255.255.0

Objectifs pédagogiques

- Configurer une authentification simple OSPF
- Configurer une authentification MD5 OSPF
- Tester la connectivité

Présentation

Cet exercice porte sur l'authentification simple OSPF et sur l'authentification MD5 (message digest 5) OSPF. Vous pouvez activer l'authentification dans OSPF pour échanger des informations de mise à jour du routage de manière sécurisée. Si vous configurez une authentification simple, le mot de passe est envoyé sur le réseau sous forme de texte en clair. L'authentification simple est utilisée lorsque les périphériques d'une zone ne prennent pas en charge l'authentification MD5, qui est plus sûre. Si vous configurez une authentification MD5, le mot de passe n'est pas envoyé sur le réseau. MD5 est considéré comme le mode d'authentification OSPF le plus sûr. Lorsque vous configurez l'authentification, vous devez utiliser le même type d'authentification pour l'intégralité de la zone. Dans cet exercice, vous allez configurer une authentification simple entre R1 et R2, puis une authentification MD5 entre R2 et R3.

Tâche 1 : configuration d'une authentification simple OSPF

Étape 1. Configuration d'une authentification simple OSPF sur R1

Pour activer une authentification simple sur R1, passez en mode de configuration du routeur à l'aide de la commande **router ospf 1** à l'invite de configuration globale. Envoyez ensuite la commande **area 0 authentication** pour activer l'authentification.

```
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
```

Finalement, un message s'affiche et indique que la contiguïté avec R2 est désactivée. R1 perd toutes les routes OSPF de sa table de routage jusqu'à ce qu'il parvienne à authentifier les routes avec R2. Bien que vous n'ayez pas encore configuré de mot de passe, R1 demande à ses voisins d'utiliser l'authentification dans les mises à jour et les messages de routage OSPF.

La commande **area 0 authentication** active l'authentification pour toutes les interfaces de la zone 0. Cette commande est suffisante pour R1, car il n'a pas besoin de prendre en charge d'autre type d'authentification.

Pour configurer R1 avec un mot de passe d'authentification simple, passez en mode de configuration d'interface pour la liaison avec R2. Envoyez alors la commande **ip ospf authentication-key cisco123**. Cette commande définit le mot de passe d'authentification **cisco123**.

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

Étape 2. Configuration d'une authentification simple OSPF sur R2

Vous avez configuré l'authentification sur R1 pour toute la zone. R2 pouvant prendre en charge à la fois l'authentification simple et l'authentification MD5, les commandes sont saisies au niveau de l'interface.

Passez en mode de configuration d'interface pour S0/0/0. Précisez que vous utilisez une authentification simple à l'aide de la commande **ip ospf authentication**. Envoyez alors la commande **ip ospf authentication-key cisco123** pour définir le mot de passe d'authentification **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
```

Une fois ces tâches de configuration terminées, vous devez finalement voir un message indiquant que la contiguïté est rétablie entre R1 et R2. Les routes OSPF sont réinstallées dans la table de routage.

Étape 3. Vérification des résultats

Votre taux de réalisation doit être de 50 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 2 : configuration d'une authentification MD5 OSPF

Étape 1. Configuration d'une authentification MD5 OSPF sur R3

Pour activer une authentification MD5 sur R3, passez en mode de configuration du routeur à l'aide de la commande **router ospf 1** à l'invite de configuration globale. Envoyez ensuite la commande **area 0 authentication message-digest** pour activer l'authentification.

```
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
```

Finalement, un message s'affiche et indique que la contiguïté avec R2 est désactivée. R3 perd toutes les routes OSPF de sa table de routage jusqu'à ce qu'il parvienne à authentifier les routes avec R2.

Pour configurer R3 avec le mot de passe d'authentification MD5, passez en mode de configuration d'interface pour la liaison avec R2. Envoyez alors la commande **ip ospf message-digest-key 1 md5 cisco123**. Cette commande définit le mot de passe d'authentification OSPF **cisco123**, protégé par l'algorithme MD5.

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

Étape 2. Configuration d'une authentification MD5 OSPF sur R2

Sur R2, passez en mode de configuration d'interface pour la liaison avec R3. Envoyez la commande **ip ospf authentication message-digest** pour activer l'authentification MD5. Cette commande est nécessaire sur R2 car ce routeur utilise deux types d'authentification.

Envoyez alors la commande **ip ospf message-digest-key 1 md5 cisco123** pour définir le mot de passe d'authentification.

```
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
```

Après l'envoi de cette commande, attendez quelques instants que les routeurs convergent. Vous devez voir un message sur R2 et R3 indiquant que la contiguïté de voisins est rétablie. Vous pouvez confirmer que R2 a réinstallé les routes OSPF et que R3 est un voisin OSPF de R2.

```
R2#show ip route
<résultat omis>

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
```

Étape 3. Vérification des résultats

Votre taux de réalisation doit être de 100 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 3 : test de la connectivité

L'authentification doit maintenant être correctement configurée sur les trois routeurs. Par conséquent, PC1 doit maintenant être en mesure d'envoyer une requête ping à PC3. Cliquez sur **Check Results**, puis sur **Connectivity Tests** pour voir si cela fonctionne.