Exercice PT 2.4.6 : configuration de l'authentification PAP et CHAP

Diagramme de topologie

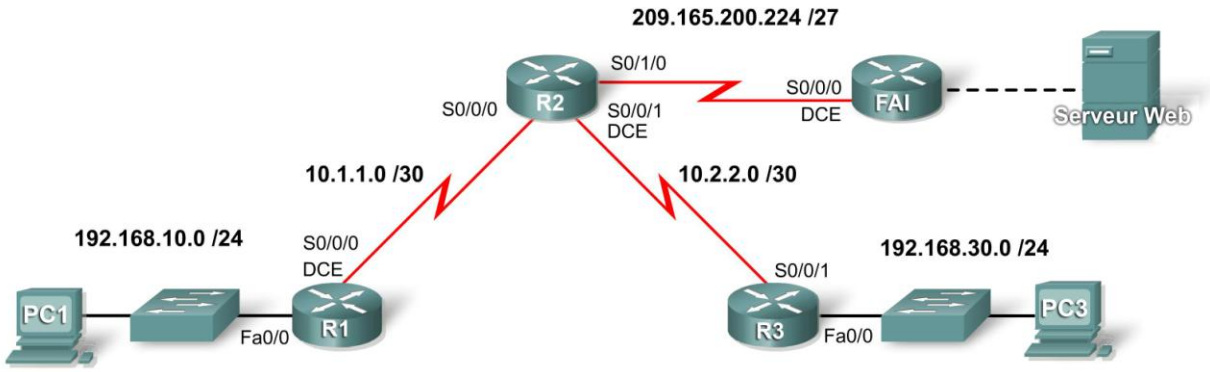

Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau
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
FAI	S0/0/0	209.165.200.226	255.255.255.252
	Fa0/0	209.165.200.1	255.255.255.252
Serveur Web	Carte réseau	209.165.200.2	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 le routage OSPF
- Configurer l'authentification PAP entre R1 et R2
- Configurer l'authentification CHAP entre R3 et R2

Présentation

L'encapsulation PPP permet deux types d'authentification différents : PAP (Password Authentication Protocol ou protocole d'authentification du mot de passe) et CHAP (Challenge Handshake Authentication Protocol ou protocole d'authentification à échanges confirmés). PAP utilise un mot de passe sous forme de texte en clair, tandis que CHAP fait appel à une empreinte numérique à sens unique qui offre plus de sécurité que PAP. Au cours de cet exercice, vous allez configurer à la fois les types PAP et CHAP et examiner la configuration de routage OSPF.

Tâche 1 : configuration du routage OSPF

Étape 1 : activation du protocole OSPF sur R1

Avec un paramètre *process-ID* de **1**, activez le routage OSPF à l'aide de la commande **router ospf 1**.

Étape 2 : configuration des instructions réseau sur R1

En mode de configuration du routeur, ajoutez tous les réseaux connectés à R1 à l'aide de la commande **network**. Le paramètre *area-id* OSPF est de **0** pour toutes les instructions **network** dans cette topologie.

```
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
```

Étape 3 : configuration des instructions réseau sur R2 et R3

Répétez les étapes 1 et 2 pour les routeurs R2 et R3. Consultez la table d'adressage pour déterminer les instructions correctes. Sur R2, n'annoncez *pas* le réseau 209.165.202.224/30. Vous allez configurer une route par défaut à la prochaine étape.

Étape 4 : définition et redistribution de la route par défaut OSPF

- Sur R2, créez une route statique par défaut vers FAI à l'aide de la commande **ip route 0.0.0.0 0.0.0.0 s0/1/0**.
- À l'invite du routeur, envoyez la commande **default-information originate** pour inclure la route statique dans les mises à jour OSPF envoyées depuis R2.

Étape 5 : vérification de la connectivité de bout en bout

À ce stade de la configuration, tous les périphériques doivent être en mesure d'envoyer des requêtes ping vers tous les emplacements.

Cliquez sur **Check Results**, puis cliquez sur l'onglet **Connectivity Tests**. L'état doit avoir la valeur « correct » pour les deux tests. Les tables de routage de R1, R2 et R3 doivent être complètes. R1 et R3 doivent avoir une route par défaut comme indiqué dans la table de routage de R1 ci-dessous :

```
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
<résultat omis>

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
```

Étape 6 : vérification des résultats

Votre taux de réalisation doit être de 40 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 2 : configuration de l'authentification PAP

Étape 1 : configuration de R1 pour utiliser l'authentification PAP avec R2

- Sur R1 en mode de configuration globale, entrez la commande **username R2 password cisco123**. Cette commande permet au routeur distant R2 de se connecter à R1 en utilisant le mot de passe **cisco123.**
- Modifiez le type d'encapsulation en PPP sur l'interface s0/0/0 de R1 à l'aide de la commande **encapsulation ppp**.
- Sur l'interface série, configurez l'authentification PAP à l'aide de la commande **ppp authentication pap**.
- Configurez le nom d'utilisateur et le mot de passe qui seront envoyés à R2 à l'aide de la commande **ppp pap sent-username R1 password cisco123**. Packet Tracer n'évalue pas la commande **ppp pap sent-username R1 password cisco123** mais celle-ci est nécessaire pour configurer l'authentification PAP.
- Revenez en mode d'exécution privilégié et lancez la commande **show ip interface brief** pour remarquer que la liaison entre R1 et R2 s'est désactivée.

```
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 down
Vlan1                  unassigned      YES manual administratively down down
```

Étape 2 : configuration de R2 pour utiliser l'authentification PAP avec R1

Répétez l'étape 1 pour R2, en utilisant la liaison série vers R1.

N'oubliez pas que le nom utilisé dans la commande **username** *nom* **password** *motdepasse* est toujours le nom du routeur distant, alors que dans la commande **ppp pap sent-username** *nom* **password** *motdepasse*, il s'agit du nom du routeur source.

Remarque : Packet Tracer active la liaison, mais sur un équipement réel vous devez utiliser les commandes **shutdown** puis **no shutdown** sur l'interface pour forcer une nouvelle authentification de PAP. Vous pouvez aussi simplement recharger les routeurs.

Étape 3 : test de la connectivité entre PC1 et le serveur Web

Lancez la commande **show ip interface brief** pour voir que la liaison entre R1 et R2 est maintenant activée. L'accès au serveur Web à partir de R1 doit maintenant être rétabli. Pour le tester, envoyez un paquet ping de PC1 au serveur 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
```

Étape 4 : vérification des résultats

Votre taux de réalisation doit être de 70 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 3 : configuration de l'authentification CHAP

Étape 1 : configuration de R3 pour utiliser l'authentification CHAP avec R2

- En mode de configuration globale pour R3, entrez la commande **username R2 password cisco123**.
- Sur l'interface s0/0/1, lancez les commandes **encapsulation ppp** et **ppp authentication chap**, ce qui permet d'activer l'encapsulation PPP et l'authentification CHAP.
- Lancez la commande **show ip interface brief** pour voir que la liaison entre R2 et R3 s'est désactivée.

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

Étape 2 : configuration de R2 pour utiliser l'authentification CHAP avec R3

Répétez l'étape 1 utilisée pour R2, en changeant le nom en R3, puisque R3 est le routeur distant.

Étape 3 : test de la connectivité entre PC3 et le serveur Web

À l'aide de la commande **show ip interface brief**, vous pouvez voir que la liaison entre R2 et R3 est maintenant activée et que PC3 peut envoyer une requête ping au serveur Web.

Étape 4 : 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.