Etude du protocole OSPF

Authentification de l'échange des tables

ACL

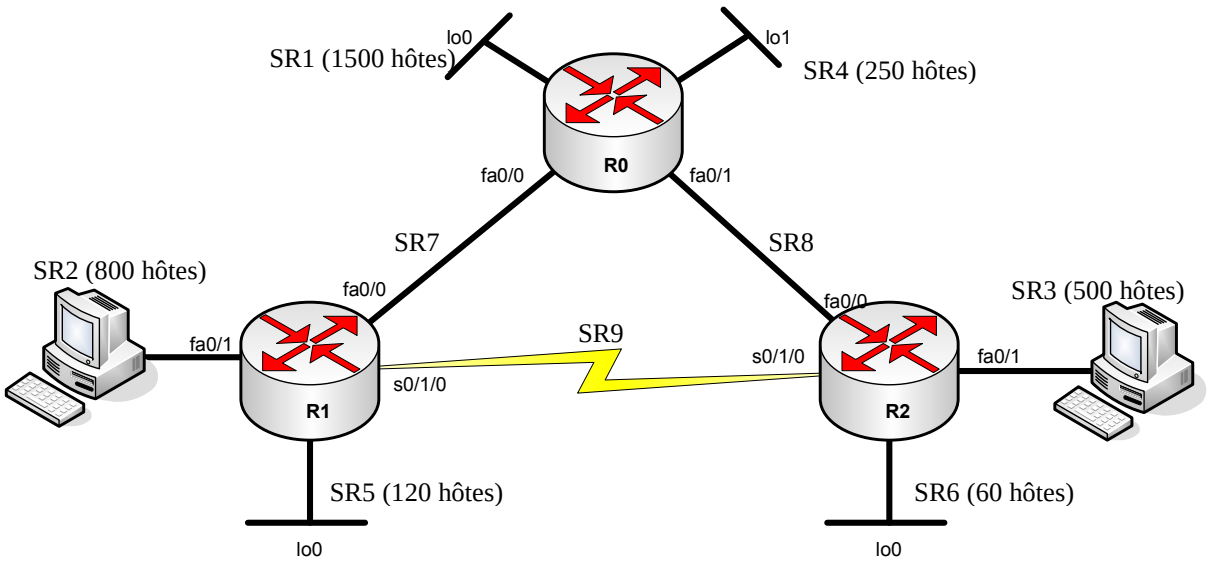
1 Subnetting

Soit l'adresse réseau 139.124.16.0/20. Vous devez découper cet espace pour satisfaire les besoins suivants :

	Nb Hôtes	@ réseaux	masque
SR1	1500		
SR2	800		
SR3	500		
SR4	250		
SR5	120		
SR6	60		
SR7	2		
SR8	2		
SR9	2		

2 Topologie et configuration de base

La topologie à mettre en œuvre est la suivante :



avec pour le plan d'adressage (où SRn.m désigne la m^{ième} adresse dans le sous-réseau n):

Équipement	**Fa0/0**	**Fa0/1**	**Loopack 0**	**Loopack 1**	**S0/1/0**
R0	SR7.1	SR8.1	SR1.1	SR4.1	
R1	SR7.2	SR2.1	SR5.1		SR9.1
R2	SR8.2	SR3.1	SR6.1		SR9.2
PC1	SR2.10				
PC2	SR3.10				

.

AVANT DE CONTINUER, ASSUREZ VOUS QUE TOUTES LES INTERFACES SOIENT UP !!!!

3 Prévisions d'OSPF

Pour chaque routeur déterminer l'identifiant qu'il aura dans le processus OSPF ?

Nom du routeur	ID OSPF
R0	
R1	
R2	

Complétez ce tableau en indiquant pour les réseaux ci-dessous quel routeur devrait être le DR et le BDR.

	DR	BDR
Entre R1-R0		
Entre R2-R0		
Entre R1 et R2		

4 Configuration d'OSPF

ATTENTION DE NE PAS ENCORE CONFIGURER OSPF SUR R1 et R2 !

Configurez le routage OSPF sur `R0.`

Au bout de quelques instants (un peu plus de 40 s), au moyen de la commande `sh ip ospf interface`, indiquez pour chaque interface de R0 son état ?

R0	DR	BDR
Fa0/0		
Fa0/1		

Configurez maintenant le routage OSPF sur les routeurs R1 et R2.

Une fois l'adjacence créée, au moyen des commandes `sh ip ospf interface` et `sh ip ospf neighbor`, indiquez pour les réseaux ci-dessous quel routeur fait office de DR et de BDR ?

Segment Ethernet	DR	BDR
Entre R1-R0		
Entre R2-R0		

Ces résultats sont-ils conformes à ce que vous aviez prévu à l'étape 3 sur les prévisions OSPF ?
Pourquoi ?

5 Trucage des élections

Nous allons faire en sorte maintenant que `R1` et `R2` soient toujours DR. Pour cela, au moyen de la commande `ip ospf priority`, attribuer à leurs interfaces fa0/0 les priorités `100` et `200`.

Sur `R1` et `R2`, au moyen des commandes `sh ip ospf interface` et `sh ip ospf neighbor`, complétez le tableau ci-dessous ?

Segment Ethernet	DR	BDR
Lien R0 - R1		
Lien R0 – R2		

Dans la table de voisins de `R0`, la priorité associée à ses voisins a-t-elle été modifiée ?

Les routeurs `R1` et `R2` ont-ils pour autant changé de statut (DR ou BDR) ?

Pourquoi ?

Nous allons maintenant provoquer une réélecrion. Pour cela, en même temps sur les trois routeurs, utilisez la commande `clear ip ospf process` (n'oublier pas de répondre `yes` à la question posée).

Au moyen des commandes `sh ip ospf interface` et `sh ip ospf neighbor`, indiquez pour les réseaux ci-dessous quel routeur fait office de DR et de BDR ?

Segment Ethernet	DR	BDR
Lien R1 – R0		
Lien R2 – R0		

Ces résultats sont-ils enfin conformes aux prévisions ?

6 Redistribution de routes

Définissez sur `R2`, l'interface de `loopback0` comme la route par défaut, puis propager cette route par défaut à l'ensemble de la zone OSPF.

Quel est le préfixe de la route par défaut dans la table de routage de `R2` ?

Quel est le préfixe de la route par défaut dans la table de routage de `R0` et `R1` ?

7 Equilibrage de charge

Examiner la table de routage de R0.

Quel chemin est emprunté pour atteindre le réseau SR9 ?

Que se passera-t-il si l'on fait un ping depuis R0 pour atteindre l'adresse 139.124.31.201 ?

8 Modification des timers

Sur les routeurs `R1` et `R2`, trouvez pour l'interface `fa0/1` la valeur des compteurs `Hello` et `Dead` (utiliser pour la commande `sh ip ospf interface fa0/0`).

Valeur du compteur Hello :

Valeur du compteur Dead :

Quelles sont les valeurs de ces deux compteurs sur une ligne série ?

Hello :
Dead :

Modifier ensuite, ces valeurs en les doublant (utiliser la commande `(config-if)#ip ospf`)

Que se passe t-il ? Pourquoi ?

Modifier sur R0 de telle sorte que le problème soir résolu.

9 Authentification de l'échange des tables de routage

La configuration de l'authentification de l'échange des tables de routage se fait en deux étapes

1. Configuration d'une clef d'échange ;
2. L'activation de l'authentification utilisant la clef d'échange.

9.1 Configuration de la clef d'échange

La configuration de la clef d'échange se fait sur les interfaces que l'on souhaite sécuriser (attention donc, les deux routeurs en vis-à-vis devront utiliser la même clef).

Ici vous commencerez par le routeur R0. Pour cela, sur l'interface fa0/0, entrez la commande :

```
(config-if)# ip ospf message-digest-key 1 md5 nemesis
```

indiquant que nous utiliserons pour l'authentification la chaîne "nemesis" cryptée via md5

Puis sur l'interface fa0/1, entrez la commande :

```
(config-if)# ip ospf message-digest-key 1 md5 invidia
```

indiquant que nous utiliserons pour l'authentification la chaîne "invidia" cryptée via md5

9.2 Activation de l'authentification

L'activation de l'authentification se fait dans le processus de routage en indiquant qu'une authentification sera utilisée pour la zone de backbone.

```
(config-router)#area 0 authentication message-digest
```

Que se passe-t-il au bout de quelques temps sur R1 et R2 ?

9.3 Configuration de l'authentification sur R1 et R2

Corriger le problème précédant en activant l'authentification sur R1 et R2.

10 ACL

Votre RSSI ne veux plus voir sur le réseau d'autres flux que les flux TCP. Pour cela, il opte pour une politique de découragement des utilisateurs, et vous demande donc d'autoriser uniquement les flux TCP à entrer par les interfaces de liaisons entre vos routeurs (tout autre trafic étant interdit).

Sur chacun de vos routeurs, mettez en place les ACLs nécessaires à l'application de cette politique de sécurité.

N'oubliez pas de tester votre ACL[1].

[1] et de regarder vos tables de routage !