

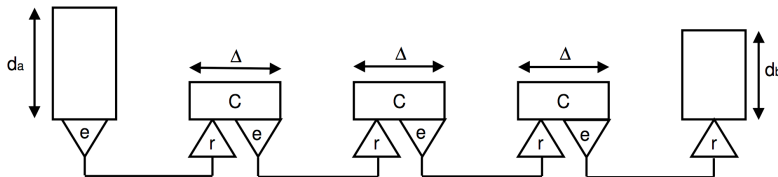
Objectif

Dans ce TD, nous allons discuter différents aspects liés à l'administration du réseau notamment : l'interconnexion, les VLAN, le routage statique et l'adressage ainsi que le routage dynamique à travers les protocoles RIP et OSPF. Vous disposez d'une partie annexe qui pourra vous servir à répondre aux différentes questions.

I. Interconnexion

1. On souhaite interconnecter deux réseaux locaux (LAN). Le premier LAN de type 802.3 (Ethernet) est composé d'une seule machine sous Windows et un commutateur (switch). Le deuxième LAN de type 802.5 (TokenRing) est composé d'une machine sous Mac OS X et un routeur. Dessiner avec précision la pile protocolaire de tout le matériel utilisé dans cette interconnexion (équipement et câbles).

2. Soit une voie de communication (un câblage) entre deux machines A et B mise en œuvre par un assemblage linéaire de 4 voies de communication V_1, V_2, V_3, V_4 (voir Figure ci-dessous). Les voies sont donc interconnectées deux à deux par des switch : C_1, C_2, \dots , etc. qui reçoivent l'intégralité d'une trame avant de la transmettre. Soit Δ le délai de transit d'un switch (délais que mets 1 paquet pour passer l'équipement). Les machines A et B ont un temps de traitement des paquets de données respectivement de d_A et d_B (d_a et d_b dans la Figure). Dans chaque machine, tous les traitements s'effectuent en parallèle. Le débit des voies de communication est D . Soit L la longueur des paquets échangés en bit. On négligera les délais de propagation ;



2.a. Quels sont les processus impliqués dans l'échange entre A et B qui peuvent se dérouler en parallèle ?

2.b. Déterminer le délai d'acheminement entre A et B ?

2.c. Quels sont les débits possibles sur les tronçons suivants (l'indice d'un switch étant son ordre de gauche à droite):

- A, C_1
- C_1, C_2
- C_2, C_3
- C_3, B

2.d. même question que la précédente, en supposant qu'il y a un contrôle de flux. Un mécanisme de contrôle de flux permet de limiter le débit de l'émetteur à ce que la voie de communication ou le récepteur est capable de recevoir.

2.e. Quel est le débit possible entre A et B ?

2.f. Avec l'application numérique suivante, déterminer le graphe du débit utilisateur entre A et B en fonction de L et paramétré par Δ :

- $L = 64$ à 1518 octets
- $D = 10 \text{ Mb/s}$
- $\Delta = d_A = d_B \in \{40\mu\text{s}, 1\text{ms}, 10\text{ms}\}$

2.g. Une technique de commutation rapide permet de commencer la commutation avant d'avoir stocké toute la trame. Seule une portion (entête) du message (correspondant au champ d'adresse) est analysée. On suppose que cette fraction du message est de longueur $l \leq L$ bits.

2.g.1. Quel est le délai d'acheminement entre A et B ?

2.g.2. Quels sont les débits utilisateurs ?

2.g.3. Quel est l'avantage de cette technique ?

II. VLAN

1. Citer 3 avantages de l'utilisation des VLANs dans un LAN. Donner à chaque fois un exemple pour montrer comment les VLANs permettent de réaliser l'avantage cité.

2. Rappeler le principe de la configuration statique des VLAN. Dans une telle configuration, peut-il y avoir des ports spéciaux ?

3. Quelle est l'utilité du protocole 802.1Q (VLAN tagging) ?

4. Pourquoi est-il plus difficile d'attaquer un réseau appartenant à un VLAN ? Donnez un exemple d'attaque possible sur un VLAN.

5. Les administrateurs du service informatique de l'ISTIC ont défini, entre autres, 2 VLAN : un VLAN "enseignant-chercheur" et un autre VLAN "stagiaires".

5.a. Justifiez la nécessité d'une telle configuration ?

5.b. Une machine "stagiaire" peut-elle contacter une machine "enseignant-chercheur" sans passer par Internet ? Si oui, expliquer comment ?

6. Combien d'interfaces au minimum doit avoir un routeur pour router des paquets entre 3 VLAN différents ?

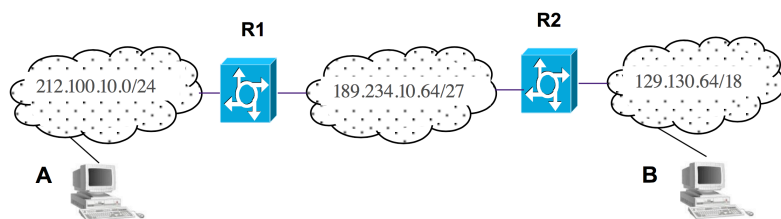
7. Soit un routeur R ayant 3 interfaces Ethernet. R est incompatible avec l'encapsulation/tagging 802.1Q (i.e. qui ne pas assurer le marquage 802.1Q).

7.a. R peut-il assurer le routage inter-VLAN? Si oui, jusqu'à combien de VLAN R peut assurer le routage?

7.b. Si R est capable de faire le routage inter-VLAN, expliquer les grandes lignes de la configuration (les points essentiels à prendre en considération lors de sa configuration)

III. Routage Statique et Adressage

Soit le réseau suivant (pour le réseau droit lire 129.130.64.0/18) qui comprend deux machines A (sous Windows) et B (sous Linux) équivalentes de point de vue capacités matérielles :



1. Assigner des adresses aux 2 machines A et B ainsi qu'aux deux routeurs R1 et R2.
2. En utilisant votre adressage, quelle doit être la passerelle par défaut pour la machine A et pour la machine B?
3. Quelle est l'utilité de la passerelle par défaut pour les machines A et B?
4. Le schéma donné par la figure ci-dessous, est-il un schéma logique ou un schéma physique? Justifier votre réponse et compléter le schéma.
5. Nous avons examiné la machine B avant le nouvel adressage dicté par cet exercice (voir le résultat de la commande **ifconfig -a**). Indiquez les changements qu'on devrait constater avec la commande **ifconfig -a** sur B (après le nouvel adressage)

hostnameOfA:~# **ifconfig -a**

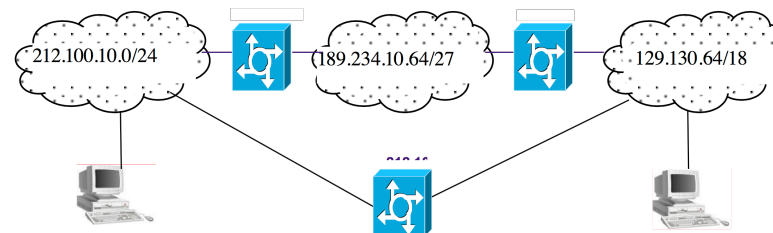
```
eth0  Link encap:Ethernet  HWaddr d4:cc:ff:c5:89:10
      inet addr:192.168.1.20  Bcast: 192.168.1.255  Mask:255.255.255.0
      ....
```

```
eth1  Link encap:Ethernet  HWaddr d4:aa:5a:ca:8a:2b
      BROADCAST MULTICAST  MTU:1500  Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
      Interrupt:17  Memory:c2000000-c2012800
```

```
lo    Link encap:Local Loopback
      inet addr:127.0.0.1  Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING  MTU:16436  Metric:1
      RX packets:9555 errors:0 dropped:0 overruns:0 frame:0
      TX packets:9555 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:1157550 (1.1 MiB)  TX bytes:1157550 (1.1 MiB)
```

6. Faire le schéma physique correspondant sachant que entre R1 et A (R2 et B resp.) nous utilisons un switch.
7. Dans le réseau de droite, est-il nécessaire de vérifier qu'aucun autre ordinateur ne dispose de la même adresse MAC de A?
8. Décrivez (soit en listant les tables soit les commandes) le routage qu'il faut initialiser sur les machines et les routeurs pour que l'on puisse échanger des données entre le réseau de A et le réseau de B.
9. En utilisant l'Annexe. Lister les lignes de commandes nécessaires à la configuration de la machine B et le routeur R1 (pas de configuration à froid!).

Avec le temps et l'évolution des besoins, notre réseau précédent a été enrichi par un nouveau routeur R3 ayant les mêmes capacités matérielles que R1 et R2:



10. Assigner les adresses pour R3.
11. Quelle modification sur le routage doit-on faire? À quoi peut servir R3?

12. Est-il intéressant d'utiliser un protocole de routage (argumenter) ? Comment se serait passée l'évolution des tables lorsque l'on a ajouté R3 ?

IV. Routage Dynamique

Dans cette partie se basera principalement sur l'analyse des protocoles RIP (Routing Information Protocol, RFC 2453 – version 2) et OSPF (Open Shortest Path First, RFC 2328 – version 2). Comme vu en cours, dans le calcul des meilleures routes, RIP se base sur l'algorithme Vecteur de Distance ("Distance Vector"), tandis que OSPF se base sur l'algorithme SPF ("Shortest Path First"). Plusieurs routes menant à un même réseau peuvent être rapportées par différents moyens (protocoles RIP, OSPF, routes statiques, etc.). Pour un routeur, il faut choisir la meilleure. Pour cela chaque moyen d'apprendre une route a un coût appelé distance administrative. Les distances administratives standard sont les suivantes : directement connecté (0), route statique (1), RIP (120), OSPF (110).

IV.a Routage Dynamique avec RIP

Lire attentivement l'annexe (partie II.A : protocoles de routage dynamique – résumé sur le protocole RIP) avant de répondre aux prochaines questions. Aidez vous éventuellement avec le support du cours.

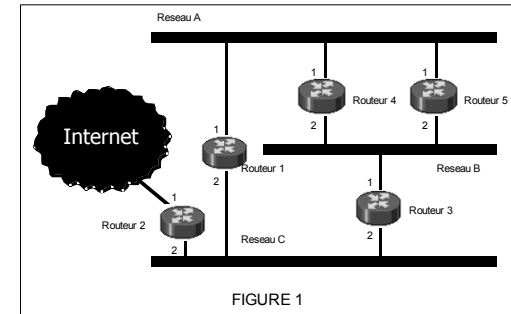
1. RIP est implémenté dans le réseau de la figure ci-dessous (sans les options *split horizon* et *poison reverse*). Les interfaces des routeurs sont données par leurs indices.

Donnez **progressivement** l'évolution des tables de routage qui seront échangées à partir de l'instant $t = T_0$ entre les routeurs. On suppose qu'à l'instant $t = T_0$, chaque routeur **ne connaît que** les réseaux qui lui sont directement connectés. Quel est le temps de convergence ?

Important : On suppose que lorsque deux **Routeur_x** et **Routeur_y** envoient simultanément une table de routage à un autre routeur, sachant que l'indice $x < y$, les routes de Routeur_x sont traitées **avant** celles de Routeur_y. Dans la réalité, les routes reçues en premier sont traitées avant les autres qui arrivent après.

On notera les tables de routage sous la forme :

Destination	Chemin (routeur)	Métrique	Interface



2. Le réseau est sans pannes et les tables de routage sont stabilisées. Le routeur Routeur₂ tombe en panne à l'instant $t = T_1$. Donnez progressivement l'évolution des tables de routage des autres routeurs (Routeur_{1/3/4/5}) jusqu'à la stabilisation (i.e. convergence) en indiquant la valeur de timer/compteur associée à chaque route (exemple : une route nouvellement rafraîchie aura comme valeur du compteur 3 minutes, i.e. 180 s). Quelle est la valeur du temps de convergence depuis la panne ?

IV.b Routage Dynamique de RIP à OSPF

Lire attentivement l'annexe (partie II.B : protocoles de routage dynamique – résumé sur le protocole OSPF) avant de répondre aux prochaines questions. Aidez vous éventuellement avec le support du cours.

- OSPF permet de résoudre les principales faiblesses du protocole RIP. Citez ces principales faiblesses.
- Quel est l'intérêt, avec OSPF, de la définition des zones par rapport à RIP
- On s'intéresse au calcul de la charge réseau induite par les messages de contrôle (i.e. autres que les messages de données) échangés par les protocoles RIP et OSPF. On considère un réseau de n routeur et une topologie en **anneau**. Dans le cas de OSPF, on suppose que tous les routeurs appartiennent à la même zone. Pour simplifier le calcul, on suppose qu'une entrée de table de routage (une route) est stockée sur **4 octets**. (la taille fixe des entêtes OSPF ou RIP est ignorée)
 - Combien de voisin possède chaque routeur ?
 - à partir de combien de routeurs, on risque d'avoir des routeurs inaccessible au sens RIP ?
 - On suppose que tous les routeurs sont stables (leurs tables de routage ne changent plus). Calculer (en fonction de n) la charge réseau (durant 1 minute) induite par les messages de contrôle dans le cas de RIP ensuite OSPF.
 - Dans notre cas, quelle est la condition que la charge réseau induite par RIP soit moins lourde que celle de OSPF ?

4. Les messages utilisés par OSPF sont décrits dans le tableau suivant :

Type de paquet OSPF	Description
Type 1 – HELLO	Etablit et maintient les informations d'adjacence avec les voisins
Type 2 - Database description packet (DBD)	Décrit le contenu de la base de donnée d'état de lien d'un routeur OSPF
Type 3 - Link State Request	Fais (demande) des requêtes sur les bases de données
Type 4 - Link State Update (LSU)	Transportes les annonces de link-state (LSA - Link State Advertissement) pour les routeur voisins.
Type 5 - Link State Acknowledgement (LSACK)	Accusé de réception pour les LSA

Neuf types de LSA existent. Le type « **Router LSA** » : est émis par un routeur OSPF pour informer de son lien qui l'attache à la zone. Le type « **Network LSA** » : est généré par le DR (Designated Router) afin de décrire les routes attachées dans la zone.

Notons que même s'il n'y a pas de changement de routes, OSPF maintient un rafraîchissement régulier des routes. A chaque LSA un timer (âge) est associé (30 minutes par défaut). Si l'âge est expiré, le routeur qui avait émis cette entrée, envoi un LSU (type 4 dans le tableau) à tous les routeurs OSPF.

Election : Pour élire le DR (Designated Router) et le BDR (Backup Designated Router), les routeurs comparent leur priorité (champs dans les paquets Hello) durant le processus d'échange des paquets Hello. Celui qui a la priorité la plus forte est élu DR et le deuxième routeur ayant la priorité la plus grande est élu BDR. Dans la réalité et en absence de pannes, le premier routeur enclenché devient DR et le second BDR. Si le DR ne répond pas suffisamment rapidement aux LSA envoyés par le BDR (i.e. si le *dead interval* tombe à 0), le BDR prend le relais du DR et un nouveau BDR est élu. Le DR utilise le processus/protocole d'inondation pour renvoyer ces informations à tous les autres routeurs de la zone correspondante assurant ainsi que tous les routeurs ont la même information. Le BDR réalise les mêmes tâches que le DR mais seulement quand celui-ci tombe en panne.

4.a. OSPF utilise l'algorithme SPF et les trois sous protocoles : Hello, échange et inondation. Faites les bonnes associations entre les tâches qu'un routeur OSPF doit assurer et le sous protocole correspondant.

Découvrir les routes	sous protocole Hello
Maintenir la base de données topologique	algorithme SPF
Etablir la liste des routeurs voisins opérationnels	sous protocole d'échange
Elire les meilleures routes à utiliser	sous protocole d'inondation
Elire un routeur désigné et un routeur de secours	

4.b. Dans un réseau OSPF, nous avons relevé la capture réseau suivante :

200	273.418043	22.0.0.17	224.0.0.5	OSPF	Hello Packet
...<que des Hello émanant de 22.0.0.17>...					
909	1135.048002	22.0.0.28	224.0.0.5	OSPF	Hello Packet
914	1139.091217	22.0.0.17	224.0.0.5	OSPF	LS Update
915	1139.092162	22.0.0.28	224.0.0.5	OSPF	LS Update
916	1139.122872	22.0.0.17	224.0.0.5	OSPF	LS Update
918	1141.090714	22.0.0.17	224.0.0.5	OSPF	LS Acknowledge
919	1141.091924	22.0.0.28	224.0.0.5	OSPF	LS Acknowledge
922	1143.582651	22.0.0.17	224.0.0.5	OSPF	Hello Packet
923	1145.047518	22.0.0.28	224.0.0.5	OSPF	Hello Packet

Détail des paquets numéro 200 et 907:

Frame 200 (90 bytes on wire, 90 bytes captured)

Ethernet II, Src: Cisco_1b:6f:e3 (00:0d:ed:1b:6f:e3), Dst: IPv4mcast_00:00:05

(01:00:5e:00:00:05)

Internet Protocol, Src: 22.0.0.17 (22.0.0.17), Dst: 224.0.0.5 (224.0.0.5)

Open Shortest Path First

OSPF Header

OSPF Version: 2

Message Type: Hello Packet (1)

Packet Length: 44

Source OSPF Router: 17.17.17.22 (17.17.17.22)

Area ID: 0.0.0.22

Packet Checksum: 0xca61 [correct]

Auth Type: Null

Auth Data (none)

OSPF Hello Packet

Network Mask: 255.0.0.0

Hello Interval: 10 seconds

Options: 0x12 (L, E)

Router Priority: 1

Router Dead Interval: 40 seconds

Designated Router: 0.0.0.0

Backup Designated Router: 0.0.0.0

OSPF LLS Data Block

Frame 907 (94 bytes on wire, 94 bytes captured)

Ethernet II, Src: Cisco_1b:6f:e3 (00:0d:ed:1b:6f:e3), Dst: IPv4mcast_00:00:05 (01:00:5e:00:00:05)

Internet Protocol, Src: 22.0.0.17 (22.0.0.17), Dst: 224.0.0.5 (224.0.0.5)

Open Shortest Path First

OSPF Header

OSPF Version: 2

Message Type: Hello Packet (1)

Packet Length: 48

Source OSPF Router: 17.17.17.22 (17.17.17.22)

Area ID: 0.0.0.22

Packet Checksum: 0x7c1a [correct]

Auth Type: Null

Auth Data (none)

OSPF Hello Packet

Network Mask: 255.0.0.0

Hello Interval: 10 seconds

Options: 0x12 (L, E)

Router Priority: 1

Router Dead Interval: 40 seconds

Designated Router: 22.0.0.17

Backup Designated Router: 0.0.0.0

Active Neighbor: 28.28.28.22

OSPF LLS Data Block

4.b.1. En se basant sur la capture donnée, avec quelle périodicité sont émis les paquets Hello ? A quelle adresse sont émis ? Que représente cette adresse d'après vous ?

4.b.2. Donnez les principales informations contenant dans les paquets Hello avec leurs significations.

4.b.3. Expliquez les principales différences entre les paquets 200 et 907.

5. Rappelez le temps de convergence (obtenu dans la question IV.a.2.) suite à la panne du routeur 2.

6. Au bout de combien de temps au maximum, une panne de routeur est détectée dans OSPF ?

7. Citez les principales étapes et messages OSPF échangés, lorsqu'un routeur est détecté en panne par un de ses voisins?

8. Au bout de combien de temps un DR est élu en général ? Justifiez votre réponse.

9. Dédurre le DR et l'instant de diffusion de son élection en se basant sur la capture donnée précédemment (sachant que le paquet numéro 200 est le premier émis dans le réseau.)

10. Voici un extrait du RFC de OSPF (version 2) : « *In general, when a router's interface to a network first becomes functional, it checks to see whether there is currently a Designated Router for the network. If there is, it accepts that Designated Router, regardless of its Router Priority... (Otherwise, the router itself becomes Designated Router if it has the highest Router Priority on the network) ..* ». Justifiez pourquoi ?

11. En se basant sur la capture donnée précédemment, à quel moment le BDR est élu ? Justifiez votre réponse ?

12. Voici le détail des paquets précédents numéro : 914, 915 et 916 :

Frame 914 (98 bytes on wire, 98 bytes captured)

Ethernet II, Src: Cisco_1b:6f:e3 (00:0d:ed:1b:6f:e3), Dst: IPv4mcast_00:00:05

(01:00:5e:00:00:05)

Internet Protocol, Src: 22.0.0.17 (22.0.0.17), Dst: 224.0.0.5 (224.0.0.5)

Open Shortest Path First

OSPF Header

OSPF Version: 2

Message Type: LS Update (4)

Packet Length: 64

Source OSPF Router: 17.17.17.22 (17.17.17.22)

Area ID: 0.0.0.22

Packet Checksum: 0x0f49 [correct]

Auth Type: Null

Auth Data (none)

LS Update Packet

Number of LSAs: 1

LS Type: Router-LSA

LS Age: 1 seconds

Do Not Age: False

Options: 0x22 (DC, E)

Link-State Advertisement Type: Router-LSA (1)

Link State ID: 17.17.17.22

Advertising Router: 17.17.17.22 (17.17.17.22)

LS Sequence Number: 0x80000002

LS Checksum: 0xb599

Length: 36

Flags: 0x02 (E)

Number of Links: 1

Type: Transit ID: 22.0.0.17 Data: 22.0.0.17 Metric: 1

IP address of Designated Router: 22.0.0.17

Link Data: 22.0.0.17

Link Type: 2 - Connection to a transit network

Number of TOS metrics: 0

TOS 0 metric: 1

Frame 915 (98 bytes on wire, 98 bytes captured)

Ethernet II, Src: Cisco_04:60:00 (00:1f:ca:04:60:00), Dst: IPv4mcast_00:00:05 (01:00:5e:00:00:05)

Internet Protocol, Src: 22.0.0.28 (22.0.0.28), Dst: 224.0.0.5 (224.0.0.5)

Open Shortest Path First

OSPF Header

OSPF Version: 2

Message Type: LS Update (4)

Packet Length: 64

Source OSPF Router: 28.28.28.22 (28.28.28.22)

Area ID: 0.0.0.22

Packet Checksum: 0x2611 [correct]

Auth Type: Null

Auth Data (none)

LS Update Packet

Number of LSAs: 1

LS Type: Router-LSA

Frame 916 (94 bytes on wire, 94 bytes captured)

Ethernet II, Src: Cisco_1b:6f:e3 (00:0d:ed:1b:6f:e3), Dst: IPv4mcast_00:00:05 (01:00:5e:00:00:05)

Internet Protocol, Src: 22.0.0.17 (22.0.0.17), Dst: 224.0.0.5 (224.0.0.5)

Open Shortest Path First

OSPF Header

OSPF Version: 2

Message Type: LS Update (4)

Packet Length: 60

Source OSPF Router: 17.17.17.22 (17.17.17.22)

Area ID: 0.0.0.22

Packet Checksum: 0x500c [correct]

Auth Type: Null

Auth Data (none)

LS Update Packet

Number of LSAs: 1

LS Type: Network-LSA

LS Age: 1 seconds

Do Not Age: False

Options: 0x22 (DC, E)

Link-State Advertisement Type: Network-LSA (2)

Link State ID: 22.0.0.17

Advertising Router: 17.17.17.22 (17.17.17.22)

LS Sequence Number: 0x80000001

LS Checksum: 0x57be

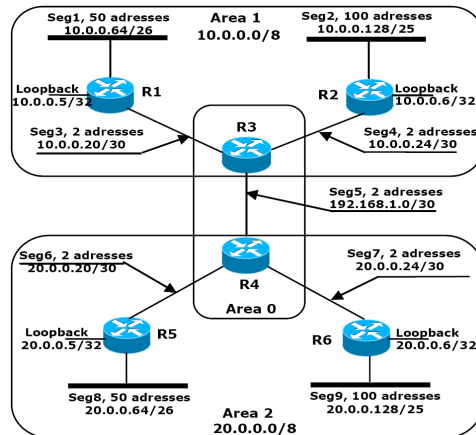
Length: 32

Netmask: 255.0.0.0

Attached Router: 17.17.17.22

Attached Router: 28.28.28.22

- 12.a. Extraire brièvement les principales informations des entêtes OSPF.
- 12.b. Résumer la signification des champs LSA. Quel est le type des LSA transportés ? Expliquer les différents rôles entre ces 3 messages?
13. Soit un réseau configuré avec OSPF dont la topologie est la suivante :



- 13.a. On supposera, dans un premier temps, que tous les routeurs appartiennent à une aire (zone) unique, soit aire 0. Interprétez, quand c'est possible, les informations étiquetées dans les réponses suivantes obtenues avec différentes commandes.

R3#show ip ospf database

OSPF Router with ID (10.0.0.7) (Process ID 1)
Router Link States (Area 0) **1**

Link ID	ADV Router	Age	Seq#	Cksum	Link count
10.0.0.5 2	10.0.0.5	580	0x80000002	0x004C11	4 9
10.0.0.6	10.0.0.6	586	0x80000002	0x00361C	4
10.0.0.7	10.0.0.7	556	0x80000005	0x00D85B	6
10.0.0.8	10.0.0.8	556	0x80000004	0x00CF48	5
20.0.0.5	20.0.0.5	730	0x80000002	0x009986	4
20.0.0.6	20.0.0.6	730	0x80000002	0x008391	4

Net Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum
192.168.1.2 3	10.0.0.8 4	557	0x80000001	0x00E750

R4#show ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.0.0.7 5	1	FULL/BDR 6	00:00:32	192.168.1.1 7	Fa0/0
20.0.0.5	0	FULL/-	00:00:37	20.0.0.22	S0/0/1
20.0.0.6	0	FULL/-	00:00:38	20.0.0.26	S0/0/0

R3#show ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.0.0.8	1	FULL/DR 6	00:00:38	192.168.1.2	Fa0/0
10.0.0.5	0	FULL/- 8	00:00:34	10.0.0.22	S0/0/1
10.0.0.6	0	FULL/-	00:00:38	10.0.0.26	S0/0/0

- 13.b. Comme dit en cours, une des fonctionnalités majeures de OSPF est le support du routage hiérarchique en découpant le domaine de routage plusieurs zones. La Figure précédente illustre un tel découpage en trois aires. Les routeurs sont configurés en conséquence. Interprétez les informations étiquetées dans les réponses suivantes.

R3#show ip ospf database

OSPF Router with ID (10.0.0.7) (Process ID 1)

Router Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum	Link count
10.0.0.5	10.0.0.5	1936	0x80000002	0x004C11	
10.0.0.6	10.0.0.6	1941	0x80000002	0x00361C	
10.0.0.7	10.0.0.7	1095	0x80000006	0x003C30	
10.0.0.8	10.0.0.8	816	0x80000005	0x003C2E	
20.0.0.5	20.0.0.5	2085	0x80000002	0x009986	
20.0.0.6	20.0.0.6	2085	0x80000002	0x008391	

Net Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum
192.168.1.2	10.0.0.8	93	0x80000002	0x00E551

Summary Net Link States (Area 0) **1**

Link ID	ADV Router	Age	Seq#	Checksum
10.0.0.0 2	10.0.0.7	269	0x80000001	0x008C94
20.0.0.0	10.0.0.8	149	0x80000001	0x00976F

Router Link States (Area 1)

Link ID	ADV Router	Age	Seq#	Checksum	Link count
10.0.0.5	10.0.0.5	221	0x80000003	0x007BFC	
10.0.0.6	10.0.0.6	226	0x80000005	0x006209	
10.0.0.7	10.0.0.7	915	0x80000003	0x0041A2	

Summary Net Link States (Area 1)

Link ID	ADV Router	Age	Seq#	Checksum
20.0.0.0	10.0.0.7	149	0x80000001	0x00A75F
192.168.1.2	1.0 10.0.0.7	304	0x80000001	0x00DC85

R3#show ip ospf interface brief

Interface	PID	Area	IP Address/Mask	Cost 3	State	Nbrs
Fa0/0	1	0	192.168.1.1/30	1	BDR	1/1
Lo0	1	1	10.0.0.7/32	1	LOOP	0/0
Se0/0/1	1	1	10.0.0.21/30	781	P2P 4	1/1
Se0/0/0	1	1	10.0.0.25/30	781	P2P	1/1

ANNEXES

I. Configuration et Administration

- Pour activer/désactiver une interface d'une machine:

#ifconfig eth0 up pour activer et

#ifconfig eth0 down pour désactiver

- Exemple de modification d'adresse IP en ligne de commande d'une machine sous Linux

à froid :

a. en modifiant le fichier **/etc/network/interfaces** comme suit :

auto eth0 (le nom de l'interface réseau concernée)

iface eth0 inet static

(adresse saisie manuellement et non pas en automatique (ex. par DHCP). Sinon: *iface eth0 inet dhcp*)

address 192.168.1.20 (adresse IP de l'interface)

netmask 255.255.255.0 (le masque de réseau)

gateway 192.168.1.254 (adresse de la passerelle par défaut)

broadcast 192.168.1.255

b. en redémarrant le service réseau avec **#service networking restart** ou **#/etc/init.d/networking restart**

à chaud :

a. Configurer une adresse IP: **#ifconfig eth0 192.168.1.20 netmask 255.255.255.0 broadcast 192.168.1.255**

b. Ajout d'une passerelle (route) par défaut : **#route add default gw 192.168.1.254**

- Pour ajouter une route (sous routeur) :

#enable

#configure terminal

Router(config)#**ip route 192.168.10.0 255.255.255.0 192.168.1.253**

(une route vers le réseau 192.168.10.0/24 et qu'il faut passer pour cela par le routeur 192.168.1.253. Format: *ip route <réseau distant> <masque réseau réseau distant> <passerelle d'accès>*)

Router(config)#**ip route 0.0.0.0 0.0.0.0 192.168.100.254**

(configuration de passerelle/route par défaut qui est 192.168.100.254)

- Exemple de modification d'adresse IP (sous routeur) :

Router(config)#**interface Ethernet0/0 (choix de l'interface)**

Router(config-if)#**ip address 192.168.10.254 255.255.255.0**

Router(config-if)#**no shutdown** (activation de l'interface)

II. Protocoles de routage dynamique

A. Résumé sur le protocole RIP :

- Les routes diffusées par un routeur sont les routes propres et les routes apprises.
- Un routeur RIP (version 2) transmet à ses voisins tous les vecteurs de distance : i.e. les triplets <adresse du réseau à atteindre qu'il connaît, masque de ce réseau, sa distance vers ce réseau>
- Le rafraîchissement des informations de routage se fait **toutes les 30 secondes**.
- La métrique est le nombre de sauts qui est limitée à 15. 16 signifie 'l'infini !' : le réseau est inaccessible.
- Si des routes redondantes apparaissent, RIP retient la meilleure (i.e. celle qui a la distance la plus petite)
- Pour une nouvelle route apprise, un routeur RIP incrémente sa distance
- A l'issue d'un certain délai appelé temps de convergence (variable selon la taille du réseau) chaque routeur connaît un moyen d'atteindre chaque réseau existant.
- A la réception d'une route, le timer ou compteur temporel associé à cette route est donc de **3 minutes**.
- Si une route n'est pas rafraîchie dans les 3 minutes, la métrique devient infinie (métrique de 16).
- Une route existante dans la table et de métrique 16 est retirée des tables **après 4 minutes**.
- A la réception d'une route de métrique 16, la route en question est retirée
- Option « Split horizon » : une information de routage reçue d'une interface n'est jamais retransmise sur celle-ci
- Option « Poison reverse » : une panne détectée est immédiatement signalée sans attendre le prochain cycle de diffusion des tables

B. Résumé sur le protocole OSPF :

- OSPF utilise une base de données distribuée qui permet de garder en mémoire l'état des liaisons (*Link-State*) du réseau. Ces informations forment une description de la topologie du réseau et de l'état de l'infrastructure (bases de données topologique : *Link-State Database*) mais ne servent pas directement de table de routage. Elle contient toutes les routes possibles pour une même destination.
- Les tables de routage OSPF sont formées à partir des meilleures routes apprises grâce à l'algorithme Dijkstra SPF (Shortest Path First)
- OSPF utilise les paquets *Hello* et deux timers associés : l'intervalle *Hello* et l'intervalle Mort (Dead ou Deadline) afin de s'assurer si un voisin est toujours présent ou pas

4. ➤ L'intervalle Hello définit à quelle fréquence un routeur émetteur doit envoyer les paquets Hello. Il est souvent réglé à 10 seconds en Ethernet
5. ➤ L'intervalle Dead spécifie la durée qu'un routeur récepteur doit attendre avant de déclarer le voisin absent (ou mort). Il est souvent réglé à 40 seconds en Ethernet
6. ➤ Un AS est divisé en plusieurs zones de routage (*area*)
7. ➤ Chaque zone possède sa propre topologie et ne connaît pas la topologie des autres zones.
8. ➤ Chaque routeur d'une zone donnée ne connaît que les routeurs de sa propre zone et la façon d'atteindre la zone centrale ou zone *backbone* (*area 0*). Cette dernière est constituée uniquement de routeurs connectés entre eux.