CISCO

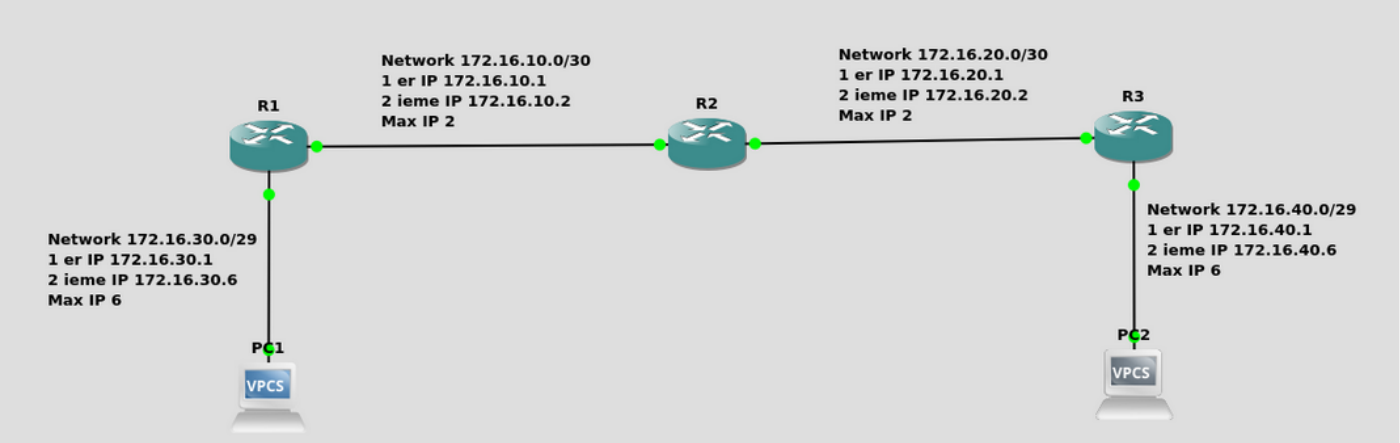
Le Routage

Le routage Satique

Le routage.

Le routage est le mécanisme par lequel des chemins sont sélectionnés dans un réseau pour acheminer les données d'un expéditeur jusqu'à un ou plusieurs destinataires.

> Laboratoire à mettre en place sur GNS3



Le routage Statique:

Le routage statique et par principe la mise en place et la mise à jour de toutes les routes de façon manuelle.

TP Mise place de route statiques:

1. Mettre en place les IPs Pour le réseau 172.16.30.0
2. ping du PC1 au R1
3. faire un show arp sur le PC1

```
show arp
ca:01:bb:f2:00:1d  172.16.30.1 expires in 112 seconds
```

4. mettre en place le réseau 172.16.40.0 et faire de même sur le PC2 et le R3
5. mettre en place les réseaux 172.16.10.0 et 172.16.20.0 et ping de R1 vers R2 et R vers R3
6. Avec la commande ci-dessous vous pourrez voire les IPs des routeurs de façon claires:

```
show ip interface brief
```

7. Essayez de ping depuis PC1 vers R2

```
PC1> ping 172.16.10.2
172.16.10.2 icmp_seq=1 timeout
172.16.10.2 icmp_seq=2 timeout
172.16.10.2 icmp_seq=3 timeout
```

> Le PING ne marche pas !!

8. faire un trace pour essayer de comprendre pourquoi ça ne fonctionne pas

```
trace to 172.16.10.2, 8 hops max, press Ctrl+C to stop
 1   172.16.30.1   7.250 ms  9.966 ms  9.439 ms
 2     *  *  *
```

On voit que le trace arrive bien au routeur R1 mais ne reviens pas.Le PC1 connais la route pour sortir de son réseau mais R2 ne connais pas sa route pour aller vers 172.16.30.0
On va afficher les routes de R2 pour en être sûr:

```
R2(config)#do show ip route
Codes: C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/30 is subnetted, 2 subnets
C       172.16.20.0 is directly connected, FastEthernet0/1
C       172.16.10.0 is directly connected, FastEthernet1/0
```

> Pour le moment R2 ne connait que les routes vers les réseaux qui sont directement connectés.

9. Ajouter une la bonne route a R2.
La route vers un réseau et son prochain saut “next hope” donc par quel chemin connu il va falloir passer pour atteindre le réseau souhaité. Pour PC1 son prochain saut est R1 par

défaut car c'est la passerelle "gateway" qu'on lui spécifi au paramétrage du réseau.
Exemple d'ajout de route :

```
ip route NETWORK MASK INTERFACE|IP_next_hope
```

Après avoir paramétré la bonne route sur R2 vers le réseau 172.16.30.0. On devrait avoir un autre résultat en faisant le trace:

```
PC1> trace 172.16.10.2
trace to 172.16.10.2, 8 hops max, press Ctrl+C to stop
 1   172.16.30.1   9.759 ms  9.178 ms  9.700 ms
 2     **172.16.10.2   15.317 ms (ICMP type:3, code:3, Destination port unreachable)

PC1> ping 172.16.10.2

84 bytes from 172.16.10.2 icmp_seq=1 ttl=254 time=15.280 ms
84 bytes from 172.16.10.2 icmp_seq=2 ttl=254 time=16.142 ms
84 bytes from 172.16.10.2 icmp_seq=3 ttl=254 time=15.686 ms
84 bytes from 172.16.10.2 icmp_seq=4 ttl=254 time=16.526 ms
```

On peut aussi voire la table de routage de R2:

```
R2(config)#do show ip route
Codes: C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
S       172.16.30.0/29 is directly connected, FastEthernet1/0
C       172.16.20.0/30 is directly connected, FastEthernet0/1
C       172.16.10.0/30 is directly connected, FastEthernet1/0
```

On voit bien que le réseau 172.16.30.0 est noté en **S** si on se reporte au descriptif plus haut on voit que cette route est dite **statique**.

10. Ajouter les bonnes routes à R1, R2 et R3.

> Normalement si vous avez mis toutes les routes sur chaque routeurs il devrait y avoir 4 routes 2 en C connecté directement et 2 en S statique

11. Ping du PC1 au PC2:

```
PC1> trace 172.16.40.2
trace to 172.16.40.2, 8 hops max, press Ctrl+C to stop
 1   172.16.30.1   6.005 ms  9.693 ms  9.101 ms
 2   172.16.10.2   19.738 ms  19.612 ms  19.656 ms
 3   172.16.20.1   29.667 ms  30.046 ms  29.425 ms
 4   *172.16.40.2   49.806 ms (ICMP type:3, code:3, Destination port unreachable)
```

> Il ne faut pas oublier de mettre une gateway sur les PC sinon le ping arrive mais ne reviens pas.

Le Routage Dynamique

Contrairement au routage statique (voir cours Ajouter une route statique sur un routeur Cisco), le routage dynamique permet d'avoir une plus grande flexibilité pour l'administrateur réseau, en cas de panne d'un lien, le calcul pour trouver un lien de secours se fera automatiquement entre les routeurs mais sa mise en œuvre est un peu plus complexe.
Alors qu'avec le routage statique l'administrateur devra :

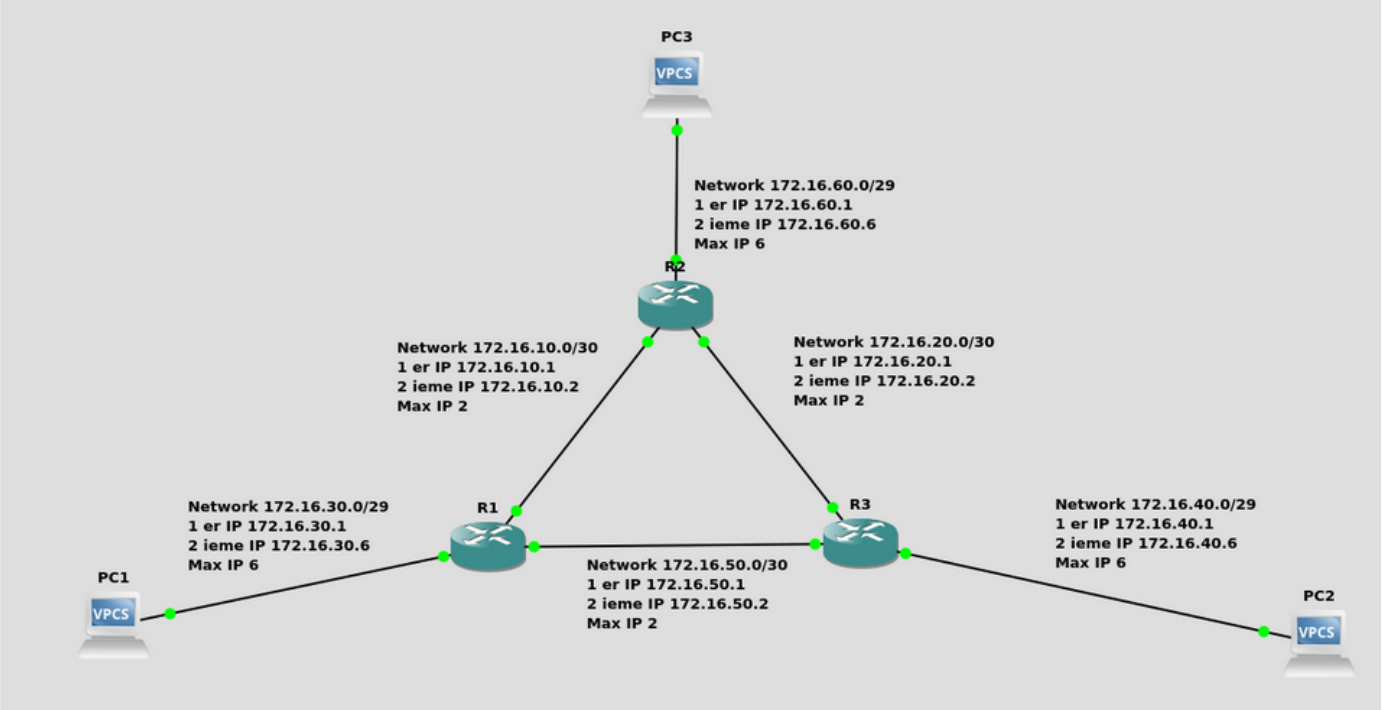
- Maintenir les tables de routage des différents routeurs
- En cas de panne une intervention manuelle est nécessaire

RIP (Routing Information Protocole)

Les caractéristiques:

- Le protocole de routage RIP fait partie des protocoles de routage de vecteur de distance.
- Sa distance administrative est égal à 120 (utile si plusieurs protocoles de routage sont utilisés, ça permet au routeur d'utilisé la route la plus rapide pour arriver à destination)
- La métrique utilisée est le nombre de saut (1 routeur = 1 saut).
- Le nombre de saut maximum est de 15, à partir de 16 routeurs le paquet est perdu.
- Trois instances de temporisation:
  - Mise à jour de la table de routage toutes les 30 secondes.
  - Temporisation d'invalidation = 180 secondes sans nouvelle de cette route, le routeur marque le routeur de destination injoignable.
  - Temporisation d'effacement = 240 secondes sans nouvelle de la route injoignable, le routeur l'efface de sa table de routage au bout de 240s.
- Envoi ses mises de routage sur toutes les interfaces du routeur par défaut, et envoi la totalité de sa table de routage.

Laboratoire à mettre en place sur GNS3



TP Mise place de route dynamique avec RIP

1. Ajouter les IPs manquantes sur le schéma.
2. ping de PC1 -> R1, PC2 -> R3 et PC3 -> R2.
3. Activer le Protocole RIP (Ce qui est après -> n'est pas à mettre) sur R1.

```
router rip
version 2 -> utilisation de la version 2 de RIP
no auto-summary -> désactivation de l'agrégation de routes
```

4. déclarer les réseau connus sur R1.

> *Ici nous allons déclarer tous les réseaux qui sont connus du routeur.*

```
network 172.16.50.0
exit
```

5. Faire les modifications sur R2 et R3.
6. regarder les routes sur R1, R2 et R3.
   Exemple sur R1 :

```
R1(config)#do show ip route
Codes: C - connected, S - static, 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
```

```
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
R       172.16.60.0/29 [120/1] via 172.16.10.2, 00:00:09, FastEthernet1/0
C       172.16.50.0/30 is directly connected, FastEthernet0/1
R       172.16.40.0/29 [120/1] via 172.16.50.2, 00:00:06, FastEthernet0/1
C       172.16.30.0/29 is directly connected, FastEthernet1/1
R       172.16.20.0/30 [120/1] via 172.16.50.2, 00:00:06, FastEthernet0/1
                       [120/1] via 172.16.10.2, 00:00:09, FastEthernet1/0
C       172.16.10.0/30 is directly connected, FastEthernet1/0
```

> Le protocole RIP a partagé les routes entre tout les routeurs.

7. Faire un trace de PC1 a PC3.

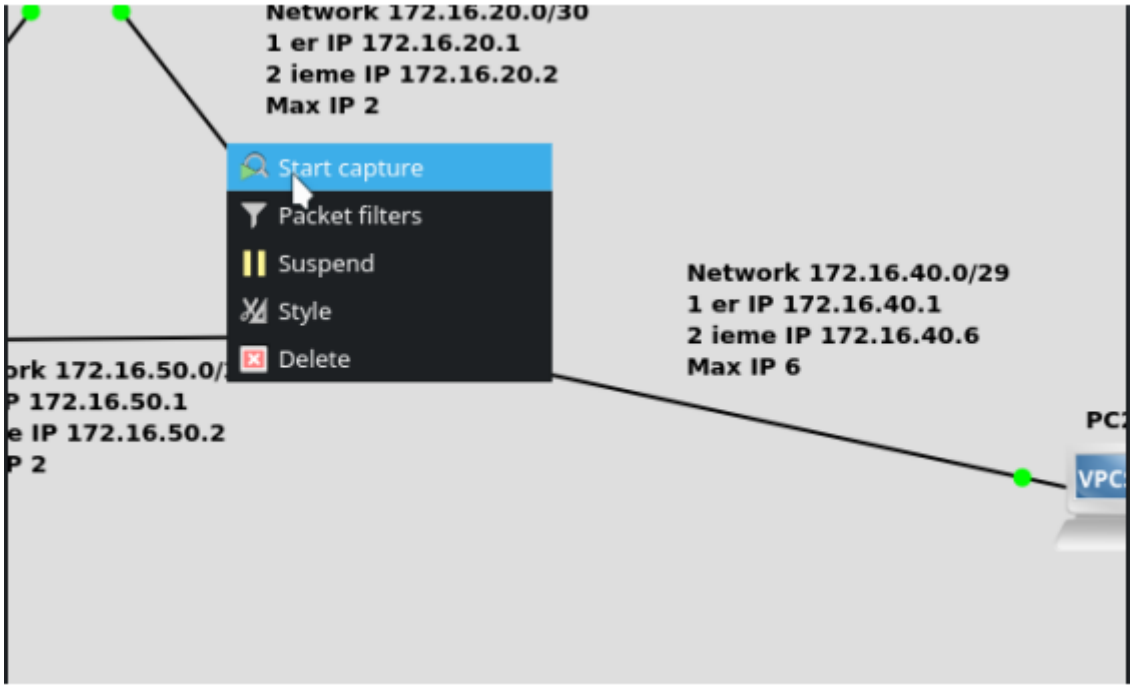
```
PC1> trace 172.16.60.2
trace to 172.16.60.2, 8 hops max, press Ctrl+C to stop
 1   172.16.30.1   10.025 ms  9.459 ms  9.988 ms
 2   172.16.10.2   29.570 ms  30.084 ms  29.367 ms
 3   *172.16.60.2   49.833 ms (ICMP type:3, code:3, Destination port unreachable)
```

8. Faire un trace entre tout les PC.
9. Afficher le résumé du protocole RIP.

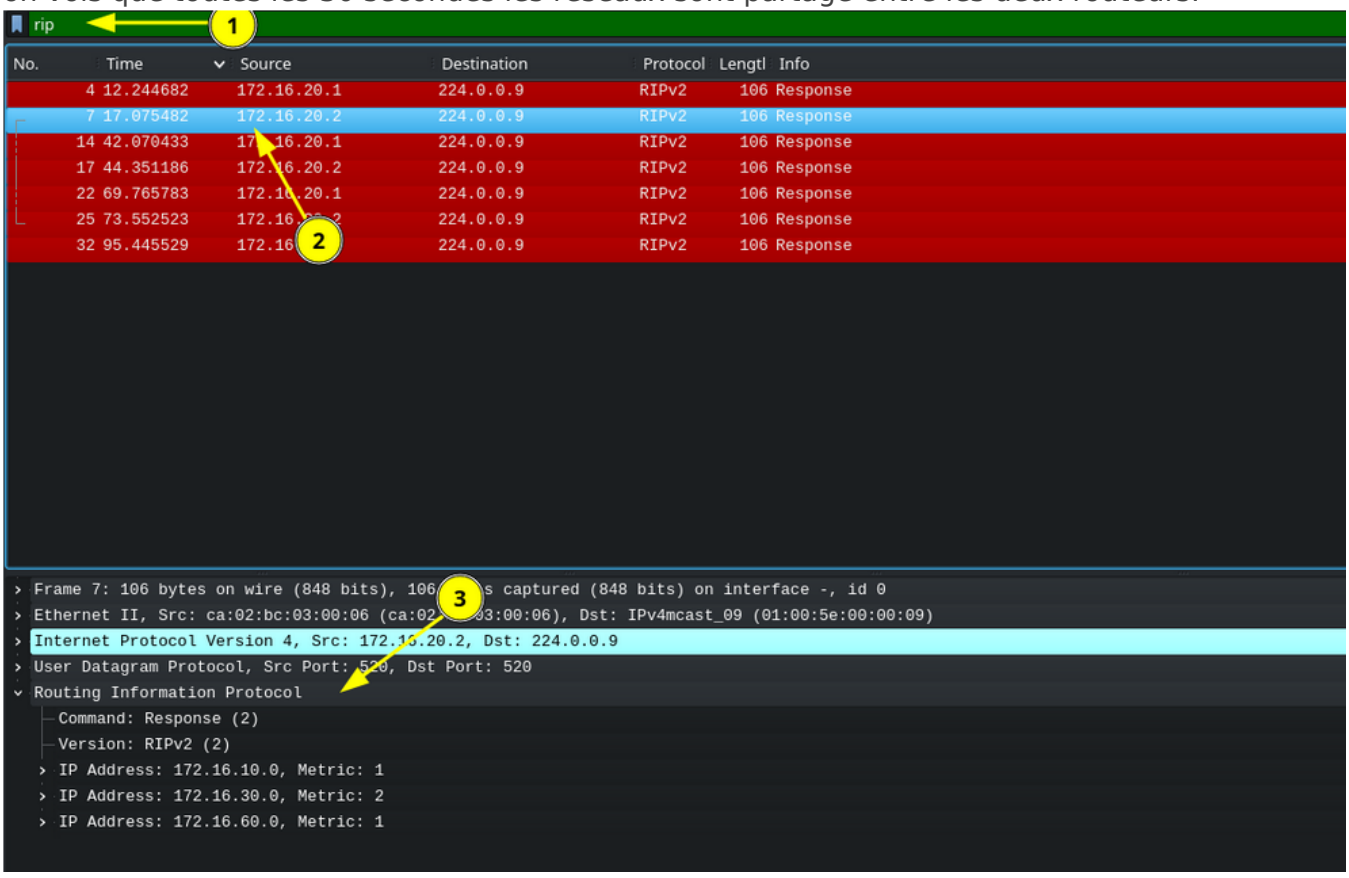
```
do show ip protocols
Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Sending updates every 30 seconds, next due in 17 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Redistributing: rip
  Default version control: send version 2, receive version 2
    Interface             Send  Recv  Triggered RIP  Key-chain
    FastEthernet0/1       2     2
    FastEthernet1/0       2     2
    FastEthernet1/1       2     2
  Automatic network summarization is not in effect
```

```
  Maximum path: 4
  Routing for Networks:
    172.16.0.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.16.50.2          120      00:00:03
    172.16.10.2          120      00:02:55
  Distance: (default is 120)
```

10. Capturer les paquets RIP via wireshark.



on vois que toutes les 30 secondes les réseaux sont partagé entre les deux routeurs:



Ces interactions font beaucoup de bruit sur le réseau on va donc faire en sorte de limiter les envoies de ces paquets au réseau (Comprendre PCs).

11. Limiter les envoie des paquets RIP sur le réseau des routeur.
    Il faut regarder via Wireshark sur les interface des Routeurs vers les PCs pour voire ce qu'il se passe. Il faut biensûr mettre le filtre rip afin de ne cibler que le protocole RIP.

On vois bien que le réseau LAN prends aussi les envoie des réseau via le protocole RIP. Pour palier ce soucis nous allons arrêter d'envoyer ces paquets sur ces interfaces:

1. Arrêter Wireshark.
2. Arrêter les interfaces sur les interfaces souhaitée:

```
router rip
passive-interface fastEthernet 1/1
```

3. Vérifier ce qu'on a fait:

```
show ip protocols | section Passive
Passive Interface(s):
  FastEthernet1/1
```

4. Relancer un Wireshark pour voire le résultat.

> *Il n'y a plus le protocol RIP sur le réseau vers les PCs !!*

> Attention les réseaux qui ne sont pas directement connectés ne sont pas partagés par défaut.
> La solution en mode router rip:
> `redistribute static`

OSPF (Open Shortest Path First).

Les caractéristiques:

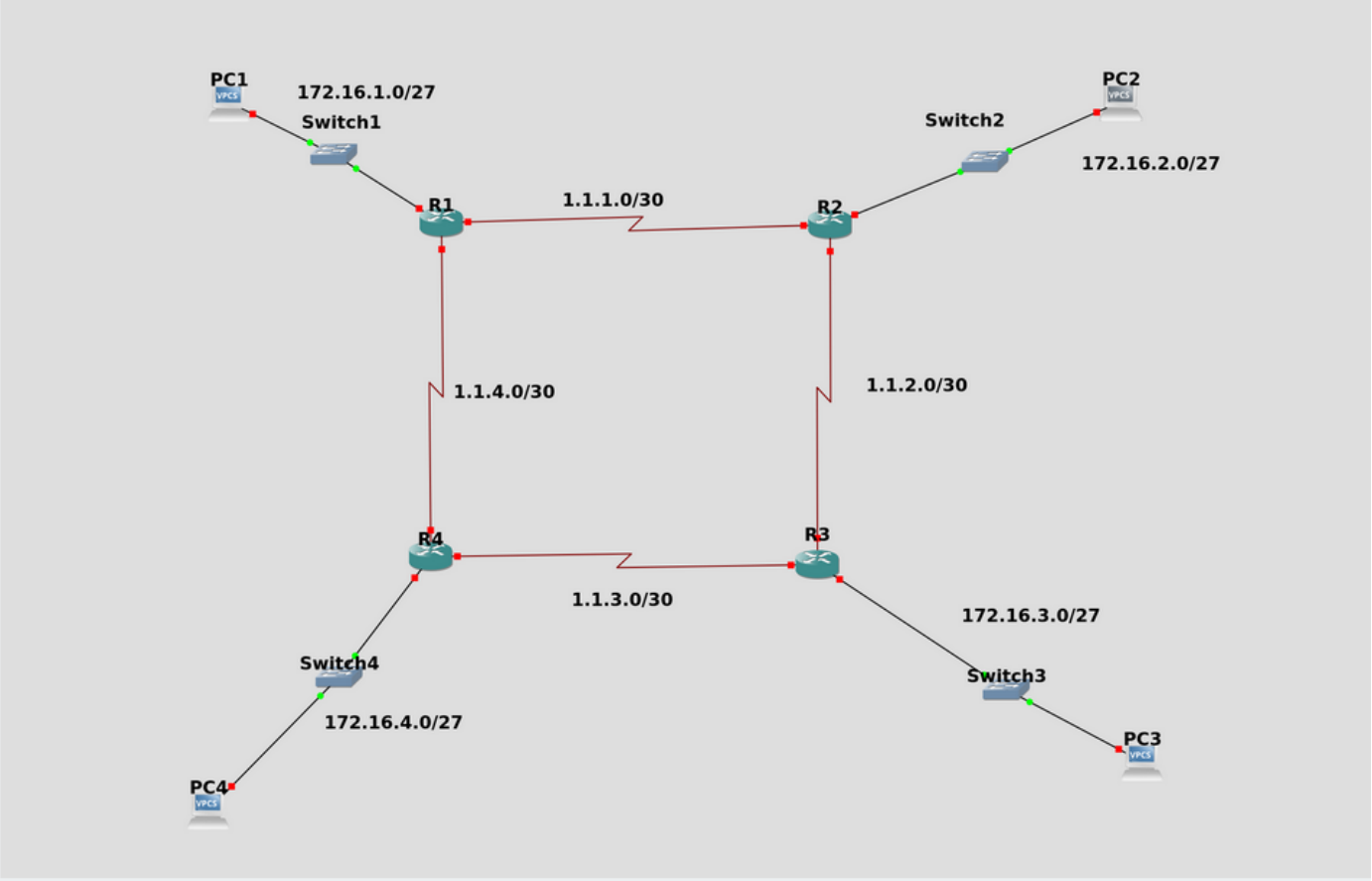
Le protocole de routage OSPF (Open Shortest Path First) est un protocole de type Link-State. C'est un protocole standard et ouvert utilisé par plusieurs constructeurs. OSPF utilise l'algorithme de Dijkstra pour déterminer le meilleur chemin vers le réseau de destination.

OSPF est utilisé par les routeurs pour établir une session de voisinage entre eux. Lorsqu'un routeur avec OSPF activé est allumé sur le réseau, il va vouloir se présenter aux autres routeurs voisins et essayer de monter une session avec eux.
La distance administrative de OSPF est 110. OSPF est utilisé avec des adresses IPv4. Pour IPv6, le protocole de routage est OSPFv3.

OSPF utilise 3 tables pour stocker les différentes informations concernant les routeurs voisins et le réseau :

- **Neighbor Table** : Cette table contient la liste des voisins du routeur ainsi que leurs informations.
- **Topology Table** : Cette table contient tous les différents chemins possibles vers les différents sous-réseau, qu'ils soient bons ou mauvais.
- **Routing Table** : Cette table contient la liste des chemins réellement utilisés pour atteindre le sous-réseau de destination.

Laboratoire à mettre en place sur GNS3.



TP Mise place de route dynamique avec OSPF:

- Paramétrer les IPs des routeurs et des PCs
- Faire un ping entre entre les PCs et leur routeurs.
- Nommer le routeur pour R1 ce sera 1:

```
router ospf 1
router-id 1.1.1.1 #pour caque routeur cette IP change
```

- Déclarer les réseaux connus attention ici il faudra déclarer le réseau et le wildcard qui est le masque inversé. Pour 255.255.255.0 le wildcard sera donc 0.0.0.255 et il faudra aussi définir l'area dans laquelle les réseau serons partagés:

```
network 172.16.1.0 0.0.0.31 area 0
```

- Faire un ping de PC1 à PC2.
- Faire un trace entre PC1 et PC2.

```
PC1> trace 172.16.2.2
trace to 172.16.2.2, 8 hops max, press Ctrl+C to stop
 1   172.16.1.1   9.436 ms  9.814 ms  9.299 ms
 2   1.1.1.2   9.823 ms  9.150 ms  9.762 ms
 3   *172.16.2.2   29.351 ms (ICMP type:3, code:3, Destination port unreachable)
```

- Supprimer le lien entre R1 et R2.

```
PC1> trace 172.16.2.2
trace to 172.16.2.2, 8 hops max, press Ctrl+C to stop
 1   172.16.1.1   9.491 ms  10.021 ms  9.479 ms
 2   1.1.4.2   19.983 ms  19.853 ms  19.770 ms
 3   1.1.3.1   29.823 ms  29.064 ms  29.431 ms
 4   1.1.2.1   39.797 ms  39.650 ms  39.405 ms
 5   *172.16.2.2   60.118 ms (ICMP type:3, code:3, Destination port unreachable)
```

> Si vous voulez partager aussi les route distribuée par RIP et les routes statiques
> `redistribute static metric 20 subnets`
> `redistribute rip subnets`

> On peut en conclure que dans certaines topologies OSPF apporte de la tolérance de panne !

- Remettre le lien en place à la même place qu'avant
- Redémarrer R1 et R2
- Lancer wireshark (**VITE**) entre R1 et R2 --> clic gauche sur le lien start wireshark
  On peut voire ici les différents types de paquets qui servent au fonctionnement d'OSPF:

ospf

No.	Time	Source	Destination	Protocol	Lengtl	Info
5	8.985569	1.1.1.2	224.0.0.5	OSPF	80	Hello Packet
8	14.890834	1.1.1.1	224.0.0.5	OSPF	80	Hello Packet
9	14.891287	1.1.1.2	224.0.0.5	OSPF	84	Hello Packet
10	14.891933	1.1.1.1	224.0.0.5	OSPF	68	DB Descriptio
11	14.891986	1.1.1.1	224.0.0.5	OSPF	84	Hello Packet
12	14.892320	1.1.1.2	224.0.0.5	OSPF	68	DB Descriptio
13	14.892499	1.1.1.1	224.0.0.5	OSPF	148	DB Descriptio

- **HELLO PACKET**:
  Les paquets hello sont envoyés sur une période de temps sur toutes les interfaces dans le but d'établir et de maintenir des relations de voisinage. Les paquets Hello sont multicast sur les réseaux ayant une capacité de multidiffusion, ce qui permet la découverte dynamique des routeurs voisins. L'occupation des différences entre les paquets hello peut former des relations de voisinage en convenant de certains paramètres.
- **DATABASE DESCRIPTION PACKET:**
  Au moment de l'initialisation de la contiguïté, ces paquets sont échangés. Ces paquets décrivent le contenu de la base de données topologique. La base de données peut être décrite à l'aide de plusieurs paquets. Une procédure de réponse à l'interrogation est utilisée pour la description de l'utilisation de plusieurs paquets. Parmi les routeurs, l'un est désigné comme maître et l'autre esclave. Les paquets de description de base de données sont envoyés par l'esclave après l'envoi des paquets de description de base de données par le maître.
- **LINK STATE REQUEST PACKET:**
  Un routeur peut trouver que les parties de sa base de données topologique sont obsolètes, après l'échange de paquets de description de base de données avec un routeur voisin. Le paquet de demande d'état de liaison est utilisé pour demander les éléments de la base de données du voisin qui sont plus à jour. Il peut être nécessaire d'utiliser plusieurs paquets de demande d'état de liaison.
- **LINK STATE UPDATE PACKETS:**
  Informations sur la structure des paquets et les champs de mise à jour de l'état de liaison

- Lister les routeurs voisins

```
R3#show ip ospf database

            OSPF Router with ID (172.16.3.1) (Process ID 3)

        Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
172.16.1.1      172.16.1.1      1393        0x8000000D 0x007CB7 5
172.16.2.1      172.16.2.1      1394        0x80000008 0x00F842 5
172.16.3.1      172.16.3.1      1647        0x80000005 0x00A573 5
172.16.4.1      172.16.4.1      1649        0x80000004 0x0082AD 5
```

Services Annexes

Services Annexes

Le DHCP

Dynamic Host Configuration Protocol est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station ou d'une machine, notamment en lui attribuant automatiquement une adresse IP et un masque de sous-réseau.

Schéma de fonctionnement du protocole

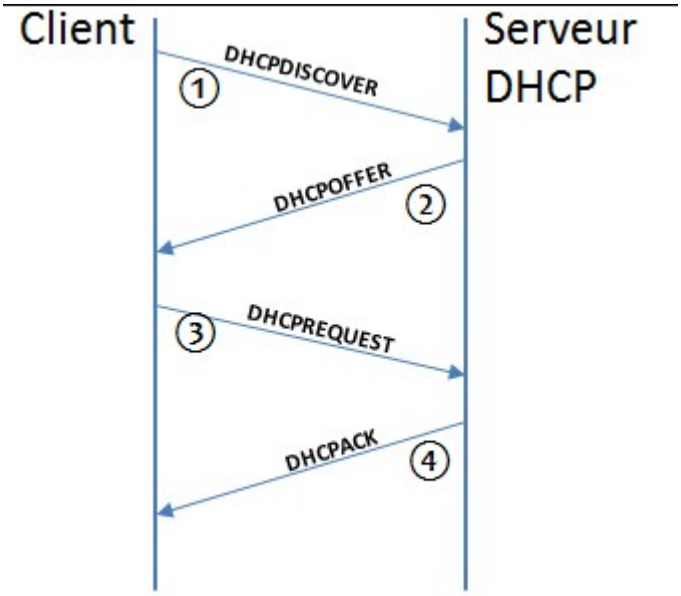
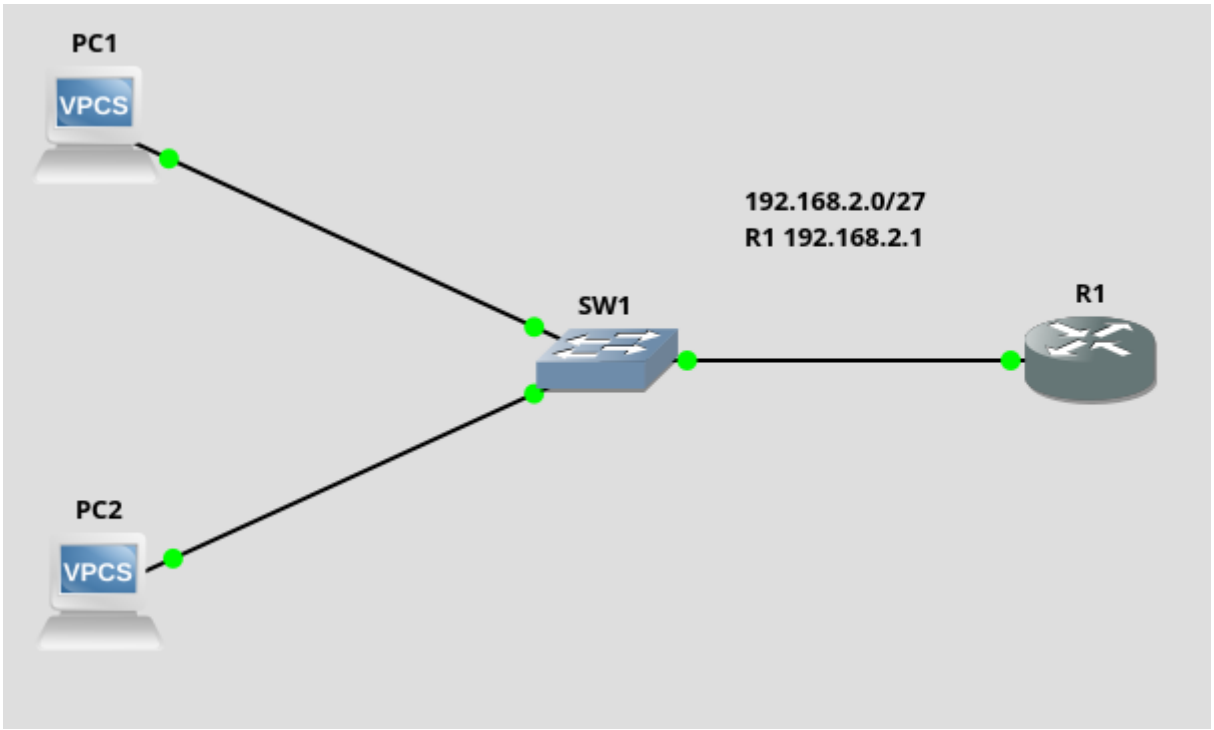


Schéma utilisé pour le DHCP



Mise en place de serveur DHCP

1. Mise en place

```
configure terminal
# Activation du service DHCP
service dhcp
# Définition du range d'adresse qui ne seront pas distribuées (gateway par exemple)
ip dhcp excluded-address 192.168.2.1 192.168.2.10
# Entrer dans le mode de configuration du service
ip dhcp pool NOMDUPOOL
# Définition du réseau qui sera partagé
network 192.168.2.0 255.255.255.224
# Définition du lease
lease 0 8
# Définition de la passerelle
default-router 192.168.2.1
exit
```

2. Sur le PC1 on va tester le DHCP

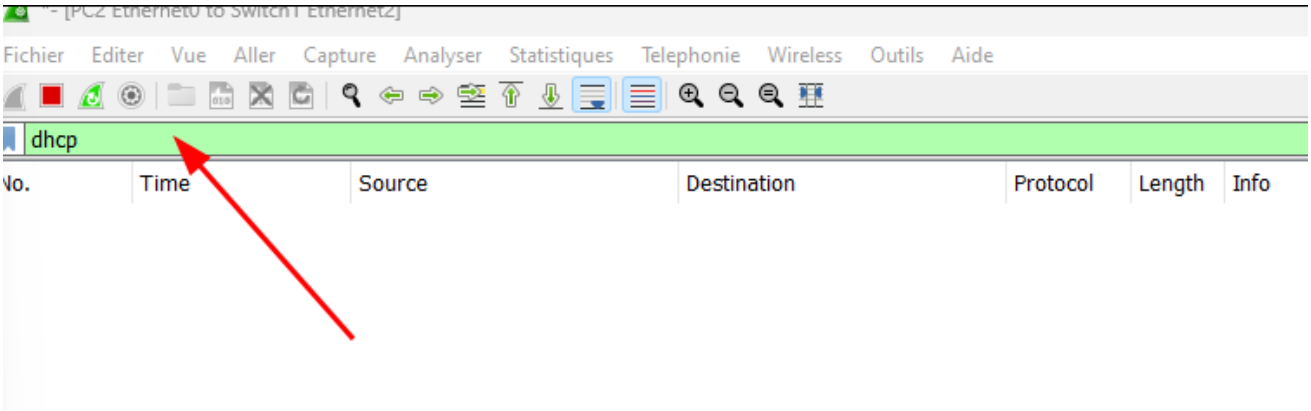
```
PC1> ip dhcp
DDORA IP 192.168.2.11/27 GW 192.168.2.1
```

Ping pour tester:

```
PC1> ping 192.168.2.1

84 bytes from 192.168.2.1 icmp_seq=1 ttl=255 time=0.138 ms
84 bytes from 192.168.2.1 icmp_seq=2 ttl=255 time=0.272 ms
84 bytes from 192.168.2.1 icmp_seq=3 ttl=255 time=0.267 ms
84 bytes from 192.168.2.1 icmp_seq=4 ttl=255 time=0.335 ms
84 bytes from 192.168.2.1 icmp_seq=5 ttl=255 time=0.241 ms
```

3. Sur le PC2 nous allons regarder ce qu'il se passe entre la requête et la réception de l'adresse IP
    1. Activer wireguard
        1. Cliquer droit sur le lien entre SW1 et PC2
        2. Cliquer sur start capture
        3. Démarrer la capture
    2. Filtrer sur DHCP



3. Lancer la requête DHCP sur le PC2

```
PC2> dhcp
DORA IP 192.168.2.12/27 GW 192.168.2.1
```

4. Regarder ce qu'il se passe sur wireshark

8	198.964945	0.0.0.0	255.255.255.255	DHCP	406	DHCP Discover - Transaction ID 0xfadfb42f
9	199.964627	192.168.2.1	192.168.2.12	DHCP	342	DHCP Offer - Transaction ID 0xfadfb42f
10	201.973924	0.0.0.0	255.255.255.255	DHCP	406	DHCP Request - Transaction ID 0xfadfb42f
11	201.975918	192.168.2.1	192.168.2.12	DHCP	342	DHCP ACK - Transaction ID 0xfadfb42f

Services Annexes

Cisco AP - Passer du mode CAPWAP au mode Autonome

1 - Avoir un accès à l'AP via un port console .

2 - Lors du démarrage de l'AP **spamme la touche** `ESC`

```
u-boot>> setenv ipaddr 192.168.2.33
u-boot>> setenv netmask 255.255.255.192
u-boot>> setenv gatewayip 192.168.2.1
u-boot>> setenv serverip 192.168.2.51
u-boot>> saveenv
```

Modifier avec vos préférence (IP, MASK etc ...)

Sécurisation

Sécurisation

AJOUT D'UN MOT DE PASSE

1. Se mettre en mode configuration

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#
```

2. Mettre en place une sécurité renforcée:

```
enable secret 4 MONPASSWORD
```

3. Mettre en place le mot de passe en clair dans le conf

```
R1(config)#enable password MONMOTDEPASSE
```

4. Test du mot de passe

```
R1#disable
R1>enable
Password:
R1#
```

5. Rendre le mot de passe illisible dans le configuration

```
R1(config)#service password-encryption
```

Sécurisation

MISE EN PLACE DE LA CONNEXION VIA SSH SUR UN ROUTEUR

Dans un premier temps il faut mettre en place un domaine sur le routeur et il faut aussi que le routeur ai un hostname.

1. Mise en place du domaine

```
R2#ena
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip domain-name megaproduction.local
```

2. Activation du SSH version 2 sur le routeur
   - Génération de la clé SSH

```
R2(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R2.megaproduction.local


% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)
```

   - Activation de SSH

```
R2(config)#ip ssh version 2
```

Mise en place de certaine options (Pas obligatoire)

- Log des connexion sur la console
  `ip ssh logging events`
- Trois essaie max pour la connexion
  `ip ssh authentication-retries 3`

On va maintenant mettre en place l'authentification pour le SSH

1. Mise en place de l'authentification

```
R2(config)#aaa new-model
R2(config)#aaa authentication login default local
R2(config)#aaa authorization exec default local
```

2. Ajout d'un nouvel utilisateur

```
username admin secret MONPASSWORD
```

3. Vérification de la version de SSH

```
R2(config)#do show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQChcducKh2B5ggTiLfh5MssfYNvX7v/NZpTWImO7pw0
rBpZ9efkb1aUNZ0pv6lTQHE5Fp4wqh3cjgIiPrK5VmgihmerKDonLJF7cPWdEWXLJHFnS0Lk1Q0UI11x
DmAcI0iMs3nb1B18e//hasJYyS8XfgnE0bnbp5FHvM+DF3bnNQ==
```

PROBLÈMES RENCONTRES:

Des problèmes d'algorithme de chiffrement à la connexion:

```
root@debian:~# ssh admin@192.168.1.1
Unable to negotiate with 192.168.1.1 port 22: no matching key exchange method found. Their
offer: diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-
sha1
```

Solution:

```
ssh admin@192.168.1.1 -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedKeyTypes=+ssh-rsa -o
KexAlgorithms=diffie-hellman-group1-sha1  -o Ciphers=aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc
```