

24/11/2024

Bloc 2 semestre 3 -4 – atelier 5 – Configuration Etherchannel et haute disponibilité sur les switchs et les routeurs

Document de l'atelier :

- [Bloc2_sem3-4_atelier-04_redondance_etherchannel-exo-1-depart.pkt](#)
- [Bloc2_sem3-4_atelier-04_redondance_HSRP_partie 1.pkt.](#)
- [Bloc2_sem3-4_atelier-04_redondance_Troubleshoot_HSRP.pka](#)
- [Bloc2_sem3-4_atelier-04_redondance_etherchannel-avancer.pkt](#)
- [wlc_pt two wlans wpa radius-fr.pkt](#)

Table des matières

1	Introduction :	3
2	Présentation	3
3	Exercice 1 : Mise en œuvre d'HSRP	4
3.1	Schéma réseaux :	4
3.1.1	Objectif de la configuration finale	4
3.2	Configuration :	5
3.3	Configuration Etherchannel sur DLS1	8
3.3.1	Vérification avec show etherchannel summary	9
3.4	Configuration du Mode VTP pour ALS1 et ALS2	10
3.4.1	Étapes de Configuration	10
3.4.2	Vérification du Statut VTP	11
3.5	Configuration de Domaine VTP	12
3.5.1	Création du Domaine VTP et Configuration de la Version sur DLS1	12
3.5.2	Création des VLANs sur le Serveur VTP (DLS1)	12
3.5.3	Vérification des VLANs sur ALS 1 et ALS2	13
3.5.4	Configuration Révision	13
3.5.5	Number of Existing VLANs	14
3.6	Configuration des Ports en Mode Access avec PortFast	14
3.7	Vérification de la Connectivité entre VLANs et Analyse des Résultats	14
3.8	Configuration Requise pour le Routage Inter-VLAN	15
3.9	Configuration HSRP pour la Redondance de Lien	15
3.10	Vérification de la Configuration HSRP	17
3.11	Vérification du Routage entre DLS1 et DLS2	17
3.12	Vérification de la Connectivité entre les VLANs	17
4	Exercice 2 : Travaux pratiques – Configuration du protocole HSRP sur des routeurs	18
4.1	La table d'adressage est la suivante	18
4.2	Objectifs	19
4.3	Contexte/scénario	19
4.4	Création du réseau et vérification de la connectivité	19
4.4.1	Câblez le réseau conformément à la topologie	19
4.4.2	Configurez les PC hôtes	20
4.4.3	Initialisez et redémarrez les routeurs et les commutateurs selon les besoins	21
4.4.4	Configuration des paramètres de base pour chaque routeur	22
4.4.5	Configuration des paramètres de base pour chaque commutateur	24
4.4.6	Vérification de la connectivité entre PC-A et PC-C	25
4.4.7	Configuration du protocole RIP et du routage par défaut	26
4.4.8	Vérification de la connectivité	26
4.5	Configuration de la redondance au premier saut avec HSRP	28
4.5.1	Détermination du chemin du trafic Internet pour PC-A et PC-C	28
4.5.2	Session ping sur PC-A et rompez la connexion entre S1 et R1 et S2 et R2	29
4.5.3	Configuration du protocole HSRP sur R1 et R3	30

4.5.4	Résultats des étapes HSRP et ping.....	32
4.5.5	Résultat de la déconnexion du commutateur lié à R1.....	33
4.5.6	Vérification des paramètres du protocole HSRP sur R1 et R3.....	34
4.5.7	Modifiez les priorités HSRP.....	35
4.5.8	Remarques générales	36
4.5.9	Tableau récapitulatif des interfaces des routeurs	36
4.6	Configuration HSRP avec répartition de charges sur R1 et R3	37
4.7	Validation de la répartition de charges en mode Round Robin avec HSRP	38
5	Exercice 3 : Packet Tracer – Dépannage du protocole HSRP.....	39
5.1	Topologie.....	39
5.2	Table d'adressage	39
5.3	Objectif	40
5.4	Contexte/scénario.....	40
5.5	Procédure de dépannage	40
5.5.1	Ordinateurs de bureau et portables	40
5.5.2	Analyse et dépannage de R1.....	41
5.5.3	Dépannage de R2.....	42
6	Exercice 4 : Etherchannel avancé	46
6.1	Vérification de la formation des EtherChannels.....	53
7	Configuration d'un contrôleur sans fil avec deux VLANs, WPA et authentification RADIUS.....	57
7.1	Configuré les serveurs RADIUS	58
7.2	Configuré mes réseaux sans fil (WLAN).....	59
7.3	Configuré le routeur.....	60
7.4	Configuré les points d'accès et PC	63
7.5	Verification.....	64
8	Annexes.....	65
9	Conclusion :.....	66
10	Webographie :.....	67

1 Introduction :

L'EtherChannel est une technologie permettant de regrouper plusieurs liens physiques entre des périphériques réseau, créant ainsi un lien logique pour augmenter la bande passante et fournir une redondance. Dans cet exercice, nous allons configurer et vérifier des EtherChannels entre plusieurs commutateurs à l'aide de différents protocoles tels que PAgP (Port Aggregation Protocol) et LACP (Link Aggregation Control Protocol), tout en prenant en compte les exigences spécifiques de configuration des VLANs, des trunks et des priorités de routeurs.

Nous allons également examiner les différents modes de négociation d'EtherChannel, notamment les modes desirable, auto, active, et passive, et configurer les VLANs natifs et les ports d'EtherChannel pour assurer un fonctionnement optimal. En outre, l'exercice met l'accent sur la configuration de la topologie réseau, l'optimisation de la connectivité et la garantie que les configurations respectent les meilleures pratiques en matière de redondance, de performances et de gestion du trafic réseau.

2 Présentation

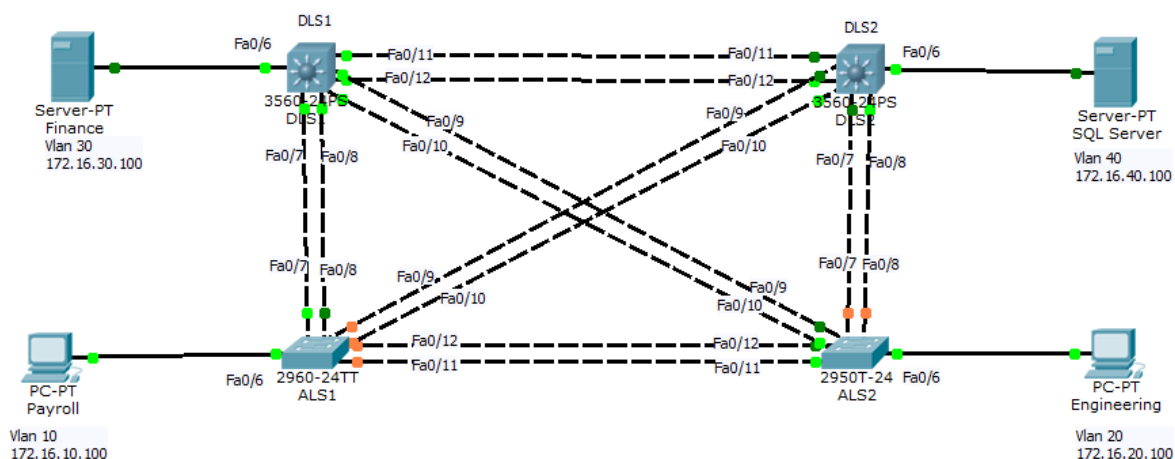
L'objectif de cet atelier est de mettre en place une configuration d'Etherchannel entre plusieurs switches afin d'augmenter la bande passante et d'assurer une meilleure redondance. L'Etherchannel permet de combiner plusieurs connexions physiques en une seule liaison logique pour augmenter la capacité de transfert et garantir la haute disponibilité du réseau. Cela permet de traiter les connexions comme si elles formaient une seule liaison.

3 Exercice 1 : Mise en œuvre d'HSRP

J'ai utilisé le fichier de départ suivant :

[Bloc2 sem3-4 atelier-04 redondance etherchannel-exo-1-depart.pkt](#)

3.1 Schéma réseaux :



3.1.1 Objectif de la configuration finale

L'objectif de cette configuration est d'assurer une architecture réseau redondante et performante en combinant l'Etherchannel et le protocole HSRP. J'ai configuré des liaisons Etherchannel entre les switches de distribution (DLS1 et DLS2) et les switches d'accès (ALS1 et ALS2) afin d'augmenter la bande passante et garantir la redondance des connexions.

Sur DLS1, les ports Fa0/9 à Fa0/12 sont utilisés pour établir l'Etherchannel avec ALS1 et ALS2, et j'ai configuré HSRP pour que ce switch soit la passerelle primaire des VLAN 10 (Payroll) et VLAN 30 (Finance). De même, sur DLS2, les ports Fa0/7 à Fa0/10 sont configurés pour l'Etherchannel avec ALS1 et ALS2, et HSRP y est défini comme passerelle primaire pour les VLAN 20 (Engineering) et VLAN 40 (SQL Server). Les switches d'accès ALS1 et ALS2 utilisent respectivement les ports Fa0/9 à Fa0/12 et Fa0/7 à Fa0/10 pour les connexions Etherchannel vers DLS1 et DLS2.

Les VLAN configurés sont :

- **VLAN 10** : 172.16.10.0/24 (Payroll)
- **VLAN 20** : 172.16.20.0/24 (Engineering)
- **VLAN 30** : 172.16.30.0/24 (Finance)
- **VLAN 40** : 172.16.40.0/24 (SQL Server)

Cette configuration permet une communication réseau fluide, une augmentation de la bande passante et une haute disponibilité grâce à HSRP et Etherchannel.

3.2 Configuration :

En premier j'ai vérifié les VLAN autorisés sur les ports trunk du switch DLS1 à l'aide de la commande show interfaces trunk et j'ai constaté qu'il manquait certains VLAN sur les interfaces Fa0/7, Fa0/8, Fa0/11, et Fa0/12.

```
DLS1#show interfaces trunk
Port      Mode      Encapsulation  Status        Native vlan
Fa0/9     auto      n-802.1q       trunking      1
Fa0/10    auto      n-802.1q       trunking      1

Port      Vlans allowed on trunk
Fa0/9     1-1005
Fa0/10    1-1005

Port      Vlans allowed and active in management domain
Fa0/9     1
Fa0/10    1

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/9     1
Fa0/10    1
```

Pour corriger cela, j'ai configuré ces interfaces en mode trunk avec l'encapsulation dot1q en utilisant les commandes suivantes :

```
DLS1(config)#interface FastEthernet0/7
DLS1(config-if)#switchport trunk encapsulation dot1q
DLS1(config-if)#switchport mode trunk
DLS1(config)#interface FastEthernet0/8
DLS1(config-if)#switchport trunk encapsulation dot1q
DLS1(config-if)#switchport mode trunk
DLS1(config)#interface FastEthernet0/11
DLS1(config-if)#switchport trunk encapsulation dot1q
DLS1(config-if)#switchport mode trunk
DLS1(config)#interface FastEthernet0/12
DLS1(config-if)#switchport trunk encapsulation dot1q
DLS1(config-if)#switchport mode trunk
```

Après ces configurations, j'ai exécuté la commande show interfaces trunk pour vérifier les VLAN autorisés sur les trunks. La capture d'écran montre que les ports Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, et Fa0/12 autorisent désormais correctement les VLAN 1-1005.

```
Port      Vlans allowed on trunk
Fa0/7     1-1005
Fa0/8     1-1005
Fa0/9     1-1005
Fa0/10    1-1005
Fa0/11    1-1005
Fa0/12    1-1005
```

En ce qui concerne DLS2, tout était correctement configuré, j'ai donc laissé la configuration telle qu'elle était.

Pour ALS1 j'ai vérifié les VLAN autorisés sur les ports trunk du switch à l'aide de la commande show interfaces trunk. J'ai constaté qu'il manquait certains VLAN sur les interfaces Fa0/7, Fa0/8, Fa0/9, et Fa0/10.

```
ALS1#show interfaces trunk
Port                Mode                Encapsulation    Status        Native vlan
Fa0/11              auto                n-802.1q         trunking      1
Fa0/12              auto                n-802.1q         trunking      1

Port                Vlans allowed on trunk
Fa0/11              1-1005
Fa0/12              1-1005

Port                Vlans allowed and active in management domain
Fa0/11              1
Fa0/12              1

Port                Vlans in spanning tree forwarding state and not pruned
Fa0/11              none
Fa0/12              none

ALS1#
```

J'ai effectué la configuration suivante pour corriger cela :

```
ALS1(config)#interface FastEthernet0/7
ALS1(config-if)#switchport trunk encapsulation dot1q
ALS1(config-if)#switchport mode trunk
ALS1(config)#interface FastEthernet0/8
ALS1(config-if)#switchport trunk encapsulation dot1q
ALS1(config-if)#switchport mode trunk
ALS1(config)#interface FastEthernet0/9
ALS1(config-if)#switchport trunk encapsulation dot1q
ALS1(config-if)#switchport mode trunk
ALS1(config)#interface FastEthernet0/10
ALS1(config-if)#switchport trunk encapsulation dot1q
ALS1(config-if)#switchport mode trunk
```

Après configuration, la commande show interfaces trunk montre que les ports Fa0/7, Fa0/8, Fa0/9, et Fa0/10 autorisent les VLAN 1-1005 comme les autres ports trunk (Fa0/11 et Fa0/12). Cela garantit que toutes les connexions nécessaires sont correctement configurées pour le trunking, permettant ainsi le passage des VLAN entre ALS1 et les autres équipements réseau.

```
Port                Vlans allowed on trunk
Fa0/7               1-1005
Fa0/8               1-1005
Fa0/9               1-1005
Fa0/10              1-1005
Fa0/11              1-1005
Fa0/12              1-1005
```

De même pour ALS2, j'ai trouvé qu'il y avait FastEthernet0/6 qui était en trop, je les ai donc remis en mode access.

```
ALS2#show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/6	desirable	n-802.1q	trunking	1
Fa0/7	desirable	n-802.1q	trunking	1
Fa0/8	desirable	n-802.1q	trunking	1
Fa0/9	desirable	n-802.1q	trunking	1
Fa0/10	desirable	n-802.1q	trunking	1
Fa0/11	desirable	n-802.1q	trunking	1
Fa0/12	desirable	n-802.1q	trunking	1

```
Port Vlan allowed on trunk
```

Fa0/6	1-1005
Fa0/7	1-1005
Fa0/8	1-1005
Fa0/9	1-1005
Fa0/10	1-1005
Fa0/11	1-1005
Fa0/12	1-1005

Pour configurer le port FastEthernet0/6 sur le switch ALS2 en mode accès, voici la commande que j'ai utilisée :

```
ALS2(config)#interface FastEthernet0/6  
ALS2(config-if)#switchport mode access
```


3.3 Configuration Etherchannel sur DLS1

J'ai vérifié s'il y avait des etherchannels sur les switches avec la commande 'show etherchannel summary', ce qui n'est pas le cas pour les 4 switches.

```
DLS1#show etherchannel summary
Flags:  D - down          P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3        S - Layer2
        U - in use        f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 0
Number of aggregators:          0

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
DLS1#
ALSI#show etherchannel summary
Flags:  D - down          P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3        S - Layer2
        U - in use        f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 0
Number of aggregators:          0

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
ALSI#
```

J'ai donc configuré les ports du switch DLS1 pour établir des Etherchannels en mode LACP avec la commande channel-group X mode active.

Interface Range Fa0/7 - Fa0/8 :

```
DLS1(config)#interface range FastEthernet0/7 - 8
DLS1(config-if-range)#switchport mode trunk
DLS1(config-if-range)#channel-group 1 mode active
DLS1(config)#interface range fastEthernet 0/7 - 8
DLS1(config-if-range)#channel-group 1 mode active
```

Interface Range Fa0/9 - Fa0/10 :

```
DLS1(config)#interface range FastEthernet0/9 - 10
DLS1(config-if-range)#switchport mode trunk
DLS1(config-if-range)#channel-group 2 mode active
DLS1(config-if-range)#interface range fastEthernet 0/9 - 10
DLS1(config-if-range)#channel-group 2 mode active
```

Interface Range Fa0/11 - Fa0/12 :

```
DLS1(config)#interface range fastEthernet 0/11 - 12
DLS1(config-if-range)#switchport mode trunk
DLS1(config-if-range)#channel-group 3 mode active
```

De même pour DLS2 il faut utiliser les mêmes commandes sur les même interface.

Pour configurer les Etherchannels sur les switches ALS1 et ALS2, j'ai utilisé les mêmes commandes que pour DLS1 et DLS2 afin d'assurer la cohérence et la redondance.

Sur ALS1 :

```
ALS1(config)#interface range fastEthernet 0/7 - 8
ALS1(config-if-range)#switchport mode trunk
ALS1(config-if-range)#channel-group 1 mode active
ALS1(config-if-range)#exit
ALS1(config)#interface range fastEthernet 0/9 - 10
ALS1(config-if-range)#switchport mode trunk
ALS1(config-if-range)#channel-group 2 mode active
ALS1(config-if-range)#exit
ALS1(config)#interface range fastEthernet 0/11 - 12
ALS1(config-if-range)#switchport mode trunk
ALS1(config-if-range)#channel-group 3 mode active
ALS1(config-if-range)#
Creating a port-channel interface Port-channel 1
```

Sur ALS2 :

```
ALS2(config)#interface range fastEthernet 0/7 - 8
ALS2(config-if-range)#switchport mode trunk
ALS2(config-if-range)#channel-group 1 mode active
ALS2(config-if-range)#exit
ALS2(config)#interface range fastEthernet 0/9 - 10
ALS2(config-if-range)#switchport mode trunk
ALS2(config-if-range)#channel-group 2 mode active
ALS2(config-if-range)#exit
ALS2(config)#interface range fastEthernet 0/11 - 12
ALS2(config-if-range)#switchport mode trunk
ALS2(config-if-range)#channel-group 3 mode active
ALS2(config-if-range)#
Creating a port-channel interface Port-channel 1
```

3.3.1 Vérification avec show etherchannel summary

Après avoir appliqué ces configurations, pour vérifier que les Etherchannels sont bien établis sur ALS1 et ALS2, j'ai utilisé la commande suivante :

DLS1#show etherchannel summary

DLS2#show etherchannel summary

ALS1#show etherchannel summary

ALS2#show etherchannel summary

```
DLS1#show etherchannel summary
Flags: D - down          P - in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
       R - Layer3        S - Layer2
       U - in use        f - failed to allocate aggregator
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

Number of channel-groups in use: 3
Number of aggregators:          3

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Po1(SU)          LACP        Fa0/7(P) Fa0/8(P)
2      Po2(SU)          LACP        Fa0/9(P) Fa0/10(P)
3      Po3(SU)          LACP        Fa0/11(P) Fa0/12(P)
```

```

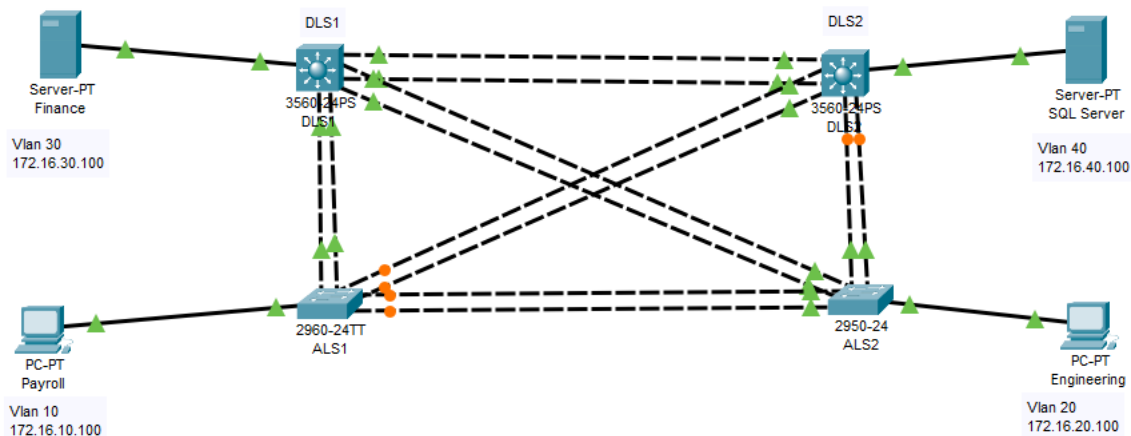
ALS2#show etherchannel summary
Flags: D - down          P - in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       U - in use       f - failed to allocate aggregator
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

Number of channel-groups in use: 3
Number of aggregators:          3

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Po1(SU)      LACP        Fa0/7(P) Fa0/8(P)
2      Po2(SU)      LACP        Fa0/9(P) Fa0/10(P)
3      Po3(SU)     LACP        Fa0/11(P) Fa0/12(P)

```

On peut vérifier avec le schéma réseau de Packet Tracer où nous voyons les interfaces se colorier en paquets de deux, soit deux triangles verts, soit deux points orange dû aux STP.



3.4 Configuration du Mode VTP pour ALS1 et ALS2

3.4.1 Étapes de Configuration

Pour configurer ALS1 et ALS2 en mode client VTP, j'ai utilisé les commandes suivantes sur chaque switch :

Sur ALS1 :

```

ALS1(config)#vtp mode client
ALS1(config)#vtp mode client
Setting device to VTP CLIENT mode.

```

Sur ALS2 :

```

ALS2(config)#vtp mode client
ALS2(config)#vtp mode client
Setting device to VTP CLIENT mode.

```

3.4.2 Vérification du Statut VTP

Pour vérifier le statut VTP après la configuration, j'ai exécuté la commande suivante sur chaque switch :

ALS1#show vtp status

```
DLS1#show vtp status
VTP Version capable      : 1 to 2
VTP version running      : 1
VTP Domain Name          :
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                : 0001.63A2.9900
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
```

Feature VLAN :

```
-----
VTP Operating Mode       : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs  : 5
Configuration Revision    : 0
MD5 digest               : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
                          0xF0 0x58 0x10 0x6C 0x9C 0x0F 0xA0 0xF7
```

ALS2#show vtp status

```
ALS2#show vtp status
VTP Version              : 1
Configuration Revision    : 0
Maximum VLANs supported locally : 255
Number of existing VLANs  : 5
VTP Operating Mode       : Client
VTP Domain Name          :
VTP Pruning Mode         : Disabled
VTP V2 Mode              : Disabled
VTP Traps Generation     : Disabled
MD5 digest               : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

Cela garantit que ALS1 et ALS2 reçoivent correctement les informations VLAN du serveur VTP (DLS1) et ne peuvent pas modifier la configuration VLAN eux-mêmes.

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

Le nombre total de 5 VLANs affichés correspond aux VLANs créés par défaut sur les switches Cisco. Ces VLANs incluent le VLAN 1, qui est le VLAN par défaut pour toutes les interfaces, et les VLANs réservés 1002 à 1005 destinés aux anciennes technologies comme FDDI et Token Ring. Ces VLANs sont automatiquement présents sur le switch et ne peuvent pas être supprimés ou modifiés. Aucun VLAN supplémentaire n'a été configuré, ce qui explique pourquoi seulement ces 5 VLANs sont visibles.

3.5 Configuration de Domaine VTP

3.5.1 Création du Domaine VTP et Configuration de la Version sur DLS1

J'ai configuré le domaine VTP avec le nom "CISCO" et utilisé la version 2 du protocole VTP sur le switch DLS1 :

```
DLS1(config)#vtp domain CISCO
DLS1(config)#vtp version 2
DLS1(config)#vtp domain CISCO
Changing VTP domain name from NULL to CISCO
DLS1(config)#vtp version 2
```

3.5.2 Création des VLANs sur le Serveur VTP (DLS1)

J'ai créé les VLANs suivants sur DLS1 :

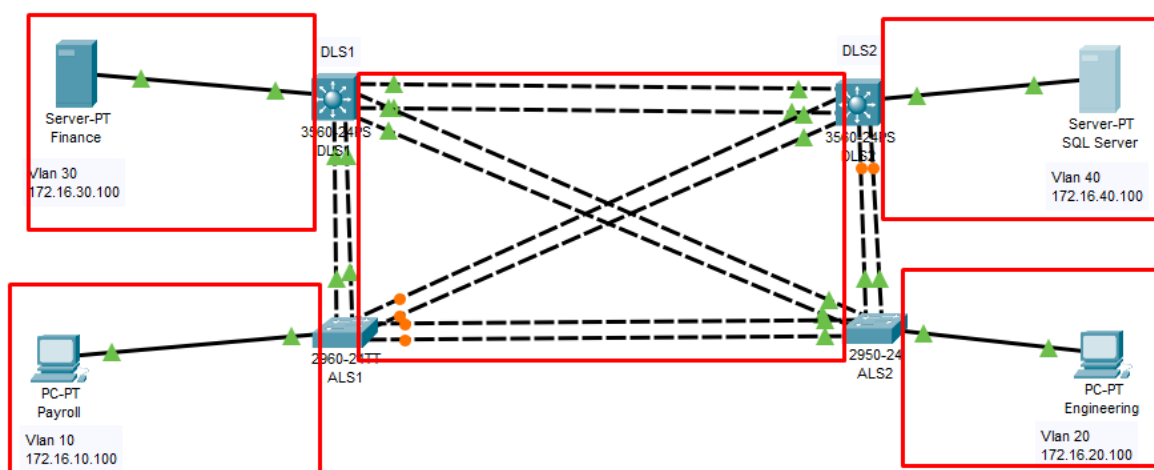
```
DLS1(config)#vlan 10
DLS1(config-vlan)#name Finance
DLS1(config)#vlan 20
DLS1(config-vlan)#name Engineering
DLS1(config)#vlan 30
DLS1(config-vlan)#name Server1
DLS1(config)#vlan 40
DLS1(config-vlan)#name Server2
```

3.5.3 Vérification des VLANs sur ALS 1 et ALS2

La commande show vlan brief montre que les VLANs 10, 20, 30, et 40 ont été propagés correctement depuis le serveur DLS1

```
ALS2#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24
10	Finance	active	
20	Engineering	active	
30	Server1	active	
40	Server2	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	



3.5.4 Configuration Révision

Définition :

La Configuration Révision est un compteur qui enregistre le nombre de modifications effectuées sur la base de données VLAN d'un serveur VTP. Chaque fois qu'un changement est apporté (création, suppression ou modification d'un VLAN), ce numéro s'incrémente automatiquement.

Impact sur le Réseau :

La Configuration Révision permet de synchroniser les VLANs sur l'ensemble des switches clients. Cela garantit que tous les switches disposent de la même configuration VLAN, facilitant ainsi la gestion centralisée du réseau et évitant des incohérences.

3.5.5 Number of Existing VLANs

Définition :

Le Number of Existing VLANs représente le nombre total de VLANs configurés sur un switch. Il inclut le VLAN 1 par défaut, les VLANs réservés (1002 à 1005), et les VLANs créés manuellement par l'administrateur. Ce nombre s'ajuste automatiquement à chaque ajout ou suppression de VLANs.

Impact sur le Réseau :

Le Number of Existing VLANs donne une vue d'ensemble des VLANs actifs sur le switch et permet de s'assurer que tous les switchs du réseau ont les VLANs nécessaires pour maintenir la connectivité. Cela simplifie la gestion centralisée des VLANs, réduit les erreurs de configuration, et garantit une infrastructure réseau cohérente et fiable.

3.6 Configuration des Ports en Mode Access avec PortFast

Pour configurer les ports Fa0/6 sur chaque switch en mode access, les assigner à leur VLAN respectif, et activer PortFast.

Sur DLS1 (VLAN 30)

```
DLS1(config)#interface FastEthernet0/6
DLS1(config-if)#switchport mode access
DLS1(config-if)#switchport access vlan 30
DLS1(config-if)#spanning-tree portfast
```

Sur DLS2 (VLAN 40)

```
DLS2(config)#interface FastEthernet0/6
DLS2(config-if)#switchport mode access
DLS2(config-if)#switchport access vlan 40
DLS2(config-if)#spanning-tree portfast
```

Sur ALS1 (VLAN 10)

```
ALS1(config)#interface FastEthernet0/6
ALS1(config-if)#switchport mode access
ALS1(config-if)#switchport access vlan 10
ALS1(config-if)#spanning-tree portfast
```

Sur ALS2 (VLAN 20)

```
ALS2(config)#interface FastEthernet0/6
ALS2(config-if)#switchport mode access
ALS2(config-if)#switchport access vlan 20
ALS2(config-if)#spanning-tree portfast
```

3.7 Vérification de la Connectivité entre VLANs et Analyse des Résultats

Pour vérifier la connectivité entre les VLANs, j'ai effectué des tests de communication en utilisant des commandes comme ping entre des périphériques situés dans des VLANs différents. Les pings ont échoué, ce qui est normal, car pour qu'un VLAN communique avec un autre VLAN, il faut qu'il y ait un routeur ou un switch de niveau 3 qui possède le routage et que le routage soit activé.

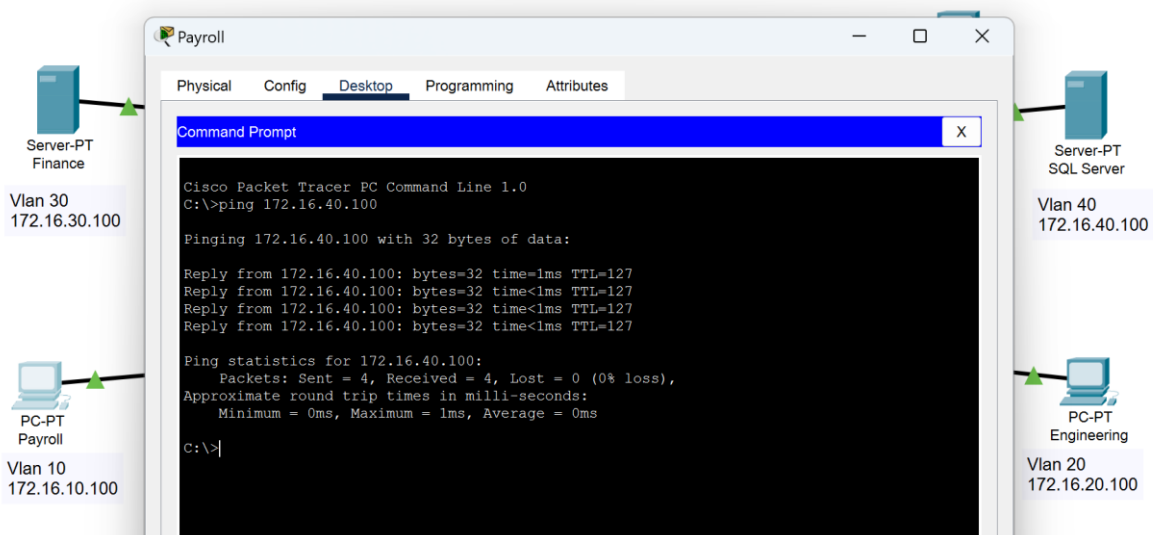
3.8 Configuration Requise pour le Routage Inter-VLAN

Sur DLS1 :

```
DLS1(config)#ip routing
DLS1(config)#interface Vlan10
DLS1(config-if)#ip address 172.16.10.2 255.255.255.0
DLS1(config-if)#no shutdown
DLS1(config)#interface Vlan40
DLS1(config-if)#ip address 172.16.40.2 255.255.255.0
DLS1(config-if)#no shutdown
DLS1(config)#router rip
IP routing not enabled
DLS1(config)#ip routing
DLS1(config)#router rip
DLS1(config-router)#
```

Résultat du Ping et Interprétation

Le ping vers l'adresse 172.16.40.100 a réussi, avec 4 paquets envoyés et 4 paquets reçus, indiquant 0% de perte. Cela signifie que la communication entre les hôtes du VLAN 10 et du VLAN 40 est établie avec succès.



3.9 Configuration HSRP pour la Redondance de Lien

Configuration sur DLS1 :

```
DLS1(config)#interface vlan 1
DLS1(config-if)#ip address 172.16.1.2 255.255.255.0
DLS1(config-if)#standby 1 ip 172.16.1.1
DLS1(config-if)#standby 1 priority 150
DLS1(config-if)#
DLS1(config)#interface vlan 10
DLS1(config-if)#ip address 172.16.10.2 255.255.255.0
DLS1(config-if)#standby 10 ip 172.16.10.1
DLS1(config-if)#standby 10 priority 150
DLS1(config-if)#
```



```
DLS1(config-if)#interface vlan 20
DLS1(config-if)#ip address 172.16.20.2 255.255.255.0
DLS1(config-if)#standby 20 ip 172.16.20.1
DLS1(config-if)#standby 20 priority 150
DLS1(config-if)#
DLS1(config-if)#interface vlan 30
DLS1(config-if)#ip address 172.16.30.2 255.255.255.0
DLS1(config-if)#standby 30 ip 172.16.30.1
DLS1(config-if)#standby 30 priority 100
DLS1(config-if)#
DLS1(config-if)#interface vlan 40
DLS1(config-if)#ip address 172.16.40.2 255.255.255.0
DLS1(config-if)#standby 40 ip 172.16.40.1
DLS1(config-if)#standby 40 priority 100
```

Configuration sur DLS2 :

```
DLS2(config)#interface vlan 1
DLS2(config-if)#ip address 172.16.1.3 255.255.255.0
DLS2(config-if)#standby 1 ip 172.16.1.1
DLS2(config-if)#standby 1 priority 100
DLS2(config-if)#
DLS2(config-if)#interface vlan 10
DLS2(config-if)#ip address 172.16.10.3 255.255.255.0
DLS2(config-if)#standby 10 ip 172.16.10.1
DLS2(config-if)#standby 10 priority 100
DLS2(config-if)#
DLS2(config-if)#interface vlan 20
DLS2(config-if)#ip address 172.16.20.3 255.255.255.0
DLS2(config-if)#standby 20 ip 172.16.20.1
DLS2(config-if)#standby 20 priority 100
DLS2(config-if)#
DLS2(config-if)#interface vlan 30
DLS2(config-if)#ip address 172.16.30.3 255.255.255.0
DLS2(config-if)#standby 30 ip 172.16.30.1
DLS2(config-if)#standby 30 priority 150
DLS2(config-if)#
DLS2(config-if)#interface vlan 40
DLS2(config-if)#ip address 172.16.40.3 255.255.255.0
DLS2(config-if)#standby 40 ip 172.16.40.1
DLS2(config-if)#standby 40 priority 150
```

3.10 Vérification de la Configuration HSRP

Pour vérifier que la configuration HSRP est correcte, utilisez la commande suivante sur DLS1 et DLS2 :

```
DLS1#show standby brief
                P indicates configured to preempt.
                |
Interface      Grp  Pri  P State      Active        Standby        Virtual IP
Vl11           1   150  P Active     local         172.16.1.3     172.16.1.1
Vl10           10  150  P Active     local         172.16.10.3    172.16.10.1
Vl20           20  150  P Active     local         172.16.20.3    172.16.20.1
Vl30           30  100  P Standby    172.16.30.3   local          172.16.30.1
Vl40           40  100  P Standby    172.16.40.3   local          172.16.40.1
DLS1#
```

3.11 Vérification du Routage entre DLS1 et DLS2

Pour vérifier la connectivité entre DLS1 et DLS2, effectuez un ping depuis DLS1 vers les adresses IP de DLS2

```
DLS1>ping 172.16.30.3
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.30.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

```
DLS1>ping 172.16.40.3
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.40.3, timeout is 2 seconds:
..!..
Success rate is 40 percent (2/5), round-trip min/avg/max = 10/15/20 ms
```

3.12 Vérification de la Connectivité entre les VLANs

Pour tester la communication entre les hôtes de différents VLANs, effectuez un ping depuis l'hôte du VLAN 10 vers l'hôte du VLAN 40 :

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.16.40.100

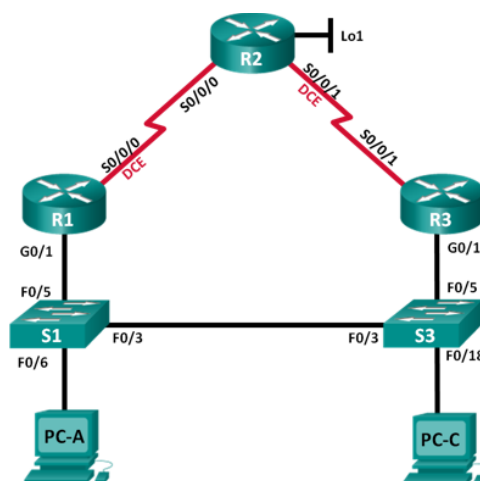
Pinging 172.16.40.100 with 32 bytes of data:

Reply from 172.16.40.100: bytes=32 time=1ms TTL=127
Reply from 172.16.40.100: bytes=32 time<1ms TTL=127
Reply from 172.16.40.100: bytes=32 time<1ms TTL=127
Reply from 172.16.40.100: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.40.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

4 Exercice 2 : Travaux pratiques – Configuration du protocole HSRP sur des routeurs

J'ai travaillé sur le réseau présenté dans le fichier [Bloc2 sem3-4 atelier-04 redondance HSRP partie 1.pkt](#).



4.1 La table d'adressage est la suivante

Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (ETCD)	10.1.1.1	255.255.255.252	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (ETCD)	10.2.2.2	255.255.255.252	N/A
	Lo1	209.165.200.225	255.255.255.224	N/A
R3	G0/1	192.168.1.3	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S3	VLAN 1	192.168.1.13	255.255.255.0	192.168.1.3
PC-A	Carte réseau	192.168.1.31	255.255.255.0	192.168.1.1
PC-C	Carte réseau	192.168.1.33	255.255.255.0	192.168.1.3

4.2 Objectifs

- Partie 1 : Création du réseau et vérification de la connectivité
- Partie 2 : Configuration de la redondance au premier saut avec HSRP

4.3 Contexte/scénario

Le protocole **Spanning Tree** permet d'assurer une redondance sans boucle entre les commutateurs d'un LAN. Toutefois, il ne permet pas d'avoir des passerelles par défaut redondantes pour les périphériques finaux en cas de défaillance d'un des routeurs. Pour pallier cela, les protocoles **FHRP (First Hop Redundancy Protocol)** permettent d'avoir des passerelles par défaut redondantes pour les périphériques finaux, sans nécessiter de configuration supplémentaire au niveau des utilisateurs. Dans ce TP, j'ai configuré le protocole **HSRP (Hot Standby Router Protocol)** de Cisco, qui est une implémentation de FHRP.

4.4 Création du réseau et vérification de la connectivité

Dans la Partie 1, j'ai configuré la topologie du réseau et mis en place les paramètres de base suivants :

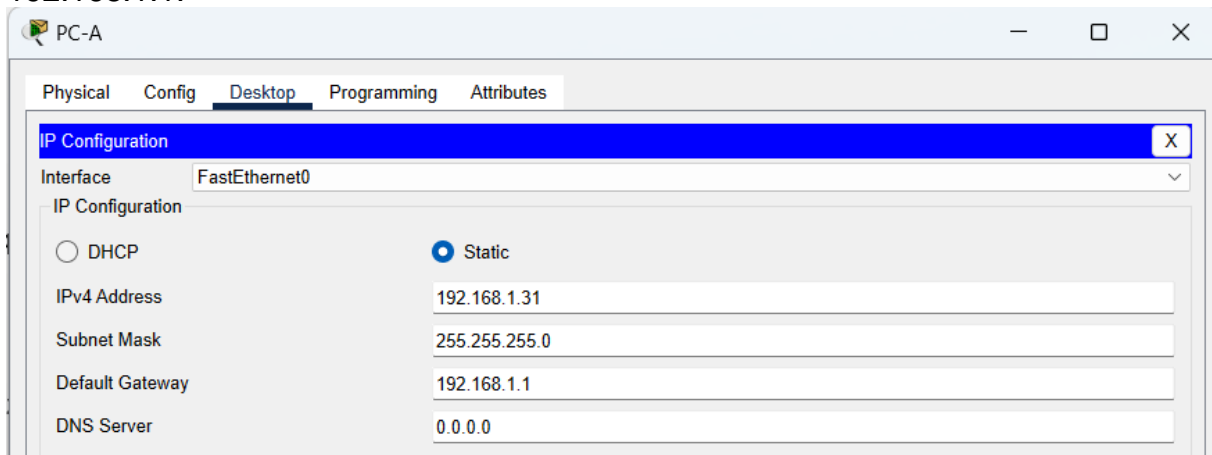
- Les adresses IP des interfaces.
- Le routage statique.
- L'accès aux périphériques.
- Les mots de passe de sécurité.

4.4.1 Câblez le réseau conformément à la topologie.

J'ai câblé le réseau conformément au schéma de la topologie en connectant tous les équipements requis et en m'assurant que le câblage était correctement effectué

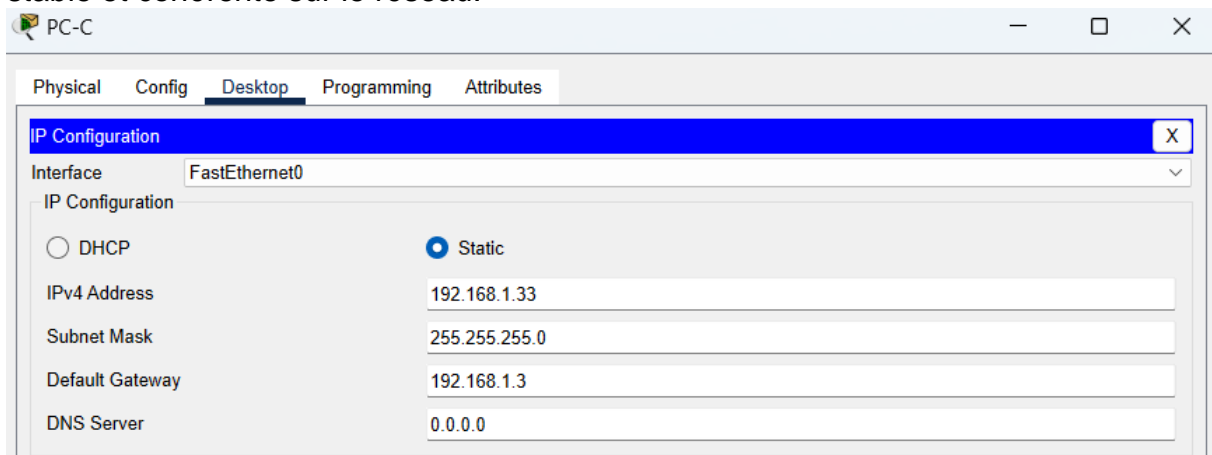
4.4.2 Configurez les PC hôtes.

Pour la configuration du PC-A j'ai configuré les paramètres suivant : l'adresse IPv4 192.168.1.31, le masque de sous-réseau 255.255.255.0, et la passerelle par défaut 192.168.1.1.




Pour le PC-C, j'ai défini l'adresse IPv4 à 192.168.1.33, le masque de sous-réseau à 255.255.255.0, et la passerelle par défaut à 192.168.1.3.

Ces configurations ont été réalisées en mode statique pour assurer une connectivité stable et cohérente sur le réseau.




4.4.3 Initialisez et redémarrez les routeurs et les commutateurs selon les besoins.

 R1


Physical Config CLI Attributes

```
!
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.0
 clock rate 128000
!
```

 R2

Physical Config CLI Attributes

```
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.0
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.0
 clock rate 128000
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 Loopback1
!
ip flow-export version 9
```

 R3

Physical Config CLI Attributes

```
interface GigabitEthernet0/1
 ip address 192.168.1.3 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 no ip address
 clock rate 2000000
 shutdown
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.0
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
!
ip flow-export version 9
```

J'ai configuré les routes nécessaires sur chaque routeur pour assurer une communication optimale entre les différents sous-réseaux.

Configuration sur R1 :

```
R1(config)#router rip
R1(config-router)#network 10.0.0.0
R1(config-router)#network 192.168.1.0
```

Configuration sur R2 :





```
R2(config)#router rip
R2(config-router)#network 192.168.1.0
R2(config-router)#network 10.0.0.0
R2(config-router)#network 209.165.200.0
```

Configuration sur R3

```
R3(config)#router rip
R3(config-router)#network 192.168.1.0
R3(config-router)#network 10.0.0.0
```

Ces routes dynamiques permettent à chaque routeur de connaître le chemin pour atteindre les sous-réseaux connectés aux autres routeurs. Après cette configuration, j'ai redémarré les routeurs et les commutateurs pour appliquer les modifications.

Puis, j'ai testé la connectivité entre PC-A et R2, de même pour PC-C.

Fire	Last Status	Source	Destination	Type	Color
	Successful	PC-A	R2	ICMP	
	Successful	PC-C	R2	ICMP	

4.4.4 Configuration des paramètres de base pour chaque routeur.

J'ai appliqué les configurations suivantes sur chaque routeur pour respecter les exigences de l'exercice :

Désactivation de la recherche DNS

Sur R1, R2, et R3, j'ai désactivé la recherche DNS pour éviter les délais lors des erreurs de commande :

```
R1(config)#no ip domain-lookup
R2(config)#no ip domain-lookup
R3(config)#no ip domain-lookup
R1(config)#no ip domain-lookup
R2(config)#no ip domain-lookup
R3(config)#no ip domain-lookup
```

Configuration des noms des périphériques

J'ai configuré le nom des routeurs en fonction de la topologie :

```
R1(config)#hostname R1
R2(config)#hostname R2
R3(config)#hostname R3
R1(config)#hostname R1
```

Configuration des adresses IP

Sur **R1** :

```
R1(config)#interface gigabitEthernet 0/1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
```

```
R1(config)#interface serial 0/0/0
R1(config-if)#ip address 10.1.1.1 255.255.255.252
R1(config-if)#clock rate 128000
R1(config-if)#no shutdown
```

Sur **R2** :

```
R2(config)#interface serial 0/0/0
R2(config-if)#ip address 10.1.1.2 255.255.255.252
R2(config-if)#no shutdown
```

```
R2(config)#interface serial 0/0/1
R2(config-if)#ip address 10.2.2.2 255.255.255.252
R2(config-if)#clock rate 128000
R2(config-if)#no shutdown
```

Sur **R3** :

```
R3(config)#interface gigabitEthernet 0/1
R3(config-if)#ip address 192.168.1.3 255.255.255.0
R3(config-if)#no shutdown
```

```
R3(config)#interface serial 0/0/1
R3(config-if)#ip address 10.2.2.1 255.255.255.252
R3(config-if)#clock rate 128000
R3(config-if)#no shutdown
```

Configuration des mots de passe

J'ai configuré le mot de passe pour le mode privilégié (class), le mot de passe de console et les accès VTY (cisco), avec la commande logging synchronous pour éviter l'interruption des commandes par les messages de console.

Sur chaque routeur :

```
enable secret class
line con 0
password cisco
login
logging synchronous
line vty 0 4
password cisco
login
logging synchronous
```


Sauvegarde de la configuration

J'ai sauvegardé la configuration en cours en tant que configuration de démarrage :

```
copy running-config startup-config
R1#copy running-config startup-config
Destination filename [startup-config]
Building configuration...
[OK]
```

Ces configurations garantissent que les paramètres de base des routeurs sont correctement appliqués et sauvegardés.

4.4.5 Configuration des paramètres de base pour chaque commutateur.

Configuration de S1

J'ai configuré le commutateur S1 avec les paramètres de base suivants :

```
S1>enable
S1#configure terminal
S1(config)#no ip domain-lookup
S1(config)#hostname S1
S1(config)#enable secret class

S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.1.11 255.255.255.0
S1(config-if)#no shutdown
S1(config)#ip default-gateway 192.168.1.1
```

```
S1(config)#line con 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#logging synchronous
```

```
S1(config)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#logging synchronous
```

```
S1#copy running-config startup-config
```

Configuration de S3

J'ai configuré le commutateur S3 avec les paramètres de base suivants :

```
S3>enable
S3#configure terminal
S3(config)#no ip domain-lookup
S3(config)#hostname S3
S3(config)#enable secret class
```

```
S3(config)#interface vlan 1
S3(config-if)#ip address 192.168.1.13 255.255.255.0
```

```
S3(config-if)#no shutdown  
S3(config)#ip default-gateway 192.168.1.3
```

```
S3(config)#line con 0  
S3(config-line)#password cisco  
S3(config-line)#login  
S3(config-line)#logging synchronous
```

```
S3(config)#line vty 0 4  
S3(config-line)#password cisco  
S3(config-line)#login  
S3(config-line)#logging synchronous
```

```
S3#copy running-config startup-config
```

Explication des commandes appliquées







1. **Désactivation de la recherche DNS :**
no ip domain-lookup permet d'éviter les délais causés par les erreurs de commande.
2. **Nom du périphérique :**
hostname S1 ou hostname S3 définit le nom des commutateurs conformément à la topologie.
3. **Mot de passe du mode privilégié :**
enable secret class définit le mot de passe chiffré pour le mode privilégié.
4. **Adresse IP de l'interface VLAN 1 :**
interface vlan 1 permet d'attribuer une adresse IP pour la gestion du commutateur.
5. **Passerelle par défaut :**
ip default-gateway configure la passerelle par défaut pour l'accès au réseau.
6. **Mot de passe de console et VTY :**
password cisco et login activent l'authentification pour la console et les sessions VTY.
7. **Logging synchronous :**
Évite l'interruption des commandes par les messages de console.
8. **Sauvegarde de la configuration :**
copy running-config startup-config sauvegarde la configuration pour la conserver après un redémarrage.

4.4.6 Vérification de la connectivité entre PC-A et PC-C.

Les requêtes ping entre **PC-A** et **PC-C** ont abouti avec succès. Le statut des tests ICMP montre que la communication est établie correctement entre les périphériques suivants :

- **De PC-A vers PC-C :** Connectivité réussie.
- **De PC-A vers R2 :** Connectivité réussie.
- **De PC-C vers R2 :** Connectivité réussie.

La configuration de base est correcte, et aucun problème de connectivité n'a été détecté.

Fire	Last Status	Source	Destination	Type	Col
	Successful	PC-A	PC-C	ICMP	
	Successful	PC-A	R2	ICMP	
	Successful	PC-C	R2	ICMP	

4.4.7 Configuration du protocole RIP et du routage par défaut

Configuration du protocole RIP

J'ai configuré le protocole RIP sur les routeurs R1, R2, et R3 avec l'ID de processus 1, en ajoutant tous les réseaux sauf 209.165.200.224/27.

Sur R1 :

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 192.168.1.0
R1(config-router)#network 10.0.0.0
```

Sur R2 :

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 192.168.1.0
R2(config-router)#network 10.0.0.0
```

Sur R3 :

```
R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#network 192.168.1.0
R3(config-router)#network 10.0.0.0
```

Configuration d'une route par défaut sur R2

Sur R2, j'ai configuré une route par défaut en utilisant l'interface Loopback1 comme sortie vers le réseau 209.165.200.224/27.

```
R2(config)#ip route 0.0.0.0 0.0.0.0 Loopback1
```

Redistribution de la route par défaut dans le processus RIP sur R2

J'ai redistribué la route par défaut dans le processus RIP en utilisant la commande default-information originate :

```
R2(config)#router rip
R2(config-router)#default-information originate
```

4.4.8 Vérification de la connectivité.

La connectivité a été vérifiée avec succès depuis R2 :

1. Ping vers 10.1.1.2 : Réussi avec un taux de succès de 100 % (5/5).

2. Ping vers 10.2.2.2 : Réussi avec un taux de succès de 100 % (5/5).

Les temps de réponse montrent des valeurs normales, indiquant une latence acceptable :

- 10.1.1.2 : Temps de réponse min/avg/max = 7/10/18 ms.
- 10.2.2.2 : Temps de réponse min/avg/max = 5/8/10 ms.

Ces résultats confirment que la connectivité entre les interfaces des routeurs est pleinement fonctionnelle.

```
R2#ping 10.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 7/10/18 ms

R2#ping 10.2.2.2









Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/8/10 ms

R2#
```

Depuis PC-A

Les résultats montrent que les requêtes ping depuis PC-A vers toutes les interfaces sur R1, R2, R3, et PC-C ont abouti avec succès. Cela signifie que :









- La connectivité de PC-A vers R1 est établie.
- La connectivité de PC-A vers R2 est établie.
- La connectivité de PC-A vers R3 est établie.
- La connectivité de PC-A vers PC-C est établie.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC-A	R1	ICMP		0.000	N	0	(edit)	
	Successful	PC-A	R2	ICMP		0.000	N	1	(edit)	
	Successful	PC-A	R3	ICMP		0.000	N	2	(edit)	
	Successful	PC-A	PC-C	ICMP		0.000	N	3	(edit)	

Depuis PC-C

Les résultats montrent que les requêtes ping depuis PC-C vers toutes les interfaces sur R1, R2, R3, et PC-A ont également abouti avec succès. Cela signifie que :

- La connectivité de PC-C vers R1 est établie.
- La connectivité de PC-C vers R2 est établie.
- La connectivité de PC-C vers R3 est établie.
- La connectivité de PC-C vers PC-A est établie.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC-C	R3	ICMP		0.000	N	0	(edit)	
	Successful	PC-C	R2	ICMP		0.000	N	1	(edit)	
	Successful	PC-C	R1	ICMP		0.000	N	2	(edit)	
	Successful	PC-C	PC-A	ICMP		0.000	N	3	(edit)	

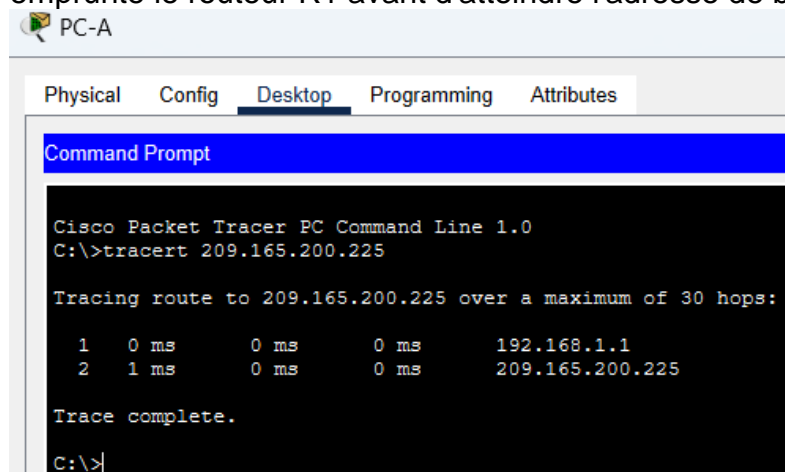
4.5 Configuration de la redondance au premier saut avec HSRP

Bien que la topologie ait été conçue avec une certaine redondance (deux routeurs et deux commutateurs sur le même LAN), PC-A et PC-C sont tous deux configurés avec une seule adresse de passerelle. PC-A utilise le routeur R1 et PC-C utilise le routeur R3. En cas de désactivation de l'un de ces routeurs ou des interfaces sur les routeurs, le PC pourrait perdre sa connexion à Internet.

Dans la Partie 2, je vais tester le comportement du réseau avant et après la configuration du protocole HSRP. Pour cela, je vais déterminer le chemin emprunté par les paquets vers l'adresse de bouclage sur R2.

4.5.1 Détermination du chemin du trafic Internet pour PC-A et PC-C.

Pour PC-A, après avoir exécuté la commande `tracert` vers 209.165.200.225, les paquets sont passés par l'adresse 192.168.1.1. Cela signifie que le chemin suivi emprunte le routeur R1 avant d'atteindre l'adresse de bouclage de R2.



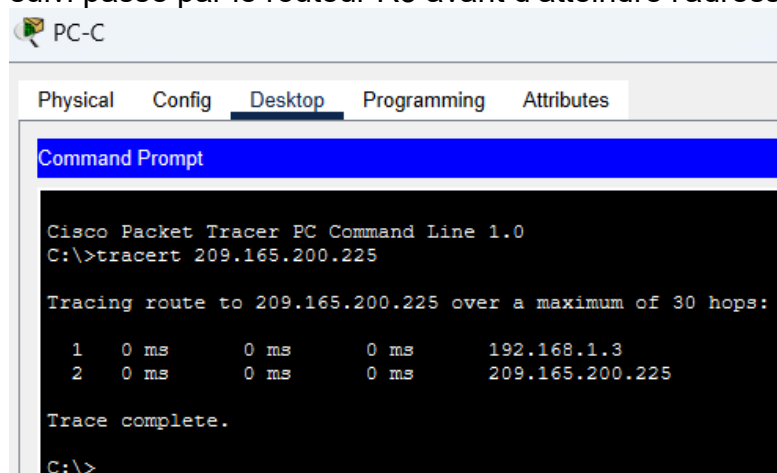
```
Cisco Packet Tracer PC Command Line 1.0
C:\>tracert 209.165.200.225

Tracing route to 209.165.200.225 over a maximum of 30 hops:

  1  0 ms    0 ms    0 ms    192.168.1.1
  2  1 ms    0 ms    0 ms    209.165.200.225

Trace complete.
C:\>
```

Pour PC-C, en exécutant également la commande `tracert` vers 209.165.200.225, les paquets sont passés par l'adresse 192.168.1.3. Ainsi, le chemin suivi passe par le routeur R3 avant d'atteindre l'adresse de bouclage de R2.



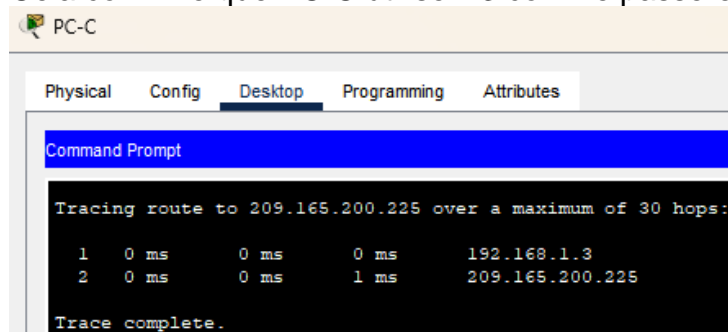
```
Cisco Packet Tracer PC Command Line 1.0
C:\>tracert 209.165.200.225

Tracing route to 209.165.200.225 over a maximum of 30 hops:

  1  0 ms    0 ms    0 ms    192.168.1.3
  2  0 ms    0 ms    0 ms    209.165.200.225

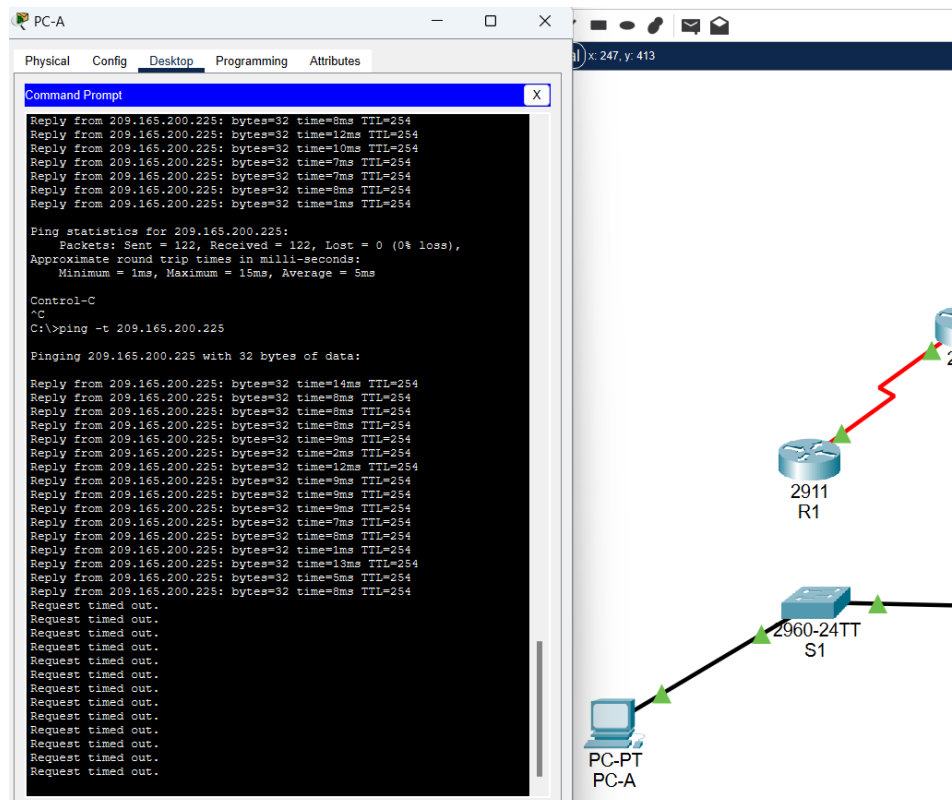
Trace complete.
C:\>
```

À partir de PC-C, la commande `tracert` vers l'adresse de bouclage 209.165.200.225 de R2 montre que les paquets ont emprunté deux sauts. Le premier saut est passé par l'adresse 192.168.1.3, correspondant au routeur R3. Ensuite, le deuxième saut a atteint directement l'adresse de bouclage 209.165.200.225 sur R2. Cela confirme que PC-C utilise R3 comme passerelle pour accéder au réseau.

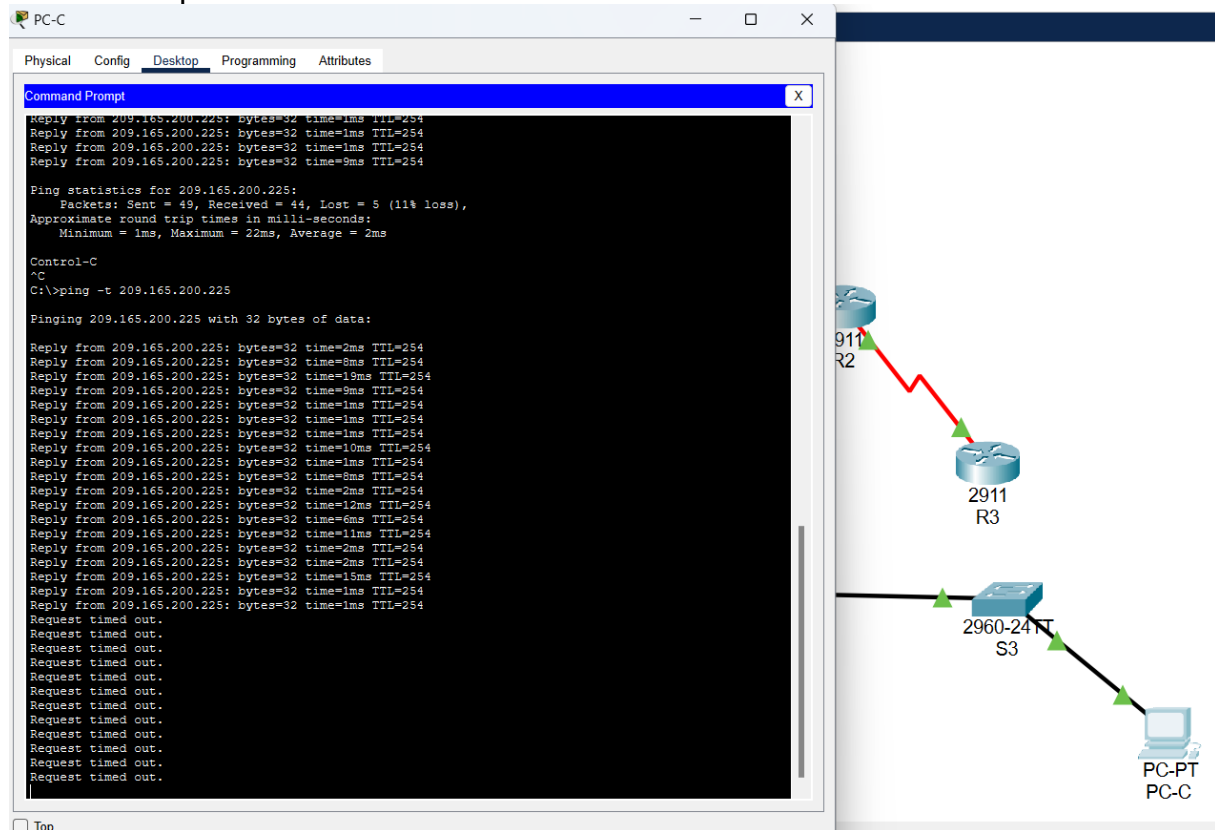


4.5.2 Session ping sur PC-A et rompez la connexion entre S1 et R1 et S2 et R2.

Lorsque la commande ping -t est en cours d'exécution depuis PC-A vers l'adresse 209.165.200.225 et que le câble Ethernet connecté à F0/5 sur S1 est déconnecté, le trafic ICMP est interrompu temporairement. Le ping échoue et affiche des messages de "Request timed out". Cela signifie que PC-A a perdu sa connexion avec le réseau en raison de la déconnexion de l'interface sur S1.



Si je répète les étapes 2a et 2b en effectuant un ping -t depuis PC-C vers l'adresse 209.165.200.225 et que je déconnecte le câble Ethernet sur F0/5 de S3, le trafic ICMP sera temporairement interrompu. Les requêtes ping afficheront des messages "Request timed out". Cela se produit parce que PC-C perd sa connexion au réseau lorsque S3 est déconnecté de R3.



Rétablissement de la connectivité

Après avoir reconnecté les câbles Ethernet sur F0/5 de S1 et S3, j'exécute à nouveau les requêtes ping depuis PC-A et PC-C vers 209.165.200.225. La connectivité est alors rétablie, et les réponses ICMP sont de nouveau reçues sans erreur, confirmant le bon fonctionnement du réseau après rétablissement.

4.5.3 Configuration du protocole HSRP sur R1 et R3.

Pour configurer le protocole HSRP sur R1 et R3, j'ai effectué les étapes suivantes pour assurer la redondance au niveau de la passerelle par défaut.

Configuration de HSRP sur R1

Sur R1, j'ai configuré l'interface GigabitEthernet 0/1 avec une priorité élevée pour en faire le routeur actif :

```
R1(config)#interface g0/1
R1(config-if)#standby version 2
R1(config-if)#standby 1 ip 192.168.1.254
R1(config-if)#standby 1 priority 150
```



```
R1(config-if)#standby 1 preempt
R1(config-if)#standby 1 authentication cisco
R1(config-if)#exit
R1(config)#exit
R1#write memory
```

Configuration de HSRP sur R3

Sur R3, j'ai configuré l'interface GigabitEthernet 0/1 avec une priorité par défaut pour en faire le routeur de secours :

```
R3(config)#interface g0/1
R3(config-if)#standby version 2
R3(config-if)#standby 1 ip 192.168.1.254
R3(config-if)#standby 1 priority 100
R3(config-if)#standby 1 preempt
R3(config-if)#standby 1 authentication cisco
R3(config-if)#exit
R3(config)#exit
R3#write memory
```

Vérification de la configuration HSRP

La commande show standby a été utilisée pour vérifier le statut de HSRP sur R1 et R3.

Sur R1, l'interface est en état Active, avec une priorité de 150 :

State is Active

Virtual IP address is 192.168.1.254

Active router is local

Standby router is 192.168.1.3, priority 100

```
R1#show standby
GigabitEthernet0/1 - Group 1
  State is Active
    18 state changes, last state change 00:23:49
  Virtual IP address is 192.168.1.254
  Active virtual MAC address is 0000.0C07.AC01
    Local virtual MAC address is 0000.0C07.AC01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.371 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.1.3, priority 100 (expires in 7 sec)
  Priority 110 (configured 110)
  Group name is hsrp-Gig0/1-1 (default)
R1#
```

Sur R3, l'interface est en état Standby, avec une priorité de 100 :

State is Standby

Virtual IP address is 192.168.1.254

Active router is 192.168.1.1, priority 150


```
R3#show standby
GigabitEthernet0/1 - Group 1
  State is Standby
    23 state changes, last state change 00:27:47
  Virtual IP address is 192.168.1.254
  Active virtual MAC address is 0000.0C07.AC01
    Local virtual MAC address is 0000.0C07.AC01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.146 secs
  Preemption enabled
  Active router is 192.168.1.1, priority 110 (expires in 8 sec)
    MAC address is 0000.0C07.AC01
  Standby router is local
  Priority 100 (default 100)
  Group name is hsrp-Gig0/1-1 (default)
R3#
```

Réponses aux questions sur HSRP

Quel routeur est le routeur actif ?

Le routeur actif est R1, comme indiqué par l'état "State is Active" sur l'interface GigabitEthernet0/1 de R1.

Quelle est l'adresse MAC pour l'adresse IP virtuelle ?

L'adresse MAC associée à l'adresse IP virtuelle 192.168.1.254 est 0000.0C07.AC01, comme indiqué sous "Active virtual MAC address".

Quelles sont l'adresse IP et la priorité du routeur en veille ?

L'adresse IP du routeur en veille est 192.168.1.3. La priorité du routeur en veille est 100, comme indiqué sous "Standby router".

4.5.4 Résultats des étapes HSRP et ping

Résultat de la commande show standby brief

Sur R1, le routeur affiche l'état Active pour le groupe 1 avec une priorité de 150. L'adresse IP virtuelle est 192.168.1.254, et le routeur en veille est 192.168.1.3 (R3).

Sur R3, le routeur affiche l'état Standby pour le groupe 1 avec une priorité de 100. L'adresse IP virtuelle est également 192.168.1.254, et le routeur actif est 192.168.1.1 (R1).

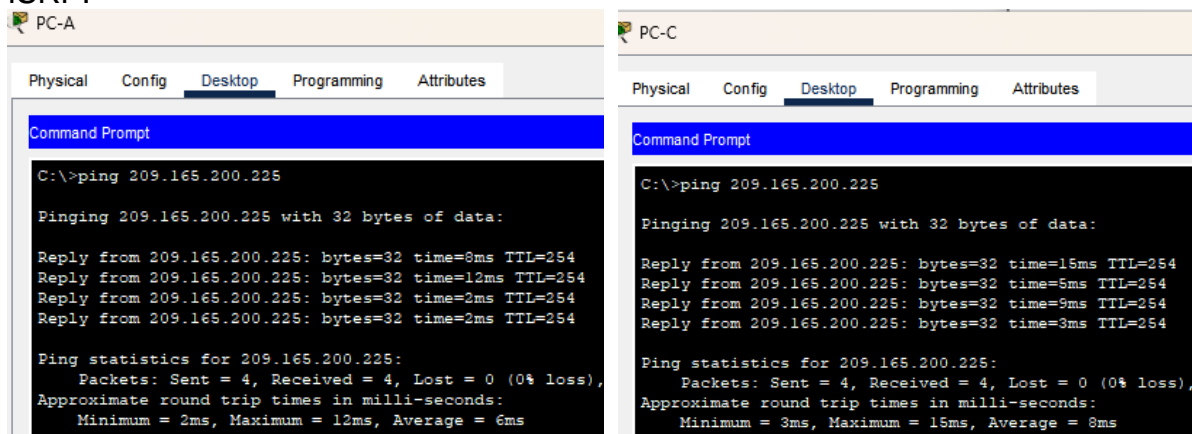
```
R3# show standby brief
                P indicates configured to preempt.
                |
Interface   Grp  Pri P State      Active        Standby        Virtual IP
Gig0/1      1    100 P Standby    192.168.1.1   local          192.168.1.254
R3#
```

Modification de l'adresse de passerelle par défaut

Pour garantir la redondance avec HSRP, j'ai modifié l'adresse de passerelle par défaut sur PC-A, PC-C, S1, et S3 en utilisant l'adresse IP virtuelle 192.168.1.254.

Vérification des paramètres avec une requête ping

Après avoir configuré l'adresse de passerelle par défaut, j'ai envoyé une requête ping depuis PC-A et PC-C vers l'adresse de bouclage 209.165.200.225 de R2. Les requêtes ping ont réussi, comme le montrent les statistiques de 0 % de perte de paquets. La connectivité est donc correctement assurée grâce à la configuration de HSRP.



The image shows two side-by-side screenshots of network device command prompts. The left screenshot is from PC-A and the right is from PC-C. Both show a successful ping to the address 209.165.200.225. The PC-A prompt shows four replies with times of 8ms, 12ms, 2ms, and 2ms, and statistics showing 0% loss. The PC-C prompt shows four replies with times of 15ms, 5ms, 9ms, and 3ms, and statistics showing 0% loss.

```
C:\>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Reply from 209.165.200.225: bytes=32 time=8ms TTL=254
Reply from 209.165.200.225: bytes=32 time=12ms TTL=254
Reply from 209.165.200.225: bytes=32 time=2ms TTL=254
Reply from 209.165.200.225: bytes=32 time=2ms TTL=254

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 12ms, Average = 6ms
```

```
C:\>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

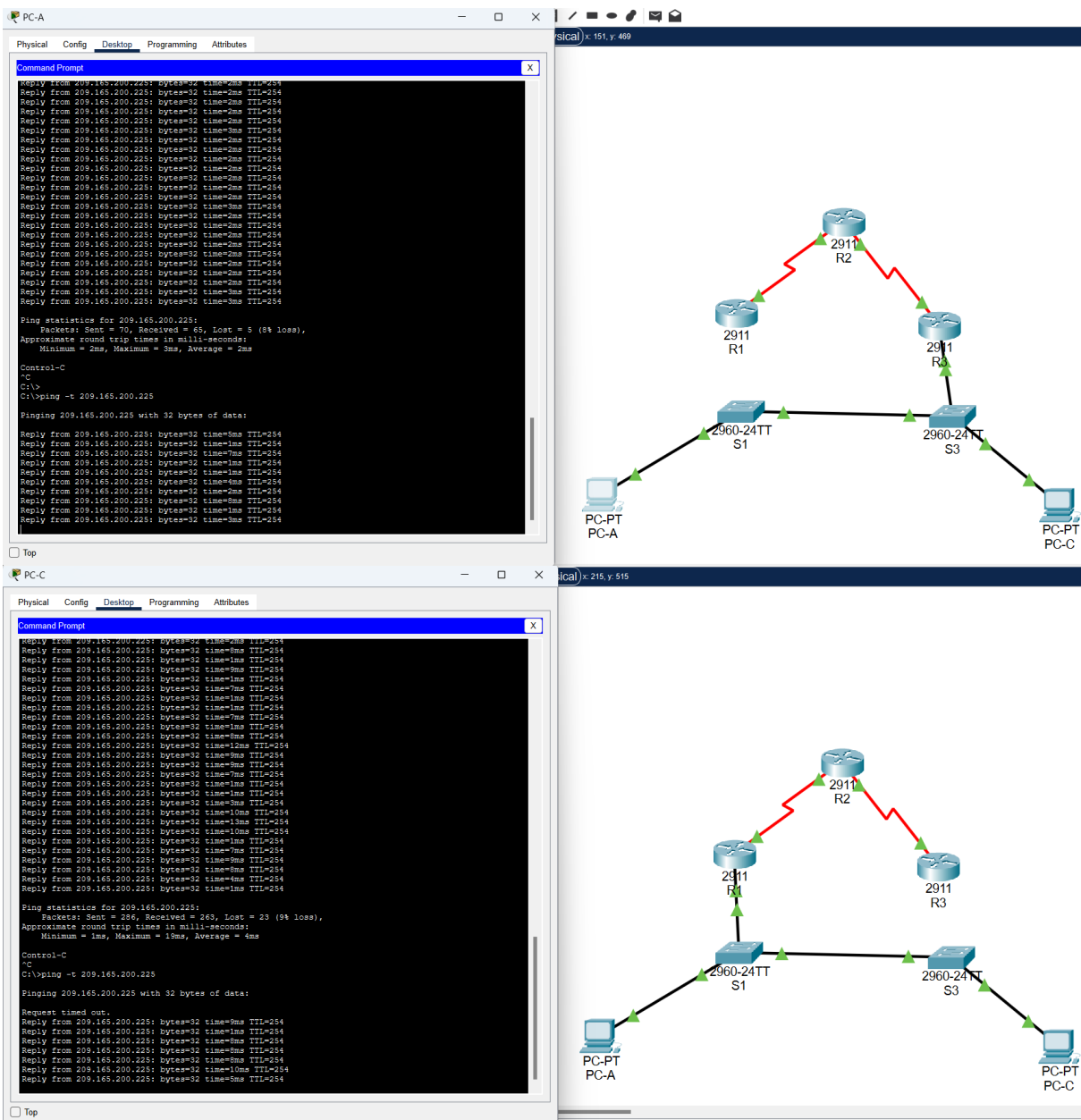
Reply from 209.165.200.225: bytes=32 time=15ms TTL=254
Reply from 209.165.200.225: bytes=32 time=5ms TTL=254
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
Reply from 209.165.200.225: bytes=32 time=3ms TTL=254

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 15ms, Average = 8ms
```

4.5.5 Résultat de la déconnexion du commutateur lié à R1.

Lorsque la commande ping -t a été exécutée depuis PC-A vers l'adresse 209.165.200.225 et que le câble Ethernet connecté à F0/5 sur S1 a été déconnecté, le trafic ICMP a continué à s'effectuer sans interruption. Les pings ont été reçus avec succès et il n'y a eu aucune perte de paquets. De même, PC-C a continué à communiquer avec succès, avec R1 reprenant le rôle de routeur actif.

Le protocole HSRP a assuré une transition fluide vers R3, permettant à ce dernier de prendre le relais comme routeur actif pour PC-A. Cela confirme que la redondance est correctement configurée et que le basculement fonctionne parfaitement, maintenant ainsi la connectivité réseau sans interruption pour l'ensemble des périphériques.



4.5.6 Vérification des paramètres du protocole HSRP sur R1 et R3.

Quel routeur est le routeur actif après l'exécution de la commande show standby brief ?

D'après les résultats de la commande `show standby brief` :

- Sur R1 : L'état de l'interface GigabitEthernet0/1 est en mode Init, et l'état du routeur actif est unknown. Cela indique que R1 n'est pas le routeur actif à ce moment-là.
- Sur R3 : L'interface GigabitEthernet0/1 est en état Active, ce qui signifie que R3 est le routeur actif à ce moment précis.

```
R1#show standby brief
                P indicates configured to preempt.
                |
Interface   Grp  Pri P State      Active      Standby      Virtual IP
Gig0/1      1    110 P Init       unknown    unknown      192.168.1.254
R1#
```

```
R3#show standby brief
                P indicates configured to preempt.
                |
Interface   Grp  Pri P State      Active      Standby      Virtual IP
Gig0/1      1    100 P Active    local      unknown      192.168.1.254
R3#
```

Quel est le routeur actif après avoir reconnecté le câble ou activé l'interface F0/5 ?

Après avoir reconnecté le câble ou activé l'interface F0/5 :

- Sur R3 : La commande show standby brief montre que R3 est passé en état Standby, avec R1 en tant que routeur actif.
- Sur R1 : L'interface GigabitEthernet0/1 de R1 est maintenant en état Active avec une priorité de 110, ce qui en fait le routeur actif.

```
R3#show standby brief
                P indicates configured to preempt.
                |
Interface   Grp  Pri P State      Active      Standby      Virtual IP
Gig0/1      1    100 P Standby    192.168.1.1 local      192.168.1.254
R3#
```

```
R1#show standby brief
                P indicates configured to preempt.
                |
Interface   Grp  Pri P State      Active      Standby      Virtual IP
Gig0/1      1    110 P Active    local      192.168.1.3  192.168.1.254
R1#
```

4.5.7 Modifiez les priorités HSRP.

Définition de la priorité HSRP sur 200 sur R3

Après avoir défini la priorité HSRP sur 200 pour R3, le routeur R3 devient le routeur actif. Cela est confirmé par la commande show standby brief, qui indique que R3 est en état Active et R1 en état Standby.

Commande pour définir le routeur actif sur R3 sans modifier la priorité

Pour forcer R3 à devenir le routeur actif sans changer la priorité, j'ai utilisé la commande suivante sur R3 :

R3(config-if)#standby 1 preempt

Cette commande permet à R3 de prendre le rôle de routeur actif si aucune condition prioritaire ne l'empêche.

```
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#interface GigabitEthernet0/1
R3(config-if)#standby 1 priority 200
R3(config-if)#standby 1 preempt
R3(config-if)#standby 1 authentication cisco
R3(config-if)#
% Invalid input detected at '^' marker.

R3(config-if)#exit
R3(config)#exit
R3#write memory
Building configuration...
[OK]
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#
%HSRP-6-STATECHANGE: GigabitEthernet0/1 Grp 1 state Standby -> Active
```

Vérification avec show standby brief

La commande show standby brief montre que R3 est le routeur actif :

```
R1#show standby brief
                P indicates configured to preempt.
                |
Interface      Grp  Pri P State      Active          Standby          Virtual IP
Gig0/1         1    110 P Standby    192.168.1.3     local            192.168.1.254
R1#
R3#show standby brief
                P indicates configured to preempt.
                |
Interface      Grp  Pri P State      Active          Standby          Virtual IP
Gig0/1         1    200 P Active     local           192.168.1.1     192.168.1.254
R3#
```

4.5.8 Remarques générales

a) Pourquoi une redondance serait-elle nécessaire dans un LAN ?

La redondance dans un LAN est essentielle pour maintenir la disponibilité du réseau en cas de défaillance d'un périphérique ou d'un lien. Elle permet de minimiser les interruptions de service en assurant un basculement automatique vers un équipement ou un chemin de secours, ce qui garantit que la connectivité reste opérationnelle même en cas de panne.

De plus, elle améliore la tolérance aux pannes en éliminant les points de défaillance uniques, ce qui augmente la résilience du réseau. La redondance peut également contribuer à l'optimisation de la répartition de charge, en équilibrant le trafic entre plusieurs chemins ou équipements, ce qui améliore les performances et la fluidité globale du réseau. En résumé, une redondance bien conçue garantit un réseau fiable, performant et résistant aux interruptions imprévues.

4.5.9 Tableau récapitulatif des interfaces des routeurs

Résumé des interfaces des routeurs					
Modèle du routeur	Interface Ethernet 1	Interface Ethernet 2	Interface série 1		Interface série 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial (S0/0/0)	0/0/0	Serial (S0/0/1) 0/0/1
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial (S0/0/0)	0/0/0	Serial (S0/0/1) 0/0/1
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial (S0/1/0)	0/1/0	Serial (S0/1/1) 0/1/1
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial (S0/0/0)	0/0/0	Serial (S0/0/1) 0/0/1

2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial (S0/0/0)	0/0/0	Serial (S0/0/1)	0/0/1
<p>Remarque : pour savoir comment le routeur est configuré, observez les interfaces afin d'identifier le type de routeur ainsi que le nombre d'interfaces qu'il comporte. Il n'est pas possible de répertorier de façon exhaustive toutes les combinaisons de configurations pour chaque type de routeur. Ce tableau inclut les identifiants des différentes combinaisons d'interfaces Ethernet et séries possibles dans le périphérique. Ce tableau ne comporte aucun autre type d'interface, même si un routeur particulier peut en contenir un. L'exemple de l'interface RNIS BRI peut illustrer ceci. La chaîne de caractères entre parenthèses est l'abréviation normalisée qui permet de représenter l'interface dans les commandes Cisco IOS.</p>						

4.6 Configuration HSRP avec répartition de charges sur R1 et R3

Pour assurer une redondance avec répartition de charges, j'ai configuré R1 et R3 avec deux groupes HSRP différents. Cela permet de distribuer le trafic entre les deux routeurs tout en maintenant la redondance en cas de défaillance.

Configuration de R1 :

```
R1# configure terminal
R1(config)# interface GigabitEthernet0/1
R1(config-if)# standby 1 ip 192.168.1.254
R1(config-if)# standby 1 priority 150
R1(config-if)# standby 1 preempt
R1(config-if)# standby 1 authentication cisco

R1(config-if)# standby 2 ip 192.168.1.253
R1(config-if)# standby 2 priority 100
R1(config-if)# standby 2 preempt
R1(config-if)# standby 2 authentication cisco

R1(config-if)# exit
R1(config)# exit
R1# write memory
```

Configuration de R3 :

```
R3# configure terminal
R3(config)# interface GigabitEthernet0/1
R3(config-if)# standby 1 ip 192.168.1.254
R3(config-if)# standby 1 priority 100
R3(config-if)# standby 1 preempt
R3(config-if)# standby 1 authentication cisco

R3(config-if)# standby 2 ip 192.168.1.253
R3(config-if)# standby 2 priority 150
R3(config-if)# standby 2 preempt
```

```
R3(config-if)# standby 2 authentication cisco
```

```
R3(config-if)# exit
```

```
R3(config)# exit
```

```
R3# write memory
```

Explication des configurations

Groupe 1 utilise l'adresse IP virtuelle **192.168.1.254** :

- **R1** est configuré avec une priorité de **150**, ce qui en fait le routeur actif pour le groupe 1.
- **R3** est en mode veille avec une priorité de **100** pour le groupe 1.

Groupe 2 utilise l'adresse IP virtuelle **192.168.1.253** :

- **R3** est configuré avec une priorité de **150**, ce qui en fait le routeur actif pour le groupe 2.
- **R1** est en mode veille avec une priorité de **100** pour le groupe 2.

4.7 Validation de la répartition de charges en mode Round Robin avec HSRP

J'ai configuré deux groupes HSRP sur R1 et R3, avec les adresses IP virtuelles 192.168.1.254 et 192.168.1.253. Pour le groupe 1, j'ai observé que R3 est en mode actif avec une priorité de 200, tandis que R1 est en mode veille avec une priorité de 110. Pour le groupe 2, R1 est en mode actif avec une priorité de 150, tandis que R3 est en mode veille avec une priorité de 100.

J'ai analysé les paquets HSRP "Hello" envoyés par les deux routeurs, ce qui m'a permis de confirmer leurs statuts respectifs d'actif et de veille pour chaque groupe. J'ai constaté que le trafic est bien réparti entre R1 et R3 grâce à l'alternance des groupes configurés. Cela valide que le protocole HSRP fonctionne en mode Round Robin et permet une répartition de charges efficace entre les deux routeurs, tout en maintenant une redondance complète du réseau.

```
R1#debug standby packets
HSRP Packets debugging is on
R1#HSRP: Gig0/1 Grp 1 Hello out 192.168.1.1 Standby pri 110 vIP 192.168.1.254
R1#HSRP: Gig0/1 Grp 1 Hello out 192.168.1.1 Standby pri 110 vIP 192.168.1.254
R1#HSRP: Gig0/1 Grp 1 Hello out 192.168.1.1 Standby pri 110 vIP 192.168.1.254
R1#HSRP: Gig0/1 Grp 1 Hello out 192.168.1.1 Standby pri 110 vIP 192.168.1.254
```

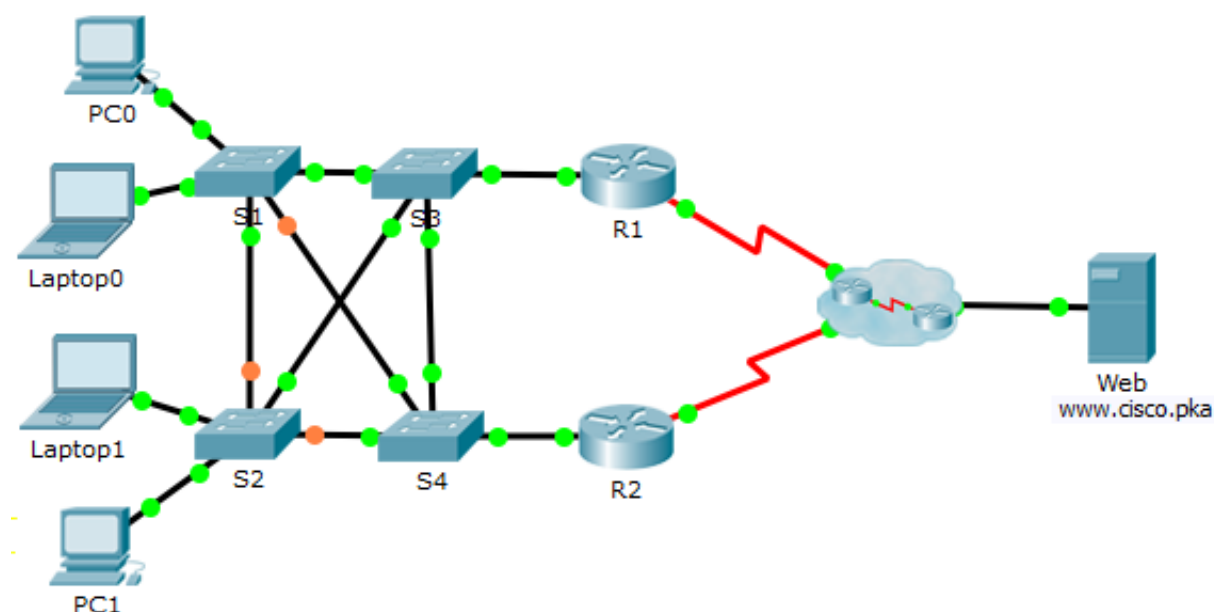
```
R3#debug standby packets
HSRP Packets debugging is on
R3#HSRP: Gig0/1 Grp 1 Hello out 192.168.1.3 Active pri 200 vIP 192.168.1.254
R3#HSRP: Gig0/1 Grp 1 Hello out 192.168.1.3 Active pri 200 vIP 192.168.1.254
R3#HSRP: Gig0/1 Grp 1 Hello out 192.168.1.3 Active pri 200 vIP 192.168.1.254
R3#
R3#HSRP: Gig0/1 Grp 1 Hello out 192.168.1.3 Active pri 200 vIP 192.168.1.254
```


5 Exercice 3 : Packet Tracer – Dépannage du protocole HSRP

J'ai utilisé le fichier :

[Bloc2_sem3-4_atelier-04_redondance_Troubleshoot_HSRP.pka](#)

5.1 Topologie



5.2 Table d'adressage

Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0	209.165.200.226	255.255.255.252	N/A
R2	G0/1	192.168.1.2	255.255.255.0	N/A
	S0/0/1	209.165.200.230	255.255.255.252	N/A
PC0	Carte réseau	192.168.1.10	255.255.255.0	192.168.1.254
Laptop0	Carte réseau	192.168.1.11	255.255.255.0	192.168.1.254
Laptop1	Carte réseau	192.168.1.12	255.255.255.0	192.168.1.254
PC1	Carte réseau	192.168.1.13	255.255.255.0	192.168.1.254
Web	Carte réseau	209.165.202.156	255.255.255.224	209.165.202.158

5.3 Objectif

L'objectif est d'identifier et de résoudre les problèmes liés au protocole HSRP sur le réseau. Je dois m'assurer que toutes les configurations respectent les exigences pour garantir une haute disponibilité du réseau.

5.4 Contexte/scénario

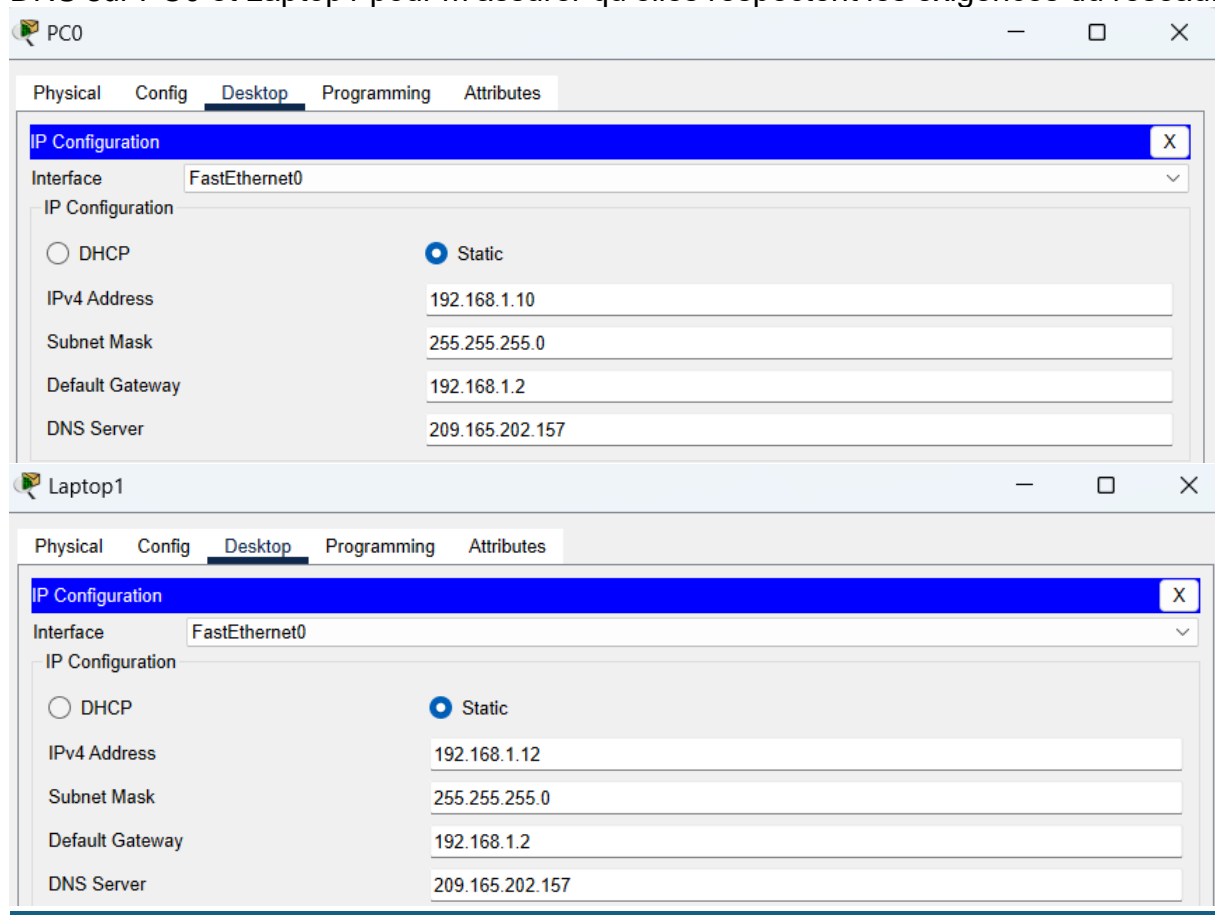
Le réseau utilise le protocole HSRP pour assurer la disponibilité en cas de panne d'un des routeurs. R1 doit toujours être le routeur actif lorsqu'il fonctionne correctement, avec R2 en secours. L'adresse IP virtuelle HSRP est 192.168.1.254, le groupe HSRP est le 1, et l'adresse du serveur DNS est 209.165.202.157. Tous les utilisateurs doivent pouvoir accéder au site www.cisco.pka tant qu'un des routeurs est opérationnel.

5.5 Procédure de dépannage

5.5.1 Ordinateurs de bureau et portables

Vérification de la configuration des ordinateurs de bureau et portables.

J'ai vérifié la configuration des adresses IP, des passerelles par défaut et des serveurs DNS sur PC0 et Laptop1 pour m'assurer qu'elles respectent les exigences du réseau.

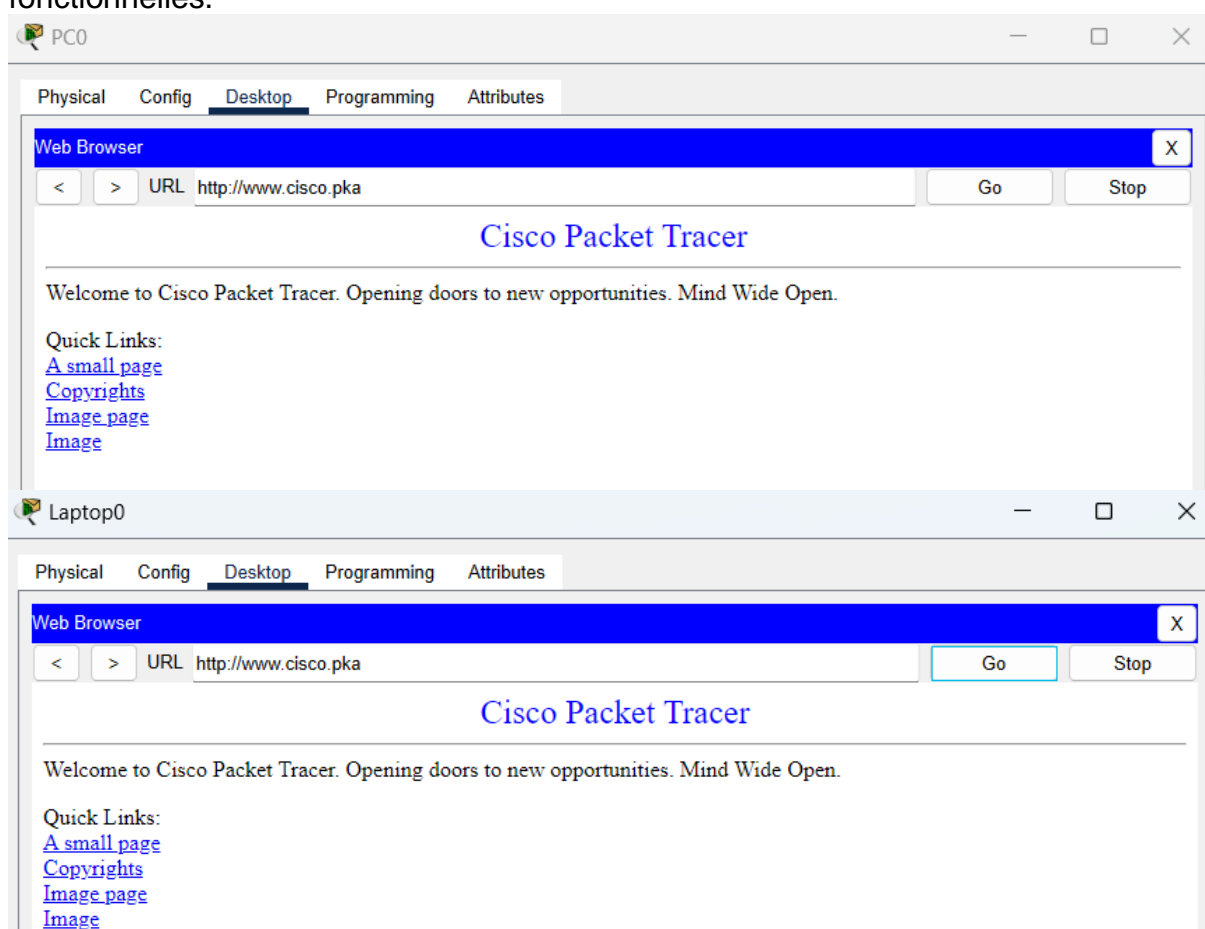


Les configurations de PC0 et Laptop1 sont incorrecte j'ai donc modifier les adresses IP pour qu'il soit dans le même sous-réseau 192.168.1.0/24, les passerelles par défaut pointent vers 192.168.1.2, et les adresses du serveur DNS sont définies sur 209.165.202.157.

Vérification de l'accès à www.cisco.pka

Les captures montrent que PC0 et Laptop0 accèdent correctement au site www.cisco.pka via le navigateur web. Cela confirme que les configurations réseau sont correctes et que le protocole HSRP assure la haute disponibilité.

Les paramètres de passerelle par défaut et de serveur DNS sont correctement appliqués, permettant une résolution de noms et une connectivité réseau fonctionnelles.



5.5.2 Analyse et dépannage de R1

Désactivation de l'interface G0/1 sur R2

Pour simuler une défaillance de R2, j'ai désactivé l'interface GigabitEthernet0/1 sur R2 en utilisant les commandes suivantes :

```
R2(config)# interface GigabitEthernet0/1
```

```
R2(config-if)# shutdown
```

Analyse des problèmes sur R1

Sur R1, après avoir exécuté les commandes show, j'ai identifié plusieurs points nécessitant une attention particulière :

1. Configuration HSRP :

La configuration de HSRP sur R1 montre que le groupe 11 est utilisé avec une priorité de 50, ce qui est trop bas pour assurer que R1 reste le routeur actif en cas de défaillance de R2. L'exigence indique que R1 doit toujours être le routeur actif lorsqu'il fonctionne correctement.

2. Commande incorrecte pour le groupe HSRP :

Le groupe 11 devrait être remplacé par le groupe 1 conformément aux exigences.

Correction des problèmes sur R1

Pour corriger la configuration de HSRP sur R1, j'ai appliqué les modifications suivantes :

```
R1(config)# interface GigabitEthernet0/1
```

```
R1(config-if)# no standby 11 ip 192.168.1.254
```

```
R1(config-if)# no standby 11 priority 50
```

```
R1(config-if)# standby 1 ip 192.168.1.254
```

```
R1(config-if)# standby 1 priority 110
```

```
R1(config-if)# standby 1 preempt
```

Ces commandes configurent le groupe 1 avec une priorité de 110, assurant que R1 est le routeur actif lorsqu'il fonctionne correctement.

Réactivation de l'interface G0/1 sur R2

Pour rétablir la connectivité sur R2, j'ai réactivé l'interface GigabitEthernet0/1 avec la commande suivante :

```
R2(config)# interface GigabitEthernet0/1
```

```
R2(config-if)# no shutdown
```

5.5.3 Dépannage de R2

Désactivation de l'interface G0/1 sur R1

Pour isoler le problème sur R2, j'ai désactivé l'interface GigabitEthernet0/1 sur R1 avec les commandes suivantes :

```
R1(config)# interface GigabitEthernet0/1
```

```
R1(config-if)# shutdown
```

Identification des problèmes sur R2

En exécutant les commandes de diagnostic sur **R2**, j'ai identifié que le problème provient de la configuration du groupe HSRP. **R2** utilise le groupe **111**, alors que le réseau est configuré pour utiliser le groupe **1** conformément aux exigences réseau.

Configuration actuelle sur R2 :

```
interface GigabitEthernet0/1
```

```
standby 111 ip 192.168.1.254
```

```
standby 111 priority 110
```

Correction du problème sur R2

Pour corriger la configuration du groupe HSRP sur R2, j'ai remplacé le groupe 111 par le groupe 1 avec les commandes suivantes :

```
R2(config)# interface GigabitEthernet0/1
R2(config-if)# no standby 111 ip 192.168.1.254
R2(config-if)# no standby 111 priority 110
R2(config-if)# standby 1 ip 192.168.1.254
R2(config-if)# standby 1 priority 100
R2(config-if)# standby 1 preempt
```

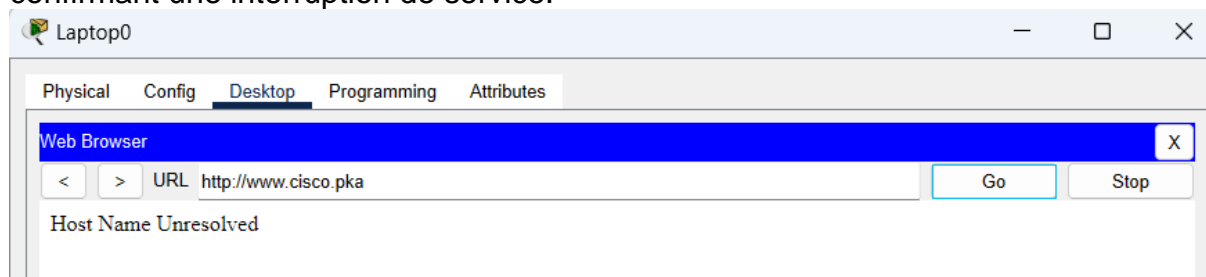
Vérification de la correction

Pour vérifier que R2 est maintenant correctement configuré avec le bon groupe HSRP, j'ai utilisé la commande suivante :

```
R2# show standby brief
```

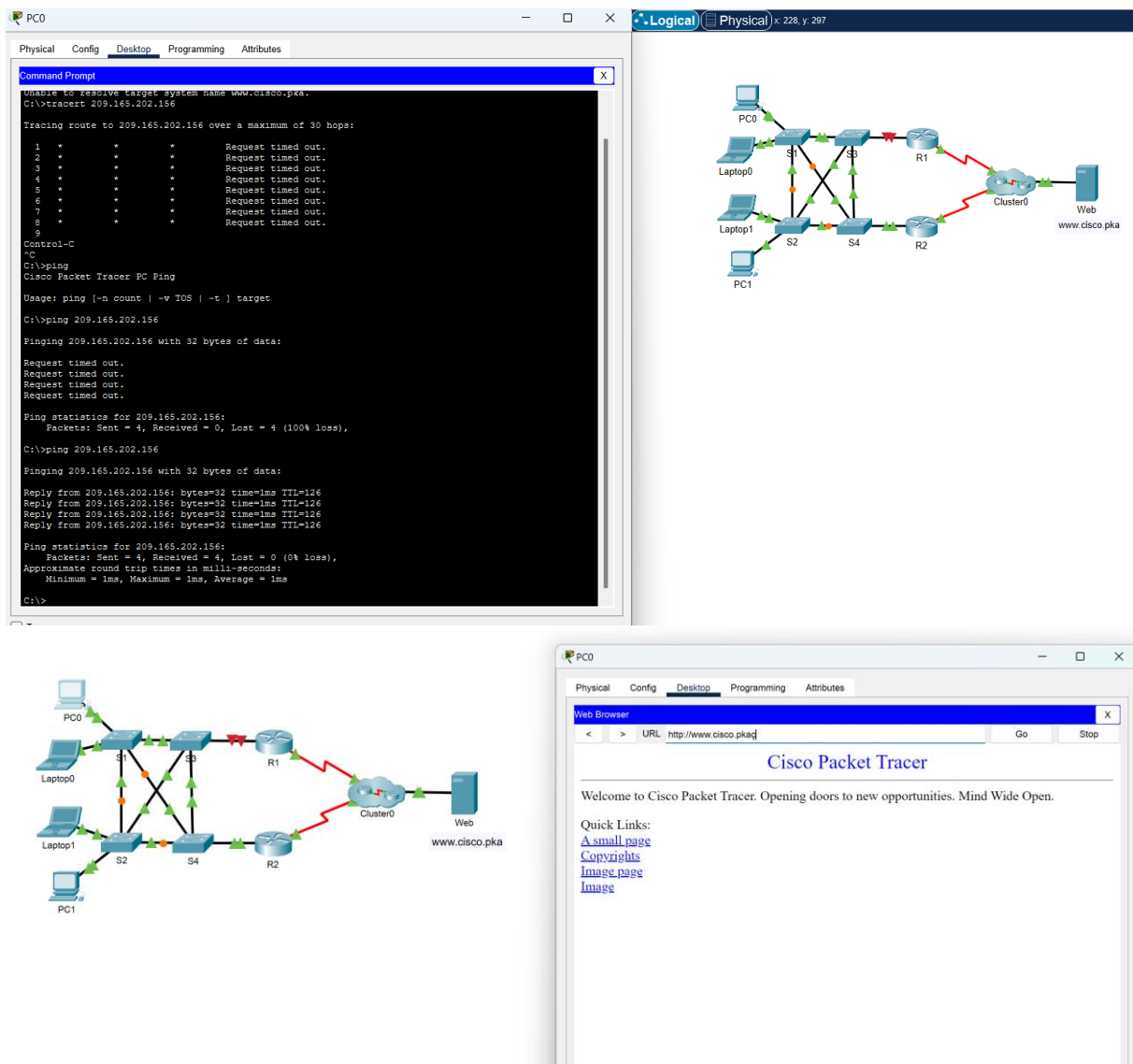
Cela confirme que R2 utilise bien le groupe 1 avec l'adresse IP virtuelle 192.168.1.254 et une priorité de 100.

Avant la mise en place de la redondance avec le protocole HSRP, je ne parvenais pas à accéder au site web www.cisco.pka en cas de défaillance d'un des routeurs. Lorsque l'un des routeurs tombait en panne, les ordinateurs de bureau et les portables perdaient leur connectivité vers le site web, entraînant un message d'erreur indiquant "Host Name Unresolved". Les requêtes ping et tracertr échouaient également, confirmant une interruption de service.



Après avoir configuré correctement HSRP pour assurer la redondance entre R1 et R2, la haute disponibilité du réseau a été garantie. Désormais, lorsque l'un des routeurs est hors service, le second routeur prend automatiquement le relais. Grâce à cette configuration, l'accès au site www.cisco.pka est rétabli de manière transparente, et les utilisateurs peuvent continuer à accéder au site web sans interruption. La redondance mise en place permet ainsi d'assurer une connectivité fiable et continue, même en cas de panne de l'un des équipements du réseau.

Bloc 2 semestre 3 -4 – atelier 5 – Configuration Etherchannel et haute disponibilité sur les switches et les routeurs



The image displays a Cisco Packet Tracer environment. On the left, a Command Prompt window shows the results of a traceroute and ping command to the IP address 209.165.202.156. The traceroute shows a path through several hops, with the final hop being the destination IP. The ping command shows a 100% success rate with a round trip time of approximately 1ms.

On the right, a network diagram is shown. It includes a PC0, Laptop0, Laptop1, PC1, and a Web server. The network is connected via a series of switches (S1, S2, S3, S4) and routers (R1, R2). The Web server is connected to a Cluster0, which is connected to the routers. The network is configured with Etherchannel and HSRP for high availability.

Below the Command Prompt, another network diagram is shown, which is identical to the one on the right. It shows the same topology of devices and connections.

On the right side of the image, a Web Browser window is open, displaying the Cisco Packet Tracer website. The URL is <http://www.cisco.pka>. The page includes a welcome message and quick links to a small page, copyrights, image page, and image.

Réactivation de l'interface G0/1 sur R1

Pour rétablir la connectivité réseau après le dépannage, j'ai réactivé l'interface GigabitEthernet0/1 sur R1 avec la commande suivante :

```
R1(config)# interface GigabitEthernet0/1
```

```
R1(config-if)# no shutdown
```

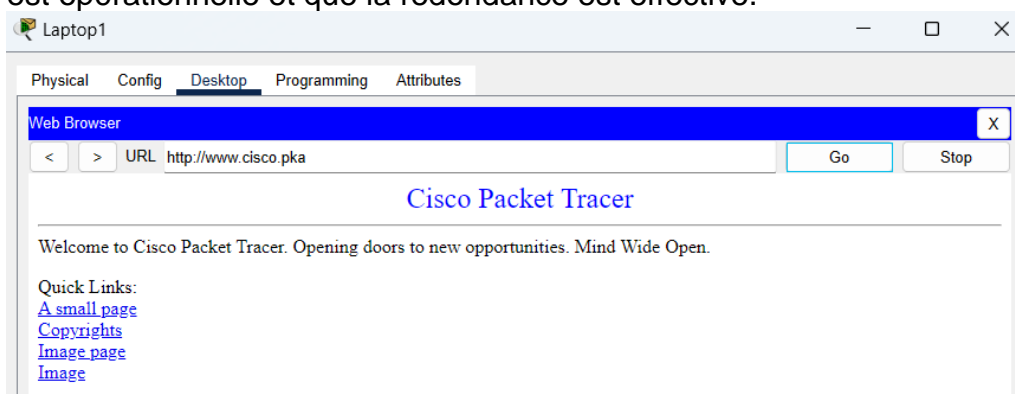
Pour garantir une connectivité réseau stable et vérifier que toutes les exigences du protocole HSRP sont respectées, j'ai suivi ces étapes :

Vérification de la connectivité et des exigences HSRP

J'ai effectué une vérification pour m'assurer que les ordinateurs de bureau et portables peuvent accéder au site www.cisco.pka et que le protocole HSRP est correctement configuré.

Accès à www.cisco.pka

Les tests d'accès montrent que tous les ordinateurs de bureau et portables peuvent se connecter à www.cisco.pka avec succès. Cela confirme que la connectivité réseau est opérationnelle et que la redondance est effective.



Vérification des exigences HSRP

Les résultats des commandes show standby brief indiquent que le protocole HSRP est correctement configuré :

- Sur R1 :
 - L'interface GigabitEthernet0/1 est dans le groupe 1 avec une priorité de 110.
 - L'état est Active, confirmant que R1 est le routeur actif.
 - L'adresse IP virtuelle est 192.168.1.254.
- Sur R2 :
 - L'interface GigabitEthernet0/1 est dans le groupe 1 avec une priorité par défaut de 100.
 - L'état est Standby, indiquant que R2 est prêt à prendre le relais en cas de défaillance de R1.
 - L'adresse IP virtuelle est également 192.168.1.254.

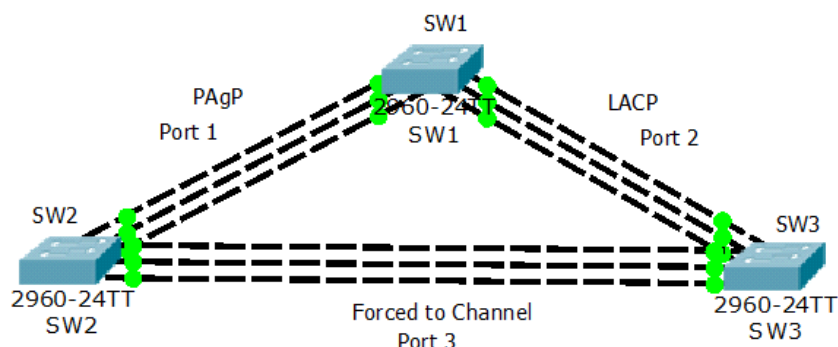
```
R2#show standby brief
                P indicates configured to preempt.
                |
Interface  Grp  Pri P State  Active        Standby        Virtual IP
Gig0/1     1    100 Standby 192.168.1.1   local          192.168.1.254
R2#
```

```
R1#show standby brief
                P indicates configured to preempt.
                |
Interface  Grp  Pri P State  Active        Standby        Virtual IP
Gig0/1     1    110 P Active 192.168.1.2   local          192.168.1.254
R1#
```

6 Exercice 4 : Etherrchannel avancé

J'ai réalisé le réseau suivant, en y ajoutant des postes afin de faire les tests nécessaires pour montrer le fonctionnement du réseau :

[Bloc2 sem3-4 atelier-04 redondance etherchannel-avancer.pkt](#)



Quelques opérations d'EtherChannel :

Vlan 2 et Vlan 3 sont déjà configurés sur tous les commutateurs.

- Le lien de SW1 à SW2 nécessite PAgP comme protocole de canal. SW1 et SW2 étiquetteront le port-canal 1.

SW1 initiera le canal, nous utiliserons le mode souhaitable, ce qui signifie qu'il demande activement de former un canal :

```
SW1(config-if)#interface FastEthernet0/1
SW1(config-if)#channel-group 1 mode desired
SW1(config-if)#interface FastEthernet0/2
SW1(config-if)# channel-group 1 mode desired
```

- SW2 n'initiera pas le canal, nous utiliserons le mode automatique, ce qui signifie qu'il attend de canalisier jusqu'à ce qu'on lui demande :

```
SW2(config)#interface FastEthernet0/1
SW2(config-if)# channel-group 1 mode auto
SW2(config-if)#interface FastEthernet0/2
SW2(config-if)# channel-group 1 mode auto
```

- Le lien de SW1 à SW3 nécessite LACP comme protocole de canal SW1 et SW3 étiquetera port-channel2

SW1 initialisera le canal :

```
SW1(config-if)# interface FastEthernet0/5
SW1(config-if)# mode groupe de canaux 2 actif
SW1(config-if)# interface FastEthernet0/6
SW1(config-if)# mode groupe de canaux 2 actif
```

SW3 n'initialisera pas le canal :

```
SW3(config)#interface FastEthernet0/5
SW3(config-if)# mode groupe de canaux 2 passif
SW3(config-if)#interface FastEthernet0/6
SW3(config-if)# mode groupe de canaux 2 passif
```

- Le lien de SW2 à SW3 n'utilisera pas PAgP ou LACP pour canaliser. SW2 et SW3 étiquetteront le port-canal 3.

```
SW2(config-if)#interface FastEthernet0/8
SW2(config-if)# mode groupe de canaux 3 activé
SW2(config-if)#interface FastEthernet0/9
SW2(config-if)# mode groupe de canaux 3 activé
```

```
SW3(config-if)#interface FastEthernet0/8
SW3(config-if)# mode groupe de canaux 3 activé
SW3(config-if)#interface FastEthernet0/9
SW3(config-if)# mode groupe de canaux 3 activé
```

-Le port-canal 1 doit négocier dynamiquement une liaison. SW1 initiera la négociation. SW2 ne lancera pas :

```
SW1(config-if)# interface FastEthernet0/1
SW1(config-if)# switchport mode dynamic desired
SW1(config-if)#interface FastEthernet0/2
SW1(config-if)# switchport mode dynamic desired
SW1(config-if)#interface Port-channel 1
SW1(config-if)# switchport mode dynamic desired
```

- Port-canal 2 doit négocier dynamiquement une liaison. SW3 lancera la liaison. SW1 ne lancera pas.

```
SW3(config-if)#interface FastEthernet0/5
SW3(config-if)# switchport mode dynamic desired
SW3(config-if)#interface FastEthernet0/6
SW3(config-if)# switchport mode dynamic desired
SW3(config-if)#interface Port-channel 2
SW3(config-if)# switchport mode dynamic desired
```

- Le port-canal 3 doit être forcé à se connecter et les deux extrémités de cette liaison ne doivent jamais pouvoir devenir un port d'accès.

```
SW3(config-if)#interface FastEthernet0/8
SW3(config-if)# mode switchport trunk
SW3(config-if)#interface FastEthernet0/9
SW3(config-if)# mode switchport trunk
SW3(config-if)#interface Port-channel 3
SW3(config-if)# mode switchport trunk
```

```
SW2(config-if)#interface FastEthernet0/8
SW2(config-if)# mode switchport trunk
SW2(config-if)#interface FastEthernet0/9
SW2(config-if)# mode switchport trunk
SW2(config-if)#interface Port-channel 3
SW2(config-if)# mode switchport trunk
```

- SW1 est la racine du VLAN 1, SW2 est la racine du VLAN 2 et SW3 est la racine du VLAN 3 :

```
SW1(config)#spanning-tree vlan 1 root primaire
SW2(config)#spanning-tree vlan 2 root primary
SW3(config)#spanning-tree vlan 3 root primary
```

-Le port-canal 1 utilisera le VLAN 1 natif par défaut, fa0/1 et fa0/2 appartiennent au VLAN 1.

-Le port-canal 2 utilisera le VLAN 2 natif :

```
SW3(config)#interface FastEthernet0/5
SW3(config-if)#switchport trunk native vlan 2
SW3(config-if)#interface FastEthernet0/6
```



```
SW3(config-if)#switchport trunk native vlan 2
SW3(config-if)#interface Port-canal 2
SW3(config-if)#switchport trunk native vlan 2
```

```
SW1(config-if)# interface FastEthernet0/5
SW1(config-if)# switchport trunk native vlan 2
SW1(config-if)#interface FastEthernet0/6
SW1(config-if)# switchport trunk native vlan 2
SW1(config-if)#interface Port-channel 2
SW1(config-if)#switchport trunk native vlan 2
```

-Le port-channel 3 utilisera le VLAN 3 natif :

```
SW2(config-if)# interface FastEthernet0/8
SW2(config-if)# switchport trunk native vlan 3
SW2(config-if)#interface FastEthernet0/9
SW2(config-if)# switchport trunk native vlan 3
SW2(config-if)#interface Port-channel 3
SW2(config-if)# switchport trunk native vlan 3
```

```
SW3(config-if)# interface FastEthernet0/8
SW3(config-if)# switchport trunk native vlan 3
SW3(config-if)#interface FastEthernet0/9
SW3(config-if)# switchport trunk native vlan 3
SW3(config-if)#interface Port-channel 3
SW3(config-if)# switchport trunk native vlan 3
```

-Le port physique supplémentaire à chaque port-channel :

Ajoutez le port fa0/3 au port-channel 1 :

```
SW1(config-if)# interface FastEthernet0/3
SW1(config-if)# mode channel-group 1 souhaitable
SW1(config-if)# mode switchport dynamic souhaitable
```

```
SW2(config)#interface FastEthernet0/3
SW2(config-if)# mode channel-group 1 auto
```

Port fa0/7 au port-channel 2 :

```
SW1(config-if)#interface FastEthernet0/7
SW1(config-if)# switchport trunk native vlan 2
SW1(config-if)# mode channel-group 2 actif
```

```
SW3(config-if)#interface FastEthernet0/7
SW3(config-if)# switchport trunk native vlan 2
SW3(config-if)# channel-group 2 mode passive
SW3(config-if)# switchport mode dynamic desired
```

Ajoutez le port fa0/10 au port-channel 3 :

```
SW3(config-if)#interface FastEthernet0/10
SW3(config-if)# switchport trunk native vlan 3
SW3(config-if)# channel-group 3 mode on
SW3(config-if)# switchport mode trunk
```

```
SW2(config-if)#interface FastEthernet0/10
SW2(config-if)# switchport trunk native vlan 3
SW2(config-if)# channel-group 3 mode on
SW2(config-if)# switchport mode trunk
```

```
S1(config-if)#exit
S1(config)#interface Port-channel1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 1
S1(config-if)# switchport trunk allowed vlan 1,2,3
S1(config-if)#exit
S1(config)#interface Port-channel2
S1(config-if)# switchport mode trunk

S1(config-if)# switchport trunk native vlan 2
S1(config-if)# switchport trunk allowed vlan 1,2,3
S1(config-if)#
S1(config-if)#exit
S1(config)#interface Port-channel3
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 3
S1(config-if)# switchport trunk allowed vlan 1,2,3
S1(config-if)#
```

J'ai d'abord vérifié le trunking sur chacun des commutateurs afin de confirmer le mode de liaison et les VLAN autorisés. Sur SW1, j'ai entré la commande « show int trunk » pour observer que le port-channel Po1 était en mode « desirable », encapsulé en 802.1q, avec l'état « trunking » et un VLAN natif en VLAN 1. Les VLAN autorisés sur ce trunk sont 1 à 3, et j'ai pu constater que les VLAN 1, 2 et 3 sont actifs dans le domaine de gestion. Le VLAN 1 est en état de forwarding dans le spanning-tree.

Sur SW2, j'ai répété la même vérification. Le port-channel Po3 est configuré en mode « on », encapsulé en 802.1q, avec un trunk opérationnel et un VLAN natif réglé sur le VLAN 3. Tous les VLAN 1 à 3 sont autorisés et actifs, et cette fois-ci les VLAN 1, 2 et 3 sont tous en état de forwarding dans le spanning-tree.

Sur SW3, le port-channel Po3 est également en mode « on », encapsulé en 802.1q, en trunk, avec le VLAN natif à 3. Les VLAN 1 à 3 sont autorisés, actifs et en état de forwarding dans le spanning-tree.

Ensuite, j'ai vérifié l'état de l'EtherChannel. Sur SW1, avec la commande « show etherchannel summary », j'ai vu que le groupe 1 (Po1) utilise le protocole PAgP, avec les interfaces Fa0/1, Fa0/2, Fa0/3 toutes actives (indiquées par (P)). Le groupe 2 (Po2) utilise LACP, et j'ai remarqué que sur Fa0/6 l'état était « I » (stand-alone), alors que Fa0/5 et Fa0/7 étaient en (P), donc bien intégrées dans le channel.

Sur SW3, la même commande m'a indiqué deux groupes : Po2 en LACP avec Fa0/5, Fa0/6, Fa0/7 toutes en (P), et Po3 sans protocole d'agrégation négocié (indiqué par « - ») avec Fa0/8, Fa0/9, Fa0/10 toutes en (P). La configuration entre SW3 et SW2 n'utilise donc pas de protocole d'agrégation dynamique, c'est-à-dire pas de PAgP ni de LACP sur Po3.

```
S3#show etherchannel summary
Flags: D - down          P - in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
       R - Layer3        S - Layer2
       U - in use        f - failed to allocate aggregator
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

Number of channel-groups in use: 2
Number of aggregators:          2

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
2      Po2(SU)        LACP        Fa0/5(P) Fa0/6(P) Fa0/7(P)
3      Po3(SU)        -           Fa0/8(P) Fa0/9(P) Fa0/10(P)
S3#
```

Sur SW2, le groupe Po1 utilise PAgP (avec Fa0/1, Fa0/2, Fa0/3 en (P)) et le groupe Po3 n'a pas de protocole négocié (marqué « - »), mais les interfaces Fa0/8, Fa0/9, Fa0/10 sont en (P), ce qui confirme la configuration statique de ce bundle.

```
S2#show etherchannel summary
Flags: D - down          P - in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
       R - Layer3        S - Layer2
       U - in use        f - failed to allocate aggregator
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

Number of channel-groups in use: 2
Number of aggregators:          2

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Po1(SU)        PAgP        Fa0/1(P) Fa0/2(P) Fa0/3(P)
3      Po3(SU)        -           Fa0/8(P) Fa0/9(P) Fa0/10(P)
S2#
```

let's verify the trunking:

SW1(config-if)#do show int trun

Port	Mode	Encapsulation	Status	Native vlan
Po1	desirable	n-802.1q	trunking	1

Port Vlans allowed on trunk

Po1 1-3

Port Vlans allowed and active in management domain

Po1 1,2,3

Port Vlans in spanning tree forwarding state and not pruned

Po1 1

SW2(config-if)#do show int trun

Port	Mode	Encapsulation	Status	Native vlan
Po3	on	802.1q	trunking	3

Port Vlans allowed on trunk

Po3 1-3

Port Vlans allowed and active in management domain

Po3 1,2,3

Port Vlans in spanning tree forwarding state and not pruned

Po3 1,2,3

SW2(config-if)#

SW3(config-if)#do show int trun

Port	Mode	Encapsulation	Status	Native vlan
Po3	on	802.1q	trunking	3

Port Vlans allowed on trunk

Po3 1-3

Port Vlans allowed and active in management domain

Po3 1,2,3

Port Vlans in spanning tree forwarding state and not pruned

Po3 1,2,3

let' verify the EtherChannel operation:

SW1#show etherchannel summary

Flags: D - down P - in port-channel

I - stand-alone s - suspended

H - Hot-standby (LACP only)

R - Layer3 S - Layer2

U - in use f - failed to allocate aggregator

u - unsuitable for bundling

w - waiting to be aggregated

d - default port

Number of channel-groups in use: 2

Number of aggregators: 2

Group	Port-channel	Protocol	Ports
1	Po1(SU)	PAgP	Fa0/1(P) Fa0/2(P) Fa0/3(P)
2	Po2(SU)	LACP	Fa0/5(P) Fa0/6(I) Fa0/7(P)

Notice between SW3 and SW2 there is no negotiation as denoted by the characters - in the following output:

```
SW3#show etherchannel summary
Flags: D - down      P - in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
       R - Layer3     S - Layer2
       U - in use     f - failed to allocate aggregator
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port
```

Number of channel-groups in use: 2
Number of aggregators: 2

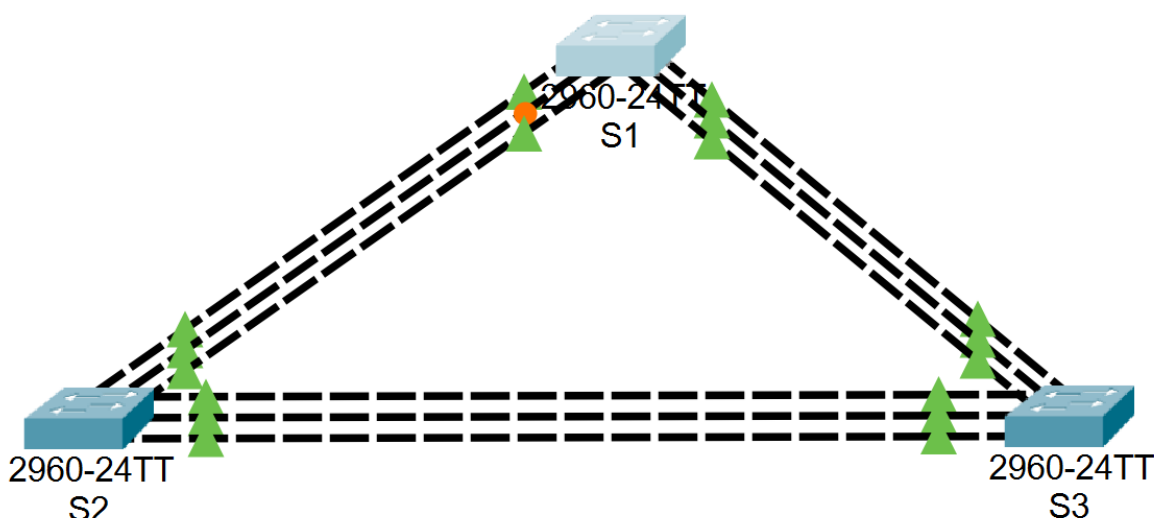
Group	Port-channel	Protocol	Ports
2	Po2(SU)	LACP	Fa0/5(P) Fa0/6(P) Fa0/7(P)
3	Po3(SU)	-	Fa0/8(P) Fa0/9(P) Fa0/10(P)

```
SW2#show etherchannel summary
Flags: D - down      P - in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
       R - Layer3     S - Layer2
       U - in use     f - failed to allocate aggregator
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port
```

Number of channel-groups in use: 2
Number of aggregators: 2

Group	Port-channel	Protocol	Ports
1	Po1(SU)	PAgP	Fa0/1(P) Fa0/2(P) Fa0/3(P)
3	Po3(SU)	-	Fa0/8(P) Fa0/9(P) Fa0/10(P)

6.1 Vérification de la formation des EtherChannels



J'ai vérifié la formation des EtherChannels à l'aide des commandes « show etherchannel summary » et « show etherchannel port ». Cela m'a confirmé la présence de groupes utilisant PAgP, LACP ou une agrégation statique, avec certains ports actifs et d'autres en attente. Le résultat illustre le fonctionnement normal de l'EtherChannel, offrant redondance, répartition de la charge et résilience face aux pannes individuelles de liens.

```
S1#show etherchannel summary
Flags: D - down          P - in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
       R - Layer3        S - Layer2
       U - in use        f - failed to allocate aggregator
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

Number of channel-groups in use: 3
Number of aggregators:          3

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1       Po1(SD)           PAgP      Fa0/1(I) Fa0/2(I) Fa0/3(I)
2       Po2(SU)           LACP      Fa0/5(P) Fa0/6(P) Fa0/7(P)
3       Po3(SD)           -
S1#show etherchannel port
Channel-group listing:
-----
Group: 1
-----
Port-channels in the group:
-----
Port-channel: Po1
-----
Age of the Port-channel = 00d:00h:17m:08s
Logical slot/port = 2/1      Number of ports = 0
GC = 0x00000000      HotStandBy port = null
Port state = Port-channel
Protocol = PAgP
Port Security = Disabled
```

```

Group: 2
-----
                Port-channels in the group:
                -----

Port-channel: Po2      (Primary Aggregator)
-----

Age of the Port-channel   = 00d:00h:17m:08s
Logical slot/port        = 2/2          Number of ports = 3
GC                        = 0x00000000    HotStandBy port = null
Port state                = Port-channel
Protocol                  = LACP
Port Security              = Disabled

Ports in the Port-channel:

Index  Load  Port      EC state      No of bits
-----+-----+-----+-----+-----
0      00     Fa0/7     Active        0
0      00     Fa0/6     Active        0
0      00     Fa0/5     Active        0
Time since last port bundled:  00d:00h:05m:18s   Fa0/5
Group: 3
-----
                Port-channels in the group:
                -----

Port-channel: Po3
-----

Age of the Port-channel   = 00d:00h:07m:14s
Logical slot/port        = 2/3          Number of ports = 0
GC                        = 0x00000000    HotStandBy port = null
Port state                = Port-channel
Protocol                  = -
Port Security              = Disabled

```

S1#

Vérification des trunks et VLAN natifs

J'ai vérifié les trunks et le VLAN natif en utilisant la commande « show interface trunk », ce qui m'a confirmé que les liens entre les commutateurs étaient bien configurés en mode trunk, avec le VLAN natif correctement défini. Les VLAN autorisés et actifs sont visibles, ainsi que leur état en spanning-tree, assurant une communication correcte à travers le réseau.

S1#show interface trunk

Port	Mode	Encapsulation	Status	Native vlan
Po2	on	802.1q	trunking	2

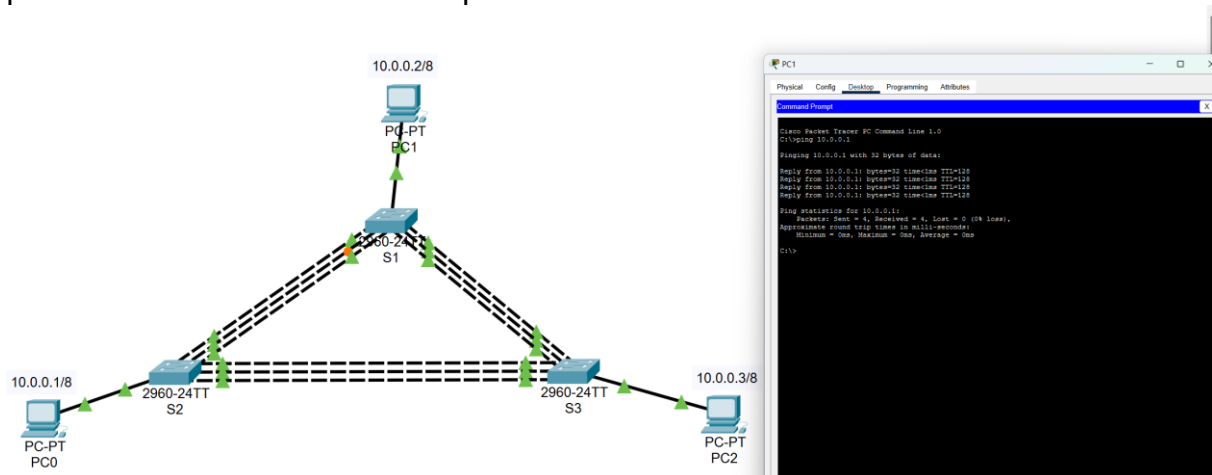
Port	Vlans allowed on trunk
Po2	1-3

Port	Vlans allowed and active in management domain
Po2	1,2,3

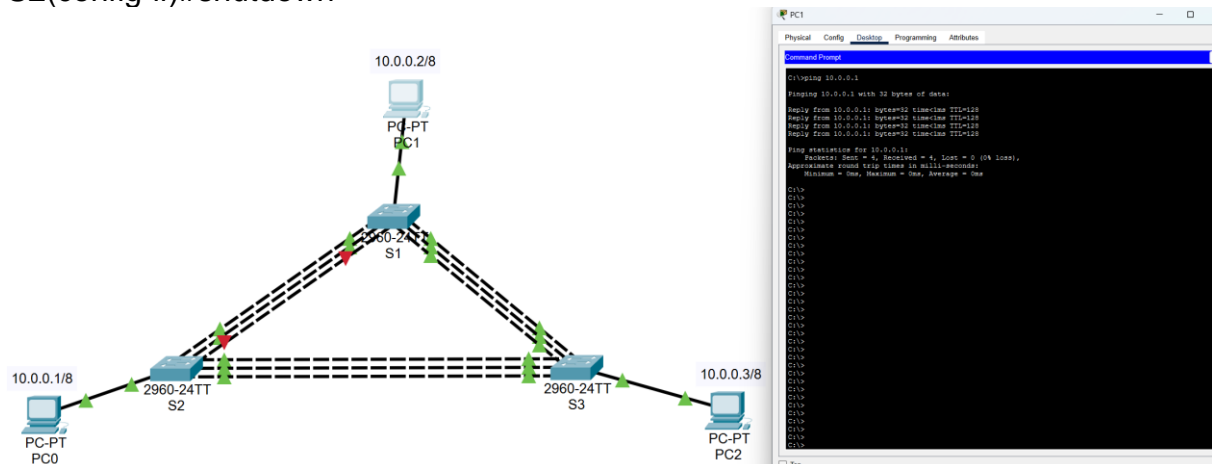
Port	Vlans in spanning tree forwarding state and not pruned
Po2	1,2,3

Test de résilience en cas de panne physique

Pour tester la résilience, j'ai simulé une panne physique en désactivant un port sur S2 (« shutdown » sur l'interface f0/3). Malgré cette coupure, le réseau a continué de transmettre le trafic, prouvant qu'avec EtherChannel, la perte d'un lien n'interrompt pas la connectivité. Les autres liens dans l'EtherChannel ont pris le relais, permettant aux postes de continuer à communiquer normalement.



S2(config)#interface f0/3
S2(config-if)#shutdown



Vérification du rôle STP par VLAN

J'ai vérifié le rôle de chaque commutateur dans le spanning-tree par VLAN. Grâce à « show spanning-tree vlan X », j'ai observé pour chaque VLAN qui est le pont racine (root bridge) et le rôle des interfaces (désignées, racine, bloquées). Par exemple, S2 est le root bridge pour le VLAN 2, tandis que pour le VLAN 1 et le VLAN 3, S2 n'est pas la racine. Ces informations confirment que le spanning-tree est opérationnel et que la topologie est optimisée par VLAN.

```
S2#show spanning-tree vlan 1
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
             Address     0005.5E72.3E36
             Cost        19
             Port        1(FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0001.42BA.B52A
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Po3	Desg	FWD	9	128.28	Shr
Gi0/1	Desg	FWD	19	128.25	P2p
Fa0/1	Root	FWD	19	128.1	P2p
Fa0/2	Altn	BLK	19	128.2	P2p

```
S2#show spanning-tree vlan 2
VLAN0002
  Spanning tree enabled protocol ieee
  Root ID    Priority    24578
             Address     0001.42BA.B52A
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24578  (priority 24576 sys-id-ext 2)
             Address     0001.42BA.B52A
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Po3	Desg	FWD	9	128.28	Shr
Fa0/1	Desg	FWD	19	128.1	P2p
Fa0/2	Desg	FWD	19	128.2	P2p
Fa0/9	Desg	FWD	19	128.9	P2p
Fa0/8	Desg	FWD	19	128.8	P2p
Fa0/10	Desg	FWD	19	128.10	P2p

```
S2#show spanning-tree vlan 3
VLAN0003
  Spanning tree enabled protocol ieee
  Root ID    Priority    24579
             Address     0006.2A45.4C19
             Cost        9
             Port        28(Port-channel3)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

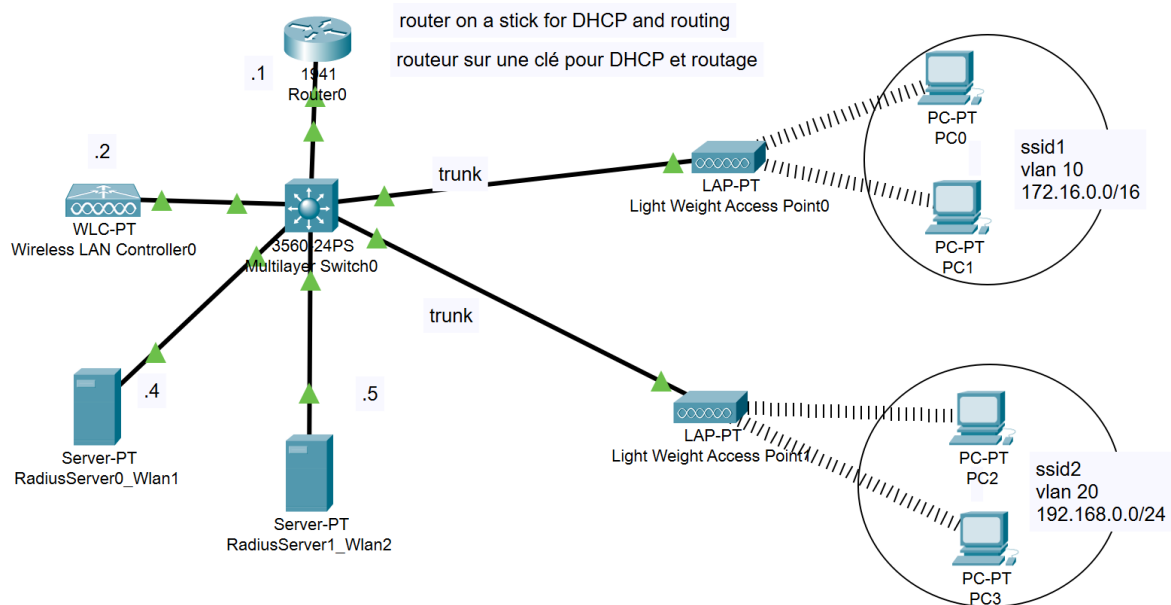
  Bridge ID  Priority    32771  (priority 32768 sys-id-ext 3)
             Address     0001.42BA.B52A
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Po3	Root	FWD	9	128.28	Shr
Fa0/1	Desg	FWD	19	128.1	P2p
Fa0/2	Desg	FWD	19	128.2	P2p
Fa0/9	Desg	FWD	19	128.9	P2p
Fa0/8	Desg	FWD	19	128.8	P2p
Fa0/10	Desg	FWD	19	128.10	P2p

S2#

7 Configuration d'un contrôleur sans fil avec deux VLANs, WPA et authentification RADIUS

J'ai utilisé le réseau suivant en réglant les problèmes, [wlc_pt_two_wlans_wpa_radius-fr.pkt](#)



7.1 Configuré les serveurs RADIUS

J'ai configuré les serveurs RADIUS en définissant le WLC comme client RADIUS, en spécifiant son adresse IP et une clé secrète partagée (« CiscoSecret »). J'ai créé des comptes utilisateurs (par exemple « wlc1 » et « wlc2 ») avec leurs mots de passe sur chaque serveur RADIUS. Ainsi, le WLC peut authentifier les clients sans fil via ces serveurs, garantissant une sécurité WPA avec authentification centralisée.

The screenshot shows the configuration interface for RADIUSServer0_Wlan1. The 'Services' tab is selected. Under the 'AAA' section, the 'Service' is set to 'On' and the 'Radius Port' is 1645. The 'Network Configuration' section shows a table with one entry: Client Name 'wlc', Client IP '10.0.0.2', Server Type 'Radius', and Key 'CiscoSecret'. The 'User Setup' section shows a table with one entry: Username 'wlc1' and Password '1234'.

Client Name	Client IP	Server Type	Key
1 wlc	10.0.0.2	Radius	CiscoSecret

Username	Password
1 wlc1	1234

The screenshot shows the configuration interface for RADIUSServer1_Wlan2. The 'Services' tab is selected. Under the 'AAA' section, the 'Service' is set to 'On' and the 'Radius Port' is 1645. The 'Network Configuration' section shows a table with one entry: Client Name 'wlc', Client IP '10.0.0.2', Server Type 'Radius', and Key 'CiscoSecret'. The 'User Setup' section shows a table with one entry: Username 'wlc2' and Password '1234'.

Client Name	Client IP	Server Type	Key
1 wlc	10.0.0.2	Radius	CiscoSecret

Username	Password
1 wlc2	1234

7.2 Configuré mes réseaux sans fil (WLAN)

J'ai configuré mes réseaux sans fil (WLAN) sur le contrôleur afin de proposer deux SSID distincts, chacun associé à un VLAN dédié. J'ai activé une sécurité WPA2, en spécifiant l'adresse du serveur RADIUS ainsi que le secret partagé, et j'ai choisi un chiffrement AES. Enfin, j'ai validé que chaque WLAN est bien attribué aux AP concernés, garantissant une segmentation propre, une authentification centralisée et une sécurité renforcée.

The screenshot shows the 'AP Groups' configuration page in the Wireless LAN Controller interface. The left sidebar has tabs for 'Physical', 'Config', and 'Attributes', with 'Config' selected. Under 'Config', there are sub-tabs for 'GLOBAL', 'Wireless LANs', 'AP Groups', and 'DHCP'. The 'AP Groups' sub-tab is active. The main area shows the configuration for the 'default-group'. It includes a table for 'Wireless LANs' with columns 'In AP Group', 'Name', and 'SSID'. Two entries are listed: 'wlan1' with 'ssid1' and 'wlan2' with 'ssid2', both with the 'In AP Group' checkbox checked. Below this is a table for 'Access Points' with columns 'In AP Group', 'Name', 'MAC Address', and 'Status'. Two entries are listed: 'Light Weight Access Point1' with MAC '0001.6454.0A01' and 'Light Weight Access Point0' with MAC '0090.0C1D.B201', both with the 'In AP Group' checkbox checked and status 'Online'.

In AP Group	Name	SSID
<input checked="" type="checkbox"/>	wlan1	ssid1
<input checked="" type="checkbox"/>	wlan2	ssid2

In AP Group	Name	MAC Address	Status
<input checked="" type="checkbox"/>	Light Weight Access Point1	0001.6454.0A01	Online
<input checked="" type="checkbox"/>	Light Weight Access Point0	0090.0C1D.B201	Online

The screenshot shows the 'WLANs' configuration page in the Wireless LAN Controller interface. The left sidebar has tabs for 'Physical', 'Config', and 'Attributes', with 'Config' selected. Under 'Config', there are sub-tabs for 'GLOBAL', 'Wireless LANs', 'AP Groups', and 'DHCP'. The 'Wireless LANs' sub-tab is active. The main area shows the configuration for the 'wlan1' WLAN. It includes fields for 'Name' (wlan1), 'SSID' (ssid1), and 'VLAN' (10). Below these is the 'Authentication' section with radio buttons for 'Disabled', 'WEP', 'WPA-PSK', 'WPA2-PSK', 'WPA', and 'WPA2'. The 'WPA2' option is selected. Below this is the 'RADIUS Server Settings' section with fields for 'IP Address' (10.0.0.4) and 'Shared Secret' (CiscoSecret). The 'Encryption Type' is set to 'AES'. At the bottom, there are radio buttons for 'Central Control' with options 'Central switching, central authentication', 'Local switching, central authentication', and 'Local switching, local authentication'. The 'Local switching, local authentication' option is selected. At the bottom of the page are buttons for 'New', 'Remove', and 'Save'.

In AP Group	Name	MAC Address	Status
<input checked="" type="checkbox"/>	Light Weight Access Point1	0001.6454.0A01	Online
<input checked="" type="checkbox"/>	Light Weight Access Point0	0090.0C1D.B201	Online

7.3 Configuré le routeur

J'ai configuré le routeur en mode « router-on-a-stick » pour gérer plusieurs VLANs. Sur l'interface GigabitEthernet0/0, j'ai créé deux sous-interfaces : GigabitEthernet0/0.10 pour le VLAN 10, avec l'adresse 172.16.0.1/16, et GigabitEthernet0/0.20 pour le VLAN 20, avec l'adresse 192.168.0.1/24. L'interface principale G0/0 est en 10.0.0.1/8, jouant le rôle de gateway pour un premier réseau.

J'ai configuré le DHCP sur le routeur, en excluant certaines adresses de chaque réseau, puis en créant des pools DHCP pour fournir des adresses IP aux clients connectés aux différents VLANs. Les adresses par défaut et les masques ont été définis, ainsi que le routeur par défaut (gateway) pour chaque segment.

Enfin, les interfaces inutilisées, comme GigabitEthernet0/1, sont désactivées (shutdown). Cette configuration permet au routeur d'assurer le routage inter-VLAN, de fournir des adresses IP dynamiques et d'assurer une segmentation logique du réseau.

```
Router#show r
```

```
Building configuration...
```

```
Current configuration : 1220 bytes
```

```
!
```

```
version 15.1
```

```
no service timestamps log datetime msec
```

```
no service timestamps debug datetime msec
```

```
no service password-encryption
```

```
!
```

```
hostname Router
```

```
!
```

```
!
```

```
!
```

```
!
```

```
ip dhcp excluded-address 10.0.0.1
```

```
ip dhcp excluded-address 10.0.0.2
```

```
ip dhcp excluded-address 10.0.0.3
```

```
ip dhcp excluded-address 10.0.0.4
```

```
ip dhcp excluded-address 10.0.0.5
```

```
ip dhcp excluded-address 172.16.0.1
```

```
ip dhcp excluded-address 192.168.0.1
```

```
!
```

```
ip dhcp pool VLAN10
```

```
network 172.16.0.0 255.255.0.0
```

```
default-router 172.16.0.1
```

```
ip dhcp pool VLAN20
```

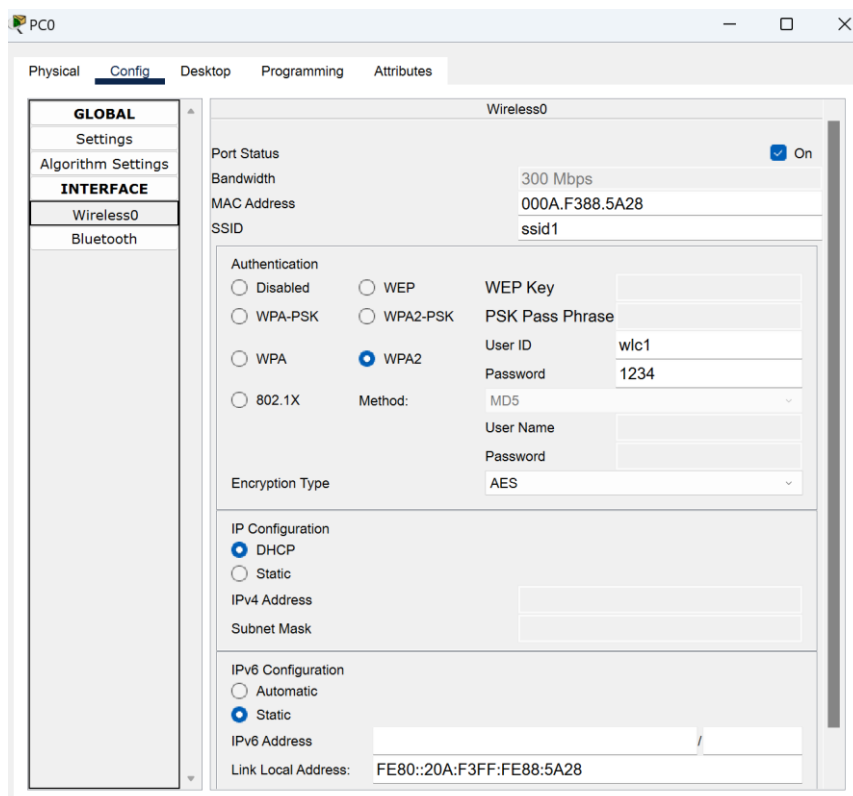
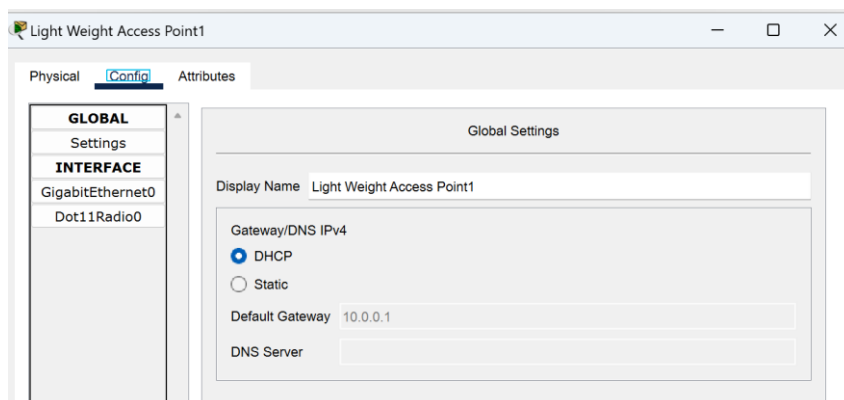
```
network 192.168.0.0 255.255.255.0
```

```
default-router 192.168.0.1
!
!
!
ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO1941/K9 sn FTX1524AWQX
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
interface GigabitEthernet0/0
ip address 10.0.0.1 255.0.0.0
duplex auto
speed auto
!
interface GigabitEthernet0/0.10
encapsulation dot1Q 10
ip address 172.16.0.1 255.255.0.0
!
interface GigabitEthernet0/0.20
encapsulation dot1Q 20
ip address 192.168.0.1 255.255.255.0
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
```

```
shutdown
!  
interface Vlan1  
no ip address  
shutdown  
!  
router rip  
!  
ip classless  
!  
ip flow-export version 9  
!  
!  
!  
!  
!  
!  
!  
line con 0  
!  
line aux 0  
!  
line vty 0 4  
login
```

7.4 Configurer les points d'accès et PC

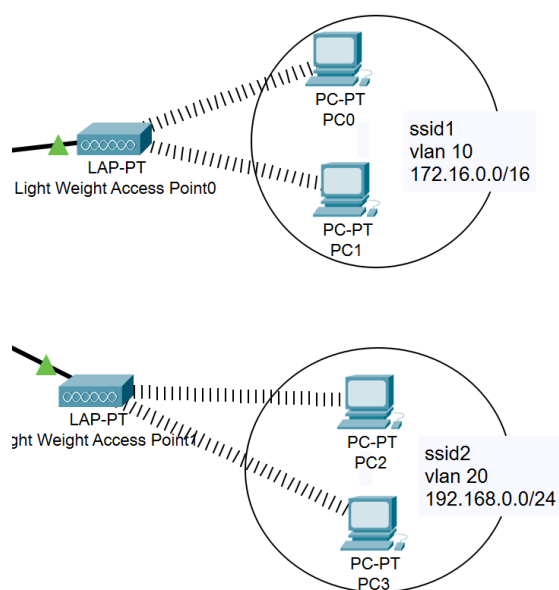
J'ai configuré les points d'accès légers (Light Weight AP) pour qu'ils obtiennent leur adresse IP via DHCP et utilisent le routeur comme passerelle par défaut. Du côté des PC, j'ai paramétré les connexions sans fil pour se connecter aux SSID correspondants, en WPA2, avec authentification via les identifiants RADIUS (par exemple, utilisateur « wlc1 » et mot de passe « 1234 »). Ainsi, les clients sans fil obtiennent une adresse IP automatiquement et s'authentifient de manière sécurisée, assurant un accès réseau fiable et protégé.



7.5 Verification

J'ai testé la connectivité entre les points d'accès légers et le routeur via des paquets ICMP (ping). Le tableau montre que les tests sont concluants (« Successful »), prouvant que les points d'accès communiquent correctement avec le routeur et confirment la configuration réseau réussie.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	PC1	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC3	PC2	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC0	PC3	ICMP		0.000	N	2	(edit)	(delete)
	Successful	PC1	Router0	ICMP		0.000	N	3	(edit)	(delete)
	Successful	Light Wei...	Light Weight Acce...	ICMP		0.000	N	4	(edit)	(delete)
	Successful	RadiusS...	PC2	ICMP		0.000	N	5	(edit)	(delete)
	Successful	PC1	RadiusServer1_W...	ICMP		0.000	N	6	(edit)	(delete)



8 Annexes

Fiche technique HSRP

Principes généraux

HSRP est un protocole propriétaire de CISCO et VRRP est un protocole standard (non propriétaire) décrit par l'IETF dans la RFC 579.

En cas de panne de la passerelle par défaut, HSRP ou VRRP bascule sur un routeur de secours pour assurer la continuité, et ce, de façon transparente pour les utilisateurs. Pour cela, on place plusieurs routeurs au sein d'un même groupe logique auquel on assigne une adresse IP et une adresse MAC virtuelle unique pour le groupe ; un des routeurs est désigné comme routeur actif (nominal), les autres sont dans un mode passif (Standby). En s'envoyant régulièrement des messages HSRP/VRRP (hello), les routeurs du groupe surveillent la présence effective et opérationnelle du routeur actif. S'ils ne reçoivent plus de message du routeur actif pendant un délai défini, le routeur passif du groupe ayant la priorité la plus élevée prend le statut de routeur actif.

Un routeur peut agir en mode préemptif : si le routeur actif R1 est tombé en panne et qu'un routeur passif R2 a pris le rôle actif, lors de son redémarrage, R1 reprendra automatiquement le rôle actif s'il a une priorité plus élevée.

HSRP et VRRP ne gèrent pas l'équilibrage de charge sur les passerelles par défaut, ce que fait le protocole GLBP.

Commandes IOS

Exemple de configuration de deux routeurs R1 et R2

```
R1(config)#interface fa0/0
R1(config)#standby 10 ip 20.0.0.254
R1(config)#standby 10 preempt
```

La « commande standby » place le routeur en mode HSRP. « 10 » est le numéro du groupe HSRP auquel appartiendra le routeur. Par défaut il a la priorité « 100 ». L'adresse IP 20.0.0.254 correspond à l'adresse IP virtuelle de la passerelle qu'il faudra configurer sur les hôtes.

La commande utilisant la clause « preempt » rend actif le mode HSRP du routeur.

```
R2(config)#interface fa0/0
R2(config)#standby 10 ip 20.0.0.254
R2(config)#standby 10 priority 200
R2(config)#standby 10 preempt
```

Ici, R2 sera prioritaire sur R1 puisqu'il a une priorité de 200.

La commande « show standby brief » permet de connaître l'état HSRP du routeur.

9 Conclusion :

Cet exercice a permis de mettre en œuvre et de vérifier les configurations EtherChannel avancées sur un réseau multi-commutateurs. Grâce à l'utilisation de protocoles tels que PAgP et LACP, nous avons démontré l'efficacité de l'agrégation de liens pour augmenter la bande passante et assurer une redondance réseau, tout en réduisant le risque de défaillance des connexions physiques.

En configurant les ports en mode trunk et en ajustant les VLANs natifs pour chaque port-channel, nous avons optimisé la communication entre les différents périphériques, garantissant ainsi la stabilité et la performance du réseau. De plus, l'utilisation des modes de négociation comme desirable, auto, active, et passive a permis de tester et d'assurer que les connexions sont formées correctement selon les exigences spécifiques.

Enfin, les commandes de vérification telles que `show etherchannel summary` ont confirmé que l'EtherChannel fonctionne comme prévu, avec les agrégations de liens correctement établies. Cet exercice a renforcé les compétences en matière de configuration d'EtherChannel et de gestion de la redondance, des éléments clés pour un réseau robuste et performant.

10 Webographie :

1. **Cisco - Documentation officielle sur EtherChannel**
 - URL: https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/l2vpn/62x/b-etherchannel-configuration-guide/b-etherchannel-configuration-guide_chapter_010.html
 - **Description** : Cette ressource fournit une documentation détaillée sur la configuration et la gestion d'EtherChannel sur les appareils Cisco. Elle couvre les concepts de base ainsi que des exemples pratiques pour la configuration de PAgP, LACP, et des modes de négociation de trunk.
2. **Cisco - EtherChannel (Link Aggregation) Configuration Guide**
 - URL: https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/l2vpn/62x/b-etherchannel-configuration-guide/b-etherchannel-configuration-guide_chapter_020.html
 - **Description** : Ce guide présente les étapes pour configurer EtherChannel dans un environnement réseau Cisco, y compris les options de protocole comme PAgP et LACP, et les meilleures pratiques pour une gestion optimisée du réseau.
3. **Packet Tracer Help - Cisco Networking Academy**
 - URL: <https://www.netacad.com/courses/packet-tracer>
 - **Description** : Le site de Cisco Networking Academy propose des cours et des ressources pour apprendre à utiliser Cisco Packet Tracer. Cet outil est essentiel pour la simulation de réseaux, y compris les configurations de VLAN, EtherChannel, et bien plus encore.
4. **EtherChannel Configuration Guide - NetworkLessons.com**
 - URL: <https://networklessons.com/cisco/ccna-routing-switching-200-125/etherchannel>
 - **Description** : Ce guide offre des explications claires et des tutoriels sur EtherChannel, y compris les différents protocoles et modes de négociation. Il est adapté aux personnes préparant la certification CCNA et désireuses de maîtriser la configuration d'EtherChannel.
5. **TechTarget - EtherChannel Overview**
 - URL: <https://searchnetworking.techtarget.com/definition/EtherChannel>
 - **Description** : Un article détaillant les bases du protocole EtherChannel, les différents types de liens et leur utilité dans un réseau professionnel. Il aborde aussi les avantages d'EtherChannel pour la redondance et la montée en bande passante.
6. **Cisco - Spanning Tree Protocol (STP) Documentation**
 - URL: https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/l2vpn/62x/b-etherchannel-configuration-guide/b-etherchannel-configuration-guide_chapter_010.html
 - **Description** : Un guide pour comprendre l'interaction entre EtherChannel et le protocole Spanning Tree, essentiel pour éviter les boucles dans le réseau et assurer la stabilité de l'agrégation de liens.