**Etherchannel et haute disponibilité sur les switchs et les routeurs**

B\*\*

14/12/2024

Eloham Caron

Bts SIo 2 SISR

Table des matières

[1. Introduction 3](#_Toc185106429)

[2. HSRP 3](#_Toc185106430)

[3. Mise en œuvre d’HSRP 4](#_Toc185106431)

[a) Vérification des trunks sur les trois switches (DLS1, ALS1, ALS2) : 4](#_Toc185106432)

[b) Activer le trunk : 6](#_Toc185106433)

[c) DLS1 –– DLS2 : 7](#_Toc185106434)

[d) DLS1 –– ALS2 | DSL2 –– ALS1 8](#_Toc185106435)

[4. VTP (VLAN Trunking Protocol) : 9](#_Toc185106436)

[e) Pour changer le mode VTP sur les switches ALS1 et ALS2 et les mettre en mode client, suivez les étapes ci-dessous. 9](#_Toc185106437)

[5. a. Configurer les interfaces en mode trunk (manuellement pour chaque interface) : 10](#_Toc185106438)

[6. EtherChannel 10](#_Toc185106439)

[f) Vérification de l'EtherChannel 11](#_Toc185106440)

[g) DLS2 : 12](#_Toc185106441)

[h) ALS1 : 12](#_Toc185106442)

[i) ALS2 : 13](#_Toc185106443)

[j) Noter que nombre de Vlans est de 5, pourquoi ? 13](#_Toc185106444)

[7. Créer le domaine VTP sur le serveur DLS1 et configurer les VLANs 15](#_Toc185106445)

[k) a. Configurer le domaine VTP et la version 2 15](#_Toc185106446)

[l) Comment expliquez-vous les changements en ce qui concerne la Configuration révision et « Number of existing VLANs » ? 18](#_Toc185106447)

[8. Configurer les ports connectés aux différents hôtes en mode access (fa0/6 ) 19](#_Toc185106448)

[m) Sur DLS1 (VLAN 30) 19](#_Toc185106449)

[n) Sur DLS2 (VLAN 40) 19](#_Toc185106450)

[o) Sur ALS1 (VLAN 10) 20](#_Toc185106451)

[p) Sur ALS2 (VLAN 20) 20](#_Toc185106452)

[q) Configuration des vlan : 20](#_Toc185106453)

[r) DSL1 : 20](#_Toc185106454)

[s) DSL2 : 21](#_Toc185106455)

[t) ALS1 : 21](#_Toc185106456)

[u) ALS2 : 21](#_Toc185106457)

[v) Configuration des différente interfaces : 21](#_Toc185106458)

[w) Faire un ping depuis l’hôte sur le Vlan 10 vers l’hôte sur le VLAN 40. Quel en est le résultat et pourquoi ? 22](#_Toc185106459)

[9. Exercice 2 : Travaux pratiques – Configuration du protocole HSRP sur des routeurs 28](#_Toc185106460)

[x) Configurez les PC hôtes. 29](#_Toc185106461)

[y) Configurez les paramètres de base pour chaque routeur. 29](#_Toc185106462)

[z) Configurez les paramètres de base pour chaque routeur. 30](#_Toc185106463)

[aa) Configurez les paramètres de base pour chaque commutateur. 31](#_Toc185106464)

[bb) Configuration de la redondance au premier saut avec HSRP 33](#_Toc185106465)

[cc) Démarrez une session ping sur PC-A et rompez la connexion entre le commutateur qui est connecté au routeur HSRP actif (R1). 39](#_Toc185106466)

[dd) Vérifiez les paramètres du protocole HSRP sur R1 et R3. 39](#_Toc185106467)

[ee) Modifiez les priorités HSRP. 41](#_Toc185106468)

[ff) présenter vos configurations 42](#_Toc185106469)

[gg) montrer que la répartition de charges est réalisée selon le mode Round Robin 42](#_Toc185106470)

[10. Exercice 3 : Packet Tracer – Dépannage du protocole HSRP 43](#_Toc185106471)

[11. Exercice 4 :Etherrchannel avancé 51](#_Toc185106472)

[hh) SW1 Configuration de Port-Channel 1 avec PAgP 51](#_Toc185106473)

[ii) Vérifions le trunking : 53](#_Toc185106474)

[jj) Vérifions le fonctionnement de l'EtherChannel : 54](#_Toc185106475)

[12. SD-WAN 63](#_Toc185106476)

[13. Conclusion : 68](#_Toc185106477)

[14. Source : 69](#_Toc185106478)

# Introduction

Dans un environnement réseau professionnel, la fiabilité et la disponibilité des services sont essentielles. La mise en place de mécanismes de haute disponibilité, comme l’EtherChannel sur les commutateurs et le protocole HSRP sur les routeurs, permet d’assurer une continuité de service en cas de défaillance d’un lien ou d’un équipement. En agrégeant plusieurs liens physiques en un seul canal logique, l’EtherChannel augmente à la fois la bande passante et la résilience du réseau, tandis que l’utilisation d’HSRP garantit une bascule rapide vers un routeur redondant sans interrompre le trafic. Cette approche intégrée renforce la robustesse de l’architecture, réduit les temps d’arrêt et maintient une qualité de service optimale pour les utilisateurs finaux.

# HSRP

Le **protocole HSRP** (Hot Standby Router Protocol) est un protocole propriétaire développé par Cisco Systems destiné à assurer la haute disponibilité des passerelles par défaut dans un réseau. Il permet à plusieurs routeurs de travailler ensemble de manière redondante, de sorte qu'en cas de défaillance d'un routeur principal, un autre prend automatiquement le relais sans interruption de service pour les utilisateurs finaux.

**Fonctionnement de HSRP**

1. **Configuration d'un groupe HSRP** : Plusieurs routeurs sont configurés pour appartenir au même groupe HSRP. Chaque groupe HSRP est identifié par un numéro unique.
2. **Élection des rôles** :
   * **Routeur Actif** : C'est le routeur principal qui gère le trafic en tant que passerelle par défaut pour le réseau local.
   * **Routeur de Standby** : Ce routeur surveille l'état du routeur actif et est prêt à prendre le relais en cas de défaillance de ce dernier.
   * **Routeurs de Candidats** : Les autres routeurs du groupe restent en veille et peuvent devenir le routeur de standby si nécessaire.
3. **Adresse IP Virtuelle** : HSRP utilise une adresse IP virtuelle et une adresse MAC virtuelle partagées entre les routeurs du groupe. Les dispositifs du réseau local utilisent cette adresse IP virtuelle comme passerelle par défaut.

**Avantages de HSRP**

* **Haute Disponibilité** : Assure que la passerelle par défaut reste disponible même en cas de défaillance d'un routeur.
* **Simplicité de Configuration** : Facile à configurer sur les équipements Cisco.
* **Flexibilité** : Permet la configuration de multiples groupes HSRP pour différentes sous-réseaux ou VLANs.
* **Priorisation** : Possibilité de définir des priorités pour influencer l'élection des rôles actifs et standby.

**Comparaison avec d'autres Protocoles**

* **VRRP (Virtual Router Redundancy Protocol)** : Standard ouvert similaire à HSRP, utilisé pour la redondance des routeurs.
* **GLBP (Gateway Load Balancing Protocol)** : Permet non seulement la redondance mais aussi le partage de charge entre plusieurs routeurs.

# Mise en œuvre d’HSRP

Une image contenant ligne, texte, diagramme, Tracé

Description générée automatiquement

## Vérification des trunks sur les trois switches (DLS1, ALS1, ALS2) :

Analyse des interfaces trunk pour vérifier la cohérence de la configuration et l’état des VLANs.

**DLS1** :

Les ports Fa0/9 et Fa0/10 sont en trunk, transportant le VLAN 1 (natif), en état "forwarding" pour le Spanning Tree.

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

**ALS1** :

Les ports Fa0/11 et Fa0/12 sont configurés en trunk, mais aucun VLAN n’est en "forwarding" dans le Spanning Tree.

Une image contenant texte, capture d’écran, nombre, Police

Description générée automatiquement

**ALS2** :

Les ports Fa0/6 à Fa0/12 sont en trunk, mais Fa0/10 est bloqué dans le Spanning Tree pour éviter une boucle.

Une image contenant texte, capture d’écran, nombre, affichage

Description générée automatiquement

## Activer le trunk :

Le trunk permet de transporter plusieurs VLANs entre deux switches via une seule liaison physique. Dans le schéma, les liens pointillés entre DLS1 et ALS1, ainsi qu’entre DLS2 et ALS2, représentent des trunks, qui utilisent l'encapsulation **802.1Q** pour identifier et séparer les VLANs sur une même connexion.

Une image contenant ligne, texte, diagramme, Tracé

Description générée automatiquement

Pour activer le trunk sur le port **FastEthernet0/8** de DLS1, on utilise les commandes suivantes

* switchport trunk encapsulation dot1q : Définit le protocole d'encapsulation VLAN.
* switchport mode trunk : Configure le port en mode trunk pour transporter plusieurs VLANs.

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement

La configuration sur **FastEthernet0/7** de DLS1 est similaire à celle de Fa0/8, avec les mêmes commandes :

* switchport trunk encapsulation dot1q
* switchport mode trunk Cela permet de créer un autre lien trunk entre les switches pour assurer la communication entre les VLANs.

Une image contenant texte, Police, capture d’écran, ligne

Description générée automatiquement

## DLS1 –– DLS2 :

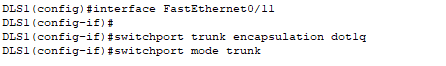
Les liens entre **Fa0/11** de DLS1 et **Fa0/10** de DLS2, ainsi que **Fa0/12** de DLS1 et **Fa0/12** de ALS1, doivent être configurés en mode **trunk** pour permettre la transmission des VLANs entre ces équipements.

Une image contenant texte, ligne, diagramme, capture d’écran

Description générée automatiquement

**Activation du Trunk sur DLS1 (Fa0/12)**

* Sur **Fa0/12** de DLS1, les commandes suivantes sont utilisées pour activer le trunk :
* switchport trunk encapsulation dot1q : Définit le protocole d'encapsulation.
* switchport mode trunk : Configure l'interface en mode trunk.



**Activation du Trunk sur DLS1 (Fa0/11)**

* Les mêmes étapes sont suivies pour le port **Fa0/11** de DLS1 :
* switchport trunk encapsulation dot1q
* switchport mode trunk Cela permet d'établir une liaison trunk entre DLS1 et DLS2, garantissant la communication entre les VLANs.

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement

## DLS1 –– ALS2 | DSL2 –– ALS1

Les ports concernés par les trunks sont **Fa0/9** et **Fa0/10** sur **ALS1**, qui se connectent respectivement à **DLS1** et **DLS2**. Ces liens permettent de transporter les VLANs entre les switches.

Une image contenant ligne, diagramme, texte, Parallèle

Description générée automatiquement

**Activation du Trunk sur ALS1 (Fa0/9)**

* Pour configurer le port **Fa0/9** sur ALS1 en mode trunk, les commandes suivantes sont utilisées :
* interface FastEthernet0/9 : Sélection du port.
* switchport mode trunk : Activation du mode trunk pour transporter les VLANs.

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement

**Activation du Trunk sur ALS1 (Fa0/10)**

* La configuration pour le port **Fa0/10** est similaire :
* interface FastEthernet0/10
* switchport mode trunk  
  Cela permet une communication VLAN entre ALS1, DLS1 et DLS2.

Une image contenant texte, Police, capture d’écran, ligne

Description générée automatiquement

# VTP (VLAN Trunking Protocol) :

Le **VTP** est un protocole Cisco utilisé pour gérer la propagation des informations VLAN à travers un réseau. Il permet aux switches de diffuser, d'ajouter, de modifier ou de supprimer des VLANs de manière centralisée.

**Mode Serveur** :

Le switch en mode **serveur** est responsable de la création, de la gestion et de la diffusion des informations VLAN sur le réseau. C'est le mode par défaut des switches Cisco. Les VLANs créés sur un switch serveur sont automatiquement propagés aux autres switches.

**Mode Client** :

Un switch en mode **client** reçoit et applique les informations VLAN provenant des serveurs. Il ne peut pas créer, modifier ou supprimer de VLANs ; il se contente de recevoir et de propager les informations des VLANs configurés sur le serveur.

**Mode Transparent** :

Un switch en mode **transparent** n'envoie pas de mises à jour VTP, mais il applique les informations VLAN reçues des serveurs. Cela permet d'ajouter des VLANs manuellement sans affecter la propagation des VLANs aux autres switches.

## Pour changer le mode VTP sur les switches ALS1 et ALS2 et les mettre en mode client, suivez les étapes ci-dessous.

1. **1. Passer les switches ALS1 et ALS2 en mode client VTP :**

* Connectez-vous à chaque switch via la console ou SSH.
* Entrez en mode de configuration globale (conf t).
* Changez le mode VTP pour **client**.

**Commandes pour ALS1 et ALS2 :**

1. **Sur ALS1 :**

Une image contenant texte, capture d’écran, Police, reçu

Description générée automatiquement

1. **Sur ALS2 :**



# a. ****Configurer les interfaces en mode trunk (manuellement pour chaque interface) :****

Utilisez les commandes suivantes pour chaque interface individuelle (7 et 8, 9 et 10, 11 et 12) avant de les agréger en EtherChannel.

**Pour les interfaces GigabitEthernet 0/7 et 0/8 :**

Une image contenant texte, Police, capture d’écran, ligne

Description générée automatiquement

**Configurer EtherChannel entre FastEthernet 0/9 et 0/10 :**





**Configurer EtherChannel entre FastEthernet 0/11 et 0/12 :**



# EtherChannel

EtherChannel est une technologie de commutation qui permet de regrouper plusieurs liens physiques entre des périphériques réseau (comme des commutateurs ou des routeurs) pour créer une connexion logique unique. Ce regroupement de liens améliore la bande passante, la tolérance aux pannes et la redondance, tout en permettant de mieux répartir la charge entre les différents liens.

Le but est d’**augmenter la vitesse** et la **tolérance aux pannes** entre les commutateurs, les routeurs et les serveurs. Elle permet de simplifier une topologie Spanning-Tree en diminuant le nombre de liens.

Un lien EtherChannel groupe de 2 à 8 liens actifs de 100 Mbit/s, 1 Gbit/s et 10 Gbit/s, plus éventuellement de 1 à 8 liens inactifs en réserve qui deviennent actifs quand des liens actifs sont coupés.

**Avantages :**

* **Bande passante accrue** : Regroupement des liens pour plus de capacité.
* **Redondance** : Continuité du trafic si un lien échoue.
* **Répartition de la charge** : Trafic réparti sur les liens du groupe.
* **Gestion simplifiée** : Le groupe est vu comme un seul lien logique.

**Protocoles :**

* **PAgP** (Cisco, négociation automatique)
* **LACP** (Standard IEEE, négociation automatique)

## Vérification de l'EtherChannel

La commande show etherchannel summary permet de vérifier l'état des agrégats de liens (EtherChannel) sur un switch Cisco. Elle affiche un résumé des interfaces EtherChannel configurées et leur état.

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquementAucun groupe EtherChannel actif. Aucun port ni protocole configuré.

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Même constat : pas de groupe ni de port EtherChannel configuré.

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Pas d'EtherChannel actif, aucune interface associée à un port-channel.

## DLS2 :

Configurer EtherChannel entre FastEthernet 0/7 et 0/8 :



Configurer EtherChannel entre FastEthernet 0/9 et 0/10 :



Configurer EtherChannel entre FastEthernet 0/11 et 0/12 :



## ALS1 :

Configurer EtherChannel entre FastEthernet 0/7 et 0/8 :



Configurer EtherChannel entre FastEthernet 0/9 et 0/10 :



Configurer EtherChannel entre FastEthernet 0/11 et 0/12 :



## ALS2 :

Configurer EtherChannel entre FastEthernet 0/7 et 0/8 :



Configurer EtherChannel entre FastEthernet 0/9 et 0/10 :

Une image contenant texte, Police, capture d’écran, ligne

Description générée automatiquement

Configurer EtherChannel entre FastEthernet 0/11 et 0/12 :

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement

Après avoir configuré l'EtherChannel, vous pouvez vérifier l'état des agrégations de lien.

Vérifiez les EtherChannels avec la commande suivante :

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

## Noter que nombre de Vlans est de 5, pourquoi ?

Le nombre de VLANs est de 5 afin de segmenter efficacement le réseau en fonction des besoins organisationnels et de sécurité. Chaque VLAN peut correspondre à un département ou un groupe d'utilisateurs spécifique, ce qui permet de contrôler le trafic réseau, d'optimiser la gestion du réseau et de renforcer la sécurité en isolant les communications entre les différents segments. En choisissant cinq VLANs, nous répondons aux critères d'organisation et de performance, tout en assurant une gestion simplifiée du réseau.

Une image contenant texte, diagramme, ligne, cercle

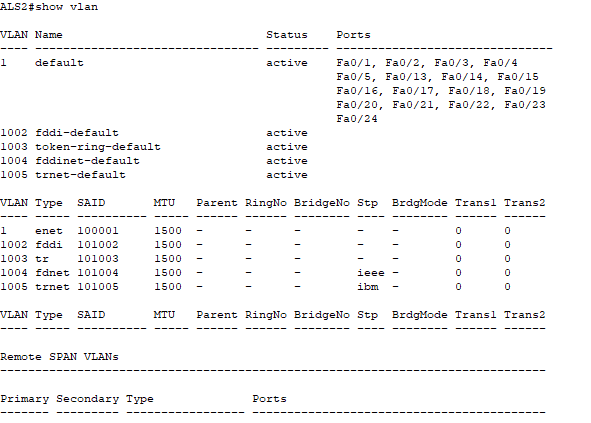
Description générée automatiquement

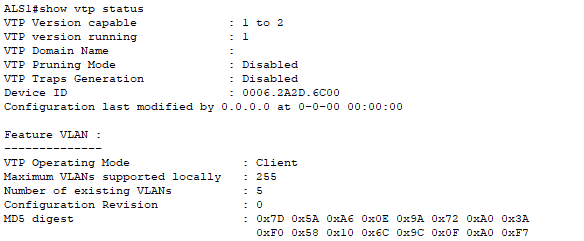
Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Créer le domaine VTP sur le serveur DLS1, de nom CISCO (on utilisera la version 2 du protocole VTP) et créer les VLANs 10 de nom Finance,20 de nom Engineering, 30 de nom Server 1, et 40 de nom Server2

Vérifier le statut des Vlans sur ALS2.



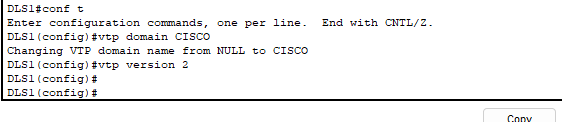


# ****Créer le domaine VTP sur le serveur DLS1 et configurer les VLANs****

Sur DLS1, suivez ces étapes pour configurer le domaine VTP (nommé CISCO), utiliser la version 2 du protocole VTP, et créer les VLANs.

## a. ****Configurer le domaine VTP et la version 2****

* Connectez-vous à **DLS1** et passez en mode privilégiée



Une image contenant texte, capture d’écran, Police, nombre

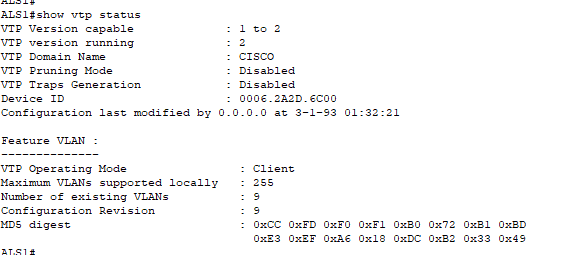
Description générée automatiquement

Ils se sont bien télécharger derrière :

ALS1

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement



Vérifier les vlan

ALS2

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

DLS2

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Une image contenant texte, capture d’écran, Police, nombre

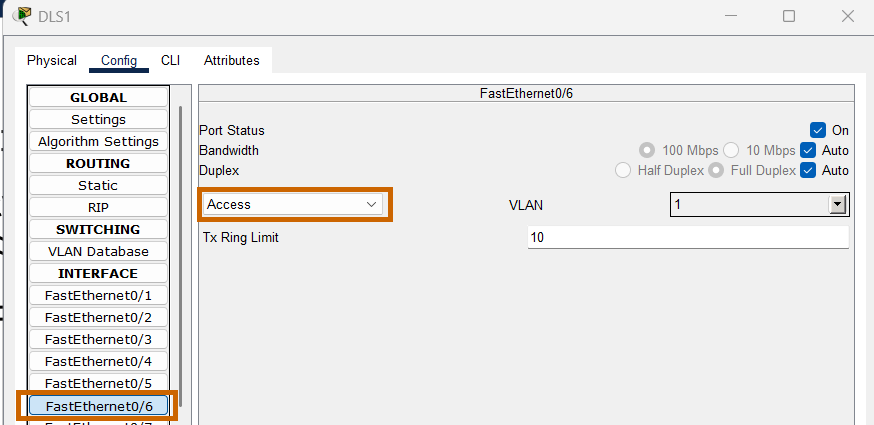
Description générée automatiquement

## Comment expliquez-vous les changements en ce qui concerne la Configuration révision et « Number of existing VLANs » ?

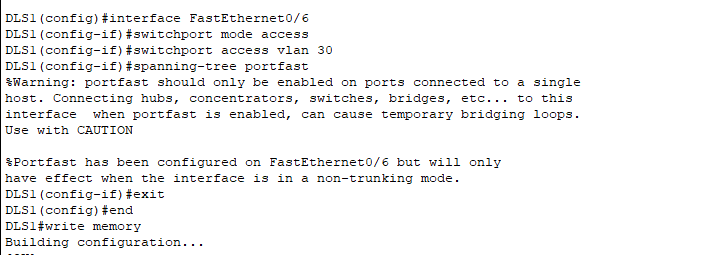
Les changements observés, notamment en ce qui concerne la configuration révision et le nombre de VLANs existants, s'expliquent par le fonctionnement du VTP. Chaque modification de la configuration des VLANs sur le serveur VTP (DLS1) entraîne une incrémentation du numéro de révision de la configuration. Les commutateurs du domaine VTP, comme ALS2, reçoivent ces annonces VTP et mettent à jour leur configuration si le numéro de révision est supérieur à celui qu'ils possèdent actuellement. Par conséquent, lorsque des VLANs sont créés ou modifiés sur DLS1, ces changements se propagent automatiquement aux autres commutateurs du domaine VTP. Ainsi, le nombre de VLANs existants sur ALS2 augmente pour refléter les VLANs définis sur DLS1. Ces modifications, telles que l'incrémentation du numéro de révision et l'augmentation du nombre de VLANs, sont des indications normales que la synchronisation VTP fonctionne correctement, assurant une gestion cohérente et centralisée des VLANs dans le réseau.

# Configurer les ports connectés aux différents hôtes en mode access (fa0/6 )

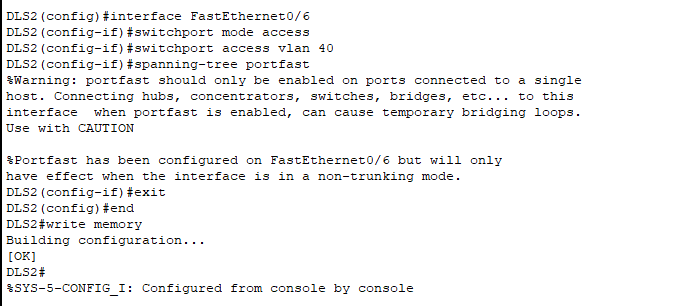
Tous les ports connectés aux différents hôtes sur le commutateur DLS1 ont été configurés en mode accès (Access Mode). Chaque port a été assigné au VLAN approprié, comme illustré pour le port FastEthernet0/6 configuré pour le VLAN 10.



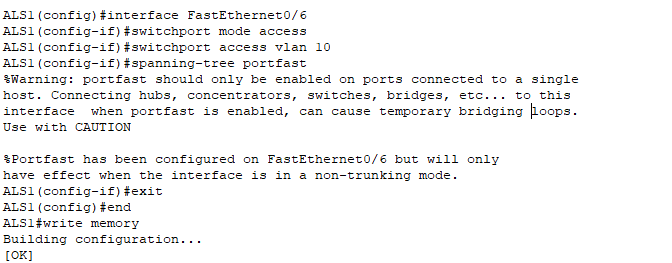
## Sur DLS1 (VLAN 30)



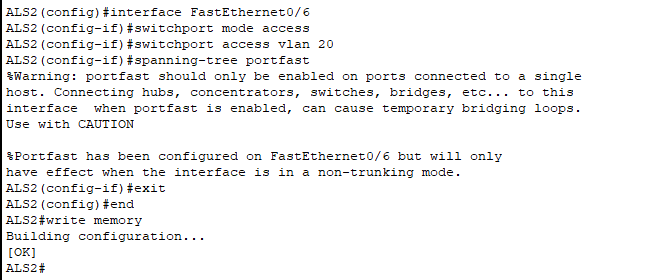
## Sur DLS2 (VLAN 40)



## Sur ALS1 (VLAN 10)

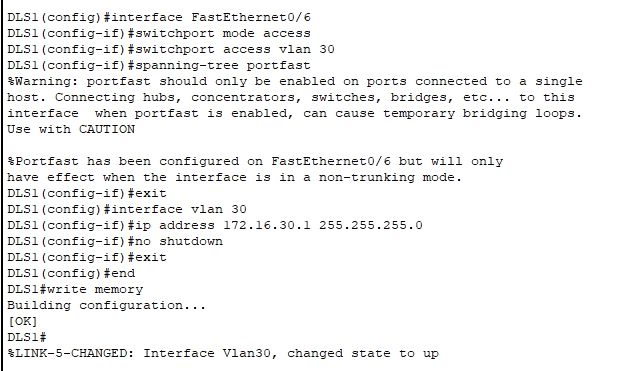


## Sur ALS2 (VLAN 20)

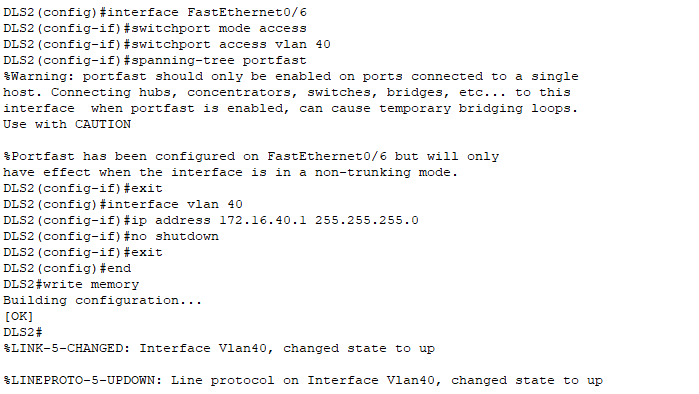


## Configuration des vlan :

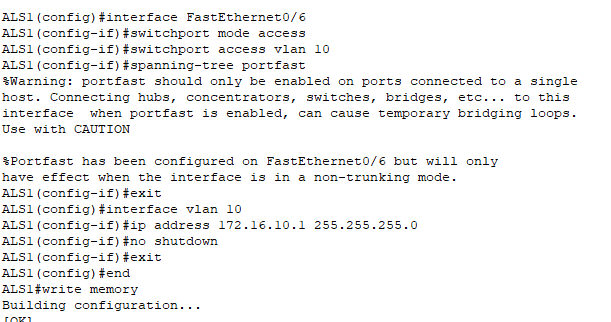
## DSL1 :



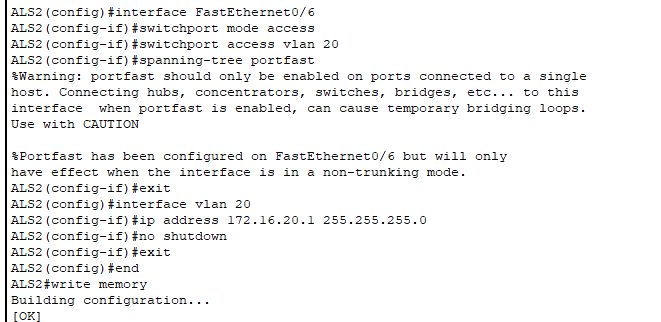
## DSL2 :

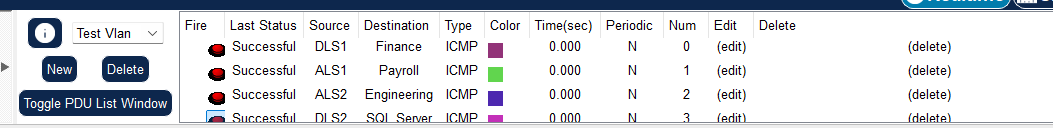


## ALS1 :



## ALS2 :





## Configuration des différente interfaces :

Pour vérifier la connectivité entre différents VLANs, il est nécessaire de tester la communication entre des périphériques appartenant à des VLANs distincts à l’aide des commandes **ping** ou **traceroute**. Si la connectivité attendue échoue, les causes possibles incluent :

* Une mauvaise configuration du routage inter-VLAN,
* Un problème de trunking,
* Des restrictions imposées par des ACL.

Un routage inter-VLAN correctement configuré et une configuration de trunking appropriée sont essentiels pour assurer la communication entre VLANs.

## Faire un ping depuis l’hôte sur le Vlan 10 vers l’hôte sur le VLAN 40. Quel en est le résultat et pourquoi ?

Actuellement, le **ping** entre les VLANs n’est pas possible car il n’y a pas de routeur pour assurer le routage inter-VLAN. Pour permettre la communication entre les VLANs sur les switches, il est nécessaire d'attribuer une adresse IP à chaque switch via le VLAN correspondant. Cela permet aux switches de jouer un rôle de passerelle pour le trafic entre les VLANs, facilitant ainsi le routage inter-VLAN sans besoin immédiat d’un routeur dédié.

DLS1

Une image contenant texte, capture d’écran, Police, document

Description générée automatiquement

DLS2 :

Une image contenant texte, capture d’écran, Police, document

Description générée automatiquement

ALS1 :

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

ALS2 :

Une image contenant texte, capture d’écran, Police, document

Description générée automatiquement

Par défaut, le routage inter-VLAN n'est pas activé sur ces switches. Pour permettre le transfert de trafic entre les VLANs, il est nécessaire d’activer le routage en utilisant la commande suivante : ip routing. Cette commande permet au switch de gérer le routage entre les différents VLANs configurés. Une fois cette fonctionnalité activée et des adresses IP attribuées aux interfaces VLAN correspondantes, le switch pourra assurer la communication entre les VLANs sans nécessiter de routeur externe.

|  |  |
| --- | --- |
|  |  |

Évidemment, cela est impossible à réaliser sur ces switches, car ils fonctionnent au niveau 2 du modèle OSI. Les switches de niveau 2, notamment ceux de marque Cisco, ne prennent pas en charge le routage inter-VLAN. Pour assurer cette fonctionnalité, il est nécessaire d’utiliser un switch de niveau 3 ou un routeur dédié.

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement

Pour configurer **HSRP** afin d’assurer une redondance de lien, suivez les directives suivantes :

Le switch **DLS1** doit être configuré comme routeur actif pour les VLANs 1, 10 et 20 avec une priorité de **150** pour ces VLANs. Il sera le routeur inactif pour les VLANs 30 et 40 avec une priorité de **100**. Inversement, le switch **DLS2** doit être configuré comme routeur actif pour les VLANs 30 et 40 avec une priorité de **150**, et comme routeur inactif pour les VLANs 1, 10 et 20 avec une priorité de **100**.

En complément des adresses IP réelles attribuées à **DLS1** et **DLS2**, configurez une adresse IP virtuelle pour chaque VLAN, comme suit :

* **VLAN 1** : 172.16.1.1
* **VLAN 10** : 172.16.10.1
* **VLAN 20** : 172.16.20.1
* **VLAN 30** : 172.16.30.1
* **VLAN 40** : 172.16.40.1

Une fois cette configuration effectuée, vérifiez la configuration de **HSRP** en vous assurant que **DLS1** est bien le routeur actif pour les VLANs 1, 10 et 20, et que **DLS2** est le routeur actif pour les VLANs 30 et 40.

Ensuite, vérifiez le routage entre **DLS1** et **DLS2** pour assurer une communication fluide entre les VLANs. Pour tester cette connectivité, effectuez un **ping** depuis un hôte du **VLAN 10** vers un hôte du **VLAN 40**.

Si le ping échoue, cela peut être dû à une mauvaise configuration du routage inter-VLAN, une absence de trunking ou des restrictions ACL. Vérifiez ces éléments pour résoudre le problème.

**Configuration pour DLS1**

|  |  |
| --- | --- |
|  | interface vlan 1  ip address 172.16.1.2 255.255.255.0  standby 1 ip 172.16.1.1  standby 1 priority 150  interface vlan 10  ip address 172.16.10.2 255.255.255.0  standby 10 ip 172.16.10.1  standby 10 priority 150  interface vlan 20  ip address 172.16.20.2 255.255.255.0  standby 20 ip 172.16.20.1  standby 20 priority 150  interface vlan 30  ip address 172.16.30.2 255.255.255.0  standby 30 ip 172.16.30.1  standby 30 priority 100  interface vlan 40  ip address 172.16.40.2 255.255.255.0  standby 40 ip 172.16.40.1  standby 40 priority 100 |

**Configuration pour DLS2**

|  |  |
| --- | --- |
|  | conf t  interface vlan 30  ip address 172.16.30.3 255.255.255.0  standby 30 ip 172.16.30.1  standby 30 priority 150  interface vlan 40  ip address 172.16.40.3 255.255.255.0  standby 40 ip 172.16.40.1  standby 40 priority 150  interface vlan 1  ip address 172.16.1.3 255.255.255.0  standby 1 ip 172.16.1.1  standby 1 priority 100  interface vlan 10  ip address 172.16.10.3 255.255.255.0  standby 10 ip 172.16.10.1  standby 10 priority 100  interface vlan 20  ip address 172.16.20.3 255.255.255.0  standby 20 ip 172.16.20.1  standby 20 priority 100 |

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

* **DLS1** est en état **actif** pour le **VLAN 1** avec une priorité de **150**, ce qui est conforme à la configuration.

Une image contenant texte, capture d’écran, Police, document

Description générée automatiquement

* **DLS2** est en état **standby** pour le **VLAN 1** et le **VLAN 10**, avec une priorité de **100**, ce qui est également conforme à la configuration.

Ping pour verifier la connexion l

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Le **ping** vers 172.16.30.3 depuis **DLS1** affiche un taux de réussite de **60 %** (3 sur 5). Cela indique une communication instable ou intermittente. En revanche, le **ping** vers 172.16.40.3 réussit à **100 %** (5 sur 5), montrant une connectivité fiable vers cette adresse.

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Le **ping** vers 172.16.30.3 depuis **DLS2** réussit à **100 %** (5 sur 5) à deux reprises. Cela confirme une connectivité stable entre **DLS2** et l'adresse 172.16.30.3.

Une image contenant texte, capture d’écran, Police, conception

Description générée automatiquement

Le **ping** vers 172.16.30.3 depuis un hôte affiche un taux de réussite de **100 %** (4 sur 4). Les temps de réponse varient entre **<1 ms** et **20 ms**, indiquant une communication fiable avec des performances acceptables.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Le **ping** vers 172.16.40.3 depuis un hôte affiche également un taux de réussite de **100 %** (4 sur 4). Les temps de réponse varient entre **<1 ms** et **92 ms**, montrant une connectivité stable mais avec des délais légèrement plus élevés par moments.

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

Une image contenant texte, diagramme, carte, ligne

Description générée automatiquement

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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 |

## Configurez les PC hôtes.

|  |  |
| --- | --- |
| Une image contenant texte, logiciel, Icône d’ordinateur, nombre  Description générée automatiquement | Une image contenant texte, capture d’écran, logiciel, nombre  Description générée automatiquement |

Les configurations de **PC-A** et **PC-C** ont été correctement remplies avec des adresses IP statiques, des masques de sous-réseau et des passerelles par défaut adaptés, assurant une communication fluide entre les deux machines.

## Configurez les paramètres de base pour chaque routeur.

On se rend compte qu’il non pas de route

Configuration de **R1**

|  |  |
| --- | --- |
| enable  conf t  router rip  network 10.0.0.0  network 192.168.1.0 |  |

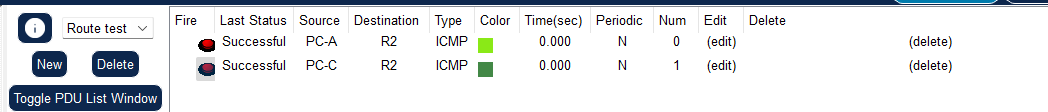
Configuration de **R2**

|  |  |
| --- | --- |
| enable  conf t  router rip  network 192.168.1.0  network 10.0.0.0  network 209.165.200.0 |  |

Configuration de **R3**

|  |  |
| --- | --- |
| enable  conf t  router rip  network 192.168.1.0  network 10.0.0.0 |  |

Après avoir configuré les routes sur **R1**, **R2**, et **R3** avec le protocole **RIP** en ajoutant les réseaux concernés, les **pings** entre **PC-A** et **PC-C** fonctionnent correctement. Cela montre que le routage était le point manquant dans la configuration initiale pour permettre la communication entre les appareils sur différents réseaux.



### 

## Configurez les paramètres de base pour chaque routeur.

La commande **no ip domain-lookup** sur les routeurs Cisco désactive la fonction de résolution de noms de domaine. Voici comment elle fonctionne et pourquoi elle est utile :

**Fonctionnement :**

* Par défaut, lorsqu’une commande incorrecte ou incomplète est saisie, le routeur tente de résoudre cette entrée comme un nom de domaine en envoyant une requête DNS (Domain Name System) pour trouver une adresse IP associée.
* Cette tentative de résolution peut prendre du temps, bloquant l’accès au terminal pendant plusieurs secondes, voire minutes.

1. Désactivez la recherche DNS.

no ip domain-lookup







1. Configurez le nom du périphérique conformément à la topologie.







Configuration R1 :

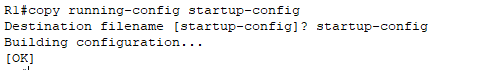
|  |  |
| --- | --- |
| enable  conf t  hostname R1  no ip domain-lookup  interface gigabitEthernet 0/1  ip address 192.168.1.1 255.255.255.0  no shutdown  interface serial 0/0/0  ip address 10.1.1.1 255.255.255.252  clock rate 128000  no shutdown  interface serial 0/0/1  ip address 10.1.1.1 255.255.255.252  clock rate 128000  no shutdown  enable secret class  line con 0  password cisco  login  logging synchronous  line vty 0 4  password cisco  login  logging synchronous |  |

Configuration R3 :

|  |  |
| --- | --- |
| enable  conf t  hostname R3  no ip domain-lookup  interface gigabitEthernet 0/1  ip address 192.168.1.3 255.255.255.0  no shutdown  interface serial 0/0/1  ip address 10.2.2.1 255.255.255.252  clock rate 128000  no shutdown  enable secret class  line con 0  password cisco  login  logging synchronous  line vty 0 4  password cisco  login  logging synchronous |  |

**copy running-config startup-config** permet de sauvegarder la configuration en cours (**running-config**) dans la mémoire de démarrage (**startup-config**). Cela garantit que les modifications sont conservées même après un redémarrage du routeur.

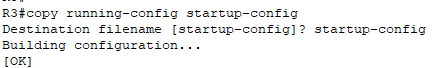
R1 :



R2 :



R3 :



## Configurez les paramètres de base pour chaque commutateur.

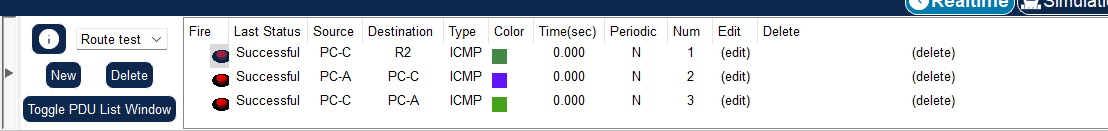
**Configuration de S1 :**

|  |  |
| --- | --- |
| enable  configure terminal  no ip domain-lookup  hostname S1  enable secret class  interface vlan 1  ip address 192.168.1.11 255.255.255.0  no shutdown  ip default-gateway 192.168.1.1  line con 0  password cisco  login  logging synchronous  line vty 0 4  password cisco  login  logging synchronous |  |

**Configuration de S3 :**

|  |  |
| --- | --- |
| enable  configure terminal  no ip domain-lookup  hostname S3  enable secret class  interface vlan 1  ip address 192.168.1.13 255.255.255.0  no shutdown  ip default-gateway 192.168.1.3  line con 0  password cisco  login  logging synchronous  line vty 0 4  password cisco  login  logging synchronous |  |

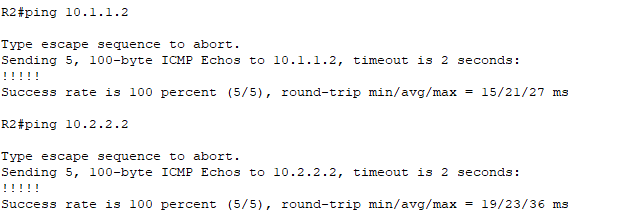
**Vérifiez la connectivité entre PC-A et PC-C :**



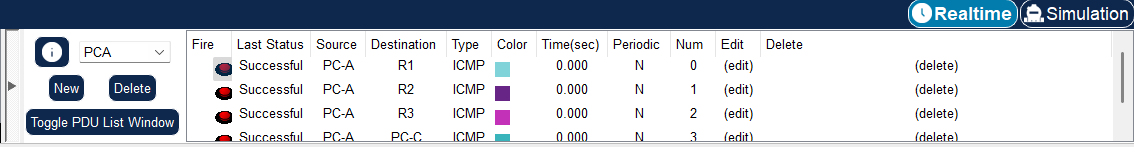
Configurez le routage :



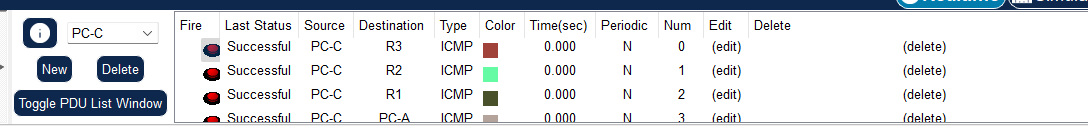
Vérifiez la connectivité.



PC-A

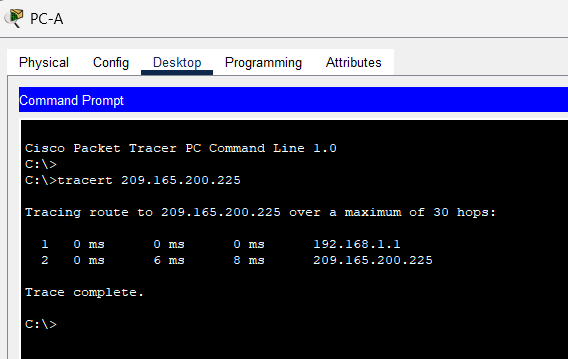


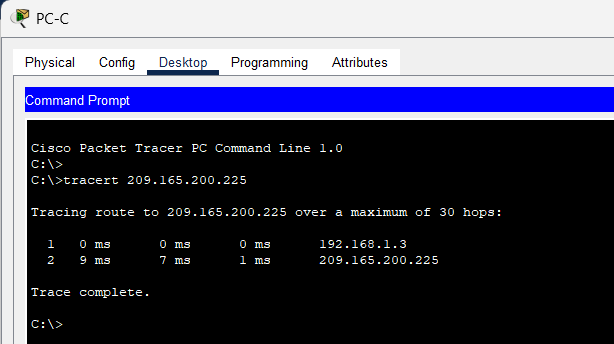
PC-C

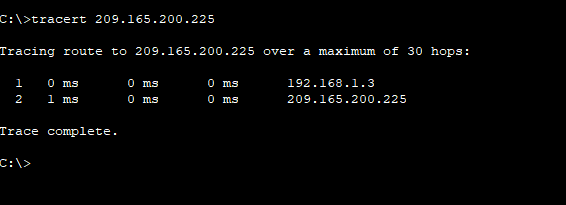


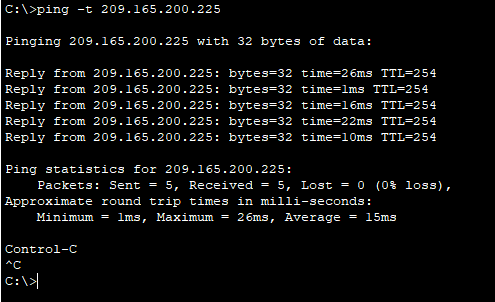
## Configuration de la redondance au premier saut avec HSRP

Déterminez le chemin du trafic internet pour PC-A et PC-C.

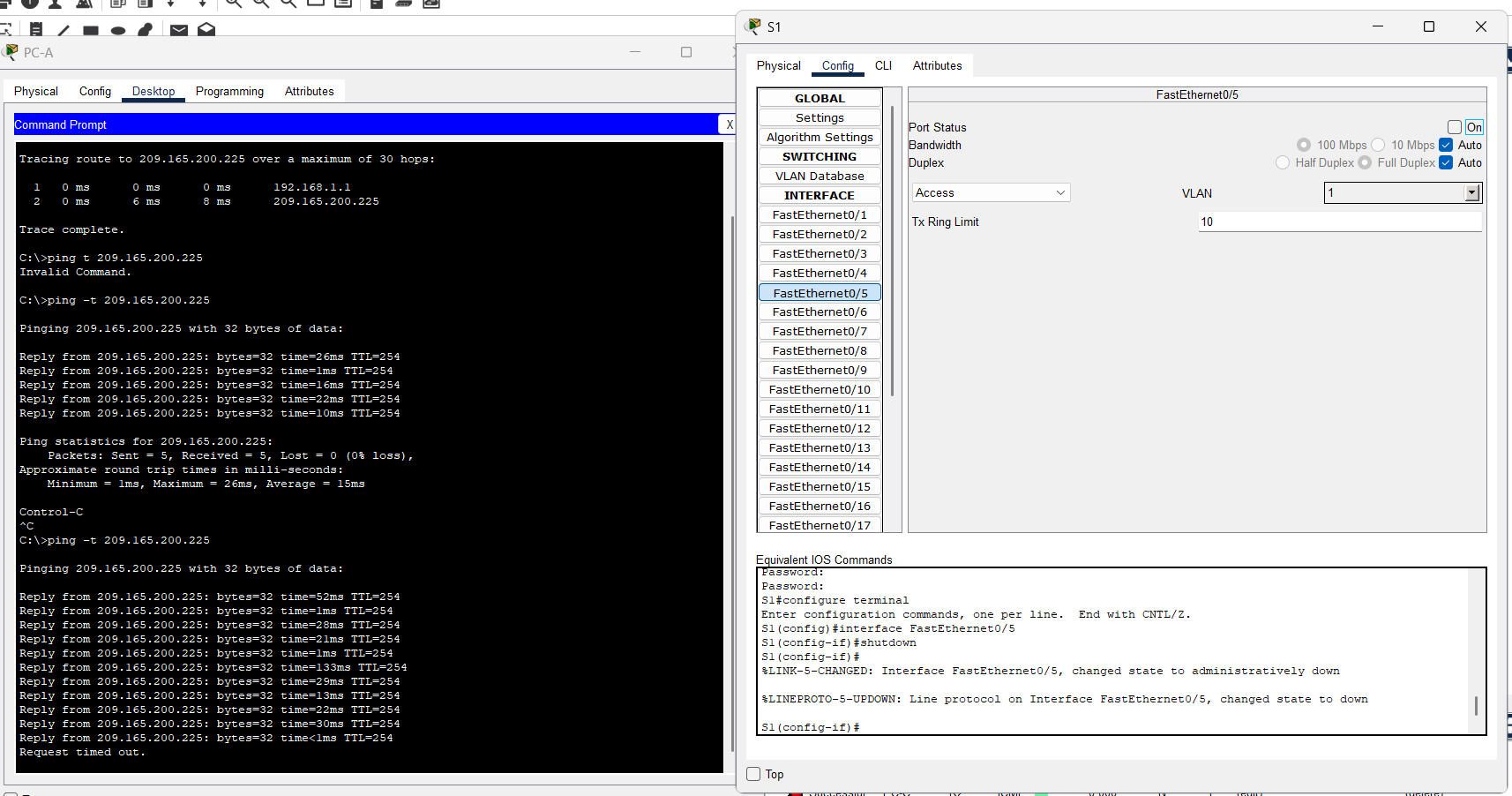




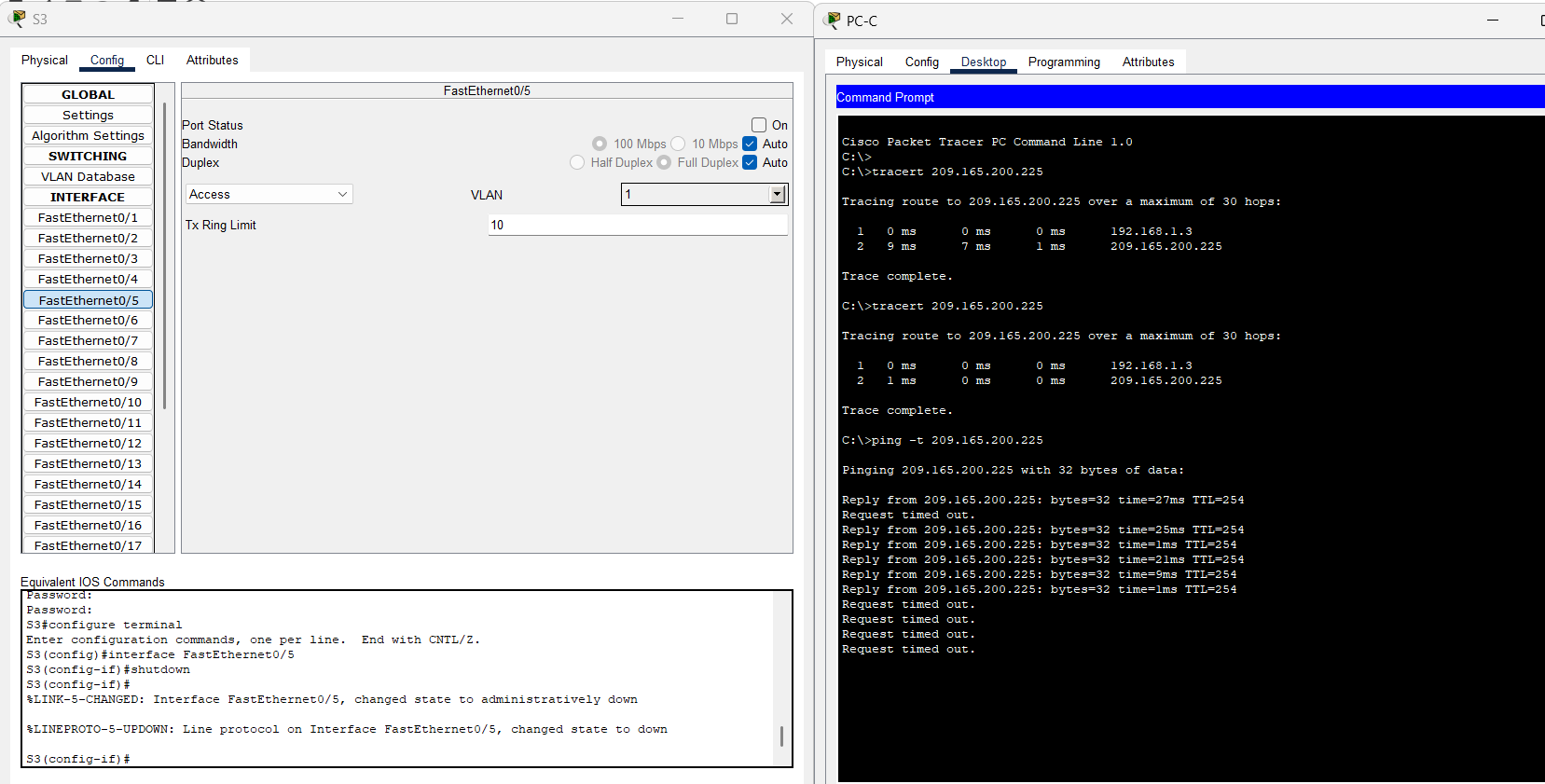




1. Pendant le traitement de la requête ping, déconnectez le câble Ethernet de F0/5 sur S1. Vous pouvez également désactiver l’interface S1 F0/5, ce qui revient au même.



1. Quels seraient les résultats si vous répétiez les étapes 2a et 2b sur PC-C et S3 ?



La connexion se refait bien d’elle-même quand on reconnecte

**Configurez le protocole HSRP sur R1 et R3.**

Au cours de cette étape, vous allez configurer le protocole HSRP et remplacer l’adresse de passerelle par défaut sur PC-A, PC-C, S1 et S2 par l’adresse IP virtuelle du protocole HSRP. R1 devient le routeur actif via la configuration de la commande de priorité du protocole HSRP.

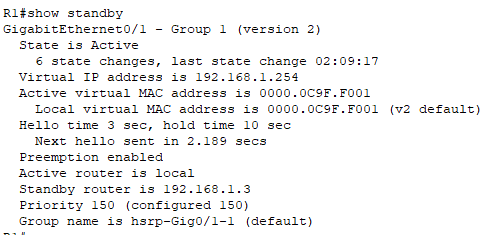
**Configuration de R1**

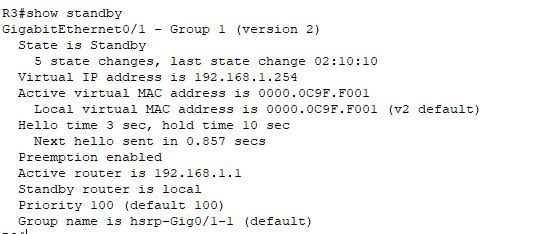
|  |  |
| --- | --- |
|  | configure terminal  interface GigabitEthernet0/1  standby 1 ip 192.168.1.254  standby 1 priority 150  standby 1 preempt  standby 1 authentication cisco  standby version 2  exit  write memory |

**Configuration de R3**

|  |  |
| --- | --- |
|  | configure terminal  interface GigabitEthernet0/1  standby 1 ip 192.168.1.254  standby 1 priority 100  standby 1 preempt  standby 1 authentication cisco  standby version 2  exit  write memory |

#### Vérifiez le protocole HSRP en exécutant la commande show standby sur R1 et R3.





1. À l’aide des résultats illustrés ci-dessus, répondez aux questions suivantes :

* Quel routeur est le routeur actif ?

Le routeur actif est **R1**.

**Justification :**

* Dans la sortie de la commande **show standby** pour **R1**, il est indiqué que l’état est **"Active"** et que **"Active router is local"**.
* Pour **R3**, l'état est **"Standby"** et il est précisé que **"Active router is 192.168.1.1"**, qui correspond à **R1**.

La priorité configurée de **150** sur **R1** est supérieure à celle de **100** sur **R3**, ce qui permet à **R1** d’être le routeur actif.

**Quelle est l’adresse MAC pour l’adresse IP virtuelle ?**

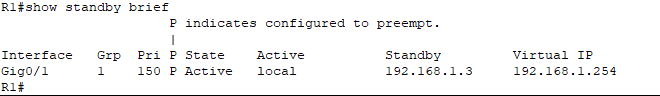
L’adresse MAC virtuelle est **0000.0C9F.F001**. Elle est identique pour les deux routeurs (**R1** et **R3**) car ils font partie du même groupe **HSRP**.

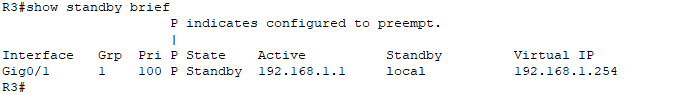
**Quelles sont l’adresse IP et la priorité du routeur en veille ?**

**Adresse IP du routeur en veille :** **192.168.1.3** (correspondant à **R3**).

**Priorité du routeur en veille :** **100**.

1. Exécutez la commande show standby brief sur R1 et R3 pour afficher un récapitulatif de l’état du protocole HSRP. L’exemple de résultat est affiché ci-dessous.



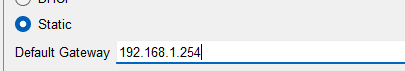


Ces résultats confirment que **R1** est le routeur **actif** avec une priorité de **150**, tandis que **R3** est le routeur **de secours** avec une priorité de **100**. L'adresse IP virtuelle partagée est **192.168.1.254**.

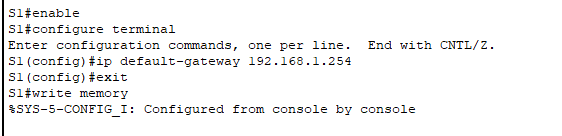
1. Modifiez l’adresse de passerelle par défaut pour PC-A, PC-C, S1 et S3. Quelle adresse devez-vous utiliser ?

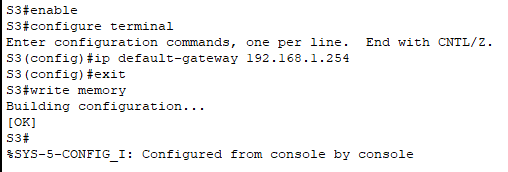
L’adresse de passerelle par défaut à configurer pour **PC-A**, **PC-C**, **S1** et **S3** est : 192.168.1.254

Cette adresse correspond à l'adresse IP virtuelle configurée avec **HSRP** pour assurer une redondance et une haute disponibilité du réseau.

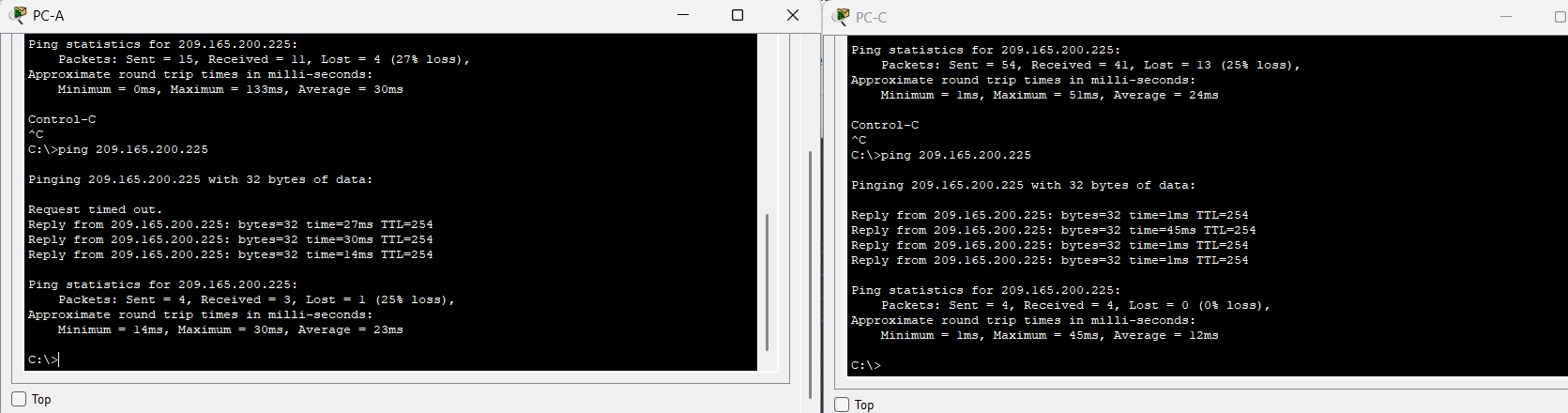


Pour changer la passerelle par défaut sur **S1** et **S3**, utilisez les commandes suivantes :

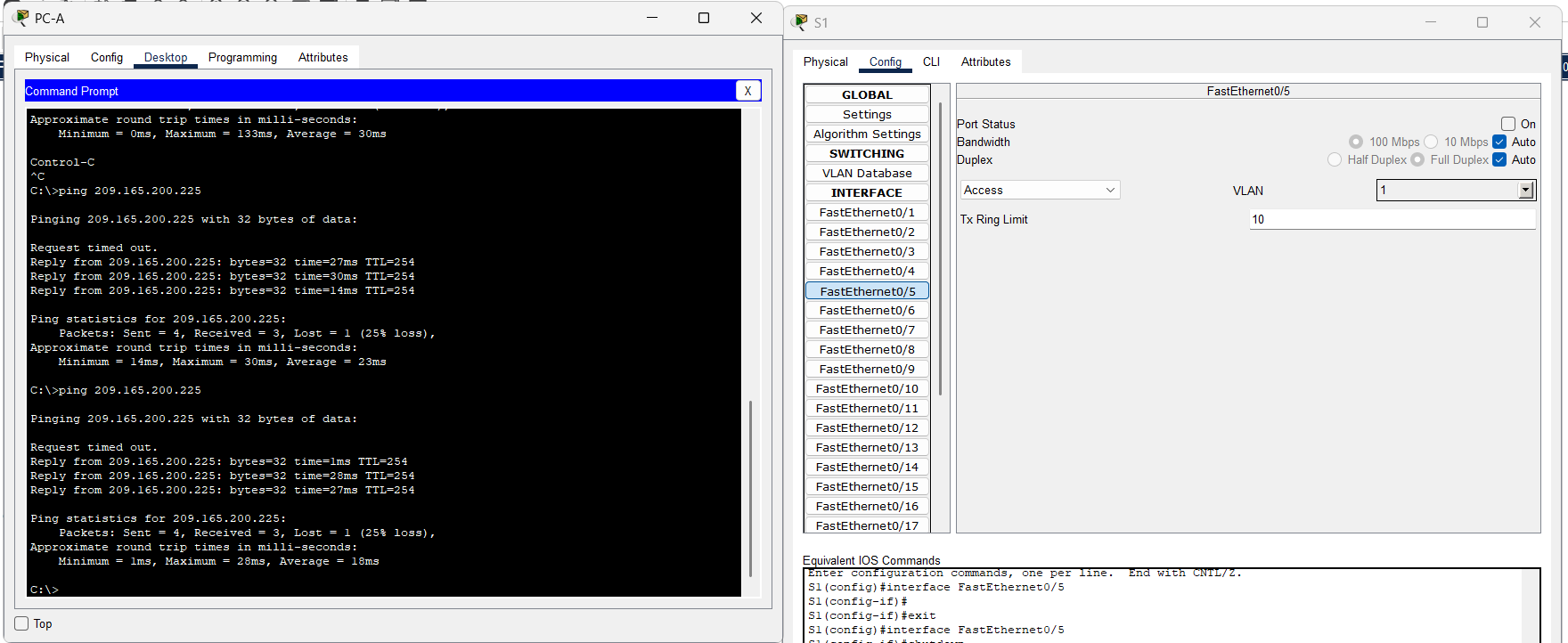




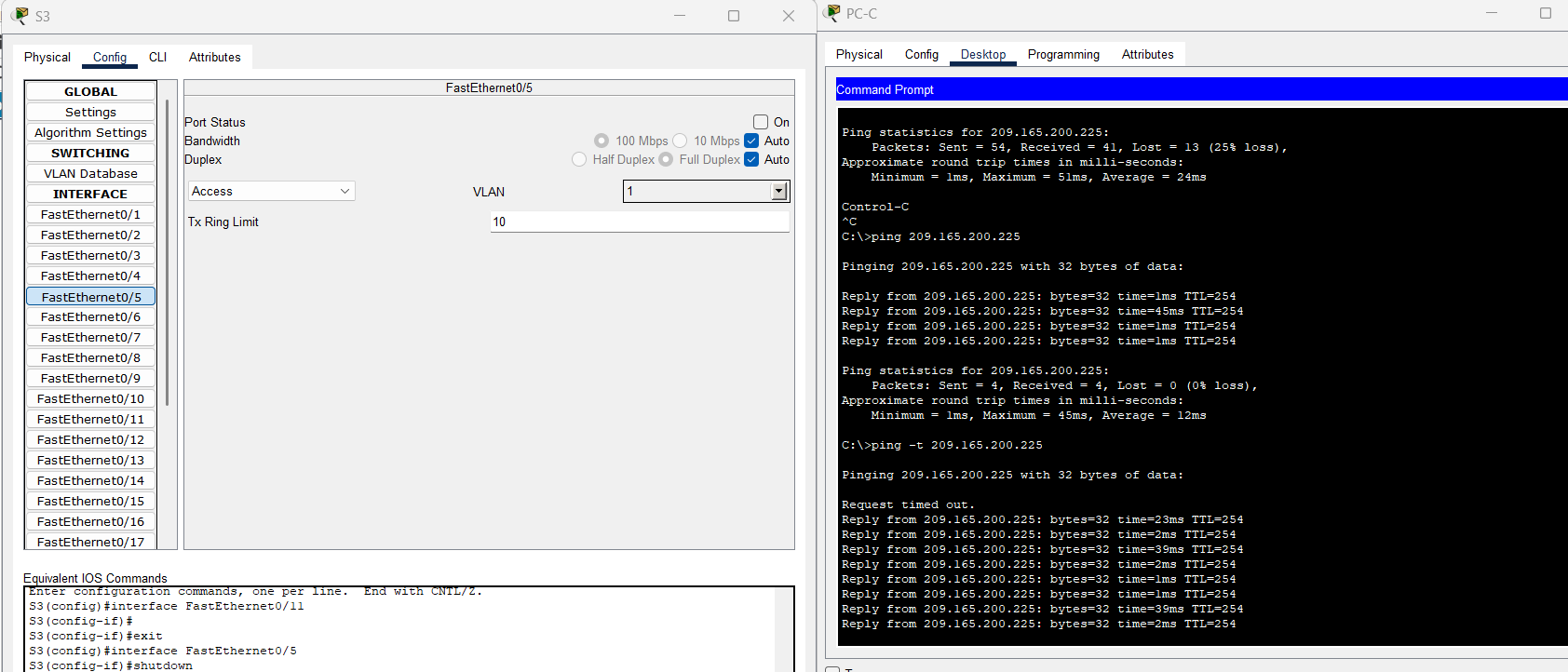
**Vérifiez les nouveaux paramètres. Envoyez une requête ping à partir de PC-A et de PC-C vers l’adresse de bouclage de R2. Les requêtes ping ont-elles abouti ?**



## Démarrez une session ping sur PC-A et rompez la connexion entre le commutateur qui est connecté au routeur HSRP actif (R1).



Dans cette capture, le **ping** démarre correctement depuis **PC-A** vers l'adresse de destination. Après avoir rompu la connexion entre le commutateur connecté au routeur **HSRP** actif (**R1**), on observe une brève interruption des réponses, indiquant une perte momentanée de paquets. Cependant, le protocole **HSRP** permet à **R3** de prendre le relais rapidement, et le ping reprend avec succès. Cela confirme que le basculement fonctionne bien, avec seulement un micro temps d'arrêt avant que la nouvelle ligne ne prenne le relais.

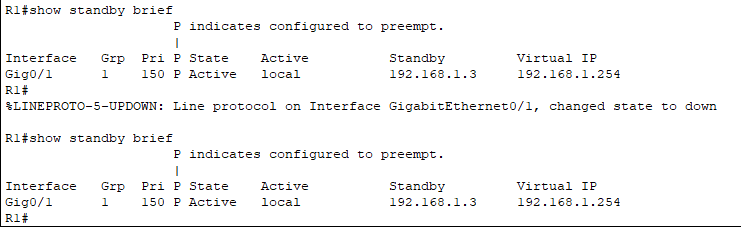


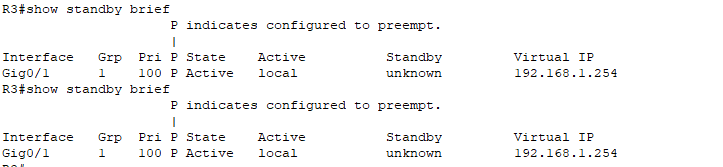
Dans les deux captures, les sessions **ping** depuis **PC-A** et **PC-C** fonctionnent correctement. Lors de la coupure de la connexion avec le commutateur relié au routeur **HSRP** actif (**R1**), on observe un bref arrêt des réponses. Cela est dû au temps nécessaire pour que **R3** prenne le relais. Après cette courte interruption, le **ping** reprend normalement, indiquant que le basculement **HSRP** fonctionne correctement.

## Vérifiez les paramètres du protocole HSRP sur R1 et R3.

Exécutez la commande show standby brief sur R1 et R3.

Quel routeur est le routeur actif ?



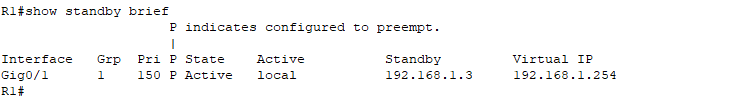


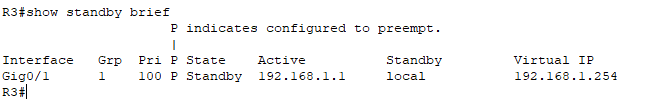
Le routeur actif est **R3**.

**Justification :**

* Dans la sortie de la commande **show standby brief** pour **R3**, l'état est indiqué comme **"Active"** avec une priorité de **100**.
* Sur **R1**, bien que la priorité soit de **150**, l'interface **GigabitEthernet0/1** est passée à l’état **down**, empêchant **R1** de rester actif.
* Lorsque l'interface de **R1** est désactivée, **R3** prend le relais et devient le routeur actif par défaut.

**Reconnectez le câble entre le commutateur et le routeur ou activez l’interface F0/5. Quel est à présent le routeur actif ? Expliquez votre réponse.**





Le routeur actif est maintenant **R1**.

**Explication :**

* Après avoir reconnecté le câble ou activé l’interface, **R1** revient à l'état actif.
* La sortie de la commande **show standby brief** montre que **R1** est en état **"Active"** avec une priorité de **150**, supérieure à celle de **R3** (**100**).
* Grâce à la commande **preempt**, **R1** reprend automatiquement le rôle de routeur actif lorsqu’il revient en ligne, car sa priorité est plus élevée.

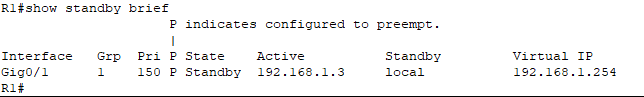
Cela garantit que le routeur avec la priorité la plus élevée assure le routage en cas de retour à la normale.

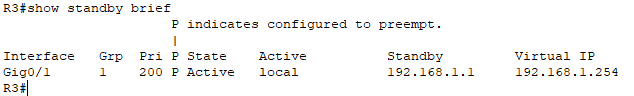
## Modifiez les priorités HSRP.

Définissez la priorité HSRP sur 200 sur R3. Quel est le routeur actif ?

|  |  |
| --- | --- |
| configure terminal  interface GigabitEthernet0/1  standby 1 priority 200  standby 1 preempt  standby 1 authentication cisco  exit  exit  write memory |  |

Exécutez la commande permettant de définir le routeur actif sur R3 sans modifier la priorité. Quelle commande avez-vous utilisée ?





Le routeur actif est **R3**.

**Justification :**

* Après avoir configuré la priorité **HSRP** sur **R3** à **200**, celle-ci dépasse la priorité de **R1** (qui est à **150**).
* Le message **%HSRP-6-STATECHANGE: GigabitEthernet0/1 Grp 1 state Standby -> Active** confirme que **R3** est passé de l'état **"Standby"** à **"Active"**.
* La commande **standby 1 preempt** permet à **R3** de prendre automatiquement le rôle de routeur actif dès que sa priorité devient la plus élevée.

1. **Pourquoi une redondance serait-elle nécessaire dans un LAN ?**

La redondance dans un réseau local (LAN) est avant tout un gage de continuité de service et de fiabilité. En mettant en place des chemins de communication multiples entre les équipements et en doublant certains composants critiques, on s’assure qu’en cas de défaillance matérielle, de panne d’un lien ou même d’une maintenance planifiée, le trafic puisse automatiquement basculer vers une autre route disponible. Cette approche limite les interruptions de service, réduit les risques de perte de données et maintient la productivité des utilisateurs, ce qui est particulièrement bénéfique pour une entreprise. Par ailleurs, la redondance peut également aider à équilibrer la charge sur le réseau, améliorant ainsi la qualité du service, la disponibilité des ressources et l’efficacité globale du LAN.

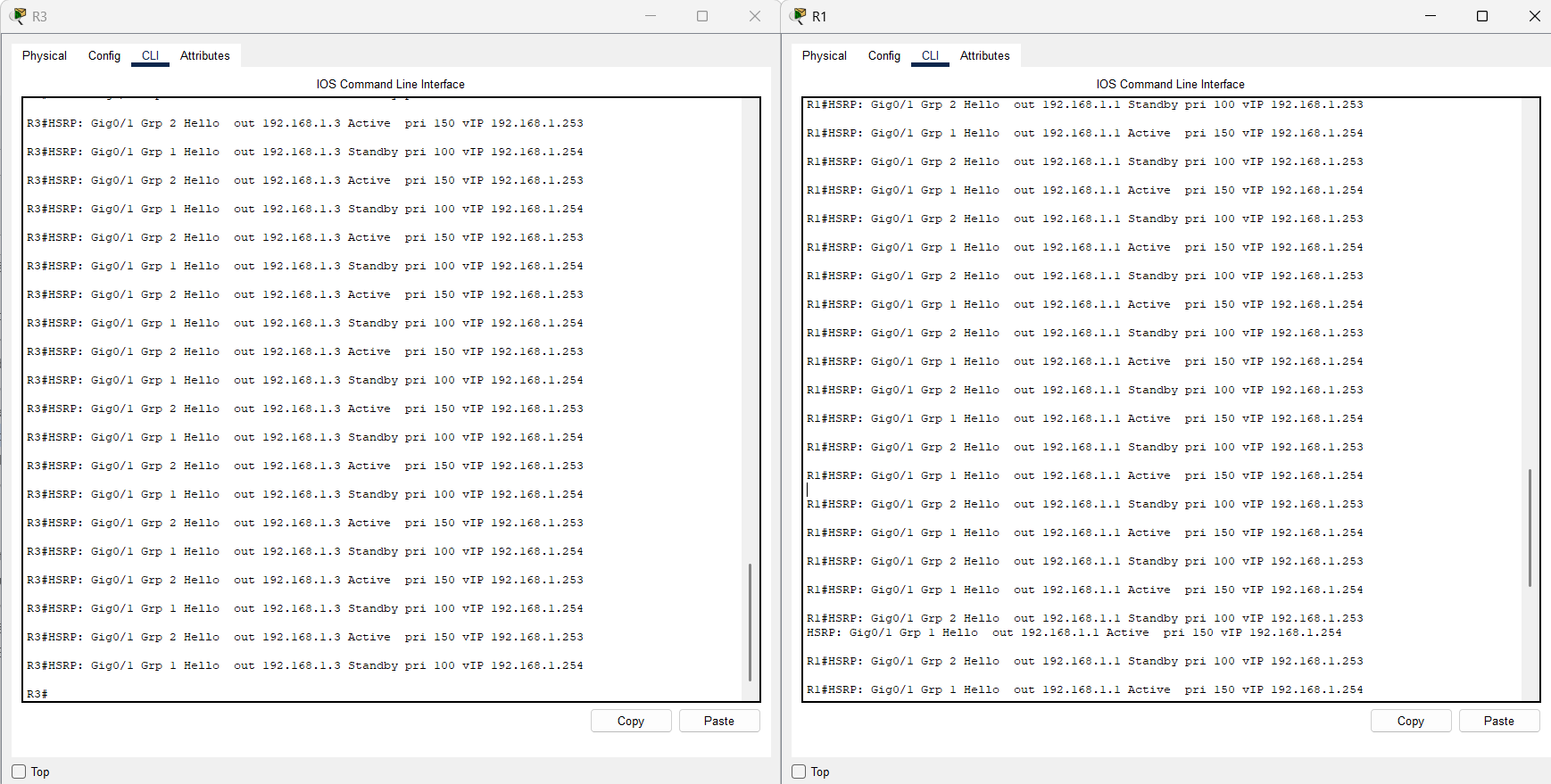
## présenter vos configurations

|  |  |
| --- | --- |
| interface GigabitEthernet0/1  standby 1 ip 192.168.1.254  standby 1 priority 150  standby 1 preempt  standby 1 authentication cisco  standby 2 ip 192.168.1.253  standby 2 priority 100  standby 2 preempt  standby 2 authentication cisco | interface GigabitEthernet0/1  standby 1 ip 192.168.1.254  standby 1 priority 100  standby 1 preempt  standby 1 authentication cisco  standby 2 ip 192.168.1.253  standby 2 priority 150  standby 2 preempt  standby 2 authentication cisco |

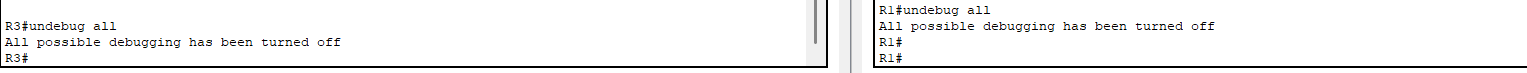
## montrer que la répartition de charges est réalisée selon le mode Round Robin

Grâce à la configuration de deux groupes HSRP distincts (avec les adresses IP virtuelles 192.168.1.254 et 192.168.1.253) répartis entre R1 et R3, la répartition de charge est assurée de manière alternée. Les valeurs de priorité mises en place, dont celles de R1 (110) et de R3 (200) pour le groupe 1, permettent d’établir clairement les rôles Active et Standby. L’analyse des paquets HSRP « Hello » confirme la prise en compte de ces priorités et la bonne attribution des statuts, garantissant ainsi une continuité de service ainsi qu’un équilibre de la charge réseau entre les deux routeurs.

debug standby packets

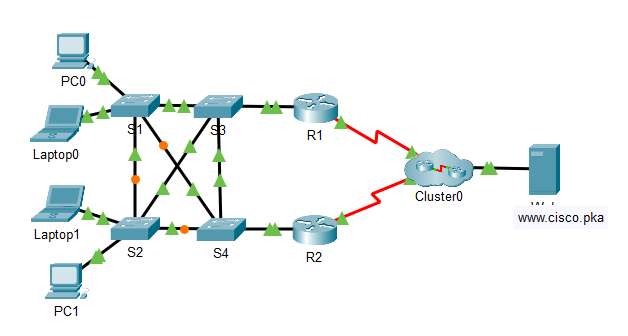


Pour mettre fin au débogage des paquets HSRP (« standby packets ») sur un routeur Cisco, il suffit d’entrer la commande suivante en mode privilégié :

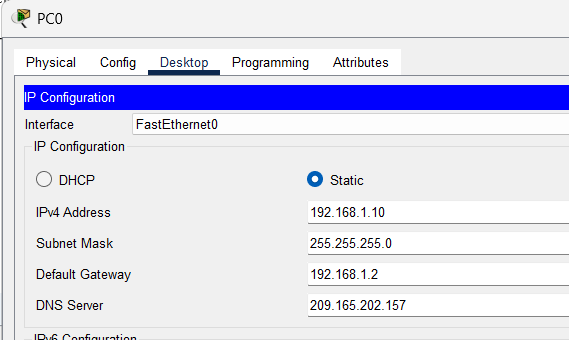


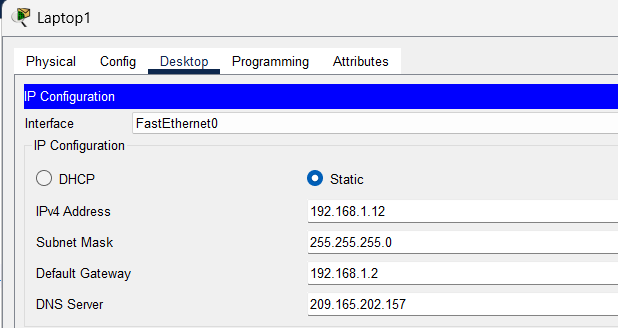
# Exercice 3 : Packet Tracer – Dépannage du protocole HSRP

Au cours de cet exercice, vous allez identifier et résoudre les problèmes relatifs au protocole HSRP sur le réseau. Vous vérifierez également que toutes les configurations HSRP respectent les exigences réseau.

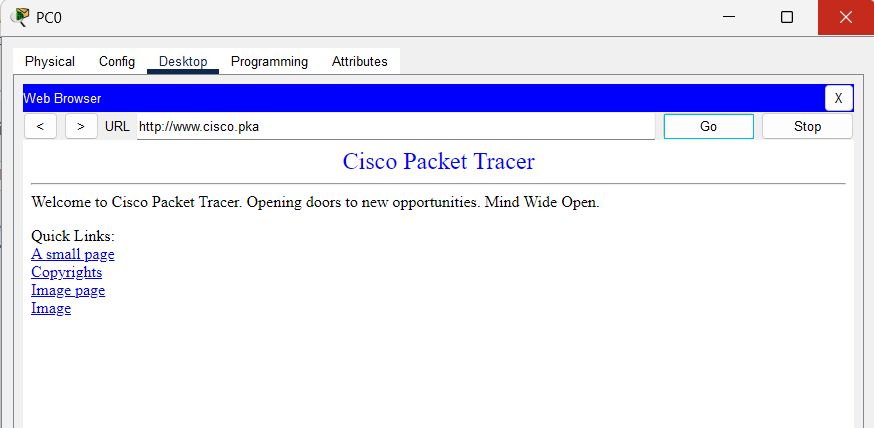


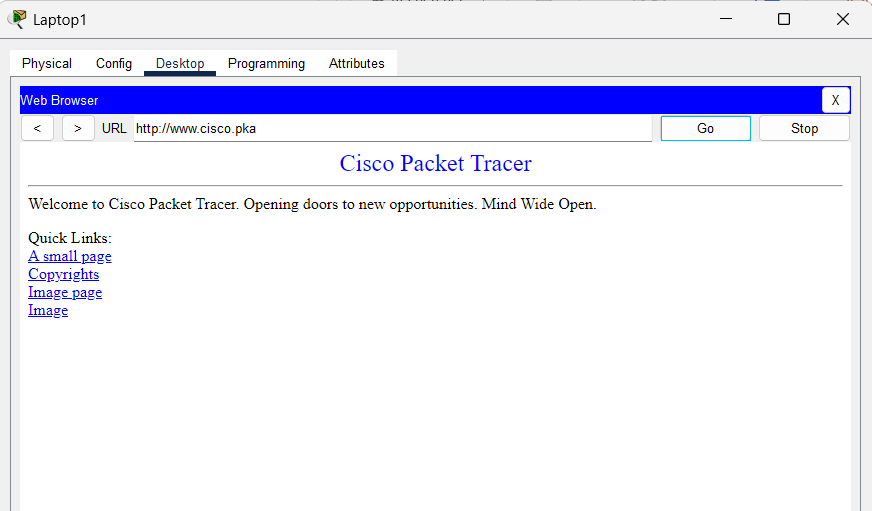
Ordinateurs de bureau et portables



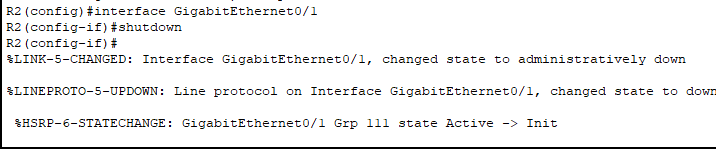


Sur la base des exigences réseau listées ci-dessus, vérifiez que les ordinateurs de bureau et portables peuvent accéder à [www.cisco.pka](http://www.cisco.pka).





Dépannez R1.



Utilisez des commandes show pour identifier les problèmes. Consignez et corrigez tout problème détecté sur R1.

**R1 :**

|  |
| --- |
| version 15.1  no service timestamps log datetime msec  no service timestamps debug datetime msec  no service password-encryption  hostname R1  no ip cef  no ipv6 cef  license udi pid CISCO1941/K9 sn FTX152452E3  no ip domain-lookup  spanning-tree mode pvst  interface GigabitEthernet0/0  no ip address  duplex auto  speed auto  shutdown  interface GigabitEthernet0/1  ip address 192.168.1.1 255.255.255.0  ip nat inside  duplex auto  speed auto  standby version 2  standby 11 ip 192.168.1.254  standby 11 priority 50  interface Serial0/0/0  ip address 209.165.200.226 255.255.255.252  ip nat outside  interface Serial0/0/1  no ip address  clock rate 2000000  shutdown  interface Vlan1  no ip address  shutdown  ip nat inside source list 1 interface Serial0/0/0 overload  ip classless  ip route 0.0.0.0 0.0.0.0 Serial0/0/0  ip flow-export version 9  access-list 1 permit 192.168.1.0 0.0.0.255  line con 0  line aux 0  line vty 0 4  login  end |

**R2 :**

|  |
| --- |
| version 15.1  no service timestamps log datetime msec  no service timestamps debug datetime msec  no service password-encryption  hostname R2  no ip cef  no ipv6 cef  license udi pid CISCO1941/K9 sn FTX1524V236  no ip domain-lookup  spanning-tree mode pvst  interface GigabitEthernet0/0  no ip address  duplex auto  speed auto  shutdown  interface GigabitEthernet0/1  ip address 192.168.1.2 255.255.255.0  ip nat inside  duplex auto  speed auto  shutdown  standby version 2  standby 111 ip 192.168.1.254  interface Serial0/0/0  no ip address  ip nat outside  clock rate 2000000  shutdown  interface Serial0/0/1  ip address 209.165.200.230 255.255.255.252  ip nat outside  interface Vlan1  no ip address  shutdown  ip nat inside source list 1 interface Serial0/0/1 overload  ip classless  ip route 0.0.0.0 0.0.0.0 Serial0/0/1  ip flow-export version 9  access-list 1 permit 192.168.1.0 0.0.0.255  no cdp run  line con 0  line aux 0  line vty 0 4  login  end |

Réactivez l’interface G0/1 sur R2.



Dépannez R2.



Utilisez des commandes show pour identifier d’éventuels problèmes. Consignez et corrigez tout problème détecté sur R2.

|  |
| --- |
| version 15.1  no service timestamps log datetime msec  no service timestamps debug datetime msec  no service password-encryption  hostname R2  no ip cef  no ipv6 cef  license udi pid CISCO1941/K9 sn FTX1524V236  no ip domain-lookup  spanning-tree mode pvst  interface GigabitEthernet0/0  no ip address  duplex auto  speed auto  shutdown  interface GigabitEthernet0/1  ip address 192.168.1.2 255.255.255.0  ip nat inside  duplex auto  speed auto  standby version 2  standby 111 ip 192.168.1.254  interface Serial0/0/0  no ip address  ip nat outside  clock rate 2000000  shutdown  interface Serial0/0/1  ip address 209.165.200.230 255.255.255.252  ip nat outside  interface Vlan1  no ip address  shutdown  ip nat inside source list 1 interface Serial0/0/1 overload  ip classless  ip route 0.0.0.0 0.0.0.0 Serial0/0/1  ip flow-export version 9  access-list 1 permit 192.168.1.0 0.0.0.255  no cdp run  line con 0  line aux 0  line vty 0 4  login  end |

En comparant la configuration de R2 avec celle de R1, on constate un problème de cohérence au niveau de la configuration HSRP. Sur R1, le groupe HSRP utilisé est le groupe 11, tandis que sur R2, c’est le groupe 111 qui est configuré. Pour que les deux routeurs participent correctement au même groupe de redondance, ils doivent utiliser le même numéro de groupe HSRP et la même adresse IP virtuelle. Cette incohérence empêche R2 de prendre part au fonctionnement normal du groupe HSRP et, par conséquent, d’assurer la redondance attendue.

**Commande de vérification :**

* show standby sur R2 pour vérifier le groupe HSRP actuel et l’état du routeur dans ce groupe.

**Correction recommandée :**  
Modifier la configuration HSRP sur R2 afin d’utiliser le groupe 11 au lieu de 111, et s’assurer que l’adresse IP virtuelle est identique à celle de R1. Par exemple :

configure terminal

interface GigabitEthernet0/1

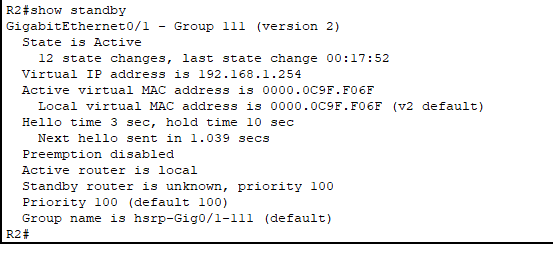
no standby 111 ip 192.168.1.254

standby 11 ip 192.168.1.254

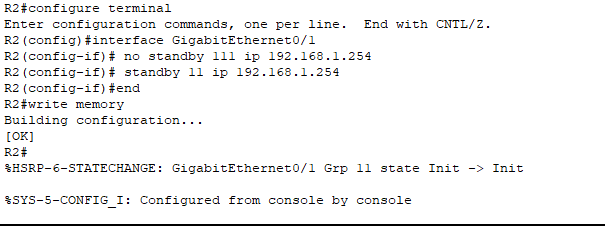
end

write memory

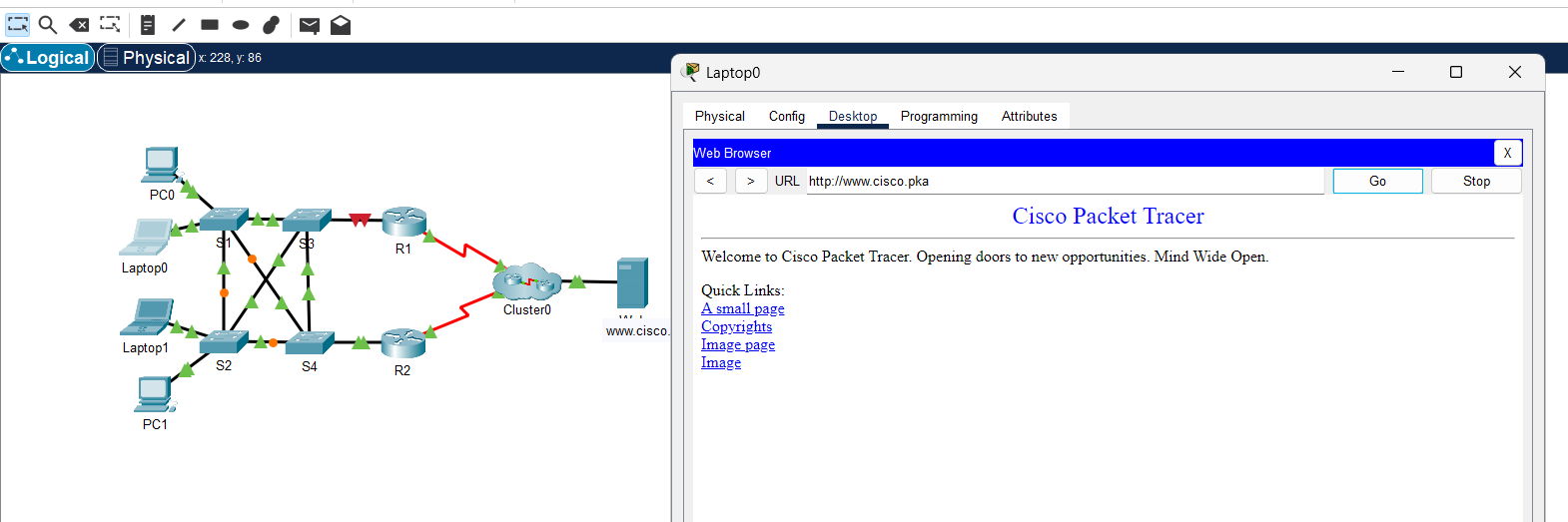
Après cette correction, R2 fera partie du même groupe HSRP que R1, permettra le basculement correct en cas de défaillance et contribuera à la redondance attendue.

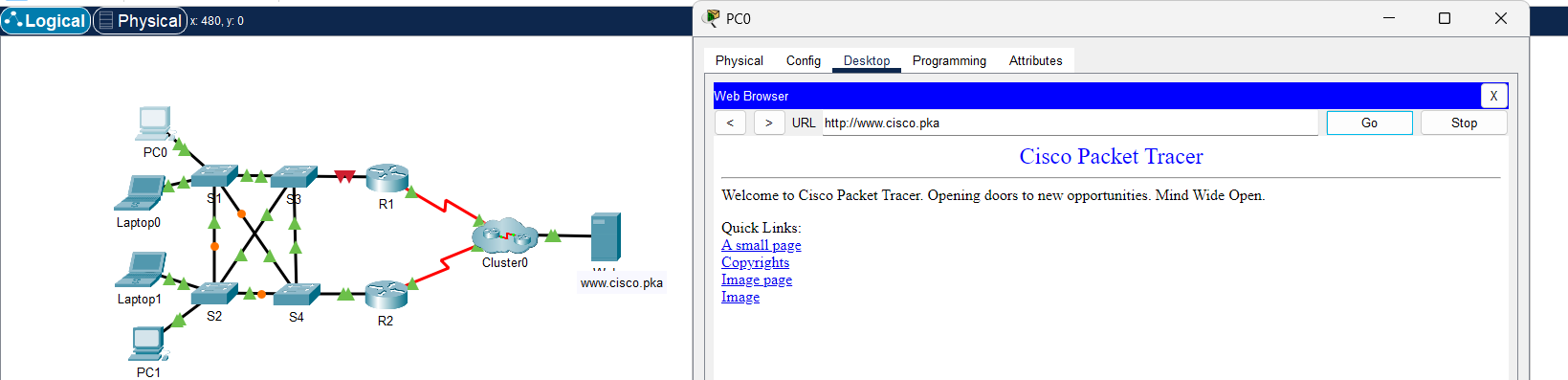


Comme le montre la sortie de la commande show standby sur R2, le routeur est actuellement « Active » pour le groupe HSRP 111, avec une adresse IP virtuelle 192.168.1.254. Le problème, comme identifié précédemment, est que ce groupe 111 ne correspond pas à celui utilisé par R1, qui est le groupe 11. Cette incohérence empêche l’établissement correct de la redondance HSRP entre R1 et R2.

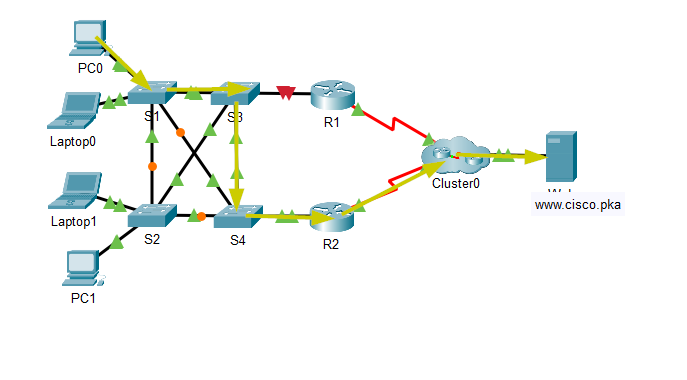


Après cette modification, R2 fera partie du même groupe HSRP que R1 et pourra ainsi participer correctement à la redondance du réseau, assurant le basculement automatique en cas de défaillance de l’un des routeurs.

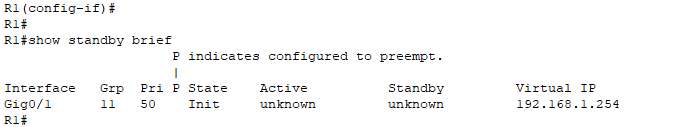


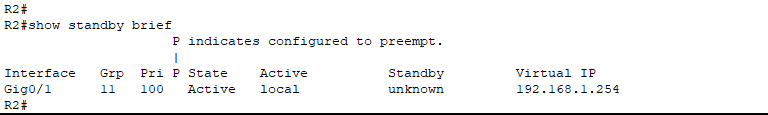


Après avoir corrigé le groupe HSRP sur R2 pour qu’il corresponde à celui de R1, la redondance est désormais opérationnelle. Le trafic bascule correctement en cas de défaillance, et les postes clients peuvent accéder sans interruption à la ressource distante. Le bon fonctionnement visible dans le navigateur depuis PC0 et Laptop0 confirme que la configuration HSRP est à présent cohérente et efficace.

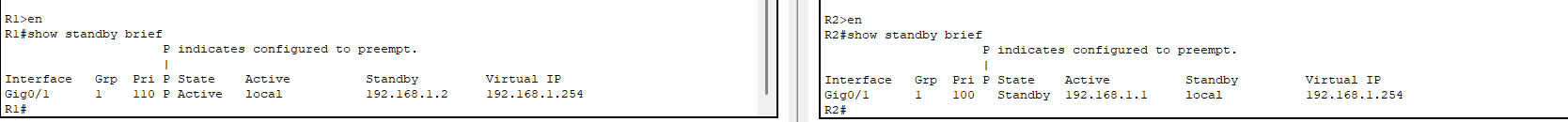


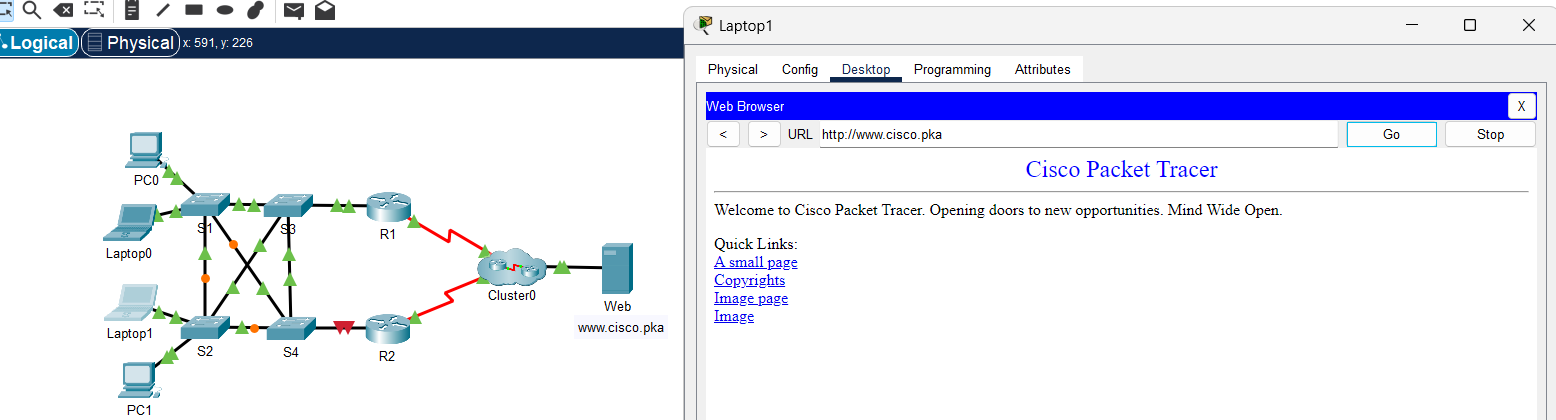
#### Vérifiez la connectivité.



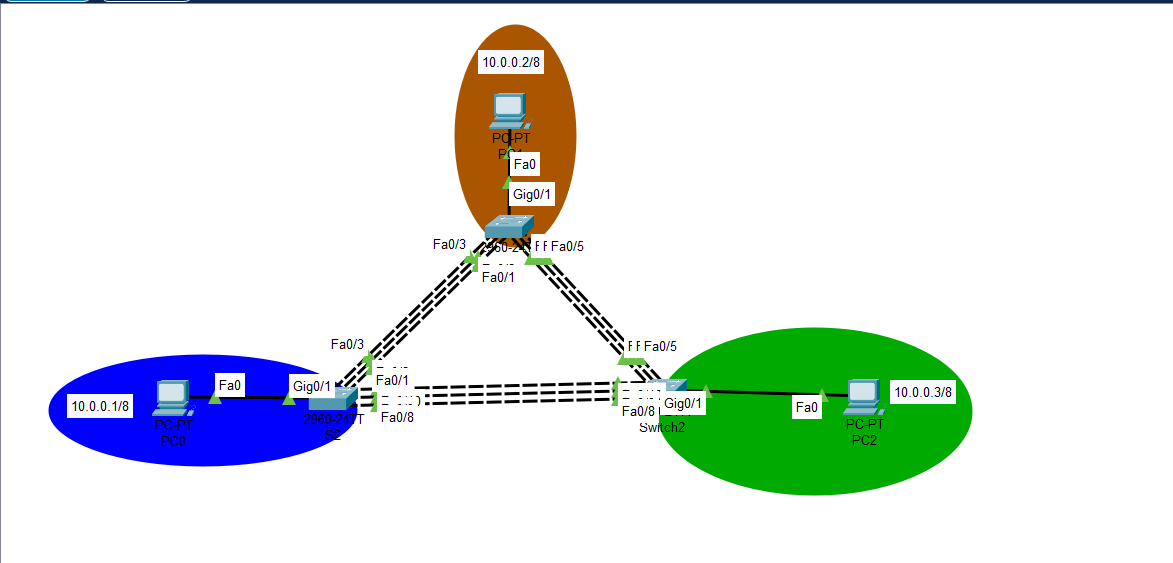


Puis :





# Exercice 4 :Etherrchannel avancé



## SW1 Configuration de Port-Channel 1 avec PAgP

|  |
| --- |
| interface FastEthernet0/1  channel-group 1 mode desirable  switchport mode dynamic desirable  interface FastEthernet0/2  channel-group 1 mode desirable  switchport mode dynamic desirable  interface FastEthernet0/3  channel-group 1 mode desirable  switchport mode dynamic desirable  interface FastEthernet0/5  channel-group 2 mode active  switchport trunk native vlan 2  interface FastEthernet0/6  channel-group 2 mode active  switchport trunk native vlan 2  interface FastEthernet0/7  channel-group 2 mode active  switchport trunk native vlan 2  interface Port-channel 1  switchport mode dynamic desirable  interface Port-channel 2  switchport trunk native vlan 2  spanning-tree vlan 1 root primary |

**SW2 :**

|  |
| --- |
| interface FastEthernet0/1  channel-group 1 mode auto  interface FastEthernet0/2  channel-group 1 mode auto  interface FastEthernet0/3  channel-group 1 mode auto  interface FastEthernet0/8  channel-group 3 mode on  switchport trunk native vlan 3  switchport mode trunk  interface FastEthernet0/9  channel-group 3 mode on  switchport trunk native vlan 3  switchport mode trunk  interface FastEthernet0/10  channel-group 3 mode on  switchport trunk native vlan 3  switchport mode trunk  interface Port-channel 3  switchport trunk native vlan 3  spanning-tree vlan 2 root primary |

**SW3 :**

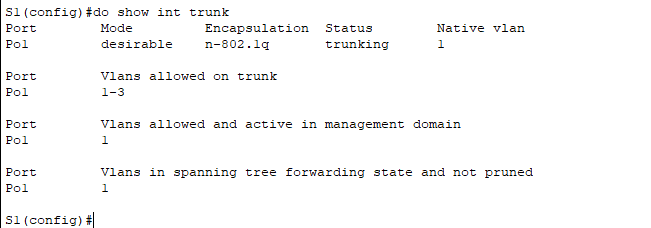
|  |
| --- |
| interface FastEthernet0/5  channel-group 2 mode passive  switchport trunk native vlan 2  switchport mode dynamic desirable  interface FastEthernet0/6  channel-group 2 mode passive  switchport trunk native vlan 2  switchport mode dynamic desirable  interface FastEthernet0/7  channel-group 2 mode passive  switchport trunk native vlan 2  switchport mode dynamic desirable  interface FastEthernet0/8  channel-group 3 mode on  switchport trunk native vlan 3  switchport mode trunk  interface FastEthernet0/9  channel-group 3 mode on  switchport trunk native vlan 3  switchport mode trunk  interface FastEthernet0/10  channel-group 3 mode on  switchport trunk native vlan 3  switchport mode trunk  interface Port-channel 2  switchport trunk native vlan 2  interface Port-channel 3  switchport trunk native vlan 3  spanning-tree vlan 3 root primary |

Cette configuration complète rassemble toutes les commandes nécessaires pour **SW1**, **SW2**, et **SW3** avec l’agrégation de liens (**PAgP**, **LACP**, et mode **on**), le paramétrage des trunks et des VLANs natifs, ainsi que la configuration de **STP** pour désigner le root bridge pour chaque VLAN.

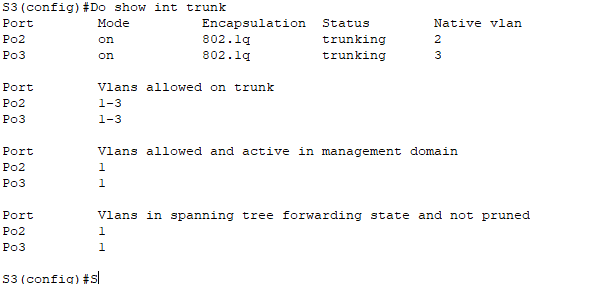
## Vérifions le trunking :

**SW1 :**

Do show int trunk

****

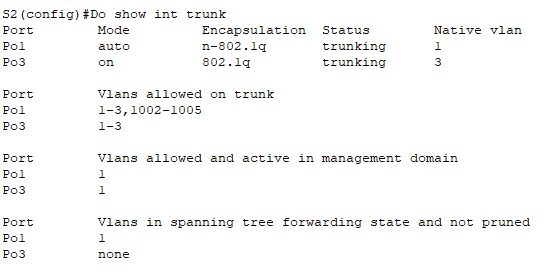
**SW2 :**

****

Do show int trunk

**SW3 :**

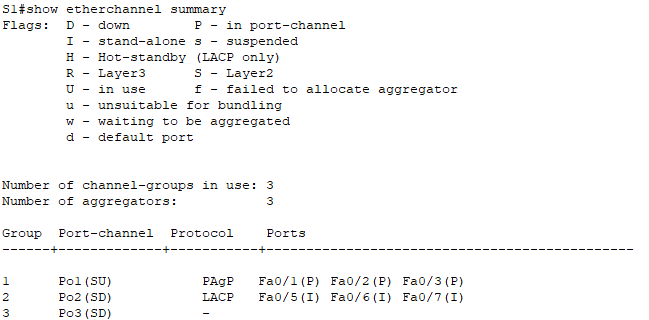
Do show int trunk

****

## Vérifions le fonctionnement de l'EtherChannel :

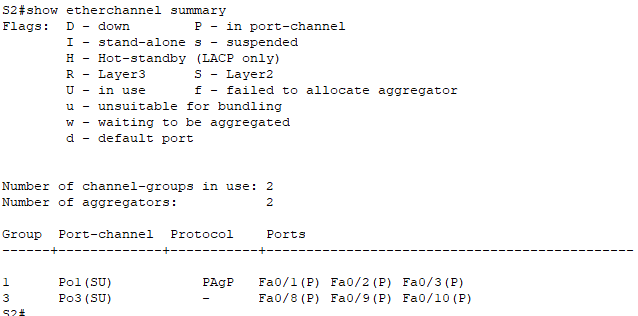
**S1**

Show etherchanel summary

****

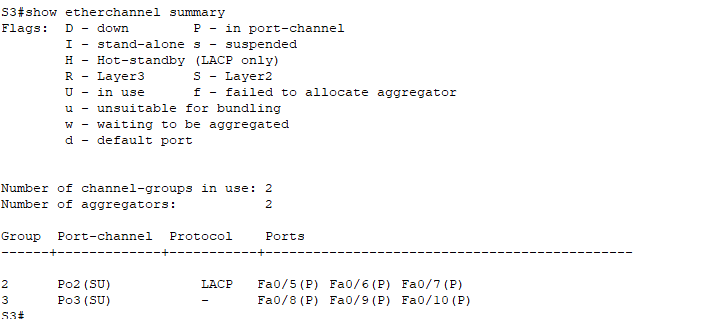
**S2**

Show etherchanel summary

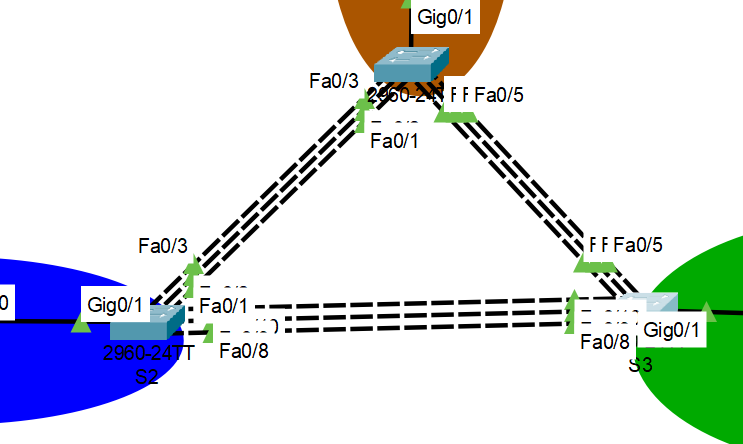
****

**S3**

Show etherchanel summary

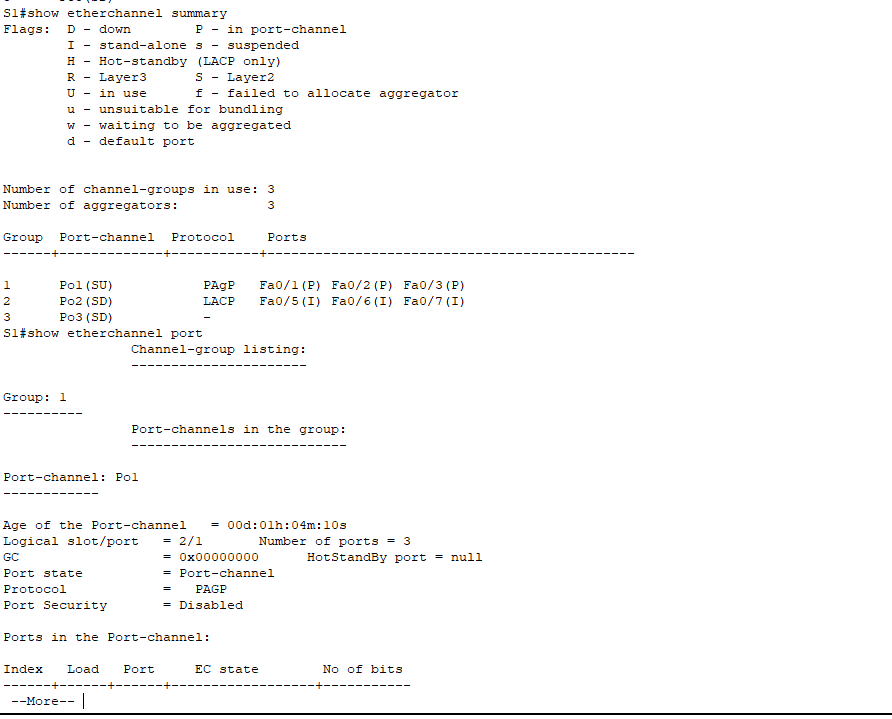
****

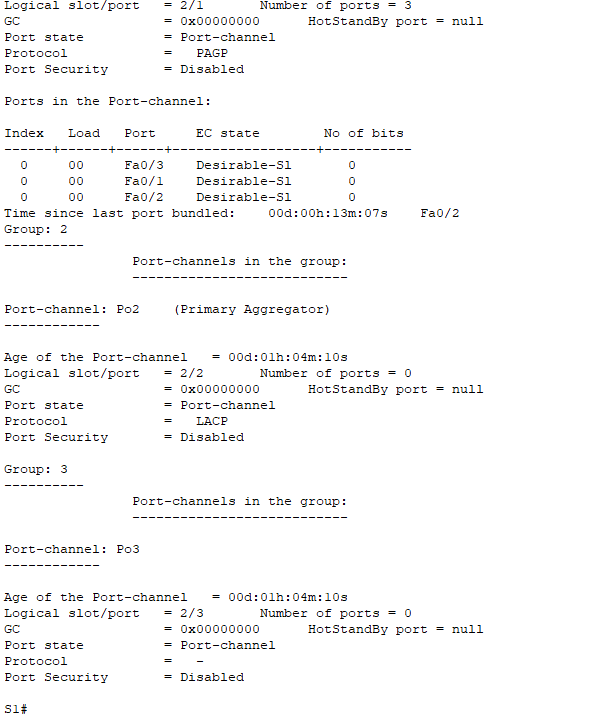
Montrer en quoi ce réseau fonctionne et illustre Etherchannel (protocole, pannes….)

****

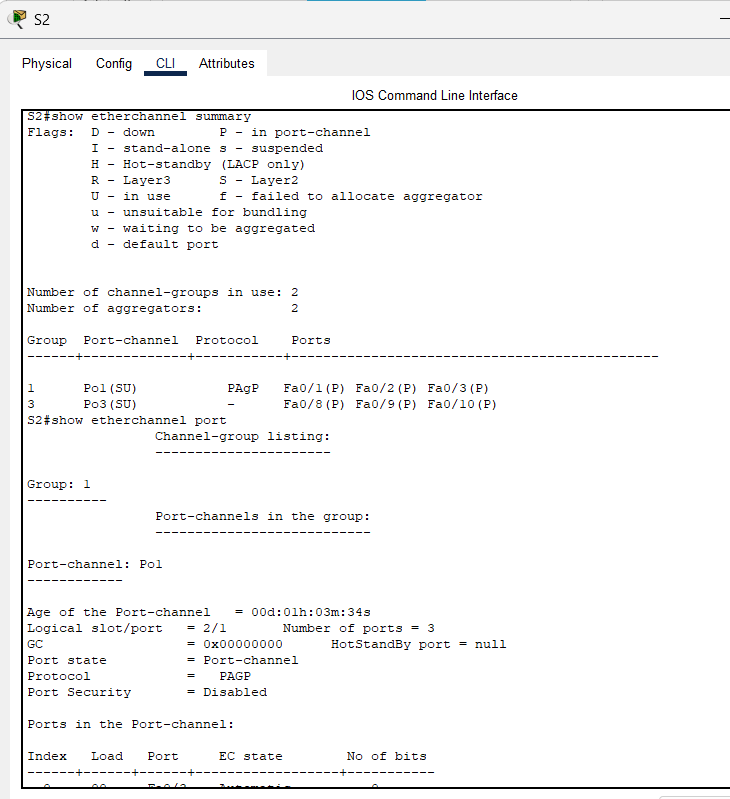
Vérification de la formation des EtherChannels

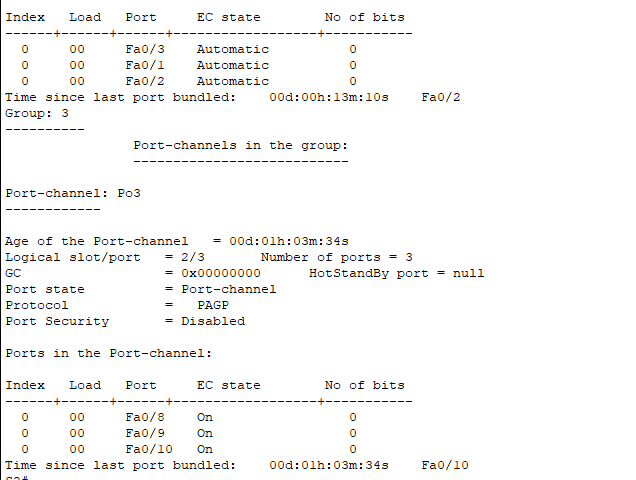
**S1 :**

****

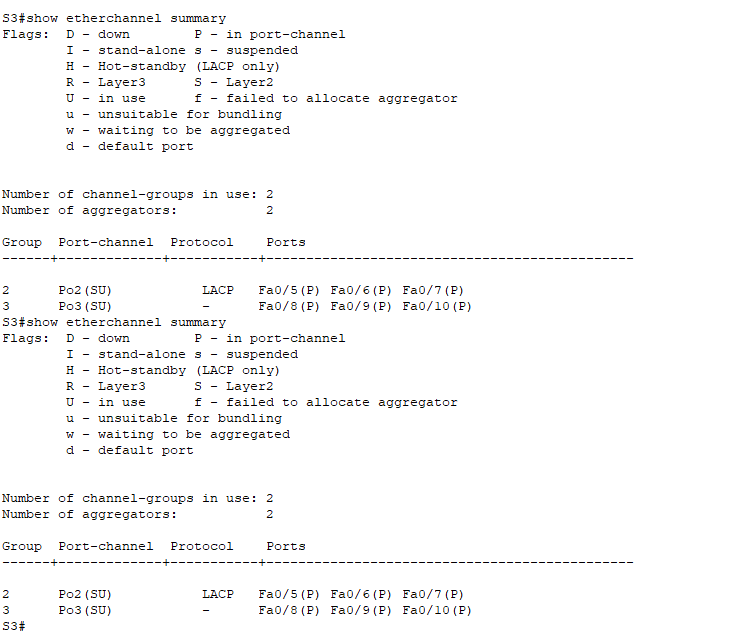
****

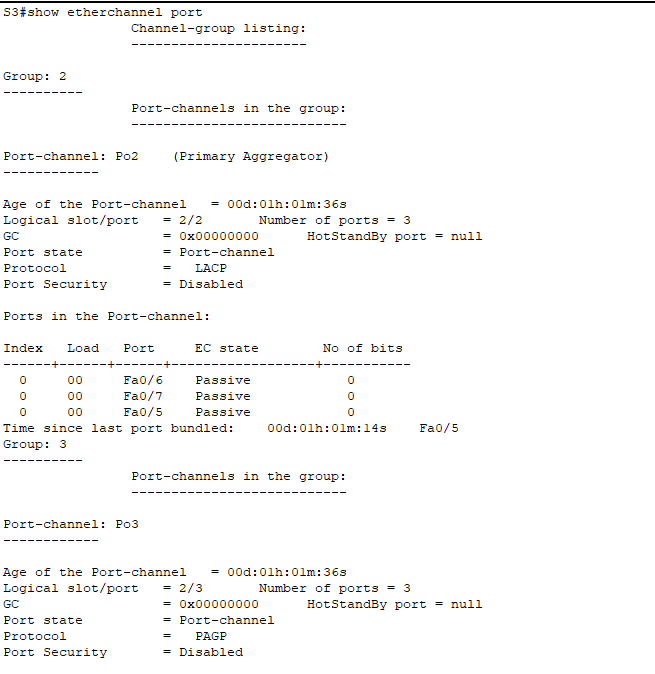
**S2 :**

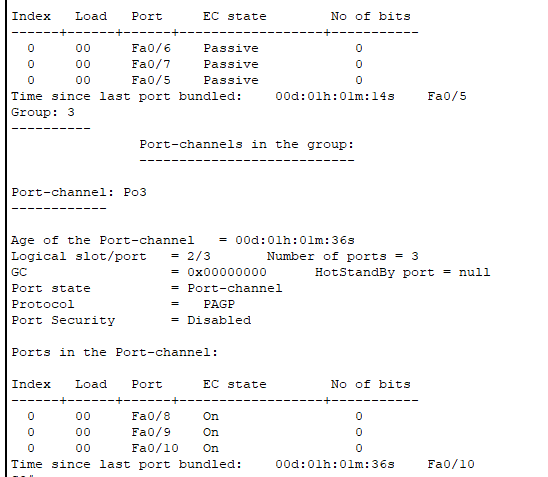
****

****

**S3 :**

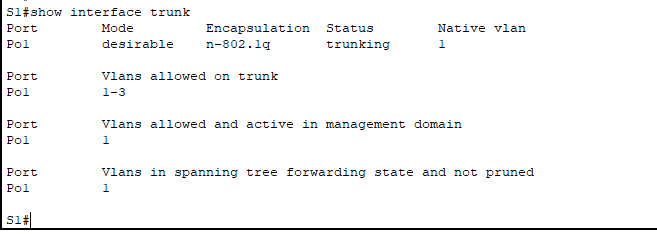
****

****

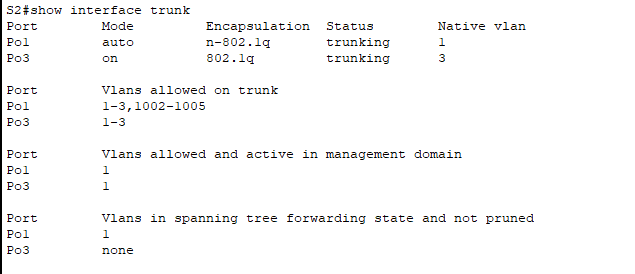
****

Vérification des trunks et VLAN natifs

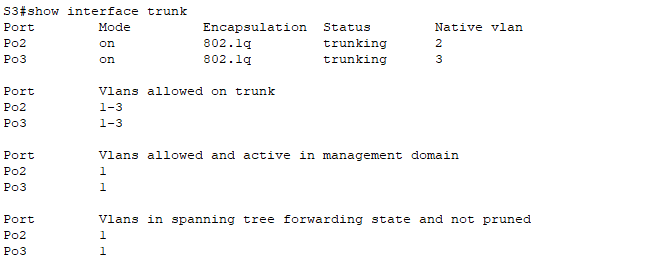
S1

****

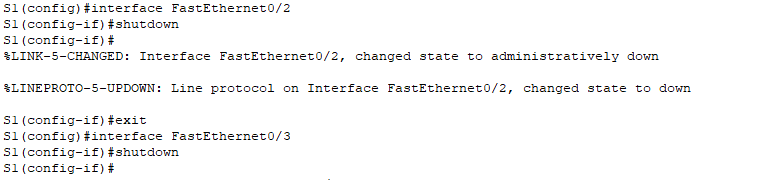
S2

****

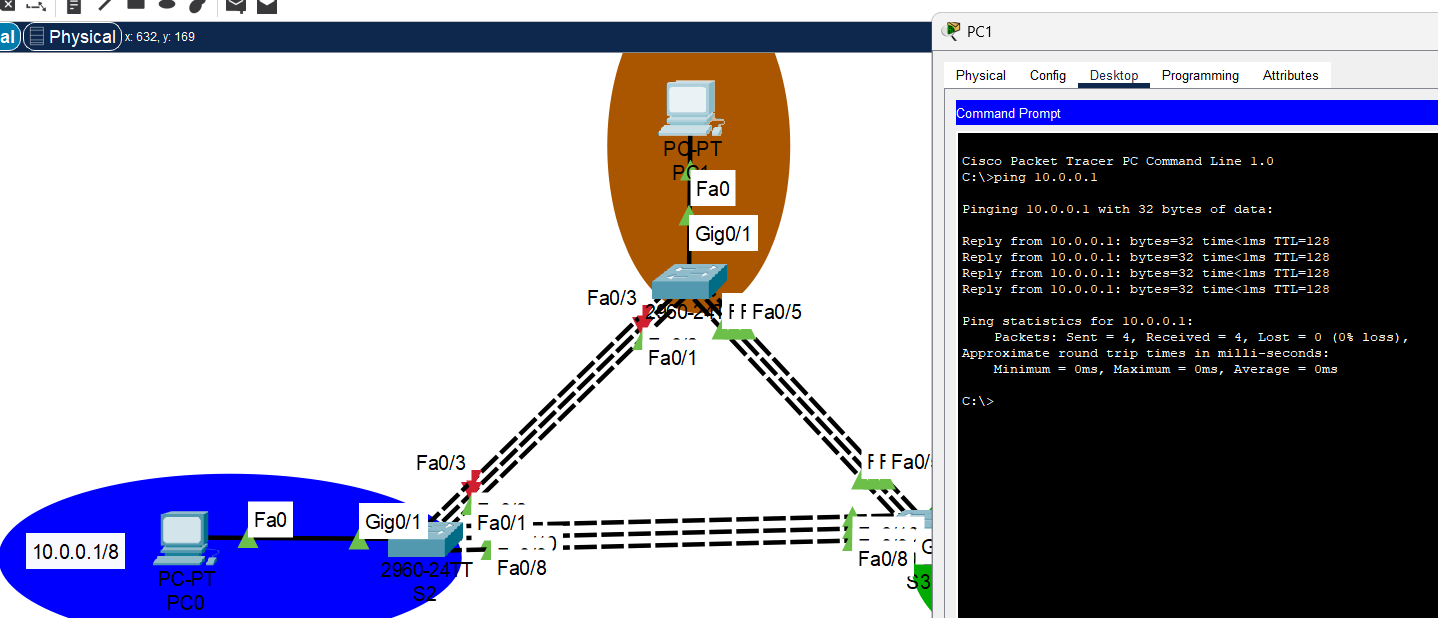
**S3**

****

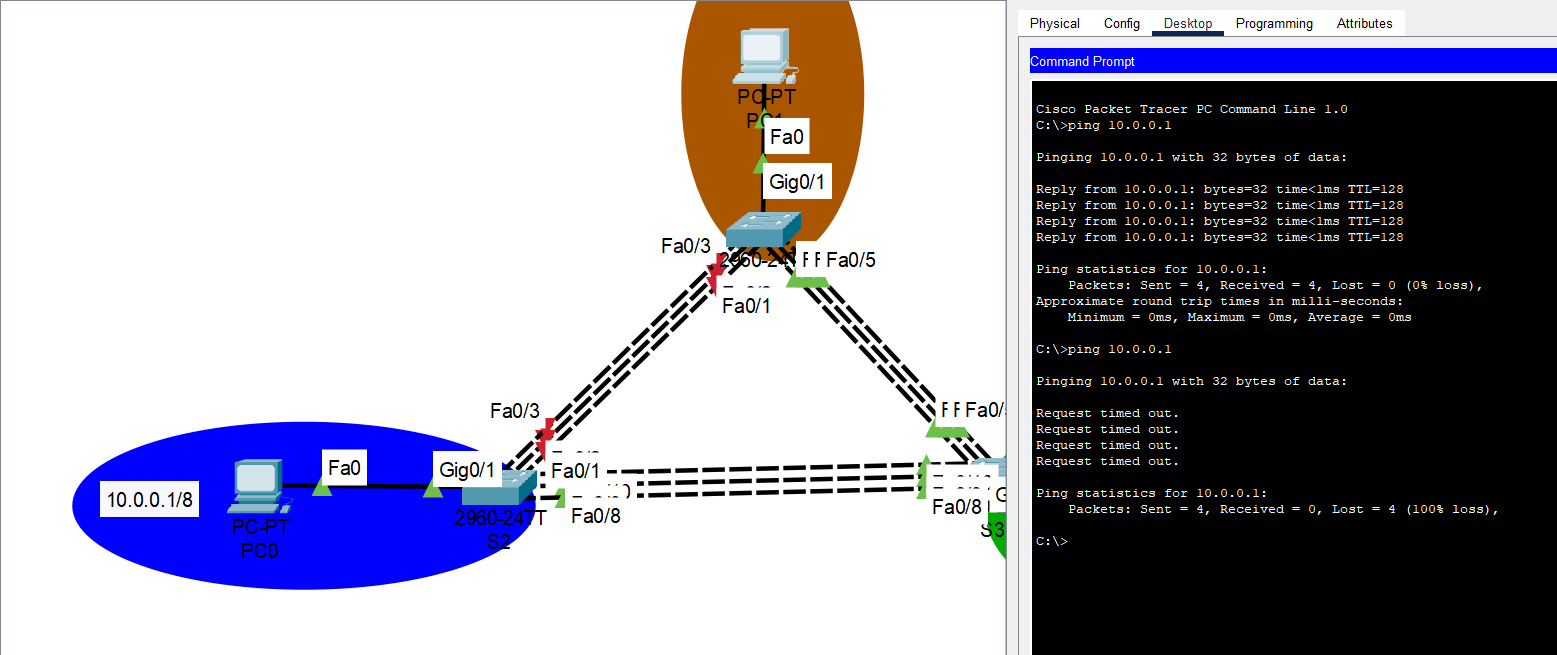
Puisque l’EtherChannel permet la tolérance aux pannes, nous allons tester la résilience en cas de panne physique.

****

Nous avons désactivé les interfaces FastEthernet0/2 et FastEthernet0/3 de S1 en utilisant la commande shutdown. Cela simule une panne physique de ces liaisons.

****

Nous observons le résultat du ping depuis PC1 vers l'adresse 10.0.0.1. Malgré la désactivation des interfaces sur S1, les pings fonctionnent toujours correctement.

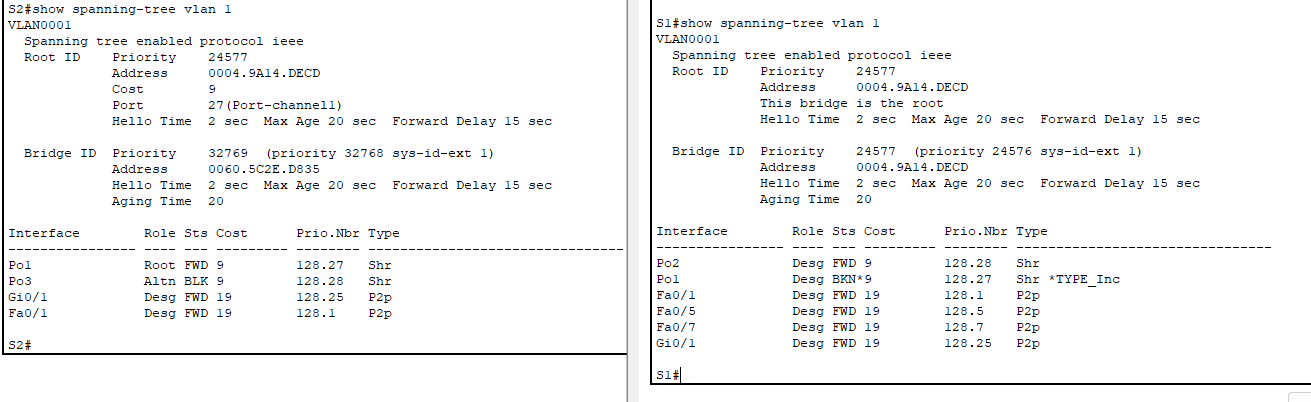


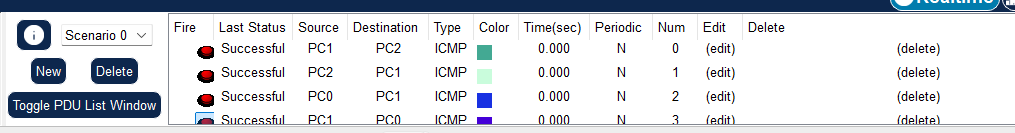
Dans cette simulation, après avoir coupé toutes les interfaces de l'**EtherChannel**, la connexion est complètement interrompue, comme le montrent les **pings échoués** depuis **PC1** vers **10.0.0.1**.

**Explication :**

* Lorsque toutes les interfaces de l'**EtherChannel** sont désactivées, il n'y a plus de chemin alternatif disponible pour le trafic.
* Cela est **normal** compte tenu de notre configuration actuelle, qui repose uniquement sur ces interfaces pour la redondance. Sans elles, le réseau ne peut pas rediriger le trafic.

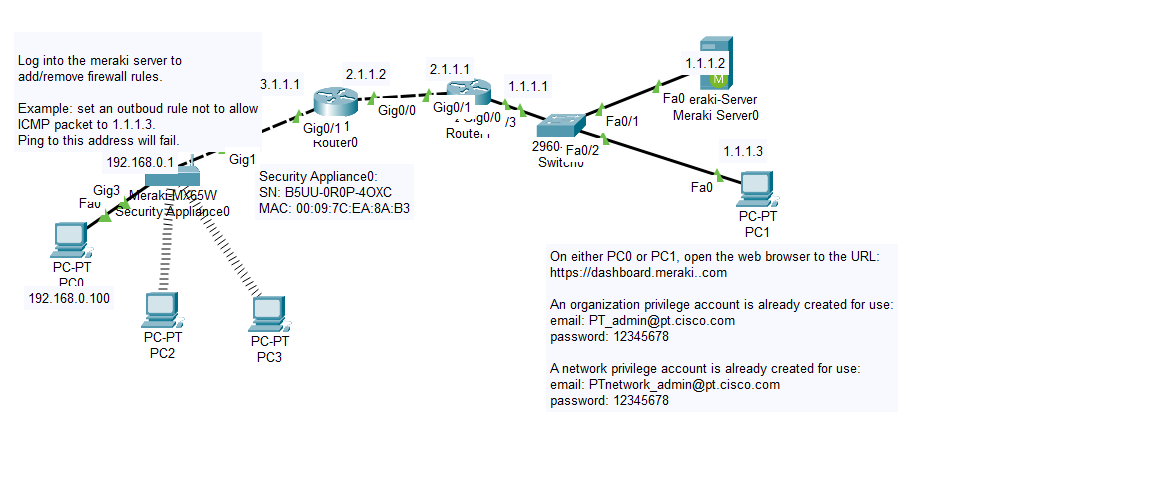
Pour éviter cela, il faudrait ajouter des chemins redondants supplémentaires ou configurer des liaisons alternatives pour garantir une tolérance aux pannes complète.

Les résultats de la commande **show spanning-tree vlan 1** sur **S2** (à gauche) et **S1** (à droite). **S1** est le root bridge pour le **VLAN 1**, comme l'indiquent son adresse MAC **0040.94A1.DECD** et sa priorité de **24577**. Sur **S2**, le chemin principal vers le root bridge passe par **Port-channel 1** (Po1), qui est en état **Root FWD** avec un coût de **9**, tandis que **Port-channel 3** (Po3) est en état **Altn BLK** pour éviter une boucle. Les autres interfaces sur **S1** et **S2** sont en mode **Desg FWD**, ce qui signifie qu'elles transmettent le trafic normalement. Cela confirme que le **Spanning Tree Protocol (STP)** fonctionne correctement pour garantir la redondance et éviter les boucles dans le réseau.

Scenario 

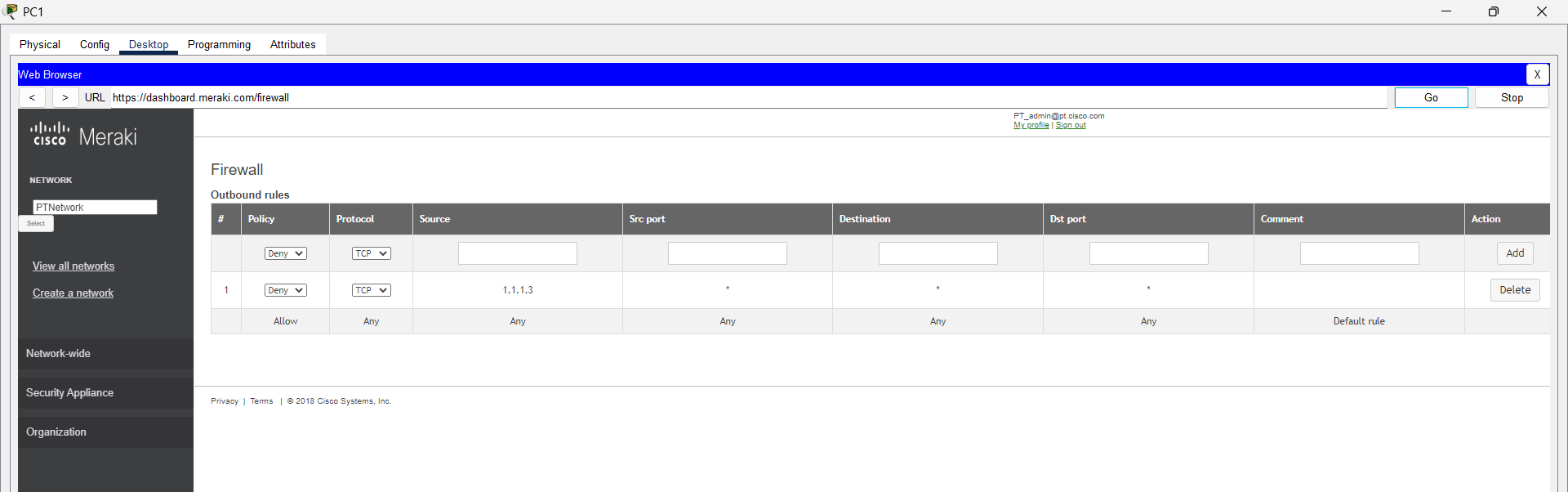
Nous avons mis en place une infrastructure réseau robuste en utilisant des mécanismes de redondance et d'agrégation de liens avec **EtherChannel** (PAgP, LACP et mode statique) pour assurer une meilleure résilience face aux pannes physiques. Grâce à l’utilisation du **Spanning Tree Protocol (STP)**, nous avons évité les boucles réseau tout en optimisant le trafic avec des root bridges désignés pour chaque VLAN. Cette configuration garantit une continuité de service et une tolérance aux pannes, permettant au réseau de s'adapter dynamiquement en cas de défaillance de liens. Ainsi, nous avons créé un environnement réseau fiable, résilient et performant, illustrant l'importance des bonnes pratiques de redondance dans une architecture LAN.

# SD-WAN



La première capture illustre une infrastructure réseau utilisant un appliance Cisco Meraki pour la gestion centralisée des dispositifs de sécurité et de connectivité. Cisco Meraki permet de gérer les pare-feu, les switches et les points d’accès via une interface cloud centralisée accessible à l’URL https://dashboard.meraki.com. Dans cette configuration, les utilisateurs peuvent ajouter ou supprimer des règles de pare-feu, configurer des politiques de sécurité et surveiller le trafic réseau en temps réel.

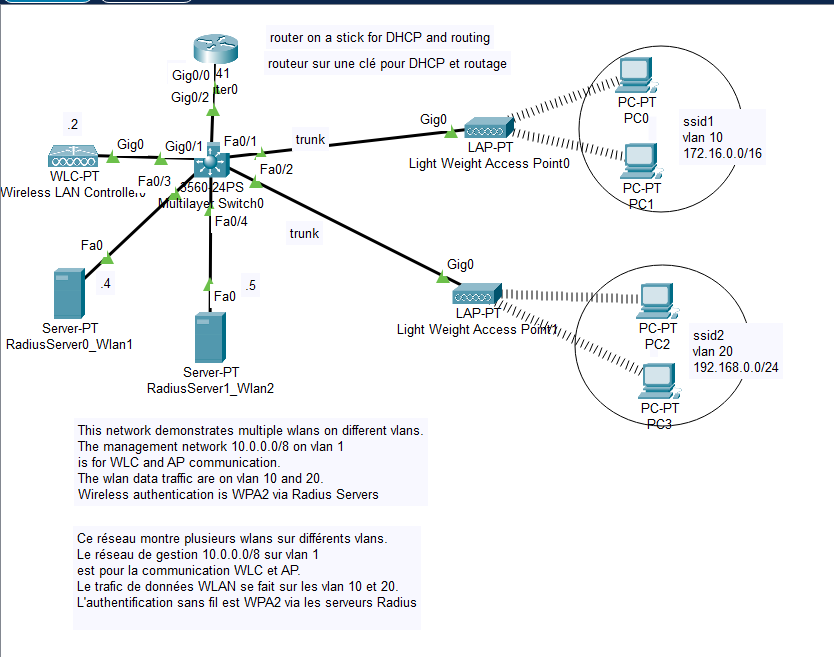
Le réseau comprend plusieurs PC connectés à l'appliance Meraki et un serveur Meraki. Les adresses IP attribuées montrent une segmentation claire du réseau. Le rôle de l'appliance est de filtrer le trafic et d'appliquer des politiques de sécurité en fonction des besoins, assurant une protection efficace contre les menaces et le contrôle des flux de données.



La deuxième capture montre l'interface de gestion du pare-feu Cisco Meraki via le tableau de bord cloud. Une **règle de pare-feu sortante** a été ajoutée pour **bloquer le trafic ICMP** (ping) vers l’adresse **1.1.1.3**. La configuration de cette règle inclut :

* **Policy :** Deny (Bloquer)
* **Protocol :** TCP (bien que pour un blocage ICMP, il aurait été préférable d’utiliser ICMP directement)
* **Source :** 1.1.1.3
* **Destination :** Toutes adresses (\*)

Cependant, sur **Packet Tracer**, Cisco Meraki ne fonctionne pas réellement. Son utilisation est purement **visuelle** et **simulationnelle**, mais aucune action ou traitement réel ne se produit dans le réseau simulé.

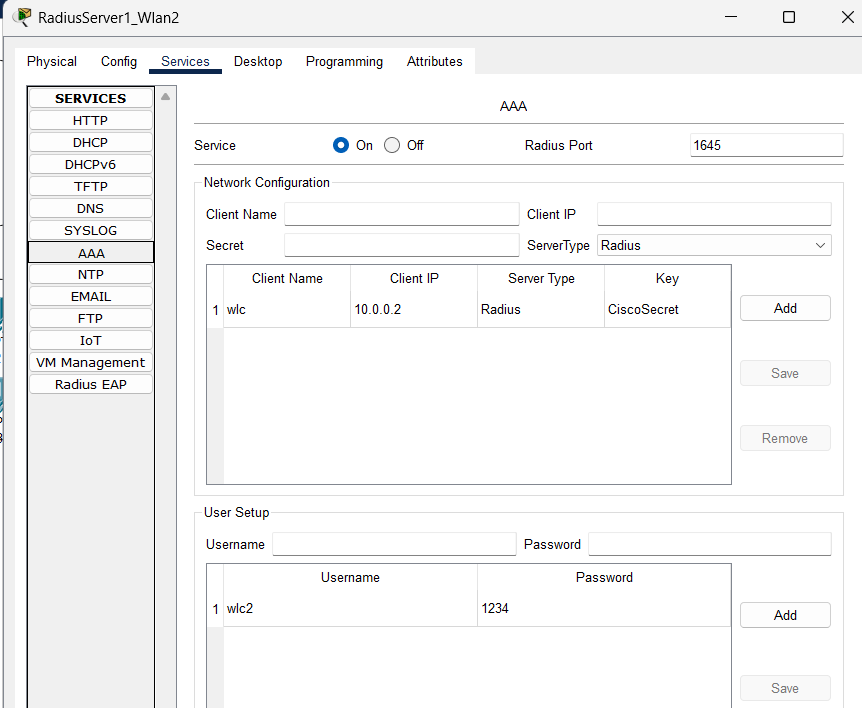
 **Multilayer Switch0**

|  |
| --- |
| version 12.2(37)SE1  no service timestamps log datetime msec  no service timestamps debug datetime msec  no service password-encryption  hostname Switch  spanning-tree mode pvst  interface FastEthernet0/1  switchport trunk encapsulation dot1q  switchport mode trunk  interface FastEthernet0/2  switchport trunk encapsulation dot1q  switchport mode trunk  interface FastEthernet0/3  interface FastEthernet0/4  interface FastEthernet0/5  interface FastEthernet0/6  interface FastEthernet0/7  interface FastEthernet0/8  interface FastEthernet0/9  interface FastEthernet0/10  interface FastEthernet0/11  interface FastEthernet0/12  interface FastEthernet0/13  interface FastEthernet0/14  interface FastEthernet0/15  interface FastEthernet0/16  interface FastEthernet0/17  interface FastEthernet0/18  interface FastEthernet0/19  interface FastEthernet0/20  interface FastEthernet0/21  interface FastEthernet0/22  interface FastEthernet0/23  interface FastEthernet0/24  interface GigabitEthernet0/1  switchport trunk encapsulation dot1q  switchport mode access  interface GigabitEthernet0/2  switchport trunk encapsulation dot1q  switchport mode trunk  interface Vlan1  no ip address  ip classless  ip flow-export version 9  line con 0  line aux 0  line vty 0 4  login  end |

Configuration des radius :

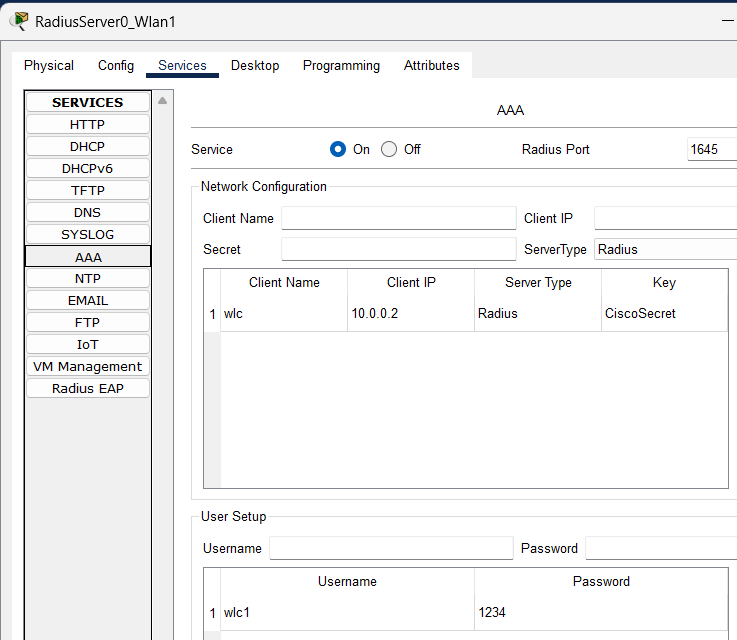
Radius 1:

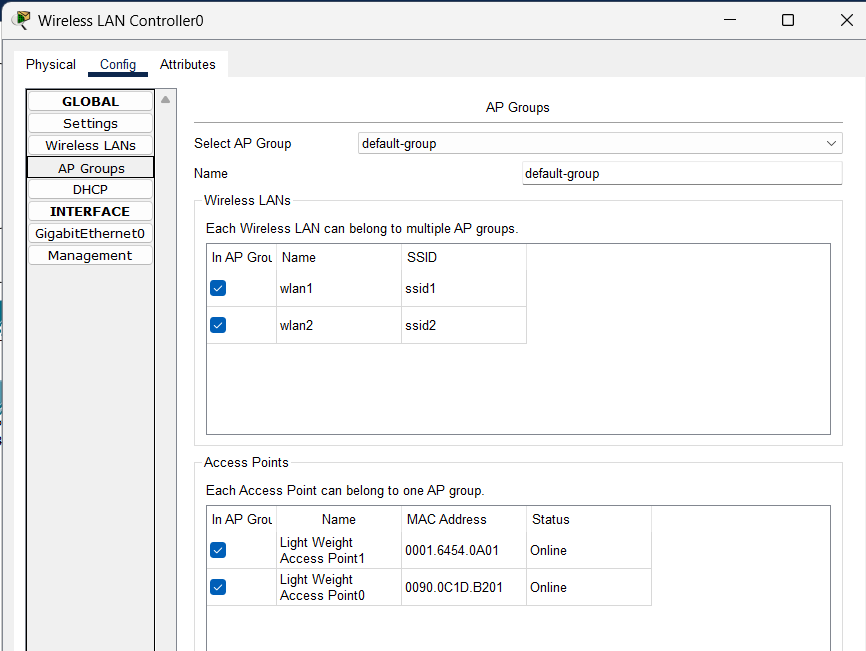
Je configure le serveur RADIUS en activant le service et en précisant le port RADIUS (1645). Je saisis ensuite le nom du client (ex. “wlc”) et son adresse IP, ainsi qu’un secret partagé. Cela permet d’authentifier de manière sécurisée la borne WLAN ou le contrôleur WLAN qui se connectera au serveur. Je définis également un compte utilisateur avec nom et mot de passe afin que le serveur puisse valider les identifiants lors de la connexion Wi-Fi.



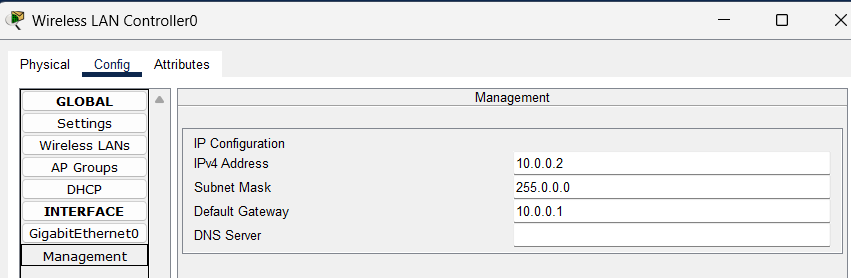
Radius 2:

Ici, je configure un second serveur RADIUS ou un autre profil similaire. Je vérifie que le service est actif, le port correct, et j’ajoute un client avec une clé secrète. L’objectif est de garantir l’authentification des utilisateurs et la cohérence de la sécurité du réseau sans fil, en ayant éventuellement un second serveur pour assurer la redondance ou un domaine d’authentification différent.

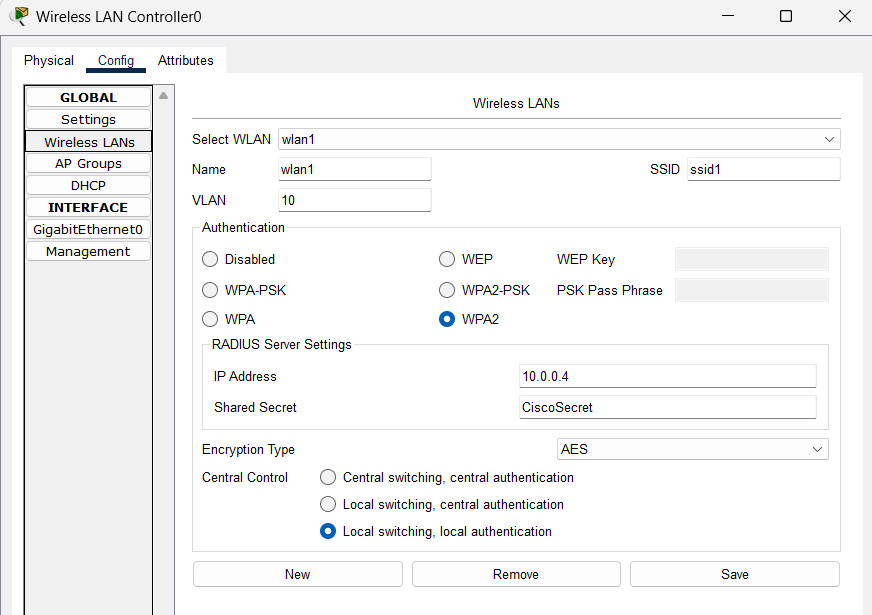




Je me trouve sur le contrôleur WLAN et j’associe des points d’accès à des groupes AP, ainsi que des SSID à ces groupes. Je coche les cases pour inclure les réseaux sans fil (wlan1, wlan2) dans le groupe par défaut. Cela me permet de regrouper et de déployer facilement plusieurs SSID sur les points d’accès sélectionnés et d’assurer une gestion cohérente des réseaux Wi-Fi.



Je renseigne la configuration IP du contrôleur WLAN, incluant l’adresse IP, le masque de sous-réseau, la passerelle par défaut et le serveur DNS. Cela garantit que le contrôleur est correctement positionné sur le réseau, peut communiquer avec les autres équipements (comme le serveur RADIUS) et fournir les services de gestion aux bornes Wi-Fi.



Je configure un réseau sans fil (wlan1) avec le SSID correspondant, en choisissant la méthode d’authentification (WPA2) et en indiquant l’adresse IP du serveur RADIUS ainsi que le secret partagé. Le choix de WPA2 et l’utilisation du RADIUS renforcent la sécurité de l’authentification et du chiffrement des données, assurant un accès Wi-Fi fiable et protégé.

# Conclusion :

L’adoption de l’EtherChannel et du protocole HSRP dans le cadre d’une architecture réseau professionnelle apporte une réelle valeur ajoutée en termes de disponibilité et de performance. En conjuguant agrégation des liens, équilibrage de charge et redondance, ces technologies garantissent une continuité de service même en présence de pannes ou d’interventions de maintenance. Les utilisateurs bénéficient ainsi d’une expérience optimale, tandis que l’entreprise préserve la fluidité de ses opérations et limite les risques liés aux interruptions de réseau.

# Source :

 **Configuration de l'EtherChannel sur les commutateurs Cisco avec LACP et PAgP** : Cet article offre une explication détaillée sur la configuration de l'EtherChannel en utilisant les protocoles LACP et PAgP sur les commutateurs Cisco. Il couvre les avantages de l'EtherChannel, les scénarios d'utilisation, ainsi que des exemples de configuration.

[Réseau Formations](https://www.networkstraining.com/cisco-switch-etherchannel-configuration/?utm_source=chatgpt.com)

 **Configuration des EtherChannels - Cisco** : Cette documentation officielle de Cisco fournit des instructions complètes sur la configuration des EtherChannels, y compris l'utilisation des protocoles PAgP et LACP, les directives de configuration et les considérations relatives au Spanning Tree Protocol.

[Cisco](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-7/configuration_guide/lyr2/b_177_lyr2_9300_cg/configuring_etherchannels.html?utm_source=chatgpt.com)

 **EtherChannel sous Cisco avec LACP** : Cet article explique comment configurer l'EtherChannel en utilisant le protocole LACP sur les commutateurs Cisco. Il aborde les modes de LACP, la configuration des VLANs autorisés et natifs, ainsi que des commandes pour vérifier l'état de l'EtherChannel.

[IT Connect](https://www.it-connect.fr/etherchannel-sous-cisco-avec-lacp/?utm_source=chatgpt.com)

 **Configuration de l'EtherChannel LACP sur un commutateur Cisco IOS** : Ce guide pratique montre les étapes pour configurer un EtherChannel en utilisant LACP sur un commutateur Cisco IOS, avec des exemples de configuration et des explications sur les modes actif et passif de LACP.

[Must Be Geek](https://www.mustbegeek.com/configure-lacp-etherchannel-in-cisco-ios-switch/?utm_source=chatgpt.com)

 **EtherChannel - Wikipédia** : Cette page offre une vue d'ensemble de la technologie EtherChannel, y compris son historique, ses avantages, ses limitations et ses composants. Elle compare également EtherChannel avec la norme IEEE 802.3ad.

[Wikipédia](https://en.wikipedia.org/wiki/EtherChannel?utm_source=chatgpt.com)

https://cisco.goffinet.org/ccna/redondance-de-liens/cisco-etherchannel-configuration-

verification-depannage/#:~:text=EtherChannel%20(IEEE%20802.3ad)%20est,en%20un%20seul%20lien%20logique.